

3CX PBX VoIPソフトフォン上でSIP/TLSセキュリティを有効化する。
(スクリーンショットは3CXからの許可を得て使用。)

音声および映像の接続セキュリティは、HTTPSと同様に機能します。通話を始めるにあたり、セキュアなバージョンのSIPSはデジタル証明書を使用してエンドポイントを認証し、TLSトンネルを確立します。暗号化されていないSIPが通常TCPポート5060で動作するのに対し、SIPSはTCPポート5061を使用します。またSIPSによって確立されたセキュアな接続は、安全なバージョンのトランスポートプロトコル(**SRTP**)で使用されるマスターキーを生成するためにも使用されます。SRTPは実際の通話データに機密性を提供します。

Mitel PBXシステム上でRTPプロトコル暗号化を実行する。
(スクリーンショットはMitelからの許可を得て使用。)

レビュー アク ティビティ： セキュアなアプリケーションプロトコル

次の質問にお答えください。

1. サーバーに弱い暗号を取り決めるよう強制するのは、HTTPSに対するどのようなタイプの攻撃ですか？
2. クライアントとサーバーは、TLSセッションに暗号スイートECDHE-ECDSA-AES256-GCM-SHA384を用いることで合意しました。対称暗号化アルゴリズムの主な強みは何ですか？
3. SFTPが接続を保護するために使用するセキュリティプロトコルは何ですか？SFTPサーバーはデフォルトでどのポートをリッスンしますか？
4. SMTPサーバーによって配達されるメッセージを送信するにあたり、メールクライアントはどのポートとセキュリティ方式を使用すべきですか？
5. S/MIMEを使用する際、メッセージを暗号化するために用いられるのはどの鍵ですか？
6. VoIPの会話内容が盗聴されるのを防ぐのはどのプロトコルですか？

トピック11C

セキュアなリモートアクセス プロトコルを実装する



対象試験範囲

- 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。
- 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ます。
- 4.1 与えられたシナリオに基づいて、適切なツールを利用して組織のセキュリティを評価することができます。（SSHのみ）

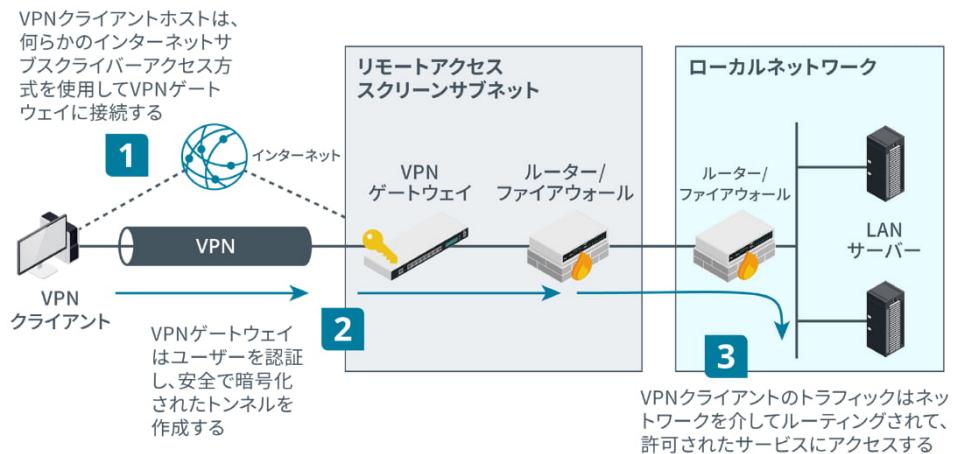
モバイルワークが普及した今日、大半のネットワークは、離れた場所にいる従業員、請負業者、顧客が自身のネットワークリソースにアクセスするのをサポートする必要があります。多くの場合、これらのリモート接続ではインターネットなど信頼できない公共ネットワークが使用されます。結果として、セキュアなリモートアクセスプロトコルをどのように実装するかを理解することが、情報セキュリティのプロフェッショナルであるあなたの業務の主要な一部になるでしょう。

また、ユーザーが個々のホストにリモートでアクセスする必要があるケースも多くあります。これは、管理者がワークステーション、サーバー、ネットワークアプライアンスをリモートで管理できるようにするために最も一般的に実装されていますが、一般ユーザーにデスクトップへのアクセスを提供する目的でも用いられます。

リモートアクセスアーキテクチャ

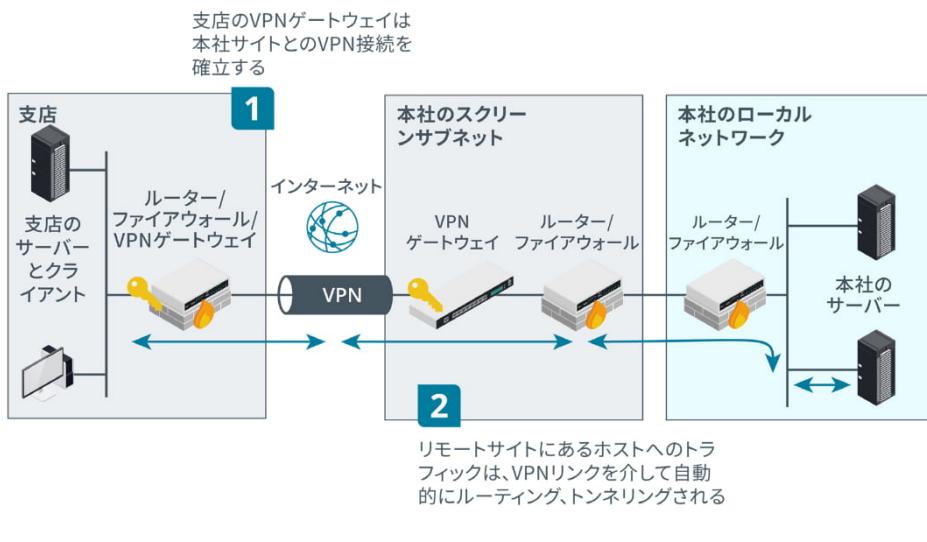
リモートアクセスとは、ユーザーのデバイスが有線または無線で直接ネットワークに接続しないことを意味します。接続は中間ネットワーク上で、またはそれを経由して行なわれます。歴史的に見ると、リモートアクセスでは電話システムや、おそらくはプライベートリンク（リース回線）に接続するアナログモデムが使用されてきました。今日、大半のリモートアクセスはインターネット上で動作する**仮想プライベートネットワーク(VPN)**として実装されています。リモートアクセスの管理には、ローカルネットワークの管理と本質的に同じタスクが含まれます。許可されたユーザーだけがローカルネットワークリソースと通信チャネルへのアクセスを許可されるようにしなければなりません。リモートワークステーションやサーバーのセキュリティを確保することはさらに難しく、リモートログインが悪用される可能性も高いために、別の複雑性が生じます。

リモートアクセスVPNを用いることで、クライアントはプライベートネットワークのエッジ上にあるVPNゲートウェイに接続します。これは「テレコミューター」モデルと呼ばれるもので、ホームワーカーや現場で働く従業員が企業ネットワークに接続するのを可能にします。VPNプロトコルはセキュアな**トンネル**を確立し、パケットがISPのルーターを通過する場合でも、コンテンツの秘密が保たれます。



リモートアクセスVPN。(画像提供: © 123RF.com)

VPNはサイト間モデルでもデプロイされ、2つまたはそれ以上のプライベートネットワークを接続できます。リモートアクセスVPN接続が通常クライアントによって開始されるのに対し、site-to-site VPNは自動的に動作するよう構成されます。ゲートウェイはVPNの基礎となるプロトコルを用いてセキュリティ情報を交換します。これによってゲートウェイ間に信頼関係が確立され、データをトンネリングするセキュアな接続が構築されます。各サイトのホストは、VPNに関する情報で構成する必要がありません。また各サイトのルーティングインフラストラクチャは、トラフィックをローカルで配達するか、VPNトンネルで送信するかどうかを決定します。



Site-to-Site VPN。(画像提供: © 123RF.com)

トランスポートレイーセキュリティ VPN

長年使用されてきたVPNプロトコルがいくつかあります。Point-to-Pointトンネリングプロトコル(PPTP)などのレガシープロトコルは、十分なセキュリティを提供しないためにあまり使用されなくなっています。VPNを構成するにあたり、現在ではトランスポートレイーセキュリティ(TLS)やIPSecの方が選択肢として好まれています。

General Information

- Disabled:** Disable this server
Set this option to disable this server without removing it from the list.
- Server mode:** Remote Access (SSL/TLS + User Auth)
- Backend for authentication:** Classroom AD (selected)
- Protocol:** UDP
- Device mode:** tun
- Interface:** WAN
- Local port:** 1194
- Description:** Classroom AD VPN
A description may be entered here for administrative reference (not parsed).

Cryptographic Settings

- TLS authentication:** Enable authentication of TLS packets.
- Peer Certificate Authority:** Classroom CA

pfSenseセキュリティアプライアンス内でOpenVPNサーバーを構成する。
(スクリーンショットはRubicon Communications, LLC.からの許可を得て使用。)

TLS VPN（依然としてSSL VPNと呼ばれることが多い）は、ポート443（または任意のポート番号）を使用するリモートアクセスサーバーを必要とします。クライアントはTLSを用いてサーバーに接続を行い、それによってサーバーのクライアントへの接続を認証します（また、クライアントの証明書をサーバーが認証するオプションもあります）。これにより、ユーザーが認証情報を送信する暗号化されたトンネルが生成され、通常はRADIUSサーバーによって処理されます。ユーザーが認証されて接続が完全に確立されると、VPNゲートウェイはセキュアなソケット経由でローカルネットワークへのすべての通信をトンネリングします。

User Authentication Settings	
Username	<input type="text" value="Bobby"/> Leave empty when no user name is needed
Password	<input type="password" value="*****"/> Leave empty when no password is needed <input type="password" value="*****"/> Confirm
Cryptographic Settings	
TLS authentication	<input checked="" type="checkbox"/> Enable authentication of TLS packets. <input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
Peer Certificate Authority	<input type="text" value="Classroom VPN CA"/>
Client Certificate	<input type="text" value="Classroom VPN User (CA: Classroom VPN CA)"/>
Encryption Algorithm	<input type="text" value="AES-128-CBC (128 bit key, 128 bit block)"/>
Auth digest algorithm	<input type="text" value="SHA1 (160-bit)"/> Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.
Hardware Crypto	<input type="text" value="No Hardware Crypto Acceleration"/>

pfSenseセキュリティアプライアンス内で、相互認証に用いるクライアントの証明書を構成する。
(スクリーンショットはRubicon Communications, LLCからの許可を得て使用。)



ポートはTCPかUDPのいずれかです。特に音声や映像などレイテンシーに影響を受けやすいトラフィックをトンネリングする際に、パフォーマンスがわずかに優れているUDPが選ばれる傾向があります。デフォルトのファイアウォールポリシーではTCPの方が使用しやすいでしょう。UDPを介したTLSはデータグラムTLS(DTLS)とも呼ばれます。

OpenVPNはオープンソースのTLS VPNの一例です(openvpn.net)。OpenVPNはTAP（ブリッジ）モードで動作して第2層フレームをトンネリングするか、TUN（ルート）モードで動作してIPパケットを転送します。別のオプションとしてMicrosoftの**Secure Socketトンネリングプロトコル(SSTP)**があり、Point-to-Pointプロトコル(PPP)の第2層フレームをTLSセッションでトンネリングします(docs.microsoft.com/en-usopenspecs/windows_protocols/ms-sstp/70adc1df-c4fe-4b02-8872-f1d8b9ad806a)。Point-to-Pointプロトコル(PPP)は幅広く使用されているリモートダイヤルインプロトコルです。これは広くサポートされているチャレンジハンドシェイク認証プロトコル(CHAP)を介して、IPトラフィックのカプセル化に加え、IPアドレス割り当てと認証を行います。

インターネットプロトコルセキュリティ

トランスポート・レイヤー・セキュリティは、独立したセキュアポートを使用するか、アプリケーション・プロトコルのコマンドを使用してセキュアな接続をネゴシエートすることにより、アプリケーションレベルで適用されます。インターネットプロトコルセキュリティ(IPSec)はOSIモデルのネットワークレイヤー（第3層）で機能するので、特定のアプリケーションを構成することなく実装できます。IPSecは（データパケットを暗号化することで）機密性と、（各パケットに署名することで）完全性およびアンチリプレイの両方をもたらします。主な欠点は、データ通信にオーバーヘッドが加わることです。IPSecはローカルネットワーク上の通信を保護するために、またリモートアクセスプロトコルとして使用できます。



IPv6の策定が進められていた際、新しいプロトコルを介したすべてのトラフィックはセキュアであるべきだと考えられていたので、IPSecは必須のコンポーネントと見られていました。近年RFCが改正されたため、現在ではIPSecがIPv6向けに推奨されていますが、必須ではなくなりています(tools.ietf.org/html/rfc6434#page-17)。

IPSecを用いる各ホストにはポリシーを割り当てる必要があります。IPSecポリシーは認証メカニズムを設定し、また接続のプロトコルとモードも設定します。ホスト間で接続を確立するために、少なくとも1つの一致するセキュリティ方式が存在しなければなりません。IPSecには2つの中核プロトコルがあり、ポリシーに応じて1つだけ、または両方を適用できます。

認証ヘッダー(AH)

認証ヘッダー(AH)プロトコルは、IPヘッダーを含むパケット全体、および（通信を行うホストしか知らない）共有共通鍵に暗号ハッシュ化を行い、そのHMACを完全性チェック値(ICV)としてヘッダーに追加します。受信者はそのパケットと鍵に対して同じ関数を実行し、同じ値を導出してパケットが改変されていないことを確認するはずです。ペイロードは暗号化されていないので、このプロトコルは機密性を提供しません。また、ICVにIPヘッダーフィールドが含まれているので、IPアドレスが書き換えられるため、NATゲートウェイを通過するとチェックが失敗します。結果として、AHが使用されることはありません。



AHを使用するIPSecデータグラム – ペイロードとIPヘッダーの完全性は完全性チェック値(ICV)によって保証されますが、そのペイロードは暗号化されません。

カプセル化セキュリティペイロード(ESP)

カプセル化セキュリティペイロード(ESP)は機密性、認証、完全性を提供します。これは単にHMACを計算するだけでなく、パケットを暗号化するために用いられます。ESPはパケットにヘッダー、トレイラー（暗号関数にパディングを与えます）、そして完全性チェック値の3つのフィールドを付与します。AHと違い、ESPはICVを計算する際にIPヘッダーを除外します。



ESPを使用するIPSecデータグラム – 元のパケットのTCPヘッダーとペイロードはESPの中にカプセル化され、機密性を提供するために暗号化されます。



ESPでは通常、機密性（対称暗号）のアルゴリズムと認証/完全性（ハッシュ関数）のアルゴリズムが一緒に適用されます。とは言え、片方だけを使用することも可能です。

IPSecのトランSPORTモードとトンネルモード

IPSecは2つのモードで使用できます。

- トランSPORTモード – このモードは、プライベートネットワーク上の各ホスト間の通信を保護するために使用されます（エンドツーエンドの実装）。ESPがトランSPORTモードで適用されると、各パケットのIPヘッダーは暗号化されず、ペイロードデータだけが暗号化されます。AHがトランSPORTモードで使用されている場合、IPヘッダーの完全性を提供します。



AHとESPをトランSPORTモードで使用するIPSecデータグラム。

- トンネルモード – このモードはセキュアでないネットワークを経由したVPNゲートウェイ間で行われる通信に使用されます（VPNを生成します）。これはルーター実装とも呼ばれます。ESPの場合、IPパケット全体（ヘッダーとペイロード）が暗号化され、新しいIPヘッダーを持つデータグラムとしてカプセル化されます。通常は機密性が必要となるため、AHにはトンネルモードにおける実際の使用例がありません。



ESPをトンネルモードで使用するIPSecデータグラム。

The screenshot shows the pfSense IPsec configuration interface under the 'Mobile Clients' tab. The 'Edit Phase 2' screen is displayed. The 'General Information' section is set to 'Disabled'. The 'Mode' is set to 'Tunnel IPv4'. The 'Local Network' is set to 'Network' with address '0.0.0.0 / 0'. The 'NAT/BINAT translation' is set to 'None'. The 'Protocol' is set to 'ESP'. A note at the bottom states 'ESP is encryption, AH is authentication only.'

pfSenseセキュリティアプライアンス内で、ESP暗号化によってIPSecトンネルを構成する。
(スクリーンショットはRubicon Communications, LLCからの許可を得て使用。)



IPSecの根底にある原則は、IPv4とIPv6で同じですが、ヘッダーのフォーマットが異なっています。IPv6ではIPSecが拡張ヘッダーを使用するのに対し、IPv4においてはESPとAHに新規のIPプロトコル番号（50と51）が割り当てられ、トранSPORTモードとトンNELモードのどちらが用いられるかに応じて、元のIPヘッダーを修正するか、元のパケットをカプセル化します。

インターネット鍵交換

IPSecの暗号化とハッシュ化関数は、共有共通鍵に依存しています。双方のホストが共通鍵をやり取りし、互いの身元を確かめる必要があります（相互認証）。そうでない場合、その接続は中間者攻撃やスプーフィング攻撃に対して脆弱です。インターネット鍵交換(IKE)プロトコルは、セキュリティアソシエーション(SA)と呼ばれる認証と鍵交換を扱います。

Phase 1 Proposal (Authentication)	
<u>Authentication Method</u>	Mutual RSA Must match the setting chosen on the remote side.
<u>My identifier</u>	My IP address
<u>Peer identifier</u>	Peer IP address
<u>My Certificate</u>	Classroom VPN Select a certificate previously configured in the Certificate Manager.
<u>Peer Certificate Authority</u>	Classroom VPN CA Select a certificate authority previously configured in the Certificate Manager.

Phase 1 Proposal (Algorithms)	
<u>Encryption Algorithm</u>	AES 256 bits
<u>Hash Algorithm</u>	SHA1 Must match the setting chosen on the remote side.
<u>DH Group</u>	2 (1024 bit) Must match the setting chosen on the remote side.
<u>Lifetime (Seconds)</u>	28800

pfsenseセキュリティアプライアンス内でIKEを構成する。
(スクリーンショットはRubicon Communications, LLCからの許可を得て使用。)

IKEのネゴシエーションは次の2つのフェーズで行われます。

- フェーズIは2つのホストの身元を確立し、ディフィー・ヘルマンアルゴリズムを用いて鍵合意を行い、セキュアなチャネルを生成します。ホストを認証するにあたっては、次の2つの方法が一般的に用いられています。
 - デジタル証明書 – 両ホストは、双方に信頼されている認証局が発行した証明書を使って互いを識別します。
 - 事前共有鍵（グループ認証） – 両方のホストに同じパスフレーズが設定されます。
- フェーズIIはフェーズIで生成されたセキュアなチャネルを使用し、IPSecセッションにおいてAHやESPでの暗号アルゴリズムと鍵サイズを使用するかを決定します。

レイヤー 2トンネリングプロトコルとIKE v2

IKEの最初のバージョンは、サイト間VPNなど、2つのピアホストの相互認証を保証するよう最適化されています。それ自体は、クライアントのユーザー アカウントがリモートネットワークディレクトリに認証を行う単純な手段を提供するものではありません。結果としてリモートアクセスVPNには、IPSecとレイヤー 2トンネリングプロトコル(**L2TP**) VPNプロトコルの組み合わせがしばしば用いられます。

レイヤー 2トンネリングプロトコル/IPSec VPN

通常、L2TP/IPsec VPNは次のように機能します。

1. クライアントとVPNゲートウェイが、事前共有鍵またはIKE用の証明書を用いてインターネット上でセキュアなIPSecチャネルを構築する。
2. VPNゲートウェイがL2TPを用いてトンネルを構築し、Point-to-Pointプロトコル(PPP)フレームとしてカプセル化されたローカルネットワークデータを交換する。こうしたトラフィックの二重カプセル化によるオーバーヘッドの増加が、主な欠点となっています。
3. ユーザーがEAPまたはCHAPを用いてPPPセッションで認証を行う。

IKE v2

IKEの最初のバージョンにおける欠点は、アップデートされたプロトコルによって対処されました。IKE v2にはいくつかの追加機能があり、スタンダードアロンのリモートアクセスVPNソリューションとして使用される人気のあるプロトコルになっています。主な変更点は次のとおりです。

- EAP認証方式をサポートしており、RADIUSサーバーに対するユーザー認証などを可能にしています。
- 単純化された接続セットアップ – IKE v2はシングル4メッセージセットアップモードを規定しており、セキュリティを損なうことなく帯域幅を削減しています。
- 信頼性 – IKE v2ではNATトラバーサルとMOBIKEマルチホーミングが可能です。マルチホーミングとは、スマートフォンをはじめ、複数のインターフェイス (Wi-Fiと携帯電話など) を持つクライアントがインターフェイス間で切替えを行っても、IPSec接続を維持できることを意味します。

L2TP/IPSecに比べ、IKE v2を使用した方が効率的です。このソリューションはさらに幅広くサポートされつつあり、Windows 10ではネイティブサポートになっています。

VPNクライアント構成

VPNクライアントを構成するにあたり、OSがネイティブでそのVPNのタイプをサポートしていないければ、クライアントソフトウェアをインストールする必要がある場合があります。例えば、OpenVPNはクライアントのインストールを必要とします。そしてVPNゲートウェイのアドレス、VPNプロトコルのタイプ（自動検知できない場合）、ユーザー名、アカウントの認証情報でクライアントを構成します。また、VPNコンセントレータによって信頼されるクライアントの証明書をそのマシンにデプロイし、VPNクライアントが利用できるようにする必要もあるでしょう。それに加えて、VPN接続の運用方法に関しても設定する必要があります。

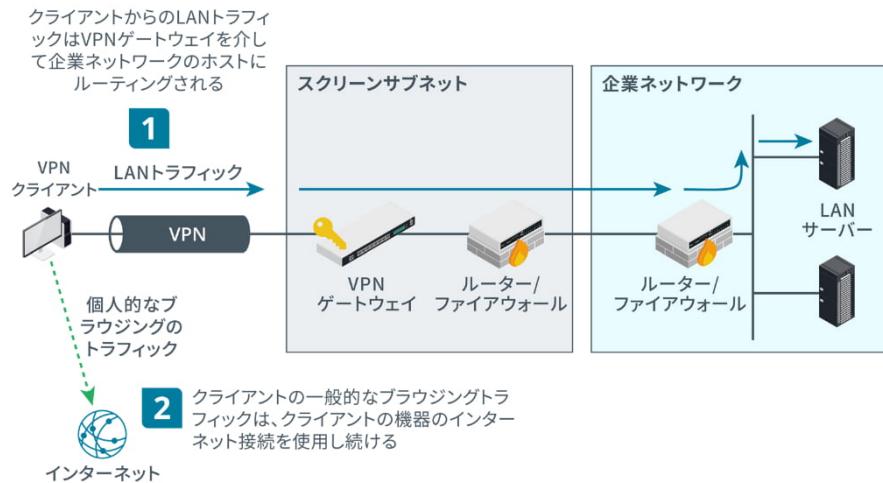
Always-On VPN

伝統的なリモートアクセスVPNソリューションでは、ユーザーが接続を開始して認証情報を入力する必要があります。Always-on VPNは、信頼できるネットワーク経由のインターネット接続が検知されるたびに、キャッシュされているユーザーの認証情報を用いてコンピューターがVPNを確立することを意味します。MicrosoftはWindows ServerとWindows 10クライアント向けのAlways-On VPNを用意しており(docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn-always-on-vpn/deploy/always-on-vpn-deploy-deployment)、自動接続するようにOpenVPNクライアントを構成することができます(openvpn.net/vpn-server-resources/setting-your-client-to-automatically-connect-to-your-vpn-when-your-computer-starts)。

スプリットトンネルとフルトンネル

リモートアクセスVPNに接続しているクライアントがインターネット上の他のサイトへのアクセスを試みる際、その接続を管理する2つの方法があります。

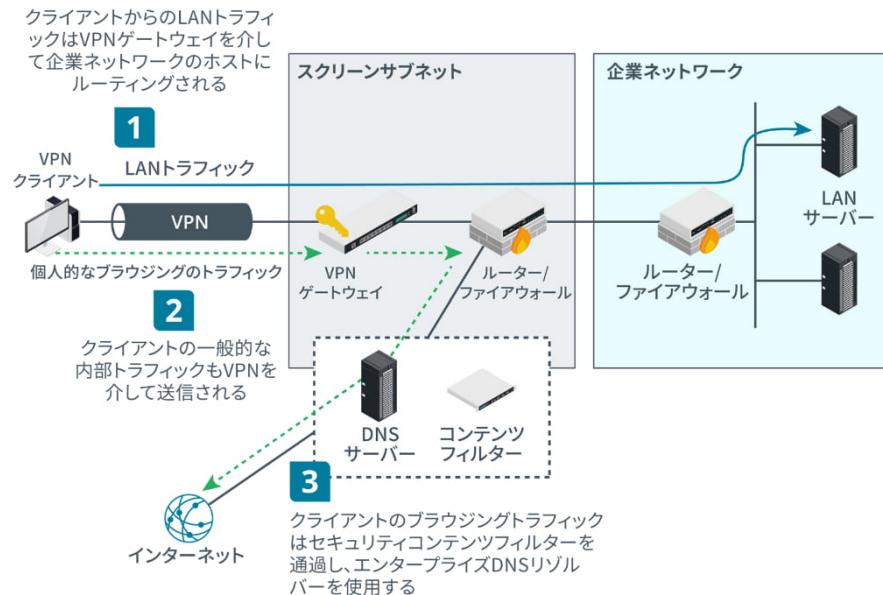
- **スプリットトンネル** – クライアントはその「ネイティブ」IP構成とDNSサーバーを用いてインターネットに直接アクセスします。



スプリットトンネルのVPNトラフィックフロー。(画像提供: © 123RF.com)

- **フルトンネル** – インターネット接続は企業ネットワークによって仲介され、クライアントのIPアドレスとDNSサーバーを変更し、場合によってはプロキシを使用します。

フルトンネルの方が優れたセキュリティを提供しますが、必要となるネットワークアドレス変換とDNSの作動のために、特にクラウドサービスなど、一部のWebサイトに関する問題が発生します。それはまた、より多くのデータがVPNリンク経由で伝送されることを意味します。



フルトンネルのVPNトラフィックフロー。(画像提供: © 123RF.com)

リモートデスクトップ

リモートアクセスVPNは、ユーザーのPCまたはスマートフォンをセキュアなトンネル経由でローカルネットワークに接続します。リモートネットワーク接続のもう1つのモデルとして、リモート管理プロトコルによってローカルネットワーク内のホストに接続するというものがあります。Secure Shell (SSH)などのプロトコルは端末アクセスだけをサポートしていますが、グラフィカルデスクトップに接続できるその他のツールが多数あります。GUIリモート管理ツールは、リモートホストからの画面と音声データをクライアントに送信し、マウスとキーボードの入力をクライアントからリモートホストに転送します。

Microsoftの**リモートデスクトッププロトコル(RDP)**を使用することで、物理的なマシンに1対1ベースでアクセスできます。それとは別に、ネットワークサーバー上で動作している仮想デスクトップまたは個別のアプリへのアクセスを可能にするリモートデスクトップゲートウェイを、サイトが運用することもできます(docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds)。リモートデスクトップに代わる選択肢として、人気のあるものがいくつかあります。その大半はWindows以外のプラットフォーム（macOSとiOS、Linux、Chrome OS、Androidなど）へのリモートアクセスをサポートしています。その例としてTeamViewer (teamviewer.com/en)や**仮想ネットワークコンピューティング(VNC)**があり、複数のプロバイダーによって実装されています（特にrealvnc.com/enが有名）。

