ソリューションブリーフ

自治体情報セキュリティ対策向けソリューション

インターネット通信の監視とインシデントの予防

新たな自治体情報セキュリティ対策の要件とA10 ネットワークスのソリューション

自治体の情報資産を保護するためのセキュリティとして、自治体の内部ではインターネット接続セグメント・LG-WAN 接続セグメント・マイナンバー接続セグメントの三層分離による対策、インターネット向けのアクセスや自治体の Web サーバのセキュリティには自治体セキュリティクラウドの整備による対策がこれまで取られてきましたが、近年のサイバー攻撃の増加や新たな脅威に対応するために新たなセキュリティ対策が必要とされています。それに合わせて自治体向けのセキュリティガイドラインの見直しが行われており、セキュリティ専門人材による監視機能の強化、近年増加する HTTPS 通信を始めとする SSL/TLS による暗号化通信に対する監視機能や、災害時の Web サーバへのアクセス集中を想定した負荷分散の機能、自治体事務の効率化に資するメールやファイルの無害化機能などが新たな要件として挙げられています。主にネットワークレベルで自治体情報セキュリティ対策に求められる要件には、以下の 3 点があります。

- インターネット通信に対する通信の監視
- 暗号化通信の復号対策とセキュリティ
- Webサーバに対するセキュリティ

また、上記に加え、今後自治体においてクラウドサービスの活用による業務効率化も求められています。クラウドサービスを快適に利用して活用するためには、そのトラフィック特性に合わせたネットワーク構成が必要となります。

A10 ネットワークスの Thunder CFW シリーズが持つ機能を利用すると、以下のようにこれらの要件に対応できます。

- プロキシサーバ機能によるインターネット通信監視とクラウドサービス向けトラフィックの最適化
- SSL/TLS可視化機能（SSLインサイトソリューション）による暗号化通信の復号対策とセキュリティ強化
- アプリケーションデリバリコントローラ（ADC）機能によるWebサーバに対するセキュリティ強化

次節からは、この 3 つのソリューションの詳細を示します。

プロキシサーバ機能によるインターネット通信監視とクラウドサービス向けトラフィックの最適化

A10 Thunder CFW はプロキシサーバの機能を有しており、アクセス管理とアクセス制御、アクセスログの取得、各種セキュリティ機能を用いることで、自治体内からのインターネットアクセスの監視とセキュリティ強化に利用できます。大規模な通信セッションを処理できる高い性能を持ち、コストパフォーマンスに優れます。Active Directoryなどを始めとした各種認証基盤と連携でき、ユーザーやグループを指定してのアクセス制御を行うことができます。インターネットへのアクセスログを記録でき、後述する SSL/TLS 通信可視化の機能を併せて利用することで、URL に含まれるサブディレクトリも含めたより詳細なログの取得を行うことができます。

動的にアップデートされる情報に基づいた URL カテゴリフィルタリングや脅威インテリジェンスによるセキュリティにより、不正サーバへのアクセスや悪意のあるアクセスを防ぐこともできます。ファイアウォールの機能を統合しており、レイヤ 4 でのステートフルファイアウォールによる不正通信への防御やアプリケーション識別を利用してのアプリケーションの可視化と通信制御を行うこともできます。IaaS や各拠点、クライアントとの IPsec-VPN 接続による暗号化通信も可能です。上位プロキシへのプロキシチェインもできます。

また、近年自治体で必要とされているクラウドサービスの活用のための、クラウドサービス向けのトラフィック最適化の機能も有しています。

一般に Microsoft 365 などのグループウェアを始めとするクラウドサービスを利用すると大規模な通信セッションとインターネット向けトラフィックが生じ、プロキシサーバやファイアウォールを始めとする既存のセキュリティ機器やインターネット回線・WAN 回線などがひっ迫

課題：

- 自治体の情報セキュリティ対策とクラウドサービス活用の両立
- インターネット通信に対する通信の監視
- 暗号化通信の復号対応とセキュリティ
- Webサーバに対するセキュリティ

解決策：

- A10 Thunder CFWシリーズの利用による多様なセキュリティ要件への対応
- プロキシサーバ機能の利用によるインターネット向け通信のアクセス制御とアクセスログの取得、およびクラウドサービス向け通信のトラフィック振り分けによる通信ボトルネックの回避
- 高速なSSL/TLS通信の復号と多様なセキュリティ機器との連携による高度なセキュリティ対策の実現
- リバースプロキシ・ファイアウォール・WAF・広域負荷分散の機能によるWebサービスの可用性とセキュリティの強化

メリット：

- プロキシサーバ・SSL/TLS通信可視化・Webサービス向け機能のオールインワンライセンスによる提供
- クラウドサービス活用により生じる大規模な通信を高速に処理可能なアーキテクチャ
- URLフィルタやコンテンツ無害化・マルウェアスキャン製品、次世代ファイアウォールやIPS/IDS、標的型攻撃防御製品やフォレンジック製品などの多様なセキュリティ機器と連携ができ、高速・低遅延な処理が可能なSSL/TLS通信の可視化機能

します。クラウドサービス自体は基本的にドメイン名で規定されており、コンテンツ配信ネットワークなどを利用していることからIPアドレスが頻繁に更新され、トラフィックの制御を既存のルーティングで行うことは困難です。

A10 Thunder CFWのプロキシサーバ機能を利用することで、ドメイン名に基づく通信トラフィックの制御が可能になります。これにより、クラウドサービス活用のボトルネックとなりやすい既存のプロキシサーバなどをバイパスしたり、クラウドサービス向けトラフィックを増設した通信回線に適切に分散させたりするなどの処理が容易になり、少ない運用コストで快適なクラウドサービスの活用が実現されます。また、通常のWebアクセスに関してはこれまで通りプロキシサーバにチェインしたりその他のセキュリティ機器に向けたりするなどの柔軟な処理が可能です。

