職場の情報セキュリティ管理者のための

スキルアップガイド

2015年9月

IPA 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

はじめに

ITは、今やどのような企業や組織にとっても当たり前のものとなりました。パソコンやインターネットのほか、最近ではスマートフォンなどをはじめとする様々な端末や機器も利用できるようになり、当たり前のものとなったITを「いかに高度に」「いかに効果的に」使うかが、企業や組織の競争力に直結する時代になっています。

こうした流れの中で、情報セキュリティ対策は、必要不可欠なものとなりました。ひとたび企業や組織が保有する重要情報が漏えいするような事故が起こると、それまでに企業や組織が積み上げてきた社会的な信頼や評判にも大きな影響を与えかねません。情報セキュリティに関する技術や攻撃は日増しに高度化しており、組織側には従来以上に強固な対策が求められるようになっています。

上のような情報セキュリティの重要性を踏まえて、本ガイドでは、ITを利用する組織において情報セキュリティ対策を実施する際の実施体制や、情報セキュリティ対策を担う人材について説明しています。特に本ガイドでは、情報システム部門などのIT専門部門ではなく、ITを利用する部門（本ガイドでは「現場部門」と表現します）において対策を推進する**情報セキュリティ管理者**の重要性に着目し、その役割を解説しました。

また、情報セキュリティ管理者の役割を具体的に示すために、最近特に注目されている**情報セキュリティ上の脅威**を取り上げ、被害を防ぐためにはどのような対策が必要なのかを、例として紹介しています。その他、本ガイドでは、自組織に必要な情報セキュリティ対策のレベルを把握した上で、それに応じた情報セキュリティ業務を洗い出し、情報セキュリティ管理者を育成するまでを視野に入れ、それぞれ参考となる情報を掲載しています。

独立行政法人情報処理推進機構（IPA）では、情報セキュリティを担う人材の育成の推進に向けて、情報セキュリティ人材育成上の課題を調査しました。ここから導き出した「人材育成上のヒント」を抜粋で掲載しています。またIPAは、2014年8月にi コンピテンシ ディクショナリを活用した**「情報セキュリティ強化対応スキル指標」**を発表しました。本ガイドでは、情報セキュリティ管理者の育成の際に、この情報セキュリティ人材強化対応スキル指標を活用する方法や、情報処理技術者試験についても紹介しています。

本ガイドが、現場部門の情報セキュリティ管理者やその育成に課題を感じている方々のための参考資料となれば幸いです。

※ 本ガイドは、以下のような方を読者として想定しています。

- ITを専門に担当する部門ではないが、業務でITを利用する部門で、情報セキュリティ業務を担当する方（現場部門の情報セキュリティ管理者）
- 情報セキュリティ管理者を育成する役割を担う方（経営層・管理層・人材育成担当者等）

※本書で使用している「まもるくん」は、IPAが主催する「ひろげよう情報モラル・セキュリティコンクール」の応援隊長キャラクターです。http://www.ipa.go.jp/security/keihatsu/pr.html

目次

以下に該当する方は、本ガイドの前編である「ITのスキル指標を活用した情報セキュリティ人材育成ガイド(2014年8月発行)」をご覧ください。

- 企業の情報システム部門等のIT専門部門において情報セキュリティ業務を担当している方
- ITに関する製品・サービスを提供する企業（ITベンダー等）で情報セキュリティ業務を担当している方
- 情報セキュリティに関する製品・サービスを提供している方（情報セキュリティベンダーの方）

情報セキュリティに関して高度な専門性を有する人材の育成に関心をお持ちの方も、ぜひご覧ください。
http://www.ipa.go.jp/jinzai/hrd/security/
からPDF形式でダウンロードできます。

あなたの組織に迫る脅威と対策

あなたの組織は大丈夫ですか？

ITを利用している組織では、知らないうちにパソコンがウィルスに感染してしまったり、組織の外部から不正なアクセスが行われ、情報が盗まれてしまうことなどがあります。このようなことが起こると、組織にとって重大な被害や損害につながる可能性がありますが、こうした事象を引き起こす可能性のことを情報セキュリティの分野では**「脅威（きょうい）」**といいます。

本ガイドでは、このような情報セキュリティ上の脅威のうち、IPAの「情報セキュリティ10大脅威2015」を踏まえて、特に現場部門での対策が有効な脅威を取り上げ、想定される被害の例と求められる対策を説明します。本ガイドで取り上げる脅威と被害の例は以下のとおりです。

～ 本ガイドで取り上げる脅威と被害の例 ～

① **標的型攻撃**による内部情報の漏えい
② **内部不正**による情報漏えい
③ インターネットバンキング等による金銭被害
④ WEBサービスへの**不正ログイン**

ここで、**「標的型攻撃」「内部不正」「不正ログイン」**という、昨今の新聞やニュースでも見かけるような重要なキーワード（下図のオレンジ色の文字）が登場しますので、次のページでは、まずこれらの重要キーワードについて解説します。

ITの発展に伴って情報セキュリティを脅かす攻撃の手口も日々高度化・巧妙化しています。「普通のお知らせメールだと思って開封したメールが実はウィルスに感染しており、深刻な情報漏えいが起きてしまった」「知らないうちに自分のパスワードが盗まれ、アカウントが乗っ取られてしまった」など、気づかないうちに被害にあってしまうことも少なくないのが現状です。

特に、次から次へと新しい攻撃の手口が生み出される昨今では、その時点で必要な情報セキュリティ対策を実施するだけでなく、将来にわたり常に適切な対策を実施し続けることが必要です。「昨日まで大丈夫だったから今日も大丈夫」とはいえないのが情報セキュリティの世界であり、こうした状況の中で、情報セキュリティを担う人材の役割はますます重要なものとなっているのです。

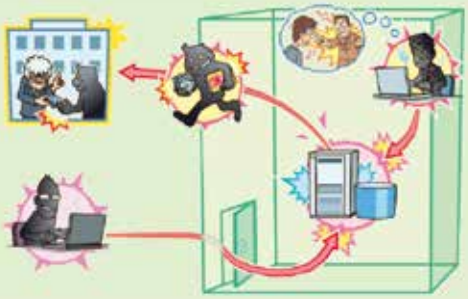
重要 KEY WORD

標的型攻撃

不特定多数の相手ではなく、特定のターゲット（企業や組織など）に対して、個人情報や機密情報などの重要情報を盗み取ったり破壊活動を行うようなサイバー攻撃を「標的型攻撃」と呼びます。標的型攻撃の手口は日増しに巧妙化しているため、万全な対策は難しいのが現状であり、企業や組織にとっては高いレベルでの警戒が必要です。

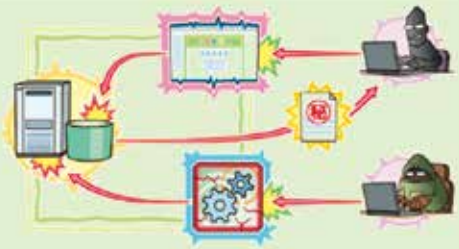
内部不正

企業や組織の内部関係者が顧客情報や製品情報などの重要情報を盗み出すような不正行為を「内部不正」と呼びます。風評被害を恐れて実際の被害が公表されることは少ないのですが、ひとたび事故が発生すると、被害の規模や範囲は非常に大きくなります。組織側の日頃のマネジメントも疑問視されるため、組織にとっても非常に大きなダメージをもたらす可能性があります。



不正ログイン

無関係な第三者が不正にログインを行うことを「不正ログイン」といいますが、こうした不正ログインによってインターネットバンキングなどで勝手に送金が行われるような金銭被害も増えています。推測しやすい単純なパスワードを使っていたり、複数のウェブサイトで同じパスワードを使い回していると、一つのサイトでパスワードが漏えいした際に、同じパスワードを使っている他のサイトにも勝手にログインされてしまうことがあります。



上のような情報セキュリティ上の脅威によって、情報漏えい等の被害を起こさないようにするためには、組織としてどのような取り組みが必要なのでしょうか。

次のページからは、組織において情報セキュリティ対策を実施するために必要な体制に加えて、情報セキュリティを担う人材の役割について説明します。

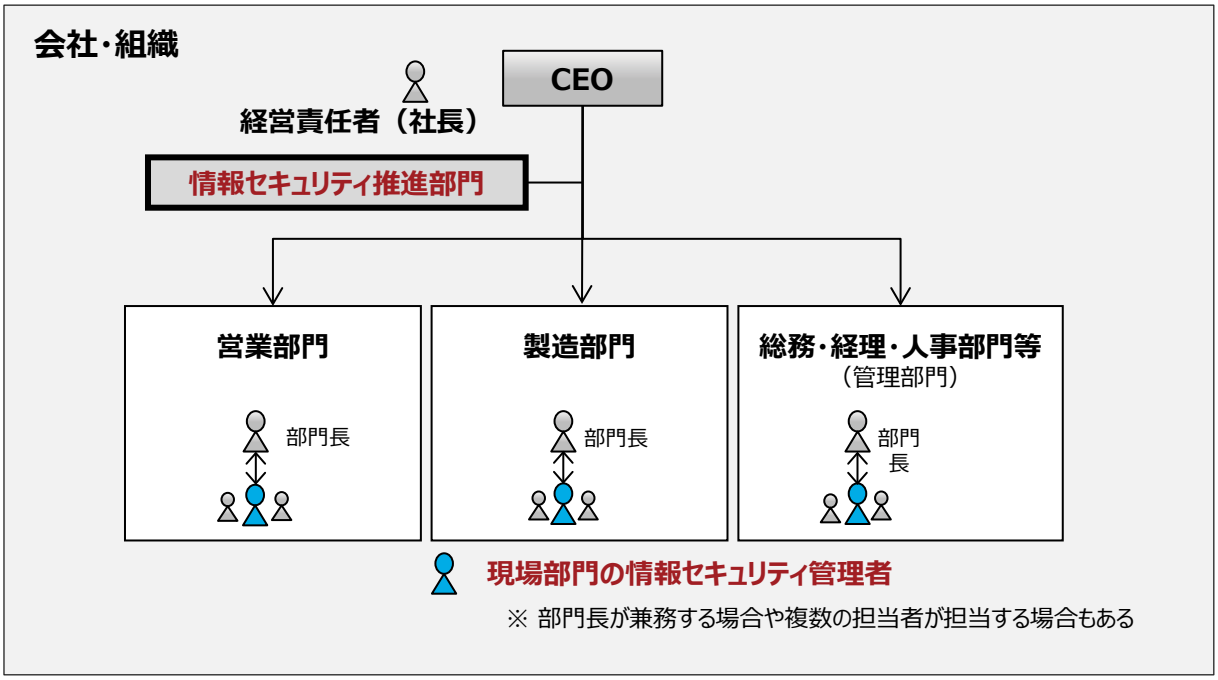
組織に求められる情報セキュリティ対策の実施体制

組織の規模にかかわらず、組織全体として十分な情報セキュリティ対策を実施するためには、適切な体制と役割分担が必要です。情報セキュリティ対策は、一度実施すればよいものではなく、継続的かつ日常的に実施すべきものであるため、対策の検討・立案とともに、定期的な見直しや実施状況の確認なども行える体制が望まれます。ここでは、組織の中で情報セキュリティ対策を立案し、継続的に実施するための体制や役割分担に関するポイントを紹介します。

情報セキュリティ対策の実施体制例

情報セキュリティ対策を推進する上でのポイントは、情報セキュリティ対策を立案・推進するミッションをもった組織（下図の**「情報セキュリティ推進部門」**）や責任者を設置するとともに、各部門にもそれぞれ対策を推進する役割である**情報セキュリティ管理者**を配置することです。

情報セキュリティ推進部門は、組織全体としての情報セキュリティポリシーやルールの策定、情報セキュリティ対策の統括を担います。一方、各部門の情報セキュリティ管理者は、各部門の業務実態にあわせて組織全体のルールや対策を推進するとともに、現場部門固有の情報セキュリティ上の課題についての対策を推進します。これにより、組織全体として統一され、かつ、業務実態に即した情報セキュリティ対策が可能となります。



本ガイドにおいて特に注目するのは、前ページ図中の「情報セキュリティ管理者」です。ここでいう「情報セキュリティ管理者」とは、情報システム部門などのITを専門とする部門や情報セキュリティ対策を専門とする部門ではなく、それ以外のIT利用部門（本ガイドでは「現場部門」と表現します）において、情報セキュリティ対策を推進する役割を指しています。

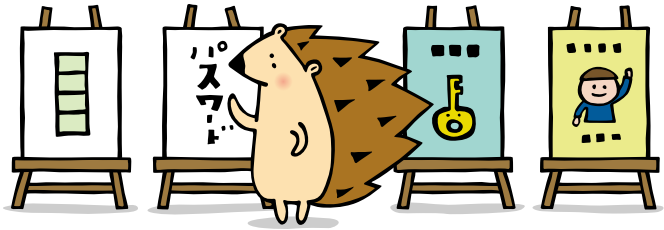
情報セキュリティ推進部門は組織全体の情報セキュリティ対策を立案・推進するミッションを持つため、できるだけ情報セキュリティに関して高い専門性を持った人材を配置することが理想的です。これらの人材の役割や育成方法は、p.2で紹介した「情報セキュリティ人材育成ガイド」に掲載しています。なお、小規模な組織の場合は、すべての役割を一人の人材が担うことも考えられます。

現場部門の情報セキュリティ管理者の役割

現場部門の情報セキュリティ管理者は、**情報セキュリティに関する組織全体のルールや施策を、それぞれの現場部門の業務の実態にあわせて推進する役割**を担います。具体的には、部門の情報セキュリティの管理責任を持つ上位者（部門長等）からの指示を受けながら、部門のメンバーに対する呼びかけを行ったり、対策の実施状況を把握し、改善を図ったりする業務を担当します。多くの組織で、このような業務を担当する役割がすでに置かれていると考えられますが、本ガイドでは、この役割の重要性を改めて紹介しています。

なお、現場部門の情報セキュリティ管理者は、部門長が担当したり、部門のメンバーが複数人で担当したりする場合も想定されます。組織の規模や形態にあわせて、情報セキュリティ管理者の活躍形態にもさまざまな形が考えられます。

現場部門の情報セキュリティ管理者には、自部門に求められる情報セキュリティ対策についてしっかりと理解した上で、その運用を現場部門で確実に浸透させ、情報セキュリティ対策を着実に推進することが求められます。また、社内の他部門や社外での情報セキュリティに関する各種情報（事故事例・対策例等）を入手し※、自部門内での情報セキュリティ意識の向上や対策に生かしていくことも、重要な役割の一つです。この役割は、現場部門でヒト、モノ、情報を適切に管理し、情報セキュリティに起因する事件や事故を発生させないために、ひいては、組織に対する顧客や社会からの信頼を守るためにも、きわめて重要なものになっています。



※情報セキュリティの各種情報の入手には、IPAセキュリティセンターのホームページもご利用ください。
http://www.ipa.go.jp/security/

次のページからは、情報セキュリティを脅かす何らかの事象が発生し、その結果として組織に対する顧客や社会の信用を低下させる恐れがある例として４つのケースを取り上げ、想定される被害の例とその原因を解説します。また、被害を防ぐために望まれる対策を説明するとともに、そのようなケースを例に、現場部門の情報セキュリティ管理者の役割や具体的な業務について紹介します。

ケース1

標的型攻撃による内部情報の漏えい

☞ こんなことが起きるかもしれません！

ある日、海外の競合他社が、自社の極秘プロジェクトとして開発中の未公開の新製品にきわめて類似する機能を持った製品を発表。内部調査の結果、**自社の研究開発部門で厳重に管理されていたはずの重要技術情報が外部に流出した**形跡があることが明らかになった！

■ なぜこんなことが起きるのですか？

情報漏えいの原因はさまざまですが、最近では「標的型攻撃」の危険性も広く知られてきました。標的型攻撃は、電子メール等に添付されたウィルス等により組織内部の端末等を攻撃し、遠隔操作によって機密情報を盗むような攻撃のことです。例えば公的機関を装ったメールや自社製品に対するクレームのメールなど、一見怪しくないメールや受信者が関心を持つメール、急いで開封する必要があると思わせるようなメールも報告されており、手口がますます巧妙化しています。これらのメールの添付ファイルを開いたり、メールに記載されているURLをクリックしてウェブサイトを開いたりすると、そこに仕込まれているウィルスに感染し、不正なプログラムが勝手にインストールされてしまいます。この不正なプログラムが、外部からの遠隔操作によって重要情報を外部に発信し、情報漏えいにつながることがあるのです。

■ 被害を防ぐためにどうすればよいでしょうか？

標的型攻撃の攻撃者は、ターゲットとする企業や組織の業務内容などを念入りに調べた上で、情報セキュリティ上、一見問題のないメールを装って侵入を試みます。そのため、技術的にこの攻撃を完全に防ぐことは難しいと言われており、**一人一人のユーザーの日頃の注意力や警戒心**もこの攻撃に対する有効な対策となります。ユーザーの警戒心を高めるためには、お知らせを流したり、部門内で定期的に勉強会を開くなどの方法で、最近発生した標的型攻撃のニュースや手口を広く知らせることも有効です。そのような巧妙な手口があることを、多くのユーザーが事前に知っていれば、安易に添付ファイルを開いたり、URLをクリックする前に、「もしかしてこれは･･･」という気持ちが働く可能性を高めることができます。

現場部門で活用しているパソコンに対して、ウィルス対策ソフトの導入・更新（アップデート）などの決められた情報セキュリティ対策が確実に実施されているかどうか、その実施状況を把握するとともに、ユーザーへの注意喚起等を通じてその実施を徹底することは非常に大切です。また、一般的なユーザーのパソコンに重要な情報が保存されていると、情報漏えいのリスクがより高まってしまうため、重要な情報は安易に保存しないといった対策も有効です。

以下のチェックリストで、あなたの組織の今の状況を確認してみましょう。

あなたの組織は大丈夫？

＜あなたの組織の現状をチェック！＞

- □ 部門内のすべてのパソコンに、ウィルス対策ソフトが導入されていますか。
- □ ウィルスチェックを頻繁に実施していますか（動作が遅くなるからなどの理由でウィルスチェックを長い間省略しているパソコンはありませんか）。
- □ ウィルス対策ソフトの更新（アップデート）をきちんと実施していますか。また、その実施状況を確認し、実施されていないユーザーには注意喚起を行っていますか。
- □ 部門のユーザーは、「怪しいメールは開封しない」、「疑わしいメールのURLはクリックしない」、「不審な添付ファイルは開かない」などの基本的なルールを理解していますか。また、そのような基本ルールを学んだり、周知する機会はありますか。
- □ 部門のユーザーは、ウィルス対策ソフトから「ウィルスに感染しました」という警告メッセージが画面に表示された場合、まず何をすればよいかを知っていますか。
- □ ウィルス感染や情報漏えいが発覚した場合の報告手順や担当者は定められていますか。また、現場部門の情報セキュリティ管理者は、その内容をきちんと知っていますか。

■ 情報セキュリティ管理者の仕事①

この欄では、取り上げたケースに関連付けて、現場部門で情報セキュリティ対策の推進を担う情報セキュリティ管理者の仕事を紹介します。

「部門内の情報資産の情報セキュリティを維持するために必要な業務を遂行する」ことは情報セキュリティ管理者の主な仕事です。規模の大きな組織では、組織全体で定めた情報セキュリティ対策を現場部門で確実に遂行することが重要です。一方、規模の小さな組織などは、組織の状況にあわせて、現実的な、必要な情報セキュリティ対策を考えることが必要な場合もあります。

情報セキュリティ対策の推進にあたっては、**他の部門の担当者との連携**も重要です。例えば、ここで取り上げたケース１のような被害を防ぐためには、組織全体の情報セキュリティ対策の立案・推進を担う部門と連携した上で、組織外部での事故事例等を入手し、それらを現場部門へ周知して注意喚起を図ることや標的型攻撃に対する訓練等を推進することなども有効です。

たとえばこんな役割の担当者とも連携します

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）

セキュリティに関する事故が発生した直後の**被害拡大防止策の実施**や**被害からの復旧業務の実施**を担う役割。ウィルス感染などが発覚した場合は、組織内のこうした役割を担う方に報告します。

ケース2

内部不正による情報漏えい

☞ こんなことが起きるかもしれません！

ある日、自社の顧客から、個人情報を渡した記憶のない同業他社から広告メールが届くようになったとの問合せを受けた。内部調査の結果、**自社の営業部門が保有する顧客情報が外部に流出している**ことが明らかになった！

■ なぜこんなことが起きるのですか？

情報漏えいを引き起こす要因の一つとして「内部不正」が挙げられます。情報セキュリティ対策を考える際には、組織の外部からの攻撃への対策に加えて、内部の関係者による不正を防ぐことも重要です。内部の関係者は正当なアクセス権限を持っているため、組織内部の情報に容易にアクセス可能な状態にあります。そのため、内部の関係者が悪意を持った場合は、**外部からの侵入よりもずっと簡単に情報を盗み出すことが可能**です。実際に、システムの保守管理の担当者が大量の顧客情報を持ち出して名簿業者に販売したという事件もありました。また、元社員が退職直後にまだ削除されていない自分のIDを使って顧客情報を盗み出した事例なども報告されています。

■ 被害を防ぐためにどうすればよいでしょうか？

内部不正が発生する原因には、組織内での人事評価や給与等の処遇面に対する不満のほか、借金等による生活苦、本人が納得できない不当な解雇等があります。こうした問題に対して、現場部門のみで対応することは難しいかもしれません。しかし、情報システムのアクセス管理がいい加減で、誰もが自由に内部の情報にアクセスできてしまうことや、情報システムの操作の記録や監視を行っていないことが、不正行為を助長する場合もあり、こうした面については現場部門でも対応が可能です。現場部門に可能な対策としては、**アクセス権限を個人別に適切に設定したり、退職者のアクセス権の抹消などの権限の管理業務を確実に行う**ことが重要となります。また、アクセス状況や操作についての監視を行うほか、監視を行っていることを**ユーザーに周知する**ことも、不正行為の抑止につながります。

IPAの調査結果※によれば、不正行為の7割以上は単独で作業が行える監視の厳しくない場所で発生しています。不正行為を防ぐためには、重要情報を扱う業務を**複数人員で実施する体制**のほか、**作業の記録**なども重要です。（※IPA テクニカルウォッチ「組織の内部不正防止へ取り組み」2012年）

また、外部の企業等に業務委託を行う際は、情報セキュリティに関する取り決めを文書で明確化するほか、契約にこうした情報セキュリティに関する内容が盛り込まれているかを確認することも重要です。

以下のチェックリストで、あなたの組織の今の状況を確認してみましょう。

＜あなたの組織の現状をチェック！＞

あなたの組織は大丈夫？

- □ ユーザーの管理・監督権限に応じて、適切なアクセス権限を設定していますか（多くのユーザーが管理者アカウントを自由に利用できるような設定になっていませんか）。
- □ 退職者や異動・担当を交替したユーザーのIDやアクセス権は、その直後に適切に削除・変更を行っていますか（長期間そのままにされているIDはありませんか）。
- □ 重要な情報を保存しているコンピュータは、管理監督者の目の届くところに置く、別室に置いて入退室記録をつける、部屋に鍵をかけるなどの対策を行っていますか。
- □ 重要な情報が保存されているコンピュータでは、アクセスログを記録していますか。
- □ アクセスログの記録を行っていることを、外部委託先や一時的な従業員も含めて、ユーザーに周知していますか。
- □ 一時的な従業員も含め、重要な情報を扱う作業は、管理監督者の目の届くところで行われていますか（単独で重要な情報にアクセスしている従業員はいませんか）。
- □ 情報システムの運用や保守管理等を、自部門から外部の企業に委託する際に、情報セキュリティに関する取り決めを文書で明確化していますか。

■ 情報セキュリティ管理者の仕事②

情報セキュリティ管理者は、現場部門において**情報セキュリティ対策が必要な情報資産（データ等）を洗い出した上で、それぞれに対する対応策を整理・確認**します。情報資産に対するアクセス権限の設定や確認は、こうした仕事の一環です。また、組織全体のルールに則って、現場部門における具体的な情報セキュリティ対策の実施方法を検討し、**周知**します。特に内部不正には、不正の重大さを認識していないケースもみられます。よって、情報が重要な資産であり、持ち出しは禁止されているという規則や、アクセスログ等が管理されており、不正はすぐに発見されるということを、組織内で十分に周知することも重要です。

たとえばこんな役割の担当者とも連携します

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）

企業内のセキュリティ業務全体を俯瞰し、自組織の**情報セキュリティ戦略**や**ポリシーの策定**等を推進する役割。現場のルールを検討する際は、こうした役割の方に相談することも考えられます。

ケース3

インターネットバンキング等による金銭被害

☞ こんなことが起きるかもしれません！

ある日、経理部門で、自社の銀行口座から業務上記録のない出金が行われていることが分かった。内部調査の結果、**何者かが、自社のID・パスワードを使い、インターネットバンキングで自社の銀行口座からお金を不正に引き出している**ことが明らかになった！

■ なぜこんなことが起きるのですか？

会員制ウェブサイトや有名企業を装って、「アカウントの有効期限が近づいています」「登録内容の再入力が必要です」などというメッセージとともに偽のウェブサイトへのリンクを貼ったメールを送り、偽のウェブサイト上で銀行口座の情報やネットバンキングサービス等のID・パスワードのほか、クレジットカード番号を盗み取るような詐欺をフィッシング詐欺と呼びます。最近では、こうしたフィッシング詐欺等を通じて盗み出した情報をもとに、**ユーザー本人になりすまして預金の不正な引き出しやカードの不正利用等を行う犯罪**が増えており、法人口座を対象とした被害も急増しています。その手口はますます巧妙化する傾向にあり、「個人情報の漏えい事件が発生しました」というメールでユーザーを不安にさせて偽のサイトへ誘導するケースや、偽の画面であるにも関わらず「偽画面にご注意！」と表示して本物の画面に見えるように作り込まれているケースも発見されています。

■ 被害を防ぐためにどうすればよいでしょうか？

上のような被害に遭わないためには、まず、インターネットバンキングなどを業務で利用するユーザーが、フィッシング詐欺のような手口に引っ掛からないようにすることや、同じように情報が盗まれる可能性があるウィルスに感染しないようにすることが重要です。そのためには、パソコン上で利用している**ソフトウェアの更新やウィルス対策ソフトの導入・更新を着実に行う**ことが必要です。また、具体的な事例や最新の手口に関する情報を収集して、**ユーザーに周知しておく**ことも有効です。

また、インターネットバンキングなどを業務で利用する場合に、利用記録をつけるなどの**組織内のルールがある場合は、これらのルールを確実に守る**ようにします。

以下のチェックリストで、あなたの組織の今の状況を確認してみましょう。

あなたの組織は大丈夫？

＜あなたの組織の現状をチェック！＞

- □ インターネットバンキングを利用できるユーザーは、必要最小限に限定されていますか。また、ID・パスワードは、限定されたユーザーにしか分からない状態になっていますか。（管理簿を見れば誰もがログインできるような状態になっていませんか。）
- □ インターネットバンキングを利用できるパソコンは限定されていますか。また、そのパソコン上に、ウィルス対策ソフトが導入され、定期的にウィルスチェックを行っていますか。また、ウィルス対策ソフト自体もきちんと更新されていますか。
- □ インターネットバンキングを利用できるパソコン上で動くOSやブラウザなどのソフトも、セキュリティパッチの公開に合わせて、きちんと更新されていますか。
- □ インターネットバンキングを利用する際のルールが決められていますか。（利用記録をつける、定期的に利用履歴と照合する、パスワードを推測されにくいものにして定期的に変更するなど）
- □ インターネットバンキングを利用するユーザーに、不審に感じた場合の確認方法を周知していますか。（ログイン履歴や取引履歴を確認する、金融機関に電話するなど）
- □ インターネットバンキングを利用するユーザーが、フィッシング詐欺や不正送金被害等に関する最新動向を知る機会がありますか。（勉強会や連絡発信など）

