

情報セキュリティ対策ベンチマーク

1. 概要

企業等の組織は、適正と考える水準、すなわち株主、消費者、取引先のみならず社会全体から「望まれる水準」において情報セキュリティに取り組むことが求められている。しかし、その水準は一律ではなく、企業の業態や保有する情報資産等の属性によって異なると考えられる。現在、独立行政法人 情報処理推進機構で公開されている「情報セキュリティ対策ベンチマーク」¹は、これらの属性をもとに企業等の組織を分類し、それぞれのグループに対して「望まれる水準」と現状を比較できる自己診断ツールである。

情報セキュリティ対策ベンチマークの評価項目は、対策の取組状況を把握するための評価項目（25項目）と、組織プロフィールに関する評価項目（15項目）で構成される。対策ベンチマークのシステムは、組織プロフィールに基づき回答機関を分類した上で、該当するグループにおいて「望まれる水準」を設定する。この「望まれる水準」とは、企業アンケート等のデータから、グループごとに導出したものである。

また、対策の取組状況を把握するための評価項目に対する回答値から、回答機関のトータルスコアを算出し、回答企業的水準をレーダーチャート等で表示する（図1参照）。これは、回答機関の水準と望まれる水準を同時に提示し、その差分を可視化することにより、各機関が優先的に取り組むべき項目を明確にするためである。さらに、推奨される取組も併せて提示することにより、具体的な改善策実施へとつながるように促す。

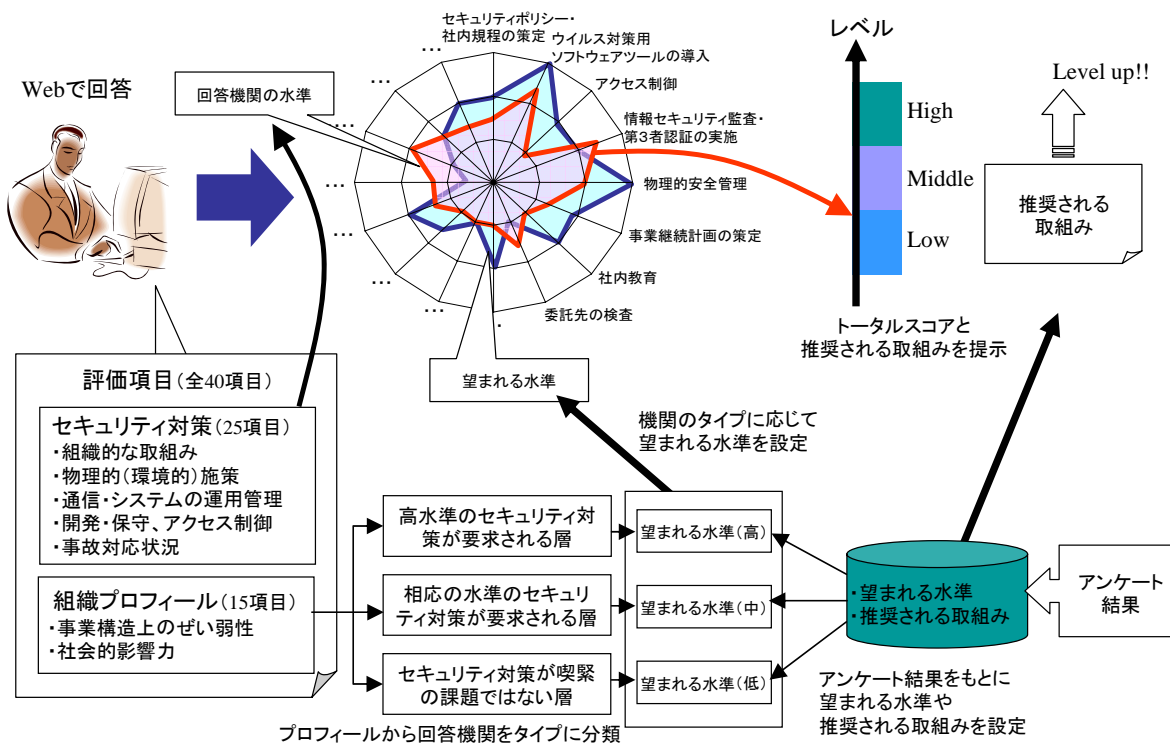


図 1 情報セキュリティ対策ベンチマークのイメージ

¹ <http://www.ipa.go.jp/security/benchmark/index.html>

2. 位置付け

情報セキュリティ対策ベンチマークの目的として、情報セキュリティ対策を実施していない、あるいは簡易な対策しか行っていない企業に対し、セルフチェックを通じて情報セキュリティの取組を活性化させることを想定しているが、こういった企業は、中堅・中小企業が中心になると思われる。このため、中堅・中小企業における利活用を促進すべく、可能な限り評価項目の数を抑えている。なお、アンケート結果によれば、大企業にも、一部取組が十分でない項目があることが判明していることから、中堅・中小企業のみならず、大企業も本ベンチマークを積極的に活用することが重要である。

また、第三者認証制度を始めとする高次のレベルを目指して向上していくことも重要であることから、ISMS 適合性評価制度²や情報セキュリティ監査との整合性に配慮することが望ましい。そこで、情報セキュリティ対策ベンチマークの評価項目は、まず ISMS 認証基準 (Ver.2.0) の詳細管理策³をベースに策定された。さらに、その後規格化された JIS Q 27001:2006 の付属書 A 管理目的及び管理策に基づき、専門家の WG によって評価項目の見直しを実施した。なお、見直しに当たっては、継続性や既存のデータ資産との整合性、平易な言葉の使用と曖昧な表現の排除、企業内の部門単位の利用や公的機関の利用への対応等に配慮した。

なお、情報セキュリティガバナンスの確立という観点からすれば、情報セキュリティの実務担当者ではなく、経営層の担当責任者がセルフチェックを通じて対策の必要性に気づくことが望ましい。このため、経営層向けに平易な言葉を使用するとともに、単に対策を「行っている」/「行っていない」ではなく、ガバナンスの観点から見た対策の取組方(成熟度)を評価の基準としている。

3. 想定される効果

①経営層に対する目標の明確化と意識の啓発

自社の情報セキュリティの水準に不安を抱く機関の経営層が、本ベンチマークに基づくセルフチェックを通じて自社の現状と望まれる水準との差を把握し、目標を明確に理解することができる。組織にとっては、自らと同じタイプのグループの取組状況に基づく指標が示されるため、実際の対策を検討する上で有用である。また、経営層が自らセルフチェックを行うことにより、自身に求められる役割を発見し、組織としての取組のあるべき姿を理解するという啓発効果も期待できる。

②共通の尺度によるグループ内統制の実現

企業が株式の持ち合いや子会社・関連会社などと企業群を形成して事業活動を行っている場合、社会からはグループ全体としての一共同体とみなされるため、中核企業はグルー

² 財団法人日本情報処理開発協会 (JIPDEC) が運営する、情報セキュリティ対策に関する国内での第三者評価制度 (<http://www.isms.jipdec.jp/>)。2006年7月からは財団法人日本適合性認定協会 (JAB) でも、審査登録機関の認定申請の受付を開始している。

³ ISMS 評価基準の付属書であり、JIS X 5080:2002 (国際標準 ISO/IEC 17799:2000) を参照して ISMS 構築に必要なセキュリティ対策を定義している。ISMS 評価基準では、詳細管理策から適切な管理目的及び管理策を選択することを求めている。

②組織プロフィール

組織プロフィールについては、一般的な属性に加え、事業構造上のぜい弱性や社会的影響力に着目する形で構成した。なお、企業内の部門単位で利用する場合も、従業員数や拠点数、売上など、基本的に企業の単位で回答する。また、公的機関が利用する場合、企業の用語は適宜対応する言葉に置き換えて回答するものとする。

- (a) 従業員数（派遣、アルバイトを含む）及びそのうちの正規職員の割合
- (b) 売上高、国内外の拠点数（支社・支店・営業所）
（公的機関の場合は予算、国内外の拠点数を回答）
- (c) 業種
- (d) 国家や社会基盤、経済基盤に与える影響の観点から見た公益性
- (e) 事業が、顧客の生命・身体・財産・名誉等に与える影響の大きさ
- (f) 主要な業務に関わる業務プロセスのうち、情報システム（外部のシステムを含む）に依存している割合
- (g) 主要な業務に関わる業務プロセスのうち、インターネットに依存している割合
- (h) 主要な情報システムについて、（月間）売上高に影響を及ぼさないで済む許容停止時間
（公的機関の場合は、主要業務に影響を及ぼさないで済む許容停止時間を回答）
- (i) 主要な情報システムが営業日に「24 時間」停止した場合の、当該日の売上高への影響
（公的機関の場合は、影響無しと回答）
- (j) 情報セキュリティ関連の事故が発生した場合のブランド（企業イメージ）への影響
- (k) 元請や代理店、フランチャイジー等のビジネスパートナーへの依存度
- (l) 重要情報（国家機密、営業機密、プライバシー情報等）の保有、管理または使用状況
- (m) 個人情報の取扱量
- (n) 離職率（直近の1年間に退職・転職された従業員の割合）
- (o) 事業活動に影響を与えるような情報セキュリティ関連の事故の発生経験

(2) 機関分類

機関分類に際しては、組織プロフィールから「事業構造上のぜい弱性」と「社会的影響力」の2つを分類軸として算出⁴し、それらに基づいて分類する。

[分類軸1] 社会的影響力

組織の価値、社会的責任、保有する情報資産の性質などをもって IT 事故が発生した場合に社会に与える影響度の高さを評価するもの。組織の価値とは、売上規模やブランドイメージに対して IT 事故が及ぼす影響の大きさを指す。社会的責任とは、事業の公益性（国家、社会、経済等）や、IT 事故が発生した場合の消費者への影響度（生命・身体・財産・

⁴ 組織プロフィールの内容から「事業構造上の脆弱性」、「社会的影響力」を算出する計算式は、「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」（2005年3月）で実施された企業アンケートの結果を統計的に分析して設定されたもの。

名誉等)の高さを指す。情報資産とは、重要情報の保有量(国家機密、営業機密、プライバシー等)を指す。IT事故が発生した場合の社会的影響の大きい企業ほど、社会的責任の観点からも高いレベルの対策が必要であると考えられる。

〔分類軸2〕事業構造上の脆弱性

事業の情報システム依存、業務の外部依存性、関与者の範囲などをもって、自社が抱える事業構造上のぜい弱性の高さを評価するもの。事業の情報システム依存とは、業種特性や基幹業務の情報システム依存度を指す。業務の外部依存性とは、代理店等への依存度、インターネットへの依存度、正社員・非正社員の比率を指す。関与者の範囲とは、拠点数、海外拠点の有無、従業員の離職率を指す。これらの数値が高いほどIT事故に対してぜい弱である(統制が困難でIT事故が発生しやすい、もしくはIT事故が深刻化する可能性がある)と考えられ、リスクマネジメントの観点からも高いレベルの対策が必要であると考えられる。

具体的には、「事業構造上のぜい弱性」、「社会的影響力」のいずれの値も高い層を「高水準のセキュリティレベルが要求される層」、いずれかの値が高い層を「相応の水準のセキュリティレベルが望まれる層」、いずれの値も低い層を「情報セキュリティ対策が喫緊の課題でない層」として、3グループに分類する。

①高水準のセキュリティレベルが要求される層

事業構造上のぜい弱性が高く、かつIT事故が発生した場合の社会的影響が大きい機関にとっては、高水準のセキュリティレベルが要求される。例えば、IT依存度が高く、かつ大量の個人情報を取り扱う金融・保険業や情報サービス、また広範なサプライチェーンマネジメントを構築している大手製造業等が該当する。

②相応の水準のセキュリティレベルが望まれる層

事業構造上のぜい弱性もしくは社会的影響力のいずれか一方だけが高い機関には、IT事故の社会的影響は小さいが発生もしくは深刻化する可能性があるタイプと、IT事故が発生しやすいわけではないが、発生すると社会的影響が大きいタイプがあり、いずれも①ほどではないが、相応な水準でのセキュリティ対策が望まれる。例えば、多数の顧客情報を抱える卸売・小売業や、拠点数の多い大手建設業等が該当する。いずれの場合も、情報セキュリティ対策ベンチマークを活用するなどして自社の状況を分析し、望まれる水準に応じた対策に取り組む必要がある。

③情報セキュリティ対策が喫緊の課題でない層

事業構造上のぜい弱性と社会的影響力のいずれも高くない機関にとっては、情報セキュリティ対策が喫緊の課題ではない。例えば、中小の建設業や製造業、卸売・小売業等が該当する。ただし、これらの機関も、ネットワーク社会の一員として最低限の対策を講じる必要があり、情報セキュリティ対策ベンチマークを活用するなどして望まれる水準に応じた対策の実施が望まれる。

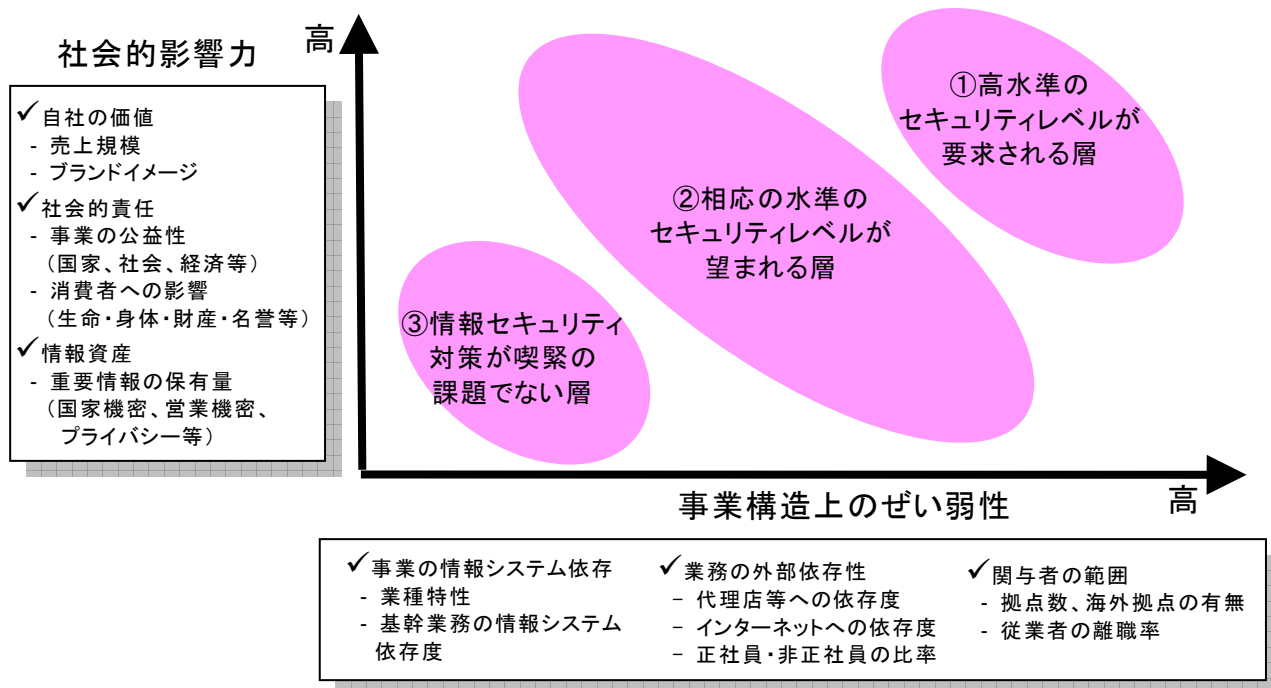


図 3 要求される情報セキュリティの水準に基づく分類

(3) 推奨される取組

Web ツールによるセルフチェックの結果は、その目的により、「経営者向けのエグゼクティブサマリ」と「実務者向けのアドバイス」の2通りに分けて提示する形を想定する。

前者については、経営層の理解とトップダウンの対策実施を目指し、可視化された比較表や偏差値などを用いて説明する。また、後者については、「対策のポイント」や「解説」を提示する。

(4) 評価項目の改訂案

JIS Q 27001:2006 の付属書 A 管理目的及び管理策に基づき、専門家の WG がとりまとめた評価項目の改訂案を以下に示す。

<p>大項目 1. 情報セキュリティに対する組織的な取組状況</p>
<p>①情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。 (ポリシーや規程は、サンプルのコピーではなく、自組織の事業やリスクを鑑みた内容であることが重要です。また、そうしたポリシーや規程を実践するためには、定めた規程類を関係者に十分に周知させると共に、規程類の順守状況を点検し、必要に応じて見直すことが大切です。)</p>
<p>説明 ポリシーや規程を組織にとって有効なものとするためには、自組織の状況に見合った内容にする必要があります。そのためには、サンプルのコピーではなく、自組織の事業やリスクを鑑みた内容とすることが重要です。また、対策の実効性を確保するためには、定めた規程類を役員や全従業員に対して十分に周知すると共に、規程類の順守状況を適宜点検し、必要に応じて見直すことが大切です。</p>
<p>対策のポイント</p> <ul style="list-style-type: none"> ●情報セキュリティポリシーや管理規程が策定されているか ●ひな形、サンプルなどのコピーではなく、組織内での十分な討議や検討を経て、自組織の事業やリスクに見合った内容となっているか ●ポリシーは全組織をカバーしているか ●組織の長ないし上級役員が承認しているか ●全従業員（派遣を含む）や関連する外部関係者に対して周知させているか ●定期的に見直すための手続を定めているか ●あらかじめ定められた間隔、または重大な変化が発生した場合に、見直しを実施したか ●改訂結果について、組織の長ないし上級役員の承認を得て、再度周知したか ●従業員がポリシーや関連規程類を順守していることを点検・監査するための手続を定めているか ●組織内の情報セキュリティ対策や情報システムに関する点検や監査の実施を推進しているか ●情報システムが、業務以外の目的で利用されることを防止するための措置を講じているか ●情報システムに対し、いわゆるネットワーク検査やモニタリングを行うなどして、ポリシーの実施状況を確認しているか
<p>解説</p> <p>効果的な情報セキュリティ対策を実現するためには、情報セキュリティに関するポリシーや関連する諸規程を定めて組織内部における統制の方針や手順などを明らかにし、それを確実に実践することが重要です。</p> <p>そうしたポリシーや関連する諸規程を定めるに当たっては、ひな型やサンプルあるいは他組織の事例などをコピーし、会社名や組織名あるいは役職名などを単純に置き換えるだけでは、自組織に合った効果的な統制を実現することが難しい場合があります。なぜなら、統制のあり方は、組織によってそれぞれ異なるからです。組織の実状に沿ったポリシーや規程類を策定するためには、内部での十分な討議を経て、自組織の業務や組織体制との整合を図っていくことが重要です。</p> <p>また、組織内カンパニー制を採用して、各部署が独立性を持って事業を営んでいる場合など、特殊なケースを除いて、一般的には組織全体で共通のポリシーとした方が良いでしょう。一緒に仕事をする複数の部署で、それぞれに考え方の異なるポリシーを定めているようだと、情報セキュリティの実現は難しくなります。</p> <p>そのこととも関連しますが、情報セキュリティポリシーを正しく実践するためには、会社で言えば社長や上級の役員が、ポリシーの策定に関与し、その実現に自ら責任を持つことが重要です。さもなければ、必要なリソースを投入することや、組織全体として必要な約束事を実践することが難しくなります。</p> <p>ポリシーや規程類を策定したならば、それを関連する従業員（派遣を含む）や外部関係者全員に対して周知、徹底する必要があります。関連する従業員が認知していないポリシーや規程類は、「絵に描いた餅」に過ぎません。加えて、情報セキュリティに関連する事故は、一人の不注意や怠慢から発生し、大きく広がることもあるのです。</p> <p>また、ポリシーや諸規程は、一度定めたら終わりで未来永劫使い続けられるとは限りません。一般の規程などでもそうですが、関連する法令が変わったり、情報システムに関連する技術が変化したりといった周りの環境の変化に追従していかなければ、せっかく作ったポリシーや諸規程も形骸化してしまいます。特に情報技術の進展はめざましく、1年も経てば情報システムを取り巻く脅威に大きな変化が起こっているかも知れません。こうした変化に対応するためには、ポリシーや諸規程類を定期的に見直すことが必要ですので、見直し自体を規定として定めておき、組織の義務として確実に実施することが望まれます。</p> <p>既に策定済みのポリシーや規程類については、見直しが必要となっていないか、定期的な見直しが確実に実施されるような規定が含まれているかを確認してください。また、企業合併や組織再編、法改正、事故といった、管理上大きな変化があった場合にも、その都度見直しが実施されるような規定が含まれていることが望まれます。</p> <p>そうした規定に沿って改訂を実施した結果についても、最初のポリシーや規程類の策定時点と同様に、やはり組織の長や上級役員の承認を得ること、従業員に再度周知、徹底することが重要です。</p>

さらに、従業員によるポリシーや関連規程類の順守を確認することにより、ポリシーや規程を実効的なものとすることも重要です。たとえば、インターネット上の掲示板への不適切な書込みや、業務とは無関係の Web サイトからのスパイウェアなどの不正なプログラムダウンロードを防止するため、従業員が組織の PC を業務以外の用途に使用することがないようにポリシーや規程で明示しておくことが望めます。その場合、ポリシーや規程類に則って、組織内の情報セキュリティ対策の実施状況や情報システムの設定・管理などについて点検や監査を行うこと、また、情報システムに対していわゆるネットワーク検査やモニタリングを実施することで、ポリシーの実施状況を確認しておくといよいでしょう。なお、情報システムを監査するツールは悪用されると危険であることから、開発及び運用システムとは分離し、権限のない従業員には触れさせないようにしておくことが望めます。

(丁)

②経営層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか。

（推進体制を整備するためには、経営層がリーダーシップを発揮すること、各担当者の権限と責任を明文化することなどが重要です。また、法令順守のためには、順守すべき法令を正確かつ網羅的に把握することが必要です。）

説明 推進体制を整備するためには、経営層がリーダーシップを発揮すること、各部署の活動を調整する組織を整備すること、各担当者の権限と責任を明文化することなどが重要です。また、法令順守のためには、順守すべき法令などを正確かつ網羅的に把握することが必要です。さらに、組織の活動に関する説明責任を果たすため、種々の活動に関する記録を残すと共に、特に法令などによって保存が求められる文書については、記録を適切に保護することが求められます。

対策のポイント

- 組織内の情報セキュリティのあり方を決定したり、各部署の活動を調整したりする組織が整備されているか
- その組織の責任者は経営層の人間が担当しているか
- その組織において、情報セキュリティに関する適切な責任や資源配分を検討しているか
- 単独行動による不正行為をけん制するため、職務や権限を適切に分離しているか
- 関係当局や情報セキュリティの専門家との連絡体制を構築しているか
- 事業を遂行する上で順守すべき法令、基準、規制などを網羅的に、かつ正確に把握しているか
- 他者の知的財産権を保護するための手続を定め、それを実践しているか（たとえば、ソフトウェアの不正コピーを予防するための手当てなど）
- 個人情報保護のために必要な対策を定め、それらを実施しているか
- 不正競争防止法で保護される情報の要件を把握しているか
- 自組織が実施した様々な活動について、それらを記録する仕組みはあるか
- 特に法定の保存文書について、厳格な管理を実施しているか

解説

実効的な情報セキュリティ対策の推進には、組織全体としての取組が必要です。そのためには、経営層のリーダーシップと各組織のセキュリティ上の責任が明確化されている必要があります。また、企業などの情報セキュリティのあり方を決定する組織や各部署の活動を調整する組織を設置し、監査やコンプライアンスの実践といった役割を持たせることが必要です。

情報セキュリティのあり方を決定する組織の責任者は、経営層の中から任命することが望めます。なぜなら、情報セキュリティは、その組織の経営方針やビジネスプロセスなどと密接に関わるものだからです。情報セキュリティは、保有する情報資産や業務に不可欠な情報システム、情報セキュリティ上の事故が発生した場合の業務への影響などのファクターを考慮しながら推進すべきであり、そのためには、情報セキュリティ担当の責任者は、情報セキュリティと経営の両方に目配りができる立場にすることが重要です。

情報セキュリティ対策の推進に当たって、情報セキュリティ担当責任者は、まず、必要なリソースを、その組織の情報セキュリティ上のニーズやプライオリティに応じて分配するという役割を担う必要があります。リソースの分配とは具体的には、予算の配分であったり、人的リソースの配分であったりということになります。情報セキュリティ上プライオリティの高い項目にはより多くのスタッフと予算を割り当てて、優先的に実施することになります。さらに、必要に応じて個々の対策を推進する責任者を任命してもよいでしょう。

職務や権限を一人に集中させると不正行為を招きやすい状況に陥ることがあるので、これをけん制するため、職務や権限を適切に分散させることが重要です。

事業を遂行する上で順守すべき法令、基準、規制などを網羅的に把握しておくことは組織として当然のことですが、情報技術の変化は年々早くなっており、それに伴って、法律や規制が新たに制定される、修正が加えられる頻度も増していくことが予想されます。したがって、事業に関わる法律や規制についての定期的な情報収集とその業務への影響の分析、順守するための取組の徹底が求められています。

