一般社団法人エコ・ペーパーレス協議会

テレワーク検定

テレワークはじめの一歩　第3章

学習マップ

NOW

第1章
テレワークの基礎知識
- テレワークの基本
- なぜテレワーク？

第2章
テレワークの心構え～考え方編
- テレワークの心構え

第3章
情報セキュリティー対策
- テレワークと情報セキュリティー

第4章
テレワークの前に準備しましょう！
- 必要な機材と便利な使い方
- スムーズにテレワークを行うコツ

第5章
まとめ
- 実例１
- 実例２
- 実例３
- 終わりに

第3章　情報セキュリティー対策

インターネットや情報通信機器を利用するにあたり理解しておくべき対策について学習しましょう。

エコ・ペーパーレス協議会
テレ検
Since2016

テレワークと情報セキュリティー

インターネットや情報通信機器を利用するうえで情報セキュリティー対策を理解していることは当然といえます。一般的な情報セキュリティーの考え方や心がけ、対策はテレワーク時も同様に理解し実施すべきです。
ここからは一般的にも応用できる情報セキュリティー対策について学習しましょう。

情報を取り扱っている認識

テレワーカーも「企業の一員」として情報セキュリティー対策を行う必要があります。

まずはテレワーカー自身が業務を行うにあたり**「企業の秘密情報」や「個人情報」という重要な情報を取り扱っている**という意識が重要です。

テレワークでは、自宅やサテライトオフィスあるいはカフェなど場所を問わずに働くことが可能です。そのため、情報のやりとりにインターネットを利用したり、従業員以外の第三者が立ち入る場所での作業をしたりします。
また、１人や少人数で働く機会が多くなりますが、この際に自身が「重要」な情報を扱っているということを決して忘れてはいけません。

参考：秘密情報と機密情報の違い

秘密情報	秘密：（１）隠して人に知らせないこと。公開しないこと。また，その事柄。「－にする」「－がもれる」「企業－」と定義。（大辞林第３版） 一般に多数用いられており、秘しておきたいことを表すための一般的な用語として用いられる。
機密情報	機密：「重要な秘密。主に政治上・軍事上の事柄についていう。「国家の－」「－文書」」と定義。（大辞林第３版） 国の組織の事務分掌を定めるときに「機密に関すること」のように用いられる用例が多い。

企業にとって重要な情報

「企業にとって重要な情報」が何か、どのような形態か確認します。

企業にとってその情報が企業外に漏れると、企業の事業運営上または経営上で重大な問題を引き起こす可能性のある情報が「重要な情報」です。

- 自社にとって何が重要な情報か
- 情報はどのような形で保管、管理されているか
- 情報の持ち出せる人や方法、ルールは決まっているのか
- 情報の処分方法は決まっているのか

このような対策を確認してテレワークを行いましょう。

重要な情報 例	• お客様から預かっている個人情報 • 企業で働く従業者の個人情報 • 企業運営のための企業情報 • ノウハウ等の機密情報
情報の形態 例	• 図面や書類 • データ • メール • CDなどのメディア

情報漏えいの先にあるもの

情報漏えいを起こすと企業の経営にも大きなダメージを与えます。

例えば「企業の秘密情報」は一度でも漏えいすると、たちまち情報の資産としての価値が失われてしまい、その回復は非常に困難になります。それにより企業の経営に致命的な悪影響を与える場合もあります。
また近頃よく報道もされていますが、「個人情報」も同様に一度でも漏えいしてしまうと企業経営に悪影響を及ぼします。

情報漏えい事件一例

業種	概要
教育・研究業	委託業者の派遣従業員により3,504万件の顧客情報が流出し、一部はダイレクトメールの送付に利用。最終的には、取締役2名が引責辞任。
通信業	外部からの不正アクセスを受け、最大2,200万件のＩＤが外部流失した可能性を公表。
銀行・信託業	過去の顧客取引データ（合計672万人分）を記録したコムフィッシュ（記録メディア）を紛失。

