ソリューションブリーフ

HTTPS通信の可視化による高精度な脅威URLへのアクセス防止とコンテンツフィルタリングによる情報漏洩の防止

キヤノンマーケティングジャパンGUARDIANWALL WebFilterとA10のSSLインサイトの連携

常時HTTPS化の流れとHTTPS通信に潜む脅威

近年、多様化するサイバー犯罪への対処や情報機関からの盗聴、スヌーピングや改ざん、データの窃盗を防ぐために、主にWebサイトへのアクセスを中心に通信データの常時HTTPS化の流れが進んでいます。当初はクレジットカードでの取引やユーザーログイン情報など、機密性の高いデータ通信のみを暗号化していましたが、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、ブラウザの表示にWebサイトの暗号化への対応状況が表示されるようになっていたり、多くのクラウドサービスがHTTPSでの接続を前提としていることから、すでに通信プラットフォームを流れる大部分のWebリクエストとレスポンスがHTTPS化されています。

その一方で、悪意のあるWebサイトが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、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、HTTPS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も増えてきています。日々新しくなる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HTTPS通信に隠れた脅威の対策が必須となっています。

しかし、多くのセキュリティ機器はHTTPS通信量の増加に追いつく性能を持っていません。既存のセキュリティ機器でHTTPS通信の復号と検査を行う場合、HTTPを検査する場合と比較して大幅にパフォーマンスが低下し、所望のネットワーク性能を得るためには多くの機器を利用する必要があります。また、複数の機器でHTTPS通信の検査を行うことで、その処理による通信遅延も大きくなります。

HTTPS通信の可視化：SSLインサイトソリューション

A10ネットワークスのA10 Thunderシリーズにより提供されるSSLインサイトソリューションにより、HTTPS通信に隠れた脅威を可視化し、通信プラットフォームのパフォーマンスを落とすことなくセキュリティ機器での脅威検知と防御を実現できます。SSLインサイトを利用すると、A10 Thunderがクライアントとインターネット間のHTTPS通信をはじめとするTLS/SSL通信をインターセプトし高速に復号します。復号したトラフィックをセキュリティ機器に送ることで、通信データに含まれる脅威の検査と分析を実現できます。トラフィックの分析が終了し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。A10のSSLインサイトソリューションは格段に優れたHTTPS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）を持ち、高速なSSL/TLS通信の可視化を実現できます。

SSLインサイトを導入する際には、A10 Thunderを自組織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ます。平文化した通信データはインライン型・パッシブ型のセキュリティ機器で検査できるとともに、ICAPを通じて外部のICAPサーバーとの連携を行うことができます。トラフィックを一度復号すれば複数の機器で検査でき、SSL/TLS通信の復号と再暗号化に伴う通信遅延を最小に抑えられます。

HTTPS通信に隠れた脅威に対するWebフィルタリングとコンテンツフィルタリング

SSLインサイトとGUARDIANWALL WebFilterの連携

A10 Thunderシリーズの提供するSSLインサイトソリューションにより復号したHTTPS通信をキヤノンマーケティングジャパン株式会社のGUARDIANWALL WebFilterで検査することで、HTTPS通信に対するWebフィルタリングとコンテンツフィルタリングを実現できます。これによりHTTPS通信に含まれる脅威URLへのアクセスのブロックや、個人情報や機密情報のHTTPS通信を通じた漏洩を防止できます。

GUARDIANWALL WebFilterのWebフィルタリングは、高いカテゴリヒット率を持つCYREN社のURLデータベースを採用しており、収集された世界各国の脅威情報に基づきURLデータベースをリアルタイムに更新します。未知の脅威は脅威情報と連携して自動でブロックします。偽メールによってフィッシングサイトへ誘導された場合も、これらの機能によりサイトへのアクセスを遮断でき、フィッシング対策の軸となる「意図しないアクセス」を阻止し、個人情報を守ります。また、コンテンツフィルタリングの機能も持ち、添付されるファイルの種類（拡張子）だけでなく、その内容も検査できます。コンテンツフィルタリングの

課題：

- HTTPS通信の宛先URLに応じた適切なアクセス制御
- HTTPS通信を悪用した脅威を検知するための高速なHTTPS通信の可視化とセキュリティの強化
- 組織内の機密情報のHTTPS通信を通じた漏洩の防止

解決策：

A10 ThunderのSSLインサイトソリューションによりHTTPS通信を高速に可視化（復号）し、キヤノンマーケティングジャパン株式会社のWebフィルタリング製品GUARDIANWALL WebFilterと連携することで、HTTPS通信の高精度なWebフィルタリングによる脅威URLへのアクセス防止とHTTPS通信に含まれるコンテンツに対するフィルタリングを実現

メリット：

- 高いカテゴリヒット率を持つURLデータベースを持ち、脅威情報との連携が可能なGUARDIANWALL WebFilterをHTTPS通信のWebフィルタリングに適用することで、脅威URLへのアクセスを自動ブロック
- GUARDIANWALL WebFilterの独自技術によるコンテンツフィルタリングにより、アップロードされるファイルに含まれるキーワードや個人情報を検査して情報漏洩を防止
- 大規模なセッションを処理可能なA10 ThunderによるHTTPS通信の高速な復号/再暗号化により高い通信パフォーマンスを維持

図1：A10 Thunderによる SSL インサイトソリューションと
キヤノンマーケティングジャパン GUARDIANWALL WebFilterとの連携

対象として「キーワード検査」や「個人情報検査」などを指定することが可能で、機密情報や個人情報の情報漏洩を阻止できます。個人情報検査ではマイナンバーや個人情報を独自技術で解析し検知できます。サイトアクセスログの収集や外部送信データのアーカイブにも標準対応しており、統計情報から問題のある端末を特定し管理者へ通知するなど、運用を支援する機能も豊富に備えています。

A10 の SSL インサイトソリューションと GUARDIANWALL WebFilter との連携ソリューションを図1に示します。A10 Thunder を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（透過型での構成も可能です）。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。GUARDIANWALL WebFilter は ICAP サーバーとして動作し、A10 Thunder が ICAP クライアントとして動作することで、GUARDIANWALL WebFilter 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Webサーバーに向けたHTTP/HTTPSトラフィックをインターセプトし、HTTPの場合はそのまま、HTTPSの場合はトラフィックを復号して平文化したトラフィックをICAPによりGUARDIANWALL WebFilterに送信し、GUARDIANWALL WebFilterでHTTP/HTTPS通信のWebフィルタリングとコンテンツフィルタリングを実施
2. GUARDIANWALL WebFilterからHTTP/HTTPSリクエストの送信可否をICAPでA10 Thunderに通知。アクセスをブロックする場合はGUARDIANWALL WebFilterの規制画面をクライアントに転送
3. HTTP/HTTPSリクエストの送信がGUARDIANWALL WebFilterに許可された場合、平文化されたHTTPSトラフィックをA10 Thunderが再暗号化しWebサーバーにフォワード。HTTPトラフィックはそのままフォワード
4. Web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
5. HTTPS通信の場合は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、一旦復号した後再暗号化しクライアントに送信

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はクライアントが A10 Thunder を信頼できる必要があるため、A10 Thunder とクライアントには共通の証明書がインストールされている必要があります。A10 Thunder には自組織の持つ任意の証明書をインストールして利用できます。

HTTPS トラフィックに含まれるリクエスト内容を平文で GUARDIANWALL WebFilter に渡すことで、HTTP だけでなく HTTPS 通信に対しても高度な Web フィルタリングを実現できます。クライアントと A10 Thunder の間、および A10 Thunder と Web サーバーとの間のコネクションは暗号化したまま保持されるため、なりすましやデータ窃盗は防止されます。

この構成でユーザー認証が必要な場合は、A10 Thunder がプロキシサーバーとして動作しているため、ユーザー認証を A10 Thunder 上で行う形を取ります。A10 Thunder は認証サーバーと連携した各種認証方式に対応しています。認証したユーザー情報やクライアント IP の情報は GUARDIANWALL WebFilter に送信でき、ユーザーに応じた Web フィルタリングのルールを適用できます。

上記に加え、負荷分散機能を利用することで、複数の GUARDIANWALL WebFilter サーバーの利用も可能です。あるサーバーに障害が発生した場合には、冗長化された別のサーバーに通信データを送信でき、高可用性とスケーラビリティをともに実現できます。

その他の特長

A10 ネットワークスの SSL インサイトソリューションでは、一度復号した TLS 通信を GUARDIANWALL WebFilter に ICAP で連携するだけでなく、パッシブ型・インライン型の複数のセキュリティ機器に送信して検査できるため、復号し平文化された HTTPS 通信をサンドボックス機器や次世代ファイアウォール、IPS/IDS、SIEM 製品やフォレンジック製品に渡すことで、クライアントとサーバー間で送受信される HTTPS トラフィックをともに検査でき、多層防御を実現できます。これにより、特定サイトからのダウンロードに含まれるマルウェアなどの脅威も検知できます。

SSL インサイトソリューションは L2/L3 の多様なネットワーク構成に対応でき、既存のネットワーク環境に合わせた柔軟な導入が可能です。ポート 443 に限らず全てのポートでの SSL/TLS トラフィックの復号もできます。必要な性能に応じ単一アプライアンスおよび複数アプライアンスでの導入ができ、冗長構成をとることで可用性も担保できます。また、詳細なポリシー設定により、トラフィックの種類、発信元 / 宛先 IP アドレスや利用者の情報、その他の属性に応じてどの暗号化セッションを復号して検査対象とするか、どのセッションを暗号化されたままにして検査対象から除外しておくかを制御することもできます。

キヤノンマーケティングジャパン株式会社について

キヤノングループは、グローバル企業として世界中で幅広い事業を展開しています。その一員として、日本国内を中心にマーケティング活動やソリューション提案を担っているのが、キヤノンマーケティングジャパングループです。私たちは、社員一人ひとりがお客さまに最も近い存在として、「顧客主語」と「ものづくりへの参画」を実践し、お客さまの価値を最大化するお手伝いをしていきます。

私たちは、イメージング分野におけるキヤノンの開発力と幅広い製品群、IT の技術力など、さまざまな強みを生かし、お客さまに最適なソリューションを提供します。 https://canon.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_CMJ_GWWF_and_A10　Nov 2020