【教育コンテンツ】

Orchestrating a brighter world NEC

池田糖化グループ

ICT使用基準

システム使用基準・外部サービス使用基準

２０１９年４月１日 第１版

はじめに

本研修の目的

当社では、処方・製造フロー・見積書など自社内の情報や、お客様からお預かりしているOEM情報・新商品情報・個人情報などを保有し、従業員はこれらの情報を業務に活用しています。

※「当社」とは「池田糖化グループ」をいう

これらの情報は、ICT（Information and Communication Technology）を活用することでいつでも利用できるため、迅速に効率よくビジネスをすすめることができます。

とても便利なICTですが、使い方を一歩誤ると、重要な業務情報が流出したり、ウイルスに感染したり、不正にシステムを使用されたりするリスクがあります。

本コースでは、業務におけるICT使用において想定されるさまざまなリスクを理解し、被害に合わないために従業員が何に気をつけなければならないのか、何をしなければならないのかを学んでいただきます。

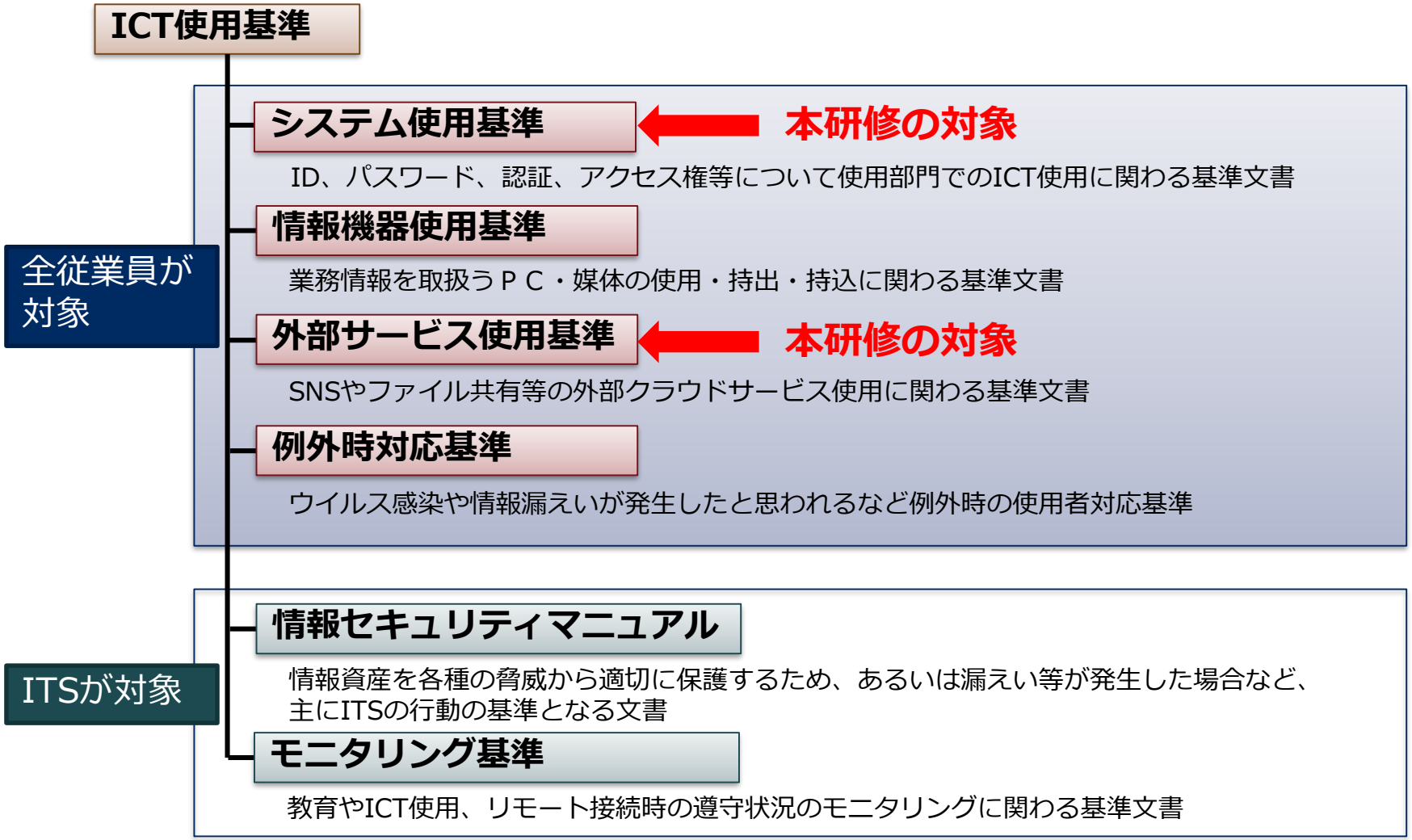
※本研修では学習の手助けのため、用語集を用意しております。以下のボタンをクリックしていただくと別ウィンドウで用語集のページが開きますので、必要に応じてご利用ください

用語集

ICT使用基準の構成

ICT使用基準は以下の複数の文書で構成されています。

- 本研修は「システム使用基準」について説明します。



目次

第1章　実際の事件・事故

この章では、実際に起きた不適切なアカウントの取り扱いに起因するセキュリティ事件・事故を取り上げ、解説します。

「自分の身にも起こるかもしれない」

ということを意識して学習してください。

用語チェック　PC/スマートデバイス/モバイルデバイス

スマートデバイス

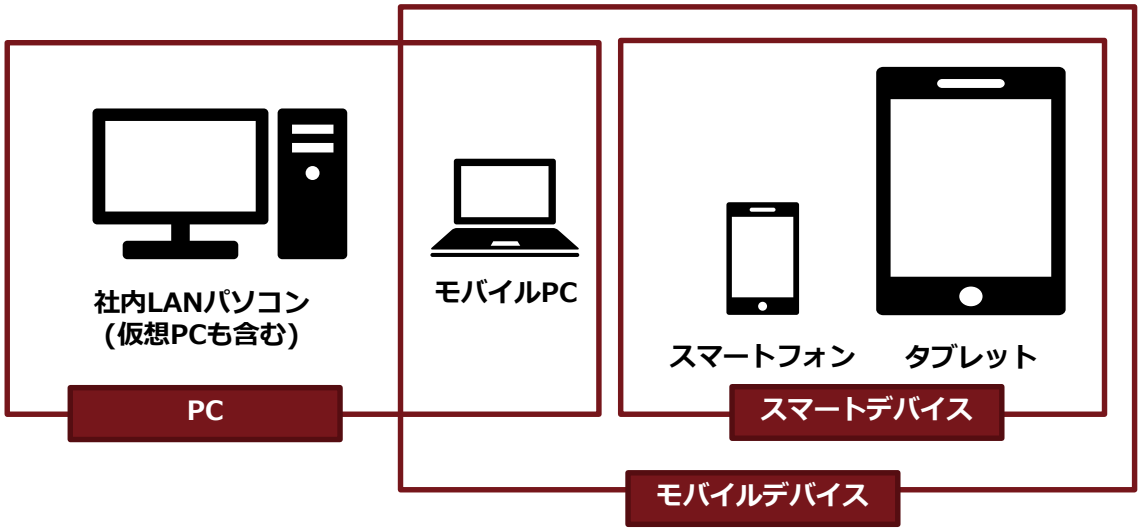
- iPhone のようなスマートフォンや iPad のようなタブレットを総称した呼び名。

モバイルデバイス

- スマートデバイスとモバイルPCを合わせてモバイルデバイスと呼ぶ。

PC

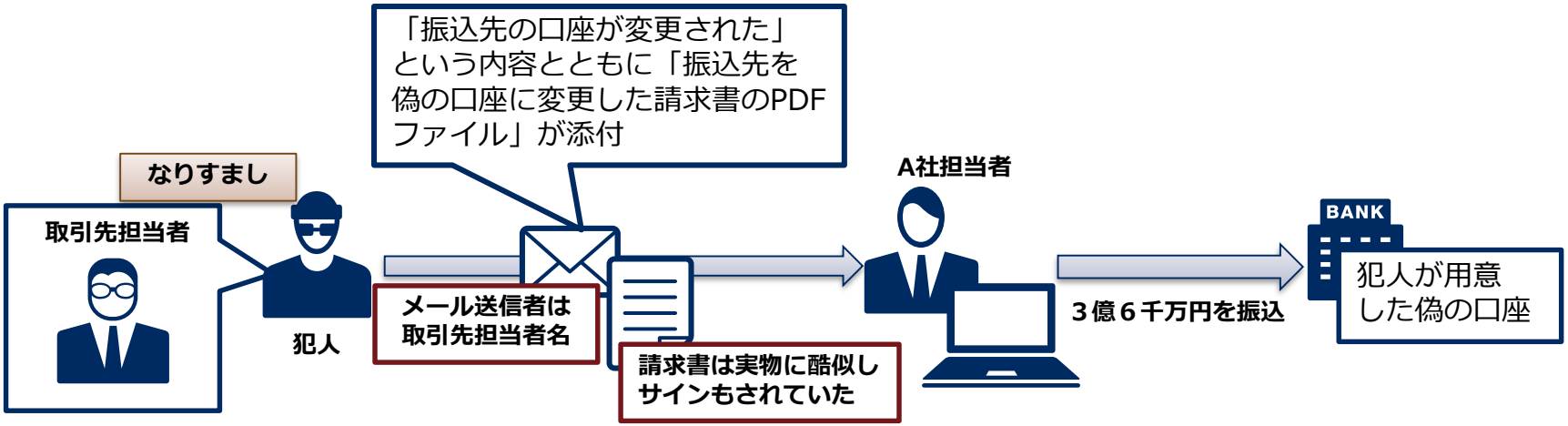
- 社内LANパソコン(仮想PCも含む)とモバイルPCの総称



1.1 ビジネスメール詐欺～3億8千万円を振り込まされる

事件の経緯

- A社が海外の金融会社からリースしている旅客機の料金に関するメールを担当者が受信。
  - メールには、「料金の振込先の口座が香港の銀行に変更された」という内容とともに、先に送付されていた**正規の請求書の訂正版として**「**振込先を偽の口座に変更した請求書**のPDFファイル」が添付されていた。
- A社担当者が偽の口座に約3億6000万円を振り込んでしまった。



- 米国にあるA社貨物事業所でも似た手口のなりすましメールが届き、約2400万円をだまし取られた。

2回騙され、トータル約3億8千万円が騙し取られた

1.2 クラウドメールサービスの認証情報を狙ったフィッシング

法人が利用するクラウドメールサービスの認証情報をフィッシングにより搾取される被害が2018年4月から6月にかけ、9件公表される

- 外部に転送するよう設定変更された
- 迷惑メールの送信に悪用された

某大学のケース

- 教職員および学生に対し、大学で利用しているクラウドメールサービスのログイン画面に似せた偽のサイトに誘導するフィッシングメールが届く
  - 経緯
    - 1,037のメールアドレス宛に送付された
    - 教職員等29名が偽のサイトにアクセス
    - 不正に外部に転送するよう設定を変更された
    - 5/23にフィッシングメールの存在を検知
    - 5/28に一人の教員のメールが転送されていることが発覚
  - 被害
    - 29のメールアドレスに5/15～5/30に届いたメール3,512通が外部に転送され、個人情報等が流出した

1.2.1 認証情報漏えい後に生じる問題

認証情報が漏洩すると…

- 漏れたアカウントになりすまされる
  - 漏れたアカウントに与えられている権限でシステムの利用が可能
    - このケースでは、迷惑メールの送信に利用された
    - 閲覧可能な情報の漏えい（組織内の機密情報など）
  - 前述の「ビジネスメール詐欺」に悪用される
- 漏れた認証情報がパスワードリスト攻撃に利用される

  →詳細は「 1.3 パスワードの使い回しは危険」で解説
- ログインされることで、そのアカウントの個人情報が漏えいする
  - **お客様に損害が発生する**
    - お客様に迷惑がかかる
  - 個人情報が他の犯罪に用いられる
    - オレオレ詐欺
    - ダイレクトメール
    - フィッシング詐欺
    - 訪問販売
    - 電話による勧誘
    - ソーシャルエンジニアリング
  - 被害者に対する賠償が発生する
    - お詫びにもコストがかかる
    - 訴訟コスト
    - 損害賠償コスト

参考：個人情報漏洩時の費用（1/2）

個人情報漏洩時の費用

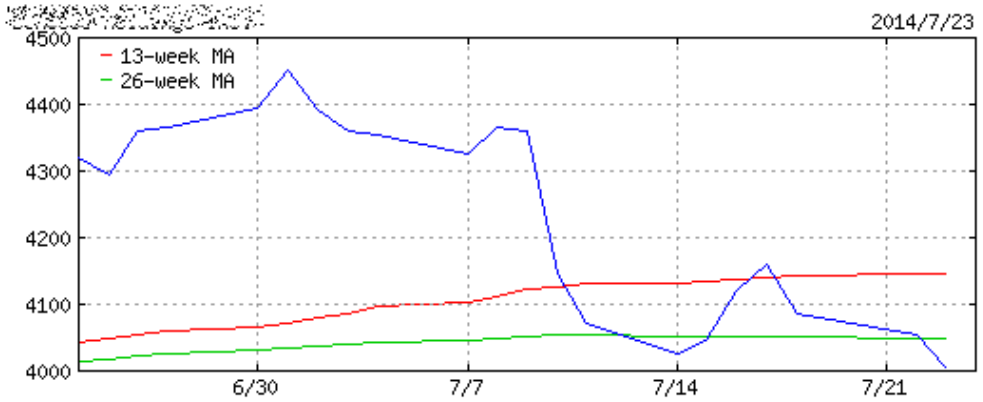
- お詫びの品

時期	概要	お詫びの品	
2004年	某プロバイダが452万人分の個人情報を漏えい	金券500円	**約22億円**
2007年	某印刷会社が委託先の会員情報863万人分を漏えい	金券500円	**約43億円**
2009年	某証券会社が会員情報49000人分を漏えい	金券10000円	**約5億円**
2015年	某テーマパーク運営会社が株主6249人分の個人情報を漏えい	金券1000円	**約630万円**
2014年	某通信教育会社が顧客情報2895万人分を漏えい	金券500円	**約145億円**