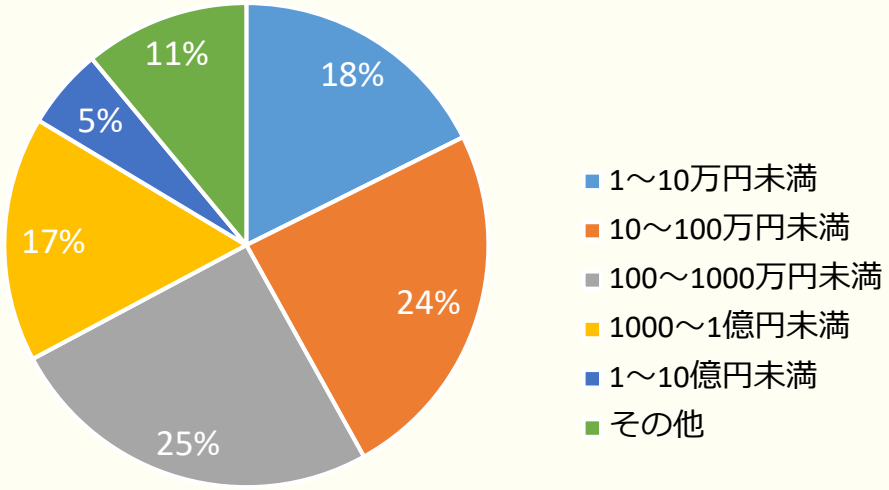
情報漏えいによる企業の責任

情報漏えいを起こすと企業は多額の損害賠償を支払う責任が生じます。

情報漏えいにより、企業の情報資産の価値が落ちてしまうだけでなく、情報漏えいにより被害を受けた各所へ損害賠償を支払う責任が生じます。

情報漏えいの内容により金額に差はありますが、企業には高額の賠償を支払う責任があるという事を忘れてはいけません。

一件当たりの想定損害賠償額（2015年）



一件当たり平均損害賠償額

3億3705万円

引用：
2015年情報セキュリティーインシデントに関する調査報告（速報版）
（日本ネットワークセキュリティ協会）

情報漏えいによる個人の代償

情報漏えいを起こした個人が、人事上の処罰を受ける可能性もあります。

従業員に情報漏えいの危機意識を強く持ってもらうために、就業規則に罰則を規定している企業もあります。日々の業務や何気ない行動から情報漏えいにより企業損害を与えた場合、処罰を受ける可能性があるのです。

自分の人生を狂わせないためにも、情報漏えいを起こさない強い意識が重要になります。

【懲戒処分の種類例】

・懲戒解雇：会社からのペナルティの中で最も重い処分。特定の行為に対する「制裁」として即時に解雇。
・諭旨解雇：趣旨や理由を諭し告げ、企業と従業員が話し合い両者納得の上での解雇処分。
・出勤停止：始末書の提出＋就労を一定期間禁止し、その期間の賃金を支給しない処分。
・減給：　　始末書の提出＋一定の期間、一定の割合で減給する処分。
・けん責：　始末書の提出により強く戒める処分。

情報セキュリティー対策の心構え

情報セキュリティー対策はバランスを保ち運用されるものだという認識が必要です。

情報資産を守るためには、「ルール」「人」「技術」の三位一体のバランスがとれた対策を実施し、全体のレベルを落とさないようにすることがポイントとなります。そのためテレワーカー（人）も企業が定めた「ルール」「技術」を理解し確実にそれを実行していくことが求められます。

