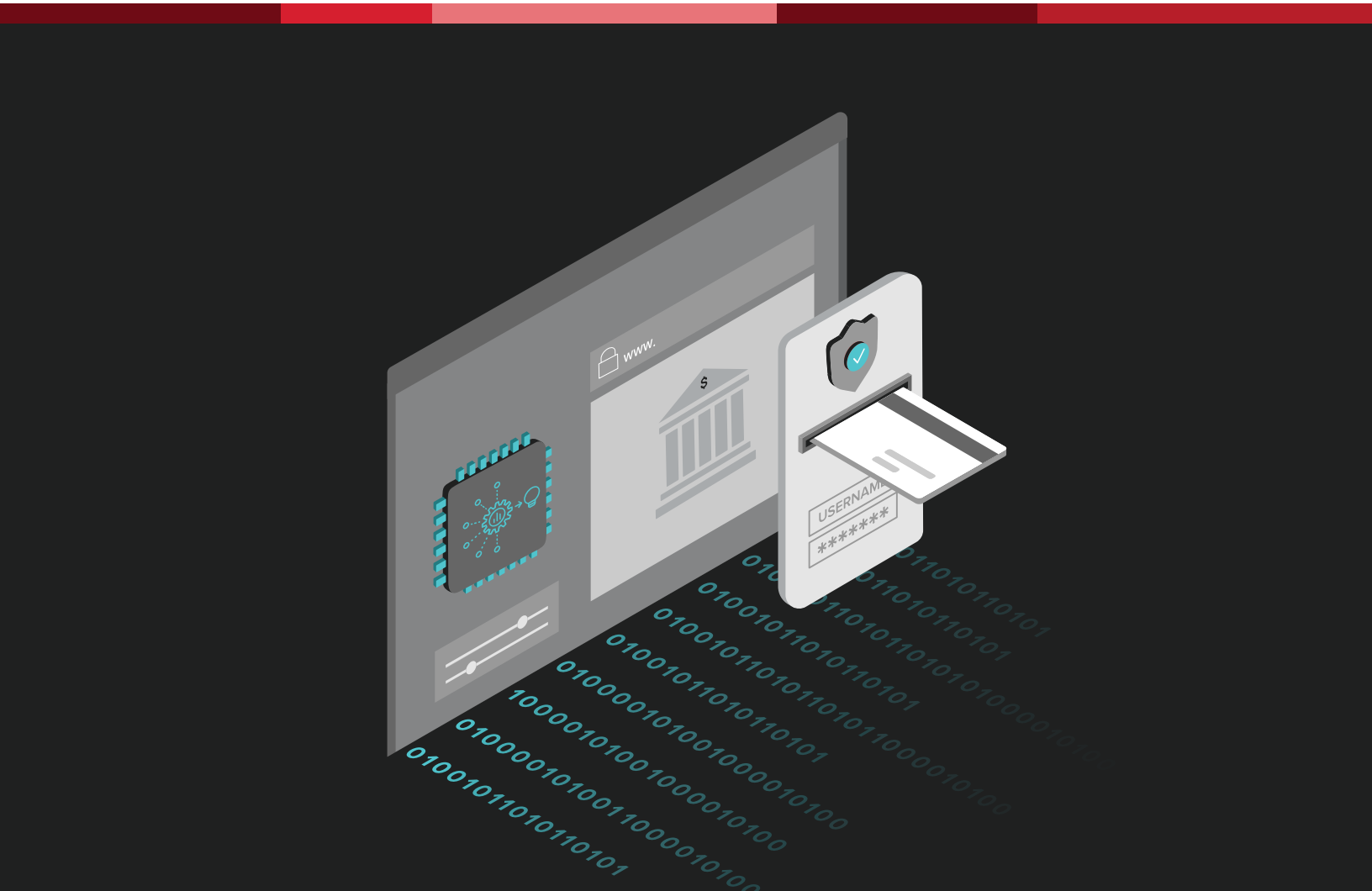
ケーススタディ

F5により北米の信用組合が顧客体験を99%向上させることに成功

同時に不正行為による損失も84%激減



COVID 19 によって、デジタルシフトは少なくとも 2 年加速し、一部では最大で 5 年加速すると推定されています。信用組合は、運用業務の多くをオンラインで行うようになっていますが、大手金融サービス企業のような高度な不正対策ができないことから、不正行為者にとっての格好の標的になっています。同時に、オンラインでの顧客体験に悪影響を与えないことも、顧客獲得、エンゲージメント、顧客維持の指標を維持したい信用組合にとって重要です。

このケーススタディで紹介する信用組合は、F5 の不正対策技術を使用することで、組合員のオンライン顧客体験における摩擦を 99.5% と大幅に削減し、不正行為による損失を 84% 防止しました。

デジタル時代の信用組合

独立系非営利団体の BAI* によると、デジタルバンキングは技術導入において「アーリーマジョリティ」カーブから「レイトマジョリティ」段階へと移行しつつあります。BAI が実施した調査では、銀行顧客の半数以上が、デジタル商品について、パンデミック以降その利用機会が増えたと回答し、その 87% がパンデミック後も利用増加を継続する予定があると回答しています。これは、不正行為に対するデジタル攻撃対象が増えることを意味します。また、パンデミックによって、スミッシング / フィッシング、ソーシャルエンジニアリング詐欺などの手法で顧客情報を盗もうとする行為が増加しています。このような行為に対抗するためには、不正行為を減らすと同時に、オンライン顧客体験を向上させる、総合的な不正対策ソリューションが必要です。

デジタルシフトが進んでいる最中、残念ながら、信用組合は、大手銀行よりも簡単な標的であると不正行為者に思われています。この主な理由は、信用組合では、不正防止技術への投資が、大手金融機関に比べて限定的であるということです。

大手銀行と同じサービスを提供しなければならないというプレッシャーから、信用組合は、適切に保護するために必要なサイバーセキュリティや不正対策インフラストラクチャを備えていない中でオンラインバンキングサービスを提供しなければならないという、苦しい立場に追い込まれています。さらに、信用組合は、さまざまなデジタルタッチポイントにおいて、優れたオンライン体験を組合員に提供することにも苦労しています。

幸いなことに、F5 は、信用組合向けに、すぐに使え、導入が簡単な、セキュリティと不正対策ソリューションを手頃な価格で提供しています。

顧客：北米のある信用組合

100 億ドル以上の AUM を有する北米のある信用組合は、アカウント乗っ取りの結果として発生するオンライン不正送金 / 不正支払いによる損失を削減したいと考えていました。

課題：アカウント乗っ取りの増加により、送金不正行為が多発

COVID 19 により、この信用組合はデジタル活動に力を入れていました。多くの金融機関と同様、この信用組合でも、不正行為による損失は拡大していました。

不正行為者は、顧客のアカウントを乗っ取り、オンラインのデジタル Web およびモバイルチャネルを介して、複数の不正送金取引を行っていました。この信用組合の既存の認証対策とデバイス ID ソリューションの回避に成功した不正行為者は、不正送金を行い、資金をミュールアカウントに吸い上げて、この信用組合の顧客口座から資金を流出させていました。

