

ブラウザ・セキュリティで
エンドポイントおよび企業全体を
Webベースの攻撃から保護



Contents

本書の内容

はじめに	3
問題：Webの利用拡大がもたらしたセキュリティ・リスクの増大	3
名声ではなく金銭的利益を求めようになったハッカー	4
従来型のセキュリティ対策でWebベースの攻撃を防げない理由	5
シグネチャベースのソリューション	5
ファイアウォール	5
新しいセキュリティ対策が求められるWebトランザクション	6
シグネチャが不要な技術	6
チェック・ポイントのWebCheckとは	6
高精度エミュレーション	7
WebCheckの仕組み	7
インターネット上の脅威に対する防御	7
アクティブ・セーフティ機能	7
必要不可欠なセキュリティ・レイヤ	9
WebCheckの利点	9
各種ブラウザをサポート	9
集中管理とログ機能	9
シグネチャには依存しない	9
あらゆる状況で常にPCを保護	9
快適な動作	10
まとめ	10
付録I：高精度エミュレーション技術について	10
WebCheckを使用しない場合	11
WebCheckを使用する場合	11

はじめに

新しいタイプのWebベースの脅威が出現している今日、企業には、従来よりも一層優れたセキュリティ対策を実施することが求められています。エンドポイントを狙う脅威の多くは、これまででも有効に機能していた攻撃手法と、さらに巧妙化した新しい配布および感染の手法を組み合わせるようになっていきました。この結果、エンドポイントに対する攻撃は防御が非常に難しく、以前の攻撃よりもさらに深刻な被害をもたらすようになっています。

この技術白書では、新しいタイプのWebベースの攻撃が登場してきた背景とその特徴、そしてWebベースの攻撃がこれほどまでに広がっている理由について解説します。ここで理解する必要があるのは、従来型のエンドポイント・セキュリティ対策は依然として重要であるものの、焦点を当てるべき対象が適切ではないために、新しいWebベースの攻撃には十分に対処することができないという点です。

強力なWebセキュリティを実現するためには、ソフトウェアやその設定だけでなく、ユーザの行動も管理の対象とする必要があります。シグネチャベースのセキュリティ・ソフトウェアだけで新しいタイプの攻撃を防ぐことはできません。また、悪意のあるソフトウェアが見つかった場合にそれを駆除するだけというような対策では、最新の攻撃に対処することはできません。本書の後半からは、これらのWebベースの攻撃に対するチェック・ポイントの企業向けソリューション「WebCheck™ for Check Point Endpoint Security」について説明します。

問題：Webの利用拡大がもたらしたセキュリティ・リスクの増大

今日のハッカーは、企業の社員や派遣社員などが行うWeb閲覧操作を狙って企業データを盗み、金銭的利益を得ようとしています。Web閲覧に企業PCが使用された場合、その操作が業務上のものであるか私的なものであるかに関係なく、データが盗み出される可能性があります。ハッカーは、ユーザのオンライン活動を逐一追跡し、あらゆる手段を用いてユーザのほんのわずかな隙を突こうとするのです。

多くの企業は、セキュリティに関して誤った認識を持っています。つまり、従来型のエンドポイント・セキュリティ対策では、Webベースの脅威に対して十分な効果が得られないにもかかわらず、そのように認識している企業は少ないということです。以下に、ハッカーなどの犯罪者グループがインターネットを利用して悪意のあるプログラムを配布した最近の事例を示します。これは、数あるインシデントのほんの一例に過ぎません。

- 2009年6月、「Nine Ball」と呼ばれる大規模攻撃によって4万以上のWebサイトが改ざんされました。Nine Ballは、これらのサイトのページにマルウェアを埋め込み、そのページを閲覧したユーザを別のサイトにリダイレクトしてさらなるマルウェアをダウンロードさせようとしています。¹
- 2009年5月、「Gumblar」と呼ばれるWebサイト改ざん攻撃が短期間の間に連続して行われ、メディアの注目を集めました。Gumblarに感染したWebサイトを閲覧したユーザは、キーロガーなどのマルウェアをダウンロードさせられます。²
- 2009年2月、バラク・オバマ大統領のキャンペーン用ブログ・サイトであるmy.barackobama.comが、マルウェアへの感染を引き起こすコンテンツに訪問者を誘導するために悪用されました。³
- 2009年2月、米政府の旅行サイトであるgovtrip.comがハッキングされ、政府関係者をマルウェアに感染させるために使用されました。⁴
- 2008年9月、SQLインジェクション攻撃によってBusiness WeekのWebサイトにマルウェアが埋め込まれました。Googleの統計によると、同サイト全体の10%にあたるページが改ざんされ、訪問者がマルウェアに感染するように細工されていました。⁵

