【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

情報機器使用基準

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。

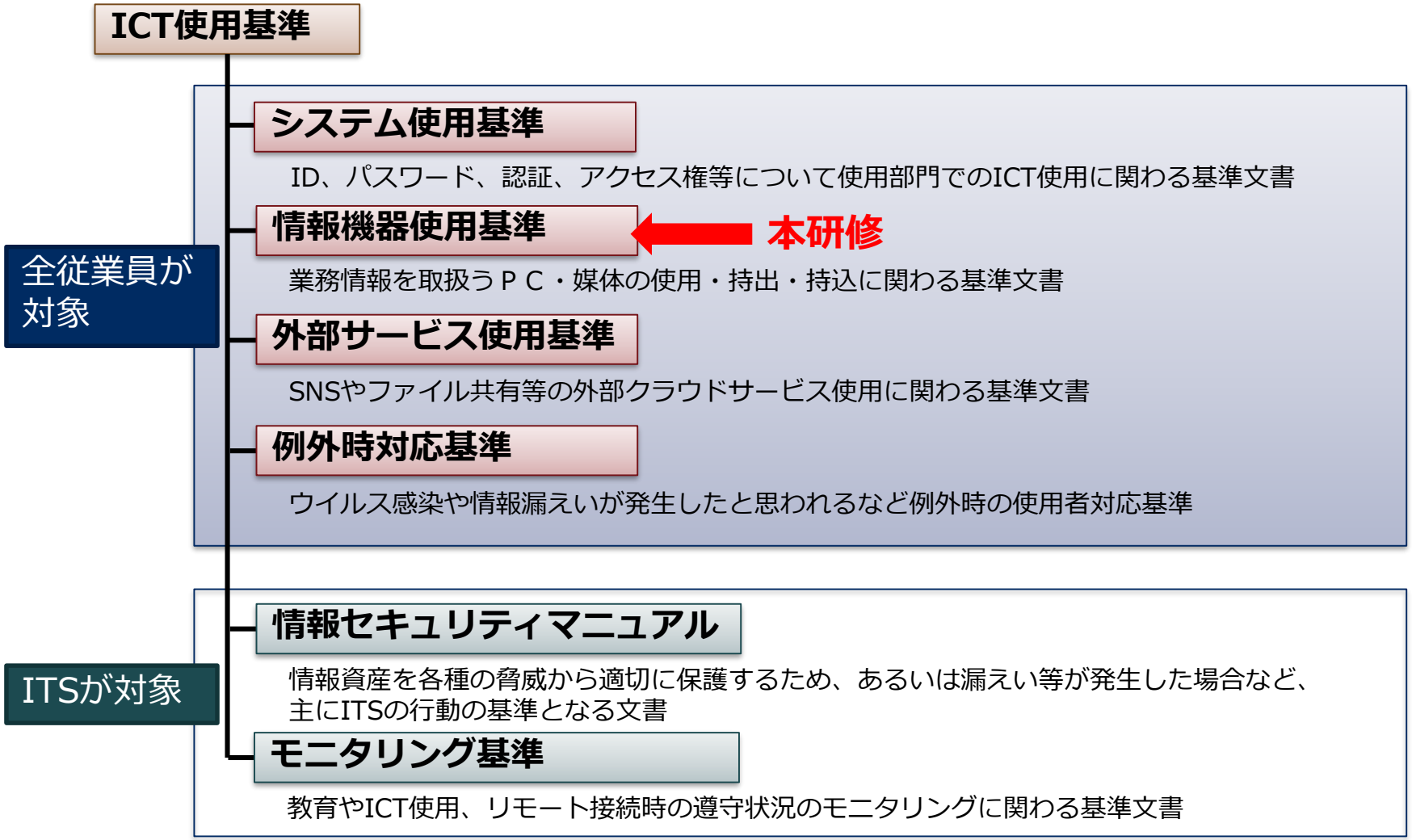
※本研修では学習の手助けのため、用語集を用意しております。以下のボタンをクリックしていただくと別ウィンドウで用語集のページが開きますので、必要に応じてご利用ください

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「情報機器使用基準」について説明します。



目次

第1章　実際の事件・事故

実際の事件・事故を通してセキュリティの大切さを学びます。

第2章　情報機器使用基準

業務情報を取扱うPC・媒体の使用・持出・持込に関わる基準文書

第1章　実際の事件・事故

この章では、実際に起きたPCやスマートフォンなどの情報機器やUSBメモリなどの電子媒体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

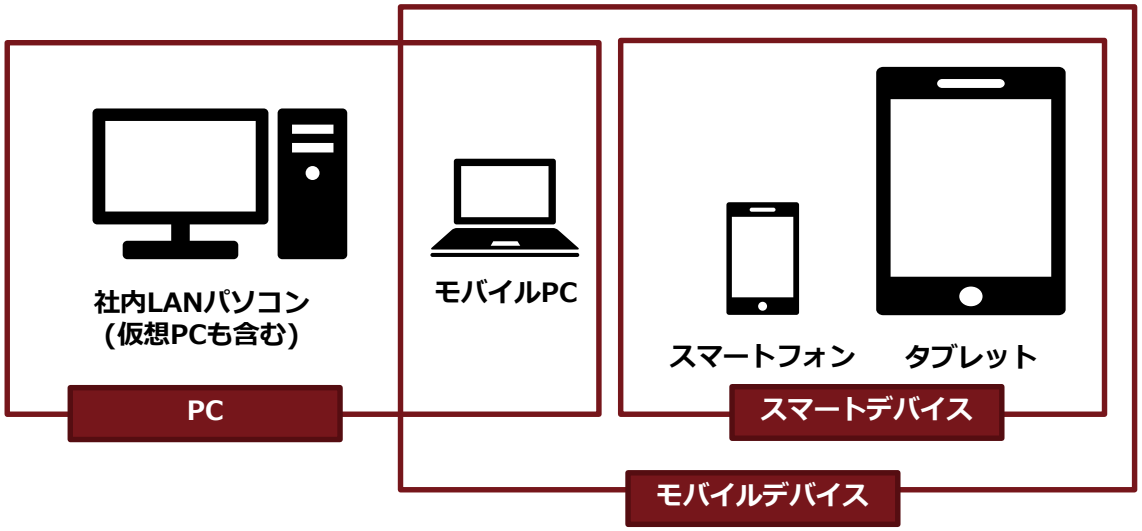
- iPhone のようなスマートフォンや iPad のようなタブレットを総称した呼び名。

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 モバイルデバイス、電子媒体持ち出しにともなう事件事故（1/2）

事件事故を起こした組織	事件事故概要
スポーツ用品総合商社	従業員が自転車により帰宅する途中、盗難に遭い、モバイルＰＣを入れた鞄が持ち去られた。 モバイルＰＣには、顧客450人分の氏名や住所、電話番号、メールアドレスなどが保存されていた。
大学	医学部の教員が出張中、宿泊先のホテルでモバイルＰＣの紛失に気付いた。その後の調査で、空港を利用した際、搭乗待合室のシートにモバイルＰＣを置き忘れたことがわかった。 モバイルＰＣには、担当科目における学生約3000人分の成績と顔写真などが保存されていた。 同大では、大学でモバイルＰＣを持ち出す際は申告が義務付けられていたが、同教員は手続きを行っていなかった。
高校	高校の教諭が生徒の個人情報を含むUSBメモリを紛失した。その後、紛失したUSBメモリに含まれる個人情報が記載された書類が匿名で高校所在地である都道府県に郵送されたことで問題が発覚した。 教諭は所属長に紛失を報告していなかった。 USBメモリはその後も回収されていないため、個人情報が漏えい、悪用される可能性がある。
金属加工会社	取引先の個人情報や業務情報が保存されたスマートフォンを従業員が帰宅途中の電車内で紛失した。翌日、警察や交通機関に届け出たが見つからなかった。 紛失したスマートフォンには、取引先約200人の氏名や電話番号、メールアドレス、および業務情報などが記録されていた。 同社では、紛失した端末から社内システムやメールシステムへのアクセスを遮断するなど対策を強化している。
ガス会社	委託先従業員が飲酒後に駅ロータリー内で業務用のモバイルＰＣを入れた鞄を隣に置いて眠ってしまい、目を覚ましたところ、鞄を紛失していることに気付いた。 同モバイルＰＣには、1万件以上の顧客情報が含まれていた。

1.1 モバイルデバイス、電子媒体持ち出しにともなう事件事故（2/2）

- モバイルデバイスや電子媒体が失われるだけであればたいしたことはない
- その中にOEM処方や顧客情報など**重要な情報が含まれていると大変なことになる**
  - 情報が流出、不正利用される恐れ
  - システムが不正利用される恐れ
    - モバイルデバイスにID、パスワードを記憶させたままの状態で紛失し、ロックを解除された場合は、システムに繋げられてしまう恐れがある
  - その後の対応に時間や手間がかかる
  - 損害賠償
  - 企業イメージの低下

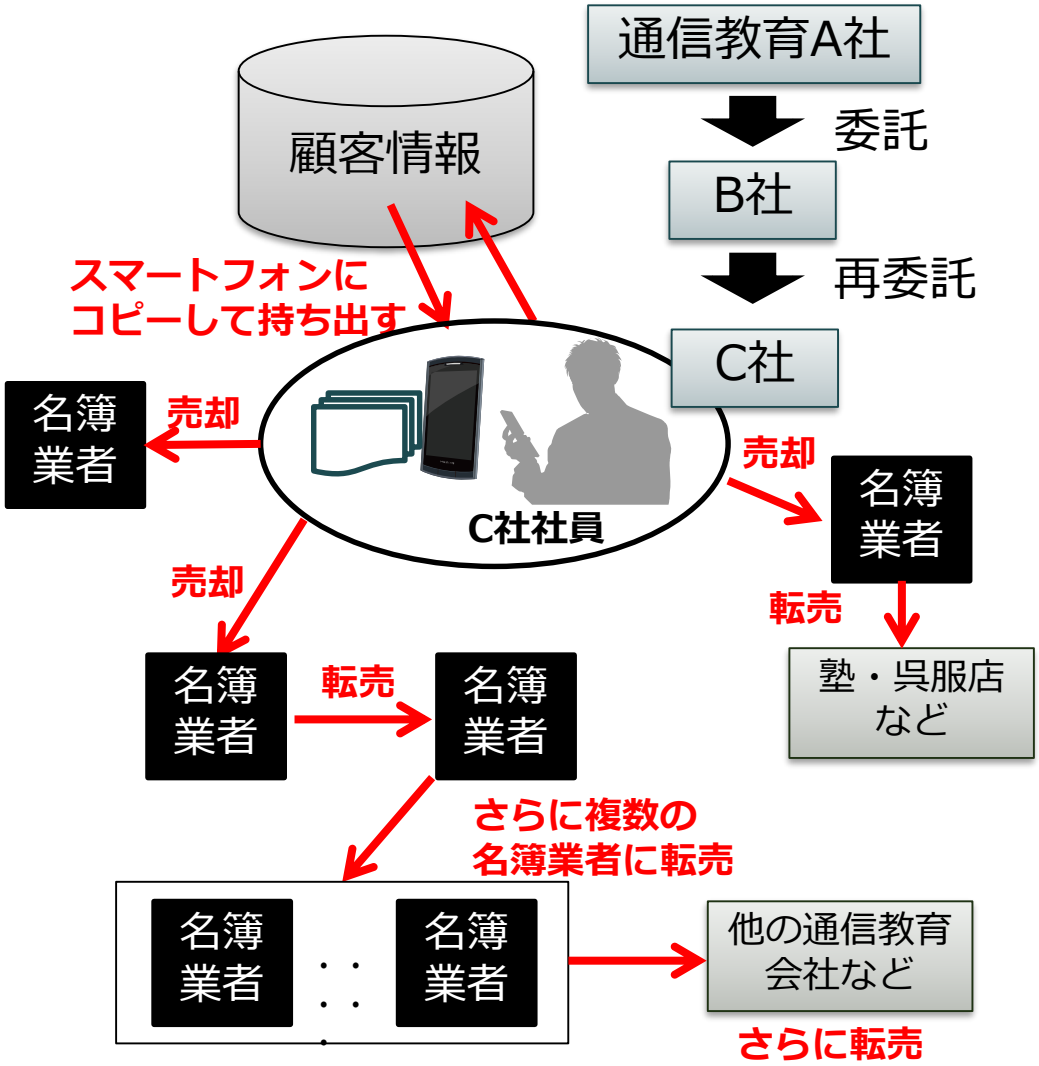
etc.

原則として、重要な情報をモバイルデバイスや電子媒体に格納して持ち出してはいけません

- やむを得ず情報を格納して持ち出す際には、所属長の許可を得てから持ち出しましょう。
- 持ち出し中は「肌身離さず」を原則として、紛失・盗難等の事件事故がないように気をつけましょう。

1.2 スマートデバイスによる不正な情報持ち出し（1/2）

委託先の社員が4,858万人もの個人情報を盗み出し、名簿業者に売却



1.2 スマートデバイスによる不正な情報持ち出し（2/2）

スマートデバイスは、データを格納することが可能

- PCに接続することで機密性の高いデータを転送することができる
  - データを格納した状態でスマートデバイスを紛失すると、そのデータが漏れることにもなりかねない

業務上、やむを得ない場合を除いて、原則データを
スマートデバイスに格納しないようにしましょう

悪意を持ってデータを盗もうとされた場合、防ぐのは困難

- 普段からそのような行為をさせないような環境を維持することで抑止する

→業務で会社資産の情報を取り扱うことができるスマートデバイスを以下のみに制限

- **ITSが使用を許可した社有のスマートデバイス**
  - **使用が許可されたスマートデバイスには、必ず許可されたことを示すシールを貼付すること**

「許可されたことを示すシール」が貼付されていないスマートデバイスは
業務で使用しないでください

私物のスマートデバイスは、業務で使用してはいけません。
業務上必要な場合は、正式な手順を踏んで、スマートデバイスの貸与を
申請するようにしましょう。

第2章　情報機器使用基準

当社では業務でPCやスマートフォンなどの情報機器やUSBメモリなどの電子媒体を使用します。これら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、当社では業務情報を取扱うPCや媒体の使用・持出・持込に関わるルールを定め、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「情報機器使用基準」について解説します。

2.1 本文書の目的

本文書は、業務情報を取扱うPCや媒体の使用・持出・持込に関わるルールを「遵守事項」としてまとめたものである。

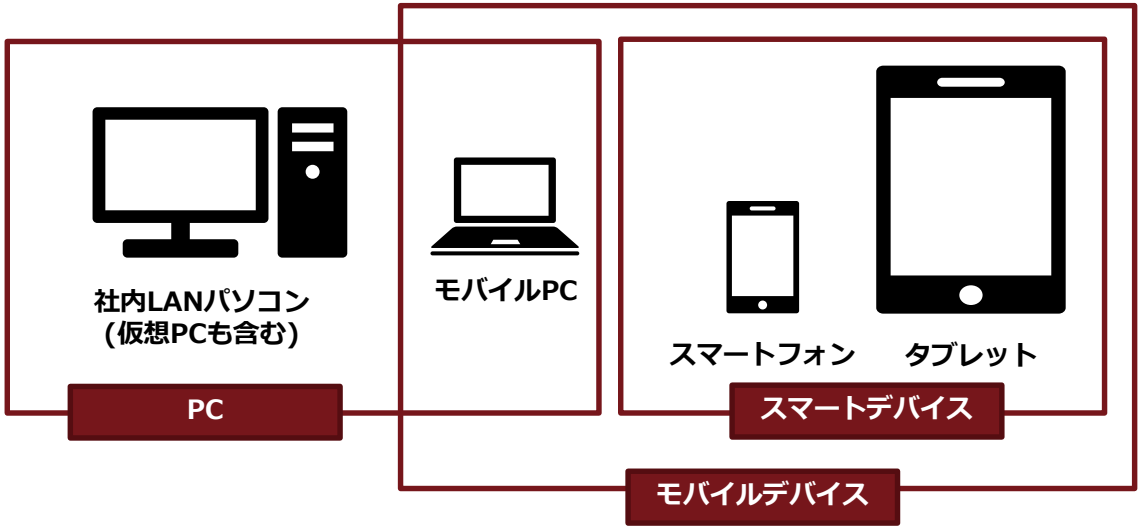
以下のような場面において、当社が定めた遵守事項があるので、各自内容を理解し、社内LANパソコンや媒体の使用時に実践すること。

- PCの使用に関する遵守事項
- スマートデバイスの使用に関する遵守事項
- 使用可能なネットワークと使用時のリスク
- モバイルデバイスの持ち出しに関する遵守事項
- 電子媒体の使用に関する遵守事項

2.2 PCの使用に関する遵守事項

PCの使用が不適切だと、事件事故に繋がりかねないこと理解すること

- PCの不適切な使用が原因で、情報漏えいや不正アクセス等の事件事故につながる事例があとを絶たない。当社においても、同様の事件事故が起こりかねないことを常に意識して使用する必要がある。
- 当社では、PCの使用にともなう事件事故を防ぐため、PCの使用には一定の制限を設けている。



具体的な遵守事項は次ページ以降

2.2.1 使用可能PCの制限

業務で使用可能なPCは会社支給のPCのみである

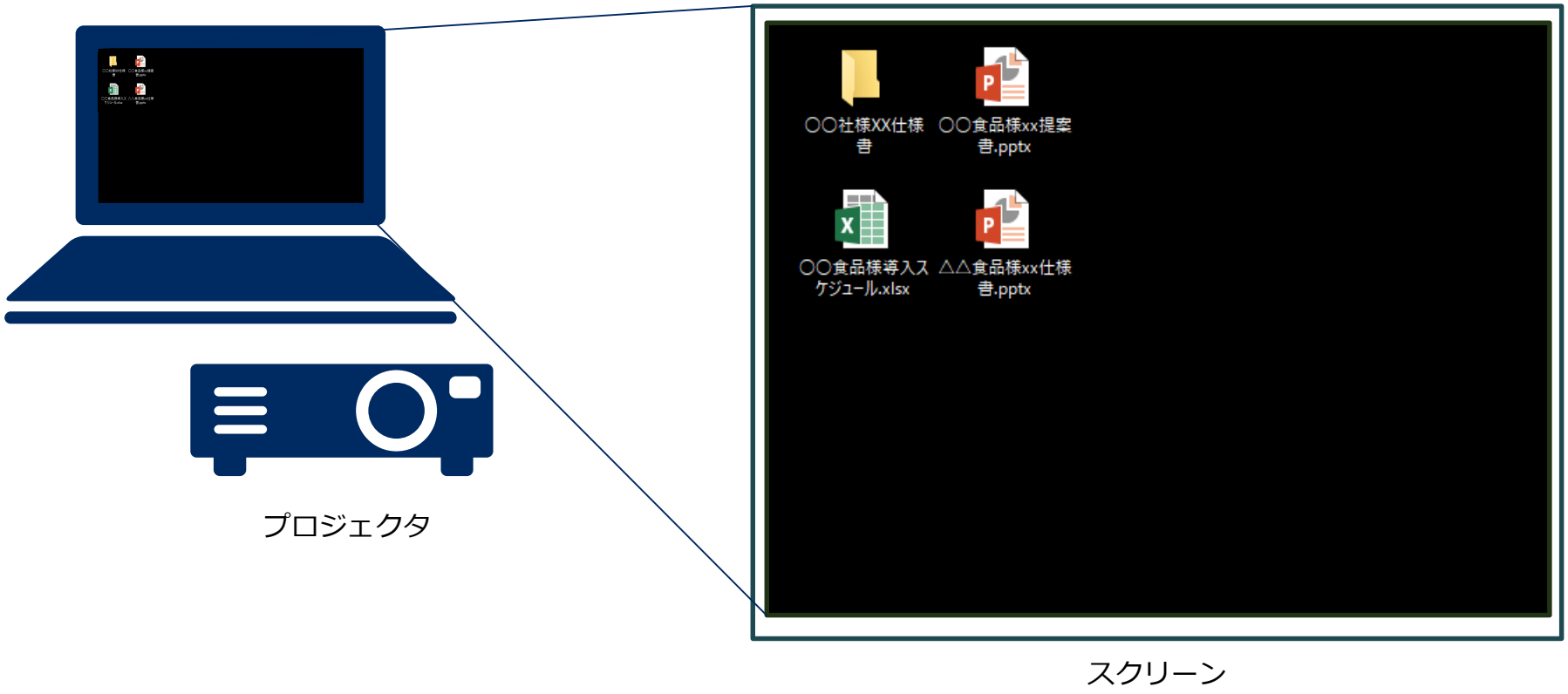
- 業務で使用可能なPCは**ITSが使用を許可した社有のPC（社内LANパソコン(仮想PCも含む)、モバイルPC）のみ**である。**私有PCの業務での使用は禁止**する。
  - モバイルPCに関しては、別途許可されたことを示すシール等を他の従業員から視認できる位置に貼付しなければない

許可済みシールのイメージ
※実際の運用時には異なる可能性があります

    - 許可済みモバイルデバイスとは、ITSが使用を許可した社有のモバイルＰＣとスマートデバイスの総称
  - 私有PCの社内ネットワークへの接続禁止
- 会社支給のPCを業務目的以外に使用してはならない。

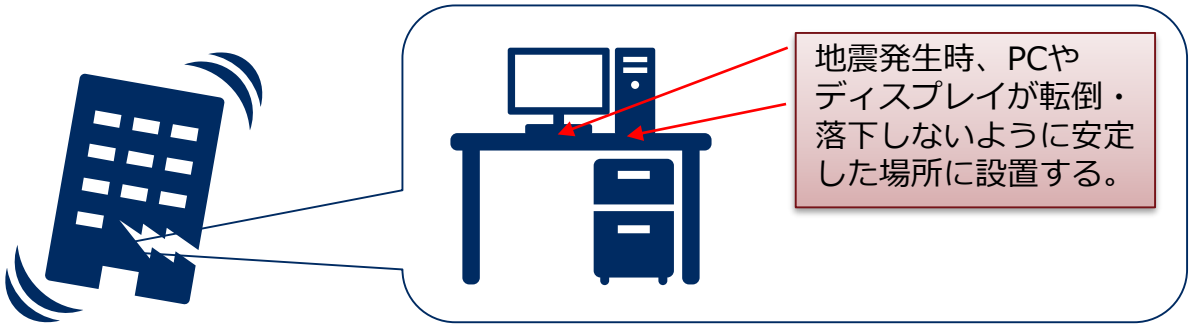
2.2.2 クリアスクリーン

- PCを使用中、離席する際は画面を表示したままにしないこと
  - 「Windowsキー」＋「Lキー」を同時に押すことですぐに画面ロックが可能。
- リモート接続などで画面を社外の方に見せる可能性がある場合は、デスクトップ上に不要なアイコンやショートカットを配置してはならない
  - プレゼンする際などにデスクトップが映ってしまうと、デスクトップ上のアイコンの情報から、顧客名などが漏れてしまう



