モバイル、アプリ、IoT のセキュリティ

世界中のデータとデバイスを保護

国家が支援するサイバー攻撃や悪意のある攻撃者がオンラインで激増する中、Google の製品とサービスは安全性から切り離せないものだと考えています。Google では、専門知識を共有することにより、進化し続けるサイバーリスクに社会が対処できるように しています。人々、組織、政府に対する保護 をこれまで以上に重視しており、 すべての人にとってより安全な世界 を築くために、最先端のサイバーセキュリティを 前進 させる取り組みを継続的に行っています。

そのため、増え続ける脅威に対処し、時代を先取りしたセキュリティ ソリューションを常に進化させることが不可欠となります。特に、インターネットに接続したあらゆるデバイスとアプリを保護するためには、生活者に対して、利用するデバイスとその機能を選べる安全な環境を提供しなければなりません。

課題

インターネット接続に伴う代償

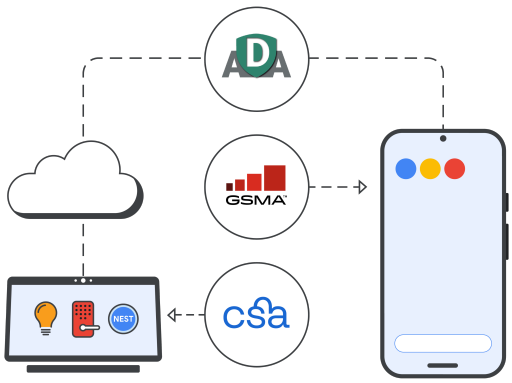
私たちは、日常生活で多くのアクティビティをスマートフォン、アプリ、IoT デバイスから行っています。オンラインで過ごす時間はますます増え、その過程で銀行や医療情報などの貴重なデータを共有する機会も同様に増え続けています。このため、巧妙なサイバー犯罪者は、これまで以上にこのようなデバイスを標的にして、機密情報を入手しようとしているのです。

デバイスとデータの増加に伴う脅威の増加

現在、世界にはプリンタやガレージドア開閉装置など推定 170 億台の IoT デバイス があり、それぞれには簡単にハッキング可能なソフトウェア（一部はオープンソース）が数多く搭載されています。[1] 全体として、 侵害された IoT デバイスの数は 2020 年にはほぼ倍増 しました。[2]

- IoT デバイスにより、私たちはますますつながりを深めていますが、インターネットに接続した製品のセキュリティ品質を測定する世界標準は存在せず、生活者はデバイスのセキュリティに関する意思決定を情報不足の状態で行っています。
- 生活者には購入する食品やクリーニング用品に含まれる成分を知る権利があるのと同じように、デジタル製品についても透明性を確保する権利があるべきです。
- モバイル デバイスは攻撃ベクトルの 1 つにすぎず、デバイスの相互接続により、セキュリティの透明性を大規模に展開することへのニーズが高まっています。そのため、コネクテッド デバイスのエコシステムのセキュリティは、ネットワークやシステムのセキュリティと同じくらい重要なのです。

Google と業界団体との連携



Google のソリューション

Google は、モバイル、アプリ、IoT のセキュリティを通じて、インターネットに接続したデバイスのセキュリティと透明性を向上させています。

モバイル セキュリティ

オープンソースのオペレーティング システムである Android は、階層化されたセキュリティ アプローチを活用して、モバイル デバイスを安全に保ちます。

- 階層化されたセキュリティ
  - 検証済みの起動、ロールバック保護、工場出荷時設定へのリセット保護により、最新かつ最も安全な Android バージョンが保証されます。
  - PIN と生体認証により、外部からのアクセスを防ぎます。
  - 「デバイスを探す」は、盗難や紛失に遭った際に、デバイスを見つけたりデータを完全に消去する機能です。
- 個人情報とパスワードの保護
  - 2 段階認証、セキュリティ キーとしての電話、パスワード マネージャーにより、Google アカウントを外部のアクセスから保護します。
  - セキュリティ診断と高度な保護のオプションにより、デバイスは安全かつスムーズに動作し続けます。
- フィッシングに対する保護対策
  - Phone by Google と Messages by Google は、詐欺やフィッシング攻撃を検出して防止する機能です。
  - Google セーフ ブラウジングは、世界中で 50 億台を超えるデバイスを保護しています。

アプリのセキュリティ

すぐに使用できるマルウェア対策は、悪意のあるアプリを排除し、データの安全性に関する情報により、ユーザーがアプリをダウンロードする際に透明性を確保します。

- Google Play ストア : すべてのアプリは、機械学習による検出ツールと人間のアナリストによって、ダウンロードが可能な状態になる前に審査されます。データの安全性セクションでは、アプリが収集するデータの種類とそのデータの用途について説明します。
- Google Play プロテクト : 毎日 1,250 億以上のアプリをスキャンし、セキュリティ リスクが検出された場合に通知、削除、無効化します。
- App Defense Alliance (ADA): Google は、モバイル脅威検出の大手パートナーと協力して App Defense Alliance を立ち上げました。このアライアンスは、インテリジェンスを共有し、検出で連携することにより、有害な可能性のあるアプリケーション（PHA）から Android ユーザーを保護します。

IoT セキュリティ

IoT セキュリティ ラベルは、どのようなデータが収集されているかなど、デバイス上のプライバシーとセキュリティの慣行を明確に示します。

- Google には、 IoT セキュリティ ラベリング スキーム に関する基本方針が 5 つあります。その 5 つとは、ライブ ラベル、評価スキーム、柔軟性と組み合わされたセキュリティ ベースライン、広範にわたる透明性、採用インセンティブです。
- Connectivity Standards Alliance (CSA) と GSM Alliance (GSMA) と協力して、既存ならびに今後の規制要件に対応する業界全体の認証プログラムを標準化しています。

Google の基本方針

Google では、インターネットに接続したデバイスのセキュリティと透明性を向上させるために 3 つの基本方針を適用しています。

徹底した防御 : Google は、スムーズで効果的に機能する強力な防御を構築するために、連携して機能する複数のセキュリティ アーキテクチャを利用しています。

オープンで透明: 透明性こそ Google の信念です。プラットフォーム ユーザーに情報を提供し、知識を共有して保護を強化することで、オープンソース エコシステムはクローズド エコシステムよりもっと安全になると考えています。

Google とそのエコシステムの優れた点: Google 社内と業界全体の専門家チームと提携して、何十億人ものユーザーの安全を確保しています。

アプリケーション

IoT セキュリティ ラベルを使って、生活者自身でコントロール

確立された IoT セキュリティ ラベルがなければ、デバイス メーカーが従うべき世界標準などありません。またユーザーには、自分のデバイスがデータを保護しているかどうかを確認できる可視性もないのです。IoT セキュリティを前進させ、生活者の手にコントロールを戻すには、業界が団結しなければなりません。Google は、自社のプロセスとパートナーシップを通じて、IoT セキュリティ ラベリング スキームの実現に取り組んでいます。

まず、脆弱性があるかもしれない場所を特定するために、外部のセキュリティ調査に投資します（Google Nest は Google の脆弱性報酬プログラムに参加しており、脆弱性を発見した Google 外部のセキュリティ研究者に報酬を提供しています）。

それからリリース後の少なくとも 5 年間は、重大なバグのパッチと修正を発行します。

2019 年以降に開発されたすべての Google デバイスでは、確認付きブートを使用して、必ず適切なソフトウェアが実行され、アクセスが保護されるようになっています。たとえば、Google Nest デバイスは、NIST、ETSI、ISO によって開発されたものなど、業界で認められたサードパーティのセキュリティ標準を使用して検証されています。

これらの標準と安全なソフトウェア開発ライフサイクル (SDLC) により、生活者が不十分なセキュリティ プラクティスにさらされる可能性が減り、オープンで安全なインターネットを利用できるようになります。

業界への投資とマイルストーン

2007 セーフ ブラウジングは、ユーザーが危険なウェブサイトにアクセスしたときに事前に警告するために確立され、現在では 50 億台を超えるデバイスを保護しています。

2010 Google 透明性レポートがリリースされ、政府や企業のポリシーと行動がプライバシー、セキュリティ、オンライン情報へのアクセスにどのように影響するかが示されました。2018 年には、Android 固有の透明性レポートも追加しました。

2017 Google Play プロテクトがリリースされました。これは現在最も広く展開されているマルウェア対策ソリューションで、30 億台以上のデバイスで 1 日 1,250 億を超えるアプリをスキャンしています。

2019 セキュリティ キーは、Android の組み込み機能として導入され、2020 年には iPhone にも導入されました。

2022 Google Play がリリースしたデータ セーフティ セクションは、アプリがユーザーのデータを収集、共有、保護する方法に関する情報をさらに提供し、App Defense Alliance による独立したセキュリティ レビューを完了したすべてのアプリに対して、最初のバッジシステムを開始しました。

2023 パスキー : パスワードのない未来は、FIDO Alliance と世界中の技術リーダーと共にオープン スタンダードを推進してきた 10 年を経て、拡張されたパスキー サポートによって動き始めています。

Google のアプローチ

オープンで安全なデジタル世界への取り組み

セキュリティ上の懸念は、さまざまなネットワークにまたがるデバイス数が増加し、データ量が多くなるほど高まっていきます。Google は、製品開発、透明性基準、業界とのパートナーシップを通じて、コネクテッド デバイス セキュリティの未来を前進させています。

Google の製品戦略の基盤は、製品がデフォルトで安全であるようにすることです。セーフ ブラウジング、Google Play プロテクト、組み込みのセキュリティ キーがモバイル デバイスとアプリを保護し、Google 製品にトップレベルのセキュリティを提供します。

問題への取り組み方をオープンで透明なものにし、インターネットに接続したデバイスのセキュリティに関する知識を共有することで、民主的なセキュリティ運用が行われるようにしています。Google は、階層化されたセキュリティ アプローチにより、クローズド エコシステムよりもオープンソース エコシステムの方が安全であると考えています。

CSA、ADA、GSMA の内部で協力することにより、サイバーセキュリティにおける最先端の機能を前進させて、インターネットとすべての人の未来がより安全になるよう努めています。

Google は、インターネットに接続したデバイスのセキュリティ基準を引き上げ、すべての人にとってより安全なオンライン環境の標準を定めることに取り組んでいます。コネクテッド デバイスのセキュリティにおける Google の進歩についての詳細は、g.co/connecteddevicesafety をご覧ください。

ソース : [1] CNBC Cyber Report, Jan 9, 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, July 20, 2021