独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

平成25年度　IT人材における情報セキュリティの育成ニーズ・課題調査

最終報告書（概要版）

平成26年3月
IT人材育成本部
HRDイニシアティブセンター

目次

1.1.背景・目的

■ 当事業の経緯・背景

- 経産省の「情報セキュリティ人材の育成指標等の策定事業（H24年）」を受けて、IPAではスキル指標（CCSF）を拡充した。（→情報セキュリティ強化対応CCSF）
- IPAの中期計画では、この「スキル指標の利用率向上」を3ステップにて達成を目指す。
- しかし、スキル指標を提供するだけでは、情報セキュリティ人材育成のモチベーションとなりえず、利用率も上がらない。

IT人材における情報セキュリティの育成ニーズ・課題調査事業を実施

■ 当事業の目的

- ITベンダーやユーザー企業の情報システム部門のIT人材における情報セキュリティの具体的な育成ニーズ・課題を調査する。
- 情報セキュリティ人材の活躍イメージにつなげ、人材育成をドライブする。

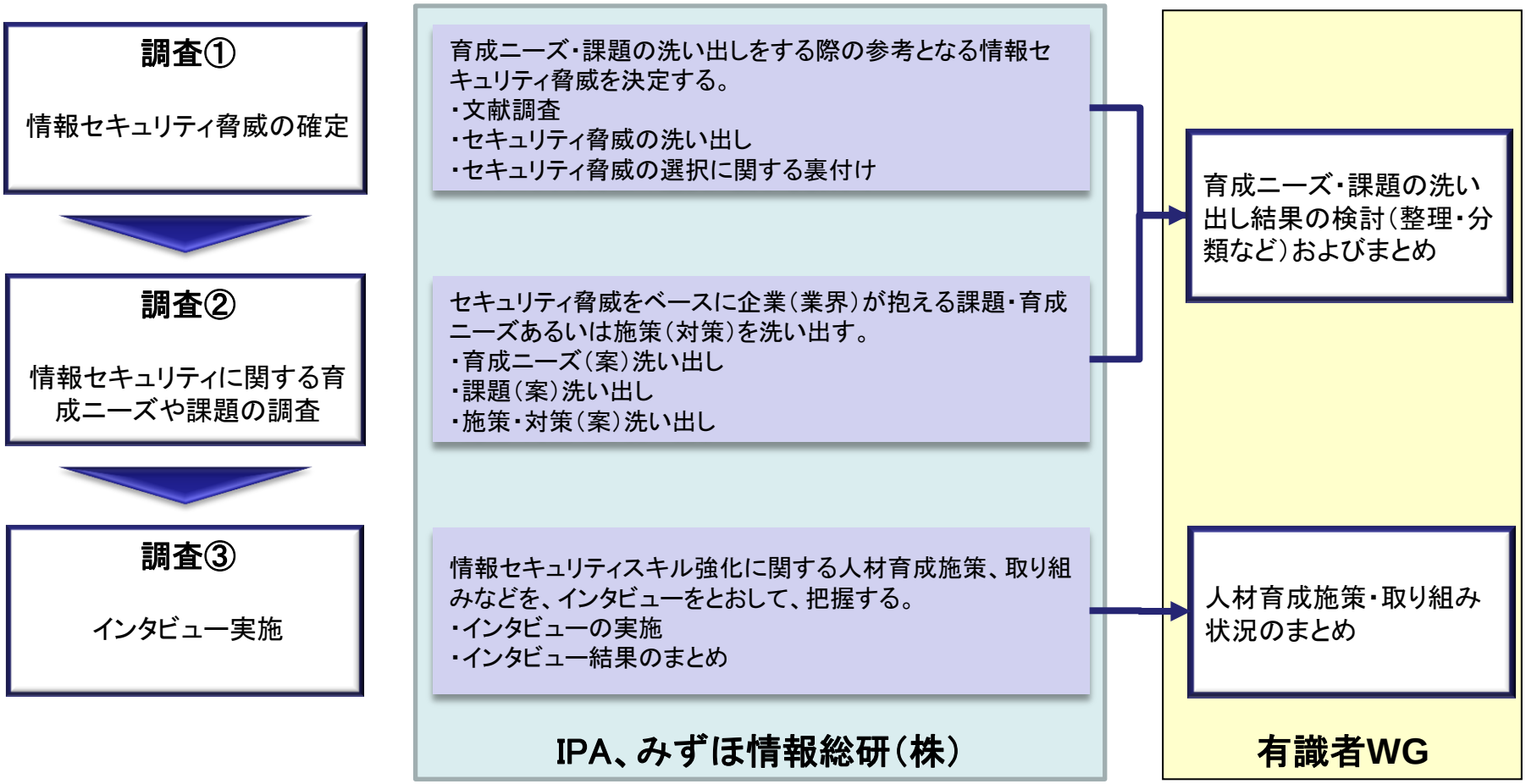
1.1.背景・目的

- 当事業で対象とする「情報セキュリティを担うIT人材」の範囲
  - 「ITSS人材およびUISS人材」の母集団が107万人のグループ(※)で、他者に情報サービスを提供する者を指す。
  - 一般企業社員及び学生や非就業者、組込み技術者、ホワイトハッカー等は含まない。情報サービスを提供するITベンダー企業でも、管理部門の社員は対象ではない。

区分	業務分類	必要なスキルの例
IT人材 (約107万人)	ユーザー企業の 情報システム部門	他者に安心・安全な情報サービスを提供する上で必要なスキル
	ITベンダー企業 (エンジニアが対象、 管理部門は含まない)	
	情報セキュリティ専門企業 (エンジニア)	セキュリティ脅威をビジネスチャンスに変える高度なスキル
IT人材以外の 全般	ユーザー企業（業務担当）	一般的な情報セキュリティ リテラシ ※IT人材白書の人数推計による
	学生・非就業者	

1.2.実施作業内容

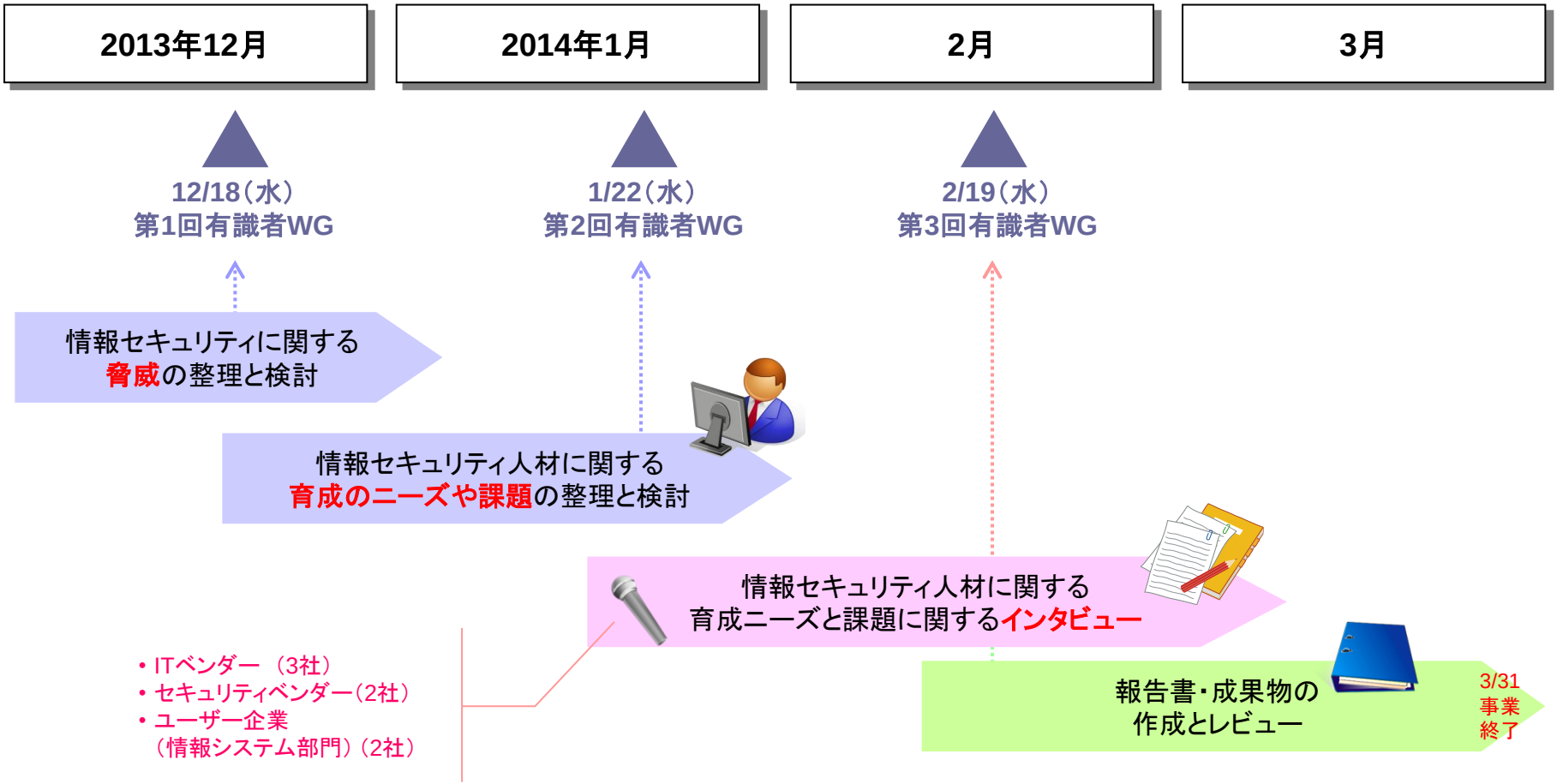
- 当調査は調査①～③で構成。
- 各種調査した結果について、その内容を複数の有識者で確認し、議論を通してオーソライズするため、有識者をメンバーとするWGを設置。



1.2.実施作業内容

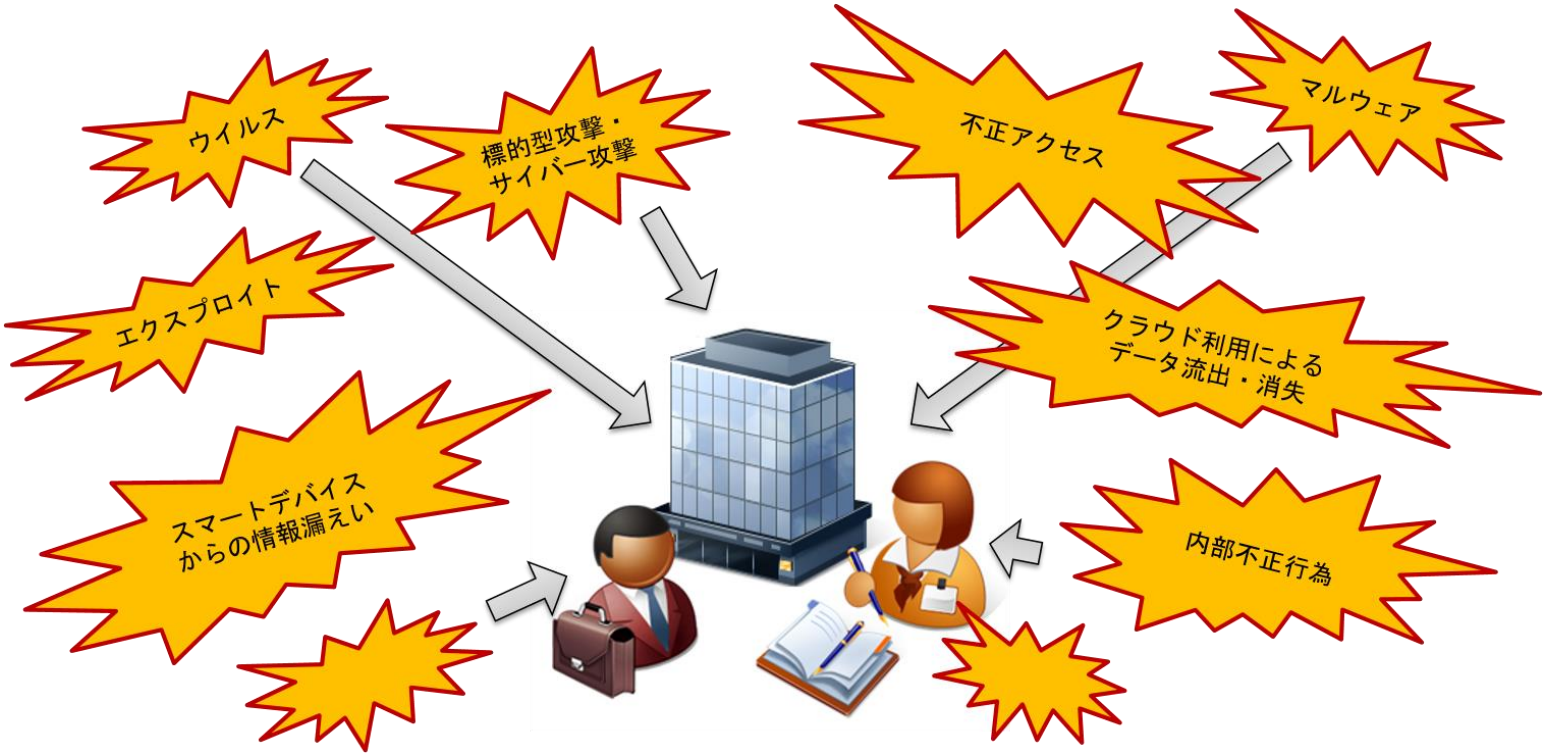
■ 調査スケジュール

– 前半で、情報セキュリティに関する脅威や企業内で求められる対策についての整理・検討を行った上で、後半でそれらの調査結果に基づいて、情報セキュリティ人材に関する育成のニーズや課題を整理し、成果物を取りまとめた。



2.1.企業に求められる情報セキュリティ対策（選定した脅威）

- 近年注目を浴びている企業における情報セキュリティ上の脅威に着目し、人材育成を含めた対策が特に必要と判断される脅威を選定した。



2.1.企業に求められる情報セキュリティ対策（選定した脅威）

- 脅威は、IPA、JNSA、アンチウイルスベンダーのレポート等より、40以上の脅威を対象とした。
- 対象の脅威から、4つの観点のもと、6つの脅威を選定した。

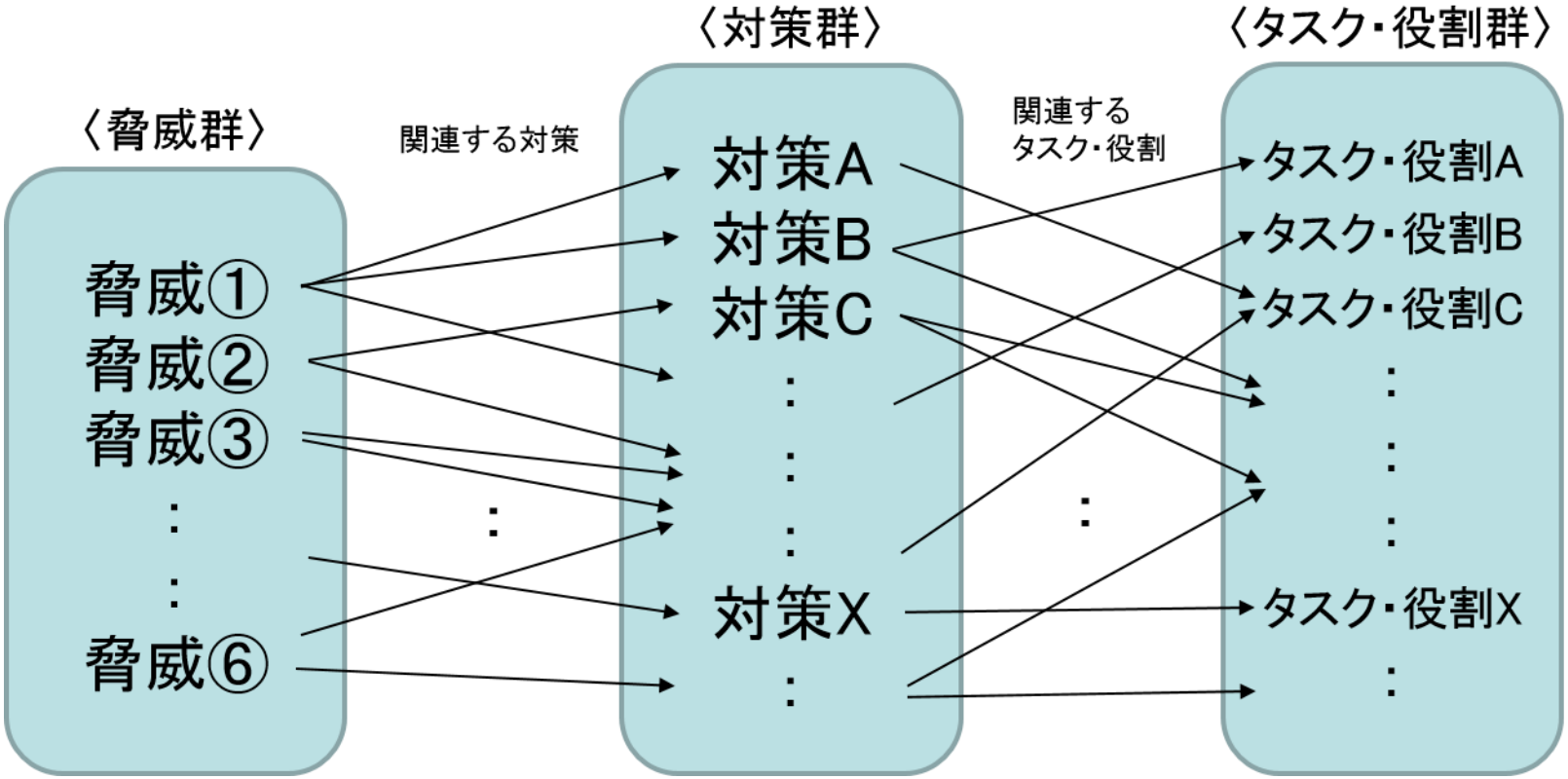
[A]IPA	[B]JNSA	[C]アンチウイルスベンダー
標的型攻撃、標的型諜報攻撃、サイバー攻撃	標的型攻撃、サイバー攻撃	標的型攻撃(サイバー攻撃)
ウェブサイトを狙った攻撃	著作権法改正への抗議攻撃	スマートフォン・モバイル
スマートデバイスを狙った悪意あるアプリ、ウイルス	スマートフォンに迫る脅威	マルウェア・エクスプロイト、ウイルス
ウイルス、マルウェア	ウイルス、ワーム	データ消失・データ侵害
予期せぬ業務停止(クラウド)	サーバの障害とデータ消失	クラウド
脆弱性を突いた攻撃	クラウドの課題	ツールキット・不正アプリ
フィッシング詐欺	ネットバンキング	SNS
内部犯行	情報セキュリティ人材不足	ネットバンキング
パスワード流出の脅威	不正アクセス禁止法	情報セキュリティ人材
不正アクセス	管理ミス、誤操作、設定ミス	著作権法
制御システムの情報セキュリティ対策	目的外利用	不正アクセス禁止法
マイナンバー法案	紛失、置き忘れ	ハクティビズム
スパムメール	バグ、セキュリティホール	脆弱性(ゼロデイなど)
サイバー空間上のデモ活動	内部犯行、内部不正行為	スパム
DDoS		
電子証		
電子政		

No.	脅威・セキュリティ事象	概要
1	標的型攻撃、サイバー攻撃 (マルウェア、ウイルスを含む)	特定のターゲット(企業・組織、サービス、個人など)に対して、個人情報や機密情報などの重要情報の搾取や破壊活動といった特定の目的のために行われるサイバー攻撃が増加している。
2	不正アクセス	ウェブサイトに対する不正アクセスを行い、クレジットカード情報等の重要情報を窃取される事例が報告され、2012年から引続き共通的な[illegible]つ集団による攻撃等が増加している。
3	エクスプロイト	ゼロデイ攻撃や正しいセキュリティパッチ適用が実施されていないシステム上の脆弱性を悪用した被害が依然として発生している。ウェブシステム運用管理者だけではなくウェブシステム等の利用者(クライアント)まで脅威が広がっている。
4	クラウド利用におけるデータ消失・流出	クラウドサービスのような外部リソースをデータの保管手段として活用は、災害対策を含む可用性向上策として有効な一方、自組織の管理が及ばない範囲での被害発生のリスクを持つ。
5	スマートデバイスからの情報漏えい	各企業においてBYOD(Bring Your Own Device)の利用ケースが増加し、モバイル機器等、従来型システム以外からの情報漏えいのリスクが懸念されている。
6	内部不正・うっかりミス	組織内部者による、顧客情報や製品情報などの漏えいといった不正行為による情報セキュリティ上のインシデント

- 4つの観点
  - 注目度、理解度の観点
  - 脅威の影響範囲の観点
  - 対策との結びつきの観点
  - 脅威の普遍性の観点

2.2.情報セキュリティ対策が求められる各場面において活躍するIT人材

- 選定した6つの脅威に対する複数の対策の中から、特に重要と判断される対策、その対策を担う人材のタスク・役割を整理した。
- 脅威と対策、関連するタスク・役割は、以下の関係である。
- タスク・役割は、「情報セキュリティ強化対応CCSF」に関連している。