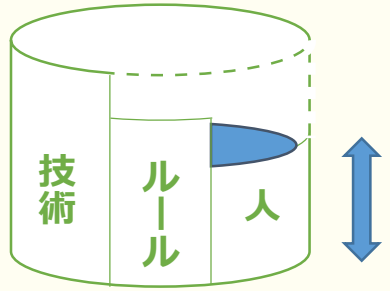
企業が情報セキュリティー対策を行うために重要なこと

①保護すべき情報資産を洗い出す
②どのような脅威や脆弱性、リスクがあるのかを十分に把握、認識
③②を行ったうえで体系的な対策を実施

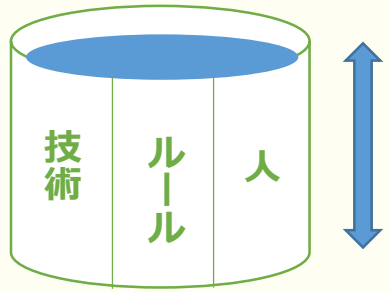
情報セキュリティー対策の特徴

「最も弱いところが全体のセキュリティーレベルになる」

どこか１箇所に弱点があると、他の対策をいくら強化しても全体のセキュリティーレベルの向上にはつながらない。



バランスが悪い情報セキュリティー対策



バランスが取れた情報セキュリティー対策

情報セキュリティー対策～人と技術の対策～

「技術的なセキュリティー対策」と「人のセキュリティー対策」を確認しましょう。

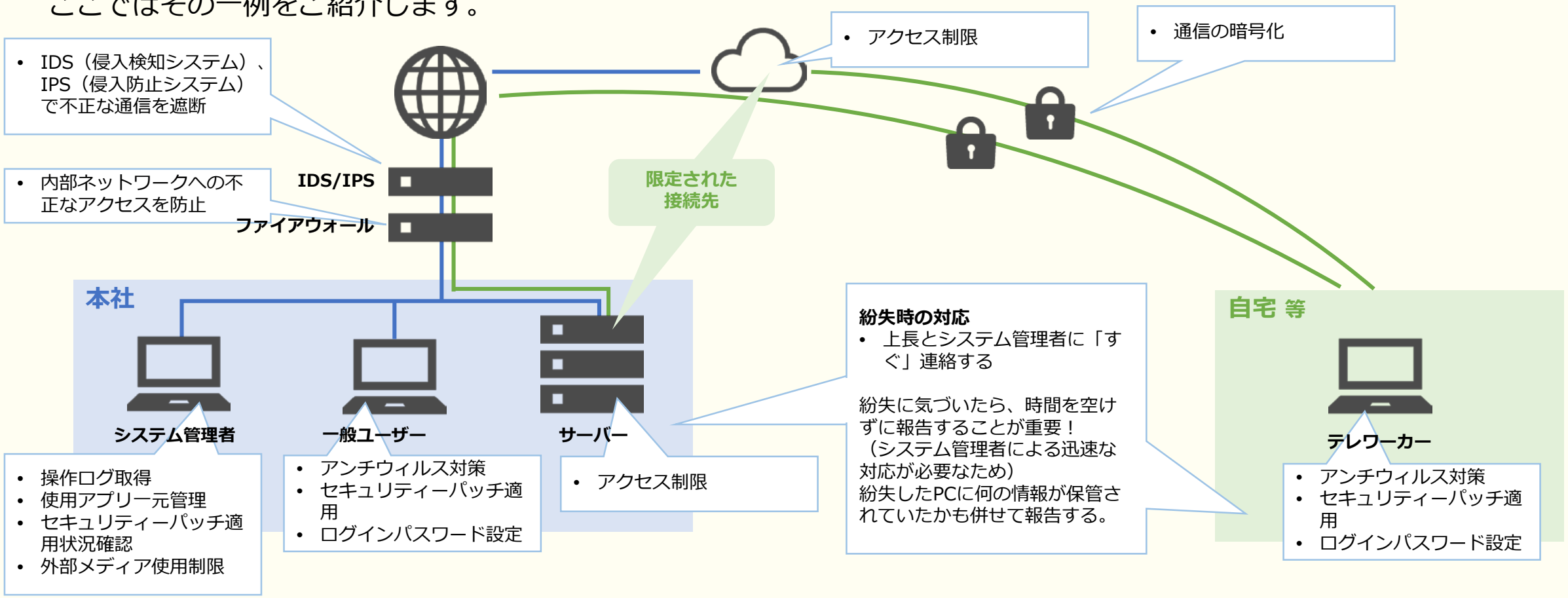
このような情報セキュリティーについて各企業で対策を設けており、社内の安全管理措置強化や委託先などの監督の強化が義務付けられています。テレワーク時も会社の規定に沿った対策をする必要があり、テレワーカーは人の対策を確認し、守ることが重要になります。

技術的対策	人の対策
・個人のコンピューターを守ること （ウイルス対策、情報の暗号化、脆弱性解消など） ・企業のネットワークやシステムを守ること （ファイアウォール、IPS（侵入防止）対策など）	・企業はセキュリティー対策ルールや体制を決め、 それを従業員が守ること

技術的対策

まず、情報セキュリティー対策における「技術的対策」について簡単に確認しましょう。

技術的対策は、企業の情報システム部など関連部署が対策を行っています。
ここではその一例をご紹介します。



人の対策：情報漏えい対策の基本

情報セキュリティー対策における「人の対策」について確認しましょう。

企業が定めたセキュリティー対策ルールや体制をもとに、情報漏えいが起きないよう注意することが必要です。

また、下記の基本項目は独立行政法人情報処理推進機構が推奨する項目です。企業のルールに入っていなかった場合も、仕事を行う上で重要な内容になります。必ず確認して守るようにしましょう。