¹ <http://www.networkworld.com/news/2009/061609-nineball-websense-attack.html?hpg1=bn>

² http://news.cnet.com/8301-1009_3-10244529-83.html

³ http://www.xiom.com/whid/2009/14/My.BarackObama.com_Infects_Visitors_With_Trojan

⁴ http://www.xiom.com/whid/2009/22/federal_travel_booking_site_spreads_malware

⁵ <http://www.xiom.com/whid-2008-35>

新たな攻撃がもたらすリスクの増大

- PCベースではなくWebベースが主流
- 金銭的利益が目的
- 目立たないように活動
- ソーシャル・エンジニアリングを活用
- 感染力を持つ
- 短期間のうちに変異

名声ではなく金銭的利益を求めようになったハッカー

ハッキングという行為は、10年ほど前までは世間の注目を集めるためにウイルスを作成するといった種類のもので主流でしたが、今日では、水面下で行われるより悪質性の高い行為へと変化しています。その結果、今日の企業は以前よりもはるかに厄介なインターネット上の脅威にさらされるうえ、それらに対抗する術もないという状況に置かれるようになっていきます。

10年前、ハッキングは主に名声を得るために行われており、金銭的利益を動機とするものはそれほど多くありませんでした。高度なトロイの木馬や攻撃手法は存在していたものの、今日のように、それらが金銭的利益を得るために使われることはほとんどなかったのです。メディアで盛んに取り上げられた電子メール・ウイルスの「I Love You」や「Melissa」のように、従来の攻撃は人目を引くように行われ、広範囲に影響を及ぼしました。多くの企業は、こうしたマルウェアへの対策として、シグネチャベースのアンチウイルス製品などのデスクトップ・アプリケーションや、ファイアウォールなどのゲートウェイ・セキュリティ・アプリケーションを導入しました。

しかし今日では、金銭的な利益がハッキングの新たな目的になっています。その背景としては、非常に多くのユーザがインターネット上で金融取引を行うようになったことで、金銭的利益を得られる機会が大きくなったということが挙げられます。PayPalやeGoldなどのサービスを使えば、簡単に匿名での送金を行うことができます。また、手軽に使用できるハッキング・ツールが登場し、それほどスキルのない個人が利用するようになっただけでなく、国際的な犯罪者組織も新たな収益源として、あるいは高コストで高リスクな従来型の犯罪手法から脱却する手段としてハッカーの力を求めるようになっていきます。高度で複雑な犯罪手法がウイルスやトロイの木馬、ワームなどと融合し、スパイウェアやアドウェア、キーロガー、rootkitといった従来型の攻撃手法を超える威力を持つようになったのです。新しいタイプのWebベースの攻撃には、大きく次の3つの特徴があります。

- 目立たないように活動する。これは、感染先のPC上で存在を気付かれないようにすることを目的としています。そのため、PCは感染してもパフォーマンスや安定性がわずかに低下するといった程度の症状しか表れません。
- 攻撃対象が特定されており、発覚や検知を免れるため極めて少ない数しか使用されない。そのため、特定の脅威がメディアで大きく取り上げられることが少なくなっています。
- 深刻な被害。ユーザがまったく気づかないうちに個人データや個人情報が盗まれたり、PCが乗っ取られボットネット（集中コントロールして大規模攻撃を仕掛けるために利用できる大量のコンピュータ群）として悪用される場合があります。

Webベースの攻撃では、ドライブバイ・ダウンロード（自動ダウンロード）や、PHPおよびAjaxの脆弱性の悪用が行われる場合もあります。これらはいずれも、最近の攻撃で特に多く使用されています。これらの攻撃は金銭的利益を得ることを目的とし、被害が深刻で、多くの場合目立たないように活動します。また、以前の脅威と同様に感染力を持ち、広範囲に拡散します。

