入札に負けない提案を可能とするパロアルトネットワークスのPAシリーズ

はじめに
（最近のセキュリティトレンド：ゼロトラストモデル）

ゼロトラストとは？

- 企業を狙ったサイバー攻撃は増え続けており，もはや従来の境界集中型セキュリティ戦略では攻撃を防ぎ切れないことは明白となってきている．こうしたアーキテクチャの機能不全の原因は，「組織のネットワーク 内は安全」という時代遅れの思い込みと，従来の対策ではネットワー ク境界を通過するアプリケーショントラフィックに十分な可視性や制御，保護を提供できない．

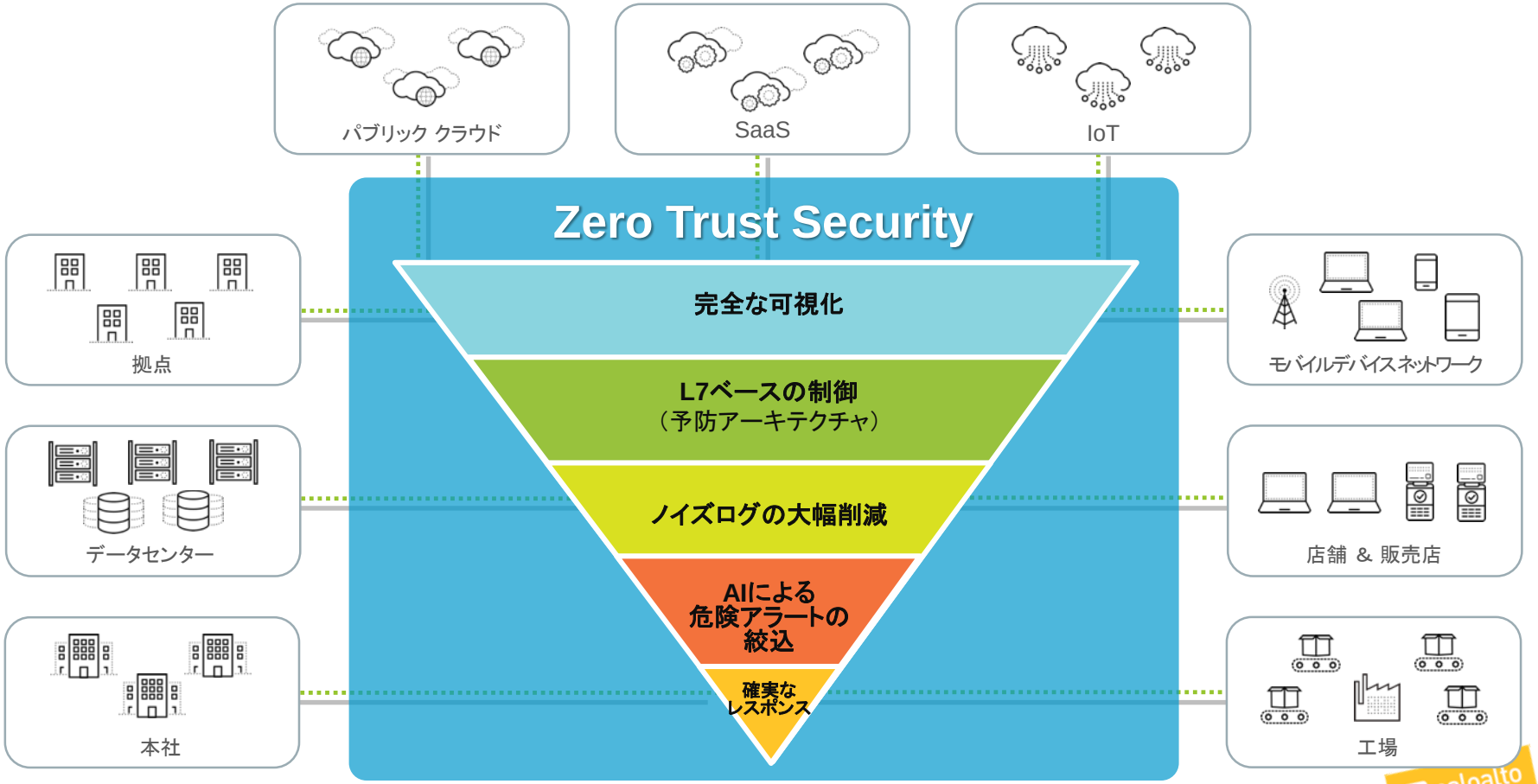
- Forrester Research が初めて紹介した概念，「ゼロトラスト」は，信頼できるという前提を取り除いて穴だらけの境界集中型戦略の欠陥に対応する，従来とは異なるセキュリティ モデル

- ゼロトラストで展開される基本セキュリティ機能では，どこにあるかに関係なく，すべてのユーザ，デバイス，アプリケーション，データリソースおよびそれらすべての間の通信トラフィックにポリシーが適用され，保護が提供される．

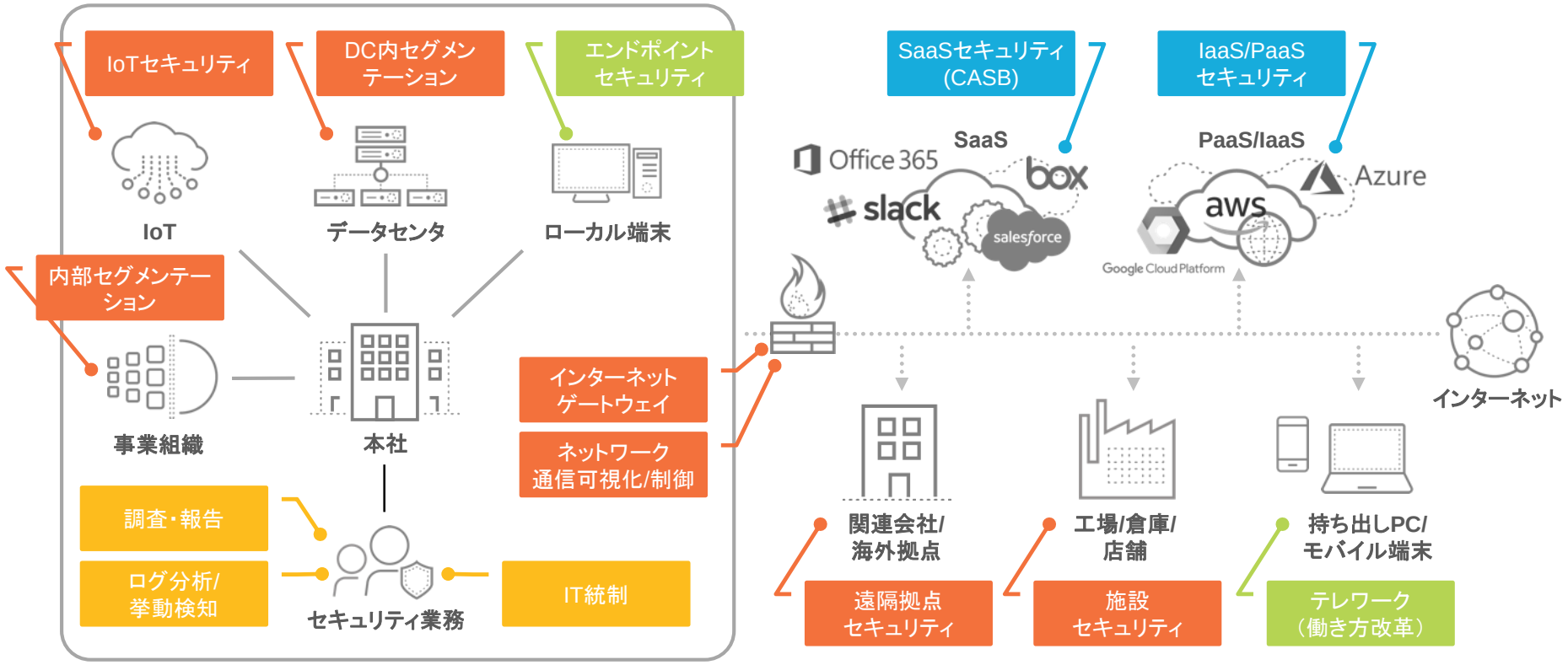
ゼロトラストの基本的な考え方

1. 社内・社外ネットワーク問わず，全てのリソースが安全な方法でアクセスされる
2. 「必要最低限の情報だけを知る」ことをベースにアクセス制御する
3. 何も信頼できないことを前提に全てを検証する
   - クローズドネットワークにおいても同様の考え
4. 全てのトラフィック，パケットを検査するとともにログを取得する
5. 「最も機密性の高い情報は何でどこにあるか？」を起点に，内側から外側に向けてセキュリティを設計する

