コロナ時代のセキュリティ動向と
テレワーク利用時の対策

総務省　サイバーセキュリティ統括官室
参事官補佐
梅城　崇師

自己紹介

2007年総務省入省。
2013年内閣サイバーセキュリティセンター参事官補佐。
2016年から再び総務省にて、電波行政・放送行政・電気通信事業行政に携わり、
2019年より現職（サイバーセキュリティ統括官室 参事官補佐）。

情報処理安全確保支援士

2016年10月に創設された
サイバーセキュリティ分野唯一の国家資格
全国で約２万人が活躍

第019712号

各府省庁対抗による競技形式のサイバー攻撃対処訓練
「NATIONAL 318(CYBER) EKIDEN 2017」で優勝（総務省）

1. 最新のサイバーセキュリティ動向

2. テレワークにおけるセキュリティ確保

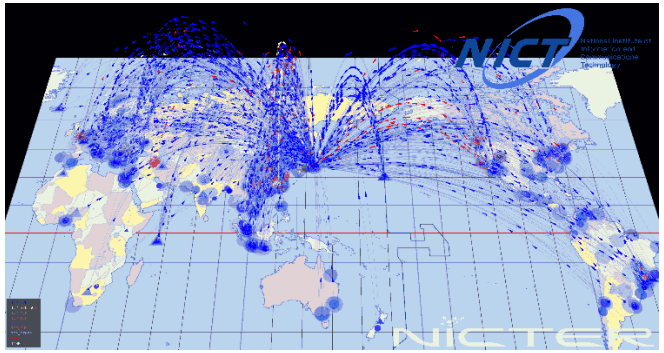
3. 無線LAN（Wi-Fi）の利用・提供におけるセキュリティ確保

4. 総務省におけるその他の取組

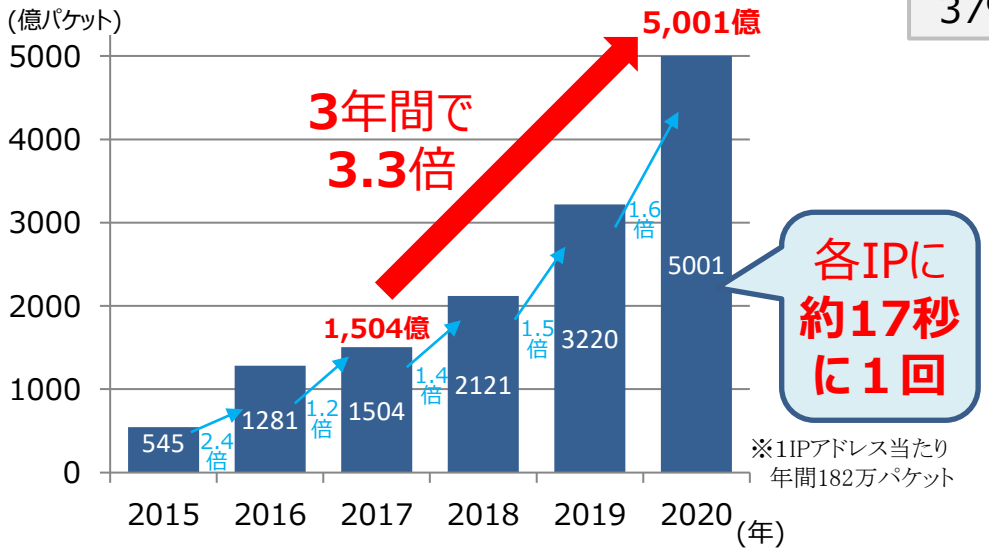
NICTERによるサイバー攻撃観測

➢ 国立研究開発法人情報通信研究機構(**NICT**)では、大規模サイバー攻撃観測網である**NICTERにおいて、未使用のIPアドレス30万個(ダークネット)を活用**し、グローバルに**サイバー攻撃の状況を観測。**

NICTERにより観測されるサイバー攻撃の様子

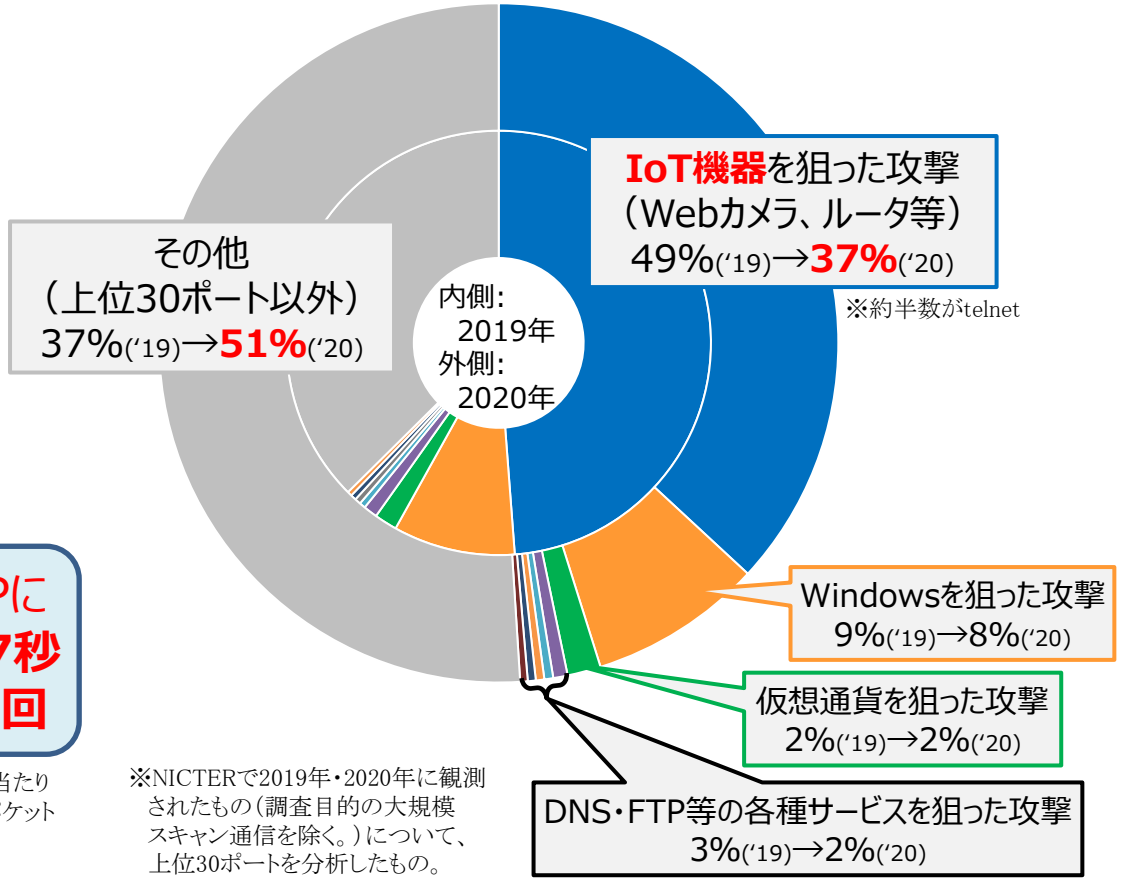


NICTERで１年間に観測されたサイバー攻撃関連の通信数



NICTERにより観測された通信の内容（上位30ポートの分析）

✓ **IoT機器を狙った攻撃が依然としてトップ**
✓ **攻撃(対象ポート)が年々多様化**



※NICTERで2019年・2020年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位30ポートを分析したもの。

IoT機器がサイバー攻撃の対象として狙われやすい理由

➢ IoTの進展が企業活動や製品・サービスのイノベーションを加速する一方で、IoT特有の性質と想定されるリスクをもつことから、これらの性質とリスクを踏まえたセキュリティ対策を行うことが必要。

1）脅威の影響範囲・影響度合いが大きい

攻撃を受けると、ネットワークを介してシステム・サービス全体へその影響が波及（自動車・医療等における致命的影響等も存在）

2）IoT機器のライフサイクルが長い

工場の制御機器等をはじめ10年以上の長期にわたって使用され、構築・接続時に適用したセキュリティ対策が危殆化

3）IoT機器に対する監視が行き届きにくい

画面がなく問題の発生がわかりづらい上に、人目が行き届きにくく勝手なネットワーク接続をされかねない

4）IoT機器側とネットワーク側の環境や特性の相互理解が不十分である

IoT機器の運用を担う制御系のチームと、情報ネットワーク系のチームの双方でセキュリティ要件の整合をとらなければ、必要な安全性等をみたせない

5）IoT機器の機能・性能が限られている

適切な暗号等のセキュリティ対策を適用できない場合が存在

6）開発者が想定していなかった接続が行われる可能性がある

閉域網として設計された後でネットワーク接続が実施されるなど、開発者が当初想定していなかった使われ方をする場合に影響が発生

（出展：IoTセキュリティガイドラインver1.0　平成28年7月　IoT推進コンソーシアム・総務省・経済産業省）

サイバー攻撃の脅威の増加

➢ 新型コロナへの対応として、テレワークの普及拡大や社会全体のデジタル・トランスフォーメーション（DX）が進みつつある中、サイバー攻撃も増加。

４月　国内高校の半数が利用するClassi社が**不正アクセス**を受け、**IDや暗号化パスワード等が流出**した可能性が判明。

５月　NTTコミュニケーションズ従業員の**テレワーク環境(仮想デスクトップ)に係るアカウント及びパスワードが窃取**され、**顧客情報（防衛省等の政府機関を含む）が流出**した可能性が判明。

６月　ホンダが**サイバー攻撃**を受け、**世界の９工場で生産を一時停止**。

７月　Twitter社で**ソーシャルエンジニアリング**により社内ツールが不正利用され、詐欺投稿が行われ、**データも流出**した可能性が判明。

８月　国内数十社において、**VPN機器の脆弱性を悪用した不正アクセス**が行われVPN接続用のパスワードなどが流出した可能性が判明。

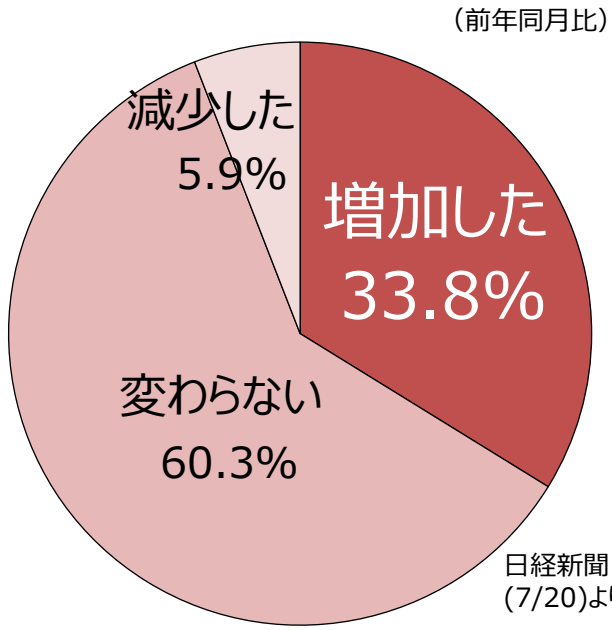
９月　ドコモ口座が悪用され、第三者が**不正に入手した口座番号、暗証番号等を使用**した口座振替による**不正出金**が判明。

10月　原子力規制委員会が、**不正アクセス**を受け、メール等のやりとりを含む**外部とのアクセスを遮断**。

11月　カプコンが、**オーダーメイド型ランサムウェアによる標的型攻撃**を受け、**個人情報・人事情報・開発資料等が流出**した可能性が判明。

12月　楽天が、**クラウド型**営業管理システムの**設定不備**を突かれ、**個人情報・営業情報等にアクセス**された可能性が判明。

2020年４月以降に受けたサイバー攻撃



社内システム・設備の停止や提供しているサービスの停止といった企業活動そのものに影響する攻撃が増加

（piyolog、各社公表資料、各種報道等より総務省作成）

中小企業に対するサイバー攻撃

- 中小企業であっても実際にサイバー攻撃の標的となっている。
- 大企業のセキュリティ対策が進展するにつれ、取引関係にある中小企業を踏み台にするパターンも。
- 自社には狙われる情報がない、という考え方はもはや通用しない。（他社に迷惑→損害賠償責任も）

【中小企業におけるサイバー攻撃対策に関するアンケート調査】（大阪商工会議所）
（期間：2017年３～６月／回答数：315社／関西の中小企業等）https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf

✓中小企業であっても、**標的型攻撃メールの受信（18%）**や**ランサムウエアによる被害（７%）**にあっている

○具体的な被害例
- ランサムウエアによる感染で、１部署のデータ全て暗号化された
- なりすましメールの添付資料を開いたことで、情報が漏洩した
- 自社ホームページがアクセス不能になり、修復に１カ月ほどかかった
- メールアカウントが乗っ取られた
- ホームページのセキュリティーホールを突かれ、悪意のあるリンクを埋め込まれた

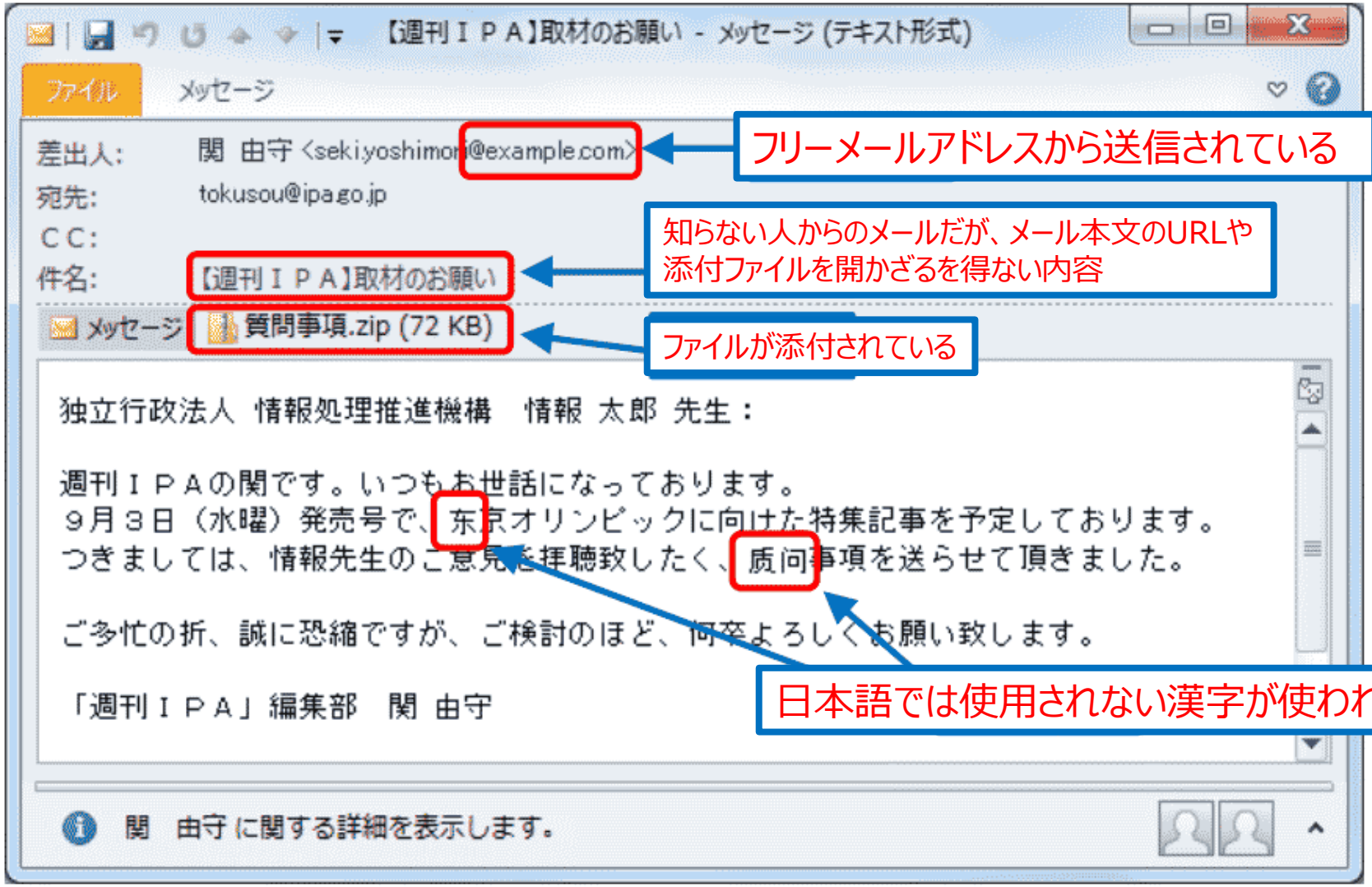
【サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査】（大阪商工会議所）
（期間：2019年２～３月／回答数：118社／全国の従業員100人以上の企業）https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190510sc.pdf

