HTTPS 通信を高精度に Web フィルタリング

デジタルアーツ i-FILTER と A10 の SSL インサイトソリューションの連携

課題：

- 増大する HTTPS 通信に対する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

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、デジタルアーツのWebフィルタリングソフトウェアi-FILTERと連携することで、HTTPS通信の高精度なWebフィルタリングを実現

メリット：

- 業界最高水準の i-FILTER のデータベースを HTTPS 通信の Web フィルタリングに利用し、高精度に脅威を検知
- 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
- FireEye NX、Trend Micro DDI との連携により未知の脅威に対するセキュリティの強化も可能

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を防ぐ目的で、Web サイトを HTTPS 化（SSL/TLS 化）する常時 HTTPS 化が主流となってきています。常時 HTTPS 化により Web サイトの信頼性と通信の安全性を高められる一方、HTTPS 通信が情報漏えいの抜け道やサイバー攻撃の隠れ蓑として悪用されることも増えてきており、企業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、既存の Web フィルターやプロキシサーバー、サンドボックス、ファイアウォールなどで HTTPS 通信の復号を行って通信の検査を行った場合、膨大な CPU リソースが必要になり、これまで通りの十分な性能が得られない問題があります。

A10 ネットワークスの Thunder シリーズが提供する SSL インサイトソリューションを利用することで、SSL/TLS の高速な処理が可能になります。Thunder シリーズによって HTTPS 通信を高速に復号し、平文の検査を行った後、再暗号化して通信を行うことが可能になり、HTTPS 通信に隠れた脅威を検出できます。復号した HTTPS リクエストをデジタルアーツ社の Web フィルタリングソフトウェアである i-FILTER で検査することで、HTTPS 通信に対する高精度の Web フィルタリングが可能になります。

カテゴリ数、登録件数そして精度ともに業界最高水準の Web フィルタリング製品である i-FILTER のデータベースと A10 ネットワークスの高速な SSL/TLS 通信可視化ソリューションとの連携により、HTTPS 通信に隠れた脅威に対する有効な防御が実現できます。

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を防ぐ目的で、HTTPS（HTTP over SSL/TLS）を用いてデータを暗号化する Web アプリケーションが増加しています。多くの Web アプリケーションは当初、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 HTTPS により暗号化していましたが、近年は全ての Web リクエストとレスポンスを暗号化する常時 HTTPS 化の流れが加速しています。クラウドサービス等の利用が拡大してサーバー証明書の発行が容易になったり、検索サイト等でも HTTPS 化されたサイトが上位の検索結果に表れるようになったり、スマートフォンから HTTPS 化されていないサイトへのアクセスをあえて遅延させたりするような動きもあることから、NSS Labs の調査では 2019 年までに 75% のエンタープライズのトラフィックが暗号化されると予測されています。[*1]

その一方で、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 通信を利用する SNS やクラウドストレージ経由でボット化したクライアントへの指令を行ったりするなど、HTTPS 通信が情報漏えいの抜け道やサイバー攻撃の隠れ蓑として悪用されることも増えてきています。日々継続して新しくなるサイバー攻撃の手法に追従し、企業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。

[*1] https://www.nsslabs.com/company/news/press-releases/nss-labs-predicts-75-of-web-traffic-will-be-encrypted-by-2019/

社内ユーザーを保護するためには、企業は暗号化通信を含む全てのトラフィックを検査しなくてはなりません。その一方で、多くのセキュリティデバイスは暗号化トラフィックを検査できず、HTTPS通信を復号し検査できる数少ないデバイスも、急増するHTTPS通信量のペースに追いつく性能を持っておらず、企業の防御に深刻なギャップがあります。

HTTPS通信の高精度なWebフィルタリング

A10ネットワークスのSSLインサイトとデジタルアーツi-FILTERとの連携

A10ネットワークスは、HTTPS通信の高精度なWebフィルタリングを実現するために、デジタルアーツ社と提携しました。A10 Thunderシリーズによる SSLインサイトソリューションを利用することで、HTTPS通信を終端し高速に復号することが可能になります。復号したトラフィックをデジタルアーツ社の提供するWebフィルタリング製品であるi-FILTERで検査することで、HTTPS通信に対する高精度なWebフィルタリングが実現できます。

i-FILTERは、情報漏洩対策とWebの有効利用のための企業向けWebフィルタリング製品として、多くの企業で採用されており、業界最大級のWebフィルタリングデータベースと高度なフィルタリング技術により、不適切なWebサイトの閲覧を高精度で遮断することができ、情報漏洩を防ぐとともに、そのアクセス内容を記録・確認・保存することを可能にします。セキュリティ機関と連携した脅威情報サイトのデータベースも内包することで、情報窃取目的の通信も遮断します。また、同じデジタルアーツ社のメールセキュリティ製品であるm-FILTERと連携[*2]し、隔離された標的型メールなどに記述されたリンクへのアクセスをi-FILTER でブロックすることなども可能となり、標的型攻撃に対する包括的なソリューションを提供しています。

A10のSSLインサイトソリューションとi-FILTERとの連携ソリューションでは、A10 Thunderが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。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（図1）。i-FILTER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、i-FILTER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. 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i-FILTERに送信し、i-FILTERでHTTP/HTTPS通信のWebフィルタリングを実施

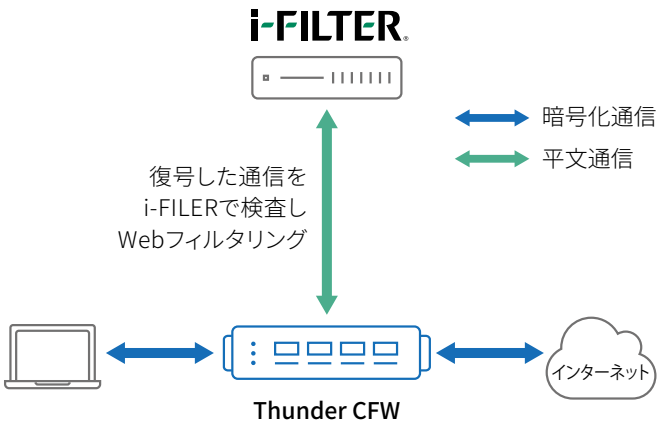

図1：Thunder CFWによるHTTPS通信の可視化とデジタルアーツi-FILTERとの連携

2. i-FILTERからHTTP/HTTPSリクエストの送信可否をICAPでThunderに通知。アクセスをブロックする場合はi-FILTERから転送されたブロック画面をThunderからクライアントに転送
3. HTTP/HTTPSリクエストの送信がi-FILTERに許可された場合、平文化されたHTTPSトラフィックを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

クライアントと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を防止できます。HTTPSトラフィックに含まれるリクエスト内容を平文でi-FILTERに渡すことで、HTTPS通信に対しても高度なWebフィルタリングを実現します。i-FILTERはHTTP 通信、HTTPS 通信のいずれにも対応したWebフィルタリングのデータベースを保持しており、通信に応じて最適なWebフィルタリングを実現します。

この構成でユーザー認証が必要な場合は、Thunderアプライアンスがプロキシサーバーとして動作しているため、ユーザー認証もThunder上で行う形を取ります。Thunderアプライアンス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i-FILTERに送信されるため、i-FILTER側でユーザーやクライアントIP、ユーザーグループに応じた個別の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より、複数のi-FILTERサーバーの利用も可能です。i-FILTERサーバーの障害時には、平文化された通信データを利用可能なi-FILTERサーバーに送信することができ、高可用性とスケーラビリティをともに実現できます。

[*2] i-FILTER Ver.10以上とm-FILTER Ver.5以上の組合せでのみ連携可能です。

FireEye NXやTrend Micro DDIとの連携による未知の脅威に対するセキュリティの強化

i-FILTERでは、近年増加するゼロデイ攻撃などの未知の脅威に対しての防御策として、FireEye社のサンドボックス製品であるNXシリーズやTrend Micro社のネットワーク可視化製品Deep Discovery Inspector（DDI）シリーズとも連携するソリューションを提供しています。この連携ソリューションを利用すると、FireEye NXやTrend Micro DDIで脅威を検知した際のWebサイト情報が動的にi-FILTERに通知され、そのサイトへのアクセスをi-FILTERでブロックできるようになります。ただし、FireEye NXやTrend Micro DDIはそのままではHTTPS通信を検査できないため、HTTPS通信に隠れた脅威の検知は困難な問題がありました。

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SSL/TLS通信を複数のデバイスに送信して検査することが可能なため、図2のように、復号し平文化されたHTTPS通信をFireEye NXやTrend Micro DDIにミラーポートを経由して渡すことで、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るようになります。この結果、特定サイトからのダウンロードなどでマルウェアなどの脅威が検知されれば、その情報が動的にi-FILTERと連携され、悪意のあるサイトへのアクセスを遮断することが出来るようになります。

これにより、HTTPS通信に対しても未知の脅威に対する防御を実現でき、更なるセキュリティの強化を実現できます。

特長とメリット

A10ネットワークスのThunderシリーズによるSSLインサイトソリューションとデジタルアーツi-FILTERの連携ソリューションのメリットは以下になります。

- 格段に優れたHTTPSコネクション数とスループット（最大40Gbps）
- 全てのポートに渡るHTTPSトラフィックの復号
- 業界最高水準のWebフィルタリング製品であるi-FILTERのデータベースを利用したHTTP/HTTPS通信のWebフィルタリングの実現
  i-FILTERやFireEye NX、Trend Micro DDIなどの複数セキュリティ製品への復号データの送信と負荷分散
- FireEye NX、Trend Micro DDIでのHTTPS通信の検査と脅威検知、および検知した脅威に基づくi-FILTERでの動的なWebフィルタリング
- 多様なネットワーク構成への対応

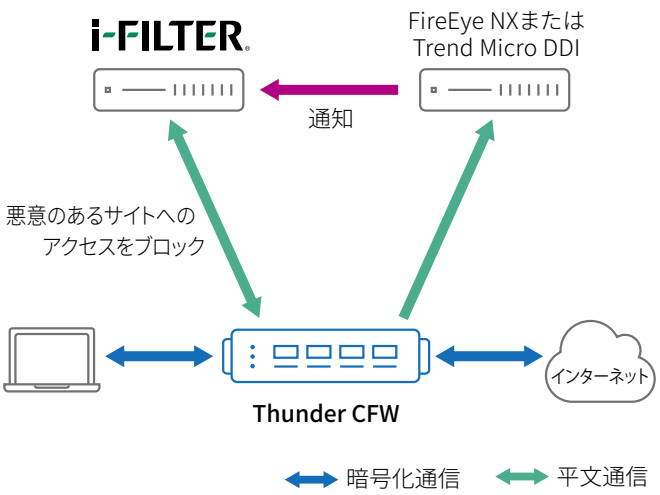

図2：FireEye NXやTrend Micro DDIと連携した動的な脅威サイトへのアクセスブロック

結論

転送中のデータを暗号化するWebアプリケーションが増えるにつれて、HTTPS通信が企業の防御にとって危険な盲点となりつつあります。高速なHTTPS通信の可視化を実現できるA10 Thunderシリーズを、カテゴリ数、登録件数そして精度ともに業界最高水準のWebフィルタリング製品であるデジタルアーツ社のi-FILTERと共に利用することで、HTTPS通信の高速・高精度なWebフィルタリングを実現し、有効な防御を提供できます。また、SSLインサイトで復号したデータをFireEye NXやTrend Micro DDIで検査することにより、HTTPS通信に含まれた未知の脅威を検出し、i-FILTERとの連携による動的なアクセス制限を実現することが可能になります。

デジタルアーツ株式会社について

デジタルアーツは、フィルタリング技術を核に、情報セキュリティ事業を展開する企業です。製品の企画・開発・販売・サポートまでを一貫して行い、国産初のWebフィルタリングソフトを市場に出したメーカーならではの付加価値を提供しています。また、フィルタリング製品の根幹を支える国内最大級のWebフィルタリングデータベースと、世界27の国と地域で特許を取得した技術力が高く評価されています。国内でトップシェアを誇るWebフィルタリングソフトとして、家庭及び個人向け「i-フィルター」・企業向け「i-FILTER」「i-FILTER ブラウザー & クラウド」を提供する他、企業向けとしてゲートウェイ型電子メールセキュリティソフト「m-FILTER」、クライアント型電子メール誤送信防止ソフト「m-FILTER MailAdviser」、セキュア・プロキシ・アプライアンス製品「D-SPA」、ファイル暗号化・追跡ソリューション「FinalCode」を提供しています。

http://www.daj.jp

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。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、世界各国の拠点からお客様をサポートしています。

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提供することを使命としています。

詳しくはホームページをご覧ください。
www.a10networks.co.jp
Facebook：http://www.facebook.com/A10networksjapan

A10ネットワークス株式会社
〒106-0032
東京都港区六本木三丁目2番1号
住友不動産六本木グランドタワー33階
TEL : 03-4520-5700
FAX: 03-4520-5701
jinfo@a10networks.com
www.a10networks.co.jp

海外拠点

北米（A10 Networks本社）
sales@a10networks.com
ヨーロッパ
emea_sales@a10networks.com
南米
latam_sales@a10networks.com
中国
china_sales@a10networks.com
香港
HongKong@a10networks.com
台湾
taiwan@a10networks.com
韓国
korea@a10networks.com
南アジア
SouthAsia@a10networks.com
オーストラリア/ニュージーランド
anz_sales@a10networks.com

お客様のビジネスを強化するA10のアプリケーションサービスゲートウェイ、Thunderの詳細は、A10ネットワークスのWebサイト**www.a10networks.co.jp**をご覧になるか、A10の営業担当者にご連絡ください。

Part Number: A10-SB_i-FILTER-JA-01
Mar 2018