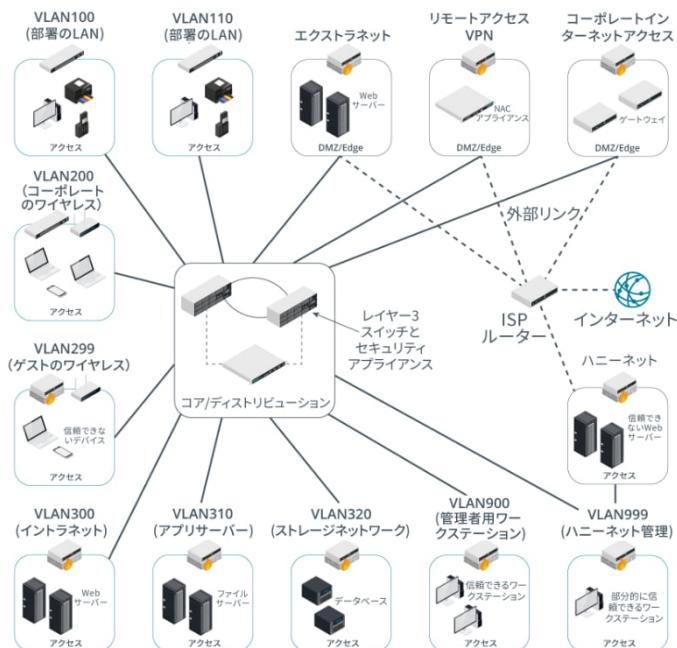


大規模なネットワークでは、ワイヤレスステーションとデスクトップワークステーションを分離したり、サーバーをそれぞれのグループに置いたりと、異なるホストグループを表現するためにさらに多くのゾーンが必要になる場合があります。Ciscoのエンタープライズセキュリティーアーキテクチャは、コアレイヤーとディストリビューションレイヤーを使用してアクセスロックを相互接続していますが、それぞれのアクセスロックは異なるゾーンやビジネス機能を表しています。



エンタープライズセキュリティーアーキテクチャ。(画像提供: © 123RF.com)

## 非武装地帯

さまざまなセキュリティゾーンを区別する上で最も重要なことは、ホストがインターネットに面しているかどうかです。インターネットに面したホストはインターネットからのインバウンド接続を受け入れ、インターネット上のホストに接続を行います。インターネットに面したホストは1つ以上の**非武装地帯(DMZ)**内に配置されます。DMZは境界またはエッジネットワークとも呼ばれます。DMZの基本的な原則は、トラフィックがそこを直接通過できないことです。DMZによって、外部のクライアントはWebサーバーなどプライベートシステム上のデータにアクセスできますが、内部ネットワーク全体のセキュリティが侵害されることはありません。DMZの両側にあるホスト間で通信が必要になった際には、DMZ内のホストがプロキシの役割を果たします。一例を挙げると、インターネットのホストがインターネット上のWebサーバーとの通信をリクエストした場合、DMZ内のプロキシがそのリクエストを受け取ってチェックします。有効であると判断されたリクエストは、その宛先に転送されます。外部のホストには、DMZの背後に何があるのか（もしあれば）全くわかりません。

**エクストラネット**サービスとインターネットサービスはいずれも、インターネットに面している可能性が高いのです。エクストラネットまたはパブリックアクセスサービスを提供するホストは、1つ以上の非武装地帯の中に配置されなければなりません。そこには通常、Webサーバーやメールサーバー、その他の通信サーバー、プロキシサーバー、リモートアクセスサーバーが置かれます。インターネットから侵害を受けている可能性があるために、内部ネットワークがDMZ内のホストを完全に信頼することはありません。こうしたホストは**要塞ホスト**と呼ばれ、攻撃対象領域を可能な限り減らすために最低限のサービスを実行します。ユーザーアカウント認証情報など、内部ネットワークのセキュリティリスクとなり得るデータで要塞ホストが構成されることはありません。

DMZの中で実行されるサービスは、それぞれ異なるセキュリティ要件を持っているので、複数のDMZが必要になる可能性があります。

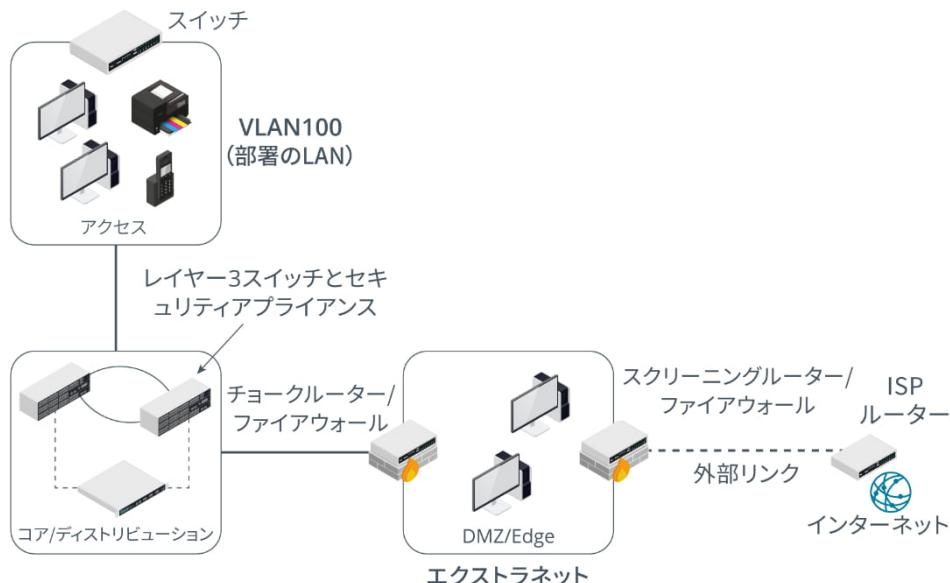
- 従業員によるWebブラウジングやその他のインターネットサービスへのアクセスを可能にする、プロキシまたはセキュアWebゲートウェイをホストするDMZ。
- メールサーバー、VoIPサーバー、または会議サーバーなどの通信サーバーをホストするDMZ。
- 仮想プライベートネットワーク(VPN)を介してローカルネットワークにリモートアクセスを提供しているサーバー用のDMZ。
- 許可されたクラウドアプリケーションへのトラフィックをホストするDMZ。
- フロントエンド、ミドルウェア、およびバックエンドの各サーバーを隔離する多層構成DMZ。

## 非武装地帯のトポロジー

DMZを構成するには、外部インターフェイス上と内部インターフェイス上で2つの異なるセキュリティ構成を有効化しなければなりません。DMZとイントラネットは異なるサブネット上にあるので、両者の間で通信を転送する必要があります。

### スクリーンサブネット

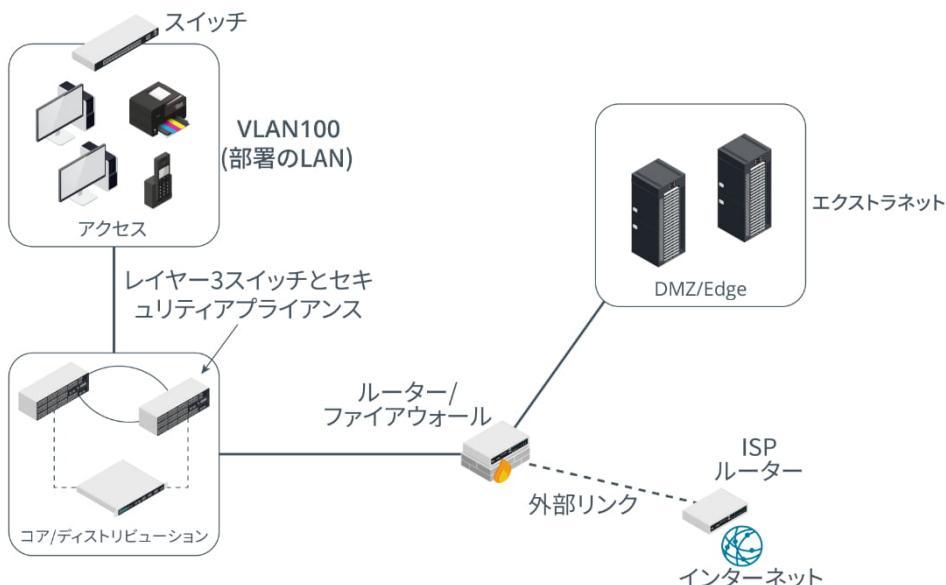
スクリーンサブネットは、DMZの両側に配置された2つのファイアウォールを使用します。エッジファイアウォールは外部パブリックインターフェース上のトラフィックを制限し、許可されたトラフィックがDMZ内のホストに届くようにします。エッジファイアウォールはスクリーニングファイアウォールまたはスクリーニングルーターと呼ぶことができます。内部ファイアウォールは、DMZ内のホストとLAN上のホストとの通信をフィルターします。このファイアウォールは choke point とも呼ばれます。 choke point は意図的に狭めたゲートウェイで、よりよいアクセス制御とより簡単な監視を可能にします。



スクリーンサブネット DMZ トポロジー。 (画像提供：© 123RF.com)

## トリプルホームファイアウォール

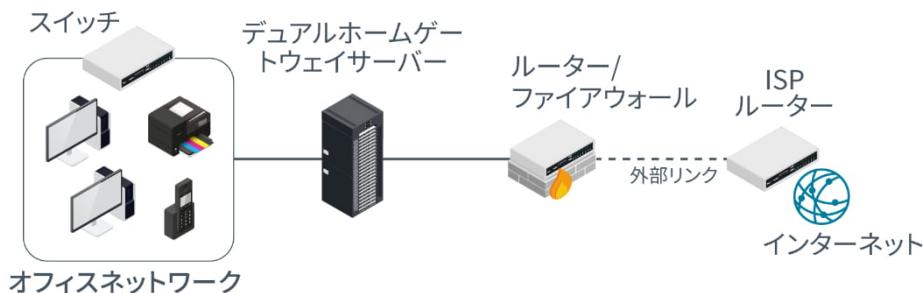
DMZは、3つのネットワークインターフェイスを持つルーター / ファイアウォールアプライアンスを用いて確立されることもあり、これはトリプルホームと呼ばれます。インターフェイスの1つはパブリックインターフェイスに、もう1つはDMZに、そして3つ目はLANに接続します。ルーティングとフィルタリングのルールにより、これらインターフェイス間でどの転送が許可されるかが判断されます。これによって、スクリーンサブネットと同じ種類の構成が可能になります。



トリプルホームファイアウォールDMZトポロジー。(画像提供：© 123RF.com)

## スクリーンホスト

より小規模なネットワークには、DMZを実装する予算や技能がないかもしれません。その場合は、インターネットアクセスは**スクリーンホスト**として機能する、デュアルホームのプロキシゲートウェイサーバーを使用して実装できます。



スクリーンホスト。(画像提供：© 123RF.com)

DMZ（またはDMZホスト）という用語が、インターネットからの接続を受け入れるローカルネットワーク上のホストを意味するものとして、SOHOルーターベンダーによって使用されることもあります。これは構成が簡単で、何らかのアクセス問題の解決を容易にしますが、ネットワーク全体が侵入やDoSに対して非常に脆弱になります。企業のDMZは個別のネットワークインターフェイスとサブネットによって確立されているので、DMZ内のホストとLAN間のトラフィックは転送される（およびファイアウォールルールの対象とする）必要があります。ほとんどのSOHOルーターには、真のDMZを生み出すのに必要なポートまたはルーティング機能がありません。

## IPv6が持つ意味

企業のクラウドサービスへのアクセス方法や、クライアントがWebサーバーやその他の公開サーバーへのアクセス方法などについて、IPv6は構内ネットワークに影響を及ぼします。

IPv6はクライアントやサーバー上、さらにはネットワークアプライアンス（ルーターおよびファイアウォール）においてデフォルトで有効化されていることもあるので、その管理とセキュリティの計画を立てる必要があります。IPv6が有効化されているものの管理されていなければ、バックドアや隠れチャネルとして悪用される恐れがあります。IPv6はまた、近隣探索でのスプーフィングやDoS攻撃など、新種の攻撃ベクトルを晒し出します([tools.cisco.com/security/center/resources/ipv6\\_first\\_hop](https://tools.cisco.com/security/center/resources/ipv6_first_hop))。

各ホストには、IPv4トポロジーと同じゾーンに対応するIPv6アドレスを割り当てる必要があります。またファイアウォールは、IPv4の場合と同じセキュリティ構成を実現する、または（よりよい選択肢である場合には）IPv6をブロックするACLと共に構成しなければなりません。ここでの問題の1つに、IPv6はいかなるタイプのアドレス変換も行うこと目的とはしていない、ということがあります。プライベートアドレスとパブリックアドレスのマッピングによって内部/外部のトラフィックフローを覆い隠すのではなく、IPv6のルーティングとファイルタリングのポリシーは、それに相当するIPv4アーキテクチャと同様になるよう構成しなければなりません。

 Internet SocietyはIPv6が持つセキュリティ上の意味に関するホワイトペーパーを刊行しています ([internetsociety.org/wp-content/uploads/2019/03/deploy360-ipv6-security-v1.0.pdf](https://internetsociety.org/wp-content/uploads/2019/03/deploy360-ipv6-security-v1.0.pdf))。サービスをIPv6へ移行することに関するInfobloxのホワイトペーパーは、より有益な状況を提供しています([infoblox.com/wp-content/uploads/2016/04/infoblox-whitepaper-seven-deadly-traps-of-ipv6-deployment\\_0.pdf](https://infoblox.com/wp-content/uploads/2016/04/infoblox-whitepaper-seven-deadly-traps-of-ipv6-deployment_0.pdf))。

## セキュアなネットワーク設計に関するその他の検討事項

ネットワーク設計は、データセンターやクラウドについても検討する必要があります。データセンターはサーバーとクライアントワークステーション機器の組み合わせというよりも、サーバーのホスティングを目的とした施設です。

### イーストウェストトラフィック

データセンターを出入りするトラフィックはノースサウス（南北）トラフィックと呼ばれます。このトラフィックは、データセンター外のクライアントがリクエストを行い、レスポンスを受け取ることを表しています。クラウドやその他のインターネットサービスをサポートするデータセンターでは、ほとんどのトラフィックは実際のところ、そのデータセンター内のサーバー間のものです。これはイーストウェスト（東西）トラフィックと呼ばれます。

ソーシャルメディアへの投稿の一部として写真をアップロードするクライアントのことを考えてみましょう。この画像ファイルは分析サーバーにより、ポリシー違反（例えば公序良俗に反しているとか、著作権違反を犯しているなど）の有無についてチェックされ、検索/インデックスサービスがその画像のメタデータで更新され、コンテンツデリバリーネットワーク(CDN)を提供するサーバーにその画像が複製されると共に、バックアップサーバーにもコピーされる、といった経過を辿ります。クラウドに対する単一のリクエストは複数のリクエストに連鎖され、そのクラウド内で転送される傾向があります。

イーストウェストラフィックが圧倒的に多いため、セキュリティ設計が複雑になります。もし、これらの連鎖したトランザクションのそれそれが、ファイアウォールや他のセキュリティ機器を通過することになると、深刻なボトルネックが生じます。そうした要件のために、サーバー間を行き来するトラフィックを監視できる、仮想化されたセキュリティアプライアンスの開発が促進されています([blogs.cisco.com/security/trends-in-data-center-security-part-1-traffic-trends](http://blogs.cisco.com/security/trends-in-data-center-security-part-1-traffic-trends))。

