KASPERSKY lab

ネット決済保護技術による
オンライン取引の保護

重要なのはやはりお金

今ではオンライン決済のできないインターネット環境など考えられません。B2B International が 2013 年に実施した調査によると、銀行やオンラインショップを定期的に利用するインターネットユーザーは 98 % にのぼります。

しかし、オンライン決済の急増に伴い、インターネット詐欺も同じくらい急激に増加しています。現金を騙し取る手段は数多くありますが、おそらく最もよく使われる手口は、オンライン決済システムを騙して、自分が本物のアカウント所有者であると認識させる方法でしょう。ひとたび所有者になりすますことができれば、被害者の資金を使って、どのような取引も可能になってしまいます。

詐欺師が個人情報を手に入れる方法

詐欺師は所有者の名前（またはクレジットカード番号、登録されているエイリアスなど）と正しいパスワード（暗証番号、コードワードなど）を入力します。決済システムにユーザー本人であると信じ込ませるには、これで十分なのです。

しかし、そもそもサイバー犯罪者たちは、どうやってこのデータを入手しているのでしょうか。多種多様なツールや手口が使用されていますが、最もよく見られるのはトロイの木馬を使う方法です。詐欺師たちは、コンピューターをトロイの木馬に感染させれば、ほとんどの情報を自由に盗めるようになります。サイバー犯罪者は、次のいずれかの方法で機密データを入手しています。

- 悪意あるコードを送り込み、メモリを読み取るなどの操作をブラウザーから無断で行い、ログイン ID とパスワードの詳細情報を収集する。あるいは銀行取引の内容（金額、銀行口座など）の書き換えを行う
- 本物の Web サイトに似せたフィッシングページを使って個人情報を盗み見る
- スクリーンショットを撮影する
- キー入力やマウスクリックの内容を記録する
- 入力されたユーザーデータの収集を目的としたさまざまな手法を使ってオンライントラフィックを傍受する

ほとんどの場合、ユーザーは銀行口座を確認するまで、自分の個人情報が盗まれたことに気づきません。

B2B International の調査では、インターネットユーザーの 59 % が、オンラインバンキング詐欺が心配であると回答しています。では、信頼性の高い保護はどこで受けられるでしょうか。

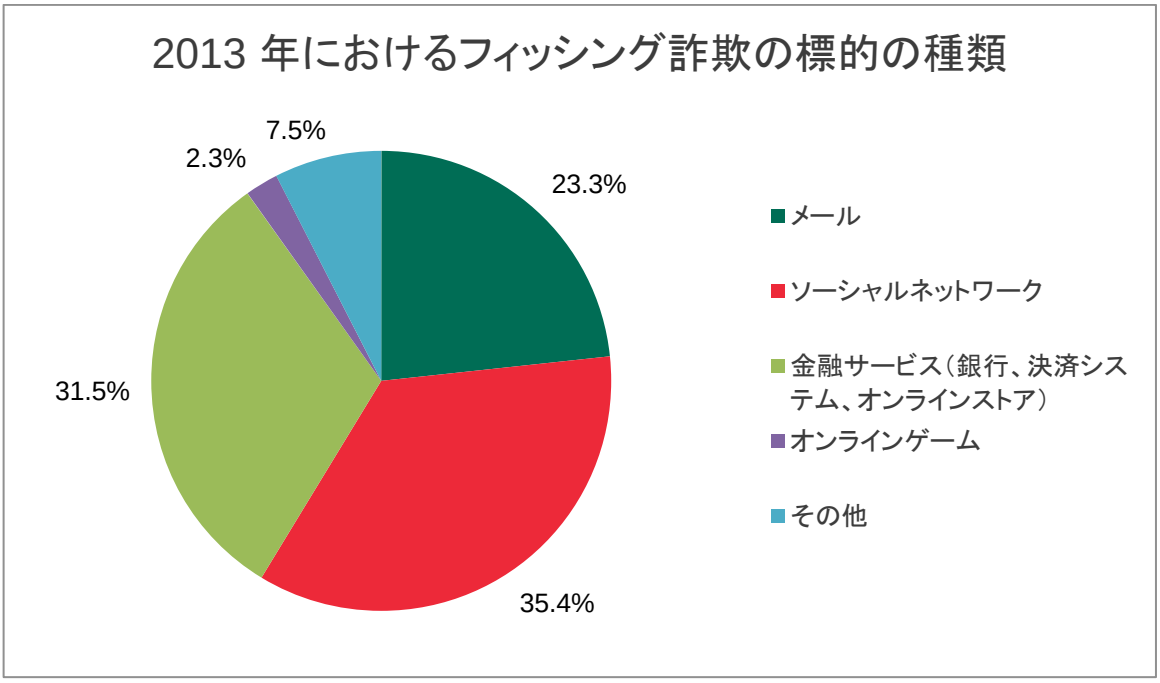

図 1: Kaspersky Lab のアンチフィッシングコンポーネントで検知されたフィッシング詐欺の主な標的の内訳。このコンポーネントは、ユーザーがフィッシングリンクをクリックしようとするたびに起動します。リンクがスパムメールに記載されたものか、Web ページ上のものかは関係ありません。このグラフから、フィッシング攻撃全体の約 3 分の 1 が金融機関や電子決済機関、銀行、オンラインストアやネットオークションを標的としていることがわかります。2013 年全体では、世界中でフィッシング攻撃に遭ったインターネットユーザーの数は、3 億 9600 万人を超えています。出典：Kaspersky Security Network

従来のアンチマルウェアツール

従来のアンチマルウェアプログラムは、トロイの木馬に感染するリスクを大幅に低減するツールを備えています。アンチフィッシング、Web アンチウイルス、ファイルアンチウイルスなどの技術はさまざまな段階で悪意あるコードの侵入を防ぎます。しかし、詐欺師たちは次々に巧妙な手口を考え出し、従来の保護手段を回避できる改造版のマルウェアを多数開発しています。

複数の段階にわたって包括的なセキュリティを実現する製品を利用することは極めて重要です。マルウェアがコンピューターに侵入する段階や、何らかのアクションを実行しようとする段階など、あらゆる段階を厳重に管理しなければなりません。何より、すべてのセキュリティレベルをしっかりと統合する必要があります。

ネット決済保護技術が統合されたカスペルスキー製品には、まさにこうした理由から、従来の優れたアンチマルウェアツールをすべて組み合わせるだけでなく、オンライン決済やオンライン取引でコンピューターを保護するために特別に開発されたさまざまな新技術が搭載されています。

ネット決済保護技術

Kaspersky Lab のネット決済保護技術は、次の 3 つのコンポーネントで構成されています。

信頼できるバンキング

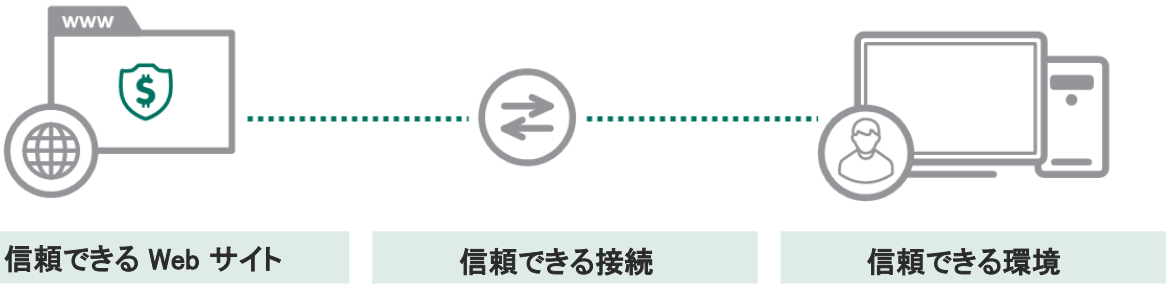

図 2: Kaspersky Lab のネット決済保護の仕組み

信頼できるサイト

ユーザーは銀行やオンライン決済システムの Web サイトを利用する際、アクセス方法を選択することになります。メールやブラウザーに表示されたリンクをクリックする方法や、アドレスを URL バーに入力する方法もありますが、あらかじめ作成しておいたサイトのリストを、カスペルスキー製品のウィンドウから選択することもできます。

サイトが読み込まれる前に、そのサイトの URL が、信頼できるアドレスのデータベースと自動的に照合されます。このデータベースは、Kaspersky Lab が管理しているものか、またはユーザーが指定したものです。一致するアドレスが見つかった場合、ブラウザーがネット決済保護モードに切り替わり、不審なコードの挿入を防ぐとともに、すべてのオンライン操作に対して特別なセキュリティが適用されます。データベースで一致するものが見つからない場合、Web サイトを検査してフィッシング詐欺を見つけ出すヒューリスティック分析が実行されます。ヒューリスティックエンジンが Web サイトのコンテンツを危険と判断すると、実行しようとした取引がブロックされます。これにより、詐欺師がホストしている偽サイトではなく、銀行や決済システムの正規サイトを開くことができます。

信頼できる接続

オンラインバンキングやオンライン決済で接続するサーバーが、本物であるかどうかを確認することも重要です。Kaspersky Lab のデジタル証明書検証サービスを使用することで、サイトが間違いなく正規のものであることを確認できます。証明書を検証できない場合、カスペルスキー製品のネット決済保護機能により、そのオンライン決済サイトへのアクセスがブロックされます。この動作プロセスの時間を短縮するため、ネット決済保護機能は証明書の検証のたびに、判定結果を一定期間ローカルに保存します。そのため、ブラウザーがネット決済保護モードで動作しているときに、サイトに接続しようとすると、まずローカルキャッシュに判定結果がないかが確認されます。Kaspersky Security Network への問い合わせは、判定結果がない場合にのみ行われます。

信頼できる環境

ネット決済保護機能は、オンラインでの購入や決済が行われる前に、その取引が実行されるコンピューターのセキュリティを必ずチェックします。OS のぜい弱性のスキャンもその一部です。この処理は高速で実行されますが、そのスピードは、オンラインバンキングのセキュリティを脅かすことが判明している特定のタイプのぜい弱性（強力な権限を得るために利用されるぜい弱性など）をスキャンすることで実現しています。ぜい弱性が存在すると銀行取引が危険にさらされるため、Windows Update を使用した自動モードでぜい弱性を除去することが求められます。

ブラウザー[1] をネット決済保護モードで起動すれば、すべての個人情報を詐欺師による窃盗や改ざんから保護することができます。ネット決済保護は、ブラウザー経由の悪質コードの侵入、メモリの読み取り、偽ウィンドウの表示をブロックすることでこれを実現し、不正な機能停止や改善からプラグインとプロファイルを守ります。また、スクリーンショットの撮影をブロックすることもでき、GDI、DirectX、OpenGL のようなアプリケーションプログラミングインターフェイスを使ったデスクトップ全体の撮影も防ぎます。

このほか、Web ブラウザーがネット決済保護モードで動作している場合、信頼できないアプリケーションはクリップボード（コピー＆ペースト操作時に重要なデータが一時的に保存される場合があります）にアクセスできなくなります。したがって、サードパーティソフトウェアにクリップボードにアクセスされて、パスワードやログイン ID が盗まれることはありません。

さらに、以下の 2 つのオプションによって、ハードウェアキーボードから入力する重要データの傍受を防ぐことができます。

- セキュリティキーボード：ユーザーの画面に表示され、マウスを使って操作するキーボード
- 入力情報の漏えい防止：特別なドライバーを使用して、ハードウェアキーボードからのデータ入力を保護する機能

ネット決済保護の重要な機能には、保護されたブラウザーモードによるブラウザーの保護強化もあります。この機能は、保護されたブラウザーのアドレス空間を常時スキャンし、何らかのルートキットによって不審なモジュールがロードされていないかを確認します。そのようなモジュールが発見された場合、新しい Web ページが開き、ユーザーへの警告が表示されます。

ネット決済保護を使用した決済取引が完了すると、自動的に通常のブラウザーウィンドウに戻り、そこで処理を終了するか、オンラインストアでショッピングを続けることができます。

搭載製品

安全なオンライン取引を実現するネット決済保護技術は、以下の製品に搭載されています。

[1] ネット決済保護機能は、主要 Web ブラウザー（Internet Explorer、Mozilla Firefox、Google Chrome）の最新バージョンをサポートします。

個人向け製品

- カスペルスキー インターネット セキュリティ

法人向け製品

- カスペルスキー スモール オフィス セキュリティ

利点

ネット決済保護は ID を必要とするすべてのサイトで機能し、決済システムとの通信には HTTPS プロトコルが使用されます。また、ユーザーは銀行や決済システム、オンラインストアを、信頼するサイトのリストに個別に追加できます。

ネット決済保護の主な利点は以下のとおりです。

- 保護メカニズムが必要な時に、必要な場所で自動的に動作します。
- ブラウザーウィンドウの表示の変化から、保護メカニズムが機能していることがわかります。
- 保護メカニズムは、あらかじめ何らかの設定をしておかなくても有効にすることができます（ただし、最低限の設定と初回のみの確認が必要となる Web サイトもあります）。柔軟な設定により、サイトのコンテンツに応じてネット決済保護を有効化または無効化できます。
- ユーザーがあらかじめ選択しておいたサイトでは、デスクトップ上の専用のショートカットを使用して、ネット決済保護モードをすばやく起動することもできます。これにより、サイトへの便利で安全なアクセスが可能になります。
- 高度なアンチマルウェアソリューションとのネイティブ統合により、ほとんどの詐欺手法に対処する多層保護が実現します。

Kaspersky Lab が開発したネット決済保護技術は、オンラインバンキングや決済取引を最大限に保護するものです。これを実現する、信頼できるサイト、信頼できる接続、信頼できる環境によって、オンライン決済処理のすべての段階で、深いレベルでのコントロールが可能になります。こうした革新的な技術が、オンラインバンキング取引だけではなく、あらゆるインターネットアクティビティにおけるセキュリティと保護を極限まで強化します。

業界のエキスパートが保証する品質

ネット決済保護技術は、第三者機関によるテストで高い評価を受けています。

- AV-TEST Innovation Award 2013
- MRG Effitas Online Banking/Browser Security
- Matousec Online Payments Threats
- Matousec Online Payments Threats 2