■ 情報セキュリティ管理者の仕事③

現場部門の情報資産の情報セキュリティを維持するために、ウィルス対策ソフトの導入や更新、OSやブラウザの更新などを確実に実施することは、情報セキュリティ管理者の重要な役割です。ケース３のような事態に限らず、こうした脅威による被害を防ぐためには、こうした**基本的な情報セキュリティ対策を着実に実施する**ことが非常に大切です。

また、ケース３のような被害を防ぐためには、ネットバンキングなどのウェブサービスを利用するユーザーを限定する（誰もが自由に利用できる状態にしない）ことや、例えば利用記録をつけるなど、サービスを利用する際のルールを決めること、そして、それらのルールを周知・徹底することなども有効です。組織全体のルールが存在する場合は、その範囲内で**現場部門の業務に即した運用方法を検討する**ことが求められます。

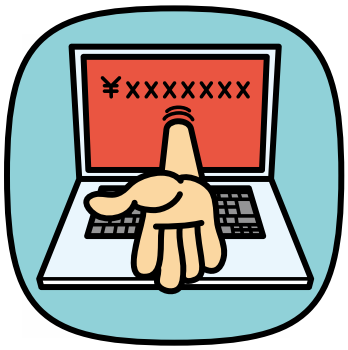
その他、現場部門で組織全体のルールを運用する中で、その部門だけではなく組織全体として取り組んだほうが効率的・効果的であると思われる取り組みについては、**組織全体の情報セキュリティ対策を立案・推進する部門に提言を行う**ことなども重要です。

ケース4

WEBサービスへの不正ログイン

☞ こんなことが起きるかもしれません！

ある日、業務上購入した記録のないきわめて高額な品物の請求書が届いた。内部調査の結果、総務部門が事務用品の購入に利用しているウェブサイトで、**何者かが自社のID・パスワードを使って不正にログインし、自社の業務には無関係な高額商品を購入した**記録が見つかった！



■ なぜこんなことが起きるのですか？

他人に推測されやすいIDやパスワードを複数のウェブサイトで使い回していると、あるウェブサイトからIDやパスワードが漏えいした際に、そのID・パスワードが他のウェブサイトで使われて、**登録情報が漏えいしたり、登録しているクレジットカードの情報などが不正に使われる**可能性があります。例えば、ショッピングサイトに不正ログインされた場合、登録している情報を使って勝手に注文されたり、貯まっているポイントを勝手に使われたりするなどの被害を受ける可能性があります。業務で用いるサイトも含めてウェブ上でのアクセスが可能なサイトはこうした被害を受ける可能性があるため、企業や組織のユーザーにとっても十分な対策が必要です。

■ 被害を防ぐためにどうすればよいでしょうか？

不正ログインによる被害を防ぐためには、推測されにくいパスワードを使い、同じパスワードを複数のウェブサイトで使い回さないなど、**パスワードに関する基本的な事項をルール化するとともに、ユーザーに対してその遵守を徹底する**ことが重要です。パスワードそのものを把握することは難しくても、例えばユーザーによる自己点検などで、ルールに沿っているかどうかをチェックしたり、必要に応じて注意喚起することが大切です。

また、業務上でウェブサービスを利用する際は、**利用記録などをつけ、利用状況を明らかにしておく**ことも有効です。

また、利用するウェブサービスそのものについても、定期的に見直しを実施し、利用していないウェブサービスや不要だと判断されるウェブサービスについては、アカウントを削除するなどの対応を行うことも重要です。

以下のチェックリストで、あなたの組織の今の状況を確認してみましょう。

あなたの組織は大丈夫？

＜あなたの組織の現状をチェック！＞

- □ 123456, admin, password などの当然推測されそうな単語を避けることは当然ながら、意味のある単語にしない、最低８文字以上にするなどの、パスワードに関する基本的なルールを定めていますか。
- □ パスワードに関するルールをユーザーに対して周知し、守ることを徹底していますか（せっかく定めたルールが形骸化していませんか）。
- □ パスワードに関するルールをユーザーが守っているかどうかを、定期的にリマインドしていますか。また、守っていないユーザーに注意喚起などを行っていますか。
- □ 組織内で利用しているウェブサービスやウェブサービス上で扱っている重要情報を、組織として把握していますか。
- □ 万が一、ウェブサービスの不正利用が発覚した場合のために、組織内で利用しているウェブサービスの利用状況を記録していますか。
- □ 組織内で利用するウェブサービスの利用状況や必要性を定期的に見直し、利用していないウェブサービスや必要性の低いウェブサービスについては、アカウントを削除するなどの対応を行っていますか。

■ 情報セキュリティ管理者の仕事④

自分が所属する**現場部門の情報資産を把握し、適切な情報セキュリティ対策が実施されているかどうかを確認する**ことも、情報セキュリティ管理者の重要な仕事にあたります。ケース４のような被害を防ぐ前提として、現場部門で利用しているウェブサービスやそこで扱っている重要情報をあらかじめ把握・整理しておき、それぞれの情報に対して十分な対策が行われているかどうかを確認しておくことも重要です。

確認の結果、十分な対策が行われていない情報資産に対しては、組織全体のルールに沿って対策を検討します。対策を運用するにあたり、調整が必要な場合や要望がある場合は、以下に示す役割の担当者と連携して適切な対策を実現します。

たとえばこんな役割の担当者とも連携します

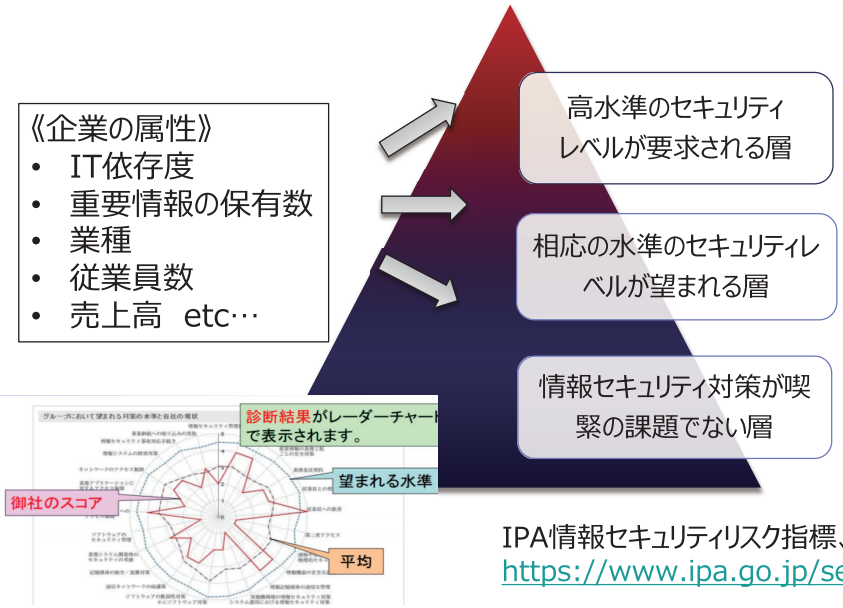
セキュリティアドミニストレータ（ISセキュリティアドミニストレータ）

組織全体の情報システム（IS）戦略やIT戦略と情報セキュリティ戦略との相互連携を図る役割。情報セキュリティ戦略を具体化し、現場部門に指示します。こうした役割を有する組織では、現場部門のルール策定の際に報告や調整が必要なこともあります。

