セキュリティ用語集

ICT-24セキュリティオペレーションサービス（ICT-24SOC）
補足説明資料

https://www.ntt-at.co.jp/product/ict24soc/

2025年3月

NTTアドバンステクノロジ株式会社

（セキュリティ用語集）前提

想定対象者：

・ネットワークの知識があり、セキュリティに関する知識を概念的に得たい人を対象としています。

・各項目については概念を理解することを優先して記述しています。

・詳細についてはより専門的な解説書や、機器メーカ・サービスプロバイダのマニュアル等を参照して下さい。

記述方法：

・各項目は全体像の理解を深めるために、詳細の説明を省略しています。

・説明文は分かり易さを優先しており、厳密でない場合があります。

・文章は適切な情報源に基づき、新たに書き起こしています。

本資料では、本資料名である「セキュリティ用語集」を「用語集」とも記載しています。

※ 記載されている会社名や製品名は、各社の商標または登録商標です。

（用語集）目次（1／6）

（用語集）目次（2／6）

（用語集）目次（3／6）

攻撃手法　・・・つづき

（用語集）目次（4／6）

（用語集）目次（5／6）

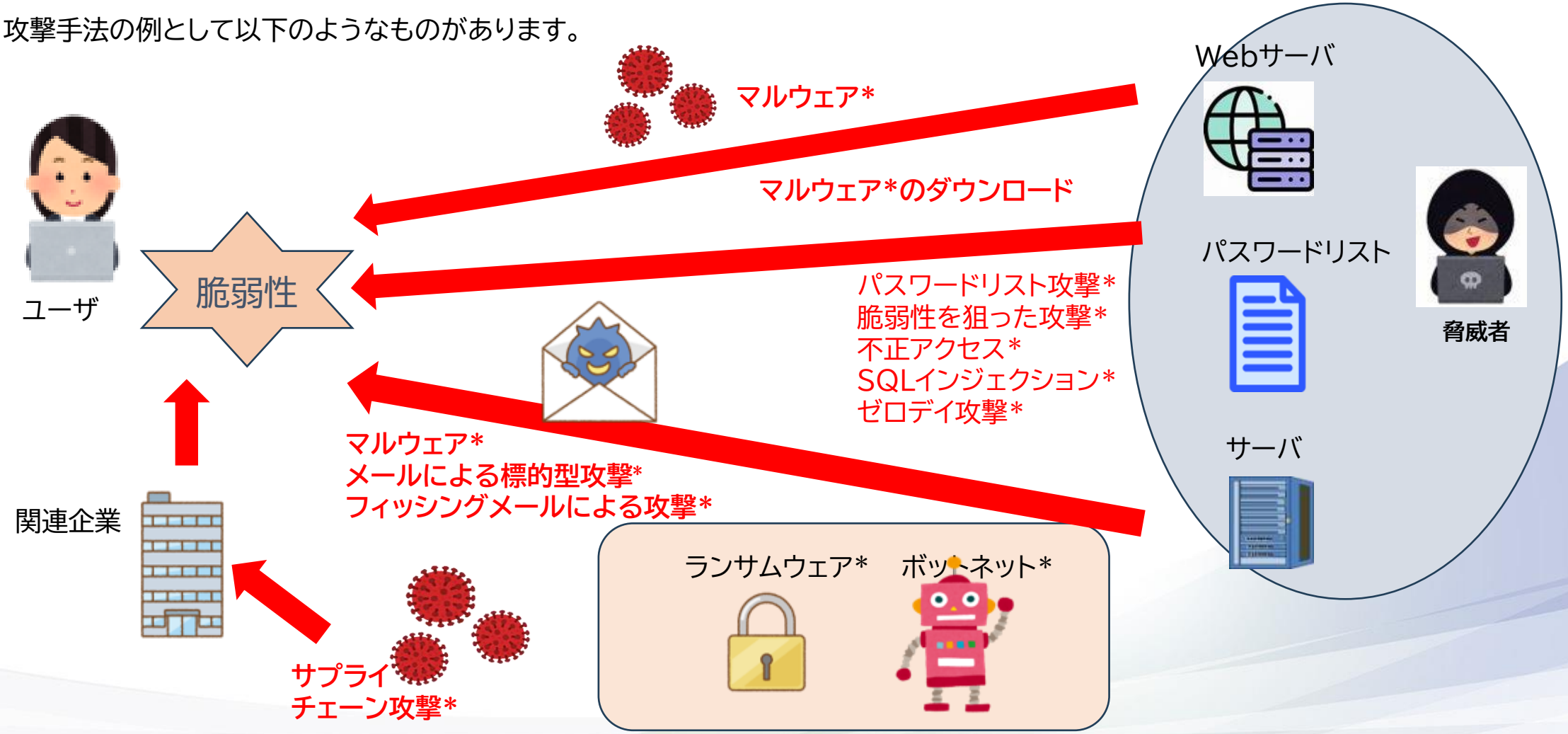
（用語集）目次（6／6）

（用語集）

概念図

（用語集）概念図(攻撃手法)

脅威者が行う攻撃手法の例として以下のようなものがあります。

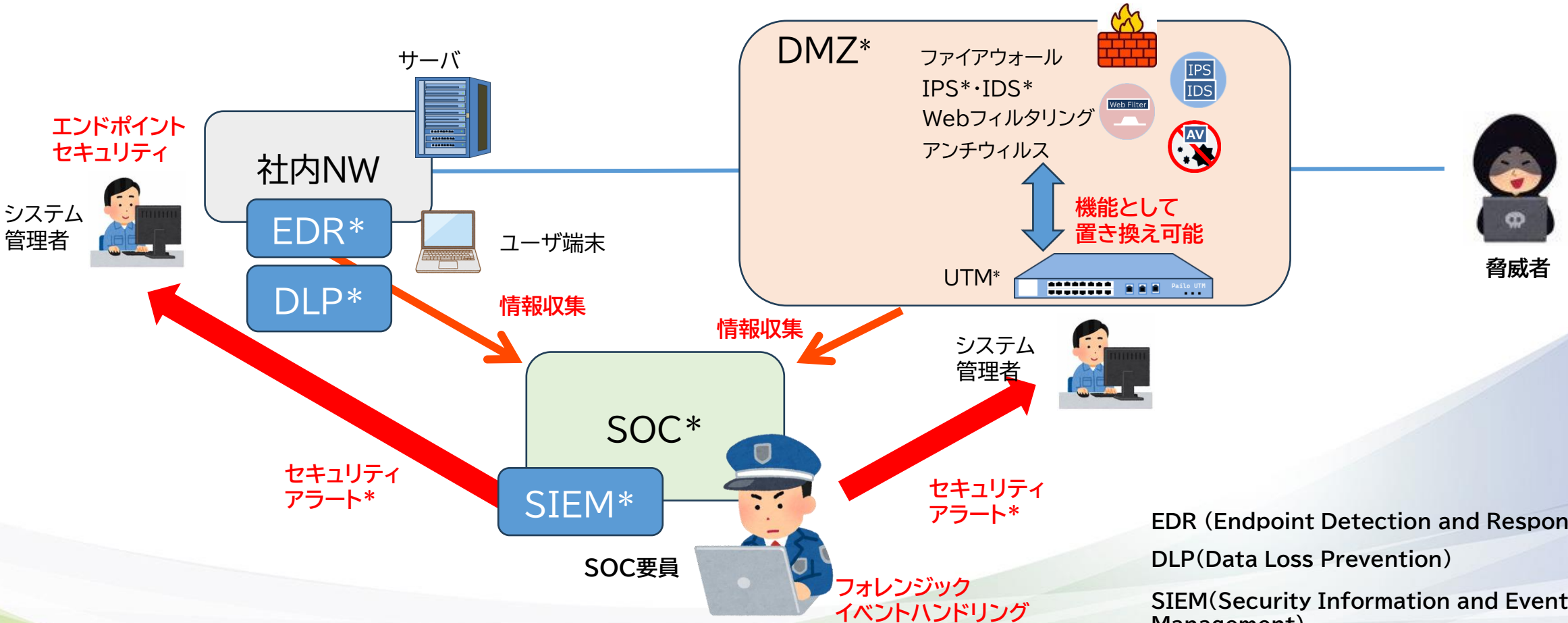


(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）概念図（防御手法）

脅威者が行う攻撃への防御手法例として、社内NW内に配置するユーザ端末、サーバに設置するEDR*、DLP*や、DMZ*に設置するUTM*、ファイアウォール*、IPS*、IDS*等、これらをSOC*で監視するためのSIEM*等が使われます。



EDR（Endpoint Detection and Response）

DLP（Data Loss Prevention）

SIEM（Security Information and Event Management）

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

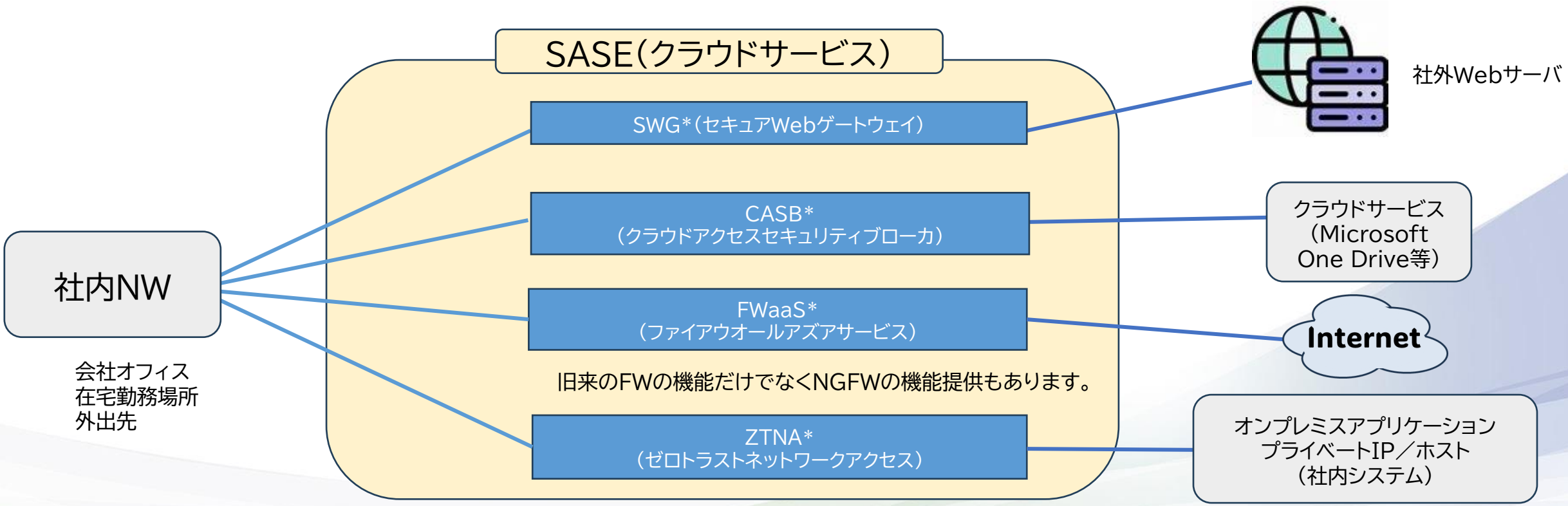
*） 詳細は「用語集」を参照して下さい

（用語集）概念図（SASE）

SASE（サシー - Secure Access Service Edge）は、ネットワーク機能、セキュリティ機能を1つのクラウドサービスで提供するものです。

この概念は2019年に米国の調査会社ガートナー（Gartner）社が提唱しました。

テレワークなどの普及で境界型セキュリティ対策*では安全性確保が複雑になったこと、情報システム担当者の業務負荷が増大していることへの対応からSASEが注目されるようになりました。



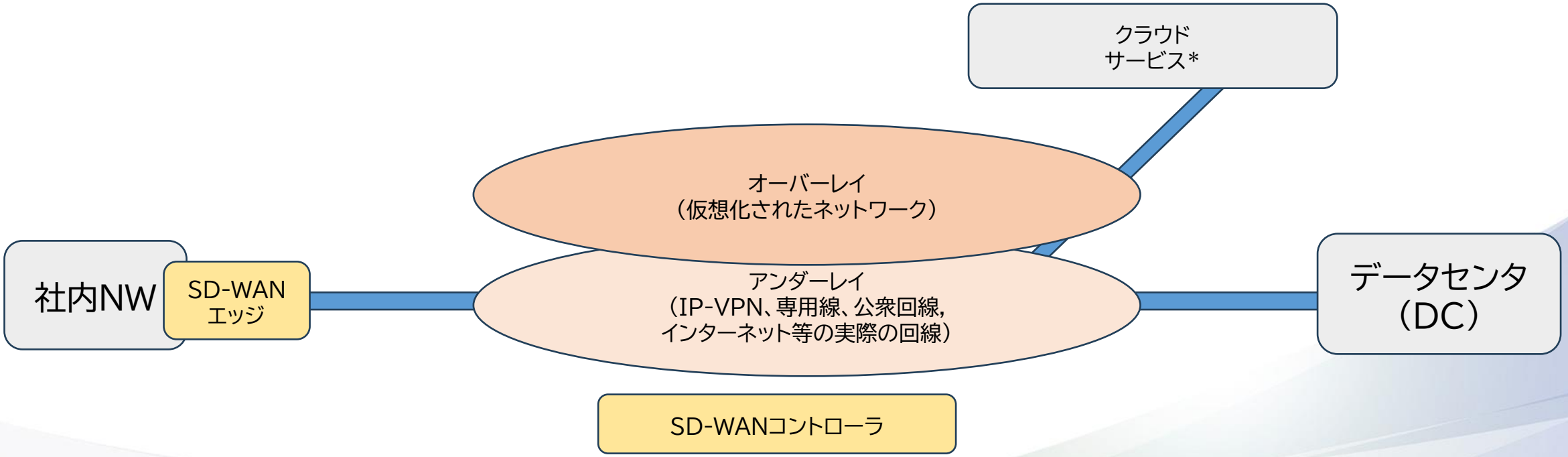
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）概念図（SD-WANの基本）

SD-WAN*（Software Defined Wide Area Networking）はソフトウェアによって仮想的な広域ネットワークを構成するものです。

実際に使用している回線の種別（専用線、LTE等のモバイル回線等）にかかわらず企業WANを構成できるようになります。これらの回線をアンダーレイ回線として用い、これらを仮想化したオーバレイ回線としてメインの回線、バックアップ回線等を設定できます。



（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）

脅威・脆弱性・リスク

（用語集）脅威・脆弱性・リスクの関係

セキュリティ上の脅威、脆弱性、リスクは各々次の通りです。

・**脅威**：情報システムに害を与える事象を言います。

・**脆弱性**：脅威をもたらす攻撃に弱い状態を言います。

・**リスク**：脅威により脆弱性を突かれて侵入され、情報窃取などの被害を受けることを言います。

リスクは、**脅威が発生**し、その脅威に対する**脆弱性が存在**するときに**発生**することとなります。

（具体的な例として、10mの津波が発生する可能性に対して、5mの防潮堤では洪水のリスクがありますが、15mではリスクは低減されます。）

- 「脅威」、「脆弱性」が存在すると「リスク」が発生する
- 「脅威」が存在しても「脆弱性」が低減されている場合は「リスク」も低減される

リスクの低減には次が有効です。
・脅威の低減（エアギャップ等脅威者からのアクセスを制限）
・脆弱性の低減（ソフトウェアのアップデート、防御機能の実装等）

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

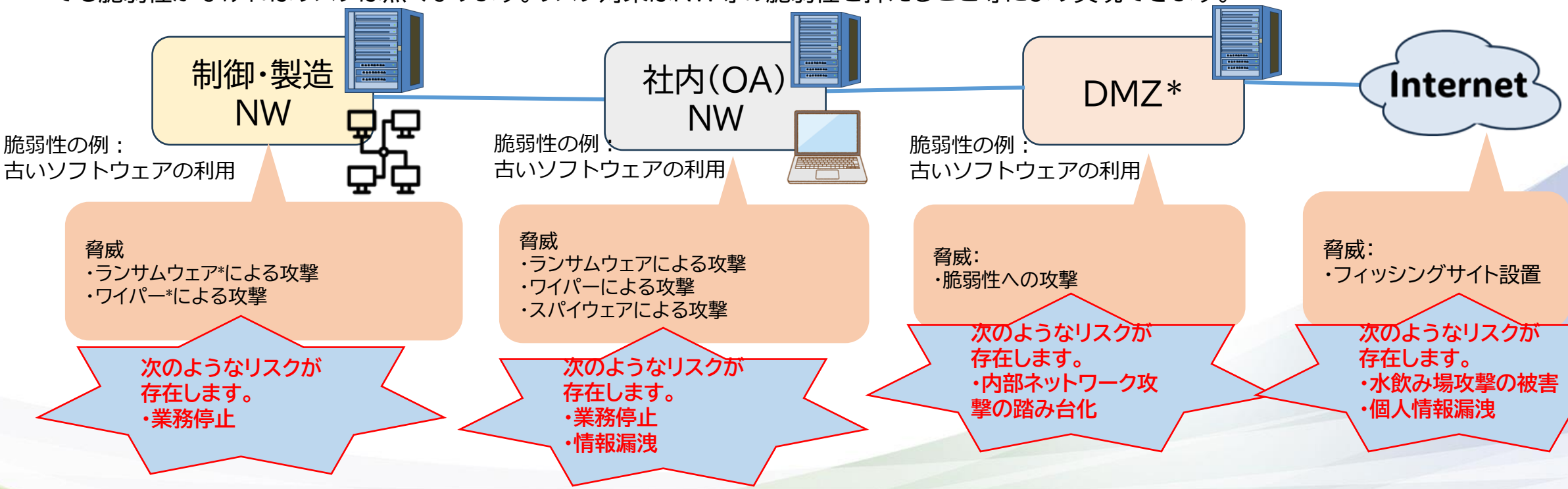
*） 詳細は「用語集」を参照して下さい

（用語集）セキュリティ上の脅威

一般的な組織のネットワーク（NW）における、脅威、脆弱性、リスクの例を示します。

NWの各箇所に対する脅威、脆弱性、リスクの例を示します。

脅威は悪意のある攻撃者から攻撃される可能性、脆弱性はNW等のもろさ、リスクはこれらにより受ける損害の可能性を示します。脅威が有っても脆弱性がなければリスクは無くなります。リスク対策はNW等の脆弱性を抑えること等により実現できます。