Zero Trust Security with Prevention Architecture and Automation



企業内における様々なセキュリティポイント



昨今のサイバーセキュリティに必要なものは？

1. ネットワーク利用状況の把握とアプリケーション制限
   - 回線帯域の利用状況と設計
   - コンプライアンス違反のアプリケーション利用の把握や制限
2. 不審な通信の検知
   - TCP/UDPポート番号の誤用による不審な通信の検知
   - シグネチャベースでは検知できない不信な通信の検知
3. アプリケーション単位でのポリシー制御やQoS/経路制御など
4. クラウドと連携した最新の脅威情報に基づくトラフィック検査

- **アプリケーションレベルでの可視化（App-ID）**
- **コンプライアンス違反の把握と制御（HTTP Header Insertion）**

次世代FWの特徴（アプリケーション識別機能（App-ID））

業務アプリ

私用アプリ

1 識別

SaaSからSNS，有害なファイル共有まで、**2,800以上のアプリケーションを自動的に識別**

2 可視化

アプリ/ユーザ*ごとに通信状況を可視化，**リスクの高い通信を一目で把握**可能に

*AD連携時やSyslog連携などユーザ識別機能（User-ID）利用時

3 制御

アプリ/ユーザ*ごとにアクセスの許可/禁止のポリシを設定，**危険・不要な通信を制御**

アクセス制御の設定例

- クラウドサービスごとに許可/禁止
- ユーザー/部署ごとに許可/禁止
- 条件設定による制限付き許可

次世代FWと言っても…（App-IDの特徴（vs. 競合他社））

- パロアルトネットワークス：App-ID
  - PAを通過する全ての通信を対象としてアプリケーションを識別
  - Default（初期状態）設定で，アプリケーション識別を実行
  - 本機能使用によるスループットの劣化ナシ
  - 全ての通信を精査した上で，” Unknown “のあぶり出しが可能
    - つまり，疑わしい通信を識別および制御が可能

- 競合他社：アプリケーション識別
  - 設定により識別するアプリケーションを選択
    - 全ての通信を対象とする場合，サポートする全てのアプリケーションを識別する設定が必要
  - アプリ識別設定をすることによるスループットの劣化
    - データシートには，以下のような記載となっており，「NGFWスループット」での比較が重要
      - FWスループット　　：L4（レガシー）レベルでのパフォーマンス
      - NGFWスループット　　：（限定的な）アプリケーション識別機能をONとしたパフォーマンス

とあるメーカのデータシート…

- どちらにおいてもアプリケーション識別機能をONにすると…

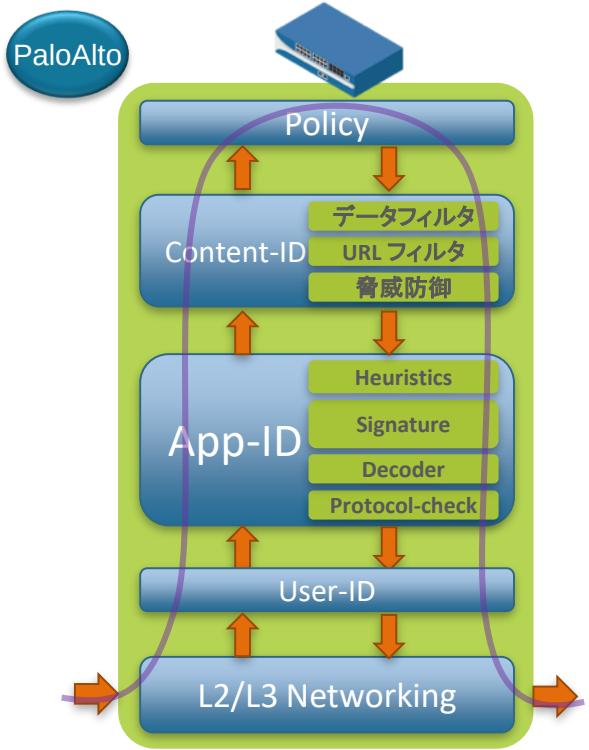
ファイアウォール・スループット（Gbps）	
理論上	14.5
実運用環境下[2]	4.2
VPNスループット（AES-128ビット暗号化、Gbps）	1.6
NGTPスループット（Mbps）	
実運用環境下[1]	250
同時接続数（単位： 100万）[1]	3.2/6.4

C社データシート

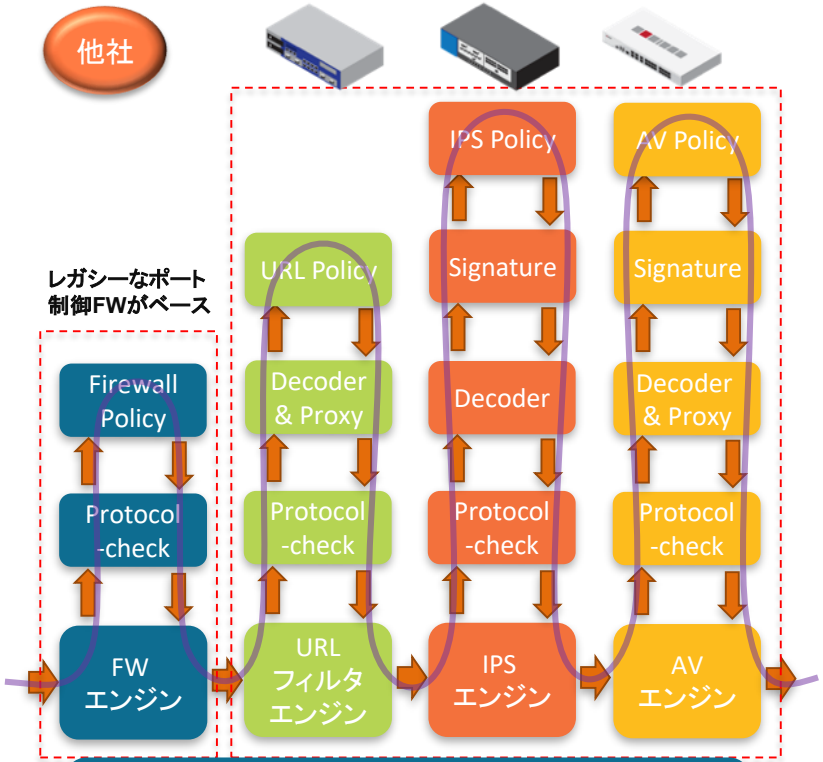
IPv4 ファイアウォールスループット（1518 / 512 / 64 バイトUDPパケット）	160 / 160 / 110 Gbps
アプリケーション制御スループット（HTTP 64 K）[2]	40 Gbps
NGFWスループット（エンタープライズトラフィック混合）[2、4]	20 Gbps
脅威保護スループット（エンタープライズトラフィック混合）[2、5]	13 Gbps