できていますか？情報漏えい対策 基本項目

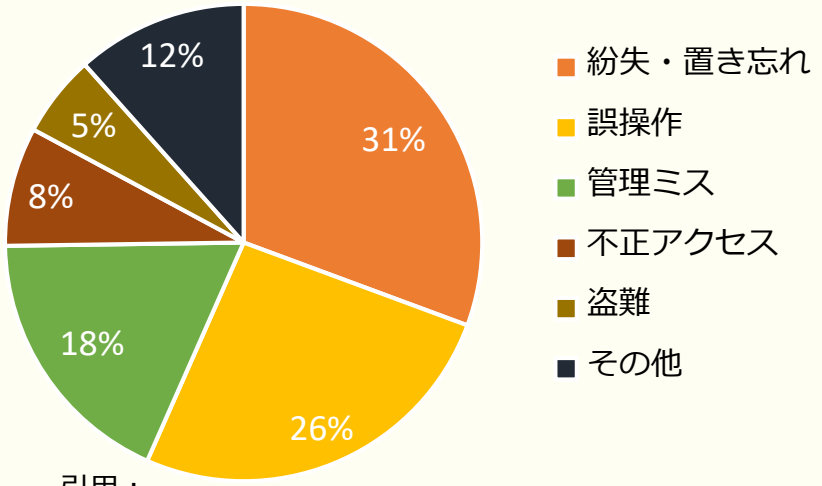
① 企業(組織)の情報資産を許可なく持ち出さない
② 企業(組織)の情報資産を未対策のまま目の届かない所に放置しない
③ 企業(組織)の情報資産を未対策のまま廃棄しない
④ 私物(私用)の機器類(パソコンや電子媒体)やプログラム等のデータを、許可なく企業(組織)に持ち込まない
⑤ 個人に割り当てられた権限を、許可なく他の人に貸与または譲渡しない
⑥ 業務上知り得た情報を、許可なく公言しない
⑦ 情報漏えいを起こしたら、自分で判断せずにまず報告

人の対策：情報漏えい対策基本項目①

企業(組織)の情報資産を許可なく持ち出さないとはどういうことでしょうか。

自宅などで業務（テレワーク）を実施するために、**勝手に**企業(組織)のパソコンや、業務情報が格納された電子媒体あるいは書類を持ち帰ることは禁止です。

個人情報漏えいの原因（2015年）



引用：
2015年情報セキュリティーインシデントに関する調査報告（速報版）
（日本ネットワークセキュリティ協会）

近年では、企業(組織)で情報資産を扱う上でのセキュリティーポリシーや管理手順を定めているものの「管理ルールがあるのにそれを守らせることができなかった」 場合に情報漏えいが発生しています。また管理者の目の行き届かない場面で情報資産を利用し、使用者の不注意が原因の盗難や紛失･置忘れも発生しています。リスクを回避するために、**よほどの理由がない限りは情報資産の持ち出しは避けましょう**。

持ち出しの許可を得た場合

安全が確認できない環境での情報資産の利用も注意が必要！

- **持ち出すパソコンには十分なセキュリティー対策が必要！**
  ＝使用するパソコンの設定や利用方法にも注意が必要です！
  - 社外のネットワーク（街中の無料Wi-Fiなど）に何もセキュリティー対策をせずに繋げることはしない。
  - パソコンにパスワードや暗号化の対策を行う。
- **持ち出すデータも暗号化！**
  - 万が一、データを格納したデバイス（パソコンやUSBメモリなど）を紛失や盗難にあっても、大切なデータをある程度、情報漏えい事故から保護できる。

人の対策：情報漏えい対策基本項目②

企業(組織)の情報資産を未対策のまま目の届かない所に放置しないとはどういうことでしょうか。

不特定多数の人たちの**目に触れる場所に、各種情報資産をさらさない**ようにしましょう。

やってはダメ！

- 業務上大切な書類を机の上に放置したまま席を離れる、または帰宅する
- 複合機やプリンターに出力した書類を、すぐに取りに行かない
- 起動中のパソコンを他の人が利用できる状態で席を離れる（パスワードによるロックをしない）
- 持ち運び可能なパソコンを机の上に放置して帰宅する
- 大切な情報が格納された電子媒体や書類を、鍵のかかるキャビネットなどにしまわない
- 個人宛の伝言メモを誰でも見えるところにおく

自分（1人の従業員）が気をつけていても、従業員全員が気をつけていないと情報漏えいが起きてしまいます。
重要な書類や電子媒体、持ち出しが可能なパソコンは、使わない時は鍵がかかるキャビネットなどに格納しましょう。
また、コワーキングスペースなどで業務を行っている際、一時席を離れる際は、起動中のパソコンにパスワードロックのできるスクリーンセーバーが動作するよう設定し、情報をのぞき見られることが無いようにしましょう。

持ち出しの許可を得た場合

安全が確認できない環境に情報資産を放置しないよう注意が必要！

- **情報が入ったカバンの保管場所にも注意が必要！**
  <危険な行為>
  - 情報の入ったカバンを電車の網棚に置いて居眠りをした…。
  - 情報の入ったカバンを持って居酒屋などに立ち寄った…。

→目を離した隙に情報資産（カバンの中身）を紛失・盗難・盗み見のリスクを回避。

人の対策：情報漏えい対策基本項目③

企業(組織)の情報資産を未対策のまま廃棄しないとはどういうことでしょうか。

重要な書類や電子媒体を、一般ごみと一緒にゴミ箱に捨てることは言語道断です。

やってはダメ！

- 業務で使用していたパソコンのハードディスクを消去せずに廃棄する
- 業務情報が記録された電子媒体や書類を、何の対策もせずにそのままゴミ箱に廃棄する

紙文書やCDは、物理的に情報を裁断することで他者が情報を読めなくすることができますが、パソコンや電子媒体に保存された情報は「ファイル削除」などの操作をしても、復元ツール等を用いて情報を取り出すことが可能です。重要情報の入ったパソコンや記憶媒体を廃棄する場合は、消去ソフトウェアを利用するなど、情報を確実に消去する措置が必要です。

情報資産を廃棄する場合

情報の形態に応じた正しい廃棄が必要！

- **書類やCD-Rなどはシュレッダーで裁断するか溶解処理！**
  ＝物理的に情報を裁断し、重要情報を他者が読めなくなるような処分が必要
- **パソコンや電子媒体は、消去ソフトや専門業者を利用！**
  ＝電子データを他者が読めなくなるような処分が必要
  - フロッピーディスクは分解して中身をはさみで切る。
  - USBメモリ等のフラッシュメモリ、パソコン用のHDDもファイルの削除では不十分！消去ソフトを使うか壊して捨てる。または専門業者に依頼する。
  - FAXやコピー機も要注意。捨てる時は専門業者に依頼する。
  - デジタルカメラ、携帯電話も要注意!!

人の対策：情報漏えい対策基本項目④-1

私物(私用)の機器類(パソコンや電子媒体)やプログラム等のデータを、許可なく企業(組織)に持ち込まないとはどういうことでしょうか。

自宅などで業務（テレワーク）を実施するために、**勝手に**私物パソコンや電子媒体を使用することは大変危険です。

やってはダメ！

- 私物のパソコンを持ち込んで、企業のネットワークに接続
- 業務に必要のない情報(データ)や業務に必要のない私物のプログラムを業務中に利用
- 業務と無関係のフリーウェアまたはシェアウェアプログラムをインターネットからダウンロード
- 業務に関係のないWEBサイトを業務用のパソコンで閲覧
- 業務で使用する電子メール(アドレス)を、私用で使用
- 情報を格納することのできるUSBメモリなどの電子媒体を持ち込んで、業務用のパソコンに接続

私物の情報機器を持ち込む危険性

持ち込んだ私物のパソコンやUSBメモリなどの外部記憶装置がウイルスに感染していた場合、そこから企業内の他のパソコンやサーバにウイルスを感染させる可能性があります。もしそのウイルスがスパイウェアであった場合は、業務情報などがインターネットを通じて流出する可能性が考えられます。

私物使用の許可を得た場合

BYOD（Bring Your Own Device）

BYODとは、従業員が私物の端末などを企業内に持ち込んで業務で利用すること。
私用のスマートフォンなどから企業の情報システムにアクセスし、必要な情報を閲覧したり入力したりすることなどを意味します。
コスト低減や効率向上のメリットもありますが、情報漏えいの危険性が増加するデメリットもあります。
そのため状況に応じ、企業（組織）が確認し必要ならば許可をする方針が多く取られています。
自分勝手なBYODはとても危険なため、絶対に行ってはいけません。

人の対策：情報漏えい対策基本項目④-2

私物(私用)の機器類(パソコンや電子媒体)やプログラム等のデータを、許可なく企業(組織)に持ち込まないとはどういうことでしょうか。

自宅などで業務（テレワーク）を実施するために、**勝手に**私物パソコンや電子媒体を使用することは大変危険です。

許可されていないプログラムの危険性

WEBサイトからダウンロードしたり、外から持ち込んだりしたプログラムそのものが、スパイウェアの可能性があります。基本的に業務に関係のないプログラムの利用はやめましょう。どうしても業務に必要な場合は、管理者の許可･管理のもとで利用しましょう。

許可されていないインターネット上のサービスを利用する危険性

- 企業(組織)の重要な情報を許可されていないネットワーク(オンライン)ストレージサービスを利用して保管
- 情報共有サービスを利用して情報管理

このような際、安易な設定や使い方で情報漏えいが起こる場合があります。インターネットサービスを利用する場合はサービスの仕組みや設定方法などをよく理解した上で、管理者の許可を受けてから利用しましょう。