情報セキュリティの分野において特にコンプライアンスが求められる法律には、著作権法（ソフトウェアの

不正コピーの防止など、知的財産権の侵害防止)、不正競争防止法、個人情報保護法、電子署名法、e-文書法などがあります。これらの法律については、その趣旨を正確に理解して、順守に向けた取組を行うことが必要です。
(丁)

③重要な情報資産(情報及び情報システム)を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱をするための方法を定めていますか。
(情報資産をその重要性に応じて管理するためには、レベル分け、レベルに応じた表示や取扱方法などの指針及び情報の管理責任者を定める必要があります)

説明 情報セキュリティ対策を効率的に、かつ高いコスト効果をもって実施するためには、重要な情報資産をあらかじめ把握するとともに、その情報資産の重要度に応じて管理することが必要です。また、情報資産の管理責任者や利用できる人の範囲などを情報資産の重要度に応じて、あらかじめ定めておくことで、取扱がずさんになることを防ぎます。その際、管理すべき情報資産には、情報システムだけでなく情報そのものも含むこと、また情報は、電子媒体に限らず紙媒体などについても管理が必要であることに留意する必要があります。

対策のポイント

- 重要な情報資産の目録を作成しているか
- 情報資産の管理責任者を明確に定めているか
- 情報の重要性に応じた分類及び取扱の指針を定めているか
- 情報システムから出力した情報についても、重要性のレベルや取扱が明確になっているか
- 分類及び取扱の指針に従って情報を分類した上で、重要性のレベルに応じた表示と取扱を行っているか。
- 情報資産を利用できる部署や人などの範囲を定めているか

解説

情報セキュリティ対策の最初のステップとして、重要な情報資産を記録した目録を作成する必要があります。主な情報資産には、情報と情報システムがあります。情報には、個人情報のように外部に漏えいした場合に顧客に迷惑をかけるものや、改ざんされると問題になるホームページのコンテンツのようなものがあります。情報システムには、個人情報が保管されているものや障害が発生すると業務が停止してしまうものなどがあります。

情報資産は、その機密性(情報が漏えいしないように保持すること)、完全性(情報が正しいこと)、可用性(必要な時に利用できること)の3つの観点から見た重要度に応じて分類します。たとえば、漏えいしたら困るような情報は、求められる機密性が高いといえます。また、Web上の公開情報などは、求められる機密性は高くはありませんが、改ざん、DoS攻撃などにより、Webが見られない状態になることは防がなければなりません。よって、求められる完全性や可用性は高いということがいえます。このような観点から情報資産の重要度を分類し、重要度に応じた取扱の指針を規定します。守るべき情報資産が明確になったら、さらに、それらの情報資産の管理責任者を定め、重要性のレベルに応じた表示や取扱の方法を定めて実施します。その際、守るべき情報は、電子的な情報に限りません。紙に印刷された情報も、電子的な情報と同様に守るべき情報資産です。冒頭に挙げたような各種の重要情報をプリントアウトした書類は、たとえば鍵のかかる書庫に保管する必要があります。印刷した重要情報をプリンタのトレイに置きっ放しにするなどということはあってはなりません。

加えて、情報資産を利用できる部署や従業員の範囲を定める必要があります。その範囲は規程類などに明記され、従業員に周知されていることが望まれます。
(丁)

④重要な情報(たとえば個人データや機密情報など)については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。
(適切な措置とは、業務プロセスごとの作業責任者や作業手順の明確化、取扱者の限定、処理の記録や確認などを指します。また、業務プロセスは、手作業で行うか、情報システムに依存するかを問いません。)

説明 重要情報の入手、作成、利用、保管、交換、提供、消去、破棄などに当たっては、そうした一連の業務プロセスごとの作業責任者や作業手順の明確化、取扱者の限定、処理の記録や確認などが必要です。

対策のポイント

- 各業務プロセスにおける作業責任者や作業手順を明確化し、その手順に基づいて作業を実施しているか
- 各業務プロセスにおける作業を適切な担当者のみ限定し、その作業担当者の認証や権限付与の状況を確認しているか
- 重要情報に対するアクセスの記録・保管、権限外作業の有無の確認など、対策の実施状況を把握しているか
- 組織内外での情報の交換について、ルールと手順を定め、その手順に基づいて作業を行っているか
- 重要な情報が消失、変更、誤用されないよう、操作ミスを検討した運用方法を定めているか
- 重要な情報について、漏えいや不正利用を防ぐために、保護対策を実施しているか

解説

個人データや営業秘密など特に重要な情報については、その情報が電子化されているかどうかによらず、入手、作成、利用、保管、交換、提供、消去、破棄など一連の業務プロセスごとにセキュリティを考慮した処理の手順を定めておく必要があります。業務プロセスごとに行うべき作業とその実施責任者を定義し、誰が実施しても間違いがないように明確に手順を定めておくこと、実施状況をチェックする責任者を設置し、作業が手

順通りに実施されていることを確認することが求められます。

セキュリティを考慮した処理の手順とは、たとえば次のようなものです。

- (1) 情報の入手・作成時には、情報の分類と格付けを行う。
- (2) 利用に際しては、業務目的以外の利用の禁止や、ルールや手順に沿った取扱いを行う。
- (3) 保存に際してはアクセス制御やバックアップといった基本的な保護対策を確実に行う。
- (4) 情報の交換に際しては、情報の送信や運搬の際に、情報漏えいが起こらないような対策を行う。
- (5) 情報の提供に際しては、提供先で適切な情報の取扱いがなされるような措置を行う。
- (6) 消去や破棄に際しては、破棄された文書や電子媒体からの情報漏えいが起こらないよう、紙は裁断などを行い、電子的情報は復元が困難なように、消去ソフトで消去するなどしてから破棄する。
- (7) 電子データの公開に際しては、公開しようとするファイルの取り違えや、ファイルのプロパティ（属性）情報の消し忘れなどによる不用意な情報の流出を防止するため、十分な確認を行う。

各業務プロセスにおける作業は決められた担当者だけが実施するようにしておく必要があります。具体的には、情報が保管されているシステムや書庫にアクセスできる人を制限する、あるいはアクセスできる情報を作業担当者ごとに制限することが求められます。

また、作業担当者の交代が多い組織では、作業担当者の ID 管理や作業権限の定期的なチェックが必要になります。作業担当者には、それぞれ別の ID を付与し、誰が作業を実施したのかが識別できるようにします。複数の作業担当者が一つの ID を共有することは、情報にアクセスしたのが誰なのかを後から特定することができないといった問題があるので避けるべきです。また、各作業担当者が実施可能な作業についても、作業担当者ごとに個別に必要な十分なだけの権限を付与し明確化しておくことが必要です。

重要情報に対するアクセスの記録を取得し、一定の期間保管しておく必要もあります。アクセスの記録は定期的にチェックし、不正なアクセスが行われていないかどうか、権限外の作業が行われていないかなどの点についてチェックすることも有効な管理策です。

重要な情報の消失、変更、誤用、漏えい、不正利用を防ぐため、担当者の操作ミスや不正も考慮した運用方法や保護対策を策定・実施する必要があります。

(丁)

⑤外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。

(セキュリティ上の理由とは、たとえば情報の漏えいや消失、情報あるいは情報システムの誤用などの防止を指します。)

説明 外部の組織に業務を委託する際の契約書には、情報の漏えいや消失の防止、情報あるいは情報システムの誤用の防止を徹底するために、それらに関する条件を記載しておく必要があります。記載すべき条件には、委託先が実施すべき業務の内容、委託先が提供するサービスに関するサービスレベルの保証、委託先が委託業務に関して実施すべき安全管理措置などがあります。さらに、そうした契約条件に沿って適切に業務が遂行されていることを確認するため、報告や記録を求めることも大切です。

対策のポイント

- 委託業務に際して締結する契約書に、業務内容、サービスレベル及び委託先に提供する重要な情報に関する安全管理措置や機密保持などの責任などを明確に定め記載しているか
- 委託業務の確実な実施や委託先でのセキュリティ対策実施状況を報告や記録により確認しているか
- 委託業務内容の変更について把握し、記録しているか

解説

外部の組織に業務を委託するということは、自組織で定めたセキュリティポリシーが適用されない、あるいは、実施しているセキュリティ対策の効果が及ばないところで業務が行われるということであり、組織内向けの対策とは異なる対策が必要になります。新規の委託契約を結ぶ場合には、契約書に業務内容、サービスレベル、委託先に提供する重要な情報に関する安全管理措置や機密保持などの責任といったセキュリティ上の要求事項を記載するようにします。

既に結んでいる契約についてはまず、どのような業務を委託しているのかを正確に把握することが必要です。委託している業務が明らかになったら、それぞれの業務について、委託先との間で交わされている契約の内容が委託する業務の内容や情報資産の重要性を鑑みて適切かどうかを確認し、セキュリティ上の要求事項が記載されていなかったり、適切なセキュリティ管理が望めないような記述となっていたりする場合には、契約書にそれらを追加、修正できないかどうかを委託先と協議してみる必要があります。

委託先において、セキュリティについての要求を満たすために必要なセキュリティ対策が実施されていることを背景に、委託業務が確実に実施されていることが確認できるように、報告や記録を提出してもらう必要があります。

委託する業務内容に変更がある場合には、変更の内容やその変更がサービスや安全性に及ぼす影響を把握し、

記録しておくことが望めます。
(了)

⑥従業員（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。
(従業員に情報セキュリティについての要求を順守させるためには、従業員の管理責任者を明確にし、従業員が守るべきルールなどを明確にし、それらを周知させておく必要があります。)

説明 すべての従業員に対して、採用や退職の際に、セキュリティ上の義務や、退職後の守秘義務など、セキュリティ上の順守事項を誓約させることで、注意義務を自覚させるとともに、就業規則や服務規律などに明示するなどして、情報セキュリティ対策に実効性を持たせます。さらに、退職や異動に際しては、貸与した資産の返却を確認すること、付与したアクセス権限を削除することも大切です。

対策のポイント

- 従業員（派遣を含む）を採用する際に、経歴、資格などが職務にふさわしいかを十分に審査し、さらに守秘義務契約を締結しているか
- 雇用契約時に、セキュリティ上の義務を明示しているか
- 就業規則ないし服務規律に、従業員が順守すべき事項を明示しているか
- 退職に際して、情報資産の返却確認やアクセス権限の削除を確実にしているか
- 退職に際して、退職後における守秘義務を退職予定の従業員に再確認しているか
- セキュリティ違反を犯した従業員に対する懲戒手続を整備しているか
- 採用から雇用、退職まで、従業員の管理を行う体制と責任が明確になっているか

解説

情報セキュリティ対策の基本の一つは、人のマネジメントです。すべての従業員に対して、採用や退職の際に、情報セキュリティ上の義務や、業務上知りえた機密情報を(退職後も)外部に漏らさないことなど、セキュリティ上の順守事項を誓約させることで、一人一人に情報セキュリティ上の注意義務を自覚させるとともに、情報セキュリティ対策を実効性のあるものにすることができます。具体的には、従業員（派遣を含む）の採用・退職に際して、業務遂行時の情報セキュリティ上の義務や、在職中及び退職後の守秘義務に関する書面を交わすことなどです。現在業務に携わっている従業員で、まだ守秘義務契約を交わしていない人についても、改めて書面を交わすとよいでしょう。

雇用契約時には、すべての採用者に対して、従うべき情報セキュリティ上の義務を明示してください。また、実際に業務に就く前に採用時の研修などでパスワードを扱う際の順守事項、ウイルス対策や OS・ソフトウェアの修正プログラムの適用を適切に実施すること、電子メールを使用する際の注意など、各人が守るべき事項について教育する必要があります。

就業規則ないし服務規律に、従業員が順守すべき情報セキュリティ上の要求事項を明示しておくことも必要です。定期的に就業規則ないし服務規律の順守状況をチェックし、順守されていない場合には、従業員に対して、順守の徹底を促すことも重要です。

従業員の退職時には、コンピュータや記憶媒体、書類などの情報資産が返却されたことや、その従業員の ID に設定されたアクセス権限が削除されていることを確認する必要があります。

従業員がセキュリティ違反を犯した場合には、相応に対応すべく、就業規則などに懲戒手続を定めておくことが望めます。懲戒手続を設けることで抑止効果も期待できます。

さらに、これらの事項が適切に遂行されるように、人事管理の体制や責任について明確にしておくことが重要です。

(了)

⑦経営層や派遣を含む全ての従業員に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施していますか。

(情報セキュリティ教育は、全員に漏れなく定期的に行うことが大切です。セキュリティ対策上の順守事項、禁止事項の徹底とともに、情報セキュリティの脅威と対策についても教育します。)

説明 従業員に対する教育は、情報セキュリティ対策の有効性を向上させるために必要不可欠です。関係者全員に対する教育を適切に実施し、その効果が得られていることを確認することによって、技術的なセキュリティ対策との相乗効果を期待できます。特に、保護すべき情報資産へのアクセス管理を確実なものとするために、パスワードや鍵の管理の徹底はとて大切です。

