作って終わりではない
ゼロトラストセキュリティの運用サイクル

キヤノンITソリューションズ株式会社
サイバーセキュリティラボ
山田　和政

私たちについて

- キヤノンITソリューションズはキヤノンマーケティングジャパングループのITソリューション事業を担う企業です。
- 私たちはその事業の中でも、専門知識を駆使してお客様の業界・業種に共通するセキュリティの課題を解決する組織として活動しています。
- マルウェア解析やスレットハンティングの豊富な経験を活かし、お客様のビジネスをサイバー脅威から守ります。

本セッションの概要

- ゼロトラストを導入する理由
- ゼロトラストモデルの実現
- ゼロトラストと上手く付き合っていくために
- 弊社が提供する脅威分析サービスの紹介

ゼロトラストを導入する理由

ゼロトラストとは

これまで安全とされてきた仕組みも含めた**全て**を**信頼せず検証する**

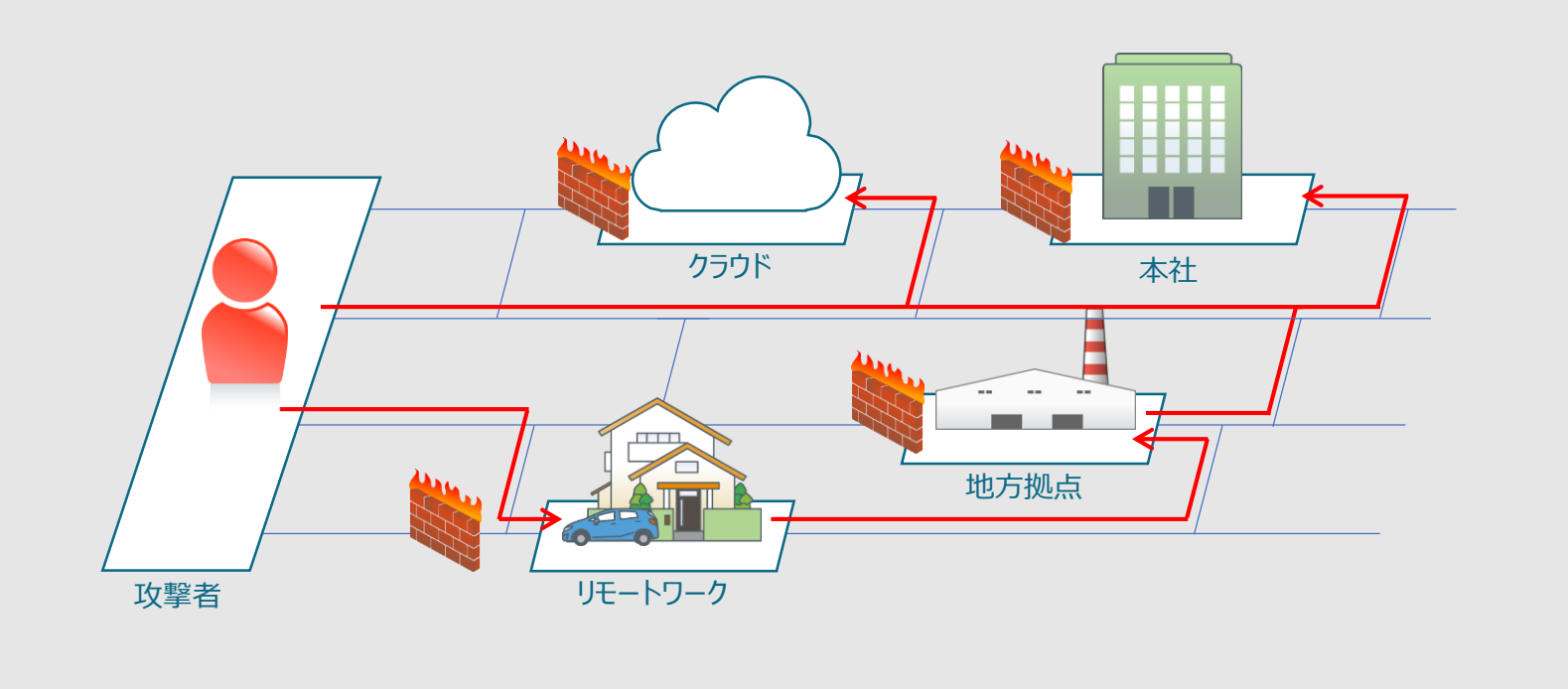
新たなセキュリティのコンセプトです。

要素	懸念
VPN	不正アクセスされるのでは？
ファイアウォール	すり抜けられるのでは？
アンチウイルス	検知出来ないマルウェアが存在するのでは？
社内ネットワーク	内部に悪意を持ったユーザーが居るのでは？
業務サーバー	既に攻撃者の踏み台にされているのでは？
取引先からのEメール	成りすましによる詐欺なのでは？
ユーザーアカウント	パスワードが漏えいしているのでは？

全てのリソースの利用を原則禁止する

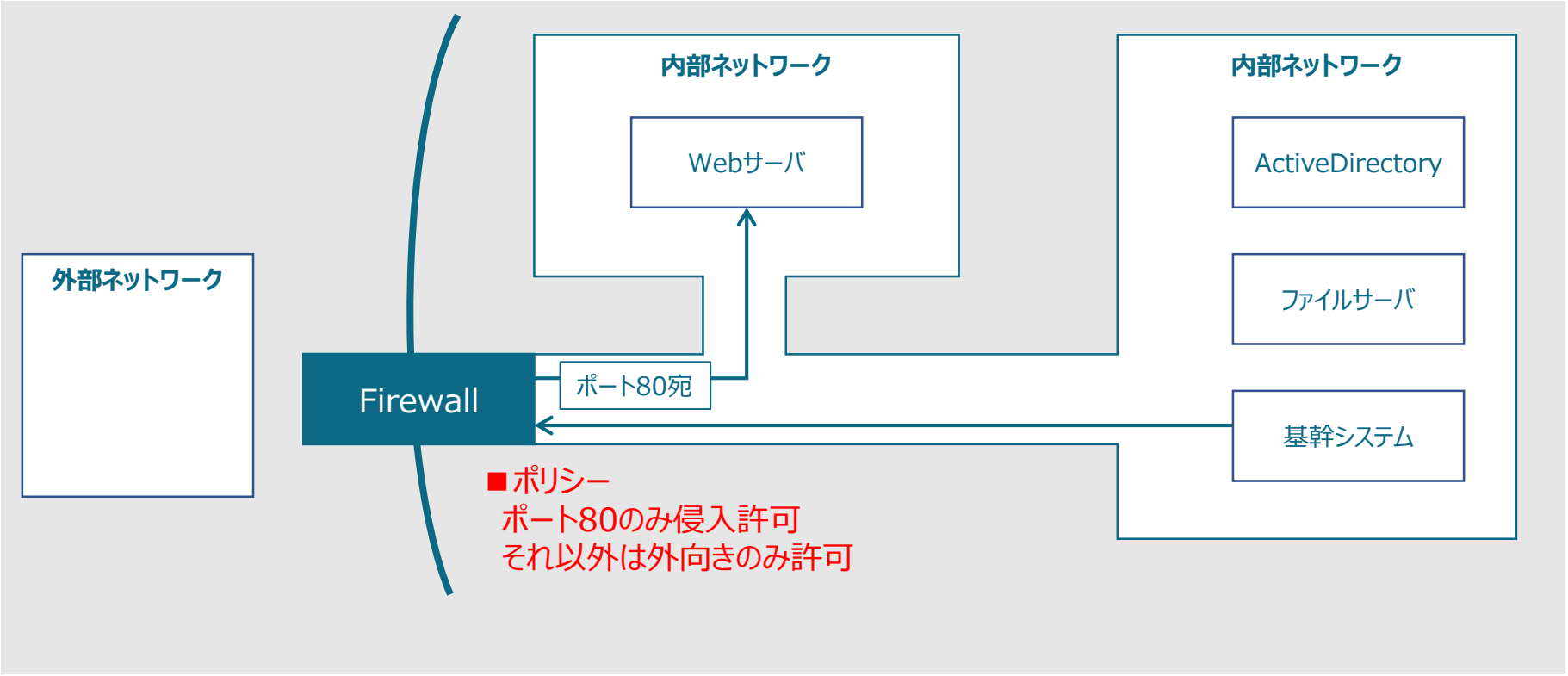
必要に応じてリクエストを検証し限定的に利用を許可する

なぜ、ゼロトラストが必要？



ITインフラの成長やクラウドコンピューティングの進歩により情報システムの脱・境界化が進みました。それに合わせて境界防御では手当しきれない脅威が増加し、日本国内でも境界を突破されたことによる大きな被害が報道されるようになりました。そこで、脅威が侵入したとしても**被害を最小化する方法**としてゼロトラストが求められています。

境界型セキュリティのイメージ

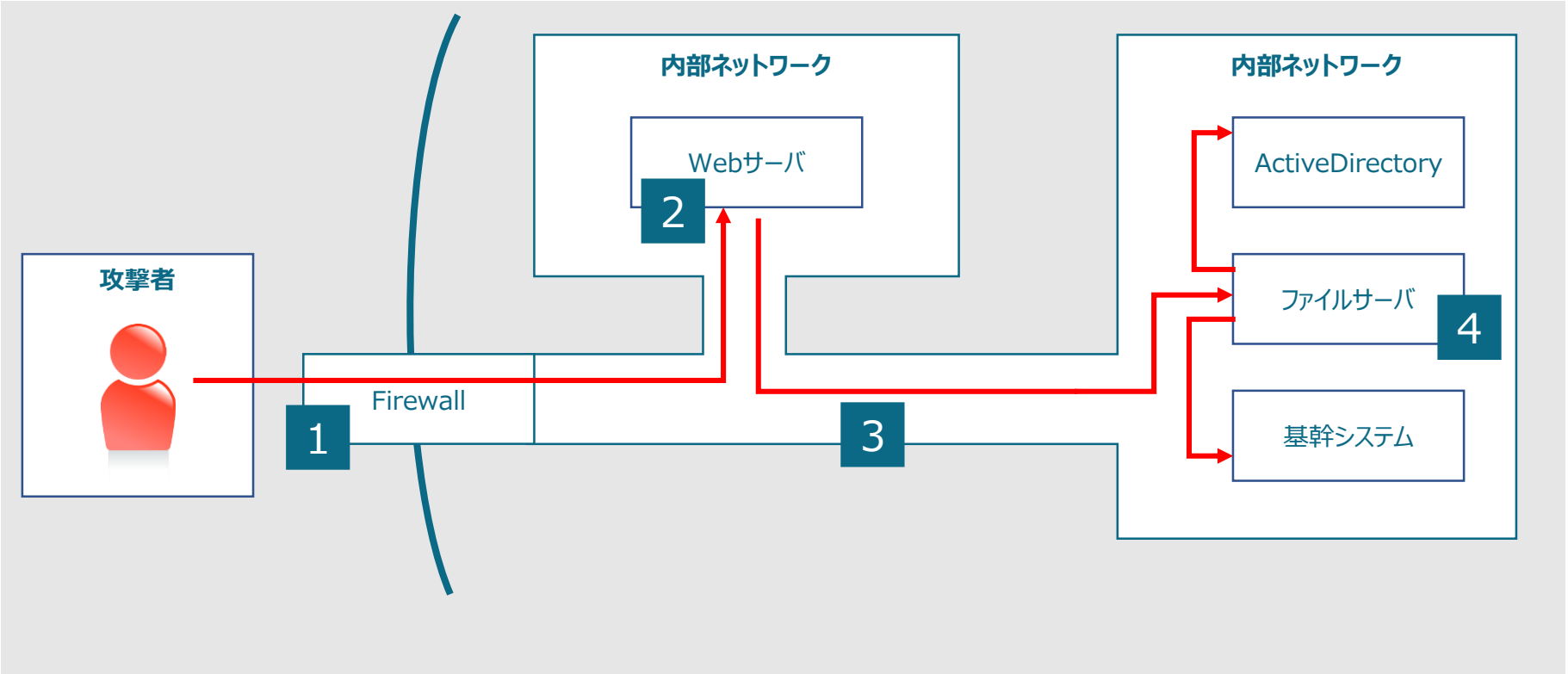


典型的な境界型セキュリティを例に挙げてゼロトラストの必要性を確認します。

ここにFirewallで外敵の侵入を防ぐ企業ネットワークがあります。この企業ではWebサーバを公開しており、ポート80番宛ての通信だけは例外的に内部へ通しています。

