テレワークセキュリティガイドライン
解説書

平成１６年１２月

総務省

－目次－

本書の位置付け

本書は、「テレワークセキュリティガイドライン（以下、ガイドラインと記述する）」を補完するための解説書です。本書では、ガイドラインに記載された事例や考え方について、より詳細に説明し、テレワークに関する情報セキュリティ対策を行ううえでの具体的な実施内容や留意点などを掲載しています。

ガイドラインを読了いただき、「情報セキュリティに対して更に興味を持たれた方」、「ガイドラインに物足りなさを感じた方」、「テレワークを導入するうえで更なる知識を身に付ける必要がある方」は、是非、本書を活用してください。

本書の読み方

本書では、ガイドラインの流れに沿って解説していきますが、ガイドライン部分と解説部分を一目で見分けられるように、ガイドライン部分をグレー（  ）で囲んでいます。

また、本解説書のうち、どの部分を参照すべきなのかを「テレワーク実施形態別参照項目」に示しています。次ページの「テレワークの実施形態」に目を通していただいたうえで、P.３の「テレワーク形態の分類」をご覧いただき、該当する形態を選択してください。該当形態の記号をP.４の「テレワーク実施形態別参照項目」の一覧表に当てはめていただくことにより、解説書のどの部分を参照すればよいのかを判断することが可能です。

なお、本書の読み方については、以下をご覧ください。

（※）

⇒ 説明が必要な用語については、文中の用語の後に（※）を付けて記載し、巻末の用語集で解説しています。

（解説）

⇒ ガイドラインの内容について、「なぜそうするのか」等について解説しています。

（実施方法）

⇒ ガイドラインの内容について、「どのように」実施するのか、または「何をポイントに」実施するのかを解説しています。

HOW TO 編

⇒ 技術的実施方法を中心に、「どのように」実施すればよいかについて、「HOW TO 編」にまとめて記述しています。

テレワークの実施形態

テレワークには以下のように様々な実施形態が存在しますが、それぞれ注意すべき情報セキュリティ事項が異なります。以下では、３つのテレワーク実施形態について説明したうえで、それぞれの形態における情報セキュリティ上の留意点について記述します。

● 施設利用型テレワーク

ICT（※）を活用して、テレワークセンター（テレワークを行うために設けられた施設）や立ち寄り型オフィスなど、自宅を除いた勤務先以外の施設を就業場所とするテレワーク。

【情報セキュリティ上の留意点】

テレワークセンター等においては、適切な情報セキュリティ対策が行われている拠点もあり、自宅利用型やモバイル型と比較して安全性の高い通信環境が用意されている場合が多いと言えます。しかしながら、施設利用型テレワークは、不特定多数のテレワーク勤務者と施設を共有することになるため、以下の脅威に対して特に注意しなくてはなりません。

- ソーシャルエンジニアリング（※）による盗聴
- 端末の盗難による情報漏えい

● 自宅利用型テレワーク

ICT を活用して、自宅を就業場所とするテレワーク。近年、ブロードバンドが急速に普及し、一般家庭でも比較的容易にテレワークを実施することが可能となってきています。

【情報セキュリティ上の留意点】

自宅でインターネットを利用し、テレワークを行う場合は、ウイルス・ワーム（※）など、外部からの不正な攻撃から情報資産を守るための情報セキュリティ対策を行ったうえで、安全な通信経路を確保しなければなりません。以下に、特に注意すべき脅威を記述します。

- ウイルス・ワーム感染
- 悪意ある第三者による不正アクセス（※）
- 踏み台（※）やなりすまし（※）を利用した不正侵入（※）

● モバイル型テレワーク

ICT を活用して、施設に依存せず、いつでも、どこでも仕事が可能な状態のテレワーク。近年、モバイルパソコンが普及し、携帯電話や無線 LAN（※）によるアクセスが容易となったことにより、モバイル型テレワークが急速に普及しています。

【情報セキュリティ上の留意点】

モバイル型テレワークにおいて通信を行う場合には、①「インターネットを利用する形態」と、②「ダイヤルアップにより通信経路を確立する形態」の２つの

パターンが想定されます。①については、前述した自宅利用型テレワークにおける脅威に加え、「端末の紛失・盗難による情報漏えい」について特に注意しなければなりません。②については、インターネットを利用するわけではないため、①と比較すると脅威は薄れますが、的確な対策を施す必要があります。以下に、特に注意すべき脅威を記述します。

- 端末の紛失・盗難による情報漏えい
- ウイルス・ワーム感染
- 悪意ある第三者による不正アクセス
- 踏み台やなりすましを利用した不正侵入

● オンライン

オンラインとは、パソコンがインターネットや LAN などのネットワークにつながっている状態のことを指します。

テレワークにおけるオンライン環境では、電子メール・Web・グループウェア（※）などを利用した業務が想定されます。

● オフライン

オフラインとは、パソコンがインターネットや LAN などのネットワークにつながっていない状態のことを指します。

テレワークにおけるオフライン環境において行われる対象業務としては、プログラム開発、会計業務、翻訳、データ入力などが想定されます。

テレワーク形態の分類

以下の表では「テレワークの実施形態」で記述したそれぞれのテレワーク形態をオンライン／オフラインの区分で分類しています。

表１　テレワーク形態分類表

	オンライン (ネットワークを利用する)	オフライン (ネットワークを利用しない)
施設利用型テレワーク	A	B
自宅利用型テレワーク	C	D
モバイル型テレワーク	E	F

テレワーク実施形態別参照項目

前項で分類されたテレワーク実施形態別に、必要とされる情報セキュリティ対策を表で整理しています。該当する記号に沿って、参照すべき対策項目をご覧ください。

表２　テレワーク実施形態別参照項目

対策項目	A	B	C	D	E	F
１．情報セキュリティの基本的な考え方						
(ア)情報セキュリティ対策について						
・情報セキュリティポリシーの策定	◎	◎	◎	◎	◎	◎
２．「ルール」についての対策						
(ア)組織として遵守すべきルール	◎	◎	◎	◎	◎	◎
(イ)システム管理者に遵守させるべきルール	◎	○	◎	○	◎	○
(ウ)テレワーク勤務者に遵守させるべきルール	◎	◎	◎	◎	◎	◎
３．「人」についての対策						
(ア)情報セキュリティ教育・啓発活動	◎	◎	◎	◎	◎	◎
(イ)規則・契約による管理	◎	◎	◎	◎	◎	◎
(ウ)情報セキュリティ事故発生後の対応	◎	◎	◎	◎	◎	◎
４．「技術」についての対策						
(ア)テレワーク端末における対策						
・ウイルス・ワーム感染防止対策	○	△	◎	○	◎	○
・端末等の紛失・盗難対策	○	○	○	○	◎	◎
・不正侵入・踏み台対策	○	ー	◎	ー	◎	ー
(イ)通信経路における対策	○	ー	◎	ー	◎	ー
(ウ)社内システムにおける対策						
・ウイルス・ワーム感染防止対策	○	ー	◎	ー	◎	ー
・ウイルス・ワーム蔓延防止対策	○	ー	◎	ー	◎	ー
・不正侵入・不正アクセス対策	○	ー	◎	ー	◎	ー
・情報漏えい対策	○	ー	◎	ー	◎	ー

◎特に注意してご覧ください
○注意してご覧ください
△目を通すことをお薦めします

はじめに

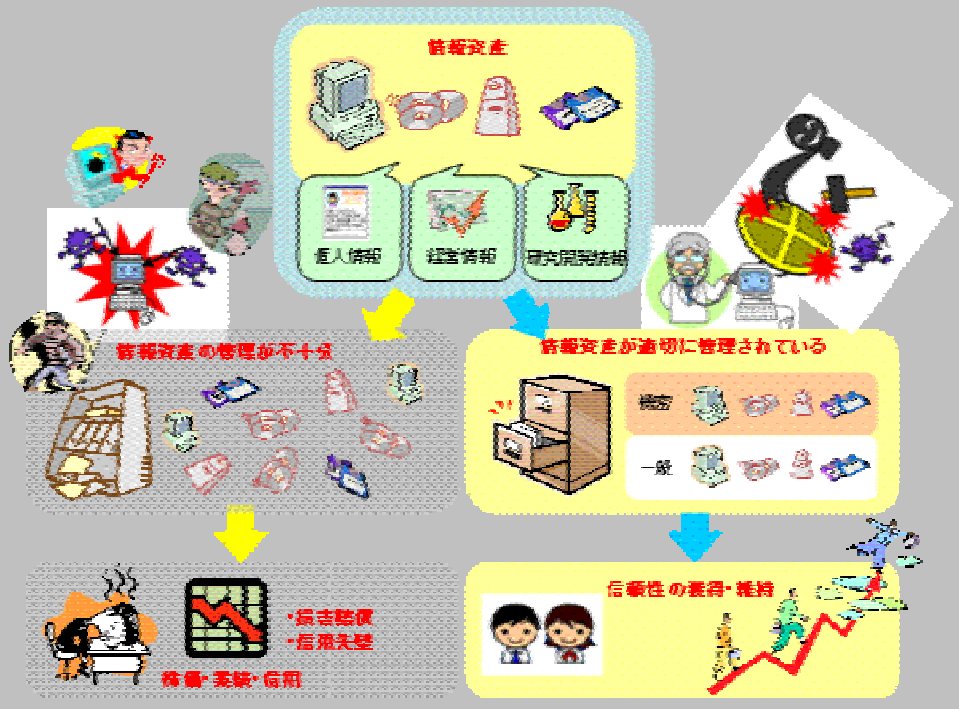
ICT 技術の進歩により、今日の企業活動においては、企業は様々な情報資産（電子データ、紙文書、情報システム等）を保有し活用しています。

これらの情報資産は企業活動において非常に重要な位置を占めるまでに至っていますが、その多くは、「電子データ」として管理されています。電子データは紙媒体とは異なり、「容易にコピー可能」、「改ざん検知が困難」、「直接目に見えない」等の特性があるため、電子データの管理は、紙媒体の管理と比較すると、脅威の存在が格段と大きくなっているとも言えます。一旦、電子データの破壊・改ざん、システム停止や情報漏えいなどの情報セキュリティ事故が発生してしまうと、その企業において企業活動が停止するだけでなく、社会的な影響も発生し、信用失墜に発展するなど多大な損害が生じてしまうおそれがあります。

◆情報セキュリティ事故の例
- 社員が電車の網棚に、顧客情報の保存されているノートパソコンの入ったカバンを置き忘れたことが原因で大量の顧客情報が漏えいした。
- テレワークを実施する際、ウイルス対策ソフトの定義ファイルを最新のものに更新していなかったため、新種のウイルスに感染してしまった。

現実の情報セキュリティ事故がもたらす被害については、直接的・間接的、顕在的・潜在的、短期、中長期など、いくつかの要素がありますが、例えば情報漏えい事件による顕在的・短期的な損害賠償額だけでも、組織に莫大な影響を与えることとなります。また、個人情報の保護に関する法律（※１）の施行も予定されており、情報の安全な管理義務について違反した場合は、行政による処分が下される場合もあります。

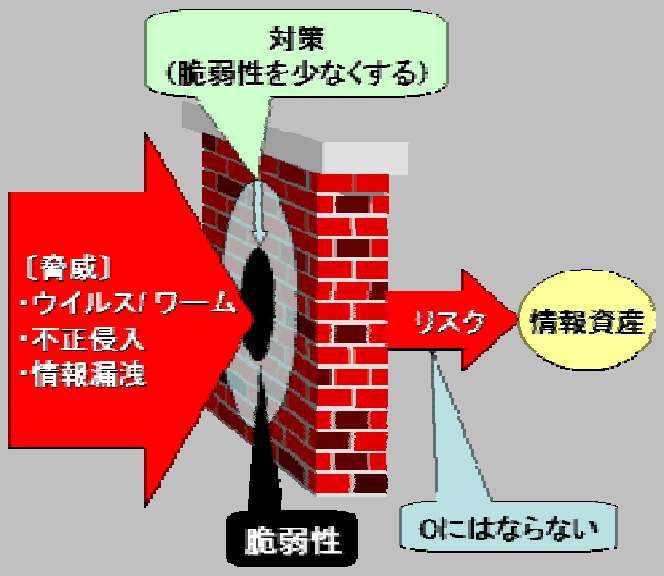
図１　情報セキュリティ対策の必要性



※１　個人情報の保護に関する法律…個人の情報と利益を保護するために、個人情報を取得し取り扱っている事業者（過去 6 ヶ月間継続して 5000 件を超える個人情報を取り扱う者）に対し、利用目的の特定及び制限、適切な取得、取得に際する利用目的の通知、または公表、安全管理、第三者提供の制限などの義務と対応を定めた法律です。これらに違反した場合、行政処分を下され、さらに主務大臣の命令に反した場合には罰則が適用されることになります。2005 年 4 月より全面施行が予定されています。

このような社会的背景を踏まえ、今日の企業活動においては、そこで扱う情報資産を洗い出し、その取扱いに対して、どのような脅威や脆弱性（弱点）、リスクがあるのかを十分に把握、認識したうえで、しかるべき対策を実施する必要があります。

（参考）図２　脅威、脆弱性、対策及びリスクの関係図



★情報資産が存在する環境には必ず何らかの弱点があります。情報セキュリティでは、その弱点を「脆弱性」、弱点を突く行為を「脅威」と呼び、弱点を攻められる危険性のことを「リスク」と呼びます。脅威から情報資産を守るためには、適切な「情報セキュリティ対策」を講じ、脆弱性を減少させることにより、リスクを回避する必要があります。しかしながら、十分考慮したうえで対策を行っても、リスクをゼロにすることはできないため、適宜対策の見直しを行う必要もあります。

（解説）

● 情報資産

情報資産とは、組織がその価値を認識しているもので、何らかの保護を必要としているシステム全体の構成要素またはその一部のことを指します。従って、単にハードウェアやソフトウェアのみならず、様々なものから構成されています。

例）

- 情報、データ（例：顧客情報、商品情報 等）
- ハードウェア（例：パソコン、サーバ（※）等）
- ソフトウェア（例：OS（※）、アプリケーションソフト等）
- 通信設備（例：電話、光ファイバ 等）
- 記録媒体（※）（例： CD-R（※）、DVD-RAM（※） 等）
- 書類（例：契約書、規定集 等）
- 施設、設備（例：社屋、電源 等）

- 人員（例：正社員、派遣社員、契約社員、顧客 等）
- 商品、製造物（例：開発成果物、商品 等）
- サービス（例：情報提供サービス、計算処理サービス 等）
- 組織イメージ（例：企業イメージ、評判、信用 等）

● 脅威

脅威とは、情報資産に影響を与え、損失を発生させる直接の要因となる事故や不正行為などを指します。

例）

- ウイルス・ワーム感染、蔓延
- 不正侵入・不正アクセス
- 端末の紛失・盗難
- 盗聴・改ざん
- 情報漏えい
- 天変地異
- 停電
- 人的ミス
- ソフトウェアの不正利用
- 内部者による不正犯罪

● 脆弱性

脆弱性とは、情報資産が存在する環境において、情報セキュリティ上の問題となる可能性がある弱点のことを指します。多くの場合は、OS やソフトウェアのセキュリティホール（※）などが脆弱性となりますが、設定ミスや管理体制の不備なども脆弱性の一つとなることがあります。

例）

- ウイルス対策ソフト（※）を導入していない
- 端末を適切に管理できていない
- 重要な情報資産に対する保護が十分でない
  （暗号化（※）をしていない、アクセス制御（※）を実施していない　など）
- パスワード（※）管理が徹底されていない
- 情報セキュリティ管理体制が構築されていない
- 従業員の情報セキュリティに対する意識レベルが低い

● リスク

システムやネットワークに期待される状態、つまり正常な状態が、事故や不正行為などによって変動し、差異が生じたときに損失が発生します。情報セキュリティ上のリスクとは、この損失が生じる可能性を指します。

● 情報セキュリティ対策

情報セキュリティ対策とは、情報資産を取り巻く環境に存在する脆弱性を減少させる手段を講じることです。様々な脅威を未然に防ぎ、情報財産を構成する CIA（機密性、可用性、完全性）を維持するためにも適切な情報セキュリティ対策を行う必要があります。

⇒　「CIA について」は、P.２７を参照してください。

１．情報セキュリティの基本的な考え方

（ア）情報セキュリティ対策について

では、適切な情報セキュリティ対策とは何を実施すれば良いのでしょうか。情報セキュリティ対策を行ううえで、企業として重要視しなければならないことは、「情報セキュリティポリシー」の策定です。

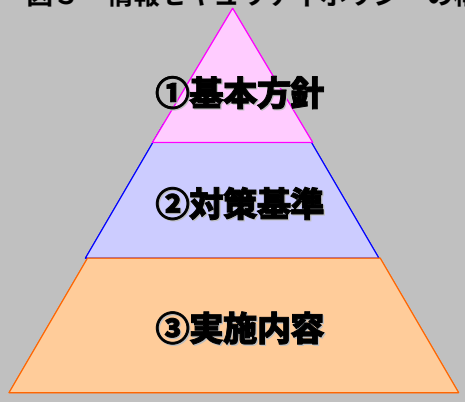
情報セキュリティポリシーとは、その企業で行うべき「情報セキュリティに関する方針や行動指針」を意味し、組織として統一のとれた情報セキュリティレベルを保つために策定するものです。

情報セキュリティポリシーは、図３の通り①全体の根幹となる「基本方針」、②基本方針に基づき実施すべきことや守るべきことを規定する「対策基準」、③対策基準で規定された事項を具体的に実行するための手順を示す「実施内容」の３つの階層で構成されています。（注）

情報セキュリティポリシーの策定に当たっては、第一に考慮すべきこととして、まず「基本方針」を明確に定める必要があります。

基本方針に記述される内容は、その企業の企業理念、経営戦略、企業規模、保有する情報資産、業種・業態などにより異なるため、自社の企業活動に合致した情報セキュリティ行動指針となる基本方針を定める必要があります。

図３　情報セキュリティポリシーの構成



注　情報セキュリティポリシーは、①「基本方針」のみを指す場合も、①「基本方針」と②「対策基準」の２つを指す場合も、①「基本方針」、②「対策基準」、③「実施内容」のすべてを指す場合もあり、前述した ISO/IEC17799 においては、①「基本方針」を「ポリシー」と呼んでいます。しかし、本ガイドラインにおいては、①②③のすべてを含む概念として情報セキュリティポリシーという用語を用います。

（解説）

「基本方針」、「対策基準」、「実施内容」策定時のポイントを紹介します。

①「基本方針」

基本方針には、組織や企業の代表者による「なぜ情報セキュリティが必要であるのか」や「どのような方針で情報セキュリティを考えるのか」、「顧客情報はどのような方針で取り扱うのか」といった宣言が含まれます。本書に基本方針の事例があるので参照してください。

⇒　「情報セキュリティ基本方針」（例）については、P.１３を参照してください。

②「対策基準」

対策基準は、具体的な情報セキュリティ対策を検討する際に参照される規定の集まりです。そのため適用範囲（対象者、対象システム）や対策要求レベル等を明確に記述します。本書では、テレワークに関連する対策基準として以下の事例を示します。本事例はあくまでテレワークに関連する部分の事例であり、すべての内容を網羅したものではないことをご了承ください。

対策基準例

- 「ウイルス対策基準」（例）
- 「ハードウェア／ソフトウェア対策基準」（例）
- 「リモートアクセス（※） 対策基準」（例）
- 「クライアント端末対策基準」（例）

⇒　上記の「対策基準例」については、P.９９の「参考資料４：情報セキュリティポリシーにおける対策基準（例）」を参照してください。

③「実施内容」

実施内容には、それぞれの対策基準ごとに、実施すべき情報セキュリティ対策の内容を具体的に記載します。本書ではガイドラインに沿って、最低限実施すべき実施事例を示しています。

⇒　実施内容の推奨事例については、後述する「ルール」、「人」、「技術」の各項の対策を参照してください。

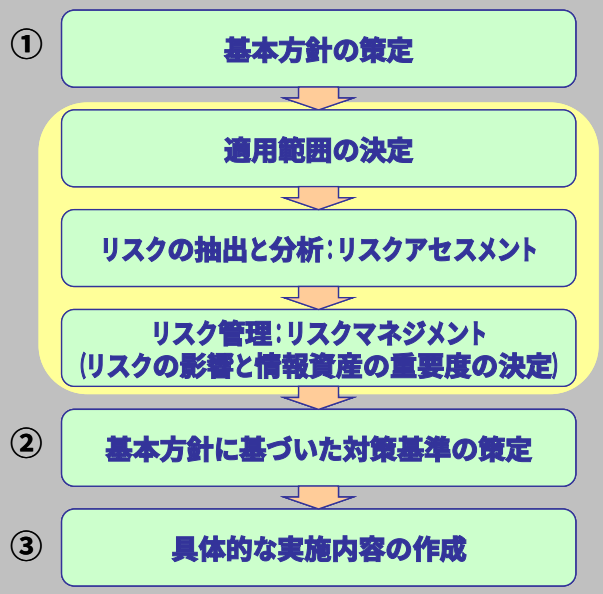
図１　情報セキュリティポリシーの例

基本方針については策定例を示しましたが、その後、どのように対策基準、実施内容を策定すれば良いのでしょうか。本ガイドラインでは、「情報セキュリティマネジメントシステム（ISMS）(※５)」の概念に基づき情報セキュリティポリシーを作成する方法を簡単に紹介します。

図４では、情報セキュリティマネジメントシステムの概念に則して、①基本方針の策定から②対策基準の作成、③実施内容の作成までを実施する手順について示しています。技術的に情報セキュリティ保護要件(※６)を完全に満たすことは難しいとともに、情報セキュリティ対策には費用が発生します。よって企業が持つ情報資産の重要度や特質を考慮した②対策基準、③実施内容を決定する必要があります。(この作業を「適用範囲の決定」、「リスクアセスメント」、「リスクマネジメント」といいます。) このように、適切な「自己分析」に基づいた、しかるべき情報セキュリティポリシーを策定することが重要です。

※５　情報セキュリティマネジメントシステム･･･企業や組織が情報セキュリティを確保・維持するために情報セキュリティ管理体制を構築し、継続的にリスクを管理していく枠組みのこと。ISMS（Information Security Management System）とも呼ばれています。

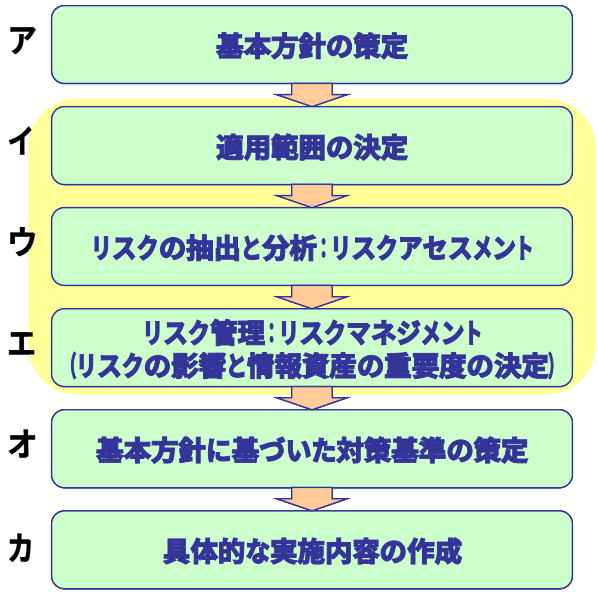
図４　情報セキュリティマネジメントシステム（ISMS）に基づいた情報セキュリティポリシー策定手順



（解説）

ガイドラインの図４では、情報セキュリティマネジメントシステムの概念に基づいた情報セキュリティポリシーについて、①基本方針の策定から②対策基準の作成、③実施内容の作成までを実施する手順について紹介しましたが、本書では、図２の流れに沿って、それぞれの記載例または実施手順を解説します。

図２　情報セキュリティマネジメントシステムに基づいた
情報セキュリティポリシー策定手順



ア．基本方針の策定

基本方針の策定においては、企業や組織が自身の情報セキュリティを確保・維持するために、どのような基本方針のもとに情報セキュリティを確保していくのかを明確にすることが必要です。また、情報セキュリティを確保・維持するためには、企業や組織全体の取り組みとして活動することが重要です。そのため、企業であれば経営層、組織であればそのトップの職位の方により、基本方針を宣言することが望ましいとされています。

「なぜ、情報セキュリティを確保・維持しなければならないのか」は、企業や組織により異なります。そのため基本方針の内容も異なってきますが、参考として次項に基本方針の事例を示します。

情報セキュリティ基本方針の例

200X 年 XX 月 XX 日

情報セキュリティ基本方針（例）

（宣言文）

昨今、機密情報の漏えいやウイルス・ワームの感染による被害などの問題がクローズアップされているが、当社においては、このような事故の発生を防ぐためにも、近年の情報化・ネットワーク化の進展に見合った適切な情報セキュリティ対策を行う必要がある。そこで、当社が法令に準拠し情報セキュリティを重視することをここに宣言し、情報セキュリティ水準の向上を目指す。

１． 定義

(1) 脅威

情報資産に影響を与え、損失を発生させる直接の要因となる事故や悪意ある行為など。

(2) 脆弱性

情報資産が存在する環境において、情報セキュリティ上の問題となる可能性がある弱点のこと。

(3) リスク

システムやネットワークに期待される状態、つまり正常な状態が、事故や不正行為などによって変動し、差異が生じたときに損失が発生する。この差異が生じる可能性のことを指す。

(4) 情報セキュリティ基本方針

当該基本方針を指し、当社の情報セキュリティの方針を示すもの。

(5) 情報セキュリティ対策基準

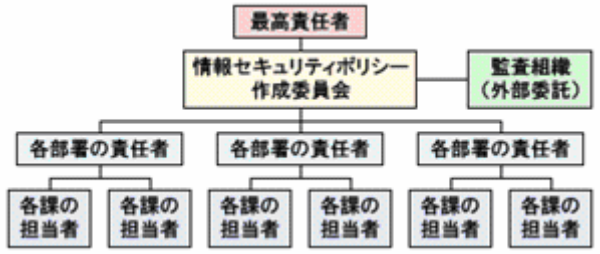
社員が行動規範として遵守しなければならない共通のルールを定める。基本方針の枠組みに応じて規定される文書である。

(6) 情報セキュリティ実施内容

情報セキュリティ実施内容は、対策基準の下層に位置する文書である。対策基準で記述された文書をより具体的に、配布すべき対象者ごとに内容をカスタマイズして記述するものである。

２．体制

当社の情報セキュリティ管理体制を以下の通り定める。



3．情報セキュリティ対策

(1) 人的セキュリティ

情報セキュリティに関する権限や責任を定め、すべての従業員及び委託契約社員に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が行われるように必要な対策を講ずる。

(2) 技術的セキュリティ

ウイルス･ワーム、不正アクセス、情報漏えい等の脅威から情報資産を保護するため、ウイルス･ワーム対策、不正アクセス対策等の技術的な対策を講ずる。また、システムやネットワークの監視等、運用面での対策を講ずる。

4．適用対象者

当基本方針は、原則として当社において業務を遂行する者のすべてに適用される。

具体的には、以下の通りである。

･経営層
･従業員
･協力会社社員
･情報セキュリティ管理者
･システム管理者

5．適用対象者の義務

(1) 同意の義務

情報セキュリティ基本方針の適用対象者は、自分に課せられた情報セキュリティ対策基準及び情報セキュリティ実施内容をよく理解したうえで、同意の意思表示をしなければならない。

(2) 遵守の義務

情報セキュリティ基本方針の適用対象者は、情報セキュリティ対策基準及び情報セキュリティ実施内容をよく理解し、遵守しなければならない。

6．罰則

社員の過失によって、当社の情報セキュリティに対し、重大な損害を与えた、もしくは与えかねない悪質な行為が認められた場合は、就業規則等に準じその処分を決定する。

7．監査の実施

情報セキュリティポリシーが正しく遵守され、有効に機能しているかどうかを検証するため、定期的にセキュリティ監査を実施する。

8．評価及び見直しの実施

情報セキュリティポリシーの有効性を保持するため、セキュリティ監査の結果や情報通信技術の進展に合わせ、適宜、情報セキュリティポリシーの見直しを図り、最善の方策を追求する。

イ．適用範囲の決定

「基本方針」が決まった後は、情報セキュリティポリシーの適用範囲を決定します。企業や組織が自身の情報セキュリティを確保・維持するためには、どのような基本方針のもとに情報セキュリティを確保していくのかを明確にし、それがどの組織、業務等に適用するかを決める必要があります。以下に適用範囲を決めるポイントの事例について示します。

◆ 実施方法

図３　情報セキュリティポリシーにおける適用範囲の定義事例

業務	情報セキュリティポリシーの対象となる業務について定義します。 例：テレワークによるプログラム開発、データエントリー作業、契約業務等
組織	テレワークを実施する企業および組織を定義します。 例：○○会社、○○事業部等
場所	情報セキュリティポリシーの対象となる場所を定義します。 例：企業、組織、チームの所在地、テレワーク勤務者の自宅、サテライトオフィス等
資産	テレワークで取り扱う情報資産を定義します。 例：パソコン、メール、ファイル、記録媒体等

ウ．リスクアセスメント

情報セキュリティポリシーの適用範囲を定めた後は、「リスクアセスメント」を実施する必要があります。

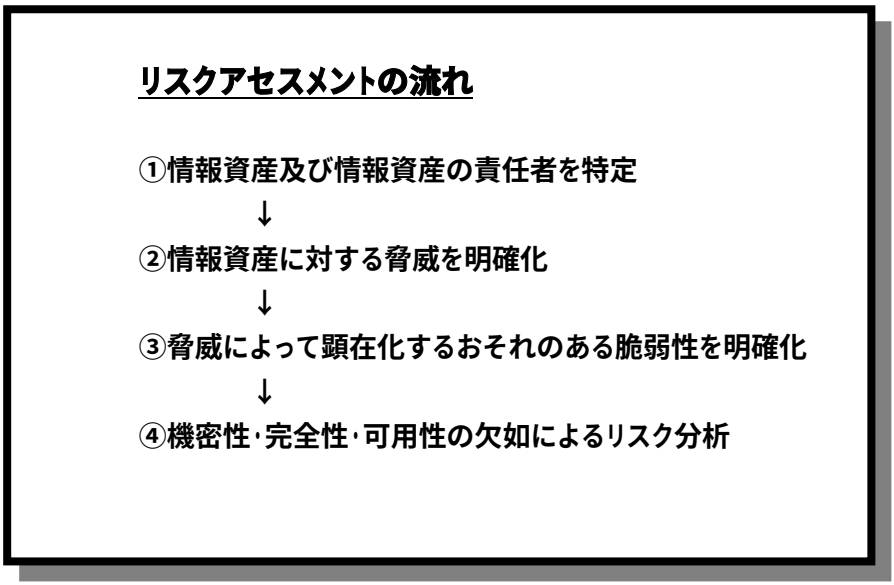
リスクアセスメントとは、それぞれの情報資産に対する脅威及び脆弱性を明確にし、リスクが顕在化した場合の影響（損害額や被害）と、脅威及び脆弱性の程度に応じた発生の可能性を算定することであり、機密性、完全性、可用性をもとに情報資産を評価します。

組織の各部署や担当において、それぞれが保有する情報資産について適切なリスクアセスメントがなされるためには、それぞれの実施者によりリスクアセスメントに適切な結果が得られるように、組織として統一の手順、決定方法等を定めて作業を行っていくことが重要です。

●リスクアセスメントの流れ

情報資産とその責任者を特定し、その情報資産に対してどのような脅威があり、その脅威によって顕在化する脆弱性が考えられるのかを把握します。そして、脅威を評価した結果、事業がどのような影響を受けるかを明確にします。

図４　リスクアセスメントの流れ



①情報資産及び情報資産の責任者を特定

当該作業は、組織が資産の価値及び重要度に対応した保護のレベルを設定していくために必要な作業です。情報資産とその責任者は、資産目録を作成しながら特定することをお勧めします。資産目録には「情報資産の管理責任者」、「保管形態」、「保管場所」、「保管期間」、「廃棄方法」、「用途」、「利用者の範囲」などが含まれます。

表３　資産目録の例

資産区分	資産名	管理責任者	保管形態	保管場所	保管期間	破棄方法	用途	利用者の範囲
ハードウェア	テレワーク用パソコン	システム部長	社内および在宅で利用	社内又は在宅対象者宅	10年	データ完全消去後破棄処理	サーバアクセス用及び、ドキュメント作成	情報システム担当
ハードウェア	業務用サーバ	システム部長	サーバルーム内稼動	サーバルーム	10年	データ完全消去後破棄処理	業務システム用サーバ	情報システム担当
ハードウェア	社内システムアクセス制御機器	システム部長	サーバルーム内稼動	サーバルーム	10年	データ完全消去後破棄処理	社内システムアクセス認証制御	情報システム担当
情報	顧客管理データ	営業部長	電子データ	顧客データベース	15年	データ消去	顧客管理	営業担当者
情報	売上データ	営業部長	電子データ	売上データベース	15年	データ消去	企業戦略、事業計画策定	経営企画担当
ソフトウェア	業務用ソフトウェア	システム部長	電子データ	CD-ROMファイルサーバ	15年	媒体粉砕データ消去	業務A用システムソフト	情報システム担当
設備	サーバルーム	システム部長（設備管理者兼務）	電源、空調管理が装備	ビル内	20年	ビル撤去	業務システム用サーバ社内システムアクセス制御機器	情報システム担当

なお、資産目録には、情報資産のライフサイクルを明確にするために、収集・利用・破棄などの項目についても記述する場合があります。

②情報資産に対する脅威を明確化

組織及びシステムに対して被害や損失をもたらす潜在的な原因を明確にするために、脅威を洗い出します。

表４　脅威の一覧表の例

具体的な脅威	脅威発生の頻度
台風、火事、地震	レベル１
停電、漏水、空調故障	レベル１
パソコン紛失、盗難	レベル３
サーバオペレータ操作ミス、パソコン操作ミス	レベル２
サーバ故障、ネットワーク機器誤動作、社内ネットワーク障害、回線障害	レベル２
ウイルス・ワーム感染、ウイルス・ワーム蔓延	レベル３
不正アクセス（ネットワーク、業務システム）、踏み台	レベル２
ソフトウェアの不正利用、記録媒体の不正使用	レベル２
改ざん、盗聴、紛失、情報漏えい	レベル２
記録媒体の劣化	レベル２

※「脅威発生の頻度」の分類例

レベル３：発生する頻度が高い。（目安として、3ヶ月に1回もしくはそれ以上）

レベル２：発生する可能性はあり。（目安として、半年もしくは1年に1回程度）

レベル１：発生する可能性がほとんどない。（目安として、5年に1回程度発生）

③脅威によって顕在化するおそれのある脆弱性を明確化

　脆弱性とは、脅威を顕在化させる情報資産が持つ弱点やセキュリティホールを意味します。そのため、脆弱性は情報セキュリティ管理対策を適用すべき部分とも言えます。情報資産ごとに、その脆弱性と関連する脅威を洗い出して明記します。

表５　脆弱性の一覧表の例

資産名	脆弱性	関連する脅威	脅威発生の頻度	顕在化のレベル
顧客管理データ／コンサルティングデータ	誰でも読み込めるデータである／コピー・持ち出しが容易	盗聴	レベル２	レベル２
	誰でも読み込めるデータである／コピー・持ち出しが容易	盗難	レベル３	レベル２
	バックアップをしていない	記録媒体の劣化	レベル２	レベル３
業務ソフトウェア（OSも含む）	セキュリティホール	不正アクセス／改ざん／情報漏えい	レベル２	レベル２
	アクセス制御をしていない	不正アクセス／改ざん／情報漏えい	レベル２	レベル３
	不要なアカウント（※）／パスワード管理が不徹底	不正アクセス／改ざん／情報漏えい	レベル２	レベル３
	ソフトウェア資産管理をしていない	ソフトウェアの不正利用	レベル２	レベル３
	バージョンアップをしていない	不正アクセス／改ざん／情報漏えい	レベル２	レベル３
	利用ログ（※）を取得していない	不正アクセス／改ざん／情報漏えい	レベル２	レベル３
業務用サーバ・社内システムアクセス制御機器	壊れやすい、熱に弱い	データ損失／記録媒体の劣化故障、誤動作、障害	レベル２	レベル２
	ウイルス対策ソフトを導入していない	ウイルス・ワーム感染、ウイルス・ワーム蔓延	レベル３	レベル２
	設定ミス（アクセス権、アカウント情報）	不正アクセス／改ざん／情報漏えい	レベル２	レベル３
	物品管理をしていない	盗難	レベル３	レベル２
	保守契約なし	故障	レベル２	レベル２
	操作方法の教育をしていない	サーバオペレータ操作ミス	レベル２	レベル２
	リソース管理をしていない	サーバ障害／社内ネットワーク障害	レベル２	レベル３
	バックアップをしていない	記録媒体の劣化	レベル３	レベル２
配布パソコン	壊れやすい、熱に弱い	データ損失／記録媒体の劣化故障、誤動作、障害	レベル２	レベル２
	ウイルス対策ソフトを導入していない	ウイルス・ワーム感染、ウイルス・ワーム蔓延	レベル３	レベル３
	設定ミス（アクセス権、アカウント情報）	不正アクセス／改ざん／情報漏えい	レベル２	レベル３
	物品管理をしていない	盗難	レベル３	レベル３
	保守契約なし	故障	レベル２	レベル３
	操作方法の教育をしていない	パソコン操作ミス	レベル２	レベル３
	持ち出しやすい	盗難、紛失	レベル２	レベル３
	バックアップをしていない	記録媒体の劣化	レベル３	レベル３
サーバルーム	災害に弱い	台風／火事／地震	レベル１	レベル２
	戸締り不備、物理侵入が容易／入退室・入館管理をしていない	不正アクセス／ソフトウェアの不正利用／記録媒体の不正使用／盗難	レベル２	レベル２
	ファシリティーが充実していない	停電／漏水／空調故障	レベル１	レベル２
	ファシリティーが充実していない	故障／誤動作／障害	レベル２	レベル２
	ファシリティーが充実していない	記録媒体の劣化	レベル２	レベル２

