セキュリティフォーラム2022

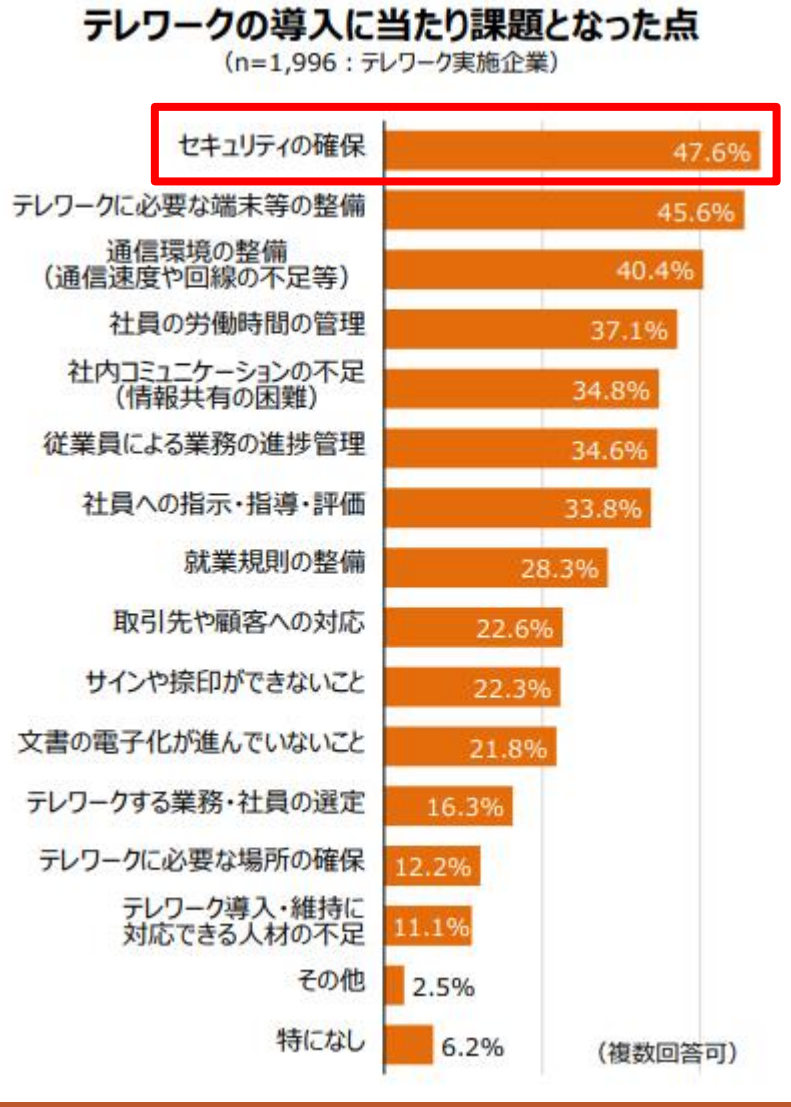
共同利用型サテライトオフィスを利用する際のセキュリティ配慮のポイントとは？

一般社団法人セキュアIoTプラットフォーム協議会
事務局長
白水 公康

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



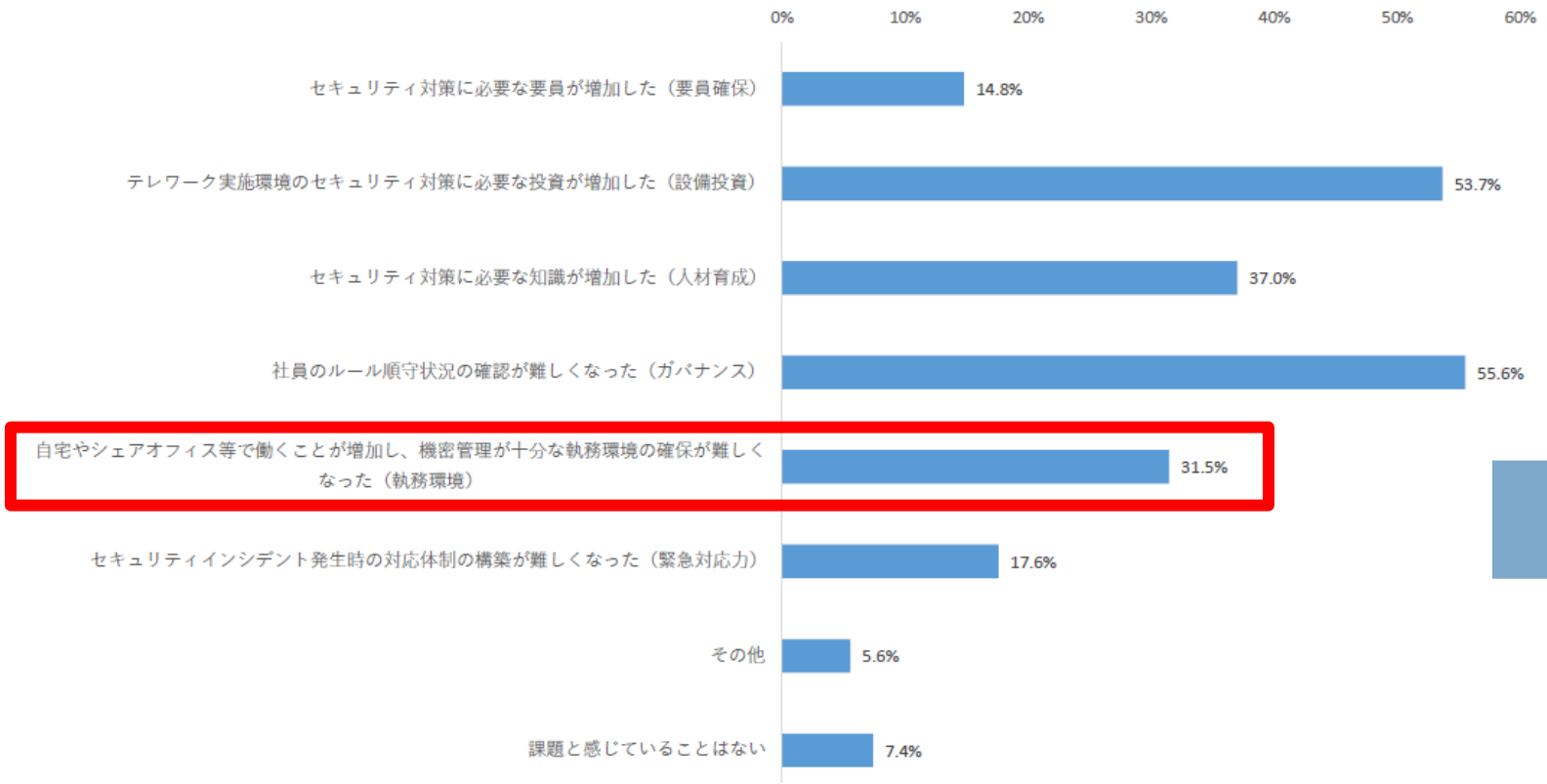
テレワーク利用企業の中で、セキュリティに対する意識が高まっている。

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：「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）

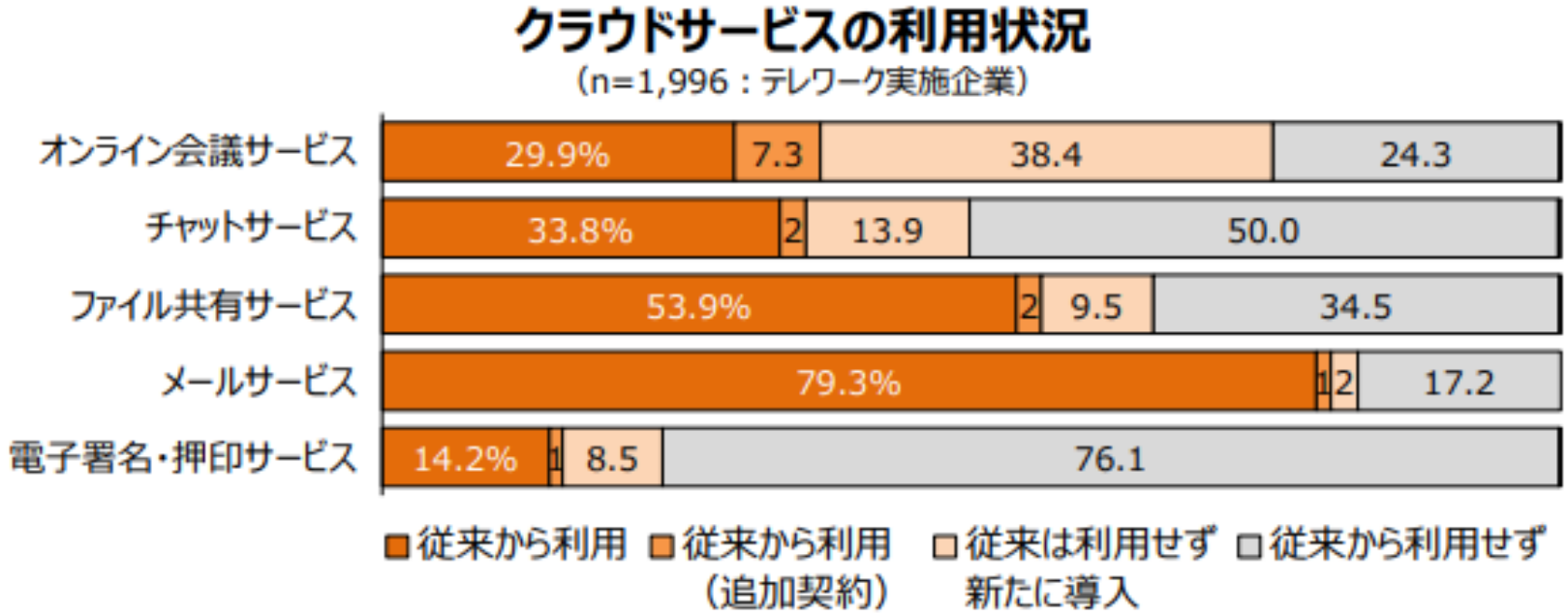


テレワーク実施企業側にも「働く環境」の安全性に対する意識が高まってきている。

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

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。**

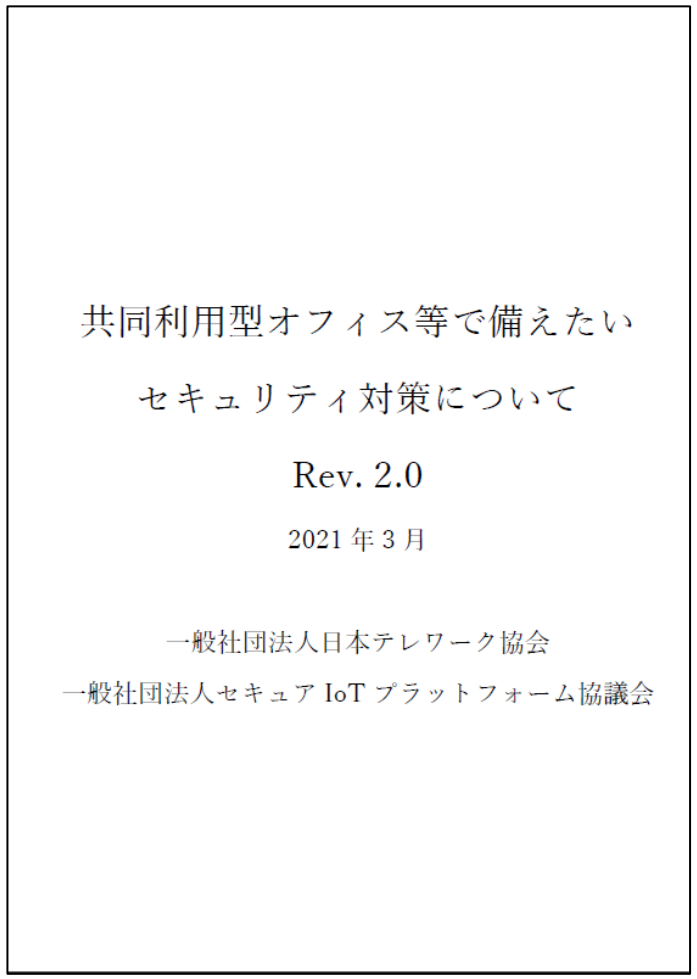
IPA 情報セキュリティ10大脅威 2021 (2021年8月21日)

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	NEW テレワーク等のニューノーマルな働き方を狙った攻撃
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの不正ログイン
不正アプリによるスマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

コロナ禍の影響により、テレワークが常態化。
今までテレワークに取り組むことができなかった業種においても導入の動きが促進され、その前提としてセキュリティ実装が求められている。

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



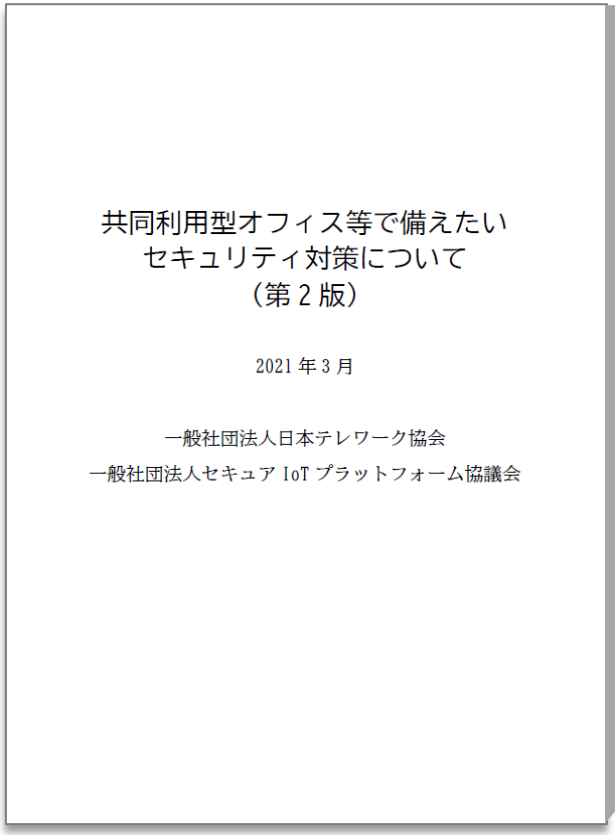
コワーキングスペースやレンタルオフィスなどの**共同利用型オフィスにおけるセキュリティに係る課題と対策**について取りまとめたドキュメント。
日本テレワーク協会とSIOTP協議会で共同の検討会を立ち上げ、テレワーク協会は事業者・利用者の視点で、SIOTP協議会はサイバーセキュリティ技術の視点でそれぞれの課題への対処方法を整理。

総務省令和３年度予算「情報通信利用促進支援事業費補助金（地域サテライトオフィス整備推進事業）」における提案事業のセキュリティ要件に採用

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



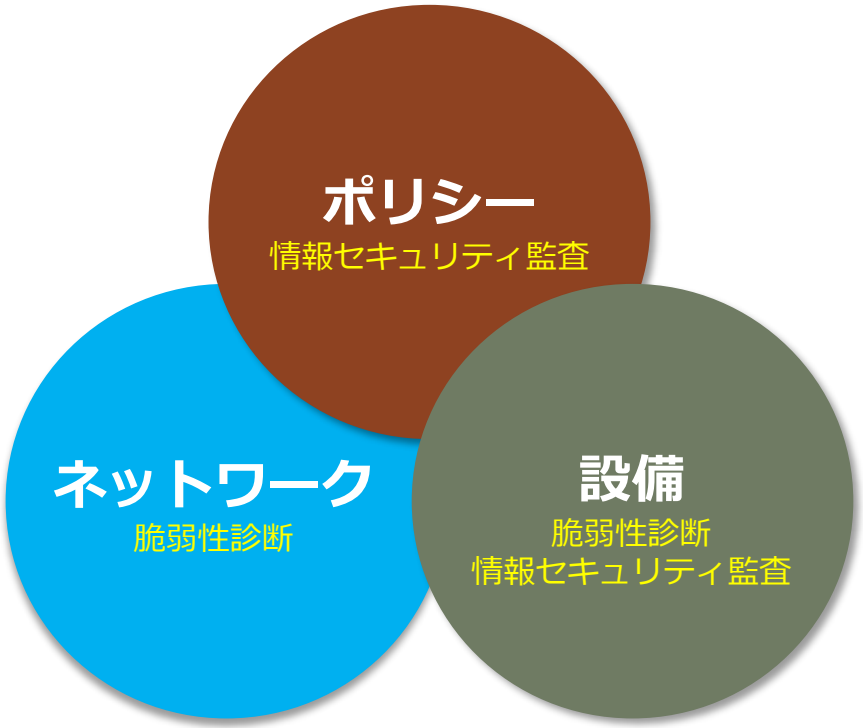
セキュリティ課題と対策

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

認証基準への適合性について

本プログラムの認証を希望する事業者の運営する施設が、ポリシー、ネットワーク、設備について認証基準の基本対策に適合しており、利用者が信頼して安全にテレワークできる環境か、認証機関が指定した検査事業者による検査において総合的に評価する。



	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

共同利用型オフィス等で備えるべきセキュリティ対策を見える化

検査事業者による適合性審査と判定

検査事業者は検査結果に基づき、セキュリティレベルを審査・判定

	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
	D	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

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。