



# 「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」 ポイント解説

---

セキュアIoTプラットフォーム協議会  
白水公康

テレワーク

=

業務

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



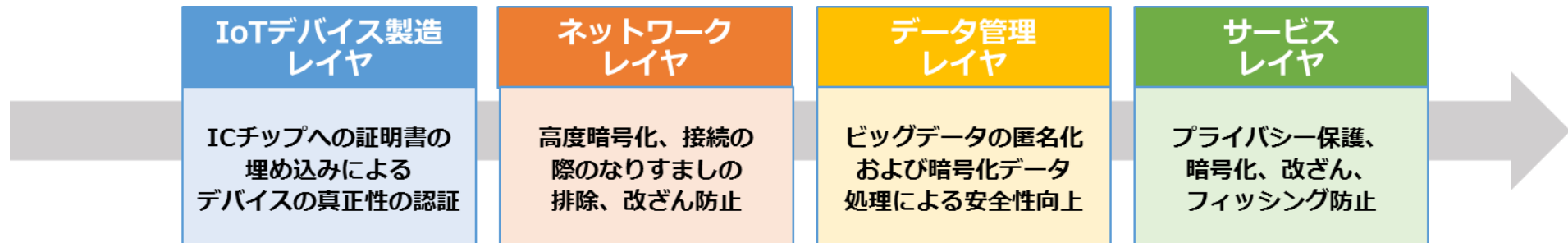
“場” にフォーカスして  
テレワークセキュリティのお話しをします

# 一般社団法人セキュアIoTプラットフォーム協議会



日本の産業界の知見を集約し、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。  
 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。

事業	<ul style="list-style-type: none"> <li>・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</li> <li>・IoT利活用推進および事例構築</li> <li>・共同実証実験(POC)の実施</li> <li>・最新IoT関連情報の発信</li> <li>・セキュリティ人材の育成</li> </ul>
設立年月日	2017年4月3日
役員構成	<ul style="list-style-type: none"> <li>・ 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)</li> <li>・ 理事：後藤 厚宏 (情報セキュリティ大学院大学 学長)</li> <li>白鳥 則郎 (中央大学研究開発機構 教授)</li> <li>田口 勉 (Neutrix Cloud Japan 株式会社 代表取締役社長 CEO)</li> <li>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)</li> <li>神部 永志 (セコムトラストシステムズ株式会社常務執行役員)</li> <li>眞柄 泰利 (サイバートラスト株式会社 代表取締役社長)</li> <li>三木 俊明 (株式会社ラック アソシエイト)</li> <li>・ 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)</li> <li>森本 登志男 (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)</li> </ul>



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

Rev. 2.0

2021年3月

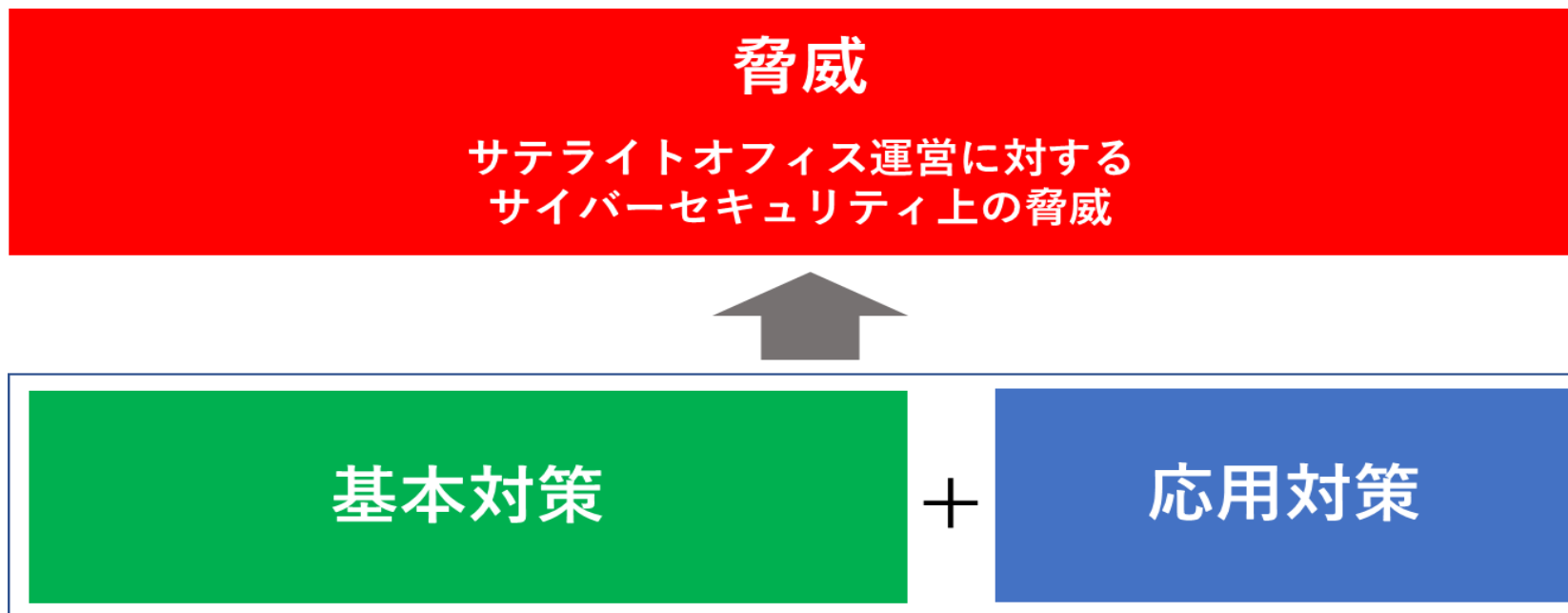
一般社団法人日本テレワーク協会  
一般社団法人セキュアIoTプラットフォーム協議会

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】

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。

# 共同利用型オフィスのセキュリティ課題と対策

## 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

情報  
資産

## 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

カテゴリ	基本対策
管理体制 (セキュリティポリシー・トレーニング等)	セキュリティポリシーの策定
	利用規約の策定・利用者からの同意
	事故発生対応マニュアルの整備
	トレーニング・定期チェック
	最新のセキュリティ情報の収集・確認
入退室管理・利用者情報	利用者の本人確認
	個人情報の適切な管理
	Webサイトの適切な管理
	利用ログの取得・管理



カテゴリ	基本対策
ネットワーク機器 (無線LANアクセスポイント・ルーター等)	最新のファームウェアの適用
	管理者パスワードの適切な設定
	無線LANアクセスポイントの適切な設定
	無線LANアクセスポイントのパスワードの設定と管理
	利用者の端末間通信の禁止設定
	業務用ネットワークとの分離
	アクセスログの適切な管理
ネットワーク接続機器 (複合機・防犯カメラ等)	最新のファームウェアの適用
	管理者パスワードの適切な設定
	機器設定の確認
	複合機のインターネット接続の禁止
	複合機に蓄積されたデータの消去

カテゴリ	基本対策
レンタルPC	インストールされたソフトウェアの最新化
	環境設定の初期化・復元
物理設備	オンライン(Web)会議等の音声利用のための場所の確保