SSL/TLS 通信を含む通信のネットワークフォレンジックの実現

三菱スペース・ソフトウエアの Dynamic MSIESER と A10 の SSL インサイトソリューションの連携

課題：

- HTTPS や SMTPS をはじめとする SSL/TLS 通信を悪用したネットワーク上の脅威への対策
- 情報セキュリティインシデント発生時の、SSL/TLS で暗号化された通信データの内容も含めた原因調査の実現

解決策：

- A10 Thunder® の SSL インサイトソリューションにより SSL/TLS 通信を高速に可視化（復号）
- 三菱スペース・ソフトウエアの Dynamic MSIESER により、SSL インサイトソリューションで可視化（復号）された SSL/TLS 通信の記録とそれに基づくネットワークフォレンジック

メリット：

- Dynamic MSIESER と A10 Thunder の組み合わせにより、SSL/TLS 通信を復号した状態で記録でき、情報セキュリティインシデント発生時の原因調査が容易に
- 大規模なセッションを処理可能な A10 Thunder により HTTPS 通信を高速に復号 / 再暗号化し、高い通信パフォーマンスを維持
- HTTPS や SMTPS も含むすべてのポートに渡る SSL/TLS 通信の復号と記録を実現

三菱スペース・ソフトウエア株式会社

DynamicMSIESER
ダイナミック エムシーサー

SSL/TLS 通信の増大とネットワークフォレンジックの困難化

近年、データの盗聴・改ざん・窃盗を防ぐために、通信データの SSL/TLS による暗号化の流れが進んでいます。サーバー証明書の発行が容易になったことに加え、Web サイトの HTTPS 対応が検索ランキングへ影響するようになったことやブラウザに Web サイトの暗号化への対応状況が表示されるようになったこと、多くのクラウドサービスが HTTPS での接続を前提としていることなどから、現在では通信の大部分が SSL/TLS により暗号化されています。

通信パケットを全て記録し情報セキュリティインシデント発生時の原因究明を行うことを目的としてネットワークフォレンジック製品を利用している場合、通信が SSL/TLS で暗号化されていると通信データの内容を確認することができません。多くのネットワークフォレンジック製品はミラーポートで通信パケットを記録することから、自身で SSL/TLS 通信を復号して平文のデータを記録することもできず、結果として情報セキュリティインシデント発生時の原因究明が SSL/TLS 化された通信の増大によって十分に行えなくなるリスクがあります。

SSL/TLS 通信を可視化する A10 の SSL インサイトソリューションと Dynamic MSIESER との連携

A10 Thunder シリーズで利用できる SSL インサイトソリューションを利用することで、通信パフォーマンスを落とすことなく SSL/TLS 通信を可視化できます。このソリューションを導入する際には、A10 Thunder アプライアンスを組織内部にあるクライアントとインターネットの間に設置する必要があります。クライアントとインターネット間の HTTPS や SMTPS などの SSL/TLS 通信をインターセプトして復号し、平文化した通信データをインライン型・パッシブ型・ICAP サーバー型のセキュリティ機器に転送して検査することができます。トラフィック分析のために復号された通信データは再暗号化され、目的のアドレスに転送されます。

三菱スペース・ソフトウエア社のネットワークフォレンジック製品 Dynamic MSIESER はこの SSL インサイトソリューションとの連携が可能です。SSL インサイトにより可視化された通信をミラーポートで Dynamic MSIESER に送ることで、SSL/TLS 通信は復号された状態で Dynamic MSIESER に記録されます。(図 1)

Dynamic MSIESER はネットワーク上の通信データを記録し、情報セキュリティインシデント対策を行うためのネットワークフォレンジックシステムです。「いつ」「誰が」「どこへ」「どのように」「どのような」情報を送受信したかを記録し、メールの送受信や Web サイトの閲覧履歴などの監査証跡を残すことができます。情報漏えいやマルウェア感染などの情報セキュリティインシデントが発生した際に、これらの記録データを基にした調査を可能にします。ミラーポートからパケットをキャプチャするため容易に導入でき、高い処理性能により大容量のデータでもパケットロスや解析遅延なく安定稼働し、長期のデータ保管が可能です。メールや Web アクセス、ファイル共有などの送信ファイルの内容を検査することができ、送信ファイルに個人情報や機密情報があった場合には管理者に通知する機能を持ちます。

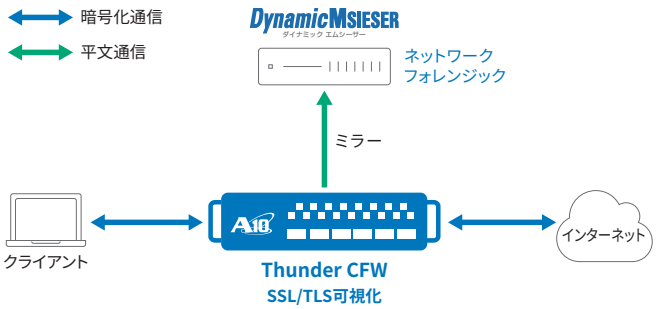

図1：A10 ThunderによるSSLインサイトソリューションと Dynamic MSIESERとの連携

Dynamic MSIESERはミラーポートで通信パケットをキャプチャすることから、通常はHTTPSやSMTPSのようなSSL/TLS通信を復号できず、暗号化された通信内容を解析することができません。キャプチャされたパケットの中のSSL/TLS通信に潜む脅威を可視化するためには、図1のようにSSL/TLS可視化ソリューションとの連携が必要になります。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たA10 Thunderシリーズは、クライアントから見るとプロキシサーバーとして動作します。透過型で配置することも可能です。A10 ThunderはSSL/TLS通信をインターセプトし、SSL/TLS通信を復号して、ミラーポートを通じてDynamic MSIESERに復号した通信を送信します。SSL/TLS通信の流れは以下のようになります。

1. A10 Thunderがクライアントから通信先のサーバーに向けたトラフィックをインターセプトし、SSL/TLS通信を復号し、ミラーポートを通じてDynamic MSIESERに送信し、復号されたパケットをキャプチャ
2. 平文化されたSSL/TLSトラフィックをA10 Thunderが再暗号化し通信先サーバーにフォワード
3. 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
4. A10 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、復号した後ミラーポートを通じてDynamic MSIESERに送信
5. 復号された通信を再暗号化しクライアントに送信
   ※HTTPやSMTPなどの平文通信の場合は復号せずにそのままミラーポートを通じてDynamic MSIESERに送信

SSL/TLS通信の特性上、リクエストの復号とレスポンスの再暗号化のためにクライアントがA10 Thunderを信頼する必要があるため、A10 Thunderにはクライアントが信頼できる証明書がインストールされているか、クライアント側にA10 Thunderと同じ証明書が信頼できる証明書としてインストールされている必要があります。A10 Thunderには任意の証明書をインストールして利用することができます。

SSL/TLS通信に含まれるリクエスト/レスポンスを平文でDynamic MSIESERに渡すことで、これまで通信データの内容が把握できなかったSSL/TLS通信に対しても、平文の通信と同様に、通信内容の確認が可能になります。特にSSL/TLS通信で送受信されたファイルの内容や、HTTPSでアクセスしたURIなどが全て記録できるようになり、マルウェアファイルをいつ受信したかの確認や情報漏えいの検査、URIも含めた不正アクセスの調査が可能になります。クライアントとA10 Thunderの間、およびA10 Thunderと通信先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は防止されます。

一度復号するとミラーポートだけでなくインライン型のファイアウォールなどのセキュリティ機器にも復号した通信を送ることができるため、他のセキュリティ製品との連携も可能です。また、A10 Thunder自身を冗長化して可用性を高めることもできます。

その他のA10 ThunderによるSSLインサイトとDynamic MSIESER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SSL/TLSコネクション数の処理能力とスループット（1台で最大25Gbps、2台で最大50Gbps）
- 全てのポートに渡るSSL/TLSトラフィックの復号
- L2/L3の多様なネットワーク構成に対応し、既存の環境に応じた柔軟な構成が可能
- 復号の対象とするSSL/TLS通信の指定などが可能な詳細なポリシー設定

三菱スペース・ソフトウエア株式会社について

三菱スペース・ソフトウエアは、1962年に設立されたシステム・エンジニアリング会社です。宇宙開発で培った様々な技術をもとに、現在9つの分野で事業を展開しています。”Make a Smart Society”を企業ビジョンとし、宇宙開発で培った高度な科学技術、最先端の情報技術を駆使し、高品質・高信頼のソリューションで、「安心して快適に暮らせる未来の社会創り(smart society)」を目指します。情報セキュリティソリューションの分野では、標的型サイバー攻撃、不正アクセス、情報漏えいなどの脅威に対する独自の情報セキュリティソリューションを提供しています。
https://www.mss.co.jp/

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

A10ネットワークス株式会社
www.a10networks.co.jp
a10networks.co.jp/contact

お問い合わせ：

Part Number: A10_SB_DynamicMSIESER_and_A10 Apr 2020