【教育コンテンツ】

Orchestrating a brighter world

NEC

池田糖化グループ

リモート接続基準

２０１９年4月1日 第1版

はじめに

本研修の目的

当社（池田糖化工業(株)グループ）では、OEMレシピ（処方）や顧客情報などさまざまな情報を保有し、従業員はこれらの情報を業務に活用しています。

これらの情報は、社内ネットワークを介して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。また、一部の従業員は、モバイルＰＣやスマートデバイスなどのモバイルデバイスを使用し、リモート接続で社内ネットワークに接続することで、いつでも、どこでも、これらの情報を利用することができます。

一方で、情報が盗まれたり書き換えられたりしたというニュースが世間を騒がせることも多々あります。情報を取り扱う以上、このようなリスクは避けられません。

出先から、モバイルデバイスを用いてリモート接続を行う場合、利便性が高い反面、リスクも高いことを意識しなければなりません。

本コースでは、モバイルデバイスを用いたリモート接続において想定されるさまざまな脅威から、社内の重要な情報を守るために、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。

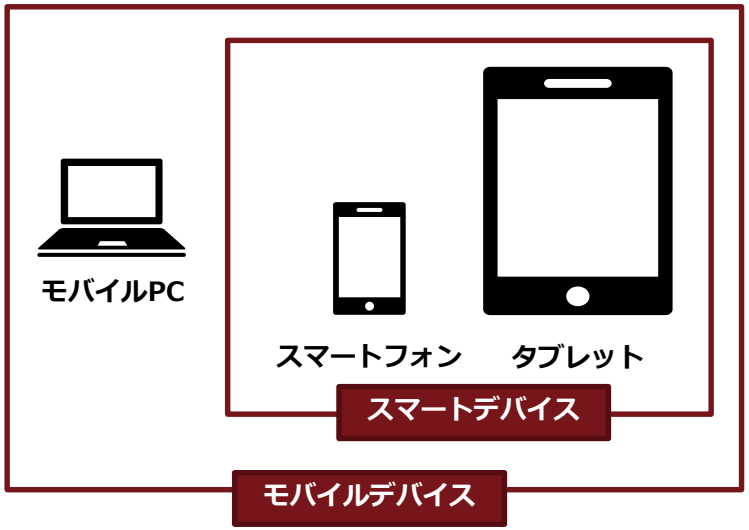
用語チェック　スマートデバイスとモバイルデバイス

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。



目次

第1章　実際の事件・事故

この章では、実際に起きたモバイルデバイスに関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。

1.1 モバイルデバイス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、新千歳空港を利用した際、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。
人材派遣会社	従業員が帰宅途中の電車内で業務用のモバイルＰＣを紛失。警察へ届けたが発見されていない。 所在不明となっているモバイルＰＣには、業務メールや社内資料などをが保存されていた。求人サイトの会員の氏名や住所、電話番号、メールアドレスのほか、施設の名称や住所、電話番号、担当者、メールアドレスなどの情報が含まれている可能性がある。
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。
図書館	移動図書館で利用しているモバイルＰＣが所在不明となった。 所在不明となったモバイルＰＣには、同館で図書館利用カードを作成した利用者の個人情報19万3844件が保存されていた。氏名や電話番号、生年月日、登録者番号、予約、貸出状況などが含まれる。
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 モバイルデバイス持ち出しにともなう事件事故（2/2）

モバイルデバイス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レシピ（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**

- 流出、不正利用される恐れ
- 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.

