初級レベル研修

はじめてのセキュリティ

オンラインセミナー
ウェビナー

一般社団法人　情報通信設備協会

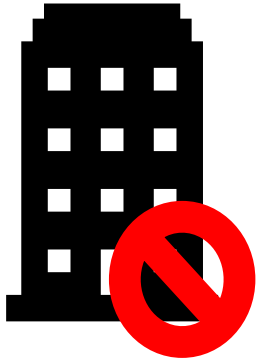
V1.4

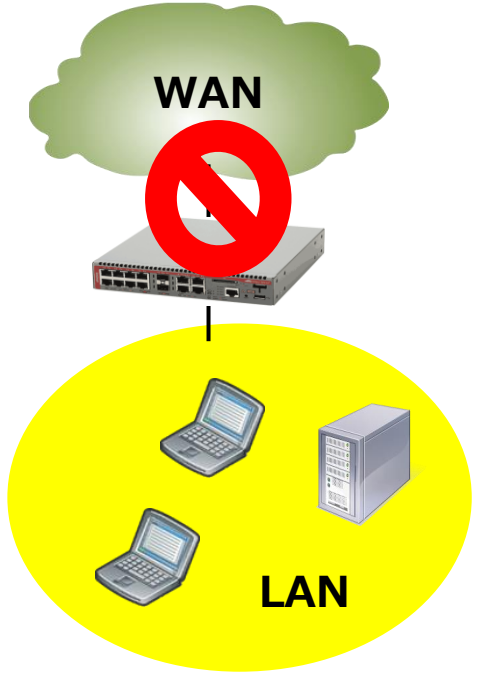
目次

①セキュリティとは

セキュリティとは

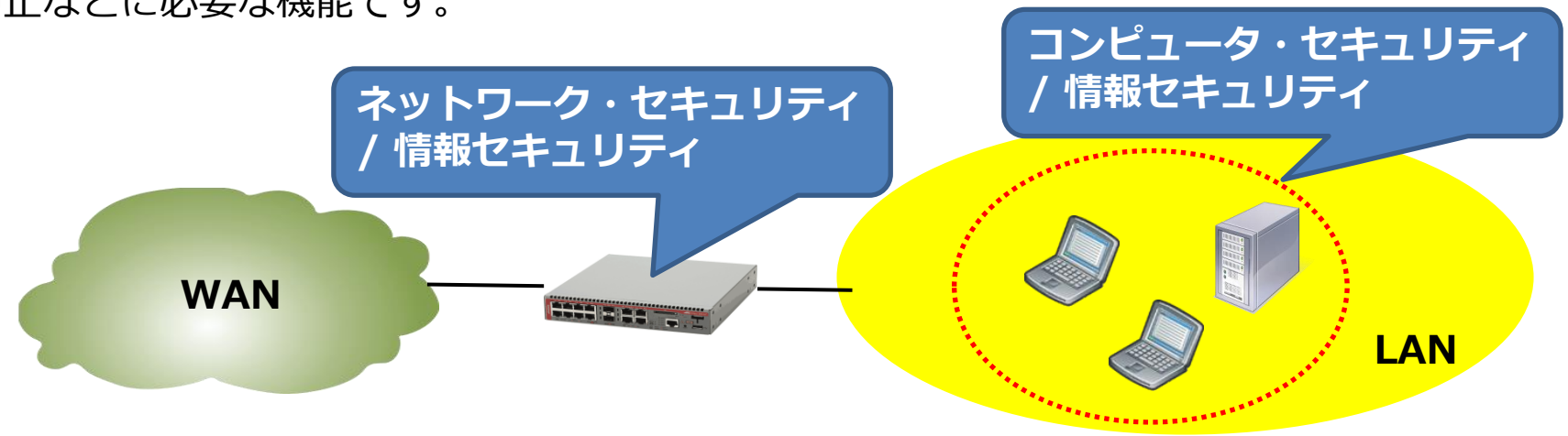
- セキュリティとは、脅威や危険から解放するための様々な方法や手段のことです。
- セキュリティには、個人の家や財産などを守るためのもの、ビルなどの施設を守るためのもの、国家を守るためのもの、ITシステムを守るためのもの、などがあります。
- 本セミナーでは、主にITシステムを構成するコンピュータ、ネットワークや情報を守るITセキュリティについて説明していきます。





ITセキュリティ

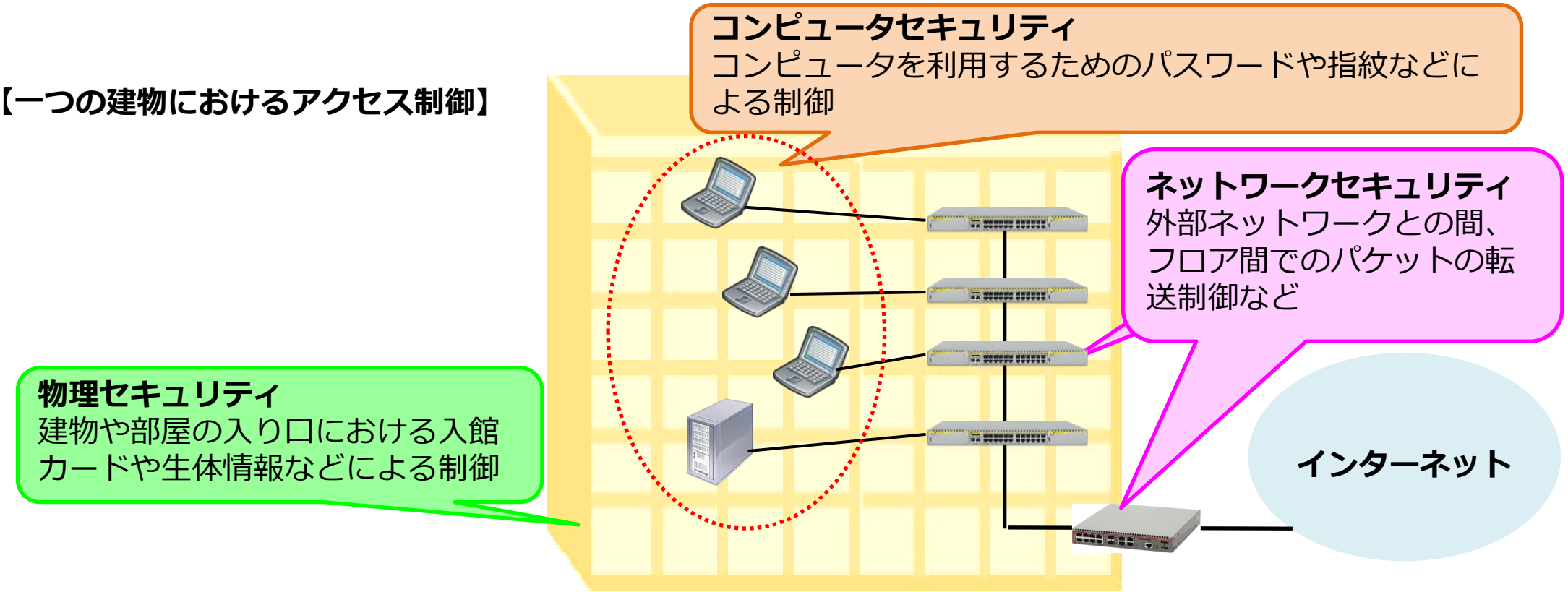
- ITセキュリティとは、ITシステムを構成するコンピュータやそのコンピュータを接続するネットワークに関するセキュリティの総称です。
- ITセキュリティは、以下のセキュリティになります。セキュリティを確保するためには、以下の各セキュリティにおいてアクセス制御の機能を適用する必要があります。
  - コンピュータ・セキュリティ
    - ネットワークに接続された端末やサーバーなどのコンピュータにおけるセキュリティで、コンピュータやコンピュータ上のプログラムを保護するのに必要な機能です。
  - ネットワーク・セキュリティ
    - ネットワークを構成する通信機器（=ネットワーク機器）におけるセキュリティで、主にネットワークへの不正侵入を防止するのに必要な機能です。
  - 情報セキュリティ
    - コンピュータならびにネットワーク機器上の情報管理に関するセキュリティで、情報へのアクセス制御や改ざん防止などに必要な機能です。



アクセス制御

- アクセス制御とは、端末やネットワークへのアクセスを制御すること、もしくはその仕組みになります。セキュリティを高めるためには、複数のアクセス制御機能を組み合わせる必要があります。
- 一つの建物におけるアクセス制御は、制御対象の違いにより、コンピュータセキュリティ(情報セキュリティ含む)、ネットワークセキュリティ、物理セキュリティ(建物や部屋などへの入場制限)に分かれます。
- 主にコンピュータセキュリティやネットワークセキュリティにおいて、アクセス制御を正しい方法で通過しないことを「不正アクセス」と言います。

【一つの建物におけるアクセス制御】



②脅威

情報セキュリティ10大脅威

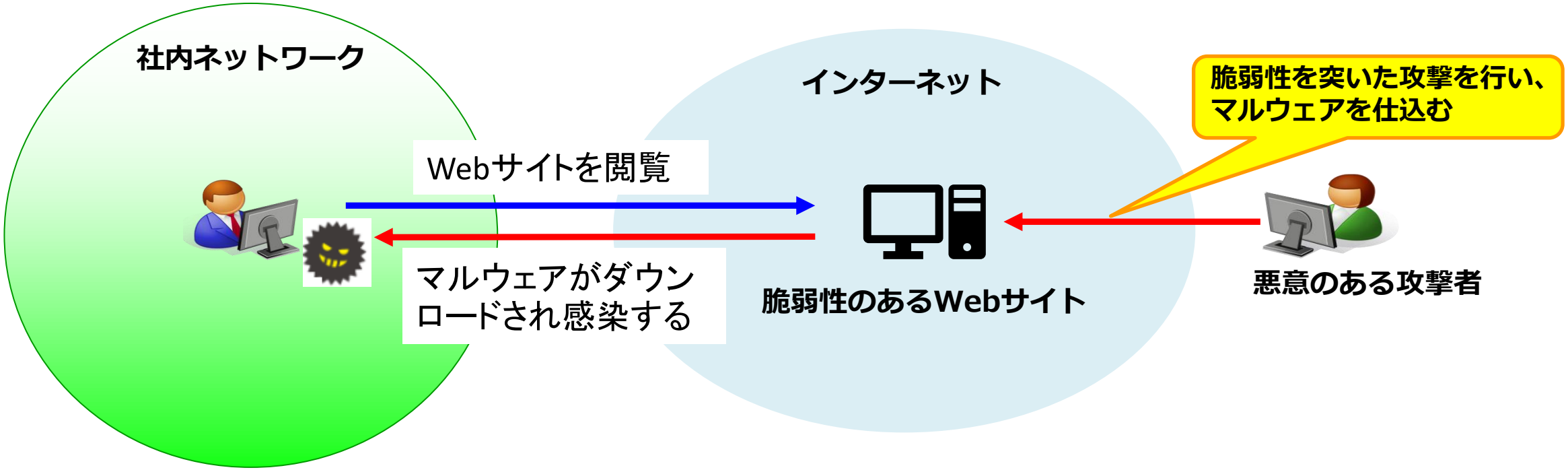
- IPA（情報処理推進機構）が出している情報セキュリティ10大脅威の2024年版は以下になります。なお、個人については順位はありません。
- 組織に対する脅威では、ランサムウェアによる被害や標的型攻撃による機密情報の窃取が上位を占めています。

出典：IPA（情報処理推進機構）

順位	組織	前年順位	個人（順位なし）
1位	ランサムウェアによる被害	1位	インターネット上のサービスからの個人情報の窃取
2位	サプライチェーンの弱点を悪用した攻撃	2位	インターネット上のサービスへの不正ログイン
3位	内部不正による情報漏えい等の被害	4位	クレジットカード情報の不正利用
4位	標的型攻撃による機密情報の窃取	3位	スマホ決済の不正利用
5位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	6位	偽警告によるインターネット詐欺
6位	不注意による情報漏えい等の被害	9位	ネット上の誹謗・中傷・デマ
7位	脆弱性対策情報の公開に伴う悪用増加	8位	フィッシングによる個人情報等の詐取
8位	ビジネスメール詐欺による金銭被害	7位	不正アプリによるスマートフォン利用者への被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求
10位	犯罪のビジネス化(アンダーグラウンドサービス)	10位	ワンクリック請求等の不当請求による金銭被害