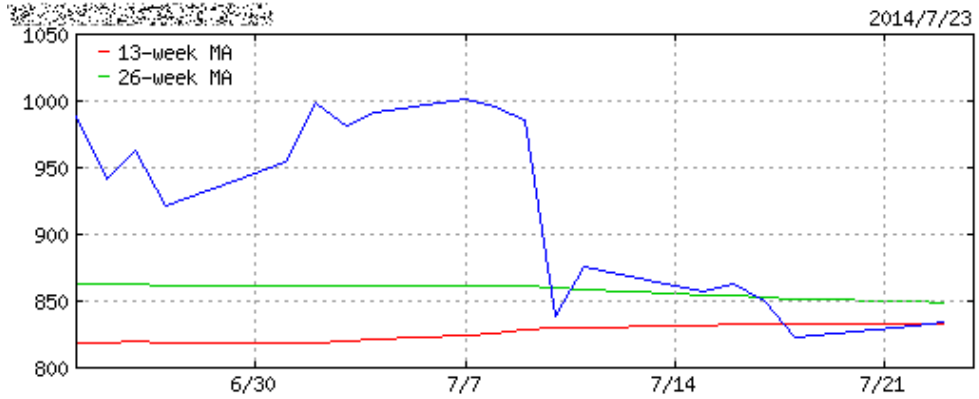
- お詫びの品送付等に伴う費用
  - 某通信教育会社のケースでは金券合わせ200億円とも言われる
    - 事件が発覚した四半期の特損は260億円（問い合わせ対応や調査・情報セキュリティ対策等）
- 損害賠償
  - 基礎的な情報が漏れた場合
    - 某自治体で氏名、住所、電話番号、生年月日が漏れたケース　→　慰謝料1万円＋弁護士費用5000円
  - プライバシー度が高い情報が漏れると高額
    - 某エステティック会社のケース　→　原告13名に一人あたり慰謝料3万円と弁護士費用5000円
1名については2万2000円プラス遅延損害金

参考：個人情報漏洩時の費用（2/2）

- 株価暴落



漏えいした某通信教育会社の株価



漏えいした情報を名簿業者から購入し
DMを送付した別の通信教育会社の株価

- 間接的な損失も
  - 会員の退会等、得意先や顧客の減少
  - 指名停止等ビジネスへの影響
  - 企業イメージ低下による売上損失

1.3 パスワードの使い回しは危険（1/2）

パスワードリスト攻撃（アカウントリスティング攻撃）

- 2018年8月　某クレジットカード会社が提供するWebサービスにおいて、945名のアカウントに対し、本人以外の第三者による不正ログインが発生、会員情報が閲覧された可能性があることがわかった。
  - ログインの試行回数と成功回数の割合から、攻撃者が何らかの方法で入手したアカウント情報を用いる「パスワードリスト攻撃」だったと説明。同社経由の情報流出について否定した。

当てずっぽうでログインを
試みても通常は成功しない

よそで流出したIDとパスワードのリストを用いて
ログインを試みた場合、成功率が飛躍的に高まる

ID	Password
taro	taro0401
hanako	H-123Abc
…	…
…	…
…	…

- 2018年8月　某電力会社会員サービスにおいて不正ログインが発生、会員149名分、合わせて12万7430ポイントが不正に交換された。
  - 同社は、不正ログインに使用されたIDとパスワードは外部で入手されたものと説明している。

1.3 パスワードの使い回しは危険（2/2）

パスワードを使い回すと…

- 他のシステムからIDやパスワードが漏えいした後、その情報を攻撃者が悪用する可能性がある
- 不正ログインの成功率が高い

IDやパスワードを異なるシステムで使い回してはいけない

パスワードを含むID情報が漏えいすると……

- そのIDの権限でシステムが悪用される

パスワードを含むID情報は、悪用されないように社内ルールに基づき適切な管理を徹底する必要があります。

1.4 大規模な被害を引き起こしたランサムウェア「WannaCry」

症状

- 感染したコンピュータではファイルが暗号化されて使えなくなる。また、画面上に身代金（300ドル相当のビットコイン）を支払うよう指示する画面が現れる。
- Windows OSを悪用し、**ネットワークに接続されている社内LANパソコン**に感染拡大を試みる。

被害

- １５０の国や地域で合わせて２０万件以上
- 英国（医療機関、自動車工場）、ロシア（政府省庁）、スペイン（通信事業者）、フランス（自動車会社）、アメリカ（物流業者）などが被害を受けたとニュース報道あり

感染した場合に表示される画面の一例
出典：世界中で感染が拡大中のランサムウェアに悪用されているMicrosoft製品の脆弱性対策について（2017年5月18日 IPA）

1.4.1 ランサムウェアとは

ランサムウェアとは

- 感染した PC内のデータを暗号化することで使用不能にしたうえで、**「データを人質」**に、復号と引き換えに**「身代金」を要求する**マルウェア
- ネットワークドライブが暗号化されると被害が甚大
- 他にも、画面をロックすることで操作不能にすることで**「感染端末自体を人質」**にするタイプもある
- 「身代金要求型マルウェア」とも呼ばれる

使用しているPCがランサムウェアに感染したら…

- HDD上のファイルがすべて使えなくなります
- 共有ドライブのファイルも暗号化されてしまい使えなくなります

元に戻すために身代金を支払いますか？

ランサムウェアはファイルを暗号化した後、身代金要求の画面を表示する

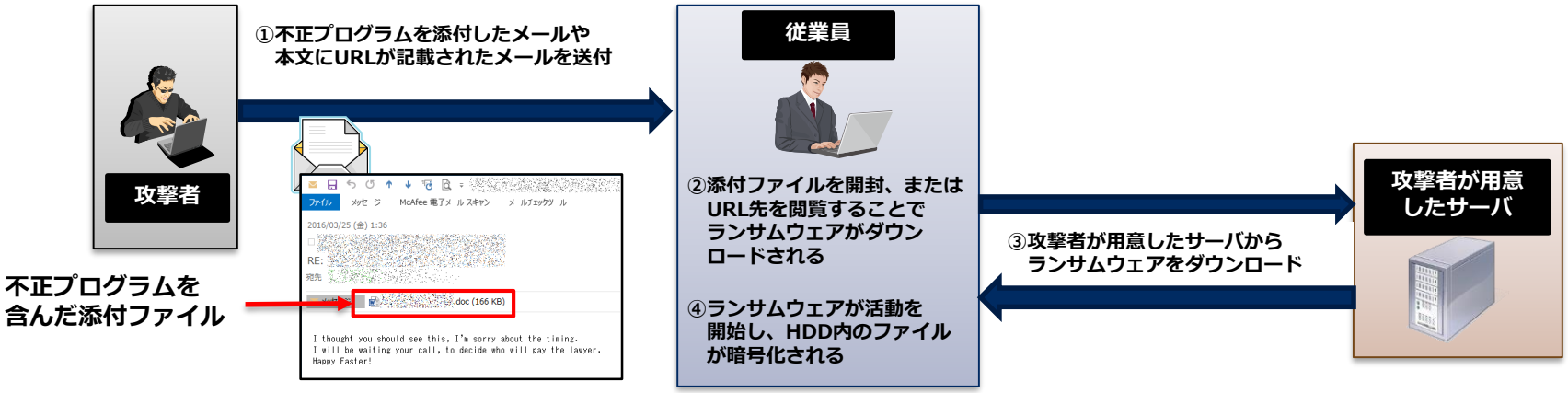
攻撃者に身代金を支払うと暗号化を解除するために必要なツールがダウンロード可能になる

ただし、身代金を支払ったからといって必ずファイルが元に戻るわけではない

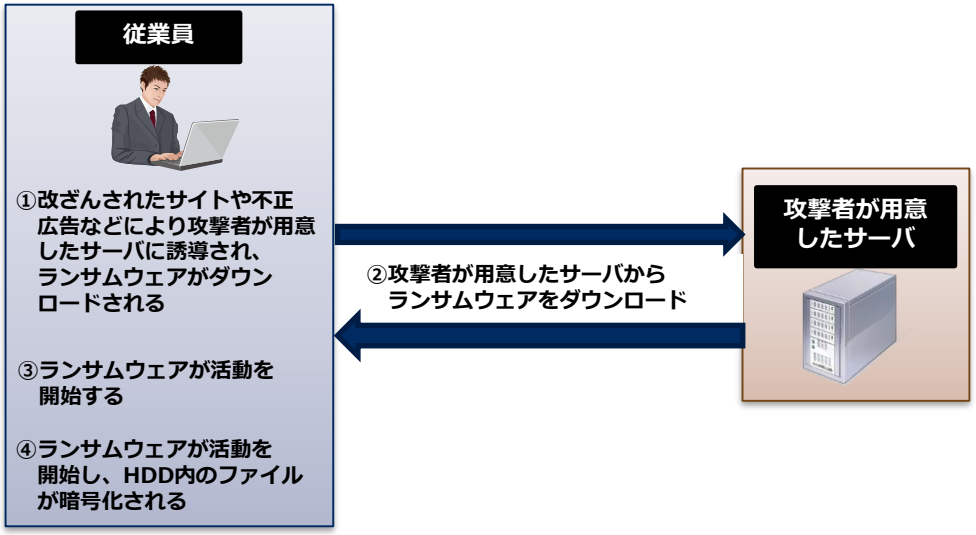
1.4.2 ランサムウェアの侵入経路

主な侵入経路はメールとWebアクセス

- メール経由の例



- Webアクセス経由の例



※説明のため、仕組みを簡略化しています

1.4.3 ランサムウェア対策

以下の2点が重要

- ランサムウェアに感染しないこと
- 万が一感染し暗号化されたとしても、元に戻せるように定期的にバックアップを取るようにすること

ランサムウェアに感染しないためには

- **不審なメールの添付ファイルは開かない**
- **メールやSNSなどに記載されているURLに不用意にアクセスしない**
- **OSやアプリケーションを常に最新の状態に保つ**
- セキュリティソフトを導入し、定義ファイルを常に最新にする
- 共有資源のアクセス権を必要最低限にとどめる
- ランサムウェア対策ソリューションの導入

データを元に戻せるようにするためには

- **定期的にバックアップ**を行う

第2章　システム使用基準

当社では業務で様々なシステムを使用します。これらシステムは、使い方を誤ると情報漏えいやウイルス感染、不正アクセスなどを引き起こすきっかけになりかねません。そのため、当社ではシステムの使用にあたって、ID、パスワード、認証、アクセス権等についてルールを定め、事件事故につながらないように配慮しています。

この章ではそのルールである「システム使用基準」について解説します。

2.1 本文書の目的

本文書は、当社従業員が業務において社内システム等を使用する際に必要なID、パスワード、認証、アクセス権等におけるルールを「遵守事項」としてまとめたものである。

以下のような場面において、当社が定めた遵守事項があるので、各自内容を理解し、システム使用時に実践すること。また、システム使用にあたってはID申請を行うこと。

- 情報機器使用のためのID申請に関する遵守事項
- 社内システム等のID管理についての遵守事項
- ソフトウェアの使用・導入についての遵守事項
- インターネット使用時の遵守事項
- ブラウザ使用時の遵守事項
- 社外メール使用時の遵守事項
- 重要情報（電子データ）の取扱に関する遵守事項

2.2 情報機器使用のためのID申請に関する遵守事項

IDが必要な業務について

- 以下の社内システム等の使用にあたっては、IDが必要である
  - PCの使用
  - モバイルPC・スマートデバイスの使用
  - サイボウズ（共有メール・Kintoneを含む）
  - 電子メール
  - ホストシステム
  - ITS情報サービス
  - Quebel-i
  - IISシステム・在庫管理システム
  - 人事システム（SMILE)
  - 会計システム（MJS)

  ※上記は代表的なシステムで他にもID申請が必要になるシステムがあります

IDの取得には申請が必要

- 「誓約書」を提出し、所属長の承認後、ITSへ提出すること。
- 「システム使用申請書」を提出し、所属長の承認後、ITSへ提出すること。

IDが悪用されると、社外に重要情報が漏れたり、不正に操作されたりする可能性があるため、IDおよびパスワードは大切に管理することが重要

具体的な遵守事項は次ページ以降

2.3 社内システム等のID管理についての遵守事項

ID、パスワードは適切に管理しなければならない

- 取得したIDおよびパスワードはその**使用者が管理する**必要がある
- ID使用者は原則として**本人だけが知っているパスワードを使用する**

  ※一部パスワードが管理者から与えられるものもあり、その場合は管理者もパスワードを知っている

  - パスワードは**他人に教えてはならない**
  - パスワードは**第三者の目に触れる場所に掲示してはならない**
    - 付箋紙に記述しディスプレイに貼る等
- 異動・退職時は、必ず、所属長に確認の上ITSに連絡すること

2.3.1 パスワードのルール

パスワードは、以下に示す考え方に基づき設定することを推奨する。
（ただし、システムによってはこのような設定が使用できないものもある。）

- パスワードの文字列はシステムで最低文字数が決められているが、8文字以上を推奨する
- パスワードの文字列は使用するシステムで設定可能な文字種（英大文字、英小文字、数字、記号）のすべてを組み合わせること
- 単純なパスワードは類推される可能性があるので使用しないこと
  - 名前、生年月日、製品名、会社名、家族の名前、電話番号、**社員番号、**車のナンバー、キーボードの配列順等あるいはこれらの組み合わせ
    - 悪い例　Taro0104（1/4生まれの太郎さんの場合）、nec2018、cybozulive、qwertyui、1qazxsw2
    - **社員番号をスマートフォンのパスコードとして設定しないこと。**
    - IDと同じ文字列をパスワードとして設定しないこと。
- 短いパスワードは短時間で破られる可能性があるので使用しないこと
- 異なるシステムで同じパスワードを使い回さないこと
  - パスワードリスト攻撃

良いパスワードの例
#t2TKjWcMJtv　　3isW_pR8seP9

2.4 ソフトウェアの使用・導入についての遵守事項

以下のようなリスクがあることを理解した上で使用すること

- 不正なソフトウェア（アプリ）や脆弱性のあるソフトウェア（アプリ）を誤ってインストールしてしまい、脆弱性を突いた攻撃を受ける可能性がある
  - 使用者が自由にソフトウェア（アプリ）をインストールできると……
    - トロイの木馬と呼ばれる不正なマルウェアが組み込まれたソフトウェア（アプリ）を誤ってインストールしてしまうといった被害が実際に発生している
- ライセンス違反
  - 市販製品やシェアウェアはもちろんのこと、フリーソフトにもライセンスが設定されている場合があるので注意する
  - 会社で購入したソフトウェアを自宅PCにインストールしてはならない

具体的な遵守事項は次ページ以降

2.4.1 ソフトウェア使用における制限

当社では、ソフトウェアのインストール権限を制限している

- 従業員が使用するIDでは、ソフトウェアのインストールができないように制限をしている
  - ソフトウェアをインストールしたい場合は、「ITSへの依頼書」を使用し、インストールを依頼すること

当社では、使用可能なソフトウェアを制限している

- 許可されたソフトウェア以外のインストールを禁止している
  - 許可されたソフトウェアは、マルウェアなどが混入していないことを確認したり、新たな脆弱性が発見されていないかベンダーの情報をチェックしたり、万が一脆弱性が見つかったら修正方法を皆さんにお知らせしたりする対象となっている。
  - 許可されたソフトウェアでも、使い方によっては問題を引き起こす場合があるので、一部のソフトウェアは**条件付きで使用可**としている。使用時には条件を確認すること。
  - 使用したいソフトウェアがある場合は、ITSに申請し、許可を得る必要がある。

