2013 情財第 0284 号（変更契約番号 2013 情財第 386 号）

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（詳細版）

平成 26 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

目　次

（空白）

第1章　調査概要

1.　調査の背景・目的

近年、情報セキュリティ上のリスクが高度化・多様化し、情報サービスを提供する側にもさらなる情報セキュリティ分野の人材育成の強化が求められている。こうした状況を踏まえて、経済産業省は 2012 年度に「平成 24 年度情報セキュリティ対策推進事業（情報セキュリティ人材の育成指標等の策定事業）」を実施し、IT スキル標準（ITSS）、情報システムユーザースキル標準（UISS）、組込みスキル標準（ETSS）の既存の３スキル標準[1]の見直し案等についての検討を行った。独立行政法人情報処理推進機構（以下「IPA」という。）では、IT 人材のスキル向上を目的とし、３スキル標準及び共通キャリア・スキルフレームワーク（CCSF[2]）等のスキル指標を整備しており、経済産業省の見直し案を受けて、IT 人材の育成において情報セキュリティを強化する場合の指標として参照することを目的とする「情報セキュリティ強化対応 CCSF」を作成・公表している。

今後、IPA では、情報サービスを提供する企業（IT ベンダー）やユーザー企業の情報システム部門において、スキル指標を活用した情報セキュリティ人材育成の動機づけを図るとともに育成促進を目的とした一連の事業を進めることを計画している。

現在整備されているスキル指標は、情報セキュリティの脅威に対応するためのタスクやスキルが整理され、網羅性の観点からの完成度が高い一方、懸念する具体的な脅威に対するタスクやスキルとの関係が明示されにくい面もある。そのため、スキル指標を活用して、情報セキュリティ人材育成の取り組みの動機づけや効果的な育成促進を図る上では、IT ベンダーやユーザー企業の情報システム部門において顕在化している情報セキュリティに対する具体的な課題を取り上げた上で、求められる対応を明らかにし、その対応を担う人材の必要性やその人材を育成するための課題等を明確化することが効果的である。

こうした問題意識を踏まえて、本調査では、第一段階として、人材育成へのスキル指標の活用を意識した上で、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や育成課題についての調査を行った。

✧✧✧

なお、本調査は「情報セキュリティを担う IT 人材」を対象とするものであるが、その範囲は、図 1 に示すとおりである。

---

[1] IT スキル標準（ITSS）IT Skill Standard / Skill Standard for IT Professional
情報システムユーザースキル標準（UISS）：Users' Information Systems Skill Standards
組込みスキル標準（ETSS）：Embedded Technology Skill Standards

[2] CCSF：Common Career Skill Framework

「情報セキュリティを担う IT 人材」は、「ITSS 人材」および「UISS 人材」の 107 万人[3]を指す。ユーザー企業の中で、情報システム部門に所属しない人材（IT 業務を担当しない人材）及び学生や非就業者、ETSS が対象とする組込み技術者のほか、ホワイトハッカー等の人材は含まれない。また、情報サービスを提供する IT ベンダーの中でも、情報サービスを提供しない管理部門の人材は対象には含まれない。

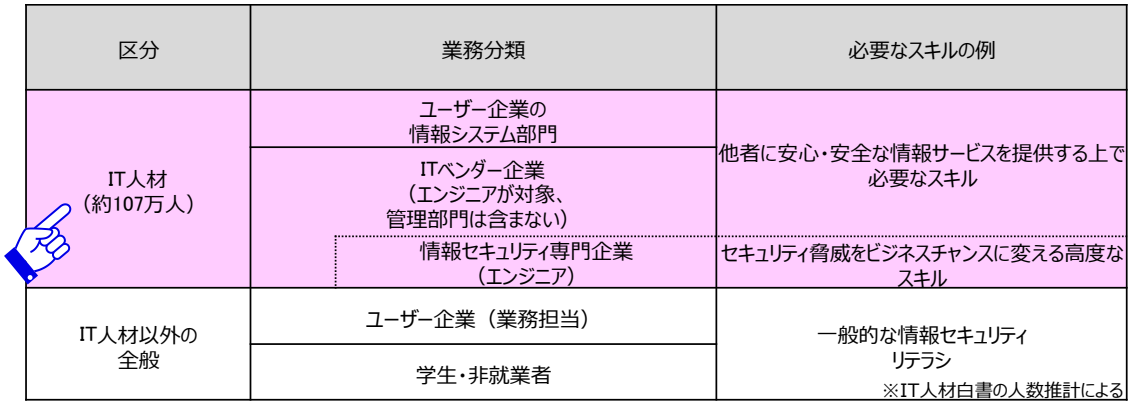

図 1　「情報セキュリティを担う IT 人材」の範囲

[3]「IT 人材白書 2013」の推計結果に基づく。

2. 実施内容

本調査では、まず、情報セキュリティを担う IT 人材の育成ニーズや課題の洗い出しを行う際の前提として、情報セキュリティ上の脅威を選定するための分析を実施した。脅威は、情報セキュリティを担う IT 人材を育成する重要性を示す際の背景として注目するためのものである。また、この分析では文献等に基づいて情報セキュリティに関する事象の抽出と分類を行う。これらの分析結果に基づいて、本調査において中心的に取り上げる情報セキュリティ上の脅威を選定した。

続いて、選定した情報セキュリティ上の脅威に基づき、文献調査等によって企業の抱える育成ニーズや課題についての調査を実施した。その後、文献調査及び有識者ワーキンググループ（WG）における検討結果等も踏まえて、インタビュー調査を実施し、情報セキュリティを担う IT 人材の育成に関する取り組みの状況や課題等についての把握を試み、それらを成果物として取りまとめた。

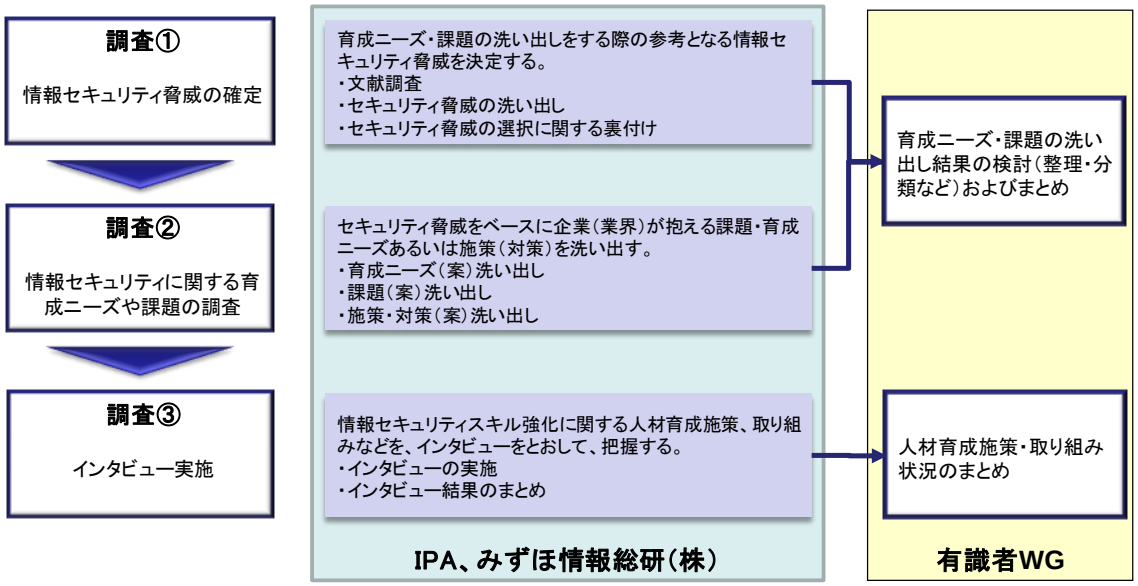

図 2　本調査の流れ

なお、本調査の成果は、本報告書（最終報告書詳細版）に取りまとめるとともに、最終報告書概要版、冊子成果物としても別途示している。

3. 実施体制

本調査の実施体制を、以下に示す。

本調査は、IPA 内の HRD イニシアティブセンターにより実施され、みずほ情報総研株式会社が、具体的な調査業務を担当した。

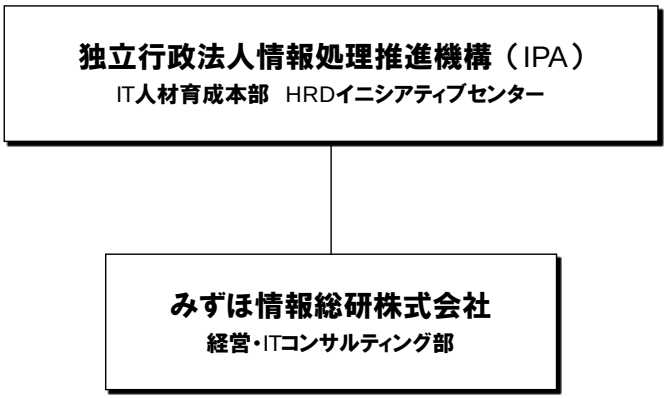

図 3　本調査の実施体制

第2章　有識者ワーキンググループの編成等

本調査では、調査の妥当性を確保し、調査結果に有識者の知見を取り入れるために、有識者ワーキンググループ（以下、「有識者 WG」という。）を設置し、計３回の WG を開催した。本章では、その概要を示す。

1.　委員構成

有識者 WG の構成員は、以下のとおりであった[4]。

(1)　座長

大木榮二郎　　工学院大学　学長補佐　教育支援機構長　教授

(2)　委員（敬称略／50 音順）

小屋晋吾	トレンドマイクロ株式会社　執行役員　統合政策担当部長
塩崎哲夫	富士通株式会社　クラウド事業本部　チーフアーキテクト
杉浦　昌	日本電気株式会社　CSIRT 推進センター　シニアエキスパート
浜田達夫	一般社団法人日本情報システム・ユーザー協会　常務理事
安田　守	株式会社野村総合研究所　情報セキュリティ部長

(3)　オブザーバ

委員参画企業

経済産業省 商務情報政策局 情報処理振興課

(4)　事務局・調査実施機関

秋元裕和	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　センター長
木村美子	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　研究員
原田奈美	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　事業グループ　研究員
武田俊幸	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　企画グループ

みずほ情報総研株式会社

[4] 所属・役職に関する情報は、平成 26 年 3 月時点のもの。

2. 開催概要

有識者 WG は、表 1 のとおり開催された。

表 1　有識者 WG 開催記録

回	日程	議題
第 1 回	2013 年 12 月 18 日（水）	• 事業概要説明 • 情報セキュリティ上の脅威の抽出と洗い出し • 情報セキュリティ上の脅威の選定
第 2 回	2014 年 1 月 22 日（水）	• 各脅威において注目する人材 • 情報セキュリティを担う IT 人材育成ニーズと課題 • 情報セキュリティを担う IT 人材育成に関する課題と取り組み例
第 3 回	2014 年 2 月 19 日（水）	• インタビュー調査結果報告 • 最終報告書概要版（原案）の検討

