セキュリティフォーラム2021

共同利用型サテライトオフィスを利用する際の セキュリティ配慮のポイントとは

セキュアIoTプラットフォーム協議会
白水公康

今日のテーマ

テレワーク ＝ 業務

共同利用型オフィス
- サテライトオフィス
- レンタルオフィス
- コワーキングスペース　etc

≒ 職場

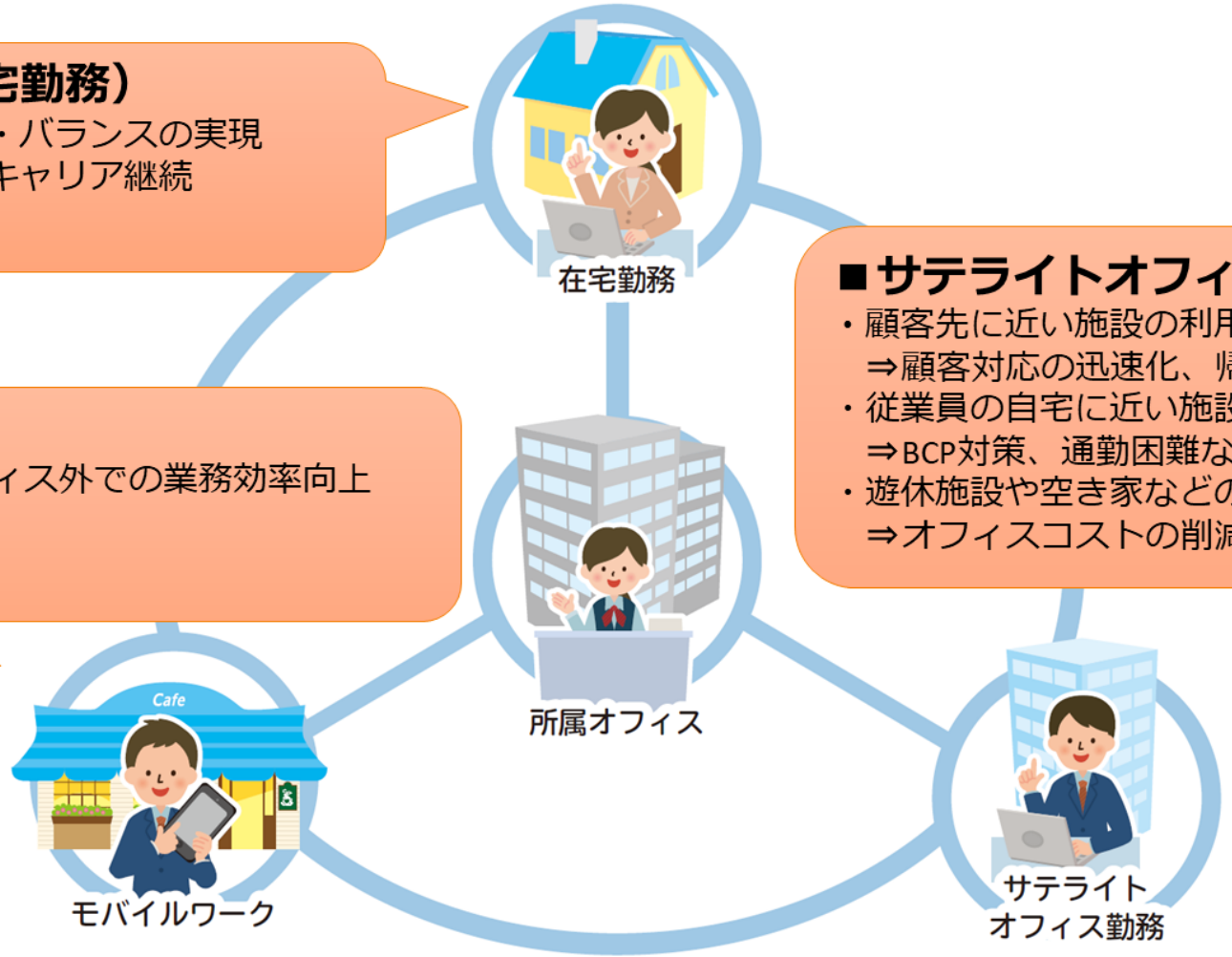
“場”にフォーカスして
テレワークセキュリティのお話しをします

テレワークの形態

■在宅勤務（終日在宅勤務）
・従業員のワーク・ライフ・バランスの実現
・育児・介護期の従業員のキャリア継続
・業務効率の向上

■モバイルワーク
・営業職など、所属オフィス外での業務効率向上
・移動時間の有効活用
・顧客先での迅速な対応

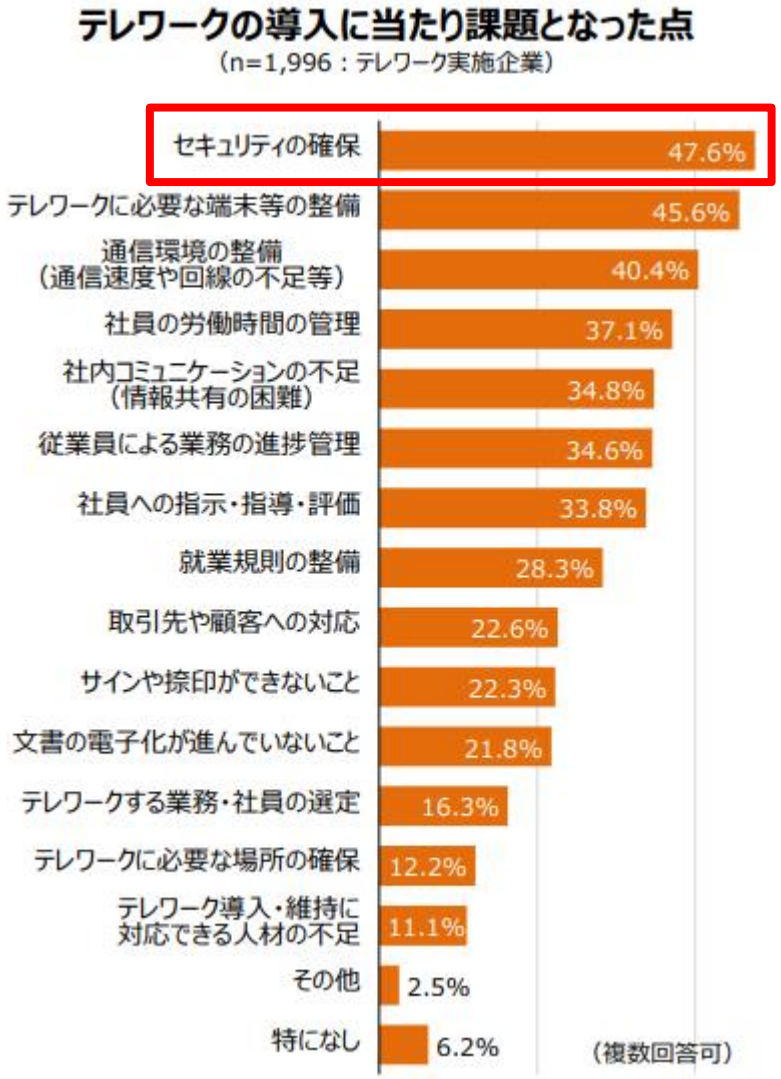
