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

目次

はじめに

【背景】

東京オリンピック・パラリンピック競技大会の開催に向けて、都心の交通渋滞緩和を目的とした首都圏企業に対するテレワークの推進が進められているほか、感染症対策としてもテレワークが推進されている。また、テレワークを実施できる共同利用型オフィス等についても更なる充実が必要と考えられる。

一方でパスワードが設定されていない無線LANが提供されるなど、セキュリティ上の安全性を考慮したオフィス運用となっていないケースも散見される。

サイバー攻撃等は年々高度化・複雑化している状況を考慮すると、共同利用型オフィス等のセキュリティ対策は喫緊の課題と言わざるを得ない。

【利用目的】

共同利用型オフィス等運営事業者に対して、サイバーセキュリティ上の課題と解決策を解説するとともに、安全な共同利用型オフィス等を設営・運営するために必要となる要件を明らかにすることを目的とする。

また、共同利用型オフィス等利用企業に対しても、「どのような共同利用型オフィス等環境を選択すべきか？」という点で参考としてご覧いただきたい。

<u>共同利用型オフィス等運営事業者</u>

- ✓ 安心してテレワークができる環境や仕事場に求められる要件とは？
- ✓ 選ばれる共同利用型オフィス等となるには、どのようなセキュリティが必要か？

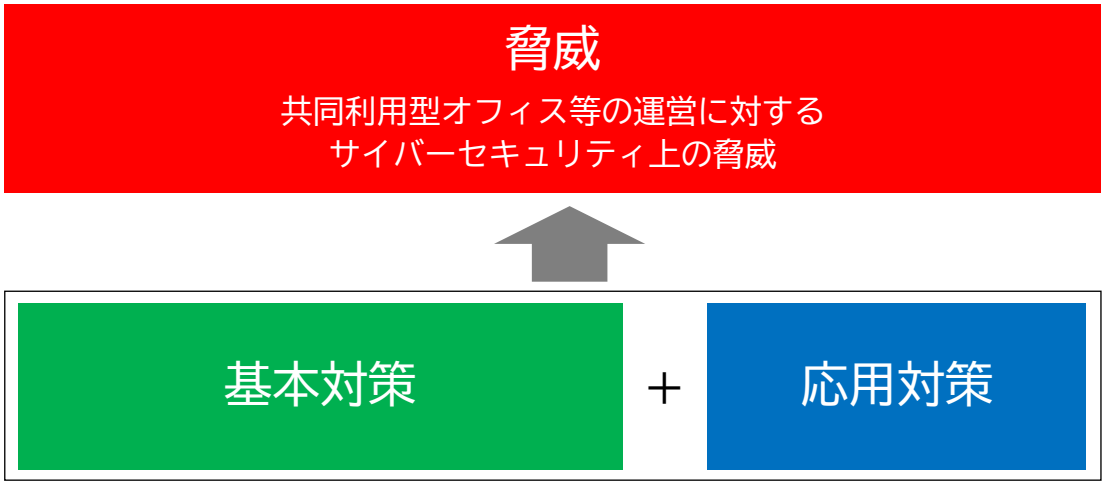
<u>利用者</u>

- ✓ どのような共同利用型オフィス等であれば安心して仕事ができるか？

【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」、及び状況に応じて更に望まれる「応用対策」から構成。

安全な共同利用型オフィスの構築には「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等の定義】

本ガイドにおいて対象とする「共同利用型オフィス等」は以下の通りである。

○ 民間企業が運営する共同利用型コワーキングスペース*1、レンタルオフィス*2、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*1、レンタルオフィス*2、シェアオフィス

*1）コワーキングスペース：専用の個室スペースを持たず、デスク単位で契約する共有型のオープンなオフィススペース。

*2）レンタルオフィス：事務所に必要な備品や通信設備などがあらかじめ備えられた空間。個室空間となっていることが多く、通常の事務所とほぼ同等の機能を保有。

※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）、ホテルなどの宿泊施設）については対象外とする。

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）

【脅威】

- サイバーセキュリティ対策は、技術的対策を万全にしていても、人のミスや運用の不備によりセキュリティ事故が発生するケースが多い。

【基本対策】

対策①：セキュリティポリシーの策定

共同利用型オフィス等におけるセキュリティに関する考え方や方針、セキュリティを確保するための体制など、運用規定を明文化したセキュリティポリシー（セキュリティに関する基本方針）を策定する。