各 WG での討議の内容（抜粋）を、「３．議事概要」に示す。

3. 議事概要

第１回から第３回の有識者 WG において議論・検討された内容の抜粋（要約）を、以下に示す。

(1) 第１回有識者 WG

① 今求められている情報セキュリティを担う人材

- 組織の中でセキュリティ対策を行う上で課題になっているのが、対策を推進する人材が不足している点である。マネジメントの人材を活用する手段もあるが、セキュリティ人材としては十分ではない。そのため、マネジメントの中でも、特にセキュリティ対策推進に特化したマネジメント人材に焦点を当てる必要がある。
- セキュリティ対策には、セキュリティポリシーやルールを策定する人材のほか、教育を行うためのコンテンツを作る人材、ガイドラインに基づいて監査を行う人材等、様々な人材が必要であるが、特に本調査では、セキュリティを担う技術者に焦点を当てていることを明示する必要がある。
- 本調査において、個人が様々なスキルを身に付ける必要性を示唆できるとよい。例えば、標的型攻撃の対策といっても、多くのスキルが必要になる。しかし、ウイルス対策やネットワークの監視等のスキルが限定されている人材が多く、セキュリティ対策に様々な人材が必要になっている。上述の点は、あらゆるセキュリティベンダーが苦労している部分でもある。
- 従来では、ある１つのスキルを持っていれば対策は可能であった。しかし、近年は脅威同士が連動しており、複数のスキルを保有していることが必要になっている。
- IT の分野では５～６年程前から、特定分野のスキルではなく、複数のスキルを保有する“山脈型モデル”が重要であると言われている。そのような人材は、セキュリティ対策を組織全体で推進するためには重要である。
- 企業にとって、セキュリティを担う技術者は、長年現場で経験を積んでいるほど活用しにくくなっている。セキュリティ業界におけるキャリアパスが明確されていないことが大きな問題であると考えている。
- キャリアパスが明確化されていないと、いくら周囲から技術を認められていても、それ以上キャリアアップできる可能性が低くなってしまう。
- 組織として、セキュリティを長年経験した技術者の使い道が分からないという面もあり、マネジメント人材として活躍していくしかないのが現状である。一方で、長年経験を積んだ技術者がマネジメントの方面に進んでしまうと、後継者への技術の継承が進まず、育成につながらないという問題もある。

② 本調査で取り上げる情報セキュリティ上の脅威について

- 過失・怠慢等のような古典的な脅威であっても、現実的に大きな課題となっているため、脅威として加えることはできないか。ほかにも、例えば内部不正において、不正だけではなく過失・怠慢を含めることも可能である。
- 内部犯行という表現は、意図的な行動に限定されている。しかし、実際は、ルールは存在するものの守られない場合も多く、人がルールを守らないという点が組織における大きな脅威になっている。
- 内部不正の“不正”という表現は取り締まるという意味にとらわれ易い。不正ではないインシデントについては、事前予防という形で入れるのも良い。
- クラウドサービスに関しては、クラウド事業者だけでなく、ユーザー側においても暗号化等による対策が必要である。
- クラウド事業者側の視点だけではなく、クラウドを利用する側の視点も必要である。
- 経営者にインパクトを与える上では、ケーススタディを取り上げるとより現実的で効果的である。
- ケーススタディについては、脅威の中に事例として取り上げる方向で検討を行う。また、今回取り上げた脅威とは別に検討が必要な項目がケーススタディより存在した場合は追加して取り上げる可能性もある。
- 脅威を受けている対象（技術、組織体制、組織運用等）を示すと、経営者にとって分かりやすいのではないか。例えば、脅威を受ける対象が技術であれば、プログラムの脆弱性の問題から、対策としてセキュアなコーディングやセキュアなチェックが必要である。
- １つの脅威に対してベーシックな対策を含めて、全ての対策を記述すると訴求力が失われてしまうため、経営者・管理者が理解しやすい対策に絞り込みたい。
- 対策を網羅的に記述することも重要であるが、情報セキュリティ人材育成を動機付けるキャッチーで訴求力のある結論を出していきたい。
- 企業の経営側からの視点では、今、必要な人材や、その人材を企業内で育成すべきかアウトソーシングするか等を示した企業規模毎・業種毎の指針が必要である。
- 焦点を当てる脅威を選定することは、全体像を見据えながら訴求するメッセージを明確化する上では良い。しかし、脅威を選定した後で、全体像を振り返ったときに選定した脅威が妥当であったか確認し、さらに、脅威を選定し直した段階で現状の人材像でカバーできている範囲を確認することで、また改めて全体像を振り返っていくような流れが望ましい。

(2) 第 2 回有識者 WG

① 脅威や対策の選定について

- 特定の脅威に限らない脅威「全体」は非常に重要である。ユーザー企業同士で議論すると、この「全体」の部分が焦点になることが多い。JUAS の「企業 IT 動向調査」によれば、CISO を設置している企業は大企業でも全体の 4 分の 1 程度である。実態としては、CISO を補佐する「セキュリティリーダー」のような人材が現場を動かしている。セキュリティリーダーは、経営に対して説得・提案を行い、シナリオを描いた上で経営層を動かして、その考え方を現場に伝え指導する役割を担っている。ユーザー企業では、この「セキュリティリーダー」がキーパーソンになっている。
- ユーザー企業では、セキュリティ対策を全部自社内で行う企業と外部にすべて任せる企業に二極化している。そのような企業に対して、自社内で実施すべき範囲と外部に任せても問題のない範囲についての考え方を示せると良い。
- 「クラウド利用におけるデータ消失・流出」の原因としてよくあるのがバックアップミスやオペレーションミスである。また、ファイアウォールの設定ミスやアクセスコントロールミス、ID・パスワードの不正利用によるものも多い。このように考えると、資料に記載されたセキュリティパッチの展開よりも、アクセスコントロールの適切な管理のほうが、対策としてはイメージしやすい。また、対策を担う職種としては、IT サービスマネジメントが適していると思われる。
- 「クラウド利用におけるデータ消失・流出」に対する対策としては、パッチマネジメントではなく、アクセスコントロールの運用のほうが分かりやすい。

② ベンダー人材の位置づけについて

- 「対策に関連する人材像」にはベンダーとユーザーの両方の視点が入っているという点について冒頭で示しておく必要があるのではないか。
- IT ベンダーの経営層や人材育成担当者とユーザーの人材育成担当者が、同じ成果物を閲覧することを考えると、資料 3 では IT ベンダー側とユーザー側で、それぞれどのようにして解釈すればよいのかを示す必要がある。
- インシデント発生時の対策か、システムが開発される段階での対策かによって対策は異なる。「不正アクセスにおける対策」には、インシデント発生時の対策があるが、そもそもプログラム自体に脆弱性が存在することもあり、どのタイミングでの対策なのかを示す必要がある。
- 対策の説明には、フェーズを示したほうが分かりやすい。
- 成果物に記載する対策を、各フェーズで書いたほうが理解しやすいのか、フェーズを意識せず冒頭でまとめて述べたほうが理解しやすいかについては、成果物を作成

する段階で検討したほうが良い。

③ 情報セキュリティを担う人材のニーズについて

- 情報セキュリティ人材が足りないことを示すだけではなく、人材が足りないことが企業にどのような影響を及ぼすのかまで踏み込んで示す必要がある。
- 経営者に対する説得力を高めるため、報告書では、セキュリティ人材に対して足りないと感じている度合が、他の職種と比べて高いことを示せれば効果的である。
- セキュリティ人材の流動性を含めたキャリアパスの例やモデルを示すことができれば、企業にとっては育成の方法が、個人にとっては自分の成長がイメージできるため、有益なのではないか。
- 企業内でのキャリアパスとは異なるセキュリティ技術者としてのキャリアパスを示すことができれば、セキュリティ技術者のキャリアパスがイメージされるようになるのではないか。
- 特化した専門性よりも幅広い能力を求める日本の組織のあり方と情報セキュリティ人材の育成について、業界としてどのように捉えていくか、何らかの提言があってもよいと感じた。
- 企業内で活躍するためには、セキュリティだけしか知らないという状態では難しく、ある程度幅広い能力を持った人材が重要である。また、そのような人材が各企業に必ず必要であるということを明示することが重要である。日本のユーザー企業では、ジョブローテーションも頻繁に行われ、経験がないのに突然セキュリティの担当者になる場合もある。日本の企業におけるセキュリティ人材の育成は、このような前提で考える必要がある。
- 社外からセキュリティの専門家を獲得しようとするユーザー企業は少ないのが現状である。セキュリティに関しては、コンサルティング会社を活用している企業が半分程度に上る。こうした日本の企業の実態も踏まえておくことが重要である。

④ 本調査の成果物について

- セキュリティの専門家ではない読者を想定した資料に専門用語が多く含まれていると、拒絶される恐れがあるため、その点には留意が必要である。
- 大企業はすでに情報セキュリティに関しても十分な対策を実施している場合が多いと考えられるため、今回の読者としては中堅規模の企業を想定する必要があるのではないか。

(3) 第 3 回有識者 WG

① インタビュー調査結果について

- インタビュー調査結果では、情報セキュリティに関する様々な人材像が混在している。大きく分類すると、セキュリティのスペシャリストと、IT を専門とした業務を行う管理者・担当者、現場の技術者や利用者等のセキュリティを知っていたほうが望ましい人材の３つに分類される。
- セキュリティに関する人材育成を考える上では、事業を行うために必要な情報セキュリティ人材の量と質と情報セキュリティ人材の育成方針の２点が重要である。
- 情報セキュリティを担う人材の育成について、一定レベルまでは教育によって育成可能であるが、それ以上のレベルになると、コミュニティでの専門家による情報共有等に頼らなければならないというインタビュー調査結果は非常に興味深い。
- 情報セキュリティを担う人材のような専門的人材の処遇や育成の方法は、日本ではまだ確立していない。これらについては、今後の検討課題であるといえる。
- 情報セキュリティ対策を、単に事故が多いから対策を行うと考えていると、“なぜ事故を防ぐために投資をしなければならないのか”という発想になりがちである。資料に、現場のセキュリティ担当者だけでなく、全社的にセキュリティマインドを身につけたほうが良いとの意見もあるように、日本では“事件・事故対応のための情報セキュリティ対策”という考えに留まっているという印象を受ける。これでは、必要最低限の人数で対策を行う発想は変わらないため、情報セキュリティは企業の機能であるという点を社会で共有していかなければならない。
- 情報セキュリティを担う人材にも、例えば、企業内でサービス・ビジネスを促進する人材や、セキュリティのノウハウを保有しながら社外教育等のビジネスを創出する人材も必要である。
- 情報セキュリティの分野の現状は、20 年前の IT の状況と類似している。IT と経営については、相互の距離を縮めるため、見える化等の IT と経営の関係について長期間かけて説明することで理解を促した。経営層は情報セキュリティに対して危機意識はあるが、具体的なことまで理解できていないことが多い。IT と同様に、セキュリティと経営の関係を見える化し説明・提案をすると、経営に対するセキュリティの重要性について理解を得ることができる。現在ユーザー企業同士でも、見える化や説明責任を果たすことのできる人材の育成について議論している。上のような観点から、セキュリティと経営の関係に関する理解を促進していくために“経営と現場をつなぐキーマンの育成”が重要である。IT の場合は、経営と IT の関係を学び、経営の中での IT の必要性を説明した人材がキーマンであった。そのような人材が、情報セキュリティ人材においても必要である。
- ユーザ企業のセキュリティ担当者は、特に IT インフラに関する業務を担当してい

