ソリューションブリーフ

SSL/TLS通信に対するWebフィルタリング/無害化/ウイルススキャン

ALSI InterSafe WebFilterおよびOPSWAT MetaDefenderとA10 SSLインサイトソリューションの連携

SSL/TLS通信の増大とセキュリティの盲点

近年、スヌーピングや改ざん、データの窃盗を防ぐために、HTTPSを始めとする通信データのSSL/TLSによる暗号化の流れが進んでいます。サーバー証明書の発行が容易になり、Webサイトの HTTPS化への対応度合いが検索サイトでのランキングに影響したり、利用が拡大するクラウドサービスの多くがHTTPSでの接続を前提としたりしていることから、すでに通信プラットフォームを流れる大部分の通信がSSL/TLS通信となっています。

その一方で、フィッシングサイトなどの悪意のあるWebサイトの多くがHTTPS化されていたり、HTTPSのポータルサイトに表示される広告にマルウェアが仕込まれたり、HTTPS経由でダウンロードするドキュメントファイルに悪意のあるマクロやコードを仕込んだ画像を埋め込んだり、メールの添付ファイルを開くとSSL/TLS通信を通じてマルウェアをダウンロードして端末をボット化したり、感染した端末からHTTPS通信を利用するSNSやクラウドストレージ経由で機密情報をアップロードさせるなど、SSL/TLS通信がサイバー攻撃の隠れ蓑や情報漏洩の抜け道として悪用されることが増えています。サイバー攻撃の手法に追従し、組織のセキュリティを担保するにはSSL/TLS通信に隠れた脅威の対策が必須となっています。

政府機関や自治体、金融機関などの高度なセキュリティを求められる組織においては、これまでもWebフィルタリングやコンテンツの無害化によるファイルなどに埋め込まれた脅威の排除、ウイルススキャンによる防御など、多層化されたネットワークセキュリティ環境を構築していますが、SSL/TLS通信に対しては十分な検査能力を持っていない、または検査する場合には大幅に性能が低下するなど、増大するSSL/TLS通信に対して十分なセキュリティを担保できなくなりつつあります。

SSL/TLS通信に対する高精度なWebフィルタリングとコンテンツ無害化および高検知率のウイルススキャンの実現

A10ネットワークスのA10 Thunderシリーズで利用できるSSLインサイトソリューションを利用することで、通信パフォーマンスを落とすことなくSSL/TLS通信を可視化できます。Thunderアプライアンスを組織内部にあるクライアントとインターネットの間に設置することで、クライアントとインターネット間のSSL/TLS通信をインターセプトして復号し、復号して平文化した通信データをインライン型・パッシブ型・ICAPサーバー型のセキュリティ機器に転送して検査できます。トラフィック分析のために復号された通信データは再暗号化され、目的のアドレスに転送されます。

このSSLインサイトソリューションをアルプスシステムインテグレーション株式会社（以下、ALSI）の提供する高精度Webフィルタリング製品ALSI InterSafe WebFilter、およびOPSWAT社の提供するセキュリティ製品MetaDefenderと連携させることにより、SSL/TLS通信に対するWebフィルタリング・コンテンツ無害化・ウイルススキャンを同時に実現することができます。これによって、高度なセキュリティが求められる組織でのSSL/TLS通信に潜む脅威への多層的な防御が実現できます。

ALSI InterSafe WebFilterは、URLデータベースに基づいてWebアクセスをコントロールし、不正サイトへのアクセスや書き込みをブロックする国産Webフィルタリングソフトです。国内最大クラスの148カテゴリ、網羅率98%を有する高精度URLデータベースは大手携帯キャリア3社での採用をはじめ、日本国内での高いマーケットシェアを持ちます。さらに、未知のURLをクラウド上で判定する「高度分類クラウド」や国・地域別にアクセスを可視化する「Geoスコープ」により最新の脅威に対応し、安全なWebアクセス環境を実現します。