※「顕在化のレベル」の分類例

レベル３：頻繁且つ容易に脆弱性が顕在化しやすい。

レベル２：専門知識を持つ者が実施した場合であっても、脆弱性の顕在化する可能性があるかもしれない。偶発的に発生し脆弱性が顕在化する可能性があるかもしれない。

レベル１：専門知識を持つ者が試行錯誤しても脆弱性の顕在化が困難である。

④機密性・完全性・可用性の欠如によるリスク分析

情報資産の機密性、完全性、可用性が損なわれたときの影響を情報資産の管理者により正確に判断する必要があります。

そのため、初めに機密性、完全性、可用性の評価基準を作成します。そして、これらの評価基準をもとに各情報資産に対してリスク分析を実施します。

表６　機密性の評価基準の例

レベル	説明
3	情報が漏えいした場合、事業への影響は深刻である
2	情報が漏えいした場合、事業への影響は大きい
1	情報が漏えいした場合、事業への影響はほとんどない

表７　完全性の評価基準の例

レベル	説明
3	情報が改ざんされた場合、事業への影響は深刻である
2	情報が改ざんされた場合、事業への影響は大きい
1	情報が改ざんされた場合、事業への影響はほとんどない

表８　可用性の評価基準の例

レベル	説明
3	情報が消去された場合、事業への影響は深刻である
2	情報が消去された場合、事業への影響は大きい
1	情報が消去された場合、事業への影響はほとんどない

リスク分析は、定量的にリスクレベルを算定する場合もあれば定性的の場合もあります。

前述のリスクアセスメントの方法により、リスク評価の評価算出（測定）方法は大きく異なります。簡略化したリスク値の算出の例として、以下に式を示します。

リスク値＝情報資産（C＋I＋A）×脅威レベル×脆弱性レベル

各情報資産に対するそれぞれの脅威に対する脆弱性から各リスク値を算出し、その数値により管理対策適用の優先度を判断します。以下に実施例を示します。

表９　リスク値算出表の例　（１／２）

資産名	機密性 完全性 可用性 （合計値）	脆弱性	関連する 脅威	脅威発生の 頻度	顕在化の レベル	リスク値	対策 優先順位
顧客管理データ／コンサルティングデータ	3 3 3 （合計９）	誰でも読み込めるデータである／コピー・持ち出しが容易	盗聴	レベル２	レベル２	36	
		誰でも読み込めるデータである／コピー・持ち出しが容易	盗難	レベル３	レベル２	54	2
		バックアップをしていない	記録媒体の劣化	レベル２	レベル３	54	2
業務ソフトウェア（OSも含む）	2 3 2 （合計７）	セキュリティホール	不正アクセス／改ざん／情報漏えい	レベル２	レベル２	28	
		アクセス制御をしていない	不正アクセス／改ざん／情報漏えい	レベル２	レベル３	42	3
		不要なアカウント／パスワード管理が不徹底	不正アクセス／改ざん／情報漏えい	レベル２	レベル３	42	3
		ソフトウェア資産管理をしていない	ソフトウェアの不正利用	レベル２	レベル３	42	3
		バージョンアップをしていない	不正アクセス／改ざん／情報漏えい	レベル２	レベル３	42	3
		利用ログを取得していない	不正アクセス／改ざん／情報漏えい	レベル２	レベル３	42	3
業務用サーバ・社内システムアクセス制御機器	3 2 2 （合計７）	壊れやすい、熱に弱い	データ損失／記録媒体の劣化 故障、誤動作、障害	レベル２	レベル２	28	
		ウイルス対策ソフトを導入していない	ウイルス・ワーム感染、ウイルス・ワーム蔓延	レベル３	レベル２	42	3
		設定ミス（アクセス権、アカウント情報）	不正アクセス／改ざん／情報漏えい	レベル２	レベル３	42	3
		物品管理をしていない	盗難	レベル３	レベル２	42	3
		保守契約なし	故障	レベル２	レベル２	28	
		操作方法の教育をしていない	サーバオペレータ操作ミス	レベル２	レベル２	28	
		リソース管理をしていない	サーバ障害／社内ネットワーク障害	レベル２	レベル３	42	3
		バックアップをしていない	記録媒体の劣化	レベル３	レベル２	42	3

表１０　リスク値算出表の例　（２／２）

資産名	機密性 完全性 可用性 （合計値）	脆弱性	関連する 脅威	脅威発生の 頻度	顕在化の レベル	リスク値	対策 優先順位
配布パソコン	3 2 2 （合計７）	壊れやすい、熱に弱い	データ損失／記録媒体の劣化故障、誤動作、障害	レベル２	レベル２	28	
		ウイルス対策ソフトを導入していない	ウイルス・ワーム感染、ウイルス・ワーム蔓延	レベル３	レベル３	63	1
		設定ミス（アクセス権、アカウント情報）	不正アクセス／改ざん／情報漏えい	レベル２	レベル３	42	3
		物品管理をしていない	盗難	レベル３	レベル３	63	1
		保守契約なし	故障	レベル２	レベル３	42	3
		操作方法の教育をしていない	パソコン操作ミス	レベル２	レベル３	42	3
		持ち出しやすい	盗難、紛失	レベル２	レベル３	42	3
		バックアップをしていない	記録媒体の劣化	レベル３	レベル３	63	1
サーバルーム	3 3 3 （合計９）	災害に弱い	台風／火事／地震	レベル１	レベル２	18	
		戸締り不備、物理侵入が容易／入退室・入館管理をしていない	不正アクセス／ソフトウェアの不正利用／記録媒体の不正使用／盗難	レベル２	レベル２	36	
		ファシリティーが充実していない	停電／漏水／空調故障	レベル１	レベル２	18	
		ファシリティーが充実していない	故障／誤動作／障害	レベル２	レベル２	36	
		ファシリティーが充実していない	記録媒体の劣化	レベル２	レベル２	36	

⇒　リスクアセスメントには様々な手法があるため、組織に合ったリスクアセスメントの方法を選択し、実施する必要があります。情報セキュリティに関するリスクアセスメント手法の参考文献として下記を参照してください。

- DISK PD3002:1998 (Guide to BS7799 Risk Assessment and Risk Management)
- GMITS (Guidelines for the Management for IT Security) ISO/IEC TR 13335:1998

エ．リスクマネジメント

リスクアセスメントが終わったら、今度は「リスクマネジメント」を実施します。
リスクマネジメントとは、リスクアセスメントの結果を受けてリスクに対応するための対策を検討することです。

● 脆弱性に対する対策の優先順位の決定

すべての脆弱性についての対策の実施は困難であるため、リスク値の高い順に従って優先順位を決定します。このとき、対策費用も考慮し、対策費用とリスクの軽減のバランスを十分検討し、具体的な対策を検討していきます。
対策を検討する場合に、以下の４つから「何が適切か」を判断していきます。リスクに対応する対策のうち、どれを選択・適用するかについては、効果、費用、実現可能性などをもとにして、総合的に判断する必要があります。

①リスクを低減する
②リスクを受容する
③リスクを回避する
④リスクを移転する

①リスクを低減する

管理対策を適用し、情報資産に対する脅威や脆弱性に対してリスク値を下げる方策を採用します。どの程度のリスク値が軽減され、残留リスクはどの程度なのかを算出する必要があります。

例）
バックアップ（※）を定期的に実行するようにして、記録媒体の劣化に伴う可用性確保を実施し、リスク値を下げます。

②リスクを受容する

管理対策を選択後も残留するリスク値が高い場合は、追加の管理策を検討し、リスク値を受容可能な範囲に下げる必要があります。

例）
ウイルス対策ソフトを導入しても、最新のウイルス定義ファイルをダウンロードするまでの間は感染する恐れがあるということをリスクとして認識します。

③リスクを回避する

コスト上対応が難しい場合や①、②が適用できない場合、リスクを回避するために、情報資産自体を破棄したり、リスクの発生が伴う作業・操作・業務を廃止したりするなどの対応をとります。

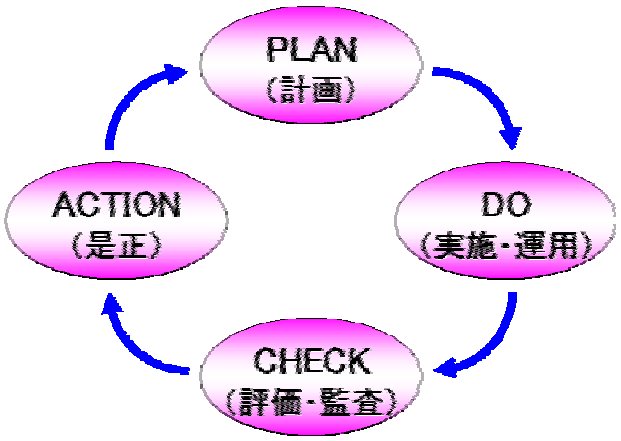
例）
社内顧客システムへのアクセスについては、土日及び夜間の接続を禁止する。

④リスクを移転する
契約等によりリスクを移転します。リスクに対する保険の採用や、業務やサービスの委託契約により他者へリスクを移転することです。
例）
社内にサーバルームを作るのではなく、ファシリティーが充実したデータセンター等を用いたり、災害保険等へ加入したりします。

● 情報セキュリティに関するＰＤＣＡサイクルについて

リスクマネジメントを実施するうえで、必ず考慮しなければならないのが、PDCA サイクルを意識することです。情報セキュリティに関する PDCA サイクルとは、「Plan（計画）」－「Do（実施・運用）」－「Check（評価・監査）」－「Action（是正）」の各作業を継続的に繰り返し実施することを指し、情報セキュリティレベルの向上には欠かせないプロセスとして位置付けられています。

図５　情報セキュリティに関する PDCA サイクル



Plan－計画

情報セキュリティ基本方針、目標、対象、プロセス及び手順を確立し、リスクアセスメント、リスクマネジメントや情報セキュリティ対策事項の適用などについて計画を立てます。

情報セキュリティ管理体制（ルールにて後述）を中心に各関連組織からの協力を得ながら、現実的な実施内容になるように計画する必要があります。

例）
新たにテレワークを導入する場合には、導入スケジュール、関連する情報セキュリティ対策の改定、システムの設計と構築、利用方法の教育、利用申請フローの策定や問い合わせ窓口体制等を決定します

Do－実施・運用

計画した内容について、組織への適用・運用・管理などの実施を徹底させる段階です。

各部署への事前の周知や既存システムとの併用期間、問い合わせ窓口などについても考慮しておくことが必要です。

例）

テレワーク運用においては、情報セキュリティ対策の実施内容をもとに、利用者のアカウント（※）申請受付（新規、利用停止、削除）による利用者管理や端末管理業務、システムの監視、問い合わせの対応等を実施します。

Check－評価・監査

情報セキュリティ基本方針、目標に対して、実施した内容が監査を通して遵守されているかを確認します。遵守されていない場合は、対応策を検討するためにその理由についても調査する必要があります。

また、期待したとおり情報セキュリティレベル向上が実現されているかを確認します。実施により業務上に問題が発生していないかなども確認する必要があります。最終的には、これらの点検実施内容結果を経営層に報告します。

例）

テレワーク利用者や情報システム担当者に対して、情報セキュリティ対策の遵守状況をヒアリング及び調査を通して監査し、その結果を経営層に報告します。

Action－是正

点検実施内容結果のレビューをもとに、経営層が是正・改善処置及び予防処置を検討し、Plan（計画）へ続きます。

例）

経営層は、監査を通して情報セキュリティ対策の遵守状況を把握し、遵守されていない部分や対策が形骸化している部分については、その理由に対するヒアリング及び調査を指示します。

そして、遵守状況を改善するための方法（実施内容の変更、適用方法・手段の変更、手順の変更、教育内容の変更等）を検討し、その実施を計画します。

オ． 対策基準の策定

PDCA を意識したリスクマネジメントまで終わったら、基本方針に基づき、対策基準を策定する必要があります。

対策基準はテレワークに特化したものではなく、物理的セキュリティ・人的セキュリティ等も含みます。テレワークの範囲だけで情報セキュリティポリシーを策定するのではなく、企業や組織全体で情報セキュリティポリシーの策定に取り組むことが必要です。

企業や組織の範囲、業務の形態や範囲によって、必要となる対策基準の内容が異なってきます。また、情報セキュリティポリシーの基本方針・対策基準・実施内容は、それぞれが関連性をもって体系的に作成されるべきものです。専門家を含めた情報セキュリティ委員会等を発足し、ISO/IEC17799 や JIS X 5080 等の要求事項を参考にして策定することを推奨します。以下では、P.９９の「参考資料４：情報セキュリティポリシーにおける対策基準（例）」に記述する「ウイルス対策基準」、「ハードウェア／ソフトウェア対策基準」、「リモートアクセス対策基準」、「クライアント端末対策基準」以外の対策基準例をご紹介します。

⇒ ISO/IEC17799 や JIS X 5080 については、P.７９の「参考資料１：代表的な情報セキュリティ基準について」を参照してください。

● 対策基準項目の例

- 組織管理基準
  情報セキュリティ運営委員会の運営体制、情報セキュリティ管理責任者、関連部門の責任者等の体制について、また外部委託等第三者の情報資産へのアクセスによるリスクや契約条件等の規定を記述します。
- 文書管理基準
  文書の発行、変更、承認、廃止等の管理基準について記述します。
- 人材管理基準
  情報セキュリティの教育及び訓練、採用条件、罰則規定等について記述します。
- リスク評価管理基準
  リスクアセスメント及びリスクマネジメントについての基準について記述します。
- 情報セキュリティ監査基準
  内部及び外部の監査の基準、問題が発生した場合の是正処置、予防処置等の対応基準について記述します。
- 情報セキュリティ事故管理基準
  情報セキュリティ事故・事件の対処方法、再発防止のための是正・予防処置等についての基準について記述します。
- 事業継続管理基準
  大規模災害により事業が中断される場合を想定した対策、事業継続のための計画、試験（机上試験・模擬試験）、見直し等についての基準を記述します。

- **情報資産管理基準**
  資産目録の作成、維持管理、分類の指針、情報資産分類のラベル付けとその扱いについての基準等を記述します。
- **物理環境管理基準**
  入退出管理、物理的セキュリティ境界の管理、装置、電源、ケーブル等の設置条件及び管理､クリアデスク及びクリアスクリーン等についての基準を記述します。
- **委託先管理基準**
  外部の委託先の管理基準について記述します。
- **情報システム開発管理基準**
  システム開発を行う場合の情報セキュリティ要求事項(入力データの妥当性、内部処理の管理、出力データの妥当性等)、暗号化による管理、ソースプログラムの変更管理（更新・変更等のバージョン管理）等の基準について記述します。
- **情報システム運用管理基準**
  システム（サーバ・ネットワーク・アプリケーション等）の運用管理基準（パスワード管理、アクセス制御、電子メールの運用、データのバックアップ、ログ管理等）についての基準を記述します。

以上の対策基準の項目や内容は、企業や組織によって分類やまとめ方が異なります。あくまでも事例であることをご了承ください。

カ．実施内容の作成

対策基準を策定した後は、具体的な実施内容を作成する必要があります。実施内容については、「２.『ルール』についての対策」、「３.『人』についての対策」、「４.『技術』についての対策」を参照してください。

※６　情報セキュリティ保護要件･･･情報セキュリティ対策を実施するうえでは、以下の「情報セキュリティ保護要件」を考慮する必要があります。

●機密性：許可された者だけが情報にアクセスできるようにすること。

●完全性：情報及び処理方法が正確かつ完全であること。

●可用性：認可された利用者が必要なときに情報にアクセスできること。

（解説）

●　ＣＩＡについて

情報資産に関する説明でも触れましたが、「ＣＩＡ」とは、情報セキュリティを保護するための要件でもある①機密性（Confidentiality)、②完全性（Integrity)、③可用性（Availability）の頭文字です。この３つのうち、どれか一つが欠けていても、十分な情報セキュリティを維持することはできません。状況に応じて、それぞれがバランスよく保たれていることが情報セキュリティ対策を行ううえで大切なポイントとなります。

①　機密性

不特定多数へ公開されるものを除き、一般的に情報へのアクセスは、許可された人だけが、許可された方法によってのみ行います。この特性を「機密性」と呼びます。

②　完全性

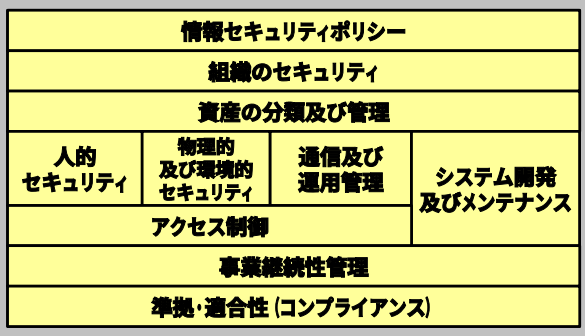
記録されている情報は、常にその内容の一貫性が維持されていなければなりません。悪意の有無を問わず、本来は意図しないところで書き換えられたり、消去されたりしないことが求められます。この特性を「完全性」と呼びます。

③　可用性

必要なときにその情報を利用できるかどうか、それを表す特性が「可用性」です。必要なときに利用できない情報は、例えそれ自体に価値があったとしても、実際の企業活動に利益をもたらしません。その観点から可用性は情報セキュリティの３つ目の本質とされています。

なお、参考として情報セキュリティマネジメントシステム（ISMS）の内容として求められる要件を図５に示します。

図５　情報セキュリティマネジメントシステム（ISMS）の内容として求められる要件



出典：ISO/IEC17799 を基に作成

（解説）

ISO/IEC17799 では、情報セキュリティマネジメントシステム（ISMS）の実施規範が規定されており、情報セキュリティマネジメントシステム（ISMS）を構築するために必要な要件が詳細に掲載されています。

表１１　情報セキュリティマネジメントシステム（ISMS）の構成要件

分野		内容
管理分野1	セキュリティ基本方針	経営陣における情報セキュリティの基本方針の宣言、従業員への通知・公表、ＰＤＣＡサイクルの管理（見直し・評価等）等についての規定
管理分野2	組織のセキュリティ	情報セキュリティ推進に責任を持つ情報セキュリティ運営委員会の運営体制、情報セキュリティ管理責任者等の体制についての規定
管理分野3	資産の分類および管理	資産目録の作成、維持管理、分類の指針、情報資産分類のラベル付けとその扱いについての規定
管理分野4	人的セキュリティ	人的要因によるリスク軽減を目的に、情報セキュリティの教育及び訓練、採用条件等についての規定
管理分野5	物理的および環境的セキュリティ	入退出管理策、物理的セキュリティ境界の管理、設備条件及び管理等についての規定
管理分野6	通信および運用管理	情報処理システムの運用管理のセキュリティについての規定
管理分野7	アクセス制御	利用者の情報アクセス管理やネットワークアクセス制御についての規定
管理分野8	システムの開発および保守	システムへの情報セキュリティ要件、アプリケーションソフトに対する情報セキュリティ要件、情報の秘匿・認証、暗号鍵の管理等についての規定
管理分野9	事業継続管理	大規模災害により事業が中断される場合を想定した対策、事業継続のための計画、試験、見直し等についての規定
管理分野10	適合性	知的所有権、プライバシー保護などの法的措置への準拠（適合性）についての規定

⇒　情報セキュリティマネジメントシステム（ISMS）についての詳細は、P.８１の「参考資料２：情報セキュリティマネジメントシステム（ISMS）について」を参照してください。

⇒　情報セキュリティマネジメントシステムの構成要件についての詳細は、P.８２の「参考資料３：地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書のセルフチェックリスト」を参照してください。

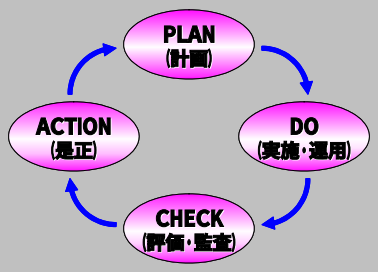
従業員の情報セキュリティ意識を高め、情報セキュリティポリシーの形骸化を防ぐために、経営層がトップダウンで情報セキュリティポリシーを従業員全員に周知・徹底することも必要です。情報セキュリティにおいて最も重要なことは、組織内の従業員すべてが、情報セキュリティに関して共通の認識を持つことです。例えば、「個人情報」に関する定義についても、組織内のすべての従業員が同じ認識を持てるように、教育や訓練を実施する必要があります。同時に、情報セキュリティ対策について、それぞれの従業員がすべきことは何かを十分に認識させる必要もあります。個々の従業員による不断の努力によって組織全体の情報セキュリティが支えられているということを、経営層が積極的に伝えることが重要です。

さらに、あらゆる脅威に対して対策をとることは困難であることから、情報セキュリティ事故発生のリスクをゼロにすることはできませんが、情報セキュリティに関する PDCA サイクル（※７）を通してリスク管理することにより、情報セキュリティレベルを向上していくことも重要です（図６）。

※７　情報セキュリティに関する PDCA サイクル…情報セキュリティレベル維持に必要な各行動を表し、周期的に実行することにより実行効果を高めること。

- Plan　：　情報セキュリティ対策事項の具体的計画を策定する。
- Do　　：　計画・目標に基づいて対策事項の実施・運用を行う。
- Check　：　対策事項を実施した結果の評価・監査を行う。
- Action：　経営層による見直しを行い、対策事項について是正する。

図６　情報セキュリティに関する PDCA サイクル



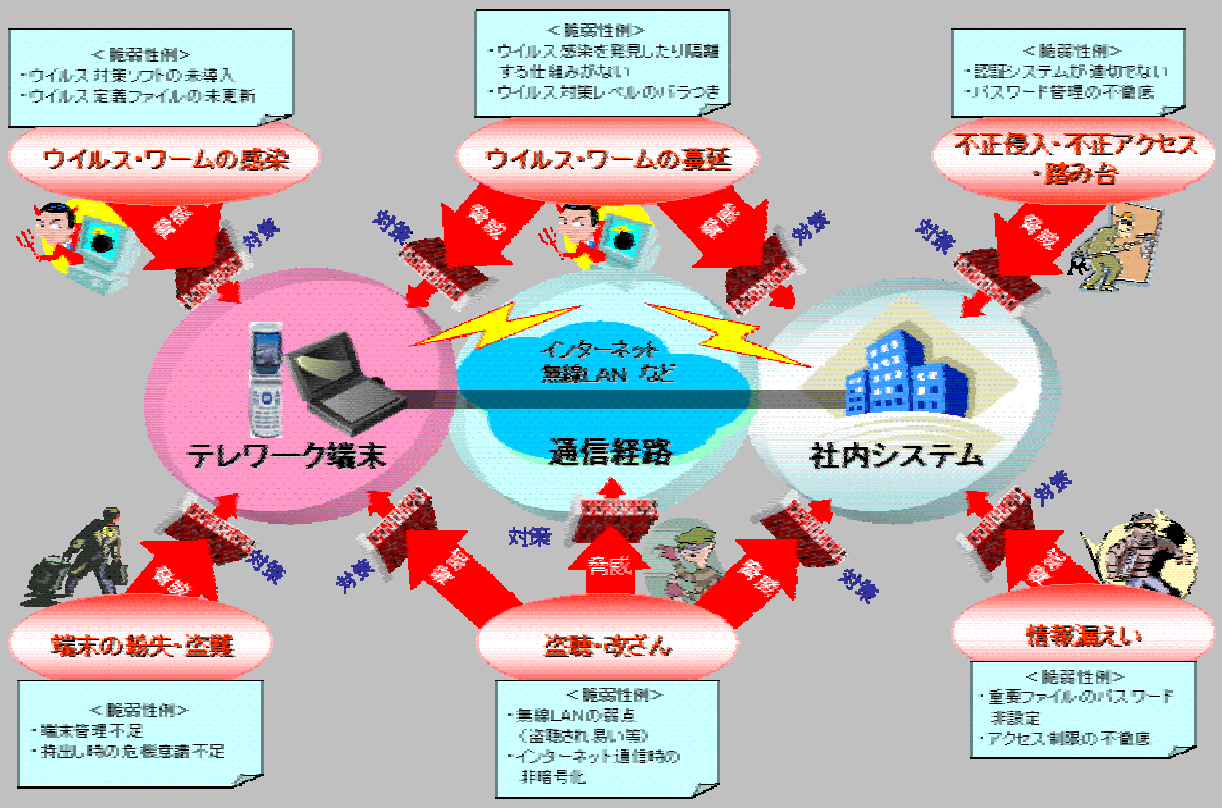
（解説）

PDCA サイクルについては、P.２３の「情報セキュリティに関するＰＤＣＡサイクルについて」を参照してください。

（イ）テレワークにおける情報セキュリティ対策のポイント

近年におけるテレワークでは、誰でも利用することができる反面、誰でも不正な行為を実行することもできてしまうインターネットを活用したり、持ち運び可能なノートパソコンを用いて多地点で業務を実施したりするため、ウイルス・ワーム（※６）の感染、パソコンや記録媒体の紛失・盗難、電子データ漏えいなど、様々な「脅威」や脅威の発生を誘引する情報資産の「脆弱性（弱点）」が存在します。以下では、テレワークにおける脅威と脆弱性について図７に示します。

図７　テレワークにおける脅威と脆弱性について



（解説）

テレワークに関する脅威について理解を深めるために、以下に具体的な事故・事例を示します。

●ウイルス・ワームの感染・蔓延

- ワーム感染・蔓延
  企業から支給されたパソコンを家に持ち帰りインターネットに接続したが、ウイルス対策ソフトの定義ファイルを最新のものに更新していなかったために、新種のワームに感染。感染に気付かずに企業に戻り、そのままパソコンを LAN に接続したところ、企業内にワームが蔓延してしまった。

・ **機密書類がネット上に流出**
ウイルスが原因で、私用パソコンに保存した機密書類がインターネット上に流出した。

●不正侵入・不正アクセス・踏み台

・ **他人のアカウントで不正にオンライン株取引**
情報処理サービス会社の従業員が、不正に入手した顧客情報のユーザ ID とパスワードを利用して金融会社の顧客になりすまし、不正なオンライン取引を行った。

●端末の紛失・盗難

・ **顧客情報を紛失**
従業員が電車の網棚に、顧客情報の保存されているノートパソコンの入ったカバンを置き忘れたことが原因で、顧客情報の漏えいに繋がった。

・ **機密情報の流出**
システム会社で働くアルバイトが、持ち込んだ個人用のパソコンにデータをコピーして持ち出し、名簿販売業者に売却したことが原因で機密情報が流出した。

●盗聴・改ざん

・ **ホームページ改ざん**
大企業や官庁のホームページが狙われ、ホームページが改ざんされた。その後、同じような手口で、ホームページの改ざんが相次いだ。

・ **無線 LAN による電子メールの盗聴**
暗号化の設定を行わずに無線 LAN を使用していたために、業務で利用していた電子メールの内容が漏えいしてしまった。

●情報漏えい

・ **個人データ流出**
資料の請求のために登録された氏名、住所、年齢、メールアドレスなどの個人情報が漏えいした。登録情報の中には、プライバシーの侵害にも繋がりかねない項目もあったため、大きな問題となった。

・ **機密情報などを消去せずパソコン廃棄**
個人で購入したパソコンを職場に持ち込んで業務に利用していた従業員が、パソコンを廃棄する際に、道路にパソコンを複数回たたきつけただけで不燃ゴミとして出した。業務で利用されていた機密情報データは消去されず、パソコンを拾って操作した業者が機密情報を悪用し、情報漏えいに繋がった。

２．「ルール」についての対策

情報セキュリティポリシーを定着させるためには、情報資産の利用方法や情報セキュリティ対策適用のための手続き、情報資産の管理方法や取扱方法について決定し、遵守していく必要があります。情報セキュリティレベルの向上に責任を持つ人は、これらのルールを作成し、各情報セキュリティ対策が適切に実施されることを管理していきます。このルールが適切に実施されないと、「人」に対する情報セキュリティ対策、「技術」に対する情報セキュリティ対策が無意味となるおそれがあります。

（ア）組織として遵守すべきルール

テレワークの情報セキュリティに関する管理体制及び責任の所在を明確にすることは重要なことです。

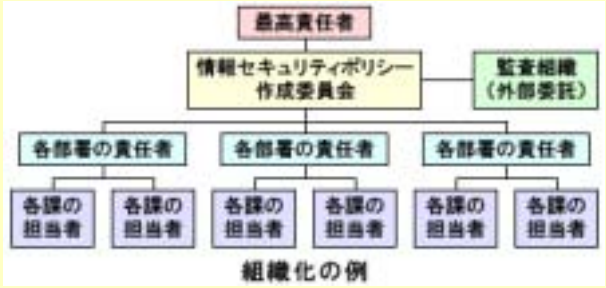
また、テレワーク環境においても情報セキュリティルールが正しく遵守されているか、現場の状況に適合しているかなどについて、定期的なチェック（監査）を実施することで、情報セキュリティルールの見直し及び定着を図ります。監査は不正な行為の抑止効果としても有効です。

◆事例

(1) 情報セキュリティ管理体制（図９）

① 情報資産の管理方法・管理責任者を規定する。

図９　事例（１）情報セキュリティ管理体制



（解説）

テレワークを行う場合の情報セキュリティ管理体制にはテレワーク勤務者以外に以下のようなメンバーが参画し、企業や組織全体で情報セキュリティ対策に取り組むことが重要です。

・ 最高責任者
　テレワークの情報セキュリティ対策は企業や組織全体で取り組むべきものです。最高責任者はテレワークを行う企業や組織の経営者や部門長等、最高責任を有する職位者を含めることが重要です。

・ 情報セキュリティポリシー作成委員会
　情報セキュリティポリシー作成委員会には、テレワークに関するシステム部門、管理部門、現場部門等が幅広く参加することが望まれます。特にテレワーク勤務者が所属する現場部門を含めないと、情報セキュリティポリシーが実情に合わないものになり、結果的にルールが守れない等の弊害が生じてしまします。

・ 監査組織
　監査組織は、情報セキュリティ対策の遵守状況を把握するための重要な組織です。この場合、監査をする部門と、監査される部門を分離（責務の分離）し、厳格に監査が行われる必要があります。そのため、第三者である外部の監査専門家に監査を依頼することも考えられます。

・ 各部署の責任者
　各部の責任者は、ルールの定着及び改善のためのパイプ役となります。各部の事情を考慮した普及方法の検討を行うとともに、現場に適していないルールについては、その改善要望を報告します。

(1) 情報セキュリティ管理体制
① 情報資産の管理方法・管理責任者を規定する。

（解説）

　情報資産の管理方法が明確でない場合には、適切に情報資産が扱われない可能性があり、情報セキュリティ事故の発生確率が高くなると言えます。情報資産の管理方法は、誰もが管理できる方法で明確に示す必要があります。
　車・宝石・土地・お金等の個人資産については、誰のものか明確であるため各個人によってしっかり守られているように、情報資産についても「誰のものか」を明確にして、管理される必要があります。
　情報資産が誰のものかが曖昧な場合には、その管理方法や管理手順が改善されないばかりか、盗難等の事故に遭遇したとしても気付かない場合もあります。そのため、情報資産を明確に定義し、管理責任者を明確にしておくことが重要です。

（実施方法）

以下のように、情報資産の洗い出しと管理責任者の選定を行います。

① 情報資産の分類
- 管理する必要があると思われる情報資産を列挙します。
- その情報資産について、下記の表を参考に、資産区分（ハードウェア・ソフトウェア・情報等の区分）や保管形態、保管場所、用途、利用者の範囲（誰が利用可能か）を整理します。

② 管理責任者の選定
- 情報資産ごとに、誰が管理するのが適任か、またその責任を負うことが可能かを判断のポイントとして、管理責任者を決定します。

⇒ 本作業に関する詳細は、P.１６「ウ．リスクアセスメント」を参照してください。

表１２　情報資産目録と管理責任者（例）

資産区分	資産名	管理責任者	保管形態	保管場所	保管期間	破棄方法	用途	利用者の範囲
ハードウェア	テレワーク用貸与パソコン	システム部長	社内および在宅で利用	在宅対象者宅	10年	データ完全消去後破棄処理	サーバアクセス用及び、ドキュメント作成	テレワーク勤務者
ソフトウェア	業務用ソフトウェア	システム部長	電子データ	CD-ROM ファイルサーバ	15年	媒体粉砕･データ消去	業務用システムソフト	テレワーク勤務者
ハードウェア	業務用サーバ	システム部長	サーバルーム内稼動	サーバルーム	10年	データ完全消去後破棄処理	業務システム用サーバ	情報システム担当
ハードウェア	社内システムアクセス制御機器	システム部長	サーバルーム内稼動	サーバルーム	10年	データ完全消去後破棄処理	社内システムアクセス認証制御	情報システム担当
情報	顧客管理データ	営業部長	電子データ	顧客データベース	15年	データ消去	顧客管理	テレワーク勤務者
情報	営業情報	営業部長	電子データ	ファイルサーバ	15年	データ消去	コンサルティング業務	テレワーク勤務者

(1) 情報セキュリティ管理体制
② 管理責任者に権限を与えること。

（解説）

情報資産の「管理責任者の権限」には以下を含みます。

① 情報資産を守る権限

個人資産は、鍵を購入したり、金庫や車庫に保管したり、監視システムを導入したりするなどの方法で、個人資産を守るためにお金をかけて対策を行っています。情報資産を守る場合も、対策方法の選択や費用をかけることに対する権限を管理責任者に与えることが必要です。

② 情報資産へのアクセス権の決定権限

管理責任者に情報資産へのアクセス権（情報資産に対して「誰が」、「何を（読取・書込み）するか」）を決定する権限を与え、情報資産の適切な利用を維持していくことが必要です。

（実施方法）

以下の方法で、情報資産のアクセス権を決定します。

① 情報資産の「Ｃ：機密性」、「Ｉ：完全性」、「Ａ：可用性」について評価を行います。
② 情報が格納されているシステムやファイルサーバを特定します。
③ 情報資産の利用者が誰であるかを分類します。（事例はテレワーク勤務者です）
④ 利用者に対して、どの情報資産についてアクセスを可能にするかということを規定します。
このとき、「Ｃ：機密性」を中心にアクセスの可否を決定します。
- ◎：アクセス可
- ○：アクセス可であるがコピーは禁止
- ×：アクセス不可

⑤ 利用者が情報資産についてアクセスした場合のデータの扱いを規定します。
このとき、「Ｉ：完全性」を中心に読み取り・書き込みの可否を決定します。
- Ｒ：読み取りのみ
- Ｒ／Ｗ：読み取り書き込み可

なお、必要に応じて複製（コピー）の可否を規定します。

表１３　情報資産に対するアクセス権の設定例

情報資産		情報資産のCIA			資産の場所	テレワーク勤務者のアクセス権			
区分	情報資産例	C:機密性	I:完全性	A:可用性		アクセス可否		データの扱い	
お客様情報	企業情報	△	◎	△	公開ＷＥＢ	○	アクセス可	Ｒ	読み取りのみ
	企業情報	◎	○	△	Ａシステム	×	アクセス不可	-	-
	顧客管理データ	◎	◎	△	ファイルサーバＡ	○	アクセス可	Ｒ	読み取りのみ
契約関連情報	提案書	○	○	△	業務システムＡ	○	アクセス可	Ｒ／Ｗ	読み書き可
	見積書	◎	○	△	業務システムＢ	○	アクセス可	Ｒ／Ｗ	読み書き可
	契約書	◎	○	△	業務システムＢ	○	アクセス可	Ｒ／Ｗ	読み書き可
財務情報	売上データ	◎	◎	◎	業務システムＢ	○	アクセス可	Ｒ	読み取りのみ
	取引データ	◎	◎	◎	業務システムＢ	×	アクセス不可	-	-
システム情報	設計書	◎	○	△	ファイルサーバＢ	○	アクセス可	Ｒ／Ｗ	読み書き可
	プログラムファイル	◎	○	◎	ファイルサーバＢ	○	アクセス可	Ｒ／Ｗ	読み書き可
社内システム	業務マニュアル	○	△	△	イントラネット	○	アクセス可	Ｒ	読み取りのみ
	社員録	◎	◎	○	イントラネット	○	アクセス可	Ｒ	読み取りのみ

(1) 情報セキュリティ管理体制
③ 事件・事故が発生した場合の連絡先・対応先・責任者を規定すること。

（解説）

「ウイルスに感染した」、「パソコンが盗まれた」等の場合には、どのように対応したらよいのでしょうか？

事件や事故が発生した時点で対応策を考えていては、対応が遅れ、被害が拡大する可能性があります。まずは、「誰に連絡すればよいか」（連絡先）、「どんな対応をすればよいか」（対応方法・対応者）、「誰が事件や事故の後処理をするのか」（責任者）について、あらかじめ明確に規定しておく必要があります。

