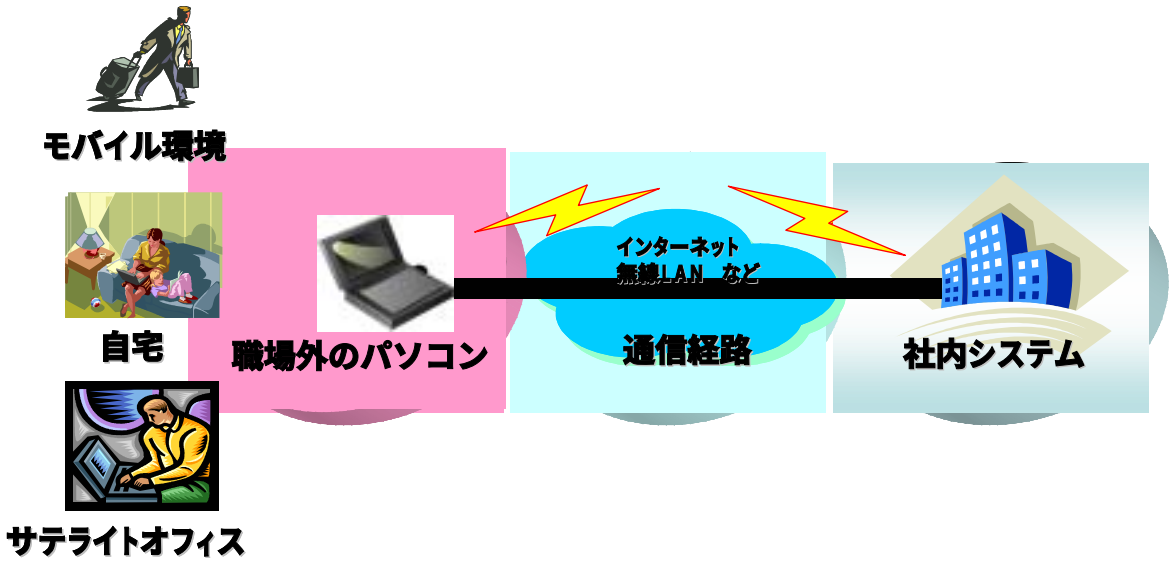
別添２

# 職場外のパソコンで仕事をする際のセキュリティガイドライン

## ～ウィニー等ファイル交換ソフトを介したウィルスなどによる情報漏えい対策のために～




平成１８年４月

総務省

# 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。

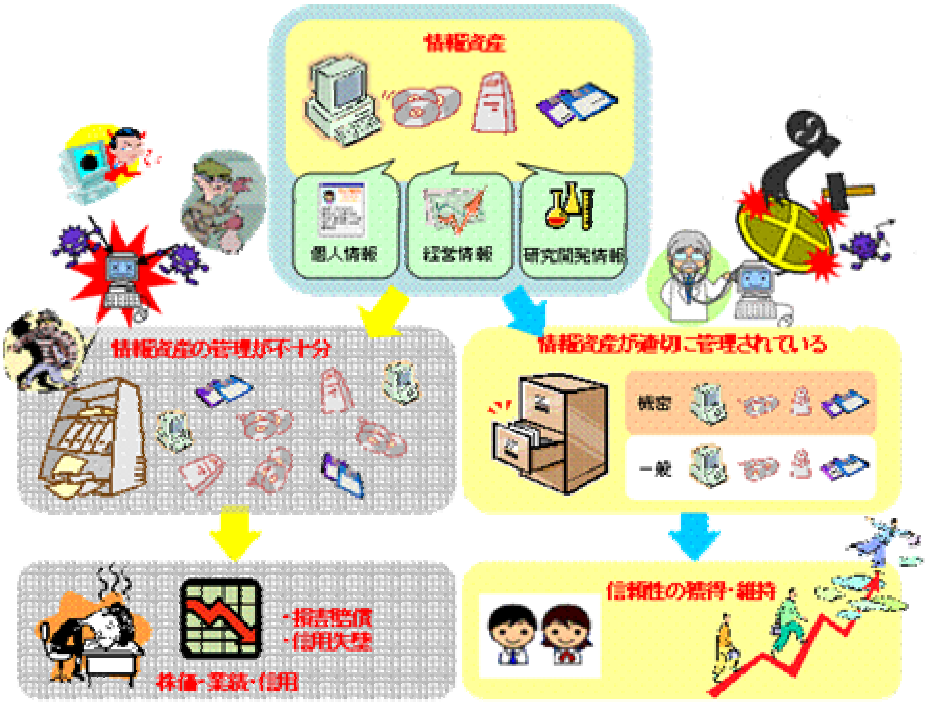
◆情報セキュリティ事故の例

- 業務に利用するパソコンが暴露ウィルスに感染していたため、顧客情報や企業秘密などが漏えいした。
- 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。
- 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）により、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。

※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。

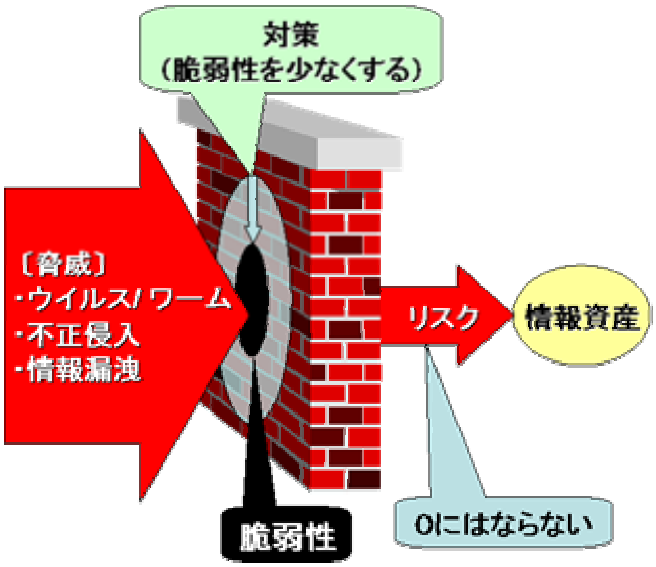
**図１　情報セキュリティ対策の必要性**




　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、体系的な対策を実施する必要があります。（※２）

※２　体系的な情報セキュリティ対策と情報セキュリティポリシーの考え方については、２０ページ以下の「参考」をご参照下さい。

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。（図２）

特にインターネットを活用することの多い職場外でのパソコン使用では、ウイルス・ワーム（※３）による被害、企業電子データの改ざん、機密情報の漏えいなどによる社会的被害・損害が発生するおそれが高いと言えます。このため、職場外でパソコンを使って仕事を安心・安全に行うためには、情報セキュリティ対策について十分な考慮と適切な措置が必要となります。

このガイドラインはこのような状況を踏まえ、企業･組織における情報セキュリティ対策の一助となるよう、「テレワークセキュリティガイドライン（平成 16 年 12 月総務省）」を援用し、職場外のパソコンで仕事をする際の対策を主眼として再編したものです。

このガイドラインで示した内容は、あくまでも職場外でパソコンを使用する際に想定される危険性を前提に、モデルケースとしての対策等を例示するものであり、すべての情報セキュリティ対策を網羅したものではありません。情報セキュリティ対策とは、各企業の企業規模、業種・業態、取り扱う情報の内容や、そこにあるリスク、各企業の対策方針などによって個別具体的に検討対処する必要があるものであることをご理解ください。

具体的には、職場外で従業員がパソコンを使って業務を行う企業を前提として、基本的に実施すべき情報セキュリティ対策を紹介することとしています。したがいまして、SOHO や個人事業者等の方にとっては、本ガイドラインの記載内容をそのまま当てはめることができない箇所もある点、ご了承願います。

なお、対策の詳細については、「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）」をご参照下さい。

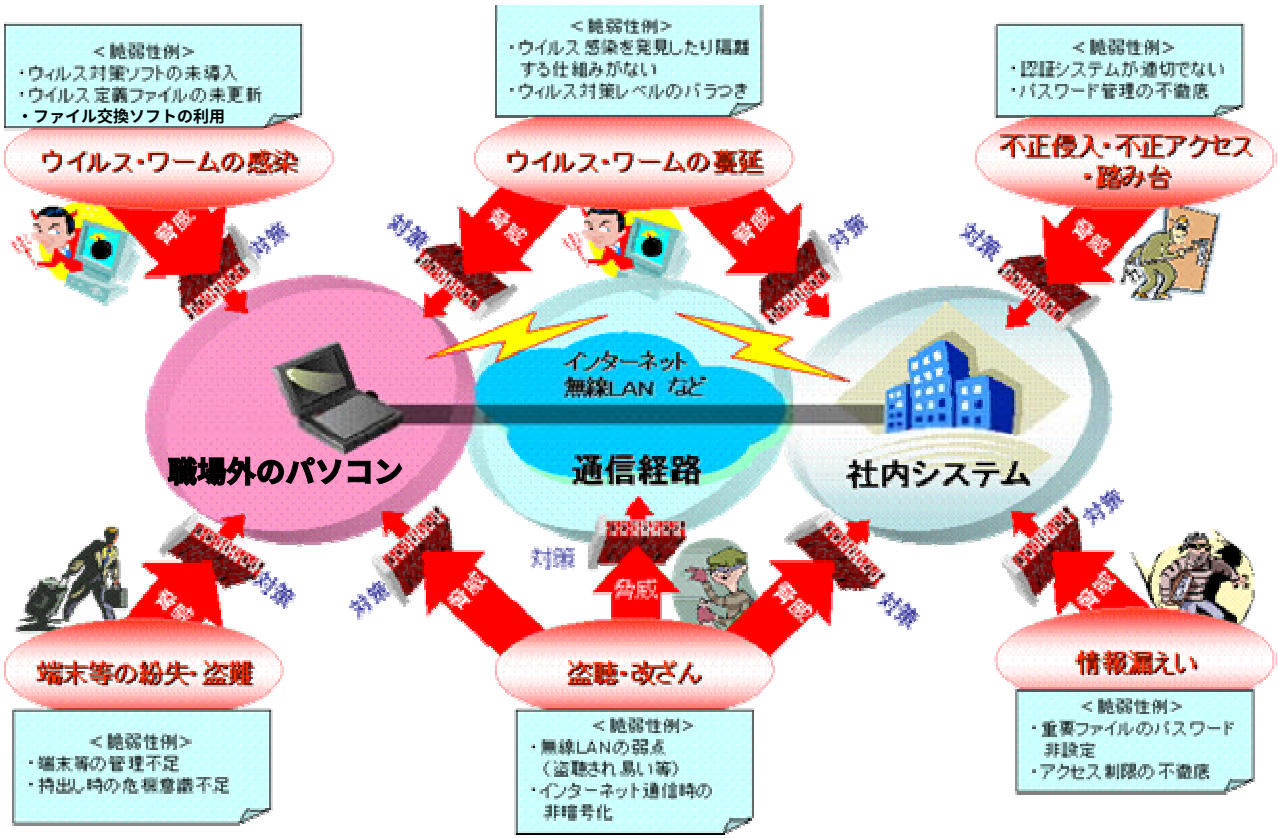
※３　ワーム…自己増幅を繰り返しながら破壊活動を行うプログラム。

# １．職場外のパソコンで仕事をする際の情報セキュリティ対策のポイント

職場外のパソコンで仕事を行う場合、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します。このため、ウイルス・ワームの感染、パソコンや記録媒体の紛失・盗難、ファイル交換ソフトを介して感染するアンチニー（※４）などによる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、職場外でパソコンを使用する際の脅威と脆弱性について図３に示します。

※４　アンチニー･･･ファイル交換ソフトのウィニー（Ｗｉｎｎｙ）でやり取りされるファイルを介して感染するコンピュータウィルス。パソコン内の情報をインターネット上に流出するなどの被害をもたらす。

図３　職場外のパソコンで仕事をする際の脅威と脆弱性について




上図のように、職場外でパソコンを使用する場合には様々な脅威や脆弱性が存在します。企業における社内システムや機密情報などの重要な情報資産を守るための情報セキュリティ対策ポイントは、「ルール」・「人」・「技術」の三位一体のバランスがとれ

た対策が実施されていることです（図４）。

**「ルール」**

基本方針に従った対策基準や実施内容において、「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を適用及び運用していくうえでの決まり事です。ルールに従い対策を適用することにより、実施内容の形骸化や不履行を防ぎ情報セキュリティレベルを維持することが重要です。

**「人」**

情報セキュリティのために決めたルールを守るのは面倒と思われがちです。しかし、人的ミスは重大な情報セキュリティ事故につながります。各個人レベルでの情報セキュリティに関する知識や認識を高く保つことが重要です。

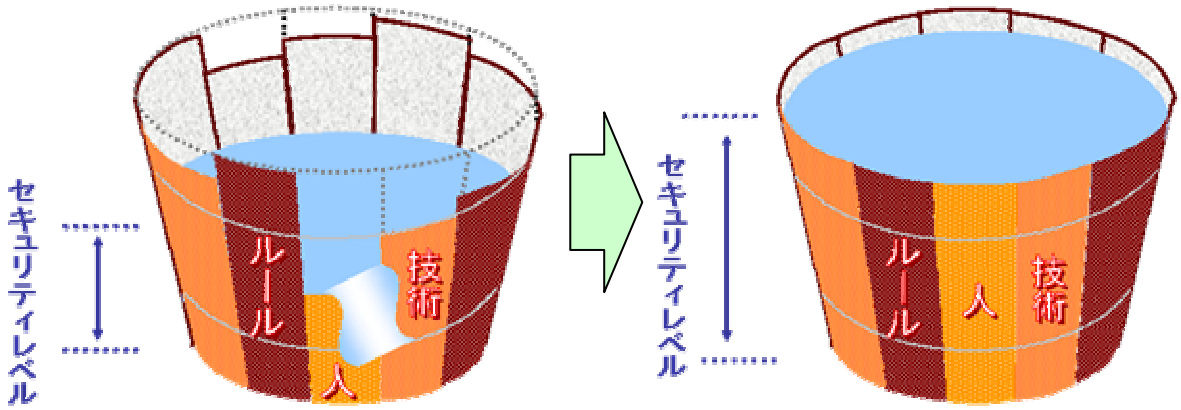
　組織で行われている情報セキュリティ対策は、技術への投資に偏重しており、「人」に対する投資は十分に行われていない場合も見受けられます。しかしながら、情報セキュリティ事故を未然に防ぐためには、積極的に「人」への投資（情報セキュリティ管理者教育、従業員教育・啓発活動）を行うことが重要です。

**「技術」**

情報通信技術の進歩により、様々な情報セキュリティ対策技術が開発され、数多くの製品・サービスがあります。守るべき情報資産に合わせ、適切な技術対策を選択することが重要です。

図４　情報セキュリティバランス

・バランスが悪い情報セキュリティ対策　・バランスがとれた情報セキュリティ対策




「ルール」、「人」、「技術」のバランスが悪いと、対策として不十分になり、全体の情報セキュリティレベルは低下してしまう。

「ルール」、「人」、「技術」の対策がバランスよく保たれていると、高い情報セキュリティレベルを維持できる。

**情報セキュリティ対策として重要と思われる事例を大まかに示せば次ページのとおりとなります。それぞれの説明やその他の事例については９ページ以降をご覧下さい。なお、情報セキュリティ対策は、設定するリスクの種類や程度に応じて様々ですから、実際に作成する対策は、個々のリスクを検討の上、こうした事例を取捨選択･加除修正していく必要があります。**

## ＜職場外のパソコンで仕事をする際のセキュリティ対策１８か条＞

### 「ルール」

① 情報セキュリティ管理体制（管理者の選任、情報資産の管理方法の策定など）を構築する。

② 職場外でパソコンが使用される場合でも、情報セキュリティポリシーが正しく守られているか、定期的なチェック（監査）を実施する。

③ 社内システムへアクセスするためのアカウント（※５）については、管理方法を明確に定め、厳格に管理する。

④ 従業員にパソコンを貸し出す際には、「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」などを把握しておく。

⑤ 業務用に貸し出されたパソコンは許可された目的内で利用条件に従って適切に用いる。

⑥ 一時的に職場外に持ち出すデータは原本ではなく、原本からの複製とする。

⑦ 私物のパソコンを業務に利用する場合には、インストールされているソフトを確認するなど定められた利用条件に従う。

⑧ ネットワークを用いて業務を実施する際には、指定された通信手段を用いる。

### 「人」

⑨ トップダウンにより情報セキュリティポリシーを周知・徹底する。

⑩ 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、日々、教育・啓発活動を実施する。

⑪ 就業規則や外部委託契約にデータの持ち出しに当たっての許可など機密保持規定や罰則規定を設ける。

⑫ セキュリティ事故発生時は、直ちに定められた担当者に連絡する。

### 「技術」

⑬ ウイルス対策ソフトをインストールし、最新の定義ファイルに定期的に更新する。

⑭ ＯＳ（※６）及びソフトウェアにおいては、パッチ（※７）の更新を定期的に行う。

⑮ ＯＳのログイン時などのパスワードは、他人に推測されにくいものとし、定期的に更新を行う。

⑯ 機密性の高いデータを保存・送信する際には必ず暗号化する。

⑰ 社内システムと持ち出し用パソコンの環境の境界線にはファイアウォール（※８）やルータ（※９）などを設置し、不必要なアクセスを遮断する。

⑱ 社内システム内にある重要データは、安全な領域（※１０）に格納するとともにアクセス権限の付与は必要最低限とする。

※５　アカウント…ネットワーク及び社内システムにログインする際の権利（ユーザ ID など）。

※６　ＯＳ…メモリやハードディスクの管理やキーボードなどの入出力機能など、パソコンに基本的な動作をさせるために必要なソフト。

※７　パッチ…不具合の修正等への対応を行うため、アプリケーションの一部分を書き換えるプログラム。

※８　ファイアウォール…不正アクセスなどからサーバやＰＣを保護するための機器のこと。

※９　ルータ…通信経路の管理を実施しているネットワークを構成する機器のこと。

※１０　安全な領域…守るべき重要な情報資産が、危害や損傷などを受けずに正常な状態でいられる領域のこと。情報セキュリティの三大要素である機密性、完全性、可用性が適切に確保されている必要があり、耐震設備や入退出管理設備などの「物理的」なものだけでなく、アクセス制御や認証など「論理的」な情報セキュリティ対策も含めた検討が必要。

## ２．「ルール」についての対策

情報セキュリティポリシー（※１１）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ように管理していきます。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。

※１１　情報セキュリティポリシー･･･２０ページ以降の「参考」をご参照下さい。なお、このガイドラインでは情報セキュリティポリシーを構成する「基本方針」「対策基準」「実施内容」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言う用語を用いています。

### （ア）組織として守るべきルール

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、職場外でパソコンを使用する環境においても情報セキュリティのルールが正しく守られているか、現場の状況に合っ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、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５)

① 情報資産の管理方法・管理責任者を規定する。

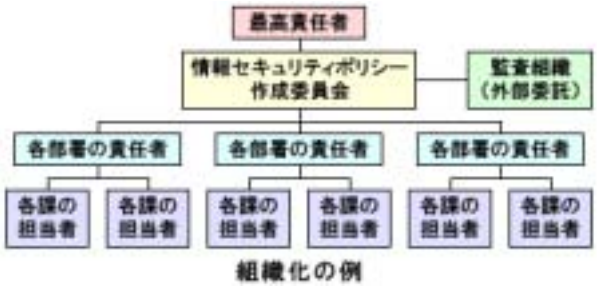
② 管理責任者に権限を与える。

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。

(2) 定期的な監査の実施

職場外でのパソコン使用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などによる監査を実施する。

図５　事例　情報セキュリティ管理体制



## （イ）システム管理者が守るべきルール

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・移転などを行った場合、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、端末を企業側から貸し出す場合においては利用状況などについて適正な管理を行い、また、社内システムへ外部からアクセスする際の通信経路の申込み・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６）

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。

② アカウントの発行・廃止・変更は、管理者の承認を得る。

③ 不用なアカウントの削除は徹底する。

(2) 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）」などを管理する。複数の従業員でパソコンを使い回す場合、返却時にデータが削除されていることを確認する。

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し出す。また、返却されたパソコンは、ウイルスチェックを行うとともに、不要なソフトウェア（ファイル交換ソフトなど）がインストールされていないか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。

③ 私物のパソコンを利用させるときは、貸し出し用のパソコンと同様のセキュリティ対策がなされているか確認する。

(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、ＶＰＮ（※１２）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。また、決められた通信経路以外を使うことを禁止する。

※１２　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。

図６　事例　アカウントパスワード管理

## （ウ）パソコン使用者が守るべきルール

職場外でパソコンを使用する際には、不特定多数の人目に触れる場所などでは周囲の環境に十分配慮する必要があります。職場外で使用するパソコンは、社内環境と異なり、様々な場所での利用が想定され、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、職場外で従業員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、ルールが守られるためには、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などに配慮し、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など）

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（※１３）やＵＳＢメモリ（※１４）などの持ち運び可能な電子媒体）を持ち出す場合には、紛失、盗難、置き忘れなどに注意する。

③ 自分以外の者にパソコンを使用されないようにする。

(2) パソコンで利用するデータの取扱い （図７）

① 電子データを「機密」「一般」など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など、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 一時的に職場外で参照する場合など、原本である必要性がないものは、複製を持ち出す。

⑤ 情報漏えいの危険を最低限に抑えるため、外部に持ち出すデータは必要最小限とし、不要なデータはこまめに削除する。（※１５）

⑥ 作業を終えたデータは適宜安全な領域（社内のファイル・サーバなど）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。

(3) 公私区分

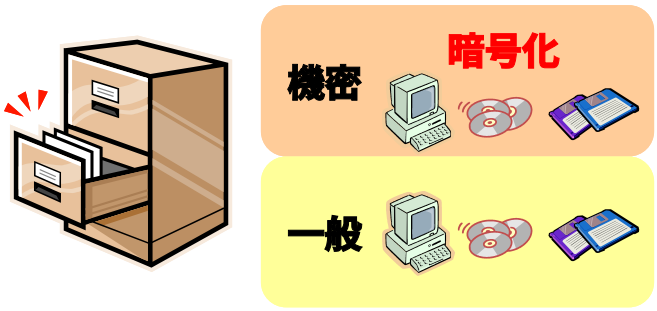
① 業務用に貸し出されたパソコンを許可された目的以外で用いることを禁止する（業務に関係のないファイルをダウンロードしたり、業務に必要のないソフトウェア（ファイル交換ソフトなど）の導入･使用を禁止するなど）。

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、インストールされているソフトを確認するなど、定められた利用条件に従う（例えば漏えいすると困るような情報は扱わない。どうしても扱う必要がある場合は業務用に貸与されたものと同等のセキュリティ対策を行うなど）。

※１３　ＣＤ－Ｒ／ＲＷ…書き込み可能なＣＤ-ＲＯＭ。うち、ＣＤ－ＲＷは消去も可能なもの。
※１４　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。
※１５　ただし、テレワークなど職場外でのパソコン使用が長期又は恒常的で、職場外のパソコンで新たなデータを加えたり創成したりする場合は、そうしたデータの改ざんや破壊に対応するため外部記録装置（ＣＤ－Ｒ／ＲＷ、ＵＳＢ、外部ハードディスクなど）への保存などのバックアップを実施することが適切となります。

図７　事例　パソコンで利用するデータの取扱い



## 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」すなわち従業員やシステム管理者などが、定められ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、以下のような対策により各個人レベルで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などを活用し、情報セキュリティ教育を定期的に実施する。　（図８）
(2) 情報セキュリティに関する冊子を作成し配布する。

また、例えば、従業員全員を対象に、以下のような分かりやすい「標語」を作成し、常に意識させることが効果的です。（例えば、情報セキュリティ標語が記載されたカードを作成し、常に携帯させるという方法もあります。）

**「情報セキュリティ標語」（例）**
**一、ウイルス定義ファイルの更新を業務開始前に必ずチェックすること。**
**二、業務終了後はパソコン、記録媒体、機密文書は必ず施錠した場所に保管すること。**
**三、業務用に貸し出されたパソコンを私用目的に利用しないこと。また第三者に触れさせないこと。**
**四、私物パソコンであっても業務に使用するものには、不要なソフトウェアをインストールしないこと。**
**五、電子データの送信については送信時に宛先を確認すること。**
**六、機密性の高い電子データについては暗号化して保存すること。**
**七、機密性の高い電子データを送信する際には必ず暗号化すること。**
**八、業務用に貸与されたパソコンに業務に不要なソフトはダウンロード及びインストールしないこと。**
**九、パスワードは、他人に推測されにくく、機械的な処理でも割り出しにくいものとすること。また、パスワードは定期的に変更すること。**
**十、情報セキュリティ事故（パソコン故障／盗難／紛失、データ破壊、ウイルス感染、不正アクセスなど）発生時や対応策がわからない場合は、直ちに担当の○○○に相談すること。**

図８　事例　情報セキュリティ教育


## （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。そのため、機密情報の外部流出を防ぐための機密保持規定（データの持ち出しに当たっては暗号化などの機密保持対策などがきちんとされていることについてチェックし、許可を得ることなど）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９）
(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９　事例　機密保持条項の規定


機密保持･罰則規定

## （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 パソコンがウイルス・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。**

# 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。技術的対策は様々な脅威に対して「認証」、「検知」、「制御」、「防御」を自動的に実施するものであり、こうした技術を適切に取り入れておく必要があります。ここでは職場外でパソコンを使用する環境を「パソコン」、「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）職場外で用いるパソコンにおける対策

職場外で用いるパソコンは、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、パソコンを職場外で使用する場合に必要となる対策について述べます。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パッチ適用など）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

職場外でパソコンを使用して業務を行う場合、そのパソコンでインターネットを利用することも多いと考えられます。このため、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。

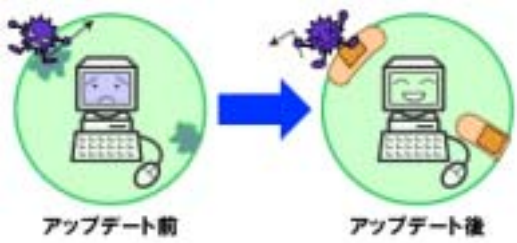
◆事例

(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。

(2) 最新のパッチを適用　（図１０）
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。

(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などを開く前に、ウイルス対策ソフトによる検査を実行する。

図１０　事例　最新のパッチ適用




## パソコン等の紛失・盗難対策

職場外にパソコンを持ち出すと、悪意ある第三者が近づきやすい環境にさらされます。そのため、パソコン内の電子データを暗号化するなどして、他人によるパソコンの不正操作を防ぎ、電子データの取り出しやパソコン等の紛失・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) パソコンにはスクリーンセーバー（※１６）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。
(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。
(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。
(4) パソコンにはハードディスクの暗号化または BIOS（※１７）パスワードを設定する。
(5) 「機密」と区分された電子データを記録媒体に保存する場合は暗号化を行う。

※１６　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。

※１７　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。

## 不正侵入・踏み台対策

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、パソコン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、パソコンが外部から「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、パソコンが「踏み台（※１８）」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、下記のようにパソコンを適正な状態にしておく必要があります。

※１８　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(※１９)を導入する。
(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。
(3) 不審なサイトへはアクセスしない。

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

## （イ）通信経路における対策

職場外でパソコンを使用する場合は、インターネットなどを利用した電子データの送受をすることもあると考えられます。電子データの送受に当たっては、電子データの盗聴、横取り、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する際には、ＶＰＮなどによりデータを暗号化し、安全な通信経路を確保する。

(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。(※２０)

※２０　無線ＬＡＮの情報セキュリティの具体的対策については、「安心して無線ＬＡＮを利用するために（総務省）」（http://www.soumu.go.jp/joho_tsusin/lan/index.html）を御参照下さい。

## （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。職場外のパソコンから社内システムにアクセスできるようにするなど、外部とのやり取りを可能とすることは、社内システムへの不正侵入・不正アクセスの可能性を高めることにもつながります。また、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も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

職場外のパソコンのみではなく、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、「パソコンにおける対策」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）。

(2) ウイルス・ワームに感染したパソコンは即座に隔離する（本人への通知・アクセスの制限などを含む）。

## 不正侵入・不正アクセス対策

悪意ある第三者は、インターネットなど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、正規の利用者（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など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１１）
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（※２１）を行う。

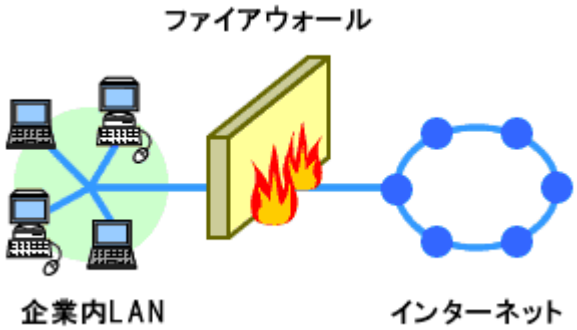
(2) 社外から社内システム／ネットワークへのアクセス制御
社外から社内システム／ネットワークへのアクセスについては、ユーザごと（各個人別）にアクセス権の設定を行うともに、パスワードはワンタイムパスワード（※２２）などを利用し認証機能を強化する。

(3) 守るべき電子データ（機密情報・個人情報など）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、ファイアウォールなどで守られた安全な領域に保存するとともに、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。

※２１　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。

※２２　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。

図１１　事例　ファイアウォールの設置




## 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状況についてアクセスログ（※２３）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。

※２３　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。

# 参考．情報セキュリティ対策の基本的な考え方

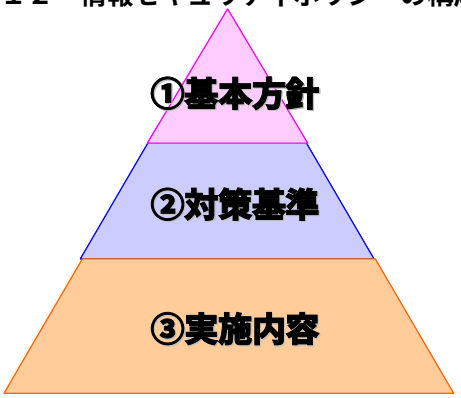
## • 情報セキュリティ対策について

情報セキュリティ対策をきちんと行うためには、個別的･対処療法的なものではなく、体系的に行うことが重要です。このために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１２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。

図１２　情報セキュリティポリシーの構成




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。

参考として次ページに基本方針の例を示します。

## （参考）　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**

***「脅威」、「脆弱性」、「リスク」、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」などの用語について定義***

**2．体制**

***「情報セキュリティ委員会」、「情報セキュリティ主管部門」、「情報セキュリティ管理者」などについて規定***

**3．情報セキュリティ対策**

***情報資産を保護するための情報セキュリティ対策について、分類し、それぞれの概要を説明（人的セキュリティ対策、技術的セキュリティ対策など）***

**4．適用対象者**

***従業員のみならず、経営層や情報セキュリティ管理者、協力会社従業員などについても適用される旨を規定***

**5．適用対象者の義務**

***適用対象者は情報資産を扱う上で、情報セキュリティポリシーに同意し、遵守しなければならない旨を規定***

**6．罰則**

***従業員本人の過失または故意によって、情報セキュリティに対し、重大な損害を与えた場合の処分規定を就業規則などに含めることを規定***

**7．教育及び啓発**

***定期的または必要に応じて、情報セキュリティに関する教育及び啓発活動を行い、セキュリティポリシーの周知徹底を図る旨を規定***

**8．評価及び見直しの実施**

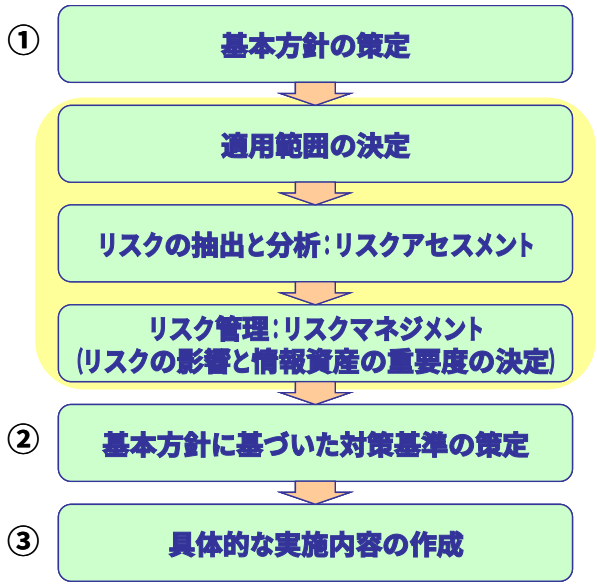
***情報セキュリティポリシーの遵守状況の監査、セキュリティ対策の評価など、状況の変化を踏まえ、適宜情報セキュリティポリシーの見直しを実施する旨を規定***

**以上**

**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。ここでは、「情報セキュリティマネジメントシステム（ISMS）（※２４）」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１３では、情報セキュリティマネジメントシステム（ISMS）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(※２５)を完全に満たすことは難しく、また、情報セキュリティ対策には費用が発生します。このため企業が持つ情報資産の重要度や特質を考慮して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。

図１３　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



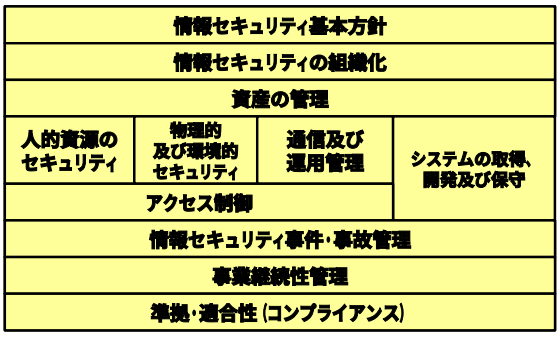

※２４　情報セキュリティマネジメントシステム･･･　企業や組織が情報セキュリティを確保・維持するために情報セキュリティ管理体制を構築し、継続的にリスクを管理していく枠組みのこと。ISMS（Information Security Management System）とも呼ばれています。

※２５　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。

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１４に示します。

図１４　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



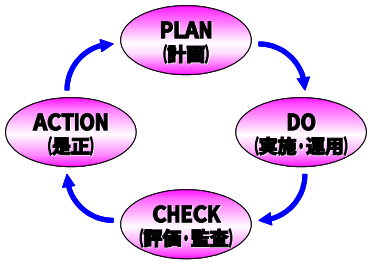

出典：ISO/IEC17799 を基に作成

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。情報セキュリティで最も重要なことは、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（※２６）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１５）。

図１５　情報セキュリティに関する PDCA サイクル




※２６　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。

## 問い合わせ先について

本ガイドラインの内容につきましては、下記までお問い合わせください。

【問い合わせ先】

総務省　情報通信政策局　情報通信政策課　情報セキュリティ対策室
ＴＥＬ：０３－５２５３－５７４９
ＦＡＸ：０３－５２５３－５７５２
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