対策のポイント

- ポリシー及び関連規程を従業員（派遣を含む）が理解し、実践するために必要な教育を実施しているか
- パスワードの管理や暗号鍵の管理について教育を行なっているか
- 単に出来合いの教材だけでなく、自組織の状況に即した適切な教材を用意しているか
- 教育は、定期的に、従業員全員に漏れなく実施しているか
- 教育が有効であることを確認するための手立てを用意しているか

解説

従業者に対する教育は、情報セキュリティ対策の有効性を向上させるために必要不可欠なものです。従業者に対する教育には、ポリシーや関連規程の周知といった全体を俯瞰するための事項から、パスワードの管理や暗号鍵の管理、電子メールを使用する際の注意点といった個別の項目まで幅広く実施する必要があります。

基本的・一般的な事項については市販されている教材を使用することで、費用と効果のバランスをとることができますが、事業活動に直接関わる項目や、特に重点を置いている項目、対策を徹底したい項目については、自組織の状況に即した教材を作成するなどの工夫をすることも必要です。

また、職位や職種によって、情報セキュリティ上の責任が異なるので、教育や研修は、すべての従業者に共通のものと、従業者の職位や職種(情報セキュリティ管理者向け、一般従業員向け、管理職向けなど)に応じたものとに分けて実施すると効果的です。

教育は1度実施しただけで、100%の効果が得られるというものではないので、半年ごとや1年ごとというように定期的を実施することが必要です。新規採用や異動の際にも適宜教育を行います。また、社会状況の変化や技術の進歩に伴い、新規に教育すべき項目が出てくるので、それらにキャッチアップするためにも、派遣を含むすべての従業者に定期的な教育を実施することが必要となります。

教育の効果は従業者一人一人によっても異なります。すべての従業者の教育効果を一定のレベル以上とするためには、効果を確認するためのテストを実施したり、何らかのインセンティブを設けたりするなどの施策が必要な場合もあります。情報セキュリティ上の事故が発生したと仮定した事故対応訓練を実施することは、実際に事故が発生した場合の被害を低減することや従業者の意識喚起に効果があります。

(丁)

大項目 2. 物理的（環境的）セキュリティ上の施策

①特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。
（特にセキュリティを強化したい建物や区画については、ゲートや間仕切りを設けるなどして、境界を明確にし、入退館や入退室管理を実施する、あるいは警報装置の設置などを行います。また、荷物の受渡し場所や外部者の作業場所を確保するなど、セキュリティを考慮して物理的に区域を分けるようにします。）

説明 重要な情報や関連する設備が数多く存在する場所については、セキュリティ対策として特段の配慮が必要となります。このような場所（建物や区画）については、入室可能な人をできるだけ制限したり、外部からの侵入者に対する防護策を強化したりすることが必要です。対策としては、ゲートや間仕切りを設けるなどして、境界を明確にし、入退館や入退室管理を実施する、あるいは警報装置の設置などを行います。また、荷物の受渡し場所や外部者の作業場所の確保、外来者の来訪履歴の保管も大切です。

対策のポイント

- 特にセキュリティを強化したい物理的の区域を定め、この区域の内外において順守すべきセキュリティ上の規程を整備しているか
- 侵入を防止するために必要な建物や警報設備などの基準を設定しているか
- 敷地及び建物に入ることができる人を制限しているか
- その制限の対象になる人を識別できるようにしているか
- 入退館（室）の履歴を記録し、その記録を適切に管理しているか
- 訪問者や清掃業者などの立ち入りできる区域が明確になっているか

解説

重要な情報や関連する設備が存在する区域の安全性を保つためには、管理者の意識だけに頼らず、安全管理措置として守るべき事項を規程として整備し、徹底することが必要です。その区域内の情報資産の重要度に応じて物理的な区域分けを行い、安全管理措置の必要な区域（安全区域）とその他の区域の境界を適切に設定します。また、その境界の内外において順守すべき防犯や防災などの安全管理措置について、規程類を整備し、ルールを徹底する必要があります。

物理的の区域のレベル分けは、たとえば来客ゾーン、一般執務ゾーン、機密ゾーンのように多段階となることがあり、場所も一箇所とは限りません。それぞれの場所で必要なセキュリティレベルを保つためには、各種保安設備の設置基準を作成することが必要です。具体的には、ICカードや個人認証などを利用した入退室の監視設備の設置基準、また、赤外線や振動センサなど防犯用の各種警報設備の設置基準などを設定することが求められます。

区域内の安全確保のためには、この境界内に立ち入る人をできるだけ少なくすることが大切です。そのためには、重要な場所の施錠管理を徹底すること、さらに、ICカードなどによる、セキュリティレベルに応じた入室制限を行うことが必要になります。

防犯設備などによる侵入対策に加え、許可された人物であるかどうかを一目で確認できることも重要です。よく利用される対策としては、ゲストと従業員を名札の色で識別する方法などが挙げられます。

万が一の際に事故原因を究明できるよう、安全区域内に入った人物が誰であるかを確認する必要があります。また、記録を採ることは犯罪や不正行為の抑止にもつながります。そのためには、ICカードによる個人識別などを利用して、入退室の記録を管理する、あるいは入退室時の記帳管理を徹底するといった取組が必要です。

（了）

②顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。
（自組織の建物や事務所には、思ったよりも多くの外来者が出入りしている事があります。そうした外来者に守って頂くべきルールをあらかじめ定めておくことが重要です。）

説明 建物や事務所の中には、数多くの情報や関連する設備が所在しています。これらの情報や設備に触れる機会のある外来者に対しては、それぞれのリスクの状況を踏まえたルールの制定と、それに従った運用を行うことが必要です。

対策のポイント

- 外部の人々の出入りによって、どのようなリスクが生じるかを検討し、その結果、明らかになったリスクについて適切な対策を実施したか
- 外来者が建物内や室内で作業する場合、適切な管理の下で作業を行わせているか
- 立ち入りを許した区域内で訪問者や清掃業者などへの応対を実施しているか
- 顧客との打合せ場所や案内時の導線などにおいて、セキュリティ上の配慮を行っているか

解説

建物には、情報システムベンダのメンテナンスやビルのメンテナンス業者、清掃業者、配送業者、什器業者、コンサルタント、常駐の業務委託先社員などいろいろな種類の外部の人が出入りします。

建物に出入りする委託業者のリスクを検討する際は、以下の点がポイントとなります。

- ・ 外部業者の業務内容と業務上必要な行動範囲の洗い出し
- ・ 外部業者が起こす故意や過失による盗難や盗み見、損壊や紛失などの分析
- ・ そうした盗難や盗み見、損壊や紛失などが発生した場合の影響の分析

また、環境の変化や新しいリスクに対応するため、上記の検討を定期的にも実施することも重要です。

多くの場合、リスク評価の結果、様々なリスクが確認されます。この中で、影響の大きなリスクについては、対策の実施が必要です。また、対策の中には、すぐに実施することが可能ではなく、多額の費用や長い期間を要するものがあります。こうした対策が必要と判断されたリスクについては、対策の実施計画を定め、実施状況を適切に管理することが必要です。

具体的には、たとえば次のような対策があります。

- ・ 顧客が来訪した際に、執務室内や他の打合せの様子が不用意に知られないように、打合せ場所やそこに案内する際の導線などを考慮する
- ・ 外部の人がサーバールームなどの重要な部屋に入退室する際は、カメラ付携帯電話などの物品の持ち込みや持ち出しを制限する
- ・ 清掃業者による清掃作業は、従業者が在室している時間帯（たとえば執務時間内）に実施する
- ・ 運送業者は、必ず受付を通るといった受け渡しの手続きを決めて、順守を依頼する
- ・ 外部の人が建物内や室内で作業をする場合は、その行動範囲を限定するとともに、執務室など安全区域に入る場合には、自組織の従業者が必ず立ち会う

(了)

③重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。

(安全性に配慮した配置または設置とは、たとえば、重要なシステムの安全な場所への設置、盗み見の防止や盗聴防止などに配慮した設置、配線類の地下や床下への埋設、浸水、火災、地震などを考慮した配置などを行います。)

説明 重要な情報機器や配線については、偶然の事故による損壊や外部の者による盗み見や損壊を防ぐなど、安全上の配慮が必要です。偶然の事故に対しては、機器の転倒防止、漏水被害対策、周辺での飲食禁止、踏みつけや引っ張りによる断線の防止など、設備本体や周辺で起こりうる事故を洗い出し、それらに備えた対策を行うことが重要です。また、外部の者による盗み見や損壊に対しては、機器や配線などに、容易に接触できないようにすることが重要です。

対策のポイント

- 基幹業務システムや機密情報を保有する情報システムを、許可された者だけが立ち入ることのできる安全な場所に設置しているか
- 執務室の入口から見えないように情報処理設備を配置または設置しているか
- 使用中に画面を盗み見されないように配置を工夫しているか
- 不用意な損傷、傍受による盗聴などに配慮して、電源コードや通信ケーブルを配置しているか
- 重要な情報システムについて、地震などによる転倒の防止、水漏れなどによる被害の予防、停電時の代替電源の確保などを実施しているか

解説

基幹業務システムや機密情報を保有しているシステムは、一般の従業員や来訪者から隔離し、容易に触れられない場所に設置することが重要です。入場制限の無いパブリックエリア（廊下、通路、打ち合わせ場所など）からは確実に隔離する必要があります。また、施錠や入退室管理、さらに多段階のセキュリティ区分を設定することも重要です。

安全管理を行う際、情報処理の機器本体だけに注意が行きがちですが、設備の安全面を考えると、電源や通信ケーブルなどの配線の保護も重要です。情報処理設備や配線などを悪意による損壊などから保護するためには、それらに容易に接触できないようにすることが大切です。そのためには、まず機器や配線などの設備が入口や通路などから容易に見えないようにすることが重要です。

カウンターや通路、打ち合わせ場所から情報機器の画面などが容易にのぞき見できてしまうと、画面に表示されている情報が漏えいするだけでなく、当該端末で実施できる作業を来訪者に伝えているようなものです。このような状況を避けるためには、事務所レイアウトや画面の向きなどを変更し、外部者や担当外の従業者が画面を覗けないようにするなどの工夫が必要です。

複数の組織が入居するテナントビルなどでは、組織として管理の手が及ばないケーブルシャフト扉の施錠などの管理状況の確認が望まれます。

また、機器の転倒や漏水など偶然の事故への対策も必要です。重要な情報機器は日常の業務を行う場所とは

別のセキュリティ境界内に設置し、情報機器や配線についても地震や火災、踏みつけや引っ張りによる断線や緩みなど、災害や過失による損壊への対策を行うとともに、停電時の代替電源を確保しておくことも求められます。また、こうした区画内では飲食を禁止するなど、禁止行為を定めることも必要です。
(丁)

④重要な書類、モバイル PC、記憶媒体などについて適切な管理を行っていますか。
(適切な管理とは、たとえば、保管キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉碎廃棄などを言います。また、重要な書類には、情報システムに関する文書を含みます。)

説明 書類や電子的な記憶媒体などによって情報が漏えいする事故が数多く発生しています。保管キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉碎廃棄など、重要な情報が記録されている書類や記憶媒体を適切に管理することが必要です。また、重要な書類などが他の物品に紛れてしまう事によって不適切な取扱が起きないように、日ごろから、事務所や会議室の整理整頓に心がけることも大切です。

対策のポイント

- 重要な書類、モバイル PC、記憶媒体などを適切に管理しているか
- 重要な書類、モバイル PC、記憶媒体などは、物理的に破壊するなどしてから処分しているか
- 重要なデータやライセンス付きのソフトウェアなどを格納した装置や記憶媒体を破棄する際は、中のデータを確実に消去しているか
- 事務所内の机上、書庫、会議室などの整理整頓を実施しているか
- 事務所、机、保管キャビネットなどの施錠管理を実施しているか
- 郵便物、FAX、印刷物などの放置禁止や保護を実施しているか
- 情報システムに関する情報も重要書類として取り扱い、施錠保管などを実施しているか

解説

適切な管理が行われていない書類やモバイル PC、記憶媒体などから情報が漏えいする事故が数多く発生しています。重要な情報が記録されている書類やモバイル PC、記憶媒体については、適切な管理が必要ですが、非常に身近なものであるため、管理が行き届きにくいという面もあります。情報漏えいを防止するためには、次のような管理を徹底する必要があります。

まず、重要な情報が記録されている書類やモバイル PC、記憶媒体などについての管理方法を定めることが必要です。この管理方法には、作成、利用、修正、保管、廃棄の工程ごとにその業務を行うことのできる人の明確化と、その実施を確かにするための技術的対策や手順の策定が含まれます。たとえば、機密情報はキャビネットに施錠保管し、担当者以外がその情報を参照する場合には、その機密情報の管理責任者の事前の承認を得るというルールを定めることなどです。

