

[ASPコード : A801240]

LGWAN-ASPサンドボックスサービス (標的型攻撃対策) 概要

2018年3月
公共営業本部
asp@paloaltonetworks.com

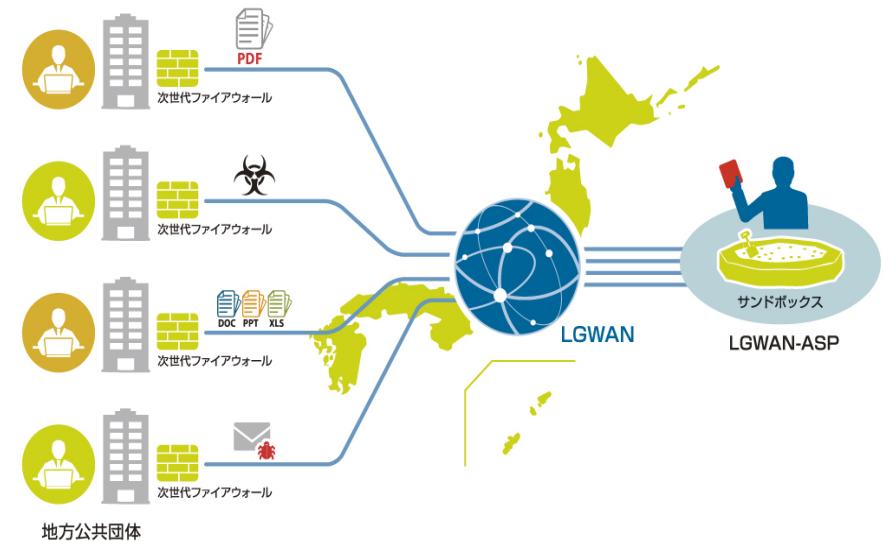


はじめに

- 弊社では、地方公共団体を相互に接続する「総合行政ネットワーク(LGWAN)」へ接続する団体を標的型攻撃などのサイバー攻撃から保護する脅威分析クラウドサービス「ASP型サンドボックスサービス(標的型攻撃対策)」の提供を開始しました。
- 2016年から行政手続き上の利用が開始された「社会保障・税番号制度(マイナンバー制度)」の運用におけるセキュリティ対策に対応しており、インターネットに接続されていないLGWAN上で利用できる国内初の脅威分析クラウド型のサンドボックスサービスです。

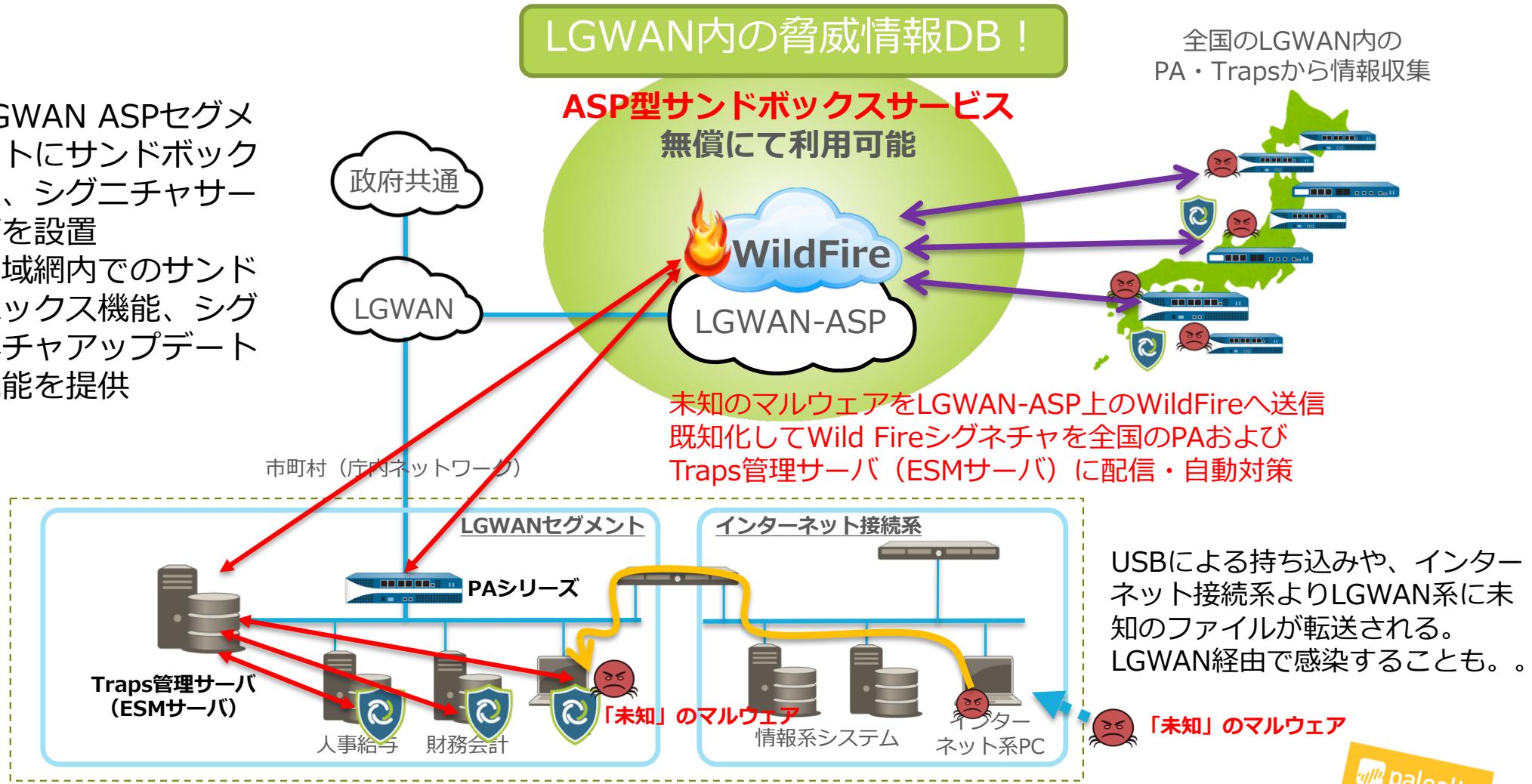
サービス詳細

- WildFireサンドボックスサービス
 - 各地方公共団体にて信頼性のない発信元等から受信するファイルをLGWAN ASP上のWildFireサンドボックス環境にて検査し、ファイルの健全性を確認します。マルウェアと判定された場合は、迅速にシグネチャを自動生成し、ご利用のPAデバイスへ配信します。また、この脅威データベースはTrapsでも利用することができます。
- シグネチャ提供サービス
 - LGWAN-ASP内に設置したシグネチャ提供サーバより以下のシグネチャを提供します。（週次更新）
 - アンチウィルスシグネチャ
 - アプリケーション、脅威シグネチャ



サービス提供イメージ

- LGWAN ASPセグメントにサンドボックス、シグニチャサーバを設置
- 閉域網内でのサンドボックス機能、シグネチャアップデート機能を提供



ご提供条件

- 本サービスのご利用にはお申し込みが必要です
- 対象製品:
 - PA-220/PA-500/PA-800/PA-3000/PA-3200/PA-5000/PA5200/PA-7000シリーズ
PAN-OS 6.1.20以降、およびPAN-OS7.1以降
 - Traps4.1以降
- PAサブスクリプション:
 - Threat Prevention(必須) WildFire(必須)、URL Filtering (推奨)

※ 各製品（ハードウェアおよびソフトウェア）がEoLを迎えた場合、LGWAN-ASPサンドボックスサービスへの接続はサポートされません。詳細は以下を参照してください。

<https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-summary>
<https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates>

PAシリーズ・Trapsの動作環境

- 動作OS: PANOS 6.1.20以上 (7.1以上を推奨)
Traps4.1以上 (Traps動作OS詳細は次ページを参照)
- サブスクリプション: TP(必須)、WF(必須)、URL F(推奨)
- 検査プラットフォーム: Windows 7(64bit)
- 検査対象ファイル:
 - Windows実行形式ファイル(dll, exe)
 - Microsoft Officeファイル(ppt/pptx, doc/docx, xls/xlsx, rtf)
 - Adobe PDFファイル (pdf)
 - Java (jar, class)
- サンドボックスレポートの参照には、LGWAN ASPセグメントと通信可能なPAに対して、Webブラウザアクセスが必要です
- シグネチャダウンロードには、LGWAN ASPセグメントと通信可能なPC等からのダウンロードが必要です

Traps エージェント動作OS詳細

※ 赤字はTraps5.0にて対応

ワークステーション(Windows/Mac)

- Windows XP (32ビット版, SP3以降)
- Windows Vista (32/64ビット版, SP1以降)
- Windows 7 (32/64ビット版, Homeエディションを除く)
- Windows Embedded 7 (Standard/POSReady)
- Windows 8 (32/64ビット版)
- Windows 8.1 (32/64ビット版)
- Windows Embedded 8.1 Pro
- Windows 10 Pro (32/64ビット版) (CB, CBB)
- Windows 10 Enterprise (CB, CBB, LTSB)
- **Windows 10 Fall Creators Update 1709**
- Mac OS 10.10, 10.11, 10.12, **10.13**
- Windows Server 2003 (32ビット版, SP2以降)
- Windows Server 2003 R2 (32ビット版, SP2以降)
- Windows Server 2012/2012 R2 Server Core
- Windows Server 2008 (32/64ビット版)
- Windows Server 2008 R2 (32-bit, 64-bit)
- Windows Server 2012 (全てのエディション)
- Windows Server 2012 R2 (全てのエディション)
- Windows Server 2016 Standard

★最新のシステム要件は下記を参照してください。

<https://www.paloaltonetworks.com/documentation/global/compatibility-matrix/traps/where-can-i-install-the-traps-agent>

ワークステーション(Linux)

- **CentOS 6, 7**
- **Red Hat Enterprise Linux 6, 7**
- **SUSE for Enterprise 12.1, 12.2**
- **Ubuntu Server 12, 14, 16**

仮想環境OS (最小バージョン)

- VMware Horizon View RDS 7.1/Horizon View VDI 7.1
- Citrix PVS 7.13/XenDesktop RDS 7.13/XenDesktop VDI 7.13
- Microsoft Server 2008 R2 RDS/Server 2012 R2 RDS/Server 2016 RDS

仮想アプリケーション

- Citrix XenApp 7.13
- VMware AppVolumes 2.12 / ThinApp 5.2.2

必要ハードウェア

- CPU : Intel Pentium 4以降(SSE2命令サポート)
AMD Opteron/Athlon 64以降 (SSE2命令サポート)
- メモリ : 512MB以上 (推奨2GB以上)
- ハードディスク : 200MB以上 (推奨20GB以上)

※別途 .NET Frameworkのインストールが必要な場合があります



よくある質問 1

- サービスはいつから開始していますか?
 - PAシリーズ向けは2015年9月14日より試験運用開始し、10月1日よりサービス開始しています。
 - Trapsは2017年6月1日よりサービスを開始しています。
- 本サービスを使用するにはどうすればいいですか?
 - 必要な機材とサブスクリプションをご購入いただき、弊社へお申し込みをお願いします。
- 「無償」とはどういう意味ですか?
 - 必要な機材とサブスクリプションをご購入いただければ、本サービスのご利用には費用はかかりません。
- PA-200、PA-2000、PA-4000、VM版は対象外ですか?
 - 現時点では対象外とさせていただいております。
- 本サービスのWildFireサンドボックス検査はWindows XPは対象外ですか?
 - 現時点では、Windows 7のみを対象とさせていただいております。
- WildFireシグニチャ生成時、外部にファイルを転送しているのでしょうか?
 - 外部への転送は行わず、LGWAN ASP上で生成されます。
- 他のWildFire利用ユーザとシグネチャは共有されるのでしょうか?
 - LGWAN ASP利用者とのみ共有されます。Internet上のWildFireクラウド利用者とは共有されません。
- WildFire以外のシグネチャアップデートはどのように実施するのですか?
 - LGWAN ASP上のシグネチャ提供サーバよりPC等の端末にダウンロードしていただき、PAへインストールする形になります。

よくある質問 2

- WildFireの無償版は使用可能でしょうか？
 - 申し訳ございませんが、本サービスでは使用できません。
- URLフィルタリングは必要ですか？
 - 必須ではありませんが、論理的にInternetアクセスができないセグメントであったとしても、ボットネットレポートの作成などにURLフィルタリングのサブスクリプションを使用しています。
- Traps単体の利用時にもWildFireのサブスクリプションは必要ですか？
 - 必要ありません。Trapsのライセンスのみでご利用いただけます。
- シグネチャ提供サーバの更新頻度はInternet上のものと同様でしょうか？
 - 現時点では、週次での更新をしています。
- シグネチャ提供サーバで、ライセンスの取得/更新やOSの取得は可能ですか？
 - 現時点では、ライセンス、OSなどの取得はオンラインではできず、別途Internet上の弊社サーバからダウンロードいただき、オフラインで移行していただく必要があります。
- シグネチャ提供サーバを利用して、シグネチャの自動更新は可能ですか？
 - 自動更新の仕組みは提供しておりませんが、PAシリーズのXML API機能を使うことで外部からシグネチャの更新を行うことは可能です。
- 使用可能な接続形態は？
 - L3モードでの接続形態を提供します。L1 (vwire) , L2モードについては、環境により提供可能です。構成詳細については、別途ご相談ください。
- 設定方法を教えてください。
 - お申し込みいただいた後に「サンプルコンフィグレーション」「初期導入手順書」「ASP型サンドボックス運用手順書」をご提供しますので、そちらを参考にしてください。