# SSL通信の可視化とFireEye

## 暗号化による可視性とセキュリティの低下への対応

**課題：**

マルウェアや標的型攻撃のようなサイバー攻撃を阻止するためには、暗号化されたSSL通信を含む、あらゆる種類のトラフィックを検査しなければなりません。1024ビットから2048ビットSSL鍵への移行やSSL使用の拡大により、暗号化されたデータを復号/検査できる、強力で高性能なプラットフォームをが必要とされています。

**ソリューション：**

A10ネットワークスは、FireEyeと提携し、SSLトラフィックをインターセプトして高度な脅威分析を行うソリューションを提供しています。A10 Thunder CFWの機能であるSSLインターセプトは、FireEye脅威対策プラットフォーム（FireEye Threat Prevention Platform）による暗号化されたトラフィックの検査を実現し、CPUを集中的に使用する復号化処理の負荷を軽減します。

**利点：**

- SSLトラフィックの高速な復号化により、企業防衛における盲点を排除
- 進化した脅威を検出し、大きな犠牲をもたらすデータ漏えいや知的財産の損失を阻止
- 複数のFireEye脅威対策プラットフォームの負荷を分散して使用可能時間を最大化
- パフォーマンスと処理能力を拡張し、サイバー攻撃に効率的に対抗

攻撃者は、クライアントのコンピューターを危険にさらすマルウェアを利用して、脆弱なエンドユーザーに狙いを定めています。マルウェアに一度感染してしまうと、クライアントコンピューターはボットネットに知らない間に入ってしまいC&C（コマンドアンドコントロール）サーバーに情報を中継して、1台のコンピューターだけでなくネットワーク全体をスパイや侵入の脅威に露出させてしまう可能性もあります。

同時に、第三者が機密情報にアクセスすることを防ぐために、ますます多くのアプリケーションがデータを暗号化しています。Secure Sockets Layer（SSL）やその後継であるTransport Layer Security（TLS）のようなテクノロジーが、ネットや電子メールのトラフィックの安全を確保するために使われています。SSLはあらゆる場所で利用されています。つい先頃まで、主なWebサイトは、クレジットカード取引やユーザーログインなどの機密取引のみを暗号化していましたが、今日では、多くのWebアプリケーションは、あらゆるWebリクエストとレスポンスを、SSLを用いて暗号化しています。2014年1月時点で、実に100万の主要なWebサイトのうち、SSLを用いているWebサイトは前年と比較して48%増加しました。[1]

SSLの利用の拡大は、マルウェアやウイルス、フィッシング対象攻撃などの悪意あるコンテンツのトラフィック検査を行おうとした場合に問題となります。Webサイト、電子メールやファイル交換を保護する製品の多くは暗号化されたトラフィックの検査ができず、また増大し続けるSSL暗号化の要求に耐えられなくなっており、結果、企業防衛の盲点になっています。

ハイパフォーマンスセキュリティプラットフォームA10 Thunder® CFW（Convergent Firewall）は、負荷分散機能を拡張すると同時に、FireEye®インフラストラクチャーの弾力性を確保し、また暗号化されたトラフィックの可視化と、FireEye NXシリーズや、EXシリーズ、FXシリーズプラットフォームのようなセキュリティデバイスがすべてのトラフィックを検査して巧妙なサイバー攻撃を検出することを可能にします。

## SSL通信の可視化とFireEye

SSLインターセプト、あるいはSSLフォワードプロキシは、サーバーとクライアントの間で別々のSSLで保護されたセッションをもつ2つのSSL終端点で構成されるテクノロジーです。図1は、SSLインターセプトの機能を表しています。インライン構成での導入時は、以下のように動作します。

- クライアントとFireEyeアプライアンスの間に設置されているA10 Thunder CFWアプライアンスは、送信SSLトラフィックをインターセプトし、暗号化されていないトラフィックをFireEyeアプライアンスに送信
- FireEyeアプライアンスはトラフィックが高度な脅威にさらされていないか検査し、正統なトラフィックを転送
- FireEyeアプライアンスとインターネットの間に配置された第2のA10 Thunder CFWアプライアンスは、FireEyeアプライアンスからトラフィックを受け取ってデータを暗号化し、外部サーバーに送信