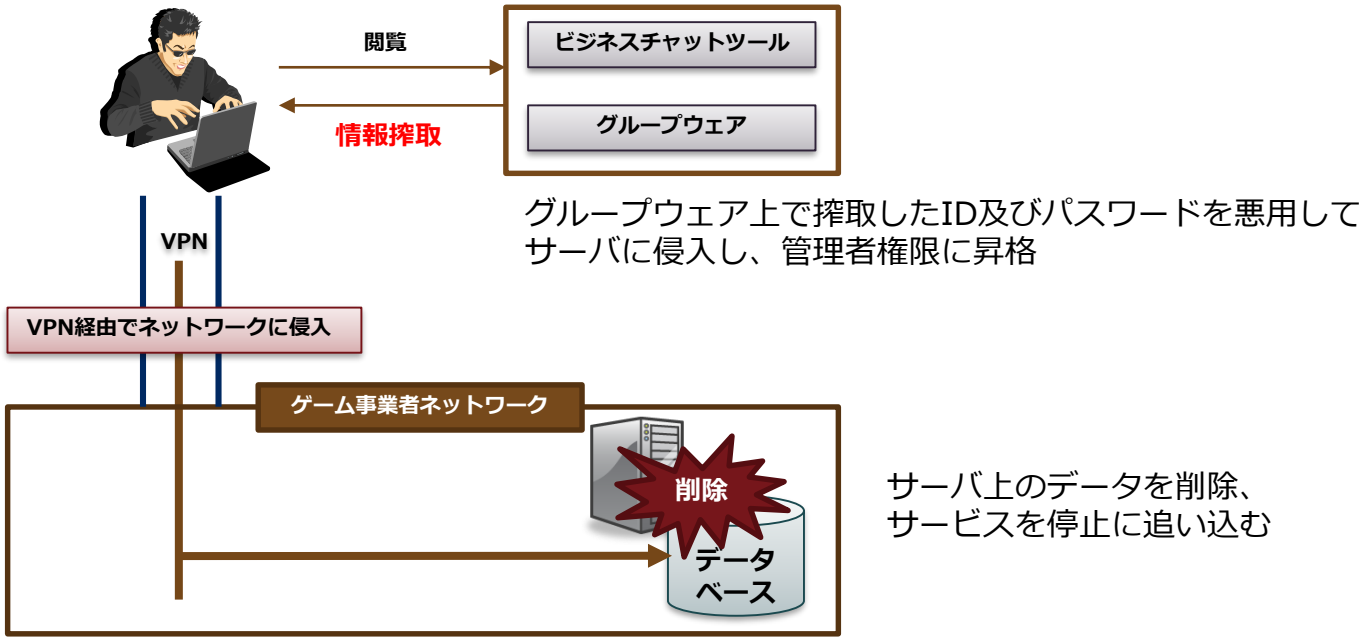
原則として、重要な情報をモバイルデバイスに格納して持ち出してはいけません

- やむを得ず情報を格納して持ち出す際には、上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 VPNが悪用され社内システムが不正アクセス（1/2）

ゲームサービス事業者が運営するサーバがサイバー攻撃を受け、オンラインゲーム13タイトルのサービスが停止

- **VPNで社内ネットワークに侵入され**、サービスに対する妨害が行われた



グループウェア上で搾取したID及びパスワードを悪用して
サーバに侵入し、管理者権限に昇格

サーバ上のデータを削除、
サービスを停止に追い込む

VPNやビジネスチャットツールのアカウント情報の入手方法は不明

- ログから複数の従業員のアカウントが悪用されたことが確認できた
  →アカウントの管理に問題があった

1.2 VPNが悪用され社内システムが不正アクセス（2/2）

パスワードを含むアカウント情報が漏洩すると……

- 社外から侵入される
- そのアカウントの権限でシステムが悪用される
  - 特にVPNが悪用されると、外部から社内ネットワークに侵入されることになる

紹介した事例ではビジネスチャットツールのアカウント情報が異なるシステムで使われた

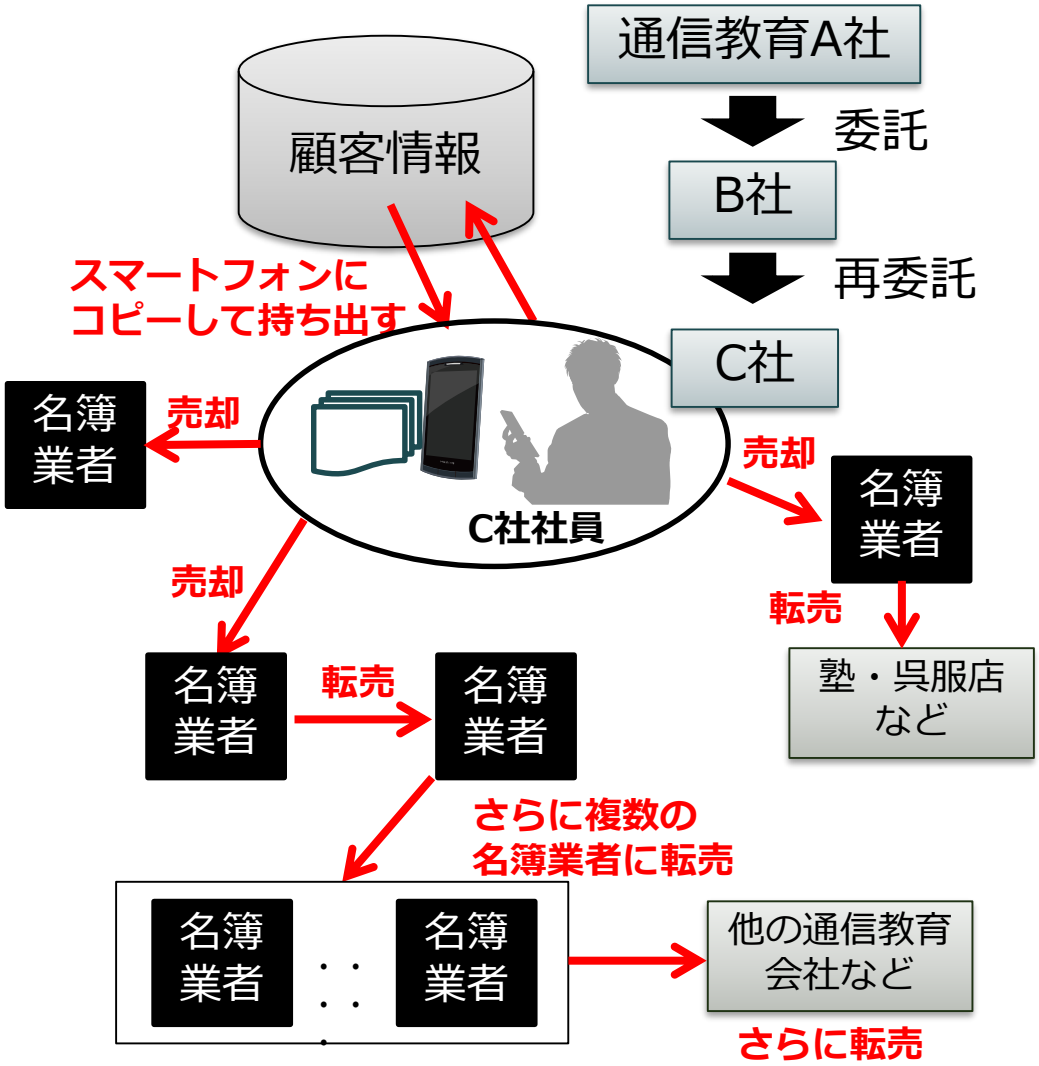
- このような攻撃をパスワードリスト攻撃（アカウントリスティング攻撃）と呼びます