（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）脅威者の目的

脅威者がサイバー攻撃を行う目的には、金銭窃取、国家の利益のための他国に対する諜報活動、産業スパイ、影響工作、破壊活動等があります。

これらは犯罪者グループ、国家支援の脅威者等により実行されます。

脅威者

- 金銭窃取
  - 主にサイバー犯罪組織が資金を得るために行ってきましたが、近年、Z国の国家支援脅威者Lazarusによる、兵器開発のための外貨稼ぎ、Y国軍に関係する脅威者の小遣い稼ぎと思われる活動も確認されています。
- 他国への諜報活動
  - 敵対関係にある国の政府関係者に対する情報収集等の活動です。X国の国家支援脅威者が隣国との紛争に関係し、西側諸国の外交官を装ってNATO加盟国の政府関係者に接触し、外交政策、国防計画等の情報を窃取しようとした例が有ります。
- 産業スパイ
  - 企業の秘密情報を盗み出す活動です。例えばY国の脅威者からと見られる、Y国のIPアドレスからの侵入が2020年11月に三菱電機に対して有りました。
- 影響工作
  - 影響工作（Influence Operation）は「特定の政治的、社会的、経済的目標を達成するために標的となる個人、集団の認識や行動を意図的に変えることを目的とした活動」で、X国、Y国による敵対国家に対する偽情報流布などが有りました。
- 破壊活動（ワイパー型）
  - 標的となった組織のシステムを破壊し、業務を停止させることを目的としています。X国によるその隣国への侵攻に関連して、隣国のエネルギー企業を標的として産業用制御システムのディスクを消去し、大規模停電に繋げたマルウェアIndustroyerが使われた例が有ります。

(注)APT：Adanced Persistent Threat – 高度で長期間にわたる脅威

(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）脅威者の例（X国）

X国は対外情報庁（SVR - 対外諜報を担当していた旧KGBの後継組織）、X国連邦軍参謀本部情報総局（GRU）、およびこれらの関連グループが主な脅威者グループです。

これらの脅威者グループはインターネットを含む広い範囲で諜報活動等を行っています。

X国の脅威者

脅威者の特徴	SVRに関係する脅威者グループにはAPT29が有ります。GRUの傘下の85th Special Service Center（GTsSS）の26165部隊（別名Fancy Bear、Fighting Ursa）、29155部隊（別名Ember Bear、Cadet Blizzard、UAC-0056）に関係する脅威者グループとしてAPT28が有ります。
サイバー攻撃例	・SVRに関連したものとして、スピアフィッシング*の手法等を用い、外国政府の政策・経済情報・軍事情報、科学技術情報、外国政府の諜報・防諜活動情報を調査・窃取する活動等が有ります。 ・GRUの26165部隊はウクライナ紛争に係る攻撃、国家としての情報戦、オリンピックの反ドーピング調査・報道妨害、英国における暗殺未遂事件捜査の妨害、米国・フランス・ドイツの選挙プロセスへの影響行使のためのサイバー攻撃を行いました。
インターネット利用環境	・X国政府は独自OSであるRed OS（CentOS/RHEL系）、Astra Linux等の利用を推奨しています。 ・X国は国内からのFacebook等へのアクセスをブロックしています。2020年以降X国で販売されるスマホには政府が指定する特定のアプリのインストールが義務付けられています。X国外のインターネットから国内ンっとワークの切り離し実験を複数回行っています。

(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

(注)APT：Adanced Persistent Threat – 高度で長期間にわたる脅威

（用語集）脅威者の例（Y国）

Y国は国家支援の脅威者が国外への情報窃取・産業スパイ等の多彩なサイバー攻撃活動を行っていることが知られています。また、国として大規模な情報のブロック等を行うGreat Firewall、トラフィックを監視してマルウェアを埋め込んだりDDoS攻撃を行うGreat Cannon等を運営しています。

Y国は国の計画として国産の大型旅客機の開発プロジェクトを立ち上げた後、エアバス社の関連企業への侵害が行われる等公開された方針と似た攻撃が行われる場合が有ります。

Y国の脅威者

脅威者の特徴	2015年にサイバー戦、電子戦、宇宙空間における作戦を含む情報戦を統括する戦略支援部隊が設立されました。その後2024年に同部隊は解体され、ネットワーク空間部隊（サイバー）が設立されました。これらおよび中国安全部（MSS - Ministry of State Security）が中国の脅威者に関与しています。
サイバー攻撃例	・2010年頃：Y国のBlack Tech（別名Earth Hundun、Palmerworm）は台湾、日本、香港・米国等の政府、産業、技術、メディ等を標的に情報窃取を行いました。 ・2020年11月：日本のM社の子会社が使用するクラウドサービスへのサイバー攻撃が中国のIPアドレスから行われました。
インターネット利用環境	・Great Firewall（金盾 - きんじゅん）：Y国政府により運営されているインターネットの検閲・監視機能を言います。Y国政府が隠蔽しようとしている文言をブロックする等しています。 ・Great Cannon：Y国政府の運営するサイバー攻撃システムです。トラフィックを監視し、特定の標的にマルウェアを植え付ける、DDoS攻撃を行う等をします。 ・Y国は独自OSとしてKylinを使用しています。

(注)APT：Adanced Persistent Threat – 高度で長期間にわたる脅威

(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）脅威者の例（Z国）

Z国の国家支援の脅威者としてZ国軍傘下の組織が有ります。

この組織は対外的な諜報活動等を行う組織で、サイバー攻撃も担当しています。隣国のK国その他の国に対する諜報活動や、外貨獲得活動が行われています。2013年2月にはK国の金融機関・放送局の多くのコンピュータを停止させる攻撃を行いました。この準備のためにフィッシングサイト*等を経由してあらかじめ主要なコンピュータにマルウェア*を仕込み、一斉に動作させる手口が使われました。

Z国の脅威者

脅威者の特徴	よく知られている脅威者グループとしてラザルスグループ（Lazarus Group）が有ります。なりすまし、正規に見える企業（フロント企業）を隠れ蓑にして悪意ある活動等を行います。別名としてHidden Cobra、APT38が有ります。Z国の複数の脅威者グループはサイバー攻撃に使用するインフラを共用する傾向が有ります。利用するマルウェアにはWannaCry等が有ります。 国連のZ国専門委員会での調査によるとZ国はサイバー攻撃により30憶ドルの資金を不正に窃取し核開発計画等に利用しているとしています。
サイバー攻撃例：	・2015年頃、LazarusがB国の中央銀行から資金窃取のために国際銀行間通信協会（SWIFT）の通信設備を侵害して悪用しました。 ・2022年頃、Lazarusが日本の暗号資産関連企業、取引所を標的としたと報道されました。
インターネット利用環境	・インターネットアクセスは政府用等の特別許可がある場合や、外国人のみに許されています。一般国民は国内専用の光明ネットワーク（Kwangmyong）のみ使用出来ます。 ・Z国の開発したOSとしてRed Star OSというLinuxベースのOSが使われています。そのバージョン3.0はmacOSに似たUIが使われています。

(注)APT：Adanced Persistent Threat – 高度で長期間にわたる脅威

(注)説明文は分かり易さを優先したため、厳密でない場合があります。

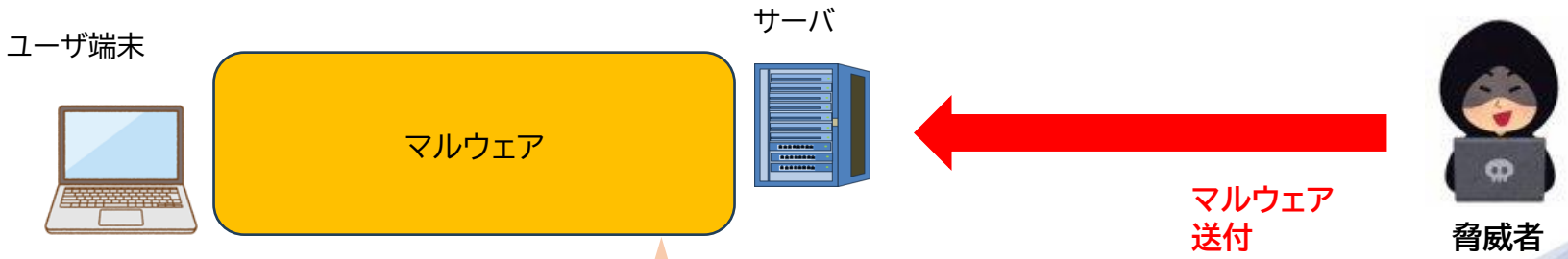
*） 詳細は「用語集」を参照して下さい

攻撃手法

（用語集）マルウェア

マルウェア（Malware）はウィルス、ワーム、トロイの木馬*、スパイウェア*等のユーザの意図と異なる悪意のある動きをするプログラムを言います。

マルウェアのうち、ウィルスは感染対象のソフトウェアに感染して活動するマルウェアです。ワームは単独で活動が可能で自身を複製して増殖してゆくものを言います。トロイの木馬は他の正規のプログラムに偽装して活動するマルウェアです。スパイウェアはPC等に密かにインストールされ、ユーザの個人情報等を収集するマルウェアです。



マルウェアによる主なリスクには以下があります。
・個人情報等の秘密情報窃取
・ファイルの改ざん
・デバイスが乗っ取られ、組織内・他組織への攻撃の踏み台になる
・ボット*による感染

マルウェアは次の方法等で感染する場合があります。
・メールの添付ファイル
・開放ポートの脆弱性を使用するなど、ネットワーク経由で侵入
・フィッシングサイト*等の不正サイトへのアクセスにより感染
・ソフトウェアの脆弱性を突いて侵入

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

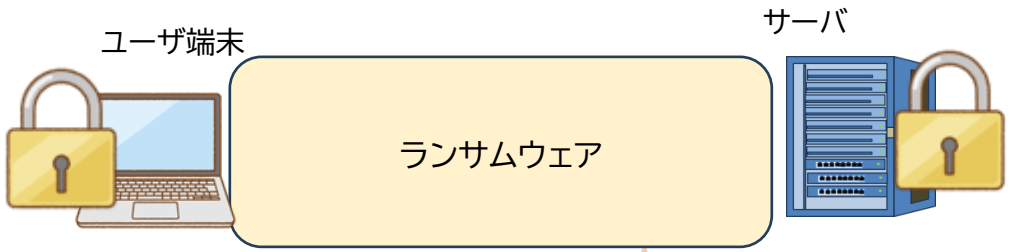
*） 詳細は「用語集」を参照して下さい

（用語集）ランサムウェア

ランサムウェア（Ransomware）は被害を受けた組織の重要なデータを暗号化したり、PCをロックしたりして使用不能にし、それらの解除を引き換えに身代金を請求するマルウェアです。

「暗号化したデータを復号」するために身代金を要求するだけでなく、「身代金を支払わないとデータを公開する」と更に脅迫する二重脅迫（Double Extortion）が行われる場合もあります。身代金の支払いには第三者の口座を経由した金銭や、やり取りが匿名化できる暗号資産などでの請求がされる場合があります。

ランサムウェアによる攻撃を受けた場合、次のようなリスクにも留意が必要です。
・ばらまき型の攻撃を受けた場合：金銭目的での新たな攻撃を受ける可能性があります。
・標的型の攻撃を受けた場合：脅威者が標的とした情報の窃取のために繰り返し、新たな標的型攻撃を受ける可能性があります。



警告！

あなたの大切なデータは暗号化されてしまいました。
これを修復するためには＄300相当の支払いが必要です。
制限時間を過ぎると、データは完全に失われます。

ランサムウェアからのメッセージ（イメージ）

ランサムウェアの主な感染経路には次があります。
・メール添付ファイル
・悪意のあるWebサイト
・VPN機器経由
・リモートデスクトップ経由

主な防御方法は次の通りです。
・従業員への教育
・セキュリティパッチの適用、OS等の最新化

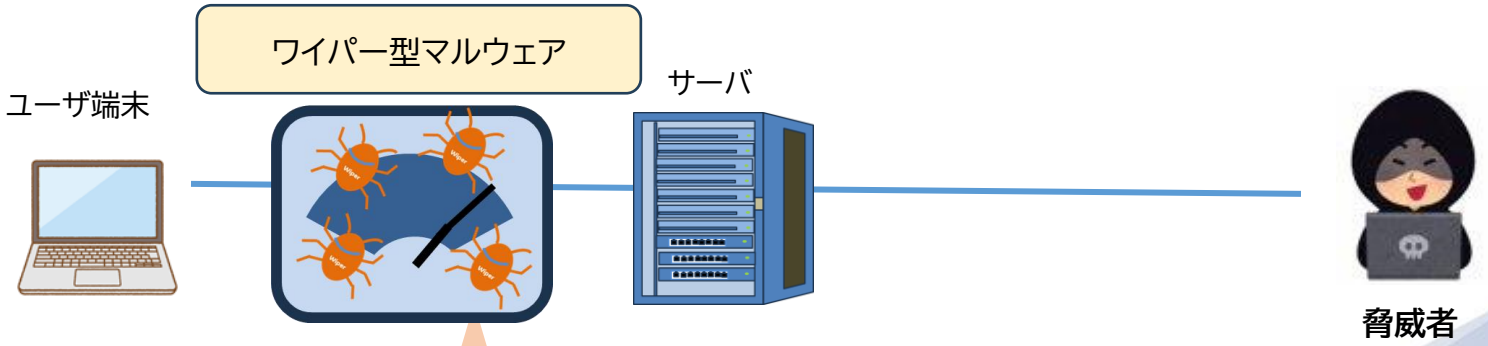
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）ワイパー型マルウェア

ワイパー(Wiper)型マルウェアは標的となったシステムを使用不能にすることを目的としています。

具体的な例として、サウジアラビアのエネルギー企業サウジアラムコを狙ったマルウェア「Shamoon」等があります。情報窃取した後情報を消去します。



ワイパー型マルウェアの特徴として以下があります。
・不正ソフトウェアを経由しての感染、悪性サイトの閲覧等多様な経路で感染する場合があります。
・機能として最終的にディスク上のデータを破壊したり削除したりします。

ランサムウェアのように身代金を要求してそれが支払われても復元用鍵を引き渡さない等の業務妨害等が真の目的であるワイパー型マルウェアも存在します。

ワイパー型マルウェアによるリスクは次の通りです。
・情報奪取を伴う場合があるため情報漏洩のリスクが存在
・業務妨害等を目的とした攻撃の可能性があり、業務継続上のリスクが存在

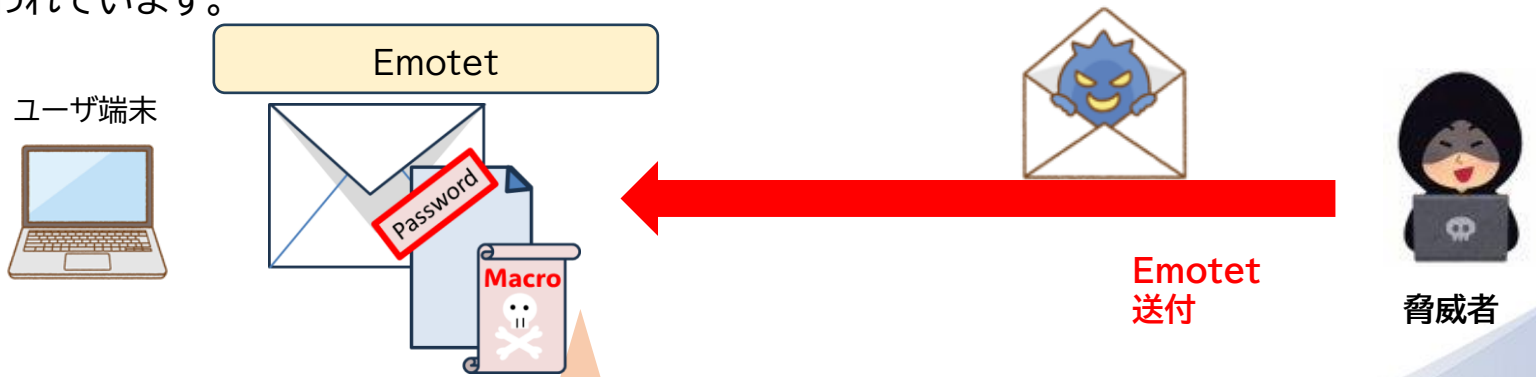
(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）Emotet（マルウェア）

Emotetは主に電子メールの添付ファイルを介して感染するマルウェアです。感染後はボットネットとして動作したり、他のマルウェアを更に感染させたりします。

Emotetの作者は感染したコンピュータを使用してボットネットを構成し、これをDoS攻撃等を行うためのインフラとして販売していたことが知られています。欧州刑事警察機構EUROPOL等がドイツ等に置かれていたC＆Cサーバを停止させ一旦は壊滅させられましたが、現在でもEmotetに感染させる攻撃は継続して行われています。



Emotetによる被害を防ぐには下記等があります。
・従業員へ手口や対策を周知
・メールのセキュリティ対策強化

Emotetは次により感染します。
・悪性なマクロを含む添付ファイル
・パスワード付きZIPファイルを悪用し、ウイルス対策ソフトによる検知を回避
・正規のメールのやり取に割り込んだり、内容を装うなどで正規の返信を偽装
・Microsoft OneNoteを悪用してファイルを転送

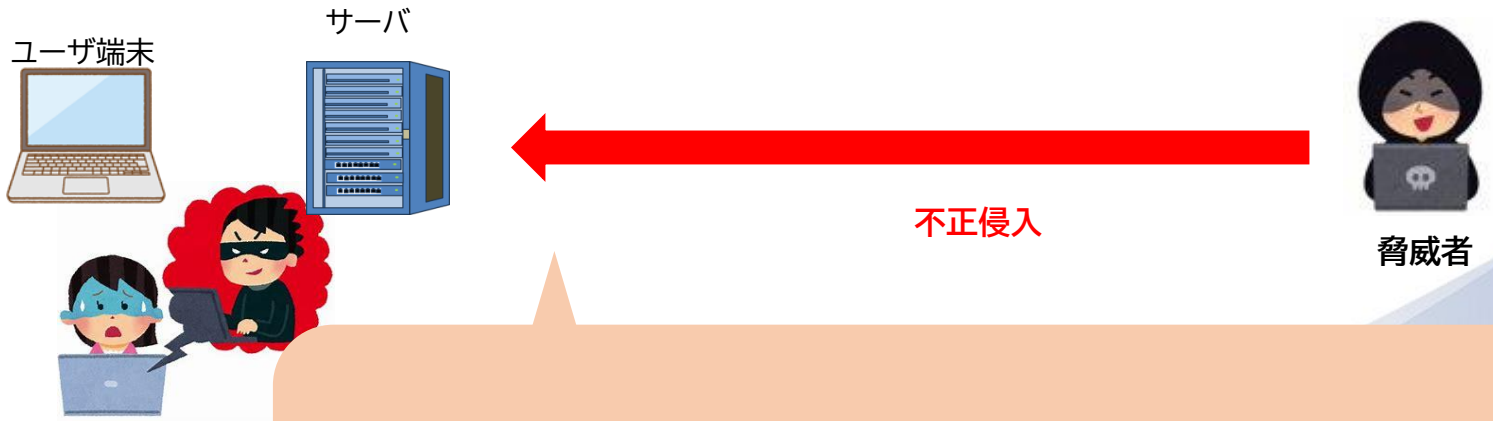
(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）不正アクセス

不正アクセスは、アクセス権限のない脅威者が端末やサーバ等に侵入する攻撃を言います。

不正アクセスを受けた場合、Webサイトの改ざん、ウイルス感染、システム停止、機密データ・個人データの漏洩、データ・ファイルの消去・窃取、データの暗号化と身代金請求、再度侵入可能となるバックドアの設置等が行われる場合があります。