2.2.情報セキュリティ対策が求められる各場面において活躍するIT人材

- 選定した6つの脅威への対策として、特に重要と判断されたタスク、役割の分類を示す。
- タスク、役割はテクニカル系とマネジメント系に大別され、脅威によって特に重要タスク、役割は異なる。

No.	脅威・セキュリティ事象	脅威への対策として特に重要なセキュリティに関連するタスク・役割				
		テクニカル系				マネジメント系
		システムライフサイクル			管理	事業戦略
		①ITシステム企画	②システム開発・構築	③システム運用	④情報セキュリティマネジメント	⑤情報セキュリティ戦略
1	標的型攻撃、サイバー攻撃（マルウェア、ウイルスを含む）			◎		
2	不正アクセス		◎	◎		
3	エクスプロイト		◎			
4	クラウド利用におけるデータ消失・流出	◎		◎		
5	スマートデバイスからの情報漏えい					◎
6	内部不正・うっかりミス				◎	

※上記では、特に重要と判断されたタスク、役割を明示しているが、脅威に対しては1つではなく、テクニカル系、マネジメント系の両面の対策（トータルセキュリティ）が必要である。

2.2.情報セキュリティ対策が求められる各場面において活躍するIT人材①

① 標的型攻撃・サイバー攻撃（マルウェア、ウイルスを含む）

脅威への対策として重要なタスク・役割

- システム運用において、セキュリティ障害管理（事故の検知、初動対応、分析、復旧等）のタスクを実行する役割

関連する専門分野例
ITSS：ITサービスマネジメント（システム管理）
UISS：セキュリティアドミニストレータ（インシデントハンドラ）

《詳細》

脅威への対策例

各企業の検討動向として特出すべき点としては、「事故も想定した対策の検討」である。これは、標的型攻撃の巧妙性を配慮し、標的型攻撃を受けた場合に、すべての対応を技術的（システム的）に担保することが不可能であり、事故発生も想定とした対策（ルール）と、事前の組織的対策（攻撃を受けた場合に被害を最小化すべき対応を事前に教育する等）が検討されている。そのため、技術的対策だけでなく、組織的対策を踏まえて、標的型攻撃が発生した場合の事故も想定した上で、**被害最小化するための情報セキュリティ対策を進める体制（CSIRT等）**が求められている。

注目した対策

被害最小化するための情報セキュリティ対策を進める体制（CSIRT等）

IPA「2012年版　10大脅威」より

2.2.情報セキュリティ対策が求められる各場面において活躍するIT人材②

② 不正アクセス

脅威への対策として重要なタスク・役割

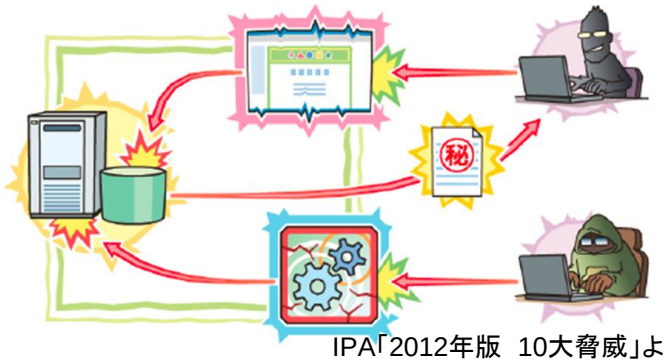
- システム開発・構築において、システム設計におけるセキュリティ面の検討や決定などのタスクを実行する役割
- システム運用において、セキュリティ管理のタスクを実行する役割

関連する専門分野例
ITSS：ITスペシャリスト（セキュリティ）、ITサービスマネジメント（運用管理）
UISS：システムデザイナー、ISオペレーション

《詳細》

脅威への対策例

ウェブサーバの脆弱性を悪用し、ウェブサイトの改ざん、サーバの設定ファイルの公開やクレジットカード情報等の重要情報の窃取等の事例が発生している。企業の対策としては、システムの改修、不正アクセスの検知・遮断対策及び重要な個人情報の暗号化や利用者に対するパスワード強化の呼びかけ等、**システム設計や運用**の対策だけではなく、**不正アクセスを模した手法によるコンピュータシステムの安全性を検査する手法など具体的な攻撃手法の理解**も求められている。



IPA「2012年版　10大脅威」より

注目した対策

①セキュリティを考慮したシステム設計
②システム運用におけるセキュリティ管理

2.2.情報セキュリティ対策が求められる各場面において活躍するIT人材③

③ エクスプロイト

脅威への対策として重要なタスク・役割

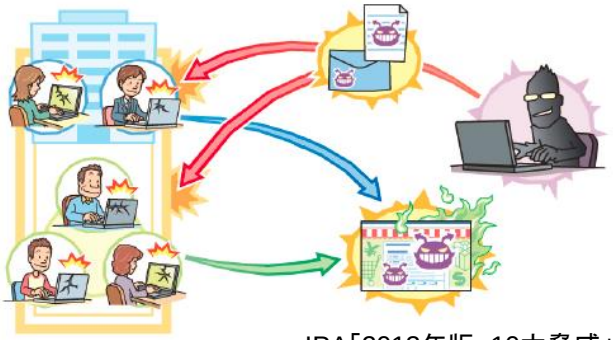
- システム開発・構築において、システム設計におけるセキュリティ面の検討や決定などのタスクを実行する役割