組織に求められる情報セキュリティ対策のレベル

組織の業務内容やITの活用方法、ITに対する依存度などによって、その組織に求められる情報セキュリティ対策の内容やその実施に必要な役割は異なってきます。そのため、他の組織の取り組みを参考にしつつも、自組織の情報セキュリティ対策を検討する際は、組織の現状や方針に基づいて判断することが必要です。こうした判断の際には、IPAが提供する**情報セキュリティリスク指標**が活用できます。

情報セキュリティリスク指標は、組織の情報セキュリティマネジメントの実施状況を自ら評価することによって**組織が抱えるリスクを把握するための指標**です。この指標によって、組織に求められる情報セキュリティ対策の水準は、以下のとおり３つに分けられます。



IPA情報セキュリティリスク指標、ベンチマークによる診断
https://www.ipa.go.jp/security/benchmark/

社会を支える重要なインフラや生命・財産に関連するシステムを扱っている組織は「高水準のセキュリティレベルが要求される層」に該当します。また、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」に該当します。

業務上、ITをほとんど使っていない企業の場合は「情報セキュリティ対策が喫緊の課題でない層」に該当します。ただし、パソコンや電子メールなど、少しでもITを活用していれば、何らかの情報セキュリティ対策は必要であり、全く対策をしなくてもよいわけではありませんので、この点には注意が必要です。

このように、組織の情報セキュリティ対策を検討する際は、**業務内容に見合った情報セキュリティの水準を見極める**必要があります。

情報セキュリティ対策ベンチマークの紹介

IPAでは、情報セキュリティリスク指標に基づく組織の情報セキュリティ対策自己診断テスト「情報セキュリティ対策ベンチマーク」のサイトを開設しています。このサイトでは、クリックで設問に答えるだけで、自分の組織に求められる情報セキュリティレベルや組織の情報セキュリティ対策の実施状況を診断し、他社とも比較することができます。また、必要な取り組みについての解説を参照することも可能です。

■ IPA情報セキュリティ対策ベンチマーク
http://www.ipa.go.jp/security/benchmark/

設問は、情報セキュリティ対策の実施状況に関するもの（左図）が計27問、事業内容等に関するもの（右図）が計19問題の全46問から構成され、30分程度で診断が可能になっています。

診断結果は、ウェブサイト上で参照できるほか、PDFファイルでのダウンロードも可能です。

診断結果では、**自組織に求められる情報セキュリティの水準（グループⅠ・Ⅱ・Ⅲ）が判定される**ほか、そのグループの平均値や望まれる水準値と自組織のスコアがグラフ上で比較できます（左図）。

また、左図のほかにも、同程度の従業員規模の企業や同業種の企業との比較グラフも出力され、多面的な観点から、自組織の情報セキュリティ対策の実施状況を分析することができます。

診断結果とともに、推奨される取り組みの例も示され、対策強化のための参考にすることも可能です。

情報セキュリティ管理者の育成のヒント

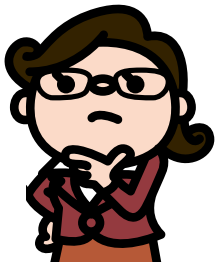
組織内で適切な情報セキュリティ対策を実施するためには、情報セキュリティを担う人材を配置することが必要です。しかし、情報セキュリティの分野はITに関する一定の知識を必要とすることも多く、その人材の育成には課題が多いのが現状です。こうした現状を踏まえて、ここでは、IPAが実施した調査（※）の結果から、情報セキュリティ管理者の育成に関するヒントを紹介します。

（※）平成25年度、IPA IT人材育成本部HRDイニシアティブセンターは、「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」を実施しました。この調査では、ITベンダーや情報セキュリティベンダー、ユーザー企業において情報セキュリティを担う人材の育成に関する現状と課題を整理するとともに、情報セキュリティを担う専門人材の育成に向けたガイドブック（本冊子の前編）を作成しました。調査の詳細は、http://www.ipa.go.jp/jinzai/hrd/security/ をご覧ください。

■ 情報セキュリティ対策の実施に関する悩み

情報セキュリティ対策の実施や現場部門の情報セキュリティ管理者に関する課題として、たとえば以下のような点が挙げられます。

① 情報セキュリティ管理者のスキルアップが難しい。
② 現場が情報セキュリティの重要性を理解してくれない。
③ 経営層に対して、情報セキュリティ対策の重要性を効果的に伝えられず、組織全体としての対策が進まない。



①は、多くの組織で聞かれる課題です。情報システム部門等の専門部署に所属する情報セキュリティの管理者は専門性の高い人材が専任で担うこともありますが、現場部門の情報セキュリティ管理者は、他の本業と兼任で情報セキュリティ対策の推進を担当することが多くなります。そのような場合、その担当者のスキルアップは、より難しい課題となります。

②は、情報セキュリティ管理者の採用や選任時に関する課題ともいえるほか、情報セキュリティ管理者が情報セキュリティ対策を実際に実施する際の大きな課題でもあります。

③は、現場部門としては情報セキュリティ対策をもっと強化したいと考えているが、経営層などの上層部の理解が得られないなどといった場合の課題です。

■ こんな取り組み例があります！

前ページのような課題に対して、IPAの調査では、有識者WGによる議論やインタビュー調査を通じて、以下のような取り組み例や意見が集まりました。組織によって置かれた状況は様々に異なるため、以下の例がそのまま活用できるとは限りませんが、情報セキュリティ対策の実施や情報セキュリティ管理者の育成に関する課題の解決に向けたヒントとしてご紹介します。

1 情報セキュリティ管理者のスキルアップが難しい。

部門に専任の情報セキュリティ管理者が配置されていることは少なく、多くの担当者は数年で異動・交代することが一般的であるため、限られた期間で効果的にスキルアップする必要がある。**情報セキュリティマネジメントに関する資格などの学習**も効果的である。

たとえ情報セキュリティ管理者が専任であったとしても、**自社のビジネスや業務に関する知識**を習得することが重要である。自社の業務に関する知識がないと、自社にとって有効な情報セキュリティ対策を立案・実施することは難しい。

情報セキュリティに関する最新の技術動向などについては、**外部のセキュリティコンサルタントから情報を収集**している。

2 現場が情報セキュリティの重要性を理解してくれない。

セキュリティに関する事故を経験したことがあるかないかによって、現場部門のセキュリティ意識は大きく異なる。以前事故が発生したことをきっかけに、経営者がセキュリティ対策を現場横断的な重要なテーマとして掲げ、組織全体としての取り組みを始めることができた。

情報セキュリティに関する専任組織を設置したほか、**各組織にも情報セキュリティ管理者を置いた**ことで、情報セキュリティに対する意識が組織全体として向上した。

3 経営層に対して、情報セキュリティ対策の重要性を効果的に伝えられず、組織全体としての対策が進まない。

企業にとってのセキュリティ対策は、今や単なる事故の予防ではなく、**企業のサービスの機能・品質の向上の一環である**ということを、経営者に伝える必要がある。

経営層に対してセキュリティの重要性を伝えられる人材の有無によって、経営層の理解が変わる。これは、経営とＩＴの関係と同じであり、“経営と現場をつなぐキーマンの育成”が鍵である。

情報セキュリティ強化対応スキル指標のご紹介

IPAでは、従来のITスキル標準（ITSS）や情報システムユーザースキル標準（UISS）等のスキル標準を包含する形で統合整理した、業務（タスク）とスキルの辞書データを**「ｉコンピテンシ ディクショナリ」**として公開しています。このｉコンピテンシ ディクショナリを参照することで、スキル標準の区別を意識することなく、スキル指標としてIT関連業務に携わる人材の役割、タスクやスキルを確認することができます。

IPAでは、情報セキュリティを担うIT人材の育成促進を目的として、ｉコンピテンシ ディクショナリから情報セキュリティ関連のタスクとスキルを抜粋しコンパクトに整理した**「情報セキュリティ強化対応スキル指標」**を公表しました（2014年8月公開、2015年8月改訂）。これは、ITベンダー企業と一般企業に必要な、情報セキュリティを担う人材の役割定義を例示し、役割ごとに想定されるセキュリティ業務（タスク）とそれに必要なスキルを対応づけて紹介したものです。

ここでは、「情報セキュリティ強化対応スキル指標」の使いかたを紹介します。情報セキュリティ強化のための人材育成の参照モデルとして、ご活用いただくことを想定しています。

「情報セキュリティ強化対応スキル指標」は、IPAのホームページからダウンロードしてご利用ください。

★情報セキュリティ強化対応スキル指標のダウンロード ★
http://www.ipa.go.jp/jinzai/hrd/security/
IPAホームページ＞IT人材の育成＞情報セキュリティスキル強化についての取組

情報セキュリティ強化対応スキル指標で例示した役割

「情報セキュリティ強化対応スキル指標」では、一般企業に必要と思われる情報セキュリティ人材の役割分担例として以下を定義しています。

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）	自社の情報セキュリティ戦略やポリシーの策定等を推進する役割。戦略策定のほか、戦略実行体制の確立や開発組織の統括も担う。また、企業内のセキュリティ業務全体を俯瞰し、アウトソース等のリソース配分の判断・決定も行う。
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）	自社の情報セキュリティ対策の具体化や実施を統括する役割。企業全体としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込み、対策の立案や実施（指示・統括）、その見直しなどを行う。また、利用者に対する教育等も実施する。
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）	自社内のセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧業務の実施において、自らあるいは適切な対応者をアサインして対応にあたる役割。被害の拡大防止のために、適切かつ迅速な対応が求められる。
情報セキュリティマネジメント※	情報システムの利用部門にあって、部門の情報セキュリティリーダとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の目的・内容を適切に理解し、情報及び情報システムを安全に活用するために、情報セキュリティが確保された状況を実現し、維持・改善する。

※本書で説明した「現場の情報セキュリティ管理者」は、情報セキュリティ強化対応スキル指標においては**「情報セキュリティマネジメント」**として役割定義しています。

情報セキュリティ強化対応スキル指標の使い方

「情報セキュリティ強化対応スキル指標」を見ると、「タスクプロフィール」と「職種一覧」に「情報セキュリティマネジメント」の定義が記述されており、その役割の**業務内容の例を参照できます**（以下はその一部を抜粋したものです）。

タスクプロフィール	タスクプロフィールの説明
情報セキュリティマネジメント	情報システムの利用部門において、部門の情報セキュリティリーダとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の目的・内容を適切に理解し、情報及び情報システムを安全に活用するために、情報セキュリティが確保された状況を実現し、維持・改善する。

「タスクプロフィール×タスク対応表」には「情報セキュリティマネジメント」等のタスクが定義されており、情報セキュリティ業務に関連する**具体的なタスクを参照できます**。

タスク大分類コード	タスク大分類	タスク中分類コード	タスク中分類	タスク小分類コード	タスク小分類	新ビジネス別 情報セキュリティ関連業務							
						コンサルタント（情報リスクマネジメント） D-030-010	ITアーキテクト（セキュリティアーキテクチャ） D-030-020	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） D-030-030	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） D-030-040	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） D-030-050	セキュリティマネージャ（組込みセキュリティ） D-030-060	情報セキュリティマネジメント D-030-080	ITスペシャリスト（セキュリティ） D-030-070
US02	IT運用コントロール	US02.1	IT運用管理	US02.1.1	ユーザ管理							○	○
				US02.1.2	オペレーション管理								○
		US02.2	情報セキュリティ管理	US02.2.1	情報セキュリティの運用				○	◎		◎	○
				US02.2.2	情報セキュリティの評価と検証				○			◎	○
US03	システム運用管理	US03.1	障害管理	US03.1.1	障害対応								○
				US03.1.2	障害記録・再発防止								○
		US03.2	問題管理	US03.2.1	問題コントロールの開始								○
				US03.2.2	エラーコントロール								○
		US03.3	性能管理	US03.3.1	パフォーマンスとキャパシティの管理								○
		US03.4	構成管理	US03.4.1	構成管理の計画策定と設計								○
				US03.4.2	構成管理の実施								○
		US03.5	資源管理	US03.5.1	ハードウェアの管理								○
				US03.5.2	ソフトウェアの管理								○
				US03.5.3	データの管理								○
				US03.5.4	ネットワーク資源の管理								○
		US03.6	リリース管理	US03.6.1	リリースの計画、準備と実施								○
		US03.7	セキュリティ障害管理	US03.7.1	事故の検知							○	○
				US03.7.2	事故の初動処理					◎		◎	○
				US03.7.3	事故の分析					◎		○	○
				US03.7.4	事故からの復旧					◎		○	○
				US03.7.5	再発防止策の実施					◎		○	○
				US03.7.6	セキュリティの評価					◎			○

「職種×スキル対応表」には、以下のように、**職種・専門分野別に求められるスキルも定義されており、人材育成の参考にすることができます**。

表記説明
各職種の定義（「職種一覧」　参照）に基づいて、特に必要なスキル項目に◎を記入
（「（共通技術）　IT基礎」、「ITヒューマンスキル」を除く）

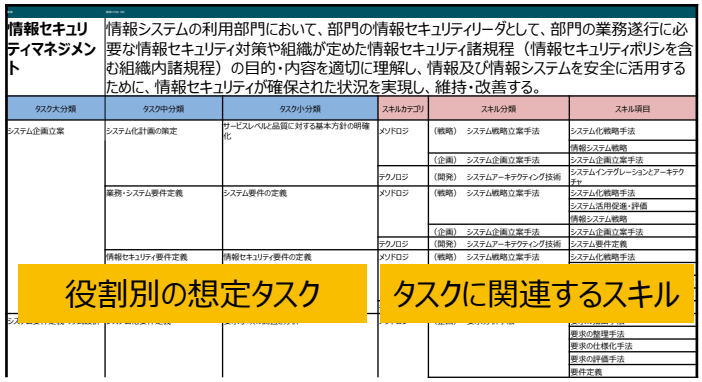
スキル項目コード	スキルカテゴリ	スキル分類	スキル項目	情報セキュリティ人材 コンサルタント（情報リスクマネジメント） HS-010-010	ITアーキテクト（セキュリティアーキテクチャ） HS-020-010	セキュリティアドミニストレータ（情報セキュリティアドミニストレータ） HS-030-010	セキュリティアドミニストレータ（ISセキュリティアドミニストレータ） HS-040-010	セキュリティアドミニストレータ（インシデントハンドラ） HS-050-010	セキュリティマネージャ（組込みセキュリティ） HS-060-010	情報セキュリティマネジメント HS-080-010
S150030010	メソドロジ	（支援活動）リスクマネジメント手法	リスク管理手法	◎		◎	◎			◎
S150030020			情報セキュリティ管理手法	◎	◎	◎	◎			◎
S150040010		（支援活動）ITガバナンス	ITガバナンス手法							
S150040020			内部統制							
S150060010		（支援活動）資産管理手法	資産管理に関する手法							
S150060020			知的資産の管理活用手法							
S150070010		（支援活動）ファシリティマネジメント手法	ファシリティマネジメント							
S150080010		（支援活動）事業継続計画	BCP策定手法							
S150080020			災害対策管理手法							
S150090010		（支援活動）システム監査手法	システム監査							
S150100010		（支援活動）標準化・再利用手法	ソフトウェア開発プロセスの標準化手法		◎				◎	
S150100020			ソフトウェアエンジニアリングの標準化手法		◎				◎	

さらに、「役割×タスク×スキル表」として、それぞれの情報セキュリティ人材の役割ごとに、タスク一覧とそれを実行するために必要なスキルを関連づけた表を用意しています。

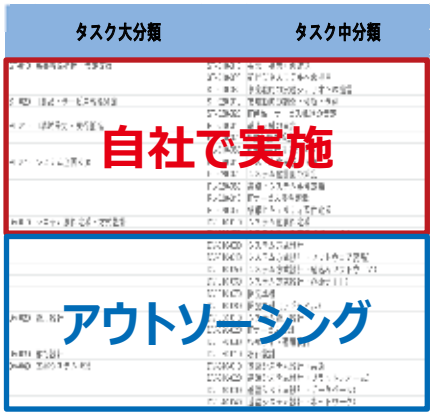
情報セキュリティ強化対応スキル指標の活用例（１）「タスクデータ」の活用

スキル指標にある「タスク」データを使った活用例を紹介します。
情報セキュリティ人材の「役割×タスク×スキル表」にあるデータは、役割別の業務とスキルが一覧になっています。これを利用して役割別の「職務定義書」などを作ることができます。
また、タスク一覧のデータを加工すれば、セキュリティ関連業務を一覧で参照できますので、どの業務をアウトソーシングするか等情報セキュリティ関連業務の切り分けの検討にも使うことができます。

例1）職務定義書



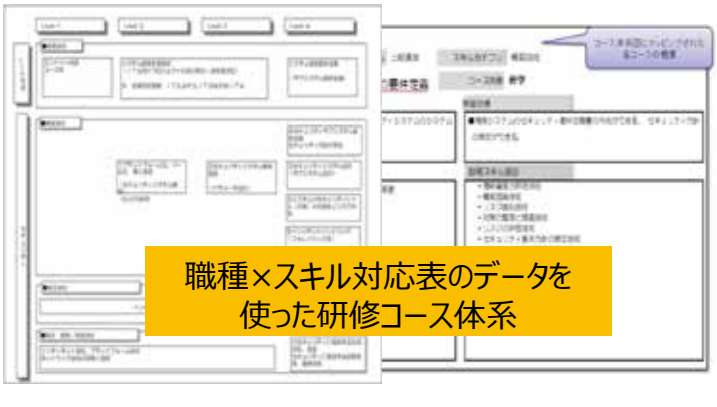
例2）アウトソーシングの検討



情報セキュリティ強化対応スキル指標の活用例（２）「スキルデータ」の活用

スキル指標にある「スキル」データを使った活用例を紹介します。
「職種×スキル対応表」にあるデータは、自社でレベル別にカテゴライズして、育成プログラム（研修ロードマップ）を作成することができます。「職種×スキル対応表」のデータを加工すれば、スキル診断や保有量調査等に利用することもできます。

例3）育成プログラムの検討



例4）スキル診断

i コンピテンシ ディクショナリのご紹介

iCD i Competency Dictionary

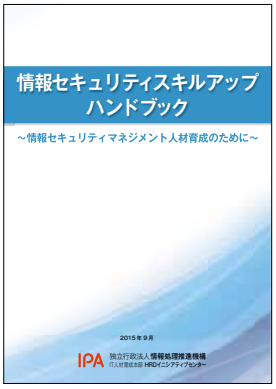
本書で紹介した以外に、自社で独自に情報セキュリティ人材の役割分担の定義をしたい場合等は、「i コンピテンシ ディクショナリ」をダウンロードしてご利用ください。

i コンピテンシ ディクショナリのダウンロード
http://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/

「情報セキュリティスキルアップハンドブック」のご紹介

本書で紹介した「情報セキュリティ管理者」の具体的な育成方法については、別冊の**「情報セキュリティスキルアップハンドブック~情報セキュリティマネジメント育成のために~」**をご利用ください（定価1,000円（税込））。

目次



※冊子の入手方法については　http://www.ipa.go.jp/jinzai/hrd/security/　をご覧ください。

「情報セキュリティマネジメント試験」のご紹介

本書で紹介した「情報セキュリティ管理者」のスキルの確認には、国家試験である情報処理技術者試験の「情報セキュリティマネジメント試験」をご利用ください。情報セキュリティマネジメント試験は平成28年春から開始します。

情報処理技術者試験センターホームページ
http://www.jitec.ipa.go.jp/

IPA

職場の情報セキュリティ管理者のための スキルアップガイド

２０１５年９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/
東京都文京区本駒込二丁目 28 番８号
文京グリーンコートセンターオフィス 15 階

※ 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。