不正アクセスの被害にあわないために次のような対策が有効です。
・認証情報を窃取されないよう、不審なWebサイトにID、パスワードなどを入力しない
・セキュリティホールを防ぐためにOSなどの最新化、パッチ適用を行う

不正アクセスの手口として次のようなものもあります。
・組織が利用しているクラウドサービスへの不正アクセス
・認証情報窃取（フィッシング、水飲み場攻撃、キーボードロギング等による）
・セキュリティ脆弱性への攻撃（SQLインジェクション、OSコマンドインジェクション、ルートキット攻撃、バッファオーバフロー攻撃等による）

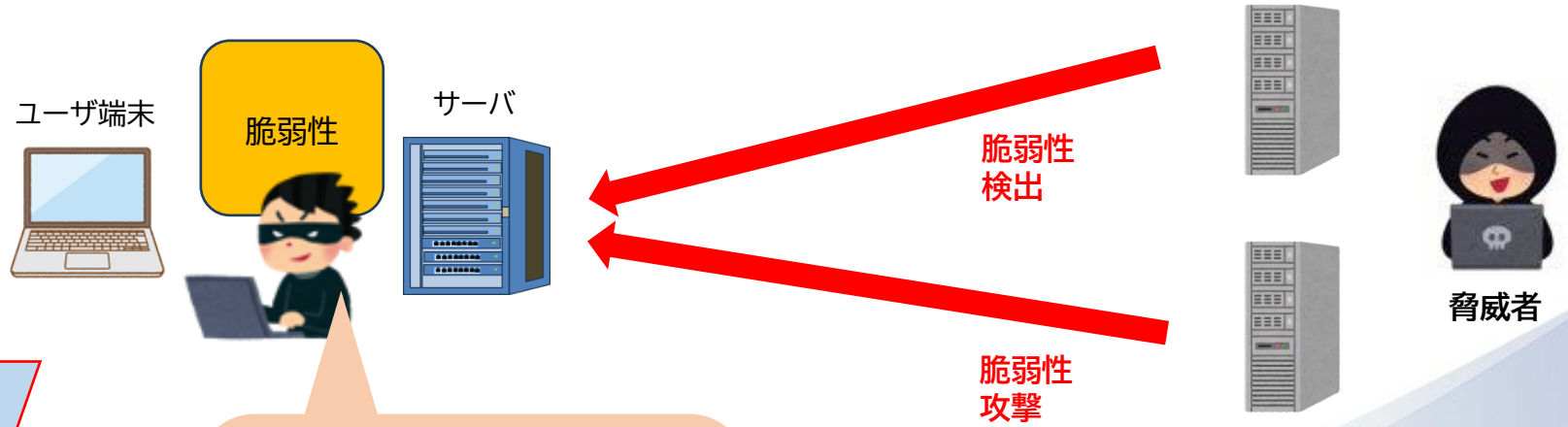
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）脆弱性を狙った攻撃

脆弱性を狙った攻撃は、ユーザ端末、サーバに存在する脆弱性（ソフトウェア、ハードウェア等に存在する欠陥）を突く攻撃です。

脆弱性を狙う攻撃には例えば、クロスサイトスクリプティング（XSS）、クロスサイトリクエストフォージェリ（CSRF）、バッファオーバフロー攻撃、ディレクトリ・トラバーサル攻撃等があります。これらはプログラミングの不備、設定の不備、古いバージョンのソフトウェアの存在等が原因で生じた脆弱性を狙うもので、脅威者により利用者が想定していない操作が行われます。



脆弱性を突かれた攻撃を受けないためには次のような対策が有効です。
・OS,アプリケーションの最新化
・アノマリ検知機能のあるIPS
などを利用（ゼロデイ脆弱性に有効な場合があります）

脅威者は脆弱性のあるシステムを検出・選択・攻撃、もしくは検出せずに最初から攻撃コードを使った攻撃を試みます。
ユーザ端末を攻撃する場合、NW機器等の脆弱性を使用してこれらを踏み台として利用する場合もあります。

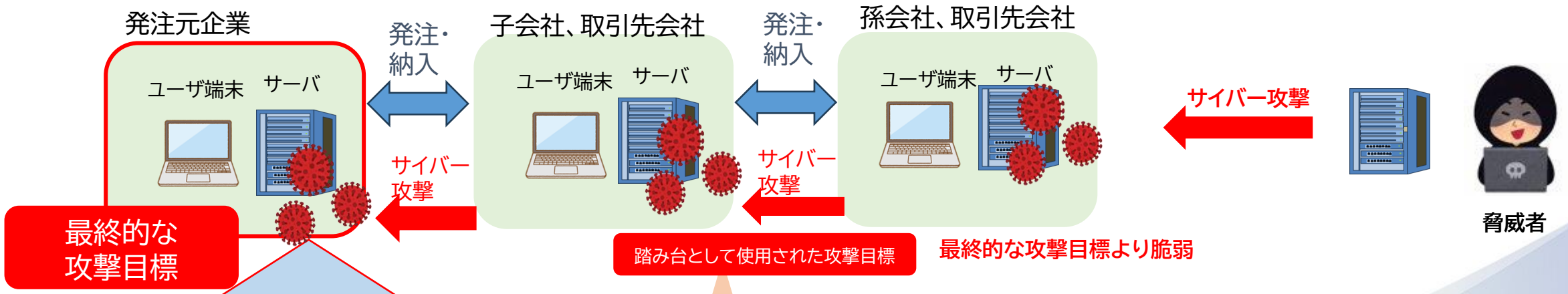
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）サプライチェーン攻撃

サプライチェーン攻撃は、企業等の組織間の業務上の関係を悪用してサイバー攻撃の踏み台として利用する攻撃です。

セキュリティレベルの高い企業を攻撃目標としたとき、それよりもセキュリティレベルの低い取引先や子会社、更にはそれらからの取引先を経由することで侵入が容易となる場合があります。複数の中・小規模の企業が侵害の対象となったとき、実はそれらに関連する大企業が最終的な攻撃目標であったことが判明する場合もあります。



サプライチェーン攻撃を受けた場合のリスク等は次の通りです。
・被害が自社だけでなく取引先等他の組織に及ぶ
・関連企業のセキュリティ対策の監査により自社へのサイバー攻撃を予防

サプライチェーン攻撃には次のようなものがあります。
・ソフトウェアサプライチェーン攻撃：ソフトウェアの製造工程、提供工程に対して侵害するものです。オープンソースコードや、アップデートコードに悪意あるコードを混在させて標的とする組織のソフトウェアに侵入します。
・サービスサプライチェーン攻撃：マネージドサービスプロバイダなどのサービス事業者を侵害し、その顧客企業に対してマルウェアを配布するものです。
・ビジネスサプライチェーン攻撃：標的となる企業の関連組織、子会社、取引先を侵害し、怪しまれにくい業務上の繋がりを利用して標的組織に侵入します。

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

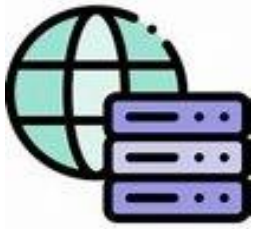
（用語集）SQLインジェクション

SQLインジェクションは、Webサーバの入力フォームに脅威者がDBアクセス用のコマンドであるSQL文を含む文字列を入力することでDBの操作を行う攻撃です。Webサーバが入力フォームの入力に対するチェックを怠る等の脆弱性が存在する場合にリスクとなります。

標的となったWebサーバ

ソースプログラム

```
sqlstring = ”select * from
 nameTable where id =  ’” +
 InputName + ”’”
```



SQLインジェクション攻撃

脅威者

入力文字列

John’;drop table nameTable--

実行されるSQL文

1文目：select * from nameTable where id = John
2文目：drop table nametable（以下コメント）

上記例は下記のように動作します。
・本来の動作：
　入力された文字列の名前のレコードをDBから抽出
・脅威者の入力した文字列による動作：
　名前Johnのレコードを選択する。また、テーブルnameTableを削除する。

対処方法として、入力データから”;”等の記号を削除する等があります。

SQLインジェクションの脆弱性があると次のリスクが存在することになります。
・脅威者がWebサーバのプログラムと同じ権限でマルウェアを実行可能

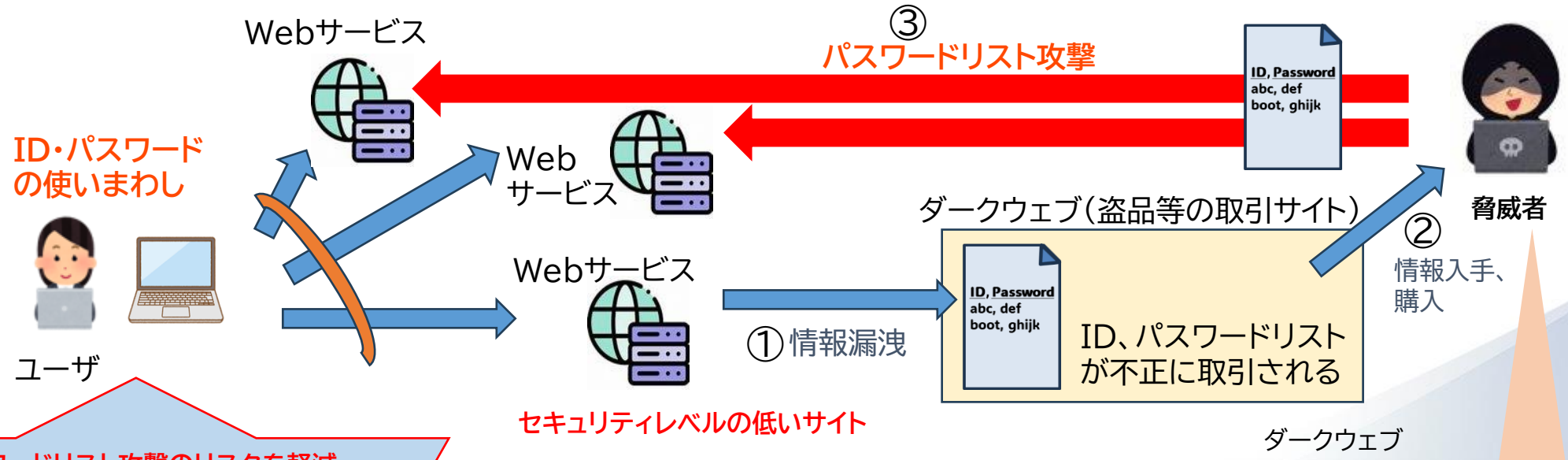
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）パスワードリスト攻撃

パスワードリスト攻撃は、脅威者が入手したIDとパスワードのリストを使用して、インターネットに公開しているサービスへの不正アクセスを試みるものです。

インターネット上で活動する脅威者が窃取した情報等を取引するダークウェブ等ではWebサイトから窃取されたID、パスワードのリストが販売・公開されています。脅威者はこれらをダウンロード、購入して金融関連Webサイト等にログインを試み、資金の摂取を行うことがあります。



パスワードリスト攻撃のリスクを軽減するには、IDパスワードの使いまわしを行わないようにします。また、ダークウェブをモニタし、漏洩したID、パスワードと一致するものを使わないようにします。

ユーザがID、パスワードの使いまわしをしたり、古いID、パスワードをそのまま使用し続けていると、それと一致するID、パスワードがセキュリティレベルの低いサイトから漏洩してしまうことがあります。これがダークウェブ上で公開されることがあり、これを使用して手当たり次第にログインが試みられてしまう場合があります。

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

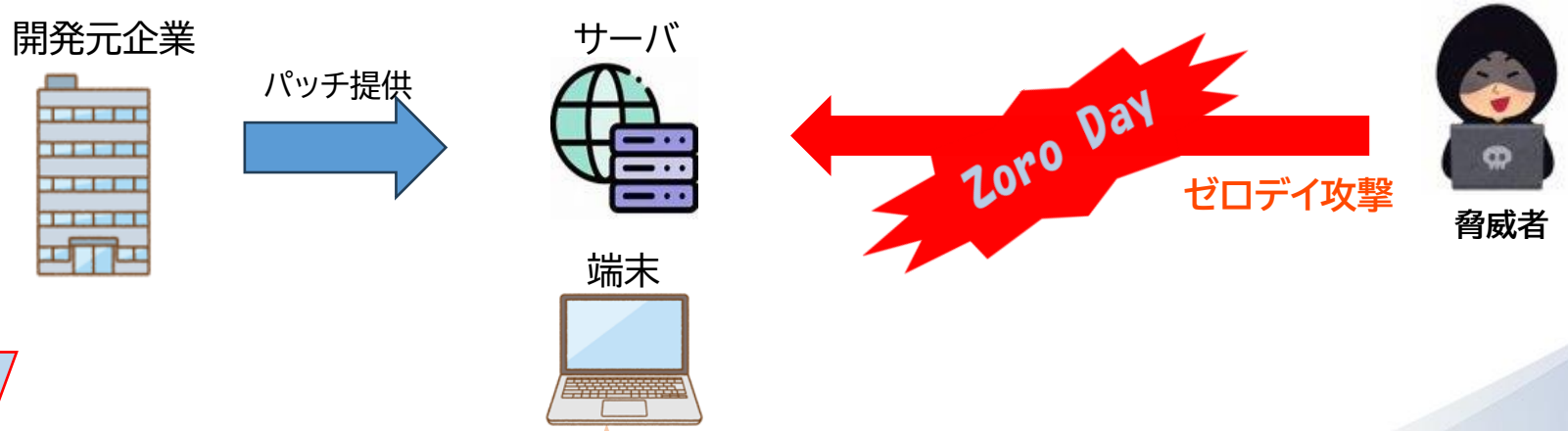
*） 詳細は「用語集」を参照して下さい

（用語集）ゼロデイ攻撃

ゼロデイ(zero-day)攻撃は、脆弱性へのパッチがダウンロード可能となる1日目よりも前(0日目)に攻撃が行われるものです。

脆弱性は開発元により発見され、もしくは第三者により発見され開発元に通知(CERTを経由して通知される場合があります)される場合があります。この後開発元がプログラムを修正し、パッチが発行されます。

国家支援の脅威者、金銭目的の脅威者は自ら脆弱性を探したり、他の脅威者が発見した脆弱性を購入したりします。これらの脆弱性がパッチ発行前に攻撃されるとゼロデイ攻撃になります。



ゼロデイ攻撃のリスクを低減するには次のような対策があります。
・基本的なセキュリティ対策の実施(OSなどのアップデート)
・サンドボックスの利用

中国や北朝鮮等の国家支援の脅威者はゼロデイ脆弱性を利用することで知られています。これらの脅威者は世界の先端技術の窃取、金銭目的での金融機関への侵害等を行っています。

(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*) 詳細は「用語集」を参照して下さい

（用語集）DoS攻撃、DDoS 攻撃

Dos（Denial of Service）攻撃は、標的となるシステムに大量のデータや、悪意あるパケットを送り、システムを誤動作させるものです。

大量のデータを送るのはフラッド型と呼ばれ、プログラムの脆弱性を突く悪意あるパケットを送付するのは脆弱性型と呼ばれます。

大量のPCを踏み台にしてDoS攻撃を行うものはDDoS（Distributed Denial of Service）攻撃と呼ばれます。

DoS攻撃、DDoS攻撃を受けた場合のリスクは次の通りです。
・被害のあったサイトへのアクセスができなくなる
・企業のWebサイトが被害にあった場合社会的信用低下につながる

DDoS攻撃はボット*（Bot）を使用したり、発信元IPアドレスを詐称したパケットを無関係な複数システムに送付した応答を利用したりして大量のパケットを標的のシステムに送りつけます。踏み台となった各々のシステムには少数のパケットだけを送信するため、それらの単体のシステムでは踏み台として悪用されたことを気づけない場合があります。

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）SSL／TLS暗号化に伴う脅威

SSL／TLS通信はやり取りするデータを暗号化する通信の方式です。

ファイアウォール（FW）を超えてユーザ端末、社外Webサーバ間でSSL／TLS通信を行う場合、データが暗号化されるため、監視装置（IPS、IDS等）でのマルウェア検知等ができなくなります。

対策としてFW等で暗号を解き、内容を確認して再度暗号化して送信する方式の機器を導入する方法等があります。

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）Webサービス経由の攻撃（XSS）

Webサーバの脆弱性を利用した攻撃としてクロスサイトスクリプティング（XSS）、クロスサイトリクエストフォージェリ（CSRF）等があります。

XSSの攻撃の概要は次の通りです。脅威者がWebサーバに悪意のあるスクリプトを書き込み、ユーザがブラウザでこれを読みだしてブラウザ上で実行することにより秘密の情報を窃取されたり、不正な操作を行われたりします。

Webサーバで入力されたメッセージの安全性をチェックし、HTML、JavaScriptの特殊文字をエスケープする処理を行うことで防ぐことができます。

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）スキャン攻撃

スキャン攻撃は脅威者が侵入容易な標的を探したり、標的となった組織への侵入経路を探索するためにシステム、NW機器の脆弱性を調査する目的で行われます。

具体的には、サーバ等の各ポートに対して特定のパケット（データ）を送信し、その応答を調査します。この応答により、該当ポートを使用しているプログラムの種別、バージョンが分かり、脆弱性の存在するプログラムか否かが分かります。この結果を用いてサーバ等を選択して攻撃対象にします。

脆弱性の例：
・ポート22（SSH）で、推測しやすいID、パスワードでの通信を許容
・オート24（SMTP）で認証不要なメール中継サーバが動作

ポートからの応答イメージ

TelnetなどでWebサーバにアクセスすると下記のような文字列を返す場合があります。

```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2018 10:20:29 GMT
Server: Apache/ 2.4.25
Last-Modified: Fri, 21 Aug 2018 12:10:06 GMT
```