関連する専門分野例
ITSS：ITスペシャリスト（セキュリティ）
UISS：システムデザイナー

《詳細》

脅威への対策例

システムの運用管理側では、運用時だけではなく、システム設計からの対策が必要であり、ソフトウエアの**脆弱性の有無**を定期的に診断し、可能な限り更新を適用すること及びバージョンアップが出来ない場合の想定、**被害が出にくいネットワーク構成や出口対策の検討**が必要である。また、システムの利用者は、クライアントソフトの脆弱性対策として、ウイルス対策ソフトの適用やタイムリーにソフトウェアの更新を行うこと以外にも一般的なウェブサイトの閲覧操作でウイルス感染する可能性があることの注意喚起が必要である。



IPA「2013年版　10大脅威」より

注目した対策

脆弱性に対する対策方針の決定やセキュリティアーキテクチャと対策との整合性確保

2.2.情報セキュリティ対策が求められる各場面において活躍するIT人材④

④クラウド利用におけるデータ消失・流出

脅威への対策として重要なタスク・役割

- ITシステム企画において、システム化計画の具体化（要件定義、アーキテクチャの設計等）のタスクを実行する役割
- システム運用において、セキュリティ管理のタスクを実行する役割

関連する専門分野例
ITSS：ITアーキテクト（セキュリティアーキテクチャ）、ITサービスマネジメント（運用管理）
UISS：ISアーキテクト、ISオペレーション

《詳細》

脅威への対策例

クラウドサービス利用に関しては、データ消失のリスクに加え、クラウドサービス利用の場合、具体的な被害状況が把握しにくい。そのため、「データ消失」時の確認や対応だけではなく「二次的な情報漏洩被害」に関する対策についても検討する必要がある。クラウドの利用は、今後も増加すると見込まれ、**クラウド活用を前提としたシステム設計段階からのセキュリティへの配慮（セキュリティバイデザイン）**等、クラウドサービスの提供側の対応と同時に**クラウド利用時の利用側の対策**が求められている。

IPA「2013年版　10大脅威」より

注目した対策

①セキュリティアーキテクチャの設計
②ファイアウォールやアクセスコントロールの適切な管理

2.2.情報セキュリティ対策が求められる各場面において活躍するIT人材⑤

⑤ スマートデバイスからの情報漏えい

脅威への対策として重要なタスク・役割

- 事業戦略、経営戦略の中で、情報セキュリティ戦略の策定のタスクを実行する役割

関連する専門分野例
ITSS：コンサルタント（情報リスクマネジメント）
UISS：セキュリティアドミニストレータ（情報セキュリティアドミニストレータ）

《詳細》

脅威への対策例

例えば、PCと同様にスマートフォン端末を管理するためのツールであるMDM（Mobile Device Management）は、リモートワイプによって利用できるサービスはスケジュール管理及びメールの送受信に限定されていたが、現在では、ローカルワイプも普及し、「紛失・盗難時のデータ消去」等に関しても、複数の実施方法が求められる等の**対応が高度化**している。今後、BYODの普及が見込まれることから、企業側ではBYOD向けシステムのセキュリティ要件、BYOD利用の運用ルールの明確化、インシデント発生時の措置などの新たなデバイスの特性を理解した対策や企業のガバナンスが必要となっている。

注目した対策

組織、企業における情報セキュリティ戦略を策定

IPA「2012年版　10大脅威」より

2.2.情報セキュリティ対策が求められる各場面において活躍するIT人材⑥

⑥内部不正・うっかりミス

脅威への対策として重要なタスク・役割

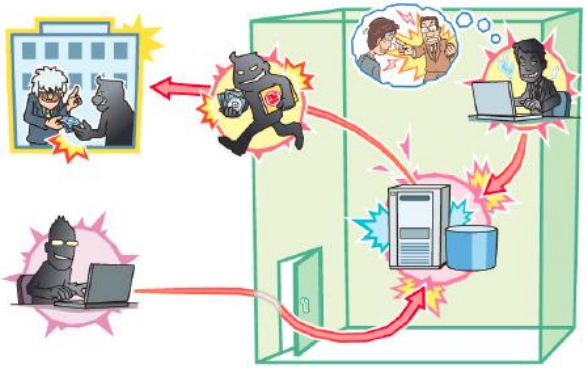
- 情報セキュリティマネジメントにおいて、セキュリティ方針の策定、セキュリティ基準の策定のタスクを担う人材

関連する専門分野例
ITSS：コンサルタント（情報リスクマネジメント）
UISS：セキュリティアドミニストレータ（ISセキュリティアドミニストレータ）

《詳細》

脅威への対策例

内部不正は風評被害が発生する恐れや、取引先などの関係者との調整がつかないなどの理由から組織内部で処理されてしまう傾向にあり、各組織が自らの経験などをもとに個別に対策を講じているのが実情である。対策には資産管理、技術的管理、証拠確保、コンプライアンス、職場環境、事後管理などの多角的な取組が必要であり、**ポリシー等の制度設計**とフォレンジック等の技術的観点の両面での取組を行う多様な人材が必要である。



注目した対策

社内におけるセキュリティを含めた制度設計

IPA「2013年版　10大脅威」より

2.3.情報セキュリティを担うIT人材の育成に関する課題

- 情報セキュリティを担うIT人材の育成課題は大きく4つある。
- 企業における情報セキュリティに対する優先度やIT依存度等により、課題への取り組みは企業によって様々である。
- 課題①～③については、順序性がある。

■ 企業・組織内の課題

課題①
対象人材の必要性に関する理解不足
→
課題②
対象人材の育成の難しさ
→
課題③
対象人材の企業内の処遇

■ 企業・組織外の課題

課題④
外部要因

2.3.情報セキュリティを担うIT人材の育成に関する課題

■ 企業・組織内の課題

課題①
対象人材の必要性に関する理解不足

- **経営層をはじめ、対象人材の必要性について理解が不足している**
- **経営層をはじめ、自社においてどのような対象人材が必要か、具体的に理解していない**

《具体例》
- 経営層の理解が得にくい
- そもそも（情報セキュリティの必要性が）理解されていない
- 経営層が対象人材の育成の必要性を重視していない　など

課題②
対象人材の育成の難しさ

- **育成や習得に時間やコストがかかる**
- **必要となる知識やスキルが多い／わからない**
- **セキュリティ以外にも幅広い知識と経験が必要（ハイレベルな人材には教育のみでは到達しない）**
- **情報セキュリティを志望する人が少ない場合もある**

《具体例》
- スキルの維持が難しい
- 専門的な知識だけでなく、一般的知識・経験の教育について一朝一夕には行かない
- パーソナルな資質や、事業を創っていく能力の方が重要視されており、上に上がる試験がある訳でもない
- ビジネスの観点からものが見られる情報セキュリティ人材が必要
- 人材の異動による知識の継承が難しい　など

2.3.情報セキュリティを担うIT人材の育成に関する課題

■ 企業・組織内の課題

課題③ 対象人材の企業内の処遇

- **対象人材を適切に評価することが難しい**
- **企業にとって専門的すぎる人材の扱いが難しい**（活躍の場がないと転職する）
- **自組織の人材育成計画やキャリアパスモデルになじまない**
- **セキュリティ関連部署のステータスが低い場合がある**
- **情報セキュリティに人を割く余裕がない場合もある**（兼任の場合も）

《具体例》
- 情報セキュリティ業務が特殊なため、自組織の人材育成計画やキャリアパスモデルになじまない
- 専門性を重視して採用した人材の将来的なキャリアパスに苦労している
- 情報セキュリティ業務の担当者のスキルが世間と比べてどうなのか評価できない／外部の評価制度もない　など

■ 企業・組織外の課題

課題④ 外部要因

- **質の高い人材の確保が困難／求めるレベルの人材が獲得できない**
- **人材の流動性が高い（転職が多い）**
- **教育やアウトソースの面で、外部サービスを利用すると（高い）コストがかかる場合もある**

《具体例》
- 情報セキュリティ人材の育成には外部教育サービスに頼らざるを得ず、高額のコストがかかる
- 情報セキュリティ分野の専門性をせっかく身につけた人材が、しばしば他企業等に転職してしまう
- 情報セキュリティ人材は全般的に不足している。特に、攻撃の解析など高度なスキルを持つ人材については、絶対数が日本に少ない　など

2.4.先進的企業の特徴からみる解決策

- セキュリティについて先進的に取り組んでいる企業を対象に、インタビュー調査を実施した。特徴的な結果を以下に示す。
  - 企業として情報セキュリティに対する意識が高い
    - 経営層の意向や自社他社問わず近年よく発生するセキュリティインシデント等がきっかけとなり、企業意識として情報セキュリティの必要性を高く理解している。
  - 自社にとって必要となるセキュリティ対策を理解している
    - ITユーザー、ITサービス提供企業として、自社のIT依存度を正確に把握し、必要となるセキュリティ対策を見極めている。
  - 経営とセキュリティを踏まえた判断を行っている
    - 必ずしも資金や人的リソースが足りているわけではなく、必要となるセキュリティ対策を満足に行えていない場合もある。その場合、優先順位を付けたり、対策のレベルを落とすなどセキュリティリスクと上手く付き合う判断を行っている。
  - 職種、職務レベルに合わせた教育・育成を行っている（質の向上）
    - 人材を「セキュリティのスペシャリスト」、「ITを専門とした業務を行う管理者・担当者」、「ITを専門としないリテラシーとしてセキュリティを知っていたほうが望ましい担当者・利用者」の3つに分類し、社内教育や研修をはじめ社外活動や外部セミナーの受講など職種、職務レベルに合わせた教育・育成を行い、企業としてセキュリティレベルの底上げを図っている。
  - ポジション、キャリアパスが設定できている
    - セキュリティを専門とする人材に対し、活躍の場を提供できなかったり、適切な評価ができないと離職するケースがあるため、その点を留意している。

2.4.先進的企業の特徴からみる解決策

■ 情報セキュリティを担うIT人材の育成課題4つに対する解決の方針を示す。

課題①
対象人材の必要性に関する理解不足

解決の方針①
各企業は、**自社のIT依存度を把握した上で、具体的にどのような対策や人材が自社において必要か（事業を行うために必要な情報セキュリティを担うIT人材の量と質）を整理する**必要がある。その上で、各企業において、対策を施すもしくはリスクと共存する、自社で育成するもしくは役割をアウトソースするといった決断をすべきである。

課題②
対象人材の育成の難しさ

解決の方針②
セキュリティに限らず人材育成は時間やコストを要する。また、ITやセキュリティの高度化、多様化の流れを止めることはできない。最新の技術や先端の事象に囚われて場当たり的な対策や育成を行うのではなく、例えば情報セキュリティの３要素である「機密性」「完全性」「可用性」に基づいて企業における対策や育成の判断を行うなど、**セキュリティを加味した企業戦略、育成方針が必要**である。