た人材が多い。インフラといっても、その企業にとってのインフラであることから、ビジネスに関する知識も有している。また、ユーザー企業では５～７年程度の周期でローテーションが行われるのが、一般的ではないか。

② 最終報告書概要版（原案）の検討

- 例えば、“情報セキュリティ対策の優先順位が設定できていない”、“セキュリティ対策に必要な人材が理解できていない”等、具体的に足りていない項目を示すと分かりやすい。
- 「経営の理解が足りない」等のネガティブな表現ではなく、経営者に対しては、情報セキュリティ人材の育成による効果等、ポジティブな表現で表したほうが望ましい。企業では、自社のビジネス範囲内で育成すべき人材像を、ビジネスリスクを踏まえて決めていく必要がある。また、一般企業の中で情報セキュリティをリードしている人材を例に出して紹介することで、より経営層の理解が高まるのではないか。
- 情報セキュリティについては、企業の負担から付加価値へと転換していくことが必要であるという議論をしてきた。付加価値のようなプラスの面は冒頭で述べ、被害の大きさ等のマイナスの面は後半で述べる等、「経営層の理解が足りない」という表現には工夫が必要である。
- ユーザー企業の中には、専門的な業務はアウトソースするため情報セキュリティについて理解する必要性を感じていない企業もある。そのため、アウトソースする側も情報セキュリティについて理解しておく必要があることを記載しておくと良い。
- 情報セキュリティを実際に運用するには、セキュリティやネットワーク等の専門知識に加え、ヒューマンスキルを活用した社内・外への折衝能力が求められる。そのため、情報セキュリティ担当者はヒューマンスキルも含めた広範囲なスキル・知識を有する必要がある。
- 上のような人材は、業務とビジネス、IT、セキュリティについて浅く広く知識を有する人材である。そのため、知識・スキルの深さ・広さで表現してはどうか。
- 最近の情報セキュリティは、脅威を起こす攻撃者側に人間の意識が存在するという点が特徴の１つとなっている。そのため、脅威ベースで考えると、今後も常に情報セキュリティ人材は不足するのではないか。

第3章　情報セキュリティ上の脅威の選定

本調査では、情報セキュリティを担う IT 人材の育成ニーズや課題の洗い出しを行う際の前提として、情報セキュリティ上の「脅威」を選定するための分析を実施した。本調査で選定する脅威は、情報セキュリティを担う IT 人材育成の重要性を示す際の背景として着目するためのものである。

情報セキュリティの分野では、きわめて幅広く多種多様な脅威に対する対応が求められている。しかし、本調査の成果物の読者に対して、情報セキュリティを担う IT 人材の重要性を伝える上で、広範な脅威に対する全方位的な対応の必要性を示すことは、必ずしも効果的であるとは言いがたい。また、情報セキュリティに関する網羅的な対策の必要性を示す既存の資料はすでに数多く存在している。本調査では、成果物の想定読者である企業が、CCSF を活用した情報セキュリティを担う IT 人材の育成に、これまでに以上に積極的に取り組むようになることを目指して、まずは読者の注意喚起が行いやすい脅威を選定し、それを糸口として情報セキュリティを担う IT 人材の重要性や CCSF の活用法を示すこととした。

こうした認識に基づいて、本調査では、まず文献調査に基づいて脅威の収集、選定を実施し、その後、選定結果に対する分析を行った。本章には、その結果を示す。

図 4　情報セキュリティ上の脅威の例

1. 文献調査結果

文献調査において、IT 人材における情報セキュリティの育成ニーズや課題の洗い出しをする際に参考となる情報セキュリティ上の脅威を文献から収集した。

(1) 収集の観点

以下の 3 つの観点に基づいて、情報セキュリティ上の脅威を文献から収集した。

- **情報セキュリティ事象の網羅性を踏まえた観点**

  情報セキュリティ事象の網羅性を担保するための一例として、「情報セキュリティの分類」がある。情報セキュリティ上の脅威を収集する段階で、特定の事象に偏ることなく収集するために、「情報セキュリティの分類」を参考とする。「情報セキュリティの分類」には、(A)、(F)、(G) 等の脅威と (B) ～ (E) の対策が含まれており、脅威と対策の関係をセットにした内容を一体として情報セキュリティ上の脅威として捉える。

表 2 情報セキュリティの分類

(A) 攻撃：ウイルス、サイバー攻撃、侵入検知、フィルタリング　等
(B) 情報セキュリティマネジメント（運用・体制）：セキュリティポリシー、監査、ISMS、CISO・CSIRT の設置　等
(C) 教育：要員教育、管理者教育、非正規社員・協力会社教育、倫理教育　等
(D) 情報管理：個人情報保護、知的財産保護、プライバシー、データの格付け　等
(E) セキュリティインシデント発生時の対応：体制、ルール　等
(F) 内部不正
(G) その他（標的型攻撃メール、フィッシングサイト、ボット　等）

- **「情報セキュリティ強化対応 CCSF」の定義による観点**

  本調査では、「情報セキュリティ強化対応 CCSF」で定義した IT 人材の活躍イメージがわきやすく人材育成強化が動機づけられる情報セキュリティ上の脅威を選定するため、情報セキュリティ上の脅威に関する文献調査においても、「情報セキュリティ強化対応 CCSF」のタスクや職種等を参考とする。具体的には、脅威を対策とセットで選定するため、脅威を選定すれば対策が決まり、順に対策に必要なタスク、そのタスクを担う人材を整理する。

- **具体的な脅威事例の観点**

  セキュリティ上の脅威の選定では、実際に足元で発生している脅威や今後被害が増すと想定される脅威を選定することが、情報セキュリティを担う IT 人材の強い育成ニ

ーズや課題認識を拾い上げることにつながると期待できる。そのため、近年、発生している具体的な脅威事例を調査する。

(2) 対象文献

以下に、今回調査対象とした文献を示す。人材育成関連の文献は、参考資料として活用した。

表 3　対象文献・参考文献

【対象文献】

① 2013 年版 10 大脅威　身近に忍び寄る脅威！　-（独）情報処理推進機構

② 情報セキュリティ白書 2013　　-（独）情報処理推進機構

③ 2012 年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】
-（NPO）日本ネットワークセキュリティ協会

④ 2012 年 セキュリティ 10 大ニュース　-（NPO）日本ネットワークセキュリティ協会

⑤ 2012 年度インターネット脅威年間レポート　　-TREND MICRO

⑥ インターネット セキュリティ脅威レポート 第 18 号　-Symantec

⑦ McAfee 脅威レポート :2013 年第 2 四半期　-McAfee

⑧ 2013 年の脅威予測　-McAfee

【参考文献】

⑨ 平成 24 年度情報セキュリティ対策推進事業（情報セキュリティ人材の育成指標等の策定事業）　-経済産業省

⑩ IT 人材白書 2013　-（独）情報処理推進機構

⑪ IT スキル標準概要　-（独）情報処理推進機構

⑫ 情報セキュリティ強化対応 CCSF　-（独）情報処理推進機構

(3) 抽出方法

情報セキュリティ上の脅威は、上記対象文献（情報源）の中から、近年発生している具体的な脅威事例やセキュリティ事象に関連すると考えられるキーワードから抽出した。ただし、各文献での掲載（見出し項目等）を基本材料とした。

(4) 抽出結果

対象文献を、発行元と業種を基に【A】～【C】の３つに分類した。

【A】: IPA が発行元である２文献（表 3 の①、②が該当）
【B】: JNSA が発行元である２文献（表 3 の③、④が該当）
【C】: アンチウイルスベンダーが発行元である４文献（表 3 の⑤～⑧が該当）

分類毎の抽出結果を以下に示す。数字は、当該脅威や情報セキュリティ事象が確認できる文献数である。

表 4　情報セキュリティ事象の抽出結果

【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	2	標的型攻撃、サイバー攻撃	1	標的型攻撃（サイバー攻撃）	4
ウェブサイトを狙った攻撃	2	著作権法改正への抗議攻撃	1	スマートフォン・モバイル	3
スマートデバイスを狙った悪意あるアプリ、ウイルス	2	スマートフォンに迫る脅威	1	マルウェア・エクスプロイト、ウイルス	3
ウイルス、マルウェア	2	ウイルス、ワーム	1	データ消失・データ侵害	2
予期せぬ業務停止（クラウド）	2	サーバの障害とデータ消失	1	クラウド	2
脆弱性を突いた攻撃	2	クラウドの課題	1	ツールキット・不正アプリ	2
フィッシング詐欺	2	ネットバンキング	1	SNS	2
内部犯行	2	情報セキュリティ人材不足	1	ネットバンキング	1
パスワード流出の脅威	1	不正アクセス禁止法	1	情報セキュリティ人材	1
不正アクセス	1	管理ミス、誤操作、設定ミス	1	著作権法	1
制御システムの情報セキュリティ対策	1	目的外利用	1	不正アクセス禁止法	1
マイナンバー法案	1	紛失、置き忘れ	1	ハクティビズム	1
スパムメール	1	バグ、セキュリティホール	1	脆弱性（ゼロデイなど）	1
サイバー空間上のデモ活動	1	内部犯行、内部不正行為	1	スパム	1
DDoS 攻撃	1	不正な情報持ち出し	1	フィッシング	1
電子証明書の悪用	1			ソーシャルエンジニアリング	1
電子政府推奨暗号リスト	1			国や地域に特化	1
				アドウェア	1

2. 情報セキュリティ上の脅威の洗い出し

文献より抽出された脅威やセキュリティ事象の結果（表 4）から、注目度、理解度等の選定の観点に基づき、脅威を選定する。選定した結果を必要に応じて細分化や統合を行うことで、脅威の洗い出しを実施した。

(1) 選定の観点

本調査では、あくまで企業における人材育成を意図した脅威の選定を行うにあたり、以下の観点に基づいて、選定した。

- 注目度、理解度の観点
  - 新しすぎる脅威は一般的に顕在化していない可能性があり、注目・理解されていないので選択しない
  - 古い既知の脅威は、理解されているが新鮮さ・注目度が低いため、選択しない
- 脅威の影響範囲の観点
  - 広範囲な対象を狙った脅威を選定する
  - 企業（IT 人材）に影響のある脅威を中心に選択する
  - インターネットバンキングなど金融関係等の特定機関に特化した脅威は選択しない
- 対策との結びつきの観点
  - あらゆる人材が対策を担う場合、対象となる人材の選択が困難になるため選択しない
- 脅威の普遍性の観点
  - 掲載量が多く、掲載される文献や発行元に偏りのない脅威を中心に選択する
  - 掲載される文献や発行元に偏りがあっても、企業におけるセキュリティ上の脅威として注目すべきと判断される場合は選択する

(2) 細分化と統合

上記観点に基づき選定した脅威において、脅威の内容が重複している場合や複数の脅威が一つにまとまっている場合、脅威の細分化や統合を行い、整理した。

(3) 洗い出し結果

上記の観点に基づいて選定した脅威に対して、細分化や統合を行い、情報セキュリティ上の脅威を洗い出した結果を以下に示す。「内部犯行」「内部犯行、内部不正行為」について、アンチウイルスベンダーが発行する文献に関連する脅威の記載はないが、企業におけるセキュリティ上の脅威として注目すべきと有識者 WG 及び事務局にて判断され

