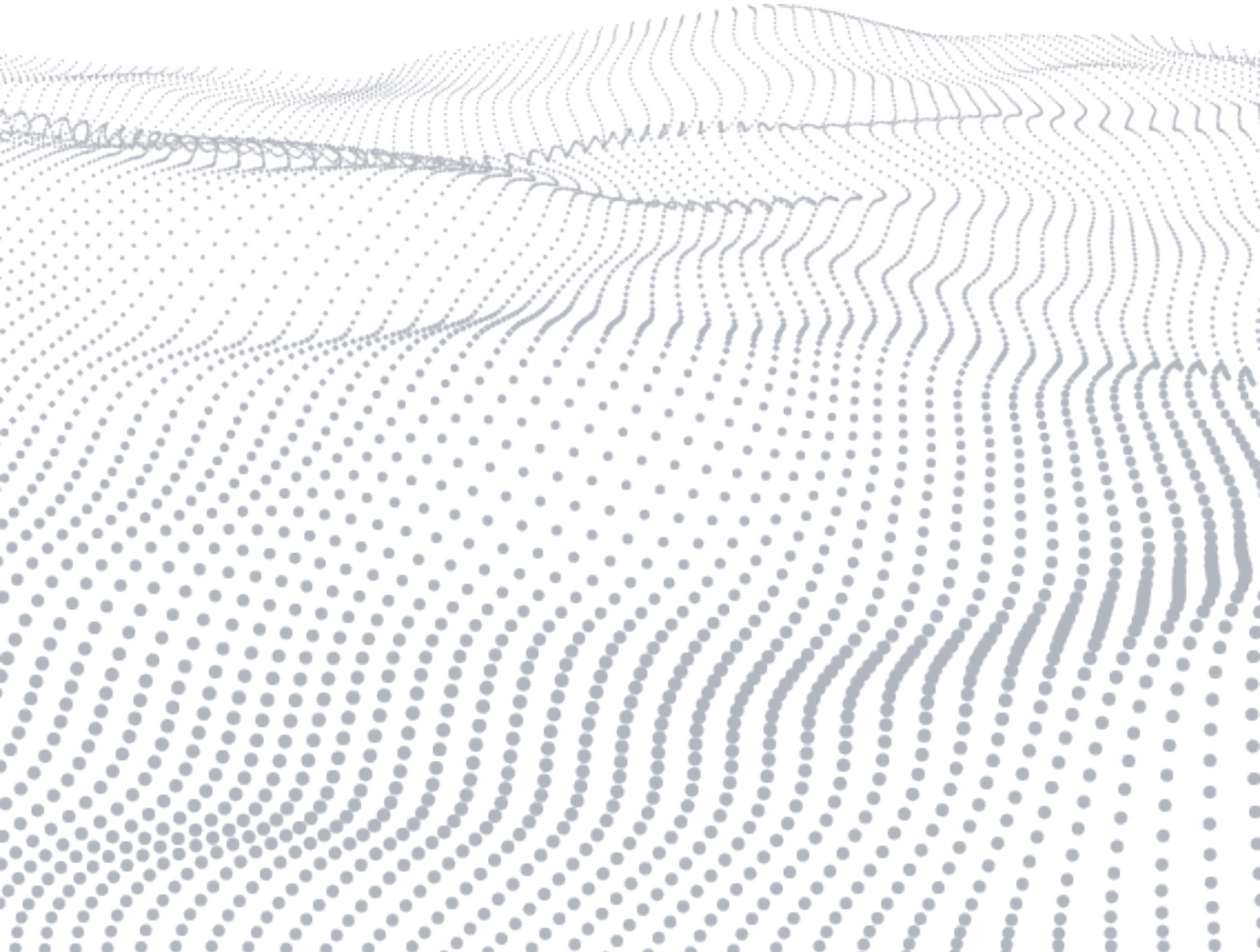
BLACKDUCK®

ホワイトペーパー

数字で見る金融サービス業界における モバイル・アプリケーションのセキュリティ・リスク



モバイル・アプリケーション・セキュリティの現状を調査するため、ブラック・ダック サイバーセキュリティ・リサーチセンター（CyRC）は Black Duck® Binary Analysis（BDBA）を使用して 3,000 本を超える人気 Android アプリケーションを分析しました。この調査は 18 のカテゴリでダウンロード回数と売上高の上位にランキングしているアプリケーションを対象に実施しており、モバイル・アプリケーション・セキュリティの中でも特に重要な以下の 3 項目に絞って分析を行っています。

- **脆弱性：**アプリケーションのオープンソース・コンポーネントに既知の脆弱性が存在するかどうか
- **情報漏洩：**秘密鍵、トークン、パスワードなどの機微なデータをアプリケーション・コードや設定ファイルに埋め込んでいないか
- **モバイル機器のアクセス許可：**アプリケーションがモバイル機器のデータや機能へのアクセスを必要以上に要求していないか

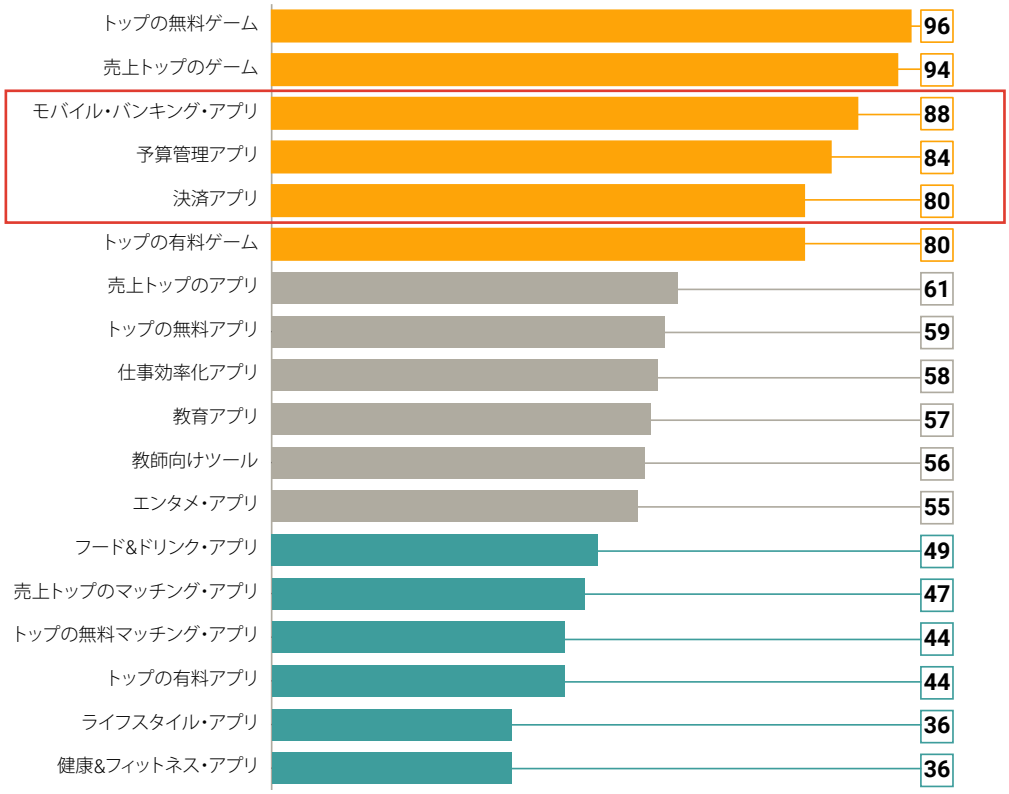
今回の分析により、現在使われているアプリケーションの大半に既知の脆弱性のあるオープンソース・コンポーネントが含まれていることが判明しました。それ以外にも、機微なデータがアプリケーションのコードに埋め込まれていることや、モバイル機器のアクセス許可が必要以上に要求されていることなど、セキュリティ上の問題が広く蔓延していることも明らかになっています。そしてこれらの問題は、今回分析した 3 つの FSI カテゴリ（決済アプリ、モバイル・バンキング・アプリ、予算管理アプリ）では特に深刻でした。

FSI に関する調査結果の概要

金融アプリケーションは機微な情報を取り込んで管理するため、私たちはそれが当然セキュアなものと信頼しています。しかし CyRC の調査結果を見ると、これはあまりにも楽観的な思い込みであるかもしれません。

CyRC がスキャンした全 3,335 本のアプリケーションのうち 2,115 本（63%）に脆弱なコンポーネントが含まれていました。脆弱性の見つかったアプリケーション 1 本当たりの脆弱性の数は平均 39 個です。これを FSI アプリケーションに限ってみると、その数字はさらに跳ね上がります。

全体的な CVE（共通脆弱性識別子）のデータを分析する中で、最も驚くべき結果が見られたのはモバイル・バンキング・アプリです。スキャンした全 107 本のモバイル・バンキング・アプリのうち 94 本に脆弱性が含まれていました。その割合は 88% で、全体の平均値 63% を大きく上回っています。モバイル・バンキング・アプリ全体では合計 5,179 個の脆弱性が見つかっており、脆弱性の見つかったアプリケーション 1 本当たりの脆弱性の数は平均 55 個です。つまり、これらのアプリが全体的なアプリケーション・セキュリティの足を引っ張る結果となっています。



1 本のアプリケーションが要求するアクセス許可の数（平均）

これらの調査結果は、モバイル FSI アプリケーションがその他のアプリケーションと同様にセキュアではないという明白な事実を示しています。

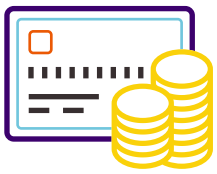
オープンソース脆弱性に関する調査結果

CyRC がオープンソースのセキュリティを調査したところ、すべてのカテゴリの中で脆弱性の数が 3 番目に多かったのがモバイル・バンキング・アプリです。解決策が存在する脆弱性と存在しない脆弱性の両方がこの順位であり、修正が迅速に行われていないこと、そして解決策の存在しない脆弱性に対する取り組みが不十分であることがうかがえます。

これらのアプリには、金銭に関する機微な個人情報を預けているため、そのリスクは非常に大きなものとなります。今回の調査で見つかったオープンソース脆弱性のほぼ 40% は、標準的なセキュリティ・プラクティスおよびツールさえ導入していれば容易に対処できていたはずです。言い換えれば、これら脆弱性の約 40% には、既に解決策が存在しています。

また、CyRC の分析では、オープンソース脆弱性を含む FSI アプリケーションの割合が非常に高かったこと、そしてアプリケーション 1 本当たりの脆弱性の数も多かったことが懸念すべき点として指摘されています。

脆弱なアプリケーション 1 本当たりの脆弱性の個数（平均）



決済アプリ =41

モバイル・バンキング・アプリ =55

予算管理アプリ =51

3 つの FSI カテゴリの中で、解決策の存在する悪用可能な脆弱性が最も多く見つかったのは、モバイル・バンキング・アプリ（39%）でした。

情報漏洩に関する調査結果

簡単に言えば、情報漏洩とは開発者が意図せず個人情報などの機微なデータをアプリケーションのソースコードや設定ファイルに残してしまうことです。あるいは開発者が意図的にこれらの情報をソースコードなどに残し、意図しないセキュリティ問題を引き起こす場合もあります。これらの情報が攻撃者の手に渡ってしまうと、悪用される危険性があります。今回の CyRC の調査では、人気ランキング上位のアプリケーションも情報漏洩の問題とは無縁でないことが明らかになっています。CyRC は、すべてのアプリケーションを対象に、以下のものを含む様々な主要な情報漏洩について分析しました。

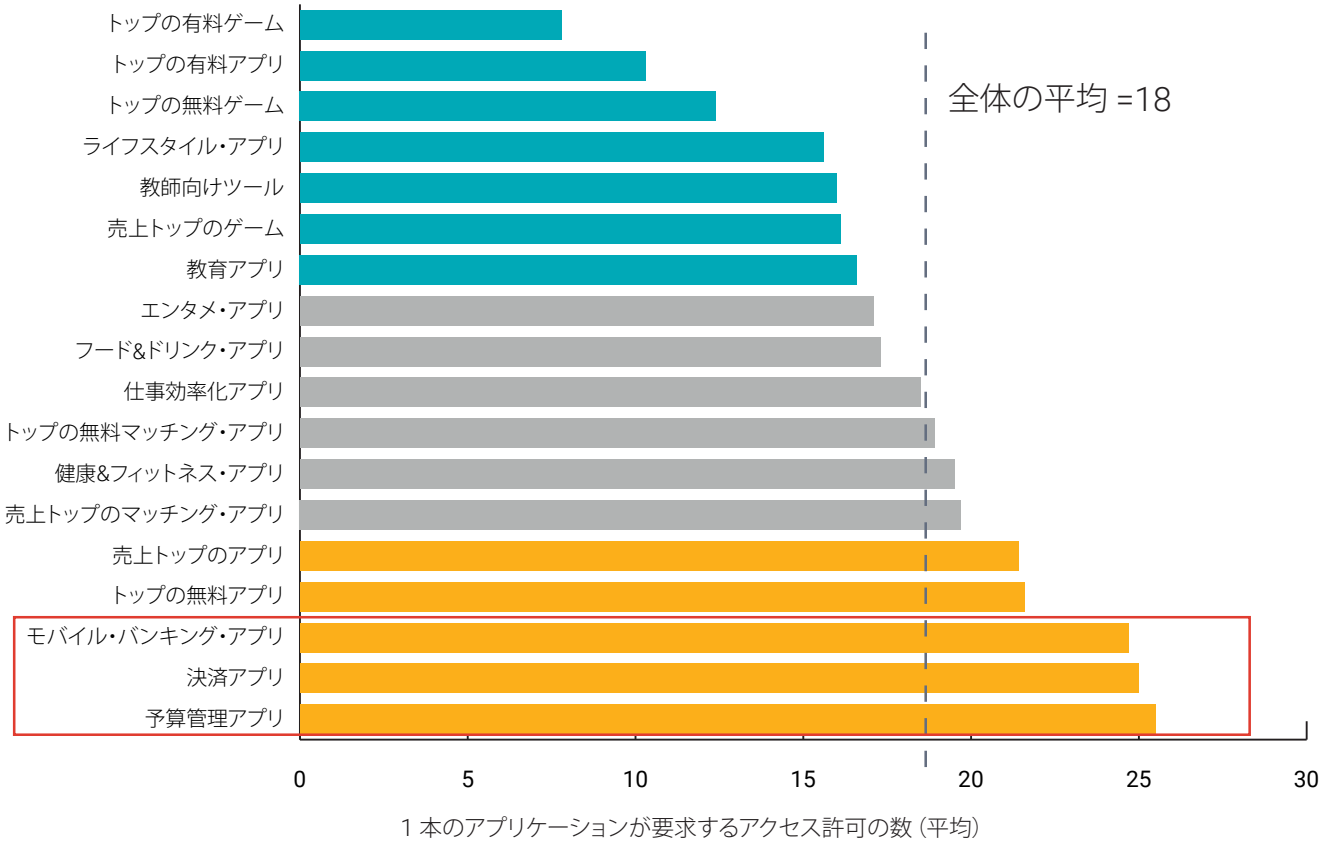
トークン、キー（鍵）、パスワード：これらの情報（AWS キー、Google Cloud トークン、ユーザーの資格情報など）を開発者が残したままにしていると、非常に大きな潜在的リスクが生じます。これらの情報が第三者の手に渡ると、サーバーやシステム、重要資産への不正アクセスが可能となります。そこから攻撃者は知的財産（IP）を盗んだり、マルウェアを仕掛けたり、演算リソースを起動してアプリケーションの所有者に損害を与えたりできます。