以下は、アカウント乗っ取りと不正送金が起こる仕組みです。

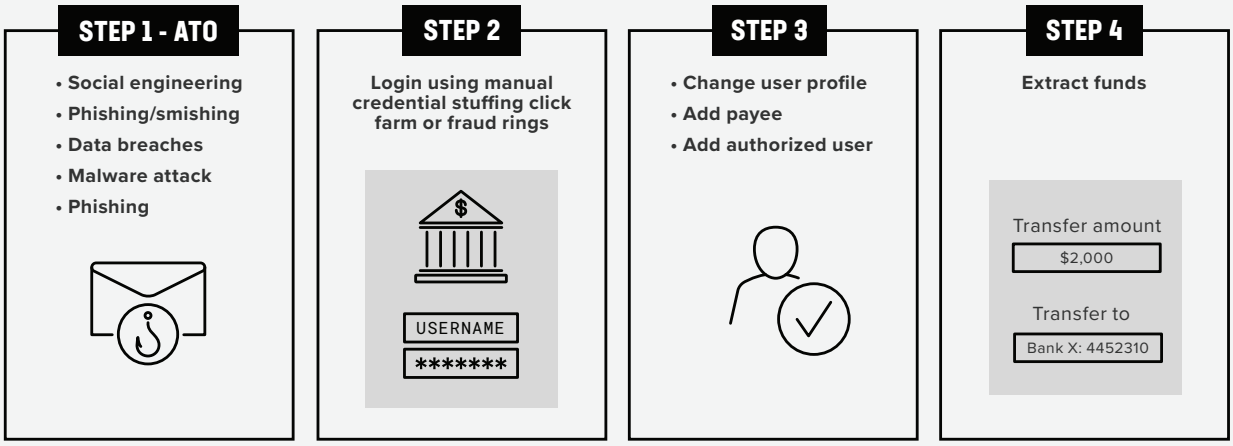


図 1：アカウント乗っ取りと不正送金

Juniper Research*** がプレスリリースの中で触れている調査によると、e コマース、航空券、送金、銀行サービスなどさまざまな業種の企業が今後 5 年間で累積 2,000 億ドル以上を損失します。また、このプレスリリースによると、「調査により、デジタル送金は不正支払いの成長分野であり、2020 年から 2024 年にかけて損失が 130% 増加することも判明しました」。この信用組合では、不正行為が急増しているだけでなく、不正行為による損失に対する対策も効果がありませんでした。また、ログイン時の多要素認証（MFA）により組合員に不要な摩擦を与えていました。その結果、多くの正規の顧客がオンライン体験において摩擦を受けることになりましたが、実際には不正行為による損失は減少せず、不正行為のリスクも軽減されませんでした。

F5 の不正防止ソリューションによるサポート

この信用組合に対し、F5 のボット対策および不正対策技術は、自動化されたボット攻撃による不正行為と、不正行為者による手動での不正行為の検出および対策をサポートしました。

F5 のボット対策技術を導入したところ、ログイン時のトランザクションの 40% が、実際はクレデンシャルスタッフィングによる悪意のある自動化の結果であることがわかりました。

クレデンシャルスタッフィングとは、サイバー犯罪者があるアプリケーションから盗んだユーザー認証情報を使って、別のアプリケーションでその認証情報をテストすることです。攻撃者は、高度な自動化ツールやボットを使用して、アプリケーションのログイン機能を狙い、時には 1 日あたり数十億回の攻撃を実行します。

多くのユーザーはオンラインサービス間でパスワードを使い回すため、F5 は、盗まれた認証情報リストの 0.1% ～ 2% が通常ターゲットサイトで有効であり、そこからアカウント乗っ取り（ATO）につながる可能性があることを発見しています。また、毎年何十億もの盗まれた認証情報がダークウェブに流出し、販売されているため、攻撃者は常に豊富な認証情報を ATO 攻撃に使用できます。

F5 は、高度な自動化攻撃の結果として、この信用組合のアカウントが広範囲にわたって乗っ取られていることを明らかにして、これらをリアルタイムで検知およびブロックできました。

F5 の不正防止技術を導入したところ、この信用組合にとって重大な不正行為を検知できました。F5 は、不正行為に関連していると見られたユーザーの行動、環境、デバイス、ネットワーク信号を使用してオンライン不正請求を検知しています。F5 が数百の独自の信号によって確認し、収集および分析した異常の例を示します。これにより、不正行為による損失を数千万ドル削減できました。F5 が収集および分析したテレメトリに基づき発見した異常は以下のとおりです。

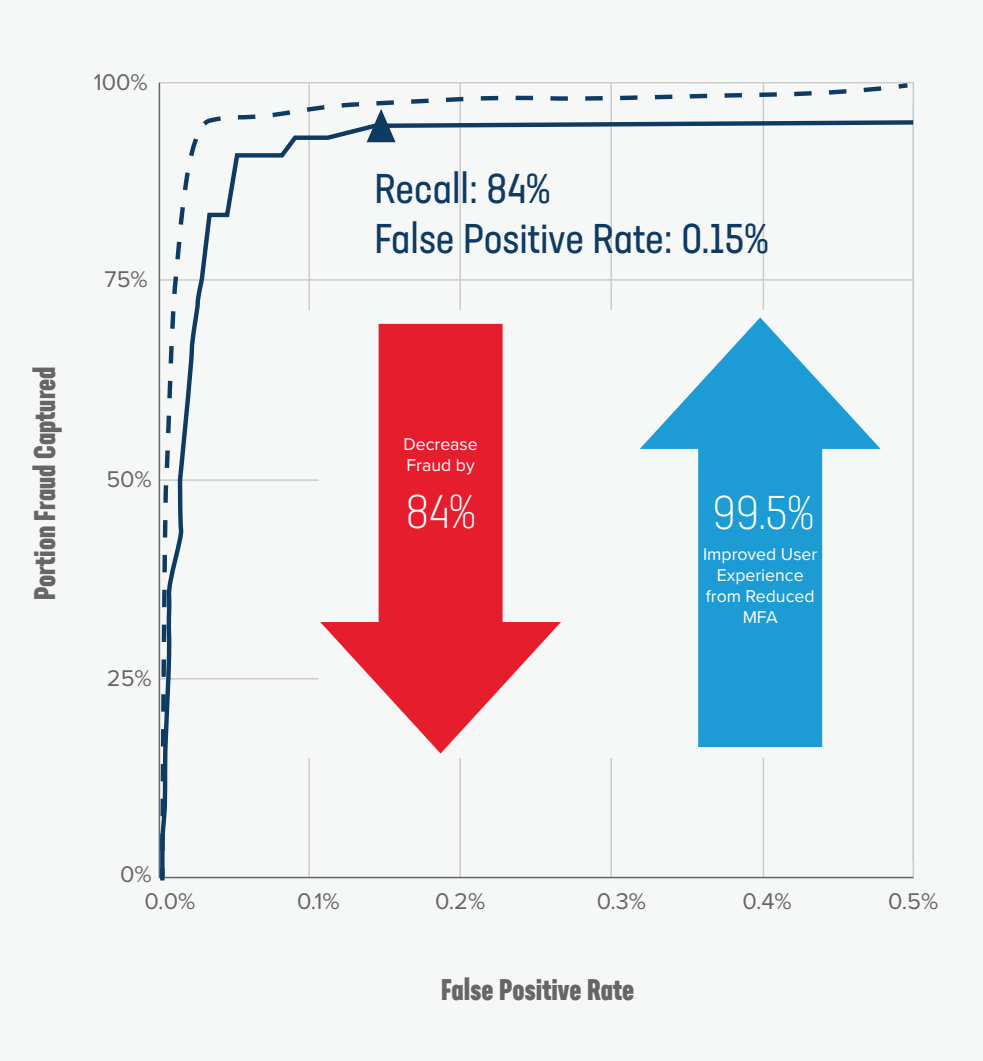
- コピー＆ペースト：不正行為者がログインフォームのフィールドにデータを定期的にコピー＆ペーストしていることが確認されました。正規のユーザーは通常このような行為はしません。
- 画面の切り替え：ブラウザウィンドウと別のウィンドウを切り替えて使用していることが確認されました。これは恐らく、盗んだ認証情報のリストからカット＆ペーストしているものだと思われます。
- 異様な画面領域使用：不正行為者のブラウザウィンドウには、かなりの使用可能面積が残されていました。これは恐らく、盗んだ認証情報のリストをテキストファイルで横に表示できるようにするためだと思われます。
- デバイスとの親和性：同じデバイスから多数の組合員がログインしていることが複数回確認されました。
- 環境のなりすまし：不正行為者が、ブラウザのユーザーエージェント、OS のバージョン、アプリケーションのバージョンなど、それぞれの環境を隠す、または偽装しようとしている行為が確認されました。JavaScript のトップコントリビュータである F5 のなりすまし対策機能は、市場で最も成熟しているものの 1 つです。
- VPN の利用：多くの場合、不正行為者は、VPN からログインしていました。これも身を隠すために使用する方法の 1 つです。

結果と投資利益率

この信用組合の結果は明確でした。以下のように、不正行為による損失の大幅な削減、ユーザーの摩擦の軽減、極めて低い偽陽性率という形で、驚くべき投資利益率（ROI）を示しました。

1. 悪意のある自動化（ログイントラフィックの 40%）の検知とリアルタイムのブロック
2. 年間不正検知率の向上：84%
3. ユーザーの摩擦 / 不要な MFA チャレンジの削減：99.5%
4. 極めて低い偽陽性率：0.015%

図 2：不正検知の一部と偽陽性率



これらの結果により、この信用組合は、F5 の技術に対する投資の価値をすぐに実感できました。現在では、業務に悪影響を与えることなく、不正検知が向上し、不正行為による損失が削減され、さらに組合員のオンラインユーザー体験が著しく改善されました。

詳しくは、F5 の担当者にお問い合わせいただくか、f5.com をご覧ください。

* https://www.bai.org/banking-strategies/article-detail/covid-19-pushes-digital-banking-adoption-to-the-tipping-point/
** https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion
*** https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion