2019 年 6 月 25 日

独立行政法人情報処理推進機構（IPA）

欧州ネットワーク情報セキュリティ機関（ENISA）
「インダストリー4.0 サイバーセキュリティ：課題と提言」

This is a translation undertaken by IPA and therefore is not official translation of ENISA.
The official version is in English and on the ENISA site http://www.enisa.europa.eu/

本文書は、ENISA の文書 “Industry 4.0 - Cybersecurity Challenges and Recommendations” を独立行政法人 情報処理推進機構（IPA）が翻訳したものであり、ENISA による公式の翻訳ではありません。日本語へ翻訳した本文書の著作権は、IPA に帰属します。
本文書は、原文にできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体である IPA は、本翻訳文書に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。原文のありのままの内容を理解する必要のある場合は、ENISA ウェブサイトに掲載されている原文をお読み下さい。

Industry 4.0 - Cybersecurity Challenges and Recommendations
https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

Copyright © 2019 独立行政法人情報処理推進機構

ENISA は、インダストリー4.0 のサイバーセキュリティを促進し、関連するイノベーションをセキュアな方法で幅広く普及させるために、様々な利害関係者グループへの概念レベルの提言を本文書に記す。

Copyright © 2019 独立行政法人情報処理推進機構

1. はじめに

この文書は、インダストリー4.0 および産業用 IoT(IIoT)のセキュリティ/セキュリティ対策の採用における主な課題を特定するために実施されたギャップ分析の結果を提供する。

ENISA の調査「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」[1]は、IoT のイノベーションの導入によってもたらされた産業システム/サービスの進化に関連するセキュリティおよびプライバシーの課題に取り組むことにフォーカスしている。その主な目的は、関連するセキュリティとプライバシーの課題、脅威、リスクおよび攻撃シナリオをマッピングし、インダストリー4.0/スマートマニュファクチャリングの IoT セキュリティを確保するグッドプラクティスを集めることである。

この文書はその調査に基づいて、インダストリー4.0 および産業用 IoT のセキュリティやセキュリティ対策の採用における主な課題を特定するために実施されたギャップ分析の結果を提供している。さらにインダストリー4.0 のサイバーセキュリティおよび関連するイノベーションをセキュアな方法で幅広く普及することを促進するために、異なる利害関係者グループへの概念レベルの提言を記載している。

この ENISA からの概念レベルの提言の採用は、EU 全体へのインダストリー4.0 サイバーセキュリティの拡大への貢献、今後発生する関連作業の土台の構築、および将来の開発の基礎の提供を目的としている。

この文書において ENISA は、インダストリー4.0 のサイバーセキュリティに関連する問題へ全体的かつ包括的にアプローチしており、「人」、「プロセス」および「技術」のカテゴリー毎に「課題」と「提言」を関連付けている。これは ENISA の調査「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」との一貫性を保っている。さらに「提言」は、課題に取り組む対象読者単位で分類される。（下図の 5 つの利害関係者グループのアイコンがガイダンスとして使用される。「提言」に引き続くアイコンは、その「提言」がアイコンの示す利害関係者グループに対するものであることをあらわす。）

[1] ENISA "Good Practices for Security of IoT in the context of Smart Manufacturing"
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot（2018 年 11 月）
*IPA による翻訳版：https://www.ipa.go.jp/files/000073490.pdf

Copyright © 2019 独立行政法人情報処理推進機構

2. 人

インダストリー4.0の出現によって、旧来のOT環境に新しい技術がもたらされる。したがって、そのような環境で働く OT に精通した人々は、変化に適応していく必要がある。

課題：IT/OT セキュリティの専門知識・意識を醸成、連携する必要がある

情報セキュリティの専門知識および意識の不足は、インダストリー4.0 のセキュリティ対策の採用を妨げる大きな障壁となっている。新たなソリューションの展開に携わる人々が、IT セキュリティまたは OT セキュリティのいずれかの知識しか持っていないということがよくある。しかし、インダストリー4.0 とスマートマニュファクチャリングは複数の分野にまたがる専門知識を必要としている。（例えば、ネットワーク・セキュリティ、組込システム、OT/IT セキュリティなど。）セキュリティの問題をきちんと理解している、能力のあるスペシャリストを探すことは非常に難しくなっている。

インダストリー4.0 の出現は、旧来の OT 環境に新しい技術をもたらしているが、そうした環境で働く OT に精通した人々は、変化に適応していく必要がある。これらの人々は、OT 環境を長期にわたってどう運用するかという知識はあるが、今日では旧来のやり方を変え新しいインダストリー4.0 の機能を受け入れる必要がある。そのような技術をよく知らないということは、スマートマニュファクチャリングにおけるインダストリー4.0 ソリューションのセキュアな利用に重要となる「新たな能力」に欠けた従業員ということになる。その「新たな能力」には、とりわけ下記が含まれる。

- セキュリティ違反による異常をモニター、防御、検知するため制御セキュリティの知識とスキル
- インダストリー4.0 ソリューションで用いられる新しいプロトコルのセキュリティ側面
- コンポーネントやサービスのセキュリティ機能を使うためのスキル（十分な説明がなされていないと、ユーザーにとっては非常に複雑に思える）
- レガシーなシステムとのセキュアな統合の方法
- 複雑なサプライチェーンにおける情報システムのセキュリティ

さらに、大規模な製造企業は、OT 機器を使用する従業員のトレーニングに遅れをとっていることがよくある。それどころか、最初に従業員が使いこなせるかどうか確認せずに、インダストリー4.0 のセキュリティソリューションを採用している。また、IT/OT コンバージェンス（融合）とインダストリー4.0 システムに特化した最新のサイバーセキュリティ・トレーニングは限られた数しかなく、そのようなトレーニングは多くの場合、これらの領域のすべての重要な側面をカバーしておらず、非常に高価で、また特定の産業分野のニーズに合っていない。

Copyright © 2019 独立行政法人情報処理推進機構

提言：IT および OT セキュリティの分野横断的（cross-functional）な知識の習得を促進する

基本的な産業制御のセキュリティとインダストリー4.0/スマートマニュファクチャリングへのセキュアな移行方法についての意識を高めることが最も重要である。IoT とインダストリー4.0 のセキュリティに詳しい人材の不足に対処するには、そのような知識を組織の内外で培うことが不可欠である。インダストリー4.0 組織内のセキュリティ担当者は、IT/OT コンバージェンスおよびスマートマニュファクチャリングに必要なすべての側面を網羅する最先端のサイバーセキュリティ・トレーニングを受ける必要がある。また、学校や大学でのトレーニングや講座（より多くの人に届くようローカライズを検討する）は、若い世代のインダストリー4.0 セキュリティの理解を深めることになるため、長期的には意識の向上に貢献するだろう。

IT および OT セキュリティの分野横断的な知識の習得を促進するための ENISA の提言は下記のとおりである。

- IT および OT の専門家間での分野横断的なセキュリティおよびセーフティ知識の交換を促進する。
- 最先端技術、ベストプラクティス、IT/OT システムをセキュアに統合するための方法論およびツールに関する知識を含む、インダストリー4.0 へ移行する業界におけるセキュリティ教育/トレーニングを立ち上げる。
- トレーニングの有効性を高め、関連するサイバーセキュリティの問題に OT/IT セキュリティ専門家がさらに効率的に対処できるように、インダストリー4.0 セキュリティに焦点を当てたオーダーメイドのトレーニングコースをつくる。
- すべてのスタッフに IoT およびインダストリー4.0 固有の認識および教育/トレーニングを提供するためのコンピテンシー（能力）・プロファイルを作成する。
- 業界全体のセキュリティとセーフティに関する知識の不足に対処し、次世代の IT および OT セキュリティ専門家を育成するためのプログラムを、学校や大学で導入する。
- OT 要員のためのサイバー・カルチャーおよびサイバー衛生（cyber-hygiene [訳注]個人のセキュリティ認識を醸成する取組み）の入門コースを編成する。逆に、IT 要員やすべてのスタッフのためのセーフティ・カルチャーおよびセーフティ衛生（safety-hygiene [訳注] 個人のセーフティ認識を醸成する取組み）のコースを編成する。OT 要員にはセキュリティの概念を、そして IT 要員にはセーフティの概念を、それら 2 つの概念がうまく連携できるところ、できないところについて特に言及しつつ紹介する。

Copyright © 2019 独立行政法人情報処理推進機構

インダストリー4.0 導入の様々な段階にあるインダストリー4.0 のオペレータは、新しい技術のセキュアな実装と既存の技術のセキュアなメンテナンスのための適切なガバナンス体制を整備していないことがよくある。

課題：組織のポリシーが不完全で、セキュリティへの投資に消極的である

インダストリー4.0 導入の様々な段階にあるインダストリー4.0 のオペレータは、新しい技術のセキュアな実装と既存の技術のセキュアなメンテナンスのための適切なガバナンス体制を整備していないことがよくある。定義されたセキュリティプログラムが整備されていることはまれで、一般的にセキュリティとセーフティがともに考慮されている包括的なプログラムの整備は不足している。また、セキュリティに関する従業員の役割と責任が明確に定義されておらず、サイバーセキュリティ・エコシステムの中でセーフティ担当者を考慮した最低限のプランがあるだけである。これによって、企業のレジリエンスの不足と潜在的なセキュリティ侵害に対する脆弱性を招いている。

これはサイバーセキュリティが収益拡大やコスト削減へ及ぼす影響が不明瞭なため、企業の取締役会レベルのトピックとしてこれまで認識されてこなかったことが原因である。実際多くの技術革新は、サイバーセキュリティよりも拡張される機能やビジネス上の価値にフォーカスしている。（言い換えれば、技術革新に関連するリスクの潜在的な悪影響を後回しにしている。）典型的な例は、クラウドへの移行が進行中の製造企業である。一般的にこうした企業は、コスト削減や情報へのユビキタスなアクセスの恩恵を受けるためにクラウドソリューションの採用を決定する。この移行において、セキュリティは高いプライオリティの課題として考慮されるべきであり、意思決定やコスト削減同様、重要な役割を果たすべきである。特に、製造企業がパブリッククラウドを選択した場合には、企業のレジリエンスが高まる一方、データやオペレーションが漏洩するリスクが増大する。

さらに、インダストリー4.0 ベンダー/オペレータでは、システムやソリューションのセキュリティの確保は、トップレベル・マネジメント（経営層）のコミットメントおよび予算の確保を必要とするということは強調しておく価値がある。しかしながら、サイバーセキュリティへの投資が利益を生み出すということへの目に見える明確な関連性がないため、セキュリティ侵害によって直接経済的損失を被った際にはじめて、サイバーセキュリティへの十分な考慮がなされるということがよくある。コストとセキュリティの必要性との適切なバランスを取り決めることは、依然課題となっている。

Copyright © 2019 独立行政法人情報処理推進機構

サイバーセキュリティへの投資は、経済的損失への恐れだけで決定されるべきではない。産業や組織にとって、サイバーセキュリティを単なるコストと見なすだけではなく、重要なビジネスチャンスと見なすことも同様に重要である。

提言：インダストリー4.0 セキュリティの経済的および経営上のインセンティブを促進する

セキュリティの不足がビジネスの継続性に影響を与えることは明白である。インダストリー4.0も、関連するオペレーションの重要性や関連するセーフティへの影響を考えると、例外ではない。この点において、ビジネス継続性のためのベストプラクティスは、サイバーセキュリティ・ソリューションへの投資を促し、インダストリー4.0 の妨げのないオペレーションをサポートするための原動力となる。

サイバーセキュリティへの投資は経済的損失への恐れだけで決定されるべきではない。産業界や組織にとって、サイバーセキュリティを単なるコストとして見なすだけではなく、重要なビジネスチャンスであると見なすことも同様に重要である。サイバーセキュリティはセキュアで信頼・信用のおける製品やサービスの提供につながるので、ビジネスにおいて重要な競争上の強みとなる。したがって、サイバーセキュリティはビジネスチャンスを妨げる因子ではなくビジネスに必要な因子である。

とはいえ、セキュリティの役割と重要性を特定するためには、組織やビジネスの成熟度とメンタリティをさらに高める必要があることを考えると、インダストリー4.0 セキュリティへの投資を奨励するために、経済的および行政的刺激策も必要である。

インダストリー4.0 セキュリティの経済的および行政上のインセンティブを奨励するために ENISA は以下のことを推奨する。

- トップレベル・マネジメント（経営層）がサイバーセキュリティの専門家や CISO（Chief Information Security Officer 最高情報セキュリティ責任者）と議論や意見交換できる管理体制を確立する。
- 財政支援や連携活動を含む、中小企業のための予算獲得スキームや、セキュアなインダストリー4.0 エコシステムへの移行をサポートする団体を創設する。
- IT/OT 環境、コンポーネント、およびシステムのイノベーションや研究開発活動を奨励する。
- 企業がセキュリティの側面を含んだ長期的で持続可能なビジネス戦略を立てられるよう、インダストリー4.0 サイバーセキュリティの一様で安定した法的環境を確立する。
- インダストリー4.0 セキュリティの認証スキームの開発を検討する（評価の対象を定義する

Copyright © 2019 独立行政法人情報処理推進機構

際には、固有の特殊性を考慮に入れる)。認証スキームは、マーケットの協調を促進し、顧客の信頼を向上させ、新しいビジネスチャンスを招く。

- さまざまな利害関係者との意見交換や切望される相乗効果から得られる恩恵を享受するために、インダストリー4.0 サイバーセキュリティにフォーカスした官民のパートナーシップを促進する。

Copyright © 2019 独立行政法人情報処理推進機構

3. プロセス

エコシステム固有の複雑さのため、法的責任（liability）を明らかにするのは非常に難しい。

課題：インダストリー4.0 製品のライフサイクルに対する法的責任が十分定義されていない

インダストリー4.0 サイバーセキュリティ・インシデントの説明責任義務が不明確なままであるため、インダストリー4.0 サイバーセキュリティの法的責任は、未解決の問題となっている。インダストリー4.0 の使用ライフサイクルやサプライチェーンには多くの利害関係者が関与しているので、セキュリティ・インシデント直後の法的責任分担は現在のところ困難となっており、一般的な法的責任条項のみ適用可能である。

エコシステム固有の複雑さのため、法的責任を明らかにするのは非常に難しい。産業用 IoT 機器の多くは、通常、（異なる管理上、法律上の制約を受けることがある）分散した場所にある複数のベンダー（機器に組み込まれるソフトウェアのベンダーも含む）によって製造される多くのコンポーネントから組み立てられている。サプライチェーンの複雑さが関連する問題をさらに悪化させている。このように、法的責任分担は依然として未解決の問題となっている。

サイバーセキュリティの観点では、インダストリー4.0 機器の製造業者は、製造する製品に適正なレベルのセキュリティを実現できる機能を含めることが求められている。同様に、インダストリー4.0 のオペレータは、これらのセキュリティ機能を使用し、製造業者によって提供されるすべてのセキュリティ・アップデートを適用することが求められている。実際の状況は、さらに複雑である。インダストリー4.0 ソリューションの（特に IT システムと比較すると）長い寿命と長期のメンテナンス（ソフトウェアのパッチ適用など）に関わる財務上のコミットメントが、それらソリューションの製造業者、ユーザー、オペレータへの負担を一層重くしている。接続されたインダストリー4.0 ソリューションの分割所有権、明確でない、または明記されていない役割の割り当て、および調達契約やサービス内容合意書（SLA）の規定が十分でないことが、さらに法的責任問題を複雑にしている。

提言：インダストリー4.0 の当事者間の法的責任を明確にする

インダストリー4.0 のパラダイム（枠組み）は、通常、製造/産業エコシステムに新たな技術お

Copyright © 2019 独立行政法人情報処理推進機構

よび新たなサービスをもたらす。このパラダイムのサイバー・フィジカル特性を考えると、セキュリティとセーフティは強固に結びついている。したがって、そのような製品やサービスのエンドユーザーや消費者を保護することだけでなく、包括的で安定した法的枠組みによる投資を奨励することも考慮して法的責任上の懸念事項を検討することは、特に重要である。欧州委員会は最近、IoT や AI（人工知能）のような新たな技術の法的責任問題の状況を説明した「Staff Working Document」[3]を公開した。この文書は今後発生する作業の参照ドキュメントとして役立つ。

インダストリー4.0 の利害関係者のどこで法的責任が生じるのかという疑問は、相違する、多様な利害関係者間において起きている。例えば、開発者、製造業者、供給者、ベンダー、アフターサービス・サポート・オペレーター、サードパーティー・プロバイダ、エンドユーザーなどである。

インダストリー4.0 当事者の法的責任を明確にするには、ENISA は以下のことを推奨する。

- 特に既存の法令のギャップが明確となっている場合は、EU や各国の法令、判例法に照らして法的責任問題に対処する。
- サプライチェーンの利害関係者間の責任を明確にするために、調達に関する専門用語を調整する。例えば、サービス内容合意書（SLA）や調達の契約書におけるインダストリー4.0 のサイバーセキュリティ要件を指定する。
- 未解決のサイバーリスクを移転し、企業が責任を負う可能性があるサイバーセキュリティ・インシデントの影響を軽減するサイバー保険の可能性を評価する。
- 責任の所在に関する法律について、エンドユーザーや消費者の意識を向上させる。
- 法的責任に関係するインダストリー4.0 のオペレータの法的義務を明確にする。

インダストリー4.0 のセキュリティ標準類やイニシアチブの分断化は、製造業にとって特に深刻である。 大手製造企業の事業施設は、通常世界中に広がっている。

課題：インダストリー4.0 技術標準の分断化

IoT やインダストリー4.0 に関連する標準類やポリシーのイニシアチブの現在の状況は、各セクター（自動車、医療、消費者など）のセキュリティおよび各セクターにまたがるセキュリティの両側面をカバーしており、極めて幅広い。IoT の観点では、多くの概念レベルの参照ドキュメントだけでなく、ベースライン、グッドプラクティス、チェックリストやガイダンス[4]が公開されている。特に接続された産業用システムや製造システムに関しては、関連する利害関係者にとっ

[3] EC Staff Working Document “Liability for emerging digital technologies” http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51633（2018 年 4 月）

[4] ENISA の オンラインツール「IoT とスマートインフラストラクチャのセキュリティ」で、ENISA IoT セキュリティベースラインとのマッピングに関連する標準類やイニシアチブの最新リストを公開している。：https://www.enisa.europa.eu/iot-tool

Copyright © 2019 独立行政法人情報処理推進機構

てガイドラインとなる有益なソース（情報源）もある[5]。

しかし、インダストリー4.0/スマートマニュファクチャリングに関しては、状況は少し異なる。これらの分野が新しく生まれたものであるという特質を考えると、全体論的方法でセキュリティに取り組む包括的なイニシアチブは遅れている。それでも、既存のいくつかの注目すべき事例（IEC 62443[6]や IUNO/Industrie4.0[7]など）を参照することは重要である。したがって、関心のある企業は、現在、インダストリー4.0/スマートマニュファクチャリングの幅広い領域の一部にのみ対応しているドキュメントを利用している。

インダストリー4.0 のセキュリティ標準類やイニシアチブ間の分断化は製造業界にとって特に深刻である。大手製造企業の事業施設は、通常世界中に広がっている。したがって、グローバルなレベルでの標準化への取り組みの統一の不足によって、ある企業の他国にまたがる事業施設間で、それぞれが異なるスキームに依存しており、セキュリティの専門知識やソリューションをコラボレーション、およびシェアできない。さらに、企業間のセキュアなコラボレーションもまた阻害されている。と同時に、ENISABaseline Security Recommendations for IoT[8], UK Government Code of Practice for Consumer IoT Security[9], NIST Internal Report 8228[10]といった、異なる標準間のマッピングをするイニシアチブが徐々に発展していることは、将来に期待が持てる。一方、そのようなイニチアチブは IoT セキュリティ分野の均一化の促進に貢献しており、今後インダストリー4.0 エコシステムへと拡張させていくことが望ましい[11]。

さらに、インダストリー4.0 のセキュリティ標準類やガイドラインの提言を実施するための体系的な方策も必要とされている。現在の、目標達成のための実用的な方法の欠如は、製造業界のシステム/サービスのセキュリティの著しい多様性を招いている。

---

[5] ENISA "Good Practices for Security of IoT in the context of Smart Manufacturing" Annex C
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

[6] IEC 62443 family of standards：https://www.iec.ch/index.htm

[7] IUNO project homepage：https://iuno-projekt.de/

[8] ENISA “Baseline IoT Security Recommendations”
https://www.enisa.europa.eu/publications/baselinesecurity-recommendations-for-iot（2017 年 10 月）

[9] Code of Practice for Consumer IoT Security： https://www.gov.uk/government/collections/secure-by-design

[10] NIST Internal Report 8228 (Draft) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf

[11] ENISA "Good Practices for Security of IoT in the context of Smart Manufacturing" Annex B
https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Copyright © 2019 独立行政法人情報処理推進機構

提言：インダストリー4.0 のセキュリティ標準類の取り組みを統合させる

現在のインダストリー4.0 サイバーセキュリティの技術標準類の分断化に対応するためには、大きなギャップやオーバーラップがあったとしても関連する取り組みを統合させることが必要である。ひとつの選択肢は、インダストリー4.0 セキュリティに特化したベースライン標準の採用である。これらの選択に沿って、そのような取り組みが最近 IoT の観点で起きているということが希望を与えてくれている[12]。

あるいは、さまざまな情報源から複数のセキュリティ標準をマッピングして完全な参照ドキュメントを提供し、すべての必要なセキュリティ管理策を考慮しているイニシアチブおよびガイドラインを調査することは有益である。いずれにせよ、標準化活動はインダストリー4.0 エコシステムのさまざまな当事者の意見に基づいて、関連する要件を公正かつ包括的に表現し、最終的により広範に採用されるようにする必要がある。

インダストリー4.0 のセキュリティ標準類に対する取り組みを調和させるために、ENISA は以下を推奨する。

- インダストリー4.0 セキュリティの全範囲に対応する標準化活動を立ち上げる。
- 潜在的なギャップ、すなわち既存の標準がインダストリー4.0 のセキュリティ要件に適切に対処しているかどうかを調べるために、インダストリー4.0 のセキュリティに関する現在の標準の分析を行う[13]。
- 関連する技術標準の開発における合意を確実にするために、インダストリー4.0 当事者のマルチ利害関係者間の対話を促進する。
- 標準化活動（ENISA2、NIST8、UK DCMS7 によるものなど）間のマッピング方式を開発、維持して、標準間の共通点と相乗効果を探る。

[12] ETSI TS 103 645 “Cyber Security for Consumer Internet of Things” https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf（2019 年 2 月）

[13] 関連する ENISA の調査： “IoT Security Standards Gap Analysis” https://www.enisa.europa.eu/publications/iotsecurity-standards-gap-analysis（2019 年 1 月）

Copyright © 2019 独立行政法人情報処理推進機構

製造業におけるサプライチェーン管理は、関係する当事者や利害関係者の大多数が認識している、周知の課題である。

課題：サプライチェーン管理の複雑さ

製造業におけるサプライチェーン管理は、関係する当事者や利害関係者の大多数が認識している、周知の課題である。サプライチェーンの特性はその企業によるが（たとえば、大企業は製品のコンポーネントを自社で製造しているため、サプライチェーンの大部分を管理できるかもしれない）、通常、企業は一部のコンポーネントの製造を他の企業に依存している。最近では、スマートマニュファクチャリングがサプライチェーンにさらに影響を与える新しい機能（エンドツーエンドの可視性、予測分析、自動化、およびデータ駆動型の意思決定）を導入するにつれて、状況はさらに複雑になっている。したがってサプライチェーンはパフォーマンスの観点から、より動的、柔軟、相互依存的、かつ要求が厳しくなっている。ただし、サプライチェーンの相互依存性が高まると、既存のセキュリティリスクおよび新しいリスクの出現による影響が大きくなる。

多数の人、組織、プロセスが関わるため、スケーラビリティは最も重要な問題の 1 つである。このような場合、企業は多くの決定を下す必要があり（例：ベンダーの選択、コラボレーションの方法の合意、組織プロセスの確立）、それらの決定に基づいて最終製品のセキュリティが左右される。すべてのコンポーネントをそのソースまで追跡できないと、製品のセキュリティに対する信頼をさらに損ねるため、サプライチェーンを効果的に管理することは不可欠である。信頼性の概念もまた注目に値する。なぜなら企業は、彼らが彼らのパートナーに与える信頼の度合いを明確にし、あらゆる残留リスクを管理する必要があるからである。

さまざまな国の立法の影響を受ける可能性のあるサプライチェーン関係者が多いということは、セキュリティ・インシデントがさまざまな場所や段階で発生する可能性があることも意味している。このようなインシデントは、商品、サービス、または情報の交換に関連している可能性があり、その結果、サプライチェーン全体にエラーやリスクが広がる可能性がある[14]。問題の原因を特定することは非常に困難になっており、連鎖して起こる影響の可能性を予測することも非常に困難である。いずれにしても、サプライチェーンのあらゆる時点でのセキュリティ侵害が最終製品のセキュリティに悪影響を及ぼす可能性があることは明らかである。

サプライチェーンの複雑さは、関係する様々な当事者に適用可能なセキュリティ標準とソリューションの利用に悪影響を及ぼしている。したがって、様々な当事者やプロセスに様々な要件が適用され、これがさらに面倒な問題になることがよくある。

[14] ENISA Infonote on Supply Chain Attacks
https://www.enisa.europa.eu/publications/info-notes/supply-chainattacks（2017 年 8 月）

Copyright © 2019 独立行政法人情報処理推進機構

提言：サプライチェーン管理プロセスをセキュアにする

サイバーセキュリティは共有の責任である。複雑なサプライチェーンと複数の関係者が関わっている IoT とインダストリー4.0 にとって、これはさらに差し迫った現実となっている。インダストリー4.0 をセキュアにするには、コラボレーションがすべてである。インダストリー4.0 には多くのプレイヤー、多くの相互依存関係、そして多くの側面が存在している。他の組織への信頼の度合いが、最終的にリスクアセスメントプロセスと適切なセキュリティ管理策の導入につながるため、信頼はセキュアなサプライチェーンの根源である。

大規模サプライチェーンに伴う複雑さとリスクへの対処とは、どれだけの信頼を置くことができるか、そして適切なレベルのセキュリティを定義するために受け入れることができる残留リスクが何であるかを特定することである。

もう 1 つの重要な考慮事項は、サプライチェーン全体にわたるセキュリティの包括的な管理である。2 つのエンティティ間のやり取りをセキュアにすることは、そのようなやり取りがより長いサプライチェーンの一部にすぎない場合、適切ではない。エンドツーエンドのセキュリティは、インダストリー4.0 が成功するための前提条件である。

サプライチェーン管理プロセスを完全に理解しセキュアにするために、ENISA は以下を推奨する。

- 潜在的なインダストリー4.0 サプライチェーンリスクを特定するために、定期的にリスクアセスメントを実施する。
- 各サプライヤの信頼度を定義し、この定義を定期的に見直す。
- サイバー脅威インテリジェンスを考慮して、現在進行中の脅威の状況を監視する。
- 製品が広く受け入れられているセキュリティ基準および認証スキームに準拠しているサプライヤを信頼する。
- 具体的な技術的セキュリティ管理策（証明書など）の代わりに信頼モデルを適用する。
- インダストリー4.0 の製品とサービスのセキュアなソフトウェア開発ライフサイクルに従うことによって、デジタルサプライチェーンのセキュリティを確保する。

Copyright © 2019 独立行政法人情報処理推進機構

4. 技術

インダストリー4.0 機器、プラットフォームおよび既存のシステムへのフレームワークの導入と統合により、相互運用性の問題が生じる。

課題：インダストリー4.0 機器、プラットフォーム、およびフレームワークの相互運用性

インダストリー4.0 機器、プラットフォームおよび既存のシステムへのフレームワークの導入と統合により、相互運用性の問題が生じる。産業環境では、さまざまな機器間の相互接続性を確保することは、特にサポートが切れてから長く経過している機器を考慮する際には、しばしば困難となる。そのため、インダストリー4.0 機器とレガシーなシステムとの円滑な統合を確保するセキュアなソリューションを促進することが不可欠である（例えば、異なるネットワークや他のプロトコルの場合に透明性の高い通信を保証するためのゲートウェイなど）。

さらに、相互運用性の欠如は、インダストリー4.0 機器で使用されている独自プロトコルに関連している。異なるベンダーの機器やプラットフォームを利用する場合、相互運用性を保証することが常に可能とは限らない。機器/プラットフォーム間の相互運用性を確保することは、シームレスな操作のためだけでなく、セキュリティについても同様である。したがって、インダストリー4.0 ソリューションの機能とセキュリティを向上させるためには、必ずしもセキュアではない独自プロトコルの問題に取り組み、共通のフレームワークを採用することが不可欠である。

最後に、相互運用性の概念は、通信プロトコルやさまざまなアプリケーションフレームワークについてだけ言及しているのではない。インダストリー4.0 の複雑なサプライチェーンでは、セキュリティの相互運用性の概念が浮上している。つまり、プラットフォーム、機器、プロトコル、およびフレームワークにわたって共通のセキュリティベースラインを確保することは非常に困難である。サプライチェーンの最も弱い部分がサプライチェーン全体に悪影響を及ぼす可能性があるため、これらすべての要素にわたって共通のサイバーセキュリティ・レイヤを統一することは非常に困難な課題である。

提言：セキュリティの相互運用性のためのインダストリー4.0 のベースラインを確立する

セキュリティの相互運用性の課題は、特にレガシーなシステムとの統合を考えた場合、インダス

Copyright © 2019 独立行政法人情報処理推進機構

トリー4.0 エコシステムに関連している。相互運用性とセキュリティの課題の大部分は、様々な製造元の、様々な通信プロトコルの機器の相互接続（重要なコンポーネントと重要ではないコンポーネントの両方）に由来する。そのため、インダストリー4.0 の機器、プラットフォーム、およびフレームワークの相互運用性、およびセキュリティ対策の実践を確実にし、促進することが不可欠である。

セキュリティの相互運用性に関するインダストリー4.0 ベースラインを確立するために、ENISA は以下を推奨する。

- 共通のセキュリティ言語を促進する相互運用性フレームワークの使用[15]、およびインダストリー4.0 コンポーネント用のプロトコルの使用を奨励する。
- サイバーセキュリティの 3 つの側面すべて、つまり人、プロセス、および技術をカバーするために、サプライチェーン全体のパートナーおよび企業間の固有のセキュリティレベルを定義する。
- オープンでアクセス可能な、相互運用性を確認できるラボおよびセキュリティを確認できるテストベッドを促進する。

インダストリー4.0 のセキュリティの確保の難しさは、特にレガシーなインフラストラクチャとの統合を考える場合、接続される産業用機器およびシステムの技術的性能の欠如からも生じる。

課題：インダストリー4.0 とスマートマニュファクチャリングを妨げている技術的な制約

インダストリー4.0 のセキュリティの確保の難しさは、特にレガシーなインフラストラクチャとの統合を考える場合、接続される産業用機器およびシステムの技術的性能の欠如からも生じる。組み込みシステムの制約は、特にローエンドの ICS や PLC の場合には大きな課題となる。それらの機器はセキュリティに直接影響する多くの問題に直面しているためである。

例えば、以下の制約について考慮する。

- 処理性能に制限があり、装置の適切なサイズおよび競争力のある価格を維持しながら長時間の動作を保証しなければならないという要件は、設計段階における包括的なセキュリティ機能の実装にかなり影響を与える。
- インダストリー4.0 機器を設計するときに基本的な保護メカニズムを考慮しないと、機器のセキュリティに悪影響が及ぶ。ローエンドの機器に関しては、そのような基本的な保護メカニズムをサポートしていないため、無線によるパッチ適用やソフトウェアの更新は、ほとんどの場合実行不可能なソリューションである。
- 暗号化や認証などのより高度なセキュリティ対策が欠けていると、産業プロセスに最も近

[15] 注目に値すべき例：NIST の Cyber Security Framework および IEC 62541 (OPC UA).

Copyright © 2019 独立行政法人情報処理推進機構

い機器の保護レベルが低下する。ネットワークを保護するだけの非常に一般的なアプローチは不十分である（例えば、攻撃者がネットワークに侵入した場合、機器は攻撃に対して脆弱である）。

最後に、技術的制約に関連したギャップを考えると、インダストリー4.0 システム専用のサイバーセキュリティツールは一般的にあまりに少なすぎるかまたは高価すぎる。OT 環境でのネットワーク監視、自動資産検出、および設定と変更管理のためのツールは、OT システムのセキュリティレベルを高め、可用性を高めてきた。しかしそのようなツールは、新しいインダストリー4.0 をサポートするための準備がまだ十分に整っていないため、セキュリティの面でギャップが生じている。インダストリー4.0 の世界に適応したセキュリティソリューションを開発し、このような困難な問題に対処することが必要である。

提言：インダストリー4.0 セキュリティの確保のための技術的対策の適用

エコシステムの複雑さとスケーラビリティを考えると、IoT とインダストリー4.0 セキュリティすべてに適合するソリューションはない。複数のソリューションを組み合わせて、これらのソリューションがセキュリティを犠牲にすることなく、また、ユーザビリティの要素も考慮に入れて柔軟性と拡張性に対応できるようにする必要がある。この文脈における柔軟性の概念はまた、サイバーセキュリティの経済学、すなわち採用される解決策が、体系的な費用便益分析の結果としてもたらされるべきであるということにも言及しており、そうして間違いなくセキュアで信頼できる製品/サービスの恩恵を受けることができるようになる。

リスク分析に基づいてインダストリー4.0 のコンポーネント、サービス、およびプロセスに対するベースラインのセキュリティ推奨事項を特定することは、この分野の困難な技術的制約への解決策に取り組むための最初のステップである。ENISA は、IoT エコシステムの各セクターにまたがり、インダストリー4.0 の個々のセクターにも関連するガイドラインを発行している。

インダストリー4.0 のセキュリティを確保するための技術的対策の適用に関して、ENISA は以下を推奨する。

- 方法論的なリスクアセスメントを考慮に入れて、インダストリー4.0 のセキュリティアーキテクチャを定義する。
- すべてのインダストリー4.0 コンポーネント、機器、サービス、プロトコル、通信、およびプロセスに、セキュリティ・バイ・デザイン、プライバシー・バイ・デザイン、およびプライバシー・バイ・デフォルトの原則を適用する。
- 実装されたサイバーセキュリティ・ソリューションの成熟度を定期的に評価し、現在のお

Copyright © 2019 独立行政法人情報処理推進機構

よび新たな脅威の状況を監視することで、サイバー脅威インテリジェンスを検討する。

- インダストリー4.0 の展開に関する業界のサイバーセキュリティを監視する。また、レガシーなシステムやインフラストラクチャにも対応する。
- フェイルセーフで効率的な運用を指針として、インダストリー4.0 コンポーネントおよびサービスのライフサイクル全体にわたる継続的な更新性およびアップグレード性を実現する。
- インダストリー4.0 のサイバーセキュリティ標準およびサイバーセキュリティのベストプラクティスの動向を追跡し、不要な機能を削除することも検討しながら、リスクアセスメントの対象となる関連するセキュリティ対策を適切に実施するようにする。

Copyright © 2019 独立行政法人情報処理推進機構

「提言」のまとめ

インダストリー4.0 セキュリティ専門家（OT/IT セキュリティ）

・IT および OT セキュリティに関する分野横断的な知識の習得を促進する
・セキュアなサプライチェーン管理プロセス
・セキュリティの相互運用性に関するインダストリー4.0 ベースラインを確立する
・インダストリー4.0 のセキュリティを確保するための技術的対策の適用

インダストリー4.0 オペレータ（ソリューションプロバイダ、製造業者）

・IT および OT セキュリティに関する分野横断的な知識の習得を促進する
・インダストリー4.0 当事者間の法的責任を明確にする
・インダストリー4.0 セキュリティに対する経済的および行政的インセンティブの促進
・セキュアなサプライチェーン管理プロセス
・セキュリティの相互運用性に関するインダストリー4.0 ベースラインを確立する
・インダストリー4.0 のセキュリティを確保するための技術的対策の適用

規制機関

・インダストリー4.0 当事者間の法的責任を明確にする
・インダストリー4.0 セキュリティに対する経済的および行政的インセンティブの促進
・インダストリー4.0 セキュリティ標準類の取り組みを統合させる
・セキュリティの相互運用性に関するインダストリー4.0 ベースラインを確立する

標準化コミュニティ

・インダストリー4.0 セキュリティ標準類の取り組みを統合させる
・セキュリティの相互運用性に関するインダストリー4.0 ベースラインを確立する

学術機関と研究開発団体・組織

・IT および OT セキュリティに関する分野横断的な知識の習得を促進する
・セキュリティの相互運用性に関するインダストリー4.0 ベースラインを確立する

Copyright © 2019 独立行政法人情報処理推進機構

ENISA について

欧州連合ネットワーク情報セキュリティ機関（European Network and Information Security Agency：ENISA）は、欧州連合（EU）、その加盟国、民間部門およびヨーロッパ市民のためのネットワークおよび情報セキュリティの専門知識を集約している機関である。ENISA はこれらのグループと協力して、情報セキュリティにおけるグッドプラクティスに関するアドバイスや提言を提供している。これは、EU 加盟国が関連する EU 法の実施を支援し、ヨーロッパの重要な情報インフラおよびネットワークのレジリエンスの向上に役立っている。ENISA は、EU 全体のネットワークおよび情報セキュリティの向上に取り組む、国境を越えたコミュニティの発展を支援することによって、EU 加盟国における既存の専門知識の強化を促進している。
ENISA の詳細については、下記ウェブサイトを参照。
www.enisa.europa.eu

連絡先
本文書に関するメディアからの問い合わせ先：press@enisa.europa.eu

謝辞
ENISA の調査「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」（2018 年 11 月）において、意見とフィードバックを寄せていただいたすべての専門家に感謝する。

著者
Dr. Apostolos Malatras
Christina Skouloudi
Aggelos Koukounas

著作権表示
©欧州ネットワーク情報セキュリティ機関（European Network and Information Security Agency: ENISA）, 2019
出典が明示されている場合に限り、複製を許可するものとする。
Catalogue number: TP-03-19-407-EN-N
ISBN: 978-92-9204-293-6
DOI: 10.2824/143986

Vasilissis Sofias Str 1
151 24 Maroussi, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

Copyright © 2019 独立行政法人情報処理推進機構