たため、選定に含めた。

【A】IPA		【B】JNSA		【C】アンチウイルスベンダー	
スマートデバイスを狙った悪意あるアプリ、ウイルス	2	スマートフォンに迫る脅威	1	スマートフォン・モバイル	3

→「**スマートデバイスからの情報漏えい**」として整理した。

【A】IPA		【B】JNSA		【C】アンチウイルスベンダー	
ウイルス、マルウェア	2	ウイルス、ワーム	1	マルウェア・エクスプロイト、ウイルス	3

→「**エクスプロイト**」として整理した。「ウイルス、マルウェア」の脅威内容を確認すると、アンチウイルスソフトを導入すれば解決するような内容ではなく、標的型攻撃の一部として記載する。よって「ウイルス、マルウェア」は下記の標的型攻撃と統合する。

【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	2	標的型攻撃、サイバー攻撃	1	標的型攻撃（サイバー攻撃）	4

→上記と併せて、「**標的型攻撃・サイバー攻撃（マルウェア、ウイルスを含む）**」として整理した。

【A】IPA		【B】JNSA		【C】アンチウイルスベンダー	
予期せぬ業務停止（クラウド）	2	クラウドの課題	1	クラウド	2

→「**クラウド利用におけるデータ消失・流出**」として整理した。

【A】IPA		【B】JNSA		【C】アンチウイルスベンダー	
不正アクセス	1	不正アクセス禁止法	1	不正アクセス禁止法	1

→「**不正アクセス**」として整理した。

【A】IPA		【B】JNSA		【C】アンチウイルスベンダー	
脆弱性を突いた攻撃	2	バグ、セキュリティホール	1	脆弱性（ゼロデイなど）	1

→親和性より、上記の「**エクスプロイト**」と統合した。

【A】IPA	【B】JNSA	【C】アンチウイルスベンダー

内部犯行	2	内部犯行、内部不正行為	1	—	—

→「**内部不正・うっかりミス**」として整理した。

洗い出した結果を以下に示す。本調査では、「標的型攻撃、サイバー攻撃（マルウェア、ウイルスを含む)」、「不正アクセス」、「エクスプロイト」、「クラウド利用におけるデータ消失・流出」、「スマートデバイスからの情報漏えい」、「内部不正・うっかりミス」の６つの脅威を選定した。

表 5　選定した脅威

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窃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思想を持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やうっかりミスによる情報セキュリティ上のインシデント

3. 情報セキュリティ上の脅威の選定に関する裏付け

選定した脅威について、「資産・保護対象」、「攻撃者（脅威源）」、「影響」について分析した結果を以下に示す。下表の通り、今回の選定は概ね各項目を網羅した脅威を選択している。

No	脅威	資産・保護対象	攻撃者（脅威源）					影響			具体的事象
			内部者	特権者	外部者	関係者	その他	C	I	A	
1	標的型攻撃、サイバー攻撃（マルウェア、ウイルスを含む）	企業が保有する重要情報			◎			◎			・重要情報（開発情報等）の漏えい ・クライアント保有の重要情報（個人情報・取引情報等）の漏えい
2	不正アクセス	サーバ保存の重要情報			◎			◎	○		・クレジットカード情報を不正入手 ・Web 情報の改ざん
3	エクスプロイト	サーバ、クライアント保存の重要情報			◎			◎			・サーバ保有の重要情報の漏えい ・クライアント保有の重要情報の漏えい
4	クラウド利用におけるデータ消失・流出	クラウドサービス保存の重要情報・サービス機能			○	◎			○	◎	・クラウドに保存したデータが消失 ・サービス機能の停止／低下
5	スマートデバイスからの情報漏えい	スマートフォンで扱う重要情報	◎		○			◎			・不正アプリによる電話帳情報等の漏えい ・スマホの置忘れによる重要情報の漏えい
6	内部不正・うっかりミス	開発情報・営業秘密情報	◎	○				◎			・元社員による営業情報の持ち出し ・内部者から競合他社への漏えい

4. 選定した脅威と対策、タスク・役割の関係

脅威に対して、企業は一つの対策を実施すれば十分というわけではなく、複合的な対策（トータルセキュリティ）が必要である。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・役割の関係は以下のようになる。

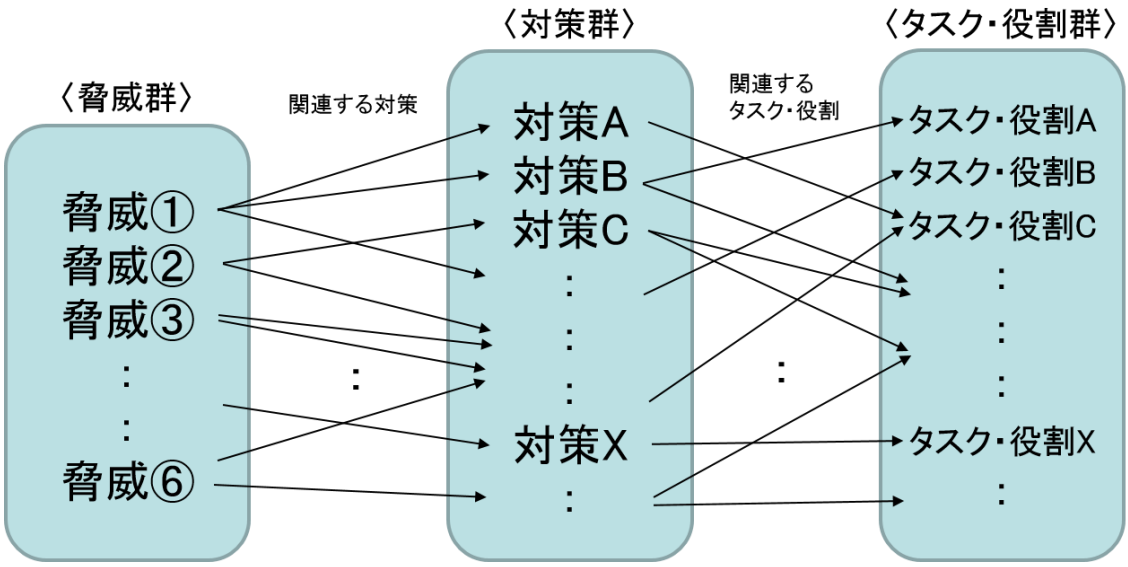

図 5　脅威、対策、タスク・役割の関係

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・役割を整理する際に以下の資料を参考とした。

表 6　参考文献

① 標的型サイバー攻撃の事例分析と対策レポート　（IPA）
② 標的型攻撃／新しいタイプの攻撃の 実態と対策　（IPA）
③ スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン第一版（BYOD 基礎資料追加版）　（JSSEC）
④ 企業が実施すべきスマートデバイス利用時のセキュリティ対策　（HISOL）
⑤ クラウドサービス利用のための情報セキュリティマネジメントガイドライン　（METI）
⑥ クラウドセキュリティガイドライン活用ガイドブック（ドラフト）　（METI）
⑦ 組織における内部不正防止ガイドライン　（IPA）
⑧ 安全なウェブサイトの作り方　改定第６版　（IPA）
⑨ 不正アクセス対策のしおり　（IPA）
⑩ スマートフォンのセキュリティ対策のしおり　（IPA）
⑪ 標的型攻撃メール対策のしおり　（IPA）

⑫　中小企業における組織的な情報セキュリティ対策ガイドライン　(IPA)

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・役割を以下に示す。タスク・役割は、「情報セキュリティ強化CCSF」に関連している。

①　標的型攻撃、サイバー攻撃（マルウェア、ウイルスを含む）

対策例	各企業の検討動向として特筆すべき点としては、「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）	
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	
上記タスク・役割に関連する職種・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）

②　不正アクセス

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。
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	
脅威への対策として重要なタスク・役割	① 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 ② 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	
上記タスク・役割に関連する職種・専門分野例	ITSS：	① IT スペシャリスト（セキュリティ） ② IT サービスマネジメント（運用管理）
	UISS：	① システムデザイナー ② IS オペレーション

③ エクスプロイト

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、ソフトウェ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。	
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	
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	
上記タスク・役割に関連する職種・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

④ クラウド利用におけるデータ消失・流出

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。	
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	
脅威への対策として重要なタスク・役割	①　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 ②　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	
上記タスク・役割に関連する職種・専門分野例	ITSS：	①　IT アーキテクト（セキュリティアーキテクチャ） ②　IT サービスマネジメント（運用管理）
	UISS：	①　IS アーキテクト ②　IS オペレーション

⑤　スマートデバイスからの情報漏えい

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、インシデンド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	
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	
上記タスク・役割に関連する職種・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）

⑥　内部不正・うっかりミス

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	
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	
上記タスク・役割に関連する職種・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）

選定した脅威への対策として特に重要と判断したセキュリティに関連するタスク・役割の分類を以下に示す。ただし、以下には特に重要と判断されたタスク、役割を明示しているが、脅威に対抗するには１つではなく、テクニカル系、マネジメント系などの複数の対策（トータルセキュリティ）が必要であることに留意する必要がある。

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				◎	

図 6　タスク・役割の分類

第4章　IT 企業の情報セキュリティに関する育成ニーズや課題の事前調査

1.　文献調査結果

３章で選定した脅威を含めた情報セキュリティ上の脅威に対する IT 企業の抱える育成ニーズや課題を調査した。育成ニーズや課題については、「情報セキュリティ強化対応 CCSF」で定義した IT 人材の活躍イメージがわきやすく、人材育成強化を動機づけるように分類した。

(1)　収集の観点

以下の 3 つの観点に基づいて、企業の情報セキュリティに関する育成ニーズや課題、人材育成面での対策、施策を文献から収集した。

- **マクロ視点とミクロ視点での情報収集**

  育成ニーズや育成課題等の洗い出しにおいて、マクロ視点でのニーズや課題の洗い出しは、全体動向を把握する上では効果的である一方、具体的なニーズや課題という面では、不十分な面があると考えられる。そのため、想定した脅威に対する企業等での取組や対策事例、情報セキュリティ関連サービス提供事例などから、ミクロ視点での具体的なニーズ、課題を洗い出す。

- **情報セキュリティ対策ガイドラインからの育成ニーズの洗い出し**

  人材育成ニーズの源泉は、脅威に対する情報セキュリティ対策の必要性である。特に、企業が新たな対策を進める際には、情報セキュリティ対策ガイドラインを参考とする場合が多い。そのような観点から、文献調査では、新たな IT 環境（クラウド、モバイルなど）に対する情報セキュリティ対策ガイドラインから育成ニーズの洗い出しを行う。

- **「情報セキュリティ強化対応 CCSF」活用の配慮**

  本調査では、「情報セキュリティ強化対応 CCSF」で定義した IT 人材の活躍イメージがわきやすく人材育成強化が動機づけられるような分類を行うため、文献調査においても、「情報セキュリティ強化対応 CCSF」のタスクや職種等を予め念頭におく。