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

パスワードを含むアカウント情報は、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。

1.3 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



1.3 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（スマートフォン、タブレット）**
  - **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。

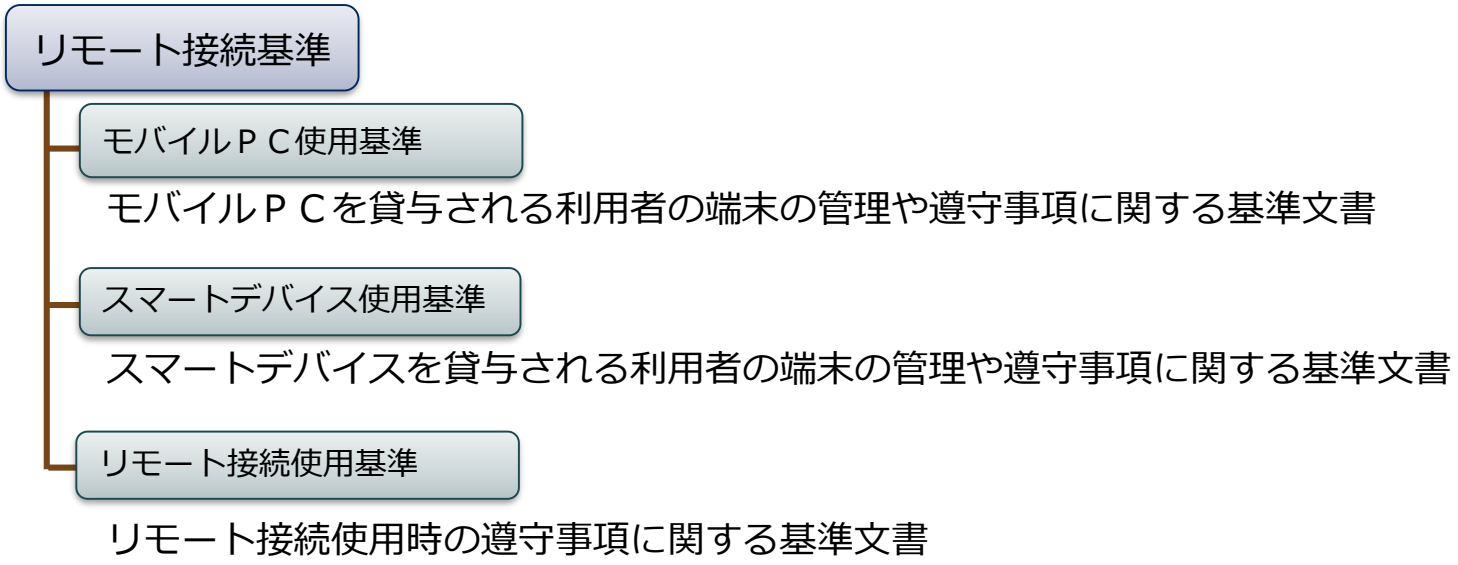
第2章　リモート接続基準

モバイルデバイスを用いてリモート接続を行う場合、利便性が高い反面、リスクも高いため、当社ではルールを定めています。

この章ではそのルールである「リモート接続基準」について解説します。

リモート接続基準とは

リモート接続基準は以下のように複数の文書で構成される



- リモート接続基準はモバイルデバイスやリモート接続を行う上で、事件事故を防ぐために必要な最低限度のルール
  - このルールには、明確な目的や理由があるので、それらを正しく理解することがルール遵守の肝となる
  - ルールが作られた目的や理由を正しく理解した上で、そのルールを守ること