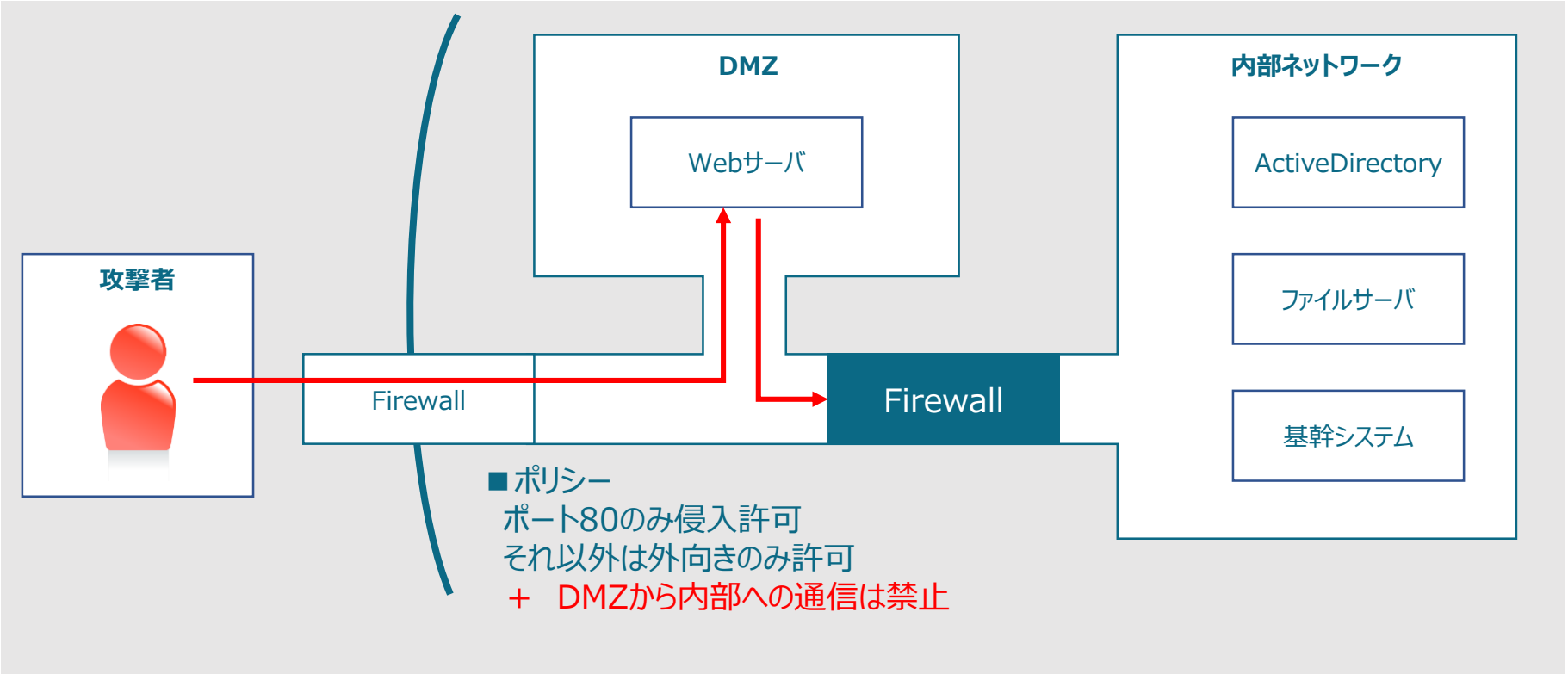
このようなネットワークに対して攻撃者が取る戦術のセオリーがあります。

境界型セキュリティに対する攻撃者の発想



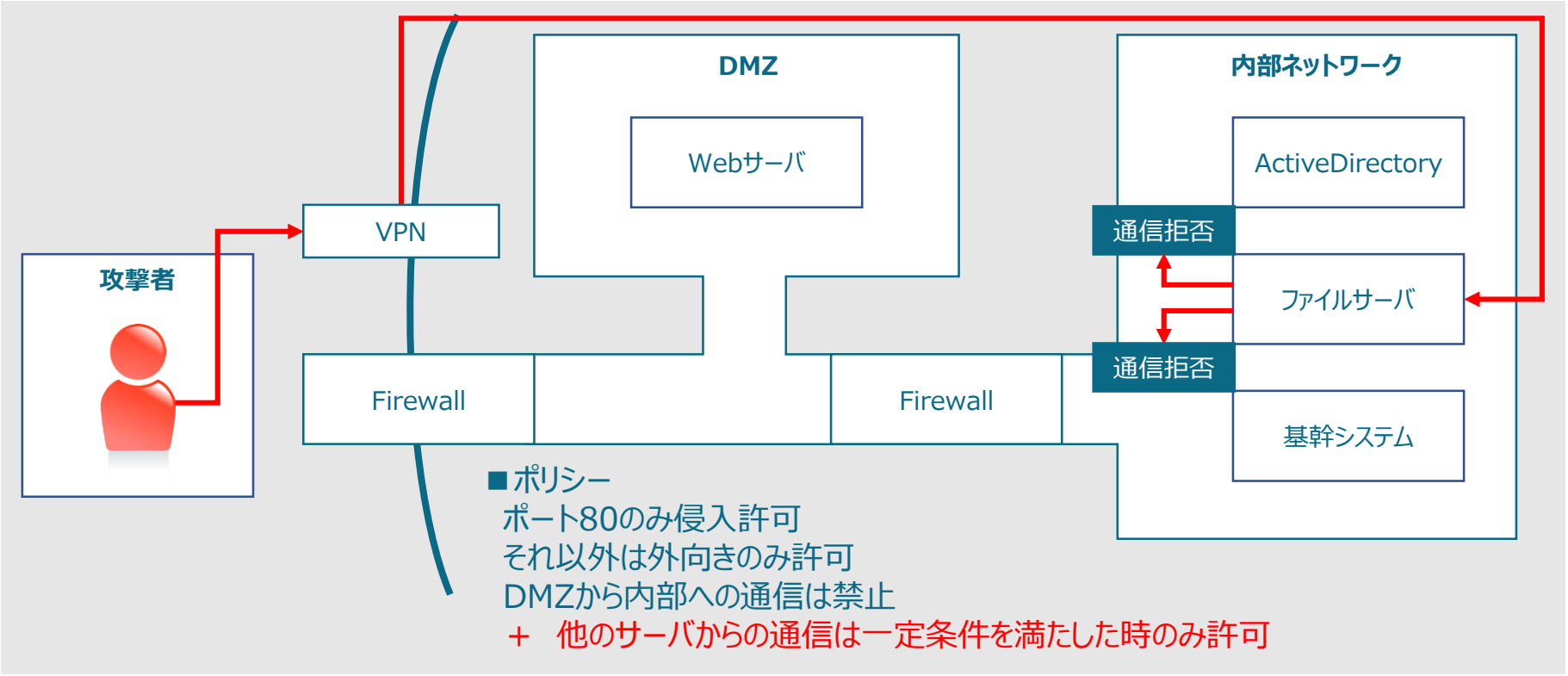
1 偵察	2 侵害	3 探索	4 水平展開
ポートスキャン サービススキャン 脆弱性スキャン	脆弱性の悪用 バックドアの永続化	端末の列挙 リソースマッピング	ブルートフォース 中間者攻撃 セッションハイジャック

攻撃されることを前提としたDMZ



公開サーバを踏み台にした攻撃にはDMZの構築が有効です。Webサーバが置かれたDMZはもはや信頼できない場所であり、内部ネットワークへの通信は境界線により遮断されています。重要なデータは信頼できる内部ネットワークに保管します。