(2)　対象文献

以下に、今回調査対象とした文献を示す。

表 7　対象文献

①	平成 24 年度情報セキュリティ対策推進事業(情報セキュリティ人材の育成指標等の策定事業)　-経済産業省
②	情報セキュリティ人材の育成に関する基礎調査　-（独）情報処理推進機構
③	IT 人材白書 2013　-（独）情報処理推進機構
④	情報セキュリティ白書 2013　-（独）情報処理推進機構
⑤	情報セキュリティ?材育成に係る現状と今後の検討課題について　-内閣官房情報セキュリティセンター
⑥	耐災害性を強化した情報システムの在り方等に関する調査　-内閣官房情報セキュリティセンター
⑦	インシデント報告対応レポート [2013 年 1 月 1 日～2013 年 3 月 31 日]　-JPCERT/CC
⑧	標的型サイバー攻撃の事例分析と対策レポート　-（独）情報処理推進機構
⑨	標的型攻撃／新しいタイプの攻撃の 実態と対策　-（独）情報処理推進機構
⑩	スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン第一版（BYOD 基礎資料追加版）　-JSSEC
⑪	企業が実施すべきスマートデバイス利用時のセキュリティ対策　-日立ソリューションズ
⑫	クラウドサービス利用のための情報セキュリティマネジメントガイドライン -経済産業省
⑬	組織における内部不正防止ガイドライン　-（独）情報処理推進機構
⑭	安全なウェブサイトの作り方　改定第 6 版　-（独）情報処理推進機構
⑮	不正アクセス対策のしおり　-（独）情報処理推進機構
⑯	スマートフォンのセキュリティ対策のしおり　-（独）情報処理推進機構
⑰	中小企業における組織的な情報セキュリティ対策ガイドライン -（独）情報処理推進機構

(3) 抽出方法

IT 企業の育成ニーズ、育成課題、人材育成面での対策、施策は、上記対象文献（情報源）の中から、具体的に説明している内容、関連すると判断される内容より抽出した。

(4) 抽出結果

抽出結果を以下に示す。

❑育成ニーズ

- 調査対象となったユーザー企業の 77.2%、IT ベンダー企業の 75.7%が IT 人材(情報セキュリティ）の人数やスキルが足りていないと回答
- 調査対象となった IT ベンダー企業の８割が、セキュリティに関連するどの職種（「セキュリティ戦略・統括」「企画・設計」「開発・構築」「運用・管理」「セキュリティに関するコンサルティング・教育」の６職種）でも人員不足、スキル不足を感じている

- 調査対象となったユーザー企業の８割が､セキュリティに関連するどの職種(同上）でも人員不足、スキル不足を感じている
- 国内における情報セキュリティに従事する技術者約 26.5 万人のうち、約 16 万人が質的に不足、さらに 8 万人が量的に不足している
- 情報セキュリティ対策ガイドラインで明記されている対策を担当する人材が必要

❑育成課題

〈認識〉

- 経営層が情報セキュリティ人材の育成の必要性を重視していない
- 情報セキュリティ業務は苦労する割に報われないとして、組織内で敬遠されがちである
- そもそも（育成の必要性が）理解されていない。

〈専門的なスキル〉

- 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ため、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。
- 人材の異動による知識の継承が難しい
- 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

〈一般的なスキル・専門領域の拡大〉

- 情報セキュリティ対策に関する意識が低い職員の存在(職員による差が大きい)
- 社内の情報セキュリティ教育が足りない
- 情報セキュリティ技術は常に変化しているため、ある技術に固執するのではなく、柔軟に専門領域を広げていく能力も必要

〈評価〉

- 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
- セキュリティ人材を経営者が適切に評価することは困難

〈外部委託〉

- 情報セキュリティに関わる部分を本来は外部委託したくないが、現状では専門的人材のキャリアパス等を考えると外部委託せざるを得ない
- 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

〈地位・ポジション・キャリアパス〉

- 情報セキュリティ上の脅威に対応するポジションは無い

- 何も検討していない。担当者の独学（優先順位が低い）
- 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

〈IT ベンダー企業〉

- あまり専門的な人材を育成してしまうと中年以降に孤立しがちになる
- 現場はセキュリティしか知らない人材の言うことは聞かないため、他の職種を経験してもらうことが重要
- 複数領域の専門を持っていなければならない
- システム開発経験、運用経験、ＩＴマネジメント経験などの幅広い知識と経験が求められている（育成が難しい）
- 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である。
- 情報セキュリティを希望する人が少ない

〈セキュリティベンダー〉

- 人材の流動性が高い（転職等）
- 新たな脅威への対応負荷が大きい
- ITSS の達成度はセキュリティ技術者には適用しにくい（評価しづらい）
- 情報セキュリティ人材は全般的に不足しており、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
- セキュリティに詳しい人ばかりが昇進していく訳ではない

〈ユーザー企業〉

- 情報セキュリティ対策に関する取り組みは、多くのユーザー企業において、専任人材ではなく他の IT 業務と兼任する人材により遂行されている
- OJT にて勝手に育つのを待つしかない状況、そもそもセキュリティ人材の育成をユーザー企業が検討しているケースは少ないのでは。
- 本業が忙しく、情報セキュリティにまで人材が割けない
- 経営層の理解や認識が足りない
- 経営の理解が得にくい
- 社内に情報セキュリティ業務の適任者が少ない
- 採用をしたいが、情報セキュリティ業務への応募者が少ない
- セキュリティの専任担当者を置く余裕はない（特別扱いできない）
- どこがゴールなのかわからない（情報セキュリティ技術は常に変化している）

❑人材育成面での対策、施策

- 情報セキュリティ関連の資格取得や認定を受けた場合、採用での優遇、給与アップ、補助金の支給等の取り組みを行っている企業がある。

2. 育成ニーズ及び育成課題、人材育成面での対策及び施策の洗い出しと分類、確認方針の策定

文献より抽出された育成ニーズ及び育成課題、人材育成面での対策及び施策の結果の洗い出しと分類を行い、インタビュー調査における確認方針を策定した。

(1) 洗い出しと分類

文献調査の結果、全体的な傾向に関する育成ニーズや育成課題は多く確認できるが、特定の脅威に関連した具体的な育成ニーズや育成課題は確認されない。同様に、人材育成面での具体的な対策、施策に関する情報量は多くはない。また、人材育成ニーズの源泉は、脅威に対する情報セキュリティ対策の必要性であるという考えから、育成ニーズの１つに「情報セキュリティ対策ガイドラインで明記されている対策を担当する人材が必要」と挙げたが、ある脅威に対して情報セキュリティ対策を施すと判断した場合に出てくるであろう育成ニーズであり、直接的な特定の脅威に関連した育成ニーズではない。このように、特定の脅威に関連した具体的な育成ニーズや育成課題がないのは、その前段階として現在抱えている課題を、企業が解決できていない可能性が考えられる。そのため、抽出した育成課題について、同系統のものをグルーピングし、整理を行った。その結果を以下に示す。情報セキュリティを担う IT 人材の育成課題は大きく４つに分けられ、組織内（企業内）での課題が３つ、組織外の課題が１つ存在する。また、課題①～③には順序性がある。例えば、課題①が解決し、人材育成に取り組み始めても課題②があり、育成を進めると課題③に直面する。

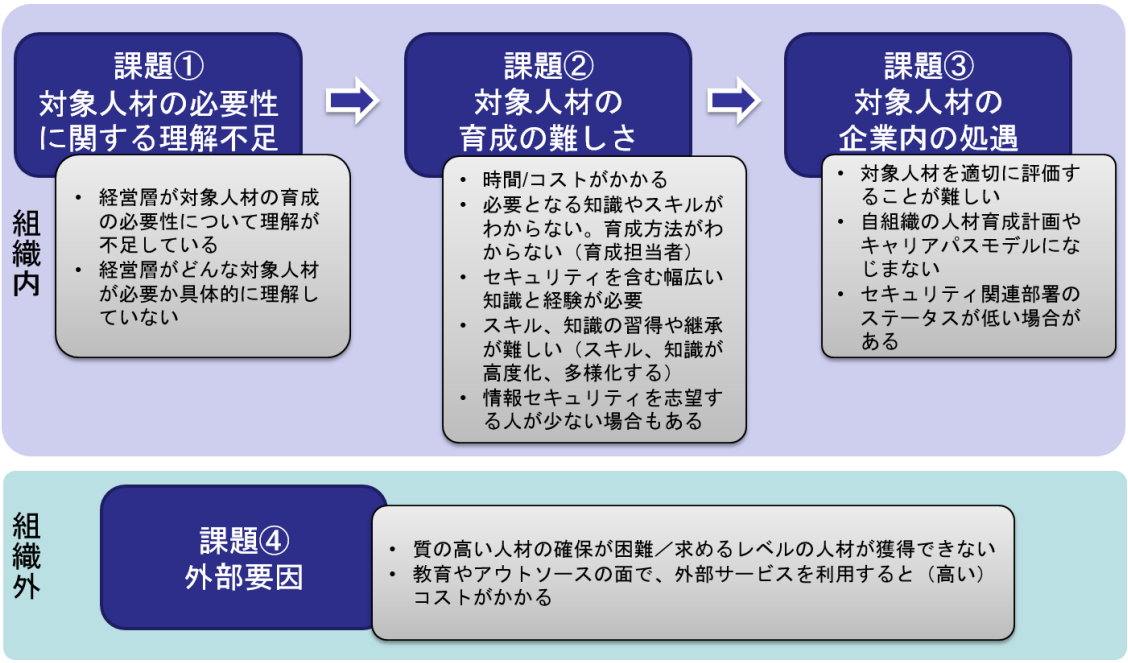

図 7　情報セキュリティを担う IT 人材の育成課題（案）

(2) 確認方針の策定

図 7 に示した情報セキュリティを担う IT 人材の育成課題のうち、課題①～③について、企業としての解決策や方針を見出すことができるかどうかで、対象人材の育成状況は変わってくると思われる。対象人材の育成に先進的に取り組んでいると思われる企業は課題①～③に対する解決策や方針を見出していることを確認方針とし、インタビュー調査でその確認を行う。また、課題④については、企業が情報セキュリティ対策を進める際に外部委託する場合や対象人材を外部から調達する場合などに、外部要因に関する課題の有無をはじめ、実際どのような印象、感覚を持っているかを、インタビュー調査で合わせて確認する。

■確認方針

A) 企業が情報セキュリティを担う IT 人材の育成を進める際に、組織内外の課題として以下の４つの課題に直面する。また、以下の課題①～③には順序性がある。

① 対象人材の必要性に関する理解不足
② 対象人材の育成の難しさ
③ 対象人材の企業内の処遇
④ 外部要因

B) 対象人材の育成に先進的に取り組んでいると思われる企業は、課題に対する解決策や方針を見出している。

第5章　インタビューの実施

1.　インタビュー調査概要

(1)　調査の趣旨と概要

IT ベンダーやセキュリティベンダー、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育成ニーズや育成課題についての実態を把握するため、前章で策定した確認方針を検証するために、インタビュー調査を行った。概要は以下の通りである。

表 8　インタビュー調査の概要

調査対象	● 情報システムを受託開発するＩＴベンダー ● 情報セキュリティ専門企業 ● ユーザー企業の情報システム部門
対象数	対象人材の育成に先進的に取り組んでいると思われる企業 7 社
調査方法	対面によるインタビュー調査
調査期間	2014 年 1 月下旬～2014 年 3 月上旬

(2)　調査項目

今回のインタビュー調査における調査項目とインタビュー項目は、以下のとおりである。

表 9　調査項目

（A）　情報セキュリティに対する意識
（B）　情報セキュリティ対策内容と関連する体制
（C）　育成に関する取り組み
（D）　育成に関する課題
（E）　対象人材の処遇、環境
（F）　外部委託、その他

表 10　インタビュー項目

■ **情報セキュリティ上の脅威に対する企業側の認識と対策について**

- 企業のガバナンスにおける情報セキュリティの位置づけと重要性
- 企業内の情報セキュリティを担う組織・人員体制
  （どのような役割を持った人材が、どのような組織に、どのくらいの規模で配置されているか）
- 情報セキュリティ対策における昨今の課題とその優先度
- 本調査で選定された脅威に対する情報セキュリティ対策の現状と課題（外部委託等）
- 自社の情報セキュリティ対策のあり方（理想像）とその実現に向けた課題

■ **情報セキュリティを担う IT 人材に関するニーズと育成の課題について**

- 情報セキュリティを担う IT 人材の職務についての考え方（専任／兼務等）
- 対象人材のキャリアパス（採用、ローテーション、キャリア目標等）
- 対象人材の過不足感（現在特に不足している人材）
- 対象人材の育成の仕組みと育成に関する課題
- CSIRT（Computer Security Incident Response Team）の設置状況
- 今後育成すべきと考えている情報セキュリティを担う IT 人材

1.2　調査対象

今回のインタビュー調査の対象は、以下のとおりである。

表 11　インタビュー調査対象

インタビュー先企業の区分	企業数
情報システムを受託開発する IT ベンダー	3 社
情報セキュリティ専門企業	2 社
ユーザー企業の情報システム部門	2 社

2. インタビュー結果概要

IT ベンダーやセキュリティベンダー、ユーザー企業の情報システム部門に対しインタビューを行った結果の抜粋（要約）を、以下に示す。

（A） 情報セキュリティに対する意識

IT ベンダーからは、経営層のセキュリティに対する意識の高まりや、セキュリティ事故によって、全社的に情報セキュリティに対する意識は高まっており、対策や組織の拡充が進められているという声が多く寄せられた。ただ、経営層によっては、情報セキュリティ上の脅威を経営上のリスクとして捉えていない場合もあり、企業毎の意識の高さには差異があるという指摘もあった。

セキュリティベンダーからは、自社内での意識の高さはもちろんのこと、人材の輩出やサービスの展開によって、各企業の意識を高めていきたいとの声が寄せられた。

ユーザー企業の情報システム部門からは、顧客の機密情報を扱っている場合は、情報漏えい等の脅威は経営リスクとして捉えやすく、全社的に情報セキュリティに対する意識は高いとの声が寄せられた。一方で、IT ベンダーと同様に、経営層の中には情報セキュリティ対策は保険のような位置づけであるという認識を持つ場合もあり、人材面や資金面等で十分な対策が行えているかというとそうではないとの意見もあった。

情報セキュリティに対する意識は高まってきてはいるものの、セキュリティに対する考え方によっては、情報セキュリティに関わる人材の必要性に対する理解に差異が生まれている現状が見られる。

調査対象	インタビュー結果概要
IT ベンダー	● 2000 年代初期から、経営層が情報セキュリティの必要性を理解したことを契機に、2004 年頃 CSIRT を構築した。 ● 経営層は、セキュリティを最重要項目として掲げ、その推進に取り組んでいる。実際に、顧客から万全なセキュリティ対策は最も多く求められている。 ● 企業毎の経営層で理解不足に差異が生まれている要因として、経営層の中には情報セキュリティ上の脅威をリスクとして考え、そのリスクは早急に潰さなければならないという考え方を持つ方と、情報セキュリティ上の脅威をリスクと認識していない考え方を持つ方の 2 通りが存在することが考えられるのではないか。 ● 自社で目立ったセキュリティ事故を起こしていないが、他企業の事故事例を自社の問題として捉え、都度、体制やルール等の見直しを図ってきた。

調査対象	インタビュー結果概要
	● 過去に、情報漏えい事故を起こし、会社としての信頼を低下してしまったことを契機に、グローバルでセキュリティ対策を重点的に取り組むようになった。 ● 自社要因・他社要因含めてセキュリティ事故が起きたことや、公共ビジネスに関して高いセキュリティが要求されていること等から、セキュリティに対する意識が高まっている。 ● 情報セキュリティ（対策）を必要としない部署は存在しないと考えている。
セキュリティベンダー	● セキュリティに関しては、今後も顧客に対して幅広いサービスを展開する方針である。 ● 情報セキュリティに関するサービスを提供するだけではなく、業界内へ情報セキュリティの経験・知見を持った人材を多く輩出している。 ● 営業やコーポレート部門等の情報セキュリティに業務として直接的に関わりのない人材においても、専門性の高い人材が近くにいることで、問題発生時の対応や情報共有等の体制が整っており、セキュリティに対する意識が自然と高まっている。
ユーザー企業の情報システム部門	● 顧客の機密情報を預かる業務を行っていることもあり、元々セキュリティ（特に情報漏えい）に関する意識が高く、物理セキュリティやルールの徹底等、セキュリティ全般に留意してきた。経営層も、セキュリティ対策の必要性には理解がある。 ● 情報漏えい等の情報セキュリティ上の脅威は、重要な経営リスクと捉えていることから、セキュリティを自社のリスクマネジメントの一環として全社で認識している。 ● ただ、経営層の中には、セキュリティ対策に対する考え方として保険のような対策であるという認識が残っており、人材面や資金面等、十分な対策が行えているかというとそうではない。 ● 過去にインシデントが発生したこともあり、セキュリティに対する意識はより高まっている。

（B）　情報セキュリティ対策内容と関連する体制

IT ベンダーからは、CSIRT の構築や役職（CISO など）、部署単位でのセキュリティ担当の設置等、情報セキュリティ対策と関連する体制を整えているとの声が多く寄せられた。

セキュリティベンダーからは、セキュリティに関する情報提供、教育、人材派遣、緊

急対応、システム企画・保守等の体制を自社単独で整えており、セキュリティベンダーだけではなくすべての IT 企業でこの体制が必要であるとの意見もあった。

ユーザー企業の情報システム部門からは、ISMS の構築や、事業所毎・拠点毎でのセキュリティ対策組織の設置等、組織の拡充を進めているとの声が寄せられた。

情報セキュリティに対する意識の高まりによって、組織の拡充が進められているが、十分な体制であるかというとそうではなく、今後アウトソーシング等も行いながら継続して体制を整えていく必要があると考えられる。

調査対象	インタビュー結果概要
IT ベンダー	● 「自身の企業情報システムを対象とする情報セキュリティへの取り組み」と「製品・サービスの情報セキュリティ確保に向けた取り組み」を支える組織として、対外 CSIRT 組織との連絡窓口として役割を担う組織や、顧客システムを対象とした CSIRT、製品に対する CSIRT、社内システムに対する CSIRT の４つの組織を設置している。 ● CSIRT は各事業部だけではなく、グループ会社にも設置しており、脆弱性対策とインシデント対応（事前、事後）を進めている。また、製品・サービスのセキュリティ確保の基本方針策定、体制の確立・技術開発・教育、セキュリティを考慮した製品・サービス開発方法の継続的な検討・実施等も行っている。 ● セキュリティガバナンス・マネジメントを行う部署や、情報セキュリティに関する役職（CISO）のほか、フォレンジック・監査・監視を行う CSIRT、法律対応を行う部署を設置している。 ● CSIRT を設置し、グループ全体の平時・有事のセキュリティコントロールを行っている。 ● 情報システムのユーザーとしての立場と、IT ベンダーとしての立場の両面でセキュリティ対策を実施している。 ● プロジェクト毎にセキュリティ責任者を設置し、製品やサービスに対する安全性を担保している。 ● 外向けにセキュリティ監査サービスを展開する部署もあることから、CSIRT も含めセキュリティ人材は多い。
セキュリティベンダー	● セキュリティの診断や情報提供、コンサルティング・教育サービス、顧客に合わせた人材派遣、緊急対応を行う部署と、情報セキュリティに関するサービスの開発、システム企画・開発・保守を行う部署を設置している。 ● ウイルスやマルウェア等の調査・研究を行う部署を設置しており、自社内での情報セキュリティに関する情報共有やインシデ

調査対象	インタビュー結果概要
	ント対応等の役割も同時に担っている。
ユーザー企業の情報システム部門	● 本社には、経営層を含めて構成される情報セキュリティに関するガバナンスを策定する組織と、ルールの策定や監査等のマネジメントを行う組織を設置している。 ● ISMS（Information Security Management System）やマネジメントシステム等のルールや体制を管理・推進する部署を設置している。また、CSIRT の仕組みも構築予定である。 ● ISMS は、CIO の役割と兼務したグループ ISMS 最高責任者と、グループ ISMS の統括推進担当・内部監査担当、本社・販売系・生産系・その他の事業部門で区分し、構成されている。 ● 事業部毎の IT 依存度によって求められるセキュリティレベルが異なるため、それぞれにルールの周知・徹底、セキュリティ教育を行う組織を設置している。 ● 拠点毎に、データセンターやネットワークの管理、虚弱性の判断等を行う、セキュリティ専門人材を配置している。（20～30名程度）

（C）　育成に関する取り組み

IT ベンダーからは、情報セキュリティ専門の教育体系を構築してはいないが、情報セキュリティに関わる人材に対しては、研修等によって教育を行っているとの声が寄せられた。

セキュリティベンダーからは、情報セキュリティに関する社内研修や OJT によって育成を行い、さらに社外活動にも積極的に取り組ませるようにしているとの声が寄せられ、情報セキュリティの知識・スキル向上に向けた意識の高さがうかがえる結果となった。

ユーザー企業の情報システム部門からは、IT ベンダー同様にセキュリティ専門の教育体系は構築していないが、IT 研修の受講や資格取得等を推進しているとの声が寄せられた。

情報セキュリティを IT に係る研修の一部に盛り込んでいる企業は多いものの、情報セキュリティを専門とした教育は少ない現状が見られる。

調査対象	インタビュー結果概要
IT ベンダー	● SE の教育体系を構築しており、その中にセキュリティの要素が組み込まれている。ただ、セキュリティ専門の教育プログラムは存在していないが、ペネトレーションテスト用のツールの使い方やセキュアコーディング等については必要に応じて教