伝統的に、これらのリモートデスクトップ製品はクライアントアプリを必要とします。HTML5で導入されたcanvas要素は、ブラウザーが比較的短い遅延でデスクトップを描写し更新できるようにしています。また音声も扱うことができます。これは**HTML5 VPN**またはクライアントレスリモートデスクトップゲートウェイと呼ばれています(guacamole.apache.org)。またこのソリューションはWebSocketと呼ばれるプロトコルを使用しており、個別のHTTPリクエストのオーバーヘッドを必要とすることなく、サーバーとクライアント間での双方向メッセージの送信を可能にしています。

アウトオブバンド管理とジャンプサーバー

リモートアクセス管理とは、セキュアなチャネルを使用してネットワークアプライアンスまたはサーバーを管理する具体的な使用例を指します。管理機能を実行するために用いるセキュア管理ワークステーション(SAW)は厳重に隔離する必要があります、管理チャネルへのアクセスに必要なソフトウェア（最小限のWebブラウザー、リモートデスクトップクライアント、またはSSH仮想端末など）以外はできればインストールしてはいけません。SAWはインターネットへのアクセスを禁止するか、あるいは少数の承認されたベンダーサイト（パッチ、ドライバ、サポート入手するため）へのアクセスに制限すべきです。また、このデバイスは厳格なアクセス制御と監査の対象とし、悪用を可能な限り早期に検知できるようにする必要があります。

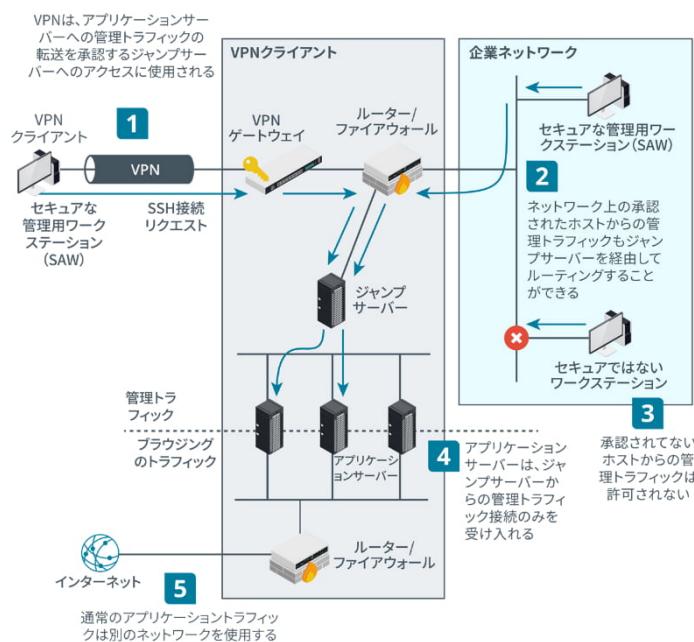
アウトオブバンド管理

リモート管理の方式は、インバンドまたは**アウトオブバンド(OOB)**のいずれかとして説明されます。インバンド管理リンクは、「プロダクション（本番稼働中の）」ネットワーク上の他の通信のトラフィックを共有するものです。シリアルコンソールやルーターのモデムポートは物理的にアウトオブバンドの管理方式となります。イーサネットとIPを介してブラウザベースの管理インターフェイスや仮想端末を使用している際、管理アクセスに用いるポートを物理的に分離されたネットワークインフラストラクチャへ接続することで、リンクをアウトオブバンドにすることができます。これを実装するのはコストがかさみますが、アウトオブバンド管理の方が安全であり、プロダクションネットワークに影響を及ぼす問題が発生した際も、デバイスへのアクセスが維持されます。インバンド接続では、VLANを用いて管理トラフィックを隔離することにより、よりよいセキュリティを実装することができます。これにより、管理インターフェイスを通過するトラフィックを傍受者が閲覧したり改変したりするのが難しくなります。とは言え、この種類の仮想OOBであっても、システム全体にわたるネットワーク障害によってアクセスが損なわれる可能性があります。

ジャンプサーバー

DMZやクラウドバーチャルネットワークなど、インターネットに接続しているホストを管理する課題の1つに、その中に位置しているサーバーやアプライアンスへの管理用のアクセスを提供するというものがあります。一方ではリンクが必要であり、他方では管理インターフェイスがネットワークの残りの部分への拠点として侵害されたり悪用される可能性があります。結果として、安全なゾーン内の各ホストの管理用インターフェイスへのアクセスが許可されている管理ホストは、厳重にコントロールする必要があります。ゾーンの中で多種多様なサーバーが動作している場合、このタイプのコントロールの構成と監査は複雑になります。

この複雑性に対するソリューションの1つに、単一の管理サーバー、または**ジャンプサーバー**をセキュアなゾーンに追加するというものがあります。ジャンプサーバーは必要な管理用ポートとプロトコル（通常はSSHまたはRDP）だけを動作させます。管理者はまずジャンプサーバーに接続し、それからジャンプサーバーを用いてアプリケーションサーバー上の管理インターフェイスに接続します。アプリケーションサーバーの管理インターフェイスには、ACL（ジャンプサーバー）の中にエントリーが1つだけあり、その他のすべてのホストによる接続の試みを拒否します。

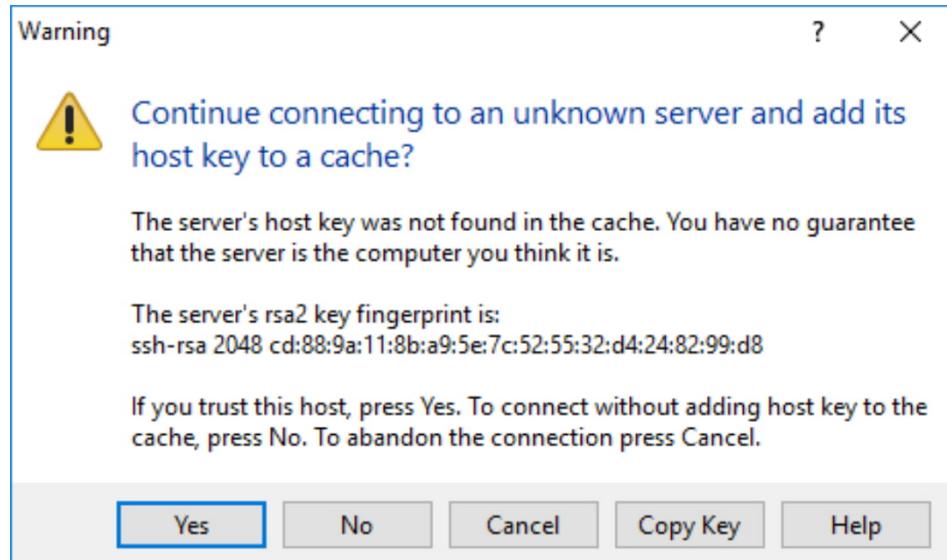


ジャンプサーバーを用いて管理トラフィックを保護する。

Secure Shell

Secure Shell (SSH)は、コマンドライン端末へのセキュアなリモートアクセスを取得する主要な手段です。SSHの主な使用例として、リモート管理やセキュアファイル転送(SFTP)があります。主要なNOSプラットフォームで使用できるように、さまざまな商用およびオープンソースのSSH製品が提供されています。その中最も幅広く使用されているのがOpenSSH (openssh.com)です。

SSHサーバーは、公開鍵と秘密鍵のペア（ホスト鍵）によって識別されます。ホスト名の公開鍵へのマッピングは、各SSHクライアントで手動で保持することができます。またSSHホスト鍵管理用に設計されたエンタープライズソフトウェア製品も多数存在します。



PuTTY SSHクライアントを用いてSSHサーバーのホスト鍵を確認する（スクリーンショットはPuTTYからの許可を得て使用）。



ホストの侵害が疑われる場合、ホスト鍵を変更しなければなりません。サーバーまたはアプライアンスの秘密鍵を取得した脅威アクターは、そのサーバーまたはアプライアンスを装い、通常は他のネットワークの認証情報を取得する目的で中間者攻撃を実行できます。

サーバーのホスト鍵は、クライアントが認証資格情報を送信するための、セキュリティで保護されたチャネルを確立するために使用されます。

SSHクライアント認証

SSHは、クライアントとSSHサーバー間の通信に対してさまざまな認証方法をサポートしています。以下の認証方法は、/etc/ssh/sshd_configファイルを用いることで、サーバー上で必要に応じて個々に有効または無効にすることができます。

- ユーザー名/パスワード – クライアントが提示した認証情報は、SSHサーバーによって、ローカルユーザーデータベースまたはRADIUS/TACACS+サーバーを使用して検証されます。
- 公開鍵認証 – 各リモートユーザーの公開鍵が、SSHサーバー上の各ローカルアカウントに許可された鍵のリストに追加されます。
- Kerberos – クライアントは、ユーザーがワークステーションにログオンした際に取得したKerberos認証情報(Ticket Granting Ticket)を、GSSAPI (Generic Security Services Application Program Interface)を使用してサーバーに送信します。SSHサーバーはTicket Granting Service (Windows環境ではドメインコントローラー) にコンタクトしてその認証情報を検証します。



有効なクライアント公開鍵を管理することは、極めて重要なセキュリティタスクです。近年のWebサーバーへの攻撃の多くは、ずさんな鍵管理に原因があることが判明しています。ユーザーの秘密鍵が侵害された場合は、アプライアンスから公開鍵を消去した上で、ユーザーの（修復された）クライアントデバイス上で鍵のペアを再度生成し、公開鍵をSSHサーバーにコピーしてください。またユーザーのアクセス許可が取り消された場合は、必ず公開鍵を消去してください。

SSHコマンド

SSHコマンドは、ホストに接続して認証方法をセットアップするために使用されます。アカウント名「bobby」とパスワード認証を用いて10.1.0.10のSSHサーバーに接続するには、以下のコマンドを実行します。

```
ssh bobby@10.1.0.10
```

次のコマンドは新しい鍵ペアを生成し、それをリモートサーバー上のアカウントにコピーします。

```
ssh-keygen -t rsa
```

```
ssh-copy-id bobby@10.1.0.10
```

SSHプロンプトで、標準のLinuxシェルコマンドを使用することができます。exitを用いて接続を閉じます。

またscpコマンドを使用して、リモートサーバーからローカルホストにファイルをコピーできます。

```
scp bobby@10.1.0.10:/logs/audit.log audit.log
```

ローカルホストからリモートサーバへファイルをコピーするには、この引数を逆にします。ディレクトリとサブディレクトリの中身を（再帰的に）コピーするには-rオプションを使用します。