書類やモバイル PC、記憶媒体の廃棄処理が不適切であったことに起因する情報漏えい事故も数多く起こっています。書類や記憶媒体などはメディアシュレッターを用いて粉碎処理すること、重要なデータやライセンス付きのソフトウェアなどを消去する場合は、ファイルの削除だけでなく、意味のないデータを上書する、あるいはデータ消去ソフトウェアやデータ消去装置を用いるなどして中のデータを確実に消去することが望まれます。その際は、情報システムや PC に内蔵されている HDD (ハードディスクドライブ) にも注意が必要です。さらに、大量廃棄で専門廃棄業者を利用する際は廃棄証明を入手することなども重要です。

また、事務所内の机上、書庫、会議室など、身近な場所の整理整頓を行い、重要な情報が記録されている書類や記憶媒体が他に紛れ込まないようにすることが必要です。

放置された郵便物、FAX、印刷物の盗難により、情報が漏えいする場合があります。このような事故を防止するためには、次のような管理が必要です。

- ・ 郵便物受けの施錠管理
- ・ 郵便物の授受管理
- ・ FAX 着信物の早期回収
- ・ FAX 送信時の番号確認、事前・事後の電話連絡
- ・ プリントアウトした印刷物の早期回収

情報システムに関する文書類の流出が機密情報漏えいにつながる可能性もあることから、そうした文書も他の重要情報と同様に、施錠管理や適切な廃棄処理といった管理を徹底する必要があります。

(丁)

大項目 3. 通信ネットワーク及び情報システムの運用管理状況

①情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。

(適切な保護には、開発環境、テスト環境と運用環境の分離、変更管理の実施、開発での本番データの使用制限などが含まれます。)

説明 システム開発には、多数の作業者が関与するなど、大きなリスクが潜在しています。そのため、システム開発から本番運用への移行を踏まえ、十分な受け入れテストの実施、運用システムと開発システムの分離、運用システムの変更管理手順の策定、個人情報などの重要なデータを含む本番データの使用制限などの対策が重要となります。

対策のポイント

- 情報システムの運用環境を開発環境やテスト環境から隔離しているか
- 個人情報などの重要なデータを不用意にテストに用いないためのルールを定めているか
- 運用環境の変更について規程を定めているか
- 運用環境の変更を規程に沿って行うと共に、その過程や結果を記録しているか
- 必要な場合、情報システムの性能や容量の管理を行っているか
- 情報システムの受け入れについて、十分なテストを行っているか

解説

運用中の情報システムやデータは、適切に管理することが必要です。システム開発においては、開発費用の削減のために新たなテスト用のシステムを構築せず、運用中の情報システムを利用したテストを行う場合があります。しかし、重要なシステムの開発においては、運用環境への影響を防止するため、別途開発環境やテスト環境を用意し、開発及びテストを実施することが望まれます。

個人情報や機密情報などを取り扱うシステムで、開発したシステムの最終的な検証に本番データ（実在する個人のデータなど）を用いて行う場合があります。そのような場合には、次の点を明確にすることが必要です。

- ・ 本番データを使用しなければならない理由と検証すべき範囲
- ・ テストに使用する本番データの重要度
- ・ 作業員、作業場所及び作業に用いる装置の制限
- ・ データの持ち出し、コピーなどの禁止
- ・ 本番データを利用する際の承認手続き
- ・ 使用後の消去手続きと確認方法

開発したシステムを運用環境へ移行する際や、運用環境の変更の際には、予想外のトラブルが発生する場合があります。そのため、システムや運用環境の変更について、変更作業の承認や手順、変更内容の記録などの規程を定め、トラブルが発生するリスクを軽減するとともに、万が一トラブルが発生した場合の対応方法などを明確にしておくことが必要です。また、システムや運用環境の変更については、規程を踏まえた手続きが行われているかを確認することが必要です。変更によるトラブルが発生していない場合でも、規程が形骸化している場合があるので、変更後には必ず作業内容を確認することが必要です。また、緊急にシステムの変更が必要な場合も想定されます。こうした場合に備え、事前に連絡体制や判断基準などを定めておくことも重要です。新しい情報システムの受け入れにあたっては、あらかじめ要求事項や基準を明確にした上で、それが満たされていることを確認するために、十分なテストを行うことが求められます。

運用中の情報システムでは、利用状況の変化やデータの蓄積などにより、システム資源の状況が大きく変化します。これらの状況の変化がシステムの円滑な運用に影響を与えないよう、情報システムの利用状況を定期的に把握するとともに、計画に沿った変更や季節変動などの要因を考慮し、必要なシステムの性能や容量を予測することが必要です。予測結果がシステムの能力を超えるような場合には、拡張計画を立案し、不要なシステムトラブルを未然に防ぐことが望まれます。

(丁)

②情報システムの運用に際して、必要なセキュリティ対策を実施していますか。

(必要なセキュリティ対策には、各種手順書の作成、ルールに従った運用、監視、ログの取得と分析などが含まれます。)

説明 情報システムや通信ネットワークの運用管理に必要な情報セキュリティ対策には、セキュリティの確保に必要な事項を含む各種手順書の作成、手順書などのルールに従った運用の実施とその監視、ログの取得と分析などが含まれます。また、運用システムを安定して稼働させるためには、情報システムの性能や容量を監視することも大切です。

対策のポイント

- システム運用におけるセキュリティ要求事項を明確にしているか
- 情報システムの運用手順書を整備しているか
- 日々のシステム運用に不手際が生じないようにするための工夫をしているか

- システムの運用状況を点検しているか
- セキュリティ関連のイベントのログを取得しているか
- 設備の使用状況を記録しているか
- イベントログや設備の使用状況に関する記録を定期的に点検しているか
- 不正行為の証拠を隠蔽するなどの目的で、システムログや各種の記録が、改ざんや消去などされないように配慮しているか
- システム内のサーバや端末などの機器類について、常に時刻が同期するよう設定しているか

解説

情報システムに求められるセキュリティ要件は、情報システムの機能ごとに異なります。どのような業務でどのような情報システムが利用されているのか、またその情報システムへのアクセス権の設定などが、アクセスする人間の職務に対応しているのかということについても詳しく調査し、それぞれの情報システムに必要な機能について、それぞれ適切なセキュリティ機能を実装されているか確認してください。

情報システムを適切に運用するためには、安定運用やセキュリティの観点からの監視やバックアップ、またニーズの変更に伴い各種機器の設定の変更などが必要になります。管理者または利用者がこうした作業を安全に実施するためには、マニュアル（手順書類）を整備しておく必要があります。マニュアルには、正しく運用が実施されているかどうかを判断するための指針やサービスレベルを記載し、これらを管理するための仕組みを盛り込むことを忘れないようにしてください。マニュアルは誰でもが理解できるようにシンプルでわかりやすいものでなければいけません。また、「～してはならない」という記述は網羅性に欠ける場合があります。どうすれば正しい作業ができるのかという点に着目し、「～すること」というルールを書き方ができるように業務の見直しを行うことも必要です。

特に重要なシステムの運用では、実施した操作や検出された障害、セキュリティに関連する事象（イベント）について記録しておくことが必要です。

マニュアル通りの正しい作業ができているかどうかを点検するのは管理者の役目です。情報システム管理者はそれぞれの情報システムから得ることのできる記録をもとに、すべての利用者が正しい作業を実施できているかどうかを確認してください。また、問題の早期発見に努めるという意味で、定期的な確認作業が必要になります。できれば、組織内に情報システムに関するサービスデスクを設置し、情報システムの利用における相談などを一元的に受けられるようにすると良いでしょう。

情報システムを安定的に運用するためには、利用者の活動やセキュリティ事象、管理者・運用担当者の作業、障害といったセキュリティログや設備の使用状況について記録し、それらを定期的に点検して異常の有無を確認する必要があります。また、不正行為の証拠を隠蔽する目的で、それらの記録が改ざん、消去などされる可能性があることから、そうした行為が行えないよう、安全に管理することが重要です。

なお、正確な記録のためには、正確な時刻管理が重要です。コンピュータのクロックには狂いが生じるものがあるので、システム内のサーバや端末などの時刻を確認して狂いがあれば修正する手順を整え、実践することが望まれます。

（丁）

③不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウェアなど）への対策を実施していますか。

（不正プログラム対策には、ウイルス対策ソフトの導入や、パターンファイルの更新を適時行うこと、ぜい弱性を解消することなどが含まれます。）

説明 不正プログラム対策には、ウイルス対策ソフトを導入し、パターンファイルの更新を適時行うことなどが含まれます。また、定期的なウイルス検査を実施し、万が一問題が生じた場合にとるべき処置を周知しておくことも大切です。

対策のポイント

- ウイルス対策ソフトを適切に導入しているか
- パターンファイルの更新を適切に行っているか
- 各サーバやクライアント PC について、定期的なウイルス検査を行っているか
- 情報システムの利用者は、ウイルス対策や問題が生じた場合における必要な処置について十分に認識しているか
- 外部で使用したモバイル PC を内部ネットワークに接続する前に、ウイルス駆除などの（検疫）処理を行っているか
- 不正プログラムによる攻撃などに悪用されないよう、ぜい弱性の解消（修正プログラムの適用）を行っているか

解説

ウイルスやワームなどの悪意のある不正なソフトウェアに対する技術的な対策としては、インターネットなど外部とのネットワーク接続点におけるゲートウェイ型のウイルス対策ソフトの導入や、クライアント PC、サーバへのファイル監視型のウイルス対策ソフトなどの導入があります。

現在、一般に市販されているウイルス対策ソフトは、新種のウイルスへの対応など完全にウイルスを検出、遮断できるものではありません。このため、ウイルスやワームに感染した場合に、被害を最小範囲に留め、組織全体に広まらないようにするためには、発見から対応までの迅速な行動が求められます。このためには、発見時にはネットワークケーブルを抜くといった、利用者が実施できる行動に加えて、情報セキュリティあるいは情報システムの管理担当部署に対する迅速な報告と、管理部署から必要な対策を関係者に指示する手順が必要です。

迅速な状況報告を行うためには、ウイルスやワームを発見したすべての従業員が担当部署に情報を伝達できるように担当部署や責任者への報告手順を構築することから始めてください。また、情報を集約する場所として情報セキュリティ委員会やSOC（セキュリティオペレーションセンター）を指定し、報告された情報に基づいて適切な行動を指示する責任者を配置する必要があります。発生した状況に対する適切な対応を実現するには、すべての情報が責任者の元に届く仕組みが必須条件となるだけでなく、これらの情報を評価・判断するための技術者の配置も必要になります。組織内にこれらの要員をおくことができない場合は、アウトソーシングによる監視サービスなどを導入することも検討してください。

ウイルス対策においては、ウイルス対策ソフトウェアの導入だけではなく、パターンファイルの更新や情報収集を行うための体制を構築することが重要です。インベントリ管理ソフトウェアなどを利用して、ウイルス対策ソフトウェアのパターンファイルが最新のものとなっているか、定期的なウイルススキャンは行われているか、OS やアプリケーションのパッチ（修正プログラム）が正しく当てられているか、不正なアプリケーションが導入されていないか検査することによって、感染抑止効果を得ることができます。また、モバイル PC を内部ネットワークに接続する前にウイルス感染の有無などをチェックする検疫処理も効果的です。

ウイルス対策はどうしてもウイルスに感染したときの対応策ばかりを考えがちですが、未然に防ぐという観点でウイルス対策ソフトの使用状況の管理を行うこと、また従業員に対してウイルス感染による被害に関する教育を行うなどして、感染抑止機能を充実させることも重要な対策となります。

(了)

④導入している情報システムに対して、適切なぜい弱性対策を実施していますか。

（適切なぜい弱性対策には、セキュリティを考慮した設定や、パッチ（修正プログラム）の適用、バージョン管理や構成管理、変更管理などが含まれます。）

説明 適切なぜい弱性対策には、ぜい弱性情報や脅威情報の定期的な入手、不要なサービスの停止といったセキュリティを考慮した設定、パッチ（修正プログラム）の適用、バージョン管理や構成管理、変更管理などを含まれます。

対策のポイント

- ぜい弱性情報や脅威情報を定期的に収集しているか
- ぜい弱性や脅威に大きな変化があった場合には、リスクを改めて評価し、ソフトウェアへのパッチ（修正プログラム）適用などの必要な措置を実施しているか
- パッチについてテスト・適用が適切になされているか
- 情報システムの導入に際して、不要なサービスを停止するなど、セキュリティを考慮した設定を実施しているか
- Web サイトの公開にあたっては、不正アクセスや改ざんなどを受けないように、適切な設定やぜい弱性の解消を行っているか