2.1 対象となるモバイルデバイス

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（以下、許可済みモバイルデバイスと呼ぶ）

- 許可済みモバイルデバイスの特徴
  - 会社が管理しているため適切なセキュリティ対策が取られている
  - 必要に応じてMDM（モバイルデバイス管理）用のエージェントを導入している場合があり、これによりITSが使用状況を監視することができる

許可済みモバイルデバイスは業務で会社資産の情報を取り扱うことができる

許可済みモバイルデバイス以外は、適切なセキュリティ対策が取られていない可能性があるため、業務に使用してはならない

許可済みモバイルデバイスには必ず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りません

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

「許可されたことを示すシール」が貼付されていないモバイルデバイスは業務で使用してはならない

2.2 使用可能なソフトウェア（アプリ）

許可済みモバイルデバイスでは使用可能なソフトウェア（アプリ）を制限している

- 主に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）がインストールされることを防ぐため
  - 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
- 正規のソフトウェア（アプリ）であっても、脆弱性と呼ばれる弱点が見つかることがあり、そのまま使うと危険な場合がある
  - **使用可能なソフトウェア（アプリ）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**

使用可能なソフトウェアおよび外部サービス一覧

- **一覧に登録されているソフトウェア（アプリ）に関しては使用可**
  - ただし、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（アプリ）は**条件付きで使用可**とする

「使用可能なソフトウェアおよび外部サービス一覧」に登録されているソフトウェア（アプリ）以外は使ってはならない

使用したいソフトウェア（アプリ）が一覧に存在しない場合は、申請し、許可が得られた後、使うようにする

2.3 使用可能な外部サービス

許可済みモバイルデバイス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

- **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。**

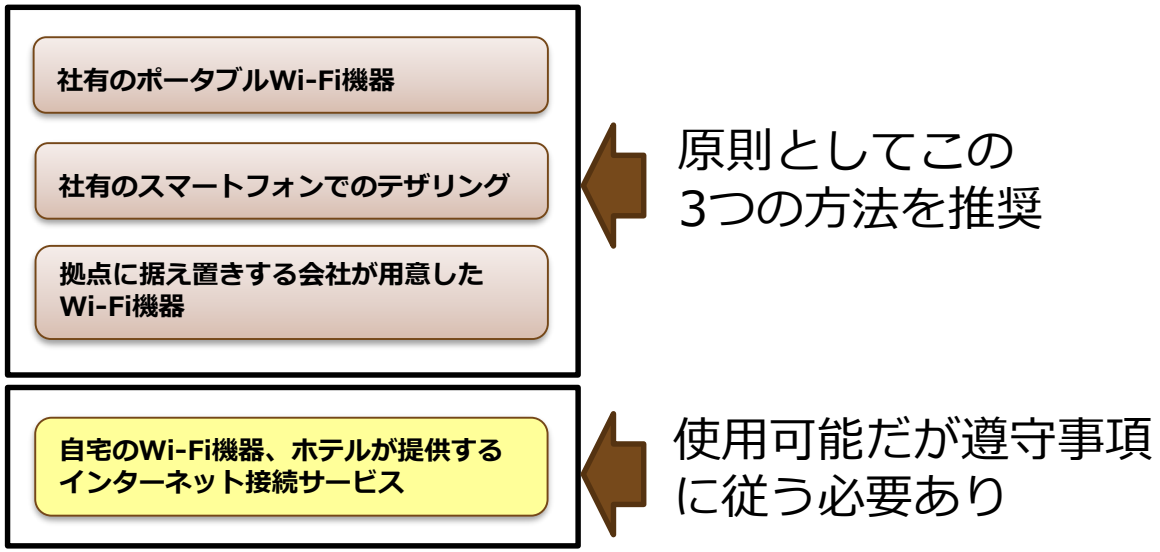
「使用可能なソフトウェアおよび外部サービス一覧」に登録されている外部サービス以外は使ってはいけない

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、使うようにする

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）

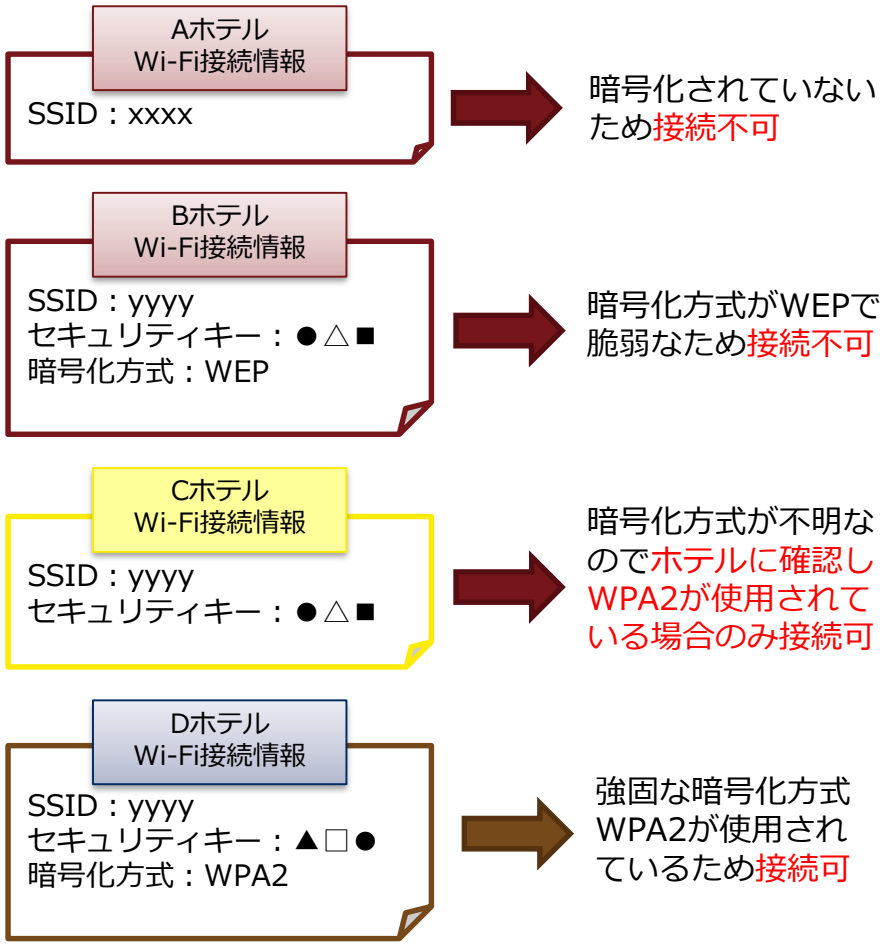
- 許可済みモバイルデバイスをホテル提供のWi-Fiに接続、使用するのは、**やむを得ない場合のみ**とする
  - ITSが提供するリモート接続ソフトウェア以外は使用してはならない

- 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。

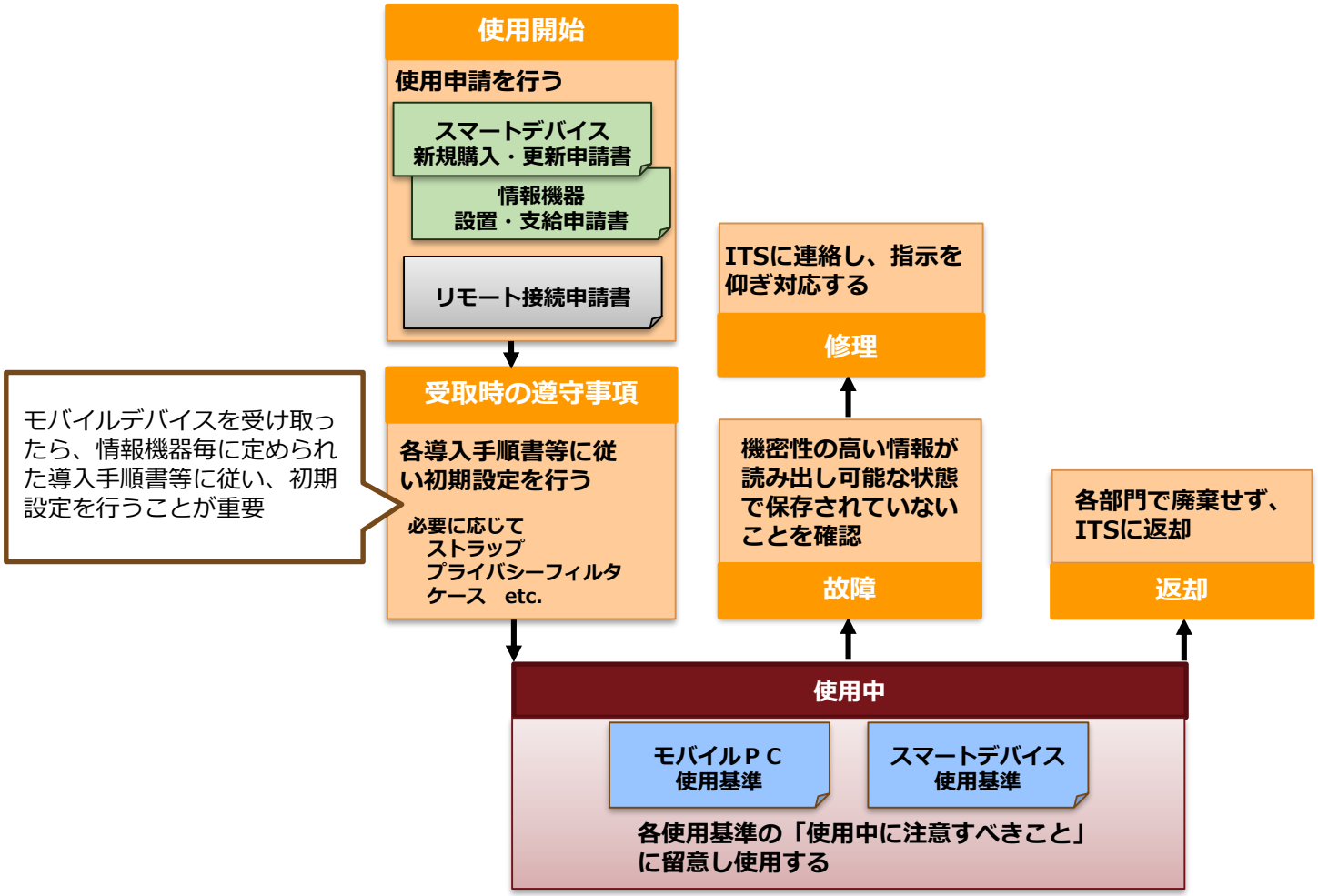
ホテルが使用しているWi-Fiアクセスポイント、またはルータには脆弱性が潜んでいる可能性があることを念頭において使用すること。