2.5 インターネット使用時の遵守事項

インターネットに接続すること自体がリスクであることを理解すること

- インターネットは便利な半面、ウイルス感染、不正アクセス等の脅威にさらされる可能性がある
- 使用しないわけにはいかないので、以下原則を意識し、リスクがあることを意識して使用する

業務以外の目的で使用しない

具体的な遵守事項は次ページ以降

2.5.1 業務に関係のないサイトの使用の制限

- 電子メールやWebサイト閲覧等のインターネット使用において、**業務目的以外の使用を禁止**する
- 業務上閲覧が必要なWebサイトがフィルタリングで閲覧できない場合には、個別にITSに確認すること

当社では一部のWebサイトに対し、閲覧自体ができないようフィルタリングをおこなっている。

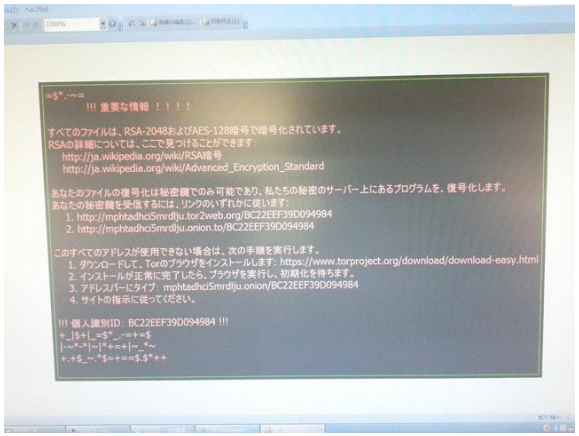
上のような画面が表示された場合、**該当するWebサイトを閲覧しようとしたことが記録される**。また、状況によっては、調査にご協力いただくこともある。

また、業務上、閲覧が必要な場合はITSに相談すること。業務上必要であることが確認できれば、フィルタリングの対象から外すことが可能である。

2.5.2 危険を感じたら、速やかにネットワークを切断する（1/3）

危険を感じたら、速やかにネットワークを切断すること

不審な画面が表示された



実際に社内で発生したランサムウェアの画面

ウイルス対策ソフトが警告を発した

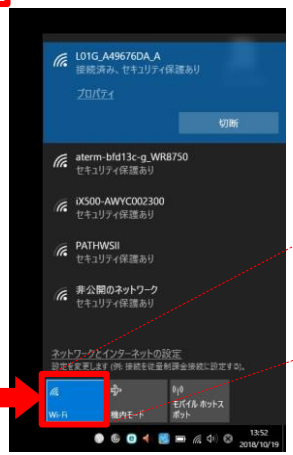
少しでも危険を感じたら、ネットワークから切り離す

2.5.2 危険を感じたら、速やかにネットワークを切断する（2/3）

PCの場合のネットワーク切断手順

- 有線の場合は**抜線後、すぐにITSに報告**すること。
- 無線（Wi-Fi）の場合は下記手順に従い、**ネットワークから切り離した後、すぐにITSに報告**すること。

①タスクバー上のアイコンをクリックする



②Wi-Fiをクリックする

③Wi-Fiが無効になれば切り離し完了

2.5.2 危険を感じたら、速やかにネットワークを切断する（3/3）

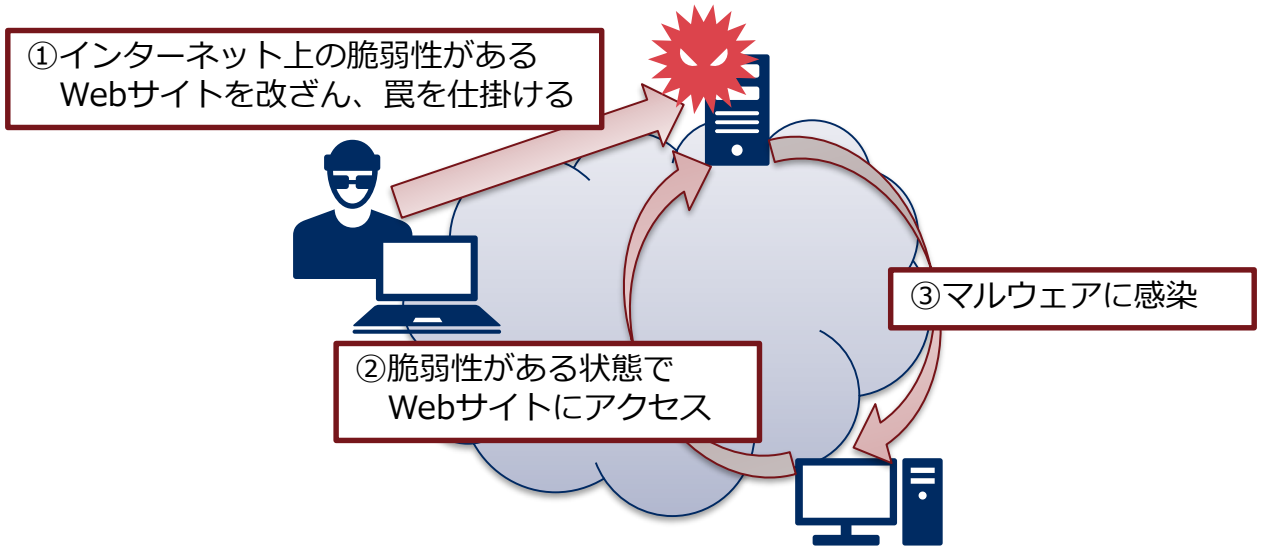
スマートデバイスの場合

- **通信事業者が提供する通信（モバイル通信）および無線通信機能（Wi-Fi、Bluetooth）をオフにする**
  - iOSの仕様変更により、**「機内モード」にしてもWi-FiやBluetoothがオンになることがある**ため、「機内モード」への変更ではなく、以下の手順を行うこと。

2.6 ブラウザ使用時の遵守事項

以下のようなリスクがあることを理解した上で使用すること

- 罠が仕掛けられているWebサイトにアクセスしただけでマルウェアに感染したり、PCを乗っ取られたりする可能性がある。
  - 特に脆弱性があるバージョンのブラウザを使用している際はリスクが高い
  - 設定が不適切な場合もリスクが高い



具体的な遵守事項は次ページ以降

2.6.1 使用ブラウザの制限と設定

使用するブラウザは、**ITSが使用を許可したブラウザのみ**とする

- 使用を許可したブラウザは以下
  - Internet Explorer Ver11
  - Chrome
  - Firefox
- 使用するブラウザは**ITSが指定しているバージョン**を使用すること

使用する**ブラウザの設定は勝手に変更してはならない**

- ITSから設定変更の指示があった場合は、速やかに指示に従い変更すること。

2.7 社外メール使用時の遵守事項

以下のようなリスクがあることを理解した上で使用すること

- うっかりミスが情報漏えいにつながりかねないこと
  - メール誤送信
    - メールの宛先を間違えることで、機密情報などが漏れる。
    - 不特定多数にメールする際、誤ってTOやCCにメールアドレスを入れてしまうことで、メールアドレスが漏えいする。
- 添付ファイルにおける注意
  - Excelファイルの場合、非表示列に機密情報が含まれたまま送付してしまった事例があるため、注意すること
    - 例えば、いったんPDFファイルに変更後、内容を確認し送付するなどの対策を行う
- メールには盗み見されるリスクがあること
  - メールは通常暗号化されないため、ネットワークを盗聴されると、メールの中身も盗み見される。
- さまざまな攻撃がメールを介して行われること
  - マルウェアの感染
    - メールの添付ファイルにマルウェアを潜ませ、添付ファイルを開くことでマルウェアに感染させるなどする。あるいは、メール内に記載したURLにアクセスすることでマルウェアに感染させるなどする。
  - 標的型攻撃
    - 特定の組織、個人を対象とした攻撃。主にメールを用いて攻撃する。
  - ビジネスメール詐欺
    - 経営幹部や取引先の実在する人物などになりすまして送金指示メールを従業員に送りつけ、用意した口座に送金させるなどする。
  - フィッシング詐欺
    - メール内に記載したURLにアクセスさせ、偽のログイン画面等を表示し、認証情報などを詐取する。

具体的な遵守事項は次ページ以降

2.7.1 誤送信防止のための確認

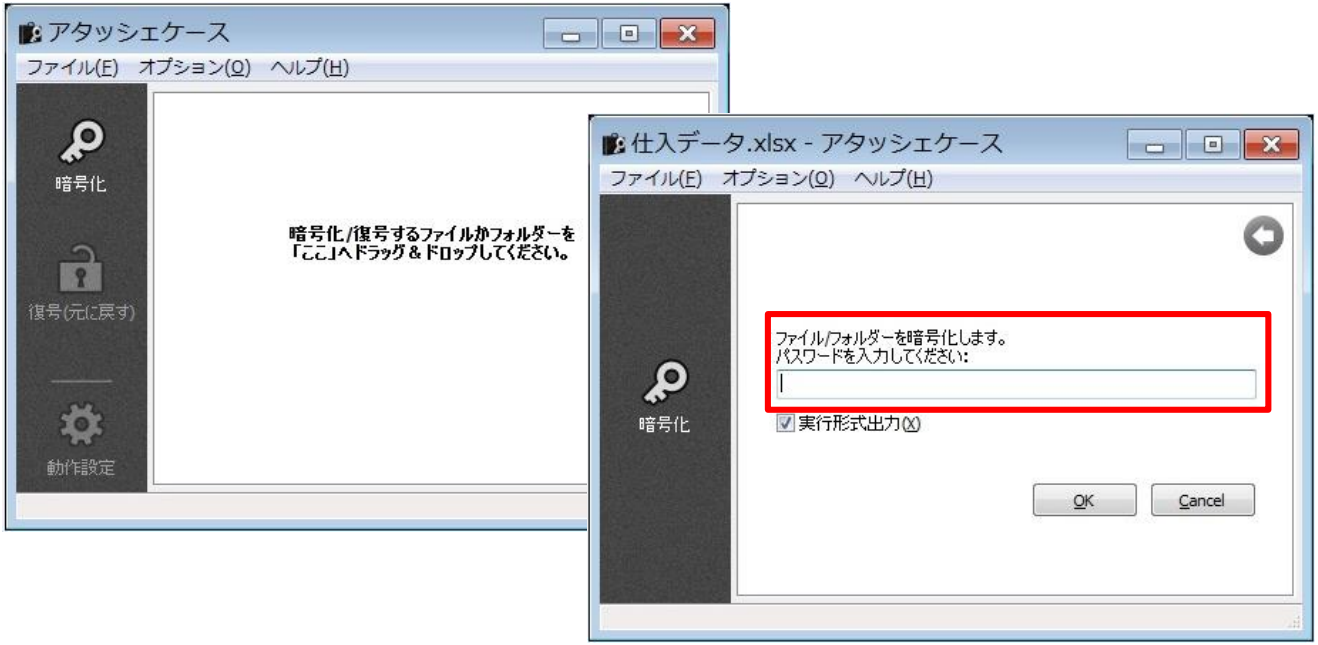
重要情報を電子メールにて送信する場合、**送信先のメールアドレスに間違いがないか確認の上**、送信すること

- 「To」「Cc」「Bcc」に入力した宛先は適切か？
- メールアドレスに入力ミスはないか？
- ダイレクトメールなど不特定多数に電子メールを送信する場合、TOやCCに入れず、BCCに入れているか？

2.7.2 メールの盗み見対策　機密情報送信時の処置

重要情報や個人情報などの機密情報をメールにて送受信する場合は、以下ルールに従い送受信すること

- 機密情報を**本文に記載せず**、添付ファイル内に記載する。
- 添付ファイルは、**当社指定の圧縮ソフトを用いるか、Officeファイルであれば Officeの機能を用い、適切なパスワードを設定し暗号化**すること。
  - 適切なパスワードに関しては、「2.5 ID・パスワード使用に関する遵守事項」を参考に設定すること。
- 暗号化の**パスワードは、電子メール以外の安全な別の手段**を用いて相手と共有すること。



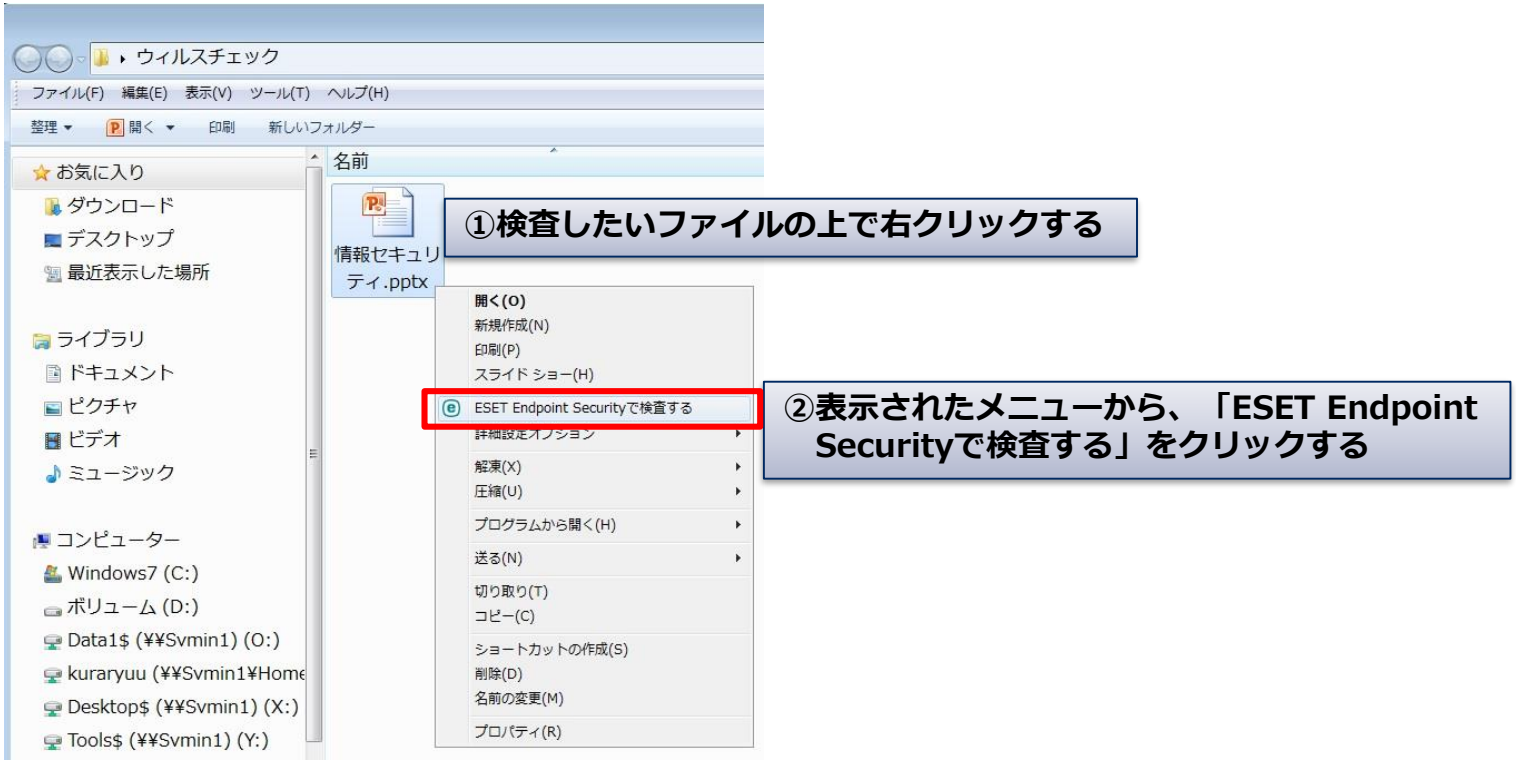
アタッシェケースによるパスワード設定例

2.7.3 メール使用時のウイルス対策（1/2）

メールを介したマルウェアの感染は、適切にウイルス対策を実施することである程度防げる

- 「情報機器使用基準」の「2.2.5マルウェア対策」に従い、適切にウイルス対策ソフトを使用すること。

- 添付ファイル送信時の注意事項
  - 電子メールで添付ファイルを送信する時は、必ずウイルス対策ソフトにより検査を行い、マルウェアに感染していないことを確認した上で送信すること。



2.7.3 メール使用時のウイルス対策（2/2）

- 添付ファイル受信時の注意事項
  - 電子メールで添付ファイルを受信した時は、サーバに保存する前に、以下を参考に自分のPC上でウイルスチェックを行うこと。
    - デスクトップ上の「ウイルスチェックフォルダ」に保存後、ウイルスチェックを実施した上でサーバに移動させるなどし、添付ファイルを使用して必要な業務を行うこと。

①添付ファイルをデスクトップの「ウイルスチェック」フォルダに保存

②表示されたメニューから、「ESET Endpoint Securityで検査する」をクリックする

  - 業務終了後も添付ファイルを保存する必要がある場合は、ネットワーク上の自分専用もしくは部門用のサーバにコピーして、ウイルスチェックフォルダ内に保存している添付ファイルを削除すること。

標的型攻撃では未知のマルウェアが使用されることがある

- **ウイルス対策ソフトでは検知できない**マルウェアも存在するため、業務に必要ではないファイルは原則開かないこと。

2.7.4 不審なメールに対する処置（1/2）

基本的な対応

- 以下のような**不審な兆候があるメールの添付ファイル、文中のURLは安易に開いたり、クリックしたりしない**こと。
  - 覚えのない相手やフリーのメールアドレスからのメール
  - 文面の日本語がおかしい
  - 文字化けしている
- 不審な兆候があるメールを受信した場合は、ITSに連絡すること。
  - メールの削除はITSから削除指示があった場合に実施する。
- 広告メールやスパムメールを受信した場合は、これを転送しないこと。

手口が巧妙な場合は上記「不審な兆候」がないケースもあるので注意すること

ビジネスメール詐欺やフィッシング詐欺メールによる手口が巧妙化しており、見破りにくくなっている

- メール文面、添付ファイル、やり取り等に不審な点が見つからないこともあることを常に意識しておく
  - 正しい日本語
  - 適切に見える送信元
  - 何回かやり取りをしており、その間不審な兆候がない
  - 適切に見えるリンク先（HTMLメールを使用することで、実際のリンク先を偽装）

2.7.4 不審なメールに対する処置（2/2）

ビジネスメール詐欺やフィッシング詐欺対策

- メールの真正性の確認
  - メールアドレスの偽装に注意する
    - 特にドメイン名（@マーク以降）の偽装
- 請求書等重要な内容についてはメール以外の方法で事実確認する
  - 直接電話する
- メールの盗み見防止
  - OS・アプリケーションを最新に保つ
  - メールアカウントや認証情報の適切な管理（不正ログイン防止）
- 業務目的外でのメールの使用制限
- メール本文のURLが正規のものかどうか分からない場合はクリックしない

2.8 重要情報（電子データ）の取扱に関する遵守事項

以下のようなリスクがあることを理解した上で使用すること

- 重要情報が漏えいすると損害賠償請求を受けたり、会社の信頼の低下、社会的評価の低下など大きな影響を及ぼす可能性がある

具体的な遵守事項は次ページ以降

2.8.1 対象となる重要情報（電子データ）と秘密区分表示

重要情報（電子データ）とは以下を指す

- レシピ情報
- 個人情報

重要情報（電子データ）には秘密区分を表示しなければならない

- 秘密区分の種類
  - 社外秘
  - 部外秘
  - 関係者外秘
  - コピー厳禁
  - 持出厳禁
  - 保存禁止
- ファイル名、表紙に区分がわかるようにすること
  - 例
    - 【コピー厳禁】○○レシピ情報.xls

2.8.2 重要情報（電子データ）の管理（1/2）

重要情報（電子データ）は入手～利用～保管～廃棄等の一連の流れにおいて、常に適切に管理しなければならない

- 入手時の遵守事項
  - 入手時には安全な方法で入手すること
    - データを取引先と合意した方法で暗号化した上で許可されたUSBメモリあるいは新品のディスクメディア（DVD-R等）にコピーし、手渡しでUSBメモリあるいは新品のディスクメディアを受け取る
    - 「2.3.2 メールの盗み見対策　機密情報送信時の処置」に従い、電子メールにより入手する
- 入手後の取扱における遵守事項
  - 扱う情報の重要度・アクセス可能範囲を意識して、意図しない範囲に共有・漏洩しないよう適切な管理を行うこと
  - 入手した重要情報（電子データ）は、適切なアクセス制限が施された共有サーバ上およびクラウドシステム上にのみ保管すること
    - 許可なくコピー、持ち出ししないこと
    - 適宜バックアップを取得すること（※共有サーバ上はシステムでバックアップされるため除外）
  - 目的外使用の禁止
- 移送、送信時の遵守事項
  - 重要情報（電子データ）が保存された媒体（USBメモリ、DVD-Rなど）や電子機器（PC等）を移送する際は、ITSが定めた手段でデータを暗号化すること
  - 重要情報（電子データ）を電子メールで送信する際は、 「2.3.2 メールの盗み見対策　機密情報送信時の処置」に従うこと

2.8.2 重要情報（電子データ）の管理（2/2）

- 重要情報返却時の遵守事項
  - 返却時には安全な方法で返却すること
    - 入手時に使用したディスクメディア（DVD-R等）を手渡しで返却する
    - データを取引先と合意した方法で暗号化した上で許可されたUSBメモリあるいは新品のディスクメディア（DVD-R等）にコピーし、手渡しでUSBメモリあるいは新品のディスクメディアを渡し、返却する
    - 「2.3.2 メールの盗み見対策　機密情報送信時の処置」に従い、電子メールにより返却する
- 重要情報削除時の遵守事項
  - 今後使用する必要がない重要情報は削除すること
    - ゴミ箱からも削除すること
    - メールで送受信していた場合は、メール削除後、ゴミ箱からも削除すること

