Google

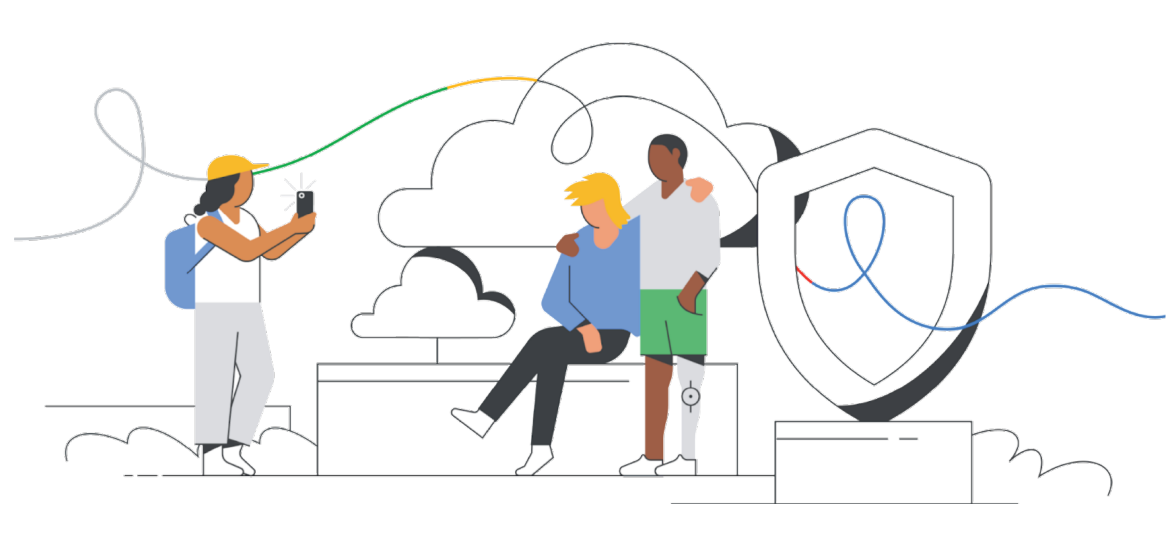
これまでのサイバーセキュリティの実績

Safer with Google

Google は、すべての人にとって安全なインターネットを実現するために、日々取り組んでいます。

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。



時代を超えて革新を続ける

2004 年の Gmail のリリースから 2022 年の Protected Computing の導入まで、Google はサイバーセキュリティ技術の先駆者となり、人々、組織、社会にとってより安全な未来を創造するために、製品、プラットフォーム、パートナーシップを継続的に革新してあらゆるクラスの脅威を排除してきました。

- 安全な製品とプラットフォームの開発
- アジャイルなセキュリティ チームの構築
- プログラムとパートナーシップの育成
- イノベーションと従業員のトレーニングに欠かせない資金の提供

人々のニーズとインターネットが進化する中、Google は常に変化するサイバー脅威を軽減するために、新しいテクノロジーの最前線に立ち続け、Google を利用することで、もっと安全な毎日を過ごしていただけるよう取り組んでいます。

2004 年 Gmail 迷惑メール対策

Google は、AI 主導のメール保護をいち早く構築した先進企業の一社です。

99.9% の危険なメールや疑わしいメールは Gmail によって ブロック されています。

2007 年 セーフ ブラウジング

ユーザーが危険なウェブサイトにアクセスしたときに警告を発することで、世界中のデバイスをプロアクティブに保護し、2020 年にはこれらのオンライン保護を強化されたセーフ ブラウジングに進化させました。

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。

2008 年 Google パスワード マネージャー

パスワード マネージャーの導入により、パスワードを覚えたり入力したりすることなく、より簡単かつ安全にサインインできるようになりました。現在では、さまざまなプラットフォームで利用される Chrome でのログインの 50% でパスワード マネージャーが使用されています。

10 億件のパスワードの侵害を毎日 チェック

2009 年 reCAPTCHA

クレデンシャル スタッフィングやアカウントの乗っ取りを阻止し、悪意のあるソフトウェアや偽ユーザーによる不正行為を防止するために、詐欺およびボット管理のソリューションを取得しました。

500 万 のウェブサイトを 防御

2010 年 ゼロトラスト

Google は、組織的な一連のサイバー攻撃であるオペレーション オーロラをかわした後、今では「ゼロトラスト」として知られるデフォルトで安全なアーキテクチャを構築するため、アプローチを革新しました。これにより、攻撃ベクトルが少なくなるほか、データを失う機会も減り、ユーザーが依存するシステムをより細かく制御できるようになります。Google は、連邦政府全体にゼロトラスト モデルを展開する米国政府の取り組みを支援しており、BeyondCorp Enterprise にパッケージ化して、あらゆる企業がゼロトラスト モデルを活用できるようにしました。

2010 年 Threat Analysis Group（TAG）

オペレーション オーロラの後、Google は政府が支援する重大な犯罪サイバー脅威の検出、分析、妨害を担当する専門家の専門チームを編成しました。TAG は歴史上最大のランサムウェア攻撃である Wanna Cry が北朝鮮発であることを追跡し、インド、ロシア、アラブ首長国連邦からの hack-for-hire（雇われハッカー）のエコシステムの例を共有しました。

2010 年 Google バグハンター

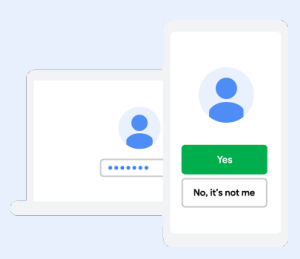
Google の脆弱性報奨プログラムは、Google 製品でバグを見つけて賞金を獲得したい高校生、弁護士、IT 専門家や愛好家の注目を集めています。このような人々の動機はさまざまですが、使命は同じです。それは、未発見の脆弱性を見つけて、オンラインサービスでの安全・安心を確保することです。

何百万ドルもの報酬が 2010 年以降支払われています。

2010 年 レッドチーム

敵対的な考え方で Google をハッキングすることで、その防御を強化しつつ、防御でのギャップを見つけるために立ち上げました。このチームは、世界中で現在の脅威に対応し、セキュリティ制御を改善し、攻撃の検出、防止を実施し、新しくより優れたフレームワークを推進することで、全体的なクラスの脆弱性を排除しています。

2011 年 2 段階認証プロセス



Google は、デフォルトで 2 段階認証プロセス（2SV）を提供した最初の企業の 1 つです。2021 年には 1 億 5,000 万人を超えるユーザーに対して 2SV を自動的に有効にし、安全で簡単なログイン方法を提供した最初の企業となりました。たとえパスワードが盗まれても、アカウントは保護されています。

2SV 以降、侵害されたアカウントが 50% 減少

2013 年 プロジェクト シールド

プロジェクト シールドは、脅威を特定し、セキュリティ コミュニティと法執行機関で対応できるようにすることで、100 か国以上で分散型サービス拒否攻撃（DDoS）からニュース、人権団体、選挙サイト、政治組織、キャンペーンを保護するのに役立ってきました。

150 以上のウェブサイトを現在ウクライナで 保護

2014 年 プロジェクト ゼロ

安全でオープンなインターネットの確保に向けて、ソフトウェア、ハードウェア、Google 製品など、インターネット全体でゼロデイ エクスプロイトを追跡する専門のタスクフォースです。このタスクフォースは「Meltdown」と「Spectre」の詳細を初めて示した団体で、これにより開発者が CPU の脆弱性に迅速に対処し、ソフトウェア サプライ チェーン全体に緩和策を適用できるようになりました。

2017 年 高度な保護機能プログラム（APP）

ジャーナリストや政府関係者など、注目されやすくリスクの高いユーザー向けのセキュリティ キーを含む特別な保護機能です。

300 以上の連邦政府によるキャンペーンを 保護

2017 年 Google Play プロテクト

世界で最も広く展開されているモバイル脅威に対する保護サービスで、Google の機械学習を使用して常に適応、改善されている Google Play プロテクトは、アプリのマルウェアを自動的にスキャンし、Android スマートフォンでのユーザーの支払いを暗号化します。

1,000 億以上のアプリでマルウェアを毎日スキャン

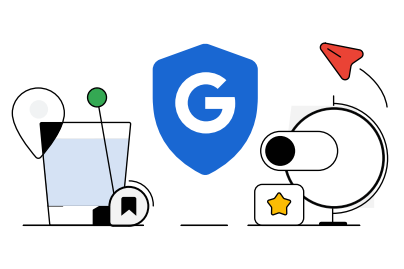
1 億 5,000 万 のユーザーの支払いを毎日 暗号化

2018 年 Titan セキュリティ キー

Titan セキュリティ キーは、エンドツーエンドの Google ソリューションを必要とするユーザー向けに作成しました。このキーは FIDO に準拠しており、Google だけでなく他の場所でも使用できます。

2019 年 パスワードレス再認証

Android での FIDO のサポートが拡張され、ユーザーがパスワードなしでシームレスに PIN または生体認証だけでウェブサイトにログインできるようになりました。



2019 年 Chronicle

Google のコア インフラストラクチャ上に特殊なレイヤーとして構築された Chronicle は、クラウドベースのセキュリティの提供に向けて導入され、企業が生成する大量のセキュリティとネットワーク データを非公開で保持、分析、検索できるように設計されています。

2021 年 サイバーセキュリティの推進に向けた投資

Google は、サイバーセキュリティの強化、ゼロトラスト プログラムの拡大、ソフトウェア サプライ チェーンの安全確保、オープンソース セキュリティの強化に取り組んでいます。Google Career Certificate プログラムでは、IT サポートやデータ分析などの分野で 10 万人のアメリカ人をトレーニングすることを約束しました。

100 億ドルをサイバーセキュリティの取り組みに向けて投入

2021 年 Confidential Computing

Google Cloud Confidential Computing は、重要なセキュリティ、安全性、プライバシーの確保に向けて導入されました。これは、処理中のデータを暗号化する画期的なテクノロジーであり、保存中や転送中などライフサイクル全体でデータを安全に保つことができます。最も機密性の高いデータでも、自信を持ってクラウドに移行できるようになりました。

2021 年 Google オープンソース セキュリティ チーム（GOSST）

GOSST は、世界中のユーザーが依存しているオープンソース ソフトウェアのセキュリティの向上のために作成されました。Open Source Security Foundation（OpenSSF）と提携した Google は、ソフトウェア サプライ チェーンを保護し、ソフトウェア エコシステム全体の長期的なセキュリティを可能にするフレームワークである Supply-Chain Levels for Software Artifacts（SLSA）を開発してリリースしました。

1 億ドルをサードパーティのオープンソース セキュリティ オペレーションに投入して脆弱性の修正を支援

2022 年 ポスト量子暗号標準化

Google は、未来を見据えた公開鍵暗号システムの解読とデジタル通信の侵害を防ぐ次世代暗号システムの開発を継続的に行っています。アメリカ国立標準技術研究所は、標準化に向けて Google が関与する提出物（SPHINCS+）を選択しました。

2022 年 Protected Computing

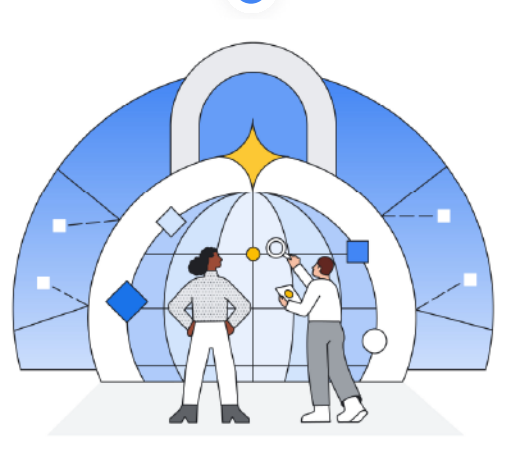
Google は Protected Computing を発表しました。これは、データを処理する方法、タイミング、場所に変革をもたらす、進化したテクノロジーのツールキットで、データのプライバシーと安全性を技術的に保証します。この実現に向けて、データのフットプリントを最小限に抑え、データの匿名化を行い、機密データへのアクセスを制限しています。これにより、会話のプライバシーを完全に守りながら、Android がテキスト内で次にくるフレーズを提案できるのです。

2022 年 Mandiant と Google Cloud

Mandiant は、世界最大の組織におけるサイバーセキュリティの最前線で得られたリアルタイムの詳細な脅威インテリジェンスを提供します。Google Cloud のクラウドネイティブ セキュリティ サービスと組み合わせ、企業や公的機関がセキュリティ ライフサイクル全体で保護されるようにしています。

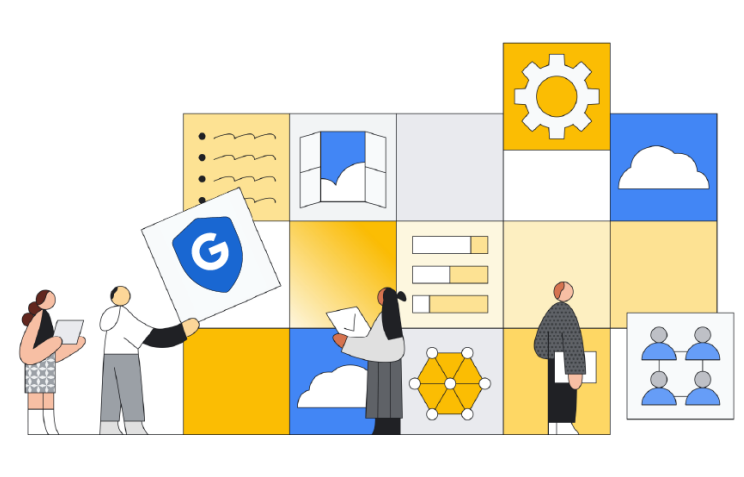
2023 年 パスキー：パスワードのない未来

Google は、10 年以上前からパスワードのない未来に向けて取り組んできました。2013 年に FIDO Alliance に参加し、パスワードのない世界に向けたオープン スタンダードを推進してきました。2023 年には、パスキー テクノロジーにより FIDO サインイン標準のサポートを Android と Chrome にも拡大し、真のパスワードのない未来へのプラットフォームがついに実現します。



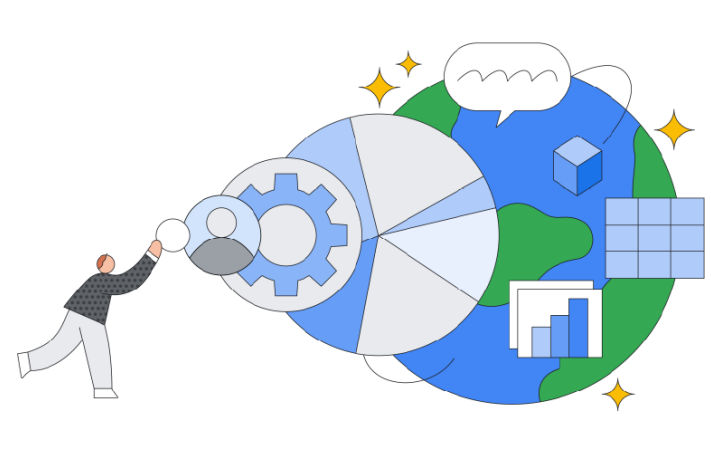
テクノロジーが利用される範囲がますます拡大する時代において、社会の真の可能性を解き放つ鍵となるのは、信頼できるテクノロジーなのです。

Google は、セキュリティに関する知識を実践に活かしながら、引き続き、人々、企業、政府と協力して安全を守り、サイバーセキュリティの新時代を切り開いていきます。



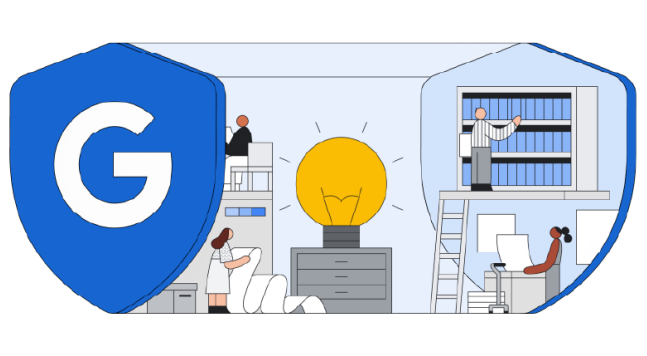
人々、企業、政府を保護

セキュリティは、Google の製品戦略の基盤です。そのため、すべての Google 製品には保護機能が組み込まれており、デフォルトで安全が確保されています。



進化するサイバーセキュリティのリスクに対処できる社会に

Google は、オープンソースの可能性を解き放つことで社会に力を与え、Google の知識と専門能力を業界とオープンに共有して、エコシステムをより安全に保ちます。



未来のテクノロジーを推進

Google は、次世代のサイバー脅威から社会を守りたいと考えています。今まで培った AI の専門知識を基に、セキュリティ イノベーションの限界を押し広げる次世代のアーキテクチャを設計しています。

Google で毎日をもっと安全に

Visit g.co/safety/cyber

Google