たとえば、JSON Web Token（JWT）は当事者間で情報を安全に受け渡す手段として使われます。JWT は暗号化が可能ですが、通常は暗号化せずに使用されます。JWT はデジタル署名された秘密鍵を必要とし、基本的には資格情報としての役割を果たします。このため、必要以上に長く保持することは避ける必要があります。ソースコードに残ったままの JWT は容易にデコードできるため、攻撃者はこの情報を悪用してアプリケーションを攻撃できます。

今回の調査では、モバイル・バンキング・アプリに 4 つ、予算管理アプリに 3 つの JWT が見つかりました。これは大きな懸念材料です。

モバイル機器のアクセス許可に関する調査結果

CyRC は Black Duck を使用して人気 Android アプリケーションに紐付けられたモバイル・アクセス許可を調査しました。CyRC のチームはまず、1 本のアプリケーションがユーザーに対して要求するアクセス許可の平均値（カテゴリごと、および全体）を調べ、その平均値から 2 σ（標準偏差）を超える数のアクセス許可を要求するアプリケーションに着目しました。このようにして、平均的なアプリケーションよりもはるかに多くのアクセス許可を要求するアプリケーションに特別な注意を払いました。



全カテゴリで見ると、1 本のアプリケーションが要求するアクセス許可の数は平均で 18 でした。一方、FSI アプリケーションはこれよりもはるかに多くのアクセス許可を要求しています。

- 予算管理アプリ：平均 26 個のアクセス許可
- 決済アプリ：平均 25 個のアクセス許可
- モバイル・バンキング・アプリ：平均 25 個のアクセス許可

まとめ

Black Duck Binary Analysis による分析で明らかになったのは、FSI アプリケーションが他の業界のアプリケーションよりもセキュアであると考えるべきではないという現実です。

また、今回の分析で見つかった脆弱性とリスクのほとんどは防ぐことができたか、容易に修正が可能なものであったのも事実です。にもかかわらず修正ができていないのは、強力なアプリケーション・セキュリティ・プラクティスおよびツールを導入していないことに理由があります。

ブラック・ダックの Black Duck SCA や Black Duck Binary Analysis などのソリューションを利用すれば、セキュリティ・チームはオープンソース脆弱性、潜在的な情報漏洩を含むインスタンス、およびモバイル・アクセス許可に関するデータを得ることができます。これらのツール、およびそこから得られる情報を活用することにより、情報に裏付けられた行動を起こし、アプリケーション・セキュリティの徹底を図ることができます。

Black Duck Binary Analysis の詳細は、ブラック・ダックの Web サイトをご参照ください。

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。

詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp