6つの鍵

SSLの盲点を排除する6つの鍵

SSLトラフィックの検査に必要な要件

この瞬間にも悪質なトラフィックが御社のシステムにアクセスしているかもしれません

SSLの利用頻度は毎年高まっており、**2016年までにインターネットトラフィックの67%が暗号化されると予測されています**[1]。残念ながら、暗号化を活用しているのはセキュリティ意識の高い組織やユーザーだけではありません。ハッカーも悪事を隠すために暗号化を利用しています。また、ファイアウォールや脅威防止ソリューションの多くはSSLを復号化する機能を備えていますが、進化する復号化の要求には追いつくことができない状況です。

ハッカーが暗号化によって防御を通過できた場合、攻撃対象の組織ではダウンタイムが発生し、売上が減少し、顧客の反感を買い、知的財産を失います。さらにはデータ侵害の修復や信頼回復のため多額の費用が発生します。

SSL検査を導入しなければ、組織は攻撃のリスクにさらされるという厳しい現実に直面します。暗号化されたトラフィックを隠れ蓑にしたハッカーは、ネットワークに侵入してマルウェアをインストール、複数のエンドポイントでデータを盗み出すことができるのです。

暗号化された悪質なトラフィックに対する最善の防御策は、次に紹介する6つの重要な要件を満たすSSL検査プラットフォームの導入です。

1. 出典：Sandvine Global Internet Phenomena Spotlight: Encrypted Internet Traffic report, 2015年5月

ハッカーの侵入を阻止する
6つの鍵

SSL検査製品のベンダーを評価する際に特に重視しなければならないのは、パフォーマンス、
コンプライアンス、可用性、セキュリティです。効果的なSSL検査プラットフォームは、
次に紹介するすべての機能を備えている必要があります。

01.

SSLパフォーマンスの要求を満たすこと

新しいソリューションを導入するときは常に**パフォーマンスが重視されますが、増加し続ける負荷に対応する必要がある**ソリューションの場合は特に重要です。SSL検査のパフォーマンスが現在と将来両方のニーズを満たすことを確認するためには、次のことを行う必要があります。

- 2048ビットおよび4096ビットSSL鍵を使用した、SSL検査時のスピード測定
- Diffie-Hellmanや楕円曲線暗号の混在するトラフィックの評価
- SSL検査プラットフォームが、トラフィックのピーク時でも余裕を持ってスループット要件に対応できることの確認

02.

コンプライアンスの要求事項への対応

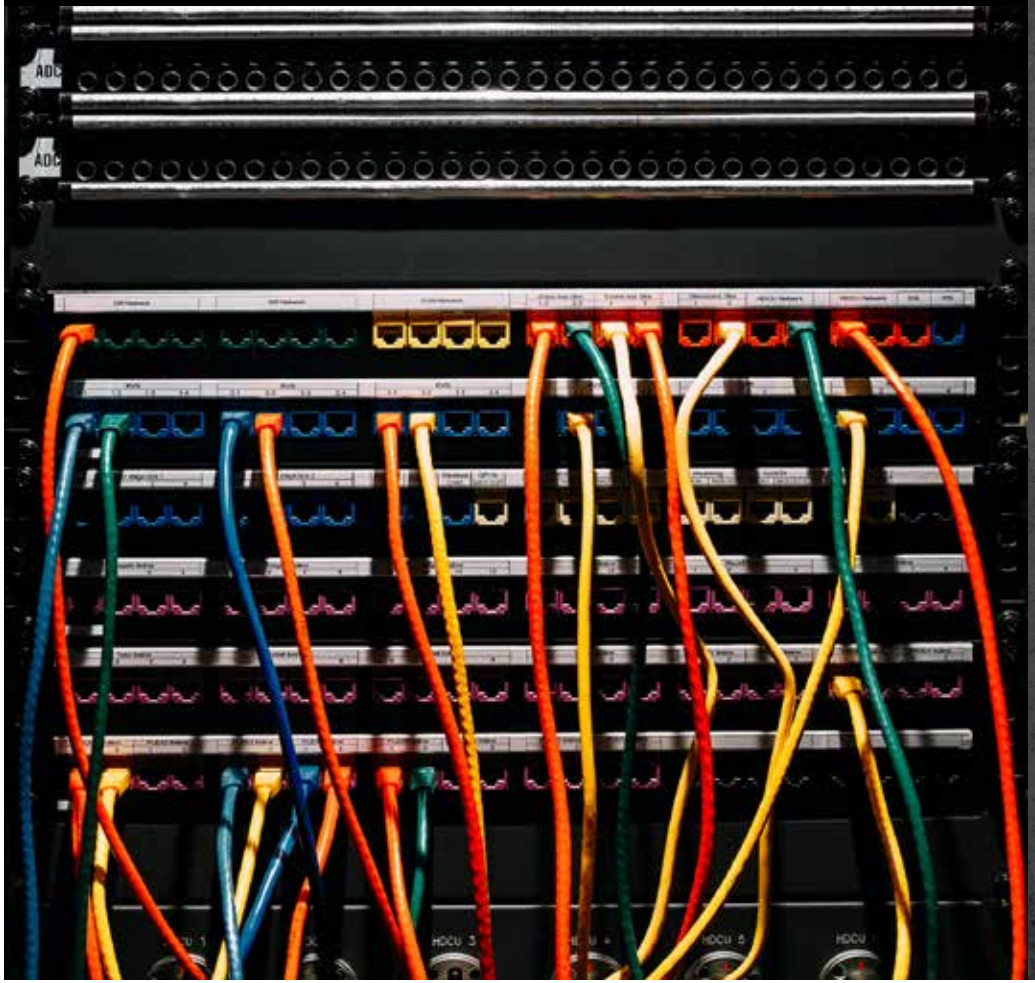
HIPAA、SOX、ECPA（電気通信におけるプライバシー保護法）など、データのプライバシー保護のための法規制が世界各地で制定されているため、**現在企業はさまざまなコンプライアンス基準に対応する作業に追われています。**こうした法規制を順守するため、金融、医療業界などの多くの企業は機密性の高いデータを保護しなければなりません。

SSLトラフィックを検査しながらコンプライアンスを維持するため、ITセキュリティチームは次のことが可能なプラットフォームを探す必要があります。

- タイプごとにWebトラフィックを分類し、医療サイトや銀行サイトに送信される通信などの機密データは暗号化された状態で維持
- 自動更新されるURLバイパスリストと手動で定義するURLバイパスリストのサポート

03.

複雑な導入要件のサポート



すべてのセキュリティ基盤をサポートするため、大半の組織は複数のベンダーが提供するさまざまセキュリティデバイスを導入しています。

SSL検査プラットフォームは、これらすべてのデバイスが利用できるようにトラフィックを復号化できなければなりません。そのためには、次の機能を備えている必要があります。

- インターネットへのアウトバウンドトラフィックと企業サーバーへのインバウンドトラフィックの復号化
- 高度なトラフィックステアリングを通じて、複数のセキュリティデバイスへのインテリジェントなトラフィックのルーティング
- 主要ベンダーのさまざまなセキュリティソリューションとの統合

04.

セキュリティインフラストラクチャーのアップタイムとキャパシティの最大化

セキュリティインフラストラクチャーは、常に稼働してサイバー攻撃をブロックし、データの盗難を阻止しなければなりません。セキュリティインフラストラクチャーに障害が発生すれば、脅威が検出されず、結果として破壊的な攻撃が発生して収益が減少し、ブランドイメージに影響が及ぶ可能性があります。**優れたSSL検査プラットフォームは、既存のセキュリティインフラストラクチャーのアップタイムを最大限に高め、リスクを低減できるはずです。**次のような機能を備えたプラットフォームを探すようにしてください。

- 負荷分散によるセキュリティ環境の拡張
- 障害が発生したセキュリティデバイスを検知してルーティングを迂回することによる、ネットワークのダウンタイム回避
- 高度なモニタリングをサポートし、ネットワークやアプリケーションのエラーのすばやい特定

05.

SSL証明書と鍵の安全な管理

SSL証明書および鍵は、暗号化通信の信頼性の基盤になります。証明書や鍵のセキュリティが低下すると、攻撃者はこうした証明書や鍵を悪用してデータを盗み出す場合があります。アウトバウンドおよびインバウンド両方のSSLトラフィックを可視化するために、**SSL検査プラットフォームは数十、数百、あるいは数千の証明書と鍵を管理できなければなりません。**効果的なSSL検査プラットフォームは、次の機能を備えている必要があります。

- SSL検査プラットフォームに保管されている SSL鍵の保護
- 証明書の検出および制御機能を装備するサードパーティのSSL証明書管理ソリューションとの統合
- FIPS 140-2 Level 2およびLevel 3の鍵管理のサポート

06.

すべての標準に準拠した暗号化トラフィックの復号化

暗号化されたトラフィックの量が増加する一方で、組織と攻撃者が利用する暗号化技術のレベルもますます高度化しています。**悪質な人物から保護するため、4096ビットSSL鍵、楕円曲線暗号、Perfect Forward Secrecy（PFS）などの技術が導入され始めています。**こうした技術の進歩に遅れを取らないように、SSL検査プラットフォームは次の機能を備えている必要があります。

- 4096ビットSSL鍵長と高度なSSLおよびTLS暗号化のサポート
- SSLへの再暗号化を含むすべてのデータの復号化
- トラフィックを復号化できない場合は管理者に通知

企業にとって、悪質な暗号化トラフィックに対する最善の防御は、これら6つの重要な基準を満たすSSL検査プラットフォームを導入することです。これらの要件を満たさないシステムを利用していると、組織がリスクにさらされ、脅威に侵入されてしまう可能性があります。

A10ネットワークスのアプリケーションデリバリーコントローラーThunder ® ADC製品ラインの提供するSSLインサイト機能を利用すれば、暗号化されたデータを含むすべてのネットワークデータを分析し、組織を脅威から完全に保護することができます。

A10のSSLインサイトによって、次のことが可能です。

- SSLトラフィックの復号化を高速で行うことによる、企業防衛における**盲点の排除**
- 複数のサードパーティーセキュリティアプライアンスの負荷を分散し、**アップタイムを最大化**
- サイバー攻撃に効率的に対抗するため**パフォーマンスと処理能力を拡張**
- 高度な脅威を検出し、**犠牲の大きいデータ漏えいや知的財産の損失を阻止**

十分なSSL検査を行えなければ、攻撃の次の犠牲者は御社になるかもしれません

暗号化されたトラフィックの脅威を検知し、重要なデータとシステムを保護するA10 Thunder ADCの詳細は、**www.a10networks.co.jp/ssl-insight** をご覧になるか、**営業窓口**までお問い合わせください。

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。

URL：http://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
brazil@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-EB-14101-JA-01　JAN 2016