不要なポートを開放、脆弱なソフトウェアを動作させたときのリスク：
・脅威者による侵入
・他の組織への攻撃の踏み台化
・組織内秘密情報の漏洩

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

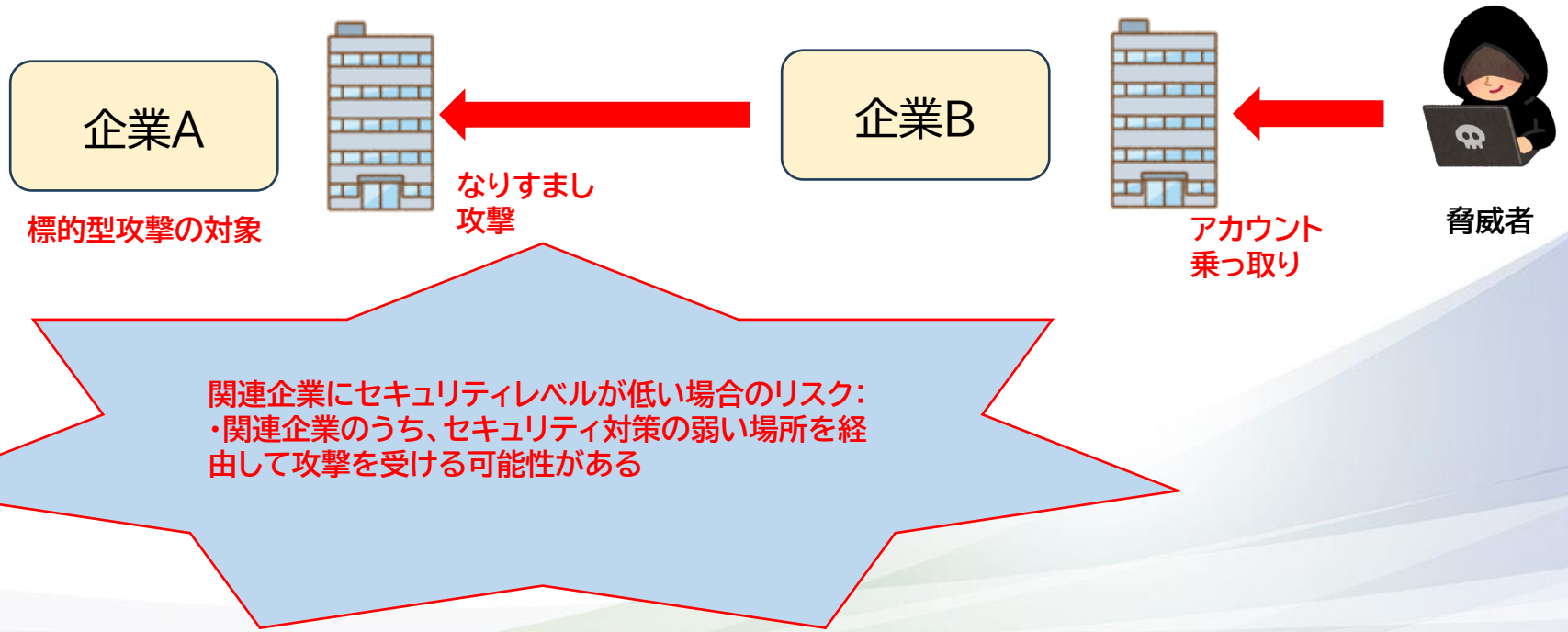
（用語集）標的型攻撃

標的型攻撃とは、脅威者が秘密情報を盗み取ること等を目的として特定の個人や組織を狙う攻撃です。

標的型攻撃で狙われるのは脅威者が目的とした情報を持つ組織等だけではなく、その関連組織、関連企業等よりセキュリティ防御が弱い箇所が狙われることがあります。

例えば航空機製造企業の情報を盗み出すために、より小規模の関連企業が狙われたことがあります。当初は複数の企業が個別に狙われたと想定されましたが、それらに同じ大企業からの発注があったことで脅威者の狙いが発注元にあると推定されました。標的を定めない攻撃は「ばらまき型攻撃」と呼ばれます。

攻撃手法:
脅威者は企業Aの情報を狙っている場合に、関連企業である企業Bのアカウントを乗っ取り、フィッシングメールを企業Aに送付する場合があります。



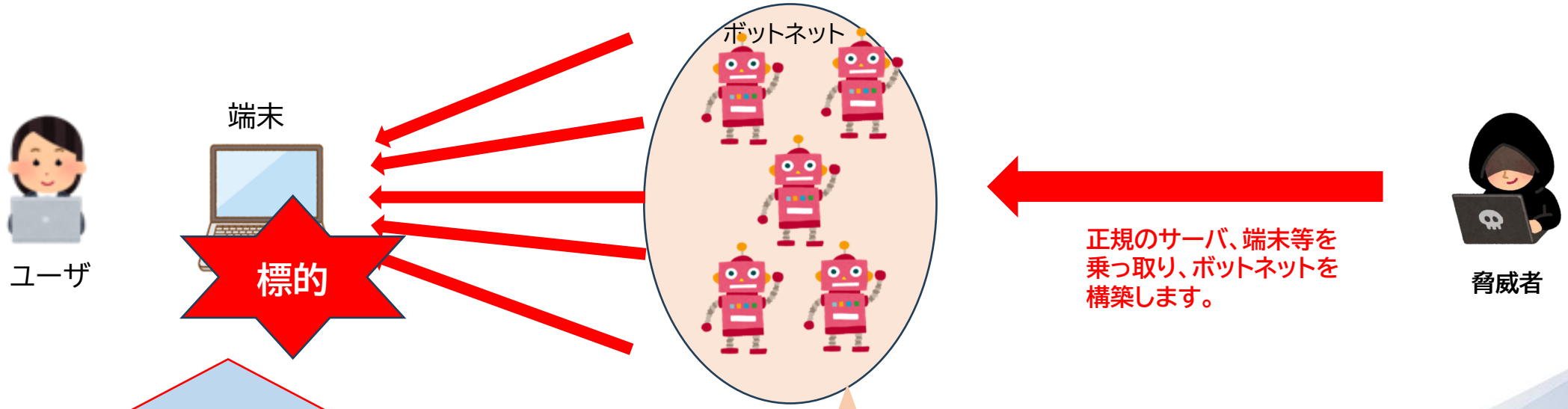
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）ボットネット、ボット

ボットネット（Botnet）はボットというマルウェアにより脅威者に不正に乗っ取られ正規のシステム等の、多数のシステムからなるネットワークを示します。

正規のシステムの所有者は、脅威者により踏み台等に悪用されていることを気づかない場合が多いです。



自社システムがボットネットに加えられた場合のリスクは次の通りです。
・他社に対する攻撃に加担することで対外的な信用失墜につながります
・IPアドレスが悪用されているため、正規の通信がブロックされる場合があります。

ボットネットを使った攻撃には以下のようなものがあります。
・多数のコンピュータを使ったDoS*攻撃（DDoS - Distributed Denial of Service、分散型DoS）攻撃を行います。
・多数のアドレスからのスパムメールを送信します。これにより脅威者がスパムメールフィルタの機能を回避して悪意のあるメールを標的に送りつけることができます。

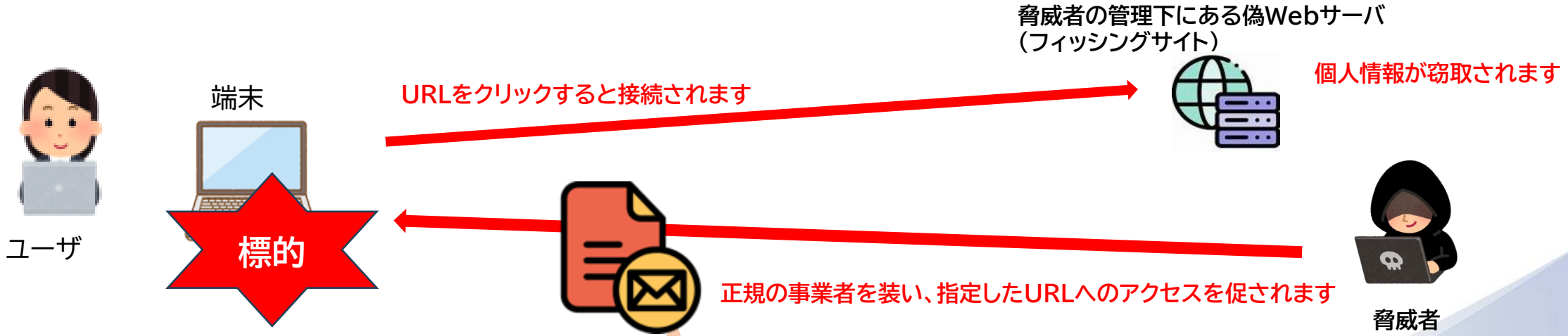
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）フィッシングメールによる攻撃、フィッシングサイト

フィッシングメールは、脅威者が正規のものを装った偽のメールを標的に送り、偽サイトに誘導した上でID、パスワード等の個人情報を窃取する攻撃を言います。この時使われる偽サイトをフィッシングサイトと言います。

偽のメールに使われる題材としてインターネットショップに登録されているクレジットカード情報が無効になっている、宅配便配達時に不在だった、等があり、住所、氏名、カード番号等の窃取が試みられます。



フィッシングメールによる攻撃のリスクを軽減するには以下の方法等があります。
・送信元、送信先を確認
・正しい日本語になっているか確認

フィッシングメールによる攻撃例の詳細は次の通りです。
・正規の配送業者を装い、配送時に不在・情報不足等の理由で配送不可であったと偽ります。
・再配達が必要な場合は指定したURLをクリックして配送情報の入力を促されます。
・入力した個人情報等は脅威者に窃取され、なりすましに使われ、新たな被害が発生することとなります。

【スピアフィッシング（Spear Phishing）】
スピアフィッシングのうち、標的を絞ったものをスピアフィッシングと呼びます。

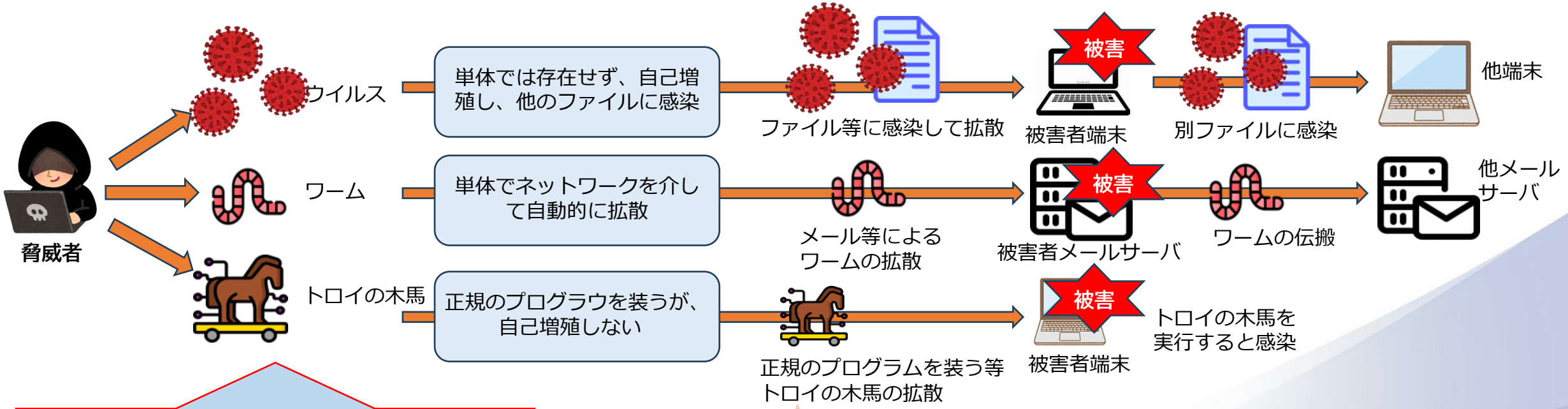
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）ウイルス、ワーム、トロイの木馬

マルウェア（Malware）の主な種類として、ウイルス（Virus）、ワーム（Warm）、トロイの木馬（Trojan Horse）があります。

ウイルスはファイル等に感染、ワームはネットワークを経由して自己増殖、トロイの木馬は正規のソフトを装いバックドアを開く等の特徴があります。なお、ウイルスはマルウェア全般を指す言葉として使われる場合が有りますが、ここでは狭い意味でファイル等に感染するものを示します。



マルウェアに対する十分な対策がなされていない場合のリスクは次の通りです。
・トロイの木画を持ち込ませない、クリックしない等の対策を行わないと感染の危険が高まります。

マルウェアの種類により感染経路、発生する被害内容が異なり、それぞれ適切な対策が必要です。例えばトロイの木馬では正規のアプリケーションであっても通常と異なる場所にインストールされているなどの異常を見逃さないようにする等個別に対策が必要になります。

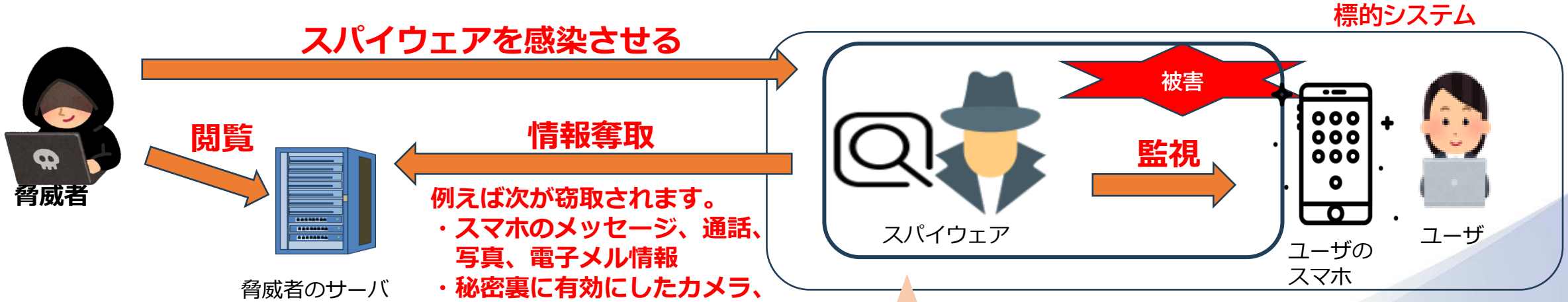
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）スパイウェア

スパイウェア(Spyware)は、標的となったコンピュータに不正に侵入し、ユーザの個人情報や位置情報、メールの内容、連絡先等を収集し、ユーザに気づかれることなく脅威者に情報を送信します。

使われ方として、金銭目的の脅威者によりユーザの金融情報を窃取したり、国家の諜報機関等が他国の政府要人の活動や反政府組織のメンバの行動を監視するなどがあります。有名なスパイウェアにはイスラエルのNSO Groupが開発して主に政府組織に販売されたPegasus等があります。Pegasusの場合、監視対象が数百人に及ぶ企業経営者、政府関係者が監視対象となっていたことがあります。



スパイウェアによるリスクは次の通りです。
・PCなどに投入したID、パスワードの漏洩
・スマホによるリアルタイムでの盗聴等

標的のスマホにスパイウェアを感染させる方法として、法執行機関が標的を一時的に逮捕し、持ち物検査を装い感染させた例もあります。特定のWebサーバの閲覧、メールの添付ファイルを経由しての感染方法もあります。また、スパイウェア感染のためだけにスマートフォンの脆弱性を調査、攻撃手法の開発を行う試みも行われています。

(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）ショルダーハッキング

ショルダーハッキング（Sholder Hacking）は、肩越しに他人の認証情報や秘密情報を覗き見る攻撃方法です。

公共の場所、他部署の人が出入りするオフィス内で自分のコンピュータ、スマートフォンを使用している際に脅威者が直接、望遠カメラ利用等で画面を覗き見る等を示します。これが行われた場合、被害者は被害があったことを気づかない場合が多いです。

ショルダーハッキングのリスクが高い例はとして次があります。
・自宅の窓、扉を開けた状態等での在宅勤務実施
・外部からガラス窓越しに端末画面が視認可能

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

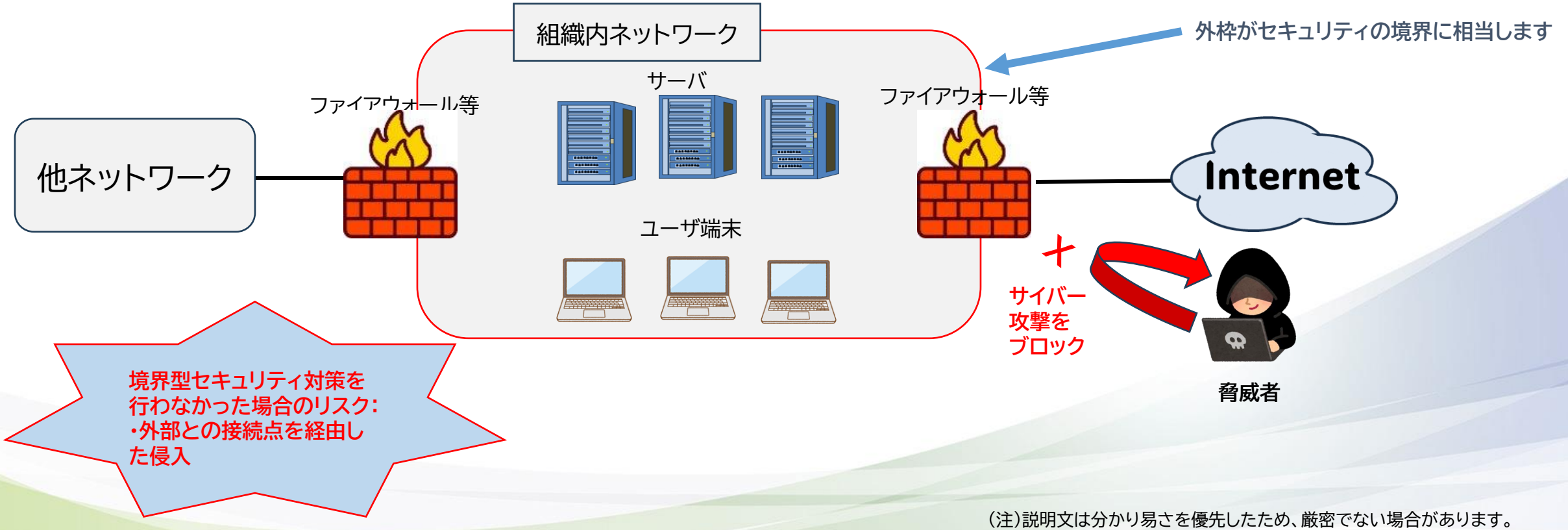
防御手法

防御手法
- 従来型の防御方法 -

（用語集）境界型セキュリティ対策

境界(ペリミタ - perimeter)型セキュリティ対策とは組織内のNWと組織外のNWとの間にファイアウォール、IPS等を設置して分離することでセキュリティ対策を実施する方式です。

これは新たにゼロトラスト型セキュリティ対策が提唱されたことに対して、従来のNW設備によるセキュリティ対策を示すために作られた用語です。



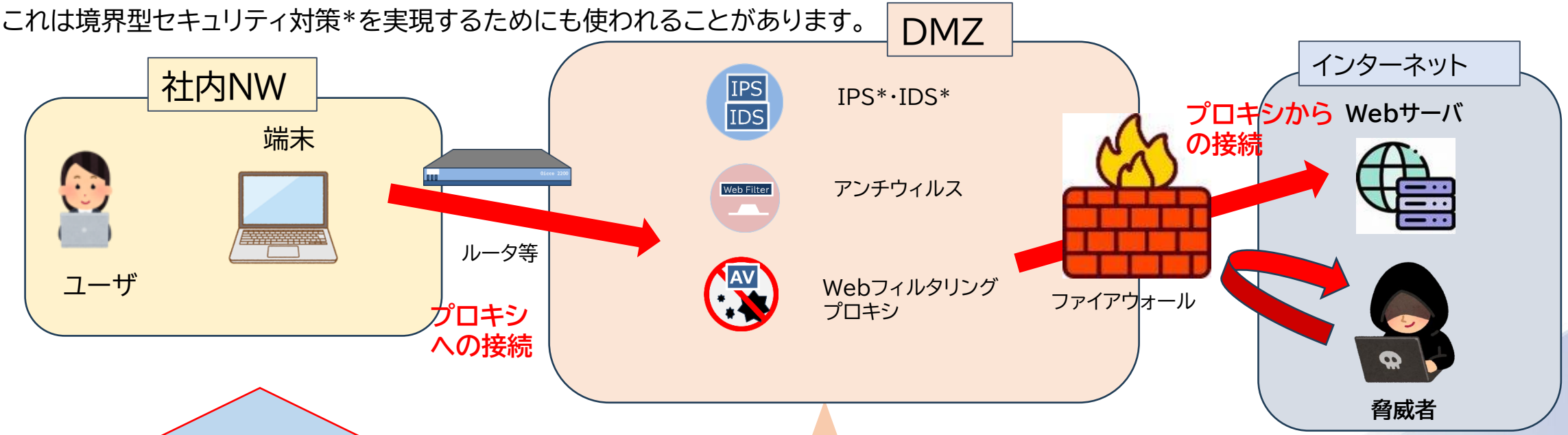
(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）DMZ

DMZ(非武装地帯 - DeMilitarized Zone)は、社内NWとインターネットとを接続する場合に、これらの間に特別なNWを設置することで外部からの不正アクセス、内部からの情報流出などを防ぐものです。

これは境界型セキュリティ対策*を実現するためにも使われることがあります。



DMZを設けることにより低減できるリスクは次の通りです。
・インターネットからアクセスできるサーバを踏み台とした攻撃
・プロキシを経由による情報漏洩の防止

DMZは元々軍事用語として使われており、緊張状態にある2国・地域間の軍事境界線に設定された軍事活動を行わないことを両国・地域で同意した地域を示します。
通常、インターネット側からはDMZ内のシステム、社内NWからもDMZ内のシステムへのみアクセス可能に設定します。これによりインターネットと社内NW間で直接通信しないようにして、必ずDMZ内のシステムで適切な処理を通すことが出来ます。

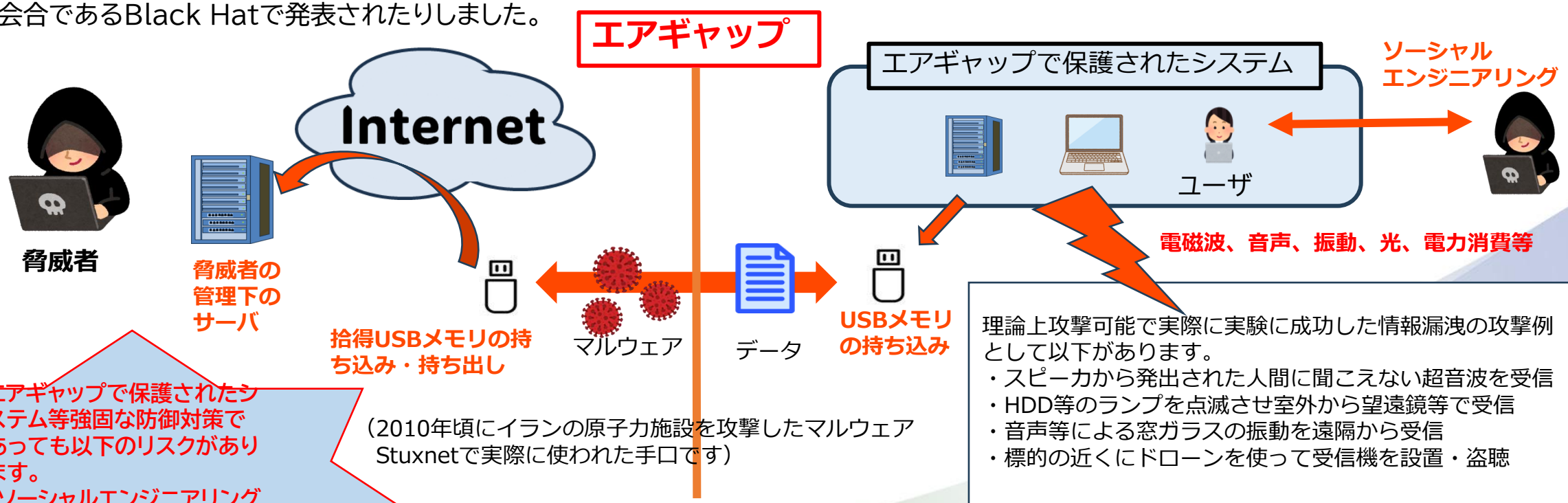
(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）エアギャップ

エアギャップ（Air Gap）は、外部のネットワークとシステム間を物理的、論理的に切り離すことでシステムを防御する手法を言います。これを利用すると重要インフラ等の高いレベルのセキュリティを確保する都ができます。

しかしながら、これに対する攻撃手法も存在します。例えば、ソーシャルエンジニアリング、外部から持ち込まれた記録媒体に組み込まれたマルウェア経由、電磁波・音声・振動・光・電力消費値等の隠れた通信経路（Covert Channel - 隠れチャネル）での攻撃が実際に使われたり、ハッカーの会合であるBlack Hatで発表されたりしました。



（2010年頃にイランの原子力施設を攻撃したマルウェア Stuxnetで実際に使われた手口です）

理論上攻撃可能で実際に実験に成功した情報漏洩の攻撃例として以下があります。
- スピーカから発出された人間に聞こえない超音波を受信
- HDD等のランプを点滅させ室外から望遠鏡等で受信
- 音声等による窓ガラスの振動を遠隔から受信
- 標的の近くにドローンを使って受信機を設置・盗聴

エアギャップで保護されたシステム等強固な防御対策であっても以下のリスクがあります。
- ソーシャルエンジニアリング
- 不適切な記憶媒体の扱い
- 電磁波等による情報漏洩

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

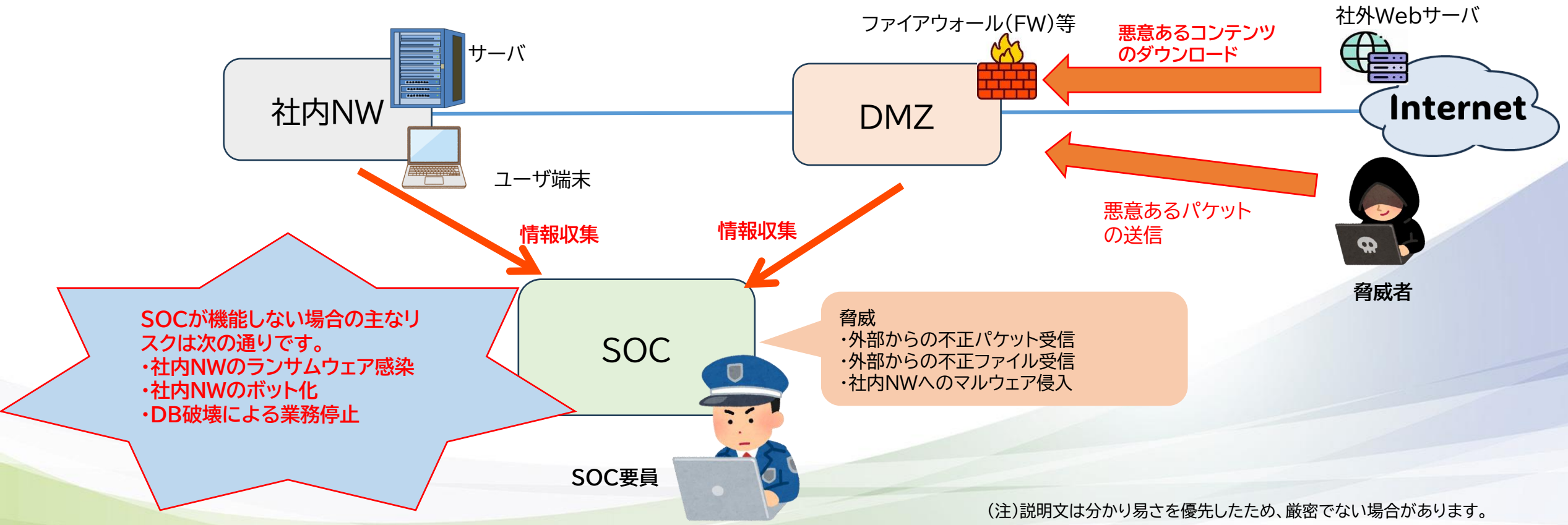
*） 詳細は「用語集」を参照して下さい

防御手法
- SOC組織 -

（用語集）SOC

SOC（セキュリティオペレーションセンタ、Security Operation Center）は、サイバー攻撃の検知・分析及び、対策を行う組織です。

SOCではFW、センサ等のセキュリティ機器・ネットワーク機器、サーバ等を監視し、ログの分析を行います。組織がサイバー攻撃を受けた場合は影響範囲を特定し、攻撃経路を推定し、対処・対策を行います。



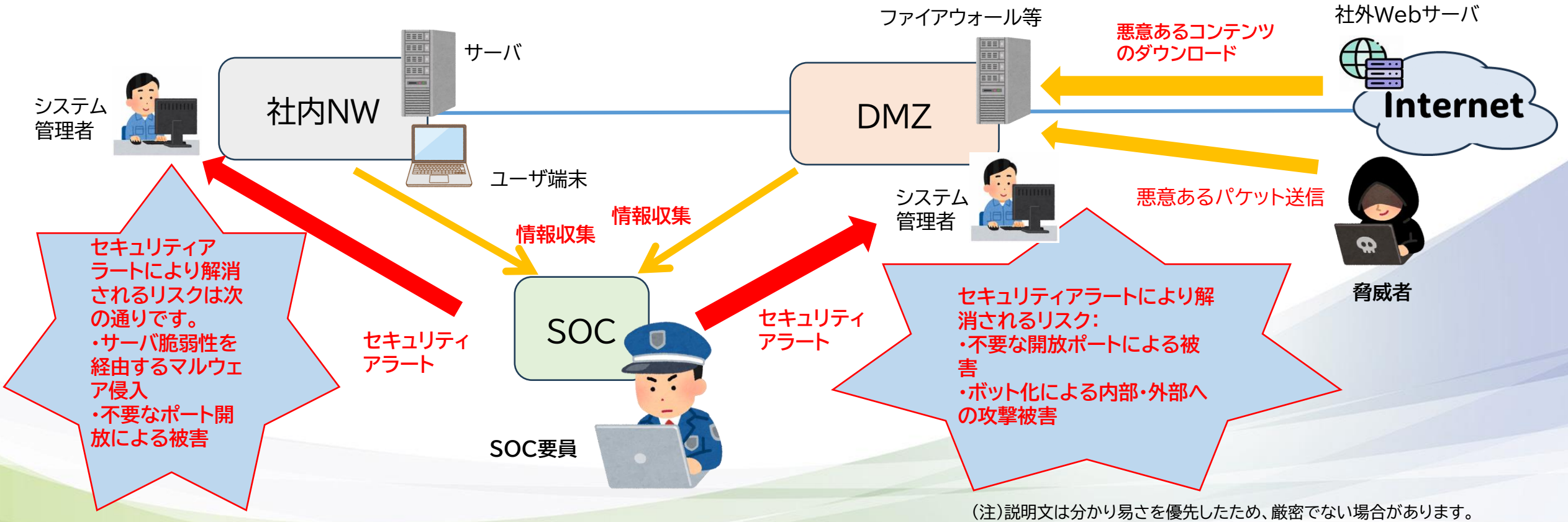
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）セキュリティアラート

SOCでサイバー攻撃等の脅威を検知した場合、サーバ管理者等にセキュリティ上の警告（セキュリティアラート）を発出する場合があります。

脅威者による特定の脆弱性を狙ったパケット送付等を検知した場合、該当する脆弱性の修復確認等を促すセキュリティアラートがSOCから発出される場合があります。



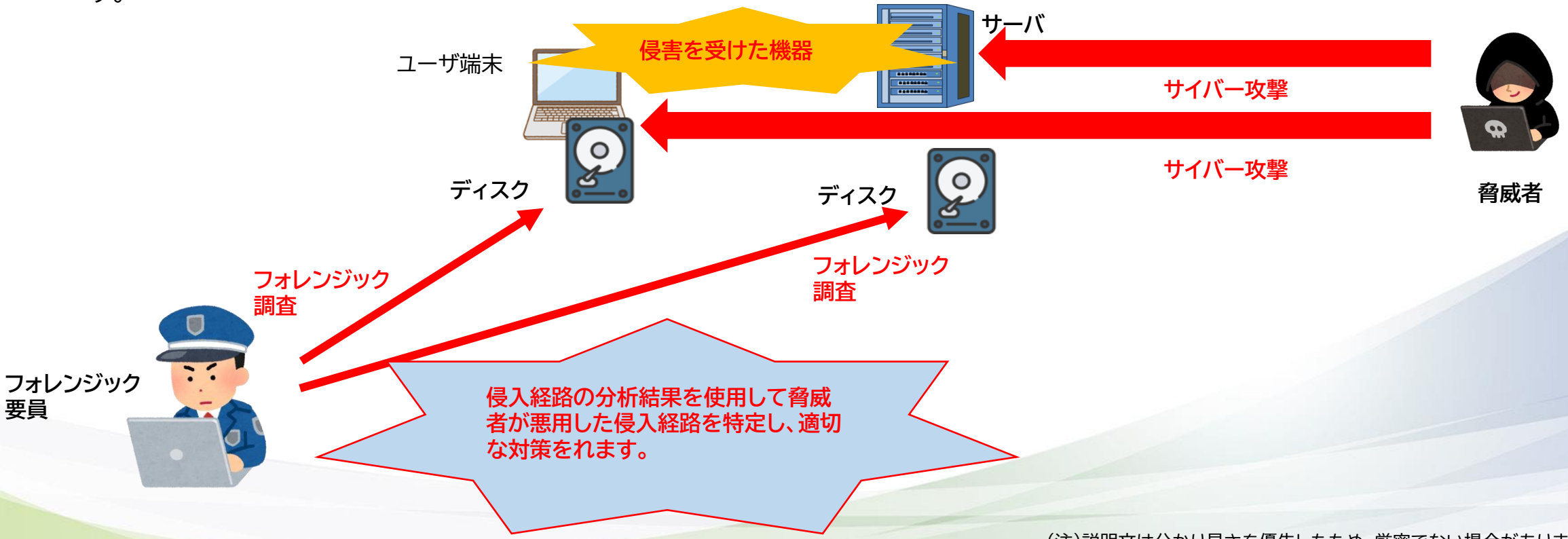
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）フォレンジック

フォレンジック（デジタルフォレンジック）は、サーバ、ユーザ端末がマルウェア感染した場合等にその分析を行うものです。ファイルのタイムスタンプ、残存する脆弱性、新たに設置されたファイル等を調査して侵入経路、マルウェアの挙動の推定等を行います。

HDD・SSD内のデータや、可能であればメモリ上の情報を使い、脅威者が使用した初期侵入経路、侵害順序、横方向展開経路、ログファイルの改ざんの可能性、機密ファイル参照の可能性等を調査します。この結果、悪用された開放ポートの停止、脆弱性パッチの適用等の対策を行います。



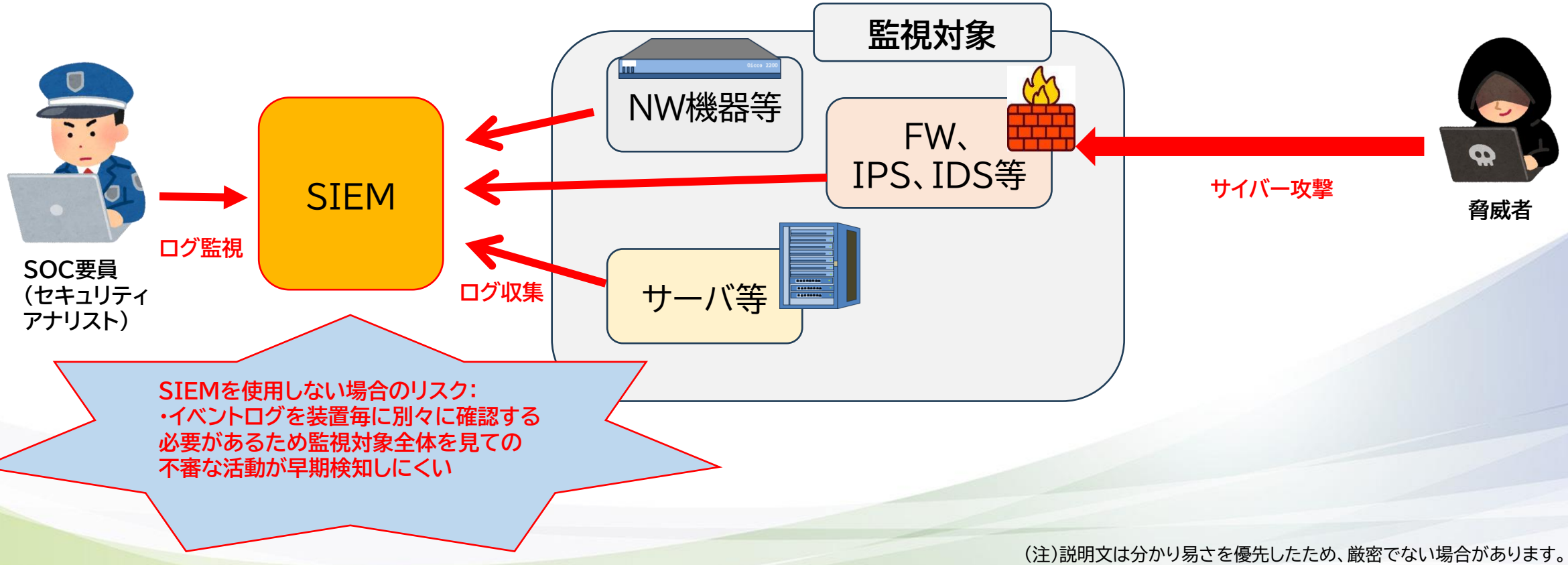
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）SIEM

SIEM(セキュリティ情報とイベント管理、Security Information and Event Management)は組織内(社内)NW内の様々な機器からのイベントログの情報を集約します。

ログは集約され、統合して分析することで組織が定めた行動ルールに違反する活動を調べることができます。例えば、あるユーザが複数経路から短時間にログイン失敗を繰り返した等の不審な活動を検知した場合、それをセキュリティアナリストに通知する等します。



