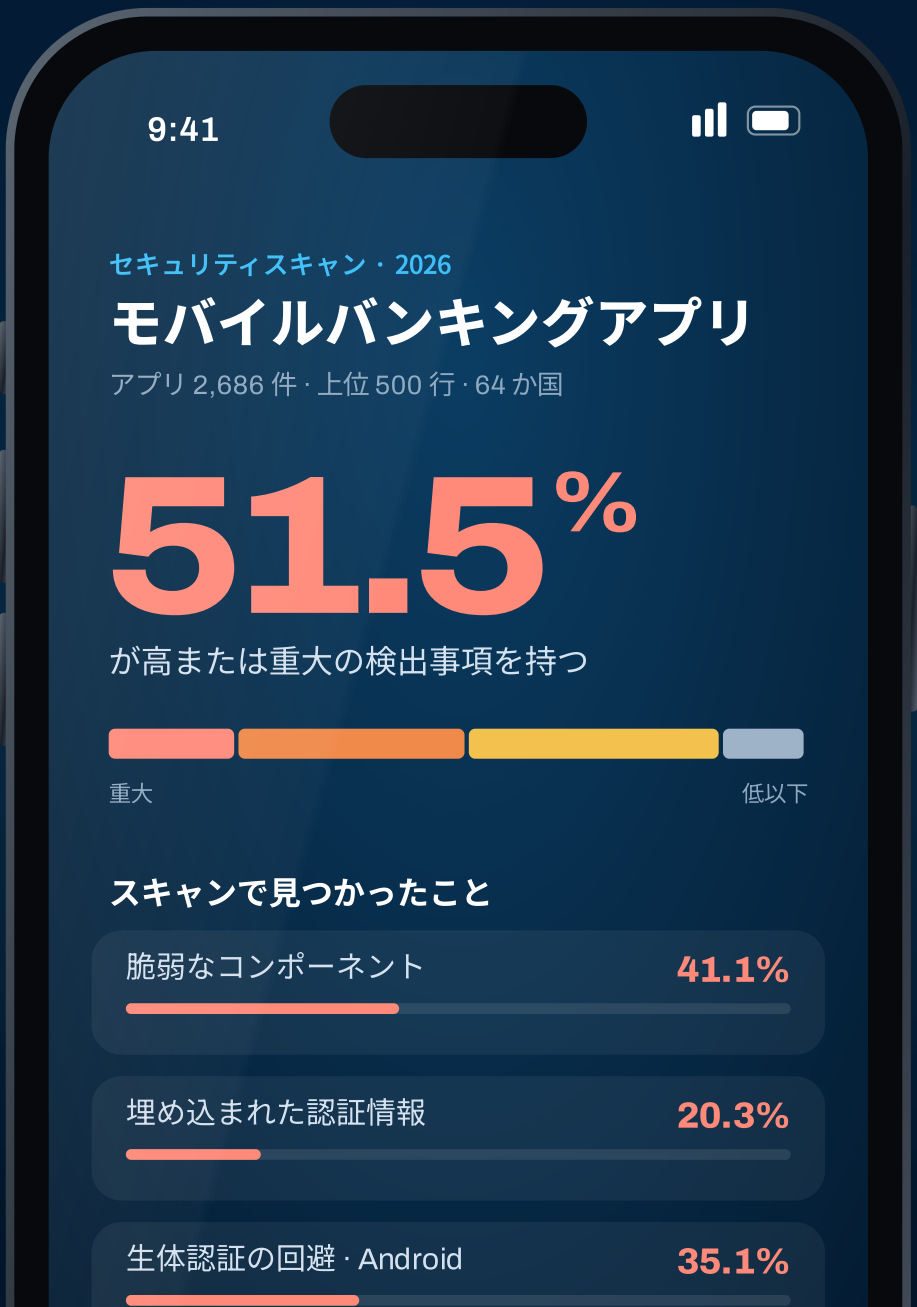
Ostorlab

モバイルバンキング アプリ セキュリティ レポート 2026

64 か国の上位 500 行が Android・iOS・HarmonyOS 向けに提供するバンキングアプリ 2,686 件の中身と、それが不正対策にとって何を意味するか。

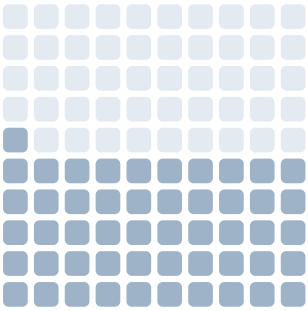


主な調査結果

最も深刻な検出事項を抱えるのは独立系ネオバンクです。

ネオバンクのアプリのスキャン結果は、従来型銀行のアプリよりも高または重大と評価される割合が高く（61.1% 対 51.2%）、その差はすべて独立系ネオバンクによるものです。従来型銀行が所有するネオバンクは、親銀行とほぼ同じ傾向を示します。

51.2%

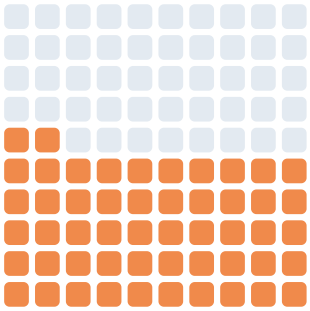


従来型銀行

店舗型のリテール銀行・法人向け銀行

アプリ 2,596 件

52.5%

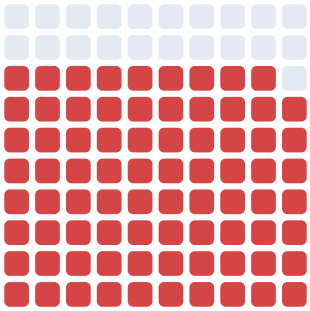


銀行系ネオバンク

従来型銀行のデジタルブランド

アプリ 61 件

79.3%



独立系ネオバンク

従来型の親銀行を持たないデジタル専業銀行

アプリ 29 件

差を生む要因

OAuth によるアカウント乗っ取り（高・重大）

6.1%
24.1%

安全でないシリアル化（高・重大）

6.4%
17.2%

Google API キー以外の埋め込み認証情報

19.8%
48.3%

一方で、最新の防御では先行

パスキー API を統合

4.6%
37.9%

アプリ／端末のアテステーション

19.9%
48.3%

鍵にひも付いた生体認証

74.0%
100.0%

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

目次

アプリ 2,686 件、全十一章。

各行から該当ページに移動できます。

主な調査結果：独立系ネオバンク 02
サマリー 04
九つの数字で見る本レポート 05

01 調査方法 06
全地域から集めたアプリ 2,686 件 07
三種類のエビデンスと、すべての数値に共通する五つのルール 08

02 バンキングアプリの作られ方 09
リスクが最も高いのはハイブリッド Web アプリ 10
一つのプラットフォーム、多数の銀行 11
更新は頻繁、それでも古い端末で動作 12
6〜9 週ごとに新リリース 13

03 アプリに含まれるもの 14
分析 SDK はほぼ全アプリに、不正対策 SDK はごく一部に 15
AI バンクはまだアプリの中にない 16

04 スキャンで見つかったこと 17
アプリの半数に深刻な検出事項 18
コードとプライバシーの検出事項は大半のアプリに 19
五件に一件のアプリが秘匿すべき認証情報を埋め込んでいる 20
十件に四件のアプリが既知の脆弱性を含む 21
プラットフォームごとに異なる弱点 22

05 認証と決済 23
パスキーのコードはあっても、パスキーは使えない 24
銀行のウェブサイトはアプリを指定しているか 25
生体認証の多くは鍵にひも付くが、三分の一は回避可能 26

06 シールディング：アプリが備える保護 27
コードに見つかった保護機能 28
チェックの多くは SDK が担う 29
防御を多層化しているアプリは少ない 30

07 アプリの外側 31
銀行ドメイン：耐量子化は進むが、脆弱性の報告先は乏しい 32
アプリの実態と合わないプライバシーラベル 33
Web 以外でも応答する銀行サーバー 34
六行に一行に公開された侵害記録 35
銀行が従う規制と、銀行自身の表明 36

08 脅威の動向 37
十行に四行がトロイの木馬の標的リストに 38
2026 年：攻撃者は銀行自身のアプリを悪用する 39
アプリのすり替えに銀行は気づけるか 40
被害額はどこに流れるか 41

09 地域・銀行タイプ・国別の結果 42
すべてに優れた地域はない 43
国別の結果 44
地域別に見た最も安全な銀行アプリ 45

10 ケーススタディ 46
CyberDakait：七つのトロイの木馬と一本の電話 47
WindRelay：被害者自身のアプリで組まれたローン 48
Hirudo：バンキングアプリをすり替えるトロイの木馬 49
コピーの中では、あらゆるチェックが偽装されうる 50
AI の認証情報になった Google API キー 51

11 次に取るべき対策 52
2026 年に銀行が取るべき対策トップ 10 52

A 定義とデータに関する注記 53

現代の不正を防ぐ対策は、いまだに少数派です。

今年は 64 か国の上位 500 行が提供するモバイルバンキングアプリ 2,686 件を調査しました。銀行は頻繁にアプリを更新しており、大半のアプリは基本的な対策を備えています。しかし、パスキー、アテステーション、ランタイムシールディングなど、現在の攻撃に有効な保護機能を備えたアプリは依然として少数です。

アプリの半数に深刻な検出事項

自動スキャンで高または重大の検出事項が見つかったアプリは 51.5% に上ります。低を超える検出事項がないアプリは 11.8% にとどまります。主な原因は、アプリに埋め込まれた認証情報（Google API キーを除いて 20.3%）と既知の脆弱性を持つコンポーネント（41.1%）です。

強固な認証はまだ広がり始めた段階

パスキー API を統合しているアプリは 4.9% にすぎず、アプリ／端末のアテステーションを使うアプリは 20.2% です。Android では、生体認証を鍵にひも付けているアプリが大半であるにもかかわらず、35.1% のアプリにスキャナーが回避できる生体認証フローがあります。

攻撃者はアプリそのものを狙うように

上位 500 行のうち 192 行のアプリが、公開されているバンキング型トロイの木馬の標的リストに載っています。2026 年には Hirudo や Gigabud などのキャンペーンがさらに踏み込み、被害者の端末上で正規のバンキングアプリを置き換えたり複製したりしました。英国では、2025 年の承認済みプッシュ型決済（APP）詐欺による損失の 52% がモバイルバンキング経由でした。

シールディングは部分的には一般的、全体としてはまれ

Android では 69.9% のアプリが root 化を検知しますが、商用またはプラットフォームのシールディング製品を組み込んでいるアプリは 26.9% にすぎません。本データはアプリに含まれるものを示すもので、それが攻撃にどこまで耐えるかは示しません。その評価には実機テストが必要です。

スキャンから得られた三つの結果

51.5%



のアプリに高または重大の検出事項がある

アプリ 2,686 件中 1,384 件

35.1%



の Android アプリに、スキャナーが回避できる生体認証フローがある

Android アプリ

4.9%



のアプリがパスキー API を統合。フィッシングで盗まれたパスワードを無効にする対策

九つの数字で見る本レポート。

コンポーネント 01

41.1%

のアプリが既知の脆弱性を持つコンポーネントを含む

アプリ 2,686 件中 1,103 件

第 04 章 · 17 ページ →

秘密情報 02

20.3%

のアプリが API キー、アクセストークン、秘密鍵などの秘密情報を埋め込んでいる

アプリ 2,686 件中 544 件（Google API キーを除く）

第 04 章 · 17 ページ →

古い端末 03

96%

のアプリが、セキュリティパッチの提供が終了したバージョンにインストール可能

Android 99% · HarmonyOS 100% · iOS 72%

第 02 章 · 12 ページ →

アテステーション 04

20.2%

のアプリがアプリ／端末のアテステーションを使用

コードを読めたアプリ 2,602 件中 525 件

第 05 章 · 23 ページ →

シールディング 05

26.9%

の Android アプリがランタイムシールディング製品を組み込んでいる

商用またはプラットフォーム製品、Android アプリ

第 06 章 · 27 ページ →

AI 06

アプリ 2 件

が大規模言語モデル（LLM）の API を参照。LLM SDK を組み込んだアプリはなく、端末上の ML を使うアプリは 28.3%

アプリ 2,686 件中。バーコード、文字、顔のモデルが中心

第 03 章 · 14 ページ →

トロイの木馬 07

38%

の銀行のアプリが、公開されているバンキング型トロイの木馬の標的リストに載っている

上位 500 行中 192 行。リストの大半は 2021〜2023 年のもの

第 08 章 · 37 ページ →

耐量子暗号 08

71%

の到達可能な銀行 Web ホストが耐量子 TLS をネゴシエート

完了したハンドシェイク 1,038 件中 732 件

第 07 章 · 31 ページ →

詐欺被害 09

52%

の英国の詐欺被害額（2025 年）がモバイルバンキング経由

承認済みプッシュ型決済詐欺 576.4百万ポンドのうち 301.8百万ポンド（UK Finance）

第 08 章 · 37 ページ →

第 01 章

01

調査方法

64 か国の上位 500 行のバンキングアプリ 2,686 件をダウンロードし、Android・iOS・HarmonyOS の各アプリを Ostorlab の自動セキュリティ分析にかけました。



画面：国別・地域別のサンプル。

2,686

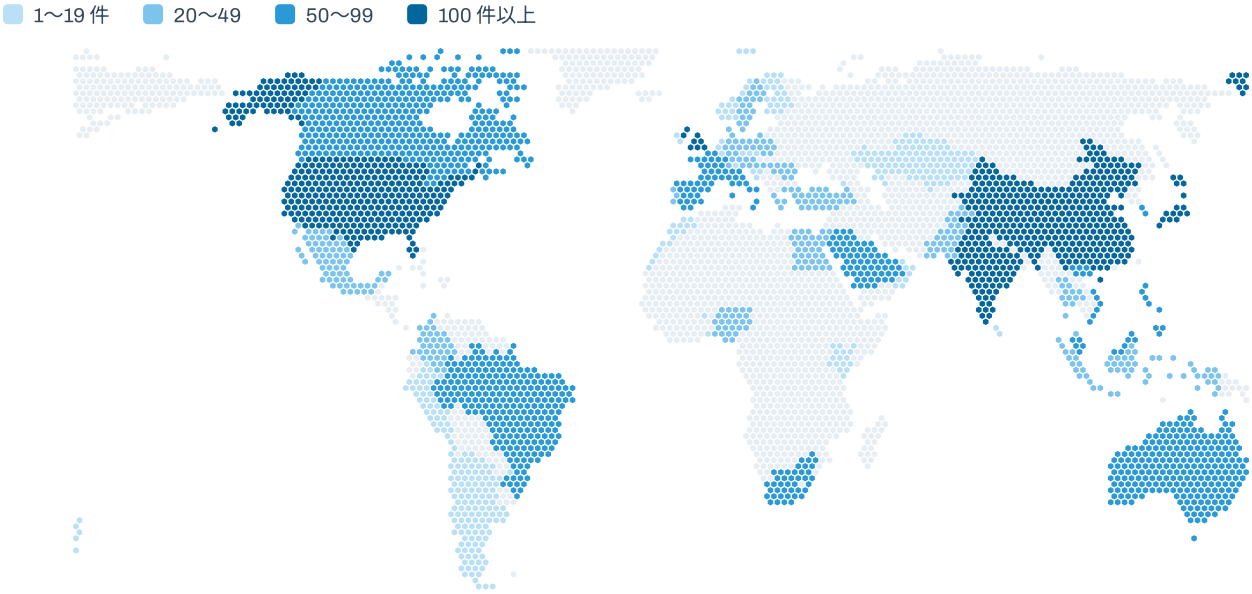
件のアプリ（64 か国の上位 500 行）

全地域から集めたアプリ 2,686 件。

サンプルは上位 500 行のアプリ 2,686 件で、そのうち 29 行はグローバルなシステム上重要な銀行（G-SIB）です。対象は Android、iOS、HarmonyOS です。

全大陸の 64 か国の銀行

図 1.1

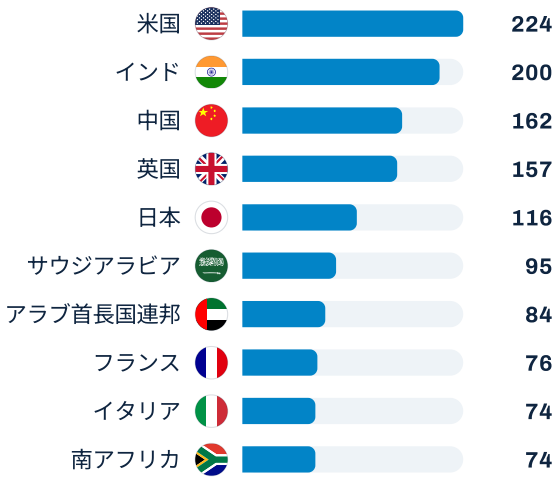


国別の分析アプリ数（銀行の本拠地市場別）。2,841 件のストア掲載を収集し、うち 155 件はダウンロードできませんでした。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

上位十市場

図 1.2

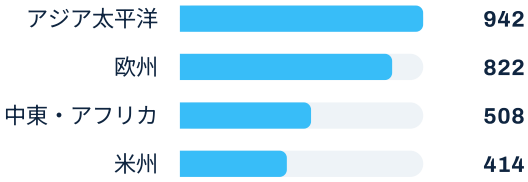


アプリ数（銀行の本拠国別）。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

最大の地域はアジア太平洋

図 1.3



アプリ数（銀行の本拠地域別）。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

三種類のエビデンスと、すべての数値に共通する五つのルール。

本レポートの各図は Ostorlab によるアプリ分析に基づいています。グラフ、本文、キャプションが一致するよう、すべての数値は同じ五つのルールに従っています。

アプリのインベントリ

各アプリの構成要素を一覧化：フレームワーク、SDK、権限、保護機能、通信先ホスト。全 2,686 件のアプリ。

自動セキュリティスキャン

Ostorlab のスキャナールールが脆弱性を検出し、深刻度を評価して OWASP MASVS に対応付けます。ルールはプラットフォームごとに異なります。全 2,686 件のアプリ。

コントロールのシグナル

認証、決済、プライバシーの各コントロールに関する十六項目のチェック。それぞれ判定の根拠となったコード上のエビデンスを伴います。全 2,686 件のアプリ。

数値の読み方

01 すべての割合に分母を明記

各割合が何件のアプリを対象にしたものかを、グラフ下のキャプションに記載しています。

02 プラットフォーム固有のルールはそのプラットフォーム内で集計

Android のみに存在するルールは、全アプリではなく Android アプリに占める割合として報告します。

03 不明は推測せず件数を示す

パック済みまたは読み取れないコードはチェックの分母から除外し、除外した件数を示します。

04 Google API キーは別に集計

Google はアプリに含めることを前提としているため、認証情報の主要な数値からは除外しています。

05 銀行名は公表しない

エビデンスは実在のアプリから取得していますが、銀行名は伏せ、秘密情報はすべてマスクしています。

数値を読む際の注意

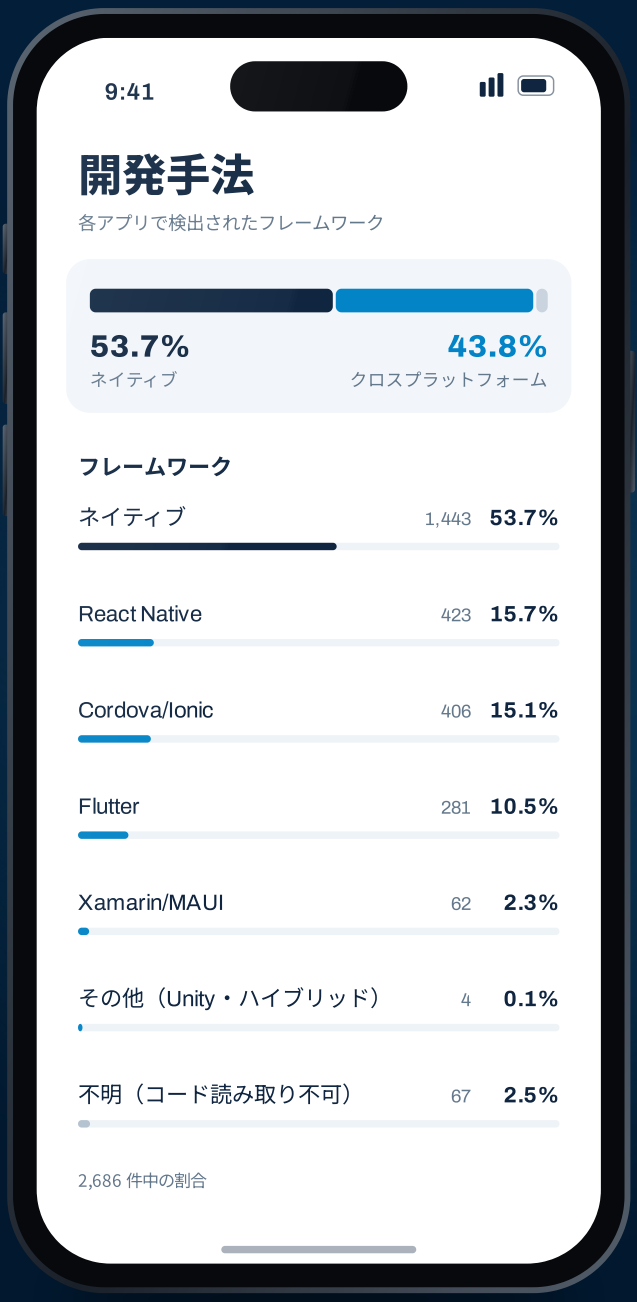
検出事項とは、配布パッケージ内でスキャナーのルールが一致したことを意味します。問題が存在することのエビデンスであり、本番環境で悪用可能であることの証明ではありません。深刻度はスキャナーの評価に従い、重大、高、中、低の四段階です。スキャナーはさらに低い二つの評価も用います。「潜在的」は、キーのような形式の文字列など、実際の欠陥である可能性があるものの人による確認が必要なパターンを示します。「堅牢化」は、欠けている安全策を示します。アプリは、重大、高、中、低のうち最も深刻な検出事項で評価され、「潜在的」と「堅牢化」の検出事項はその評価を変えません。グラフでこれらを数える場合は、その旨を明記しています。

第 02 章

02

バンキングアプリの作られ方

大半の銀行は今もネイティブで開発していますが、アプリの十件に四件はクロスプラットフォームのフレームワーク上で動いています。この選択はセキュリティの結果にも表れます。



画面：各アプリで検出されたフレームワーク。

43.8%

のアプリがクロスプラットフォームのフレームワークで構築されている

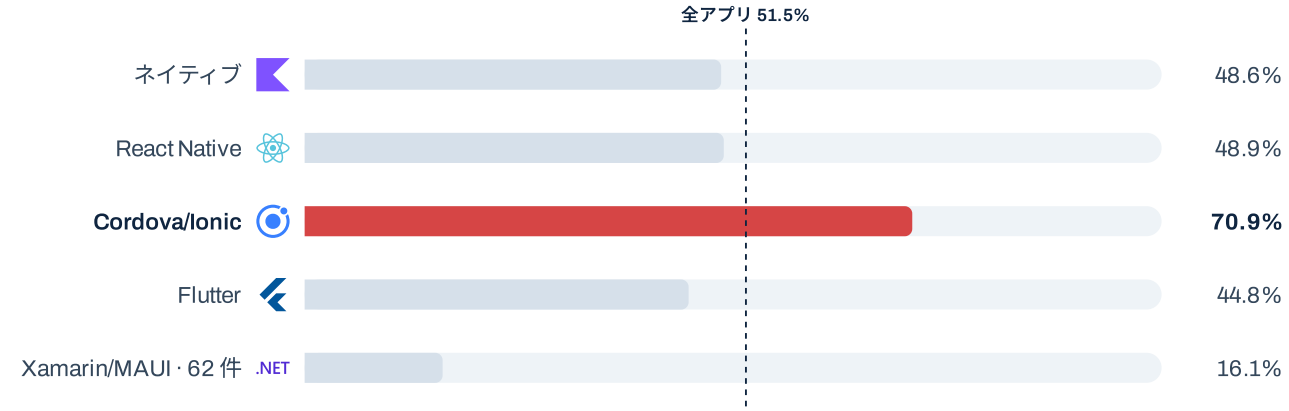
アプリ 2,686 件中 1,176 件

リスクが最も高いのはハイブリッド Web アプリ。

Cordova と Ionic のアプリは、Web アプリをネイティブのシェルに包んだものです。サンプルの 15.1% を占め、その 70.9% に高または重大の検出事項があります。ネイティブアプリでは 48.6% です。

Cordova・Ionic アプリの 70.9% に深刻な検出事項

図 2.1

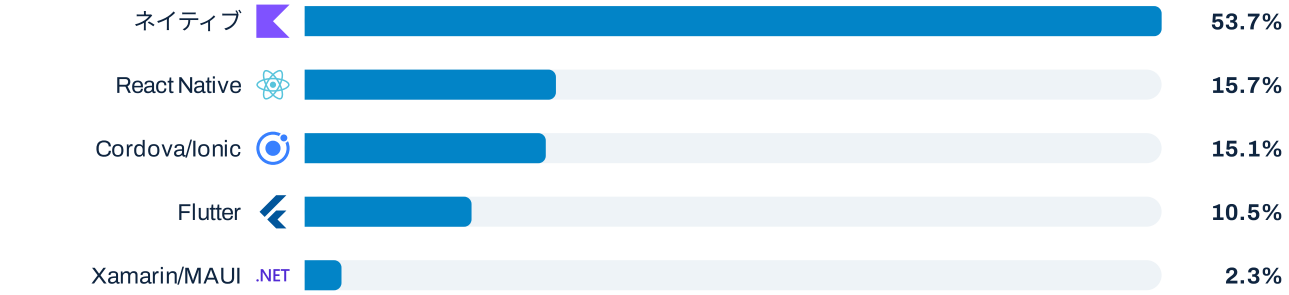


高または重大の検出事項を持つアプリの割合（フレームワーク別）。破線：全 2,686 件のアプリ。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

バンキングアプリの大半は今もネイティブで開発

図 2.2



フレームワーク別のアプリ 2,686 件の割合。コードを読めなかった 67 件は表示していません。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

Cordova と Ionic のアプリは脆弱なコンポーネントでも最多（72.2%）で、その大半は Web レイヤーに同梱された古い JavaScript ライブラリです。

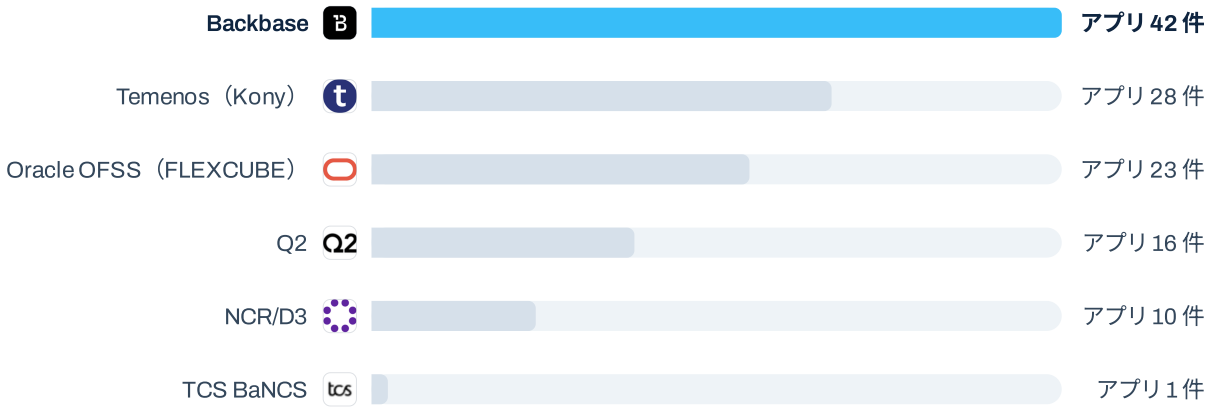
ネイティブ（48.6%）、React Native（48.9%）、Flutter（44.8%）の間に明確な差はありません。Xamarin と MAUI のアプリが最も良好に見えますが、62 件の小さな集団であり、認証情報の埋め込みは最も多くなっています（43.5%）。

一つのプラットフォーム、多数の銀行。

多くの銀行はアプリを一から開発せず、デジタルバンキングプラットフォームのライセンスを受けて自行ブランドで提供しています。サンプルのうち 120 件のアプリに、6 種類のこうしたプラットフォームのいずれかのコード上の特徴が見られます。

最も多く検出されたバンキングプラットフォームは Backbase

図 2.3



アプリ数。アプリ 2,602 件中 120 件が既知のプラットフォームの特徴と一致。一致には識別可能なプラットフォームのコードが必要なため、これらの件数は下限値です。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

> **プラットフォームが共有されている場合、その一つの脆弱性が利用行すべてに及ぶ可能性があります。**

なぜ重要か

共有プラットフォームのコードにある欠陥は、その上に構築されたすべてのアプリの欠陥です。修正はベンダーのリリースを待ち、さらに各銀行がそれを配布するまで届きません。一つの脆弱性の公表で、多数の銀行が同時に危険にさらされる可能性があります。

あるべき姿

プラットフォームベンダーに、ソフトウェア部品表（SBOM）、セキュリティテストの結果、合意したパッチ適用期限を求めてください。ベンダーのセキュリティアドバイザリは、自社のものと同じくらい注意深く追跡してください。

更新は頻繁、それでも古い端末で動作。

銀行はアプリをプラットフォームの最新状態に保っています。Android アプリの 72.1% が最新の Android API をターゲットにしています。しかし、どのプラットフォームでも、大半のアプリはセキュリティパッチの提供が終了した OS バージョンにもインストールできます。

どのプラットフォームでも、大半のアプリがパッチ未提供の OS にインストール可能

図 2.4



最小 OS バージョンを読み取れたアプリに占める割合（プラットフォーム別）。宣言された最小 OS バージョンが、セキュリティパッチが提供されている最古のバージョン（Android 14、iOS 18。HarmonyOS アプリは Android のバージョンを宣言）より古い場合に数えます。これはアプリが許容する範囲を示すもので、顧客が実際に使っている OS ではありません。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

古い端末のサポートはビジネス上の判断です。顧客は端末を使い続けるからです。リスクは、既知の未修正の欠陥を抱えたシステム上でアプリが動くことです。パッチ未提供のバージョンを拒否する Android アプリは 0.5% にとどまり、iOS では 28.5% が iOS 18 以降を要求しています。銀行はログイン時にパッチレベルを確認し、更新が提供されなくなった端末では高リスクの操作を制限できます。

各アプリをインストールできる最古のバージョン

図 2.5

Android と HarmonyOS · Android のバージョン

	Android	HarmonyOS
4 以前	0.8%	4.0%
5	4.4%	12.8%
6	5.3%	7.8%
7	17.4%	24.3%
8	19.5%	19.5%
9	13.1%	13.0%
10	16.5%	12.4%
11	7.0%	3.4%
12	12.8%	2.9%
13	2.7%	0.0%
14 以降	0.5%	0.0%

iOS · iOS のバージョン

	iOS
11 以前	1.8%
12	2.1%
13	5.0%
14	6.5%
15	27.0%
16	23.1%
17	5.9%
18 以降	28.5%

インストール可能な最古のバージョン別に見た、各プラットフォームのアプリの割合。各棒はそのバージョンちょうどを示し、該当するアプリはそれより新しいすべてのバージョンにもインストールできます。パッチが提供されている最古のバージョンは Android 14 と iOS 18 です。

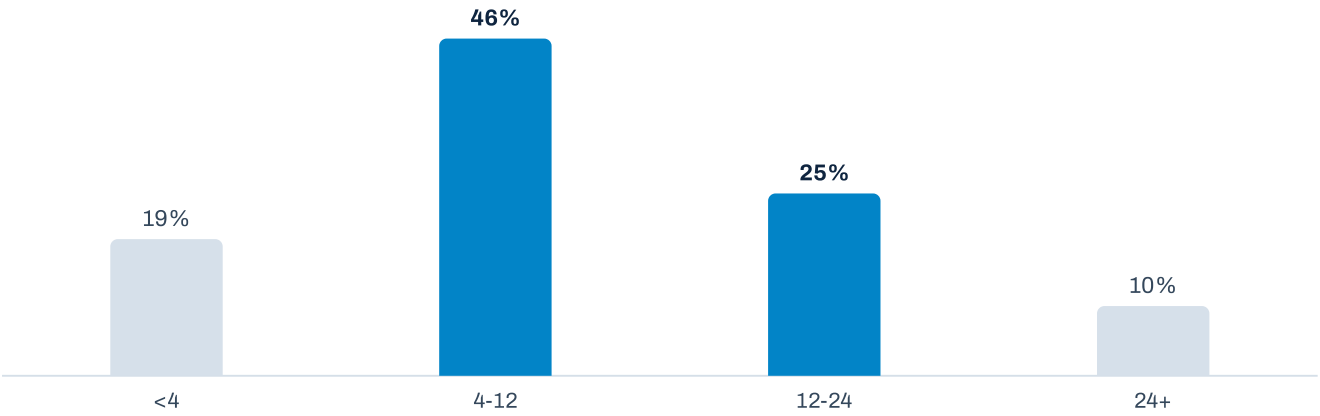
出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

6〜9 週ごとに新リリース。

Android アプリの中央値は年 8.9 回以上のリリース（Google Play のレビューから再構成）、iOS アプリの中央値は 6.0 回（App Store のバージョン履歴）です。HarmonyOS のストアは現行バージョンしか掲載しないため、HarmonyOS は測定できませんでした。頻繁なリリースは強みです。本レポートの検出事項に対する修正は、リリースを通じて顧客に届くからです。

大半のアプリは年 4〜24 回リリース

図 2.6



Google Play のレビューからリリース履歴を再構成できた Android アプリの割合（年間リリース数別）。中央値は 8.9 回で、レビューされなかったリリースは数えられないため下限値です。iOS：中央値 6.0 回（App Store のバージョン履歴から）。

出典 本レポートのために収集した Google Play と App Store の掲載情報およびレビュー。

75.1%
の Android アプリ（Play の更新日があるもの）が直近 90 日以内に更新

6.8%
が一年以上更新されていない

38億
Android アプリの Google Play インストール数の合計（下限値）

サイズ

ダウンロードサイズの中央値は Android で 68 MB、iOS で 38 MB、HarmonyOS で 129 MB です。これらのアプリのネイティブライブラリの半数は既知のサードパーティ SDK 由来で、銀行自身のものと特定できるのは 4% にすぎません。サードパーティのコードについては次章で取り上げます。

リリースは速く、コンポーネントは古い

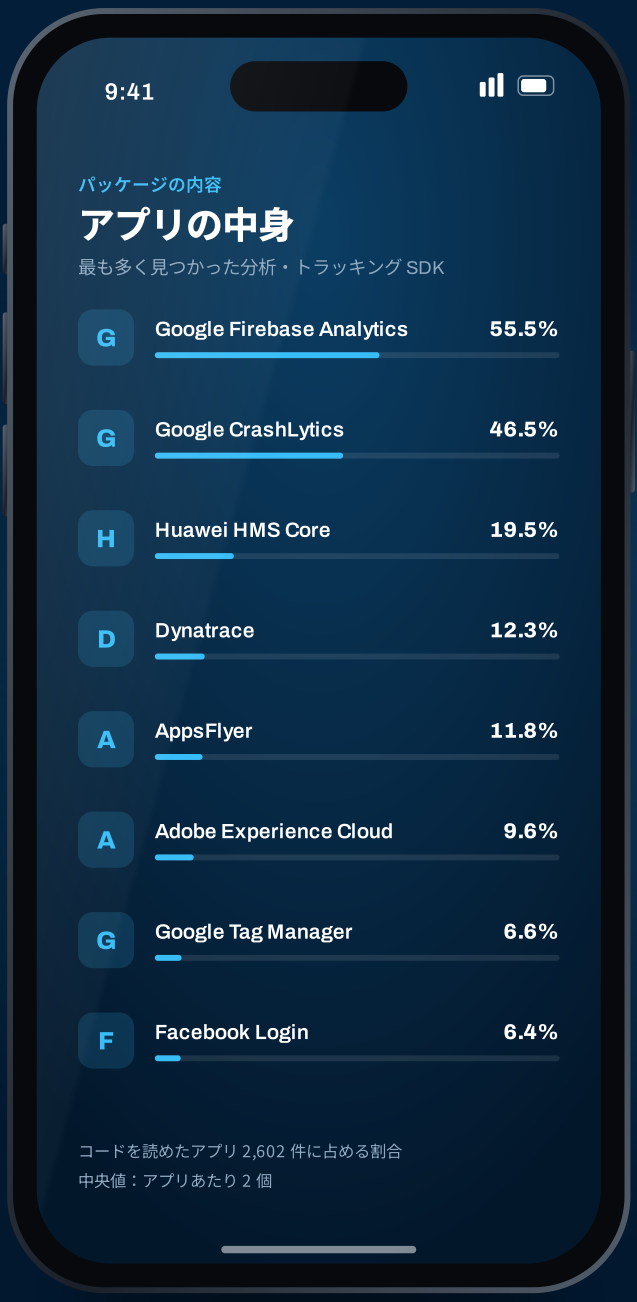
頻繁にリリースしても、すべての構成要素が最新に保たれるわけではありません。第 4 章で示すとおり、41.1% のアプリは今も既知の脆弱性を持つコンポーネントを同梱しています。