■サテライトオフィス勤務（施設利用型勤務）
・顧客先に近い施設の利用
⇒顧客対応の迅速化、帰社時間削減による効率化
・従業員の自宅に近い施設の利用
⇒BCP対策、通勤困難な人材の活用、
・遊休施設や空き家などの活用
⇒オフィスコストの削減



テレワークの実態と課題

テレワーク実施企業が考える課題

・テレワークの導入にあたっては「セキュリティの確保」が最大の課題

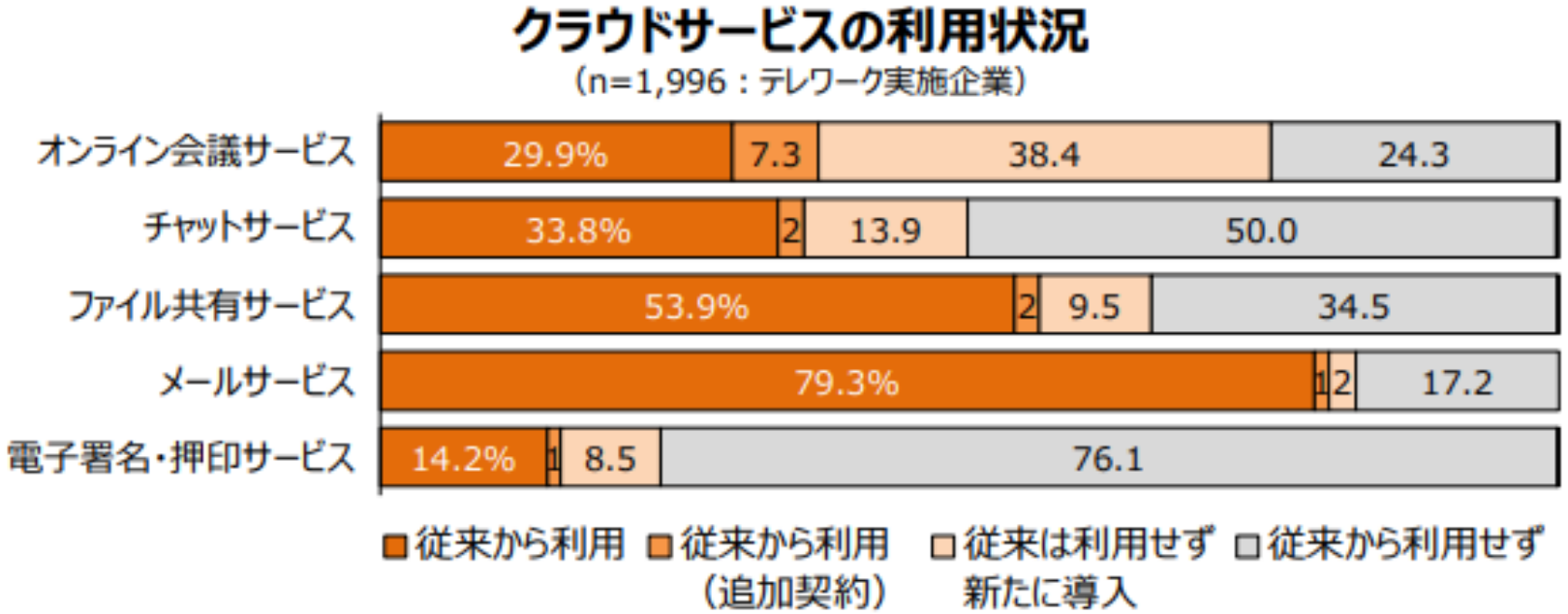


テレワーク利用企業の中で、セキュリティに対する意識が高まっている。

総務省「テレワークセキュリティに関する２次実態調査」
・実施期間：2020年12月16日～2021年1月8日
・サンプル数：5,037社(うちテレワーク実施企業1,996社)
https://www.soumu.go.jp/main_content/000744642.pdf

