テレワークと
スモールオフィスのための

ネットワーク
セキュリティガイド

ZJMR2020611284

目次

テレワークとスモールオフィスのためのネットワークセキュリティガイド	**1**
謝辞	**2**
編集者	2
寄稿者	2
はじめに	**3**
目的	**4**
ドキュメントの構成	**5**
ネットワーク端末の購入	**6**
モデム、ルーター、アクセスポイントの種類	6
モデム	6
ルーター	6
モデムとルーターのハイブリッド	7
中継器	7
携帯電話信号ブースター	7
一般的な使用方法	8
必要となるセキュリティ機能	9
ネットワーク機器の購入先	10
基本的な端末設定	**11**
初期アクセス	11
内部および外部ネットワークインターフェイス	11
パスワード	12
端末とネットワーク管理のアプリ	12
基本的なネットワーク設定	**13**
端末の場所	13
WiFiネットワーク名の作成	13
ゲストネットワークの構築	14
自動更新の有効化	14
トラフィックの暗号化	**15**
Wired Equivalent Privacy（WEP）	15
WiFi Protected Access（WPA）	15
WiFi Protected Access Version 2（WPA2）	15
WiFi Protected Access Version 3（WPA3）	16
WiFi Protected Setup（WPS）	16
ネットワークの追加設定	**17**
ファイアウォール	17
端末の強化	17
ドメインネームシステム（DNS）	18
リモート設定	18
ユニバーサルプラグアンドプレイ（UPnP）	19
メディアアクセス制御（MAC）アドレスホワイトリスト	19

スモールビジネス向けのガイドライン	**20**
頭字語と略語	**21**
ネットワークセキュリティのチェックリスト	**22**
CIS Controlsへのマッピング	**23**
CIS Control	23
防御対策	23
本ドキュメントについて	**24**

テレワークとスモールオフィスのためのネットワークセキュリティガイド

謝辞

CIS Controls をはじめとするCISの業務を支援するために、貴重な時間を費やし尽力頂いた多くのセキュリティ専門家の皆様に感謝いたします。CISの製品は、業界全体から有志としてご協力いただいた皆様の貴重な時間と尽力の産物であり、より安全ななオンライン体験を多くの人に提供しています。

編集者
Joshua M. Franklin, CIS

寄稿者
Aaron Piper, CIS
Alan B. Watkins, ABW Consulting, LLC
Stephen Campbell, Non-State Threat Intelligence, LLC
Uros Trnjakov, Oxfam GB
Maurice Turner, Center for Democracy & Technology (CDT)
Michael K. Wicks, CIS
Robin Regnier, CIS
Aaron Wilson, CIS
Phil Langlois, CIS

はじめに

ルーター、モデムなどのネットワーク端末は、プライベートネットワークからインターネットにアクセスするための入口として機能します。これらのネットワーク端末は家庭用に開発、販売されている一方で、小規模の組織でも購入されることが多く、プロフェッショナルな企業環境でも使用されています。さらに、テレワークの導入は増加傾向にあり、雇用者の立場にある者はテレワークベースの従業員が企業情報を自宅で安全に取り扱うことを前提にテレワーク業務へ移行させているケースが多くなっています。一般的に、雇用主は、パーソナルネットワークの端末構成やセキュリティ保護の実態を把握できていませんが、適切に設定されていない家庭用端末は組織全体に影響を及ぼす恐れがあります。

小規模な組織やテレワークの従業員が使用するネットワーク端末は、高度なエンタープライズ情報技術（IT）環境で使用されるネットワーク端末に比べて機能面が大きく劣り、充てられる費用も少なくなります。このような機能面で劣る端末も、より大規模で経費のかかる端末と同様に、多くの脅威に晒されことになります。ネットワーク端末への脅威としては、ブラウジングの履歴やWebアクティビティへのスパイ行為、接続端末への危害、ルーター内の脆弱性の悪用などが挙げられます。しかし幸いなことに、これら端末に備わるセキュリティ設定を構成すれば、その防御対策を大幅に強化でき、居住空間の他の人々、近所の住人、インターネット上で遠隔から攻撃をしかける相手からデータを保護するデータセキュリティを確立できます。

目的

本ガイドは、個人や組織による汎用ルーター、モデムなどのネットワーク端末のセキュリティ保護を支援することを目的としています。ネットワーク端末を使用する際は、サイバーセキュリティに配慮することが必要不可欠となるため、これら端末のセキュリティ保護を行うことは重要です。

- 何者かがあなたのネットワークにアクセスした場合、税務情報、従業員に関する個人識別情報（PII）、社外の者と共有が禁止さ機密情報など、会社にとって重要なファイルを読み取られる恐れがあります。

- ネットワーク内のルーターやコンピューターシステムが侵害されると、ボットネットの一部となり、インターネットに接続されている他のコンピューターシステムや組織への攻撃に使用される恐れがあります。

- 企業がサイバーセキュリティの業界標準を遵守していない場合、安全でないコンピューターネットワークやシステムが原因で発生するデータ漏洩や損失に対して何らかの責任が生じる可能性があります。

- 企業がサイバーセキュリティ保険に加入している場合や、保険への加入を検討する場合、多くの保険会社は、企業と顧客の機密情報を保護するために、適切かつ妥当なセキュリティ対策を企業に対して要求します。

小規模オフィスやホームオフィス（**SoHo オフィス**）のために作られたネットワーク端末が多数存在しますが、SoHo ネットワーク端末は、より高価な「エンタープライズクラス」の端末と比較した場合、セキュリティ機能の点で必ずしも同等であるとは限りません。本ガイドでは、「エンタープライズクラス」の端末については説明しません。なぜならば、これらエンタープライズクラスの端末を適切に使用し維持するには高い経費がかかり、専門的な知識が必要になるためです。また、アップデートのダウンロードやインストール、テクニカルサポートのために有料のサブスクリプション契約が必要となる場合もあります。本ガイドは、汎用ネットワーク端末のセキュリティオプションを適切に設定することを目的としており、高度なネットワーク機能の利用をサポートするものではありません。

また、本ガイドは、企業やその他組織を対象としていますが、個人での使用にも適用できます。テレワークなどに携わる方は、本ガイダンスに従ってホームネットワーク端末を設定することをお勧めします。ユーザーの状況に応じて、必要な内容を参照してください。

ドキュメントの構成

本ドキュメントの構成は次のとおりです。

- ネットワーク端末の購入
- 基本的な端末設定
- 基本的なネットワーク設定
- トラフィックの暗号化
- ネットワーク管理
- セキュリティの維持

以下の情報も記載されています。

- 頭字語と略語の一覧
- 信頼できる外部組織が提供する、小企業向けオンラインリソースへのリンク

ネットワーク端末の購入

ルーター、モデムなどのネットワーク端末を購入した場合、例外もありますが、セキュリティ機能を後から追加できません。つまり、**端末を購入して代金を支払う前に**、組織に適したセキュリティ対策が設定できる端末を調査、吟味、確認します。次のガイドでは、端末の購入前に検討すべき機能について説明します。

モデム、ルーター、アクセスポイントの種類

ネットワーク端末には多くの用語があり、同じ意味で使用されることがよくあります。以下は、一般的な用語を定義し、組織や在宅勤務者が購入対象製品を十分に理解して購入できるように用意したものです。購入を検討する場合、販売店の従業員に積極的に質問し、端末の製造元のWebサイトで内容を確認してください。

モデム

モデムは、インターネットサービスプロバイダ（ISP）とネットワーク通信を行うためのもので、小規模なオフィスやホームオフィスがインターネットにアクセスするために必要な主要端末です。ISPとは、インターネットにアクセスするためにあなたが料金を支払う会社です。モデムはISPから供給されることが多いですが、使用期間が長くなるほど、自分で購入して管理する方が安くなります。この場合、端末の設定、トラブルシューティング、運用を行うためにISPにアクセス権を付与する必要があります。モデムは、**ケーブルボックス**または**デジタル加入者線（DSL）モデム**とも呼ばれます。

ルーター

ルーターは、通常、内部ネットワークを管理するネットワーク端末で、ネットワーク全体の**ハブ**として機能します。小規模なオフィスやホームオフィスでは、ルーターは物理的な（通常は青色の）イーサネットケーブルを介して直接モデムに接続され、通常はインターネットから見てモデムの**後ろ**（内部ネットワーク側）に設置されます。類似するものにネットワーク**スイッチ**と呼ばれる端末がありますが、追加のイーサネット接続を形成するために用いられ、ルーター機能はありません。古いルーターは物理的なイーサネットケーブルしか接続できない場合がありますが、新しいルーターは、ワイヤレスアクセスポイント（WAP）としても機能して端末をワイヤレスで接続します。新しいルーターはファイアウォールとしても機能し、Dynamic Host Control Protocol（DHCP）を介してインターネットプロトコル（IP）アドレスを管理します。本ドキュメントでは、主にルーターのセットアップ、使用方法、保守に関して説明しています。

モデムとルーターのハイブリッド

ルーターとモデムは、元は別の端末でしたが、最近店頭で販売されているモデムや ISP が提供するモデムのほとんどにはルーターが組み込まれています。これらの端末は「モデム」や「ルーター」と混同される場合があり、端末がハイブリッドかどうかを区別するための確認が必要です。これらは「ゲートウェイ」とも呼ばれます。