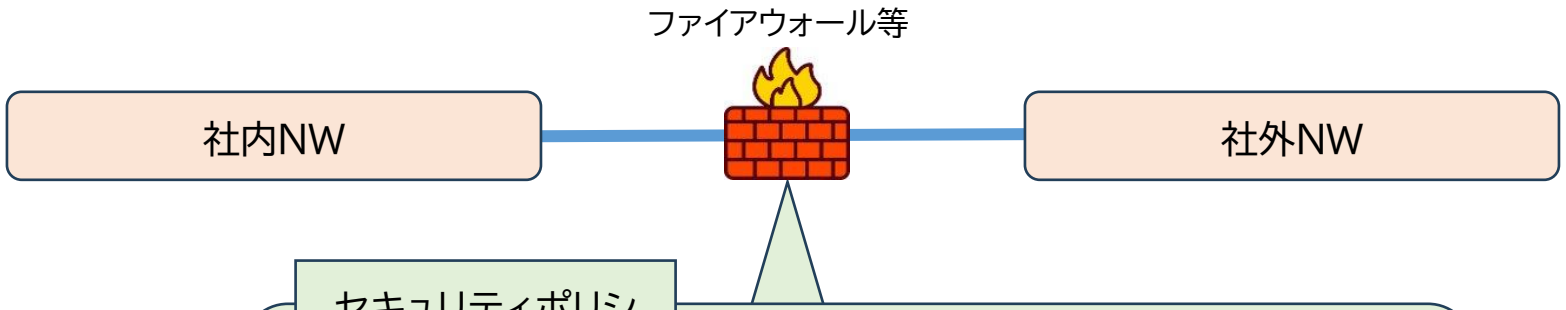
(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）セキュリティ設定／セキュリティポリシ

セキュリティ機器に登録するセキュリティ設定／セキュリティポリシは、ファイアウォール等の動作を決めるためのルールを定めるものです。

社外NWと社内NWとを接続するファイアウォールでの設定では、条件を満たしたパケット、セッションに対する通過・遮断等を指定します。これにより社内NWを保護します。



セキュリティポリシ

例えば、社内から外部へのDNSクエリを許可し、逆方向を禁止するには下記の王な設定を行います。
・内部のIPアドレスから外部向けのUDP 53への通信を許可
・外部から内部のIPアドレス向けのUDP 53への通信を禁止

セキュリティポリシを適切に設定しない場合のリスク：
・ファイアウォール等による適切な保護が行えない

● 類似の用語で「情報セキュリティポリシ」は企業等が自社の情報を脅威から守るために定める方針等を指します。

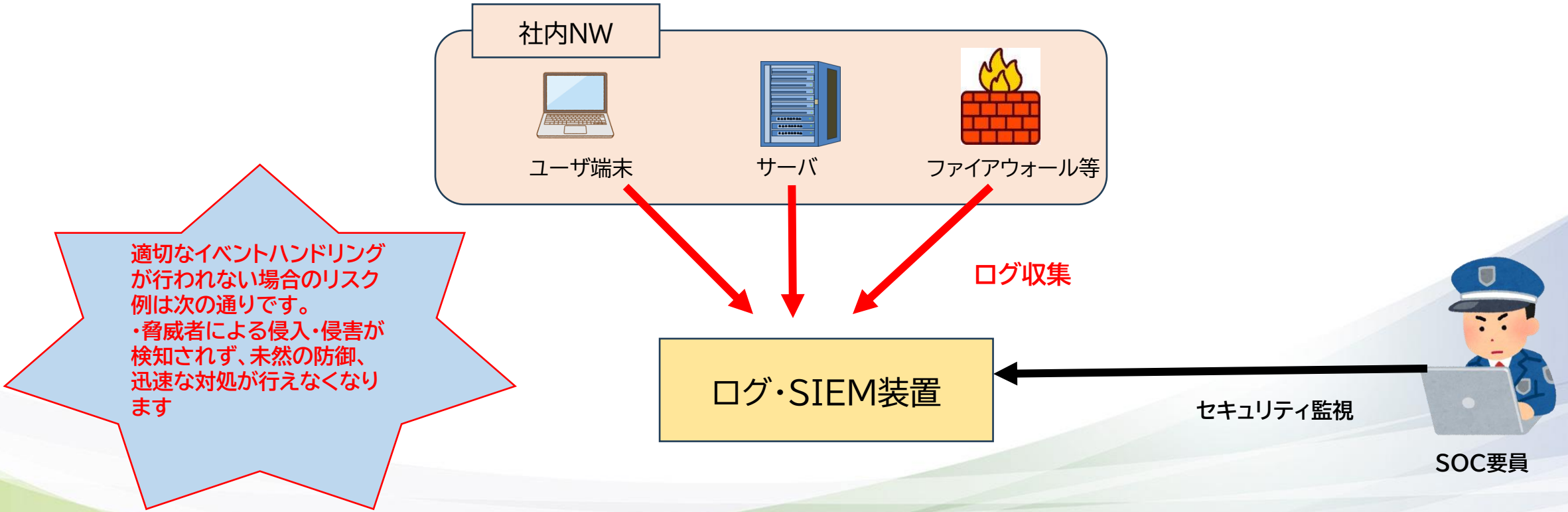
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）イベントハンドリング

ユーザのログイン、構成の変更、ファイルのダウンロード等のイベントはログに記録されます。これらのイベントの有害・無害の判定、また、対策検討・実施依頼等のイベントハンドリングが組織のセキュリティ確保に必要となります。

例えば、脅威者による侵入事例では、不適切なログイン、承認されないファイルダウンロード等が行われる場合があり、これらのイベントを組み合わせて解析することで一連の侵害の活動を検知することができることがあります。



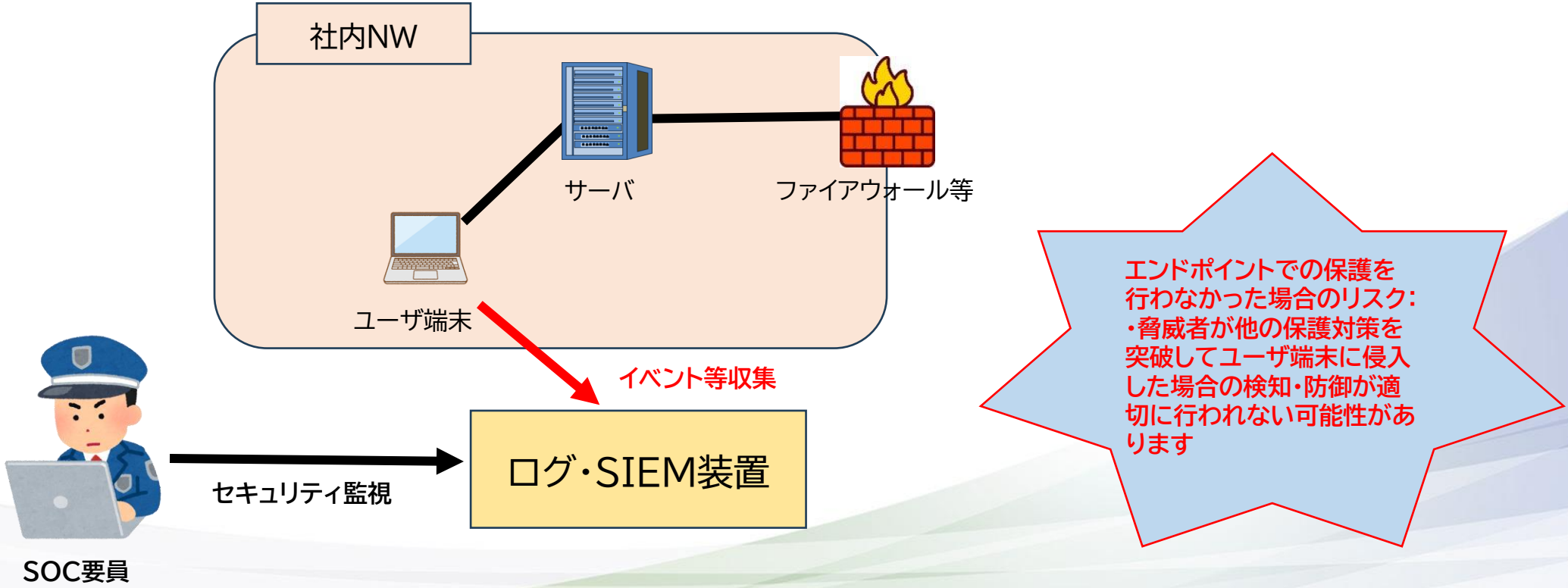
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）エンドポイントセキュリティ

エンドポイントセキュリティ（Endpoint Security）とは、ネットワークに接続される端末機器等の末端のデバイス（エンドポイント）を保護するための機能を言います。

これにはアンチウィルスソフト（EPP - Endpoint Protection Platform）、次世代アンチウィルス（NGAV - Next Generation Anti-Virus）、マルウェア検知・隔離（EDR - Endpoint Detection and Response）、情報漏洩防御（DLP - Data Loss Prevention）などがあります。



（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

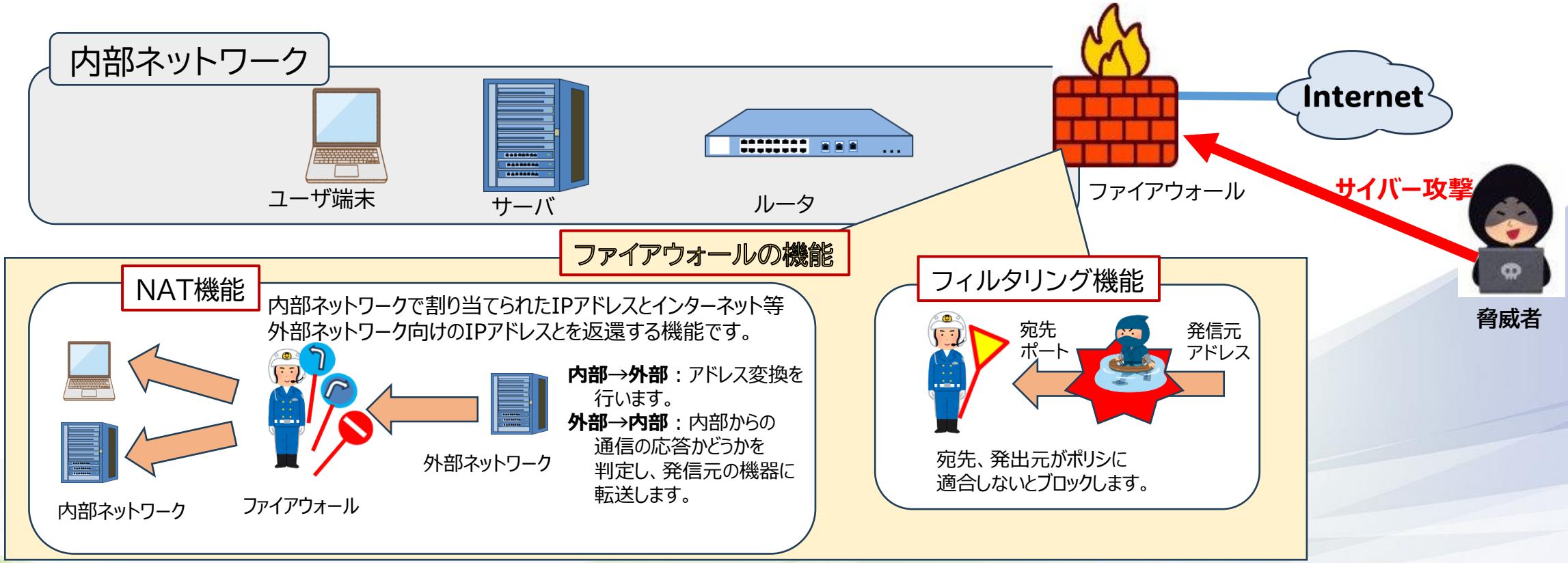
防御手法
- 防御機能 -

（用語集）FW（ファイアウォール）

ファイアウォール（FW – Firewall）は、外部のネットワークと内部のネットワークの間に設置し、外部からの侵入を阻止する装置です。

ファイアウォールの主な機能として、不正な通信を遮断するフィルタリング機能、アドレス変換を行うNAT（Network Address Translation）機能などが有ります。

フィルタリング機能の例として、通信可否リストに基づく静的フィルタリング（ポート番号・プロトコル、IPアドレスを利用します）があります。



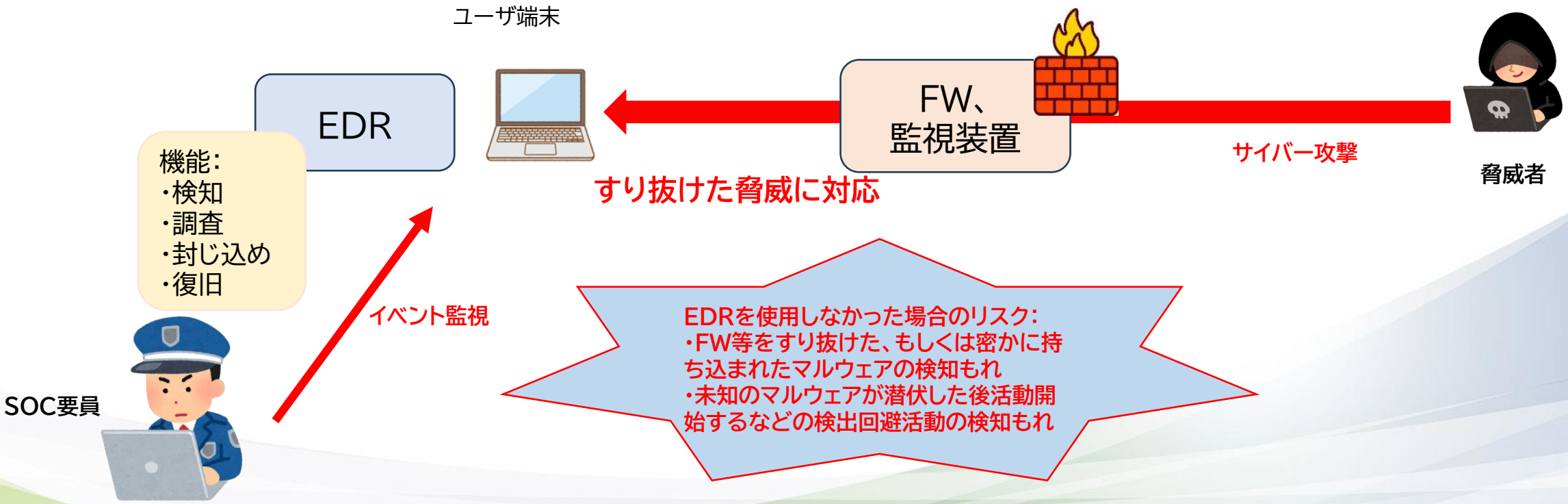
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）EDR

EDR（Endpoint Detection and Response）はユーザ端末等のエンドポイントのデバイスを保護するための機能です。EDRは対象となるデバイスの状況を監視し、不審な活動を検知し、対処を行います。

EDRは侵害を検知し、隔離・駆除等を行います。



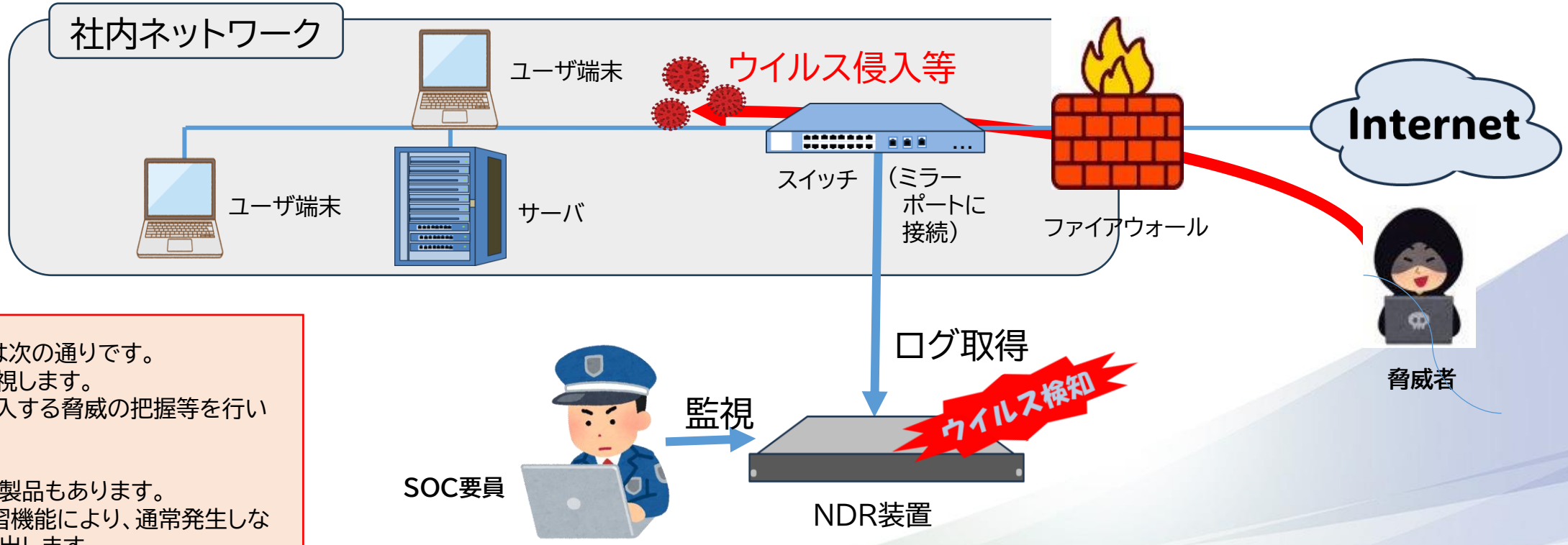
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）NDR

NDR(Network Detection and Response)は、ネットワーク機器を通過するトラフィックを抽出して分析し、外部からの攻撃、内部不正等の兆候を検知する手法を言います。トラフィックの抽出にはネットワーク機器のミラーポートへの接続等が使われます。

FW等の防護策をすり抜けたり、VPN等を経由した侵入等を検知出来ます。



NDRの主な特徴は次の通りです。
・ネットワークを監視します。
・ネットワークに侵入する脅威の把握等を行います。

以下の機能を持つ製品もあります。
・AIを使用した学習機能により、通常発生しない不審な通信を検出します。

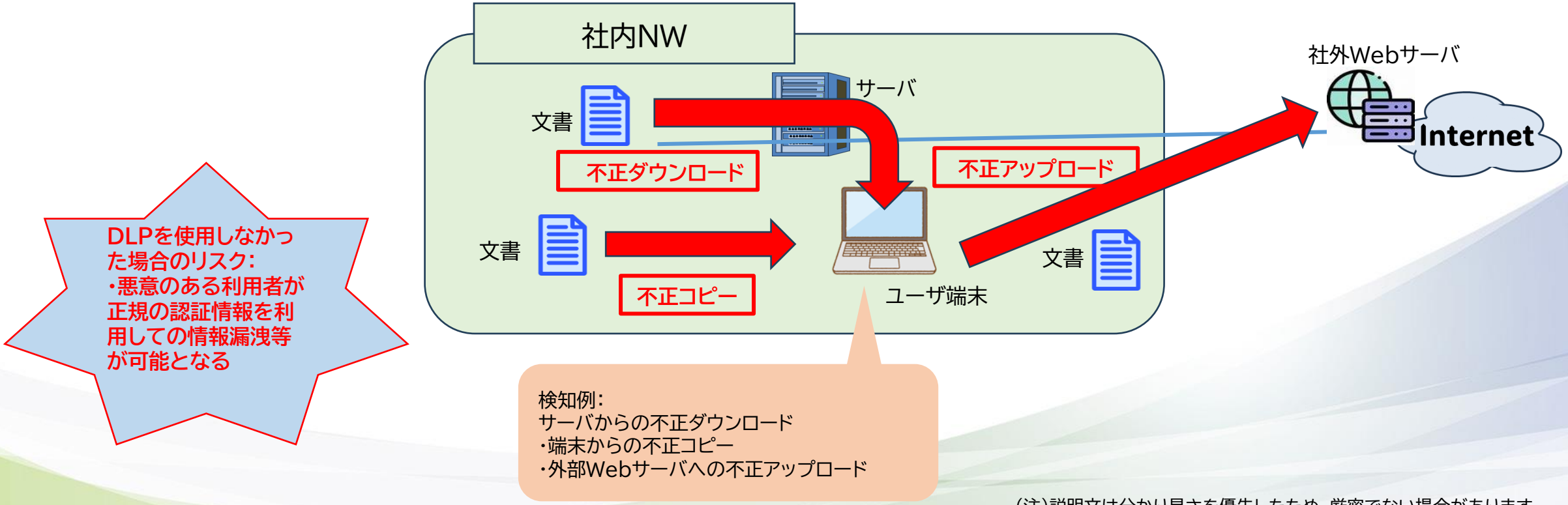
(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）DLP