2.2.3 PCの設置

- 社内に常設するPCは地震等による転倒、落下を防ぐため、安定した場所に設置すること。



- 社内で使用するモバイルPCは以下のような盗難対策を施さなければならない
  - 帰宅時に机の引き出しやキャビネット等施錠できる場所に保管する

2.2.4 私有品のPC接続禁止

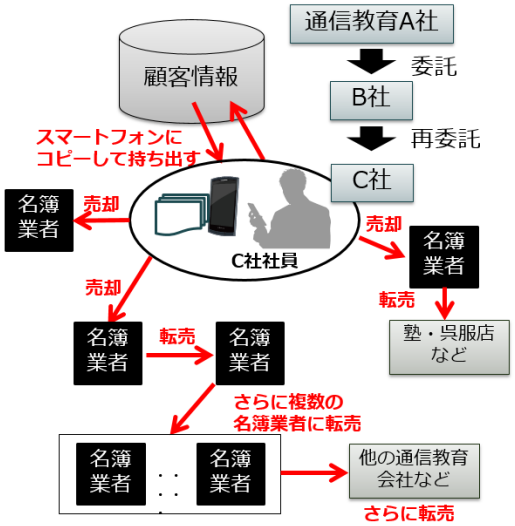
ITSが使用を許可した社有のPCに私有品（USBメモリ、スマートフォン等）の接続を禁止する

- 社有のPCから私有品に対し、データのコピー等をさせないため
- マルウェア等が社内に持ち込まれることを防ぐため

※私有スマートデバイスの業務での使用自体禁止　→参考：2.3.1 使用可能スマートデバイスの制限

1.2 スマートデバイスによる不正な情報持ち出し（1/2）

委託先の社員が4,858万人もの個人情報を盗み出し、名簿業者に売却



2.2.5 マルウェア対策（1/2）

導入されているマルウェア対策ソフトについて

- 必ず、常駐、監視させておかなければならない
  - 使用するファイルへのアクセスおよび電子メールの受信時には、常時スキャンできる状態で使用すること。
- ウイルス定義データベースが最新に保たれていなければならない
  - 最新でない場合、新しいマルウェアの検出、駆除ができない可能性がある。

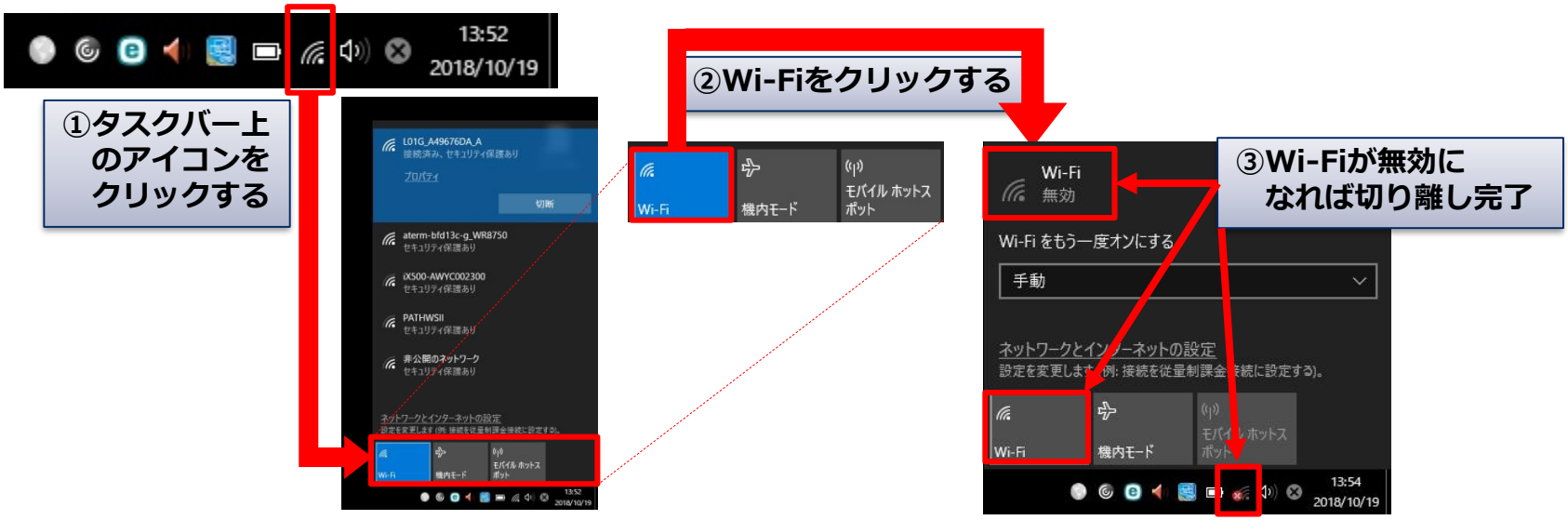
常駐、監視している状態

ウイルス定義データベースが
最新に保たれている状態

2.2.5 マルウェア対策（2/2）

マルウェアに感染した場合、または感染が疑われる場合

- マルウェア対策ソフトがマルウェアを検知した場合、またはマルウェアに感染、もしくは感染が疑われる場合は、以下を実行すること。
  - 感染拡大の防止、遠隔からの操作を防止するため、**ネットワークから速やかに切り離す**こと。
    - LANケーブルの抜線
    - 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す



  - **PCのシャットダウン、再起動、電源断は行わない**こと。
    - 一部のマルウェアはシャットダウン時やシャットダウン後の起動時に不正な動作を行うことがあるため。
  - **ITSに速やかに連絡し、対応方法について指示を仰ぐ**こと。
  - ITSの指示に従って、マルウェアを隔離あるいは駆除すること。
  - マルウェア被害の影響範囲が社外にまで至っているかを確認し、影響が確認された場合、あるいはその可能性がある場合、その事実について速やかにITSに報告すること。

2.2.6 PCの修理・返却

PCを修理する場合

- ITSが提供しているPCの修理を依頼する場合は、IT推進委員等の担当者から修理を依頼すること。
  - 修理を依頼する場合は、機密性の高い情報が読み出し可能な状態で保存されていないことを確認した上で修理を依頼すること。故障の状況により、保存されている情報の確認や保護が実施できない場合には、ITSに確認し、指定された方法にて修理を依頼すること。

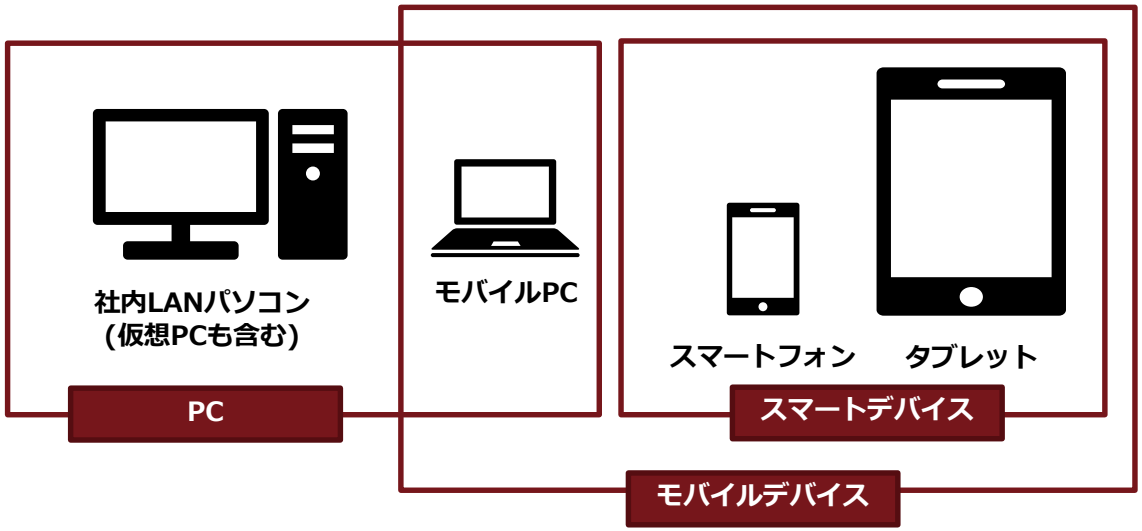
PCを返却する場合

- PCはITSの資産であるため、PCが不要になった場合は、各部門で廃棄せず、ITSに返却すること。
  - データを読み出せない状態にして廃棄しないと、廃棄PCのHDDからデータを復元されてしまう危険性があるため

2.3 スマートデバイスの使用に関する遵守事項

スマートデバイスの使用が不適切だと、事件事故に繋がりかねないこと理解すること

- スマートデバイスの不適切な使用が原因で、情報漏えいや不正アクセス等の事件事故につながる事例があとを絶たない。当社においても、同様の事件事故が起こりかねないことを常に意識して使用する必要がある。
- 当社では、スマートデバイスの使用にともなう事件事故を防ぐため、スマートデバイスの使用には一定の制限を設けている。



具体的な遵守事項は次ページ以降

2.3.1 使用可能スマートデバイスの制限

業務で使用可能なスマートデバイスは会社支給のスマートデバイスのみである

- 業務で使用可能なスマートデバイスは**ITSが使用を許可した社有のスマートデバイス（スマートフォン、タブレット）のみ**である。**私有スマートデバイスの業務での使用は禁止**する。
  - スマートデバイスに関しては、別途許可されたことを示すシール等を他の従業員から視認できる位置に貼付しなければない

許可済みシールのイメージ
※実際の運用時には異なる可能性があります

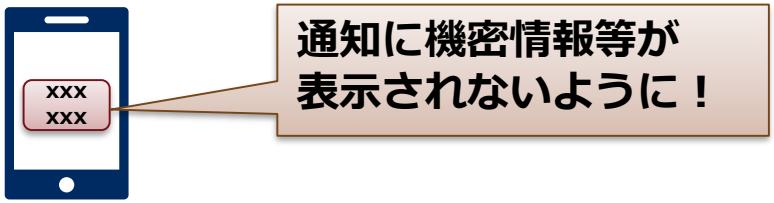
    - 許可済みモバイルデバイスとは、ITSが使用を許可した社有のモバイルＰＣとスマートデバイスの総称
  - 私有スマートデバイスの社内ネットワークへの接続禁止
- 会社支給のスマートデバイスを業務目的以外に使用してはならない。

スマートデバイスと連携するスマートウォッチ等について

- 会社支給のスマートデバイスの着信確認等で私物のスマートウォッチやスマートバンドを使用、連携することについては特に禁止とはしないが、以下に留意して使用すること
  - 連携に使用するアプリは、App Storeで公開されているアプリ以外禁止とする
  - スマートウォッチやスマートバンドの中には、収集した情報を外部に送信、保管しているものがある
    - 個人情報保護に対する取り組みが適切ではないベンダーによる製品も存在するため、会社支給のスマートデバイスと連携させるかどうかは慎重に判断する必要がある
    - **使用に伴い、当社に不利益が生じた場合、使用者に責任を問う可能性がある**

2.3.2 スマートデバイスの他者への使用制限

- スマートデバイスは肌身離さず携帯すること。
- 第三者に操作されないためにパスコードを設定すること。
  - パスコードはITSの指示に従い、各自が設定すること。
  - パスコードは第三者に開示しないこと。
  - パスコードを手帳等に記入する場合は、モバイルデバイスと一緒に管理（保管）しないこと。
  - **パスコードに社員番号を設定しないこと。**
- ロック機能を有効にし、第三者が無断で使用できないようにすること。
  - 生体認証（Touch ID、Face ID等）の使用は許可する。
  - 一定時間未使用時に自動的に画面をロックするよう設定すること。（推奨時間３分）
- ロック画面上に表示する通知などの情報は最小限にすること。



- アプリ自体がロック機能を持っている場合は、それも有効にすること。
  - **重要情報を記憶できるアプリの場合は、生体認証（Touch ID、Face ID等）を設定することを必須とする**
- スマートデバイスを他人に譲渡・貸与しないこと。
  スマートデバイスの使用者を無断で変更しないこと。
  - 使用者の変更が必要な場合には、いったんITSに返却後、再度貸し出しを受けること。

2.3.3 データ転送および充電

データ転送について

- 初期設定およびバックアップ・リストア、OSアップデート、充電等を除き、社内LANパソコンへのデータ転送を目的としたケーブル接続は禁止する。
- データ転送は、使用が許可された外部サービス経由で行うこと。

社有のスマートデバイスを**私有PC等に接続しない**こと。

ストレージ機能を有するカードリーダー等、社有品であっても許可されていない周辺機器を接続しないこと。

2.3.4 マルウェア対策

iOS以外のスマートデバイスの使用者の場合

- 導入されているマルウェア対策ソフトの設定を変更せず、常駐設定にして、ファイルへのアクセスおよび電子メールの受信時には、常時スキャンできる状態で使用すること。
- ウイルス定義データベースが最新に保たれていなければならない。

マルウェアに感染した場合、または感染が疑われる場合

- マルウェア対策ソフトがマルウェアを検知した場合、またはマルウェアに感染、もしくは感染が疑われる場合は、以下を実行すること。
  - 感染拡大の防止、遠隔からの操作を防止するため、**ネットワークから速やかに切り離す**こと。
    - 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
  - **スマートフォンの電源断、再起動は原則、行わない**こと。
    - 一部のマルウェアは電源断時やその後の起動時に不正な動作を行うことがあるため。
    - ただし、**操作を受け付けないなどネットワークから切り離せない場合のみ、電源断を許可する**。
  - **ITSに速やかに連絡し、対応方法について指示を仰ぐ**こと。
  - ITSの指示に従って、マルウェアを隔離あるいは駆除すること。
  - マルウェア被害の影響範囲が社外にまで至っているかを確認し、影響が確認された場合、あるいはその可能性がある場合、その事実について速やかにITSに報告すること。

2.3.5 スマートデバイスの修理・返却

スマートデバイスを修理・返却する場合

- 社有のスマートデバイスの修理・返却を依頼する場合は、ITSに連絡、相談すること。

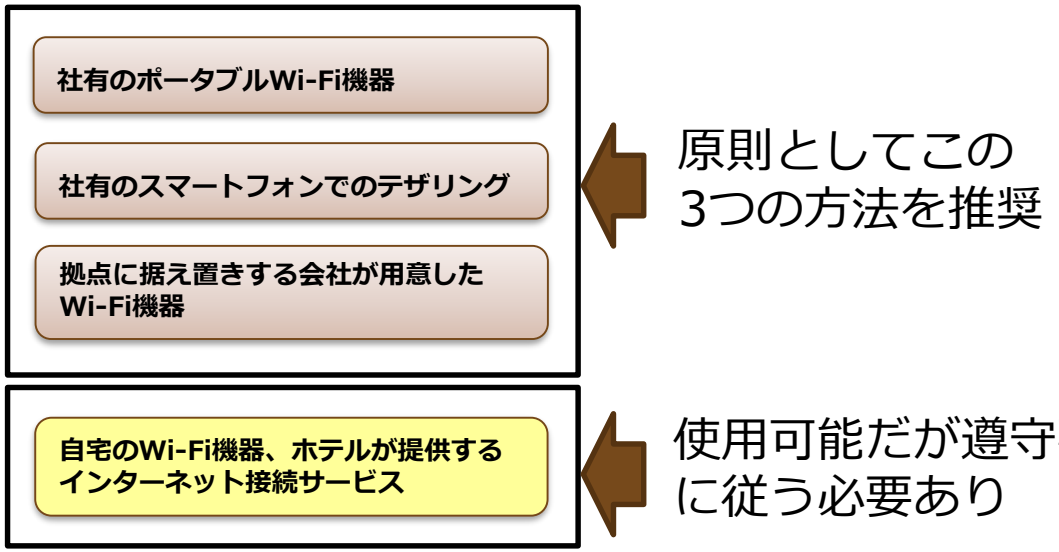
2.3.6 位置情報について

- 業務時間内は、社有のスマートデバイスの位置情報共有設定をONにしておくこと

2.4 使用可能なネットワークと使用時のリスク

許可済みモバイルデバイスでは使用可能なネットワークを制限している

- 社内ネットワークに直接接続することは禁止
- 使用可能なネットワークは下記のみ
  - 通信事業者が提供する通信手段（4G/3G等）
  - 以下のWi-Fi接続方法



無料のWi-Fiスポットなどは危険性が高いため、許可済みモバイルデバイスを接続することは禁止する

- 無料のWi-Fiスポットはセキュリティ対策が不適切な場合がある
- 正規の無料Wi-Fiスポットと同一あるいは紛らわしい文字列のアクセスポイント名（SSID）を設定した偽Wi-Fiスポットである可能性もある

2.4.1　自宅Wi-Fiの危険性

自宅Wi-Fiには以下のようなリスクがある

1. 使用するWi-Fi機器が**適切なセキュリティ機能を有していない**
2. 使用するWi-Fi機器で**適切なセキュリティ機能が設定されていない**
3. 使用するWi-Fi機器に**脆弱性が存在している**

自宅でWi-Fi機器を使用している方は、この３つのリスクを認識しておくこと

2.4.1(1)　適切なセキュリティ機能を実装したWi-Fi機器を使用する

1. 使用するWi-Fi機器が**適切なセキュリティ機能を有していない**
2. 使用するWi-Fi機器で**適切なセキュリティ機能が設定されていない**
3. 使用するWi-Fi機器に**脆弱性が存在している**

Wi-Fi機器には、通常セキュリティ機能が搭載されているが、古い機器の場合、強固なセキュリティ機能が搭載されていない可能性がある

現在ではWEPの暗号化は短時間で解読されてしまうことがわかっており、使うのは危険

WEPしか対応していない機器は使わない方がよい

WPA2の使用を推奨

そのためにはWPA2をサポートする機器を使う必要がある

機器が保持しているセキュリティ機能の確認のため、使用するWi-Fiアクセスポイントまたはルータの暗号化方式をITSに報告後、許可を得ること。
暗号化方式が不明な場合は、機種名を報告すること。

適切なセキュリティ機能を実装したWi-Fi機器を使用するようにしましょう。
万が一、使用しているWi-Fi機器が適切なセキュリティ機能を実装していない場合は、許可済みモバイルデバイスを接続しないようにしましょう。

用語チェック　WEP・WPA・WPA2

WEP

- 「Wired Equivalent Privacy」の略称。初期の無線ネットワークのセキュリティ強化のための仕組み。脆弱性が確認されており現在では利用が推奨されていない。

WPA

- 「Wi-Fi Protected Access」の略称。無線ネットワークのセキュリティ強化のための仕組み。WEPの脆弱性が確認されたため、より強化されたセキュリティ仕組みとして考え出された。現在となってはよりセキュリティが強化されたWPA2の使用が推奨されている。

WPA2

- 無線ネットワークのセキュリティ強化のための仕組みであるWPA(Wi-Fi Protected Access)のバージョン２。WPAよりもさらにセキュリティが強化されている。

暗号化の強度比較

WEP　＜　WPA　＜　WPA2

2.4.1(2)　セキュリティ機能を適切に設定する

1. 使用するWi-Fi機器が**適切なセキュリティ機能を有していない**
2. 使用するWi-Fi機器で**適切なセキュリティ機能が設定されていない**
3. 使用するWi-Fi機器に**脆弱性が存在している**

たとえ使用しているWi-Fi機器がセキュリティ機能を有していても、基本的に設定しないと有効になりません

- 暗号化方式を選択する際は**WPA2を選択、設定する**
- **セキュリティキー（機器によってはパスワードや暗号化キー等呼び方が異なる）には、英大文字、英小文字、数字、記号などを組み合わせ、できるだけ複雑な値を設定する**
- **MACアドレスフィルタリング（許可されていない端末以外は接続できないようにする）を有効にする**

適切な暗号化方式（WPA2等）を採用すること。

MACアドレスフィルタリングなどを施し、許可された端末以外は容易に接続できないようにすること。

Wi-Fi機器を管理するためのアカウントについて
・デフォルトパスワードは変更する
・パスワードは、英大文字、英小文字、数字、記号などを組み合わせ、できるだけ複雑な値を設定する
・可能な場合はアカウント名も変更する

自宅Wi-Fiを使用する際は、**Wi-Fi機器のセキュリティ機能を適切に設定しましょう。**

用語チェック　MACアドレスフィルタリング

MACアドレスフィルタリング

- Wi-Fiアクセスポイント等に特定の機器のみを接続させることを目的としたセキュリティ機能。無線LANの機器に出荷時に割り振られているアドレス（MACアドレスと呼ぶ）をWi-Fiアクセスポイント側に登録することで登録されている機器以外接続できないようにフィルタリングする機能。

2.4.1(3)　セキュリティ機能を適切に設定する

1. 使用するWi-Fi機器が**適切なセキュリティ機能を有していない**
2. 使用するWi-Fi機器で**適切なセキュリティ機能が設定されていない**
3. 使用するWi-Fi機器に**脆弱性が存在している**

Wi-Fi機器には販売後に脆弱性と呼ばれる弱点が見つかることがある

- Wi-Fi機器を乗っ取られたり、悪用されたり、設定を変更されたりする可能性がある

使用するWi-Fiアクセスポイント、またはルータのファームウェアを最新のバージョンに更新すること。

新しいファームウェアが出ているかどうかの確認方法、ファームウェアのバージョンアップ方法は使用している機器によって異なるので、必ずマニュアルで確認してください。

自宅Wi-Fiを使用する際は、**安全のためWi-Fi機器を最新の状態にしましょう。**

用語チェック　ファームウェア

ファームウェア

- 機器を制御するために組み込まれているソフトウェア。機器に脆弱性が見つかった場合、開発元がその脆弱性を修正するため新しいバージョンのファームウェアを提供することがある。

NEC製Wi-Fi機器Atermのファームウェア更新画面イメージ（出典：NEC）

2.4.2　ホテル提供のWi-Fiの危険性（1/3）

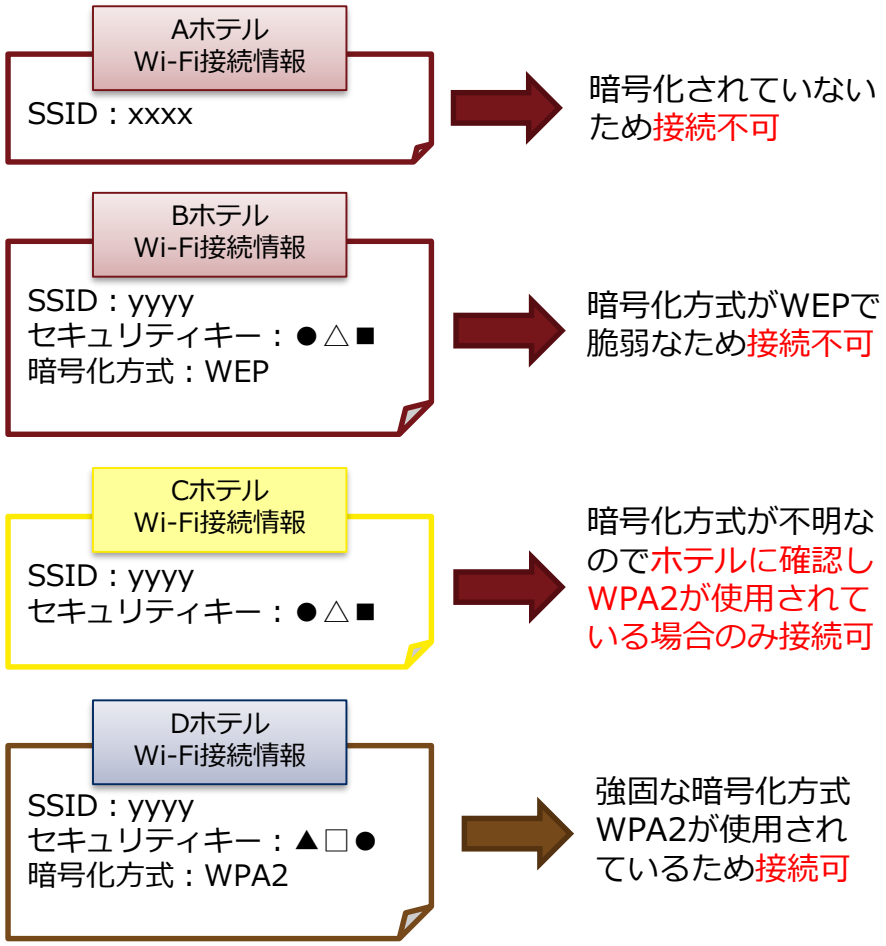
- 許可済みモバイルデバイスをホテル提供のWi-Fiに接続、使用するのは、**やむを得ない場合のみ**とする
  - ITSが提供するリモート接続ソフトウェア以外は使用してはならない

- ホテル提供のWi-Fiには、「2.4.1　自宅Wi-Fiの危険性」と同じリスクがある
  - その上、対策が取られているかどうかはそのホテルのWi-Fiサービスの運用次第
  - 最悪の場合、なんの対策も取られておらず、無防備な状態である可能性もある

適切な暗号化方式（WPA2等）が採用されていない場合（暗号化なし、WEP、WPA等）は使用しないこと。

2.4.2　ホテル提供のWi-Fiの危険性（2/3）

ホテルが採用しているWi-Fiの接続可否の例



2.4.2　ホテル提供のWi-Fiの危険性（3/3）

その他、遵守事項

不特定多数の利用者が共有しているネットワークであることを常に念頭において使用すること。

- そのネットワークに接続することでウイルスに感染したり、他の利用者から不正アクセスを受けるかもしれない

モバイルデバイスのOSが使用可能なものであり、最新のバージョンであることを確認すること。

ホテルが使用しているWi-Fiアクセスポイント、またはルータには脆弱性が潜んでいる可能性があることを念頭において使用すること。

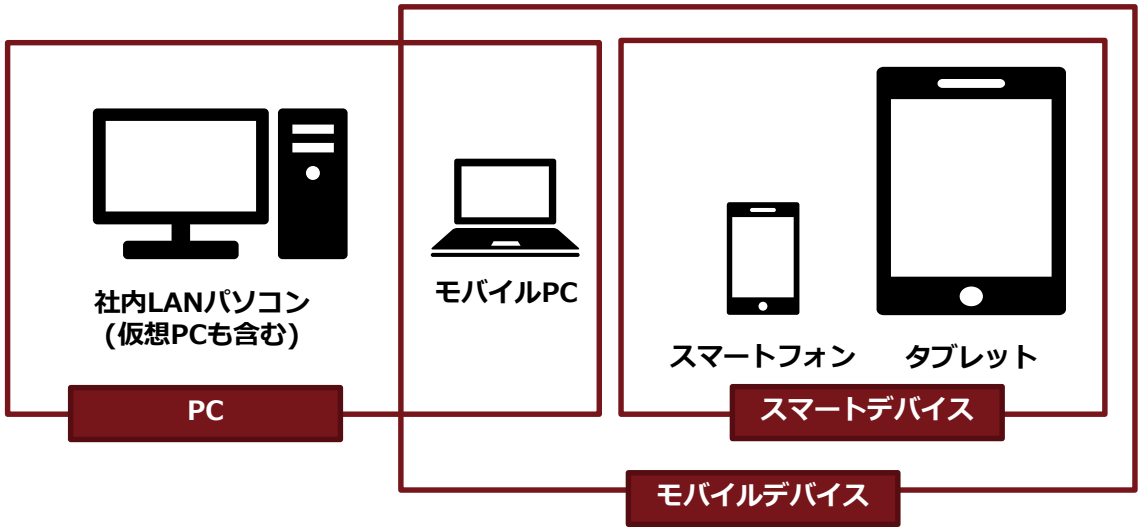
- ファームウェアが古く、脆弱性が修正されていないまま使用している可能性がある。
- 悪意のある人物に、脆弱性が悪用され、Wi-Fi機器が乗っ取られると、そのネットワークを流れる通信が盗聴されたり、悪質なサイトに誘導されたりする可能性がある。

ホテル提供のWi-Fiについてはセキュリティが確保されていない可能性があるので、許可済みモバイルデバイスを接続するのは**「やむを得ない場合のみ」**

2.5 モバイルデバイスの持ち出しに関する遵守事項

PC、スマートデバイスの中でも、モバイルデバイスは持ち出しが可能であるため、持ち出しにともなう事件事故に備える必要がある

- モバイルデバイスを持ち出した際に、盗難・紛失、情報が漏えいするリスクがある



具体的な遵守事項は次ページ以降

2.5.1 モバイルデバイス持ち出し時の注意事項

モバイルデバイスに関連するセキュリティ事故でもっとも多いのは、持ち出し時に紛失したり、盗難にあったりするケース

- 当社ではモバイルデバイスの持ち出し時の紛失・盗難対策を「社外持ち出し時の注意事項」として「モバイルＰＣ使用基準」「スマートデバイス使用基準」に記載

社外持ち出し時の注意事項

1.ローカル（端末内に保存される領域）に不要なデータがないことを確認の上、持ち出すこと。
2.移動時の交通機関や人混みの中では、盗難に遭わないよう、適切にモバイルデバイスを取り扱うこと。
3.紛失防止のため、モバイルデバイスは常に手元に置き、放置しないこと。
4.社外でモバイルデバイスを使用する際は、盗み見に注意して安全な場所で使用すること。やむを得ず周辺に他者がいる状態で使用する場合には、壁を背にして他者から覗かれないよう配慮する、またはプライバシーフィルタを使用するなど覗き見を防止すること。
5.紛失に気付いた場合は、速やかにITSに報告すること。

