A10 は SSL 可視化市場 3 年連続シェア No1！※

SSL に潜む脅威を可視化する

サイバー攻撃の約半数は暗号化通信にその身を隠しています

SSL/TLS の利用の拡大につれて、攻撃者が自身の攻撃を暗号化通信に隠して企業に侵入する「SSL/TLS に潜む脅威」も顕著化してきました。攻撃は暗号化され、セキュリティ装置で検知されません。そのため企業では、セキュリティ装置に検査する前に、暗号化通信を復号して可視化することが必要になります。

さらに、働き方改革やデジタルトランスフォーメーションの推進により Office 365 や G Suite などのクラウドサービスの利用も増え、無料 / 個人アカウントの利用による情報漏洩等のセキュリティリスクなども懸念されます。

SSL/TLS 時代における課題

約半数の攻撃は暗号化通信に隠れていた

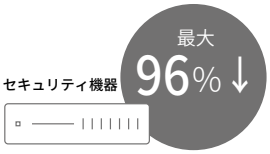
サイバー攻撃に遭った企業は 80% あり、そのうち 41% は攻撃が暗号化通信に潜んでいた [*1]

暗号化通信に隠れた攻撃だった割合

SSL/TLS 暗号化通信に潜む攻撃の実情

セキュリティ機器は SSL 処理に適していない

高い負荷がかかる SSL 処理により、最大 96% の性能ダウン



セキュリティ機器で SSL 暗号化 / 復号を行った場合のパフォーマンス

SSL/TLS 処理性能の実情

*1 https://www.a10networks.co.jp/news/press/cybersecurity-report.html ※ Source: ITR「ITR Market View：サイバー・セキュリティ対策市場 2019」SSL 可視化市場：ベンダー別売上金額シェア (2016 ～ 2018 年度予測)

A10 のソリューション：SSL/TLS を高速に可視化！

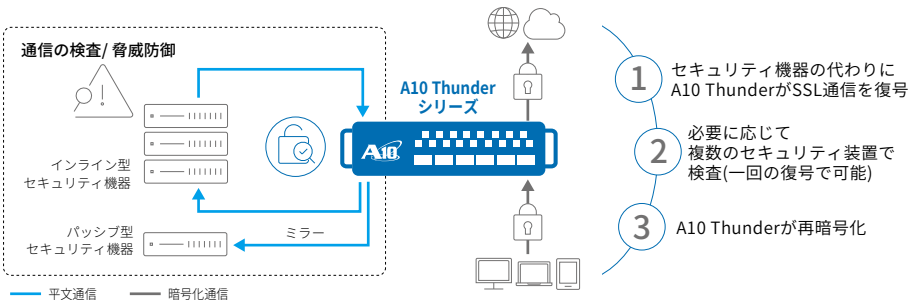
セキュリティ強化

導入済のセキュリティ機器をそのまま利用して SSL/TLS トラフィックをもれなく検査

A10 Thunder CFW の SSL インサイト（SSL 可視化）は、組織内のクライアントから外部サイト宛ての SSL 通信内容を復号することで可視化し、セキュリティ製品に転送、再度暗号化して外部に転送することで SSL に隠れた脅威の検知を支援する機能です。
A10 Thunder シリーズは、SSL/TLS 処理専用ハードウェアを搭載し (* 一部モデルを除く) 高速な暗号化 / 復号処理を実現。さらに CPU の性能を最大限引き出すことに成功した A10 の独自 OS ACOS (Advanced Core Operating System) により、セキュリティ機器の性能を最大化して、効率良く暗号化通信のセキュリティチェックを行うことができます。

SSL インサイトにおいて動作確認済みのセキュリティ製品一覧

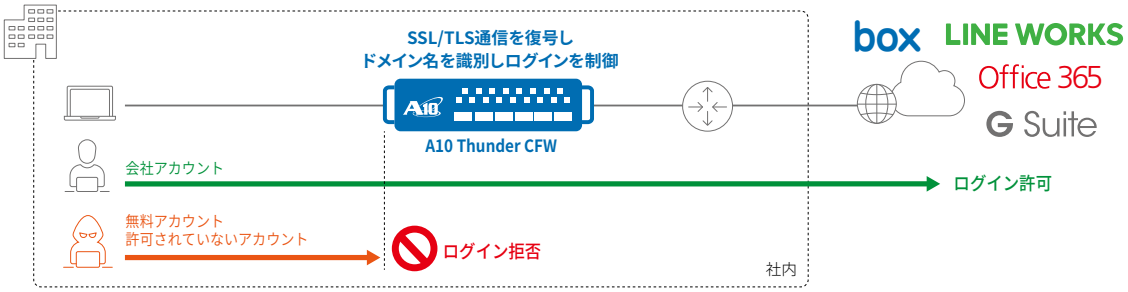
- デジタルアーツ i-FILTER
- FireEye NX シリーズ
- トレンドマイクロ Deep Discovery Inspector
- SonicWall Super Massive
- Cisco FirePower
- RSA Security Analytics
- Juniper JATP
- Palo Alto PA シリーズ
- ALSI InterSafe WebFilter



シャドー IT 対策

自社内からクラウドサービスへの個人 / 無料アカウントでのアクセスを禁止

A10 Thunder CFW をプロキシとして導入、社内からクラウドサービスへのアクセス時に A10 Thunder CFW の SSL 可視化（SSL インサイト）機能で暗号化されたログイン情報を可視化することにより、個人や無料アカウントでのクラウドサービスへのログインをブロックし、情報漏洩を防止します。
宛先ドメイン名を識別して通信を振り分けることも可能なため、クラウドサービス利用時に増大する既存プロキシの負荷を軽減することも可能です。



A10のSSLインサイト（SSL復号）を選ぶ理由

連携可能なセキュリティ製品が豊富

A10は日本国内においても、あらゆる主要セキュリティベンダーと密に連携しています。

情報交換や連携に関する検証を行っており、技術的ノウハウや資料が蓄積されています。

要件に合わせた柔軟な構成が可能

Thunder シリーズは、L2/L3両方に対応しているほか、一度の復号処理で複数のセキュリティデバイスによる検査が可能、また、URLカテゴリベースで可視化をバイパスするなど、お客様の既存の環境に合わせた柔軟な構成に対応します。

圧倒的なコストパフォーマンス

SSL可視化機能をもつ他社製品と比較し、約1/2の価格（※同等レベルのSSL復号スループットを持つ製品との比較）

更にThunder シリーズなら、追加ライセンスなしでクラウドへの通信最適化機能も利用可能です。

他社製品に対する強み

A10は、柔軟な構成と優れた運用性、セキュリティ機能などの様々な付加価値をオールインワンで提供します。

機能	A10	B社	備考
パフォーマンス	◎		A10は、最大40GbpsのSSL処理性能
可視化対象デバイスの負荷分散機能	○	×	A10は、デフォルトで可視化対象デバイスの負荷分散とヘルスチェックが可能。 可視化対象デバイスのスケールアウト構成が可能
SSHプロトコルの可視化	○	×	A10は、SSH、SCP、sFTPの可視化可能
プロキシ連携	○	×	A10は、背後にプロキシのある構成をサポート
HSM連携	○	×	A10は、FIPS 140-2 Level 3に準拠しHSMデバイスと連携可能
スクリプトによるトラフィック制御	○	×	A10は、TCLベースのaFlexスクリプトをサポートし、 可視化後のHTTPトラフィックのエンジニアリングが可能
送信元MACアドレスが セキュリティデバイスになる構成	○	×	A10は、再暗号化時に、送信元MACに依存せず動作可能。 セキュリティデバイスがL3構成、SNATを行う場合も動作可能
完全なTCPスタックの実装と管理機能	○	×	A10は、L7レベルでSSLトラフィックをプロキシとして終端可能。 完全なTCPスタックをサポートし、ストリームを制御可能
SSL Retransmit	○	×	A10は、SSL Retransmitサポート
明示型プロキシ機能	○	×	A10は、明示型プロキシ機能とSSL可視化を併用可能
ICAP連携	○	×	A10は、ICAP連携とSSL可視化を併用可能
L2/L3ネットワーク構成	○	L2のみ	A10は、L2、L3の両方の構成をサポート（可視化対象のセキュリティデバイスもL2、L3の両方の構成をサポート） Passiveモード（TAPモード）のデバイスへの可視化もサポート
冗長化機能	○	×	A10は、Active-Standby冗長化機能サポート（VRRP-A） L2構成時も単独でL2ループ防止機能を実装。

LEARN MORE

ABOUT THE 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

Part Number: A10-SSL Insight SEP 2019