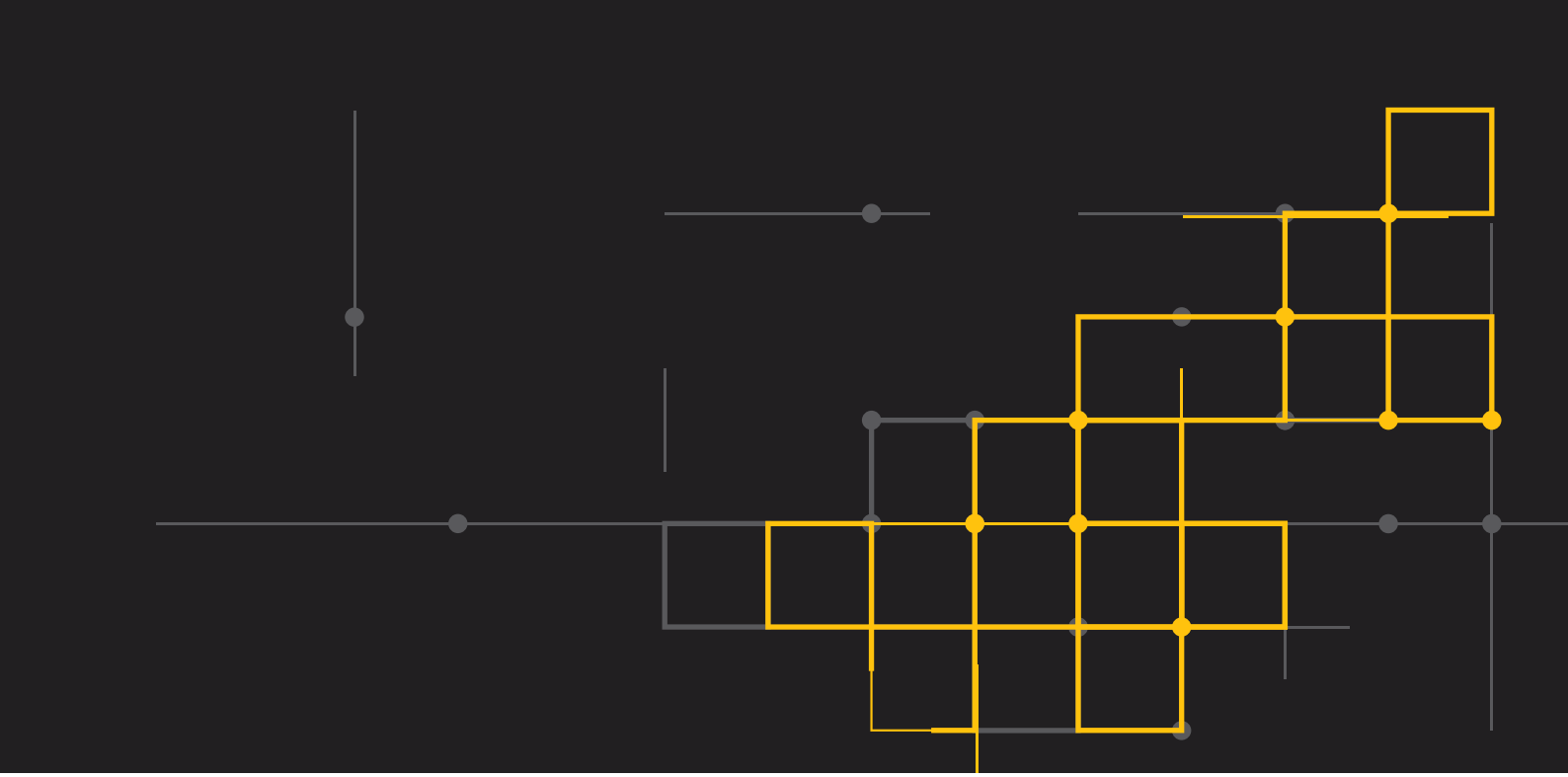

次世代のセキュア Web ゲートウェイ:
セキュリティアーキテクチャの基本

プロキシベースのセキュア Web ゲートウェイアーキテクチャが、Web ベースの脅威の防御に効果的な理由

Symantec

今や Web は仕事や生活や娯楽の中心となっており、そのためサイバー犯罪の格好の標的にもなっています。企業を標的としたサイバー犯罪はますます増加しており、Web をベースとした脅威の数、多様性、巧妙さはかつてないほど高まっている状況です。

多くの企業では Web セキュリティに対する自社のアプローチを見直すことによってこの問題に対応しており、これは前向きな動きだといえます。しかし、現在の Web セキュリティテクノロジ、特にセキュア Web ゲートウェイ（Web プロキシソリューションともいう）については、誤解されていたり逆効果につながっていたりする場合もあります。

Web プロキシアーキテクチャを詳しく見てみると、Web プロキシアーキテクチャが果たす役割はこれまで以上に重要になっています。さらに、Web をベースとした今日の脅威に対する包括的な保護を提供できる事実上唯一のアーキテクチャがこの Web プロキシアーキテクチャであることも明らかになっています。

このホワイトペーパーでは、Web プロキシが提供する機能、プロキシアーキテクチャは包括的な Web 防御に今なお不可欠である理由、そして高度な Web ベース脅威に対する企業の防御力を高めるために、次世代ファイアウォール（NGFW）などの他のソリューションと Web プロキシをどのように連携できるかについて簡単に説明します。

Web プロキシとは何か?

Web プロキシとは、簡単に言えば Web サイトを出入りするトラフィックを処理するサーバーです。たとえば、ユーザーが表示したい Web サイトのアドレスをブラウザに入力した場合、ブラウザが Web プロキシにその要求を送信します。その後、Web プロキシは要求を確認して認証や承認といったセキュリティに関するタスクを実行し、問題がなければそのページをホストするサーバーに要求を送信します。また、Web プロキシは要求されたコンテンツをユーザーのブラウザに送信する前に、マルウェアなどの脅威が潜んでいないかも確認します。

> プロキシアーキテクチャは、Web をベースとした
> 今日の高度な脅威に徹底的な保護を提供する
> 唯一のアーキテクチャです。

つまり、Web プロキシは Web トラフィックの「検疫」サービスを提供します。ユーザーと HTTP/HTTPS サイトの間ですべてのトラフィックを検査し、すべての URL を分類します。これにより、ポリシーに従って悪質なサイトやページを識別してブロックする一方で、問題のない URL へのアクセスを維持できます。

IT 業界では、「SWG（Secure Web Gateway）」と Web プロキシという言葉が同じ意味で使われる場合も多くあります。しかし、すべての SWG がプロキシというわけではないので、注意が必要です。SWG が導入された当初は、勤務中の Web ショッピングを防ぐなど、企業や組織のポリシーを適用することが目的でした。脅威がまん延する今の時代、SWG は Web ベースのサイバー犯罪、マルウェア、フィッシングなどを包括的に防御するための Web プロキシを組み込んでおく必要があります。

なぜなら、SWG へプロキシを組み込むことを明確に義務付けておけば、すべてのトラフィックをプロキシで中断できるからです。すべての Web トラフィックが Web プロキシで中断されれば、プロキシを通過するすべてのコンテンツをスキャンし、分析結果を待ってからユーザーにデータを送信できます。また、プロキシは、検査や制御をすり抜けてインターネットに送られるトラフィックが発生しないように、認証を実行することもできます。

プロキシベースの SWG にできて NGFW にできないこと

プロキシを備えていない SWG の導入や NGFW などのテクノロジ（TAP ポートや SPAN ポートの導入など）では、トラフィックを中断できません。TAP ポートデバイスや SPAN ポートデバイスではゲートウェイがネットワークの脇に設置されており、トラフィックを途中で止めるのではなく、側を通り過ぎるときにトラフィックを観察します。

NGFW はストリームベースの検出手法を利用しているため、ストリーミングを行いながら送信中のトラフィックを検査します。このような仕組みには固有の弱点があります。ゲートウェイや NGFW が時間内に脅威を検出しない場合、またはトラフィックフローを中断するための TCP リセットパケットを時間内に送信しない場合、マルウェアなどの脅威が社内ネットワークに到達してしまう可能性があります。また、ストリームベースのスキャニングの性質から、断片化されたパケットを使用して時間をかけてマルウェアが配信され、検出をすり抜ける恐れもあります。プロキシはその性質上、オブジェクト全体が組み立てられてスキャンされるまでは、オブジェクトが配信されません。

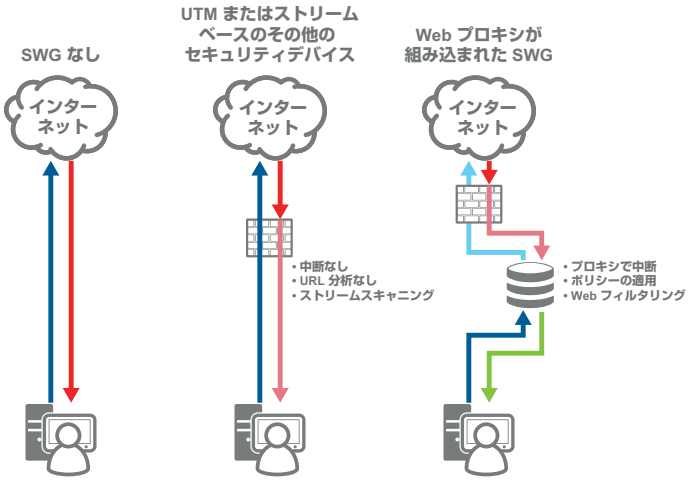

図 1 – プロキシベースのセキュア Web ゲートウェイが他の SWG と異なる理由

さらに、NGFW はアプリケーションを的確に分類するため、トラフィックがデバイスを通過できるように設計されています。このアプローチについて、Network World 誌は Clear Choice 試験の中で、「意図しない結果を招きやすく、危険な構成になる可能性がある。これは憂慮すべき問題点だ」と指摘しています。

同じく重要な点として、NGFW の導入では、ユーザーが要求した URL に関する情報の効果的な収集や分析ができません。NGFW ソリューションでは通常、ドメインのみを分類します。一方、Web プロキシアーキテクチャは URL を分類できるため、きめ細かなポリシー制御が可能です。これにより、IT セキュリティチームや管理者は、悪質なコンテンツだけをブロックして、サイト自体へのアクセスは許可できます。

この機能のメリットを十分に理解するためには、Microsoft や CNN などの主要なサイトで悪質なコンテンツが見つかった場合を考えてみてください。通常の NGFW ではサイト全体をブロックする必要がありますが、Blue Coat ProxySG などの Web プロキシソリューションなら、1 つの URL だけをブロックし、サイトの残りの部分へのアクセスは許可できます。

この ProxySG の機能を補完しているのが、Symantec Global Intelligence Network の一環である Global Intelligence Network です。このネットワークは、7,500 万人を超えるユーザーと 1 日 10 億件以上の要求から、新しい脅威に関するインテリジェンスを収集しています。これによって、NGFW ベンダーよりもはるかに高い可視性を実現しているのです。たとえば、シマンテックが実施した試験で、悪質な URL の上位 125 個を特定し、その情報をシマンテックの SWG と業界トップクラスの NGFW の両方に渡しました。シマンテックの SWG ではすべての URL にフラグが付けられましたが、NGFW には次のような重大な問題がありました。

- **76 個の URL を「未知」と分類。**これは、NGFW テクノロジでは悪質なサイトの 61% が分類すらされないことを意味しています。
- **マルウェアと特定された URL は 5 つのみ。**つまり、残りの 95% は見逃してしまう恐れがあります。
- **NGFW ではいくつかの重大な分類ミスがありました。**いくつかのサイトは検索エンジンまたは個人のサイトであると分類されましたが、これらは悪質な恐れのあるサイトです。これらの URL は、どれだけ注意深いファイアウォール管理者でもブロックできないでしょう。

また、Global Intelligence Network は、シマンテックのすべての製品にリアルタイムのフィードバックループを提供しています。これによって、新しい脅威が検出されると、システムがリアルタイムでアップデートされます。たとえば、シマンテックのマルウェア分析アプライアンスのサンドボックスソリューションで新しい脅威が検出されたとしましょう。当該マルウェアに関する情報は Global Intelligence Network にリアルタイムで送信されるとともに、他のすべてのシマンテック製品でも共有されます。したがって、その脅威をホストしている URL を即座にブロックできます。

また、Web プロキシには、Web ページの操作とポリシーに関する独自の機能があります。たとえば、ヘッダーの非表示、追加、書き換えなどは、Web ポリシーで利用できる Web プロキシ独自の機能です。Web プロキシは URL の書き換えやリダイレクトに加え、Web ページ上のスクリプトの分析や操作も行えます。

プロキシが独自に備えるこの性質は、プロトコルコンプライアンスの適用にも使用できます。プロキシは 2 つの個別の接続（カンバセーションのそれぞれの側に 1 つずつ）を使用してアプリケーション層で動作し、プロトコル標準に準拠しているかを検証して、準拠していないトラフィックを遮断するかまたは修正する機能を提供します。たとえば、ストリーミングプロキシはプロトコルコンプライアンスを適用することで、バッファオーバーフロー攻撃を完全に阻止できます。

また、同じ機能によって、カンバセーションの一方からもう一方へとプロトコルを変換することもできます。たとえば、クライアントが IPv4 のみに対応している場合、プロキシを使用して IPv6 Web サーバーにカンバセーションを送信することで、クライアント側が IPv6 に未対応でもアクセスが可能になります。同じく、IPv6 のみに対応しているクライアントや環境から Web プロキシを介して IPv4 Web サーバーにアクセスすることもできます。

つまり、NGFW はセキュリティを確保できる仕組みとは言い切れないのです。企業のポリシーを適用する場合には十分に機能するかもしれません。しかし、デバイスに過剰な負荷を与えることでデバイスを機能不全に陥らせ、デバイスのパフォーマンスを低下させたり脅威を阻止できない状態にしたりする Web 経由の脅威を防ぐことはできません。

NGFW にできて SWG にできないこと

それでは、NGFW の代わりに Web プロキシを使用するべきなのでしょうか。そうではありません。

NGFW は、アプリケーションの保護や標準的な Web ベースプロトコル以外のプロトコルの保護、パケットベースの脅威の検査など、Web プロキシが対応していない特定の領域でその効果を発揮します。企業の IT リーダーには、このような特別な保護の必要性を判断することが求められます。必要な場合には、NGFW を導入することで多層型防御に優れた防御機能を追加できるかもしれません。

しかし、今日の脅威の多くは Web を介して企業に侵入しており、業界トップクラスの Web セキュリティで企業を保護することが最優先なのは明らかです。SWG ソリューションに Web プロキシを組み込めば、強固なセキュリティソリューションの土台となるはずです。

Web プロキシにまつわる誤解

セキュア Web ゲートウェイについて最も多い懸念は、今日の企業ネットワークを行き来する大量の Web トラフィックを処理する設計ではないため、速度が遅いのではないかということです。

実際には、プロキシアーキテクチャを組み込んだ SWG は、遅延を発生させることなく大量のトラフィックを処理できます。シマンテックの ProxySG で、非常に良い例があります。プロトコルの最適化と最速の評価技術に加え、特許取得済みの Web キャッシュ技術を利用することで、ProxySG アプライアンスは多くの場合、プロキシアーキテクチャなしでの実績を超える優れた Web パフォーマンスを提供します。

皮肉なことに、NGFW ソリューションについて公表されているパフォーマンスの数値は、非常に誤解を招きやすいものです。NGFW のパフォーマンスは、機能ごとに測定される傾向があります。NGFW のベンダーは通常、ファイアウォール、脅威防止、VPN 機能のスループットを個別に記載しますが、これらは各機能に最善の環境で測定された数値です。そのため、たとえばファイアウォールと脅威防止を同時に実行すれば、数値は確実に低下します。一般に、NGFW ソリューションの重要なセールスポイントとなるのは総合的なパフォーマンスです。そのため、実環境におけるアプライアンスの実際のパフォーマンスとこれらの数値とは区別して考えることが重要です。

また、次世代のセキュリティ機能や最新のセキュリティ技術との統合についても心配はいりません。シマンテックのソリューションは、業界トップクラスのセキュリティ技術のほとんどと連携できるからです。シマンテックは ICAP などの業界標準のインターフェースを使用することで、ホワイトリスト、サンドボックス、静的コード分析といった重要な新しいセキュリティテクノロジ、さらには最新のマルウェア対策や DLP などのテクノロジを統合する、真に安全な制御ポイントを提供します。

結論

今日、Web 脅威への全面的な防御を実現する唯一の方法は、プロキシベースのセキュア Web ゲートウェイアーキテクチャを使用して、Web を経由するすべてのトラフィックを遮断することです。基幹ネットワークを脅威の侵入から保護することは、最優先で取り組むべき課題です。SWG にプロキシアーキテクチャを組み込むことで、Web を経由するすべてのトラフィックを処理対象とする必要があるでしょう。

ProxySG などのセキュア Web ゲートウェイソリューションを使用すると、すべてのトラフィックを検査し、既知の脅威とリアルタイムに検出された脅威の両方をブロックするポリシーを設定できます。シマンテックが提供するプロキシアーキテクチャは、すべての Web トラフィックの徹底的な検査とマルウェアのスキャンに必要となる高いパフォーマンスも実現します。

さらに重要な点として、プロキシアーキテクチャを使用して Web 経由の脅威を防御することにより、セキュリティをまったく新しい視点で見られるようになります。つまり、予想外の事態に対する一連の防御だけでなく、ビジネスを強化する手段として見えてくるのです。潜在的な脅威を心配する必要がなくなれば、新しい可能性に集中できるからです。

シマンテックについて

シマンテックコーポレーション(NASDAQ: SYMC)は、サイバーセキュリティ業界をリードする世界的企業です。さまざまな場所に保管されている大切なデータを守るため、企業や政府機関、個人のお客様を支援しています。エンドポイントからクラウド、インフラまでを高度な攻撃から守るため、世界中の企業がシマンテックの戦略的統合ソリューションを選択しています。また、世界中で 5 千万以上の個人やご家庭が、自宅などで使用するデバイスそしてデジタルライフを守るためにノートンと LifeLock 社の製品を使用しています。シマンテックのサイバーインテリジェンスネットワークは民間が運営するネットワークとしては世界最大規模を誇ります。このネットワークが、先進的な脅威をいち早く発見し、お客様を守ります。詳しくは www.symantec.com/ja/jp/ をご覧ください。

株式会社シマンテック
〒107-0052 東京都港区赤坂1-11-44 赤坂インターシティ | www.symantec.com/ja/jp/

SYMC_wp_Next-Gen_Secure_Web_Gateway_JP_v1a