WEBサイトの危険性

サイト上で指定された操作をするだけで、意図せず悪意のあるプログラムを実行させる悪意のあるWEBサイトも多く存在します。またウイルス・スパイウェア対策が十分に施された環境でも、対策ソフトが検知できないウイルスやスパイウェアも存在します。また近年では不特定多数ではなく、特定企業や個人を標的としたスパイウェアも出現しています。業務に関係のないWEBサイトの利用はやめましょう。

誤った操作で情報漏えいする危険性

- 持ち込んだ私物のパソコンやUSBメモリなどの外部記憶装置を利用する際に、不用意に大切な業務情報が格納され、意図せずに情報を持ち出してしまう可能性
- 電子メールを私用で使った際に、誤って大切な業務情報を流出させる可能性
- ブログや掲示板への不用意な書き込みから、無意識に、大切な業務情報を流出させる可能性

このような可能性があるため自身の行動にも注意が必要です。

人の対策：情報漏えい対策基本項目⑤

個人に割り当てられた権限を、許可なく他の人に貸与または譲渡しないとはどういうことでしょうか。

個人に割り当てられた権限は、企業から与えられた**職権と同様**です。

やってはダメ！

- 業務で使用する情報や機器に設定された利用者IDとパスワードを安易に貸し借りする行為
- 利用者IDやパスワードを忘れないために紙に記載して、誰でも見られる場所に放置する行為（例：ディスプレイに貼る）

企業では、業務で使用する情報や機器にも担当者ごとに利用者権限が与えられています。つまり、利用者IDごとに利用権限が定義されていて、利用者IDはパスワードまたは個人認証で保護されます。
これらの利用者IDやパスワードを共有したり、貸し借りしたりすることは、情報セキュリティー上、非常に大きな問題を引き起こす可能性があるので、絶対に行ってはいけません。

人の対策：情報漏えい対策基本項目⑥

業務上知り得た情報を、許可なく公言しないとはどういうことでしょうか。

「業務上知り得た情報を口外しない」とうことは守秘義務として、情報を取り扱う**社会人としての常識**です。

やってはダメ！

- ビルのエレベーターで、周りの人が聞こえる音量で仕事の話をする
- 使用しているパソコンにのぞき見防止のフィルターもせず、移動の新幹線や喫茶店で仕事をする
- 業務に関係ないブログや掲示板、SNSに自己紹介のつもりで仕事の話をアップする
- 会社にかかってきた電話に、業務担当者の情報（氏名や連絡先）などを伝える

守秘義務については、入社時に企業から教えられるものですが、長期勤務などの慣れもあり、いつの間にか忘れられる傾向にあります。ちょっとした気の緩みから情報漏えいを起こすことがあるので注意が必要です。
日頃の会話はもちろん「ショルダーハッキング」といわれる肩越しののぞき見行為にも注意しましょう。