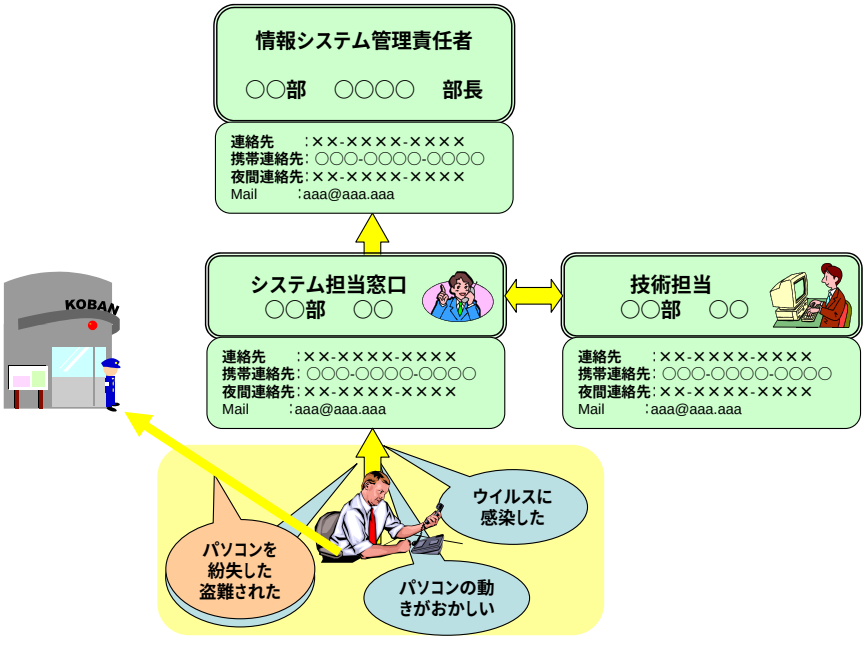
（実施方法）

事件や事故が発生した場合の連絡体制図を作成します。

- 様々な事件や事故に対しても窓口をできる限り一つにして、テレワーク勤務者が連絡先を迷わないようにすべきです。
- 連絡先を忘れたり、わからない場合がないように、連絡体制図を携帯したり、携帯電話に連絡先を登録したりすることも良い方法です
- パソコンの紛失・盗難は、「財布を落とした」、「自転車を盗まれた」と同じことです。パソコン自体にも価値はありますが、情報資産も内容によっては大変大きな価値がある場合があります。事件・事故の事実を証明するためにも、直ちに警察に届出することも連絡体制で決めておく必要があります。

⇒ 情報セキュリティ事故発生後の対応については、P.５２の「（ウ）情報セキュリティ事故発生後の対応」を参照してください。

図６　事件・事故発生時の連絡体制の例



(2) 定期的な監査の実施
テレワーク環境において情報セキュリティ対策事項が遵守されているか、定期的にヒアリング等による監査を実施する。

（解説）

テレワーク勤務者は企業内で勤務する従業員と異なり、一人または少数の単位で業務を行います。企業内の場合は、他者とのコミュニケーションにより自然にルールが定着する場合もありますが、テレワーク勤務者へのルールの定着は特に配慮が必要です。そのため、組織とのコミュニケーションの機会を増やす意味でも、定期的に監査及びヒアリング等を行い、ルールの定着に努めるとともに、コミュニケーションの機会を増やす必要があります。

（実施方法）

テレワーク勤務者への監査として、テレワーク勤務者の勤務状況、テレワーク環境に関する課題等のヒアリングとともに、監査用のチェックシートを作成し、定期的な監査を行うことでセキュリティ意識の向上を図ることをお勧めします。

⇒ 情報セキュリティマネジメントシステム（ISMS）に基づいた情報セキュリティ監査を行う際には、P.８２の「参考資料３：地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書のセルフチェックリスト」を参照してください。

⇒ テレワーク勤務者のセルフチェックまたは簡易監査のためのチェックシートは、P.１１９の「参考資料８：情報セキュリティチェックリスト」を参照してください。

（イ）システム管理者に遵守させるべきルール

悪意を持つ第三者が本人に成り代わって、社内システムへの認証アクセス権の申込みや、通信経路の申込み・移転等を行った場合、社内システムへの不正なアクセスは容易に可能となります。そのため、テレワーク端末を企業側から貸し出す場合においては利用状況等について適正な管理を行い、また、通信経路の申込み・移転・廃止についても、明確なルールを定め、情報セキュリティ事故発生への早期対応に備える必要があります。

◆事例

(1) アカウントとパスワード管理のルール （図１０）

① 社内システムのアクセス用アカウントの発行については、その利用目的が明確になっているかを確認し、利用期限を設け、アカウントを発行すること。

② アカウントの発行・廃止・変更は、管理者の承認を得ること。

③ 不用なアカウントの削除は徹底すること。

図１０　事例（１）アカウントパスワード管理

（解説）

① アカウントの発行について

情報資産へのアクセス制御は一般的にアカウントとパスワードで実施されますが、アカウントの発行は、「誰が」(Who)、「何のために」(Why)、「いつからいつまで」(When)、「どんなシステムまたは情報資産へ」(What)、「どのようにするか」(How)等を明確にしておく必要があります。

◎アカウント種類例

- メールアカウント
- グループウェア等のアプリケーションを利用するためのアカウント
- リモートアクセスするためのアカウント
- ファイルサーバへアクセスするためのアカウント
- Ｗｅｂを閲覧するためのアカウント　等

② アカウントの発行や廃止・変更

「ちょっとお願い」と言われて、アカウントを俗人的に簡単に発行していては適切にユーザを管理しているとは言えません。アカウント発行・廃止・変更は、情報資産の責任者の許可を得て設定する承認フローをもとに実施することが必要です。

③ 不用なアカウントの削除

アカウントの発行はルールに従って行われたとしても、転勤や退社等により不必要になったアカウントが、承認フローを経ず廃止されないまま放置される可能性があります。アカウントの廃止が行われないまま放置されていると、そのアカウント情報を第三者が知り得た場合、転勤や退社した従業員に成り代わって簡単に情報資産にアクセスできてしまいます。削除対象のアカウントが存在しないかを、定期的に調査する必要があります。

（実施方法）

●アカウントの発行・変更・削除について

アカウントの発行・変更・削除に関する申請書とフローを作成し、システム管理責任者はアカウントの発行・変更・削除について承認します。また、アカウントの確認を行うためのフローも作成し、定期的なアカウント調査を実施します。

以下に、アカウントの申請フローと確認フロー、メールアカウントの申請書の例を示します。

図７　アカウントの申請フローの例

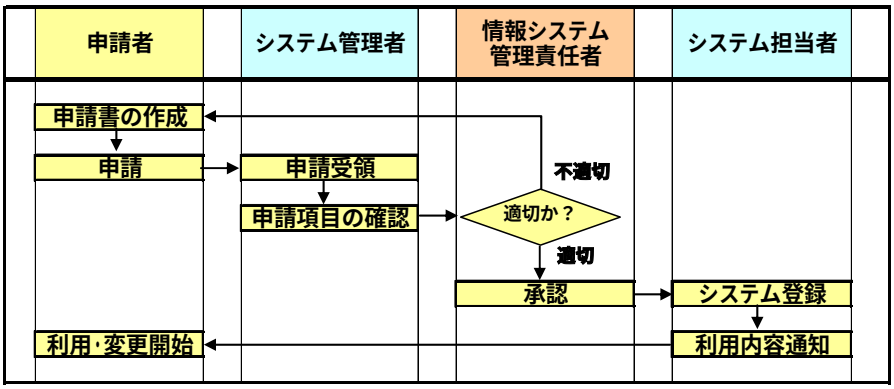


図８　アカウントの確認フローの例

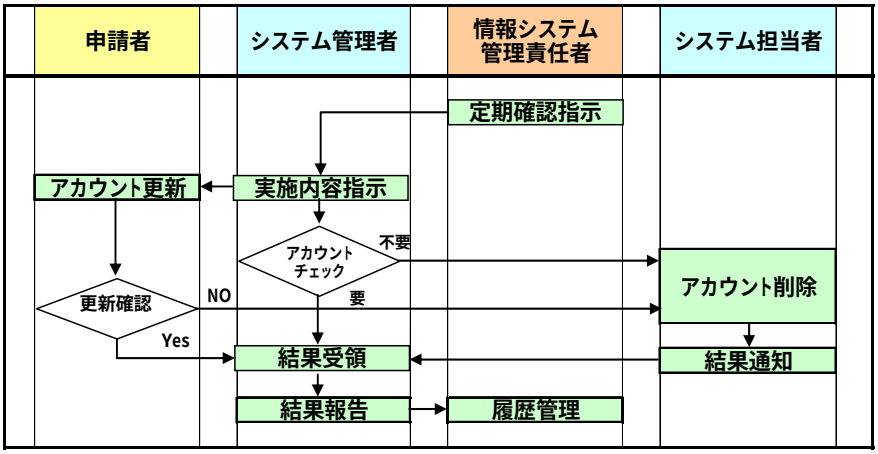


図９　メールアカウント申請書の例

申請日	年　月　日	
申請区分	□新規　□利用延長　□削除	□メール転送

申請者	ふりがな		
	氏名		
	所属等		
	第1希望アカウント		@nnn.nnn.nnn
	第2希望アカウント		@nnn.nnn.nnn
	メールパスワード		
	転送先アドレス	@nnn.nnn.nnn	
	コンピュータ名	システム管理者が決定後、責任者および本人にメールで通知します	

責任者	ふりがな		
	氏名	印	
	所属等		
	メールアドレス		@nnn.nnn.nnn

電子メール利用目的	
電子メール転送理由	

利用期間	年　月　日 ～　年　月　日　(※原則〇年間)

遵守事項	･故意、過失のいずれによっても、社内情報の漏洩がないように責任を持って利用すること。 ･申請したメールアカウントが不要になった場合は、直ちにその旨を情報システム管理責任者へ連絡すること。

情報システム管理責任者

●パスワードの管理について
　パスワードは安全なパスワードを設定し、定期的に変更する必要があります。

⇒　具体的な方法については、P.７１の HOW TO 編「３．パスワード」の項を参照してください。

◆事例
(2)テレワーク端末の管理
① パソコンの貸出し・返却及びパソコン利用状況について、「氏名」「担当業務」「パソコン機種」「連絡先」「返却期限」「情報セキュリティ対策状況（ＯＳ、パッチ、ウイルス定義ファイル等）」等を管理すること。パソコンを共用する場合、返却時にデータが削除されていることを確認すること。
② パソコンを貸し出すときは、最新の情報セキュリティ対策がなされたパソコンを貸与すること。また、返却されたパソコンは、ウイルスチェックを行うなど情報セキュリティ状態について調査を行い、適切な対処を行うこと。

（実施方法）

① テレワーク端末（パソコン）の管理簿事例
　管理責任者は以下のようなパソコンの管理簿を作成し、パソコンの利用状況について把握します。

表１４　テレワーク端末管理簿の例

所属 利用者氏名	利用場所 (住所等)	連絡先	管理 責任者	端末等の使用状況					市販ソフトの インストール状況	貸出し時の状況	返却時の状況	
				機 種 製造番号	ウイルス対策 状態	OSの種類 パッチ状況	データ削除	使用目的	ソフト (シリアルNO)	貸出し日時	返却期限	返却日時

　パソコンのハードディスク（※）内にあるデータは、ハードディスクをフォーマットしても完全には削除されない場合があります。また、貸出し用パソコンを利用する場合、データが残っている場合があるので、返却時または貸出し時にデータ消去用のツールを用いてデータを完全に消去する必要があります。

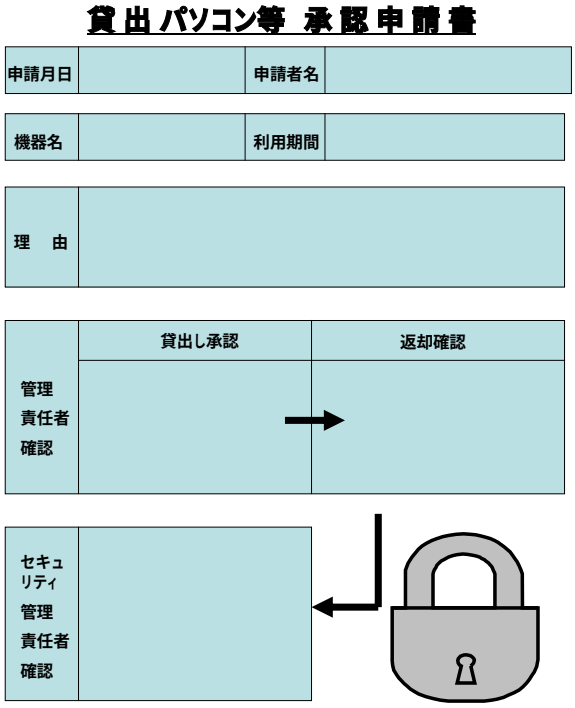
⇒　データの消去方法については、P.７３の HOW TO 編「６．ハードディスクや記録媒体の廃棄」の項を参照してください。

② パソコン等の貸出し

申請者は、パソコンの貸出しについての承認を管理責任者に必ず得るようにします。また、貸し出されるパソコンは、最新の情報セキュリティ対策がなされたものを貸出し、前述のテレワーク端末管理簿とともに管理します。

なお、パソコンの返却時には、そのパソコンがウイルスに感染していないかを必ず確認して、社内へのウイルス持ち込みを防止することが大切です。

図１０　パソコン貸出し申請書の例



◆事例

(3) 通信経路の申込み・移転・廃止

通信経路（インターネット接続、専用線、無線ＬＡＮ、ＶＰＮ（※１３）等）の申込み・移転・廃止を行う場合は、管理責任者の承認を得て行うこと。また、決められた通信経路以外の方法を禁止すること。

※１３　ＶＰＮ…インターネット等の公衆回線網上で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。

（解説）

テレワーク勤務者がオンラインで業務を行う場合、情報資産があるデータセンター等のサーバへアクセスするために用いる通信経路については、あらかじめシステム管理者に通信経路の申込みを行うようにします。テレワーク勤務者が通信経路を勝手に申し込んだり、移転したりすることは、不正アクセスの危険性につながります。また、誤って通信経路を廃止した場合は通信の可用性が損なわれることになります。

アカウントの削除がなされない場合が多いのと同様に、通信経路もテレワーク勤務者が変更になっても、確保されたままとなる可能性もあります。よって、通信経路の申込み・移転・廃止は、定められた手順で実施する必要があります。

（実施方法）

以下のような通信経路の申込み・移転・廃止のフローを規定して、情報システム管理者が管理を行います。

回線の廃止もれを確認するために、定期的に回線番号（ＩＤ）番号や、ＶＰＮ（※）装置のログ等を確認し、利用されていない通信経路を調査します。

図１１　回線申請フローの例

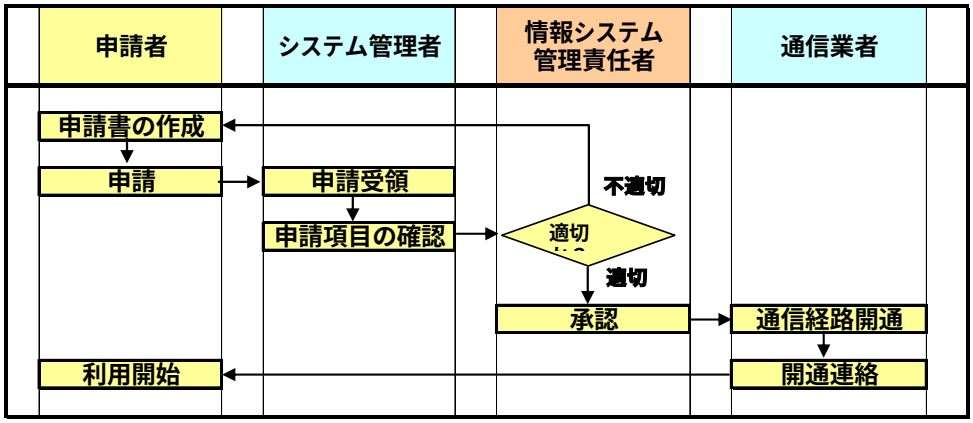
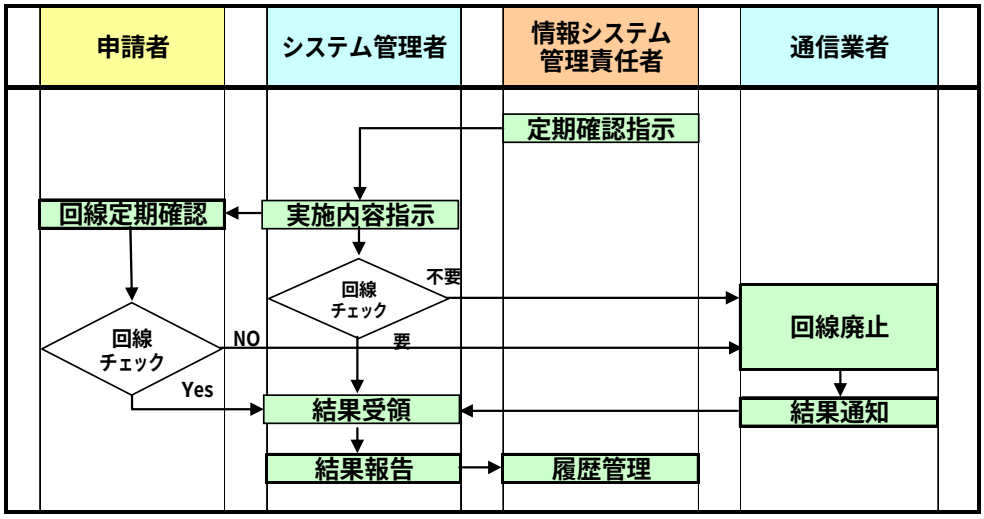


図１２　回線定期確認フローの例



（ウ）テレワーク勤務者に遵守させるべきルール

テレワークは時間・空間的束縛から開放された多様な就労・作業形態を可能にする利点がありますが、不特定多数の人目に触れる場所等では周囲の環境に十分配慮する必要があります。テレワーク端末側は、社内環境と異なり様々な場所での設置が想定され、その分、悪意のある第三者が侵入しやすい環境でもあります。以下では、テレワーク勤務者がパソコンを使用する際、守るべきルールについて記述します。

なお、テレワークは、誰もが最初からスムーズに実施できるとは限りません。ルールが遵守されるためにも、個々人の現在の業務スキル、情報セキュリティに関する知識や意識等に配慮し、適切な教育を行っていくことが重要です。詳しくは「３．人についての対策」を参照してください。

◆事例

(1) パソコンの利用環境

① 持出し許可されたパソコンの使用は、定められた利用条件に従う。（不特定多数の人の目に触れる場所での使用については、のぞき見されないように配慮する等）

② 移動など許可された場所以外にパソコンや記録媒体（ＣＤ－Ｒ／ＲＷ（※１４）やＵＳＢメモリ（※１５）等の可搬な電子媒体）を持ち出す場合には、紛失、盗難、置き忘れ等に注意する。

③ サテライトオフィス（テレワークセンター）（※１６）や自宅でパソコンを利用する場合は、自分以外の者がパソコンを使用できないように配慮する。

※１４　ＣＤ－Ｒ／ＲＷ…書き込み可能なＣＤ。うち、ＣＤ－ＲＷは消去も可能なもの。

※１５　ＵＳＢメモリ…ＵＳＢコネクタに接続して利用する、持ち運び可能な記録媒体。

※１６　サテライトオフィス（テレワークセンター）…企業等が自社の勤務者のテレワーク実施施設として設置する小規模なオフィスのこと。最近では「テレワークセンター」という呼び方が一般的になっている。（出展：「テレワーク白書 2003」社団法人日本テレワーク協会）

（解説）

① テレワークは「どこでも」「いつでも」業務が可能である代わりに、ソーシャルエンジニアリングの危険性も高いと言えます。飛行機の機内で、重要なデータを盗み見された事件も実際に発生しています。電車・飛行機・ホテルのロビー等の不特定多数が往来する場所でのパソコンの利用は、のぞき見等に対して十分な配慮が必要です。

② ＵＳＢメモリ（※）等のように容易に可搬できる電子記録媒体が開発され、データの運搬は大変便利になりました。しかし、小型軽量である分、置き忘れたり、落としたりする可能性が大きくなります。持ち運ぶことができる電子記録媒体に収容されたデータについては、暗号化をしたり、ファイルにパスワードをかけておくことが必要です。

⇒ データの暗号化の方法については、P.７２の HOW TO 編「４．ディスクの暗号化」の項を参照してください。

③ 自分以外の者にパソコンを使用させないようにするためには、以下のような方法があります。

- パソコンのスクリーンセーバー（※）解除時のパスワード認証
- ＯＳのログイン（※）パスワード認証
- 指紋等のバイオメトリクス認証（※）等

いずれもパスワードと組み合わせて利用するため、適切なパスワード設定が重要です。

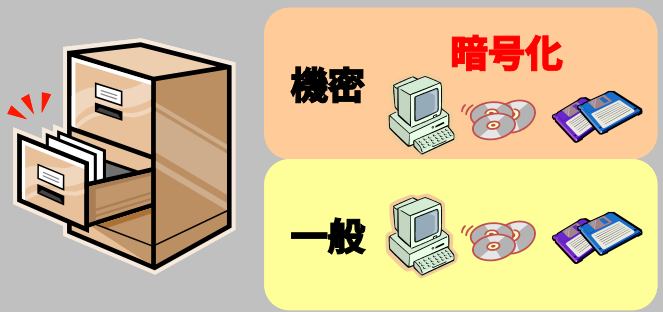
⇒ パスワードの設定方法については、P.７１の HOW TO 編「３．パスワード」の項を参照してください。

◆事例

(2)パソコンで利用するデータの取扱い （図１１）

① 電子データを「機密」「一般」等２つ以上に分類し、「一般」以外の電子データは暗号化する。
② 業務上必要のない情報へのアクセスを禁止する。
③ 「機密」に分類された電子データについては、電子データ復旧を目的とした電子データのバックアップ等、許可された場合を除き印刷や電子データコピーを制限する。
④ 作業を終えたデータは適宜安全な領域（社内のファイル・サーバ等）へ保管するなどし、パソコン上のデータは必要最低限のデータのみとすること。

図１１　事例（２）パソコンで利用するデータの取扱い



（解説）

① 電子データの暗号化

ア）なぜ暗号化を行う必要があるのでしょうか？

パソコンで取り扱う電子データには、契約書・設計書等の文書ファイルやプログラムのソースコード等があります。万一盗難にあってもデータを暗号化していれば解読や改ざんが困難になります。

イ）何を暗号化するのでしょうか？

暗号化をする必要がある情報資産は、「Ｃ：機密性」と「Ｉ：完全性」の確保の必要性が高いものを対象に検討します。

リスクアセスメントで解説したように、下記のレベルにより判断する方法があります。

表１５　機密性の評価基準の例

レベル	説明
3	情報が漏えいした場合、事業への影響は深刻である
2	情報が漏えいした場合、事業への影響は大きい
1	情報が漏えいした場合、事業への影響はほとんどない

表１６　完全性の評価基準の例

レベル	説明
3	情報が改ざんされた場合、事業への影響は深刻である
2	情報が改ざんされた場合、事業への影響は大きい
1	情報が改ざんされた場合、事業への影響はほとんどない

例：ある情報資産についての評価

- 「機密性」３：情報が漏えいした場合、事業への影響は深刻である
- 「完全性」３：情報が改ざんされた場合、事業への影響は深刻である

３＋３＝６

上記のように、定量的な判断による分類と「見ることが許されるのは誰か」を判断しながら定性的に分類する方法があります。

例：定性的な分類方法

- 「社外秘」：社外の人は見てはいけない。見せてはいけない。
- 「関係者外秘」：関係者以外の人は見てはいけない。見せてはいけない。
- 「公開」：誰もが見ることが可能

ウ）誰が機密性を決めるのでしょうか？

新しく作成した電子ファイルについては、その都度機密レベルを決める必要がありますが、ある程度カテゴリーを決めておくことにより機密レベルの判断が容易になります。例えば、幹部会議資料は「社外秘」とするようなカテゴリーが考えられます。リスクアセスメントでは、情報資産の管理責任者を決めましたが、機密性の区分は情報資産の管理責任者が決定します。

エ）他には分類があるのでしょうか？

「極秘」、「機密」、「社外秘」、「公開」等の分類があります。

本ガイドラインではわかりやすく、「機密」と「一般」の２種類に分けていますが、通常３～４種類に分類します。

オ）暗号化の対象は？

何を暗号化するかは、企業や組織によって異なりますが、「Ｃ：機密性」と「Ｉ：完全性」の合計が一定値以上であることを目安に暗号化されることをお勧めします。

② 必要のない情報へのアクセス制限

ウイルス感染の機会を減らすためや情報漏えいを避けるために、業務上必要のない情報へのアクセスを制限します。

③ 利用の制限

「機密」に分類された電子データであっても、印刷された状態は暗号が解かれた状態であるため、機密性が損なわれます。また、外部への持ち出しも容易になります。電子データの不要なコピーについても機密性の管理対象が増え、盗難・紛失の機会が増えてしまいます。

④ 必要最低限のデータ

パソコン上のデータを必要最低限にすることで、盗難・紛失時の被害を最小に抑えられます。また、可用性が保たれた安全な領域にデータを保存しておくことにより、パソコンの故障等によるデータ損失を防止できます。

（実施方法）

⇒ 暗号化の詳細については、P.７３の HOW TO 編「５．ファイルやフォルダの暗号化」の項を参照してください。

◆事例

(3)公私区分

① 業務用に貸与されたパソコンを許可された目的外で用いることを禁止する。

② 業務用に貸与されたソフトウェアを許可なく私用パソコンにインストールすることを禁止する。

③ 私用パソコンを業務に利用する場合には、定められた利用条件に従うこと。

（解説）

① システム管理者は、業務用に貸与するパソコンに対し、業務アプリケーションの動作確認を行ったり、ウイルス対策ソフトを統一して導入したりしています。許可された目的外で利用してしまうと、業務アプリケーションやウイルス対策ソフト等の機能を阻害する場合があります。また、勝手に様々なソフトをインストールしたり、任意の Web サイトからファイルをダウンロードしたりすることにより、ウイルス感染等の脆弱性をついた攻撃を受けやすく、データの破壊や盗難される可能性が高くなります。

② 業務用に貸与されたソフトウェアを許可なく私用のパソコンにインストールした場合、ソフトウェア使用許諾等に記載されている事項に抵触する場合があります。

③ 私用パソコンを業務で利用する場合は、以下のような利用条件を規定することが大切です。

ア） ウイルス対策ソフトは指定されたものを利用する。

イ） パーソナルファイアウォール（※）を利用する。

⇒ ウイルス対策及びパーソナルファイアウォールについては、P.６９の HOW TO 編「１．ウイルス対策」、P．７４の「７．ファイアウォール」の項を参照してください。

３．「人」についての対策

情報セキュリティ対策の「ルール」・「人」・「技術」のうち、実施が最も難しいのは「人」の部分です。今日発生している情報漏えい事件の根源的な原因の多くは、関係者による内部犯行であると言われていることからも分かるように、適切なルールがあっても「人」すなわちテレワーク勤務者やシステム管理者等が定めた事項を遵守しなければ意味がありません。ルールを定着させるためには、以下のような対策を講ずることにより各個人レベルにおける情報セキュリティ意識の向上を図ることが重要です。

（ア）情報セキュリティ教育・啓発活動

従業員の情報セキュリティに関する認識を確実なものにするために、教育・啓発活動は欠かすことができません。情報セキュリティ教育・啓発活動は一過性のものではなく、日々の活動及び定期的な実施が重要です。

◆事例

(1) 社内外の研修や勉強会及びｅラーニング（※１８）等を活用し、情報セキュリティ教育を定期的に実施する。　(図１２)

※１８　ｅラーニング…パソコンや通信ネットワークを利用して教育を行うこと。遠隔教育や個人のライフサイクルにあわせた自己啓発学習などに多く利用されている。

（解説）

テレワーク勤務者は会社と離れた場所で業務を行うため、知識や意識の伝達が遅れがちとなってしまいます。そのため、情報セキュリティに関する集合教育を年に数回程度実施し、情報セキュリティの基礎知識や企業の情報セキュリティポリシーについて指導することが効果的です。なお、その際、情報セキュリティの知識やノウハウを豊富に持つ外部機関に講義を依頼することも有効な手段です。

また、テレワーク形態をうまく活用し、ｅラーニング（※）を採用することも、情報セキュリティ知識を底上げするという観点で効果を期待することができます。ｅラーニングは、「実践演習を伴う教育には不向き」、「自己管理が必要」といった問題がありますが、「都合の良いときに学習可能」、「個人のペースで学習可能」、「導入費用を安価に抑えられる」といったメリットを享受できるため、状況に応じて積極的に採用されることを推奨します。なお、ｅラーニングについても、専門の外部機関によるサービスを活用することが有効です。

さらには、情報セキュリティに関する Web サイトを参考にしたり、情報セキュリティに関する書籍・CD・ビデオ等を活用するなどし、情報セキュリティの意識レベルを向上させることも可能です。

参考サイト：総務省「国民のための情報セキュリティサイト」
http://www.soumu.go.jp/joho_tsusin/security/index.htm

(2) 情報セキュリティに関する冊子を作成し配布する。

（解説）

単に情報セキュリティポリシーにおける「対策基準」や「実施内容」等の書類や分厚いセキュリティ教本等を配布するだけでは効果を期待することはできません。配布物は、情報セキュリティ対策の実施内容を中心にポイントを絞った簡易冊子とし、読みやすく、理解しやすいものとするとよいでしょう。なお、「テレワーク勤務者向け」、「システム管理者向け」というように対象者別に冊子を作成すると、より効果的です。

また、冊子の配布のみならず、適宜、説明会を開催するなどして、さらなる意識向上を図ることをお勧めします。

（情報セキュリティ教育・啓発活動の注意点）

上記において、情報セキュリティリテラシーを向上させるための施策について述べてきましたが、情報セキュリティの意識レベルが一定レベル以上に保たれていなければならず、たった一人の人間によるずさんな管理が重大な情報セキュリティ事故を招いてしまうという意識をテレワーク勤務者に持たせることが大切です。そして、そのような情報セキュリティに対する意識を正しく教育・啓発することが、企業における大切な情報セキュリティ対策の一つとなるのです。

以下において、情報セキュリティ教育及び啓発活動を実施するうえでの注意点を説明します。

●教育・啓発活動のタイミング

情報セキュリティ教育については、いつ実施するかという問題があります。まず、第一に実施しなければならないのが、情報セキュリティポリシー策定直後のタイミングです。情報セキュリティポリシーの必要性及び内容について、時間をかけて教育する必要があります。また、社内システムや業務アプリケーションなどの情報資産を初めて利用する前にも、適切な教育を実施すべきです。さらには、新しいシステムを導入したり、手順の変更などがあった場合にも教育し直すことが必要です。

また、教育及び啓発活動は定期的に実施し、情報セキュリティに関する知識や、最新の情報セキュリティ事故などに関する情報を与えることが重要です。

●教育の内容

教育すべき内容としては、「情報セキュリティ事故発生時の報告手順」、「パスワードの取扱いについて」、「ウイルス・ワームへの対処方法」、「記録媒体の取扱いについて」などが考えられますが、これらの内容を教育する場合、「何が起こるか」、「どう対処するか」、「再発防止のために何ができるか」などの点について、テレワーク勤務者及び各担当者に対し、それぞれの職責に応じてできることは何かという点を明確に伝える必要があります。

なお、教育には、時事性のある具体的な内容を引用し、現実的な内容とすることが良いとされています。

●委託契約社員などへの教育

業務に係わるすべての利用者に対して教育を実施することを前提とした場合、委託契約社員などへの教育も必要となる場合があります。委託契約社員などに対する契約書では、必要な教育を受けていること前提とすることをお勧めします。

必要に応じて、組織内での教育に参加してもらい、社員と同等の情報セキュリティに関する認識を持ってもらうことが重要です。また、情報セキュリティポリシーや実施手順は企業によって内容が異なるため、職務経験が十分な委託契約社員に対しても、十分な教育が必要です。

（イ）規則・契約による管理

自社の従業員であっても、些細なミスや内部不正行為が大きな企業損失に拡大することもあります。テレワークは、様々な環境で業務を行うことが可能になることから、機密情報の外部流出を防ぐための機密保持規定を設けるとともに、抑止効果としてルールに違反した場合の罰則規定を設けることも有効です。

◆事例

(1) 就業規則（個人レベルの誓約書等を含む）及び外部委託契約には、機密保持条項を規定する。　（図１３）

(2) 就業規則及び外部委託契約には、ルール違反による事故が発生した場合の罰則規定を記載する。（抑止効果）

図１３　事例（１）機密保持条項の規定

機密保持･罰則規定

（解説）

●機密保持について

経営者とテレワーク勤務者の間で機密保持契約や守秘義務契約を結ぶことも、情報セキュリティ対策の一つです。しかし、機密保持の対象となる情報が何かということについて明確にしていない組織も多いようです。例えば「個人情報について正しく取扱うこと」という規定があったとしても、対象となる情報が明確になっていない場合、その契約は正しく履行されるとは限りません。情報分類によって明確にされた情報の重要性についても、テレワーク勤務者に認識してもらうことが重要です。

なお、機密保持は、正社員のみならず、委託契約社員や委託業者等にも適用することをお勧めします。

●雇用条件

テレワーク勤務者を雇用する際の条件にも情報セキュリティに対する責任について記述することが必要です。具体的には、ルール違反時の罰則規定や、場合によっては損害賠償規定も含め、就業規則及び委託契約に明記すべきでしょう。

なお、雇用期間中だけでなく、雇用終了後や勤務時間外にも守るべき情報セキュリティに関する事項、そしてこれらの責任を守らなかった場合にとる措置についても検討する必要があります。

（ウ）情報セキュリティ事故発生後の対応

情報セキュリティ事故が発生した場合は、迅速な対応策をとれるように連絡体制を整えたり、訓練（予行演習）をしたりしておくことも重要です。早期発見／早期対応することにより、情報セキュリティ事故の影響を最小限に抑えることが可能です。また、情報セキュリティ事故の原因を分析し、再発防止に努めることも重要となります。

◆事例

(1) 事故発生時の連絡体制を定める。

(2) 情報セキュリティ事故への対処マニュアルを作成する。

① 情報セキュリティ事故（パソコン紛失、盗難、ウイルス・ワーム感染）が発生した場合は、直ちに担当の○○○へ連絡する。

② テレワーク端末がウイルス・ワームに感染していると判明した場合、直ちに社内ネットワークへの接続を遮断する。

(3) 情報セキュリティ事故発生後は、要因を特定し、適正な対策を行うことにより、再発を防止する。

（解説）

情報セキュリティ事故が発生した場合、被害を最小限に抑えるためにも、テレワーク勤務者は定められたルールに従い、適切な対応をとらなければなりません。情報セキュリティ事故の対応方法を説明するうえで、「インシデント」という言葉を用いて、事故発生後に何を行うべきか解説します。

●インシデントとは

「インシデント（incident)」は「事件、出来事、事変」などを意味し、情報セキュリティにおいては、「情報資産の機密性、完全性、可用性が損なわれる事象」をインシデントと呼びます。

●インシデントの分類

・ 機密性を侵害するインシデントの例
ノートパソコンを紛失したことにより、保存されていた機密情報が漏えいする。
・ 完全性を侵害するインシデントの例
公開 Web サーバが不正アクセスを受け、サイトの内容が改ざんされる。
・ 可用性を侵害するインシデントの例
DoS 攻撃（※）を受け、メールサーバが停止する。

●インシデント対応の順序

インシデント対応の順序は大別すると以下の３項目となります。

(1) 初動処理 → (2) 復旧 → (3) 事後対応

(1) 初動処理

① 事前準備

事故が起きた場合、初動処理を適切に行うかどうかで、被害の範囲が大きく変わってきます。初動処理を行うためには、インシデントに対する事前準備が必要です。「インシデント対応マニュアル」などにより初動処理の手続きが明文化されており、教育・啓発活動によって対応手順が周知徹底されていれば、被害を最小限に食い止めることができるはずです。

インシデント対応マニュアルに記載すべき事項は、情報セキュリティ責任者や、インシデント対応フローなどが挙げられます。インシデント対応フローについては、次ページの「図１３　インシデント対応フローの例」に例示しているので、参考にしてください。

② 初動処理

しっかりとした事前準備が行われている場合には、対応マニュアルを参照しながらその指示に従いましょう。対応マニュアルが存在しない場合は、情報システム担当者等と連絡を取り合いながら適切な対応を行う必要があります。

(2) 復旧

① 原因の追究

初動処理によって被害の拡大を一時的に回避した後は、当然、元の状態に復旧しなければなりません。復旧するためには、まず、インシデントの内容や、検知方法、被害状況等を照らし合わせ、インシデント発生の原因を特定する必要があります。

② 被害範囲の特定

次に、把握した原因を元に、直接的な被害及び間接的な被害の影響範囲を見極めます。

③ システムの復旧

インシデント発生の原因が判明し、被害範囲を特定したら、システム管理者はシステムの復旧作業を開始します。

(3) 事後対応

① 評価

システムが復旧した後には、まず事故発生の原因分析を行い、情報セキュリティ対策上の落ち度はなかったか、情報セキュリティポリシー上欠落している事項はなかったかなどについて、評価を行う必要があります。