レビュー アク ティビティ：

セキュアなリモートアクセスプロトコル

次の質問にお答えください。

1. 次の記述は正しいですか、誤りですか？TLS VPNはWebベースのネットワークリソースへのアクセスしか提供できない。
2. MicrosoftのTLS VPNソリューションは何ですか？
3. プライベートネットワーク上でデータの機密性を保つには、どのIPSecモードを使用しますか？
4. 多くの場合IPSecと同時に使用され、リモートアクセスクライアントVPNにユーザー認証を提供するのはどのプロトコルですか？
5. IKE v2がIKE v1に勝っている点は何ですか？
6. SSHサーバーの身元をクライアントに対して確認するのはどのような情報ですか？

レッスン11

概要

ローカルネットワークのアクセスと管理、アプリケーションサービス、そしてリモートアクセスとその管理に関してセキュアなプロトコルを構成できる必要があります。

セキュアなネットワークプロトコルを実装するためのガイドライン

ネットワークプロトコルを実装または再構成する場合は、次のガイドラインに従ってください。

- 重要なネットワークアドレス割り当て(DHCP)、名前解決(DNS)、ディレクトリアクセス(LDAP)、時刻同期(NTP)サービスの可用性を確保する。ネットワークを監視して不正なサービスを検知・除去する。
- サービスの可用性を監視するためにSNMPの使用を検討する。
- 認証用の証明書や共有鍵、およびTCP/UDPポートの使用など、アプリケーションプロトコルをセキュアにするための要件を評価する。認証情報のセキュアな配送を保証し、安全な使用に向けて構成ドキュメントを作成する。
 - HTTPSで使用する証明書をWebサーバーにデプロイする。
 - セキュアなSMTP、POP3、IMAPで使用する証明書をメールサーバーにデプロイする。
 - FTPSまたはSFTPで使用する証明書もしくはホスト鍵をファイルサーバーにデプロイする。
 - S/MIMEで使用する証明書をメールクライアントにデプロイする。
 - SIPSとSRTPで使用する証明書をVoIPのゲートウェイとエンドポイントにデプロイする。
 - TLS VPN、IPSec、L2TP/IPSecで使用する証明書または共有鍵をVPNゲートウェイとクライアントにデプロイする。
 - 証明書またはホスト鍵でRDPゲートウェイとSSHサーバーを構成する。ユーザー認証情報または公開鍵を使用してクライアント認証を構成する。
- サーバーとネットワークインフラストラクチャのセキュアなリモート管理のために、セキュア管理ワークステーション(SAW)とアウトオブバンドネットワークインターフェイスまたはジャンプレサーべーを実装する。

レッスン12

ホストのセキュリティソリューションを実装する

レッスン概要

効果的なネットワークアーキテクチャ設計、プロトコル構成、ファイアウォールや侵入検知などのアプライアンスの使用により、セキュアなネットワーク環境が利用できるようになりますが、ネットワークホスト上に構成されたセキュリティシステムについても検討する必要があります。セキュリティ手順とソリューションは、PCやラップトップからスマートフォンや組込みコントローラーまで、ネットワークがサポートする必要があるさまざまなホストタイプによって複雑になっています。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- セキュアなファームウェアを実装する。
- エンドポイントセキュリティを実装する。
- 組み込みシステムのセキュリティのリスクについて説明する。

トピック12A

セキュアなファームウェアを実装する



対象試験範囲

- 1.2 与えられたシナリオに基づいて、可能性あるインジケーターを分析して攻撃のタイプを特定することができる。
- 3.2 与えられたシナリオに基づいて、ホストまたはアプリケーションのセキュリティソリューションを実装することができる。
- 5.3 組織的なセキュリティに関連するポリシーの重要性を説明することができる。

ネットワークとコンピューティングデバイスを支えるハードウェアのセキュリティは見落とされがちです。1つには、ほとんどの企業がこの分野で独自の調査を行うことが難しいためです。サプライチェーンで脅威アクターを特定するには、市場とセキュリティ機関に頼る必要があります。それでも、製品を評価し、購入やデバイス構成に関する推奨事項を作成できるように、セキュアなシステム設計に関連する問題を理解することが重要です。

ハードウェアRoT（信頼の起点）(Root of Trust)

ハードウェアRoTまたはトラストアンカーは、構成証明を提供できるセキュアなサブシステムです。構成証明とは、システムによって作成されたステートメントが受信者にとって信頼できるものであるという意味です。例えば、コンピューターがネットワークに接続されると、「私のオペレーティングシステムのファイルは悪意のあるバージョンに置き換わっていません」と宣言するレポートをNetwork Access Control (NAC)サーバーに提出する場合があります。ハードウェアRoTは、ブートメトリック（様々な測定値）とOSファイルをスキャンして署名を確認し、レポートに署名します。NACサーバーは、署名エンティティの秘密鍵が安全であることを信頼できれば、署名とレポートの内容も信頼できます。

RoTは通常、**TPM (Trusted Platform Module)**と呼ばれる暗号プロセッサによって確立されます。TPMは暗号化キー、ハッシュ化パスワードや、ユーザーやプラットフォームのその他の識別情報をハードウェアベースで保存するための仕様です。チップセットの一部やCPUの組み込み機能として実装されます。

それぞれのTPMには、ユニークで変更不能な非対称秘密鍵（承認キー）が埋め込まれています。この承認キーは、キーの保存、署名、暗号化操作で使用されるさまざまなタイプのサブキーを作成するために使用されます。またTPMは、通常パスワードで識別される所有者の概念もサポートしています（ただし、これは必須ではありません）。セットアッププログラムの管理者権限を持つ者はTPMの所有権を取得し、そのサブキーを破壊して再生成することができます。TPMはWindowsではtpm.mscコンソールまたはグループポリシーを介して管理できます。企業ネットワークでは、TPMへのキープロビジョニングはKMIP (Key Management Interoperability Protocol)を介して一元管理できます。