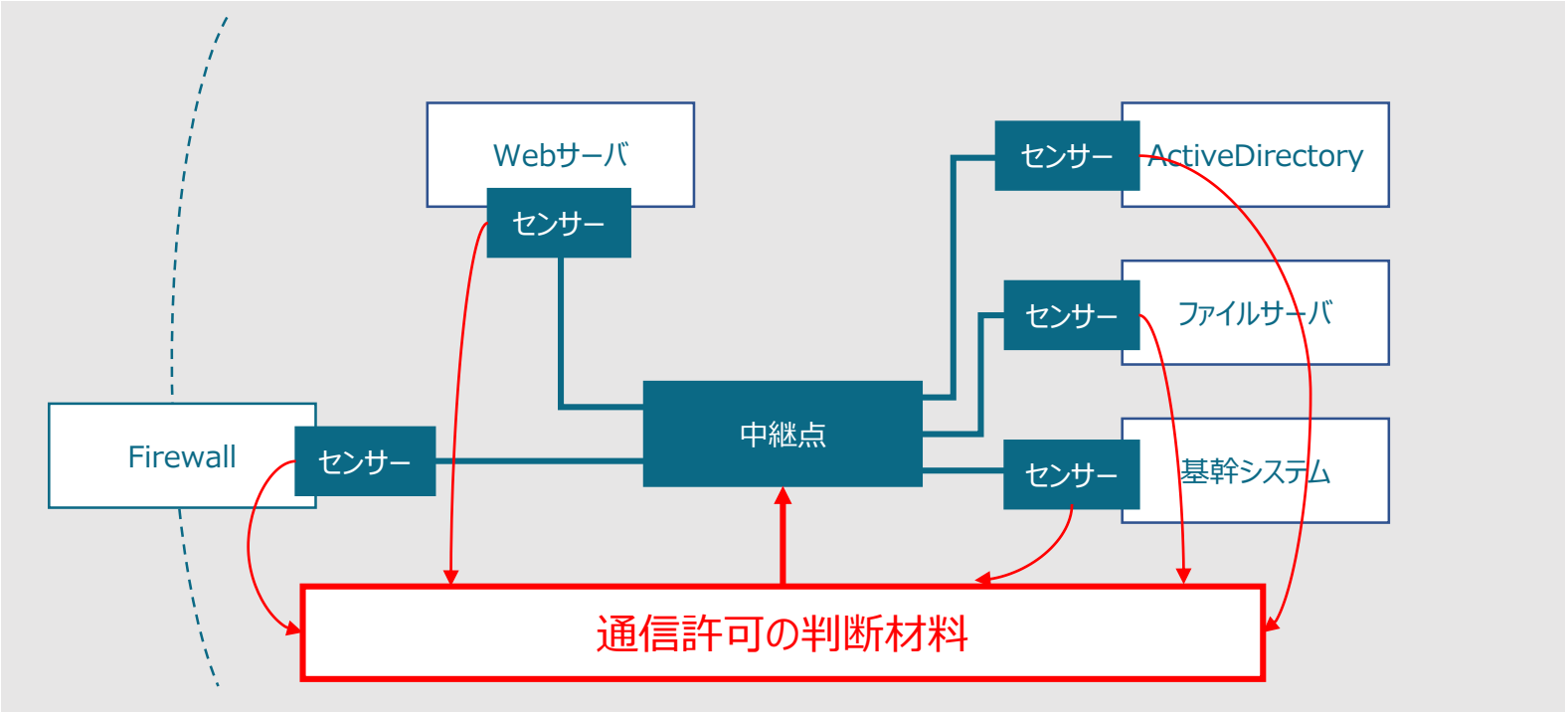
DMZからゼロトラストへ



ではDMZを介さずに内部ネットワークが攻撃を受けたら？2020年後半に報道された大規模なVPN侵害の事例は、これが机上の空論ではない事を証明しています。

この問いに対する一つの答えがゼロトラストです。内部ネットワークであろうと全ての通信を信頼せず、例外的に通信を許可する場合は疑いの目を向けて検査します。

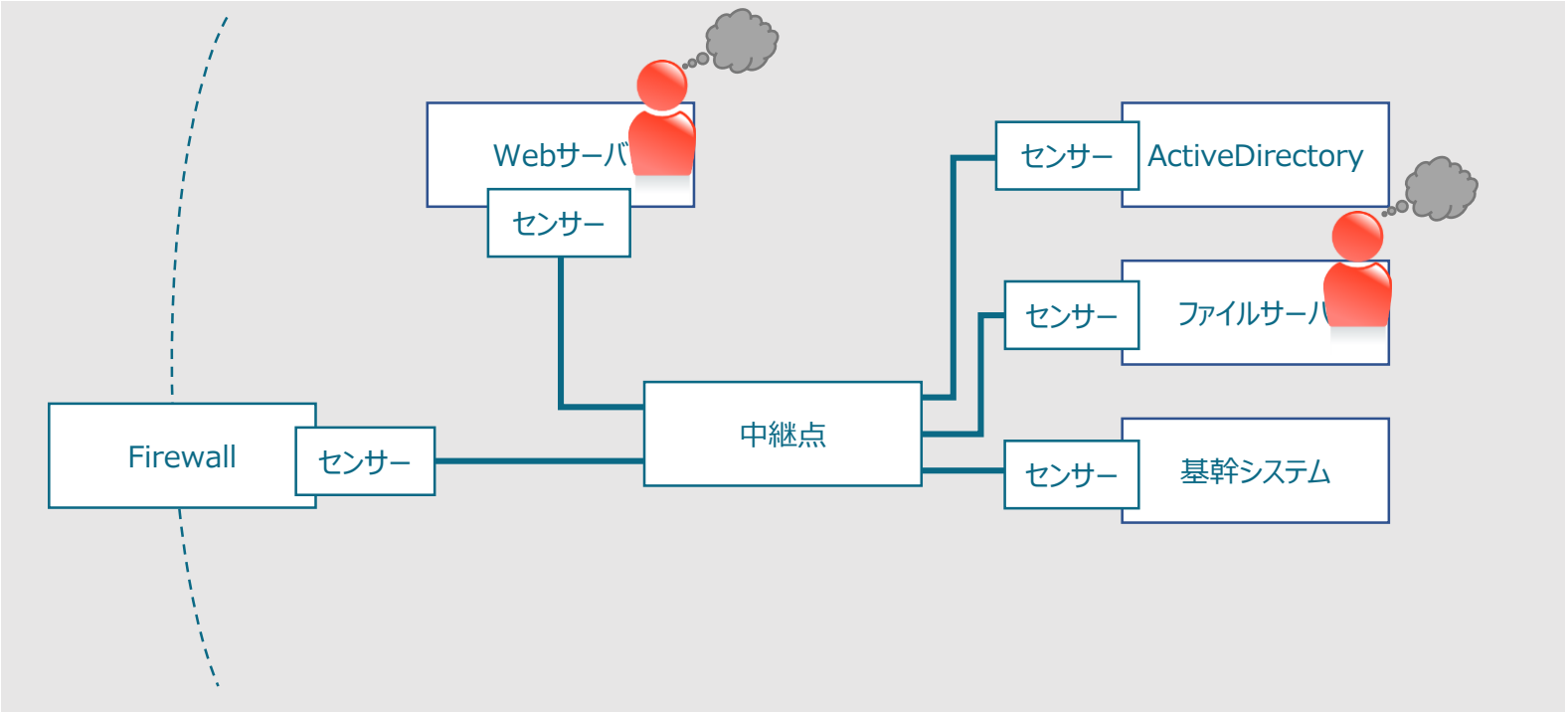
ゼロトラストのイメージ



ゼロトラストを実現するにはまずデバイス、アカウント、データなど全てのリソースの情報をリアルタイムで収集できるようなセンサーを用意します。集められた情報はリソースの中継点に送られ通信許可の判断が下されます。

ゼロトラストは内部に侵入した攻撃者に多くの制約を課します。

攻撃者に課される制約



侵害	探索	水平展開
センサーを停止する方法あるいはセンサーに気付かれない方法が必要	大規模なスキャンは控える長い時間を掛けて少しずつ探索する	ブルートフォースや中間者攻撃等の強引な手法は控える別口で認証情報を得る必要がある

攻撃者目線での評価

- 境界モデル

  内部侵入して権限を獲得することがテーマ

  監視の目が薄いので思い切った行動をとれる

- ゼロトラストモデル

  引き続き、内部侵入して権限を獲得することがテーマ

  ただし検知されないよう、やるべき作業が増え、取れる手段も限定される

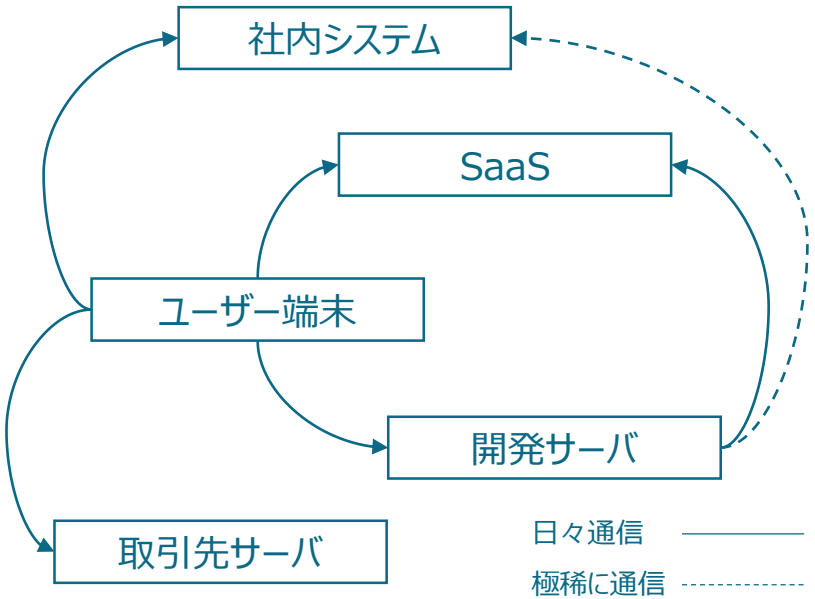
ゼロトラストは攻撃者にとって技術的・時間的な制約が多く、侵入したとしても目的を果たすことが難しくなります。

これによって**初期被害を最小化し、早い段階で対処できる**ようにする事がゼロトラストを導入する理由といえます。

ゼロトラストモデルの実装

ゼロトラストの第一歩

正常なネットワークフロー

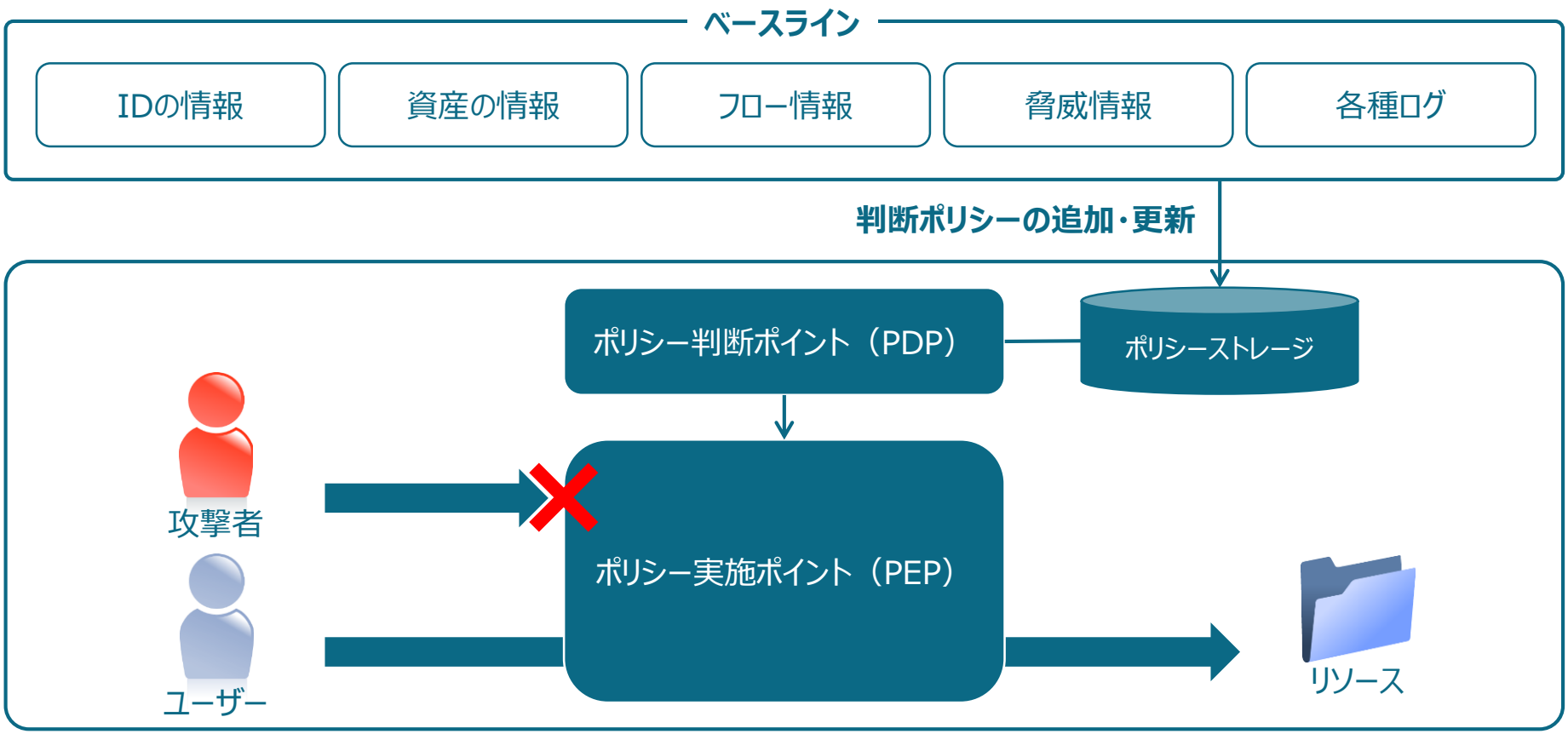


ネットワークフローの判断基準

ユーザー端末 → 社内システム は 信頼度〇
開発サーバ → 社内システム は 信頼度△
開発サーバ → 取引先サーバ は 信頼度×

ゼロトラスト導入の第一歩は正常な状態（ベースライン）を把握することです。そのうえで、ベースラインから外れたものは許可しない、アラートを上げる、または追加の情報を求められる仕組みを作ればゼロトラストの実現に近づきます。

ゼロトラストの心臓部



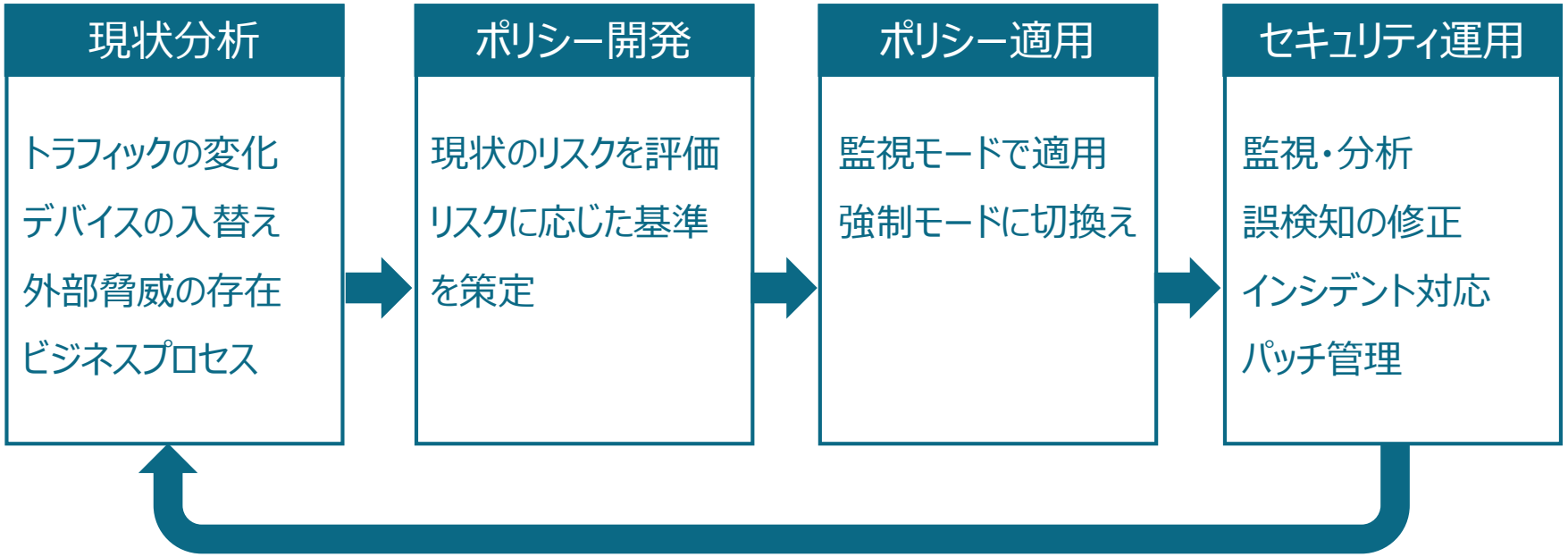
ゼロトラストを謳うソリューションは、ベースラインと比較して現状のリスクを算出し、どの程度の権限を与えるか判断する仕組み（PDP・PEP）を持っています。ゼロトラストモデルの構築は「ベースラインの活用とPDP・PEPの実装をどう具現化するか」と言い換えられます。

PDP・PEPの動作イメージ

これはPDP・PEPの実装としてID認識プロキシを構築する場合のイメージです。ポリシーに基づき信用スコアを算出し、通信毎に適切な権限を付与できるよう設定します。このポリシーこそがゼロトラストの能力を決める重要な要素であり、裏を返せば懸念すべき点でもあります。

ゼロトラストと上手く付き合っていくために

ゼロトラストの運用サイクル



組織によってビジネスプロセスが異なるため、動的ポリシーは各組織で定義する必要があります。また、導入当初は機能していたポリシーがビジネスの変化によって機能しなくなる可能性もあります。したがって、ポリシーの更新作業はゼロトラストの運用サイクルの中で重要な位置を占めています。

ポリシー更新の前提条件

1

守りたいリソースが列挙できているか？

例：ネットワークトラフィック、デバイス、保管されたファイル、ユーザーアカウント

2

そのリソースの状態を可視化できているか？

例：アクセスの急増、これまでにないリクエスト、エラーの発生状況

ゼロトラストの運用サイクルの中でポリシーを更新し、その効果を確認するには二つの前提条件が必要です。これを実現するには、異なる形式の様々なデータソースを一元管理して分析できるような可視化ソリューションが必要になります。

情報可視化の薦め

情報源の特徴	パケット	テキストログ	エンドポイント
導入し易さ	◎	△	×
監視範囲の広さ	○	◎	×
分析の解像度	○	×	◎

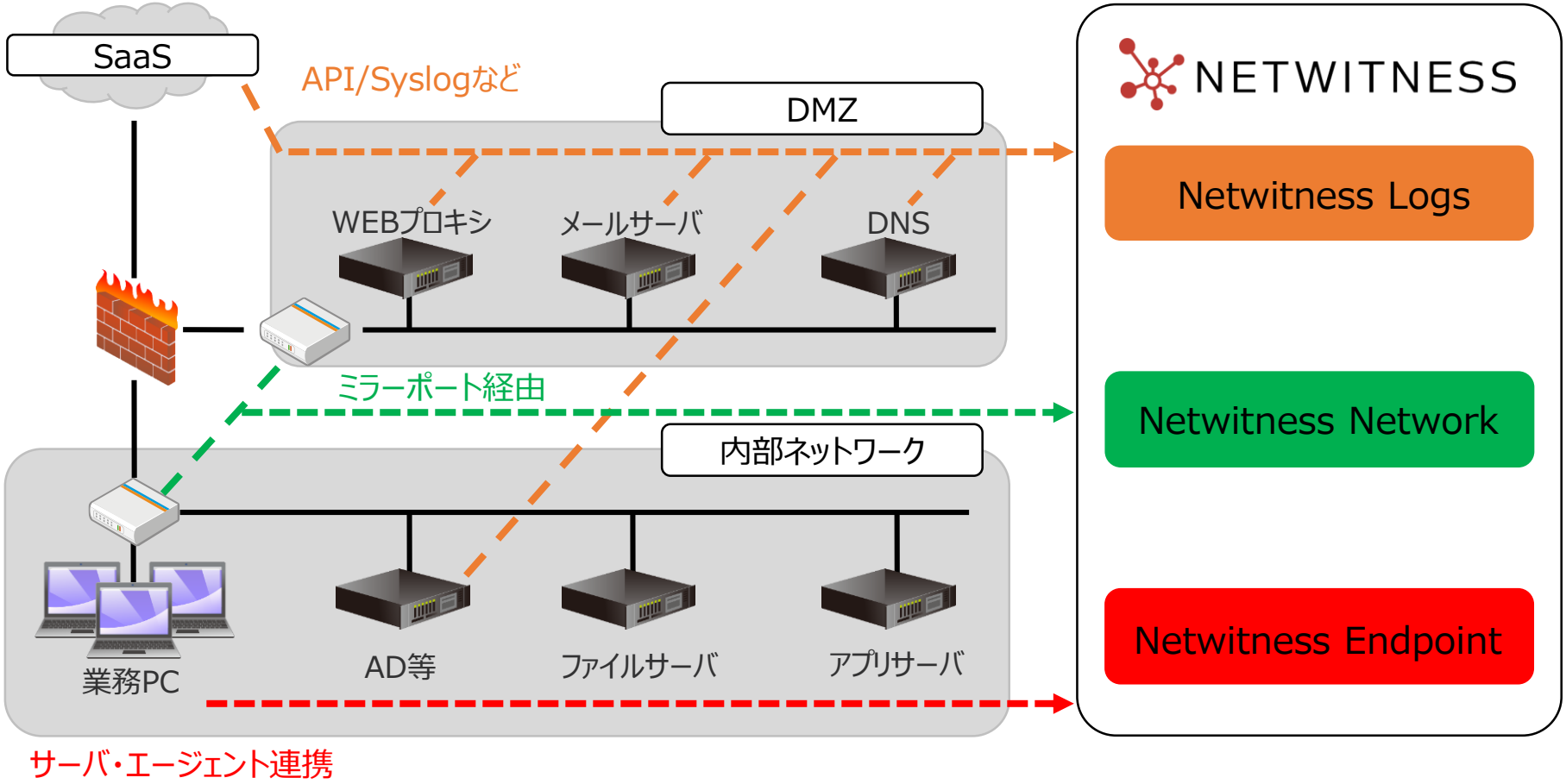
テキストログは情報量が少ないため広い範囲から情報を集めることが出来ます。しかし情報量が少ないゆえ詳細の把握は苦手で、出力設定および取り込み設定にも手間がかかります。

エンドポイントは端末内の挙動を高い精度で可視化できますが、監視対象の端末全てにエージェントをインストールする必要があり、組織が大きくなるほどコストがかかります。

パケットはテキストログとエンドポイントの中間に位置するようなカバー範囲の広さと情報の解像度を持ちます。何よりもスイッチのミラーポートに接続するだけですぐに分析を始められる点が大きな魅力です。

弊社では全くのゼロから始めようというお客様にはパケットの可視化をお勧めてしています。

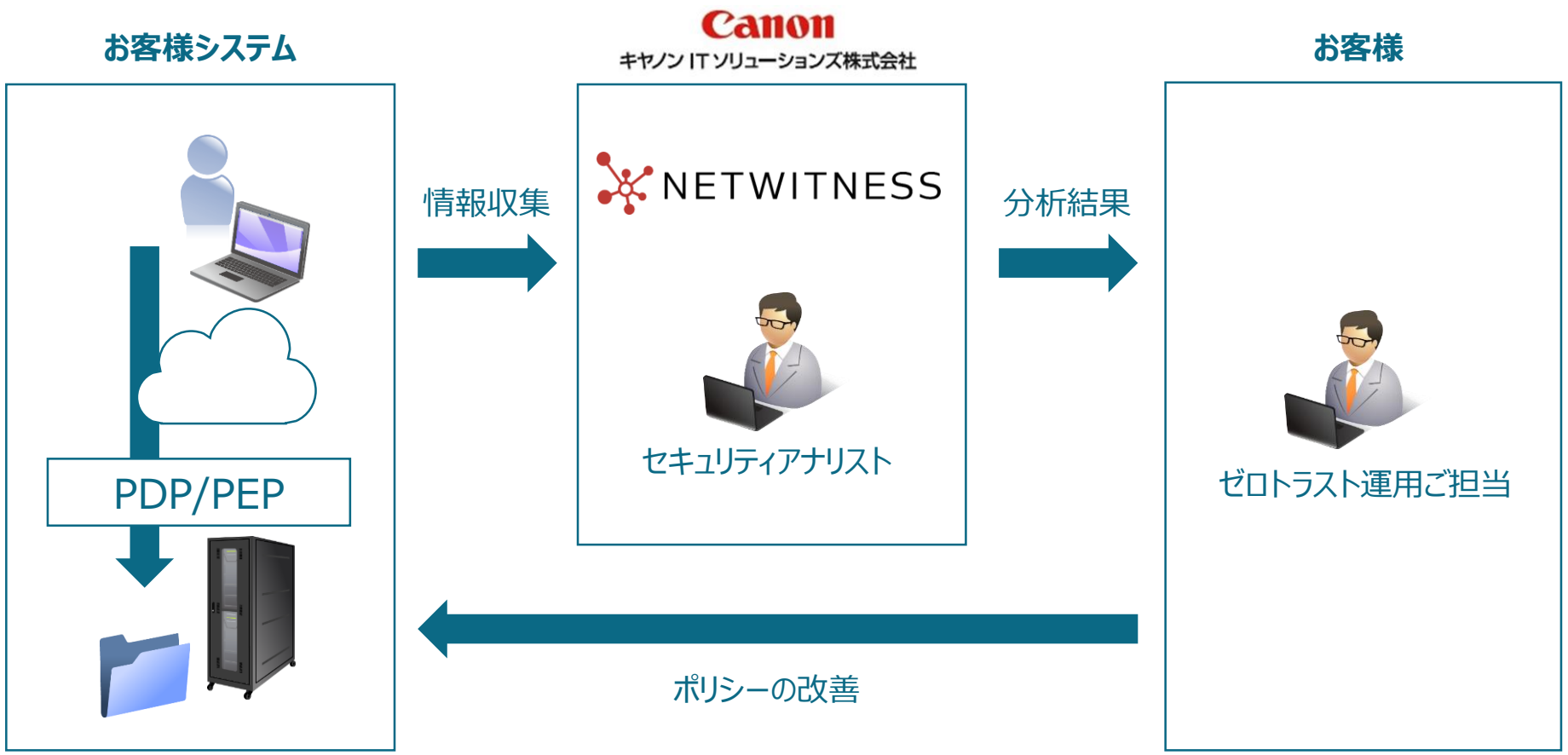
RSA Netwitness Platform の紹介



パケット分析から始めて他の情報の可視化に展開できるように、弊社ではパケット、テキストログ、エンドポイントの全てをカバーできる統合型SIEM **RSA Netwitness Platform** の導入・運用を推奨しています。

弊社が提供する脅威分析サービス の紹介

ゼロトラストにおけるNetwitnessのポジション



Netwitnessはお客様の環境から多くの情報を収集・分析し、お客様がポリシーを更新するための洞察を提供することが出来ます。特にパケット分析は他の情報源と比べて導入しやすく、かつ全体像を把握するのに向いています。脅威分析に習熟した弊社のセキュリティアナリストがこれをサポートします。

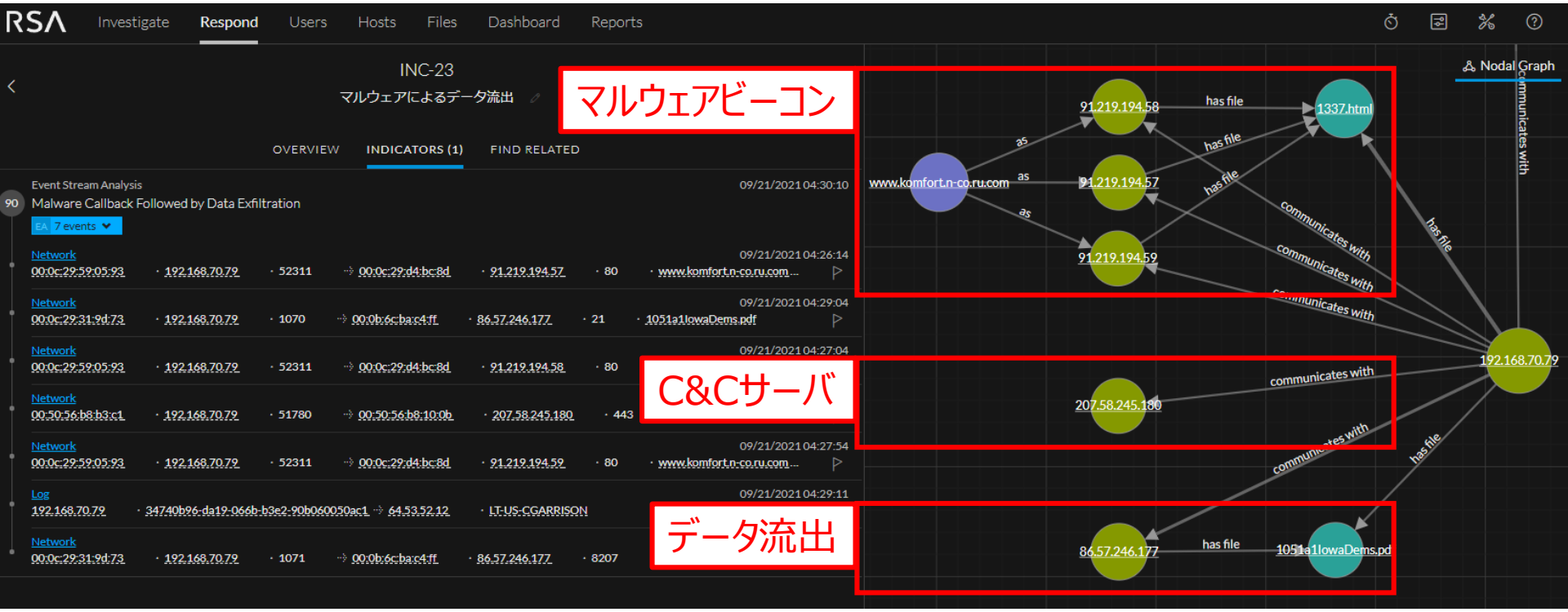
トラフィック全体に対する可視化

グレーアウトしている項目は脅威と判定されたパケット

現時点で脅威と判定されていないパケットも分析可能

Netwitnessは脅威と判定されたパケットだけでなく、正常と判断されたパケットを含むすべてのトラフィックを分析することが出来ます。これにより、巧妙な攻撃者がセキュリティソリューションに検知されないような手法を用いたとしても、人間の目で追跡することが出来るようになります。

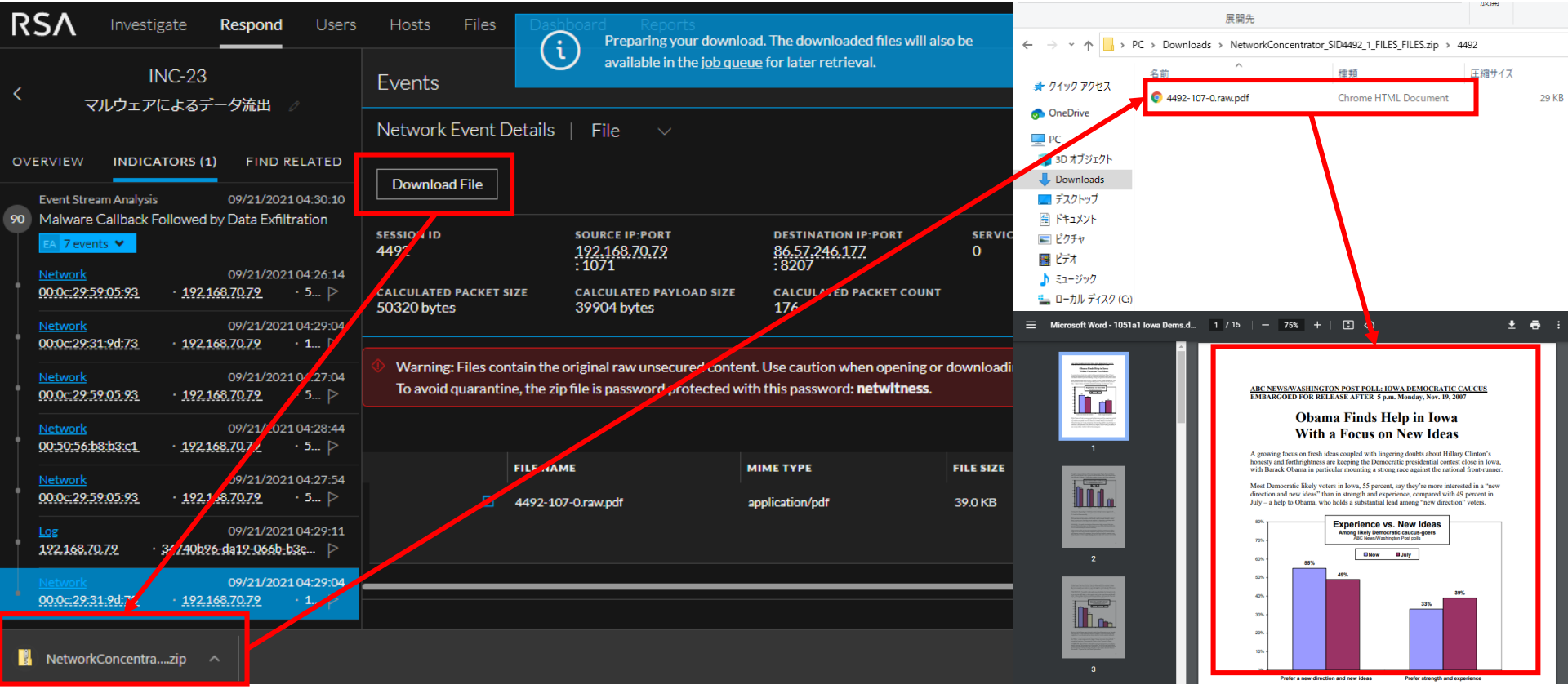
インシデントの全体像を把握



ネットワークに潜む脅威を発見した場合、その全体像をグラフで表現することが出来ます。

インシデントの影響範囲を速やかに特定できることに加え、この脅威を防ぐためにどのようにポリシーを変更すべきか検討する切っ掛けを与えてくれます。

パケットの再構築

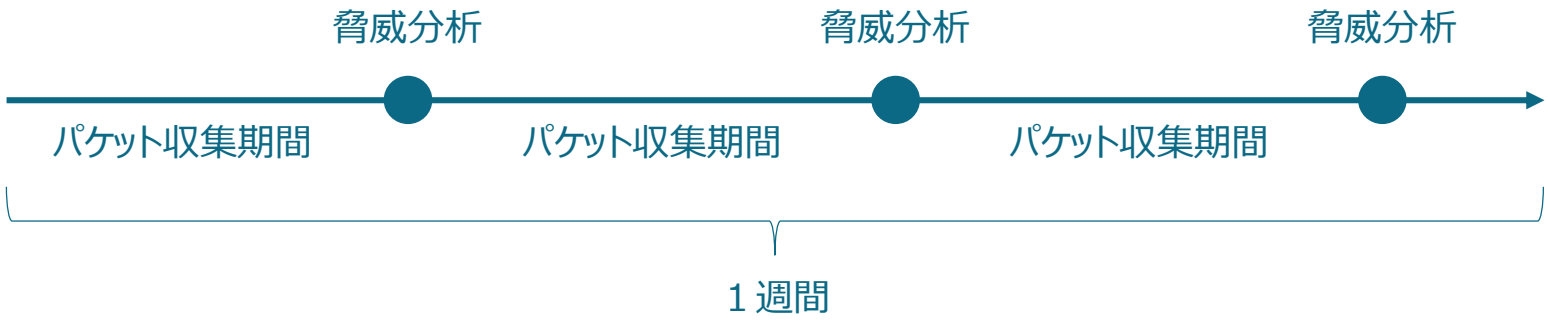


脅威として特定されたパケットから元のデータを再構築することが可能です。攻撃者が使ったプログラムファイルや漏えいしたデータなどをお客様の手元で確認することが出来るようになり、フォレンジックや証拠保全にもご利用頂けます。

脅威分析サービス

お客様の要望に応じて週に複数回パケットを分析します

その日の分析が終わった時点で即日分析レポートを提出します



１か月毎に分析結果を総括した月次レポートを提出します

月次報告会ではポリシー改善に向けたアドバイザリをご提供します

まとめ

ゼロトラストソリューションの性能を完全に引き出すには、お客様による適切な運用が必要です。

その為にお客様は、運用の判断材料を集めるという新たな課題に取り組む必要があります。

RSA NetwitnessとキヤノンITソリューションズの脅威分析サービスがその課題解決を強力にサポートいたします。

ゼロトラストの価値を最大限に引き出すために、私たちがお客様のビジネスに貢献できる日を楽しみにしています。