F社データシート

この違いはなんで？



1つのエンジンで処理をするのでパフォーマンスの劣化が少ない



相互機能間での検査結果の連携はなく，各々全ての工程を実施．
各機能の設定は，個別に管理

SaaS利用時のトラフィック制御
HTTP Header Insertion

同じアプリケーションでも，リスクは異なる！

企業用アカウント

Office 365 Enterprise account

G Suite

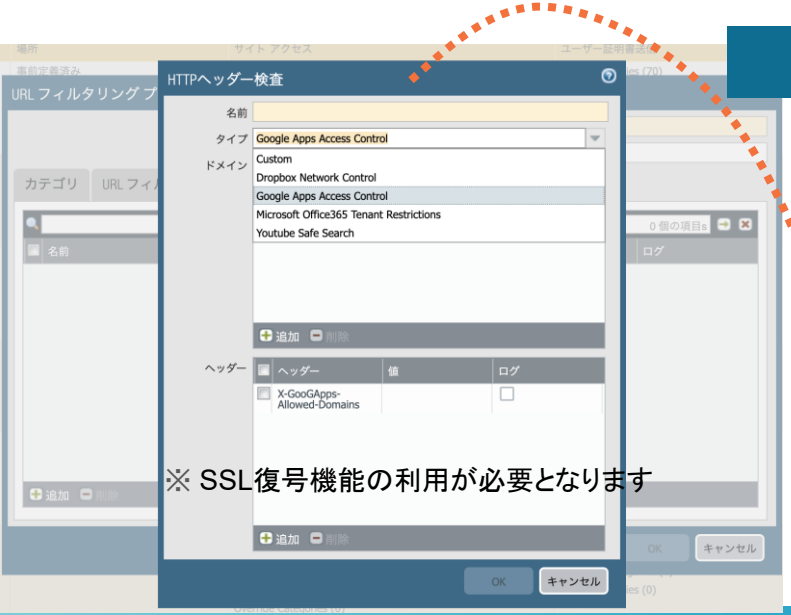
無料 / コンシューマ用アカウント

Office 365 Home / personal accounts

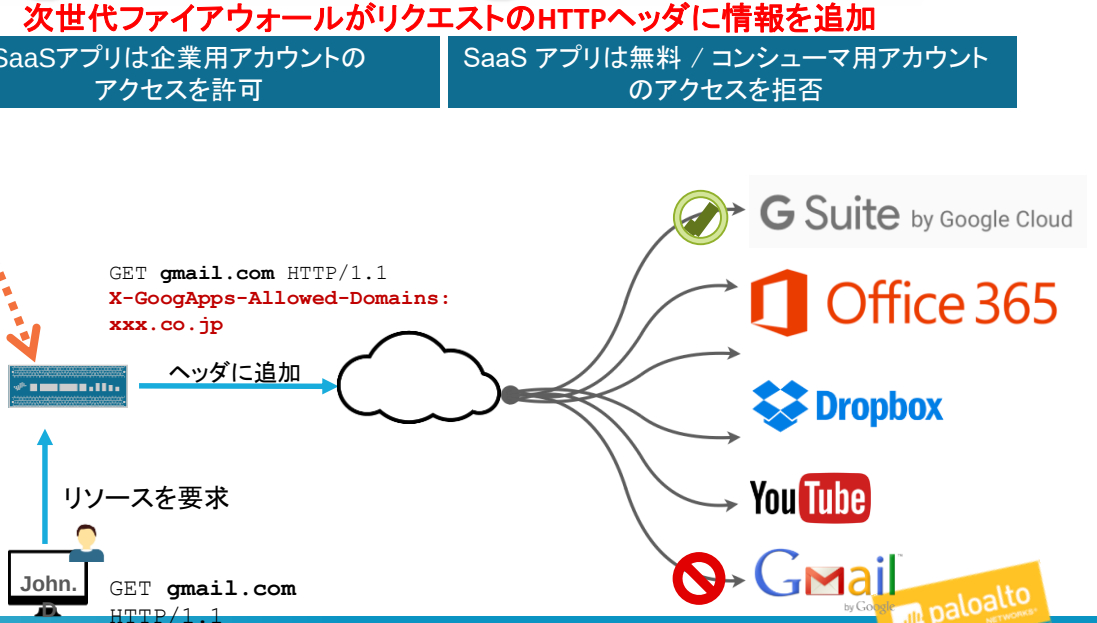
Gmail

次世代ファイアウォールがリクエストのHTTPヘッダに情報を追加

SaaSアプリは企業用アカウントのアクセスを許可	SaaS アプリは無料 / コンシューマ用アカウントのアクセスを拒否



※ SSL復号機能の利用が必要となります



運用者の悩み…

- FW導入/ リプレース時に
  - 既存Policyの要/ 不要の判断がつきづらい
  - Policyの最適化（アドレス集約，Policy削除）
  - Policyのアップデート（アプリケーションレベルでの制御へ）
  - Policyの事前動作チェック方法は？
    - テスター等不要でPolicyが期待する動作としてくれるか？

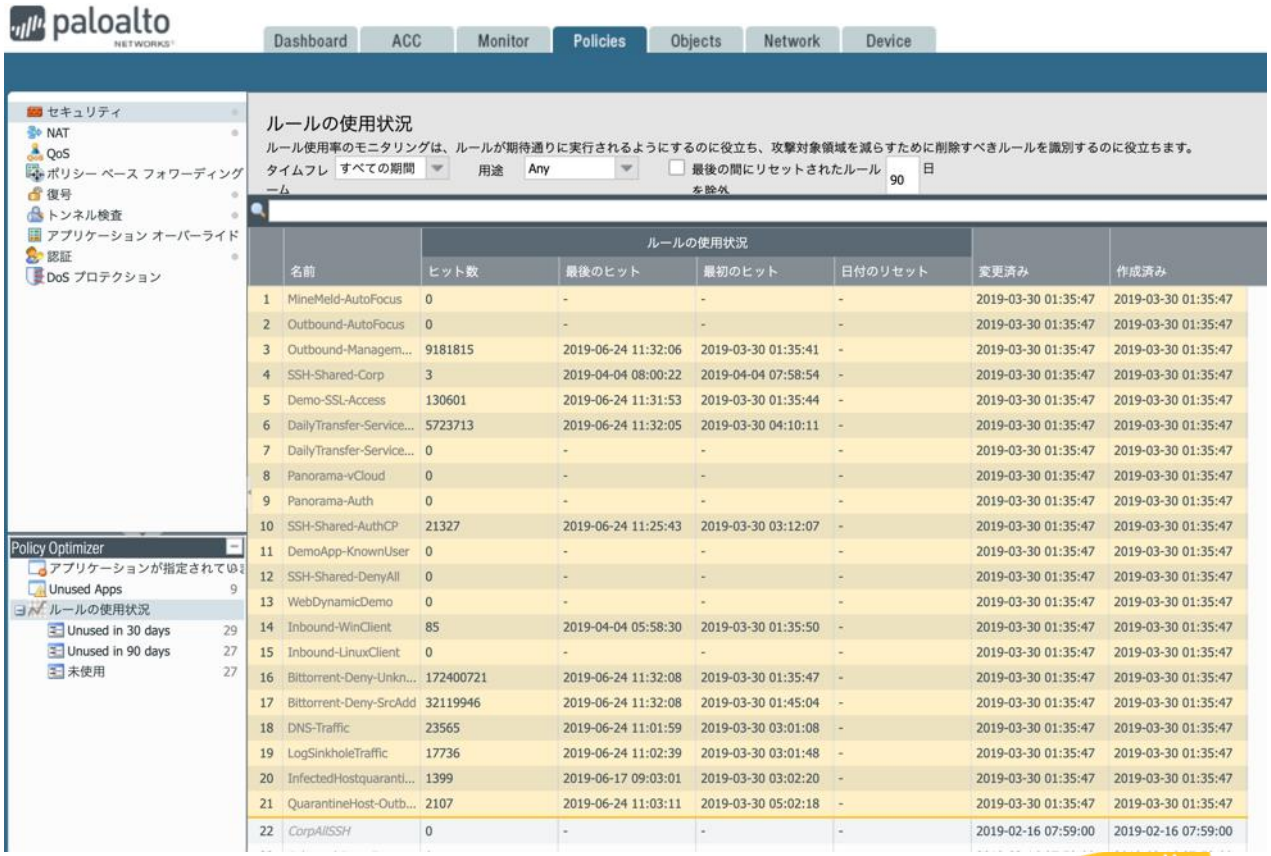
- **既存Policyの要/ 不要を動的に判断（Rule Hit Counter）**
- **既存Policyの最適化（Policy Optimizer）**
- **Policyの事前動作確認（Test Security Policy Match）**

ルール毎のヒットカウンタとタイムスタンプ

- 該当するルールにヒットしたカウントやタイムスタンプをPolicy画面で表示
  - FWリプレース時の既存Policyからの移植後，不要なPolicy（利用していないPolicy）のあぶり出しが可能