調査対象	インタビュー結果概要
	育している。 ● 情報セキュリティ専門の育成体系ではなく、システム開発を行う人材に対する育成体系の中に、情報セキュリティの要素が組み込まれている。 ● 社内でキャリアフレームワークとして CDP（Career Development Program）を整備しており、セキュリティに関する職種・役割の定義も含まれている。 ● 研修ではなく、OJT による育成が基本である。 ● セキュリティに関する高度教育として、CSIRT が主催する社内コミュニティがあり、社外講師を招く等、技術情報を共有するセミナーを開催している。 ● 開発、システム管理など役割毎、部署毎に研修メニューがあり、セキュリティコンサルやフォレンジックなど専門的なセキュリティスキルを要する役職には専門の研修がある。 ● e-leaning 等を活用した、国内外で行われる内部の研修が中心に推奨している。
セキュリティベンダー	● OJT と社内での研修を中心に育成を行っている。 ● 社内研修は、入門向けのコースと入門より上位向けのコースを設置しており、セキュリティ検査やマルウェア、フォレンジック、ログ解析等を教育内容とし、現場担当者が教育を行うのではなく、専任の教育担当が教育を行う。 ● 特定の技術に対するスキル・知識が偏らないために、ローテーションを行う。 ● 社外活動に積極的に取り組ませている。（講演、執筆、CTF、セプキャン等） ● 中途採用や社内公募を積極的に行っている。 ● 社員全員のセキュリティ意識を底上げする目的で、セキュリティに関するセミナーを開催しており、全員参加を義務付けている。
ユーザー企業の情報システム部門	● IT の研修の中には、セキュリティ単独のものはないが、PHP 等の開発言語の研修の中に、セキュアプログラミング等の要素を盛り込んでいる。 ● IT パスポートや基本情報技術者試験、情報セキュリティアドミニストレータ試験の研修講座を保有している。 ● 専門人材の育成として、外部の専門家を招いた研修を行ってい

調査対象	インタビュー結果概要
	る。内容としては、実際のサーバをローカルで組み、攻撃を模擬するような研修である。 ● 情報セキュリティ専門の研修は行っておらず、IT に関する研修の中の一部として含まれている程度である。

（D）　育成に関する課題

IT ベンダーからは、情報セキュリティに関わる人材には適正と経験が重要であることから、育成が難しいとの声が多く寄せられた。

セキュリティベンダーは、IT ベンダー同様、個々の適正の見極めの難しさや、求められる知識・スキルの多様化による難しさ、明確なキャリアパスの提示等を課題として挙げていた。

ユーザー企業の情報システム部門からは、多種多様な顧客のニーズへの対応から、求められる知識・スキルも多様化しており、情報セキュリティに関わる人材に必要な知識・スキルを構築することが難しく、体系的な育成が行えていないとの声が寄せられた。

適正の見極めや経験の重要性、知識・スキルの多様化を課題として掲げる企業が多く、セキュリティに係る人材育成は難しいとの意識が高いことがうかがえる。

調査対象	インタビュー結果概要
IT ベンダー	● 情報セキュリティに関して専門性の高い人材は育成が難しく、社外のコミュニティ等で関係を築く等、自発的にスキルを向上する必要がある。 ● セキュリティには、知識・スキルだけではなく、ある程度のセンスが必要であり、人それぞれに適正があることに加え、経験も求められる。 ● 技術も重要であるが、経験も非常に重要である。そのため、知識・スキルや経験が、ゼロの状態から育成していくことは難しい。 ● セキュリティには適正が求められるため、関わる人材の見極めが必要である。 ● 情報セキュリティに関して専門性の高い人材は、その人が持つ特性によって役割が異なることに加え、環境にも左右されること等から、育成が難しい。 ● 情報セキュリティに関して専門性の高い人材とジェネラリストはいるが、セキュリティの感度のある技術者（現場の有識者レベル、ローレベル）の人材が不足している。

調査対象	インタビュー結果概要
	● 活躍の場を継続して与えられるような仕組みでないと、魅力を感じなくなり転職する割合が高まるリスクがある。 ● 情報セキュリティに関わる人材の質には課題を感じている。BYOD だけ取っても予想外の使われ方をすることもあり、ルールの策定は難しい。 ● 人材の量が不足しているとは思わないが、多ければ多いほど新しい取り組みが出来る。 ● 社内認定と評価が関連付けられておらず、評価・処遇が不透明であることが課題である。
セキュリティベンダー	● ある程度のレベルに達した人材に対しては、会社として次のステージを提供できないと転職する可能性が高まるリスクがある。（キャリアパスが曖昧） ● 管理職を望まない傾向がある。（技術者のままでいたいという意識が強い人材が多い。） ● 分野や人間性によって、得手不得手があり、適性の見極めが難しい。 ● プログラミングやウイルス解析等の技術に関する知識・スキルだけではなく、社会情勢に対する知識等、様々な知識が求められている。
ユーザー企業の情報システム部門	● 人材の数は不足していないが、多種多様な顧客のニーズへの対応を課題として捉えている。顧客のニーズにあわせて事業展開するため、どうしても後追いになり、慢性的にスキルレベルが不足している。 ● IT に関する幅広い知識や様々な知識が求められることに加えて、顧客のニーズも反映する必要があるため、育成計画が作りにくい。 ● セキュリティに関わる人材に求められる要素の定義が難しく、人材育成を行う上での課題となっている。 ● グローバルでのスキルに関する共通的な体系を構築することは、各国で契約方法や雇用関係が異なることから難しい。

（E）　対象人材の処遇、環境

IT ベンダーからは、情報処理技術者試験や CISSP、GIAC 等の資格を推奨し、人材のローテーションも積極的に行っているとの声が寄せられた。一方で、人材を評価する上では、事件・事故数や研修の受講率等、定量的に評価することは難しく、その人の存在

によって可能になったことや事後対応等の定性的な観点で評価せざるを得ないとの声も寄せられた。

セキュリティベンダーからも、資格・試験については IT ベンダー同様に、CISSP や情報処理技術者試験を積極的に推奨している声が寄せられた。また、情報セキュリティの技術一本でも部長職以上の待遇をしているという声もあり、管理職ではない情報セキュリティに係る人材のキャリアパスが見られた。

ユーザー企業の情報システム部門についても、IT ベンダー同様に資格・試験の推奨やローテーションは行っているとの声が寄せられた。また、全社として情報セキュリティに対する意識が高まっていることから、セキュリティ関連部署のステータスが低いということはないとの声もあった。

資格・試験については報奨金を出している企業は多いが、育成に対する難しさと同様に、人材評価も難しいと感じている企業が多く、キャリアパスや待遇と人材評価の関連性は明確に定まっていない現状が見られる。

調査対象	インタビュー結果概要
IT ベンダー	● 人材評価は、ITSS を基準としている。セキュリティは、事故が起こった際に重宝されるものであるため、明示的な評価基準には含まれていない。 ● 情報処理技術者試験のみ報奨金を出している。 ● 専門的な人材は GIAC（Global Information Assurance Certification）や CISSP（Certified Information Systems Security Professional）の取得や blackhat 系のセミナーへの参加などに対して支援をしている。 ● 部署が持つ技術・スキルの発展のために、人材のローテーションは積極的に行っている。 ● 情報セキュリティ人材の評価基準について、事件・事故数や研修の受講率等の定量的な評価は難しく、その人材の存在によって可能になったことや事後対応等の定性的な観点を重視し評価している。 ● CSIRT やフォレンジックを業務として行う人材に対して求められるスキルは、グローバルでフレームが定められている。 ● CISSP 等、広く様々な資格を取得することを推奨している。報奨金等については、研修に対して援助をしている。情報処理技術者試験は開発者としては基本であり、取得している人が多い。 ● 資格取得については、昇格の条件としている職階もある。
セキュリティベン	● 四半期ごとに業務上の実績や社外活動による成果を鑑みて表

調査対象	インタビュー結果概要
ダー	彰を行っている。 ● CISSP や GIAC、情報処理技術者試験、Cisco などのベンダー系の資格など幅広い資格を推奨している。CISSP のみ報奨金をだしている。 ● 技術一本でも、部長職以上の待遇をすることもある。 ● セキュリティに関するスキル体系を整理しており、その体系に沿った評価を行っている。 ● 製品と関連付けられた社内認定制度を保有している。 ● 多くの資格・試験を推奨しており、受験に係る援助も適宜行っている。 ● 短期から長期まで、定期的にジョブローテーションを行っている。
ユーザー企業の情報システム部門	● セキュリティ担当者が長く留まることはなく、定期的にローテーションを行っている。 ● セキュリティ関連部署のステータスが低いことはない。 ● 情報処理技術者試験やCiscoなどベンダー系の資格の取得を推奨しており、それぞれ報奨金を出している。 ● IT の基本的な知識としての資格については、昇格の条件として利用されるほか、資格手当が支給される仕組みになっている。ただ、情報セキュリティに関わる資格を推奨するような仕組みではない。

(F)　外部委託、その他

IT ベンダーからは、情報セキュリティの教育に対して外部サービスを利用しているとの声が多く寄せられた。また、情報セキュリティ対策に対する機運は高まっていくと思われるが、すべての企業で充実した体制を整えることは難しいため、アウトソーシングを含め検討したほうが良いのではないかという指摘もあった。

セキュリティベンダーからは、顧客からのニーズとして、業種別に偏りがあるのではなく、IT 依存度が高い企業ほどニーズが高い傾向があるとの声が寄せられた。

ユーザー企業の情報システム部門からは、教育やペネトレーションテスト等に外部のサービスを利用しているとの声が寄せられた。

調査対象	インタビュー結果概要
IT ベンダー	● セキュリティ教育に、外部サービスを使うことはある。

調査対象	インタビュー結果概要
	● セキュリティだけを取り上げた教育メニューは徐々に廃れていくのではないか。 ● 各人材に対する教育の必要性を最適化することは難しい。 ● あるレベルまでは教育によって育成可能だが、その後は機会を与え、自発的な成長を促すしかない。 ● 経営層の理解があり、予算を十分に用意しないとセキュリティは継続しない。 ● 技術者やコンサルタントを内部監査に巻き込むことで、セキュリティ部門への引き込みを図っている。 ● セキュリティサービスを行っている部署では、特に人材が不足している。 ● 今後セキュリティに対する機運は高まると思うが、すべての企業で育成するのは現実的ではなく、アウトソースすることも前提としたほうが良いのではないか。 ● 本社の CSIRT がグループ会社の運用も管理している。
セキュリティベンダー	● セキュリティサービスのニーズとして、業種別では偏っておらず、業種やベンダー・ユーザーというよりも IT 依存度が高い企業ほどニーズがある傾向である。コンサルティング業務は、大手企業の顧客が多い傾向がある。 ● 特定のサービスというよりは、全般的にニーズが高い。 ● 顧客の要望に応じたセキュリティ対策の提案・コンサルティングに対しても、多くのニーズがある。
ユーザー企業の情報システム部門	● 情報セキュリティ対策の確認として、内部だけではなく外部に委託しペネトレーションテストを依頼している。 ● 専門的な高度教育については外部サービスを利用する。 ● CSIRT は情報システム子会社にあり、インシデントの際の権限や判断は本社のマネジメント部門が担う。（日本型 CSIRT） ● 親会社と情報システム子会社の距離が非常に近い。 ● 経営層と現場の情報セキュリティ対策への認識をつなぐ人材が必要であるのと同様に、IT ベンダーとユーザー企業をつなぐ人材も必要であり、自社の状況に対する情報セキュリティ対策の必要性を IT ベンダーに伝えきれていない側面もユーザー企業側にある。

第6章　考察

本調査において、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の整理を行い、育成課題に対する先進的な取り組みの実態に関する調査を行った。

1.　確認方針に関する検証

インタビュー調査結果に基づき、事前に策定した確認方針に関する検証を行った。

■確認方針

A)　企業が情報セキュリティを担う IT 人材の育成を進める際に、組織内外の課題として以下の４つの課題に直面する。また、以下の課題①～③には順序性がある。

①　対象人材の必要性に関する理解不足

②　対象人材の育成の難しさ

③　対象人材の企業内の処遇

④　外部要因

インタビュー調査の結果、課題に対し一定の回答を得られたことから、４つの課題は存在していると考えられる。これ以外にも課題がある可能性はあるが、インタビュー調査では確認されていない。また、課題①～③には一定の順序性はあるものの、課題①に対し企業として十分な解決策や方針を見出さなくとも、課題②、③に直面している企業もあることを留意する必要がある。

■確認方針

B)　対象人材の育成に先進的に取り組んでいると思われる企業は、課題に対する解決策や方針を見出している

インタビュー調査の結果、対象人材の育成に先進的に取り組んでいると思われる企業は、課題に対する解決策や方針を見出しているだけでなく、見出し続けているようである。インタビュー調査を行った企業は、総じて情報セキュリティに関する意識が高い企業であるが、IT の高度化、多様化に関連し、求められる情報セキュリティ対策も常に変化しており、その変化に対応し続けている。

また、インタビュー調査を経て、課題①～④を補完、整理した結果を以下に示す。

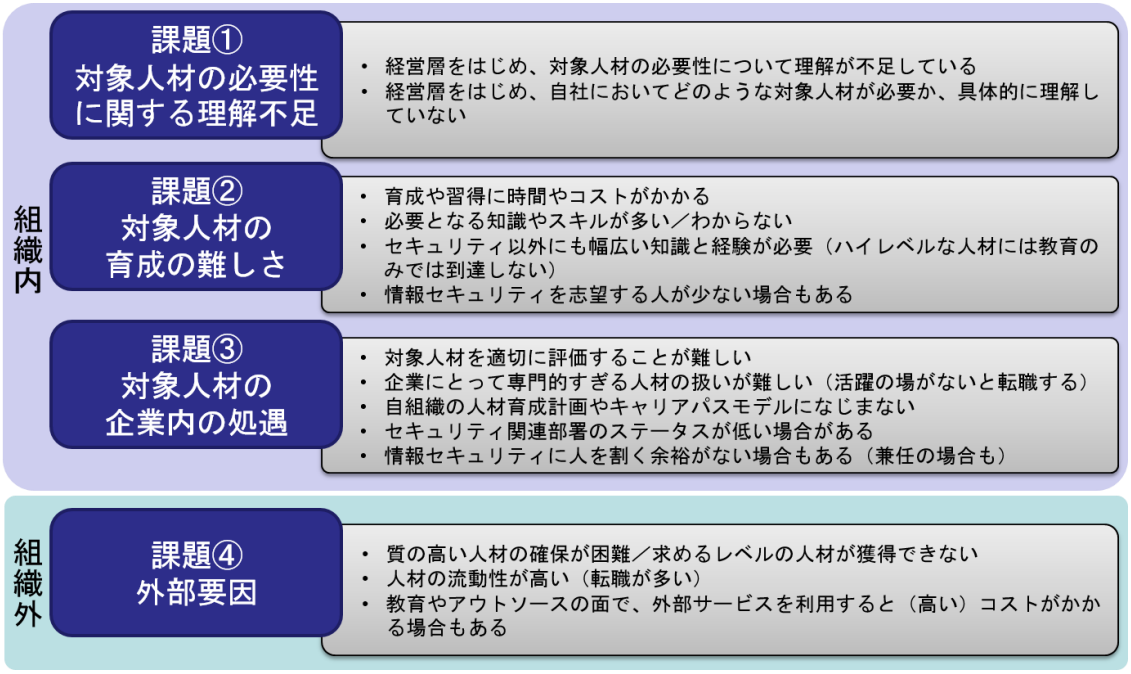

図 8　情報セキュリティを担う IT 人材の育成課題

2.　先進的な取り組み事例から考えられる課題に対する解決の方針

今回の調査結果に基づいて、企業が抱える課題に対しての解決の方針を検討した。

(1)　課題①「対象人材の必要性に関する理解不足」に対する解決の方針

近年、情報セキュリティ対策の必要性が叫ばれており、企業の経営層は、その必要性や経営リスクや IT リスクへの対応の 1 つに情報セキュリティ対策があることを理解している。しかし、経営層に限らず、自社にとって具体的にどのような情報セキュリティ対策が必要であるべきか、ひいてはその情報セキュリティ対策を担う人材として、どのような人材が必要なのかを理解できていない可能性がある。

各企業はまず、自社の IT 依存度や IT サービスを把握（≒AsIs）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であるべきか（≒ToBe）を整理する必要がある。その上で、セキュリティ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人的リソース部分をアウトソーシングするといった経営的な判断を行い、現実的な解として事業を行う上で必要な情報セキュリティを担う IT 人材の量と質を決定すべきである。

(2)　課題②「対象人材の育成の難しさ」に対する解決の方針

情報セキュリティ分野に限らず人材育成は時間やコストを要する。また、IT や情報セキュリティ技術、また脅威の高度化、多様化の流れは今後も続いていくであろう。この

ような状況のもと、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は、企業にとって得策ではない。例えば、情報セキュリティに関連する最新の技術や先端の事象も情報セキュリティの３要素である「機密性」「完全性」「可用性」という不変的な要素に基づいており、情報セキュリティの３要素を企業に置き換えて対策や育成の必要性の判断を行うなど、情報セキュリティを加味した企業の IT 戦略、育成方針が必要である。

(3) 課題③「対象人材の企業内の処遇」と課題④「外部要因」に対する解決の方針

企業や社会において、情報セキュリティに関する意識や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 人材の絶対数がまだまだ少ないことが要因の一つになっている。そのためこれらの解決には、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、また経営層や一部の担当者だけでなく、企業全体・社会全体として情報セキュリティに対する意識を身につけ、情報セキュリティに関する要求やニーズが高まっていくことが必要不可欠である。その第一歩として、各企業が自社に求められる情報セキュリティ対策を理解し、それに対し企業としてどのようなアクションをするか、経営的な判断を下すことが必要である。

3. 企業にとって必要な情報セキュリティを担う IT 人材

企業によって、IT 依存度や IT サービスの内容、IT の利活用シーンは異なるため、自社に必要な情報セキュリティ対策や人材は企業毎に異なる。しかし、上記の解決の方針で言及した「自社の IT 依存度等を把握した上で、具体的にどのような情報セキュリティ対策や人材が自社において必要であるべきか」を判断できる役割を担う人材が、大企業、中小企業問わず、どの企業においても共通に必要で重要である。近年、経営と情報セキュリティの両面に関連する役職として CISO（Chief Information Security Officer）が注目されているが、必ずしも CISO の育成を推奨しているわけではない。例えば、情報システム部門の担当者が自社において必要な情報セキュリティ対策や人材を経営層に対し説明し、経営層が経営の観点から判断しても、企業の機能として問題ない。企業は、自社の経営戦略や IT 戦略の一環として情報セキュリティ戦略（対策）を立案・推進する役割を担う人材を、育成等の方法により確保すべきである。例えば、ユーザー企業であれば、自社の IT 利用環境を正確に把握し、必要な情報セキュリティ対策を整理し、企業のリスクとして対策しなければどうなるのかを、経営的視点も踏まえながら経営層に対し説明、提案できる人材である。IT ベンダーやセキュリティベンダーであれば、自社の IT サービスやビジネスの中でセキュリティを実装することが信頼を含めた付加価値を生み、さらにマネタイズに繋がることやセキュリティを軸とした新規事業の優位性などを、経営的視点も踏まえながら経営層に対し説明、提案できる人材である。役職や部門ではなく、この役割（を担う人材）を企業として保持する必要がある。

4. 企業に求められる情報セキュリティ対策のレベルの考え方

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、企業の属性により３つの層に分けられる。

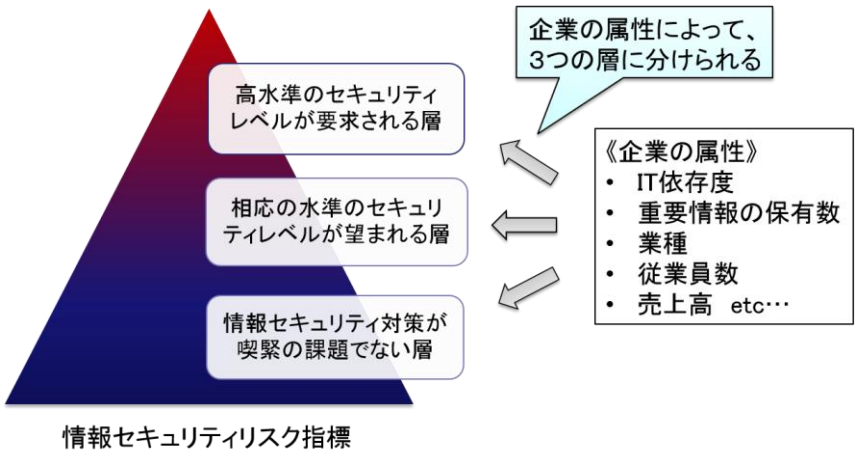

図 9　企業に求められる情報セキュリティ対策のレベルの考え方

例えば、重要インフラ、生命、財産に関連するシステムを扱っている企業であれば、「高水準のセキュリティレベルが要求される層」に、中小企業でも IT 依存度が高い企業であれば、「相応の水準のセキュリティレベルが望まれる層」に、農業を営んでおり IT をほとんど使っていない企業であれば、「情報セキュリティ対策が喫緊の課題でない層」に当てはまる。企業は、自社に必要な対策のレベルを見極める必要がある。ただし、IT を使っていれば何かしらの情報セキュリティ対策が必要であり、全く対策をしなくてもよいわけではないので、この点には注意が必要である。

■情報セキュリティリスク指標（独立行政法人 情報処理推進機構）
https://www.ipa.go.jp/security/benchmark/

5. 情報セキュリティ強化対応 CCSF の活用シーン

「情報セキュリティ強化対応 CCSF」には、IT ベンダーとユーザー企業における IT 人材のタスクの一覧と関連するスキルや人材像が、情報セキュリティに関するものも含め体系化されている。企業において必要な情報セキュリティ対策が決まり、求められるタスクまで具体化できれば、どのようなスキルが必要になるか、またそのスキルを持った人材像を明らかにする際に、「情報セキュリティ強化対応 CCSF」が有効である。

■情報セキュリティ強化対応 CCSF（独立行政法人 情報処理推進機構）
http://www.ipa.go.jp/jinzai/hrd/security/

◯調査にご協力頂いた企業一覧（50 音順）
株式会社 NTT データ
株式会社カスペルスキー
大日本印刷株式会社
日本アイ・ビー・エム株式会社
株式会社日立製作所
株式会社ラック
株式会社リコー

「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（詳細版）

発行日　2014 年 3 月 31 日
発行者　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
所在地　〒 113 −6591
東京都文京区本駒込 2 −28−8
文京グリーンコート　センターオフィス
電話　03−5978−7504（代表）
URL　http://www.ipa.go.jp/jinzai/hrd/index.html