パロアルトネットワークス製品・ソリューション概要と教育委員会向けガイドラインに基づいた提案ポイント

教育情報セキュリティポリシーに関するガイドライン

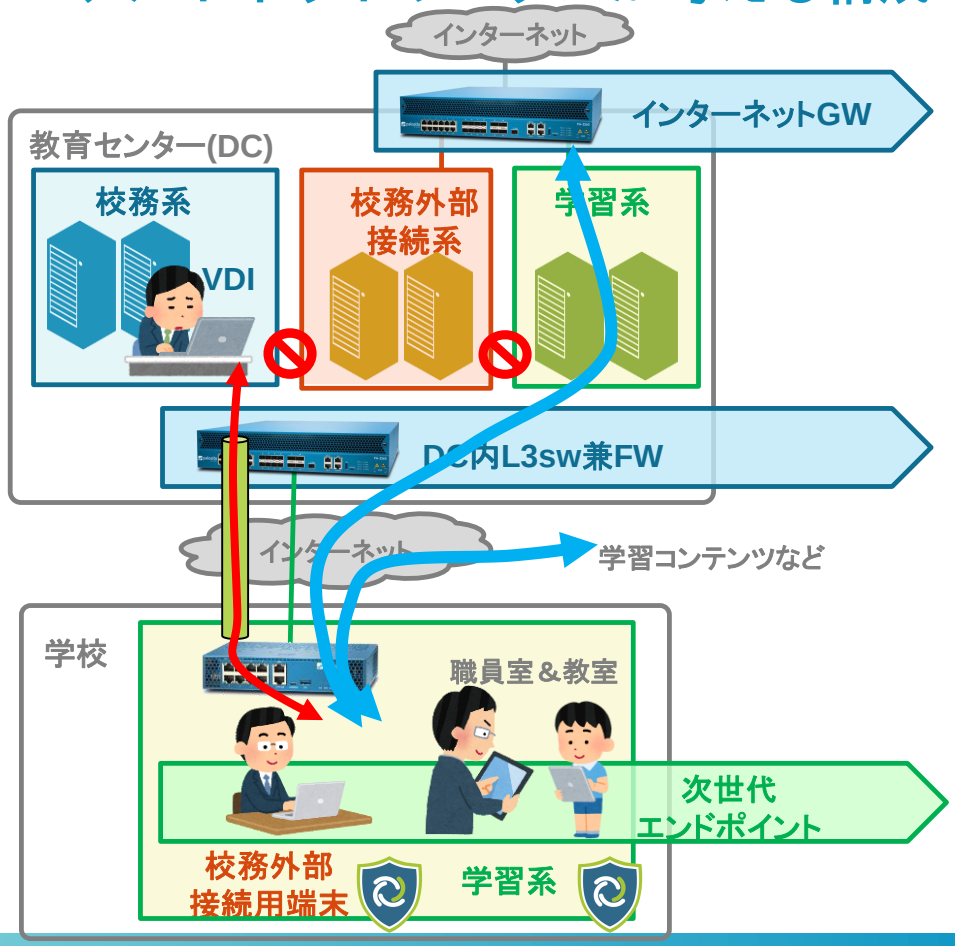
（１１）ネットワークの分離

①教育情報システム管理者は、校務系システム及び学習系システム間の通信経路の物理的又は論理的な分離をするとともに、校務系システム及び校務外部接続系システム間の通信経路を物理的又は論理的に分離し、それぞれで適切な安全管理措置を講じなければならない。

②教育情報システム管理者は、校務系システムと校務外部接続系システム及び学習系システム間で通信する場合には、ウイルス感染のない無害化通信など、適切な措置を図らなければならない。

市町村の強靭化と同様
ネットワークの分離と無害化することを求められている

パロアルトネットワークスが考える構成



【インターネットGW用ファイアウォール】
- 次世代FWが、入口対策および出口対策を1台で実現し、インターネットからの攻撃を防御
- 校務外部接続系、学習系を厳密にアクセス制御し、トラフィックをすべて可視化
- クラウド型サンドボックスと連携し、5分単位で更新されるシグネチャを用いてゼロディマルウェアを防御

【DC内部L3sw兼ファイアウォール】
- 校務系、校務外部接続系の基盤の防御や、学習系サーバーへのアプリケーション可視化
- DCへの不審なアクセスを検知と防御

【次世代エンドポイントセキュリティ/Traps】
- AVソフトウェアの置き換えとして、パターンファイルレスで未知のマルウェア及びランサムウェアなどの感染から端末を防御
- メール無害化せずに、教育情報セキュリティガイドラインの要件を満たすことが可能

なぜ？

教育委員会様ネットワークでの昨今の課題

1. **ネットワーク分離による現場での業務負担増**
   - 先生が職員室と教室の往復が不要に（教室でも校務システムが使えるように）
   - 職員室端末でもインターネットが使えるように
   - メール無害化による現場の手間や負担増

2. **Youtube動画のアクセス制御**
   - Youtube動画は閲覧禁止。でも、特定の教育コンテンツはYoutubeに…

3. **有害コンテンツのアクセス制御**
   - Webプロキシによるフィルタリングの費用負担増
   - インターネットアクセスのボトルネック？
   - Google/ Yahooの検索結果としての有害コンテンツ対策。セーフサーチの導入の検討

4. **SSL暗号通信に対する対応**
   - インターネットではSSL暗号化通信が増加しており、対策が必要

5. **コスト**
   - ガイドラインを満たしつつ、機器を集約しないと不要なコストが…

課題1：教育情報セキュリティガイドラインでの「無害化」対策について

（注７）無害化通信とは、インターネットメールに添付されたファイルの削除やHTMLメールをテキストデータ化することによってテキスト本文のみを校務系システムで閲覧可能とすること（メール無害化）や、仮想デスクトップ等の画面転送プロトコルを用いた技術によりインターネット接続を前提としたシステムからのウイルス感染がないようにすること（通信の無害化）の総称となる。

なお、ファイルの取り込みにおいては、ファイル無害化機器（ソフトウェア、サービス等も含む）の活用が考えられるが、従来のパターンマッチング型のウイルス対策製品だけでなく、ゼロデイ攻撃を対象にしたウイルス対策製品を利用し無害であることを確認した上でファイルを取り込む方法もある。

次世代ファイアウォールでのWildFireおよびエンドポイントでのTrapsを導入することで、専用のメール無害化/ファイル無害化製品を導入しなくとも、ガイドラインの要件を満たせます！

課題1：端末のセキュリティ対策とメール無害化をTrapsで実現

従来型

メール無害化
製品

アンチウィルス
ソフトウェア

＋

シグネチャ更新サーバ
管理サーバなど

VS

パロアルトネットワークスの
ご提案

次世代エンドポイントセキュリティ
Traps

ゼロディマルウエア対策
振る舞い検知
パターンファイルレス
管理コンソールはクラウド
（サーバなど不要）

Trapsで統合し、ガイドラインの要件を満たし、トータルコスト削減および運用負担軽減

次世代エンドポイントセキュリティ Trapsのご紹介

パターンファイルレス

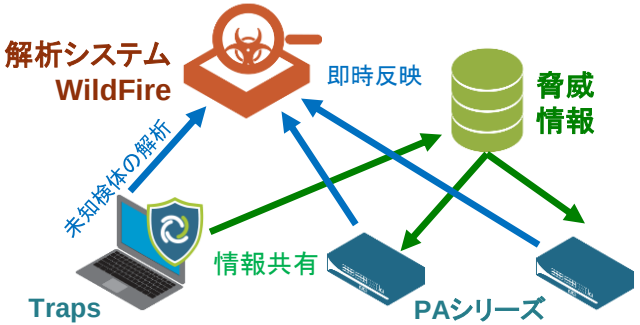
定期的なパターンファイルのダウンロードが不要で運用負担少ない
攻撃テクニックの振る舞いを検知することで未知ウィルスも感染を阻止

最新の脅威インテリジェンスを活用

WildFireと連携した世界規模の最新の脅威情報にて実行の直前にファイルの危険性を判断することで、ゼロディマルウェアも実行を阻止

クラウド型管理コンソール

導入はクライアントPCにエージェントを導入するだけなので、簡単に導入可能
ポリシー設定やイベント検知まですべて管理操作はクラウド上の仮想コンソールにて実行



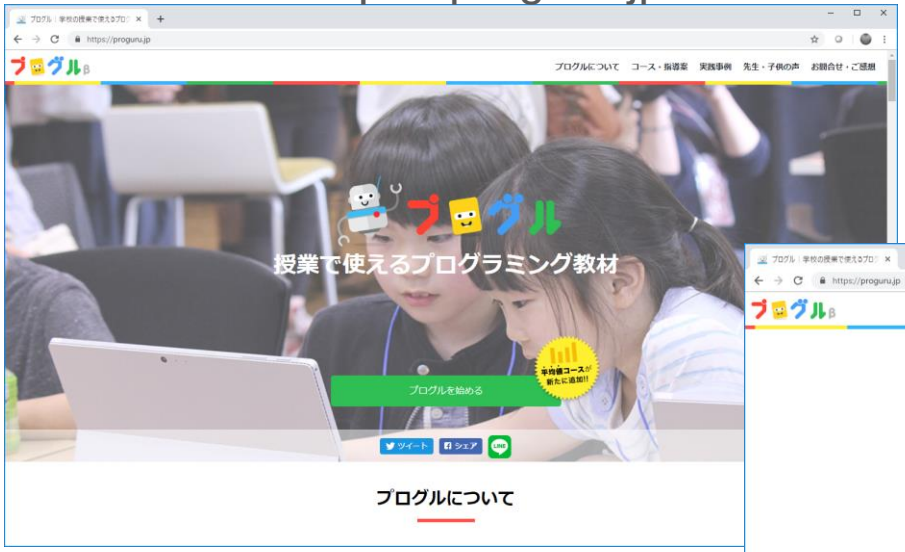
世界中で最初の1台にならない限り、
情報が既に登録されている

従来型ウイルス対策製品とTrapsの違い

項目	次世代型 Traps	従来型 ウイルス対策	従来型 ウイルス対策の課題
既知ウイルスの検知	○	△	一部の定義ファイルのみ配信 解析自動化ができず、対応が遅い
亜種（未知ウイルス）	○	×	最新バージョンでは 亜種に対応できるものあり
マクロ・ファイルレス攻撃	○	×	対応が難しい
パッチ未適用状態の保護	○	×	エクスプロイト 対策機能がない
解析結果の確認 感染後の検知	○	×	検出時にログが表示されるのみ
PCのパフォーマンス負荷	○	×	定義ファイルをメモリ展開し、 ファイルスキャンで負荷上昇

課題２：特定のYoutube動画だけを視聴させたい

例）プログル　https://proguru.jp/



埋め込まれた
Youtube動画

App-IDにカスタムアプリケーションとして
登録することで容易に制御可能です！

課題３：有害コンテンツへのアクセス防止について

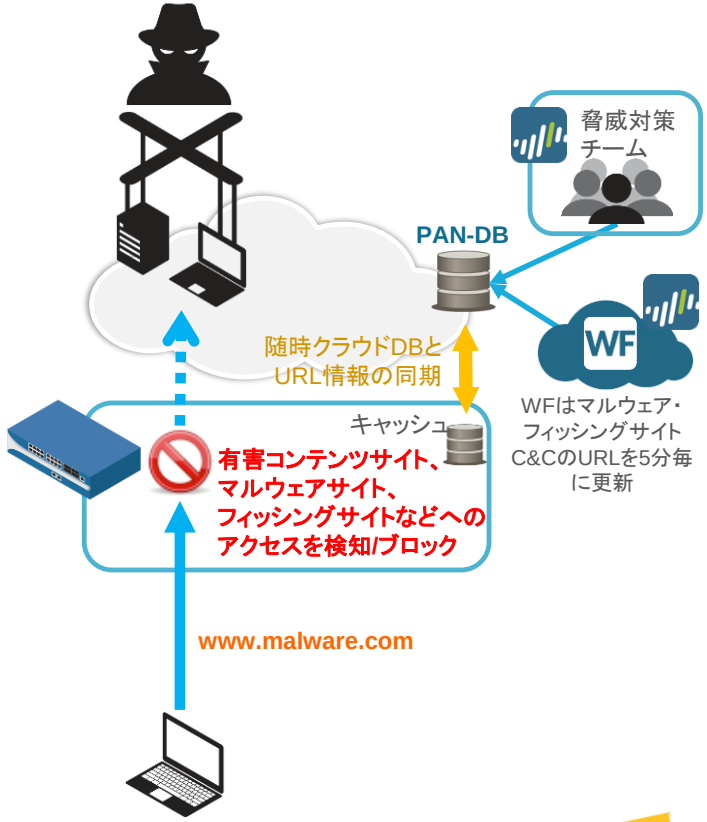
- 一般的にはWebプロキシによる有害コンテンツをフィルタ
  - 導入目的/ メリット
    - 有害コンテンツのWebサイトのフィルタ
    - HTTP通信に対するコンテンツキャッシュ効果によるレスポンス向上とインターネット回線の負荷軽減
    - Webアクセスに対するアクセスログ
  - デメリット
    - セッション数の増加によるスループットの低下
    - 端末にプロキシ設定が必要となる
    - プロキシ対応していないアプリケーションは使えない
    - HTTPS通信に対してキャッシュ効果はない
    - 維持・運用費用（クライアント数でのライセンス課金等）

PAシリーズによる有害コンテンツのフィルタ

- パロアルトネットワークスの次世代ファイアウォールの標準機能として下記の機能を提供します。(Webプロキシ/キャッシュ機能は提供しておりません)
  1. 通過するHTTP/HTTPS通信のアクセスログアクセスログのSyslogサーバへのログ転送
  2. URLベースでのアクセス制御(ホワイトリスト/ブラックリスト)
     ※URLの指定にはワイルドカードによる指定が可能
  3. アクセス制御には、許可、禁止、警告画面、パスワード付き警告画面が利用可能です。
  4. SSL復号機能(脅威防御するためには別途脅威防御サブスクリプションが必要です)

- URLフィルタリングサブスクリプション(有償)にて、クラウド上のデータベースPAN-DBが利用可能となり、**有害コンテンツアクセス防止**および**サイバー攻撃防御/出口対策**が可能です
  1. カテゴリベースでのトラフィックの可視化とアクセス制御
  2. 危険なWebサイトへのアクセス禁止

  ※セキュリティ脅威に関連するマルウェア、フィッシング、C&Cの3つのカテゴリ情報はWildFireサンドボックスの分析結果に基づき5分間隔で更新されます。これら3つのカテゴリのWebサイトへのアクセスは禁止を推奨いたします。



機能比較：Webプロキシ vs. PAシリーズ

	Webプロキシ	PAシリーズ URLフィルタリング機能
キャッシュ機能	○ 昨今のインターネットではSSL通信が増加し、 実質キャッシュ効果がなくなりつつある。	×
Webアクセスログ	○	○
Webアクセス制御 （ホワイトリスト/ブラックリスト）	○	○
Webアクセス制御 （カテゴリベース）	△（製品に依存）	○
Webアプリ識別	△（製品に依存）	○
アンチウィルス	△（製品に依存）	○
C&C検知/脅威検知	△（製品に依存）	○
SSL復号	△（製品に依存）	○
ログ相関分析	×	○
http/https以外の通信の監視と制御	×	○

セーフサーチ機能との連携

■設定方法

■警告画面

「セーフサーチを適応」を有効化している場合、GoogleやYahooでセーフサーチではない検索を実行すると、警告を表示し、セーフサーチ設定を促します。警告画面表示後、セーフサーチを設定する画面へ誘導するリンクも表示されます。

尚、この機能を利用するには、GoogleおよびYahooへのアクセスにSSL復号機能が必須です。

課題4：SSL暗号通信の対応

想定条件		大規模 120校		中規模 80校	小規模 40校
同時利用PC台数 （120台/校を想定）		14,400台		9,600台	4,800台
想定される最大セッション数 （50セッション/台を想定）		720,000		480,000	240,000
インターネット回線速度 (想定）		～4G	～2G	～1G	～1G
推奨機種		PA-5220	PA-3260	PA-3250	PA-3220
製品仕様	最大同時セッション	4,000,000	3,000,000	2,000,000	1,000,000
	SSL復号最大同時セッション	400,000	300,000	200,000	100,000
	脅威スループット （APP-ID+TP+URL+WF）	9Gbps	4.7Gbps	3Gbps	2.2Gbps
本体 (HA構成)		PAN-PA-5220-AC*2台	PAN-PA-3260*2台	PAN-PA-3250*2台	PAN-PA-3220*2台
サブスクリプション HA構成 5年一括契約	AV/AS/IPS	PAN-PA-5220-TP-5YR-HA2*2個	PAN-PA-3260-TP-5YR-HA2*2個	PAN-PA-3250-TP-5YR-HA2*2個	PAN-PA-3220-TP-5YR-HA2*2個
	URLフィルタリング	PAN-PA-5220-URL-5YR-HA2*2個	PAN-PA-3260-URL-5YR-HA2*2個	PAN-PA-3250-URL-5YR-HA2*2個	PAN-PA-3220-URL-5YR-HA2*2個
	WildFire	PAN-PA-5220-WF-5YR-HA2*2個	PAN-PA-3260-WF-5YR-HA2*2個	PAN-PA-3250-WF-5YR-HA2*2個	PAN-PA-3220-WF-5YR-HA2*2個
	DNS Security(※)	PAN-PA-5220-DNS-5YR-HA2*2個	PAN-PA-3260-DNS-5YR-HA2*2個	PAN-PA-3250-DNS-5YR-HA2*2個	PAN-PA-3220-DNS-5YR-HA2*2個
アクセサリー		PAN-PA-5200-RACK4*2個	PAN-PA-2RU-RACK4*2個		

基本的にSSL復号のスループットおよび最大同時セッション数のボトルネックより推奨モデルを選定。
※DNS SecurityサブスクリプションはPAN-OS 9.0以降でご利用いただけます。

課題5 ：コスト

■機器費用
- コアL3スイッチ装置
- ファイアウォール装置
- アンチウィルス製品
- IDS/IPS装置
- Webプロキシ(URLフィルタリング、ログ取得)
- VPN装置
- サンドボックス装置

＋

■各製品の導入費用、設計費用

■各製品の保守費用

＋

■多数の製品のオペレーションおよびログ確認
運用負担 大

VS

パロアルトネットワークス
次世代ファイアウォール

■機器費用
■導入、設計費用
■保守費用
■管理、監視が容易

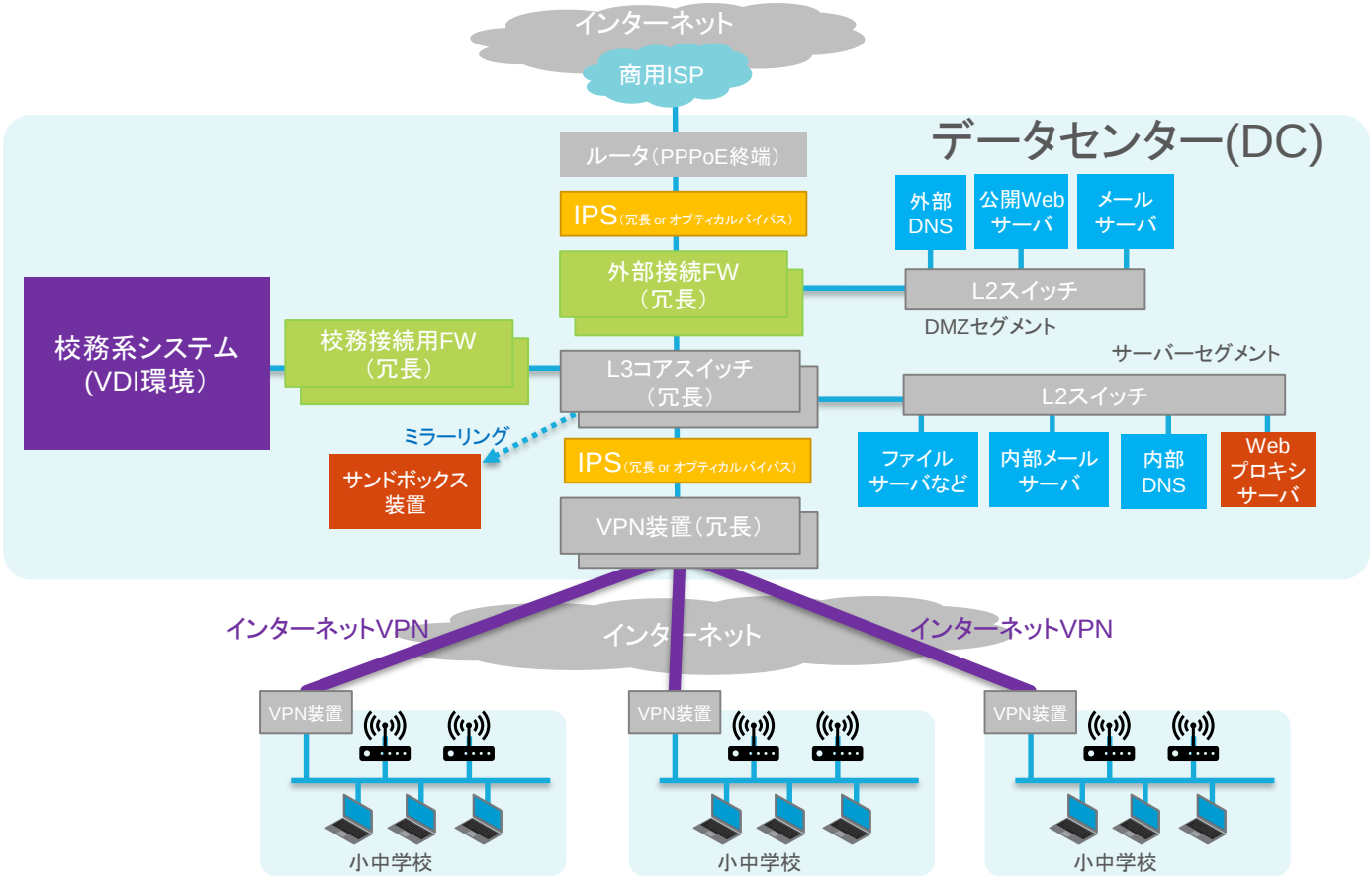
＋

ネットワークのセキュリティ強化

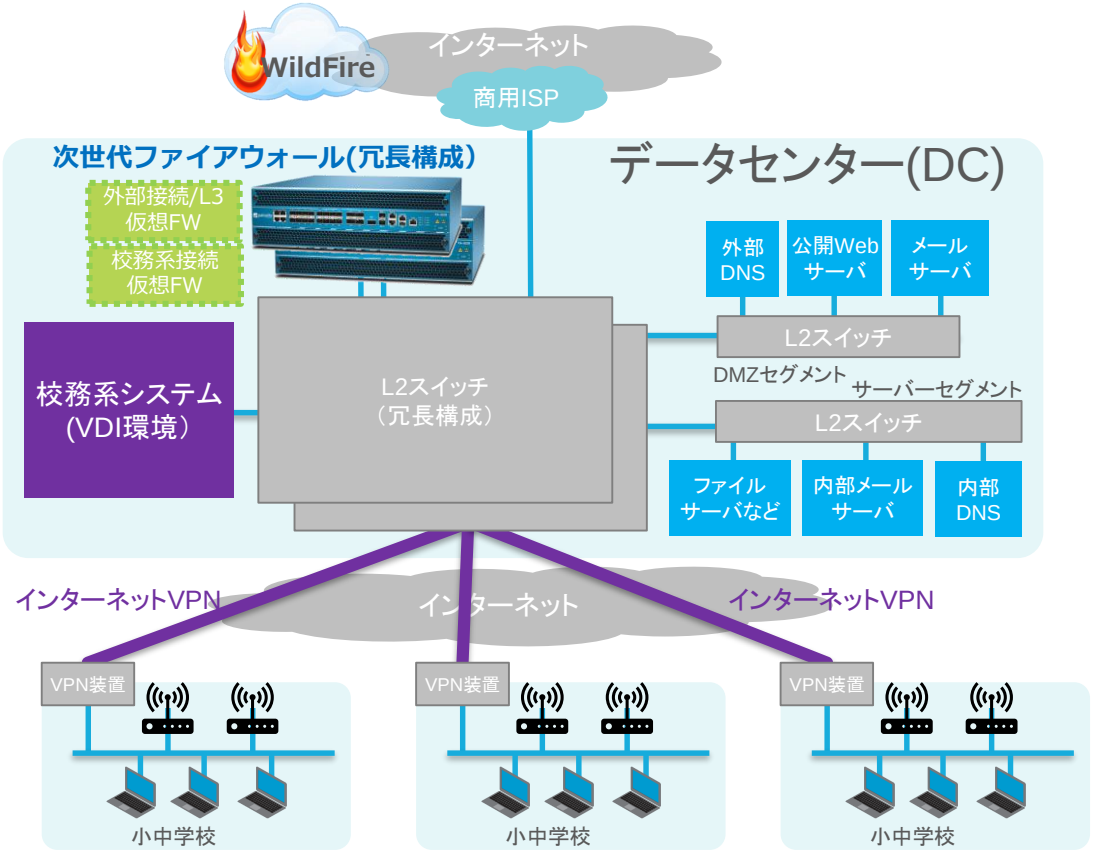
パロアルトネットワークス次世代ファイアウォール優位性

- 豊富な次世代ファイアウォール機能
  - アプリケーション識別(App-ID)、ユーザ識別(User-ID)、脅威防御(IPS)、アンチウィルス、アンチスパイウェア、WildFireサンドボックス連携、URLフィルタリング、ファイルブロッキング、SSL復号、VPN機能などを1台で提供可能
- 多くの機能を利用しても安定した動作
  - 多くの他社製品ではPAシリーズと同等の次世代ファイアウォール機能を有しているが、実際に利用すると高負荷になり劇的なスループット低下、さらに動作が不安定になるトラブルを起こすケースが多く、サポートしている機能が十分に利用できない
    （なので、従来セキュリティ機能単位で製品を分けざるを得なかった）
  - パロアルトネットワークスの場合には、様々な機能を利用しても動作は安定しており、また、ポリシー変更やシグネチャ更新によるユーザトラフィックへの影響なし。そのため運用作業も安心して容易に行えます。
- 世界最速の検知および防御能力
  - WildFireによる検体収集能力の高さ、およびサンドボックス解析の結果に基づき出口対策及び入口対策のためのシグネチャ生成を5分単位で実行することで、最新の攻撃の検知および防御や感染後の被害拡大防止可能
- 使いやすいGUIとレポート機能
  - 統一された画面構成と操作性の高いGUI管理環境を提供
  - 各種ログや情報を可視化することで直感的に把握でき、さらに詳細ログも簡単な操作で検索が可能

DCでの従来の典型的なインターネット接続境界面のセキュリティ構成



パロアルトネットワークス次世代ファイアウォールによる構成案



次世代ファイアウォールにて下記の機能を提供

- ルータ機能（PPPoE終端/OSPF/BGP）
- L3コアスイッチ機能（L3機能を集約）
- ファイアウォール（仮想ファイアウォール）
- トラフィック可視化とアプリケーション制御
- 脅威防御（IPS/アンチウィルス/アンチスパイウェア）
- URLフィルタリング（有害コンテンツフィルタ）
- URLフィルタリング（脅威防御/出口対策）
- WildFireサンドボックス連携によるゼロディ攻撃検知/防御
- IPsecVPN終端
- SSL復号機能

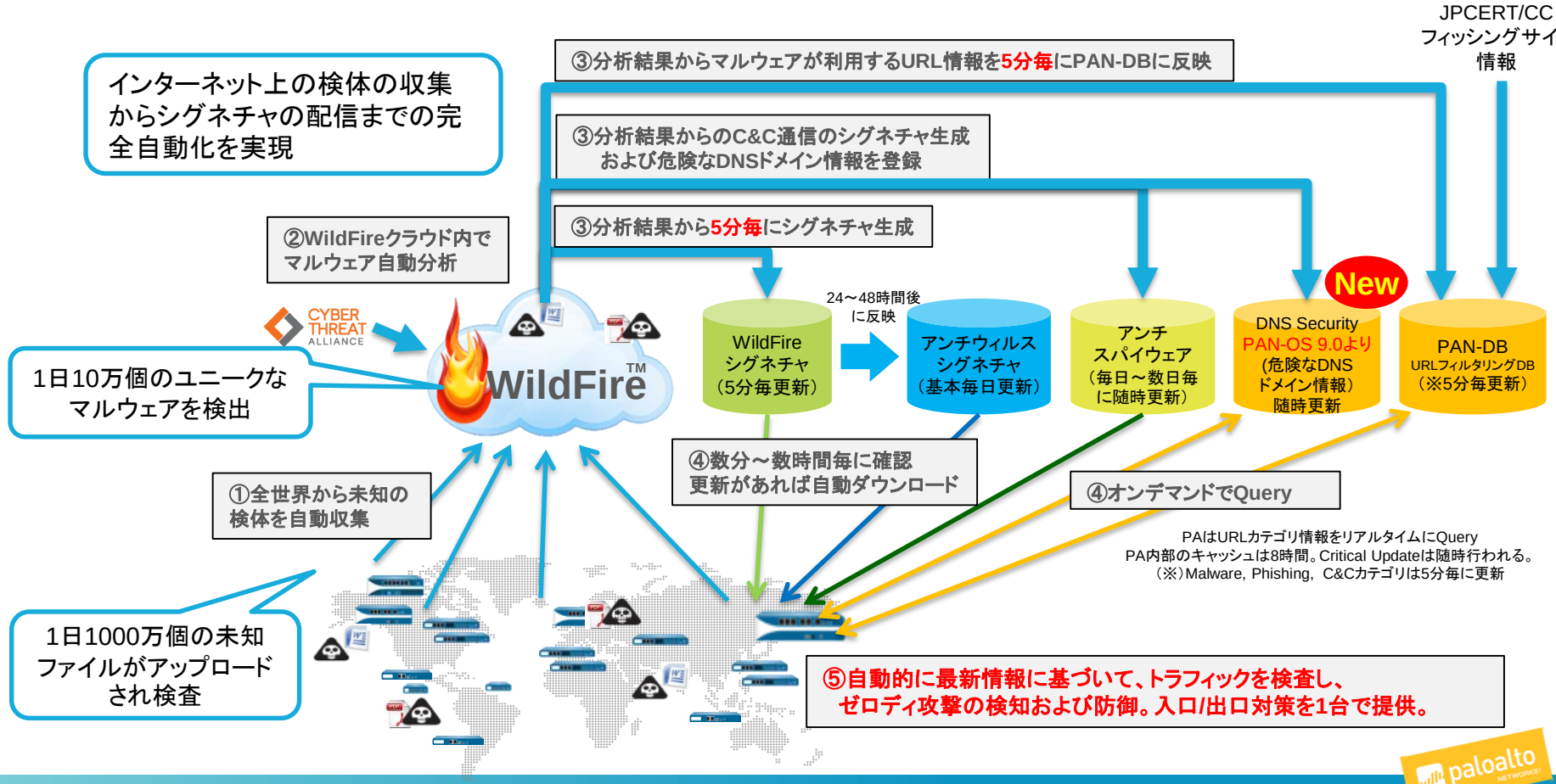
ハイアベイラビリティにて信頼性の高い冗長構成を提供

- 基幹装置としての高い信頼性と、安定したステートフルフェイルオーバー機能
- バージョンアップ時にもセッション情報を引き継ぐことで、ネットワーク無停止で作業可能

機器を集約することによるメリット

- 冗長構成も含めて、設計および構築がシンプル
- 運用管理面においても装置数が少ないことで負担軽減
- 通信不具合時の切り分け工数削減

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



教育情報セキュリティ対策推進での必須品

完全な可視化・コンテンツ制御・SSL複合化機能など

PA-5220/5250/5260
県教育委員会様、DC・SP事業者様向け、高負荷NW集約用

PA-3220/3250/3260
県市教育委員会様
DC・学校内GW/LAN向け

PA-820/850
県市教育委員会様
DC・学校内GW/LAN向け

PA-220
県市町村教育委員会様
学校内GW/LAN向け

端末感染防止

校務・学務端末向け
未知の攻撃対策用エンドポイントセキュリティ製品。
Ver.5.0よりクラウド型管理コンソールにも対応。

Traps
Advanced Endpoint Protection

おわり