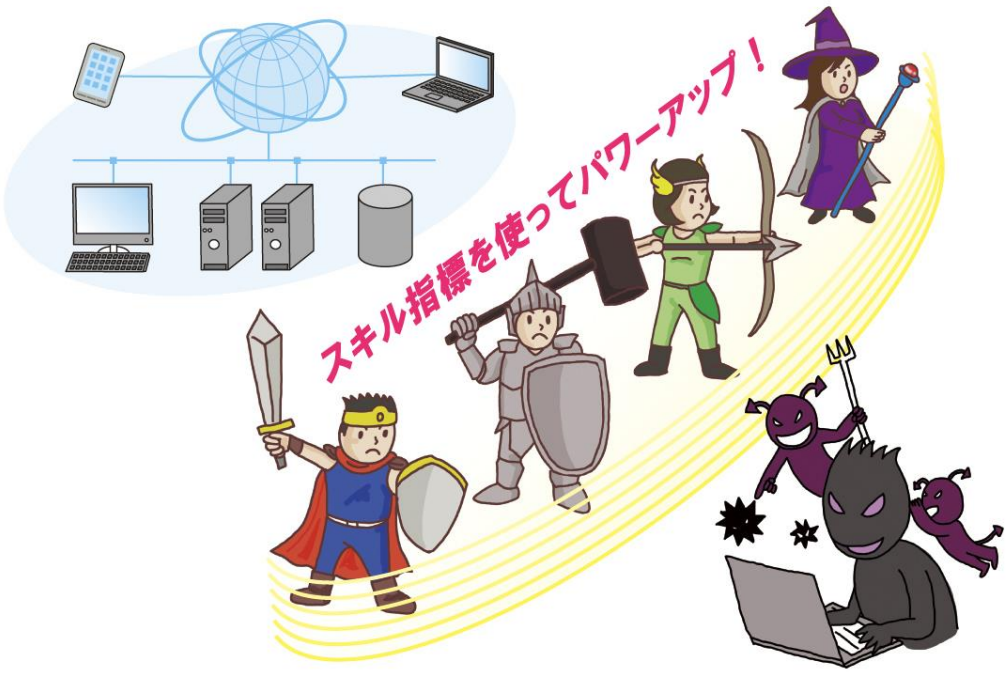
IPA Better Life with IT

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

～情報セキュリティ上の脅威から企業を護るために～



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

本ガイドのねらい

情報セキュリティ対策は、今や企業にとって必要不可欠なものとなっています。ひとたび企業が保有する顧客情報が漏えいするような事故が起こり、それが世間に知られると、**それまでに企業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、企業側には、以前にも増して強固な対策が求められるようになっています。

このように、情報セキュリティ対策の重要性が高まるにつれて、最近では、それを担う人材の育成が重要な課題として注目されるようになりました。本ガイドは、こうした流れを受けて実施された「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」の成果として作成されたものです。本ガイドでは、企業が対策を行うべき50種類以上の情報セキュリティ上の脅威のなかから、最近特に注目されている脅威を６つ取り上げ、その脅威によって発生する被害を防ぐためには**どのような対策が必要なのか**、また、その対策を実施するためには、**どのような役割（人材）が重要なのか**を、例として紹介しています。

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推進に向けて、2014年8月**「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。当ガイドでは、情報セキュリティを担う人材として登場する役割とそれらに必要なスキルについて、この「情報セキュリティ人材強化対応スキル指標」を**活用する方法も**紹介しています。

情報セキュリティを担う人材の育成に関しては、様々な課題が指摘されており、多くの企業が悩みを抱えているという現状があります。そこで、こうした課題の解決に向けた一助として、今回実施された調査を通じて得られた情報を**「情報セキュリティを担う人材育成のヒント」**としてまとめました。

さらに、情報セキュリティ対策は組織全体として実施することがきわめて重要であり、それが人材の育成にもつながるという観点から、**「組織において求められる情報セキュリティ対策」**についても簡単に紹介しました。

本ガイドが、情報セキュリティを担う人材育成に課題を感じているユーザー企業やITベンダー、セキュリティベンダーの皆様のための参考資料となれば幸いです。

※ 本ガイドは、以下のような読者を対象として想定しています。

- **ユーザー企業、ITベンダー、セキュリティベンダー等の企業経営層**
- **ユーザー企業、ITベンダー、セキュリティベンダー等において、情報セキュリティを担う人材の育成に携わっている方**

目次

本ガイドではまず、企業にとっての大きなリスクになり得る情報セキュリティ上の脅威に着目します。情報セキュリティ上の脅威としては様々なものが知られていますが、本ガイドでは、最近特に注目度が高いと考えられる脅威を６つ取り上げました。

さらに、それぞれの脅威による被害を防ぐために必要な対策やそのための簡易チェックリストを示すとともに、そのような対策を実際に企業で行うために必要な役割（人材）を紹介しています。

あなたの企業に迫る脅威！

あなたの企業は大丈夫ですか？

企業の規模や業種に関係なく、多くの企業でITが利用されています。今やパソコンや電子メールは業務において必要不可欠なものです。また、ITの高度化、多様化の流れもあり、クラウドサービスやスマートデバイスなど新しいサービスや技術が出てきており、ビジネスシーンで利活用されることも多くなってきました。ついついITの利便性に目が行きがちですが、適切な情報セキュリティ対策を講じなければ、企業の大切な「情報資産」が侵害される恐れがあることは忘れてはいけません。

今回、独立行政法人情報処理推進機構（IPA）HRDイニシアティブセンターでは、企業における情報セキュリティ上の多数の脅威に注目し、その中でもより対策が必要と考えられる脅威を６つ取り上げました。これらの脅威をもとに、今一度あなたの会社の情報セキュリティ対策を振り返ってみましょう。

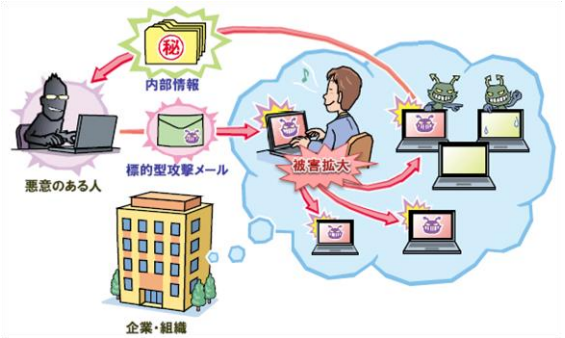
～ 本ガイドで取り上げる脅威 ～

① 標的型攻撃・サイバー攻撃
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

※ 上記に掲載した脅威以外にも、DDoS攻撃やパスワードを含めた情報の漏えいなど多くの脅威がありますが、これらの脅威にも対策は必要になります。

① 標的型攻撃・サイバー攻撃（マルウェア、ウイルスを含む）

不特定多数の相手ではなく、特定のターゲット（企業・組織など）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を行うサイバー攻撃を「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、企業にとっては十分な警戒が必要です。