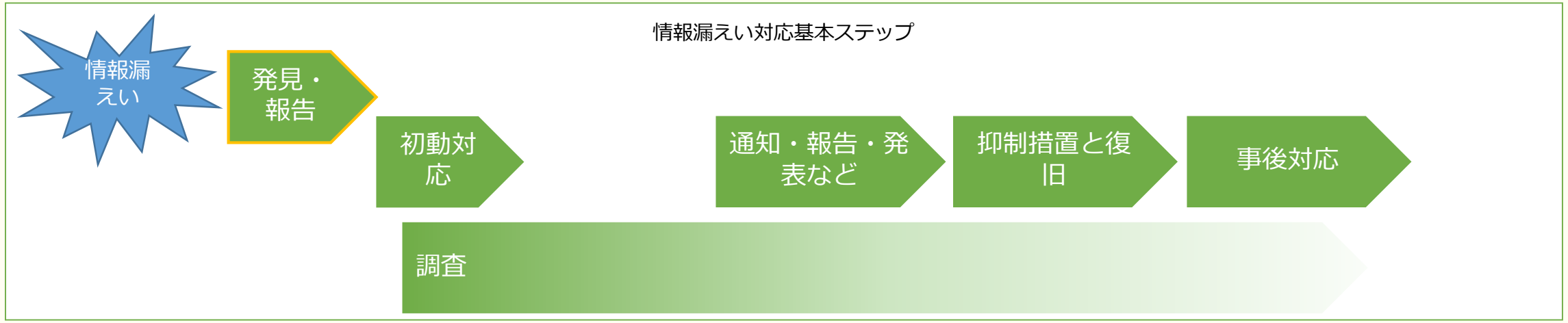
人の対策：情報漏えい対策基本項目⑦

情報漏えいを起こしたら、自分で判断せずにまず報告とはどういうことでしょうか。

何らかの誤りで情報漏えいを起こした場合や情報漏えいを発見した場合は、自分で何とかしようとする前に、**まず上司や管理者に報告**しましょう。

自社のことだけでなく、個人情報を漏えいされた最終的な被害者、顧客、取引先、株主、親会社、子会社、従業員など情報漏えいにより被害を受ける様々な関係者の被害を最小限に抑える必要があります。自社の経営方針に基づき全体のバランスを考えながら被害の最小化を図ることが重要です。
そのため情報漏えい発生時は、まず報告をして関連部門も交えて被害を最小限に抑える対策を取ることが重要です。

「情報漏えいによる直接的・間接的被害を最小限に抑える」



ICT活用の裏に潜む危険

テレワークは情報通信機器やインターネットを用いるため、注意すべき点があります。

テレワークでは、情報通信機器を活用しインターネットを通じて業務を行います。そのため、自分の業務の足回りとなる**インターネットや電子メールに様々な脅威が潜んでいることを十分理解したうえで、インターネットや情報通信機器を活用**しましょう。

インターネットに潜む脅威

- フリーソフトのインストール時や、インターネット閲覧時にスパイウェアに感染
- ページ内リンクをクリックしたことで架空請求が発生（ワンクリック詐欺）
- P2Pファイル交換ソフトによる情報漏えい

電子媒体に潜む脅威

- USBメモリを接続したことでマルウェアに感染

電子メールに潜む脅威

- 銀行など大手企業の名を語ったメールから偽サイトに誘導され個人情報流出（フィッシング詐欺）
- メールや添付ファイル開封時にマルウェアに感染
- 関係ないファイルを添付し送信したことで情報漏えい
- 宛先を間違えたことによる情報漏えい

インターネットに潜む危険①

様々な方法でマルウェアに感染してしまいます！

メールやWEBサイトにはマルウェアに感染させるワナがしかけられている可能性があります。マルウェアに感染すると、情報漏えいを促進したり、感染したパソコンを踏み台にして社内ネットワークに潜入したりします。**感染経路が多岐にわたることを認識し注意してインターネットを活用**しましょう。

様々な感染経路

メールからの感染

添付ファイルがウイルスに感染していたり、添付ファイル自体がウイルスだったことにより感染。

- メールなりすまし（差出人メールアドレスを詐称）
- 一見通常のファイルに見えるように添付ファイルの拡張子の名前を細工する
（二重拡張子を使用　例document.pdf.exe）

WEBサイトからの感染

マルウェアがしかけられたWEBサイトを閲覧したり、サイト内で指定された動作（リンクをクリックなど）をしたことで感染。

攻撃する際、攻撃先は大きく２種類ある。
- 標的が不特定多数の場合
- 標的は決まっている場合（水飲み場攻撃）

攻撃対象先によりマルウェアを仕掛けるサイトを分けている。

USBメモリからの感染

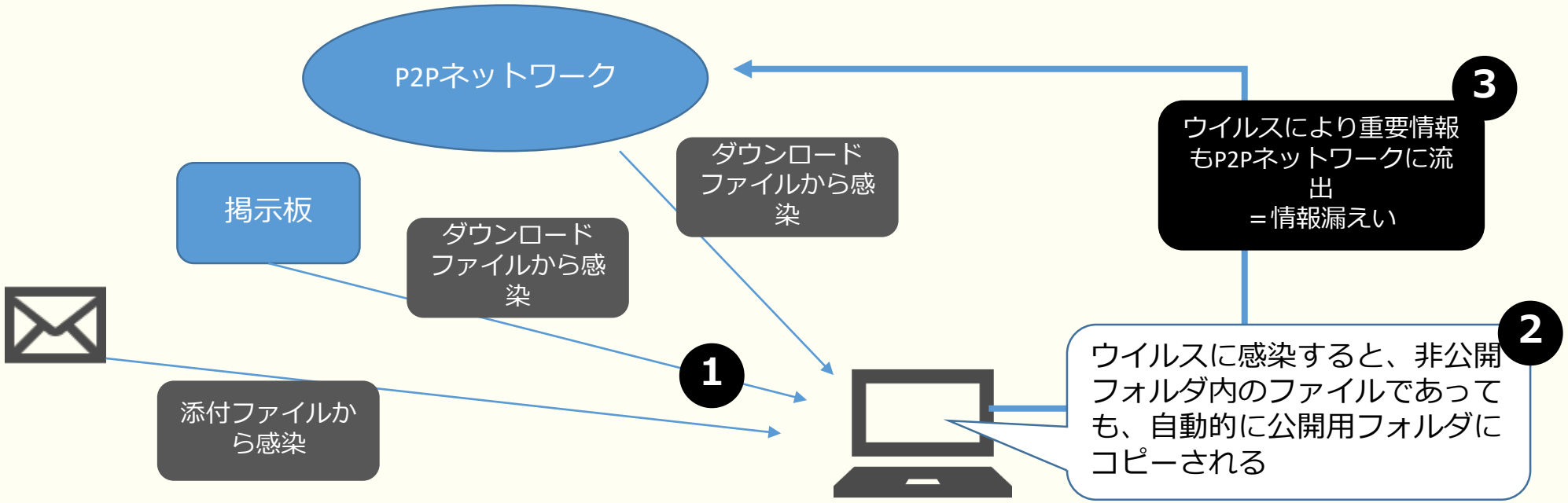
USBメモリを挿入するとファイルを自動再生する機能を悪用しUSBメモリからパソコンへ感染。（Windows XPやVistaの場合、設定なしに自動再生が行われます）
感染したパソコンに使用したUSBを媒介に他のパソコンへ感染が広がる。