クライアントとサーバーの両方の観点から、統制された環境内で、クライアントネットワークでのみ復号化される端末相互間で暗号化されたセッションを用います。SSLによってできたセキュリティの盲点が排除されます。送受信されるネットワークトラフィックは適切に検査され、脅威は軽減されます。

内蔵のロードバランシング機能により、A10 Thunder CFWは高い可用性と拡張性を提供し、複数のFireEyeプラットフォーム導入を可能にします。そして、ソフトウェア、ハードウェア、またはネットワークに障害があった場合には、故障したデバイスをバイパスすることができます。十分な冗長性を確保するため、複数のA10 Thunder CFWをクライアントとFireEyeプラットフォーム間、またFireEyeプラットフォームと外部サーバー間にインストールすることも可能です。

[1] Netcraft、January 2014 Web Server Survey

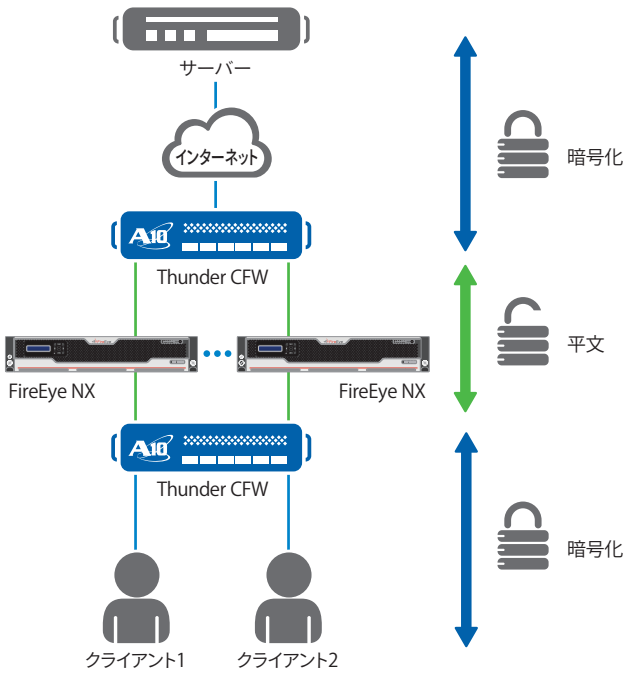


*図 1：Thunder CFW が SSL トラフィックの復号化と複数台の FireEye NX シリーズプラットフォームの負荷分散を実施*[2]

また、A10 Thunder CFW の提供する強力なアプリケーションデリバリーパーティション（ADP）機能を利用すると、複数の layer 3 virtual（L3V）パーティションを 1 台のアプライアンス上で構成し、ハードウェアを統合することが可能です。パーティションに区切られた A10 Thunder CFW は、1 台のハードウェアプラットフォーム上でトラフィックの復号化と再暗号化の両方を行うことが可能です。ADP 機能の活用により、企業はハードウェアと運用にかかる費用を軽減することができます。

## SSL 処理の課題

安全なセッションのセッティングや終了、多くのセッションを同時に暗号化と復号化する SSL の終端は、CPU に非常に大きな負荷がかかります。セキュリティの強化には、CPU 能力の増強が求められます。

暗号化の強度は SSL 鍵長によってある程度決まります。2048 ビット鍵 SSL 証明書には、1024 ビット鍵証明書と比べて、暗号化には約 3.4 倍多く、復号化には約 6.3 倍多くの処理能力が必要とされます。4096 ビット鍵証明書には、1024 ビット鍵証明書と比べ、およそ 25 倍多くの処理能力が必要とされます。

アメリカ国立標準技術研究所（NIST）の SP800-131A によって促進された、1024 ビットから 2048 ビット鍵長への移行は、SSL トラフィックの暗号化・復号化を行うデバイスに負荷を与えています。最低限の鍵長以上の SSL 証明書によってセキュリティ強化を行う場合、サーバーやロードバランサーの劇的なパフォーマンス向上が求められます。従って、SSL トラフィックをインターセプトしたり、検査するために用いるデバイスには、多くの SSL の毎秒のコネクション数（CPS）を確立するため、また拡張された鍵長の SSL 鍵を取り扱うために、複数のセッションを同時に行うことのできるコンピューター処理能力が必要です。

## SSL 高速化ハードウェアを搭載した A10 Thunder CFW

安全なコネクションのセットアップは、SSL コネクションを確立する際に最も CPU の処理能力を必要とする部分です。セッションにおけるバルクデータの暗号化と復号化は CPU 負荷が大きいですが、程度はそれほど高くありません。A10 Thunder CFW は、複数の安全なコネクションの同時管理に最適です。A10 ネットワークスは、ADC（アプリケーションデリバリーコントローラー）として SSL インターセプト機能を初めて提供したメーカーであり、パワフルで豊富な機能を持つ A10 Thunder CFW プラットフォームとともに、非常に優れた SSL コネクションレートを提供しています。A10 Thunder CFW は 64 ビットの Advanced Core Operating System（ACOS®）上に構築されているため、拡張性に優れています。また、アプリケーションとトラフィックの高速化を行うハードウェアによって最高のパフォーマンスを実現します。すべてのモデルは強力な CPU を搭載しており、SSL の負荷軽減をサポートします。また、多くのモデルでは、幅広い高パフォーマンスと、多くの SSL セッションを同時に管理するために最適な複数のチップを搭載した SSL 高速化モジュールを搭載しています。

従来の CPU リソースを使用して SSL 接続を確立する場合、SSL の鍵長が増えるとパフォーマンスが大幅に低下します。新しい SSL 高速化ハードウェアを備えた A10 Thunder CFW は、1024 ビットと 2048 ビットの鍵長でほぼ同等のパフォーマンスを提供し、本番環境で 4096 ビット鍵を高速処理することのできる非常に強力なパワーを有しています。

A10 の ACOS が持つ幅広い機能により、A10 Thunder CFW のお客様は、インターセプトしてセッションを確保するものと、そのまま暗号化しておくものとをコントロールできます。

ハイパフォーマンスセキュリティプラットフォームの A10 Thunder CFW 製品ラインは、お客様のアプリケーションに、高可用性、加速性、安全性を提供します。更なるメリットとして、すべての機能とパフォーマンスは、追加ライセンスの購入なしで利用可能です。

## FireEye 脅威対策プラットフォーム

FireEye 脅威対策プラットフォームには、すべての FireEye アプライアンスとクラウドベース製品が含まれます。今日の進化したサイバー攻撃に対処する、ネットワーク、電子メール、コンテンツ、モバイル、フォレンジック、およびエンドポイントソリューションが含まれます。FireEye 脅威対策プラットフォームは、特許取得済の実績がある Multi-Vector Virtual Execution™（MVX）テクノロジーによりリアルタイム検出と進化した脅威対策を実現しています。

MVX エンジンは、信頼性の低い Web オブジェクトや電子メール添付ファイル、コンテンツファイルやモバイルアプリを機器化された仮想マシン環境の中で実行することで、ゼロデイ攻撃や APT 攻撃を捕獲・確認します。MVX エンジンは、拡張性と正確でタイムリーな保護を、主要な攻撃ベクター（インターネット、電子メール、モバイル）に提供するように設計されています。そして、素早いイベント優先付けとインシデント対応を可能にする実行可能な脅威インテリジェンスも提供しています。

[2] アプリケーションデリバリーパーティション（ADP）機能により、1 台の A10 Thunder CFW アプライアンス上に復号化と再暗号化機能をホスティングすることが可能

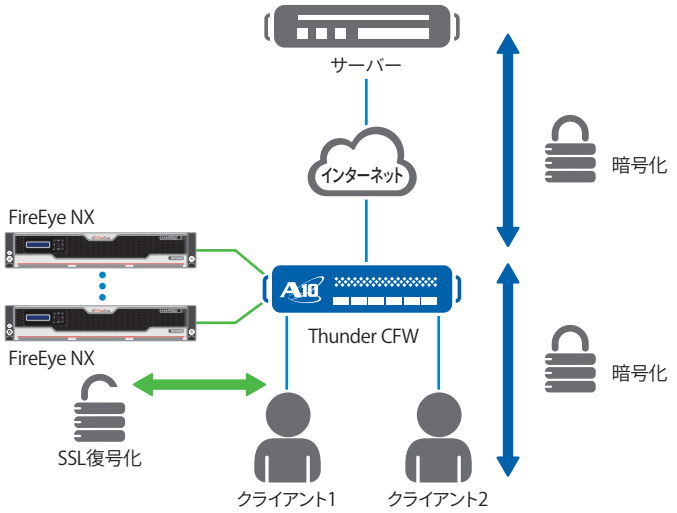


*図2：パッシブモードで導入された FireEye 脅威対策プラットフォーム*

FireEye プラットフォームは、パッシブモードで構成することもできます（図2）。復号化されたトラフィックは FireEye デバイスに複製されるため、トラフィックを検査し、必要に応じて攻撃を軽減することができます。パッシブモードでは、FireEye デバイスは、本番環境のネットワークに中断なく容易に統合することが可能です。この導入モデルでは、FireEye 脅威対策プラットフォームは、ネットワークトラフィックフローを使用せず、ネットワーク影響を与えないため、評価段階に最適です。

## 結論

SSL インターセプト機能を備えた A10 Thunder CFW は、FireEye 脅威対策プラットフォームとの組み合わせにより、ネットワークの防御戦略を目指す企業にとって優れたソリューションを提供します。大量のトラフィックが検査できていない場合は、企業防衛に危険な盲点が発生している可能性があります。FireEye の脅威対策プラットフォームは検証され、A10 Thunder CFW との組み合わせで機能することが証明されています。SSL インターセプトによって、以下のことが可能です。

- A10 の 64 ビット Advanced Core Operating System（ACOS）と専用セキュリティプロセッサーによる、パフォーマンス、可用性、拡張性の最大化
- 暗号化データを含むすべてのネットワークデータの分析と、徹底した脅威対策の実施
- 業界最高レベルのコンテンツ検査ソリューションによる、サイバー攻撃の回避

A10 は非常に強力な SSL オフロードソリューションを提供し以下のことを実現します。

- 2048 ビットおよび 4096 ビット鍵を含む、SSL 使用の拡大と高まる暗号化基準に対する投資を将来にわたって保証
- セキュリティアプライアンスの追加購入の必要なく高速な SSL 復号化を実現し、設備投資を軽減。A10 Thunder CFW はトラフィックを復号化して、FireEye 脅威対策プラットフォームだけでなく、データ漏えい防止デバイス、ネットワークファイアウォールや、URL コンテンツフィルタリング製品をはじめとした複数の検査デバイスに送信することで、復号化とセキュリティの中心的な機能を提供
- 企業防衛における盲点の排除。A10 Thunder CFW では、CPU のパフォーマンスとハードウェアによる高速化処理に幅広いオプションが提供されるため、環境に合わせて最適なモデルを選択できます。A10 Thunder CFW は重要なサービスの提供、ラックスペースを最大活用、消費電力の軽減を実現

## FireEye について

FireEye® は、次世代のサイバー攻撃から、世界中の民間企業や官公庁をリアルタイムで防御するために専用設計された、仮想マシンベースのセキュリティ・プラットフォームを発明した企業です。高度なサイバー攻撃は、次世代ファイアウォールや IPS、アンチウイルス、各種ゲートウェイなど、シグネチャベースのセキュリティ対策を容易にすり抜けてしまいます。FireEye® 脅威対策プラットフォーム™ は、攻撃ライフサイクル全体で、モバイル、Web、電子メール、ファイル・システムといった主要な攻撃経路にわたり、シグネチャを利用しないリアルタイムでダイナミックな脅威防御策を組織へ提供します。FireEye プラットフォームの核となる仮想実行エンジンは、FireEye Threat Intelligence によって補完されており、サイバー攻撃をリアルタイムに検出・防御することができます。FireEye のソリューションは、「Forbes Global 2000」企業の 730 社を含む、世界 67 か国以上の 4,700 を超える組織で利用されています。

## A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はアプリケーションネットワーキングおよびセキュリティ分野におけるリーダーとして、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ご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**
〒105-0001
東京都港区虎ノ門 4-3-20
神谷町MTビル 16階
TEL : 03-5777-1995
FAX: 03-5777-1997
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-19112-JA-01
June 2016