第 03 章

03

アプリに含まれるもの

バンキングアプリの大部分は他者が書いたコードです。分析、クラッシュレポート、不正検知、地図、スキャナー。SDKはそれぞれ独自のデータフローと独自の脆弱性を持ち込みます。



画面：最も多く見つかった分析・トラッキング SDK。

80.6%

のコードを読めたアプリが、分析またはトラッキングの SDK を組み込んでいる

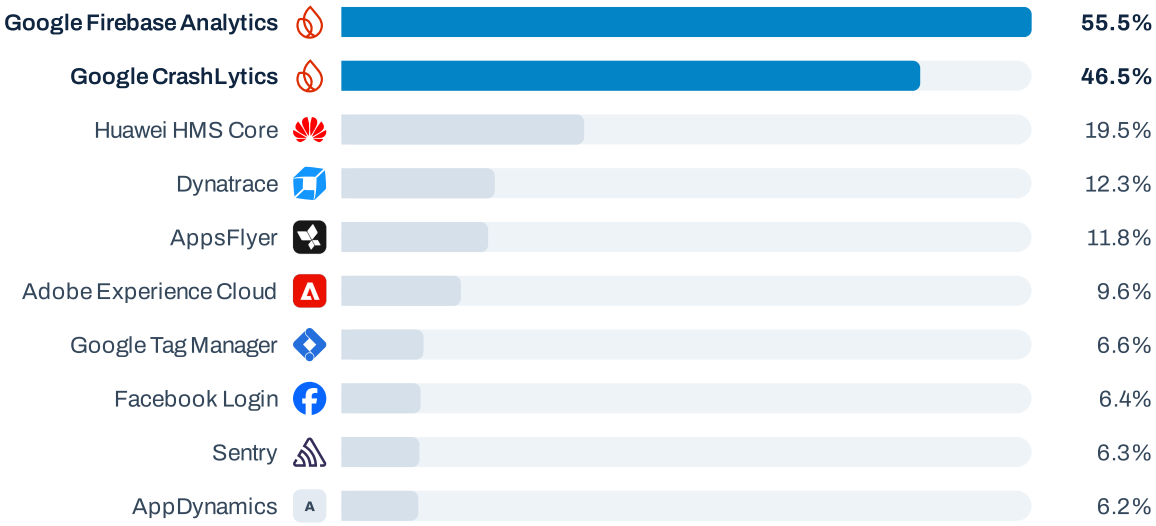
アプリ 2,602 件中 2,096 件

分析 SDK はほぼ全アプリに、不正対策 SDK はごく一部に。

Google の Firebase Analytics は 55.5% のアプリに含まれています。一方、銀行がアカウント乗っ取りをリアルタイムで検知するために使う不正対策・端末リスク専用の SDK は 12.1% です。

トラッカーの上位は Google の Firebase Analytics と Crashlytics

図 3.1

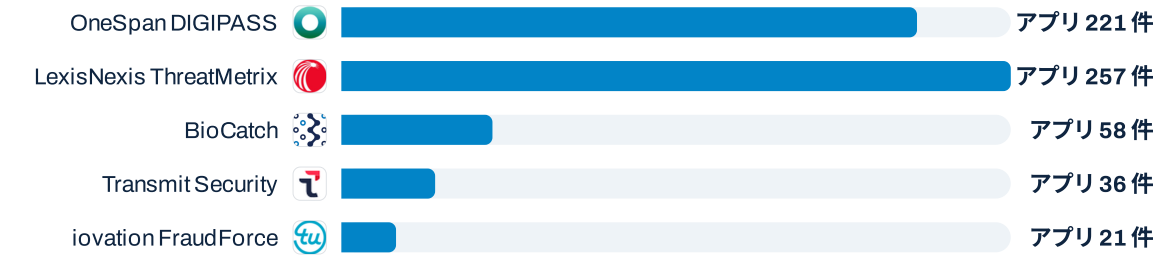


コードを読めたアプリ 2,602 件に占める割合。トラッカーのシグネチャは Exodus Privacy のデータベースによる。Huawei HMS Core は HarmonyOS アプリの 64% に含まれ、Huawei のプッシュ通知、位置情報、分析サービスを提供します。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

専門のセキュリティ SDK を使うアプリは少数

図 3.2



アプリ数。認証 SDK：アプリの 9.3%。不正対策・端末リスク SDK：12.1%。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

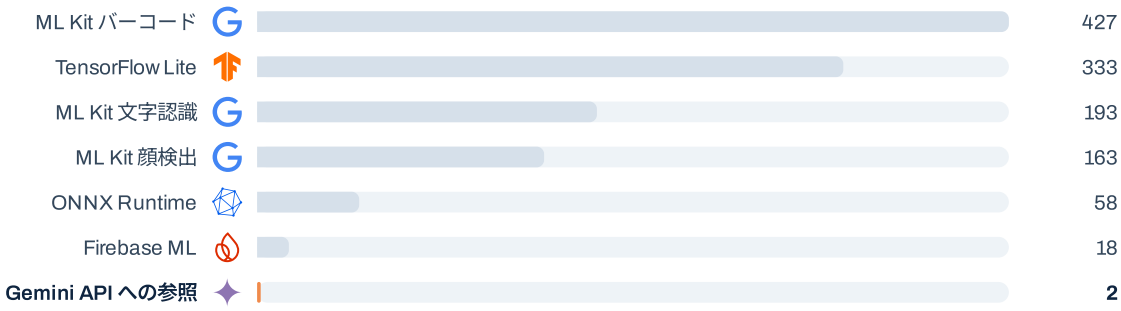
専門 SDK は iOS アプリに集中しています。不正対策・端末リスク SDK を組み込んでいるのは、iOS アプリの 35.3% に対し Android では 8.8% です。複数のベンダーが多数の銀行にサービスを提供しているため、そのセキュリティの影響は個々のアプリをはるかに超えます。

AI バンクはまだアプリの中にない。

28.3% のアプリが端末上の機械学習を搭載していますが、そのほぼすべてはバーコード、書類、顔の読み取り用です。大規模言語モデルの SDK を組み込んだアプリはありません。LLM API を参照するアプリは 2,686 件中 2 件で、AI プロバイダーのキーが埋め込まれたアプリは見つかりませんでした。

端末上の ML はバーコード、文字、顔の読み取りに

図 3.3

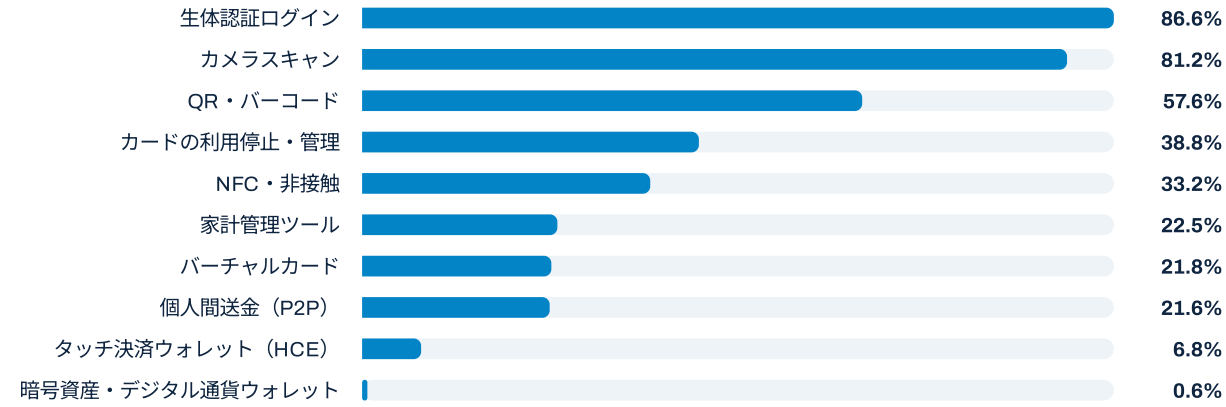


アプリ数。Gemini API への参照：アプリが Gemini API のエンドポイントを記述しているもの。LLM SDK を組み込んだアプリはありません。LLM 機能が完全に銀行のサーバー側で動いている場合、アプリには現れません。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

生体認証ログインとカメラスキャンはほぼ全アプリに

図 3.4



アプリ 2,686 件に占める割合。コード、リソース、権限から検出。コードに存在する機能が無効化されている場合もあります。暗号資産・デジタル通貨ウォレットのライブラリ：アプリのコードにウォレットまたはブロックチェーンのライブラリが含まれる場合に数えます。そのアプリが暗号資産取引を提供していることを示すものではありません。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

チャットボット・バーチャルアシスタント SDK を持つアプリは認証情報の埋め込みが多い

図 3.5



Google API キー以外の認証情報を一つ以上埋め込んでいるアプリの割合。チャットボット SDK とは、Dialogflow、Kore.ai、Kasisto、Watson Assistant などのベンダー製チャットボット・バーチャルアシスタントのライブラリで、大規模言語モデルではありません。Gemini API を記述しているアプリは 2 件のみで、いずれもチャットボット SDK は組み込んでいません。大手銀行ほどチャットボットを導入し SDK も多く組み込む傾向があり、これは相関であって因果ではありません。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

第 04 章

04

スキャンで見つかったこと

Ostorlab の自動スキャンでは、アプリの半数に高または重大の問題が一つ以上見つかりました。埋め込まれた認証情報と古いコンポーネントが上位を占め、各プラットフォーム固有の問題が続きます。



画面：サンプル中の実在アプリのスキャンレポート。

18.4%

のアプリに重大の検出事項がある

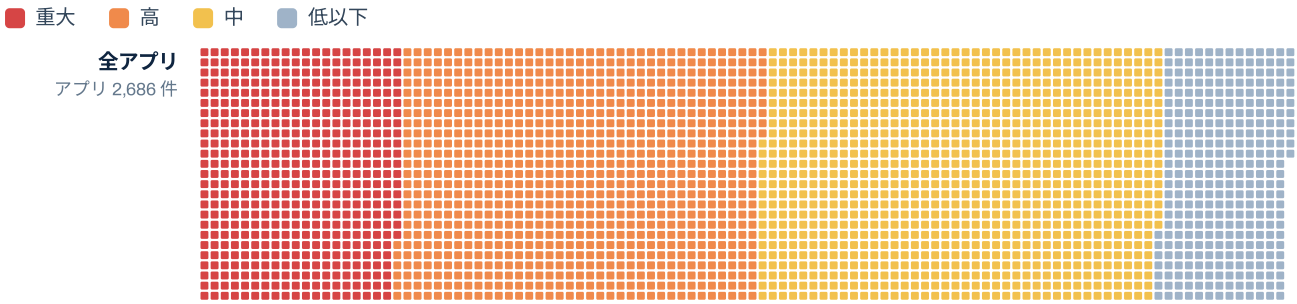
アプリ 2,686 件中 494 件

アプリの半数に深刻な検出事項。

各アプリは最も深刻な検出事項で評価しています。Android では 54.2% のアプリに高または重大の問題があり、iOS では 36.2% です。重大の検出事項が最も多いのは HarmonyOS アプリで 31.6% に上り、その主因は古いコンポーネントです。

全 2,686 件のアプリを最も深刻な検出事項別に表示

図 4.1

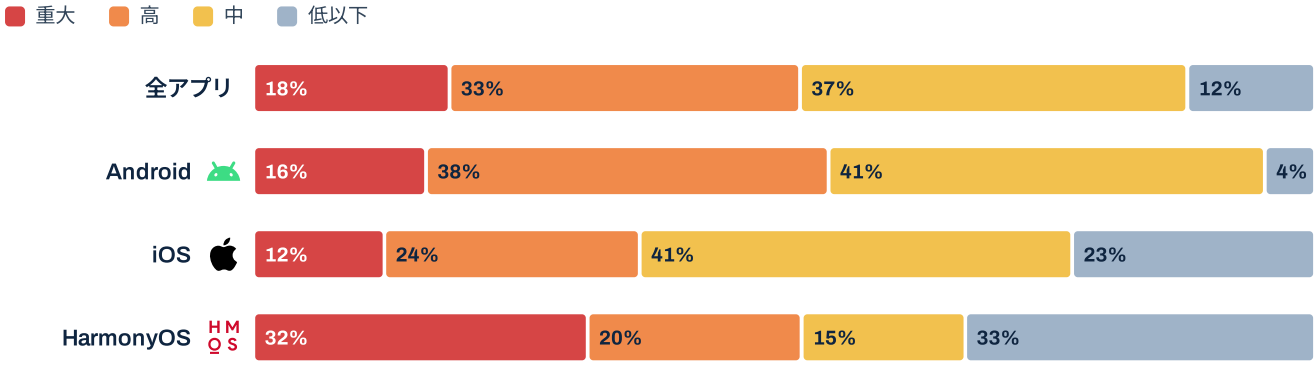


一つの四角が一件のアプリで、深刻度順に並べています。低以下には、最も深刻な検出事項が低、「潜在的」、「堅牢化」のアプリと、検出事項のないアプリを含みます。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

重大の検出事項が最も多いのは HarmonyOS アプリ

図 4.2



最も深刻な検出事項別のアプリの割合。全 2,686 件のアプリ。低以下には、最も深刻な検出事項が低、「潜在的」、「堅牢化」のアプリと、検出事項のないアプリを含みます。iOS と HarmonyOS で低以下の割合が大きいのは、これらのプラットフォームのスキャナールールが少ないことも一因です。

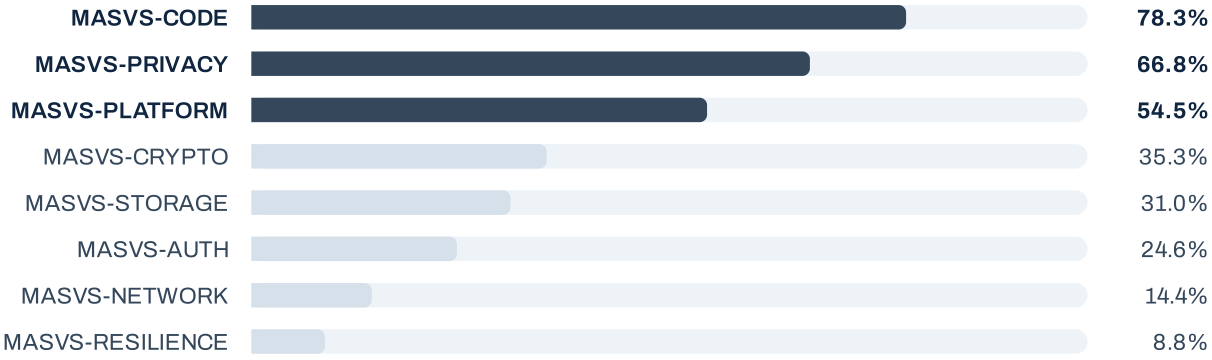
出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

コードとプライバシーの検出事項は大半のアプリに。

検出事項の大半は、モバイルアプリセキュリティの業界標準である OWASP MASVS のコントロールグループに対応します。重大、高、中、低の検出事項を数えると、コードに関する検出事項は 78.3% のアプリに、プライバシーに関する検出事項は 66.8% のアプリに見られます。iOS と HarmonyOS のアプリには暗号と認証の検出事項がなく、そのためこれらのグループの割合は低くなっています。

OWASP MASVS の各コントロールグループで検出事項があるアプリの割合

図 4.3



各グループで重大、高、中、低のいずれかの検出事項を持つアプリの割合（2,686 件中）。「潜在的」と「堅牢化」の検出事項は除外しています。Android の検出事項の 15% はどのグループにも対応しません。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。



サンプル中の実在アプリのスキャン

スキャナーが報告した一つのアプリ

検出事項 766 件、評価は一つ

サンプル中のこの Android アプリには、重大 2 件、高 2 件、中 757 件、低 5 件の検出事項があります。本レポートの他のアプリと同様、最も深刻な検出事項で評価され、評価は**重大**です。

一つのルールが一つのアプリで何度も一致することがあります。中の件数が多いのは、一つのシリアル化ルールが数百か所の呼び出し箇所に一致したためで、修正すべき問題としては一件です。

スキャナーはこのほか、「潜在的」を 98 件、「堅牢化」を 2 件報告しました。「潜在的」は実際の欠陥である可能性があるものの人による確認が必要なパターンを、「堅牢化」は欠けている安全策を示します。いずれもアプリの評価は変えません。

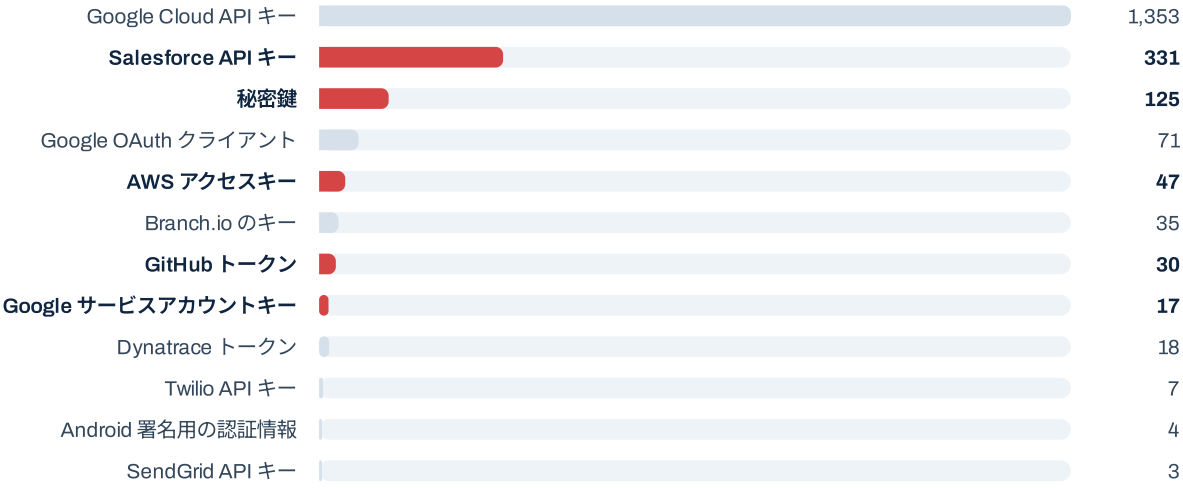
MASVS-AUTH-2 MASVS-CODE-1 MASVS-CODE-3 MASVS-CODE-4 MASVS-NETWORK-1 MASVS-PRIVACY-1 MASVS-PRIVACY-3 MASVS-PRIVACY-4 MASVS-STORAGE-1 MASVS-STORAGE-2

五件に一件のアプリが、秘匿すべき認証情報を埋め込んでいる。

59.8% のアプリに、識別可能な形式の認証情報が一つ以上含まれています。その大半は Google API キーで、Google はアプリに含めて配布することを前提に設計しています。これらのキーは Maps や Firebase などのサービスでプロジェクトを識別するもので、秘匿ではなく、クラウドプロジェクトで設定する制限（アプリの署名、指定した API）によって保護されます。各キーが制限されているかどうかはテストしていません。これらを除いても、20.3% のアプリが秘密鍵、クラウドのキー、アクセストークンを含んでいます（Android 18%、iOS 21%、HarmonyOS 28%）。

Google API キーに次いで多いのは Salesforce のキーと秘密鍵

図 4.4



スキャナーの認証情報ルールが各種別を検出したアプリ数。一つのアプリが複数を含む場合があります。別の手法であるパッケージ全体の検索では、Google API キーは Android アプリの 80%、HarmonyOS アプリの 71%、iOS アプリの 31% で見つかります（51 ページ）。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。



サンプル中の実在アプリのスキャンより。値はマスク済み

バンキングアプリは誰でもダウンロードでき、中身を読むことができます。

一つのアプリのパッケージ

この Android アプリには 4 種類の秘密情報の候補が含まれています。Google API キー、Sentry DSN、Firebase データベースのアドレス、署名付きトークンなどです。いずれもアプリをダウンロードした人なら誰でも読み取れます。

Google API キーは、アプリの配布後に新たなアクセス権を得ることがあります。51 ページのケーススタディを参照してください。

あるべき姿

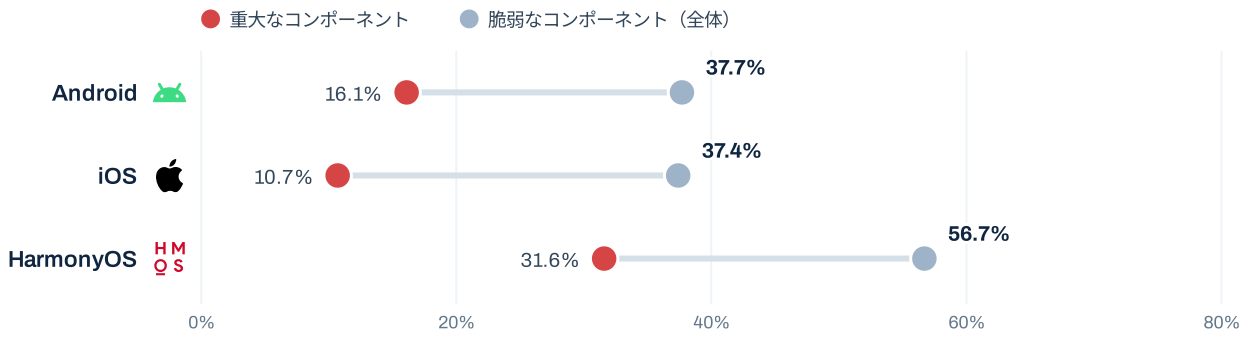
秘密情報はサーバー側に置き、アプリには短期間有効なトークンを発行してください。Google Maps のようにキーをアプリに含める必要がある場合は、アプリの署名と必要な API に制限したうえで、利用状況を監視してください。

十件に四件のアプリが既知の脆弱性を含む。

41.1% のアプリに、脆弱性が公表されているサードパーティのコンポーネントが含まれ、18.2% には重大と評価されたものが含まれています。最も状況が悪いのは HarmonyOS アプリです。

脆弱なコンポーネントが最も多いのは HarmonyOS アプリ

図 4.5

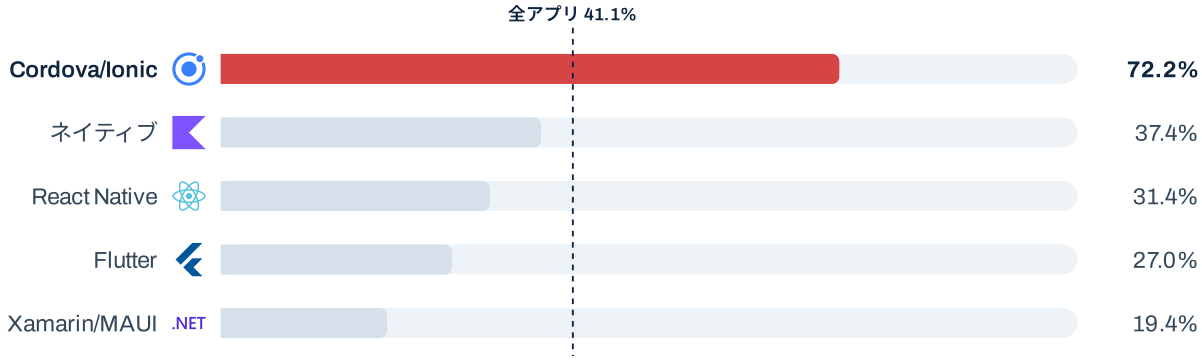


プラットフォーム別のアプリの割合。ラベルは脆弱なコンポーネントを一つでも持つアプリの割合です。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

Cordova・Ionic アプリの 72.2% が脆弱なコンポーネントを含む

図 4.6



フレームワーク別のアプリの割合。破線：全 2,686 件のアプリ。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

なぜ解消されないのか

コンポーネントは他のコンポーネントによって取り込まれます。銀行が自社のコードを毎月更新していても、自社で管理できない SDK の中に何年も前のライブラリが含まれたまま配布されることがあります。

あるべき姿

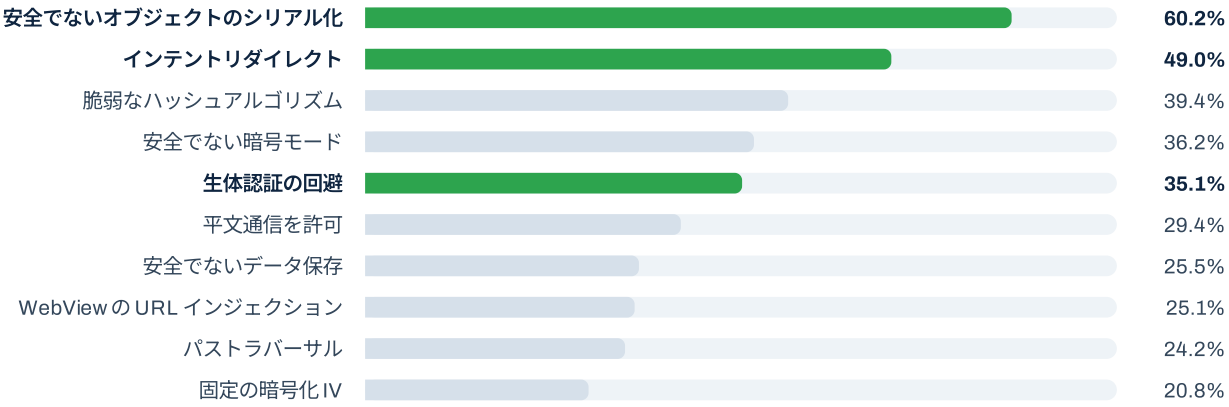
リリースごとにソフトウェア部品表（SBOM）を作成し、それに照らしてアドバイザリを追跡し、重大なコンポーネントの修正期限を設けてください。SDK ベンダーにも同じことを求めてください。

プラットフォームごとに異なる弱点。

スキャンルールの多くは一つのプラットフォームにしか存在しないため、アプリはプラットフォーム内で比較しています。Android ではコードレベルの問題が中心です。iOS では設定の問題が上位を占めます。HarmonyOS では古いコンポーネントと Web コードが上位です。

Android：シリアル化とインテントリダイレクトが上位

図 4.7



Android アプリに占める割合。Android 専用ルール。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

iOS：設定の問題が上位

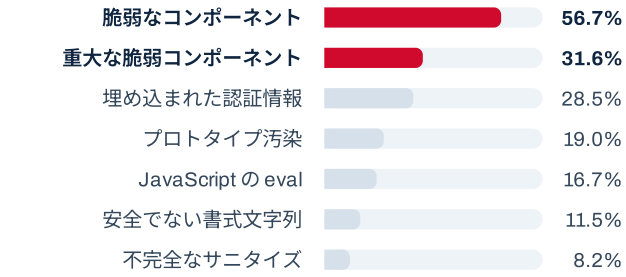
図 4.8



iOS アプリに占める割合。ユニバーサルリンクを使えば、別のアプリがログインのリダイレクトを横取りする OAuth 乗っ取りを防げます。

HarmonyOS：古いコンポーネントと Web コードが上位

図 4.9



HarmonyOS アプリに占める割合。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

第 05 章

05

認証と決済

パスキー、アテステーション、鍵にひも付いた生体認証によって、盗まれたパスワードや改ざんされたアプリの悪用価値は大きく下がります。これらは広がりつつありますが、その歩みはゆっくりです。



画面：パスキーの確認画面のイメージ（実在のアプリではありません）。

4.9%

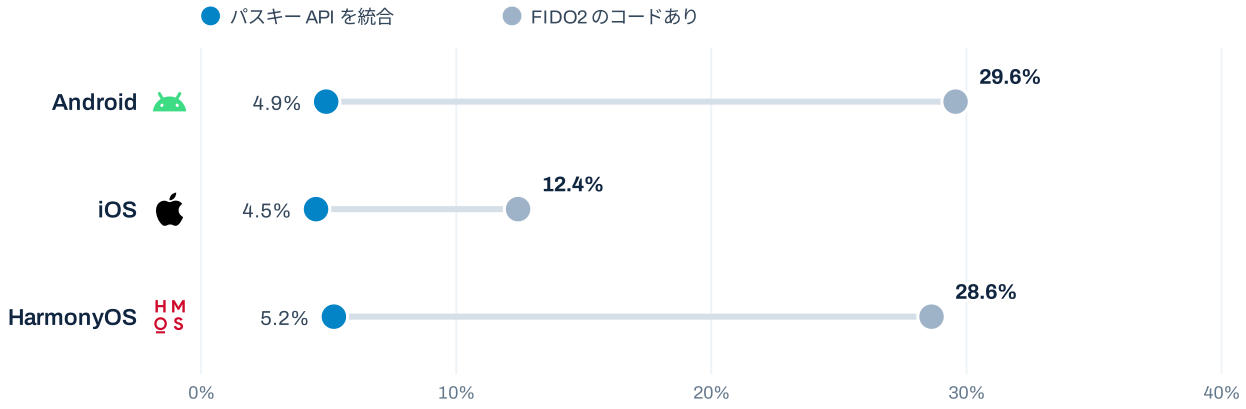
のアプリがパスキー API を統合

パスキーのコードはあっても、パスキーは使えない。

Android アプリの三分の一近くが FIDO2 または WebAuthn のコードを含んでいますが、パスキー API を呼び出しているのは 4.9% にすぎません。iOS では 4.5% です。コードは他のライブラリに含まれて入り込むことがあり、その場合は機能が有効になっていません。

FIDO2 のコードはよく見られるが、パスキー API はまれ

図 5.1



プラットフォーム別のアプリの割合。パスキー API を統合：アプリが Credential Manager、Google FIDO2 API、または Apple のパスキー API を呼び出していること。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

79.8% のアプリがアテステーションを一切使っていない

図 5.2

	強	弱のみ	なし
Android	16.0%	2.8%	81.2%
強：Play Integrity · 弱：SafetyNet のみ（非推奨）			
iOS	3.6%	17.2%	79.2%
強：App Attest · 弱：DeviceCheck のみ（App Attest 未確認）			
HarmonyOS	20.9%	4.5%	74.5%
強：Play Integrity 13.4%、HMS Safety Detect 7.5% · 弱：SafetyNet のみ（非推奨）			

コードを読めたアプリに占める割合（プラットフォーム別）。強：銀行のサーバーがアプリと端末の両方を検証できる。弱のみ：古い方式または端末のみの確認で、強い方式を併用していない。App Attest と DeviceCheck は Apple、Play Integrity と SafetyNet は Google、HMS Safety Detect は Huawei のサービスです。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

アテステーションにより、銀行のサーバーは、リクエストが正規の端末上の正規のアプリから送られたものかを確認できます。Hirudo のようなリパッケージされたアプリに対する主要な防御策ですが、79.8% のアプリは使っていません。サーバーがその結果を実際に適用しているかどうかは、アプリからは確認できません。

銀行のウェブサイトはアプリを指定しているか。

パスキーとアプリリンクは、銀行のウェブサイトがアプリを指定している場合にのみ機能します。各銀行の公開関連付けファイルを読み、アプリが記載されているかを確認しました。

保存済みログイン情報とパスキー用にアプリを指定している銀行サイトは少数

図 5.3



保存済みログイン情報とパスキーの共有を許可するアプリとして、銀行のウェブサイトが指定しているアプリの割合（プラットフォーム別）。銀行ドメインの apple-app-site-association と assetlinks.json から読み取り。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

16%
の iOS アプリは、関連付けファイルにテストビルドのアプリ ID も記載している銀行のもの

92
Apple の関連付けファイルを持つ銀行ドメイン 226 件のうち、本番以外のアプリ ID を記載しているもの

88
Android の assetlinks ファイルを持つ銀行ドメイン 217 件のうち、本番以外のパッケージを記載しているもの



当社のチェックが読み取った、ある銀行のファイル

ある銀行の関連付けファイル

この銀行のファイルは、ユニバーサルリンク用に iOS アプリを指定しているため、銀行サイトへのリンクでアプリが開きます。一方、Web 認証情報用にはアプリを指定していないため、アプリは銀行のパスキーを提供できません。さらに、本番アプリと並んでテストビルドのアプリ ID が 4 件記載されています。

脆弱性ではなく、衛生管理の問題

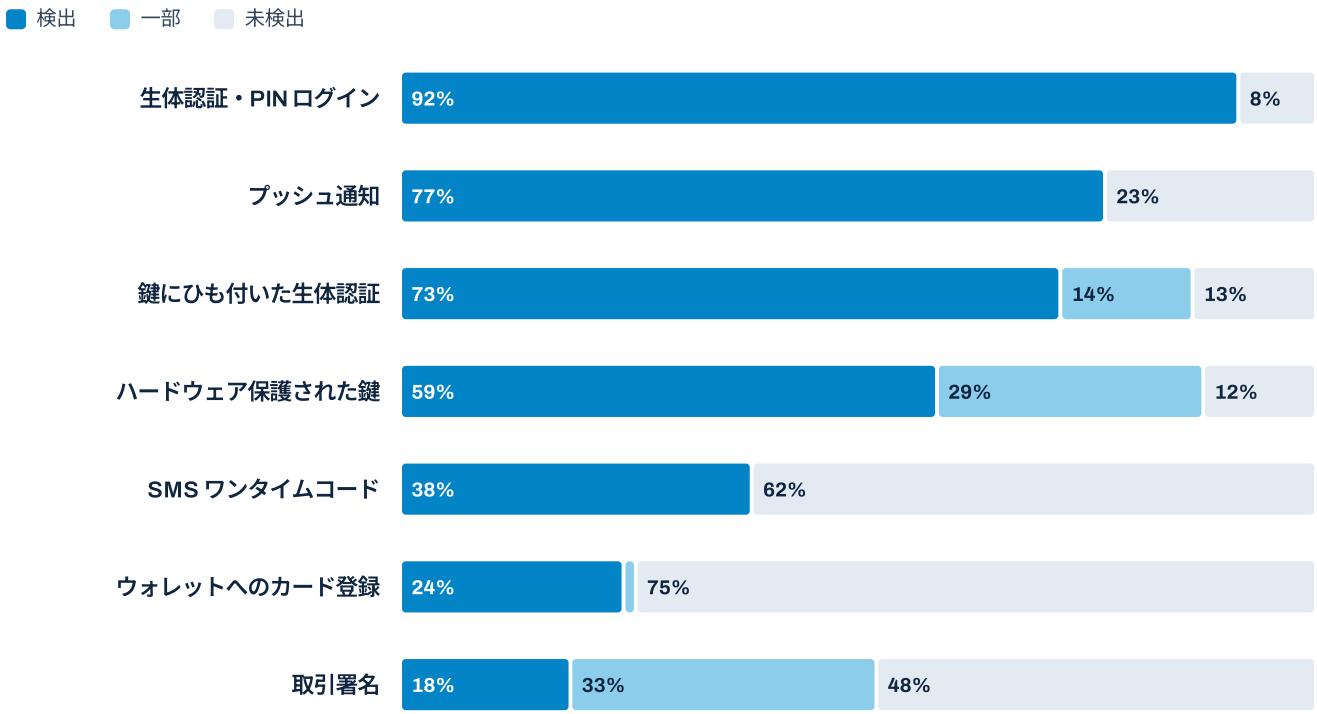
これらのエントリを使えるのは、銀行が署名したアプリだけです。しかし、本番のファイルにテストビルドが記載されていると、銀行の内部ビルド識別子が誰にでも分かり、顧客が決して使うべきでないビルドでもリンクや認証情報が機能し続けます。より大きな問題はエントリの欠落です。それがなければ、アプリはパスキーをまったく提供できません。

生体認証の多くは鍵にひも付くが、三分の一は回避可能。

Android アプリの生体認証の使い方を判別できた範囲では、73.2% が暗号鍵に確認をひも付けており、11.4% はマルウェアが偽装できる「はい／いいえ」の判定として扱っています。また、スキャナーは Android アプリの 35.1% で回避可能な生体認証フローを検出しました。一方、Android アプリの三分の一と iOS アプリの大半が、SIM スワップ攻撃の標的となる SMS ワンタイムコードに対応しています。

アプリのサインインと決済承認の方法

図 5.4



全プラットフォームのアプリ 2,686 件に占める割合。検出：コード上に明確なエビデンスあり。一部：エビデンスの一部のみ。アテステーションと不正対策 SDK は 24 ページと 15 ページで扱っています。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

回避可能な生体認証

回避可能なフローは、別の箇所で鍵にひも付いた生体認証を使っているアプリにも存在しえます。偽装された「はい」で何も解除されないよう、重要な操作はすべて鍵にひも付いた経路を通すべきです。

SMS コードと SIM スワップ

SIM スワップ攻撃では、詐欺師が携帯電話事業者を言いくるめ、被害者の電話番号を自分の管理する SIM に移させます。以後、SMS ワンタイムコードはすべて顧客ではなく攻撃者に届きます。端末と取引にひも付いたコードは SMS を経由しません。

第 06 章

06

シールディング：アプリが備える保護

ランタイムシールディングは、root 化された端末、デバッガー、フッキングツール、改ざんされたアプリのコピーを検知します。三つのプラットフォームすべてで、全アプリのコードからこれらの保護機能を探しました。



