

## PRESS RELEASE

2014年12月25日  
 株式会社インターネットイニシアティブ

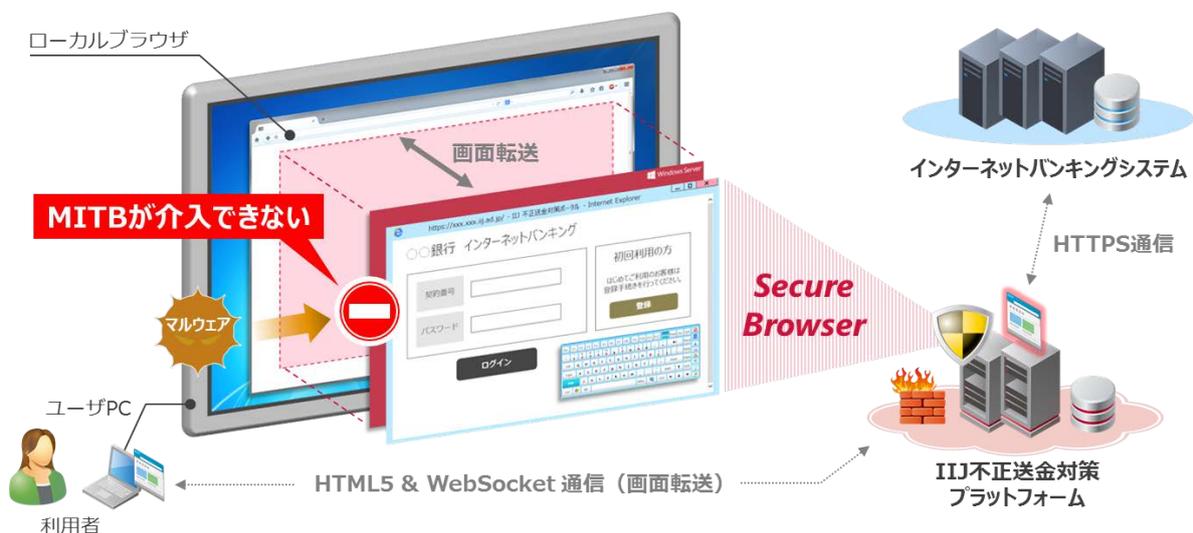
### IIJ、バンキングマルウェア感染による不正送金を防ぐ IIJ 不正送金対策ソリューションを提供開始

株式会社インターネットイニシアティブ(本社:東京都千代田区、代表取締役社長:勝 栄二郎、コード番号:3774 東証第一部、以下 IIJ)は、マルウェア感染によるインターネットバンキングの不正送金被害を未然に防ぐ「IIJ 不正送金対策ソリューション」の提供を開始しました。

昨今、フィッシング詐欺やマルウェア感染により、インターネットバンキング利用者の預貯金が別口座に不正送金される事件が急増し、警察庁の発表では、2014年上半期(1~6月)の被害総額は18億5200万円となり、昨年の約9倍に増加しています。そのような不正送金の手口が巧妙化するなかで、最近では、利用者がインターネットバンキングシステムにログインした後にブラウザを乗っ取り、情報を改ざんするMITB(Man in the Browser)攻撃(\*1)が増えつつあります。IIJ 不正送金対策ソリューションは、従来のウイルス対策ソフトでは検知が難しいバンキングマルウェア(\*2)感染によって不正送金を行うMITB攻撃への根本的な防御対策として有効なソリューションです。

本ソリューションでは、インターネットバンキングにアクセスするための仮想アプリケーション環境を提供します。本環境からユーザPCへはブラウザの画面情報のみが転送、表示されますので、ユーザPCを介した通信情報の窃取や画面の改ざんを防御することが可能です。仮にユーザPCがバンキングマルウェアに感染していたとしても、マルウェアは通信経路に介入できず、ユーザは安全にバンキングシステムを利用することができます。

#### ■IIJ 不正送金対策ソリューション イメージ図



## ■IIJ 不正送金対策ソリューションの特長

### ・金融機関のお客様

本ソリューション導入にあたって既存のバンキングシステムを改修する必要はなく、導入済みのセキュリティ対策(ワンタイムパスワード、リスクベース認証等)と連携した活用により、更に強固なセキュリティ対策が可能になります。また、バンキングシステムへのアクセスを本ソリューション経由に限定することで、多数あるブラウザやそれらのバージョンへの対応といった開発負荷を大幅に軽減することが可能になります。

### ・ユーザ(利用者)側

専用アプリケーションやブラウザプラグインなどのインストールは不要なため、導入による負担はありません。従来と同様のユーザビリティを維持しています。

本ソリューションは、すでに国内のメガバンクで採用され、個人向けサービスにおいてご利用いただいています。今後はスマートデバイスや法人向けサービスについても順次対応する予定です。

IIJ 不正送金対策ソリューションは、金融機関だけでなく、インターネット上でビジネスを展開するさまざま企業にとって、ユーザが安心してサービスを利用するために最適なソリューションです。IIJ では、今後もサービス提供側、ユーザ側ともに安全にインターネットでのサービスを利活用できるよう、多彩なソリューションを展開してまいります。

(\*1)バンキングマルウェアに感染したPCを利用して不正送金を行う攻撃。バンキングマルウェアに感染したPCを使用してインターネットバンキングへアクセスすると、正規のユーザが通常どおり認証を通過した後、バンキングマルウェアがポップアップ画面を表示したり、送金リクエストの送金先口座を異なる口座に書き換えるなどの処理を行う。不正送金に気付きにくく、また銀行側も正常な処理と何ら違いがないため検知が困難。

(\*2)ユーザがインターネットバンキングサービスを利用しようとしたときに動作を開始するマルウェア

### 報道関係お問い合わせ先

株式会社インターネットイニシアティブ 広報部 増田、小河

TEL: 03-5205-6310 FAX: 03-5205-6377

E-mail: [press@iij.ad.jp](mailto:press@iij.ad.jp) URL: <http://www.iij.ad.jp/>