DLP（情報漏洩対策 - Data Loss Prevention）は、データそのものを監視し、その流出を防ぐ機能を持ちます。

基本的な機能としてデバイス制御、データ監視、印刷・コピー制限、Webサーバアクセス制限、メール制御等の機能があります。重要な情報の判別にはフィンガープリント、キーワード等が使われます。



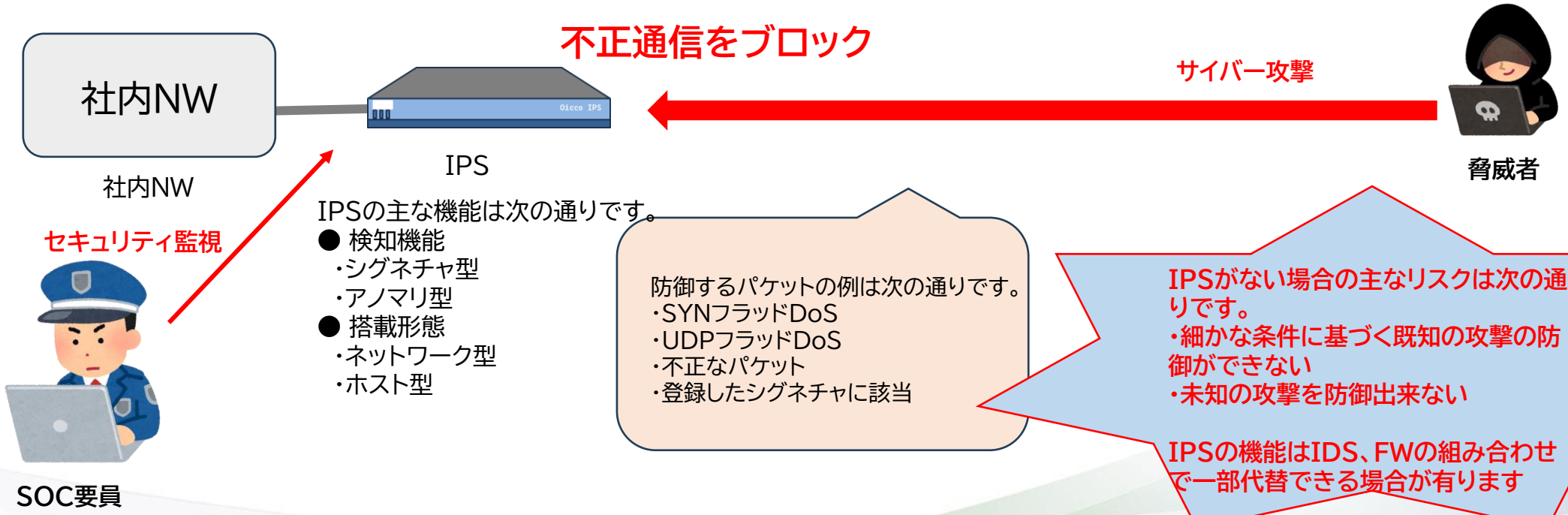
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）IPS

IPS（不正侵入防止システム - Intrusion Prevention System）は、ネットワークに対する不正な侵入を検知・ブロックするシステムです。

IPSにはネットワーク上に設置するネットワーク型IPS（NIPS - Network-based IPS）、ホスト上に設置されるホスト型IPS（HIPS - Host-based IPS）があります。



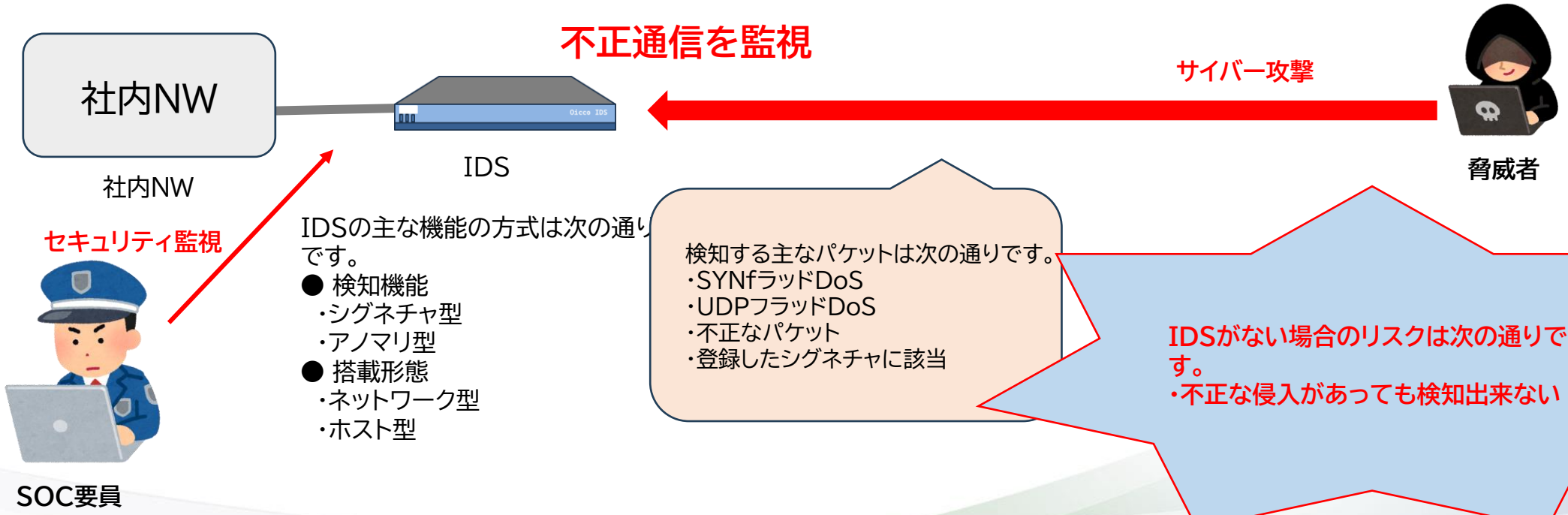
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）IDS

IDS（不正侵入検知システム - Intrusion Detection System）は、ネットワークに対する不正な侵入を検知して管理者に通知等を行うシステムです。

IDSはネットワークを監視するためのネットワーク型IDS（NIDS - Network-based IDS）、コンピュータを監視するためのホスト型IDS（HIDS - Host-based IDS）があります。



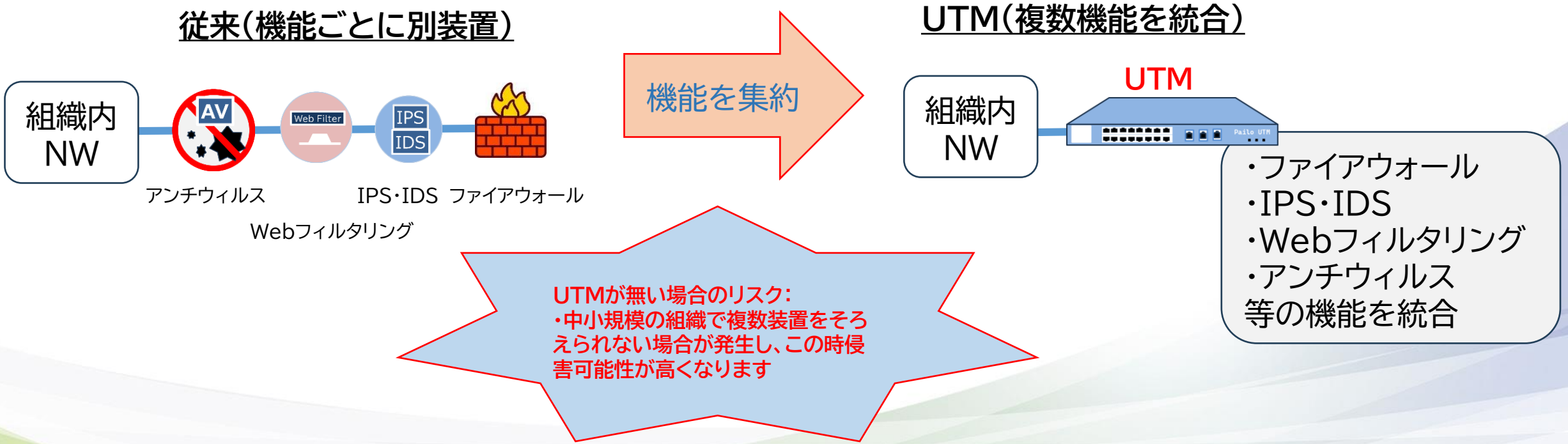
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）UTM

UTM（Unified Threat Management）は複数のセキュリティ機能をまとめた製品を言います。

備えられる機能には、ファイアウォール、IDS・IPS、Webフィルタリング（有害な不正サイトへのアクセス制限）、アンチウイルス・スパム等があります。



（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

防御手法
- クラウド対応 -

（用語集）SASE

SASE(Secure Access Service Edge)は下記のようなセキュリティ機能、ネットワーク機能をクラウド上で提供する方式です。

・VPN、リモートアクセス、SD-WANなどのNWサービス

・ファイアウォール、IDS／IPS、ウィルス対策等を統合したUTM

ユーザ
システム

SASE(クラウド上で実現)

SASEは以下のような機能をクラウド上に実現します。
・SWG(Security Web Gateway):ウェブゲートウェイ機能
・CASB(Cloud Access Security Broker):クラウドアクセス用リソース管理機能
・FWaaS(FireWall as a Service):FW機能
・ZTNA(Zero Trust Network Access):ゼロトラストに基づくアクセス管理機能

セキュリティ監視

SOC要員

SASEを使用しなかった場合のリスク:
・アプライアンス等のセキュリティ機器を個別に備える必要がある

● SASEは「サシー」と読みます

(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）SWG

SWG（Secure Web Gateway）は、組織のユーザとインターネットの間に設置し、企業のデータの保護及びセキュリティポリシに従った制御を行います。

SWGはWebサーバとの間のトラフィックで不審なコンテンツのフィルタリングを行います。これにより悪意あるコンテンツや情報漏洩を阻止したり、許可されていないユーザの行為をブロックしたりします。

SWGの機能には以下のものがあります。
・URLフィルタリング
・マルウェアのスキャン
・アプリケーション制御
　- コンテンツフィルタリング
　- データ損失防止（DLP）

SWGを設けない場合のリスクは次のとおりです。
・FWの該当機能などを用意する必要があいます

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）CASB

CASB（Cloud Access Security Broker）（キャスビー）は、Microsoft One Drive等のクラウドサービスへの組織内NWからのアクセスのセキュリティ管理を一元管理します。

主な機能として、利用状況の可視化、データセキュリティ、脅威防御等が有ります。

CASBの導入方式には以下があります。
・API型：クラウド上のサービスにAPIで連携する構成
・インライン型：クラウドサービスに接続するまでの通信経路内にCASBを配置する構成
・ログ分析型：アクセス先のURLをベースに通信を監視します。

CASBを使用しない場合のリスクは次の通りです。
・潜在的なリスクの早期発見が困難

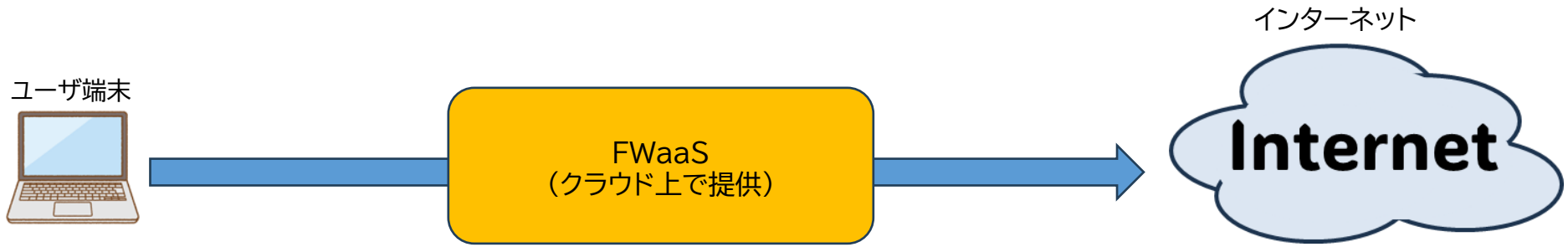
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）FWaaS

FWaaS（FireWall as a Servuce）はクラウドサービスとしてFWの機能を提供します。

従来の旧式のFW同様の機能をクラウド上で提供しています。



FWaaSはクラウドサービスとの統合が容易です。
ソフトウェアのアップデートがベンダにより行われます。

FWaaSを利用しない場合のリスクは次の通りです。
・ハードウェアでのボトルネックが発生する可能あり

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

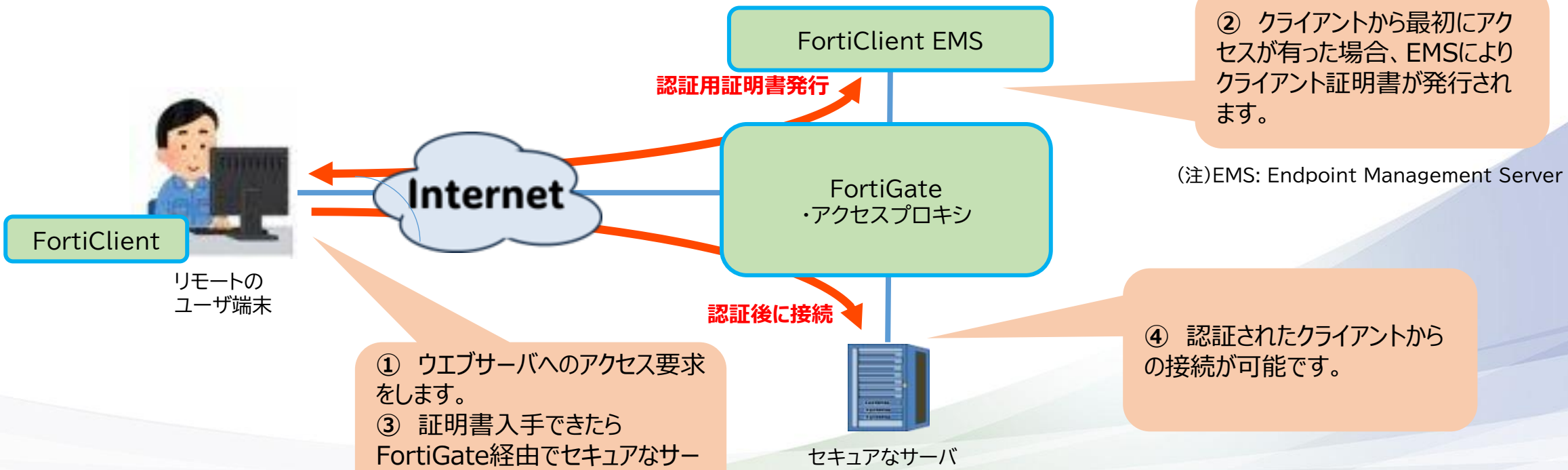
*） 詳細は「用語集」を参照して下さい

（用語集）ZTNA （FortiGateの例）

ZTNA（Zero Trust Network、ゼロトラストネットワークアクセス Access）では、ユーザからのアクセス要求がある度にユーザの認証情報や端末のセキュリティ状態が確認されます。

従来の境界型セキュリティ対策*と異なり、組織内、組織外にかかわらずアプリケーションへのアクセスがある度に認証・認可を行います。

以下の概念図ではFortiGate ZTNAの構成を示します。



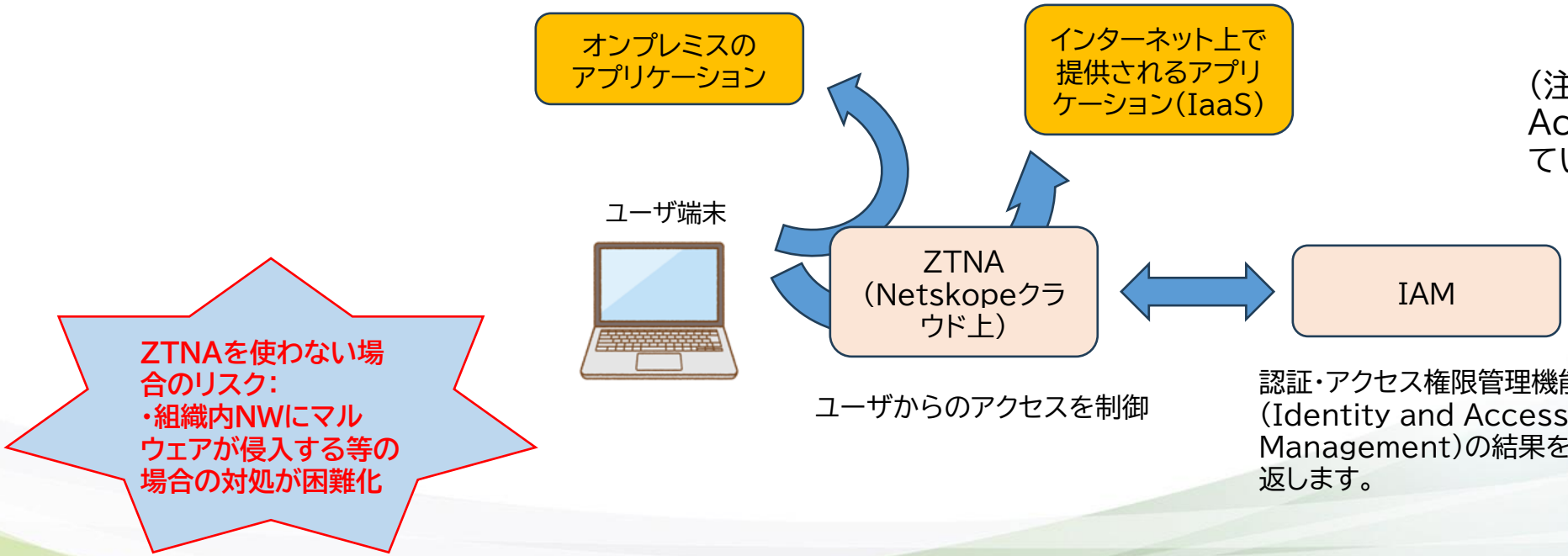
(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）ZTNA （Netskopeの例）

ZTNA（ゼロトラストネットワークアクセス - Zero Trust Network Access）では、ユーザからのアクセス要求がある度にユーザの認証情報や端末のセキュリティ状態が確認されます。

従来の境界型セキュリティ対策*と異なり、組織内、組織外にかかわらずアプリケーションへのアクセスがある度に認証・認可を行います。



（注）NPA（Netskope Private Access）製品での構成例を示しています。

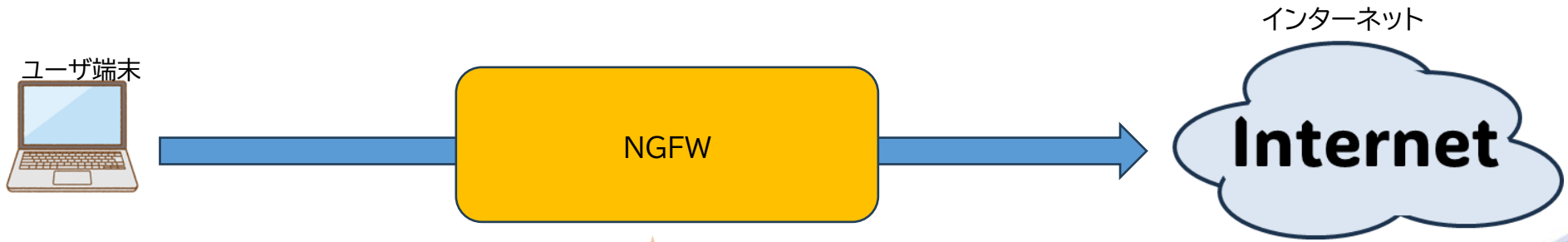
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）NGFW

NGFW（Next Generation FireWall）は従来のFWの機能に加え、アプリケーション層（HTTP等）の通信内容を解析し不審なアクセスを検知して通信可否の判断する機能を持ちます。

従来の旧式のFWの基本的機能である、発信元のIPアドレス、宛先のポート番号等を元に通信可否を判断するもの等が行われます。NGFWでは、アプリケーション層での通信内容を解析して、どのアプリケーションが通信を行っているか等の従来はIDS/IPS等で実施していたディープパケットインスペクション等も実現されています。



NGFWを使用せずに従来型のFWを使用した場合のリスクは次の通りです：
・同等の機能を装備するにはIDS／ISPを別途用意する必要がある

NGFWの応用例として次のようなアプリケーション毎の細かい制限等があります。
・一般的なWebへのアクセスは許可し、特定のWebサービスの利用だけを禁止

NGFWは、従来のFWになかった侵入防止システム（IPS）、ディープパケットインスペクション（DPI）、アプリケーション制御等の機能が含まれます。

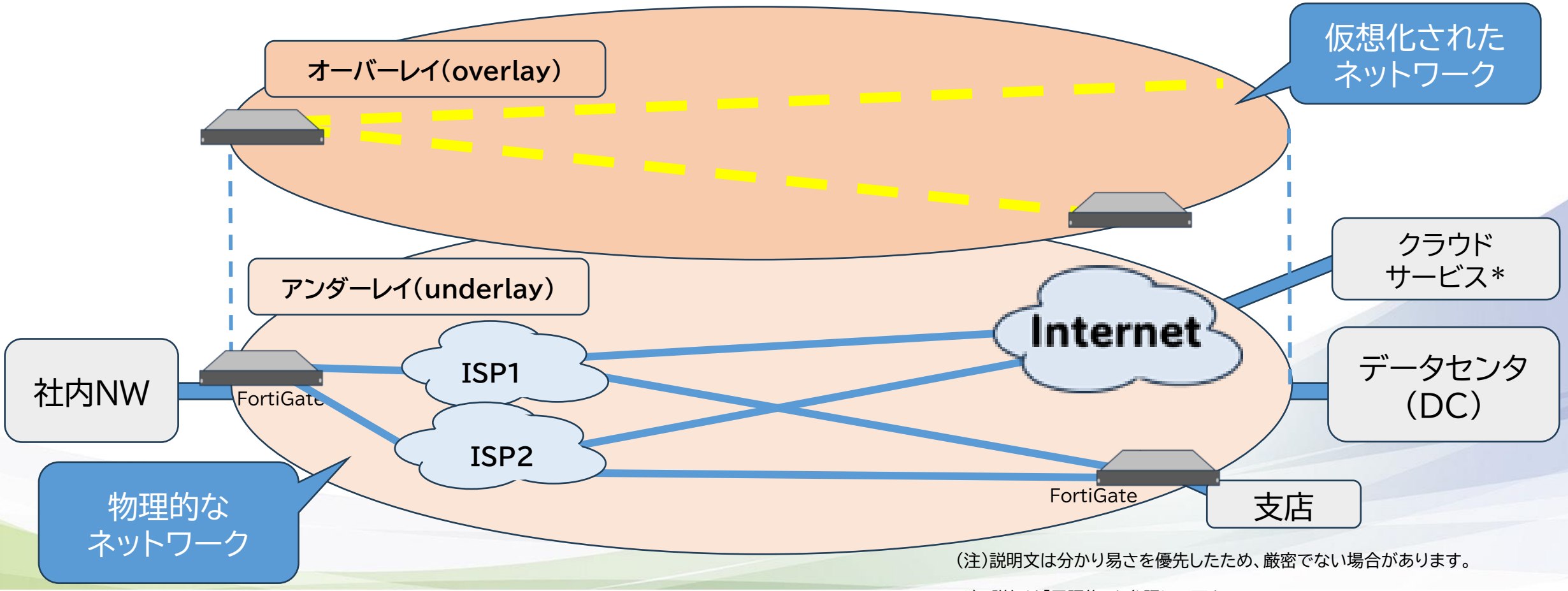
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）SD-WAN（FortiGateの例））

SD-WAN*（Software Defined Wide Area Networking）はソフトウェアによって仮想的な広域ネットワークを構成するものです。

物理的な回線をアンダーレイと呼び、種々（IP-VPN、専用線、公衆回線、インターネット、モバイル回線等）の回線を組み合わせることが出来ます。これらを用いて仮想敵なオーバレイ回線に対応させてメインの回線、バックアップの回線等設定し、回線障害時に自動的に迂回させる等が行えます。



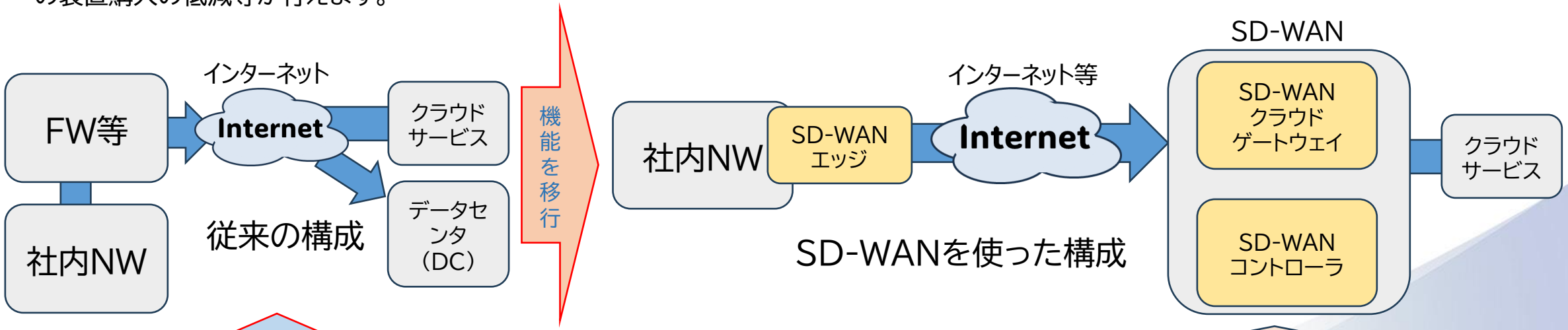
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）SD-WAN

SD-WAN（Software Defined Wide Area Network）はソフトウェアによって仮想的な広域ネットワークを作る技術を言います。

これはSDN（ソフトウェア定義ネットワーク - Software Defined Network）の技術をWAN（広域通信網 - Wide Area Network）に適用したものです。これを利用することにより、クラウドコンピューティングへの接続との親和性が良く、ネットワークの拡張性があり、負荷分散時の装置購入の低減等が行えます。



SD-WANを使わなかった場合のリスクには次のようなものがあります。
・クラウドサービス利用のためのFW等装置購入が必要
・拡張時にセキュリティ確保の工数増大

主に以下の機能～構成されます。
・SD-WANエッジ：オフィス等の拠点に設置されその拠点でのNW接続を管理します。
・SD-WANクラウドゲートウェイ：クラウドサービスとの間での通信確保します。
・SD-WANコントローラ：SD-WAN全体の設定、管理、監視を行います。

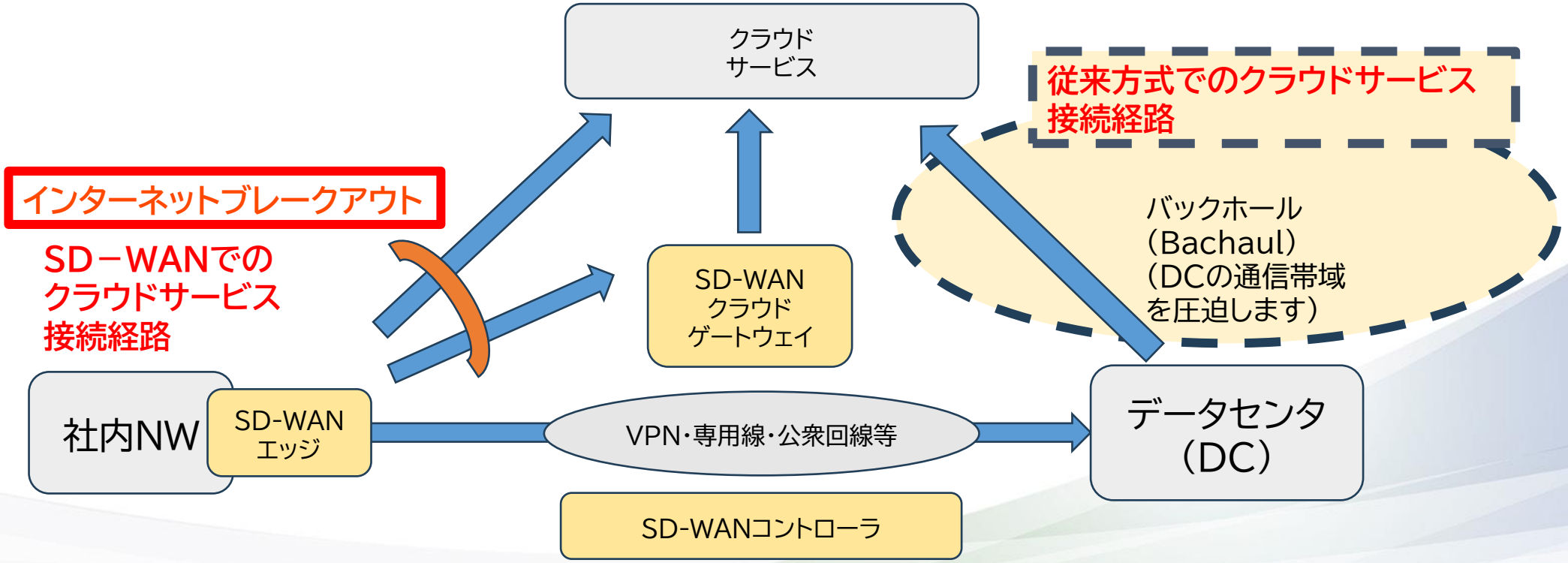
（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）インターネットブレークアウト

インターネットブレークアウトは、SD-WAN*（Software Defined Wide Area Networking）で接続先によってインターネットを経由して接続する機能を言います。

従来は各拠点からインターネットへ接続する場合、本社のデータセンタ（DC）経由で接続する場合があり、通信が輻輳（ふくそう、混雑）につながります。SD-WANでは接続先アプリケーションを識別し、それぞれ別の回線を割り当てることができ、危険の少ないクラウドサービスに対して直接インターネット経由で接続することができます。この機能をインターネットブレークアウトと言います。



（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

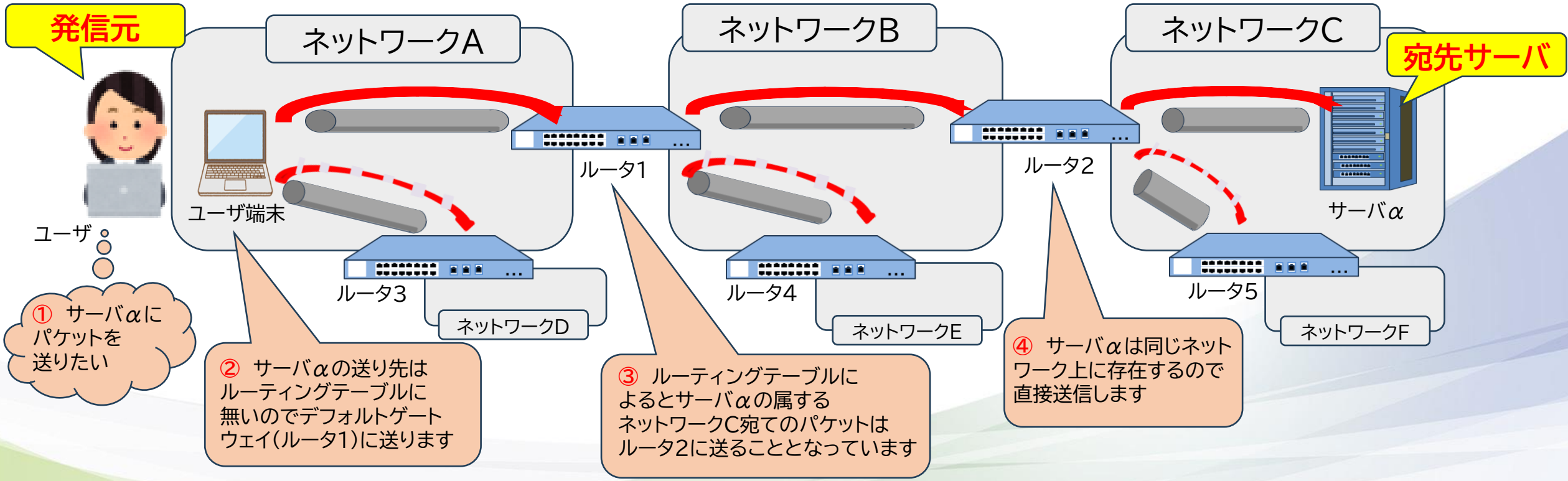
（用語集）

インターネットサービス

（用語集）ルーティング

IPパケットのルーティングは、PC等が送信したIPパケットを宛先のサーバ等に送り届けるために、中継に使用すべきルータ等のネットワーク機器等を選択して経由させる手法を言います。

各ネットワーク機器はルーティングテーブル(指定されたIPアドレスをどのネットワーク機器に転送するかが記述されている表)を持っており、これに基づき転送先を選択します。明確に転送先が選択できないIPパケットはデフォルトゲートウェイに転送します。ルーティングテーブルの設定方法にはあらかじめ固定的に設定する静的(スタティック)ルーティング、隣接するルータへ情報を伝搬させる動的(ダイナミック)ルーティング等の方式が有ります。



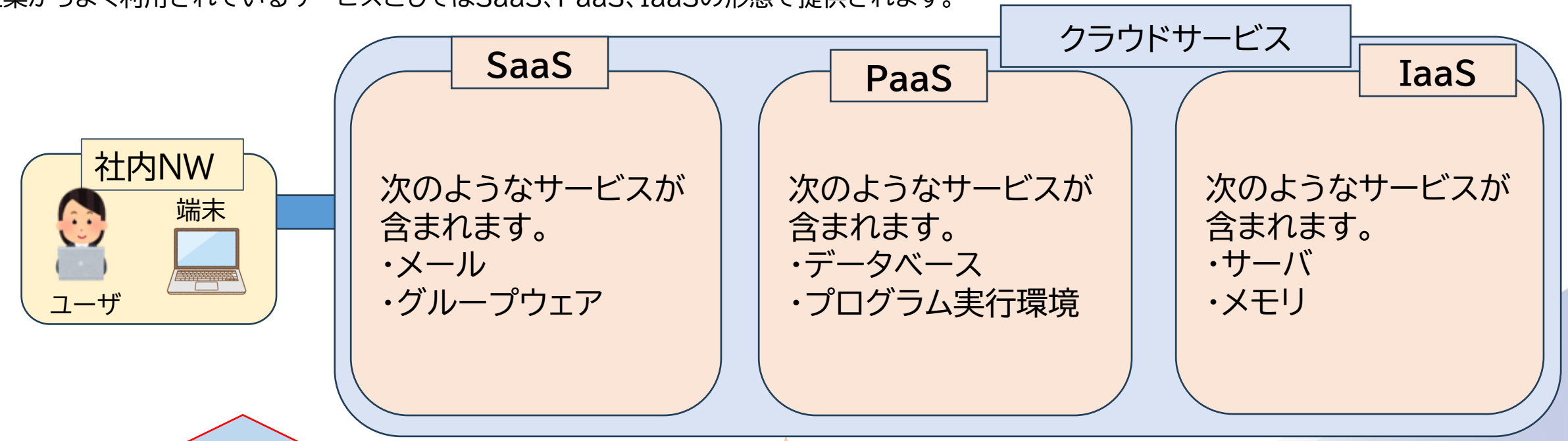
(注)説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

（用語集）クラウドサービス（SaaS、PaaS、IaaS）

クラウドサービス（Coud Service）は、インターネット経由で利用できるソフトウェアやインフラなどの機能が利用できるサービスです。

企業からよく利用されているサービスとしてはSaaS、PaaS、IaaSの形態で提供されます。



クラウドサービスを利用しない場合のリスクは次の通りです。
・利用した場合に削減できる導入・運用コストが高価となる

クラウドサービスの種別は次のようなものです。
・SaaS（Software as a Service）：メール機能等ソフトウェア（アプリケーション）機能のみを提供
・PaaS（Platform as a Service）：プログラムの実行環境等プラットフォーム機能を提供
・IaaS（Infrastructure as a Service）：サーバ等のインフラ機能を提供

（注）説明文は分かり易さを優先したため、厳密でない場合があります。

*） 詳細は「用語集」を参照して下さい

お客様と共に進化し続けるバリューパートナー

お客様に真摯に向き合い、時流を読みながら常に革新的なご提案を行い、
新しい価値を生み出し続けるパートナーでありたい、それが私たちの目指す姿です。