補足）マルウェアとは：コンピュータウイルス、スパイウェア、ボットなどの不正なプログラムを指します。

インターネットに潜む危険②

P2Pファイル交換ソフトを利用したことによる情報漏えい事例です。

P2Pファイル交換ソフトは、情報が流出する危険性の高いソフトウェアと言われています。
業務で使うパソコンでP2Pファイル交換ソフトは絶対に利用してはいけません。



補足）P2Pファイル交換ソフトとは：インターネット上で、P2Pネットワーク内にある不特定多数のコンピュータ間でファイル(データ)をやり取りできるソフトウェア。自分のパソコン内で公開したいフォルダを設定し、そのフォルダ内のファイルを共有する。

インターネットに潜む危険③

インターネットの危険はマルウェアに感染する以外にも発生します。

情報漏えいは、マルウェアとは関係ない「自らの行い」によっても発生してしまいます。特に宛先などを間違えて送信してしまう**誤送信は絶対にあってはいけません**。

業務情報など社内情報だけでなく、宛先（お客様）の個人情報（組織名称やメールアドレス、氏名など）も重要な情報であり、決して情報を漏えいさせてはいけません。
どんなに気をつけていても、うっかりミスをおかしてしまうのが人間です。忙しくてつい…ということもありますが、日ごろから注意してメールを利用することが重要です。

メール誤送信の種類

- 宛先アドレスを手入力した際の打ち間違い
- アドレス帳からの誤選択
- BCC扱いに入れるべきところをTO扱いやCC扱い
- 流用したメールの宛先や本文を変更すべきところをそのまま送信
- 間違ったファイルを添付

メール誤送信の対策例

- メール送信後に送信トレイに留める設定にする（２段階送信）
  送信ボタンをクリックしてもメールはすぐに送信されず、送信トレイにメールが残る。「送受信アイコン」をクリックするなど再度指示をしないとメールは送信されない。
- メール送信後、設定した時間（例：1分後）まで送信されない設定にする

参考資料

- THE Telework GUIDEBOOK 企業のためのテレワーク導入・運用ガイドブック（国土交通省、総務省、厚生労働省、経済産業省）
- 「自宅でのテレワーク」という働き方（厚生労働省リーフレット）
- テレワークではじめる働き方改革（厚生労働省）
- 初めての情報セキュリティー対策のしおり（独立行政法人情報処理推進機構）
- 情報セキュリティー読本　四訂版（独立行政法人情報処理推進機構）
- 秘密情報の保護ハンドブック～企業価値向上に向けて～（経済産業省）
- 改正個人情報保護法の概要と 中小企業の実務への影響（経済産業省）
- 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（経済産業省）
- 情報漏えい対策のしおり　企業（組織）で働くあなたへ7つのポイント!!（独立行政法人情報処理推進機構）
- 企業（組織）おける最低限の情報セキュリティー対策のしおり（独立行政法人情報処理推進機構）
- 情報漏えい発生時の対応ポイント集　情報が漏えいしてしまった時、何をすべきか！！（独立行政法人情報処理推進機構）
- テレワークセキュリティガイドライン（第3版）（総務省）
- 情報通信機器を活用した在宅勤務の適切な導入及び実施のためのガイドライン（厚生労働省）


エコ・ペーパーレス協議会
テレ検
Since2016