Windows_h_rgb.jpg



安全なオンライン エクスペリエンス

ホワイト ペーパー

2009 年 2 月

このドキュメントは暫定版であり、このソフトウェアの最終的な製品版の発売時に実質的に変更されることがあります。

このドキュメントに記載されている情報は、対象事項に関する発行時における米国 Microsoft Corporation の考えを表しています。マイクロソフトは市場の変化に対応する必要があるため、このドキュメントの内容に関する責任をマイクロソフトは問われないものとします。また、発行日以降に発表される情報の正確性を保証できません。

このホワイト ペーパーは情報提供のみを目的としています。マイクロソフトは、この文書およびその記載事項について、明示と暗示とを問わずなんら保証を行いません。

この文書およびソフトウェアを使用する場合は、適用されるすべての著作権関連の法律に従っていただくものとします。このドキュメントのいかなる部分も、米国 Microsoft Corporation の書面による許諾を受けることなく、その目的を問わず、どのような形態であっても、複製または譲渡することは禁じられています。ここでいう形態とは、複写や記録など、電子的な、または物理的なすべての手段を含みます。ただしこれは、著作権法上のお客様の権利を制限するものではありません。

マイクロソフトは、このドキュメントに記載されている事項に関して、特許、申請中特許、商標、著作権、および他の知的財産権を所有する場合があります。マイクロソフトからの書面のライセンス同意書の記載事項に従う場合を除き、このドキュメントを所持することは、その所有者にこれらの特許、商標、著作権、および他の知的財産権を付与するものではありません。

注記がない限り、例として示された会社、組織、製品、ドメイン名、電子メール アドレス、ロゴ、人名、場所、イベントは架空のものであり、実際の会社、組織、製品、ドメイン名、電子メール アドレス、ロゴ、人名、場所、イベントとは無関係です。

© 2009 Microsoft Corporation. All rights reserved.

Microsoft、Internet Explorer、Internet Explorer ロゴ、Smartscreen、Windows および Windows ロゴは Microsoft group of companies の商標です。

このドキュメントで使用されている実在の会社名および製品名は、該当各社の商標です。

目次

[はじめに 3](#_Toc225243871)

[Internet Explorer 8 がオンラインの安全を保つ方法 4](#_Toc225243872)

[サイバー犯罪はどのように実行されるのか 6](#_Toc225243873)

[利用者への攻撃に対する防御 6](#_Toc225243874)

[どうすれば安全になるのでしょう? 6](file:///C:\Documents%20and%20Settings\ksaku\デスクトップ\A%20Safer%20Online%20Experience%20FINAL(JA)%20-%20Final.docx#_Toc225243875)

[悪意のある Web サイトのブロック 7](#_Toc225243876)

[Social Engineering Attacks ソーシャル エンジニアリング攻撃 8](#_Toc225243877)

[無料のゲームや映画、テレビ番組を提供する Web サイト 9](#_Toc225243878)

[フィッシング攻撃 9](#_Toc225243879)

[コンピューターへの攻撃に対する防御 10](#_Toc225243880)

[ドライブバイ攻撃とは何か? 11](#_Toc225243881)

[結論 11](#_Toc225243882)

# はじめに

インターネットはほとんどあらゆる場面で私たちの生活を大きく広げました。関心のある情報や人々とつながり、いつでも楽しみが得られ、必要な答えが見つかり、かつてない生産性が可能になりました。しかし私たちの日常がインターネットに依存するようになるにつれて、オンライン犯罪も増大しています。

サイバー犯罪者はますます洗練され狡猾になっています。たとえば:

**マルウェア**はサイバー犯罪に使われるソフトウェアで、銀行の口座情報を盗み、すべての入力を記録し、悪意のあるソフトウェアやスパム メールを送信し、コンピューターに損害を与えます。

**フィッシング**はサイバー犯罪者が銀行のような正規の組織に成り済まし、クレジット カード番号や口座情報のような個人情報をだまし取ろうとするものです。

いずれの手口でも多くの場合、一見正当に見えて実は有害なリンクのクリックやファイルのダウンロードをさせるよう企まれています。しかしサイバー犯罪者はより巧妙な手口で Web サイトに潜り込み、あなたの知らない間にコンピューターを攻撃しています。この手口には、ますます危険な脅威となっている “クロスサイト スクリプティング” と “クリックハイジャッキング” が含まれています。