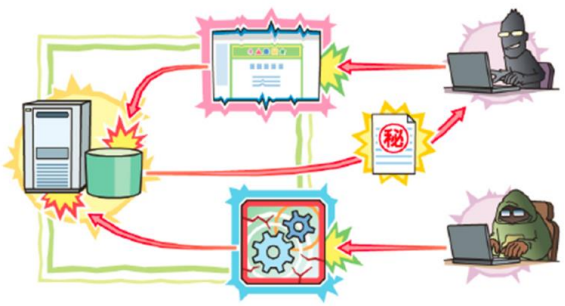


例えば
こんな危険が・・・

システム内部に潜入したウイルスがバックドアを設置し、攻撃者配下のサーバと通信を行うことで、システム内部の情報が攻撃者から筒抜け状態になります。内部からのハッキングを想定していないシステムは、このような攻撃に対して脆弱です。

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ています。また、共通的な思想を持つ集団によって、ウェブサイトを改ざんされ、主張を誇示する攻撃等が増加しています。

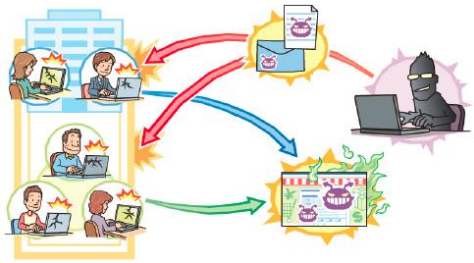


例えば
こんな危険が・・・

ウェブサイトから顧客情報が流出したり、ウイルスの配布に悪用されることで、企業や組織の信頼喪失に繋がります。また、権威あるサイトの内容が悪意ある内容に書き換えられた場合、企業や組織の権威を損なうことになります。

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ます。直接的な攻撃から特定のシステムへの潜伏、ウイルス拡散を意図したと思われる事例もあり、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ます。



例えば
こんな危険が・・・

クライアントソフト等の脆弱性を放置しておくことで、ウイルス感染のリスクが高くなります。ソフトウェアの更新を行うことの必要性や更新の方法を把握しておらず、個人情報が窃取されたり、金銭的な損失、PCを遠隔から操作されるなどの様々な被害が考えられます。

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する手段は、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があります。また、適切なアクセスコントロールがなされていない場合、情報流出のリスクがあります。

例えば
こんな危険が・・・

外部のクラウドにデータが集約される形となるため、ネットワークの影響を大きく受け、企業や組織の事業が停止する可能性があります。

⑤スマートデバイスからの情報漏えい

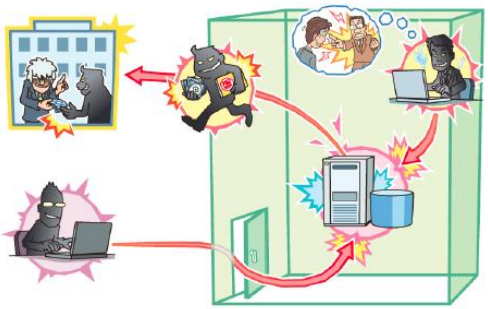
各企業においてBYOD（Bring Your Own Device）の利用ケースが増加し、モバイル機器等、従来型システム以外からの情報漏えいのリスクが懸念されています。

例えば
こんな危険が・・・

取引先情報の記憶やメールのやり取りが可能なスマートデバイスの紛失や悪意あるアプリケーションのインストールによって、情報が漏洩する恐れがあります。

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が発生することもあります。風評被害等が懸念され、被害が公表されることは少ないのですが、インシデントが発生すると、被害の規模は非常に大きく、企業の内部統制やマネジメントも疑問視されるため、組織にとって大きな脅威であると言えます。

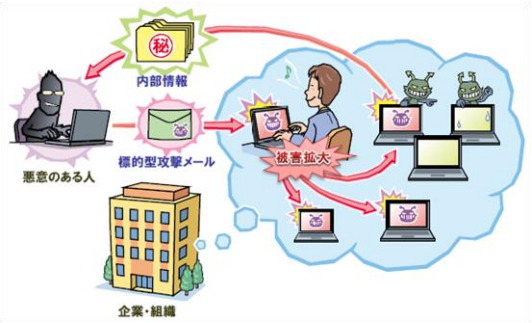


例えば
こんな危険が・・・

社内システムにアクセスできる権限を持つ従業員は、自らの権限を利用して内部システムにアクセスし、業務妨害、重要情報・顧客情報などの持ち出しによる情報漏えいを行うことができる。

脅威1

標的型攻撃・サイバー攻撃



不特定多数の相手ではなく、特定のターゲット（企業・組織や個人など）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を狙って行われるサイバー攻撃を「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、企業にとっては十分な警戒が必要です。

■ 必要な対策は実施されていますか？

標的型攻撃として、近年、**電子メールを通じて企業内部のシステムに侵入し、不正なプログラム等によって機密情報を盗むような攻撃**が増えています。最近では、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、または急いで開封する必要がある印象を与えるようなメールも増えており、手口がますます巧妙化しています。また、侵入後、気づかれないまま組織の情報を盗み続けていたというケースも発見されています。

こうした「新しいタイプのサイバー攻撃」に対しては、社内のシステムの設計・設定、ウィルス対策ソフトの導入・運用を適切に行うなどの一般的な対策をしっかりと実施するのは当然のことながら、**システムの利用者に対する教育を徹底する**ことや、**万が一の事故の発生も視野に入れ、その際に被害を最小化できるような対策を十分に講じておく**ことなども重要です。

あなたの企業は大丈夫？

＜対策実施チェックリスト＞

- □ ウィルス対策ソフトを社内のすべてのコンピュータに導入し、ウィルスチェックやウィルス対策ソフトの更新を頻繁に実施していますか。
- □ 社内のメール利用者に対して、「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」などの基本事項についての教育が徹底されていますか。
- □ ウィルス対策ソフトから「ウィルスに感染した」という警告メッセージが表示された場合、まず何をすればよいか、すべての従業員が十分に理解していますか。
- □ 標的型攻撃を防御・検知するためのシステムの監視を行っていますか。また、そのような機能をもったセキュリティ対策ソフトを導入していますか。
- □ ウィルス感染や情報漏えいが発覚した場合の組織としての緊急対応手順は定められていますか。また、その手順は関係者に周知されていますか。

■ 被害を防ぐためには、こんな役割も重要です！

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

標的型攻撃の攻撃者は、攻撃対象の企業を調べた上で、セキュリティ上一見問題のないメールを巧妙に装って侵入を試みます。技術的な対策だけでは防御しきれない高度な攻撃が行われる可能性があるため、一般的な予防策をしっかりと講じておくほかにも、万が一、予期せぬウィルス感染や情報漏えいなどの事故が発生した場合に、それを**できるだけ早期に検知する**ことや、**迅速な対処によって被害を最小限に食い止める**ことが非常に重要です。

