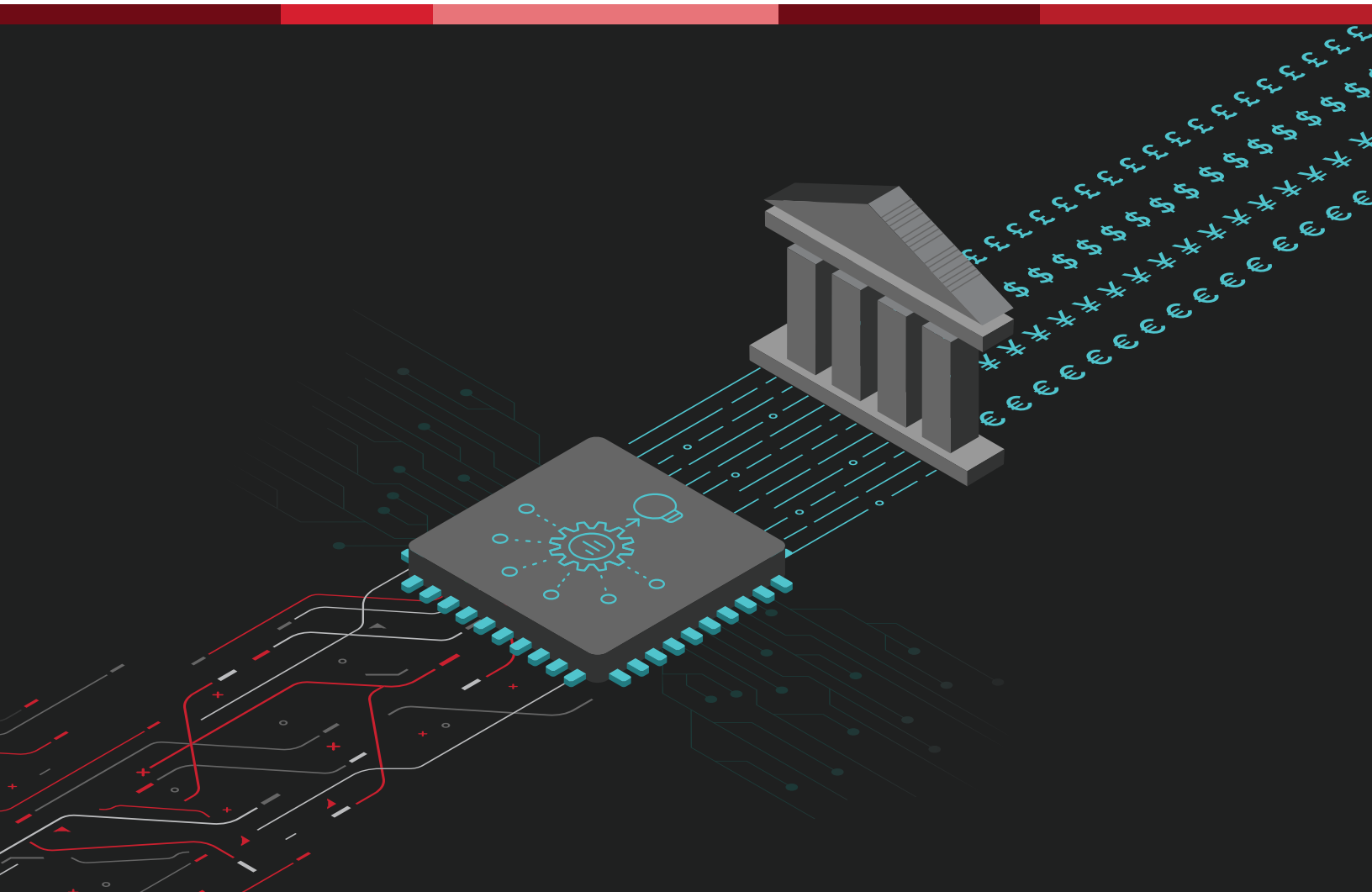
ケーススタディ

F5は、デジタルバンクが既存の不正対策ソリューションの177%の不正を検知することに貢献しています



F5 DISTRIBUTED CLOUD ACCOUNT PROTECTION が金融企業にもたらすメリット

不正行為を確実に検知および排除することで、以下のことを実現します。

1. さらに多くの不正行為の検知
2. 偽陽性率（FPR）の低下
3. 不正対策パフォーマンスの向上
4. 不正行為による損失の削減と利益の増加

COVID-19 により、デジタルシフトは少なくとも 2 年加速しました。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。

Experian Global Identity and Fraud Report によると、

- モバイルのアカウント乗っ取り（ATO）は過去 4 年間で 2 倍に増加しています。
- 退職金口座への不正行為が過去 1 年間で 180% 増加しています。

顧客：北米の銀行

10 億ドル以上の AUM と数百万人の顧客を持つ北米のデジタルバンクは、不正行為による損失を削減したいと考えていました。この銀行の顧客の 90% 以上はオンラインで取引をしています。リテールバンキングの顧客との取引は主に Web およびモバイルアプリケーションで行われています。

課題：アカウント乗っ取りと不正アカウント開設

この銀行では、COVID-19 に起因する不正行為による損失がピークを迎えていて、2020 年 5 月の損失だけでも過去最大級となりました。不正行為者は、被害者のアカウントを乗っ取り（ATO：アカウント乗っ取り）、オンラインバンキング経由で複数の不正送金を行っていました。また、不正行為者は、盗まれた ID（サードパーティ不正行為）と合成 ID（ファーストパーティ不正行為）を使って、複数の不正アカウントを作っていました（AO：不正アカウント開設）。不正行為者は、これらのアカウントをドロップアカウントとして利用して、COVID-19 関連の複数の政府給付パッケージを悪用し、他の銀行や信用組合で ATO 不正行為を行いこのドロップアカウントに送金していました。また、この銀行の顧客の何人かは、標的型のスミッシング / フィッシングキャンペーンの被害に遭いました。この銀行によると、不正行為の 60% は ATO、40% は AO に端を発するものでした。この不正行為の 60% 以上では、金銭目的以外の行為（住所変更や振込先の追加など）が行われていました。これは不正行為者が送金前の下調べのために行ったものでした。この銀行では、主要なデバイス識別ソリューションとレガシー不正対策エンジンを導入していましたが、これらのシステムでは、上記のような不正行為の 80% 以上を検知できませんでした。

F5 が選ばれる理由

F5 は、アプリケーションセキュリティの提供において、信頼できるリーダーです。攻撃トラフィックをリアルタイムで正確に検知してアプリケーションを保護する、AI を活用した F5 のソリューションと同じ精度が、オンライン不正行為の確実な検知と排除にも提供されます。

解決策：不正行為による損失の削減

さらなる不正行為の確実な検知と排除。F5 は、この銀行に対し、業務に悪影響を及ぼすことなく、さらに多くの不正行為を確実に検知および排除することを提案しました。F5 が提供する F5® Distributed Cloud Account Protection というソリューションは、人工知能と F5 のネットワークインサイトの力を活用して、安全かつ正確に不正取引を特定するので、企業は不正取引による損失を排除できます。Distributed Cloud Account Protection により、この銀行は、業務に影響を与えることなく、さらなる不正行為を特定できるようになりました。その結果、損失は大幅に減少しました。

