共同利用型オフィス
セキュリティ認証プログラムについて

セキュアIoTプラットフォーム協議会
白水公康

一般社団法人セキュアIoTプラットフォーム協議会

セキュアIoTプラットフォーム協議会は、日本の産業界の知見を集約し、

全世界のIoT機器およびサービスに対し、安心・安全な新社会基盤を創出する。

2020年までに全世界で500億台以上がネットワークに接続されるIoT機器利用者が、
安心・安全にIoT機器やそのサービスを利活用できるよう、
全世界標準かつデファクトなセキュリティ基盤を構築する。

国際標準や国の指針に定義されているセキュリティ要件を具現化するための実装レベルの仕様作りを目指す。

IoTデバイス製造レイヤ	ネットワークレイヤ	データ管理レイヤ	サービスレイヤ
ICチップへの証明書の埋め込みによるデバイスの真正性の認証	高度暗号化、接続の際のなりすましの排除、改ざん防止	ビッグデータの匿名化および暗号化データ処理による安全性向上	プライバシー保護、暗号化、改ざん、フィッシング防止

一般社団法人セキュアIoTプラットフォーム協議会

事業	・次世代IoTセキュリティ標準の規格化およびデファクトスタンダード化に向けての普及活動 ・IoT利活用推進および事例構築 ・共同実証実験(POC)の実施 ・最新IoT関連情報の発信 ・セキュリティ人材の育成 ・セキュリティ関連認証事業
設立年月日	2017年4月3日
法人形態	一般社団法人
参加企業種別	・半導体メーカー ・クラウドサービス事業者 ・データアナリティクスサービス事業者 ・アプリケーション開発ベンダー ・サービス提供事業者 ・IoT機器製造メーカー ・データセンター事業者 ・セキュリティベンダー ・システムインテグレーター ・関連協議会 ・自治体 ・大学/学術機関
役員構成	・理事長：辻井 重男　（中央大学研究開発機構フェロー・機構教授、東京工業大学名誉教授） ・理事　：後藤 厚宏　（情報セキュリティ大学院大学 学長） 白鳥 則郎　（中央大学研究開発機構 教授） 田口　勉　（Neutrix Cloud Japan 株式会社　代表取締役社長 CEO） 長谷川 聡　（株式会社ユビキタスAIコーポレーション 代表取締役社長） 椛澤 慎之助　（セコムトラストシステムズ株式会社執行役員） 眞柄 泰利　（サイバートラスト株式会社 代表取締役社長） 三木 俊明　（株式会社ラック アソシエイト） ・監事　：佐々木 良一　(東京電機大学総合研究所特命教授兼サイバーセキュリティ研究所所長) 森本 登志男　(キャリアシフト株式会社 代表取締役、前佐賀県最高情報統括監(CIO) 総務省地域情報化アドバイザー)
会費	・入会金：10万円 ・正会員：年会費:20万円、準会員:5万円　賛助会員：無料　学術会員：無料 ・初年度会費は、入会時期によって2期に分けて設定（4～9月入会:20万円/10～3月入会:10万円/正会員の場合）
HP	https://www.secureiotplatform.org/

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

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

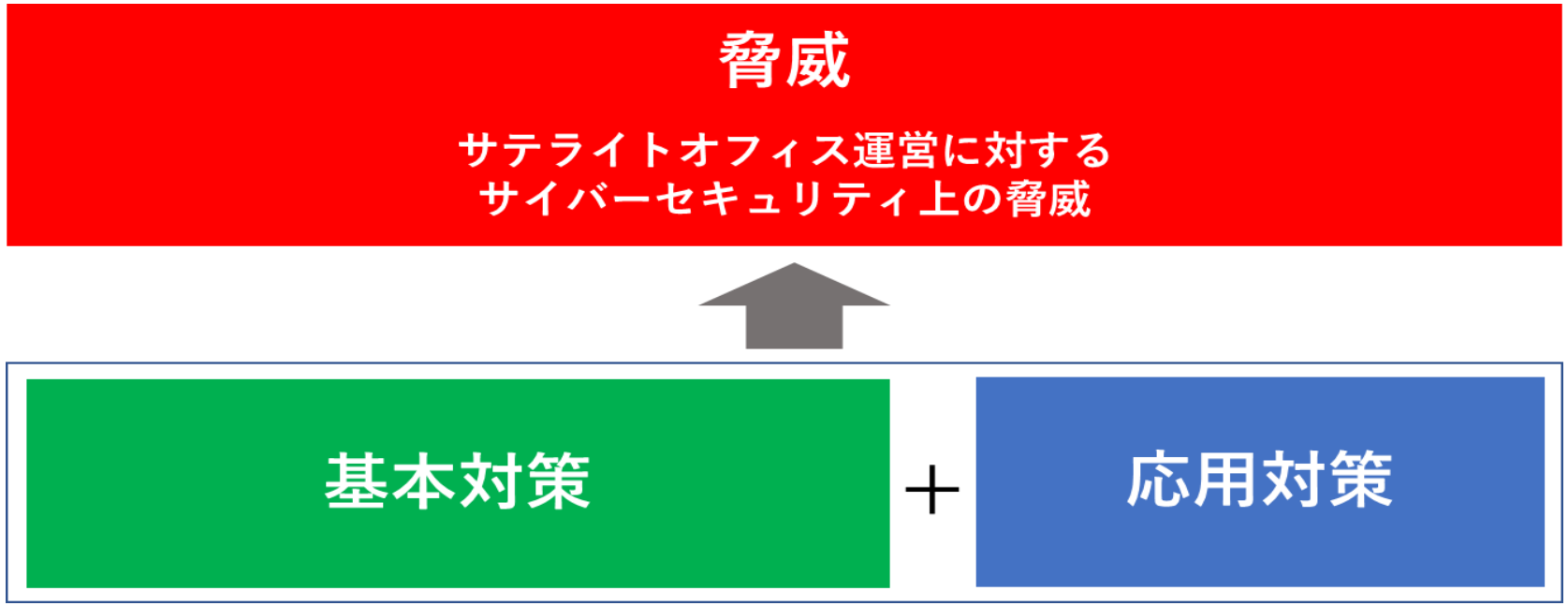
一般社団法人セキュア IoT プラットフォーム協議会

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。

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

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（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

ルール・人・技術のバランスが取れた対策が重要

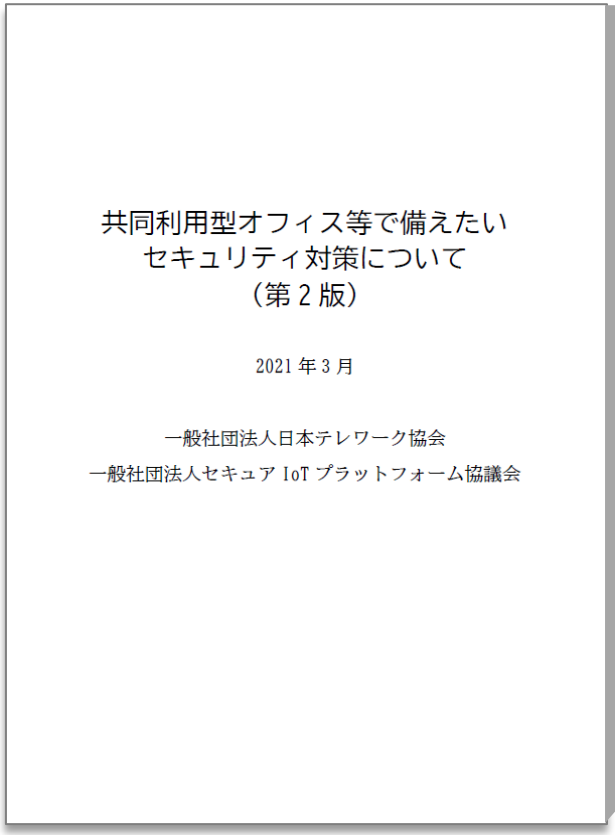
守るべき6つのポイント

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）

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


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）

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

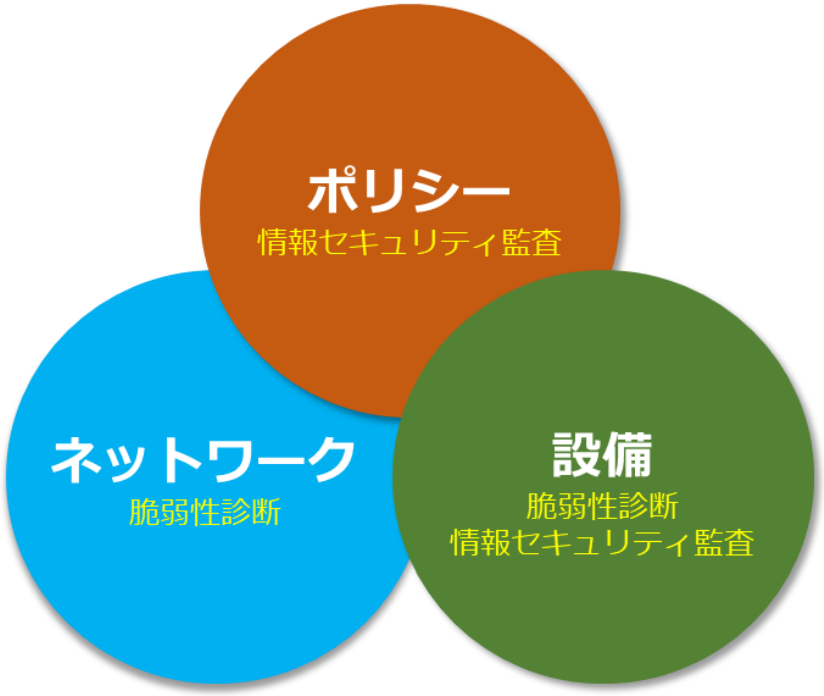
セキュリティ課題と対策

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

共同利用型オフィスセキュリティ認証プログラム

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

情報セキュリティ監査：評価一覧

セキュリティ課題と対策		検査科目				基準		
		#	項目	分類	確認内容	★	★★	★★★
1	管理体制（セキュリティポリシー・トレーニング等）	1	基本対策	基本対策①	セキュリティポリシーの策定	●	●	●
		2		基本対策②	利用規約の作成・利用者からの同意	●	●	●
		3		基本対策③	事故発生対応マニュアルの整備	●	●	●
		4		基本対策④	トレーニング・定期チェック	●	●	●
		5		基本対策⑤	最新のセキュリティ情報の収集・確認	●	●	●
2	入退室管理・利用者情報	6	基本対策	基本対策①	利用者の本人確認	●	●	●
		7		基本対策②	個人情報の適切な管理	●	●	●
		8		基本対策③	Webサイトの適切な管理	●	●	●
		9		基本対策④	利用ログの取得・管理	●	●	●
		10	応用対策	応用対策⑤	電子的な入退室管理システムの導入	-	▲	●
		11		応用対策⑥	生体認証システムの導入	-	▲	●
		12		応用対策⑦	会員区分の明確化	-	▲	●
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）	13	基本対策	基本対策①	最新ファームウェアの適用	●	●	●
		14		基本対策②	管理者パスワードの適切な設定	●	●	●
		15		基本対策③	無線LANアクセスポイントの適切な設定	●	●	●
		16		基本対策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	●	●	●
		17		基本対策⑤	利用者の端末間通信の禁止設定	●	●	●
		18		基本対策⑥	業務用ネットワークとの分離	●	●	●
		19		基本対策⑦	アクセスログの適切な管理	●	●	●
		20	応用対策	応用対策⑧	高度なセキュリティの導入	-	▲	●
4	ネットワーク接続機器（複合機・防犯カメラ等）	21	基本対策	基本対策①	最新ファームウェアの適用	●	●	●
		22		基本対策②	管理者パスワードの適切な設定	●	●	●
		23		基本対策③	機器設定の確認	●	●	●
		24		基本対策④	複合機のインターネット接続の禁止	●	●	●
		25		基本対策⑤	複合機に蓄積されたデータの消去	●	●	●
		26	応用対策	応用対策⑥	IDカードやパスワードによる複合機の出力管理	-	▲	●
5	レンタルPC	27	基本対策	基本対策①	インストールされたソフトウェアの最新化	●	●	●
		28		基本対策②	環境設定の初期化・復元	●	●	●
		29	応用対策	応用対策③	のぞき見防止フィルタ	-	▲	●
6	物理設備（ロッカー等）	30	基本対策	基本対策①	オンライン（Web）会議等の音声利用のための場所の確保	●	●	●
		31	応用対策	応用対策②	スマートロッカーの導入	-	▲	●
		32		応用対策③	シュレッダー、溶解BOXの導入	-	▲	●

●	準拠が必要
▲	一部準拠で可
-	評価対象外

脆弱性診断

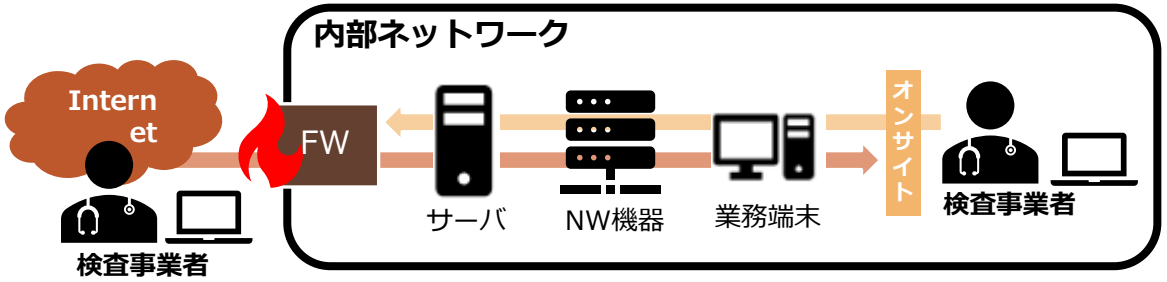
セキュリティ監査に加えて、技術的脆弱性診断を実施し、認証基準の対象となるネットワークおよび設備の**サイバーセキュリティ対策への適合性を検査する。**

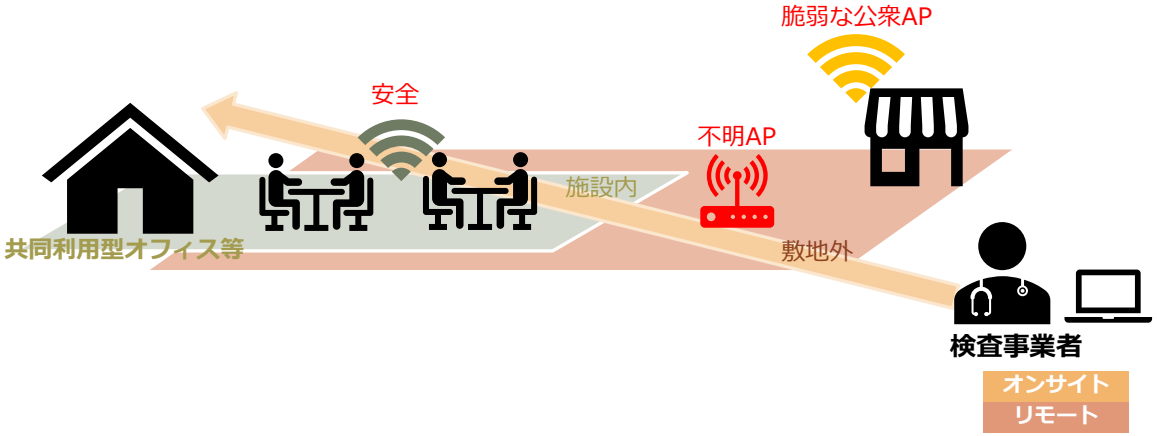
検査手法①：ネットワーク脆弱性検査

ネットワーク機器およびサーバー、OS、データベース、ミドルウェアに対して、既知の脆弱性やセキュリティ上危険な設定がされたパラメーターなど不正侵入の要因となる要素を調査

検査手法②：WiFi脆弱性検査

施設内や敷地外に存在するアクセスポイントを対象に、無線通信の暗号強度、脆弱な設定が無いか調査。無線LAN環境における盗聴、なりすまし(アクセスポイント)、不正侵入の可能性を確認





脆弱性診断：評価一覧

			検査方法	基準		
				★	★★	★★★
ネットワーク脆弱性検査	ホストのスキャン	ポートスキャン	TCP全ポートに対するポートスキャンにより、ホストの応答を確認する	▲	●	●
		実行中のサービスの検出	バナー情報などからソフトウェアバージョンを検知する	▲	●	●
			バージョンに存在する脆弱性を調査する	▲	●	●
	ネットワークサービスの脆弱性	DNSに関する調査	再帰問い合わせの可否を確認する	-	▲	●
			DNSゾーン転送の可否を確認する	-	▲	●
		メールサーバに関する調査	メールサーバでの第三者中継の可否を確認する	-	▲	●
			VRFYコマンド、EXPNコマンドの可否を確認する	-	▲	●
		FTPに関する調査	anonymousユーザの許可・権限を確認する	-	▲	●
		Windowsネットワークサービスに関する調査	インターネット経由でのアクセス可否を確認する	-	▲	●
			システム・ユーザ情報の取得可否を確認する	-	▲	●
			Nullセッション接続の可否を確認する	-	▲	●
		SNMPに関する調査	SNMPによるシステム情報の取得可否を確認する	-	▲	●
			デフォルトコミュニティ名（public,private)による接続可否を確認する	-	▲	●
		SSHサーバに関する調査	パスワード認証が許可されていないか確認する	-	▲	●
		データベースサーバに関する調査	インターネット経由でのアクセス可否を確認する	-	▲	●
	Webサーバの脆弱性	Webサーバの脆弱性	サポートするHTTPメソッドを確認する	-	▲	●
			TRACE/TRACKのサポート有無を確認する	-	▲	●
			Apache系のExpectヘッダXSS有無を確認する	-	▲	●
			Apache系の403エラーUTF7XSS有無を確認する	-	▲	●
			IISのレスポンスヘッダによる内部IPアドレス開示有無を確認する	-	▲	●
			SSL証明書の正当性を確認する	-	▲	●
			SSLv2サポートの有無を確認する	-	▲	●
			弱い暗号化方式の使用可否を確認する	-	▲	●
	各種OSの脆弱性	Windowsの既知の脆弱性	バージョン・得られたシステム情報より、未適用パッチを特定する	▲	●	●
		その他各種OSの既知の脆弱性	バージョン情報より既知の脆弱性を特定する	▲	●	●
	悪意あるソフトウェア	バックドアの調査	バックドアの可能性が高い、非標準ポートで動作しているサービスを確認する	-	▲	●
		P2Pソフトウェアの調査	P2Pソフトウェアが動作していないか確認する	-	▲	●
	ネットワーク機器の脆弱性	各種ネットワーク機器の既知の脆弱性	機器が特定できた場合、既知の脆弱性を確認する	▲	●	●
WIF脆弱性検査	アクセスポイントのスキャン	SSIDをブロードキャストしているアクセスポイントの検	診断地点にてビーコン信号を発信しているアクセスポイントを検出する	▲	●	●
		アクセスポイントの調査	検出されたアクセスポイントを管理下・非管理を確認する	-	▲	●
		電波到達範囲の調査	検出されたアクセスポイントを敷地内外における電波到達範囲を確認する	▲	●	●
	アクセスポイントの脆弱性	脆弱な設定のアクセスポイントの調査	無線通信の暗号強度を診断し、open、WEP等を使用しているセキュリティを弱める脆弱な設定のアクセスポイントを確認する ※WPAはWEPの弱点に対応し、鍵生成、鍵交換、改ざん検知の仕組みを組み込み改良した方式のため本検査における脆弱性として指摘対象外する	▲	●	●
	アクセスポイントの脆弱性	アクセスポイントへの侵入試行	非管理のアクセスポイントが内部ネットワークに接続されているか確認する	-	▲	●

●	準拠が必要
▲	一部準拠で可
-	評価対象外

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。