✓「**取引先がサイバー攻撃被害を受け、それが自社に及んだ経験**」がある企業は**４社に１社（25%）**。
その結果、「情報漏洩」（５社）、システムダウン（３社）、データ損壊（３社）など実害も出ている。

✓「**取引先がもしサイバー攻撃を受け、その被害が自社にも及んだ場合**、採り得る対処」としては、「口頭や文書での注意喚起」（51%）、「**損害賠償請求**」（**47%**）、「セキュリティソフト・ハード導入の依頼／要件化」（37%）、「**取引停止**」（**29%**）など。

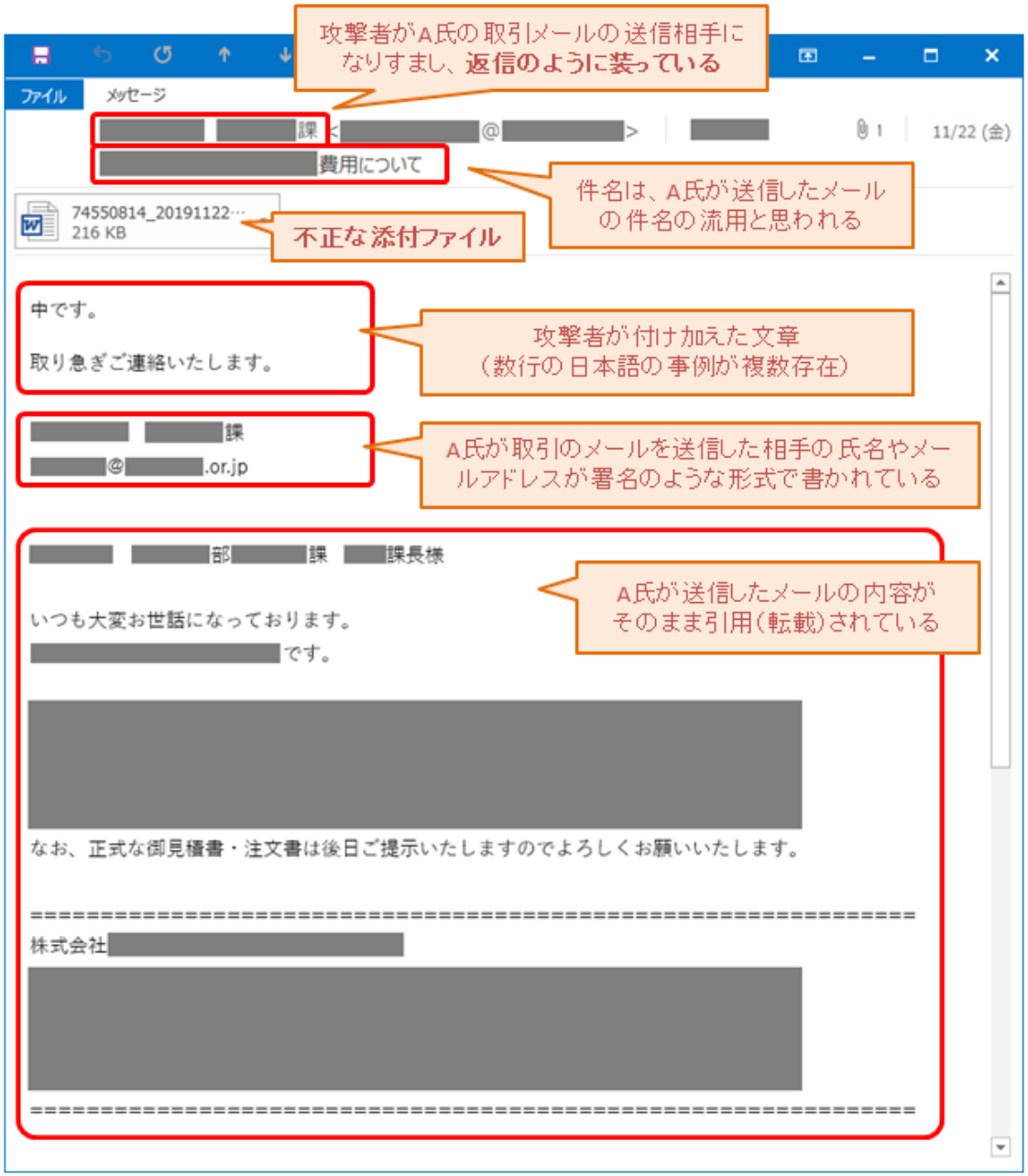
✓「中小企業は今後どうしていくべきか」については、「中小企業自身が自衛すべき」（60%）、「国や自治体が支援すべき」（45%）、「IT企業や損保会社が安価・簡便なセキュリティサービスを提供すべき」（30%）など。

不審メール



独立行政法人情報処理推進機構　IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」（2015年1月9日）を加工

Emotet（エモテット）



Emotet（エモテット）

- ✓ 世界的な被害を出すマルウェアの一種
  （マルウェア＝不正な動きをするソフトウェア）
- ✓ 国内でも2019年から大流行
  （2014年に最初に確認され機能追加）

1. メールの**添付ファイル**か**URLダウンロード**で感染
2. 感染すると攻撃者からの指示を受け様々な悪さをすることが可能
   （ファイルを暗号化したり、情報を漏えいさせたり等）
3. 過去メール、アドレス帳、ログイン情報等を攻撃者が収集
4. なりすましメールが**非常に巧妙**
   - ・実在の人からのメール
   - ・本人のアカウントから送信されること
   - ・実際のやりとりメールも利用

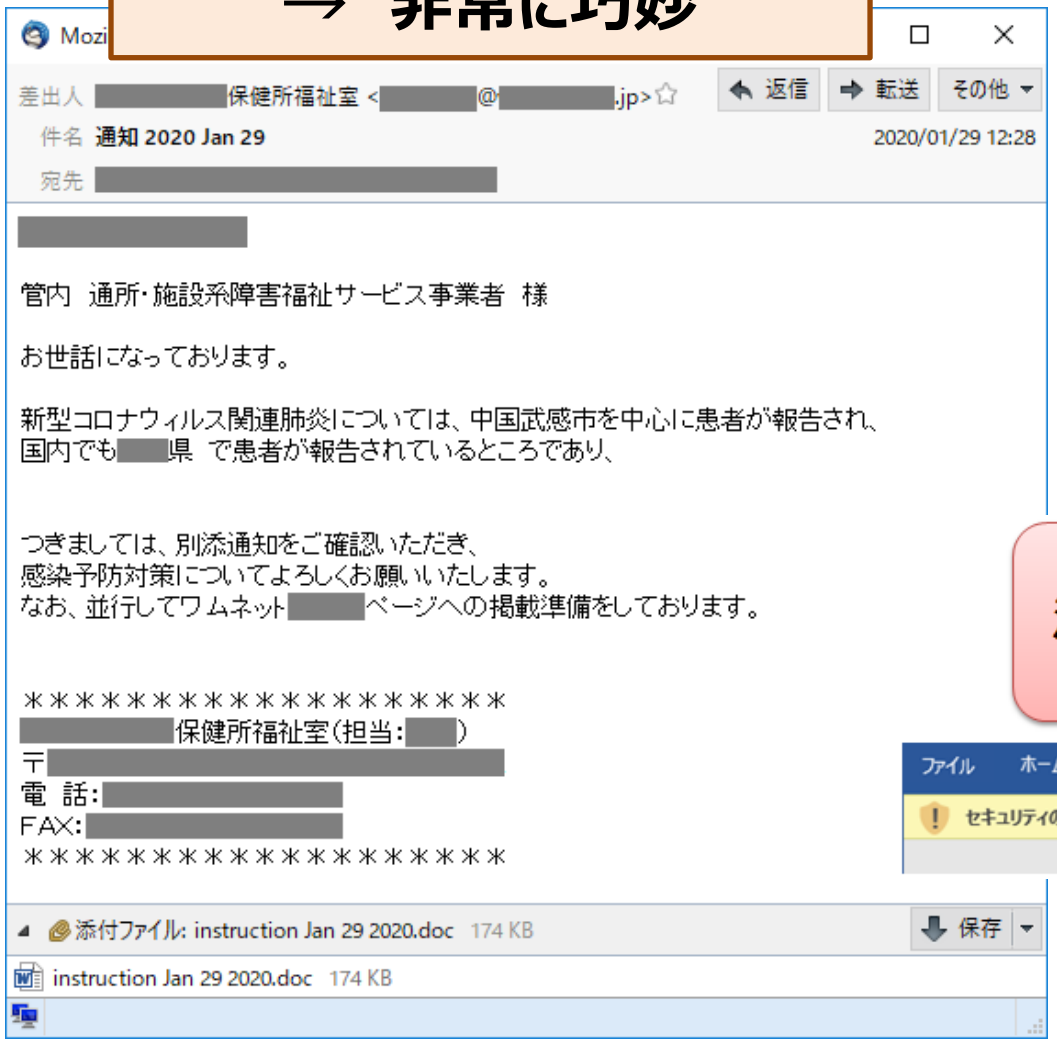
「「Emotet」と呼ばれるウイルスへの感染を狙うメールについて」より引用
https://www.ipa.go.jp/security/announce/20191202.html

Emotet（エモテット）

✓ コロナの流行当初時にコロナの話題

✓ 保健所から、管轄事業者宛を装う

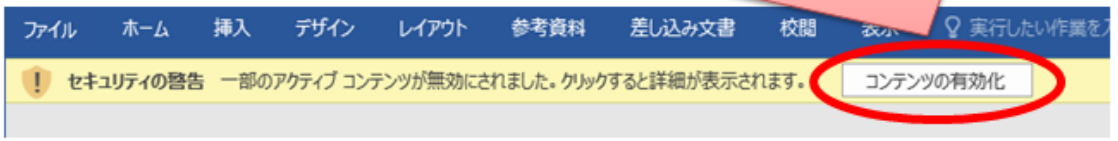
→ **非常に巧妙**



✓ Emotetが仕込まれた添付ファイルや
ダウンロードさせられたファイルは、
「マクロ」というプログラムが埋め込まれている

✓ **マクロを実行せず、送信元に確認を！**

注意！ このパソコン上で、<u>文書ファイルに埋め込まれている</u>
<u>マクロ(プログラム)等の実行を許可する</u>という意味の
ボタン。このボタンをクリックすると、悪意のあるマクロ
が動作し、ウイルスに感染させられてしまう。



「「Emotet」と呼ばれるウイルスへの感染を狙うメールについて」より引用
https://www.ipa.go.jp/security/announce/20191202.html

1. 最新のサイバーセキュリティ動向

2. テレワークにおけるセキュリティ確保

3. 無線LAN（Wi-Fi）の利用・提供におけるセキュリティ確保

4. 総務省におけるその他の取組

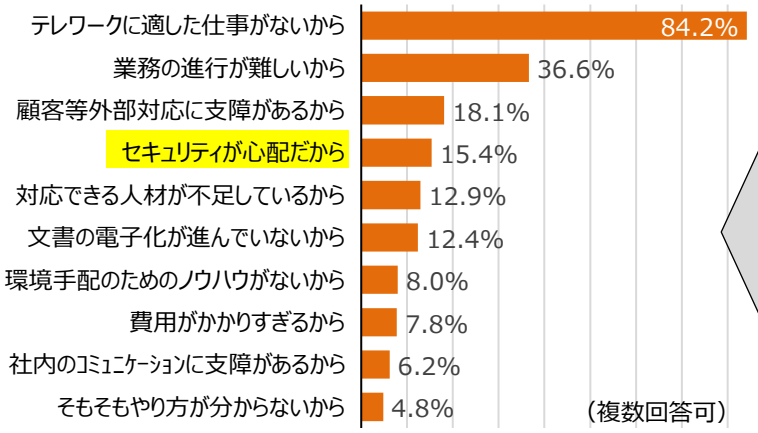
テレワークセキュリティに関する実態調査結果①

➢ 企業等におけるテレワークに関するセキュリティ等の実態を把握するための調査をWebアンケートにより実施。
（地域：全国　期間：2020.7.29-8.24　手法：調査票郵送・Web回答　対象数：30,000（従業員10名以上）　回答数：5,433（テレワーク実施企業1,569））

調査結果の詳細は「総務省　テレワーク　セキュリティ」で検索

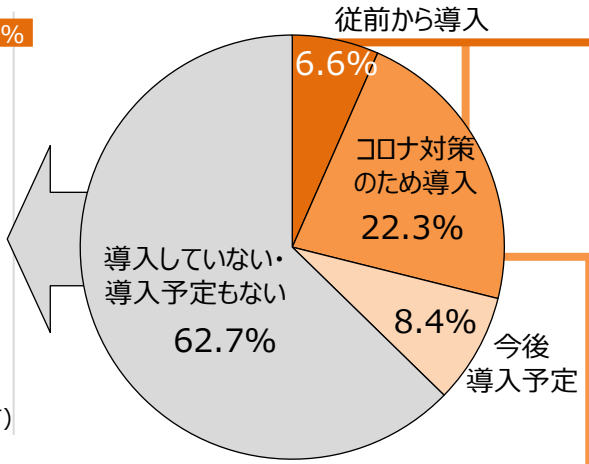
テレワークを導入しない理由

（n=3,406：テレワーク未導入企業）



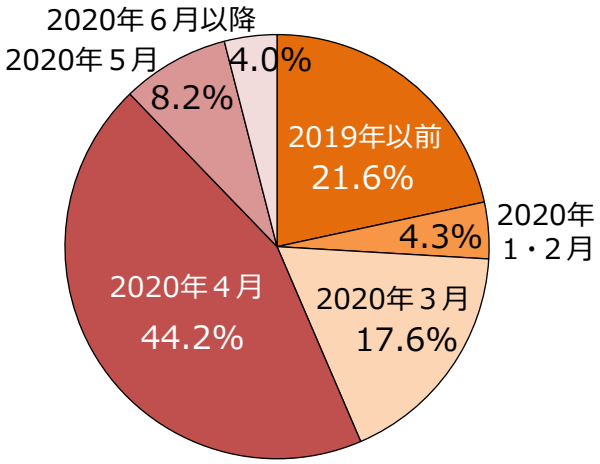
テレワークの導入状況

（n=5,433）



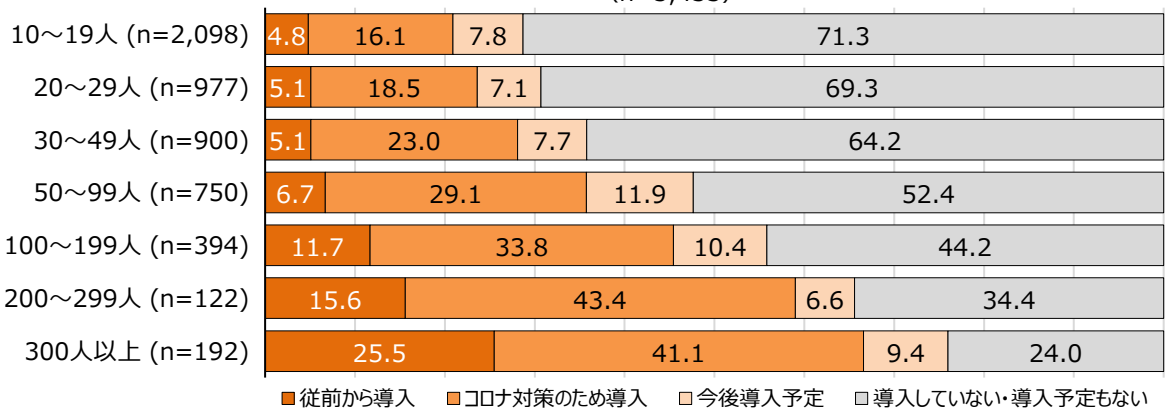
テレワークの導入時期

（n=1,569：テレワーク導入企業）



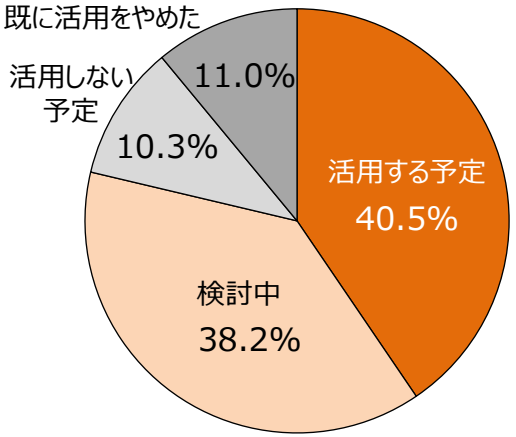
テレワークの導入状況（従業員規模別）

（n=5,433）



新型コロナ収束後のテレワーク活用予定

（n=1,209：コロナ対策のためテレワーク導入した企業）



テレワークセキュリティガイドラインの改定

- 総務省では従来から「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示してきた。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、**2020年９月**には、**実践的かつ具体的で分かりやすい内容のチェックリスト**を作成・公表。
- 「**テレワークセキュリティガイドライン**」についても、テレワークを取り巻く環境やセキュリティ動向の変化に対応するため全面的な改定検討を行ってきており、改定案について意見公募を実施中。（2/15～3/5）

テレワークセキュリティガイドライン

（2018年４月　第４版）

2004年12月初版
2006年４月第２版
2013年３月第３版

【想定読者像】

- ✓ システム管理者のほか経営層や利用者を幅広く対象
- ✓ 専任の担当や部門が存在
- ✓ 基本的なIT用語は仕組みとして理解しているレベル
- ✓ 基本的なシステム設定作業は、補助解説なく実施可能

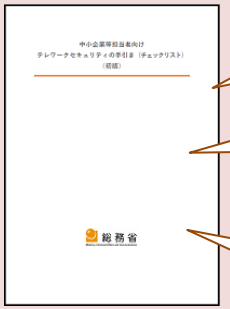
追加

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)

（2020年９月　初版）

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本的なIT用語は聞いたことがあるレベル
- ✓ 基本的なシステム設定作業は検索しながら実施可能



テレワーク方式を特定し、その方式に**対応するチェックリストを確認**

チェックリストは**最低限のセキュリティを確実に確保**してもらうためのものに限定

テレワーク用ソフトについて、**設定解説資料を作成**し具体的設定を解説

全面改定

【テレワーク環境・セキュリティ動向の変化】

- ✓ テレワークは「一部の従業員」が利用するものから、Web会議を含め、一般的な業務・勤務形態に
- ✓ システム面でも、クラウドサービスの普及やスマートフォン等の活用が進むなど、アーキテクチャが変化
- ✓ 標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況も発生

【ガイドライン改定の主要なポイント】

- ✓ テレワーク方式を再整理した上で、テレワークによって実現する業務内容や、セキュリティ統制の容易性等から、適した方式を選定するフローチャートを掲載。
- ✓ 経営者・システム管理者・従業員の立場それぞれにおける役割を明確化。
- ✓ 採るべきセキュリティ対策の分類や内容を全面的に見直し
- ✓ テレワークセキュリティに関連するトラブルについて、具体的事例を含め全面見直し
  （事例紹介のほか、セキュリティ上留意すべき点や、採るべき対策についても明示）

テレワークセキュリティガイドラインとチェックリストの違い

<table>
<tr><th></th><th>テレワークセキュリティガイドライン
の想定読者像</th><th>中小企業等担当者向けテレワークセキュリティ
の手引き（チェックリスト）の想定読者像</th></tr>
<tr><td>対象属性</td><td>システム・セキュリティ管理者のほか
経営者やテレワーク勤務者を幅広く対象</td><td>システム・セキュリティ管理者</td></tr>
<tr><td>セキュリティ
予算</td><td>外部委託コストは
必要に応じて捻出しうるレベルも対象</td><td>外部委託コストの捻出は難しいレベル</td></tr>
<tr><td>セキュリティ
推進体制</td><td>専任の担当・担当部門が
存在する組織も対象</td><td>専任は存在しない</td></tr>
<tr><td>セキュリティ
リテラシ</td><td>「適切に…」等の読者に解釈を委ねるような
抽象的な要求に対して、
対応内容を検討・判断し、対策を実行できる</td><td>「適切に…」等の読者に解釈を委ねるような
抽象的な要求だけでは、
対応すべき内容がわからない</td></tr>
<tr><td rowspan="2">ITリテラシ</td><td>VPN・フィルタリング・アンチウイルス等の
基本的なIT用語は
仕組みとして理解している</td><td>VPN・フィルタリング・アンチウイルス等の
基本的なIT用語は聞いたことがあり、
利用シーンがイメージできる</td></tr>
<tr><td>システム設定作業は、基本的な内容であれば、
無理なく行うことができる</td><td>システム設定作業は、基本的な内容であれば、
インターネット検索によって調べながら
行うことができる</td></tr>
<tr><td>対象とする
セキュリティ対策
のイメージ</td><td>
<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="3">難易度</th></tr>
<tr><th>低</th><th>中</th><th>高</th></tr>
<tr><td rowspan="3">重要度</td><td>高</td><td>基本</td><td>基本</td><td>発展</td></tr>
<tr><td>中</td><td>基本</td><td>基本</td><td>発展</td></tr>
<tr><td>低</td><td>基本</td><td>基本</td><td>発展</td></tr>
</table>
</td><td>
<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="3">難易度</th></tr>
<tr><th>低</th><th>中</th><th>高</th></tr>
<tr><td rowspan="3">重要度</td><td>高</td><td>◎</td><td>○</td><td>－</td></tr>
<tr><td>中</td><td>○</td><td>○</td><td>－</td></tr>
<tr><td>低</td><td>－</td><td>－</td><td>－</td></tr>
</table>
</td></tr>
</table>

意見募集中であり、記載内容は変わる場合があります。

手引きの構成とチェックリスト作成に当たっての考え方

- 手引きは、主に第１部・第２部から構成。
  - ✓ **第１部**で、本手引きの読者は自分の組織が採用する**テレワーク方式を確認・特定**
  - ✓ **第２部**では、第１部で特定した**テレワーク方式に対応するチェックリストを確認**
- チェックリストについては、セキュリティ確保を図る上で**優先対応**すべきものが**わかりやすいよう配慮**
  - ✓ セキュリティ**重要度**が**高**く、対策**実施**が**易**しいものは「◎」、**それ以外**を「○」として、優先順位をつけて整理
  - ✓ セキュリティ**重要度**が**低**いものや、対策**実施**が**難**しいものは、チェックリスト**対象外**として整理
- テレワークで**広く使われているソフトウェア**については、具体的な設定例として、**設定解説資料を作成**※
  - ※ 手引きの初版では、オンライン会議システムとして、Microsoft Teams、Cisco WebEx Meeting、Zoomの３製品分の解説資料を作成（第２版に向けて、順次拡張していく予定）

	第１部	第２部	参考
手引きの構成	1 はじめに 2 テレワーク方式の確認 3 テレワーク方式の解説 4 テレワーク環境で想定される脅威の解説	1 テレワーク方式ごとの**セキュリティ対策チェックリスト** 2 セキュリティ対策チェックリストの設定例一覧 →**補足文書として設定解説資料を用意** 3 テレワーク環境のセキュリティ対策と想定脅威一覧	• 用語集 • テレワークセキュリティに関する参考情報
読者の行動	• 自社に適合しているテレワーク方式の確認・特定 • 自社のテレワーク環境において想定される脅威の理解	• 第１部で特定したテレワーク方式に対応したチェックリストの特定 • 当該チェックリスト記載のセキュリティ対策実施 • 各セキュリティ対策に紐づく脅威の確認	（下記を必要に応じて実施） • 本書記載の用語の理解 • 参考文献等の閲覧 • 困った場合の問合せ先

テレワークセキュリティガイドラインの改定

- 総務省では従来から「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示してきた。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、**2020年９月**には、**実践的かつ具体的で分かりやすい内容のチェックリスト**を作成・公表。
- 「**テレワークセキュリティガイドライン**」についても、テレワークを取り巻く環境やセキュリティ動向の変化に対応するため全面的な改定検討を行ってきており、改定案について意見公募を実施中。（2/15～3/5）

テレワークセキュリティガイドライン

（2018年４月　第４版）

2004年12月初版
2006年４月第２版
2013年３月第３版

【想定読者像】

- ✓ システム管理者のほか経営層や利用者を幅広く対象
- ✓ 専任の担当や部門が存在
- ✓ 基本的なIT用語は仕組みとして理解しているレベル
- ✓ 基本的なシステム設定作業は、補助解説なく実施可能

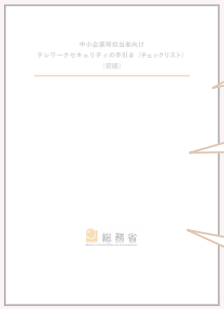
追加

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)

（2020年９月　初版）

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本的なIT用語は聞いたことがあるレベル
- ✓ 基本的なシステム設定作業は検索しながら実施可能



テレワーク方式を特定し、その方式に**対応するチェックリストを確認**

チェックリストは**最低限のセキュリティを確実に確保**してもらうためのものに限定

テレワーク用ソフトについて、**設定解説資料を作成**し具体的設定を解説

全面改定

【テレワーク環境・セキュリティ動向の変化】

- ✓ テレワークは「一部の従業員」が利用するものから、Web会議を含め、一般的な業務・勤務形態に
- ✓ システム面でも、クラウドサービスの普及やスマートフォン等の活用が進むなど、アーキテクチャが変化
- ✓ 標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況も発生

【ガイドライン改定の主要なポイント】

- ✓ テレワーク方式を再整理した上で、テレワークによって実現する業務内容や、セキュリティ統制の容易性等から、適した方式を選定するフローチャートを掲載。
- ✓ 経営者・システム管理者・従業員の立場それぞれにおける役割を明確化。
- ✓ 採るべきセキュリティ対策の分類や内容を全面的に見直し
- ✓ テレワークセキュリティに関連するトラブルについて、具体的事例を含め全面見直し
  （事例紹介のほか、セキュリティ上留意すべき点や、採るべき対策についても明示）

テレワークセキュリティガイドラインの改定（案）概要

第４版（2018年４月）

はじめに

✓ セキュリティ対策の必要性や本ガイドラインの位置付け等を記載。

1. テレワークにおける情報セキュリティ対策の考え方

✓「ルール」「人」「技術」のバランスのとれた対策の必要性を説明。
✓ テレワークの方式を6種類に整理し、その概要と対策の考え方を簡単に説明。
✓ 私用端末利用（BYOD）やクラウドサービス利用の留意点を追加。
✓「経営者」「システム管理者」「テレワーク勤務者」のそれぞれの立場について簡単な説明。

2. テレワークセキュリティ対策のポイント

✓「経営者」「システム管理者」「テレワーク勤務者」の類型ごとに実施すべき対策を記載。
✓ 第3版で33項目だったものを、計43項目に再編。（無線LANの脆弱性対策（VPNの利用、https接続等）やSNS利用の留意事項等を追加）
✓ 対策事項は、6個の脅威カテゴリに分類。

3. テレワークセキュリティ対策の解説

✓「2. テレワークセキュリティ対策のポイント」で明示した内容について、対策分野ごとに詳細に解説。
✓「実施するべき基本的な対策」（基本的対策事項）と、「実施することが望ましい対策」（推奨対策事項）に分けて解説。
✓「トラブル事例や対策」や「コラム」を追加。

※上記のほか、「用語集」「参考リンク集」がある。

分割

- テレワーク**環境の変化**（感染症対応）等を追加
- **想定読者（チェックリストとの差異）**の項目を追加
- 経営者・管理者・勤務者の**役割を具体的に列挙**（適切な役割分担の重要性についても強調）
- テレワークやセキュリティの環境変化を踏まえ、
  - **クラウドサービス**の利用上の**考慮事項を追記**
  - サイバー攻撃の高度化を踏まえ、**ゼロトラストセキュリティ**に関する項目を追加
- **方式選定にもガイドラインは活用**されているため、
  - テレワーク方式の解説を章として独立・増強
  - **選定フローチャート**や**特性比較表**を新規作成
- テレワークの利用の広がりに合わせて、
  - **テレワーク方式を７種類に再編**（変更・細分化）
  - **派生的な構成**についても明記
- テレワーク利用の広まりや、サイバー攻撃の深刻化に対応するため、**対策事項を全面見直し**(倍増)
  例）オンライン会議システムのセキュリティ対策や、VPN機器のファームウェアアップデート等を新たに追加
- 対策事項を、13個の対策カテゴリに分類
- 各対策事項の詳細な解説についても、近年の動向を踏まえて全面的に見直し
- トラブル事例の対策に当たっては、複数対策が紐付く場合もあるため、章として独立
- 近年の実事例等を踏まえ、事例を全面更新

第５版（意見募集中）

第１章 はじめに

✓ 背景、目的、テレワークの形態、想定読者等を説明。

第２章 テレワークにおいて検討すべきこと

✓「ルール」「人」「技術」のバランスのとれた対策の必要性を説明。
✓「経営者」「システム・セキュリティ管理者」「テレワーク勤務者」の適切な役割分担の重要性と、各立場の役割を具体的に説明。
✓ テレワークを取り巻く環境変化を踏まえ、クラウドサービスの有効性やセキュリティ上の留意事項に関して説明。
✓ サイバー攻撃が高度化している状況を踏まえ、セキュリティ手法として注目されるゼロトラストセキュリティに関する考え方を説明。

第３章 テレワーク方式の解説

✓ テレワーク方式を7種類に再整理し、各方式について、基本的構成に加えて派生的な構成まで詳細に解説。
✓ 各テレワーク方式に特有のセキュリティ上の留意点について説明（各方式共通の対策は第4・5章）。
✓ 実現しようとする業務内容等を踏まえ、適した方式を選定するフローチャートや、各方式の特性比較表を掲載。

第４章 テレワークセキュリティ対策一覧

✓「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」の役割ごとに、実施すべきセキュリティ対策を記載。（セキュリティ対策は「基本対策」と「発展対策」に区分。）
✓ テレワークが一般的な業務形態となってきたことに対応し、対策項目は98項目に倍増
✓ 対策分類は、13個のカテゴリに細分化し、見通しを整理。

第５章 テレワークセキュリティ対策の解説

✓ 第4章で明示した内容について、対策分類ごとに詳細に解説。

第６章 テレワークにおけるトラブル事例と対策

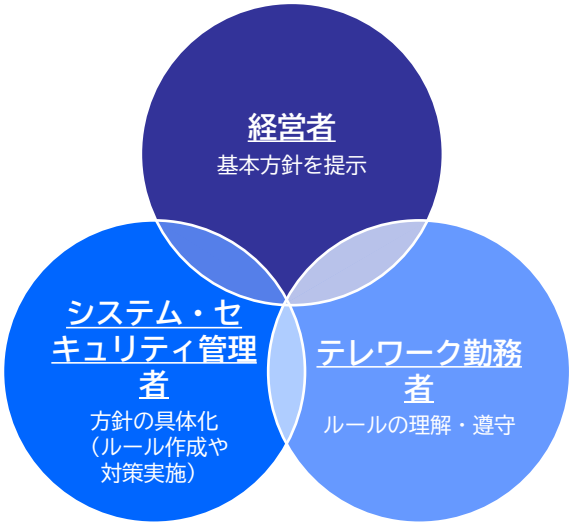
✓ トラブル事例を具体的に紹介した上で、セキュリティ上留意すべき点や、本ガイドライン内のどの対策が有効であるかを説明。