第3章　外部サービス使用基準

当社では業務で外部サービスを使用することがあります。これらサービスは、使い方を誤ると情報漏えいやウイルス感染、不正アクセスなどを引き起こすきっかけになりかねません。そのため、当社では外部サービスの使用についてルールを定め、事件事故につながらないように配慮しています。

この章ではそのルールである「外部サービス使用基準」について解説します。

3.1 本文書の目的

本文書は、従業員が業務において外部サービスを使用する際に必要なルールを「遵守事項」としてまとめたものである。

以下のような場面において、当社が定めた遵守事項があるので、各自内容を理解し、外部サービス使用時に実践すること。

- 外部サービス使用
- SNSの使用

3.2 外部サービス使用に関する遵守事項

以下のようなリスクがあることを理解した上で使用すること

- 外部サービスは他社によるサービスであるため、情報を社外に預けることになる
  - 外部サービス運営会社から情報が漏えいする可能性がある
  - 外部サービス運営会社の都合で急遽サービスが停止される可能性がある
- SNSの場合、自らのミスで会社を危険にさらす可能性がある
  - 公式アカウントで不正確な情報により、会社の商品やサービスの売上に影響がでる可能性がある。
  - 公式アカウントで業務と無関係なユーザや企業をフォローすることにより、その個人・企業の活動を賛同していると勘違いされる可能性がある。
  - 個人アカウントによる発言が会社を代表する意見と捉えられてしまう可能性がある。
- 匿名掲示板の閲覧は、風評被害の確認のためのみ、許可する。
  - 書き込みは禁止とする。

具体的な遵守事項は次ページ以降

3.2.1 使用可能な外部サービスの制限

当社では使用可能な外部サービスを制限している

- 外部サービスによっては、意図せず外部に情報が公開されてしまったり、トラブルに巻き込まれたりする可能性があるため
  - 以前、あるグループ内情報共有サービスでは、デフォルトで誰もがその情報にアクセス可能な設定になっていたため、社外秘の情報がインターネット上に拡散したことがある

「使用可能なソフトウェアおよび外部サービス一覧」に記載されている外部サービス以外は使用しないこと。

- 一覧に登録されている外部サービスは安全性やサービス提供事業者による規約をITSが確認しているため使用可
  - ただし、確認したサービスが**完全に問題がないという保証はできない。会社の情報を他人に預けているという意識を常にもって使用すること。**
- 使用したい外部サービスが一覧に存在しない場合は、申請し、許可が得られた後、使うこと

業務で使用する情報は、**「使用可能なソフトウェアおよび外部サービス一覧」に記載されている外部サービス以外に保存しないこと。**

外部サービスを使用する際は、**使用するIDをITSへ連絡すること。**

- IDが変更となった場合は、速やかに連絡すること

3.2.2 外部サービスの使用について

業務で外部サービスを使用するケースとしては主に以下を想定している

- 社外でお客様にプレゼンテーションするために、ITSが許可したストレージサービスに資料を保存し閲覧する。
- お客様が指定した外部サービスにお客様が指定した情報を登録、保存する。
  - 同外部サービスに対し、ITSが使用を許可している場合に限る
- ITSが許可した外部サービスを使用して電子メールを送受信する。
- ITSが許可した外部サービスを使用して部員やお客様と業務連絡を行う。
- 投稿が許可された掲示板サービスを使用し、お客様の質問に対して回答する。
- 風評被害の確認のために、ITSが許可したSNSや匿名掲示板を閲覧する。

以下のようなケースでは、業務で外部サービスを使用してはならない

- ITSが許可していない外部サービスはいかなる場合も業務で使用してはならない。
- **業務で使用が許可された外部サービスのIDを私有の情報機器で使用してはならない。**

3.3 使用可能なSNSの制限

当社では使用可能な外部サービスを制限している

- SNSサービスの使用方法を誤ると、他利用者からのクレームを受けたり、組織に対する中傷が行われたり、発言が本で炎上騒動に発展したりするなど、トラブルに巻き込まれる可能性があるため

「使用可能なソフトウェアおよび外部サービス一覧」に記載されているSNSサービス以外は使用しないこと。

- 一覧に登録されているSNSサービスは安全性やサービス提供事業者による規約をITSが確認しているため使用可
  - ただし、確認したサービスが**完全に問題がないという保証はできない。会社の情報を他人に預けているという意識を常にもって使用すること。**
- 使用したいSNSサービスが一覧に存在しない場合は、申請し、許可が得られた後、使うこと

SNSサービスを使用する際は、**使用するIDをITSへ連絡すること。**

- IDが変更となった場合は、速やかに連絡すること

3.3.1 SNSの使用について

業務でSNSサービスを使用するケースと注意点を以下にまとめる

区分	用途	使用方法
広報業務	• 会社の公式アカウントとして、広報活動を行う	• 重要情報を投稿しない • 不正確な情報を投稿しない • 安易なユーザフォローをしない • 私有機器での広報業務用のアカウント使用禁止 • **他利用者からのクレーム、中傷、炎上等がある場合は、ITSに速やかに報告すること**
業務連絡	• グループを作成し、社内・部内のメンバーと情報共有する • お客様や取引先等と業務連絡する	• **私有機器での業務連絡用のアカウント使用禁止**

以下のようなケースでは、業務でSNSサービスを使用してはならない

- ITSが許可していない外部サービスはいかなる場合も業務で使用してはならない。
- **業務で使用が許可された外部サービスのIDを私有の情報機器で使用してはならない。**

SNSの私的利用時の注意

- 私有機器を用いて、プライベートでの使用時には以下に配慮すること
  - 業務に関する情報を発信しない
  - 当社所属であると認知されている場合、その発言が会社を代表する意見と受け取られる可能性があるため、以下を推奨する
    - 極力、当社所属であることを明かさない
    - 設定上、可能なら会社情報を登録しない、あるいは非公開の設定とするなどして、当社所属であることを開示しない
  - 当社所属であることを開示する場合、あるいはすでに周知されている場合、**自らの発言により起こり得る問題の責任を負う可能性があることを意識して使用する**

第4章　これだけは守ろう（行動指針）

ICT使用基準は、ICT使用において、事件事故を防ぐために必要な最低限度のルールです。

第2章、第3章では、このルールの説明だけではなく、なぜこのようなルールが必要なのかも解説しましたが、最後に最低限度、守るべき点を行動指針としてまとめます。

ルールはもちろんですが、本章で解説する行動指針を常に心がけるようにしてください。

4.1　2つの行動指針（1/2）

当社では、業務でICTを使用する上で以下の2つの行動指針を定めている

1.各自が守る意識をもって行動する

2.セキュリティ対策を継続する

4.1　2つの行動指針（2/2）

1.各自が守る意識をもって行動する

- ICTの使用者一人ひとりが、**情報漏えいリスクを意識して、当社の重要な情報を守るべく注意深く行動する**ようにしましょう。
- **利便性ではなく、安全性を重視する**ことを意識してください。
- ICTを使っていて気づいたことがあれば、情報共有してください。

2.セキュリティ対策を継続する

- ICT使用者は、一定の教育を受け、試験に合格した方を対象としますが、**運用状況の確認や環境の変化への対応のため、定期的に教育を受講**していただきます。
- **積極的に意見を出して、運用改善および安全性の強化に協力してください。**
- セキュリティ対策は世の中のセキュリティ動向とともに、その内容も変化する可能性があります。最新のICTを使用基準を参照し、ルールに沿って行動するようにしてください。