## ゼロトラスト

**ゼロトラスト**は、境界セキュリティが完全に堅牢である可能性は低い、という考え方方が土台となっています。現在のネットワーク上には、トラフィックが境界デバイスやDMZによる監視を逃れる機会があまりに多く存在しています。ゼロトラストは継続的認証や条件付きアクセスといったシステムを用いることで、脅威アクターによる特権エスカレーションやアカウント侵害を軽減します。

もう1つのゼロトラストテクニックに、マイクロセグメンテーションを適用させるというものがあります。マイクロセグメンテーションは、個々のノードが独自のゾーンにあるかのようにポリシーを適用するセキュリティプロセスです。イーストウェストラフィックと同じく、これを実装するには新世代の仮想化されたセキュリティアプライアンスが必要となります([vmware.com/solutions/micro-segmentation.html](http://vmware.com/solutions/micro-segmentation.html))。

# レビューアク ティビティ：

## セキュアなネットワーク設計

次の質問にお答えください。

1. 最近行われたセキュリティ評価によって、あなたの会社のネットワーク設計は過度に統合されていると結論づけられました。大きく異なる機能や目的を持つホストが、ネットワークの同じ論理エリアにひとまとめにされているのです。そのせいで、脅威アクターはこれまでこのネットワークホストの広大な領域を容易に侵害することができました。このネットワーク設計のセキュリティを改善するために、あなたはどのようなテクニックを提案しますか？その理由は？
2. あなたはあるクライアントとネットワークアーキテクチャの再設計について話し合っており、エクストラネットとインターネットの違いは何かと訊かれました。それをどう説明しますか？
3. セキュアなネットワーク設計においてサブネット化が有益なのはなぜですか？
4. 企業のDMZはどのように実装できますか？
5. イーストウェストトラフィックを計算に入れた設計が必要なのは、どのようなタイプのネットワークですか？

# トピック9B

## セキュアなスイッチングとルーティングを実装する



### 対象試験範囲

1.4 与えられたシナリオに基づいて、ネットワーク攻撃に関する可能性のあるインジケーターを分析することができる。

3.1 与えられたシナリオに基づいて、セキュアなプロトコルの実装を行うことができる。  
(ルーティングとスイッチングのみ)

3.3 与えられたシナリオに基づいて、セキュアなネットワークデザインを実装することができる。

低レベルのネットワーク機能に対する攻撃が、非常に有効である場合があります。機密性、完全性、可用性を実証するネットワーク設計を実装するには、スイッチとルーターを適切な設定で構成しなければなりません。それらのデバイスを用いてネットワークアクセス制御メカニズムを強化し、耐障害性の高いパスをネットワーク内に確立することができます。

### 中間者攻撃と第2層攻撃

多くの場合、OSIモデルで第1層および第2層と呼ばれる、物理レイヤーやデータリンクレイヤーにおける攻撃は、情報収集、つまりネットワークマッピングやネットワークトラフィックの傍受に焦点を当てています。

#### 中間者/オンパス攻撃

脅威アクターは低レベルのデータリンクプロトコルにおけるセキュリティの欠如を利用して、**中間者(MitM)攻撃**を実行することもできます。中間者攻撃またはオンパス攻撃は、脅威アクターが2つのホストの間に陣取り、それらホスト間のすべての通信を気づかれることなく捕捉し、監視し、中継することを指します。オンパス攻撃はトラフィックを密かに改変するためにも使用されます。例えば、中間者ホストはワークステーションに偽装したWebサイトフォームを表示し、ユーザーの認証情報を取得しようとすることができます。別の一般的なオンパス攻撃として、DNSクエリへの応答を偽装し、偽装したWebサイトにユーザーをリダイレクトさせる、というものがあります。オンパス攻撃は、両方のホストがセキュアな認証情報を交換するという相互認証を用いて撃退することができます。しかし第2層においては、そうした制御を導入するのが常に可能なわけではありません。

#### MACクローニング

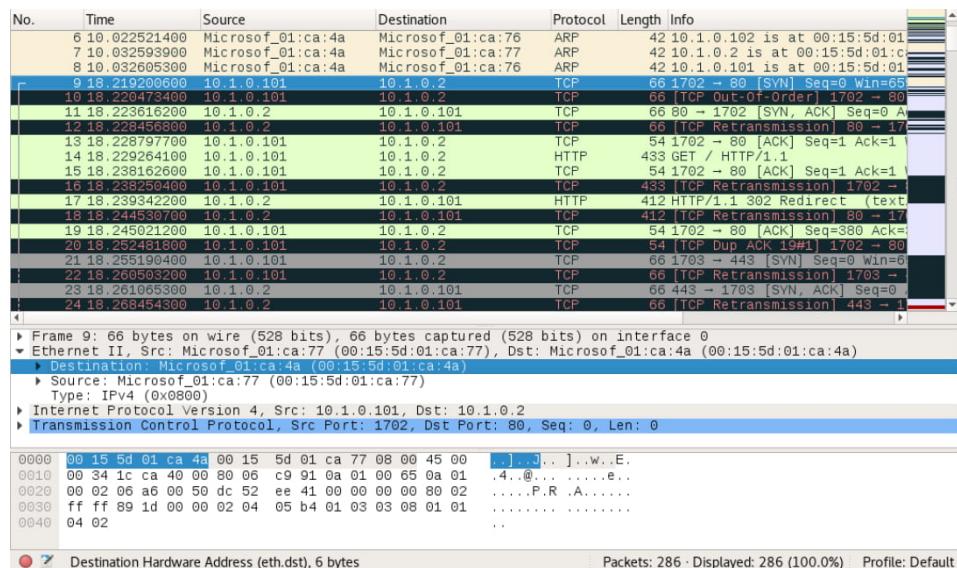
**MACクローニング**（またはMACアドレススプーフィング）は、アダプタインターフェイス上に設定されたハードウェアのアドレスを変更すること、または任意のMACアドレスの使用を有効化することです。各ネットワークインターフェイスには、ベンダーによって出荷時に独自のMACアドレスが割り当てられます。OSコマンド、ネットワークドライバ構成の変更、および**パケット工作**ソフトウェアの使用によって、ソフトウェア内で簡単に上書きすることができます。そのために、セキュリティインシデントを調査する際、またはセキュリティ管理の一部をMACアドレスに依存する際に、さまざまな問題が生じることになります。表示されたデバイスのアドレスが信頼できない場合があるからです。

## ARPポイズニングとMACフラッディング攻撃

ホストはアドレス解決プロトコル(ARP)を使用することで、IPアドレスを所有するローカルセグメント上のホストを発見します。

### ARPポイズニング攻撃

**ARPポイズニング**攻撃では、Ettercapなどのパケット工作ツールが使用して、不適切なARPリプライパケットをブロードキャストします。ARPにはセキュリティメカニズムがないので、受信側のデバイスはこの通信を信頼し、偽装されたアドレスで自身のMAC:IPアドレスキャッシュテーブルを更新します。



ARPポイズニングを示す、Wiresharkで開かれたパケットキャプチャ。  
(スクリーンショットは[wireshark.org](http://wireshark.org)からの許可を得て使用。)

このスクリーンショットは、典型的なARPポイズニング攻撃の際に捕捉されたパケットを示しています。

- 第6～第8フレームにおいて、攻撃側のマシン（MACアドレスの末尾が:4a）は、IPアドレス.2および.102を有すると称しつつ、不当なARPリプライを他のホスト(:76および:77)に送信しています。
- 第9フレームにおいて、.101/.77のホストは、.2のホストにパケットの送信を試みますが、攻撃側のホスト(宛先MACアドレス:4a)によって受信されました。
- 第10フレームにおいて、攻撃側のマシンは実際の.2ホストに第9フレームを再送します。再送信を強調するために、Wiresharkではそのフレームが黒と赤で表示されます。
- 第11、第12フレームでは、第11フレームで攻撃側のホストが受信し、第12フレームで正当なホストに再送信された、.2からのリプライを見ることができます。

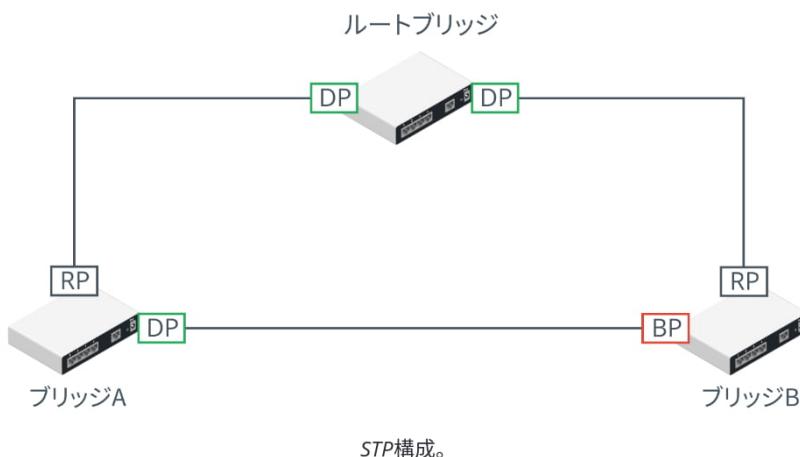
通常、ターゲットはサブネットのデフォルトゲートウェイ（他のネットワークにアクセスするルーター）です。ARPポイズニング攻撃が成功した場合、リモートネットワークを宛先とするすべてのトラフィックが脅威アクターに送信されることになります。脅威アクターは、通信を監視し、次いで検知を避けるためにそれらをルーターに転送することで、またはパケットを転送する前にそれらを改変することで、中間者攻撃を実行することができます。また、パケットを転送しないことでサービス拒否攻撃を実行することもできます。

## MACフラッディング攻撃

ARPポイズニングがホストを標的にする一方、**MACフラッディング**はスイッチを攻撃するために使用されます。脅威アクターの目的は、MACアドレステーブルを保存するために用いるスイッチのメモリを枯渉させることです。スイッチは**MACアドレステーブル**を用いることで、ユニキャストトラフィックを正しい宛先に転送するために、どのポートを使用するかを決定します。テーブルをオーバーフローさせると、スイッチはMACベースの転送を停止し、すべてのポートからユニキャストトラフィックを転送する、ハブのように機能するようになります。これにより、脅威アクターはより簡単にネットワークトラフィックをスニッフィングできます。

## ループ防止

イーサネットスイッチの第2層転送機能は、ブリッジと呼ばれるより旧式のネットワークアプライアンスのそれと類似しています。複数のブリッジ（最近はスイッチとして実装されている）を有するネットワークにおいては、フレームが意図された宛先へと向かうパスが1つ以上存在する場合があります。第2層プロトコルであるイーサネットには、Time To Live（有効期間）という概念はありません。従って、第2層のブロードキャストトラフィックは、複数のパスを有するネットワークを無限にループし続ける可能性があります。第2層ループは、**スパニングツリープロトコル(STP)**によって防止できます。スパニングツリーは、ブリッジが自ら階層構造をとり、ループの形成を防止する手段です。



STP構成。

このダイアグラムは、3つのブリッジ（またはスイッチ）のネットワークで、ループの防止が必要な最小の構成を示しています。ルートブリッジには、ブリッジAとブリッジBに接続される2つの指定ポート(DP)があります。またブリッジAとBのいずれにも、ルートブリッジのインターフェイスに接続されるルートポート(RP)があります。またブリッジAとBは相互に直接接続されています。ブリッジAでは、このインターフェイスがアクティブであり、ブリッジBへのトラフィックはそれを介して直接転送されます。ブリッジBでは、このインターフェイスがブロック(BP)されてループを防止しており、ブリッジAへのトラフィックはルートブリッジ経由で転送しなければなりません。

## ブロードキャストストーム防止

STPは主に、**ブロードキャストストーム**の防止を目的にしています。スイッチはすべてのポートからのブロードキャスト、マルチキャスト、および宛先が未知のユニキャストトラフィックを転送します。ブリッジで構成されたネットワークにループが含まれていると、ブロードキャストトラフィックはそのネットワークを流れ、他のスイッチによって增幅され、元のスイッチに戻ることになります。するとそのスイッチはそれぞれのブロードキャストフレームを再度ブロードキャストして指數関数的増幅（ストーム）を引き起こしてしまい、すぐさまスイッチを機能停止に追い込むと共に、ネットワークをクラッシュさせます。

ループはあるパッチパネルポートから別のパッチパネルポートにパッチケーブルを接続することで、または2つの壁のポートを接続することで、偶然生じることもあるが、悪意を持って故意に生み出されることもあります。通常、STPはループを検知してクローズすることになっており、結果として数秒間の障害が発生し、次いでパフォーマンスの低下が継続します。しかし、STPが誤って構成されたり、脅威アクターがその妨害に成功したりすることもあります。スイッチのストーム制御設定は、一定のしきい値を超えるブロードキャストトラフィックをレート制限するバックアップメカニズムです。

### BPDU (Bridge Protocol Data Unit)ガード

脅威アクターは不正なスイッチを使用して、またはスイッチの模倣を目的としたソフトウェアを使用して、STPへの攻撃を試みるかもしれません。特定の宛先MACアドレス向けのフレームを転送するために使用する正しいポートをスイッチが知らない場合（例えば、キャッシュが直前にフラッシュされた場合など）、そのスイッチはすべてのポートに宛先が未知のユニキャストフレームを転送します。STPのトポロジーを変更することで、スイッチがより頻繁にキャッシュをフラッシュし、ユニキャストトラフィックのすべてのポートへの転送をより頻繁に行う可能性が高まります。そのせいでネットワークのパフォーマンスに深刻な影響が生じ、スニッフィング攻撃をサポートすることもあります。

スイッチポートの構成は、クライアントデバイス向けに指定されたポート（アクセスポート）経由のSTPの使用を防止するものでなければなりません。アクセスポートは、STPの変更によりポートに接続しようとするとクライアント機器が遅延するのを防ぐために、portfastコマンドで設定します。それに加え、**BPDUガード**設定を適用する必要があります。それにより、BPDUを受信するportfast構成のポートが無効化されます（[cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2gx/configuration/guide/stp\\_enha.html](https://cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2gx/configuration/guide/stp_enha.html)）。BPDU (Bridge Protocol Data Unit)はトポロジー情報を交換するために使用されるものであり、アクセスポート上で受信することは想定されないので、BPDUガードは設定ミスや悪意ある攻撃からの防御となります。

### 物理ポートセキュリティとMACフィルタリング

不正なデバイスに起因するリスクや、パッチケーブルの正しくない設置によってループの生じる可能性があるために、物理スイッチポートやスイッチハードウェアへのアクセスは、セキュアなサーバールームやロック可能なハードウェアキャビネットを用いて、許可されたスタッフにのみ制限すべきです。セキュアでない壁のポートに不正なクライアントデバイスが接続されるのを防止するには、管理ソフトウェアを使用してウォールポートがケーブル接続するスイッチポートを無効にするか、またはパッチケーブルをポートから物理的に取り外すという方法があります。ただし、この方法でポートを完全に無効にした場合、管理上の負荷やエラーの可能性が増大するおそれがあります。また、脅威アクターは有効なポートからデバイスを取り外して自分のノートPCを接続することもできるため、完全な保護が提供されるわけではありません。このため、**ポートセキュリティ**を確保するためのより高度な手段が開発されてきました。

### MACフィルタリングとMAC制限

スイッチにおける**MACフィルタリング**の構成とは、どのMACアドレスに特定のポートへの接続を許可するかを定義することを意味します。これを行うには、有効なMACアドレスの一覧を作成するか、許可されるアドレス数の限度を指定します。例えば、ポートセキュリティがMACアドレス2つを上限として有効化されている場合、スイッチは最初の2つのMACを記録してそのポートに接続し、接続を試みている他のMACアドレスのマシンからのトラフィックをすべて拒否します（[cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw\\_book/lsw\\_m1.html](https://cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book/lsw_m1.html)）。これにより、MACフラッディング攻撃からの保護が提供されます。

### DHCPスヌーピング

もう1つの選択肢として、**DHCP (Dynamic Host Configuration Protocol)**スヌーピングを構成するというものがあります。DHCPは、クライアントをネットワークに接続する際に、サーバーがそのクライアントにIPアドレス情報を割り当てるようとするプロトコルです。DHCPスヌーピングは、アクセスポートに到着したこのトラフィックを検査し、ホストが自分のMACアドレスを偽装しようとしていないことを確認します。これは、不正な（または誤った）DHCPサーバーが

ネットワーク上で動作するのを防ぐためにも使用されます。DHCPスヌーピングにより、信頼できるものとして構成されたポートからのDHCPメッセージのみが許可されます。加えて、DHCPスヌーピングと共に構成できる動的ARP検査(DAI)というものがあり、信頼できないポートに接続されたホストが、不当なARPリプライをそのセグメントに大量に送りつけるのを防ぎます。DAIはIP ARPマッピングの信頼できるデータベースを保持しており、ARPパケットが有効に構築され、有効なIPアドレスを使用していることを保証します([cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html](http://cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html))。

```
NYCORE1>
NYCORE1#
*Mar 1 00:02:27.991: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 00:02:46.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
NYCORE1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NYCORE1(config)#ip arp inspection vlan 1,999
NYCORE1(config)#
*Mar 1 00:07:20.561: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/23, vlan 1.([0023.049
0.0000/192.168.16.21/00:07:20 UTC Mon Mar 1 1993])■
```

Ciscoスイッチ上のARP検査を構成する。

## ネットワークアクセス制御

エンドポイントセキュリティは、ネットワークアクセスをデバイスレベルで制限することを目的とした、一連のセキュリティ手順と技術です。エンドポイントセキュリティは、DMZなどのトポロジーや、ファイアウォールなどの技術によって確立される境界セキュリティへの着目と対照をするものです。エンドポイントセキュリティはそれらを置き換えるのではなく、多層防御を加えます。

IEEE 802.1X規格は、**PNAC (Port-based Network Access Control)**のメカニズムを定義するものです。PNACは、スイッチ（またはルーター）がAAAサーバーを使用して、ポートを有効化する前に接続されたデバイスを認証することを意味します。**ネットワークアクセス制御(NAC)**製品は認証範囲を拡大して、デバイスがネットワークアクセスを取得するために満たさなければならない最小限のセキュリティ構成を定めるデバイスピリシーまたはプロファイルを、管理者が策定できるようにします。これは正常性ポリシーと呼ばれます。一般的なポリシーでは、マルウェア感染、ファームウェアおよびOSのパッチレベル、パーソナルファイアウォールの状態、最新のウイルス定義の存在といった項目がチェックされます。また、レジストリのスキャンやファイルの署名の確認が解決策となることもあります。正常性ポリシーは、NAC管理サーバー上でレポートおよび構成ツールとともに定義されます。

**ポスマニアセメント**は、ホストがクライアントデバイスに対して正常性チェックを行い、正常性ポリシーの遵守を検証するプロセスです。ほとんどのNACソリューションはエージェントと呼ばれるクライアントソフトウェアを使用し、ウイルス対策やパッチの適用状態といったデバイスに関する情報、禁止されたアプリケーションの存在に関する情報、および正常性ポリシーによって定義された他のあらゆる事項に関する情報を集めます。

Id	Description	Actions	Target Role	Action		
				CLONE	DELETE	PREVIEW
defaults	Fingerbank Profiling	Reevaluate Access Action email_admin_action Log message	isolation	CLONE	DELETE	PREVIEW
1100001	Nessus Scan	Reevaluate Access Action email_admin_action Log message	registration	CLONE	DELETE	PREVIEW
1100002	OpenVAS scan	Reevaluate Access Action email_admin_action Log message	registration	CLONE	DELETE	PREVIEW
1100003	MAC Vendor isolation example	Reevaluate Access Action email_admin_action Log message	isolation	CLONE	DELETE	PREVIEW
1100004	Ancient OS isolation example	Reevaluate Access Action email_admin_action Log message	isolation	CLONE	DELETE	PREVIEW

Packet Fence Open Source NACでポリシー違反を定義する。  
(スクリーンショットは[packetfence.org](http://packetfence.org)からの許可を得て使用。)

エージェントは、クライアント上にソフトウェアアプリケーションとしてインストールされる永続的なものと、非永続的なものがあります。非永続的な（または溶解する）エージェントは、ポスマチャーアセスメントの際にメモリにロードされますが、デバイスにインストールされることはありません。

This section is for scanners, you will be able to configure scan engine and rules here.

**Scan Engine**

Name	Scan Engine
ADD SCAN ▾	Nessus Nessus 6 <b>OpenVAS</b> WMI

Packet Fenceは、NessusやOpenVASなどの脆弱性スキャナ、Windows Management Instrumentation (WMI) クエリ、ログ解析ツールを含む、いくつかのスキャニングテクニックの使用をサポートしています。  
(スクリーンショットは[packetfence.org](http://packetfence.org)からの許可を得て使用。)

NACソリューションの中には、エージェントレスのポスチャーアセスメントを行えるものもあります。これは、スマートフォン、タブレット、Internet of Things (IoT)デバイスなど、NACソリューションが幅広いデバイスをサポートしなければならない場合に有益ですが、エージェントレスソリューションではクライアントに関するより簡素な情報しか利用できません。

## ルートセキュリティ

ルートセキュリティに対する攻撃が成功すると、脅威アクターはトラフィックを本来の宛先からリダイレクトさせることができます。インターネット上では、脅威アクターがユーザーになりすましてサイトに誘導できるようになるかもしれません。企業ネットワークではファイアウォールやセキュリティゾーンの回避が容易になり、ラテラルムーブメントやデータ流出が可能になるでしょう。

ネットワーク間やサブネット間のルートは手動で構成することもできますが、ほとんどのルーターは互いに通信を行って、ルートを自動的に発見します。動的ルーターはルーティングプロトコルを用いてルートに関する情報を交換します。このトラフィックを、その他のタイプのデータに用いられるチャネルから切り離すことが重要です。ルーティングプロトコルが効果的で完全なセキュリティメカニズムを常に有しているわけではないので、アクセスが極めて厳格に制御されている環境でそれらを機能させる必要があります。

```
vyos@RT3-INT:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.1.253, eth1
B>* 10.1.0.0/24 [20/0] via 172.16.1.253, eth0, 00:10:25
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.16.0.252/30 [20/1] via 172.16.1.253, eth0, 00:10:25
C>* 172.16.1.252/30 is directly connected, eth0
C>* 192.168.1.0/24 is directly connected, eth1
C>* 192.168.2.0/24 is directly connected, eth2
vyos@RT3-INT:~$
```

静的構成や直接接続、BGP (Border Gateway Protocol)ルーティングプロトコルから得られたルートなどの異なるソースから取得されたルートを表すサンプルのルーティングテーブル。

ルーティングは多数の脆弱性の影響を受けますが、そこには次のようなものがあります。

- なりすまされたルーティングの情報（ルートインジェクション）— 認証がない、または弱い認証のルーティングプロトコルは、ルートテーブルポイズニングに対して脆弱です。これは、そのトラフィックが監視ポートに誤って導かれる（スニッフィング）、ブラックホール（実在しないアドレス）に送信される、またはネットワークを絶え間なくループしてDoSを引き起こす、といったことを意味します。ほとんどの動的ルーティングプロトコルは、各デバイス上で構成される共有共通鍵を介したメッセージ認証をサポートしています。しかし、それを管理するのは困難です。また通常は、どのピアからルート更新を受け入れるかをルーターが識別する方法も構成することができます。これにより、不正なルーターを単にシステムへ加えるのが難しくなります。脅威アクターは既存のルーターを侵害し、その構成を変更する必要に迫られるでしょう。
- ソースルーティング — これはIPヘッダー内のオプションを使用し、パケットがネットワーク内で辿る経路（ストリクト）や、パケットが通過しなければならない「経由地点」（ルーズ）を前もって定めることです。これはIPアドレスを偽装したり、ルーター/ファイアウォールファイラーを回避するために悪用することができます。ソースルーティングされたパケットをブロックするよう、ルーターを構成することができます。
- 基礎となるオペレーティングシステム内でのソフトウェアの悪用。ハードウェアルーター（およびスイッチ）にはオペレーティングシステムが組み込まれています。例えば、Ciscoのデバイスは通常、Internetwork Operating System (IOS)を使用しています。他のネットワークオペレーティングシステムに比べると、IOSなどでは悪用可能な脆弱性が少なくなっています。WindowsなどのコンピューターOSと比較して、攻撃対象領域が少なくなっているのです。



その一方で、SOHOプロードバンドルーターはパッチが適用されていないエクスプロイトに対して特に脆弱である場合があります。

# レビュー アク ティビティ：

## セキュアなスイッチングとルーティング

次の質問にお答えください。

1. ネットワークの偵察を行っている脅威アクターにとって、ARPポイズニングツールが有益なのはなぜですか？
2. 悪意のある脅威アクターが、標準スイッチポートに接続されたホストからスイッチングループを発生させるのを、あなたはどう防ぎますか？
3. ARPポイズニングを軽減するはどのポートセキュリティ機能ですか？
4. **dissolvable agent**とは何ですか？

# トピック9C

## セキュアなワイヤレスインフラ ストラクチャを実装する



### 対象試験範囲

- 1.4与えられたシナリオに基づいて、ネットワーク攻撃に関する可能性のあるインジケーターを分析することができます。  
3.4与えられたシナリオに基づいて、ワイヤレスセキュリティ設定をインストール、構成することができます。

ほとんどの組織には有線と無線（ワイヤレス）の両方のネットワークがあり、従業員が施設内を移動している際もアクセスできるようになっています。潜在的な脅威や脆弱性を理解することで、組織の情報システムインフラストラクチャのワイヤレス部分をしっかりと保護することができます。

### ワイヤレスネットワークの設置に関する検討事項

ワイヤレスネットワークの設置に関する検討事項とは、承認されたWi-Fiアクセスポイントの良好な可用性を保証する要素を指します。つぎはぎだらけのカバー範囲を持つネットワークは、不正なエビルツイン攻撃に対して脆弱です。



5GHzの周波数帯には、オーバーラップしていないチャネルを構成する空間がより多くあります。また、WAPはチャネルを結合して帯域幅を改善することもできますが、これは干渉のリスクを増大させます。

### WAP (Wireless Access Point)の配置

インフラストラクチャベースのワイヤレスネットワークは、1つ以上のワイヤレスアクセスポイントから構成されており、それぞれのアクセスポイントは有線ネットワークに接続されています。[アーキテクチャ](#)アクセスポイントは、有線ネットワークとの間でトラフィックを転送するものです。各WAPはMACアドレスによって識別されますが、そのアドレスは基本サービスセット識別子(Basic Service Set Identifier : BSSID)とも呼ばれます。各ワイヤレスネットワークはその名称、または[サービスセット識別子\(SSID\)](#)によって識別されます。

ワイヤレスネットワークは2.4GHzまたは5GHzの無線帯域で動作します。それでの無線帯域は多数のチャネルに分割され、各WAPは特定のチャネルを使用するよう構成する必要があります。パフォーマンス上の理由により、次に挙げるさまざまなタイプの干渉を減らすために、選択するチャネルの間隔はできるだけ広くしなければなりません。

- 同一チャネル干渉(CCI) —近接した2つのWAPが同じチャネルを使用する時、信号が衝突して再送信が必要となるために、それらWAPはそのチャネル内で帯域幅を求めて競合します。
- 隣接チャネル干渉(ACI) —チャネルは5MHz程度の間隔しかありませんが、Wi-Fiは20MHzのチャネルスペースを必要とします。WAP用に選択されたチャネルに十分な間隔がないと、干渉パターンによって多数の数のエラーと帯域幅の損失が発生します。例えば、それぞれの範囲内にある2つのアクセスポイントが、2.4GHz帯域においてチャネル1と6で構成されれば、それらは互いに重複しません。そこにチャネル3を使用する第3のアクセスポイントが追加されると、そのアクセスポイントは、他の2つのアクセスポイントが用いている周波数の一部を使用することになるので、3つのネットワークすべてが干渉してしまいます。

## サイト調査とヒートマップ

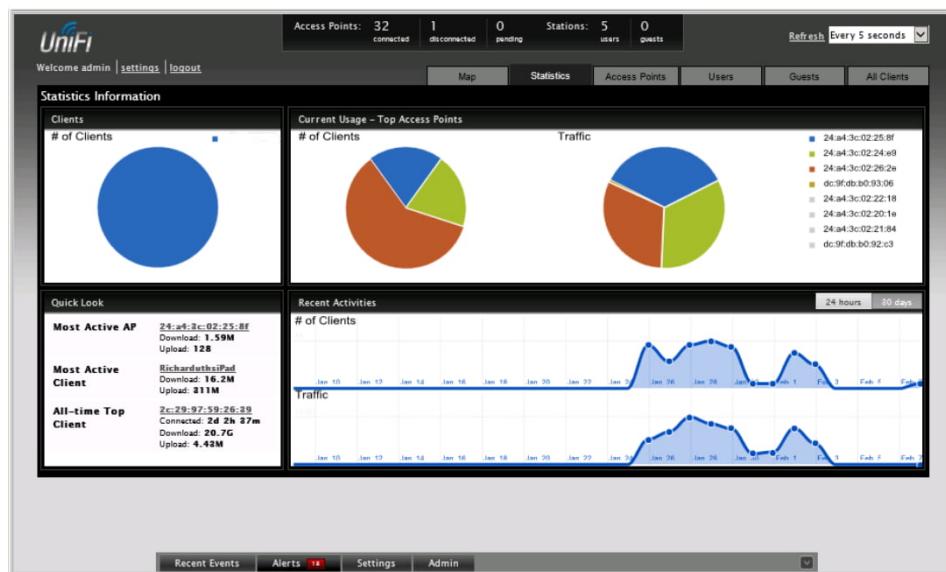
カバー範囲と干渉にまつわる諸々の要素とは、エリア全体がカバーされ、それでいて重複をできる限り少なくするよう、WAPを配置・構成しなければならない、ということを意味しています。サイト調査は、カバーすべきエリア全体の信号強度とチャネル使用を測定するために行われます。サイト調査は、その現場の建築図から始まりますが、そこにはバックグラウンド干渉の発生を指し示すいくつかの特徴が記されています。そうした特徴として、固体壁、反射面、モーター、電子レンジなどが挙げられます。調査は、Wi-Fiアナライザソフトウェアがインストールされた、Wi-Fi機能を持つラップトップやモバイル機器によって行われます。Wi-Fiアナライザは、調査員がエリア周辺を移動するのに合わせ、一定間隔の各ポイントで受信した信号に関する情報を記録します。

それらの結果を組み合わせて分析することで、ヒートマップが作成されます。ヒートマップは信号が強い場所（赤）と弱い場所（緑/青）、どのチャネルが使用されているか、およびどのように重複しているかを示します。次にこのデータは、送信出力を調整してWAPの範囲を狭める、WAPのチャネルを変更する、新たなWAPを追加する、またはWAPを新しい場所へ物理的に移動するといったことにより、設計を最適化するために用いられます。

## コントローラーとアクセスポイントのセキュリティ

サイト調査が可用性を保証するのに対し、ネットワークの機密性と完全性は、認証と暗号化を構成することで保証されます。そうした設定を手動で各WAPに構成することができますが、数十または数百のWAPを有する企業ネットワークでは大変な負担になります。アクセスポイントが個別に管理されている場合、これは設定エラーに結びつき、どのクライアントがどのアクセスポイントに接続されているか、あるいはどのクライアントまたはアクセスポイントが一番多くトラフィックを処理しているかといった、ワイヤレスデブロイの全体像を得るのが難しくなります。

企業ワイヤレスソリューションは各デバイスを個別に構成するのではなく、**ワイヤレスコントローラー**を実装して管理と監視を集中化しています。コントローラーはハードウェアアプライアンスであることもあれば、サーバー上で動作するソフトウェアアプリケーションであることもあります。



UniFi Wireless Networkの管理コンソール。  
(スクリーンショットはUbiquiti Networksからの許可を得て使用。)

ファームウェアに十分な処理論理が組み込まれていて、自律的に機能し、ワイヤレスコントローラーを使用することなくクライアントを処理できるアクセスポイントは、自律分散型（ファット、太った）WAPと呼ばれます。一方、機能させるためにワイヤレスコントローラーを必要とするアクセスポイントは集中管理型/軽量化（シン、痩せた）WAPと呼ばれます。

コントローラーとアクセスポイントは物理的に安全にする必要があります。それらを改ざんすることで、脅威アクターが不正なWAPやエビルツインWAPを挿入し、ログオンの傍受を試みることができるようになります。これらのデバイスは、セキュアな管理インターフェイスや強力な管理者認証情報を用いて、スイッチやルーターのように管理しなければなりません。

## Wi-Fi Protected Access

サイト設計と同じく、ワイヤレスネットワークはセキュリティ設定を伴って構成される必要があります。暗号化がなされないと、ワイヤレスネットワークを通過するパケットを、範囲内にいる全員が傍受して読み取れてしまいます。その選択は、さまざまなWi-Fiセキュリティ標準をサポートするデバイス、認証インフラストラクチャのタイプ、およびWLANの目的によって決定されます。セキュリティ標準は、サポートされている暗号プロトコル、暗号化キーを生成する方法、ネットワークに参加（またはアソシエート）しようとするときに、ワイヤレスステーションを認証するために利用可能な手段。

**WPA (Wi-Fi Protected Access)**の最初のバージョンは、初期の**WEP (Wired Equivalent Privacy)**標準における重大な脆弱性を是正することを目的としたものです。WEPと同じく、バージョン1のWPAはRC4ストリーム暗号を使用していますが、**TKIP (Temporal Key Integrity Protocol)**と呼ばれるメカニズムを追加して暗号を強化しています。

Personalize settings for each band or enable Smart Connect to configure the same settings for all bands.

OFDMA: <input checked="" type="checkbox"/> Enable <a href="#">?</a>	Sharing Network
Smart Connect: <input type="checkbox"/> Enable <a href="#">?</a>	
2.4GHz: <input checked="" type="checkbox"/> Enable	
Network Name (SSID): TP-Link_2200	<input type="checkbox"/> Hide SSID
Security: WPA/WPA2-Personal	
Version: WPA2-PSK	
Encryption: AES	
Password: tplinkpassword	
Transmit Power: High	
Channel Width: Auto	
Channel: Auto	
Mode: 802.11b/g/n mixed	
5GHz: <input checked="" type="checkbox"/> Enable	
Sharing Network	
Network Name (SSID): TP-Link_2200_5G	<input type="checkbox"/> Hide SSID
Security: WPA2/WPA3-Personal	
Version: WPA3-SAE	
Password: tplinkpassword	
Transmit Power: High	
Channel Width: Auto	
Channel: Auto	
Mode: 802.11ax only	

ワイヤレス暗号化と認証セッティングを用いてTP-LINK SOHOアクセスポイントを構成する。この例では、2.4GHz周波数帯においてはWPA2-Personalセキュリティによるレガシー接続が可能である一方、5GHzネットワークは、WPA3-SAE認証を用いる802.11ax (Wi-Fi 6)対応のデバイス向けになっています。（スクリーンショットはTP-Link Technologiesからの許可を得て使用。）

WEPもオリジナルバージョンのWPAも、継続的に使用できるほどセキュアであるとは考えられていません。WPA2は128ビットの鍵を有するAES (Advanced Encryption Standard)暗号アルゴリズムを使用しており、CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)と共にデプロイ (展開) されます。AESはRC4を、CCMPはTKIPを置き換えるものです。CCMPは認証された暗号化を提供しますが、その目的はリプレイ攻撃をより困難にすることです。

とは言えWPA2における脆弱性も発見されており、今後はWPA3に置き換えられることになります。WPA3の主な特徴は以下の通りです。

- **同等性同時認証(SAE: Simultaneous Authentication of Equals)** — ディフィー・ヘルマン鍵共有を基にしたプロトコルで、WPAの4ウェイハンドシェイク認証と接続メカニズムを置き換えるものです。
- オープン認証の強化(Enhanced Open) — オープン認証方式の暗号化を有効にします。
- 暗号プロトコルの更新 — **AES Galois Counter Mode Protocol (GCMP)**の動作モードで、AES CCMPを置き換えるものです。エンタープライズ認証方法が192ビットAESを使用しなければならないに対し、パーソナル認証は128ビットか192ビットのいずれかを使用できます。
- 管理フレームの保護(MFP: Management Frame Protection) — 鍵回復攻撃から保護するために、これらの使用を義務づけています。



Wi-Fiのパフォーマンスは、最新の802.11標準のサポートにも左右されます。最新世代(802.11ax)はWi-Fi 6として市場展開されています。以前の標準はこれを遡る形でWi-Fi 5 (802.11ac)およびWi-Fi 4 (802.11n)と命名されています。このパフォーマンス標準は、WPAセキュリティ仕様と平行して開発されたものです。ほとんどのWi-Fi 6デバイスと一部のWi-Fi 5およびWi-Fi 4製品は最初から、またはファームウェア/ドライバのアップデートを通じてWPA3をサポートしているはずです。

## Wi-Fi認証方法

ネットワークのセキュリティを確保するには、有効なユーザーだけが接続していることを確認できる必要があります。Wi-Fi認証は、パーソナル、オープン、エンタープライズの3種類に分かれます。またパーソナル認証のカテゴリーには、事前共有鍵認証(PSK)と同等性同時認証(SAE)の2つの方法があります。

### WPA2事前共有鍵認証

WPA2において、**事前共有鍵(PSK)**認証はパスフレーズを使用することで、通信の暗号化に用いられる鍵を生成します。ユーザーグループが同じ共通鍵を共有するので、これはグループ認証とも呼ばれます。アクセスポイントがWPA2-PSKモードにセットされている場合、管理者は8文字から63文字のASCII文字のパスフレーズを設定します。これは、PBKDF2鍵ストレッチアルゴリズムを用いて（64文字の16進値として表現される）256ビットのHMACに変換されます。このHMACはペアワイズマスターキー(PMK)と呼ばれます。アクセスポイントと、ネットワークに接続する各ノードには、同じ共通鍵を設定しなければなりません。PMKはさまざまなセッション鍵を導出するために、WPA2の4ウェイハンドシェイクの一部として使用されます。



すべての種類のWi-Fiパーソナル認証は、パスフレーズを標的とした辞書攻撃またはブルートフォース攻撃に対して脆弱であることが示されています。パスフレーズは最低でも14文字以上にして、クラッキングによるリスクを軽減させなければなりません。

## WPA3パーソナル認証

WPA3でもパスフレーズを使用してパーソナルモードのステーションの認証が行われますが、この共通鍵を用いてセッション鍵を共有する方法が変更されています。ここで用いられる仕組みは、パスワード認証鍵交換(Password Authenticated Key Exchange : PAKE)とも呼ばれます。WPA3では、さまざまな攻撃に対して脆弱であることが判明した4ウェイハンドシェイクに代わり、同等性同時認証(SAE)プロトコルが用いられます。SAEはDragonflyハンドシェイクを使用しますが、これは基本的に楕円曲線ディ菲ー・ヘルマン鍵共有であり、パスワードから導出されたハッシュ値とデバイスのMACアドレスを組み合わせてノードの認証を行います。SAEを使用すれば、脅威アクターがハンドシェイクをスニッフィングしてそのハッシュ値を取得し、オフラインのブルートフォース攻撃や辞書攻撃を用いてパスワードを発見しようと試みるのが不可能になります。Dragonflyは一時的（エフェメラル）なセッション鍵も組み込んでおり、前方秘匿性(forward secrecy)を提供します。



アクセスポイント用の構成インターフェイスは、これらのメソッドに対して異なるラベルを使用できます。例えば、WPA2-PSKおよびWPA3-Personalではなく、WPA2-PersonalおよびWPA3-SAEと表示されているかもしれません。加えて、アクセスポイントはWPA3専用に、またはレガシーWPA2をサポートするように（WPA3-Personal Transitionモード）構成することもできます。専門家はすでにWPA3-Personalにおける脆弱性を発見していますが、その1つに、ダウングレード攻撃によってWPA2を使用させるというものがあります([wi-fi.org/security-update-april-2019](https://wi-fi.org/security-update-april-2019))。

## Wi-Fi Protected Setup

アクセスポイントを安全に設定するのは、個人宅のコンシューマーにとっては比較的複雑なことから、各ベンダーは独自に**WPS (Wi-Fi Protected Setup)**と呼ばれる自動設定システムを開発しています。WPSを用いるには、アクセスポイントとワイヤレスステーション（クライアントデバイス）の両方がWPSに対応していなければなりません。通常、これらのデバイスにはプッシュボタンがあります。アクセスポイントとアダプターのボタンを同時に押すことで、PINを使用して両デバイスを関連付け、アダプターをWPA2を使用してアクセスポイントに関連付けることができます。このシステムはランダムなSSIDとPSKを生成します。デバイスがプッシュボタン方式をサポートしていない場合は、（WAPに印字されている）PINを手動で入力することができます。

残念なことに、WPSはブルートフォース攻撃に対して脆弱です。PINは8文字ですが、数字の1つはチェックサムで、残りの文字は4文字と3文字の個別の2つのPINとして認証されます。これら個別のPINにブルートフォース攻撃を仕掛けるのははるかに簡単であり、通常は1時間もあればクラックできます。また、管理者インターフェイスを介してWPSを無効にしても、実際にはプロトコルが無効化されていない、あるいはそれを無効化するオプションがないモデルもあります。ブルートフォース攻撃を検知した場合に侵入者を締め出せるAPもありますが、その有効期限が切れた後に攻撃を再開できるケースもあります。これに対抗するには、締め出し期限を延長します。しかしそのせいで、APがサービス拒否(DoS)攻撃に対して脆弱になります。WAPを設定する際は、WPSを安全に実行するためにベンダーがどのような対策を取っているかや、セキュリティを確保するのに必要なファームウェアのレベルを確認することが不可欠です。

WPA3と一緒に発表されたEasy Connect方式は、Wi-Fiネットワークへのアクセスに必要な情報と共にクライアントデバイスを安全に設定する手法として、WPSを置き換えることを目的としています。Easy ConnectはDevice Provisioning Protocol (DPP)のブランド名です。接続する各デバイスは、公開鍵と秘密鍵のペアで設定する必要があります。Easy ConnectはQRコードやNFCタグを用いて各デバイスの公開鍵を通信します。スマートフォンはEasy Connectコンフィギュレーターアプリとして登録されており、そのQRコードを用いてWAPと連携します。次に、コンフィギュレーターアプリでそのQRコードやNFCタグをスキャンすることで、各クライアントデバイスを連携させることができます。これはWPSにまつわるセキュリティ問題を解決するだけでなく、Wi-Fi接続可能なヘッドレスIoTデバイスを設定する簡単な方法となっています。



クイックレスポンス(QR)コードは、任意の英数字またはバイナリ文字列を正方形のブロックパターンの中にエンコードするバーコード標準です。このコードは、あらゆるタイプのデジタルカメラを用いてスキャンすることができます。

## オープン認証とキャプティブポータル

オープン認証を選択すると、クライアントを認証する必要がなくなります。このモードは、パブリックWAP（または「ホットスポット」）で使用されます。またWPA2では、これはリンクを介して送信されるデータが暗号化されないことを意味します。オープン認証は、ブラウザ経由で管理される二次的な認証メカニズムと組み合わせることができます。クライアントが公開ホットスポットに接続してブラウザを起動すると、**キャプティブポータル**またはスプラッシュページにリダイレクトされます。これによってクライアントは、ホットスポットプロバイダーのネットワークで認証されます（HTTPS経由であるためログインは安全です）。このポータルは、Wi-Fiサービスにアクセスするための利用条件を課したり、支払いを受けたりするように設計されていることもあります。

オープンワイヤレスを使用する場合、ユーザーは機密性のあるWebデータをHTTPS接続経由でのみ送信する必要があります、SSL/TLSが有効になっている電子メール、VoIP、IM、およびファイル転送サービスしか使用してはいけません。別のオプションとして、ユーザーが仮想プライベートネットワーク(VPN)に接続するというものがあります。ユーザーはまずオープンホットスポットに接続し、それからVPN接続を開始します。これにより、ユーザーのコンピューターとVPNサーバーの間に暗号化された「トンネル」が生成されます。そうすることで、誰かがオープンWi-Fiネットワーク上で盗聴を行い、通信を傍受できる恐れがない状態で、ユーザーはWebを閲覧したり、電子メールサービスに接続したりすることができます。ユーザーの所属する企業がVPNを提供することもあります、サードパーティのVPNサービスプロバイダーが利用されることもあります。当然、ユーザーはサードパーティを利用する際、それを暗黙のうちに信頼できる必要があります。VPNは認証ベースのトンネリングを使用して、「内部の」認証方法を設定しなければなりません。

WPA3ではWi-Fi Enhanced Openというモードを実装することができます。これはOWE(Opportunistic Wireless Encryption)を使用するものです。OWEはDragonflyハンドシェイクを用いることで、ネットワークへの参加に用いる一時的(エフェメラル)なセッション鍵を共有します。これは、各ステーションが異なるセッション鍵を使用しているために、あるステーションが別のステーションからのトラフィックをスニッフィングできないことを意味します。とは言え、アクセスポイントの認証はやはりありません。

## エンタープライズ/IEEE 802.1X認証

パーソナルモードの認証にまつわる主な問題点として、鍵またはパスフレーズの配布において適切に安全を確保することができず、ユーザーが安全でないフレーズを選んでしまう、というものがあります。また、すべてのユーザーが同じ鍵を共有するため、パーソナル認証はアカウントングを提供することができません。

パーソナル認証に代わるものとしてエンタープライズ認証方式があり、拡張認証プロトコル(EAP)メカニズムを使用するためにIEEE 802.1Xを実装しています。802.1XはEAP over Wireless(EAPoW)を使用することで、他のあらゆる種類のネットワークアクセスを許可することなく、アクセスポイントが認証データを転送できるようにするものです。これは、アクセスポイントのセキュリティ方式として、WPA2エンタープライズまたはWPA3エンタープライズを選択することで設定されます。

エンタープライズ認証においては、ワイヤレスステーションがアソシエーションをリクエストすると、WAPはEAPoWトラフィックのチャネルだけを有効化します。これはサブリカントの認証情報を、有線ネットワーク上のAAA (RADIUSまたはTACACS+) サーバーに転送して認証を行います。サブリカントが認証されると、AAAサーバーはサブリカントにマスターキー(MK)を送信します。するとサブリカントと認証サーバーは、そのMKから同じペアワイズマスターキー(PMK)を導出します。AAAサーバーはそのPMKをアクセスポイントに送信します。ワイヤレスステーションとアクセスポイントはそのPMKを使用し、WPA2の4ウェイハンドシェイクかWPA3のSAE方式を用いてセッション鍵を導出します。



使用される鍵についてより詳しく知るには、[tldp.org/HOWTO/8021X-HOWTO/intro.html](http://tldp.org/HOWTO/8021X-HOWTO/intro.html)を参照してください。