中継器

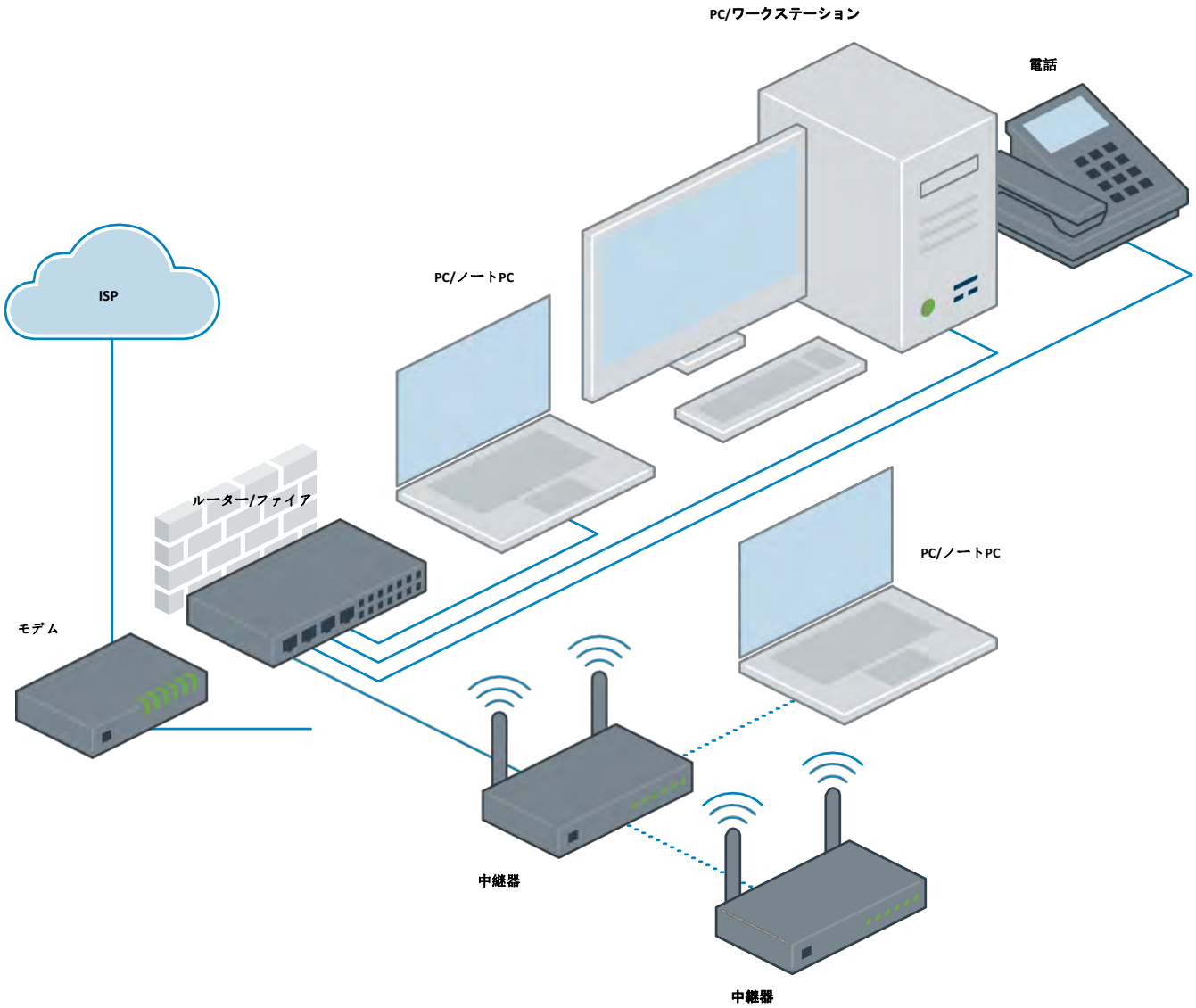
中継器は**ブリッジモード**の WAP です。つまり、自宅やオフィスに WiFi ネットワークを拡張する手段として機能します。中継器は、無線電波が弱いか、存在しない場所で使用し、利用エリアを拡張するために使用します。WiFi ネットワークを拡張するこの方法は、ユーザーと端末所有者の両方に様々な利点をもたらします。たとえば、別のワイヤレスネットワークを構築することが可能になったり、モデムからのイーサネットケーブルの配線が不要になります。主な利点として、ネットワーク名を少しだけ変えて 2 つの個別の WAP を使用したり、接続が必要な端末やコンピューターごとに複数のワイヤレスネットワーク設定が不要となることが挙げられます。信号が十分に強い場合、ワイヤレス端末は中継器に自動的に接続できます。中継器は ISP から提供される場合もあり、家電量販店やインターネットから別途購入する場合もあります。これらは、**WiFi 中継器または WiFi レンジエクステンダー**と呼ばれることもあります。

携帯電話信号ブースター

携帯電話信号ブースターは、携帯電話ネットワークへのアクセスを簡素化するため、WiFi 中継器と同様に動作します。これらの端末は、個人や組織の自宅やオフィスが携帯電話の受信範囲に入っていない場合に必要です。このような状況は、電波塔が遠いか、部屋の壁が携帯電話の電波を遮断する素材でできていることが原因です。携帯電話信号ブースターは、多くの場合モデムに直接接続します。これらの端末は、セルラーエクステンダー、フェムトセル、セルラーゲートウェイとも呼ばれます。

一般的な使用法

次の図は、これら端末の一般的設置例です。端末をネットワークアーキテクチャにどのように配置するかによって、セキュリティに影響が生じる場合があります。



必要となるセキュリティ機能

ホームオフィス用のルーター市場は非常に競争が激しく、頻繁に新しい機能が追加されます。以下は、新しいホームネットワーク端末に搭載されるセキュリティ関連の機能の例です。これら項目すべてがホームネットワークのセキュリティに重要とは言えませんが、購入を決定する際に検討する価値があります。

- **ソフトウェアアップデートの頻度**：端末の製造元から定期的にセキュリティ更新プログラムが提供され、問題が解決されます。
- **自動更新**：製造元から提供されたセキュリティ更新プログラムが端末にインストールされます。
- **WPA3**：Wireless Protected Access Version 3（WPA3）は、WiFi 規格の最新バージョンで、攻撃者によるトラフィックのスパイ行為やルーターへの攻撃を防ぐための新しい認証および暗号化プロトコルが含まれています。
- **ゲストネットワーク**：信頼できる端末と信頼できない端末の境界線として機能します。また、一時的なパスワードなどを使用することで WiFi ネットワークパスワードを提供することなく、個人がネットワークにアクセスできます。
- **内蔵型ファイアウォール**：トラフィックが内部ネットワーク上の 端末に到達するのをブロックします。
- **内蔵型仮想プライベートネットワーク（VPN）**：ネットワーク端末から VPN プロバイダへのトラフィックを暗号化し、ISP がトラフィックを見ることができないようにします。VPN プロバイダはトラフィックを見ることができるため注意が必要です。
- **VPN アクセスを許可**：サードパーティ VPN がネットワーク上で動作することを許可またはブロックできます。端末とネットワークのセキュリティには重要ではありませんが、状況によっては便利な場合があります。
- **ペアレンタルコントロール**：子供が成人向けやその他の不適切なコンテンツにアクセスできないようにすることができます。また、従業員が不正なコンテンツにアクセスしないようにすることもできます。成人向け、または違法なコンテンツサイトには、コンピューターが感染するおそれのあるマルウェアや危険なコンテンツが含まれていることがよくあります。
- **2 段階認証（2FA）**：2FA を一部のネットワーク端末で有効にすると、アクセスが必要なユーザーに対して端末へのアクセス権を付与できます。

ネットワーク機器の購入先

ネットワーク端末は、近くの家電量販店、オンラインショップ、ISP などから購入できますが、重要な点は、**信頼** *できるソース*から端末を入手することです。例えば、中古の端末を購入することはリスクがあります。理由として、誰かが既にパスワードを知っていて、端末に長期的にアクセスできる可能性があるためです。また、中古の端末は故障する可能性が高く、ベンダーのサポートがないため、インターネットにアクセスできないという根本的な問題が生じる場合があります。

基本的な端末設定

パッケージから新しい端末を取り出した後、製造元に登録します。登録することで、端末に問題が発生した場合に備えて、端末の保証サービスを受けられます。また、デジタル多用途ディスク（DVD）、コンパクトディスク（CD）、ユニバーサルシリアルバス（USB）ドライブなどの物理メディアや、端末に付属する認証情報（端末のファームウェアやパスワードなど）を安全な場所に保管するのも賢明です。ルーターを工場出荷時の設定にリセットしたり、組織のIT担当者にアクセス権を付与したりする際に便利です。

ISPが端末を提供してサービスを設定している場合は、モデムやルーターは適切に設定されていると考えて良いでしょう。ただし、管理者アカウントの追加、変更、または無効化の方法とパスワードの変更方法を確認する必要があります。また、端末を電源に接続した後、ISP接続がアクティブになると、端末が起動してワイヤレスネットワークがアクティブになります。ワイヤレスネットワークをアクティブにしたくない場合は、調査してオフにするか（無効にする）、すぐに製造元によってデフォルトでオンに設定されているすべてのWiFiネットワークの設定を行います。最後に、ルーターを使用するためにユーザーにアカウントサインアップを要求する端末メーカーもあります。

初期アクセス

端末のユーザーマニュアルには、**管理ポータル**にアクセスする方法が記載されており、管理ポータルでルーターの設定を変更できます。ポータルにアクセスする最も一般的な方法は、アプリケーションまたはWebページを使用する方法です。アプリケーションを使用してルーターを制御すると、ルーターにアクセスできるコンピューターシステムが制限されるため便利です。より一般的な方法は、ブラウザーを開き、192.168.1.1や192.168.0.1などの特定のWebアドレスを使用して管理ポータルにアクセスする方法です。必須ではありませんが、WiFiの代わりにイーサネットなどの有線接続を使用して管理作業を行う方が安全です。ブラウザーでHTTPではなくHTTPSを使用しているWebポータルのほうが、より安全です。http://cisecurity.orgよりも、https://cisecurity.orgの方がより安全性が確保されることになります。

内部および外部ネットワークインターフェイス

ルーターとモデムには、複数のネットワークカードが搭載されています。ルーターには、接続されている各ネットワーク用のネットワークカード（または*インターフェイス*）が必要で、ルーターには外部ネットワークと内部ネットワークが存在します。これは、ルーターがISPのネットワーク（外部インターフェイス）とホームネットワーク（内部インターフェイス）の間のゲートウェイとして機能するためです。一部の端末では、これらの両方のインターフェイスに個別のパスワードが設定されています。ISPは外部インターフェイスに常にアクセスする必要があり、ルーターが提供するアクセスのタイプに注意し、可能な限りアクセス制御を試みます。ファイアウォールをルーター（多くの場合、1つのネットワーク端末の機能として搭載）と組み合わせて使用すると、外部端末が内部ネットワークにアクセスできないように制御できます。

パスワード

パスワードは、**認証**と呼ばれるプロセスを介してネットワーク端末にアクセスするために使用される主要な資格情報です。すべてのパスワードは、8文字以上にするなど、強力なパスワードにする必要があります。ネットワーク端末の設定で使用する管理者パスワードは、工場出荷時の設定から独自のものに変更し、必要がなければ個人や他のサービス、プラットフォーム、アプリケーションと共有してはいけません。ネットワークパスワードを組織で使用する場合は特に重要ですが、家庭で使用する場合は必須ではありません。

ルーターの管理者パスワードは内部ネットワークインターフェイスのパスワードであり、WiFiネットワークのパスワードとは全く別のものに設定します。ネットワーク端末に使用されるパスワードには、次のような種類があります。

- **WiFi ネットワークのパスワード**：ワイヤレスネットワークへのアクセスに使用します。このパスワードは、他人と共有する可能性があります。
- **内部ルーターの管理者パスワード**：内部ルーターの設定ダッシュボード、またはモバイルアプリ用アプリケーションへのアクセスする際使用します。
- **ISPのパスワード**：ISPのオンラインポータルにサインインし、アカウント管理に使用します。
- **管理アプリケーションのパスワード**：ルーターによっては、ルーターを制御するモバイルアプリケーションを提供しており、パスワードで保護できます。

警告：多くのルーターには、パスワードが予め設定されています。また、ルーターモデルのデフォルトパスワードの多くは、インターネットに接続しWeb検索で簡単に入手できるため、管理パスワードを変更し、デフォルトのパスワードを使用しないことが**非常に重要**です。

端末とネットワーク管理アプリ

ルーターの製造元によっては、管理機能用のネットワーク管理アプリケーションも提供しています。最も一般的なものは、携帯電話用アプリケーション（アプリ）であり、これらのアプリを使用すると、パスワードを使用してルーターにアクセスできます。2FAがオプションとして利用できる場合もあり、より高い安全性を確保できます。モバイル端末を使用してルーターの設定やメンテナンス作業を行う場合は、端末に最新のソフトウェアアップデート（自動アップデートを推奨）を適用するように設定します（端末ロック画面の使用など）。

基本的なネットワーク設定

新しいネットワーク端末を電源に接続すると、端末が起動して 2 つの WiFi ネットワークのブロードキャストが自動的に開始する場合があります。これら2つのWiFi ネットワークには、同じネットワーク名またはSSIDが付けられますが、名前の末尾に動作周波数が付く 場合があります。たとえば、5 ギガヘルツ（GHz）ネットワークの名前は、**SampleNetworkName-5Ghz** のように表示されます。これは、WiFi が2.4 Ghz と5 GHzの2 つの周波数で動作し、それぞれの周波数で別々のネットワークをブロードキャストするからです。ネットワーク名を区別する例として、**SampleNetworkName _2** と **SampleNetworkName _5** がありますが、サインイン資格情報を取得した後、必要に応じてこれら両ネットワークを変更し管理できます。

端末の場所

ネットワーク端末が物理的に配置されている場所によって、セキュリティは大きく変わります。ネットワーク端末は、公共の場所や家庭への来訪者から離れた場所に保管する必要がありますが、ルーターに物理的にアクセスできる状態では、ワイヤレスネットワークのパスワードを入力せずに、ネットワークへアクセスができる場合があります。これは、イーサネットケーブルをルーターに接続してからコンピューターに接続し、管理ポータルにアクセスすることで簡単に実行できます。また、すべての内部ネットワークインターフェイスでパスワードを変更できない場合があるので、ルーターを物理的なセキュリティで保護することが重要になります。

WiFi ネットワーク名の作成

ネットワーク名を作成する際注意すべき点は、近隣やオフィスで個人や組織を特定できる名前を作成しないことです。これは、独立した建物にある組織にとっては問題となりませんが、密集した都市部で働く在宅勤務者にとっては問題となります。そのため、いずれの場合も、ネットワーク端末のタイプを識別するために設定された通常のデフォルト名を別の名に前変更します。ネットワーク名を設定する際、特定の個人の名前、組織名、住所、部屋番号（たとえば、Apartment516WiFi）を含める必要があるかどうかをよく考えましょう。

WiFi ネットワーク名の作成に関するもう1つの注意事項は、WiFi ネットワーク名のブロードキャストを行わないことです。これは**SSID クローキング**とも呼ばれます。10 年以上前は、ネットワーク名を非表示にすることはベストプラクティスと考えられていましたが、最近ではこの問題に対する一般的な意見は年々変化しています。基本的なワイヤレスハッキング機器はネットワークを検出できるため、SSID クローキングでは、攻撃者からネットワークの存在を隠すことはできません。しかし、SSID クローキングは、**認証された**ユーザーがネットワークに接続する際問題を引き起こすことがよくあります。これは、プライマリーコンピューターと付随するモバイル端末またはIoT 端末の両方にも当てはまります。つまり、SSID クローキングのセキュリティ上の利点は疑わしいものであり、ネットワークをブロードキャストする利点の方が重要であることは明白です。従って、SSID クローキングは推奨しませんが、推奨する意見もあったりと賛否両論な状況です。

ゲストネットワークの構築

ゲストネットワークは、機密データが保存されている端末と、信頼できない端末を分離する場合に便利です。来訪者がWiFi ネットワーク接続を必要とする際、2 つの別々のルーターを使うか、ルーターのゲストネットワーク機能を使うか、いずれかの方法で対応できます。WiFi ネットワークのパスワードは、できるだけ限られた少人数の、かつ信頼できる人と共有することが重要です。2 つの個別のルーターを使用し、それぞれに個別のパスワードとモデムへの独立した接続（これが重要なポイントです）を行えば、信頼できる端末と信頼できない端末を簡に簡単に分離できます。この構成の欠点は、コストと管理面です。一部のルーターには、ゲストネットワーク機能が組み込まれているため、端末間をある程度分離でき、ネットワークのWiFi パスワードを共有する必要がなくなります。一部のゲストネットワーク機能では、一時的なパスワードやスケジュール制限（営業時間内のみ利用可能など）も使用できます。