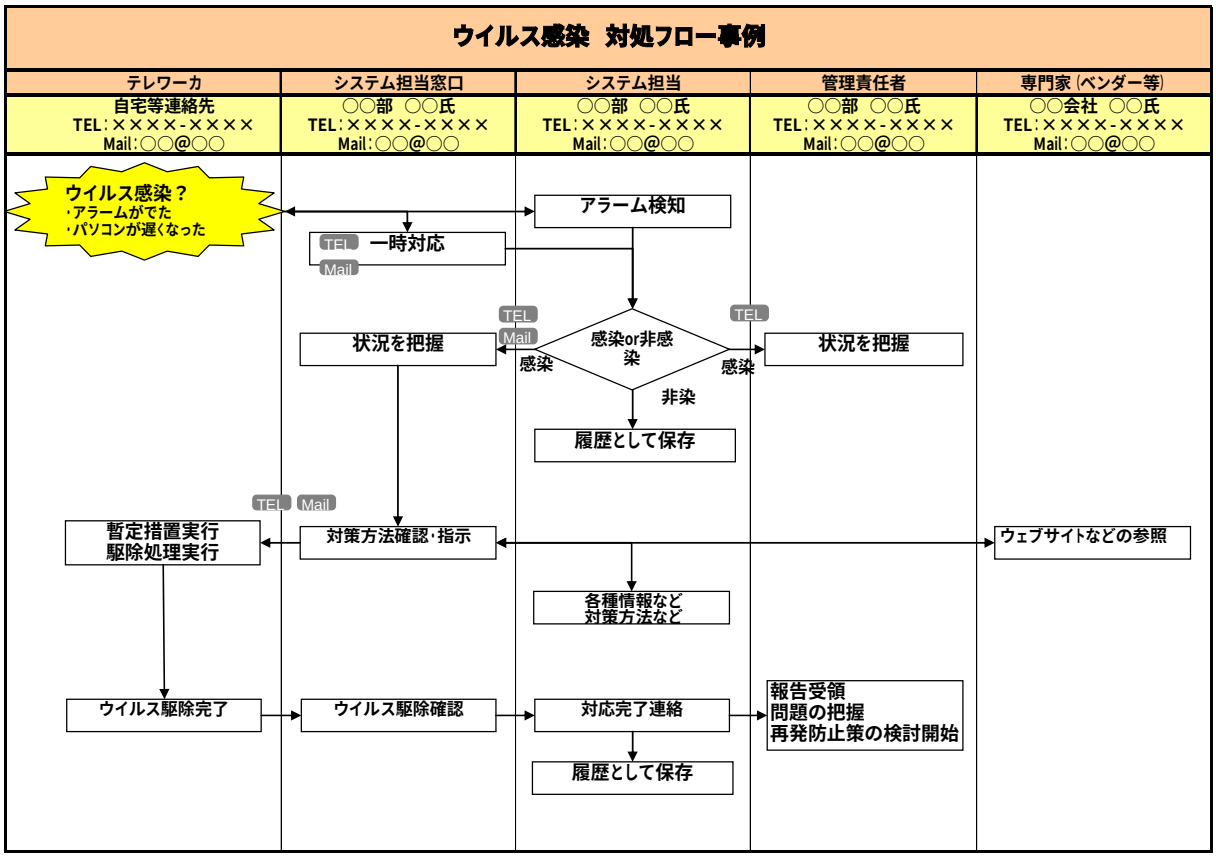
② 再発防止

原因分析による評価結果によって、再発防止策を検討します。

③ 公的機関への報告

インシデントの内容によっては、情報セキュリティを扱う公的機関に被害状況及び対応状況等について報告すべきものもあります。

図１３　インシデント対応フローの例



4．「技術」についての対策

技術的対策は「ルール」や「人」では対応できない部分を補完するものです。技術的対策は種々の脅威に対して「認証」、「検知」、「制御」、「防御」を自動的に実施するものであり、適切に対策を講じておく必要があります。ここではテレワーク環境を「テレワーク端末」、「通信経路」、「社内システム」に区分し、それぞれの情報セキュリティ維持のために最低限実施すべきことを示します。

（ア）テレワーク端末における対策

テレワークの特徴でもあるテレワーク端末では、社内環境と異なり、情報セキュリティ対策に関して「管理しづらい」または「管理できない」状況に陥りやすく、様々な脅威が存在します。以下では、パソコンをテレワーク端末として使用する場合に必要となる対策について記述します。なお、下記作業は、情報セキュリティ管理者やシステム管理者等の指示のもとで統一的に実施することが重要です。また、パソコンの情報セキュリティ管理（ウイルス定義ファイル更新やＯＳパッチ適用等）は、ひとりひとりが対応するには困難な場合があるため、ソフトウェア等を自動的に管理する仕組みを導入し、対策をより強化することが効果的です。

ウイルス・ワーム感染防止対策

テレワークにおいては、インターネットを利用する場合が多いため、最も発生確率が高いウイルス・ワームの脅威に対する対策は適切に実施する必要があります。

◆事例

(1) ウイルス対策ソフトのインストール及び定義ファイルの更新
ウイルス感染を検査し、感染したウイルスを駆除するため、ウイルス対策ソフトをインストールする。また、最新のウイルスに対応した定義ファイルに常時更新する。

(3) 外部より入手したファイルに対するウイルスチェック
受信メールに添付されたファイルや、インターネットからダウンロードしたファイル等を開く前に、ウイルス対策ソフトによる検査を実行する。

（解説）

やり取りしたデータ（メールの送受信、第三者からのデータまたはソフトウェアのダウンロード、CD-ROM によるデータの受け渡し等）の中にウイルスが混入している場合がありますが、これらを人的に対処することは不可能と言えます。

そのため、ウイルス感染によるデータの破壊や改ざんにより OS 及びアプリケーションソフトが異常な動作をしたり制御不能に陥ってしまったりする場合があります。コンピュータが意図しない動作を勝手にしたり、情報の漏えいなどが発生したりする危険性もあります。

また、ウイルスに感染した端末がネットワークに接続していると、他のコンピュータにも同じウイルスやワームを蔓延させてしまい、被害が急速に拡大してしまうことになります。

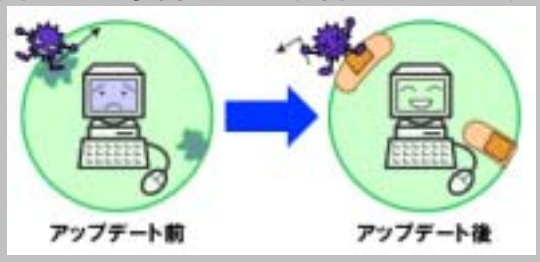
このようなウイルスの被害から防御するためには、それぞれのコンピュータにウイルス対策ソフトを導入しなければなりません。ウイルス対策ソフトを導入すると、多種多様なウイルスについて感染していないかどうかを自動的に検査することが可能になります。

それぞれのコンピュータが最新のウイルスにいち早く対応することができれば、自己のコンピュータへのウイルス感染を予防するだけでなく、ネットワークへのウイルス、ワームの蔓延を防止することができます。

⇒ ウイルス対策についての詳細は、P.６９の HOW TO 編「１．ウイルス対策」の項を参照してください。

(2) 最新のパッチを適用 （図１４）
OS 及びソフトウェアの脆弱性を突いたウイルス感染を防止するため、最新のパッチを適用する。また、システム管理者のアナウンス等によってパッチの適用がコントロールされている組織については、それに従う。

図１４　事例（２）最新のパッチ適用



（解説）

OS 及びアプリケーションには、セキュリティホールが存在していたり、情報セキュリティ対策機能が不足していたりすることがあります。

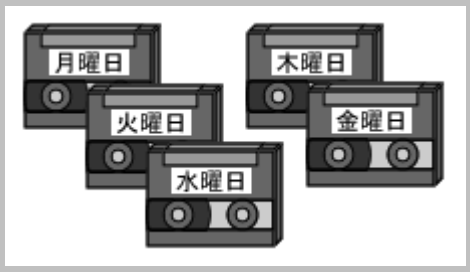
セキュリティホールとは、コンピュータの OS やソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを言います。セキュリティホールが残された状態でコンピュータを利用していると、セキュリティホールに対しての攻撃（バッファオーバーフロー（※）など）によるシステム異常が発生したり、ウイルスに感染したりする危険性があります。

セキュリティホールを塞ぐには、メーカーから配布されるパッチによって、OS やソフトウェアのアップデートが必要です。ただし、一度セキュリティホールを塞いでも、また新たなセキュリティホールが発見される可能性があるため、常に OS やソフトウェアの更新情報を収集して、できる限り迅速にアップデートを行わなければなりません。

既に業務に利用している環境では、パッチを適用する前に動作試験の実施が必要となる場合もあるため、利用環境によっては、管理者が適切な適用ルールを策定しておく必要があります。

(4) 電子データのバックアップ　(図１５)
ウイルス感染によって引き起こされる電子データ改ざんや電子データ破壊に対応するため、外部記録装置（ＣＤ－Ｒ／ＲＷ、ＵＳＢメモリ、外部ハードディスク等）への保存等、常時電子データのバックアップを実施しておく。

図１５　事例（４）電子データのバックアップ



（解説）

ウイルス感染による電子データの改ざんや電子データの破壊に対する最終的な防御方法は、外部記録装置にバックアップを残しておくことです。バックアップが残されていれば、少なくともバックアップした時点まで、データを復旧することが可能になります。

一般的なバックアップ方法は、テープメディア（※）や MO ディスク（※）、CD-R、DVD メディアなどの記録媒体に保管する方法ですが、それ以外にも情報セキュリティが保たれた（アクセス制御が適切になされ、ウイルスチェックや定期的にバックアップが実行されている）ファイルサーバに保管する方法などがあります。

バックアップによる対策はウイルス感染に限らず、人為的なミスによるデータの消去やコンピュータの故障、紛失などによるデータ紛失の対策にもなるため、業務データを操作したり、プログラム開発、ホームページ制作などの業務を行ったりする端末にとっては、とても重要なセキュリティ対策と言えます。

⇒　バックアップについての詳細は、P.７０の HOW TO 編「２．バックアップ」の項を参照してください。

端末等の紛失・盗難対策

テレワーク端末は、様々な場所での利用が想定され、その分、悪意ある第三者が近づきやすい環境にさらされることもあります。パソコン内の電子データを暗号化するなどして、他人によるテレワーク端末の不正操作を防ぎ、電子データの搾取及びパソコン等の紛失・盗難による情報漏えいを防止することができます。

◆事例

(1) 端末にはスクリーンセーバー（※１９）をかけ、解除する際、パスワードを問われるように設定する。また、パスワードは定期的に更新する。

※１９　スクリーンセーバー…ディスプレイの焼き付きを防止するために、一定時間アクセスがなかったら、画面上に動画を展開するプログラム。

（解説）

テレワーク端末は、移動中や出先において、端末を紛失したり、盗難にあったりすることによって、そのコンピュータに格納されている機密情報、個人情報などのデータが漏えいしてしまう可能性があります。

対策方法としては、スクリーンセーバーにパスワードをかけることで、端末を置いて離席している間に、端末を他人に利用されることを防ぐことが考えられます。なお、OS の種類によっては、スクリーンセーバーの解除時にログオン画面に戻すという機能が装備されているものもあります。

また、他人に推測されないような適切なパスワードを設定することが大切です。

⇒　パスワードについての詳細は、P.７１の HOW TO 編「３．パスワード」の項を参照してください。

(2) ＯＳへのログインパスワードを設定し、定期的に更新する。

（解説）

OS へのログインパスワードを適切に設定しておけば、端末が第三者に利用されてしまう場合にも、簡単には端末に格納されているデータを利用できないようにすることができます。

⇒　パスワードについての詳細は、P.７１の HOW TO 編「３．パスワード」の項を参照してください。

(3) パソコン内の機密と区分された電子データはファイル暗号化を行う。

（解説）

スクリーンセーバーや OS へのログオンに適切なパスワードを設定していても、何らかの理由で第三者に端末に格納されているデータにアクセスされる危険性は残されます。そのため、重要なファイルは暗号化しておくことが大切です。ファイルを暗号化するためには、専用のソフトウェアや OS に装備されているツールを利用してください。

また、現在一般的に利用されているワープロソフト、表計算ソフト、データベース（※）ソフトといった代表的なアプリケーションには、ドキュメントファイルに対して、パスワードを付けた保存機能が提供されているため、ファイル自体の暗号化とともに、このようなパスワード設定を複合して利用すると、さらに強固なセキュリティ対策になります。

⇒ 電子データの「機密」等の区分方法については、P.４５の「ルールについての対策」の「事例（２）パソコンで利用するデータの取扱い」の解説を参照してください。

⇒ ファイルに対する暗号化についての詳細は、P.７３の HOW TO 編「５．ファイルやフォルダの暗号化」の項を参照してください。

(4) 端末にはハードディスクの暗号化または BIOS（※２０）パスワードを設定する。

※２０ BIOS…コンピュータに接続された周辺機器を制御するプログラム。

（解説）

システムに正常にログオンできないようにした場合にも、端末の設定を変更されたり、コンピュータを分解して直接ハードディスクを操作されてしまったりすることも考慮しておかなければなりません。そのためには、BIOS（※）というコンピュータ自体を制御するプログラムの設定情報を変更できないようにすることや、ハードディスクを暗号化することが大切です。

⇒ ディスクに対する暗号化についての詳細は、P.７２の HOW TO 編「４．ディスクの暗号化」の項を参照してください。

(5) 機密と区分された電子データを記録媒体へ格納する場合は暗号化を行う。

（解説）

フロッピーディスク、CD-R、DVD メディア、USB メモリなど、外部メディアに機密データを移動またはコピーする場合には、それらのメディアの紛失や盗難に備えて、メディアまたはファイルを暗号化したり、パスワードを設定したりすることが大切です。

最近販売されている USB メモリなどでは、製品内に暗号化のツールが同梱されているものも増えているため、購入時にそのような製品を選択することも検討してください。

⇒ 電子データの「機密」等の区分方法については、P.４５の「ルールについての対策」の「事例（２）パソコンで利用するデータの取扱い」の解説を参照してください。

⇒ ディスクに対する暗号化についての詳細は、P.７２の HOW TO 編「４．ディスクの暗号化」の項を参照してください。

不正侵入・踏み台対策

テレワーク勤務者の知らないうちに悪意のあるソフトウェアをダウンロードしたり、テレワーク端末に悪意のあるソフトウェアを仕掛けられたりすることで、テレワーク端末が外部から「乗っ取られた状態」となり、電子データを盗難・改ざんされる危険性があります。また、テレワーク端末が「踏み台（※２０）」となって、社内システムに接続されたり、第三者に対して危害を加えたりする危険性があることから、下記のように端末を適正な状態にしておく必要があります。

※２１　踏み台…利用者が気付かないうちに第三者に乗っ取られ、不正アクセスや迷惑メール配信の中継地点に利用されているコンピュータのこと。

◆事例

(1) ＯＳのファイアウォール機能を利用する。または、パーソナルファイアウォールソフト(※２２)を導入する。

※２２　パーソナルファイアウォールソフト…不正アクセス等からパソコンを保護するためのソフトウェア。

（解説）

インターネットに接続する端末については、外部との境界に適切な防御壁を設置しておかなければ、ネットワークに不正に侵入されたり、端末に不正に侵入されたりすることがあります。

外部のネットワーク（インターネット）から内部のネットワークや端末を防御するためには、ファイアウォール（※）を導入しなければなりません。ファイアウォールには、ネットワーク全体を防御するものと、端末自体を防御するものがあります。

ファイアウォールにはソフトウェアとして提供されているものや、システムが組み込まれたハードウェアとして提供されているものなど、様々な種類のものがありますが、いずれの製品であっても、外部からの不正なパケットを遮断する機能や許可されたパケットだけを通過させる機能を持っています。最近では、ルータ（※）にファイアウォールの機能が装備されているものが多くなっています。

一般的なファイアウォールは、通過させるパケットや遮断するパケットに対する詳細なルールを設定して利用するため、TCP/IP プロトコルなどに対して、ある程度の知識を必要とします。TCP/IP プロトコルやインターネットについての基本的な知識を習得したうえで、適切な状態にファイアウォールを設置することができれば、情報セキュリティを一段階強化させることにつながります。

端末自体を防御するためには、パーソナルファイアウォールを導入することも大切です。パーソナルファイアウォールは、ハッカーからの不正侵入を防いだり、自分のコンピュータを外部から見えなくしたりすることが可能になります。なお、最近では、ウイルス対策ソフトとともにパッケージングした商品も増えてきているので、それらの導入も検討してください。

⇒　ファイアウォールについての詳細は、P.７４の HOW TO 編「７．ファイアウォール」の項を参照してください。

(2) 業務用に支給されたソフトウェア以外はダウンロード及びインストールしない。

（解説）

ソフトウェアによっては、外部にパスワードなどの情報を発信するスパイウェア（※）や、外部からの不正侵入を助けるためのトロイの木馬（※）が埋め込まれている場合があります。

対策としては、業務用に支給されたソフトウェア以外は、インストールしないことが大切です。業務上、何らかの機能を持つソフトウェアが必要な場合には、できる限り信頼できるメーカーのソフトウェアであることを確認することが大切です。なお、その場合には、事前にシステム担当者にそのソフトウェアを導入するということを申請し、許可を得ることをお勧めします。

また、インターネットの Web サイトでは、アクセスした端末に、利用者の同意をとらずにソフトウェアをダウンロードしようとする場合もあります。そのため、信頼できない Web サイトには接続しないなどの注意も必要です。

(3) 不審なサイトへはアクセスしない。

（解説）

OS や Web ブラウザのセキュリティホールや、ユーザのセキュリティ設定によっては、Web ページに埋め込んだプログラムによって、不正な行為を行うことができます。Web サイトによっては、そのサイトにアクセスしてきた端末に対して、ウイルスやトロイの木馬、スパイウェアを仕込むことがあります。

このような不審なサイトへのアクセスはなかなか防御が困難ですが、業務で利用している端末でインターネットにアクセスする場合には、できる限り慎重に利用することが大切です。

電子メールや Web ブラウザで、Web サイトに接続するときには、常に接続先の URL アドレスを認識する癖をつけて、自分が利用しようとしている Web サイトが安全なものであるか（または自分が接続しようとする Web サイトのアドレスであるか）ということを事前に確認することが必要です。

なお、それらのサイトにウイルスが埋め込まれている場合であっても、ウイルス対策ソフトが導入されていれば感染を防御することができます。

（イ）通信経路における対策

テレワークでは、インターネットを利用した電子データの送受をすることが想定されることから、電子データの盗聴、搾取、改ざん等の可能性があるため、暗号化された通信等、安全性の高い通信経路を確保する必要があります。

◆事例

(1) インターネットを利用したテレワークを実施する際には、ＶＰＮ等によりデータを暗号化し、安全な通信経路を確保する。

（解説）

インターネットで利用される HTTP（Web ページの閲覧に利用）や POP（メールの受信に利用）というプロトコルでは、データが暗号化されていません。そのため、暗号化されていないパケットデータは、通信経路において、盗聴または改ざんすることが可能になります。

VPN などを利用すると、ネットワーク全体の通信データを暗号化することができます。さらに、HTTPS プロトコルを使用して、Web ページのやり取りを暗号化したり、IMAP プロトコルを使用して、電子メールの受信データを暗号化したりすることも検討してみましょう。

また、遠隔地から社内システムにアクセスする他の手段として RAS（※）を利用することも可能です。

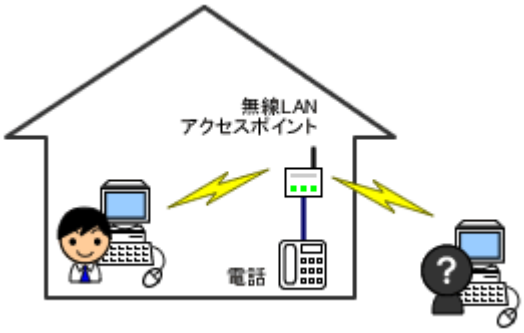
⇒ 通信データの暗号化についての詳細は、P.７５の HOW TO 編「８．通信データの暗号化」の項を参照してください。

⇒ RAS についての詳細は、P.７７の HOW TO 編「９．RAS（リモートアクセスサービス）」の項を参照してください。

(2) 無線ＬＡＮを利用する際には、暗号化機能を用いることで安全性を高める。

（解説）

図１４　無線 LAN イメージ



無線 LAN では、データの送受信に無線を利用しているため、遠隔地からアクセスポイント（※）を利用される危険性があります。

そのため、無線 LAN の機器に適切なセキュリティ設定を行わないままで使用した場合には、無線 LAN のアクセスポイントから内部のネットワークに侵入されることがあります。ネットワークに侵入されてしまうと、データの盗聴や改ざんなどの重大な被害を受ける可能性があります。また、侵入したネットワークを介して、インターネットから外部のコンピュータに危害を加える際の踏み台として利用されることもあります。

無線 LAN を利用する場合には、「WEP（※）による暗号化」、「MAC アドレスによるフィルタリング」、「SSID（※）の設定」が必須です。または、「WPA-PSK 方式（※）の暗号化技術」を導入する方法もあります。

⇒　無線 LAN についての詳細は、P.７７の HOW TO 編「１０．無線 LAN」の項を参照してください。

（ウ）社内システムにおける対策

社内システムには企業にとって守るべき電子データが多く存在します。テレワーク環境の特徴とも言える脆弱性を狙った不正侵入・不正アクセス、または社内システムからウイルスを蔓延させてしまう脅威などに対して十分な対策を行う必要があります。

ウイルス・ワーム感染防止対策

テレワーク端末側のみではなく、当然社内システムのサーバ及び社内ネットワークに接続されたパソコンについてもウイルス対策が必要です。実施すべき事項については、「テレワーク端末における対策」中の＜ウイルス・ワーム感染防止対策＞部分を参照してください。

ウイルス・ワーム蔓延防止対策

社内システムがウイルス・ワームに感染すると、多数のテレワーク端末にも感染し、ひいては社会全体に大きな影響を与えてしまう可能性があります。蔓延防止策は技術的にも運用的にも困難が伴いますが、「早期発見・早期対応」と「検知・制御」を考慮した対策を行う必要があります。

◆事例

(1) ウイルス・ワームがネットワーク上に蔓延することを防御するための仕組みとしてネットワーク上に流れるウイルスを検知し、駆除するシステムを導入する（運用体制の整備を含む）。

（解説）

ウイルス対策ソフトを適切に導入していない端末がネットワークに接続された場合には、ネットワーク上にウイルス・ワームが蔓延してしまう可能性があります。また、その端末にトロイの木馬等が組み込まれてしまった場合には、ネットワークに侵入する入り口として利用されてしまうこともあります。

そのような脅威から社内システム及びテレワーク端末を守るため、社内システムにウイルス防御システム（※）を導入し、ネットワーク上のウイルスを検出・除去したり、ウイルスに感染したパソコンをネットワークから隔離したりする仕組みを構築することをお勧めします。

なお、ウイルス防御システムを導入する際には、ウイルス・ワーム感染時に、迅速かつ円滑に対応可能な運用管理体制を築くことがポイントとなります。

(2) ウイルス・ワームに感染した端末は即座に隔離する（本人への通知・アクセスの制限等を含む）。

（解説）

たった 1 台の端末がウイルスに感染しただけで、ネットワーク自体やネットワークに接続されているその他多数のコンピュータに影響を与えてしまうことがあります。

ウイルス対策ソフトによっては、ウイルスやワームに感染した端末から接続のリクエストがあった場合に、その端末からの接続を一定時間拒否（アクセス制限による隔離）したり、管理者に連絡したりするような仕組みを持つものがあります。ウイルス・ワームに感染した端末を早期に発見し、まずは隔離（本人への通知・アクセスの制限等を含む）することが重要です。

不正侵入・不正アクセス対策

悪意ある第三者は、テレワーク環境を経由してシステムの脆弱性を探し、社内システムへ不正に侵入したり、アカウント保持者になりすまし社内システムへ不正にアクセスするなど、情報資産を悪用する場合があります。社内システムへアクセスするポイントや社内の守るべき情報資産との境界線にはファイアウォール等を設置することで不正侵入を防止する対策や、本人であることを厳密に確認する認証を行うことで情報資産へのアクセスを制御し、不正アクセスを防止する対策を行う必要があります。

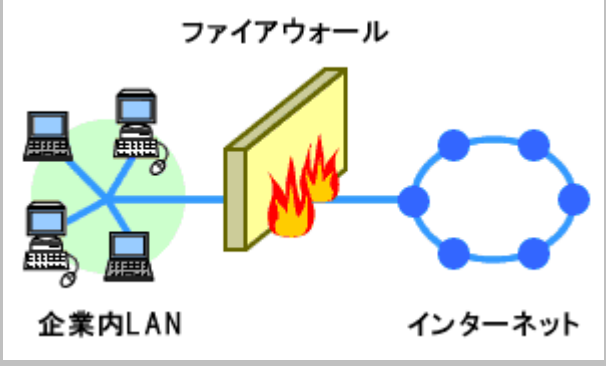
◆事例

(1) ファイアウォールやルータの設置　（図１６）

社内システムとの境界線にはファイアウォールやルータを設置し、パケットフィルタリング（※２３）を行う。

※２３　パケットフィルタリング…送られてきたデータを検査して通過させるかどうか判断する機能のこと。

図１６　事例（１）ファイアウォールの設置



（解説）

⇒　P.６１の「不正侵入・踏み台対策」事例(1)の解説を参照してください。

(2) 社外から社内システム／ネットワークへのアクセス制御
社外から社内システム／ネットワークへのアクセスについては、ユーザごと（各個人別）にアクセス権の設定を行うともに、パスワードはワンタイムパスワード（※２４）等を利用し認証機能を強化する。
※２４　ワンタイムパスワード…一度限りしか使えないパスワードを生成することを可能にした認証方式のこと。

（解説）

社外から接続するユーザには、適切なユーザ権限を設定することが大切です（ユーザ権限については、次の事例(3)の説明を参照してください）。また、ワンタイムパスワード（※）と呼ばれる一度しか利用できないパスワードを接続の要求のたびに配布する仕組みを持つことで、ネットワーク全体の情報セキュリティ強度を高めることができます。

(3) 守るべき電子データ（機密情報・個人情報等）へのアクセス制御
社内システム内にある守るべき電子データは、ファイアウォール等で守られた安全な領域に格納するとともに、アクセス権はユーザごと（各個人や組織）に権限を設定し、認証機能を利用してアクセスを制御する。

（解説）

社内のコンピュータに蓄積されている重要な電子データについては、必ず外部（インターネット）からは接続できない領域に配置することが大切です。また、社内のネットワークからであっても、特定のユーザ以外には接続できないように、各ユーザにユーザアカウントを配布したうえで、それぞれの情報資産に対する適切なユーザ権限を設定する必要があります。

ユーザ権限は、ファイルサーバやデータベースサーバなどで個別に設定することも、ネットワーク全体でまとめて設定することも可能です。いずれの場合にも、ユーザごとやグループごとに個別の権限を設定することができます。

たとえば、サーバに対しては、アドミニストレータ（管理者）権限（※）やユーザ（利用者）権限などがあります。データベースの場合には、データの登録や削除の権限、読み取りの権限、プログラムの実行権限などが設定できます。ある程度のユーザ数を持つネットワークの場合には、ユーザ権限を管理するための認証サーバを用意することで、ネットワーク全体の管理業務を軽減させることが可能になります。

それぞれのユーザアカウントを使用するためには、すべてのユーザが自分の所有す

るユーザ名とパスワードを使用して、本人性の確認のためにユーザ認証を受けなければなりません。もちろん、ユーザごとに適切な権限を設定していても、すべてのユーザがパスワードを設定していなかったり、誰にでもわかるようなパスワードを設定していたりしては何の意味もありません。適切なユーザ管理のためには、適切なパスワード管理が必須と言えます。

情報漏えい対策

不正侵入・不正アクセスによる情報漏えいを即座に検知・制御することは困難ですが、社内システムへの利用やアクセスログ（※２５）を収集することで不正侵入・不正アクセスによる情報漏えいの調査追跡が可能となります。

※２５　アクセスログ…サーバやルータの動作を記録したもの。アクセス元及びアクセス先の情報を記録し、利用者動向の分析や事故発生時の原因特定などに用いる。

◆事例

社内システムに接続した履歴の保存及び管理を行い、定期的に不正侵入・不正アクセスによる情報漏えいの調査を行う。

（解説）

ネットワークやシステムへの不正侵入・不正アクセスをリアルタイムで把握することは難しいものですが、ネットワークとインターネットの接続情報、Web サーバ、データベースサーバ、ファイルサーバ等に対するアクセス履歴を適切に保存しておくことによって、不正侵入・不正アクセスを調査追跡することが可能になります。

代表的なアクセスログ（※）には、以下のものがあります。

① ファイアウォールのログ：不正アクセスや攻撃の経歴情報が記録されます。
② ルータのアクセスログ:インターネットからのすべての接続情報が記録されます。
③ Web サーバのアクセスログ：Web サーバに対する接続情報が記録されます。
④ データベースサーバのアクセスログ：データベースに対するリクエストが記録されます。
⑤ リモートアクセスに関するログ：接続者ＩＤ、接続時間、接続の可否等の履歴が記録されます。

最近では、ファイルサーバに対して、アクセスログを保管して、どの端末からどのファイルに対してアクセスがあったのかということを管理することができるようにするソフトウェアも登場しています。社内に保管している情報資産の内容によっては、そのようなソフトウェアを導入することで、脅威の発生を抑止するとともに、情報漏えいが発生した場合に調査追跡を詳細に行うことが可能になります。

＜HOW TO 編＞

１．ウイルス対策

ウイルス対策には、主に、①ウイルス対策ソフトの導入、②ゲートウェイ型サービスの利用、③Web サービスによるウイルスチェックがあります。

① ウイルス対策ソフト

もっとも一般的な方法は、使用しているコンピュータにウイルス対策ソフトを導入することです。ウイルス対策ソフトには、数多くの種類があり、クライアント用だけでなく、サーバ用も販売されています。

② ゲートウェイ型

多くのプロバイダ（※）では、メールサーバ契約のオプションとして、ウイルス対策を実施しています。このようなサービスを利用すると、送受信するすべてのメールに対して、自動的にウイルス対策を実施してくれます。

③ Web サービス

いくつかのウイルス対策ソフトのメーカーでは、自社の Web サイトでウイルススキャンをサービスとして提供しています。ただし、無料のサービスの場合には、ウイルスの発見だけで、ウイルスの駆除は実行してくれないものもあるので、Web サイト上の説明をよく読んでから利用してください。

また、ウイルス対策ソフトとは異なり、リアルタイムにウイルスをチェックすることができるわけではないため、ウイルスに感染しているかどうかをチェックすることはできても、ウイルスの感染を予防することはできません。そのため、電子メールのやり取りやホームページの閲覧などを行う場合には、このような Web サービスによるウイルスチェックに頼らずに、必ずウイルス対策ソフトをインストールするようにしてください。

●ウイルス対策ソフトの機能

ウイルスを駆除するためには、コンピュータにウイルス対策ソフトを導入する必要があります。ウイルス対策ソフトは、ワクチンソフト、アンチウイルスソフトと呼ばれることもあります。一般的に、ウイルス対策ソフトはコンピュータの電源がオンであるときには常に起動した状態になり、外部から受け取るデータを常時監視することで、インターネットや LAN、フロッピーディスクなどからコンピュータがウイルスに感染することを防ぎます。また、逆に電子メールなどで外部に送信するデータにウイルスが含まれていないこともチェックしてくれます。コンピュータがウイルスに感染してしまった場合には、コンピュータからウイルスを除去する機能も持っています。

●ウイルス対策ソフトを利用するうえでの注意事項

現在のウイルス対策ソフトは、そのほとんどが今までのウイルスに対応するウイルス検知用データからウイルスを見つけ出す仕組みになっています。そのため、コンピュータにウイルス対策ソフトがインストールされていても、ウイルス検知用データが

古いままでは、新しいウイルスに感染してしまう危険性があります。このような検知用データは、一般的に「ウイルス定義ファイル」や「パターンファイル」、「シグネチャファイル」、「対策データ」などと呼ばれています。

最新のウイルス検知用データはたいていの場合、インターネットで配信するようになっていますが、これらのデータを受け取るためには、定期的にウイルス対策ソフトのメーカーと契約を結ぶ必要があります。一般的なウイルス対策ソフトでは、購入してから 1 年ごとに、ウイルス検知用データをダウンロードするための契約を更新する場合が多いようです。なお、最初からコンピュータにインストールされているウイルス対策ソフトの場合には、お試し版として 90 日程度の契約しか含まれていないことがあるので注意が必要です。

⇒ ウイルスについての詳細情報は、P.１１２の「参考資料５：代表的なウイルス」、P.１１３の「参考資料６：ウイルスの活動内容」、P.１１４の「参考資料７：代表的なウイルス」を参照してください。

２．バックアップ

安全にコンピュータを利用するためには、定期的なバックアップが不可欠です。端末では、ワープロソフトや表計算ソフトなどで作成したドキュメントファイルを始めとして、送信した電子メールや受信した電子メール、よく利用するホームページの URL アドレスなども、バックアップしておかなければなりません。

バックアップには、フロッピーディスクや MO ディスク、CD-RW（※）、DVD-RAM などの外部の記録媒体を利用する方法と、バックアップ用のファイルサーバにコピーする方法があります。

バックアップするファイルの数が多いときには、手動でファイルをコピーするのはとても大変な作業になってしまいます。その場合には、OS に付属しているバックアップツールや市販のバックアップソフトの導入を検討してみるとよいかもしれません。

なお、バックアップに使用した外部の記録媒体は、外に持ち出したり、机の上に放置したりすることは避けなければなりません。情報資産の分類によっては、鍵のかかる場所に保管するなど、適切な保管方法を検討してください。

●バックアップに利用されるメディア

・テープ

サーバにおいて最も一般的な方法は、テープドライブを利用するバックアップです。テープドライブで使用できるメディアは、ドライブごとに異なり、現在では DDS(※)、DLT（※）、LTO（※）といったディスクが多く使用されています。

・外部記録媒体

テープよりも安価で、高速に利用できるのが DVD-RAM や MO ディスク、CD-R といった外部記録媒体です。DVD-RAM などの DVD メディアでは、4.7GB といった大容量のデータを保存することもできます。

・ハードディスク
　RAID（※）を利用して複数のディスクに、データを分散して格納することもバックアップの一種と言えます。また、最近では大容量のハードディスクでも安価に入手できるようになったため、テープの代わりのバックアップメディアとして利用されることも多くなってきました。個人用においても、外付けのハードディスクにバックアップするという方法は、簡単で確実なバックアップ方法と言えます。

３．パスワード

　現在、コンピュータを利用するうえでは、様々な場面でパスワードを利用することになります。主に、以下のような場面で、パスワードを利用します。

　端末へのログオン時
　ネットワークへの接続時
　スクリーンセーバーの解除時
　システムの利用時
　プロバイダへの接続時

●適切なパスワード
　適切なパスワードとは、他人に推測されにくく、ハッキングツール（※）などの機械的な処理で割り出しにくいものを言います。適切なパスワードの作成条件としては、以下のようなものがあります。

・名前などの個人情報からは推測できないこと
・英単語などをそのまま使用していないこと
・アルファベットと数字が混在していること
・適切な長さの文字列であること

　逆に、危険なパスワードとしては、以下のようなものがあります。

・自分や家族の名前、ペットの名前
・電話番号や郵便番号、生年月日など、他人から類推しやすい情報
・従業員コード
・辞書に載っているような一般的な英単語
・"aaaaa"など、同じ文字の繰り返し
・ユーザ名と同じ文字列
・短かすぎる文字列

　インターネットなどで配布されているハッキングツールの中には、機械的にパスワードを推測する機能を持つものがあります。それらのハッキングツールでは、辞書に載っている英単語や簡単な英数字の繰り返し（123 や abc、aaa など）を自動的に組み合わせることで、パスワードを探し出そうとします。このようなハッキングツールで

パスワードを割り出されないようにするためには、機械的に推測される可能性が高い文字列を使わないようにすることが大切です。

●パスワードの保管方法
　適切なパスワードを設定しても、パスワードが他人に漏れてしまえば意味がありません。パスワードの保管に関しては、以下の点について特に注意してください。

・パスワードは、同僚などに教えないで、秘密にすること
・ユーザ名やパスワードを電子メールでやりとりしないこと
・パスワードのメモを作ったり、ディスプレイにそのメモを貼ったりしないこと
・パスワードを Web ブラウザなどのソフトウェアに記憶させないこと

●パスワードの定期的な変更
　安全なパスワードを作成し、パスワードの保管方法も徹底したとしても、同一のパスワードを長期間使い続けることは避けなければなりません。定期的にパスワードを変更するようにしましょう。また、定期的な変更といっても、2 つか 3 つのパスワードをあらかじめ決めておいて、使いまわすのは避けるようにした方がよいでしょう。

　パスワードを定期的に変更しなければならない理由には、以下のようなものがあります。

・他人に推測されにくいパスワードでも、ハッキングツールを使って長時間かければパスワードが割り出されてしまうこと
・仮にパスワードが割り出されてしまっても、被害を受け続けることを避けることができること

●パスワードの自動生成
　上記のような条件を満たすパスワードを作ることが困難な場合には、パスワード生成ソフトを利用するという方法も検討してください。パスワード生成ソフトは、指定した条件からランダムなパスワードを作り出してくれる機能を持つソフトウェアです。

４．ディスクの暗号化

　重要な情報資産や機密性の高い情報資産については、端末の紛失や盗難に備えて、ディスク自体を暗号化することも検討してください。
　ディスクを暗号化するソフトウェアを導入すると、指定したディスク全体を暗号化することができます。ソフトウェアによっては、内蔵のハードディスクだけでなく、MO ディスクやフロッピーディスクなどの記録媒体、ファイルサーバ上の共有フォルダに対しても、暗号化を行うことができるようになっています。

５．ファイルやフォルダの暗号化

重要な情報資産や機密性の高い情報資産については、個々のファイルまたはファイルを格納しているフォルダごとに、暗号化を設定するという方法も考えられます。ファイルやフォルダの設定には、専用の暗号化ソフトや OS に付属している機能を利用してください。

ただし、これらの暗号化の機能は、端末にログオンされてしまうと、普通に使用できてしまうこともあるため、端末にログオンするためのパスワードは必ず設定し、他人から推測されにくいものにしておかなければなりません。

また、これらの暗号化は、ファイルのコピーなどによって解除されてしまうこともあるため、必ずマニュアル等の説明をよく読んでから利用するようにすることと、過信せずに、あくまでも最終手段として考えることが大切です。

６．ハードディスクや記録媒体の廃棄

企業や組織の情報が漏えいするのは、ネットワーク経由とは限りません。コンピュータを廃棄したり、他人に譲渡したり、貸与されていたコンピュータを返却したりする場合には、搭載されているハードディスクから情報が漏えいする可能性があります。中古のコンピュータに前の所有者が利用していたデータがそのまま残されていたというトラブルが発生しているだけでなく、企業で利用していた形跡のある中古のコンピュータを意図的に購入して、そこに保存されているデータを探し出すという方法で機密情報を入手するという手口も実際に使われているようです。

特に注意が必要なのは、格納されているデータを削除したり、ハードディスクをフォーマットしただけで、コンピュータを処分してしまう場合です。画面上でデータが消えているように見えても、実際にはハードディスク上にデータが残されたままになっていることがあり、特殊なソフトウェアを利用することで、削除されたはずのファイルを復元することが可能です。

不要になったコンピュータのハードディスクの処理方法には、以下のようなものがあります。

・データ消去用のソフトウェアを利用する。
・専門業者のデータ消去サービスを利用する。
・コンピュータのハードディスクを取り出して、物理的に破壊してしまう。

これらの方法には、いずれも一長一短があり、残念ながら現時点では、絶対にこの方法が最良であるとは断言できません。これらの方法を企業・組織の情報資産の重要度に応じて組み合わせて、最適な方法を取るようにしましょう。また、当然のことですが、フロッピーディスクや MO ディスク、CD-R などの記録媒体を廃棄する場合にも、同様の処理を心がけなければなりません。

７．ファイアウォール

ファイアウォールとは、本来火災などから防御するための防火壁のことを言います。火災のときに被害を最小限に食い止めることから、インターネットの世界では、外部のネットワークからの攻撃や不正なアクセスから自分たちのネットワークやコンピュータを防御するためのソフトウェアやハードウェアをファイアウォールと呼ぶようになりました。

現在のファイアウォールには、主に 2 通りのものがあります。一つは家庭などにおいて、1 台のコンピュータを防御することを目的としたパーソナルファイアウォールで、もう一つは、企業や家庭のネットワーク全体を防御する本来のファイアウォールです。

ファイアウォールの設置は、外部のネットワークに接続した環境にとっては、必須と言える情報セキュリティ対策です。ただし、ファイアウォールを設置しても、それがネットワークに対する完全な情報セキュリティ対策になるわけではありません。あくまでも、ネットワークに対する攻撃や不正アクセスに対する情報セキュリティ対策の一つとして考える必要があります。

●パーソナルファイアウォール

パーソナルファイアウォールは、クライアントのコンピュータに導入するソフトウェアです。パーソナルファイアウォールを導入すると、そのコンピュータに対して、インターネットからの不正な侵入を防いだり、ウイルスの侵入を防御したり、自分のコンピュータを外部から見えなくしたりすることが可能になります。

パーソナルファイアウォールは、ウイルス対策ソフトと同様に、パソコンショップや家電販売店などで、パッケージソフトとして販売されています。最近では、ウイルス対策ソフトと組み合わせて、総合的な情報セキュリティ対策ツールとして販売していることも増えてきています。

必ず、ソフトウェアのマニュアルをよく読んで、購入したソフトウェアを自分の利用環境に合わせて設定するようにしてください。

また、プロバイダによっては、情報セキュリティサービスとして、ウイルスチェックとともに、ファイアウォール機能を提供している場合もあります。必要に応じて、それらのサービスの利用を検討してください。

●ファイアウォール

ファイアウォールは、インターネットと社内の LAN との間に設置するものです。この場合のファイアウォールの基本的な機能は、外部からの不正なアクセスを社内のネットワークに侵入させないことです。具体的には、外部からの不正なパケットを遮断する機能や、許可されたパケットだけを通過させる機能を持っています。このようなファイアウォールは、ソフトウェアとして提供されているものと、機器として提供されているものがあります。また、最近では、ルータにファイアウォールの機能が装備されているものが多くなっています。

●ファイアウォールの主要な機能
　ファイアウォールの主要な機能には、以下のようなものがあります。なお、これらの機能は機種によって異なるので、注意してください。

・フィルタリング機能
　不正なパケットを遮断して、許可されたパケットだけを通過させます。

・アドレス変換機能
　外部のネットワークと内部のネットワークにおいて、相互に IP アドレスを割り当てる機能です。

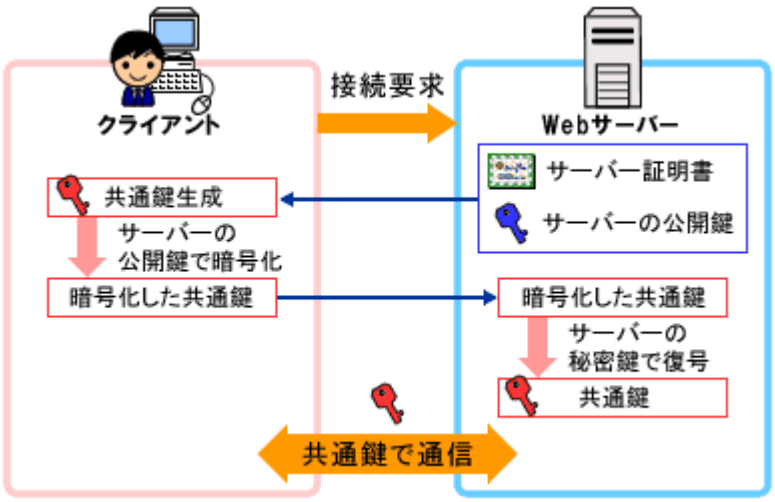
・遠隔操作、監視機能
　別のコンピュータからファイアウォールの設定を行ったり、ログを確認したりできる機能です。

８．通信データの暗号化

　会社と自宅を接続して、会社内の情報資産にアクセスしたり、サーバに接続する場合には、通信経路を暗号化する必要があります。通信経路の暗号化には、様々な方法がありますが、代表的なやり方には①SSL（※）による暗号化、②VPN による暗号化があります。

①SSL による暗号化
　SSL（Secure Socket Layer）とは、インターネット上でデータを暗号化して送受信する方法の一つです。
　通常、インターネットでは、暗号化されずにデータが送信されています。そのため、通信途中でデータを傍受されると、情報が第三者に漏れてしまう可能性があります。また、相手のなりすましに気付かずに通信すると、データがなりすましの相手に取得されてしまう可能性があります。そのため、クレジットカード番号や個人情報を扱う多くのホームページでは、通信途中での傍受やなりすましによる情報漏えいを防ぐ目的で、SSL を利用しています。
　利用者が SSL を利用できるサーバとデータをやり取りする場合には、Web サーバと利用者のコンピュータが相互に確認を行いながらデータを送受信するようになるため、インターネットにおける通信内容を暗号化すると同時に、なりすましの防止が実現されます。また、最近では、ホームページだけでなく、電子メールを SSL でやり取りするサービスも登場しています。
　ただし、SSL による暗号化を利用するには、サーバ側のサービス（アプリケーション）やクライアント側のソフトウェアが SSL に対応している必要があるため、すべての通信データに対して暗号化を実現できるわけではないという点に注意しなければなりません。

図１５　SSL による通信イメージ



IE（Internet Explorer）や Netscape などの SSL に対応した Web ブラウザを利用して、SSL で保護されたサイトに接続すると、通信相手の認証が行われ、通信データが自動的に暗号化されるようになります。このとき、主な Web ブラウザでは、ステータス欄に鍵のマークが表示されます。たとえば、IE では、SSL 接続を行っている場合には、右下のステータス欄に鍵のマークが表示されるようになっています。なお、この鍵のマークをダブルクリックすると、サーバ証明書の詳細情報を確認することができます。

図１６　SSL による通信のステータス

②VPN（Virtual Private Network）による暗号化

VPN は、通信データを暗号化することにより、インターネット回線を利用して、2 つの拠点（会社と自宅など）間を安全に接続することができる情報セキュリティ技術です。VPN を実現するには、それぞれの拠点において、VPN に対応した機器を用意する必要があります。最近では、VPN の機能が装備されたルータも増えてきました。

VPN で利用される代表的なプロトコルには、IPsec（※）や PPTP（※） があります。IPsec は IP のパケット自体を暗号化してやり取りする規格で、PPTP は 2 台のコンピュータ間で暗号化して通信する規格です。

９．RAS（リモートアクセスサービス）

RAS（リモートアクセスサービス）は、電話回線や ISDN（※）回線を使用して、外部のコンピュータから社内の LAN に接続することができる技術です。遠隔地から LAN に接続できるという便利さはありますが、RAS の回線をハッキングされてしまうと、ファイルサーバやデータベースサーバに直接侵入されてしまう危険性があります。

RAS を使用する場合には、コールバックという機能を利用することで、利用時の安全性を高めることができます。コールバックとは、通信回線から接続を要求してきた利用者に対して、認証後に接続を切断してから、あらかじめ登録されている電話番号をサーバが呼び出して接続する方式のことです。コールバックを利用すると、サーバ側から電話をかけ直すことになるため、テレワーク勤務者が通信料金を最初の発信分のみまたは負担額なしにできるというメリットもあります（最初の発信分の負担はコールバックの方式によって異なります）。

１０．無線 LAN

無線 LAN における一般的な情報セキュリティ対策には、WEP による暗号化、MAC アドレスによるフィルタリング、SSID の設定があります。もしくは、WPA-PSK 方式や WPA-EAP 方式（※）の暗号化技術を導入する方法もあります。

WEP は無線区間でデータを暗号化する機能です。暗号化を行うと、無線区間でデータを傍受されてしまっても、そのデータを解読することが困難になります。なお、現在 WEP による暗号化では 64 ビットまたは 128 ビットの暗号化鍵が使用されていますが、ビット数の大きい鍵の方が暗号解析に要する時間が長くなるので、できる限り 128 ビットの暗号化鍵を使用するようにしてください。また、より安全を確保する方策として、WEP で利用する暗号化鍵を推測しにくいものにしたうえで、暗号化鍵を定期的に変更することが重要です。しかしながら、WEP による暗号化は無線 LAN を安全に利用できることを保証するものでないため、データが解析される危険性があるということを常に認識して使用するようにしてください。

MAC アドレスによるフィルタリングは、無線 LAN のアクセスポイントにクライアントの MAC アドレスを登録しておくことにより、接続を許可するクライアントを制限できるという機能です。MAC アドレスによるフィルタリングを使用すると、外部からのネットワークへの侵入が難しくなります。しかしながら、利用可能な MAC アドレスを割り出し、詐称することが技術的には可能であるため、この点も意識しておく必要があります。

SSID とは、無線 LAN のネットワークの識別子であり、アクセスポイントと同一の SSID を設定した無線 LAN のクライアントのみが通信可能です。アクセスポイントの SSID の設定に際しては、氏名など容易に推測できる文字列を使用しないことと、SSID に「ANY」を設定したクライアントや SSID を空欄にしているクライアントからの接続を拒否するように設定することが大切です。また、機器によっては、ステルス機能という外部の第三者からの SSID 検索に応答しないようにする機能が装備されている場合もあります。機器のマニュアル等をよくお読みのうえ、できるだけ万全のセキュリティ対策機能を導入するようにしてください。

より高い情報セキュリティ対策を求める場合には、WPA-PSK 方式や WPA-EAP 方式の暗号化を利用する方法があります。

WPA-PSK 方式は、WEP に比べて強固な暗号化方式である TKIP（※）を採用しています。また、アクセスポイントと、これに接続するすべてのコンピュータに共通の文字列を登録しておき、この文字から生成される 128 ビットの PSK（Pre-Shared Key:事前共有鍵）によりコンピュータを認証します。なお、設定する文字数は 13 文字以上が理想的です。

WPA-PSK 方式は一般家庭や小規模のオフィスでは十分な情報セキュリティ対策です。しかし、企業や組織で無線 LAN を使用する場合には、より情報セキュリティの強固な WPA-EAP 方式の導入を推奨します。WPA-EAP 方式は、ユーザ認証「IEEE802.1x（※）」と新しい暗号化方式「TKIP」等を組み合わせたセキュリティ方式です。WPA-EAP 方式の特徴は、認証サーバによりクライアントを個別に認証して、クライアントごとに異なる鍵を安全な形で配信する点と、通信中はパケットごとに暗号化鍵を変更する点です。WPA-EAP 方式の導入には、認証サーバ設置等の高度な IT スキル、及びコストがかかりますが、高い情報セキュリティを施すことが可能になります。このことを踏まえたうえで導入を検討すべきでしょう。

参考資料１：代表的な情報セキュリティ基準について

ここでは、国外及び国内の情報セキュリティ基準の中で、代表的なものを取り上げ、それぞれについて解説します。本解説書では、様々な情報セキュリティ基準について触れていますので、しっかりと理解することが大切です。

表１７　代表的な情報セキュリティ基準

情報セキュリティ規格名称	概要
BS7799	BS7799 とは、BSI（英国規格協会）によって規定された情報システムセキュリティ管理のガイドラインで、BS7799-1 と BS7799-2 がある。BS7799-1 は情報セキュリティマネジメント（ISMS）の実施規範という位置付けである。これに対し BS7799-2 は情報セキュリティマネジメントの要求事項・仕様を定めた規格であり、この要求事項に合致した情報セキュリティマネジメントの仕組み（情報セキュリティマネジメントシステム）の構築、運用を行っている企業および組織に対して認証登録を行っている。
ISO/IEC17799	ISO/IEC17799 とは、BS7799-1 である情報セキュリティマネジメント実施規範の部分が ISO 標準として認定されたもの。
JIS X 5080	JIS X 5080 とは、ISO/IEC17799 が日本語に翻訳され、日本工業規格（JIS）として策定されたもの。
情報セキュリティマネジメントシステム：ISMS（Information Security Management System）	企業や組織が情報セキュリティを確保・維持するために、情報セキュリティポリシーに基づいた情報セキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのこと。
ISMS 適合性評価制度	企業の情報セキュリティマネジメントシステム(ISMS)が、ISO/IEC17799 に準拠していることを認定する、財団法人 日本情報処理開発協会(JIPDEC)の評価制度。BS7799-2 を基に作成された。
ISO/IEC TR 13335：GMITS （Guidelines for the Management for IT Security）	情報セキュリティ管理をするための手引書であり、各組織のセキュリティレベルを確保し、維持するためのガイドライン。

「表１７　代表的な情報セキュリティ基準」で説明した通り、BS7799、ISO/IEC17799、JIS X 5080、情報セキュリティ管理基準、ISMS 適合性評価制度は、それぞれ情報セキュリティマネジメントシステム（ISMS）について規定したものです。以下の図において、各基準が策定された流れを示します。

図１７　情報セキュリティマネジメントに関する基準の流れ

参考資料２：情報セキュリティマネジメントシステム（ISMS）について

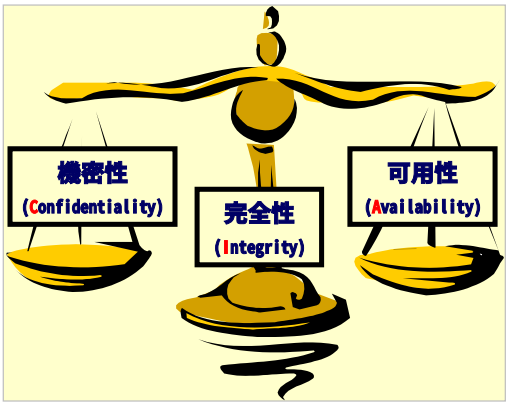
情報セキュリティマネジメントシステム（ISMS）の目的

「情報セキュリティマネジメントシステム（ISMS）」は、広範な脅威から情報を保護し、事業の継続性を確保し、事業継続上のダメージを最小化するとともに、収入、投資に対する収益、ビジネスチャンスを最大化する。

ISMS構築の意義

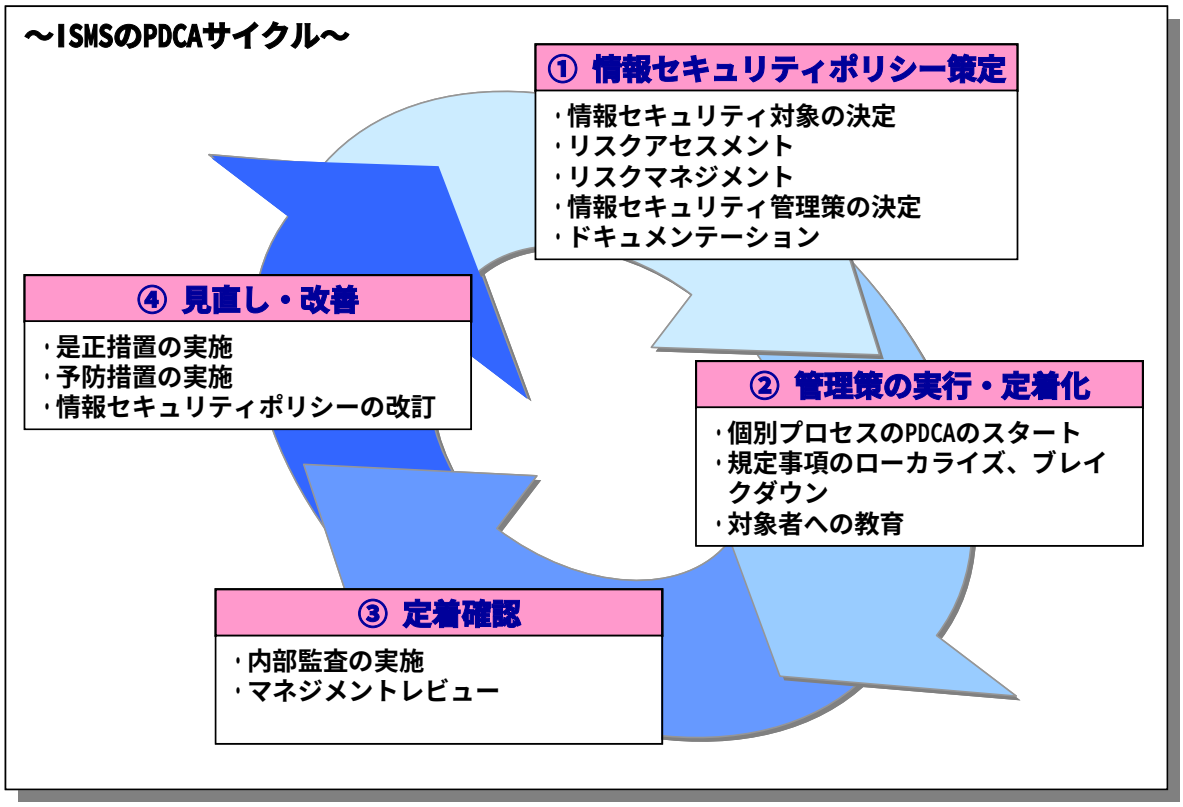
- 正式なマネジメントフレームワークを確立
  ＜組織的／一元的対応＞
- BS7799/ISMSおよび顧客要求事項による関連する情報セキュリティ対策の選択
  ＜網羅性＞
- 自己測定・自己改善プロセス
  ＜継続性＞

情報セキュリティの視点（＝C.I.A.）



情報セキュリティマネジメントシステム（ISMS）とは何か

ISMS とは、個別の問題ごとの詳細管理策の他に、組織のマネジメントとして、自らのリスク評価によって必要なセキュリティレベルを決定し、プランを持ち、資源配分して、システムを運用することです。



参考資料３：地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書のセルフチェックリスト

総務省では、全国の地方公共団体において、情報セキュリティポリシーに基づくセキュリティ対策の実施状況をチェックし、見直し・改善に生かすための有効な手法とされる情報セキュリティ監査の在り方について調査研究を行いました。

参考：地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書
http://www.soumu.go.jp/s-news/2003/031225_12.html#03

「地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書（以下、調査研究報告書）」における「セルフチェックリスト」は、地方公共団体職員が自団体の情報セキュリティポリシーの遵守状況等について、セルフチェック(自己点検)を行うための点検・評価項目を記載したもので、調査研究報告書における「地方公共団体情報セキュリティ管理基準」の中から、基本的な項目または優先順位の高い項目を選び出して作成したものです。

なお、本セルフチェックリストは、地方公共団体向けに記述されており、情報セキュリティのすべてを網羅するものではありませんが、ISO/IEC17799 を JIS 化した JIS X 5080 に準拠した記述内容となっており、情報セキュリティマネジメントシステムにおける構成要件の詳細を確認するには最適な資料です。

表１８　地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書のセルフチェックリスト

項番	管理基準項番	マネジメント領域	項目	目的	コントロール(管理目標)	サブコントロール(管理状況)	JISX 5080	ポリシーの例示	ガイドライン(H15.3版)要求事項及び説明	ガイドライン区分	判断基準		技術的検証項目
											パターン	参考(パターン1、2において実施の前提となる要件のガイド)	
1	1	1．セキュリティの基本方針	1.1 情報セキュリティ基本方針	A　情報セキュリティのための最高情報統括責任者(CIO)の指針及び支持を規定するため	1) 情報セキュリティポリシーは、首長等によって承認され、適当な手段で、全職員に公表し、通知すること	1) 情報セキュリティポリシーには、最高情報統括責任者(CIO)、CISO等、各管理者の責任を明記すること	3.1.1	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	3		
2	2					2) 情報セキュリティポリシーには、情報セキュリティの管理に対する地方公共団体の取組み方法を明記すること	3.1.1	1.4	ガイドライン(H15.3版)のIII-2-(2)に基づく確認事項	◎	3		
3	3					3) 情報セキュリティポリシーには、使用する用語の定義を明記すること	3.1.1	1.2	ガイドライン(H15.3版)のIII-2-(3)に基づく確認事項	◎	3		
4	4					4) 情報セキュリティポリシーには、その位置づけ、並びに関係者の遵守義務を明記すること	3.1.1	1.3	ガイドライン(H15.3版)のII-4に基づく確認事項	◎	3		
5	5					5) 情報セキュリティポリシーには、情報セキュリティ対策の目的を明記すること	3.1.1	1.1	ガイドライン(H15.3版)のIII-2-(3)に基づく確認事項	◎	3		
6	6					6) 情報セキュリティポリシーには、情報セキュリティ対策の適用範囲を明記すること	3.1.1	2.1	ガイドライン(H15.3版)のII-5に基づく確認事項	◎	3		
7	7					7) 情報セキュリティポリシーには、情報セキュリティ対策の重要性を明記すること	3.1.1	1.1	ガイドライン(H15.3版)のII-4に基づく確認事項	◎	3		
8	8					8) 情報セキュリティポリシーの制定･改廃は、情報セキュリティの目標を支持する首長等の決裁とすること	3.1.1		ガイドライン(H15.3版)II-4に基づく確認事項 JIS X5080では、意向声明書を含めることとしているが、各地方公共団体の文書管理規程や情報公開規程の定めを考慮し、首長等の決裁をもってこれに代わるものとする	◎	2	首長等の決裁が規則等で決められていること	
9	9					9) 情報セキュリティポリシーには、関連する法令への遵守等を明記すること	3.1.1	2.8	ガイドライン(H15.3版)のIII-2-(5)-⑧に基づく確認事項	◎	3		
10	10					10) 情報セキュリティポリシーには、セキュリティ教育を実施するよう明記すること	3.1.1	1.7(2)	ガイドライン(H15.3版)のIII-2-(5)に基づく確認事項	◎	3		
11	11					11) 情報セキュリティポリシーには、セキュリティ教育の要求事項を明記すること	3.1.1	2.5.(2)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	3		
12	22					22) 情報セキュリティポリシーには、コンピュータウイルス及び他の悪意のあるソフトウェアの予防及び検出を含めること	3.1.1	2.6.(5)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	3		
13	23					23) 情報セキュリティポリシーには、緊急時対応計画を含めること	3.1.1	2.7(4)	ガイドライン(H15.3版)III-2-(5)-⑦に基づく確認事項	◎	3		
14	24					24) 情報セキュリティポリシーには、ポリシー違反に対する措置を含めること	3.1.1	2.9	ガイドライン(H15.3版)III-2-(5)-⑨に基づく確認事項	◎	3		
15	25					25) 情報セキュリティポリシーには、セキュリティの事件･事故の報告を含めること	3.1.1	2.5.(3) 2.7(4)	ガイドライン(H15.3版)III-2-(5)-⑤及び⑦に基づく確認事項	◎	3		
16	26					26) 情報セキュリティポリシーには、情報セキュリティマネジメントにかかわる一般的権限を有する要員の責任の定義を含めること	3.1.1	2.5.(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	3		
17	27					27) 情報セキュリティポリシーには、情報セキュリティマネジメントにかかわる特定権限を有する要員の責任の定義を含めること	3.1.1	2.5.(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	3		
18	29					29) 情報セキュリティポリシーを、地方公共団体全体にわたって、利用可能かつ理解し易い形で利用者に適切に知らせること	3.1.1	1.7(2)	ガイドライン(H15.3版)のII-6に基づく確認事項	◎	1	利用者に周知する手順が確立していること	

19	34	2. 組織のセキュリティ	2.1 情報セキュリティ基盤	B	地方公共団体内の情報セキュリティを管理するため	1) セキュリティを主導するための明瞭な方向付け及び最高情報統括責任者（CIO）、CISO等による目に見える形での支持を確実にするために、当該地方公共団体の組織・体制を設置すること	1) セキュリティを主導するための明瞭な方向付け及び最高情報統括責任者（CIO）、CISO等による目に見える形での支持を確実にするために、当該地方公共団体の組織・体制を設置すること	4.1.1	2.2	ガイドライン(H15.3版)のIII-2-(2)に基づく確認事項	◎		2	体制表が決められていること	
20	40					2) 当該地方公共団体の組織・体制は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること	6) すべてのセキュリティ関連活動の責任は、当該地方公共団体の組織・体制に属する特定の者に集約すること	4.1.1	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎		2	体制の役割で規定されていること	
21	41					3) 情報セキュリティの管理策の実施を調整するために、地方公共団体の関連部門からの管理者の代表を集めた委員会を設置すること	1) 管理者の代表を集めた委員会では、地方公共団体全体の情報セキュリティのそれぞれの役割及び責任への同意を得ること	4.1.2	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎		2	委員会の役割で規定されていること	
22	43						3) 管理者の代表を集めた委員会では、地方公共団体全体の情報セキュリティの発議（例えば、セキュリティの意識向上プログラム）への同意及び支持を得ること	4.1.2	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎		2	委員会の役割で規定されていること	
23	47						7) 管理者の代表を集めた委員会では、目に見える形で地方公共団体全体への情報セキュリティに対する支援促進を行うこと	4.1.2	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎		2	委員会の役割で規定されていること	
24	48					4) 個々の資産の保護に対する責任及び特定のセキュリティ手続きの実施に対する責任を、明確に定めること	1) 情報セキュリティポリシーには、地方公共団体内のセキュリティの役割及び責任の割り当てに関する全般的な手引を規定すること	4.1.3	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎		3		
25	49						2) 情報セキュリティポリシーには、個別のサイト、システム又はサービスに関する詳細な手引を追加することを明記すること	4.1.3	1.9	ガイドライン(H15.3版)のIII-1に基づく確認事項 ガイドライン(H15.3版)のIII-3に基づく確認事項	◎		3		
26	50						3) 個々の物理的資産及び情報資産に限定した責任、並びに緊急時対応計画のようなセキュリティ対策を明確に定義すること	4.1.3	1.9	ガイドライン(H15.3版)のIII-3-(2)に基づく確認事項	◎		3		
27	51						4) 地方公共団体では、セキュリティの開発及び実行に対して全般的な責任をもち、管理策の識別を支持するために、一人の情報セキュリティ管理者を任命すること	4.1.3	2.3(1)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎		3		
28	52						5) 各情報資産に責任者を任命し、個々の情報資産の責任者はその資産のセキュリティに対して最終的な責任を持つこと	4.1.3	2.3(1)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎		3		
29	54						7) 各管理者が責任を負う範囲は明確に規定すること	4.1.3	2.3(1)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎		3		
30	56						9) 各資産又はセキュリティ手順に対する管理者の責任を定め、その詳細を文書化すること	4.1.3	2.3.(1)	ガイドライン(H15.3版)のIII-2-(5)-⑤に基づく確認事項	◎		3		
31	57						10) 承認の権限の範囲は、明確に定義され、文書化されること	4.1.3	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎		3		
32	58					5) 新しい情報処理設備に対する最高情報統括責任者（CIO）、CISO等による認可手続を確立すること	1) 新しい設備は、その目的及び用途について、適切な利用部門の管理者の承認を得ること	4.1.4	2.6(4)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎		2	規則等で定められていること	
33	72					8) 情報セキュリティポリシーの実施状況を、内部・外部の者がチェックし、見直すこと	1) 情報セキュリティポリシーには、情報セキュリティの基本方針及び責任を記述すること	4.1.7	1	ガイドライン(H15.3版)Ⅰ、Ⅱに基づく確認事項	◎		3		
34	78		2.2 第三者によるアクセスのセキュリティ	C	第三者によってアクセスされる地方公共団体の情報処理設備及び情報資産のセキュリティを維持するため	1) 地方公共団体の情報処理施設への第三者のアクセスに関連づけてリスクを評価し、適切な管理策を実施すること	6) 外部とのアクセスにかかわるすべてのセキュリティ要求事項又は内部管理策は、第三者との契約書に反映させること	4.2.1.3	2.6(3)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎		2	規則等で定められていること	
35	81					2) 地方公共団体の情報処理施設への第三者アクセスにかかわる取り決めは、正式な契約に基づくこと	1) 契約には、地方公共団体の情報セキュリティポリシー及び標準類に適合することを確実にするために、すべてのセキュリティ要求事項を含めるか又は引用すること	4.2.2	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎		2	規則等（契約締結基準等）で定められていること	

36	103					23) 契約書には、障害対策の取り決めを含めることを考慮すること	4.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤及び⑦ に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
37	106					26) 契約書には、変更管理の明確な設定された手続を含めることを考慮すること	4.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤及び⑦ に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
38	107					27) 契約書には、要求される物理的保護の管理策及びそれらの管理策の実施を確実にするための仕組みを含めることを考慮すること	4.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤及び⑦ に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
39	108					28) 契約書には、利用者及び管理者に対する方法、手順及びセキュリティについての訓練を含めることを考慮すること	4.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤及び⑦ 記載のポリシー遵守体制に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
40	109					29) 契約書には、悪意のあるソフトウェアからの保護を確実にするための管理策を含めることを考慮すること	4.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤及び⑦ 記載のポリシー遵守体制に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
41	110					30) 契約書には、セキュリティ事件・事故及びセキュリティ違反についての報告、通知及び調査に関する取り決めを含めることを考慮すること	4.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤及び⑦ に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
42	111					31) 契約書には、第三者と下請け業者とのかかわりを含めることを考慮すること	4.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤及び⑦ に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
43	112					32) 契約書には、個人情報を含む特に重要な情報の暗号化の実施、目的外利用の禁止、受託者以外の者への提供の禁止などを含むこと		2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤及び⑦ に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
44	113		2.3 外部委託	D 情報処理の責任を別の組織に外部委託した場合における情報セキュリティを維持するため	1) 情報システム、ネットワーク及び/又はデスクトップ環境についての、マネジメント及び統制の全部又は一部を外部委託する組織のセキュリティ要求事項は、当事者間で合意される契約書に記述されること	1) 外部委託契約書等には、法的な要求事項（例えば、データ保護に関連して制定された法律）をどのように満たすかを取り扱うこと	4.3.1	2.5.(1)、(4)	ガイドライン(H15.3版) III-2-(5)-⑤、⑦に基づく確認事項 外部委託に対する管理指針の一つ	◎	2	規則等（契約締結基準等）で定められていること	
45	114					2) 外部委託契約書等には、受託業者を含め、外部委託にかかわるすべての当事者がそれぞれのセキュリティの責任についての認識を確実にするためにどのような取り決めが適切であるかを取り扱うこと	4.3.1	2.5(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
46	115					3) 外部委託契約書等には、地方公共団体の情報資産の完全性及び機密性をどのように維持し、それを検証するかを取り扱うこと	4.3.1	2.5(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
47	116					4) 外部委託契約書等には慎重な取扱いを要する地方公共団体の業務情報への認可された利用者によるアクセスを制約及び制限するために、どのような物理的及び論理的管理策を用いるかを取り扱うこと	4.3.1	2.5(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	○
48	117					5) 外部委託契約書には災害の際に、サービスの可用性をどのように維持するかを取り扱うこと	4.3.1	2.5.(1)、(4)	ガイドライン(H15.3版) III-2-(5)-⑤、⑦に基づく確認事項 外部委託に対する管理指針の一つ	◎	2	規則等（契約締結基準等）で定められていること	○
49	118					6) 外部委託契約書には外部委託した装置については、どのようなレベルの物理的セキュリティを施すかを取り扱うこと	4.3.1	2.5.(1)、(4)	ガイドライン(H15.3版) III-2-(5)-⑤、⑦に基づく確認事項 外部委託に対する管理指針の一つ	◎	2	規則等（契約締結基準等）で定められていること	○
50	119					7) 外部委託契約書等には監査する権利を取り扱うこと	4.3.1	2.5(1)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎	2	規則等（契約締結基準等）で定められていること	
51	123	3. 資産の分類及び管理	3.1 資産に対する責任	E 地方公共団体の資産の適切な保護を維持するため	1) 情報システムそれぞれに関連づけて重要な資産について目録を作成し、維持すること	2) 情報システムそれぞれに関連づけて重要な資産について目録を作成すること	5.1.1	2.3	ガイドライン(H15.3版) III-2-(4)に基づく確認事項	◎	2	規則等で定められていること	

52	124					3) 情報システムそれぞれに関連づけて個人情報を含む特に重要な情報について目録を作成すること		2.3	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	2	規則等で定められていること	
53	125					4) 各資産を、その現在の所在とともに、明確に識別すること	5.1.1	2.3	ガイドライン(H15.3版)III-2-(4)に基づく確認事項	◎	2	規則等で定められていること	○
54	129		3.2 情報の分類	F 情報資産の適切なレベルでの保護を確実にするため	1) 情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要及びこのような必要から起こる業務上の影響（例えば、情報への認可されていないアクセス又は情報の損傷）を考慮に入れておくこと	1) 情報及び重要なデータを取り扱うシステムからの出力は、それが地方公共団体に対して持つ価値及び取扱い重要度によってラベル付けすること	5.2.1	2.3(2)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	ラベル付けの手順が確立していること	
55	134					6) 情報（例えば、文書、データ記録、データファイル又は記録媒体）の分類を定める責任及びその分類を定期的に見直す責任は、その情報の作成者又は指定された管理者にあること	5.2.1	2.3	ガイドライン(H15.3版)III-2-(4)-③に基づく確認事項	◎	2	規則等で定められていること	
56	136				2) 地方公共団体が採用した分類体系に従って情報のラベル付け及び取扱いをするための、一連の手順を定めること	2) 各分類について、複製に適用する取扱い手順を定めること	5.2.2	2.3(1) 2.3(2)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	取り扱い手順が確立していること	
57	137					3) 各分類について、保存に適用する取扱い手順を定めること	5.2.2	2.3(2)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	取り扱い手順が確立していること	
58	138					4) 各分類について、郵便による伝達に適用する取扱い手順を定めること	5.2.2	2.3(2)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	取り扱い手順が確立していること	
59	139					5) 各分類について、ファクシミリによる伝達に適用する取扱い手順を定めること	5.2.2		外部との情報のやりとりに際して、適用すべき事項である		1	取り扱い手順が確立していること	
60	145					11) 各分類について、破棄に適用する取扱い手順を定めること	5.2.2	2.3(2)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	取り扱い手順が確立していること	
61	146					12) 取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを付けること	5.2.2	2.3	ガイドライン(H15.3版)III-2-(4)-③に基づく確認事項	◎	2	規則等で定められていること	
62	148	4. 人的セキュリティ	4.1 職務定義及び雇用におけるセキュリティ	G 人による誤り、盗難、不正行為又は設備の誤用のリスクを軽減するため	1) セキュリティの役割及び責任は、地方公共団体の情報セキュリティポリシーで定められたとおりに、職務定義書のなかに文書化すること	1) セキュリティの役割及び責任を文書化したものには、セキュリティ基本方針を実行又は維持するための一般的な責任のすべてを含めること	6.1.1	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	3		
63	149					2) セキュリティの役割及び責任を文書化したものには、特定の資産を保護するための具体的な責任を含めること	6.1.1	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	3		
64	150					3) セキュリティの役割及び責任を文書化したものには、特定のセキュリティの手続を含めること	6.1.1	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	3		
65	151					4) セキュリティの役割及び責任を文書化したものには、特定のセキュリティ活動を進めるための具体的な責任を含めること	6.1.1	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	3		
66	165				3) すべての職員及び情報処理設備の外部利用者は、機密保持又は守秘義務を雇用条件の一部として同意すること	1) 既存の職務規程（機密保持条項を含むもの）の効力が及ばない臨時職員及び外部委託者に対しては、情報処理設備へのアクセスを認める前に、機密保持契約書への署名を要求すること	6.1.3	2.5(1)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	2	規則等で定められていること	
67	169				4) 雇用条件には、情報セキュリティに対する職員の責任について記述してあること	3) 著作権法又はデータ保護に関連して制定された法律等に基づく、職員の責任及び権利を明確にすること	6.1.4	2.8	ガイドライン(H15.3版)のIII-2-(5)-⑧に基づく確認事項	◎	2	規則等で定められていること	
68	173		4.2 利用者の訓練	H 情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の業務のなかで利用者が地方公共団体のセキュリティ基本方針を維持していくことを確実にするため	1) 地方公共団体の基本方針及び手順について、地方公共団体のすべての職員及び関係する外部利用者を適切に教育し加えて定期的に更新教育を行うこと	1) 教育には、セキュリティ要求事項、法律上の責任及び業務上の管理策とともに、情報又はサービスへのアクセスを許可する前に実施する、情報処理設備の正しい使用方法（例えば、ログオン手順、パッケージソフトウェアの使用方法）に関する訓練を含むこと	6.2.1	2.5(2)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	2	教育内容が定められていること	
69	174		4.3 セキュリティ事件・事故及び誤動作への対処	I セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため並びにそのような事件・事故を監視してそれらから学習するため	1) セキュリティ事件・事故は、適切な連絡経路を通して、できるだけ速やかに報告すること	1) 事件・事故の正式な報告手順を、事件・事故への対処手順とともに確立すること	6.3.1	2.5(3)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	1	報告手順、対処手順が確立していること	
70	175					2) 事件・事故の正式な報告を受けたならば直ちに取るべき措置に着手できるようにすること	6.3.1	2.5.(3)	ガイドライン(H15.3版)III-2-(5)-⑤に基づく確認事項	◎	1	報告を受けた際の処理手順が確立していること	

71	176					3) すべての職員及び請負業者に、セキュリティ事件・事故の報告手順を認識させておくこと	6.3.1	2.5(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	認識させるための手順が確立していること	
72	177					4) すべての職員及び請負業者に、セキュリティ事件・事故をできるだけ速やかに報告するよう要求すること	6.3.1	2.5(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則、契約等で規定されていること	
73	179				2) 情報サービスの利用者に対して、システム若しくはサービスのセキュリティの弱点、又はそれらへの脅威に気づいた場合若しくは疑いをもった場合は、注意を払い、かつ報告するよう要求すること	1) すべての職員及び受託業者が、事件・事故の発生を知った場合又はその疑いを持った場合は、できるだけ速やかに、自分の管理者又はサービス提供者に対し直接報告するよう手順を確立すること	6.3.2	2.5(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則、契約等で規定されていること	
74	192				5) 地方公共団体のセキュリティ基本方針及び手順に違反した職員に対する、正式な懲戒手続を備えていること	1) 違反した職員に対する、正式な懲戒手続は、重大な又は度重なるセキュリティ違反を犯した疑いのある職員に対して、正しく、かつ、公平な取扱いを確実にするものであること	6.3.5	2.9	ガイドライン(H15.3版) III-2-(5)-⑨に基づく確認事項	◎	1	手続の手順が確立していること	
75	193	5. 物理的及び環境的セキュリティ	5.1 セキュリティが保たれた領域	J 業務施設及び業務情報に対する認可されていないアクセス、損傷及び妨害を防止するため	1) 地方公共団体は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること	1) セキュリティ境界を明確に定義すること	7.1.1	2.4(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	セキュリティ境界定義の手順が確立していること	○
76	196					4) 敷地又は建物への物理的アクセスを管理するために、有人の受付又はその他の手段を設けること	7.1.1	2.4.(2)	ガイドライン(H15.3版) III-2-(5)-④に基づく確認事項	◎	2	規則等で定められていること	
77	200				2) 認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によってセキュリティの保たれた領域を保護すること	1) セキュリティが保たれた領域への訪問者を監視すること	7.1.2	2.4(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	監視の手順が確立していること	
78	202					3) セキュリティが保たれた領域への訪問者に立ち入り許可を求めさせること	7.1.2	2.4(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	許可の手順が確立していること	
79	203					4) セキュリティが保たれた領域への入退の日付・時間を記録すること	7.1.2	2.4.(2)	ガイドライン(H15.3版) III-2-(5)-④に基づく確認事項	◎	2	手順等で定められていること	
80	204					5) セキュリティが保たれた領域への訪問者には、認可された特定の目的に限ってのアクセスを認めること	7.1.2	2.4.(2)	ガイドライン(H15.3版) III-2-(5)-④に基づく確認事項	◎	2	手順等で定められていること	
81	207					8) 取扱いに慎重を要する情報及び情報処理設備へのアクセスは認可された者だけに制限すること	7.1.2	2.4(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	手順等で定められていること	
82	208					9) アクセスの認可の妥当性を確認するために、暗証番号付きの磁気カードといった認証管理策を用いること	7.1.2	2.4(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	管理策実施の手順が確立していること	
83	210					11) すべての要員に、目に見える何らかの形状をした身分証明の着用を要求すること	7.1.2	2.4(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
84	214				3) セキュリティが保たれた領域の選択及び設計においては、火災、洪水、爆発、騒擾、その他の自然又は人為的災害による損害の可能性を考慮すること	3) 主要な設備は、一般の人のアクセスが避けられる場所に設置すること	7.1.3	2.4.(2)	ガイドライン(H15.3版) III-2-(5)-④に基づく確認事項	◎	2	規則等で定められていること	
85	218					7) 要員が不在のときは扉及び窓に施錠すること	7.1.3	2.4.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
86	229					18) 特に重要とされる情報について、第三者が管理するものから物理的に分離しておくことが困難な場合において、電磁的情報漏洩への対策を施すこと		2.4.(2)	ガイドライン(H15.3版) III-2-(5)-④に基づく確認事項	◎	2	規則等で定められていること	
87	233					3) セキュリティが保たれた領域を無人にするときは、物理的な施錠を行うこと	7.1.4	2.4(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
88	235					5) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスを許可するときは、アクセスができる範囲を限定し、アクセスが必要な場合に限ること	7.1.4	2.4.(2)	ガイドライン(H15.3版) III-2-(5)-④に基づく確認事項	◎	1	アクセス管理の手順が確立していること	
89	236					6) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは認可の下におくこと	7.1.4	2.5(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	アクセス管理の手順等で定められていること	

90	237					7) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは監視下におくこと	7.1.4	2.4(2)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	2	アクセス管理の手順等で定められていること	
91	238					8) あるセキュリティ境界の中にセキュリティ要求事項の異なる領域が存在するときは、その領域の間に、物理的アクセスを管理するための障壁及び境界を追加すること	7.1.4	2.4.(2)	ガイドライン(H15.3版)III-2-(5)-④に基づく確認事項	◎	2	規則等で定められていること	
92	254		5.2 装置のセキュリティ	K 資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため	2) 装置は、停電、その他の電源異常から保護すること	2) 電源の多重化をすること	7.2.2	2.4.(1)	ガイドライン(H15.3版)III-2-(5)-④に基づく確認事項	◎	2	規則等で定められていること	
93	255					3) 無停電電源装置（UPS)を設置すること	7.2.2	2.4(1)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
94	268				3) データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること	2) ネットワークのケーブル配線を、電線管を使用する、又は公衆域を経由する配線経路を避けることなどによって、認可されていない傍受又は損傷から保護すること	7.2.3	2.4(1)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
95	274					8) 認可されていない装置がケーブルに取り付けられているかどうかについて調査すること	7.2.3	2.4.(3)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	1	調査の手順が確立していること	
96	277				4) 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施すること	3) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守について記録すること	7.2.4	2.6.(4)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	1	記録の手順が確立していること	
97	279					5) 装置を保守するために搬出する場合、適切な管理策を施すこと	7.2.4	2.6.(4)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	1	搬出の手順が確立していること	
98	282				5) 所有権に関係なく、地方公共団体の敷地外で情報処理のために装置を使用する場合は、管理者が認可すること	2) 事業所外に持ち出した装置及び媒体は一般の場所に放置しないこと	7.2.5	2.6.(4)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
99	289				6) 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に上書きすること	1) 個人情報を含む特に重要な情報資産を記録した媒体等の処分の際には、確実に消去すること		2.3.(2)	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	消去の手順が確立していること	
100	291					3) 取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアが、消去又は上書きされているか確認すること	7.2.6	2.6.(4)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	1	確認の手順が確立していること	○
101	297		5.3 その他の管理策	L 情報及び情報処理設備の損傷又は盗難を防止するため	1) 地方公共団体は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、書類及び取外し可能な記憶媒体に対するクリアデスク方針の適用、並びに情報処理設備に対するクリアスクリーン方針の適用を考慮すること	6) PC、コンピュータ端末及び印字装置は、使用しないときは、施錠、パスワード又は他の管理策によって保護すること	7.3.1	2.4.(2)	ガイドライン(H15.3版)III-2-(5)-④	◎	1	アクセス管理の手順が確立していること	○
102	300					9) 取扱いに慎重を要する情報又は機密情報を印刷した場合、印字装置から直ちに取り出すこと	7.3.1	2.5.(2)	ガイドライン(H15.3版)III-2-(5)-⑤	◎	2	手順等で定められていること	
103	301				2) 装置、情報又はソフトウェアは指定場所から無認可では持ち出しできないこと	1) 許可を得て持ち出すときは、持出し時及び返却時に記録を残すこと	7.3.2	2.6.(2)	ガイドライン(H15.3版)III-2-(5)-⑥	◎	1	持ち出しの手順が確立しており、その中で定められていること	
104	302					2) 認可されていない資産の移動が行われていないか、現場検査を実施すること	7.3.2	2.6.(2)	ガイドライン(H15.3版)III-2-(5)-⑥	◎	1	検査の手順が確立していること	
105	304	6. 通信及び運用管理	6.1 運用手順及び責任	M 情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため	1) セキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと	1) 操作手順は、正式な文書として取り扱うこと	8.1.1	1.9	ガイドライン(H15.3版)III-3-(2)に基づく確認事項	◎	2	規則等で定められていること	
106	305					2) 操作手順を変更する場合は管理者によって認可されること	8.1.1	1.9	ガイドライン(H15.3版)III-3-(2)に基づく確認事項	◎	2	規則等で定められていること	
107	306					3) 操作手順には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	1.9	ガイドライン(H15.3版)III-3-(2)に基づく確認事項	◎	3		

108	307					4) 操作手順には、スケジュール作成に関する要求事項を含む、各作業の詳細な実施に関する指示を明記すること なお、スケジュール作成に関する要求事項の中には、他のシステムとの相互依存、もっとも早い作業の開始時刻、及びもっとも遅い作業の完了時刻を含むこと	8.1.1	1.9	ガイドライン(H15.3版) III-3-(2)に基づく確認事項	◎		3		
109	308					5) 操作手順には、作業中に発生し得る誤り又はその他の例外状況の処理についての指示を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	1.9	ガイドライン(H15.3版) III-3-(2)に基づく確認事項	◎		3		
110	309					6) 操作手順には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	1.9	ガイドライン(H15.3版) III-3-(2)に基づく確認事項	◎		3		
111	311					8) 操作手順には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	1.9	ガイドライン(H15.3版) III-3-(2)に基づく確認事項	◎		3		
112	312					9) 情報処理・通信設備に関連するシステムの維持管理活動の手順書を作成すること	8.1.1	1.9	ガイドライン(H15.3版) III-3-(2)に基づく確認事項	◎		1	維持管理の手順が確立し定まっていること	
113	313				2) 情報処理設備及びシステムの変更について管理すること	1) 情報処理設備及びシステムの変更のすべてに対する十分な管理を確実にするために、正式な管理責任及び手順が定められていること	8.1.2	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎		1	変更管理の手順が確立していること	
114	314					2) 運用プログラムは、厳重な変更管理の下に置くこと	8.1.2	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎		1	変更管理の手順が確立していること	
115	317					5) 重要な変更を識別及び記録すること	8.1.2	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎		1	識別、記録の手順が確立していること	○
116	318					6) 重要な変更の潜在的な影響の評価をすること	8.1.2	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎		1	影響評価の手順が確立していること	○
117	319					7) 変更の申出を正式に承認する手順を確立すること	8.1.2	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎		1	承認の手順が確立していること	
118	321					9) 上手くいかない変更を中止すること及び復帰することに対する責任を明確にした手順を確立すること	8.1.2	2.6.(1)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎		1	変更中止及び復帰の手順が確立していること	
119	322				3) セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任及び手順を確立すること	1) 情報システムの故障及びサービスの停止に対処できるように、手順を定めること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎		1	故障及びサービス停止対処の手順が確立していること	
120	323					2) Dos攻撃に対処できるように、手順を定めること	8.1.3	2.6.(6) 2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑥及び⑦に基づく確認事項	◎		1	サービス妨害への対処の手順が確立していること	
121	324					3) 不完全又は不正確な業務データに起因する誤りに対処できるように、手順を定めること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎		1	誤り対処の手順が確立していること	
122	325					4) 機密性に対する違反に対処できるように、手順を定めること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎		1	違反対処の手順が確立していること	
123	326					5) 通常の障害対策計画手順には、事件・事故の原因の分析及び識別を含めること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎		2	規則等で定められていること	○
124	327					6) 通常の障害対策計画手順には、再発を防止するための対策の計画及び実施を含めること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎		2	規則等で定められていること	
125	328					7) 通常の障害対策計画手順には、監査証跡及びこれに類する証拠の収集を含めること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎		2	規則等で定められていること	
126	329					8) 通常の障害対策計画手順には、事件・事故からの回復によって影響を受ける、又は回復にかかわる人々への連絡を含めること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎		2	規則等で定められていること	
127	330					9) 通常の障害対策計画手順には、監督機関等に対する措置の報告を含めること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項 ただし、報告先については各地方公共団体の規程に従うものとする	◎		2	規則等で定められていること	

128	332					11) 潜在的な契約違反若しくは規制要求事項への違反に関連した証拠、又は、民事若しくは刑事訴訟（例えば、コンピュータの誤用又はデータ保護に関連して制定された法律に基づいたもの）での証拠として使用するために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦等のに基づく確認事項	◎	1	保管の手順が確立していること	
129	334					13) セキュリティ違反からの回復及びシステム故障の修正を行うための措置は、慎重に、かつ、正式に管理されること	8.1.3	2.6.(6)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	管理の手順が確立していること	
130	335					14) 事件・事故管理手順では、身分が明らかで、認可された要員だけに、作動中のシステム及びデータに対するアクセスを、許すことを考慮すること	8.1.3	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦等のに基づく確認事項	◎	2	手順等で考慮されていること	
131	337					16) 事件・事故管理手順では、非常措置は、最高情報統括責任者（CIO）、CISO等に報告し、手順に従ってレビューを行うことを考慮すること	8.1.3	2.5.(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	手順等で考慮されていること	
132	340					2) セキュリティ監査は、独立性を維持すること	8.1.4	2.10.(1)	ガイドライン(H15.3版) III-3-(1)-⑤等のに基づく確認事項	◎	2	規則等で定められていること	
133	348					4) 開発施設、試験施設及び運用施設を分離すること	8.1.5	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
134	349					5) 開発ソフトウェアと運用ソフトウェアとは、可能ならば、異なるコンピュータで、又は異なる領域若しくはディレクトリで実行すること	8.1.5	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
135	357				6) 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れること	1) 外部委託による施設管理においては、取扱いに慎重を要する又は重要で、地方公共団体で管理すべき適用業務の識別をすること	8.1.6	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	識別のための手順が確立していること	
136	358					2) 外部委託による施設管理においては、業務用ソフトウェアの管理者からの承認取得をすること	8.1.6	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項 通常運用ばかりでなく、障害対応手順など業務システム管理者との調整が不可欠である	◎	2	規則等で定められていること	
137	361					5) 外部委託による施設管理においては、関連するすべてのセキュリティ作業を有効に監視するための手順及び責任に関するそれぞれの割り当てを考慮すること	8.1.6	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項 通常運用ばかりでなく、障害対応手順など業務システム管理者との調整が不可欠である	◎	2	契約等で考慮されていること	
138	362					6) 外部委託による施設管理においては、セキュリティ事件・事故の報告及び処理についての責任及び手順を考慮すること	8.1.6	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項 通常運用ばかりでなく、障害対応手順など業務システム管理者との調整が不可欠である	◎	2	契約等で考慮されていること	
139	368		6.2 システムの計画作成及び受け入れ	N システム故障のリスクを最小限に抑えるため	2) 新しい情報システム、改訂版及び更新版の受け入れ基準を確立し、その受け入れ前に適切な試験を実施すること	2) 管理者は、新しいシステムを受け入れるための要求事項及び基準を文書化すること	8.2.2	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	管理者の役割として定められていること	
140	370					4) 新しい情報システム、改訂版及び更新版の受け入れ基準を確立し、その受け入れ前に適切な評価を実施すること	8.2.2	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	評価の手順が確立していること	○
141	383		6.3 悪意のあるソフトウェアからの保護	O ソフトウェア及び情報の完全性を保護するため	1) 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること	1) 悪意のあるソフトウェアからの保護は、セキュリティに対する認識、システムへの適切なアクセス、及び変更管理についての管理策に基づくこと	8.3.1	2.6.(5)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	管理手順が確立していること	○
142	384					2) ソフトウェア使用許諾契約の遵守を要求し、無認可のソフトウェアの使用を禁止する地方公共団体としての個別方針を考慮すること	8.3.1	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	管理手順が確立していること	

143	386					4) 予防又は定常の作業としてコンピュータ及び媒体を走査するための、コンピュータウイルスの検出ソフトウェア及び修復ソフトウェアの導入及び定期更新を考慮すること	8.3.1	2.6.(5)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	管理手順が確立していること	○
144	389					7) 出所の不明確な若しくは無認可の電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、ファイル使用前のコンピュータウイルス検査を考慮すること	8.3.1	2.6.(5)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	検査の手順が確立していること	
145	390					8) 電子メールの添付ファイル及びダウンロードしたファイルのすべてに対し、使用前の悪意のあるソフトウェアの検査を考慮すること	8.3.1	2.6.(5)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	検査の手順が確立していること	
146	392					10) コンピュータウイルス感染についての報告、及びコンピュータウイルス感染からの回復に関する管理の手順及び責任について考慮すること	8.3.1	2.6.(5)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	手順及び責任が確立していること	
147	393					11) コンピュータウイルス感染からの回復のための適切な侵害時の対応策を考慮すること、これには、データ及び、ソフトウェアのバックアップ並びに回復の手順を含むこと	8.3.1	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎	1	回復手順が確立していること	○
148	395					13) 悪意あるソフトウェアに関する警告情報が、正確かつ役立つことを確実にするための手順を考慮すること	8.3.1	2.7.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎	1	警戒情報取得、利用の手順が確立していること	
149	396					14) 管理者は、単なるいたずらと真のコンピュータウイルスとを識別するために、適切な情報源(例えば、定評のある刊行物、信頼できるインターネットサイト、又はコンピュータウイルス対策ソフトウェア供給業者)の利用を確実にすること	8.3.1	2.6.(5)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	警戒情報取得、利用の手順が確立していること	
150	410		6.4 システムの維持管理(Housekeeping)	P 情報処理及び通信サービスの完全性及び可用性を維持するため	3) 障害については報告を行い、是正処置をとること	1) 情報処理又は通信システムの問題に関して利用者から報告された障害は、記録すること	8.4.2	2.5.(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則等で定められていること	
151	411					2) 報告された障害の取扱いについては、明確な規定があること	8.4.2	2.5.(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則等で定められていること	
152	415		6.5 ネットワークの管理	Q ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため	1) ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること	2) ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にすること	8.5.1	2.6.(1) 2.6.(3)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	アクセス管理の手順が確立していること	○
153	416					3) ネットワークの管理者は、個人情報を含む特に重要な情報を無認可のアクセスから保護することを確実にすること		2.5(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	アクセス管理の手順が確立していること	○
154	422		6.6 媒体の取扱い及びセキュリティ	R 財産に対する損害及び業務活動に対する妨害を回避するため	1) コンピュータの取外し可能な付属媒体(例えば、テープ、ディスク、カセット)及び印刷された文書の管理手順があること	2) 不要になったことで地方公共団体の管理外となる媒体のすべてについて、認可を必要とすること	8.6.1	2.3.(2)	ガイドライン(H15.3版) III-2-(5)-③に基づく確認事項	◎	1	認可の手順が確立していること	
155	424				1) コンピュータの取外し可能な付属媒体(例えば、テープ、ディスク、カセット)及び印刷された文書の管理手順があること	4) すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること	8.6.1	2.3.(2)	ガイドライン(H15.3版) III-2-(5)-③に基づく確認事項	◎	1	保管の手順が確立していること	
156	425					5) コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書化すること	8.6.1	2.3.(2)	ガイドライン(H15.3版) III-2-(5)-③に基づく確認事項	◎	3		
157	426				2) 媒体が不要となった場合は、安全、かつ、確実に処分すること	1) 媒体の安全な処分のための、正式な手順を確立すること	8.6.1	2.3.(2)	ガイドライン(H15.3版) III-2-(5)-③に基づく確認事項	◎	1	処分の手順が確立されていること	
158	441				3) 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること	10) 個人情報など重要な情報の取扱い手順の策定においては、配布先及び認可された受領者の一覧表の定期的な間隔での見直しについて考慮すること	8.6.3	2.3.(2)	ガイドライン(H15.3版) III-2-(5)-③に基づく確認事項	◎	2	手順等で定められていること	

159	443				4) 認可されていないアクセスからシステムに関する文書を保護すること	2) システムに関する文書にアクセスできる者は、人数を最小限に抑えること	8.6.4		各地方公共団体の業務上の必要性に応じて実施すべき事項		2	手順等で定められていること	
160	445					4) システムに関する文書で、公衆ネットワークの中で保持されるもの、又は公衆ネットワーク経由で提供されるものは、適切に保護されること	8.6.4	2.6.(1) 2.6.(3)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	保護の手順が確立していること	
161	456		6.7 情報及びソフトウェアの交換	S 当該地方公共団体と他の組織との間で交換される情報の紛失、改ざん又は誤用を防止するため	2) 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護するために管理策を適用すること	1) 媒体の配送においては、すべての認可された宅配業者について管理者の合意を得ること	8.7.2		ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則等で定められていること	
162	480				4) 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること	3) 電子メールの使用に関しての個別方針には、電子メールを使うべきでないときに関する指針を含めること	8.7.4.2		各地方公共団体の関連する諸規定(文書管理規程など)に準ずる必要がある		3		
163	494				5) 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入すること	10) 電子オフィスシステムのセキュリティにおいては、緊急時に用いる代替手段についての要求事項及び取り決めについて考慮すること	8.7.5	2.6.(1)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
164	499				6) 電子的に公開した情報の完全性を保護するように注意すること	5) 公開のシステムに入力し、そこで処理する情報は、遅滞なく、完全、かつ、正確に、処理すること	8.7.6		業務上の必要性に応じて、各地方公共団体の判断で実施されるべき事項		1	処理の手順が確立していること	
165	506				7) 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な手順及び管理策を持つこと	5) 職員に、ファクシミリを用いる上での問題点を意識させること	8.7.7		業務上の必要性に応じて、各地方公共団体の判断で実施されるべき事項		2	規則等で定められていること	
166	522	7. アクセス制御	7.1 アクセス制御に関する業務上の要求事項	T 情報へのアクセス制御をするため	1) アクセス制御についての業務上の要求事項を定義し、文書化することにより、周知ならびに実効性を担保すること	16) アクセス制御の規則を定める際は、設定前に管理者又はその他の承認を必要とする規則とそのような承認を必要としない規則との区別をすること	9.1.1.2		ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	留意事項として定められていること	○
167	523		7.2 利用者のアクセス管理	U 情報システムへの認可されていないアクセスを防止するため	1) 複数の利用者を持つすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること	1) 複数の利用者を持つ情報サービスへのアクセスは、正式な利用者登録手続によって管理すること	9.2.1	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	登録の手順が確立している	○
168	524					2) 利用者登録手続において、利用者との対応付けができ、又、利用者に自分の行動に責任を負わせることができるように、一意な利用者IDを用いること	9.2.1	2.6.(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	手順等で定められていること	○
169	528					6) 利用者登録手続において、地方公共団体のセキュリティポリシーと整合しているか(例えば、職務権限の分離に矛盾する恐れはないか)を検査すること	9.2.1	2.6.(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	検査の手順が確立していること	○
170	532					10) 利用者登録手続において、アクセスの条件を理解していることを示している宣言書への署名を利用者に要求すること	9.2.1		登録手続に際してどの程度まで実施するかは各地方公共団体の諸規定との関連性を考慮する必要がある		2	規則等で定められていること	
171	534					12) 利用者登録手続において、サービスを使用するために登録されているすべての人の正規の記録を維持管理すること	9.2.1				1	管理の手順が確立していること	
172	536					14) 利用者登録手続において、もはや必要のない利用者ID及びアカウントがないか定期的に検査し、あれば削除すること	9.2.1	2.6.(3)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	検査の手順が確立していること	○
173	538				2) 特権の割り当て及び使用は、制限し、管理すること	2) 各システム製品に関連した特権と、特権が割り当てられる必要がある業務区分に関連した特権とを識別すること	9.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	特権割り当ての手順が確立していること	○
174	539					3) 個人に対する特権は、使用の必要性に基づき、又、事象毎に、すなわち、必要とされる場合に限って、その機能上の役割の最小限の要求事項に従って、割り当てること	9.2.2	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	特権割り当ての手順が確立していること	○
175	541					5) 特権の割り当てにおいて、利用者に対する特権の許可が必要ないように、システムルーチンの開発及び使用を促進すること	9.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	2	規則等で定められていること	○

176	542					6) 特権の割り当てにおいて、特権は、通常の業務用途に使用される利用者IDとは別の利用者IDに、割り当てること	9.2.2	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	特権割り当ての手順が確立していること	○
177	544				3) パスワードの割り当ては、正規の管理手続によって統制すること	2) パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に求めること	9.2.3		各地方公共団体の諸規定との関連性に応じて適用の判断をする必要がある事項		1	パスワード管理手順が確立していること	
178	549					7) パスワード管理手続の取組において、利用者は、パスワードの受領を知らせること	9.2.3		外部委託の際には、厳格な適用が必要である		1	パスワード管理手順が確立していること	
179	554				4) データ及び情報サービスへのアクセスに対する有効な管理を維持するため、最高情報統括責任者（CIO）、CISO等は、利用者のアクセス権を見直す正規の手順を、定期的に実施すること	3) 利用者アクセス権の見直しにおいて、特権の割り当てを定期的に検査して、認可されていない特権が取得されてないことを確実にすること	9.2.4		外部委託の際には、厳格な適用が必要である		1	見直し手順が確立していること	○
180	555		7.3 利用者の責任	V 認可されていない利用者のアクセスを防止するため	1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと	1) すべての利用者に、パスワードを秘密にしておくように助言すること	9.3.1	2.5.(4)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	利用者に周知する手順が確立していること	○
181	556					2) すべての利用者に、パスワードをメモに記録して保管しないように助言すること	9.3.1	2.5.(4)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	利用者に周知する手順が確立していること	
182	557					3) すべての利用者に、システム又はパスワードに対する危険の兆候が見られる場合は、パスワードを変更するように助言すること	9.3.1	2.5.(4)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	利用者に周知する手順が確立していること	○
183	558					4) すべての利用者に、最短6文字の質の良いパスワード（例えば、他人が容易に推測できない又は、同一の文字・数字だけの文字列でない）を選択すること	9.3.1	2.5.(4)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項	◎	1	利用者に周知する手順が確立していること	○
184	561					7) すべての利用者に、古いパスワードを再使用したり、循環させて使用したりしないように助言すること	9.3.1	2.4(1) 2.5(4)	ガイドライン(H15.3版) III-2-(5)-⑥及び⑦に基づく確認事項	◎	1	利用者に周知する手順が確立していること	○
185	563					9) すべての利用者に、自動ログオン処理にパスワードを含めないように助言すること	9.3.1	2.5.(4)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎	1	利用者に周知する手順が確立していること	○
186	570				2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	5) 無人運転の装置の利用者に、PC又は端末装置は、使用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって認可されていない使用からセキュリティを保つように保護するように助言すること	9.3.2		各地方公共団体の運用手順などに応じて適用の判断をする必要がある事項		2	規則等で定められていること	
187	575		7.4 ネットワークのアクセス制御	W ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は地方公共団体全体への影響が大きく、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	5) ネットワークサービスの使用についての個別方針は、業務上のアクセス制御方針と整合していること	9.4.1	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	整合させるための手順が確立していること	○
188	577				2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止すること	2) 指定された接続経路には、専用線又は専用電話番号を割り当てること	9.4.2	2.4(3)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
189	580					5) 指定された接続経路では、ネットワーク上で無制限に探索（roaming）することを防止すること	9.4.2	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
190	581					6) 指定された接続経路では、外部のネットワーク利用者には、指定された業務システム及び/又はセキュリティゲートウェイを使用させること	9.4.2	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
191	583					8) 地方公共団体内の利用者グループのために別々の論理領域[例えば、仮想私設網（Virtual Private Network：VPN）]を設定することによって、ネットワークアクセスを制限すること	9.4.2	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○

192	585				3) 遠隔地からの利用者のアクセスには、認証を行うこと	1) コールバックの手順及び制御を用いるとき、地方公共団体は、転送機能を持つネットワークサービスを用いないこと	9.4.3		業務上の必要性など各地方公共団体で事情に即して適用の判断をする必要がある事項		2	規則等で定められていること	
193	588				4) 遠隔コンピュータシステムへの接続は、認証されること	1) 遠隔コンピュータシステムへの接続は、認証されること	9.4.4	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	認証の手順が確立していること	○
194	593				6) 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御策の導入を考慮すること	3) 適切なネットワークの経路指定又はセキュリティゲートウェイ技術を組み込むことの、費用対効果を考慮すること	9.4.6		ガイドライン(H15.3版) III-2-(4)-⑤に基づく確認事項	◎	2	留意事項として定められていること	
195	604		7.5 オペレーティングシステムのアクセス制御	X 認可されていないコンピュータアクセスを防止するため	2) 情報サービスへのアクセスは、安全なログオン手続を経て達成されること	1) コンピュータシステムへログインするための手順は、認可されていないアクセスの恐れを最小限に抑えるように設計すること	9.5.2	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
196	609					6) ログオン情報が正しいかどうかの検証は、すべての入力データが完了した時点で行い、誤り条件が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを指摘しないこと	9.5.2		ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	
197	616					13) ログオンの失敗時には、失敗した試みを記録していること	9.5.2		ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	○
198	620				3) すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用毎に一意に識別できるもの(利用者IDなど)を保有すること	2) 明らかに業務上の利点がある例外的状況において、利用者のグループ又は特定の業務に対して、共有利用者IDを用いる場合、管理者の承認を文書で得ること	9.5.3		ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	
199	623				4) 質の良いパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること	3) パスワードの管理システムでは、質の良いパスワードを選択させるようにすること	9.5.4	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
200	625					5) パスワードの管理システムでは、利用者がパスワードを選択する場合、仮のパスワードは最初のログオン時に変更させるようにすること	9.5.4	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
201	626					6) パスワードの管理システムでは、以前の利用者パスワードの記録を、一定期間、維持し再使用を防止すること	9.5.4		ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	○
202	629					9) パスワードの管理システムでは、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードを保存すること	9.5.4	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
203	631				5) システムユーティリティの使用は制限され、厳しく管理されること、システムユーティリティのために認証手順を使用すること	1) 業務用ソフトウェアからのシステムユーティリティの分離を考慮すること	9.5.5		ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	
204	643				8) リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供すること	2) 残業時間又は延長時間の運転の要求がない場合、接続時間を通常の就業時間に制限すること	9.5.8		ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	
205	645		7.6 業務用ソフトウェアのアクセス制御	Y 情報システムが保持する情報への認可されていないアクセスを防止するため	1) 業務用ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限されること	2) 情報へのアクセス制限では、業務用システムへのアクセスを制御するための情報の表示を考慮すること	9.6.1	2.3(2)	ガイドライン(H15.3版) III-2-(5)-③に基づく確認事項	◎	2	手順等で考慮されていること	○
206	646					3) 情報へのアクセス制限では、利用者向けの文書を適切に編集して、アクセスを認可されていない情報又は業務用システム機能に関する利用者の知識を限定すること	9.6.1	2.5.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項 特に外部へ開発・運用を委託する場合は、必ず指導・確認しなければならない	◎	2	手順等で定められていること	○
207	647					4) 情報へのアクセス制限では、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御することを考慮すること	9.6.1	2.6.(1)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	手順等で考慮されていること	○

208	649					6) 情報へのアクセス制限では、その出力に対して余分な情報を取り除くことを確実にするために、このような出力の定期的な見直しも行うことを考慮すること	9.6.1	2.5.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項 特に外部へ開発・運用を委託する場合は、必ず指導・確認しなければならない	◎	1	見直しの手順が確立していること	○
209	652	7.7 システムアクセス及びシステム使用状況	Z 認可されていない活動を検出するため	1) 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること		1) 監査記録には、利用者IDを含めること	9.7.1	2.6.(1)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
210	653					2) 監査記録には、ログオン及びログオフの日時を含めること	9.7.1	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
211	654					3) 監査記録には、可能ならば、端末のID又は所在地を含めること	9.7.1	2.6.(3)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
212	655					4) 監査記録には、システムへのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
213	656					5) 監査記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	2.6.(5)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	○
214	666			2) 明確に認可された活動だけを利用者が実行することを確実にするために、情報処理設備の使用状況を監視する手順を確立すること		10) 監視項目には、認可されていないアクセスの試みを含むこと、その中には、失敗したアクセスの試みを含めること	9.7.2.1	2.7.(1)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎	2	規則等で定められていること	
215	667					11) 監視項目には、認可されていないアクセスの試みを含むこと、その中には、ネットワークのゲートウェイ及びファイアウォールについてのアクセス方針違反及び通知を含めること	9.7.2.1	2.7.(1)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎	2	規則等で定められていること	
216	668					12) 監視項目には、認可されていないアクセスの試みを含むこと、その中には、侵入検知システムからの警告を含めること	9.7.2.1	2.7.(1)	ガイドライン(H15.3版) III-2-(5)-⑦に基づく確認事項	◎	2	規則等で定められていること	
217	669					13) 監視項目には、システム警告又は故障を含むこと、その中には、コンソール警告又はメッセージを含めること	9.7.2.1	2.6.(1)	ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	
218	671					15) 監視項目には、システム警告又は故障を含むこと、その中には、ネットワーク管理警報を含めること	9.7.2.1	2.6.(1)	ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	
219	683			5) 監査記録の正確を保障するためにコンピュータの時計は正しく設定すること		2) コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること	9.7.3	2.7.(1)	ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	2	規則等で定められていること	○
220	685	7.8 移動型計算処理及び遠隔作業	AA 移動型計算処理(mobile computing)及び遠隔作業(teleworking)の設備を用いるときの情報セキュリティを確実にするため	1) ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、正式な個別方針を採用すること		2) 個別方針にはモバイルコンピュータの利用に関する運用について、物理的保護、アクセス制御、暗号技術、バックアップ及びコンピュータウイルス対策についての要求事項などを含めること	9.8.1		業務上の必要性など各地方公共団体の事情に即して適用の判断をする必要がある事項 ただし、モバイルを利用する場合には実施しなければならない		3		
221	686					3) 個別方針には、移動型設備をネットワークに接続する場合の規則並びに助言、及び公共の場所で移動型設備を使用する場合の手引も含めること	9.8.1		業務上の必要性など各地方公共団体の事情に即して適用の判断をする必要がある事項 ただし、モバイルを利用する場合には実施しなければならない		3		
222	690					7) モバイルコンピュータの利用に関する利用者教育を実施すること	9.8.1		業務上の必要性など各地方公共団体の事情に即して適用の判断をする必要がある事項 ただし、モバイルを利用する場合には実施しなければならない		2	規則等で定められていること	
223	695					12) 移動型計算処理の設備を用いて、公衆ネットワークを経由して行われる業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されること	9.8.1		業務上の必要性など各地方公共団体の事情に即して適用の判断をする必要がある事項 ただし、モバイルを利用する場合には実施しなければならない		2	規則等で定められていること	

224	697					14) 大切な取扱いに慎重を要する及び／又は影響の大きい業務情報が入っている装置は、無人の状態で放置しておかないこと（可能ならば、物理的に施錠するか、又は装置のセキュリティを確保するために特別な錠を用いること）	9.8.1		業務上の必要性など各地方公共団体の事情に即して適用の判断をする必要がある事項 ただし、モバイルを利用する場合には実施しなければならない 又、個人情報など機密性の高い情報を含む機器をモバイルを利用してはならない		2	規則等で定められていること	
225	727	8. システムの開発及び保守	8.1 システムのセキュリティ要求事項	AB 情報システムへのセキュリティの組み込みを確実にするため	1) 新しいシステム又は既存のシステムの改善に関する業務上の要求事項を記した文書には、管理策についての要求事項を明確にすること	5) 情報システム担当者は、JIS X5070(ISO 15408)などITセキュリティ評価・認証制度において認証されたセキュリティレベルの高い製品の利用を考えること	10.1.1	2.6.(4)	ガイドライン(H15.3版) III-2-(6)-⑥に基づく確認事項 各省庁の調達におけるセキュリティ水準の高い製品等の利用方針(平成13 年3 月29日、行政情報化推進各省庁連絡会議了承)の方向に沿うものである	◎	2	規則等で定められていること	○
226	730		8.2 業務用システムのセキュリティ	AC 業務用システムにおける利用者データの消失、変更又は誤用を防止するため	1) 業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を検査すること	1) 業務処理(transaction)、常備データ（名前、住所、参照番号）及び各種パラメタの入力を検査すること	10.2.1		業務上の必要性に応じて各地方公共団体での事情に即して適用の判断をする必要がある ただし、実施できることが望ましい		2	規則等で定められていること	
227	739					10) 入力データのもっともらしさを試験する手順について考慮すること	10.2.1		完全性の確保のために必要な事項		2	規則等で定められていること	
228	753				3) 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮すること	1) メッセージ認証の必要性を決定し、最も適切な実施方法を明らかにするために、セキュリティリスクの評価を行うこと	10.2.3	2.5.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項 特に外部へ開発・運用を委託する場合は、必ず指導・確認しなければならない	◎	1	メッセージ確認及びリスクアセスメントの手順が確立していること	○
229	754				4) 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をすること	1) 出力データの妥当性確認には、出力データが適当であるかどうかを試験するためのもっともらしさの検査を含むこと	10.2.4	2.6.(2)	ガイドライン(H15.3版) III-2-(5)-③に基づく確認事項	◎	1	確認の手順が確立していること	○
230	759		8.3 暗号による管理策	AD 情報の機密性、真正性又は完全性を保護するため	1) 個人情報など重要な情報資産を保護するため、暗号化を用いる際の個別管理方針を定めること	1) 個人情報など重要な情報資産に対するリスクの評価及び管理策の一環として、暗号化による解決策が適切であるかを判断すること	10.3.1	2.3.(2)	ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	1	暗号化の手順及びリスクアセスメントの手順が確立していること	○
231	761					3) 暗号化を用いる際の個別管理方針を定める場合、かぎを紛失した場合、かぎのセキュリティが脅かされた場合、又はかぎが損傷した場合の暗号化情報を回復させる方法など、かぎ管理対策を取り決めること	10.3.1	2.3.(2)	ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	3		
232	762					4) 暗号化を用いる際の個別方針を定める場合、個別管理方針の実施に当たって役割及び責任について定めること	10.3.1	2.6.(1)	ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	3		
233	763					5) 暗号化を用いる際の個別管理方針を定める場合、かぎ管理の実施に当たって役割及び責任について定めること	10.3.1	2.6.(1)	ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	3		
234	764					6) 暗号化を用いる際の個別管理方針を定める場合、暗号化による適切な保護レベルをどのように決定するかを定めること	10.3.1	2.3.(2)	ガイドライン(H15.3版) III-2-(5)に基づく確認事項	◎	3		
235	774				3) 電子文書の真正性及び完全性を保護するために、電子署名を用いること	4) 電子署名に使用される暗号かぎは、アルゴリズムの種類、及び品質、並びに使用されるかぎの長さを考慮し、暗号化に使用されるものとは異なること	10.3.3	2.6.(1)	電子署名を利用する際の管理に必要となる事項 注)重要な情報資産の暗号化に使用される暗号かぎは、その用途のためにのみ利用する必要がある	◎	1	かぎ管理の手順が確立していること	
236	775					5) 電子署名を用いるときは、電子署名がどのような条件の基で法的拘束力を持つかの条件を規定した関連法令を考慮すること	10.3.3	2.6.(1)	電子署名を利用する際の管理に必要となる事項	◎	2	規則等で定められていること	
237	804		8.4 システムファイルのセキュリティ	AE IT プロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため	1) システムの完全性を確保するため、システムファイルへのアクセスは制御されなければならないそのため運用システムでのソフトウェアの実行を管理すること	7) ソフトウェアの新版への更新の決定には、その版のセキュリティ、すなわち、新しいセキュリティ機能の導入又はこの版に影響を及ぼすセキュリティ問題の数及び危険度を考慮すること	10.4.1		可用性の確保を考慮するうえで必要な事項		1	リスクアセスメントの手順が確立していること	

238	808				2) システム試験データを保護し、管理すること	1) システム及び受け入れの試験は、通常、できるだけ運用データに近い、十分な量の試験データで行うこと	10.4.2	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項 システム試験は可能な限り実運用状況を再演することが望ましいため、必要な量のデータを用いる	◎	1	試験の手順が確立していること	
239	815				3) プログラムソースライブラリへのアクセスに対しては、厳しい管理を維持すること	1) 可能な限り、プログラムソースライブラリは、運用システムに含めないこと	10.4.3	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に関する要求事	◎	2	規則等で定められていること	
240	820					6) プログラムリストは、セキュリティの保たれた環境に保持されること	10.4.3		ガイドライン(H15.3版) III-2-(5)-④に基づく確認事項	◎	1	保管の手順が確立していること	
241	835		8.5 開発及び支援過程におけるセキュリティ	AF 業務用システム及び情報のセキュリティを維持するため	1) 情報システムの変更の実施を厳しく管理し、正式な変更管理手順を確実に実行すること	11) 業務用ソフトウェア及び運用の変更過程では、業務の中断を最小限に抑えるように変更が実行されることを確実にすること	10.5.1	2.6.(4)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
242	865				5) 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために、管理策を用いること	5) ソフトウェア開発を外部委託する場合、コードの品質についての契約要求事項について考慮すること	10.5.5	2.5.(1)	ガイドライン(H15.3版) III-2-(5)-⑤に基づく確認事項 外部委託に対する管理指針の一つ	◎	2	規則等 (契約締結基準等) で定められていること	
243	869	9. 緊急時対応計画	9.1 緊急時対応計画の種々の面	AG 業務活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため	1) 地方公共団体全体を通じて業務継続のための活動を展開し、かつ、維持するための管理された手続が整っていること	3) 合意された業務目的及び優先順位に沿って業務継続戦略を明確にし、文書化すること	11.1.1	1.9	ガイドライン(H15.3版) III-2-(4)に基づく確認事項 特に、開発・運用を外部委託する場合には、事業者に対して確実に要求し、実施の確認がとれるようにしなければならない	◎	3		
244	872					6) 業務継続管理が地方公共団体の手続及び機構に確実に組み込まれるようにすること	11.1.1	1.9	ガイドライン(H15.3版) III-2-(4)に基づく確認事項 特に、開発・運用を外部委託する場合には、事業者に対して確実に要求し、実施の確認がとれるようにしなければならない	◎	1	組み込むための手順が確立していること	
245	875				2) 緊急時対応のための活動は、業務手続の中断を引き起こし得る事象を特定することから始めること	2) 起こり得る障害を特定する活動及びリスクアセスメントを行う活動の実施には、業務資源及び手続の管理者が全面的に関与すること	11.1.2	1.9	ガイドライン(H15.3版) III-2-(4)に基づく確認事項 特に、開発・運用を外部委託する場合には、事業者に対して確実に要求し、実施の確認がとれるようにしなければならない	◎	2	規則等で定められていること	
246	896				5) すべての計画が整合したものになることを確実にするため、又、試験及び保守の優先順位を明確にするために、一つの緊急時対応計画の枠組みみを維持すること	12) 緊急時対応計画作成の枠組みみでは、必要に応じて、計画の構成要素を実行する代わりの責任者を任命すること	11.1.4		ガイドライン(H15.3版) III-2-(5)に基づく確認事項 責任の在り方については各地方公共団体の事情に即して判断する必要がある	◎	1	枠組みみ維持の手順が確立していること	
247	915	10. 適合性	10.1 法的要求事項への適合	AH 刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を明確に定め、文書化し、さらに要求事項に適合する特定の管理策、及び個々の責任も同様に明確に定め、文書化すること	12.1.1				3		
248	917				2) 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は、法的制限事項に適合するように、適切な手続を実行すること	2) ソフトウェア製品の取得手続に関する標準類を発行すること	12.1.2.2				2	規則等で定められていること	
249	935				3) 地方公共団体の重要な記録は、消失、破壊及び改ざんから保護されること	9) 保持期間が終了した後、地方公共団体にとって必要ないならば、そのシステムは、記録を適切に破棄できること	12.1.3		法的要求事項への対応という観点であるため、文書管理及び情報公開など関連する諸規定との整合性を考慮する必要があり、各地方公共団体の判断で実施することが望ましい		1	破棄の手順が確立していること	
250	938					12) 主要な情報の出典一覧を維持管理すること	12.1.3		法的要求事項への対応という観点であるため、文書管理及び情報公開など関連する諸規定との整合性を考慮する必要があり、各地方公共団体の判断で実施することが望ましい		2	規則等で定められていること	
251	939					13) 重要な記録及び情報を消失、破壊及び改ざんから保護するための適切な管理策を実行すること	12.1.3	2.6.(1)	ガイドライン(H15.3版) III-2-(5)-⑥に基づく確認事項	◎	1	保護の手順が確立していること	

252	940				4) 関連する法令に従って個人情報を保護するために、適切な管理策を用いて統制を行なうこと	1) データ保護の担当責任者を任命し、その責任者は、管理者、利用者及びサービス提供者に対して、従うべき手続きについて指導すること	12.1.4	2.3	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	データ保護の責任体制が確立していること	
253	941				4) 関連する法令に従って個人情報を保護するために、適切な管理策を用いて統制を行なうこと	2) 個人情報を構造化されたファイルに保管しようという提案のいかなるものについてもデータ保護の担当責任者に報告することは、データ保有者の責任であること	12.1.4	2.3	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	データ保護の責任体制が確立していること	
254	942					3) 関連法規法令に定められるデータ保護の原則に対する意識を確実にすることは、データ保有者の責任であること	12.1.4	2.3	ガイドライン(H15.3版)III-2-(5)-③に基づく確認事項	◎	1	データ保護の責任体制が確立していること	
255	943				5) 情報処理施設の使用には管理者の認可を要するものとし、そのような施設の不適切な使用を防ぐための管理策を用いること	1) 業務以外の目的又は認可されていない目的のために、管理者の承認にこれらの施設を使用することは、施設の不適切な使用と見なされること	12.1.5	2.6(2)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	
256	953				7) 職員又は地方公共団体に対する措置を支援するには、十分な証拠を持つこと	3) 紙文書の場合、どのような調査をおこなっても、原本に手が加えられないことが、証明できること	12.1.7.3		法的要求事項への対応という観点であるため、文書管理及び情報公開など関連する諸規定との整合性を考慮する必要があり、各地方公共団体の判断で実施することが望ましい		1	証拠保存の手順が確立していること	
257	972		10.3 システム監査の考慮事項	AJ システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため	1) 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重に計画を立て、合意されること	8) すべてのアクセスは、照合用の証跡を残すために、監視され、記録されること	12.3.1	2.10.(1)	ガイドライン(H15.3版)III-3-(1)に基づく確認事項	◎	2	規則等で定められていること	○
258	975				2) システム監査ツールは、ソフトウェア又はデータファイルへのアクセスの誤用又は悪用を防止するために保護されること	2) システム監査ツールは、テープライブラリ、又は利用者の領域で保持しないこと	12.3.2	2.6(2)	ガイドライン(H15.3版)III-2-(5)-⑥に基づく確認事項	◎	2	規則等で定められていること	

参考資料４：情報セキュリティポリシーにおける対策基準（例）

本資料は、対策基準の策定例として提示するものです。そのため、以下の対策基準（例）は、それぞれの企業にそのまま当てはまるものではありません。実際に対策基準を策定する際には、企業の規模・業態・特性などを十分に考慮し、企業に適合したものとする必要があります。

また、それぞれの対策基準（例）には、ガイドラインに記載していない内容も含まれていることをご了承ください。

テレワーク環境で想定される対策基準の策定例を示します。

① ウイルス対策基準
② ハードウェア／ソフトウェア対策基準
③ リモートアクセス対策基準
④ クライアント端末対策基準

①ウイルス対策基準

「ウイルス対策基準」（例）

１．趣旨

本基準は、ウイルス・ワームによって引き起こされるシステムの破壊や情報漏えいの被害を未然に防ぐことを目的とする。

２．対象者

・テレワーク勤務者
・情報システム管理者

３．対象システム

パソコン及びメールゲートウェイサーバ

４．遵守事項

４．１　ウイルス対策ソフトの導入

(1) テレワーク用のパソコンにはクライアント用のウイルス対策ソフトを導入する。
(2) テレワーク勤務者用メールサーバにはメールゲートウェイとしてウイルス対策ソフトを導入する。
(3) ウイルス対策ソフトは以下の機能を有すること。
① 定義ファイルの自動更新
② メールの常時スキャン

４．２　ウイルス対策ソフトの利用

(1) テレワーク勤務者は、パソコンに導入されたウイルス対策ソフトを起動状態とし、メール及びファイルのアクセス時には常時スキャンできるように設定しなければならない。
(2) テレワーク勤務者は、常時スキャンだけではなく○週間に一度、パソコン全体のファイルのスキャンを実施することとする。

(3) テレワーク勤務者は、定義ファイルを毎日一度は更新するように設定しなければならない。
(4) テレワーク勤務者は、ウイルス対策ソフトの契約満了までに更新しなければならない。

４．３　パソコンのＯＳ及びアプリケーションの利用
(1) パソコンのＯＳは、最新の状態に維持しなければならない。
(2) 業務で利用する○○アプリケーションは最新の状態に維持しなければならない。

４．４　パソコンにおける電子メールを介してのウイルス被害の防止
(1) ファイルを添付してメールを送る場合は、該当ファイルがウイルスに感染していないことを確認しなければならない。
(2) 電子メール利用中に、ウイルスの発見や、ウイルスに感染したと思われる症状を発見した場合は、「インシデント対応手順（※１）」に基づき対応しなければならない。
(3) 送信元が不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審なファイルに対しては、これに操作を加えてはならない。

※１　インシデント対応手順：事件や事故が発生した場合の対応手順

４．５　ウイルス・ワームに関する啓発教育の実施
テレワーク勤務者は、パソコンの利用開始時にウイルス・ワーム対策手順についての研修を受けなければならない。

４．６　システム管理者におけるウイルス対策窓口の設置
(1) システム管理者は、ウイルス被害の状況を迅速に収集するために、ウイルス対策窓口を設置し、周知徹底しなければならない。
(2) ウイルス対策窓口は、ウイルス被害状況を掌握し問題発生の初期対応を実施する。

４．７　ウイルス対策ソフトがウイルスを検知または感染した場合
(1) テレワーク勤務者は、ウイルス対策ソフトの機能を利用し、速やかにウイルスを駆除しなければならない。
(2) 駆除した結果または感染した事実を「インシデント対応手順」に基づきウイルス対策窓口へ報告しなければなない。

４．８　ウイルスに感染した場合
(1) テレワーク勤務者は、以下の症状が発生した場合は、ウイルス対策窓口に連絡し、対応方法を教えてもらわなければならない。
- パソコンの動きが急に遅くなった
- ファイルを立ち上げたら何か警告が表示された　等々

(2) ウイルス対策窓口は、テレワーク勤務者にネットワークからパソコンを切断することを指示し、パソコンの調査を開始しなければならない。
(3) ウイルスが他者へ感染している可能性がある場合は、「インシデント対応手順」に従い、速やかに対応しなければならない。
(4) テレワーク勤務者は、ネットワークから切り離されたパソコンについて、ウイルス対策ソフトの機能を利用し、ウイルスを駆除しなければならない。

６．例外処置

業務都合により本基準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７．罰則

本基準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。

②ハードウェア／ソフトウェア対策基準

「ハードウェア・ソフトウェアの購入及び導入基準」（例）

１．趣旨

本基準は、テレワーク業務で使用するハードウェア・ソフトウェアの標準製品を定めて運用管理することにより、組織的に統一された情報セキュリティ対策の実現を容易にし、管理の効率化を図り、導入時の設定ミス等を防止することを目的とする。

２．対象者

・テレワーク勤務者
・情報システム管理者
・情報セキュリティ委員会のメンバー

３．対象システム

本基準は、テレワーク業務で使用するために購入及び導入する、ハードウェアとソフトフェアを対象とし、その他の業務に利用されるものは対象外とする。

４．遵守事項

４．１　標準製品リストの作成

(1) 情報セキュリティ委員会は、テレワーク業務で使用する以下の標準製品を定め、標準製品リストを作成し、すべてのテレワーク勤務者に通知しなければならない。

● ハードウェア

① パソコン
・ デスクトップパソコン、ノートパソコン、サーバ機器等

② ネットワーク機器
・ ルータ、スイッチングハブ、ＶＰＮ装置等

● ソフトウェア

① リモートアクセス関連ツール
・ ＶＰＮ通信用ソフト

② 業務で必ず利用するソフトウェア
・ 標準 OS
・ 表計算、文書作成、プレゼンテーションソフト

③ ウイルス対策ソフト
・ クライアントウイルス対策ソフト
・ メールウイルス対策ソフト

④ 電子メールソフト
・ 標準電子メールソフト

⑤ Web ブラウザ
・ 標準ブラウザ

⑥ 不正侵入対策
・ パーソナルファイアウォール

⑦ バックアップソフト
・ ファイルのバックアップ
・ パソコンのデータすべてのバックアップ
⑧ 暗号化ソフト
・ ファイルやフォルダの暗号化ソフト
・ 通信経路の暗号化ソフト
⑨ 業務アプリケーション
・ グループウェア
・ 圧縮・解凍ソフト

(2) テレワーク勤務者は、情報セキュリティ委員会から標準以外の製品の購入及び導入を承認された場合を除き、標準製品リストで定められた製品を購入及び導入しなければならない。

(3) 情報システム管理者及び情報セキュリティ委員会は、標準製品を決定するにあたり、必要なセキュリティ機能、スペックを備え、サポート、ライセンス条件、価格、などの条件が適切であることを評価しなければならない。さらに、既存の情報システムに悪影響を及ぼさないものを選択しなければならない。製品のセキュリティホールやその他の不具合に関する情報の提供、パッチ発行等の対応が悪い製品は、標準製品に指定してはならない。

(4) 情報システム管理者は、セキュリティ上の問題やその他のトラブルを防止するために、標準製品における適切な設定を検証して決定し、設定ミスを防止するために、設定マニュアルを作成しなければならない。また、パソコンの貸出し時には、適切な情報セキュリティ研修または操作説明を行うこと。

(5) 情報セキュリティ委員会は、標準製品リストを定期的（年○回）に審議し、変更が生じた場合には、速やかにすべてのテレワーク勤務者に通知しなければならない。

４．２　標準製品の購入及び導入

(1) 情報システム管理者は、標準製品の発注、保守契約、ライセンス、インストールメディア等を一括して管理する。

(2) 情報システム管理者は、購入処理を行った製品を資産管理台帳に登録しなければならない。

(3) 標準製品の購入を行うテレワーク勤務者は、申請書を情報システム管理者に提出しなければならない。

(4) 情報システム管理者は、申請を受けた標準製品の発注処理を行い、業務で利用するソフトウェアのインストールと設定、ネットワーク接続の設定、各種ソフトウェアの最新パッチを適用したうえでテレワーク勤務者に送付する。製品購入時にインストールされているものや、OS に付属するソフトウェアであっても、標準製品として認められないものは、排除すること。

(5) 情報システム管理者は、各部署からの申請により、再インストール等のためにライセンス上問題のないインストールメディアの貸出しをする。情報システム管理者は貸出し記録を作成し、管理しなければならない。

４．３　私用パソコンを利用する場合の購入及び導入

(1) テレワーク業務を行う勤務者で、個人で保有するパソコンを利用する場合は、指定された標準製品を使用しなければならない。

(2) 私用パソコンを利用するテレワーク勤務者が標準外製品を購入及び導入する必要がある場合は、情報セキュリティ委員会に標準外製品を使用する理由、製品名、製品の種類等の必要事項を明記し、申請を行わなければならない。

(3) 標準外製品の申請を受けた情報セキュリティ委員会は、申請の妥当性を討議し、その結果を申請者に通知する。

(4) 情報セキュリティ委員会の承認を得て導入された標準外製品の私用パソコンを利用するテレワーク勤務者は、標準外製品の使用を停止した場合、情報セキュリティ委員会に使用停止の申請をしなければならない。

(5) 情報セキュリティ委員会は、使用を許可した標準外製品を情報システム管理者に通知し、情報システム管理者は、標準外製品を管理台帳に登録しなければならない。

４．４　標準外製品の購入及び導入

(1) テレワーク業務上の理由で、標準外製品を購入及び導入する必要がある勤務者は、情報セキュリティ委員会に標準外製品を使用する理由、製品名、製品の種類、管理者等の必要事項を明記し申請を行わなければならない。

(2) 標準外製品の申請を受けた情報セキュリティ委員会は、申請の妥当性を討議し、その結果を申請者に通知する。

(3) 情報セキュリティ委員会の承認を得て標準外製品の使用を行う従業員は、標準外製品の使用を停止した場合、情報セキュリティ委員会に使用停止の申請をしなければならない。

(4) 情報セキュリティ委員会は、使用を許可した標準外製品を情報システム管理者に通知し、情報システム管理者は、標準外製品を管理台帳に登録しなければならない。

(5) 情報セキュリティ委員会は、標準外のネットワークソフトウェアに対して使用許可の判断を行う場合、必要に応じて情報セキュリティ関連の専門家に妥当性の審査を依頼しなければならない。

(6) テレワーク勤務者が標準外製品の購入及び導入を行う場合は、事前に既存の情報システムへの影響を検討し、セキュリティ上の安全性を確認し、情報システム管理者のチェックを受けてから使用しなければならない。

(7) テレワーク勤務者が標準外製品の購入及び導入を行う場合は、自己の責任において購入及び導入の手続きを行い、ライセンス、インストールメディアの管理を厳密に行わなければならない。

(8) 情報セキュリティ委員会は、既存の情報システムにセキュリティ上のトラブルが発生した場合、標準外製品の購入及び導入を行うテレワーク勤務者に対し、当該製品の設定変更や社内ネットワークからの切り離し、当該製品の使用停止等を命じることがある。

４．５　リモートアクセス用ネットワーク機器の購入及び導入について

(1) テレワーク勤務者がオンラインで業務するためのリモートアクセス用ネットワークを構成する機器（ルータ、ＶＰＮ装置等）については、情報システム管理者が、購入及び導入を行うものとし、テレワーク勤務者が許可なく購入及び導入を行ってはならない。

(2) 情報システム管理者は、「リモートアクセス対策基準」に基づき、主要なネットワーク機器の導入を行わなければならない。

(3) テレワーク環境のために購入した製品は、管理台帳に登録するため、情報システム管理者に申請しなければならない。購入した製品は、情報システム管理者のもとで管理するものとする。

４．６　管理台帳の作成管理

(1) 情報システム管理者は、申請された情報をもとにパソコンやネットワーク機器の管理台帳を作成し、新規登録、変更、削除を管理しなければならない。

(2) 管理台帳には、標準製品、標準外製品の両方を登録しなければならない。

５．例外処置

業務都合等により本基準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６．罰則

本基準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。

③リモートアクセス対策基準

「リモートアクセスサービス利用基準」（例）

１．趣旨

本基準は、テレワーク勤務者がインターネットやダイヤルアップ等により社内ネットワークを利用する、リモートアクセスサービスの利用にあたり、情報資産を外部から守ることを目的とする。

２．対象者

・ テレワーク勤務者
・ 情報システム管理者

３．対象機器・対象システム

下記を本基準の遵守義務対象機器・対象システムとする。

・ テレワークにおけるリモートアクセスで利用する機器
（パソコン、PDA、携帯電話など）
・ テレワークにおけるリモートアクセスシステム
・ ＶＰＮ装置
・ テレワークにおけるリモートアクセスサーバ
・ インターネット接続システム

４．遵守事項

４．１　使用機器に関する遵守事項

(1) テレワーク勤務者は、インターネット接続やダイヤルアップ等による社内ネットワークへのアクセスにおいて、情報システム管理者が指定した機器を利用しなければならない。

(2) テレワーク勤務者は、インターネット接続やダイヤルアップ用のルータ・モデムなどによる社内ネットワークへの接続手段を、情報システム管理者の許可を得て設置しなければならない。

(3) テレワーク勤務者が使用するパソコンは、社内環境への接続において「テレワーク端末におけるセキュリティ対策基準」に基づいて設定されなければならない。

４．２　機器の管理に関する遵守事項

(1) テレワークにおけるリモートアクセスで使用するパソコン及び携帯電話は情報セキュリティ委員会が定めるテレワーク勤務者のみ利用することができる。

(2) テレワークにおけるリモートアクセスで使用するパソコン及び携帯電話の管理は、所有するテレワーク勤務者が行わなければならない。

(3) テレワークにおけるリモートアクセスの管理は、情報システム管理者が行わなければならない。

４．３　利用環境に関する遵守事項

(1) テレワークにおけるリモートアクセスで利用できる機器は、情報セキュリティ委員会の定める機器でなければならない。

・ノート型パソコン
・PDA
・携帯電話

(2) テレワークにおけるリモートアクセスの利用場所は、情報セキュリティ委員会の定める場所でなければならない。
・外出先（国内、海外）
・営業所・関連会社等、関連施設
・ユーザ先
・自宅

(3) テレワークにおけるリモートアクセスによる接続は、情報セキュリティ委員会の定める通信形態でなければならない。
・インターネットＶＰＮ経由（パソコン、携帯電話）
・公衆回線（電話回線、INS 回線、携帯電話）

(4) テレワークにおけるリモートアクセスで利用できるサービスは、情報セキュリティ委員会の定めるものでなければならない。
・http/https を利用したサービス
・電子メールサービス
・ファイル転送サービス
・ファイル共有サービス
・業務システムとして導入しているサービス

４．４　アカウント管理に関する遵守事項

(1) テレワーク勤務者は、「ハードウェア・ソフトウェアの購入及び導入基準」に準拠したパソコンを利用しなければならない。

(2) テレワークにおけるリモートアクセスで利用するパソコン及び携帯電話は、テレワーク勤務者が情報システム管理者に申請し、テレワーク勤務者情報（識別番号、パスワード等）を入手しなければならない。
・テレワーク勤務者名
・利用場所
・利用目的
・利用期間
・接続機器（機器種別、OS 種類）
・接続形態

(3) 情報システム管理者は、テレワーク勤務者情報（テレワーク勤務者、識別番号、パスワード等）の登録・変更・削除を適宜行い、それを管理しなければならない。

４．５　アクセス制御に関する遵守事項

(1) テレワークにおけるリモートアクセスでは、社内にアクセスできるサーバ及びサービスは必要最低限にしなければならない。

(2) テレワークにおけるリモートアクセスでは、テレワーク勤務者ごとにアクセスできるサーバ及びサービスを決めることとする。

(3) テレワークにおけるリモートアクセスでは、社内に設置されたサーバのみにアクセスすることができる。ただし、申請により許可された社員についてはインターネットへアクセスすることもできる。

４．６　テレワークにおけるリモートアクセスサーバに関する遵守事項

(1) テレワークにおけるリモートアクセスサーバは、テレワーク勤務者情報を管理することができなければならない。

(2) テレワークにおけるリモートアクセスサーバは、テレワーク勤務者認証（発信者識別、ワンタイムパスワード）に対応していなければならない。

(3) テレワークにおけるリモートアクセスサーバは、通信手段としてコールバックまたはＶＰＮに対応していなければならない。

(4) テレワークにおけるリモートアクセスサーバは、接続記録を蓄積でき各種データを保管できなければならない。

- 接続成功
- 接続失敗
- 接続の開始時間と終了時間
- 接続時のアカウント名
- 発信者識別
- 障害情報（エラー情報）

４．７　テレワーク端末に関する遵守事項

(1) テレワーク端末は、利用するテレワーク勤務者を識別（テレワーク勤務者識別名・パスワード）し、該当者以外は利用できないようにしなければならない。

(2) テレワーク端末は、「テレワーク端末等におけるセキュリティ対策基準」を満たし、かつ「ウイルス対策基準」を満たしていなければならない。

(3) テレワーク端末は、リモートアクセスに対応していなければならず、それを利用しなければならない。

(4) テレワーク端末は、通信手段として発信者識別・ＶＰＮに対応していなければならず、それを利用しなければならない。

(5) テレワーク端末は、情報セキュリティ委員会が定めたソフトウェアがイントールされ、正常に動作する状態でなければならない。

４．８　利用手順に関する遵守事項

(1) テレワーク勤務者は、テレワークにおけるリモートアクセスを行う場合、テレワーク端末とテレワーク勤務者を識別する情報を入力し、テレワークにおけるリモートアクセスサーバで認証されなければならない。

(2) 認証方法はワンクイムパスワード等を利用し、個人を確定する認証方式を用いなければならない。

(3) テレワーク勤務者は、インターネットを利用してテレワークにおけるリモートアクセスを利用する場合、ＶＰＮによる通信を行わなければならない。

(4) テレワーク勤務者は、ダイヤルアップによるリモートアクセスを利用する場合、コールバック機能を使用し認証しなければならない。

(5) テレワーク勤務者は、テレワークにおけるリモートアクセス利用のための教育を受け一定のレベルになっていることが望ましい。

４．９　検査と監視に関する遵守事項

(1) 情報システム管理者は、定期的（年○回）に外部で使用するパソコン及び携帯電話が適切に利用されているか検査しなければならない。

(2) テレワークにおけるリモートアクセスサーバは、接続記録を蓄積・管理し、定期的（毎月）に解析しなければならない。

(3) 情報システム管理者は、定期的（年○回）にダイヤルアップツール及びサーバ、モデムなどによる社内ネットワークへの接続環境が不正に用意されていないか検査しなければならない。

４．１０　緊急対応に関する遵守事項

(1) 情報システム管理者は、テレワークにおけるリモートアクセスサーバに対し、外部から侵害・侵入された場合、テレワークにおけるリモートアクセスを停止し、原因調査及び対策を実施しなければならない。

(2) テレワーク勤務者は、テレワークにおけるリモートアクセスで使用するパソコン及び携帯電話で使用するパスワードを忘れた場合に、システム管理者に連絡し、速やかに新たなパスワードへ変更しなければならない。

(3) テレワーク勤務者は、テレワークにおけるリモートアクセスで使用するパソコン及び携帯電話を紛失した場合は、速やかに情報システム管理者に報告し具体的な指示を受け、対処しなければならない。

(4) テレワーク勤務者は、テレワークにおけるリモートアクセスで使用するパソコンに障害が発生した場合、速やかに情報システム管理者に報告し、システムの再構築をしなければならない。

４．１１　物理セキュリティ遵守事項

(1) テレワークにおけるリモートアクセスで使用するパソコン及び携帯電話は、所有者の周囲に置き管理できるようにし、使用しないときには、定められた場所で保管しなければならない。

(2) テレワークにおけるリモートアクセスサーバは、情報システム管理者以外が触れないように安全で予防対策がなされた場所に設置されなければならない。

５．例外処置

業務都合等により本基準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６．罰則

本基準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。

④クライアント端末対策基準

「テレワーク端末におけるセキュリティ対策基準」（例）

１．趣旨

本基準は、テレワーク端末（パソコン）上の機密性・完全性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

２．対象者

・ テレワーク勤務者

・ 情報システム管理者

３．対象システム

・ 貸与されたパソコン

・ 私用パソコン

４．遵守事項

４．１　パソコンの使用制限

(1) テレワーク勤務者が業務において使用できるパソコンは、システム管理者が支給・貸与したパソコンを利用することとする。

(2) 私用パソコンを利用する場合は、標準セキュリティ対策を実施し、システム管理者のチェック及び情報システム管理責任者の承認を得た場合のみ可能とする。

４．２　パソコンに導入するソフトウェア

(1) システム管理者がテレワーク勤務者に支給･貸与するパソコンは、「ハードウェア／ソフトウェアの購入及び導入基準」で規定されたソフトウェアを導入することとする。従って、それ以外のソフトウェアを導入してはならない。

(2) (1)にて指定したソフトウェア以外で、業務上やむを得ず導入しなければならないソフトウェアは、情報システム管理者に申請し、許可を得なければならない。

(3) テレワーク勤務者は、導入したソフトウェアを常に最新の状態で使用することとし、情報システム管理者が提供するソフトウェア情報をもとに修正プログラム等を導入しなければならない。

４．３　パソコンの他者への利用の制限

(1) テレワーク勤務者は、パソコンに対するパスワード管理を徹底しなければならない。

(2) テレワーク勤務者は、席を離れる場合、第三者が無断でパソコンを利用できないようにパソコンにロックを掛けなければならない。

(3) テレワーク勤務者は、持ち運ぶことができるノートパソコンでは、基本認証以外にも BIOS 上での認証を行うようにしなければならない。

(4) テレワーク勤務者は、業務用に支給されたソフトウェア以外はダウンロード及びインストールしてはならない。

(5) テレワーク勤務者は、不審なサイトへアクセスしてはならない。

４．４　パソコンでの情報の取り扱い

(1) テレワーク勤務者は、「機密」と区分された情報を利用する場合には、機密情報を取り扱う許可を情報システム管理者に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏えいに備え、暗号化等の対策を実施しなければならない。

(2) テレワーク勤務者は、パソコンで一時的に機密情報を取り扱う場合、取り扱い後には、不必要となった情報を削除し、いつまでも保持してはならない。

４．５　パソコンでの技術的対策

(1) ウイルス対策

テレワーク勤務者は、「ウイルス対策基準」に規定されている遵守事項を徹底しなければならない。

(2) 電子データのバックアップ

テレワーク勤務者は、常時電子データのバックアップを実施しなければならない。

(3) ファイアウォール機能の設定

テレワーク勤務者は、ＯＳのファイアウォール機能を利用するか、パーソナルファイアウォールソフトを導入しなければならない。

(4) 通信経路の暗号化

テレワーク勤務者は、インターネットを利用したテレワークを実施する場合は、パソコンにＶＰＮ通信用の設定を行い、安全な通信経路を確保しなければならない。

(5) パソコンへのアクセス制御

テレワーク勤務者は、ＯＳへのログインパスワードを設定し、定期的に更新しなければならない。

４．６　パソコンの移設

(1) パソコンの設置場所（住所等）を勝手に移設してはならない。

(2) テレワーク勤務者は、パソコンの設置場所の住所等の変更が必要な場合には、情報システム管理者に申請し、許可を得なければならない。

４．７　ノートパソコンの利用上の注意事項

(1) テレワーク勤務者は、社外にノートパソコンを持ち出す場合、盗難・窃盗に注意し取り扱わなければならない。

(2) テレワーク勤務者は、社外でノートパソコンを利用する場合、情報の盗み見に注意し利用しなければならない。

５．例外処置

業務都合等により本基準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

６．罰則

本基準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。

参考資料５：ウイルスの代表的な感染経路

ウイルスの代表的な感染経路には、以下のものがあります。

●電子メールの添付ファイル

ウイルスの感染経路として一般的なのは、電子メールの添付ファイルです。電子メールの添付ファイルとして送信されたウイルスを誤って実行してしまうと、そのウイルスに感染してしまいます。

●電子メールの HTML スクリプト

添付ファイルが付いていない電子メールであっても、HTML メールであればウイルスを送信することができます。HTML メールはホームページと同様に、メッセージの中にスクリプトと呼ばれるプログラムを挿入することが可能なため、スクリプトの形でウイルスを侵入させておくことができるのです。電子メールソフトによっては、HTML メールのスクリプトを自動的に実行する設定になっているものがあり、その場合には電子メールをプレビューしただけでウイルスに感染してしまいます。

●ホームページの閲覧

現在の Web ブラウザは、ホームページ上で様々な処理を実現できるように、JavaScript や VBScript、ActiveX コントロール、Java などのプログラムを実行できるようになっています。そのため、これらのプログラムにウイルスが埋め込まれたホームページを閲覧した場合は、コンピュータがウイルスに感染してしまいます。

●ネットワークのファイル共有

ウイルスによっては、感染したコンピュータに接続されているファイル共有用のネットワークドライブを探し出して、特定の拡張子を持つなど、ある条件で探し出したファイルに感染していくタイプのものがあります。このようなウイルスは社内のネットワークを通じて、他のコンピュータやサーバにも侵入する可能性があります。とても危険度が高く、完全に駆除することが難しいのが特徴です。

●マクロプログラムの実行

マイクロソフト社の Office アプリケーション（Word、Excel、PowerPoint、Access）のマクロ機能を利用して感染するタイプのウイルスがあります。これらは、マクロウイルスと呼ばれています。Office アプリケーションのマクロ機能では、高度なプログラム開発言語である VBA（Visual Basic for Applications）を使用することができるため、ファイルの書き換えや削除など、コンピュータを自在に操ることが可能になります。そのため、マクロウイルスに感染したドキュメントは、ファイルを開いただけで VBA で記述されたウイルスが実行されて、自己増殖などの活動が開始されます。

参考資料６：ウイルスの活動内容

ウイルスの代表的な活動内容には、以下のものがあります。

●自己増殖

ウイルスのほとんどは、インターネットや LAN を使用して、他の多くのコンピュータに感染することを目的としています。特にワーム型と呼ばれるウイルスは、自分自身の複製を電子メールの添付ファイルにして送信したり、ネットワークドライブに保存されているファイルに感染したりするなど、ユーザの操作を介さずに自動的に増殖していきます。

●コンピュータシステムの破壊

ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものまで様々です。

●メッセージや画像の表示

いたずらを目的としたウイルスは、一定期間潜伏して、ある日時に特定のメッセージや画像を表示することがあります。

●トロイの木馬型

感染したコンピュータの内部に潜伏するタイプのウイルスをトロイの木馬と呼びます。この中でもバックドアを作成するタイプのウイルスは極めて悪質なもので、インターネットを通じて、感染したコンピュータを外部から自由に操作されてしまうこともあります。

参考資料７：代表的なウイルス

これまでに、世界中で数多くのウイルスが作り出され、ネットワークなどを通じて広められてきました。ここでは、それらの中から代表的なウイルスを紹介します。なお、ウイルスによっては、同じウイルスを改変して作られた亜種と呼ばれる別のバージョンが発生することもあります。同じウイルスでも、亜種によって動作が異なる場合もありますが、ここでは代表的な亜種の動作を取り上げています。

●Nimda（ニムダ）

電子メールの送信、ネットワークドライブへのファイルコピー、Web サーバ経由の感染など、様々なルートによる感染方法を持ち、世界中で猛威を振るったウイルスです。多数の感染経路を持つ強力なワームとして、その後の多くのウイルスがこの Nimda の影響を受けています。

コンピュータの設定を変更して、ファイルの拡張子を見えなくしたり、隠しファイル属性のファイルを表示しないようにしたりすることで、感染状態を気付かせないようにするという動作も行います。

●Klez（クレズ）

Nimda に類似した活動を行うワーム型のウイルスです。大きな特徴としては、ウイルス付きメールを送信する際に発信元の偽装が行われたことが挙げられます。発信元の偽装は、過去に受信された電子メールの中から任意に選ばれた送信元のメールアドレスを使用することで行われます。そのため、電子メールの送信者のコンピュータが必ずしも感染しているとは限らず、電子メールの送信元をウイルスの感染元として特定するという方法では感染元が判明しません。

●Bugbear（バグベア）

トロイの木馬型のウイルスで、ハッキングツールをコンピュータに埋め込むことで、外部からのリモートコントロールを可能にするという機能を持っています。内部に埋め込まれるハッキングツールは、特定のポートをオープンして、外部からファイルの実行やプロセスの終了を可能にするものです。さらに、収集したパスワードをコンピュータ名、ユーザ名とともに特定のメールアドレスに電子メールとして送信するという機能も持っています。

また、ウイルス対策ソフトやファイアウォールソフトなど、一部のセキュリティ対策ソフトの正常な動作を妨害するという機能も装備されていました。

●Badtrans（バッドトランス）

トロイの木馬型のウイルスで、電子メールを介して増殖します。Badtrans に含まれているハッキングツールのプログラムである“kdll.dll”はメモリに常駐して、感染したコンピュータのすべてのキー入力をユーザ名や入力時刻などとともに記録して、電子メールで任意のメールアドレスに送信します。

●CodeRed（コードレッド）

セキュリティホールが残されている Web サーバに感染するウイルスです。このウイルスはサーバのメモリ上で動作するという特徴があり、ハードディスクにはウイルスが保存されません。CodeRed に感染した Web サーバは、情報を要求してきたコンピュータに対して、本来の Web ページではなく、以下のようなメッセージを表示する HTML ファイルだけを送信するようになります。

```
Welcome to http://www.worm.com!
Hacked  By Chinese!
```

ただし、ウイルスに感染してから 10 時間が経過すると、ウイルス自身が自動的にサーバを元の状態に戻し、再び本来の Web ページを表示します。

●Sircam（サーカム）

Nimda と同様の動作を行うワーム型のウイルスです。電子メールの宛先として、コンピュータ内のアドレス帳や HTML ファイルからメールアドレスを探し出すという特徴があります。コンピュータに保存されている HTML ファイルからメールアドレスを探し出すようになったため、それまでのウイルスとは異なり、インターネット上のホームページに記載されている連絡先のメールアドレスに対してもウイルスが送信されることがあります。

●LOVELETTER（ラブレター）

VBScript で記述されたワームです。Outlook またはチャットで利用する IRC クライアントプログラムを介して感染します。感染したコンピュータに対しては、特定の拡張子を持つファイルを探し出して、自分自身のコピーでファイルを書き換えるという行為も行います。

●Happytime（ハッピータイム）

トロイの木馬型のワームで、HTML 形式の電子メールを介して感染します。セキュリティ対策の施されていない電子メールソフトを使用している場合には、このウイルスが埋め込まれた HTML 形式の電子メールをプレビューするだけで、ウイルスに感染してしまいます。また、1 月 12 日や 3 月 10 日など、システム日付の月と日の数字の合計が 13 の日付になると、コンピュータのすべてのドライブに保存されている拡張子 DLL と拡張子 EXE のファイルを削除します。

●MTX（マトリックス）

ハッキングツールを持つワームです。このウイルスに感染すると、ハッキングツールをコンピュータ内部に生成することから、ウイルスドロッパとも呼ばれています。常駐するハッキングツールは、あるホームページからプログラムをダウンロードしようとするものでした（実際には成功しなかったようです）。

●Melissa（メリッサ）

マイクロソフト社のワープロソフトである Word で動作するマクロウイルスです。Word 文書に“ Melissa ”という名前のマクロモジュールを作成して感染します。このウイルスは Word の標準テンプレートファイルに感染するため、Word を起動するたびにウイルスが活動します。Melissa は、ウイルス付きの電子メールを自動的に送信するという機能を初めて装備したウイルスでもあります。

●Laroux（ラルー）

マイクロソフト社の表計算ソフトである Excel で動作するマクロウイルスです。このウイルスに感染したファイルを開くとウイルスに感染し、その後、そのコンピュータで開いたすべての Excel ファイルに、ウイルスをコピーします。

●MSBlaster（エムエスブラスター）

トロイの木馬型ワームです。Windows のセキュリティホールを利用して、コンピュータ内に“ MSBLAST.EXE ”というファイルを埋め込むことで増殖します。感染したコンピュータは、システムを起動するたびに、このファイルを実行するようになり、常に他のコンピュータへの感染を試みるようになります。

また、決められた日時（2003 年 8 月 16 日午前 0 時）に、マイクロソフト社の windowsupdate.com に対して一斉に DoS 攻撃（サービス拒否攻撃）を実行するという機能も持っていました。なお、このウイルスには以下のメッセージが埋め込まれていたため、別名ラブサンとも呼ばれています。

I just want to say LOVE YOU SAN!! billy gates why do you make this possible ?
Stop making money and fix your software!!

●SQLSlammer（スラマー）

マイクロソフト社のサーバ用データベースソフト SQL Server 2000 に感染するタイプのウイルスです。このウイルスはメモリ上に常駐するだけで、ファイルとしては保存されません。感染活動以外には特別な破壊活動は行いませんが、常に感染活動を繰り返すため、ネットワーク上のトラフィックの急激な増大をもたらし、全世界のインターネットに大きな影響を与えました。

●Lovgate（ラブゲート）

トロイの木馬型ウイルスで、電子メールやネットワークの共有フォルダを経由して感染します。このウイルスの特徴としては、共有フォルダに対するパスワードを推測する機能が装備されていたことが挙げられます。なお、共有フォルダにパスワードが設定されていた場合にも、ウイルス自身が「1234」、「password」、「admin」、「server」、「login」、「abc」といった多数のパスワードを使用して接続を試みる仕組みが搭載されていました。

●Mydoom（マイドゥーム）

電子メールの添付ファイルを通じて感染するワーム型のウイルスです。特徴的な動作としては、特定のサイトに対する DoS 攻撃（サービス拒否攻撃）やハッキングツールとしてのバックドアの作成なども行うことが挙げられます。

ハッキングツールは、外部の不正ユーザがファイルの実行やプロセスの終了などのリモートコントロールを行ったり、そのコンピュータに保存されている情報をダウンロードしたりすることを可能にするものです。

●Netsky（ネットスカイ）

トロイの木馬型のワームで、非常に多くの亜種が作られたことから、世界中で猛威を振るいました。電子メールまたはネットワークの P2P ファイル共有ソフトを経由して感染を広げますが、亜種の中には、Nimda のようにネットワークドライブへのファイルコピーによって増殖するものもあります。

電子メールの添付ファイルが実行されたときには、ワームのプログラム自身を services.exe という名前でシステムのフォルダにコピーして、コンピュータ内の設定ファイルを変更します。このとき、偽のエラーメッセージを表示して、ユーザにウイルスに感染したことに気付かせないようにする機能も持っています。

●Bagle（バグル）

システムに常駐するトロイの木馬型ワームで、電子メールの添付ファイルを介して感染します。電子メールの添付ファイルが実行されたときには、ワームのプログラム自身を bbeagle.exe という名前でシステムのフォルダにコピーして、コンピュータ内の設定ファイルを変更します。このとき、Windows に装備されている電卓のアプリケーションを起動して、ユーザに感染したことを気付かせないようにしています。

ハッキングツールが作成されると、外部のユーザが感染したコンピュータのコマンドを実行することができるようになってしまいます。

●Sobig（ソービッグ）

電子メールの添付ファイルを通じて感染するトロイの木馬型のワームです。2003 年 5 月に発見された亜種では、電子メールの送信者アドレスを「support@microsoft.com」とすることによって、マイクロソフト社からの電子メールであるかのように偽っていました。

●Mimail（ミメイル）

電子メールの添付ファイルによって感染するトロイの木馬型のワームです。このウイルスは、Outlook Express や Outlook を適切な対策を施さずに使用している場合に、受信した電子メールをプレビューしただけでウイルスの活動が開始されます。

このウイルスの大きな特徴の一つは、コンピュータから収集したメールアドレスへ電子メールを送信する際に、送信者名を「admin@(受信者のメールアドレスのドメイン名)」と詐称することです。また、本文に、受信者のメールアドレスが有効期限切れになるといった内容を記載することによって、受信者が添付ファイルを実行してしまうように仕組まれています。

●Swen（スウェン）

トロイの木馬型のワームで、多くの感染経路を持つ非常に感染力の強いウイルスです。Outlook Express や Outlook を適切な対策を施さずに使用している場合に、受信した電子メールをプレビューしただけでウイルスの活動が開始します。

感染経路の一つは電子メールですが、このウイルスはメールアドレスをコンピュータから収集するだけでなく、インターネット上のニュースグループを検索して収集します。また、電子メールの件名や本文、送信者のメールアドレスは複数確認されていますが、マイクロソフト社からの電子メールを装ったり、メールサーバからの送信エラーを装ったりするものもあります。

電子メール以外には、ネットワーク上の共有フォルダ、インターネット上の IRC（インターネット・リレー・チャット）、ファイル共有ソフト（KaZaA）を利用して感染活動を行います。

感染活動以外にも、ウイルス対策ソフトやファイアウォールソフトの動作を終了したり、レジストリエディタを使用できなくしたり、外部のハッカーサイトに接続して感染したコンピュータ台数の統計を更新したりする機能も持ちます。

●Antinny（アンティニー）

日本製のファイル共有ソフト「Winny」を利用して感染するウイルスです。このウイルスに感染すると、特定のフォルダに自身のコピーを格納して、Winny のアップロード用フォルダに設定することで感染を拡大していきます。また、デスクトップのイメージを jpeg ファイルでキャプチャして、Winny の共有フォルダに保存するという機能も持っていたため、画面上に表示されていた内容によっては、機密情報の漏えいにつながる場合もあります。

●Sasser（サッサー）

このウイルスに感染したコンピュータは、特定のポートを開けたうえで、ネットワークに対して、OS の脆弱性を利用した攻撃を行います。その脆弱性に対するセキュリティパッチが適用されていないコンピュータは、感染元のコンピュータからウイルス本体をダウンロードして感染してしまいます。

このウイルスは、攻撃先のコンピュータを探すために、ランダムな IP アドレスに対するスキャンを連続的に行うため、コンピュータ及びネットワーク全体の速度が低下するという影響も受けます。

参考資料８：情報セキュリティチェックリスト

定期的に簡易監査を行うための情報セキュリティチェックリストとして、情報セキュリティ管理者とテレワーク勤務者向けの情報セキュリティチェックシートの例を下記に示します。

情報セキュリティチェックリストは、情報システム構成、テレワーク実施形態や業務内容等（取り扱う情報の範囲）によりチェック項目が異なりますので、実情に合わせて作成してください。

【情報セキュリティ管理者用】 テレワークに関する情報セキュリティチェックリスト	
内容	確認
【情報セキュリティポリシー】	
情報セキュリティポリシーは、テレワークによる勤務体制における危険性を考慮したものになっていますか？	□
【情報セキュリティ管理体制】	
テレワーク勤務者に対して、情報セキュリティ事故発生時の連絡方法が明確に定められていますか？	□
テレワーク勤務者に対して、情報セキュリティ対策事項が遵守されているか、定期的にヒアリングや監査を実施していますか？	□
【アカウントとパスワード管理】	
アカウントの発行方法や運用管理ルールを設けていますか？	□
【テレワーク端末管理】	
パソコンの貸出し･返却管理を実施していますか？	□
パソコンの返却時にデータ削除およびウイルスチェックを実施していますか？	□
パソコンの貸出し時にパッチやウイルス定義ファイルが適切であるか確認していますか？	□
【通信経路の管理】	
各種回線接続サービスの申込み方法についてルール化していますか？ また同様に変更･廃止に対してルール化していますか？	□
【情報セキュリティ教育･啓発】	
情報セキュリティの意識向上のための教育や啓発活動を実施していますか？	□
【規則と契約】	
外部委託の際に機密保持契約を締結していますか？	□
就業規則に情報セキュリティに関する規定を定めていますか？	□
【ウイルス対策】	
サーバにウイルス対策ソフトは導入していますか？	□
ウイルス対策ソフトの導入をルール化していますか？	□
ウイルス対策ソフトの定義ファイルの更新を正しくルール化していますか？	□

【ファイアウォール】	
社内のネットワークにファイアウォールが適切に導入されていますか？	□
【無線LAN】	
無線LANの利用におけるルールを明確にしていますか？	□
【不正アクセス/侵入対策】	
ルータのログはチェックして、定期的に保存していますか？	□
Webサーバーのログはチェックして、定期的に保存していますか？	□
【OSやソフトウェアの脆弱性対策】	
使用しているOSやソフトウェアについては、新しいパッチが配布されているかどうかをチェックしていますか？	□
使用しているOSやソフトウェアについての新しいパッチを随時適用していますか？	□
社内のコンピュータに対するパッチの適用ルールを明確にしていますか？	□
【パスワードの管理】	
各ユーザに対して、パスワードのルールを明確に決定していますか？	□
各ユーザに対して、パスワードの管理方法（ディスプレイにメモを貼り付けないなど）を明確に決定していますか？	□
【端末の盗難】	
持ち運びを行う可能性のある端末のディスクやUSBメモリなどに対して、暗号化のルールを決定していますか？	□
重要なドキュメントファイルやフォルダに対する暗号化やパスワードの設定をルール化していますか？	□

【テレワーク勤務者用】 テレワークに関する情報セキュリティチェックリスト	
内容	確認
【情報セキュリティ管理体制】	
情報セキュリティ事故（パソコン紛失、盗難、ウイルス・ワーム感染）が発生した場合の連絡先を知っていますか？	□
【アカウントとパスワード管理】	
アカウントの申請・変更・削除の依頼方法を知っていますか？	□
【情報セキュリティ教育・啓発】	
情報セキュリティの意識向上のための教育を受けましたか？	□
情報セキュリティ十ヶ条を知っていますか？携帯して常に確認できるようにしていますか？	□
情報セキュリティに関する冊子を読みましたか？	□
【規則と契約】	
情報の持ち出しがどのように制限されているか知っていますか？	□
就業規則にセキュリティに関する規定があることを知っていますか？ 違反した場合どのような罰則があるか知っていますか？	□
【ウイルス対策】	
ウイルス対策ソフトを導入していますか？	□
ウイルス対策ソフトの定義ファイルは正しく更新されていますか？	□
【ファイアウォール】	
使用する端末にパーソナルファイアウォールが導入されているか、自宅のネットワークにファイアウォールが導入されていますか？	□
【無線LAN】	
無線LANのアクセスポイントには、WEPによる暗号化を設定し、暗号鍵を定期的に変更していますか？	□
無線LANのアクセスポイントには、他人から推測されにくいSSIDを設定していますか？	□
無線LANのアクセスポイントには、MACアドレスのフィルタリングを設定していますか？	□
【OSやソフトウェアの脆弱性対策】	
使用しているOSやソフトウェアについては、新しいパッチが配布されているかどうかをチェックしていますか？	□
使用しているOSやソフトウェアについての新しいパッチを随時適用していますか？	□
【パスワードの管理】	
OSへのログインやサービスを利用するためのパスワードは、適切な長さを持ち、他人からは推測されないものになっていますか？	□
パスワードを記載したメモなどをディスプレイに貼り付けたり、机の引き出しにしまったりしていませんか？	□

【端末の盗難】	
ハードディスクやBIOSにパスワードを設定してありますか？	□
持ち運ぶ端末に不要なファイルを格納していませんか？	□
重要なファイルを格納したUSBメモリなどのメディアには、暗号化やパスワードを設定していますか？	□
重要なドキュメントファイルには、暗号化やパスワードを設定していますか？	□

用語集

英数字

■ BIOS

Basic Input/Output System の略。
コンピュータに接続されたディスクドライブ、キーボード、ビデオカードなどの周辺機器を制御するプログラム。

■ CD-R

データを一度だけ書き込むことができる CD-ROM。媒体によって、650M バイトや 700M バイトといった大量のデータを保存できます。
CD-R はデータの読み取り方式が CD-ROM と同じであるため、ほとんどの場合、CD-R に記録されたデータは普通の CD-ROM ドライブで読み込むことができます。

■ CD-RW

書き換えを可能にした CD メディア。媒体によって、650MB や 700MB といったデータを書き込むことができます。
CD-R は一度書き込んだデータを消去することはできませんが、CD-RW では何度でもデータを消去して、新たに別のデータを書き込むことができます。また、最近の CD-ROM ドライブや DVD-ROM ドライブは、ほとんどの場合、CD-RW に書き込まれたデータを読み取ることが可能です。そのため、日常的なドキュメントなどのバックアップに適したメディアであると言えます。

■ DDS

Digital Data Storage（デジタル・データ・ストレージ）の略。データ用のテープメディア。
元々は音楽用のメディアとして開発された DAT をコンピュータ用のバックアップメディアに利用できるようにしたものです。
DDS では、規格によって、2GB、4GB、12GB、24GB、36GB などの容量のメディアが存在します。また、圧縮機能を使用することで、それぞれのメディアで倍の容量を格納することもできます。コストパフォーマンスも良く、現在のもっとも一般的なバックアップメディアの一つと言えます。

■ DLT

Digital Linear Tape（デジタル・リニア・テープ）の略。
主にサーバのバックアップに使用されるテープメディア。DDS に比べて、ドライブもメディアも高価ですが、その代わりに高い信頼性と転送速度を持ちます。規格によって、20GB（圧縮時最大 40GB）、35GB（圧縮時最大 70GB）などの容量のメディアが存在します。

■ DoS 攻撃

Denial of Service attack（デナイアル・オブ・サービス・アタック）攻撃。サービス拒否攻撃のこと。

DoS とは、インターネットを利用した代表的な攻撃方法の一つです。Web サーバやメールサーバなどに対して、過大な負荷をかけるために、大量のサービス要求のパケットを送りつけることで、相手のサーバやネットワークを使用不能にします。

■ DVD-RAM

書き換え可能な DVD の規格のうちの一つ。

DVD フォーラムによって策定された統一規格です。記憶容量は片面 2.6GB、両面 5.2GB のものと、片面 4.7GB、両面 9.4GB のものがあります。DVD-RAM は、現在の DVD メディアの中で、唯一殻付き（ケースに入っているもの）のメディアが存在します。殻付きのメディアを利用する場合は、ドライブが対応していなければなりませんが、直接メディアの記憶面に触れてしまうことがないため、汚れに強く、取り扱いが容易であるというメリットがあります。

DVD-RW や DVD+RW に比べて、DVD-ROM との互換性が低いという欠点がありますが、最近の DVD-ROM ドライブでは DVD-RAM のメディアを読み出すことができるものが増えてきました。

■ e ラーニング

パソコンや通信ネットワークを利用して教育を行うこと。自己啓発学習や遠隔教育などに多く利用されています。

■ ICT

Information Communication Technology の略。

既存の概念であった IT（情報技術）という無機的要素に、コミュニケーションという有機的要素を付加した言葉。

■ IEEE802.1X

LAN におけるユーザ認証の方式の規格。

IEEE802.1x は、無線 LAN だけでなく、有線も含んだユーザ認証の方式です。クライアントが接続を要求した場合には、認証サーバである Radius（ラディウス）サーバが認証処理を行います。クライアントが認証された場合には、セッションごとに暗号化鍵が与えられます。なお、IEEE802.1x では通常暗号化を行わないため、無線 LAN を利用する場合には WEP による暗号化を利用します。

■ IPsec

IP security の略。

IPsec とは、IP パケットの暗号化と認証を行なう技術です。暗号化モードには、「トンネルモード」と「トランスポートモード」があり、「トンネルモード」は、IP パケット全体を暗号化するのに対して、「トランスポートモード」はデータ部分だけを暗号化します。

■ ISDN

ISDN（Integrated Services Digital Network）は、電話、ファクシミリ、データ通信を統合化したデジタル通信網のことです。電話線を使った ISDN では、通信速度 64kbps の通信用チャネル 2 本と、通信速度 16kbps の制御用チャネル 1 本が利用可能です。そのため、2 本の通信チャネルを使用できるので、電話をかけながらインターネットに接続することができます。

■ LTO

Linear Tape-Open（リニア・テープ・オープン）の略。
主にサーバのバックアップに使用されるテープメディア。多くの LTO 機器は、転送速度 40MB/s～80MB/s、テープ長 580m で容量 400GB(データ圧縮時)をサポートしています。将来的には、より高転送速度・容量増とすることが計画されています。

■ MO ディスク

MO（Magneto-Optical）ディスクは、レーザーと磁気を併用した記録メディアのことを指す。読み書きが可能な大容量のメディアで、レーザーと磁気を利用してディスク上のデータの読み書きを行います。

■ OS

Operating System(オペレーティング・システム）の略。
コンピュータを動作させるための基本的な機能を提供するシステム全般のこと。例えば、メモリやディスクなどのハードウェアの制御、キーボードやマウスといったユーザインタフェースの処理、画面への表示とウィンドウの制御など、コンピュータが動作するための数多くの基本処理を行っています。さらに、コンピュータシステムを管理するための数多くのツールが用意されています。

■ PPTP

Point to Point Tunneling Protocol の略。
コンピュータ間で認証、リンクの確立を実施し、データを暗号化して送受信する機能を持ちます。

■ RAID

複数のハードディスクをまとめて 1 台のハードディスクとして管理する技術。
データを分散して記録するため、高速化や安全性の向上が図られます。また、高速性や安全性のレベルにより、RAID-0 から RAID-5 まで 6 つのレベルがあります。

■ RAS

Remote Access Service の略。
電話回線や ISDN 回線などを通じて遠隔地のコンピュータやネットワーク機器にダイヤルアップ接続し、遠隔地のシステムを利用することです。

■ SSID

Service Set Identifier（サービス・セット・アイデンティファイァ）の略。
無線 LAN で特定のコンピュータや通信機器で構成されるネットワークを指定して、接続するためのユニークな識別コードのことです。ESS ID（イー・エス・エス・アイ・ディ）とも呼ばれています。
無線 LAN で送信するパケットのヘッダに含まれ、受信側は、SSID が一致しない場合は、そのパケットを無視するため通信ができません。

■ SSL

Secure Socket Layer（セキュア・ソケット・レイヤ）の略。
インターネットにおいてデータを暗号化したり、なりすましを防いだりするためのプロトコルのこと。ショッピングサイトなどで、個人情報や機密情報をやりとりする際に広く使われています。

■ TKIP

Temporal Key Integrity Protocol（テンポラル・キー・インテグリティ・プロトコル）の略。
WPA-PSK や WPA-EAP の暗号化方式で使用されているプロトコルのこと。

■ USB メモリ

USB とは、Universal Serial Bus（ユニバーサル・シリアル・バス）の略で、コンピュータに様々な周辺機器を接続することができる外部ポートを指します。
USB メモリは、USB を経由してパソコンの HDD と同様にドライブとして認識され、データの書き込みや読み込みが可能となります。

■ VPN

Virtual Private Network の略。
インターネット等の公衆回線網で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。専用回線を導入するよりコストを抑えることが可能です。また、インターネット上で認証技術や暗号化を用いて保護された仮想的な専用回線を提供する場合もあります。

■ WEP

Wired Equivalent Privacy（ワイアード・エクイヴァレント・プライバシー）の略。
無線 LAN の規格である IEEE802.11 で採用されている暗号化方式。
無線 LAN は無線区間内での傍受が簡単であるため、この WEP を使用した暗号化によって送信されるデータの解読を困難にします。
製品によって、64 ビットと 128 ビットの異なる長さの暗号化鍵が利用されています。

■ WPA-PSK 方式

業界団体である Wi-Fi Alliance（ワイファイ・アライアンス）が制定したセキュリティ規格の一つ。WPA は Wi-Fi Protected Access（ワイファイ・プロテクテッド・アクセス）の略で、EAP は Extensible Authentication Protocol（エクステンシブル・オーセンティケーション・プロトコル）の略。
企業向けの暗号化方式で、外部の認証サーバを利用して暗号化を行います。

■ WPA-EAP 方式

業界団体である Wi-Fi Alliance（ワイファイ・アライアンス）が制定したセキュリティ規格の一つ。WPA は Wi-Fi Protected Access（ワイファイ・プロテクテッド・アクセス）の略で、PSK は Pre-Shared Key（プリ・シェアード・キー）の略。
外部の認証サーバを用いずに、PSK を利用して暗号化を行う方式です。

あ行

■ アカウント
コンピュータやネットワークで、ユーザを識別するための情報。ユーザカウントには、ユーザ名、パスワード、環境設定、使用権限などが含まれます。

■ アクセス制御
ユーザアカウントの持つ権限、属性等により、利用できる情報資源を制御すること。アクセス制御を行うシステムとしては、OS、グループウェア、アプリケーション（市販・自社開発）、ネットワーク機器等があります。また、アクセス制御の対象となる情報資源としては、ファイル、フォルダ、プリンター、ネットワーク等があります。

■ アクセスポイント
インターネットを利用する際に、ユーザが最初に接続する通信設備、または通信設備が置かれている場所。ユーザは、モデムや TA などの接続先として、自分の利用するアクセスポイントの電話番号を指定します。また、無線 LAN の場合には、電波を中継する通信設備をアクセスポイントと呼んでいます。アクセスポイントを有線の LAN につないでおくことで、無線 LAN を使用したクライアントがネットワークに接続できるようになります。

■ アクセスログ
システムの利用履歴として出力される情報です。多くの場合アクセス制御を実施しているシステムにて取得します。監査証跡としてアクセスログを保存しておく必要があります。

■ アドミニストレータ権限
コンピュータやネットワーク、データベースの管理者、または管理する権限のこと。管理者とは、あらゆる権限を与えられるユーザを表します。そのため、アドミニストレータ権限を乗っ取られてしまうと、コンピュータシステムを破壊されたり、格納されているデータを改ざんされてしまう可能性があります。

■ 暗号化
大事な情報を他人には知られないようにするため、データを見てもその内容がわからないように、定められた規則でデータを変えてしまうこと。暗号化されたデータは、復号という処理によって元のデータに戻すことができます。

■ ウイルス対策ソフト
ウイルスからコンピュータを防御するためのソフトウェアのこと。アンチウイルスソフトやワクチンソフトとも呼ばれています。コンピュータに侵入したウイルスを駆除したり、電子メールなどで送信するファイルにウイルスが含まれていないかどうかをチェックしたりすることもできます。

■ **ウイルス防御システム**
パソコンに導入するウイルス対策ソフトとは異なり、ネットワーク上のパケットを監視しウイルス検出／廃棄するシステムのこと。

か行

■ **記録媒体**

コンピュータで作成したデータを保存しておくもの。記憶メディアや記録メディア、または単にメディアと呼ばれることもあります。現在のコンピュータで利用されている記録媒体には、ハードディスク、フロッピーディスク、CD-ROM、MO ディスクなどがあります。

■ **グループウェア**

社内の情報共有基盤として用いられるソフトウェアの一種で、電子メール機能、スケジュール機能、ファイル共有機能、ワークフロー機能、電子掲示板等の機能を組み合わせたソフトウェアです。

さ行

■ サテライトオフィス
企業等が自社の勤務者のテレワーク実施施設として設置する小規模なオフィスのこと。最近では「テレワークセンター」という呼び方が一般的です。

■ サーバ
ネットワーク上で情報やサービスを提供するコンピュータのこと。逆に、サーバに対して、情報やサービスを要求するコンピュータをクライアントと言います。たとえば、インターネットでは、Web サーバやメールサーバ、DNS サーバなどが使用されています。

■ スクリーンセーバー
コンピュータを一定時間操作しなかった場合に表示するプログラムのこと。本来は CRT ディスプレイでの焼きつき（長時間同じ文字を表示し続けると、画面上に文字の痕跡が残されてしまうこと）を防止するための機能でした。現在の OS に搭載されているスクリーンセーバーでは、元に戻す際に、パスワードの入力を促す機能が搭載されているため、離席中に他人に自分のコンピュータを不正に使用されることを防ぐために利用することができます。

■ スパイウェア
コンピュータのデータを盗聴、盗難、破壊するために仕掛けられたプログラムのこと。

■ セキュリティホール
OS やソフトウェアにおいて、情報セキュリティ上の欠陥となる不具合のこと。セキュリティホールが残された状態でコンピュータを使用すると、ハッキングに利用されたり、ウイルスに感染したりする可能性があります。特に、ホームページなどにおいて、インターネット上で公開しているサーバには、誰もがアクセスすることができるため、セキュリティホールは必ず塞がなければなりません。

■ ソーシャルエンジニアリング
人間の心理的な隙などを突いて、コンピュータに侵入するための情報を盗み出すこと。ソーシャルには“社会的な”という意味があります。ソーシャルエンジニアリングの方法には、様々なものがあるため、万全な対策が取りにくいという点に注意しなければなりません。

た行

■ テープメディア
磁気による記録媒体のこと。テープカセットなので、検索が遅い、追加書き込みがしにくいなどの欠点がありますが、大量のデータを保存できる上に、安価であるため、サーバのバックアップ用記録媒体として一般的に使用されています。

■ トロイの木馬
コンピュータの内部に潜伏して、システムを破壊したり、外部からの不正侵入を助けたり、そのコンピュータの情報を外部に発信したりするプログラム。
トロイの木馬は感染能力を持つプログラムではないため、本来はウイルスに含まれるものではありませんが、現在では利用者には分からないように悪意のある行為を働くことがあるため、広義の意味で、ウイルスの一つとして扱われることがあります。

■ データベース
コンピュータにデータを蓄積するソフトウェアまたはそのデータの集まりのこと。データベースを利用することで、大量のデータを高速に検索し、集計することができます。データベースは、社内システムやショッピングサイトなどで利用されています。

な行

■ **なりすまし**

他のユーザのふりをすること。または、他のユーザのふりをして行う不正行為のこと。たとえば、その当人であるふりをして電子メールを送信したり、社内システムにログインしデータベースを改ざんしたりする行為などが挙げられます。

は行

■ バイオメトリクス認証
「指紋」、「虹彩」、「静脈」などの身体的特徴によって本人確認を行なう認証方式のこと。暗証番号やパスワードなどに比べ、原理的に極めて「なりすまし」しにくい認証方式であるため、関心が高まっています。

■ パスワード
本人であることを確認するために、ユーザ名とともに入力する文字列。銀行のキャッシュカードの暗証番号も、一種のパスワードです。

■ ハッキングツール
ハッキングとは、高度なコンピュータ技術を利用して、システムを解析したり、プログラムを修正したりする行為のこと。ハッキングツールとは、ハッキングに利用されるソフトウェアを指します。本来ハッキングには高い技術力が必要でしたが、技術を持たない人でも簡単にハッキングできるように作られたソフトウェアです。ハッカー自身が利用するツールと、トロイの木馬としてターゲットに侵入させるものがあります。

■ バックアップ
データを磁気テープなどの別の記録媒体に保存して、大事なデータの複製を作っておくこと。バックアップを取っておくことで、データが壊れてしまったときに、バックアップ時の状態に復元することができます。

■ パーソナルファイアウォール
個人で利用するためのファイアウォール製品。ソフトウェアとして提供されることが多く、インターネットに接続するコンピュータにインストールして利用します。

■ バッファオーバーフロー
代表的なセキュリティホールの一つ。メモリの領域を超えた量のデータが読み込まれた場合に、プログラムが異常な動作を行うこと。もしくは、そのような動作を利用した攻撃方法のこと。たとえば、バッファオーバーフローのセキュリティホールが残されている Web サーバでは、インターネットから不正なプログラムが実行されたり、システムが停止されてしまったりする危険性があります。

■ ハードディスク
パソコン等に搭載されている、電子データを格納する装置。パソコンには通常内蔵されていますが、データの格納領域を増やす場合には、外部に増設するための外部ハードディスクを利用することもあります。

■ **ファイアウォール**

外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステムのこと。またはシステムが導入された機器。ファイアウォールには“防火壁”の意味があります。火災のときに被害を最小限に食い止めるための防火壁から、このように命名されています。
また、ウイルス対策ソフトに機能が統合された、個人向けのパーソナルファイアウォールソフトもあります。

■ **不正アクセス**

利用する権限を与えられていないコンピュータに対して、不正に接続しようとすること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともあります。日本国内においても、インターネットに接続されたコンピュータに対する不正アクセスによる被害が急増したため、これらの行為を処罰する不正アクセス禁止法が施行されました。

■ **不正侵入**

利用する権限を与えられていないネットワークやコンピュータに侵入して、不正にネットワークやコンピュータを操作する行為。

■ **踏み台**

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元の IP アドレスによって、犯人が特定されてしまう可能性があります。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、犯人が自分のコンピュータを探しにくくします。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と言います。

■ **プロバイダ**

インターネットに接続できるサービスを提供する事業者のこと。電子メールを送ったり、ホームページを閲覧するためには、通常、プロバイダと契約する必要があります。

ま行

■ **無線 LAN**

無線通信でデータの送受信をする LAN のこと。各端末には無線 LAN カードが必要で、中継機器を経由して通信を行なう方式と、無線 LAN カード同士が直接通信を行なう方式があります。

ら行

■ ログ

コンピュータが保有するユーザの接続時刻や処理内容などを記録したファイル。通常は、ログを参照することで、コンピュータが正常に動作しているかどうかを管理することができます。たとえば、Web サーバの場合には、管理している Web サイトに訪問してきたユーザの情報が格納されます。

■ ログイン

コンピュータやネットワークの利用を開始するために、ユーザが認証を行って、コンピュータを使用可能な状態にすること。一般的には、ユーザ名とパスワードを用いて、ユーザ認証を行います。

■ リモートアクセス

外出先や自宅、サテライトオフィス（テレワークセンター）等から、社内ＬＡＮ等へ接続する方法や手段。リモートアクセスの方法としては、以下の種類があります。

- ダイヤルアップ：電話回線等の公衆回線を利用してアクセスする方法
- インターネット接続：インターネット利用して社内ＬＡＮへ接続する方法
- 専用線接続:サテライトオフィス等と社内ＬＡＮとを専用線で接続する場合もリモートアクセスという場合もあります。

■ ルータ

セグメントと呼ばれるネットワークの単位にネットワークを分割する装置のこと。もしくは、別のセグメントのネットワークへ通信する際の経路情報の管理を行う装置のこと。ルータは、ネットワークをセグメントに分割することで、セグメント外に不要な通信を流さない役割を担います。また、個々のコンピュータ自身で通信する相手の経路情報を管理させないため、ルータを使うことで、効率的な通信が実現されます。

わ行

■ ワーム
他のファイルに寄生して増殖するのではなく、自分自身がファイルやメモリを使って自己増殖を行うタイプのウイルス。

■ ワンタイムパスワード
個人が記憶するパスワードではなく、装置やソフトウェアにより一度限りのパスワードを生成し、そのパスワードを入力してアクセス等を行う仕組みのことです。パスワード生成装置は、持ち運びできる小型なものでカードやキーホルダーになっています。

「テレワークセキュリティガイドライン解説書」

第１版　２００４年１２月２７日

総務省　情報通信政策局　情報流通振興課　情報流通高度化推進室
ＴＥＬ：０３－５２５３－５７５１
ＦＡＸ：０３－５２５３－５７５２