これらの脅威の多くは、単にコンピューターのソフトウェア、特に Web ブラウザーを最新の状態に更新し続けるだけで軽減できます。古いブラウザーでは今日の脅威に対処できませんし、新しいブラウザーであっても必要な水準の保護が提供できないものもあります。このホワイト ペーパーでは、オンラインでの安全を保つための Windows® Internet Explorer® 8 の新しい拡張されたセキュリティ機能について説明した上で、サイバー犯罪者の手法のいくつかについて明らかにし、実際の攻撃に対する防御の実例について一通りのご案内をいたします。

# Internet Explorer 8 がオンラインの安全を保つ方法

安全は最も重要な関心事項であるとお客様から伺っています。そのため私たちは継続的に製品の安全のための機能の有効性を監視し、サイバー犯罪者の戦術の変化に対応して防御のアプローチを進化させています。私たちは ”多層防御” 原則に基盤を置く、安全への完全なアプローチを取っています。これによりソフトウェアとサービスをよりセキュアにし、現在と将来の脅威から防御し、サイバー犯罪者が危険を及ぼすのに利用する手口をユーザーが察知し避ける手助けをします。防御機能の一部は目に見える形で詐欺的なコンテンツやサイトを避けるのに役立ちます。また一部の機能はバックグラウンドでコンピューターへの攻撃を防御するよう動作します。

こうした作業の一環として Internet Explorer 8 に、オンラインで安全を保つための業界トップの機能を詰め込みました。

私たちの製品はマルウェアやフィッシングを含む現在の脅威だけでなく、知らない間にコンピューターを危うくするような将来の脅威からあなたを保護するのに役立ちます。他のブラウザーの場合、このレベルの保護が提供できないか、サードパーティのアドオンのダウンロードや設定が必要になりますが、Internet Explorer 8 では最初から保護機能が含まれており、既定で機能が有効になっています。また現時点でウイルスや安全の問題についての 24 時間無料の電話サポートが提供されている、唯一のブラウザーです[[1]](#footnote-2)。

一例として、Internet Explorer 7 のフィッシング防止機能を向上させた SmartScreen® フィルターでは、フィッシング以上に極めて急速に増大している脅威であるマルウェアへの防御が追加されました。アンチ マルウェアの機能は、悪意のあるサイトを訪問したり悪意のあるプログラムのダウンロードを試みたりすると、警告やブロックの画面を表示する動作をします。

私たちの製品はフィッシング サイトの表示を毎月数百万回もブロックしていますが、マルウェアの脅威の規模は現在フィッシングより顕著に大きくなっています。Internet Explorer 8 が日々サイバー犯罪者のユーザーにマルウェアをインストールさせようとする企みをブロックする回数は、ユーザーへのフィッシングの企てをブロックする回数の 10 倍です。200 回のダウンロードうちの少なくとも 1 回は、Internet Explorer 8 の SmartScreen フィルターがユーザーを保護したマルウェアです。この保護機能は以前のバージョンにはなかった物です。さらに私たちの調査によれば、Internet Explorer 8 は現在市場にある他のどのブラウザーよりも、ソーシャル エンジニアリングを通じたマルウェアの攻撃に対する良い防御機能を持っています。

これがあなたやあなたの友人、家族が今すぐInternet Explorer 8 にアップグレードすべき理由です。そうする事で 40 人に 1 人が**今週**受けるであろう攻撃から守られるのです。

# サイバー犯罪はどのように実行されるのか

# どうすれば安全になるのでしょう?

すぐにできるもっとも重要な事は、ブラウザーのアップグレードです。今すぐ Internet Explorer 8 を [www.microsoft.com/ie8](http://www.microsoft.com/ie8). からダウンロードしましょう。

PC 上のその他のソフトウェアを最新に保つ事も必要です。Microsoft Update を使い、すべての重要な更新やオプションの更新をインストールします。ブラウザーのアドオンやその他のアプリケーションも最新にしましょう。

また最新のアンチウイルス製品をインストールし、パターン ファイルを常に更新すべきです。

ファイアウォールやアンチウイルス ソフトウェアからのセキュリティ警告には注意を払いましょう。ただしこのホワイト ペーパーで説明しているような偽のセキュリティ警告も警戒してください。ファイアウォールは常に有効にし、アンチウイルス ソフトウェアは更新を行いましょう。最後に、利用しているインターネット サービス プロバイダーが迷惑メール対策を提供していないか確認しましょう。そうすることで、望まない詐欺的な電子メールを受信せずに済ます事ができます。

これらの手順についての詳細や、フィッシング、マルウェア、その他の脅威についてさらに知りたい方は、[www.microsoft.com/protect](http://www.microsoft.com/protect). を訪問してください。

それではサイバー犯罪者はあなたをどのように脅かすのでしょうか?

今日のオンライン上の脅威は大きく二つの型に分類できます。**利用者への攻撃**と**コンピューターへの攻撃**です。

**利用者への攻撃**は、利用者を騙して安全でない行為をさせようとする企みです。こうした企みは無料のゲームや銀行からの電子メール、果てはセキュリティ警告のように、何かしら親切で親しみがあるように見えるでしょう。リンクをクリックしたり詐欺サイトに情報を入力するようあなたを仕向ける事で、サイバー犯罪者はあなたの銀行口座情報やお気に入りサイトのログインユーザー名とパスワードを収集し、個人情報を盗みとったりスパム メールを送信するための悪意のあるソフトウェアをインストールさせます。残念ながらこの問題では、利用しているオペレーティング システムやブラウザーを問わず、ダウンロードやリンク、サイトが信頼できるのかを判断するという重荷が利用者に背負わされる事になります。私たちはこうした脅威に対して、ユーザーが判断をくだせるように、詐欺を見抜くための情報や、この種の攻撃を避けるために必要な情報を提供する、というアプローチをとっています。

**コンピューターへの攻撃**はあまり一般的ではありませんが、同様に危険なものです。この攻撃では多くの場合、あなたの同意も自覚もなしにコンピューターに悪意のあるプログラムが送り込まれます。こうした攻撃は、訪問した Web サイトやコンピューターにインストールされているソフトウェアの脆弱性を梃にして、悪意のあるソフトウェアのインストールや個人情報の改ざんを通じて行われます。この攻撃の大半はコンピューター上のソフトウェアを最新に保つ事で回避できますが、Internet Explorer 8 にはこの種の攻撃を防ぎ、避けるための機能も含まれています。

# 利用者への攻撃に対する防御

サイバー犯罪者は常に詐欺的なソーシャル エンジニアリング攻撃を利用しており、その手口はあまり疑り深くない Web ユーザーを餌食にしています。あたかも自分の銀行から送られたように見える電子メールや、ゲームや映画などの人気のあるコンテンツを検索した結果、インスタント メッセージに含まれる無料での提供をうたったリンクや広告、ソーシャル ネットワーキング サイト (SNS) からの偽の通知など、犯罪者が試していない手口はありません。これらの攻撃はあたかも本物に見えるように仕組まれており、犠牲者が危険性に気付いた時には、既に手遅れになっていることが殆どです。マイクロソフトはより信頼性の高いブラウズができるよう、こうした攻撃の標的になった時の保護を提供する SmartScreen フィルターを Internet Explorer 8 向けに開発しました。

SmartScreen フィルターは、進化し続ける Web 上の脅威とソーシャル エンジニアリングの脅威からユーザーを保護するよう設計された一連の技術です。SmartScreen は “URL 評価基準 (URL レピュテーション ベース)” です。この機能では、ファイルのダウンロードや潜在的にフィッシング可能なサイトをホストしているサーバーの Web アドレスを評価して、悪意のあるソフトウェアの提供や個人情報の盗み取りをする既知のサイトに該当しないか判定します。

SmartScreen は、高度な情報収集と、最も問題となる最新の攻撃サイトを見つけるため毎日数百万の web アドレスを評価しようと疑いのあるサイトを報告してくださる数億人のユーザー コミュニティーによって、その機能が高められています。あなたもこのコミュニティーの一員です。もし悪意のあるソフトウェアを提供しているサイトや動作に疑いのあるサイトを見つけたら、報告してください。”セーフティ” メニューをクリックして “SmartScreen フィルター機能” を選択し、”安全でない Web サイトを報告する” をクリックします。

SmartScreen の分析は、今日出現している悪意のあるソフトウェアに対する幅広い防御を提供するために、一般的なアンチウイルス製品と同様 **Windows Defender** やマイクロソフトの**悪意のあるソフトウェアの削除ツール**と協調して機能します。

## 悪意のある Web サイトのブロック

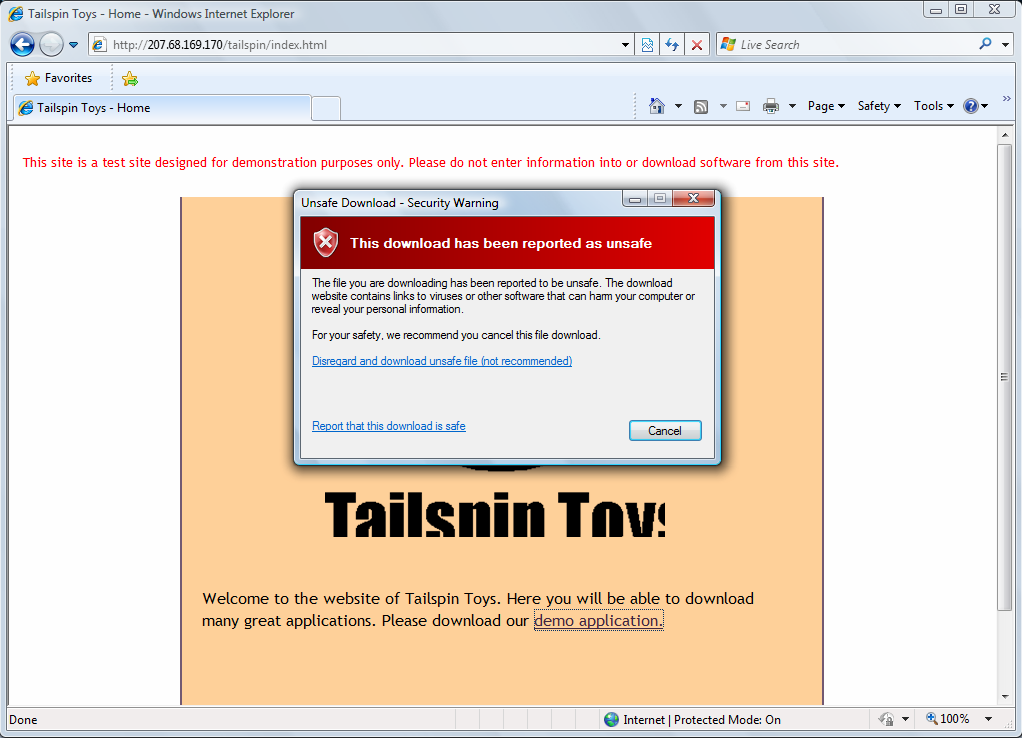
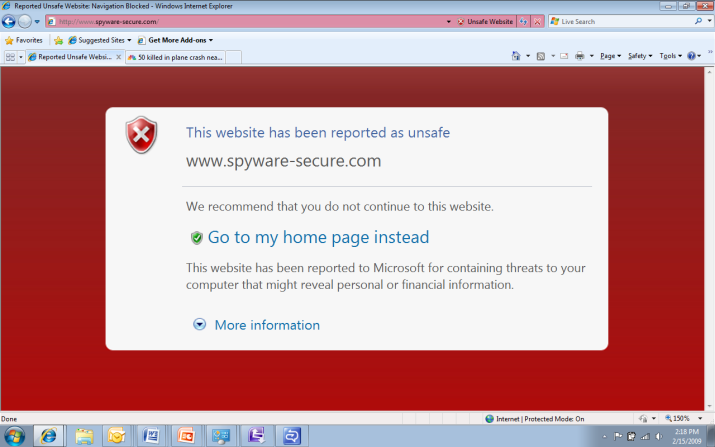
****SmartScreen が悪意のある Web サイトを検知すると、Internet Explorer 8 はサイト全体をブロックします。また正当なサイト上にホストされたマルウェアやフィッシングに対する “外科的ブロック” も行います。これはサイトの他の部分に影響を与えることなしに、悪意のあるコンテンツだけをブロックします。マルウェアを提供している既知のサイトにアクセスした場合の動作を説明しましょう。Internet Explorer 8 はページを表示せず、攻撃サイトの代わりに図 1 に示したような画面を表示します。Internet Explorer 8 では画面をより分かりやすい見え方になるようデザインを変更し、同種の攻撃を見分けて避ける方法についての為になる情報を提供するリンクも含むようにしました。もう一つの新機能は悪意のあるダウンロードからの防御です。安全でないと報告されているダウンロードを試みると、左側のような画面が表示されます。

図 1: 安全でないと報告済みのサイトやダウンロードを SmartScreen がブロックした時の表示

## Social Engineering Attacks ソーシャル エンジニアリング攻撃

サイバー犯罪者は、彼らの攻撃を正当な Web サイトやセキュリティ警告と偽るために尽力しています。攻撃サイトが識別され報告されると、SmartScreen はユーザーが犠牲になる前にこうした Web サイトを自動時にブロックできます。しかしこのようなサイトは毎日物凄い数が作り出されているので、攻撃がどのような見かけをしているのか、またどうすれば攻撃を避けられるのかを知る事は重要です。ここでは、攻撃者があなたを騙そうとする方法の例を紹介しましょう。

**偽のアンチ ウイルス警告**

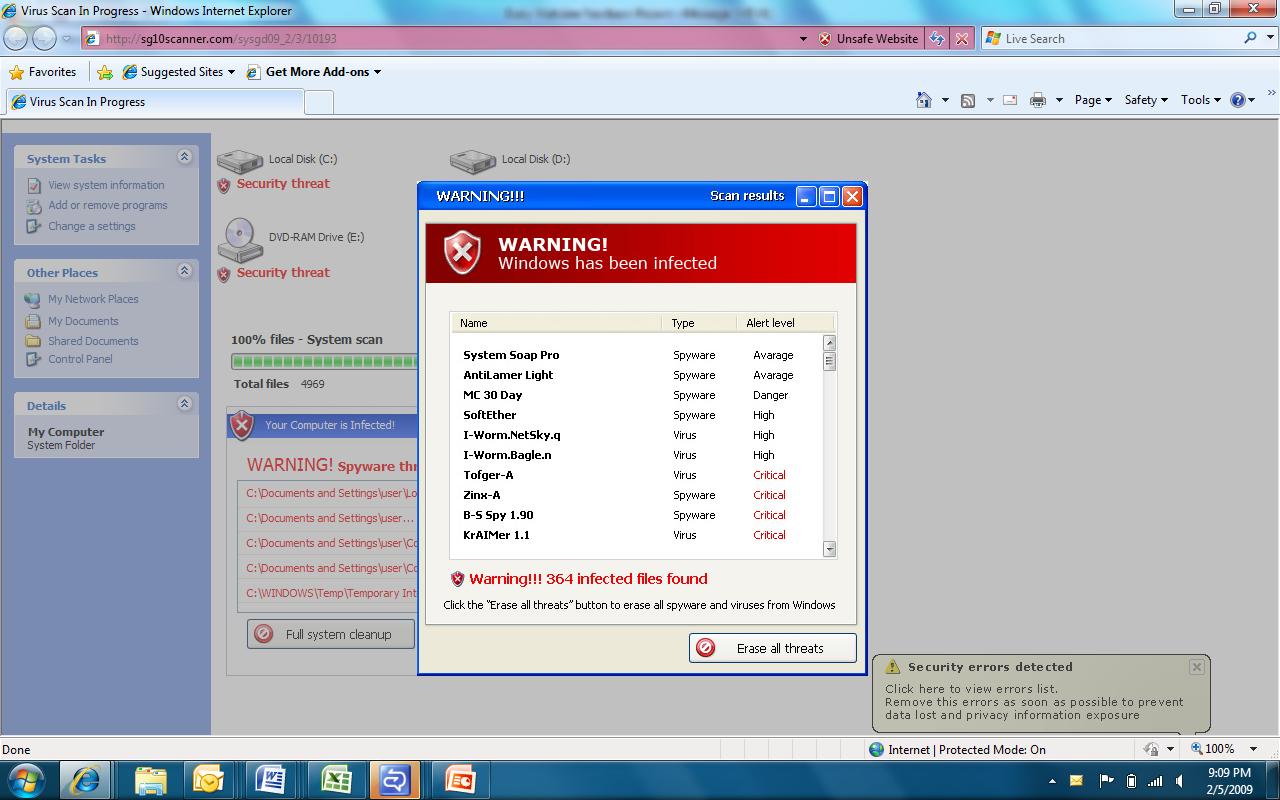
**

図 2: 偽のセキュリティ警告でだまして悪意のあるプログラムをインストールさせようとしています

このよく使われるソーシャル エンジニアリング攻撃は、上掲の図のようなアンチ ウイルスの表示を見て自分のコンピューターがウイルスに感染しているのではないかと心配する気持ちに付け込みます。この攻撃では、専門的に見えるポップアップが偽のアンチ ウイルス ソフトウェア会社から表示されます。これは一見 Windows からの警告のようです。しかし実際にはこれは警告のように見せかけた Web ページで、ダウンロードさせようとしている “解決方法” は、コンピューターにマルウェアを感染させるものです。SmartScreen は毎日膨大な数のこのような攻撃をブロックしていますが、怪しげに見えるアンチ ウイルス警告への注意は怠らないでください。たとえばポップアップ ウィンドウのボーダー (画面の淵) がコンピューター上の他のウィンドウと異なっているように見える場合や、ウィンドウを消しているのにまたポップアップするような場合は、怪しいと考えるべきです。

## 無料のゲームや映画、テレビ番組を提供する Web サイト



図 3: 無料のゲームや映画、テレビ番組を提供する Web サイトは悪意のあるソフトウェアをインストールさせようとしているかもしれません

ゲームや映画、テレビ番組が – 特にそれが無料なら – 嫌いな人はいないでしょう。サイバー犯罪者もその事をよく知っています。この手の攻撃は、費用なしにある種のエンターテイメントを提供する “無料の” Web サイトを訪問した際によく行われます。“ゲーム” の検索結果や誰かから送られてきたサイトへのリンクが、こうしたサイトへの誘導をしています。多くの場合、無料のダウンロード提供のリンクをクリックすると、無料のコンテンツだけでなく悪意のあるソフトウェアも付いてきます。SmartScreen はマイクロソフトに報告されているこうしたサイトをブロックしますが、話がうますぎるように見えるサイトや無料提供には注意を怠らないでください。そうしたサイトはたぶん怪しいでしょう。

## フィッシング攻撃

フィッシング攻撃者は正当な立場の人物や企業に成り済まし、銀行情報やユーザー名とパスワードを伝えても良いと信頼させようとします。たとえば、銀行から送信されたように見える電子メールを受信し、他の金融機関と合併するためにあなたの口座情報を確認する必要があると伝えられるかもしれません。このフィッシング電子メールの目的は偽のサイトへのリンクをクリックさせ、ユーザー名やパスワード、その他の個人情報を “確認” させる事です。こうした情報は攻撃者があなたの口座や個人情報にアクセスするのに使われます。攻撃者はどんどん精錬されており、その電子メールや Web サイトはあなたが日々付き合っている会社の物とまったく同じように見えます。Internet Explorer 8 の SmartScreen フィルターは自動的に既知のフィッシング サイトを警告します。また攻撃の兆候を示すためのツールも含まれています。現時点で Internet Explorer は毎週 100 万以上フィッシングの企てをブロックしています。

Internet Explorer 8 の SmartScreen フィルターは、インターネット上のコンテンツをより安全にブラウズできるよう、既知のフィッシング Web サイトを警告します。フィルターは Web サイトのコンテンツに既知のフィッシング テクニックが使われていないか分析し、Web サイトの信頼性を評価するため情報源の世界的なネットワークを利用します。

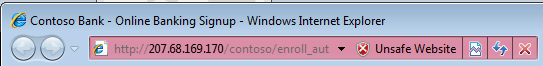


図 4: Internet Explorer 8 がフィッシング詐欺を警告しています。タイトル バーには銀行名が表示されていますが、強調表示されたドメインは銀行の URL ではない事に注意してください。

SmartScreen によるフィッシングからの防御に加えて、Internet Explorer 8 はドメイン名の強調表示を行うはじめてのブラウザーでもあります。この機能により訪問している Web サイトを正しく知る事ができます。ドメイン名の強調表示によって Web アドレス (URL) の判定が容易になり、紛らわしい URL を使って騙そうとする詐欺的なフィッシング サイトを避けるのに役立ちます。アドレス バーの中でドメイン名は黒字で強調表示され、URL のその他の部分は灰色で表示されるので、サイトの正しい識別が簡単にできます。

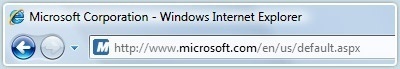


図 5: Internet Explorer 8 は訪問したリンク中のドメイン名を強調表示するので、実際にどこにいるのか確認できます。

# コンピューターへの攻撃に対する防御

ユーザーを騙して悪意のあるソフトウェアをインストールさせたり個人情報を提供させたりするだけでなく、サイバー犯罪者は改ざんした正当なサイトを使った ”ドライブ バイ” 攻撃を、古いソフトウェアやプラグインを利用して実行します。Internet Explorer 8 には、SmartScreen フィルターが既知の攻撃をブロックし潜在的な脅威を識別する手助けをするだけでなく、それ以外にもオンライン時のドライブ バイ攻撃をかわすのに役立つ組み込みのセキュリティ機能と更新が含まれています。

こうした機能の多くはバックグラウンドで動作し、ソフトウェア コンポーネントが正しく動作するよう保ち、サイバー犯罪者がコンピューター上のファイルや設定にアクセスするのを妨げ、犯罪者のソフトウェアがコンピューター上でこっそり実行されるのを防ぎます。また多くの種類の攻撃が古くて脆弱なソフトウェアを狙っているので、ユーザー自身が行うべき事として重要なのは、すべてのソフトウェアを最新のセキュリティ更新でアップデートする事です。

## ドライブバイ攻撃とは何か?

Internet Explorer 8 に含まれているテクノロジーは、”クロスサイト スクリプティング” や “クリック ハイジャッキング” を含むある種の攻撃からユーザーを防御しています。こうした攻撃は気づくのが難しく、多くの場合ユーザーが訪問する正当な Web サイトを踏み台にしています。

**クロスサイト スクリプティング:** クロスサイト スクリプティングはユーザーが利用している Web サイトの脆弱性を利用して攻撃を試みます。この攻撃では、ユーザーに改ざんされた Web サイトのアドレスを含む電子メールが届けられる事があります。このリンクをクリックすると正規の Web サイトに誘導されますが、このサイトはキー入力をキャプチャーしてログイン ユーザー名とパスワードを記録できる悪質なコンテンツを含むよう改ざんされています。Internet Explorer 8 には、この種の攻撃を検知し有害なスクリプトを無効にするクロスサイト スクリプティング フィルターが含まれています。他のブラウザーと異なり、Internet Explorer 8 にはこの機能が最初から備わっており、既定で有効になっています。



図 6: Internet Explorer 8 が潜在的なクロスサイト スクリプティングの脆弱性を検知し、有害なスクリプトを無効にします

**クリックジャッキング:** クリックジャッキングは現在持ち上がりつつあるオンラインでの脅威で、攻撃者の Web ページはユーザーを騙してそれと気づかない形で別のページのコンテンツをクリックさせようとします。たとえば悪意のあるページ内に正規の Web サイトが “フレーム” として隠されています。悪意のあるページ内でクリックすると、実際には何かの購入申し込み、ブラウザーやコンピューターの設定の変更、あるいはサイバー犯罪者が報酬を得られる広告の表示など、別の物をクリックした事になります。これは複雑な攻撃ですが、Internet Explorer 8 は Web サイト開発者に正規のページが “フレーム化” されるのを防止しこの種の攻撃からサイトを保護する手段を提供します。

# 結論

私たちが学習や仕事、検索、買い物などで Web に依存し続けているにつれ、サイバー犯罪の洗練された手口に対して脆弱になりつつあります。オンラインの安全を保つ事は Web ブラウザーがユーザーに対して行う事ができる最も重要な事項の一つです。Internet Explorer 8 は Windows ベースのコンピューターにおいて、使い始めたその時から安全なオンライン エクスペリエンスを提供でき、現在と将来のオンラインでの脅威に対して劇的に強化されたレベルの保護が提供できる唯一のブラウザーです。今すぐブラウザーをアップデートし、コンピューター上のその他のソフトウェアも最新にしましょう。そして一般的な攻撃を認識して避ける方法を学びましょう。そうする事でコンピューターと個人情報へのより強力な保護が得られます。

1. (お住まいの地域での電話番号は、www.microsoft.com/protect/support/.でご確認ください) [↑](#footnote-ref-2)