テレワークの実態：クラウドサービスの活用

- テレワークにおいてはクラウドサービスが広く利用されている



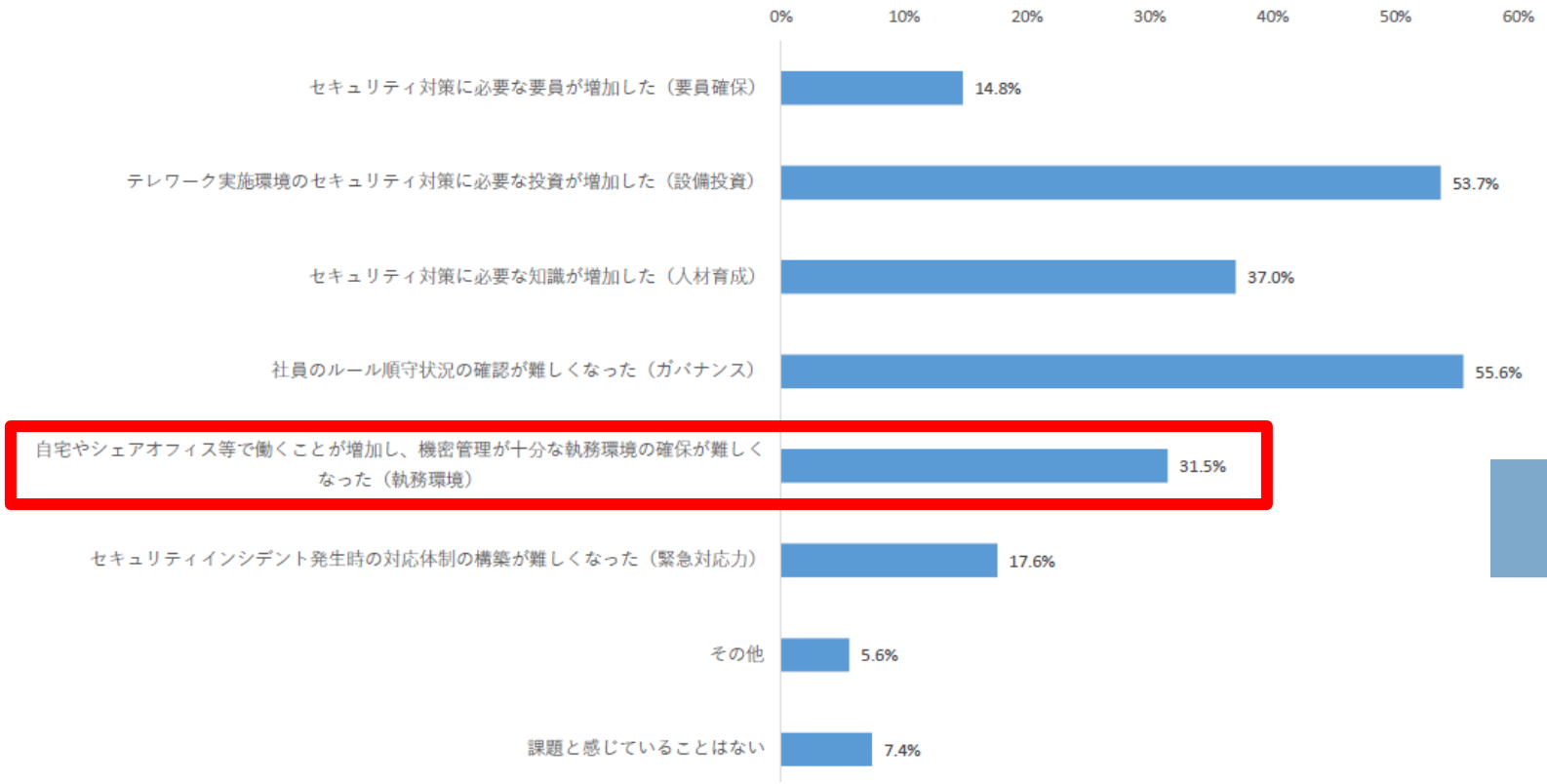
総務省「テレワークセキュリティに関する２次実態調査

クラウド利用には、安全なネットワーク環境が求められる。
安心安全なネットワークが整備されているワークプレイスを
選択することが必要。

テレワークの実態：「働く環境」に対する意識

・テレワークセキュリティに対して、自社で解決する課題に加えて、30%を越える企業が「働く環境の機密管理の確保」について指摘。

図Ⅱ-1-9:テレワーク実施時のセキュリティ上の課題（テレワーク実施経験企業）

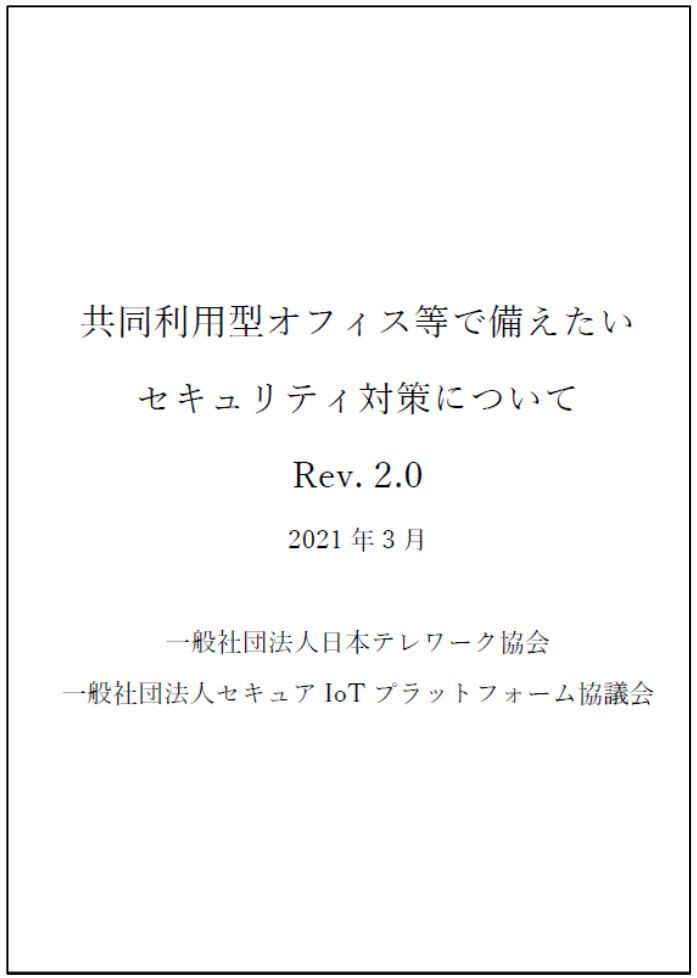


テレワーク実施企業側にも「働く環境」の安全性に対する意識が高まってきている。

IPA（情報処理推進機構）「ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査(組織調査)」
・実施期間：2020年11月18日～12月11日
・サンプル数：505社
https://www.ipa.go.jp/files/000089972.pdf

共同利用型オフィスにおけるセキュリティ対策

共同利用型オフィス等で備えたいセキュリティ対策について