最近では、公的機関だけではなく、一般の民間企業に対しても、標的型メールを用いて機密情報を盗み出すような攻撃が増えています。企業では、こうした標的型攻撃を受けた場合の事後対応策を予め想定しておき、万が一、利用者が誤って不正なメールを開いてしまった場合などには、それらの事後対応策を迅速に実施することで、**自社の信頼や評判を揺るがすような甚大な被害が発生する前に、被害を最小限にとどめる**ことが重要です。

■ その役割を担う人材の例

情報セキュリティ強化対応スキル指標から

情報セキュリティ強化対応スキル指標では、**セキュリティに関する事故（セキュリティインシデント）が発生した場合に必要な役割**として、以下のような人材を示しています。企業では、情報システム部門の担当者や情報システムの運用を担う担当者が、以下のような業務について理解し、必要に応じてその役割を担うことが求められます。

自社向け

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。

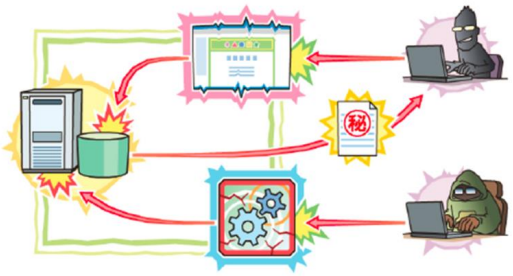
顧客向け

ITサービスマネジメント
（システム管理）

顧客の情報システムの日々の運用業務やシステム基盤の管理業務を担い、円滑な運用を実現する役割。運用時に**セキュリティインシデントをモニタリング**し、インシデントが発生した場合には、被害拡大防止等の初動対応を担う。

脅威2

不正アクセス



セキュリティ対策の弱い部分を突いて、企業のWEBサイトや内部のシステムに悪意のあるユーザーが不正にアクセスし、顧客情報などの重要情報や機密情報を盗んだり、企業のWEBサイトを改ざんしたりするなどして、自社だけではなく自社の顧客にまで被害を及ぼすような攻撃も増えています。

■ 必要な対策は実施されていますか？

不正アクセスとは、他人のIDやパスワードを使ったり、ソフトウェアのセキュリティ上の弱点を悪用したりするなどして、本来は利用権限のないコンピュータを不正に利用し、**重要な情報を盗んだり、内部のデータやプログラムを改ざんする攻撃**のことです。最近では例えば、ユーザーがパスワードの管理の負担を減らすために、複数のWEBサイトで同じパスワードを用いることも増えています。しかし、こうした場合、あるWEBサイトのパスワードが流出すると、他のWEBサイトに対して同じパスワードを試行され、不正アクセスが成功してしまうことがあります。

不正アクセスによる攻撃者の侵入を許してしまった場合は、**顧客情報のような重要情報が漏えいする可能性もある**ほか、一見気づかないような形で企業のWEBサイトが改ざんされ、**閲覧者に対してウィルスを自動的にダウンロードするようなプログラムが埋め込まれる**こともあり、このような攻撃も増えています。自社の顧客が利用するWEBサイトがこうした攻撃を受けると、**顧客にまで被害が及んでしまう可能性がありますので**、十分な警戒が必要です。

あなたの企業は
大丈夫？

＜対策実施チェックリスト＞

- ☐ 123456, admin, password などの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、定期的に変更するなど、パスワードに関する基本的なルールが社内で徹底されていますか。
- ☐ 自分の席を離れる際は、パスワードで保護されたスクリーンセーバーでパソコンを保護することをルール化していますか。
- ☐ 退職した従業員の ID など、不要な ID を放置せず、きちんと削除していますか。
- ☐ ユーザーごとにアクセス権を設定し、定期的な見直しや管理を行っていますか。
- ☐ 企業内のネットワークやコンピュータに、ファイアウォールなどの外部からの不正アクセスを検知・遮断する仕組みを導入していますか。
- ☐ 自社が提供しているサービスについて、不正アクセス対策を実施していますか。
  （例：不正アクセス対策　http://www.ipa.go.jp/security/fusei/ciadr.html）

■ 被害を防ぐためには、こんな役割も重要です！

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

不正アクセスを防ぐための方策として、日頃から**セキュリティに関するルールを明確にし、ユーザーにルールを守ってもらうための管理**をしっかりと行うことも重要です。パスワードに関するルールなどについては、ユーザーへの教育を通じて企業全体の意識を高めるとともに、安全性の低いパスワードは設定できないようにするなどのシステム上の対応も効果的です。こうしたルールの検討・整備やその実施を推進するためには、**企業内でセキュリティ管理業務を担う担当者を明確にしておく**ことが重要となります。

セキュリティ管理業務には、例えばユーザーごとのアクセス権限を設定する、不正アクセスを監視する仕組みを導入するといった技術的な業務から、ユーザーに対する教育を実施するという管理的な業務まで、幅広い業務が含まれます。このような管理業務は、**情報漏えいやデータの破壊などのセキュリティに関する事故を防ぐ上で、非常に重要な意味を持っている**といえます。

■ その役割を担う人材の例

情報セキュリティ強化対応スキル指標から

情報セキュリティ強化対応スキル指標では、セキュリティ管理のタスクを実行する役割として、以下のような人材を示しています。企業でのセキュリティ対策や管理を十分に行うためには、**必ずしも専任者である必要はありませんが、以下のような役割を持った担当者を明確にし、その担当者が責任を持って対策や管理を進めることがポイント**です。

自社向け

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。

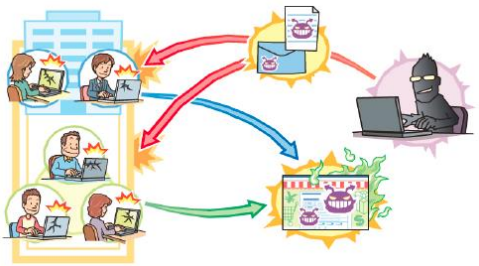
顧客向け

ITサービスマネジメント
（運用管理）

顧客の情報システムの運用管理の責任者として、ITサービスマネジメントの統括責任を担う。セキュリティの面では、**運用するシステムのセキュリティマネジメントに関する方針や計画を策定し、具体的な対策の実施を統括する**。

脅威3

エクスプロイト



プログラムの弱点（脆弱性）を狙った攻撃は「エクスプロイト」と呼ばれています。自社で構築したシステムや利用しているソフトウェアに脆弱性があると、そこに付け込んだ攻撃が行われることがあります。最近では、まだ広く知られていない未知の脆弱性が狙われる攻撃も増えています。

■ 必要な対策は実施されていますか？

多くのユーザーに利用されているソフトウェアや脆弱性がよく発見されるようなソフトウェアは、エクスプロイトの対象として狙われやすいといえます。そのため、例えば、Windows や Microsoft Office, Internet Explorer, Adobe Reader など、利用者が多いソフトウェアについては、脆弱性の発見に関する情報やそのための修正プログラム（セキュリティパッチ）に関する情報に注意を払い、**公表されたら迅速にセキュリティパッチを適用する**必要があります。

また、自社でシステムを開発する際も、開発後に脆弱性が発見されて外部から攻撃を受け、企業の評判を傷つけるような事態を防ぐために、**設計・開発の段階から、セキュリティに関する知見を持った技術者が参加し、安全性の高いシステムを実現する**ことが重要です。特に外部から不特定多数のユーザーがアクセスできるWEBシステムについては、十分な対策が求められます。

あなたの企業は
大丈夫？

＜対策実施チェックリスト＞

- □ 社内のコンピュータ上で利用しているソフトウェアの修正プログラム（セキュリティパッチ）が公表されたら迅速に適用していますか。セキュリティパッチが適用されずに長期間そのまま利用されているコンピュータはありませんか。
- □ セキュリティパッチの適用状況をきちんと把握していますか。また、それを把握し、管理する担当者は決められていますか。
- □ 情報システムを設計・開発する際に、セキュリティに関する仕様や基準、要求事項などを明確にしていますか。
- □ 開発した情報システムのテストを行う際に、外部からの攻撃などを意識したセキュリティに関するテストも実施していますか。
- □ 現在運用している自社のWEBシステムに脆弱性がないか、検査を行ったことはありますか。

■ 被害を防ぐためには、こんな役割も重要です！

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

エクスプロイトによる被害を防ぐためには、**脆弱性対策**をしっかりと行うことが重要です。特に日頃利用しているソフトウェアの脆弱性が発見され、修正プログラム（セキュリティパッチ）が公表されたら、自社内のコンピュータに迅速に適用することが必要です。また、こうした対策を企業で実際に実現するためには、「不正アクセス」のページでも紹介したような、**セキュリティパッチの公表状況を把握し、責任を持って社内にその適用を指示・統括する担当者を決めておく**ことも重要となります。

また、自社が提供するWEBシステム等の安全性を高めるためには、セキュリティに関する知識を持ち、**設計・開発の段階からセキュリティ対策を考慮する技術者の役割**も重要です。高いスキルを持った攻撃者による高度な攻撃が増加する昨今では、システムの設計・開発時から最大限の対策を実施することが求められています。

■ その役割を担う人材の例

情報セキュリティ強化対応スキル指標から

情報セキュリティ強化対応スキル指標では、システム設計・開発の段階でセキュリティ対策を考慮する役割として、以下のような人材を示しています。ますます高度化する攻撃による被害を防ぐためには、**以下のような技術系の人材の能力を最大限に活用し、セキュリティ対策が十分に考慮された安全なシステムを構築する**ことが望まれます。

自社向け

システムデザイナー

自社で用いるシステムの要件定義から、システム基盤（インフラストラクチャ）の分析・設計及び構築を担う役割。**ネットワークの構成やアプリケーション基盤の設計の際に、セキュリティを考慮した設計を行う**。

顧客向け

ITスペシャリスト
（セキュリティ）

情報システムの設計・開発・運用において、情報セキュリティに関する高い専門性を発揮するスペシャリスト。
セキュリティインシデントが発生した際は、高度な技術的スキルを駆使して原因の究明や復旧対応等も担う。

脅威4

クラウド利用におけるデータ消失・流出

手軽に利用できるクラウドサービスは広く普及し、多くの企業に利用されています。社外のリソースを活用することは、災害対策を含むシステムの可用性向上策として有効な一方で、自社の管理が及ばない領域で被害が発生するリスクもあり、自社内のセキュリティ対策とは異なる注意が必要です。

■ 必要な対策は実施されていますか？

自社でシステムを構築するよりも安価で手軽に利用できるクラウドサービスは、広く普及しています。しかし、クラウドサービスでは、インターネット経由でサービス提供事業者のリソースを活用するため、**事業者側で発生したトラブル等によってデータの消失が起こる可能性**があります。また、IDやパスワードが盗まれ、不正なユーザーが「なりすまし」によって自社のデータにアクセスし、**データの流出や改ざんが起こる危険性**も指摘されています。

こうした被害を防ぐためには、重要な情報はクラウド上に保存しない、サービス提供事業者のセキュリティ対策を確認する、自社でもバックアップを取っておく、などの対策が重要です。また、今後はクラウドサービスを一部利用することを想定して自社システムの設計を行い、**クラウドサービスの利用も含めた形でセキュリティ対策を考える**ことがますます重要になるといえます。

あなたの企業は
大丈夫？

＜対策実施チェックリスト＞

- □ 外部のクラウドサービスを利用する際のリスク（データの消失・流出や改ざんなど）について認識していますか。
- □ 自社のどのような情報がクラウドサービス上にあるか、把握していますか。
- □ クラウドサービスの利用・管理に関する責任者や実務担当者を決めていますか。
- □ クラウドサービスを提供する事業者が実施しているセキュリティ対策の具体的な内容や水準を把握していますか。
- □ クラウドサービスを利用する際の ID やパスワードは、適切に管理していますか。特に「なりすまし」を防ぐために、推測されにくいものになっていますか。
- □ クラウドサービスの停止時や障害発生時に、情報が手元で（自社内で）利用できるような対策が取られていますか。

■ 被害を防ぐためには、こんな役割も重要です！

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

クラウドサービスは、今後さらに利用・普及が進み、企業の情報システムに不可欠なサービスになっていくと考えられます。つまり、今後の情報システムを設計する際は、**クラウドサービスの利用をあらかじめ想定した設計**を行うことがますます重要になるでしょう。情報システムのセキュリティ対策も、クラウドサービスの利用を前提として検討することが求められるようになると考えられます。

このように考えると、クラウドサービスを安全に利用するためには、**システム企画の段階から、セキュリティに配慮してシステム全体のアーキテクチャ等を設計するという役割**が、今後より一層重要になっていくことは明らかです。さらに、システム全体を設計する段階で、必要なセキュリティ対策やその水準を明らかにし、それに適したクラウドサービスを選定するという業務も、現在以上に重要になると予想されます。

■ その役割を担う人材の例

情報セキュリティ強化対応スキル指標から

情報セキュリティ強化対応スキル指標では、システム設計の段階でアーキテクチャの設計等を担う役割として、以下のような人材を示しています。クラウドサービスの利用に限らず、**安全性の高いシステムを実現するためには、設計の段階から、以下のような役割を持った人材の技術的な知見を活かす**ことが望まれます。

自社向け

ISアーキテクト

自社内の情報システム基盤の構築・維持・管理を主に担う役割。**自社のIT戦略に基づき、自社システムのアーキテクチャ設計を行う**ほか、基盤の整備や品質統制のための取り組みなども行う。

顧客向け

ITアーキテクト
（セキュリティアーキテクチャ）

強固なセキュリティ対策が求められる**情報システムのアーキテクチャの設計を担う**役割。システムの企画・開発・構築・運用の各工程において、情報セキュリティ対策が十分に機能し、維持されることを担保する**組織設計、ルール設計、プロセス設計**もあわせて行う。