多くの企業は、Webベースの攻撃を防げるだけのインターネット・セキュリティ対策をすでに講じていると考えていますが、実際には対策はまだ不十分なのが現状です。そして残念ながら、エンドポイント・セキュリティ・ソフトウェアを提供しているベンダーのほとんどは、これら最新のWebベースの脅威による攻撃を防ぐことのできる製品をまだ提供できていないのです。

従来型のセキュリティ対策でWebベースの攻撃を防げない理由

PCベースのセキュリティ・ソフトウェアは、今日でも依然として非常に重要な存在ではありますが、新しいWebベースの攻撃に対処するために十分な機能を備えているとはいえません。各タイプのソリューションは、少なくとも1つの重要な問題を抱えています。

シグネチャ・ベースのソリューション

このタイプのソリューションに該当するのは、アンチウイルスやアンチスパイウェア、シグネチャ・ベースの侵入防御システム (IPS) といったPCベースのセキュリティ・ソフトウェアです。

10年前、シグネチャ・ベースのソリューションは、新しい攻撃に対応することに問題を抱えていました。これは、昨今のような自動化され、頻繁に変異し、わずかな数しか流通しないカスタム型の攻撃が登場する以前の話ですから、今日のマルウェアの姿を見れば、専門家やアナリストらによってアンチウイルスの凋落やその死を主張する論考が数多く発表されているのも当然といえます。¹

アンチウイルスの問題点は、1998年の「Morris」ワーム、1999年の「Melissa」、そして2000年の「I Love You」に素早く対応することができなかったという点に表れています。これらはいずれもメールで大量送信され、変異のペースがそれほど早くない比較的「ローテク」なウイルスです。このようなウイルスですらうまく対処できなかったアンチウイルス（およびその類似技術であるアンチスパイウェア、IDSなど）が、複合化し一層洗練された最新のウイルスやワームにどうやって対応するのでしょうか。実際問題として対応できていない訳ですが、最近の脅威の問題点は、数百万ではなく数千といった単位で少数しか流通せず、常に変異し、感染先のPCごとに自らの特徴（シグネチャ）を変え、ユーザの注意を引こうとするのではなく自らの存在を隠べいしようとするところなのです。

アンチウイルスやアンチスパイウェアなどのセキュリティ・ソリューションは、攻撃を受けた後の駆除作業には効果的ですが、ゼロアワー型のWebベースの攻撃に対してはほとんど無力です。

ファイアウォール

デスクトップ・ファイアウォールは、シグネチャ・ベースのセキュリティ・ソフトウェアが無力なゼロアワー攻撃や変異、標的型のネットワーク攻撃に対しても有効に機能します。これが可能であるのは、デスクトップ・ファイアウォールが、ユーザや管理者が明示的に許可していないすべてのトラフィックの着信を禁止するという簡潔で明快なルールに基づいて動作するからです。

「無害と分かっているもの以外はすべて拒否」というこのルールは、「あきらかに有害であると分かっているもの以外はすべて許可」というシグネチャ・ベースの製品のルールとは対照的です。脅威の侵入を防ぎ、PCを保護するという点において、ファイアウォールがシグネチャ・ベースのソリューションよりはるかに効果的であるのは明らかです。

しかし、デスクトップ・ファイアウォールにもいくつかの欠点があります。まず、デスクトップ・ファイアウォールは通常、ユーザが要求したTCPの80番ポート（HTTPトラフィックの標準ポート）でのトラフィックを許可します。つまり、ユーザがHTTP接続を開始した場合、ファイアウォールはPCに着信するHTTPトラフィックをそのまま許可することになります。この結果、ファイアウォールが動作するPCの80%以上にスパイウェアなどのマルウェアが存在していることが多くの報告で指摘される状況となっています。²

またファイアウォールは、「ユーザの行動」ではなく「ユーザのコンピュータ」を保護することに焦点を当てています。ほとんどの場合、ユーザとマルウェアがオンラインで直接やり取りすることを防ぐことはできません。

¹ <http://havemacwillblog.com/campaigns/the-avid-campaign/>

² Check Point ZoneAlarmの統計による

他の何にも代えられないネットワーク・ベースの保護を提供するデスクトップ・ファイアウォールは、依然としてエンドポイント・セキュリティに不可欠な要素であり続けています。しかし、ことWebベースの攻撃に関しては、十分な効果を発揮しているとはいえないのが現状です。

