News Release

2025 年 7 月 9 日
株式会社日立システムズ

急増するインターネットバンキングの不正送金被害を防ぐ
スマートフォン環境向けセキュリティオプション「PhishWall Mobile SDK」の提供を開始

モバイル環境でのインターネットバンキング利用増加を背景に、標準ブラウザー利用時のセキュリティ対策強化に貢献

「PhishWall Mobile SDK」の画面イメージ

株式会社日立システムズ（以下、日立システムズ）は、金融機関などの Web サイトを模した不審なサイトを検知する「PhishWall プレミアム」[*1] と同様の機能をスマートフォンの標準ブラウザー利用時にも実現させた、「PhishWall Mobile SDK」[*1] の提供を本日より開始します。

「PhishWall プレミアム」は、コア技術である「PhishWall 認証」[*2] によりインターネットバンキングにおける取り引きの安全性を高め、不正送金・フィッシング詐欺防止を図るために、国内の金融機関約 200 行に導入されています。

近年、不正送金詐欺の被害が急増しており、その手口のほとんどがフィッシングによるものです。PC と比較しスマートフォン利用時におけるセキュリティ対策は手薄になりがちな現状を受け、不審なサイトを検知する「PhishWall プレミアム」の機能をスマートフォン環境でも実現させた「PhishWall Mobile SDK」を開発しました。

これにより、スマートフォン環境からインターネットバンキングをご利用のお客さまを狙う不正送金詐欺の被害を防ぎ、インターネットバンキングをより安全に利用できる環境作りをサポートします。

*1 「PhishWall プレミアム」および「PhishWall Mobile SDK」は、「フィッシング・不正送金対策　PhishWall シリーズ」の一機能として提供します。
*2 「PhishWall 認証」は、セキュリティ性の高い認証技術で DNS スプーフィング（ドメイン名を不正な名称に書き換えること）に有効とされ、特許第 4942101 号(P4942101)を取得しています。

■背景

インターネットバンキングの不正送金被害件数が前年の 4 倍以上・過去最多の 4,000 件超え

金融機関の口座管理用のスマートフォン向けアプリケーションの普及を受け、スマートフォン利用時の対応が急務

・金融機関のスマートフォン向け口座管理アプリケーションの普及とモバイルアクセスの増加

警察庁の発表[*3]によると、令和 6 年におけるインターネットバンキングによる不正送金被害件数は 4,369 件、被害額は 86.9 億円で前年同様、被害額は高止まりしています。

さらに、犯罪の手口も SMS を用いた詐欺行為などが多様化しています。

・狙われるセキュリティのぜい弱性

しかしながらスマートフォンなどモバイル環境ユーザーのセキュリティ意識は PC 利用者と比較しても低い傾向があり[*4]、犯罪グループもこのぜい弱性対策の差に付け込んで、さまざまな手口でのフィッシングによる不正送金詐欺の被害が増加しています。生成 AI などを利用した巧妙な手口が次々と出てくるなか、スマートフォン利用時のセキュリティ対策が急務となっています。

*3 出典：警察庁「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

*4 出典：独立行政法人 情報処理推進機構「2022 年度 情報セキュリティの倫理と脅威に対する意識調査−【脅威編】−」
https://www.ipa.go.jp/security/reports/economics/hjuojm0000007fh1-att/000108321.pdf

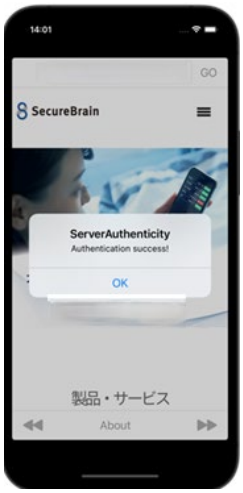
■特長

①アプリケーションのインストール時に接続先 Web サイトの真正性を担保

各金融機関の口座管理アプリケーションに「PhishWall Mobile SDK」を組み込むと、インストール時にアプリケーションが、遷移する Web サイトの URL を認証してサイトの真正性を担保します。

②標準ブラウザー利用時でも Web サイトの真正性を担保し、フィッシング詐欺被害を防ぐ

スマートフォンの標準ブラウザーにおいても「PhishWall 認証」によって、正規の URL かどうかを判別します。SMS に添付されているリンクをクリックすることで詐欺サイトに誘導されるケースにおいても、不審なサイトの検知機能が作動し警告表示を行うことにより詐欺サイトへのアクセスを未然に防ぎます。



■今後の展望

日立システムズは、昨今の多様化するフィッシングによる不正送金詐欺などのさまざまなセキュリティ脅威からインターネットバンキングを利用するお客さまの資産を守り、より安全にインターネットを利用できる環境作りをサポートしていきます。

■PhishWall プレミアムについて

利用者のクライアント PC 内にソフトウェアをインストールして利用します。Web ブラウザーの通信や PC 内のウイルスの挙動を監視します。インターネットバンキングの利用者が不審なサイトにアクセスした際に通知する機能[*5]と、PC が MITB（マン・イン・ザ・ブラウザー）攻撃[*6]型ウイルスに感染していないかチェックしウイルスを無効化（または駆除）する機能を備えています。

詳細は https://www.hitachi-systems.com/solution/s106/phishwall/premium/ をご覧ください。

*5 不審なサイトへのアクセスや MITB 攻撃側ウイルスをすべて検知・無効化することを保証するものではございません。

*6 MITB（マン・イン・ザ・ブラウザー）攻撃：何らかの手段でウイルスに感染したクライアント PC から行われる攻撃です。この攻撃では、ウイルスは Web ブラウザーに対し、不正なログイン画面をポップアップさせ利用者のインターネットバンキングへのログイン情報などを抜き取る。MITB 攻撃は利用者のクライアント PC に感染したウイルスによって行われるため、Web サーバー側のセキュリティ対策では回避できません。

■日立システムズについて

日立システムズは、強みであるさまざまな業種の課題解決で培ってきたお客さまの業務知識やノウハウを持つ人財が、日立グループ各社やビジネスパートナーと連携し、One Hitachi で Lumada 事業を中心に展開することにより、お客さまのデジタル変革を徹底的にサポート。日立グループのサステナビリティ戦略の下、環境・社会・企業統治を考慮した経営を推進することで、国連が定める持続可能な開発目標 SDGs の課題解決に向けた価値を創出し、企業理念に掲げる「真に豊かな社会の実現に貢献」してまいります。

詳細は https://www.hitachi-systems.com/ をご覧ください。

お問い合わせ先

株式会社日立システムズ

お問い合わせ Web フォーム

https://www.hitachi-systems.com/form/contactus.html