脅威5

スマートデバイスからの情報漏えい

スマートフォンなどのモバイル機器（スマートデバイス）の普及が進むにつれ、業務で利用する機会も急速に増えています。こうしたモバイル機器は手軽に利用できる反面、紛失や悪意のあるアプリケーションの導入によって、業務情報が漏えいするリスクも大きく、こうしたリスクへの対策が求められています。

■ 必要な対策は実施されていますか？

スマートフォンやタッチパネル式のタブレット端末は、日常的に業務で利用されるようになってきました。しかし、こうした機器は手軽に持ち運べる反面、**置き忘れ・紛失や盗難などのリスク**も非常に大きいため、それをあらかじめ想定した対策が必要です。何の対策もされていない場合、**機器を落としただけで重要な情報が社外に漏れてしまう可能性**があり、きわめて危険です。

また、スマートデバイスを社外に持ち出して外部のネットワークに接続する場合、適切な対策が行われていないと、**機器に保存されている情報が外部に漏れてしまう恐れ**があるため、アクセス権限の管理なども重要です。さらに、従来型の携帯電話と異なり、パソコンと同じ利用環境で動作するスマートデバイスは、これまでパソコンやネットワークを攻撃のターゲットとしていた攻撃者の“次の狙い目”になりつつあるため、**パソコンと同じようなウィルス対策**も必要です。

＜対策実施チェックリスト＞

あなたの企業は
大丈夫？

- □ 紛失・盗難対策として、スマートフォンなどのモバイル機器の利用時に、パスワード入力しなければ使えない「パスワードロック」を設定していますか。
- □ ウィルス対策として、スマートフォンなどのモバイル機器のOSを、常に最新のバージョンにアップデートしていますか。
- □ スマートフォンのアプリは、メーカーやキャリアのアプリケーション・ストアなど、信頼できる場所からインストールしていますか。
- □ 業務で利用するスマートフォンなどのモバイル機器に、業務とは関係のないアプリが数多くインストールされていませんか。
- □ 私用のモバイル機器を業務上で利用することは、現状ではあまり推奨されませんが、利用可とする場合は、モバイル機器用のセキュリティソフトを導入するなど、適切なセキュリティ対策を利用者に義務付けていますか。

■ 被害を防ぐためには、こんな役割も重要です！

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

情報セキュリティ対策の不備やセキュリティに関する事故によって、自社の社会的信頼が損なわれるような事態が発生すると、事業戦略や経営戦略を実現する上での大きな足かせとなります。したがって、**十分な情報セキュリティ対策を行っておくことは、各企業の事業戦略や経営戦略を実現する上での前提である**ともいえます。

こうした**具体的なセキュリティ対策を方向付けるものが企業全体としての情報セキュリティ戦略**です。事業戦略や経営戦略を踏まえて情報セキュリティ戦略を策定するという役割は、企業の大小を問わず非常に重要な役割といえるでしょう。特に企業でのスマートデバイスの導入などにはリスクも伴うため、情報セキュリティ戦略を踏まえて決定することが望ましいといえます。また、利用時の具体的なルールの策定も、戦略に従って行うことが重要です。

■ その役割を担う人材の例

情報セキュリティ強化対応スキル指標から

情報セキュリティ強化対応スキル指標では、事業戦略や経営戦略を踏まえた情報セキュリティ戦略の策定を担う役割として、以下のような人材を示しています。情報セキュリティ戦略を策定する人材には、**事業戦略や経営戦略を十分に理解した上で、企業活動の安全性を高めながらも利便性を損なわないような適切な戦略を策定できる能力と経験**が求められます。

自社向け

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。

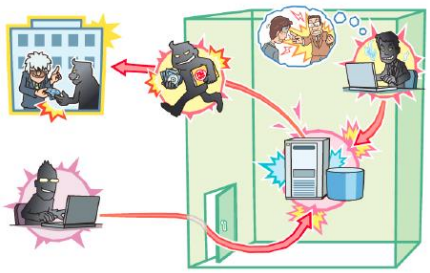
顧客向け

コンサルタント
（情報リスクマネジメント）

ビジネス機能内で**情報マネジメントが適切に実現される土台としての組織体制の整備や組織内の各種ルール整備等に関する支援を担う役割**。組織ガバナンスやリスクマネジメント、コンプライアンス等に関する領域において、ITソリューションを前提としたコンサルティングを行う。

脅威6

内部不正・うっかりミス



近年、従業員や元従業員等が情報を盗み出したり、システムを停止させたりするような事件が発生しています。外部からの攻撃を想定したセキュリティ対策は、正当な権限のある内部者の不正行為に対しては十分な効果を発揮できません。外部からの攻撃に加えて、内部の不正やミスを防ぐための対策も重要です。

■ 必要な対策は実施されていますか？

外部からの攻撃に対して十分な対策を実施するほかにも、**正当な権限を持つ内部の関係者による不正やうっかりミスを防ぐような体制・ルールづくり**も重要です。過去には、委託社員が「システムの動作確認」と称してホストコンピュータにアクセスし、顧客の口座情報を盗み出した事例や、退職した元社員が退職直後にまだ削除されていない自分のIDを使って内部の顧客情報を盗み出した事例などが報告されています。また、悪意のある不正行為のほかにも、うっかりした操作ミスなどによって重要なデータが削除されてしまうことなどもあります。

IPAのレポート（「組織の内部不正防止へ取り組み」2012年）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職場で発生しています。不正やうっかりミスを防ぐためには、**複数人員による実施体制**のほか、**作業の記録やバックアップ**などの対策も重要です。

あなたの企業は大丈夫？

＜対策実施チェックリスト＞

- □ 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。
- □ 社員の管理・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。多くの従業員が、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。
- □ 重要な顧客情報などを保存しているコンピュータは、管理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。
- □ 個人情報などの機密情報については、保存されているファイルにもパスワードを設定するなど、二重三重の対策を工夫していますか。
- □ 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。
- □ 重要な情報については、担当者を決めて定期的にバックアップを取っていますか。

■ 被害を防ぐためには、こんな役割も重要です！

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実行する役割

事業戦略や経営戦略に基づく情報セキュリティ戦略が策定されたら、**戦略に基づく情報セキュリティマネジメントを実現するために、具体的なセキュリティ方針やセキュリティに関するルール・基準などを策定する**ことが必要です。戦略は大きな方向性や目標を示すものですが、それを達成するための方法については、具体的なルールや基準として示すことが求められます。

内部者による不正やミスは、技術的な対策が難しい脅威です。外部からの攻撃を防ぐために高度な技術を導入しても、権限を持った内部の関係者がアクセスすれば、重要な情報に自由にアクセスできてしまいます。こうした事態を防ぐためには、**ルールづくり**が不可欠です。機密情報は一人で扱わないなど、**組織としてのルールを整備し、その遵守を義務付ける**ことが重要であり、組織内で責任を持ってその役割を担う担当者を決めておくことが望まれます。

■ その役割を担う人材の例

情報セキュリティ強化対応スキル指標から

情報セキュリティ強化対応スキル指標では、**情報セキュリティ戦略に基づく具体的なルールや基準を策定する役割**として、以下のような人材を示しています。これらの役割を担う場合は、ルールや基準の策定に加えて、その実施の徹底やルールの見直しなどの役割をあわせて担うことが重要です。

自社向け

セキュリティアドミニストレータ
（ISｾｷｭﾘﾃｨｱﾄﾞﾐﾆｽﾄﾚｰﾀ）

情報セキュリティ戦略やポリシーを具体的なルールや計画に落とし込み、その実行（ないしは実行の指示）のほか、維持・管理や見直しを行う役割。また、インシデント対応に備えて**日頃のマネジメントや教育等の実施**も担当する。

顧客向け

コンサルタント
（情報リスクマネジメント）

ビジネス機能内で**情報マネジメントが適切に実現される土台としての組織体制の整備や組織内の各種ルール整備等に関する支援を担う役割**。組織ガバナンスやリスクマネジメント、コンプライアンス等に関する領域において、ITソリューションを前提としたコンサルティングを行う。

情報セキュリティ強化対応スキル指標のご紹介

「**iコンピテンシ・ディクショナリ**」とは、ITスキル標準（ITSS）や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３つのスキル標準を包含する形で整理した、タスクとスキルのデータのことです。この iコンピテンシ・ディクショナリを参照することで、３つの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・ディクショナリを活用した**「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）。

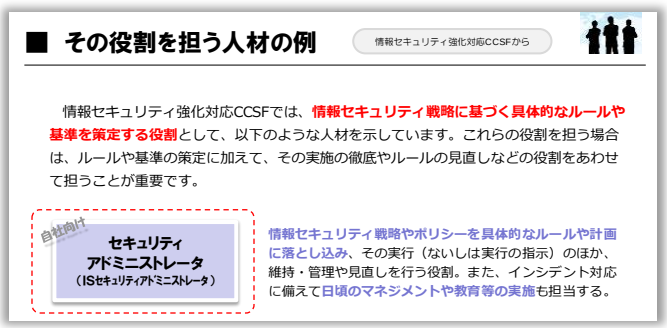
これは、情報セキュリティを担う人材としてITベンダー企業とユーザー企業に必要な役割定義を例示し、役割ごとに想定される業務（タスク）とそれに必要なスキルを対応づけて紹介したものです。

ここでは、「情報セキュリティ強化対応スキル指標」の参照方法を紹介しています。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のダウンロード（独立行政法人情報処理推進機構（IPA））**
http://www.ipa.go.jp/jinzai/hrd/security/

情報セキュリティ強化対応スキル指標の参照のしかた

「情報セキュリティ強化対応スキル指標」を活用すると、本ガイドで紹介した人材が担うべき具体的な業務などを確認することができます。


■ その役割を担う人材の例

情報セキュリティ強化対応CCSFから

情報セキュリティ強化対応CCSFでは、**情報セキュリティ戦略に基づく具体的なルールや基準を策定する役割**として、以下のような人材を示しています。これらの役割を担う場合は、ルールや基準の策定に加えて、その実施の徹底やルールの見直しなどの役割をあわせて担うことが重要です。

自社向け

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）

情報セキュリティ戦略やポリシーを具体的なルールや計画に落とし込み、その実行（ないしは実行の指示）のほか、維持・管理や見直しを行う役割。また、インシデント対応に備えて**日頃のマネジメントや教育等の実施**も担当する。

例えば、本ガイドのp.19には、自社の情報セキュリティに関する方針や基準を策定する役割を担う人材として「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）」が紹介されています。

「情報セキュリティ強化対応スキル指標」を見ると、「職種シート」に、「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）」の定義が記述されており、その人材の**ミッションや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）。

職種コード	出自	職種	専門分野	解説
HS-040-010	情報セキュリティ人材	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	【ミッション】 全社の情報資産へのセキュリティにおける社内外からの脅威やリスクへの対応に責任を持ち、特にIS戦略と情報セキュリティ戦略との相互連携を図る。情報セキュリティ戦略やポリシーを企画・計画に落とし込み、実装（ないしはその指示）・提供・維持・管理を行う。 【活動内容】 セキュリティの活動領域として以下を実施する。 ● IT基盤構築・維持・管理 ・品質統制フレームワークの運営　（各プロジェクトに対するガバナンスの実施） ・ IS導入計画の策定 ●セキュリティ ・セキュリティ基準の策定 ・セキュリティ事故と対応の分析 ・セキュリティ対応の見直し ※平成24年度に「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）によって検討されたスキル標準等の見直し案の方針を受けて作成した UISS視点の人材モデル。

「タスクプロフィール×タスク対応表」には「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）」のタスクが定義されており、**具体的な業務内容（タスクレベル）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）	ITアーキテクト（セキュリティアーキテクチャ）	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）	IS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）	インテグレーション（インテグレーション）	セキュリティマネージャ（統括管理セキュリティ）	ITスペシャリスト（セキュリティ）
						D-030-01	D-030-02	D-030-03	D-030-04	D-030-05	D-030-06	D-030-07
PL-020	システム企画立案	PL-020-020	システム化計画の策定	PL-020-020-080	サービスレベルと品質に対する基本方針の明確化		◎		◎		○	
				PL-020-020-020	システム要件の定義		◎		◎		○	
		DV-140-020	プロジェクト計画策定	DV-140-020-090	品質保証計画の策定				○		◎	
				DV-140-020-100	リスク管理計画の策定				○		◎	
				DV-140-030-110	品質管理				○		◎	
				DV-140-030-120	リスク管理				○		◎	
		US-020-020	情報セキュリティ管理	US-020-020-010	情報セキュリティの運用				○	◎		○
				US-020-020-020	情報セキュリティの評価と検証				○			○
MC-020	情報セキュリティマネジメント	MC-020-010	情報セキュリティ戦略と方針の策定	MC-020-010-010	基本戦略の策定	◎		◎	◎		○	
				MC-020-010-020	情報資産の評価	○		◎	◎		○	○
				MC-020-010-030	脅威とリスクの識別	○		◎	◎		○	○
				MC-020-010-040	リスクの評価	○		◎	◎		○	○
				MC-020-010-050	セキュリティポリシーの策定	○		◎	◎		○	○
		MC-020-020	情報セキュリティの運用	MC-020-020-010	情報セキュリティガバナンス	○			◎		○	○
				MC-020-020-020	情報セキュリティの周知と教育	○			◎		○	○
		MC-020-030	情報セキュリティの見直し	MC-020-030-010	情報の収集と評価	○			◎		○	○
				MC-020-030-020	運用上の問題点整理と分析	○			◎		○	○
				MC-020-030-030	技術上の問題点整理と分析	○	◎		◎		○	○
				MC-020-030-040	新たなリスクの整理と分析	○			◎		○	○
				MC-020-030-050	セキュリティポリシーの更新	○			◎		○	○
MC-030	品質マネジメント	MC-030-010	品質管理のコントロール	MC-030-010-010	品質マネジメントシステムの運用		◎		◎		○	
				MC-030-010-020	品質標準および品質管理実践基準の定義		◎		○		○	
				MC-030-010-030	品質の測定、モニタリングおよび改善		◎		○		○	

また、「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詳しく定義されており、育成の参考にすることができます**。

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	ITSS	情報セキュリティ人材						
				ITスペシャリスト	コンサルタント	ITアーキテクト	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	インテグレータ	セキュリティマネージャ	セキュリティオペレーション
				セキュリティ	情報セキュリティマネジメントシステム	セキュリティアーキテクチャ	情報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	インテグレーション	統括セキュリティマネジメント	統括セキュリティオペレーション
				HI-060-060	HS-010-010	HS-020-010	HS-030-010	HS-040-010	HS-050-010	HS-060-010	
S110060010	メソドロジ	（戦略）　システム戦略立案手法	システム化戦略手法		◎	◎		◎			
S110060020			システム活用促進・評価		◎	◎		◎			
S110060030			ソリューションビジネス		◎			◎			
S110060040			業務プロセス		◎			◎			
S110060050			現行システムの調査・分析手法		◎			◎			
S110060060			事業戦略の把握・分析の手法		◎			◎			
S110060070			情報システム戦略		◎	◎		◎			
S120010020		（企画）　システム企画立案手法	システム企画立案手法		◎	◎		◎			
S120010030			ソリューション提案手法					◎			
S120020020			契約事務手法					◎			
S130100090			プロジェクト資源マネジメント					◎			
S150010040			品質マネジメント手法	◎		◎		◎			
S150010050			品質マネジメントシステム構築手法			◎		◎			
S150010090			品質保証に関する手法	◎		◎		◎			
S150030010		（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		◎	◎	◎	◎			
S220010010		（開発）　システムアーキテクティング技術	システム要件定義	◎	◎	◎		◎			◎
S220010020			システムインテグレーションとアーキテクチャ			◎		◎			

さらに、「職種×タスク×スキル表」で、それぞれの情報セキュリティ職種・専門分野について、タスク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。各社のタスク経験調査やスキルの保留量調査、また職務定義書等にも利用することができます。

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定義をしたい場合は、オリジナルの「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。

情報セキュリティ強化対応スキル指標に定義されている職種の紹介

ITアーキテクト
（セキュリティアーキテクチャ）

「情報セキュリティ強化対応スキル指標」に集約されているタスク・スキルの情報から、情報セキュリティを担う人材のイメージをつかむことができます。例えば下表は、情報セキュリティ強化対応スキル指標の「ITアーキテクト（セキュリティアーキテクチャ）」のタスクやスキルを抜粋して、“職務定義書”のような形でまとめたものです。この専門分野は、強固なセキュリティ対策が求められる情報システムのアーキテクチャ設計のほか、情報セキュリティ対策が十分に機能し、維持されることを担保する組織設計、ルール設計、プロセス設計を担う役割として定義されていますが、情報セキュリティ強化対応スキル指標を活用することで、その職務を具体的に把握することができます。

職種	職務の内容（例）				
ITアーキテクト（セキュリティアーキテクチャ）	システム設計を担うITアーキテクトのうち、強固なセキュリティ対策が求められるITアーキテクチャの設計を担う専門分野。 ビジネスおよびIT上の課題を分析し、セキュリティ要件として再構成する。システム属性、仕様を明らかにし、情報システムの安全性や信頼性をセキュリティ面から実現する				
タスク大分類	タスク中分類	タスク小分類	スキルカテゴリ	スキル分類	スキル項目
システム企画立案	システム化計画の策定	サービスレベルと品質に対する基本方針の明確化	メソドロジ	（戦略） システム戦略立案手法	システム化戦略手法
					情報システム戦略
				（企画） システム企画立案手法	システム企画立案手法
			テクノロジ	（開発） システムアーキテクティング技術	システムインテグレーションとアーキテクチャ
	業務・システム要件定義	システム要件の定義	メソドロジ	（戦略） システム戦略立案手法	システム化戦略手法
					システム活用促進・評価
					情報システム戦略
				（企画） システム企画立案手法	システム企画立案手法
			テクノロジ	（開発） システムアーキテクティング技術	システム要件定義
	情報セキュリティ要件定義	情報セキュリティ要件の定義	メソドロジ	（戦略） システム戦略立案手法	システム化戦略手法
					システム活用促進・評価
					情報システム戦略
				（企画） システム企画立案手法	システム企画立案手法
			テクノロジ	（開発） システムアーキテクティング技術	システム要件定義
システム要件定義・方式設計	システム化要件定義	要求事項の調査と分析	メソドロジ	（企画） 要求分析手法	要求の抽出手法
					要求の整理手法
					要求の仕様化手法
					要求の評価手法
					要件定義
				（企画） 非機能要件設定手法	プラットフォーム要件定義手法
			テクノロジ	（開発） システムアーキテクティング技術	システム要件定義
					システムインテグレーションとアーキテクチャ
					アプリケーション共通基盤要件定義手法
					IT基盤構築プロセス
				（非機能要件） 非機能要件（可用性、性能・拡張性）	非機能要件の基礎
		非機能要件の定義	メソドロジ	（企画） 要求分析手法	要求の抽出手法
					要求の整理手法
					要求の仕様化手法
					要求の評価手法
					要件定義
				（企画） 非機能要件設定手法	プラットフォーム要件定義手法
			テクノロジ	（開発） システムアーキテクティング技術	システム要件定義
					システムインテグレーションとアーキテクチャ
					アプリケーション共通基盤要件定義手法
					IT基盤構築プロセス
				（非機能要件） 非機能要件（可用性、性能・拡張性）	非機能要件の基礎
					システム信頼性、性能設計
	システム方式設計	適用製品・技術の評価と選定	メソドロジ	（実装） アーキテクチャ設計手法	アーキテクチャ設計手法
					アプリケーションアーキテクチャ設計手法
					インダストリパッケージ設計・開発手法
					インフラストラクチャアーキテクチャ設計手法
					データアーキテクチャ設計手法
			テクノロジ	（開発） システムアーキテクティング技術	システム要件定義
					システムインテグレーションとアーキテクチャ
					アプリケーション共通基盤要件定義手法
					アプリケーション共通基盤設計手法
					IT基盤構築プロセス
					システム間連携技術
					システム方式設計
					オブジェクト指向技術
				（組込み・計測・制御） ヒューマンインターフェース技術	インタフェース設計
基盤システム構築	基盤システム設計（情報セキュリティ）	セキュリティの設計	メソドロジ	（実装） アーキテクチャ設計手法	アーキテクチャ設計手法
			テクノロジ	（非機能要件） セキュリティの基礎技術	情報セキュリティ
					情報保証と情報セキュリティ
					情報倫理とセキュリティ
					セキュリティ・アーキテクチャ技術
					アプリケーションセキュリティ
					情報プラットフォームのセキュリティ技術
					ネットワークのセキュリティリスク
					暗号技術
					セキュリティと個人情報
					保証、信用、信頼のメカニズム
					セキュリティ技術の理解と活用

情報セキュリティを担う人材育成のヒント

情報セキュリティを担う人材は、企業にとって、近年ますます重要性を増しています。しかし、情報セキュリティの領域は高い専門性を必要とすることも多く、それを担う人材の育成には課題も多いのが現状です。こうした現状を踏まえて、ここでは、本調査の結果から、情報セキュリティを担う人材の育成に関するヒントをご紹介します。

■ 情報セキュリティを担う人材の育成についての悩み

情報セキュリティを担う人材は、ユーザー企業・ITベンダー企業の双方にとって重要です。自社の情報を護るという観点では、ユーザー企業もITベンダー企業も同じ課題を抱えているといえます。

また、情報セキュリティに関する高い専門性を持ったスペシャリストを育成するという観点で考えると、ITベンダーやセキュリティベンダーが主な対象となります。

上のような、自社の情報を護る「自社の情報セキュリティ対策」と、高い専門性を持ち、顧客に対してセキュリティサービスを提供することもある「情報セキュリティを担う専門人材の育成」という２つの観点から、人材に関する主な課題を整理すると、例えば以下のような課題があげられます。

自社の情報セキュリティ対策

- ✓ 現場が情報セキュリティの重要性を理解してくれない。
- ✓ 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、企業全体としての対策が進まない。
- ✓ 情報セキュリティ担当者のスキルアップが難しい。

情報セキュリティを担う専門人材の育成

- ✓ 専門性の高い人材の育成方法が分からない。
- ✓ 専門性は高いが、スキルの幅が広がらない。
- ✓ 専門性は高いが、ビジネスマインドが身につかない。

■ こんな取り組み例があります！

前ページのような悩みに対して、本調査では、有識者WGにおけ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を収集しました。企業によって、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ない場合もあるとは思いますが、情報セキュリティを担う人材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。

自社対策

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、全社的な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担当者を置いた**ことで、セキュリティに対する意識が全社的に向上した。

自社対策

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、企業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。

自社対策

（特にユーザー企業では）情報セキュリティ担当者のスキルアップが難しい。

ユーザー企業には、専任の情報セキュリティ担当者は少なく、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。

ユーザー企業では、情報セキュリティ担当者も、**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。

専門人材

情報セキュリティに関する専門性の高い人材の育成方法が分からない。＜研修方法＞

緊急時にスムーズに対応できるように**セキュリティインシデント（セキュリティに関する事故等）の模擬訓練**を取り入れている。模擬訓練ではあるが、緊張感を持って行えば効果は高い。

スキルアップを目的として、スキルの高いメンバーによる組織の枠を超えたチームを作り、**CTF（Capture the Flag）**に参加している。

ネットワーク運用部門と共同で、**ネットワークフォレンジックが体験できる環境**を用意し、社内研修を実施している。

専門人材

情報セキュリティに関する専門性の高い人材の育成方法が分からない。＜育成制度＞

ハイレベルの人材は、その分野に強い興味があるため、自発的に技術を学ぶ。そのため、教育よりも、**自発的な取り組みを阻害しない環境**を整備したり、興味のある者同士でコミュニケーションを行うための**コミュニティづくりなどの支援**を行うことが重要である。

ハイレベルのセキュリティ技術者は、様々な部署に点在して配置されるため孤立しやすい。**セキュリティ技術者間の連携を促進する**ことも課題である。

セキュリティを担当する人材は、開発業務に携わる人材などとは異なる指標で評価する必要がある。このため、**セキュリティを担当する人材については、従来とは別の評価・認定の仕組みが必要である**と考えている。

専門人材

情報セキュリティに関する専門性は高いが、スキルの幅が広がらない。

情報セキュリティの分野でのキャリアアップを希望する場合も、ある程度のスキルの幅は必要である。そのため、スキルの幅を広げることに関心がない人材に対しても、**様々な経験をさせる機会を与える**ようにしている。

専門人材

情報セキュリティに関する専門性は高いが、ビジネスマインドが身につかない。

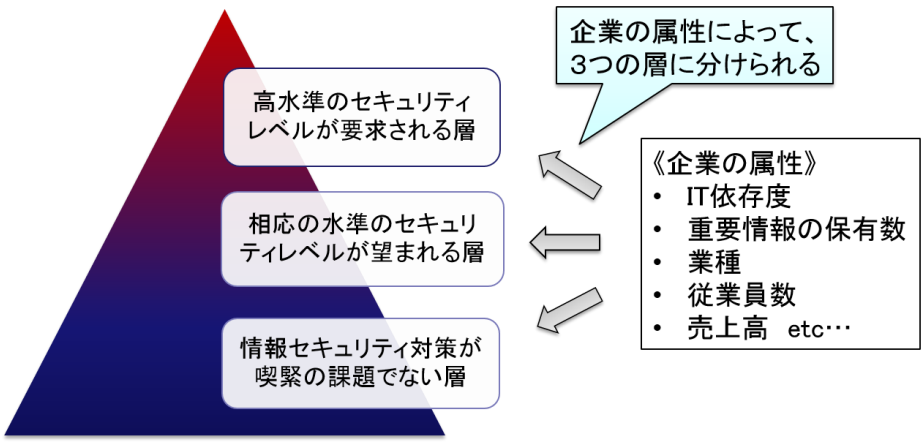
IT企業としては、情報セキュリティの専門性を活かして、**最終的にはビジネスを創造できるような人材に育ってほしい**という思いがある。専門性が高い人材に対しては、新しい事業を創出するように促したり、それまでに培った**ノウハウを現場で活かすために他部門に配属する**などの取り組みを行っている。

ご参考

組織において求められる情報セキュリティ対策のレベル

企業によって、ITへの依存度や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ります。そのため、周囲の企業が行っている情報セキュリティ対策は参考にはなりますが、自社の状況に基づいて判断することが求められます。こうした判断の際には、**情報セキュリティリスク指標**などが活用できます。

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システムの実施状況を自らが評価する**「情報セキュリティ対策ベンチマーク」の中で示されている企業が抱えるリスクを表す指標**です。企業はこの指標によって、３つの層に分けられます。



情報セキュリティリスク指標

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、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が関連しているものを使っていれば、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ありませんので、この点には注意が必要です。

このように、企業は**自社の属性に合った情報セキュリティ対策のレベルを見極めていく**必要があります。

■ 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（IPA））
https://www.ipa.go.jp/security/benchmark/

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

情報セキュリティ上の脅威から企業を護るための人材育成ガイド

2014年8月発行
2015年5月改訂

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

本冊子は、「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」の成果として作成されたものです。


IPA