NIST Special Publication
NIST SP 800-161r1

システム及び組織におけるサプライチェーンのサイバーセキュリティリスクマネジメントのプラクティス

Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication
NIST SP 800-161r1

システム及び組織におけるサプライチェーンのサイバーセキュリティリスクマネジメントのプラクティス

Jon Boyens
Angela Smith
Computer Security Division
Information Technology Laboratory

Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon
Boston Consulting Group

本出版物は、https://doi.org/10.6028/NIST.SP.800-161r1 から無料で入手可能である。

2022 年 5 月

米国商務省
長官 *Gina M. Raimondo*

米国国立標準技術研究所
所長兼標準技術担当次官 *Laurie E. Locascio*

発行機関

本出版物は、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が 2014 年の連邦情報セキュリティ近代化法（FISMA：Federal Information Security Modernization Act）、合衆国法典（U.S.C）第 44 編第 3551 条以下、及び公法（P.L：Public Law）113 条 -283 条に基づく法的責任を果たすために策定したものである。NIST は、連邦政府情報システムに対する最低限の要件を含んだ情報セキュリティ標準及びガイドラインを策定する責務を負う。そうした標準及びガイドラインは、国家安全保障システムにおいては、それらのシステムに対して政策権限を行使する適切な連邦政府担当官の明示的な承認なしに適用してはならない。このガイドラインは、行政管理予算局（OMB：Office of Management and Budget）による通達（Circular）A-130 号の要件と一致している。

本出版物のいかなる内容も、法的権限の下で商務長官（Secretary of Commerce）が連邦政府機関に順守を義務付けた標準及びガイドラインを否定するものと解釈されることは望ましくない。また、これらのガイドラインは、商務長官、行政管理予算局長（Director of the OMB）、又はその他の連邦政府担当官の既存の権限を変更するもの、又はそれらに代わるものと解釈されることは望ましくない。本出版物は、非政府組織が自由に使用してもよく、米国における著作権の対象外であるが、NIST に帰属する。

米国国立標準技術研究所、特別出版物（Special Publication）800-161 改訂第 1 版
NIST SP 800-161r1、全 326 ページ（2022 年 5 月）
CODEN：NSPUE2

本出版物は、https://doi.org/10.6028/NIST.SP.800-161r1 から無料で入手可能である。

本出版物では、試行的手順や概念を適切に説明するために、特定の商業エンティティ、機器、又は資料が記載されている場合がある。そうした記載は、NIST による推奨又は承認を意図するものではなく、それらのエンティティ、機器、又は資料が、必ずしも目的のために利用できる最良のものであるということを意図するものでもない。

本出版物では、NIST が担う法的責任に従って現在策定している他の出版物を参照する場合がある。概念及び方法論を含む本出版物に記載された情報は、そのような関連出版物の完成前であっても、連邦政府機関によって使用されることがある。したがって、各出版物が完成するまでの間、現行の要件、ガイドライン、及び手順が存在する場合は、それらは引き続き有効である。計画の策定及び移行のために、連邦政府機関は、NIST によるそうした新たな出版物策定の進展を綿密に追うことが望まれる。

各組織は、パブリックコメント期間中にすべてのドラフト出版物をレビューし、NIST にフィードバックを提供することが推奨される。上記の出版物に加え、多くの NIST サイバーセキュリティ関連出版物が https://csrc.nist.gov/publications から入手可能である。

本出版物に対する意見の送付先：scrm-nist@nist.gov
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

寄せられたすべての意見は、
情報公開法（FOIA：Freedom of Information Act）に基づき公開対象である。

コンピュータシステム技術に関する報告

米国国立標準技術研究所（NIST）の情報技術研究所（ITL：Information Technology Laboratory）は、米国の計量と標準に関するインフラにおいて技術的リーダーシップを発揮することにより、米国経済と公共福祉を発展させている。また、ITL は、試験、試験方法、参照データ、概念実証の実施、及び技術分析を開発し、情報技術の開発と生産的利用を促進している。ITL の責務には、連邦政府情報システムにおける国家安全保障関連情報以外の情報を対象とした、費用対効果の高いセキュリティ及びプライバシーのための管理上、行政上、技術的、及び物理的な標準とガイドラインを策定することが含まれる。Special Publication 800 シリーズでは、情報システムセキュリティに関する ITL の研究、ガイドライン、及び普及の取り組み、並びに産業界、政府、及び学術機関との共同活動について報告している。

概要

組織は、悪意のある機能が潜在的に含まれている可能性のある製品及びサービス、偽の製品及びサービス、あるいはサプライチェーンにおける稚拙な製造手法及び開発慣行が原因で脆弱性を有する製品及びサービスに関連するリスクについて懸念している。これらのリスクは、自らが取得する技術がどのように開発、統合、及び展開されているか、又は製品及びサービスのセキュリティ、レジリエンス、信頼性、安全性、完全性、及び品質を確実にするために使用されるプロセス、手順、標準及びプラクティスについての事業体の可視性及び理解の低下に関連している。

本出版物は、組織のすべてのレベルでサプライチェーン全体のサイバーセキュリティリスクを識別すること、アセスメントすること、及び軽減することに関するガイダンスを組織に提供する。本出版物では、サプライチェーンのサイバーセキュリティリスクマネジメント（C-SCRM）戦略の実施計画、C-SCRM ポリシー、C-SCRM 計画、及び製品及びサービスのリスクアセスメントの策定に関するガイダンスを含む、マルチレベルの C-SCRM 特有のアプローチを適用することによって、C-SCRM をリスクマネジメント活動に統合している。

キーワード

取得、C-SCRM、サイバーセキュリティサプライチェーン、サプライチェーンのサイバーセキュリティリスクマネジメント、情報通信技術、リスクマネジメント、サプライヤ、サプライチェーン、サプライチェーンのリスクアセスメント、サプライチェーンアシュアランス、サプライチェーンリスク、サプライチェーンセキュリティ

謝辞

著者一同 – Jon Boyens（NIST：米国国立標準技術研究所）、Angela Smith（NIST）、Nadya Bartol（BCG：Boston Consulting Group）、Kris Winkler（BCG）、Alex Holbrook（BCG）、及び Matthew Fallon（BCG） – より、Alexander Nelson（NIST）、Murugiah Souppaya（NIST）、Paul Black（NIST）、Victoria Pillitteri（NIST）、Kevin Stine（NIST）、Stephen Quinn（NIST）、Nahla Ivy（NIST）、Isabel Van Wyk（NIST）、Jim Foti（NIST）、Matthew Barrett（Cyber ESI）、Greg Witte（Huntington Ingalls）、R.K. Gardner（New World Technology Partners）、David A. Wheeler（Linux Foundation）、Karen Scarfone（Scarfone Cybersecurity）、Natalie Lehr-Lopez（ODNI/NCSC）、Halley Farrell（BCG）の各氏、並びに、NIST SP 800-161 の最初の著者である Celia Paulsen（NIST）、Rama Moorthy（Hatha Systems）、及び Stephanie Shankles（米国退役軍人省（U.S. Department of Veterans Affairs））の貢献に感謝の意を表する。また、サプライチェーンの管理に関する貴重な洞察及び多様な視点を提供してくれた C-SCRM コミュニティにも感謝したい。特に、2015 年の公開以降、NIST SP 800-161 の実装に関する経験及び文書を共有してくれた各省庁及び関係機関、並びに、附属書 F への意見の提供に協力してくれた、高耐久性セキュリティフレームワーク（Enduring Security Framework）の公共及び民間メンバーに感謝している。

特許開示に関する通知

通知：情報技術研究所（*ITL*）は、本出版物のガイダンス又は要件に準拠するために使用が必要となる可能性のある特許請求項の所有者に対して、そうした特許請求項を *ITL* に開示するよう要請している。ただし、特許所有者は、*ITL* の要請に応じる義務はなく、*ITL* は、本出版物に適用される可能性のある特許を特定するための特許調査を実施していない。

本出版物の公開日において、及び、本出版物のガイダンス又は要件に準拠するために使用が必要となる可能性のある特許請求項を特定するよう要請を行った時点において、*ITL* はそうした特許請求項を特定していない。

ITL は、本出版物の使用に際して特許侵害を回避するためにライセンス許諾が不要であるという表明、又は暗示していない。

目次

図

表

1. はじめに

情報通信技術（ICT）及び制御・運用技術（OT）は、地理的に多様なルートから成り、複数の階層による外部委託で構成される、複雑でグローバルに分散され、広範囲に及ぶ、相互接続されたサプライチェーンエコシステムに依存している。このエコシステムは、ICT/OT 製品及びサービスの研究、開発、設計、製造、取得、納入、統合、運用、保守、廃棄、及びその他の利用又は管理のために相互作用する公共及び民間分野のエンティティ（例えば、取得者、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダ）[1]で構成されている。これらの相互作用は、一連の技術、法律、ポリシー、手順及びプラクティスによって形成され、それらの影響を受ける。

このエコシステムは、高度に洗練され、費用対効果が高く、再利用可能な一連のソリューションを提供するまでに進化してきた。公共及び民間分野のエンティティは、このソリューションエコシステムを急速に採用し、市販製品、特注のシステムに対するシステムインテグレータのサポート、及び外部サービスプロバイダへの依存度を高めてきた。その結果、これらのエンティティの複雑さ、多様性、及び規模が増大している。

本出版物内で**サプライチェーン**という用語は、製品及びサービスの調達から始まり、製品及びサービスのライフサイクルを通じて拡張される、各々が取得者である事業体の複数の階層間におけるリソースとプロセスの一連の結びつきを指す。

このサプライチェーンの定義を前提とすると、**サプライチェーン全体のサイバーセキュリティリスク** [2, 3]とは、サプライヤ、そのサプライチェーン、その製品、そのサービスから発生する可能性のある損害又は侵害の可能性を指す。サプライチェーン全体のサイバーセキュリティリスクは、サプライチェーンを経由する製品及びサービス内の脆弱性又は曝露（エクスポージャー）を悪用する脅威、又は、サプライチェーン自体内の脆弱性又は曝露（エクスポージャー）を悪用する脅威の結果である。サプライチェーン全体のサイバーセキュリティリスクの例としては、以下のものがある。

1）小型装置の製造業者が、他国で設計資料を盗まれた結果、知的財産と市場シェアを失う。

2）小型装置の製造業者が、サプライチェーンの三階層下のサプライヤがランサムウェアによる攻撃を受けたことにより、重要な製造コンポーネントの供給が停止する。

3）ある店舗チェーンで、自社のデータ共有ポータルにアクセスできる冷暖房空調設備ベンダが関係する大規模なデータブリーチが発生する。

なお、NIST の出版物の目的上、SCRM 及び C-SCRMは同じ概念を指していることに注意されたい。一般的なプラクティスにおいては、C-SCRMは、従来のサプライチェーンのリスクマネジメント（SCRM）と従来の情報セキュリティが結びつく領域にある。

[1] サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの定義については、用語集を参照。

[2] 2015 年版の SP 800-161 では、NIST は「ICT サプライチェーン」という用語を使用した。 サイバーセキュリティリスクは、ICT サプライチェーン及び非技術サプライチェーンの両方を含む、すべての製品及びサービスのサプライチェーンで発生し得るため、今回の改訂版では、この用語を意図的に使用しなくなった。

[3] 用語を合わせるため、本出版物の目的上「サプライチェーンのサイバーセキュリティリスク」という表現は、「サプライチェーンのサイバーリスク」と同義と見なすことが望ましい。 同様に、「サプライチェーンのサイバーセキュリティリスクマネジメント」という表現は、「サプライチェーンのサイバーリスクマネジメント」と同義と見なすことが望ましい。

組織は、本出版物の範囲外で、SCRM に対して異なる用語及び定義を使用しても良い。本出版物では、SCRM のサイバーセキュリティ以外の側面の多くを扱っていない。

複数の競合ベンダのサプライチェーンを通じて提供される技術ソリューションは、低コスト、相互運用性、迅速なイノベーション、製品機能の多様性などの大きな利点をもたらす。これらのソリューションは、プロプライエタリ、政府開発、又はオープンソースのいずれの場合でも、公共及び民間分野の顧客のグローバルな基盤のニーズを満たすことができる。しかし、そのような利点を生むのと同じ要因が、サプライチェーンから直接的又は間接的に生じるサイバーセキュリティリスクの可能性も高める。サプライチェーン全体のサイバーセキュリティリスクは、検知されないことが多く、取得者及びエンドユーザにインパクトを与える。例えば、展開されたソフトウェアは一般的に市販製品（COTS: Commercial-Off-The-Shelf）であり、複数の階層で開発又は調達された小規模の COTS 又はオープンソースソフトウェアコンポーネントが含まれている。事業体全体で展開されたソフトウェアの更新は、既知の脆弱性を持つ小規模 なCOTS コンポーネントを更新できないことが多く、その中には、コンポーネントの脆弱性が大規模な事業体向けソフトウェアで悪用可能である場合も含まれる。ソフトウェアユーザは、大規模な COTS ソフトウェア内の基地の脆弱性を持つ小規模なコンポーネントを検知できない場合がある（例えば、透明性の欠如、不十分な脆弱性管理など）。C-SCRM プラクティスの標準化されていないという性質は、組織とそのサプライチェーンのメンバー（例えば、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダ）の両方にとって、サプライチェーン全体のサイバーセキュリティリスクの一貫した測定及び管理を困難にするため、さらなる複雑性をもたらす。

本出版物で、サプライチェーンのサイバーセキュリティリスクマネジメント（C-SCRM）について説明しているプラクティス及び管理策は、情報技術（IT）環境及び制御・運用技術（OT）環境のどちらにも適用され、IoT も含まれる。ICT 製品及びサービスに依存する IT 環境と同様に、OT 環境も OT 及び ICT の製品及びサービスに依存しており、ICT/OT 製品、サービス、サプライヤ、及びそれらのサプライチェーンから生じるサイバーセキュリティリスクを伴う。
事業体は、OT 関連のサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダを C-SCRM活動の範囲内に含めることが望ましい。

政府機関は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと関わりを持つ際、連邦政府の拠点の広がりと、個々の政府機関が多様で矛盾したC-SCRM要件を実施する可能性が高いことを慎重に考慮することが望ましい。この複雑さを克服するには、省庁間の協調及び協力が必要である。2018 年の連邦調達サプライチェーンセキュリティ法（FASCSA：Federal Acquisition Supply Chain Security Act）の可決は、連邦調達安全保障会議（FASC：Federal Acquisition Security Council）を設立することで、連邦政府の調達活動におけるサプライチェーンセキュリティの問題に対する政府全体としてのアプローチを構築し、この懸念に対処することを目的としていた。FASC は、調整及び情報共有の中心としての機能を果たし、連邦政府の事業体全体の取得プロセス及び調達における C-SCRM に対処する調達セキュリティへの調和されたアプローチとして機能する。さらに同法は、行政管理予算局（OMB：Office of Management and Budget）及び FASC が発行したガイダンスに沿って、政府機関によるサプライチェーンのリスクマネジメントの進捗及び有効性に関する報告を求めることで、SCRM を連邦情報セキュリティ近代化法（FISMA：Federal Information Security Modernization Act）に組み込んだ。

本出版物では、リスクマネジメント階層のレベル 1 を表すために「事業体」という用語を使用していることに留意されたい。実際には、組織は、より大きな事業体構造（例えば、連邦政府機関、又は企業）内のあらゆる規模、複雑さ、又は位置付けのエンティティとして定義されている。この定義によれば、事業体は組織であるが、個々の上級幹部が固有のリスクマネジメント責任を負う、階層の最上位に存在する[NISTIR 8286]。複数の組織が 1つの事業体を構成する場合もある。このような場合、1つの事業体に、ステークホルダー及び活動が事業体レベルと組織レベルの両方で定義された複数のレベル 1 が存在する可能性がある。事業体レベルで実施されるレベル 1 の活動は、下位の組織内で完了された 活動に情報を与えることが望ましい。事業体及び組織は、本出版物に記載されているC-SCRMプラクティスを、それぞれの固有の事業体構造に基づいて、適宜、必要に応じてテーラリングする。本出版物では、「組織」という用語を参考資料（例えば、他の NIST 出版物、規制における用語）から継承している場合がある。このトピックに関する詳細なガイダンスについては、NISTIR 8286「サイバーセキュリティ及びエンタープライズリスクマネジメント（*ERM*）の統合（*Integrating Cybersecurity and Enterprise Risk Management (ERM)*）」を参照のこと。

1.1. 目的

サプライチェーンのサイバーセキュリティリスクマネジメント（C-SCRM）は、サプライチェーン全体のサイバーセキュリティリスクの曝露（エクスポージャー）を管理し、適切な対応戦略、ポリシー、プロセス、及び手順を策定するための体系的なプロセスである。本出版物の目的は、サプライチェーン全体のサイバーセキュリティリスクの管理を支援するために、組織全体でリスクマネジメントプロセス及び軽減管理策の識別、アセスメント、選択、及び実装を行う方法についてのガイダンスを事業体に提供することである。このガイダンスの内容は、SCRM の観点、権限、及び法的考慮事項が異なる様々な分野の共有責任である。

本出版物で提供する C-SCRMガイダンスは、万能ではない。むしろ、本出版物全体にわたるガイダンスは、各事業体の固有の規模、リソース、及びリスク環境に合わせて採用、テーラリングすることが望ましい。このガイダンスを採用する事業体は、C-SCRMプラクティスを内部でどう実装するかという点において異なる可能性がある。そのため、本出版物では、事業体で見られる C-SCRMプラクティスを説明し、事業体が C-SCRM を実装して成熟させる際に考慮するためのC-SCRMプラクティスの一般的な優先順位（すなわち、基本的プラクティス、持続的プラクティス、強化的プラクティス）[4]を提供する。しかし、本出版物は、事業体がケイパビリティ（能力）及び成熟度の様々な状態に到達するために従うべき具体的なロードマップを提供するものではない。

本出版物で特定されたプロセス及び管理策は、ポリシー、ガイドライン、対応戦略、及びその他の情報源からの事業体固有の要件で修正又は拡張することができる。本出版物は、事業体が特定のミッション及びビジネスニーズ、脅威、及び運用環境に合わせてテーラリングされた C-SCRM 戦略を策定することを可能にするものである。

1.2. 対象読者

C-SCRMは、特定の事業体構造に関わらず、ガバナンスの観点から、そのように管理されることが望ましい事業体全体にわたる活動である。

本出版物は、C-SCRMに関わる以下のような多様な読者に役立つことを意図している。

- 認可権限のある担当者（AO）、最高情報責任者、最高情報セキュリティ責任者、プライバシー保護責任者を含む、システム、情報セキュリティ、プライバシー、又はリスクマネジメント及び監督に責任を持つ個人
- ミッション又はビジネスオーナー、プログラムマネージャ、システムエンジニア、システムセキュリティエンジニア、プライバシーエンジニア、ハードウェア及びソフトウェア開発者、システムインテグレータ、取得又は調達担当者を含む、システム開発に責任を持つ個人
- 認定を受けたプロジェクトマネージャ及び／又は統合プロジェクトチーム（IPT）メンバーを含む、プロジェクトマネジメントに関連する責任を持つ個人
- 調達担当者、契約担当者を含む、取得及び調達に関連する責任を持つ個人

[4] 本出版物の第 3.4 節を参照。

- プログラムマネージャ、調達担当者、システムインテグレータ、プロパティマネージャを含む、ロジスティクス又は廃棄に関連する責任を持つ個人

- ミッション又はビジネスオーナー、システム所有者、情報所有者又は情報管理者、システム管理者、ビジネス継続計画者、システムセキュリティ又はプライバシー責任者を含む、セキュリティ及びプライバシーの実装及び運用に責任を持つ個人

- 監査人、監察官、システム評価者、管理策アセッサー（査定者）、独立した検証者及び妥当性確認者、アナリストを含む、セキュリティ及びプライバシーのアセスメント及び監視に責任を持つ個人

- 業界パートナーを含む、コンポーネント製品及びシステムの製造、セキュリティ及びプライバシー技術の開発、あるいは、情報セキュリティ又はプライバシーをサポートするサービス又はケイパビリティ（能力）の提供を行う商業エンティティ

1.3. クラウドサービスプロバイダ向けガイダンス

本出版物で説明する外部システムサービスプロバイダには、クラウドサービスプロバイダが含まれる。本出版物は、クラウドサービスプロバイダのセキュリティに対する連邦政府機関のアセスメントに関して提供されるガイダンスに代わるものではない。本出版物をクラウドサービスプロバイダに適用する場合、連邦政府機関は、まず、米国連邦リスク承認管理プログラム（FedRAMP：Federal Risk and Authorization Management Program）のクラウドサービスセキュリティガイドラインを使用し、次にFedRAMP が対応していないプロセス及び管理策に関して本出版物を適用することが望ましい[5]。

1.4. 読者プロファイル及び本書の利用ガイダンス

本出版物の幅広い読者を考慮して、読者のユースケースに最も密接に関連する本書の節を指し示すために、いくつかの読者プロファイルを定義した。一部の読者は複数のプロファイルに属するだろうから、該当するすべての節を読むことを考慮することが望ましい。事業体内におけるC-SCRMケイパビリティ（能力）又は機能の実装に責任を持つ読者は、役割に関わらず、本出版物全体が自分のユースケースに適用可能と考えることが望ましい。

1.4.1. エンタープライズリスクマネジメント及び C-SCRM のオーナー及び運営者

これらの読者は、エンタープライズリスクマネジメント及びサプライチェーンのサイバーセキュリティリスクマネジメントに責任を持つ人員である。これらの読者は C-SCRMポリシー及び標準の策定を支援したり、サプライチェーン全体のサイバーセキュリティリスクのアセスメントを実施したり、事業体の他の部分の対象分野の専門家としての役割を果たす場合がある。本出版物全体は、このプロファイルに適合する読者に関連しており、推奨される。

1.4.2. 事業体、政府機関、ミッション及びビジネスプロセスのオーナー及び運営者

これらの読者は、事業体内部でリスクを生む、及び／又はリスクを管理する活動に責任を持つ人員である。また、ミッション又はビジネスプロセスにおける自らの職務の一環として、そうしたリスクを負う場合もある。

[5] クラウドサービスに関して、FedRAMP は低インパクト、中インパクト、高インパクトシステムに適用できる[FedRAMP]。
これらの読者は、事業体におけるサプライチェーン全体のサイバーセキュリティリスクの管理に責

任を持つ場合がある。このグループに属する読者は、サプライチェーンのサイバーセキュリティリスクマネジメントに関する一般的な知識及びガイダンスを求めている場合がある。以下の箇所を読むことが推奨される。

- 第 1 節：はじめに
- 第 2 節：事業体全体のリスクマネジメントへの C-SCRMの統合
- 第 3.3 節：C-SCRM意識向上及びトレーニング
- 第 3.4 節：C-SCRMの重要なプラクティス
- 第 3.6 節：専用リソース
- 附属書 A：C-SCRMセキュリティ管理策
- 附属書 B：C-SCRM管理策の概要
- 附属書 E：FASCSA

1.4.3. 取得及び調達のオーナー及び運営者

これらの読者は、事業体の調達又は取得機能における役割の一部として、C-SCRMに責任を持つ人員である。取得人員は、取得及び調達ライフサイクルにおける一般的な責任の一部として、C-SCRM活動を実行する場合がある。これらの人員は、事業体の C-SCRM人員と緊密に連携して、取得及び調達に関する C-SCRM活動を実行する。以下の箇所を読むことが推奨される。

- 第 1 節：はじめに
- 第 2.1 節：C-SCRMのビジネスケース
- 第 2.2 節：サプライチェーン全体のサイバーセキュリティリスク
- 第 3.1 節：取得における C-SCRM
- 第 3.3 節：C-SCRM意識向上及びトレーニング
- 附属書 A：C-SCRMセキュリティ管理策
    - o これらの読者は、サプライヤ契約に必須の管理策に特に注意を払い、一次請負業者及び二次請負業者者の双方の当事者との合意にそれらの管理策を含めることが望ましい。
- 附属書 F：ソフトウェアのサプライチェーンセキュリティに関するガイダンス

1.4.4. 情報セキュリティ、プライバシー、又はサイバーセキュリティの運用者

これらの読者は、事業体の重要なプロセス及び情報システムの機密性、完全性、及び可用性を保護することに対して運用面の責任を持つ人員である。これらの読者は、責任の一部として、サプライチェーンのサイバーセキュリティリスクアセスメントの実施、及び／又は、C-SCRM管理策の選択及び実装に直接又は間接的に関与している可能性がある。小規模な事業体では、これらの人員がC-SCRMの実装に責任を負う場合があり、第 1.3.1 節をガイダンスとして参照することが望ましい。以下の箇所を読むことが推奨される。

- 第 1 節：はじめに
- 第 2.1 節：C-SCRMのビジネスケース
- 第 2.2 節：サプライチェーン全体のサイバーセキュリティリスク
- 第 3.2 節：サプライチェーンの情報共有

- 第 3.4 節：C-SCRMの重要なプラクティス
- 附属書 A：C-SCRMセキュリティ管理策
- 附属書 B：C-SCRM管理策の概要
- 附属書 C：リスクレベルフレームワーク
- 附属書 G：リスクマネジメントプロセスにおける C-SCRM活動
- 附属書 E：FASCSA
- 附属書 F：ソフトウェアのサプライチェーンセキュリティに関するガイダンス

1.4.5. システム開発、システムエンジニアリング、及びシステム実装人員

これらの読者は、情報システムのシステム開発ライフサイクル（SDLC）内の活動を実行することに責任を持つ人員である。SDLC に関する責任の一部として、これらの読者は、運用レベルの C-SCRM活動の実行に責任を持つことになる。特にこれらの人員は、自らの担当する情報システムの範囲内で、サプライチェーンを通じて提供される製品及びサービスから生じるサイバーセキュリティリスクを管理するために、C-SCRM管理策を実装することに関与する可能性がある。以下の箇所を読むことが推奨される。

- 第 1 節：はじめに
- 第 2.1 節：C-SCRMのビジネスケース
- 第 2.2 節：サプライチェーン全体のサイバーセキュリティリスク
- 第 2.3.4 節：レベル 3 - 運用
- 附属書 A：C-SCRMセキュリティ管理策
- 附属書 B：C-SCRM管理策の概要
- 附属書 C：リスクレベルフレームワーク
- 附属書 F：ソフトウェアのサプライチェーンセキュリティに関するガイダンス
- 附属書 G：リスクマネジメントプロセスにおける C-SCRM活動

1.5. 背景

C-SCRMには、研究開発、設計、製造、取得、納入、統合、運用及び保守、廃棄、並びに事業体の製品及びサービスの全体的な管理などの、SDLC 全体にわたる活動が含まれる。C-SCRMはサプライチェーン全体のサイバーセキュリティリスクに対処するための重要な領域であるため、事業体は C-SCRM を SDLC 内に統合することが望ましい。C-SCRMは、サプライチェーン全体のサイバーセキュリティリスクを、体系的及び意図的に管理することである。C-SCRMは事業体の認識及び自覚を必要とし、図 1-1 に示すように、セキュリティ、適合性、安全性、信頼性、ユーザビリティ、品質、完全性、効率性、保守性、拡張性、及びレジリエンスが交わる位置にある。これらの側面は、事業体がC-SCRMに取り組む際の考慮事項の層であり、C-SCRMによって良いインパクトを受けることが望ましい。

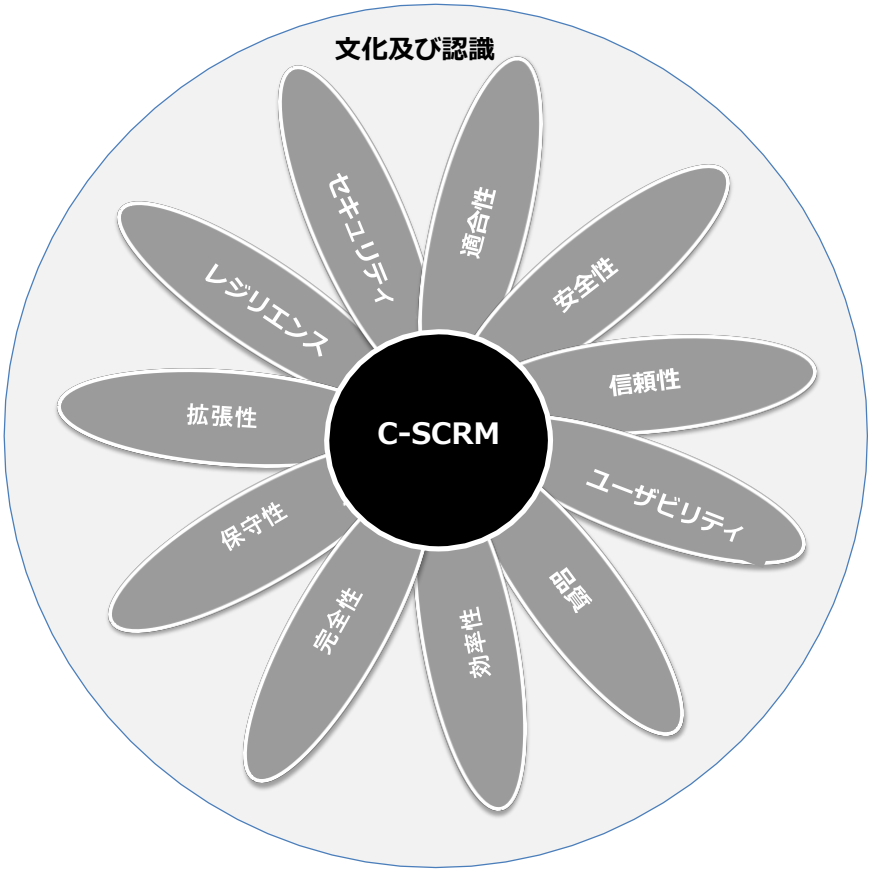

図 1-1：C-SCRM の要素

- **文化及び認識**とは、C-SCRMの成功の土台を作る、組織の共有された価値観、プラクティス、目標、及び態度のセットである。これには、C-SCRMの重要性及びその失敗による悪い結果を認識するための、個人及び事業体の態度及び理解に影響を与える学習プロセスが含まれる[6]。
- **セキュリティ**は、（a）サプライチェーンを説明する情報（例えば、論理的及び物理的な製品及びサービスの経路に関する情報）、（b）サプライチェーンを通過する情報、製品、及びサービス（例えば、製品及びサービスに含まれる知的財産）、及び／又は（c）サプライチェーンに参加している関係者（製品又はサービスのライフサイクルを通じて、製品又はサービスに触れるすべての人）に関する情報の機密性、完全性、及び可用性を提供する。
- **適合性と**は、サプライチェーン並びに提供される製品及びサービスが、事業体及びその目的にとって正しく適切なものであることに焦点を当てたものである。
- **安全性と**は、製品又はサービスが、死亡、負傷、職業病、機器又は資産の損傷又は喪失、あるいは環境への損害を引き起こす可能性がある状態から免れることを確実にすることに焦点を当てたものである[7]。
- **信頼性と**は、製品又はサービスが、規定された期間、予測可能な方法で、定義されたとおりに機能する能力に焦点を当てたものである[8]。

[6] NIST SP 800-16
[7] NIST SP 800-160 Vol.2
[8] NIST SP 800-160 Vol.2

- **ユーザビリティと**は、特定のユーザが、特定の利用状況において、製品又はサービスを利用する際に、有効性、効率性及び満足を伴って特定の目標を達成できる度合いに焦点を当てたものである[9]。
- **品質と**は、コンポーネントの意図された機能又はサービスの提供を制限したり、コンポーネント又はサービスの障害につながったり、悪用の機会を提供したりする可能性がある脆弱性及び弱点を軽減しながら、パフォーマンス、技術、及び機能面の仕様を満たす又は上回ることに焦点を当てたものである。
- **効率性と**は、製品又はサービスによってもたらされる意図された結果の適時性に焦点を当てたものである。
- **保守性と**は、製品又はサービスが、将来得られる利益の拡大をサポートするために、過去の経験に基づく変更及び改善に対応するための容易さに焦点を当てたものである。
- **完全性と**は、不適切な修正又は改ざんから製品及び製品のコンポーネントを保護し、真正性及びペディグリーを確実にすることに焦点を当てたものである。
- **拡張性**とは、製品又はサービスの成長及び需要の増大に対応する能力である。
- **レジリエンスと**は、製品、サービス、又はサプライチェーンが、変化する状況に備え、適応し、破壊に耐えて迅速に回復するための事業体の能力を確実にサポートすることに焦点を当てたものである。レジリエンスには、意図的な攻撃、事故、又は自然発生する脅威やインシデントに耐え、回復する能力が含まれる。

1.5.1. 事業体のサプライチェーン

現代の事業体は、自らのミッションをサポートするために複雑な情報システム及びネットワークを運用している。これらの情報システム及びネットワークは、サプライヤ、開発者、及びシステムインテグレータによって提供される ICT/OT[10] 製品及びコンポーネントで構成されている。また、事業体は、以下を含む数多くの製品及びサービスを取得して展開している。

- 開発者が提供する、事業体内で展開するために構築された情報システム用のカスタムソフトウェア。
- システムインテグレータ、又は、その他の *ICT/OT* 関連のサービスプロバイダが提供する、事業体の境界[11]の内部又は外部にある情報システム及びネットワークの運用、保守、及び廃棄サポート。
- 外部システムサービスプロバイダが提供する、認可境界の内部と外部の両方に配置される、事業体の業務をサポートするための外部サービス。

[9] NIST SP 800-63-3

[10] NIST SP 800-37, Rev. 2 では、制御・運用技術を以下のように定義している。
物理環境と相互作用する（又は物理環境と相互作用するデバイスを管理する）プログラム可能なシステム又はデバイス。これらのシステム／デバイスは、デバイス、プロセス、事象の監視及び／又は制御を通じて、直接的な変化を検知又は引き起こす。例としては、産業用制御システム、ビル管理システム、防火システム、及び物理的アクセス制御メカニズムがある。

[11] 連邦政府情報システムの場合、これは認可境界であり、NIST SP 800-53, Rev. 5 で以下のように定義されている。
認可権限のある担当者によって運用を認可される、情報システムのすべてのコンポーネント。これには、情報システムが接続されている、個別に認可されたシステムは含まれない。

これらのサービスは、情報システム又はサービスの SDLC 全体にわたって存在している場合があり、以下のようなものである可能性がある。

- 事業体、開発者、システムインテグレータ、又は外部システムサービスプロバイダが雇用するスタッフによって実行されている。
- 事業体、開発者、システムインテグレータ、又は外部システムサービスプロバイダによって物理的にホストされている。
- 開発環境、情報システム及びコンポーネントを輸送する物流／配送環境、又は適用可能なシステム及び通信インタフェースによってサポートされている、又は、構成されている。
- プロプライエタリ、オープンソース、又は市販（COTS）のハードウェア及びソフトウェア。

このエコシステム内の異なる関係者によって実施されるサービス及び関連活動に対する責任及び説明責任は、通常、事業体とサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの間で交わされる合意文書によって定義される。

1.5.2. 事業体内におけるサプライヤの関係

事業体は、自らの戦略面及び運営面の目的の達成を可能にする様々な製品及びサービスを提供するために、サプライチェーンに依存している。サプライチェーン全体のサイバーセキュリティリスクの識別は、取得事業体とそのサプライヤ及びサービスプロバイダの間に存在する情報の非対称性によって複雑になっている。取得者は、取得した技術がどのように開発、統合、及び展開されるか、及び、取得するサービスがどのように納入されるかについて、十分な可視性及び理解が不足していることが多い。さらに、C-SCRMプロセス、手順、及びプラクティスが不十分である又は欠如している取得者は、サプライチェーン全体のサイバーセキュリティリスクの曝露（エクスポージャー）の増加を経験する可能性がある。サプライチェーン全体のサイバーセキュリティリスクの曝露（エクスポージャー）のレベルは、提供される製品及びサービスと、それらがサポートするミッション、ビジネスプロセス、及びシステムの重要性との関係に大きく左右される。事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと様々な関係を持っている。図 1-2 は、これらの多様な関係が、事業体のサプライチェーンの可視性及び管理にどう影響するかを表している。

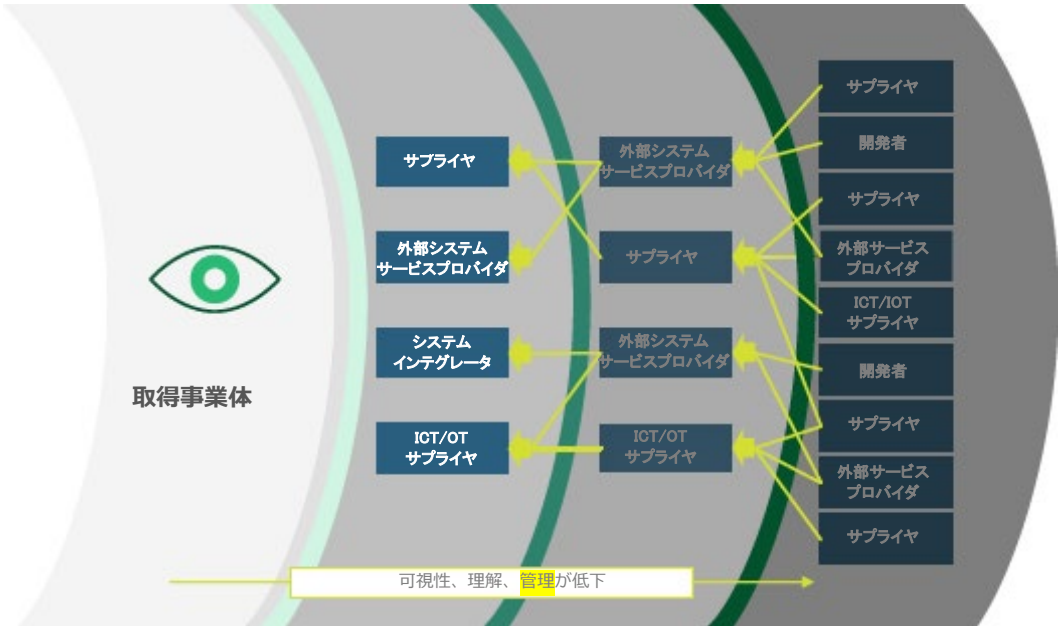

図 1-2：事業体のサプライチェーンの可視性、理解、管理

サプライチェーンの関係は、例えば、連邦政府機関の認可境界内で運用される複雑な情報システムをシステムインテグレータが開発したり、連邦政府機関の情報システム及びリソースを外部サービスプロバイダが管理したりするなど、密接に入り交じっている。これらの関係は、通常、詳細な機能、技術、及びセキュリティ要件を定め、場合によってはカスタム開発、又は製品及びサービスの大幅なカスタマイズを規定する合意（契約など）に左右される。これらの関係において、システムインテグレータ及び外部サービスプロバイダは、事業体と協力して、深刻度及びリスクのアセスメント、並びにコスト／便益分析の結果に基づいて、適切と考えられるプロセス及び管理策（本出版物内に記載）を実装できる可能性がある。これには、必要なアシュアランス目的の達成に対するより高い信頼性を確実にするために、サプライチェーンの上流における流動的な要件が含まれる場合がある。そのような要件を拡張する決定は、何が実現可能で費用対効果が高いかの認識とのバランスをとらなければならない。システムインテグレータ及び外部サービスプロバイダがC-SCRMプロセス及び管理策を実装することを期待される度合いは、それらの追加要件に従わないことによってもたらされる事業体へのリスクと比較して検討することが望ましい。多くの場合、システムインテグレータ及び外部サービスプロバイダと直接協力して、適切な軽減プロセス及び管理策を事前に識別することが、より費用対効果の高い戦略を構築するのに役立つ。

ICT/OT製品をサプライヤから調達することで、それらのサプライヤと取得者の間に直接的な関係が確立される。この関係も、通常、取得者とサプライヤとの間の合意に左右される。しかし、サプライヤによって開発される商用 ICT/OT は、通常、グローバル市場向けの一般的な目的のために設計されており、個々の顧客の固有の運用環境又は脅威環境に合わせてテーラリングされてはいない。事業体は、IT ソリューションが目的に適合[12]しているか、必須のセキュリティ機能及びケイパビリティ（能力）が含まれているか、品質及びレジリエンス力の期待を満たしているか、ライフサイクルを通してその製品又は製品コンポーネントのライフサイクルを通じてサプライヤによるサポートを必要とするかどうかを判断するために、自らの固有のC-SCRM要件に関するデューデリジェンス及び調査を実施することが望ましい。

[12] 「目的に適合（fit for purpose）」とは、目的又はサービスレベルを満たすことができるプロセス、構成アイテム、IT サービスなどを非公式に説明するために使用される用語である。 目的に適合するためには、適切な設計、実装、管理策、及び保守が必要である。（出典：Information Technology Infrastructure Library (ITIL) Service Strategy [ITIL Service Strategy].）

可能な限りサプライヤと直接対話することを含む可能性がある、製品についての取得者の調査結果のアセスメントは、これから得られた知見のアセスメントは、取得者が既存の ICT/OT 製品及びサービスの特徴及びケイパビリティ（能力）を理解したり、サプライヤに対する期待及び要件を設定したり、市場によってまだ満たされていないC-SCRMのニーズを識別したりするのに役立つ。また、取得者のニーズを少なくとも部分的にサポートする可能性がある新しいソリューションを識別するのにも役立てることができる。概して、このような調査及びサプライヤとの関わりによって、取得者は、市場提供品との整合性を図り推進するための要件をより明確にし、自らの環境における製品の購入、構成、及び使用についてリスクベースの決定を行うことができるようになる。

コスト及びリソースの管理

サプライチェーン全体のサイバーセキュリティリスクの曝露（エクスポージャー）と、C-SCRMプラクティス及び管理策を実装するコスト及び便益のバランスをとることは、取得者のC-SCRMに対する取得者の全体的なアプローチの重要な要素であることが望ましい。

事業体は、C-SCRMプラクティス及び管理策の実装には追加の財政的及び人的リソースが必要であることを認識することが望ましい。サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダからの、より高いレベルのテスト、文書、又はセキュリティ機能を要求することは、製品又はサービスの価格を上昇させる可能性があり、その結果、取得者のコストが増加する可能性がある。これは、汎用的な用途向けに開発されていて、特定の事業体のセキュリティ又はC-SCRM要件に合わせてテーラリングされていない製品及びサービスに特に当てはまる。C-SCRMプラクティス及び管理策を要求して実装するかどうかを決定する際、取得者は、これらの管理策を実装するコストと、実装しないリスクの両方を考慮することが望ましい。

取得者は、可能かつ適切な場合には、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダに対し、C-SCRM をサポートする証拠を提供する可能性がある適用可能な既存データ及び文書（例えば、ISO 27001 などの関連規格のベンダ認証）を再利用する機会を与えることが望ましい。これを行うことで、取得者及びサプライヤのコストが削減される。ただし、場合によっては、追加情報又は異なる情報が必要となり、再アセスメントが求められるために、文書の再利用が適切でない可能性がある（例えば、以前に監査されたサプライヤが、まだ生産されていない新しい製品を開発している場合）。いずれにせよ、取得者は取得プロセスの早い段階で、セキュリティ考慮事項を識別して含めることが望ましい。

1.6. NIST SP 800-39、NIST SP 800-37, Rev 2、及び NIST SP 800-53, Rev 5 を使用してC-SCRMガイダンスを構築するための方法論

本出版物では、事業体、ミッション及び運用レベルのC-SCRMガイダンスを提供することで、[NIST SP 800-39]のマルチレベルのリスクマネジメントアプローチを適用している。また、[SP 800-37, Rev. 2]のためのナビゲーションシステムを導入し、ユーザがより簡単に本出版物の関連する節に注目できるようにしている。最後に、本出版物には、[NIST SP 800-53, Rev. 5]を基にした、特定のC-SCRM管理策の拡張オーバーレイが含まれている。

本出版物に含まれるガイダンス／管理策は、既存の分野横断的なプラクティスに基づいて構築されており、システム、製品、及びサービスのライフサイクル全体を通じて、サプライチェーン全体の関連するサイバーセキュリティリスクを管理するための事業体の能力を高めることを意図している。本出版物は、C-SCRMのための独立した文書（例えば、ポリシー、アセスメント及び認可[A&A]計画、及びC-SCRM計画）を策定するか、既存の政府機関文書に統合するかのいずれかの柔軟性を事業体に与えていることに注意する必要がある。

[FIPS 199]によると、個々のシステムについては、このガイダンスはすべてのインパクト分類の情報システムで使用することが推奨されている。政府機関は、より高いインパクトレベルのシステム、又は特定のシステムコンポーネントにこのガイダンスを適用することを優先してもよい。最後に、本出版物は、事業体及び事業体のミッション及びビジネスレベルでのC-SCRM戦略及び実装計画、並びに、事業体における運用レベルのC-SCRMシステム計画の策定及び実装について説明している。運用レベルのC-SCRM計画は、サプライチェーンのサイバーセキュリティリスクアセスメントから情報を得て、特定の政府機関のミッション及びビジネスニーズ、運用環境、及び／又は実装技術に合わせてテーラリングされたC-SCRM管理策を含むことが望ましい。

リスクマネジメントプロセスへの統合

本出版物内のプロセスは、[NIST SP 800-39]で説明されているリスクマネジメントプロセス及び階層（例えば、事業体、ミッション、システム）のすべてのレベルにおいて、事業体の既存のSDLC及び事業体環境に統合されることが望ましい。第2節では、[NIST SP 800-39]のリスクマネジメント階層及びアプローチの概要を提供し、リスクマネジメントプロセスにおけるC-SCRM活動を識別する。附属書Cでは、[NIST SP 800-39]の第2節の基づき、ICT/OTに関するSCRM活動の記述及び説明を提供する。附属書Cの構成は[NIST SP 800-39]を反映したものである。

*SP 800-37, Revision 2*のコンテキストにおける*C-SCRM*の実装

本出版物で説明されているC-SCRM活動は、[NIST SP 800-37, Rev. 2]で説明されているリスクマネジメントフレームワークと密接に関係している。特に、運用レベルで実施されるC-SCRMプロセスは、[NIST SP 800-37, Rev 2]の一部として完了したステップを厳密に反映し、及び／又は、それらのステップへのインプットとして機能することが望ましい。レベル1及び2で完了したC-SCRM活動は、可能かつ適切な場合は、運用レベル及びRMFタイプのプロセスへのインプット（例えば、リスクアセスメント結果）を提供することが望ましい。第2節及び附属書Cでは、C-SCRMと[NIST SP 800-37, Rev. 2]の関連性をさらに詳しく説明している。

1.7. 他の出版物との関係、及び出版物の要約

本出版物は、他のNIST出版物内で推奨されている概念を基にして、それらの概念をサプライチェーンのサイバーセキュリティリスクマネジメントの中で使用するためにテーラリングしている。こうした関係があることから、本出版物は、基礎となるフレームワーク、概念、方法論を向上させ続けるために、その概念の多くを継承し、他のNIST出版物を参照している。これらのNIST出版物には、以下が含まれる。

- **NIST サイバーセキュリティフレームワーク（CSF）バージョン 1.1（NIST Cybersecurity Framework (CSF) Version 1.1）：**組織がサイバーセキュリティリスクをより適切に管理及び低減するための、既存の標準、ガイドライン及び手法に基づく任意ガイダンス。また、組織の内部と外部の両方のステークホルダーの間で、リスク及びサイバーセキュリティの管理に関するコミュニケーションを促進するよう策定されている。
- **FIPS 199、連邦政府の情報および情報システムに対するセキュリティ分類規格（*Standards for Security Categorization of Federal Information and Information Systems*）：**連邦政府の情報及び情報システムが不正アクセス、不正利用、漏えい、破壊、改ざん、又は破棄によって侵害された場合における、機密性、完全性、及び可用性に対する政府機関の懸念の度合い、並びに、政府機関の資産及び業務への潜在的インパクトに応じて、連邦政府の情報及び情報システムを分類するための規格。
- **SP 800-30, Revision 1、リスクアセスメントの実施の手引き（*Guide for Conducting Risk Assessments*）：**連邦政府情報システム及び組織のリスクアセスメントの実施に関するガイダンスであり、SP 800-39 のガイダンスを詳述している。リスクマネジメント階層の3つのティアすべてで実施されるリスクアセスメントは、識別されたリスクに対応する適切な行動方針を決定するために必要な情報を上級幹部／管理職に提供する、全体的なリスクマネジメントプロセスの一部である。
- **SP 800-37, Revision 2、情報システム及び組織のためのリスクマネジメントフレームワーク：セキュリティ及びプライバシーのためのシステムライフサイクルアプローチ（*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*）：**リスクマネジメントフレームワーク（RMF）について説明し、情報システム及び組織にRMFを適用するためのガイドラインを提供している。RMFは、セキュリティ及びプライバシーリスクを管理するための、統制がとれ、構造化された、柔軟なプロセスを提供する。このプロセスには、情報セキュリティの分類化、管理策の選択、実装及びアセスメント、システム及び共通管理策の認可、継続的な監視が含まれる。
- **SP 800-39、情報セキュリティリスクの管理：組織、ミッション、及び情報システムの観点（*Managing Information Security Risk: Organization, Mission, and Information System View*）：**連邦政府情報システムの運用及び使用に起因する、組織の業務（すなわち、ミッション、機能、イメージ、及び評判）、組織の資産、個人、他の組織、及び国家に対する情報セキュリティリスクを管理するための、統合された組織全体のプログラムのガイダンスを提供している。
- **SP 800-53, Revision 5、組織と情報システムのためのセキュリティおよびプライバシー管理策（*Security and Privacy Controls for Information Systems and Organizations*）：**敵対的攻撃、ヒューマンエラー、自然災害、構造的な障害、外国の諜報機関エンティティ、及びプライバシーリスクを含む多様な一連の脅威及びリスクから、組織の業務及び資産、個人、他の組織、及び国家を保護するために、情報システム及び組織のためのセキュリティ及びプライバシー管理策のカタログを提供している。

- **SP 800-53B、組織と情報システムのための管理策ベースライン（*Control Baselines for Information Systems and Organizations*）：**連邦政府のためのセキュリティ及びプライバシー管理策ベースラインを提供している。3つのセキュリティ管理策ベースライン – 各システムインパクトレベル（すなわち、低インパクト、中インパクト、及び高インパクト）ごとに 1 つ – 、及びインパクトレベルに関係なくシステムに適用される 1つのプライバシーベースラインがある。
- **SP 800-160 Vol. 1、システムセキュリティエンジニアリング（*Systems Security Engineering*）：**システム、ケイパビリティ（能力）、及びそれらのシステムによって提供されるサービスを構成する機械的、物理的及び人的要素を含む、より防御力が高く存続可能なシステムを開発するために必要なエンジニアリング主導の観点及び行動について扱っている。
- **SP 800-160 Vol. 2, Revision 1、サイバーレジリエントなシステムの開発：システムセキュリティエンジニアリングアプローチ（*Developing Cyber Resilient Systems: A Systems Security Engineering Approach*）：**リスクマネジメントプロセスと連動したシステムライフサイクルプロセスに関するシステムエンジニアリングの観点に基づいて、識別されたサイバーレジリエンスの成果を達成するためのハンドブックであり、組織の経験及び専門知識がその目的にとって何が正しいかを判断するのに役立つことを可能にする。
- **SP 800-181, Revision 1、サイバーセキュリティ教育のための国家計画（*NICE*）サイバーセキュリティワークフォースフレームワーク（*National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*）：**サイバーセキュリティ業務に関する情報を説明及び共有するための基本的な参考文献。サイバーセキュリティ業務をタスク記述として表現し、学生、求職者、及び従業員を含む学習者に基礎知識を提供する知識及びスキル記述について説明している。
- **NISTIR 7622、連邦政府情報システムのための概念的なサプライチェーンのリスクマネジメントプラクティス（*Notional Supply Chain Risk Management Practices for Federal Information Systems*）：**連邦政府の情報システムへのサプライチェーンリスクの軽減に役立つ幅広いプラクティスを提供している。サプライチェーン全体の理解及び可視性を得るための手段を提供する、反復可能かつ商業的に合理的なサプライチェーンアシュアランスの方法及びプラクティスの概念的なセットを、連邦政府各省庁及び関係機関に習得させることを目指している。
- **NISTIR 8179、致命度解析プロセスモデル：システム及びコンポーネントの優先順位付け（*Criticality Analysis Process Model: Prioritizing Systems and Components*）：**組織が、最も重要で、追加のセキュリティ又はその他の保護を必要とする可能性のあるシステム及びコンポーネントを識別するのに役立つ。
- **NISTIR 8276、サプライチェーンのサイバーリスクマネジメントにおける重要なプラクティス：業界からの意見（*Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*）：**あらゆる組織がサプライチェーンに関するサイバーセキュリティリスクを管理するために使用できる一連の重要なプラクティスを提供している。この出版物で示されている重要なプラクティスは、任意の規模、範囲、及び複雑さの組織で、堅牢なC-SCRM機能を実装するために使用できる。これらのプラクティスは、政府及び業界の既存のC-SCRMリソースに含まれる情報と、2015年及び2019年のNIST研究イニシアチブで収集された情報を組み合わせている。
- **NISTIR 8286、エンタープライズリスクマネジメント（*ERM*）のためのサイバーセキュリティリスクの識別及び見積（*Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*）：**事業体内部の個々の組織が、コミュニケーション及びリスク情報の共有を通じて、事業体の ERM プロセスへのインプットとして提供するサイバーセキュリティリスク情報を改善するのに役立つ。

- **NISTIR 8286A、エンタープライズリスクマネジメントのためのサイバーセキュリティリスクの識別及び見積（*Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*）：**リスク許容度、リスク選好度、及びそのコンテキストにおけるリスクを決定する方法を説明するための例及び情報を提供している。エンタープライズリスクレジスタの作成をサポートするため、この報告書では、事業体の資産に対する脅威及び脆弱性の潜在的なインパクトに基づいて、様々なシナリオの文書化について説明している。事業体のリスクプロファイルに統合されたサイバーセキュリティリスクレジスタを通じて、様々な脅威事象の起こりやすさ及びインパクトを文書化することは、後に、事業体のサイバーセキュリティリスク対応及び監視を優先順位付けと伝達に役立つ。
- **NISTIR 8286B、エンタープライズリスクマネジメントのためのサイバーセキュリティリスクの優先順位付け（*Prioritizing Cybersecurity Risk for Enterprise Risk Management*）：**
  ステークホルダーのリスクのガイダンス、並びに、リスクの識別及び分析に関する詳細を提供している。この2つ目の出版物では、事業体の目的に対する潜在的インパクトの観点から、それらの各リスクの優先順位を決定することの必要性、及び、そのリスクを適切に処理するための選択肢を説明している。この報告書では、エンタープライズリスクレジスタ全体をサポートするサイバーセキュリティリスクレジスタ（CSRR）に、リスクの優先順位及びリスク対応情報をどのように追加するかを説明している。リスク対応の選択及び将来予想されるコストに関する情報は、事業体全体のサイバーセキュリティリスクに対する複合的な視点を維持するために使用され、ミッションの成功を確実にするためのリスク戦略の確認及び調整に使用される場合がある。

また、本出版物は、他の規制、政府報告書、標準、ガイドライン、及びベストプラクティスから概念及び作業も利用している。これらのリソースの全リストは、附属書 H で確認できる。

重要ポイント[13]

サプライチェーン：ICT/OTは、公共及び民間分野のエンティティ（例えば、取得者、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT関連のサービスプロバイダ）で構成される、グローバルに分散し、相互接続されたサプライチェーンエコシステムに依存している。

サプライチェーンの製品及びサービス：事業体がサプライチェーンに依存している製品及びサービスには、システム及びシステムコンポーネントの提供、オープンソース及びカスタムソフトウェア、運用サポートサービス、システム及びサービスの運用、並びに、システムサポートの役割の実行が含まれる。

サプライチェーンのメリット及びリスク：このエコシステムは、コスト削減、相互運用性、迅速なイノベーション、製品機能の多様性、及び複数の競合ベンダを選択する能力などのメリットを提供する。しかし、これらのメリットを提供する同じメカニズムが、サプライチェーン全体の様々なサイバーセキュリティリスクをもたらす可能性もある（例えば、サービスレベル低下を引き起こし、事業体の顧客基盤からの不満につながる、サプライヤの供給停止）。

サプライチェーンのサイバーセキュリティリスクマネジメント（C-SCRM）：本出版物で説明されているように、C-SCRMとは、事業体がサプライチェーン全体のサイバーセキュリティリスクを管理するのを支援することを目的とした、体系的なプロセスである。事業体は、独自の戦略、運用、及びリスクの状況に最も適合するように、本出版物で説明されているプラクティスを識別、採用、及びテーラリングすることが望ましい。

C-SCRMの範囲：C-SCRMには、情報セキュリティ及びプライバシー、システム開発者及び実装者、取得、調達、法務、並びに人事などの、幅広いステークホルダーグループが含まれる。C-SCRMは、システム開発ライフサイクル（SDLC）の開始から廃棄までの全体にわたる活動を対象としている。さらに、サプライチェーン全体で識別されたサイバーセキュリティリスクは、重要な事業が異なるリスクの種類（例えば、財務リスク、戦略的リスク）にさらされる総量を事業体が確実に把握するためのリスクマネジメントプロセスの一環として、集約及びコンテキスト化されることが望ましい。

[13] 重要ポイントでは、その節の本文から重要な点を説明している。 定義については、附属書Hの用語集を参照。

2. 事業体全体のリスクマネジメントへのC-SCRMの統合 [14]

C-SCRM は、[NIST SP 800-39]で説明され、図 2-1 に示されている事業体全体のリスクマネジメントプロセスに統合することが望ましい。このプロセスには、以下の連続的かつ反復的なステップが含まれる。

- リスクの枠組み化。リスクベースの意思決定のためのコンテキストと、事業体の情報通信技術及びサービス、並びに関連するサプライチェーンの現在の状態を規定する。
- リスクのアセスメント。重要度、脅威、脆弱性、起こりやすさ [15]、インパクト、及び関連情報をレビューし、解釈する。
- リスクへの対応。リスクアセスメントの結果に基づいて、軽減管理策を選択、テーラリング、及び実装する。
- リスクの監視。リスクの曝露（エクスポージャー）とリスク軽減の有効性を継続的に監視する。これには、効果的な事業体コミュニケーションと継続的な改善のためのフィードバックループを使用した情報システム又はサプライチェーンの変更の追跡が含まれる。

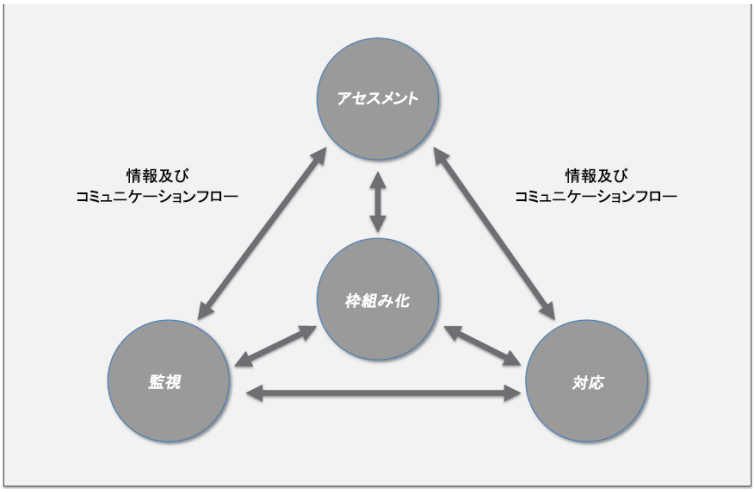

図 2-1：リスクマネジメントプロセス

サプライチェーン全体のサイバーセキュリティリスクの管理は、事業体全体の文化の変革と、協調的かつ分野横断的なアプローチを必要とする複雑な作業である。効果的なサプライチェーンのサイバーセキュリティリスクマネジメント（C-SCRM）には、事業体内部のステークホルダー（例えば、部門、プロセス）と事業体外部のステークホルダー（例えば、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダ）が、良好な C-SCRM の成果を確保するために積極的に協力し、コミュニケーションを取り、行動することが必要である。C-SCRM を成功させるには、サプライチェーン全体にわたるサイバーセキュリティリスクの潜在的な影響に対する意識と備えを強化するための、事業体全体の文化的変革が必要である。

[14] 各省庁は、大統領令 14028 号の「Improving the Nation's Cybersecurity」に従って、附属書 F を参照してこのガイダンスを実装することが望ましい。
[15] C-SCRM の目的において、起こりやすさとは、脅威が特定の期間内に脆弱性を悪用する確率と定義される。数学では、起こりやすさと確率は根本的に異なる概念であるが、両者の違いは本出版物の範囲外であることに留意されたい。

事業体は、サプライチェーン全体のサイバーセキュリティリスクを管理するアプローチに、複数の分野やプロセス（例えば、情報セキュリティ、調達、事業体のリスクマネジメント、エンジニアリング、ソフトウェア開発、IT、法務、人事）の視点を取り入れることを目指すことが望ましい。事業体は、事業体のより広範なリスクマネジメント活動の一部として、これらのプロセスを橋渡しし、統合するための明確な役割を定義しても良い。この統合されたアプローチは、C-SCRM の優先順位を識別し、ソリューションを開発し、C-SCRM を総合的なリスクマネジメントの意思決定に組み込むための事業体の取り組みの不可欠な部分である。事業体は、取得、SDLC、及び事業体のより広範なリスクマネジメントプロセスの一部として、C-SCRM 活動を実施することが望ましい。組み込まれた C-SCRM 活動には、機能の重要度及び提供された製品やサービスへの依存度の判断、該当するリスクの識別とアセスメント、適切な緩和策の決定、選択したリスク対応措置の文書化、C-SCRM 活動のパフォーマンスの監視が含まれる。サプライチェーンリスクの曝露（エクスポージャー）は事業体間で（場合によっては事業体の内部でも）異なるため、ビジネス及びミッション固有の戦略とポリシーが、事業体全体の C-SCRM の基調と方向性を定めることが望ましい。

組織は、テーラリングされた C-SCRM 計画が、以下のように設計されることを確実にすることが望ましい。

- リスクは価値の追求に不可欠であるため、リスクを排除するのではなく管理する。
- 絶えず出現する、あるいは進化する脅威に対して、運用が適応できるようにする。
- 自らの組織、プログラム、及びそれらをサポートする情報システム内で生じた変化に対応する。
- 民間部門のグローバル ICT サプライチェーンの急速に進化するプラクティスに適応する。

2.1. C-SCRMのビジネスケース

今日、すべての事業体が、ビジネス及びミッションを遂行するためにデジタル技術に大きく依存している。デジタル技術は ICT/OT 製品で構成され、サービスを通じて提供及びサポートされる。C-SCRM は、デジタル技術の使用から生じるサプライチェーン全体のサイバーセキュリティリスクに対処するために、すべての事業体が備えておく必要がある重要なケイパビリティ（能力）である。各事業体の C-SCRM ケイパビリティ（能力）の深さ、範囲、成熟度は、そのビジネス又はミッションの独自性、事業体固有のコンプライアンス要件、運用環境、リスク選好度、及びリスク許容度に基づくことが望ましい。

C-SCRM ケイパビリティ（能力）を確立して維持することは、以下のような多くの重要な利点を生み出す。

- 確立された C-SCRM プログラムにより、事業体は、サプライチェーンの弱点及び脆弱性の影響を最も受けやすい重要資産を理解できるようになる。
- C-SCRM は、C-SCRM の侵害が発生した場合に、重大なビジネスの中断につながるイベントを効果的に検知し、対応し、復旧するための事業体の能力を強化することにより、サイバーセキュリティの脅威によるサプライチェーンの侵害の起こりやすさを低減する。
- 明確な構造、目的、C-SCRM ケイパビリティ（能力）との整合性、及び既存の C-SCRM プロセスの優先順位付け、統合、合理化を通じて、運用及び事業体の効率化が達成される。

- 取得した製品が高品質で、真正性、信頼性、レジリエンス、保守容易性があり、セキュアで安全であるというアシュアランスが高まる。
- サプライヤ、サービスプロバイダ、及びそれらが提供する技術製品やサービスが信頼できるものであり、パフォーマンス要件を満たすため信頼できるというアシュアランスが高まる。

C-SCRM は、事業体の業務から生じるリスクの曝露（エクスポージャー）を管理するためのあらゆる取り組みの基本である。C-SCRM のプロセスと管理策を実装するには、取得者とその開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダによる人的投資、ツールへの投資、及びインフラへの投資が必要である。しかし、事業体が C-SCRM のプロセス及び管理策の確立と展開に投入するリソースは限られている。そのため、事業体は C-SCRM のリソース投入を決定する際に、潜在的なコストと利点を慎重に比較検討し、必要なリソースを C-SCRM に投入しなかった場合に生じる可能性のあるリスクの曝露（エクスポージャー）の影響を明確に理解した上で意思決定を行うことが望ましい。

受け入れなければならない費用便益のトレードオフがあるものの、サプライチェーンをよりセキュアにする必要性は、政府と民間分野の双方にとって不可欠である。2018 年の SECURE Technology Act[16]の可決、FASC の設立、及び NIST Interagency or Internal Report（NISTIR）8276 の *Key Practices in Cyber Supply Chain Risk Management* に収録されている 2015 年及び 2019 年のサプライチェーンのサイバーリスクマネジメントにおけるケーススタディからの所見は、「C-SCRM ケイパビリティ（能力）は、あらゆる事業体のリスク態勢の重要かつ基礎的なコンポーネントである」という幅広い公共及び民間分野の合意を示している。

2.2. サプライチェーン全体のサイバーセキュリティリスク

サプライチェーン全体のサイバーセキュリティリスクとは、サプライヤ、そのサプライチェーン、及びその製品又はサービスによってもたらされるサイバーセキュリティリスクから生じる損害又は侵害の可能性を指す。これらのリスクの例には、以下が含まれる。

- システムインテグレータの代理として活動しているインサイダー（内部関係者）が機密の知的財産を盗み、その結果、重要な競争上の優位性が失われる[17]。
- 国家の代理として活動している代理人が、政府機関に販売されたシステムで使用されるサプライヤ提供の製品コンポーネントに、悪意のあるソフトウェアを挿入する。ブリーチが発生し、その結果、いくつかの政府との契約が失われる。
- 政府機関の代理として活動しているシステムインテグレータが、脆弱なコードを再利用し、国家安全保障に関わるミッションクリティカルなデータのブリーチにつながる。
- 組織的に犯罪行為を行う事業体が偽造品を市場に投入し、その結果、顧客の信頼と信用を失う。
- ある企業が、より大きな調達の重要なコンポーネントの生産を請け負っているが、その企業は、十分に審査されていないサプライヤからの製品のラベルを付け替えている。信頼できない重要なコンポーネントが運用システムに導入されており、交換部品を供給する信頼できるサプライヤが存在しない。

[16] SECURE Technology Act - Public Law 115-390: https://www.govinfo.gov/app/details/COMPS-15413
[17] サプライチェーン全体のサイバーセキュリティリスクとして認定するために、インサイダー脅威は、特に第三者のインサイダー脅威の事例を取り上げている。

このようなリスクは、サイバーセキュリティサプライチェーンの脅威が既存の脆弱性を悪用することで現実化する。図 2-2 は、関連する脅威が該当する脆弱性を悪用する可能性と、それによってもたらされる潜在的なインパクトから生じるサプライチェーンのサイバーセキュリティリスクを示している。

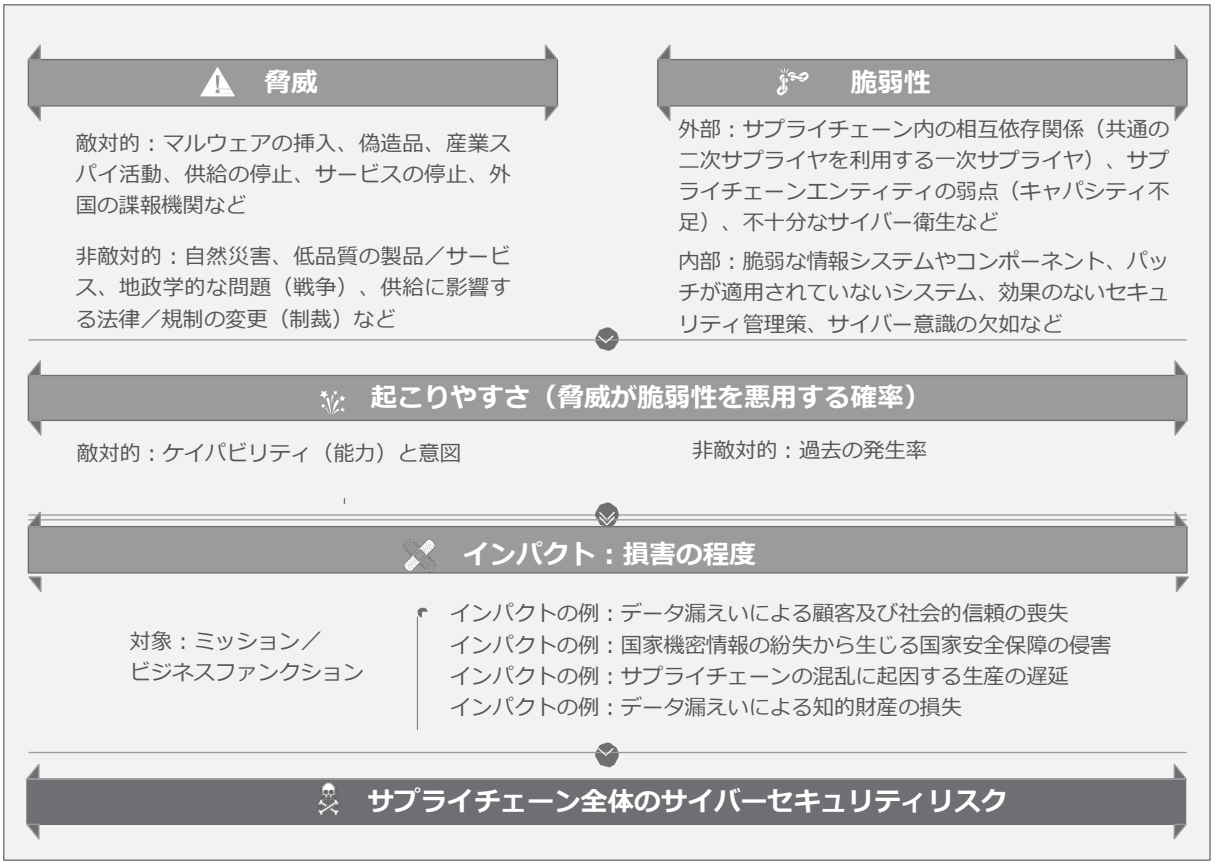

図 2-2：サプライチェーン全体のサイバーセキュリティリスク

サプライチェーンのサイバーセキュリティの脆弱性は、顧客の不満につながるサービスレベルの低下から、知的財産の盗難、重要なミッションやビジネスプロセスの劣化に至るまで、事業体のミッションに継続的な悪影響を及ぼす可能性がある。しかし、このような脆弱性が悪用されたり発見されたりするには、何年もかかる場合がある。また、ある事象がサプライチェーンの脆弱性による直接的な結果であったのかどうかを判断することが困難な場合もある。サプライチェーンの脆弱性は相互に関連していることが多く、事業体を連鎖的なサイバーセキュリティリスクにさらす可能性がある。例えば、主要なクラウドサービスプロバイダでの大規模なサービス停止は、事業体のサプライチェーン内の複数のエンティティにサービスや生産の中断を引き起こし、複数のミッション及びビジネスプロセスに悪影響を及ぼす可能性がある。

2.3. マルチレベルのリスクマネジメント [18]

事業体全体でリスクマネジメントを統合するために、[NIST SP 800-39]では、図 2-3 に示すように、様々な観点からリスクに対処する 3 つのレベルについて説明している。3 つのレベルは、1）事業体レベル、2）ミッション及びビジネスプロセスレベル、3）運用レベルである。C-SCRM では、3 つすべてのレベルの関与が必要である。

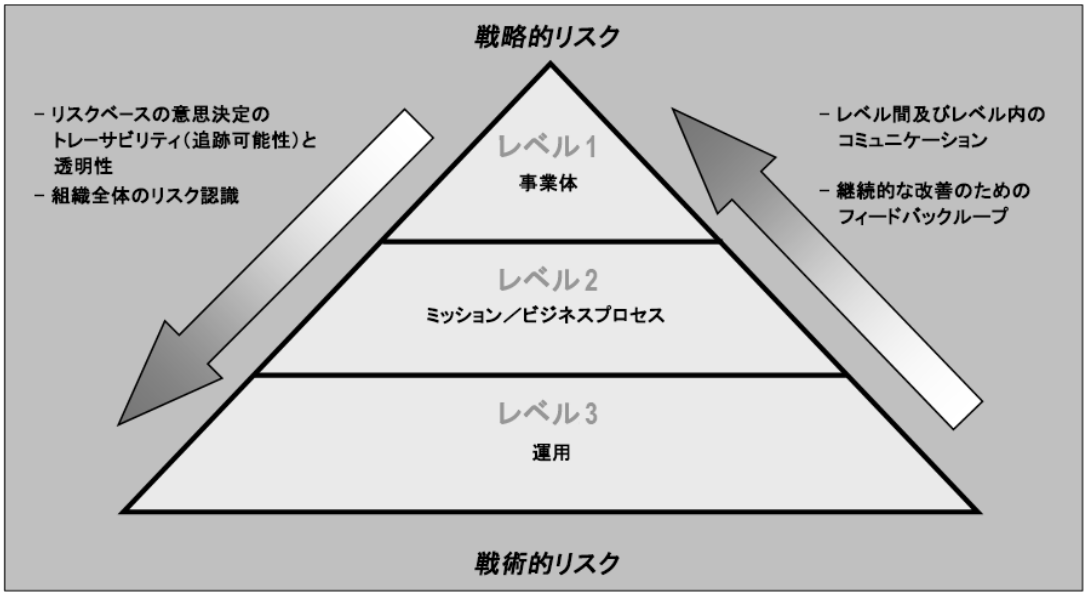

図 2-3：事業体全体のマルチレベルリスクマネジメント[19]

マルチレベルリスクマネジメントでは、事業体のリスク関連活動の継続的な改善と、C-SCRM に既得権を持つステークホルダー間の効果的なレベル間及びレベル内のコミュニケーションを全体の目的として、C-SCRM プロセスが 3 つのティアにわたってシームレスに実行される。

C-SCRM の活動は、一個人から委員会、部局、集中型のプログラムオフィス、その他の事業体構造に至るまで、事業体内の様々な個人又はグループによって実行される。C-SCRM の活動は、各事業体の構造、文化、ミッション、及びその他の多くの要因に応じて、事業体ごとに異なる。3 つのレベルそれぞれの C-SCRM 活動には、様々な上位レベルの C-SCRM 成果物の作成が含まれる。

- レベル 1（事業体）では、全体的な C-SCRM 戦略、ポリシー、及び実装計画によって、事業体全体で C-SCRM を管理する方法の基調、ガバナンス構造、及び境界が設定され、ミッション及びビジネスプロセスレベルで実行される C-SCRM 活動の指針となる。

[18] 各省庁は、附属書 F を参照して、大統領令 14028 号の「*Improving the Nation's Cybersecurity*」に従ってこのガイダンスを実施することが望ましい。
[19] 図 2-2 に示されている概念に関する追加情報は、[NIST SP 800-39]に記載されている。

- レベル 2（ミッション及びビジネスプロセス）では、中間レベルの C-SCRM 戦略、ポリシー、及び実装計画は、事業体レベルで示されたコンテキストと方向性を前提として、それを特定のミッション及びビジネスプロセスに合わせてテーラリングする。
- レベル 3（運用）では、C-SCRM 計画は、情報システムがビジネス要件、機能要件、及び技術要件を満たしているかどうか、及び適切にテーラリングされた管理策が含まれているかどうかを判断するための基準を提供する。これらの計画は、レベル 2 で提供されるコンテキストと方向性の影響に大きく影響される。

図 2-4 は、マルチレベルリスクマネジメントの構造と、各レベルで策定される関連する戦略、ポリシー、及び計画の概要を示している。各レベルでの具体的な活動の詳細については、第 2.3.1 節から第 2.3.5 節を参照のこと。

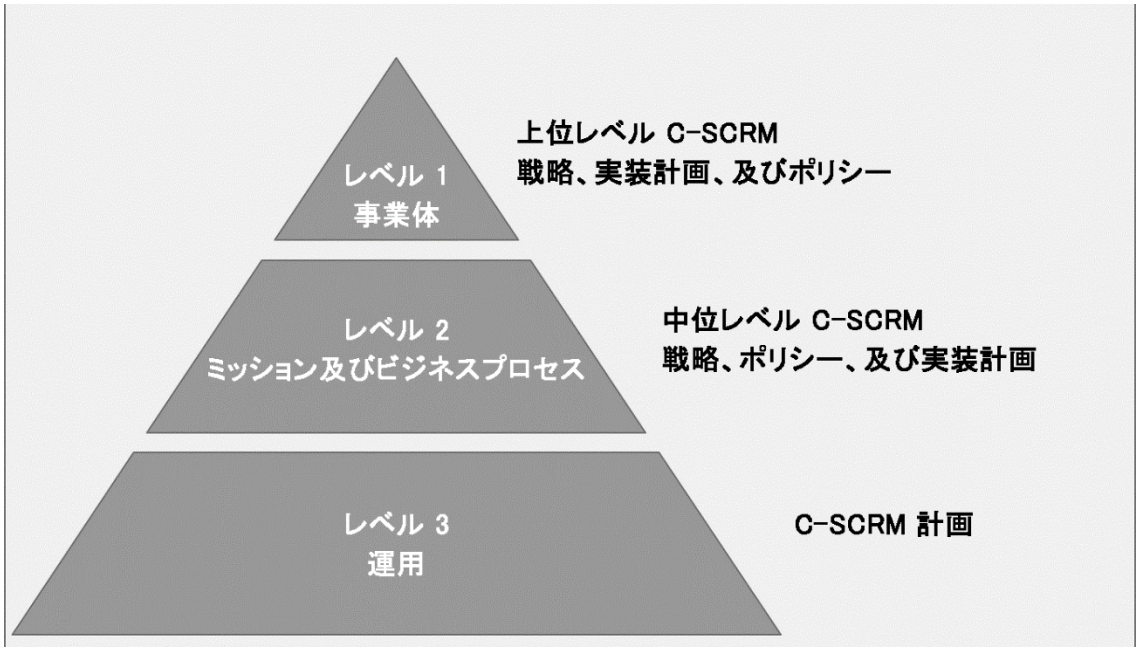

図 2-4：事業体全体のマルチレベルリスクマネジメントにおける C-SCRM 文書

2.3.1. 3つのレベルにまたがる役割と責任

C-SCRM を実装するには、事業体は、サプライチェーン全体のサイバーセキュリティリスクを効果的に管理するために、調整されたチームベースのアプローチと共有責任モデルを確立する必要がある。事業体は、C-SCRM 関連のポリシーを確立して遵守し、プロセス（多くの場合、本質的には企業横断型）を策定して従い、プログラム的及び技術的な軽減技術を採用することが望ましい。調整されたチームアプローチは、暫定的又は正式なものにかかわらず、事業体がサプライチェーンの包括的かつ多角的な分析を効果的に実施し、リスクに対応し、外部のパートナー／ステークホルダーとのコミュニケーションを取り、C-SCRM の適切なリソースに関する幅広い合意を得ることを可能にする。C-SCRM チームは、複数の視点と専門知識のインプット及び関与から導き出される意思決定と活動を実行するために協力することが望ましい。チームは、個々の事業体又は専門分野に明確に割り当てられるべき C-SCRM の責任とプロセスを活用するが、それらに代わるものではない。C-SCRM の効果的な実装には、C-SCRM 関連の活動やリスクに対する責任及び説明責任を、多様なステークホルダーグループに分散させる、共有責任モデルの採用が含まれることが多い。事業体が分野横断的なアプローチから利益を得る C-SCRM 活動の例としては、戦

略的な調達戦略の策定、要請書への C-SCRM 要件の組み込み、識別されたサプライチェーンリスク、特に重大であるとアセスメントされたリスクを軽減する最善の方法についてのオプションの決定などが挙げられる。

C-SCRM チームのメンバーは、情報セキュリティ、調達、事業体のリスクマネジメント、エンジニアリング、ソフトウェア開発、IT、法務、人事など、事業体の重要なプロセスの様々な側面に関与する多様な人々で構成することが望ましい。C-SCRM を支援するために、これらの各メンバーは、各自の専門分野に特有の事業体のプロセスやプラクティスの専門知識、及びシステム又はシステムを流れる情報の技術的側面と相互依存性についての理解を提供することが望ましい。C-SCRM チームは、事業体の既存のリスクマネジメント機能の延長である場合、事業体のサイバーセキュリティリスクマネジメント機能の一部として成長した場合、又は別の部門で運営されている場合がある。

分野横断的な C-SCRM チームを結成するための鍵は、事業体内の全く異なる機能間の障壁を取り除くことである。多くの事業体は、必要かつ適切な機能分野からの代表者を集めた、上級幹部のワーキンググループまたは評議会を設立することによって、トップからこのプロセスを開始する。ワーキンググループの目標、目的、権限、会議の頻度、及び責任の概要を概説した憲章を策定することが望ましい。この評議会が結成されると、分野横断的なアプローチをミッション、ビジネスプロセス、及び業務レベルでどのように運用可能にするかを決定できる。これは、より高頻度で定期的な会議を開催し、より運用的で戦術的に焦点を絞った C-SCRM の課題に取り組むことができるミッション及びビジネスプロセスの代表者で構成されるワーキンググループの形をとることが多い。

表 2-1 は、各レベルの C-SCRM ステークホルダーの概要と、対応するレベル内で実行される具体的な C-SCRM 活動を示している。これらの活動は、直接的な C-SCRM 活動であるか、C-SCRM に影響を与えるかのいずれかである。

表 2-1：サプライチェーンのサイバーセキュリティリスクマネジメントのステークホルダー[20]

レベル	レベル名	一般的なステークホルダー	活動
1	事業体	エグゼクティブリーダーシップ： CEO、CIO、COO、CFO、CISO、 最高技術責任者（CTO）、 最高取得責任者（CAO）、 最高プライバシー保護責任者（CPO）、 CRO など	• 事業体の C-SCRM 戦略を定義する。 • ガバナンス構造と運用モデルを形成する。 • 事業体のリスクを枠組み化し、リスクの管理方法の基調を定める（例えば、リスク選好度の設定）。

[20] 中小規模の企業では、C-SCRM ステークホルダーにこのような高度な区分別化が見られない可能性がある。

レベル	レベル名	一般的なステークホルダー	活動
			• 上位レベルの実装計画、ポリシー、目標、及び目的の概要を定義する。 • 事業体レベルの C-SCRM の意思決定を行う。 • C-SCRM PMO を結成する。
2	ミッション及びビジネスプロセス	ビジネスマネジメント： プログラムマネジメント[PM]、 プロジェクトマネージャ、 統合プロジェクトチーム（IPT）メンバー、研究開発（R&D）、 エンジニアリング（SDLC 監督）、 取得及びサプライヤ関係マネジメント／原価計算、及び信頼性、安全性、セキュリティ、品質、C-SCRM PMO などに関連するその他のマネジメント	• ミッション及びビジネスプロセス固有の戦略を策定する。 • ポリシーと手順、ガイダンス、及び制約条件を策定する。 • 新しい IT プロジェクト及び／又は関連する取得の開始時に脆弱性を軽減する。 • ビジネス、技術、及び取得環境をサイバー脅威又は攻撃にさらすシステム、人、又は組織の欠陥をレビュー及びアセスメントする。 • C-SCRM 実装計画を策定する。 • 事業体リスクフレームワークをミッション及びビジネスプロセスに合わせてテーラリングする（例えば、リスク許容度を設定する）。 • ミッション及びビジネスプロセス内のリスクを管理する。 • C-SCRM PMO を結成する及び／又は C-SCRM PMO と協力する。 • C-SCRM をレベル 1 に報告し、レベル 3 からの報告に基づいて行動する。

レベル	レベル名	一般的なステークホルダー	活動
3	運用	システムマネジメント：アーキテクト、開発者、システム所有者、QA／QC、テスト、契約担当者、C-SCRM PMO スタッフ、制御エンジニア、及び／又は制御システム運用者など	• C-SCRM 計画を策定する。 • C-SCRM ポリシー及び要件を実装する。 • レベル 1 及びレベル 2 で指定された制約条件を守る。 • C-SCRM を個々のシステムのコンテキストに合わせてテーラリングし、SDLC 全体に適用する。 • C-SCRM をレベル 2 に報告する。

C-SCRM プロセスは、事業体のリスク関連活動の継続的な改善と、効果的なレベル間及びレベル内のコミュニケーションを全体の目的として、3 つのリスクマネジメントレベルにわたって実施されることが望ましく、これにより、事業体のミッション及びビジネスの成功に共通の利益を持つすべてのステークホルダーの間で、戦略的活動と戦術的活動の両方が統合される。コンポーネント、システム、プロセス、ミッションプロセス、又はポリシーのいずれに対処する場合でも、リスクマネジメント活動が可能な限り情報に基づいたものになるように、各レベルで関連する C-SCRM ステークホルダーを関与させることが重要である。図 2-5 は、3 つのレベルにわたる主要な C-SCRM 文書間の関係を示している。

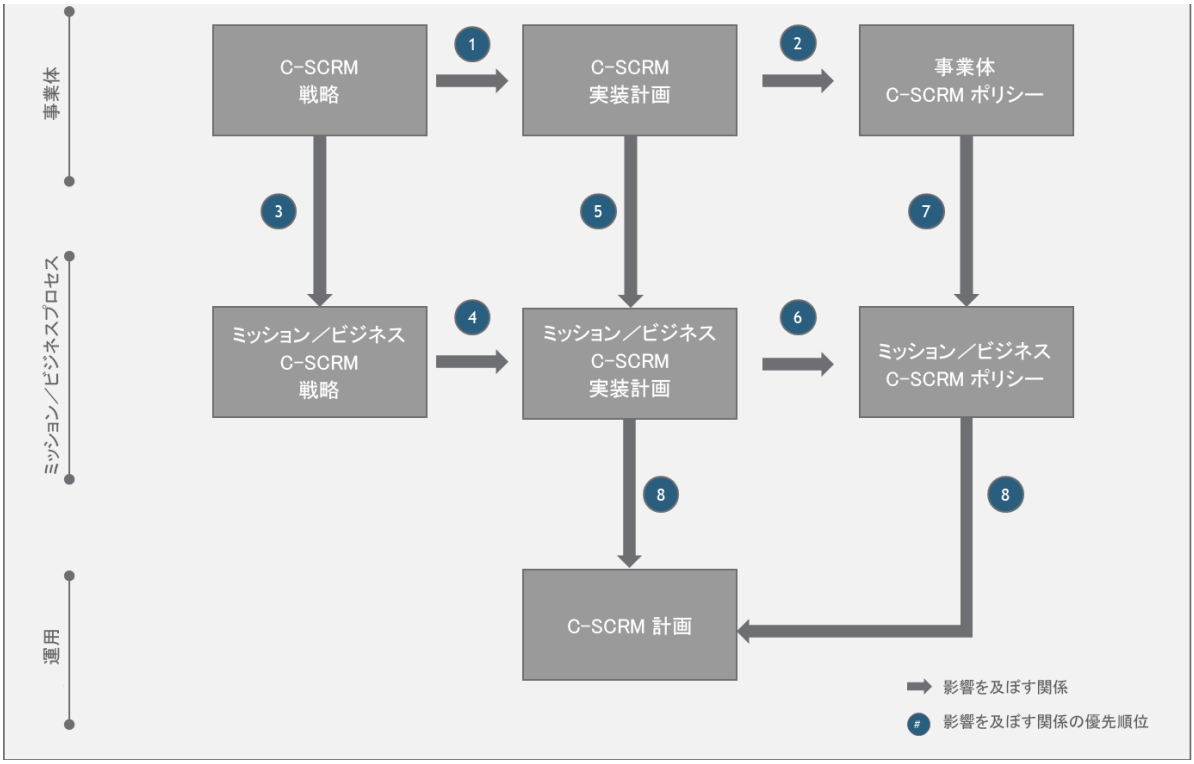

図 2-5：C-SCRM 文書間の関係

以降の節では、各レベルでの役割と活動の例を示している。ただし、事業体はそれぞれ異なるため、これらの活動は、リストされているレベルとは異なるレベルで、個々の事業体の環境に応じて実行される場合がある。

附属書 A は、組織がレベル 1、レベル 2、及びレベル 3 の C-SCRM 活動の指針として役立てるようテーラリングされたキャパシティで利用できる、多くのミッション及びビジネスの C-SCRM 管理策を提供している。テーラリングは、組織のリスクマネジメントニーズに限定することが望ましく、組織が代替のリスク対応の行動方針を評価する際には、C-SCRM のポリシー、ケイパビリティ（能力）、及び管理策を実装しない場合のコストを分析することが望ましいことに留意されたい。これらのコストには、低品質の製品や偽造品、サプライヤによる知的財産の悪用、サプライヤによるミッションクリティカルな情報の改ざんや侵害、脆弱なサプライヤ情報システムを介したサイバー攻撃の曝露（エクスポージャー）などが含まれる可能性がある。

2.3.2. レベル 1：事業体

効果的な C-SCRM には、上級幹部及び管理職からのコミットメント、直接的な関与、継続的なサポートが必要となる。事業体は、政府機関全体の SCRM 活動を主導する責任を、政府機関の特定の組織構造にかかわらず、管理職レベルの個人、オフィス（専門スタッフによるサポート）、又はグループ（例えば、リスク委員会、エグゼクティブ運営委員会、エグゼクティブリーダーシップ評議会）に指定することが望ましい。サプライチェーン全体のサイバーセキュリティリスクは、あらゆる主要な事業部門にわたって存在する可能性があるため、事業体は、サプライチェーンの活動（例えば、取得と調達、情報セキュリティ、情報技術、法務、プログラムマネジメント、サ

プライチェーンと物流）に関与する上級幹部に対して、C-SCRM の役割と責任を確実に定義することが望ましい。管理職による C-SCRM 活動の監督を確立しなければ、事業体は、製品及びサービスを効果的にセキュアにする方法について、組織全体でリスクを判断する能力が制限される。

レベル 1（事業体）は、包括的な C-SCRM 戦略、C-SCRM ポリシー、及び C-SCRM を事業体全体でどのように実装するかを規定する上位レベルの実装計画を提供することにより、事業体全体の C-SCRM 活動の基調と方向性を設定する。レベル 1 では、上級幹部及び管理職がリスク管理者（機能）と C-SCRM について協力し、C-SCRM に関する決定を行い、レベル 2 及びレベル 3 に決定を委任し、C-SCRM のための事業体全体のリソース割り振りの優先順位付けを可能にするガバナンス構造が形成される。レベル 1 の活動は、C-SCRM の軽減戦略が事業体の戦略的な目標と目的に合致していることを確実にするのに役立つ。レベル 1 の活動は、レベル 2 及びレベル 3 で C-SCRM がどのように実施されるかを方向付け、制約する C-SCRM 戦略、ポリシー、及び上位レベルの実装計画に結実する。

サプライチェーンにおけるサイバーセキュリティリスクの所有権と説明責任は、最終的には組織のトップにある。

- 意思決定者は、組織のリスクプロファイル、リスク選好度、及びリスク許容度のレベルに基づいて情報を得る。プロセスでは、リスク判断のエスカレーションが、いつ、どのように発生する必要があるかに対処することが望ましい。
- 所有権は、組織のミッション、業務、又は情報システムに対する執行権限に基づいて、政府機関内の認可権限のある担当者に委任することが望ましい。
- 認可権限のある担当者は、日常的なリスクマネジメントに責任を負う指定職員に、さらに責任を委任しても良い。

C-SCRM は、上級幹部及び管理職からの説明責任、コミットメント、監督、直接的な関与、継続的なサポートを必要とする。事業体は、サプライチェーンの活動（例えば、取得及び調達、情報セキュリティ、情報技術、法務、プログラムマネジメント、サプライチェーンと物流）に関与する上級幹部に対して、C-SCRM の役割と責任が定義されていることを確実にすることが望ましい。レベル 1 では、通常、取締役会が事業体全体のすべてのリスクを評価及び軽減する責任を負う。これは一般的に、事業体のリスクマネジメント（ERM：Enterprise Risk Management）評議会を通じて達成される。効果的な C-SCRM では、最高経営責任者（CEO）、最高リスク管理責任者（CRO）、最高情報責任者（CIO）、最高法務責任者（CLO）／法律顧問、最高情報セキュリティ責任者（CISO）、最高取得責任者（CAO）など、一般的に ERM 評議会内のリーダー達からの視点を収集し、CIO と CISO からの助言や勧告を取締役会に通知する。

CIO 及び／又は CISO は、取締役会の ERM 評議会に情報を提供するための詳細な分析を提供するために、C-SCRM 指向の組織を結成しても良い。C-SCRM 評議会は、事業体のサプライチェーンにおけるサイバーセキュリティリスクの優先順位を設定し、管理するためのフォーラムとして機能する。C-SCRM 評議会又はその他の C-SCRM 指向の組織は、C-SCRM の事業体全体の戦略を策定する責任を負う。C-SCRM 戦略は、ERM 評議会によって確立された事業体の前提条件、制約条件、リスク許容度、優先順位／トレードオフを明確化する。C-SCRM は、取締役会の ERM 評議会内の CIO 及び／又は CISO のメンバーシップを通じて、組織の全体的な事業体リスクマネジメントに統合される。

また、これらのリーダーは、事業体のミッションとビジネスプロセスにまたがる総合的な一連のポリシーを策定して公布し、C-SCRM ケイパビリティ（能力）の確立と成熟、及び団結した一連

の C-SCRM 活動の実施を導く責任及び説明責任を負う。リーダーは、C-SCRM 活動を推進し、事業体に対する協調的な C-SCRM 指向のサービス及びガイダンスの支点として機能させるために、C-SCRM PMO 又はその他の専用の C-SCRM 関連機能を確立することが望ましい。また、リーダーは、実施計画を詳述し、C-SCRM 活動を実行する責任及び説明責任を負う、ミッション及びビジネスプロセスレベルでのリーダーの役割を明確に説明することが望ましい。事業体は、C-SCRM 活動に対する管理職による監督を確立しなければ、製品及びサービスを効果的にセキュアにする方法について、組織全体でリスクを判断する能力が制限されることを考慮することが望ましい。

C-SCRM のガバナンス構造と運用モデルは、C-SCRM の権限、責任、意思決定権限を決定し、C-SCRM プロセスが事業体内でどのように達成されるかを定義する。最善の C-SCRM ガバナンス及び運用モデルは、事業体のビジネス及び機能面の要件を満たすものである。例えば、厳しい予算の制約や厄介な C-SCRM 要件に直面している事業体は、意思決定の権限を一元化し、ベンダのリスクアセスメントなどのリソース集中型タスクの責任を統合するために C-SCRM PMO に依存するガバナンス及び運用モデルを検討することができる。対照的に、ミッションとビジネスプロセスが高度な自律性で管理されている事業体や、高度に差別化された C-SCRM 要件を持つ事業体は、分散化された権限、責任、及び意思決定の権限を選択することができる。

レベル 1 では、C-SCRM のガバナンス構造と運用モデルを定義することに加えて、事業体の C-SCRM を枠組み化するために必要な活動を実行する。C-SCRM の枠組み化は、事業体がサプライチェーン全体のサイバーセキュリティリスク（例えば、脅威、脆弱性、リスクインパクト [21]、リスクの起こりやすさ）、制約条件（例えば、事業体のポリシー、規則、リソースの制限）、選好度と許容度、及び優先順位とトレードオフについての前提条件を明確にし、事業体全体の C-SCRM の決定を導くプロセスである。リスクの枠組み化プロセスは、事業体がサプライチェーン全体のサイバーセキュリティリスクをどのようにアセスメント、対応、監視するかを決定する C-SCRM 戦略を確立するために必要なインプットを提供する。事業体の C-SCRM 戦略の実行を導くために、上位レベルの実装計画も策定することが望ましい。リスクの枠組み化プロセスについては、附属書 C でさらに詳しく説明されている。

リスクの枠組み化プロセス及び C-SCRM 戦略から情報を得て、レベル 1 は事業体の C-SCRM ポリシーを提供する。C-SCRM ポリシーは、C-SCRM プログラムの目的を確立し、事業体の C-SCRM 責任の概要を示し、事業体全体の C-SCRM の役割を定義して権限を付与し、適用できる C-SCRM コンプライアンスと実施の期待及びプロセスの概要を示す。附属書 C は、C-SCRM 戦略と C-SCRM ポリシーのテンプレートの例を提供している。

レベル 1 で実施されるリスクアセスメント活動は、サプライチェーン全体のサイバーセキュリティリスクのアセスメント、対応、及び監視に焦点を当てている。レベル 1 のリスクアセスメントは、事業体のレベル 1 フレームステップ（すなわち、前提条件、制約条件、選好度、許容度、優先順位、及びトレードオフ）に基づいている場合もあれば、複数のミッション及びビジネスプロセスにわたって完了するリスクアセスメントに基づいて事業体レベルの前提条件を集約したものである場合もある。例えば、レベル 1 のリスクアセスメントでは、サプライチェーンの製品又はサービスを通じて生じる事業体の目的に対する脅威への曝露（エクスポージャー）をアセスメントする場合がある。レベル 1 のリスクアセスメントは、レベル 2 で完了したリスクアセスメントを集約及び再コンテキスト化して、事業体の主要目的に対するリスクシナリオを記述することを目的としている場合もある。

[21] リスクインパクトとは、情報又はシステムの機密性、完全性、又は可用性の喪失が、組織の運営、組織の資産、個人、他の組織、又は国家（米国の国家安全保障上の利益を含む）に及ぼす影響を意味する[800-53 R5]。

報告は、サプライチェーン全体のサイバーセキュリティリスクを管理する方法について、情報に基づいた意思決定を行うために必要なコンテキストをレベル 1 の意思決定者に提供する上で重要な役割を果たす。報告では、事業体全体の傾向に焦点を当て、C-SCRM が事業体全体でどの程度実装されているか、C-SCRM の有効性、及びサプライチェーン全体のサイバーセキュリティリスクに関連する状況を含めることが望ましい。C-SCRM の報告では、リーダーシップの緊急の注意及び／又は活動を必要とする状況を強調することが望ましく、一定期間にわたる C-SCRM のリスクとパフォーマンスの傾向を強調することによって利益が得られることもある。事業体内の C-SCRM の責任者及び説明責任者は、リーダーと協力して、頻度、範囲、形式などの報告の要件を識別することが望ましい。報告には、第 3.5.1 節で詳しく説明されている指標を含めることが望ましい。

レベル 1 の活動は、最終的に、事業体のミッション及びビジネスプロセスがサプライチェーン全体のサイバーセキュリティリスクを管理するための包括的なコンテキストと境界を提供する。レベル 1 のアウトプット（例えば、C-SCRM 戦略、C-SCRM ポリシー、ガバナンス、運用モデル）は、各ミッション及びビジネスプロセスのコンテキストに合わせて、レベル 2 でさらにテーラリング及び精緻化される。また、レベル 1 のアウトプットは、下位レベルの C-SCRM アウトプットから繰り返し情報を得て、その結果を受けて更新されるのが望ましい。

複雑な事業体では、レベル 1 の活動は事業体レベルで完了する場合と個々の組織レベルで完了する場合があることに留意されたい。事業体のレベル 1 の活動は、組織のレベル 1 の活動を形成し、導くことが望ましい。

追加情報は、本出版物の附属書 *A* と、*NIST SP 800-53 Rev. 5* の *SR-1*、*SR-3*、*PM-2*、*PM-6*、*PM-7*、*PM-9*、*PM-28*、*PM-29*、*PM-30*、及び *PM-31* で見つけることができる。

2.3.3. レベル 2：ミッション及びビジネスプロセス

レベル 2 では、事業体のミッション及びビジネスプロセスが、サプライチェーン全体のサイバーセキュリティリスクをどのようにアセスメントし、対応し、監視するかについて取り組む。レベル 2 の活動は、レベル 1 で示された C-SCRM 戦略とポリシーに従って実行される [22]。このレベルでは、プロセス固有の C-SCRM 戦略、ポリシー、及び実装計画によって、各ミッション及びビジネスプロセス内で事業体の C-SCRM の目標と要件をどのように満たすかが決まる。ここでは、特定の C-SCRM プログラムの要件が定義及び管理され、これには、コスト、スケジュール、パフォーマンス、セキュリティ、及び様々な重要な非機能要件を含める。これらの非機能要件には、（故障率などの狭義の）信頼性（reliability）、（保守・運用性を含む広義の）信頼性（dependability）、安全性、セキュリティ、品質などの概念が含まれる。

レベル 2 の役割には、プログラムマネージャ、研究開発、取得／調達など、各ミッション及びビジネスプロセスの代表者が含まれる。レベル 2 の C-SCRM 活動は、事業体のミッション及びビジネスプロセスのコンテキストの中で C-SCRM に対処する。各ミッション及びビジネスプロセスの特定の要件に合わせて C-SCRM の実装をテーラリングするために、具体的な戦略、ポリシー、及び手順を策定することが望ましい。上位レベルの事業体戦略及び実装計画をさらに発展させるために、事業体内の様々なミッション領域又は事業部門は、独自にテーラリングしたミッション及びビジネスレベルの戦略と実装計画を作成する必要がある場合があり、上位レベルの C-SCRM 戦略で規定された制約条件の範囲内で、かつ C-SCRM ポリシーに準拠して、確実に C-SCRM が実行されることが望ましい。レベル 2 の戦略及び実装計画の策定と実行を容易にするために、事業体は、各ミッション及びビジネスプロセスの代表者で構成される委員会を結成することで利益を

[22] 詳細については、[NIST SP 800-39、第 2.2 節]を参照のこと。

得ることができる可能性がある。ミッションとビジネスプロセスの間の調整と協力は、リスク認識を促進し、サプライチェーン全体のサイバーセキュリティリスクを識別し、事業体と C-SCRM アーキテクチャの開発をサポートするのに役立つ。また、C-SCRM PMO は、サービス（例えば、ポリシーテンプレート、C-SCRM の特定分野専門家（SME）サポート）の提供を通じて、レベル 2 での C-SCRM の実装を支援することもできる。

サプライチェーンに対する、及びサプライチェーンを介した多くの脅威は、サプライヤ、開発者、システムインテグレータ、外部のシステムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの第三者関係の管理において、レベル 2 で対処される。C-SCRM はミッションプロセスに直接的にも間接的にもインパクトを与える可能性があるため、このレベルの C-SCRM 活動を理解、統合、及び調整することは極めて重要である。レベル 2 の活動は、特定のミッション及びビジネスプロセスの脅威、脆弱性、インパクト [23]、及び起こりやすさに合わせて、事業体の C-SCRM フレームをテーラリングして適用することに焦点を当てている。レベル 1 のアウトプット（例えば、C-SCRM 戦略）から情報を得て、ミッション及びビジネスプロセスは、事業体の全体的な戦略を特定のミッション及びビジネスプロセスに合わせてテーラリングする C-SCRM 戦略を採用する。レベル 2 では、事業体は、プロセスに対する事業体のポリシーをコンテキスト化するミッション及びビジネスプロセスに固有のポリシーを発行することもできる。

特定のミッション及びビジネスプロセスの事業体リーダーは、C-SCRM 戦略に従って C-SCRM 実装計画を策定及び実行することが望ましい。C-SCRM 実装計画は、ミッション及びビジネスプロセス内で C-SCRM 戦略を運用できるようにするための、より詳細なロードマップを提供する。C-SCRM 実装計画では、ミッション及びビジネスプロセスは、C-SCRM の役割、責任、実装マイルストーン、日付、監視と報告のプロセスを規定することになる。本出版物の附属書 D は、C-SCRM 戦略、実装計画、及び C-SCRM ポリシーのテンプレート例を提供している。

レベル 2 で実行される C-SCRM 活動は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダへのミッションとビジネスプロセスの依存関係から生じるリスクの暴露（エクスポージャー）のアセスメント、対応、監視に焦点を当てている。サプライチェーンに対するリスクの曝露（エクスポージャー）は、サプライチェーンへの一次的な依存関係、又は個々の情報システムもしくはその他のミッション及びビジネスプロセスへの二次的な依存関係の結果として発生する可能性がある。例えば、重要なプロセスが依存する複数の情報システムに重要なシステムコンポーネント又はサービスを提供しているサプライヤが原因で、リスクの曝露（エクスポージャー）が発生する可能性がある。また、情報システムとは無関係のベンダが提供する製品やサービス、及びこれらの製品やサービスが全体的なミッション及びビジネスプロセスの目的において果たす役割によってもリスクが発生する可能性がある。事業体は、サプライチェーン全体のサイバーセキュリティリスクについて、従来とは異なる原因を考慮することが望ましい。これらのリスクは、オープンソースソフトウェアの使用から生じるものなど、C-SCRM プロセスを回避したり、免れたりする可能性がある。事業体は、サプライチェーン全体で従来とは異なるサイバーセキュリティリスクを管理するためのポリシーや管理策を確立することが望ましい。

[23] これらのインパクトは、情報又はシステムの機密性、完全性、又は可用性の喪失が、組織の運営、組織の資産、個人、他の組織、又は国家（米国の国家安全保障上の利益を含む）に及ぼす影響を指す[SP 800-53 Rev. 5]。

レベル 2 での報告は、ミッション及びビジネスプロセスのリーダーに、ミッション及びビジネスプロセスの範囲内で C-SCRM を管理するために必要なコンテキストを提供する上で重要な役割を果たす。レベル 2 で扱われるトピックは、レベル 1 で扱われるトピックを反映したものとなるが、対応する特定のミッション及びビジネスプロセスに焦点を当てるように再編成することが望ましい。レベル 2 の報告には、レベル 1 及びレベル 2 で定義された、事業体が規定したリスク選好度及びリスク許容度の記述とは対照的に、ミッション及びビジネスプロセスのパフォーマンスを示す指標を含めることが望ましい。報告の要件は、ミッション及びビジネスプロセスのリーダーのニーズとレベル 1 のニーズを満たすように定義することが望ましい。

レベル 2 の活動からのアウトプットは、レベル 3 での C-SCRM 活動の実行方法に大きなインパクトを与える。例えば、リスク許容度と共通管理策ベースラインの決定は、レベル 2 で定義された後、レベル 3 で個々の情報システムのコンテキストに合わせてテーラリング及び適用される場合がある。また、レベル 2 のアウトプットは、レベル 1 のアウトプットに繰り返し影響を与え、さらに洗練させるためにも使用することが望ましい。

追加情報は、本出版物の附属書 *A* と、*NIST SP 800-53 Rev. 5* の *SR-1*、*SR-3*、*SR-6*、*PM-2*、*PM-6*、*PM-7*、*PM-30*、*PM-31*、及び *PM-32* に記載されている。

2.3.4. レベル 3：運用

レベル 3 は、事業体の SDLC（研究開発、設計、製造、納入、統合、運用及び保守、システムの廃棄／廃止など）の一部として、調達の実施及びシステム関連の C-SCRM 活動の実行を含む、運用活動に責任及び説明責任を負う人員で構成される。これらの人員には、システム所有者、契約責任者、契約責任者の代理人、設計者、システムエンジニア、情報セキュリティの専門家、システムインテグレータ、及び開発者が含まれる。これらの人員は、C-SCRM 管理策（請負業者などの外部関係者に適用されるものを含む）の管理、実装アシュアランス、及び監視に加えて、ミッション及びビジネスプロセスをサポートするための SDLC 全体にわたるシステム及びコンポーネントの取得、開発、及び維持に対処するための C-SCRM 計画を策定する責任を負う。C-SCRM PMO が確立されている事業体では、製品のリスクアセスメントなどの活動を一元化された共有サービスとして提供してもよい。

レベル 3 では、レベル 1 及びレベル 2 で完了した C-SCRM 活動によって提供されるアウトプットにより、事業体は RMF [NIST 800-37r2]に従って運用レベルで C-SCRM を実行する準備を行う。C-SCRM は、C-SCRM 計画の策定及び実装を通じて、情報システムに適用される。これらの計画は、レベル 1 及びレベル 2 で定義された前提条件、制約条件、リスク選好度と許容度、優先順位、及びトレードオフに大きく影響される。C-SCRM 計画は、取得（カスタムと既製品の両方）、要件、アーキテクチャ設計、開発、納入、設置、統合、保守、廃棄／廃止といった SDLC のすべてのシステムに C-SCRM 活動をどのように統合するかを決定する。一般に、C-SCRM 計画は実装に特化したものであり、ミッション及びビジネスプロセスをサポートするシステムのポリシーの実装、要件、制約条件、及び影響を規定する。

レベル 3 の活動は、サプライチェーンを通じて提供される ICT/OT 関連の製品及びサービスのうち、事業体が使用しているもの、又はシステム認可境界の範囲内にあるものから生じる、運用レベルでのリスクの曝露（エクスポージャー）を管理することに焦点を当てている。レベル 3 の C-SCRM 活動は、運用レベルの（例えば、システム又はシステムコンポーネント内の）脆弱性を悪用する潜在的なサプライチェーンのサイバーセキュリティ脅威の起こりやすさ及びインパクトを分析することから始まる。該当する場合、これらのリスクアセスメントは、レベル 1 及びレベル 2 で完了したリスクアセスメントから情報を得ることが望ましい。リスクの決定に応じて、事業体は、リスクの曝露（エクスポージャー）を低減するための代替の行動方針（例えば、受容、回避、軽減、共有及び／又は移転）を評価することが望ましい。リスク対応は、RMF [NIST 800-37r2]に従って SLDC 全体で C-SCRM 管理策を選択、テーラリング、実装、及び監視することによって達成される。選択された C-SCRM 管理策は、多くの場合、レベル 1 及びレベル 2 から継承された共通管理策とレベル 3 の情報システム固有の管理策の組み合わせで構成される。

レベル 3 での報告は、C-SCRM の実装、効率性、有効性、及び特定のシステムのサプライチェーンにおけるサイバーセキュリティリスクへの全体的な曝露（エクスポージャー）レベルに焦点を当てるのが望ましい。システムレベルの報告は、迅速な調整とリスク状況への対応を可能にする戦術レベルの洞察を、システム所有者に提供することが望ましい。レベル 3 の報告には、レベル 1、2、及び 3 で定義された事業体のリスク選好度の記述とリスク許容度の記述に対するパフォーマンスを示す指標を含めることが望ましい。

レベル 3 の重要な活動は、C-SCRM 計画の策定である。C-SCRM 計画には、適用されるセキュリティ管理策情報に加えて、システム、その分類、運用状況、関連する合意事項、アーキテクチャ、重要なシステムの担当者、関連する法律、規制、ポリシー、及び緊急時対応計画に関する情報が含まれる。C-SCRM では、継続的な衛生管理が重要であり、C-SCRM 計画は、実装された C-SCRM 管理策の継続的監視のための参照情報として保守及び使用されることが望ましい生きた文書である。C-SCRM 計画は定期的に参照されることを意図しており、定期的に見直して更新することが望ましい。これらは、コンプライアンス要件を満たすために作成された文書ではない。むしろ、事業体は、3 つのレベルすべてにおいて、C-SCRM 活動と決定を形成し、調整し、情報提供し、実行するための計画を、これまでどのように効果的に採用し続けているかを実証できることが望ましい。
レベル 3 の C-SCRM 活動の一環として収集された情報は、C-SCRM 戦略及び実装計画をさらに洗練させるために、レベル 1 及びレベル 2 で完了した C-SCRM 活動に繰り返し情報を提供することが望ましい。

追加情報は、本出版物の附属書 *A* と、*NIST SP 800-53 Rev. 5* の *SR-1*、*SR-2*、*SR-6*、*PL-2*、*PM-31*、及び *PM-32* に記載されている。

2.3.5. C-SCRM PMO

様々な運用モデル（例えば、集中型、分散型、ハイブリッド型）は、事業体とそのミッション及びビジネスプロセス全体にわたる C-SCRM 活動を促進する。そのようなモデルの 1 つは、特定の C-SCRM 活動に対する責任を中央の PMO に集中させ、割り当てるものである。このモデルでは、C-SCRM PMO は他のミッション及びビジネスプロセスに対するサービスプロバイダとして機能する。その結果、ミッション及びビジネスプロセスは、事業体の C-SCRM の目標と目的を達成するための責任の一部として、C-SCRM PMO からサービスを選択して要求する責任を負う。PMO が提供できる様々な有益なサービスには、以下のようなものがある。

- アドバイザリーサービス及び対象分野の専門知識
- 内部 C-SCRM ワーキンググループ、評議会、又はその他の調整機関の議長
- ツール、ジョブ支援、意識向上、及びトレーニングのテンプレートの一元化されたハブ
- サプライヤ及び製品のリスクアセスメント
- 外部ステークホルダーとの連絡
- 情報共有管理（例えば、部門／政府機関内、FASC との間）
- C-SCRM リスクレジスタの管理
- 事業体の C-SCRM ガバナンスのための事務局／人員配置機能
- C-SCRM プロジェクト及びパフォーマンス管理
- C-SCRM の説明会、プレゼンテーション、及び報告

C-SCRM PMO は、通常、事業体とそのミッション及びビジネスプロセス全体にわたる C-SCRM 戦略と実装の推進を支援するのに役立つ C-SCRM SME で構成される。C-SCRM PMO は、事業体全体の C-SCRM 活動を監督する責任及び説明責任を負う専任の管理職レベルの責任者が含まれている場合もあれば、そのような責任者に報告する場合もある。C-SCRM PMO は、専任の人員で構成するか、情報セキュリティ、調達、リスクマネジメント、エンジニアリング、ソフトウェア開発、IT、法務、人事など、事業体のいくつかのプロセスから C-SCRM に責任を持つ代表者をマトリクス組織として含めることが望ましい。C-SCRM PMO がレベル 1 であるかレベル 2 であるかに関わらず、C-SCRM PMO に分野横断的な代表者を含めることが重要である。

C-SCRM PMO の責任には、事業体全体でどのように C-SCRM を適用するかについての方向付けに役立つサービスを事業体のリーダーに提供することが含まれる場合がある。C-SCRM PMO は、サプライチェーン全体のサイバーセキュリティリスクに対する事業体の選好度と許容度の確立を含むリスクの枠組み化プロセスを通じて、レベル 1 のステークホルダーを導くための SME の サポートを提供することができる。さらに、説明責任を負うリスク管理者は、事業体の C-SCRM 戦略及びポリシーを起草する責任を PMO に委任することもできる。C-SCRM PMO は、内部又は外部のエンティティとの C-SCRM 情報共有を調整することもできる。最後に、PMO は、レベル 1 のステークホルダーがサプライチェーン全体のサイバーセキュリティリスクの統合的な観点を養うのに役立つように、C-SCRM に焦点を当てた管理職レベルの説明会を（例えば、リスク管理者機能や取締役会などに対して）実施することができる。

レベル 2 では、C-SCRM PMO は、基本戦略及び、特定のミッション及びビジネスプロセス内でさらにカスタマイズできる一連のポリシー、手順、及びガイドラインを含む C-SCRM スターターキットを開発することができる。この PMO は、プロセス固有の C-SCRM 戦略を策定し、C-SCRM 実施計画を策定する際に、ミッション及びビジネスプロセス内のステークホルダーに SME コンサルティングサポートを提供することもできる。この責任の一環として、C-SCRM PMO は、事業体のミッション及びビジネスプロセスにおける C-SCRM の共通管理策ベースラインについて助言したり、共通管理策ベースラインを策定したりする場合がある。また、C-SCRM PMO は、技術及び非技術に関連する製品及びサービスのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダに焦点を当てた C-SCRM リスクアセスメントを実施する場合もある。

レベル 1 及びレベル 2 での C-SCRM PMO の責任は、最終的にレベル 3 の運用レベルでの C-SCRM 活動に影響を与える。C-SCRM PMO は、C-SCRM 管理策の選択、テーラリング、及び監視について、SDLC 全体を通じてチームに助言することができる。最終的に、C-SCRM PMO は、リスクマネジメントレベル全体で C-SCRM のアウトプットを生成する活動に責任を負う場合がある。C-SCRM サービスを一元化することにより、事業体は、高品質の C-SCRM サービスを事業体の他の部門／担当者に提供する統合チーム内の専門的なスキルセットを活用する機会を得る。リスクアセスメントサービスを一元化することで、事業体は他の方法（例えば、分散型モデルで）では不可能なレベルの標準化を実現できる場合がある。また、事業体は、PMO のリソースが C-SCRM の活動に専念している場合、C-SCRM の責任に加えて複数の役割を果たす可能性がある分散型モデルのリソースと比較して、コスト効率性も実現できる場合がある。

C-SCRM PMO モデルは、一般的に、異なる一連のミッション及びビジネスプロセスにわたって C-SCRM のプラクティスを標準化する必要とする、より大規模で複雑な事業体に適している。最終的に、事業体は、利用可能なリソースとコンテキストに応じた、適用可能かつ適切な C-SCRM 運用モデルを選択することが望ましい。

重要ポイント [24]

C-SCRM のビジネスケース。 C-SCRM は、重要なシステムの理解、サプライチェーンの侵害の可能性の低減、運用と事業体の効率化、製品の品質及びセキュリティの問題の減少、提供されるサービスの確実性と信頼性の向上など、多くの利点を事業体に提供する。

サプライチェーンにおけるサイバーセキュリティリスク。 サプライヤ、そのサプライチェーン、及び提供される製品又はサービスとの関係から生じる損害や侵害の可能性は、人間又は人間以外の脅威がシステム、製品、サービス、又はサプライチェーンエコシステムに関連する脆弱性を悪用することに成功すると具現化する。

マルチレベルの分野横断的な C-SCRM。 [NIST SP 800-39]で説明されているように、マルチレベルのリスクマネジメントとは、事業体（例えば、CEO、COO）、ミッション及びビジネスプロセス（例えば、ビジネスマネジメント、研究開発）、及び運用（例えば、システムマネジメント）のレベルで、サプライチェーンのサイバーセキュリティリスクマネジメント活動を目的を持って実行し、継続的に改善することである。各レベルには、複数の分野（例えば、情報セキュリティ、調達、事業体のリスクマネジメント、エンジニアリング、ソフトウェア開発、IT、法務、人事）のステークホルダーが含まれ、C-SCRM を共同で実行し、継続的に改善する。

C-SCRM PMO。 C-SCRM PMO として知られる専門オフィスは、事業体の他の部門／担当者にサポート製品（例えば、ポリシーテンプレート）及びサービス（例えば、ベンダのリスクアセスメント）を提供することにより、事業体の C-SCRM 活動をサポートすることができる。C-SCRM PMO は、事業体によって、3 つのレベルにわたってサポートを提供する場合もあれば、レベル 1 又はレベル 2 に位置する場合もある。

C-SCRM はライフサイクルプロセスである。 C-SCRM 活動は、適用される事業体のライフサイクルプロセス（例えば、SDLC）全体で統合及び実行することが望ましい。例えば、システムでは、サプライチェーンのサイバーセキュリティリスクは、運用フェーズ及び保守フェーズで具現化する可能性があり、実際に具現化している。組織は、サプライチェーンのサイバーセキュリティリスクを継続的にアセスメント、対応、及び監視するために、適切な C-SCRM 活動が実施されていることを確実にすることが望ましい。

[24] 重要ポイントでは、その節の本文から重要な点を説明している。定義については、附属書 H の用語集を参照のこと。

3. 重要成功要因

サプライチェーン全体で進化するサイバーセキュリティリスクにうまく対処するために、事業体は、複数の内部プロセス及びケイパビリティ（能力）を関与させ、事業体レベル及びミッション領域を超えてコミュニケーションとコラボレーションを行い、事業体内のすべての個人がサプライチェーン全体のサイバーセキュリティリスクの管理における自分の役割を理解することを確実にする必要がある。事業体には、サプライチェーンのサイバーセキュリティ管理策及びプラクティスに有効性を伝達し、実装する最善の方法を決定し、監視するための戦略が必要である。事業体は、サプライチェーンのサイバーセキュリティリスクマネジメント管理策を内部で伝達することに加え、C-SCRM に関する知見を交換するために同業者と関与することが望ましい。これらの知見は、事業体がどの程度うまくいっているかを継続的に評価し、どこを改善する必要があるか、及び どのように C-SCRM プログラムを成熟させるための措置を講じるかを識別するのに役立つ。この節では、C-SCRM を成功させるために必要な事業体のプロセスとケイパビリティ（能力）を取り上げる。本出版物ではこれらの重要成功要因を取り上げているが、これは事業体による C-SCRM の実行の成功に貢献する一連の要因を網羅したものではない。重要成功要因は流動的であり、環境及び事業体自体のケイパビリティ（能力）の進歩に伴って時間と共に進化していく。

3.1. 取得における C-SCRM [25]

サプライチェーン全体のサイバーセキュリティリスクマネジメントを強化するためには、調達及び契約管理のライフサイクルプロセスのすべてのステップ内で、C-SCRM の考慮事項を取得活動に統合することが不可欠である。このライフサイクルは、調達担当職員がニーズを識別することから始まり、要件の計画及び明確化、実行可能な供給源の識別及びアセスメントするための調査の実施、入札公募、C-SCRM 要件への適合性を確認するための提案の評価、並びに入札者及び提案された製品及び／又はサービスに関連する C-SCRM リスクのアセスメントのプロセスが含まれる。契約締結後は、サプライヤが契約上の合意で明示された諸条件を満たしていること、及びその製品及びサービスが期待及び要求どおりであることを確実にする。サプライチェーンのサイバーセキュリティリスクに影響を及ぼす可能性がある変更の監視は、ライフサイクルを通じて実施されることが望ましく、当初のアセスメントの再評価のきっかけとなったり、軽減対応を必要としたりする場合がある。

事業体は、事業を実施し、ミッション及び経営目標を達成するために、市販製品と外部委託サービスに大きく依存している。ただし、製品及びサービスは、オープンソースソフトウェアの場合と同様に、共有サービスを事業体内のプロバイダに依存すること、又は新たなニーズを満たすために既存の製品を別の目的で使用することで、調達プロセス以外でも取得できることを強調することが重要である。C-SCRM は、こうした他の「取得」プロセスにも対処しなければならない。

事業体は、サプライチェーン全体のサイバーセキュリティリスクに対処し、取得プロセスの各フェーズで C-SCRM 活動を実施することに加え、全体的なリスクの曝露（エクスポージャー）の低減を推進する取得戦略を策定し、実行することが望ましい。このような戦略を適用することで、事業体はサプライチェーン全体、特定の調達プロセス内、および事業体全体のサイバーセキュリティリスクを低減することができる。事業体は、C-SCRM を取得活動に統合する取得ポリシー及びプロセスを採用することによって、目標とするリスク低減成果を実現するための取り組みを支援し、指示し、情報を提供することになる。

[25] 各省庁及び関係機関は、大統領令 14028 号、国家のサイバーセキュリティの向上（Improving the Nation’s Cybersecurity）に従ってこのガイダンスを実装するときに附属書 F を参照することが望ましい。

さらに、業界で認められている一連の標準及びガイドライン（NIST 800-53, Rev.5、NIST CSF など）に沿った C-SCRM 管理策を採用することにより、事業体は、サプライチェーン全体のサイバーセキュリティリスクと、対応する C-SCRM プラクティスの全体的な網羅範囲を確実にすることができる。C-SCRM 管理策は、事業体自体、一次請負業者、及び二次請負業者を含む、サプライチェーンの様々な参加者に適用される場合がある。事業体は、ICT/OT 製品及びサービスの開発及び実装を一次請負業者と二次請負業者に大きく依存しているため、SDLC 内で実装されたこれらの管理策は二次請負業者に伝わる可能性が高い。サプライチェーン及び SDLC 全体に適用可能な C-SCRM 管理策を確立することは、事業体が、サプライチェーン全体のサイバーセキュリティリスクを管理するすべての参加者を支援するために、サプライヤ及び下請サプライヤとの共通の用語群と一連の期待を確立するのに役立つ。

3.1.1. C-SCRM 戦略及び実装計画における取得

事業体の C-SCRM 戦略及び実装計画は、サプライチェーン全体のサイバーセキュリティリスクの曝露（エクスポージャー）の長期的かつ持続的な低減の達成に向けて事業体を導く。事業体は、C-SCRM 戦略及び実装計画の中核部分として、取得プロセスを通じて、このリスクをどのように管理するかに取り組むことが望ましい。

サプライチェーンのサイバーセキュリティリスクには、サプライヤの事業体、製品、サービス、及びサプライヤ自体のサプライヤ及びサプライチェーンから生じるものが含まれる。C-SCRM PMO は、C-SCRM の考慮事項を取得に統合するための具体的な戦略及び実装計画を策定する際に役立つ可能性がある。C-SCRM に関連する取得活動には、以下が含まれる。

- サプライヤ関係管理の取り組みの一環として、C-SCRM の認識を高め、期待事項を伝達する。
- 必要な規定及び保護が実施されていることを確実にするために、調達要求の一部として満たさなければならない、取得のセキュリティ要件のチェックリストを確立する。
- 外部の共有サービスプロバイダを活用するか、C-SCRM PMO を利用して、サプライヤ、製品、及び／又はサービスのアセスメント活動を共有サービスとして、取得を含む他の内部プロセスに提供する。
- 入札者の責任に関する決定を通知し、入札者のリスク態勢又は特定の製品又はサービスに関連するリスクを識別及びアセスメントするために、デューデリジェンスを実施する。
- 入念に検査され承認されたライブラリから、オープンソースソフトウェアを取得する。
- 供給源選択評価に C-SCRM の基準を含める。
- 適用される規制及び法律の参考文献に基づき、該当する場合には禁止されているサプライヤのリストを確立し、参照する。
- 事業体又はその他の受け入れ可能な適格リストプログラム活動 [CISA SCRM WG3] で定義された厳格なプロセスを通じて、事業体のセキュリティ要件への準拠を実証した承認された製品リスト、又は推奨サプライヤ又は適格サプライヤのリストを確立し、そこから調達する。
- ソフトウェア製品、論理回路搭載製品（すなわち、ハードウェア）を含む製品が、政府機関が承認した適切なプロトコルに準拠したソフトウェア部品表と共に供給されることを確実にする。

C-SCRM 戦略及び実装計画では、C-SCRM プログラムの実装に必要な取得セキュリティ関連の基本要素を扱うことが望ましい。この戦略をサポートするため、事業体の責任者は、取得における C-SCRM の価値と重要性を促進し、必要な活動のために十分な専用の資金が確保されることを確実にすることが望ましい。このようにすることで、事業体が、プログラム又はビジネスプロセスに対する責任と、成果の達成に向けた進捗に対する説明責任を確実にするのに役立つ。事業体は、C-SCRM 活動を確実に完了できるようにするために、取得及びプロジェクトの活動に十分な時間を組み込むことが望ましい。事業体はまた、役割及び責任を割り当てることが望ましく、その中には、本質的に事業体間に共通でチームベースのものもあれば、取得プロセスに特有のものもある。最後に、役割及び責任が理解され、責任者の期待に沿った形で実行されることを確実にするために、取得要員に対して関連するトレーニングが提供されることが望ましい。

事業体のケイパビリティ（能力）、リソース、事業の制約条件、並びにサプライヤとの関係、契約、取得したサービス、及び製品の既存のポートフォリオは、現実的かつ達成可能な戦略上の道筋を定めるために必要なベースラインのコンテキストを提供する。このベースラインの出発点は、パフォーマンスの進捗と成果を追跡してアセスメントするためのマーカーとしても機能する。

重要な最初のステップは、事業体のサプライヤとの関係、契約、及びこれらのサプライヤが提供するすべての製品又はサービスが含まれている最新かつ正確なインベントリが存在することを確実にすることである。この情報により、これらのサプライヤを、組織が定めた戦略的に関連するグループ分けにマッピングすることが可能になる。例えば、サプライヤをアセスメントした結果、複数のカテゴリ（例えば）、「戦略的／革新的」、「ミッションクリティカル」、「持続的」、又は「標準／非必須」）にグループ分けにつながる可能性がある。このセグメント化により、サプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）の更なる分析と理解が容易になり、事業体とそのミッション及びビジネスプロセスにとって最も戦略的又は事業上重要なこれらのサプライヤに着目し、優先順位を割り当てるのに役立つ。単一の供給源への過度の依存など、どの製品及びサービスがリスク軽減及びリスク領域において、より高い信頼度を必要とするかを識別することは有用である。また、このインベントリとマッピングは、C-SCRM の契約の文言と評価基準の選択及びテーラリングを容易にする。

追加情報は、本出版物の附属書 *A*、*[NISTIR 8179]*、及び *NIST SP 800-53, Rev. 5* の *SA-1*、*SA-2*、*SA-4*、*SR-5*、*SR-13* に記載されている。

3.1.2. 取得プロセスにおける C-SCRM の役割

事業体は調達を実施する際に、取得チーム及び／又は統合プロジェクトチーム [26] のメンバーとして取得プロセスに参加する様々な特定分野の専門家を指名することが望ましい。これには、プログラム担当職員、技術及びセキュリティの専門知識を持つ担当者、及び供給・調達のコミュニティの代表者が含まれる。調達の要件は、特定の目的に対応し、特定の目的に合わせてテーラリングされ、コンプライアンスの義務が満たされることを確実にする一方で、サプライチェーンのサイバーセキュリティリスクに効果的に対処するためには、ミッションの重要度、データの機密性、及び運用環境などのコンテキスト的要因も考慮しなければならない。

このコンテキスト的基盤は、調達チームが特定の調達要件に関連するリスクの許容度を効果的に測定するための準備が整い、本出版物で説明する C-SCRM 管理策及び [NIST SP 800-53 Rev 5] の管理策のうち、どの管理策が特定の取得に関連していて、考慮する必要があるかを決定するた

[26] 統合プロジェクトチームは、FAR により定義されている取得チームと同等である。

めの段階を設定する。計画部門又は取得担当職員は、この管理策の選択プロセスを完了するために情報セキュリティ担当者と相談し、これらの管理策を要件文書及び契約に組み込むために調達担当職員と協力することが望ましい。セキュリティは、調達の決定において重要な要素である。このため、事業体は、ICT/OT 関連製品又はサービスを購入する際、「技術的に許容可能な最低価格」（LTPA：Lowest Price, Technically Acceptable）の供給源選定プロセスの使用を避けることが望ましい。

取得ポリシー及びプロセスは、[NISTIR 7622] で説明されているように、調達及び契約管理のライフサイクルプロセス管理プロセスの各ステップ（すなわち、調達の計画、要件の定義と策定、市場分析の実施、調達の完了、コンプライアンスの確保、及び C-SCRM のリスク状況に影響を与える変更のパフォーマンスの監視）に C-SCRM の考慮事項を組み入れる必要がある。これには、ICT/OT 関連のチャージカードを購入する際に、サプライチェーン全体のサイバーセキュリティリスクに対処することを確実にすることが含まれる。

「調達の計画」ステップでは、調達する商品又はサービスの必要性及び重要度を、その必要性及び重要度のレベルの判断を促進する要因の説明とともに識別する必要がある。これは、どの程度のリスクを許容できるか、誰が計画の策定に関与することが望ましいか、及び満たす必要がある特定の要件の策定についての情報を提供する。この活動は通常、取得者のミッション及びビジネスプロセスのオーナー又は被指名人が、調達担当職員又は契約責任者の代理人と協力して主導する。

計画フェーズでは、事業体は、パフォーマンス、スケジュール、費用の目的を明記することに加えて、サプライチェーン全体のサイバーセキュリティリスクに対処するための要件を策定及び定義することが望ましい。このプロセスは通常、取得者のミッション及びビジネスプロセスのオーナー又は被指名人が、調達担当職員又は C-SCRM チームの他のメンバーと協力して開始する。

要件が定義されると、事業体は通常、潜在的なサプライヤの市場分析を完了する。市場調査及び分析活動では、潜在的又は事前に認定された供給源の可用性を調査する。このステップは通常、取得者のミッション及びビジネスプロセスのオーナー又は指名された代理人によって開始される。事業体は、サプライヤのリスクプロファイルを作成するために、潜在的なサプライヤ及び／又は製品に対するより堅牢なデューデリジェンス調査を実施するときに、このフェーズを使用することが望ましい。デューデリジェンスの一環として、事業体は、サプライチェーン内の相互依存関係を識別する手段として、人気の高い製品又はサービスの市場集中を考慮してもよい。事業体はまた、潜在的なサプライヤからの証拠の最初の審査と収集のために、情報提供依頼書（RFI）、公募市場調査通知（SSN：Sources Sought Notice）、及び／又はデューデリジェンスの質問票を使用してもよい。事業体は、初期の C-SCRM デューデリジェンスリスクアセスメントを網羅的なものとして扱うことは望ましくない。この調査の結果は、調達アプローチの形成及び要件の精緻化にも役立つ。

最後に、事業体は、提案依頼書（RFP）又は見積依頼書（RFQ）を発行するための作業ステートメント（SOW）、パフォーマンス基準業務記述書（PWS）、又は業務趣意書（SOO）を発行して、調達ステップを完了する。RFP 又は RFQ に回答するすべての入札者は、関連する重要な C-SCRM 基準に照らして評価されることが望ましい。また、RFP のレビュープロセスには、調達固有のサプライヤのリスクアセスメントを含めることが望ましい。アセスメント基準は、定義された C-SCRM 要件によって多くの情報が提供され、事業体、そのセキュリティプロセス、及びそのセキュリティ追跡記録に関する情報の範囲が含まれるが、これらに限定されない。回答レビュープロセスには、調達、ミッション及びビジネスプロセスオーナー、適切な情報システム所有者、技術専門家などの複数の C-SCRM ステークホルダーが関与する。購入に先立ち、事業体は、製品又はシステムコンポーネントの品質、脆弱性の真正性、及びその他の関連するサプライチェーンのサ

イバーセキュリティリスク要因を識別し、アセスメントすること、及び展開前にこのリスクアセスメントを完了することが望ましい。

契約履行後は、事業体は、サプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）を変えるような変更がないか監視することが望ましい。このような変更には、事業体又はシステムの内部の変更、サプライヤの運用又は構造の変更、製品の更新、地政学的又は環境的な変化が含まれる場合がある。契約には、受容可能なレベルまで適切に軽減できないサプライチェーンのサイバーセキュリティリスクに対する変更が生じた場合に、契約終了の根拠となる条項を含めることが望ましい。最後に、事業体は、サプライチェーン全体のサイバーセキュリティリスクのアセスメント、対応、監視を行う能力を強化するために、取得プロセスで得た教訓を継続的に適用することが望ましい。

表 3-1 は、調達プロセスの各ステップにおいて、C-SCRM アセスメントが実施される可能性がある時点の概要を示している。

表 3-1：調達プロセスにおける C-SCRM

調達プロセス	サービスのリスクアセスメント	サプライヤのリスクアセスメント	製品のリスクアセスメント
調達の計画	サービスのリスクアセスメント、必要なサービスの重要度、その他のコンテキスト（実行されたファンクション、システム／データへのアクセスなど）、目的に適合	目的に適合	必要な製品の重要度、その他のコンテキスト（運用環境、データ、ユーザなど）、目的に適合
要件の定義又は策定	該当する C-SCRM 管理策又は要件の識別	該当する C-SCRM 管理策又は要件の識別	該当する C-SCRM 管理策又は要件の識別
市場分析の実行	初期リスクアセスメント（デューデリジェンスの質問票など）	初期リスクアセスメント（デューデリジェンスの質問票など）	製品オプション及びリスク要因の調査
入札公募／調達実行	C-SCRM 要件が満たされていることの確認、リスクアセスメントの完了	C-SCRM 要件が満たされていることの確認、リスクアセスメントの完了	展開前のリスクアセスメント
運用及び保守	継続的なリスク監視	継続的なリスク監視	継続的なリスク監視

プロセス活動に加えて、システムの最終用途又はシステムコンポーネントを曖昧にする、ブラインド購入又はフィルタリングされた購入を使用する、不正開封防止パッケージを必須とする、信頼された又は管理された配布を使用するなど、多くの有用な取得セキュリティ強化ツール及び技術が利用可能である。サプライチェーンのサイバーセキュリティリスクアセスメントの結果は、状況に最も適した戦略、ツール、手法を導き、情報を提供することができる。ツール、技術、及びプラクティスは、システム開発ライフサイクル全体を通じて、不正な製造、盗難、改ざん、偽造品の挿入、

悪意のあるソフトウェア又はバックドアの挿入、及び不適切な開発プラクティスに対する保護を提供する場合がある。

サプライチェーン全体及び取得ライフサイクル全体にわたるサイバーセキュリティリスクを効果的かつ継続的な管理を確実にするために、契約上の合意及び契約管理に以下が含まれることが望ましい。

- 契約及びメカニズムに適用されるセキュリティ要件が、受注の資格条件として満たされていること。
- 該当する場合、品質アシュアランス監視計画又は同等のパフォーマンス監視の手法に関連した C-SCRM パフォーマンス目標を含む、管理策のフローダウン（二次請負業者への適用）要件。
- 継続的なコンプライアンスを確実にするための、サプライヤのセキュリティ要件順守の定期的な妥当性再確認。
- 事業中断が深刻であると判断された場合の受け入れ可能な逸脱と、中断が深刻であると見なされるかどうかを判断するためのベースライン基準を含む、脆弱性、インシデント、及びその他の事業中断に関する情報の伝達及び報告のためのプロセス及びプロトコル。
- リスクの曝露（エクスポージャー）の軽減、被害を最小化、及びタイムリーな是正処置又はインシデントからの復旧をサポートするための、識別されたサプライチェーンリスク又はリスクインシデントへの対応に関する、政府、サプライヤ、及びその他の該当する第三者機関の役割、責任、及び行動を扱う諸条件。

妥当性確認及び妥当性再確認手法には、必要な認証、現地の視察、第三者機関によるアセスメント、自己証明など、様々なものがある。必要な手法の種類と厳密さは、取得するサービス又は製品の重要度、及び対応するアシュアランス要件に見合ったものであることが望ましい。

C-SCRM の取得プロセスに統合するための追加ガイダンスは、附属書 C で提供されており、これは、[NIST SP 800-39] リスクマネジメントプロセスへの C-SCRM の拡張オーバーレイを示している。さらに、事業体は、そのドメイン（例えば、重要インフラ分野、州政府）に固有の取得及び調達のポリシー、規制、及びベストプラクティスを参照し、従うことが望ましい。

追加情報が、本出版物の附属書 *A*、及び *NIST SP 800-53, Rev. 5* の *SA-1*、*SA-2*、*SA-3*、*SA-4*、*SA-9*、*SA-19*、*SA-20*、*SA-22*、*SR-5*、*SR-6*、*SR-10*、及び *SR-11* に記載されている。

3.2. サプライチェーンの情報共有

事業体は、サプライチェーンに起因するリスクに絶え間なくさらされている。効果的な情報共有プロセスは、事業体がサプライチェーン全体のサイバーセキュリティリスクを理解し軽減するために重要な情報にアクセスできること、及びこれらのリスクから利益を得る可能性がある他者、又はこれらのリスクを認識する必要がある他者と関連情報を共有できることを確実にするのに役立つ。

サプライチェーン全体のサイバーセキュリティリスクの識別、アセスメント、監視、及び対応を支援するため、事業体は情報共有プロセス及び活動を C-SCRM プログラムに組み入れることが望ましい。これには、同業他社、ビジネスパートナー、及びサプライヤとの情報共有に関する合意の確立が含まれる場合がある。サプライチェーンリスク情報（SCRI：Supply Chain Risk Information）を共有コミュニティ内で交換することにより、事業体は、その共有コミュニティの集合知、経験、及びケイパビリティ（能力）を活用して、事業体が直面する可能性がある脅威をより完全に理解することができる。さらに、SCRI を共有することで、事業体は特定の産業分野や機関を標的とした攻撃キャンペーンをより的確に検知することができる。ただし、事業体は、情報共有分析センター（ISAC：Information Sharing and Analysis Center）などの正式な共有体制を通じて情報共有が行われることを確認することが望ましい。非公式又は管理されていない情報共有は、事業体を潜在的な法的リスクにさらす可能性がある。

連邦政府の事業体は、省庁間での情報共有を促進し、C-SCRM 情報共有活動の政府全体の中心的なファシリテータの役割を果たす FASC の情報共有機関と効果的に関わるためのプロセスを確立することが望ましい。

NIST SP 800-150 は、以下のような SCRI 共有関係の確立及び参加のための重要なプラクティスを説明している。

- ビジネスプロセス及びセキュリティポリシーをサポートする情報共有の目標及び目的を定める。
- SCRI の既存の内部情報源を識別する。
- 情報共有活動の範囲を規定する [27]。
- 情報共有ルールを確立する。
- 情報共有への取り組みに参加する。
- 追加のコンテキスト、修正、又は改善提案を提供することによって、積極的に指標の充実に取り組む。
- SCRI を公開、利用、分析し、SCRI に基づいて行動するために、セキュアで自動化されたワークフローを使用する。
- SCRI 共有に関する合意を積極的に確立する。
- 機密情報のセキュリティ及びプライバシーを保護する。
- 情報共有活動に対する継続的サポートを提供する。

[27] 情報共有活動の範囲には、サプライヤの最新のリスクアセスメントで承認されたデータ分類レベルと、そのサプライヤに対して承認されたデータの種類を含めることが望ましい。例えば、特定の分類レベル（例えば、ビジネス上の機密）でデータに対してアセスメントが実施されたが、新たな分類レベル（例えば、制限）のデータを含むように業務範囲を変更した場合、リスクアセスメントの情報を更新する必要がある。

以下の表 3-2 に示すように、SCRI は製品、サービス、又は供給源に関連するサプライチェーンのサイバーセキュリティ関連の特徴及びリスク要因を記述し、識別する。それは様々な形（例えば、生データ、サプライチェーンネットワークマップ、リスクアセスメント報告書）で存在する場合があり、情報の信頼度と信ぴょう性のアセスメントを容易にするメタデータが付属していることが望ましい。事業体は、特定の情報の共有又は報告が義務付けられているのか任意なのか、及びその時期、並びに情報の取り扱い、保護、及び分類に関して順守する必要がある要件があるのかどうか記述した、確立されたプロセス及び手順に従うことが望ましい。

表 3-2：製品、サービス、又は供給源に関連するサプライチェーンの
特徴及びサイバーセキュリティリスク要因 [28]

供給源、製品、又はサービスの特徴	リスク指標、分析、及び所見
• 特徴及び機能性 • システム特権を含む、データ及び情報へのアクセス • インストール環境又は運用環境 • 特定の製品又はサービス、及び関連するサプライチェーン、コンパイルチェーンのセキュリティ、真正性、及び完全性 • 期待どおりに製品又はサービスを生産及び提供する供給源の能力 • 供給源に対する外国の統制又は影響（例えば、外国資本、供給源及び外国企業体の間の個人的及び職業的関係、供給源が本社を置いている又は事業を行っている外国の法体制）[29] • 市場における代替供給源 • コンポーネントの来歴及びペディグリー • サプライチェーンの関係及び場所	• 脅威情報に指標（攻撃に関連するシステムの中間生成物又は観察可能なもの）、戦術、技術、及び手順（TTP：Tactics, Techniques and Procedures）が含まれている • セキュリティアラート又は脅威インテリジェンス報告書 • 国家安全保障、国土安全保障、国家重要インフラ、若しくは製品又はサービスの使用に関連するプロセスへの影響 • 連邦政府のシステム、プログラム、又は施設の脆弱性 • 脅威レベル及び脆弱性レベルのアセスメント／スコア • 製品、材料、又はサービスによって引き起こされる事業体の業務又はミッションに対する損失、損傷、侵害の潜在的なインパクト又は損害、及び潜在的なインパクトの起こりやすさ、損害、又はシステムの悪用可能性 • リスク軽減のためのキャパシティが識別されている
• 地政学的、法的、管理／内部統制、財務の安定性、サイバーインシデント、個人及び物理的セキュリティ、又は製品、サービス、又は供給源のセキュリティ、安全性、完全性、レジリエンス、信頼性、品質、統合的信頼性、又は真正性の分析の要因となるようなその他の情報など、潜在的なリスク要因	

[28] 製品、サービス、又は供給源に関連するサプライチェーンの特性及びサイバーセキュリティのリスク要因は、完全に網羅されていない。

[29] 米国通商代表部（USTR：United States Trade Representative）が毎年作成するスペシャル 301 条報告書（Special 301 Report）は、知的財産の扱いについての補足ガイダンスを提供している（https://ustr.gov/issue-areas/intellectual-property/special-301）。

3.3. C-SCRM トレーニング及び意識向上

事業体内の多数の個人が、C-SCRM の成功に貢献する。これには、情報セキュリティ、調達、リスクマネジメント、エンジニアリング、ソフトウェア開発、IT、法務、人事、及びプログラムマネージャが含まれる。これらのグループの貢献の例には、以下が含まれる。

- システム所有者は、情報システムの開発、調達、統合、変更、運用、保守、及び／又は最終廃棄に対する責任の一環として、運用レベルで C-SCRM の多面的な責任を負う。
- 人事管理は、個人が適切な C-SCRM プロセス及び手順でトレーニングされていることを確実にするのに役立つ身元調査とトレーニングポリシーを定義し、実装する。
- 法務は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの契約における調達に含まれる、C-SCRM 固有の契約文言の草案作成又はレビューを支援する。
- 取得／調達は、取得プロセスに組み込まれたサプライヤアシュアランスプラクティスを実装するプロセスを定義する。
- エンジニアリングは、製品を設計し、オープンソースコンポーネントの使用に関する既存の要件を理解しなければならない。
- ソフトウェア開発者は、コードのテスト及び修正を含め、ソフトウェアの弱点と脆弱性が可能な限り早い時点で識別され、対処されることを確実にする。
- 出荷及び受入は、重要なコンポーネントが入っている箱が、輸送中又は倉庫で不正開封されていないことを確実にする。
- プロジェクトマネージャは、プロジェクト計画が策定され、プロジェクトの計画及び実行の一環として C-SCRM の考慮事項が含まれていることを確実にする。

情報システムのエンドユーザを含む事業体内の全員が、サプライチェーン全体のサイバーセキュリティリスクを管理する役割を担っている。事業体は、C-SCRM を不可欠な部分として含むセキュリティ文化全体を醸成することが望ましい。事業体は、この文化を醸成するために様々なコミュニケーション手法を利用でき、従来の意識向上及び役割ベースのトレーニングは、そのコンポーネントの一つに過ぎない。

事業体のすべての個人は、事業体にとっての C-SCRM の重要性、各自の固有の役割及び責任、及びインシデントを報告するためのプロセス及び手順に関連するものを理解できるように、適切なトレーニングを受けることが望ましい。このトレーニングは、全体的なサイバーセキュリティ意識向上トレーニングに統合することができる。事業体は、レベル 1 内で広範囲のベースライントレーニング要件を定義することが望ましく、これらの要件はレベル 2 及びレベル 3 内の特定のコンテキストに基づいてテーラリング及び調整されることが望ましい。

サプライチェーン全体のサイバーセキュリティリスクの管理において、より重要な役割を持つ個人は、自分の責任範囲、自分が責任を負う特定のプロセス及び手順の実装、及びインシデント、中断、又はその他の C-SCRM 関連事象の発生時に取るべき行動を理解するのに役立つ、テーラリングされた C-SCRM トレーニングを受講することが望ましい。事業体は、C-SCRM の役割及び責任に対処するために、具体的な役割ベースのトレーニング基準を確立し、役割固有の C-SCRM トレーニングを開発することが望ましい。事業体はまた、いくつかの特定の役割のために、既存の役割ベースのトレーニングに C-SCRM のコンテンツを追加することを検討してもよい。詳細については、第 3.3 節の意識向上及びトレーニングの管理策を参照のこと。

事業体は、C-SCRM ワークフォースのトピックの共通語彙の形成手段として、NIST サイバーセキュリティ教育のための国家計画（NICE：National Initiative for Cybersecurity Education）フレームワーク[30]を利用することが推奨される。これは、事業体が役割固有の C-SCRM の責任に関連するトレーニングを開発し、サイバーセキュリティワークフォース関連のトピックを伝達するのに役立つ。NICE フレームワークは、カテゴリ、専門分野、職務役割、知識、スキル、及び能力（KSA：Knowledge, Skills, and Abilities）、及びサイバーセキュリティ業務を記述するタスクの概要を示している。

3.4. C-SCRM の重要なプラクティス[31]

サプライチェーンのサイバーセキュリティリスクマネジメントは、複数の分野における既存の標準化されたプラクティス、及び常に進化し続ける一連の C-SCRM ケイパビリティ（能力）に基づいて構築されている。C-SCRM の重要なプラクティスは、本出版物全体で説明されている C-SCRM プラクティスのサブセット特に強調し、これらに注意を向けることを意図している。事業体は、追加の C-SCRM ケイパビリティ（能力）に進む前に、これらの重要なプラクティスで基本レベルの成熟度を達成することを優先するのが望ましい。事業体は、これらのプラクティスの実装を、事業体固有のコンテキスト（例えば、利用可能なリソースとリスクプロファイルに基づく）に応じて、適用可能かつ適切なものにテーラリングすることが望ましい。C-SCRM の重要なプラクティスは、[NISTIR 8276] などの NIST 標準及びガイドライン、並びにその他の適用可能な国内及び国際標準に記載されている。C-SCRM プラクティスには、事業体全体での C-SCRM の統合、正式なプログラムの確立、重要な製品、サービス、及びサプライヤの把握と管理、事業体のサプライチェーンの理解、重要なサプライヤとの密接な協力、レジリエンス及び改善活動に重要なサプライヤを含めること、サプライヤ関係全体のアセスメント及び監視、及びライフサイクル全体の計画が含まれる。

3.4.1. 基本的プラクティス

システムインテグレータとの相互作用を成功させ、生産的に行うためには、基本的なプラクティスを導入することが重要である。サプライヤは、標準化されたプラクティスの導入に関して、様々なレベルである可能性がある。以下は、事業体がより高度な C-SCRM プラクティスを開発し実行する能力を向上するために段階的に実装することができる、推奨される分野横断的な基本的なプラクティスの具体例である。

- 中核となる専門的かつ分野横断的な C-SCRM プログラムマネジメントオフィス及び／又は C-SCRM チームを確立する。
- C-SCRM の確立及び／又は強化について、上級幹部のサポートを得る。
- 事業体全体のリスクアセスメントプロセス（NIST SP 800-30, Rev. 1「リスクアセスメントの実施の手引き（Guide for Conducting Risk Assessments）」[NIST SP 800-30 Rev. 1]に準拠）を含む、リスクマネジメント階層及びリスクマネジメントプロセス（NIST SP 800-39「情報セキュリティリスクの管理（Managing Information Security Risk）」[NIST SP 800-39]に準拠）を実装する。
- C-SCRM の要件を統合し、これらの要件を事業体のポリシーに組み込む事業体ガバナンス構造を確立する。

[30] NIST SP 800-181「サイバーセキュリティ教育のための国家計画（*NICE*）サイバーセキュリティワークフォースフレームワーク（*National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*）」を参照。
[31] 各省庁及び関係機関は、大統領令 14028 号、国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）に従ってこのガイダンスを実装するときに附属書 F を参照することが望ましい。

- 事業体のサプライヤ、製品、及びサービスの重要度を識別及び測定するプロセスを策定する。
- C-SCRM とは何か、なぜこれが非常に重要なのかについての認識を高め、理解を促進する。
- 取得／調達のポリシー及び手順（連邦政府に適用される連邦情報技術取得改革法（Federal Information Technology Acquisition Reform Act）[FITARA]のプロセスを含む）及び調達カードプロセスに、C-SCRM を策定し、及び／又はこれを統合する。スーパーバイザー及びマネージャは、職員が C-SCRM に関する能力を高めることを目指すことも確実にすることが望ましい。
- 連邦情報処理規格（FIPS：Federal Information Processing Standards）199 のインパクトレベルを判断するための、一貫性があり、適切に文書化され、反復可能なプロセスを確立する。
- [FIPS 199] のインパクトレベルが定義された後、サプライヤのリスクアセスメントプロセス（重要度分析、脅威分析、脆弱性分析を含む）を確立し、優先順位に基づいて使用を開始する。
- 品質アシュアランス及び品質管理のプロセスとプラクティスを含む品質及び信頼性プログラムを実装する。
- サプライチェーン、サイバーセキュリティ、製品セキュリティ、物理的セキュリティ及びその他の関連プロセス（例えば、法務、リスク管理者、人事、財務、エンタープライズ IT、プログラムマネジメント／システムエンジニアリング、情報セキュリティ、取得／調達、サプライチェーンロジスティクス）のための、明示的で協調的かつ専門分野固有の役割、説明責任、構造、及びプロセスを確立する。
- ポリシー、ガイダンス、及び管理策の適切な実装を確実にするために、情報セキュリティ及び C-SCRM に十分なリソースが割り振られることを確実にする。
- C-SCRM 関連の国家機密情報にアクセスし共有するために、C-SCRM の主要な役割及び責任を持つ、十分な許可を有する要員を確保する。
- NIST SP 800-53 Revision 5「組織と情報システムのためのセキュリティおよびプライバシー管理策（Security and Privacy Controls for Information Systems and Enterprises）」[NIST SP 800-53, Rev. 5]に記載されている、適切かつテーラリングされた一連のベースライン情報セキュリティ管理策を実装する。
- セキュリティ及び品質の要件を順守することを確実にするための、内部のチェック及び内部の均衡を確立する。
- 例えば、認定された相手先ブランド製造業者（OEM：Original Equipment Manufacturer）[32] 又はその認定代理店及び認定再販業者からの購入に関するガイドラインを含む、サプライヤマネジメントプログラムを確立する。
- セキュリティインシデントの識別、対応、及び軽減を成功させるための堅牢なインシデントマネジメントプログラムを実装する。このプログラムは、サプライチェーンのサイバーセキュリティに起因するものを含め、セキュリティインシデントの根本原因を識別できるものであることが望ましい。
- サプライヤ及びサービスプロバイダが自らの製品の脆弱性を積極的に識別し、開示していることの妥当性を確認するための内部プロセスを確立する。
- 事業体全体のリスクを管理するために、組み込みソフトウェアのコンポーネントを管理及び監視するガバナンスケイパビリティ（能力）を確立する（例えば、重要度、脆弱性、脅威、及び悪用可能性と組み合わせた SBOM）。

[32] 本出版物の目的上、相手先ブランド製造業者（*Original Equipment Manufacturer*）という用語には、部品の本来の製造業者（*Original Component Manufacturer*）が含まれる。

3.4.2. 持続的プラクティス

持続的プラクティスは、サプライチェーンのサイバーセキュリティリスクマネジメントの有効性を高めるために使用されることが望ましい。これらのプラクティスは、基本的なプラクティスを含み、基本的なプラクティスに基づいている。基本的なプラクティスを幅広く標準化し、実装した事業体は、サプライチェーンのサイバーセキュリティリスクマネジメントのケイパビリティ（能力）を高めるための次のステップとして、以下を考慮することが望ましい。

- 脅威情報に基づくセキュリティプログラムを確立し、協働する。
- 重要なサプライヤのセキュリティケイパビリティ（能力）及びプラクティスをアセスメントするために、第三者機関によるアセスメント調査、現地の視察、正式な認証（例えば、ISO 27001）などの信頼構築メカニズムを使用する。
- リスクプロファイルに対する潜在的な変更のために、サプライヤ、サプライヤの製品及びサービス、並びにサプライチェーン自体の継続的な監視及び再アセスメントのための正式なプロセス及び間隔を確立する。
- 事業体全体の代理権を持つ責任者に、事業体のミッションの必須事項と戦略的目標及び目的に合致した C-SCRM の決定を行う権限を与えるために、リスク選好度及びリスク許容度を定義するための C-SCRM リスクプロファイル（又はミッション及びビジネス領域に固有のリスクプロファイル）についての事業体の理解を利用する。
- 事業体のサプライチェーンサイバーセキュリティ脅威及びリスクに対する知見を高め、一連の広範な政府機関、民間部門、又は国家安全保障に影響する可能性があるサプライチェーン全体のサイバーセキュリティリスクに対して調整された総合的なアプローチを確実にするのに役立てるため、ISAC、FASC、及びその他の政府機関と関わる形式化された情報共有機能を利用する。
- 事業体のサイバーセキュリティプログラム責任者と調整して、C-SCRM リスクプロファイルの上位のリスクを最上位の事業体リスク委員会に上げる。
- 情報セキュリティ、調達、リスクマネジメント、エンジニアリング、ソフトウェア開発、IT、法務、人事を含む、C-SCRM に関わる事業体のプロセス全体にわたって、該当する役割のトレーニングカリキュラムに、C-SCRM 固有のトレーニングを組み込む。
- C-SCRM の考慮事項をシステム及び製品ライフサイクルのあらゆる側面に統合し、システムエンジニアリング、サイバーセキュリティプラクティス、及び取得のための、一貫性があり、適切に文書化された、反復可能なプロセスを実装する。
- 事業体が定めた C-SCRM 要件を、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの合意の契約文言に統合する。
- 緊急時対応計画、インシデント対応、及び災害時復旧計画及びテストに、重要なサプライヤを含める。
- サイバーセキュリティプラクティスを改善するため、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと関わり合う。
- リスクを認識している責任者を確保し、C-SCRM 実装の完全性を能動的な管理を可能にし、事業体の C-SCRM プロセス及びプラクティスの有効性を高めるために、C-SCRM 測定基準を定義し、収集し、報告する。

3.4.3. 強化的プラクティス

強化的プラクティスは、適応的及び予測的な C-SCRM ケイパビリティ（能力）に向けて前進することを目標に持つ事業体が適用することが望ましい。事業体は、持続的なプラクティスが事業体全体で幅広く実装され、標準化された後で、強化的プラクティスを進めることが望ましい。

- 実行の一貫性と効率性を促進し、他の重要な C-SCRM 活動に必要な重要リソースを利用可能にするために、適用可能で実用的な場合は、C-SCRM プロセスを自動化する。
- サプライチェーン全体のサイバーセキュリティリスクの起こりやすさ及びインパクトに関する不確実性を低減し、リスク対応へのリソースの割り振りを最適化し、投資利益（すなわち、対応の有効性）を測定するために、確率論的アプローチ（例えば、ベイズ分析）を応用する定量的リスク分析を採用する。
- 事後対応型から、リスクプロファイルの変更が発生する前にこの変更に対応するという予測型 C-SCRM 戦略及び計画に移行するために、主要な C-SCRM 測定基準（すなわち、将来的な指標）から得られる知見を適用する。
- C-SCRM プラクティスの強化及び改善のために、必要に応じて実践コミュニティ（例えば、センターオブエクセレンス）を設立する、または参加する。

本出版物に含まれるガイダンス及び管理策は、既存の多くの専門分野にわたるプラクティスに基づいて構築されており、システム、製品、及びサービスのライフサイクル全体を通じて、サプライチェーン全体のサイバーセキュリティリスクを戦略的に管理するための事業体の能力を高めることを意図している。C-SCRM の重要なプラクティスの要約については、表 3-3 を参照。

3.5. ケイパビリティ（能力）実装の測定及び C-SCRM 測定指標

事業体は、C-SCRM プログラムの効率性と有効性を、プログラム自体の継続的な測定を通じて、積極的に管理することが望ましい。事業体は、様々な方法を使用して自己の C-SCRM プログラムの有効性を測定し、管理することができる。

- NIST CSF などのフレームワークを使用して C-SCRM ケイパビリティ（能力）をアセスメントする。
- C-SCRM イニシアチブの完了に向けた進展を測定する。
- 期待される成果に向けた C-SCRM イニシアチブのパフォーマンスを測定する。

すべての方法は、様々なデータ収集、分析、コンテキスト化、及び報告活動に依存している。まとめると、これらの方法は、最終的にリスク曝露（エクスポージャー）の低減、及び事業体のセキュリティ成果の改善を示す進展及び結果を追跡し、報告するために使用されることが望ましい。

C-SCRM パフォーマンス管理は、事業体及び財務面に、複数のメリットをもたらす。主なメリットとしては、C-SCRM のパフォーマンスに対するステークホルダーの説明責任の強化、C-SCRM 活動の有効性の向上、法律、規則、及び規制への順守の証明、リソース割り振りの決定のための定量化可能なインプットの提供、サイバーサプライチェーンインシデントのインパクトの低減又はサプライチェーンインシデントを経験する確率の低下に関連するコスト回避が含まれる。

事業体は、C-SCRM ケイパビリティ（能力）のベースラインを設定するために、NIST CSF のインプリメンテーションティアなどのフレームワークを使用できる。これは、事業体が C-SCRM プラクティスの厳しさと高度化を追跡及び評価するための有用なコンテキストを提供する。フレームワークのトピックに対する進捗は、ティアにおけるケイパビリティの進捗を示す順序（すなわち、1～5）尺度を使用して測定される。以下に、NIST CSF のティアを適用することで C-SCRM ケイパビリティ（能力）を測定する方法の例を示す。

- CSF ティア 1：事業体は、サプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）、又はより大きなエコシステムにおける自らの役割を理解していない。事業体は、サプライチェーン全体のサイバーセキュリティリスクを識別、アセスメント、低減するために、他のエンティティと協力したり、そのためのプロセスを整備したりしていない。
- CSF ティア 2：事業体は、サプライチェーン全体のサイバーセキュリティリスク及びより大きなエコシステムにおける自らの役割を理解している。事業体は、サプライチェーン全体のサイバーセキュリティリスクを管理するケイパビリティ（能力）、又はより大きなエコシステムでエンティティと関わり、情報共有するケイパビリティ（能力）を内部で正式化していない。
- CSF ティア 3：サプライチェーン全体のサイバーセキュリティリスクを管理するための事業体全体のアプローチが、事業体のリスクマネジメントポリシー、プロセス、及び手順によって実施されている。これには、サプライチェーン全体のサイバーセキュリティリスクとその他の事業体リスクの管理のバランスを取るガバナンス構造（例えば、リスク審議会）が含まれている可能性が高い。ポリシー、プロセス、及び手順が、意図したとおりに一貫して実装され、継続的に監視及びレビューされている。担当者は、任命されたサプライチェーンのサイバーセキュリティリスクマネジメントの責任を果たすための知識とスキルを有している。事業体は、ベースライン要件をサプライヤ及びパートナーに伝達するための正式な合意を得ている。事業体は、外部の依存関係を理解し、事象に応じて事業体内でリスクベースのマネジメントに関する決定を行うことができるようにするために、パートナーと協力して情報を共有している。
- CSF ティア 4：事業体は、事象が発生する前にサイバーセキュリティ及びサプライチェーンセキュリティを改善するために、パートナーとの間で積極的に情報を利用及び配布し、リアルタイム又はほぼリアルタイムの情報を利用している。事業体は、外部サプライヤ及びパートナー、内部の関連する機能領域、及び事業体の全レベルにおいて、サプライチェーンのサイバーセキュリティリスクマネジメントに関する制度化された知識を活用している。事業体は、サプライヤ、バイヤー、及び他のパートナーとの強力な関係を築き、維持するために、公式な（例えば、合意）及び非公式なメカニズムを使用して、積極的にコミュニケーションを図っている。

ケイパビリティ（能力）の構築は、戦略及び計画の実現、ポリシー及びガイダンスの確立、トレーニングへの投資、プログラムリソースの投入を含む、強固な計画的基盤を確立することから始まる。この基盤となるケイパビリティ（能力）が導入されると、事業体は、プログラムの様々な領域における C-SCRM ケイパビリティ（能力）の目標とする状態へ向けたプログラムの戦略的方向性を定めるために、事業体はこれらの進捗チャートを使用することができる。表 3-3 は、C-SCRM 実装モデルの例を示している。

表 3-3：C-SCRM プラクティス実装モデルの例 [33]

実装レベル	関連する C-SCRM プラクティス
基本的	• C-SCRM PMO の確立 • C-SCRM に対する責任者のサポートの獲得 • 事業体レベルにわたる C-SCRM ポリシー • C-SCRM の階層の定義 • C-SCRM のガバナンス構造 • 適切に文書化された、一貫性のある C-SCRM プロセス • C-SCRM を意識した文化の確立 • 品質及び信頼性プログラム • 取得／調達ポリシーへの C-SCRM の統合 • FIPS 199 インパクトレベルの決定 • C-SCRM に関する明示的な役割 • 適切かつ専用の C-SCRM リソース • C-SCRM 管理策ベースラインの定義 • コンプライアンス確保のための C-SCRM の内部抑制と均衡 • サプライヤマネジメントプログラム • 確立されたインシデントマネジメントプログラムへの C-SCRM の包含 • サプライヤが脆弱性を開示することを確実にするためのプロセス
持続的	• 脅威情報に基づくセキュリティプログラム • 第三者によるアセスメント、現地の視察、及び正式認定の使用 • 正式なサプライヤ監視プログラム • 定義された C-SCRM リスク選好度及びリスク許容度 • 正式化された情報共有プロセス（例えば、FASC との関わり） • 管理職／リスク委員会への C-SCRM リスクの定期的な報告 • 正式な C-SCRM トレーニングプログラム • C-SCRM の SDLC への統合 • C-SCRM の契約上の合意への統合 • サプライヤのインシデント対応、災害時復旧、及び緊急時対応計画への参加 • サイバーセキュリティプラクティス改善のためのサプライヤとの協力 • C-SCRM 測定基準の正式な定義、収集、及び報告
強化的	• C-SCRM プロセスの自動化 • 定量的リスク分析の使用 • 予測的及び適応的な C-SCRM 戦略及びプロセス • 実践コミュニティの設立又は参加

[33] C-SCRM のケイパビリティ（能力）の詳細については、第 3.4 節の「C-SCRM の重要なプラクティス」を参照。

3.5.1. パフォーマンス測定指標による C-SCRM の測定

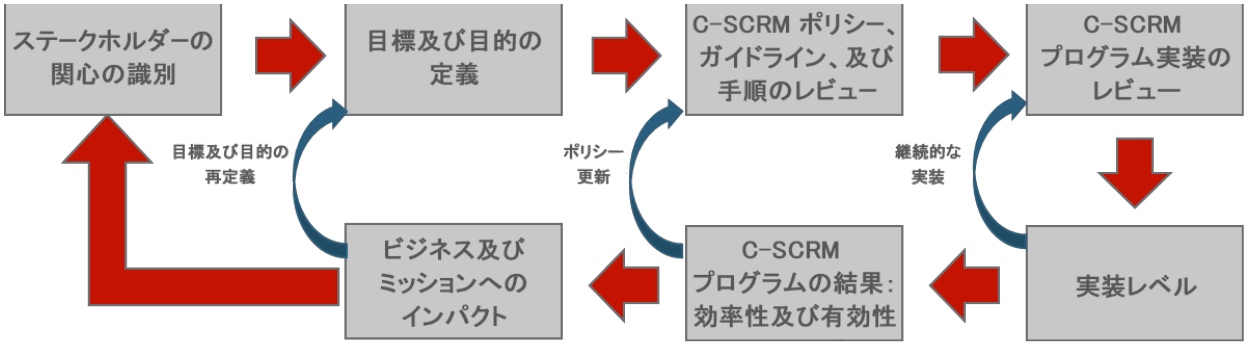

図 3-1：C-SCRM 測定基準策定プロセス

事業体は通常、意思決定を容易にし、情報セキュリティプログラムにおけるパフォーマンス及び説明責任を改善するために、情報セキュリティ測定指標に依存している。事業体は自らの C-SCRM プログラム内で同様のメリットを得ることができる。さらに事業体は、 ERM プロセスを通じて C-SCRM 測定基準を取締役会に報告することが望ましい。図 3-1 は、以下を含む、[NIST SP 800-55, Rev. 1] で概説されている測定基準の策定プロセスを示している。

- **ステークホルダーの関心の識別：**C-SCRM の第一次ステークホルダー（例えば、CISO、CIO、CTO）及び第二次ステークホルダー（例えば、CEO／政府機関の長、COO、CFO）を識別し、各ステークホルダー又はステークホルダーグループに必要なコンテキストに基づいて要件を定義／測定する。
- **目標及び目的の定義：**事業体の戦略的及び C-SCRM 固有のパフォーマンス目標及び目的を識別し、文書化する。これらの目標は、事業体の戦略的計画、C-SCRM ポリシー、要件、法律、規制などの形で表明される可能性がある。
- **C-SCRM ポリシー、ガイドライン、及び手順のレビュー：**これらの文書で概説され、事業体全体で C-SCRM を導き／実装するために使用される、望ましい C-SCRM プラクティス、管理策、及び期待事項を識別する。
- **C-SCRM プログラム実装のレビュー：**新たな測定指標を導き出すために使用される知見を提供できる既存のデータ、測定指標、及び証拠をすべて収集する。これらは、C-SCRM 計画、POA&M（plan of action & milestones：行動計画とマイルストーン）、サプライヤアセスメントなどに含まれる場合がある。
- **実装レベル：**プログラム実装の進捗状況を示すために、識別された C-SCRM 標準、ポリシー、及び手順に対する測定指標を策定し、マッピングする。これらの測定指標は、C-SCRM ケイパビリティ（能力）の優先順位付け及び投資に関する決定を下す際に、考慮されることが望ましい。
- **効率性及び有効性に関する C-SCRM プログラムの結果：**望ましい C-SCRM の成果が達成されているかどうかを測定するために、C-SCRM の効率性及び有効性の測定指標を策定し、識別された戦略及びポリシーの目的にマッピングする。これらの測定指標は、ポリシーの更新の一部と見なされることが望ましい。
- **ビジネス及びミッションへのインパクト：**C-SCRM のインパクト（例えば、ビジネスプロセスのコスト削減への貢献、国家安全保障リスクの低減）に関する知見を提供するために、識別された事業体の戦略的目的及び C-SCRM 固有の目的に対する測定指標を策定し、マッピングする。これらの測定指標は、目標及び目的の更新の一要素と見なされることが望ましい。

情報セキュリティ測定指標と同様に、C-SCRM に焦点を当てた測定指標は、事業体の様々なレベルで達成することができる。表 3-4 は、3 つのリスクマネジメントレベルにおける測定指標トピックの例を示している。

表 3-4：リスクマネジメントレベルにおける測定指標トピックの例

リスクマネジメントレベル	測定指標トピックの例
レベル 1	• 下位レベルでのポリシー採用 • 下位レベルでのポリシー採用の適時性 • リスク選好度及び許容のステートメントの順守 • レベル 2 全体で差別化されたリスク曝露（エクスポージャー）のレベル • 規制上の義務の順守 • 顧客の要件への準拠
レベル 2	• 軽減戦略の有効性 • C-SCRM 活動全体の時間配分 • ミッション及びビジネスプロセスレベルのリスク曝露（エクスポージャー） • ミッション及びビジネスプロセスにおける C-SCRM 要件の採用の度合いと品質 • レベル 3 による C-SCRM PMO の使用
レベル 3	• 管理策の有効性の設計 • 管理策の運用の有効性 • 管理策の費用効率

事業体は、特定の測定指標を策定する取り組みを開始する前に、対象となるステークホルダーグループと共に、識別された C-SCRM の目標及び目的の妥当性確認をすることが望ましい。事業体は、C-SCRM 測定指標を策定する際に、ステークホルダーの最優先事項に焦点を当て、現実的に提供され、収集することができるデータに基づいた測定指標を目標とすることが望ましい。確立された各測定指標には、その測定指標に関連する目標及び目的が達成されているかどうかを評価するために使用される特定のパフォーマンス目標があることが望ましい。事業体は、各測定指標を形式化し、その測定指標に関連するあらゆる情報の参照元として機能する測定指標テンプレートの使用を考慮することが望ましい。最後に、事業体は、測定指標が継続的に期待される知見が継続的に提供し、C-SCRM に関する事業体の全体的な戦略目的に合致していることを確実にするために、ステークホルダーとの正式なフィードバックループを策定することが望ましい。

3.6. 専用リソース

サプライチェーン全体のサイバーセキュリティリスクを適切に管理するために、事業体はこの取り組みに資金を割り当てることが望ましい。リソースのニーズを識別し、適切で経常的、かつ専用の資金を確保するための措置を講じることは、C-SCRM 戦略及び実装の計画の取り組みに組み込まれ、事業体の予算編成、投資レビュー、及び資金管理プロセスに組み込まれる必要がある、不可欠かつ重要な活動である。適切なリソースを利用できることは、C-SCRM プログラムのケイパビリティ（能力）の確立及び維持のための重要で主要な成功要因である。実現可能な場合、事業体は、C-SCRM 態勢を改善するために既存の資金源を活用するよう推奨されることが望ましい。専用資金が継続的に利用可能できることで、事業体はそのケイパビリティ（能力）を長期にわたって持続、拡大、成熟させることができるようになる。

C-SCRM 資金の確保及び割り当ては、C-SCRM の重要性、国家安全保証及び経済安全保障との関連性、並びにミッション及びビジネスプロセスと資産の保護、継続性、及びレジリエンスを確実にすることへの責任者のコミットメントの典型である。

資金調達はり、目標及び行動指向の計画を促進する。リソースのニーズを調査し、資金を割り振ることで、予算編成及び戦略的計画プロセスが促進される。効果的な事業体は、まず戦略的ロードマップを作成するための一連の目標及び目的を定義し、有限なリソースの割り当て及び割り振りを通じてそれらを達成する道筋を定める。C-SCRM の目的に関係する専用資金を確立することで、パフォーマンスの説明責任を果たすための条件が設定され、担当の職員は、効率的かつ効果的であり、C-SCRM のケイパビリティ（能力）を向上させ、セキュリティ強化の成果を達成することを継続的に探求するという考え方を採用することを余儀なくされる。

多くの場合、リソースはが乏しく、多くの競合する目的で必要であるため、新たな資金調達又は資金の増額が課題となることがある。資金には限りがあるため、優先順位付けが余儀なくされる。C-SCRM の責任者は、まず既存のリソースの制約条件内で何が達成できるかを検討し、追加リソースに対する自らの要求を明確にし、優先順位を付け、主張できるようにする必要がある。新たな投資の提案の場合、事業体のミッション及びビジネス目的に照らして計画された取り組みを調整することが必要になる。適切に実行されると、体系的な計画プロセスは、C-SCRM プロセスとこれらの目標との調和を強化することができる。

多くの C-SCRM プロセスは、既存のプログラム及び事業活動に組み込むことが可能かつ望ましく、利用可能な資金を使用して適切に実行できる可能性がある。ただし、最初の C-SCRM プログラムケイパビリティ（能力）を確立するために、1 回限りのリソースの投入が必要となる可能性がある。これには例えば、C-SCRM の専門知識を持つ新規職員の採用、C-SCRM プログラムガイダンス策定を支援する請負業者のサポートの取り付け、又は役割ベースの C-SCRM トレーニングのコンテンツ開発の必要性が含まれる可能性がある。また、繰り返し発生する C-SCRM プログラムのニーズをすべて満たすためのリソースが不足する可能性もある。既存の資金を C-SCRM への取り組みに再配分したり、新たな資金又は追加資金を要求したりすることが必要になる可能性がある。事業体はまた、現実的な場合には常に、共有サービスを活用する機会を模索することが望ましい。

共有サービスを使用することで、少ないリソースの利用を最適化し、サービス、システム、又はツールへの費用効率の高いアクセスを提供するセンターオブエクセレンスにケイパビリティ（能力）を集中させることができる。事業体は、C-SCRM のリソース及びケイパビリティ（能力）への費用効率の高いアクセスを可能にする、下位レベルのエンティティ全体での費用分担メカニズムを採用することができる。C-SCRM の共有サービスモデルを追及する事業体は、このようなモデルの課題も認識しておくことが望ましい。共有サービス（例えば、C-SCRM PMO）は、事業体全体が、かなり同質的な一連の C-SCRM 戦略、ポリシー、及びプロセスに依存している場合に最も効果的である。多くの場合、C-SCRM サービスを一元的に提供するには、堅牢な技術インフラが必要である。共有サービスモデルのメリットを十分に得るためには、事業体のシステムがプロセスの自動化と集中型の配信をサポートできることが望ましい。

短期的及び将来的にどのような選択肢が利用可能及び実行可能となる可能性があるかを理解するには、予算／財務責任者との協議が重要である。これらの責任者は、ニーズを正当化する最善の方法、新たな資金要求の時間枠及びプロセスに関しても助言することができる。経常的な資金の確保と 1 回限りの資金調達の要求では、従うべきプロセスが異なる可能性が高い。例えば、C-SCRM のケイパビリティ（能力）をサポートする新たな情報システムの資金調達には、事業体の投資審査委員会の承認を得るために提示する正式な投資対効果検討書の作成が必要となる可能性がある。リソースニーズを継続的な費用と 1 回限りの費用に分けること、又は予算編成、リソースに関する意思決定、及び利用可能な資金の割り振りと管理に合わせた費用カテゴリに分類することが、組織にとって有益である場合がある。

C-SCRM PMO は、経常的リソースと非経常的リソースの両方の要件を把握し、それらの要件を利用可能な資金調達源及び資金源にマッピングした複数年にわたる C-SCRM プログラムの予算を策定し維持するために、ミッション及びビジネスプロセス及び予算責任者と連携することに主な責任を持つことが推奨される。事業体は、必要な調達資金額、時期、及び目的を理解するために、C-SCRM プログラムのケイパビリティ（能力）を実装し、必要な C-SCRM プロセスを継続的に実行するために必要なリソース（人又は物）の種類とレベルを識別し、アセスメントすることが望ましい。これらの識別された各リソースニーズに関連する費用は、人件費、契約、トレーニング、出張、ツール、システムなどの関連する費用カテゴリの項目を含む予算に取り込まれ、累積され、反映される。これにより、事業体は、既存のリソースレベル内で何を達成できるのか、及びどこに埋める必要があるギャップがあるのかについてのベースラインを理解できるようになる。実際の資金の割り振りは、単一の C-SCRM 予算に一元化される場合もあれば、事業体全体に分散され、個々の部門又はミッション及びビジネスプロセス領域の予算に反映される場合もある。資金が実際にどのように割り当てられるかに関わらず、C-SCRM の予算と資金の状況を一元的に把握することは、新たな要求を正当化し、優先順位に関する決定について通知し、特定の活動及びその活動を達成できる期間についての期待を調整する有用な情報源となる。

C-SCRM プログラムの資金調達が、その資金調達に関連したパフォーマンス測定指標によって、事業体の予算内で明確に表現されることを確実にすると、結果に対する説明責任を果たすことが推進される。予算要求、パフォーマンス計画、及び報告書内で専用の資金を目に見える形にすることで、責任者は C-SCRM プロセスと目的の達成に注意を向けざるを得なくなる。予算は定期的に要求され、正当化されなければならない。このプロセスによって、責任者と監督責任者は、割り振られたリソースの有効性と効率性を追跡し、測定できる。これはさらに、プログラム及び業務の C-SCRM 担当者がパフォーマンスを追跡し、管理するための推進的な機能を果たす。

重要ポイント [34]

取得における C-SCRM。取得活動への C-SCRM の統合は、C-SCRM プログラムの成功にとって極めて重要である。C-SCRM の要件は、取得ライフサイクル全体にわたって組み込まれることが望ましい。C-SCRM 活動には、サービス、サプライヤ、及び製品のリスクアセスメントの実施、関連する C-SCRM 管理策の識別、デューデリジェンスの実施、及びサプライヤの継続的監視が含まれる。

サプライチェーンの情報共有。事業体は、情報共有プロセス及び活動を C-SCRM プログラムに取り入れることで、サプライチェーン全体のサイバーセキュリティリスクを理解し軽減するために重要な情報にアクセスできるようになる。サプライチェーン全体のサイバーセキュリティリスクに関する知見を得て、コミュニティ全体の経験から学ぶために、事業体は、同業他社、業務提携先、サプライヤ、及び情報共有コミュニティ（例えば、ISAC）と関わることが望ましい。

C-SCRM 意識向上及びトレーニング。事業体は、サプライチェーン全体のサイバーセキュリティリスクが事業に与える可能性がある潜在的なインパクトと、リスク軽減のためのベストプラクティスの採用方法をユーザに教育するために、事業体全体及び役割ベースのトレーニングプログラムを採用することが望ましい。厳格な C-SCRM トレーニングは、事業体が C-SCRM を意識した文化に移行する際の主要な成功要因である。

C-SCRM の重要なプラクティス。本出版物では、事業体が採用し、独自のコンテキストに合わせてテーラリングすることが望ましい C-SCRM の基本的、持続的、及び強化的プラクティスについて概説している。事業体は、高度な C-SCRM ケイパビリティ（能力）に焦点を当てる前に、重要なプラクティスの基準レベルの成熟度を達成することを優先するのが望ましい。

ケイパビリティ（能力）実装測定及び C-SCRM 測定指標。事業体は、C-SCRM プログラムの効率性と有効性を積極的に管理することが望ましい。まず、事業体は、C-SCRM の目的に向けた進捗を測定する基準として C-SCRM フレームワークを採用することが望ましい。次に、事業体は、具体的な運営面の目的という視点から事業体の進捗を定期的に一見することができる定量的パフォーマンス測定指標及び目標許容度を作成し、実装することが望ましい。

専用リソース。可能であり、かつ該当する場合、事業体は C-SCRM に専用の資金を投入することが望ましい。そうすることのメリットには、戦略的で目標指向の計画の促進、事業体の C-SCRM プラクティスの実行と成熟に対する内部ステークホルダーの説明責任の促進、及び事業体の責任者による進捗の継続的監視が含まれる。

[34] 重要ポイントでは、その節の本文から重要な点を説明している。定義については、附属書 H の用語集を参照。

参考文献

[CISA SCRM WG3] Cybersecurity and Infrastructure Agency – Working Group 3 (2021) *Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists* (Arlington, Virginia). Available at https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders- Lists_508.pdf

[COSO 2011] Rittenberg L, Martens F (2012) *Enterprise Risk Management: Understanding and Communicating Risk Appetite.* (Committee of Sponsoring Organizations of the Treadway Commission), Thought Leadership in ERM. Available at https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk- Appetite.pdf

[COSO 2020] Martens F, Rittenberg L (2020) *Risk Appetite – Critical to Success: Using Risk Appetite To Thrive in a Changing World*. (Committee of Sponsoring Organization of the Treadway Commission), Thought Leadership in ERM. Available at https://www.coso.org/Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf

[Defense Industrial Base Assessment: Counterfeit Electronics] Bureau of Industry and Security, Office of Technology Evaluation (2010) *Defense Industrial Base Assessment: Counterfeit Electronics*. (U.S. Department of Commerce, Washington, D.C.). Available at https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense- industrial-base-assessment-of-counterfeit-electronics-2010/file

[FedRAMP] General Services Administration (2022) *FedRAMP*. Available at http://www.fedramp.gov/

[GAO] Government Accountability Office (2020) *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*. (U.S. Government Accountability Office, Washington D.C.), Report to Congressional Requesters GAO-21-171. Available at https://www.gao.gov/assets/gao-21-171.pdf

[CNSSI 4009] Committee on National Security Systems (2015) *Committee on National Security Systems (CNSS) Glossary* (CNSS, Ft. Meade, Md.), CNSSI 4009-2015. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[EO 14028] Executive Order 14028 (2021) Improving the Nation's Cybersecurity. (The White House, Washington, DC), DCPD-202100401, May 12, 2021. https://www.govinfo.gov/app/details/DCPD-202100401

[FASCA] Federal Acquisition Supply Chain Security Act of 2018 (FASCA), T*itle II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act of 2018*, Pub. L. 115-390, 132 Stat. 5173. Available at https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[FSP] Cyber Risk Institute (2020) *Financial Services Cybersecurity Framework Profile Version 1.0.* Available at https://cyberriskinstitute.org/the-profile/

[ISO 9000] International Organization for Standardization (2015) *ISO 9000:2015 — Quality management — Fundamentals and vocabulary* (ISO, Geneva). Available at https://www.iso.org/standard/45481.html

[ISO 28001] International Organization for Standardization (2007) *ISO 28001:2007 — Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance* (ISO, Geneva). Available at https://www.iso.org/standard/45654.html.

[ISO Guide 73] International Organization for Standardization (2009) *ISO Guide 73:2009 — Risk management — Vocabulary* (ISO, Geneva). Available at https://www.iso.org/standard/44651.html

[ISO/IEC 2382] International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 2382:2015 — Information technology — Vocabulary* (ISO, Geneva). Available at https://www.iso.org/standard/63598.html

[ISO/IEC 20243] International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 20243-1:2018 – Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products Part 1: Requirements and recommendations* (ISO, Geneva). Available at https://www.iso.org/standard/74399.html

[ISO/IEC 27000] International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary* (ISO, Geneva). Available at https://www.iso.org/standard/73906.html

[ISO/IEC 27002] International Organization for Standardization/International Electrotechnical Commission (2022) *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls* (ISO, Geneva). Available at https://www.iso.org/standard/75652.html

[ISO/IEC 27036] International Organization for Standardization/International Electrotechnical Commission (2014) *ISO/IEC 27036-2:2014 – Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements* (ISO, Geneva). Available at https://www.iso.org/standard/59680.html

[ISO/IEC/IEEE 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2015) *ISO/IEC/IEEE 15288:2015 — Systems and software engineering — System life cycle processes* (ISO, Geneva). Available at https://www.iso.org/standard/63711.html

[ITIL Service Strategy] Cannon D (2011) *ITIL Service Strategy* (The Stationary Office, London),
2nd Ed.

[NDIA] National Defense Industrial Association System Assurance Committee (2008) *Engineering for System Assurance*. (NDIA, Arlington, VA). Available at https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems- engineering/sse-committee/systems-assurance-guidebook.ashx.

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NIST SCRM Proceedings 2012] National Institute of Standards and Technology (2012) *Summary of the Workshop on Information and Communication Technologies Supply Chain Risk Management*. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=913338

[NIST SP 800-16] deZafra DE, Pitcher SI, Tressler JD, Ippolito JB (1998) Information Technology Security Training Requirements: a Role- and Performance-Based Model. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-16. https://doi.org/10.6028/NIST.SP.800-16

[NIST SP 800-30 Rev. 1] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[NIST SP 800-32] Kuhn DR, Hu VC, Polk WT, Chang S-jH (2001) Introduction to Public Key Technology and the Federal PKI Infrastructure. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-32. https://doi.org/10.6028/NIST.SP.800-32

[NIST SP 800-34 Rev. 1] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[NIST SP 800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[NIST SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[NIST SP 800-53 Rev. 5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5.Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[NIST SP 800-53A Rev. 5] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5.https://doi.org/10.6028/NIST.SP.800-53Ar5

[NIST SP 800-53B] Joint Task Force (2020) Control Baselines for Information Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020.https://doi.org/10.6028/NIST.SP.800-53B

[NIST SP 800-55 Rev. 1] Chew E, Swanson MA, Stine KM, Bartol N, Brown A, Robinson W (2008) Performance Measurement Guide for Information Security.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-55, Rev. 1.https://doi.org/10.6028/NIST.SP.800-55r1

[NIST SP 800-64] Kissel R, Stine KM, Scholl MA, Rossman H, Fahlsing J, Gulick, J (2008) Security Considerations in the System Development Life Cycle.(National Institute of Standards and Technology, Gaithersburg, MD), (Withdrawn) NIST Special Publication (SP) 800-64 Rev. 2.https://doi.org/10.6028/NIST.SP.800-64r2

[NIST SP 800-100] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007.https://doi.org/10.6028/NIST.SP.800-100

[NIST SP 800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[NIST SP 800-160 Vol. 1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[NIST SP 800-160 Vol. 2] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[NIST SP 800-171 Rev. 2] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2, Includes updates as of January 28, 2021. https://doi.org/10.6028/NIST.SP.800-171r2

[NIST SP 800-172] Ross RS, Pillitteri VY, Guissanie G, Wagner R, Graubart R, Bodeau D (2021) Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-172. https://doi.org/10.6028/NIST.SP.800-172

[NIST SP 800-181 Rev. 1] Petersen R, Santos D, Wetzel KA, Smith MC, Witte GA (2017) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[NIST SSDF] National Institute of Standards and Technology (2022) *NIST Secure Software Development Framework*. Available at https://csrc.nist.gov/projects/ssdf

[NISTIR 7622] Boyens JM, Paulsen C, Bartol N, Shankles S, Moorthy R (2012) Notional Supply Chain Risk Management Practices for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7622. https://doi.org/10.6028/NIST.IR.7622

[NISTIR 8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179

[NISTIR 8276] Boyens J, Paulsen C, Bartol N, Winkler K, Gimbi J (2021) Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8276. https://doi.org/10.6028/NIST.IR.8276

[NISTIR 8286] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[NTIA SBOM] *The Minimum Elements For a Software Bill of Materials (SBOM)*, NTIA and Department of Commerce, 2021 https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[OMB A-123] Office of Management and Budget (2004) Management's Responsibility for Internal Control. (The White House, Washington, DC), OMB Circular A-123, December 21, 2004. Available at https://georgewbush-whitehouse.archives.gov/omb/circulars/a123/a123_rev.html

[OMB A-130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[SAFECode 1] Software Assurance Forum for Excellence in Code (2010) *Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain*. Available at http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf

[SAFECode 2] Software Assurance Forum for Excellence in Code (2009) *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain*. Available at http://www.safecode.org/publication/SAFECode_Supply_Chain0709.pdf

[SwA] Polydys ML, Wisseman S (2008) *Software Assurance in Acquisition: Mitigating Risks to the Enterprise. A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing.* (National Defense University Press, Washington, D.C.) Information Resources Management College Occasional Paper. Available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf

附属書 A：C-SCRM セキュリティ管理策 [35]

C-SCRM 管理策の概要

NIST はセキュリティ管理策を以下のように定義している。

> システムとその情報の機密性、完全性、可用性を保護するために、情報システムに対し規定された管理的、運用的、技術的管理策 (すなわち、保護手段又は対抗策)。 [FIPS 199]

[NIST SP 800-53, Rev. 5]は、情報セキュリティ管理策のカタログで多数のサプライチェーンのサイバーセキュリティ関連の管理策を定義している。この節は、[NIST SP 800-53, Rev. 5]の拡張オーバーレイとして構成されている。C-SCRM 関連の管理策を識別し、追加の補足ガイダンスによってこれらの管理策を強化し、必要に応じて新規管理策を提供する。C-SCRM 管理策は、[NIST SP 800-53, Rev. 5]の 20 の管理策ファミリーにまとめられている。このアプローチによって、C-SCRM 管理策の実装をアセスメントする際に、[NIST SP 800-53A, Rev. 5]で説明しているセキュリティ管理策アセスメント技法の使用が容易になる。

本出版物に記載されている管理策は、事業体が内部で実装すること、また、該当する場合及び契約上の合意書で明記されている場合には、請負業者及び二次請負業者に求めることを意図したものである。[NIST SP 800-53, Rev. 5]と同様に、セキュリティ管理策及び拡張管理策は、事業体のニーズに基づいて管理策／拡張管理策を削除、追加、又は特殊化するための出発点である。この節の各管理策は、C-SCRM に適用可能であるため、ここに記載されている。[NIST SP 800-53, Rev. 5]の管理策のうち、ここに記載されていない管理策は、C-SCRM に直接適用可能であると見なされないため、本出版物には含まれていない。本出版物の各種 C-SCRM 管理策の詳細及び補足ガイダンスは第 4.5 節に収録されている。

C-SCRM 管理策の概要

第 2 節で説明するリスクマネジメントプロセスの対応ステップでは、事業体はサプライチェーン全体のサイバーセキュリティリスクを軽減するための管理策を選択、テーラリング、及び実装する。[NIST 800-53B]は、[FIPS 199]の高・中・低の影響度の一連の情報セキュリティ管理策を記載している。この節では、これらの管理策によって情報システム及びコンポーネント、並びにサプライチェーンインフラストラクチャに対するリスクを軽減するのにどのように役立つかについて説明する。この節には、関連する管理策及び補足ガイドラインを含む 20 の C-SCRM 管理策ファミリーを示している。

図 A-1 は、[NIST SP 800-53, Rev. 5]の C-SCRM 関連管理策を識別、改良し、C-SCRM 補足ガイダンスを追加するために使用されたプロセスを示しており、以下のステップを表している。

1. C-SCRM に適用可能な個々の管理策及び拡張管理策を[NIST SP 800-53, Rev. 5]から選択して抽出する。
2. C-SCRM にどのように適用されるかを判断するために、これらの管理策を分析する。

[35] 各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

3. C-SCRM に関するすべての懸念が対処されたかどうかを判断するために、結果として得られた一連の管理策及び拡張管理策を評価する。
4. [NIST SP 800-53, Rev. 5]に現在定義されていない、追加の管理策を策定する。
5. 関連する二次請負業者にフローダウンする管理策を識別する。
6. 各 C-SCRM 管理策に適用可能なレベルを設定する。
7. 各 C-SCRM 管理策に C-SCRM 固有の補足ガイダンスを策定する。

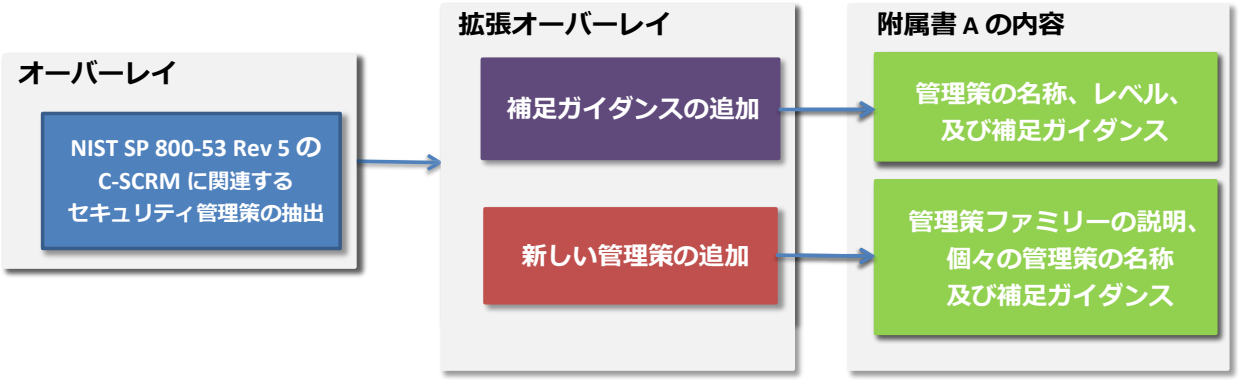

図 A-1：NIST SP 800-161, Rev. 1 の C-SCRM セキュリティ管理策

なお、[NIST SP 800-53, Rev. 5]は C-SCRM 関連の管理策及び管理策ファミリーを提供している。本出版物には、これらの管理策を、概要又は追加ガイダンス、及び元の[NIST SP 800-53, Rev. 5]の管理策への参照及び補足ガイダンスの詳細とともに記載している場合がある。

事業体全体での *C-SCRM* 管理策

表 A-1 に示すように、本出版物の C-SCRM 管理策には、事業体を構成する 3つのレベルが指定されている。これは、附属書 C のリスクマネジメントプロセスの対応プロセスで説明するように、事業体、その様々なミッション、及び個々のシステムに固有の C-SCRM 管理策の選択を容易にすることを目的としている。管理策の選択時に事業体は、本節の C-SCRM 管理策を使用して、リスクアセスメントに基づいてテーラリングするために適切な C-SCRM 管理策を識別することが望ましい。事業体は、レベルごとに適用可能な C-SCRM 管理策を選択し、実装することで、C-SCRM に適切に対処していることを確実にすることになる。

製品及びサービスを取得するための C-SCRM 管理策の適用

取得者は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダなど、取得者に製品及びサービスを提供する様々な種類の事業体に対して C-SCRM 要件を伝達する際の基準として、C-SCRM 管理策を使用してもよい。取得者は、「NIST SP 800-161, Rev. 1 の管理策に従っていることを確実にする」のような汎用的な要件ステートメントを使用するのを避けるべきである。取得者は、取得するサービス又は製品の具体的なユースケースに関連する管理策を選択する際には、十分に注意しなければならない。取得者は、その取得活動全体で C-SCRM を統合することが推奨される。取得における C-SCRM の役割の詳細は、本出版物の第 3.1 節に記載する。

この節に記載されている管理策は具体的な契約文言を提供していないことを認識することが重要である。取得者は、特定の C-SCRM 要件を含めて各自の契約文言を策定するために、本出版物をガイダンスとして使用することが望ましい。以降の節では、取得者に対する C-SCRM の期待事項に関して、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの役割について詳しく説明する。

事業体は、これらの管理策が導入されているかどうかを確認するために、事業体の要件の測定及び準拠についてのサプライヤの自己アセスメント、取得者のレビュー、又は第三者アセスメントなど、複数の技法を使用してもよい。事業体は、ニーズを満たしているかどうかを確認するために、確立された第三者アセスメントに最初に注目することが望ましい。事業体は、C-SCRM 要件を定義するときに、確立された第三者アセスメントが、特定の要件すべてに対応していない可能性があることに気付くことがある。このような場合には、対応の要件を正当化するために追加の証拠が必要となることがある。この目的で取得されるデータは適切に保護されるべきであることに注意されたい。

サプライヤ

サプライヤは取得者に対して、市販製品（COTS）ソリューションを提供するか、又は連邦政府の環境では政府調達向け既製品（GOTS）ソリューションを提供する可能性がある。COTS ソリューションには、商用ライセンス許諾ソリューション／製品などの非開発品目（NID）が含まれる。GOTS ソリューションは政府機関専用のライセンス可能ソリューションである。サプライヤは、規模は小規模から大規模まで、専門的な企業から多角的な企業まで、単一の国に拠点を置く企業から多国籍企業まで、多様な集団である。サプライヤはまた、その洗練度、リソース、及びプロセスとソリューションの透明性／可視性の点でも多種多様である。

サプライヤが導入している C-SCRM のレベルとタイプは様々である。これらのプラクティス及びその他の関連するプラクティスにより、SCRM 評価に必要な証拠を提供することができる。活用することができる連邦政府のリソースの例として、信頼できるサプライヤを対象とした国防総省マイクロエレクトロニクスアクティビティ（DMEA）認定がある。適切な場合は、C-SCRM 実装の証拠となる可能性がある既存のデータ及び文書を再利用する機会をサプライヤに与える。

事業体は、サプライヤに課されるサプライチェーンのサイバーセキュリティ要件の程度、サプライヤの製品の開発又は製造過程を可視化することに対するサプライヤの意欲又は能力、及びサプライヤが自らのソリューションにセキュリティ及びサプライチェーンのプラクティスをどのように適用するかが、サプライヤとの取引を行うコストに直接影響する可能性があるかどうかを検討することが望ましい。事業体又はシステムインテグレータがより高いレベルの透明性をサプライヤに要求する場合は、このような要件によって生じる可能性があるコストへの影響を考慮しなければならない。サプライヤは、増大するコスト又は自らの知的財産に対する認識されたリスクを回避するために、調達に参加しないことを選択できるが、これにより事業体の供給又は技術の選択肢が制限される。さらにサプライヤは、顧客から複数の様々なサプライチェーンサイバーセキュリティ要件群が課され、これらに顧客ごとに準拠しなければならないことから生じるリスクに直面する可能性がある。サプライヤに要求する透明性の度合いは、内在するリスクに対処するのに十分な、サプライヤの重要度に見合ったものであることが望ましい。

開発者及び製造業者

開発者及び製造業者とは、システム、システムコンポーネント（ソフトウェアなど）、又はシス

テムサービス（アプリケーションプログラミングインタフェース[API]など）を開発又は製造する人員である。開発は、事業体内部又は外部エンティティを介して行われる可能性がある。開発者は通常、特権アクセス権限を維持し、SDLC 全体にわたって必要不可欠な役割を果たす。開発者及び製造業者が行う活動と製造する成果物は、セキュリティ強化又は新たな脆弱性の導入につながる可能性がある。したがって、開発者が C-SCRM 要件及び管理策の対象となり、かつこれらを熟知していることが不可欠である。

システムインテグレータ

システムインテグレータは、カスタム開発、テスト、運用、メンテナンスなどのカスタマイズされたサービスを取得者に提供する。このグループは通常、取得者からの提案依頼に対し、取得者の要件に合わせてカスタマイズされたソリューション又はサービスで回答する。システムインテグレータからのこのような提案には、何層ものサプライヤ、及び他のベンダ又は二次請負業者とのチーム編成の取り決めなどが含まれ得る。システムインテグレータは、取得者の C-SCRM 要件に基づいてこのようなビジネスエンティティの精査及び検証が行われることを確実にすることが望ましい。システムインテグレータとの関係において得られる視覚化レベルのために、取得者は厳格なサプライヤ受け入れ基準と、識別されたリスク又は潜在的なリスクに対処するためのあらゆる関連対策を要求する裁量権を有する。

情報システムサービスの外部システムサービスプロバイダ

事業体は、ミッション及びビジネスファンクションの一部を実行又はサポートするために外部システムサービスプロバイダを使用する[NIST SP 800-53, Rev. 5]。システム及びサービスを外部委託することで、外部委託されたファンクションを取得者が把握及び制御する能力が低下するという、サプライチェーンのサイバーセキュリティに関する一連の懸念が生じる。したがって、C-SCRM 要件を定義し、調達合意書にそれらを記載し、提供されるサービスを監視し、サービスが定められている要件に準拠しているかどうかを評価する上で、さらなる厳格さが事業体に求められる。誰がサービスを実行するかに関係なく、これらのサービスを使用することで発生する事業体のシステム及びデータに対するリスクの責任及び説明責任は、最終的には取得者が負う。事業体はこのリスクに対処し、ミッション及びビジネスプロセスオーナー又はリスク管理者と協力してこのリスクを受容するために、一連の代替 C-SCRM 管理策を実装することが望ましい。契約、省庁間合意、事業協定、ライセンス合意、及び/又はサプライチェーン取引などの手段を通じて C-SCRM 要件を伝達し、その後、検証及び監視するために、様々な手法を使用することができる。

その他の ICT/OT 関連のサービスプロバイダ

サービスプロバイダは、コンサルティングから、ウェブサイトコンテンツの公開、清掃サービスまで、幅広い様々な機能を履行することができる。その他の ICT/OT 関連のサービスプロバイダには、サービスを提供する手段として ICT/OT への物理的又は論理的アクセスを必要とするか、又は技術を使用する必要があるプロバイダ（ドローンを使用して動画／写真を撮影する空中写真撮影家や、クラウドベースの動画監視機能を使用して施設をリモートで監視するセキュリティ企業など）が含まれる。サービスプロバイダによるアクセス又は利用の結果、サプライチェーンのサイバーセキュリティリスクが事業体にもたらされる可能性が高まる。

制御・運用技術は、効果的に保護するためには特殊なスキルやケイパビリティ（能力）を適用する必要があるという運用上及びセキュリティ上の独自の特性を有している。エンタープライズアーキテクチャ全体に重要な OT コンポーネントが含まれる事業体はしばしば、このようなデバイス、システム、又は機器のセキュアな実装とメンテナンスを専門サービスプロバイダに依頼することがある。ICT 又は OT システムへの認可されたアクセスを含んでいる可能性があるサービスを提供する事業体又は個人はすべて、事業体の C-SCRM 要件に準拠することが望ましい。事業体は、ミッション上重要な資産及び／又は安全性に関連する資産を管理する ICT/OT 関連のサービスプロバイダに対し、特別な精査を適用することが望ましい。

C-SCRM セキュリティ管理策の選択、テーラリング、及び実装

事業体全体の C-SCRM を提供する費用効果の高いリスクベースのアプローチを確実にするために、本節で定義する C-SCRM 管理策は、[NIST SP 800-53, Rev. 5]に記載されているガイダンスを使用して、個々の事業体のニーズと環境に基づいて選択及びテーラリングされることが望ましい。本出版物で定義される C-SCRM ベースラインは、広範囲かつ多様な一連の構成要素の基本的なニーズに対処する。事業体は、（i）事業体の情報システムを取得及び運用する環境、（ii）事業体が実施する業務の性質、（iii）事業体、ミッション及びビジネスプロセス、サプライチェーン、及び情報システムが直面する脅威の種類、及び（iv）情報システム及びサプライチェーンインフラストラクチャにより処理、保存、又は伝送される情報の種類に基づいて、セキュリティ管理策を選択、テーラリング、及び実装しなければならない。

取得者は最初の一連のセキュリティ管理策を選択した後で、選択した管理策を事業体内の特定の条件に合わせて適切に変更し、より緊密に一致させるために、NIST SP 800-53B の「組織と情報システムのための管理策ベースライン（*Control Baselines for Information Systems and Organization*）」に従ってテーラリングプロセスを開始することが望ましい。C-SCRM 管理策の実装前に、事業体内の該当する担当者（認可権限のある担当者、認可権限のある担当者による指定代理人、リスク管理者［機能］、最高情報責任者、又は情報セキュリティ責任者など）がテーラリングを調整及び承認することが望ましい。さらに事業体には、個々の情報システムレベルで特定のプログラムをサポートするために事業体レベルでテーラリングプロセスを（必要なテーラリングされたベースラインとして、又はポリシー、プログラム、あるいはシステム固有のテーラリングの出発点として）実行するか、又は事業体レベル、プログラム／ミッションレベル、及びシステム固有のアプローチの組み合わせを使用して実行することができる柔軟性がある。

決定の根拠を含む、選択とテーラリングに関する決定は、レベル 1、2、3 及び附属書 C の C-SCRM 文書に含め、事業体の適切な担当者が C-SCRM 計画承認プロセスの一環として承認することが望ましい。

C-SCRM 管理策の形式

表 A-1 は、既存の[NIST SP 800-53, Rev. 5]の管理策又は拡張管理策に関する補足 C-SCRM ガイダンスを提供する管理策に対して本出版物で使用されている形式を示している。

[NIST SP 800-53, Rev. 5]に親管理策がない C-SCRM 管理策は通常、[NIST SP 800-53, Rev. 5]で説明している形式に従い、該当するレベルが追加される。新しい管理策には、[NIST SP 800-53, Rev. 5]と整合性があり、既存の管理策識別子と重複しない識別子が割り当てられる。

表 A-1：C-SCRM 管理策の形式

管理策識別子　管理策名 補足 C-SCRM ガイダンス： レベル： 関連管理策： 拡張管理策： **(1)** 管理策名 | 拡張管理策名 補足 C-SCRM ガイダンス： レベル： 関連管理策：

C-SCRM 管理策 AC-3 及び SCRM 拡張管理策 AC-3(8) を使用した C-SCRM 管理策の形式の例を以下に示す。

AC-3　アクセス実施

補足 C-SCRM ガイダンス：情報システム及びサプライチェーンに適切なアクセス実施メカニズムが導入されていることを確実にする。これには、サプライチェーンのニーズに対応するために連携して動作する可能性がある物理アクセス実施メカニズム及び論理アクセス実施メカニズムの両方が含まれる。事業体は、アクセス実施の詳細な定義を確実にすることが望ましい。

レベル：2、3

関連管理策： AC-4

拡張管理策：

(8) アクセス実施 | アクセス認可の取り消し

(1) 補足 C-SCRM ガイダンス：アクセスが不要となったか、若しくはアクセス権限を悪用又はアクセス権限に違反したサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが事業体のシステムにアクセスできないことを確実にするために、迅速な取り消しが重要である。例えば、「バッジフリッピング」という状況では、あるシステムインテグレータ事業体から別のシステムインテグレータ事業体に契約が移転するが、その契約をサポートする担当者は変わらない。このような場合、事業体は既存のアカウントを無効にし、古いクレデンシャルを廃止し、新たなアカウントを設定し、全く新しいクレ

デンシャルを発行することが望ましい。

レベル：2、3

本出版物における C-SCRM 管理策の使用

第 4 節の残りの部分では、NIST SP 800-53, Rev. 5 の 拡張 C-SCRM オーバーレイを提供する。この節では、NIST SP 800-53, Rev. 5 の管理策と C-SCRM 管理策の関係を以下のいずれかの方法で示す。

- [NIST SP 800-53, Rev. 5]の管理策又は拡張管理策が、C-SCRM の基本管理策として機能する情報セキュリティ管理策であるが C-SCRM 固有ではないと判断された場合、本出版物には含まれていない。
- [NIST SP 800-53, Rev. 5]の管理策又は拡張管理策が C-SCRM に関連すると判断された場合、管理策が適用されるレベルも記載される。
- [NIST SP 800-53, Rev. 5]の拡張管理策が C-SCRM に関連すると判断されたが親管理策はそのように判断されなかった場合、親管理策の番号と名称が含まれるが、補足 C-SCRM ガイダンスはない。
- 関連する[NIST SP 800-53, Rev. 5]の管理策／拡張管理策がない C-SCRM 管理策／拡張管理策は、その名称及び管理策／拡張管理策の本文とともに記載されている。
- すべての C-SCRM 管理策には、その管理策が適用されるレベルと、該当する場合には補足 C-SCRM ガイダンスが含まれる。
- 拡張管理策が C-SCRM 管理策を実装するメカニズムを提供する場合、拡張管理策は補足 C-SCRM ガイダンスに記載されるが、個別には収録されていない。
- 以前の[NIST SP 800-161]の管理策の撤回又は再編成が[NIST SP 800-53, Rev. 5]で既に反映されている場合、これは含まれない。

以下の新しい管理策及び拡張管理策が追加された。

- C-SCRM 管理策 MA-8 – メンテナンス監視及び情報共有が「メンテナンス」管理策ファミリーに追加された。
- C-SCRM 管理策 SR-13 – サプライヤのインベントリが「サプライチェーンのリスクマネジメント」管理策ファミリーに追加された。

C-SCRM セキュリティ管理策

ファミリー：アクセス制御

[FIPS 200]は、アクセス制御の最小限のセキュリティ要件を以下のように規定している。

> 組織は、権限を付与されたユーザや権限を付与されたユーザのために代行するプロセスの情報システムへのアクセスを制限するとともに、デバイス（他の情報システムを含む）や権限を付与されたユーザに実行が許可されるトランザクション（処理）と機能の種類についても制限しなければならない。

サプライチェーンを通過するシステム及びコンポーネントには、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダを含む様々な個人及び事業体がアクセスする可能性がある。このようなアクセスが原因で意図せずに情報の不正な公開、改ざん、又は破壊が発生しないことを確実にするために、このようなアクセスを定義及び管理することが望ましい。このアクセスは、認可されている事業体（及びこれらの事業体内の認可されている個人）に必要なアクセスの種類、期間、及びレベルのみに制限し、サプライチェーンのサイバーセキュリティへの影響がないか確認するために監視すべきである。

AC-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、アクセス制御ポリシーを定めているサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダのアクセス制御ポリシーを規定し、合意（契約文言など）に含めることが望ましい。これらのポリシーには、サプライチェーン及び情報システムへの物理的アクセス及び論理アクセスの両方が含まれていることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：1、2、3

AC-2 アカウント管理

補足 C-SCRM ガイダンス：この管理策を使用すると、サプライチェーンにおける活動及び行為者のトレーサビリティ（追跡可能性）を確立するのに役立つ。この管理策は、サプライチェーンにおける行為者へのアクセス認可が継続的に適切であることを確実にするためにも役立つ。事業体は適切な実装を確実にするために、一連の役割を定義し、認可レベルを関連付けることを選択してもよい。事業体は、請負業者の担当者のアカウントが契約履行期間を超えないことを確実にしなければならない。特権アカウントは、適切に調査された請負業者の担当者に対してのみ設定することが望ましい。事業体はまた、継続又は緊急事象においてミッション上重要なシステム又はミッションイネーブリングシステムへのアクセスが必要な請負業者の担当者のために、一時的又は緊急アカウントを確立及び管理するためのプロセスを導入していることが望ましい。例えば、パン

デミック事象において、病気のために勤務できない既存の請負業者担当者の業務を、新規請負業者スタッフが一時的に担当する必要が生じる場合がある。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

AC-3 アクセス実施

補足 C-SCRM ガイダンス：情報システム及びサプライチェーンに適切なアクセス実施メカニズムが導入されていることを確実にする。これには、サプライチェーンのニーズに対応するために連携して動作する可能性がある物理アクセス実施メカニズム及び論理アクセス実施メカニズムの両方が含まれる。事業体は、アクセス制御違反に対処するために定義済みの結果フレームワークが導入されていることを確実にすることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) アクセス実施 | アクセス認可の取り消し

補足 C-SCRM ガイダンス：アクセスが不要となったか、若しくはアクセス権限を悪用又はアクセス権限に違反したサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが事業体のシステムにアクセスできないことを確実にするために、迅速な取り消しが必要不可欠である。事業体は、請負業者及び二次請負業者がアクセスクレデンシャル（トークン、PIV 又は CAC カードなど）を事業体に即時に返却する要件を合意に含めることが望ましい。事業体はまた、アクセス認可の取り消しを速やかに処理するためのプロセスを導入しなければならない。例えば、「バッジフリッピング」という状況では、あるシステムインテグレータ事業体から別のシステムインテグレータ事業体に契約が移転するが、その契約をサポートする担当者は変わらない。このような場合、事業体は既存のアカウントを無効にし、古いクレデンシャルを廃止し、新たなアカウントを設定し、全く新しいクレデンシャルを発行することが望ましい。

レベル：2、3

(2) アクセス実施 | 管理されたリリース

補足 C-SCRM ガイダンス：事業体と第三者間でのリリースのためにサプライチェーンに関する情報を管理することが望ましい。事業体とそのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの間で情報が交換される可能性がある。事業体の情報の管理されたリリースにより、開示に関連するリスクから保護することができる。

レベル：2、3

AC-4 情報フローの実施

補足 C-SCRM ガイダンス：サプライチェーン情報は、大規模なサプライチェーンを通過

し、様々な連邦政府ステークホルダー、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダなど、幅広いステークホルダーに到達する可能性がある。要件と情報フローの実施方法を規定することで、必要な情報のみがサプライチェーンの様々な参加者に伝達されることが確実になる。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) 情報フローの実施 | メタデータ

補足 C-SCRM ガイダンス：C-SCRM に関連するメタデータは幅広く、SDLC 内の活動が含まれる。例えば、システム及びシステムコンポーネント、取得の詳細、及び納入に関する情報はメタデータとして扱われ、適切な保護を必要とする可能性がある。事業体は、サプライチェーンセキュリティに直接関連するメタデータを識別し、該当するメタデータを保護するために情報フローの実施が実装されていることを確実にすることが望ましい。

レベル：2、3

(2) 情報フローの実施 | ドメイン認証

補足 C-SCRM ガイダンス：C-SCRM のコンテキストでは、事業体はサプライチェーンに関する情報及びサプライチェーンを通過する情報の様々な発信元ポイント及び宛先ポイントを規定することが望ましい。これにより、事業体はサプライチェーン内の情報フローを把握することができる。

レベル：2、3

(3) 情報フローの実施 | メタデータの検証

補足 C-SCRM ガイダンス：C-SCRM では、データの妥当性確認及びそのメタデータとの関係が重要である。サプライチェーンで伝送されるデータの多くは、関連するメタデータを検証することで妥当性確認が行われる。サプライチェーンへのペイロードを許可する前に、妥当性確認のために適切なフィルタリングと検査が導入されていることを確実にする。

レベル：2、3

(4) 情報フローの実施 | 情報フローの物理的又は論理的分離

補足 C-SCRM ガイダンス：事業体は、情報システム及びサプライチェーン情報[36]フローの分離を確実にすることが望ましい。暗号化手法（デジタル署名など）などの様々なメカニズムを実装することができる。事業体とそのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダ間の情報フローの扱いは、特に公共ネットワークを活用する場合には難しいことがある。

レベル：3

AC-5 職務の分離

補足 C-SCRM ガイダンス：事業体は、情報システム及びサプライチェーンコンポーネントの両方の取得を必要とする決定について、適切な職務の分離が確立されていることを確実にすることが望ましい。職務の分離は、開発者に対して、開発者が作成したコードを開発環境から本番環境へプロモートする権限を拒否するなど、事業体のサプライチェーンに入るコンポーネントに対して適切な保護が導入されることを確実にするのに役立つ。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

[36] サプライチェーンサイバーセキュリティリスク情報は、連邦調達サプライチェーンセキュリティ法（FASCA）でのこの用語の定義に基づき、本出版物の用語集で定義されている。

AC-6　最小特権

補足 C-SCRM ガイダンス：C-SCRM 補足ガイダンスについては、拡張管理策を参照。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

拡張管理策：

(5) 最小特権 | 非組織ユーザによる特権アクセス

補足 C-SCRM ガイダンス：事業体は、事業体のサプライチェーン及び関連するサプライチェーン情報への特権アクセスを事業体外部のユーザが所有できないようにするための保護策が導入されていることを確実にすることが望ましい。事業体ユーザに、独立したコンサルタント、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが含まれている場合、関連するアクセス要件では、アクセス可能な情報及び／又はコンポーネント、期間、頻度、使用するアクセス手法、及びアクセスすることができるユーザについて、最小特権メカニズムを使用して正確に定義する必要がある可能性がある。重要なコンポーネントと重要でないコンポーネントを理解しておくと、事業体外部のユーザの最小特権アクセスに関して定義する必要がある可能性がある詳細レベルを理解するのに役立つ場合がある。

レベル：2、3

AC-17　リモートアクセス

補足 C-SCRM ガイダンス：サプライチェーンへのリモートアクセスの頻度はますます増加している。目的が情報システムの開発、メンテナンス、運用のいずれであっても、事業体はセキュアなリモートアクセスメカニズムを実装し、調査済みの担当者のみにリモートアクセスを許可することが望ましい。事業体のサプライチェーン（分散ソフトウェア開発環境を含む）へのリモートアクセスは、事業体又は請負業者の担当者のみに限定し、かつ、これらの担当者が各自のタスクを実行するために必要な場合のみに限定することが望ましい。セキュアな VPN を使用する、多要素認証を採用する、規定した営業時間内又は規定した場所からのみにアクセスを制限するなどのリモートアクセス要件を、合意において適切に定義しなければならない。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) リモートアクセス | メカニズムに関する情報の保護

補足 C-SCRM ガイダンス：事業体は、詳細な要件が適切に定義されていることを確実にし、また情報システム及びサプライチェーンに関する情報へのアクセスが不正利用及び開示から保護されていることを確実にすることが望ましい。サプライチェーンデータ及びメタデータの開示又はアクセスは、事業体のミッションプロセスに重大な影響を与える可能性があることから、サプライチェーン及び担当者の両方のプロセスを調査するために適切な対策が実施され、適切な保護が実装されることを確実にしなければならない。このような情報へのリモートアクセスが要件に含まれていることを確実にする。

レベル：2、3

AC-18 ワイヤレスアクセス

補足 C-SCRM ガイダンス：事業体のサプライチェーンには、サプライチェーンのロジスティクスをサポートするワイヤレスインフラストラクチャ（無線自動識別デバイス［RFID］サポート、ソフトウェアコールホーム機能など）が含まれることがある。サプライチェーンシステム／コンポーネントは、事業体自体の環境内又はシステムインテグレータあるいはサプライヤからの納入時など、ある場所から別の場所へ移動するときに、サプライチェーンを通過する。適切でセキュアなアクセスメカニズムがサプライチェーン内に導入されていることを確実にすることで、情報システム及びコンポーネントと、出荷時に使用されるロジスティクス技術及びメタデータを保護することができる（追跡センサ内など）。事業体は、サプライチェーンに対する適切なワイヤレスアクセス制御メカニズムをポリシーで定義し、適切なメカニズムを実装することが望ましい。

レベル：1、2、3

AC-19 モバイルデバイスのアクセス制御

補足 C-SCRM ガイダンス：サプライチェーンでのモバイルデバイス（ラップトップ、タブレット、電子リーダー、スマートフォン、スマートウォッチなど）の使用が普及している。これらは、事業体の業務を直接サポートし、サプライチェーンロジスティクス、情報システムとしてのデータ、及び事業体又はシステムインテグレータのサプライチェーンを通過するコンポーネントを追跡するときに使用される。事業体のサプライチェーンコンポーネントを管理する際は、該当する場合にはアクセス制御メカニズムが明確に定義及び実装されていることを確実にする。このような実装の例には、サプライチェーンを通過するコンポーネントを追跡する RFID のリモート携帯型機器で使用するために実装されるアクセス制御メカニズムなどがある。アクセス制御メカニズムは、このデバイスに関連するすべてのデータ及びメタデータにも実装すべきである。

レベル：2、3

AC-20 外部システムの使用

補足 C-SCRM ガイダンス：事業体の外部情報システムには、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの情報システムが含まれる。直接的かつ継続的な監視が可能な取得者の内部事業体とは異なり、外部サプライヤ関係では、情報は必要に応じて共有される可能性があり、またこの情報は合意において明確化されていることが望ましい。このような外部情報システムからサプライチェーンへのアクセスを監視及び監査することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：1、2、3

拡張管理策：

(1) 外部システムの使用 | 認可された使用に限定

補足 C-SCRM ガイダンス：この拡張管理策は、サプライチェーンの曝露（エクスポージャー）を、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダのシステムに限定するのに役立つ。

レベル：2、3

(2) 外部システムの使用 | 組織が所有していないシステム ― 使用制限

補足 C-SCRM ガイダンス：事業体が所有するものではないデバイス（個人所有デバイスの持ち込み[BYOD]ポリシーなど）は、サプライチェーン全体のサイバーセキュリティリスクへの事業体の曝露（エクスポージャー）を増大させる。これには、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが使用するデバイスが含まれる。事業体は、事業体が所有していないデバイスの事業体外部の担当者による使用をレビューし、このようなデバイスの使用を許可するか、又はデバイスを提供するかに関してのリスクベースの意思決定を行うことが望ましい。事業体は、受容不可能なレベルのリスクをもたらす事業体外部の担当者にはデバイスを提供することが望ましい。

レベル：2、3

AC-21 情報共有

補足 C-SCRM ガイダンス：サプライチェーン内で情報を共有することは、サプライチェーン全体のサイバーセキュリティリスクを管理するのに役立つ可能性がある。この情報には、システム及びコンポーネントの脆弱性、脅威、重大度、又は納入情報が含まれる可能性がある。事業体のサプライチェーン内で認可された個人のみがこの情報にアクセスすることができることを確実にするために、この情報共有を慎重に管理することが望ましい。事業体は、一時的な要件、情報に関する要件、契約上の要件、セキュリティ要件、アクセス要件、システム要件、及びその他の要件に関して情報共有の境界を明確に定義することが望ましい。事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの情報共有など、サプライチェーン活動内での意図しない又は意図的な情報共有を監視及びレビューすることが望ましい。

レベル：1、2

AC-22 公的にアクセス可能なコンテンツ

補足 C-SCRM ガイダンス：C-SCRM のコンテキストでは、公的にアクセス可能なコンテンツには、情報依頼書、提案依頼書、又はシステム及びコンポーネントの納入に関する情報が含まれる。適切なコンテンツのみが、公的に利用することができるように単独でリリース又は他の情報とともにリリースされることを確実にするために、この情報をレビューすることが望ましい。

レベル：2、3

AC-23 データマイニングの保護

補足 C-SCRM ガイダンス：事業体は一次請負業者に対し、この管理策をインサイダー脅威活動の一部として実装し、この要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

AC-24 アクセス制御の決定

補足 C-SCRM ガイダンス：事業体は、サプライチェーンへの認可されたアクセスをサポートするために、アクセス制御の決定を割り当てることが望ましい。システムインテグレータ又は外部サービスプロバイダを使用する場合には、アクセス制御の決定の要件と要件の実装方法の間に整合性があることを確実にする。このためには、多くの場合は事業体及びシステムインテグレータの間又は事業体及び外部サービスプロバイダの間で確立される事前の関係の一部として、サービス内容合意書でこのような要件を定義する必要があることがある。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：1、2、3

ファミリー：意識向上及びトレーニング

[FIPS 200]では、意識向上及びトレーニングの最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）組織の情報システムの管理者及びユーザが、自らの活動に関連するセキュリティリスクと組織の情報システムのセキュリティに関して適用される法律、大統領令、指令、ポリシー、規格、指示、規制又は手順を認識していることを確実にし、（ii）組織の人員に対し、割り当てられた情報セキュリティ関連の職務及び責任を果たすための適切なトレーニングが実施されていることを確実にしなければならない。

本出版物では C-SCRM を含めるために[FIPS 200]の意識向上及びトレーニングの管理策を拡張する。人員に C-SCRM の懸念事項を認識させることは、C-SCRM 戦略成功にとって重要である。C-SCRM の意識向上及びトレーニングは、問題領域と、サプライチェーン全体のサイバーセキュリティリスクを軽減するのに役立つ可能性がある適切なプロセス及び管理策への理解を提供する。事業体は、情報セキュリティ、調達、事業体リスクマネジメント、エンジニアリング、ソフトウェア開発、IT、法務、人事、及びその他を含む、事業体内のすべてのレベルで個人に対して C-SCRM 意識向上及びトレーニングを提供することが望ましい。事業体はまた、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと協力して、事業体のサプライチェーンと相互作用する人員が、必要に応じて C-SCRM 意識向上及びトレーニングを受けていることを確実にすることが望ましい。

AT-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、サプライチェーンの責任を負う担当者を対象とした C-SCRM 及び役割ベースの特定のトレーニングを含む、トレーニングのポリシー及び手順の策定、文書化、及び配布を管理する特定の担当者を指名することが望ましい。事業体は、サプライチェーンのサイバーセキュリティリスクマネジメントのトレーニング及び意識向上をセキュリティトレーニング及び意識向上ポリシーに統合することが望ましい。C-SCRM トレーニングは、事業体及びその請負業者の両方を対象とすることが望ましい。このポリシーは、情報システム所有者、取得、サプライチェーンロジスティクス、システムエンジニアリング、プログラムマネジメント、IT、品質、及びインシデント対応など、サプライチェーンに関係する又は影響を及ぼす個人又は機能に対して、サプライチェーンのサイバーセキュリティに関する役割ベースのトレーニングが義務付けられることを確実にすべきである。

C-SCRM トレーニング手順は以下を扱うことが望ましい。

a. サプライチェーン及びシステム／要素のライフサイクル全体において、悪い結果をもたらす可能性がある役割を行う個人に対して機会及び手段を制限するための役割。
b. 事業体の担当者と、事業体に雇用されていないが SDLC 全体でサプライチェーンに関わる個人の間の相互作用に関する要件。
c. C-SCRM トレーニングへの、C-SCRM 活動から得たフィードバック及び教訓の組み入れ。

レベル：1、2

AT-2　リテラシートレーニング及び意識向上

補足 C-SCRM ガイダンス：C-SCRM 固有の補足ガイダンスは拡張管理策で提供される。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

拡張管理策：

(1) リテラシートレーニング及び意識向上 | 実践的な演習

補足 C-SCRM ガイダンス：事業体は、サプライチェーンのサイバーセキュリティ事象及びインシデントをシミュレートする実践的な演習をリテラシートレーニングで提供することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

(2) リテラシートレーニング及び意識向上 | インサイダー脅威

補足 C-SCRM ガイダンス：事業体は、サプライチェーン内でのインサイダー脅威の潜在的な兆候の認識及び報告に関するリテラシートレーニングを提供することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

(3) リテラシートレーニング及び意識向上 | ソーシャルエンジニアリング及びマイニング

補足 C-SCRM ガイダンス：事業体は、サプライチェーンに関連するソーシャルエンジニアリング及びソーシャルマイニングの潜在的な事例及び実際の事例の認識及び報告に関するリテラシートレーニングを提供することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

(4) リテラシートレーニング及び意識向上 | 疑わしい通信及び異常なシステム動作

補足 C-SCRM ガイダンス：事業体のサプライチェーンシステムにおける不審な通信又は異常な動作の認識に関するリテラシートレーニングを提供する。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

(5) リテラシートレーニング及び意識向上 | 持続的標的型攻撃（*APT* 攻撃）

補足 C-SCRM ガイダンス：事業体のサプライチェーンにおける持続的標的型攻撃（APT 攻撃）での不審な通信の認識に関するリテラシートレーニングを提供する。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

(6) リテラシートレーニング及び意識向上 | サイバー脅威環境

補足 C-SCRM ガイダンス：事業体のサプライチェーン環境に固有のサイバー脅威に関するリテラシートレーニングを提供する。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2

AT-3 役割ベースのトレーニング

補足 C-SCRM ガイダンス：取得プロセス全体でサプライチェーンリスクに対処することは、C-SCRM を効果的に実行するために不可欠である。取得要員である人員は、調達実施時に含める必要がある C-SCRM の要件、条項、及び評価要因と、各取得フェーズへの C-SCRM の組み込み方法に関するトレーニングを受ける必要がある。同様の拡張トレーニング要件を、脅威アセスメント実施の責任を負う人員に合わせてテーラリングすることが望ましい。脅威及び識別されたリスクに対応するには、対諜報活動の意識向上及び報告に関するトレーニングが必要である。事業体は、開発者がセキュアな開発プラクティスと脆弱性スキャンツールの使用に関するトレーニングを受けることを確実にすることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

拡張管理策：

(7) セキュリティトレーニング | 物理的セキュリティ管理策

補足 C-SCRM ガイダンス：C-SCRM は、製造、出荷、受領、施設への物理的アクセス、インベントリ管理、倉庫管理など、サプライチェーン内の多数の物理セキュリティメカニズム及び手順の影響を受ける。開発及び運用サポートを事業体に提供する事業体及びシステムインテグレータの人員は、このような物理的セキュリティメカニズムの扱い方と、関連するサプライチェーン全体のサイバーセキュリティリスクに関するトレーニングを受けることが望ましい。

レベル：2

(8) 役割ベースのトレーニング | 対諜報活動トレーニング

補足 C-SCRM ガイダンス：公共部門の事業体は、そのリソースがサプライチェーン内における外国の敵対者の存在を示す可能性がある一連のデータソースを収集、解釈し、これに基づいて対処することができるようにする専門の対諜報活動意識向上トレーニングを提供することが望ましい。対諜報活動トレーニングでは、最低でも、既知の危険な兆候、主要な情報共有コンセプト、及び報告の要件を扱うことが望ましい。

レベル：2

AT-4 トレーニングの記録

補足 C-SCRM ガイダンス：事業体は、C-SCRM 固有のトレーニングに関する文書、特に取得及び対諜報活動における主要人員に関連する文書を維持することが望ましい。

レベル：2

ファミリー：監査及び説明責任

[FIPS 200]では、監査及び説明責任に関する最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）非合法的、不正、又は不適切な情報システム活動を監視、分析、調査、及び報告することができるようにするために必要な範囲で、情報システム監査記録を作成、保護、及び維持し、（ii）個々の情報システムユーザに対して各自の活動の説明責任を負わせるために、ユーザの活動を一意的にそのユーザまで追跡することができることを確実にしなければならない。

C-SCRM の監査及び説明責任の管理策は、サプライチェーンのサイバーセキュリティインシデント又は侵害の発生時に役立つ情報を提供する。事業体は、適切な監査メカニズム（システムログ、侵入検知システム[IDS]ログ、ファイアウォールログ、紙媒体の報告書、フォーム、クリップボードチェックリスト、デジタル記録など）を使用して、情報システムの境界内でサプライチェーンのサイバーセキュリティ関連の事象を指定及び監査することを確実にすることが望ましい。また、これらの監査メカニズムは、事業体のポリシーによって定義されている適切な時間枠内で機能するように構成することが望ましい。事業体はシステムのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダに対しても同様の作業を行うことを推奨し、このような監視に関する要件を合意に含めることができる。ただし事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダのシステムを含む、事業体の境界外のシステムには、監査メカニズムを展開すべきではない。

AU-1 ポリシー及び手順

> 補足 C-SCRM ガイダンス：事業体は、サプライチェーン情報システム及びネットワークの監査を含めるための監査及び説明責任のポリシー及び手順の策定、文書化、配布を管理する特定の担当者を指名しなければならない。監査及び説明責任のポリシー及び手順では、追跡活動と、構成管理など他の様々なサプライチェーン活動に対するその可用性を適切に扱うことが望ましい。サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの活動は、取得者のサプライチェーン情報システム及びネットワーク内でこれらの機能が実行される場合を除き、このようなポリシーには含めないことが望ましい。監査及び説明責任のポリシー及び手順では、特定のサプライヤの品質と、事業体及び事業体のサプライチェーンにこれらのサプライヤがもたらすリスクを調査する手段として、サプライヤ監査が適切に扱われることが望ましい。
>
> レベル：1、2、3

AU-2 イベントロギング

> 補足 C-SCRM ガイダンス：情報システム又はサプライチェーンネットワーク内の観察可能な事象は、事業体の SDLC コンテキスト及び要件に基づき、サプライチェーンの監査可能な事象として識別されることが望ましい。監査可能な事象には、ソフトウェア／ハードウェアの変更、サプライチェーン情報システムへのアクセスの失敗、又はソースコードの

移動などがある。このような事象に関する情報は適切な監査メカニズムによってキャプチャされ、追跡可能かつ検証可能であることが望ましい。キャプチャされる情報には、事象の種類、日時、長さ、発生頻度などがある。監査はとりわけ、インサイダー脅威により引き起こされるサプライチェーン情報システム又はネットワークの不正使用を検出するのに役立つ可能性がある。ログは、運用上の傾向と長期的な問題を識別する際の主要なリソースである。したがって、事業体はシステム上の問題があるかどうかを判断するために、ベンダの契約更新時点でログのレビューを組み込むことが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。レベル：1、2、3

AU-3 監査記録の内容

補足 C-SCRM ガイダンス：サプライチェーン事象の監査記録は、記録保管の要件に準拠しており、必要に応じて所見の完全性及び記録情報とその情報源の機密性を保持する方法でセキュアに取り扱い及び維持されることが望ましい。特定の状況では、監査記録が管理又は法的手続きで使用されることがある。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

AU-6 監査記録のレビュー、分析、及び報告

補足 C-SCRM ガイダンス：事業体は、サプライチェーン及び情報セキュリティの両方の監査可能な事象が、分析及び報告のために適切に絞り込まれ、相関付けられていることを確実にすることが望ましい。例えば、新しいメンテナンス又はパッチアップグレードに無効なデジタル署名が含まれていることが確認された場合、無効な署名は情報セキュリティの監査可能な事象であるが、パッチ到着の識別はサプライチェーンの監査可能な事象に該当する。この 2つの事象の組み合わせから、C-SCRM に有用な情報が提供される可能性がある。事業体は、特定のベンダにおけるリスクの変化（アクティブな脅威インテリジェンス、リスクプロファイルなど）に基づいて監査記録レビューのレベルを調整することが望ましい。契約では、監査の所見がどのように報告及び調整されるかを明確に扱うことが望ましい。

レベル：2、3

拡張管理策：

(1) 監査記録のレビュー、分析、及び報告 | 非技術的ソースからの情報との相関

補足 C-SCRM ガイダンス：C-SCRM のコンテキストでは、非技術的ソースには、事業体のセキュリティ又は運用ポリシーの変更、調達又は契約プロセスの変更、及びサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及

びその他の ICT/OT 関連のサービスプロバイダからの、システム／コンポーネントの更新、拡張、パッチ、又は廃止／廃棄に関する通知などが含まれる。

レベル：3

AU-10　否認防止

補足 C-SCRM ガイダンス：事業体は、情報システム及びサプライチェーンネットワークの両方の独自性及び完全性を保護するために、否認防止手法を実装することが望ましい。否認防止を必要とする可能性がある例としては、コンポーネント、サプライチェーンの通信、及び納入受領情報を記述するサプライチェーンメタデータがある。情報システムの場合の例としては、ソフトウェアのパッチ又はメンテナンスアップグレード、大規模ハードウェアシステムでのコンポーネントの交換などがある。このようなコンポーネントの出所が OEM であることを検証することは、否認防止の一環である。

レベル：3

拡張管理策：

(1) 否認防止 | アイデンティティとの関連性

補足 C-SCRM ガイダンス：この拡張管理策は、サプライチェーンのトレーサビリティを支援し、来歴の正確性を促進する。

レベル：2

(2) 否認防止 | 情報作成者のアイデンティティのバインディングの妥当性確認

補足 C-SCRM ガイダンス：この拡張管理策は、来歴とサプライチェーン内のコンポーネントの関係の妥当性を確認する。したがって、この拡張管理策により来歴の完全性が確実になる。

レベル：2、3

(3) 否認防止 | 過程管理

補足 C-SCRM ガイダンス：過程管理は、サプライチェーンでの来歴及びトレーサビリティの基盤である。また、システム及びコンポーネントの完全性の検証にも役立つ。

レベル：2、3

AU-12 監査記録の生成

補足 C-SCRM ガイダンス：事業体は、関連するすべてのサプライチェーン監査可能事象をキャプチャするために、監査記録の生成メカニズムが導入されていることを確実にすることが望ましい。このような事象の例としては、コンポーネントバージョンの更新、検収テスト結果からのコンポーネント承認、ロジスティクスデータキャプチャインベントリ、又は輸送情報などがある。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

AU-13 情報開示の監視

補足 C-SCRM ガイダンス：C-SCRM のコンテキストでは、情報開示はオープンソース情報などの複数の手段を通じて発生する可能性がある。例えば、サプライヤが提供した正誤表から、事業体のシステムに関する情報のうち、システムに対するリスクを増大させる情報が明らかになることがある。事業体は、データの漏えいを検知するため請負業者のシステムに対する監視が導入されていること、及びベンダが事業体に対し、事業体が定義する

時間枠に従い、潜在的又は実際の漏えいが発生した場合は可能な限り速やかに事業体に通知するという要件を、契約文言に含めていることを確実にすることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

AU-14 セッション監査

補足 C-SCRM ガイダンス：事業体は、サプライチェーンのセキュリティリスクを識別するために、セッション監査に非連邦政府の契約従業員を含めることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

AU-16 組織横断的監査ロギング

補足 C-SCRM ガイダンス：C-SCRM のコンテキストでは、この管理策には事業体によるシステムインテグレータ又は外部サービスプロバイダのインフラストラクチャの使用が含まれる。事業体は契約に、ベンダとの監査情報要件及び情報交換の合意の調整に関する文言を追加することが望ましい。

レベル：2、3

拡張管理策：

(4) 組織横断的監査ロギング | 監査情報の共有

補足 C-SCRM ガイダンス：事業体とそのシステムインテグレータ又は外部サービスプロバイダの間で分散監査環境又は監査データ共有環境のいずれを管理する場合も、事業体は監査情報共有プロセスの要件を確立することが望ましい。システムインテグレータ及び外部サービスプロバイダと事業体の場合、事業体は、そのミッション運用保護のニーズに対応するために適切な保護が導入されていることを確実にする上で必要な、関連する監査情報を取得することを確実にするために、必要な監査データの種類と提供することができる内容に関するサービス内容合意書に、事前に合意しなければならない。監査情報の収集及び共有について、情報システム及びサプライチェーンネットワークの両方の対象範囲が扱われていることを確実にする。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

ファミリー：アセスメント、認可、及び監視

[FIPS 200]では、承認、認可、及びセキュリティアセスメントの最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）セキュリティ管理策がその適用において有効であるかどうかを判断するために、組織の情報システムでセキュリティ管理策を定期的にアセスメントし、（ii）組織の情報システムの欠陥を訂正し、脆弱性を削減又は排除する目的で考案された行動計画を策定し、実装し、（iii）組織の情報システムの運用及び関連する情報システム接続を認可し、（iv）管理策の継続的な有効性を確実にするために情報システムのセキュリティ管理策を継続的に監視しなければならない。

事業体は、サプライチェーンのリスクマネジメントプロセス及び本出版物で定義されている関連管理策の使用などを含め、C-SCRM を継続的セキュリティアセスメント及び認可活動に統合することが望ましい。これには、事業体の情報システムをアセスメント及び認可する活動と、該当する場合にサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの外部アセスメントが含まれる。サプライチェーンの側面には、文書化、事業体内又は事業体間での過程管理及びシステム相互接続の追跡、サプライチェーンのサイバーセキュリティトレーニングの検証、サプライヤのセキュリティへの準拠表明の検証、製品／コンポーネントの完全性、及び手動での検査技法を含む、純正コンポーネントの検査を使用した偽造品又はマルウェア（トロイの木馬など）を検出する非侵襲的アプローチのための検証ツール及び技法などが含まれる。

CA-1 ポリシー及び手順

補足 C-SCRM ガイダンス：サプライチェーンのサイバーセキュリティのアセスメント及び認可ポリシーと手順の策定及び実装を、管理策アセスメント及び認可のポリシー、及び関連する C-SCRM 戦略／実装計画、ポリシー、及びシステムレベルの計画に統合する。サプライチェーン全体のサイバーセキュリティリスクに対処するために、事業体は管理策アセスメント及び認可の C-SCRM 活動を方向付ける C-SCRM ポリシーを策定すること（又は必要に応じて既存のポリシーに統合すること）が望ましい。C-SCRM ポリシーでは、事業体内で管理策アセスメント及び認可を実施する C-SCRM の役割及び責任、役割間のあらゆる依存関係、及び役割間の相互作用を定義することが望ましい。事業体全体のセキュリティ及びプライバシーリスクは、継続的にアセスメントし、またサプライチェーンのリスクアセスメント結果を含めることが望ましい。

レベル：1、2、3

CA-2 管理策アセスメント

補足 C-SCRM ガイダンス：管理策アセスメント計画に、関連する C-SCRM 管理策及び拡張管理策が組み込まれていることを確実にする。管理策アセスメントは、情報システムとサプライチェーンの両方のアセスメントを対象としていることが望ましく、また事業体に関連する管理策及び拡張管理策のベースラインセットが識別され、アセスメント

に使用されることを確実にすることが望ましい。管理策アセスメントには、サプライヤ監査、レビュー、及びサプライチェーン関連情報を含めることができる。事業体は、サプライチェーンのリスクアセスメントにおけるプロバイダとの協働に関する戦略などの情報収集戦略を策定する。このような協力により、事業体はプロバイダからの情報を活用し、冗長性を削減し、リスク対応のための潜在的な行動方針を識別し、プロバイダの負荷を軽減することができる。C-SCRM 人員が管理策アセスメントをレビューすることが望ましい。

レベル：2、3

拡張管理策：

(1) 管理策アセスメント | 特化したアセスメント

補足 C-SCRM ガイダンス：事業体は、継続的監視、インサイダー脅威アセスメント、悪意のあるユーザのアセスメントなどの様々なアセスメント技法及び方法論を使用することが望ましい。これらのアセスメントメカニズムはコンテキスト固有であり、事業体は、そのサプライチェーンを理解し、アセスメントを実施して適切な保護が実装されていることを検証するために必要な一連の手段を定義する必要がある。

レベル：3

(2) 管理策アセスメント | 外部組織からの結果の活用

補足 C-SCRM ガイダンス：C-SCRM では、事業体はサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダに対して外部セキュリティアセスメントを使用することが望ましい。外部アセスメントには、認証、第三者アセスメント、及び連邦政府の環境では他の各省庁及び関係機関が実行する事前アセスメントが含まれる。国際標準化機構（ISO）、国家情報保証パートナーシップ（National Information Assurance Partnership）（コモンクライテリア）、及びオープングループトラステッドテクノロジーフォーラム（Open Group Trusted Technology Forum）（OTFF）からの認証も、政府機関のニーズに対応している限り、非連邦政府及び連邦政府事業体が同様に利用することができる。

レベル：3

CA-3 情報交換

補足 C-SCRM ガイダンス：システムと他のシステム間での情報又はデータの交換では、サプライチェーンの観点から精査が必要である。これには、直接相互接続するコンポーネント／システムのインタフェースの特性及び接続、又は開発者、システムインテグレータ、外部システムサービスプロバイダ、その他の ICT/OT 関連のサービスプロバイダ、及び場合によってはサプライヤの間でこれらのコンポーネント／システムを通じて共有されるデータを理解することが含まれる。異なるセキュリティ又はプライバシーポリシーが適用されている異なるセキュリティ又はプライバシードメイン内のシステム間で情報が転送されると、このような転送が 1 つ以上のドメインセキュリティ又はプライバシーポリシーに違反するリスクが生じるため、事業体が定義したシステム情報交換の要件に準拠していることを確実にするために、適切なサービス内容合意書が導入されていることが望ましい。このような相互接続の例を以下に示す。

a. 事業体及びシステムインテグレータの間で共有されている開発及び運用環境
b. 既製品プライヤへの製品更新／パッチ管理接続
c. 外部サービスプロバイダ共有環境内にある処理システムでのデータ要求及び取得トランザクション

事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：3

CA-5 行動計画及びマイルストーン

補足 C-SCRM ガイダンス：システムレベルの行動計画及びマイルストーン（POA&M）について、事業体は C-SCRM 向けに個別の POA&M が存在しており、情報システム及びサプライチェーンの両方が含まれていることを確実にする必要がある。C-SCRM POA&M には、システムの認可前又は認可後に完了することが推奨される実行対象タスク、タスクの完了に必要なリソース、タスクを満たすために設定されたマイルストーン、マイルストーンとタスクの完了予定日が含まれていることが望ましい。事業体は、関連する弱点、情報システム又はサプライチェーンの弱点のインパクト、弱点に対処するための改善、及び継続的監視活動を C-SCRM POA&M に含めることが望ましい。C-SCRM POA&M は認可パッケージの一部として含まれることが望ましい。

レベル：2、3

CA-6 認可

補足 C-SCRM ガイダンス：認可権限のある担当者は認可の決定に C-SCRM を含めることが望ましい。これを実現するには、C-SCRM 計画又はシステムセキュリティ計画及び C-SCRM POA&M に記載されているサプライチェーンリスク及び代替管理策を、意思決定プロセスの一環として認可パッケージに含めることが望ましい。重要度、脅威、及び脆弱性分析のアウトプットに基づいてリスクを判断し、関連する代替管理策を選択することが望ましい。認可権限のある担当者は、本出版物の第 2 節にあるガイダンスと NISTIR 8179 を使用してアセスメントプロセスを手引きすることができる。

レベル：1、2、3

CA-7 継続的監視

補足 C-SCRM ガイダンス：この管理策に関する C-SCRM 固有のガイダンスについては、本出版物の第 2 節を参照。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

拡張管理策：

(3) 継続的監視 | トレンド分析

補足 C-SCRM ガイダンス：継続的監視／トレンド分析で収集された情報は、重要度分析、脆弱性及び脅威分析、並びにリスクアセスメントなどの C-SCRM 決定のインプットとして利用することができる。また、インシデント対応に使用でき、インサイダー脅威などのサプライチェーンのサイバーセキュリティ侵害を潜在的に識別することができる情報も提供される。

レベル：3

ファミリー：構成管理

[FIPS 200]では、構成管理の最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）組織の情報システム（ハードウェア、ソフトウェア、ファームウェア、及び文書を含む）のベースライン構成及びインベントリをそれぞれのシステム開発ライフサイクル全体について確率及び維持し、（ii）組織の情報システムに採用されている情報技術製品のセキュリティ構成設定を確立及び適用しなければならない。

構成管理は、SDLC 全体を通じて情報システム及びネットワーク内のシステム、コンポーネント、及び文書に対して行われた変更を追跡するのに役立つ。これは、システム、コンポーネント、及び文書に対してどのような変更が行われたか、誰が変更を行ったか、及び誰が変更を認可したかを把握する上で重要である。構成管理はまた、認可された変更と認可されなかった変更を判別するときに、サプライチェーンのサイバーセキュリティ侵害調査に証拠を提供する。事業体は構成管理管理策を事業体独自のシステムに適用し、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダによる構成管理管理策の使用を推奨することが望ましい。構成管理の詳細については、NISTIR 7622 を参照。

CM-1 ポリシー及び手順

補足 C-SCRM ガイダンス：構成管理はサプライチェーンのほぼすべての側面に影響する。構成管理は、SDLC 及びサプライチェーンを通じてコンポーネントを追跡することを含め、事業体がコンポーネントの来歴を確立することができる能力にとって不可欠である。適切に定義及び実装された構成管理ケイパビリティ（能力）は、SDLC 及びサプライチェーン全体を通じて、コンポーネントが真正であり、不適切な改ざんが行われてないというアシュアランスを高める。事業体は構成管理のポリシー及び手順を定義するときに、事業体の情報システムの境界へのコンポーネントの導入及び境界からのコンポーネントの除外の手順を含め、SDLC 全体に対処することが望ましい。構成管理ポリシーには、構成アイテム、構成アイテムと対応するメタデータのデータ保持、及び構成アイテムとそのメタデータの追跡を組み込むことが望ましい。事業体は、構成管理ポリシーに関してサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと連携することが望ましい。

レベル：1、2、3

CM-2 ベースライン構成

補足 C-SCRM ガイダンス：事業体は、ステークホルダーの合意内容の文書化、正式なレビュー、及び確保を含む、情報システム及び開発環境両方のベースライン構成を確立することが望ましい。ベースラインの目的は、SDLC 全体を通じたコンポーネント、コード、及び／又は設定の変更を追跡するための出発点を提供することである。ベースライン構成の定期的なレビュー及び更新（すなわち、再ベースライン設定）は、トレーサビリティ及び来歴にとって不可欠である。ベースライン構成では、事業体の運用環境と、関連するすべてのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダによる組織の情報シス

テム及びネットワークへの関与を考慮しなければならない。例えばシステムインテグレータが組織の既存のインフラストラクチャを使用する場合、アクセスと運用に関して合意された適切な一連の基準を反映するベースラインを確立するために、適切な対策を取ることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) ベースライン構成 | 開発及びテスト環境

補足 C-SCRM ガイダンス：事業体は、該当するサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの開発、テスト（及び該当する場合はステージング）環境のベースライン構成と、インタフェースのすべての構成を保守するか、又は保守を求めることが望ましい。

レベル：2、3

CM-3 構成変更管理

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワーク内と SDLC 全体で構成設定及び変更管理を決定、実装、監視、及び監査することが望ましい。この管理策は、C-SCRM のトレーサビリティをサポートする。以下の NIST SP 800-53, Rev. 5 の拡張管理策 CM-3 (1)、(2)、(4)、及び (8) は、C-SCRM で変更管理データを収集及び管理するために使用することができるメカニズムである。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

(1) 構成変更管理 | 自動化された文書化、通知、及び変更禁止

補足 C-SCRM ガイダンス：事業体は、情報システムと、基盤となるシステム及びネットワーク又は相互運用システム及びネットワークを保護する上で不可欠な一連のシステム変更を定義することが望ましい。このような変更は、重要度分析（コンポーネント、プロセス、及び機能を含む）と、（リソースの制約条件などが原因で）まだ改善されていない脆弱性が存在する場所に基づいて定義することができる。変更管理プロセスではまた、この管理策が引き続き必要とされているとおりに機能することを確実にするために、既存のセキュリティ管理策に影響する可能性がある変更を監視することが望ましい。

レベル：2、3

(2) 構成変更管理 | 変更のテスト、妥当性確認、及び文書化

補足 C-SCRM ガイダンス：変更の実装を最終決定する前に、システムに対する変更のテスト、妥当性確認、及び文書化を行う。

レベル：2、3

(3) 構成変更管理 | セキュリティ及びプライバシーに関する代表者

補足 C-SCRM ガイダンス：事業体のセキュリティ及びプライバシーに関する代表者を構成変更管理機能のメンバーにする必要がある。

レベル：2、3

(4) 構成変更管理 | 構成の変更の防止又は制限

補足 C-SCRM ガイダンス：事業体により定義された状況におけるシステムの構成の変更を防止又は制限する。

レベル：2、3

CM-4 インパクト分析

補足 C-SCRM ガイダンス：事業体は、情報システムと、基盤となるシステム及びネットワーク又は相互運用システム及びネットワークに対する変更を検討して、これらの変更が既存のセキュリティ管理策に影響し、サプライチェーン全体のサイバーセキュリティリスクの受容可能なレベルを維持するために追加又は異なる保護が必要になるかどうかを判断することが望ましい。システムエンジニア及びシステムセキュリティエンジニアなどのステークホルダーの視点を C-SCRM に提供するために、これらのステークホルダーがインパクト分析活動に含まれていることを確実にする。NIST SP 800-53, Rev. 5 の拡張管理策 CM-4 (1) は、テスト環境を通じてもたらされる可能性がある脆弱性から情報システムを保護するために使用することができるメカニズムである。

レベル：3

(1) インパクト分析 | 独立したテスト環境

システムへの変更を運用環境に実装する前に、個別のテスト環境でこれらの変更を分析し、欠陥、弱点、非互換性、又は意図的な悪意などに起因するセキュリティ及びプライバシーに対する影響があるかどうかを確認する。

レベル：3

関連管理策：SA-11、SC-7

CM-5 変更に対するアクセス制限

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワークに対する変更に関する物理及び論理アクセスの制限に関する要件が定義され、事業体のアクセス制限の実装に含まれていることを確実にすることが望ましい。例としては、ソフトウェアコンポーネントの更新の一元管理プロセスと更新又はパッチの展開の変更に対するアクセス制限などがある。

レベル：2、3

拡張管理策：

(2)変更に対するアクセス制限/自動化されたアクセス実施及び監査記録

補足 C-SCRM ガイダンス：事業体は、自動化されたアクセス実施と、情報システムと基盤となるシステム及びネットワークの監査を確実にするためのメカニズムを実装することが望ましい。

レベル：3

(3)変更に対するアクセス制限 | ライブラリに関する特権の限定

補足 C-SCRM ガイダンス：事業体は、ソフトウェアライブラリが構成アイテムとして扱われる可能性があり、ライブラリへのアクセスを管理及び制御すべきであることに注意することが望ましい。

レベル：3

CM-6 構成設定

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワークと SDLC 全体で構成設定の変更機能を監督することが望ましい。監督方法には、定期的な検証、報告、及びレビューなどがある。その結果生成される情報は、事業体の情報システム及びネットワークにアクセスすることができるか、接続しているか、又はそれらのシステム及びネットワークの構築に携わる様々な関係者と、知る必要性に基づいて共有することができる。変更は実装前にテスト及び承認されるべきである。変更発生時に指名された事業体担当者に警告するために、構成設定を監視及び監査することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) 構成設定 | 自動化された管理、適用、及び検証

補足 C-SCRM ガイダンス：事業体は、可能な場合には構成設定の管理、適用、及び検証に自動化メカニズムを採用することが望ましい。

レベル：3

(2) 構成設定 | 認可されていない変更への対応

補足 C-SCRM ガイダンス：事業体は、構成設定に対する認可されていない変更が、指名されたセキュリティ又は IT 人員に警告されることを確実にすることが望ましい。サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダがこのような認可されていない変更の責任を負う場合、これはトレンドを監視するために記録及び追跡されるべき C-SCRM インシデントと見なされる。より包括的な見解を得るには、事前に定義された特定の一連の C-SCRM ステークホルダーが、サプライチェーンにおける認可されていない変更の影響をアセスメントすることが望ましい。影響のアセスメント時には、関連するステークホルダーが、包括的な解決策を確実にするための適切な軽減戦略の定義と実装を支援することが望ましい。

レベル：3

CM-7 最小機能性

補足 C-SCRM ガイダンス：最小機能性により、攻撃対象領域が縮小される。事業体は、最小機能性を規定及び実装することができる柔軟性を有するコンポーネントを選択することが望ましい。事業体は、情報システム及びネットワークと SDLC 全体で最小機能性を確実にすることが望ましい。事業体システムに接続している認可されていないハード

ウェアを使用することで生じる可能性がある脆弱性から情報システム及びネットワークを保護するために、NIST SP 800-53, Rev. 5 の拡張管理策 CM-7 (9) のメカニズムを使用することができる。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：3

拡張管理策：

(1) 最小機能性 | 定期的なレビュー

補足 C-SCRM ガイダンス：事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

(2) 最小機能性 | 認可されていないソフトウェア

補足 C-SCRM ガイダンス：事業体は、許可されていないソフトウェアを規定及び検出するための要件を定義し、適切なプロセスを展開することが望ましい。少なくとも、評判が悪いソフトウェア又は認可されていないソフトウェアを使用しないという要件を定義することで、この作業を促進することができる。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

(3) 最小機能性 | 認可されたソフトウェア

補足 C-SCRM ガイダンス：事業体は、許容可能なソフトウェアを規定するための要件を定義し、適切なプロセスを展開することが望ましい。評判の良いソフトウェアのみを使用するという要件を定義することで、この作業を促進することができる。これには、新しいソフトウェア及びソフトウェア更新が事業体の環境に導入されるときに警告を求めるという要件も含まれる。このような要件の例としては、事業体によってコードの評価が可能であり、コードが受け入れ可能であると判断された場合にのみオープンソースソフトウェアを許可することなどがある。

レベル：3

(4) 最小機能性 | 限定された特権を備えた制限環境

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワーク上のソフトウェア、ファームウェア、及び情報の完全性を保証するために、コード実行時にデジタル署名などのコード認証メカニズムが実装されていることを確実にすることが望ましい。

レベル：2、3

(5) リモートアクセス | メカニズムに関する情報の保護

補足 C-SCRM ガイダンス：事業体は、バイナリ又はマシン実行可能なコードを OEM／開発者又はその他の受け入れ可能な検証済みの供給源から直接取得することが望ましい。

レベル：3

(6) 最小機能性 | バイナリ又はマシン実行可能コード

補足 C-SCRM ガイダンス：従わざるを得ないミッション又は運用上の要件のために保証が限定されているか又は無保証であり、ソースコードを伴わないソフトウェア製品の使用を例外として認める場合、認可権限のある担当者による承認は、事業体がそのようなソフトウェア製品のより広範なアセスメントの一部としてサプライチェーンのサイバーセキュリティリスクアセスメントを明示的に取り入れていること、並びに識別及びアセスメントされたリスクに対処するための代替管理策が実装されていることを条件とする。

レベル：2、3

(7) 最小機能性 | 認可されていないハードウェアの使用の禁止

事業体は、許可されていないハードウェアを規定及び検出するための要件を定義し、適切なプロセスを展開することが望ましい。少なくとも、評判が悪いハードウェア又は認可されていないハードウェアを使用しないという要件を定義することで、この作業を促進することができる。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

CM-8 システムコンポーネントのインベントリ

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワーク内の重要なコンポーネント資産が資産インベントリに含まれていることを確実にすることが望ましい。このインベントリには、重要なコンポーネントの説明責任に関する情報も含まれていなければならない。インベントリの情報には、例えば、ハードウェアインベントリ仕様書、ソフトウェアライセンス情報、ソフトウェアバージョン番号、コンポーネント所有者、及び、 ネットワーク接続コンポーネント又はデバイスの場合はマシン名及びネットワークアドレスが含まれる。インベントリ仕様書には、製造業者、デバイスの種類、モデル、シリアル番号、物理的な場所が含まれる場合がある。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。必要な情報のみがサプライチェーンの様々な参加者に伝達されることを確実にするために、事業体は要件と情報フローの実施方法を規定することが望ましい。情報のサブセットが下流に提供される場合、サブセット情報の作成者に関する情報が必要である。事業体は、購入したソフトウェア、オープンソースソフトウェア、社内開発ソフトウェアを含む、適用可能で適切なソフトウェアクラスの SBOM の作成を検討することが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って SBOM の追加ガイダンスとすることが望ましい。

レベル：2、3

拡張管理策：

(1) システムコンポーネントのインベントリ： | インストール中及び削除中の更新

補足 C-SCRM ガイダンス：事業体は情報システム、情報システムコンポーネント、又はネットワークコンポーネントをインストール、更新、又は削除する際に、重要なコンポーネントを追跡するためのトレーサビリティを確保するために、インベントリを更新する必要がある。さらに、サプライチェーン保護の正確なインベントリを確保するために情報システムの構成を更新してから、適宜ベースラインを再設定する必要がある。

レベル：3

(2) システムコンポーネントのインベントリ | 自動化されたメンテナンス

補足 C-SCRM ガイダンス：事業体は、インストール、更新、及び削除について、情報システム及びネットワークのコンポーネントインベントリの変更が監視されることを確実にするために、自動化されたメンテナンスメカニズムを実装することが望ましい。事前に定義された頻度と、定義されている各コンポーネントに関する関連インベントリ情報の自動収集を使用して自動化されたメンテナンスを実行するときには、事業体は、評価のために関連するステークホルダーに対し更新が利用可能であることを確実することが望ましい。インサイダー脅威がセキュリティメカニズムをバイパスするリスクを低減するために、事前に定義されるデータ収集頻度は予測しにくいことが望ましい。

レベル：3

(3) システムコンポーネントのインベントリ | 説明責任情報

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワークコンポーネントの説明責任情報が収集されることを確実にすることが望ましい。システム／コンポーネントインベントリ情報は、取得を開始する個人、及びシステム／コンポーネントを管理又は使用することができる関連人員などの対象エンドユーザを識別することが望ましい。

レベル：3

(4) システムコンポーネントのインベントリ | アセスメント済みの構成及び承認された偏差

補足 C-SCRM ガイダンス：アセスメント済みの構成及び承認された偏差を文書化して追跡しなければならない。情報システム及びネットワークのベースライン構成に対する変更によってサプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）が増大しないことを確実にするために、変更はすべて、関連するステークホルダーによるレビューを必要とする。

レベル：3

(5) システムコンポーネントのインベントリ | 集中化されたリポジトリ

補足 C-SCRM ガイダンス：事業体は、事業体のすべての情報システム、ネットワーク、及びそのコンポーネントからのコンポーネントを含む集中化されたリポジトリを実装してもよい。インベントリの集中化されたリポジトリは、情報システム、ネットワーク、及びそのコンポーネントの算定を効率化する機会を提供する。このようなリポジトリは、侵害又はブリーチされたか、又は軽減措置が必要なコンポーネントの位置及び責任者を事業体が迅速に識別するのにも役立つ可能性がある。事業体は、適切なコンポーネントの説明責任に必要なサプライチェーン固有の情報（サプライチェーンの関連性及び情報システム、ネットワーク、又はコンポーネントオーナーなど）が集中化されたインベントリに含まれていることを確実にすることが望ましい。

レベル：3

(6) システムコンポーネントのインベントリ | 自動化された位置追跡機能

補足 C-SCRM ガイダンス：事業体は、情報システムコンポーネントの物理的な位置を追跡する自動メカニズムを採用するときに、的確なインベントリであることを確実にするために、情報システム、ネットワーク、及びコンポーネントの追跡ニーズを組み入れることが望ましい。

レベル：2、3

(7) システムコンポーネントのインベントリ | システムへのコンポーネントの設定

補足 C-SCRM ガイダンス：事業体は、コンポーネントをシステムに設定するときに、情報システム及びネットワークと関連するすべてのコンポーネントのインベントリが作成され、これらがマークされ、適切に設定されていることを確実にすることが望ましい。これにより、情報システム及びネットワークに関連するすべてのコンポーネントのインベントリの迅速な作成が容易になり、また重要であると見なされ、情報シス

テム及びネットワーク保護活動の一環として差別化処理を必要とするコンポーネントを追跡することができるようになる。

レベル：3

(8) システムコンポーネントのインベントリ | オープンソースプロジェクトの *SBOM*

補足 C-SCRM ガイダンス：事業体が SBOM のないオープンソースプロジェクトを使用していて SBOM を必要とする場合、事業体は 1）オープンソースプロジェクトに SBOM の生成機能を提供するか、2）このケイパビリティ（能力）を追加するためにプロジェクトにリソースを提供するか、又は 3）オープンソースプロジェクトの各バージョンを最初に使用するときに SBOM を生成する必要がある。

レベル：3

CM-9 構成管理計画

補足 C-SCRM ガイダンス：事業体は、C-SCRM が構成管理計画活動に組み込まれていることを確実にすることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

拡張管理策：

(1) 構成管理計画 | 責任の設定

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワークの構成管理活動に対処するためにすべての関連する役割が定義されていることを確実にすることが望ましい。事業体は、構成管理の要件及びケイパビリティ（能力）が適切に扱われているか、要件の定義、策定、テスト、市場調査及び分析、調達の提案及び契約、コンポーネントのインストール又は削除、システム統合、運用、及びメンテナンスのサプライチェーン活動に含まれていることを確実にすることが望ましい。

レベル：2、3

CM-10 ソフトウェアの使用制限

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワーク内で使用されるソフトウェアのライセンスが文書化、追跡、及び維持されていることを確実にすることが望ましい。追跡メカニズムは、アクセス制御情報及びプロセスまでユーザ及びライセンスの使用を追跡することができる機能を提供することが望ましい。例えば、従業員の解雇時には「指名ユーザ」ライセンスを取り消し、この変更を反映するためにライセンス文書を更新することが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation’s Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) ソフトウェアの使用制限 | オープンソースソフトウェア

補足 C-SCRM ガイダンス：事業体はソフトウェアについて検討する際に、オープンソース又は商用ライセンスコンポーネントを含むすべての選択肢及び対応するリスクをレビューすることが望ましい。事業体は、オープンソースソフトウェア（OSS）を使用する際には、来歴、構成管理、ソース、バイナリ、再利用可能なフレームワーク、再利用可能なライブラリのテスト及び使用に関する可用性、及びサプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）レベルに影響する可能性があるその他の情報に関する、オープンソースコミュニティの一般的な手順を理解及びレビューすることが望ましい。統合開発環境（IDE）及びウェブサーバなど、現在事業体が使用しているオープンソースソリューションは多数ある。事業体は以下を行うことが望ましい。

a. OSS 及び関連文書の利用状況を追跡する。
b. OSS の利用がライセンス条件に準拠しており、これらの条件が事業体にとって受け入れ可能なものであることを確実にする。
c.ソフトウェアの配布は複製及び配布を制御するライセンス合意に関連しているため、ソフトウェアの配布を文書化及び監視する。
d. オープンソース開発者から提供される OSS のサプライチェーンを評価し、定期的に監査する（来歴、構成管理、再利用可能ライブラリの使用に関する情報など）。この評価は、公開されていることが多い既存の文書を取得し、また、事業体が関与した可能性があるソフトウェアの更新及びダウンロードプロセスに基づく経験を使用することで実行することができる。

レベル：2、3

CM-11 ユーザがインストールしたソフトウェア

補足 C-SCRM ガイダンス：この管理策は、事業体に雇用されていない、事業体の情報システム及びネットワークのユーザに拡張される。これらのユーザは、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダなどであることがある。

レベル：2、3

CM-12 情報の位置

補足 C-SCRM ガイダンス：様々な物理的位置に存在する情報は、情報の特定の位置に応じて、サプライチェーン全体の様々なサイバーセキュリティリスクにさらされる可能性がある。様々な物理的位置から提供又は運用されるコンポーネントも、特定の提供元又は運用の位置に応じて様々なサプライチェーンリスクにさらされる可能性がある。事業体はアクセス制御を制限し、バックアップ／復元、パッチ適用／アップグレード、及び情報転送／共有のために許可する位置と許可しない位置を規定することで、これらのリスクを管理することが望ましい。NIST SP 800-53, Rev. 5 の拡張管理策 CM-12 (1) は、コンポーネントの自動位置特定を有効にするために使用することができるメカニズムである。

レベル：2、3

拡張管理策：

(1) 情報の位置 | 情報の位置をサポートする自動化されたツール

事業体の情報と個人のプライバシーを保護するための管理策が導入されていることを確実にするために、自動化ツールを使用してシステムコンポーネントに関する事業体定義の情報を識別する。

レベル：2、3

CM-13 データアクションのマッピング

補足 C-SCRM ガイダンス：個人情報の他に、機密情報又は国家機密情報に対するシステムによるデータアクションのマップを理解及び文書化する必要がある。データアクションのマッピングはまた、モノのインターネット（IoT）デバイス、組み込み又はスタンドアロンの IoT システム、又は IoT システム・オブ・システムのデータアクションをマッピングする目的で実施されることが望ましい。処理されている国家機密情報又は IoT 情報、その機微性及び／又は物理的なモノ又は物理的な環境への影響、機密情報又は IoT 情報の処理方法（データアクションが個人に対して可視化されているか、又はシステムの別の部分で処理されるかなど）、及び誰がリスクの度合いをアセスメントする上で重要な多数のコンテキスト的要因を提供するかを把握する。データマップは様々な方法で示すことができ、詳細さのレベルは事業体のミッション及びビジネスニーズに基づいて異なる可能性がある。データマップは、事業体が使用するシステム設計成果物のオーバーレイであることがある。このマップの策定では、対象となるデータアクションとシステムの一部として識別されるコンポーネントに関して、プログラム及びセキュリティ人員間の連携が必要になることがある。

レベル：2、3

CM-14 署名されたコンポーネント

補足 C-SCRM ガイダンス：事業体は、信頼されている証明書機関からデジタル署名されたコンポーネントを使用して、取得したハードウェア及びソフトウェアコンポーネントが真正かつ有効であることを検証することが望ましい。インストールを許可する前にコンポーネントを検証することは、事業体がサプライチェーン全体のサイバーセキュリティリスクを低減するのに役立つ。

レベル：3

ファミリー：緊急時対応計画

[FIPS 200]では、緊急時対応計画の最小限のセキュリティ要件を以下のように規定している。

> 組織は、緊急事態における重要な情報リソースの可用性及び運用の継続性を確実にするために、緊急時における対応、バックアップ運用、及び組織の情報システムの災害後の復旧計画を確立、維持、及び効果的に実装しなければならない。

サプライチェーンのサイバーセキュリティの緊急時対応計画には、システムコンポーネントの代替サプライヤ、システム及びサービスの代替サプライヤ、重要なシステムコンポーネントの代替納入経路、及びサプライチェーンに対するサービス拒否攻撃に関する計画が含まれる。このような緊急時対応計画は、特に既存のサービスプロバイダが重要なミッション機能をサポートするサービスを納入するときに、このプロバイダが効果的な運用継続計画を導入していることを確実にするのに役立つ。さらに、代替処理サイトなどの緊急時対応計画に使用される様々な技法には独自のサプライチェーンが存在し、独自のサイバーセキュリティリスクを伴う。事業体は必要に応じて、サプライチェーン全体のサイバーセキュリティリスク及び緊急時対応計画活動に関連する依存関係を理解及び管理することを確実にすることが望ましい。

CP-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、C-SCRM を緊急時対応計画ポリシー及び関連する SCRM 戦略／実装計画、ポリシー、及び SCRM 計画に統合することが望ましい。このポリシーは情報システム及びサプライチェーンネットワークを対象とし、少なくとも以下のようなシナリオに対処することが望ましい。

a. 予定外のコンポーネント故障及びその後の交換
b. 機能の強化、メンテナンス、アップグレード、最新化に関する予定されている交換及び
c. 製品及び／又はサービス中断

レベル：1、2、3

CP-2 緊急時対応計画

補足 C-SCRM ガイダンス：事業体は、データ又は運用の損失又は劣化を軽減するための準備ができていることを確実にするために、サプライチェーンの情報システム及びネットワークの緊急時対応計画を定義及び実装することが望ましい。侵害からの保護を確実にし、適切なフェイルオーバー及び許容可能な運用状態へのタイムリーな復旧を提供するために、サプライチェーン、ネットワーク、情報システム（特に重要なコンポーネント）、及びプロセスのための緊急時対応を導入しておくことが望ましい。

レベル：2、3

拡張管理策：

(1) 緊急時対応計画 | 関連計画との調整

補足 C-SCRM ガイダンス：サプライチェーンリスクの緊急時対応計画の策定について、関連計画を担当する事業体の部署と調整する。

レベル：2、3

(2) 緊急時対応計画 | 処理能力計画

補足 C-SCRM ガイダンス：この拡張管理策は、サプライチェーンネットワーク又は情報システムコンポーネントの可用性を確保するのに役立つ。

レベル：2、3

(3) 緊急時対応計画 | 外部サービスプロバイダとの調整

補足 C-SCRM ガイダンス：事業体は、外部サービスプロバイダから提供されるサプライチェーンネットワーク、情報システム、及びコンポーネントに、サービス中断を削減又は防止するか、若しくはタイムリーな復旧を確実にするための（人員、機器、及びネットワークリソースを含む）適切なフェイルオーバー機能が存在していることを確実にすることが望ましい。事業体は、サービス内容合意書の一部として緊急時対応計画要件が定義されていることを確実にすることが望ましい。この合意書には、運用継続を確実にするために、サービス拒否攻撃発生時の重要なコンポーネント及び機能のサポートを扱う特定の条項が含まれていることがある。事業体は、サービスプロバイダの既存の緊急時対応計画のプラクティスを識別し、事業体のミッション及びビジネスニーズに基づき必要に応じてこれらを強化するために、外部サービスプロバイダとの調整を行うことが望ましい。このような調整は、コスト削減と効率的な実装を支援する。事業体は、ミッション及びビジネス上重要なサービス又は製品、若しくはミッション及びビジネスイネーブリングサービス又は製品を提供する一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：3

(4) 緊急時対応計画 | 重要な資産の識別

補足 C-SCRM ガイダンス：運用継続性を確保するために、重要な資産（ハードウェア、ソフトウェア、及び担当者を含む）が識別され、適切な緊急時対応計画の要件が定義及び適用されていることを確実にする。このプロセスの主要なステップは、コンポーネント、機能、及びプロセスに対して重要度分析を実行して、すべての重要な資産を識別することである。重要度分析に関する追加のガイダンスについては、第 2 節及び NISTIR 8179 を参照。

レベル：3

CP-3 緊急時対応トレーニング

補足 C-SCRM ガイダンス：事業体は、緊急時対応トレーニングに重要なサプライヤが含まれていることを確実にすることが望ましい。 事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation’s Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) 緊急時対応トレーニング | シミュレーションイベント

補足 C-SCRM ガイダンス：事業体は、重要なサービスの提供における役割及び責任を担うサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが、緊急時対応トレーニング演習に含まれていることを確実にすることが望ましい。

レベル：3

CP-4 緊急時対応計画テスト

補足 C-SCRM ガイダンス：事業体は、緊急時対応テストに重要なサプライヤが含まれていることを確実にすることが望ましい。事業体はサービスプロバイダと連携して、一次製造サイトからバックアップサイトへのフェイルオーバーなどの継続性／レジリエンシーケイパビリティ（能力）をテストすることが望ましい。このテストは、トレーニング演習とは別に実行するか、又は演習中に実行することができる。事業体は C-SCRM 脅威アセスメントのアウトプットを参照して、事業体が C-SCRM 脅威事象にどの程度耐えることができるか、及び／又はこのような事象からどの程度復旧することができるかをテストするためのシナリオを策定することが望ましい。

レベル：2、3

CP-6 代替保管サイト

補足 C-SCRM ガイダンス：サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダによって管理されている場合、代替保管サイトは事業体のサプライチェーンネットワーク内にあるものと見なされる。事業体はサプライチェーンのサイバーセキュリティの適切な管理策をこれらの保管サイトに適用することが望ましい。

レベル：2、3

拡張管理策：

(1) 代替保管サイト | 一次サイトからの分離

補足 C-SCRM ガイダンス：この拡張管理策は、サプライチェーンネットワーク、情報システム、及び情報システムコンポーネントのレジリエンシーを確保するのに役立つ。

レベル：2、3

CP-7 代替処理サイト

補足 C-SCRM ガイダンス：サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダにより管理されている場合、代替処理サイトは事業体のサプライチェーン内にあるものと見なされる。事業体はサプライチェーンの適切なサイバーセキュリティ管理策をこれらの処理サイトに適用することが望ましい。

レベル：2、3

CP-8 通信サービス

補足 C-SCRM ガイダンス：事業体は、重要な情報システムをサポートするためにサプライチェーンの代替通信サービスプロバイダを組み入れることが望ましい。

レベル：2、3

拡張管理策：

(1) 通信サービス | 一次プロバイダ及び代替プロバイダの分離

補足 C-SCRM ガイダンス：一次プロバイダ及び代替プロバイダの分離により、サプライチェーンのサイバーセキュリティに対するレジリエンスが促進される。

レベル：2、3

(2) 通信サービス | プロバイダの緊急時対応計画

補足 C-SCRM ガイダンス：C-SCRM では、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの緊急時対応計画で、必要に応じてインフラストラクチャ、サービス、プロセス、及び人員の分離が提供されることが望ましい。

レベル：2、3

CP-11 代替通信プロトコル

補足 C-SCRM ガイダンス：事業体は、サプライチェーンのレジリエンスを確立するために、代替通信プロトコルケイパビリティ（能力）の組み込みの一環として、重要なサプライヤが緊急時対応計画、トレーニング、及びテストに含まれていることを確実にすることが望ましい。

レベル：2、3

ファミリー：識別及び認証

[FIPS 200]では、識別及び認証の最小限のセキュリティ要件を以下のように規定している。

> 組織は、組織の情報システムへのアクセスを許可する前提条件として、情報システムユーザ、ユーザの代理として動作するプロセス、又はデバイスを識別し、これらのユーザ、プロセス、又はデバイスのアイデンティティを認証（又は検証）しなければならない。

NIST SP 800-161、「連邦情報システム及び組織におけるサプライチェーンリスクマネジメントのプラクティス（*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*）」は、サプライチェーンネットワーク内の個人（ユーザ）及び個人の代理として動作するプロセスに加えて、コンポーネントの識別及び認証を含めるように[FIPS 200]の識別及び認証管理策ファミリーを拡張している。識別及び認証は、事業体のサプライチェーンネットワーク内で個人、個人の代理として動作するプロセス、及び特定のシステム／コンポーネントのトレーサビリティ（追跡可能性）を提供するので、C-SCRM にとって重要である。識別及び認証は、サプライチェーン全体のサイバーセキュリティリスクを適切に管理して、サプライチェーンのサイバーセキュリティ侵害のリスクを低減し、かつサプライチェーンのサイバーセキュリティ侵害の証拠を生成するために必要である。

IA-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、サプライチェーンネットワーク内の重要な役割とプロセスが定義され、事業体の重要なシステム、コンポーネント、及びプロセスがトレーサビリティのために識別されることを確実にするために、事業体が定義した間隔で、アイデンティティ及びアクセス管理のポリシー及び手順をレビュー、拡張、及び更新することが望ましい。これには、従来の識別及び認証では考慮されなかった可能性がある重要なコンポーネントのアイデンティティが含まれていることが望ましい。サプライチェーンネットワーク内のすべてのアイテムに識別を提供するには莫大なコストがかかるため、独自の裁量で行うことが望ましいことに注意する必要がある。事業体は関連する C-SCRM 戦略／実装計画、ポリシー、及び C-SCRM 計画を更新することが望ましい。

レベル：1、2、3

IA-2 識別及び認証（組織のユーザ）

補足 C-SCRM ガイダンス：事業体は、識別及び要件が定義され、ICT/OT システム又はサプライチェーンネットワークにアクセスする事業体ユーザに適用されていることを確実にすることが望ましい。事業体ユーザには、従業員、従業員と同等のステータスを持つと見なされる個人（請負業者、客員研究員など）、及び請負業者の役割を果たすシステムインテグレータなどが含まれる。「役割の期間」などの基準は、使用する識別及び認証メカニズムを定義するときに役立つ可能性がある。事業体は適切な実装を確実にするために、一連の役割を定義して認可レベルを関連付けてもよい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサ

イバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

IA-3 デバイスの識別及び認証

補足 C-SCRM ガイダンス：事業体は、サプライチェーン内のデバイス及びソフトウェアを明瞭かつ明確に識別し、識別されたらアイデンティティが真正であることを検証するケイパビリティ（能力）を実装することが望ましい。一意のデバイスごとの識別及び認証を必要とするデバイスは、種類、デバイス、又は種類とデバイスの組み合わせによって定義されることが望ましい。認証を必要とするソフトウェアは、ソフトウェアパッケージをリリースする事業体のソフトウェアパッケージの検証及び認証を可能にするソフトウェア識別タグ（SWID）によって識別されることが望ましい。

レベル：1、2、3

IA-4 識別子管理

補足 C-SCRM ガイダンス：識別子により、発見可能性及びトレーサビリティが向上する。事業体のサプライチェーン内で、システム、個人、文書、デバイス、及びコンポーネントに識別子を割り当てることが望ましい。場合によっては、識別子は概念化から廃止に至るシステムのライフサイクル全体を通じて維持されることがあるが、最低でも事業体内のシステムの耐用期間にわたって維持される。

ソフトウェア開発では、構成アイテム認識が完了したコンポーネントに識別子が割り当てられることが望ましい。デバイス及びオペレーティングシステムでは、アイテムが出荷及び受領又はダウンロードによって事業体の所有又は管理下に移転される時点など、アイテムが事業体のサプライチェーンに入る時点で識別子が割り当てられることが望ましい。

サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダは通常、サプライチェーン内での追跡のために独自の識別子を使用する。事業体はトレーサビリティ及び説明責任のために、これらの識別子を事業体が割り当てた識別子と相関付けることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation’s Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：IA-3 (1)、IA-3 (2)、IA-3 (3)、及び IA-3 (4)

拡張管理策：

(1) 識別子管理 | 組織横断的な管理

補足 C-SCRM ガイダンス：この拡張管理策は、事業体とそのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの間で識別子管理を調整することで、サプライチェーン内の要素のトレーサビリティと来歴を確保するために役立つ。これには、情報システ

ム及びコンポーネント、並びにサプライチェーン活動に関わる個人が含まれる。

レベル：1、2、3

IA-5 オーセンティケータ管理

補足 C-SCRM ガイダンス：この管理策は、サプライチェーン全体を通じたトレーサビリティと否認防止を容易にする。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) オーセンティケータ管理 | 出荷前のオーセンティケータ変更

補足 C-SCRM ガイダンス：この拡張管理策は、事業体のサプライチェーン内での過程管理を検証する。

レベル：3

(2) オーセンティケータ管理 | フェデレーションによるクレデンシャル管理

補足 C-SCRM ガイダンス：この拡張管理策は、事業体のサプライチェーン内での来歴及び過程管理を容易にする。

レベル：3

IA-8 識別及び認証（非組織のユーザ）

補足 C-SCRM ガイダンス：サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダは、サービス納入のために事業体のサプライチェーンを利用する可能性がある（開発／統合サービス、製品サポートなど）。事業体は、識別クレデンシャルの確立、監査、使用、及び取り消しと、サプライチェーン内の事業体外部ユーザの認証を管理することが望ましい。事業体はまた、インサイダー脅威により発生するリスクなどのサプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）を軽減するのに役立つように、特に取り消し管理における識別及び認証の活動を速やかに実行することを確実にすることが望ましい。

レベル：2、3

IA-9 サービスの識別及び認証

補足 C-SCRM ガイダンス：事業体は、サプライチェーン全体を通じてサービス（デジタル証明書を使用するウェブアプリケーション、労働サービスとは対照的にデータベースをクエリするサービス又はアプリケーションなど）へのアクセスのために識別及び認証が定義及び管理されていることを確実にすることが望ましい。事業体は、調達するサービスと調

達元を把握していることを確実にすることが望ましい。調達されるサービスは、事業体の検証済みサービスリストに含まれているか、又は代替管理策が導入されていることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

ファミリー：インシデント対応

[FIPS 200]では、インシデント対応の最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）適切な準備、検知、分析、封じ込め、復旧、及びユーザ対応活動を含む組織の情報システムのインシデント対応運用ケイパビリティ（能力）を確立し、（ii）インシデントを追跡、文書化し、適切な組織の担当者及び／又は権限を持つ者に報告しなければならない。

サプライチェーンの侵害は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダなどに広がることがある。事業体は、インシデントに関するどの情報を、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、その他の ICT/OT 関連のサービスプロバイダ、及び関連する省庁間組織にいつどのように報告又は共有するかなどを含めて、インシデント対応管理策が C-SCRM に対処していることを確実にすることが望ましい。インシデント対応は、インシデントがサプライチェーンに関連しているかどうかを判断するのに役立つ。

IR-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、インシデント対応のポリシー及び手順、並びに関連する C-SCRM 戦略／実装計画及びポリシーに C-SCRM を統合することが望ましい。ポリシー及び手順は、サプライチェーンを複雑化させるか又は影響を及ぼす可能性があるサプライチェーン関連インシデント及びサイバーセキュリティインシデントへの対処方法に関する方向性を提供しなければならない。特定のミッション又はシステム環境で作業する個人は、サプライチェーンのサイバーセキュリティ関連のインシデントを認識する必要がある。インシデント対応ポリシーは、脅威及びインシデントにいつどのように対処し、報告し、管理すべきかを記述していることが望ましい。

さらにこのポリシーは、サイバー脅威又はインシデントが発生した場合の FASC（連邦調達安全保障会議）及びより広範なサプライチェーン内のその他のステークホルダー又はパートナーへの伝達の時期、方法、及び担当者を定義することが望ましい。FASC が特定の供給源、対象品目、又は手順に関連する情報を要求する場合、又は供給源、対象調達、又は対象品目に関連する重大なサプライチェーンリスクがあると結論付ける合理的な根拠があると行政機関が判断した場合には、各省庁及び関係機関は FASC に対しサプライチェーンリスク情報を通知しなければならない。このような状況では、行政機関は FASC に対し、1）サプライチェーンリスクの軽減、識別、又は管理を促進するための機関の活動において識別されたサプライチェーンリスク情報、及び 2）2018 年連邦調達サプライチェーンセキュリティ法（FASCSA）41 U.S.C. § 4713 に従って機関が行った対象調達活動、及び 41 U.S.C. § 4713 に従って機関により発行されたすべての指令に関するサプライチェーンリスク情報を含む、供給源又は対象品目に関連する情報を提出する。

サプライチェーンのサイバーセキュリティインシデントのすべての関係者に通知するために、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの合意において、サプライチェーンパートナーとの双方向コミュニケーションを定義することが望ましい。インシデント情報は、必要に応じて連邦捜査局（FBI：Federal Bureau of Investigation）、米国コンピュータ

緊急対応チーム（US CERT：United States Computer Emergency Readiness Team）、及び国家サイバーセキュリティ・通信統合センター（NCCIC：National Cybersecurity and Communications Integration Center）などの事業体と共有することもできる。インシデントの重大度に応じて、サプライチェーンにおける情報伝達の加速化が必要となることがある。情報伝達、対応、是正処置、及びその他の関連活動が迅速に実施されることを確実にするために、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの間で適切な合意を得ておくことが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル 2 及びレベル 3 では、効率的で調整されたインシデント対応への取り組みを確実にするために、手順及び事業体固有のインシデント対応手法を導入しており、トレーニングが完了しており（運用セキュリティ[OPSEC]及び適切な脅威のブリーフィングをトレーニングに組み入れることを検討）、及びサプライチェーン全体で調整された情報伝達が確立されていなければならない。

レベル：1、2、3

拡張管理策：

(1) ポリシー及び手順 | *C-SCRM* インシデント情報の共有

事業体は、インシデント対応のポリシー及び手順で、サプライチェーンにおけるインシデント及びその他の重要リスク評価指標に関する情報の効果的な共有に関するガイダンスを提供することを確実にすることが望ましい。ガイダンスでは少なくとも、公共のデータリポジトリ、有料サブスクリプションサービス、社内脅威インテリジェンスチームなど多様なデータソースからのインシデント情報の収集、合成、及び配布を扱うことが望ましい。

公共部門で運営される事業体は、サイバー脅威又はインシデントの発生時に、連邦調達安全保障会議（FASC：Federal Acquisition Security Council）及びより広範なサプライチェーン内のその他のステークホルダー又はパートナーなどとの間の省庁間提携関係による情報伝達の時期及び方法に関する具体的なガイダンスを含めることが望ましい。

各省庁及び関係機関は以下の時点で FASC に対しサプライチェーンリスク情報を通知しなければならない。

1) FASC から特定の供給源又は対象品目に関連する情報を要求された場合
2) 供給源、対象調達、又は対象品目に関連する重大なサプライチェーンリスクがあると結論付ける合理的な根拠があると行政機関が判断した場合

このような状況では、行政機関は FASC に対し、以下を含む供給源又は対象品目に関する情報を提供しなければならない。

1) サプライチェーンリスクの軽減、識別、又は管理を促進するための組織の活動において識別されたサプライチェーンリスク情報

2) 2018 年連邦調達サプライチェーンセキュリティ法（FASCSA：Federal Acquisition Supply Chain Security Act of 2018）41 U.S.C. § 4713 に従って機関が行った対象調達活動、及び 41 U.S.C. § 4713 に従って機関により発行されたすべての指令に関連するサプライチェーンリスク情報

レベル：1、2、3

IR-2 インシデント対応トレーニング

補足 C-SCRM ガイダンス：事業体は、インシデント対応トレーニングに重要なサプライヤが含まれていることを確実にすることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

IR-3 インシデント対応テスト

補足 C-SCRM ガイダンス：事業体は、インシデント対応テストに重要なサプライヤが含まれ、及び／又はインシデント対応テストが重要なサプライヤに提供されていることを確実にすることが望ましい。

レベル：2、3

IR-4 インシデント対応

補足 C-SCRM ガイダンス：組織の C-SCRM インシデント対応プロセスを引き起こす可能性がある疑わしいサプライチェーンのサイバーセキュリティ事象。サプライチェーン事象の例については、附属書 G：タスク 3.4 を参照。C-SCRM 固有の補足ガイダンスは拡張管理策で提供される。

レベル：1、2、3

拡張管理策：

(1) インシデント対応 | インサイダー脅威

補足 C-SCRM ガイダンス：この拡張管理策は、インサイダー脅威への C-SCRM 情報システム、ネットワーク、及びプロセスの曝露（エクスポージャー）を制限するのに役立つ。事業体は、インサイダー脅威インシデント対応ケイパビリティ（能力）が、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの、認可境界内の ICT/OT システムにアクセスすることができる人員に関連するインサイダー脅威の可能性を明らかにすることができることを確実にすることが望ましい。

レベル：1、2、3

(2) インシデント対応 | インサイダー脅威 — 組織内連携

補足 C-SCRM ガイダンス：この拡張管理策は、インサイダー脅威への C-SCRM 情報システム、ネットワーク、及びプロセスの曝露（エクスポージャー）を制限するのに役立つ。事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが、インサイダー脅威の調整に含まれていることを確実にすることが望ましい。

レベル：1、2、3

(3) インシデント対応 | サプライチェーンとの連携

補足 C-SCRM ガイダンス：サプライチェーンセキュリティのインシデント及び対応の管理には多数の事業体が関与することがある。インシデントの初回処理及び行動方針の決定（場合によっては「行動なし」となることがある）の後に、事業体は情報伝達、インシデント対応、根本原因、及び是正処置を容易にするために、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、その他の ICT/OT 関連のサービスプロバイダ、及び関連する省庁間組織と連携する必要がある可能性がある。より包括的なインシデント対応アプローチを可能にするために、事業体は、調整された一連の主要な役割の人員を通じて情報をセキュアに共有することが望ましい。サプライチェーンのサイバーセキュリティインシデント対応をサポートすることができる成熟したケイパビリティ（能力）を持つサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダを選択することは、サプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）を削減する上で重要である。関係の性質が原因でインシデント対応の透明性が限られている場合は、一連の受け入れ可能な基準を合意（契約など）で定義する。以前のインシデントから得た教訓に基づいて、合意のレビュー（及び潜在的な改訂）を行うことが推奨される。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2

(4) インシデント対応 | 統合インシデント対応チーム

補足 C-SCRM ガイダンス：事業体は、サプライチェーンインシデントの統合インシデント対応チームの一部として、フォレンジックチーム及び／又はケイパビリティ（能力）を含めることが望ましい。関連性があり実用的な場合には、必要な地域代表者及びサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダを統合インシデント対応チームに含めることが望ましい。

レベル：3

IR-5 インシデント監視

補足 C-SCRM ガイダンス：事業体は、インシデント、対応の決定、及び活動を追跡及び文書化するための要件がサプライヤとの合意に含まれていることを確実にすることが望まし

い。

レベル：2、3

IR-6 インシデント報告

補足 C-SCRM ガイダンス：C-SCRM 固有の補足ガイダンスは拡張管理策 IR-6(3) で提供される。

レベル：3

拡張管理策：

(1) インシデント報告 | サプライチェーンとの連携

補足 C-SCRM ガイダンス：事業体からサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダへの、又はこの逆方向でのセキュリティインシデント情報の伝達を保護する必要がある。事業体は、サプライヤ及びその他の関係する省庁間組織との合意に基づいて情報がレビューされ、送信の承認を受けることを確実にすることが望ましい。この報告のエスカレーション又はこの報告からの例外はすべて、合意において明確に定義されているべきである。事業体は、インシデント報告データが伝送時に適切に保護され、承認されている個人のみがこのデータを受信することを確実にすることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：3

IR-7 インシデント対応支援

補足 C-SCRM ガイダンス：C-SCRM 固有の補足ガイダンスは拡張管理策 IR-7(2) で提供される。

レベル：3

拡張管理策：

(1) インシデント対応支援 | 外部プロバイダとの連携

補足 C-SCRM ガイダンス：事業体と一次請負業者の合意では、インシデント対応の支援を提供するために政府が承認又は指定した第三者が利用可能であるか又は必要となる条件と、このような第三者の役割及び責任が規定されているべきである。

レベル：3

IR-8 インシデント対応計画

補足 C-SCRM ガイダンス：事業体は、重要なサプライヤ、及び連邦政府の環境では省庁間パートナー及び FASC との情報共有の責任を含むインシデント対応計画を調整、策定、及び実装することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

関連管理策： IR-10

レベル：2、3

IR-9 情報流出対応

補足 C-SCRM ガイダンス：サプライチェーンは情報流出に対して脆弱である。事業体は、情報流出対応計画にサプライチェーン関連の情報流出を含めることが望ましい。これには、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの連携が必要となることがある。この連携を実施する方法の詳細を合意（契約など）に含めることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：3

関連管理策：SA-4

ファミリー：保守

[FIPS 200]では、メンテナンスの最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）組織の情報システムの定期的かつタイムリーなメンテナンスを実施し、（ii）情報システムのメンテナンスを実行するために使用するツール、技法、メカニズム、及び作業員の効果的な管理を提供しなければならない。

メンテナンスは、事業体とは別のエンティティによって実行されることがよくある。このため、メンテナンスはサプライチェーンの一部となる。メンテナンスには、更新及び交換の実施が含まれる。サプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）のアセスメント、C-SCRM 管理策の選択、それらの管理策の実装、及び管理策の有効性の監視などを含むメンテナンスの状況に、C-SCRM が適用されることが望ましい。

MA-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、事業体のすべての情報システム及びネットワークのメンテナンスに関するポリシー及び手順、並びに関連するすべての SCRM 戦略／実装計画、SCRM ポリシー、及び SCRM 計画に C-SCRM が含まれていることを確実にすることが望ましい。多くのメンテナンス契約では、ミッション、事業体、及びシステム固有の情報が、事業体とそのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの間で共有され、これにより脆弱性及び攻撃の機会をもたらしている。多くの場合、システムのメンテナンスはシステムインテグレータに外部委託されるため、適切な措置を講じなければならない。メンテナンスを外部委託していない場合でも、サプライチェーンはアップグレード、パッチ、メンテナンスの頻度、交換部品、及びシステムメンテナンスのその他の側面に影響を及ぼす。

システム及びネットワークの両方についてメンテナンスポリシーを定義することが望ましい。メンテナンスポリシーは、リモートアクセス、アクセス権限を持つメンテナンス作業員の役割及び属性、更新頻度、契約期間、更新又はメンテナンスに使用される論理的経路及び手法、及び監視と監査のメカニズムなどのリスクアセスメント（重要度分析を含む）に基づいて管理策を反映していることが望ましい。メンテナンスポリシーは、明示的に許可又は禁止されるツールを記述していることが望ましい。例えばソフトウェアメンテナンスの場合、契約にはシステム又はコンポーネントのメンテナンスに必要なソースコード、テストケース、及びアイテムへのアクセシビリティを記述することが望ましい。

メンテナンスポリシーは各レベルで改良及び拡大されることが望ましい。レベル 1 では、メンテナンス活動を含む SDLC 全体に C-SCRM を適用すべきことをポリシーで明示的に主張することが望ましい。レベル 2 では、ミッション運用のニーズと重要な機能をポリシーに反映することが望ましい。レベル 3 では、特定のシステムニーズを反映することが望ましい。非ローカルメンテナンスなどのレベル 1 での要件は、レベル 2 及びレベル 3 にフローすることが望ましい。例えば、レベル 1 で非ローカルメンテナンスが許可されていない場合、レベル 2 又はレベル 3 でも許可されないことが望ましい。

事業体は、関連する一次請負業者に該当するメンテナンスポリシー要件を伝達して、一次

請負業者がこの管理策を実装し、この要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：1、2、3

MA-2 管理されたメンテナンス

補足 C-SCRM ガイダンス：C-SCRM 固有の補足ガイダンスは拡張管理策 MA-2 (2) で提供される。

拡張管理策：

(1) 管理されたメンテナンス | 自動化されたメンテナンス措置

補足 C-SCRM ガイダンス：事業体は、サプライチェーンシステム及びネットワークに対する自動化されたメンテナンス措置がすべてメンテナンスポリシーに従って管理されていることを確実にすることが望ましい。自動化されたメンテナンス措置の例には、COTS 製品パッチ更新、障害通知フィードバックを備えたコールホーム機能などがある。これらの措置を管理するには、必要に応じて調査又はフィルタリングを提供する適切なサポートメカニズムを使用してステージングプロセスを確立する必要がある場合がある。重要なシステム及びコンポーネントの場合、ステージングプロセスは特に重要である可能性がある。

レベル：3

MA-3 メンテナンスツール

補足 C-SCRM ガイダンス：メンテナンスツールはサプライチェーンの一部として見なされる。メンテナンスツールにはそれ自体のサプライチェーンもある。メンテナンスツールを選択、注文、保管、及び統合するときを含め、事業体がメンテナンスツールを取得又はアップグレードするときには（開発環境又はテストツールの更新など）、C-SCRM を統合することが望ましい。事業体は、外部サービスプロバイダが使用しているメンテナンスツールを含め、メンテナンスツールの継続的なレビュー及び承認を行うことが望ましい。事業体はまた、メンテナンスツールの交換部品を評価するときに C-SCRM を統合することが望ましい。この管理策は、政府機関がメンテナンスツールの取得、運用、及び監督をどのように扱うかに応じて、レベル 2 及び レベル 3 の両方で実行されることがある。

レベル：2、3

拡張管理策：

(1) メンテナンスツール | ツールの検査

補足 C-SCRM ガイダンス：事業体は、ICT サプライチェーンインフラストラクチャのメンテナンスツールが期待どおりであることを検証するために、受け入れテストを展開することが望ましい。メンテナンスツールは、適切な書類手続きにより認可され、初回の検証で主張されているとおりであることが検証され、脆弱性、適切なセキュリティ構成、及び記述されている機能についてのテストが行われることが望ましい。

レベル：3

(2) メンテナンスツール | 媒体の検査

補足 C-SCRM ガイダンス：事業体は、サプライヤが事業体の情報システムに対して使用する診断及びテストプログラムが含まれている媒体が、期待どおりに動作し、必要な機能のみを提供することを検証することが望ましい。メンテナンスツールからの媒体の使用は、事業体のポリシー及び手順に整合しており、事前に承認されていることが望ましい。事業体は、機能性が、合意されている機能性を超えていないことを確実にすることが望ましい。

レベル：3

(3) メンテナンスツール | 認可されていない移動の防止

補足 C-SCRM ガイダンス：サプライチェーンからのシステム及びネットワークメンテナンスツールの認可されていない移動は、事業体による制御が及ばない場所にツールがある場合に、改ざん、偽造品への交換、マルウェア混入などのサプライチェーンリスクをもたらす可能性がある。システム及びネットワークメンテナンスツールには、統合開発環境（IDE）、テスト、又は脆弱性スキャン機能などが含まれる可能性がある。C-SCRM では、事業体がメンテナンスツールの移動を明示的に認可、追跡、及び監査することが重要である。システム及びネットワークツールは、事業体／情報システムへのアクセスが許可された後でも引き続きシステム所有者の財産／資産であり、移動され事業体内の別の場所で使用される場合は追跡することが望ましい。現在使用されているか又は保管されている ICT メンテナンスツールは移動のための適切な調査が完了するまでは、事業体の施設から移動することを許可されるべきではない（すなわち、メンテナンスツールの移動は、移動について認可されている範囲を超えるべきではなく、事業体で確立されているポリシー及び手順に従って実施すべきである）。

レベル：3

MA-4 非ローカルメンテナンス

補足 C-SCRM ガイダンス：請負業者の人員によって非ローカルメンテナンスが提供される可能性がある。関連するリスクを管理するために、適切な保護策を導入することが望ましい。内部メンテナンス作業員に適用される管理策は、同様のメンテナンス役割を果たすすべてのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダにも適用され、外部サービスプロバイダとの契約上の合意を通じて施行される。

レベル：2、3

拡張管理策：

(1) 非ローカルメンテナンス | 同等のセキュリティ及びサニタイズ

補足 C-SCRM ガイダンス：サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダがシステ

ム又はシステムコンポーネントに対して非ローカルメンテナンス又は診断サービスを実行する場合、事業体は以下を確実にすることが望ましい。

- 非ローカル環境が事業体及びベンダ間の合意に基づいてメンテナンス及び診断の適切なセキュリティレベルを満たしていることを検証するために適切な措置が講じられている。
- コンポーネントに含まれている事業体固有のデータをすべて削除するために適切なレベルのサニタイズが完了している。
- コンポーネントがサニタイズされていることを確実にするために適切な診断が完了しており、事業体システム又はサプライチェーンネットワークに戻す前に悪意のある混入が行われることが防止される。

事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

MA-5 メンテナンス作業員

補足 C-SCRM ガイダンス：メンテナンス作業員は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダによって雇用されていることがある。したがって、関連するリスクを管理するために適切な保護策を導入することが望ましい。内部メンテナンス作業員に適用される管理策が、同様のメンテナンス役割を果たす請負業者の作業員にも適用され、また外部サービスプロバイダとの契約上の合意を通じて実施されるべきである。

レベル：2、3

拡張管理策：

(1) メンテナンス作業員 | 外国人

補足 C-SCRM ガイダンス：重要な非国家安全保障システム／サービスにアクセスする外国人の調査では C-SCRM を考慮しなければならず、またこの調査は関連するすべての請負業者の作業員まで拡大されなければならない。事業体は、外国人に関連するすべての制限又は調査要件を合意で規定し、この要件を関連する二次請負業者にフローダウンすることが望ましい。

レベル：2、3

MA-6 タイムリーなメンテナンス

補足 C-SCRM ガイダンス：事業体は、予備部品、交換部品、又は代替ソースを相手先ブランド製造業者（OEM）、認可されている販売代理事業者、又は認可されている再販業者から購入し、適切なリードタイムを確実にすることが望ましい。OEM を利用できない場合は、認可されている販売代理事業者から取得することが望ましい。OEM 又は認可されている販売代理事業者を利用できない場合は、認可されている再販業者から取得することが望ましい。事業体は、販売代理事業者又は再販業者が認可されているかどうかの検証を得ることが望ましい。可能であれば、事業体は認可されている販売代理事業者／販売業

者承認リストを使用することが望ましい。唯一の代替策が、認可されていない販売代理事業者又は非公式市場からの購入である場合、使用すべき追加リスク軽減策を識別するための重要度及び脅威分析の再確認を含む、リスクアセスメントを実行することが望ましい。例えば、事業体は供給源を調査し、偽造品、不適切な行為、又は犯罪歴がないことを確認することが望ましい。重要度及び脅威分析の詳細については、第 2 節を参照。事業体は、重要な OEM 部品の取得を必要な時間枠内で完了できない可能性がある場合、可能であればその部品のベンチストックを確保しておくことが望ましい。

レベル：3

MA-7 フィールドメンテナンス

補足 C-SCRM ガイダンス：事業体は、厳格さと品質管理のさらなるチェックが必要な場合、現実的又は可能であれば、信頼できる施設を使用することが望ましい。信頼できる施設は、承認リストに記載されており、追加の管理策が導入されていることが望ましい。

関連管理策：MA-2、MA-4、MA-5

レベル：3

MA-8 メンテナンス監視及び情報共有（新規）

管理策：事業体は、システム及びコンポーネントの状況を監視し、範囲外及び規格外のパフォーマンスをサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダに伝達する。事業体は、この情報を政府・業界間データ交換プログラム（GIDEP：Government-Industry Data Exchange Program）にも報告することが望ましい。

補足 C-SCRM ガイダンス：コンポーネントの故障率を追跡すると、取得者が緊急時対応、代替供給源、及び交換に関する計画を策定するのに役立つ有用な情報が提供される。故障率は、システム及びコンポーネントの品質及び信頼性を監視するときにも役立つ。この情報から、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダに、是正処置及び継続的改善に関する有用なフィードバックが提供される。レベル 2 では、政府機関が故障率を追跡してサプライヤ（OEM及び／又は認可された販売代理事業者）に伝達することが望ましい。故障率と、根本原因などの故障を示している可能性がある問題は、レベル 3 で事業体の技術人員（開発者、管理者、又はメンテナンスエンジニアなど）によって識別され、レベル 2 へ伝達されることが望ましい。これらの人員は、問題を検証し、技術的代替策を識別することができる。

関連管理策： IR-4(10)

レベル：3

ファミリー：媒体保護

[FIPS 200]では、媒体保護の最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）紙媒体及び電子媒体の両方の情報システム媒体を保護し、（ii）情報システム媒体上の情報へのアクセスを認可されているユーザのみに制限し、（iii）情報システム媒体を廃棄又は再利用のためにリリースする前に、その媒体をサニタイズ又は破棄しなければならない。

媒体自体が、サプライチェーンを移動するか、又は事業体のサプライチェーンに関する情報を格納しているコンポーネントであることがある。これには、紙媒体又は電子ファイルのシステム文書、取得者情報が含まれている出荷及び納入文書、ソフトウェアコードが含まれているメモリスティック、又は永続媒体が組み込まれている完全なルータ又はサーバなど、物理的及び論理的媒体の両方が含まれる。媒体に含まれる情報は機密情報であることがある。また、媒体は概念化から廃棄まで SDLC 全体にわたって使用される。事業体は、媒体保護管理策が事業体の媒体、及びサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダから受け取った媒体の両方に適用されていることを確実にすることが望ましい。

MP-1 ポリシー及び手順

> 補足 C-SCRM ガイダンス：サプライチェーン全体を通じて、各種の物理的及び電子的媒体に関する様々な文書と情報が配布される。この情報には、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダからの様々な機密情報や知的財産が含まれている可能性があるため、適切に保護されることが望ましい。また、媒体保護のポリシー及び手順は、事業体のサプライチェーン及び SDLC 全体における媒体を含め、サプライチェーンの懸念事項に対処することが望ましい。
>
> レベル：1、2

MP-4 媒体保管

> 補足 C-SCRM ガイダンス：媒体保管管理策には C-SCRM 活動が含まれることが望ましい。事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの媒体保管要件（暗号化など）を規定し、合意（契約文言など）に含めることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。
>
> レベル：1、2

MP-5 媒体移送

> 補足 C-SCRM ガイダンス：事業体は、媒体が事業体又は事業体外部の人員により移送されるときに C-SCRM 活動を組み入れることが望ましい。移送及び保管時に媒体を保護する技法には、暗号化技法や承認済み管理人サービスなどがある。

レベル：1、2

MP-6　媒体のサニタイズ

補足 C-SCRM ガイダンス：事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの媒体のサニタイズポリシーを規定し、合意（契約文言など）に含めることが望ましい。媒体は SDLC 全体を通じて使用される。サプライチェーンを移動又はサプライチェーンに存在する媒体の出所は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダなど、あらゆる場所である可能性がある。媒体は、新規であるか、修復されたものか、又は再利用されているものである可能性がある。媒体のサニタイズは、媒体を使用、再利用、又は廃棄する前に情報が削除されていることを確実にする上で重要である。プライバシー情報又はその他の機密情報（CUI など）が含まれている媒体については、事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

関連管理策：MP-6(1)、MP-6(2)、MP-6(3)、MP-6(7)、MP-6(8)

ファミリー：物理的及び環境的保護

[FIPS 200]では、物理的及び環境的保護の最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）情報システム、機器、及び該当する運用環境への物理的アクセスを認可されている個人に制限し、（ii）物理的プラントを保護し、情報システムのインフラをサポートし、（iii）情報システムにサポートユーティリティを提供し、（iv）情報システムを環境的ハザードから保護し、（v）情報システムを含む施設で適切な環境管理策を提供しなければならない。

サプライチェーンは物理的環境及び論理的環境にわたっている。物理的要因には、サプライチェーン内の個人又は事業体間でのある場所から別の場所へのサイバーコンポーネント（又はデバイス）の輸送に影響する可能性がある天候及び道路状況が含まれる。C-SCRM リスクマネジメントプロセスの一環として物理的及び環境的リスクに適切に対処しない場合、これらのリスクは、事業体が重要なコンポーネントをタイムリーに受領することができる能力に悪影響を与え、そこからさらにミッション運用を実行することができる能力に影響を与える可能性がある。事業体は、サプライチェーン内に適切な物理的及び環境的管理策を実装することを要件とすることが望ましい。

PE-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、独自の物理的及び環境的保護のポリシー及び手順に C-SCRM プラクティス及び要件を統合することが望ましい。保護の度合いは、統合の度合いに対応していることが望ましい。物理的及び環境的保護ポリシーは、サプライチェーンの物理的インタフェースに適切な保護が導入されており、このような保護の監査が行われることを確実にすることが望ましい。

レベル：1、2、3

PE-2 物理的アクセス認可

補足 C-SCRM ガイダンス：事業体は、認可されていて物理的アクセスを必要とする個人だけが、情報、システム、又はデータセンター（機密など）にアクセスすることができることを確実にすることが望ましい。このような認可では、個人がその物理アクセスに関連して実行が許可される動作と許可されない動作（表示、変更／構成、何かの挿入、何かの接続、削除など）が規定されることが望ましい。合意では物理的アクセス認可の要件が扱われることが望ましく、また事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。非政府職員に対する認可は、認可の文書化を含み、このような認可に関連するすべての前提条件又は制約条件（個人は政府職員によって案内される必要がある、個人はバッチを付けなければならない、個人は通常の営業時間内での物理アクセスが許可されるなど）を規定する承認済みの手続きに従って行われることが望ましい。

レベル：2、3

拡張管理策：

(1) 物理的アクセス認可 | 職位又は役割によるアクセス

補足 C-SCRM ガイダンス：役割に基づく物理的アクセスの認可には、連邦政府機関職員（政府機関／省庁の職員など）及び非連邦政府機関職員（サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダなど）を含めることが望ましい。役割ベースの認可を使用する場合、その役割又は職位に対して許可されるアクセスの種類及びレベルは事前に確立されて文書化されていなければならない。

レベル：2、3

PE-3 物理的アクセス制御

補足 C-SCRM ガイダンス：物理的アクセス制御には、事業体のサプライチェーンに関わる個人及び事業体が含まれることが望ましい。サプライチェーンインフラストラクチャ及び関連するすべての要素へのアクセスを付与する前に、事業体が定義した要件及びポリシーに基づく調査プロセスを導入することが望ましい。アクセスの確立、メンテナンス、及び取り消しプロセスは、事業体のアクセス制御ポリシーに厳格に対応していることが望ましい。事業体所有又は外部サービスプロバイダ所有の物理的な施設及びデータセンターにアクセスする必要があるサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダに対する取り消しの速さは、各自の契約で実行される活動に応じて管理されることが望ましい。個人又は事業体のニーズがなくなった場合には、迅速な取り消しが重要である。

レベル：2、3

拡張管理策：

(1) 物理的アクセス制御 | システムアクセス

補足 C-SCRM ガイダンス：物理的アクセス制御は、請負業者の人員まで拡大されることが望ましい。サプライチェーンインフラストラクチャ及び関連するすべての要素への物理的アクセスをサポートするサービスを提供する請負業者リソースはすべて、アクセス制御に準拠することが望ましい。ポリシー及び手順は、類似する物理アクセスレベルの従業員に適用されているポリシー及び手順と整合していることが望ましい。

レベル：2、3

(2) 物理的アクセス制御 | 施設及びシステム

補足 C-SCRM ガイダンス：施設のセキュリティチェックの範囲、頻度、及び／又はランダム性を決定する際は、事業体は秘密聴取機器から生じる漏出リスクに対する説明責任を負うことが望ましい。このような機器には、盗聴器、ロービングバグ、偽装携帯電話基地局、及び機密情報を事業体の外部に転送することができるその他の傍受技術が含まれる。

レベル：2、3

(3) 物理的アクセス制御 | タンパー保護

補足 C-SCRM ガイダンス：タンパー保護は、製品のサイバーセキュリティリスクを低減する上で重要である。事業体は、妥当性確認済みのタンパー保護技術をサプライチェーン内に実装することが望ましい。重要な製品の場合、事業体はサプライヤがタンパー保護メカニズムを実装しているかどうか、及び実装している場合はどの程度まで実装しているかを要件にし、アセスメントすることが望ましい。このアセスメントには、サプライヤの上流サプライチェーンエンティティにこのようなメカニズムが必要であるかどうか、及びどのように適用されているかを含めることもできる。

レベル：2、3

PE-6 物理的アクセスの監視

補足 C-SCRM ガイダンス：サプライチェーン経由を含め、事業体又は外部サービスプロバイダの施設、データセンター、情報、及び物理的資産に物理的にアクセスする個人は、事業体の従業員、オンサイト又は遠隔地の請負業者、訪問者、その他の第三者（請負業者の事業体と契約しているメンテナンス作業員など）、又は上流サプライチェーンの事業体に在籍する個人である可能性がある。事業体は、サプライチェーン全体のサイバーセキュリティリスクを低減するためにこのような個人の活動を監視するか、又は合意において監視することを要件とすることが望ましい。

レベル：1、2、3

PE-16 搬入及び搬出

補足 C-SCRM ガイダンス：この拡張管理策は、事業体の情報システム又はサプライチェーンからのハードウェアコンポーネントの物理的な搬入及び搬出時に発生するサイバーセキュリティリスクを低減する。これには、移送時のセキュリティ、搬入されるコンポーネントの妥当性確認、及びサニタイズ手順の検証などが含まれる。リスクに基づく考慮事項には、コンポーネントのミッションにおける重要度、及び開発、運用、又はメンテナンス環境（機密の統合及びテストラボなど）などがある。

レベル：3

PE-17 代替作業サイト

補足 C-SCRM ガイダンス：事業体は、サプライチェーンインフラストラクチャ内にいるか又は代替作業サイトを使用してサプライチェーンインフラストラクチャにアクセスしている事業体の従業員又は請負業者の人員に関連するサイバーセキュリティリスクからの保護を組み入れることが望ましい。これには、代替作業サイトからも作業する可能性がある第三者の人員が含まれることがある。

レベル：3

PE-18 システムコンポーネントの設置場所

補足 C-SCRM ガイダンス：物理的及び環境的ハザード又は中断は、取得されて事業体の設置場所に物理的に移送された製品、又はその予定がある製品の可用性に影響する。例えば事業体は、政府機関の業務にとって重要な情報システムコンポーネントの代替サプライヤの計画を策定するときに、これらの情報システムコンポーネントの製造、保管、又は配送先の場所を組み入れることが望ましい。

レベル：1、2、3

関連管理策：CP-6、CP-7

PE-20 資産の監視及び追跡

補足 C-SCRM ガイダンス：事業体は、可能かつ現実的である場合には常に、資産位置情報技術を使用して、サプライチェーンのエンティティ間及び保護領域間で移送されるシステム及びコンポーネント、若しくは実装、テスト、メンテナンス、又は廃棄のための待機保管所にあるシステム及びコンポーネントを追跡することが望ましい。手法には RFID、デジタル署名、又はブロックチェーンなどが含まれる。これらの技術は、以下に対する保護に役立つ。

a. 偽造品に交換するためのシステム又はコンポーネントの流用
b. システム又はコンポーネントの機能及びデータ（コンポーネント内に含まれているデータ及びコンポーネントに関するデータを含む）の機密性、完全性、又は可用性の損失

c. 重要なコンポーネントのサプライチェーン及びロジスティクスプロセスの中断資産位置情報技術は、保護ケイパビリティ（能力）を提供する他に、インシデント管理に使用することができるデータを収集するのに役立つ。

レベル：2、3

PE-23 施設の場所

補足 C-SCRM ガイダンス：事業体は、サプライヤに関連するリスクをアセスメントするときに施設の場所（データセンターなど）を組み込むことが望ましい。要因には、地理的位置（米国本土［CONUS］、米国本土外［OCONUS］など）、1 つ以上の関連施設に導入されている物理的保護、このような施設のローカル管理及び制御、潜在的な環境的ハザード（高リスク地震帯に位置しているなど）、及び代替施設の場所などが含まれる。事業体は、製造又は配送センターの場所が地政学的、経済的、又はその他の要因による影響を受ける可能性があるかどうかについてもアセスメントすることが望ましい。重要なベンダ又は製品の場合、事業体はベンダ（又は上流のサプライチェーンプロバイダ）の施設の場所に関する要件又は制限を契約に具体的に記載し、この要件を関連する二次請負業者にフローダウンすることが望ましい。

レベル：2、3

関連管理策：SA-9(8)

ファミリー：計画

[FIPS 200]では、計画の最小限のセキュリティ要件を以下のように規定している。

> 組織は、情報システムに対して導入されているか又は予定されているセキュリティ管理策と、情報システムにアクセスする個人の行動規則を記述する、組織の情報システムのセキュリティ計画の策定、文書化、定期的な更新、及び実装を行わなければならない。

C-SCRM は、セキュリティアーキテクチャ、他の事業体エンティティとの連携、及びシステムセキュリティ計画の策定などの活動を含め、セキュリティ計画に影響を与えることが望ましい。サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダから製品及びサービスを取得するときには、事業体はこれらの事業体と施設を共有するか、事業体の施設にこれらのエンティティの従業員を配置するか、又はこれらのエンティティに属する情報システムを使用することがある。このような状況及びその他の該当する状況では、事業体のプロセス、情報システム、及びサプライチェーンを移動するシステム及びコンポーネントを適切かつ確実に保護することを確実にするために、事業体はこれらのエンティティと共にそのセキュリティ計画策定活動を調整することが望ましい。事業体はセキュリティアーキテクチャを確立する際に、事業撤退するサプライヤ又は特定コンポーネントの製造を停止するサプライヤを含めるために、サプライチェーン全体のサイバーセキュリティリスクを管理するときにコンポーネント及びサプライヤの多様性を確保することが望ましい。最後に、第 2 節及び附属書 C に記述するように、事業体は C-SCRM 管理策をリスク対応フレームワーク（レベル 1 及びレベル 2）と C-SCRM 計画（レベル 3）に統合することが望ましい。

PL-1 ポリシー及び手順

補足 C-SCRM ガイダンス：セキュリティ計画のポリシー及び手順は C-SCRM を統合することが望ましい。これには、取得又は開発の要件と、その後のシステム、システムインタフェース、及びネットワーク接続の実装、運用、及びメンテナンスを形成するための C-SCRM のセキュリティポリシー、運用ポリシー、及び手順を作成、配布、及び更新することが含まれる。C-SCRM ポリシー及び手順は、レベル 1 での C-SCRM 戦略及び実装計画とレベル 3 でのシステムセキュリティ計画及び C-SCRM 計画へのインプットを提供し、これらの計画からガイダンスを得る。レベル 3 では、C-SCRM の観点から SDLC 全体が対象とされていることを確実にする。

レベル：2

関連管理策：PL-2、PM-30

PL-2 システムセキュリティ及びプライバシー計画

補足 C-SCRM ガイダンス：システムセキュリティ計画（SSP）は C-SCRM を統合することが望ましい。事業体は、個々のシステムに対して独立した C-SCRM 計画を策定し、その SSP に SCRM 管理策を統合してもよい。システムセキュリティ計画及び／又はシステムレベルの C-SCRM 計画は、レベル 1 での C-SCRM 戦略及び実装計画と、レベル 1 及びレベル 2 での C-SCRM ポリシーへのインプットを提供し、これらの計画及びポリシー

からガイダンスを得る。内部調整の他に、事業体は SSP を策定及び維持するために、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと連携することが望ましい。例えば、システムを構築及び運用する際には、事業体とシステムインテグレータの人員の間で大規模な連携及び協力が必要となる。このような連携及び協力は、システムセキュリティ計画又は独立した C-SCRM 計画で扱うことが望ましい。これらの計画ではまた、サプライヤ又は外部サービスプロバイダが取得者の要件をカスタマイズできないようにすることを検討すべきである。サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダも、連邦政府機関の情報を処理する非連邦政府（すなわち、請負業者の）システムに対する C-SCRM 計画を策定し、この要件を関連する二次請負業者にフローダウンすることが推奨される。

第 2 節、附属書 C、及び附属書 D は、C-SCRM 戦略、ポリシー、及び計画のガイダンスを提供する。本出版物（NIST SP 800-161, Rev. 1）は、SSP の C-SCRM の部分に使用することが望ましい。

レベル：3

関連管理策：PM-30

PL-4 行動規則

補足 C-SCRM ガイダンス：行動規則は、請負業者の人員及び内部政府機関職員に適用される。請負業者の事業体は、従業員が該当する行動規則を順守することを確実にする責任を負う。個々の請負業者がこの管理策を理解し、この管理策に準拠していることを実証するまでは、これらの請負業者に対して政府機関のシステム又はデータへのアクセスを付与するべきではない。この管理策に準拠できないと、このような個人からアクセス権が削除されることがある。

レベル：2、3

PL-7 業務構想文書

補足 C-SCRM ガイダンス：業務構想文書（CONOPS）には、事業体が C-SCRM の観点からどのようにシステムを運用する意図があるかについて記述されていることが望ましい。サプライチェーン全体のサイバーセキュリティリスクに対処するために、C-SCRM を統合し、該当するシステムの SDLC 全体を通じて管理及び更新されることが望ましい。

レベル：3

PL-8 セキュリティ及びプライバシーアーキテクチャ

補足 C-SCRM ガイダンス：セキュリティ及びプライバシーアーキテクチャは、基盤となるシステム及びネットワークと作成されている情報システムに対するセキュリティ及びプライバシー保護の手法、メカニズム、及びケイパビリティ（能力）の実装を定義し、方向付ける。セキュリティアーキテクチャは、SDLC 全体を通じてセキュリティが組み込まれていることを確実にすることができるため、C-SCRM にとって不可欠である。事業体は、

ゼロトラストアーキテクチャの実装を検討し、またシステム開発者／エンジニア及びシステムセキュリティエンジニアがセキュリティアーキテクチャを十分に理解していることを確実にすることが望ましい。この管理策は連邦政府機関の従業員と非連邦政府機関の従業員の両方に適用される。

レベル：2、3

拡張管理策：

(1) セキュリティ及びプライバシーアーキテクチャ | サプライヤの多様性

補足 C-SCRM ガイダンス：サプライヤの多様性により、情報セキュリティ及びサプライチェーンの懸念に対処するための選択肢が提供される。この管理策は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダに関連しているため、事業体はこの管理策を組み入れることが望ましい。

事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、又はその他の ICT/OT 関連のサービスプロバイダが事業体の要件を満たすことができなくなった場合（企業が倒産した、又は契約上の義務を果たさなくなった場合など）に備えて、これらの代替候補を計画しておくことが望ましい。該当する場合には、特定の事象（陳腐化、低パフォーマンス、製造の問題など）の発生時に、各種部品を異なる製造業者の類似価格の類似モデルに交換することができることを契約文言として規定しておくことが望ましい。

取得セキュリティアセスメントにおいて既製品（商用又は政府調達向け）コンポーネントのサプライヤの多様性を組み入れる。代替サプライヤの評価には、例えば機能パリティ、相互運用性、コモディティコンポーネント、及び複数の納入経路を提供することができる能力が含まれることが望ましい。例えば、ソフトウェアコンポーネントのソースコード、ビルドスクリプト、及びテストを所有している場合、事業体は必要に応じてソフトウェアコンポーネントのメンテナンスを他者に割り当てることができる可能性がある。

レベル：2、3

PL-9 一元管理

補足 C-SCRM ガイダンス：C-SCRM 管理策は、レベル 1 では C-SCRM 戦略及び実装計画を通じて、またレベル 1 及び レベル 2 では C-SCRM ポリシーを通じて一元的に管理される。第 2 節で説明した C-SCRM PMO は、レベル 1 及びレベル 2 で C-SCRM 管理策を一元管理する。レベル 3 では、C-SCRM 管理策は SSP 及び／又は C-SCRM 計画を通じて情報システムベースで管理される。

レベル：1、2

PL-10 ベースラインの選択

補足 C-SCRM ガイダンス：事業体は、管理策ベースラインに C-SCRM 管理策を含めることが望ましい。事業体は、各レベルで識別される C-SCRM 要件に基づいて C-SCRM 管理策を識別及び選択することが望ましい。C-SCRM PMO は、様々なグループ、対象コミュニティ、又は事業体全体の共通する C-SCRM 要件を満たす C-SCRM 管理策ベースラインの識別を支援することができる。

レベル：1、2

ファミリー：プログラムマネジメント

[FIPS 200]では、プログラムマネジメントの最小セキュリティ要件を規定していない。

[NIST SP 800-53, Rev.5]では、「プログラムマネジメント管理策は ... 組織レベルで実装されるもので、個々の情報システムに向けられたものではない。」と記述されている。これらの管理策は事業体全体（すなわち、連邦政府機関）に適用され、事業体の包括的な情報セキュリティプログラムをサポートする。プログラムマネジメント管理策は、事業体全体の C-SCRM 活動をサポートし、これらの活動にインプット及びフィードバックを提供する。

すべてのプログラムマネジメント管理策は C-SCRM のコンテキストで適用されることが望ましい。連邦政府機関内では、C-SCRM PMO 機能又は類似の機能がプログラムマネジメント管理策の実装の責任を負う。第 3 節では、C-SCRM PMO 及びその機能と責任に関するガイダンスを提供している。

PM-2 情報セキュリティプログラムの責任者の役割

補足 C-SCRM ガイダンス：情報セキュリティ責任者（CISO など）及び政府機関の取得担当責任者（最高取得責任者[CAO]又は調達担当責任者[SPE]など）は、C-SCRM と、事業体内の CIO、施設／物理セキュリティ責任者、及びリスク管理者（機能）などの他の該当する上級人員との事業体横断的な連携及び協力の責任を負う。この連携は、特定の各省庁及び関係機関の事業体構造及び関連する上級人員の特定の職位に関係なく行われることが望ましい。この連携は、C-SCRM PMO 又はその他の類似する機能によって実施される可能性がある。第 2 節で、C-SCRM の役割及び責任に関する詳細なガイダンスを提供している。

レベル：1、2

PM-3 情報セキュリティ及びプライバシーリソース

補足 C-SCRM ガイダンス：政府機関の C-SCRM 要件の実装を成功させるには、事業体の C-SCRM プログラムに、専用の持続した資金提供及び人材が必要である。本出版物の第 3 節では、C-SCRM プログラムへの専用資金提供に関するガイダンスを提供している。事業体はまた、資金計画及び投資要求プロセスによって資金が適切に割り振られることを確実にするために、C-SCRM 要件を大規模な IT 投資に統合することが望ましい。例えば、C-SCRM を拡張して事業体のサプライチェーンのインベントリ又はロジスティクス管理の効率性を確保及び改善するために、RFID インフラストラクチャが必要である場合には、計画及び実装を成功させることを確実にするために適切な IT 投資が必要となる可能性がある。他の例としては、重要なコンポーネントの開発又はテスト環境への投資などがある。この場合、このミッションをサポートする特定の C-SCRM 要件を満たすための適切な情報システム、ネットワーク、及びコンポーネントを取得及び保守するために資金提供及びリソースが必要となる。

レベル：1、2

PM-4 行動計画及びマイルストーンプロセス

補足 C-SCRM ガイダンス：C-SCRM の項目をすべてのレベルで POA&M に含めることが望ましい。組織は C-SCRM アセスメント報告書に基づいて POA&M を策定することが望ましい。POA&M は、アセスメントで識別された C-SCRM 管理策の欠陥に対して計画された是正処置と、これらの措置の進捗状況の継続的監視を文書化する目的で、組織が使用することが望ましい。

レベル：2、3

関連管理策：CA-5、PM-30

PM-5 システムインベントリ

補足 C-SCRM ガイダンス：最新のシステムインベントリを維持することは、C-SCRM の基本である。システムインベントリがない場合、事業体はシステム及びサプライヤの重要度を識別できなくなる可能性があり、これによって C-SCRM 活動を実行できなくなる可能性がある。該当するすべてのサプライヤが識別され、重大度で分類化されことを確実にするには、事業体は関連するサプライヤの情報をシステムインベントリに含め、インベントリを最新かつ正確に維持することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

PM-6 パフォーマンス尺度

補足 C-SCRM ガイダンス：事業体は、C-SCRM 活動の実装、効率性、有効性、及び影響を追跡するために、パフォーマンス尺度を使用することが望ましい。C-SCRM PMO は、適切な対象読者及び意思決定者の識別と、データ収集、分析、及び報告のガイダンスの提供を含めるために、他の該当するステークホルダーと協力して C-SCRM のパフォーマンス尺度を作成する責任を負う。

レベル：1、2

PM-7 エンタープライズアーキテクチャ

補足 C-SCRM ガイダンス：エンタープライズアーキテクチャを設計及び維持する際に C-SCRM を統合することが望ましい。

レベル：1、2

PM-8 重要インフラ計画

補足 C-SCRM ガイダンス：重要インフラ計画を策定及び維持する際に C-SCRM を統合することが望ましい。

レベル：1

PM-9 リスクマネジメント戦略

補足 C-SCRM ガイダンス：リスクマネジメント戦略では、サプライチェーン全体のサイバーセキュリティリスクに対処することが望ましい。本出版物の第 2 節、附属書 C、及び附属書 D では、リスクマネジメント戦略への C-SCRM の統合に関するガイダンスを提供している。

レベル：1

PM-10 認可プロセス

補足 C-SCRM ガイダンス：認可プロセスを設計及び実装する際に C-SCRM を統合することが望ましい。

レベル：1、2

PM-11 ミッション及び事業プロセスの規定

補足 C-SCRM ガイダンス：事業体のミッション及びビジネスプロセスでは、サプライチェーン全体のサイバーセキュリティリスクに対処することが望ましい。事業体は、ミッション及びビジネスプロセスの定義に対処するときには、ミッション成功のためのサポートプロセスに C-SCRM 活動が組み入れられていることを確実にすることが望ましい。例えば、コンポーネントが故障した場合に容易に取り外し及び交換することができるように設計及び実装された重要なミッション機能をサポートするシステムで、多少信頼できないハードウェアコンポーネントを使用する必要があることがある。交換が必要となった場合にサプライヤがコンポーネントの予備部品を準備して利用可能にすることを確実にするために、C-SCRM 活動を定義する必要がある。

レベル：1、2、3

PM-12 インサイダー脅威対策プログラム

補足 C-SCRM ガイダンス：インサイダー脅威対策プログラムは C-SCRM を含んでおり、政府機関のシステム及びネットワークにアクセスすることができる連邦政府機関及び非連邦政府機関の個人に合わせてテーラリングすることが望ましい。この管理策は請負業者及び二次請負業者に適用され、SDLC 全体を通じて実装されることが望ましい。

レベル：1、2、3

PM-13 セキュリティ及びプライバシー要員

補足 C-SCRM ガイダンス：セキュリティ及びプライバシー要員の策定及び改善により、関連する C-SCRM トピックが、プログラムによって作成されたコンテンツ及びイニシアチブに統合されることを確実にすることが望ましい。第 2 節で、C-SCRM の役割及び責任に関する情報を提供している。NIST SP 800-161 を、セキュリティ及びプライバシー要員プログラムに含めるトピック及び活動の情報源として使用することができる。

レベル：1、2

PM-14 テスト、トレーニング、及び監視

補足 C-SCRM ガイダンス：事業体は、組織のシステムに関連するサプライチェーンリスクのテスト、トレーニング、及び監視活動の実施に関する組織の計画が維持されることを確実にするプロセスを実装することが望ましい。C-SCRM PMO は、C-SCRM をテスト、トレーニング、及び監視計画に統合する方法に関するガイダンスとサポートを提供することができる。

レベル：1、2

PM-15 セキュリティ及びプライバシーのグループ及び団体

補足 C-SCRM ガイダンス：セキュリティ及びプライバシーのグループ及び団体との接点には、C-SCRM 実践者及び C-SCRM の責任を負う人員を含めることが望ましい。取得、法務、重要インフラ、及びサプライチェーンの各グループ及び団体を組み入れることが望ましい。C-SCRM PMO は、参加することでメリットを得る可能性がある政府機関の人員、参加する特定のグループ、及び関連トピックを識別するのに役立てることができる。

レベル：1、2

PM-16 脅威認識プログラム

補足 C-SCRM ガイダンス：脅威認識プログラムには、サプライチェーンから発生した脅威を含むことが望ましい。サプライチェーン脅威の認識に対処するときには、事業体の情報共有ポリシーの境界内のステークホルダー間で知識が共有されることが望ましい。C-SCRM PMO は、脅威情報の共有に含める C-SCRM ステークホルダーと、サプライチェーン脅威の潜在的な情報源を識別するのに役立てることができる。

レベル：1、2

PM-17 外部システム上の管理対象非機密情報の保護

補足 C-SCRM ガイダンス：外部システム上の管理対象非機密情報（CUI）に関するポリシー及び手順には、関連するサプライチェーン情報の保護が含まれていることが望ましい。逆に、外部システムは政府機関のサプライチェーンの一部であるため、これには外部システムに存在する政府機関情報の保護が含まれていることが望ましい。

レベル：2

PM-18 プライバシープログラム計画

補足 C-SCRM ガイダンス：プライバシープログラム計画には C-SCRM が含まれていることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：1、2

PM-19 プライバシープログラムの責任者の役割

補足 C-SCRM ガイダンス：プライバシープログラムの責任者の役割は、該当する C-SCRM イニシアチブ及び活動にステークホルダーとして含まれることが望ましい。

レベル：1

PM-20 プライバシープログラム情報の配布

補足 C-SCRM ガイダンス：プライバシープログラム情報の配布は、サプライチェーン全体のサイバーセキュリティリスクから保護されることが望ましい。

レベル：1、2

PM-21 開示事項のアカウンティング

補足 C-SCRM ガイダンス：開示事項のアカウンティングは、サプライチェーン全体のサイバーセキュリティリスクから保護されることが望ましい。

レベル：1、2

PM-22 個人情報の品質管理

補足 C-SCRM ガイダンス：個人情報（PII）の品質管理では、サプライチェーン全体の PII 関連のサイバーセキュリティリスクを考慮し、このリスクを管理することが望ましい。

レベル：1、2

PM-23 データガバナンス会議体

補足 C-SCRM ガイダンス：データガバナンス会議体は C-SCRM におけるステークホルダーであり、政府機関横断的な協力及び C-SCRM 活動及びイニシアチブの情報共有に（FASC などの省庁間会議体への参加などにより）含めることが望ましい。

レベル：1

PM-25 テスト、トレーニング、及び研究で使用される個人情報の最小化

補足 C-SCRM ガイダンス：個人情報に対するサプライチェーン関連のサイバーセキュリティリスクは、この管理策で説明する最小化のポリシー及び手順によって対処されることが望ましい。

レベル：2

PM-26 苦情管理

補足 C-SCRM ガイダンス：苦情管理プロセス及びメカニズムは、サプライチェーン全体のサイバーセキュリティリスクから保護されることが望ましい。事業体はまた、ベンダ又は一般の人々からの苦情を処理するときに、C-SCRM セキュリティ及びプライバシー管理策を統合することが望ましい（除外及び削除に関連する問い合わせを処理する省庁及び関係機関など）。

レベル：2、3

PM-27 プライバシー報告

補足 C-SCRM ガイダンス：プライバシー報告プロセス及びメカニズムは、サプライチェーン全体のサイバーセキュリティリスクから保護されることが望ましい。

レベル：2、3

PM-28 リスクの枠組み

補足 C-SCRM ガイダンス：C-SCRM はリスクの枠組みに含まれることが望ましい。第 2 節及び附属書 C では、リスクの枠組みへの C-SCRM の統合に関する詳細なガイダンスを提供している。

レベル：1

PM-29 リスクマネジメントプログラムの責任者の役割

補足 C-SCRM ガイダンス：リスクマネジメントプログラムの責任者の役割は C-SCRM の責任を含んでいることが望ましく、またこの役割を事業体全体での C-SCRM のコラボレーションに含めることが望ましい。第 2 節及び附属書 C では、C-SCRM の役割及び責任に

関する詳細なガイダンスを提供している。

レベル：1

PM-30 サプライチェーンのリスクマネジメント戦略

補足 C-SCRM ガイダンス：サプライチェーンのリスクマネジメント戦略（C-SCRM 戦略とも呼ばれる）は、事業体の詳細なイニシアチブ及び活動と、タイムライン及び担当する関係者を明確に記述した C-SCRM 計画で補完されることが望ましい。この実装計画を POA&M にするか、又はこの計画を POA&M に含めることができる。事業体はレベル 1 での C-SCRM 戦略及び実装計画に基づき、事業体、プログラム、及びシステム固有のニーズに対処する共通 C-SCRM 管理策を選択及び文書化することが望ましい。これらの管理策は、レベル 1 及び レベル 2 の C-SCRM ポリシーとレベル 3 の C-SCRM 計画（又は必要に応じて SSP）に繰り返し統合されることが望ましい。 リスクマネジメントに関する詳細なガイダンスについては、第 2 節及び附属書 C を参照。

レベル：1、2

関連管理策：PL-2

PM-31 継続的監視戦略

補足 C-SCRM ガイダンス：継続的監視戦略及びプログラムは、サプライチェーンのリスクマネジメント戦略に従ってレベル 1、2、及び 3 で C-SCRM 管理策を統合することが望ましい。

レベル：1、2、3

関連管理策：PM-30

PM-32 目的

補足 C-SCRM ガイダンス：特定のミッション又はビジネスファンクションをサポートするために割り当てられたシステムを、当初の目的を超えて拡張すると、これらのシステムがサプライチェーン全体のサイバーセキュリティリスクなどの意図しないリスクにさらされる。この管理策の適用には、サプライチェーンのサイバーセキュリティリスクへの曝露（エクスポージャー）の明示的な組み入れが含まれていることが望ましい。

レベル：2、3

ファミリー：職員のセキュリティ

[FIPS 200]では、職員のセキュリティに関する最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）組織内（第三者のサービスプロバイダを含む）で責任のある職位に就いている個人が、信頼のおける人物であり、その職位について確立されているセキュリティ基準を満たしていることを確実にし、（ii）解雇や異動などの人事措置の前後で組織の情報及び情報システムが保護されることを確実にし、（iii）組織のセキュリティポリシー及び手順を順守しなかった人員に対する正式な罰則を採用しなければならない。

事業体のサプライチェーンにアクセスすることができる人員は、事業体の職員のセキュリティ管理策の対象とすることが望ましい。このような人員には、取得及び契約の専門家、プログラムマネージャ、サプライチェーン及びロジスティクスの専門家、出荷及び受領スタッフ、情報技術専門家、品質管理専門家、ミッション及びビジネスオーナー、システム所有者、及び情報セキュリティエンジニアなどが含まれる。事業体はまた、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと協力して、事業体のサプライチェーンと相互作用する人員に対し、必要に応じて適切なセキュリティ管理策を適用することを確実にすることが望ましい。

PS-1　ポリシー及び手順

補足 C-SCRM ガイダンス：各レベルで、職員のセキュリティポリシー及び手順並びに関連する C-SCRM 戦略／実装計画、C-SCRM ポリシー、及び C-SCRM 計画によって、取得、管理、及びサプライチェーンセキュリティ活動の実行に関わる人員の役割が定義される必要がある。これらの役割はまた、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの関係に関連して取得者の責任を記述する必要もある。ポリシー及び手順では、システムのシステム開発ライフサイクル全体と、様々なサプライチェーンインフラストラクチャ活動に対処するために必要な役割及び責任を考慮する必要がある。

レベル 1：該当する役割には、リスク管理者、CIO、CISO、契約、ロジスティクス、納入／受領、取得セキュリティ、及びサプライチェーンのサポート活動を提供するその他の機能が含まれる。

レベル 2：該当する役割には、取得者の事業体内のプログラム管理者及び個人（請負業者を含む非連邦政府従業員など）及びプログラム成功の責任を負う者（プログラムマネージャ及びその他の個人など）が含まれる。

レベル 3：該当する役割には、要件の定義から、開発、テスト、展開、メンテナンス、更新、交換、納入／受領、及び IT までの運用システムライフサイクル全体におけるシステムエンジニア又はシステムセキュリティエンジニアが含まれる。

プログラム成功の責任を負うサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの人員の役割が、

取得者とこれらの関係者の間の合意（契約など）に明記されることが望ましい。

事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：1、2、3

関連管理策：SA-4

PS-3 職員のスクリーニング

補足 C-SCRM ガイダンス：インサイダー脅威リスクを軽減するために、職員のスクリーニングのポリシー及び手順は、情報システム、システムコンポーネント、又は情報システムサービスへの認可されたアクセスを持つ請負業者の担当者まで拡大されることが望ましい。継続的監視活動は、機密情報又は規制された情報への請負業者のアクセスレベルと同等のものであり、広範な事業体ポリシーと整合していることが望ましい。スクリーニングの要件を合意に組み入れ、二次請負業者にフローダウンすることが望ましい。

レベル：2、3

PS-6 アクセス合意書

補足 C-SCRM ガイダンス：事業体はすべての請負業者、若しくは事業体のデータ、システム、又はネットワークに物理的又は論理的にアクセスする必要があるその他の外部人員とのアクセス合意書を定義し、文書化することが望ましい。アクセス合意書には、情報システム及びサプライチェーンネットワークへの適切なアクセスレベル及びアクセス手法が記述されていることが望ましい。さらに、アクセスに関する条項が事業体の情報セキュリティポリシーと整合していることが望ましく、またこれらの条項では、特定の期間中のアクセス、特定の場所からのアクセス、又は追加の調査要件を満たしている人員のみからのアクセスの許可といった、追加の制約事項を規定する必要がある可能性がある。事業体は、アクセス合意書に従ってこれらの関係者によるアクセスをレビュー、監視、更新、及び追跡するための監査メカニズムを展開することが望ましい。時間の経過に伴って職員は変わるため、事業体はアクセス合意書に対しタイムリーで厳格な職員のセキュリティ更新プロセスを実装することが望ましい。

情報システムとネットワーク製品及びサービスが事業体内のエンティティから提供されているときには、アクセス合意書が既に存在している可能性がある。このような合意書が存在しない場合には、合意書を確立することが望ましい。

注：監査メカニズムはレベル 3 で実装することができるが、必要な更新を使用する合意プロセスをレベル 2 でプログラムマネジメント活動の一環として実装することが望ましい。

事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

PS-7 外部職員のセキュリティ

補足 C-SCRM ガイダンス：事業体の情報システム及びネットワークにアクセスすることができる第三者の人員は、事業体の職員と同じ、職員のセキュリティ要件を満たしていなければならない。このような第三者の人員の例としては、システムインテグレータ、開発者、サプライヤ、納入のために使用される外部サービスプロバイダ、ICT/OT システムを使用する請負業者又はサービスプロバイダ、若しくは事業体又はシステムインテグレータが解決できないコンポーネントの技術的な問題に対処するために招き入れたサプライヤのメンテナンス作業員などがある。

レベル：2

ファミリー：個人情報の取扱い及び透明性

個人情報の取扱い及び透明性は、PII の取扱い及び透明性に関する懸念に対処するために特別に策定された新しい管理策ファミリーである。

事業体は、一部のサプライヤは事業体の要件を超えている可能性がある包括的なセキュリティ及びプライバシープラクティス及びシステムを導入していることに注意する必要がある。事業体はサプライヤと協力して、プライバシープラクティスの範囲と、これらのプラクティスが事業体のニーズにどのように対応するかを理解することが望ましい。

PT-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、サプライチェーンの懸念事項が、PII の取扱い及び透明性のポリシー及び手順、関連する C-SCRM 戦略／実装計画、C-SCRM ポリシー、及び C-SCRM 計画に含まれていることを確実にすることが望ましい。ポリシーは、一般的なセキュリティ及びプライバシーポリシーの一部として含めることも、あるいは複数のポリシーによって表すこともできる。

手順は、一般的なセキュリティ及びプライバシープログラム及び個々の情報システムに対して確立することができる。これらのポリシー及び手順は、情報システム又はサプライチェーン内のシステム／コンポーネントをサポートするために、目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、及びプライバシーコンプライアンスに対処することが望ましい。

共有される個人情報データ、個人情報にアクセスすることができる請負業者の人員、個人情報を保護する管理策、個人情報の保持可能な期間、及び契約終了時の個人情報の取扱いが契約に記述されていることを確実にするために、ポリシー及び手順を導入する必要がある。

a. 新規サプライヤと連携する際には、合意書に一連の最新の適用されるセキュリティ要件が含まれていることを確実にする。

b. 請負業者は、情報（個人情報及びその他の機密情報）に関連する法律及びポリシーを順守する必要がある。

c. 事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：1、2、3

ファミリー：リスクアセスメント

[FIPS 200]では、リスクアセスメントの最小限のセキュリティ要件を以下のように規定している。

> 組織は、組織の情報システムの運用及びこれに伴う組織の情報の処理、保管、又は伝送によって、組織の運営（ミッション、機能、イメージ、評判を含む）、組織の資産、及び個人に対して生じるリスクを定期的にアセスメントしなければならない。

本出版物は、サプライチェーンにおける事業体のサイバーセキュリティリスクの管理に関するガイダンスを提供し、第 2 節及び附属書 *C* で説明するようにサプライチェーンのサイバーセキュリティリスクのアセスメントを統合するためにこの管理策を拡張する。

RA-1 ポリシー及び手順

補足 C-SCRM ガイダンス：リスクアセスメントは事業体、ミッション／プログラム、及び運用レベルで実行することが望ましい。システムレベルのリスクアセスメントには、サプライチェーンインフラストラクチャ（開発及びテスト環境と納入システムなど）及びサプライチェーンを通過する情報システム／コンポーネントの両方が含まれていることが望ましい。システムレベルのリスクアセスメントは SDLC と大きく交差しており、SDLC で行われる事業体のより幅広い RMF 活動を補完することが望ましい。重要度分析は、侵害された場合のミッションに対するインパクトから、ミッション上重要な機能とコンポーネントにはより高い優先順位を付けることを確実にする。このポリシーには、事業体全体でのリスクアセスメントの実行と調整に適用されるサプライチェーン関連のサイバーセキュリティの役割が含まれることが望ましい（役割の一覧と説明については第 2 節を参照）。サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダ内の該当する役割を定義することが望ましい。

レベル：1、2、3

RA-2 セキュリティ分類化

補足 C-SCRM ガイダンス：セキュリティ分類化は、レベル 1、2、及び 3 の C-SCRM にとって重要である。[FIPS 199]の分類化の他に、C-SCRM のセキュリティ分類化は、SDLC の一部として実行される重要度分析に基づいていることが望ましい。重要度分析の詳細な説明については、第 2 節及び[NISTIR 8179]を参照。

レベル：1、2、3

関連管理策：RA-9

RA-3 リスクアセスメント

補足 C-SCRM ガイダンス：リスクアセスメントには、附属書 C で詳述するように重要度、脅威、脆弱性、起こりやすさ、及びインパクトの分析が含まれていることが望ましい。レ

ビュー及び収集対象のデータには、C-SCRM 固有の役割、プロセス、並びにシステム／コンポーネント及びサービスの取得、実装、及び統合の結果が含まれる。リスクアセスメントはレベル 1、2、及び 3 で実行されることが望ましい。上位レベルでのリスクアセスメントは主に、下位レベルで実行され、そのレベル（事業体又はミッション／ファンクションレベルなど）に対する全体的なインパクトを理解するために使用される様々なリスクアセスメントの組み合わせによって構成されることが望ましい。C-SCRM リスクアセスメントは、SDLC 全体で継続的活動として実行されるリスクアセスメントを補完し、情報を提供することが望ましく、また、プロセスは ERM プロセス及びガバナンスと整合しているか、又はこれらに統合されていることが望ましい。

レベル：1、2、3

関連管理策：RA-3(1)

RA-5 脆弱性の監視及びスキャン

補足 C-SCRM ガイダンス：脆弱性の監視では、事業体のサプライチェーンにおけるサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダを対象とすることが望ましい。これには、サプライヤ、及びサプライチェーンのサイバーセキュリティを通じてサプライヤが提供する情報システム、システムコンポーネント、及び未加工インプットに対する潜在的な脆弱性を継続的に認識している状態を維持するためにデータ収集ツールを採用することが含まれる。脆弱性監視活動は、事業体の 3つのレベルすべてで実行されることが望ましい。脆弱性監視活動のスコーピングでは、事業体はサプライヤとその下請サプライヤを考慮する必要がある。事業体は、適用可能かつ適切な場合は、SBOM に記載されているコンポーネントの適切かつ完全な脆弱性アセスメントを実証するために、脆弱性開示報告書（VDR）を顧客に提出することを検討することができる。VDR には、報告された脆弱性がコンポーネント又は製品に与えるインパクト（又はインパクトの欠落）を説明する分析及び所見が含まれていることが望ましい。VDR には、CVE に対処するための計画に関する情報も含まれていることが望ましい。事業体は、顧客が利用することができるセキュアなポータルで VDR を公開し、VDR の署名日時を示すタイムスタンプ及び関連する VDR が含まれている信頼できる検証可能な秘密鍵で VDR に署名することを検討することが望ましい。事業体は、VDR で開示されていない脆弱性が発生した場合に備えて顧客向けの個別の通知チャネルを確立することも検討することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

拡張管理策：

(1) 脆弱性の監視及びスキャン | カバレッジの幅及び深さ

補足 C-SCRM ガイダンス：サプライチェーンの脆弱性を監視する事業体は、サプライヤ又は製品／コンポーネントの重要度及び／又はリスクプロファイルと、監視が行わ

れるサプライチェーンのレベル（下請サプライヤなど）に基づく監視の深さに基づいて、監視の幅を表現することが望ましい。可能な場合には、コンポーネントインベントリ（ハードウェア、ソフトウェアなど）によって、事業体が監視して脆弱性をスキャンする必要がある可能性があるサプライチェーン内の製品／コンポーネントの幅及び深さを把握することが支援される。

レベル：2、3

(2) 脆弱性の監視及びスキャン | 自動化された傾向分析

補足 C-SCRM ガイダンス：事業体は、サプライチェーン内でコンポーネントの脆弱性の傾向を長期的に追跡することが望ましい。この情報は、事業体がサプライチェーン内のリスクレベルの密度を削減する調達戦略を策定するのに役立つことがある。

レベル：2、3

RA-7 リスク対応

補足 C-SCRM ガイダンス：事業体は、サプライチェーン全体のサイバーセキュリティリスクに対応するためのケイパビリティ（能力）を事業体の全体的な対応態勢に統合し、これらの対応が事業体のリスク許容度の境界に整合しており、この境界内に収まることを確実にすることが望ましい。リスク対応には、リスク対応の識別、代替策の評価、及びリスク対応決定活動が含まれることが望ましい。

レベル：1、2、3

RA-9 重要度分析

補足 C-SCRM ガイダンス：事業体は、サプライチェーンのサイバーセキュリティリスクマネジメント活動のアセスメントへの前提条件インプットとして重要度分析を実行することが望ましい。事業体は最初に、C-SCRM リスクマネジメントプロセスの枠組み化ステップの一環として、重要度分析を実行することが望ましい。その後、アセスメントステップの活動（重要度分析、脅威分析、脆弱性分析、及び軽減戦略など）で生成される所見により、重要度分析が更新及びテーラリングされる。重要度分析とその他のアセスメントステップの活動の間には、相互に情報を提供し拡張し合うという共生関係がある。品質の高い重要度分析のために、事業体は SDLC 全体を通じて分析を繰り返し採用し、また 3つのレベルで同時に採用することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

RA-10 脅威ハンティング

補足 C-SCRM ガイダンス：C-SCRM 脅威ハンティング活動は、事業体の内部脅威ハンティング活動を補完することが望ましい。サプライチェーンのサイバーセキュリティリスクマネジメントプロセスの重要な部分として、事業体はサプライチェーンに対する脅威を積極的に監視することが望ましい。このためには、C-SCRM 及び事業体内のその他のサイバー防御志向機能の間で協力的な取り組みが必要である。脅威ハンティングのケイパビリティ（能力）は、特に事業体に脅威ハンティング活動を自身で実行するためのリソースが不足している場合には、共有サービス事業体から提供することができる。一般的な活動には、同業の事業体との情報共有と、脅威インテリジェント情報源（情報共有分析センター（ISAC：Information Sharing and Analysis Centers）及び情報共有分析機関（ISAO：Information Sharing and Analysis Organizations）で利用可能な情報源など）の積極的な利用が含まれる。これらの活動は、サイバーインシデント、合併及び買収、及び外国人による所有、支配、又は影響（FOCI）など、懸念される可能性があるサプライチェーン全体のサイバーセキュリティリスクの増大を示す兆候を識別して警告するのに役立つ可能性がある。サプライチェーン脅威インテリジェンスは、事業体のサプライヤ、情報システム、システムコンポーネント、及びこれらが提供する未加工インプットに対する脅威を追求することが望ましい。収集されたインテリジェンスにより、事業体はサプライチェーンから生じる脅威を積極的に識別して対応することができる。

レベル：1、2、3

ファミリー：システム及びサービスの取得

[FIPS 200]では、システム及びサービスの取得に関する最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）組織の情報システムを適切に保護するための十分なリソースを割り振り、（ii）情報セキュリティの考慮事項を組み入れたシステム開発ライフサイクルプロセスを採用し、（iii）ソフトウェアの使用及びインストールに関する制限を採用し、（iv）第三者プロバイダが情報、アプリケーション、及び／又は組織から外部委託されるサービスを保護するために適切なセキュリティ対策を採用していることを確実にしなければならない。

事業体はシステム及びサービスの取得を通じて ICT/OT 製品及びサービスを取得する。これらの管理策は、取得者、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、その他の ICT/OT 関連のサービスプロバイダ、及び関連する上流サプライチェーン関係の活動を扱う。検知から SDLC 及びセキュリティエンジニアリングの原則まで、サプライチェーンセキュリティの物理的及び論理的側面の両方を扱う。C-SCRM の懸念事項については[NIST SP 800-53, Rev. 5]で既に顕著に扱われている。本出版物では、これらの管理策に詳細及び改良を加えた。

SA-1 ポリシー及び手順

補足 C-SCRM ガイダンス：システム及びサービスの取得のポリシー及び手順では、チャージカードによる購入を含めるために、取得管理ライフサイクルプロセス全体で C-SCRM に対処することが望ましい。C-SCRM 調達活動とその結果の契約には、どの管理策が必須又は望ましいものであるかを扱う要件の文言又は条項が含まれていることが望ましく、また実装の仕様を含めてもよく、要件を満たしている証拠として受け入れられる内容と、要件への準拠の検証及び妥当性確認を行う方法を記述してもよい。C-SCRM が評価要因として含まれることが望ましい。

該当する調達は、ICT/OT 製品又はサービスの提供に直接関連する調達に限定されないことが望ましい。C-SCRM の考慮事項はこれらの購入に適用されなければならないが、供給される製品又はサービスの請負業者が事業体の情報の完全性、可用性、又は機密性を侵害するという受容できないリスクが発生する可能性がある製品又はサービスのすべての調達についても、C-SCRM が考慮されることが望ましい。初回のアセスメントは取得計画フェーズで実施されることが望ましく、事業体のミッション機能の重要度、事業体の高価値資産、及び供給される製品又はサービスのプロバイダがアクセスすることができる可能性がある情報の機微性を識別及び理解することで、このアセスメントに最小限の情報が提供される。

さらに事業体は、事業の所有権又は支配権の変更や、サプライヤ又は製品がサプライチェーン脅威の標的となっていることを示す実用的な情報が判明した場合など、契約履行時に発生する可能性があるサプライチェーンリスクに対処するポリシー及び手順を策定することが望ましい。サプライチェーンは合併及び買収、合弁事業、及びその他の提携に関する合意を通じて継続的に発展する。このポリシーは、事業体がこのような変化を理解し、取得した情報を使用して C-SCRM 活動に情報を提供するのに役立つことが望ましい。事業体は、例えば企業活動に関する公式発表や、サプライヤ、開発者、システム

インテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが発信する情報を監視することで、このような変化の状況を把握することができる。

連邦政府の取得プロセスにおける C-SCRM に関する詳細なガイダンスについては、第 3 節を参照。さらに各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

SA-2 リソースの割り当て

補足 C-SCRM ガイダンス：事業体は、リソースの割り振りを決定及び確立するときに C-SCRM 要件を組み入れることが望ましい。

レベル：1、2

SA-3 システム開発ライフサイクル

補足 C-SCRM ガイダンス：SDLC と C-SCRM 活動の間には密接な関係がある。事業体は、事業体と、該当するサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの両方で C-SCRM 活動が SDLC に組み入れられることを確実にすることが望ましい。SDLC には、要件や設計などの従来の SDLC 活動の他に、インベントリ管理、取得及び調達、システム及びコンポーネントの論理的納入などの活動が含まれる。SDLC に関する詳細なガイダンスについては、第 2 節及び附属書 C を参照。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

SA-4 取得プロセス

補足 C-SCRM ガイダンス：事業体は、該当する契約上の合意に C-SCRM の要件、説明、及び基準を含めるものとする。

1. 事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダから製品又はサービスを調達するときに適用し、契約上の合意に組み入れるベースライン及びテーラリング可能な C-SCRM 要件を確立するものとする。これには以下が含まれるが、これらに限定されない。

    a. 規制（特定の ICT/OT 又はサプライヤの禁止など）を対象とする C-SCRM 要件は、調達される製品又はサービスにより生じる可能性があるサプライチェーンのサイバーリスクを低減するために適用でき、また請負業者が責任、ケイパビリティ（能力）、及び統合的信頼性を十分に備えているというアシュアランスを提供する、識別及び選択された管理策を扱う。

b. オープンソースの情報及びその他の情報源に基づいて新たな脆弱性を修復することができるケイパビリティ（能力）を実証するための、サプライチェーンの重要な要素に対する要件。

c. 知的財産の所有権と、ソフトウェアコード、データ及び情報、製造、開発、又は統合環境、設計、及び専用プロセス（レビュー又は使用のために事業体に提供される場合）などの要素に対する責任を管理するための要件。

d. 製品又はシステムの期待寿命、寿命に基づいてクリティカルパスに存在している可能性がある要素、及び取り扱い終了が近づいているか又は到達している場合に必要な事柄を扱う要件。事業体は、取り扱い終了時の選択肢（交換、アップグレード、新規システムへの以降など）を把握するために、調査を実施するか、若しくは入札者又は契約している既存のプロバイダからの情報を求める。

e. 非公式市場のコンポーネントが許可される可能性があるすべての状況を明確にする。

f. 機能プロパティ、構成、及び実装情報と、関連する可能性がある開発方法、技法、及びプラクティスに関する要件。C-SCRM 評価基準の重み付けを含めるために、C-SCRM 評価基準を識別及び規定する。

2. 事業体は、以下を行うことが望ましい。

   a. 十分な供給を確保するために予備部品の取得計画を策定し、該当する場合にこの計画を実行する。

   b. 継続的な事象の発生時、又はサプライチェーンの寸断発生時に必要となる可能性がある代替供給源の取得に関する計画を策定する。

   c. サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと協力して、サプライチェーン内の他の事業体からの脆弱性に関するインプットなど、既存の受け入れ可能なインシデント対応及び情報共有プロセスを識別及び定義する。

3. 納入された製品及びサービスの検証手順と受領基準を確立及び維持する。これには以下が含まれるが、これらに限定されない。

   a. 事業体が認可する場合の検証なしでの COTS 及び GOTS 製品の受け入れ（承認済み製品のリストなど）

   b. 開発及び COTS ソフトウェア及びハードウェア情報システムの脆弱性に関するサプライヤによる妥当性確認

4. 継続的監視計画の基準に、使用中の機能、ポート、及びプロトコルの監視を含めるなど、サプライチェーンの側面が含まれていることを確実にする。第 2 節及び附属書 C を参照。

5.契約において、サプライチェーンインフラストラクチャ内に存在するサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの情報システムの監視が扱われていることを確実にする。取得した作業プロセス及び作業成果物を必要に応じて監視及び評価する。これには、ソフトウェア開発インフラストラクチャ（DevSecOps パイプライン、ソフトウェアコンテナ、及びコードリポジトリ／共有など）における脆弱性の監視が含まれるが、それに限定されない。

6. ICT/OT 製品又はサービスの使用中に検出された情報セキュリティの弱点及び脆弱性を報告するためのプロセスを伝達し、該当する場合には OEM を含む適切なステークホルダーに報告されることを確実にする。

7. 合意の諸条件を順守し続けていることを継続的にレビュー及び確認する。

各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation’s Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

関連管理策：SA-4 (1)、(2)、(3)、(6)、及び (7)

拡張管理策：

(1) 取得プロセス | システム、コンポーネント、及びサービスの構成

補足 C-SCRM ガイダンス：事業体は、コンポーネントを購入する必要がある場合には、OEM から直接購入する場合でもチャネルパートナー又は非公式市場から購入する場合でも、製品仕様が「目的に適合」しており、事業体の要件を満たしていることを確実にする必要がある。

レベル：3

(2) 取得プロセス | *NIAP* 承認済みプロテクションプロファイル

補足 C-SCRM ガイダンス：この拡張管理策は、可能な場合に事業体が米国政府のプロテクションプロファイル認定の情報アシュアランス（IA）コンポーネントを構築、調達、及び／又は使用することを要求する。NIAP 認定は OTS（COTS 及び GOTS）で取得可能である。

レベル：2、3

(3) 取得プロセス | 管理策の継続的監視計画

補足 C-SCRM ガイダンス：この拡張管理策は、C-SCRM 及び管理策の有効性の継続的監視計画に関連しているため、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダまで拡大されることが望ましい。

レベル：2、3

SA-5 システムドキュメント

補足 C-SCRM ガイダンス：情報システムの文書には、関連する C-SCRM の懸念事項（C-SCRM 計画など）を含めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：3

SA-8 セキュリティ及びプライバシーエンジニアリングの原則

補足 C-SCRM ガイダンス：以下のセキュリティエンジニアリング技法は、サプライチェーン全体のサイバーセキュリティリスクを管理するのに役立つ。

a. ICT/OT 製品又はサービスを誤使用又は悪用から保護する方法を識別するのに役立てるために、これらの製品又はサービスがそのように使用される可能性がある最大限の方法を想定する。アーキテクチャ及び設計における意図した用途と意図していない用途のシナリオに取り組む。
b. リスクアセスメントでの決定に従い、事業体のリスク許容度に基づいてネットワーク及びセキュリティアーキテクチャ、システム、及びコンポーネントを設計する（第 2 節及び附属書 C を参照）。
c. 完全に軽減されていないリスクを文書化し、幹部による受諾及び承認を得る。
d. 重要な要素の数、サイズ、及び特権レベルを制限する。重要度分析の使用は、重要な要素又は機能を判断するのに役立つ。附属書 C 及び NISTIR 8179、「重要性分析プロセスモデル：システム及びコンポーネントの優先順位付け（*Criticality Analysis Process Model: Prioritizing Systems and Components*）」の重要度分析を参照。
e. 暗号化、アクセス制御、アイデンティティ管理、及びマルウェア又は改ざん検出など、サプライチェーンのサイバーセキュリティ脆弱性を悪用することができる機会を減らすのに役立つセキュリティメカニズムを使用する。

f. 情報システムコンポーネント又は要素は、無効にすることが困難（改ざん防止技法など）であり、無効にされた場合には監査証跡、改ざんの証拠、又はアラームなどの通知方法をもたらすように設計する。
g. 納入時にサプライチェーンを通過するシステム／コンポーネント及びサプライチェーンへの不必要な曝露（エクスポージャー）又はアクセスを防ぐ納入メカニズム（ソフトウェアのダウンロードなど）を設計する。
h. 実装及び運用時に使用する、関連性がある妥当性確認メカニズムを設計する。

各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

SA-9 外部システムサービス

補足 C-SCRM ガイダンス：C-SCRM 補足ガイダンスは拡張管理策で提供される。

拡張管理策：

(1) 外部システムサービス | リスクアセスメント及び組織承認

補足 C-SCRM ガイダンス：各省庁及び関係機関は附属書 E 及び附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

(2) 外部システムサービス | プロバイダとの信頼関係の確立及び維持

補足 C-SCRM ガイダンス：プロバイダとの関係[37]は、以下のサプライチェーンセキュリティ要件を満たしていることが望ましい。

a. 要件の定義が完了しており、様々なコンポーネントへの重要度の設定及び運用コンセプトと意図した用途及び意図していない用途の関連シナリオの定義を含む、正確性と網羅性についてのレビューが行われている。
b. 要件が、ニーズ、関連するコンプライアンス推進要因、重要度分析、及びサプライチェーン全体のサイバーセキュリティリスクのアセスメントに基づいている。
c. サプライチェーンのサイバー脅威、脆弱性、及び関連するリスクが識別され、文書化されている。
d. 事業体のデータ及び情報の完全性、機密性、及び可用性の要件が定義されており、必要に応じて、システムのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと共有されている。
e. C-SCRM 要件及び情報システムのセキュリティ要件に準拠しない場合の結果が定義及び文書化されている。
f. 複数の異なるプロバイダがシステム又はミッション及びビジネスファンクションのサポートに関わるときに、請負業者間で説明責任、役割、及び責任が明確

に線引きされている。

g. 要件で、サービス契約の完了と、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの関係終了の定義が詳細に記述されている。これは、再競争、プロバイダにおける潜在的変化、及びシステム取り扱い終了プロセスの管理のために理解しておくことが重要である。
h. クラウド環境からのデータの削除など、安全でセキュアな終了を確実にするために、関係終了に関する交渉による合意を確立する。

各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

(3) 外部システムサービス | 消費者及びプロバイダの一貫した利益

補足 C-SCRM ガイダンス：この拡張管理策のコンテキストでは、「プロバイダ」にはサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが含まれる可能性がある。

レベル：3

(4) 外部システムサービス | 処理、保管、及びサービスの場所

[37] この拡張管理策のコンテキストでは、「プロバイダ」にはサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが含まれる可能性がある。

補足 C-SCRM ガイダンス：これらの場所は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの管理下にあることがある。事業体は特定の地理的場所に関連する C-SCRM リスクをアセスメントし、受容可能又は受容不可能な場所を定義すること、及び関連する C-SCRM リスクに対処するために適切な保護が導入されていることを確実にすることなど、適切なリスク対応を適用することが望ましい。

レベル：3

SA-10 開発者構成管理

補足 C-SCRM ガイダンス：開発者構成管理は、サプライチェーン全体のサイバーセキュリティリスクを低減する上で重要である。開発者は構成管理活動を実行することで、変更に対する説明責任及びオーナーシップを強化する一方で、欠陥の発生及び起こりやすさを低減する。開発者構成管理は、連邦政府機関内部の開発者及びインテグレータ又は外部サービスプロバイダの両方が実施することが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：SA-10 (1)、(2)、(3)、(4)、(5)、及び (6)

SA-11　開発者のテスト及び評価

補足 C-SCRM ガイダンス：コンポーネントの出所に応じて、この管理策の実装方法は異なることがある。OTS（既製品）コンポーネントの場合、取得者はサプライヤ（OEM）が品質又はセキュリティプロセスの一部としてテストを実施しているかどうかを判断するために、（公開されているリソースなどを使用して）調査を実施するか、又は証拠を要求することが望ましい。取得者がアプリケーション及び開発プロセスを管理している場合、このテストを SDLC の一部として求めることが望ましい。拡張管理策で説明する特定のタイプのテスト活動の他に、C-SCRM 関連テストの例としては、偽造品のテスト、コンポーネントの出所の検証、統合前の構成設定のテスト、及びインタフェースのテストなどがある。このようなタイプのテストはかなりの量のリソースを必要とする可能性があり、重要度、脅威、及び脆弱性分析（第 2 節及び附属書 C で説明）と、テスト技法の有効性に基づいて優先順位付けされることが望ましい。事業体は、開発者セキュリティテストの一部として第三者テストを必要とすることもある。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

関連管理策：SA-11 (1)、(2)、(3)、(4)、(5)、(6)、(7)、(8)、及び (9)

SA-15　開発プロセス、規格、及びツール

補足 C-SCRM ガイダンス：内部及びシステムインテグレータの開発者を手引きするための文書化及び正式に定められた開発プロセスを提供することは、サプライチェーン全体のサイバーセキュリティリスクを効果的に軽減するための事業体の取り組みにとって重要である。事業体は、この管理策を実装するときには国内規格及び国際規格とベストプラクティスを適用することが望ましい。既存の規格を使用すると、実装の整合性、信頼性があり防御可能なプロセス、及び相互運用性が促進される。事業体の開発、メンテンナンス、テスト、及び展開環境はすべてこの管理策の対象となることが望ましい。この管理策に含まれるツールには、手動ツール又は自動化ツールがある。自動化ツールを使用すると、分析の徹底性、効率性、及びスケールが促進され、サプライチェーン全体で開発プロセスに関連して発生するサイバーセキュリティリスクに対処するときに役立つ。さらに、

第 2 節及び附属書 C で説明するように、このような活動及びツールのアウトプットは C-SCRM プロセスの有用なインプットを提供する。この管理策は、内部事業体のプロセス、情報システム、及びネットワークと、該当するシステムインテグレータのプロセス、システム、及びネットワークに適用することができる。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：SA-15 拡張管理策 (1)、(2)、(5)、(6)、及び (7)

拡張管理策：

(1) 開発プロセス、規格、及びツール | 重要度分析

補足 C-SCRM ガイダンス：この拡張管理策は情報システム内で重要なコンポーネントを識別するものであり、重要なコンポーネントのために実装される特定の C-SCRM 活動を判断するのに役立つ。追加のコンテキストについては、附属書 C で説明する C-SCRM 重要度分析を参照。

レベル：2、3

(2) 開発プロセス、規格、及びツール | 脅威のモデル化及び脆弱性の分析

補足 C-SCRM ガイダンス：この拡張管理策は、関連する連邦政府機関及び請負業者の製品、アプリケーション、情報システム、及びネットワークの脅威のモデル化及び脆弱性の分析を提供する。この分析を実行すると、C-SCRM をコード改良及び変更活動に統合するのに役立つ。追加のコンテキストについては、附属書 C で説明する C-SCRM 脅威及び脆弱性分析を参照。

レベル：2、3

関連管理策：SA-15、SA-15(6)、SA-15(7)

(3) 開発プロセス、規格、及びツール | 脅威及び脆弱性情報の再利用

補足 C-SCRM ガイダンス：この拡張管理策は開発者に対し、以前の開発業務で作成された脅威及び脆弱性情報と、ツールの使用経験から得た教訓を再利用して、進行中の開発作業に情報を提供することを促す。このようにすることで、第 2 節及び附属書 C で説明する C-SCRM 活動を判断するのに役立つ。

レベル：3

SA-16 開発者が提供するトレーニング

補足 C-SCRM ガイダンス：外部及び内部の開発者向けに開発者が提供するトレーニングは、C-SCRM にとって重要である。これは、該当する開発環境を含めるために、連邦政府のシステム及びネットワークの責任を負う個人に対するトレーニングを扱う。この管理策における開発者が提供するトレーニングは、システム及びネットワークコンポーネントを

選択する個人にも適用される。開発者が提供するトレーニングには、1）ハードウェア及びソフトウェアの開発、テスト、及びメンテナンスの際の潜在的な脅威及び脆弱性を開発者が認識し、2）システム及びネットワークコンポーネントの責任を負う個人がそのようなコンポーネントを選択するときに C-SCRM を組み込むことを確実にするために、C-SCRM の資料を含めることが望ましい。開発者のトレーニングでは、セキュアなコーディングと、ツールを使用したソフトウェアの脆弱性検出のトレーニングも扱うことが望ましい。重要なソフトウェアのセキュリティに関する追加ガイダンスについては、附属書 F を参照。

レベル：2、3

関連管理策：AT-3

SA-17 開発者のセキュリティ及びプライバシーのアーキテクチャ及び設計

補足 C-SCRM ガイダンス：この管理策は、システムアーキテクチャ、設計、及びセキュリティ機能を含むコンポーネントの選択の決定に影響を与える C-SCRM 情報の使用を容易にする。例えば、システムアーキテクチャ及び設計を構成するコンポーネントの識別、複数のサプライヤ又はコンポーネントの選択を通じて可用性を確保するための特定コンポーネントの選択などがある。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：SA-17 (1) 及び (2)

SA-20 重要コンポーネントのカスタム開発

補足 C-SCRM ガイダンス：事業体は、サプライチェーン全体のサイバーセキュリティリスクのアセスメントに基づいて、特定の重要コンポーネントのカスタム開発が必要であるかどうかを判断することができる。この管理策は、この活動に関する追加のガイダンスを提供する。事業体はサプライヤ及びパートナーと協力して、重要なシステムが識別されることを確実にすることが望ましい。組織は、カスタム開発の重要ソフトウェアコンポーネントを継続的に維持することができる能力を組織が有していることを確実にすることが望ましい。例えば、ソフトウェアコンポーネントのソースコード、ビルドスクリプト、及びテストを所有している場合、組織は必要に応じてその保守を他者に割り当てることができる可能性がある。

レベル：2、3

SA-21 開発者のスクリーニング

補足 C-SCRM ガイダンス：事業体は、内部開発者のスクリーニングプロセスを実装することが望ましい。重要なコンポーネントを扱う主要な開発者を提供する可能性があるシステムインテグレータの場合、事業体は、開発者のスクリーニングのための適切なプロセスが使用されていることを確実にすることが望ましい。開発者のスクリーニングは契約の要件として含めることが望ましく、また開発サービスを提供するか又は開発環境にアクセスすることができる関連する二次請負業者へのフローダウン要求条件であることが望ましい。

レベル：2、3

拡張管理策：

(1) 開発者のスクリーニング | スクリーニングの妥当性確認

補足 C-SCRM ガイダンス：内部開発者のスクリーニングの妥当性確認を行うことが望ましい。事業体は、妥当性確認後に提供する要約データをシステムインテグレータに要求することで、システムインテグレータの開発者のスクリーニングに対して妥当性確認を行うことができる。

レベル：2、3

SA-22　サポートされていないシステムコンポーネント

補足 C-SCRM ガイダンス：適格な相手先ブランド製造業者（OEM）又は OEM の認可販売代理事業者及び再販業者から製品を直接取得することで、サプライチェーンのサイバーリスクが低減する。サポートされていないシステムコンポーネントの場合、事業体は、サポートされていないシステムコンポーネントのサプライヤと持続的な関係を持つ認可再販業者又は販売代理事業者を使用することが望ましい。

継続的なサポートのために代替ソースを購入する場合、事業体は調査済みの相手先ブランド製造業者（OEM）又はその認可販売代理事業者及び再販業者から直接取得することが望ましい。

代替ソースの使用について決定するときには、事業体のエンジニアリングリソースから代替コンポーネントオプションの相違に関するインプットが必要となる。例えば、代替策がオープンソースソフトウェアコンポーネントを取得することである場合、事業体はオープンソースコミュニティの開発、テスト、受け入れ、及びリリースプロセスを識別することが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

ファミリー：システム及び通信の保護

[FIPS 200]では、システム及び通信の保護の最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）組織の通信（すなわち、組織の情報システムが送受信する情報）を、情報システムの外部境界及び主要な内部境界で監視、管理、及び保護し、（ii）組織の情報システム内で効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発技法、及びシステムエンジニアリング原則を採用しなければならない。

事業体の通信インフラストラクチャは、ICT/OT コンポーネント及びシステムで構成されており、これらのコンポーネント及びシステムには独自のサプライチェーンがある。これらの通信により、ユーザ又は管理者は事業体のシステムにリモートアクセスし、インターネット、事業体内の他のICT/OT、請負業者のシステム、及び、場合によってはサプライヤシステムに接続することができる。事業体の通信インフラストラクチャは、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダによって提供及びサポートされることがある。

SC-1 ポリシー及び手順

補足 C-SCRM ガイダンス：システム及び通信の保護のポリシー及び手順は、事業体のプロセス、システム、及びネットワークに関連してサプライチェーン全体でのサイバーセキュリティリスクに対処することが望ましい。事業体レベル及びプログラム固有のポリシーは、このような要件を確立及び明確化するのに役立ち、対応する手順は、これらの要件を満たすための指示を提供する。ポリシー及び手順には、事業体内の複数の事業体エンティティ間の通信の調整と、事業体及びそのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの間で使用される通信方法、外部接続、及びプロセスが含まれていることが望ましい。

レベル：1、2、3

SC-4 共有システムリソース内の情報

補足 C-SCRM ガイダンス：事業体は、システムサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダと情報システムリソースを共有することが望ましい。主要な業務を外部委託する場合、様々なサプライチェーン活動をサポートする共有リソースの情報を保護することは困難である。事業体が共有するリソースが多すぎると事業体のリスクが増大する可能性があり、共有するリソースが少なすぎるとサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが効率的にサービスを提供することが困難になる可能性がある。事業体は開発者と協力して、共有するデータ、共有方法、情報の提供先（特定の役割）など、情報共有のための構造又はプロセスを定義することが望ましい。情報共有プロセスで、適切なプライバシー、配布、処理、及びクリアランスの要件を説明することが望ましい。

レベル：2、3

SC-5 サービス拒否（DoS）からの保護

補足 C-SCRM ガイダンス：C-SCRM ガイダンスの補足ガイダンスは拡張管理策 SC-5 (2) で提供される。

拡張管理策：

(1) サービス拒否からの保護 | 容量、帯域幅、及び冗長性

補足 C-SCRM ガイダンス：事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの合意に、余剰の容量、帯域幅、及び冗長性の要件を含めることが望ましい。

レベル：2

SC-7 境界保護

補足 C-SCRM ガイダンス：事業体は、政府機関のシステムと、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダのシステムの間の境界に、適切な監視メカニズム及びプロセスを実装することが望ましい。サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの合意に、境界保護に関する規定を組み入れることが望ましい。事業体、サプライヤシステム及びネットワーク、及び SDLC 全体で複数のインタフェースが存在することがある。サプライチェーンコンポーネント及びサプライチェーン情報フローの適切な境界保護を確実にするために、適切な脆弱性、脅威、及びリスクアセスメントを実施することが望ましい。脆弱性、脅威、及びリスクアセスメントは、境界保護を関連する基準のセットにスコーピングし、関連コストを管理するのに役立つ。外部サービスプロバイダとの契約では、事業体はプロバイダがその管理範囲内の環境及びネットワークに関連する境界管理の要件を満たしていることを確実にすることが望ましい。詳細については第 2 節及び附属書 C で説明する。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2

拡張管理策：

(1) 境界保護 | セキュリティツール、メカニズム、及びサポートコンポーネントの分離

補足 C-SCRM ガイダンス：事業体は、事業体の情報システム及びネットワーク内で開発、テスト、及びセキュリティアセスメントツールと運用環境及び関連監視ツールを分離することが望ましい。この管理策は、連邦政府機関及び一次請負業者を含めるために、ソフトウェア及びハードウェアの作成の責任を負うエンティティに適用される。このため、この管理策は連邦政府機関及び該当するサプライヤの情報システム及びネットワークに適用される。事業体は一次請負業者に対し、この管理策を実装してこの

要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。いずれかの環境で侵害又は情報漏えいが発生しても、分離メカニズム又は技法によって他の環境は引き続き保護されることが望ましい。

レベル：3

関連管理策：SR-3(3)

(2) 境界保護 | 認可されていない物理的接続からの保護

補足 C-SCRM ガイダンス：この管理策は、外部サービスプロバイダに適用されるため C-SCRM に関連している。

レベル：2.3

関連管理策：SR-3(3)

(3) 境界保護 | 組織外で構成されたホストからの通信のブロック

補足 C-SCRM ガイダンス：この管理策は、外部サービスプロバイダに適用されるため C-SCRM に関連している。

レベル：3

SC-8 伝送の機密性及び完全性

補足 C-SCRM ガイダンス：サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの合意に、伝送の機密性及び完全性の要件を統合することが望ましい。取得者、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダは、事業体の機密性及び完全性の要件を達成するために、既存のセキュリティメカニズム（認証、認可、又は暗号化など）を転用することができる。保護の度合いは、伝送される情報の機微性、及び事業体とサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの間の関係に基づくことが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

SC-18 モバイルコード

補足 C-SCRM ガイダンス：事業体は、情報システム及びネットワーク内での様々なモバイルコードの適用において、この管理策を使用することが望ましい。例としては、サプライチェーン情報の電子伝送（メールなど）、ソフトウェアコンポーネントの受領、RFID でのロジスティクス情報管理、又はトランスポートセンサのインフラストラクチャなどの取得プロセスがある。

レベル：3

拡張管理策：

(1) モバイルコード | 取得、開発、及び使用

補足 C-SCRM ガイダンス：事業体は、情報システムに展開するモバイルコードの取得、開発、及び使用において厳格なサプライチェーン保護技法を採用することが望ましい。例としては、取得時にモバイルコードの出所が調査済みの供給源であること、カスタムモバイルコードの開発時又はインストール前に調査済みシステムインテグレータが使用されていること、及び供給源とコードの完全性を検証するためにインストール前の受領基準の検証プロセスが導入されていることを確実にすることなどがある。モバイルコードは、基盤となる情報システム及びネットワーク（RFID デバイスアプリケーションなど）のコード、又は情報システム及びコンポーネントのコードの両方である可能性があることに注意する。

レベル：3

SC-27 プラットフォームに依存しないアプリケーション

補足 C-SCRM ガイダンス：プラットフォームに依存しない信頼できるアプリケーションを使用することは、C-SCRM に不可欠である。プラットフォームに依存しないアプリケーションの移植性が強化されていることにより、事業体はいずれかの外部サービスプロバイダが侵害された場合にプロバイダをより簡単に切り替えることができるようになり、ベンダ依存のサイバーセキュリティリスクを低減することができる。これは特に、複数のシステムが依存する可能性がある重要なアプリケーションに該当する。

レベル：2、3

SC-28 保管中の情報の保護

補足 C-SCRM ガイダンス：事業体は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの合意に、保管中の情報の保護に関する規定を含めることが望ましい。事業体はまた、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダのソースコード、テストデータ、ブループリント、知的財産情報といった保管中のデータに対し、情報システム及びネットワーク内で適切な保護を提供していることを確実にすることが望ましい。この管理策は、要件、開発、製造、テスト、インベントリ管理、メンテナンス、及び廃棄を含め、SDLC 全体で適用されることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：SR-3(3)

SC-29 異質性

補足 C-SCRM ガイダンス：異質性の技法には、異なるオペレーティングシステム、仮想化技法、及び複数の供給源の使用が含まれる。複数の供給源により、コンポーネントの可用性を高め、サプライチェーンのサイバーセキュリティ侵害のインパクトを低減させることができる。サプライチェーンのサイバーセキュリティ侵害が発生した場合、事業体は代替供給源によって、侵害の影響を受けてない可能性がある代替システム／コンポーネントに、より迅速に切り替えることができる。さらに、異種コンポーネントにより、脆弱なコンポーネントを使用しているインフラストラクチャのサブセットに対するインパクトが制限され、攻撃対象領域が削減される。

レベル：2、3

SC-30 秘匿化及び誤認誘導

補足 C-SCRM ガイダンス：C-SCRM の秘匿化及び誤認誘導の技法には、ランダムな再供

給回数の確立、場所の秘匿化、使用する偽の場所のランダムな変更、情報保管場所のランダムな変更若しくは代替サーバ又はストレージメカニズムへの移行などがある。

レベル：2、3

拡張管理策：

(1) 秘匿化及び誤認誘導 | ランダム性

補足 C-SCRM ガイダンス：サプライチェーンプロセスは、効率性及びコスト削減の目的から、必然的に予測可能、測定可能、及び繰り返し可能なプロセスで構成される。これにより潜在的なブリーチの機会が生じる。侵害から保護するために、事業体は事業体のシステム又はネットワークでその運営及び資産にランダム性を導入する技法（様々な納入事業体又は経路をランダムに切り替える、以前に予測できる方法でスケジュールが設定されていた場合にサプライヤのソフトウェア更新の受領日時を変更するなど）を採用することが望ましい。

レベル：2、3

(2) 秘匿化及び誤認誘導 | 処理場所及び保管場所の変更

補足 C-SCRM ガイダンス：処理場所又は保管場所の変更は、ダウンロード、納入、又は関連するサプライチェーンメタデータを保護するために使用することができる。事業体は情報システム及びネットワーク内でこのような技法を活用して、敵対者が標的とする活動に関する不確実性をもたらすことができる。いくつかのプロセス変更を確立し、受領、検収テスト、保管、又はその他のサプライチェーン活動などの用途をランダム化することは、サプライチェーン事象の起こりやすさを低減するのに役立つ。

レベル：2、3

(3) 秘匿化及び誤認誘導 | 誤解を招く情報

補足 C-SCRM ガイダンス：事業体は、開発している情報システムと事業体のシステム及びネットワークを保護するために、秘匿化及び誤認誘導の取り組みの一環として、誤解を招く情報を伝達することができる。このようなセキュリティへの取り組みの例としては、ハニーネットや仮想化環境などがある。誤解を招く情報を伝達するために実装を活用することができる。これらは、効果的に実装するには経験のあるリソースを必要とする高度な技法として見なされることがある。事業体がハニーポットを使用することにした場合、法務顧問と協力し、事業体のポリシーに従って実施されることが望ましい。

レベル：2、3

(4) 秘匿化及び誤認誘導 | システムコンポーネントの秘匿化

補足 C-SCRM ガイダンス：事業体は、開発されている情報システムと事業体の情報システム及びネットワークに関する情報を保護するために、様々な秘匿化及び誤認誘導の技法を採用することができる。例えば、コンポーネントの用途又はコンポーネントを使用する事業体に関する一切の情報を秘匿化又は誤認誘導するために、中央又は信頼できる第三者の倉庫への重要コンポーネントの納入を使用することができる。情

報を秘匿化し、コンポーネント又はその用途、条件、あるいはその他の属性の機密性の潜在的な損失の機会を減らすために、コンポーネントをその関連する情報から様々な物理的及び電子的納入チャネルに分離し、様々な技法によってこの情報を難読化する手法を使用することができる。

レベル：2、3

SC-36 分散処理及びストレージ

補足 C-SCRM ガイダンス：事業体のシステム及びネットワーク全体、及び SDLC 全体の両方で処理及びストレージを分散することができる。事業体は、これらの技法が両方のコンテキストで適用されることを確実にすることが望ましい。開発、製造、構成管理、テスト、メンテナンス、及び運用では、分散処理及びストレージを使用することができる。この管理策は、連邦政府機関及び請負業者を含めるために、処理及びストレージ機能又は関連インフラストラクチャの責任を負うエンティティに適用される。このため、この管理策は連邦政府機関及び該当するサプライヤの情報システム及びネットワークに適用される。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

関連管理策：SR-3(3)

SC-37 帯域外チャネル

補足 C-SCRM ガイダンス：C-SCRM 固有の補足ガイダンスは拡張管理策 SC-37 (1) で提供される。

拡張管理策：

(1) 帯域外チャネル | 確実な配信及び送信

補足 C-SCRM ガイダンス：事業体は、特定の個人又は情報システムのみが情報システム又はその開発環境及びプロセスに関する情報を受け取ることを確実にするために、セキュリティ保全措置を採用することが望ましい。例えば納入時に、カスタムチップ、カスタムソフトウェア、又は情報などの重要なコンポーネントのリリース前に、適切なクレデンシャル及び認可の文書を要求及び検証することが望ましい。

レベル：2、3

SC-38 運用セキュリティ

補足 C-SCRM ガイダンス：事業体は、適切なサプライチェーン脅威及び脆弱性の情報が該当する運用セキュリティプロセスから取得され、このプロセスに提供されていることを確実にすることが望ましい。

レベル：2、3

関連管理策：SR-7

SC-47 代替通信経路

補足 C-SCRM ガイダンス：必要かつ適切な場合には、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダが、この管理策で説明する代替通信経路に含まれることが望ましい。

レベル：1、2、3

ファミリー：システム及び情報の完全性

[FIPS 200]では、システム及び情報の完全性の最小限のセキュリティ要件を以下のように規定している。

> 組織は、（i）情報及び情報システムの欠陥をタイムリーに識別、報告、及び訂正し、（ii）組織の情報システム内の適切な場所で悪意のあるコードからの保護を提供し、（iii）情報システムセキュリティのアラート及び勧告を監視し、対応として適切なアクションを実行しなければならない。

サプライチェーンを通過するシステム及びコンポーネントのシステム及び情報の完全性は、サプライチェーン全体のサイバーセキュリティリスクを管理する上で重要である。サプライチェーン全体のサイバーセキュリティリスクの主な 2つの例として、悪意のあるコード及び偽造品の挿入があり、いずれもシステム及び情報の完全性の管理策を展開することで少なくとも部分的に対応することができる。事業体は、適切なシステム及び情報の完全性の保護が C-SCRM の一部であることを確実にすることが望ましい。

SI-1 ポリシー及び手順

補足 C-SCRM ガイダンス：事業体は、様々な完全性検証ツール及び技法の採用に関するプログラム固有の要件が明確に定義されていることを確実にすることを含め、システム及び情報の完全性のポリシー及び手順に C-SCRM を含めることが望ましい。情報システム、コンポーネント、及び基盤となる情報システム及びネットワークのシステム及び情報の完全性は、サプライチェーン全体のサイバーセキュリティリスクを管理する上で重要である。悪意のあるコード及び偽造品の挿入は、サプライチェーン全体のサイバーセキュリティリスクの主な 2つの例であり、いずれもシステム及び情報の完全性の管理策を展開することで少なくとも部分的に対応することができる。

レベル：1、2、3

関連管理策：SR-1、9、10、11

SI-2 欠陥の修正

補足 C-SCRM ガイダンス：欠陥の修正活動のアウトプットは、第 2 節及び附属書 C で説明する ICT/OT SCRM プロセスへの有用なインプットを提供する。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

拡張管理策：

(1) 欠陥の修正 | ソフトウェア及びファームウェアの自動更新

補足 C-SCRM ガイダンス：事業体は、その情報システム及びネットワーク内で、（間接的及び直接の両方の）自動更新を必要とする様々なソフトウェア資産を規定することが望ましい。この資産の規定は、重要な機能及びコンポーネントと重要ではない機能及びコンポーネントに関する情報を提供する重要度分析の結果から定義されることが望ましい（第 2 節及び附属書 C を参照）。展開前に更新を評価及び管理するためにパッチの一元管理プロセスを採用することができる。サプライヤからの直接更新を必要とするソフトウェア資産は、取得者がパッチ一元管理プロセスなどを使用して更新を特別に展開しない限り、OEM から直接提供された更新のみを受け入れることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2

SI-3 悪意のあるコードからの保護

補足 C-SCRM ガイダンス：連邦政府のシステムで動作するコードのほとんどは連邦政府によって開発されたものではないため、悪意のあるコードの脅威は多くの場合サプライチェーンから発生する。この管理策は、コードに関連する責任（コードの開発、パッチのインストール、システムアップグレードの実行など）を負う連邦政府機関及び請負業者と、該当する請負業者の情報システム及びネットワークに適用される。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：SA-11、SI-7(15)、SI-3(4)、(6)、(8) 及び (10)、SR-3(3)

SI-4 システム監視

補足 C-SCRM ガイダンス：この管理策には、ソフトウェア開発時に埋め込まれ、展開後に作動するように設定されていた悪意のあるコードなど、過去のサプライチェーンのサイバーセキュリティ侵害から発生した脆弱性の監視が含まれる。システム監視は外部サービスプロバイダによって行われることがよくある。このようなプロバイダとのサービス内容合意書は、この管理策を適切に反映するように構成されることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

拡張管理策：

(1) システム監視 | 統合された状況認識

補足 C-SCRM ガイダンス：システム監視情報は、必要に応じてサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダの情報と相関付けることができる。監視情報を相関付けた結果から、軽減が必要なサプライチェーンのサイバーセキュリティ脆弱性又は侵害が判明する可能性がある。

レベル：2、3

(2) システム監視 | 個人のリスク

補足 C-SCRM ガイダンス：高リスクとして識別される個人には、事業体の従業員、請負業者、及び事業体のシステム、ネットワーク、又はシステム環境へのアクセスを必要とするかアクセスすることができる可能性があるその他の第三者（ボランティア、訪問者など）が含まれる。事業体は、ポリシー、手順、及び該当する場合は合意書の諸条件に従い、適切な担当員と協力して、このような高リスクの個人を対象とする強化された監督機能を実装することができる。

レベル：2、3

SI-5 セキュリティのアラート、勧告、及び指令

補足 C-SCRM ガイダンス：事業体は、サプライチェーンのサイバーセキュリティの影響に関するセキュリティのアラート、勧告、及び指令を評価し、必要に応じてフォローアップを行うことが望ましい。US-CERT、FASC、及びその他の権威のあるエンティティが、C-SCRM に適用されるセキュリティアラート及び勧告を生成する。追加の法律及び規制は、追加の勧告の対象者及びその提供方法に影響する。事業体は、情報共有プロトコル及びプロセスに、製品の納入又はサービスの実行のための合意を得ている関係者とアラート、勧告、及び指令を共有することが含まれていることを確実にすることが望ましい。事業体は、そのようなアラート、勧告、及び指令に応じて取るべきアクションに関する方向性又はガイダンスを提供することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

SI-7 ソフトウェア、ファームウェア、及び情報の完全性

補足 C-SCRM ガイダンス：この管理策は、連邦政府機関及び該当するサプライヤの製品、アプリケーション、情報システム及びネットワークに適用される。サプライチェーンを通過するシステム／コンポーネントが予期しない変更の影響を受けないように完全性が必要に応じて維持されることを確実にするために、適用されるすべてのシステム及びネットワークの完全性が体系的にテスト及び検証されることが望ましい。システム及びコンポーネントの完全性もテスト及び検証されることが望ましい。該当する検証ツールには、デジタル署名又はチェックサム検証、物理コンポーネントの検収テスト、サンドボックスなどの限定特権環境へのソフトウェアの制限、使用前の隔離された環境におけるコードの実行、及びバイナリ又はマシン実行可能コードのみが使用可能な場合に、それが OEM 又は検証済みのサプライヤ又は販売代理事業者から直接得たコードであることを確実にすることなどが含まれる。この管理策のメカニズムについては、[NIST SP 800-53, Rev. 5]で詳述している。この管理策は連邦政府機関及び該当するサプライヤの情報システム及びネットワークに適用される。事業体は ICT/OT 製品の購入時に、サプライヤの完全性アシュアランスプラクティスを理解するために、デューデリジェンスを実施することが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：SR-3(3)

拡張管理策：

(1) ソフトウェア、ファームウェア、及び情報の完全性 | バイナリ又はマシン実行可能コード

補足 C-SCRM ガイダンス：事業体は、バイナリ又はマシン実行可能なコードを OEM ／開発者又はその他の検証済みの供給源から直接取得することが望ましい。

レベル：2、3

(2) ソフトウェア、ファームウェア、及び情報の完全性 | コード認証

補足 C-SCRM ガイダンス：事業体はソフトウェア、ファームウェア、及び情報の完全性を保証するために、デジタル署名などのコード認証メカニズムを実装することを確実にすることが望ましい。

レベル：3

SI-12 情報管理及び保持

補足 C-SCRM ガイダンス：特にシステムインテグレータ、サプライヤ、又は外部サービスプロバイダの機密情報が関係している場合は、C-SCRM を情報管理及び保持の要件に含めることが望ましい。

レベル：3

SI-20 汚染

補足 C-SCRM ガイダンス：サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダは、連邦政府機関の機密情報にアクセスできる可能性がある。この場合、事業体は一次請負業者に対し、この管理策を実装してこの要件を関連する二次請負業者にフローダウンすることを求めることが望ましい。

レベル：2、3

関連管理策：SR-9

ファミリー：サプライチェーンのリスクマネジメント

[FIPS 200]では、サプライチェーンのリスクマネジメントの最小セキュリティ要件を規定していない。[NIST SP 800-53, Rev.5]では新しい管理策ファミリーである「サプライチェーンのリスクマネジメント」が確立された。以下の補足ガイダンスは SR 管理策を詳しく説明し、詳細情報とその用途のコンテキストを提供する。これは SP 800-53, Rev. 5 の新しいファミリーであり、ガイダンスは SP 800-53, Rev. 5 に既に記載されている。本出版物（NIST SP 800-161, Rev. 1）には、SP 800-53, Rev. 5 のすべての SR 拡張管理策が記載されており、また以下の SR 管理策及びその拡張管理策が NIST SP 800-53, Rev. 5[SR-13]に追加されている 。読者は、本節に記載されている管理策と併せて NIST SP 800-53, Rev. 5 の SR 管理策を参照されたい。

SR-1 ポリシー及び手順

補足 C-SCRM ガイダンス：C-SCRM のポリシーはレベル 1 で事業体全体を対象に策定され、レベル 2 で特定のミッション及び機能を対象に策定されている。C-SCRM のポリシーは、深さと詳細さの度合いに応じてレベル 1、2、及び 3 で実装することができる。C-SCRM の手順はレベル 2 で特定のミッション及び機能を対象に策定され、レベル 3 で特定のシステムを対象に策定されている。情報セキュリティ、法務、リスクマネジメント、及び取得など（ただしこれらに限らない）の事業体の機能は、C-SCRM ポリシー及び手順の策定をレビューし、意見の一致を得るか、又はシステム固有の C-SCRM 手順の策定についてのガイダンスをシステム所有者に提供することが望ましい。

レベル：1、2、3

SR-2 サプライチェーンのリスクマネジメント計画

補足 C-SCRM ガイダンス：C-SCRM 計画は、システムレベルでの実装、要件、制約条件、及び影響を記述する。C-SCRM 計画は、事業体の他のリスクアセスメント活動の影響を受け、レベル 1 及びレベル 2 で定義された共通管理策ベースラインを継承してテーラリングすることができる。レベル 3 で定義された C-SCRM 計画は、事業体の C-SCRM 戦略及びポリシー（レベル 1 及びレベル 2）及び C-SCRM 実装計画（レベル 1 及びレベル 2）と連携して、事業体全体にわたるサプライチェーンのサイバーセキュリティリスクマネジメントへの体系的かつ包括的アプローチを提供する。

C-SCRM 計画は独立した文書として策定され、事業体の制約条件で必要となる場合にのみ既存のシステムセキュリティ計画に統合されることが望ましい。

レベル：3

関連管理策：PL-2

SR-3 サプライチェーンの管理策及びプロセス

補足 C-SCRM ガイダンス：本出版物の第 2 節及び附属書 C は、この管理策の実装に関する詳細なガイダンスを提供する。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's

Cybersecurity）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

拡張管理策：

(1) サプライチェーンの管理策及びプロセス | 多様な供給ベース

補足 C-SCRM ガイダンス：事業体は、重要な ICT/OT 製品及びサービスについて特に、その供給ベースを多様化することが望ましい。この演習の一環として、事業体はサプライチェーンの一次エンティティ及び下層エンティティにおける単一障害点とリスクの識別を試行することが望ましい。重要度分析の実施に関するガイダンスについては、第 2 節、附属書 C、及び RA-9 を参照。

レベル：2、3

関連管理策：RA-9

(2) サプライチェーンの管理策及びプロセス | 下層フローダウン

補足 C-SCRM ガイダンス：事業体は一次請負業者に対し、この管理策を実装し、この要件を SDLC 全体で関連する二次請負業者にフローダウンすることを求めることが望ましい。取得プロセスを使用することで、サプライチェーンを保護するための重要な手段が提供される。事業体は、調達要件の一部として、サプライヤが SDLC 全体で管理策を二次請負業者にフローダウンする必要性を含めることが望ましい。市場調査及び分析活動の一環として、事業体は潜在的なサプライヤ又は製品とその上流への依存関係（フォース及びフィフスパーティサプライヤなど）に対し、堅牢なデューデリジェンス調査を実施することが望ましく、これは事業体がサプライチェーン内での単一障害点を回避するのに役立つ可能性がある。この調査の結果は、調達アプローチの形成及び要件の調整に役立つ可能性がある。包括的なリスクプロファイルが十分に理解され、受注決定時に重み付け因子として機能することを確実にするために、サプライヤ、製品、又はサービスから発生するサイバーセキュリティリスクの評価は、契約受注決定の前に完了しておくことが望ましい。履行期間中は、定義されている管理策及び要件にサプライヤが準拠しているかどうかと、リスク状態の変化が監視されることが望ましい。取得プロセスにおける C-SCRM の役割に関するガイダンスについては、第 3 節を参照。

レベル：2、3

SR-4 来歴

補足 C-SCRM ガイダンス：SDLC 全体にわたって、システム、システムコンポーネント、及び関連データの来歴を文書化することが望ましい。事業体は、購入したソフトウェア、オープンソースソフトウェア、社内開発ソフトウェアを含む、適用可能で適切なソフトウェアクラスの SBOM の作成を検討することが望ましい。SBOM を作成するときには、[NTIA SBOM]EO 14028 NTIA SBOM 最小要素を満たすことが可能な、NTIA によりサポートされている SBOM フォーマットのみを使用することが望ましい。SBOM を作成する事業体は、プライマリコンポーネントの包含の枠組みとして[NTIA SBOM]SBOM 最小要

素を使用することが望ましい。SBOM には、検証可能な信頼できる鍵を使用してデジタル署名することが望ましい。SBOM は、組織が来歴を維持することができるようにする上で重要な役割を果たす可能性がある。ただし、SBOM の成熟に伴い、組織は SBOM が既存の C-SCRM ケイパビリティ（能力）（脆弱性管理行為、ベンダリスクアセスメントなど）に取って代わるという誤った前提に基づいて、これらのケイパビリティ（能力）の優先順位を下げることがないことを確実にすることが望ましい。SBOM と、SBOM が組織にもたらす向上した透明性は、代用となるケイパビリティ（能力）ではなく、補完的なケイパビリティ（能力）である。SBOM が提供するデータを適切に取り込み、分析し、このデータに基づいて行動することができない組織では、その全体的な C-SCRM 態勢が改善されることは恐らくない。連邦政府機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

SR-5 取得戦略、ツール、及び方法

補足 C-SCRM ガイダンス：第 3 節及び SA 管理策は、取得戦略、ツール、及び方法に関する追加のガイダンスを提供する。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（Improving the Nation's Cybersecurity）」に従って本ガイダンスを実装することが望ましい。
レベル：1、2、3

関連管理策：SA 管理策ファミリー

SR-6 サプライヤのアセスメント及びレビュー

補足 C-SCRM ガイダンス：一般に、事業体はサプライヤ若しくはサプライヤが提供するサービス又は製品のセキュリティ、完全性、レジリエンス、品質、統合的信頼性、又は真正性に関連するあらゆる情報を考慮することが望ましい。事業体は（長期的なサプライヤ間の）公平な比較を容易にするために、整合性のある一連のコアベースライン要因及びアセスメント基準にこの情報を適用することを検討することが望ましい。アセスメントを実施している特定のコンテキスト及び目的に応じて、事業体は追加の要因を選択することができる。アセスメントで使用される情報の品質（情報の関連性、網羅性、正確性など）も、重要な考慮事項である。アセスメント情報の参照元も文書化することが望ましい。C-SCRM PMO は、事業体のサプライヤアセスメントの要件、方法、及びツールを定義するのに役立つ可能性がある。各省庁及び関係機関は、附属書 E を参照してベースラインリスク要因及びアセスメントの文書化に関連する詳細なガイダンスを得て、附属書 F を参照して大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

SR-7 サプライチェーン運用セキュリティ

補足 C-SCRM ガイダンス：C-SCRM PMO は、特定のミッション及び機能に適用される OPSEC 管理策を判断するのに役立つ可能性がある。事業体のサプライチェーン又はサプラ

イチェーン内の要素から生じる敵対的脅威、又はこれらに対する敵対的脅威についての具体的な懸念がある場合、若しくは事業体のミッション又はビジネスの業務、その情報、及び／又はサービス／製品の性質から、事業体が敵対的脅威に対してより格好の標的になるときには、OPSEC 管理策は特に重要である。

レベル：2、3

SR-8 通知協定

補足 C-SCRM ガイダンス：事業体は最低でも、サプライヤに対し、サプライチェーン内で重要なサービス又は製品に関連する役割又は責任を担うエンティティとの間に、通知協定を締結することを求めることが望ましい。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：RA-9

SR-9 耐タンパー性及び検知

補足 C-SCRM ガイダンス：事業体は、耐タンパー性及び検知の管理策を、少なくとも重要なコンポーネントに適用することが望ましい。重要度分析は、どのコンポーネントが重要であるかを判断するのに役立つ可能性がある。重要度分析の実施に関するガイダンスについては、第 2 節、附属書 C、及び RA-9 を参照。C-SCRM PMO は、事業体内の重要なコンポーネント、特に複数のミッション、機能、及びシステムが使用するコンポーネントを識別するのに役立つ可能性がある。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：2、3

関連管理策：RA-9

SR-10 システム又はコンポーネントの検査

補足 C-SCRM ガイダンス：事業体は、耐タンパー性管理策が導入されていることを保証し、タンパー（改ざん）の証拠があるかどうかを調べるために、少なくとも、重要なシステム及びコンポーネントを検査することが望ましい。製品又はコンポーネントの検査は、使用前とそれ以降に定期的に実施されることが望ましい。検査の要件は、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他の ICT/OT 関連のサービスプロバイダとの契約にも含まれることが望ましい。事業体は一次請負業者に対し、この管理策を実装してこの要件を必要に応じて関連する二次請負業者にフローダウンすることを求めることが望ましい。

重要度分析は、どのシステムとコンポーネントが重要であり、調査の対象とするべきかを判断するのに役立つ可能性がある。重要度分析の実施に関するガイダンスについては、第

2 節、附属書 C、及び RA-9 を参照。C-SCRM PMO は、事業体内の重要なシステム及びコンポーネント、特に複数のミッション、機能、及びシステム（コンポーネントの場合）が使用するシステム及びコンポーネントを識別するのに役立つ可能性がある。

レベル：2、3

関連管理策：RA-9

SR-11 コンポーネントの真正性

補足 C-SCRM ガイダンス：偽造防止のポリシー及び手順を策定するには、取得、情報技術、IT セキュリティ、法務、及び C-SCRM PMO からのインプット及びこれらとの協力が必要である。ポリシー及び手順では、GIDEP 及び／又はその他の適切な事業体などの事業体に対する規制コンプライアンスの要件、契約の要件又は条項、及び偽造品報告プロセスを扱うことが望ましい。適用可能かつ適切な場合には、ポリシーで有資格入札者リスト（QBL）及び／又は有資格製造業者リスト（QML）の策定と使用も扱うことが望ましい。これにより、可能な場合には常に認可されたサプライヤを利用し、組織のサプライチェーンにこれらのサプライヤを統合することで、偽造品を防止することができる[CISA SCRM WG3]。各省庁及び関係機関は附属書 F を参照し、大統領令 14028 号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

レベル：1、2、3

拡張管理策：

(1) コンポーネントの真正性 | 偽造防止トレーニング

補足 C-SCRM ガイダンス：C-SCRM PMO は、偽造防止トレーニングを提供でき、及び／又は事業体に対してこのようなトレーニングを実施することができる可能性があるリソースを識別するのを支援することができる。C- SCRM PMO は、トレーニングを受講することが望ましい人員の識別も支援することができる。

レベル：2、3

(2) コンポーネントの真正性 | コンポーネントのサービス及び修理のための構成管理

補足 C-SCRM ガイダンス：該当する場合にはコンポーネントのサービス及び修理を事業体の全体的な構成管理プロセスに統合することを含めるために、情報技術、IT セキュリティ、又は C-SCRM PMO がコンポーネントのサービス及び修理の構成管理プロセスを確立及び実装する責任を負うことが望ましい。コンポーネントの真正性は、コンポーネントのサービス及び修理のサポートを調達するときに契約に記載することが望ましい。

レベル：2、3

(3) コンポーネントの真正性 | 偽造防止の精査

補足 C-SCRM ガイダンス：事業体は、最低でも重要なコンポーネントに対して偽造防止の精査を実施することが望ましい。重要度分析は、どのコンポーネントが重要であり、この精査の対象とするべきかを判断するのに役立つ。重要度分析の実施に関するガイダンスについては、第 2 節、附属書 C、及び RA-9 を参照。C-SCRM PMO は、事業体内の重要なコンポーネント、特に複数のミッション、機能、及びシステムが使用するコンポーネントを識別するのに役立てることができる。

レベル：2、3

関連管理策：RA-9

SR-12 コンポーネントの廃棄

補足 C-SCRM ガイダンス： IT セキュリティは C-SCRM PMO と連携して適切なコンポーネント廃棄のポリシー、手順、メカニズム、及び技法を確立するのに役立てることができる。

レベル：2、3

SR-13 サプライヤのインベントリ（新規）

管理策：

a. 以下のようなサプライヤのインベントリを策定、文書化、及び維持する。

   1. サプライチェーンのサイバーセキュリティリスクを表す可能性がある組織のティア 1 サプライヤを正確かつ最小限に反映する[設定：ティア 1 サプライチェーンを判断するための組織が定めるパラメータ]。

   2. 重要度及びサプライチェーンのリスクのアセスメント、追跡、及び報告に必要と思われる細分性のレベルである。

   3. ティア 1 サプライヤ（一次請負業者など）の以下の情報を文書化する：サプライヤのインベントリをレビュー及び更新する[設定：事業体が定める頻度]。

      i. 調達手段（すなわち、契約、タスク、又は納入指示）の一意の識別。
      ii. 供給される製品及び／又はサービスの説明
      iii. サプライヤの製品及び／又はサービスを使用するプログラム、プロジェクト、及び／又はシステム
      iv. プログラム、プロジェクト及び／又はシステム（あるいはシステムのコンポーネント）の重要度に整合する割り当てられた重要度レベル

b. サプライヤのインベントリをレビュー及び更新する[設定：事業体が定める頻度]。

補足 C-SCRM ガイダンス：事業体は、そのミッション及び機能を実行する上で多数のサプライヤに依存している。多くのサプライヤは、複数のミッション、機能、プログラム、プロジェクト、及びシステムをサポートする製品及びサービスを提供する。サプライヤの製品及びサービスがサポートするミッション、機能、プログラム、プロジェクト、システム、及びサプライヤへの事業体の依存度に基づいて、一部のサプライヤの重要度が他のサプラ

イヤよりも高いことがある。事業体は、サプライヤのインベントリに記載するサプライヤの重要度を判断するために、重大度分析を使用してどの製品及びサービスが重要であるかを判断することが望ましい。重要度分析の実施に関するガイダンスについては、第 2 節、附属書 C、及び RA-9 を参照。

レベル：2、3

関連管理策：RA-9

附属書 B：C-SCRM 管理策の概要

この附属書では、本出版物内の C-SCRM 管理策をリスト化し、必要に応じて、それらの管理策を対応する[NIST SP 800-53, Rev. 5]の管理策にマッピングしている。表 B-1 は、[NIST SP 800-53, Rev. 5]で定義されているそうした管理策を示している。低いベースライン要件は、C-SCRM に関連するものと見なされる。いくつかの C-SCRM 管理策が、C-SCRM ベースラインを形成するために、この管理策セットに追加された。さらに、一次請負業者から関連する二次請負業者にフローダウンするべき管理策は、フローダウン管理策としてリスト化されている。C-SCRM が、事業体、ミッション及びビジネス、並びに運用レベル（[NIST SP 800-39]に従えば、事業体のレベル 1、2、及び 3）での管理策の選択及び実装を必要とする、組織全体の活動であることを考慮し、表 B-1 では、管理策が実装されるべき事業体のレベルを示している。[NIST SP 800-53, Rev.5]にない C-SCRM 管理策及び拡張管理策は、管理策識別子の横にアスタリスクで注が付けられている（すなわち、MA-8 及び SR-13）。

表 B-1：C-SCRM 管理策の概要

				レベル		
管理策識別子	**管理策（又は拡張管理策）名**	**C-SCRM ベースライン**	**フローダウン管理策**	**1**	**2**	**3**
AC-1	**ポリシー及び手順**	x	x	x	x	x
AC-2	**アカウント管理**	x	x		x	x
AC-3	**アクセス実施**	x	x		x	x
AC-3(8)	アクセス実施 | アクセス認可の取り消し				x	x
AC-3(9)	アクセス実施 | 管理されたリリース				x	x
AC-4	**情報フローの実施**		x		x	x
AC-4(6)	情報フローの実施 | メタデータ				x	x
AC-4(17)	情報フローの実施 | ドメイン認証				x	
AC-4(19)	情報フローの実施 | メタデータの検証					
AC-4(21)	情報フローの実施 | 情報フローの物理的又は論理的分離					x
AC-5	**職務の分離**		x		x	x
AC-6(6)	最小特権 | 非組織ユーザによる特権アクセス				x	x
AC-17	**リモートアクセス**	x	x		x	x
AC-17(6)	リモートアクセス | メカニズムに関する情報の保護				x	x
AC-18	**ワイヤレスアクセス**	x		x	x	x
AC-19	**モバイルデバイスのアクセス制御**	x			x	x
AC-20	**外部システムの使用**	x	x	x	x	x
AC-20(1)	外部システムの使用 | 認可された使用に限定				x	x
AC-20(3)	外部システムの使用 | 組織が所有していないシステム — 使用制限				x	x
AC-21	**情報共有**			x	x	
AC-22	**公的にアクセス可能なコンテンツ**	x			x	x
AC-23	**データマイニングの保護**		x		x	x
AC-24	**アクセス制御の決定**		x	x	x	x

				レベル		
管理策識別子	**管理策（又は拡張管理策）名**	**C-SCRM ベースライ**	**フローダウン管理策**	**1**	**2**	**3**
AT-1	**ポリシー及び手順**	x		x	x	
AT-2(1)	リテラシートレーニング及び意識向上 | 実践的な演習				x	
AT-2(2)	リテラシートレーニング及び意識向上 | インサイダー脅威	x	x		x	
AT-2(3)	リテラシートレーニング及び意識向上 | ソーシャルエンジニアリング及びマイニング				x	
AT-2(4)	リテラシートレーニング及び意識向上 | 疑わしい通信及び異常なシステム動作				x	
AT-2(5)	リテラシートレーニング及び意識向上 | 持続的標的型攻撃（*APT* 攻撃）				x	
AT-2(6)	リテラシートレーニング及び意識向上 | サイバー脅威環境				x	
AT-3	**役割ベースのトレーニング**	x	x		x	
AT-3(2)	役割ベースのトレーニング | 物理的セキュリティ管理策				x	
AT-4	**トレーニングの記録**	x			x	
AU-1	**ポリシー及び手順**	x		x	x	x
AU-2	**イベントロギング**	x	x	x	x	x
AU-3	**監査記録の内容**	x	x	x	x	x
AU-6	**監査記録のレビュー、分析、及び報告**	x			x	x
AU-6(9)	監査記録のレビュー、分析、及び報告 | 非技術的ソースからの情報との相関					x
AU-10	**否認防止**					x
AU-10(1)	否認防止 | アイデンティティとの関連性				x	
AU-10(2)	否認防止 | 情報作成者のアイデンティティのバインディングの妥当性確認				x	x
AU-10(3)	否認防止 | 過程管理				x	x
AU-12	**監査記録の生成**	x	x		x	x
AU-13	**情報開示の監視**		x		x	x
AU-14	**セッション監査**		x		x	x
AU-16	**組織横断的監査ロギング**				x	x
AU-16(2)	組織横断的監査ロギング | 監査情報の共有				x	x
CA-1	**ポリシー及び手順**	x		x	x	x
CA-2	**管理策アセスメント**	x			x	x

管理策識別子	管理策（又は拡張管理策）名	C-SCRM ベースライン	フローダウン管理策	レベル 1	レベル 2	レベル 3
CA-2(2)	管理策アセスメント | 特化したアセスメント					x
CA-2(3)	管理策アセスメント | 外部組織からの結果の活用					x
CA-3	**情報交換**	x	x			x
CA-5	**実施計画及びマイルストーン**	x			x	x
CA-6	**認可**	x		x	x	x
CA-7(3)	継続的監視 | トレンド分析					x
CM-1	**ポリシー及び手順**	x		x	x	x
CM-2	**ベースライン構成**	x	x		x	x
CM-2(6)	ベースライン構成 | 開発及びテスト環境				x	x
CM-3	**構成変更管理**		x		x	x
CM-3(1)	構成変更管理 | 自動化された文書化、通知、及び変更禁止				x	x
CM-3(2)	構成変更管理 | 変更のテスト、妥当性確認、及び文書化				x	x
CM-3(4)	構成変更管理 | セキュリティ及びプライバシーに関する代表者				x	x
CM-3(8)	構成変更管理 | 構成の変更の防止又は制限				x	x
CM-4	**インパクト分析**	x				x
CM-4(1)	インパクト分析 | 独立したテスト環境					x
CM-5	**変更に対するアクセス制限**	x			x	x
CM-5(1)	変更に対するアクセス制限 | 自動化されたアクセス実施及び監査記録					x
CM-5(6)	変更に対するアクセス制限 | ライブラリに関する特権の限定					x
CM-6	**構成設定**	x	x		x	x
CM-6(1)	構成設定 | 自動化された管理、適用、及び検証					x
CM-6(2)	構成設定 | 認可されていない変更への対応					x
CM-7	**最小機能性**	x	x			x
CM-7(1)	最小機能性 | 定期的なレビュー				x	x
CM-7(4)	最小機能性 | 認可されていないソフトウェア				x	x
CM-7(5)	最小機能性 | 認可されたソフトウェア					x
CM-7(6)	最小機能性 | 限定された特権を備えた制限環境				x	x
CM-7(7)	最小機能性 | 保護された環境内でのコードの実行					x

				レベル		
管理策識別子	**管理策（又は拡張管理策）名**	**C-SCRM ベースライ**	**フローダウン管理策**	**1**	**2**	**3**
CM-7(8)	最小機能性 | バイナリ又はマシン実行可能コード				x	x
CM-7(9)	最小機能性 | 認可されていないハードウェアの使用の禁止				x	x
CM-8	**システムコンポーネントのインベントリ**	x	x		x	x
CM-8(1)	システムコンポーネントのインベントリ | インストール中及び削除中の更新					x
CM-8(2)	システムコンポーネントのインベントリ | 自動化されたメンテナンス					x
CM-8(4)	システムコンポーネントのインベントリ | 説明責任情報					x
CM-8(6)	システムコンポーネントのインベントリ | アセスメント済みの構成及び承認された偏差					x
CM-8(7)	システムコンポーネントのインベントリ | 集中化されたリポジトリ					x
CM-8(8)	システムコンポーネントのインベントリ | 自動化された位置追跡機能				x	x
CM-8(9)	システムコンポーネントのインベントリ | システムへのコンポーネントの設定					x
CM-9	**構成管理計画**		x		x	x
CM-9(1)	構成管理計画 | 責任の設定				x	x
CM-10	**ソフトウェアの使用制限**	x			x	x
CM-10(1)	ソフトウェアの使用制限 | オープンソースソフトウェア				x	x
CM-11	**ユーザがインストールしたソフトウェア**	x			x	x
CM-12	**情報の位置**				x	x
CM-12(1)	情報の位置 | 情報の位置をサポートする自動化されたツール				x	x
CM-13	**データアクションのマッピング**				x	x
CM-14	**署名されたコンポーネント**					x
CP-1	**ポリシー及び手順**	x		x	x	x
CP-2	**緊急時対応計画**	x			x	x
CP-2(1)	緊急時対応計画 | 関連計画との調整				x	x
CP-2(2)	緊急時対応計画 | 処理能力計画				x	x
CP-2(7)	緊急時対応計画 | 外部サービスプロバイダとの調整		x			x
CP-2(8)	緊急時対応計画 | 重要な資産の特定					x
CP-3	**緊急時対応トレーニング**	x	x		x	x

				レベル		
管理策識別子	**管理策（又は拡張管理策）名**	**C-SCRM ベースライン**	**フローダウン管理策**	**1**	**2**	**3**
CP-3(1)	緊急時対応トレーニング | シミュレーション イベント				x	x
CP-4	**緊急時対応計画テスト**	x			x	x
CP-6	**代替保管サイト**				x	x
CP-6(1)	代替保管サイト | 一次サイトからの分離				x	x
CP-7	**代替処理サイト**				x	x
CP-8	**通信サービス**				x	x
CP-8(3)	通信サービス | 一次プロバイダ及び 代替プロバイダの分離				x	x
CP-8(4)	通信サービス | プロバイダの緊急時対応計画				x	x
CP-11	**代替通信プロトコル**				x	x
IA-1	**ポリシー及び手順**	x		x	x	x
IA-2	**識別及び認証（組織のユーザ）**	x	x	x	x	x
IA-3	**デバイスの識別及び認証**			x	x	x
IA-4	**識別子管理**	x	x		x	x
IA-4(6)	識別子管理 | 組織横断的な管理			x	x	x
IA-5	**オーセンティケータ管理**	x	x		x	x
IA-5(5)	オーセンティケータ管理 | 出荷前のオーセンティケータ変更					x
IA-5(9)	オーセンティケータ管理 | フェデレーションによるクレデンシャル管理					x
IA-8	**識別及び認証（非組織のユーザ）**	x			x	x
IA-9	**サービスの識別及び認証**		x		x	x
IR-1	**ポリシー及び手順**	x	x	x	x	x
IR-2	**インシデント対応トレーニング**	x	x		x	x
IR-3	**インシデント対応テスト**				x	x
IR-4(6)	インシデント対応 | インサイダー脅威			x	x	x
IR-4(7)	インシデント対応 | インサイダー脅威 — 組織内連携			x	x	x
IR-4(10)	インシデント対応 | サプライチェーンとの連携		x		x	
IR-4(11)	インシデント対応 | 統合インシデント対応チーム					x
IR-5	**インシデント監視**	x			x	x
IR-6(3)	インシデント報告 | サプライチェーンとの連携		x			x
IR-7(2)	インシデント対応支援 | 外部プロバイダとの連携		x			X
IR-8	**インシデント対応計画**	x	x		x	x
IR-9	**情報流出対応**		x			x
MA-1	**ポリシー及び手順**	x	x	x	x	x
MA-2(2)	管理されたメンテナンス | 自動化されたメンテナンス措置					x
MA-3	**メンテナンスツール**				x	x

				レベル		
管理策識別子	**管理策（又は拡張管理策）名**	**C-SCRM ベースライ**	**フローダウン管理策**	**1**	**2**	**3**
MA-3(1)	メンテナンスツール | ツールの検査					x
MA-3(2)	メンテナンスツール | 媒体の検査					x
MA-3(3)	メンテナンスツール | 認可されていない移動の防止					x
MA-4	**非ローカルメンテナンス**	x	x		x	x
MA-4(3)	非ローカルメンテナンス | 同等のセキュリティ及びサニタイズ				x	x
MA-5	**メンテナンス作業員**	x			x	x
MA-5(4)	メンテナンス作業員 | 外国人		x		x	x
MA-6	**タイムリーなメンテナンス**					x
MA-7	**フィールドメンテナンス**					x
MA-8	**メンテナンス監視及び情報共有**					x
MP-1	**ポリシー及び手順**	x		x	x	
MP-4	**媒体保管**		x	x	x	
MP-5	**媒体移送**			x	x	
MP-6	**媒体のサニタイズ**	x	x		x	x
PE-1	**ポリシー及び手順**	x		x	x	x
PE-2	**物理的アクセス認可**	x	x		x	x
PE-2(1)	物理的アクセス認可 | 職位又は役割によるアクセス				x	x
PE-3	**物理的アクセス制御**	x			x	x
PE-3(1)	物理的アクセス制御 | システムアクセス				x	x
PE-3(2)	物理的アクセス制御 | 施設及びシステム				x	x
PE-3(5)	物理的アクセス制御 | タンパー保護				x	x
PE-6	**物理的アクセスの監視**	x		x	x	x
PE-16	**搬入及び搬出**	x				x
PE-17	**代替作業サイト**					x
PE-18	**システムコンポーネントの設置場所**			x	x	x
PE-20	**資産の監視及び追跡**				x	x
PE-23	**施設の場所**		x		x	x
PL-1	**ポリシー及び手順**	x			x	
PL-2	**システムセキュリティ及びプライバシー計画**	x	x			x
PL-4	**行動規則**	x			x	x
PL-7	**業務構想文書**					x
PL-8	**セキュリティ及びプライバシーアーキテクチャ**				x	x
PL-8(2)	セキュリティ及びプライバシーアーキテクチャ | サプライヤの多様性				x	x
PL-9	**一元管理**			x	x	
PL-10	**ベースラインの選択**	x			x	x

				レベル		
管理策識別子	管理策（又は拡張管理策）名	C-SCRM ベースライン	フローダウン管理策	1	2	3
PM-2	情報セキュリティプログラムの責任者の役割			x	x	
PM-3	情報セキュリティ及びプライバシーリソース			x	x	
PM-4	行動計画及びマイルストーンプロセス				x	x
PM-5	システムインベントリ		x		x	x
PM-6	パフォーマンス尺度			x	x	
PM-7	エンタープライズアーキテクチャ			x	x	
PM-8	重要インフラ計画			x		
PM-9	リスクマネジメント戦略			x		
PM-10	認可プロセス			x	x	
PM-11	ミッション及び事業プロセスの規定			x	x	x
PM-12	インサイダー脅威対策プログラム			x	x	x
PM-13	セキュリティ及びプライバシー要員			x	x	
PM-14	テスト、トレーニング、及び監視			x	x	
PM-15	セキュリティ及びプライバシーのグループ及び団体			x	x	
PM-16	脅威認識プログラム			x	x	
PM-17	外部システム上の管理対象非機密情報の保護				x	
PM-18	プライバシープログラム計画		x	x	x	
PM-19	プライバシープログラムの責任者の役割			x		
PM-20	プライバシープログラム情報の配布			x	x	
PM-21	開示事項のアカウンティング			x	x	
PM-22	個人情報の品質管理			x	x	
PM-23	データガバナンス会議体			x		
PM-25	テスト、トレーニング、及び研究で使用される個人情報の最小化				x	
PM-26	苦情管理				x	x
PM-27	プライバシー報告				x	x
PM-28	リスクの枠組み			x		
PM-29	リスクマネジメントプログラムの責任者の役割			x		
PM-30	サプライチェーンのリスクマネジメント戦略			x	x	
PM-31	継続的監視戦略			x	x	x
PM-32	目的				x	x
PS-1	ポリシー及び手順	x	x	x	x	x
PS-3	職員のスクリーニング	x	x		x	x
PS-6	アクセス合意書	x	x		x	x
PS-7	外部職員のセキュリティ	x			x	
PT-1	ポリシー及び手順		x	x	x	x

				レベル		
管理策識別子	**管理策（又は拡張管理策）名**	**C-SCRM ベースライン**	**フローダウン管理策**	**1**	**2**	**3**
RA-1	**ポリシー及び手順**	x		x	x	x
RA-2	**セキュリティ分類化**	x		x	x	x
RA-3	**リスクアセスメント**	x		x	x	x
RA-5	**脆弱性の監視及びスキャン**	x	x		x	x
RA-5(3)	脆弱性の監視及びスキャン | カバレッジの幅及び深さ				x	x
RA-5(6)	脆弱性の監視及びスキャン | 自動化された傾向分析				x	x
RA-7	**リスク対応**	x		x	x	x
RA-9	**重要度分析**		x	x	x	x
RA-10	**脅威ハンティング**			x	x	x
SA-1	**ポリシー及び手順**	x		x	x	x
SA-2	**リソースの割り当て**	x		x	x	
SA-3	**システム開発ライフサイクル**	x		x	x	x
SA-4	**取得プロセス**	x		x	x	x
SA-4(5)	取得プロセス | システム、コンポーネント、及びサービスの構成					x
SA-4(7)	取得プロセス | *NIAP* 承認済みプロテクションプロファイル				x	x
SA-4(8)	取得プロセス | 管理策の継続的監視計画				x	x
SA-5	**システムドキュメント**	x				x
SA-8	**セキュリティ及びプライバシーエンジニアリングの原則**	x		x	x	x
SA-9(1)	外部システムサービス | リスクアセスメント及び組織承認				x	x
SA-9(3)	外部システムサービス | プロバイダとの信頼関係の確立及び維持			x	x	x
SA-9(4)	外部システムサービス | 消費者及びプロバイダの一貫した利益					x
SA-9(5)	外部システムサービス | 処理、保管、及びサービスの場所					x
SA-10	**開発者構成管理**				x	x
SA-11	**開発者のテスト及び評価**			x	x	x
SA-15	**開発プロセス、規格、及びツール**				x	x
SA-15(3)	開発プロセス、規格、及びツール | 重要度分析				x	x
SA-15(4)	開発プロセス、規格、及びツール | 脅威のモデル化及び脆弱性の分析				x	x
SA-15(8)	開発プロセス、規格、及びツール | 脅威及び脆弱性情報の再利用					x
SA-16	**開発者が提供するトレーニング**				x	x

管理策識別子	管理策（又は拡張管理策）名	C-SCRM ベースライ	フローダウン管理策	レベル 1	2	3
SA-17	**開発者のセキュリティ及びプライバシーのアーキテクチャ及び設計**				x	x
SA-20	**重要コンポーネントのカスタム開発**				x	x
SA-21	**開発者のスクリーニング**		x		x	x
SA-21(1)	開発者のスクリーニング | スクリーニングの妥当性確認				x	x
SA-22	**サポートされていないシステムコンポーネント**	x			x	x
SC-1	**ポリシー及び手順**	x		x	x	x
SC-4	**共有システムリソース内の情報**				x	x
SC-5(2)	サービス拒否からの保護 | 容量、帯域幅、及び冗長性				x	
SC-7	**境界保護**	x	x		x	
SC-7(13)	境界保護 | セキュリティツール、メカニズム、及びサポートコンポーネントの分離		x			x
SC-7(14)	境界保護 | 認可されていない物理的接続からの保護				x	x
SC-7(19)	境界保護 | 組織外で構成されたホストからの通信のブロック					x
SC-8	**伝送の機密性及び完全性**		x		x	x
SC-18	**モバイルコード**					x
SC-18(2)	モバイルコード | 取得、開発、及び使用					x
SC-27	**プラットフォームに依存しないアプリケーション**				x	x
SC-28	**保管中の情報の保護**		x		x	x
SC-29	**異質性**				x	x
SC-30	**秘匿化及び誤認誘導**				x	x
SC-30(2)	秘匿化及び誤認誘導 | ランダム性				x	x
SC-30(3)	秘匿化及び誤認誘導 | 処理場所及び保管場所の変更				x	x
SC-30(4)	秘匿化及び誤認誘導 | 誤解を招く情報				x	x
SC-30(5)	秘匿化及び誤認誘導 | システムコンポーネントの秘匿化				x	x
SC-36	**分散処理及びストレージ**		x		x	x
SC-37(1)	帯域外チャネル | 確実な配信及び送信				x	x
SC-38	**運用セキュリティ**				x	x
SC-47	**代替通信経路**			x	x	x
SI-1	**ポリシー及び手順**	x		x	x	x
SI-2	**欠陥の修正**	x	x		x	x
SI-2(5)	欠陥の修正 | ソフトウェア及びファームウェアの自動更新				x	

SI-3	**悪意のあるコードからの保護**	x	x		x	x
SI-4	**システム監視**	x	x	x	x	x
SI-4(17)	システム監視 | 統合された状況認識				x	x
SI-4(19)	システム監視 | 個人のリスク				x	x
SI-5	**セキュリティのアラート、勧告、及び指令**	x	x	x	x	x
SI-7	**ソフトウェア、ファームウェア、及び情報の完全性**	x	x		x	x
SI-7(14)	ソフトウェア、ファームウェア、及び情報の完全性 | バイナリ又はマシン実行可能コード				x	x
SI-7(15)	ソフトウェア、ファームウェア、及び情報の完全性 | コード認証					x
SI-12	**情報管理及び保持**	x				x
SI-20	**汚染**		x		x	x
SR-1	**ポリシー及び手順**	x		x	x	x
SR-2	**サプライチェーンのリスクマネジメント計画**	x				x
SR-3	**サプライチェーンの管理策及びプロセス**	x		x	x	x
SR-3(1)	サプライチェーンの管理策及びプロセス | 多様な供給ベース				x	x
SR-3(3)	サプライチェーンの管理策及びプロセス | 下層フローダウン		x		x	x
SR-4	**来歴**				x	x
SR-5	**取得戦略、ツール、及び方法**	x		x	x	x
SR-6	**サプライヤのアセスメント及びレビュー**				x	x
SR-7	**サプライチェーン運用セキュリティ**				x	x
SR-8	**通知協定**	x			x	x
SR-9	**耐タンパー性及び検知**				x	x
SR-10	**システム又はコンポーネントの検査**	x	x		x	x
SR-11	**コンポーネントの真正性**	x		x	x	x
SR-11(1)	コンポーネントの真正性 | 偽造防止トレーニング	x			x	x
SR-11(2)	コンポーネントの真正性 | コンポーネントのサービス	x			x	x
SR-11(3)	コンポーネントの真正性 | 偽造防止の精査				x	x
SR-12	**コンポーネントの廃棄**	x			x	x
SR-13	**サプライヤのインベントリ**				x	x

附属書 C：リスクレベルフレームワーク [38]

事業体環境又はそのシステム／要素にインパクトを与える脆弱性が、意図的又は無意識的にサプライチェーン全体にわたって挿入される、生み出される、又は悪用される機会は数多く存在する。これらの脆弱性の悪用は、サプライチェーン脅威事象と呼ばれている。脅威シナリオは、ある特定の潜在的な脅威源又は識別された既存の脅威源、又は複数の脅威源に関連付けられた、部分的に時系列で順序付けられた、一連の別個の脅威事象である。脅威シナリオの策定と分析は、発生する可能性のある様々な種類の脅威事象を事業体がより包括的に理解し、特定の事象の起こりやすさ及びそれによる事業体へのインパクトを分析するための基礎を築くのに役立つ。この分析を実施することは、管理策のギャップを発見し、適切な軽減戦略を識別し、優先順位を付けるのに有効な方法である。[39]

脅威シナリオは、一般的に以下の 2 つの方法で使用される。

1. [NIST SP 800-30、Rev. 1]で説明されているように、リスクアセスメントから得られた、断片的であることの多い情報を、より狭い範囲の具体的なストーリーのような状況に変換して、さらなる評価を行う。これらのストーリーは、事業体が依存関係を発見したり、軽減を必要とする追加の脆弱性を発見したりするのに役立つほか、トレーニングにも使用される。

2. 特定の脆弱性の発動に成功した場合に事業体に与えるインパクトを判別し、軽減戦略のメリットを識別する。

脅威シナリオは、本出版物の附属書 G で説明しているように、事業体のサプライチェーンのサイバーセキュリティリスクマネジメントプロセスの重要なコンポーネントとして機能する。事業体は、一連の様々な脅威及び脆弱性の条件を分析し、リスクアセスメントの一環として分析できる、まとまりのあるストーリーを組み立てるために、脅威シナリオを作成する。脅威シナリオが定義されると、事業体はリスクアセスメントを実施して、そのシナリオが現実のものになる可能性がどのくらいあり、その結果として何が起こるか（すなわち、インパクト）を把握することができる。最終的には、分析した脅威シナリオの要素を使用して、サプライチェーン全体のサイバーセキュリティリスクへの事業体の曝露（エクスポージャー）レベルの結論を表すリスク判断が行われる。

リスク判断が行われると、事業体はリスクレベルフレームワークを使用して、リスクに対応するための道筋を決定する。リスクレベルフレームワーク内で、事業体は脅威シナリオ、リスク分析、識別されたリスク対応戦略、及び関連する C-SCRM 管理策を文書化する。

この附属書では、自らのニーズに最適な形にテーラリングされたリスクレベルフレームワークを策定するために、事業体が使用できる C-SCRM のリスクレベルフレームワークの例を紹介する。ここでは、このフレームワークの 6 つの使用例が記載されている。これらの例では、事業体がどのようにフレームワークをテーラリングできるかを示すために、フレームワークの実装を少しずつ変えている。各例では、1 つ以上の脆弱性を識別し、特定の脅威源を説明し、予想される事業体へのインパクトを識別し、結果として生じるリスクを軽減するのに役立つ[SP 800-161、Rev. 1] C-SCRM 管理策を提案する。

[38] 各省庁及び関係機関は、附属書 F を参照して、大統領令 14028 号の「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装することが望ましい。

[39] その他の脅威シナリオの例と脅威リストは、以下の ICT SCRM タスクフォースで確認できる： 脅威シナリオレポート（v3）（2021 年 8 月）https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf。 このレポートでは、2015 年版の NIST SP 800-161 が活用されている。

リスクレベルフレームワーク

ステップ 1：脅威シナリオの策定及び分析の計画の作成

- 目的、マイルストーン、及び期待される成果物の観点から脅威シナリオ分析の目的を識別する。
- 事業体の適用範囲、詳細レベル、及びその他の制約条件を識別する。
- 人員、時間、機器を含む、使用するリソースを識別する。
- シナリオの分析に使用するリスクレベルフレームワークを定義する。

ステップ 2：環境の特徴付け

- コアミッション及びビジネスプロセス、及び事業体の主要な依存関係を識別する。
- 事業体に関連する脅威源について記述する。該当する場合は、脅威源に利用可能な動機及びリソースを含める。
- 既知の脆弱性又は懸念のある領域をリストする。（注：懸念のある領域には、製造工場の外部委託の計画、懸案の保守契約終了、ある要素の製造中止が含まれる）。
- 既存の管理策及び計画された管理策を識別する。
- 関連する規制、標準、ポリシー、及び手順を識別する。
- 戦術、技法、及び手順（TTP）、システムの重要度、及びリスク所有者のミッション又はビジネスの優先順位についての事業体のアセスメントごとに受容可能なリスクレベル（リスクしきい値）を定義する。リスクレベル又はリスクしきい値は、グローバルサプライチェーンの弾力性、事業体の変化、及び新たなミッションの優先順位を反映するように、定期的に見直し、調整することができる。

ステップ 3：分析対象の脅威事象の作成及び選択

- 脅威源が既知の脆弱性を悪用したり、懸念のある領域にインパクトを与えたりする可能性のある方法をリストして、事象リストを作成する。（注：この情報を判断する際には、過去のデータが有用である）。
- 各脅威事象の結果として発生する可能性のある一連の結果について、簡単に要点をまとめる。
  これらは、必要に応じて大まかにすることも、具体的にすることもできる。必要に応じて、各事象の起こりやすさとインパクトを推定する。
- 定義された分析の目的及び範囲から明らかに外れている事象を排除する。
- 残った潜在的な脅威事象について、さらに詳しく記述する。脅威源が攻撃を実行するために使用する可能性のある TTP を含める。（注：記述の詳細レベルは、事業体のニーズによって異なる）。
- 定義された分析の目的及び範囲に最も適した事象を分析対象として選択する。
  一般的には、より起こりやすい、又はインパクトが大きい事象、事業体にとって懸念のある領域、及びリストされている他の事象のいくつかを表す可能性のある事象が有用な候補になる。

ステップ 4：リスクレベルフレームワークを使用した分析の実施

- 脅威事象ごとに、適用される規制、標準、ポリシー、及び手順、既存の管理策及び計画された管理策、脅威事象によって引き起こされる可能性のある損害をそれらの管理策が効果的に回避、抵抗、又はその他の方法で軽減できる範囲を考慮して、その事象が直接的にもたらす結果に留意しながら、影響を受けるであろう事業体単位及びプロセスを識別する。
- これらの結果がミッション及びビジネスプロセス、情報、資産、事業体単位、及び影響を受けるその他のステークホルダーに与えるであろうインパクトを、できれば過去のデータから定量的に、かつ既存の管理策及び計画された管理策、並びに、適用される規制、標準、ポリシー、及び手順を考慮に入れて見積もる。
  （注：「最も起こりやすい」インパクトレベルと、「最悪のケース」又は「100 年」のインパクトレベルを識別することが有益な場合がある）。
- 既存の管理策及び計画された管理策、並びに、適用される規制、標準、ポリシー、及び手順を考慮して、その次に影響を受ける可能性がある、又は影響を受けるであろう事業体単位、プロセス、情報（アクセス又はフロー）、及び／又は資産、及びその結果とインパクトレベルを、影響を受ける各重要項目の分析が完了するまで識別する（例えば、重要サーバがダウンした場合に最初に影響を受けるプロセスの 1 つは技術サポート部門かもしれないが、サーバを復旧するために新しい要素が必要であると判断した場合には調達部門も関与することになる可能性がある）。

ステップ 5：C-SCRM の適用可能な管理策の決定

- 脅威シナリオ事象がリスク所有者の受容可能なリスクレベル（リスクしきい値）を超えるリスクレベルを生み出すかどうか、どのような脅威シナリオ事象がそれに該当するかを判断する。（注：場合によっては、受容可能なリスクレベルは、軽減戦略を実装するケイパビリティ（能力）又は軽減戦略のコストに依存することがある）。既存の管理策又は新たな軽減管理策の候補を強化する機会を識別する。標準又は推奨される管理策のリストを使用すると、このプロセスを簡素化することができる。この附属書では、本出版物の附属書 A の管理策を使用する。
- シナリオのリスクを軽減する上での既存の管理策及び計画された管理策の有効性を推定する。
- 新しい管理策の候補又は強化された管理策を実装するために必要なケイパビリティ（能力）及びリソースを（資金、人員、時間の観点から）推定する。
- 適用される可能性のあるルールや規制を考慮に入れて、脅威事象の推定残留リスクを最もリソース効率の高い方法で許容可能なレベルまで低下させることができる C-SCRM 管理策、又は C-SCRM 管理策の組み合わせを識別する。（注：1 つの管理策が複数の事象のリスクを軽減するのに役立つ可能性、又はある管理策が別の事象のリスクを増大させる可能性を考慮すること）。

ステップ 6：評価／フィードバック

- 選択した管理策を実施し、その有効性を評価するための計画を策定する。
- リスクレベルフレームワークの有効性を評価し、必要に応じて改善する。

表 C-1：リスクレベルフレームワークの例

脅威シナリオ	**脅威**	
	脅威事象の説明	事象リストを作成するために、脅威源が既知の脆弱性を悪用したり、懸念のある領域にインパクトを与えたりする可能性のある方法を記述する。 脅威事象：望ましくない結果又はインパクトを引き起こす可能性のある事象又は状況。
	脅威事象の結果	脅威事象の結果を記述する。 脅威事象の結果：脆弱性に対する脅威行動が事業体の業務、資産、及び／又は個人の機密性、完全性、及び／又は可用性にもたらす影響。
影響を受ける事業体単位、プロセス、情報、資産、又はステークホルダー		影響を受ける事業体単位、プロセス、情報、資産、又はステークホルダーをリストする。
リスク	**インパクト**	ミッション及びビジネスプロセス、情報資産、又はステークホルダーに現実的に影響を及ぼすようになった脅威事象から生じるインパクト、損失、損害の推定を入力する。 推定は、過去のデータに基づいて定量的に提供することが望ましく、既存の管理策及び計画された管理策、並びに、適用される規制、標準、ポリシー、及び手順を考慮に入れることが望ましい。（注：「最も起こりやすい」インパクトレベルと、「最悪のケース」又は「*100* 年」のインパクトレベルを識別することが有益な場合がある）。 情報又はシステムの機密性、完全性、又は可用性の喪失が、事業体の業務、事業体の資産、個人、他の事業体、又は国家（米国の国家安全保障上の利益を含む）に及ぼす影響。
	起こりやすさ	特定の *1* つ以上の事象の発生可能性を入力する。 起こりやすさ：何かが起こる可能性
	リスクレベル（インパクト x 起こりやすさ）	インパクト *x* 起こりやすさを乗算してリスクスコアを入力する。 潜在的な状況又は事象によってエンティティが脅かされる度合いの指標であり、通常、以下に応じて変化する。 （*i*）状況又は事象が発生した場合に生じる有害なインパクト、及び（*ii*）その発生可能性。

	受容可能なリスクレベル	戦術、技法、及び手順（*TTP*）、システムの重要度、リスク選好度及び許容度、及びリスク所有者の戦略的目標及び目的についての事業体のアセスメントごとに、受容可能なリスクレベル（リスクしきい値）を定義する。 受容可能なリスク：事業体によって設定されたリスク選好度及びリスク許容度ステートメントの範囲に収まる、事業体の業務、資産、又は個人に対する残留リスク。
軽減	**潜在的な軽減戦略及び C-SCRM 管理策**	潜在的なリスク軽減戦略及び関連する *C-SCRM* 管理策をリストする。 C-SCRM リスク軽減：サプライチェーンにおけるサイバーセキュリティリスク、サプライチェーン全体の脅威及び脆弱性への曝露（エクスポージャー）を管理し、サプライチェーン全体のサイバーセキュリティリスクに対するリスク対応戦略を策定するための体系的なプロセス。
	軽減戦略の推定コスト	リスク軽減戦略の推定コストを入力する。
	起こりやすさの変化	起こりやすさの潜在的な変化を識別する。
	インパクトの変化	インパクトの潜在的な変化を識別する。
	選択された戦略	インパクトを軽減するために選択された戦略をリストする。
	推定残留リスク	残留リスクの推定量を入力する。 残留リスク：セキュリティ対策が適用された後に残留しているリスク。

シナリオ例

この附属書では、架空の会社「ABC Company」と上記のリスクレベルフレームワークを使用する米国政府特有の脅威シナリオの 6 つの例を示している。これらの例では、必要に応じて大まかにも脅威シナリオを具体的にも（詳細にも汎用的にも）することができることを示すために、意図的に具体性と詳細性のレベルを変えている。これらのシナリオでは、起こりやすさ、インパクト、及びリスクについてパーセンテージと基本的なスコアリング指標（すなわち、高、中、低）を使用するが、事業体は別の測定単位（CVSS スコアなど）を使用してもよい。さらに、必要に応じてリスクレベルフレームワークを適応させることができることを示すために、これらのシナリオでは、リスク対応フレームワークの実装を少し変えている。

シナリオ *1*：サプライヤに対する外国政府による影響又は統制[40]

背景

ある事業体が、プリント基板（PCB）サプライヤの脅威シナリオ分析を実施することを決定した。このシナリオでは、コンポーネントコストの予期せぬ変動に対するビジネスの感度に焦点を当てる。

脅威源

ABC Company は、年間 350 万台のパーソナルコンピュータを設計、組み立て、出荷している。同社は、顧客ベースとサプライベースの両方でグローバルに展開している。5 年前、ABC Company は売上原価を削減するために、PCB 調達の大部分を東南アジアにシフトした。ABC Company は、単一調達を避けるため、国内の 5 つの異なるサプライヤと契約を締結し、この間、それぞれのサプライヤと良好なパートナーシップを築いてきた。

脆弱性

ABC Company は複数のベンダから調達しているが、1 つの国（東南アジア）のサプライヤに依存している。このことは、単一政府の政策が材料の安定供給に劇的なインパクトを与える可能性があるため、ABC Company は地政学的な脅威にさらされている。

脅威事象の説明

この事業体では、分析の訓練のために以下のような架空の脅威を設定した。昨年、ABC Company が PCB ビジネスのほとんどを行っている国で、新しい指導部がその政府を引き継いだ。この指導部は、国内の金融及びビジネス環境の改善に焦点を当てており、国内に本社やその他の主要拠点を設置した大手企業は、同じ地域内のサプライヤとより簡単かつコスト効率よくビジネスを行えるようになるというメリットを得ることができる。しかし 2019 年 2 月に、現在の腐敗した政権は、国外で販売されるすべての電子コンポーネント及び商品に 20 % の追加税を課す新しい法律を可決した。この新しい法律は、2019 年 6 月 1 日に施行される予定であった。

[40] シナリオ 1 の文章は、以下の ICT SCRM タスクフォースを少し変えたものである（会社名の変更など）：脅威シナリオレポート（v3）（2021 年 8 月）https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf。 このレポートでは、2015 年版の NIST SP 800-161 が活用されている。

新しい法律が発表された時点での ABC Company の PCB の在庫は年間需要の約 10 % であり、これは同社が安心できる標準的な在庫レベルであった。ABC Company は 6 月までに 5 つすべてのサプライヤに追加の材料を注文するための連絡を取ったが、これらの製品の需要が、多くの海外の顧客から高まったために、すぐに不足が発生した。新しい税法が施行された 6 月 1 日までに、ABC Company の在庫レベルは年間需要の 15 % にまで達していた。

結果

2019 年 2 月から 6 月にかけて、ABC Company は新しいサプライヤとのパートナーシップを検討したが、いくつかの問題が確認された。ABC Company が接触した新しいサプライヤの 10 社に 1 社は、希望する需要を満たすために 6 か月から 18 か月というリードタイムが必要であった。そのため、ABC Company では、サプライヤの PCB のサンプルテスト、物流の詳細の確定、サプライヤ側の活動の監視（原材料の調達や新たな需要を満たすために必要な人員及び生産スペースの取得など）を含め、追加の作業が必要となった。

2 つ目の問題は、東南アジアの 5 つすべてのサプライヤとの当時の契約に最低需要要件を満たすことが含まれていたことである。すなわち、ABC Company は、3 か月から 24 か月の契約期間中は、毎月 100,000 個以上の PCB を購入することを確約していたのである。これは、ABC Company が新しい税金によるコストへの影響を簡単には回避できないことを意味していた。ABC Company は PCB のコストを吸収できたのか。20 % のコスト増により、PC の利益率は平均で 13.5 % から 4.5 % に低下した。利益率の低い ABC Company 製品の一部では、ラインを廃止し、より高い利益率を得られるハイエンドモデルで高価な PCB を使用することになる可能性があった。

影響を受ける事業体単位及びプロセス

該当なし

潜在的な軽減戦略及び C-SCRM 管理策

- サプライヤリスクの定期的なアセスメント及びレビューを実施する。[41]
- 直接的な場所だけでなく、国、地域、及びその他の要因によってサプライヤを多様化する。
- コストの影響をサプライヤ契約に組み込み、コストが高くなりすぎた場合に（サプライヤの過失であるかどうかに関係なく）、サプライヤと容易に決別できるようにする。
- 重要な時期に予期しない需要不足が発生しても適切に対応できるように、必要な在庫レベルを調整する。
- ビジネスに悪影響を及ぼす可能性のある新しい法律の事前通知を入手するために、重要なサプライヤの国又は地域でより多くのリソースを雇用する。

[41] サプライヤリスクの軽減戦略の定期的なアセスメント及びレビューが、以下の ICT SCRM タスクフォースのシナリオ 1 の原文に追加された：脅威シナリオレポート（v3）（2021 年 8 月）https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios- report-v3.pdf。 このレポートでは、2015 年版の NIST SP 800-161 が活用されている。

表 C-2：シナリオ 1

脅威シナリオ	**脅威源**	PC 用の生産コンポーネントの供給にインパクトを与える動的な地政学的状況
	脆弱性	主要な生産コンポーネントのサプライヤの地理的集中
	脅威事象の説明	ABC Company は売上原価を削減するために、プリント基板（PCB）調達の大部分を東南アジアにシフトした。 ABC Company は、単一調達を避けるために、国内の 5 つの異なるサプライヤと契約を締結した。 ABC Company が PCB ビジネスのほとんどを行っている国では、新体制が政権を担うことになった。2019 年 2 月に、この現在の腐敗した政権は、国外で販売されるすべての電子コンポーネント及び商品に 20 % の追加税を課す法律を可決した。 この法律は、2019 年 6 月 1 日に施行される予定であった。 新しい法律が発表された時点での ABC Company の PCB の在庫は年間需要の約 10 % であり、これは同社が安心できる標準的な在庫レベルであった。ABC Company は 6 月までに 5 つすべてのサプライヤに追加の材料を注文するための連絡を取ったが、需要の高まりによってすぐに不足が発生した。新しい税法が施行された 6 月 1 日までに、ABC Company の在庫レベルは年間需要の最大 15 % に達していた。
	脅威事象の結果	ABC Company は新しいサプライヤとの提携も検討したが、このアプローチには問題があることが確認された。 ABC Company が接触した新しいサプライヤの 10 社に 1 社は、希望する需要を満たすために 6 か月から 18 か月というリードタイムが必要であった。さらに、東南アジアの 5 つすべての現役のサプライヤとの現在の契約に最低需要要件が規定されていた。すなわち、ABC Company は、契約期間は 3 か月から 24 か月と違いがあるが、この期間中は、毎月 100,000 個以上の PCB を購入することを確約していたのである。これは、ABC Company が新たな税金によるコストへの影響を簡単に回避できないことを意味していた。20 % のコスト増により、PC の利益率は平均で 13.5 % から 4.5 % に低下した。

	影響を受ける事業体単位／プロセス	該当なし	
リスク	**インパクト**	高：PC 製品ラインの利益が 4000 万ドル減少	
	起こりやすさ	中：年換算で 10 % の発生確率	
	リスクレベル（インパクト x 起こりやすさ）	高：製品ラインの利益で約 400 万ドルに相当する固有のリスクレベル	
	受容可能なリスクレベル	製品ラインの利益が 1000 万ドルを超える確率が 10 % 以下	
軽減	**潜在的な軽減戦略及び C-SCRM 管理策**	FOCI を含めるためのサプライヤリスクのアセスメントとレビュー[SR-6 (1)]、サプライヤの多様性要件の採用[C-SCRM_PL- 3(1)]、サプライヤの多様性の採用[SCRM_PL-8(2)]、及び在庫レベルの調整[CM-8]。	• サプライヤリスクの定期的なアセスメントとレビューを実施する。 • 直接的な場所だけでなく、国、地域、及びその他の要因によってサプライヤを多様化する。 • コストの影響をサプライヤ契約に組み込み、コストが高くなりすぎた場合に（サプライヤの過失であるかどうかに関係なく）、サプライヤと容易に決別できるようにする。 • 重要な時期に予期しない需要不足が発生しても適切に対応できるように、必要な在庫レベルを調整する。 • ビジネスに悪影響を及ぼす可能性のある新しい法律の事前通知を入手するために、重要なサプライヤの国又は地域でより多くのリソースを雇用する。
	軽減戦略の推定コスト	該当なし	
	起こりやすさの変化	低：10 % の発生確率	
	インパクトの変化	中：製品ラインの利益で 200 万ドル	
	選択された戦略	示された軽減策を使用した戦略の組み合わせ	
	推定残留リスク	低：残留リスクレベルが PC 製品ラインの利益率の 0.02 %	

シナリオ 2：通信機器の偽造品

背景

大手企業である ABC Company は、外部のインテグレーション企業との契約によって保守されるシステムを開発した。このシステムには、相手先ブランド製造業者（OEM）から入手できなくなった共通の通信要素が必要である。OEM は代替品として新製品を提供しているが、これを使用するには約 100 万ドルの費用をかけてシステムを変更する必要がある。この要素がアップグレードされない場合、政府機関とシステムインテグレータは非公式市場のサプライヤに代替品の確保を頼らざるを得なくなる。新製品には、現在使用されている要素と比べて大きな改善点はない。

ABC Company は、新製品を受け入れるためにシステムを変更するか、生産が終了した製品を使い続けることのリスクを受容するかを判断するために、脅威シナリオ分析を実施することを決定した。

環境

環境の特徴は以下のとおりである。

- このシステムは、大規模なアップグレードや変更を行わなくてもあと 10 年間は持つと予想されており、99.9 % のアップタイム要件がある。
- 200 ドルの要素がシステム全体で 1,000 個以上使用されており、約 10 % が経年劣化や故障などの理由によって毎年交換されている。
  インテグレータは、常に約 3 か月分の在庫を確保している。
- この要素の機能性は継続的に監視されており、予期しない故障が発生した場合にはトラフィックのルートを変更して要素を交換するための効率的な手順が用意されている。
- 予期しない要素故障によって発生するシステム停止はまれで、局所的なものであり、数分で終了する。それより頻繁に起こるのは、ある要素が故障した場合に、問題を診断して修正するか、又は要素が交換されるまでの約 1 ～ 4 時間の間、システムの機能性が大幅に低下することである。
- 当該要素のような製品は、偽造品の共通の標的となっている。
- インテグレータには、偽造品の購入を制限するポリシーと、偽造品が発見された場合に従うべき手順がある[Ref. SR-11]。
- インテグレータ及び取得政府機関が承認前に要素の機能性を確認するために使用するテスト手順は限定的なものである[Ref. SR-5(2)]。

脅威事象

脅威シナリオをサポートするために、政府機関は、偽造品ソリューションの豊富な作成経験を持ち、利益を動機とするグループとして記述した、架空の脅威源を作成した。外観は真正品と同じであるが、低品質の材料が使用されている偽造品を作成して販売することで、偽造者は高い利益率を得ることができる。偽造者は、商標その他の識別特性のほとんどをコピーし、事業体によく利用されるサプライチェーンに偽造品を挿入するためのリソースを持っており、検出されるリスクはほとんど又はまったくない。偽造品は、一般的に割引価格で提供され、余剰在庫又は備蓄と

して販売されるため、無知な購入当局にとっては魅力的に見える。

低品質の要素がシステムに挿入された場合、予想以上に頻繁に故障が発生し、システムの機能性低下を引き起こす可能性がある。システム内で大量の偽造品が純正部品とランダムに組み合わされた場合、予期しないシステム停止の回数と深刻さが大幅に増大する可能性がある。政府機関とインテグレータは、システムを維持するために偽造品が購入される可能性と、そのような事象が起きた場合の潜在的インパクトの推定が、さらなる評価を行う正当な理由になり得るほど高いと判断した。

脅威シナリオ分析

サプライヤから要素を購入した人が、偽造品の影響を最初に受けることになる。ポリシーでは、入念に検査されたサプライヤから真正品の購入を試みるように要求している。この個人は、その製品が真正品であると信じさせられる必要がある。問題となっている偽造品は、目的の要素と視覚的に同じであり、割引価格で提供されているため、偽造品が購入される可能性が高い。機能性を確認するために 1 つをテストした後、全製品が保管される。

システム内の要素の 1 つを交換する必要が生じた場合、エンジニアは偽造品を取り付け、短時間でテストして正常に動作することを確認し、変更を記録する。偽造品が故障するまでに 2 年かかり、最初の故障の兆候が現れる前に最大 200 個の偽造品の要素がシステムに挿入される可能性がある。定期的に交換されるすべての要素が偽造品に置き換えられ、各偽造品が 2 年後に故障した場合、システムのコストは 10 年間で 16 万ドル増加することになる。また、必要な保守にかかる時間は、インテグレーション企業に人件費その他の費用としてかかってくる。

偽造品が故障した場合、要素を診断して交換するために約 1 ～ 4 時間かかる。この間、生産性は大幅に低下する。複数の要素が同時に故障した場合には、システム全体が故障する可能性がある。これにより、政府機関の業務に重大な損害が生じ、契約で規定されている 99.9 % のアップタイム要件に違反する可能性がある。さらに、その要素が偽造品であったために故障したと判断された場合は、偽造品の報告に関連する追加コストが発生することになる。

軽減戦略

潜在的な軽減活動として、以下のものが識別された（NIST SP 800-161, Rev. 1 の附属書 A より）。

- 開発者に SDLC の設計後のすべてのフェーズでセキュリティテスト／評価を実行するように要求する[Ref. SA-11]。
- 受け取った情報システムやシステムコンポーネントが真正品であり、改造されていないことを妥当性確認する[Ref. SR-11]。
- 情報システムの設計にセキュリティ要件を組み込む（セキュリティエンジニアリング）[Ref. PL-8、SC-36]。
- サプライヤの多様性要件を採用する[PL-8(2)]。

これらの管理策に基づいて、政府機関は以下を含む戦略を考案することができた。

- 受け入れテスト：要素が新品であること、真正品であること、及び関連するすべてのライセンスが有効であることを確認するための検査。テスト方法には、必要に応じて、訓練を受けた担当者によるデジタル画像を使用した物理検査、デジタル署名の検証、シリアル／部品番号の検証、及びサンプルの電気検査が含まれる。
- システムの設計において、（重要度分析で判別した）より重要なパスに沿って冗長要素を追加して要素の故障によるインパクトを最小化することで、セキュリティ要件を強化する。
- 入念に検査された代替サプライヤ／信頼できるコンポーネントを探す。

この戦略は、偽造品がシステムに入り込むリスクを受容したり、アップグレードされた要素を受け入れるためにシステムを変更したりするよりもコストがかからないと判断された。より厳格な取得及びテストプログラムの実装にかかる推定コストは 8 万ドルであった。セキュリティエンジニアリングの要件を強化するためのコストは 10 万ドルであった。

表 C-3：シナリオ 2

脅威シナリオ	**脅威源**	サプライチェーンに持ち込まれた偽造の通信要素
	脆弱性	OEM による生産が終了した要素 購入当局は真正品の要素のみを識別して購入することができない、又は購入したいと考えていない
	脅威事象の説明	脅威エージェントが偽造要素を信頼できる流通チェーンに挿入する。 購入当局が偽造要素を購入する。偽造要素がシステムに取り付けられる。
	脅威事象の結果	要素は以前よりも頻繁に故障し、システム停止の回数が増える。
影響を受ける事業体単位、プロセス、情報、資産、又はステークホルダー		調達 保守 OEM／サプライヤ関係
リスク	**インパクト**	中：要素の故障により 1 ～ 4 時間のシステムダウンタイムが発生
	起こりやすさ	高：脅威行為者による動機付けが大きい、及びコンポーネントの早期故障が年率換算で 25 % となる偽造品を政府機関が検出できないために脆弱性が高い
	リスクレベル（インパクト x 起こりやすさ）	中：アップタイムのしきい値を 0.5 % 超えるダウンタイムにつながる重大な短期的な中断（例えば、99.4 % < 99.9 % の要件）

	受容可能なリスクレベル	低：システムは、99 % のアップタイムしきい値に達しない確率が年率換算で 10 % 未満でなければならない	
軽減	**潜在的な軽減戦略及び C-SCRM 管理策**	受け入れテストケイパビリティ（能力）の強化[C-SCRM_SA-9、C-SCRM_SA- 10]と、システム設計におけるセキュリティ要件の強化[C-SCRM_PL-2]、及びサプライヤの多様性要件の採用[C-SCRM_PL-8(2)]	要素のアップグレードを受け入れるためのシステムの変更
	軽減戦略の推定コスト	18 万ドル	100 万ドル
	起こりやすさの変化	低：年率換算で 8 % のコンポーネント故障率	
	インパクトの変化	低：要素に障害が発生すると冗長システムコンポーネントへのフェイルオーバーが発生するが、コストは保守と交換に限定される	
	選択された戦略	政府機関レベルの検査とテスト 定義された受け入れテスト基準に合格するまで、要素を第三者に預けておく セキュリティエンジニアリングを増やす	
	推定残留リスク	低：システムダウンタイム（すなわち 99.9 % を下回るアップタイム）につながるコンポーネントの故障率は年率換算で 8 %	

シナリオ *3*：産業スパイ

背景

事業体が軍事システム及び航空宇宙システムの製造に使用する半導体（SC）を生産する企業である ABC Company は、KXY Co. の製造施設を活用するために、同社とのパートナーシップを検討している。これは、重要なシステム要素に関連するサプライチェーンに重大な変化をもたらすことを意味する。このパートナーシップが事業体に与えるであろうインパクトと、パートナーシップが完成したときのリスクに合った軽減策として実施すべきプラクティスを識別するのに役立てるために、事業体、ABC Company、及びインテグレーション企業の代表者を含む委員会が結成された。

環境

懸念されるシステムは、軍事及び航空宇宙ミッションの安全にとって不可欠なものである。機密扱いにはなっていないものの、KXY が製造を期待されている要素は特許を取得済みの独自のものであり、システムの稼働状況にとって重要なものである。システムの稼働中にこの要素が利用できなくなると、複数の政府機関や一般市民に、人命の損失や数百万米ドルの損害を含め、即時の重大なインパクトを与える可能性がある。初期のリスクアセスメントは[NIST SP 800-30, Rev. 1]を使用して実施されており、これに対する既存のリスクレベルのスコアは「中」であった。

現在、KXY は、主に商業用に焦点を当てた最先端の低コストウェハー製造を行っている。KXY が活動している国家には、知的財産／技術を獲得するために産業スパイ活動を行ってきた歴史がある。その国は半導体技術に関心を示し、軍事及び航空宇宙市場に展開するための多額の助成金を KXY に提供した。KXY は現在、米国の業界コンプライアンス要件を満たすテストインフラを持っていないが、その国家には膨大なリソースがあり、KXY がそれらの要件を満たすのに役立つ譲歩とインセンティブの両方を提供する余地がある。主な懸念事項は、KXY が活動している国家が、その影響力を利用して要素や要素の設計にアクセスできるようになることである。

委員会は、現在実施されている軽減戦略をレビューし、ABC Company、インテグレーション企業、及び事業体には、システム及びすべての重要要素（重要度分析によって判断されたもの）が特定の機能的要件を満たしていることを確実にするためのいくつかの既存のプラクティスがあると判断した。例えば、システム及び重要要素は、関連する業界標準に準拠していると判断される。[NIST SP 800-53, Rev.5]に基づく要件の一部として、政府機関にはいくつかの情報保護の要件があった（Ref. PM-11）。さらに、ABC Company には、トレーサビリティのためにほとんどの要素に RFID 技術を使用した固有のタグを付けるか、その他の方法で識別されることを必須とする、高度な在庫追跡システムがあった（Ref. SR-4）。

脅威シナリオ

過去の経験から、事業体は、KXY のホスト国が技術へのアクセス権を与えられた場合、以下の 2 つの活動のうちの 1 つを実行する可能性が高いと判断した。1）利害関係者に販売するか、2）後で悪用するための脆弱性を挿入又は識別する。これらの脅威事象のいずれかが成功するためには、ホスト国が要素の目的を理解し、要素又は要素の設計への重要なアクセス権を与えられる必要がある。これは、KXY の人事部門の協力のもと、偽装、あるいは物理的又は電子的な盗難によって達

成される可能性がある。既存の物理的管理策の要件と在庫管理の手順を考慮すると、物理的な盗難は困難である。変更された要素が購入されてシステムに統合されるためには、インテグレータレベルと政府機関レベルの両方で様々なテスト手順に合格する必要がある。現在使用されているテスト方法には、X 線検査、材料分析、電気検査、及びサンプルの加速寿命試験が含まれる。識別ラベルやスキームの変更は、基本的な検査では検出できないようにする必要がある。さらに、KXY は、要素の品質と機能性を保証するための KXY のプロセスをチェックする定期的な監査に合格する必要がある。

委員会は、既存のプラクティスがあったとしても、ホスト国が検出されることなく要素に有害な変更を加えたり、これまで認識されていなかった脆弱性を悪用したり、同盟国の 1 つに同じことを行う手段を提供したりする動機と能力を持つ可能性が 30 % あると判断した。その結果、システムの可用性や完全性が失われ、重大な損害が発生する可能性がある。[NIST SP 800-30, Rev. 1] を使用して行われた初期リスクアセスメントからの情報を使用して、委員会はこれをインパクトスコアが「高」の最悪のシナリオとして識別した。

ホスト国が利害関係者に技術を売却できる／売却し、その結果、技術的優位性が失われる可能性は約 40 % である。このシナリオが発生した場合、友好関係にある軍隊や民間人の生命が危険にさらされたり、諜報活動が損なわれたり、新しいソリューションに投資するために追加の資金が必要になったりする可能性がある。委員会は、このシナリオのインパクトスコアとして「中」を割り当てた。

委員会は、懸念される脆弱性に対する全体的な複合リスクレベルは「高」であると判断した。

軽減戦略

NIST SP 800-161, Rev. 1 の附属書 A をベースにして、以下の 3 つの大まかな戦略が委員会によって識別された：（1）トレーサビリティケイパビリティ（能力）を向上させる、（2）来歴及び情報の要件を強化する、（3）別のサプライヤを選択する。これら 3 つのオプションをさらに詳細に分析して、具体的な実装戦略、シナリオへのインパクト、及び実装コストの推定を決定した
（ここでは具体的な技術や技法は説明しないが、実際の脅威シナリオの評価には有用である）。

トレーサビリティ及び監視ケイパビリティ（能力）を向上させる。

- CM-8：システムコンポーネントのインベントリ
- IA-1：ポリシー及び手順
- SA-10：開発者構成管理
- SR-8：通知協定
- SR-4：来歴

コスト = 20 % 増
インパクト = 10 % 減

来歴及び情報の管理策の要件を強化する。

- AC-21：情報共有
- SR-4：来歴

コスト = 20 % 増
インパクト = 20 % 減

別のサプライヤを選択する。

- SR-6：サプライヤのアセスメント及びレビュー

コスト = 40 % 増
インパクト = 80 % 減

この分析に基づいて、委員会は以下のプラクティスの組み合わせを実装することを決定した。

- コンポーネントの複製や変更を阻止するために、コピーが困難な独自のラベルを開発し、これを必須とするか、ラベルを変更する[Ref. SR-3 (2)]。
- サプライヤと共有する情報量を最小限に抑える。情報をセキュアにすることを要求する[Ref. AC-21]。
- SDLC 全体を通じて来歴を保存し、更新することを要求する[Ref. SR-4]。

この管理策の組み合わせにより、推定残留リスクは、事業体がサプライヤを変更した場合よりもコスト増が少なく、パートナーシップがない状態の既存のリスクと同等であると判断された。

表 C-4：シナリオ 3

脅威シナリオ		
	脅威源	大規模なリソースを持つ国家が知的財産を盗もうとしている
	脆弱性	脅威源と関係のある企業とのパートナーシップを検討しているサプライヤ
	脅威事象の説明	国家は、KXY が業界のコンプライアンス要件を満たすのを支援し、ABC Company は KXY と提携してチップを開発する
	既存のプラクティス	システム及び要素の機能性に関する強力な契約上の要件 ABC Company の包括的な在庫追跡システム
	脅威事象の結果	国家が技術の脅威行為者を抽出したり、技術を変更したり、これまで認識されていなかった脆弱性を悪用したりする

<table>
<tr><td colspan="2">影響を受ける事業体単位、
プロセス、情報、資産、又は
ステークホルダー</td><td colspan="3">KXY サプライヤ

ABC Company インテグレータ機能テスト

技術ユーザ</td></tr>
<tr><td rowspan="4">リスク</td><td>インパクト</td><td>技術の変更／脆弱性の悪用：高</td><td colspan="2">利害関係者への
技術の売却：中</td></tr>
<tr><td>起こりやすさ</td><td>中</td><td colspan="2">中</td></tr>
<tr><td>リスクレベル
（インパクト x 起こりやすさ）</td><td colspan="3">高</td></tr>
<tr><td>受容可能なリスクレベル</td><td colspan="3">中</td></tr>
<tr><td rowspan="5">軽減</td><td rowspan="2">潜在的な軽減戦略及び
C-SCRM 管理策</td><td>（1）トレーサビリティ及び監視ケイパビリティ（能力）を向上させる</td><td>（2）来歴及び情報の管理策の要件を強化する</td><td>（3）別のサプライヤを選択する</td></tr>
<tr><td>軽減戦略の推定コスト</td><td>20 % 増</td><td>20 % 増</td><td>40 % 増</td></tr>
<tr><td>起こりやすさの変化</td><td colspan="3">中 → 低</td></tr>
<tr><td>インパクトの変化</td><td colspan="3">高 → 中</td></tr>
<tr><td>選択された戦略</td><td colspan="3">コンポーネントの複製や変更を阻止するために、コピーが困難な独自のラベルを開発し、これを必須とするか、ラベルを変更する[C-SCRM_PE-3]。

サプライヤと共有する情報量を最小限に抑える。情報をセキュアにすることを要求する[C-SCRM AC-21]。

SDLC 全体を通じて来歴を保存し、更新することを要求する[C-SCRM_SR-4]。</td></tr>
<tr><td>推定残留リスク</td><td colspan="3">中：残留リスクは、パートナーシップがない状態の既存のリスクと同等であると判断された。</td></tr>
</table>

シナリオ *4*：悪意のあるコードの挿入

背景

ABC Company は、交通管制システムに関する脅威シナリオ分析を実施することを決定した。このシナリオは、ソフトウェアの脆弱性に焦点を当てるものであり、軽減策のプラクティスに関する一般的な推奨事項を提示することが望ましい。

環境

システムはほぼ自動で稼働しており、一般的に利用可能なオペレーティングシステムを実行するコンピュータと一元管理されたサーバを使用する。ソフトウェアは社内で作成されたもので、今後 5 年間は契約に基づいてインテグレーション企業によって定期的に保守・更新される。インテグレーション企業は大手であり、ABC Company は様々なプロジェクトで同社を頻繁に利用している。また、システムが高い可用性と完全性の要件を維持することを確実にする大規模なリソースを有している。

システムに対する脅威には、システムの電源喪失、機能の喪失、又は不正なコマンドの処理を引き起こす完全性の喪失が含まれる。一部の脅威源には、自然、悪意のあるアウトサイダー、悪意のあるインサイダーが含まれる場合がある。システムには、補助発電機の電源、設計の冗長性、システムが故障した場合の緊急時対応計画など、特定の安全制御が装備されている。

脅威事象

ABC Company は、最も懸念される脅威事象は、システムの完全性を侵害する悪意のあるインサイダーによってもたらされると判断した。攻撃としては、脅威行為者がワームやウイルスをシステムに挿入して機能を低下させたり、中央サーバの 1 つから、又はリモートからアクセスするためのバックドアをサーバに作成することで、手動でシステムを制御したりすることが考えられる。攻撃の巧妙さによっては、インサイダーがシステムの制御権を獲得し、特定の安全装置を無効にし、重大な損害を引き起こす可能性がある。

この情報に基づいて、ABC Company は分析用に以下の架空の脅威事象を開発した。

> インテグレーション企業に不満を抱いた従業員 John Poindexter は、システムのコンポーネントにオープンソースのマルウェアを挿入することを決心した。その後、彼は、この操作の痕跡を残さずに会社を辞めた。このマルウェアには、John にコールホームして、50 の交通局の一部又はすべてでネットワークトラフィックを停止又は許可するためのアクセス権限を提供する機能がある。その結果、予測不可能で診断が困難な中断が発生し、多大な金銭的損失と安全上の懸念が生じることになる。

[NIST SP 800-30, Rev. 1] を使用してリスクアセスメントを実施した後、経営陣は、このシナリオの受容可能なリスクレベルは「中」であると判断した。

脅威シナリオ分析

John が成功した場合、以下のような一連の事象が発生する可能性がある。

> John は実験を実施し、1 つの交通局のサービスを短時間停止させる。これは偶然の出来事として無視され、最小限のインパクトしかない。その後、John は様々な交通局で中断を引き起こす頻度を増やしていく。これらの中断は、従業員と顧客の間で怒りを生み出すだけでなく、安全上の懸念も生み出す。インテグレーション企業はこの問題を知り、原因の調査を開始する。この企業は回避策を作成し、システムにバグがあったと推測する。しかし、悪意のあるコードは埋もれてしまい、識別が難しいため、インテグレーション企業がそれを発見することはないだろう。その後、John は一度に複数の交通システムに対して大きな中断を引き起こす。攻撃の規模が大きすぎるためにインテグレーション企業が作成した回避策は失敗し、すべての交通サービスが停止することになる。旅行者に深刻なインパクトを与えることになり、メディアが警告を発する。攻撃の方法が識別され、John が再びシステムにアクセスできないようにシステムが変更される。ただし、根源的な悪意のあるコードは残ることになる。数か月間にわたって、収益は大幅に減少する。法律上の問題が生じる。システムが安全であると公衆を安心させるために、リソースへの投資が行われる。

軽減策のプラクティス

ABC Company は、以下の改善の可能性がある領域を識別した。

- サプライチェーン要素、プロセス、及び行為者の識別を確立し、保持する[SR-4]。
- SDLC 内のアクセスと構成の変更を管理し、定期的なコードレビュー（手動でのピアレビューなど）を必須にする[AC-1、AC-2、CM-3]。
- 静的コードテストを必須にする[RA-9]。
- インシデント対応手順を確立する[IR-4]。

表 C-5：シナリオ 4

脅威シナリオ	**脅威源**	インテグレータ：悪意のあるコードの挿入
	脆弱性	インテグレータの活動の監督が最小限である、小さなコードの断片を挿入する個人に対するチェック機能がない
	脅威事象の説明	インテグレータ企業に不満を抱いた従業員が、悪意のある機能を交通ナビゲーションソフトウェアに挿入し、その後、ABC Company を退職する。
	既存のプラクティス	インテグレータ：ピアレビュープロセス 取得者：ダウンタイム、コスト、及び機能性の要件を定めた契約
	脅威事象の結果	大都市圏の 50 地区と 500 のインスタンスがマルウェアの影響を受けた。マルウェアが活動を開始すると、交通に大規模な中断が生じる。

影響を受ける事業体単位、プロセス、情報、資産、又はステークホルダー		交通ナビゲーションシステム 実装企業 法務
リスク	**インパクト**	高：大規模な交通の中断が発生し、回避策が作成されるまでの 2 週間にわたって続く。 悪意のあるコードは発見されず、脆弱性が残る。
	起こりやすさ	高
	リスクレベル（インパクト x 起こりやすさ）	高
	受容可能なリスクレベル	中
軽減	**潜在的な軽減戦略及び C-SCRM 管理策**	C-SCRM_AC-1、C-SCRM_AC-2、C-SCRM_CM-3、C-SCRM_IR-2、 C-SCRM_SA-10、C-SCRM_SA-11
	軽減戦略の推定コスト	250 万ドル
	起こりやすさの変化	高 → 低
	インパクトの変化	高（変化なし）
	選択された戦略	示された軽減策を使用した戦略の組み合わせ
	推定残留リスク	中

シナリオ *5*：意図しない侵害

背景

無知なインサイダーが、パフォーマンス、安全性、長期的なコストへの影響を理解せずに、コンポーネントをよりコスト効率の高いソリューションに置き換えた。

ABC Company は取得ポリシーに懸念を抱いており、軽減策のプラクティスを識別するために脅威シナリオ分析を実施することを決定した。選択したすべてのプラクティスは、様々なプロジェクトに適用できるもので、かつ 1 年以内に大きな成功を収められるものでなければならない。

環境

ABC Company は、様々な度合の要件を持つ、様々なシステムを多数取得している。環境が複雑であるため、ABC Company の担当者は、実際の過去の事象に基づいたシナリオを使用すべきだと判断する。

脅威事象

政府機関は、実際の事象をベースにして、以下のような脅威事象のストーリーを設計する。

> 新たに採用されたプログラムマネージャの Gill は、独自の物理環境で複雑な研究アプリケーションをサポートするために購入する 500 万ドルのシステムのコストを削減する任務を課されている。このシステムは、温度、湿度、有害な化学物質の検出に関する情報を中継するほか、様々なデータセットの保存と分析を行う責任を負う。10 秒を超える計画外停止がないようにしなければならない。そうしないと、重大な安全上の懸念及び研究が中断される可能性が生じる。ABC Company の脅威アセスメント委員会は、この種の事象の受容可能なリスクレベルスコアは 2/10 であると判断した。
>
> Gill は、システム設計に含まれる多くのコンポーネントは、彼が一般市場で購入した類似のコンポーネントと比較して価格が高いと考えている。Gill は、インテグレーション企業のジュニアエンジニアである John に、コスト削減のためにシステム設計内のいくつかのロードバランサとルータを交換するように依頼した。

脅威シナリオ分析

ABC Company は、このシナリオには以下の 3 つの潜在的な結果があると判断した。

1. 購入前に変更が不適切であると判断される（30 % の確率、インパクトなし）。
2. テスト中に変更が不適切であると判断される（40 % の確率、低インパクト）。
3. 変更の不適切性は検出されず、ルータがシステムに設置され、障害が発生し始め、サービス拒否インシデントを引き起こす（30% の確率、高インパクト）。

軽減戦略

以下の 3 つの潜在的な軽減戦略が識別された。

- 既存のトレーニングプログラムを改善し[Ref. AT-1]、重要なシステムに対して提案されたすべての変更を監視するための構成管理の管理策を追加する[Ref. CM-1]。
- テスト要件を改善する[Ref. SA-11]。
- システムの設計に冗長性及び異質性（多様性）を必須にする[Ref. SC-29、SC-36]。

構成管理の管理策を追加すると、初期段階又はテスト中に変更が拒否される可能性が高くなるが、トレーニングに 20 万ドルを投資しただけでは、要求された時間内にリスクレベルを許容可能なレベルまで引き下げることはできないと判断された。

テスト要件を改善すると、テスト中に変更が拒否される可能性が高くなるが、テストの量だけではリスクレベルを許容可能なレベルまで引き下げることはできないと判断された。

システムの設計に冗長性及び異質性を必須にすると、このような事象やその他の懸念される事象のインパクトは大幅に軽減されるが、プロジェクトのコストが倍増する可能性がある。このシナリオでは、リスクを許容可能なレベルに引き下げるには、200 万ドルの投資が必要になると判断された。

この分析の結果、ABC Company は以下のプラクティスの組み合わせを実装することを決定した。

- 構成管理委員会（CMB）による変更承認を必要とする重要なシステムの取得及び構成管理の管理策の追加を扱う担当者を対象とした、一日がかりで行う必須のトレーニングプログラム（8 万ドルの初期投資）
- 重要なシステム及び要素のテスト機器やソフトウェアへの 6 万ドルの投資
- 各プロジェクトに適切であると考えられる、設計要件の冗長性及び多様性

このプラクティスの組み合わせは、様々なプロジェクトで最も費用対効果が高く、様々な脅威によるリスクを軽減するのに役立つと判断された。

表 C-6：シナリオ 5

脅威シナリオ		
	脅威源	内部の従業員：意図しない侵害
	脆弱性	緩慢なトレーニングプラクティス
	脅威事象の説明	市販品の取得経験を持つ新しい取得責任者（AO）がハードウェアコストの削減の任務を課されている。 この AO は、多くのコンポーネントの価格が高いと考えており、エンジニアと協力して発注を変更する。
	既存のプラクティス	必須とみなされない最小限のトレーニングプログラム システムコンポーネントの基本的なテスト要件

	脅威事象の結果	購入前に変更が不適切であることが判明する。	テスト中に変更が不適切であることが判明する。	変更はテストに合格し、ルータが設置され、障害が発生し始めて、サービス拒否を引き起こす。
影響を受ける事業体単位、プロセス、情報、資産、又はステークホルダー。		なし	調達	調達、システム、ユーザ
リスク	**インパクト**	なし	低	高
	起こりやすさ	中：30 %	高：40 %	中：30 %
	リスクレベル（インパクト x 起こりやすさ）	なし	中	中
	受容可能なリスクレベル	低	中	高
軽減	**潜在的な軽減戦略及び SCRM 管理策**	トレーニングプログラムを改善し、CMB による変更承認を必須にする。	取得テストを改善する。	システムの設計を改善する。
	軽減戦略の推定コスト	20 万ドル	---	200 万ドル
	インパクトの変化	なし：変化なし	低：変化なし	高 → 低
	起こりやすさの変化	30 % →10 %	40 % →20 %	30 % → 変化なし
	新しいリスクレベル	なし	低	中
	選択された戦略	重要なシステムで作業する担当者に必須のトレーニングを義務付け、重要なシステムへの変更に対する構成管理委員会の承認を必須にする（コスト = 10 万ドル）。		
	残留リスク	低		

シナリオ *6*：システム内の脆弱な再利用コンポーネント

背景

ABC Company は、標準開発のプラクティスの一部として、社内で開発されたオープンソースのシステムコンポーネントを COTS ソリューションの開発に再利用している。最近注目を集めているサイバー攻撃は、再利用されているシステムコンポーネントに存在する脆弱性につけ込むものであり、ABC Company の顧客は、自身のリスクレベルを軽減する手段として、透明性の向上を要求している。

ABC Company は、脅威シナリオ分析を実施することにより、自社のソフトウェア製品のセキュリティを向上させ、ABC Company がこのような種類の攻撃から顧客を保護するために必要な対策を実施しているという信頼を顧客に持ってもらうために実施できる対策を決定した。

環境

ABC Company は、財務計画及び分析（FP&A）ソフトウェア市場における有名な市場リーダーである。ABC Company の顧客は、機密性の高い財務情報（決算など）の保存、処理、及び分析に Acme の FP&A ソリューションを利用している。

脅威事象

Apache Struts（広く使用されているソフトウェアコンポーネント）は、ABC Company の COTS FP&A ソリューション内のコンポーネントとして使用されている。Apache Struts 内に存在する脆弱性に対して、2021 年 3 月にパッチが適用された。金銭上の利益によって動機付けられた日和見的なサイバー犯罪組織は、COTS ソリューションの脆弱性につけ込む機会を模索していた。

ABC Company では、同社の COTS ソリューションにおけるソフトウェアの脆弱性を軽減するために、頻繁に更新を提供している。しかし、このケースでは、問題となっているソフトウェアコンポーネントはこれらの更新の一部として含まれてなかった。

問題となっている脆弱性は、ABC Company の FP&A ソリューション内に存在しており、悪用できる状態になっている。

脅威シナリオ分析

攻撃者が ABC Company の製品の脆弱性を発見した場合、以下のような一連の事象が発生する可能性がある。

> 十分なリソースを持つサイバー犯罪組織が、FP&A ソリューションの顧客インスタンスに不正なコードをインストールする可能性がある。サイバー犯罪者がこの不正なコードを使用し、世界の株式市場で取引している公開企業の機密かつ非公開の財務情報を抜き取って販売する可能性がある。この攻撃が発見されると、ABC Company は否定的な評判によって、重大な風評被害に直面する可能性がある。ABC Company がソフトウェア製品の既知の脆弱性に適切にパッチを適用しなかった結果として、ABC Company の顧客が同社に対

して法的措置を講じる可能性がある。

軽減戦略

ABC Company は、セキュアなソフトウェア開発のためのプラクティスを強化し、製品の信頼性を高めるために、以下の改善点を識別した。

- 開発されるソフトウェアがセキュアなものになるように、開発者がセキュアな開発のためのプラクティスに関するトレーニングを受け、脆弱性ツールの使用に関する指導を受けることを確実にする。
- 再利用されるシステムコンポーネントが、社内開発であるかオープンソースであるかにかかわらず、既知の脆弱性に対する標準プロセスの一環として評価されるようにする（Ref. SA-15）。
- ソフトウェア製品のライフサイクル全体で保守を支援するために、システムコンポーネントのインベントリを維持する（Ref. CM-8）。
- システムコンポーネントで脆弱性が発生していないかを継続的に監視し、修正が利用可能になったら迅速に修復を実施するように適切なプロセスが実施されることを確実にする。可能な限りこのプロセスを自動化する（Ref. CA-7、RA-5）。

表 C-7：シナリオ 6

脅威シナリオ		
	脅威源	サイバー犯罪組織：脆弱なソフトウェアコンポーネント
	脆弱性	FP&A ソフトウェア製品で使用されている再利用コンポーネントの脆弱性の状態を把握し、監視して、既知の脆弱性にパッチを適用するための更新をタイムリーに提供することができない
	脅威事象の説明	サイバー犯罪組織は、FP&A ソフトウェア製品の既知の脆弱性を悪用して不正なコードをインストールし、ABC Company の顧客によって使用されているアプリケーションインスタンス内に含まれる機密の財務情報にアクセスする。
	既存のプラクティス	ABC Company には、社内で開発したコード内の脆弱性を識別し、軽減することに焦点を当てた、包括的でセキュアな SDLC がある。 ABC Company は、自社製品の脆弱性を解消するためのパッチを頻繁にリリースしている。
	脅威事象の結果	ABC Company の 10 社を超える大手顧客が、脆弱なソフトウェアの結果として侵害される。この攻撃を取り巻く否定的な報道が、ABC Company の株価に大きなインパクト（すなわち 5 % の下落）をもたらしている。ABC Company の競合他社はこの攻撃につけ込んで、独自のセキュリティプラクティスを使用して差別化を図り、市場シェアを獲得している。 ABC Company は、影響を受けた顧客が起こした訴訟のために、多額の訴訟費用に直面している。ABC Company では、この攻撃の翌年に 5 % という異常な顧客離れが発生した。

影響を受ける事業体単位、プロセス、情報、資産、又はステークホルダー		FP&A ソフトウェア製品部門
リスク	**インパクト**	高：3500 万ドルの総コスト、多大な風評被害、及び市場シェア、株価、顧客の喪失
	起こりやすさ	高：年換算で 20 % の発生確率
	リスクレベル（インパクト x 起こりやすさ）	高：7000 万ドルの損失リスク
	受容可能なリスクレベル	中：2000 万ドル：ABC Company のリスク委員会は、顧客の製品に影響を及ぼす単一のサイバーセキュリティ事象のために 2000 万ドルを超える損失を受けることは不本意であると述べている。
軽減	**潜在的な軽減戦略及び SCRM 管理策**	• 開発されるソフトウェアがセキュアなものになるように、開発者がセキュアな開発のためのプラクティスに関するトレーニングを受け、脆弱性ツールの使用に関する指導を受けることを確実にする。 • 再利用されるシステムコンポーネントが、社内開発であるかオープンソースであるかにかかわらず、既知の脆弱性に対する標準プロセスの一環として評価されるようにする（Ref. SA-15）。 • ソフトウェア製品のライフサイクル全体で保守を支援するために、システムコンポーネントのインベントリを維持する（Ref. CM-8）。 • システムコンポーネントで脆弱性が発生していないかを継続的に監視し、修正が利用可能になったら迅速に修復を実施するように適切なプロセスが実施されることを確実にする。可能な限りこのプロセスを自動化する（Ref. CA-7、RA-5）。
	軽減戦略の推定コスト	• 開発者トレーニング：50 万ドル～ 80 万ドル • システムコンポーネントのインベントリプロセス：120 万ドル～ 150 万ドル • システムコンポーネント脆弱性の継続的監視：80 万ドル～ 120 万ドル
	インパクトの変化	高：3500 万ドル（識別された管理策に基づく変化なし）
	起こりやすさの変化	低：年換算で 5 % の発生確率
	新しいリスクレベル	中：1750 万ドル

附属書 D：C-SCRMのテンプレート [42]

1. C-SCRM戦略及び実装計画

サプライチェーン全体のサイバーセキュリティリスクに対処するため、事業体はC-SCRM戦略を策定する。実装計画を伴うC-SCRM戦略は、事業体レベル（レベル1）であるが、事業体レベルで概説されているように、異なるミッション及びビジネス領域（レベル2）が特定のミッション及びビジネスニーズに対処するために、C-SCRM戦略をさらにテーラリングしてもよい。C-SCRM戦略及び実装計画は、包括的な事業体のリスクマネジメント戦略に準拠し、適用される法律、大統領令、指令、及び規制を順守することが望ましい。

以下のテンプレートで概説されているように、戦略及び実装計画の一般的なコンポーネントには、事業体全体のリスクマネジメント要件、所有権、リスク許容度、役割及び責任、及び、エスカレーション基準による、事業体のサプライチェーンリスク曝露（エクスポージャー）低減のための戦略的アプローチが含まれる。戦略及び実装計画は、単一の文書として策定される場合もあれば、複数の文書に分割して策定される場合もあることに留意されたい。いずれにせよ、これらのC-SCRMのアウトプットは、本質的に密接に関連していることが望ましい。

1.1. C-SCRM戦略及び実装計画のテンプレート

1.1.1. 目的

戦略及び実装文書における事業体の高レベルの目的を、事業体のミッション、ビジョン、及び価値観と整合させながら概説する。様々なティアで維持されなければならない他の*C-SCRM*文書に対して、戦略及び実装文書がどの位置にあるのかを説明する。事業体の*C-SCRM*の優先順位、及びその優先順位を達成するための一般的なアプローチについて、明確な方向性を提供する。

サンプルテキスト

この戦略及び実装文書の目的は、事業体のビジョン、ミッション、及び価値観をサポートし、有効なC-SCRMケイパビリティ（能力）、プラクティス、プロセス、及びツールを事業体内部に実装するための戦略的ロードマップを提供することである。

この戦略的アプローチは、事業体のミッションの範囲に及ぶ一連の目的を中心として体系化されており、事業体全体のC-SCRMの取り組みの実装の成功及び有効性を確実にするための段階的、達成可能、かつ戦略的なアプローチを反映している。

この戦略及び実装文書では、事業体内でC-SCRMケイパビリティ（能力）を実装するために事業体が採用する、必要な中核機能、役割、責任、及びアプローチについて論じる。ミッション及びビジネスポリシー、並びにシステム計画が策定され完成すると、本文書に添付資料として組みこまれる。結束性と一貫性を確実にするため、3つのティアすべての文書を定期的に一緒にレビューすることが望ましい。

[42] 各省庁及び関係機関は、大統領令14028号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装するために、附属書Fを参照することが望ましい。

この戦略及び実装計画の焦点は、中核的な基本的ケイパビリティ（能力）の確立に意図的に向けられている。ポリシー、所有権、及び専用リソースの定義といったベースライン機能は、事業体がC-SCRMケイパビリティ（能力）を徐々に拡大及び成熟させることができることを確実にする。この計画はまた、C-SCRM機能を実行できるようになるために、スタッフの意識を高め、C-SCRMを理解するための適切なトレーニングを確保し、必要な行動特性を伸ばす必要性を認識及び強調している。

この初期戦略及び実装計画では、業界全体の調整の取り組み、プロセス、及び決定への依存も認識している。政府及び業界全体の方向性、プロセスのガイダンス、及び要件が明確化され、伝達されるにつれて、事業体は戦略及び運用上の実装計画、並びに行動を更新し、改善していく。

1.1.2. 典拠及び法令順守

***C-SCRM*戦略及び実装を管理する法律、大統領令、指令、規制、ポリシー、標準、及びガイドラインをリスト化する。**

サンプルテキスト

- 法律
  - oリスク曝露（エクスポージャー）技術の活用法によるサイバーケイパビリティ（能力）の強化及び向上（Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology）（2018年）
  - o 連邦情報セキュリティ近代化法（Federal Information Security Modernization Act）（2014年）
  - o 2019年米国国防権限法（2019 National Defense Authorization Act）第889節 – 「特定の通信及び動画監視サービス又は機器の禁止（Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment）」
  - o グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act）
  - o医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability Act）
  - o大統領令14028号（2021年5月12日）、「国家のサイバーセキュリティの向上」

- 規制
  - o ニューヨーク州金融サービス局（NYDFS：New York State Department of Financial Services）23 NYCRR 500：第 500.11 節 サードパーティサービスプロバイダのセキュリティポリシー（Third Party Service Provider Security Policy）
  - oCIP-013-1：サイバーセキュリティ – サプライチェーンのリスクマネジメント（Cyber Security – Supply Chain Risk Management）
  - o 連邦金融機関検査協議会（FFIEC：Federal Financial Institutions Examination Council）情報セキュリティハンドブック II.C.20：サードパーティサービスプロバイダの監督（Oversight of Third-Party Service Providers）

- ガイドライン
  - o NIST 800-53, Revision 5： CA-5、SR-1、SR-2、SR-3
  - o NIST 800-37, Revision 2
  - o NIST 800-161, Revision 1： 附属書C
  - o ISO 28000:2007

1.1.3. 戦略的目的

戦略的目的は、事業体レベルの*C-SCRM*管理策及び要件を決定するための基礎を確立する。各目的は、しっかりとした*C-SCRM*プラクティス及びリスク低減の成果を追求するという、事業体が掲げた目的の達成をサポートする。これらの目的が合わさって、*C-SCRM*ケイパビリティ（能力）の活性化、及び事業体の目的の効果的な追求に必要な極めて重要な要素を、事業体に提供する。

全体として、戦略的目的は、以下のような極めて重要なC-SCRMケイパビリティ（能力）及び成功要因に対処することが望ましい。

- リスクマネジメント階層及びリスクマネジメントアプローチを実装すること
- C-SCRM要件を統合し、それらの要件を事業体ポリシーに組み込む事業体ガバナンス構造を確立すること
- サプライヤのリスクアセスメントアプローチを定義すること
- 品質アシュアランス、及び品質管理プロセス及びプラクティスを含む、品質及び信頼性プログラムを実装すること
- サプライチェーン、サイバーセキュリティ、製品のセキュリティ、及び物理的セキュリティ（及びその他の関連する）機能に対する、明示的な協力的役割、構造、及びプロセスを確立すること
- ポリシー、ガイダンス、及び管理策の適切な実装を確実にするために、適切なリソースが情報セキュリティ及びC-SCRMに充てられ、割り振られていることを確実にすること
- セキュリティインシデントの識別、対応、及び軽減を成功させるための、堅牢なインシデント管理プログラムを実装すること
- 緊急時対応計画、インシデント対応、及び災害時復旧計画及びテストに、重要なサプライヤを含めること

サンプルテキスト

目的 1：サプライチェーン全体のサイバーセキュリティリスクを効果的に管理する

この目的は、事業体がC-SCRMを追求する主要な意図に対処する。事業体全体のC-SCRMプログラムを確立し、維持することで、事業体のリスク所有者は、事業体の資産、機能、及び関連サービスに対するサプライチェーンのリスクを識別、アセスメント、及び軽減できるようになる。機能の焦点、幅、及び深さの範囲を維持及び成長させることができる初期のケイパビリティ（能力）の実装は、段階的に行われ、事業体が意識向上、保護、レジリエンスなどの領域において、望ましいC-SCRM目標を達成することができることを確実にする、包括的な「人、プロセス、技術」のニーズを取り込む。

目的 2：顧客にとって信頼できる供給源となる

大規模に、事業体の多様なポートフォリオをまたがる顧客のサプライチェーンリスクに対応するには、優先順位付けのアプローチ、構造、改善されたプロセス、及び継続的なガバナンスが必要である。C-SCRMプラクティス及び管理策は、事業体の顧客に当てはまる個別の様々なサプライチェーンの脅威及び脆弱性に対処するためにテーラリングされる必要がある。この目的は、以下によって達成することができる。

- 外部プロバイダの精査プロセス、C-SCRM要件、及び監督を強化する。
- 顧客のサイバーセキュリティリスク選好度、許容度、及び環境に従って、顧客のニーズが満

たされることを確実にする。

目的 3：事業体をC-SCRM分野の業界リーダーとして位置付ける

事業体は、業界全体のサプライチェーンにおけるサイバーセキュリティリスクの管理方法に対処する改善を可能にし、推進するのに適した立場にある。したがって、事業体は、サプライチェーンリスクへの対処に関する事業体の要件及び期待について、業界関係者のコミュニケーション、動機付け、及び教育を提唱するために、この立場を利用しなければならない。

1.1.4. 実装計画及び進捗追跡

事業体の*C-SCRM*戦略的目的の進捗を追跡する方法論及びマイルストーンを概説する。事業体のコンテキストはこのプロセスに大きな影響を与えるが、事業体は、本質的に重要又は基本的なタスクの実行を促進するために、優先順位付けされた時間範囲を定義することが望ましい。そのような時間範囲を定義する一般的な用語は、「這う、歩く、走る（*crawl, walk, run*）」である。指定された時間範囲に関わらず、実践的で優先順位付けされた計画の実装は、*C-SCRM*ケイパビリティ（能力）の確立又は強化に勢いをつけるために不可欠である。

実装計画がベースライン化されると、実装計画の変更及び進捗の追跡を推進するために、問題のエスカレーションプロセス及びフィードバックメカニズムが含まれる。

サンプルテキスト

[事業体の]C-SCRM戦略目的の実行、及び、基本となる活動の持続的な運用有効性には、進捗の追跡への正式なアプローチ及びコミットメントが必要である。[事業体]は、実装計画に補助的なマイルストーン及び実装日を定義することで、戦略目的の実装を追跡し、アセスメントする。実装計画の要素を監視及び報告するには、複数の分野にまたがる責任の共有、及び事業体横断なチームベースのアプローチが必要である。

以降の実装計画は、ミッション及びビジネスのオーナーによって継続的に維持され、定期的な監督活動の一環として上級幹部チームによってレビューされる。実装計画にインパクトを与えるリスク及び問題は、ミッション及びビジネスのオーナー又はそのチームによって、上級幹部チームに積極的に提起されることが望ましい。実装計画はその後、上級幹部の裁量に従って改訂される可能性がある。

表 D-1：目的 1 – サプライチェーン全体のサイバーセキュリティリスクを**効果的に管理するための実装マイルストーン**

実装計画マイルストーン	ステータス	オーナー	優先順位	完了予定日
ポリシー及び権限を確立する	計画済み	J. Doe	今すぐ実行	XX/XX/XX
管理職による監督及び指示を確立し、提供する	完了	…	次に実行	…
C-SCRMをエンタープライズリスクマネジメント（ERM）フレームワークに統合する	遅延	…	後で実行	…

実装計画マイルストーン	ステータス	オーナー	優先順位	完了予定日
C-SCRM PMOのケイパビリティ（能力）を確立する	取り消し済み	…	…	…
役割及び責任を確立し、説明責任を割り当てる	…	…	…	…
C-SCRM計画を策定する	…	…	…	…
内部の意識向上機能を確立する	…	…	…	…
サプライチェーンのリスクアセスメントのケイパビリティ（能力）を識別、優先順位付け、及び実装する	…	…	…	…
事業体レベルのC-SCRM管理策を確立、文書化、及び実装する	…	…	…	…
C-SCRMリソース要件を識別し、持続的な資金を確保する	…	…	…	…
C-SCRMプログラムのパフォーマンス監視を確立する	…	…	…	…

表 D-2：目的 2 – 顧客にとって信頼できる供給源として機能するための実装マイルストーン

実装計画マイルストーン	ステータス	オーナー	優先順位	完了予定日
C-SCRM活動、顧客に対応する事業分野、プログラム及び提供されるソリューションを組み込む	計画済み	J. Doe	今すぐ実行	XX/XX/XX
顧客サポート人員が、サプライチェーン全体の管理要件及びサイバーセキュリティリスクに精通していることを確実にする	完了	…	次に実行	…
サイバーセキュリティのサプライチェーンアシュアランスの最低ベースラインレベルを確立する	遅延	…	後で実行	…
識別されたリスクに対応するためのプロセス、及び事業体のサプライチェーンへのインパクトを監視するためのプロセスを確立する	取り消し	…	…	…

表 D-3：目的 3 – 事業体を C-SCRM 分野の業界リーダーとして位置付けるための実装マイルストーン

実装計画マイルストーン	ステータス	オーナー	優先順位	完了予定日
ミッションクリティカルなサプライチェーンの脅威への迅速なアクセスを確実にするために、国家安全保障及び法執行機関と連携し、関与する	計画済み	J. Doe	今すぐ実行	XX/XX/XX
C-SCRM改善の機会を評価し、業界全体の共通ソリューション及び共有サービスの要件及び監督を強化する	完了	…	次に実行	…
開発者向けのセキュアなコーディングトレーニングを含む、トレーニング及び人材開発を通じたC-SCRM意識及び行動特性を提唱する	遅延	…	後で実行	…
C-SCRM関連のホワイトペーパー及び公開ガイダンスを発表する	取り消し	…	…	…

1.1.5. 役割及び責任

戦略及び実装テンプレートに責任を負う人員、及び主要な貢献者を指名する。各個人又はグループの役割及び名前に加え、必要に応じて連絡先情報（例えば、事業体の所属、住所、メールアドレス、及び電話番号）を含める。

サンプルテキスト

- 上級幹部は、以下のことを行わなければならない。
  - o 事業体のC-SCRM戦略目的及び実装計画を承認する。
  - o C-SCRMの実装及び有効性の監督を提供する。
  - o 優先順位及びリソース調達のニーズに関するC-SCRMの方向性及び決定を伝達する。
  - o 事業体のリスク選好度及びリスク許容度を決定する。
  - o 事業体のリスク態勢にインパクトを与える可能性のある、リスクの高いC-SCRM問題のエスカレーションにタイムリーに対応する。
- ミッション及びビジネスリーダーは、以下のことを行わなければならない。
  - o ミッションレベルのリスク選好度及び許容度を決定し、それらが事業体の期待に沿ったものであることを確実にする。
  - o サプライチェーンのリスクマネジメント要件、及び事業体の目的をサポートする管理策の実装を定義する。
  - o ミッションの機能及び資産の重要度分析を継続する。
  - o ミッション及びビジネス関連の調達についてのリスクアセスメントを実行する。

1.1.6. 定義

戦略及び実装テンプレートの中で説明されている主要な定義をリスト化し、必要に応じて、事業体特有のコンテキスト及び例を提供する。

サンプルテキスト

- 事業体：定義されたミッション、目標、及び境界を持ち、そのミッションを実行するために情報システムを使用し、自らのリスク及びパフォーマンスを管理する責任を持つ組織。事業体は、取得、プログラムマネジメント、財務管理（例えば、予算）、人事、セキュリティ、情報システム、情報及びミッションの管理のすべて又は一部のビジネスの側面で構成される場合がある。

- 目的：事業体の目標を広範に表現したもの、及び、業務に対する特定の目標成果。

1.1.7. 改訂及び保守

戦略及び実装テンプレートの改訂の必要な頻度を定義する。バージョン管理を実施するために、改訂表を保守する。戦略及び実装テンプレートは、更新され、すべての適切な個人（例えば、スタッフ、請負事業者、及びサプライヤ）に伝達されなければならない、生きた文書である。

サンプルテキスト

[事業体の]戦略及び実装テンプレートは、法律、ポリシー、標準、ガイドライン、及び管理策への変更は動的で進化しているため、最低でも（連邦政府の環境内で）3～5年ごとにレビューしなければならない。臨時の改訂の契機となる可能性がある追加の基準は、以下のものが含まれる。

- 戦略及び実装テンプレートにインパクトを与えるポリシーの変更
- 重要な戦略及び実装の事象
- 新技術の導入
- 新たな脆弱性の発見
- 運用又は環境の変化
- 戦略及び実装テンプレートの欠陥
- 範囲の変更
- その他の事業体固有の基準

表 D-4：バージョン管理表

バージョン番号	日付	変更／改訂の説明	影響を受ける節／ページ	変更者の氏名／肩書／事業体

2. C-SCRMポリシー

C-SCRMポリシーは C-SCRM戦略の実装を指示する。C-SCRMポリシーは、レベル1及び／又はレベル2で策定することができ、C-SCRM戦略からのリスクのコンテキスト、リスクの決定、及びリスク活動を含む、ミッション固有及びビジネス固有の要因から情報を得る。C-SCRMポリシーは、適用可能な事業体ポリシー（例えば、取得及び調達、情報セキュリティ及びプライバシー、物流、品質、及びサプライチェーン）をサポートする。C-SCRMポリシーは、事業体のC-SCRM戦略で概説されている目標及び目的に対処し、その戦略は、事業体の戦略計画から情報を得ている。また、C-SCRMポリシーはミッション及びビジネスファンクション、並びに内部及び外部の顧客要件にも対処することが望ましい。C-SCRMポリシーはまた、C-SCRMと事業体のリスクマネジメントプロセスとの統合ポイントを定義する。最後に、C-SCRMポリシーは、事業体内におけるC-SCRMの役割及び責任、それらの役割間の相互依存性、及び役割間の相互作用を、より具体的かつ詳細なレベルで定義する。レベル1のC-SCRMポリシーはより広範であるのに対し、レベル2のC-SCRMポリシーはミッション及びビジネスファンクションに固有のものである。C-SCRMの役割は、調達、リスクアセスメントの実施、サプライチェーンの脅威情報の収集、リスクベースの軽減策の識別及び実装、監視、及びその他のC-SCRM機能に対する責任を規定する。

2.1. C-SCRMポリシーのテンプレート

2.1.1. 典拠及び法令順守

***C-SCRM*ポリシーの基準となる法律、大統領令、指令、規制、ポリシー、標準、及びガイドラインをリスト化する。**

レベル1のサンプルテキスト

- ポリシー
  - [事業体の名称] エンタープライズリスクマネジメントポリシー
  - [事業体の名称] 情報セキュリティポリシー
- 法律
  - リスク曝露（エクスポージャー）技術の活用法によるサイバーケイパビリティ（能力）の強化及び向上（Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology）（2018 年）
- 規制
  - NYDFS 23 NYCRR 500：第 500.11 節 サードパーティサービスプロバイダのセキュリティポリシー
  - CIP-013-1： サイバーセキュリティ – サプライチェーンのリスクマネジメント
  - FFIEC 情報セキュリティハンドブック II.C.20：サードパーティサービスプロバイダの監督

レベル2のサンプルテキスト

- ポリシー
  - [事業体の名称] C-SCRMポリシー
  - [ミッション及びビジネスプロセスの名称] 情報セキュリティポリシー

- 規制
  - o NYDFS 23 NYCRR 500：第 500.11 節 サードパーティサービスプロバイダのセキュリティポリシー

- ガイドライン
  - o NIST 800-53, Revision 5： SR-1、PM-9、PM-30、PS-8、SI-12
  - o NIST 800-161, Revision 1： 附属書C

2.1.2. 説明

***C-SCRM*ポリシーの目的及び範囲を説明し、計画を着実に実行し、管理策を実施し、最新であることを確実にする、という事業体責任者の意向を概説する。ポリシーが適用されるティアを定義する。*C-SCRM*ポリシーの全部又は一部は、既存のポリシー又はその他のガイダンスから派生させる必要がある場合がある。**

レベル*2*の場合、*C-SCRM*ポリシーは、レベル*2*のポリシーに影響を与えるすべてのレベル*1*のポリシー及び計画をリスト化し、ミッション及びビジネスがどのようなものを包含するかについて簡潔な説明を提供し、レベル*2*の*C-SCRM*ポリシーの適用範囲（例えば、計画、システム、調達の種類など）を簡潔に記述することが望ましい。

レベル1のサンプルテキスト

[事業体] は、顧客に購入、使用、及び提供される製品、サービス、及びソリューションのリスクを懸念している。

[事業体の] C-SCRMプログラムのポリシーの目的は、[事業体] によって使用され、提供される製品、サービス、及びソリューションが信頼でき、適切にセキュアでレジリエンス力があり、要求される品質基準を満たすことができるという、改善されたアシュアランスを提供するケイパビリティ（能力）を成功裏に実装し、維持することである。

C-SCRMは、サプライチェーン全体の影響の受けやすさ、脆弱性、及び脅威を識別してアセスメントし、リスク曝露（エクスポージャー）を低減し、脅威と戦うための戦略及び軽減管理策を実装するための体系的なプロセスである。事業体全体のC-SCRMプログラムを確立して持続させることにより、[事業体の] リスク所有者は、[事業体の] ミッション資産、機能、及び関連サービスに対するサプライチェーンのリスクを識別、アセスメント、及び軽減することが可能となる。

レベル 2 のサンプルテキスト

[ミッション及びビジネスプロセス] は、[事業体の目的] に対する重要度を認識している。製品を製造する重要なコンポーネントには、複数のサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダの間の調整が含まれる。[ミッション及びビジネスプロセス] は、サプライチェーン全体のサイバーセキュリティリスクが実現することで、必要とされる品質基準に従ってタイムリーに製品を生み出す [ミッション及びビジネスプロセスの] 能力が中断されたり、完全に阻害されたりする可能性があることを認識している。

[事業体のレベル1のポリシー] によって規定されたC-SCRMの目的に基づき、[ミッション及びビジネスプロセスの] ポリシーの目的は、サプライチェーン全体のサイバーセキュリティリスクのアセスメント、対応、及び監視を可能にするC-SCRMケイパビリティ（能力）を実装することである。

事業体全体のC-SCRMプログラムによって規定されたポリシー及び要件に合ったC-SCRMケイパビリティ（能力）は、[ミッション及びビジネスプロセス] がコンポーネントの調達、及び主要製品の組み立てに関する固有の要件を満たすためにC-SCRMプロセス及びプラクティスをテーラリングする境界を提供する。

2.1.3. ポリシー

事業体の*C-SCRM*戦略計画の目標及び目的、ミッション及びビジネスファンクション、並びに、内部及び外部顧客の要件を支える、必須の高レベルのポリシーステートメントを概説する。

レベル 1 のサンプルテキスト

[事業体の] 事業体レベルのC-SCRMプログラムは、以下のケイパビリティ（能力）を実装して持続させるために確立されている。

- 対象品目の取得及び使用から生じるサイバーセキュリティリスクへの適切なリスク対応をアセスメントして提供する。
- サプライチェーン全体のサイバーセキュリティリスクのアセスメントと、ミッション、システム、コンポーネント、サービス、又は資産の重要度アセスメントに基づくリスク対応措置に優先順位を付ける。
- 全体的なC-SCRM戦略、及び高レベルの実装計画、ポリシー、及びプロセスを策定する。
- サプライチェーンのリスクマネジメントのプラクティスを、対象品目の取得及び資産管理のライフサイクルの全体を通じて統合する。
- 業界全体の基準及びガイドラインに従って、C-SCRM情報を共有する。
- 実装の進捗及びプログラムの有効性を指導及び監督する。

C-SCRMプログラムは、以下のことを行うものとする。

- [事業体の] C-SCRMプログラム管理者として機能し、C-SCRMプログラムマネジメントオフィス（PMO）の議長を務める、指名された上級幹部によって、一元的に主導及び調整される。
- [事業体の] 既存のリスクマネジメント及び意思決定のガバナンスプロセス及び構造を活用し、それらに適切に統合される。
- チームベースのアプローチを反映し、協調的で、多分野にまたがり、事業体内部で行われる性質及び構成とする。
- NISTリスクマネジメントフレームワーク及び NIST SP 800-161, Rev. 1 と整合性のある、レベルのリスクマネジメントアプローチを組み入れる。
- 成文化された規制のC-SCRM要件、及び業界全体及び事業体固有のポリシーの方向性、ガイダンス、及びプロセスを実装する。

レベル 2 のサンプルテキスト

[ミッション及びビジネスプロセスの] C-SCRMプログラムは、以下のことを行うものとする。

- [事業体の] C-SCRMプログラムによって規定された要件及びガイダンスに従って運用する。
- [ミッション及びビジネスプロセスの] 中核的な目的の追求から生じるサイバーセキュリティリスクのアセスメント、対応、及び監視を行うために必要なC-SCRMプラクティス及びケイパビリティ（能力）を適用するために、C-SCRMプログラムマネジメントオフィス（PMO）と協力する。
- サプライチェーン全体のサイバーセキュリティリスクを管理するという [事業体の] 目的をサポートするために、C-SCRM活動を適用可能な活動に統合する。
- [ミッション及びビジネスプロセス] 内のC-SCRM活動の調整に必要なリソースを割り当て、充当する。
- [ミッション及びビジネスプロセスの] 重要なサプライヤを識別し、その関係から生じるリスク曝露（エクスポージャー）のレベルをアセスメントする。
- サプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）を低減するために、リスク対応の取り組みを実装する。
- サプライチェーンプロファイルにおける [ミッション及びビジネスプロセスの] 継続的なサイバーセキュリティリスクの曝露（エクスポージャー）を監視し、識別された事業体のリスクマネジメント及びC-SCRMステークホルダーに定期的な報告を提供する。

2.1.4. 役割及び責任

***C-SCRM*ポリシーの責任者及び主要な貢献者を明記する。各個人又はグループの役割及び名前に加え、必要に応じて連絡先情報（例えば、事業体の所属、住所、メールアドレス、及び電話番号）を含める。**

レベル 1 のサンプルテキスト

- C-SCRMプログラム管理者は、以下のことに責任を負うものとする。
    - o 指名されたC-SCRMリーダーと協調及び協議して、C-SCRMプログラムの確立、策定、及び監督を主導する。
    - o C-SCRM PMOを設立し、その議長を務める。 このチームは、議長及び指名されたC-SCRMリーダーで構成され、C-SCRM戦略、実装計画、及びC-SCRM関連の問題に対処する行動の策定及び調整、プログラムの報告及び監督、並びにプログラムのリソースの識別及び推奨事項の作成に責任を負う。
    - o 必要に応じて、C-SCRMの問題を責任者にエスカレーション及び／又は報告する。
- 各 C-SCRMセキュリティ責任者は、以下のことに責任を負うものとする。
    - o C-SCRMリーダーを特定する（リーダーはC-SCRM PMOの協力的及び中核的メンバーとして参加する責任を負う）。
    - o 関連するC-SCRM機能を、事業体及び役職レベルの機能に組み込む。
    - o C-SCRMプログラムの要件を実装し、準拠する。

レベル 2 のサンプルテキスト

- C-SCRMリーダーは、以下のことに責任を負うものとする。
  - o C-SCRM PMOメンバーの関心及びニーズを示す。
  - o プログラム又は事業分野のC-SCRM計画の策定及び実行を主導及び／又は調整する。これには、そのような計画が事業体レベルのC-SCRM計画に適切に整合され、統合されることを確実にすることが含まれるものとする。

- ミッション及びビジネスプロセスのC-SCRMスタッフは、以下のことに責任を負うものとする。
  - o C-SCRM活動の最初の実行（例えば、サプライヤ又は製品のアセスメント）。
  - o C-SCRMスタッフ以外によって推進される、ミッション及びビジネス固有のC-SCRM活動のサポート。

2.1.5. 定義

ポリシー内で説明されている主要な定義をリスト化し、必要に応じて、事業体固有のコンテキスト及び例を提供する。

サンプルテキスト（レベル1及び／又はレベル2に適用）

- 対象品目：あらゆる種類のクラウドコンピューティングサービス、通信機器又は通信サービス、管理対象非機密情報プログラムの要件の対象である連邦政府又は非連邦政府情報システム上の情報の処理、及びすべての IoT/OT（例えば、組み込み又は付随的な情報技術を含むハードウェア、システム、デバイス、ソフトウェア、又はサービス）を含む情報技術。

- サプライチェーンのサイバーセキュリティリスクアセスメント：サプライチェーン全体のサイバーセキュリティリスク、それらの発生可能性、及び潜在的なインパクトの体系的な検討。

- リスク所有者：リスクを管理する説明責任及び権限を持つ人又はエンティティ。

2.1.6. 改訂及び保守

***C-SCRM*ポリシーの改訂及び保守の必要な頻度を定義する。バージョン管理を実施するために、改訂表を保守する。*C-SCRM*ポリシーは、更新され、すべての適切な個人（例えば、スタッフ、請負事業者、及びサプライヤ）に伝達されなければならない、生きた文書である。**

サンプルテキスト（レベル1及び／又はレベル2に適用）

[事業体の] C-SCRMポリシーは、法律、ポリシー、標準、ガイドライン、及び管理策の変更は動的で進化しているため、最低でも1年ごとにレビューされなければならない。臨時改訂の契機となる可能性がある追加の基準には、以下のものが含まれる。

- C-SCRMポリシーにインパクトを与えるポリシーの変更
- 重要なC-SCRMの事象
- 新技術の導入

- 新たな脆弱性の発見
- 運用又は環境の変化
- C-SCRMポリシーの欠陥
- 範囲の変更
- その他の事業体固有の基準

表 D-5：バージョン管理表

バージョン番号	日付	変更／改訂の説明	影響を受ける節／ページ	変更者の氏名／肩書／事業体

3. C-SCRM計画

C-SCRM計画はティア3で策定され、実装固有であり、ポリシーの実装、要件、制約条件、及び関連事項を提供する。これは、独立したものにすることも、システムセキュリティ及びプライバシー計画のコンポーネントにすることもできる。組み込まれる場合、C-SCRMコンポーネントは明確に識別できなければならない。C-SCRM計画は、C-SCRM管理策の管理、実装、及び監視、並びに、ミッション及びビジネスファンクションをサポートするためのSDLC全体のシステムの開発及び持続化に対処する。C-SCRM計画は、[FIPS 199] に従って、高インパクトシステム及び中インパクトシステムに適用される。

サプライチェーンが事業体間及び事業体内部で大きく異なる可能性があることを考慮すると、C-SCRM計画は個々のプログラム、事業体、及び運用状況に合わせてテーラリングされることが望ましい。テーラリングされたC-SCRM計画は、技術、サービス、システムコンポーネント、又はシステムが目的に適合しているかどうかを判断するための基礎を提供するため、管理策はそれに応じてテーラリングされる必要がある。テーラリングされたC-SCRM計画は、事業体が、ミッション及びビジネス要件並びにリスク環境に基づいて、最も重要なミッション及びビジネスファンクションにリソースを集中させるのに役立つ。

以下のC-SCRM計画のテンプレートは、一例としてのみ提供されている。事業体は、C-SCRM計画の策定及び提示のために、様々なアプローチを策定して実装する柔軟性を持っている。事業体は、C-SCRM計画のすべての関連する節を確実に把握するために、自動化されたツールを活用することができる。自動化されたツールは、コンポーネントのインベントリ、役割を果たす個人、セキュリティ管理策の実装情報、システム図、サプライチェーンコンポーネントの重要度、及び相互依存関係などのC-SCRM計画の情報を文書化するのに役立てることができる。

3.1. C-SCRM計画のテンプレート

3.1.1. システムの名称及び識別子

システムに一意の識別子及び／又は名称を指定する。適用可能な過去の名称、及び、関連するティア*1*及びティア*2*の文書タイトルを含める。

サンプルテキスト

このC-SCRM計画は、[システムの名称][一意の識別子] のセキュリティ要件の概要を提供し、システムによって伝送、処理、又は保存される情報に適した、目的に適合するC-SCRM管理策を提

供するために、実装中又は実装が計画されているサプライチェーンのサイバーセキュリティ管理策を説明する。

[一意の識別子] に対して実装されるセキュリティの保全措置は、事業体のC-SCRM戦略及びポリシーガイダンスに明記されている要件を満たしている。

3.1.2. システムの説明

システムの機能、目的、及び範囲を説明し、処理される情報の説明を含める。以下のシステム、システムコンポーネント、又はシステムサービスの研究開発、設計、製造、取得、納入、統合、運用及び保守、並びに廃棄に関連するサプライチェーンリスクを管理するためのシステムのアプローチの一般的な説明を提供する。

***C-SCRM*計画が、事業体のサプライチェーンリスク許容度、受容可能なサプライチェーンリスクの軽減戦略又は管理策、サプライチェーンリスクを一貫して評価及び監視するためのプロセス、計画を実装及び伝達するためのアプローチ、及び実施されるサプライチェーンリスク軽減措置の説明及びその正当性のコンテキストで、システムを説明していることを確実にする。説明は、レベル*1*及びレベル*2*で確立された、システムの高レベルのミッション及びビジネスファンクション、システムの認可境界、サポートするシステム及び関係を含む全体的なシステムアーキテクチャ、システムが事業体のミッションをどのようにサポートするか、及びシステム環境（例えば、スタンドアロン、マネージド／エンタープライズ、カスタム／特化型、セキュリティが制限された機能、クラウド）と整合していなければならない。**

サンプルテキスト

[事業体の] 文書マネジメントシステム（DMS：Document Management System）は、動的な情報リポジトリ、ファイル階層、及び、内部のチームのコミュニケーション及び協調を合理化するためのコラボレーション機能を提供するのに役立つ。システム内で管理されるデータには、個人情報（PII）が含まれている。DMSは、米国内の検証済みサプライヤ [サプライヤの名称] から直接購入した市販（COTS）ソリューションである。DMSは事業体のニーズを満たすように、機能的に構成されている。システムの展開又は保守のために、サードパーティのコードライブラリは利用されていない。DMSは事業体の主要な仮想プライベートクラウドプロバイダの管理レイヤー内で運用されている。

DMSは、ダウンタイムが発生した場合に1時間の目標復旧時間（RTO：Recovery Time Objective）を義務付ける、カテゴリ1のシステムである。事業体は、第一のプラットフォームでカテゴリ1のRTOが満たされない可能性がある場合に、事業体が切り替えることができる第二のプライベートクラウドプロバイダを使用して、災害復旧環境を維持する。

3.1.3. システムの情報の種類及び分類化

以下の表は、システム及び／又はその境界内のサプライチェーンによって処理、保存、又は伝送される情報の種類を規定する。事業体は、情報の種類及び暫定的なインパクトレベルを識別するために、*[NIST SP 800-60 v2]*、米国立公文書記録管理局（*NARA：National Archives and Records Administration*）の管理対象非機密情報（*CUI：Controlled Unclassified Information*）*[NARA CUI]*、又はその他の事業体特有の情報の種類を利用する。事業体は、*[FIPS 199]* の連邦政府情報及びシステムの分類化に関するガイダンスを使用して、各情報の種類のセキュリティインパクトレベルを決定する。各セキュリティ目的（すなわち、機密性、完全性、可用性）のインパクトレベル（すなわち、低、中、高）を明確にする。

サンプルテキスト

表 D-6：システムの情報の種類及び分類化

情報の種類	セキュリティの目的		
	機密性 （低、中、高）	完全性 （低、中、高）	可用性 （低、中、高）

上記の表に基づいて、各セキュリティインパクトのそれぞれの最高水準（すなわち、低、中、高）を示す。システム全体の分類を決定する。

表 D-7：セキュリティインパクトの分類化

セキュリティ目的	セキュリティインパクトレベル
機密性	☐ 低 ☐ 中 ☐ 高
完全性	☐ 低 ☐ 中 ☐ 高
可用性	☐ 低 ☐ 中 ☐ 高
システム全体のセキュリティ分類	☐ 低 ☐ 中 ☐ 高

3.1.4. システムの運用ステータス

サンプルテキスト

表 D-8：システムの運用ステータス

システムの運用ステータスを示す。2つ以上のステータスが選択される場合は、システムのどの部分が各ステータスに含まれるのかをリスト化する。

システムのステータス		
☐	運用中	システムが現在運用中であり、本番稼働している。
☐	開発中	システムが設計、開発、又は実装されている。
☐	大規模変更	システムの大規模な変更、開発、又は移行が行われている。
☐	廃棄	システムは現在運用されていない。

3.1.5. システム図／ネットワーク図、インベントリ、及びライフサイクルの活動

システムコンポーネントのインベントリを伴う最新かつ詳細なシステム図及びネットワーク図、又は、図及びインベントリ情報を確認できる場所への参照を含める。

活動がマッピングされ、追跡されることを確実にするために、上記のコンポーネントをシステムの*SDLC*に対してコンテキスト化する。*C-SCRM*活動は、ライフサイクルを通じて（スパイラル又はアジャイル技法を使用して）反復すること及び再統合することが必要である可能性があるため、これは*C-SCRM*活動の完全な適用範囲を保証する。*C-SCRM*計画の活動は、概念から開発、製造、利用、サポート、及び廃止までの全ステップで必要とされる。

サンプルテキスト

[システムの名称] コンポーネントには、以下が含まれる可能性がある。

- コンポーネントの説明
- バージョン番号
- ライセンス番号
- ライセンス保有者
- ライセンスの種類（例えば、シングルユーザ、パブリックライセンス、フリーウェア）
- バーコード／プロパティ番号
- ホスト名（すなわち、ネットワーク上のコンポーネントを識別するために使用される名称）
- コンポーネントの種類（例えば、サーバ、ルータ、ワークステーション、スイッチ）
- 製造業者
- モデル

- シリアル番号
- コンポーネントのリビジョン番号（例えば、ファームウェアのバージョン）
- 物理的な場所：（コンピュータ／サーバルーム内のコンポーネントの具体的なラックの場所を含む）
- ベンダ名

3.1.6. 情報交換及びシステム接続

システムと他のシステム間の情報交換合意（例えば、相互接続に関するセキュリティ合意書*[ISA：Interconnection Security Agreements]*、了解事項覚書*[MOU：Memoranda of Understanding]*、合意覚書*[MOA：Memoranda of Agreement]*）、合意日、他のシステムのセキュリティ認可ステータス、認可権限のある担当者名、接続の説明、及び、情報交換のフローを示す図をリスト化する。

サンプルテキスト

表 D-9：情報交換及びシステム接続

合意日	システムの名称	事業体	接続の種類又は情報交換の方法	FIPS 199 の分類	認可ステータス	認可権限のある担当者名及び役職

3.1.7. セキュリティ管理策の詳細

ライフサイクルベースのシステムセキュリティエンジニアリングプロセスの一環として実装されたセキュリティ設計原則の適用を含む、統合的信頼性があり、セキュアで、プライバシーを保護し、かつレジリエントなシステムコンポーネント及びシステムを開発するための要件に、計画が対応することを確実にするために*C-SCRM*管理策を文書化する。アセスメント、標準の運用手順、責任、ソフトウェア、ハードウェア、製品、サービス、及び*DevSecOps*の考慮事項など、関連するトピック領域を考慮する。

各管理策について、適用可能なベースラインのセキュリティ管理策がどのように実装されているかについて詳細な説明を提供する。管理策の実装に関連する成果物をすべて含める。必要に応じて、管理策のテーラリングの正当な理由を組み入れる。該当する場合、継承された管理策を提供する該当するレベル*1*及び／又はレベル*2*の*C-SCRM*ポリシーを参照する。*CIO*、*CAO*、又は*PMO*からの複数のレベル*1*のポリシーが存在する可能性がある。

サンプルテキスト

SR-6 サプライヤのアセスメント及びレビュー

実装：包括的な広域防御の情報セキュリティ戦略の一環として、事業体は、サプライチェーン全体のサイバーセキュリティリスクマネジメントに対処するためのC-SCRMプログラムを確立した。C-SCRM PMOは、事業体全体のC-SCRMのレベル2のポリシー要件に従い、[システムの名称] と統合しようとするビジネスパートナーに起因するサイバーセキュリティリスクのアセスメントを実施する責任を負う。C-SCRMトレーニング及び意識向上の資料も、 [システムの名称] へのアクセス権を受け取る前に、すべての個人に提供されなければならない。

拡張管理策：[NIST 800-161]の拡張管理策2、7、及び8を適用可能。

（2）サプライヤのレビュー
実装：C-SCRM PMOは、[システムの名称] に関連する情報システム、コンポーネント、又はサービスを取得するための契約上の合意を締結する前に、サプライチェーンのリスクアセスメント（SCRA：Supply Chain Risk Assessments）の形式でビジネスパートナーにサプライヤのレビューを提供する。レベル1の戦略及びレベル2のポリシーの文書は、ITシステム、コンポーネント、及び／又はサービスを取得しようとするビジネスパートナーにSCRA要件を課す。SCRAは、C-SCRM PMOによるサプライヤのアセスメントに備えて、ビジネスパートナーが従うべき段階的なガイドを提供する。

（7）選択／受け入れ／更新前のアセスメント
実装：レベル2のポリシーは、どの [システムの名称] の統合活動にSCRAが必要であるかを定義する。プロセス及び要件は、SCRAの標準運用手順に定義されている。

（8）オールソースインテリジェンスの使用
実装：C-SCRM PMOは、[システムの名称] のサプライチェーンのリスクアセスメントを実施する際に、オールソースインテリジェンスを利用する。

3.1.8. 役割の識別

重要なサイバーセキュリティサプライチェーン人員の役割、氏名、部署／部門、主たる電話番号及び代替電話番号、及びメールアドレスを識別するか、連絡先（例えば、ベンダの連絡先、取得の特定分野専門家*[SME]*、エンジニアリングリーダー、ビジネスパートナー、サービスプロバイダ）を役割、氏名、住所、主たる電話番号及び代替電話番号、及びメールアドレスとともに指定する。

サンプルテキスト

表 D-10：役割の識別

役割	氏名	部署／部門	主たる 電話番号	代替 電話番号	メールアドレス
ベンダの連絡窓口					
取得のSME					
エンジニアリングリーダー					
ビジネスパートナー					
サービスプロバイダ					

3.1.9. 緊急時及び非常時

緊急時又は非常時の業務の発生時に製品を取得することを選択する組織に対して、事業体は、ミッション継続を可能にするために、通常の*C-SCRM*取得プロセスを無視しなければならない可能性がある。承認済みの*C-SCRM*計画のプロセスによって調査されていない契約活動は、事業体に業務上のリスクをもたらす。

必要があれば、正式な仕事の割り当て及び承認の指揮系統なしに助言を提供できる*C-SCRM*、取得、及び法律の特定部門専門家の連絡先情報など、緊急時及び非常時に従うべき省略された取得手順を説明する。

サンプルテキスト

機器が緊急で必要となる非常時の場合、C-SCRM PMOは、正式な仕事の割り当て及び指揮系統による承認なしに支援を提供するために、C-SCRMの特定分野の専門家（SME）を通じて援助を行う。CIOは、通常の手順を無視するためのそのような免除を与える権限を持つ。C-SCRMのSMEの現在の連絡先情報を以下に示す。

- C-SCRMのSMEの連絡先（POC：Point of Contact）
  氏名
  メールアドレス
  電話番号
- 取得のSMEのPOC
  氏名
  メールアドレス
  電話番号
- 法律のSMEのPOC
  氏名

メールアドレス
電話番号

3.1.10.関連する法律、規制、及びポリシー

システムに適用可能な法律、大統領令、指令、ポリシー、及び規制（例えば、大統領令*14028*号、連邦調達規則（*FAR*：*Federal Acquisition Regulations*）、*FERC*など）をリスト化する。レベル*3*の場合、該当するレベル*1*の*C-SCRM*戦略及び実装計画、及びレベル*2*の*C-SCRM*ポリシーのタイトルを含める。

サンプルテキスト

事業体は、C-SCRM計画の管理策が、連邦情報セキュリティ近代化法（FISMA：Federal Information Security Modernization Act）を含む適用可能な法的権限、行政管理予算局（OMB：Office of Management and Budget）ポリシー及び米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が公布した連邦情報処理規格（FIPS：Federal Information Processing Standards）の出版物を含む規制要件及び外部のガイダンス、並びに内部のC-SCRMポリシー及び戦略文書と整合していることを確実にしなければならない。

以下の参考文献が適用される。

- 国家安全保障システム委員会（Committee on National Security Systems）。CNSSD 505号。「（*U*）サプライチェーンのリスクマネジメント（*SCRM*）」（*(U) Supply Chain Risk Management (SCRM)*）」
- NIST SP 800-53, Rev. 5、「組織と情報システムのためのセキュリティ及びプライバシー管理策（*Security and Privacy Controls for Information Systems and Organizations*）」
- NIST SP 800-161, Rev. 1、「システム及び組織におけるサプライチェーンのサイバーセキュリティリスクマネジメントのプラクティス（*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*）」
- OMB通達（Circular）A-130号、「戦略的リソースとしての情報の管理（*Managing Information as a Strategic Resource*）」
- 連邦政府調達サプライチェーンセキュリティ法（Federal Acquisition Supply Chain Security Act）（2018）
- 大統領令14028号（2021年5月12日）、「国家のサイバーセキュリティの向上」

3.1.11.改訂及び保守

変更日、変更の説明、及び、変更を行った個人名を識別する表を含める。少なくとも、ライフサイクルのマイルストーン、ゲートレビュー、及び重要な契約活動でレベル*3*の*C-SCRM*計画をレビュー及び更新し、必要に応じて、上位のティアの計画への準拠を検証する。事業体又は環境に対する脅威及び変更など、外生的要因の変化するインパクトに計画が適応していることを確実にする。

サンプルテキスト

表 D-11：改訂及び保守

バージョン番号	日付	変更／改訂の説明	影響を受ける節／ページ	変更者の氏名／肩書／事業体

3.1.12.C-SCRM 計画の承認

署名（電子又は手書き）、及びシステムセキュリティ計画がレビューされ、承認された日付を含める。

サンプルテキスト

認可権限のある担当者：

X _____
氏名
日付

3.1.13. 略語リスト

***C-SCRM*計画で利用されている略語を含め、詳述する。**

サンプルテキスト

表 D-12：略語リスト

略語	詳細
AO	認可権限のある担当者（Authorizing Official）
C-SCRM	サプライチェーンのサイバーセキュリティリスクマネジメント（Cybersecurity Supply Chain Risk Management）
SDLC	システム開発ライフサイクル（System Development Life Cycle）

3.1.14.添付文書

***C-SCRM* 計画をサポートするために含めることができる、関連する成果物を添付する。**

サンプルテキスト

- 契約上の合意
- 請負事業者又はサプライヤのC-SCRM計画

3.1.15.C-SCRM 計画及びライフサイクル

C-SCRM計画は、研究開発、設計、製造、取得、納入、統合、運用、及び廃棄／廃止を含む、システム及びプログラムの完全なSDLCをカバーすることが望ましい。C-SCRM計画の活動は、事業体のシステム及びソフトウェアライフサイクルプロセスに統合されることが望ましい。C-SCRM計画内の類似する管理策は、2つ以上のライフサイクルプロセスに適用することができる。以下の図は、C-SCRM計画の活動を様々なライフサイクルの例にどのように統合できるかを示している。

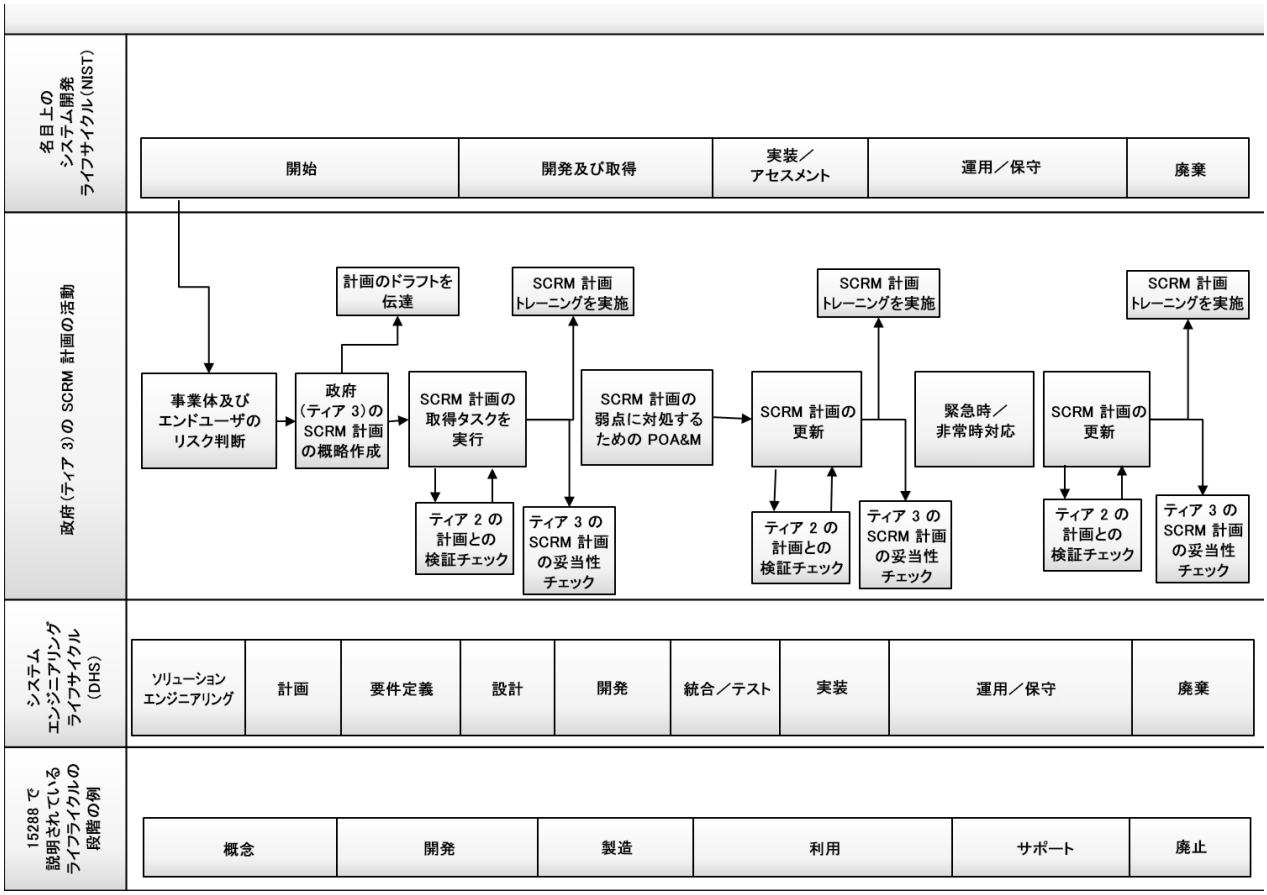

図 D-1：C-SCRM計画ライフサイクルの例

4. サプライチェーンのサイバーセキュリティリスクアセスメントのテンプレート

サプライチェーンのサイバーセキュリティリスクアセスメント（C-SCRA：Cybersecurity Supply Chain Risk Assessment）[43]は、調達者にサイバーセキュリティリスクをもたらす可能性があるすべてのサードパーティ製品、サービス、又はサプライヤ[44]のレビューの指針となる。C-SCRAのテンプレートの目的は、取得者が選択した管理策に応じて使用するか使用しないかを選択できる質問のツールボックスを提供することである。通常、C-SCRM PMOによって運用レベル（レベル3）で実行され、サプライチェーン全体の既知のサイバーセキュリティリスク、それらの出来事の発生可能性、及び事業体とその情報及びシステムへの潜在的なインパクトを含む、包括的なアセスメントを実行するために利用可能な公開情報及び機密の情報を考慮する。事業体にC-SCRAC-SCRAが殺到し、サプライヤにC-SCRAC-SCRAの要求が殺到する可能性があるため、事業体は、C-SCRAC-SCRAの厳格さに影響を与える要因として、C-SCRAC-SCRAの相対的な優先順位を評価することが望ましい。

取り上げられている他のテンプレートと同様に、以下のC-SCRAC-SCRAは一例としてのみ提供されている。事業体は、レベル1及びレベル2のリスク態勢に合わせて、以下の内容をテーラリングしなければならない。C-SCRAC-SCRAの実行は、おそらくC-SCRM運営の中で最も目に見えて時間のかかるコンポーネントであるため、専用のサポートリソース、テンプレート化されたワークフロー、及び可能な限り自動化を使用して、大規模に効率的に実行できるように設計されなければならない。連邦政府機関は、サプライチェーンのリスクアセスメントに関する追加のガイダンスについて、附属書Eを参照することが望ましい。

4.1. C-SCRMのテンプレート

4.1.1. 典拠及び法令順守

***C-SCRAC-SCRA*の実行を管理する法律、大統領令、指令、規制、ポリシー、標準、及びガイドラインをリスト化する。**

サンプルテキスト

- 法律
  - o リスク曝露（エクスポージャー）技術の活用法によるサイバーケイパビリティ（能力）の強化及び向上（2018年）
- ポリシー
  - o [事業体の名称] C-SCRAの標準的な運用手順
  - o [事業体の名称] C-SCRAのリスクアセスメント要因
  - o [事業体の名称] C-SCRAの重要度アセスメント基準
- ガイドライン
  - o NIST 800-53, Rev. 5： PM-30、RA-3、SA-15、SR-5
  - o NIST 800-37, Rev. 2
  - o NIST 800-161, Rev. 1： 附属書C
  - o ISO 28001:2007

[43] 本出版物の目的上、用語の統一を図るために、「サプライチェーンのサイバーセキュリティリスクアセスメント」という表現は「サプライチェーンのリスクアセスメント」と同義であるとみなすことが望ましい。

[44] サプライヤは、リスク曝露（エクスポージャー）技術の活用法によるサイバーケイパビリティ（能力）の強化及び向上（2018年）に定義されているように、供給源を表す場合もある。

4.1.2. 説明

_C-SCRA_のテンプレートの目的及び範囲を説明し、_C-SCRM_に対する事業体のコミットメント及びそのコミットメントの延長として_C-SCRA_の実行の義務付けについて言及する。テンプレートと事業体のリスクマネジメントの原則、フレームワーク、及びプラクティスとの関係を概説する。これには、事業体の_C-SCRA_プロセス、標準的な運用手順、及び／又はこのテンプレートの使用を管理する重要度の指定の概要を提供することが含まれる可能性がある。

サプライチェーンのサイバーセキュリティ上の不利な事象から予想される損失を低減するという利点、及びこれらのアセスメントを大規模に効率的に実行する_C-SCRM PMO_の役割を強調することで、_C-SCRA_実行のビジネスケースを強化する。

_C-SCRA_の範囲内にある事業体の境界、システム、及びサービスの概要を提供する。

読者が_C-SCRA_プロセスにさらに関与するためにアクセスする可能性がある連絡先情報、及びその他のリソースをリスト化する。

サンプルテキスト

このC-SCRAは、サイバーセキュリティリスクの結果として、危害又は侵害の可能性を持つサードパーティを介して [事業体] にもたらされるリスクを、公平に、かつ一貫して評価することを意図している。サプライチェーンにおけるサイバーセキュリティリスクには、サプライチェーンを通過する製品及びサービスに関連する曝露（エクスポージャー）、脅威、及び脆弱性、並びにサプライチェーン及びそのサプライヤに対する曝露（エクスポージャー）、脅威、及び脆弱性が含まれる。

C-SCRAテンプレートは、C-SCRAがサプライチェーンにおけるサイバーセキュリティリスクをレビューし、事業体の要求に従って適切、効率的、かつ効果的に実行されることを確実にするための戦術的ガイドラインを提供する。

サードパーティ製品、サービス、又はサプライヤを事業体の境界内に導入しようとする依頼者は、以下のテンプレートに習熟することが望ましい。これにより、依頼者は、C-SCRAのタイムリーな実行を確実にするための必須情報をC-SCRM PMOに確実に提供でき、それ以外の場合、C-SCRAのステップを順守するよう調整される。

以下のテンプレートで概説されているように、C-SCRAプロセスには5つの主要なステップが含まれる[45]。

1. 情報収集及びスコーピング分析
2. 脅威分析
3. 脆弱性分析
4. インパクト分析
5. リスク対応分析

[45] これらのステップを支える方法論の原則及びガイダンスについては、附属書Dの「アセスメント」節を参照のこと。

C-SCRAプロセスについての詳細、及び／又はC-SCRM PMOへのアセスメント依頼の提出については、[事業体のイントラネットページ] にアクセスするか、[C-SCRM PMO のメールアドレス] に連絡すること。

4.1.3. 情報収集及びスコーピング分析

依頼された*C-SCRA*の目標及び目的を定義し、システム、運用、サポートするアーキテクチャ、及び境界を適切に定義するために必要な重要情報を概説する。この情報の収集及び分析を容易にするために、依頼者に重要な質問を提供する。その後、*C-SCRM PMO*は、以降の分析及びデータ依頼のベースラインとしてこの情報を使用する。

サンプルテキスト

表 D-13：情報収集及びスコーピング分析

サプライチェーンのリスクマネジメントアセスメントのスコーピング質問表		
第1節：依頼の概要	回答記入欄	回答者
依頼者の氏名		取得者
C-SCRAの目標及び目的		取得者
システムの説明		取得者
アーキテクチャの概要		取得者
境界の定義		取得者
アセスメントの実行日		取得者
アセッサー（査定者）の氏名		取得者
第2節：製品／サービスの内部リスクの概要		
あなたの事業体は、サプライヤのこの製品／サービスの売上のうち、何パーセントを占めているか。		取得者又は サプライヤ
あなたの事業体で、その製品又はサービスはどの程度広く使用されているか。又は、どの程度広く使用される予定か。		取得者
その製品／サービスは、主要な運用地域（例えば、米国内）を踏まえて、あなたの事業体にとって地政学的リスクがある地域と見なされる地理的な場所で製造されているか。		取得者又は サプライヤ
その製品は、外国の敵対国、又は、特別な懸念がある国として識別されている国で製造又は開発されているか。		取得者
この製品又はサービスを代替サプライヤに切り替えることは、あなたの事業体にとって大きなコスト又は労力となるか。		取得者

あなたの事業体は、この製品／サービスの別のサプライヤと既存の関係があるか。		取得者
あなたの事業体は、人的及び自然的な大規模なサプライチェーンの混乱に関係なく、品質の高い製品／サービスを取得できるであろうという自信をどの程度持っているか。		取得者
あなたの事業体は、この製品／サービスの予備を保持しているか。		取得者
その製品／サービスは、目的に適合しているか（すなわち、目的又はサービスレベルを達成することができるか）。		取得者
その製品／サービスは、必須のセキュリティ機能を実行するか。実行する場合は、説明すること。		取得者
その製品／サービスは、IT ネットワーク、OT システム、又は機密情報を扱うプラットフォームへのルートアクセス権を持っているか。		取得者
その製品／サービスの侵害は、システム障害又は深刻な劣化につながる可能性がある。		取得者
システム障害又は深刻な劣化につながる侵害が発生した場合、既知の独立した信頼性の高い軽減策はあるか。		取得者
その製品／サービスは、あなたの事業体によって顧客に提供されるプラットフォームに接続しているか。又は接続する予定か。		取得者
その製品／サービスは、高価値のデータ（例えば、個人情報（PII：Personal Identifiable Information）、保護対象保健情報（PHI：Protected Health Information）、ペイメントカード業界（PCI：Payment Card Industry））を伝送、生成、維持、処理しているか。又は処理する予定か。		取得者
その製品／サービスは、高価値データ（例えば、PII、PHI、PCI）を伝送、生成、維持、処理するシステムへのアクセス権を持っているか。又はアクセス権を持つ予定か。		取得者
サプライヤは、その製品／サービスの提供の結果として、会社の施設に物理的にアクセスする必要があるか。又は、必要となる予定か。		取得者
上記の回答の全体的な考慮に基づいて、この製品／サービスはあなたの事業体にとってどの程度重要か（すなわち、重大、高、中、低）。		取得者

第3節：サプライヤの概要		
サプライヤの重要なサプライヤを識別しているか。		サプライヤ
外国か国内かを問わず、サプライヤの所有権を検証したか。		サプライヤ
サプライヤが販売代理店を使用している場合、潜在的なリスクについて調査したか。		サプライヤ
サプライヤは米国にあるか。		サプライヤ
サプライヤは、外国政府と個人的な結びつき及び／又は職業上の結びつき（サプライヤの役員、管理者、又はこれに類する役職者、従業員、コンサルタント、又は請負事業者を含む）を持っているか。		サプライヤ
サプライヤ、又は、サプライチェーンに関与するビジネスエンティティに対する外国による所有権、管理、又は影響（FOCI）は存在するか。存在する場合、そのFOCIは、米国の敵対国、又は懸念のある国によるものか。		サプライヤ
サプライヤが本社、研究開発施設、製造施設、テスト施設、包装施設、流通施設、又はサービス施設、あるいはその他の業務を有する外国の法律及び規制は、当該外国との技術又はデータの共有を要求しているか。		サプライヤ
サプライヤは、交換コンポーネントをどこから購入するかを宣言しているか。		サプライヤ
すべてのサプライヤ、二次請負業者、及び二次サプライヤの所有者及び所在地を識別し、妥当性を確認したか。		サプライヤ
サプライヤは、二次サプライヤの精査に情報を与えるために、脅威のシナリオの使用を採用しているか。		サプライヤ
サプライヤは、部品番号を製造業者まで追跡する文書を持っているか。		サプライヤ
サプライヤは、契約の履行に利用される、ハードウェア及びソフトウェアの調達先のリストを提供できるか。		サプライヤ
サプライヤは、偽造品の管理策を実施しているか。		サプライヤ
サプライヤは、他のサプライヤとの相互作用を通じて曝露される可能性のある重要なプログラムの情報を保護しているか。		サプライヤ

サプライヤは、レビュー及び検査を実施し、偽造された機器、改ざんされたハードウェア又はソフトウェア（HW/SW）、脆弱性のある HW/SW、及び／又は運用セキュリティの漏えいを検知又は回避するための保全措置を持っているか。		サプライヤ
サプライヤは、ソフトウェアを購入する際、業界標準のベースライン（例えば、CIS、NES）を使用しているか。		サプライヤ
サプライヤは、規制及び法的な義務を順守しているか。		サプライヤ
サプライヤは、展開後のセキュアな保守及びアップグレードのための手順を持っているか。		サプライヤ
第4節：ポリシー及び手順		
サプライヤは、補助的な調達ニーズを含め、サプライチェーンリスクの最小化に役立つ明確なポリシー及び手順を持っているか。		サプライヤ
サプライヤは、システムの重要度及びケイパビリティ（能力）を定義して管理しているか。		サプライヤ
調達に関係するすべての人（例えば、サプライヤ、C-SCRM PMO）が、対象のサプライチェーンに対する潜在的な脅威及びリスクを理解しているか。		サプライヤ
関わっているすべての人員の国籍はどこか。必要な場合は、関わっているすべての人員が米国民か。		サプライヤ
サプライヤは、「インサイダー脅威」の管理策を実施しているか。		サプライヤ
サプライヤは、対象の製品、システム、又はサービスと相互作用するすべての人員を検証及び監視し、脅威となるかどうかを把握しているか。		サプライヤ
サプライヤは、製品、システム、又はサービスのライフサイクル全体でリスク軽減活動を使用、記録、及び追跡しているか。		サプライヤ
サプライヤのすべての人員が、秘密保持契約に署名しているか。		サプライヤ
サプライヤは、自らの人員又はサプライヤに、環境へのリモートアクセスを許可しているか。		サプライヤ
第5節：物流（該当する場合）		
サプライヤは、文書化された追跡及びバージョン管理を実施しているか。		サプライヤ

サプライヤは、自らのサプライチェーンを中断する可能性のある（環境による、又は人為的な）事象を分析しているか。		サプライヤ
サプライヤの完成部品は、放置されたり改ざんのリスクにさらされたりすることが決してないように管理されているか。		サプライヤ
サプライヤの完成部品は、安全な場所に保管されているか。		サプライヤ
サプライヤは、自らのサプライヤからインベントリの増減を要求される際に、完全性を確実にするプロセスを持っているか。		サプライヤ
サプライヤのインベントリは、曝露（エクスポージャー）又は改ざんがないか定期的に検査されているか。		サプライヤ
サプライヤは、自らのサプライヤから調達した未使用部品及びスクラップ部品のためのセキュアな材料破壊手順を持っているか。		サプライヤ
製品及びシステムの展開のための、文書化された生産物流管理はあるか。		サプライヤ
第6節：ソフトウェア設計及び開発（該当する場合）		
サプライヤは、製品／システムの設計に取り組む予定であるすべてのサプライヤについて熟知しているか。		サプライヤ及び製造業者
サプライヤは、SDLCをセキュアなソフトウェア開発標準（例えば、Microsoftのセキュリティ開発ライフサイクル）に合わせているか。		サプライヤ及び製造業者
サプライヤは、すべての開発を米国内で実行しているか。		サプライヤ及び製造業者
開発環境へのアクセス権を持っているのは、米国民のみか。		サプライヤ及び製造業者
サプライヤは、開発者にサイバーセキュリティトレーニングを提供しているか。		サプライヤ及び製造業者
サプライヤは、信頼できるソフトウェア開発ツールを使用しているか。		サプライヤ及び製造業者
サプライヤは、開発環境を保護するために、信頼できる情報アシュアランス管理策（例えば、セキュアなネットワーク構成、厳格なアクセス制御、動的／静的な脆弱性管理ツール、侵入テスト）を使用しているか。		サプライヤ及び製造業者

サプライヤは、オープンソースソフトウェアを使用する前に妥当性確認を行っているか。		サプライヤ及び製造業者
サプライヤのソフトウェアコンパイラは継続的に監視されているか。		サプライヤ及び製造業者
サプライヤは、ソフトウェアテスト及び構成の標準を成文化しているか。		サプライヤ及び製造業者
第7節：製品又はサービス固有のセキュリティ（該当する場合、製品／サービスごとに 一つの質問表）		
製品又はサービスの名称		製造業者
製品の種類（すなわち、ハードウェア、ソフトウェア、サービス）		製造業者
製品又はサービスの説明		製造業者
部品番号（該当する場合）		製造業者
製造業者は、製品提供のための開発又は製造プロセス全体にわたって、セキュアなエンジニアリングの実装及び監督に責任を持つ、正式な事業体の役割及びガバナンスを実装しているか。		製造業者
製造業者は、ISO 27036 又は SAE AS6171などの標準に適合する、製品の完全性のためのプロセスを持っているか。		製造業者
製品は、連邦情報処理規格（FIPS）140-2 に準拠しているか。準拠している場合は、FIPS レベルを記載すること。		製造業者
製造業者は、提供するハードウェア、ソフトウェア、又はソリューションに対するセキュリティ管理要件を文書化し、伝達しているか。		製造業者
製造業者は、製品又はサービスの提供に関連して、過去1年以内に、政府事業体又は規制機関から罰金又は制裁を受けたことがあるか。ある場合は、説明すること。		製造業者
製造業者は、製品又はサービスの提供に関連して、過去1年間に訴訟を経験しているか。ある場合は、説明すること。		製造業者

製造業者は、ロジックを持つ（例えば、読み取り可能、書き込み可能、プログラム可能）ハードウェア、ファームウェア、及びソフトウェアのすべてを含む、製品、サービス、又はコンポーネントの部品表（BOM：Bill of Materials）を提供しているか。		製造業者
製品又は提供されるサービスに含まれるハードウェアコンポーネントについて、サプライヤは、相手先ブランド製造業者、又は、認可を受けた再販業者からのみ購入しているか。		サプライヤ
製造業者は、サプライヤ又はサードパーティコンポーネントがいかなる禁止リストに載っていないことを確実にするポリシー又はプロセスを持っているか。		製造業者
製造業者は、提供する製品又はソリューション内の悪意のある、及び／又は偽造されたIPコンポーネントをどのように防止しているか。		製造業者
製造業者は、提供する製品又はサービスのためのIPの完全性を管理しているか。		製造業者
製造業者は、報告された製品又はサービスの脆弱性をどのようにアセスメントし、優先順位を付け、是正しているか。		製造業者
製造業者は、攻撃者の機会を減らすために、製品又はサービスの脆弱性を適切な期間に是正することを、どのようにして確実にしているか。		製造業者
製造業者は、製品セキュリティインシデント報告及び対応プログラム（PSRT）を維持及び管理しているか。		製造業者
製品又はサービスがインパクトを受けた場合に、顧客及び外部のエンティティ（政府機関など）にインシデントが通知されることを確実にするための、製造業者のプロセスはどのようなものか。		製造業者

4.1.4. 脅威分析

脅威分析を定義するとともに、製品、サービス、又はサプライヤの脅威をアセスメントするために利用される基準を定義する。アセスメント結果の透明性を促進するために、分類の定義を含む解説を含める。

サンプルテキスト

C-SCRAの脅威分析では、以下に説明するように、製品、サービス、又はサプライヤの完全性、統

合的信頼性、真正性に対する脅威レベルを評価し、その特徴付ける。この分析は、サプライチェーンに導入される製品、サービス、又はサプライヤを侵害又は悪用する脅威行為者のケイパビリティ（能力）及び意図に基づく。分析の完了後、以下の脅威レベルのいずれかが割り当てられる。

- **重大：**情報は、敵対的又は非敵対的な脅威が差し迫っていることを示している（例えば、敵対者が製品、サービス、又はサプライヤの破壊、悪用、又は妨害に積極的に関わっている）。
- **高：**情報は、敵対的又は非敵対的な脅威が差し迫っていることを示している（例えば、資産の立地特性と相まった地理的エリアにおける深刻な干ばつにより、森林火災の可能性が高まっている）。
- **中：**情報は、敵対的又は非敵対的な脅威が事業体にインパクトを与える、又は事業体を標的とする可能性が平均的であることを示している（例えば、特定の敵対的な脅威は存在するが、製品、サービス、又はサプライヤの破壊、悪用、又は妨害に関与するケイパビリティ（能力）又は意図のいずれかが欠如している）。
- **低：**情報は、敵対的又は非敵対的な脅威が存在しない、又は存在する可能性が低い、あるいは、事業体にインパクトを与える、又は事業体を標的とする可能性が平均以下であることを示している（例えば、敵対的な脅威は、製品、サービス、又はサプライヤの破壊、悪用、又は妨害に関与するケイパビリティ（能力）と意図の両方が欠如している）。

上記の脅威分析の指定を適切に割り当てるために、C-SCRM PMO及び依頼者は、製品、サービス、又はサプライヤの業務詳細、所有構造、重要な管理人員、財務情報、リスクの高い事業、政府の制限、及び潜在的な脅威に関する情報の収集を調整するために、情報収集及びスコーピング質問表を活用することが望ましい。は、最初のデータ収集中に危険信号が観察された場合は、前述のトピックについて追加調査を実行することが望ましい。

4.1.5. 脆弱性分析

脆弱性分析と、アセスメント対象の製品、サービス、又はサプライヤの脆弱性をアセスメントするために利用される基準を定義する。アセスメント結果の透明性を促進するために、分類の定義を含む解説を含める。

サンプルテキスト

C-SCRAの脆弱性分析では、製品、サービス、又はサプライヤのライフサイクル及び／又はエンゲージメント全体を通して、脆弱性を評価し、特徴付ける。この分析には、中程度のケイパビリティ（能力）を持つ脅威行為者による悪用の容易さのアセスメントが含まれる。この分析は、サプライチェーンに導入されている製品、サービス、又はサプライヤを侵害又は悪用する脅威行為者のケイパビリティ（能力）及び意図に基づく。分析の完了後、以下の脅威レベルのいずれかが割り当てられる。

- **重大：**製品、サービス、又はサプライヤには、完全に曝露され、容易に悪用可能な脆弱性又は弱点が含まれている。
- **高：**製品、サービス、又はサプライヤには、大いに曝露され、合理的に悪用可能な脆弱性又は弱点が含まれている。
- **中：**製品、サービス、又はサプライヤには、中程度に曝露され、悪用が困難な脆弱性又は弱点が含まれている。
- **低：**製品、サービス、又はサプライヤには、限定的に曝露され、悪用される可能性が低い脆弱性及び弱点が含まれている。

上記の脆弱性分析の指定を適切に割り当てるために、C-SCRM PMO及び依頼者は、製品、サービス、又はサプライヤの運用の詳細、悪用可能性、サービスの詳細、既知の脆弱性の属性、及び軽減技法に関する情報の収集を調整することが望ましい。

4.1.6. インパクト分析

インパクト分析と、アセスメント対象の製品、サービス、又はサプライヤの重要度をアセスメントするために利用される基準を定義する。アセスメント結果の透明性を促進するために、分類の定義を含む解説を含める。

サンプルテキスト

C-SCRAのインパクト分析では、製品、サービス、又はサプライヤのライフサイクル及び／又はエンゲージメント全体を通して、インパクトを評価し、特徴付ける。この分析には、事業体の業務又はミッションに対する製品、材料、又はサービスの発生し得る損失、損傷、又は侵害に起因する潜在的な損害のアセスメントに基づいた、重要な機能及びコンポーネントを識別するための徹底した機能レビューが含まれる。分析の完了後、以下のインパクトレベルのいずれかが割り当てられる。

- **重大：**製品、サービス、又はサプライヤが設計どおりに機能しない場合、事業体全体の障害、又は例外的な時間及びリソースを使用しないと復旧できないような、重大及び／又は受容不可能なレベルの業務の劣化が生じる。
- **高：**製品、サービス、又はサプライヤが設計どおりに機能しない場合、深刻な事業体の障害、又は多大な時間及びリソースを使用しないと復旧できないような、重大及び／又は受容不可能なレベルの業務の劣化が生じる。
- **中：**製品、サービス、又はサプライヤが設計どおりに機能しない場合、重大な事業体の障害が生じるが、長期的な影響はなく、容易かつ迅速に管理できる。
- **低：**製品、サービス、又はサプライヤが設計どおりに機能しない場合、事業体への悪影響はほとんど生じず、それらの影響は長期的な結果を伴わず、容易かつ迅速に管理できる。

上記のインパクト分析の指定を適切に割り当てるために、C-SCRM PMO及び依頼者は、事業体の重要な機能及びコンポーネントに関する情報の収集、製品又はサービスの意図されたユーザ環境の識別、及びサプライヤ情報を調整することが望ましい。

4.1.7. リスク対応分析

リスク分析と、アセスメント対象の製品又はサービスのスコアをアセスメントするために利用される基準を定義する。アセスメント結果の透明性を促進するために、分類の定義を含む解説を含める。

サンプルテキスト

C-SCRAのリスク曝露（エクスポージャー）は、起こりやすさ及びインパクト分析に基づく複合的な判断を反映している。起こりやすさ分析は、以下の図で概説するように、前述の脅威及び脆弱性分析のスコアの組み合わせによってスコアリングされる。

起こりやすさのレベル	
脅威	**脆弱性**

		低	中	高	重大
	重大	中程度	高い	非常に高い	非常に高い
	高	中程度	高い	高い	非常に高い
	中	低い	中程度	高い	高い
	低	低い	低い	中程度	中程度

図 D-2：起こりやすさの判断の例

次に、C-SCRAのリスク曝露（エクスポージャー）が、該当する起こりやすさスコア及びインパクトスコアに基づいてまとめて計算される。特定の製品又はサービスに複数の脆弱性が識別された場合は、それぞれの脆弱性に対して、その起こりやすさとインパクトに基づいてリスクレベルが割り当てられるものとする。

全体的なリスクレベル					
起こりやすさ（脅威及び脆弱性）	**インパクト**				
		低	中	高	重大
	非常に高い	中	高	重大	重大
	高い	中	中	高	重大
	中程度	低	中	高	高
	低い	低	低	中	高

図 D-3：リスクレベルの判断の例

前述のリスク分析及びスコアリングは、事業体が製品、サービス、又はサプライヤの調達を進めるかどうかを決定するための手段を提供する。調達を進める決定は、事業体のすべてのティアのリスク選好度及び許容度、並びに、製品、サービス、又はサプライヤの調達に伴うリスクを管理するために実施する可能性がる軽減戦略と比較検討されなければならない。

4.1.8. 役割及び責任

***C-SCRA*ポリシーに責任を持つ人員、及び重要な貢献者を示す。各個人又はグループの役割及び名前に加え、必要な場合は連絡先情報（例えば、事業体の所属、住所、メールアドレス、及び電話番号）を含める。**

サンプルテキスト

- C-SCRM PMOは、以下のことを行うものとする。
  - o C-SCRAのポリシー、手順、及びスコアリング方法論を維持する。
  - o C-SCRAの標準運用手順を実行する。
  - o 製品、サービス、又はサプライヤを調達しようとする依頼者と連携する。
  - o 事業体のリスク態勢への情報提供に役立てるために、C-SCRAの結果を責任者に報告する。
- 各依頼者は、以下のことを行うものとする。
  - o C-SCRA依頼フォームを記入し、必要な情報をすべて提供する。
  - o C-SCRAを完了する C-SCRM PMOリソースからのすべての情報フォローアップ依頼に対処する。
  - o C-SCRA依頼の承認後、C-SCRM PMOによって義務付けられた規定又は軽減策に従う。

4.1.9. 定義

ポリシー内で説明されている重要な定義をリスト化し、必要があれば、事業体固有のコンテキスト及び例を提供する。

サンプルテキスト

- 調達：システム、製品、又はサービスを取得するプロセス。

4.1.10. 改訂及び保守

***C-SCRA*テンプレートの更新に必要な頻度を定義する。バージョン管理を実施するために、改訂表を維持する。*C-SCRA*テンプレートは、更新され、すべての適切な個人（例えば、スタッフ、請負事業者、及びサプライヤ）に伝達されなければならない、生きた文書である。**

サンプルテキスト

事業体のC-SCRAテンプレートは、法律、ポリシー、標準、ガイドライン、及び管理策への変更は動的で進化しているため、最低でも1年ごとにレビューしなければならない。臨時改訂の契機となる可能性がある追加の基準には、以下のものが含まれる。

- C-SCRAテンプレートにインパクトを与えるポリシーの変更
- 重大なC-SCRMの事象
- 新技術の導入

- 新たな脆弱性の発見
- 運用又は環境の変化
- C-SCRAテンプレートの不備
- 範囲の変更
- その他の事業体固有の基準

サンプルテキスト

表 D-14：バージョン管理表

バージョン番号	日付	変更／改訂の説明	影響を受ける節／ページ	変更者の氏名／肩書／事業体

附属書 E：FASCSA [46]

はじめに

目的、読者、及び背景

本附属書は、NIST SP 800-161 Rev. 1の内容を拡張し、サプライチェーンのリスクアセスメント要因、アセスメント文書、リスク深刻度レベル、及びリスク対応に関連する連邦行政機関に固有の追加ガイダンスを提供する。

SP 800-161 Rev. 1の本文の最初の節に記載されているように、*SECURE* 技術関連法（*SECURE Technology Act*）（公法 115-390（P.L. 115-390））の第II編である、*2018*年の連邦調達サプライチェーンセキュリティ法（*Federal Acquisition Supply Chain Security Act of 2018*）（FASCSA）は、行政機関の連携、サプライチェーンリスク情報（SCRI）の共有、及びサプライチェーンリスクに対処するための活動を改善するために制定された。この法律により、連邦政府事業体レベルの省庁間の執行機関である連邦政府調達安全保障会議（FASC：Federal Acquisition Security Council）[47]が設立された。この評議会は、連邦政府のサプライチェーンのリスク曝露（エクスポージャー）とリスクインパクトを軽減することを目的とした様々な機能を実行する権限を与えられている。

FASCSAは、FASC及び行政機関に、供給源及び対象品目の排除及び／又は撤去を含む、サプライチェーンリスクの軽減に関連する権限を付与する[48]。同法はまた、政府機関がサプライチェーンのリスクアセスメント（SCRA）を実施し、優先順位を付けることを義務付けている。本附属書のガイダンスは、以下で説明するように、このFASCSA要件に固有のものであり、政府機関レベルのC-SCRMリスクアセスメント及び対応機能と、FASCなどの権限を与えられた機関によって政府全体レベルで行われるSCRM機能との間のベースラインレベルの一貫性と調整に関する必要性に対応している。

範囲

範囲内

本附属書は、主に、対象品目の取得と使用によって生じるサプライチェーンリスクをアセスメントし、そのリスクに適切に対応することを行政機関に要求している、FASCSAの第1326条（a）の（1）に関する追加ガイダンスを各政府機関に提供することに焦点を当てている[49]。この法律は、NISTの標準、ガイドライン、及びプラクティスに従って、この活動及びそこに記載されているその他のSCRM活動を実施するよう政府機関に指示している。

---

[46] 各省庁及び関係機関は、大統領令14028号の「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装するために、附属書Fを参照することが望ましい。

[47] 読者は、FASCの権限、メンバーシップ、機能、及びプロセスに関する追加情報について、連邦政府調達安全保障会議の最終規則41 CFR パート 201 及び 201-1 を参照することが望ましい。以下を参照のこと：
https://www.govinfo.gov/content/pkg/FR-2021-08-26/pdf/2021-17532.pdf

[48] FASCSAの定義によると、対象品目は以下を意味する： あらゆる種類のクラウドコンピューティングサービス、通信機器又は通信サービス、管理対象非機密情報プログラムの要件の対象である、連邦政府又は非連邦政府情報システム上の情報の処理、すべてのIoT/OT（例えば、組み込み又は付随的な情報技術を含むハードウェア、システム、デバイス、ソフトウェア、又はサービス）を含む情報技術。

[49] 41 USC 1326（a）の（1）を参照

範囲外

FASCSAの第4713条[50]は、行政機関が対象となる調達活動を実施するための権限に関するものである。これらの活動に関する具体的なガイダンスについては、本附属書の範囲外である。FASCSAは、連邦調達規則（FAR）評議会に対し、本条項の実施に必要となる可能性がある規則を規定するよう要求している。NISTは、調和のとれたガイダンスを確実にするために、FASCや連邦調達機関コミュニティ内の省庁間の同僚と緊密に協力しており、今後もそれを継続していく予定である。

本附属書では、アセスメントの実施方法に関するガイダンスは提供していない。アセスメントは、役割ベースのトレーニング、教育、及び実務経験を通じて対処するのが最善である。NIST SP 800-30 Rev. 1の「リスクアセスメントの実施の手引き（*Guide for Conducting Risk Assessments*）」も推奨される参照文献である。政府機関は、SCRAの実行について現在及び将来の責任を負う担当者が、サプライチェーンにおけるサイバーセキュリティリスクの兆候及びそれらのリスクのアセスメントを識別し、見分けるのに十分なスキル、知識、及び深く幅広い経験を持つことを確実にするための措置を講じることが望ましい。政府機関には、分析スキルとSCRM知識の能力を高め、維持するためのトレーニングに投資することが強く推奨される。また、C-SCRM PMOスタッフやSCRAの実行に専念する責任を持つ人員には、防諜及びセキュリティのトレーニングも強く推奨される。このケイパビリティ（能力）を構築することは、従業員が敵対者に関連するサプライチェーンリスクを十分に理解及び認識することを確実にするのに役立つと同時に、リスク対応の決定と活動に対して助言とサポートを提供するリスクマネジメントの幹部を育成するのに役立つ。

NIST SP 800-161 Rev. 1「システム及び組織におけるサプライチェーンのサイバーセキュリティリスクマネジメントのプラクティス」との関係

サプライチェーンにおけるサイバーセキュリティリスクをアセスメント、対応、及びその他の方法で管理するためのプラクティスとプロセスは、NIST SP 800-161 Rev. 1の本文と附属書全体を通じて詳細に説明されている。本附属書では、連邦政府機関に合わせてテーラリング、適用される補完的な拡張ガイダンスを提供する。このガイダンスは、内部の政府機関の上級職員及び外部のFASCなどの機関の両方に対して、サプライチェーンのリスクアセスメント情報の範囲と種類、及びリスク対応の決定と活動に対するサポートと助言に使用される文書について説明している。

この拡張されたガイダンスは、アセスメント及び文書化に使用されるプロセス及びサプライチェーンリスク情報（SCRI）のベースラインの一貫性及び充足性を確実にし、特定の政府機関であれ政府全体のレベルであれ、該当する意思決定者への情報共有と勧告を容易にすることも意図している。連邦政府事業体レベルの分析と意思決定に必要なサポートという制約の中で、政府機関は、NIST SP 800-161 Rev.1の本文及び他の附属書に概説されている幅広いガイダンスと各機関のポリシー、ミッションと優先順位のニーズ、及び既存のプラクティス（これらが十分である範囲内で）に沿った方法で、自らの供給リスクをアセスメント及び管理する柔軟性を持ち続けている。

[50] 41 USC 4713

FASCSA のサプライチェーンリスクの定義と NIST SP 800-161 Rev. 1 のサプライチェーンのサイバーセキュリティリスクの定義の比較

政府機関は、FASCSA でのサプライチェーンリスクの定義が、敵対的な脅威行為者が悪意のある行為を行うか、さもなければ悪意のある損害を引き起こす意図とケイパビリティ（能力）を持っているというアセスメントから生じるリスクに焦点を絞ったものであることに留意することが望ましい。対照的に、NIST のサプライチェーンのサイバーセキュリティリスクの定義と範囲は FASCSA の定義と一致しているが、敵対者に関連するリスク及び敵対者に関連しないリスクの両方が含まれるため、範囲はより広くなっている。政府機関が NIST の標準及びガイダンスに依拠するという FASCSA の指示に沿って、政府機関は自らのアセスメントとリスク対応の活動が、サプライチェーン全体に該当するすべてのサイバーセキュリティリスクに対処することを確実にする必要がある。

サプライチェーンのリスクアセスメント（SCRA）

一般情報

FASCSAは、政府機関に対し、対象品目の取得時だけでなく、その使用中又は実行中にも、サプライチェーンのリスクアセスメントを実施し、優先順位を付けることを要求している。ほとんどの場合、これはまた、対象品目に関連する供給源をアセスメントする必要を生じさせる。政府機関が実施するサプライチェーンのリスクアセスメントは、対象品目に関連する運用環境及びユースケースに大きく依存する。政府機関は、NISTのガイドラインをどのように業務に適用するかについて柔軟性があり、SCRAを実施するための画一的なアプローチは存在しないし、存在させるべきではない。しかし、国家安全保障又は複数の政府機関のミッションにインパクトを与える可能性のあるリスクを評価するために、政府全体レベルで実施する必要が生じる可能性のあるアセスメントを容易にするためには、政府機関のSCRA情報及び文書が、デューデリジェンス及び標準化の受容可能なベースラインレベルを反映していることを確実にする必要がある。

一般に、アセスメントに使用される情報は、最大で以下の3つのカテゴリのインプットで構成される。

1）リスク環境を理解し、ユースケースに関連するリスク許容度を通知及び確立するために使用される目的とコンテキスト情報（すなわち、ユースケース固有）
2）供給源から取得したデータ又は情報
3）公的に入手可能なデータ、政府情報源（機密の情報源が含まれる場合がある）、及び／又は商用の有料の情報源から得られる、あらゆる供給源の情報

SDLCや調達のライフサイクルにおいてサプライヤ及び／又は対象品目のアセスメントが実施される場合だけでなく、目的及びコンテキストも、アセスメントで使用される情報の種類、量、及びどのような情報源から情報を得るかに関する焦点及び範囲の点で変動を引き起こす。

FASCSAは、政府機関のリソースに制約があることを認識しているが、SCRAの実施に優先順位をつけることが必要である[51]。優先順位付けは、アセスメントすることが望ましい供給源又は対象品目のサブセットのみと理解されることを意図していない。むしろ、政府機関は、リスクインパクトの重要性と可能性に見合った、一連の階層化された優先順位を確立することが望ましい。この階層化は、SCRAのタイミング、順序、範囲、及び頻度を導くため、又は強制するために使用することができる。

[51] FASCSAの第1326条（a）の（2）を参照のこと。

外部主導の優先順位（例えば、政府全体の政策の方向性、規制要件）及び政府機関が定義した優先順位付け要因に加えて、NIST SP 800-161 Rev 1は、重要なサプライヤ（すなわち供給源）及び重要なシステムとサービスに関するアセスメントを優先するよう政府機関に指示している。これらの供給源及び対象品目の侵害は、重要ではないと判断されたものよりも大きな損害をもたらす可能性が高いからである。これらのアセスメントについて、政府機関は、以下の「ベースラインリスク要因（共通、最小）」の節に記載されているすべてのベースラインリスク要因に対処することが望ましい（敵対者に関連するリスクと敵対者に関連しないリスクの両方を適切に考慮することを確実にするために、ユースケースに応じて要因を補強及び比較検討する）。特定の重要でない供給源又は重要でない対象品目について、政府機関は、サプライチェーンリスクをアセスメントする際に、この附属書に記載されているベースラインリスク要因のすべて、一部、及びどの程度まで考慮すべきかについて、自らの内部ポリシー及びプラクティスと整合し、他の任務がない限りは、裁量権を有している。ただし、重大なサプライチェーンリスクが存在する可能性がある、又は実際に存在することを示す信頼できる所見が1つ以上ある場合（後述の「サプライチェーンリスク深刻度判断基準」を参照）には、すべてのベースラインリスク要因、又はベースラインリスク要因に関するより堅牢な調査と分析を含む、より包括的なアセスメントを完了する必要がある場合がある。（以下の「リスク対応」の節に記載されているリスク対応ガイダンスを参照のこと）。

SCRAの優先順位を決定し、インパクトを評価し、リスク対応の意思決定を行い、SCRAの所見に基づく措置を講じる責任及び説明責任は、本質的に政府の機能であり、外部委託することはできない。ただし、一部の政府機関では、調査の実施、調査結果の文書化、及び関連情報のレビューについて、資格のある第三者にサポートを求める場合がある。また、調査及びアセスメントの活動を支援するために、政府機関が市販のデータ又はツールへのアクセスを取得する場合もある。SCRIへのアクセス、取り扱い、及び保護に対処するために、適切な要件が提案書及び契約には、含まれることが望ましい。これを怠ると、それ自体がセキュリティ管理策のギャップを反映し、軽減されないサプライチェーンリスクを生み出す。さらに、このようなギャップは、政府機関のSCRAの取り組みの目的全体を損なわせる可能性があり、外国の敵対者による米国に対する悪意のある活動の成功を促進する可能性さえある。さらに、政府機関の人員は、利益相反及び情報への不適切又は不正なアクセスや情報の漏えいを防ぐための保護が実施されることを確実にするために、倫理担当官及び法律顧問の指導と指示に従うことが望ましい。これは、SCRIが機密情報、専有情報、又は（場合によっては）国家機密情報である可能性があるためである。後者のカテゴリの情報については、政府機関は、国家機密情報を管理する法律、ポリシー、手続きを順守し、適切な許可、認可されたアクセス権、及び知る必要を有する人員のみにアクセスを制限しなければならない。

すべての場合において、アセスメントの実施をサポートする人員は、慎重かつ客観的に行動する義務と責任を負い、このSCRIがその後のリスク対応の決定と措置の基礎となるため、供給源又は対象品目の調査と分析において合理的な注意を払う義務と責任を負う。

ベースラインリスク要因（共通、最小）

この節では、政府機関が定義するSCRA方法論に組み込む（又は含まれる要因にマッピングする）ことが望ましいベースラインの（共通、非排他的）サプライチェーンリスク要因及びガイダンスについて説明する。これらの要因は、少なくとも重要な供給源又は重要な対象品目に関連するSCRAのリスクを調査、識別、及びアセスメントするための指針として使用される。また、リスク要因の共通のベースラインは、リスク対応の意思決定及び行動が政府機関内の様々なレベルで発生しているか、連邦政府事業体レベルで発生しているかにかかわらず、それらに情報を提供する分析の一部としてデューデリジェンスが一貫して実施されることを確実にするのにも役立つ。政

府機関は、所与のアセスメントユースケースに関連し、かつ適切であると判断した場合には、ベースライン要因以外の追加要因をアセスメントすることが望ましい。

この一連のベースライン要因を確立する目的には、以下が含まれる。

- 供給源及び対象品目のレベル設定評価
- 必要なときに、FASCが最小限の必要な情報を利用できることを確実にすること
- 政府機関間の一貫性と比較可能性の促進
- 傾向分析、又は識別されたリスク指標と実現されたリスクとの因果関係又は相関関係など、より高度な分析の実施の支援
- 潜在的な軽減オプションを識別して理解し、優先順位付けやリスク対応のトレードオフ分析／意思決定に情報を提供するのに十分な情報基盤の確立及び維持

以下の表E-1には、ベースラインリスク要因及びそれに対応する定義又は説明のリストが含まれている。また、これらの要因は、FASC最終規則（Final Rule）に含まれる要因とも一致し、整合している[52]。右端の列には、リスクの指標として識別及び検出される可能性のある情報の種類のリストが含まれている。このリストは参考資料として使用されることを意図しており、可能性のあるリスクの指標となる可能性があるものをすべて含むものではない。コンテキストに基づくリスク要因に関する情報は、政府機関が知っていることが望ましく、多くの場合、既に文書化されている（例えば、システムセキュリティ計画、又は取得計画）。これらのユースケース固有及びコンテキストに基づく要因のアセスメントは、固有のリスクを理解するのに役立ち[53]、必要なサイバーセキュリティ及びSCRM管理策並びに調達要件の識別と選択の指針となり、所与のユースケースに関連する対象品目のリスク許容度のしきい値を決定するのに役立つ。

以下の一連の脆弱性及び脅威のリスク要因は、対象品目自体又は関連する供給源又はサプライチェーンから継承される可能性のあるリスクに焦点を当てている。政府機関は、敵対的な脅威行為者からの脅威の兆候があるかどうか、侵害又は損害の起こりやすさとその結果として生じるインパクト、及び供給源及び／又は対象品目に関連するアセスメントされたリスクが、受容可能なリスク許容度レベル内にあるか、又はこのレベルを超えているかについて、情報に基づいた判断を提供するために、これらのベースライン（及び追加の）要因に関連する所見をアセスメントする。

[52] CFR パート（Part） 201-1.300 供給源及び対象品目の評価（Evaluation of Sources and Covered Articles）
[53] この目的のために定義される固有リスクとは、既存の一連の管理策を前提とした現在のリスクレベルである。

表 E-1：ベースラインリスク要因

ベースラインリスク要因	定義又はガイダンス	リスクの非排他的な指標（該当する場合）
ユースケース／コンテキスト（固有リスク）		
目的	製品又はサービスの要件と、それがどのように使用されるか、又は使用されているかを理解する。	• ニーズを満たすために市場で利用可能なオプション • ニーズの緊急性 • ニーズの期間
重要度	製品、サービス、又は供給源が重要なシステム、システムコンポーネント、サービス、又はサプライヤと見なされるかどうかを識別する。追加のガイダンスについては、NIST SP 800-161 Rev.1の本文及び用語集を参照のこと。 EOの重要なソフトウェアに関する情報については、附属書Fも参照のこと。	• サプライヤ又は対象品目（又はその中のコンポーネント）が、ミッションクリティカルな機能、生命の安全、国土安全保障、重要インフラ、又は国家安全保障上の利益を実現する役割を果たしている、又はこれらに不可欠である（すなわち、侵害された場合、損害を与える可能性がある）か、そのような機能を果たしている、あるいはそのような機能に不可欠な別の対象品目と相互依存関係を持っている。
情報及びデータ	製品、サービス、及び／又は供給源によって使用される、又はアクセス可能な連邦政府のデータ／情報の種類、量、目的、及びフローを理解し、文書化する。	• CUI又は国家機密情報にアクセスするための要件又は能力 • 連邦政府の情報は、一次請負業者又はサプライヤ以外の外部の個人又はエンティティが管理、及び／又はアクセスできるようになる。 •製品又はサービスのデータのインプット又はアウトプットが侵害された場合、生命の安全に影響を及ぼす可能性がある
対象品目又は供給源への依存	政府機関が、対象品目及び／又は供給源に依存している度合いとその理由を理解し、明確に説明する。	• 政府機関による製品又はサービスの使用の普及率 • 単一の供給源 • 市場における製品又はサービスの入手可能性 • 製品、サービス、又は供給源（又は受容可能な代替品）の入手可能性

ベースライン リスク要因	定義又はガイダンス	リスクの非排他的な指標（該当する場合）
対象品目が使用される、設置される、又はサービスが実行されるユーザ／運用環境	システムに含まれる製品、又はシステムコンポーネントとして含まれる製品についてはは、システムセキュリティ計画及び／又はC-SCRMシステム計画にユーザ環境を記述することが望ましい。労働ベースのサービスの場合は、政府機関をリスクにさらす可能性のあるユーザ環境（すなわち、実行の場所）についての関連情報を理解し、文書化する。	• システム及び／又はC-SCRMセキュリティ計画は、リスクを識別して文書化し、それらのリスクを軽減するために実装された、又は実装する必要がある適用可能な、選択されたセキュリティ管理策について記述することが望ましい • リスクに関する懸念を生じさせる、関連する環境上の考慮事項は、調達計画、及び提案書及び契約で取り上げる適用可能な管理策で文書化することが望ましい
外部政府機関の相互依存関係	データ、システム、及びミッション機能に関連する相互依存関係を理解し、識別する。	• 対象品目は、政府全体の共有サービスをサポートする機能を果たしている • 対象品目は、他の政府機関のミッションクリティカルなシステムとデータを交換する • 請負業者が、政府全体のCUIデータを保存する分析ツールを保守している
脆弱性又は脅威（継承されたリスク）		
対象品目の機能、特徴、及びコンポーネント	情報は、製品又はサービスが目的に適合しているかどうか、及び適用されるC-SCRMの範囲（本文の第1.4節を参照）が満たされているというアシュアランスがどの程度あるか、及び／又は、内在する又は軽減されていない弱点や脆弱性が存在する程度についての判断を示す。	• 期待どおりの製品又はサービスを生産及び提供する供給源の能力 • 組み込みのセキュリティ機能及びケイパビリティ（能力）、又はそれらの欠如 • 誰がセキュリティ機能を管理しているのか、又は誰がセキュリティ機能の最終的な制御権を持っているのか • セキュア構成のオプションと制約条件 • セキュリティ機能の管理と制御（誰が、どのように） • ネットワーク／インターネット接続のケイパビリティ（能力）又は要件、及び接続方法 • ソフトウェア及び／又はハードウェアの部品表

ベースライン リスク要因	定義又はガイダンス	リスクの非排他的な指標（該当する場合）
		• その機能に必要な対象品目への、又は対象品目による情報又はデータの伝送（分かっている場合は、供給源の識別、及び伝送の発信者又は受信者の場所を含む）
企業（すなわち、供給源）情報	企業に関する情報（規模、構造、主要なリーダー、及び財務状況を含む）。	• 企業の系図 • 操業年数 • M&A活動（過去及び現在） • 外国政府との契約 • 顧客基盤とトレンド • 企業リーダーの交友関係と過去の経験（外国政府又は軍隊の役員又は幹部） • 上級幹部レベルでの安定性又は高い離職率又は解雇率 • 特定の場所及び全社の従業員数 • 投資家／投資 • 外国企業への特許販売 • 財務指標とトレンド • 財務報告書／監査
品質／過去の実績	対象品目を期待どおりに生産及び提供する供給源の能力に関する情報。これには、製造／開発された製品のミスや欠陥を防止し、顧客にソリューションやサービスを提供する際の問題を回避することに関連する品質アシュアランスのプラクティスについての理解が含まれる。	• 過去の実績情報 • 関連する顧客の評価又は苦情 • リコール • 品質指標 • 品質プログラム及び／又は認定の証拠
人員	製品又はサービスのサプライチェーン内の供給源又は企業体に所属する、又は雇用されている人員に関する情報。	• インサイダー脅威対策プログラムが存在するかどうか、及び／又はサプライヤが身元調査や雇用前検証を実施しているかどうかを含む、サプライヤの人員の精査プログラム • 外国又は敵対国の諜報機関、軍隊、法執行機関、又はその他のセキュリティサービスからの雇用履歴 • 離職率 • 人員数及びコンピテンシー • 疑わしい忠誠心、非倫理的又は違法な行動及び活動の証拠

ベースライン リスク要因	定義又はガイダンス	リスクの非排他的な指標（該当する場合）
物理的	環境、構造物、施設、又はその他の資産の物理的側面に関連する情報で、それらがセキュアであるかどうか、どのようにセキュアであるか、及びそれらが損傷した場合、利用できない場合、又は侵害された場合の結果を理解するのに十分なもの。	• 物理的セキュリティのサポートを確実にする又は支援する手順及びプラクティスなど、物理的セキュリティ管理策の有効性の証拠 • 重要インフラ、機密性の高い政府資産又はミッション機能への近さ • 自然災害又は地震及び気候に関する懸念
地政学的	供給源、あるいは供給源、製品、及び／又はサービスに関連するサプライチェーンに関連する地理的な場所又は地域に関連する情報。	• 地理的な場所を中心とする政変や汚職 • 貿易ルートの混乱 • 管轄区域の法的要件 • 国又は地域の不安定性
外国人による所有、管理、又は影響（FOCI）	外国の利害関係者（例えば、外国政府、又は外国政府が所有又は管理する関係者、あるいは供給源と外国政府との間のその他の関係）による供給源又は対象品目の所有、管理、又は影響が、行使されるかどうかにかかわらず、直接的にも間接的にも、企業の経営や運営に影響を及ぼす事項を指示又は決定する権限を有する。	• 国が敵対国又は特別な懸念のある国として識別されている • 供給源又はそのコンポーネントのサプライヤが、特に懸念のある国又は敵対国を含め、外国において、本社、研究、開発、製造、試験、梱包、流通、サービス施設、又はその他の事業を有している • 供給源（その役員、取締役又は同様の職員、従業員、コンサルタント、又は請負業者を含む）と外国政府との間の識別された個人的及び／又は職業上の関係 • 供給源が本社、研究開発、製造、試験、梱包、流通、サービス施設、又はその他の事業を有している外国の法律及び規制の影響 • サプライヤに対する FOCI の性質又は程度 • 子会社及び二次請負業者を含む、サプライチェーンに関与するあらゆるビジネスエンティティの FOCI、及びその所有又は影響が、米国の敵対国又は懸念のある国によるものであるかどうか • サプライヤの一部又は全部が、外国のエンティティ又は外国の敵対者に取得される可能性があることを示す兆候

ベースライン リスク要因	定義又はガイダンス	リスクの非排他的な指標（該当する場合）
		• 法律が、その国のセキュリティサービスとの個人情報やその他の機密情報の共有を含む協力を義務付けている（独立した司法審査がない）国に所在するサプライヤ • 外国の利害関係者が持つ、サプライヤの業務又は経営、もしくはサプライチェーン内のエンティティ管理又は経営に影響を与える外国の利害関係者のケイパビリティ（能力）を示す兆候 • 取締役会のメンバー、役員、無限責任パートナー、及び上級管理職などの外国の政府関係者又はエンティティとつながりのある、またはつながりからの影響があるサプライチェーン内の主要な経営幹部 • 対象品目の設計、開発、製造、又は流通に関与する外国人又は外国出身の主要な経営幹部 • 外国又は敵対国の諜報機関、法執行機関、又はその他のセキュリティサービスとサプライヤの既知の関係 • サプライヤが、米国に対して知的財産の窃盗を行っていることが知られている国に所在している、又はそのような国の影響を受けている／そのような国に管理されている
コンプライアンス（法令遵守）／法律	コンプライアンス違反、訴訟、犯罪行為、又はその他の関連する法的要件に関する情報	• 関連する米国の法律、規則、契約、又は合意のコンプライアンスの記録 • 制裁措置のコンプライアンス • 貿易統制のコンプライアンス • 判決／罰金
不正、汚職、制裁、及び政府の利害との一致	過去又は現在の不正行為又は汚職に関する情報、及び資格停止、資格剥奪、排除、又は制裁の対象となっている情報（表E-2及び表の直前の説明も参照のこと）	• 民事訴訟又は刑事訴訟 • 不正行為の過去の履歴又は現在の証拠 • 供給源の知的財産の窃盗履歴 • テロを支援している国や、ミサイル技術や化学／生物兵器を拡散させている国への軍事物資、機器、又は技術の販売に関わっているサプライヤの取引、及び米国の利益に対して「地域的な軍事的脅威をもたらす」と国防長官が特定した取引 • 不正な技術移転に関する供給源の履歴

ベースライン リスク要因	定義又はガイダンス	包括的リスク指標（該当する場合）
サイバーセキュリティ	供給源、製品、サービス、及び／又はサプライチェーンのサイバーセキュリティのプラクティス、脆弱性、又はインシデントに関する情報	• 効果的なサイバーセキュリティポリシー及びプラクティスの証拠 • コンピュータネットワーク侵入の被害者としてのサプライヤの前歴 • 知的財産の窃盗の被害者としてのサプライヤの履歴 • 外国の諜報機関が取得品目、技術、又は知的財産を不法に収集したか、又は取得しようとしたかどうかに関する情報 • 軽減されていないサイバーセキュリティ脆弱性の存在 • サプライヤ又は対象品目に関連する、破壊、悪用、又は妨害を含む悪意のある行為の兆候 • 対象品目による米国外への情報又はデータの不正な伝送
*偽造品及び不適合品（供給源及び／又はアセスメント対象の製品に関連する場合はベースラインに含める、疑わしい場合は含める）	偽造品、偽造品の疑いがある製品、グレーマーケット、又は不適合品に関する情報	• サプライヤに関連する偽造品又は不適合品の証拠又は履歴 • サプライヤの偽造防止のプラクティス及び管理策 • グレーマーケットからのコンポーネントの調達
サプライチェーンの関係、可視性、及び管理	供給源及び／又は対象品目に関連するサプライチェーンに関する情報。	• 効果的なC-SCRM及びサプライヤの関係管理プラクティスの証拠 • （対象品目に関連する）コンポーネント又は材料は、上流サプライチェーンの単一供給源に由来する • 単一の貿易ルートへの依存 • 製品の来歴

これらのベースラインリスク要因に関する情報は、情報の種類、質、及び範囲は大きく異なる可能性があるが、一般にオープンソースから入手できるはずである。場合によっては、情報を見つけられない、又は特定の要因に該当すると見なされないことがあるため、それに応じて留意することが望ましい。調査は、アセスメントが実施される目的とコンテキストに最も関連性が高く、信頼できる情報を得られるようにテーラリングすることが望ましい（以下の「アセスメントの文書化と記録管理内容」の節の情報の質に関する説明を参照）。これらの変数のためにリスク要因レベル以下で標準化を試みることは不可能であり、また望ましいことでもない。

これらの要因に関連する所見は、客観的事実、脅威、脆弱性、又は一般的な「曝露（エクスポージャー）」に関する情報の組み合わせを反映している可能性があり、個別に、又は総合的にアセスメントした場合、リスクが存在する可能性、又は存在することを示す。また、これらの所見は、肯定的、中立的、又は否定的である場合もある。肯定的な所見は、供給源又は対象品目が、望ましい又は必要なアシュアランス属性を持っていることを示す。否定的な所見は、懸念を示すリスク、及びリスクが許容範囲内であるかどうか、軽減が必要であるかどうか、及び／又はFASCとの情報共有の必要を強いる可能性があるかについて判断する必要があるリスクが存在する、又は存在する可能性があることを示す。

注意！上記の要因に関連する1つ以上のリスク指標が存在することは、必ずしも、供給源、製品、又はサービスが実行可能なリスク、又は受容できないリスクをもたらすかどうかを示すものではなく、また、リスクの重大度を示すものでもない。また、どのような要因及び所見の組み合わせがリスクを生じさせる可能性があるか、又は逆にリスクの懸念を軽減させる可能性があるかを分析するように注意を払うことが望ましい。リスク判断に不確実性がある場合、追加のデューデリジェンス調査及び分析の実施、内部又は外部でのエスカレーション、又はリスクが軽減不可能なものであるかどうかについての助言を求める必要性が生じる可能性がある。

アセスメントとは別に、又はアセスメントの一部として、政府機関は、特定のサプライヤの使用及び特定の品目、サービス、又は材料の取得又は使用を禁止する法律又は連邦政府の規制があるかどうかを調査することが望ましい。以下のリストは、適用されるすべての法律及び規制を網羅するものではないが、米国のサプライチェーンにリスクをもたらす可能性のある、外国の所有と支配、その他の種類の外国からの影響、外国の敵対者、及び外国投資の懸念に焦点を当てている。

そのようなサプライヤの使用、又は以下のリストの個人又はエンティティからのそのような品目、サービス、又は材料の取得は、例外又は権利放棄がない限りは法律違反であり、したがって、連邦調達プロセスから除外されることが望ましい。以下の禁止事項が発効される前に既に品目を入手している場合、政府機関は、禁止された品目又はサービスを保持することが許可されるかどうか、許可される場合には、継続的な使用によってもたらされる敵対的脅威を軽減できるかどうかを判断するためのアセスメントを実施することが望ましい。

1. **SDN（Specially Designated Nationals and Blocked Persons）リスト：**財務省資産管理局（OFAC）は、EO 13694 及び EO 13757による改正を通じて、悪意のあるサイバー対応型活動に直接的又は間接的に、責任を負う、加担している、又は関与していると判断された当事者を、SDN リスト（Specially Designated Nationals and Blocked Persons リスト）に指定することを規定している。一人以上のブロックされた人物が直接的又は間接的に合計で50%以上の所有権を持つエンティティは、そのエンティティ自体が法律の運用によりブロックされていると見なされる。米国人は、直接的又は間接的であるかを問わず、ブロックされた人物とのいかなる取引も行ってはならない。
2. **SSI（Sectoral Sanctions Identifications）リスト：**財務長官によって識別されたロシア経済の分野で活動する特定の人物に課される分野別の制裁は、EO 13662に基づき、OFACが委任された権限に従って発行した指令を通じて行われた。SSIリストは、米国人が取引、資金提供、又は満期が90日を超える債券の取引を禁止されている、ロシア経済の特定分野で活動する個人を識別している。
3. **FSE（Foreign Sanctions Evaders）リスト：**OFACは、EO 13608に基づくシリア又はイランに対する米国の制裁に違反した、違反を試みた、違反を共謀した、又は違反を引き起こしたと判断された外国の個人及びエンティティのリストを公表している。また、米国の制裁の対象となる人物のために、又はその代理として、詐欺的な取引を促進した外国人のリストも掲載している。このような個人や企業を総称して「Foreign Sanctions Evaders」又は「FSE」と呼ぶ。FSEが関与する、米国人による取引又は米国内の取引は禁止されている。
4. **SAM（System for Award Management）の除外：**SAMには、米国政府全体の連邦調達プログラム及び非調達プログラム（特に断りのない限り）から除外され、連邦契約又は特定の下請請負の受領から除外され、特定の種類の連邦の財政的及び非財政的支援及び給付から除外されている企業の電子名簿が含まれている。SAMシステムは、中央請負業者登録（Central Contractor Registration）、連邦官報（Federal Register）、オンライン表明及び認証申請（Online Representations and Certification Applications）、及び除外者リストシステム（Excluded Parties List System）からのデータを統合している。また、監察総監室の除外リスト（GSA）からのデータも反映される（CFR タイトル 2、パート 180）。
5. **コルレス口座の銀行経由支払口座制裁の対象となる外国金融機関リスト（「CAPTAリスト」）：**CAPTAリストは、パート561の対象となる外国金融機関リストに代わるものである。これには、制裁措置、特定の禁止事項、又は米国企業が取引する前に厳しい条件が課される外国金融機関の名前が含まれる。
6. **ブロック対象として識別される個人：**31 CFR 560及び 31 CFR 560.304に従い、このリストに含まれる財産及び人物は、米国人の所有又は管理下にある場合、又はその範囲内にある場合には、ブロックされなければならない。
7. **BIS未検証リスト：**未検証リスト（UVL）に記載された当事者は、ライセンスの例外により、輸出管理規則（EAR）の対象となる品目を受け取る資格がない。
8. **2019年国防授権法、第889条：**権利放棄が認められない限り、NDAA第889条は、連邦政府、政府の請負業者、助成金や融資の受領者が、Huawei、ZTE、Hytera、Hikvision、Dahua、及びこれらの子会社が製造する特定の「対象通信機器又はサービス」を、「いかなるシステムの重大又は不可欠なコンポーネントとしても、あるいはいかなるシステムの一部としての重要な技術としても」調達又は使用することを禁止している。
9. サプライヤからの商品、サービス、又は材料の取得を制限するその他の連邦規制又は法律。

リスク深刻度スキーマ

政府機関がSCRAの結果に対する適切なリスク対応を判断する際に支援する参照情報として、共通のフレームワークが必要である。このスキーマは、特定の供給源又は対象品目に関連する識別されたリスクが、政府機関で確立されたC-SCRMプロセス内で管理できるか、又はリスク対応の決定又は活動のために内部又は外部のエスカレーションを必要とするかを示している。

既存の政府全体の深刻度スキーマを採用してテーラリングすることには、既に使用されている他の関連プロセス及びガイダンスとの連携及び整合の度合いを生み出すという利点がある。以下に紹介及び説明するサプライチェーンリスク深刻度スキーマ（SCRSS）は、サイバーセキュリティ又はサイバー作戦のミッションを持つ各省庁及び関係機関と協力して策定されたサイバーインシデント深刻度スキーマ（CISS）の意図と構造を反映している。

SCRSSは、CISSと似ているが、サプライチェーンリスクとサイバーインシデントの対比に焦点を当て、それに合わせてテーラリングされており、以下のような共通の見解を確実にすることを意図している。

- 特定の供給源又は対象品目に関連する、アセスメントされたサプライチェーンリスクの深刻度
- リスク対応に求められる緊急性
- リスク対応の調整又は決定に必要な階級レベル
- リスク対応の取り組みに情報を提供し、サポートするために必要な情報、文書、及びプロセス

表 E-2：リスク深刻度スキーマ

レベル	種類	説明
5	国家安全保障上の利益に関わる緊急リスク	国家安全保障上の利益に対する差し迫った、又はインパクトのある、敵対関連のリスク
4	国家安全保障上の利益に関わるリスク	国家安全保障上の利益にインパクトを与える可能性のある、敵対関連のリスク
3	重大なリスク	複数の政府機関にインパクトを与える可能性のある敵対関連のリスク
2	政府機関の高リスク	政府機関の重要なサプライヤ（すなわち供給源）、システム、コンポーネント、又は高価値の資産に関連する、非敵対関連の「高」リスク
1	政府機関の低リスク又は中リスク	他の4つのいずれのリスクレベルの説明にも該当しない、アセスメントされたリスク

表E-2のスキーマは、様々なリスクレベル又はスコアを記述して割り当てるう、政府機関が確立した既存の方法論に取って代わることを意図したものではない。むしろ、政府機関のリスクアセスメント結果を、その結果を最も密接に記述するスキーマレベルに関連付ける、マッピング参照として使用される。マッピングによって、政府機関は、その目的及びコンテキストに適した方法でリスクレベルをアセスメント及び記述するために必要な柔軟性を得ると同時に、連邦政府の事業体全体にわたって供給リスクの深刻度を一般的に記述するための標準化された語彙を作成することができる。このスキーマのフレームワークは、各レベルに関連するリスク対応の調整、情報共有、及び意思決定の責任に関する期待事項を伝達するのにも役立つ。

リスク対応ガイダンス

アセスメントされたサプライチェーンリスクのSCRSSレベルに応じて、政府機関は、追加の調査、分析、又はリスク対応の決定のために、SCRA情報をエスカレーションして内部組織内の人と共有したり、FASCなどの外部職員と連携したりする必要がある場合がある。

情報共有

レベル3以上でアセスメントされたサプライチェーンリスクは、FASCの規則により「相当なリスク」と見なされ、その後のレビュー及び潜在的な追加の分析及び措置のために、情報共有機関[54]（ISA）を通じて FASCとの情報共有が義務付けられている。各政府機関は、それぞれの判断で、FASCの情報共有プロセス及び要件に従って、識別されたレベル2又はレベル1のリスクに関する情報をFASCのサプライチェーンと自発的に共有することを選択してもよい。

アセスメントプロセスの外部で識別された、又は受け取ったSCRIは、FASC又はFBI、FCC、DHS CISAなどの他の政府組織との強制的又は自発的な共有の必要性を強いる場合もある。そのような情報の例としては、サプライチェーンの事象、サプライチェーンのインシデント、調査組織（例えば、監察総監室）から得た情報、又は政府機関のホットラインを通じて受け取った匿名の情報が含まれるが、これらに限定されない。

政府機関とFASCの間で行われるすべての情報共有は、強制的であるか自発的であるかにかかわらず、権限を付与する法律及び規則に沿った、FASCが確立した情報共有の要件及びプロセスに従って行われる必要がある。さらに、政府機関は、FASCと情報を共有するための連絡役として、政府機関の上級職員を指名することが望ましい。政府機関は、政府機関とFASCの間で情報を共有（送受信）するためのプロセスを確立し、自らの組織内でSCRIを共有するために、それぞれの組織に合わせてテーラリングされた相応の要件及びプロセスを確立することが望ましい。

注：FASCは、強制的及び自発的な情報共有の状況及び基準に関する更新又は追加のガイダンスを発行する場合がある。政府機関は、最新のFASCガイダンスを参照し、それに従うことが望ましい。

リスク対応のエスカレーション及びトリアージ

政府機関は、NIST SP 800-161 Rev. 1の本文及び附属書で広く取り上げられているように、SCRMを事業体のリスクマネジメント活動及びガバナンスに統合することの重要性を再認識している。SCRSSの相当なレベルにあると判断されたリスクについては、リスクアセスメント情報を、法律顧問を含む、政府機関内の該当する上級職員にエスカレーションする必要がある。また、政府機関は、適切な職員が、リスク対応の調整、決定、又は行動に情報を提供する、またはサポートするために、必要かつ適切な場合には国家機密情報へのアクセスを許可する十分なセキュリティクリアランスを持つことを確実にすることが望ましい。

相当であると見なされるリスクは本質的に敵対的であるため、アセスメントされたリスクへの対応、又は供給源との関与もしくはコミュニケーションの前に考慮する必要がある、法執行機関、対諜報機関、法的意味合い、又は既存の活動が存在する場合もある。政府機関が相当なリスクの情報をFASCと共有することで、これらのリスクが適切に「トリアージ」されることを確実にするために政府機関が従うべきプロセスが標準化され、合理化される。

[54] 国土安全保障省（DHS）は、主にサイバーセキュリティ・インフラストラクチャセキュリティ庁（CASA：Cybersecurity and Infrastructure Security Agency）を通じて活動しており、FASC の ISA としての役割を果たすように指定されている。 ISA は、41 U.S.C. 1323（a）（3）に規定されているように、FASC の代理として管理情報共有機能を実行する。kk

アセスメントの文書化及び記録管理

コンテンツの文書化のガイダンス

政府機関は、供給源及び／又は対象品目に関する情報をFASCと強制的に共有するために、又は政府機関の第4713条の権限の使用を含意する可能性のあるリスク対応の決定のために内部でエスカレーションする際に、アセスメント記録が本節に記載されている最小限の文書化要件を満たすことを確実にする必要がある。この文書化のベースライン標準は、十分な情報に基づいたリスク対応の決定と行動をサポートするために、堅牢で正当化できる記録が確立されている、又は確立できることを確実にするのに役立つ。また、比較可能性、再利用性、情報共有を容易にするために、文書化した内容の範囲及び構成の一貫性を促進するのにも役立つ。

文書化の要件には、リスク要因アセスメント情報の把握にとどまらず、誰がいつアセスメントを実施したかについての一般的な事実、供給源及び対象品目に関する識別子及び記述情報、アセスメント情報を取得するために使用されたデータソースの引用、個別の所見に対する信頼レベルの割り当て設定及び所見の集計分析、前提条件及び制約条件の注記が含まれる。

政府機関はまた、定義されたアセスメント及びリスク判断の方法論を有し、それに従うことが望ましい。この方法論は、特定の供給源及び／又は対象品目に関するアセスメント記録で文書化又は参照されることが望ましい。政府機関が定義した方法論からの逸脱は、アセスメント記録の一般情報の節に記述されることが望ましい。

情報が調査され、編集される際には、様々なリスク要因のカテゴリと一致する関連した所見を抽出して文書化するために、情報を整理して統合する必要がある。出典付きの情報（コンテキスト上のメタデータを含む）、特に懸念されるリスクに関する顕著な所見は、情報の完全性を保持し、リスク対応の決定又は行動をサポート及び擁護するために必要とされる可能性のある補完内容と見なされる形式で、保持又は検索可能であることが望ましい。そのため、アセスメント活動の一環として、出典付きの情報の情報源、情報の質、及び信頼性を検討し、それに応じて文書化する必要がある。大まかに言えば、質の高い情報は、タイムリーで、関連性があり、偏りがなく、十分に完全であるか、又はコンテキストの中で提供され、信頼できる情報源から得たものであることが望ましい。

文書化要件は、既存の関連するサプライチェーンのリスクアセスメントのポリシー、プロセス、及び手順に組み込まれることが望ましい。これらの要件は、法律顧問及び記録管理、CUI及び国家機密情報の管理、及びプライバシーに対する責任を負う人員を含む、政府機関内の職員との協議及び職員からの指示によって情報が提供されることが望ましい。

形式は指定されていないが、特定のアセスメント記録の内容及び文書化の最小範囲には、以下の表E-3に記載されている内容を含めることが望ましい。

表 E-3：アセスメント記録：内容及び文書化の最小範囲

一般情報	追加コメント
アセスメントの責任を負う政府機関	政府機関は、連絡窓口を特定できること、及びアセスメントをサポートした非連邦政府の人員、アセスメントをサポートするために使用されたツール、及び／又はデータソース（商業的に入手したものを含む）に関する情報を保持できることが望ましい。
アセスメントの日付、又はアセスメントが実施された時間枠	政府機関は、どの所見が一時的なものであり、時間の経過とともに変化する可能性があるかに留意することが望ましい。
供給源プロファイル：アセスメントされたサプライヤに関する識別子及び記述情報	サプライヤの正式名称、DBA名、本拠地、実際の住所、及び（異なる場合は）本社の物理的な所在地、DUNS番号及びCAGEコード、連絡先電話番号、外国企業又は国内企業として登録されている、企業WebサイトのURL、企業の系図の構造及び企業の系図内の位置（分かっている場合）、企業の規模、操業年数、及び市場セグメントを（知り得る範囲で適切に）文書化する。
アセスメントされた対象品目に関する識別子及び記述情報	製品名、一意の識別子（例えば、型番、バージョン番号、シリアル番号）、関連するNAICS及びPSC、及び簡単な説明を文書化する。
アセスメントの目的及びコンテキストの概要	アセスメントが発生した際に示された、該当するライフサイクルフェーズ（例えば、市場調査、調達活動、運用利用）を識別する。
アセスメントの方法論	文書化された方法論を参照し、そこからの逸脱を記述する。
供給源又は対象品目の調査、所見、及びリスクアセスメントの結果	リスクの所見、識別、及びアセスメントの分析を文書化する。最低限、主要な所見の要約、それらの所見の分析、及びリスクレベル判断の理論的根拠があることが望ましい。この要約では、供給源、対象品目、及び関連するサプライチェーンの潜在的又は既存の脅威（それらが本質的に敵対的、非敵対的、又は不確定であるとアセスメントされるかどうか、及びその理由）又は脆弱性に対処することが望ましい。関連する前提条件及び制約条件についての注釈を含める。
インパクトアセスメント	アセスメントの目的及びコンテキストに関連して、識別されたリスクの種類、範囲、及び深刻度を考慮して、アセスメントされたインパクトの可能性を記述する。

一般情報	追加コメント
解決していない又は受容できないリスクの軽減	満足のいくレベルまでリスクを軽減するための供給源のケイパビリティ（能力）、キャパシティ、及び意欲、及び／又はリスクを軽減する政府機関のケイパビリティ（能力）及びキャパシティに関する議論を含める。解決していない又は受容できないリスクに対処するための実行可能な軽減オプションが分かっている場合は、それを識別する。
サプライチェーンリスク深刻度スキーマに従ったリスク深刻度レベルのアセスメント	SCRSSレベル番号、及びこのレベルが割り当てられた理由の説明を含める。政府のミッション又は資産、国家安全保障、国土安全保障、又は供給源や対象品目の使用に関連する重要な機能に対して識別された影響に対処する。
リスク対応	リスク対応の決定又は行われた措置について記述する（例えば、回避、軽減、調整及びトリアージのためのFASCへのエスカレーション）。
FASCにより提供するよう指定及び指示されたその他の情報、又は政府機関の裁量により含まれるその他の情報	政府機関の機能へのインパクト、及びFASCが適切と見なすその他の情報を含め、サプライチェーンリスクのアセスメントにおいて考慮に入れる情報を記述又は提供する。
レビュー及びクリアランス	手続き、代替手段の使用、及び／又は軽減努力の実施に関連してリスクアセスメントに使用される供給源及び使用可能な情報の信ぴょう性及び信頼性が対処されることを確実にする。相当なリスクであるとアセスメントされたリスクについて、アセスメント記録が、適切な上級責任者や法律顧問を含む、適切な担当者によってレビューされ、クリアされたことを確認する。レビュー及びクリアランスは、アセスメント記録及び裏付けとなる情報が適切に保護され、マークされ、アクセス制御されていることを確実にすることも目的としている。

アセスメント記録

政府機関は、SCRA及びそれを裏付ける成果物に関して、記録管理の要件に従っていることを確実にすることが望ましい。アセスメント記録及びその関連する内容に関連する必要な保護、マーキング、取り扱い、保存、及び配布の要件と制限に対処するポリシー及び手順を整備することが望ましい。

アセスメント記録の作成をサポートするためにアセスメントサービス（例えば、分析サポート）又は商業的に提供された情報を取得する場合には、合意（例えば、契約、省庁間協定）に、範囲、データ使用の目的、及び制限、アクセス、廃棄、及び保存の権利に関する適切な要件及び制限を規定することが望ましい。

附属書 F：大統領令14028号のソフトウェアのサプライチェーンセキュリティ強化のためのガイドライン公開要請への対応

大統領令（EO：Executive Order）14028号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従ってサプライチェーンのサイバーセキュリティリスクマネジメントを実装しようとする各省庁及び関係機関は、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）のEO14028専用ウェブベースポータル（https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity）を参照することが望ましい。このガイダンスは、以下の目的でオンラインに移行された。

- NIST管轄下の関連するEOガイダンスと同じ場所に置く。
- SP 800-161, Rev. 1 に直接インパクトを与えることなく、進化するガイダンスを反映するための更新を可能にする。
- ステークホルダーとの動的かつインタラクティブな関与を促進するために、他のNISTウェブベース資産がオンラインに移行していることに伴い、トレーサビリティ及びそれらの資産との連携を提供する。

附属書 G：リスクマネジメントプロセスにおけるC-SCRM活動 [55]

リスクマネジメントとは、事業体に対して1）リスクの枠組み化（すなわち、リスクベースの意思決定のコンテキストの確立）、2）リスクのアセスメント、3）判断されたリスクへの対応、及び4）事業体のリスク関連活動における継続的改善のための、効果的な事業体の伝達及びフィードバックループを使用した継続的なリスクの監視、を求める包括的なプロセスである。図G-1は、各分析の実行順序、及び事業体、ミッション、並びに運用レベルの様々なインプットが分析に含まれることを確実にするために必要な相互作用を含む、リスクマネジメントプロセスのステップ間の関係を示している。

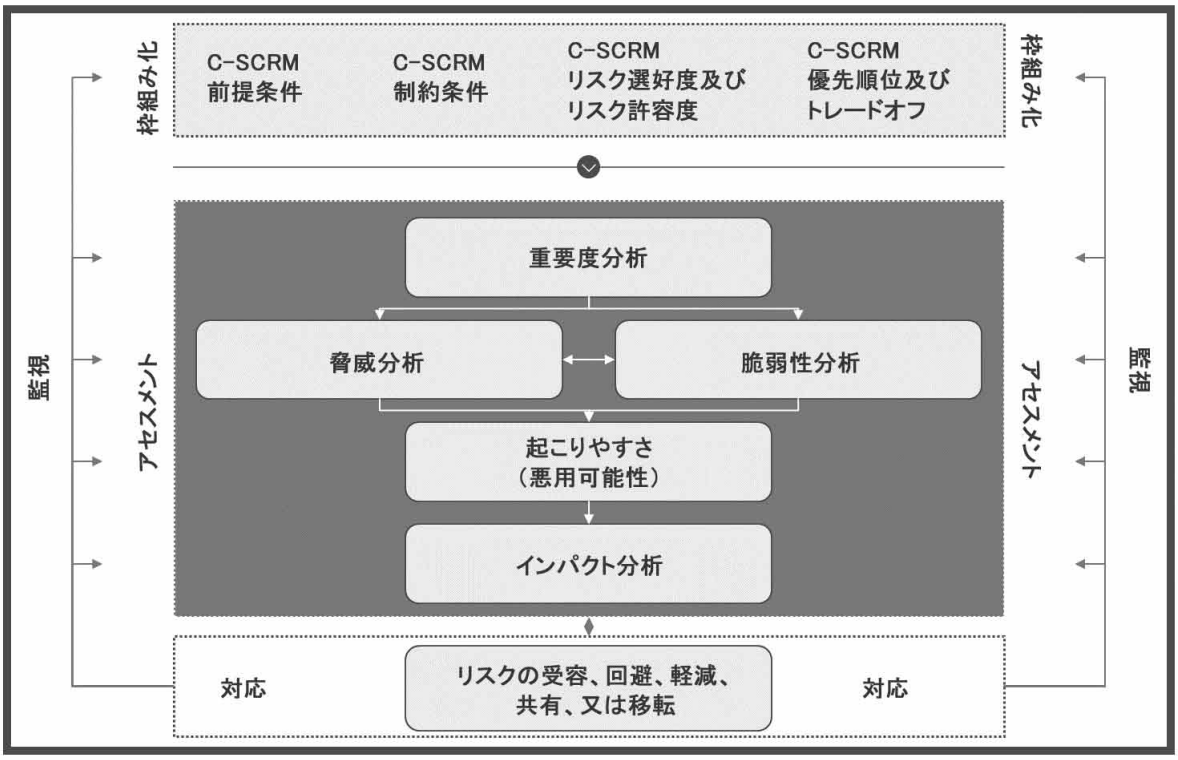

図 G-1：サプライチェーンのサイバーセキュリティリスクマネジメント（C-SCRM）

リスクマネジメントプロセスの各ステップ（枠組み化、アセスメント、対応、及び監視）は反復的であり、本質的に順次的なものではない。特定のニーズ又は状況に応じて、異なる個人が同時にステップを実行する必要がある場合がある。事業体は、リスクマネジメントのステップの実施方法（例えば、順序、厳密さの度合い、形式、及び適用の徹底度）及び各ステップの結果をどのようにキャプチャし、事業体内外で共有するかについて、大きな柔軟性を有する。特定のリスクマネジメントステップからのアウトプットは、リスクマネジメントプロセスにおける1つ以上の他のリスクマネジメントステップに直接影響を与える。

図G-2は、リスクマネジメントプロセス全体を通じて、3つのリスクフレームワークレベル内で実行されるC-SCRM活動を要約したものである。リスクマネジメントプロセスの異なるステップ間の矢印は、ステップ間の情報とガイダンスの同時的な流れを示している。

[55] 各省庁及び関係機関は、大統領令14028号「国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）」に従って本ガイダンスを実装するために、附属書Fを参照することが望ましい。

矢印は、インプット、活動、及びアウトプットがそれぞれ継続的に相互作用及び相互に影響し合っていることを示している。詳細については以降の小節で説明する。

図 G-2：リスクマネジメントプロセスにおけるC-SCRM活動

図 G-2は、各分析が実行される順序、及び分析が事業体、ミッション及びビジネスプロセス、並びに運用レベルの様々なインプットを含むことを確実にするために必要な相互作用を含む、リスクマネジメントプロセスのステップ間の関係を示している。

本節の以降の部分では、リスクマネジメントプロセスの枠組み化、アセスメント、対応、及び監視ステップ内のC-SCRM活動の詳細を説明する。小節「枠組み化」から「監視」の構成は、[NIST SP 800-39]の 3.1～ 3.4節の構成を反映している。リスクマネジメントプロセスの各ステップ

（すなわち、枠組み化、アセスメント、対応、監視）の構成には、「インプット及び前提条件」、「活動」、「アウトプット及び事後条件」が含まれる。活動は[NIST SP 800-39]に従って、さらにタスクにまとめられている。[NIST SP 800-161, Rev 1.]はリスクマネジメントプロセスのステップ及びタスクを引用しているが、[NIST SP 800-39]の他の内容を繰り返すのではなく、各ステップのC-SCRM特有のガイダンスと、インプット及び前提条件、及び活動並びに対応するタスク、アウトプット及び事後条件を提供している。本出版物では、[NIST SP 800-39]のアセスメントステップで提供されているタスクに、タスク2-0、重要度分析という1つのタスクを追加している。

対象読者

本附属書の対象読者は、サプライチェーンのリスクマネジメントプロセスを全レベル及び各レベルで実行するために、特定のC-SCRMの責任を負う個人である。例としては、事業体の他の部分（例えば、C-SCRM PMOプロセス、事業体リスクマネジメント、ミッション及びビジネスプロセスリスクマネージャ）で使用されるフレームワーク及び方法論を定義する責任を負うプロセス／機能スタッフが含まれる。その他の人員又はエンティティは、それぞれの状況に応じて、自由にガイダンスを利用することができる。

事業体全体のリスクマネジメント及びRMF

サプライチェーン全体のサイバーセキュリティリスクを管理するには、事業体、ミッション及びビジネスプロセス、並びに運用レベルで、事業体による協調的で目的を持った取り組みが必要である。本出版物では、3つのレベルにわたって効果的なリスクマネジメントを促進するために反復的に組み合わされる、異なるが補完的な2種類のリスクマネジメントアプローチについて説明する。

1番目のアプローチはFARMとして知られており、「枠組み化」、「アセスメント」、「対応」、「監視」の4つのステップで構成されている。FARMは、事業体のリスクのコンテキスト及びリスクに対する固有の曝露（エクスポージャー）を確立するために、主にレベル1及びレベル2で使用される。次に、レベル1及びレベル2からのリスクのコンテキストは、[NIST SP 800-37, Rev. 2]リスクマネジメントフレームワーク（RMF）で説明されている2番目のアプローチの一部として実施される活動に、繰り返し情報を提供する。RMFは主にレベル3[56] –運用レベル–で運用され、準備、分類、選択、実装、アセスメント、認可、及び監視の7つのプロセスステップで構成される。RMF内では、レベル1及びレベル2のFARMからのインプットがRMF準備ステップの一部として合成され、その後、RMFの各ステップを通じて反復的に適用、テーラリング、及び更新される。最終的に、レベル1及びレベル2の前提条件は、特定の運用レベル又は調達活動のコンテキストに適合するように、繰り返しカスタマイズ及びテーラリングされる。例えば、事業体がレベル1（事業体レベル）で戦略的優先順位及び脅威を決定し、その決定がレベル2のミッション及びビジネスプロセスの重要度の決定に情報を与え、次にレベル3（運用レベル）におけるRMFの一部として、システムの分類化、管理策の選択、及び管理策の実装に影響を与える場合がある。レベル間の情報の流れは双方向であり、集約されたレベル3のRMFのアウトプットは、レベル1及びレベル2で想定された前提条件を定期的に更新及び改良するのに役立つ。

[56] RMFは、共通管理策の識別など、レベル1及びレベル2に適用できるものもある。

枠組み化

インプット及び前提条件

枠組み化は、3つのレベルすべてでC-SCRMのコンテキストを確立するステップである。このステップでは、事業体のサプライチェーンの範囲及び構造、全体的なリスクマネジメント戦略、特定の事業体及びミッション並びにビジネスプロセスの戦略及び計画、及び個々の情報システムが定義される。枠組み化で収集されたデータ及び情報は、3つのレベルを通じて、他のリスクマネジメントプロセスステップにおけるC-SCRM活動の範囲策定及び微調整のためのインプットを提供する。枠組み化はまた、事業体、ミッション及びビジネスプロセスレベルのリスクマネジメント戦略の一部として、フレームワーク及び方法論の形でガイダンスが確立される場でもある。
これらのフレームワーク及び方法論は、後のステップで実行されるサプライチェーンリスクマネジメント活動の境界、標準化、及び方向性を提供する。

[NIST SP 800-39]は、リスク枠組み化を「事業体のリスク管理アプローチを形成する前提条件、制約条件、リスク許容度、及び優先順位／トレードオフのセット」と定義している。事業体全体のリスク枠組み化活動及びC-SCRMのリスク枠組み化活動は、相互に繰り返し情報を提供することが望ましい。事業体がリスクに関して想定する前提条件は、C-SCRM活動（例えば、事業体の戦略的優先順位）におけるリスクの枠組み化にフローダウンし、情報を提供することが望ましい。サプライチェーン全体のサイバーセキュリティリスクに関する事業体の前提条件が、C-SCRM活動の実行を通じて進化するにつれて、これらの前提条件をフローアップし、事業体レベルでのリスクの枠組み化方法を通知することが望ましい（例えば、個々のサプライヤに対するリスクの曝露（エクスポージャー）のレベル）。C-SCRMリスクの枠組み化プロセスへのインプットには、以下が含まれるが、これらに限定されない。

- 事業体のポリシー、戦略、及びガバナンス
- 適用される法律及び規制
- 政府機関の重要サプライヤ及び契約サービス
- 事業体プロセス（セキュリティ、品質など）
- 事業体の脅威、脆弱性、リスク、及びリスク許容度
- エンタープライズアーキテクチャ
- ミッションレベルの目標及び目的
- ミッション／プロセスの重要度
- ミッションレベルのセキュリティポリシー
- 機能の要件
- 供給されるシステム／製品コンポーネントの重要度
- セキュリティ要件

C-SCRMのリスク枠組み化は、リスクマネジメントプロセスの他のステップ（アセスメント、対応、及び監視）からのインプットもインプットとして使用する反復プロセスである。図G-3は、3つの事業体レベルに沿ったインプット及びアウトプットを持つ枠組み化ステップを示している。事業体レベルでは、活動は、事業体全体に幅広く適用される枠組み化の条件（すなわち、前提条件、制約条件、選好度及び許容度、並びに優先順位及びトレードオフ）に重点を置いている。枠組み化の目標は、サプライチェーン全体のサイバーセキュリティリスクを、事業体とその戦略的目標及び目的との関連においてコンテキスト化することである。レベル2では、枠組み化の活動は、個々のミッション及びビジネスプロセスに合わせたリスク枠組みのテーラリングに重点を覆いている（例えば、ミッション又はビジネス目的の達成におけるサービスプロバイダの役割に関する前提条件）。

最後に、レベル3では、レベル1及びレベル2で概説された条件が、RMFプロセスの各ステップに繰り返し情報を提供する。準備ステップから、個々の情報システム、供給されるシステムコンポーネント、及びシステムサービスプロバイダに関するサプライチェーン全体のサイバーセキュリティリスクを管理するためのコンテキスト及び優先順位を確立するために、レベル1及びレベル2で概説された条件が使用される。後続の各RMFステップ（「分類」～「監視」）では、適用される運用レベルの考慮事項を反映するために、これらの前提条件が繰り返し更新及びテーラリングされる。下位レベルの活動の実行中に発見された知見は、上位レベルで概説された前提条件に関して判明していることが更新される可能性があるため、情報フローはレベル間で双方向でなければならない。

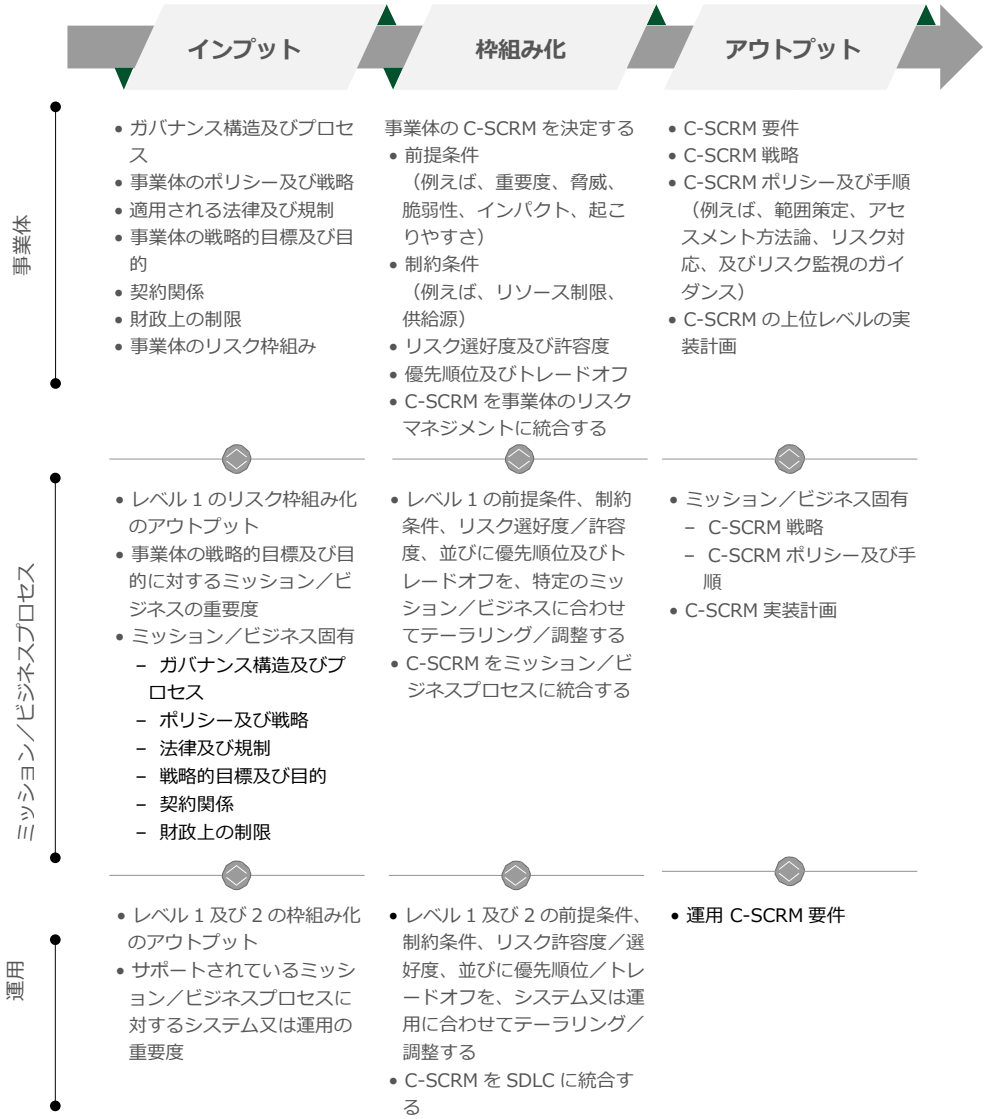

図 G-3：枠組み化ステップにおけるC-SCRM

図G-3からG-6は、3つのリスクマネジメントフレームワークレベルに沿って区分された枠組み化ステップのインプット、活動、及びアウトプットを示している。活動の左右にある大きな矢印は、リスクマネジメントプロセスの他のステップへのインプット又はそれらのステップからのアウトプットを示している。枠組み化ステップへのインプットには、他のステップからのインプット、及びC-SCRMプロセスを形成するエンタープライズリスクマネジメントプロセスからのインプットが含まれる。レベル間の上下の矢印は、上位レベルから下位レベルへの情報及びガイダンスの流れと、下位レベルから上位レベルへの情報及びフィードバックの流れを示している。矢印は、インプット、活動、及びアウトプットが継続的に相互作用及び相互に影響し合っていることを示

している。

枠組み化ステップは条件を定義するために使用されるため、事業体は、枠組み化活動の実行頻度が、FARMプロセスの後半のステップに比べて比較的少ないことに気付く場合がある。事業体は、定義された間隔（例えば、1年ごと、半年ごと）で、又は定義されたトリガー（例えば、ビジネスの変更及び／又は他のレベルからの新しい知見又は更新された知見）に基づいて、枠組み化の活動を再実行することができる。

活動

リスクの前提条件

タスク 1-1：事業体内でリスクがどのようにアセスメントされ、対応され、監視されるかに影響する前提条件を識別する。

補足ガイダンス

より広範なリスクマネジメントプロセス（[NIST SP 800-39]に記載）の中でリスク前提条件を識別する一環として、政府機関は以下を行うことが望ましい。

- 事業体全体のC-SCRMポリシーを策定する。
- 重要度を判断するために、事業体にとって重要なミッション及びビジネスプロセスと関連コンポーネントを識別する。
- 関連する契約サービス及び市販製品を含む、サプライチェーンを構成するミッション及びビジネスプロセスと情報システムを定義する。
- 国家安全保障及び国土安全保障に関する懸念事項、FIPS 199のインパクトレベル、使用範囲、又は他の重要なプロセス及び資産との相互接続／相互依存関係などの要因（これらに限定されない）を考慮し、これらの重要な要素に対するリスク対応の適用に優先順位付けを行う。
- サプライチェーンに関連する脅威源、脆弱性、結果／インパクト、及び起こりやすさを識別し、特徴付け、代表的な例を提供する。
- C-SCRMのミッション、ビジネス、及び運用レベルの要件を定義する。
- 事業体のガバナンス、文化、並びにミッション及びビジネスプロセスの多様性に応じて、適切なアセスメント方法論を選択する。
- C-SCRM活動の結果を政府機関の全体的なリスクマネジメントプロセスに統合するための手法を確立する。
- 時間の経過とともに進化する定義が常に最新であることを確実にするために、定期的にサプライチェーンのレビューを実施する。

これらのC-SCRM前提条件は、該当する場合には、エンタープライズリスクマネジメントプログラムの一部として定義された、より広範なリスク前提条件に整合していることが望ましい。主要なC-SCRMの責務（例えば、C-SCRM PMOの責務）は、各リスクマネジメントフレームワークのレベルにおいて、どの前提条件がC-SCRMのコンテキストに適用されるかを識別することである。新しいリスク前提条件（すなわち、タスク1-1）が識別された場合は、繰り返しプロセスの一部として、対応するすべての事業体リスク前提条件（すなわちタスク1-1 の事業体リスクマネジメントバージョン）の更新として提供されることが望ましい。

重要度

重要なプロセスとは、中断、破損、又は無効化された場合に、結果としてミッションの劣化又は失敗につながる可能性高いプロセスである。ミッション上重要なプロセスは、そのサポートシステムに依存しており、次にこれらのシステム内の重要なコンポーネント（例えば、ハードウェア、ソフトウェア、ファームウェア）に依存している。ミッション上重要なプロセスは、その重要なプロセスを実行するために使用される（場合によってはサポートサービスの請負業者を含む、技術又は個人により実行される）情報及びプロセスにも依存している。ミッション上重要なプロセスを下支えして実現するコンポーネント及びプロセス、又は防御的で一般的に共有される プロセス（例えば、アクセス制御、ID管理、暗号化）と非仲介アクセス（例えば、電源）を提供するコンポーネント及びプロセスもまた、重要であると考えることが望ましい。重要度分析は、ミッション上重要なプロセス、関連するシステム／コンポーネント、及び実現するインフラストラクチャ及びサポートサービスを識別及び優先順位付けするための主要な方法である。重要度分析では、内部の重要度分析では把握されない可能性がある重要なサプライヤの分析（例えばフォース及びフィフスパーティサプライヤを含むサプライチェーン相互依存関係）も行われる。

事業体は、[NISTIR 8179][57]で概説されているプロセスに基づいて、事業体リスクマネジメント活動の一環として重要度の決定を行う。可能であれば、C-SCRMはこれらの前提条件を継承し、C-SCRMのコンテキストを含めるようにこれらの前提条件をテーラリング／調整することが望ましい。C-SCRMでは、重要度のテーラリングには、各レベルの重要なプロセスに関連において、サプライチェーン内の特定プロジェクト、製品、及びプロセスの初回の重要度分析が含まれる。例えば、事業体は、レベル1において、事業体の全体的な戦略目的に対する包括的なサプライヤ関係の重要度を決定することができる。次に、レベル2において、事業体は特定のミッション及びビジネスプロセス、並びに戦略的／運用目的に対する個々のサプライヤ、製品、及びサービスの重要度をアセスメントすることができる。最後に、レベル3において、事業体は、情報システムの特定の運用状態の目的に対する供給製品又はサービスの重要度をアセスメントすることができる。

事業体は、事業体のプロセス及びシステムの運用とレジリエンスカに貢献する、主要なサプライヤ提供製品又はサービスを識別することから始めることができる。これらの要素の一部は、災害時復旧と運用継続計画の一部として把握及び定義されている場合がある。重要度の決定は、プロセス又はシステムの要求される戦略的又は運用目的を達成する上での各サプライヤ、製品、又はサービスの役割に基づいて行うことができる。要件、アーキテクチャ、及び設計は、分析に情報を提供し、運用（すなわち、事業体、ミッション及びビジネスプロセス、及び運用レベル）に必要な最小限の一連のサプライヤ提供製品及び／又はサービスを識別するのに役立つ。分析では、トップダウン及びボトムアップ分析アプローチを組み合わせる。このモデルのトップダウンアプローチにより、事業体は重要なプロセスを識別し、次に、それらのシステムをサポートする重要なプロセス、及びそれらのシステムの重要な機能をサポートする重要なコンポーネントに分析を漸進的に絞り込むことができる。ボトムアップアプローチでは、誤動作した、侵害された、又は使用不可能な重要なコンポーネントがシステムに与えるインパクト、さらには関連するミッション及びビジネスプロセスに与えるであろうインパクトを漸進的に追跡する。

この分析を実行する事業体は、重要なフォースパーティサプライヤを含めるために、政府機関システム及びサイバーセキュリティサプライチェーンの依存関係を含めることが望ましい。例えば、事業体はサードパーティサプライヤが共通のフォースパーティサプライヤから重要なインプット又はサービスを受けることによって発生するサイバーセキュリティリスクの曝露（エクスポージャー）を検出する可能性がある。

[57] NISTIR 8179、「重要度分析プロセスモデル：システム及びコンポーネントの優先順位付け（*Criticality Analysis Process Model: Prioritizing Systems and Components*）」を参照のこと。

重要度の決定は、枠組み化とアセスメントの両方ですべてのレベルで実行される反復プロセスである。枠組み化では、重要度の決定は、追加の反復又はアセスメントステップで組み込まれた詳細と利用可能な情報を使用して、上位レベルで実行されることが期待されている。重要度の決定には、以下が含まれる可能性がある。

- すべてのレベルにおける事業体の重要度分析を手引きする一連の文書化された手順があることを確実にするために、重要度分析手順を定義する。
- 事業体及びミッションの目的、目標、及び要件を識別及び優先順位付けするために、事業体及びミッションレベルの重要度分析を実施する。
- 重要なワークフローパス、システム機能、及びケイパビリティ（能力）を識別及び優先順位付けするために、運用レベルの重要度分析（すなわち、システム及びサブシステム）を実施する。
- 主要システム及びサブシステムのインプット（例えば、COTS製品）を識別及び優先順位付けするために、システム及びサブシステムコンポーネントレベルの重要度分析を実施する。
- プロセス間の相互作用及びコラボレーションを確実にするために、事業体、ミッション、システム／サブシステム、及びコンポーネント／サブコンポーネント間のインパクト及び相互作用の詳細なレビュー（例えば、ボトムアップ分析）を実施する。

サプライチェーンのインシデントが、組織の業務、資産、及び場合によってはビジネスパートナー又は顧客にもたらす可能性がある潜在的なインパクトを考慮すると、重要度に加えて、重要課題（マテリアリティ）に関する考慮事項が、サプライチェーンのリスクマネジメント戦略、リスクアセスメントのプラクティス、及びサプライチェーンリスクの全体的なガバナンスに確実に組み込まれていることを確実にすることが組織にとって重要である。重要度とは対象的に、重要課題は、その情報が投資判断を行う合理的な投資家によって、株主が利用可能な情報の組み合わせ全体を大きく変えるものとして見られていたどうかを考慮する[58]。SECのガイダンスでは以下のように記述されている。

> …サイバーセキュリティリスク及びインシデントの重要課題は、そのようなインシデントがもたらす可能性がある損害の範囲によっても異なる。これには、企業の評判、業績、顧客及びベンターとの関係に対する損害、並びに州及び連邦政府当局及び米国以外の当局による規制措置を含む訴訟、規制調査又は措置の可能性が含まれる。

重要度は、既存のシステム、又はシステムアーキテクチャと設計に基づく将来のシステム投資、開発、又は統合の取り組みに対して決定することができる。これは、監視ステップで反復を正当化する変更が識別された際に実行されることが望ましい、反復的な活動である。

脅威源

C-SCRMの場合、脅威源には、1）サプライチェーン又はサプライチェーンを横断する情報システムコンポーネントに対するサイバー／物理的攻撃などの敵対的脅威、2）偶発的なヒューマンエラー、3）機器の故障、環境制御、及び資源枯渇を含む構造的な障害、及び 4）地政学的混乱、パンデミック、経済動乱、自然災害又は人為的災害などの環境上の脅威が含まれる。敵対的脅威に関して、[NIST SP 800-39]は、事業体は、レベル1（事業体レベル）、レベル2（ミッション及びビジネスプロセスレベル）、及びレベル3（情報システム／サービスレベル）で展開される保全措置及び対策（すなわち、セキュリティ管理策）によって対処されるべき敵対者によって採用される戦術、技術、及び手順の種類の簡潔な特徴を提供し、保全措置及び対策により対処される脅威源及び対処されない脅威源の種類を明確にすることが望ましい、と述べている。

[58] 定義の詳細については、用語集を参照のこと。

脅威情報には、過去の脅威データ、事実に基づく脅威データ、又はビジネスエンティティ（例えば、サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダ）、又は技術固有の脅威データが含まれるが、これらに限定されない。脅威情報は、米国情報コミュニティ（U.S. Intelligence Community）（連邦政府機関向け）、DHS、CISA、FBI、情報共有分析センター（ISAC）、及びニュースや業界紙、パートナー、サプライヤ、及び顧客などのオープンソースの報告を含む、複数の情報源から得られる場合がある。該当する場合、事業体は、前述の情報源に加えて、サプライチェーンの脅威情報について、連邦調達安全保障会議（FASC：Federal Acquisition Security Council）の情報共有機関（ISA：Information Sharing Agency）を頼りにする場合もある。脅威情報には機密情報が含まれる可能性があるため、各省庁及び関係機関が機密情報を処理するために必要なケイパビリティ（能力）を有していることが重要である。枠組み化ステップの一部として取得された脅威情報は、事業体固有の内部及び外部特性に基づいて、脅威の状態に関する事業体の長期的な前提条件を文書化するために使用することが望ましい。アセスメントステップでは、製品又はサービスの調達に関する決定にインパクトを与える可能性がある脅威状態の短期的な変動（例えば、地政学的な事情によるもの）を説明するために、リスクアセスメントに更新された脅威情報が注入される。

サプライチェーンに関する情報（サプライチェーンマップなど）は、脅威源及びエージェントがサプライチェーンに影響を与える可能性がある場所又はアクセスポイントを識別するためのコンテキストを提供する。サプライチェーンのサイバーセキュリティ脅威は、災害、攻撃者、産業スパイなどの情報セキュリティ脅威に似ている。表G-1 は、サプライチェーンのサイバーセキュリティ脅威エージェントの例を示している。附属書Gは、表G-1にリスト化されたサプライチェーン脅威源及びエージェントの例を含む、リスク対応計画を提供している。

表 G-1：サプライチェーンのサイバーセキュリティ脅威源及びエージェントの例

脅威源	脅威	例
敵対者： 偽造品	サプライチェーンに混入された偽造品（附属書B、シナリオ1を参照）	犯罪グループが、金銭的利益を得るために偽造品のサイバーコンポーネントを取得して販売しようとする。具体的には、組織犯罪グループが、様々なグレーマーケットの再販業者を通じて取得者に販売することを目的としたサイバーコンポーネントを取得するために、廃棄されたユニットを探し、過剰在庫品を購入し、設計図を取得する[59]。
敵対者： 悪意のあるインサイダー	知的財産の損失	不満を抱いたインサイダーが、金銭的利益を含む様々な理由で、知的財産を競合他社又は外国の諜報機関に売却又は譲渡する。知的財産には、ソフトウェアコード、設計書、又は文書が含まれる。

[59] [防衛産業基盤アセスメント：偽造電子部品（*Defense Industrial Base Assessment: Counterfeit Electronics*）]を参照のこと。

脅威源	脅威	例
敵対者： 外国の諜報機関	悪意のあるコードの挿入（附属書B、シナリオ4を参照）	外国の諜報機関が、サプライチェーンに侵入し、（新しい機能を挿入したり、既存の機能を変更したりして）システムに不要な機能を埋め込み、情報を収集したり、システム稼働時にシステム又はミッションの運用を妨害[60]しようとする。
敵対者： テロリスト	不正アクセス	テロリストがサプライチェーンに侵入又はサプライチェーンを混乱させようとし、サプライチェーンを通じて情報を入手するり、又はシステムの物理的な無効化と破壊を引き起こすために、不要な機能を埋め込む可能性がある。
敵対者： 産業スパイ／サイバー犯罪者	産業スパイ活動又は知的財産の損失（附属書B、シナリオ2を参照）	産業スパイ又はサイバー犯罪者が、情報の収集又はシステム又はミッションの運用の妨害のために、サプライチェーンに侵入する方法を模索している（例えば、クレジットカード情報を盗むためのHVAC請負業者の悪用）。
敵対者： 組織的サイバー犯罪者	ランサムウェアは重要な生産プロセスの中断を引き起こす	サイバー犯罪組織が、金銭的利益のために身代金の支払いを確実にすることを期待して、ランサムウェア攻撃で組織を標的にしている。脅威源は、事業体、特に製造業者が生産の中断に大きくさらされていることを認識している。
体系的: 法律／規制	法律又は規制の複雑さは、主要なサプライヤが提供する製品及び／又はサービスの可用性にインパクトを与える	競争及び自由市場保護を弱体化させることを目的とした、各国ごとの法律、ポリシー、及びプラクティス（例えば、技術及び知的財産を外国の国内プロバイダに移転するための要件）が原因で生じる脅威[61]を含む、脆弱な腐敗防止法、規制監督の欠如、又は脆弱な知的財産への考慮。

[60] 運用を妨害する例には、サイバーセキュリティサプライチェーンに対する不正な制御を獲得すること、又は正当なアクセスを減少又は拒否するために不正なサービス要求を大量に送ることが含まれる。

[61] 情報通信技術サプライチェーンのリスクマネジメントタスクフォース：脅威評価ワーキンググループ（v3）、2021年8月（Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working Group (v3), August 2021）https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. この報告書は、NIST SP 800-161 の 2015年版を活用している。

脅威源	脅威	例
体系的： 経済的リスク	主要サプライヤのビジネスの失敗は、サプライチェーンの混乱を招く	経済的リスクは、サプライヤの財政的実行可能性に対する脅威、及び主要サプライヤの失敗によるサプライチェーンへの潜在的なインパクトから生じる。経済的リスクをもたらすサプライチェーンに対するその他の脅威には、コスト変動に対する脆弱性、単一供給源のサプライヤへの依存、疑わしいベンダを交換するためのコスト、及び企業規模によりリソース制約が含まれる[62]。
体系的： 供給の中断	レアアース（希土類金属）の生産不足は、半導体の重要な生産材料の供給不足につながる	特に供給源が地理的に単一の場所にある場合には、様々な体系的及び構造的な障害が、製品及び製品コンポーネントの供給不足を引き起こす可能性がある。
環境： 災害	地政学的又は自然災害は、サプライチェーンの混乱につながる	主要なサプライチェーンのインプットの可用性は、地政学的な変動又は自然災害による混乱の影響を受ける。これは特に、サプライヤが共通のフォースパーティサプライヤを共有している場合に該当する。
構造的： ハードウェア障害	不十分なキャパシティ計画は、クラウドプラットフォームの停止につながる	適切なキャパシティ管理策が実施されていないベンダ又はサプライヤのサービスは、予期しないリソース需要の急増が発生した場合に中断する可能性がある。
偶発的： 過失を犯すインサイダー（内部関係者）	設定エラーは、データ漏洩につながる	情報システムにアクセスできる従業員及び請負業者は、機密データの漏洩につながる可能性のあるエラーを起こしやすい。これは特に、トレーニングの不備又はプロセスギャップがエラーの機会を増大させる場合に当てはまる。

[62] 情報通信技術サプライチェーンのリスクマネジメントタスクフォース：脅威評価ワーキンググループ（v3）、2021年8月（Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working Group (v3), August 2021）https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. この報告書は、NIST SP 800-161 の 2015年版を活用している。

政府機関は 3つのレベルすべてにおいて、C-SCRM固有の脅威を識別及び精緻化することができる。表G-2は、脅威の考慮事項の例、及びサプライチェーンのサイバーセキュリティの脅威を各レベルで特徴付けるための様々な方法の例を示している。

表 G-2：サプライチェーンのサイバーセキュリティ脅威に関する考慮事項

レベル	**脅威に関する考慮事項**	方法
レベル 1	• 事業体のビジネス及びミッション • 戦略的サプライヤ関係 • 事業体のサプライチェーンの範囲に関連する地理的な考慮事項	• サプライチェーンのサイバーセキュリティ脅威を識別するための共通の出発点を確立する。 • 重要なシステム及びコンポーネントへの偽造品の混入など、事業体全体の脅威に対抗するための手順を確立する。
レベル 2	• ミッション及びビジネスプロセス • 地理的位置 • サプライヤの種類（例えば、COTS、外部サービスプロバイダ、カスタム） • 事業体全体で使用されている技術	• 事業体のミッション及びビジネスプロセスに固有の脅威情報の追加情報源を識別する。 • 利用可能な政府機関のサイバーセキュリティサプライチェーン情報（例えば、サプライチェーンマップ）を調査することによって識別された場所及びサプライヤに基づいて、潜在的な脅威源を識別する。 • 政府機関のサイバーセキュリティサプライチェーン情報を使用して、特定のミッション及びビジネスプロセスに対して識別された脅威源を詳しく調べる。 • 脅威の敵対者及び自然災害に対抗するための、ミッション固有の準備手順を確立する。
レベル 3	• SDLC	• SDLCフェーズで考慮されることが望ましい脅威の詳細レベルに基づく。 • 個々のSDLCプロセス内に脅威が挿入される可能性に基づいて、脅威源を識別及び精緻化する。

脆弱性

脆弱性とは、脅威源によって悪用又はきっかけとされる可能性がある、情報システム、システムセキュリティ手順、内部統制、又は実装における弱点である。[NIST SP 800-53, Rev. 5]。C-SCRMのコンテキストでは、サプライチェーン、提供されるサービス、システム／コンポーネントの設計、開発、製造、生産、出荷及び受領、納入、運用、及びコンポーネントの耐用年数の終了において、脅威源が悪用可能なあらゆる弱点を指す。この定義は、ID管理やアクセス制御システムなどのセキュリティリスク軽減策及び手法を含む、開発及び統合されている（すなわち、SDLC内の）サービス、システム、及びコンポーネントとサプライチェーンに適用される。FARMプロセスの枠組み化ステップで作成される脆弱性の前提条件は、脅威源によって悪用される又はきっかけとされる可能性がある弱点に関する事業体の長期的な前提条件を取り込む。アセスメントステップ中の特定時点の差異を反映するために、これらはさらに精緻化され、更新される。事業体は、以下に関してサプライチェーンのサイバーセキュリティ脆弱性の長期的な前提条件を作成する場合がある。

- サプライチェーン自体内のエンティティ（例えば、個々のサプライヤ関係）
- サプライチェーンを通じて提供され、事業体の重要なミッション及びビジネスプロセスをサポートする重要なサービス
- サプライチェーンを通じて提供され、SDLC内で使用される（すなわち、開発及び統合される）製品、システム、及びコンポーネント
- SDLCに直接インパクトを与える開発及び運用環境
- システム及びコンポーネントを（論理的又は物理的に）輸送する物流及び納入環境

脆弱性は、3つのレベル（すなわち、事業体、ミッション及びビジネスプロセス、情報システム）で異なる形で明示される。レベル1では、脆弱性は、管理及び運用体制（例えば、ポリシー、ガバナンス、プロセス）、サプライチェーンの条件（例えば、単一のサプライヤからの製品又はサービスの集中）、及び事業体プロセスの特性（例えば、重要なプロセスにおける共通システムの使用）に起因する、事業体全体としての影響の受けやすさとして示される。レベル2では、脆弱性は、ミッション及びビジネスプロセスに特有なものであり、特定のミッション及びビジネスプロセスの運用目的を達成するために特定のシステム、サプライヤから提供されるインプット、又はサービスに依存することなど、その運用体制及び条件に起因する。レベル2の脆弱性は、様々なミッション及びビジネスプロセスで大きく異なる可能性がある。レベル3内では、脆弱性は、提供される製品、SDLC、システムセキュリティ手順、内部管理策、システム実装、システムインプット、又はサプライチェーンを通じて提供されるサービス（例えば、システムコンポーネント又はサービス）における欠陥又は弱点として明示される。

事業体は、脅威源及び事象の特徴、及び事業体が脆弱性を特徴付けるために採用した全体的なアプローチと整合した、サプライチェーンのサイバーセキュリティ脆弱性を特徴付けるアプローチを識別することが望ましい。脆弱性は、単一の脅威源に関連する場合もあれば、又は複数の脅威源（敵対的、構造的、環境的、偶発的）全体に広く適用される場合もある。例えば、ネットワークの単一障害点は、環境的脅威（例えば、災害）又は敵対的脅威（テロリスト）によって引き起こされる中断の影響を受ける可能性がある。附属書Bでは、[NIST SP 800-30, Rev. 1, Appendix B]に基づき、サプライチェーンのサイバーセキュリティ脅威の例を提供している。

3つのレベルすべてが、下位レベルで識別及び文書化され、徐々に詳細になる、脆弱性を特徴付ける事業体のアプローチを決定するのに貢献することが望ましい。表G-3は、様々なレベルでサプライチェーンのサイバーセキュリティ脆弱性を特徴づける考慮事項及び様々な方法の例を提供している。

表 G-3：サプライチェーンのサイバーセキュリティ脆弱性に関する考慮事項

レベル	脆弱性の考慮事項	方法
レベル 1	• 事業体のミッション及びビジネス • 包括的なサプライヤ関係（例えば、システムインテグレータ、COTS、外部サービス） • 事業体のサプライチェーンの範囲に関連する地理的な考慮事項 • エンタープライズ及びセキュリティアーキテクチャ • 重要度	• 特に脆弱なエンティティ、場所、又は事業体を識別するために、サプライチェーンマップを含む政府機関のサイバーセキュリティサプライチェーン情報を調査する。 • 潜在的なサプライチェーンのサイバーセキュリティ脆弱性の影響の受けやすさについて、政府機関のミッションを分析する。 •潜在的なサプライチェーンのサイバーセキュリティ脆弱性の影響の受けやすさについて、サードパーティプロバイダ及びとサプライヤとの関係及び相互依存関係を調査する。 • より強固なサプライチェーンのサイバーセキュリティの考慮事項を必要とする弱点の領域を識別するために、エンタープライズアーキテクチャ及び重要度をレビューする。
レベル 2	• ミッション及びビジネスプロセス • 地理的位置 • ミッション及びプロセスレベルのサプライヤ依存関係（例えば、外部委託又は請負サービス） • 使用される技術	• 特定のミッション及びビジネスプロセス、及び該当する脅威及びサプライチェーン情報に基づいて、レベル1から分析を精緻化する。 • 該当する場合は、脆弱性の特徴付け、分類化、及びスコア付けに、共通脆弱性識別子（Common Vulnerabilities and Exposures）（CVE）及び共通脆弱性評価システム（Common Vulnerability Scoring System）（CVSS）を含む、脆弱性情報データベース（National Vulnerability Database）（NVD）[63]、又はその他の受容可能な方法論を使用する。 • 改善のための脆弱性の優先順位付けに、スコアリングガイダンスの使用を検討する。
レベル 3	• 個々の技術、ソリューション、及びサービス • システムコンポーネント又はサービスなどのサプライチェーンのSDLCインプット	• 関連するレベル2のミッション及びビジネスプロセスからのインプットに基づき、分析を精緻化する。 • 脆弱性を特徴付け、定義するため、利用可能な場合はCVEを使用する。 • 弱点を識別する。

[63] https://nvd.nist.gov/ を参照のこと。

インパクト及び損害

インパクトとは、情報又は情報システムの機密性、完全性、又は可用性の喪失が、事業体の運営、事業体の資産、個人、他の事業体、又は国家（米国の国家安全保障上の利益を含む）に及ぼす影響のことである[NIST SP 800-53, Rev. 5]。枠組み化ステップで推定されるインパクトは、様々なサイバーセキュリティ事象が事業体の主要なプロセスに及ぼす可能性がある影響に関する事業体の長期的な前提条件を表す。これらの前提条件は、インパクトの範囲、期間、又は程度を変える可能性がある特定時点の関連情報（例えば、市場の状況）が、分析に適切に反映されることを確実にするために、アセスメントステップの一部として更新及び精緻化される。

可能な場合には、事業体は、事業体リスクマネジメント活動の一環として、結果及びインパクトについて事業体が策定した前提条件を継承することが望ましい。例えば、このような活動の1つは、事業体の継続性及び緊急時への備えの責任の一環として、ミッション上重要なプロセス及びミッションイネーブリングプロセスを決定又は再検証するために、ビジネスインパクト分析（BIA）を実行することである。ただし、これらの前提条件は、まだ存在していない場合には、策定する必要がある場合がある。事業体は、事業体の資産に対する様々な種類のサイバーセキュリティ事象のインパクト又は損害（例えば、漏洩、中断、破壊、改ざん）に関する事業体の継続的な前提条件を把握するインパクト又は損害ライブラリを維持することができる。これらのライブラリは、インパクト及び損害を、個々のインパクトの種類（例えば、運用、環境、個人の安全、評判、規制／法的罰金及び罰則、ITの復旧／交換、重要インフラ分野への直接的な金銭被害）に分類することができる。

C-SCRMの場合、事業体は、サプライヤ提供製品又はサービスの可用性、機密性、及び完全性が、事業体の運営、資産、及び個人に及ぼす役割を反映するために、結果及びインパクトの前提条件を精緻化及び更新することが望ましい。例えば、重要度によっては、主要なサプライヤが提供するインプット又はサービスの損失は、事業体の運用キャパシティを低下させたり、運用を完全に阻害したりする可能性がある。本出版物において、インパクト又は損害は、事業体の主要な目的に関連しており、サプライチェーンを横断する製品又はサービス、あるいはサプライチェーン自体から生じる。

C-SCRMの結果及びインパクトは、リスクマネジメント階層の3つのレベルすべてで異なった形で現れる。インパクトの決定には、トップダウンとボトムダウンを組み合わせたアプローチが必要である。表G-4は、事業体の様々なレベルでの結果及びインパクトがどのように特徴づけられるかの例を示している。

表 G-4：サプライチェーンのサイバーセキュリティの結果及びインパクトの考慮事項

レベル	インパクトの考慮事項	方法
レベル 1	• 一般的な事業体レベルのインパクトの前提条件 • サプライヤの重要度（例えば、包括的なサプライヤ関係）	• サプライチェーン内の個々のエンティティに対する曝露（エクスポージャー）の大きさを調査する。 • サプライチェーンに対する、及びサプライチェーンを通じたサイバーセキュリティ事象に起因する、事業体の主要な機能に対するレベル1のインパクトの総計を決定するために、レベル2分析を精緻化する。

レベル	インパクトの考慮事項	方法
レベル 2	• 事業体の主要な機能におけるプロセスの役割 • ミッション／プロセス（インプット及びサービス）に対するサプライヤの重要度	サイバーセキュリティ事象の種類ごとに、以下を行う。 • サプライチェーンに対する、及びサプライチェーンを通じたサイバーセキュリティ事象からの運用レベルのインパクトによるミッション及びビジネスプロセスのインパクトの総計を決定するために、レベル3分析を精緻化する。 • 個々のサプライヤエンティティに影響を及ぼす事象によるビジネス／ミッションレベルのインパクトを識別するために、サプライヤネットワークを調査する。
レベル 3	• 上流及び下流のレベル2プロセスの重要度 • システムの重要度 • システム運用（システムコンポーネント及びサービス）に対するサプライヤの重要度	• レベル1及びレベル2の主要なプロセスに対するシステムの集約された重要度を調査する。 • システムの全体の機能に対する、供給されたシステムコンポーネント又はサービスの重要度を調査する。 • 重要なシステムインプット又はサービスの可用性を阻害する可能性がある個々のエンティティを識別するために、サプライヤネットワークを調査する。

事業体は、結果とインパクトのコンテキスト化に役立つ様々な情報源に目を向けることが望ましい。過去のデータは優先的であり、政府機関、類似する同業の事業体、サプライヤ組織、又は該当する業界調査の過去のデータをレビューすることによって収集することができる。過去のデータにギャップが存在する場合、事業体は、事業体全体で適切な個人の暗黙知を活用する専門家意見聴取手順（例えば、校正推定トレーニング）の使用を検討することが望ましい。事業体は、適切な立場の専門家（例えば、技術又はミッション及び資産のビジネスオーナー）にインタビューすることで、その事業体固有の前提条件及び依存関係を反映するように、インパクトの前提条件をテーラリングすることができる。[NISTIR 8286]は、リスクを分析するために、どのように異なる定量的及び定性的方法論を使用することができるかについて、徹底した議論を提供している。

以下は、サイバーセキュリティサプライチェーンの結果とインパクトの例である。

- マレーシアで発生した地震によって、汎用DRAM（ダイナミックランダムアクセスメモリ）の量が世界の供給量の60%に減少し、ハードウェアの保守及び新規設計での不足が発生する。
- 偽造部品を誤って調達した結果、コンポーネントの早期故障をもたらし、事業体のミッションのパフォーマンスを与える。
- 主要なクラウドサービスプロバイダでの中断が発生し、150万ドル～1500万ドルの運用ダウンタイム損失が発生する。

起こりやすさ

情報セキュリティリスク分析では、起こりやすさとは、ある脅威がある脆弱性を悪用することができる確率の主観的な分析に基づく、重み付けされた因子である [CNSSI 4009]。一般的な起こりやすさの前提条件は、事業体の事業体リスクマネジメントプロセスから継承され、C-SCRM固有の関連事項を説明するために精緻化されることが望ましい。ただし、一般的な前提条件は、まだ存在していない場合には策定する必要がある場合がある。枠組み化ステップの起こりやすさ分析では、様々な有害なサイバーセキュリティ事象の相対的な起こりやすさに関する事業体の長期的な前提条件を設定する。起こりやすさは、特定時点の状態（すなわち、内部及び外部）に基づく超短期的な変動の影響を受けるため、アセスメントステップの一環として更新及び精緻化されなければならない。

敵対的なケースでは、インテリジェンストレンドデータ、過去のデータ、及び1）敵対者の意図、2）敵対者のケイパビリティ（能力）、及び 3）敵対者の標的に関する専門家の洞察を用いて、起こりやすさを決定する場合がある。敵対的ではないケース（例えば、構造的、環境的、偶発的）では、専門家の洞察と過去のデータを用いて起こりやすさの決定を行う。利用可能な場合、過去のデータは、サプライチェーン全体でどのサイバーセキュリティリスクが発生する可能性が高いかについての不確実性をさらに削減するのに役立つ可能性がある。組織は、様々なサイバー事象を経験する確率を概算するために、過去のインシデントトラッカーなどの内部ソース又はISACなどの外部ソースを参照して過去のデータを探し出す場合がある。起こりやすさ分析では、結果及びインパクトと同じ専門家意見聴取手順の多くを活用することができる。結果及びインパクトと同様に、起こりやすさの決定は定性的又は定量的な形式に依存し、同様の技術を利用する場合がある。意思決定者に対して起こりやすさが適切にコンテキスト化されることを確実にするために、事業体は、サプライチェーンに影響を与えるサイバーセキュリティ事象について、期間を定めた起こりやすさの推定を行うことが望ましい（例えば、ある1年以内の起こりやすさ）。

起こりやすさ分析は、3つのレベルで現れ方が異なる。表G-5は、各レベルの固有の考慮事項及び方法の一部を示している。

表 G-5：サプライチェーンサイバーセキュリティの起こりやすさの考慮事項

レベル	起こりやすさの考慮事項	方法
レベル 1	• 事業体の一般的な脅威及び起こりやすさの前提条件 • レベル2及びレベル3の起こりやすさの所見 • 脅威源との接触の機会を変えるサプライヤとの全体的なエンゲージメントモデル	• 事業体の標的価値を増加させる可能性がある、国家の重要なインフラストラクチャへの影響を分析する。 • 脅威源との接触への総曝露（エクスポージャー）を決定するためにレベル2及びレベル3の分析を精緻化する。

レベル	起こりやすさの考慮事項	方法
レベル 2	• ミッション／プロセスレベルの脅威及び起こりやすさの前提条件 • サプライヤとのミッション／プロセスレベルのエンゲージメントモデル（例えば、相互作用する資産の重要度） • レベル3の関連システムの所見	• 脅威源がサプライチェーンを通じてプロセス又は資産に接触する機会をもたらすミッション及びビジネスプロセスレベルの状態を評価する。 • ミッション及びビジネスプロセスに依存する主要システムが直面しているサプライチェーン脅威状態の総計を評価する。
レベル 3	• 事業体システムの脅威及び起こりやすさの前提条件 • サプライヤ及びシステムの標的価値 • 場所及び運用条件 • サプライヤ及びシステムのセキュリティポリシー、プロセス、及び管理策 • サプライヤのシステムとの接触の性質と度合い（インプット、サービス）	• サプライチェーンを通じてSDLCに入ってくるシステムインプット、及び脅威源に遭遇する可能性を変えるシステムインプットの性質を分析する。 • 潜在的な敵対者にとっての標的価値を変える、レベル1及びレベル2のプロセスにおけるシステムの役割を評価する。 • システムが脅威源の影響を受ける可能性を高める可能性があるサプライチェーンの特性（例えば、サプライヤの所在地）を分析する。

政府機関は、政府機関のリスクマネジメントプロセスで使用される全体的なアプローチと整合する、サプライチェーンのサイバーセキュリティ侵害の起こりやすさを判断するときに使用するアプローチを識別することが望ましい。政府機関は、特に高いインパクトリスク又は重大なインパクトリスクが関与する場合は、最終的なリスク曝露（エクスポージャー）の表の作成につながるリスク分析の前提条件をすべて完全に文書化するために、適切な手順が整備されていることを確実にすることが望ましい。前提条件の可視性は、意思決定者が行動を起こせるようにする上で重要となる可能性がある。

リスクマネジメントプロセスの制約条件

タスク 1-2：事業体内のリスクアセスメント、リスク対応、及びリスク監視活動の実施に対する制約条件[64]を識別する。

補足ガイダンス

サイバーセキュリティサプライチェーンが政府機関のリスクマネジメントプロセスに統合されることを確実にするために、以下の2種類の制約条件を識別する。

1. 政府機関の制約条件
2. サプライチェーン固有の制約条件

[64] リスクマネジメントのコンテキストでの制約条件の記述については、[NIST SP 800-39]、3.1 節、タスク1-2を参照のこと。

政府機関の制約条件は、レベル1ではサイバーセキュリティサプライチェーンポリシー、レベル2ではミッション要件、及びレベル3ではシステム固有の要件を枠組み化するための総合的なインプットの役割を果たす。表G-6は、特定の政府機関及びサイバーセキュリティサプライチェーンの制約条件を示している。C-SCRMポリシー及びC-SCRM要件などのサプライチェーンの制約条件は、存在しない場合には策定する必要がある場合がある。

表 G-6：サプライチェーンの制約条件

レベル	政府機関の制約条件	サプライチェーンの制約条件
レベル 1	• 事業体のポリシー、戦略、及びガバナンス • 適用される法律及び規制 • ミッション及びビジネスプロセス • 事業体のプロセス（例えば、セキュリティ、品質） • リソースの制限	• 既存の政府機関ポリシー、戦略、及びガバナンス、適用される法律及び規制、ミッション及びビジネスプロセス、及び事業体のプロセスに基づく事業体のC-SCRMポリシー • 取得に関する規制及びポリシー • 使用可能、必須、又は制約のある供給源又は製品
レベル 2	• ミッション及びビジネスプロセス • プロセスの重要度 • エンタープライズアーキテクチャ • ミッションレベルのセキュリティポリシー	• ミッション及びビジネスプロセス、及びにエンタープライズアーキテクチャに組み込まれるC-SCRMミッション及びビジネス要件 • サプライヤのサービス契約、製品保証、及び賠償責任契約
レベル 3	• 機能要件 • セキュリティ要件	• 製品及び運用レベルのC-SCRMケイパビリティ（能力） • サプライヤ提供のシステムコンポーネントの保証及びサービス合意

制約条件を明確にするための主な手法の1つは、ポリシーステートメント又は指令によるものである。事業体のC-SCRMポリシーは、C-SCRM活動を指示するための重要な手段である。このポリシーは、適用される法律及び規制によって推進され、取得及び調達、情報セキュリティ、品質、並びにサプライチェーン及び物流を含む事業体のポリシーをサポートすることが望ましい。C-SCRMポリシーは、政府機関全体の戦略計画、中レベルのミッション及びビジネスプロセス戦略、及び内外の顧客によって明確にされた目標、目的、及び要件に対処することが望ましい。C-SCRMポリシーはまた、C-SCRMと政府機関のリスクマネジメントプロセス及びSDLCとの統合点も定義することが望ましい。

C-SCRMポリシーは、政府機関のC-SCRMチームのC-SCRM関連の役割及び責任、及びこれらの役割間の相互依存関係又は相互作用を定義することが望ましい。C-SCRM関連の役割は、サプライチェーンのサイバーセキュリティ脅威インテリジェンスの収集、リスクアセスメントの実施、リスクに基づく軽減策の識別及び実装、及び監視プロセスの実行の責任を明確にする。役割を識別及び検証することは、C-SCRM計画の実装に必要な作業量を規定するのに役立つ。C-SCRM関連の役割の例を、以下に示す。

- システム設計の完了段階でサイバー製品を規定及び選択するエンジニアリング上の意思決定に対して、サプライチェーン全体のサイバーセキュリティリスクに関する包括的なガイダンスを提供するC-SCRM PMO。
- 欠陥のあるハードウェアの識別及び交換の責任を負う調達担当者及び保守エンジニア。
- システムコンポーネントが取得事業体に受容可能であることを検証する、納入事業体及び受け入れエンジニア。
- システムの保守及びアップグレードの責任を負うシステムインテグレータ。そのスタッフは取得者の施設に常駐し、システムインテグレータの開発インフラ及び取得者の運用インフラを使用する。
- 情報システムのセキュリティ上の懸念がSDLC全体を通じて適切に識別及び対処されていることを確実にする責任を負うシステムセキュリティエンジニア／システムエンジニア。
- サイバーシステム、コンポーネント、及びサービスのエンドユーザ。

C-SCRM要件は、C-SCRMポリシー、ミッション及びビジネスプロセス、レベル2におけるその重要度、及びレベル3における既知の機能及びセキュリティ要件によって導かれることが望ましい。

リスク選好度及び許容度

タスク 1-3：事業体全体でリスク選好度及び許容度を識別する。

補足ガイダンス

広義のリスク選好度とは、事業体が価値を追求する上で受容する意思があるリスクの種類と量を表す [NISTIR 8286]。逆に、リスク許容度とは、事業体又はステークホルダーが、その目的を達成するために、法律又は規制の要件の影響を受ける可能性があることを考慮した上で、リスク対応後に残るリスクを負う用意があることを表す [NISTIR 8286]。この定義はCOSOから引用されたものであり、COSOは、リスク許容度とは、特定の目的の達成に対する変動の許容可能なレベルである、と記述している。多くの場合、リスク許容度は、関連する目的の測定に使用される単位と同じ単位で測定するのが最善である [COSO 2011]。リスクマネジメントフレームワークを確立する際には、事業体はリスクのしきい値を設定するリスク選好度及びリスク許容度のステートメントを確立することが推奨される。その後、適用可能であれば、C-SCRMは事業体のリスクマネジメントプロセスからのリスク選好度及び許容度ステートメントに整合させることが望ましい。リスク選好度及びリスク許容度は、確立されたら、時間の経過に伴い監視及び変更されることが望ましい。C-SCRMについては、C-SCRM領域での決定に情報を提供するために、これらのステートメントをコンテキスト化することが望ましい。事業体全体のC-SCRMの責任を負う担当者は、C-SCRM関連のリスク選好度及びリスク許容度ステートメントの策定において、事業体のリーダーと協力し、サポートすることが望ましい。これは、事業体のリスク戦略から提供された基準に従って行われることが望ましい（例えば、ERMのリスク分類に基づく）。

リスク選好度及び許容度のステートメントは、3つのレベルにわたるC-SCRMに関する意思決定に大きく影響する。事業体によっては、より広範な事業体リスクマネジメント活動の一環として、リスク選好度及びリスク許容度を定義する場合がある。リスク選好度が明確に定義されていない事業体では、レベル1のステークホルダーが事業体のリーダーと協力して、C-SCRMプログラムの権限の範囲内で、事業体のリスク選好度を定義及び明確にすることが望ましい。複数の組織を持つ事業体は、特定の組織、及びミッション及びビジネスプロセスに合わせてリスク選好度ステートメントをテーラリングすることができる。一般に、レベル1のリスク選好度は、事業体がその価値目的を達成できるようにするために設定される場合がある（例えば、運用コストの5%削減をサポートするサプライヤリスクの高い選好度）。レベル2及びレベル3では、組織のリスク選好度ステートメ

ントは、リスク許容度ステートメントを通じて運用される。例えば、サプライチェーンのサイバーセキュリティリスクに対する選好度が低い組織は、レベル2及びレベル3の意思決定者が戦略的価値を追求する際に、これらの意思決定者による抑制及び制御を必要とするリスク許容度ステートメントを発行する可能性がある（例えば、国家安全保障関連ミッションをサポートする組織の厳密な生産目標に基づいて作成された許容度ステートメント）。

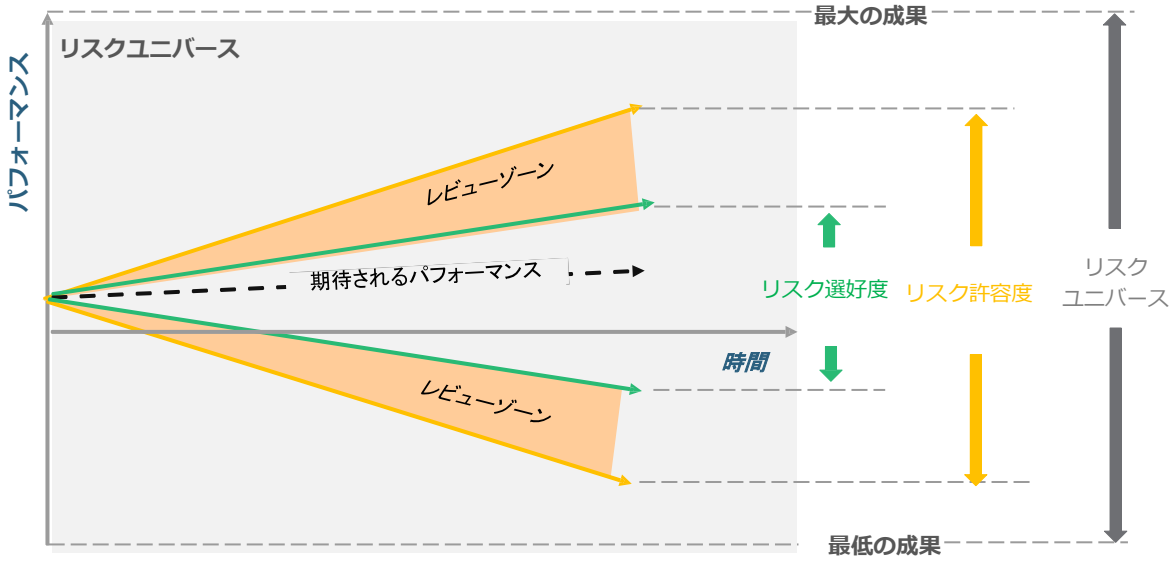

図 G-4：リスク選好度及びリスク許容度

リスク選好度及びリスク許容度は共に、組織の戦略的目的に対するパフォーマンスに基づく期待及び許容可能な境界を提供する。図G-4は、組織の運用上の意思決定者のためのガイドラインとして、リスク選好度及びリスク許容度をどのように使用することができるかを示している。リスク許容度は、組織の戦略的目的を達成するためのある程度の柔軟性を提供するために、リスク選好度を超える境界で設定される。しかし、運用上の意思決定者は、通常の状態ではリスク選好度の範囲内にとどまるように努力し、絶対に必要な場合にのみ境界を超えるようにすることが望ましい（例えば、重要な機会を生かすため、非常に不利な状況を避ける）。リスク選好度の境界の外に位置する「レビューゾーン」で観察されたパフォーマンスの期間は、運用上の意思決定及び定義されたリスク選好度及び許容度のステートメントのレビューをもたらすことが望ましい。このレビューは、組織のリスク選好度が、組織内外の運用状況を考慮した上で、引き続き適切及び適用可能であることを確実にするために重要である。例えば、世界的なパンデミックの最中に事業を行っている組織は、供給不足を回避するために、代替サプライヤを通じて付加的レベルのサイバーリスクの曝露（エクスポージャー）を引き受ける必要があると考える可能性がある。以下の図G-5は、リスク選好度及びリスク許容度のレビュープロセスを示している。

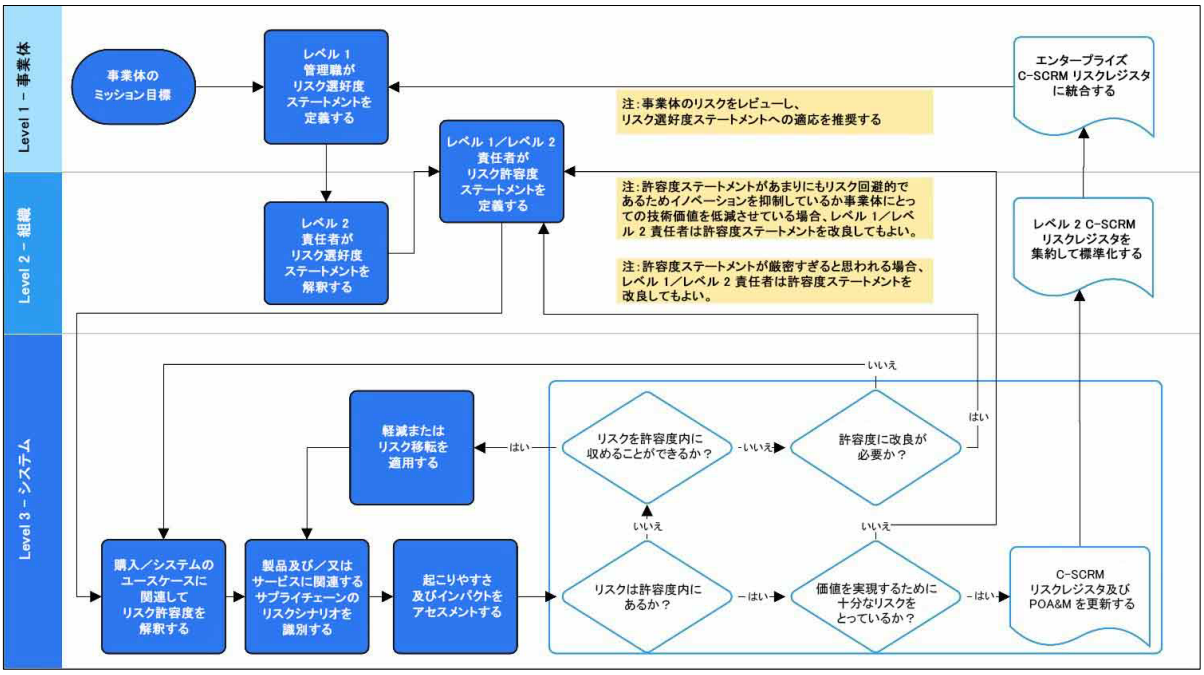

図 G-5：リスク選好度及びリスク許容度のレビュープロセス

場合によっては、組織のリーダーは、意思決定者による過剰なリスク回避行動（すなわち、選好度を下回るパフォーマンス）又はリスク追及行動（すなわち、選好度を上回るパフォーマンス）を避けるために、ガイダンスのバランスを再調整する必要があると考える場合がある。

表G-7は、事業体内でリスクを枠組み化するために、リスク選好度及びリスク許容度のステートメントがどのように連携して機能するかの追加の例を示している。

表 G-7：サプライチェーンのリスク選好度及びリスク許容度

事業体の制約条件	サプライチェーンの制約条件
市場目的に関するリスクに対する**選好度が低く**、24時間365日の稼働時間を必要とする。	契約サービス内容合意書（SLA）を10%超過する、システム中断を引き起こすサービスプロバイダの停止時間に対する**許容度が低い**（すなわち、5%以下の確率）。
国家安全保障のミッションを有する顧客に対して、99%を上回る納期どおりの製品の納入が必要な生産目的に関連するリスクに対する**選好度が低い**。	生産レベルが軍需製品の目標しきい値の99%を下回る原因となるサプライチェーンの中断に対する**許容度がほぼゼロ**（すなわち、5%以下の確率）である。
セキュリティプロセスの99%の有効性を必要とする、国家安全保障の目的に関連するリスクに対する**選好度が低い**。	国家機密情報を含むシステムにおいて、認可されている枠を10%超過する不適切な請負業者アクセスに対する**許容度が低い**（すなわち、請負業者のアクセス認可の1%以下）。

事業体の制約条件	サプライチェーンの制約条件
99.5%の可用性を必要とするミッション上重要ではない領域の運用目的に関連するリスクに対する**選好度が中程度である**。	目標復旧時間を10%超過する、重要ではないシステムの中断を引き起こすシステムコンポーネントの障害に対する**許容度は中程度である**（すなわち、15%以下の確率）。

リスクベースの意思決定を行う際にリーダーが適切な情報を有していることを確実にするために、事業体は、定義されたリスク選好度及びリスク許容度のステートメントに対するパフォーマンスを測定するための指標（例えば、重要業績評価指標 [KPI]、重要リスク指標 [KRI]）を確立することが望ましい。測定のための対応するデータソースの識別は、リスク選好度及びリスク許容度のステートメントを設定及び精緻化するために事業体で定義されたプロセスにおいて、重要な役割を果たすことが望ましい。リスク選好度及びリスク許容度は、事業体によって動的なものとして扱われることが望ましい。これには、事業体にインパクトを与える内部（例えば、新しいリーダー、戦略）及び外部（例えば、市場、環境）の変化に基づく、定期的な更新及び改訂が必要である。

事業体は、リスク選好度及びリスク許容度の全体的なレベルを確立、運用、維持する際に、サプライチェーンのサイバーセキュリティの脅威、脆弱性、制約条件、及び重要度を考慮することが望ましい[65]。

優先順位とトレードオフ

タスク 1-4：リスクの管理において事業体が考慮する優先順位とトレードオフを識別する。

補足ガイダンス

優先順位とトレードオフは、事業体のリスク選好度及び許容度のステートメントと密接に関連しており、事業体がその目的を追求する上で受容可能及び許容可能なリスクの量を伝えている。優先順位は、長期的な戦略的目的又はリスク決定の計算を変える短期的な戦略的要請の形を取る。優先順位とトレードオフから、C-SCRMは、代替案の評価及びリスク対応の決定などの対応ステップの活動に必要な、重要な戦略的コンテキストを受け取る。優先順位及びトレードオフを識別する一環として、事業体は、リスク選好度、リスク許容度、サプライチェーンのサイバーセキュリティ脅威、脆弱性、制約事項、及び重要度を考慮することが望ましい。

優先順位とトレードオフの考慮事項は、3つのレベルで現れ方が異なる。レベル1では、優先順位とトレードオフの考慮事項は、信頼性と安定性を維持したいという願望から、新しいサプライヤのコスト優位性を犠牲にして、確立された地域における既存のサプライヤとの関係を優先する可能性がある。レベル2では、優先順位とトレードオフの考慮事項は、より大規模なセキュリティプラクティスの標準化を優先して、製品チームを網羅する集中型のC-SCRMガバナンスモデルを優先する可能性がある。レベル3では、優先順位とトレードオフは、サプライチェーンに対する環境的又は地政学的リスクを回避するために、特定の地域で生産されるシステムコンポーネント／サブコンポーネントを優先する可能性がある。

[65] 連邦政府部署及び政府機関のガバナンス構造は大きく異なる（[NIST SP 800-100、2.2.2 節]を参照のこと）。 ガバナンス構造に関係なく、個々の政府機関のリスク決定は、政府機関及び下部組織に適用されることが望ましいが、その逆はない。

アウトプット及び事後条件

[NIST SP 800-39] の範囲内では、リスク枠組み化ステップのアウトプットは、事業体が長期にわたってどのようにリスクをリスクアセスメント、対応、及び監視するかを識別するリスクマネジメント戦略である。この戦略は、識別されたC-SCRM考慮事項が明確に含まれ、その結果、政府機関全体でC-SCRM固有のプロセスが確立されることが望ましい。これらのプロセスは、以下の3つのうちいずれかの方法で文書化することが望ましい。

1. 既存の政府機関文書に統合する。
2. C-SCRMを扱う一連の文書に記載する。
3. 政府機関のニーズと運用に基づいて、個別の文書及び統合された文書を組み合わせて使用する。

アウトプットがどのように文書化されているかに関わらず、リスク枠組み化ステップのアウトプットとして、以下の情報が提供されることが望ましい。

- C-SCRMポリシー
- 優先順位付けされたミッション及びビジネスプロセスと [FIPS 199] のインパクトを含む重要度
- サプライチェーンのサイバーセキュリティリスクアセスメントの方法論及びガイダンス
- サプライチェーンのサイバーセキュリティリスク対応のガイダンス
- サプライチェーンのサイバーセキュリティリスク監視のガイダンス
- C-SCRMのミッション及びビジネス要件
- C-SCRM考慮事項を統合した、改訂されたミッション及びビジネスプロセス並びにエンタープライズアーキテクチャ
- 運用レベルのC-SCRM要件
- 取得のセキュリティガイダンス／要件

リスク枠組み化ステップからのアウトプットは、前提条件がサプライチェーン全体のサイバーセキュリティリスクを効果的に管理することを可能にし、リスクアセスメント、リスク対応、及びリスク監視ステップのインプットとして機能する。

アセスメント

インプット及び前提条件

アセスメントは、前提条件、確立された方法論、及び収集されたデータを使用してリスクアセスメントを実施するステップである。サプライチェーンのサイバーセキュリティ侵害の起こりやすさ及びインパクトを評価するために、多数のインプット（重要度、リスク選好度及び許容度、脅威、脆弱性分析、ステークホルダーの知識、ポリシー、制約条件、及び要件を含む）を組み合わせて分析する。アセスメントステップの活動は、短期的な変動及び変化を考慮するために、事業体の長期的なリスク枠組み化の前提条件を更新するために使用される。

サプライチェーンのサイバーセキュリティリスクアセスメントは、事業体全体のリスクアセスメントプロセスに統合することが望ましい。C-SCRMリスクアセスメントの結果は、各リスクマネジメントフレームワークのレベルに関連する潜在的又は実際のサプライチェーン全体のサイバーセキュリティリスクを伝達するために、必要に応じて使用及び集約されることが望ましい。図G-6は、3つのレベルに沿ったインプットとアウトプットを持つアセスメントステップを示している。

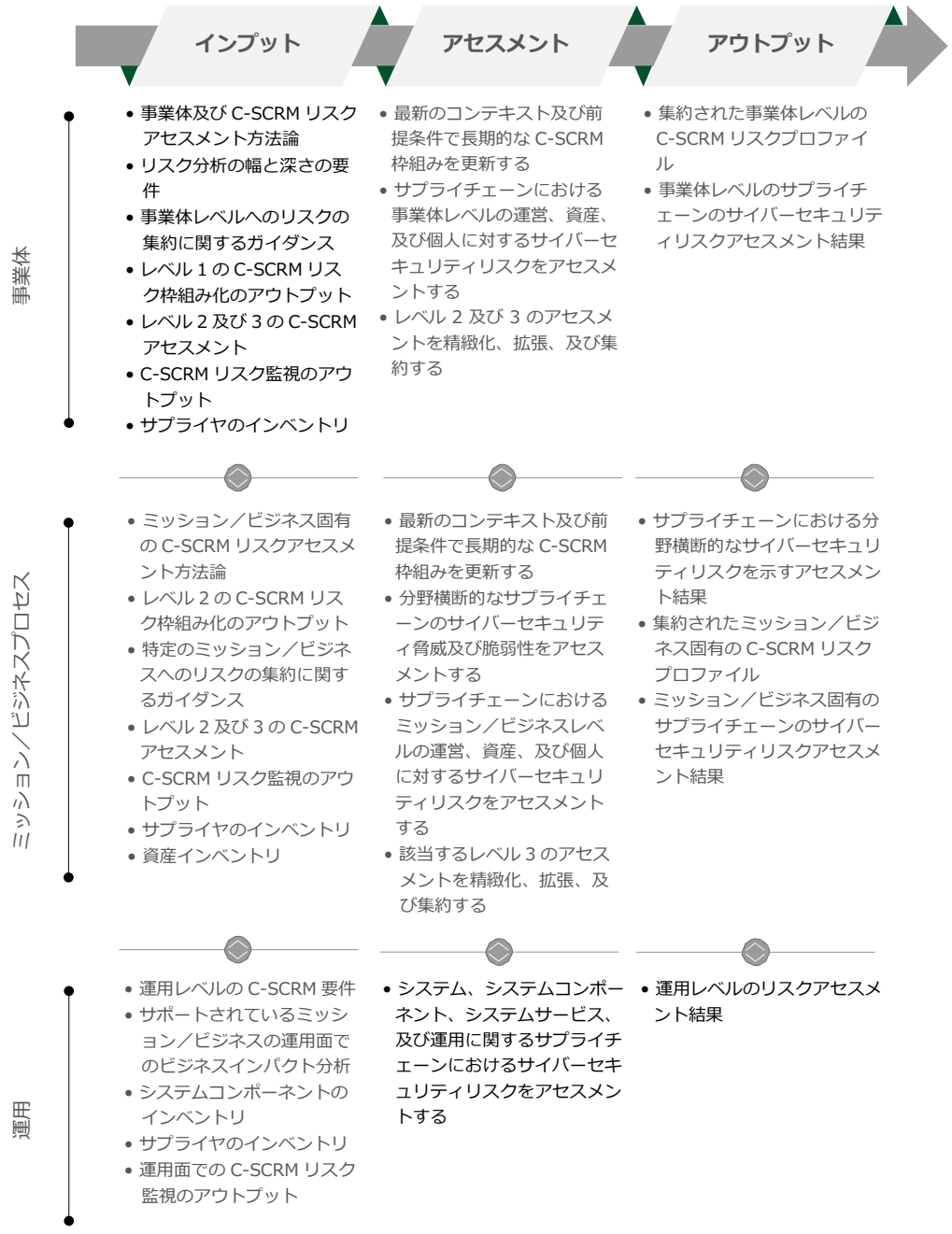

図 G-6：アセスメントステップにおけるC-SCRM[66]

重要度分析、脆弱性分析、及び脅威分析は、サプライチェーンのリスクアセスメントプロセスに不可欠である。活動の順序は、アセスメントの範囲が関連する重要なミッション及びビジネスプロセスを最小限に含むことを確実にし、これらのミッション及びビジネスプロセスに対するサプライチェーン要素の関連性及びインパクトを理解するために、重要度分析の更新から始まる。図G-5に示すように、脆弱性分析及び脅威分析は、その後任意の順序で実行することができるが、どの脆弱性が特定の脅威によってより悪用されやすいかを理解するためにすべての該当する脅威及び脆弱性が識別されていること、及び該当する場合には、識別された脆弱性及び脅威を1つ以上のミッション及びビジネスプロセス又はサプライチェーン要素に関連付けることを確実にするために、繰り返し実行することが望ましい。実行可能な脅威及び潜在的又は実際の脆弱性がアセスメントされたら、この情報は、インパクトを理解する上で重要なステップである悪用可能性の起こりやすさの評価に使用される。

[66] リスクマネジメントプロセスの詳細は附属書Cに記載されている。

これは重要度分析、脆弱性分析、及び脅威分析の統合ポイントであり、情報に基づいた正当なリスク決定をサポートするために、インパクトをさらに明確にし、コンテキスト化するのに役立つ。

活動

重要度分析

タスク 2-0：C-SCRM活動の範囲（及びリソースのニーズ）をミッション成功のために最も重要なものに絞り込むために、ミッション及びビジネスプロセス、システム、及びシステムコンポーネントの重要度分析を更新する。

補足ガイダンス

重要度分析には、事業体及び該当するサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダ、並びに関連する非システムサービス及び製品を含めることが望ましい。重要度分析は、各エンティティがミッションの優先順位に与える直接的なインパクトをアセスメントする。SDLCは、セキュリティ考慮事項がシステム／コンポーネントに組み込まれるか、又はシステム／コンポーネントの作成後に追加されるかを定義するため、サプライチェーンには、該当するシステム、サービス、及びコンポーネントのSDLCが含まれる。

事業体は、[FIPS 199] システムを含む、リスクマネジメントプロセスの枠組み化ステップで確立された重要度を更新及びテーラリングすることが望ましい。低インパクトシステムの場合、事業体は、これらのシステムと中インパクトシステム又は高インパクトシステムとの間に存在する可能性がある相互依存関係に関する重要度を最小限にアセスメントすることが望ましい。システムが事業体全体で広く利用されている場合、事業体は、低インパクトシステムにおけるコンポーネント障害又は侵害の包括的な影響を判断することが望ましい。

重要度の更新及びテーラリングに加えて、アセスメントステップでの重要度分析の実行には、以下が含まれる可能性がある。

- システム又はネットワークアーキテクチャを考慮して、どのコンポーネントに強化が必要となる可能性があるかを理解するために、依存関係の分析及びアセスメントを精緻化する。
- 重要システム／コンポーネントが製造又は開発される場所、物理的及び論理的納入経路、情報フロー、これらのコンポーネントに関連する情報の流れ及び金融取引、及びこれらのコンポーネントのサプライチェーンに関する知見を提供できるその他の利用可能な情報など、政府機関が重要システム／コンポーネントに関して有する既存の情報を取得及びレビューする[67]。
- 重要なサプライチェーンパス及び状況における変化を識別するために、サプライチェーン、履歴データ、及びSDLCに関する情報を更新する。

[67] この情報は、政府機関若しくは個々のITプロジェクト又はシステムのサプライチェーンマップから入手できる可能性がある。サプライチェーンマップは、サプライチェーンを通じた上流及び下流における商品、情報、プロセス、及び金銭の物理的及び論理的なフローを含む、サプライチェーンの説明又は描写である。サプライチェーンのエンティティ、場所、納入経路、又は取引が含まれる場合がある。

更新された重要度分析の結果は、事業体の重要なプロセス、システム、及びシステムコンポーネントを絞り込んで優先順位を付けたリストであり、サプライチェーン内の対応する依存関係の精緻な理解である。事業体はタスク1-1の重要度プロセスを使用して、重要度分析を更新することができる。

アセスメントステップではより多くの情報を利用することができるため、事業体は、重要度分析の範囲を絞り込み、粒度を上げることができる。重要なプロセス及び関連するシステム／コンポーネントを識別し、それらに重要度レベルを割り当てるときには、以下を考慮する。

- 機能分割は、プロセス及び関連する重要コンポーネントを識別し、防御機能をサポートするための効果的な手法である。
- 災害時復旧及び運用継続計画では、重要システム及びシステムコンポーネントを定義することが多く、これは重要度の割り当てに役立つ。
- 依存関係分析は、他の重要なプロセスが依存するプロセスを識別するために使用される（例えば、ソフトウェアパッチの受け入れで使用される電子署名などの防御機能）。
- すべてのアクセスポイントの識別は、重要な機能及びコンポーネントへの直接アクセスを識別し、制限するのに役立つ（例えば、最小特権の実装）。
- バリューチェーン分析により、サービス及び製品のインプット、プロセス行為者、アウトプット、並びに顧客を理解することができる。
- 悪意のある改ざんやその他の種類のサプライチェーン侵害は、SDLC全体を通じて発生する可能性がある。

結果として得られる重要なプロセス及びサプライチェーンの依存関係のリストは、図D-4に示すように、初期のC-SCRMリスクを決定する際の脆弱性分析及び脅威分析の指針及び情報を提供するために使用される。その後、リスクを受容可能なレベルまで低減するために、サプライチェーンの対策及び軽減策を選択して実装することができる。

重要度分析は繰り返し実行され、SDLC内の任意の時点で、レベルごとに同時に実行することができる。最初の繰り返しでは、ミッション及びビジネスプロセスに直接インパクトを与える重要なプロセスとシステム又はコンポーネントが識別される可能性がある。それ以降の繰り返しでは、他の各レベルで定義される重要度分析、脅威分析、脆弱性分析、及び軽減戦略からの情報が含まれる。各繰り返しにより重要度分析の結果が精緻化され、その結果、防御機能が追加される。重要度分析の結果を確立し、維持するためには、複数回の繰り返しが必要となることがある。事業体は、重要度分析の結果を文書化又は記録し、最低でも年1回はこのアセスメントをレビュー及び更新することが望ましい。

脅威及び脆弱性の識別

タスク 2-1：事業体の情報システム及びシステムが稼働する環境に対する脅威及び脆弱性を識別する。

補足ガイダンス

[NIST SP 800-39] 及び [NIST SP 800-30, Rev. 1] に記載されているように、脅威及び脆弱性の識別に加えて、事業体はサプライチェーンのサイバーセキュリティ脅威分析及び脆弱性分析を実施することが望ましい。

脅威分析

C-SCRMでは、脅威分析は、事業体内のマネジメント、取得、エンジニアリング、及び運用活動に情報を提供するために、脅威事象（附属書Cを参照）、潜在的な脅威行為者（例えば、国民国家）、及び脅威ベクトル（例えば、サードパーティサプライヤ）の具体的かつタイムリーな特徴付けを提供する[68]。潜在的な脅威のアセスメントには、オープンソース、諜報活動、対諜報活動を含む、様々な情報を利用することができる。事業体は、枠組み化ステップで定義された脅威源及び前提条件を含め、更新し、精緻化することが望ましい。脅威分析の結果は、最終的には、取得の決定、代替構築の決定、及び対応ステップで適用される適切な軽減策の策定及び選択を支援することになる。サプライチェーンの脅威分析の焦点は、重要度分析の結果に基づくことが望ましい。

事業体は、サプライチェーンのサイバーセキュリティ侵害を受けているかどうかを判断し、そのような侵害をさらに調査するために、既存のインシデント管理活動から得られる情報を使用することが望ましい。政府機関は、フォレンジック調査を含むインシデント発生後の活動の一環としてサプライチェーンのサイバーセキュリティ侵害を識別できることを確実にするために、サプライチェーンのサイバーセキュリティ侵害を構成するものの基準を定義することが望ましい。さらに、政府機関は、政府機関が定義した間隔で、サプライチェーン侵害が発生したかどうかを判断するために、事業体内のその他のインシデント情報源をレビューすることが望ましい。

サプライチェーンのサイバーセキュリティ脅威分析では、少なくとも以下のデータを把握することが望ましい。

- サプライチェーンのサイバーセキュリティに関連する攻撃が発生している間の観測
- サプライチェーンのサイバーセキュリティに関連する侵害後に収集されたインシデントデータ
- 監査メカニズムを使用して観測又は収集されたかどうかに関わらず、特定の攻撃で使用された戦術、技術、及び手順の観測
- 発生前、発生中、及び発生後の自然災害及び人為的災害

脆弱性分析

C-SCRMでは、脆弱性とは、脅威源によって悪用又は誘発される可能性がある、情報システム、システムセキュリティ手順、内部管理策、又は実装における弱点である [NIST SP 800-53, Rev. 5]。

脆弱性分析は、リスクアセスメント及び対策の選択に情報を提供する反復プロセスである。脆弱性分析は、脅威分析と並行して機能し、インパクト分析に情報を提供し、軽減すべき脆弱性の範囲及び優先順位付けに役立つ。

[68] サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダの脅威の特徴付けは、無害である可能性があることに留意する。

アセスメントステップの脆弱性分析では、サプライチェーンのサイバーセキュリティ脆弱性の前提条件を更新及び精緻化するために、枠組み化ステップで定義されたアプローチを使用することが望ましい。脆弱性分析は、最初に、重要なミッション及びビジネスプロセス、及び重要度分析によって識別されたシステム又はシステムコンポーネントに適用される脆弱性を識別することから始めることが望ましい。脆弱性の調査は、以前の重要度分析で識別されたプロセス及びコンポーネントの重要度レベルを引き上げるか、又は少なくとも再検討する必要性を示している場合がある。その後の脆弱性分析の繰り返しでは、以前の脅威アセスメントでは考慮されなかった追加の脅威又は脅威の機会が識別される場合もある。

表G-8は、3つのレベル内で観測できるサプライチェーンのサイバーセキュリティ脆弱性の例を示している。

表 G-8：事業体レベルにマッピングされたサプライチェーンのサイバーセキュリティ脆弱性の例

レベル	脆弱性に関する考慮事項	方法
レベル 1 – 事業体	1) C-SCRM計画の欠如など、事業体のガバナンス構造又はプロセスにおける欠陥又は弱点 2) サプライチェーン自体の弱点（例えば、脆弱なエンティティ、特定エンティティへの過度の依存）	1) 外部事業体への依存を脆弱性として見なす方法についてのガイダンスを提供する。 2) 社内での構築、統合的信頼性のある共有サービス及び共通ソリューションの活用など、新しい技術の代替供給源を探し出す。
レベル 2 – ミッション及びビジネス	1) 偽造品を検出するための運用プロセスが実施されていない。 2) 交換部品としてSDLCに入る、供給されたシステムコンポーネントの受け入れテストのための技術審査の実装に予算が割り当てられていない。 3) 革新的な技術の供給源からの有害な問題の影響の受けやすさ（例えば、サードパーティが所有又は管理する技術はバグが多い）	1) 汚染された製品又は偽造品を検出するためのプログラムを開発し、リソース及びトレーニングに適切な予算を割り振る。 2) 受け入れテスト（SDLCに入るコンポーネントの技術審査）に予算を割り振る。
レベル 3 – 運用	1) 要件を満たしていないシステム機能の不一致により、パフォーマンスに大きな影響を与える。	1) 機能の不一致に対処するためにエンジニアリングの変更を開始し、パフォーマンスへのインパクトのための修正をテストする。悪意のある改ざんは、システムのライフサイクルを通じて政府機関のシステムに対して起こり得る。 2) ソフトウェアベンダが公開する脆弱性開示報告書（VDR）で開示された脆弱性をレビューする。

リスクの判断

タスク 2-2：識別された脅威が、識別された脆弱性を悪用する場合の、事業体の運営及び資産、個人、他の事業体、及び国家に対するリスクを決定する。

補足ガイダンス

事業体は、既知の脅威がサプライチェーンに対して既知の脆弱性を悪用することの起こりやすさと、そのような悪用が発生した場合の結果又は悪いインパクト（すなわち、損害の大きさ）を考慮することによって、サプライチェーン全体のサイバーセキュリティリスクを識別する。事業体は、C-SCRM リスクを定性的又は定量的に判断するために、脅威及び脆弱性の情報と、起こりやすさ及び結果／インパクトの情報を使用する。レベル1及びレベル2のリスク判断からのアウトプットは、[NIST 800-37, Rev. 2] で説明されている「RMF準備 - 事業体レベル」のタスクに直接対応することが望ましく、レベル3で完了したリスクアセスメントは、「RMF準備 - 運用レベル」のタスクに直接対応することが望ましい。

起こりやすさ

起こりやすさとは、ある脅威がある脆弱性を悪用することができる確率の主観的な分析に基づく重み付けされた因子である [CNSSI 4009]。この起こりやすさを判断するには、脅威源の特徴、識別された脆弱性、及び保全措置又は軽減策の実装前及び実装中における事業体のサプライチェーンのサイバーセキュリティ侵害の受けやすさを考慮する必要がある。起こりやすさの判断では、枠組み化ステップの一部として定義された方法論を利用し、起こりやすさについて策定された前提条件を更新、精緻化、及び拡張することが望ましい。敵対的脅威の場合、この分析では、事業体のミッションを妨害する敵対者のケイパビリティ（能力）と意図の程度を考慮することが望ましい。サプライチェーンのサイバーセキュリティリスクアセスメントでは、以下の2つの観点を考慮することが望ましい。

1. サプライチェーン自体内の1つ以上の要素が侵害される起こりやすさ。これは、例えば、高品質のコンポーネントの可用性にインパクトを与えるか、又は知的財産の盗難のリスクを高めたりする可能性がある。
2. サプライチェーン内のシステム又はコンポーネントが、例えば、システムに挿入された悪意のあるコード、又はコンポーネントを損傷する激しい雷雨などによって、侵害される起こりやすさ。

場合によっては、この2つの起こりやすさが重なり合うか区別がつかない場合もあるが、いずれも政府機関がミッションを遂行する能力にインパクトを与える可能性がある。

起こりやすさの判断では、以下を考慮することが望ましい。

- サイバーセキュリティの脅威、自然災害、又は物理的セキュリティの脅威など、システム又はコンポーネントが受ける可能性がある脅威の種類を明確にする脅威の前提条件
- 敵対者のケイパビリティ（能力）、ツール、意図、標的などの、実際のサプライチェーンの脅威の情報
- 同業者又は類似の事業体におけるサプライチェーン事象の頻度に関する過去のデータ
- サプライチェーンを通じてシステム又はプロセスが侵害される確率に関する内部専門家の見解
- 外部アクセス（すなわち、システム境界外部）へのコンポーネントの曝露（エクスポージャー）
- 識別されたシステム、プロセス、又はコンポーネントの脆弱性
- サプライチェーンのサイバーセキュリティ脅威の発生確率を判断するために、完了した分析（例えば、システム分析、プロセス分析）から利用可能な弱点及び脆弱性に関する実証データ

考慮すべき要素には、脆弱性を介した攻撃を成功させることの容易さ又は困難さ、及び脆弱性を取り込む又はもたらすために採用された方法を検知する能力が含まれる。この目的は、脆弱性の正味の影響をアセスメントすることであり、これを脅威情報と組み合わせて、リスクアセスメントプロセスの一環として、定義された時間枠内での攻撃成功の起こりやすさを判断する。起こりやすさは、脅威の前提条件、又はサプライチェーンの以前の侵害、特定の敵対者のケイパビリティ（能力）、過去の侵害の傾向、又は侵害の頻度などの実際の脅威データに基づくことができる。事業体は、事業体内で利用可能及びアクセス可能なデータの種類に応じて、侵害発生の具体的な確率を判断するために、実証データと統計分析を使用する場合がある。

インパクト

事業体は、侵害のインパクト及びその侵害を軽減するインパクトを判断するために、枠組み化ステップで定義された潜在的インパクトの前提条件及び方法論を使用して、インパクト分析を開始することが望ましい。事業体は、1）事象を発生させる可能性がある脅威源の特徴、2）識別された脆弱性、及び 3）事業体の、計画又は実装された対策に基づく、このような事象の影響の受けやすさを含む、侵害による様々な悪いインパクトを識別する必要がある。インパクト分析は、侵害発生時、変更のインパクトを評価するための軽減アプローチが決定した時、及びシステム又は環境の状況又はコンテキストが変化した時に、絶えず変化するSDLCで最初に実行される反復プロセスである。

事業体は、インパクト分析の結果を使用して、特定のシステムに関連するサプライチェーン全体のサイバーセキュリティリスクの受容可能なレベルを定義することが望ましい。インパクトは、重要度、脅威、及び脆弱性の分析結果から導き出され、情報又は情報システムの機密性、完全性、又は可用性の喪失が、事業体の運営、事業体の資産、個人、他の事業体、又は国家（米国の国家安全保障上の利益を含む）に及ぼす影響の大きさに基づくことが望ましい [NIST SP 800-53, Rev. 5]。インパクトは、分析的判断を必要とする定性的尺度である可能性が高い。管理職／意思決定者は、リスクベースの意思決定、及び結果として生じるリスク及びそのような決定の結果を受容、回避、軽減、又は共有するかどうかの決定へのインプットとしてインパクトを使用する。

事業体は、サプライチェーン全体のサイバーセキュリティリスクのアセスメントの全体的な結果をリスクアセスメント報告書に文書化することが望ましい[69]。サプライチェーンのサイバーセキュリティリスクアセスメント報告書は、必要に応じて3つの事業体レベルすべてのリスクを網羅することが望ましい。事業体の構造と規模に応じて、サプライチェーン全体のサイバーセキュリティリスクに関する複数のアセスメント報告書が必要となる場合がある。政府機関は、レベル1で個々の報告書を作成することが推奨される。レベル2では、政府機関はサプライチェーン全体のサイバーセキュリティリスクを、それぞれのミッションレベルのビジネスインパクト分析（BIA）に統合することが望ましく、サプライチェーン全体のサイバーセキュリティリスクに関する個別のミッションレベルアセスメント報告書を策定することを望む場合がある。レベル3では、政府機関はサプライチェーン全体のサイバーセキュリティリスクを、それぞれのリスク対応フレームワークに統合することを望む場合がある。3つのレベルすべてのリスク対応フレームワークは相互に連結され、適切な場合には相互に参照し、C-SCRM計画と統合し、認可パッケージの一部を構成することが望ましい。

集約

事業体は、複数の個別のリスク又は低レベルのリスクを、より一般的なリスク又は高レベルのリスクに結合するために、リスク集約を使用することができる [NIST SP 800-30, Rev. 1]。リスク集約は、事業体が、組織の様々なレベルの資産とは対照的に、サプライチェーンへのリスク曝露（エクスポージャー）を理解することを目指しているため、C-SCRMにとって特に重要である。最終的には、事業体は、リスクの種類（例えば、財務、運用、法律／規制）わたる総合的なリスク曝露（エクスポージャー）の理解を深めるために、C-SCRMのリスクアセスメントの結果と他の事業体のリスクアセスメントを集約及び正規化することを望む場合がある。この集約は、事業体が複数の傘下事業体から構成されている場合には、事業体レベルで行われる可能性がある。各傘下事業体は、単一の事業体リスクレジスタ内でリスクを結合及び正規化する。レベル2のミッション及びビジネスプロセスレベルのレジスタから、単一のレベル1の事業体レベルのリスクレジスタへのリスク集約も行われる場合がある。このプロセスを容易にするために、事業体は上位のリスクプロセス（例えば、事業体リスクマネジメント）からの共通フレームワーク及び語彙を最大限に継承することが望ましい。

個別の（すなわち、重複しない）リスクに対処する場合、事業体は、レベル1及びレベル2の集約リスク曝露（エクスポージャー）の包括的な理解を容易に深めることができる。しかし、多くの場合、事業体は、下位レベルで完了したリスクアセスメントに、起こりやすさとインパクトの大きさに関する重複する推定が含まれていることに気付くだろう。このような場合、部分（すなわち、下位レベルでのリスク曝露（エクスポージャー）評価）の合計は、全体（すなわち、事業体の総リスク曝露（エクスポージャー））よりも大きくなる。このような課題を克服するために、事業体は様々な手法を採用することができる。事業体は、相互に関連するリスクの起こりやすさとインパクトを示すために、視覚化又はヒートマップの使用を選択する場合がある。事業体は、リスクの総和を数値として示す場合、相互に排他的かつ網羅的な集合（MECE）フレームワークを採用することによって、リスクアセスメントが個別のアウトプットを生成することを確実にすることが望ましい。MECEフレームワークは、インプット（例えば、脅威、脆弱性、インパクト）の分析を導き、事業体が重複する前提条件及び推定を最小限に抑えることを可能にする。事業体は、下位レベルのリスクを合計する代わりに、下位レベルからの統合されたアセスメント結果を活用する、新たな包括的なアセスメントを上位レベルで実行することを選択してもよい。そうすることで、事業体が総リスク曝露（エクスポージャー）の過大評価を引き起こすリスクの二重計上を回避するのに役立つ。事業体は、説明が困難なリスク集約（例えば、大きく異なるシナリオをまとめて1つの数値にする）を回避するために、リスク集約の際に慎重に判断することが望ましい。

[69] リスクアセスメント報告書の説明については、[NIST SP 800-30, Rev. 1]附属書Kを参照のこと。

定量的手法は、リスク集約に明確なメリットを提供する。確率的手法（例えば、モンテカルロ法、ベイズ分析）を使用することにより、事業体は、数学的に正当な方法で、類似するリスクを単一の理解しやすい数値（例えば、ドル）にまとめることができる。相互に排他的かつ網羅的な集合フレームワークは、定量的手法にとって依然として重要な要件である。

アウトプット及び事後条件

このステップの結果を以下に示す。

- 確認されたミッション及びビジネスプロセスの重要度
- システムのサプライチェーンインフラストラクチャ（例えば、SDLC）の重要な側面と、適用可能な脅威及び脆弱性との関係の確立
- 潜在的なサプライチェーンのサイバーセキュリティ侵害の起こりやすさ及びインパクトの理解
- ミッション及びシステム固有のリスクの理解
- ミッション及びビジネスプロセス又は個々のシステムに関連するサプライチェーン全体のサイバーセキュリティリスクアセスメントの文書化
- 関連するサプライチェーン全体のサイバーセキュリティリスクアセスメント結果の、事業体リスクマネジメントプロセスへの統合

対応

インプット及び前提条件

対応とは、リスクアセスメントを実施する個人が、アセスメント結果、提案された軽減策／管理策のオプション、及び提案された各オプションに対応する受容可能なリスクレベルを意思決定者に伝達するステップである。この情報は、リスクベースの意思決定に情報を提供し、導くために、適切な方法で提示されることが望ましい。これにより、意思決定者は、一連のオプション、及び様々なオプションを選択する際の対応するリスク要因に基づいて、適切なリスク対応を最終決定することができる。適切な対応は、戦術及び活動をよりよく理解するために、敵対者の活動及び行為を単に監視することである場合もある。

サプライチェーンのサイバーセキュリティリスク対応は、全体的な事業体リスク対応に統合することが望ましい。図G-6は、3つの事業体レベルに沿ったインプット及びアウトプットを伴う対応ステップを示している。

図 G-7：対応ステップにおける C-SCRM[70]

[70] リスクマネジメントプロセスの詳細は、附属書Cに記載されている。

活動

リスク対応の識別

タスク 3-1：リスクアセスメントで識別されたリスクに対応するための代替の行動方針を識別する。

事業体のリスク対応戦略は、事業体（すなわち、レベル1）及びミッション及びビジネスプロセス（すなわち、レベル2）のために策定されたリスクマネジメント戦略から情報が提供される。リスク対応戦略には、事業体がリスク対応への取り組み（例えば、受容、回避、軽減、移転、又は共有）の一環としてとる可能性がある一般的な行動方針が含まれる。軽減への取り組みの一環として、事業体はC-SCRM管理策を選択し、リスク判断に基づいてこれらの管理策をテーラリングすることが望ましい。C-SCRM管理策は、各レベルのリスクアセスメントの所見に従って適切に、3つのレベルすべてに対して選択することが望ましい。

本出版物に含まれるC-SCRM管理策の多くは、ITセキュリティ計画の一部である可能性があり、サードパーティプロバイダとの合意に要件として組み込むことが望ましい。これらの管理策はC-SCRMに適用されるため、含まれている。

このプロセスは、代替案の評価（トレードオフ分析とも呼ばれる）をサポートするために、受容可能なリスクを決定することから始めることが望ましい。

代替案の評価

タスク 3-2：リスクに対応するための代替の行動方針を評価する。

初期の受容可能なリスクレベルが定義されたら、リスク対応の行動方針を識別し、事業体が定義されたリスクしきい値を達成できるようにするための有効性を評価することが望ましい。代替案の評価は、通常レベル1又はレベル2で行われ、事業体のミッション及びプロセスを成功裡に遂行するための事業体の能力に対する、予測される事業体全体のC-SCRMのインパクトに焦点を当てる。代替案の評価がレベル3で行われる場合、SDLC又は行動方針を実装するために利用可能な時間に焦点を当てる。

分析される各行動方針には、リスク受容、回避、軽減、移転、及び共有の組み合わせを含む可能性がある。例えば、事業体は、契約条項に含まれる管理策の選択を通じて、戦略的サプライヤとリスクの一部を共有することを選択する場合がある。あるいは、事業体は、管理策を選択及び実装することで、リスクを受容可能なレベルまで軽減することを選択する場合がある。多くの場合、リスク戦略は、リスク対応の行動方針を組み合わせて活用する。

代替案の評価中に、事業体は、識別されたサプライチェーン全体のサイバーセキュリティリスクに対して、利用可能なリスク対応行動方針を分析する。この作業の目標は、事業体がC-SCRMと事業体の機能ニーズの間で適切なバランスを取ることができるようにすることである。最初のステップとして、事業体はリスク選好度及び許容度、優先順位、トレードオフ、適用される要件、及び制約条件が、コスト、スケジュール、パフォーマンス、ポリシー、及びコンプライアンスなど、より広範な事業体の要件に精通しているステークホルダーとともにレビューされることを確実にすることが望ましい。このプロセスを通じて、事業体は、その広範な要件に対するリスク対応の影響を識別する。事業体は、リスク対応の影響を包括的に理解した上で、リスクに対応するためのC-SCRM管理策の適切なバランスを識別するために、C-SCRM、ミッション、及び運用レベルのトレードオフ分析を実施することが望ましい。レベル3では、枠組み化、アセスメント、対応、及び監視プロセスを、[NIST SP 800-37, Rev. 2] で説明されているRMF選択ステップに取り込む。

リスク対応行動方針のために選択されるC-SCRM管理策は、事業体レベル及びSDLCプロセス内で適用される場所によって異なる。例えば、C-SCRM管理策は、ブラインド購入戦略の使用から、重要なコンポーネント及び設計属性（例えば、インプットの妥当性確認、サンドボックス、改ざん防止設計）の不明瞭な最終用途まで、多岐にわたる可能性がある。実装された各管理策について、事業体はその実行に責任を負う者を識別し、SDLC全体にわたって実装するための時間又は事象に基づいた計画を策定することが望ましい。複数の管理策は、幅広い潜在的リスクに対処する可能性がある。したがって、管理策が全体的なリスクにどのようなインパクトを与えるかを理解しておくことは不可欠であり、管理策を最終決定する前に、さらに別のトレードオフ分析が必要となる可能性があるため、管理策の組み合わせを選択してテーラリングする前に検討しなければならない。提案された管理策と全体的なリスクとの間の依存関係が十分に理解され、対処されていなければ、事業体は知らず知らずのうちに、1つのリスクをより大きなリスクと交換する可能性がある。

リスク対応の決定

タスク 3-3：リスクに対応するための適切な行動方針を決定する。

[NIST SP 800-39] で説明されているように、事業体は、代替案の評価、及び脅威、リスク、及びサプライチェーンの優先順位の全体的な理解に基づいて、C-SCRM管理策を選択、テーラリング、及び最終決定することが望ましい。レベル1及びレベル2では、結果として生じる決定及び選択されテーラリングされた共通管理策ベースライン（すなわち、確立されたベースラインに対する改訂）を、C-SCRM固有のリスク対応フレームワークに記載することが望ましい[71]。レベル3では、結果として生じる決定及び選択されテーラリングされた管理策を、認可パッケージの一部としてC-SCRM計画に記載することが望ましい。

リスク対応の決定は、リスク管理者が行うこともあれば、リスク管理者により事業体内の誰かに委任することもある。決定はレベル2又はレベル3に委任することができるが、インパクトの重大性と範囲によって決定が行われるレベルを決定することが望ましい。リスク対応の決定は、必要に応じて、事業体のリスク管理者、ミッションオーナー、及びシステム所有者と協力して行われる場合がある。リスク対応の決定は、事業体の既定のリスク選好度及び許容度に大きく影響される。強固なリスク選好度及び許容度の定義を使用することで、意思決定者は、事業体のリスク決定と戦略的必須事項との一貫した整合性を確実にすることができる。また、強固なリスク選好度及び許容度の定義により、事業体はリスク決定の責任を事業体の下位レベルに委任し、すべてのレベルにおいてより大きな自律性を提供することを可能にする可能性がある。

レベル1及びレベル2では、結果として生じる決定は、要件又は選択された共通管理策ベースライン（すなわち、事業体又はミッション及びビジネスプロセスレベル）に対するすべての変更と共に、C-SCRM固有のリスク対応フレームワークに記載されることが望ましい。C-SCRMリスク対応フレームワークは、他の関連するリスク対応フレームワークに影響を与える可能性がある。

リスク対応フレームワークは、以下を含むことが望ましい。

- 脅威源、脅威事象、悪用された脆弱性、及び脅威事象の結果の記述
- リスクの起こりやすさ及びインパクト、及び最終的なリスク曝露（エクスポージャー）の分析
- 選択された軽減戦略及び管理策の記述と、リスクに対する軽減策のコスト及び有効性の見積もり

[71] リスク対応フレームワークの詳細及び明示的な例は、附属書Bに記載されている。

レベル3では、結果としての得られた決定、及び選択及びテーラリングされた管理策を C-SCRM計画に記載することが望ましい。C-SCRM計画は、事前対応的に策定することが理想的だが、サプライチェーンのサイバーセキュリティ侵害に対応して策定する場合もある。最終的には、C-SCRM計画は、SDLC全体をカバーし、C-SCRMベースラインを記載し、レベル3の運用レベルでサイバーセキュリティサプライチェーンの要件及び管理策を識別することが望ましい。C-SCRM計画は、サイバーセキュリティサプライチェーンの監視のアウトプットに基づいて改訂及び更新されることが望ましい。

C-SCRM計画は、以下であることが望ましい。

- 現在事業体に実装されている事業体及びミッションの要件に基づき、適用可能なポリシー、プロセス、及び手順など、枠組み化ステップで決定した環境を要約する。
- リスク管理者、最高財務責任者（CFO）、最高情報責任者（CIO）、プログラムマネージャ、又はシステム所有者など、計画の責任を負う役割を明言する。
- CFO、最高運用責任者（COO）、取得／契約、調達、C-SCRM PMO、システムエンジニア、システムセキュリティエンジニア、開発者／保守エンジニア、運用マネージャ、又はシステムアーキテクトなど、主要な貢献者を識別する。
- （対応ステップで）代替案の評価の結果として得られた、適用可能な（レベルごとの）一連のリスク軽減策及び管理策を提供する。
- 選択された管理策のテーラリングに関する決定を、その決定の根拠を含めて提供する。
- サイバーセキュリティサプライチェーンの相互依存関係が対処されることを確実にするために、レベル間のフィードバックプロセスを記述する。
- 各固有のC-SCRM計画の範囲に適用される監視及び実施活動（適切な場合には、監査を含む）を記述する。
- 適切な場合には、C-SCRM計画の実装をサポートし、実装の有効性をアセスメントするための定性的又は定量的手段を記述する[72]。
- 計画のレビュー及び改訂を行う頻度を定義する。
- ライフサイクルのマイルストーン、ゲートレビュー、又は重要な契約活動など、改訂のきっかけとなる基準を含める。
- サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダが、合意の一部として利用可能になっている場合は、これらをC-SCRM計画に含める。

政府機関は、C-SCRM管理策をそれぞれのシステムセキュリティ計画に統合する、あるいは個別の運用レベルのC-SCRM計画を策定することを望む場合がある。レベル3では、C-SCRM計画は、[FIPS 199] に従って、高インパクト及び中インパクトのシステムに適用される。レベル1の事業体のC-SCRM戦略及びレベル2のミッションのC-SCRM戦略及び実装計画からの要件及びインプットは、フローダウンし、レベル3のC-SCRM計画の策定を導くために使用されることが望ましい。逆に、上位レベルで適用される要件及び管理策を策定及び改訂する際には、レベル3のC-SCRM管理策及び要件を考慮することが望ましい。C-SCRM計画は相互に接続され、適切な場合には相互に参照されることが望ましい。

[72] NIST SP 800-55, Rev. 1、情報セキュリティパフォーマンス測定ガイド（2008年7月）は、情報セキュリティ測定指標の策定に関するガイダンスを提供している。 政府組織は、C-SCRM計画のための固有の手段を策定するときに、この出版物の一般ガイダンスを使用することができる。http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf を参照のこと。

表G-9は、レベル1及びレベル2のリスク対応フレームワーク及びレベル3のC-SCRM計画に含まれる管理策と、それらの管理策の例をまとめたものである。

表 G-9：レベル 1、2、及び 3 の管理策

レベル	管理策	例
レベル 1	レベル2及びレベル3に事業体の共通管理策ベースラインを提供する	• すべてのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダに適用される管理策の最小限のセット • サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダの情報の処理及び保存に適用される事業体レベルの管理策 • 事業体レベルの取得者スタッフを対象としたサイバーセキュリティサプライチェーンのトレーニング及び意識向上
レベル 2	• レベル1から共通管理策を継承する • ミッション及びビジネスプロセスレベルの共通管理策ベースラインをレベル3に提供する • 何が機能しているか、及び何を変更する必要があるかについて、レベル1にフィードバックを提供する	• 特定のミッション及びビジネスプロセスのサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダに適用される管理策の最小限のセット • C-SCRMの懸念に対処するための、ID及びアクセス管理の管理策のプログラムレベルでの精緻化 • プログラム固有のサプライチェーンのトレーニング及び意識向上
レベル 3	• レベル1及びレベル2から共通管理策を継承する • レベル3のシステム固有の管理策を提供する • 何が機能しているか、及び何を変更する必要があるかについて、レベル1及びレベル2にフィードバックを提供する	• サービスプロバイダ又は個々のシステムの特定のハードウェア及びソフトウェアに適用される管理策の最小限のセット • サプライチェーンをサポートするシステムの変更管理に関する適切に厳格な受容基準（例えば、テスト環境又は統合開発環境として） • システム固有のサイバーセキュリティサプライチェーンのトレーニング及び意識向上 • SDLCとの交差

附属書Cは、事業体がC-SCRM計画活動に含めることが望ましい情報のセクション及び種類を示したC-SCRM計画のテンプレートの例を提供している。

リスク対応の実装

タスク 3-4：リスクに対応するために選択された行動方針を実装する。

事業体は、C-SCRM管理策を政府機関全体のリスクマネジメントプロセスに統合する方法で、C-SCRM計画を実装することが望ましい。

アウトプット及び事後条件

このステップのアウトプットは、C-SCRM要件に対処する一連のC-SCRM管理策であり、システム要件ベースライン及びサードパーティプロバイダとの合意に組み込むことができる。これらの要件及び結果として得られる管理策は、3つのレベルを通じてSDLC及びその他の事業体プロセスに組み込まれる。

一般的なリスクの種類の場合、このステップの結果は以下の通りである。

- 識別されたリスクに対処する、選択、評価、及びテーラリングされたC-SCRM管理策
- 提案された軽減策を受け入れた場合と受け入れなかった場合の識別された結果
- C-SCRM計画の策定及び実装

監視

インプット及び前提条件

監視は、事業体が 1）コンプライアンスを検証し、2）リスク対応策の継続的な有効性を判断し、3）事業体の情報システム及び運用環境のリスクにインパクトを与える変更を識別するステップである。

事業体、ミッション及びビジネスプロセス、運用、又はサプライチェーンに対する変更は、事業体のサイバーセキュリティサプライチェーンに直接インパクトを与える可能性がある。監視ステップは、このような変更を追跡し、これらの変更が（アセスメントステップで）インパクトに対して適切にアセスメントされることを確実にするためのメカニズムを提供する。監視の結果、サイバーセキュリティサプライチェーンが再定義される場合、事業体はサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダと連携して、影響及び相互義務を解決することが望ましい。監視ステップの重要な構成要素には、上位レベルのリスクアセスメントへ情報を提供するための、上位への情報提供（例えば、ミッション及びビジネスプロセスのアセスメントから事業体のアセスメントへの情報提供）が含まれる。これにより、事業体のリーダーは、事業体全体のリスク状況の可視性を維持することを確実にする。

事業体は、リスクを再アセスメントして適切なリスク対応を決定するために、サプライチェーンリスク事象を監視することが望ましい。これには、事象がインシデントを誘発したか、又は情報共有の必要性を強いたかを判断することが含まれることが望ましい。サプライチェーンリスク事象の例を以下に示す。

- 所有者の変更、合併、又は取得
- サプライチェーンの寸断
- 供給源及びそのサプライチェーンに影響を与える継続事象又は緊急事象
- 供給源及びそのサプライチェーンに影響を与えるランサムウェア又はその他のサイバーセキュリティ攻撃

- 供給源及び／又はそのサプライチェーンで使用されている技術に影響を与える、又は与える可能性のある重大な脆弱性に関する新たな情報
- 偽造品又は不適合製品又はコンポーネントの発見
- 製造場所又はソフトウェア開発場所の変更、特に国内から国外への変更
- OEMによる製品又は製品の重要コンポーネントの製造及び／又はサポートの終了
- 対象品目の非開示機能または特徴の証拠
- 連邦政府のデータ及び情報システムの機密性、完全性、及び可用性が、ICT製品の改修、改ざん、及び偽造を伴う攻撃に直接起因するものであるかどうかを判断するために追加の調査を必要とする通知
- 禁止された、又は認可されていない供給源によって製造された対象品目の存在
- 疑わしい外国人による所有、管理、又は影響（FOCI）の証拠
- 供給源、対象品目、及び／又は関連するサプライチェーンのリスクプロファイルに悪影響を与える可能性があるその他の変化（例えば、主要な人員の喪失、企業の財政状態の悪化、など）

事業体は、C-SCRMを既存の継続的監視プログラムに統合することが望ましい[73]。継続的監視プログラムが存在しない場合には、C-SCRMは包括的な継続的監視プログラムを確立するための触媒としての機能を果たすことができる。図G-7は、3つの事業体レベルに沿ったインプット及びアウトプットを伴う監視ステップを示している。

[73] NIST SP 800-137、連邦政府情報システム及び組織の情報セキュリティの継続的監視（ISCM）（*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*）（2011年9月）では、継続的監視プログラムの確立及び実装方法を記述している。http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf を参照のこと。

図 G-8：監視ステップにおける C-SCRM[74]

[74] リスクマネジメントプロセスの詳細は、附属書Cに記載されている。

活動

リスク監視戦略

タスク 4-1：監視活動の目的、種類、及び頻度を含む事業体のリスク監視戦略を策定する。

補足ガイダンス

事業体は、C-SCRMの考慮事項を全体的なリスク監視戦略に統合することが望ましい。サプライチェーン全体のサイバーセキュリティリスクを監視するには、政府機関が従来収集していなかった可能性がある情報へのアクセスが必要となる場合がある。情報の一部は、オープンソース、サプライヤ、又はインテグレータなど、政府機関の外部から収集する必要がある。戦略は、特に、収集するデータを含め、データから収集される特定の測定指標（例えば、ベンダによる契約コンプライアンス違反の件数）を明記し、データ収集に必要なツールに関する既存の前提条件を識別し、データの保護方法を識別し、データの報告形式を定義することが望ましい。潜在的なデータ源には以下が含まれる可能性がある。

- 政府機関の脆弱性管理及びインシデント管理活動
- 政府機関のマニュアルのレビュー
- 省庁間の情報共有
- 政府機関とサプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダとの間の情報共有
- サプライヤの情報共有
- サプライヤ、開発者、システムインテグレータ、外部システムサービスプロバイダ、及びその他のICT/OT関連のサービスプロバイダの契約上のレビュー

事業体は、サプライヤのデータが政府機関によって収集及び保存される場合には、その適切な保護を確実にすることが望ましい。また、政府機関は、サプライチェーン全体のサイバーセキュリティリスクを監視するという目的を達成するために、データを適切に評価するための追加のデータ収集及び分析ツールも必要とする場合がある。

リスク監視

タスク 4-2：コンプライアンスを検証し、リスク対応策の有効性を判断し、変化を識別するために、事業体の情報システム及び運用環境を継続的に監視する。

[NIST SP 800-39] に従い、事業体は、コンプライアンス、有効性、及び変化を監視することが望ましい。C-SCRMのコンテキストにおけるコンプライアンスの監視は、事業体のプロセス並びに供給製品及びサービスが、確立されたセキュリティ及びC-SCRM要件に準拠しているかを監視することを含む。有効性の監視には、確立されたセキュリティ及びC-SCRM要件が意図された結果をもたらすかどうかを判断するために、結果として生じるリスクを監視することが含まれる。変化の監視には、サプライチェーン全体のサイバーセキュリティリスクの受容可能なレベルを維持するために、要件及び軽減策／管理策の変更を示唆する可能性がある変化があるかどうか環境を監視する。

変化を監視するために、事業体は、サプライヤとその供給製品及びサービスをレビューする定期的な間隔を設けることが望ましい。再アセスメントの間隔は、必要に応じて、事業体にとって適切に決定することが望ましい。事業体はまた、サプライチェーン全体のサイバーセキュリティリスクの状態の変化を示唆する一連のサイクル外の誘因を識別して文書化する必要がある。誘因のカテゴリには、ポリシー、ミッション、脅威環境の変化、エンタープライズアーキテクチャ、SDLC、又は要件など、表D-6（枠組み化ステップ中）で識別した制約条件の変更が含まれる可能性があるが、これらのカテゴリ内の特定の誘因は、事業体によって大きく異なる可能性がある。

サイバーセキュリティサプライチェーンの変化の例として、2つの主要な精査済みサプライヤ[75]が特定の市場からの撤退を発表し、その結果、特定のコンポーネントの供給不足が生じることが挙げられる。この場合、サプライヤの数を減らすことで、コンポーネントの可用性及び完全性において脆弱性が発生する可能性があるかどうかを評価する必要が生じる。このシナリオでは、コンポーネントの供給不足から、潜在的なコンポーネントの不足が発生する可能性がある。残りのサプライヤがいずれも精査されていない場合、この不足により、残りのコンポーネントの完全性が不確実になる可能性がある。事業体のポリシーで精査済みコンポーネントの使用が指示されている場合、この事象によって、事業体はミッションのニーズを満たすことができなくなる可能性がある。サプライチェーンの変化は、企業の所有権変更の結果として発生することもある。所有権の変更は、特に、元の所有者とは異なる国の市民である個人への所有権の移転を伴う場合には、重大な影響を及ぼす可能性がある。

事業体は、継続的監視の結果を用いて、事業体の全レベルで既存のリスクアセスメントを定期的に更新することに加えて、再アセスメント実施の誘因を決定することが望ましい。誘因には、リソースの可用性、サプライチェーン全体のサイバーセキュリティリスクの変化、自然災害、又はミッションの破綻が含まれる可能性がある。

監視を効果的に行うためには、サプライチェーンのサイバーセキュリティリスクマネジメントの状況を、C-SCRM報告という形で事業体全体の意思決定者に伝える必要がある。報告は、報告対象者の固有のニーズを満たすようにテーラリングすることが望ましい。例えば、レベル1の意思決定者への報告では、C-SCRM実装範囲、効率性、有効性、及びサプライチェーン全体のサイバーセキュリティリスクへの曝露（エクスポージャー）の全体的なレベルを、事業体全体の集約レベルで要約することができる。報告対象者にとって適用可能で適切である場合には、報告は、レベル2及びレベル3で管理職責任者の注意を必要とする特定の領域に焦点を当てることができる。報告のテーラリングを支援するために、報告の要件は、報告対象者と協力して定義され、報告が効率的かつ効果的であることを確実にするために定期的に更新することが望ましい。

アウトプット及び事後条件

事業体は、監視ステップのサイバーセキュリティサプライチェーンのアウトプットをC-SCRM計画に統合することが望ましい。この計画は、必要に応じて枠組み化、アセスメント、及び対応ステップの繰り返し実装へのインプットを提供する。

[75] 精査済みサプライヤとは、組織が安心して取引できるサプライヤである。 この安心のレベルは、通常、組織が定義した一連のサプライチェーン基準を策定し、これらの基準に照らしてサプライヤを精査することによって達成される。

附属書 H：用語集

用語	定義
受容可能なリスク（acceptable risk）	組織によって定義されたリスク選好度及びリスク許容度の範囲に収まる、組織の業務、資産、又は個人に対する残留リスク。
調達者（acquirer） [ISO/IEC/IEEE 15288, adapted]	製品又はサービスを取得又は調達する組織又はエンティティ。
調達（acquisition） [NIST SP 800-64, adapted]	取得には、製品又はサービスの必要性を判断するプロセスから始まり、契約の締結及び完了で終わる、製品又はサービスを取得するプロセスのすべての段階が含まれる。
合意（agreement）	業務上の関係が遂行される、又は関係者間で商品が移転される際の契約条件の相互承認。例：契約、覚書、又は合意
認可境界（authorization boundary） [NIST SP 800-53 Rev. 5]	認可権限のある担当者によって運用を認可される、情報システムのすべてのコンポーネント。これには、情報システムが接続されている、個別に認可されたシステムは含まれない。
認可権限のある担当者（authorizing official） [NIST SP 800-53 Rev. 5]	情報システムの運用、又は指定された一連の共通管理策の使用を、政府機関の業務（ミッション、機能、イメージ、又は評判を含む）、政府機関の資産、個人、他の組織、及び国家に対する受容可能なリスクレベルで認可する（すなわち、責任を負う）権限を有する、連邦政府の高官又は幹部。
運用認可（authorization to operate） [NIST SP 800-53 Rev. 5]	合意された一連のセキュリティ及びプライバシー管理策の実施に基づき、情報システムの運用を認可し、政府機関の業務（ミッション、機能、イメージ、又は評判を含む）、政府機関の資産、個人、他の組織、及び国家に対するリスクを明示的に受容するために、連邦政府の高官によって下される管理上の正式な決定。認可は、政府機関の情報システムによって継承される共通管理策にも適用される。
ベースライン（baseline） [CNSSI 4009]	ある時点における、情報システムのハードウェア、ソフトウェア、データベース、及び関連文書。
C-SCRM 管理策（C-SCRM control）	サプライチェーン全体のサイバーセキュリティリスクの起こりやすさ、及び／又はインパクト／結果を低減あるいは排除する目的で定められた予防手段又は対策。

用語	定義
サプライチェーンにおけるサイバーセキュリティ侵害（cybersecurity compromise in the supply chain）	サプライチェーンにおけるサイバーセキュリティインシデント（侵害とも呼ばれる）は、システム又はそのシステムが処理、保存、又は伝送する情報の機密性、完全性、又は可用性が危険にさらされる、サプライチェーン内での出来事である。サプライチェーンインシデントは、システム、製品、又はサービスのライフサイクルにおけるどの段階でも発生する可能性がある。
サプライチェーン全体のサイバーセキュリティリスク（cybersecurity risks throughout the supply chain）	サプライヤ、そのサプライチェーン、製品、サービスに起因する損害又は侵害の可能性。サプライチェーン全体のサイバーセキュリティリスクは、サプライチェーンを通過する製品及びサービスの中にある脆弱性又は暴露（エクスポージャー）を悪用する脅威、ならびに、サプライチェーン自体の中にある脆弱性又は暴露（エクスポージャー）を悪用する脅威から生じる。
サプライチェーンのサイバーセキュリティリスクアセスメント（cybersecurity supply chain risk assessment）	サプライチェーン全体のサイバーセキュリティリスク、それらの出来事の起こりやすさ、及び潜在的なインパクトの体系的な検査。
サプライチェーンのサイバーセキュリティリスクマネジメント（cybersecurity supply chain risk management）	サプライチェーン全体のサイバーセキュリティリスクへの暴露（エクスポージャー）を管理し、適切な対応戦略、ポリシー、プロセス、及び手順を策定するための体系的なプロセス。 注：NIST の出版物の目的上、SCRM 及び C-SCRM は同じ概念を表す。これは、NIST が SCRM のサイバーセキュリティの側面のみを扱っているからである。他の組織は、SCRM に対して、本出版物の範囲に含まれない別の定義を使用している可能性がある。本出版物では、SCRM におけるサイバーセキュリティ以外の側面の多くは扱っていない。
広域防御（defense-in-breadth） [NIST SP 800-53 Rev. 5]	システム、ネットワーク、又はサブコンポーネントのライフサイクルの、システム、ネットワーク、又は製品の設計及び開発、製造、包装、組み立て、システムの統合、分散、運用、保守、廃止を含むあらゆる段階で、悪用可能な脆弱性のリスクを特定、管理、及び低減することを目的とした、多くの専門分野にわたる一連の計画的かつ体系的な活動。
劣化（degradation）	品質又はパフォーマンスの低下、その低下が引き起こされるプロセス。
開発者（developer） [NIST SP 800-53 Rev. 5, adapted]	システム、システムコンポーネント、又はシステムサービスの開発者又は製造業者、システムインテグレータ、サプライヤ及び製品の再販業者を含む一般用語。システム、コンポーネント、又はサービスの開発は、組織内部又は外部エンティティを介して行われる可能性がある。

用語	定義
要素（element）	サプライチェーン要素（*supply chain element*）を参照。
拡張オーバーレイ（enhanced overlay）	オーバーレイの目的に特化したプロセス、管理策、拡張、及び補足的な実装ガイダンスを追加するオーバーレイ。
暴露（エクスポージャー）（exposure） [ISO Guide 73, adapted]	組織及び／又はステークホルダーがリスクにさらされる度合い。
外部システムサービス（external system service） [NIST SP 800-53 Rev. 5]	外部サービスプロバイダによって提供され、組織が必要なセキュリティ及びプライバシー管理策の実施又は管理策の有効性に関するアセスメントを直接管理できないシステムサービス。
外部システムサービスプロバイダ（external system service provider） [NIST SP 800-53 Rev. 5]	合弁事業、事業提携、外部委託協定（契約、省庁間協定、事業協定などによるもの）、ライセンス契約、及び／又はサプライチェーンの交換など、様々な消費者と生産者の関係を通じて組織に外部システムサービスを提供するプロバイダ。
目的に適合（fit for purpose） [ITIL Service Strategy, adapted]	目的又はサービスレベルを満たすことのできるプロセス、構成アイテム、IT サービスなどを説明するために非公式に使用される。目的に適合（fit for purpose）するためには、適切な設計、実装、管理策、及び保守が必要である。
ICT/OT 関連のサービスプロバイダ（ICT/OT-related service providers）	ICT システム又は OT システムへの認可されたアクセスを含む可能性があるサービスを提供する組織又は個人。
インパクト（impact） [NIST SP 800-53 Rev. 5]	情報又はシステムの機密性、完全性、又は可用性の喪失が、組織の業務、組織の資産、個人、他の組織、又は国家（米国の国家安全保障上の利益を含む）に及ぼす影響。
情報通信技術（Information and Communications Technology） [ISO/IEC 2382, adapted]	データ及び情報のキャプチャ、保存、検索、処理、表示、表現、提示、体系化、管理、セキュリティ、送信、交換を含む。
情報システム（information system） [NIST SP 800-53 Rev. 5]	情報の収集、処理、維持、使用、共有、配布、又は廃棄のために体系化された個別の一連の情報リソース。
ライフサイクル（life cycle）[ISO/IEC/IEEE 15288, adapted]	システム、製品、サービス、プロジェクト、又はその他の人間が作成するエンティティの進化過程。

用語	定義
起こりやすさ（likelihood） **[ISO/IEC 27000]**	何かが起こる可能性。
重要性（materiality） 1）米国最高裁判所による TSC Industries 対 Northway の判例、 426 U.S. 438, 449 (1976)	1）米国最高裁判所が TSC Industries 対 Northway （426 U.S. 438, 449 (1976)）で明確に示した、重要性の基準（ある事実は、投資判断を下す際に「合理的な株主がその事実を重要だと考える可能性がかなり高い」場合、又は、株主が「利用可能な情報の『全体的な混合』を著しく変更させたと、合理的な投資家が考えたであろう」場合に、重要である）。
2）Commission Statement and Guidance on Public Company Cybersecurity Disclosures（公開会社のサイバーセキュリティ開示に関する委員会声明及びガイダンス）、米国証券取引委員会 17 CFR Parts 229 and 249 [Release Nos. 33-10459; 34-82746]	2）サイバーセキュリティのリスク又はインシデントの重要性は、それらの性質、程度、及び潜在的な規模、特に侵害された情報、又はビジネス及び企業の業務範囲に関連するかどうかによって決まる。サイバーセキュリティのリスク及びインシデントの重要性は、そのようなインシデントが引き起こす可能性のある損害の範囲にも依存する。これには、企業の評判、財務実績、顧客及びベンダとの関係に対する損害のほか、米国州政府当局及び米国連邦政府当局、及び米国以外の当局による規制措置を含む、訴訟又は規制に関する調査又は措置の可能性が含まれる。
組織のユーザ（organizational user） [NIST SP 800-53 Rev. 5, adapted]	組織の従業員、又は組織が従業員と同等の地位にあると見なす個人で、例えば、請負業者、客員研究者、又は別の組織から特別に派遣された個人が含まれる。
オーバーレイ（overlay） [NIST SP 800-53 Rev. 5]	テーラリングプロセス中に採用される、セキュリティ又はプライバシー管理策、拡張管理策、補足ガイダンス、及びその他の補足情報の仕様であって、セキュリティ管理策ベースラインを補完（及び、さらに改良）することを目的としている。オーバーレイの仕様は、元のセキュリティ管理策ベースラインの仕様より厳しくても厳しくなくてもよく、複数の情報システムに適用することができる。
ペディグリー（pedigree）	技術、製品及びサービスの構成と来歴の検証（妥当性確認）をペディグリーと言う。マイクロエレクトロニクスのペディグリーには、コンポーネントの材料組成が含まれる。ソフトウェアのペデ

用語	定義
	ィグリーには、特定の時点におけるコンポーネントのバージョンを含むオープンソースコード及びプロプライエタリコードの構成が含まれる。ペディグリーは、サプライヤが提供する製品、サービス、及び技術の内部構成と来歴について主張する内容が有効であるというアシュアランスを強化する。
プログラムマネージャ（program manager）	システム所有者（*system owner*）を参照。
来歴（provenance） [NIST SP 800-53 Rev. 5]	システム又はシステムコンポーネント及び関連データの起源、開発、所有権、場所、及び変更の年表。また、システム、コンポーネント、又は関連データとやりとりする、又はそれらを変更するために使用される職員及びプロセスも含まれる場合がある。
残留リスク（residual risk） [NIST SP 800-16, adapted]	管理策／対策が適用された後に残留しているリスク。
リスク（risk） [NIST SP 800-39]	潜在的な状況又は事象によってエンティティが脅かされる度合いの指標であり、通常、以下に応じて変化する。（i）状況又は事象が発生した場合に生じる有害なインパクト、及び（ii）発生の可能性。
リスク選好度（risk appetite） [NISTIR 8286]	[組織]が価値を追求する上で進んで受容する、広いレベルでのリスクの種類及び量。
リスクフレーミング（リスクの枠組み）（risk framing） [NIST SP 800-39]	組織のリスクマネジメントアプローチを形成する、一連の仮定、制約条件、リスク許容度、及び優先順位／トレードオフ。
リスクマネジメント（risk management）	政府機関の業務（ミッション、機能、イメージ、評判を含む）、政府機関の資産、個人、他の組織、及び国家に対するリスクを管理するためのプログラム及びサポートプロセス。リスク関連活動の環境の確立、リスクのアセスメント、判定されたリスクへの対応、及びリスクの長期にわたる監視が含まれる。
リスク軽減（risk mitigation） [NIST SP 800-53 Rev. 5]	リスクマネジメントプロセスから推奨された適切なリスク低減管理策／対策の優先順位付け、評価、及び実施。

用語	定義
リスク対応（risk response） [NIST SP 800-53 Rev. 5, adapted]	特定されたリスクの受容、回避、軽減、共有、又は移転を行うための、意図的で情報に基づいた決定及び行動。
リスク対応計画（risk response plan）	脅威エージェントによる特定の脆弱性の悪用が成功した場合の潜在的な結果の概要、並びに軽減戦略及びC-SCRM 管理策。
リスク許容度（risk tolerance） [NIST 8286, adapted]	組織又はステークホルダーが目的を達成するために、リスクの対応後あるいは検討後に残るリスクを負う準備ができている度合い。
非公式市場（secondary market）	公式でない、認可されていない、又は意図されていない流通経路。
セキュリティ管理策（security control） [NIST SP 800-53 Rev. 5]	情報システム及びその情報の機密性、完全性、及び可用性を保護するために、情報システム又は組織に対して規定された予防手段又は対策。
ソフトウェア部品表（software bill of materials） Exec.Order No. 14028, supra note 1, § 10(j)	ソフトウェアの構築に使用される様々なコンポーネントの詳細、及びサプライチェーン関係を含む正式な記録。ソフトウェア開発者及びベンダは、既存のオープンソースソフトウェア及び商用ソフトウェアのコンポーネントを組み合わせて製品を作ることが多い。ソフトウェア部品表（SBOM）は、ある製品内のこれらのコンポーネントを列挙したものである。
サプライヤ（supplier） [ISO/IEC/IEEE 15288, adapted] [NIST SP 800-53 Rev. 5, adapted from definition of “developer”]	製品又はサービスの供給に関して、取得者又はインテグレータと契約を結ぶ組織又は個人。これには、サプライチェーン内のすべてのサプライヤ、システム、システムコンポーネント、又はシステムサービスの開発者又は製造業者、システムインテグレータ、サプライヤ、製品の再販業者、及びサードパーティのパートナーが含まれる。
サプライチェーン（supply chain） [ISO 28001, adapted]	製品及びサービスの調達から始まり、ライフサイクル全体に及ぶ、それぞれの組織が取得者である複数の階層の組織間におけるリソースとプロセスの一連の結びつき。

用語	定義
サプライチェーン要素（supply chain element）	システム及びシステムコンポーネントの研究開発、設計、製造、取得、納入、統合、運用及び保守、及び／又は廃棄に使用される組織、エンティティ、又はツール。
サプライチェーンリスク情報（supply chain risk information） [FASCA]	次のものを説明又は特定する情報を含むが、これらに限定されない。（1）データ及び情報システムの特権へのアクセスを含む対象品目の機能、（2）対象品目が使用又はインストールされるユーザ環境に関する情報、（3）供給源が対象品目を期待どおりに製造及び納入できる能力（すなわち、サプライチェーンアシュアランス）、（4）供給源に対する外国の支配又は影響（例：外国の所有権、供給源と外国のエンティティの間における公私にわたる結びつき、供給源が本社を置く又は事業を行う外国の法体制）、（5）対象供給源の使用に関連する、国家安全保障、国土安全保障、及び／又は国家の重要機能への影響、（6）連邦政府のシステム、プログラム、又は施設の脆弱性、（7）対象供給源の代替となる市場、（8）組織の業務又はミッションに対する、製品、材料、又はサービスの損失、損傷、又は侵害による潜在的なインパクト又は損害、（9）潜在的なインパクト又は損害の起こりやすさ、又はシステムの悪用可能性、（10）対象品目及びその供給及び編成のチェーンのセキュリティ、真正性、完全性、（11）特定されたリスクを軽減する能力、（12）他のサプライチェーンリスク情報の信ぴょう性と信頼性、（13）対象品目又は対象供給源のセキュリティ、完全性、レジリエンス、品質、統合的信頼性、又は真正性の分析に考慮に入れるその他のあらゆる情報、（14）上記の情報の要約、及びサプライチェーンリスクの決定に関連すると判断されるその他の情報。
システム（system） [NIST SP 800-53 Rev. 5, adapted]	1つ以上の明示された目的を達成するために編成された、相互作用する要素の組み合わせ。 注 *1*：システムには多くの種類がある。例えば、汎用及び特殊用途の情報システム、指令・制御・通信システム、暗号モジュール、中央処理装置（CPU）及びグラフィックスプロセッサボード、産業用制御システム、飛行制御システム、武器、標的、及び射撃管制システム、医療機器及び治療システム、金融・銀行・商品取引システム、ソーシャルネットワーキングシステムなどがある。 注 *2*：システムの定義における相互作用要素には、ハードウェ

用語	定義
	ア、ソフトウェア、データ、人間、プロセス、設備、材料、及び自然発生の物理的エンティティが含まれる。 注 *3*：システムの定義には、システム・オブ・システムズが含まれる。
システムアシュアランス（system assurance） [NDIA]	システムが意図したとおりに機能し、意図的か非意図的かを問わず、ライフサイクルのどの時点にもシステムの一部として設計又は挿入された悪用可能な脆弱性がないという、根拠ある確証。
システムコンポーネント（system component）	システムの構成要素を表す個別の特定可能な情報技術資産又は制御・運用技術資産。ハードウェア、ソフトウェア、及びファームウェアを含む可能性がある。
システム開発ライフサイクル（system development life cycle） [NIST SP 800-34 Rev. 1, adapted]	システムに関連する活動の範囲。システムの開始、開発と取得、実装、運用及び保守、及び最終的な廃棄を含む。
システムインテグレータ（system integrator）	カスタム開発、テスト、運用、及び保守など、カスタマイズされたサービスを取得者に提供する組織。
システム所有者（又はプログラムマネージャ）（system owner (or program manager)） [NIST SP 800-53 Rev. 5]	システムの調達、開発、統合、変更、又は運用及び保守全般に責任を持つ担当者。
脅威（threat） [NIST SP 800-53 Rev. 5]	情報の不正アクセス、破壊、漏えい、改ざん、及び／又はサービス妨害によって、システムを通じて組織の業務、組織の資産、個人、他の組織、又は国家に有害なインパクトをもたらす可能性のある状況又は事象。
脅威分析（threat analysis）	脅威アセスメント（*threat assessment*）を参照。
脅威アセスメント（threat assessment） [NIST SP 800-53 Rev. 5, adapted]	システム又は組織に対する脅威の正式な記述及び評価。

用語	定義
脅威事象（threat event） [NIST SP 800-30 Rev. 1]	望ましくない結果又はインパクトを引き起こす可能性のある事象又は状況。
脅威事象の結果（threat event outcome）	脆弱性に作用する脅威が、組織の業務、資産、又は個人の機密性、完全性、及び／又は可用性に及ぼす影響。
脅威のシナリオ（threat scenario） [NIST SP 800-30 Rev. 1]	ある特定の脅威源、又は複数の脅威源に関連付けられた、部分的に時系列で順序付けられた、一連の個別の脅威事象。
脅威源（threat source） [NIST SP 800-53 Rev. 5]	脆弱性を意図的に悪用することを目的とした意図及び方法、又は偶発的に脆弱性をもたらす可能性がある状況及び方法。
透明性（transparency）	可視性（*visibility*）を参照。
信頼（trust） [SwA]	ある要素が別の要素に対して持つ、その別の要素が期待どおりに振る舞うであろうという信頼。
統合的信頼性（trustworthiness） [NIST SP 800-53 Rev. 5, adapted]	特定のタスクを実行し、割り当てられた責任を果たすための、当該エンティティの資格、ケイパビリティ、及び信頼性についての信用を他者に与える人、システム、又は事業体の属性の相互依存的な組み合わせ。システム（システムの構築に使用される技術コンポーネントを含む）が、あらゆる脅威に対して、そのシステムによって処理、保存、又は伝送される情報の機密性、完全性、及び可用性を維持することが期待できる度合い。
妥当性確認（validation） [ISO 9000]	客観的証拠を提示することによって，特定の意図された使用又は適用に関する要件が満たされていることを確認すること。 注：要件が満たされた。
検証（verification） [CNSSI 4009] [ISO 9000, adapted]	客観的証拠を提示することによって、規定された要件が満たされていることを確認すること。 注：意図されたアウトプットが正しい。
可視性（visibility） [ISO/IEC 27036, adapted]	サプライヤ、製品、又はサービスについて収集できる情報の量、及び、サプライチェーンを通じてどの程度までこの情報を取得できるかの度合い。

用語	定義
脆弱性（vulnerability） [NIST SP 800-53 Rev. 5]	脅威源によって悪用又はもたらされる可能性がある、情報システム、システムセキュリティ手順、内部管理策、又は実装における弱点。
脆弱性アセスメント（vulnerability assessment）[NIST SP 800-53 Rev. 5, adapted]	セキュリティ対策の妥当性を判定し、セキュリティの欠陥を特定し、提案されたセキュリティ対策の有効性を予測するためのデータを提供し、実装後にそのような対策の妥当性を確認するための、システム、製品又はサプライチェーンの要素の体系的な検査。

附属書 I：略語

A&A アセスメント及び認可（Assessment and Authorization）

AO 認可権限のある担当者（Authorizing Official）

API アプリケーション・プログラミング・インタフェース（Application Programming Interface）

APT 持続的標的型攻撃（APT 攻撃）（Advanced Persistent Threat）

BIA ビジネスインパクト分析（Business Impact Analysis）

BYOD 個人所有デバイスの持ち込み（Bring Your Own Device）

CAC 共通アクセスカード（Common Access Card）

CAO 最高取得責任者（Chief Acquisition Officer）

CEO 最高経営責任者（Chief Executive Officer）

CFO 最高財務責任者（Chief Financial Officer）

CIO 最高情報責任者（Chief Information Officer）

CISA サイバーセキュリティ・インフラストラクチャセキュリティ庁（Cybersecurity and Infrastructure Security Agency）

CISO 最高情報セキュリティ責任者（Chief Information Security Officer）

CISS サイバーインシデント深刻度判断基準（Cyber Incident Severity Schema）

CLO 最高法務責任者（Chief Legal Officer）

COO 最高執行責任者（Chief Operating Officer）

CPO 最高プライバシー保護責任者（Chief Privacy Officer）

CRO 最高リスク管理責任者（Chief Risk Officer）

CSO 最高セキュリティ責任者（Chief Security Officer）

CTO 最高技術責任者（Chief Technology Officer）

CNSS 国家安全保障システム委員会（Committee on National Security Systems）

CNSSI 国家安全保障システム委員会指示（Committee on National Security Systems Instruction）

CONUS 米国本土（Continental United States）

COSO トレッドウェイ委員会支援組織委員会（Committee of Sponsoring Organizations of the Treadway Commission）

COTS 市販品（商用オフザシェルフ）（Commercial Off-The-Shelf）

CRO 最高リスク管理責任者（Chief Risk Officer）

C-SCRM サプライチェーンのサイバーセキュリティリスクマネジメント（Cybersecurity Supply Chain Risk Management）

CSF サイバーセキュリティフレームワーク（Cybersecurity Framework）

CUI 管理対象非機密情報（Controlled Unclassified Information）

CVE 共通脆弱性タイプ一覧（Common Vulnerability Enumeration）

CVSS 共通脆弱性評価システム（Common Vulnerability Scoring System）

CWE 共通弱点タイプ一覧（Common Weakness Enumeration）

DHS 国土安全保障省（Department of Homeland Security）

DMEA 国防総省マイクロエレクトロニクスアクティビティ（Defense Microelectronics Activity）

DoD 国防総省（Department of Defense）

DODI 国防総省訓令（Department of Defense Instruction）

ERM エンタープライズリスクマネジメント（Enterprise Risk Management）

ERP エンタープライズリソースプランニング（Enterprise Resource Planning）

FAR 連邦調達規則（Federal Acquisition Regulation）

FARM 枠組み化、アセスメント、対応、監視（Frame, Assess, Respond, Monitor）

FASC 連邦調達安全保障会議（Federal Acquisition Security Council）

FASCA 連邦調達サプライチェーンセキュリティ法（Federal Acquisition Supply Chain Security Act）

FBI 連邦捜査局（Federal Bureau of Investigation）

FedRAMP 連邦リスク承認管理プログラム（Federal Risk and Authorization Management Program）

FIPS 連邦情報処理規格（Federal Information Processing Standards）

FISMA 連邦情報セキュリティマネジメント法（Federal Information Security Management Act）

FITARA 連邦 IT 調達改革法（Federal Information Technology Acquisition Reform Act）

FOCI 外国人による所有、管理、又は影響（Foreign Ownership, Control or Influence）

FSP 金融サービスのサイバーセキュリティフレームワークプロファイル（Financial Services Cybersecurity Framework Profile）

GAO 会計検査院（Government Accountability Office）

GIDEP 政府・業界間データ交換プログラム（Government-Industry Data Exchange Program）

GOTS 政府調達向け既製品（Government Off-The-Shelf）

GPS グローバル・ポジショニング・システム（Global Positioning System）

HR 人事（Human Resources）

IA 情報アシュアランス（Information Assurance）

ICT 情報通信技術（Information and Communication Technology）

ICT/OT 情報通信及び制御・運用技術（Information, communications, and operational technology）

IDE 統合開発環境（Integrated Development Environment）

IDS 侵入検知システム（Intrusion Detection System）

IEC 国際電気標準会議（International Electrotechnical Commission）

IOT モノのインターネット（Internet of Things）

IP インターネットプロトコル（Internet Protocol）／知的財産（Intellectual Property）

ISA 情報共有機関（Information Sharing Agency）

ISO/IEC 国際標準化機構（International Organization for Standardization）／国際電気標準会議（International Electrotechnical Commission）

IT 情報技術（Information Technology）

ITIL IT インフラストラクチャ・ライブラリ（Information Technology Infrastructure Library）

ITL 情報技術研究所（NIST）（Information Technology Laboratory (NIST)）

JWICS 統合世界情報通信システム
（Joint Worldwide Intelligence Communications System）

KPI 重要業績評価指標（Key Performance Indicators）

KRI 重要リスク指標（Key Risk Indicators）

KSA 知識、スキル、及び能力（Knowledge, Skills, and Abilities）

MECE 相互に排他的な項目による完全な全体集合
（Mutually Exclusive and Collectively Exhaustive）

NISPOM 国家産業保全プログラム運用マニュアル
（National Industrial Security Program Operating Manual）

NIST 米国国立標準技術研究所（National Institute of Standards and Technology）

NCCIC 国家サイバーセキュリティ・通信統合センター
（National Cybersecurity and Communications Integration Center）

NDI 非開発項目（Non-developmental Items）

NDIA 国防産業協会（National Defense Industrial Association）

NIAP 国家情報アシュアランスパートナーシップ
（National Information Assurance Partnership）

NICE サイバーセキュリティ教育のための国家計画
（National Initiative for Cybersecurity Education）

NISTIR NIST 省庁間又は内部レポート（National Institute of Standards and Technology Interagency or Internal Report）

OCONUS 米国本土外（Outside of Continental United States）

OEM 相手先ブランド製造業者（Original Equipment Manufacturer）

OGC 法律顧問室（Office of the General Counsel）

OMB 行政管理予算局（Office of Management and Budget）

OPSEC 運用セキュリティ（Operations Security）

OSS オープンソースソリューション（Open Source Solutions）

OSY セキュリティ局（Office of Security）

OT 制御・運用技術（Operations Technology）

OTS 既製品（Off-The-Shelf）

OTTF オープングループ高信頼性技術フォーラム
（Open Group Trusted Technology Forum）

O-TTPS Open Trusted Technology Provider™ 規格
（Open Trusted Technology Provider™ 規格）

OWASP オープン・ウェブ・アプリケーション・セキュリティ・プロジェクト
（Open Web Application Security Project）

PACS 物理的アクセス制御システム（Physical Access Control System）

PII 個人を識別／特定できる情報（Personally Identifiable Information）

PIV 個人アイデンティティ検証（Personal Identity Verification）

PM プログラムマネージャ（Program Manager）

PMO プログラムマネジメントオフィス（Program Management Office）

POA&M 行動計画及びマイルストーン（Plan of Action & Milestones）

QA/QC 品質保証／品質管理（Quality Assurance/Quality Control）

R&D 研究開発（Research and Development）

RFI 情報提供依頼書（Request for Information）

RFP 提案依頼書（Request for Proposal）

RFQ 見積依頼書（Request for Quote）

RMF リスクマネジメントフレームワーク（Risk Management Framework）

SAFECode コードの卓越性実現に向けたソフトウェアアシュアランスフォーラム
（Software Assurance Forum for Excellence in Code）

SBOM ソフトウェア部品表（Software Bill of Materials）

SCIF 機密情報隔離施設（Sensitive Compartmented Information Facility）

SCRI サプライチェーンリスク情報（Supply Chain Risk Information）

SCRM サプライチェーンのリスクマネジメント（Supply Chain Risk Management）

SCRSS サプライチェーンリスク深刻度判断基準（Supply Chain Risk Severity Schema）

SDLC **システム開発ライフサイクル（System Development Life Cycle）**

SECURE **リスク曝露（エクスポージャー）技術の活用法によるサイバーケイパビリティ（能力）の強化及び向上（技術関連法）（Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (Technology Act)）**

SLA **サービスレベル合意書（Service-Level Agreement）**

SME **特定分野専門家（Subject Matter Expert）**

SOO **業務趣意書（Statement of Objective）**

SOW **作業ステートメント（Statement of Work）**

SP **特別出版物（NIST）（Special Publication (NIST)）**

SSP **システムセキュリティ計画（System Security Plan）**

SWA **ソフトウェアアシュアランス（Software Assurance）**

SWID **ソフトウェア識別タグ（Software Identification Tag）**

TTP **戦術、技術、及び手順（Tactics, Techniques, and Procedures）**

U.S. **（アメリカ）合衆国（United States (of America)）**

US CERT **米国コンピュータ緊急対応チーム（United States Computer Emergency Readiness Team）**

VDR **脆弱性開示報告書（Vulnerability Disclosure Report）**

附属書 J：リソース

他のプログラム及び出版物との関係

NIST SP 800-161 の本改訂版は、政府機関による既存の事業体全体の活動、及び、NIST SP 800-161 の初回公開後に行われた一連の法律策定との統合を容易にするために、数々の NIST 出版物及びその他の出版物で説明されている概念を基にしている。これらのリソースは相互に補完し合い、事業体が、多様でますます高度化する広範な脅威から業務及び資産を保護するためにリスクベースの情報セキュリティプログラムを構築するのに役立つ。本出版物は、C-SCRM 分野が成熟し続けるのに伴い、NIST SP 800-53 のセキュリティ管理策カタログとの整合性を保つために反復プロセスを使用して改訂される予定である。

NIST 出版物

本出版物は、以下のような、初回策定の手引きとなった出版物及びプログラムの最新版、並びに、初回公開後に策定された新しい出版物を活用している。

- NIST サイバーセキュリティフレームワーク（CSF）バージョン 1.1（NIST Cybersecurity Framework (CSF) Version 1.1）
- 重要度分析、及び、高インパクトコンポーネント又はシステムに対する C-SCRM 活動のスコーピングを実施するための連邦情報処理規格（FIPS：Federal Information Processing Standards）199、連邦政府の情報および情報システムに対するセキュリティ分類規格（*Standards for Security Categorization of Federal Information and Information Systems*）[FIPS 199]
- ICT/OT の SCRM をリスクアセスメントプロセスに統合するための NIST SP 800-30, Rev. 1、リスクアセスメントの実施の手引き（*Guide for Conducting Risk Assessments*）[NIST SP 800-30, Rev. 1]
- NIST SP 800-37, Rev. 2、情報システム及び組織のためのリスクマネジメントフレームワーク：セキュリティ及びプライバシーのためのシステムライフサイクルアプローチ（*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*）[NIST SP 800- 37, Rev. 2]
- ICT/OT の SCRM をリスクマネジメントレベル及びリスクマネジメントプロセスに統合するための NIST SP 800-39、情報セキュリティリスクの管理：組織、ミッション、及び情報システムの観点（*Managing Information Security Risk: Organization, Mission, and Information System View*）[NIST SP 800-39]
- C-SCRM のコンテキストに合わせて強化及びテーラリングする情報セキュリティ管理策を提供するための NIST SP 800-53, Rev. 5、組織と情報システムのためのセキュリティおよびプライバシー管理策（*Security and Privacy Controls for Information Systems and Organizations*）[NIST SP 800-53, Rev. 5]
- 管理策ベースライン及び C-SCRM の補助的ガイダンスを体系化するための NIST SP 800-53B、組織と情報システムのための管理策ベースライン（*Control Baselines for Information Systems and Organizations*）[NIST SP 800-53B]
- サイバー脅威情報共有関係の確立及び参加のガイドラインを提供するための NIST SP 800-150、サイバー脅威情報の共有のためのガイド（*Guide to Cyber Threat Information Sharing*）[NIST SP 800- 150]

- C-SCRM のセキュリティエンジニアリングの側面に関する具体的なガイダンスについては、NIST SP 800-160 Vol. 1、システムセキュリティエンジニアリング（*Systems Security Engineering*）[NIST SP 800-160 Vol. 1] 及び NIST SP 800-160 Vol. 2, Rev. 1、サイバーレジリエントなシステムの開発：システムセキュリティエンジニアリングアプローチ（*Developing Cyber Resilient Systems: A Systems Security Engineering Approach*）[NIST SP 800-160 Vol. 2]
- CUI の機密性保護のための推奨されるセキュリティ要件については、NIST SP 800-171, Rev. 2、非連邦政府組織およびシステムにおける管理対象非機密情報（*CUI*）の保護（*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*）[NIST SP 800-171, Rev. 2]
- CUI の機密性保護のための推奨される拡張セキュリティ要件については、NIST SP 800-172、管理対象非機密情報を保護するための拡張セキュリティ要件 - *NIST SP 800-171* の補足（*Enhanced Security Requirements for Protecting Controlled Unclassified Information – A Supplement to NIST Special Publication 800-171*）[NIST SP 800-172]
- C-SCRM ワークフォースに関するトピックの共通用語集を形成する手段としての NIST SP 800-181, Rev. 1、サイバーセキュリティ教育のための国家計画（*NICE*）サイバーセキュリティワークフォースフレームワーク（*National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*）[NIST SP-800-181, Rev. 1]
- 本 Special Publication を連邦政府情報システム特有の取得プロセスに適用することの裏付けとなる参考資料については、NISTIR 7622、連邦政府情報システムのための概念的なサプライチェーンのリスクマネジメントプラクティス（*Notional Supply Chain Risk Management Practices for Federal Information Systems*）[NISTIR 7622]
- サプライヤの重要度の評価を手引きするための NISTIR 8179、重要度分析プロセスモデル：システム及びコンポーネントの優先順位付け（*Criticality Analysis Process Model: Prioritizing Systems and Components*）[NISTIR 8179]
- 民間分野における最近の C-SCRM の傾向を解明するための NISTIR 8276、サプライチェーンのサイバーリスクマネジメントにおける重要なプラクティス：業界からの意見（*Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*）[NISTIR 8276]
- エンタープライズリスクマネジメントへの C-SCRM の統合に関する内容に情報を提供するための NISTIR 8286、エンタープライズリスクマネジメント（*ERM*）のためのサイバーセキュリティリスクの識別及び見積（*Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*）[NISTIR 8286]

規制及び法律によるガイダンス

本出版物は、以下を含む規制及び法律によるガイダンスから大いに情報を得ている。

- 行政管理予算局（OMB：Office of Management and Budget）通達（Circular）A-123 号、内部統制に対する管理者の責任（*Management's Responsibility for Internal Control*）
- 行政管理予算局（OMB）通達 A-130 号、戦略的リソースとしての情報の管理（*Managing Information as a Strategic Resource*）

- 連邦調達サプライチェーンセキュリティ法（FASCA：Federal Acquisition Supply Chain Security Act）、リスクレベルの利用によるサイバーケイパビリティ（能力）の強化及び向上に関する技術関連法（*SECURE*）、*2018* 年の技術関連法の第 *II* 章（*Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act of 2018*）（*2018*）
- 公法（Public Law） 115 条 –232 条第 889 節、特定の通信及び動画監視サービス又は機器の禁止（*Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment*）
- 連邦官報（Federal Register）、第 84 巻、第 156 号、特定の通信及び動画監視サービス又は機器の契約禁止（*Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment*）、2019 年 8 月 13 日
- 連邦調達規則（FAR：Federal Acquisition Regulations）パート 4、サブパート 4.20、*Kaspersky Lab* によって開発又は提供されるハードウェア、ソフトウェア、及びサービスの契約禁止（*Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab*）
- 会計検査院（GAO：Government Accountability Office）、オフショア及び外国投資リスクに関する課題及びポリシーの考慮事項（*Challenges and Policy Considerations Regarding Offshoring and Foreign Investment Risks*）、2019 年 9 月
- 大統領令（Executive Order）14028 号、国家のサイバーセキュリティの向上（*Improving the Nation's Cybersecurity*）、2021 年 5 月 12 日
- 証券取引委員会（Securities and Exchange Commission）17 CFR Parts 229 and 249[Release Nos. 33- 10459; 34-82746]公開会社のサイバーセキュリティ開示に関する委員会声明及びガイダンス（*Commission Statement and Guidance on Public Company Cybersecurity Disclosures*）

その他の米国政府報告書

本出版物は、以下の補足的な政府報告書からも情報を得ている。

- 会計検査院（GAO）報告書、情報技術：連邦政府機関によるサプライチェーンリスク管理のための緊急措置実施の必要性（*Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*）、2020年 12 月、GAO-21-171[GAO]
- 国防総省（Department of Defense）及び国土安全保障省（Department of Homeland Security）によるソフトウェアアシュアランス取得ワーキンググループ、取得におけるソフトウェアアシュアランス：事業体へのリスクの軽減（*Software Assurance in Acquisition: Mitigating Risks to the Enterprise*）[SwA]
- 国防産業協会（NDIA：National Defense Industrial Association）、システムアシュアランスのためのエンジニアリング（*Engineering for System Assurance*）[NDIA]

標準、ガイドライン、及びベストプラクティス

[NIST SP 800-161]は、以下を含む数々の国際標準、ガイドライン、及びベストプラクティス文書からも着想を得ている。

- 連邦リスク承認管理プログラム（FedRAMP：Federal Risk and Authorization Management Program）、連邦政府のためのクラウドサービスのセキュア化（*Securing Cloud Services For The Federal Government*）[https://www.fedramp.gov/]
- 国際標準化機構／国際電気標準会議（ISO/IEC：International Organization for Standardization/International Electrotechnical Commission）15288 – システム及びソフトウェア技術 – システムライフサイクルプロセス（*Systems and software engineering – System Life Cycle Processes*）[ISO/IEC 15288]
- ISO/IEC 27036 – 情報技術 – セキュリティ技術 – サプライヤとの関係のための情報セキュリティ（*Information Technology – Security Techniques – Information Security for Supplier Relationships*）[ISO/IEC 27036]
- ISO/IEC 20243 – 情報技術 – *Open Trusted Technology ProviderTM* 規格（*O-TTPS*）– 悪意を持って汚染された製品及び偽造品の製品による影響の軽減（*Information Technology – Open Trusted Technology ProviderTM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*）[ISO/IEC 20243]
- ISO/IEC 27000 – 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム – 用語（*Information Technology – Security Techniques – Information Security Management System – Overview and Vocabulary*）[ISO/IEC 27000]
- ISO/IEC 27002 – 情報技術 – セキュリティ技術 – 情報セキュリティ管理策の実践のための規範（*Information Technology – Security Techniques – Code of Practice for Information Security Controls*）[ISO/IEC 27002]
- コードの卓越性実現に向けたソフトウェアアシュアランスフォーラム（SAFECode：Software Assurance Forum for Excellence in Code）によるソフトウェア完全性フレームワーク（*Software Integrity Framework*）[SAFECode 2]及びソフトウェア完全性のベストプラクティス（*Software Integrity Best Practices*）[SAFECode 1]
- サイバーリスク協会（Cyber Risk Institute）、金融サービスのサイバーセキュリティフレームワークプロファイル バージョン *1.1*（*Financial Services Cybersecurity Framework Profile Version 1.1*）[FSP]