以下は、一般的なアカウント乗っ取り（ATO）のステップです。

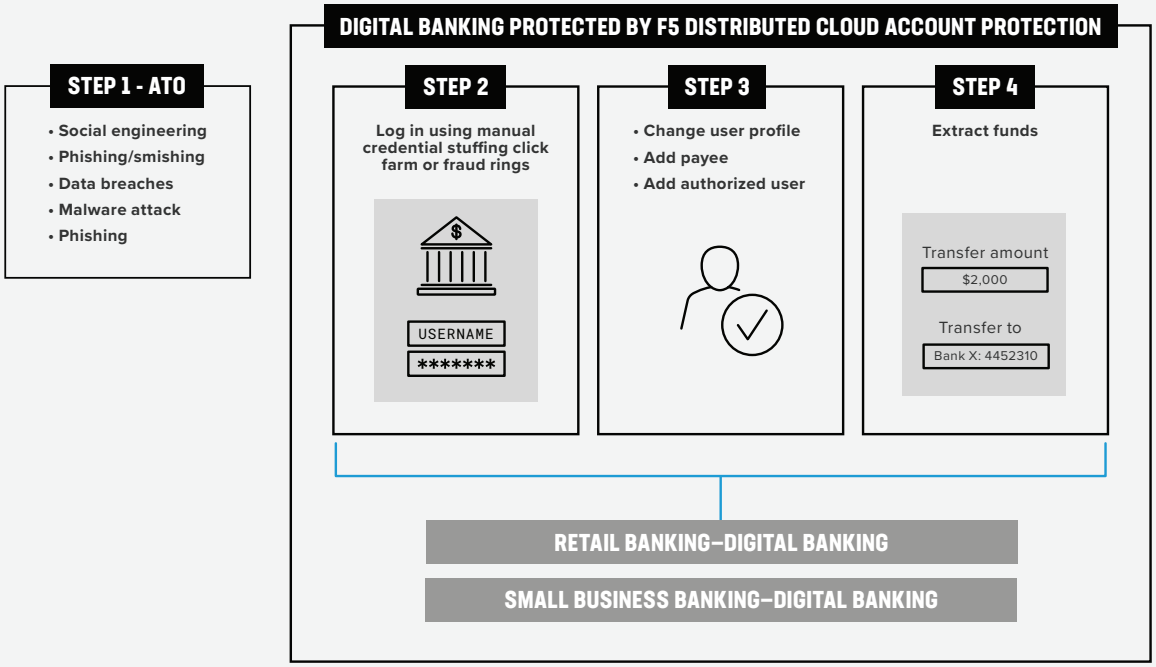


図 1：一般的な ATO のステップ

結果

Distributed Cloud Account Protection は、この顧客に偽陽性率（FPR）の低下という大きな価値をすぐにもたらしました。

- 0.1% の FPR で、177% 多くの不正行為を検知し、年間 620 万ドルを削減
- 0.5% の FPR で、276% 多くの不正行為を検知し、年間 970 万ドルを削減

このデータから導き出される結論：

Distributed Cloud Account Protection は、さらに多くの不正行為を確実に検知および排除します。この銀行では、現行のソリューションよりも極めて低い偽陽性率でさらに多くの不正行為を検知および排除できました。

Distributed Cloud Account Protection の導入により、不正行為による損失が減少しました。この銀行における不正行為による年間損失は、主にアカウント乗っ取り（ATO）と不正申請（FRAP）によるものですが、このサービスを導入してから大幅に減少しました。

Distributed Cloud Account Protection による業務への悪影響はありません。
このサービスは、ビジネス環境に悪影響を与えることなく、顕著で明確な結果をもたらしました。

業務に悪影響を及ぼすことなく不正取引を確実に検知

Distributed Cloud Account Protection は、オンライン不正行為を検知および排除するための新しい強力なソリューションを不正対策チームに提供します。

Distributed Cloud Account Protection の一意なテレメトリは、ユーザーの意図を理解することに重点を置いています。このサービスは、同じユーザーが使用する異なるブラウザやデバイス間だけでなく、F5 のネットワーク全体からの観測におけるコンテキストを接続できます。

Distributed Cloud Account Protection は、このデータと企業の不正行為ファイルを AI エンジンに送り込み、忠実度の高い単一の成果を提供します。

このソリューションは、すぐに不正行為を大幅に削減でき、その効果は AI エンジンのデータ消費量と学習量に比例して上昇します。

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。