F5 SSL Orchestratorによる SSL/TLS 通信の可視化

F5 BIG-IP 製品

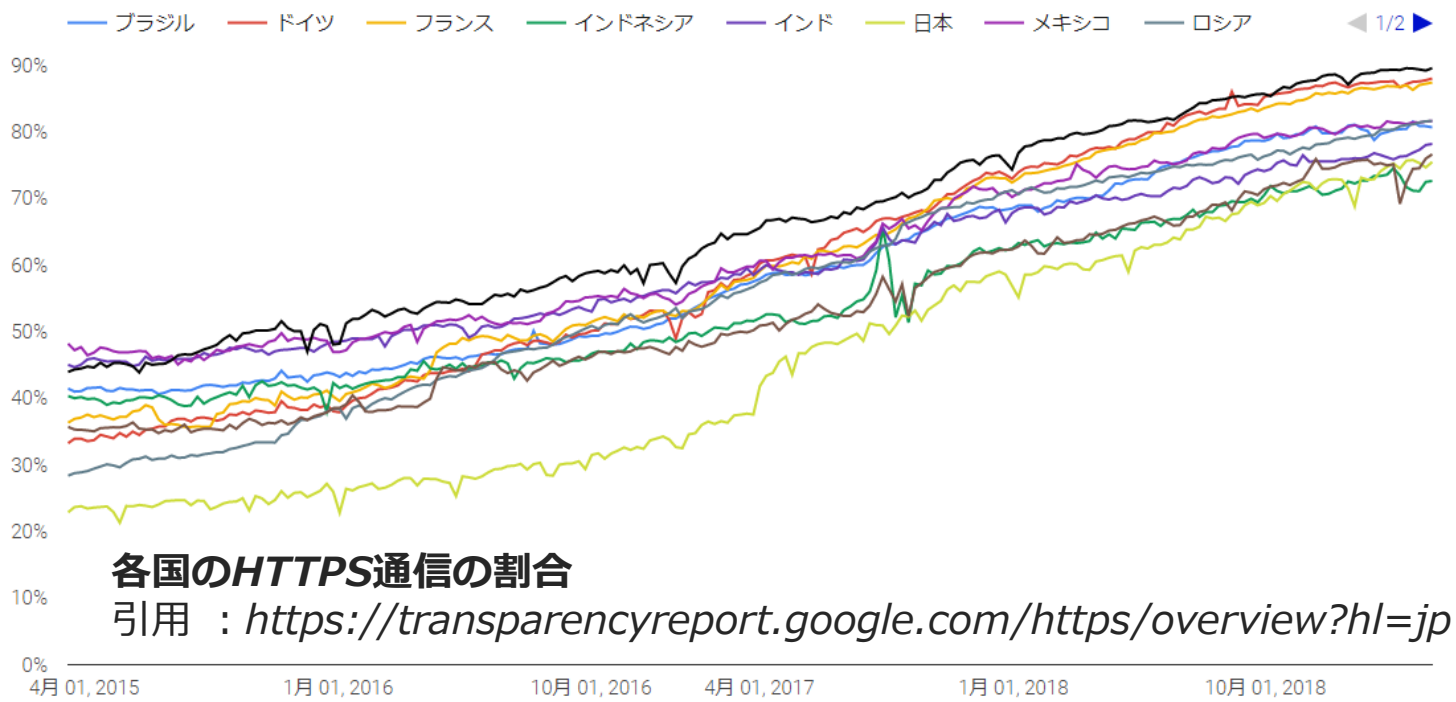
株式会社 ネットワールド

背景 (1/2)

Background

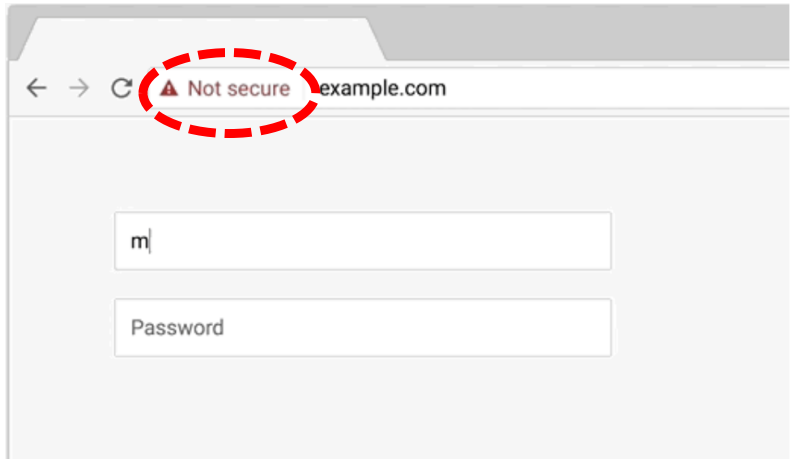
- **SSL/TLS通信の増加**

Googleは、2018年10月 「HTTPS普及に弾みが付いたことを踏まえ、**Chrome**の安全性情報も進化させる」と述べ、引き続き「デフォルトで使いやすくて安全なWeb」を目指すと宣言し、Chrome 70 より、**HTTP**ページにデータを入力すると赤色の「**保護されていない通信**」(Not Secure)の警告が開始されております。



各国のHTTPS通信の割合

引用 ：*https://transparencyreport.google.com/https/overview?hl=jp*



Google ChromeのHTTPページの警告表示

引用 ：*https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html*

© 2019 Networld Corporation All rights reserved.

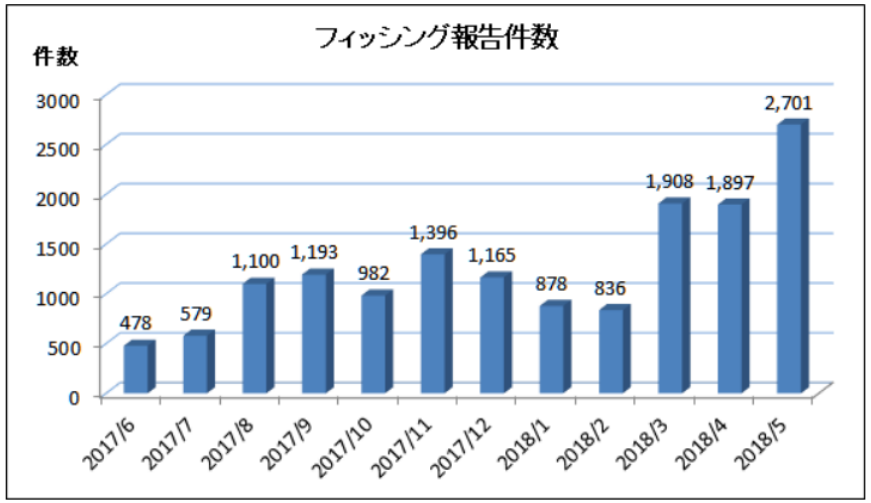
背景 (2/2)

Background

- **SSL/TLS通信に潜む脅威の増加**

WEBサイトの**常時SSL化**が進む一方で、一般的なセキュリティ製品にはSSL通信を暗号・復号化し（SSL可視化）、通信内容をチェックする機能があることがほとんどですが、通信処理性能への影響を考慮して、**SSL可視化機能を有効にできない状況**が多くのネットワークで見受けられます。

SSL通信の**身代金ウイルス（ランサムウェア）**や**詐欺サイト（フィッシングサイト）**、**マルウェア**等のセキュリティチェックは放棄されている状況となっております。



フィッシングサイト報告件数（引用：フィッシング対策協議会資料）

© 2019 Networld Corporation All rights reserved.

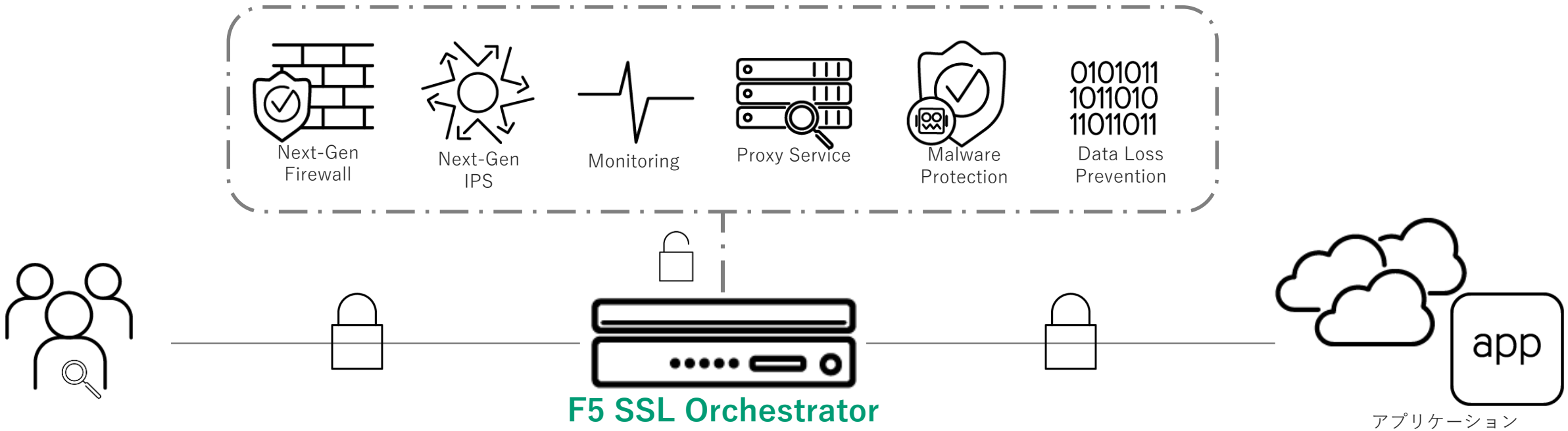
F5 SSL Orchestrator
– 概要/特徴 –

概要

Overview

- **F5 SSL Orchestrator(SSLO)**とは、BIG-IP製品で実績のある、信頼性と高パフォーマンスを持った最新のSSL復号/暗号化機能を搭載し、サードパーティ製のセキュリティ・ソリューションと連携する、SSL可視化製品です。

　ユーザへ グラフィカルな直観的で簡易な専用設定ウィザードを提供し、以前では実現できなかったネットワークトポロジー(構成)もサポートされ柔軟性を持ち、多くのユーザへご利用しやすい製品となってリリースされました。



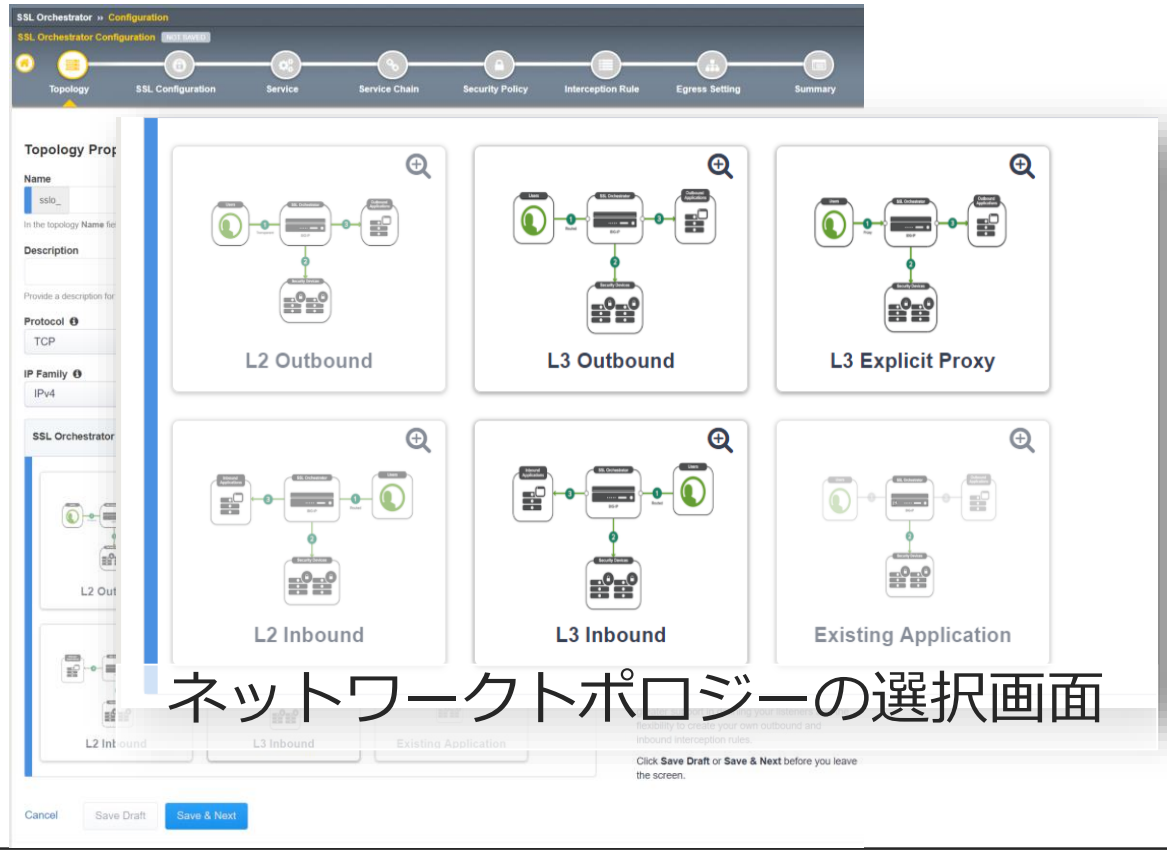
© 2019 Networld Corporation All rights reserved.

特徴（1/4）

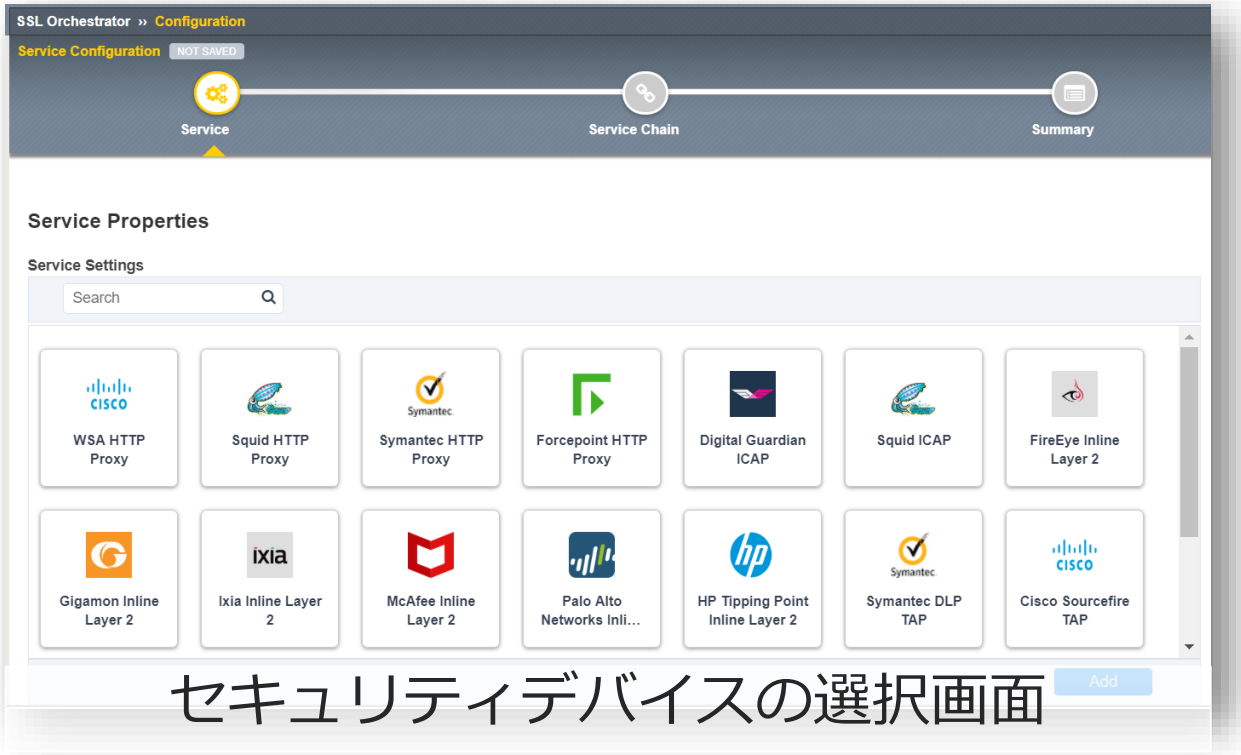
Features

- **Guided Configuration**：簡略化された直観的なGUI設定画面

  構成毎にステップ化された設定を行うことでVirtual Serverや各種Profile, iRuleが自動作成されます。
  複合化したトラフィックを転送するセキュリティデバイス用の設定画面が用意されています。



ネットワークトポロジーの選択画面



セキュリティデバイスの選択画面

© 2019 Networld Corporation All rights reserved.

特徴（2/4）

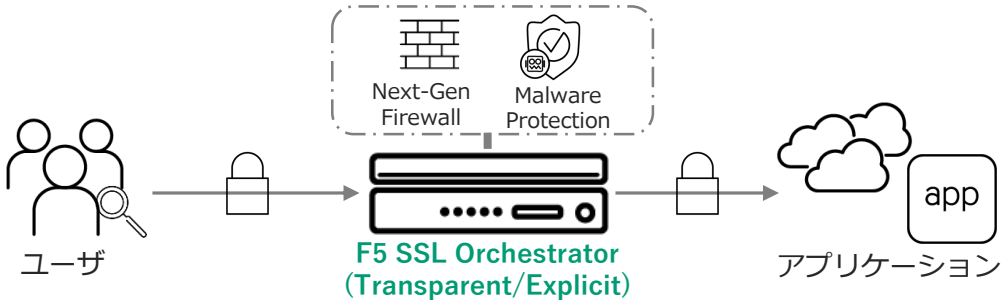
Features

- 複雑なネットワークトポロジーに対して、**柔軟な導入が可能**

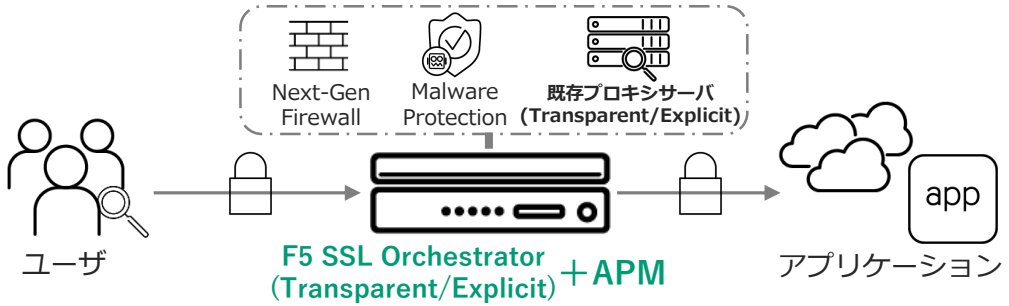
SSLO のデプロイメントモードはLayer2(指定機種)/Layer3 が存在し、SSLO自体のプロキシタイプはTransparent/Explicitに対応しております。

既存環境へ導入する場合、特にプロキシサーバが存在することが非常に多く、その場合も複数の構成に柔軟に適用可能です。SSLO の前後に既存プロキシサーバ存在する場合にもTransparentモードとして透過的に導入可能となります。

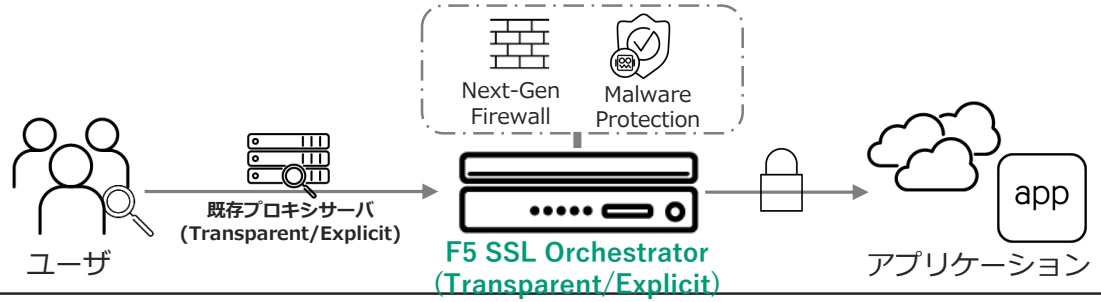
スタンダード



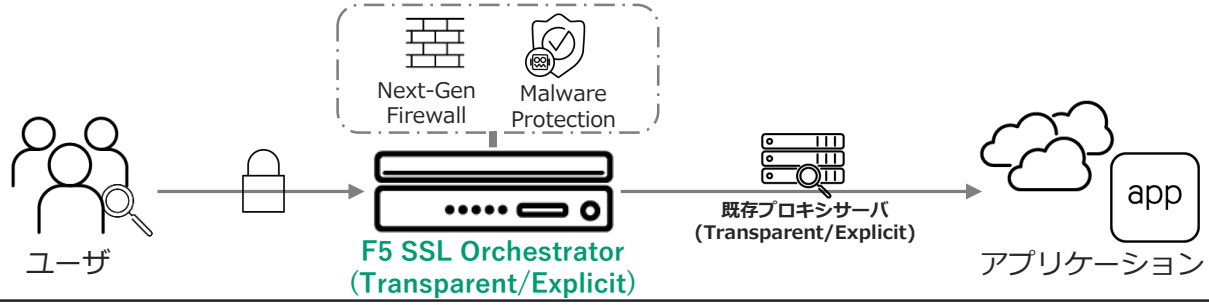
可視化対象にプロキシサーバを追加



既存プロキシサーバの後ろに配置



既存プロキシサーバの前に配置



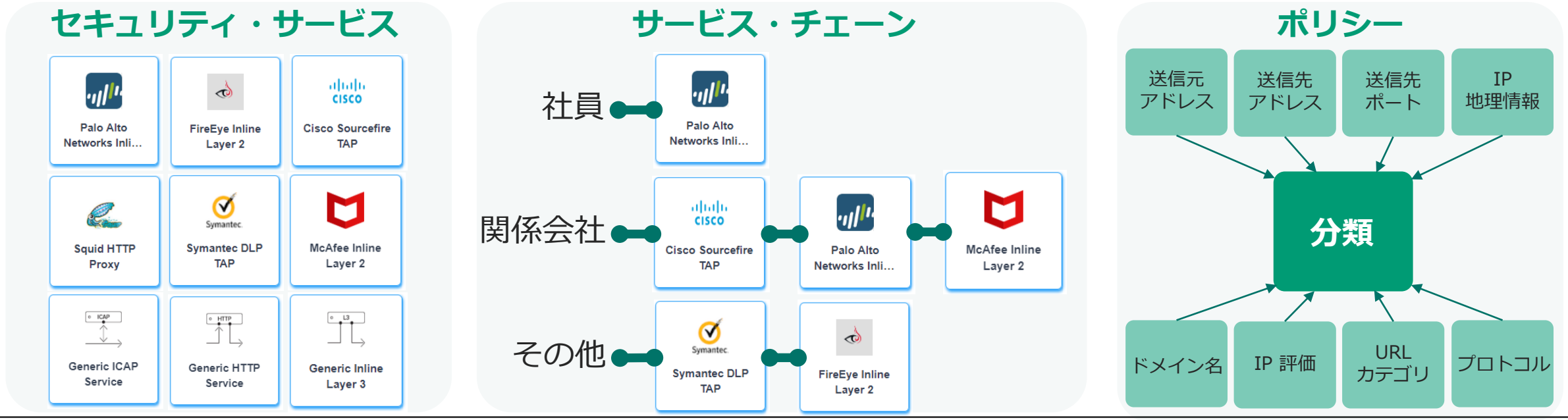
© 2019 Networld Corporation All rights reserved.

特徴（3/4）

Features

- カスタマイズ可能な **トラフィックフロー**

アンチウイルス/アンチマルウェア製品、侵入検知システム（IDS）、IPS 、次世代ファイアウォールおよびDLPなどの**セキュリティ・サービスを多段につなげる**ことができます。また、ドメイン名、コンテンツ・カテゴリ、地理的位置、IPレピュテーションを利用した**ポリシーに基づいて分類**を行い、トラフィックをバイパスするか、複号して、別のサービスに送信するかを決定できます。



© 2019 Networld Corporation All rights reserved.

特徴（4/4）

Features

- 最高クラスの**SSLオフロード/次世代暗号化プロトコルへの対応**

  最新Cipher や Apple Transport Security（ATS）などの新しい暗号化プロトコルにより、ネットワーク・セキュリティを強化するSSL Forward Secrecyが急速に普及しています。次世代暗号化へ移行すると、セキュリティ制御をせず、危険に晒すような、パッシブなSSLデバイスでは対応が困難になります。多様な暗号化サポートにより、アーキテクチャを変更することなく、新たな盲点を防ぐことができる最高の柔軟性を実現できます。

© 2019 Networld Corporation All rights reserved.

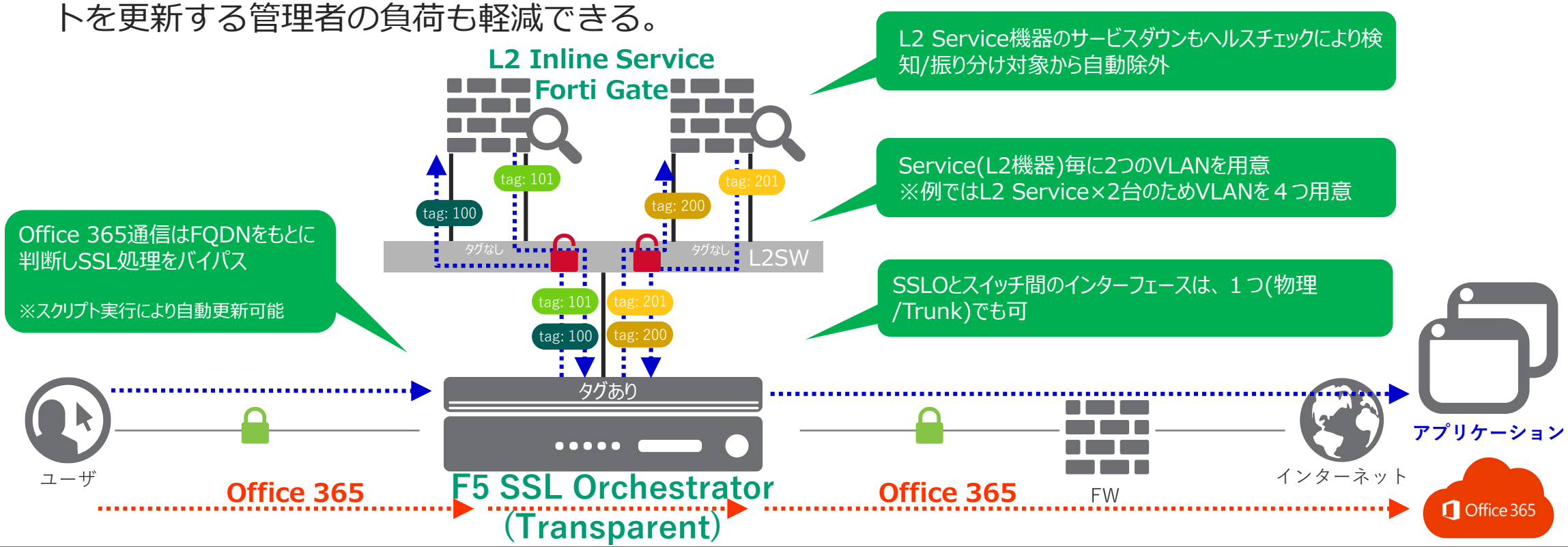
F5 SSL Orchestrator
– 構成例 –

構成例①

SSLO + FortiGate：SSL可視化 + UTM + Office 365 プロキシバイパス

SSL Orchestrator ＆ Office365 Bypass ＆ L2 Service(UTM)

- Office365利用に伴い、1ユーザ当たりのセッション数が大幅に増加
  ⇒ (脅威でない)Office365通信は、可視化対象から除外。それ以外のWEB通信はSSLOでSSLデコードし可視化トラフィックをUTM(FortiGate)に転送して検査を実施。
- UTM(FortiGate)はOffice365通信とSSLデコード処理をする必要がないため不要な検査・負荷を軽減できる。
- Office365URLは定期的に更新されるが、SSLOで自動更新スクリプトを実装することでOffice365 URLリストを更新する管理者の負荷も軽減できる。

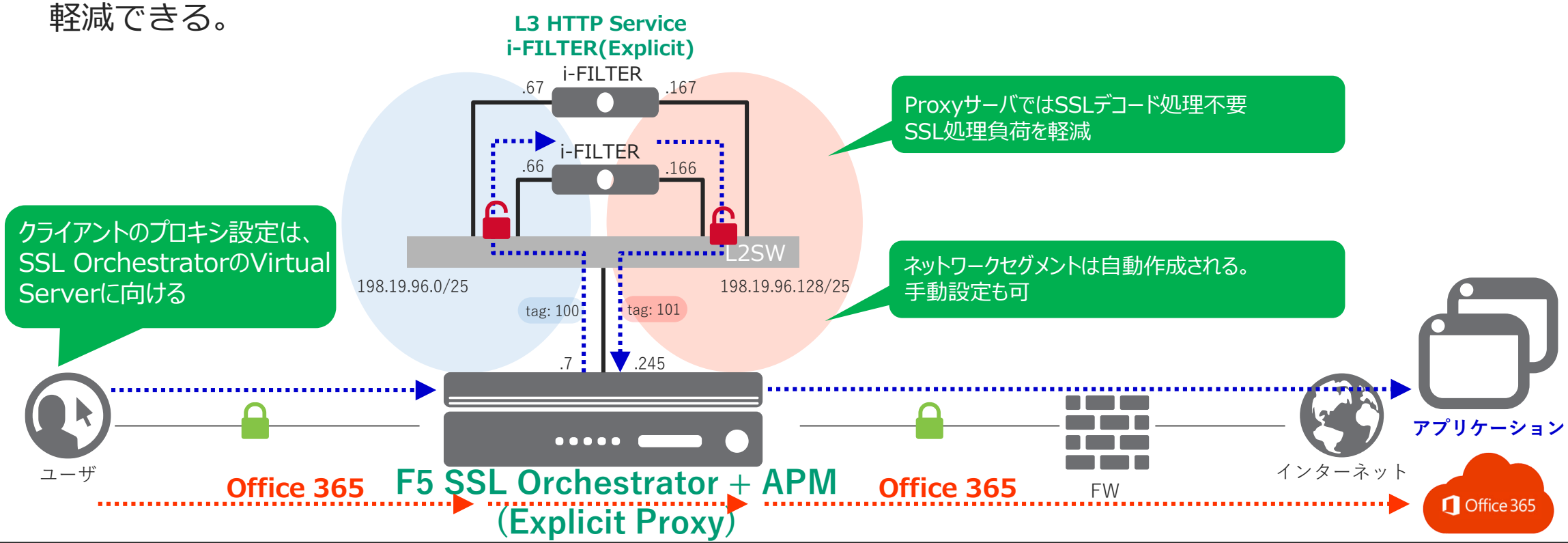


© 2019 Networld Corporation All rights reserved.

構成例②
SSLO + i-FILTER：SSL可視化 + Webフィルタリング + Office 365 プロキシバイパス

SSL Orchestrator ＆ Office 365 Bypass & HTTP Service(i-FILTER Explicit Proxy)

- Office365利用に伴い、1ユーザ当たりのセッション数が大幅に増加
  ⇒ (脅威でない)Office365通信は、可視化対象から除外。それ以外のWEB通信はSSLOでSSLデコードし可視化トラフィックをProxy Server(i-FILTER)に転送してWEBフィルタリングを実施。
- Proxy ServerではOffice365通信とSSLデコード処理をする必要がないため不要な検査・負荷を軽減できる。
- 構成例1同様に、Office365URLの定期更新は、自動更新スクリプトをSSLOで実装すること管理者の負荷も軽減できる。



© 2019 Networld Corporation All rights reserved.

F5 SSL Orchestrator
– その他 –

機種選定や動作検証について

Model selection and Verification

・**機種選定**については、お客様がご利用予定のスループット、SSL処理性能及びネットワーク構成やトラフィックフローによって必要となるスペックが異なるため、都度、お気軽にお問合せ窓口にご相談ください。

・**動作検証**については、無償にてSSLO貸出検証機で実施が可能です。SSLOとサードパーティ製品とのSSL可視化連携を試したい場合は、お気軽にお問合せ窓口にご相談ください。

© 2019 Networld Corporation All rights reserved.

お客様からよくあるご質問(1/2)

ARU ARU

Q. サポートされるL7プロトコルは何がありますか。

A. IMAP, SMTPS, POP3, FTP, HTTP がサポートされております。
※ HTTP以外の上記プロトコルはTransparentモードでサポートされております。
※ FTP はPassiveモードのみサポートしております。

Q. HA構成は可能ですか。

A. はい。Active-Standbyモードをサポートしております。
※ Scale-N構成(Active-Active-Standby)は非サポートとなります。

Q. SSLOを利用する場合に必要な購入製品を教えてください。

A. 2パターンございます。 1 つ目はSSL Orchestrator スタンドアロン製品としてはBIG-IP i2800, i5800, i10800があります。2つ目はBIG-IP LTMをベースとして、SSL Orchestratorモジュールを Add-onする組合せでご購入可能です。

Q. URLカテゴリによる分類やIPレピュテーションはSSL Orchestrator モジュールのみで可能ですか。

A. いいえ。DBを利用したURLフィルタリング・ IPレピュテーション機能は追加でサブスクリプションライセンスが必要となります。

© 2019 Networld Corporation All rights reserved.

お客様からよくあるご質問(2/2)

ARU ARU

Q. スマートフォン(Android, iOS) を利用する場合で注意すべき点はありますか。

A. Android/iOSに限らず、ブラウザできない(Non-Browser)クライアント(Dropboxアプリやアンチウィルスアップデートツールなど)からの接続に失敗する場合がございます。Non-Browser クライアントの多くは独自の信頼済み証明書ストアを保持し追加CAを認めない場合が多いです。その場合の回避方法としては、SSLOでURLを指定してバイパスする必要がございます。

特にAndroid端末では、ユーザがインポートしたCA証明書はシステム証明書ストアではなくユーザ証明書ストアにインポートされます。バージョン7.0以降、スマートフォンアプリ側で明示的にユーザ証明書ストアを信頼するようになっていなければCA証明書は信頼されず接続に失敗します。 アプリ自体の仕様になります。 https://android-developers.googleblog.com/2016/07/changes-to-trusted-certificate.html

Q. ECC と DSA の署名アルゴリズムはサポートされてますか。

A. SSLOはクライアント側のECCおよびDSA署名(Signing)アルゴリズムをサポートしておりません。 （DHE-RSAおよびECDHERSAなど、ECCおよびDHEハンドシェイクアルゴリズムはサポートされています）ただし、DSAおよびECDSA署名アルゴリズムは別々のDSAまたはECDSA署名鍵を必要とします（例：DHE-DSA、ECDHE-ECDSA）。SSLOの フルプロキシアーキテクチャとして、サーバーサイド側のECC/DSA Cipherがサポートされておりますので通常問題になることは少ないです。

Q. TLS1.3を利用して接続は可能ですか。

A. いいえ。現時点(2019/4)ではクライアントとSSLO間、SSLOとサーバ間の両方でTLS1.3はサポートされておりません。

© 2019 Networld Corporation All rights reserved.

本資料に関するご相談・ご質問などございましたらご連絡お待ちしております。

f5-info@networld.co.jp