OPSWAT MetaDefenderは重要インフラを保護するコア技術としてグローバルで導入され、多数のファイル形式に対応したコンテンツ無害化技術（Deep CDR）や、最大30種類以上のアンチマルウェアエンジンの同時利用で高い検知率のウイルススキャンを行うマルチスキャン技術（Metascan）などを備えたセキュリティ製品です。Deep CDRでは、ファイル形式、ユーザビリティを維持したコンテンツの無害化が行われ、ダウンロードファイルなどに埋め込まれたマクロや画像データに潜む脅威を除去・

課題：

- 政府機関や自治体、金融機関などの高度なセキュリティが求められる組織でのSSL/TLS通信を悪用したネットワーク上の脅威への対策
- SSL/TLS通信に対するWebフィルタリングとコンテンツ無害化、およびウイルス検知率の向上

解決策：

- A10 ThunderのSSLインサイトソリューションによるSSL/TLS通信の高速な可視化
- ALSI InterSafe WebFilterとの連携による高精度なWebフィルタリング
- OPSWAT MetaDefenderとの連携で、CDR（コンテンツの非武装化と再構築）技術によるファイル無害化、複数のウイルス対策エンジンによるウイルス検知率の大幅な向上（アップロード/ダウンロード双方に対応可能）

メリット：

- SSL/TLS通信に潜む脅威に対する多層的な防御の実現
- SSL/TLS通信の高速な復号/再暗号化による高い通信パフォーマンスの維持
- 148のカテゴリに分類され、国内最高水準の網羅率98%の国内最高水準の高精度URLデータベースとマルチスキャンエンジンによる、アップロード/ダウンロード双方に対する高精度なフィルタリングとウイルススキャン
- 多数のファイル形式に対応し、視覚的な状態を維持しつつユーザビリティを損ねないコンテンツ無害化

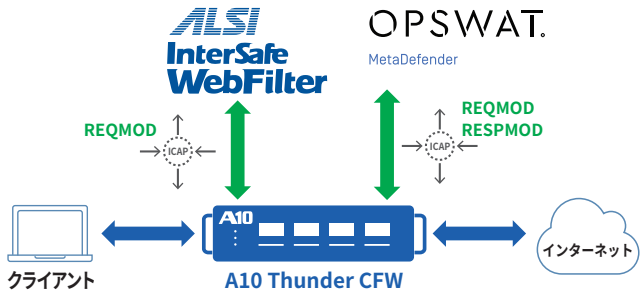

図1：A10 Thunderによる SSL インサイトソリューションと
ALSI InterSafe WebFilter および OPSWAT MetaDefender との連携

無効化します。Metascanでは世界で実績のある複数のアンチマルウェアエンジンで同時にファイルスキャンを行うことで、アップロード/ダウンロードされるファイルに含まれる脅威を各エンジンのシグネチャ、ヒューリスティック、機械学習機能により高い検知率で検査することができます。データ損失防止機能も利用することが可能です。

A10のSSLインサイトソリューションとALSI InterSafe WebFilterおよびOPSWAT MetaDefenderとの連携ソリューションを図1に示します。Thunderアプライアンスは企業の内部にあるクライアントとインターネットの間に設置し、クライアントからはプロキシサーバーとして指定する形になります。A10 ThunderはHTTP/HTTPS通信のフォワードプロキシとして動作し、HTTP/HTTPS通信をインターセプトします。ALSI InterSafe WebFilterおよびOPSWAT MetaDefenderはICAPサーバーとして動作し、ThunderアプライアンスがICAPクライアントとして動作することで、ALSI InterSafe WebFilterおよびOPSWAT MetaDefenderとの通信を行います。

この時の通信の流れは以下のようになります。

1. A10 Thunderがクライアントから通信先のサーバーに向けたトラフィックをインターセプトし、SSL/TLS通信を復号し、ICAPを通じてALSI InterSafe WebFilterおよびOPSWAT MetaDefenderに送信、Webフィルタリングやアップロードファイルのウイルススキャンを実施
2. 平文化されたSSL/TLSトラフィックをA10 Thunderが再暗号化し通信先サーバーにフォワード
3. 通信先のサーバーはリクエストを受信し、レスポンスをクライアントに送信
4. A10 Thunderが暗号化されたサーバーからのレスポンスをインターセプトし、復号した後ICAPを通じてOPSWAT MetaDefenderに送信、コンテンツの無害化やダウンロードファイルのウイルススキャンを実施
5. 復号された通信を再暗号化しクライアントに送信

※ 平文通信の場合は復号せずに通信を検査

SSL/TLS通信の特性上、リクエストの復号とレスポンスの再暗号化のためにクライアントがA10 Thunderを信頼する必要があるため、A10 Thunderにはクライアントが信頼できる証明書がインストールされていなくてはなりません（または、クライアント側にA10 Thunderと同じ証明書が信頼できる証明書としてインストールされている必要があります）。Thunderには任意の証明書をインストールして利用することができます。

SSL/TLS通信に含まれるリクエスト/レスポンスを平文でALSI InterSafe WebFilterやOPSWAT MetaDefenderに渡すことで、これまで通信データの内容が検査できなかったSSL/TLS通信に対しても、平文の通信と同様の検査が可能になります。特にHTTPSサイトへの詳細なWebフィルタリングやPOSTフィルタリング、SSL/TLS通信で送受信されたファイルに対するコンテンツ無害化と高検知率のウイルススキャンが可能になり、高いセキュリティを実現できます。クライアントとA10 Thunderの間、およびA10 Thunderと通信先サーバーとの間のコネクションは暗号化され、なりすましやデータ窃盗は防止されます。

SSLインサイトソリューションを用いると、一度の復号で複数の機器での検査を行うことができるため、復号/再暗号化に伴う通信遅延を最小にできます。また、Thunder自身を冗長化して可用性を高めることもできます。

その他のA10 ThunderによるSSLインサイトのメリットは以下になります。

- 格段に優れたSSL/TLSコネクション数の処理能力とスループット（1台で最大25Gbps、2台で最大50Gbps）
- 全てのポートに渡るSSL/TLSトラフィックの復号
- L2/L3の多様なネットワーク構成に対応し、既存の環境に応じた柔軟な構成での導入
- 復号の対象とするSSL/TLS通信の指定などが可能な詳細なポリシー設定

アルプス システム インテグレーション株式会社について

アルプス システム インテグレーション株式会社（ALSI〔アルシー〕）は、グローバルに事業を展開するアルプスアルパイン株式会社のシステムインテグレーション事業を担う戦略子会社です。「セキュリティ」「デジタル」「ファームウェア」「IoT」の4事業を展開しています。セキュリティ事業では、国内の草分けとして1996年より事業を開始したWebフィルタリングを中心とするアクセスマネージメントと、情報の保護と活用を両立する情報漏洩対策を両輪に、お客様に安心・安全を提供します。

URL：www.alsi.co.jp/

OPSWAT Japan株式会社について

2002年に設立したOPSWATは、ファイル無害化とマルチスキャンのリーディングカンパニーとして、世界の重要インフラをはじめ1500以上の組織へセキュリティソリューションを提供しています。日々高度化・巧妙化するサイバー攻撃から組織を守るために、ゼロトラストの理念「Trust no file. Trust no device.」（如何なるファイルもデバイスも信用しない）のもと研究開発を続け、世界350社以上のテクノロジー、チャネルパートナーと共に製品・ソリューションを提供しています。

OPSWAT Japan株式会社は、OPSWATのグローバル展開フェーズにおいて子会社として2018年に設立され、自治体・教育委員会をはじめ政府、金融、製造、エネルギー、ヘルスケアなどエンタープライズのお客様へパートナー様との協業・連携により、付加価値のあるサイバーセキュリティソリューションを提供しております。

URL：www.opswat.jp/

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）は、サービス事業者やクラウド事業者および企業で利用される5Gネットワークやマルチクラウドアプリケーションのセキュリティを確保します。高度な分析や機械学習、インテリジェントな自動化機能により、ミッションクリティカルなアプリケーションを保護し、信頼性と可用性を担保します。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。

www.a10networks.co.jp/
Facebook：http://www.facebook.com/A10networksjapan

Learn More

About A10 Networks

お問い合わせ
a10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.co.jp
a10networks.co.jp/contact

Part Number: A10_SB_ALSI InterSafe_and_OPSWAT MetaDefender_and_A10　Nov 2020