解説

情報資産としてのソフトウェアについては、ライセンス管理やバージョン管理だけではなく、ソフトウェア自身のぜい弱性の管理も実施しなくてはなりません。ぜい弱性に関する情報やそれを悪用した不正アクセス・ウイルスなどの脅威に関する情報は不定期に流れるため、なるべく最新情報を収集するとともに、大きな変化があった場合にはそれがどのようなリスクをもたらすのか評価し、適切に対処することが求められます。たとえば、ソフトウェアのぜい弱性はパッチ(修正プログラム)を適用することで低減することができます。しかしながら、パッチの提供は信頼のおけるソフトウェア開発元が提供しているソフトウェアに限られると考えなければなりません。すでにサポートが終了しているソフトウェアや、インターネットや雑誌添付の CD-ROM など配布されているマクロプログラムや CGI プログラムなどは、十分なぜい弱性テストが実施されていない場合もありますので、特に注意が必要です。

ソフトウェアの管理については、たとえば組織内標準システム（標準構成）という概念を取り入れ、一元管理を行うことをお勧めします。組織内標準システムとは、業務に利用するアプリケーションを特定し、利用環境を想定したセキュリティ対策をあらかじめ施したコンピュータのことを言います。ソフトウェアのぜい弱性情報などについても一元管理できるように、情報共有のための仕組みを取り入れることが望まれます。

ソフトウェアを適切に管理するためには、システムの利用者それぞれがソフトウェアのインストールを行うのではなく、たとえば情報システム担当者の責任のもとに一元的にインストールを行うことで、不要なサービスが稼動していたりする設定ミスやぜい弱性の残留を抑えることが可能になります。ソフトウェアやデータの

廃棄についても手順を定め、情報システム担当者が一元的に行うなどの取り決めをすることも、ソフトウェアに関わるトラブルの低減に役立ちます。

また、ファイアウォールや内部サーバなどは、利用環境によって設定が異なる場合が少なくありません。また Web サイトのように外部のインターネットに公開され、不正アクセスや改ざんの脅威にさらされるシステムについては、特に注意が必要です。新たな脅威に対する防御という意味でも設定の見直しを定期的実施することが必要になります。これらの作業を計画的に行うには、単なる情報収集だけではなく、設定の有効期限という概念を取り入れ、定期的に入れ替えを実施することが必要です。管理する機器が多い場合には、作業の効率化とメンテナンスのし忘れの防止のために、自動的なログ分析に基づくリアルタイムな設定変更などについても十分に検討しなければなりません。

問題が発生する予兆があるにもかかわらず、簡単に予防できない場合には専門家に相談することも必要です。事故が起こってから業者を選定するのではなく、いつでも相談できるようにあらかじめ保守サービスや運用サービスを行っている業者にコンタクトをとっておくなどの準備も重要です。

(丁)

⑤通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。

(適切な保護策には、VPN の使用や重要な情報の SSL などによる暗号化があります。)

説明 適切な保護策には、VPN の使用や重要な情報の SSL などによる暗号化があります。また、重要な情報を電子メールでやりとりする場合には、情報を暗号化しておくことも効果的です。

対策のポイント

- 外部のネットワークから内部のネットワークや情報システムへアクセスする場合に、VPN などを用いて暗号化した通信路を使用しているか
- Web にアクセスする際、必要に応じ、SSL などを用いて通信データを暗号化しているか
- 電子メールをやり取りする場合に、重要な情報を暗号化しているか

解説

ネットワークについても、その他の情報資産と同様にどのようなデータが流れるのか、セキュリティ対策はどうなっているのかといったことを調査し、重要度を決定する必要があります。重要なネットワークには優先的に適切な保護対策を実施しなければいけません。ネットワークは一見、あらゆるシステムと接続しているように見えますが、実はセグメントという考え方で部分的に分離することが可能です。重要な情報資産が接続されているネットワークについては、一般のネットワークとは別のセグメントに隔離し、認証によるアクセス制御を実施してください。アクセス制御のポリシーは、ファイルサーバのフォルダ管理と同様に、誰がアクセスして良いのか、どのような操作をして良いのか（ネットワークサービスの制限）ということ的前提として検討する必要があります。

インターネットだけではなく、内部のネットワークにおいても重要な通信は暗号化して行わなければなりません。たとえば、各部門の経理担当者が経理サーバにアクセスする場合、担当者から経理サーバまでのネットワーク経路が他の部門をまたぐこととなります。このような場合、多くの従業員に対して経路の途中で情報を傍受する機会を与えることとなります。こうした環境では、たとえ内部ネットワークであっても VPN を導入して経路を暗号化する、スイッチングハブなどを利用して部門ごとにネットワークを分離するなどの対策が必要になります。特に、無線 LAN を使用している場合には、建物の外からでも傍受できることがあるため、必ず暗号化通信の設定をしてください。

また、内部の情報システムでウェブアプリケーションを利用している場合には、アプリケーション層でのセキュリティも考慮しなければなりません。ウェブでは SSL などの暗号化プロトコルを導入することで、サーバとクライアントの間を暗号化することができます。これで通信経路上のデータは保護することができますが、情報システムに保存されたデータ、画面に表示されたデータ、プリントアウトされたデータなどは暗号化されていないわけではないので、トータルセキュリティという観点ではこれらのデータの保護対策についても検討するのを忘れないでください。

なお、インターネットを利用した本支店間の通信や、出張先・外出先からのインターネットを利用した自社システムへのアクセスなどにおいては、VPN を導入して経路を暗号化するなどの対策が必要になります。出張先のホテルなどから内部ネットワークにアクセスする場合、VPN によって経路全体を暗号化しないと、情報がホテル内のネットワークに漏れいするおそれもあります。外部からアクセスしてメールや組織内ポータルを閲覧する場合には、たとえば VPN によってセキュリティ環境が整った状態でのみ利用するというルールを作り、これを従業員に周知徹底させることが望めます。

また、重要なメールのやりとりについては、添付書類を暗号化したり、メッセージそのものを暗号化したりすることも必要になります。多くの圧縮ソフトウェアでは、ファイルの暗号化機能もサポートしていますので、それらを活用するなど、利用環境にあわせて暗号化ツールを選択してください。

(丁)

⑥モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。

(モバイル PC や USB メモリなどの記憶媒体の使用場所には、外部のパブリックスペースやリモートオフィス、自宅などを含みます。外部のセキュリティの脅威は内部よりも高いことを考慮して対策を行う必要があります。)

説明 モバイル PC や USB メモリなどの記憶媒体の使用場所には、外部のパブリックスペースやリモートオフィス、自宅などを含みます。外部では、内部での利用に比べて盗難や紛失のリスクが高いことを考慮し、外部持ち出しに関する規程を定めたり、強固な認証や暗号化などの対策を検討したりします。

対策のポイント

- モバイル PC や USB メモリ、CD などの使用や記憶媒体の外部持ち出しについて、規程を定めているか
- 外部でモバイル PC や USB メモリ、CD などの記憶媒体を使用する場合の紛失や盗難対策を講じているか
- モバイル PC にログオンする際に、利用者 ID とパスワードなどによる認証を実施しているか
- モバイル PC などに保存されているデータを、その重要度に応じて暗号化しているか

解説

モバイル PC の置き忘れや盗難による個人情報の漏えい事件が多く発生しています。モバイル PC や持ち出し可能なメディアのセキュリティについては多くの組織が危機感を持っており、なんらかの対策をとっていますが、まだ十分であるとは言えません。モバイル PC や持ち出し可能なメディアの使用や外部への持ち出しルールを決める際には、それらに記録されている情報の明細を作ることをお勧めします。また、基本的な考え方として、データとアプリケーションの分離という概念も導入する必要があります。これは、データを閲覧するためにはアプリケーションが必要であることから、そのアプリケーションの入手や利用に制限を設けることで、データの閲覧を困難にするという考え方です。

モバイル PC やメディアの持ち出しを禁止している組織も多くありますが、これによって紙媒体の持ち出しが増えてしまったというケースが少なくありません。紙媒体は最も閲覧が容易なデータ形式であると言えます。また、コピーもコンビニエンスストアなどで容易に行うことができるという点で、情報が漏えいした場合の被害が拡大しやすいと考えられます。

PC やメディアに利用者認証機構⁵を導入し論理的なロックをすることも有効な対策の一つです。利用者の認証には、「知っていること (ID、パスワード)」、「持っているもの (USB キー、IC カード)」、「本人の属性 (バイオメトリクス)」という 3 つの要素を組み合わせるよう利用するようにしてください。すべてのモバイル PC やメディアにこれらの対策すべてを導入するのではなく、情報資産の重要度や問題の予想発生頻度に応じて選択することが望まれます。

PC のハードディスクには様々なデータが保存されています。重要な情報が蓄積される場合には、それが蓄積される区画やあるいはハードディスク全体を暗号化し、PC 本体へのアクセス制限に加えて、もう一段深いセキュリティをかけておくことが重要です。

ただし、気をつけなければいけないのは、その暗号化のキーも PC の利用者認証に使用するのと同じキー (ID、パスワード、USB キーなど) で開けられてしまっただけでは意味がないということです。たとえば、部屋に入るまでに鍵のかかるドアが 5 枚あっても、すべてのドアが同じキーで開いてしまうのであれば、ドアが 1 枚しかないのと同じ理由です。

また、外部への持ち出しが容易なモバイル PC の使用や、持ち出し可能なメディアのサーバや PC への接続自体を制限することも検討すべき事項です。

最後に、モバイル PC をネットワークに接続する際のセキュリティについても検討しなければいけません。ルータやファイアウォールなどで守られたネットワーク内であれば、外部から直接攻撃を受けることは少ないでしょうが、PHS や携帯電話を介して直接インターネットに接続しているときは攻撃される危険が非常に高いと言えます。パーソナルファイアウォールを導入するなど、端末単位のセキュリティについても十分に検討する必要があります。

(丁)

⁵ 利用者を識別・認証して、その PC やメディアの利用を制限するメカニズム (例：ハードウェアトークン等)

<p>大項目 4. 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況</p>
<p>①情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理、利用者の識別と認証を適切に実施していますか。</p> <p>（適切な利用者 ID の管理には、利用者 ID の定期的な見直しによる不要な ID の削除や共用 ID の利用制限、単純なパスワードの設定禁止などがあります。）</p>
<p>説明 適切な利用者 ID の管理には、利用者 ID に関する規程の整備、利用者 ID の定期的な見直しによる不要な ID の削除や共用 ID の利用制限、本来必要ではない特権を設定した ID の発見と見直し、見破られやすい単純なパスワードの設定禁止などがあります。</p>
<p>対策のポイント</p> <ul style="list-style-type: none"> ●利用者 ID の登録や削除に関する規程を整備し、利用者の ID を定期的に見直しているか ●不要になった利用者 ID の無効設定漏れがないか、ID の不正利用がないかなどを定期的に点検しているか ●空白のパスワードや単純な文字列のパスワードを設定しないよう、利用者に求めているか ●利用者ごとに ID とパスワードを割当て、その ID とパスワードによる識別と認証を確実に実施しているか
<p>解説</p> <p>適切な利用者管理のためには、利用者の登録・削除に関する手続きを定める必要があります。登録しようとする利用者の権限や正当性の確認と、それを承認するプロセスを定めます。利用者の異動や退職によって利用者 ID が不要になった場合に、その ID が登録されたままになることは避けなければなりません。なぜなら、使用されない利用者 ID は、権限をもたない者によって不正に使用された場合に、それが不正な使用であることをすぐに発見できないことがあるためです。不要な利用者 ID は削除しなければなりません。したがって、不要になった利用者 ID を無効にする設定が漏れなくできているか、ID の不正利用がないかなどを、人事異動などのタイミングで定期的に点検する必要があります。なお、システムによっては最初から ID が組み込まれていることもあります。その場合も不要なら削除する必要があります。</p> <p>一方、利用者 ID をいくら厳密に管理しても、パスワードが設定されていない、あるいは簡単に推測できるようなパスワードが設定されていると、ID を不正に使用される可能性があります。しかし、記憶することが困難なパスワードを設定してしまったためにパスワードを紙に書いて机に張り出しておくなどの行為は本末転倒であり、絶対にあってはなりません。思い出しやすいフレーズなどをうまく利用し、数字や文字だけでなく、記号などを織り交ぜたパスワードを設定するなどの工夫が必要です。また、単純なパスワードを使用しないようにルールを定めるとともに、可能であればシステムの設定で単純なパスワードを排除するようにします。</p> <p>サービスへのアクセスごとに、利用者の ID とパスワードによる識別と認証を実施します。その際、一つの ID を複数の利用者が共有しないようにします。ID が共有されているとパスワードが利用者以外にも広く知れ渡ってしまう傾向にあり、結果的に誰でも情報にアクセスできてしまい、秘密が守れなくなります。また、その ID で情報にアクセスしたのが誰なのかを特定することが困難になります。そのため、情報が漏れる、あるいはシステムが破壊された場合に、ID は特定できても、その ID を使用したのが誰なのかを後から追跡することができず、コンプライアンス違反が発生しても、当事者を見つけることが難しくなります。また、パスワードの変更も困難になります。</p> <p>（丁）</p>

