報道関係各位
プレスリリース

2016 年 2 月 23 日
さくら情報システム株式会社
東北インフォメーション・システムズ株式会社

さくら情報システムと東北インフォメーション・システムズが共同考案 「SIM-Sign(仮称)」の特許取得 ～インターネットバンキングの不正送金を防止する取引認証方式～

さくら情報システム株式会社（本社：東京都港区、代表取締役社長：池尻 和生、以下さくら情報システム）と東北インフォメーション・システムズ株式会社（本社：宮城県仙台市、取締役社長：早坂 栄二、以下 東北インフォメーション・システムズ）は、大きな社会問題となっている金融機関のインターネットバンキングサービスにおける不正送金を防止する画期的な取引認証方式を共同で考案し、この度特許を取得しましたのでお知らせいたします。

今後、インターネットバンキングサービスを提供する金融機関、ベンダーに対して、この特許を利用した取引認証システムの採用を働きかけてまいります。

●特許の概要
○登録名
情報処理装置、認証方法及びプログラム（製品名「SIM-Sign(仮称)」）
○特許登録番号
特許　第5847345号

従来の不正送金対策は、ワンタイムパスワードを発生させるトークンと呼ばれる機器を配布したり、不正送金を行うパソコンの不審な挙動を検知するソフトウェアを配布したりする方法が一般的でした。しかしながら、最新の不正送金の手口ではパソコンやスマートフォンを不正に乗っ取ることで、単純なワンタイムパスワードやソフトウェアを用いた従来の対策では、不正送金の潜在的リスクを完全には排除できない可能性が生じています。

今回取得した特許は、スマートフォンやタブレットに内蔵されているSIMカード*と呼ばれるハードウェアを利用することで、金融機関との間に信頼できる通信環境「Trusted Path」を構築するとともに、金融機関との取引内容を第三者が改竄できないようにすることで、極めて高い安全性を保ちながら、操作的にも簡単という特長を実現しました。これは、不正送金対策の決定版となり得ると考えております。

＊ SIMカードは、通信キャリアが配布するICカードで、携帯やスマートフォンが正しく通信するために必要な情報が書き込まれており、外部からの不正なアクセスに対して極めて安全とされています。

今回の特許は、さくら情報システムの銀行向けシステム開発経験をもとにするインターネットバンキングサービスの取引認証技術と、東北インフォメーション・システムズの電子認証サービスの知見を取り入れており、両社で協力して、現状最も堅牢である「SIM-Sign（仮称)」の実現に向け、取り組んでおります。

なお、本技術については、国立研究開発法人産業技術総合研究所　大塚 玲主任研究員の監修を受けて実現いたしました。

●さくら情報システムについて

三井住友銀行およびグループ会社の基幹システムを支え、幅広いお客様にハイレベルなサービスを提供してまいりました。40 余年の豊かな経験から培ったノウハウ、技術、信頼をもとに、会計・金融・人事給与・セキュリティ・システム運用・アウトソーシングの強みを軸に、今後もお客様の課題解決をトータルにサポートしてまいります。

さくら情報システムの詳細は、http://www.sakura-is.co.jp をご覧ください。

●東北インフォメーション・システムズについて

電力業務で永年培った技術力と豊富な経験のもと、情報システムの企画・コンサルから開発・運用、そしてシステムの保守・維持管理など、総合的な情報システムサービス「トータルソリューション」を提供しています。また、電子認証技術を活用したサービス事業をとおし、お客様に最適な情報インフラの構築と安定したシステム運用サービスも提供しております。

東北インフォメーション・システムズの詳細は、http://www.toinx.co.jp/company/をご覧ください。

＜製品に関してのお問い合わせ先＞

さくら情報システム株式会社　営業本部　ビジネス推進部
担当：佐藤
電話：03-6757-7261
E-mail：solution1@sakura-is.co.jp

東北インフォメーション・システムズ株式会社　営業企画部
担当：本間・小関
電話：022-268-2821
E-mail： sol_info@toinx.co.jp

＜報道機関からのお問い合わせ先＞

さくら情報システム株式会社　営業本部　営業企画部
担当：藤原・河西
電話：03-6757-7211
E-mail：solution1@sakura-is.co.jp

東北インフォメーション・システムズ株式会社　営業企画部
担当：本間・小関
電話：022-268-2821
E-mail： sol_info@toinx.co.jp

SIM-Signについて

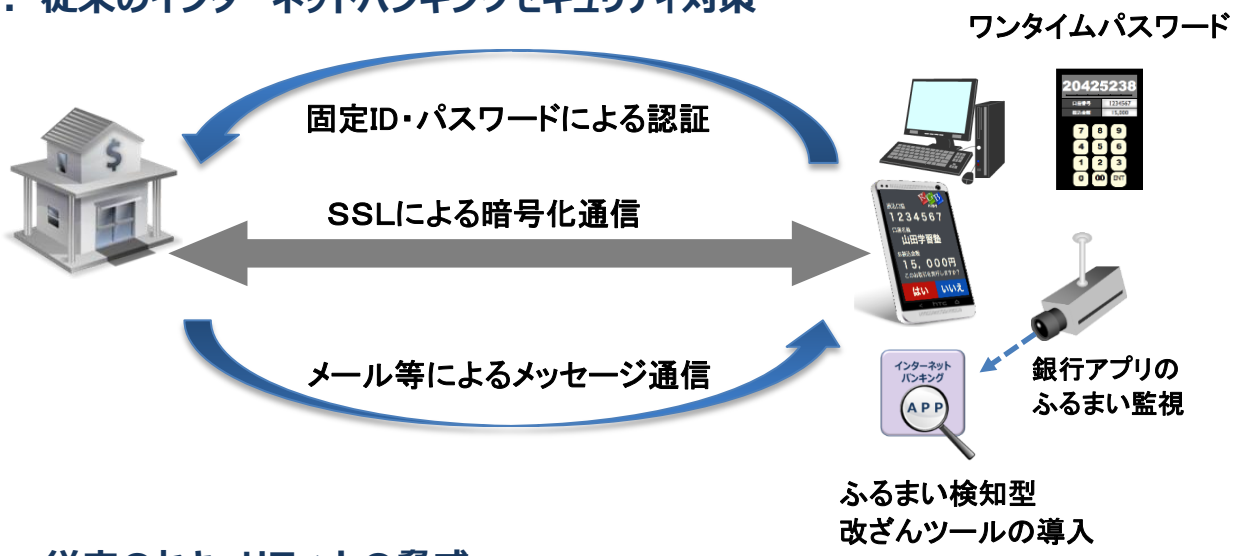
はじめに

近時金融機関における不正送金・不正アクセスが大きな問題となっており、金融機関においても、さまざまな対策が施されています。

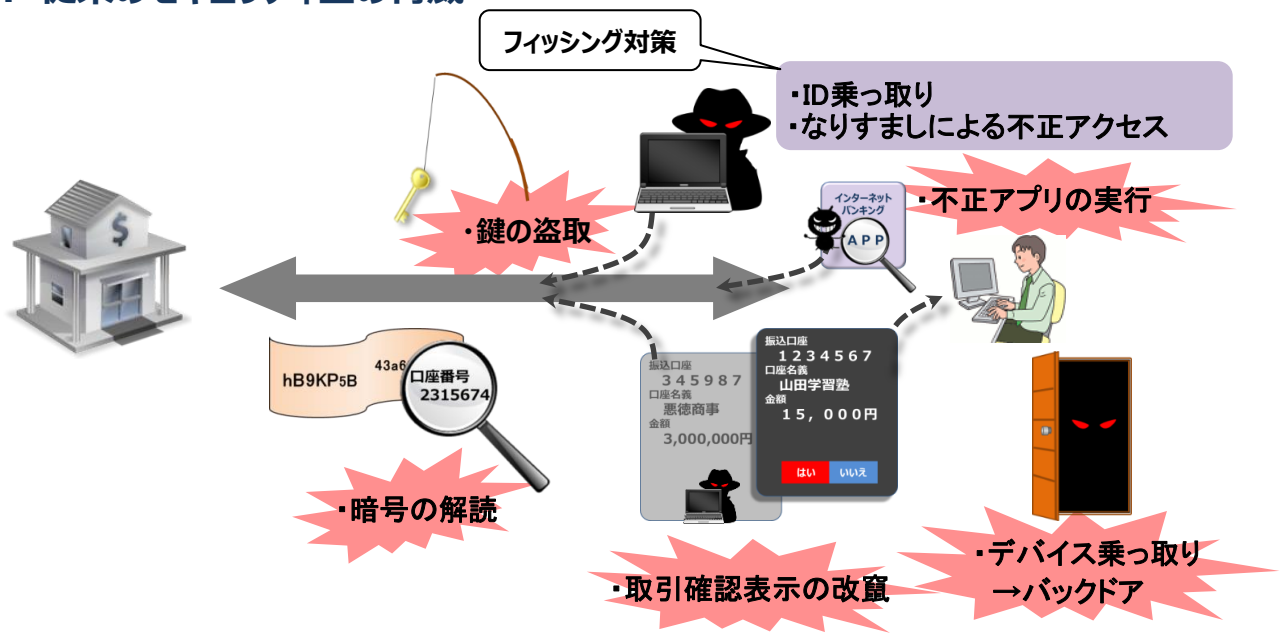
しかしながら、既存の不正への対応だけでは、その方法をすり抜ける手口が次々現れると言うイタチごっこになっている感があります。

SIM-Signは不正ソフトに個別に対処するのではなく、事前に登録されかつ登録後に改ざんされていないソフトだけを実行可能にする技術に、銀行側と利用者間で通信内容を改ざんすると確実にわかる仕組みを付加したもので、高い安全性と簡便な操作性を両立しており、取引認証の決定版です。

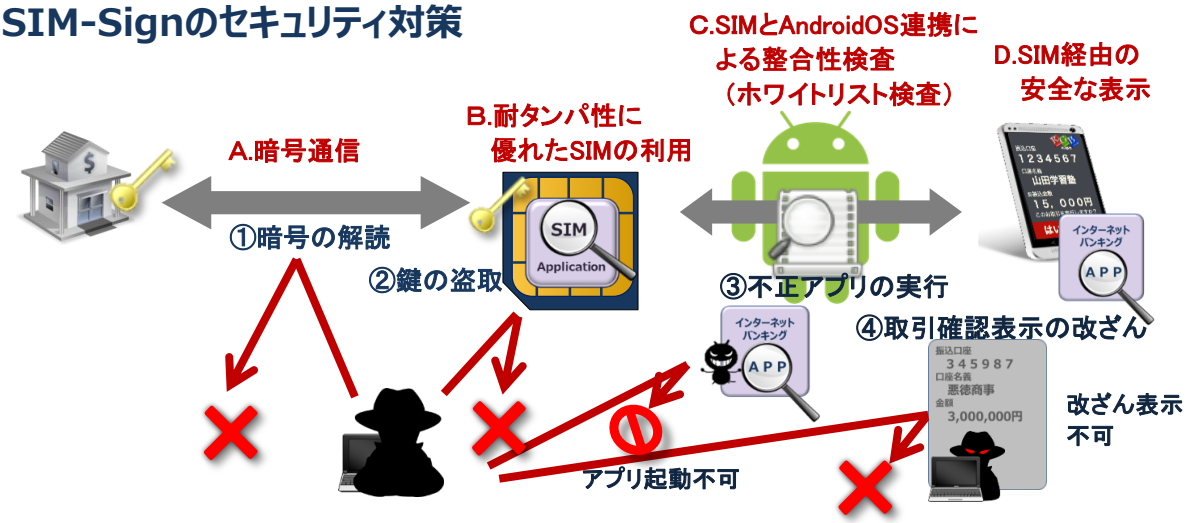
1．従来のインターネットバンキングセキュリティ対策



2．従来のセキュリティ上の脅威

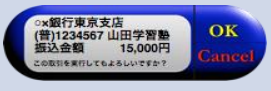
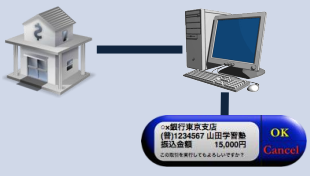


3．SIM-Signのセキュリティ対策



①暗号の解読	AES等の標準的な暗号・認証を利用した暗号プロトコルにより構成され、銀行とSIM間の暗号文の解読やなりすましは暗号理論上極めて困難。
②鍵の盗取	SIMの多くはEAL4+の安全性が確認されているため、物理解析に対して安全。
③不正アプリの実行	改ざんされた銀行アプリで不正取引を行なう手口と出来ない理由。 （1）OS等の脆弱性を利用したホワイトリスト検査機構への攻撃 ⇒ホワイトリスト検査機構はAndroid OSの機能としてシステム領域に実装されているため、利用者が意図的に端末をルート化しない限り、不正アプリによるSIMへのアクセスはできない。 （2）銀行のコード署名をかたる ⇒コード署名はデジタル署名のため、なりすまし自体が暗号理論上極めて困難。
④取引確認表示の改ざん	利用者端末の表示を改ざんするには、Android OS機能の一部（表示ライブラリ等）を改ざんする必要があるが、システム領域に実装されているため、利用者が意図的にルート化しない限り改ざんできない。

4．現状有効なMitB対策技術のまとめとSIM-Signのポジション

採用技術	ネットワーク形状	Trusted Pathの構成方法	課題
トランザクション認証機能付ワンタイムパスワード 	銀行－PCのみ 	銀行とトークンが暗号鍵を共有	・機器配布コスト発生 ・入力が面倒
スマートフォンによる取引確認 	銀行－PC，銀行－携帯 	携帯電話のメッセージング機能	マルウェア対策に不安 解消
表示機能付トークンによる取引確認（USBトークン等） 	銀行－PC－USBトークン 	銀行とトークンが暗号鍵を共有	解消 ・機器配布コスト発生 ・入力が面倒

SIM-Sign
セキュアエレメントである「SIM」を利用し以下を実現
- ・暗号鍵の安全な管理
- ・ホワイトリスト検査
- ・取引確認表示改ざんの防止
- ・スマートフォンによる取引詳細表示
- ・簡単な取引操作

※「Android」、は、Google Inc.の商標または登録商標です