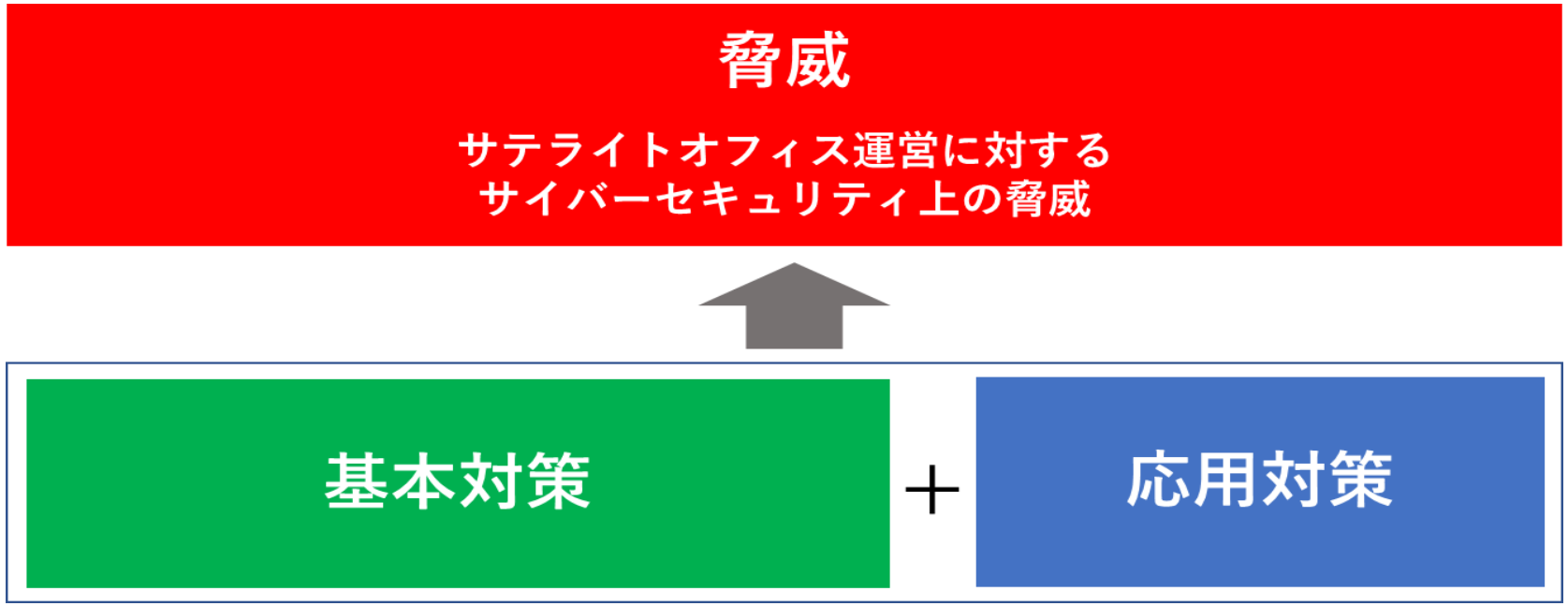


コワーキングスペースやレンタルオフィスなどの**共同利用型オフィスにおけるセキュリティに係る課題と対策**について取りまとめたドキュメント。
日本テレワーク協会とSIOTP協議会で共同の検討会を立ち上げ、テレワーク協会は事業者・利用者の視点で、SIOTP協議会はサイバーセキュリティ技術の視点でそれぞれの課題への対処方法を整理。

【対象】

- 民間企業が運営する共同利用型コワーキングスペース、レンタルオフィス、シェアオフィス
- 自治体や行政が運営する共同利用型コワーキングスペース、レンタルオフィス、シェアオフィス
  - 時間貸、会員制の共同利用型オフィス等を対象とする。
  - 在宅勤務(自宅)、モバイルワーク(カフェ、ラウンジ、移動車内(飛行機、新幹線)、ホテル客室などの宿泊施設については対象外とする。

「共同利用型オフィス等で備えないセキュリティ対策について」構成



【構成】
共同利用型オフィス等の運営に対して、サイバーセキュリティの観点で考えられる**「脅威」**とそれに対して備えるべき最低限必要な**「基本対策」**および状況に応じてさらに望まれる**「応用対策」**から構成。
安全な共同型オフィスを構築には**「基本対策」の要件を満たすことが必須事項**である。
加えて「応用対策」を実施することにより、よりセキュアな環境を整備できる。

情報セキュリティの考え方

人（運用）
- 人的要因によるセキュリティ事故の回避
- ルールの理解とコンプライアンス遵守

ルール（規定類）
- セキュリティポリシーの策定
- ISMSへの対応
- 法令への準拠

技術（システム）
- 通信端末、IoT機器の脆弱性対策
- 情報漏洩対策

ルール・人・技術のバランスが取れた対策が重要

守るべき6つのポイント

1	管理体制（セキュリティポリシー・トレーニング等）
2	入退室管理・利用者情報
3	ネットワーク機器（無線LANアクセスポイント、ルーター等）
4	ネットワーク接続機器（複合機・防犯カメラ等）
5	レンタルPC
6	物理設備（ロッカー等）

1. 管理体制(セキュリティポリシー・トレーニング等)

適切なルール作りと教育により、人的要因によるセキュリティ事故を未然に防ぐこと、万が一発生した場合にも**早期に解決できるような体制**の整備が必要

- 対策①：セキュリティポリシーの制定
  - ✓ 安全な運用規定を明文化したセキュリティポリシーを策定し利用者に明示
  - ✓ セキュリティに関する責任者 や担当組織 (担当者)を明確に する。
- 対策②：利用規約の策定・利用者からの同意
  - ✓ 利用者が利用する際の規約を策定し利用者に共有
  - ✓ 利用規約への同意書に明示的に同意（サイン等）を得て、ルールに基づいた利用を徹底
- 対策③：事故発生対策マニュアルの制定
  - ✓ 事故発生時の対策をまとめたマニュアルに基づき、早期解決を図る
  - ✓ 事故発生時の緊急連絡網も作成する
- 対策④：トレーニング/定期チェック
  - ✓ 「セキュリティポリシー」および「事故発生対策マニュアル」に基づく定期的なチェックおよびトレーニングを行い、セキュリティのためのPDCAサイクルを確立
- 対策⑤：最新のセキュリティ情報の収集・確認
  - ✓ 最新の サイバーセキュリティ情報を常に収集し、必要に応じた対策を実施
  - ✓ 機器の製造ベンダーや IPA(情報処理推進機構)からの注意喚起 に注意する

2. 入退室管理・利用者情報

本人確認と利用状況の把握、入退出管理の徹底により 、 ネットワークへの不正侵入や情報漏えいなどのセキュリティ事故の発生を防ぐ体制の整備が必要

- 対策①：利用者の本人確認
  - ✓ 写真付き身分証明書(マイナンバーカード、運転免許証、パスポートなど) による本人確認を行う
- 対策②：個人情報の適切な管理
  - ✓ 個人情報保護方針を定め公表する
  - ✓ 個人情報の取扱い方法について、 管理運用ルールを明文化し、徹底する
- 対策③： Webサイトの適切な管理
  - ✓ 利用 登録をはじめ個人情報の入力等を求める場合は、 TLS通信(https)を行う
- 対策④：利用ログの取得・管理
  - ✓ 事故発生時 の 追跡可能性を確保するため、 利用ログ 利用者、利用時間、利用リソースなどを取得
- 対策⑤(応用)：電子的な入退出管理システムの導入
  - ✓ IC カード型やスマートフォンアプリ型会員証など電子的に入退出の管理ができるシステムを導入
  - ✓ 多要素認証、生体認証システムや電子証明書により厳密にユーザーを管理することが望ましい

3. ネットワーク機器（無線LANアクセスポイント、ルーター等）

最新ファームウェアの更新や適切なネットワーク設定により、機密情報の漏洩や不正アクセスや乗っ取りを防止することが必要

- 対策①：最新のファームウェアの適用
  - ✓ ベンダーからのアップデートを定期的に確認する体制構築し、リリース後はすぐに適応する
  - ✓ 自動的にファームウェアをアップデートする機能がある場合には有効にする
  - ✓ 保守期間が過ぎたネットワーク機器は使用しない
- 対策②：管理者パスワードの適切な設定
  - ✓ 出荷時のデフォルト設定のままにせず、第三者に推測されにくい複雑なパスワードに変更
  - ✓ 管理者用パスワードについては定期的に更新する必要はない
- 対策③：無線LANアクセスポイントの適切な設定
  - ✓ 暗号化方式として最新のパッチが当たったWPA2もしくはWPA3を選択
  - ✓ 共同利用型オフィス等の外に漏れる電波を最小限にするため適切な電波強度で利用する。
- 対策④：無線LANアクセスポイントのパスフレーズの設定と管理
  - ✓ 管理者パスワードとは別の第三者に推測されにくい複雑な管理者パスフレーズを設定
  - ✓ 設定したパスフレーズは、利用者のみが知ることができる方法を徹底する
  - ✓ 不特定多数に対してパスワードを公開している場合は、一定の頻度(例：毎月)で更新する

3. ネットワーク機器（無線LANアクセスポイント、ルーター等）

- 対策⑤：利用者の端末間通信の禁止設定
  - ✓ Wi-Fiで接続している端末同士の通信を不可にすること
    →「ネットワーク分離機能」や「プライバシーセパレーター機能」と呼ばれる設定を有効化
  - ✓ 無線 LAN 対応プリンタ やネットワーク対応複合機を利用する場合は、ネットワーク構成を適切に設定する
- 対策⑥：業務用ネットワークとの分離
  - ✓ 利用者に開放するネットワークは、業務システムとは独立して設置するか、仮想的にネットワークを分離する技術である VLAN の導入し、安全に分離する
- 対策⑦：アクセスログの適切な管理
  - ✓ 高いプライバシー性を持つアクセスログは、ネットワーク機器のトラブル原因の把握や利用者からの問合せ対応等、 業務上必要な最小限の記録に留め、取り扱いには十分に注意する
- 対策⑧(応用)：高度なセキュリティの導入
  - ✓ 無線LAN アクセスポイントと接続端末等について、電子証明書等を活用して相互に認証を行い、なりすましや許可されていない端末の接続を制限することが望ましい
  - ✓ MAC アドレスのフィルタリング設定を行い、端末の接続を制限することが望ましい
  - ✓ 業務で利用サーバーへのアクセスについて多要素認証の仕組みを導入するすることが望ましい
  - ✓ 接続状況の可視化を行い、接続機器を乗っ取りや遠隔操作などから守るサービスや製品を利用することが望ましい

4. ネットワーク接続機器（複合機・防犯カメラ等）

複合機や防犯カメラなど付帯設備についても、Wi-Fi機器と同様に適切な設定と運用の実施より、一定のセキュリティ基準を担保

- 対策①：最新のファームウェアの適用
  - ✓ ベンダーからのアップデートを定期的に確認する体制構築し、リリース後はすぐに適応する
  - ✓ 自動的にファームウェアをアップデートする機能がある場合には有効にする
  - ✓ 保守期間が過ぎたネットワーク機器は使用しない
- 対策②：管理者パスワードの適切な設定
  - ✓ 出荷時のデフォルト設定のままにせず、第三者に推測されにくい複雑なパスワードに変更
  - ✓ 管理者用パスワードについては定期的に更新する必要はない
- 対策③：機器設定の確認
  - ✓ アクセス権限の範囲など、機器設定が意図したものとなっているか十分に確認を行う
- 対策④：複合機のインターネット接続の禁止
  - ✓ 原則として 外部ネットワーク に接続しない
  - ✓ ファイアウォール等を設置した上で接続 IP アドレスを制限する
- 対策⑤：複合機に蓄積されたデータの消去
  - ✓ ハードディスク蓄積データの「暗号化」および「消去」設定機能がある場合、有効化する
- 対策⑥(応用)：ID カードやパスワードによる 複合機の 出力管理
  - ✓ ID カードやパスワード入力による出力制御の仕組みを導入することが望ましい

5. レンタルPC

レンタルPC のマルウェア感染を防止することにより、利用者が取り扱う情報の漏えいを防止することが必要

- 対策①：インストールされたソフトウェアの最新化
  - ✓ OS、アプリケーションは、アップデートを行い常に最新の状態を維持する
  - ✓ サポート期限の切れた製品を利用しない
  - ✓ フリーソフトを使用する場合は、信頼性や脆弱性を確認した上で、導入は必要最低限に留める
- 対策②：環境設定の初期化・復元
  - ✓ 不要なソフトウェアのインストールやマルウェアの感染、ファイルの削除忘れ、 ブラウザの閲覧履歴が残存などのトラブル を避けるため、環境設定の初期化・復元を行った上で貸し出しを行う
- 対策③(応用)：のぞき見防止フィルタ
  - ✓ 物理的な情報漏洩を防ぐため、のぞき見防止フィルタを導入することが望ましい

6. 物理設備

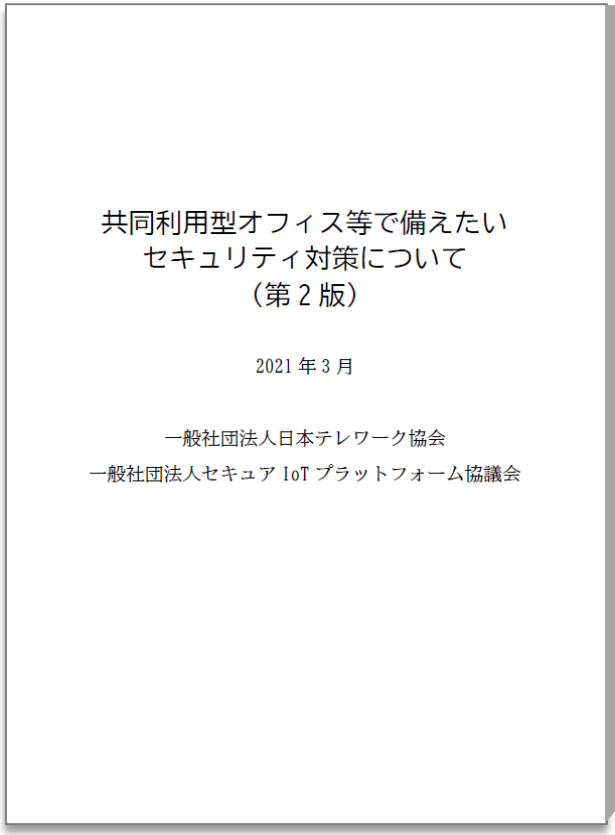
オンライン会議の音漏れによる機密情報漏洩や書類の放置など物理的な側面でセキュリティ事故を防止することが必要

- 対策①：オンライン(Web)会議等の音声利用のための場所の確保
  - ✓ 利用者は、他の利用者から隔離されている場所を確保する
  - ✓ 時間貸しの個室や会議室、ブース型等の防音設備がある施設を利用する
- 対策②(応用)：スマートロッカーの導入
  - ✓ 安全に手荷物を管理できるように、IC カード型会員証やスマートフォンで閉・開錠可能なスマートロッカーを設置することが望ましい
- 対策④(応用)：シュレッダ ー、溶解BOXの導入
  - ✓ 不要となった機密書類やメディアを安全に廃棄するためのシュレッダーや溶解BOXを設置することが望ましい

共同利用型オフィス等セキュリティ認証プログラム

安心・安全な施設環境整備

「共同利用型オフィス等で備えたいセキュリティ対策について（第2版）」を指針とし、
共同利用型コワーキングスペース、レンタルオフィス、シェアオフィス等の
情報セキュリティへの適合性を検査し、検査結果を認証



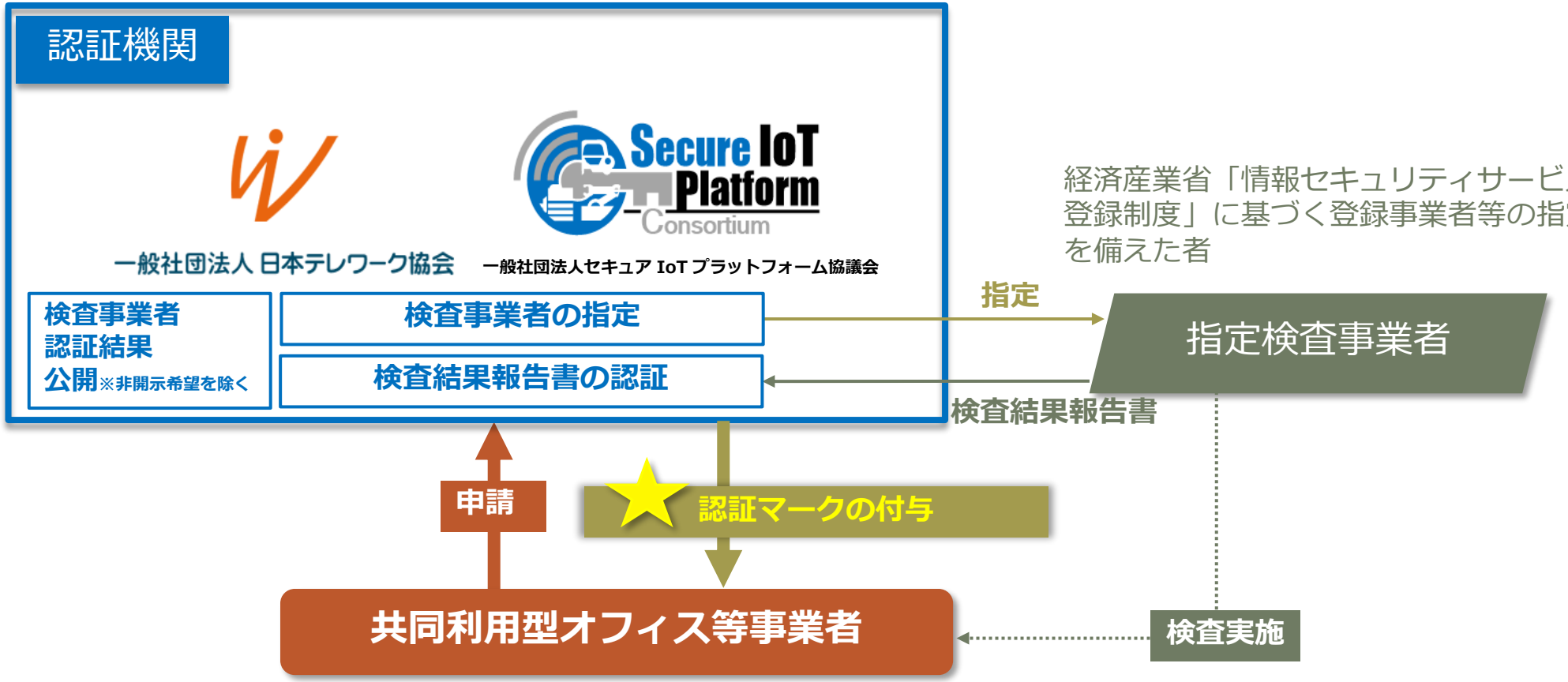
セキュリティ課題と対策

1	管理体制（セキュリティポリシー・トレーニング等）
2	入退室管理・利用者情報
3	ネットワーク機器（無線LANアクセスポイント、ルーター等）
4	ネットワーク接続機器（複合機・防犯カメラ等）
5	レンタルPC
6	物理設備（ロッカー等）

基本対策／応用対策

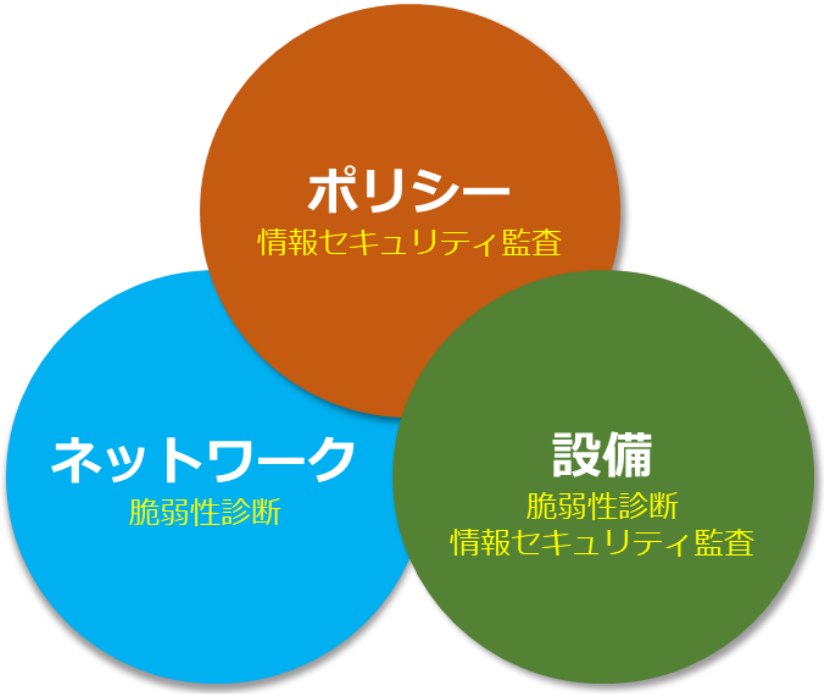
認証プログラムの運営体制

該当施設が認証基準に適合しているか検査する「指定検査事業者」と、検査結果報告を基に安全性を認証する「認証機関」により構成され独立して運用。
検査事業者の指定は規定に基づき認証機関が実施するが、検査結果報告書に記載された評価の審査・判定は、各指定検査機関がその責任において実施する。認証機関はこの審査・判定に何ら関与しない。