画面：root 化された端末上でシールディングされたアプリのイメージ。

26.9%

の Android アプリが商用またはプラットフォームのシールディング製品を組み込んでいる

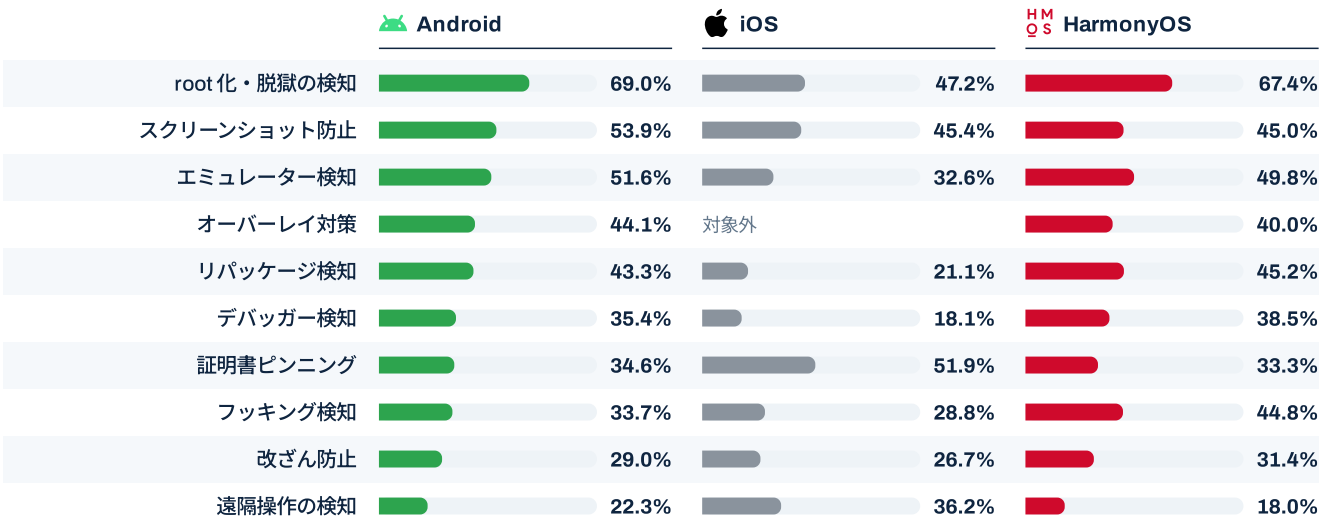
Android アプリ

コードに見つかった保護機能。

どのプラットフォームでも、大半のアプリは少なくとも root 化または脱獄された端末を確認しています。フッキングツール、改ざん、遠隔操作を検知するアプリははるかに少数です。トロイの木馬が被害者自身の端末から不正を行う際に使う画面共有や遠隔操作を検知するコードがあるのは、Android アプリの 22.3%、iOS アプリの 36.2% です。

root 化チェックは一般的、フッキングと遠隔操作のチェックはまれ

図 6.1



銀行自身のコードまたは帰属不明のコードからチェックを呼び出しているアプリの割合（プラットフォーム別）。Android の割合順。対象外：iOS ではアプリが他のアプリの上に描画できないため、オーバーレイ対策は該当しません。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

存在することと有効であることは別

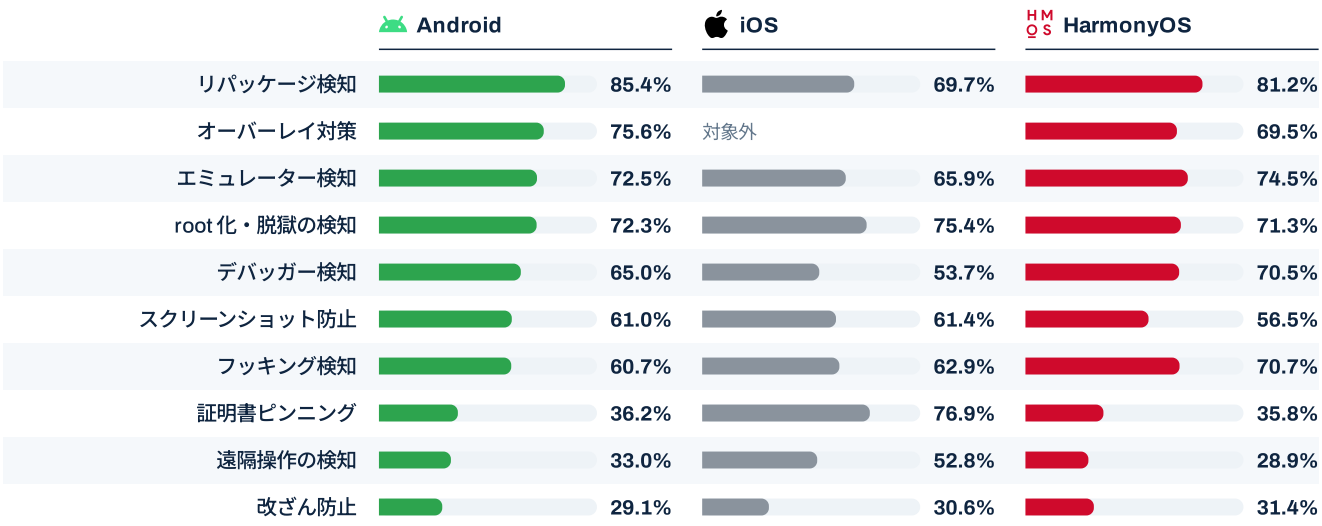
これらの結果は、アプリに保護機能が存在することを示すものです。その存在を知る攻撃者に耐えられるかどうかは示していません。その検証には実機が必要で、今後の版で実施する予定です。これらの数値は保護の上限値として扱ってください。

チェックの多くは SDK が担う。

銀行自身のコードに加え、同梱された SDK 内のチェックも数えると、Android アプリの 85.4% がリパッケージ検知を備えていますが、遠隔操作型トロイの木馬に対して最も重要な遠隔操作の検知を備えているのは 33% にすぎません。

リパッケージ検知は広く普及、改ざん防止はどのプラットフォームでもまれ

図 6.2



プラットフォーム別のアプリの割合。検出：銀行自身のコードまたは同梱された SDK 内にチェックがある。対象外：iOS にはオーバーレイ攻撃が該当しません。SDK 内のチェックは、銀行が有効にしない限りアプリを保護しません。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

防御を多層化しているアプリは少ない。

シールディングは、一つのチェックを回避されても他が無効にならないよう、多層化して初めて効果を発揮します。Android アプリの中央値では、調査対象の 10 種類の保護機能のうち 4 種類に明確なエビデンスがあり、8 種類以上を備えるアプリは 10.7% です。

調査した 10 種類の保護機能

01 **root 化の検知**
アプリのデータがさらされる root 化端末を検知します。

02 **エミュレーター検知**
アプリが実機ではなくエミュレーター上で動いていることを検知します。

03 **デバッガー検知**
実行中のアプリにデバッガーが接続されたことを検知します。

04 **フッキング検知**
Frida など、実行中のアプリを改変するツールを検知します。

05 **リパッケージ検知**
他者が署名した、改変されたアプリのコピーを検知します。

06 **改ざん防止**
アプリ自身のコードが変更されていないかを確認します。

07 **証明書ピンニング**
銀行自身のサーバー証明書のみを受け入れます。

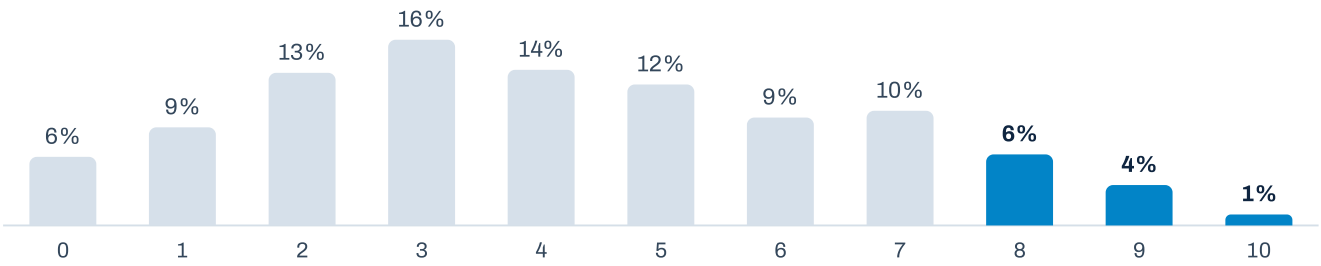
08 **オーバーレイ対策**
他のアプリが銀行アプリの上に偽の画面を描画するのを防ぎます。

09 **スクリーンショット防止**
重要な画面のスクリーンショットと画面録画を防ぎます。

10 **遠隔操作の検知**
画面共有やリモートアクセスツールを検知します。

Android アプリの中央値は 10 種類中 4 種類の保護機能

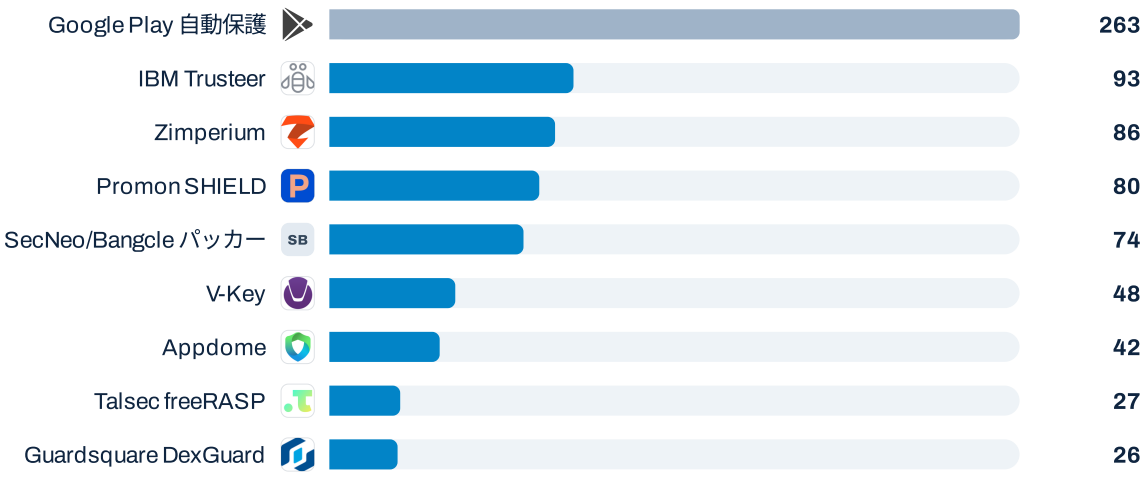
図 6.3



明確なエビデンスのある保護機能の数（10 種類中）別に見た Android アプリの割合。強調表示：8 種類以上。

最も多いシールドは Google の Play 自動保護

図 6.4



各製品を使用しているアプリ数（全プラットフォーム）。Google の Play 自動保護（pairip）は、コードで選択するものではなく、ストアが適用します。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

第 07 章

07

アプリの外側

アプリの信頼性は、その背後にあるドメイン、サーバー、組織の信頼性を超えません。銀行の Web ドメインとメールドメイン、アプリの通信先サーバー、プライバシーラベル、公開された侵害記録、各銀行が従う規制を確認しました。



画面：典型的なラベルと、スキャンで最も多く見つかった不一致。

67%

の Android アプリで、Google Play のプライバシーラベルが自身の権限や SDK と矛盾している

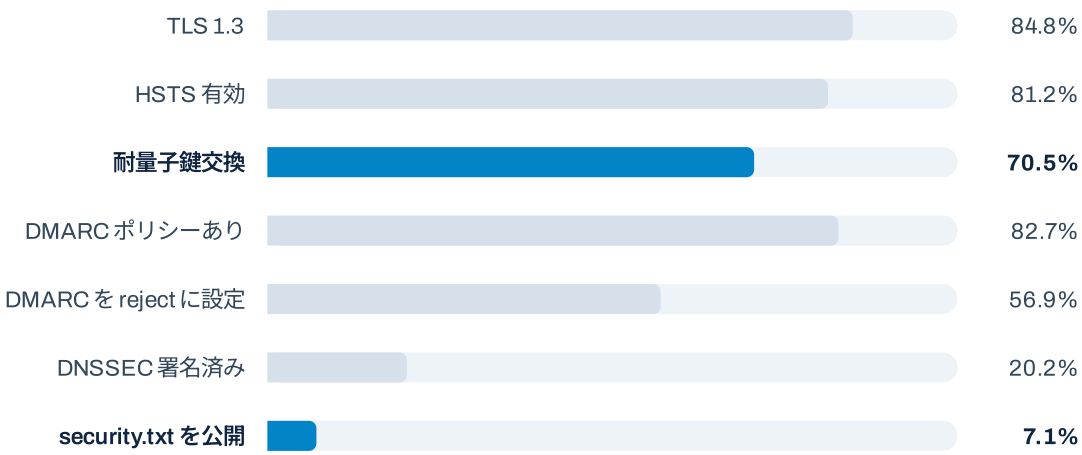
Google Play のプライバシーラベルがある Android アプリ

銀行ドメイン：耐量子化は進むが、脆弱性の報告先は乏しい。

到達できた銀行の Web ホストの 70.5% が、すでに耐量子鍵交換をネゴシエートしています。一方、基本的な衛生管理は遅れています。研究者に欠陥の報告先を伝える security.txt ファイルを公開しているドメインは 7.1% にすぎません。

耐量子 TLS は security.txt より普及

図 7.1

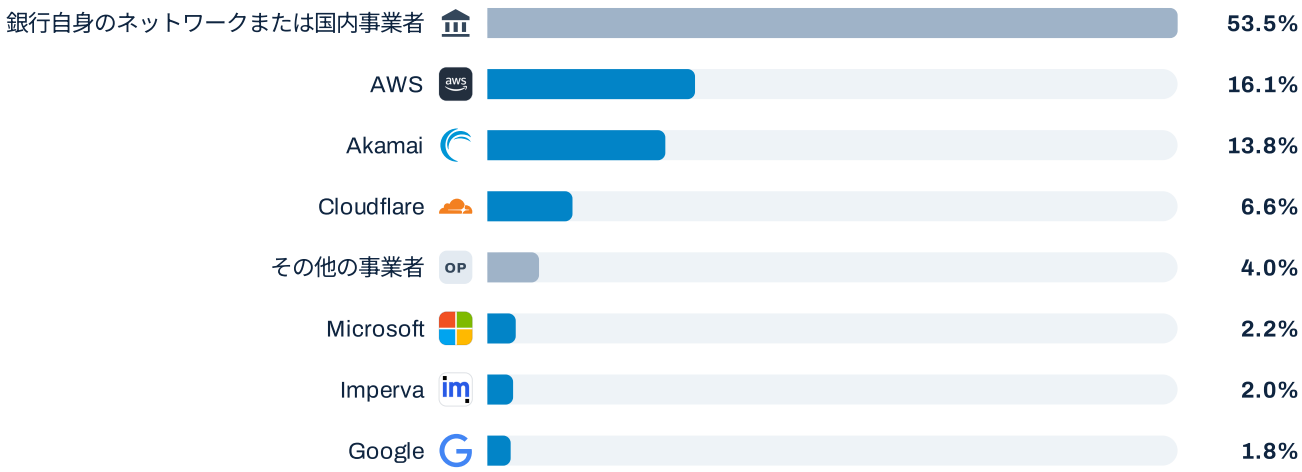


TLS と HSTS：到達可能な Web ホスト 1,140 件に占める割合。耐量子：完了したハンドシェイク 1,038 件。DNS のチェック：1,252 ドメイン。

出典 銀行ドメインに対する Ostorlab の TLS ハンドシェイクと公開 DNS レコード。

バックエンドの大半は銀行自身のネットワーク上、クラウドでは AWS が首位

図 7.2



全三プラットフォームのアプリが参照する、銀行所有のバックエンド IP アドレス 5,101 件に占める割合（公開 DNS で名前解決）。

出典 アプリが参照するホストを公開 DNS で名前解決。IP 所有者のレジストリ。

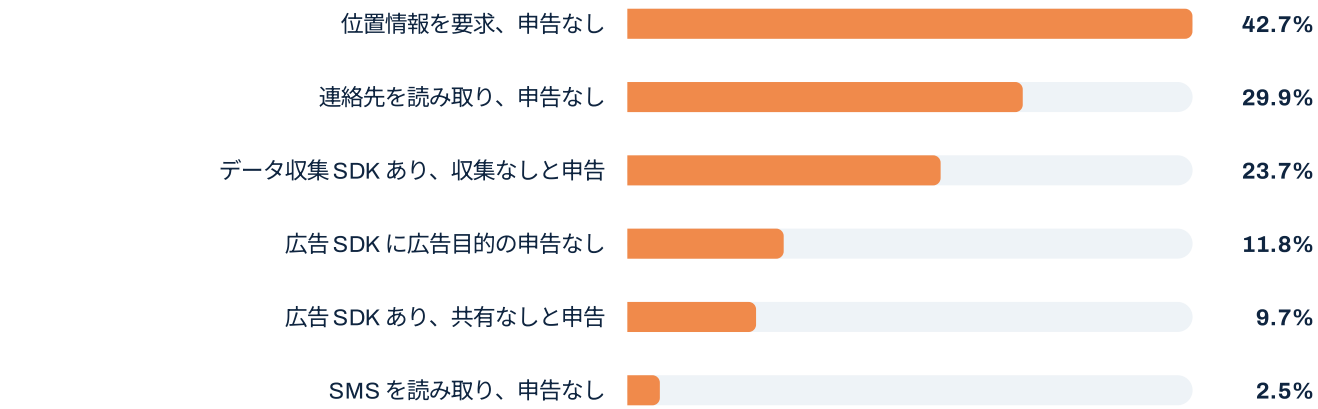
AWS、Akamai、Cloudflare、Microsoft がバックエンドアドレスの 38.7% を占めます。このいずれかで障害や侵害が起きれば、多数の銀行に同時に影響が及びます。EU の DORA は、まさにこの点を契約前に検討するよう銀行に求めており、その中には「容易に代替できない ICT 第三者サービスプロバイダーとの契約締結」（非公式訳）に当たるかどうかも含まれます（規則（EU）2022/2554 第 29 条第 1 項）。

アプリの実態と合わないプライバシーラベル。

アプリストアは、アプリが収集するデータを申告するよう開発者に求めています。Android のバンキングアプリの 67% で、その申告がアプリ自身の権限や SDK と矛盾しています。

最も多いラベルの不一致は未申告の位置情報

図 7.3



Google Play のデータ セーフティ ラベルがある Android アプリに占める割合。一つのアプリに複数の不一致がある場合があります。

出典 Google Play のデータ セーフティ ラベルを、アプリの権限および SDK と比較。

なぜ重要か

マニフェストに権限があっても、アプリが実際に使っているとは限らないため、不一致の一部は過剰に慎重なマニフェストによるものです。しかし、規制当局はラベルを約束として読みます。収集を過少に申告するラベルはコンプライアンス上のリスクであり、アプリを比較する顧客を誤解させます。

iOS のラベル

プライバシーラベルのある iOS バンキングアプリのうち 19% が、他社のアプリをまたいでユーザーを追跡するためにデータを使用すると申告しています。最も多いのは識別子と使用状況データです。

