



上からのセキュリティ:
クラウドベース・セキュリティが最新のネットワーク保護を提供できる理由

2010年2月

セキュリティ・アプローチを再考する必要性

様々なトレンドが湧き上がっている中、組織はセキュリティへの取り組みを再考しなければならない状態になっている。広く蔓延するメール・ウイルスやワームは減少したものの、ウェブを介した攻撃は上昇中だ。それというのも、メールやインスタント・メッセージ、Eコマースといった様々なアプリケーションをウェブ・ブラウザが統合しているため、そんなウェブ・ブラウザが攻撃を仕掛けるには恰好の場所になっている。

Web 2.0 や、その他の複雑なウェブ技術も、新しい 2 ステージ・ウェブ攻撃やソーシャル・エンジニアリングによる悪用を迎え入れている。実際 2009 年の第一四半期には、Web 2.0 サービスやサイトが最高記録の 21% というハッキング件数に導いている。このように、新しい攻撃方法は信頼した発信元から派生したものであったり、正当あるいは認証したメールやウェブ・コンテンツに埋め込まれているため特に危険である。

2 つの要因は、ウェブ・ベースのマルウェア脅威の成長をさらに促進させている。まず、サイバー犯罪は金銭的な動機を持ち、マルウェアを広めウェブ・ユーザの個人データを獲得しようとするのだが、犯罪者達はその手段を備えている。Web 2.0 が拡散し、テキスト形式のメールや、高度で悪質なソーシャル・エンジニアリングを使った作戦でスパムが劇的に進化し、スパマーは疑いを持たない被害者が使用しているデバイスを容易に感染させることができるようになった。ウェブ・ベースの感染を招く方法としてメールが使われ、スパマーはいとも簡単に被害者を見つけ誘い込み、ボットネットやスパイウェア、マルウェア、ブレンドされた脅威などを介してその被害者を感染させる。そして被害者を管理した上で、さらに感染を悪用させることもできる。それはすべて、たった 1 通の悪質なメールから始まり、社員がマウスをクリックするだけで組織のビジネスやネットワークがセキュリティ侵入や規定違反、機密情報の盗難にあたり、さらには侵害されてからネットワークが他のネットワークを感染させるためのインターネット脅威の源にされてしまう場合もある。

また、サイバー犯罪はウェブ・ベース攻撃を自動化することができる。変更が施されたパッキングや暗号化技術、そしてその他の不明瞭な方法を使って、攻撃者はごく簡単に同じ脅威から何千もの新しい亜種を作成することが

できる。そして、ボットネットが Fast Flux DNS などの新技術を利用し、ダイナミック・ドメインを作成するようになったため、マルウェア・サイトは一度に何週間または何ヶ月もアクティブな状態でいられるようになった。

さらに、ウェブ自体の成長が拡大していることに伴い、拡張する攻撃範囲を通じて攻撃を仕掛けられるユーザの数も上昇している。ウィルス対策の業界をリードする Kaspersky Lab は、2009 年に 3,330 万のマルウェアを発見したが、その間の新しいマルウェアの例は 1,500 万以上あったという。これは登録済みドメイン数の大きな伸びに一致し、VeriSign によるとその数は 2009 年 9 月の時点で 1 億 8500 万にもなったという。ユーザにより作成されたコンテンツやダイナミック・コンテンツ、マッシュアップなど、ソーシャル・ネットワーキングやメディア・サイトなどを提供する Web 2.0 やウェブベースの機能を考慮した場合、攻撃の発信元はそれよりも大規模なものである。

組織は、拡張していく脅威のランドスケープに対処しながら、リーズナブルな価格でセキュリティをどうすれば維持することができるのだろうか？ユーザがウェブ・リソースにアクセスできないようにするのは、非現実的な対策だろう。大方、企業は社員が優れたウェブサイトとのインタラクションにより得られる生産性やマーケティング利益を犠牲にするような妥協はしない。グーグルを使った検索や Meebo、MSN Messenger などウェブベースのインスタント・メッセージ・サイト、Facebook のようなソーシャル・ネットワーキング・サイトが提供するその価値は無視するにはもったいないからだ。

増大している脅威を回避しながら生産性を維持するため、次世代レピュテーション・サービス (Reputation Services) など、クラウドベース・セキュリティ・ソリューションを活用し、警戒姿勢を強化している組織は多い。そうした組織は、クラウドベース・セキュリティだけが実用的で IT 予算に負担を掛け過ぎることなく、常に変化している脅威のランドスケープのスピードについていけるものであると見ている。このホワイトペーパーでは、クラウドベース・セキュリティの進化と、昨今その拡張を続けている脅威のランドスケープにおける次世代レピュテーション・サービスのもたらす組織への影響と、そのセキュリティ成功へ導いていく方法について詳しく取り上げていく。

追い付けなかった初期のレピュテーション・サービス

レピュテーション・サービスは、1990 年代からセキュリティ脅威がネットワークに決して入り込まないよう、必要のないトラフィックや質の悪いトラフィックを組織が確実にブロックできるように支援してきた。ネットワークの境界線で脅威を認識し阻止することで、レピュテーション・サービスは攻撃を阻止したり、スキャン・トラフィックに必要なオン・プレミス IT フットプリント、つまり必要なスペースを減少させたほか、バンド幅やハードウェア、脅威をブロックするために必要なその他リソースに関連したコストを削減させている。ウェブ技術やウェブそのものが成長し、それらがより高度なものになるに連れ、初期のレピュテーション・サービスは、これまでのように効果的に脅威を認識したり、それらを阻止することが難しくなってきた。その効果が弱まった理由をしっかりと理解するには、どのようにサービスが進化してきたのかを理解することが大切だ。

初期のレピュテーション・サービスは既知のスパマー IP を集めた DNS ブラックリスト (DNSBL) だけに依存し、そうした IP を発信元とするトラフィックをブロックしてきた。しかし、マルウェアが正当なドメインも感染するようになってくると、レピュテーション・サービスはスパマーのドメインと、マルウェア感染によりスパミングをしている正当なドメインを区別できなくなった。つまり、DNSBL は問題の IP のうち 50% から 80% にしか対応することができなくなったわけだ。

最新のレピュテーション・サービスは IP ボリュームを DNSBL と合わせて分析し、各 IP アドレスをさらに細かく調べることができる。それにより効果は上がったものの、ボットネットやダイナミック IP の発展によりレピュテーション・サービスによる効果は 70% から 80% となっており、エンタープライズ・セキュリティの基準としては低すぎる数値である。

レピュテーション・サービス業界のリーダー達は、マルウェア・データの情報源が履歴だけであり、その依存性によりレピュテーション・サービスが時代遅れのものになることは、時間の問題であることに気付いている。無数の組

組織が直面している大変化を遂げているウェブ脅威に対処するため、業界をリードする企業は次世代レピュテーション・サービスを提供すべく買収を行っている。

図 1 で表示しているように、次世代レピュテーション・サービスは、綿密なコンテンツ検査や行動分析、マルウェアを検出しブロックするフィードバック・ループ、スパイウェア、そしてユーザが目にする前に悪質なコードを検出するなど、DNSBL とボリューム分析を組み合わせることでレベルの高い保護を提供している。その積極的なアプローチは、次世代レピュテーション・サービスを 99.9% 確実なものにし、その検出率は 98% 以上と、より効果的になっている。これまでのサービス、または現在のサービスに比べそのセキュリティの質は大幅に改善している。積極的に脅威を認識し、それに対応することでレピュテーション・サービスはネットワークの境界線でより強力な防衛を提供できるようになっている。

DNSBL に依存していた初期のレピュテーション・サービスは、過去に避けてきた既知のトラフィックしか監査できない。その点は、クレジット・ビューローに似ていると言えるだろう。

Think Passport Scan	Think Airport Metal Detector Security Scan	Think Airport Biothermal Body Xray Scanners
50% - 80% Effective	70% - 80% Effective	93% - 98.3% Effective
Assign reputation scores based on:	Assign reputation scores based on:	Assign reputation scores based on:
<ul style="list-style-type: none">• DNS Blacklisting (DNS BL) Only	<ul style="list-style-type: none">• DNS BL• Volume	<ul style="list-style-type: none">• DNS BL• Volume• Content Inspection• Behavioral Analysis
Early Services: Monitoring	Most Current Services: IP Reputation	Next-Generation: Behavioral Analysis

図 1: クラウドベース・セキュリティは、攻撃や脅威に対し高品質な保護を提供することができる。初期のサービスは基本的なパスポート・スキャンのようなもので、過去のデータのみをチェックするものだった。しかし最近のレピュテーション・サービスは空港の金属探知機のように、ネットワークに侵入しようとしている脅威の可視性においては制限がある。ところが次世代レピュテーション・サービスは、アクセスを得ようとしている動きを広範囲に渡りスキャンできるサービスを提供しているため、それは空港の生体熱を使った X 線スキャナーのようである。

クラウドベース・セキュリティが次世代技術を活用

次世代レピュテーション・サービスはメールやウェブで、より優れたレベルのセキュリティを可能にするためにクラウドから提供されたサービスである。「クラウド・アプリケーション」という言葉の定義は明確ではなく、クラウド・テクノロジーで既存のアプリケーションを拡張させたり、別の名称を付けたものだったりするが、次世代のレピュテーション・サービスは、実際にクラウドを通じてそのサービスを最大限に利用しているものである。

参加している顧客のセキュリティ・デバイスによる匿名で送られる統合データ、第三者の DNSBL、レピュテーション・データベースなどをクラウドに送るようになってきている。次世代レピュテーション・サービスは、新しい脅威をリアルタイムで確認しながら、データに基づいて統計、分析し行動を取るようになってきているため、一組織が個人で提供す

ることはできない、これまでにないレベルのセキュリティを提供できる。クラウド・セキュリティ・サービス・プロバイダーは、脅威の新たな情報をネットワーク全体に、そして顧客のネットワークにリアルタイムでストリームし、大規模な保護を確実に提供できるようになっている。それがクラウドベース・セキュリティが約束するレベルのセキュリティだ。つまり、何千ものグローバル・システムからリアルタイムに監視しているインテリジェンスを集めることで、その保護を拡大しているのである。

次世代レピュテーション・サービスは、数々のアルゴリズムや技術を統合させ、適合識別技術や行動分析を使いクラウド内にある履歴情報をまとめている（例えばスパマーのデータや分類されたウェブサイトなど）。それらは、いくつかの自動オペレーションを介し、受信するメッセージすべての動きを分析している：

- ・ 埋め込みリンクの検査
- ・ ヘッダーやコンテンツの検査
- ・ マルウェア、スパイウェア、クライムウェア、スパム・シグネチャーのスキャン
- ・ URL フィルタリング
- ・ 接続 IP の行動パターン

結果として、そのレピュテーションやメール、顧客のネットワークに侵入しようとしているウェブ・トラフィックの危険性レベルを決めることができる。ほぼ 100%の正確性で、サービス拒否攻撃やスパマー・プロービングなどを含むセキュリティ脅威を接続レベルで排除し、ローカル・アプライアンスへの負担を減少させている。また、クラウドベース・セキュリティ・サービスがウェブに渡る爆発的なトラフィックの増加をサポートするように変えられるのは、それと同様に重要なポイントだ。

クラウドベース・セキュリティが動き出すと……

次世代レピュテーション・サービスの強さを十分に理解するため、信頼していない IP アドレス（または手が加えられたメール）からネットワークにメール接続がきた場合、様々な場所にある組織で起きる状態をステップごとに検証してみよう。

インターネットから、ネットワークの境界線にメールやウェブによる大量のトラフィックがやって来る。レピュテーション・サービスはトラフィックをすべて調べ、強力な最前線の防衛法として、不要なトラフィックは接続レベルでいつでも全部ブロックできるようになっている。次に、クリーンと判断されたトラフィックはネットワークに入り、顧客のポイント・セキュリティ・ソリューションによってプロセス、ルーティングされることが許可される。コンテンツや送信者の情報、コンテキストなどを検査している間に、顧客のセキュリティ・アプライアンスが他の脅威やスパムを発見すると、そのコンテンツはブロックされる。そして、アプライアンスはそのような発見をレピュテーション・サービスに報告、その情報はネットワーク全体に送られる。

レピュテーション・サービスはデータを分析し優先順位に従って、その IP アドレスを使った特定の送信者の評価、その IP アドレスを送信元とするドメイン、IP アドレス自体の評価などについて結果を生成する。そしてサービスは評価のスコアをセキュリティ・デバイスに戻す。顧客がいかにスレッシュホールドを設定したかによるが、メール・セキュリティ・デバイスはその接続を許可または拒否することができる。

ネットワークに見られる顧客のその他のアプライアンスは、ローカルで分析する前に接続している IP からの新しいセキュリティ脅威について、クラウドに「質問」することができる。そして、この取り組み方によりローカル・アプライアンスが処理するデータが減るため、メール・トラフィックやウェブ・トラフィックが素早く転送されバンド幅の許容量を高くしておけるようになる。

メールを許可または拒否する際に評価スコアは重要だ。そのため次世代サービスは、その評価が正しいものであることに極めて重点を置いている。ウェブやメール、ネットワーク・デバイスからのポート 443 接続や spamhaus、

SORBS (Spam and Open Relay Blocking System) といった第三者の同期化、honeypotドメインなど 10 億以上の情報源から情報を収集することができる。

こうした点から、初期のレピュテーション・サービスでは不可能だったレベルの高い検出率を可能にしている。

検出率が大切な理由

1 ヶ月に 100 万件のメールを受信する組織があったとしよう。DNS ブラックリストは、およそ 50% から 80% の不要なメッセージを除去する。言い換えれば 25 万通のメールがネットワークに入り込んでいることになるわけだ。レピュテーション・サービスが IP トラフィック・ボリューム・データを考慮した場合でも、その検出率は 70% から 80% であり、15 万通のメールはネットワークの境界線をすり抜けていることになる。

次世代サービスの検出率は 98% で、1 万 7 千件のメッセージがネットワークに入り、それらをさらに詳しく検査することで脅威に対する保護を大幅に強化し、コスト削減を可能にすることができる。

クラウドベース・セキュリティに関する懸念を解消

クラウドベース・コンピューティング・サービスでは、組織が SaaS などを提供する第三者の提供者と機密データを共有しなければならない。しかし次世代のクラウドベース・セキュリティでは、デバイスがシェアするのは悪質なトラフィックに関する匿名データだけであり、機密データが露呈されることはない。

クラウドベース・セキュリティの利点

次世代レピュテーション・サービスは初期のものより遥かに効果的であり、すでに顧客が使用しているセキュリティ・アプライアンスを最大限に活かせるように支援し、組織に 4 つの大きな利点を提供している：

- ・**より速くダイナミックなセキュリティ：** 世界中からの何百万という情報をリアルタイムで収集することにより、クラウドベース・セキュリティは最新の脅威の様子やそれを阻止する力を提供できる。
- ・**ローカル・デバイスでの処理を減少：** クラウドベース・サービスはスパムを分析し、データ処理によりローカル・デバイスにかかる負担やバンド幅の消耗を減らすことで新たな脅威に集中できるようにする。
- ・**自動アップデート：** クラウドベース・サービスはクラウドを介してアップデートを出し顧客の機器に広めるため、顧客が手動でアップデートをダウンロードする必要がない。
- ・**クロスコミュニティ・カスタマーによる利点：** クラウドベース・サービスは、パターンや地理的に孤立した脅威のソースを検出し、他の場所にある顧客のデバイスに影響が及ばないようにする。

クラウドベース・セキュリティのタイミングが良い理由

ウェブで行われるビジネスが増えるに連れ、悪質な動きはそのスピードを維持し革新的な方法で攻撃を開始できるように発達している。現在に至るまで企業はそうした攻撃に対抗するため、レピュテーション・サービスに依存してきたが初期のレピュテーション・サービスは昨今の複雑な脅威に対して十分な保護を提供することができない。

リアルタイムの脅威データを連結

クラウドベース・セキュリティ・インテリジェンスを使ってローカルにあるセキュリティ・アプライアンスでリアルタイム

の脅威データを連結させ、完全な攻撃管理や予防策において最良の選択肢を提供できる。

クラウドにおけるプロセスや分析をローカル・デバイスにより提供されたデータと、いくつものグローバル・システムからのリアルタイム監視インテリジェンスを組み合わせたものが理想的なソリューションだ。次世代クラウドベース・サービスは、所有権を持つアルゴリズムとアドバンス機能を活用し、世界でもっとも効果的なレピュテーション・サービスを提供しており、その検出率は 98%以上である。クラウドベース・サービスは、ローカル・メールやウェブ・セキュリティ・アプライアンスを開放させることで不要なトラフィックの処理やアーカイブの必要を軽減させている。そしてその結果、ネットワーク処理やバンド幅に掛かるコストを削減することを可能にしている。クラウドベース・サービスは、新たに発見された脅威から顧客をリアルタイムでダイナミックに保護することができるため、その利点は参加している顧客全員に広く渡っている。

ローカル・セキュリティ・アプライアンスによるリアルタイムの脅威データとクラウドベース・セキュリティ・インテリジェンスを連結させることで、完全な攻撃管理や予防策において最良の選択肢を提供することができる。

次のステップ

次世代クラウドベース・レピュテーション・サービスがどのように作用するのかを見たい、または自分のドメインや IP の評価をチェックしてみたいという場合は、次のサイトを参照することをすすめる。

<http://www.reputationauthority.org>

WatchGuard XCS 製品シリーズに搭載されているメールやウェブ・セキュリティのパワフルな製品、WatchGuard ReputationAuthority™の詳細については次のウェブサイトを参照することをすすめる。www.watchguard.com/xcs

住所: 505 Fifth Avenue South Suite 500 Seattle, WA 98104 U.S.
WEB: www.watchguard.com
営業: 1.800.734.9905
インターナショナル・セールス: +1.206.613.0895

WatchGuard について:

1996 年より、WatchGuard Technologies は信頼でき容易に管理できるセキュリティ・アプライアンスを世界中の何百、何千という企業に提供してきました。弊社の拡張可能な脅威管理(XTM)ソリューション、Firebox X シリーズは、そのレベルでもっとも使いやすく、強力かつ信頼できるマルチレイヤーのセキュリティを連結させた優れた製品です。弊社最新のアプライアンス、WatchGuard XTM 8 Series および XTM 1050 は、高度なパフォーマンスと完全に拡張可能でありながらエンタープライズ・レベルのセキュリティを備え、お求めやすい価格でご提供しています。WatchGuard の拡張可能なコンテンツ・セキュリティ(XCS)アプライアンスは、広範囲に渡りセキュリティ、プライバシー、コンプライアンスにおいてメールやウェブ・トラフィックを保護します。WatchGuard は民間企業であり、本社は米国ワシントン州シアトルに所在し北米、ヨーロッパ、アジアパシフィック、南米にオフィスを構えています。詳細につきましては www.watchguard.com をご参照ください。

同資料における表現に保証はありません。全仕様書は変更される可能性があり、今後の製品や機能などの利用状況については弊社の意向に基づき提供します。©2010 WatchGuard Technologies, Inc. 無断複写・転載を禁じます。WatchGuard および WatchGuard のロゴは WatchGuard Technologies, Inc. の米国およびそのほかの国における登録商標あるいは商標です。そのほかすべての登録商標および商標は、各所有者に権利があります。Part No.WGCE66692_021610

脚注:

Pg.1

(1) 『The Register, Adobe Flash attack vector exploits insecure web design』2009 年 11 月 13 日

http://www.theregister.co.uk/2009/11/13/adobe_flash_wallop/

(2) 『Secure Enterprise 2.0 Forum, Web 2.0 Hacking Incidents on the Rise in Q1 2009』2009年5月5日
<http://www.secure-enterprise20.org/node/39>

Pg.2

(3) Kaspersky Lab 『Cyberthreat Landscape 2009: Outcomes, Trends and Forecasts』モスクワ 2010年1月28日

(4) VeriSign 『The Domain Name Industry Brief』 2009年12月

<http://www.verisign.com/domain-name-services/domain-information-center/industry-brief/>