自動更新の有効化

ソフトウェアの更新は、ネットワーク端末の安全性を維持するために非常に重要です。新しいセキュリティ上の欠陥や脆弱性が常に発見されており、これらの問題に防御するには、端末の製造元から提供されるアップデートをインストールすることです。残念ながら、一部の製造元では、ネットワーク端末用のソフトウェア更新プログラム作成に時間や専門知識などのリソースを要するため、セキュリティ更新プログラムを提供していない場合があります。そのため、ソフトウェアアップデートの提供実績のある製造元からルーターを購入することが重要です。ルーターを使用している場合は、アップデートが自動的に適用されるよう設定することが重要です。アップデートを手動でインストールすることも可能ですが、自動アップデートを有効にすることで抜け漏れなく適用できます。

トラフィックの暗号化

暗号化は、不正アクセスや改ざんから情報を隠すためにデータを変換するという、安全な通信方法のための技術です。暗号化には多くの種類があり、強力な暗号も存在します。一方、古い端末の機能を利用するために、旧式で効果の薄い暗号化を継続してサポートしている端末もあります。小規模オフィスやホームネットワークで適切な種類の暗号化を使用することで、他人が認を認証を行わず機密情報を見ることを防ぎます。暗号に関連するプロトコルと概念の中でも、特に暗号化と認証については、次の点を考慮してください。

Wired Equivalent Privacy（WEP）

WEP（Wired Equivalent Privacy）は、一般的な無線アクセスポイントに組み込まれた WiFi 用の暗号化技術として最初に開発された方法です。1990 年代後半に初めて導入され、現在では安全ではないと考えられているため、**いかなる状況でも使用はお勧めできません**。また、下位互換性のため、主にホームネットワーク端末での使用に限られ、暗号は無料でインターネット上で入手できるソフトウェアを使用して簡単に解読できます。

WiFi Protected Access（WPA）

WEP が解読されるようになった後、WiFi Protected Access（WPA）が WiFi 通信保護の一時的な解決策として導入されました。ネットワーク端末内では、WPA は**WPA-Personal** または**WPA-PSK（Pre-Shared Key）**として表示されることもあります。WPA は解読されませんが、WPA を使用するネットワークのセキュリティに悪影響を与える攻撃が存在します。特に、短いパスワードを使用している場合にあてはまります。WPA の解読はそれほど難しくありませんが、特殊な知識と機器が必要になることが多く、WEP よりもはるかに強力です。基本的な WPA 暗号化を使用することはお勧めしませんが、代わりに、下記の WPA2 と WPA3 を使用します。

WiFi Protected Access Version 2（WPA2）

WPA2 は、世界中のネットワークのデファクトスタンダードです。その暗号化技術は、長年にわたって強力に機能しています。WPA2 は、米国政府が採用している暗号方式の 1 つである Advanced Encryption Standard（AES）を使用しており、複数のタイプと設定の難しいエンタープライズ向けもあります。WPA2-Personal と WPA2- Enterprise の違いの 1 つとして、パスワードの配布方法があります。WPA2-Personal は、小規模オフィスやホームオフィスのニーズに十分対応できます。

WiFi Protected Access Version 3（WPA3）

WPA3 は、WiFi 向けの最新のワイヤレスセキュリティ技術であり、現在世界中の新しい端末に導入されています。WPA3 の主なセキュリティ上の利点として、長いキーサイズ（大規模な組織にとって最も望ましい）と前方秘匿性があります。特に、前方秘匿性は、ユーザーがWiFi パスワードを取得したとしても、過去のインターネットアクティビティの読み取りを防止できます。ネットワーク端末の多くは、WPA3 使用のためのソフトウェアパッチまたはソフトウェアアップデートをダウンロードできません。そのため、新しいWPA3 対応端末を購入する必要があります。

WiFi Protected Setup（WPS）

WPS は、ルーターに簡単に接続するために、一部のルーターに実装されているプッシュボタンです。WPS は、ユーザーがWiFi ネットワークに簡単に接続できるよう設計されており、4 つの異なる接続方法を提供します。残念ながら、WPS には複数の重大なセキュリティ上の欠陥が発見されました。これらの欠陥の一部は、悪用が非常に簡単で、攻撃者が許可なくWiFi ネットワークに接続できることです。WPS は、現在も有名メーカーの端末に採用されていますが、**できればWPS を無効にしてください**。ルーターにWPS が搭載されていると、ルーターに物理的にアクセスできるユーザーがネットワークパスワードを入力せずに接続し、ネットワークトラフィックを読み取ることができるからです。

追加のネットワーク構成

ルーターなどのネットワーク機器は、さまざまな方法で追加できます。詳細な構成オプションとその機能は製造元によって異なりますが、ほとんどの汎用ネットワーク端末には以下のオプションが提供されています。

ファイアウォール

ファイアウォールを設定すると、悪意のあるネットワークトラフィックや、ネットワークに侵入しようとする情報が特定の端末に到達しないよう阻止できます。ファイアウォールは通常、多くの家庭用ルーターに組み込まれていますが、それぞれの利便性と有効性を把握することは困難です。ファイアウォールが組み込まれているルーターは高価となる場合があるため、組織でこのリソースの出費に見合う価値があるか判断が必要です。一般的に、大規模で複雑なネットワークを使用している組織や、インターネットに接続するサービス（FTP、SSH など）を使用している組織は、ファイアウォールを導入したモデルの使用を検討する必要があり、ルーターのファイアウォール機能のほとんどは、「低セキュリティ」、「中セキュリティ」、「高セキュリティ」など、複数のレベルに設定できます。このガイドでは、初期設定時に一番レベルの高いセキュリティ設定を使用することをお勧めします。ユーザーが適切なWeb リソースにアクセスできない場合、小規模オフィスやホームオフィスのニーズに合わせて、セキュリティレベルを下げてください。

ほとんどのルーターは、Network Address Translation（NAT）と呼ばれる機能も備えています。NAT は、ルーターの接続先の端末やネットワークを保護し、攻撃を開始できます。NAT の使用は、**IP マスキング**または**NAT ファイアウォール**と呼ばれ、NAT は常に有効にします。

端末の強化

主に、端末上のアクティブなポートやサービスを減らし、端末を強化します。ここでのサービスとは、外部コンピューターシステムと通信するためのルーター上の「プログラム」と考えられ、ポートは、外界への扉と考えることができます。ポートは番号で識別され、場合によってはプロトコル（UDP 53、TCP 80 など）で識別されます。また、一般的に、各サービスは通信に専用のポートを使用します。実行中のサービスを削除しポートを閉じてしまうことは、ホームネットワーク端末のセキュリティ向上には不適切です。

ドメインネームシステム（DNS）

DNS は、IP アドレスを Web サイト名（**ドメイン名**とも呼ばれる）に関連付ける方法です。基本的に、内部ネットワークのコンピューターが Web ページを要求するたびに、DNS サーバーを使用してインターネット上のページの場所を検索します。ホームネットワーク端末は通常、予め設定された DNS サーバーを使用しますが、ほとんどの場合は ISP の DNS サーバーです。代替 DNS オプションも用意され、特定の非営利組織やその他の組織が提供する DNS サーバーにより、コンピューターシステムが危険な Web サイトにアクセスしないよう防御します。DNS フィルタリングを使用すると、ネットワークが危険な Web サイトへのアクセスを要求しても、要求は実行されません。他の DNS サーバーも、ISP の DNS と同じように追跡しない場合があります。

セキュリティ上の利点がある一般的な DNS サーバーは 2 つあります。Quad 9（https://www.quad9.net）と OpenDNS（https://www.opendns.com）です。組織で使用しているコンピューターワークステーション、タブレット、モバイル端末に Quad 9 または OpenDNS を個別に設定する、もしくは、ネットワーク全体を保護するようルーターを設定することもできます。職場以外で使用する端末は、個別に設定する必要があり、端末に関係なく、DNS 設定を行う場所は端末内の管理領域にあります。Quad 9 の IP アドレスは 9.9.9.9、OpenDNS の IP アドレスは 208 .67 .222 .222 です。どちらの方法でもネットワークを保護でき、DNS サーバーにいずれかの IP アドレスを使用します。

『*CIS Controls Microsoft Windows 10 Cyber Hygiene Guide*』では、Microsoft Windows 10 ワークステーションで DNS フィルタリングを正しく設定できる追加情報を提供しています。サブコントロール 7.7（23 ページ）に記載されています。https:// www.cisecurity.org/white- papers /cis-controls-microsoft-windows-10-cyber- hygiene-guide/.

リモート設定

ISP が、ネットワークに接続されているモデムに対して**リモートメンテナンスを行う**際、パスワード、デジタル証明書などの資格情報の更新が必要になる場合があります。また、ISP のネットワークにアクセスするためのデータやその他の設定情報も、定期的に確認し設定する必要があります。ISP が自分のネットワークのモデムにアクセスできるか不確かな場合は、ISP のモデムのすぐ先にルーターを設置し、次に、すべての端末をそのルーターに接続し、モデムを使用してインターネットに接続します。

ユニバーサルプラグアンドプレイ（UPnP）

ユニバーサルプラグアンドプレイ（UPnP）は、ネットワーク上の端末が簡単に通信できるネットワークプロトコルスイートです。コンピューター、プリンター、ゲーム端末などの端末間でデータ共有に使用することが多く、設定は不要です。長年にわたり、UPnPプロトコルスイートには数多くのセキュリティ問題が存在しました。これらの重大なセキュリティ上の欠陥の数と重大度を考えると、特定の端末（ゲーム端末など）が正常に機能しなくなる場合もありますが、**UPnP は常に無効にすべき**と考えられます。実際、UPnP は、端末の接続を許可するためにファイアウォールに意図的に穴を開けます。UPnPが組織の運用にどうしても必要な場合は、UPnP の最新バージョンのみを使用します。ただし、端末を購入する前に最新のUPnP を確認することは難しいので、UPnP の機能の代替として、端末を手動で設定します。

メディアアクセス制御（MAC）アドレスホワイトリスト

MAC アドレスホワイトリストを使用して、端末が WiFi または有線ネットワークにアクセスできないように制限できます。MAC アドレスは、有線またはワイヤレス接続を行う端末のシリアル番号と似ており、MAC アドレスをホワイトリストに登録するには、各端末のMAC アドレスをルーターの管理ダッシュボードに登録する必要があります。残念ながら、MAC アドレスはかんたんに詐称されてしまうので、万全なセキュリティ管理は実現できず、また、ルーターの管理が難しくなるとさらにセキュリティ管理が複雑になる恐れがあります。WiFi の設計上、攻撃者は基本的な機器を使用して、ネットワークに接続されたすべての端末のMAC アドレスを追跡できます（ネットワークが暗号化されている場合も含みます）。短いコマンドを数回使用するだけで、WiFi ネットワークにアクセスしたいユーザーは認証をせずに有効なMAC アドレスをクローンして使用できます。MACアドレスは簡単に無効化でき、またホワイトリストの設定維持には多くの工数が必要となるため、本ガイドではホワイトリストの使用を推奨しません。

小企業向けのガイドライン

多くの個人や組織が、小企業や在宅勤務者向けにガイドラインを提供しています。以下に、関連する有用情報をまとめました。

- 『*5 Steps to Better Business Cybersecurity*』、商業改善協会。
  https://www.bbb.org/council/for-businesses/cybersecurity
- 『*10 Cybersecurity Mistakes Your Small Business Cannot Afford to Make*』、連邦取引委員会（FTC）とアメリカ連邦中小企業庁（SBA）による YouTube 上の Web セミナー。
  https://www.youtube.com/watch?v=KLrnI5ZEl9Y
- 『*CyberSecure My Business, Stay Safe Online*』、NCSA（National Cyber Security Alliance）の Web サイト。
  https://staysafeonline.org/resources/?filter=.topic-cybersecure-my-business.resource-item
- 『*Guide to Enterprise Telework and Remote Access Security*』、国立標準技術研究所（NIST）。
  https://csrc.nist.gov/publications/detail/sp/800-46/rev-1/archive/2009-06-16
- 『*Secure Router Configuration – The Short List*』（Michael Horowitz 氏による Web サイト『Router Security』）。
  https://routersecurity.org/#StartHere
- 『Small Business Information Security: The Fundamentals』、国際標準技術研究所（NIST）。
  https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- 『Start with Security: A Guide for Business』、連邦取引委員会（FTC）。
  https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

頭字語と略語

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
CD	Compact Disc
CIS	Center for Internet Security
DHCP	Digital Host Control Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
DVD	Digital Versatile Disc
FTC	Federal Trade Commission
FTP	File Transfer Protocol
GHz	Gigahertz
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
MAC	Media Access Control
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
SoHo	Small Office / Home Office
SP	Special Publication
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WPA	WiFi Protected Access
WPA2	WiFi Protected Access Version 2
WPA3	WiFi Protected Access Version 3
WPAN	Wireless Personal Area Network
WPA-PSK	WiFi Procted Access - Pre-Shared Key
WPS	WiFi Protected Setup

ネットワークセキュリティのチェックリスト

ネットワーク端末購入後に実施すべき設定のチェックリストです。ただし、の手順の一部は、実際の状況に該当しない場合があります。

- ☐ 購入したネットワーク端末の製造元にユーザー登録する
- ☐ すべてのルーターとモデムのデフォルトの管理パスワードを固有のパスワードに変更する
- ☐ 固有のパスワードを使用して、ISP の Web ポータルにアクセスする
- ☐ 可能な限り、2 段階認証を有効にする。これには、ISP の Web ポータル、ルーター/モデム、モバイルアプリへのアクセスを含む
- ☐ WiFi ネットワーク名（SSID）のパスワードを固有のものに変更する
- ☐ WiFi ネットワーク名（SSID）に自分の識別情報が含まれていないことを確認する
- ☐ WiFi ネットワークのパスワードを知っているユーザーを適切に管理する
- ☐ 2.4Ghz, または5Ghzネットワークのいずれかを使用していない場合は、両ネットワークともオフにする
- ☐ すべてのルーターとモデムを、一般の人や通行人がアクセスできない場所に移動する
- ☐ すべてのルーターとモデムの自動更新を有効にする
- ☐ WPA2 または WPA3 をオンにする
- ☐ 可能であれば WPS を無効にする
- ☐ ルーターとモデムのファイアウォールを有効にする
- ☐ ネットワークアドレス変換（NAT）を有効にする
- ☐ ルーターまたはモデム、あるいはその両方で DNS フィルタリングを有効にする
- ☐ UPnP を無効にする

CIS Controls へのマッピング

次に、CIS Controls におけるセキュリティ設定項目のマッピングを記載します。ただし、すべての項目が CIS Controls に準拠しているわけではありません。

CIS Control	防御対策
該当なし	端末を製造元に登録します。
4	すべてのルーターとモデムのデフォルトの管理パスワードを固有のものに変更します。
4	固有のパスワードを使用して、ISP の Web ポータルにアクセスします。
4	可能な限り、2 段階認証を有効にします。これには、ISP の Web ポータル、ルーター/モデム、モバイルアプリへのアクセスが含まれます
該当なし	WiFi ネットワーク（SSID など）のパスワードを固有のものに変更します。
該当なし	WiFi ネットワーク（SSID など）名に自分の識別情報が含まれていないことを確認します。
4	WiFi ネットワークのパスワードを知っているユーザーを、適切に管理します。
13	2.4 GHz または 5 GHz のいずれかを使用していない場合は、両ネットワークをオフにします。
該当なし	すべてのルーターとモデムを、一般の人や通行人がアクセスできない場所に移動します。
3	すべてのルーターとモデムの自動更新を有効にします。
15	WPA2 または WPA3 をオンにします。
11	可能であれば WPS を無効にします。
12	ルーターとモデムのファイアウォールを有効にします。
11	NAT を有効にします。
7	ルーターまたはモデム、あるいはその両方で DNS フィルタリングを有効にします。
11	UPnP を無効にします。

本ドキュメントについて

本ドキュメントでは、テレワークや小規模オフィスのネットワークセキュリティ環境におけるセキュリティに対するベストプラクティスの適用方法について説明します。

本ドキュメントで使用されているツールやその他の製品に関する記述はすべて情報提供のみを目的としており、特定の会社、製品、または技術をCISが推奨しているわけではありません。