意見募集中であり、記載内容は変わる場合があります。

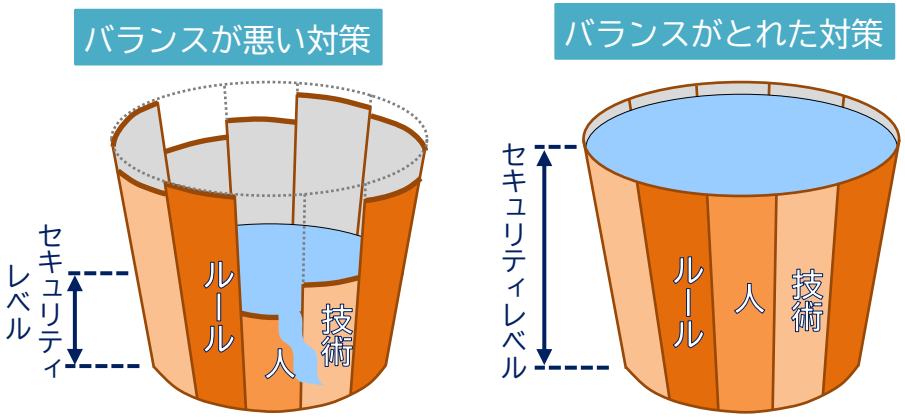
第２章　テレワークにおいて検討すべきこと

経営者、システム・セキュリティ管理者、テレワーク勤務者の役割分担

第５版で記載を**明確化**



ルール、人、技術のバランスのとれたセキュリティ対策



経営者の重要な役割

① テレワークセキュリティに関する脅威と事業影響リスクの認識
② テレワークに対応したセキュリティポリシーの策定
③ テレワークにおける組織的なセキュリティ管理体制の構築
④ テレワークでのセキュリティ確保のための資源（予算・人員）確保
⑤ テレワークにより生じるセキュリティリスクへの対応方針決定と対応計画策定
⑥ テレワークにより対応が必要となるセキュリティ対策のための体制構築
⑦ 情報セキュリティ関連規程やセキュリティ対策の継続的な見直し
⑧ テレワーク勤務者に対するセキュリティ研修の実施と受講の徹底
⑨ セキュリティインシデントに備えた計画策定や体制整備
⑩ サプライチェーン全体での対策状況の把握

システム・セキュリティ管理者の重要な役割

① テレワークに対応した情報セキュリティ関連規程やセキュリティ対策の見直し
② テレワークで使用するハードウェア・ソフトウェア等の適切な管理
③ テレワーク勤務者に対するセキュリティ研修の実施
④ セキュリティインシデントに備えた準備と発生時の対応
⑤ セキュリティインシデントや予兆情報の連絡受付
⑥ 最新のセキュリティ脅威動向の把握

テレワーク勤務者の重要な役割

① 情報セキュリティ関連規程の遵守
② テレワーク端末の適切な管理
③ 認証情報（パスワード・ICカード等）の適切な管理
④ 適切なテレワーク環境の確保
⑤ セキュリティ研修への積極的な参加
⑥ セキュリティインシデントに備えた連絡方法の確認
⑦ セキュリティインシデント発生時の速やかな報告

意見募集中であり、記載内容は変わる場合があります。

第３章　テレワーク方式の解説

テレワーク方式

第５版で記載を**再編**

第４版の テレワーク方式
会社PCの 持ち帰り方式
リモート デスクトップ方式
仮想デスクトップ方式
アプリケーション ラッピング方式
セキュアブラウザ方式
クラウド型アプリ方式

細分化

端末にデータを保存したり、クラウドを使う場合も新たに想定

端末にデータを保存したり、クラウドを使う場合も新たに想定

名称をわかりやすいものに

クラウドを使わない場合も新たに想定

名称の平仄をあわせわかりやすいものに

方式名	概要
① **VPN方式**	テレワーク端末からオフィスネットワークに対してVPN接続を行い、そのVPNを介してオフィスのサーバ等に接続し業務を行う方法
② **リモートデスクトップ方式**	テレワーク端末からオフィスに設置された端末（PC等）のデスクトップ環境に接続を行い、そのデスクトップ環境を遠隔操作し業務を行う方法
③ **仮想デスクトップ(VDI)方式**	テレワーク端末から仮想デスクトップ基盤上のデスクトップ環境に接続を行い、そのデスクトップ環境を遠隔操作し業務を行う方法
④ **セキュアコンテナ方式**	テレワーク端末にローカル環境とは独立したセキュアコンテナという仮想的な環境を設け、その環境内でアプリケーションを動かし業務を行う方法
⑤ **セキュアブラウザ方式**	テレワーク端末からセキュアブラウザと呼ばれる特殊なインターネットブラウザを利用し、オフィスのシステム等にアクセスし業務を行う方法
⑥ **クラウドサービス方式**	オフィスネットワークに接続せず、テレワーク端末からインターネット上のクラウドサービスに直接接続し業務を行う方法
⑦ **スタンドアロン方式**	オフィスネットワークには接続せず、あらかじめテレワーク端末や外部記録媒体に必要なデータを保存しておき、その保存データを使い業務を行う方法

✓各方式について解説図を作成

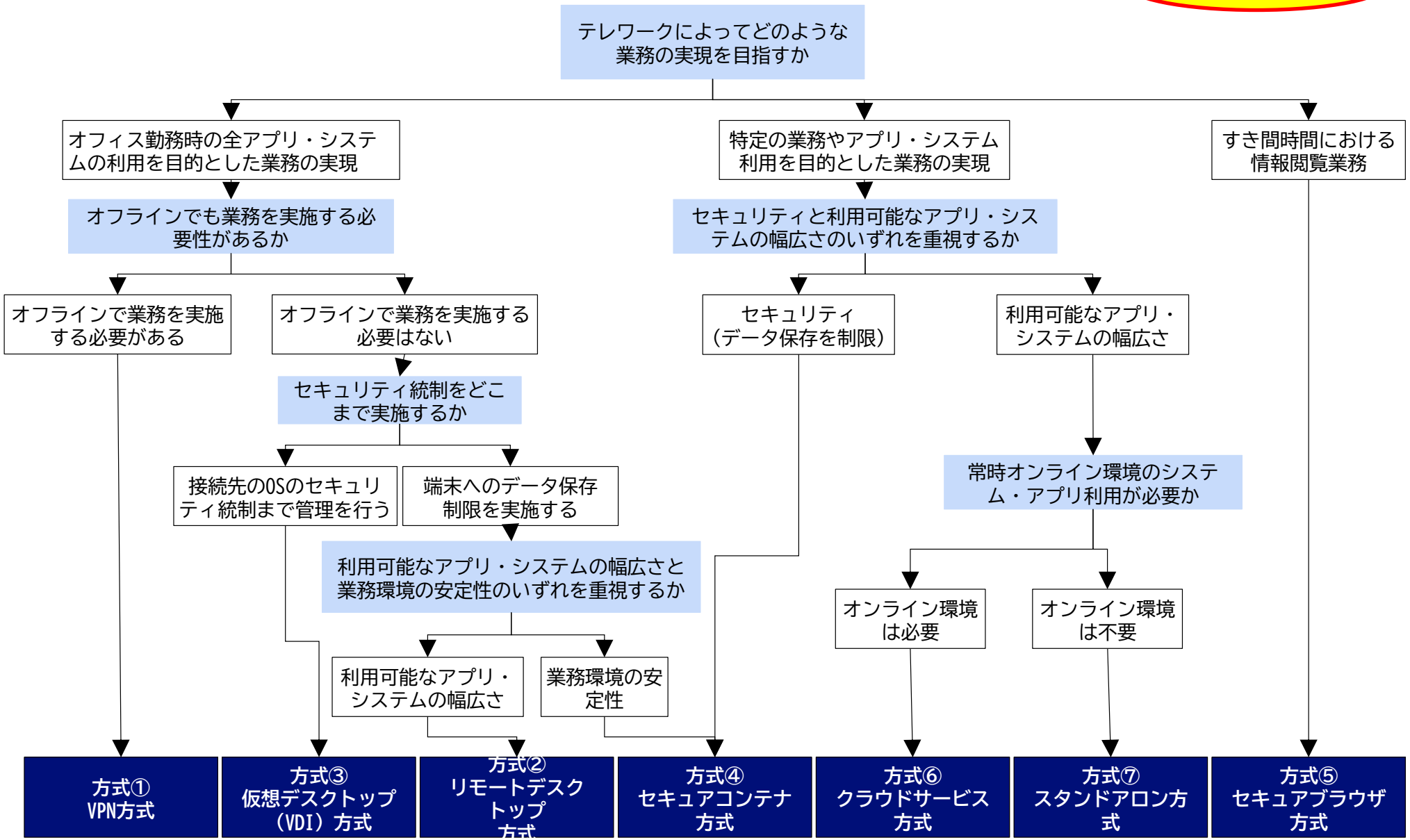
✓派生的な方式についても記載
（例：クラウド型VPNサービスを利用する形式）

✓各方式に特有のセキュリティ上の注意事項についても記載

意見募集中であり、記載内容は変わる場合があります。

第３章　テレワーク方式の解説（検討フローチャート）

第５版で**新規**に記載



意見募集中であり、記載内容は変わる場合があります。

第３章　テレワーク方式の解説（特性比較）

第５版で**新規**に記載

テレワーク方式	オフィス業務の再現性	通信集中時の影響度	システム導入コスト	システム導入作業負荷	セキュリティ統制の容易性	ポイント（想定される使い方）
①VPN方式	**S**（オフィスと同等の業務が可能）	**A**（通信影響を受けるが、端末側(ローカル)作業で一部回避可）	**B**（システム導入が必要）	**B**（環境変更を伴うシステム導入が必要）	**C**（データ管理とセキュリティ統制が必要）	業務再現性が高く、通信集中にも対応したい場合の利用が想定
②リモートデスクトップ方式	**S**（オフィスと同等の業務が可能）	**C**（通信影響を受けやすい）	**B**（システム導入が必要）	**B**（環境変更を伴うシステム導入が必要）	**A**（データ保存を制限でき、データ管理が容易）	業務再現性が高く、セキュリティやコストをバランスする場合の利用が想定
③仮想デスクトップ（VDI）方式	**S**（オフィスと同等の業務が可能）	**C**（通信影響を受けやすい）	**C**（高額なシステム導入が必要）	**C**（大きな環境変更を伴うシステム導入が必要）	**S**（データ保存を制限でき、セキュリティの集中管理が容易）	業務再現性が高く、高度なセキュリティを実現したい場合の利用が想定
④セキュアコンテナ方式	**B**（特定のアプリやシステムでの作業のみ可能）	**A**（通信影響を受けるが、端末側(ローカル)作業で一部回避可）	**B**（システム導入が必要）	**B**（環境変更を伴うシステム導入が必要）	**A**（データ保存を制限でき、データ管理が容易）	セキュリティを確保しつつ通信集中にも対応したい場合の利用が想定
⑤セキュアブラウザ方式	**C**（メールや資料閲覧に限定）	**B**（通信影響を受けるが影響は軽微）	**B**（システム導入が必要）	**B**（環境変更を伴うシステム導入が必要）	**A**（データ保存を制限でき、データ管理が容易）	セキュリティを重視した、特定業務での利用が想定
⑥クラウドサービス方式	**B**（特定のアプリやシステムでの作業のみ可能）	**S**（オフィスネットワークに接続しないため影響なし）	**A**（サービス導入費（使用量に応じた必要最小限）が必要）	**A**（比較的軽微な環境変更で利用可能）	**D**（データ管理に加え、クラウド上でのデータ管理が必要）	拡張性を重視した、特定業務での利用が想定
⑦スタンドアロン方式	**D**（端末に保存したデータのみの作業が可能）	**S**（通信をしないため影響なし）	**S**（追加のシステム・サービス不要）	**S**（システム変更不要）	**C**（データ管理とセキュリティ統制が必要）	コストと導入のしやすさを重視した臨時利用が想定

意見募集中であり、記載内容は変わる場合があります。

第４章・第５章　テレワークセキュリティ対策

対策事項の分類

第５版で記載を**見直し**

※第４版では、①情報セキュリティ保全、②マルウェア、③端末の紛失・盗難、④重要情報の盗聴、⑤不正アクセス、⑥外部サービスの利用　の６種類

対策分類	説明
ガバナンス・リスク管理	テレワークの実施に当たってのリスクマネジメントや、情報セキュリティ関連規程（ルール）の整備等に関する対策。
資産・構成管理	テレワークで利用するハードウェアやソフトウェア等の資産の特定や、その管理に関する対策。
脆弱性管理	ソフトウェアのアップデート実施等による既知の脆弱性の排除に関する対策。
特権管理	不正アクセス等に備えたシステム管理者権限の保護に関する対策。
データ保護	保護すべき情報（データ）の特定や保存されているデータの機密性・可用性の確保に関する対策。
マルウェア対策	マルウェアの感染防止や検出、エンドポイントセキュリティに関する対策。
通信の保護・暗号化	通信中におけるデータの機密性や可用性の確保に関する対策。

信頼できるクラウドサービス選定や、クラウドサービスの利用ルールに言及

セキュリティ対策の実施対象となる資産特定の重要性に言及

クリティカルな攻撃の起点になるVPN基盤等の脆弱性管理の重要性に言及

高度な攻撃で最も狙われる特権防御の重要性に言及

守るべきデータの特定と暗号化、バックアップ取得や確実な廃棄に言及

攻撃起点になりやすく、検知が難しいエンドポイントセキュリティ強化(EDR)に言及

高度な攻撃への効果が期待されるゼロトラストの観点としてEnd-to-Endでのデータ通信の暗号化（通信の保護・暗号化）に言及

対策分類	説明
アカウント・認証管理	情報システムにアクセスするためのアカウント管理や認証手法に関する対策。
アクセス制御・認可	データやサービスへのアクセスを、必要最小限かつ正当な権限を有する者のみに制限することに関する対策。
インシデント対応・ログ管理	セキュリティインシデントへの迅速な対応と、ログの取得や調査に関する対策。
物理的セキュリティ	物理的な手段による情報漏えい等からの保護に関する対策。
脅威インテリジェンス	脅威動向、攻撃手法、脆弱性等に関する情報の収集に関する対策。
教育	テレワーク勤務者のセキュリティへの理解と意識の向上に関する対策。

攻撃起点となる認証突破対策として、多要素認証に言及

ゼロトラスト観点より、最小権限によるアクセス権統制に言及

完全防御が難しいという前提のもと、インシデント発生後の事後対応に言及

オンライン会議普及に伴い、在宅環境の物理セキュリティ対策(意図せぬ画面映り込み等)に言及

セキュリティ関連機関が発信する情報の収集やコミュニティ加入の重要性に言及

注意喚起・教育等の重要性に言及

吹き出しは対策項目の見直しに当たって考慮した観点

意見募集中であり、記載内容は変わる場合があります。

第６章　テレワークにおけるトラブル事例と対策

トラブル事例

第５版で記載を**見直し**

1．VPN機器の脆弱性の放置
2．個人情報保護の強化
3．アクセス権限の設定不備
4．マルウェア感染
5．ランサムウェア
6．フィッシングメール
7．ビジネスメール詐欺（BEC）
8．USBメモリの紛失
9．無線LAN利用通信の窃取
10．第三者による画面閲覧
11．テレワーク端末の踏み台化
12．パスワードの使い回し
13．クラウドサービスの設定ミス
14．クラウドサービスの障害
15．サプライチェーン

具体的事例と対策例（VPN機器の脆弱性の放置）

1．VPN機器の脆弱性の放置

① 具体的な動向

2020年８月に、VPN機器のIDやパスワードが世界中から流出する事件
た。既知の脆弱性を放置したまま運用を続けていたVPN機器が攻撃を受
40社近くの企業に対して、不正アクセスが行われました。

2019年には、この脆弱性を悪用する攻撃が既に発生しており、該当の
造ベンダー側でファームウェアの修正が行われていますが、ファームウ
アップデートしていない機器が攻撃を受けました。

② テレワークセキュリティへの示唆

脆弱性への対応スピードが他の国と比較して日本は低いという調査結
す。その調査の中では、米国、英国、ドイツ等の諸外国では、脆弱性公表
１週間で２～５割の製品がアップデートされている中、日本ではアップデ
割合が１割にも満たないこと、また脆弱性公表から７カ月たった2020年
点でも、対応率が低いままとなっているという結果が出ています。脆弱性
攻撃は日々発見され、攻撃者は攻撃の機会を伺っています。そのため、脆
放置するのではなく、即時対応を行うことが重要です。

また、テレワークの急激な拡大に対応するため、過去に使用していて運用から外しておいたVPN機器を、設備増強用としてそのまま臨時稼働させたところ、脆弱性が潜んでいたために攻撃を受けたという企業もありました。このように、過去に使用していた機器を再利用する場合には、ファームウェアを最新の状態にして、既知の脆弱性が残っていない状態で使用することが重要です。

③ 有効な対策

	脆弱性管理（詳細解説はp.74～）
管理者C-2 基本対策	オフィスネットワークにアクセスする際に必要となるVPN機器やリモートデ プリケーション等について、最新のアップデートやパッチ適用を定期的に行
管理者C-3 基本対策	テレワークで利用する端末やソフトウェアについて、メーカーサポートが終 のを利用しないようにテレワーク勤務者に周知する。

各トラブル事例について、具体的なインシデント等の発生動向を記載。

当該トラブル事例を防ぐために、どのような点に留意すべきかを記載。

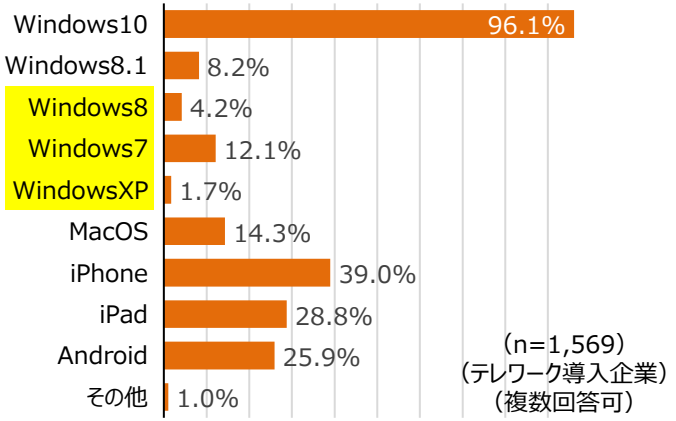
当該トラブル事例を防ぐために、第４・５章に記載された対策事項のうち該当するものを記載

意見募集中であり、記載内容は変わる場合があります。

テレワークセキュリティに関する実態調査結果②

1次調査（昨夏）

使用している会社所有の端末の種類



設問　貴社・貴団体において使用している会社所有のPC端末及び会社所有のモバイル端末（スマートフォン/タブレット）の種類をすべてお答えください。

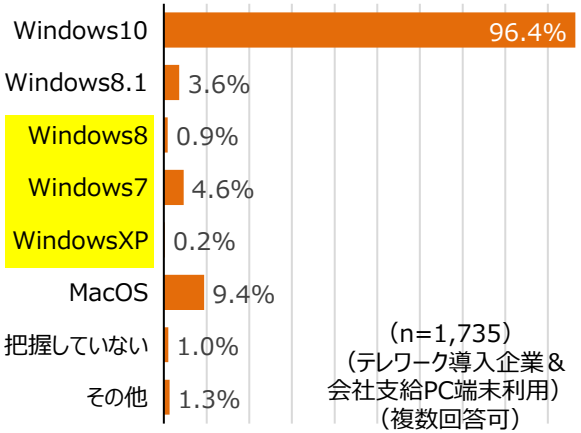
テレワーク使用端末以外（クローズ環境等）と勘違いして、誤って回答しているのではないか？

設問　テレワークで利用する会社支給のPC端末について、利用しているOSの種類を全て教えてください。

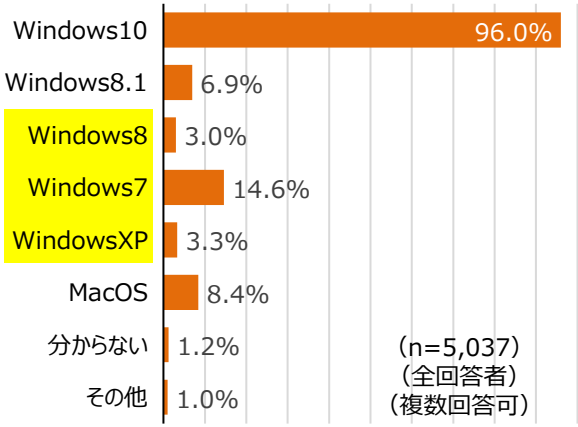
設問　職場利用・テレワーク利用に関わらず、会社所有のPC端末のOSの種類を全て教えてください。

2次調査（今冬）

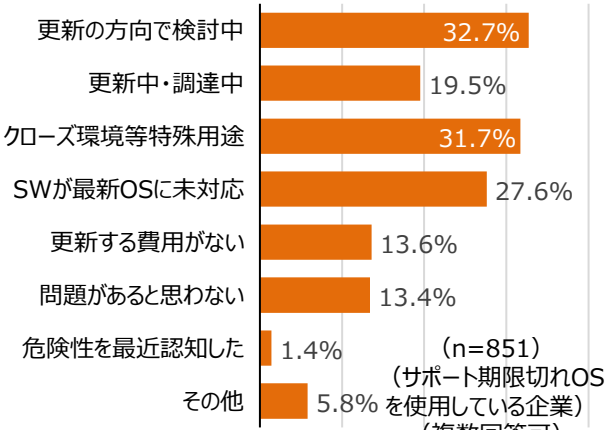
テレワークで使用する会社支給のPC端末の種類



職場・テレワークに関わらず会社所有のPC端末の種類



サポート期限が切れたOSを使用している理由



※自由回答により、ESUを使用している企業も見受けられた

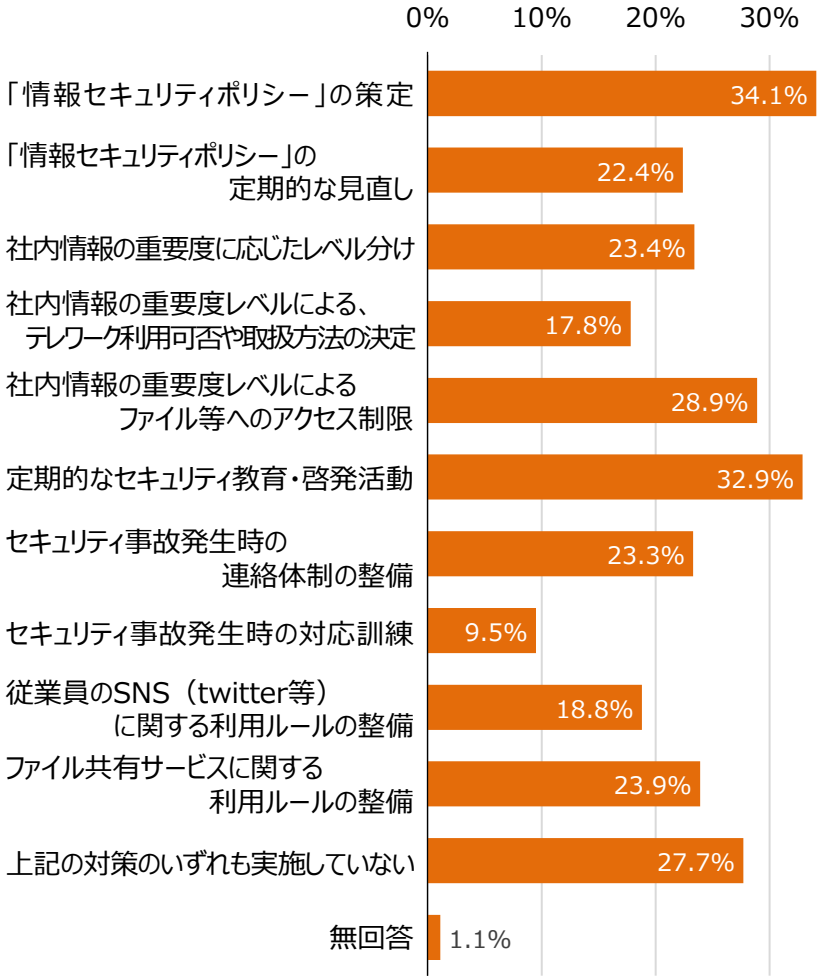
2次調査結果は速報値

テレワークセキュリティに関する実態調査結果③

- 情報セキュリティポリシーを策定している企業は約３分の１にとどまる。
- セキュリティ対策ソフトが常に最新になるように指示・設定している企業も約３分の２にとどまる。

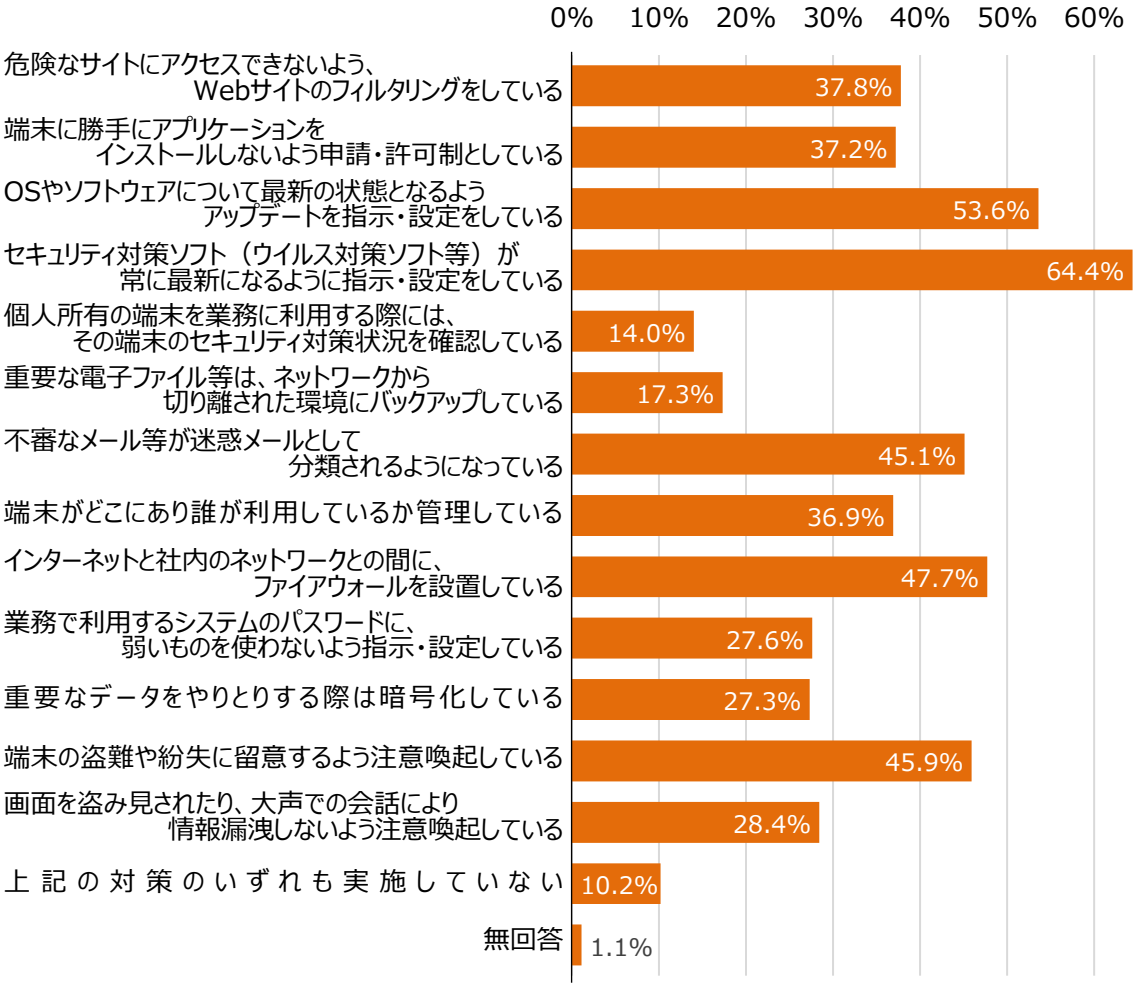
情報セキュリティの管理体制等に関する対策の実施状況

（n=1,569：テレワーク導入企業）　（複数回答可）



各種サイバー攻撃に関する対策の実施状況

（n=1,569：テレワーク導入企業）　（複数回答可）



テレワークのセキュリティに関する相談対応

- 総務省では従来から、**テレワークに関する幅広い相談**について、**テレワークマネージャー**相談事業により対応。
- 今般、中小企業等においてもテレワーク利用が急速に広まっており、適切かつ十分なセキュリティ対策がとられていない可能性もあることから、**セキュリティに関する不安**、具体的な**セキュリティ対策方法**、ルール作りや自社の実施状況の適切性の**コンサルティング**などを**相談できる窓口を開設**しています。
- **セキュリティの専門家**に対して、**無料**で気軽に相談可能ですので、是非ご利用を検討ください。

導入前のお悩み

私物のパソコンを従業員に
使わせても問題ないの？

これからテレワークの
仕組みを作りたいけど、
セキュリティは何をすればいいの？

アクセス制限が必要と聞いたけど、
何をどう設定すればいいの？

導入後のお悩み

とりあえずテレワークの
仕組みは作ったけれど、
セキュリティ的に大丈夫なの？

情報漏えいが心配だけど、
従業員への教育は必要？
何をすればいいの？

情報セキュリティのルールづくりで
考慮すべきポイントは何？

相談費用

無料

相談対応期間

2021年３月まで

相談対応方法

申込の後、相談者の希望に応じて、電話・メール・Web会議により対応します。

相談の申込先

https://www.lac.co.jp/telework/security.html

※本事業は、総務省が株式会社ラックに委託し、実施しています。
セキュリティ専門企業の同社の専門家が相談対応に当たります。

1. 最新のサイバーセキュリティ動向

2. テレワークにおけるセキュリティ確保

3. 無線LAN（Wi-Fi）の利用・提供におけるセキュリティ確保

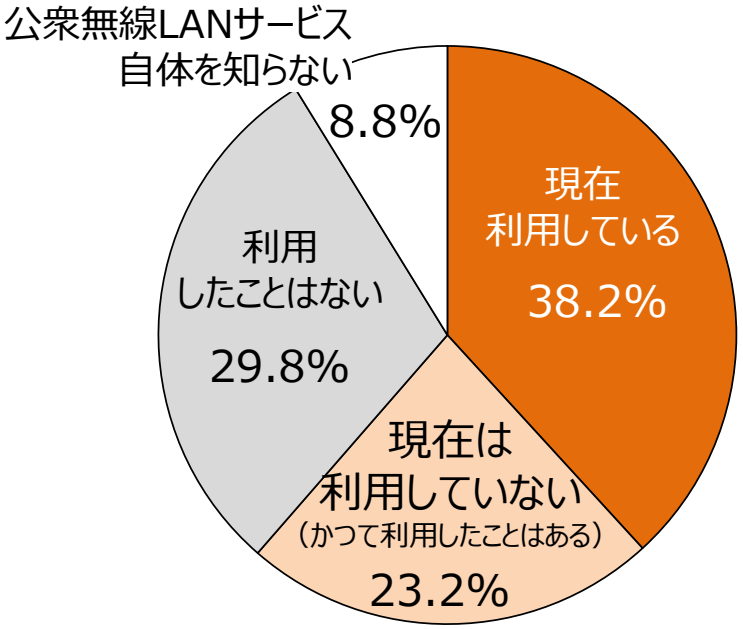
4. 総務省におけるその他の取組

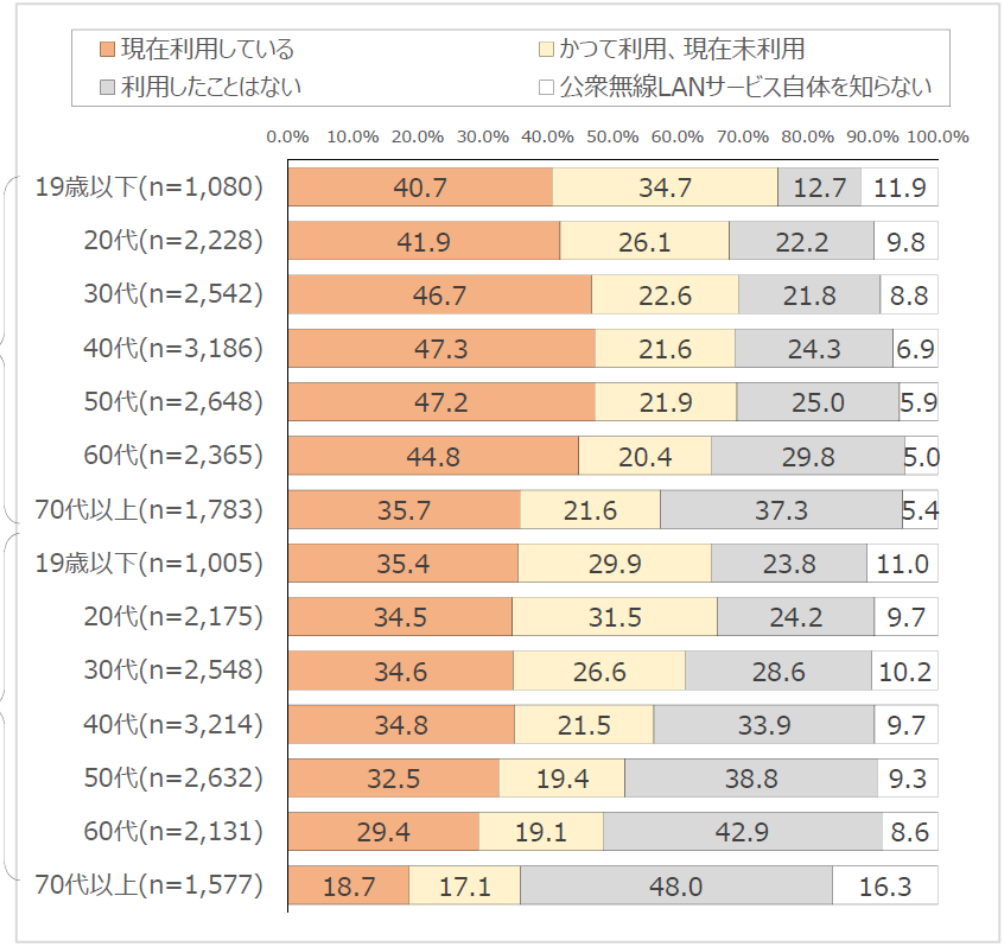
公衆無線LANの利用状況

➢ 利用者の公衆無線LANに対するセキュリティ意識等を把握するための調査をWebアンケートにより実施。
（対象地域：全国　期間：2020年2月13日～17日　調査数：31,112（無線LAN利用者1,392をスクリーニング調査））

公衆無線LANを利用しているか

（n=31,112）

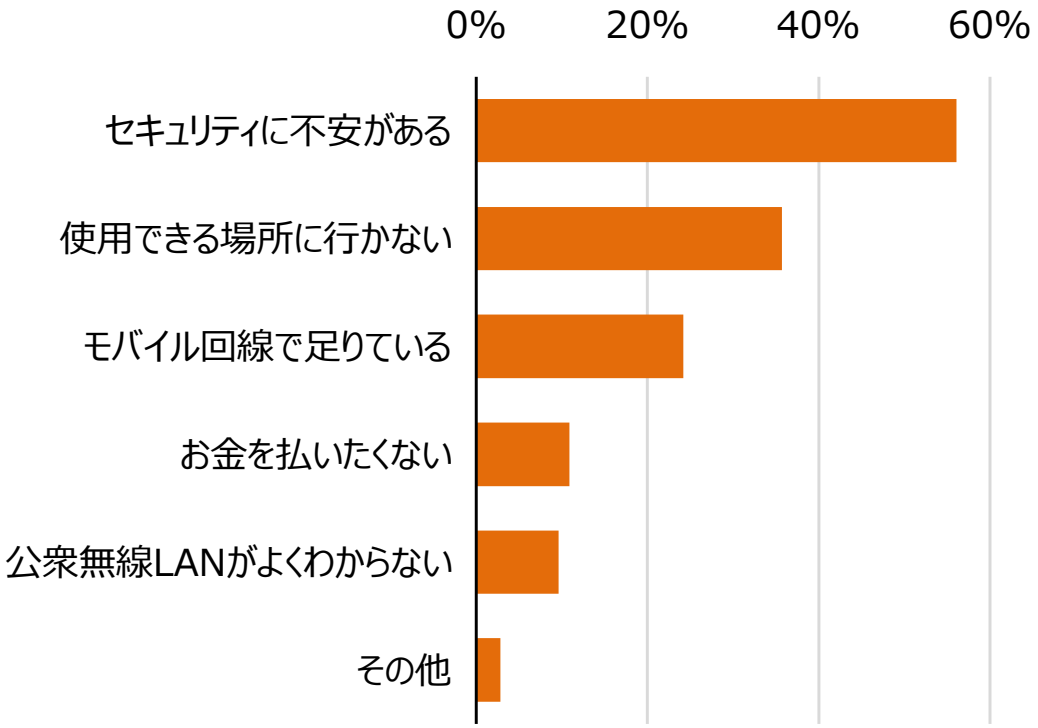




公衆無線LAN時のセキュリティ意識

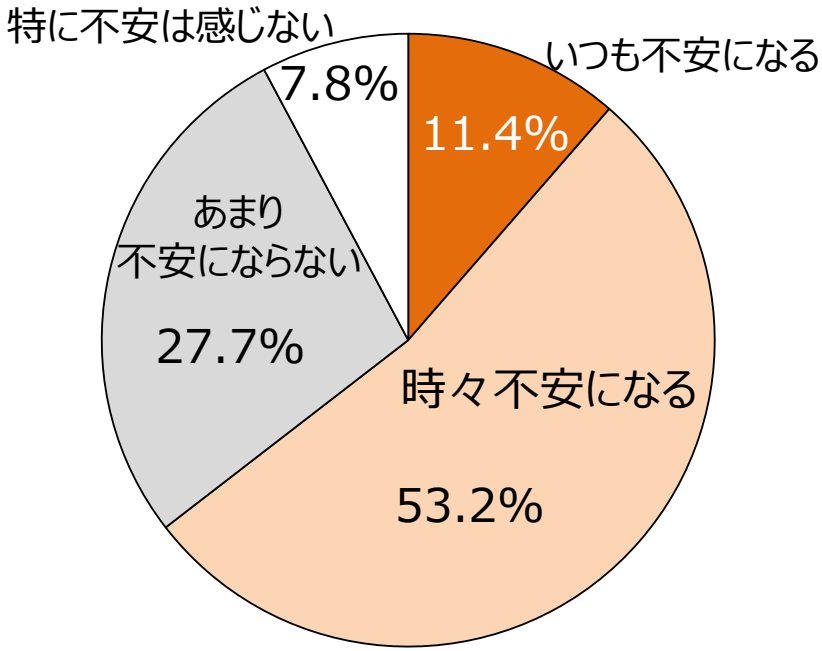
公衆無線LANを利用しなかった理由

（n=16,473：現在未利用者）



公衆無線LANで不安を感じるか

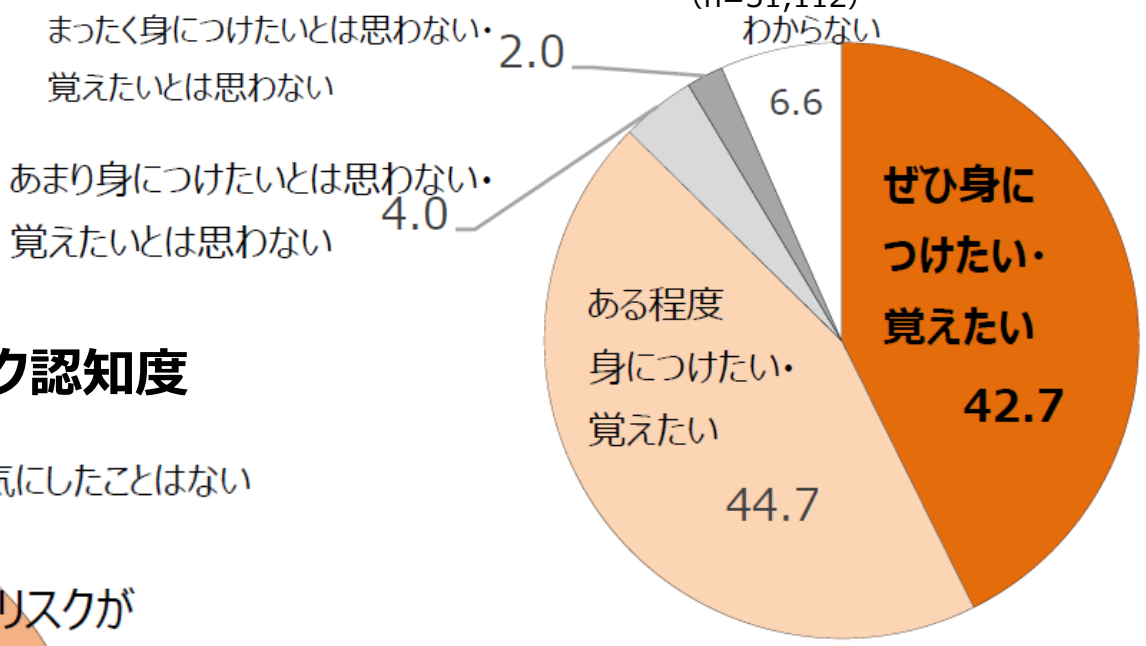
（n=1,392：公衆無線LAN利用者）



公衆無線LAN利用時のセキュリティ知識への関心

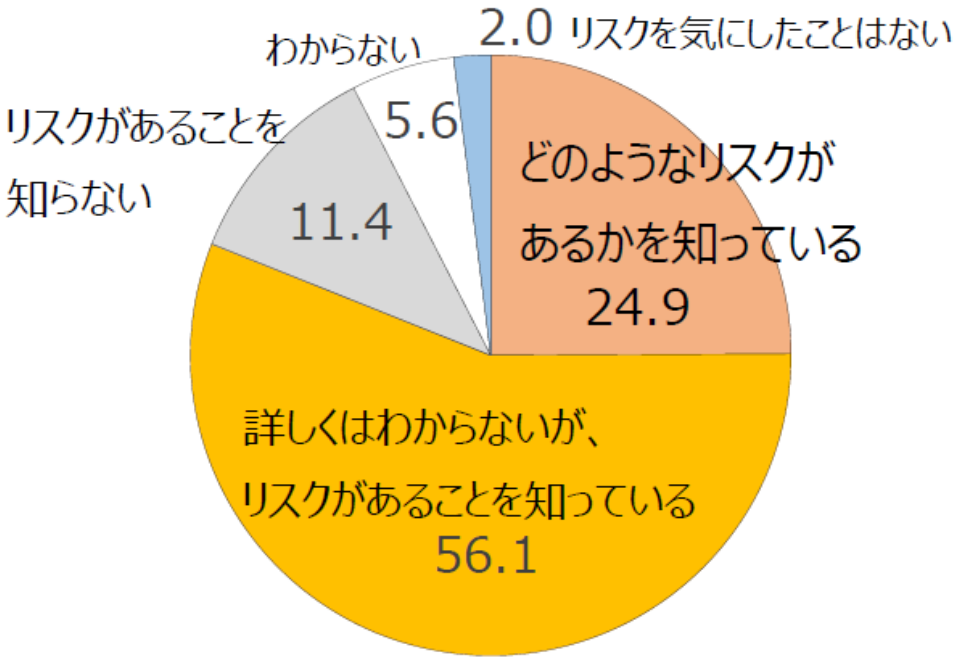
公衆無線LAN利用時のセキュリティ知識習得意向

（n=31,112）



公衆無線LAN利用時のリスク認知度

（n=28,366）

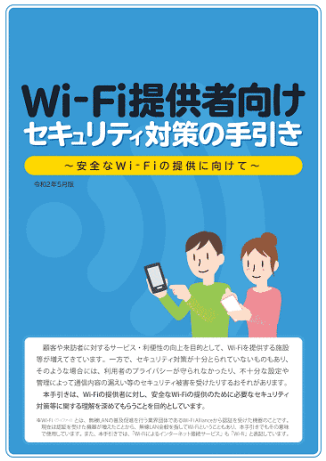


無線LANのセキュリティガイドラインの見直し

- 総務省では、無線LANの利用者・提供者向けにガイドラインを作成しており、周知啓発に活用。
- 新技術や最新のセキュリティ動向に対応するため、内容を見直し2020年５月に改定版を公表。
- 改定版については、Wi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に幅広く周知。
  https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

「Wi-Fi利用者向け 簡易マニュアル」(平成27年3月10日版)の見直しポイント

- ✓ セキュリティ対策の訴求点を明確にするため、**セキュリティ対策のポイント**を**整理**
  - ① 接続する**アクセスポイント**を**よく確認**（偽アクセスポイント対策として接続URL等を確認）
  - ② 正しい**URL**で**HTTPS通信**をしているか**確認**（Wi-Fi暗号化等に関わらず通信内容を保護）
  - ③ 自宅に設置している**機器の設定**を**確認**（管理用パスワードの変更やファームウェアアップデート等）
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**



「Wi-Fi提供者向け セキュリティ対策の手引き」(平成28年8月版)の見直しポイント

- ✓ ガイドラインの対象者の明確化（**自店利用者のみへの提供する者も対象**）
- ✓ 近年懸念されている**偽アクセスポイント対策**（認証画面のURLの周知等）を追記
- ✓ 暗号化のための**パスフレーズを公開**している場合解読の**リスクが高まる**ことを明示
- ✓ 状況に応じたセキュリティ対策の選択と**利用者への周知**が必要であることを明確化
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

「Wi-Fi利用者向け 簡易マニュアル」 概要

1　接続するアクセスポイントをよく確認しよう

- ✓ 接続しようとしているWi-Fiサービスを確認
  - 掲示されているステッカー等で、提供者やサービス内容を確認
  - 提供者が不明なものや不審と感じるものには接続しない
- ✓ 接続先の名前（SSID）を確認
  - SSIDが提供者が提供するものと同じか確認
  - 同じSSIDでも偽アクセスポイントの場合があるため、認証画面が表示された場合はURLとHTTPS通信を確認

Wi-Fiの**利用者**に対し、**安全なWi-Fiの利用**のために必要なセキュリティ対策等に関する理解を深めてもらうことを目的として作成。

2　正しいURLでHTTPS通信をしているか確認しよう

- ✓ URLが「https://」で始まるHTTPS通信により、通信全体の暗号化が可能
- ✓ ブラウザのURL入力欄に鍵マークがあることを確認
  （「！」やエラー表示が出ていないことを確認）
- ✓ URL（特にドメイン部分）を確認して、本物に巧妙に似せた偽URL・偽サイトに騙されない

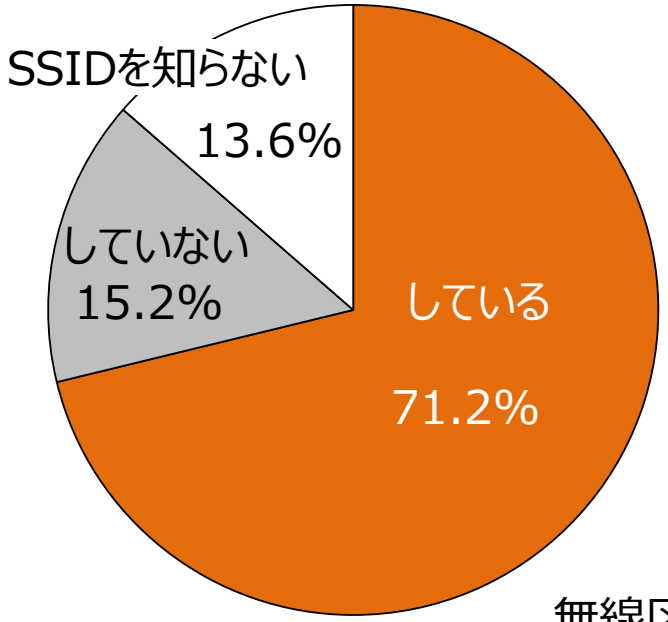
3　自宅に設置している機器の設定を確認しよう

- ✓ セキュリティ方式は「WPA2」を選択
- ✓ Wi-Fiの暗号化のためのパスワードは第三者に推測されにくいものを設定
- ✓ Wi-Fi機器の管理用パスワードも同様
- ✓ ファームウェアを最新のものに更新

公衆無線LAN利用者時のセキュリティ行動

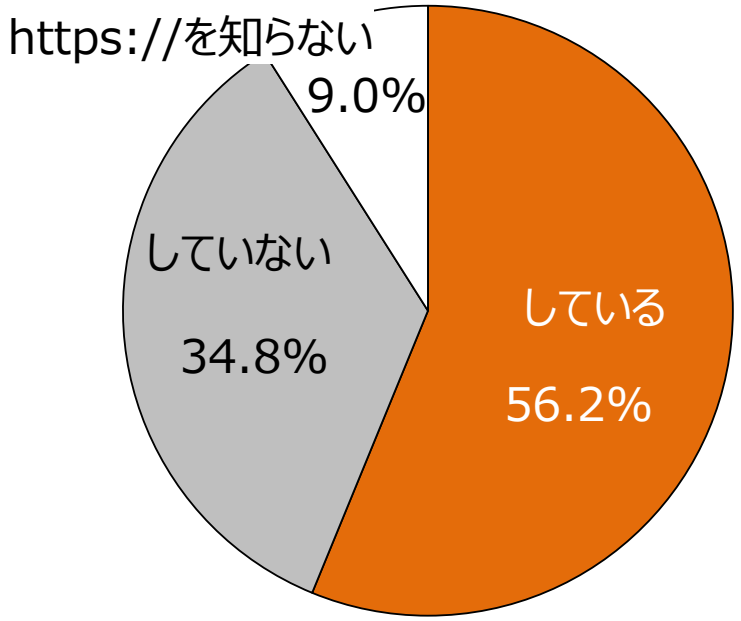
SSID確認

（n=1,392：公衆無線LAN利用者）



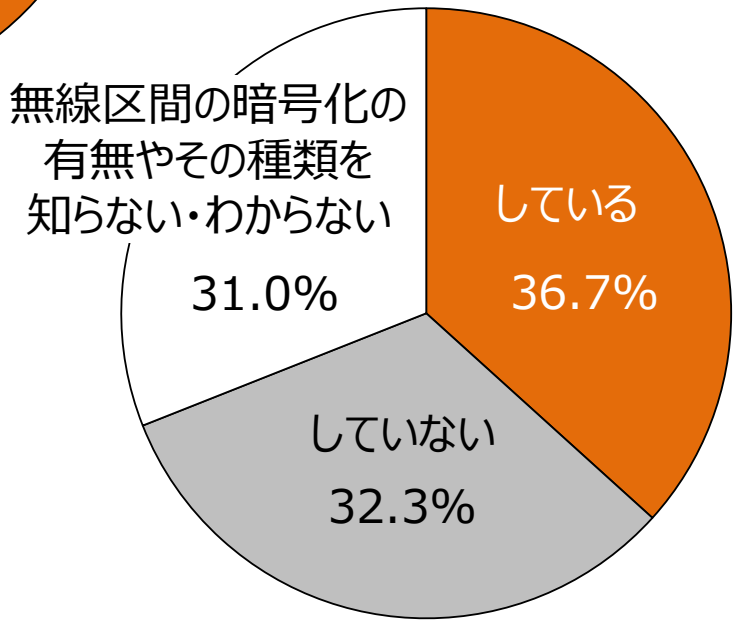
https確認

（n=1,392：公衆無線LAN利用者）

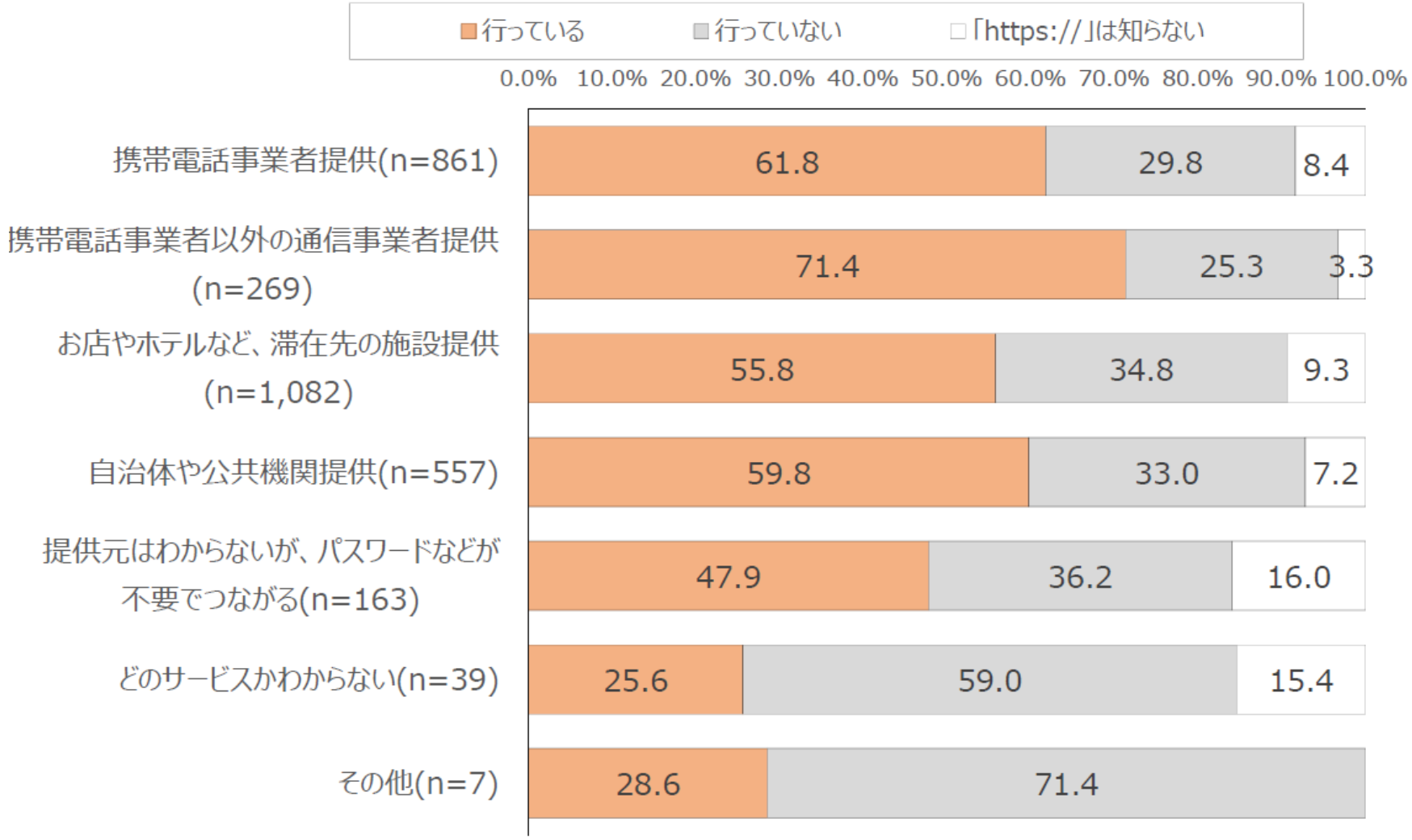


暗号化確認

（n=1,392：公衆無線LAN利用者）



https://の確認行為


行っている
行っていない
「https://」は知らない
0.0% 10.0% 20.0% 30.0% 40.0% 50.0% 60.0% 70.0% 80.0% 90.0% 100.0%
携帯電話事業者提供(n=861)
61.8
29.8
8.4
携帯電話事業者以外の通信事業者提供(n=269)
71.4
25.3
3.3
お店やホテルなど、滞在先の施設提供(n=1,082)
55.8
34.8
9.3
自治体や公共機関提供(n=557)
59.8
33.0
7.2
提供元はわからないが、パスワードなどが不要でつながる(n=163)
47.9
36.2
16.0
どのサービスかわからない(n=39)
25.6
59.0
15.4
その他(n=7)
28.6
71.4

「Wi-Fi提供者向け　セキュリティ対策の手引き」 概要

Wi-Fiの**提供者**に対し、**安全なWi-Fiの提供**のために必要なセキュリティ対策等に関する理解を深めてもらうことを目的として作成。

1　本手引きをお読みになる方へ

- ✓ Wi-Fiを提供する施設の運営者等を対象
- ✓ 利用者限定で提供している場合も対象

2 利用者を守るための対策

- ✓ 利用者への周知啓発
  （「Wi-Fi利用者向け 簡易マニュアル」の周知等）
- ✓ WPA2による暗号化
  （暗号化を実施しない場合は利用者への適切な周知）
- ✓ パスフレーズを掲示等する場合のリスク検討
- ✓ 利用者の端末を保護するための端末同士の通信禁止
- ✓ 偽アクセスポイント対策としての
  認証画面のhttps化とURLの周知

3 Wi-Fiを安全に提供するための対策

- ✓ 機器管理パスワードの変更
- ✓ 機器のファームウェアのアップデート
- ✓ 業務用ネットワークとの分離
  （物理分離・論理分離）
- ✓ 利用者情報の適切な確認
  （電子メール、SNSアカウント、SMS等）
- ✓ アクセスログの記録・保存
- ✓ 利用時間制限、メール送信制限等

4 利用者に安心を提供するための対策

- ✓ Wi-F利用者が安心して使うための適切な情報の提供
  （サービス提供者・提供条件、セキュリティ対策内容、周知等）
- ✓ 青少年有害情報のフィルタリング
- ✓ 法令に準拠した個人情報保護・通信の秘密保護

5 より使いやすいWi-Fiの提供に向けて

- ✓ 複数周波数帯での提供（2.4GHz帯＋5GHz帯）
- ✓ 干渉を避けたチャネル選択、電波の出力調整
- ✓ 共用型アクセスポイントの設置

無線LAN(Wi-Fi)の伝送規格とセキュリティ規格

伝送規格

規格名	呼称*1)	使用する周波数帯*2)	最大伝送速度*3)
IEEE 802.11b	–	2.4GHz帯	11Mbps
IEEE 802.11a	–	5GHz帯	54Mbps
IEEE 802.11g	–	2.4GHz帯	54Mbps
IEEE 802.11n	Wi-Fi 4	2.4GHz帯 & 5GHz帯	600Mbps
IEEE 802.11ac	Wi-Fi 5	5GHz帯	6.9Gbps
IEEE 802.11ax	Wi-Fi 6	2.4GHz帯 & 5GHz帯	9.6Gbps

*1) 規格名をわかりやすくするため、業界団体（Wi-Fi Alliance）が「Wi-Fi 6」といった呼称を規定しています。
*2) 5GHz帯にはW52（5.2GHz帯；制限付き屋外利用可）・W53（5.3GHz帯；屋外利用不可）・W56（5.6GHz帯；屋外利用可）があります。
*3) 規格上の速度であり、実際のデータ伝送速度はこれよりも遅くなります。

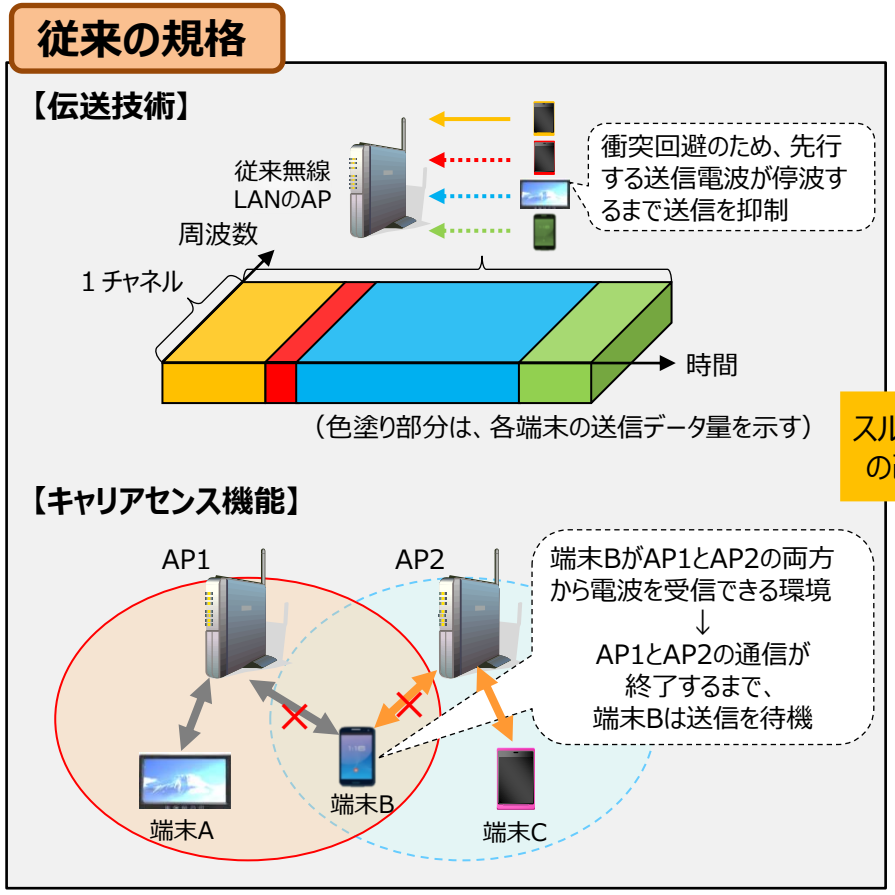
セキュリティ規格

セキュリティ強度	セキュリティ方式	特徴
	**WPA3**	2018年に発表された最新のセキュリティ技術を用いた次世代の方式。今後対応製品の普及が期待される。
	WPA2	WPAより堅牢な**現在主流のセキュリティ方式**。
	WPA	WEPの弱点を補強した方式だが、一部脆弱性があり、現在では推奨されない。
	WEP	暗号を短時間で解読する方法が知られており、現在では**容易に解読されてしまう**方式となってしまっている。
	暗号化なし	通信が暗号化されず、だれでも接続可能。

次世代無線LAN (Wi-Fi 6)の導入に向けた環境整備

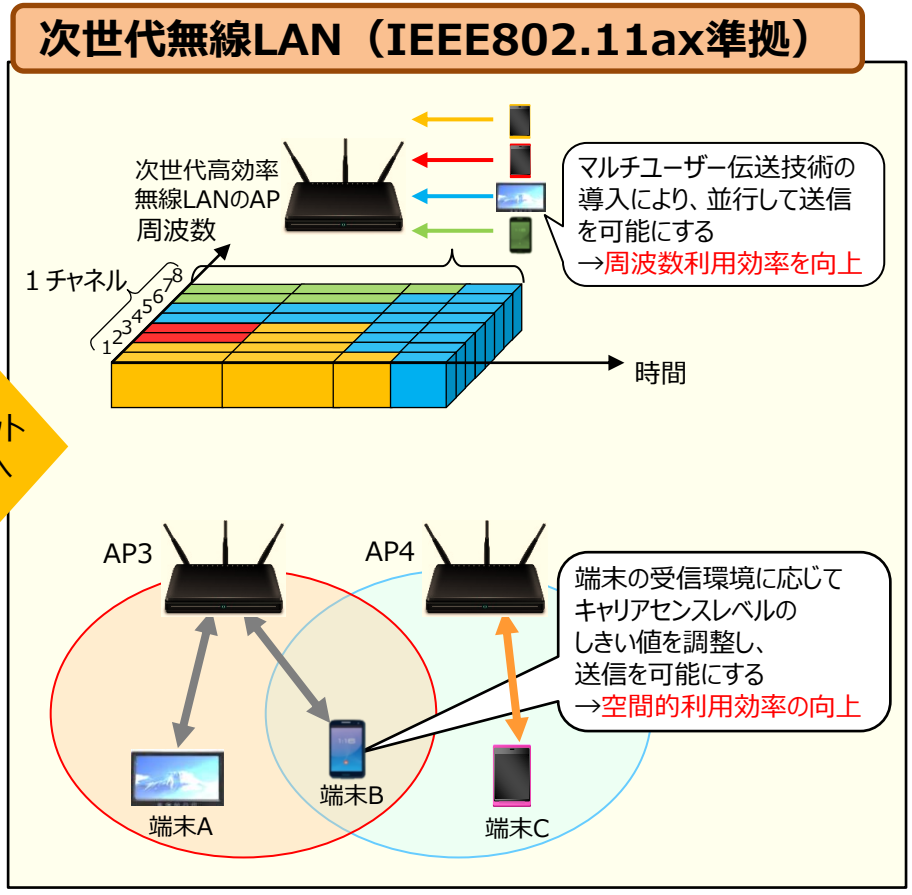
- IEEE802.11ac(Wi-Fi5)には多重伝送技術（下りマルチユーザMIMO）を導入済
- 次世代無線LAN（令和３年１月にIEEE802.11axとして標準化予定）には、新たな多重伝送技術（上り下りOFDMAと上りマルチユーザMIMO）等を導入予定
- 必要な国内での制度整備については既に実施済み。

従来の規格



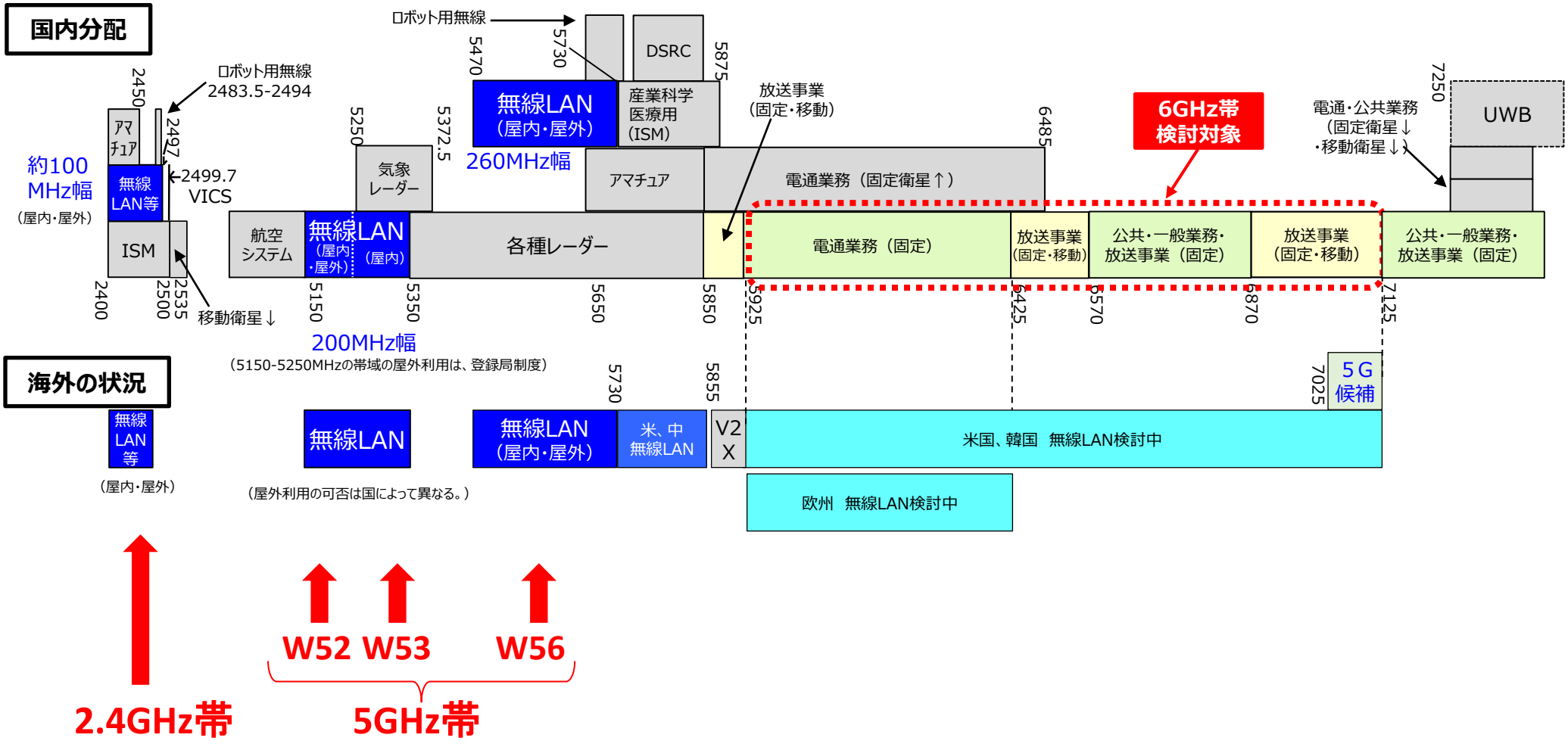
スループットの改善へ

次世代無線LAN（IEEE802.11ax準拠）



無線LANに関する周波数の状況

- 無線LANの周波数は、2.4GHz/5GHzともに他の周波数と共用
  例：2.4GHz･･･電子レンジ　／　5GHz･･･気象レーダー
  (↔5G等の携帯電話用周波数は(一部例外はあるものの)基本的には専用周波数)
- 通信容量の増加等に対応できるようにするため、無線LANの６GHz帯拡張について検討開始予定。



1. 最新のサイバーセキュリティ動向

2. テレワークにおけるセキュリティ確保

3. 無線LAN（Wi-Fi）の利用・提供におけるセキュリティ確保

4. 総務省におけるその他の取組

実践的サイバー防御演習（CYDER）

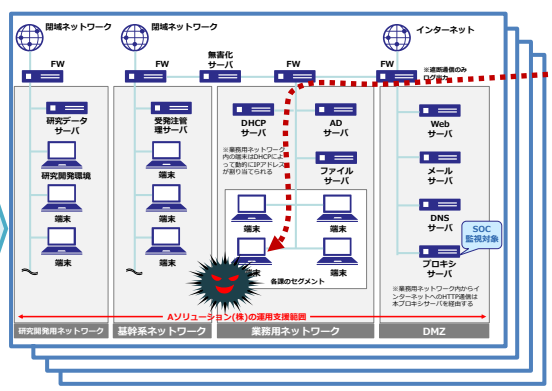
CYDER：CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**(**CYDER**)を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験**。
- **全都道府県**において、年間**100回・計3,000名規模**で実施。 参加申込 → https://cyder.nict.go.jp
  ※平成29年度：年間100回・3,009名受講／平成30年度：年間107回・2,666名受講／令和元年度：年間105回・3,090名受講

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**

演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和３年度の実施計画（予定）

コース名	演習方法	レベル	受講想定者	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムの運用担当者（システムの利用者レベルを含む）	全組織共通	４７都道府県	６５回	７月～翌年２月
B-1		中級	セキュリティ管理業務を主導する立場の者	地方公共団体	全国１１地域	２０回	９月～翌年２月
B-2				地方公共団体以外	東京・大阪・名古屋・福岡	１３回	１１月～翌年２月
C		準上級	（詳細検討中）	全組織共通	東京	２回	翌年１月～２月
オンラインA	オンライン演習	初級	システムの運用担当者（システムの利用者レベルを含む）	全組織共通	（受講者職場等）	随時	１１月～翌年２月（6~8月に試験提供予定）

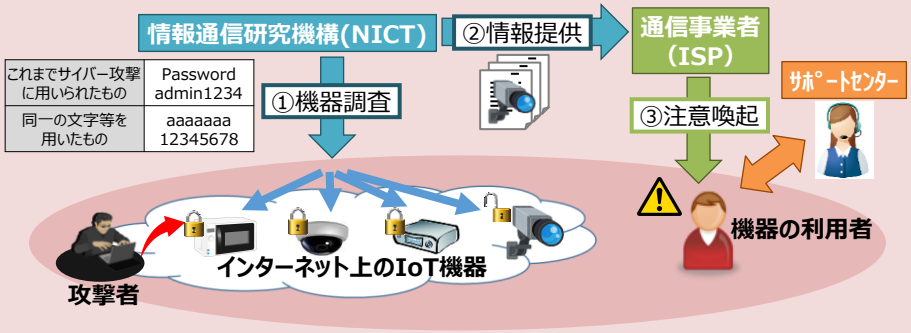
令和３年度から**新規**開設

IoT機器調査及び利用者への注意喚起

- 情報通信研究機構(NICT)が**サイバー攻撃に悪用されるおそれのあるIoT機器**を調査し、インターネット・サービス・プロバイダ(ISP)を通じた利用者への注意喚起を行う取組「**NOTICE**」を2019年２月より実施。
- NOTICEの取組に加え、**マルウェアに感染しているIoT機器**をNICTの「**NICTER**」プロジェクト※で得られた情報を基に特定し、ISPから利用者へ注意喚起を行う取組を2019年６月より開始。

※NICTが、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施。

【NOTICE注意喚起の概要】

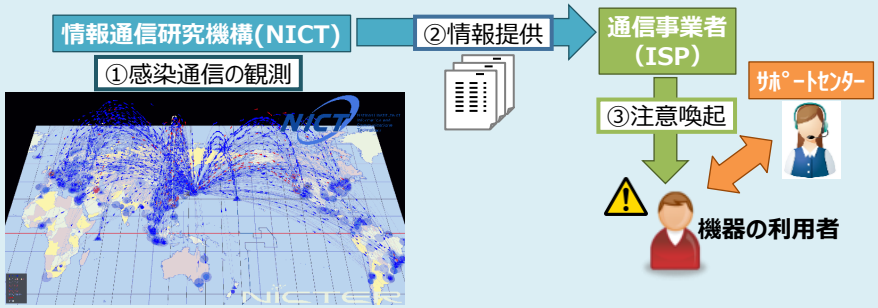


調査対象：パスワード設定等に不備があり、**サイバー攻撃に悪用されるおそれのある**IoT機器

① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力するなどして、サイバー攻撃に悪用されるおそれのある機器を特定。
② 当該機器の情報をISPに通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施。

【NICTER注意喚起※の概要】

※マルウェアに感染しているIoT機器の利用者への注意喚起



調査対象：既にMirai等の**マルウェアに感染している**IoT機器

① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。
※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群
② 当該機器の情報をISPに通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施

IoT機器調査及び利用者への注意喚起の実施状況（2020年12月度）

- 参加手続きが完了している**ISP**（インターネット・サービス・プロバイダ）は**65社**。
  当該ISPの**約1.12億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**２,００２件**の**対象を検知**しISPへ通知。
- **NICTER**による注意喚起は、１日平均**１１３件**の**対象を検知**しISPへ通知。

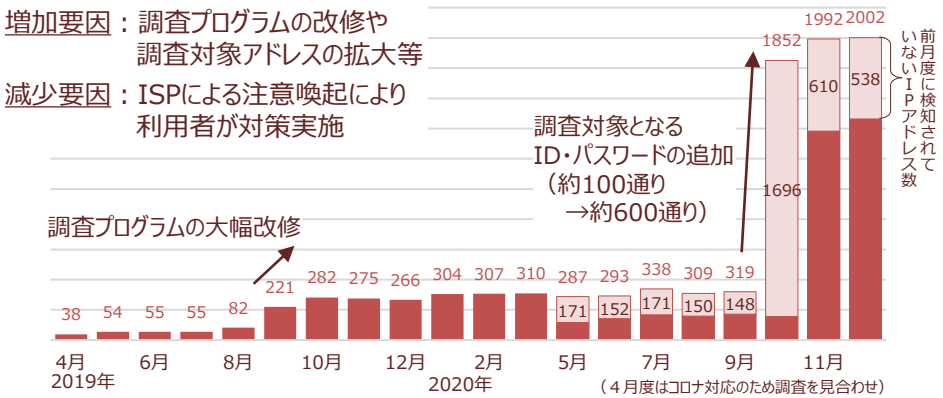
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

２,００２件（11月度:1,992件）

（参考） 2020年度の累積件数：7,392件（2019年度：2,249件）
ID・パスワードが入力可能だったもの：8.6万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

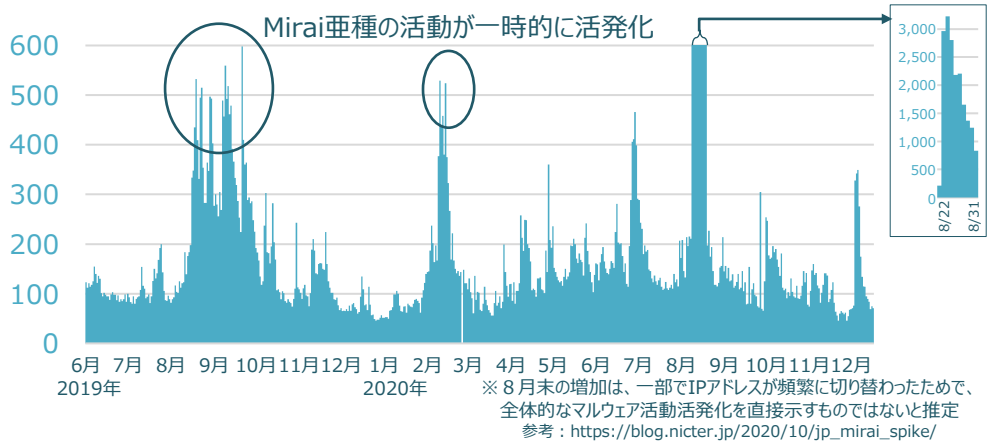
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均１１３件（11月度:114件）

（参考） 期間全体での値： １日平均187件
最小：46件(2020/12/6等)／最大：3,227件(2020/8/24)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



※８月末の増加は、一部でIPアドレスが頻繁に切り替わったためで、全体的なマルウェア活動活発化を直接示すものではないと推定
参考：https://blog.nicter.jp/2020/10/jp_mirai_spike/

NOTICE注意喚起・NICTER注意喚起のいずれについても、前月度から全体として大きな変化はありません。

(一社)デジタルライフ推進協会(DLPA)推奨Wi-Fiルータ

- 一般社団法人デジタルライフ推進協会（DLPA）は、出荷時からセキュリティ対策機能が搭載されている家庭用Wi-Fiルーターを「**DLPA推奨Wi-Fiルータ**」として推奨。
- DLPA加盟社のうち４社※がDLPA推奨Wi-Fiルーターを販売中。

※(株)アイ・オー・データ機器、NECプラットフォームズ(株)、エレコム(株)、(株)バッファロー

DLPA推奨Wi-Fiルータ

以下の２つのセキュリティ対策機能を出荷時から搭載。

① ファームウェアの自動更新

② １台ごとに固有の管理画面用ログインID又はパスワードを設定

（出典：DLPAウェブサイト https://dlpa.jp/wifi_support/）

【(一社)デジタルライフ推進協会（DLPA：Digital Life Promotion Association）について】

一般社団法人 デジタルライフ推進協会 Digital Life Promotion Association

- デジタル技術の進歩により可能となる新たなデジタル技術の活用形態＝「デジタルライフ」における利用者の利便性を守り、その健全な発展に寄与することを目的として、2010年に設立
- デジタルライフの普及・啓発活動や業界共通仕様の策定等を実施
- Wi-Fiルータや外付けハードディスク等のデジタル機器のメーカが加盟

重要IoT機器のセキュリティ対策

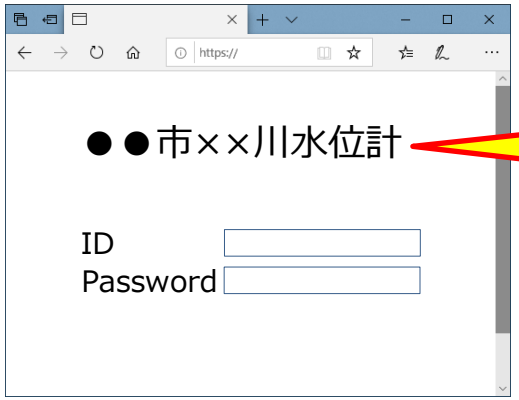
- 重要インフラ等の社会的に影響を及ぼすリスクを伴った使用をしているIoT機器（**重要IoT機器**）について、**公開する必要のない情報が公開されている**など、攻撃を受けやすい**脆弱な状態**にあるものを**検出**する。
- 検出した重要IoT機器について、利用事業者に対して**設定状況等のヒアリング**を行った上で、脆弱な状態を解消するための**注意喚起**や**対策手法の提示**を行い、**対策の完了までのトレース**を行う。

脆弱な状態の例

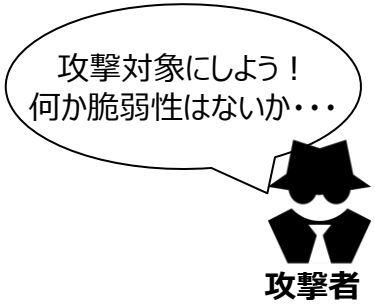
重要IoT機器

インターネットから閲覧可

管理画面



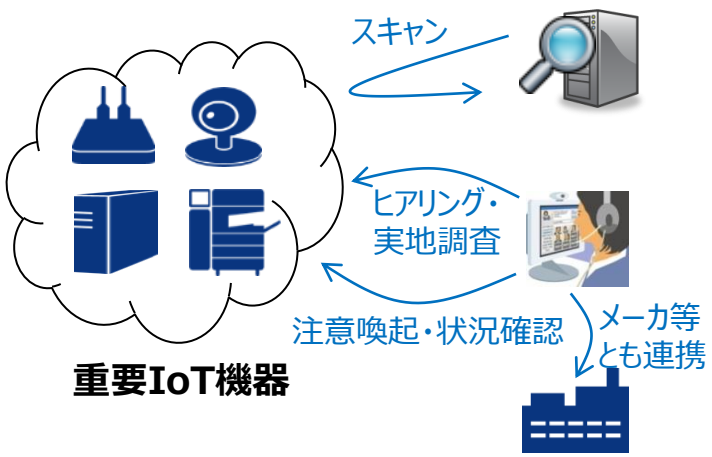
利用事業者や設置場所が推測可能な情報が表示されている



攻撃者

※脆弱な状態かどうかは、想定されるリスクをもとに利用事業者自身が判断する必要はあるが、利用事業者が認識していない場合もあるため、見つけた場合に 注意喚起 することは有効！

対策スキーム



重要IoT機器探索	重要IoT機器？ Web画面が見える？
利用者特定	画面の事業者名は？
利用環境調査	どのような用途か？ どのような設定・管理をしているか？ どのようなネットワーク環境で使っているか？
注意喚起実施	想定されるリスクはどのようなものか 対策にはどのようなものが有効か
対策状況確認	対策の実施に当たり問題はないか？