<p>②情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。</p> <p>（適切なアクセス権の管理には、アクセスできる情報システムを利用者ごとに限定すること、利用できる機能を制限すること、利用者のアクセス権をレビューすることなどがあります。）</p>
<p>説明 適切なアクセス権の管理には、あらかじめ方針を定めておき、その方針に基づいてアクセスできる情報システムを利用者ごとに限定すること、利用できる機能を制限すること、利用者のアクセス権をレビューすることなどがあります。</p>
<p>対策のポイント</p> <ul style="list-style-type: none"> ●アクセスを管理する方針を定め、利用者ごとにアクセス可能な情報（データ）、情報システム、業務アプリケーション、サービスなどを適切に設定しているか ●適切な権限付与が行われているか、必要以上の権限付与がないかなど、利用者に与えたアクセス権を定期的にレビューしているか ●特に重要な情報を格納した情報システムについては、一度のアクセスでの利用時間の制限などのアクセス条件による制御を行っているか
<p>解説</p> <p>たとえば人事データを閲覧できる利用者を制限する、あるいは派遣社員と正社員の利用できるサービスを区分するなど、利用者ごとに利用可能なサービスに制限を設けることが必要です。職務と権限に見合ったサービスを利用できるようにするとともに、権限のない者に対する制限を行う必要があります。業務アプリケーションについても、利用の可否だけでなく、同じ業務アプリケーションの中でも参照権限や変更権限などの権限区分を含めて、アクセス制御を行うことが必要です。また参照権限の中でも、一度に参照できるデータの件数を</p>

区別するなどの権限区分を設定することも考えるべきです。役職上の権限に合わせてコンピュータの提供する業務アプリケーションのサービスの利用権限を管理するために、アクセス制御を行います。

職務の変更や異動によって、本来アクセス権限を失ったはずの利用者が、異動前のアクセス権で元の部署の情報や業務アプリケーションにアクセスできてしまう事態を防止するためには、職務の変更や異動に際しては、利用者のアクセス権限を適切に変更するとともに、アクセス権を付与した利用者の範囲が適切か、定期的に見直す必要があります。

サービスへのアクセス中に離席し周囲の監視の目がないような時、不正行為が発生する可能性があります。また、必要以上に長時間の利用は、不正行為を増長させる可能性もあります。したがって、重要情報を格納した情報システムについては、一度のアクセスに対する利用時間を制限して、不正行為の発生を防止することも有効です。

(丁)

③ ネットワークのアクセス制御を適切に実施していますか。

(適切なネットワークのアクセス制御には、たとえばネットワークの分割や外部からの接続時の認証などがあります。)

説明 ネットワークへの接続に伴って、接続したネットワーク経由で侵入されるといったリスクが増大します。そのようなリスクを低減するためには、ネットワークへの適切なアクセス制御が不可欠です。ネットワークのアクセス制御には、たとえばネットワークの分割や外部からの接続時の認証などがあります。

対策のポイント

- 外部のネットワークから内部のシステムへアクセスする際(モバイル PC を使用する場合を含む)に、利用者認証を実施しているか
- サービスや情報システムにアクセス可能な利用者を制限するために、ネットワークを論理的に切り離したり、接続を制限したりしているか
- 許可されていないワイヤレスアクセスポイントの設置を禁止しているか
- 外部の無線 LAN を利用してネットワークにアクセスする場合に、セキュリティ対策を実施しているか
- 内部のネットワークに接続する端末機器について、接続時に認証しているか

解説

外部から内部のシステムへのアクセスを許す場合、利用者認証を実施して正当な利用者であることを確認する必要があります。認証の記録を残し、許可されていない行為(持ち出し禁止のファイルのコピーなど)が行われていないかどうかを利用者ごとに確認します。

また、ハードウェアベンダのリモートメンテナンスや業務提携先との情報交換など、外部の組織と何らかの形でネットワークの接続を行う際には、必要とされる機器や情報にのみアクセスができるよう、アクセス制御が必要です。ネットワークのアクセス制御には、パケットレベル、セッションレベル、アプリケーションレベルなどいくつかのレイヤーがありますが、どの方式にするかはリスク分析を行い、また費用などを勘案して決定します。

保護すべき重要なデータが入っているシステムは、それ以外のシステムが接続しているネットワークから物理的に切り離し、特定の端末あるいはネットワークセグメントからのみ操作できるようにするのが最善の策です。しかし、作業効率の面などを考慮して、便宜上、その他のシステムもつながっているネットワークに接続しなければならない場合もあります。このような場合には、物理的に切り離したのと同等のセキュリティが確保されるように、重要システムとネットワークとの間にファイアウォールを設置し、特定の端末あるいはネットワークセグメントからのみアクセスできるようにする(論理的に隔離する)ことが必要です。

ワイヤレスアクセスポイントを許可なく設置すると、建物の外など、予期しない場所からのアクセスが可能になることがあります。ワイヤレスアクセスポイントは、個別の部署が設置するのではなく、情報セキュリティ担当部署や組織内システムの管理部署の担当者など、セキュリティ上の設定に詳しい者が、正当な許可を得て設置する必要があります。

外部の公衆無線 LAN サービスでは、アクセスしている PC が相互に通信可能となり、互いに共有ファイルなどが参照できる状態になることがあります。これによって、機密データなどの重要データが、第三者によって参照されてしまう場合があります。また、パーソナルファイアウォールなどのセキュリティ対策が実施されていない場合には、ウイルスなどが容易に侵入する可能性があります。外部でネットワークに接続する場合には、PC 自体にセキュリティ対策を施しておく必要があります。

ウイルスの侵入や許可されていないデータの参照などが行われないようにするために、許可されていない PC が組織内ネットワークに接続されることを防ぐ必要があります。接続する PC を限定するためには、ネットワーク接続時に PC の認証を行うことが必要になります。

(丁)

④ 業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。

(自組織での開発、外部委託による開発を問わず、開発の際に必要なセキュリティ対策としては、仕様書にセキュリティ上の要求事項を盛り込むこと、設計や開発に際してぜい弱性を作り込まないように配慮すること、ぜい弱性を残さないための適切なシステム試験を実施することなどがあります。)

説明 業務システムは、完成してしまっただ後に改変を加えることは困難で、コストも高まります。企画、設計などの初期の段階から情報セキュリティについて配慮することが必要です。そのためには、自組織での開発、外部委託による開発を問わず、仕様書にセキュリティ上の要求事項を盛り込むこと、設計や開発に際してぜい弱性を作り込まないように配慮すること、ぜい弱性を残さないための適切なシステム試験を実施することなどが重要です。

対策のポイント

- セキュリティ上の要求事項を仕様書に盛り込んでいるか
- 入力データに対するチェック機能を適切に実装しているか
- 業務処理プロセスを適切に実装しているか
- 情報の保護機能を適切に実装しているか
- 出力データの妥当性や表示メッセージの正しさなどに関するチェックを適切に行っているか
- ぜい弱性を作り込まないために、プログラミング上の配慮がなされているか

解説

業務システムは、一旦完成してしまっただら、後から改変を加えることは困難で、コストも高まります。したがって、企画、設計などの初期の段階から情報セキュリティについて配慮することが重要であり、情報セキュリティ上の要求事項をシステムの仕様書に盛り込むことが必要です。そのためには、どのような人たちが使用するのか、どのような権限の区分があるのか、複数の業務フローの交差(複数の役割を持つ人の存在)など、扱うデータや文書の種類などを整理し、把握しておく必要があります。また、どの利用者がどのような操作を行ったのかをログに記録するなどして、あとから参照できるようにしておくことも大切です。これによって、事故が発生した場合に原因を追究することができるだけでなく、操作のログが残されていることを周知することで、使用者の悪意ある行為を未然に防ぐことにもつながります。

データの入力に際しては、業務処理プロセスに不具合があると、データが正しく入力されても、データ処理が適切に行われないということが起こります。必要な機能の動作確認、誤動作分析、ぜい弱性分析などにより、業務処理プロセスが適切に実装されているかを確認します。要求されていない数値や文字列の入力ができないように制限を設けることも必要です。数値の範囲が決まっている場合や文字の種類が決まっている場合、文字列の長さが決まっている場合などには、条件に合わないデータの入力ができないようなチェックの仕組みを組み込んでおくのが良いでしょう。

読み書きの制限や削除の制限など、システムに記録されている情報(ファイル)の保護機能が実装されている必要があります。利用者ごとに読み書きや削除の制限を変えることは最低でも必要です。その他、利用する形態に応じて、部署単位や職務形態単位など、グループごとに保護機能があることが望ましく、必要に応じてアクセス制限による保護などを実装します。

出力データが妥当であるか、また表示されるメッセージが正確であるかといった観点から検証することも重要です。

システムには、開発時には意図していなかったデータの入力などによって動作が不安定になるぜい弱性が潜んでいる場合があるため、ぜい弱性をチェックするサービスやソフトウェアなどを利用して、潜在的なぜい弱性を取り除いておく必要があります。このとき、どのようなソフトウェアを使い、どのような方法を用いてぜい弱性をチェックしたのかを後でわかるように記録しておきます。

攻撃の手法は年々進化しており、セキュリティ意識が低い開発者によって、コーディング時にぜい弱性を内包してしまうことも多くあります。開発者向けにセキュアなコーディング手法を教育する、あるいは開発ガイドラインを定めておくのもよい方法でしょう。

(丁)

⑤ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。

(選定や購入、開発や保守を外部委託している場合は、セキュリティ上の観点からの点検が可能かどうかを回答してください)

説明 ソフトウェアにセキュリティ上の問題を混入させないための管理が重要です。たとえば、選定や購入に際しては、ソフトウェアの開発元を確認すること、開発や保守に際しては、ソースコードへのアクセス管理といったセキュリティ対策の実施状況の記録やレビューの記録などを確認することが大切です。

対策のポイント

- 運用に供しようとする情報システムのソフトウェアの導入や変更に関する手順を整備しているか
- ソースコードへのアクセスを制限しているか
- 構成の変更に関する手順を整備し、厳重に管理しているか
- トロイの木馬などの不正プログラムが組み込まれていないかどうかをチェックしているか

- 外部委託によるソフトウェア開発を行う場合、使用許諾、知的所有権などについて取り決めているか
- 外部委託によるソフトウェア開発を行う場合、品質や作業範囲、標準となる契約書や合意書を用意しているか
- 開発や保守を外部委託する場合に、セキュリティ管理の実施状況を把握できるか

解説

ソフトウェアやライブラリの更新、パッチ（修正プログラム）の適用などで運用中の情報システム的环境を不用意に変更すると、情報システムの挙動に影響する可能性があります。そうしたリスクを抑えるためには、運用に供しようとする情報システムにおけるソフトウェアの導入や変更に関する手順を整備し、それに沿って対処する必要があります。

ソフトウェアの導入前に、その評価を行い、評価方法や評価内容の記録を残すことが重要です。こうしておくことでぜい弱性が見つかった場合、評価に漏れがなかったかどうかを後で確認することができます。開発元の定評は、ソフトウェアの品質の評価の目安になりますが、新しいベンチャー企業などでもしっかりした開発を行っているケースもありますので、定評は目安としてください。

ソフトウェアを含む情報資産全般の変更記録は基本的な実施事項です。変更記録により、どのような構成のソフトウェアを使用しているのか、新たなぜい弱性が見つかったときに、使用しているソフトウェアがそのぜい弱性を有するバージョンであるかどうかなどを容易に確認できるようになります。変更記録を適切に実施することにより、ソフトウェアの構成管理を行ってください。

システムの開発においては、レビューの実施と記録が特に重要です。開発プロセスを整備することにより、プログラマによる余分なコードの追加、不要なぜい弱性の残留といったことを予防することができます。レビューの項目としては、ソフトウェアの選定・購入に際しては必要なセキュリティ機能が具備されていること、既知のぜい弱性が含まれていないこと、ぜい弱性などに関する情報が提供されることがあげられます。また、設計段階では、リスク分析の結果必要とされるセキュリティ機能が盛り込まれていること、セキュリティに関する運用面の考慮もされていること、システム運用とセキュリティ運用に必要な管理者及び利用者向けの手順書類が明記されていることが挙げられます。開発段階では、開発のための十分な人員やセキュリティを考慮した環境が割り当てられていること、開発及びテスト用の機器やソフトウェアなどの環境が整備されていること、最新の攻撃手法を考慮した十分なテストが実施されていることなどが挙げられます。

各プロセスで生成される記録やドキュメント類、ソフトウェアのソースコードやデータなどの流出、紛失、盗難、改ざんなどを防止する必要があります。関係者以外には秘密にされている情報に権限のない者がアクセスできないようにするとともに、権限があっても不必要に外部に持ち出さないようにするための管理が重要です。

ソフトウェアの選定、購入、システムの開発・保守などの方針は、関係者に周知徹底することも必要です。定めた方針が周知できていることを確認する仕組みを作り、実施状況を把握します。さらに、もし方針と実施状況の間にギャップがあれば、是正処置を行います。

ソフトウェア開発を外部委託する場合、情報セキュリティと関連する項目で契約書に記載すべき項目には、ソフトウェア開発を委託する場合の使用許諾、知的所有権などについての取り決めや、品質や作業範囲に関するものがあります。可能であれば、品質の要求事項に、既知のぜい弱性を含まないようにするなどの条件を入れておくべきでしょう。

また、ソフトウェアの開発・保守を外部委託する場合に、委託先のセキュリティ管理の実施状況について確認する手段を確保することが望まれます。たとえば、情報セキュリティ対策ベンチマークのセルフチェックシートの提出を求めるなどのやり方も考えられます。

(丁)

<p>大項目 5. 情報セキュリティ上の事故対応状況</p>
<p>①万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。 (適切な対策には、たとえばシステムの二重化、バックアップと運用記録の取得、障害対応手順の明確化、外部委託先とのサービスレベルの合意などがあります。)</p>
<p>説明 情報セキュリティの重要な要素の一つである可用性に影響を与える事象のうち、影響の度合いが最も大きいのは、情報システム関連機器の障害であると言っても過言ではありません。情報システムに求められる可用性の条件を満たすためには、可用性に関する要求に対応した適切な障害対策機能の情報システムへの組み込みが欠かせません。</p>
<p>対策のポイント</p> <ul style="list-style-type: none"> ●情報システムの可用性に関する要求は明確で妥当なものか (可用性とは、情報システムを使う権限のある人がいつでも使えるようにすることをいいます) ●障害対策の実行に必要なバックアップ情報の取得や、運用記録などの確保を適切に行っているか ●障害部分の切り離し、縮退運転、情報の回復や情報システムの復旧など、障害発生時に必要となる機能を情報システムに組み込んでおり、それらが適切に機能することを検証しているか (縮退運転とは、提供する機能やサービスの対象者の絞り込みなどにより、障害時でも、必要最低限のサービスを提供できるようにすることを言います) ●障害発生時の対応手順や、障害対策処理の実施要領を策定しているか ●障害対応のスキルに関する教育や訓練を実施しているか ●情報システムの運用を外部に委託している場合、障害発生時にも所定のサービスレベルが維持されることを、委託先との間で相互に確認しているか ●システムの各種ログを取得できているか
<p>解説</p> <p>必要となる障害対策の内容は、可用性、すなわち、情報システムを使う権限のある人が、いつでも使えるようにすることに関する要求の程度によって大きく左右されます。そのため、障害対策の検討に当たっては、まず、対象となるシステムの可用性に関する要求を明確化し、その妥当性をチェックしなければなりません。可用性に関する要求として、次の事項を明確にする必要があります。</p> <ul style="list-style-type: none"> ・ 最低限運用しなければならない時間帯 ・ 情報システムが停止してから復旧・再開までに許される時間の上限（許容停止時間） <p>障害対策を検討する上で最も重要な要素には、次のようなものがあります。</p> <ul style="list-style-type: none"> ・ 対象となる障害の範囲 ・ 障害発生時における、機能の縮退、バックアップ機への切替え、システムの一時停止などの対応 ・ システム停止時の情報の回復や情報システムの復旧の手段 ・ 情報システムが停止した場合や、利用が制限された場合における、業務の遂行方法 <p>これらを中心とした障害対策の仕組みがよく検討されていないと、情報システム部門の対応とユーザ部門の対応に齟齬が生じ、全体としての障害対策が効果的に機能しないことがあります。</p> <p>また、事故への即応処理としてのシステムの切り離し、縮退機能（提供する機能やサービスの対象者の絞り込みなどにより、障害時でも、必要最低限のサービスを提供できるようにする機能）や、情報の回復や情報システムの復旧に必要な機能は、障害発生時に円滑に機能することが確認されていなければなりません。そのためには、障害対策機能に関するテストの実施や、システム環境の変化に対応するための定期的なチェックが必要となります。</p> <p>システムに組み込まれた障害対策機能が正常に実行されるためには、バックアップデータや運用の記録などが必要となります。このため、日常のシステム運用の中で、バックアップデータや運用の記録の確保も欠かせません。</p> <p>また、障害発生時における情報システム部門とユーザ部門の対応は、いずれも日常の運用から見れば大きな例外作業であることから、障害発生時に必要な対応を迅速に行うためには、以下の準備を整えておくことが望まれます。</p> <ul style="list-style-type: none"> ・ 障害検知時の報告要領 ・ 障害対策の実施責任者の設置と作業体制の確保 ・ 障害発生時のシステムの切替え手順や、情報の回復から情報システムの復旧に至るまでの処理手順や操作要領 ・ システム障害発生時における業務実施要領 <p>さらに、両部門の要員が、障害対応作業を適切に実施するためには、関係者への障害対応要領の周知や、必</p>

要なスキルに関する教育や訓練などの実施も重要な課題の一つになります。

外部にシステムの運用を委託している場合、障害発生時においても、所定のサービスレベルが保証されるようにしておくことが必要です。そのためには、委託に当たって、許容停止時間などの要求条件、委託先が障害発生時に実施すべき作業や対応などの事項を明確にしておくことが重要です。

なお、障害の検出や原因分析、対処策の検討などに必要なデータとして、様々なログを収集しておくことも必要です。

(丁)

②情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。

(事件や事故への備えには、そうした万が一の場合にとるべき行動をあらかじめ検討しておくこと、検討した結果を文書にまとめて関係者に周知しておくこと、緊急の連絡網を整備すると共に、必要な要員や資機材を揃えられるようにあらかじめ手配しておくことなどがあります。)

説明 情報セキュリティに関連する事件や事故が発生した場合に、被害の拡大を防ぎ、局所化するためには、事件や事故に必要な対応を組織全体で適切かつ迅速に実施できなければなりません。そのためには、事件や事故を想定し、実施すべき作業やその実施要領を確立するとともに、現場の要員がいざというときに対応作業を円滑に実行できるように準備しておくことが必要となります。また、個人情報などの漏えいが発生した場合に、影響を受ける可能性のある本人への連絡、主務大臣などへの報告、事実関係や再発防止策の公表などを円滑に進めるため、手順などを整備しておくことも重要です。

対策のポイント

- セキュリティにかかわる出来事、事件や事故の発生時の対応について、実施要領を定めているか
- セキュリティにかかわる出来事、事件や事故に関する対応要領を関係者に徹底しているか
- セキュリティにかかわる出来事、事件や事故の発生時の連絡網を含む対応体制を構築しているか
- セキュリティにかかわる出来事、事件や事故への対応に必要なリソースやツールを適切に準備しているか

(ここでのリソースやツールとは、障害対応要員、障害を記録するためのディスク領域、障害報告機能や分析機能などを指します)

解説

事件や事故への対応を迅速かつ適切に行うために、セキュリティにかかわる出来事、事件や事故の種類ごとに以下の準備を整えていることが望まれます。

- ・ 組織内の関係者への報告（誰にどのような報告を行うか）
- ・ 必要に応じて実施すべき緊急処置（ネットワークの遮断、システムや業務の一時停止など）の適用基準や実行手順
- ・ 被害状況の把握（被害範囲や被害の内容など）
- ・ 原因の把握と対策の実施
- ・ 被害者への連絡や外部への周知などのリスクコミュニケーションの体制の確保
- ・ 通常システム運用への復旧手順
- ・ 停止した業務の再開手順

これらの具体的な内容は、個人情報の漏えい、営業機密情報の漏えい、システムや情報の混乱、システムの長時間停止、コンプライアンス違反など、発生した事件や事故の種類によって異なります。このため、事件や事故発生時の対応要領は、それぞれの組織に与える影響が大きいと考えられる事件や事故の形態ごとに定めておかねばなりません。特に個人情報の漏えいの場合、個人情報漏えいの事実を公表することが、個人情報の保護に関する法律についての個人情報保護法に基づく各府省庁のガイドライン等に定められています。

また、情報システム部門やユーザ部門の要員が、事件や事故の緊急時対応作業を適切に実施するためには、関係者への対応要領の周知や、必要なスキルに関する教育や訓練などの実施も重要な課題の一つになります。

さらに、事件や事故の処理には、組織的な対応が不可欠です。このため、日頃から、以下のようなことについての確認も必要となります。

- ・ 緊急連絡網が確立され、常時機能するようになっているか
- ・ 責任者と対応実施体制が決まっており、当事者が自分の責任を認識しているか

事件や事故によっては、被害状況の調査や情報の回復、一時停止したシステムの再開に必要なツールやハードディスク等が必要となるため、事前に準備しておく必要があります。ただし、これらの機器はシステム環境の変化等によって使用できなくなっていたり、普段は使う機会がないために使用に手間取ったりすることがよくあります。そのような事態を防ぐために、これらが正常に稼働することを定期的にチェックすることも必要です。

(丁)

③何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。
(万が一、情報システムが停止してしまった場合に備えて、普段は情報システムで行っている業務をたとえば手作業で代替できるように、そうした業務の手順書や様式類をあらかじめ用意しておくこと、またそうした手作業を実施できる場所や資機材を確保しておくこと、さらに手作業で代替できるように要員を訓練しておくことなどが重要です。)

説明 地震、台風、水害などの自然災害による施設、システム機器、業務アプリケーション、業務データの損壊や、そのほか情報システムに生じた重大事故によって、情報システムが停止し、短期間での復旧の目処がたたなくなるような事態の発生が考えられます。このような状況においても事業の継続ができるようにするためには、情報システム全体をカバーするバックアップセンターの準備や、ソフトウェア資産や業務データのバックアップとその安全な保管、さらには手作業により業務の遂行ができるようにしておくなどの準備が必要となります。事業活動の多くを情報システムに依存している組織においては、事業継続への取組は十分に検討しておくべきです。

対策のポイント

- 情報システムが停止した場合に、自組織の業務に及ぼす影響について検討した事があるか
- 各業務の重要度や、業務システムのトラブルが業務に及ぼす影響について把握しているか
- 情報システムの停止が長期になる場合に備え、業務を継続するための方針やシナリオを策定しているか
- 情報システムの長期停止時に必要となる、バックアップセンターへの切替えや業務の手作業への切替えなどは、何時でも実施できるよう、手順の策定や関係者への周知と訓練を実施しているか
- 外部への連絡など、情報システムが長期停止に陥った場合に必要となるその他の措置についても検討し、実施要領を策定しているか

解説

今日、情報システムのトラブルは、業務プロセスの様々なところに影響する可能性があります。そこで、情報システムが停止した場合に、どのような影響が業務に生じうるかを、検討してみることが重要です。その場合、業務の重要度や、情報システムのトラブルが業務や事業に及ぼす影響の大きさについて分析し、把握していることが必要となります。さらに、情報システムの停止が長期化した場合を考慮すれば、どの業務を優先して継続させるべきか、そのための方針やシナリオ（事業継続計画）を策定しておくことが求められます。

また、事業継続計画が非常時及び復旧後の事業活動に大きな影響を及ぼすことを考えれば、計画には経営陣の承認も必要です。

バックアップセンターを用いてシステム運用を継続するようにしている場合は、バックアップセンターへの切替えが円滑に行われるようにするため、日頃から、以下のような備えが必要となります。

- ・ バックアップセンターにおける必要なシステム、運転体制の準備
- ・ バックアップセンターへの切替え要領の確立
- ・ バックアップセンターへ切替るために必要となる機能やツールの準備
- ・ バックアップセンターへの切替えに関わる要員に対する教育や訓練による対応能力の確保

障害発生時には、現用の業務データも失われていることも多いため、バックアップセンターへの切替え時や復旧後の業務再開の際に用いる業務データやソフトウェアを他の安全な場所で保管するようにしておくことも必要となります。

バックアップセンターを準備していない場合や、バックアップセンターへの切替えがうまく行えない場合には、情報システムに頼っていた業務を手作業での実施に切替えなければなりません。業務処理を手作業で行えるようにするためには、日頃から、以下のような備えが必要となります。

- ・ 手作業での業務処理要領の整備
- ・ 手作業での業務遂行時の体制やオフィスの使用方法などの検討
- ・ 手作業による業務に用いる台帳などの必要な情報の日頃からの準備

(丁)