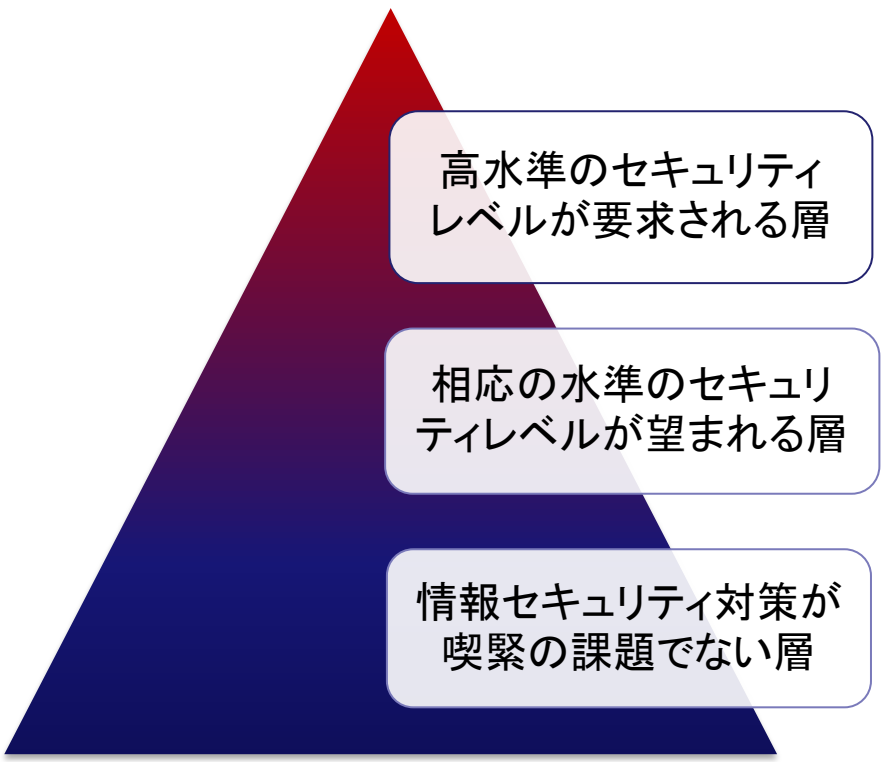
課題③
対象人材の企業内の処遇

課題④
外部要因

解決の方針③
企業や社会において、情報セキュリティの優先度が十分に高くないこと、情報セキュリティを担うIT人材の絶対数が少ないことが要因の一つである。情報セキュリティは、必要最低限の人数で対策を行うものでなく、企業の品質や機能であり、**経営層だけでなく企業全体・社会全体として情報セキュリティマインドを身につける必要がある**。

3. まとめ

- 企業に求められる人材育成を含めた情報セキュリティ対策のレベルは、『情報セキュリティリスク指標』の考え方に基づき、3つの層に分けられる。
- これらを参考に、自社に求められる対策のレベルを見極めることが必要。



情報セキュリティリスク指標

企業の属性によって、3つの層に分けられる

《企業の属性》
- IT依存度
- 重要情報の保有数
- 業種
- 従業員数
- 売上高　etc…

《例》
重要インフラ、生命、財産関連のシステムを扱っている企業
→高水準のセキュリティレベル
中小企業でもIT依存度が高い企業
→相応の水準のセキュリティレベル
農業を営んでおりITをほとんど使っていない企業
→情報セキュリティ対策が喫緊の課題でないレベル

参考：https://www.ipa.go.jp/security/benchmark/

3. まとめ

- 当調査では、情報セキュリティを担うIT人材における育成ニーズ、育成課題等を調査した。
  - 近年注目を浴びている情報セキュリティ上の脅威に着目し、その脅威に対する対策の中から重要と判断される対策、その対策を担う人材を整理した。
  - 情報セキュリティを担うIT人材の育成ニーズや育成課題を既存調査の報告書や文献を中心に抽出し、整理した。
  - 先進的に育成に取り組んでいる企業にインタビュー調査を行い、情報セキュリティを担うIT人材の育成ニーズや育成課題に対する取り組みを把握した。

- ITの高度化、多様化の中、情報セキュリティを担うIT人材の育成ニーズは存在しているものの、大きく4つの課題があり、対象とする人材の育成は思うように進んではいない。
- 一方、先進的に育成に取り組んでいる企業は、対象とする人材のスキル向上に注力しており、人材育成の方針は量より質の向上に重きを置いていることがインタビュー調査で判った。
- 今後、企業経営者や人材育成担当者は、自社のIT依存度を把握し、高度化、多様化する脅威から企業資産を守るために情報セキュリティを担うIT人材の育成を具体化させる必要がある。

おわりに

- HRDイニシアティブセンターでは、「IT人材における情報セキュリティスキル強化についての取組」として、「情報セキュリティ強化対応CCSF」の活用を推進しています。
- 「情報セキュリティ強化対応CCSF」は下記のURLからダウンロードできます。ご自由にご利用下さい。

IT人材における情報セキュリティの育成ニーズ・課題調査

報告書（概要版）

2014年3月

独立行政法人情報処理推進機構

IT人材育成本部　HRDイニシアティブセンター

http://www.ipa.go.jp/jinzai/hrd/security/index.html

※ 文中で使用されている図は、無料素材、または、IPAの公表物に掲載されているものです。