共同利用型オフィス等のセキュリティ対策に係る認証プログラム

ポリシー、ネットワーク、設備について、利用者が信頼して安全にテレワークできる環境か総合的に評価



	共同利用型オフィス等セキュリティ基本対策	対策カテゴリ	検査
1	管理体制の整備	ポリシー	情報セキュリティ監査
2	入退室・利用者情報の管理	ポリシー	情報セキュリティ監査
3	ネットワーク機器のセキュリティ対策	ネットワーク	脆弱性診断
4	ネットワーク接続機器のセキュリティ対策	ネットワーク	脆弱性診断
5	レンタルPCのセキュリティ対策	設備	脆弱性診断
6	物理設備のセキュリティ対策	設備	情報セキュリティ監査

	レベル	リスク	説明
情報セキュリティ監査	A	無	堅牢な情報セキュリティ対策が実施されており、リスク発生する可能性は低い
	B	低	情報資産・個人情報管理とネットワーク対策の見直しを継続することで、リスク発生を防止できる
	C	中	リスク発生の可能性があり、利用者への注意喚起と定期的にネットワーク検査を行いリスク把握と対策が必要
	D	高	リスク発生する可能性が非常に高く、基本対策に基づき組織的に対策構築が必要
	E	緊急	ガイドラインに基づき、セキュリティポリシーや規約の策定、体制整備から対応が必要

	レベル	リスク	説明
脆弱性診断	A	無	セキュアな状態：ガイドライン準拠
	B	低	将来的に改修が推奨される状態：直接的にシステム侵入につながらないリスク
	C	中	将来的に改修が必要な状態：システム停止やシステム設定情報の漏洩リスク
	D	高	改修が必要な状態：システム侵入やページ改ざん、機密情報や個人情報情報の漏洩リスク
	E	緊急	早急に改修が必要な状態：システム侵入やページ改ざん、情報漏洩につながる指摘事項

認証機関による認証レベルの付与

検査結果報告書の判定結果を基に、認証レベルに応じて星を付与

認証レベル	評価	リスク	説明	検査	判定基準
★★★	信頼	低	ガイドライン準拠以上の高度な情報セキュリティ対策が構築されており、利用者が信頼してテレワークが可能	情報セキュリティ監査	総合評価「A」
				脆弱性診断	総合評価「A」「B」
★★	安全	中	基本対策に適合した情報セキュリティ対策が実装されているが潜在しているリスクの確認と対策向上により安全	情報セキュリティ監査	総合評価「B」
				脆弱性診断	総合評価「B」
★	安心	注意	基本対策の一部に適合した情報セキュリティ対策が実装されているが利用者は注意してテレワークを行う必要がある	情報セキュリティ監査	総合評価「C」
				脆弱性診断	総合評価「C」
認証不可 認証には是正が必要	注意	高	サイバー攻撃や内部不正によるリスク発生の可能性が非常に高く、テレワーク環境の提供に不適合	情報セキュリティ監査	総合評価「D」「E」
				脆弱性診断	総合評価「D」「E」

●よく見られるリスク

- SSID/パスワードがオープンに公開されており、外部からのハッキングを許す環境にある
- 通信機器やネットワークに接続される機器のファームウェアが最新にアップデートされておらず、脆弱性を持ったまま運用され、マルウェアの混入を受ける恐れがある。
- 利用者の個人情報や利用ログが適切に保管されておらず、個人情報やプライバシー情報の流出の恐れがある

参考資料

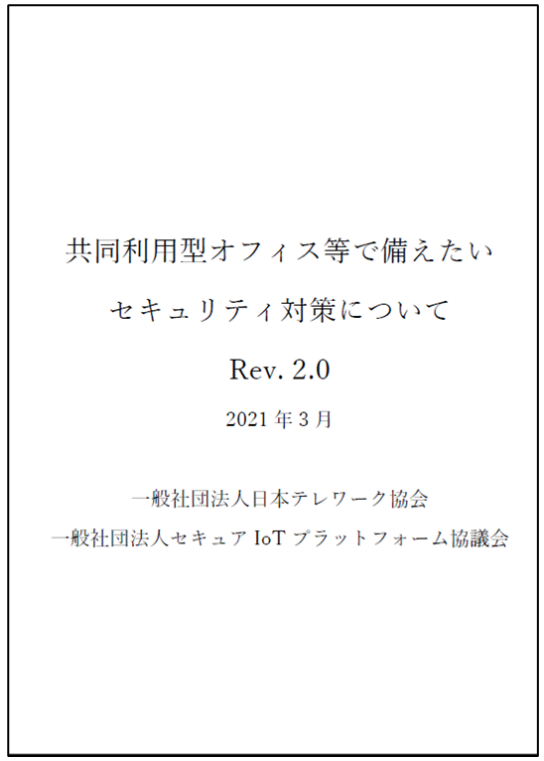
●テレワーク実施者向け

https://www.soumu.go.jp/main_content/000752925.pdf

●Wi-Fi提供者・利用者向け

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

●サテライトオフィス事業者向け


共同利用型オフィス等で備えたい

セキュリティ対策について

Rev. 2.0

2021 年 3 月

一般社団法人日本テレワーク協会

一般社団法人セキュア IoT プラットフォーム協議会

https://www.secureiotplatform.org/static/images/2021-03-17.pdf