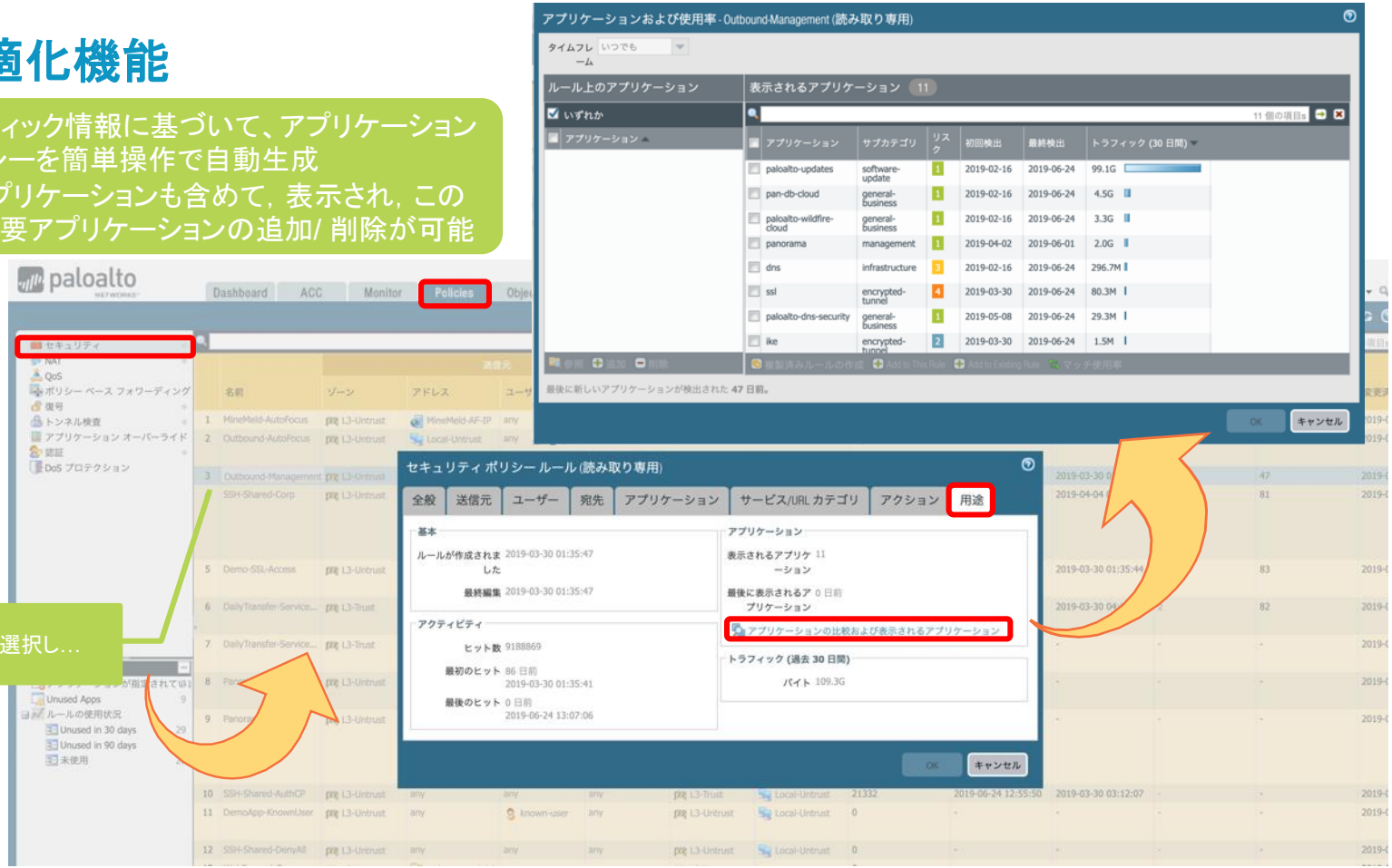
ルール毎のヒットカウンタとタイムスタンプ（続き）

- 前述画面だけでなく，専用画面での確認も可能



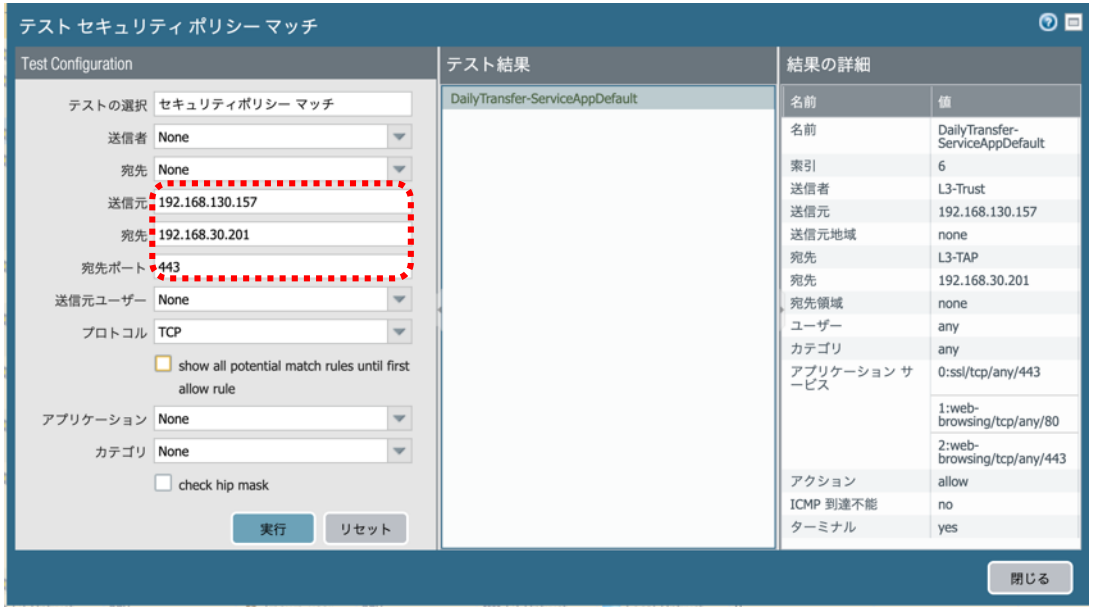
ポリシー最適化機能

- ユーザ環境のトラフィック情報に基づいて、アプリケーションベースの制御ポリシーを簡単操作で自動生成
- 依存関係のあるアプリケーションも含めて，表示され，この一覧を使って要/ 不要アプリケーションの追加/ 削除が可能



セキュリティポリシーの動作確認機能

- 設定したPolicyが適切に動作するかを確認する機能
  - （最低でも）Src. / Dst./ ポート番号を入力することで，ヒットするPolicyが確認可能



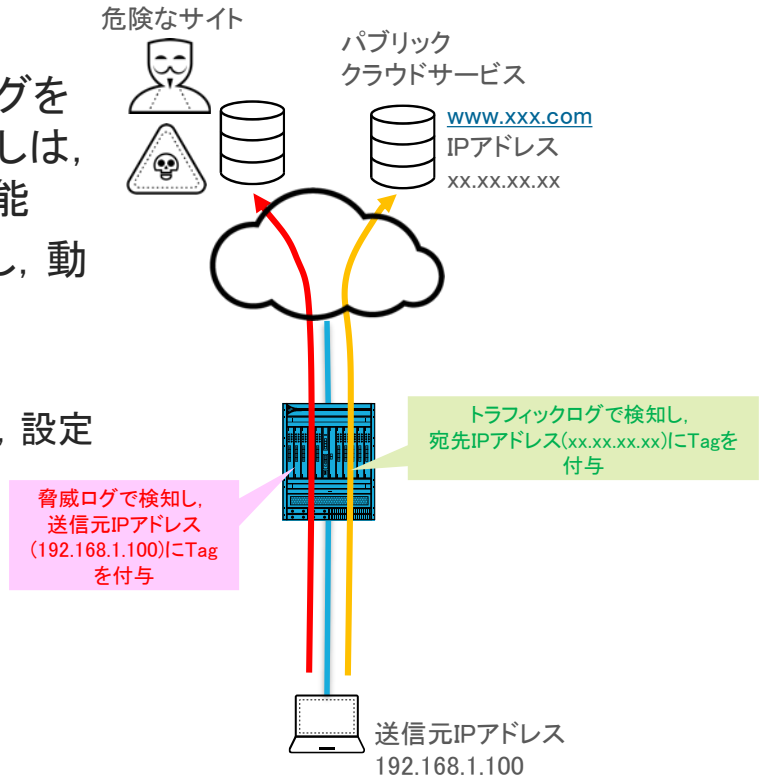
自動化による負荷軽減

- 自動化によるセキュリティは，メリット/ デメリットがある.
  - 運用者の負荷軽減
  - 新たな開発が必要？
- 開発を伴わない，いいとこ取りの自動化セキュリティとは？

- **開発不要の自動制御機能その1（Auto Tag）**
- **開発不要の自動制御機能その2（External Dynamic List（EDL））**

Auto Tag

- Auto Tagとは？
  - トラフィックログ，脅威ログ，URLフィルタログ等のログをトリガーとし，検知した通信の送信元IPアドレスないしは，宛先IPアドレスにタグを自動的に付与/ 削除する機能
  - Tagと連携するダイナミックアドレスグループを利用し，動的にポリシー適用が可能
  - PAN-OS 9.0では…
    - AutoTagで付与されたタグにタイマー機能が追加され，設定した時間が経過すると自動的にタグが削除



Auto Tagによる自動制御の例

1. マルウェアファイルのダウンロード，アンチスパイウェアでC2通信検知など，いずれかの条件に該当する端末を**自動的にインターネットの全遮断**
   - 脅威ログで検知された場合，送信元IPアドレス(=クライアントのIPアドレス）にタグをつける

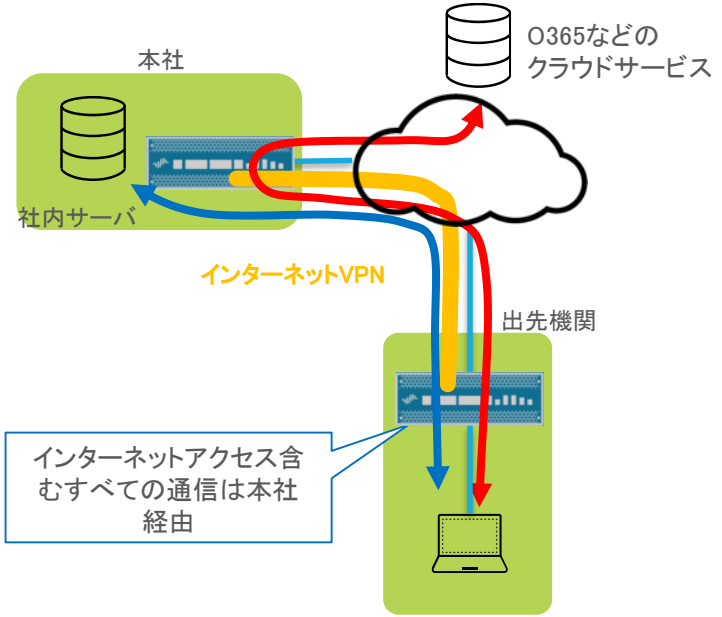
2. Windowsアップデート通信をポリシーベースフォワーディング(PBF)で**自動的に回線制御**（※インターネット回線が複数回線ある場合）
   - App-IDのトラフィックログでms-updateを検知した場合，その送信先IPアドレス(=Windowsアップデートで利用されているサーバのIPアドレス）にタグをつける

3. 端末のOS種別により**適応するポリシを自動で適応**
   - URLフィルタリングログのUser-Agent情報より，送信元IPアドレス(=クライアントIPアドレス）に端末のOSに該当するにタグをつける

AutoTagを利用したアプリケーション単位でのインターネットブレイクアウト

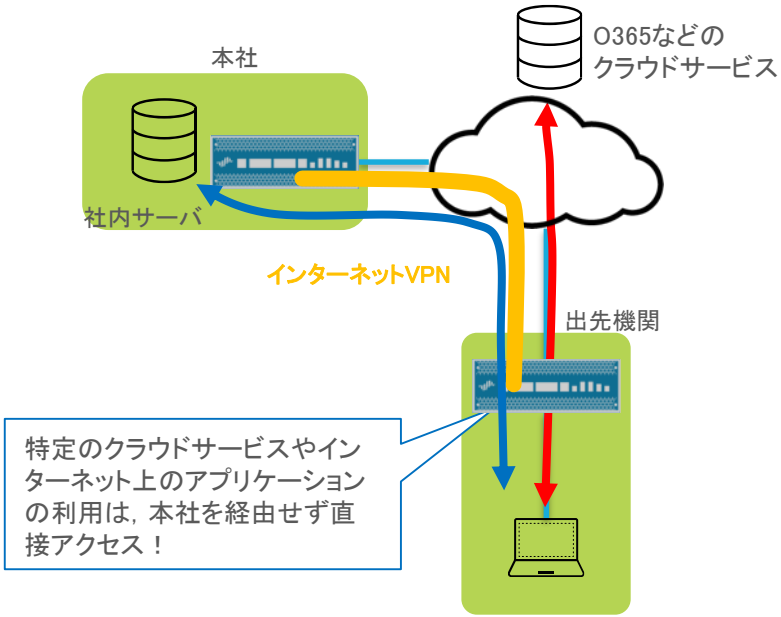
■インターネットVPNの課題

支店からクラウドサービス利用時に，本社を経由するため本社のインターネット回線を圧迫し，レスポンス低下を招く．
解消するには本社の回線増強やインターネットVPN装置のアップグレードが必要



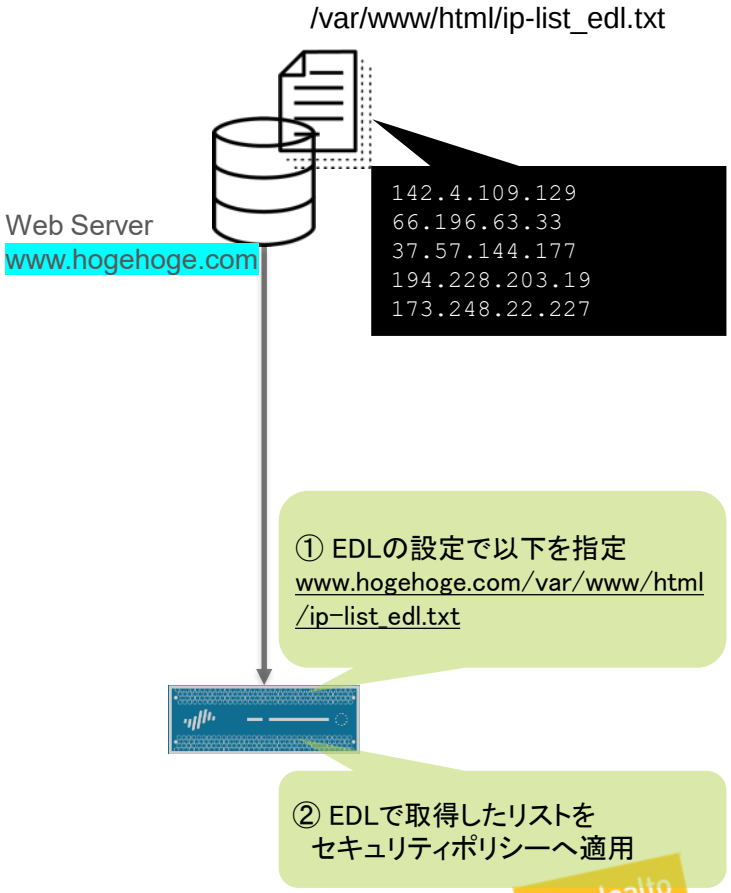
■インターネットブレイクアウトによる解決

特定のクラウドサービスやインターネット上のアプリケーションの利用に関しては，本社を経由せず直接インターネットをアクセス．
（タグが付くまでは本社経由．タグが付いた時点からブレイクアウトし，支店から直接アクセス）



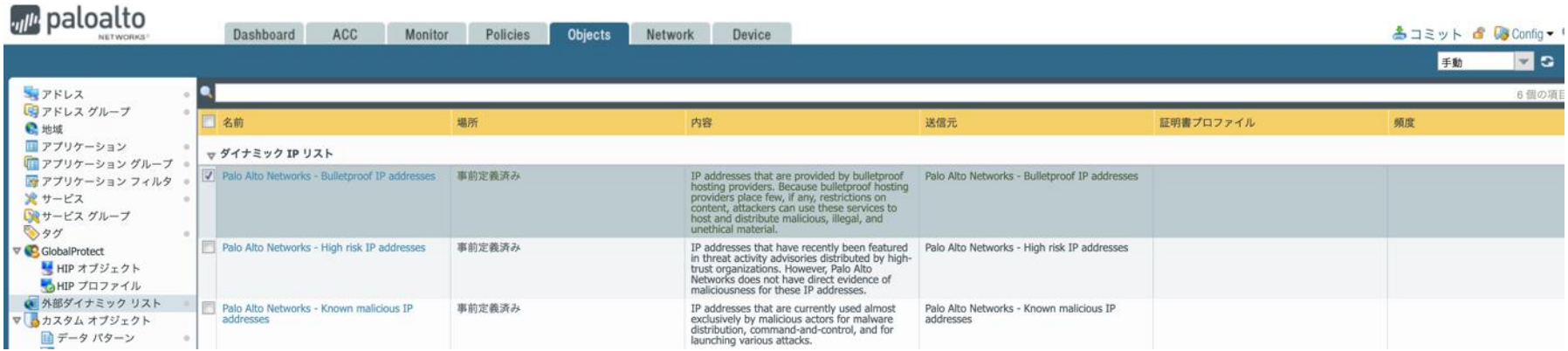
External Dynamic List（EDL）

- ユーザが任意で作成したIP address/ URLs/ Domainsが記述されたテキストファイルをWebサーバ上に格納
- PA Firewallが上記Webサーバに定期的（最低周期5分）にテキストファイルで作成されたリストを参照し，該当するPolicy等へ適用
  - PAでの設定変更およびCommit操作は不要
- EDLで取得したオブジェクトは以下に適用可能
  - Security Policy
  - URLフィルタリングプロファイル
  - アンチスパイウェアプロファイル



External Dynamic List for Bulletproof Hosts

- Bulletproof Hostingと呼ばれる，麻薬売買/ 児童ポルノ/ DoSやボットネットワークの貸し出しなどサイバー攻撃者向けのホスティングサービスの情報を，EDL機能にて提供＆動的に防御可能



高度/ 最新の脅威情報を利用したゼロデイ攻撃対策

- 未知のマルウェア/ ゼロデイ攻撃から守る術は？
  - 未知なものを既知へとかえるサンドボックス
    - ただし，他セキュリティデバイスとの連携が重要
- マルウェアはDomain Generate Algorithm（DGA）を利用し生成することで，対策が困難に…
  - DNSはコマンド＆コントロール（C2）やデータ搾取のためのトンネリング手段として悪用される
- 限定的なカテゴリベースのURLフィルタリング
  - 従来型カテゴリベースだけでなく，多角的に検査をする機構が求められる

- **未知マルウェア/ゼロディ攻撃検知および防御（WildFireサンドボックスサービス）**
- **DNSセキュリティ強化（DNSセキュリティ）**
- **URLフィルタリング（マルチカテゴリ/ リスクベース）**

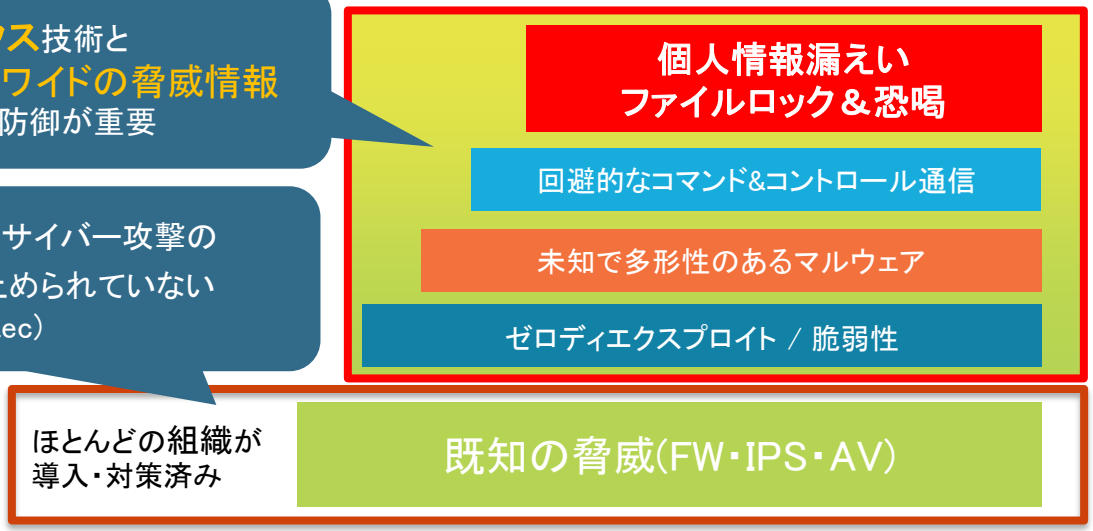
サンドボックスの必要性

昨今のインターネットサイバー攻撃の半分以上は未知の攻撃

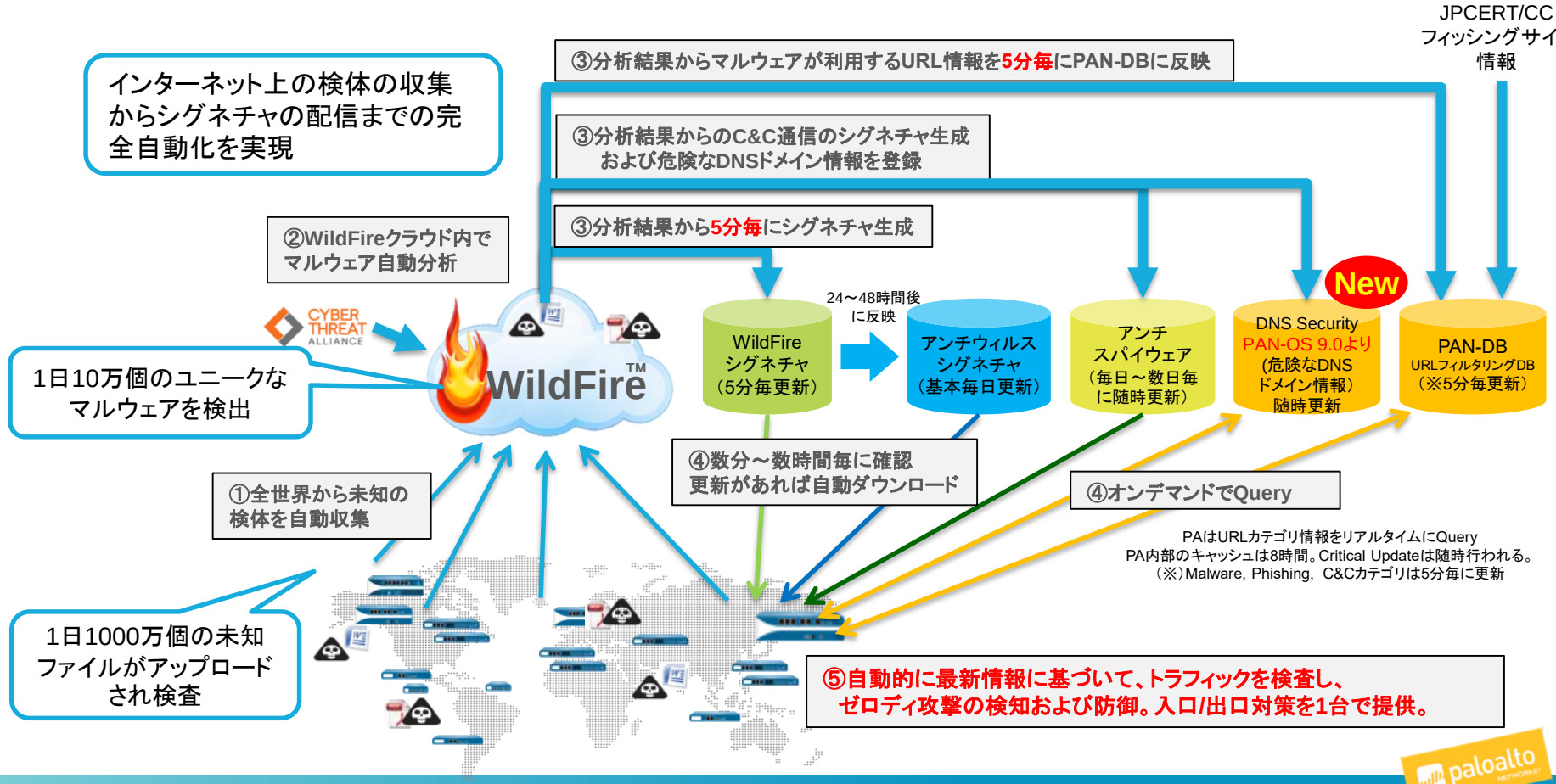
攻撃者は仮想環境で最新のアンチウィルスソフトを使って事前検証

サンドボックス技術と
リアルタイムのワールドワイドの脅威情報
を活用した自動防御が重要

ウイルス対策ソフトはサイバー攻撃の
45%程度しか食い止められていない
（Symantec）



パロアルトネットワークスの優位性 完全自動化された脅威防御



WildFire詳説

動的アンパック

静的解析

既知のエクスプロイト，
マルウェア，亜種を検出

- メモリー分析
- 機械学習
- ファイルの異常
- 悪意のあるパターン
- 既知の悪質なコード

動的解析

実行によりゼロデイ攻撃と
マルウェアを発見

- カスタムハイパーバイザ
- 行動スコアリング
- マルチバージョン分析

WF

ヒューリスティックエンジン
回避したマルウェアを
ベアメタルに誘導

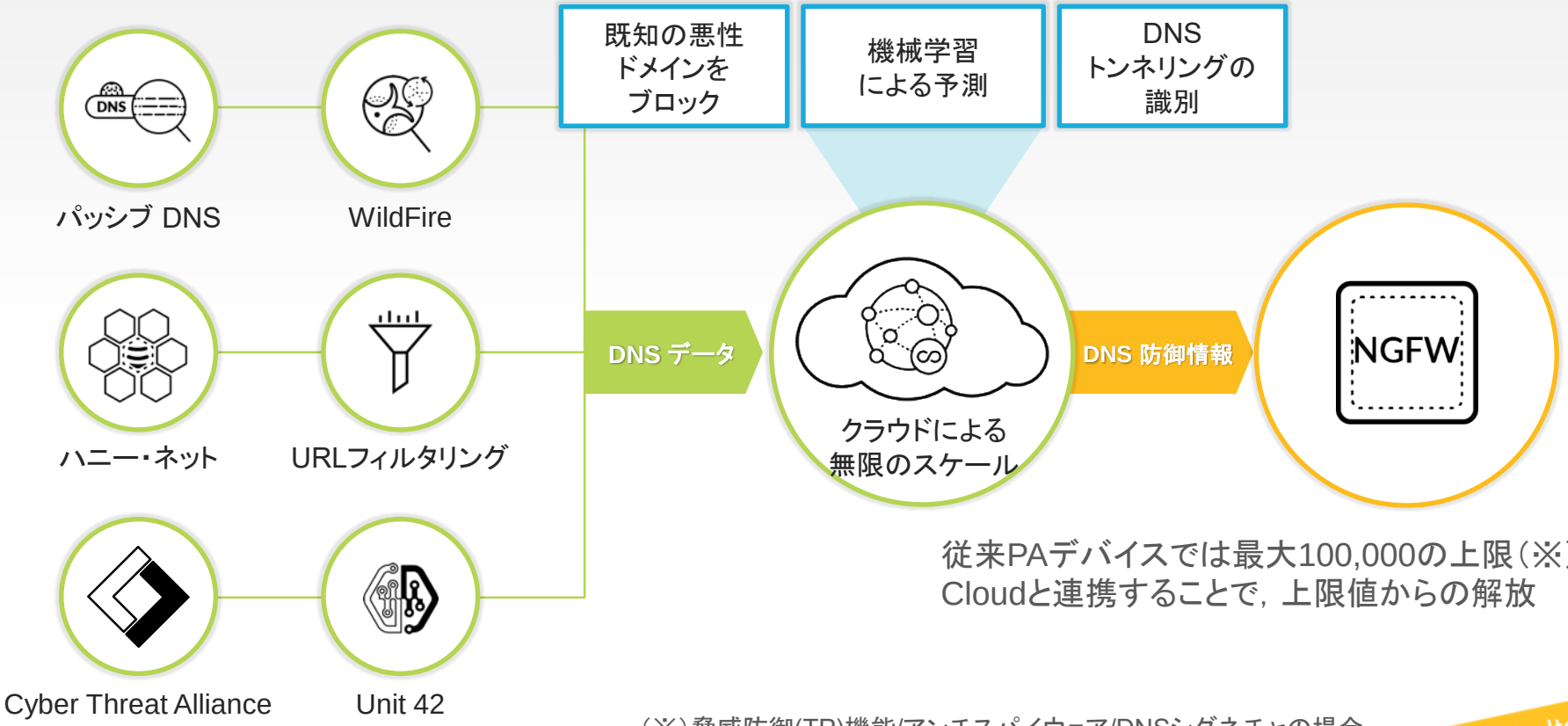
ベアメタル解析

実ハードウェア環境を使用して
VM対応の脅威を特定

- 完全な動的解析
- 実際のハードウェア
- 仮想環境なし
- ハイパーバイザーなし

Early verdict determination → Signature生成

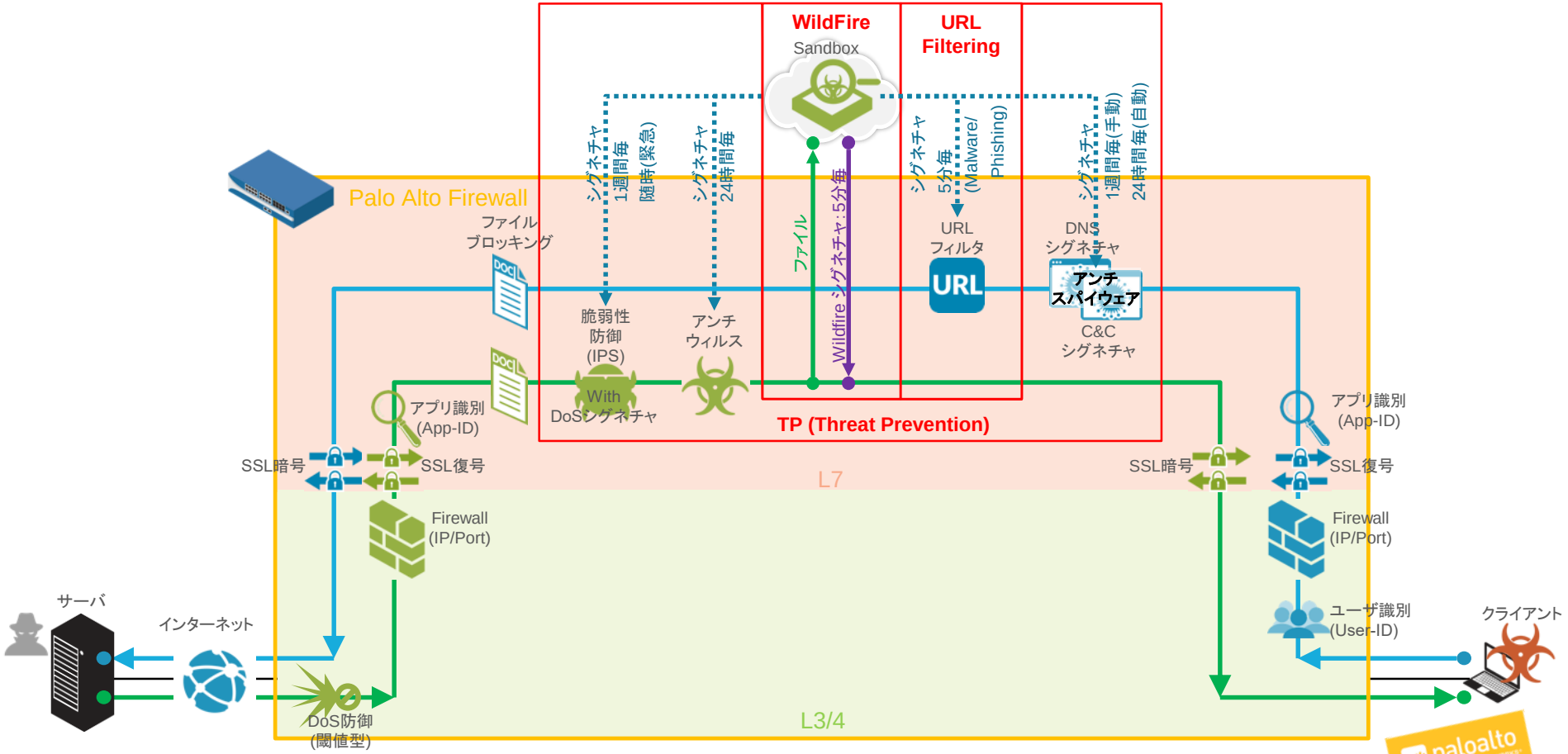
膨大なDNSデータを活用した機械学習によりDNS脅威からの保護を強化



従来PAデバイスでは最大100,000の上限（※）
Cloudと連携することで，上限値からの解放

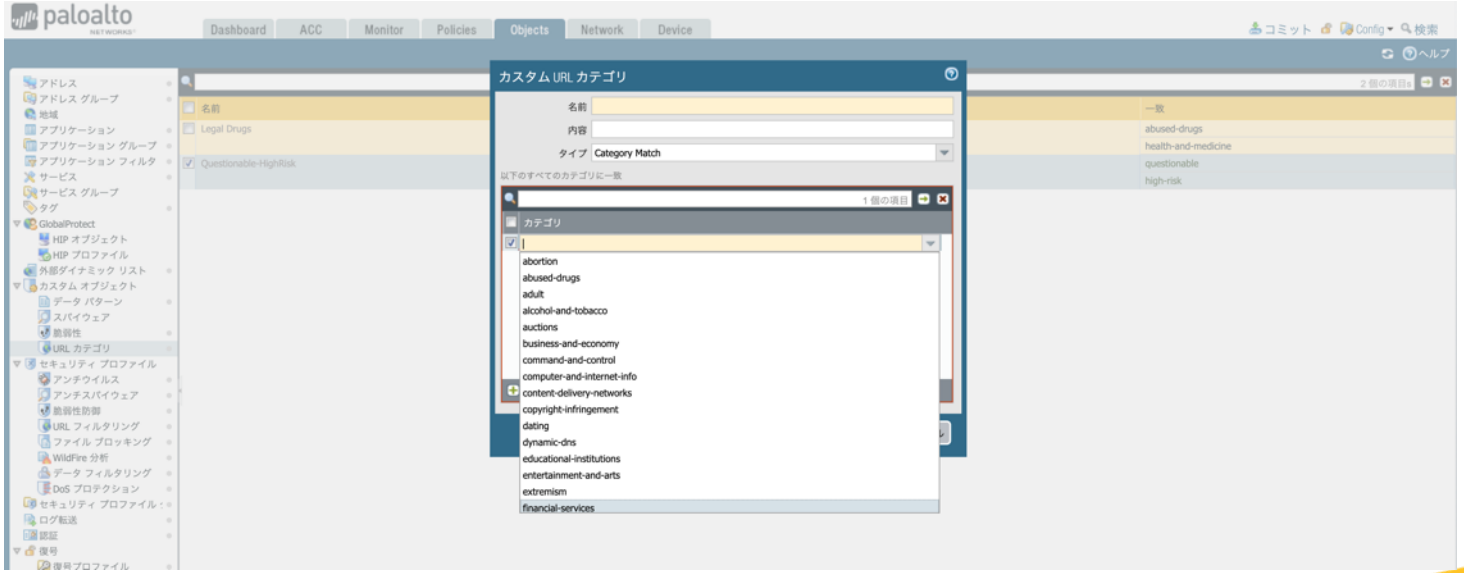
（※）脅威防御(TP)機能/アンチスパイウェア/DNSシグネチャの場合

PAシリーズの機能とサブスクリプション



URLフィルタリング（マルチカテゴリ）

- 従来の定義済みのカテゴリベースでの検査だけでなく，以下のカスタムカテゴリにて検査可能
  - 複数カテゴリをまとめたカテゴリ
  - リスクベース



URLフィルタリング（リスクベース）

カテゴリ	判別方法
High-Risk	以前マルウェア，フィッシングサイトとして立証されたサイト．または，30日以内でC2サイトとして活動をしていたことのあるサイト
	PAN-DBがCategorize完了するまでの未知のドメイン
	Maliciousサイト． 例； 特定のサイト自身がmaliciousでなくても，そのページないしは同じドメインにmaliciousホストが存在する場合　等
	ダークウェブ，違法サイト等にサービスを提供しているISP
	IPだけのサイト
Medium-Risk	すべてのCloudストレージのサイト
	以前マルウェア，フィッシングサイトとして立証されたサイト．または，過去60日でC2サイトとして活動をしていたことのあるサイト
	PAN-DBがCategorize完了するまでの未知のIPアドレス
Low-Risk	上記Riskカテゴリに分類されなかったコンテンツ
Newly-Registered Domains	直近32日以内で新たに登録されたサイト

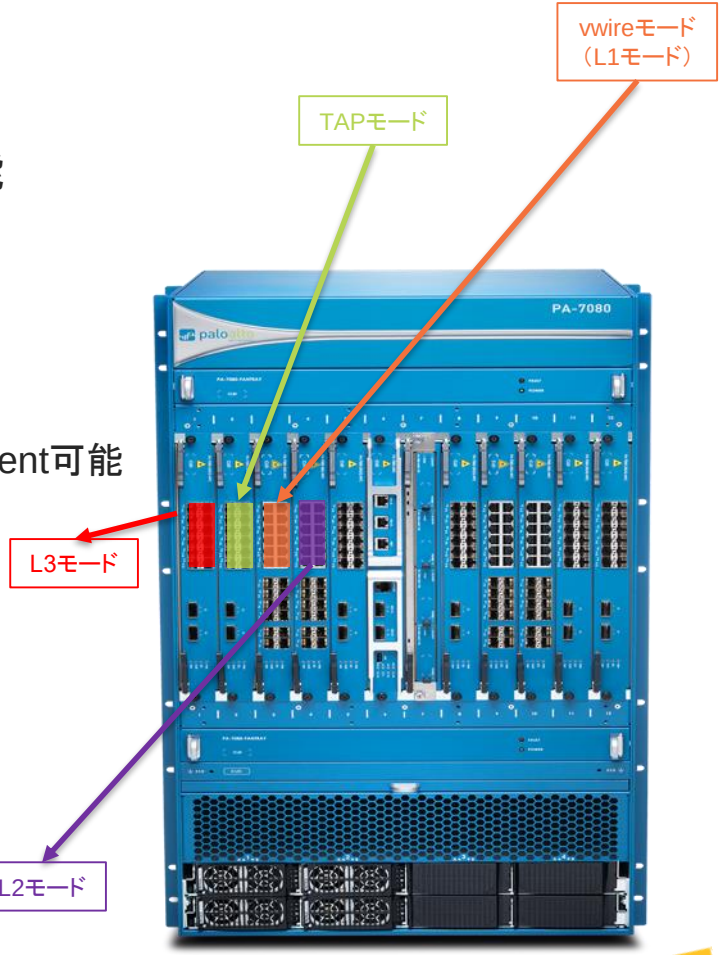
様々な運用方法

- 既存ネットワーク構成/ デザインに影響を与えない
  - 柔軟な接続形態の提供
- 設定ミスによるシステムへの影響回避
- インシデント発生時の見落とし
  - 大量のセキュリティログから日々のインシデントを拾うのは困難

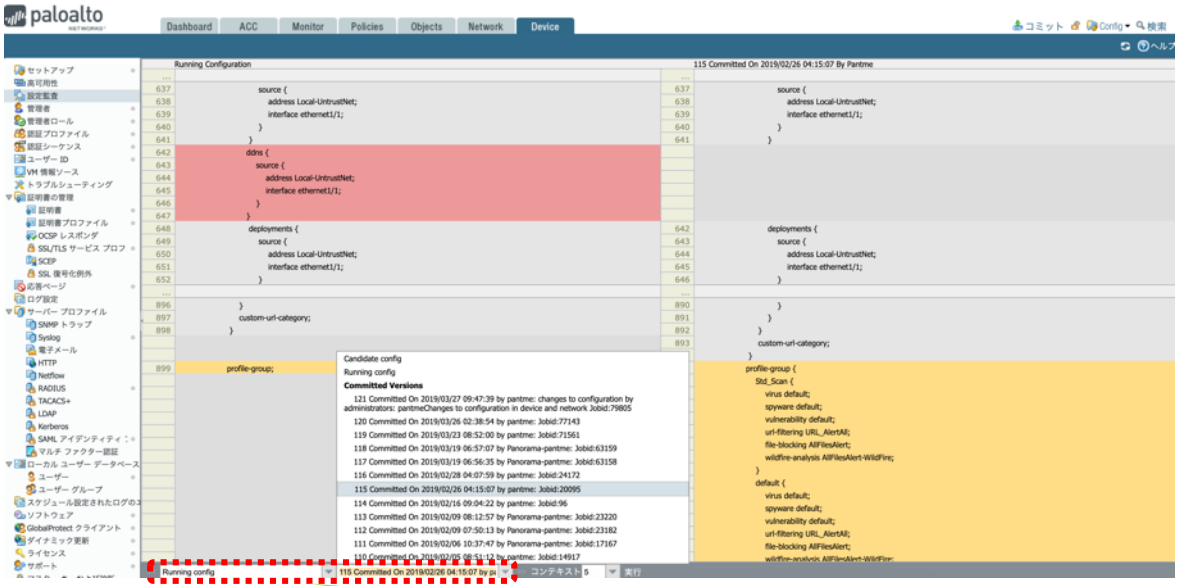
- **既存システム構成への影響を最小限にする（同一筐体での様々な接続形態）**
- **設定ミスによるシステムへの影響回避（Config Commit/ Compare）**
- **重大インシデントを素早く検知（Log Filter機能）**

同一筐体内での各種接続形態

- 下記インタフェースモードは，1筐体にて混在可能
  - TAPモード
    - ミラーリングによるトラフィックのモニタ
    - 既存トポロジへの影響なくDeployment可能
  - Vwireモード（L1モード）
    - 2つのポートをペアとして透過型機器としてDeployment可能
    - Tagged VLAN等のトラフィックも処理可能
  - L2モード
    - Untagged/ Tagged VLAN対応のモード
    - IEEE802．1Q対応
    - NAT/ VPNは利用不可
  - L3モード
    - システムのゲートウェイとして使用可能
    - Tagged VLAN L3サブインタフェースにも対応



Commit/ Compare



指定した世代のConfigのcompareが可能

- 従来の機器
  - 設定と同時に設定内容が反映
    - 万一の設定ミスの場合，即座にミスConfigで動作
- PAシリーズの場合
  - 設定したConfigは，Candidate（候補）Configとなる.
  - 「commit」コマンドを適用することで，Candidate ConfigからRunning Configへ
  - Compare機能を使用することで，過去のConfigとの差分チェックも可能

Log Filter

- 特定の条件のログを転送することで，重要なログの見落としを防ぐ
  - 例えば…
    - MalwareカテゴリのURLフィルタリングログだけをSyslogサーバに転送
    - インシデント発生時は，Criticalログだけをメールにて管理者へ通知