株式会社Geolocation Technology

IP Geolocation技術を活用した証券口座への不正対策

証券コード：4018

不正が増加する背景

口座開設の増加

2024年には国内の主要証券会社における口座開設数が前年比20%以上増加

電子マネーの普及と新NISA制度の開始により、投資人口が拡大している。

スマートフォンからの簡単な操作で、誰でも証券取引が可能になった。

増加する脅威

1 利便性に比例して、サイバー攻撃も巧妙化している。

2 フィッシングサイトによるID・パスワードの窃取が増加している。

3 二段階認証のSMS認証を突破するような高度な手口も出現している。

証券口座の乗っ取りの現状

証券口座の乗っ取りは、窃取した顧客情報（ログインIDやパスワード）を悪用する行為である。

犯罪者は実在する証券会社のウェブサイトを精巧に模倣し、ログイン情報を盗む。

証券口座が乗っ取られ、不正取引が行われる事例が急増しています。

1

2025年1月

不正アクセス件数 96件
被害額：約1.5億円

2

2025年4月

不正アクセス件数　3,556件
被害額：約2,886億円

主に、高齢者や個人投資家がターゲットにされています。

信頼性の低下
証券会社や金融市場の信頼性が損なわれます。

資産喪失
投資家の資産が一瞬で奪われるリスクがあります。

市場操作
不正売買による株価操作が市場全体に影響を与えます。

不正アクセスの手口

フィッシング詐欺

偽の証券会社サイトでユーザーのID・パスワードを盗みます。
不正なリンクを送信し、個人情報を抜き取ります。

セッションハイジャック

ユーザーがログインしている状態を狙い、悪意のある第三者がその通信内容を傍受・盗聴し、
正規のユーザーになりすまして不正な操作を行う

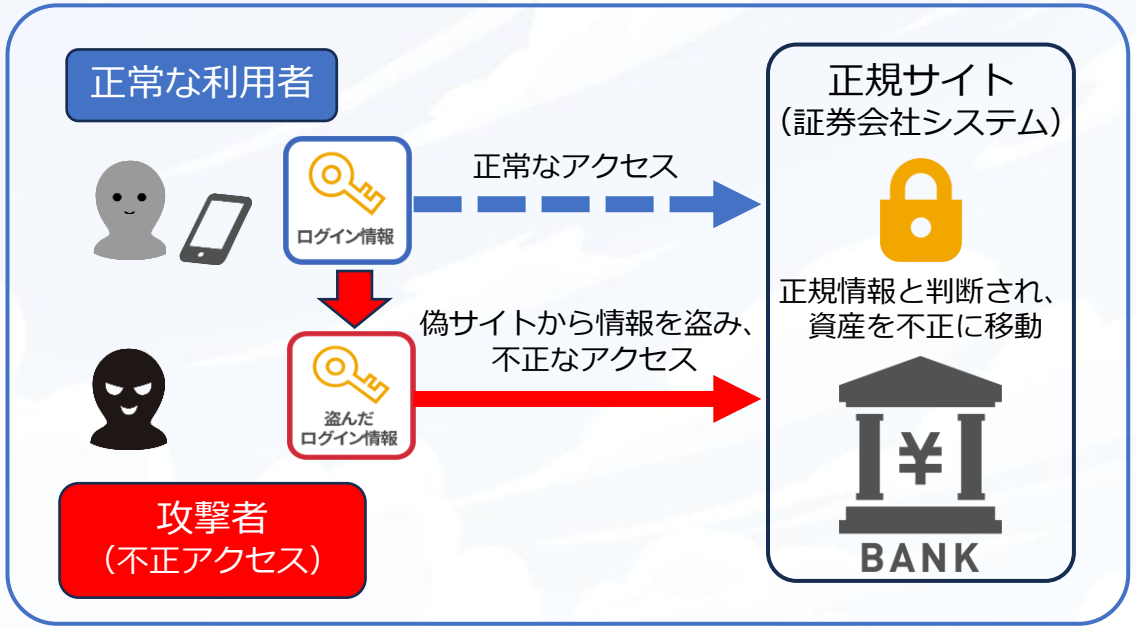
SIMスワップ詐欺

攻撃者が携帯電話の通信キャリアになりすまして不正な手続きを行い、他人の電話番号を
自分のSIMカードに紐づけて乗っ取る詐欺手法です
不正送金の手口の約3割がSMS認証突破を含むもの

不正アクセスの手口の例

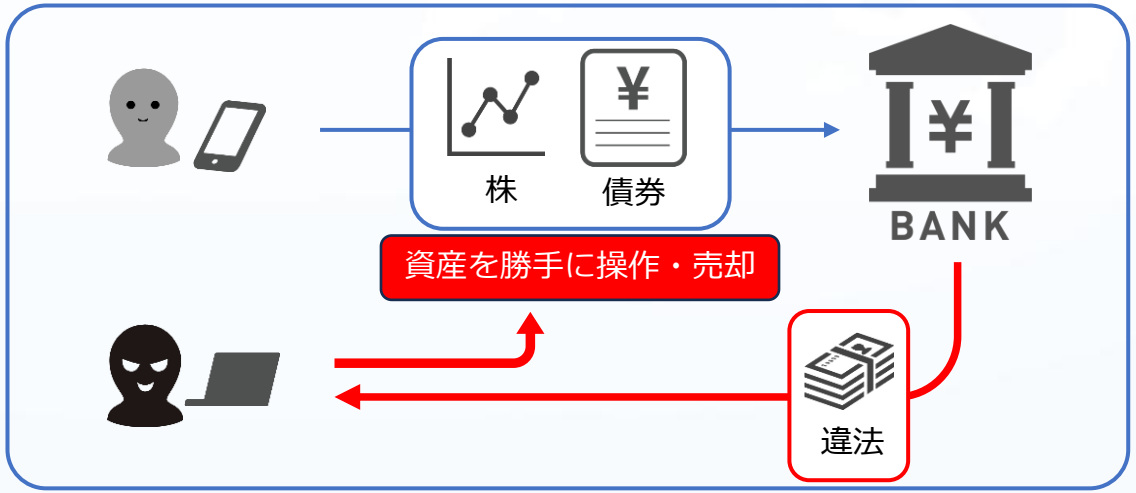
事例：フィシングによる不正アクセスの手口

ユーザーに偽のログインページを案内し、入力された情報を盗み取る手口です。
正規のログイン情報を使って不正にアクセスし、資産が移動される被害が発生します。



犯行に使われた口座でも本人特定は困難

資産の移動記録は残りますが、犯人は他人名義の口座を使うため、本人の特定が難しくなります。



証券口座の乗っ取りに対する対策

公的機関が推奨する基本対策

ログイン通知や出金通知を有効化し、異常があれば即時に気づける環境を整える
端末に最新のセキュリティソフトを導入しておく

証券会社での対策

サイバーセキュリティ基本法では、企業側が顧客情報を安全に管理する責務を持つと明記
金融機関は、情報保護管理体制の整備が義務付けられている
証券会社によっては、独自のセキュリティ基準を策定するなど、対策が加速
一部の証券会社では、普段の利用状況と比較してリスクが高いと判断する仕組みが構築

口座の利用者側の対策

ログイン情報が盗まれないために、怪しいメールやWebサイトは開かない、ログイン情報を他者に教えない、端末にセキュリティソフトを入れておく

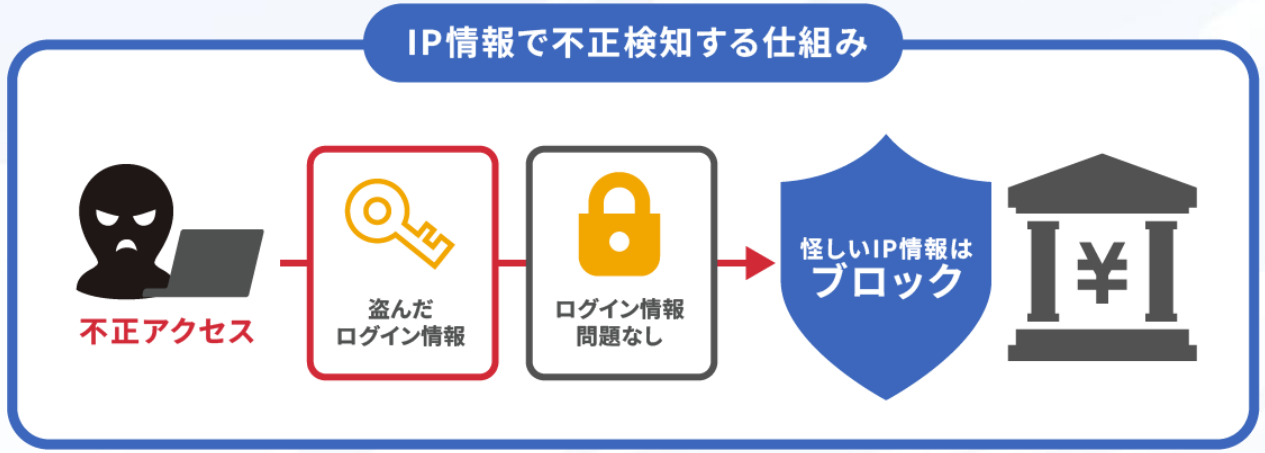
不正アクセスを検出するIP Geolocation技術

IP Geolocationとは

インターネット上の通信端末に割り当てられるIP情報を分析する技術である。

アクセスしてきた場所（国・地域・都市）や接続環境を特定できる。

例えば、ユーザーが東京に住んでいるのに、海外からのアクセスが検出された場合、即座に異常として識別される。



SURFPOINT™の基本機能

IPアドレスと位置情報や企業情報など様々な情報を紐づけたデータベースである。

各社の要望に応じてシステムに組み込みやすい形式で提供できる。

高度な解析技術

IP情報解析の機能をさらに進化させている。

アクセス時のユーザー挙動（クリックパターンや滞在時間）も統合的に判断する。

AIによるリスク評価

AIがスコアリングを行い、高リスクな挙動を検出する。

ログイン制限や本人確認フローへ誘導することもできる。

株式会社Geolocation Technology

IP Geolocation技術を活用した証券口座への不正対策

証券コード：4018