新しいセキュリティ対策が求められるWebトランザクション

新しいタイプのWebベースの脅威が出現したことを受けて、ユーザのWeb閲覧を保護する新しいシグネチャ・ベースのセキュリティ・ソリューションが登場しています。これらのトランザクション・セキュリティ製品は、フィッシング・サイトやスパイウェア配布サイトといった既知の悪意あるWebサイトのシグネチャを使用します。この種の製品の中には、悪意あるWebサイトの振る舞いを検出するシグネチャを利用するものもあります。これらの情報に基づいてより一般的なレベルで悪意あるWebサイトを識別し、ユーザがそれらのサイトにアクセスするのを防いで、PC環境の安全性を保ちます。

これらのシグネチャ・ベースのソリューションは、新しいタイプのWebベースの攻撃にいち早く対応できるものの、この種の攻撃に対して最も効果的であるとはいえません。これらは副次的なソリューションとしては有効ですが、動的に変異してシグネチャ・システムをすり抜ける脅威には対応できません。今日のウイルスがアンチウイルス・システムをすり抜けるように、最新のWebベースの攻撃はこれらのシグネチャ・ベースのWebトランザクション・セキュリティ製品をすり抜けてしまいます。

シグネチャが不要な技術

シグネチャを使用することなくWebベースの攻撃に対処できる技術もいくつか登場してきています。このタイプの技術は、次の2つに分類することができます。

手動の仮想化システム:この種のシステムは、ホスト・コンピュータのすべてまたは一部を仮想化し、インターネット側からPCに対して実行されるすべての変更操作が仮想化されたシステムで行われるようにします。これにより、有害なプログラムなどがインターネットからPCに侵入するのを防ぐことが可能です。非常に洗練された手法であるように思えますが、このタイプのソリューションでは、仮想マシン/仮想ファイル・システムと実マシン/実ファイル・システムの両方を管理する必要が生じます。また、両方のシステムについて継続的に何らかの判断を下すことが求められます。これは、一般的な企業ユーザには受け入れられないか、そもそもこうした判断を下すことができない可能性があります。

メソッド・ブロック・システム:これは、ユーザを悪意あるコードで攻撃することを可能にするWebブラウザの既知の脆弱性に焦点を当てた技術です。例えば、クロスサイト・スクリプティングの脆弱性がある場合、ハッカーは第三者のWebページに悪意のあるコードを埋め込むことができます。メソッド・ブロック・システムは、このような動作を妨害し、攻撃を実行するためのメソッドを取り除きます。この種のシステムは重要かつ必要なものですが、一部の攻撃手法(通常は1つのみ)しかブロックできず、Webベースの攻撃で使用されるさまざまな手法に単独に対処できないという点が欠点となります。

チェック・ポイントのWebCheckとは

WebCheckは、トランザクション・セキュリティなどの従来のセキュリティ技術とは異なり、あらゆるWebベースの攻撃からユーザを保護することに特化して設計されています。WebCheckの要となる技術は、Webサイトの閲覧時に通信全体を保護する仮想化エンジンです。この技術の主な目的は、シンプルかつシームレスにユーザを保護することにあります。

高精度エミュレーション

WebCheckの高精度なエミュレーション技術により、Webブラウザがアクセスするオペレーティング・システムの一部のみが仮想化され、構築された仮想システムは自動的に維持されます。したがって、導入は簡単に行うことができ、システム・メモリの使用率やパフォーマンスの低下について頭を悩ませる必要もありません。複数のオペレーティング・システムやファイル・システムの監視も不要となります。

WebCheckの仕組み

ユーザがWebサイトを閲覧するとコンピュータ・システムにさまざまな変更が加えられますが、こうした変更のほとんどは無害です。例えば、ユーザ登録のためにWebサイトのオンライン・フォームに情報を入力すると、たいいていの場合Webサーバはcookieを作成してユーザのコンピュータに保存します。

ハッカーは、Webアクセスにより生じる有用で無害な変更の中に悪意ある変更を忍び込ませます。WebCheckは、シグネチャを必要とすることなく、オペレーティング・システム・レベル/ブラウザ・レベルでこうした脅威から企業や従業員を保護します。