Web 以外でも応答する銀行サーバー。

アプリが参照する銀行所有のサーバーアドレス 5,101 件のうち、4,113 件がインターネット全体の公開観測データに含まれています。そのうち 251 件（113 行）が Web と CDN 以外のポートで応答し、79 件では既知の脆弱性に該当するバージョンのソフトウェアが稼働しています。

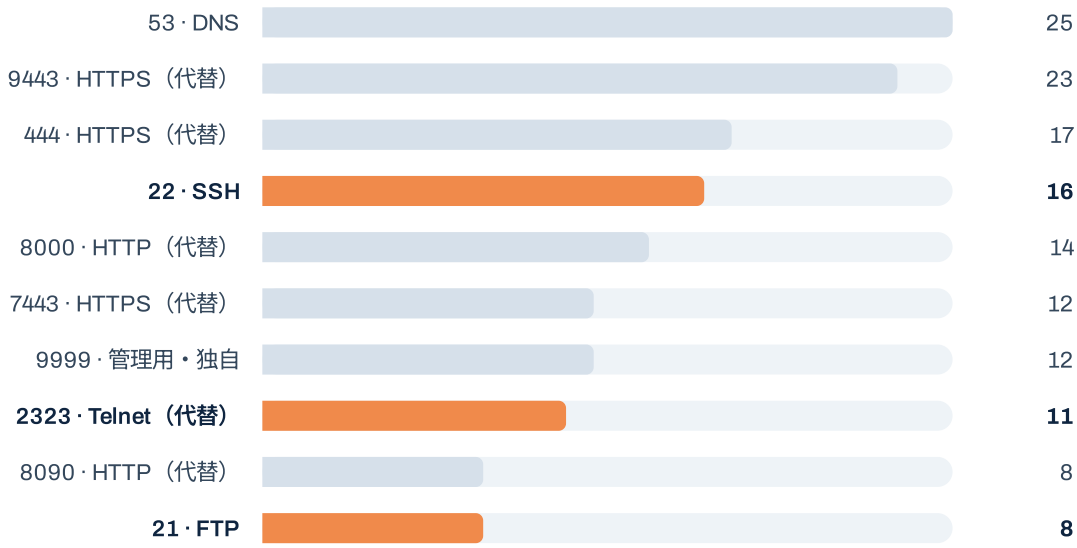
251
件の銀行 IP で Web・CDN 以外のポートが開放（113 行）

79
件の銀行 IP でソフトウェアのバージョンから CVE を推定（74 行）

25
件の銀行 IP でサポート終了製品が稼働

追加の開放ポートで多いのは DNS と HTTPS の代替ポート

図 7.4



各ポートで応答する銀行所有 IP の数（Shodan InternetDB に収録された 4,113 件中）。ポート 80 と 443、および CDN のプロキシポートは除外しています。40 を超えるポートで応答する IP 151 件は、ファイアウォールやターピットに典型的なため数えていません。

出典 Shodan InternetDB（パッシブなインデックス）。銀行のサーバーには一切リクエストを送信していません。

銀行のサーバーはスキャンしていない

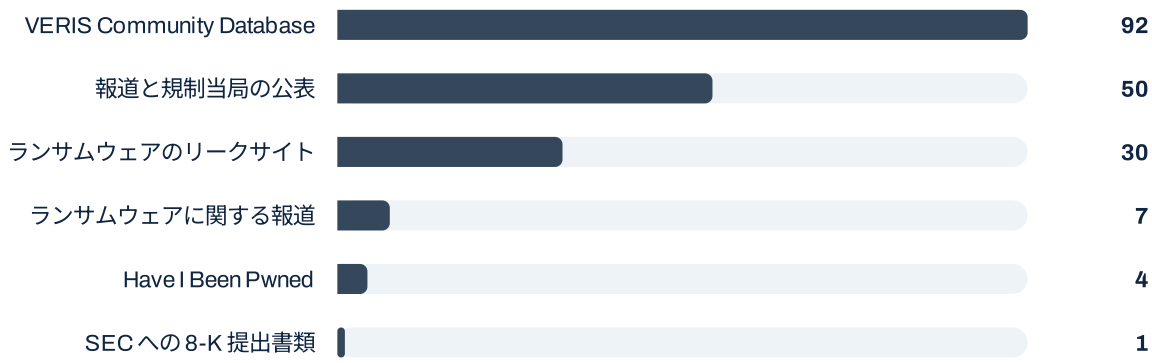
開放ポートとソフトウェアのバージョンは、インターネット全体の公開観測データ（Shodan InternetDB）から得たもので、銀行のシステムには一切触れていません。残る 988 件のアドレスはこのデータに含まれていません。閉じているのではなく、不明です。CVE は観測されたソフトウェアのバージョンから照合したもので、いずれも銀行が確認すべき手がかりです。

六行に一行に公開された侵害記録。

侵害データベース、ランサムウェアのリークサイト、規制当局の公表、SEC への提出書類を調べたところ、上位 500 行のうち 83 行（16.6%）に、公開された侵害記録が一件以上ありました。そのうち 55 行には 2020 年以降の記録があります。

侵害記録の大半は VERIS のデータベースから

図 7.5



上位 500 行の記録数。一つの銀行に複数の記録がある場合があります。照合はすべて人の目で確認しました。報道と規制当局の確認は 29 行の G-SIB のみを対象としています。

出典 VCDB、Have I Been Pwned、ransomware.live、SEC への 8-K 提出書類、報道および規制当局の公表。

記録とは何か

記録とは、公に報告されたインシデントを指します。攻撃、内部者によるアクセスの悪用、データ漏えいにつながったミス、ランサムウェアグループによる犯行声明などです。銀行のアプリに関する検出事項ではなく、多くは古い記録です。VERIS のデータベースは十年以上前までさかのぼります。

銀行名を含む CVE

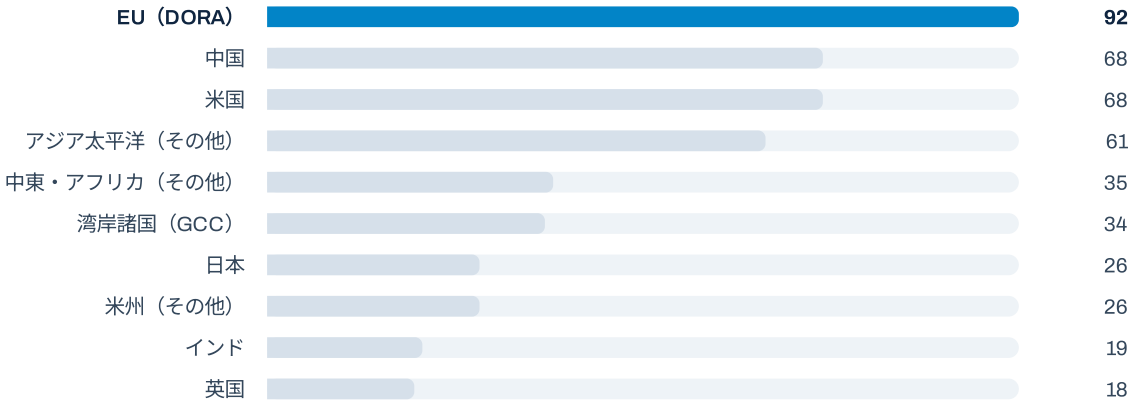
公開されている CVE レコードのうち 51 件が 37 行のブランド名と一致し、そのうち 14 件は 2025 年以降のものです。大半は古いモバイルアプリのバージョンに関するもので、ブランド名の照合には誤検知も含まれるため、検出事項ではなく手がかりとして扱っています。

銀行が従う規制と、銀行自身の表明。

サンプルのすべての銀行は、ICT リスクに関する国または地域の制度の下にあります。上位 500 行のうち 95 行は EU のデジタル・オペレーショナル・レジリエンス法（DORA）の対象です。同法は 2025 年1月から適用されており、32 ページで示したホスティング事業者などへの依存を経営の責務としています。

対象となる銀行が最も多いのは EU の DORA

図 7.6



上位 500 行の数（本拠国の制度別）。上位十グループを表示しており、ほかに 40 行が小さなグループに属しています。

出典 規制当局の登録簿と各銀行の本拠地市場。

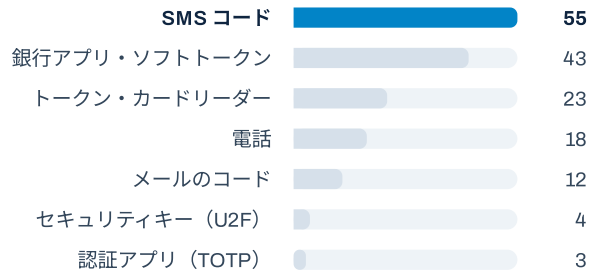
332
の上位 500 行が Apple Pay 対応カードの発行体

44
行がウェブサイトで認証の取得を表明（最も多いのは ISO 27001）

19
行が公開の脆弱性開示プログラムを運営（うち 5 行はバグバウンティあり）

最も多く案内されている二要素目は SMS

図 7.7



ウェブサイトでサインイン方法を説明している 73 行の数。一つの銀行が複数を挙げている場合があります。パスキーを案内しているのは 8 行です。

出典 銀行のウェブサイトと 2fa.directory のリスト。

表明であって、証明書ではない

認証は銀行のウェブサイト上の記載であり、証明書を検証したものではありません。少なくとも一つのドメインで security.txt ファイルを公開している銀行は 62 行、開示プログラムを明示している銀行は 19 行です。UAE 中央銀行などの規制当局が SMS ワンタイムコードの段階的廃止を進めるなかでも、最も多く案内されている二要素目は依然として SMS です。

08

脅威の動向

バンキング型トロイの木馬は攻撃対象のアプリのリストを保持しています。フィッシングキットは銀行のログインページを模倣します。この一年では、攻撃者が正規のバンキングアプリをパッチを当てたコピーに置き換える手口も現れました。



画面：公開された標的リストの形式（アプリ名はマスク済み）。

15%

の分析対象 Android アプリが、公開されているバンキング型トロイの木馬の標的リストに一つ以上載っている

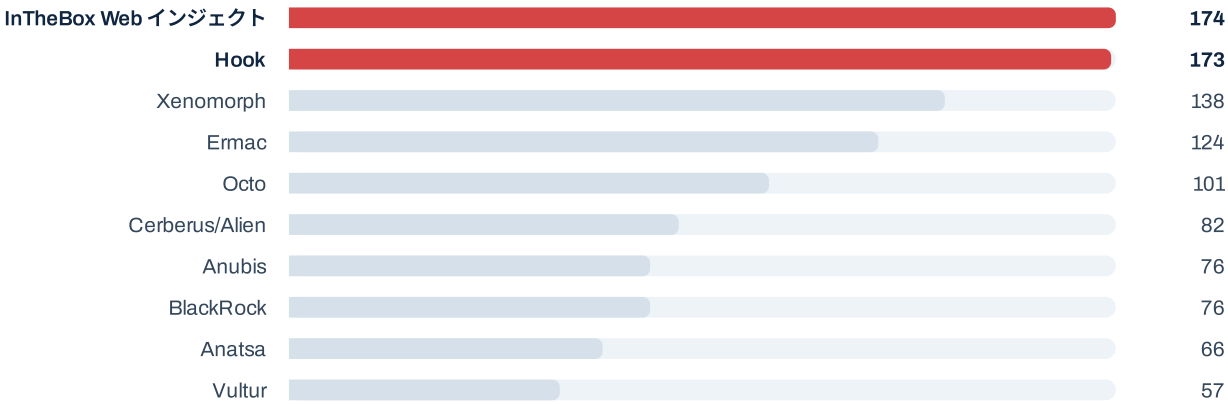
Android アプリ

十行に四行がトロイの木馬の標的リストに。

研究者は、バンキング型トロイの木馬の内部で見つかった標的リストを公開しています。これをサンプルの Android アプリと照合すると、192 行（38.4%）のアプリ 280 件が、29 ファミリーのうち少なくとも一つの標的になっています。

サンプル中で最も多くのアプリを標的にしているのは Hook と InTheBox

図 8.1



各ファミリーの公開標的リストに載っているサンプル内のアプリ数。リストは 47 件で、大半は 2021〜2023 年に ThreatFabric、Cleafy、Zimperium などが公開したものです。リストには Android のパッケージ名が記載されているため、Android のみが対象です。

出典 公開されたバンキング型トロイの木馬の標的リスト（ThreatFabric、Cleafy、Zimperium ほか）、2021〜2023 年。

フィッシングホストの 93% と、最も狙われている九行のすべてが欧州と米州に集中

図 8.2

54%
欧州
最も狙われている 9 行のうち 5 行

39%
米州
最も狙われている 9 行のうち 4 行

5%
アジア太平洋
最も狙われている 9 行には該当なし

1%
中東・アフリカ
最も狙われている 9 行には該当なし



色：銀行名を含む稼働中のフィッシングホストのうち、各地域が占める割合。ピン：その国に本拠を置く、最も狙われている九行の数。この九行で全ホストの 57% を占めます。グレー：サンプル外。銀行名は伏せています。

出典 PhishTank、OpenPhish、Phishing.Database、URLhaus。

2026 年：攻撃者は銀行自身のアプリを悪用する。

この十年、バンキング型トロイの木馬は本物のアプリの上に偽の画面を描画してきました。この一年のキャンペーンはさらに踏み込み、正規のアプリにパッチを当てる、複製する、あるいは置き換えることで、銀行自身のコードを攻撃者のために働かせています。

2016 年以降
オーバーレイ
上に重ねて描画

トロイの木馬が本物のアプリの上に偽のログイン画面や決済画面を描画し、顧客の入力内容を読み取ります。

成立する理由
正規のアプリには手が加えられず、トロイの木馬に必要なのはユーザー補助の権限だけです。

防ぐ手段
オーバーレイ対策、ユーザー補助サービスのチェック

GOLDFACTORY、2025 年
パッチ
アプリを改変

攻撃者が正規のアプリを入手し、フッキングコードを注入して再署名します。その結果、銀行自身の画面で攻撃者のコードが動きます。

成立する理由
コピーは見た目も動作も本物のアプリと同じで、整合性チェックも含めてそのまま動きますが、そのチェックはフックによって無効化されています。

防ぐ手段
銀行の鍵による署名チェック、サーバー側アテステーション

GIGABUD、2026 年
クローン
二つ目のコピーを実行

攻撃者が、自らが制御する隠れた仕事用プロファイルや仮想空間の中で正規のアプリを実行します。

成立する理由
不正検知ツールからは既知の端末上の本物のアプリに見えるため、セッションは正常に見えます。

防ぐ手段
仕事用プロファイル・仮想空間の検知、端末バインディング

HIRUDO、2026 年
すり替え
アプリを置き換え

ドロッパーが正規のアプリをアンインストールし、同じ名前、アイコン、バージョン番号を持つパッチ済みのコピーをインストールします。

成立する理由
顧客には何の変化も見えません。異なるのは署名鍵だけで、それを確認できるのは銀行のサーバーだけです。

防ぐ手段
署名鍵を確認するサーバー側アテステーション

アプリのすり替えの手順

1. 偽のアップデート
被害者がリンクや偽のストアページからドロッパーをインストールします。

2. 正規アプリの削除
ドロッパーが正規のバンキングアプリをアンインストールします。

3. コピーの再インストール
パッチ済みのコピーをインストールします。名前、アイコン、バージョンは同じで、署名鍵だけが異なります。

4. 認証情報の漏えい
コピーは正常に見えるまま、パスワードとワンタイムコードを盗み取ります。

5. 判断するのはサーバー
コピーと本物のアプリを見分けられるのは、銀行のサーバーでのアテステーションだけです。

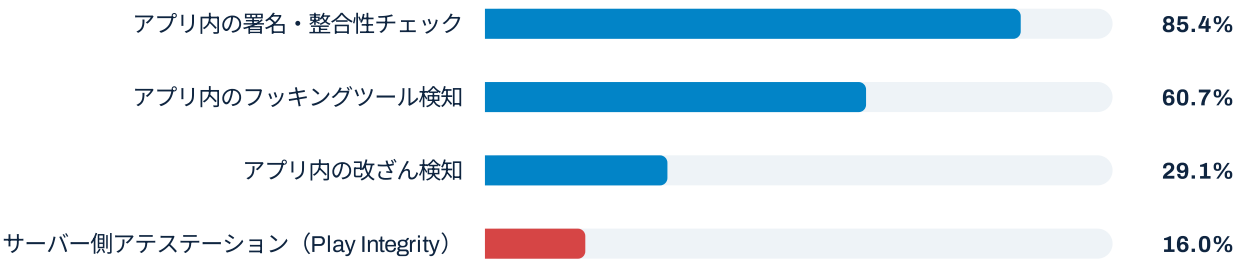
出典 Group-IB（GoldFactory、Gigabud）、ThreatFabric（Hirudo）、Ostorlab による分析。

アプリのすり替えに銀行は気づけるか。

パッチを当てたコピーは、端末上で動くどのチェックでも無効化できます。サーバーならより確実です。アプリが銀行の正規ビルドであることを示す、Google または Apple が署名した新しい証明を伴わないリクエストを拒否できるからです。その証明を要求するコードを含む Android アプリは 16% にすぎず、サーバーがそれを実際に適用しているかどうかは確認できません。

アプリ内のチェックは一般的、サーバー側のチェックはまれ

図 8.3



Android アプリに占める割合。アプリ内：銀行自身のコードまたは同梱された SDK 内で検出。サーバー側アテステーション：アプリが証明を要求するコードを含むもの。サーバーがそれを適用しているかはアプリからは確認できず、また正規でも侵害された端末であれば検証を通過しえます。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

2026 年のキャンペーン

時期	キャンペーン	種類	概要	報告元
2025 年 12月	**GoldFactory**	パッチ	タイ、ベトナム、インドネシアの正規のバンキングアプリに、整合性チェックを回避するフッキングコードが注入されました。改変されたアプリは 27 件、報告された感染は 11,000 件超です。	Group-IB
2026 年 2月〜七月	**Gigabud**	クローン	不正検知を回避するため、バンキングアプリを Android の仕事用プロファイル内で実行。侵害された端末は約 1,469 台と報告されています。	Group-IB
2026 年 5月	**ラボテスト**	パッチ	八つの市場でテストしたバンキングアプリの 58% がリパッケージ可能でした。	Promon
2026	**オーバーレイ型ファミリー**	オーバーレイ	活動中のバンキングマルウェア 34 ファミリーが、90 か国の金融ブランド 1,243 件を標的にしています。	Zimperium
2026 年 8月〜十月	**Hirudo**	すり替え	ドロッパーが、インドネシアの本物のバンキングアプリを、公開テスト鍵で署名されたパッチ済みのコピーとすり替えます。七行の八つのアプリについて、すぐに使える置き換え用のコピーが用意されていました。ケーススタディは 49 ページ。	ThreatFabric