- 持ち出す際は、**極力ローカルにデータを置かない**
- 持ち出す前に一度**ローカル内にどのようなデータがあるのか確認する**
- 持ち出しが必要なデータがある場合は、**使用が許可された外部サービス（「外部サービス使用基準」参照）上に保存することを検討する**
- モバイルデバイスのローカルに重要情報や個人情報を一時的に保存する場合は、**使用する必要性がなくなった時点で速やかに消去する**
- 必要に応じてストラップ等の取り付けなど紛失対策を行うこと

2.5.2 モバイルデバイスのセキュリティ対策

- 「モバイルＰＣ使用基準」「スマートデバイス使用基準」内の「データセキュリティ対策」も確認すること

データセキュリティ対策（モバイルデバイスでの情報保管）

1. 重要情報や個人情報は、使用が許可された外部サービス上に保存し、モバイルデバイスには保存しないこと。やむを得ず、モバイルデバイスのローカルに重要情報や個人情報を一時的に保存する場合は、使用する必要性がなくなった時点で速やかに消去すること。
2. 毎月1回、モバイルデバイスのローカルデータの確認を行い、不要な情報が保存されている場合は削除すること。スマートデバイスの場合、ローカルに保存されている電子メールデータ（携帯アドレスのメールおよび添付ファイル等）についても、不要なものは送受信ボックスおよびゴミ箱からも削除すること。

2.6 電子媒体の使用に関する遵守事項

USBメモリなどの電子媒体の使用が不適切だと、事件事故に繋がりかねないことを理解すること

- USBメモリなどの電子媒体の不適切な使用が原因で、情報漏えいや不正アクセス等の事件事故につながる事例があとを絶たない。当社においても、同様の事件事故が起こりかねないことを常に意識して使用する必要がある。
- 当社では、 USBメモリなどの電子媒体の使用にともなう事件事故を防ぐため、 電子媒体の使用には一定の制限を設けている。

具体的な遵守事項は次ページ以降

2.6.1 使用可能な電子媒体の制限

業務で使用可能な電子媒体は以下とする

- **ITSが使用を許可した社有のUSBメモリ**
- **デジタルカメラの備品として装着している部署で調達したSDカード（micro SDカード含む）、DVD-Rなどのディスクメディア**

ITSが使用を許可した社有のUSBメモリ
- 個人に割り当てられたUSBメモリ
- 部門共有のUSBメモリ

デジタルカメラの備品として装着している部署で調達したSDカード（micro SDカード含む）

DVD-Rなどのディスクメディア

私有の電子媒体を業務で使用してはならない

2.6.2 部門共有の電子媒体の使用

部門共有の電子媒体は使用部門にて管理者を決定し、**台帳などで管理をしなければならない**

- SDカード（micro SDカード含む）はデジタルカメラとセットで保管しなければならない。
- カードリーダーを貸与されている場合は、合わせて管理を行うこと。

電子媒体管理台帳

部署

管理番号	メーカー	型番	シリアル番号	責任者	使用開始日	種別（該当するものに○）
					年 月 日	USBメモリ ・ SDカード ・ デジタルカメラ ・ カードリーダ ・ その他（ ）
					年 月 日	USBメモリ ・ SDカード ・ デジタルカメラ ・ カードリーダ ・ その他（ ）
					年 月 日	USBメモリ ・ SDカード ・ デジタルカメラ ・ カードリーダ ・ その他（ ）
					年 月 日	USBメモリ ・ SDカード ・ デジタルカメラ ・ カードリーダ ・ その他（ ）
					年 月 日	USBメモリ ・ SDカード ・ デジタルカメラ ・ カードリーダ ・ その他（ ）
					年 月 日	USBメモリ ・ SDカード ・ デジタルカメラ ・ カードリーダ ・ その他（ ）
					年 月 日	USBメモリ ・ SDカード ・ デジタルカメラ ・ カードリーダ ・ その他（ ）
					年 月 日	USBメモリ ・ SDカード ・ デジタルカメラ ・ カードリーダ ・ その他（ ）

・電子媒体を使用する場合は、この台帳に記載すること
・使用の際は、紛失、盗難、コンピュータウイルス等による情報漏えい事故が起きないよう、必要な措置を講じること
・電子媒体の有無確認を定期的に実施すること

電子媒体管理台帳のイメージ（必ずしもこのフォーマットでなくてもよい）

2.6.3 部門共有の電子媒体の社内使用

部門共有の電子媒体を社内で使用する場合

- **使用記録を残すことを推奨**する
- 使用記録は電子である必要はなく、紙による管理でもよい

USBメモリ使用記録一覧表　2018年度

USBメモリ管理No：99081-1-XX　部署

使用日	使用者名	使用場所	使用目的	データの内容	返却予定日	所属長承認欄			所属長確認欄	
						使用許可印	情報保存許可印	外部持出許可印	返却日	返却確認印
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	

・USBメモリを使用とするときは、その都度この一覧表に記載し、所属長の承認を得ること
・使用の際は、紛失、盗難、コンピュータウイルス等による情報漏えい事故が起きないよう、必要な措置を講じること
・使用後は、この台帳に返却日を記載するとともに、速やかにUSBメモリを返却すること

USBメモリ使用記録のイメージ（必ずしもこのフォーマットでなくてもよい）

- ウイルス対策ソフトでスキャンし、問題がないことを確認した上で使用すること

部門共有の電子媒体使用終了時

- 速やかに保存しているデータを消去し、部門で管理している所定の場所に保管する。また、使用記録を残している場合は、返却日、データ消去の有無を記載することを推奨する。

2.6.4 部門共有の電子媒体の持ち出し、移送について

部門共有電子媒体を社外へ持ち出す場合

- 重要情報（電子データ）が保存された電子媒体は**ITSが定めた手段でデータを暗号化**すること。
- 使用記録を管理している場合は必要な情報（使用者、使用場所、格納データの内容等）を残す必要がある。
- 持ち出し先での使用が終わりデータを持ち出す必要がなくなった時点で、速やかに削除（USBメモリ等）、あるいは媒体そのものを読み出せないような手段で処分（ディスクメディア等）すること。

USBメモリ使用記録一覧表　　2018年度

USBメモリ管理No：99081-1-XX　　部署

使用日	使用者名	使用場所	使用目的	データの内容	返却予定日	所属長承認欄 使用許可印	所属長承認欄 情報保存許可印	所属長承認欄 外部持出許可印	所属長確認欄 返却日	所属長確認欄 返却確認印
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	
月　日					月　日				月　日	

・USBメモリを使用とするときは、その都度この一覧表に記載し、所属長の承認を得ること
・使用の際は、紛失、盗難、コンピュータウイルス等による情報漏えい事故が起きないよう、必要な措置を講じること
・使用後は、この台帳に返却日を記載するとともに、速やかにUSBメモリを返却すること

再掲　USBメモリ使用記録のイメージ（必ずしもこのフォーマットでなくてもよい）

移送、送信時の遵守事項

- 重要情報（電子データ）が保存された電子媒体を移送する際は、ITSが定めた手段でデータを暗号化すること。
  - デジタルカメラの記録媒体として使用するSDカードは暗号化対象外

2.6.5 電子媒体の廃棄について

電子媒体を廃棄する場合

- USBメモリ、HDD、SSDの廃棄は各自で行わず、必ずITSへ送付すること。
  - 廃棄方法が適切でない場合、データを復元されてしまう恐れがあるため、ITSが廃棄を代行する。
- USBメモリ以外の重要情報が記録された電子媒体（ディスクメディア等）を廃棄する際は、データが読み出せないようにメディアシュレッダーで処分すること。
- データが読み出せないように破壊することが困難な場合は電子媒体をITSへ送付すること。