インターネット上の脅威に対する防御

WebCheckの仮想化エンジンには、ファイアウォールのようにシンプルなルールが採用されています。ユーザによって要求されたダウンロード・ファイルは通常通りコンピュータに書き込まれますが、ドライブバイ・ダウンロードなどによってユーザの許可なくダウンロードされたファイルはエミュレーション・レイヤに書き込まれ、コンピュータには影響を及ぼしません。

Webブラウザの脆弱性を突く攻撃やドライブバイ・ダウンロード、スパイウェア、ウイルスなどによる有害な変更はすべて仮想ファイル・システム上で行われるため、ユーザは安全にWebサイトを閲覧したりリンクをクリックしたりすることが可能です。ユーザが意図的にダウンロードしたファイルのみがエンドポイントに保存されます。

仮想化エンジンによる保護が有効であるかどうかをWebブラウザで確認するには、2つの方法があります。ひとつは、Webブラウザのタイトルバーに表示されるメッセージです。WebCheckが有効であるといった内容が示されます。もうひとつは、Webブラウザのウィンドウを囲む薄い枠線です。

仮想化レイヤは随時リセットすることができます。仮想化レイヤをリセットすると、Webブラウザも初期状態にリセットされます。

アクティブ・セーフティ機能

仮想化レイヤがユーザを保護すると同時に、アクティブ・セーフティ機能によって既存の保護レイヤに対する追加レイヤや新しい保護レイヤが提供されます。

WebCheckは、フィッシング・サイトへのアクセスを防ぐため、フィッシング・シグネチャ・データベースと先進のヒューリスティック検出機能を搭載したデュアル・モードのアンチフィッシング・エンジンを使用しています。ユーザが既知のフィッシング・サイトへアクセスすると、シグネチャ・ベースの検出エンジンによって以下のような警告が表示されます。

システムの内部を 保護する 高精度エミュレーション

WebCheckの
高精度エミュレーションは、
Microsoft Windowsインターフェース
がファイルやレジストリ・キーに直接
アクセスするのを防止する技術です。
詳細については、付録Iを
参照してください。

優れた ヒューリスティック技術

WebCheckは、事前対応型のヒューリスティック・アンチフィッシング機能を備えています。以下をはじめとして、50を超える大手Webサイトが登録されています。

銀行サイト

- Bank of America
- Citibank
- Wells Fargo

コマース系サイト

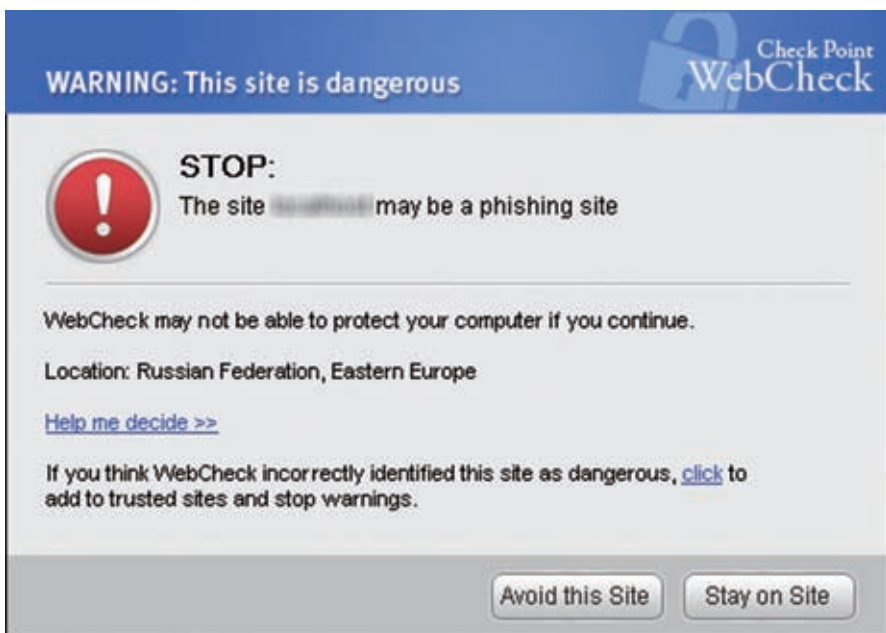
- eBay
- PayPal
- Amazon

SNS / Webメール

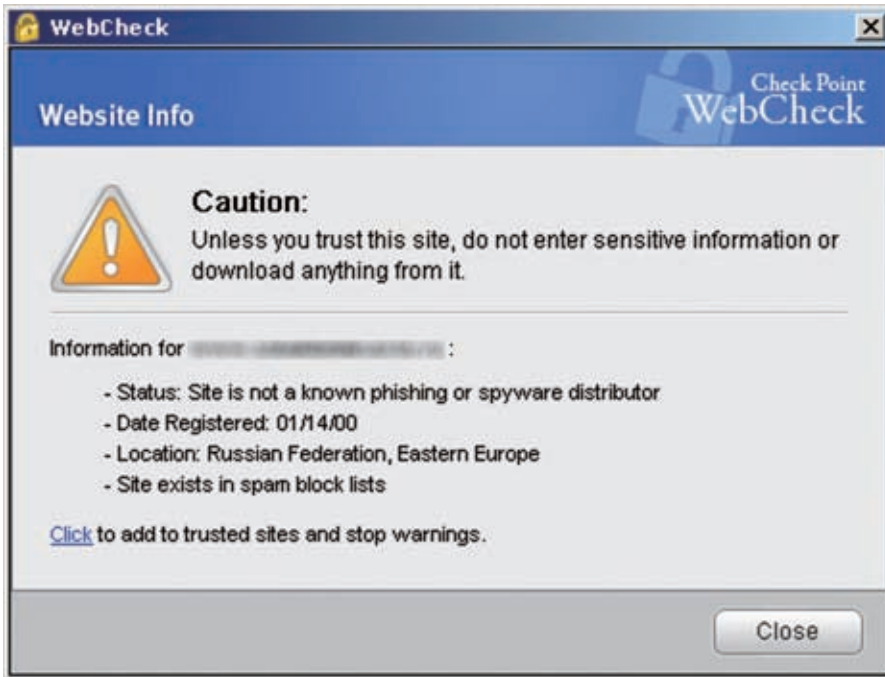
- MySpace
- Yahoo Mail
- MSN Hotmail



シグネチャとスパム・ブロック・リストだけでは、すべてのフィッシング・サイトを検出することはできません。この問題に対処するため、チェック・ポイントはフィッシング・サイトのヒューリスティック検出エンジンを開発しました。この検出エンジンには、50を超える金融サイト、ソーシャル・ネットワークワーキング・サイト、ショッピング・サイトが登録されており、登録サイトに見せかけた偽のフィッシング・サイトを検出することが可能です。ヒューリスティック検出エンジンがフィッシング・サイトを検出すると、以下のような警告がWebブラウザに表示されます。



WebCheckはまた、訪問先サイトの証明書の信頼性が不十分であるなど不審な点がある場合、サイトの評価を行ってユーザに警告します。ドメインはいつ取得されたか、スパム・ブロック・リストにIPアドレスが記載されていないか、どの国でホストされているかなど、さまざまな属性が検証され、危険なサイトでないかどうか判断されます。疑わしいサイトである場合は、以下のような警告でユーザに注意を促します。



必要不可欠なセキュリティ・レイヤ

WebCheckは、新たなセキュリティ・レイヤを追加したことにより、フィッシング・サイトや悪意のあるドライブバイ・ダウンロード、レジストリの不正な変更、アドウェア、スパイウェアとして機能するcookieなど、システムに悪影響を及ぼすさまざまな脅威に対し極めて強力な防御を実現しています。WebCheckは、Microsoft Internet ExplorerおよびMozilla Firefoxで動作します。

WebCheckの利点

各種ブラウザをサポート

WebCheckはMicrosoft Internet Explorer 6、7、8およびMozilla Firefox 2、3をサポートしており、どのWebブラウザでも同等のセキュリティを提供します。最新バージョン以外のWebブラウザであっても安全なインターネット環境を実現可能です。

集中管理とログ機能

Check Point Endpoint Securityが備えるシンプルなポリシー管理機能により、さまざまな種類/バージョンのWebブラウザが混在する環境でも一貫したセキュリティを維持することが可能です。また、ログの集中管理機能では、企業全体におけるすべてのブラウザ・セキュリティ・イベントを素早く詳細に確認することができます。

シグネチャには依存しない

先進のシグネチャも重要な役割を果たしますが、十分とは言えません。WebCheckのように、「ユーザーが明示的に要求したものでない限りはPCへの変更を破棄する」といったファイアウォールと同様のシンプルなルールが採用され、ゼロアワールの脅威にも対処可能なシステムと組み合わせる必要があります。

あらゆる状況で常にPCを保護

Webベースの攻撃はユーザーがWebサイトを閲覧した瞬間に発生します。そのためWebCheckは、インターネットからPCにマルウェアが送られてくるのを待つのではなく、仮想化レイヤおよびセキュリティ・レイヤによって常にプロアクティブな防御機能を提供します。

快適な動作

管理者は、特別な設定やメンテナンスを行う必要はありません。仮想化アクティビティはすべてユーザからは透過的に行われ、メンテナンスは一切不要です。ただし、データ消失の恐れが高い場合にのみ、ユーザにアクションが求められます。

WebCheckの機能	説明
Webブラウザの仮想化	Webブラウザ・プラグインの脆弱性やドライブバイ・ダウンロードに対するプロアクティブな防御
セキュリティ・ポリシーの集中管理	IE 6、7、8およびFirefox 2、3の集中セキュリティ管理をサポート
ログおよびレポートの集中管理	ブラウザのセキュリティ・イベントをログに記録し、レポートを生成
アンチフィッシング(シグネチャ)	既知のフィッシング・サイトにアクセスした場合、ユーザに警告
アンチフィッシング(ヒューリスティック)	Webサイトの属性を検証し、正規サイトを装ったフィッシング・サイトかどうかを識別
Webサイトのステータス・チェック	不審なサイトにアクセスした場合、ユーザに警告

まとめ

極めて巧妙な手法と従来の攻撃の特性を組み合わせたWebベースの脅威が出現したことで、Webのセキュリティ環境は大きく変化しました。従来のセキュリティ対策では、最新の脅威に対しある程度は有効であるものの、昨今頻発しているWebベースの攻撃から企業PCやユーザの個人情報を効果的に保護することはできません。

今日のWebベースの攻撃に対処するには、第三世代のソリューションが必要です。第三世代のソリューションには、最新のシグネチャ・ベースのセキュリティや、ウイルスやスパイウェアの新しい駆除メカニズム、新世代のファイアウォールといった技術をさらに上回る保護機能を提供することが求められます。

Webベースの攻撃に対して防御するには、二重のアプローチをとる必要があります。従来のセキュリティの利点と、現在主流となっている脆弱性を突く攻撃を防ぐためのWebセキュリティを統合することがまずひとつです。さらに、PCを保護するために仮想化技術を導入します。これにより、エンドポイントPCのオペレーティング・システムやファイル・システムがWebブラウザを経由して不正に書き換えられることを防ぐことができます。

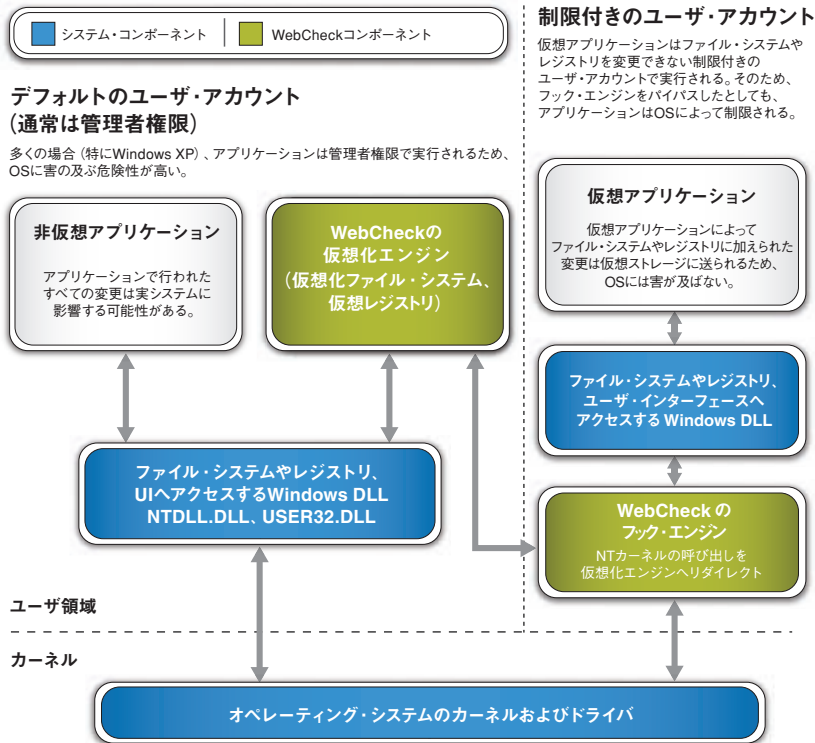
画期的かつ効果的な最新技術が統合されたチェック・ポイントのWebCheckは、企業PCの保護に最適なセキュリティ・ソリューションです。

付録I: 高精度エミュレーション技術について

チェック・ポイントのWebCheckによる高精度エミュレーション技術は、Microsoft Windows インターフェースがファイルやレジストリ・キーに直接アクセスすることを防止する技術です。以下の図に示すように、WebCheckは主に2つのコンポーネントを生成します。

- 仮想化エンジン: Windowsファイルやレジストリのコピーを作成します。
- フック・エンジン: NTカーネルの呼び出しを選択的に仮想化エンジンへリダイレクトします。

WebCheckと各コンポーネントの動作の仕組み



WebCheckを使用しない場合

多くの場合、管理者権限を持つユーザ・アカウントによって、アプリケーションがオペレーティング・システムやカーネルに自在にアクセス可能となります。これにより悪意あるコードによってオペレーティング・システムが攻撃されます。

WebCheckを使用する場合

WebCheckのフック・エンジンはNTカーネルの呼び出しを制御します。フック・エンジンは、カーネルの呼び出しがユーザからの要求によるものなのか、あるいはドライブバイ・ダウンロードにより自動で行われたものなのかを判断します。この判断は、ユーザ・インターフェースの呼び出しが想定されたものであるか (ユーザの操作によるもの)、そうでないか (ドライブバイ・ダウンロードにより自動で行われたもの) に基づいて行われます。ユーザによる呼び出しは通常通り、ユーザの作業の妨げにならない形でオペレーティング・システムに対し行われます。ユーザの許可がない呼び出しは仮想化エンジンや仮想ファイル、仮想レジストリなどの仮想化環境で扱われるため、実システムに到達することはありません。Webブラウザが終了されると、仮想化レイヤはリセットされて初期状態に戻ります。

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) は、インターネット・セキュリティにおけるトップ企業として、特にネットワーク、データ、およびエンドポイントのトータル・セキュリティを単一の統合管理フレームワークで提供できる唯一のベンダーとして広く認められています。チェック・ポイントは、セキュリティの複雑さと総所有コスト (TCO) を低減しつつ、あらゆるタイプの脅威からお客様のネットワーク環境を確実に保護するための妥協のないセキュリティ機能を実現しています。チェック・ポイントは、FireWall-1と特許技術のステートフル・インスペクションを開発した業界のパイオニアです。2009年には、新たな革新的セキュリティ技術としてSoftware Bladeアーキテクチャを開発しました。Software Bladeアーキテクチャは、導入先にあわせカスタマイズすることで、あらゆる組織、あらゆる環境のセキュリティ・ニーズにも的確でダイナミックに対応できる、安全かつ柔軟でシンプルなソリューションの構築を可能にします。チェック・ポイントは、Fortune 100社の全社を含む、何万ものあらゆる規模の企業や組織を顧客としています。数々の受賞歴のあるチェック・ポイントのZoneAlarmソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、および情報窃盗から未然に保護しています。

© 2003-2009 Check Point Software Technologies Ltd. All rights reserved.

Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, ImSecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, puresecurityのロゴ, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, totalsecurityのロゴ, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Securing Browsers to Protect Endpoints and Enterprises from Web-based Attacks

P/N:600020-J 2009.07

※記載された製品仕様は予告無く変更される場合があります。

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
 〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail: info_jp@checkpoint.com Tel: 03 (5367) 2500