- 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管理（1/2）

- 許可済みモバイルデバイスは、使用中はもちろん、貸与開始から返却までの間、**使用者が適切に管理する**必要がある



モバイルデバイスのライフサイクル

2.5　モバイルデバイスの管理（2/2）

モバイルＰＣではパスワード、スマートデバイスではパスコードの設定については以下の遵守事項を必ず守ってください。

パスワードもしくはパスコードはITSの指示に従い、各自が設定すること。

パスワードもしくはパスコードは第三者に開示しないこと。

パスワードもしくは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。

2.5.1　モバイルデバイスのセキュリティ対策（1/2）

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**

2.5.1　モバイルデバイスのセキュリティ対策（2/2）

- 「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　リモート接続使用対象者

リモート接続の使用対象者

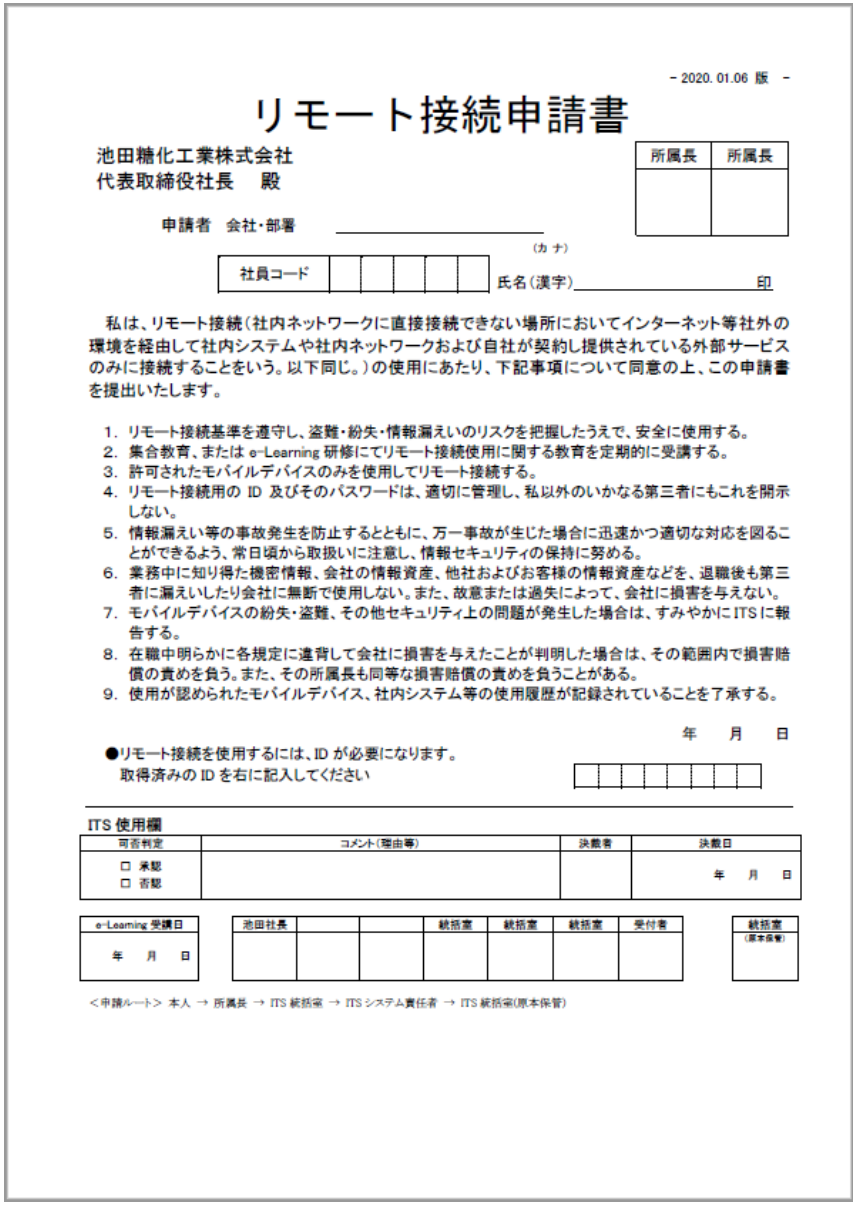
リモート接続を許可する条件として、以下のすべての条件を満たした者とする。

1.「誓約書」を提出した者。
2.所属する部門長からITS へ「リモート接続申請書」を提出された者。
3.集合教育、またはe-Learning 研修にてリモート接続使用に関する教育の受講を完了した者。
4.「IT・セキュリティに対するリテラシー」を有する者。

誰もがリモート接続できるわけではないことをご認識ください。

使用が許可されるには一定レベル以上のＩＴ・セキュリティに対するリテラシーが必要で、本教育（あるいは集合教育）の受講完了も条件となります。また、「リモート接続申請書」の提出も必要です。

参考：リモート接続申請書



－2020.01.06 版－

リモート接続申請書

所属長	所属長

池田糖化工業株式会社
代表取締役社長　殿

申請者　会社・部署 ＿＿＿＿＿＿＿＿

（カナ）

社員コード ＿＿＿＿＿＿　氏名（漢字）＿＿＿＿＿＿＿＿＿＿＿＿印

私は、リモート接続（社内ネットワークに直接接続できない場所においてインターネット等社外の環境を経由して社内システムや社内ネットワークおよび自社が契約し提供されている外部サービスのみに接続することをいう。以下同じ。）の使用にあたり、下記事項について同意の上、この申請書を提出いたします。

1. リモート接続基準を遵守し、盗難・紛失・情報漏えいのリスクを把握したうえで、安全に使用する。
2. 集合教育、または e-Learning 研修にてリモート接続使用に関する教育を定期的に受講する。
3. 許可されたモバイルデバイスのみを使用してリモート接続する。
4. リモート接続用の ID 及びそのパスワードは、適切に管理し、私以外のいかなる第三者にもこれを開示しない。
5. 情報漏えい等の事故発生を防止するとともに、万一事故が生じた場合に迅速かつ適切な対応を図ることができるよう、常日頃から取扱いに注意し、情報セキュリティの保持に努める。
6. 業務中に知り得た機密情報、会社の情報資産、他社およびお客様の情報資産などを、退職後も第三者に漏えいしたり会社に無断で使用しない。また、故意または過失によって、会社に損害を与えない。
7. モバイルデバイスの紛失・盗難、その他セキュリティ上の問題が発生した場合は、すみやかに ITS に報告する。
8. 在職中明らかに各規定に違背して会社に損害を与えたことが判明した場合は、その範囲内で損害賠償の責めを負う。また、その所属長も同等な損害賠償の責めを負うことがある。
9. 使用が認められたモバイルデバイス、社内システム等の使用履歴が記録されていることを了承する。

年　月　日

●リモート接続を使用するには、ID が必要になります。
取得済みの ID を右に記入してください

ITS 使用欄

可否判定	コメント（理由等）	決裁者	決裁日
□ 承認 □ 否認			年　月　日

e-Learning 受講日	池田社長			統括室	統括室	統括室	受付者	統括室（原本保管）
年　月　日								

＜申請ルート＞ 本人 → 所属長 → ITS 統括室 → ITS システム責任者 → ITS 統括室(原本保管)

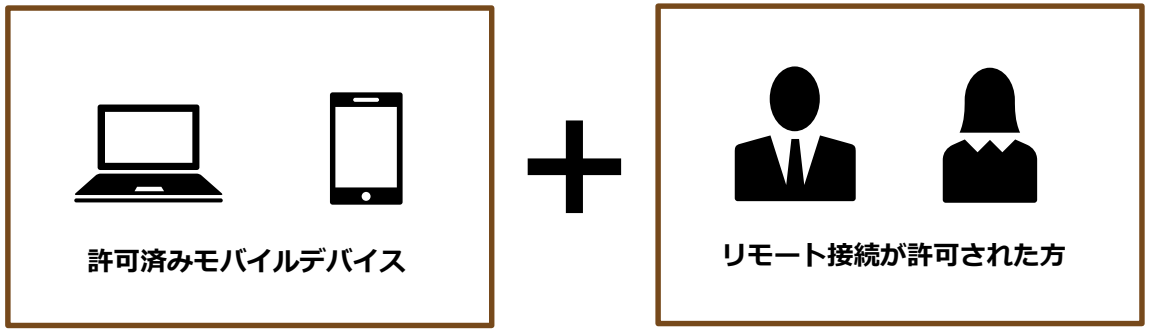
2.7　リモート接続の遵守事項（1/2）

リモート接続使用時は、「リモート接続使用基準」に記載されている遵守事項に注意しながら使用すること

使用を許可された者が、使用を許可されたモバイルデバイスのみを使用してリモート接続を行うこと。

使用を許可された者のみがリモート接続できるように、リモート接続用に付与されたアカウントは、他者に不正利用されることのないよう厳重に管理すること。

リモート接続は、「許可済みモバイルデバイスと許可された人」という組み合わせに対してのみ、使用が許されています。



2.7　リモート接続の遵守事項（2/2）

実際にリモート接続をする場面での遵守事項

公共の場でリモート接続を行う場合、情報漏えいを防ぐために以下の対策を行ったうえで使用すること。

1.マルウェア対策ソフトなどが接続可能な状態でリモート接続すること。
2.リモート接続使用時は、部外者が不正に閲覧できない状態にすること。
3.やむを得ず離席する際は、モバイルデバイスの不正利用を防止すること。

リモート接続時にはあらためてマルウェア対策ソフトが有効な状態かどうか確認しましょう。（iPhone、iPadはマルウェア対策ソフトがありませんので対象外とします）

「2.5.1　モバイルデバイスのセキュリティ対策」の「社外持ち出し時の注意事項」でも、「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。」としておりますが、リモート接続時は一層の注意を払ってください。

万が一の事件・事故に備え、速やかに対応できるよう、以下の手順や連絡先を把握しておくこと。

1.モバイルデバイスの盗難・紛失の疑いがある場合、速やかにITSへ報告する。
2.パスワード紛失、マルウェア感染、重要情報の漏えいなどの疑いがある場合、速やかにITSへ報告する。

第3章　これだけは守ろう（行動指針）

リモート接続基準は、モバイルデバイスやリモート接続を行う上で、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。

3.1　4つの行動指針（1/3）

当社では、モバイルデバイスやリモート接続を行う上で以下の4つの行動指針を定めている

1.必要以上に、業務情報を社外に持ち出さないように注意する

2.むやみに、社外で業務情報を扱わないように注意する

3.各自が守る意識をもって行動する

4.セキュリティ対策を継続する

3.1　4つの行動指針（2/3）

1.必要以上に、業務情報を社外に持ち出さないように注意する

- まずは、**できるだけ社外に業務情報を持ち出さない**ようにしましょう。
- 業務情報の持ち出しは、商談等でプレゼンテーション資料を扱うなど、やむを得ず持ち出さなければならない場合のみに限定しましょう。可能なら、使用可能な外部サービスを使用するなど、**モバイルデバイスのローカルには極力格納しない**ようにしましょう。

  モバイルデバイスをローカルに格納する場合は、商談が完了するなど**必要がなくなった時点で速やかに削除してください。**モバイルデバイス上にいつまでも業務情報を保存したままにしないよう気をつけましょう。

  また、**許可されたクラウドサービスに関しても同様です。**必要がなくなった時点で速やかに削除してください。資料をいつまでもクラウドサービス上に置いたままにしないよう注意してください。クラウドサービスの使用においては、各サービスのルールを守って使用してください。

2.むやみに、社外で業務情報を扱わないように注意する

- むやみに、**社外で業務情報を扱わないよう**注意してください。
- 社外でモバイルデバイスを使用して業務を行う場合、後ろや横から盗み見される可能性があります。「意図しない人による閲覧」を考慮し、極力、社外では業務情報を使用しないようにしましょう。特に、他に人がいる場所で業務を行う場合は注意が必要です。
- やむを得ず、使用する際は「意図しない人による閲覧」を防ぐようにしましょう。

3.1　4つの行動指針（3/3）

3.各自が守る意識をもって行動する

- モバイルデバイスおよびリモート接続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。
- モバイルデバイス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。

4.セキュリティ対策を継続する

- モバイルデバイスやリモート接続の使用者は、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。最新のリモート接続基準を参照し、ルールに沿って行動するようにしてください。