取るべき対策

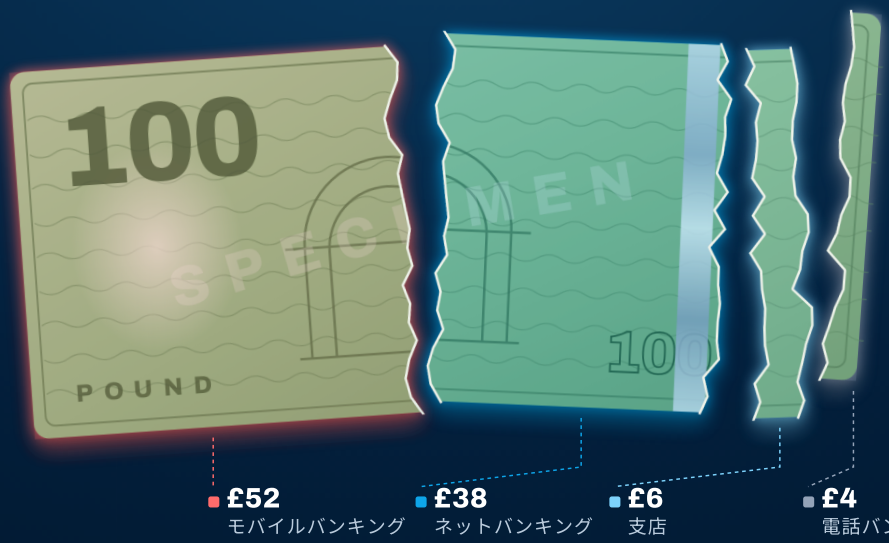
端末上で動くチェックは、時間稼ぎにすぎないものとして扱ってください。判断はサーバーで行います。ログインと決済にアテステーションを必須とし、銀行自身の鍵以外で署名されたアプリからのリクエストを拒否し、顧客のセッションを開始時の端末にひも付けてください。

被害額はどこに流れるか。

公表されている不正データには空白が多く、調査した 101 市場のうち比較可能な数値を公表しているのは 83 市場だけです。データがある市場では、同じ傾向が見られます。不正の中心は、顧客がだまされて自ら行う支払いと、スマートフォンに移っています。

図 8.4

英国の詐欺被害 100 ポンドあたり 52 ポンドがモバイルバンキングアプリから流出



576.4百万ポンド
英国における 2025 年の承認済みプッシュ型決済詐欺の被害額

79%
件数ベースで、詐欺による支払いのうちモバイルバンキングで行われた割合

88%
報告された詐欺被害のうち、英国の返金ルールに基づき返金された割合

詐欺の支払いが行われたチャネル別に引き裂いた 100 ポンド紙幣。各片の幅は、被害額に占めるそのチャネルの割合を表します。承認済みプッシュ型決済（APP）詐欺では、顧客がだまされて自ら送金します。承認済みの被害額は一年で 19% 増加し、未承認の被害額は 5% 減少しました。

出典：UK Finance『Annual Fraud Report 2026』、英国決済システム規制機関（PSR）

欧州

2024 年、EU における不正な口座振替の金額の 74% は、支払人を操って支払いを承認させたものでした。金額ベースで、カード不正はカード非対面の取引で 13 倍多く発生しています。出典：ECB と EBA の決済不正に関する報告書、2024 年データ。

返金制度は機能している

英国で 2024 年10月に返金が義務化されて以降の 18 か月間で、銀行は報告された APP 詐欺被害額の 88% を返金しました。責任は銀行側に移りつつあり、アプリ内で詐欺を止める対策の価値が高まっています。出典：英国決済システム規制機関（PSR）。

背景であって、原因ではない

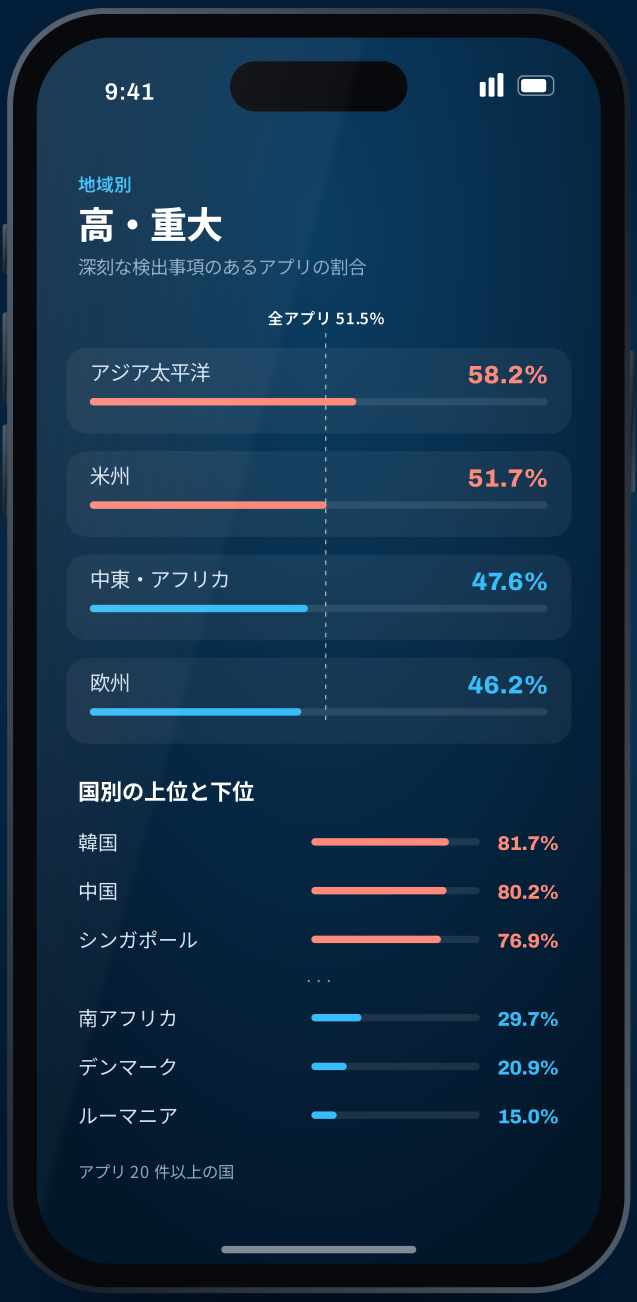
これらの統計は各市場の不正の状況を示すものです。本レポートで示したアプリの弱点が被害を引き起こしたことを示すものではありません。

第 09 章

09

地域・銀行タイプ・国別の結果

結果はプラットフォームよりも国によって大きく異なります。シールディングで先行する市場もあれば、アテステーションで先行する市場もあり、すべてで先行する市場はありません。



画面：高または重大の検出事項があるアプリ（地域別・国別）。

64

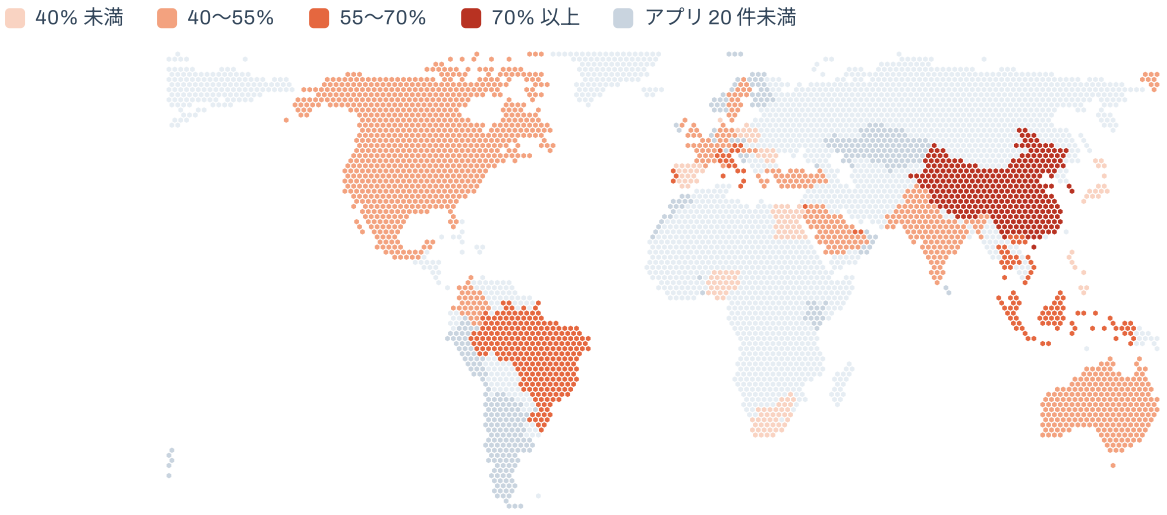
か国がサンプルに含まれる（米国や中国からトーゴ、リヒテンシュタインまで）

すべてに優れた地域はない。

アジア太平洋のアプリは、深刻な検出事項もシールディングも最も多くなっています。高または重大の検出事項が最も少ないのは欧州のアプリです。パスキーでは米州のアプリが 9.9% で先行しています。

深刻な検出事項の割合は国によって大きく異なる

図 9.1



各国のアプリに占める割合。アプリが 20 件以上ある 40 か国が対象です。グレー：サンプルに含まれるがアプリが 20 件未満の国。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

すべての指標で先行する地域・銀行タイプはない

図 9.2

グループ	アプリ数	高・重大	脆弱なコンポーネント	埋め込まれた認証情報	シールディング製品	アテステーション	パスキー API
アジア太平洋	942	58.2%	46.3%	24.5%	33.7%	20.0%	2.8%
欧州	822	46.2%	40.0%	15.7%	21.3%	16.9%	4.7%
中東・アフリカ	508	47.6%	39.0%	23.0%	19.9%	19.9%	4.3%
米州	414	51.7%	33.8%	16.2%	29.5%	23.4%	9.9%
銀行タイプ別							
従来型銀行	2,596	51.2%	40.9%	19.8%	26.4%	19.3%	4.4%
銀行系ネオバンク	61	52.5%	47.5%	24.6%	37.7%	16.4%	4.9%
独立系ネオバンク	29	**79.3%**	44.8%	**48.3%**	24.1%	**48.3%**	**37.9%**
全アプリ	*2,686*	*51.5%*	*41.1%*	*20.2%*	*26.6%*	*19.6%*	*4.8%*

各グループのアプリに占める割合。独立系ネオバンクは、他のアプリと比べて高または重大の検出事項を持つ割合がはるかに高い一方（79.3% 対 51.2%、フィッシャーの正確確率検定、p = 0.002）、銀行系ネオバンクは他と同程度です。独立系ネオバンクは、アテステーションとパスキー API でも先行しています。ただし対象は 29 件のみで、その三分の一は一つの銀行のアプリであるため、差の大きさは目安です。セルの色分けは次ページと同じです。埋め込まれた認証情報は Google API キーを除きます。地域によってプラットフォームの構成が異なるため、プラットフォーム共通のルールのみを比較しています。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

国別の結果。

サンプル中のアプリ数が多い上位 18 か国。各セルは全アプリの割合をどれだけ上回るかで色分けしています。赤はリスク、青は防御です。色のないセルは全アプリの割合以下です。

国ごとに異なるリスクと防御のパターン

図 9.3

全アプリの割合からの上振れ： リスク +5 ポイント +12 +20 防御 +5 ポイント +12 +20

国	アプリ数	高・重大	脆弱なコンポーネント	埋め込まれた認証情報	シールディング製品	アテステーション	パスキー API
米国	224	52.2%	35.3%	12.9%	33.9%	28.1%	12.9%
インド	200	50.0%	30.5%	21.0%	**43.0%**	**32.5%**	0.5%
中国	162	**80.2%**	**77.8%**	**43.8%**	**51.9%**	15.4%	5.6%
英国	157	47.1%	**57.3%**	31.2%	**43.9%**	18.5%	14.0%
日本	116	38.8%	33.6%	13.8%	6.9%	4.3%	3.4%
サウジアラビア	95	47.4%	32.6%	31.6%	17.9%	13.7%	6.3%
アラブ首長国連邦	84	**64.3%**	**59.5%**	25.0%	23.8%	28.6%	0.0%
フランス	76	43.4%	35.5%	3.9%	21.1%	9.2%	0.0%
イタリア	74	58.1%	**58.1%**	21.6%	5.4%	29.7%	2.7%
南アフリカ	74	29.7%	17.6%	**37.8%**	20.3%	**54.1%**	9.5%
マレーシア	71	57.7%	42.3%	25.4%	31.0%	25.4%	1.4%
スペイン	69	37.7%	24.6%	8.7%	**42.0%**	27.5%	7.2%
ブラジル	66	60.6%	31.8%	22.7%	27.3%	21.2%	10.6%
オーストラリア	63	54.0%	33.3%	19.0%	4.8%	23.8%	3.2%
韓国	60	**81.7%**	**71.7%**	21.7%	3.3%	3.3%	0.0%
ベトナム	56	**64.3%**	51.8%	**33.9%**	**41.1%**	25.0%	3.6%
カタール	55	41.8%	40.0%	21.8%	10.9%	25.5%	0.0%
カナダ	50	48.0%	26.0%	14.0%	12.0%	14.0%	4.0%
全アプリ	*2,686*	*51.5%*	*41.1%*	*20.2%*	*26.6%*	*19.6%*	*4.8%*

各国のアプリに占める割合。色分け：全アプリの割合を 5、12、20 ポイント以上上回るもの。中国のアプリには HarmonyOS アプリが多く含まれ、コンポーネントと重大の数値を押し上げています。

出典 Ostorlab によるバンキングアプリ 2,686 件の自動セキュリティ分析。

地域別に見た最も安全な銀行アプリ。

各地域で、アプリの弱点が同業他行より少なく深刻度も低い三行を、アルファベット順に掲載しています。スコアは表示していません。

北米

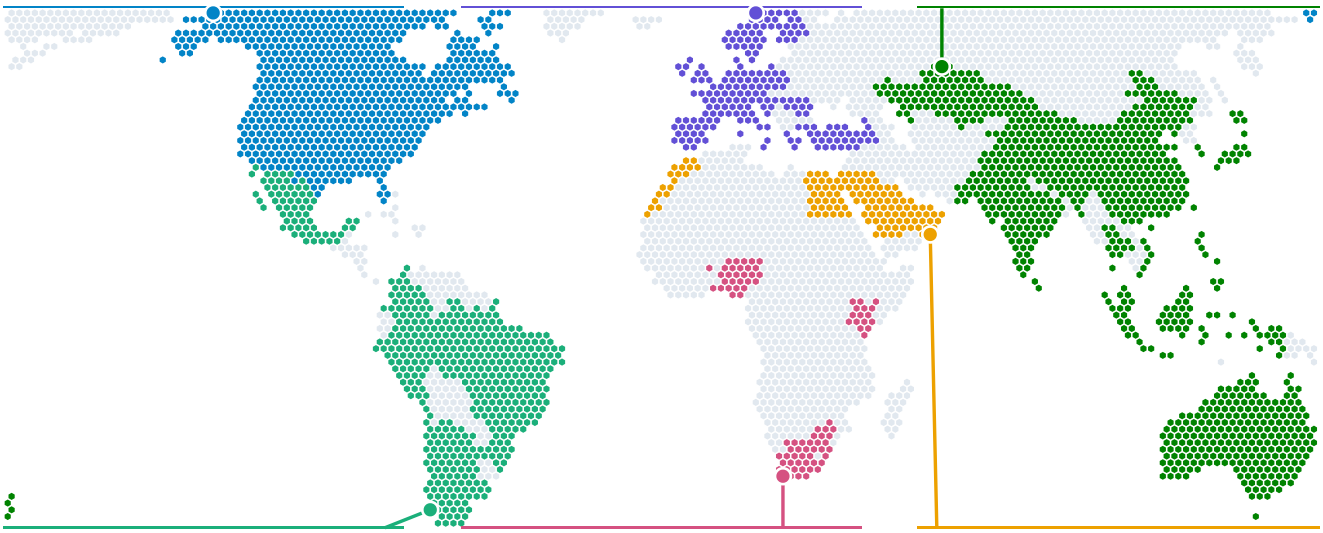
- Scotiabank — カナダ
- WaFD Bank — 米国
- Zions Bancorporation — 米国

欧州

- Ibercaja — スペイン
- Komerční banka — チェコ
- TSB — 英国

アジア太平洋

- Bandhan Bank — インド
- HBL — パキスタン
- RCBC — フィリピン



中南米

- Banorte — メキシコ
- BCP — ペルー
- Itaú — ブラジル

サブサハラ・アフリカ

- Absa — 南アフリカ
- Co-Operative Bank of Kenya — ケニア
- Rand Merchant Bank — 南アフリカ

中東・北アフリカ

- Gulf Bank — クウェート
- Qatar Islamic Bank — カタール
- Saudi Investment Bank — サウジアラビア

色：銀行を比較した国（地域ごとに一色）　グレー：比較対象外

銀行の比較方法

比較の単位は個々のアプリではなく銀行です。スキャンした各アプリには、スキャン評価（70%）と、コードに見つかった防御と弱点（30%）から値を与え、同じストアのアプリの中で順位付けします。銀行のアプリスコアは、スキャンしたすべてのアプリの平均で、アプリ数が少ない場合は中央寄りに補正します。

セキュリティの履歴も考慮

次に、過去三年間に公に報告されたその銀行のセキュリティインシデントごとに、アプリスコアを引き下げます。深刻なインシデントほど大きく、軽微なものほど小さく引き下げます。顧客を狙った詐欺は数えません。履歴が空であることは、何も見つからなかったことを意味し、何も起きなかったことを意味するものではありません。

選出の意味

スキャン済みアプリが二件以上ある銀行のうち、各地域で上位三行。選出は、検出事項が同業他行より少なく深刻度も低いことを意味します。アプリに検出事項がないことを意味するものではありません。

出典 上位 500 行のアプリに対する Ostorlab のスキャン評価とセキュリティコントロール、公に報告されたインシデント。ロゴは各銀行のウェブサイトのアイコンであり、各所有者の商標です。識別のためにのみ表示しています。

第 10 章

10

ケーススタディ

2026 年に公表された四つの攻撃を、それぞれが標的とするアプリに対する当社のスキャン結果と照らし合わせました。電話の最中にインストールさせる偽アプリから、正規アプリのすり替え、さらにはアプリの配布後に新たな権限を得るクラウドのキーまでを取り上げます。



画面：四つの事例と、それぞれの開始ページ。

4

件の 2026 年に公表された攻撃を、標的となったアプリに対する当社のスキャン結果と照合

ケーススタディ 1/4 · 偽アプリ

CyberDakait：七つのトロイの木馬と一本の電話。

インドの銀行の顧客を狙った七つの Android トロイの木馬ファミリーです。マルウェア自体はありふれたものです。攻撃を成立させているのは、先にかかってくる電話です。銀行を装った詐欺師が、被害者を言いくるめてマルウェアをインストールさせます。

7
クラスター内のトロイの木馬ファミリー

17,960+
台の感染端末（運営者自身のサーバーから集計）

7.6百万
通の SMS を被害者の端末から傍受

報告：Group-IB（2026 年10月 28 日）

攻撃の流れ

1 **電話**
銀行を装った電話の相手が、「クレジットカード保護プラン」や特典を持ちかけます。

銀行が通話中にアプリを送ることは決してないと顧客に周知する

2 **リンク**
被害者は、インドの 11 行の銀行または 2 の政府プログラムを装ったアプリファイルを受け取ります。

3 **偽のアップデート**
Google Play 風の「アップデート」画面で、アプリをインストールさせ、権限を許可させます。

4 **オーバーレイ**
銀行の画面を模したコピーが、カード情報、ログイン情報、PIN を求めます。

5 **SMS**
トロイの木馬が受信 SMS を読み取り、ワンタイムコードを運営者に転送します。

コードは単なる SMS ではなく、端末と取引にひも付ける

6 **窃取**
認証情報とコードを手にした運営者が口座を空にします。報告された被害額は 30,500 ドルを超えます。

当社のスキャン結果

アプリ内のオーバーレイ対策 **75.6%**

SMS ワンタイムコードに対応 **33.7%**

Android アプリに占める割合。オーバーレイ対策が守るのは正規のアプリだけで、通話中に送られた偽アプリでは機能しません。銀行が SMS コードを本人確認の証拠として受け入れる限り、攻撃は成功します。

防ぐことができた対策

- 銀行は通話中にアプリを送ることも、アプリのインストールを求めることも決してないと、アプリ内とすべてのチャネルで顧客に伝える。
- SMS コードを、端末と取引にひも付いた承認に置き換える。
- 通話中に現れた新しい端末や新しい送金先は、保留して確認する。

Group-IB、*False Protection, Emptied Accounts: The Seven Android Trojan Families Targeting Indian Banking Apps*、2026 年10月 28 日。
銀行名は記載していません。Group-IB はなりすまされた銀行の名前を公表していません。

ケーススタディ 2/4 · 乗っ取られたアプリ

WindRelay：被害者自身のバンキングアプリで組まれたローン。

中欧で組み合わせて使われた二つのツールです。被害者の端末を運営者に明け渡す遠隔操作型トロイの木馬 SpyNote と、被害者の決済カードの情報を NFC 経由で運び屋（ミュール）の端末に中継する WindRelay です。

2
つのツールを併用：遠隔操作型トロイの木馬と NFC リレー

3
か国が標的：チェコ、スロバキア、スロベニア

23
件のサンプル（2025 年11月〜2026 年7月に収集）

報告：Group-IB（2026 年8月 12 日）

攻撃の流れ

1 **電話**
ビッシング（音声フィッシング）の実行者が、銀行や他の信頼できる相手を装って被害者に接触します。

2 **インストール**
被害者がアプリをインストールします。SpyNote のビルドには、それぞれ被害者の名前が付けられています。

3 **カードのタッチ**
リレーアプリが、被害者にカードを端末にかざさせて PIN を入力させ、その情報を運び屋に転送します。

4 **現金化**
運び屋が中継されたカードで支払いや現金の引き出しを行います。

5 **乗っ取り**
運営者が SpyNote を通じて端末を操作し、正規のバンキングアプリを開きます。

画面の共有や遠隔操作を検知する

6 **ローン**
少なくとも一件では、運営者がそのアプリから被害者名義でローンを組みました。

ローン、送金先、限度額の変更にはサーバー側で追加認証を行う

当社のスキャン結果

アプリ内の遠隔操作の検知 **33.0%**

サーバー側アテステーション（Play Integrity） **16.0%**

Android アプリに占める割合。乗っ取りは被害者の実際の端末上で本物のアプリの中で起きるため、端末バインディングや SIM のチェックは通過します。画面が外部から操作されていることを確認できるのは、アプリだけです。

防ぐことができた対策

- 画面共有と遠隔操作を検知し、そのシグナルを銀行のリスクエンジンに送る。
- ローン、新しい送金先、限度額の引き上げには、鍵にひも付いた新たな承認を必須とする。
- カードのタッチに続いてアプリ内で PIN を求める流れを、不正のパターンとして扱う。

Group-IB、*WindRelay and SpyNote: an NFC and RAT combination in fraud*、2026 年8月 12 日。
銀行名は記載していません。Group-IB は被害を受けた銀行の名前を公表していません。

ケーススタディ 3/4 · すり替えられたアプリ

Hirudo：バンキングアプリをすり替えるトロイの木馬。

偽の画面を描画するだけにとどまらない Android のバンキング型トロイの木馬です。本物のアプリをアンインストールし、パッチを当てたコピーをインストールします。コピーに隠されたフックが、アプリ自身のセキュリティチェックに偽の回答を返します。

42
件の金融アプリが Hirudo の標的リストに

8
件のバンキングアプリ（インドネシアの 7 行）に既製のパッチ済みコピー

1
行のコードを各コピーに追加し、フッキングエンジンを読み込む

報告：ThreatFabric（2026 年10月 14 日）

攻撃の流れ

1 おとり
実際に動作するショッピング、ショートドラマ、サッカー、アダルト動画のアプリ。

2 偽のアップデート
おとりアプリがトロイの木馬をインストールし、トロイの木馬はユーザー補助と通知へのアクセスを求めます。

3 秘密情報
偽の決済画面、銀行画面、ウォレットの確認画面で PIN とパスワードを収集し、偽のパターン入力画面でロック解除コードを盗みます。

4 標的
トロイの木馬が、標的とする八つのバンキングアプリのいずれかを見つけ、その署名証明書を確認します。

5 すり替え
偽のアップデート画面からアンインストーラーを開き、その後トロイの木馬自身がパッチ済みのコピーをインストールします。

6 乗っ取り
コピーは偽造されたセキュリティシグナルを返しながら動作し、運営者は画面をリアルタイムで監視します。

保護対象のすべての操作について、Play Integrity の判定をサーバーで確認する

パッチ済みアプリの内部

コピーは元の名前とバージョン番号を保持していますが、公開されている Android のテスト鍵で署名されています。そのため、先に正規のアプリを削除する必要があります。追加された一行がフッキングエンジンを読み込み、エンジンはトロイの木馬が書き込んだファイルが存在する場合にのみ有効になります。

遠隔操作と情報収集

画面のリアルタイム閲覧とカメラのセッション、過去 90 日分の SMS の走査、そして中国、インド、メキシコ、モロッコ、タイの認証情報を標的にしています。保護されていない運営者のサーバーには、盗まれた数千件の認証情報と金融プロファイルが保存されていました。

ThreatFabric、*Hirudo: from fake updates to patched banking apps*、2026 年10月 14 日。
BleepingComputer、*Hirudo Android malware replaces banking apps to evade security checks*、2026 年10月 14 日。
銀行名は記載していません。ThreatFabric はインドネシアの銀行の名前を公表していません。当社のスキャン結果は次ページに掲載しています。

コピーの中では、あらゆるチェックが偽装されうる。

Hirudo は、攻撃者が制御するプロセスの中で銀行自身のチェックを実行し、その回答を自ら返します。Hirudo が偽装するアプリ内チェックを備えた Android バンキングアプリは 61%〜85.4% に上ります。

アプリが尋ねること	HIRUDO の回答	それを尋ねる ANDROID アプリ
署名証明書 「これは銀行の署名鍵か？」	HIRUDO の偽の回答 正規の証明書を返し、テスト鍵による署名を隠す。	署名・リパッケージのチェック **85.4%**
ユーザー補助サービス 「別のアプリが画面を操作していないか？」	HIRUDO の偽の回答 空のリストを返し、画面を操作しているトロイの木馬のサービスを隠す。	オーバーレイ・ユーザー補助悪用への対策 **75.6%**
スクリーンショット防止 「この画面は録画できるか？」	HIRUDO の偽の回答 フラグを取り除き、バンキング画面を遠隔で閲覧・録画できるようにする。	スクリーンショット防止 **61.0%**
ハードウェア鍵アテステーション 「鍵は安全なハードウェア内にあるか？」	HIRUDO の偽の回答 Google が証明書を失効させた、漏えい済みのハードウェアキーボックスで応答する。	集計対象外：他のアテステーション呼び出しと区別できないため
Play Integrity 「これは正規の端末上の正規のアプリか？」	HIRUDO の偽の回答 リクエストを攻撃者のサーバーに送り、サーバーが合格の判定を返し、アプリはそれを受け入れる。	Play Integrity の呼び出し **16.0%**

フック：ThreatFabric。割合：銀行自身のコードまたは同梱された SDK 内にチェックがある Android アプリ。Play Integrity：コードを読めたアプリ。チェックが存在することは、フックに耐えることを意味しません。

それでも有効な対策：銀行のサーバーが自ら確認する回答

- Play Integrity をサーバーで検証し、セッションと保護対象の操作にひも付ける。
- 鍵アテステーションの証明書を Google の失効リストと照合する。
- ログイン、認証情報の回復、新しい送金先、支払いの承認の各時点で、取引リスクのコントロールをサーバー側に維持する。
- ユーザー補助と画面キャプチャのシグナルは、単独でブロックする判断材料にせず、リスクスコアリングに取り込む。

出典：ThreatFabric（フック）、Ostorlab による分析（アプリ）。

ケーススタディ 4/4 · 漏えいするキー

AI の認証情報になった Google API キー。

Google は長年、AIza で始まる文字列である API キーは秘密情報ではないと開発者に説明してきました。Maps や Firebase のプロジェクトを識別するもので、アプリに含めて配布することが前提とされています。しかし、キーで何にアクセスできるかはクラウドプロジェクト側で設定され、その設定はアプリの配布からずっと後に、別のチームによって変更されることも少なくありません。

2,863
件の Gemini にアクセス可能な有効な Google API キーが公開 Web データ上で見つかった

32
件の Gemini にアクセス可能な有効なキー（人気の Android アプリ 22 件内）

82,314 ドル
悪用されたキーの被害者の一人が報告した Gemini の請求額

報告：Truffle Security（2026 年2月）、CloudSEK（2026 年4月）

無害なキーが AI の認証情報に変わるまで

1 **キーの配布**

アプリは、Google のドキュメントで認められているとおり、Maps や Firebase 用の Google API キーを含んでいます。

配布するキーはすべて、必要な API とアプリの署名に制限する

2 **Gemini の有効化**

別のチームが、同じクラウドプロジェクトで Generative Language API を有効にします。

AI の API は、キーを端末に配布しないプロジェクトに置く

3 **キーが AI へのアクセス権を獲得**

プロジェクトの既存のキーすべてから Gemini を呼び出せるようになります。アプリには何の変更もありません。

4 **悪用**

攻撃者がアプリからキーを抜き取り、Gemini にアップロードされたファイルを読み、請求額を膨らませます。ある被害者には 82,314 ドルが請求されました。

当社のスキャン結果

Android アプリ	80.3%
iOS アプリ	30.6%
HarmonyOS アプリ	71.4%

パッケージ内のいずれかの場所に Google API キーが一つ以上あるアプリの割合。全アプリでは 72.5%。キーはテストしていません。大半はおそらく Maps や Firebase に制限されていますが、アプリの開発チームはキーを見ただけでは判別できません。

防ぐことができた対策

- 各キーを、必要な API とアプリの署名証明書に制限する。
- Gemini などの AI の API は、別のクラウドプロジェクトに置く。
- 新しい API を有効にする前に、アプリで配布したことのあるキーはすべてローテーションする。

Truffle Security、*Google API keys weren't secrets, but then Gemini changed the rules*、2026 年2月 25 日。
CloudSEK、*Hardcoded Google API keys in top Android apps now expose Gemini AI*、2026 年4月 7 日。
銀行名は記載していません。いずれの出典も、キーが露出した金融機関の名前を公表していません。

2026 年に銀行が取るべき対策トップ 10。

十の対策は、それぞれ本レポートの検出事項と OWASP MASVS のコントロールグループに対応しており、不正の削減に直結する順に並べています。

01 サーバーでアプリを検証する

Play Integrity と App Attest を使い、判定をサーバーで確認し、不合格のリクエストを拒否します。パッチを当てられたアプリやすり替えられたアプリでも無効化できない、唯一の防御策です。

79.8% のアプリがアテステーションを使っていない

MASVS-RESILIENCE

02 重要な操作はすべて鍵にひも付ける

ログインと支払いの承認は、ハードウェア保護された鍵にひも付いた生体認証を通し、「はい／いいえ」の判定には決して頼らないでください。

35.1% の Android アプリに生体認証の回避の問題

MASVS-AUTH MASVS-CRYPTO

03 パスキーを提供する

パスキーによるサインインを追加し、対応する asset links と associated domains を公開して、フィッシングで盗まれたパスワードだけでは不十分な状態にしてください。

4.9% がパスキー API を統合

MASVS-AUTH

04 秘密情報をアプリから取り除く

秘密鍵、クラウドのキー、サービストークンをサーバーに移し、短期間有効なトークンを発行してください。アプリに含める必要のあるキーは、アプリの署名と必要な API に制限してください。

20.3% が Google API キー以外の認証情報を埋め込んでいる

MASVS-STORAGE MASVS-CRYPTO

05 ログインのリダイレクトを塞ぐ

ログインの戻り先には、自社アプリだけが登録できるユニバーサルリンクとアプリリンクを使い、他のアプリも登録できるカスタム URL スキームは決して使わないでください。

21.1% の iOS アプリで OAuth によるアカウント乗っ取りが可能

MASVS-PLATFORM MASVS-AUTH

06 遠隔操作とオーバーレイを検知する

root 化、フッキング、改ざん、オーバーレイ、画面共有の検知を組み合わせ、SDK にすでに含まれているチェックを有効にし、実機でテストしてください。

33% の Android アプリが遠隔操作の検知を備える

MASVS-RESILIENCE

07 配布するものを把握する

SDK とベンダーのプラットフォームを含め、リリースごとにソフトウェア部品表（SBOM）を作成し、重大なコンポーネントは定めた期限内に修正してください。

41.1% が脆弱なコンポーネントを含む

MASVS-CODE

08 すべての通信を暗号化する

平文通信を無効にし、自社 API には証明書ピンニングを適用し、WebView は自社のページに限定してください。

29.4% の Android アプリが平文通信を許可

MASVS-NETWORK MASVS-PLATFORM

09 古い端末に注意する

ログイン時に OS のパッチレベルを確認し、更新が提供されなくなった端末では高リスクの操作を制限してください。

99.5% の Android アプリが未パッチの OS で動作

MASVS-CODE

10 ラベルと連絡先を正確にする

ストアのプライバシーラベルをアプリの実際の動作と一致させ、研究者が連絡できるよう security.txt を公開してください。

7.1% の銀行ドメインが security.txt を公開

MASVS-PRIVACY

定義とデータに関する注記。

サンプル

本調査は上位500行のモバイルアプリを対象としています。Android、iOS、HarmonyOSで2,841件のアプリのストア掲載を収集し、2,686件をダウンロードして分析しました。国と地域は銀行の本拠地市場に従います。

深刻度

アプリの深刻度は、重大、高、中、低の検出事項のうち最も深刻なものです。「潜在的」（人による確認が必要なパターン）と「堅牢化」（欠けている安全策）はその評価を変えません。これらを数えるグラフでは、その旨を明記しています。高または重大とは、いずれかのレベルの検出事項が一件以上あることを意味し、低以下とは、重大、高、中の検出事項がないことを意味します。

プラットフォーム固有のルール

生体認証の回避、インテントリダイレクト、シリアル化、暗号、平文通信、データ保存のルールはAndroidのみで実行し、App Transport SecurityとプライバシーマニフェストのルールはiOSのみで実行します。これらの割合は、そのプラットフォームのアプリを分母としています。

不明な値

アプリのコードがパック済みまたは読み取れない場合、チェック結果は不明となります。それらのアプリはそのチェックの分母から除外し、その件数を図の横に示しています。シールディングのグラフでは、不明を独立した区分として示しています。

埋め込まれた認証情報

APIキー、アクセストークン、秘密鍵など、識別可能な形式の秘密情報。Google Cloud APIキーは別に集計しています。キーの有効性はテストしていません。

パスキーとアテステーション

パスキーAPIの統合とは、アプリがAndroid Credential Manager、Google FIDO2 API、またはAppleのAuthenticationServicesのパスキーAPIを呼び出していることを指します。他のライブラリに同梱されたFIDO2のクラスは数えません。アテステーションとは、Play Integrity、SafetyNet、HMS Safety Detect、App Attest、DeviceCheckのいずれかを指します。

シールディング

全三プラットフォームで、コードまたは同梱された製品に見つかった保護機能。iOSではroot化の検知の代わりに脱獄の検知を数え、オーバーレイ対策は該当しません。実機での動作は検証していません。

パッチ未提供のOSバージョン

AndroidとHarmonyOS：APIレベル34（Android 14）未満で、2026年3月以降Androidセキュリティ情報（Android Security Bulletin）のパッチが提供されていないもの。iOS：Appleが完全なパッチを提供している最古のメジャーバージョンであるiOS 18未満。

銀行側のデータ

バックエンドの露出とCVEはShodanのパッシブなインデックスであるInternetDBに基づき、バージョンから推定したもので、テストはしていません。侵害記録はVCDB、Have I Been Pwned、ransomware.live、SECへの8-K提出書類、およびG-SIBについては報道と規制当局の情報に基づき、照合はすべて人の目で確認しました。認証はウェブサイト上の表明です。

外部データ

WebとメールのチェックはDNSの1,252の銀行ドメインを対象としています。耐量子対応は、記録したTLSハンドシェイクから読み取りました。トロイの木馬の標的リストは、公開された47件のリストに基づきます。フィッシングホストは、四つの公開フィードのある時点のスナップショットに基づきます。プライバシーラベルはGoogle PlayとApp Storeから取得しました。開けなかった142行の銀行ウェブサイトについては、2025年以降の最新の公開アーカイブ（Internet Archive）を参照しました。アーカイブは稼働中のサイトより古い場合があります。

不正統計

規制当局、中央銀行、業界団体が公表した536件の数値で、それぞれ対象期間と対象母集団を併記しています。これらは各市場の不正の状況を示すもので、本レポートで示した弱点によって生じた損失を示すものではありません。

ケーススタディ

公開された研究の要約で、出典は各ページに記載しています。併記したスキャンの数値は当社によるものです。

Ostorlab

モバイルバンキングアプリ セキュリティレポート **2026**

バージョン 3 · 2026 年11月 12 日