ソリューションブリーフ

URL フィルタリングと URL/IP レピュテーションによる脅威からの防御

A10 ネットワークスの URL クラシフィケーションサービスと脅威インテリジェンスサービス

不正な Web サイトへのアクセスをいかに防ぐか

様々な産業がインターネット上で顧客との接点を持つために、また、新しいサービスを Web サービスとして提供するために、新しい Web サイトが次から次へと公開されています。これらのサイトの中には、グループウェアを始めとするクラウドサービスや必要な情報を調査するためのサイトなどの企業や組織の業務に必要なサイトだけではなく、ギャンブルや暴力的な Web サイトなどの業務中にアクセスするにはふさわしくないサイトも含まれます。加えて、フィッシングサイトやスパイウェア / マルウェアを不正にダウンロードさせるための Web サイトも日々新たに公開されています。企業や組織のセキュリティを担保するためには、正当なサイトと不正なサイトへのアクセスを適切に識別し、不正なサイトや業務と無関係なサイトにアクセスさせないように制御する必要があります。不正なサイトへのアクセスを未然に防ぐことで、セキュリティインシデントの発生を防ぐだけでなく、電子メールの不正な添付ファイルなどから始まる一連の標的型攻撃をキルチェーンの途中で防ぐことや、組織内からの情報の窃取を防ぐことも可能になります。

不正な Web サイトの URL や IP アドレスは動的に変化し、また日々めざましく増加しています。また、サイトの内容も悪意のある状態と正常な状態を日々変化させ、不正な Web サイトであることの検出を回避しようとします。そのため、正確に不正サイトの情報をとらえるには、継続的なスキャンに基づく動的に変化する脅威インテリジェンスが欠かせません。

A10 の URL クラシフィケーションサービスと脅威インテリジェンスサービス

A10 ネットワークスの A10 Thunder シリーズで利用できる URL クラシフィケーションサービスや脅威インテリジェンスサービスを利用することで、これらの不正な Web サイトへのアクセスや業務に不適切なサイトへのアクセスを制御したり、不正な送信元からのアクセスを遮断したりすることが可能になります。A10 の URL クラシフィケーションサービスを A10 Thunder シリーズの持つフォワードプロキシ機能や SSL/TLS 通信可視化機能（SSL インサイトソリューション）と併せて利用することで、インターネット上の Web サイトへのアクセスに含まれる URL を自動分類し、分類したカテゴリごとの通信制御が可能になります。また、脅威インテリジェンスサービスを利用することで不正な IP アドレスのリストを A10 Thunder CFW モデルが提供するファイアウォール機能と連携させることができ、ボットネットやスパムメールの送信元などの不正なサイトからのアクセスやそれらのサイトへのアクセスを制御することが可能になります。いずれのサービスも URL リストや IP アドレスのリストは継続的なスキャンと機械学習に基づき動的に更新され、更新されたリストがタイムリーに A10 Thunder シリーズに配信されます。これらの機能は A10 Thunder シリーズにビルトインされており、該当サービスのライセンスをアクティベーションするだけで追加の機器を導入することなく利用することができます。ライセンスは A10 Thunder シリーズに対する筐体またはインスタンス単位でのサブスクリプションライセンスとなっており、アクティベートすると同一の筐体またはインスタンス内での各アプリケーションデリバリパーティションでも利用できます。

課題：

- アクセス先の Web サイトの種類や潜在的な脅威の度合いに基づく、クライアントから Web サイトへのアクセスの適切な制御
- URL レベル、および IP アドレスレベルでの不正サイトへのアクセスを遮断することによるセキュリティの強化
- 規制への準拠等で必要になる、Web サイトの種別に基づく SSL/TLS 通信の可視化 / バイパスの判定
- 脅威 URL や脅威 IP アドレスの脅威レベルの調査

解決策：

- A10 URL クラシフィケーションサービスによるアクセス先 URL の Web サイトのカテゴリ判定
- 宛先 URL のカテゴリに基づくアクセス制御（アクセス可否の判定やトラフィックの振り分け、SSL/TLS 通信可視化の実行可否の判定など）
- 宛先 URL の評価スコア（URL レピュテーションスコア）に基づくアクセス制御
- IP アドレスの評価スコア（IP アドレスレピュテーションスコア）に基づくアクセス制御
- Threat Investigator による脅威 URL/ 脅威 IP アドレスに関する調査

メリット：

- クラウド上のデータベースとの連携による高い URL カバー率
- 自動更新される脅威インテリジェンスによる最新の脅威への対応
- URL レピュテーションスコアに基づく柔軟なトラフィック制御の実現
- A10 Thunder に機能がビルトインされており、ライセンスを追加するだけでサービスを利用することが可能

URL クラシフィケーションサービス

A10 の URL クラシフィケーションサービスには以下の機能が含まれます。

- URL クラシフィケーション
- URL レピュテーション
- Threat Investigator

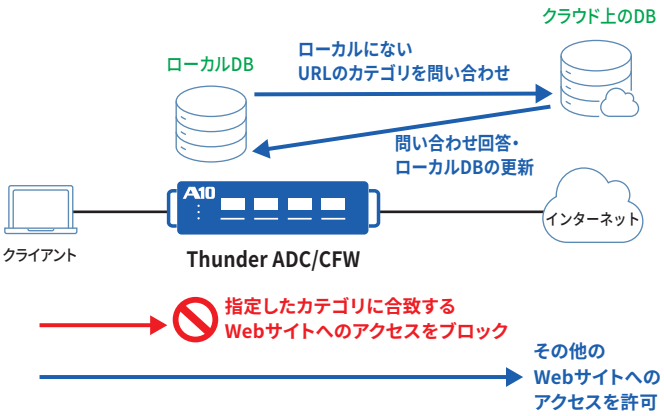

図 1：URL クラシフィケーションによるアクセス制御

URL クラシフィケーション機能により、フォワードプロキシや SSL インサイトを通過する組織内から組織外への Web アクセスに含まれる URL を 83 以上のカテゴリに自動的に分類します（図 1）。URL のデータベースは頻繁に利用されるものは A10 Thunder の内部に保持し、利用頻度の低いものはクラウド上のデータベースに配置されます。A10 Thunder 内部のデータベースにヒットしなかった場合は自動的にクラウド上のデータベースに問い合わせを行います。データベースの規模は最大級のものであり、日本語を含む 45 以上の言語に対応し、Alexa Top 100 万サイトの約 95% をカバーします。

URL クラシフィケーションの主な用途としては、A10 Thunder をフォワードプロキシとして用いた場合の URL フィルタリングへの利用があります。フィッシングサイトやマルウェアサイトなどのカテゴリを指定してアクセスをブロックすることで、組織内のメンバーが添付メールの不正な添付ファイルを開くなどして不正なサイトに誤ってアクセスすることを防いだり、追加のマルウェアのダウンロードや情報窃取のための不正サイトへのアクセスを遮断したりすることができます。加えて、ギャンブルや暴力的なサイトなどの業務上アクセスが不要なサイトへのアクセスをカテゴリ単位でブロックすることが可能です。また、近年の SSL/TLS 通信の増加に伴い、SSL/TLS 通信を可視化して検査することが必要となってきましたが、特にプライバシーが重要な金融機関や健康情報へのアクセスについては SSL/TLS 通信を可視化せずにバイパスすることが求められることがあります。A10 Thunder の SSL インサイトソリューションと URL クラシフィケーション機能を併せて利用することで、該当するカテゴリへのアクセスを SSL/TLS 可視化しないように自動的にバイパスすることも可能です。これによりプライバシーの保護を要件とする規制への準拠も容易になります。

上記の URL クラシフィケーションサービスに加え、アクセス先の URL に対する信用スコアを提供する URL レピュテーション機能（図 2）も同一ライセンス内で利用できます。この機能では、Web サイトに対する各アクセスに関して、アクセス先の URL の信用スコアを 1 から 100 の間で出力することができます（信用度が高いほどスコアが高い）。

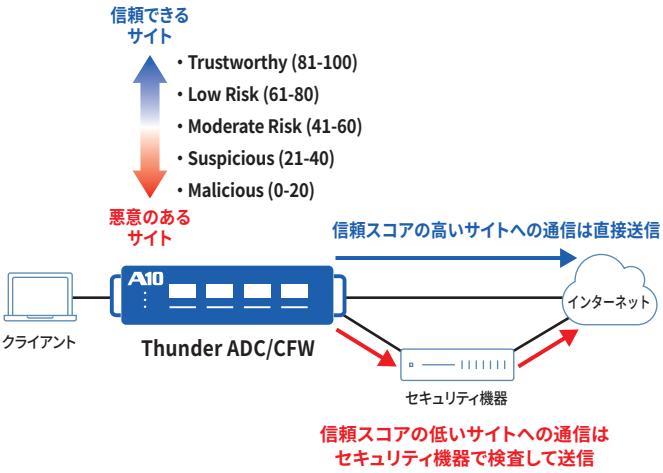

図 2：URL レピュテーションに基づくトラフィック制御例

このスコアそのもの、またはプリセットされた 5 段階の信頼度に基づいてフォワードプロキシによる通信制御や SSL インサイトによる SSL/TLS 通信の可視化例外を設定することができます。例えば、信頼度の低いサイトへのアクセスのみ SSL/TLS 通信を可視化した上でセキュリティ機器により検査を行い、信頼度の高いサイトへのアクセスはレスポンス速度を確保するために SSL/TLS の可視化やセキュリティ機器での検査は行わないようにする、などの設定が可能になります。また、この信用スコアをログとして残すことができるため、クライアントの動的な振る舞いをログからトレースすることも可能となります。URL クラシフィケーションサービスのライセンスには A10 Thunder 上で脅威情報を調査することを可能にする Threat Investigator も含まれます（図 3）。Threat Investigator に URL や IP アドレスを入力することで、その信用スコアや同じ IP アドレスに紐づく複数の URL の信用スコアなどを検索できます。これによりログなどから検出された

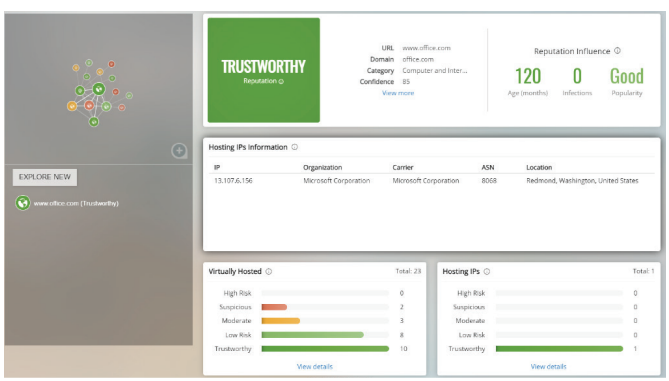

図 3：Threat Investigator

URLや宛先IPアドレスの信用スコアを確認することができ、脅威分析の一助とすることができます。Threat InvestigatorはURLクラシフィケーションサービスのライセンスがアクティベートされていれば、A10 ThunderシリーズのGUIから利用することができます。

脅威インテリジェンスサービス

A10の脅威インテリジェンスサービスを利用すると、ボットネット・スキャナー・フィッシング・スパムメールの送信元などの10種類のカテゴリに相当するIPアドレスのリストをA10 Thunder CFWシリーズのファイアウォール機能で利用することが可能になります（図4）。脅威インテリジェンスサービスはURLクラシフィケーションサービスにライセンスを追加する形でのみ利用できます（単独での導入はできません）。この脅威インテリジェンスサービスでは37億のIPアドレスを様々な観測点でモニターしており、その振る舞いなどに基づいて算出したレピュテーションスコアを基に特定した不正なIPアドレスがA10 Thunderに配信されます。IPアドレスリストは動的に更新され、最新の脅威に対しても自動的に追随することができます。

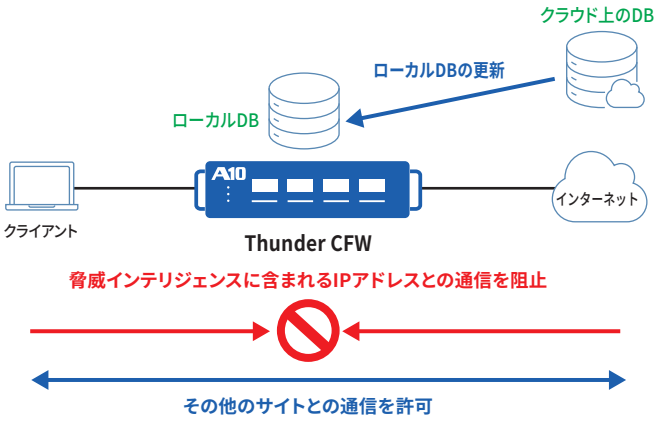

図4：脅威インテリジェンスサービスによるアクセス制御

脅威インテリジェンスサービスの主な用途としては、フォワードプロキシのインターネット側のファイアウォールで利用することで、組織内からの不正なサイトへのアクセスをIPアドレスベースで止めるために利用することが考えられます。先述したURLクラシフィケーションやURLレピュテーションによるURLベースでの防御に加え、名前解決後のIPアドレスベースでの防御を行うことで、ドメイン名を名前解決した後のIPアドレスが詐称されている場合にも有効な防御を提供できます。また、外部の不正なサイトからの組織内への侵入やC＆Cサーバとの通信を検知し阻止するためにも利用することができます。

まとめ

A10のURLクラシフィケーションサービスや脅威インテリジェンスサービスを利用することで、組織内部のクライアントから不正なサイトへの接続の検知と阻止を実現でき、動的にアップデートされるデータベースにより最新の脅威に対する有効な防御を実現することができます。これらのサービスをA10 Thunderと併せて利用する利点をまとめると以下になります。

- 追加の外部サーバ等が不要で、A10 Thunderシリーズに組み込まれた機能をアクティベートするだけで利用開始できる
- クラウド上のデータベースと連携した高いURLのカバー率
- データベースの動的な更新による最新の脅威への対応
- URLカテゴリやURLレピュテーションスコアを用いた柔軟なアクセス制御とトラフィック制御の実現
- 脅威インテリジェンスサービスによるIPアドレスベースでの不正サイトへのアクセス制御、および不正サイトからのアクセスに対する防御の実現
- URLベースおよびIPアドレスベースでの統合された脅威防御の実現

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_URL_Classification_Service Feb 2021