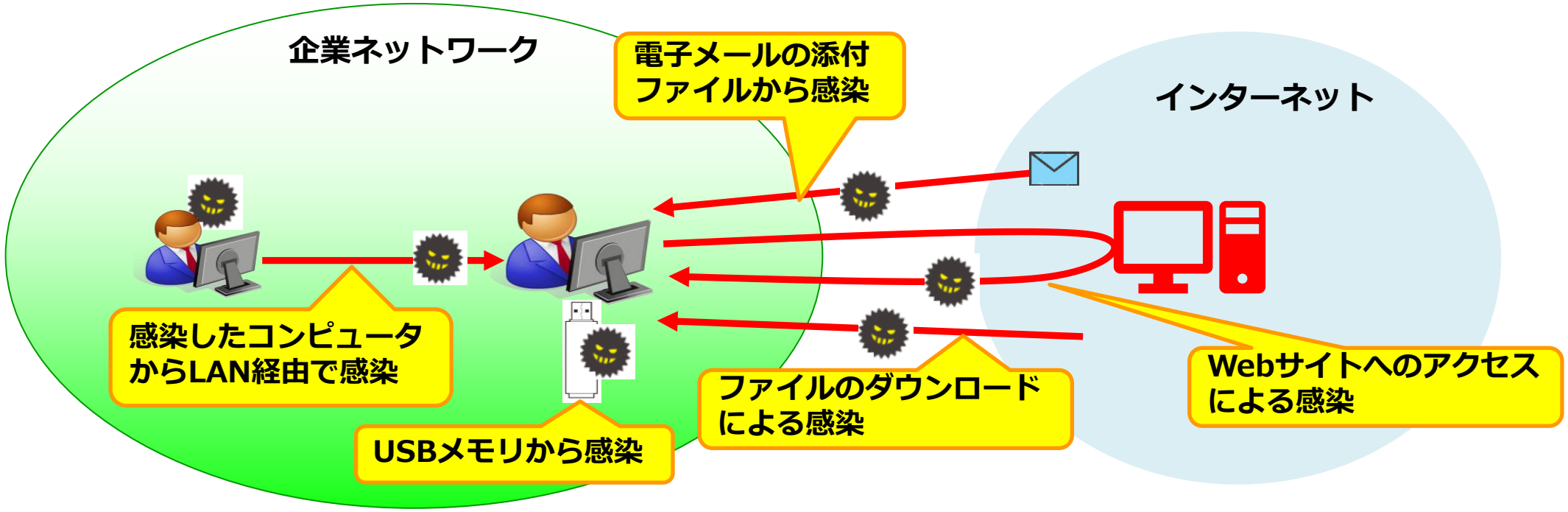
マルウェアとは

- マルウェアとは、コンピュータなどに不正な動作や有害な動作を行わせる、悪意を持ったソフトウェアやコードを総称したものです。
- マルウェアには、コンピュータウィルス、スパイウェア、トロイの木馬、バックドア、ランサムウェアなどの様々な種類が存在します。
- マルウェアの感染経路は多種存在し、Webサイトの閲覧や誘導による感染、 オペレーティングシステムの不備を悪用する感染、メールの添付ファイルからの感染などがあります。



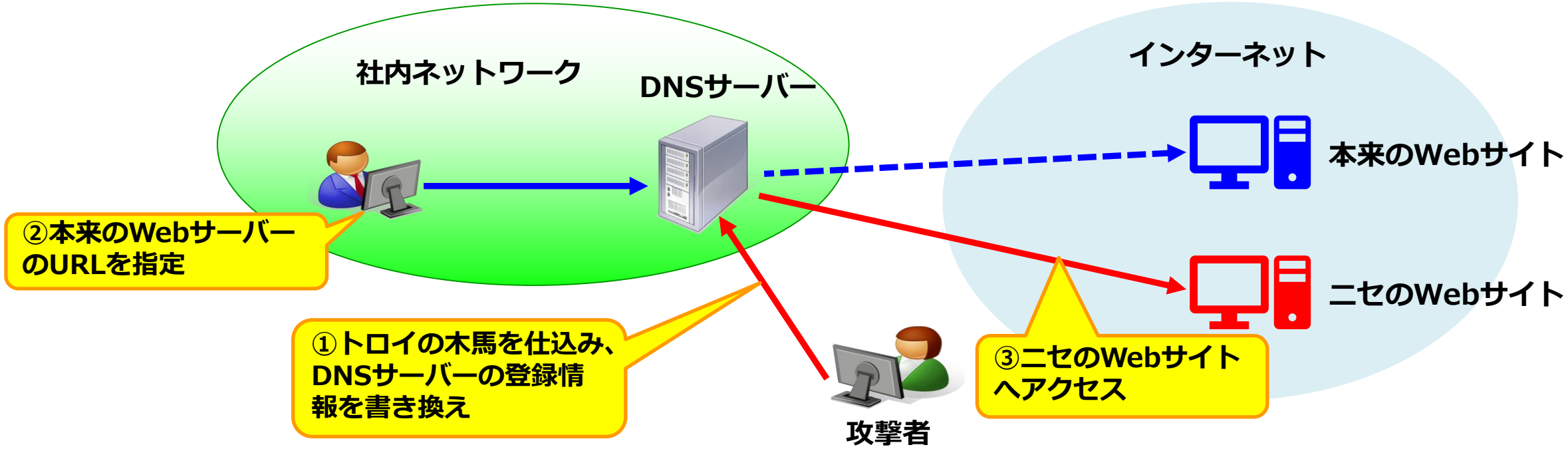
マルウェア – コンピュータウィルス

- コンピュータウイルスはマルウェアの一種で、動的に活動しないでファイルからファイルへと静的に感染するものをいいます。（日本語では一般的に「ウイルス」と呼びます。）
- コンピュータウイルスは、感染元のプログラムファイルを書き換えて自分のコピーを追加します。そのプログラムが実行された時に、自分自身をコピーすることで増殖します。
- 感染経路には、感染した別のコンピュータ経由、USBメモリー経由、電子メールの添付ファイル経由、Webサーバー経由、およびダウンロードしたファイル経由などがあります。



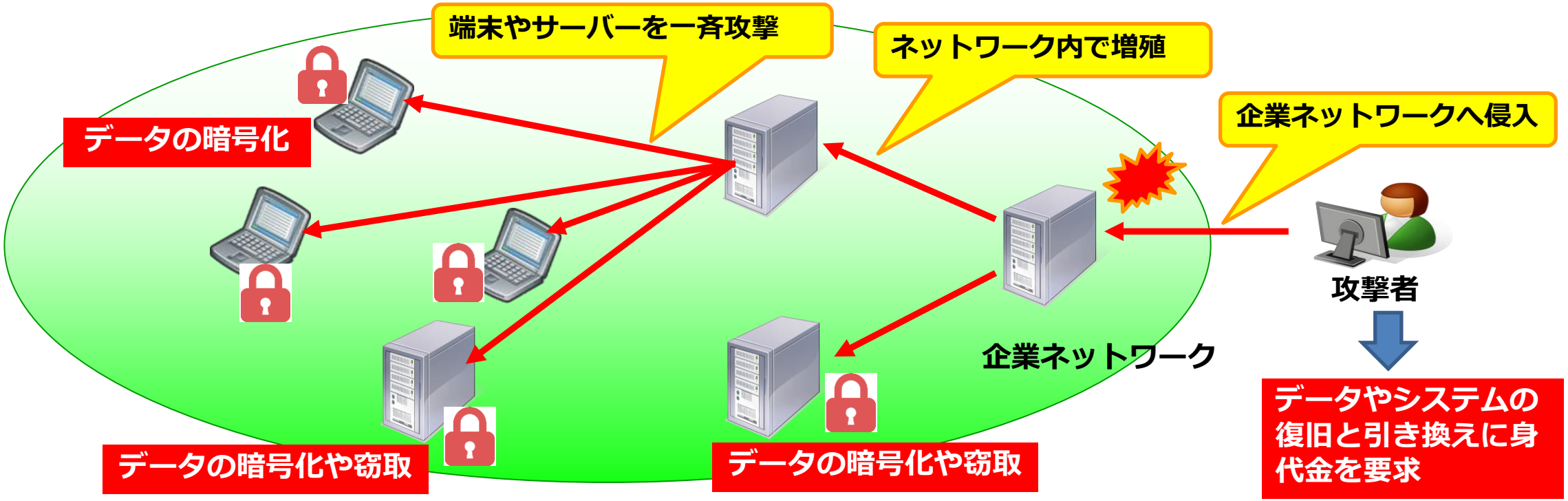
マルウェア – トロイの木馬

- トロイの木馬は、内部にマルウェアとして機能する部分を持っていながら、有用なプログラムやデータファイルとして偽装されています。内部のマルウェア機能は、何らかのトリガーにより活動を開始します。毎年、新種と膨大な亜種が作られています。
- プログラムやファイル内の悪意ある動作が実行されると、利用者が認識しないよう秘密裏に、ハードディスクやメモリ内に自分自身を複製しインストールします。トロイの木馬は、端末のネットワーク設定やファイアウォール設定を変更し、外部からの接続を可能にすることで端末を乗っ取ります。
- トロイの木馬が行う動作には、キーロギング、プログラムやファイルの追加/削除、アンチウイルスソフトの無効化、パスワードの奪取などがあります。



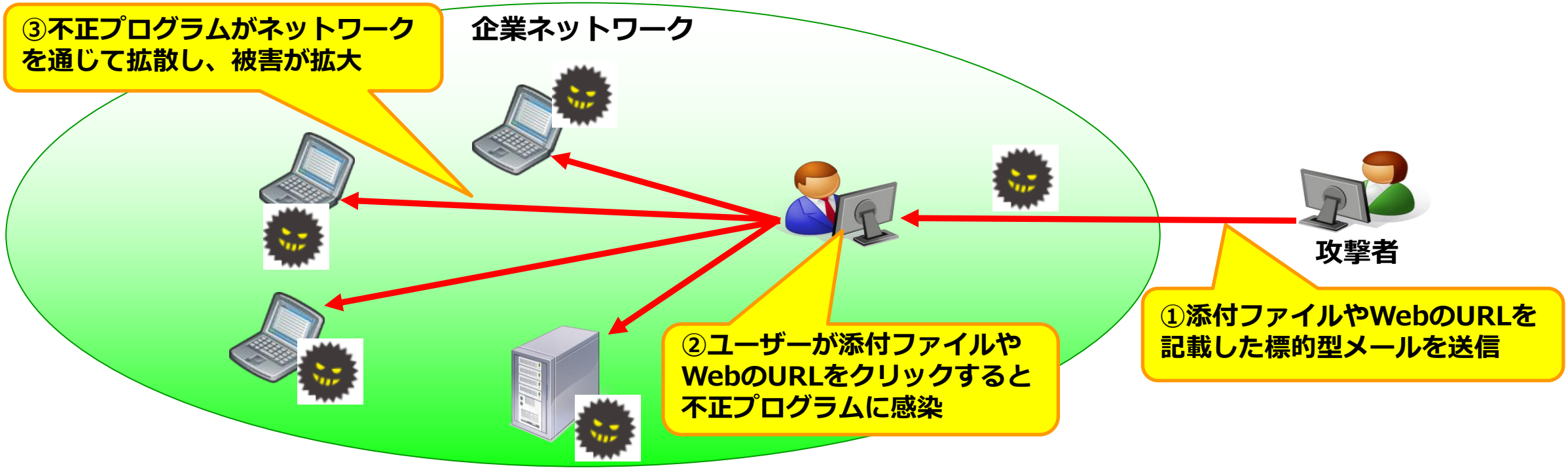
マルウェア - ランサムウェア

- ランサムウェアとは、感染したコンピュータに特定の制限をかけて、制限解除と引き換えに身代金を要求する不正なプログラムです。感染するとコンピュータのロックやファイルの暗号化が行われ、復号しない限りはファイルにアクセスできなくなるなど、企業にとって重大な被害が発生します。
- 昨今感染が再拡大しているマルウェア「Emotet」との親和性が非常に高く、Emotetに感染した後にランサムウェアに感染するケースも多いため、セキュリティ対策の重要度は高まっています。
- ランサムウェアは、ダウンロードファイルや、ネットワークサービスの脆弱性を突いてコンピュータに入り込み、一般的にはトロイの木馬として増殖します。



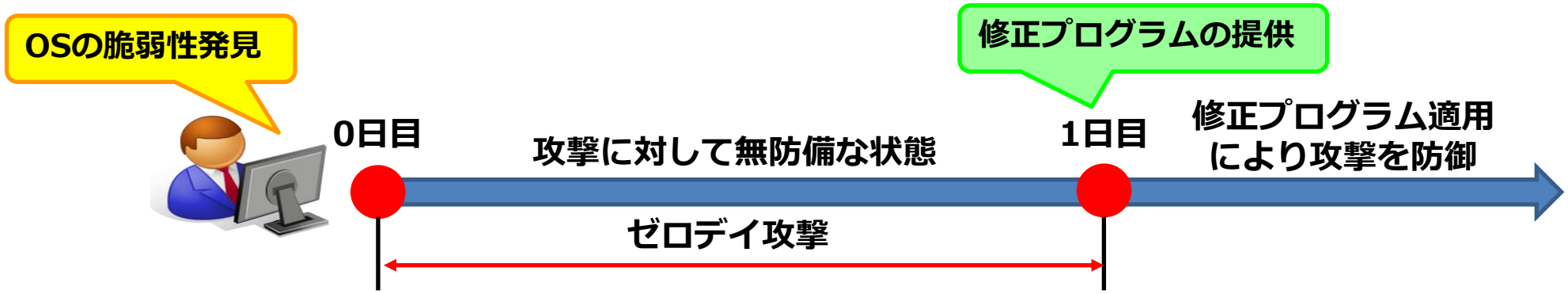
標的型攻撃

- 標的型攻撃とはサイバー攻撃の一種であり、特定の組織内の情報を狙い、その組織の所属者宛てにコンピュータウイルス添付の電子メールが送信されます。標的型攻撃の対象組織は、価値の高い知的財産を保有している政府、公共サービス機関や製造業が多くなっています。
- 企業内ネットワークに潜伏し持続的に行われる標的型攻撃は、APT攻撃（Advanced Persistent Threat）と呼ばれます。
- 標的型攻撃の攻撃手法には、前述の標的型メールやWebサイト閲覧により開始する方法、バックドアを設置して遠隔操作する方法などがあります。



ゼロデイ攻撃

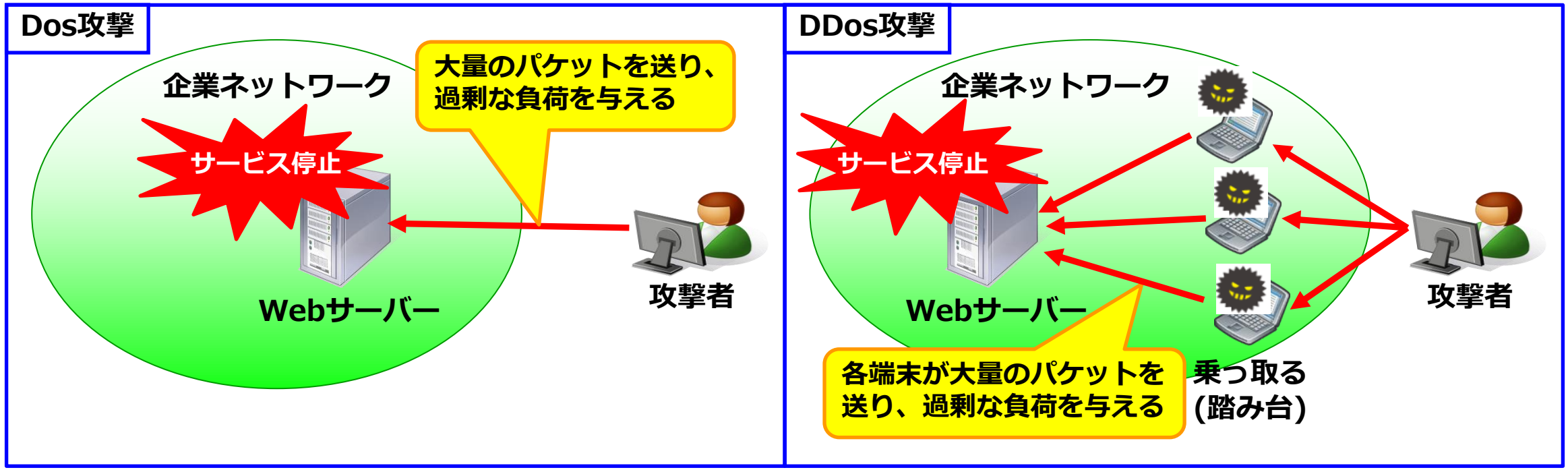
- ゼロデイ攻撃とは、オペレーティングシステムなどのセキュリティホールが発見された後、脆弱性を解消する対処方法が確立されるまでの間を利用して行われるサイバー攻撃のことです。
- ゼロデイ攻撃の方法には、マルウェア添付メールの送信やWebサイトの改ざんなどがあり、被害としてはマルウェア感染や不正アクセスなどがあります。
- 脆弱性を狙われるプログラムの代表的なものは、オペレーティングシステム、Webブラウザおよびサーバーソフトウェアがあり、オープンソースプログラムやインストールしている製品が多いプログラムで規模が拡大する傾向にあります。



【対策】セキュリティ対策ソフトの導入や不明メールの添付ファイルは開かない
サンドボックス環境の導入
EDR(Endpoint Detection and Response)製品の導入
WAF(Web Application Firewall)の導入
重要情報の暗号化や隔離
第三者による脆弱性のチェック

DoS攻撃 / DDos攻撃

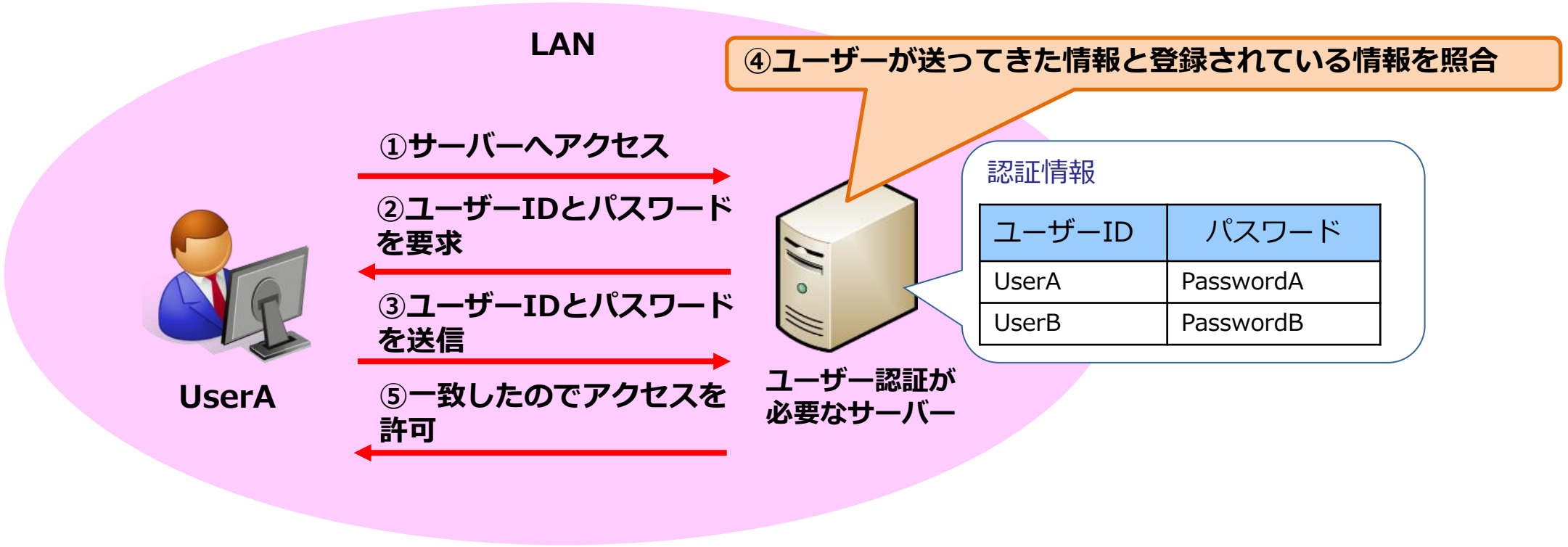
- DoS(Denial of Service)攻撃は、Webサーバーなどに過剰な負荷をかけたり、Webサーバーなどの脆弱性を突いてサービスを妨害します。DoS攻撃の被害としては、ネットワーク上のトラフィック増大による遅延や、Webサイトへのアクセス不可が挙げられます。
- DDoS(Distributed Denial of Service)攻撃は、大量のマシンを不正に乗っ取り、そのマシンを踏み台として1つのサービスに同時にDoS攻撃を行うことです。
- 攻撃としては、SYNパケットを大量に送信(SYNフラッド攻撃)、pingパケットを大量に送信、UDPポートに大量のトラフィックを送信、およびWebサーバーに大量のリクエストを送信などの方法があります。



③防御技術（アクセス制御技術）

パスワード認証

- パスワード認証は、パスワードにより利用者を確認する認証方式です。ログインIDとパスワードを事前に登録し、ログイン時に入力したユーザーIDとパスワードが登録情報と一致した場合のみサービスが利用できます。
- パスワード認証には、複数のサービスで同じパスワードを利用する「パスワードの使い回し」や、生年月日などを利用したため「パスワードが類推しやすい」などの問題があります。
- パスワード認証の欠点を補うため、 1回限り有効のパスワードを使用する「ワンタイムパスワード認証」、生体認証（後述）、多要素認証（後述）などを使用することもあります。

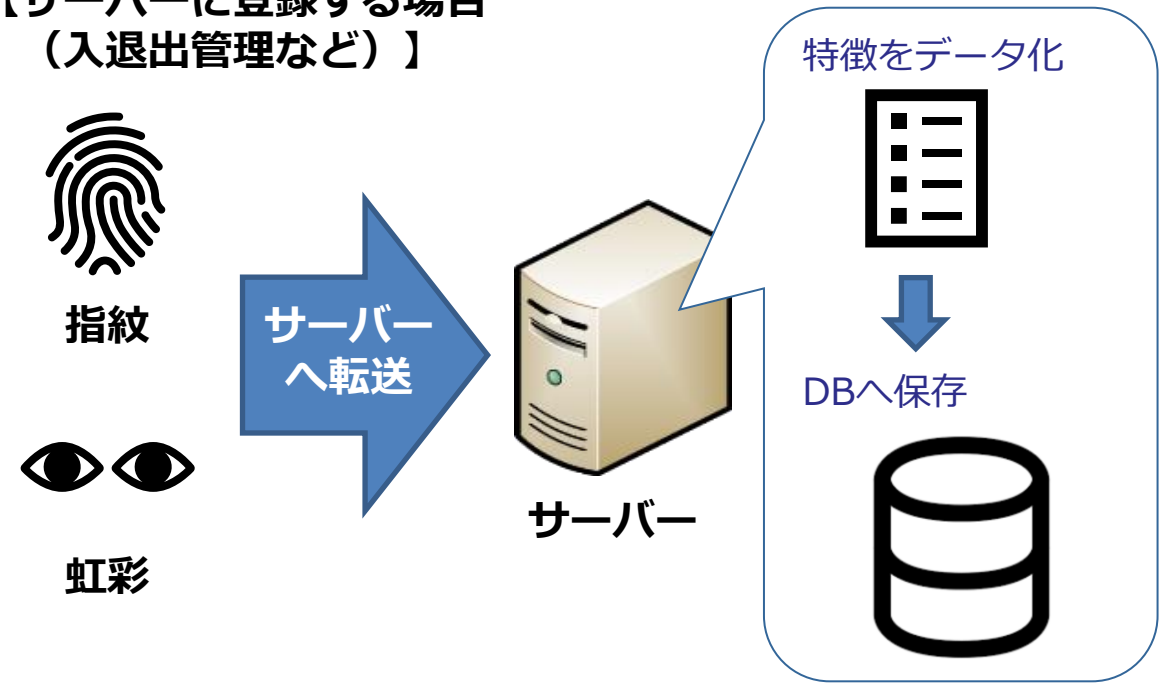


生体認証

- 生体認証は、指紋、声紋、網膜などの本人固有の身体情報による認証方式です。そのため、本人認証性が極めて高いというメリットがあります。
- 利用件数は指紋や、瞳の虹彩が多いですが、金融機関のATMやスマートフォンに採用されている指・手のひらなどの血管の形を読み取る静脈認証も増えています。
- 課題としては、怪我などにより生体認証ができない人への対応、経年変化による認証ができなくなった場合の対応、複製により認証が破られることへの対応があります。特に、複製により認証が破られてしまうと、同じ認証基盤では安全性が確保できなくなります。

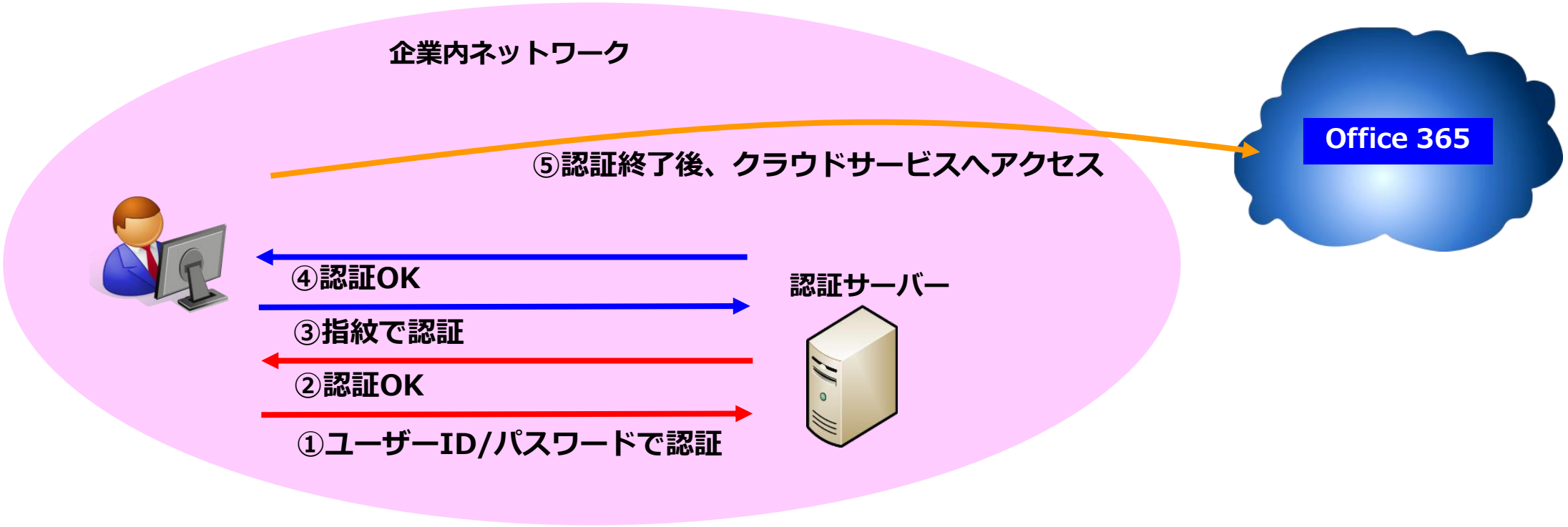
【デバイスに登録する場合（スマートフォンなど）】

【サーバーに登録する場合（入退出管理など）】



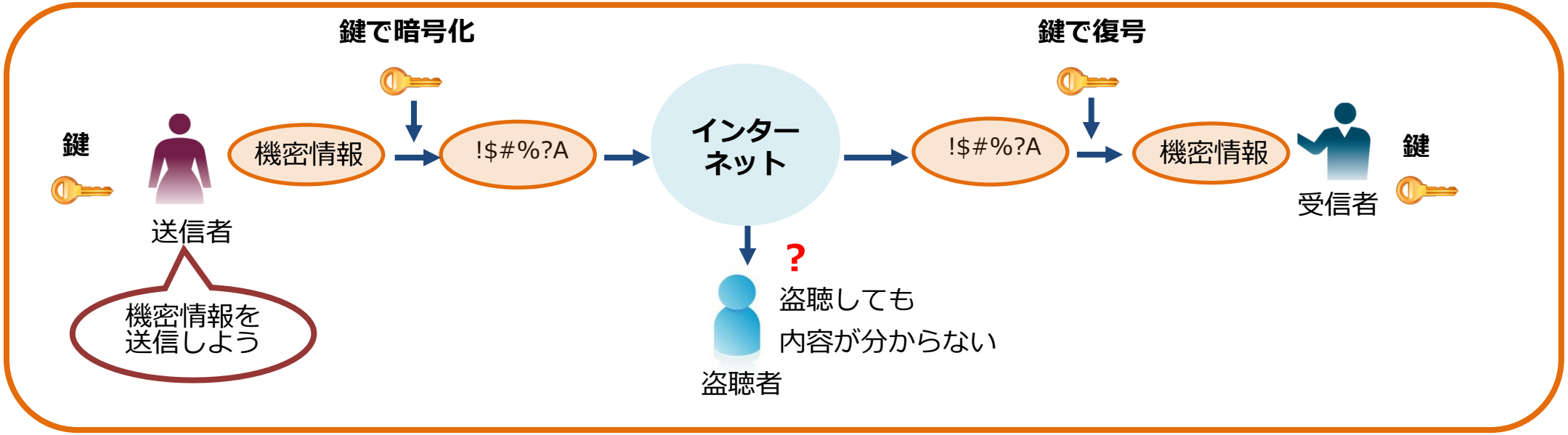
多要素認証

- 多要素認証は、パソコンなどのログイン時やシステムなどへのアクセス時に、2つ以上の方法（要素）で認証処理を行います。不正アクセスに強くセキュリティを高めるため、企業や金融サービスで導入されています。
- 多要素認証は、ID・パスワード・電話番号などの知識認証、ワンタイムパスワード・ USBセキュリティキー・トークンなど所持認証、指紋・顔・虹彩などの生体認証を組み合わせて認証を行います。
- 利用例としては、銀行のATM、WebサービスにおけるSMS(ショートメッセージサービス)認証やUSBセキュリティキーによる認証などがあります。



暗号化

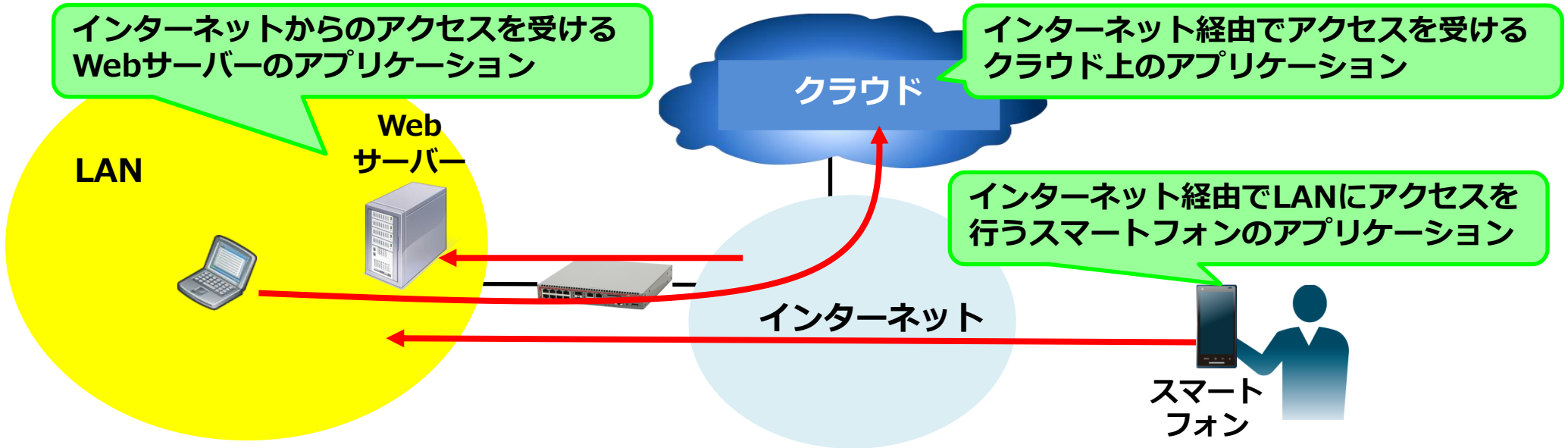
- 暗号化は、情報の受け渡しを行う当事者以外がその情報を見ても読めないように変換（=暗号化）する方法です。セキュリティを確保した通信を行うための一つの手段で、情報をサーバーや記録媒体へ保存する場合にも行うことがあります。
- 暗号化された情報を暗号文、暗号化される前の情報を平文(ひらぶん)と呼びます。通信において情報は、送信側で暗号文に変換され、受信側で平文に戻されます（=復号）。
- 暗号化や復号を行う場合は、鍵（key）が必要となります。鍵には、公開鍵、共通鍵や秘密鍵などの種類があり、鍵の長さ（=ビット数）が大きくなるほど、暗号強度※は高くなります。



※ 暗号強度とは、暗号文の解読しにくさを表したものです。暗号強度は暗号化アルゴリズムにより変わります。

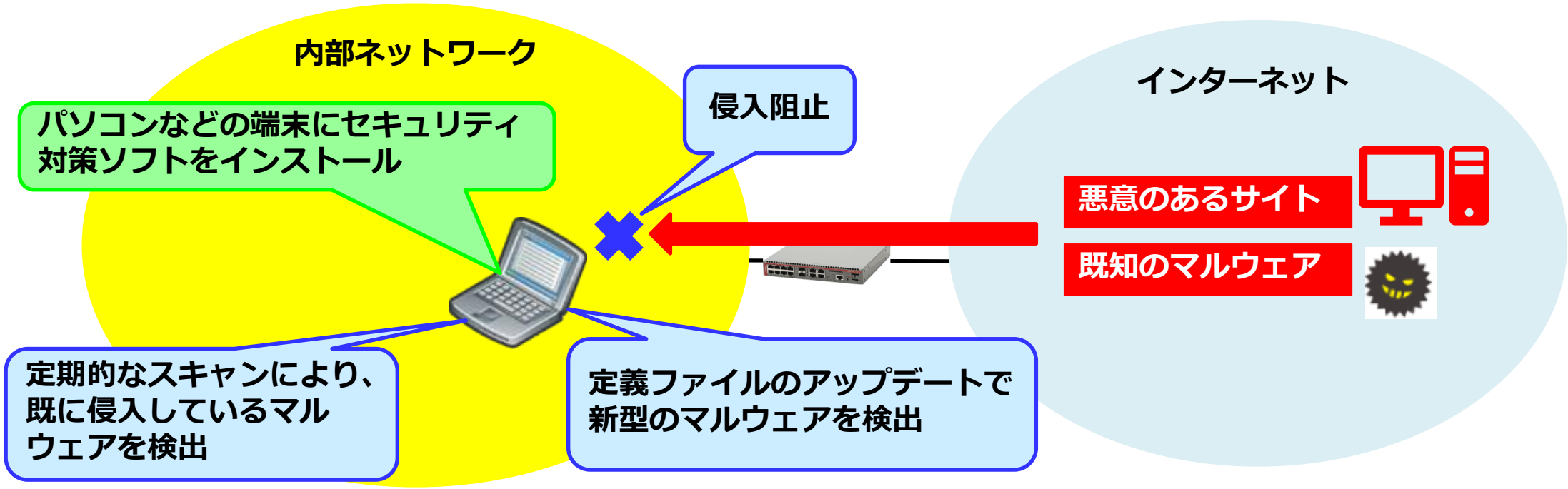
アプリケーションセキュリティ

- アプリケーションセキュリティは、アプリケーションレベルのセキュリティ対策で、盗難および乗っ取りからアプリケーションデータやコードを防御します。
- 現在のネットワークでは、内部ネットワークのアプリケーションだけでなく、クラウド上のアプリケーションを利用することもあります。そのため、アプリケーション自体の保護も重要になります。また、アプリケーションを攻撃する脅威も以前より増えています。
- アプリケーションが持つセキュリティ機能は、認証、暗号化、ログの収集、セキュリティテストなどがあります。特に、クラウド上のアプリケーション、モバイルデバイスのアプリケーション、およびWebサーバー上のアプリケーションは、外部ネットワーク経由で利用されるため十分なセキュリティ対策が必要となります。



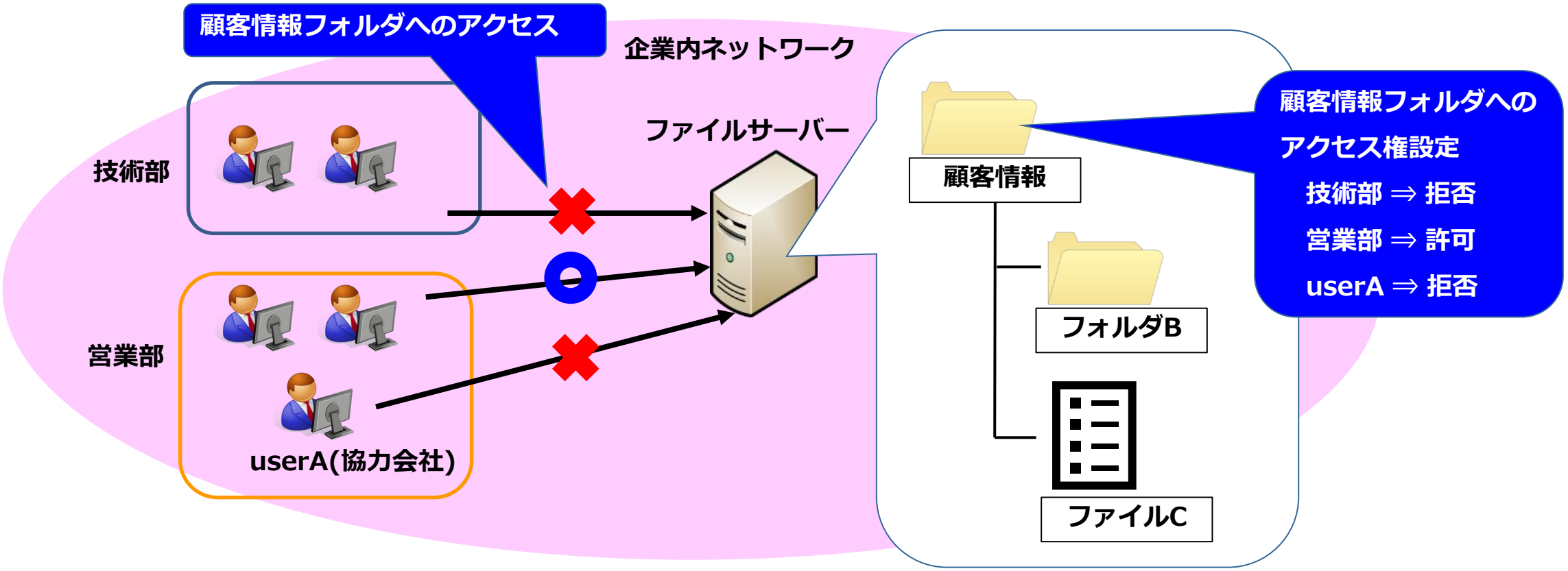
セキュリティ対策ソフト

- セキュリティ対策ソフトとは、ウイルスの駆除や感染予防に加えて、外部ネットワーク（インターネット）からの不正アクセスや端末内の情報漏洩を防止します。
- Windows10と11のパソコンには Windowsセキュリティが標準装備されており、「Windows Defenderウイルス対策」というウイルス対策プログラムが含まれています。ただ、新型のマルウェアなどに対応するまでに時間がかかることがある、迷惑メール対策ができないなどの問題点があるため、業務で使用する端末には、セキュリティ対策ソフトをインストールするのが望ましいです。
- セキュリティ対策ソフトの選定には、「性能が高く、第三者機関から評価されている」「動作が軽い」「料金」「サポートの充実度」などの点を考慮する必要があります。



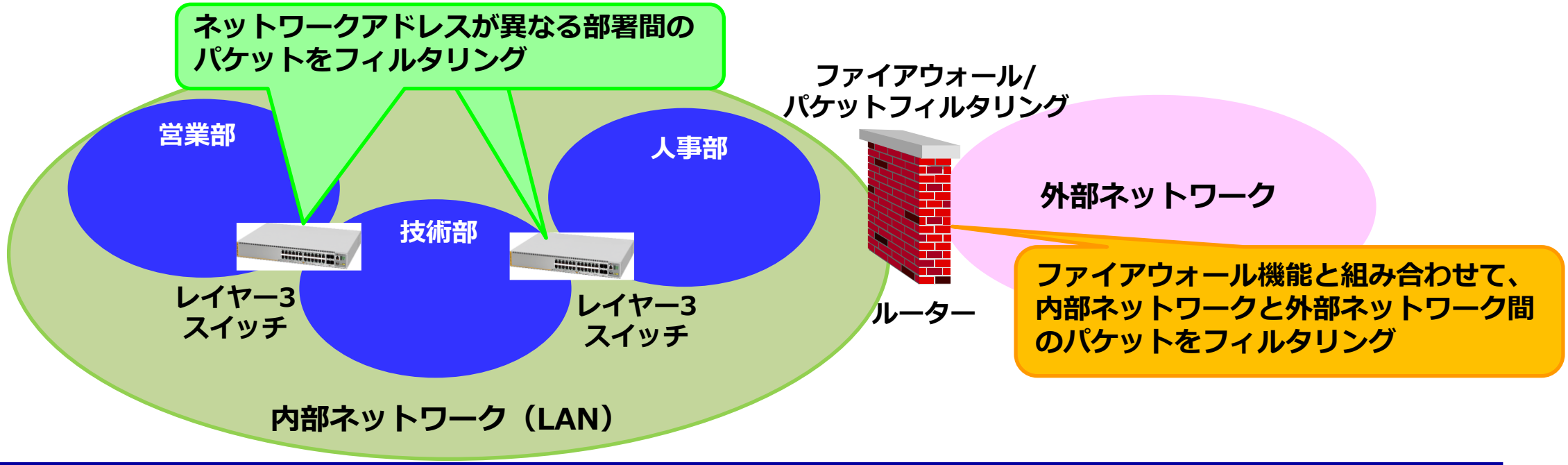
アクセス権限

- アクセス権限は、データ（ファイル）や機能などを利用する権限です。設定の対象としては、ネットワーク、サーバー、業務システム、フォルダ、ファイルなど多種に渡ります。
- ユーザーやグループ(部署など)ごとに、ファイルやフォルダに対する「参照」・「更新」・「削除」などの権限を設定することで、「不正アクセスからの重要情報の保護」、「社内情報の機密性の確保」などが可能となります。
- サーバーなどの重要機器の情報を守るためには、バックアップシステムの構築も必要となります。



パケットフィルタリング

- パケットフィルタリングとは、受信したパケットを管理者などが設定したルールに基づいて転送したり破棄したりする機能です。LAN内の異なるネットワーク間でやりとりされるパケットや、内部ネットワークと外部ネットワーク間でやりとりされるパケットに対して適用します。
- 主にレイヤー3スイッチ、ルーターなどのアプライアンス製品に組み込まれています。ルーターにおいては、ファイアウォール機能（後述）と組み合わせて設定します。
- パケットフィルタリングはパケットのヘッダ部分をチェックするため、データ部分（アプリケーションデータ）に脅威が存在する場合はフィルタリングできません。セキュリティレベルを高めるには、データ部分のチェックを行う技術が必要となります。

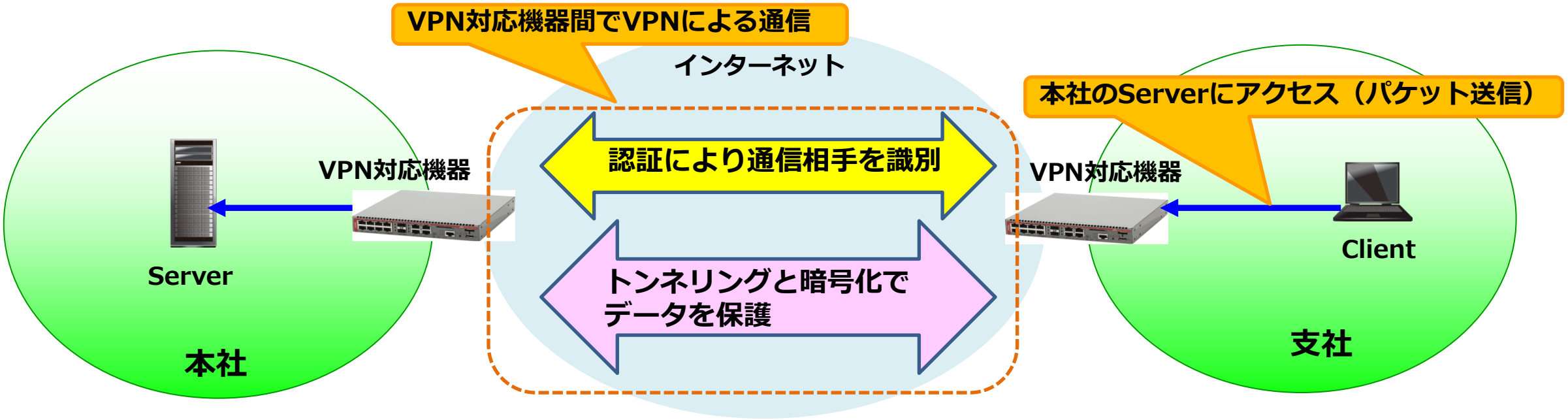


ファイアウォール

- ファイアウォールは、コンピュータネットワークにおけるネットワークの保護や、コンピュータの保護などのため、必要な通信のみを通過させるシステムのことです。
- 主にルーターなどのアプライアンス製品に組み込まれていますが、コンピュータのオペレーティングシステムが持つネットワークプログラムにあるフィルタ機能を指すこともあります。Windows OSには Windows ファイアウォール、Mac OSにはアプリケーションファイアウォールがあります。
- ファイアウォールは、以下の3種類のゾーン間で通信の可否を制御します。
  - 内部（Inside）ゾーン：外部から守るべきネットワーク
  - 外部（Outside）ゾーン：攻撃元となる可能性のあるネットワーク
  - DMZ（DeMilitarized Zone：非武装ゾーン）：内部と外部の中間に置かれるゾーンで外部ゾーンからアクセス可能

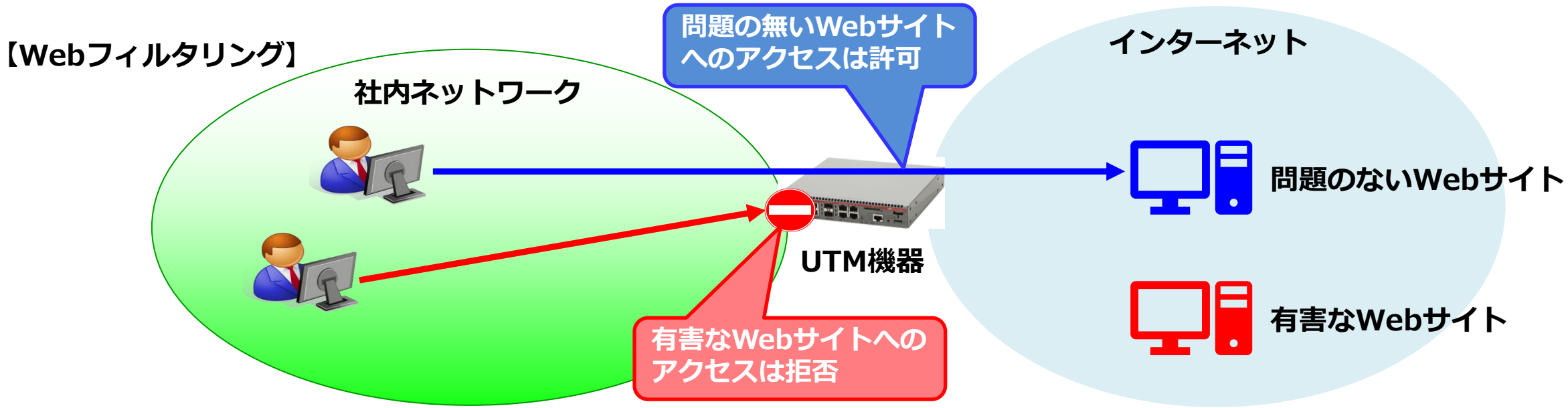
VPN

- VPN（Virtual Private Network)は、主にインターネットのような多数の利用者が存在するネットワークを利用して、企業の拠点間を接続したり、社員が自宅や外出先から会社のネットワークに接続したりする時に使用します。
- VPNでは、接続する相手を認証により識別し、トンネリングや暗号化の技術によってデータを保護します。
- VPNの構築は、拠点間接続の場合はVPN対応機器（主にルーター）間、自宅や外出先からの場合は端末とVPN対応機器の間で行います。