SSL/TLS通信の可視化による暗号化通信の復号対策

A10 Thunder CFWは、クライアントとインターネット間のHTTPS通信を始めとするSSL/TLS通信を高速に復号しセキュリティ機器での検査を実現するSSL/TLS通信可視化（SSLインサイト）の機能を有します。セキュリティ機器での検査を行った通信データは再度SSL/TLSにより暗号化され、目的のアドレスに転送されます。復号し平文化したデータは、ファイアウォール・UTM・IPSのようなインライン型のセキュリティ機器、標的型攻撃対策製品・IDS・フォレンジック製品のようなパッシブ型のセキュリティ機器、URLフィルタ・アンチウィルス・データ損失防止・コンテンツ無害化のようなICAPを通じて利用できるセキュリティ機器との連携を行うことができます。A10のSSLインサイトソリューションは格段に優れたSSL/TLS通信の処理能力とスループットを持ち、既存のセキュリティ機器の性能を十分に発揮させることが可能です。一度復号した通信を複数の機器で検査できることからSSL/TLS通信の復号と再暗号化に伴う通信遅延は最小に抑えられます。前述したフォワードプロキシ機能と併せて利用できたり、L2/L3での導入が柔軟に選択できたりするなど、多様なネットワーク構成に合わせた導入ができます。

SSL/TLS復号を行うことで、前述したように詳細なアクセスログを取得しネットワーク監視の能力を強化できるだけでなく、自治体セキュリティに求められる、暗号化通信に対するURLフィルタリングの強化やマルウェア対策の強化や、ファイル等のコンテンツを無害化する対策の実現が可能となります。また、IPS/IDSや標的型攻撃対策製品との連携により、エンドポイントセキュリティだけでは捉えられない通信の振る舞いを検知し、暗号化通信に隠れた攻撃を検知し防御するだけでなく、フォレンジック製品との連携によって、自治体内部への高度な侵入を詳細に追跡できるようになります。

上記に加え、SSLインサイトの機能を使うことで、クラウドサービスを利用するアカウントの制御も可能になります。自治体内部から許可されていないドメインやアカウントでのクラウドサービス利用を制限することができ、情報資産の外部アカウントへの漏洩を防ぐことができます。

ADC機能によるWebサーバセキュリティ

A10 Thunder CFWの持つADC機能を利用することで、サーバ負荷分散によりWebサーバなどのアプリケーションサーバの可用性を高めると共に、高速なアプリケーション配信やWebアプリケーションに対するセキュリティの強化を実現できます。A10 Thunderシリーズは独自のアーキテクチャを採用することにより高い通信処理能力を有し、TCP通信の最適化やコンテンツキャッシング、SSL/TLSのオフロードにより、高速なWebアプリケーションの配信を可能にします。また、サーバ負荷分散とともに広域負荷分散の機能を有し、オンプレミスのWebサーバへの負荷が集中したり、サーバがダウンしたりした場合にクラウド（IaaS）上のサーバに自動的に負荷分散したり切り替えたりすることができます。

また、A10 Thunder CFWにはWebアプリケーションファイアウォール（WAF）の機能や、前述したL4ファイアウォールの機能、DDoS攻撃防御の機能が統合されており、Webサーバに対する高度なセキュリティを提供します。認証基盤と連携することでWebサーバへのアクセスに対する認証・認可を行うこともできます。これらの機能を活用することで、自治体のWebサービスに求められる多様なセキュリティ要件を満たせます。

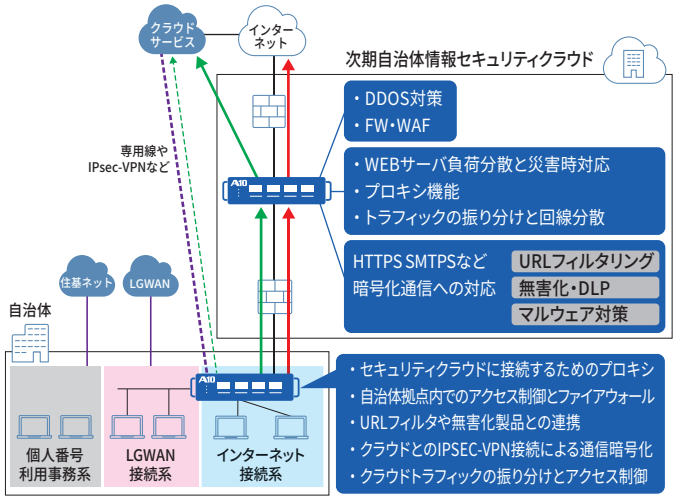

図1：自治体セキュリティにおけるA10 Thunder CFWのユースケース

まとめ

ここまで述べてきたA10 Thunder CFWを自治体のセキュリティに活用する場合の一連のユースケースについて、図1に示します。図1にあるように、自治体の各拠点、および自治体セキュリティクラウドにおいて多様な機能を利用でき、様々な要件を満たすことが可能です。A10 Thunder CFWには多くの機能が統合されており、プロキシサーバ機能・SSL/TLS可視化機能・ADC機能がオールインワンライセンスで提供されています（URLクラシフィケーションや脅威インテリジェンス、アプリケーションファイアウォール機能には筐体単位での追加ライセンスが必要です）。内部を論理分割して利用することができるため、多様な利用シーンに対応できます。前述したようにクラウドサービスの活用に適した機能も有していることから、自治体セキュリティの強化だけでなく、クラウドサービス活用による業務の効率化にも寄与します。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）は、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_Solutions_for_Local_Government　Feb 2021