

モバイルセキュリティの要はクラウドにあり

アンチウイルス（ウイルス対策ソフト）だけで万全を期すことはできません。リモート環境やモバイル環境にいる従業員にはクラウドベースの Web フィルタリングによる万全のセキュリティ対策を施すことが重要です。

最近では従業員がモバイル環境やリモート環境にいるのは例外どころか当たり前の状況になっています。そもそも従業員が本社から離れて仕事をこなすようになった背景には、顧客満足度向上の目的が挙げられます。それに加えて昨今の景気後退や、経費削減と環境保護対策を兼ねた在宅勤務の推進などもあって、勤務地の分散化が進んでいます。ブルーコートの製品管理・製品マーケティング担当バイスプレジデント、キャリア・オクスが「今や社外でも仕事をするのは当たり前」と言うように、技術が大きく進歩している結果、本社から離れたところにいる従業員であっても、内勤の同僚とほぼ変わらないコンピュータ環境をノート PC で実現できるようになりました。

時間や場所を問わない働き方が広がると、ノート PC で個人的な作業をすることも普通になります。「会社からノート PC が支給され、社外で仕事をするようになると、オフィスにいるときに比べて業務と無関係のネットサーフィンの量も飛躍的に増加します」とオクス・バイスプレジデントは指摘します。仕事用の PC でニュースやスポーツのサイトの情報を丹念に読み、お気に入りのソーシャルメディア系サイトをチェックし、ゲームに没頭することもあります。「こうした行動の 1 つ 1 つがサイバー犯に狙われ、マルウェアを仕込まれたり、情報を盗まれたりする恐れがある」と同氏は述べています。

こうした問題に対して、きわめて厳格なインターネット利用ポリシーで従業員を縛る企業もありますが、ほとんどの企業は息抜き程度のネットサーフィンを許可しています。「セキュリティ上のリスクは、業務外のネットサーフィンに起因するものが大部分を占めるからといって、IT 部門が業務外ネットサーフィンに目を光らせていては、従業員の満足度に影響が出るだけでなく、ことによっては会社の責任問題にも発展しかねません」とオクス・バイスプレジデントは指摘します。IT 部門にとっては、満足度の高い労働環境を従業員に提供するとともに、従業員が夜間や週末に仕事をする場合には安全性を確保するよう周知徹底できるかどうかのポイントです。

そんなときこそクラウドベースの Web フィルタリングサービス

IT 部門では、ネットワークレベルのマルウェア対策としては以前からゲートウェイに Web フィルタリングを導入してきましたが、モバイル利用の普及に伴ってエンドポイントでの Web フィルタリングが必須となっています。前出のオクス・バイスプレジデントは「すべてのクライアントのセキュリティ要件としてアンチウイルスと Web フィルタリングはどちらも不可欠の機能になりつつあります。アンチウイルスがあっても Web フィルタリングがなければ万全とは言えません」と言います。

クラウドベースの Web フィルタリングの場合、モバイル環境のクライアントでもゼロデイ攻撃の脅威からユーザーを保護できます。新種の脅威が出現した場合、新たに見つかった脆弱性やゼロデイ攻撃の脅威に対応するシグネチャファイルをアンチウイルスベンダーが作成してシグネチャ更新ファイルを大量配布するまでに、完全無防備な「空白の期間」が生まれます。クラウドベースの Web フィルタリングであれば、脆弱

性対策が間に合わない空白期間の対応に威力を発揮します。クラウドベースの Web フィルタリングの場合、例えばユーザーが Twitter などインスタントメッセージングのリンクをクリックしたとき、ブラウザを開いたとき、あるいは埋め込みコンテンツのあるメールを受け取ったときなど、クラウド上の最新情報に照らしてリンク先が安全かどうかを検証します。この方式こそ、Blue Coat WebPulse™によるサービスそのものにほかなりません。

セキュリティ対策の一環として Web フィルタリングの導入を検討する際、重視したいのは次の 4 つの機能です。

- **クラウドベースのサービス**：ひとくちに Web フィルタリングソリューションと言っても、ローカル環境にあるクライアント用データベースで URL の安全性を判断するソリューションの場合、アンチウィルスのシグネチャファイル更新と同様に、対応策が用意されるまでに空白期間が生じます。常に最新情報に基づいて保護できるのは、クラウドベースの Web フィルタリング以外にありません。「クライアント側から見れば、URL データベースがクラウド上に存在すること自体に最大の価値があります。ユーザーはいつでも即座に最新情報を利用できるため、更新作業も中断も不要で、空白期間もありません」（オークス・バイスプレジデント）。

クラウドベースのサービスは、クライアント側でポリシーの定義や管理を実施します。このため、IT 部門にとっては自社にふさわしい利用ポリシーを手軽に設定して適用できます。例えば、平日の午前 8 時から午後 5 時まではユーザーがスポーツ系サイトにアクセスするのを禁止し、それ以外の曜日・時間はアクセスを許可するといった具合に柔軟に設定できます。

Blue Coat WebPulse™のクラウドサービスは、ダイナミックリンクを利用して悪意のあるコンテンツを流布しようとする Web 2.0 型の脅威を発見し、危険度を判定します。新たに出現したサイト、URL、動的な Web2.0 コンテンツやリンクについて、多様なユーザーの参加で常に拡大を続けているコミュニティからリアルタイムの情報が WebPulse のサービスに提供されます。

- **クラウド側で URL を動的分析**：未知の URL に出会ったとき、それが悪意のあるサイトかどうか迅速に判断することは非常に重要です。実際、アンチウィルス製品ベンダーのソフォスによれば、インターネット上では、毎日 20,000 もの URL でセキュリティに問題が生じています。その大多数は本物の Web サイトが攻撃などによって脅威にさらされた結果ですが、その一方、サイバー犯の手で作られられる危険なサイトも毎日、多数出現しています。さらに Google の推定によれば、2008 年の時点で Web ページの総数は 1 兆に及び、それから 1 年経った今、Web ページ数はさらに増加の一途をたどっています。「この事実から考えれば、ユーザーがいつ未知のページに遭遇しても何ら不思議ではありません」（オークス・バイスプレジデント）。

その解決策となるのが、Web フィルタリングシステムです。Web ページの危険度を吟味したうえで、ユーザーにアクセスのゴーサインを出します。WebPulse の動的なリアルタイム格付けサービスは、対象となるページをほぼ瞬時に分析して格付けします。オークス・バイスプレジデントは「ブルーコート技術の場合、リアルタイムの防御機能はコストパフォーマンスに優れているため、コスト自体が気になることもありません。処理もほんの一瞬で終わります」と話しています。

WebPulse は 50 カ国語以上の言語のコンテンツを分類できます。例えば金融系のサイトのように、リスクがあるとわかっているカテゴリーに分類される場合、WebPulse はさらに詳細フィルタリングを実行してフィッシングサイトの疑いがあるかどうかをチェックします。

- 悪意がありそうな未知の URL からの防御**：あるユーザーが未知の URL のリンクに遭遇した場合、リンク先にウイルス感染の疑いのある実行ファイルや PDF ファイルがあるかもしれません。WebPulse コミュニティには 6200 万人以上が参加していますが、最初に不審なリンクに遭遇するユーザーはどうなってしまうのでしょうか。実は WebPulse の場合、たとえゼロデイ攻撃であってもユーザーは保護されます。WebPulse から「該当カテゴリなし」の格付けが返されると、ブルーコート推奨のポリシーでは素性の知れない URL からマルウェアの疑いのあるコンテンツはダウンロードしません。ただし IT 管理者が別のポリシーを選択することで他の対応方法をとることも可能です。

ユーザーに見えない舞台裏では、WebPulse のバックグラウンド格付け機能が問題のファイルをダウンロードして分析しています。ファイルはさまざまなアンチウイルススキャナで吟味され、各種シグネチャとの比較、ヒューリスティック分析、サンドボックスによるチェック、スクリプト解析などの手法を組み合わせ、当該ファイルに脅威があるかどうかを判定します。分析作業の結果、危険な URL と判定された場合、ただちに WebPulse のデータベースに登録されます。オクス・バイスプレジデントによれば「新種のマルウェアを発見する作業は 10 分とかかりません」。

- コミュニティの力**：Web フィルタリングソリューションには、インターネットコミュニティの力が生かされています。「WebPulse では、コミュニティメンバーのインターネット利用時にクラウドサービスが収集した情報に基づいて、コミュニティの全ユーザーが保護されます」（オクス・バイスプレジデント）。このため、空港、カフェ、ホテル客室で仕事をする場合はもちろん、在宅勤務時でもリスクが軽減されます。

クラウドベースの Web フィルタリングには、もう 1 つ重要なメリットがあります。ブルーコートユーザーの報告によれば、手元のアンチウイルスで検出される脅威の数が 97% も減少した例もあります。これは、WebPulse がマルウェアへのリンクをブロックし、感染ファイルをユーザー側のシステムに侵入させなくなった成果にほかなりません。「境界部分で脅威を阻止するため、ユーザーのところまで到達しないのです」とオクス・バイスプレジデントは説明します。この結果、出先での作業もわずかながら高速化して楽になり、生産性アップにつながります。

いつでもどこでも仕事ができる環境があれば、従業員の生産性は明らかに向上します。今日の厳しい経済情勢では特に生産性アップが欠かせません。しかし、いつでもどこでも仕事ができる環境は、思わぬセキュリティ上のリスクも生み出します。その点、クラウドベースの Web フィルタリングであれば、リモート環境やモバイル環境で仕事をこなすツールを従業員に提供するだけでなく、どこで仕事をしていてもマルウェアなどインターネットに潜む脅威からしっかり保護されているという安心感も与えることができます。

ブルーコートシステムズ合同会社

〒105-0021 東京都港区東新橋 1-9-2 汐留住友ビル 16 階

Tel 03-6251-9111 (代表) Fax 03-6251-9112 Mail Japan.info@bluecoat.com URL <http://www.bluecoat.co.jp>

Copyright©2009 Blue Coat Systems, Inc. All rights reserved worldwide.

Blue Coat, Blue Coat のロゴはアメリカ合衆国およびその他の国々における Blue Coat Systems, Inc. の商標または登録商標です。その他の製品名及び会社名は各社の登録商標または商号である可能性があります。仕様は予告なく変更となることがあります。