その他のUTM機能

- 前記以外のUTM機能には、以下のようなものがあります。
  - **アンチスパム**：受信したメールがスパム（迷惑）メールを送信するサーバーからかどうかを確認し、ブロックやSubject欄へアラートを追記します。
  - **Web（URL）フィルタリング**：悪意のあるWebサイトや有害なWebサイトに対して閲覧を制限し、情報の流出を防止します。
  - **アプリケーション制御機能**：許可しているアプリケーション以外の使用を禁止します。それにより、ウイルスやスパイウェアの侵入を防止します。



防御技術の位置付け

■ ITセキュリティにおける防御技術の位置付けは、以下になります。

ITセキュリティ	防御技術	主な利用機器や方法
ネットワーク・セキュリティ	認証	VPN機器間、ネットワーク機器と端末の間
	暗号化	VPN機器間、監視装置とネットワーク機器の間、無線機器（無線LANアクセスポイントと無線端末）間
	トラフィック制御	ネットワーク機器
	UTM	ルーターやUTM機器などの外部ネットワークと接続する機器
コンピュータ・セキュリティ	認証	ログイン時、ネットワークへの接続時、外部から社内ネットワークへのVPNアクセス時
	暗号化	無線端末と無線LANアクセスポイントの間でのパケット送信時、外部から社内ネットワークへのVPNアクセス時
	端末/アプリケーションの保護	・セキュリティ対策ソフトはネットワーク接続の全端末 ・アプリケーションの保護は、（特に）社外からのアクセスが発生するサーバー類（Webサーバー、社外メールサーバー、DNSサーバーなど）
情報セキュリティ	暗号化	ファイルなどの暗号化
	ファイルの保護	セキュリティ対策ソフト、ファイルやディレクトリへのアクセス権の設定

④アライドテレシスのセキュリティ製品

ルーター製品

- ルーター製品は、UTM関連を中心とした機能を提供します。
- 弊社ルーター製品が現在実装しているUTM関連機能は以下になります。機能によっては、別途有償ライセンスが必要になります。

ファイアウォール / VPN / パケットフィルタリング / IDS / IPS

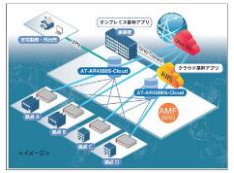
アプリケーションコントロール / IPレピュテーション / Webコントロール ※1

NFV-APLシリーズ

AT-AR4050S-5G

AT-AR4050S

AT-AR3050S



AT-AR4000S-Cloud

AT-AR2050V

AT-AR1050V

AT-AR2010V

AT-TQ6702 GEN2-R

※1 この機能を利用する場合は、有償ライセンスが必要となります。また、他のUTM関連機能とは併用ができない場合があります。

スイッチ製品

- スイッチ製品は、パケットフィルタリングや認証の機能を提供します。
- 弊社では、以下シリーズのレイヤー3スイッチやレイヤー2 plusスイッチ（レイヤー2スマートスイッチおよびレイヤー2スイッチは除く）で上記の機能を提供します。

パケットフィルタリング / 認証

SwitchBladeシリーズ

CentreCOMシリーズ

xシリーズ

XSシリーズ

GSシリーズ

SEシリーズ

SHシリーズ

FSシリーズ

無線LANアクセスポイント製品

- 無線LANアクセスポイント製品は、WPA（Wi-Fi Protected Access）※ による認証および無線端末との間でパケット暗号化の機能を提供します。通常、WPA2もしくはWPA3のバージョンを使用します。
- WPA以外に、MACアドレスによる無線端末のアクセス制御（=無線端末の認証）の機能も提供します。

認証 / 暗号化

スタンダードモデル

AT-TQm6602 GEN2

AT-TQm6702 GEN2

AT-TQm1402

アドバンストモデル

AT-TQ6702e GEN2

AT-TQ6702 GEN2

AT-TQ6602 GEN2

AT-TQ6602

AT-TQ5403e

AT-TQ1402

AT-TQ6702 GEN2-R

※ WPAとは、Wi-Fi Alliance（無線LAN製品の普及促進を図ることを目的とする業界団体） が策定したセキュリティプロトコルに、ネットワーク機器が準拠していることを示すものです。

クラウドUTMサービス

Net.CyberSecurity

- クラウド型のメリットを生かしたUTMサービスです。従来、拠点単位でインターネットの出口に設置していたUTM機器をクラウド上に統合することで、効果的かつ効率的な運用が実現するだけでなく、SD-WANやインターネットブレイクアウト環境などへの接続にも対応します。
- オプションサービスとして、クラウドEMS（Enterprise Mobility + Security）サービスがあります。このサービスは、テレワークで利用するリモート接続端末の一元管理や脆弱性の可視化などの「リモート接続端末の安全なアクセス環境」を実現します。

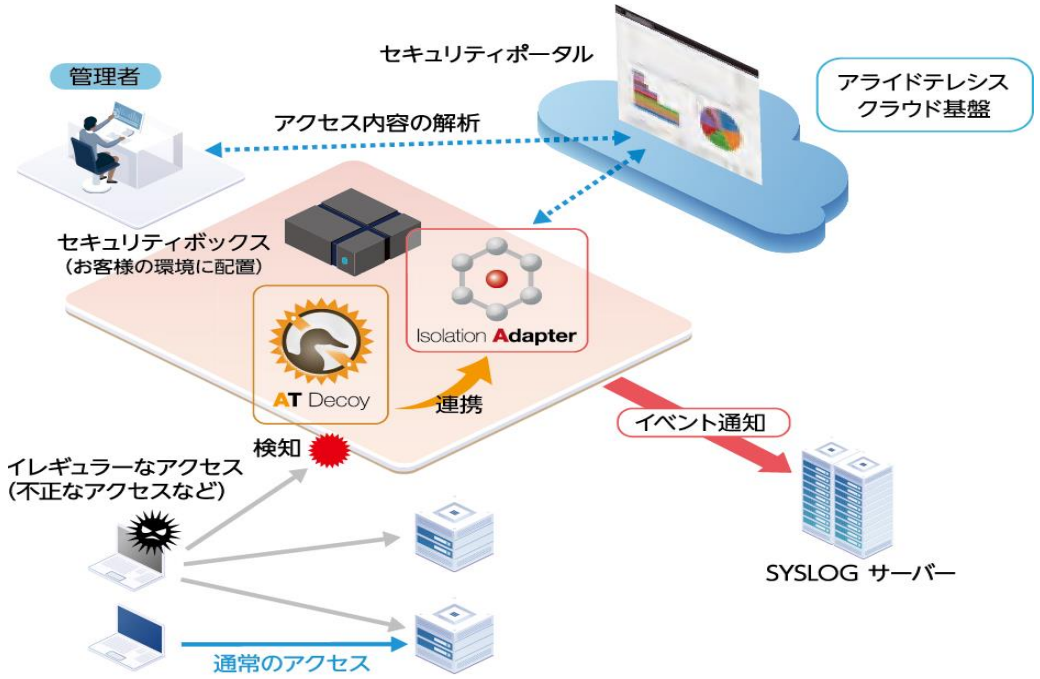
Allied Telesis

感染端末検出・制御サービス

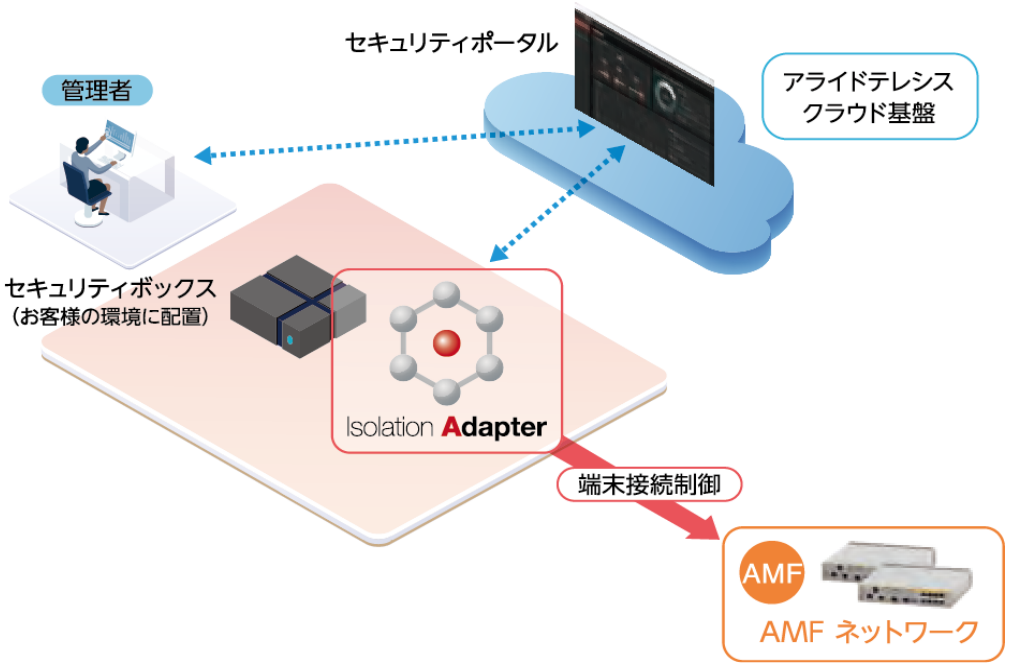
Net.CyberSecurity

- 不正アクセス検知後の初動対応を自動で行い、アクセスを制御する不正端末隔離サービス（Isolation Adapter）と、不正アクセスを検知する感染端末検出サービス（AT Decoy）です。
- 感染端末検出サービスは、LAN上に設置したセキュリティボックスを疑似サーバーとすることで、不正アクセスを検知し、送信元からマルウェアに感染した端末を検出します。不正端末隔離サービスと連携してアクセス制御を可視化することができます。
- 不正端末隔離サービスは、お客様のLAN上に設置したセキュリティボックスが、 各種セキュリティアプリケーションと連携して不正なアクセスを検知し動的にアクセスを制御します。

【感染端末検出サービス】



【不正端末隔離サービス】

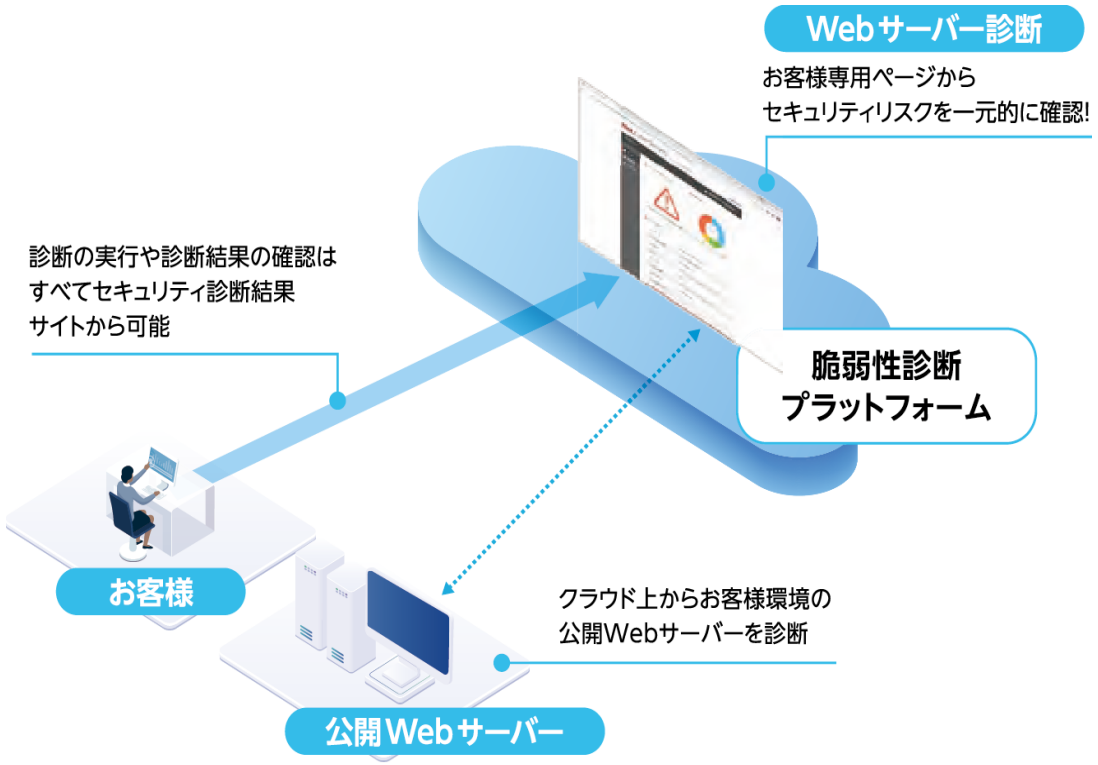


Allied Telesis

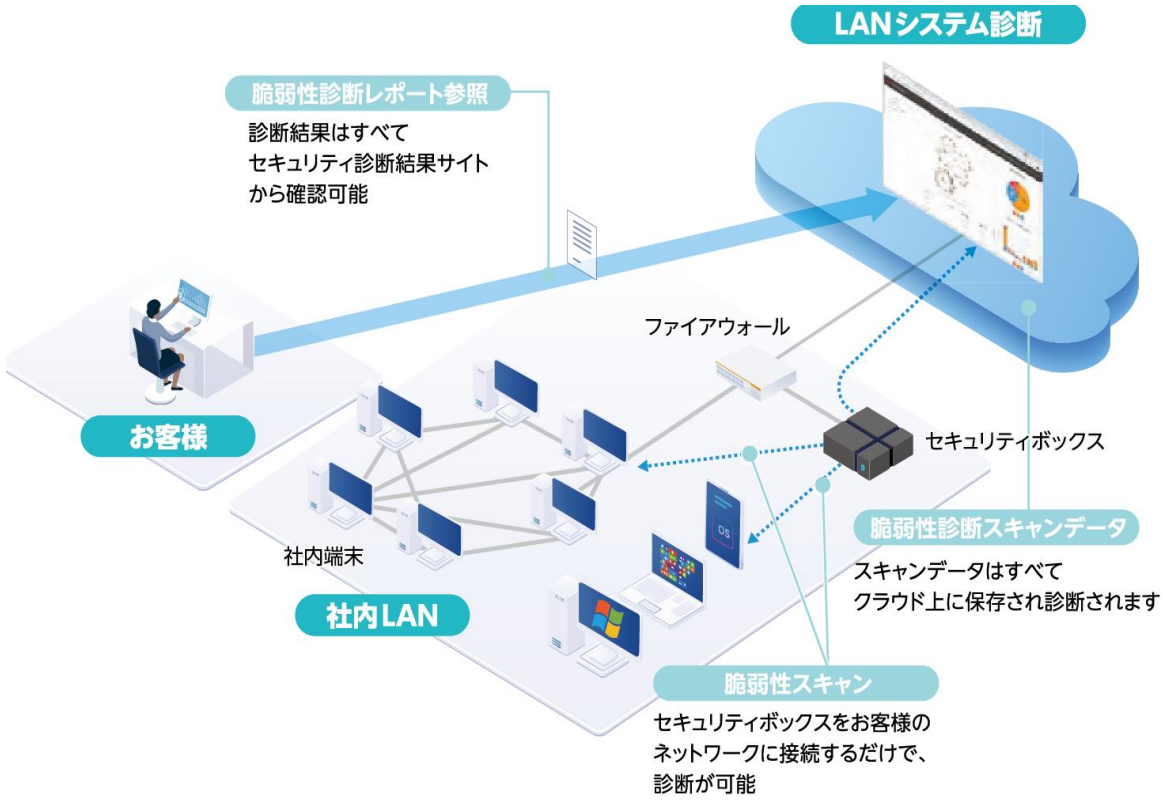
脆弱性診断サービス

- 脆弱性診断サービスには、Webサーバー診断サービスとLANシステム診断サービスがあります。診断結果は専用のセキュリティ診断結果サイトで確認できます。
- Webサーバー診断サービスは、クラウド上からお客様のWebサーバーの脆弱性を診断するサービスです。また、LANシステム診断サービスは、お客様の社内ネットワークに接続されているIP機器を対象とする脆弱性診断サービスです。

【Webサーバー診断サービス】

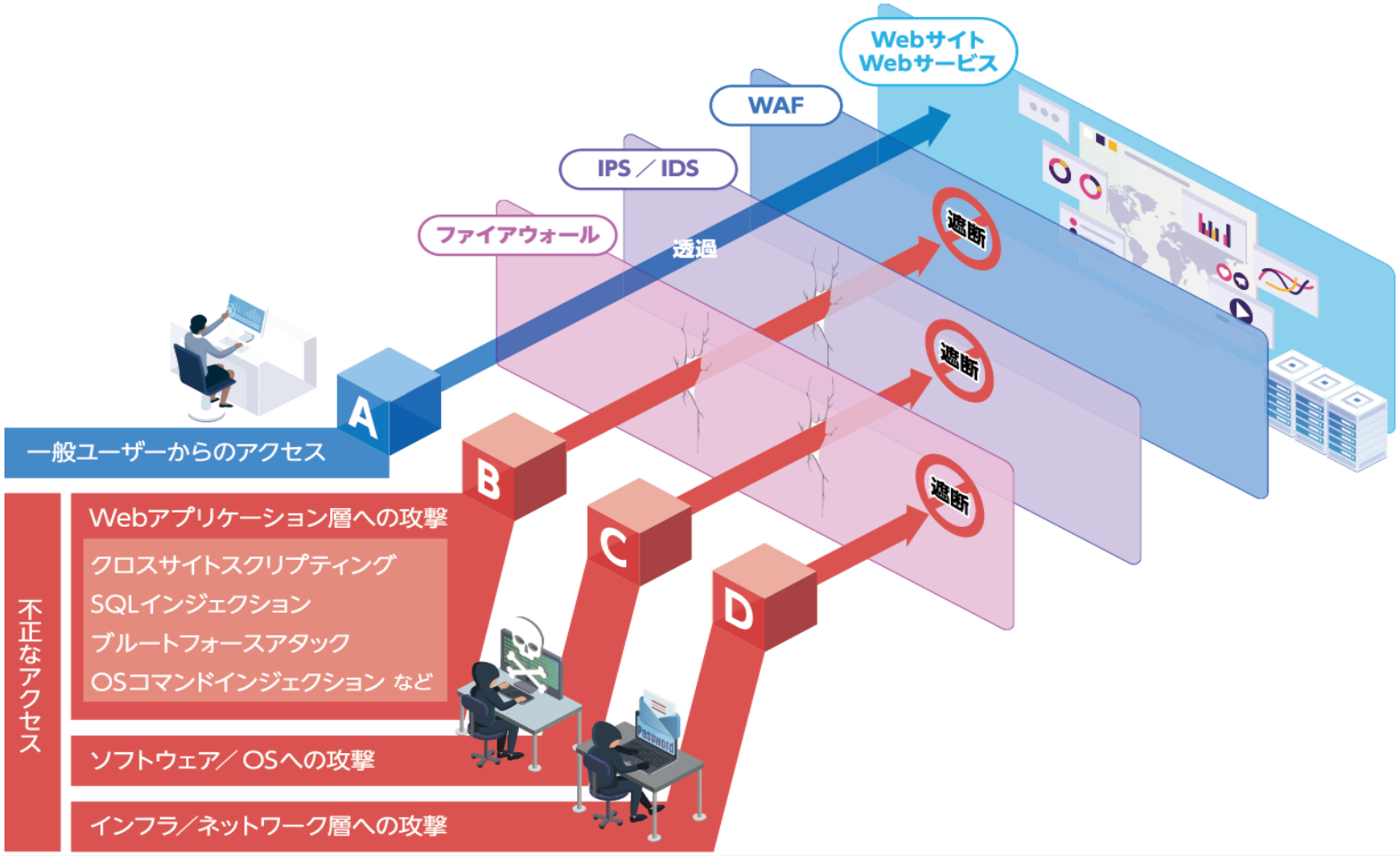


【LANシステム診断サービス】



クラウドWAFサービス

- クラウド型のWAF（Web Application Firewall）を用いたセキュリティサービスです。
- WAFは、Webサイトのアプリケーションに特化するファイアウォールで、アプリケーションデータの内容を解析します。これにより、WebサイトやWebサーバーへの攻撃を遮断し、情報漏えいやWeb改ざん、サーバーダウンを狙った攻撃などに対応します。

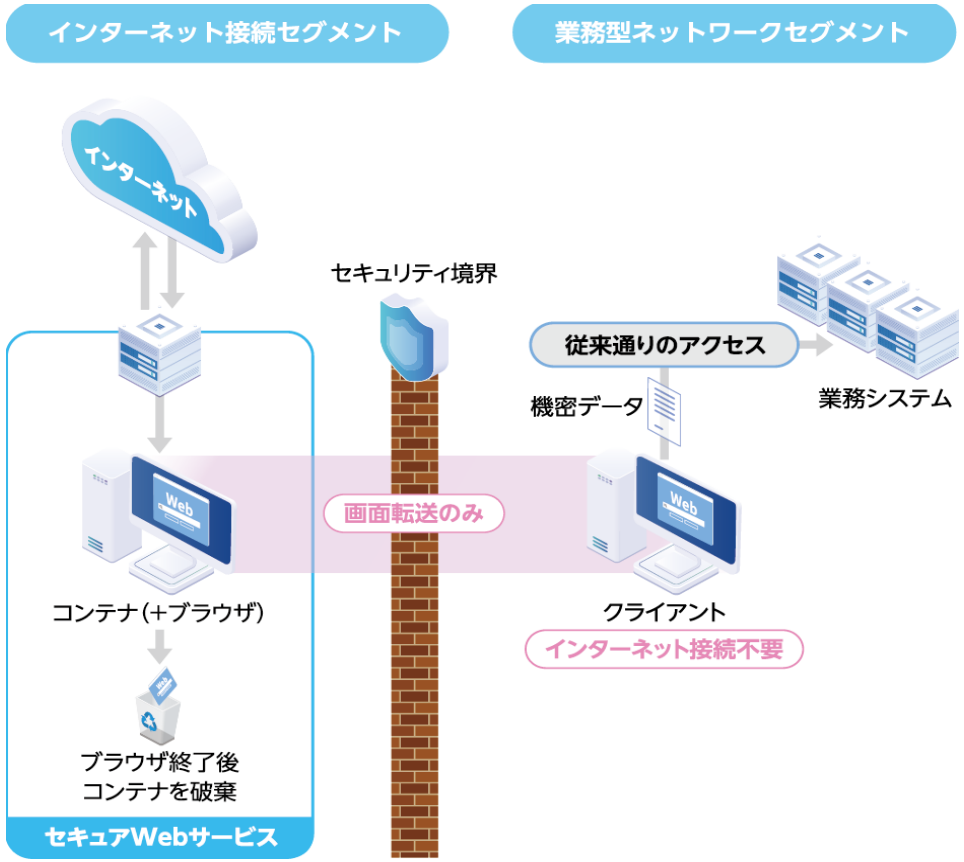


セキュアWeb/セキュアWebコンテナサービス

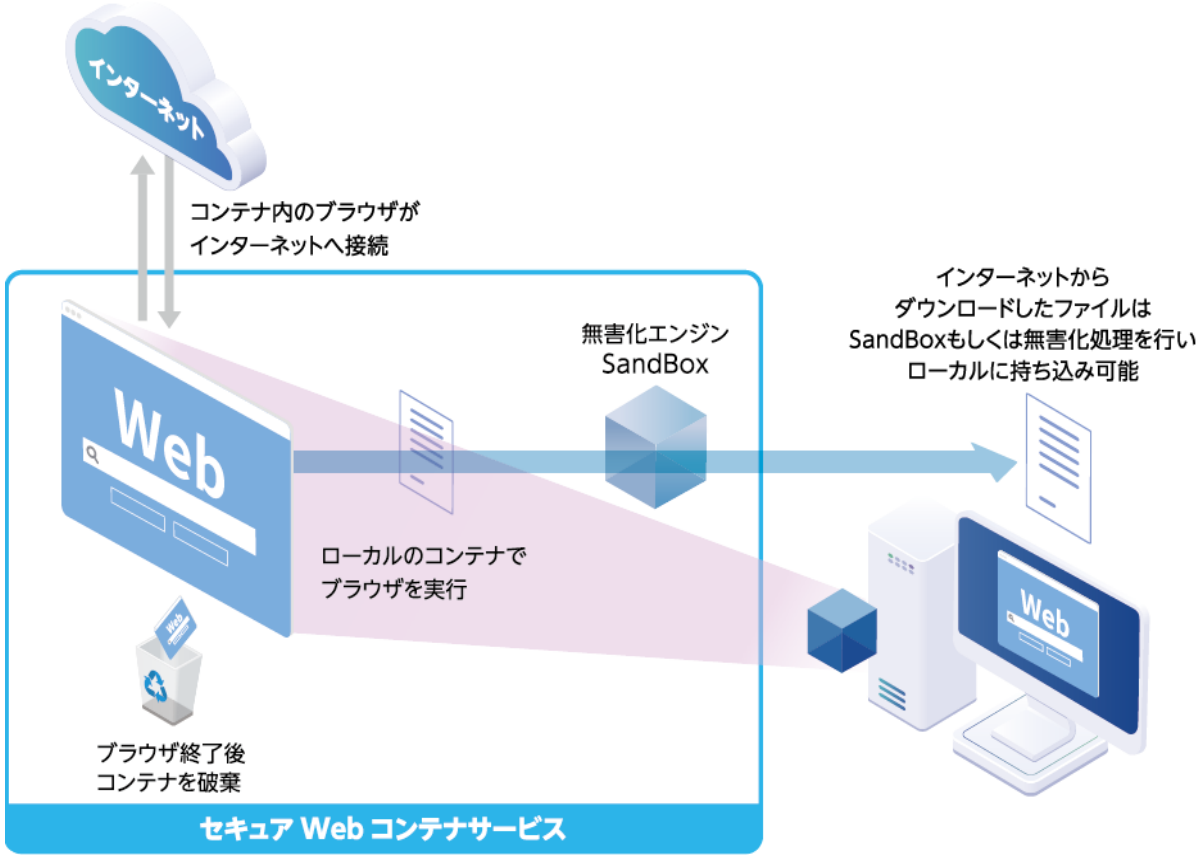
Net.CyberSecurity

- 業務系ネットワークとインターネット接続を仮想分離して、標的型攻撃やマルウェアの侵入を防ぐためのクラウド型サービスです。
- サーバーコンテナから画面のみを転送するセキュアWebサービスと、起動や表示の早いローカルコンテナを用いたセキュアWebコンテナサービスのいずれかを選ぶことができます。

【セキュアWebサービス】



【セキュアWebコンテナサービス】

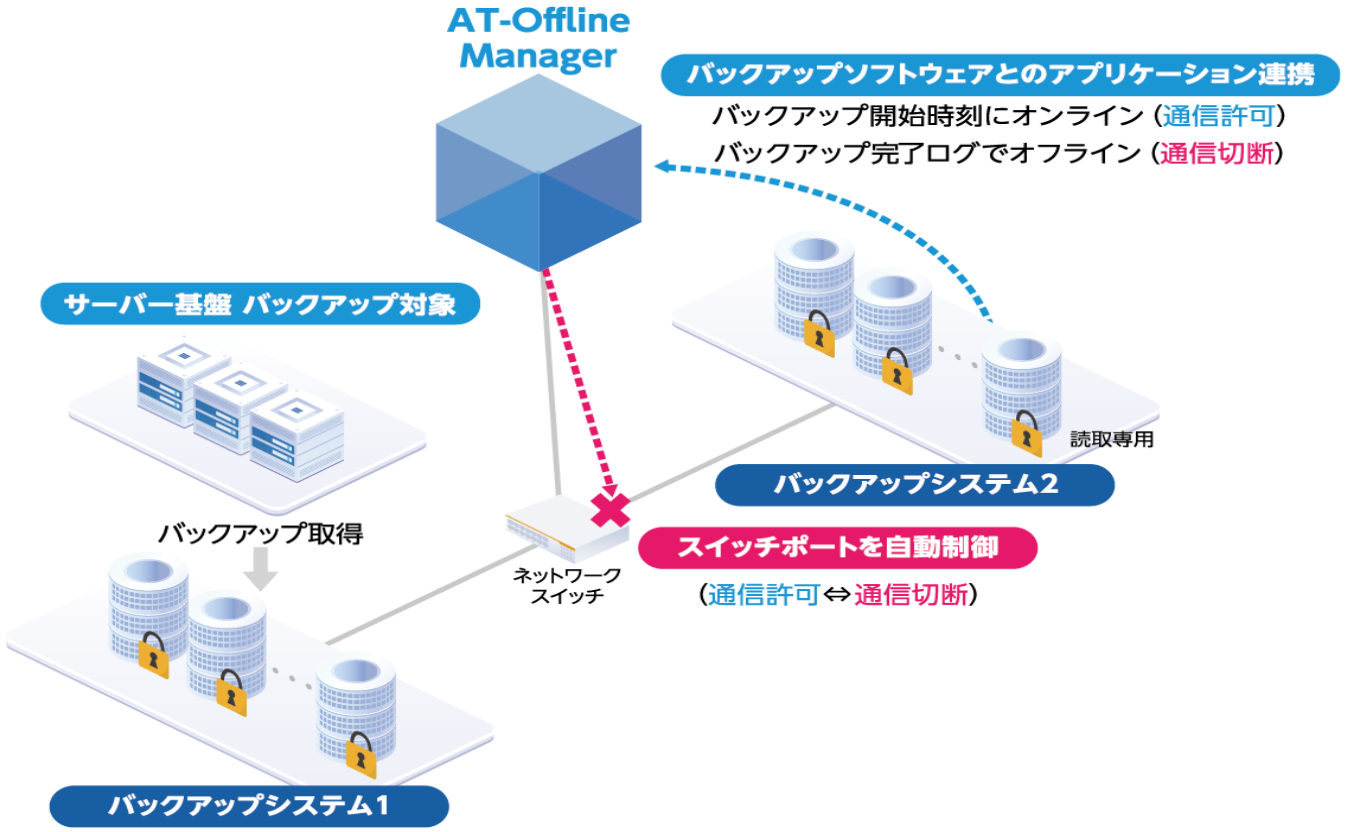


Allied Telesis

ランサムウェア対策オフラインバックアップソリューション

Net.Pro arcserve VEEAM

- ランサムウェア対策ではバックアップ環境が重要となりますが、PCや業務サーバーから直接アクセス可能なネットワークにバックアップ環境があると、バックアップ先まで感染し、暗号化されてしまうリスクが残ります。
- 本製品では、ランサムウェア対策のバックアップをネットワーク制御で自動的にオフライン化します。万が一被害に遭っても、ネットワーク経由での感染リスクを軽減することで、ランサムウェアに強いバックアップ環境を提供します。



Allied Telesis

セキュリティ製品の位置付け

■ 防御技術におけるセキュリティ製品の位置付けは、以下になります。

防御技術（対象機器）		セキュリティ製品
認証		ルーター製品(VPN) スイッチ製品、　無線LANアクセスポイント製品 クラウドUTMサービス
暗号化		ルーター製品(VPN) 、　無線LANアクセスポイント製品 クラウドUTMサービス
端末/ファイル/アプリケーションの保護	（全端末）	不正端末隔離サービス/感染端末検出サービス LANシステム診断サービス 脆弱性通知サービス フィッシングメール訓練サービス
	（Webサービス機器）	Webサーバー診断サービス クラウドWAFサービス クラウドID管理サービス セキュアWeb/セキュアWebコンテナサービス
	（サーバー機器）	ランサムウェア対策オフラインバックアップソリューション
トラフィック制御		ルーター製品 スイッチ製品
UTM		ルーター製品 クラウドUTMサービス マネージドセキュリティサービスMSS

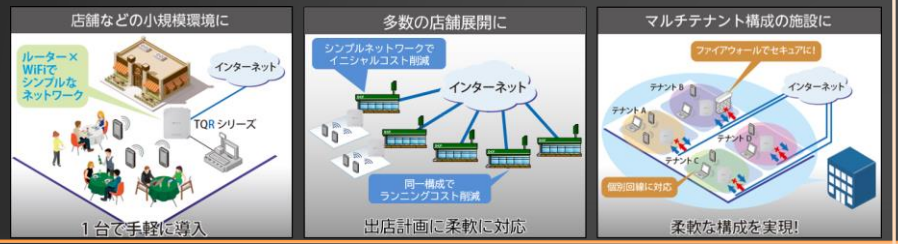
Appendix：ビデオデータシート&アライドラボのご案内

各種販促情報のご案内

新製品のご紹介(Wi-Fi6対応無線LANルーター)

AT-TQ6702 GEN2-R

- **Wi-Fi6とVPNルーターの機能を1台で提供**
- **エンタープライズ向け機能を搭載**
  - FirewallやダイナミックENAT、IPsec、VAP、Captive Portal、WPA3など各種エンタープライズ向け機能を搭載
- **AMF Plusによる一元管理に対応**
- **様々なネットワークに適用可能**
  - 小規模ブランチオフィス、コンビニエンスストアやレストランなどの店舗向けのネットワークなど、様々なネットワークをAT-TQ6702 GEN2-R 1台のみでシンプルな構成を組むことが可能



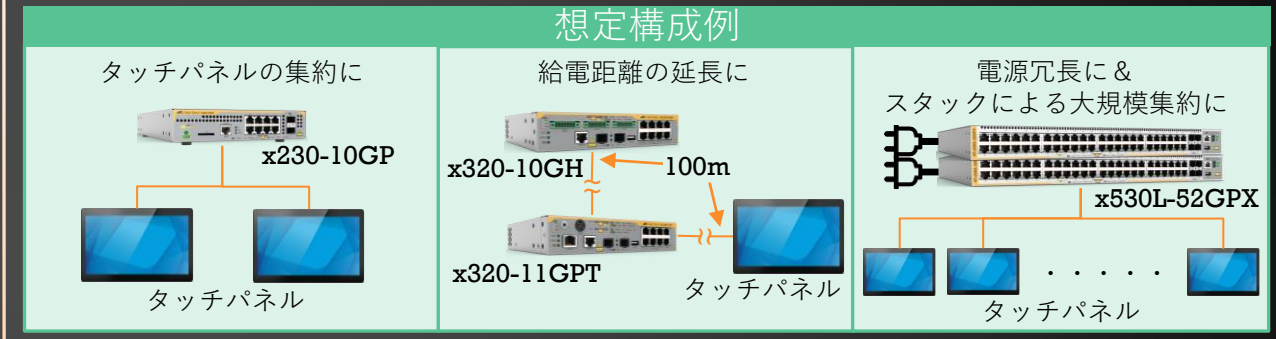
スイッチ製品協業ベンダーのご紹介

協業先：**タッチパネル・システムズ株式会社**

PoE対応タッチパネルと接続検証を実施！

検証機器：**x530L・x320・x230・AT-7101GHTm**

https://www.allied-telesis.co.jp/news/newsrelease/nr230324.html



Allied Labのご紹介

Allied Lab で検索！

アライドテレシスの技術を製品担当が分かりやすく紹介。

…第十回目：**Wi-Fi6**対応アクセスポイント比較検証
「失敗しない**Wi-Fi6**選びの手引き」

…第十一回目：統合型ネットワーク管理ソフトウェア
「**AT-Vista Manager EX**で**Network**管理者のお悩み大解決！」

…第十二回目：ネットワーク統合管理
「ネットワーク管理の手間をごそっと削減！」

…他、多数！

ビデオデータシートのご紹介

各種製品名 で検索！

製品の特長やユースケースなどを動画でご紹介します。

…**PoE++**対応マルチギガビットスイッチ
x530L GHXm シリーズ紹介

…オール**10G**レイヤー**2**スイッチ
XS910/8 紹介

…マルチギガビット対応**PoE++**インジェクター
AT-7101GHTm紹介

…他、多数！

ご清聴ありがとうございました。

Allied Telesis

今回ご紹介しましたセキュリティ製品に関して、
別途個別に相談がございましたら、お気軽に弊社
営業までお問い合わせください。