PASSLOGY™

特許取得済み認証技術
「ログインプロテクト」のご紹介

セキュリティ技術は世界平和につながる。

パスロジ株式会社
2022/1/19

「フィッシング」により「認証」が危機に陥っている！？

Eメールやショートメッセージサービス（SMS）で送られてくるメッセージから、偽のWebサイトに誘導し、ID・パスワードや個人情報を入力させて詐取する行為「フィッシング（Phishing）」。
このフィッシングによる不正アクセス事件が後を絶ちません。

この、フィッシングを起点として認証情報を詐取する手口は、「マン・イン・ザ・ミドル攻撃」、「中間者攻撃」、「バケツリレー攻撃」などと呼ばれ、ＳＮＳや金融機関、ＥＣサイト等の各種サービスに多く採用されている、ＳＭＳを利用した二段階認証でも防ぐことができず、被害が報告されています。

これは人間が、メッセージに書かれている嘘の情報を信じてしまう限り、発生してしまうのです。

パスロジはこの状況を変えるために、不正アクセスを100%防ぐ技術と考え方の提案をいたします。

■パスロジ株式会社について

PASSLOGY™

パスロジ株式会社は2000年の設立より、IT社会において日常的に行われる「ログイン」、「サインイン」といった作業「本人認証」について研究開発を行っているベンチャー企業です。日本において33件、世界各国では合計108件の特許を取得しております。（2021年12月時点）
　主力製品の認証セキュリティシステム「PassLogic」は、350社以上の企業や政府機関等に採用されています。新型コロナウイルス感染症対策によるテレワーク導入拡大にも迅速に対応し、2021年６月にはユーザー数139万件を突破いたしました。
　開発体制は「完全社内開発」で、製品は「純国産」となります。海外各国の政府・団体の影響を受ける可能性が低く、安心してご利用いただけます。

「サービスからの通知をしない」という考え方

アクティブセキュリティ

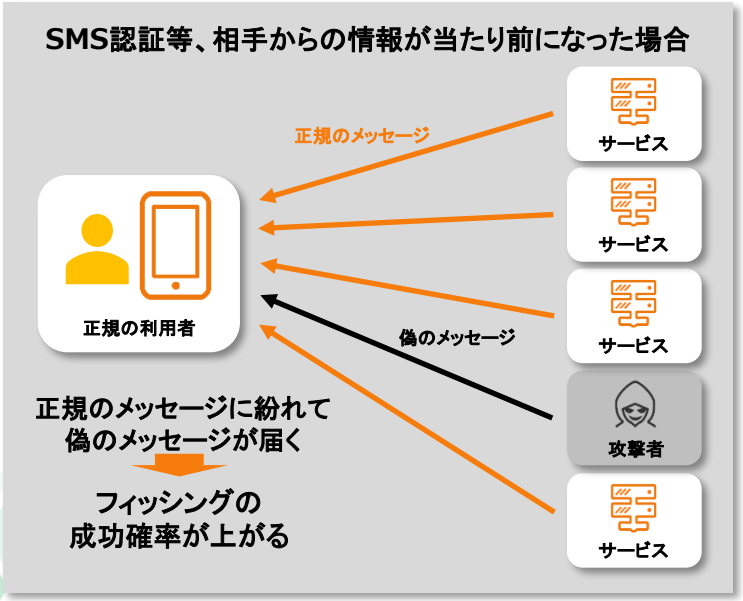
フィッシングに対抗する「アクティブセキュリティ」

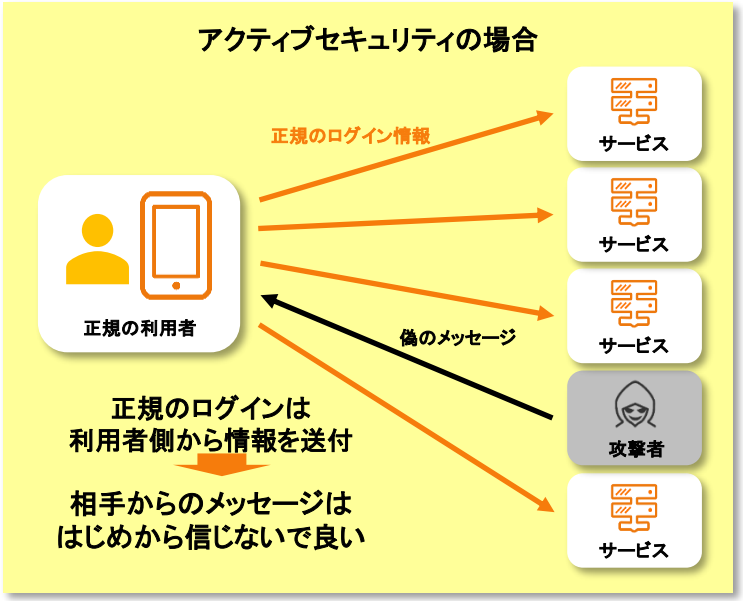
フィッシングのきっかけは「相手から送られてくる情報」です。

現在、よく利用されている認証方法「SMS認証」は、SMSメッセージを認証情報とする認証方式です。
このSMS認証の利用により、SMSメッセージが送られてくることに慣れてしまうと、偽のSMSメッセージに気づけなくなる恐れがあります。

パスロジは「相手からの情報」を信用しないことが危機回避につながると考え、「こちらから情報」を送る「アクティブ」な方法だけで認証する環境構築を推奨します。

パスロジは、この考え方を「アクティブセキュリティ」と呼び、提唱しています。
この資料で説明する認証技術**「ログインプロテクト」はこの考え方をベースに考案**されています。





認証受け付け時間を制限し、安全性を向上

ログインプロテクト

「ログインプロテクト」とは

「ログインプロテクト」は、ログイン可能な時間を極限まで減らすことで、認証のセキュリティ強度を高める技術です。

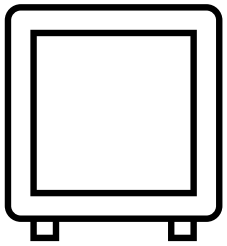
これまでの認証の仕組みとの最大の違いは、「認証を受け付けない状態が標準状態」であることです。その状態においては、ログインフォームに対していかなるパラメータ（たとえ正解であっても）を送信してもシャットアウトします。

正規の利用者がログインする際には、スマートフォンアプリをワンタップし、「これからログインする」という合図をサービスに送信します。サービス側は、合図を受け取ってから1分間だけ、ログインを待ち受ける状態になります。この間に利用者はいつも通りのログイン操作で認証します。

ログインプロテクトの概念イメージ

例えば、**【金庫】**をログインプロテクトに対応すると？

鍵穴もダイアルも
無い状態が標準



鍵穴が無いので
絶対に開錠できない

利用者がスマホでワンタップ
鍵穴やダイアルが出現

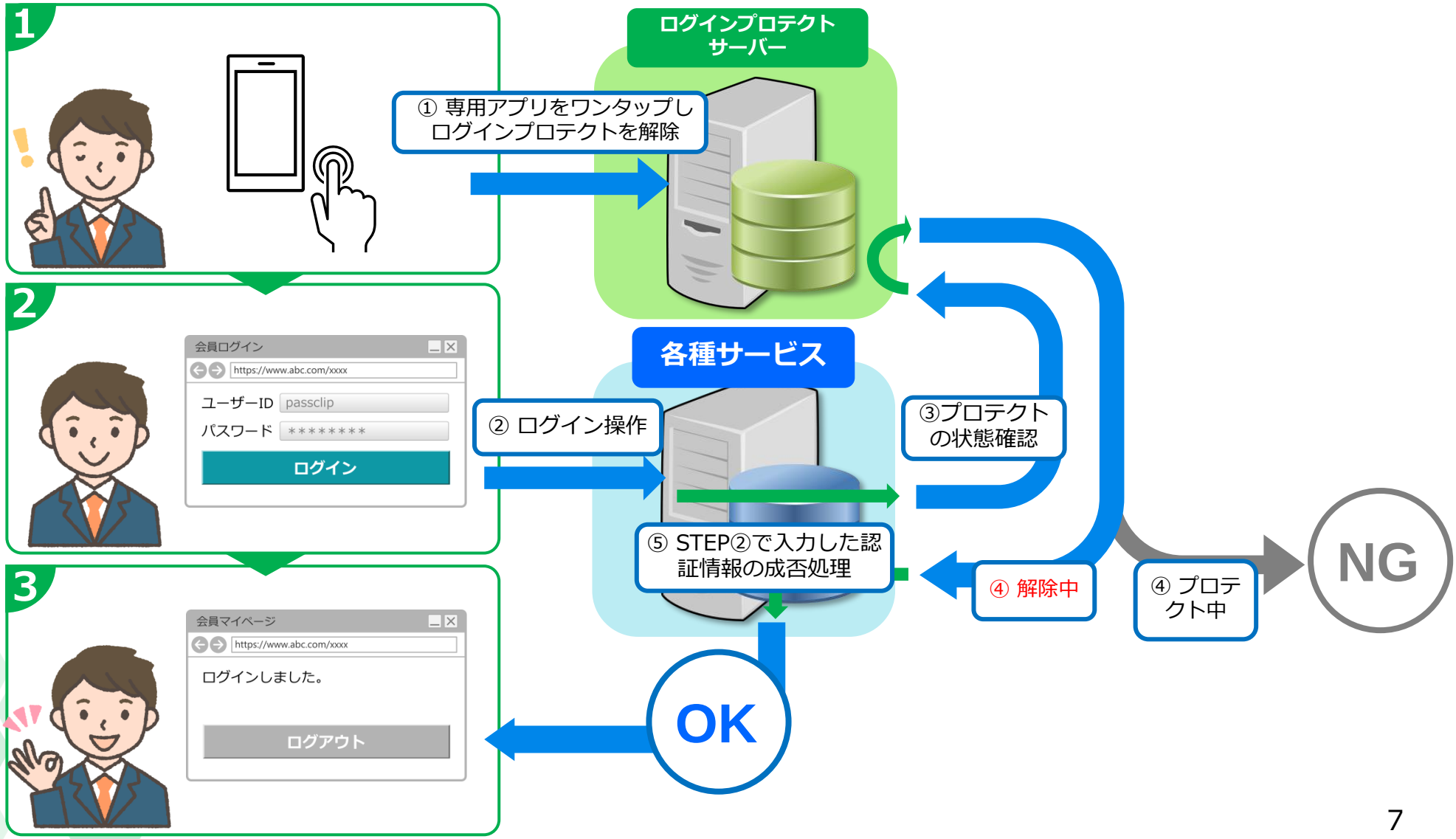
いつも通りの操作で開錠

（ワンタップだけの簡単操作で実現したことも本技術のポイント）

「ログインプロテクト」を利用したログインの流れ

ログイン操作には、利用者への通知が一切発生しない「アクティブセキュリティ」の考え方を採用！

▼利用者の操作は3ステップ



利用者への「通知」がフィッシングの隙を作る

ログインする際に通知が発生するよう、「ログインプロテクト」のログイン手順をあえて入れ替えて、
アクティブセキュリティに違反した状態を以下の通りにまとめました。この手順を例に、その問題点を確認してみます。

通知されるのが正規の手順ともなると、本物と偽物の通知がすり替わってっても違和感がなく、簡単に騙されてしまう

※「変な日本語」「怪しいアドレス」などの従来のフィッシングの特徴と比べると、近年のフィッシングは高度化しており、ITリテラシーが高くても見抜くのが極めて困難になってきている

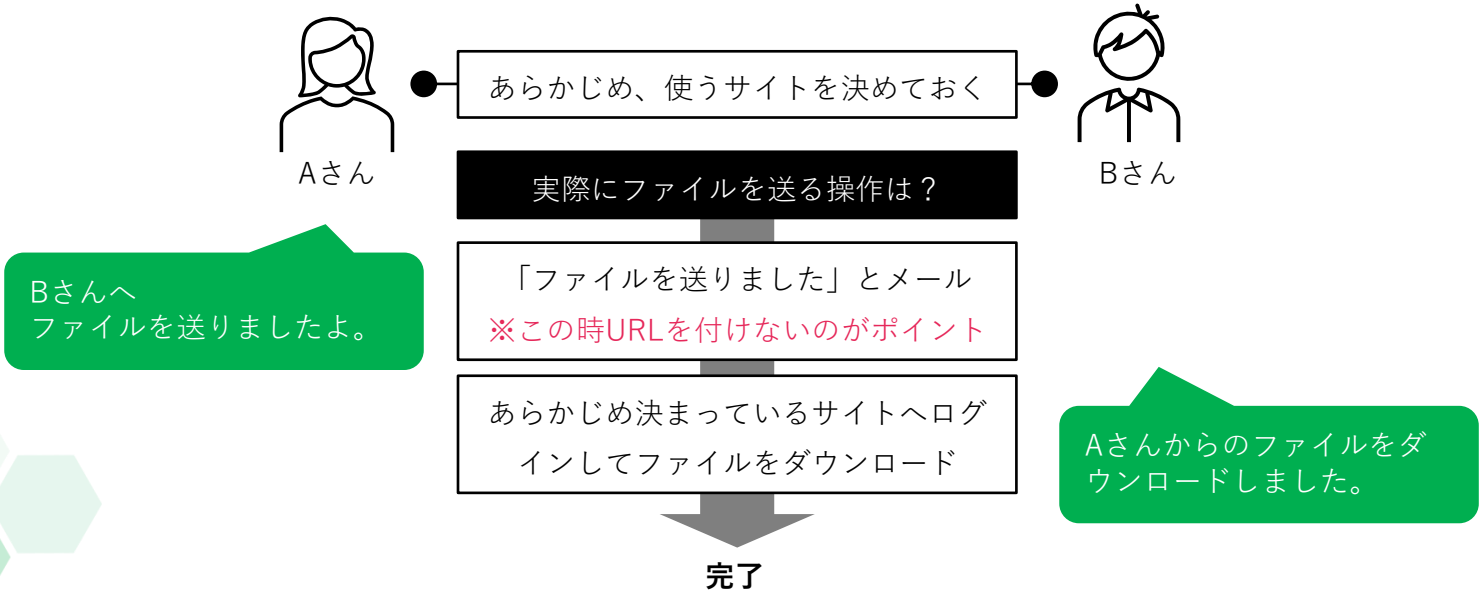
アクティブセキュリティは、あらゆるシステムに適用すべき考え方

通知を伴う「PPAP」対策が危険な理由

メールによる添付ファイルの送信方法として利用されている、パスワード付きzipファイルを送り、後からそのパスワードを別送する「PPAP」。このPPAPに代わるファイル転送方法として、クラウドストレージやファイル転送サービスの活用が始まっています。
しかし、これらのサービスの利用により、「暗号化されたzipファイルを、メールに添付しない」という意味においては対策となる一方で、ダウンロード用URLが飛び交う状況が新たに発生し、日常化してしまいます。その結果、メール内に記載されたURLをクリックすることへの警戒心が薄れ、攻撃者にとって恰好のターゲットとなる恐れがあります。

このような状況になることを防ぐために、認証の分野だけではなく、ITシステムの設計全般において「アクティブセキュリティ」の考え方を持つことが大切です。

例えば、**【PPAP対策】**にアクティブセキュリティの考え方を適用すると？



ご覧くださり有難うございました

今回は「アクティブセキュリティの概念」と弊社独自の認証技術「ログインプロテクト」に関するご紹介でしたが、弊社は「知識を用いた認証」、特に「パターン」を用いた認証「パスロジック方式」が専門となります。

とはいえ、認証に関する研究を幅広く行っておりますので、認証技術に関するご質問や、専門的な観点からの知見の収集など、弊社にお役に立てることがございましたら、お気軽にお声がけください。

（参考）パスロジック方式とは？
https://www.passlogy.com/passlogic-method

【連絡先】
パスロジ株式会社
東京都千代田区神田神保町1-6-1 タキイ東京ビル7F
ログインプロテクト担当窓口

ＴＥＬ：03-5283-2263
メール：press@passlogy.com