また、セキュリティポリシーに沿った運営を行うため、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。

利用者に対しても必要な範囲で明示する。

対策②：利用規約の策定・利用者からの同意

共同利用型オフィス等を利用者が利用する際の規約を策定する。また、会員登録や利用申請時に、利用規約への同意書に明示的に同意（サイン等）いただき、ルールに基づいた利用を徹底する。

対策③：事故発生対応マニュアルの整備

万が一の時のために事故発生時の具体的対応を記したマニュアルを整備する。この中には、事故発生時に必要となる緊急連絡先一覧も記載する。

対策④：トレーニング・定期チェック

共同利用型オフィス等運営事業者の従業員に対し、研修等のトレーニングを実施し、「セキュリティポリシー」及び「事故発生対策マニュアル」の内容を周知・徹底させる。

また、実施状況、遵守状況、理解度等について定期的にチェックを行い、必要に応じて改定を行うなど、継続的なセキュリティ確保のためのPDCAサイクル*を確立する。

*）Plan(計画)・Do（実行）・Check（評価）・Action（改善）を繰り返すことによって、継続的に改善していく手法

対策⑤：最新のセキュリティ情報の収集・確認

サイバー攻撃は年々高度化・複雑化していることから、セキュリティに関する責任者や

担当組織（担当者）は、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する。特に使用する機器の製造ベンダーやIPA（情報処理推進機構）などから発信される注意喚起については、その対策を確実にとることが求められる。

２．入退室管理・利用者情報

【脅威】

- 身元のはっきりしない利用者が入場し、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が発生するおそれがある。
- 会員制施設においても、会員のなりすましが発生するおそれがある。

【基本対策】

対策①：利用者の本人確認

時間貸の共同利用型オフィス等であっても、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った上で、利用登録を行う。また、利用登録をした者以外は入室・利用ができないよう措置する。

特にレンタルPCによるネットワーク接続サービスを行っている共同利用型オフィス等では、条例などで本人確認が義務付けられていることもあり、適切な本人確認を行う。

対策②：個人情報の適切な管理

オンライン及び紙を問わず、個人情報を取り扱う場合には、個人情報保護方針を定め公表する。また、具体的な個人情報の取扱い方法について、管理運用ルールとして明文化し、徹底する。

対策③：Webサイトの適切な管理

Webサイトにおいて利用登録をはじめ個人情報の入力等を行う場合には、TLS（https）通信を行う。また、Webサイト構築に当たっては、「安全なウェブサイトの作り方[*1]」及び「TLS暗号設定ガイドライン[*2]」を遵守する。

*1）https://www.ipa.go.jp/security/vuln/websecurity.html
*2）https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

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）を取得し、外部に漏えい等することのないよう適切に保存・管理する。

【応用対策】

対策⑤：電子的な入退出管理システムの導入

会員制共同利用型オフィス等については、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し、部外者を入場させない仕組みの導入が望ましい。

この場合、会員証に格納されている鍵に対して、有効期間の設定及び定期的な更新の仕組みや紛失時に即座に機能を失効させる仕組みが実装されていることが必要である。

また、会員証による認証に加えて、ユーザーが記憶する暗証番号の入力を組み合わせることにより、さらにセキュリティを強化することが可能となる（多要素認証*）。

*）本人であることの確認を２つ以上の要素で行う認証方式。この場合だと、本人のみが所持している会員証という要素と、本人のみが知識として記憶している暗証番号という要素の２つで認証している。

・対策⑥：生体認証システムの導入

静脈認証、指紋認証、虹彩認証*など生体情報を使った認証システムを導入し、厳密に個人の特定を行うこともセキュリティを強化するためには望ましい。

*）静脈認証、指紋認証、虹彩認証は、それぞれ、手のひら等の静脈、指紋、目の虹彩情報を用いて本人かどうかの認証を行う仕組み

このようなシステムはセキュリティの厳格化とともに、会員証等を必要としないため、利用者の利便性を高める効果もある。

対策⑦：会員区分の明確化

会員制共同利用型オフィス等においては、会員とゲスト利用のユーザー区分を行い、それぞれの利用規約を明確に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）

【脅威】

- ネットワーク機器の設定が不十分であると、利用者の通信内容が盗み見られたり、利用者の端末に不正にアクセスされたりするおそれがある。
- ネットワーク機器を介して、共同利用型オフィス等運営事業者が使用する業務用端末に不正にアクセスされるなどされ、個人情報や機密情報の漏えいや、システムの機能停止といったセキュリティ事故が発生するおそれがある。
- ネットワーク機器が攻撃者に乗っ取られることで、情報漏えいなどのほか、気付かないうちにサイバー攻撃の起点となってしまい、加害者として社会的に損害を与えてしまうこともある。

【基本対策】

対策①：最新のファームウェアの適用

ネットワーク構築時及び運用時のいずれにおいても、ネットワーク機器にセキュリティ脆弱性がないよう、ファームウェアを常に最新の状態とする。

特に運用時において、機器製造ベンダーがファームウェアをリリースした場合に速やかに適用できるよう、定期的にアップデートの有無を確認する体制を構築する。なお、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、それを有効にすることで、定期的な確認を省略することができる。

また、ネットワーク機器のセキュリティ脆弱性を修正するためのファームウェアアップデートを提供する期間は機器ベンダーや機種によりおおむね定まっている。そのため、その期間を過ぎたネットワーク機器はセキュリティ脆弱性に対応できなくなるため、使用しない。

対策②：管理者パスワードの適切な設定

ネットワーク機器の設定を変更するための管理者パスワードについて、未設定や工場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する。例えば、パスワードは十分な長さの文字列とし、アルファベット（可能であれば大文字、小文字）、数字、記号などを組み合わせ、英単語や施設名など類推されやすい文字列にしない。

なお、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。ただし、管理者パスワードを知る人物が異動・退職するなどした場合には、速やかに変更する。

対策③：無線LANアクセスポイントの適切な設定

無線LANアクセスポイントを利用する場合、無線LANのセキュリティ方式としてWPA2又

はWPA3を設定する。なお、WEP及びWPAはセキュリティ脆弱性があるため使用しない。（詳しくは、コラム「無線LANのセキュリティ方式」、「WPA2の脆弱性」をご参照ください。）

また、無線LANアクセスポイントの電波について、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

無線LANアクセスポイントの暗号化のためのパスフレーズ（WPA2/WPA3による暗号化の際に利用するパスワード）について、第三者に推測されにくい複雑なもの（管理者パスワードとは全く別のものとする。）を設定する。

また、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し、広く多数が知りうるようのないようする。例えば、次の方法がある。

・受付の際に、身元確認した上でパスフレーズ情報を伝える。
・正規の会員だけ通知を受けることができる方法で公開する。
（登録アドレスへのメール、パスフレーズで管理された会員サイトでの公開など）

また、不特定多数に対して同じパスフレーズ（パスワード）を公開・提供している共同利用型オフィス等においては、パスフレーズ（パスワード）を一定の頻度（例：毎月）で更新するなど、共同利用型オフィス等を利用しなくなった者がパスフレーズ（パスワード）を知りうる機会を可能な限り低減させる。

対策⑤：利用者の端末間通信の禁止設定

利用者が別の利用者の端末にアクセスできないように設定する。

具体的には、無線LANアクセスポイントを利用している場合には、「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にすることで、同一の無線LANアクセスポイントに接続している端末同士の通信を禁止する。（詳しくは、コラム「ネットワーク分離機能」をご参照ください。）

また、複数の無線LANアクセスポイントを利用している場合や有線でのアクセスを提供している場合には、それらが接続されるスイッチやルーターにおいて、特定のポート間通信の禁止等を設定する必要がある。

なお、利用者の端末間通信を禁止しつつ、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には、それらの機器に対してネットワーク構成を適切に設定する必要がある。

対策⑥：業務用ネットワークとの分離

利用者が利用するネットワーク機器を介して、共同利用型オフィス等運営事業者の業務用端末等にアクセスされないようにするため、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の導入により、安全に分離する。

対策⑦：アクセスログの適切な管理

ネットワーク機器は、アクセスログを記録することが可能である。アクセスログは、どの端末が、いつ、どこにアクセスしたのかという、高いプライバシー性を持つ情報であるため、記録する際は、ネットワーク機器にトラブルが発生した際の把握や利用者からの問合せ対応等、業務上の必要性に照らして最小限の記録に留める。記録・保存したアクセスログは、利用者の同意なくマーケティング等の目的に使うことや、第三者に提供することなどがないように、十分注意して取り扱うことが必要である。

アクセスログを利用者の同意なく外部に提供することはできないが、裁判官の発付する令状に従う場合は、警察等に提供することができる。例えば、外部サイトへ不正アクセスが行われた場合、アクセスログを含め、犯人を特定するための情報の提供を警察から求められる場合がある。

ネットワーク機器の運用を事業者に委託している場合は、アクセスログもその委託先事業者において記録・保存されている。その記録内容や保存期間等を把握しておき、問い合わせがあった場合の対応方法を委託先事業者と確認しておくことが求められる。

なお、アクセスログを有効に活用するためには、ネットワーク機器が正しく時刻設定されていることが重要であるため、ntp等による自動的な時刻合わせが可能な機器についてはその設定を実施する。

【応用対策】

対策⑧：高度なセキュリティの導入

例えば次のような対策により、より高度なセキュリティを確保することが望ましい。

・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、無線LANアクセスポイントのなりすましや許可されていない端末の接続を制限する。(詳しくは、コラム「電子証明書の活用（IEEE802.1x認証)」をご参照ください。)

・無線LANアクセスポイントに対し、MACアドレスのフィルタリング設定を行い、許可されていない端末の接続を制限する。(詳しくは、コラム「MACアドレスフィルタリング」をご参照ください。)

・共同利用型オフィス等運営事業者が業務で利用するサーバー等へのアクセスについて、アカウント管理を厳重に行うとともに、多要素認証の仕組みを導入するなど、不正アクセスのリスクを軽減する。

・ネットワークへの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。例えば、以下の機能を有するものを利用する。

・接続される機器の正当性の確認

・新しい機器が接続された時に通知し、認識していない機器は接続を切断

・マルウェア感染のおそれがあるサイトやフィッシングサイトへのアクセスを制限

・ネットワークに接続される機器の安全性診断を実施

４．ネットワーク接続機器（複合機・防犯カメラ等）

【脅威】

- ビジネス上の機密情報が複合機のキャッシュ（履歴）に残っている可能性があり、不正アクセスにより情報漏えいする可能性がある。
- セキュリティが十分に確保実装されていない機器がインターネットに接続されることで、情報漏えいやなど危険性があるだけでなく、攻撃者に乗っ取られて、気付かないうちにサイバー攻撃の起点となってしまう。
- ネットワークカメラのパスワードが設定されておらず、オフィスの様子が意図せずにインターネット上に公開されていることに気付いていない。
- プリントアウトした書類が放置され、物理的な情報漏えいにつながる。

【基本対策】

対策①：最新のファームウェアの適用

「２．入退室管理・利用者情報」の「対策①：最新のファームウェアの適用」と同様に、ネットワーク接続機器についても最新のファームウェアの適用を行う。

対策②：管理者パスワードの適切な設定

「２．入退室管理・利用者情報」の「対策②：管理者パスワードの適切な設定」と同様に、ネットワーク接続機器についても管理者パスワードの適切な設定を行う。

対策③：機器設定の確認

機器によっては、家庭や同一組織内での利用を想定した初期設定となっており、共同利用型オフィス等で利用するに当たっては十分なセキュリティを満たしていない場合もあることから、機器にアクセスできる者の範囲など、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

複合機は、原則として外部ネットワーク（インターネット）に接続しない。接続する必要性がある場合にも、グローバルIPアドレスを直接割り当てることは避けるとともに、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など、厳重なセキュリティ対策を実施する。

対策⑤：複合機に蓄積されたデータの消去

複合機で入出力したデータは、複合機の内蔵記録装置（ハードディスク等）に保存され続けることがあり、この蓄積データの「暗号化」や「消去（一定時間後の自動消去を含む。）」機能がある場合にはこれを有効にする。

また、このような複合機の利用に当たってのデータ取扱いに関しては利用者に適切に周知する。

【応用対策】

対策⑥：IDカードやパスワードによる複合機の出力管理

出力した書類の放置による情報漏えい事故を防ぐためには、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

【脅威】

- レンタルPCがマルウェア感染することで、その利用者が取り扱う情報が漏えいする。
- レンタルPCをのぞき見されることにより、機密情報が漏洩してしまう。

【基本対策】

対策①：インストールされたソフトウェアの最新化

レンタルPCのOS及びアプリケーションについては、サポート期限の切れた製品を利用しない。また、アップデートを行い常に最新の状態にする。

また、OS標準のセキュリティ設定（例：ファイアウォール、マルウェア検知等）についても、共同利用型オフィス等のネットワーク環境を踏まえ適切な設定を行う。

フリーソフトを使用する場合には、そのソフトの信頼性やセキュリティ脆弱性について十分に確認した上で、必要最低限のもののみインストールする。

対策②：環境設定の初期化・復元

複数の利用者でレンタルPCを共用する場合には、勝手なソフトウェアのインストールやマルウェアの感染等によるトラブル、作成した機密情報を含むファイルの削除忘れによるトラブル、ブラウザの閲覧履歴が残存することによるトラブルなどを避けるため、環境設定の初期化・復元を行った上で貸し出しを行う。

【応用対策】

対策③：のぞき見防止フィルタ

レンタルPCには、のぞき見防止フィルタを付けることが望ましい。

６．物理設備（ロッカー等）

【脅威】

- オンライン（Web）会議の際、発言の音漏れにより機密情報が漏れてしまう可能性がある。
- 書類の放置など物理的な側面でセキュリティ事故が発生する可能性がある。

【基本対策】

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

オンライン（Web）会議可能とサービス表記する共同利用型オフィス等については、時間貸しの個室や会議室、ブース型等の防音設備などを整備すること。

【応用対策】

対策②：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③：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。

コラム

無線LANのセキュリティ方式

無線LANのセキュリティ方式には、「WEP」「WPA」「WPA2」「WPA3」があり、それぞれ以下の特徴があります。

WEP	WPA	WPA2	WPA3
暗号を短時間で解読する方法が発見されており、現在では容易に解読されてしまう方式です。利用を控えてください。	WEPの弱点を補強した方式ですが、脆弱性も発見されており安全性が十分に確保できません。利用を控えてください。	WPAより強固な方式ですが、脆弱性も発見されています。ただしこの脆弱性は、無線LANアクセスポイントのファームウェアをアップデートすることで安全性を確保できます。	WPA2よりも更に安全性を高めた方式です。現時点においては最も推奨されます。今後新たに無線LANアクセスポイントを導入される場合には、WPA3に対応する機器を導入されることをお勧めします。
推奨度：×	推奨度：×	推奨度：〇	推奨度：◎

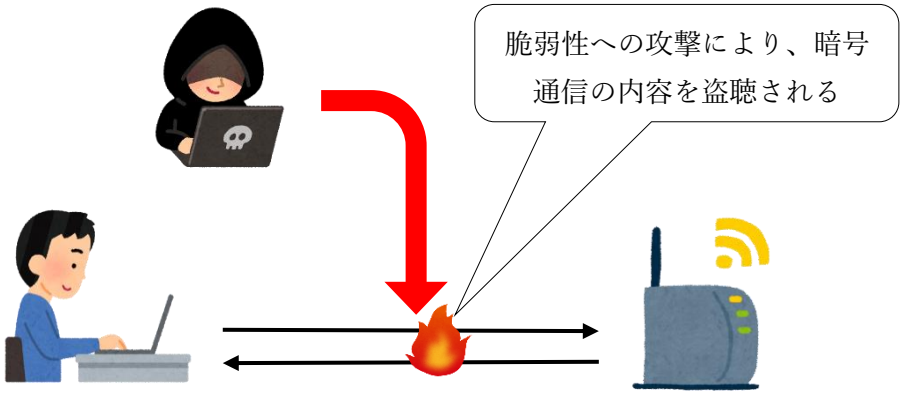
無線LANアクセスポイントを利用する場合には、WPA2（ソフトウェアアップデートが適切に行われているもの。）を利用するか、大幅にセキュリティが向上しているWPA3に対応したものを導入し、利用することを徹底してください。

※WEP：Wired Equivalent Privacy

※WPA：Wi-Fi Protected Access

WPA2の脆弱性

WPA2は広く利用されている無線LANのセキュリティ方式ですが、2018年10月16日に、暗号鍵を特定されるなど複数の脆弱性が公開されました。この脆弱性に対応するソフトウェアアップデートがされないまま利用を続けると、同じ無線LANアクセスポイントの通信範囲内いる第三者により、盗聴が行われる可能性があります。



この脆弱性の対策には、無線LANアクセスポイントのベンダーから提供されている最新のファームウェアを適用（更新）することが必要です。発売されて時間の経過した、古い無線LANアクセスポイントを利用している場合には、ファームウェアが提供されていないことがありますので、その際には最新のものへ入れ替えてください。

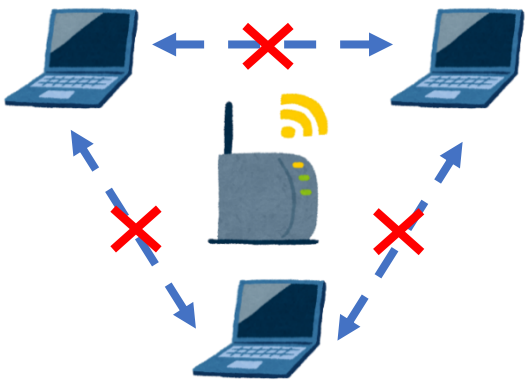
また無線LANに関する規格を策定する業界団体であるWi-Fi Allianceにより、2018年6月25日に新規格である「WPA3」が発表されました。WPA3では大幅にセキュリティが強化されています。

今後、新たに無線LANアクセスポイントを設置・入替する際には、適切なファームウェエアアップデートがされたWPA2かWPA3に対応した機器を選択してください。

ネットワーク分離機能

ネットワーク分離機能（プライバシーセパレーターとも言う）は、無線LANアクセスポイント（以下「AP」といいます。）に接続している端末同士のアクセス（例：共有フォルダへのアクセス）を禁止することができる機能です。利用者のセキュリティ保護のため、この機能を使用してください。

ただし、複数のAPがある場合において、片方のAPに接続している端末から、別のAPに接続している端末に対しての通信は禁止できません。



電子証明書の活用（IEEE802.1x認証）

電子証明書を活用したIEEE802.1x認証は、無線LANを利用するクライアントと、無線LANアクセスポイントの双方でIEEE802.1xにおける認証プロトコルを使用し、認証にはRADIUS（Remote Authentication Dial-In User Service）サーバーを利用することで、無線LANの利用において認証機能を付加する方式です。802.1x認証や、1x認証という言い方をする場合もあります。

RADIUSサーバーで認証の許可や拒否を行うことで、未認証のクライアントからの不正アクセスを排除することが可能なため、電子証明書を利用したIEEE802.1x認証を行うことを推奨します。

認証方式	EAP-TLS	EAP-TTLS	EAP-PEAP
概要	電子証明書を用いるため、セキュリティ強度が強い	ID/パスワードを用いるため、認証情報を類推、詐取される可能性がある	ID/パスワードを用いるため、認証情報を類推、詐取される可能性がある
端末側の認証	電子証明書	ID/パスワード	ID/パスワード
サーバー側の認証	電子証明書	電子証明書	電子証明書

MACアドレスフィルタリング

PCやスマートフォン等のネットワーク接続可能な端末には、機器ごとに固有の番号（MACアドレス）が製造時に割り振られています。このMACアドレスは機器ごとに一意となるように割り振られているため、MACアドレスによって機器を識別可能となります。

このため、無線LANアクセスポイントに接続する端末のMACアドレスをあらかじめ登録しておくことで、登録された端末以外の接続を防ぐことができます。

ただし、MACアドレスは比較的容易に詐称することが可能ですので、MACアドレスフィルタリングを過信しないよう留意が必要です。

（参考）チェックシート

要件	基本対策	応用対策
1. 管理体制（セキュリティポリシー・トレーニング等）		
対策①：セキュリティポリシーの策定		
共同利用型オフィス等におけるセキュリティに関する考え方や方針、セキュリティを確保するための体制など、運用規定を明文化したセキュリティポリシー（セキュリティに関する基本方針）を策定していますか？	Y/N	
セキュリティポリシーに沿った運営を行うため、セキュリティに関する責任者や担当組織（担当者）を明確にしていますか？	Y/N	
利用者に対してセキュリティポリシーを必要な範囲で明示していますか？	Y/N	
対策②：利用規約の策定・利用者からの同意		
共同利用型オフィス等を利用者が利用する際の規約を策定していますか？	Y/N	
会員登録や利用申請時に、利用規約への同意書に明示的に同意（サイン等）いただき、ルールに基づいた利用を徹底していますか？	Y/N	
対策③：事故発生対応マニュアルの整備		
事故発生時の具体的対応を記したマニュアル（事故発生時に必要となる緊急連絡先一覧を含む）を整備していますか？	Y/N	
対策④：トレーニング・定期チェック		
共同利用型オフィス等運営事業者の従業員に対し、研修等のトレーニングを実施し、「セキュリティポリシー」及び「事故発生対策マニュアル」の内容を周知・徹底させていますか？	Y/N	
「セキュリティポリシー」及び「事故発生対策マニュアル」の実施状況、遵守状況、理解度等について定期的にチェックを行い、必要に応じて改定を行うなど、継続的なセキュリティ確保のための PDCA サイクルを確立していますか？	Y/N	
対策⑤：最新のセキュリティ情報の収集・確認		
セキュリティに関する責任者や担当組織（担当者）は、最新のサイバーセキュリティ情報（使用する機器の製造ベンダーや IPA（情報処理推進機構）などから発信される注意喚起等）を常に収集し、必要に応じた対策を実施していますか？	Y/N	

2. 入退室管理・利用者情報		
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った上で、利用登録を行っており、また、利用登録をした者以外は入室・利用ができないよう措置していますか？	Y/N	
対策②：個人情報の適切な管理		
個人情報を取り扱う場合には、個人情報保護方針を定め公表し、具体的な個人情報の取扱い方法について、管理運用ルールとして明文化し、徹底していますか？	Y/N	
対策③：Web サイトの適切な管理		
Web サイトにおいて利用登録をはじめ個人情報の入力等を行う場合には、TLS（https）通信を行っていますか？	Y/N	
Web サイト構築に当たっては、「安全なウェブサイトの作り方」及び「TLS 暗号設定ガイドライン」を遵守していますか？	Y/N	
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）を取得し、外部に漏えい等することのないよう適切に保存・管理していますか？	Y/N	
対策⑤：電子的な入退出管理システムの導入		
（会員制の場合）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し、部外者を入場させない仕組みを導入しており、会員証に格納されている鍵に対して、有効期間の設定及び定期的な更新の仕組みや紛失時に即座に機能を失効させる仕組みを実装していますか？		Y/N
（会員制の場合）会員証による認証に加えて、ユーザーが記憶する暗証番号の入力を組み合わせるなど、多要素認証を採用している。		Y/N
対策⑥：生体認証システムの導入		
静脈認証、指紋認証、虹彩認証など生体情報を使った認証システムを導入していますか？		Y/N
対策⑦：会員区分の明確化		
（会員制の場合）会員とゲスト利用のユーザー区分を行い、それぞれの利用規約を明確にしていますか？		Y/N

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①：最新のファームウェアの適用		
ネットワーク構築時及び運用時のいずれにおいても、ネットワーク機器にセキュリティ脆弱性がないよう、ファームウェアを常に最新の状態にしていますか？	Y/N	
ファームウェアアップデートを提供する期間を過ぎたネットワーク機器を使用しないようにしていますか？	Y/N	
対策②：管理者パスワードの適切な設定		
ネットワーク機器の設定を変更するための管理者パスワードについて、未設定や工場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していますか？	Y/N	
ネットワーク機器の設定を変更するための管理者パスワードについて、当該パスワードを知る人物が異動・退職するなどした場合に、速やかに変更していますか？	Y/N	
対策③：無線 LAN アクセスポイントの適切な設定		
無線 LAN アクセスポイントを利用する場合、無線 LAN のセキュリティ方式として（WEP や WPA ではなく）WPA2 又は WPA3 を設定していますか？	Y/N	
無線 LAN アクセスポイントの電波について、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していますか？	Y/N	
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		
無線 LAN アクセスポイントの暗号化のためのパスフレーズ（WPA2/WPA3 による暗号化の際に利用するパスワード）について、第三者に推測されにくい複雑なもの（管理者パスワードとは全く別のもの）を設定していますか？	Y/N	
無線 LAN アクセスポイントの暗号化のためのパスフレーズ（WPA2/WPA3 による暗号化の際に利用するパスワード）について、利用者のみが知ることができる方法を徹底し、広く多数が知りうるようのないようにしていますか？ （例） ・受付の際に、身元確認した上でパスフレーズ情報を伝える。 ・正規の会員だけ通知を受けることができる方法で公開する。 （登録アドレスへのメール、パスフレーズで管理された会員サイトでの公開など）	Y/N	

（不特定多数に対して同じパスフレーズ（パスワード）を公開・提供している場合）無線 LAN アクセスポイントの暗号化のためのパスフレーズ（WPA2/WPA3 による暗号化の際に利用するパスワード）について、一定の頻度（例：毎月）で更新するなど、共同利用型オフィス等を利用しなくなった者がパスフレーズ（パスワード）を知りうる機会を可能な限り低減させていますか？	Y/N	
対策⑤：利用者の端末間通信の禁止設定		
利用者が別の利用者の端末にアクセスできないように設定していますか？ （無線 LAN アクセスポイントを利用している場合には、「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にすることで、同一の無線 LAN アクセスポイントに接続している端末同士の通信を禁止する。）	Y/N	
（複数の無線 LAN アクセスポイントを利用している場合や有線でのアクセスを提供している場合）接続されるスイッチやルーターにおいて、特定のポート間通信の禁止等を設定していますか？	Y/N	
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には、それらの機器に対してネットワーク構成を適切に設定していますか？	Y/N	
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 の導入により、安全に分離していますか？	Y/N	
対策⑦：アクセスログの適切な管理		
アクセスログを記録する際は、ネットワーク機器にトラブルが発生した際の把握や利用者からの問合せ対応等、業務上の必要性に照らして最小限の記録に留めていますか？	Y/N	
記録・保存したアクセスログは、利用者の同意なくマーケティング等の目的に使うことや、第三者に提供することなどがないように、十分注意して取り扱っていますか？	Y/N	
（ネットワーク機器の運用を事業者に委託している場合）アクセスログの記録内容や保存期間等を把握しておき、問い合わせがあった場合の対応方法を委託先事業者と確認していますか？	Y/N	
ネットワーク機器が正しく時刻設定されていますか？ （ntp 等による自動的な時刻合わせが可能な機器についてはその設定を実施する。）	Y/N	

対策⑧：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、無線 LAN アクセスポイントのなりすましや許可されていない端末の接続を制限していますか？		Y/N
無線 LAN アクセスポイントに対し、MAC アドレスのフィルタリング設定を行い、許可されていない端末の接続を制限していますか？		Y/N
共同利用型オフィス等運営事業者が業務で利用するサーバー等へのアクセスについて、アカウント管理を厳重に行うとともに、多要素認証の仕組みを導入するなど、不正アクセスのリスクを軽減していますか？		Y/N
ネットワークへの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していますか？ （機能例） ・接続される機器の正当性の確認 ・新しい機器が接続された時に通知し、認識していない機器は接続を切断 ・マルウェア感染のおそれがあるサイトやフィッシングサイトへのアクセスを制限 ・ネットワークに接続される機器の安全性診断を実施		Y/N
4. ネットワーク接続機器（複合機・防犯カメラ等）		
対策①：最新のファームウェアの適用		
ネットワーク構築時及び運用時のいずれにおいても、ネットワーク接続機器にセキュリティ脆弱性がないよう、ファームウェアを常に最新の状態にしていますか？	Y/N	
ファームウェアアップデートを提供する期間を過ぎたネットワーク接続機器を使用しないようにしていますか？	Y/N	
対策②：管理者パスワードの適切な設定		
ネットワーク接続機器の設定を変更するための管理者パスワードについて、未設定や工場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していますか？	Y/N	
ネットワーク接続機器の設定を変更するための管理者パスワードについて、当該パスワードを知る人物が異動・退職するなどした場合に、速やかに変更していますか？	Y/N	
対策③：機器設定の確認		
機器にアクセスできる者の範囲など、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っていますか？	Y/N	

対策④：複合機のインターネット接続の禁止		
複合機は、原則として外部ネットワーク（インターネット）に接続せず、接続する必要性がある場合にも、グローバル IP アドレスを直接割り当てることは避けるとともに、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など、厳重なセキュリティ対策を実施していますか？	Y/N	
対策⑤：複合機に蓄積されたデータの消去		
複合機の内蔵記録装置（ハードディスク等）に保存された入出力データについて、「暗号化」や「消去（一定時間後の自動消去を含む。）」機能がある場合にはこれを有効にしていますか？	Y/N	
複合機の利用に当たってのデータ取扱いに関し、利用者に適切に周知していますか？	Y/N	
対策⑥：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の導入をしていますか？		Y/N
5. レンタルPC		
対策①：インストールされたソフトウェアの最新化		
レンタル PC の OS 及びアプリケーションについては、サポート期限の切れた製品を利用せず、また、アップデートを行い常に最新の状態にしていますか？	Y/N	
OS 標準のセキュリティ設定（例：ファイアウォール、マルウェア検知等）について、共同利用型オフィス等のネットワーク環境を踏まえ適切な設定を行っていますか？	Y/N	
フリーソフトを使用する場合には、そのソフトの信頼性やセキュリティ脆弱性について十分に確認した上で、必要最低限のもののみインストールしていますか？	Y/N	
対策②：環境設定の初期化・復元		
（複数の利用者でレンタル PC を共用する場合）環境設定の初期化・復元を行った上で貸し出しを行っていますか？	Y/N	
対策③：のぞき見防止フィルタ		
レンタル PC にはのぞき見防止フィルタが付けられていますか？		Y/N
6. 物理設備（ロッカー等）		
対策①：オンライン会議等の音声利用のための場所の確保		
（オンライン（Web）会議可能とサービス表記する場合）時間貸しの個室や会議室、ブース型等の防音設備などを整備していますか？	Y/N	

対策②：スマートロッカーの導入		
IC カード型会員証やスマーフォンで閉・開錠可能なスマートロッカーを設置していますか？		Y/N
対策③：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 を設置していますか？		Y/N