F-SECURE CONSULTING

自動車産業向けサービス

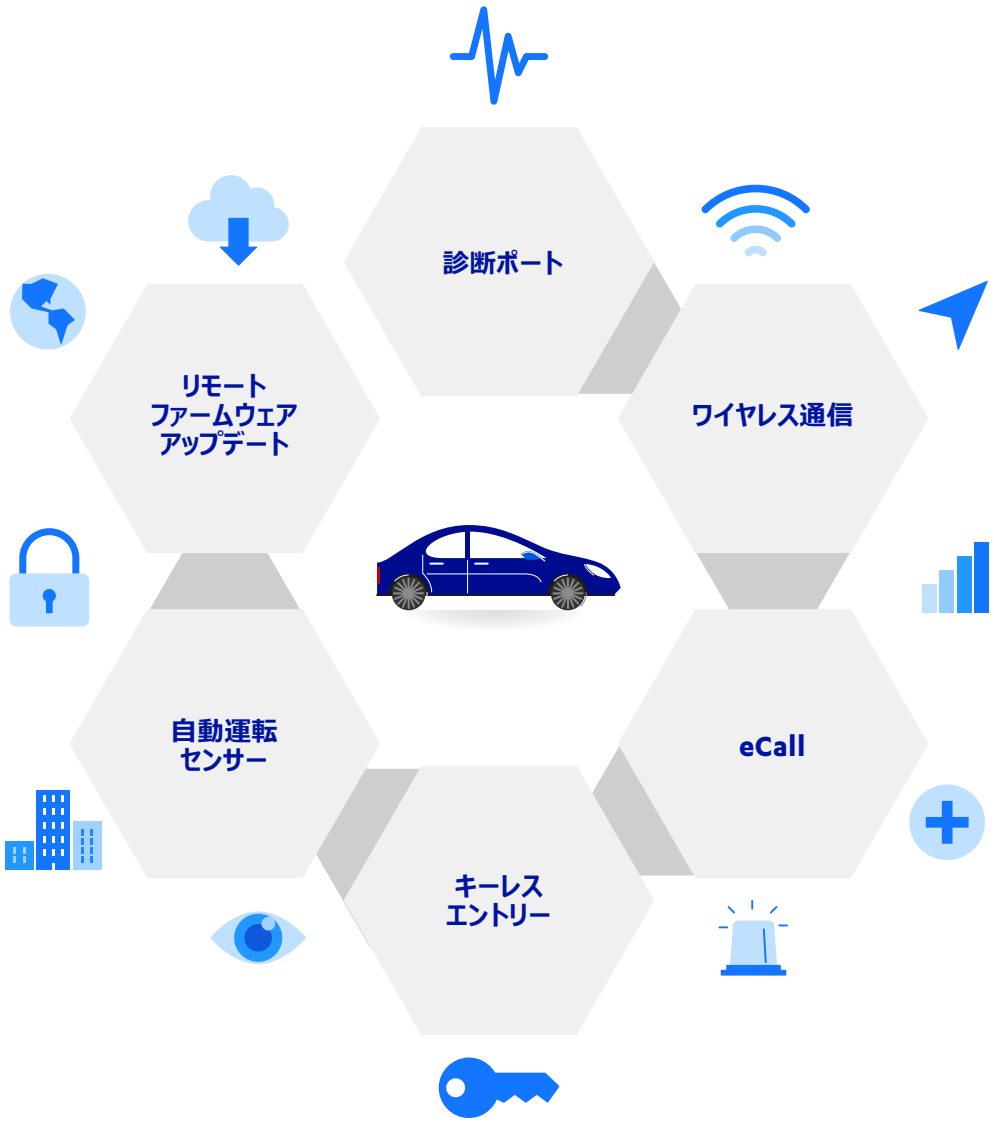
F-Secure

目次

背景

2017 年 2 月、F-Secure は航空電子機器、自動車産業、および産業用制御システム業界向けのセキュリティを専門とする業界をリードする企業「Inverse Path」社を買収[1]しました。この買収により、F-Secure Consulting はハードウェアや確実な安全性が求められる組み込みシステム（自動車用コンポーネントなど）のセキュリティを提供するうえで重要な役割を果たす、最先端のスキルを持つスタッフの獲得に成功しました。

そして現在、自動車産業分野は F-Secure Consulting の新たなコアセグメントとなりました。



[1] https://blog.f-secure.com/ja/f-secure-acquires-inverse-path/

自動車産業

現在の自動車には、かつてないほど多くの機能やテクノロジーが搭載されるようになっています。そして同時にサイバー攻撃の対象となる領域も拡大しています。

セキュリティに関する新たな懸念を払拭するには、データの盗難を目的とする脅威にフォーカスした従来の対策に加えて、顧客データやデバイス、さらに安全性が求められる自動車用コンポーネントにいたるまで、広範に及ぶ対策を実践しなければなりません。

最先端のコネクテッドカーの場合、アタック・サーフェス（攻撃対象となる可能性がある領域）として以下が考えられます。

- リモート接続された ECU[2] または TCU[3]
- 車両搭載型のテレマティクス（eCall システムなど）
- インフォテインメント接続システム（USB、Bluetooth、Wi-Fi、セルラーなど）
- 車両診断システム（OBD や TPMS など）
- キーレスシステム
- 自律走行センサー
- 携帯アプリ経由での「スマート」遠隔制御をサポートするインフラ
- カーシェアリング用アドオン

自動車産業界では安全に関する規制がすでに広く適用されていますが、開発から実装に至るあらゆる段階で細心の配慮と対策が求められるサイバーセキュリティ対策においては、成熟度・堅牢性などにおいて十分なレベルには達していないのが現状です。

F-Secure Consulting のハードウェアセキュリティチームは、伝統的なソフトウェア領域におけるセキュリティコンサルティングに精通する一方、ハードウェアセキュリティのエンジニアリングに関する深い理解と豊富な実績をもとに、業界で確固たるポジションを獲得してきました。

これらのノウハウにより、自動車・航空産業における豊富な実績と、安全性やセキュリティ、ソフトウェアとハードウェアの関係性についての深い理解に基づくサービスを提供しております。

高度な安全性を担保するためには、ハードウェアに侵入するため改変されたファームウェアコードへの対処法を事前に評価・検証する必要があります。ここではファームウェアで直接的、間接的にコントロールする I/O のすべての経路の評価に加え、安全性が重視されるコンポーネントの隔離および役割の分割が不可欠です。

F-Secure Consulting のハードウェアセキュリティチームは、こうした自動車メーカーの製品、管理下にある車両、支援インフラなど、攻撃対象となり得るすべての領域を保護することにより、自動車メーカーのセキュリティ対策を継続的にサポートします。

> 安全のため、
> 故障は許されない。

2 システムを電子回路を用いて制御するユニットの総称。主に自動車に搭載されるものを指す。
3 テレマティクス制御ユニット。ワイヤレスの追跡、診断、自動車との双方向通信の各機能を制御する組込みシステム

コアサービス

- **デザインレビュー**

  暗号化プロトコル、API 設計、さらにアプリケーションの全体構成など、上位レベルの仕様を分析できることは、製品開発の全工程を通じて脆弱性を予防する上で不可欠なものです。

  F-Secure では、常にすべてのソフトウェアとハードウェアの開発計画の初期段階から分析を行い、長期的な視点でセキュリティ対策のゴールに大きな影響を与える重要な意思決定ステップのレビューを行っています。

- **コードレビュー**

  論理回路の定義から、アセンブラや C 言語、高水準言語にいたるまで、あらゆるプログラミング言語を網羅しています。

  F-Secure では、情報セキュリティ分野における豊富な経験を独自の開発プロジェクトに組み込むことで、あらゆるサイズのコードベースを分析します。これにより、アタック・サーフェスやエントリポイントを特定し、セキュリティ上の脆弱性を発見します。

  また、F-Secure のチームはハードウェアに関する深い知識を備えており、ファームウェアを実行するアーキテクチャの物理レイヤーに近いレベルの実行方法を評価することで、ハードウェアとの統合において起こり得る潜在的な問題を特定できます。

- **ペネトレーションテスト**

  F-Secure Consulting チームは「グレーボックス」と「ブラックボックス」のペネトレーションテストにおいても豊富な経験を有しており、従来のソフトウェアに加え、特にハードウェアの構成やファームウェアのリバースエンジニアリングにも焦点を当てています。

  ハードウェアセキュリティのチームメンバーは、自動車のセキュリティ領域における研究成果を公開した初のグループでもあり、それ以降、車両プログラム全体に対する多数のペネトレーションテストを実施しています。

- **セキュリティエンジニアリング**

  たとえ問題を特定できたとしても、それを解決するためのソリューションを探し出すことは、お客様やコンサルタントが予想している以上に困難です。セキュリティ評価の本当の価値は、業務プロセスの中で十分に真価を発揮できる、現実的かつ管理可能なリスク緩和策やソリューションを選定し、提案できるかにかかっています。

  F-Secure のチームは常にこのことを念頭に置き、セキュリティエンジニアリングのベストプラクティスを重視しながら、これまで世界中の企業のソフトウェアやハードウェア製品の開発をゼロから支援してきました。

- **セキュリティの統合**

  安全性が重要になる電子製品は、クリティカルなセキュリティ課題としての対処が不可欠です。そのため、信頼できるドメインと相互接続する境界が直接 / 間接的に攻撃対象となり得るという認識のもと、徹底的な検証の実施が非常に重要になります。

  アビオニクス[4] などをはじめとする弊社のコアサービスとなる専門技術は、航空産業をはじめとする数多くの分野で培った経験の上に築き上げられております。これらをベースとして、安全性が重視されるドメイン間における一方向チャネルの制御や関連する例外の指定などについて、厳格なセキュリティ規格に従い目的通りに機能できるようになります。

[4] 航空機に搭載され飛行のために使用される電子機器

実績

弊社は自動車のセキュリティに関する公的な研究成果を世界で初めて発表しております。これまで多数の自動車メーカー / 自動車テレマティクス製造業者の製品セキュリティ対策をサポートしてきました。

最新の自動車には、エンターテインメントやテレメトリ[5]、安全対策など、ネットワークに接続可能なさまざまな機能が搭載されています。私たちのハードウェアセキュリティサービスは、日本を含む世界中のさまざまな自動車メーカーや自動車部品メーカーによって採用されており、エントリーポイント（USB などのローカル、Bluetooth や Wi-Fi などの小範囲、セルラーなどの広範囲なインタフェース）を外部の脅威から保護することで、車両の安全を確保してきました。

ハードウェアに関する詳細な知識を背景に、弊社はリモートデータ接続や車両制御通信バスに接続された内部コンポーネント（CAN[6] バストランシーバーなど）と、メインのアプリケーションプロセッサの分離状態、その間の通信フローによって生じるセキュリティの評価や脅威の検証を行います。

チームは幅広いスキルを保有しており、付帯する NFC やセルラーインターフェース、または悪意を持ったユーザーによる物理的なセキュリティ侵害など、車両の攻撃対象となり得る領域を拡大しかねない昨今の車両システム（カーシェアリング用アドオンなど）に的確に応用することができます。

さらに、拡大の一途をたどる「ブラックボックス」のテレマティクス[7]機器市場では、自動車メーカーではなくサードパーティの保険会社などが、アドオン機能として導入を加速させています。セルラー、Wi-Fi、Bluetooth 接続デバイスは、安全性を重視したバスとのブリッジとして機能する一方、こちらもアタック・サーフェスを拡大する要因となるため、F-Secure ではこれらのデバイスのセキュリティ環境を定期的に精査することで、メーカー側のリスクの低減を支援しています。

---

5 観測対象から離れた地点から様々な観測を行い、そのデータを取得する技術
6 コントローラーエリアネットワーク。ホストコンピュータなしでマイクロコントローラやデバイスが相互に通信できるように設計された、耐ノイズ性の強化が考慮された堅牢なビークルバス規格
7 移動体に移動体通信システムを利用してサービスを提供することの総称

ケーススタディ

車載インフォテインメント

常時接続型の最新の車載インフォテインメントシステムや車両テレマティクスユニットは、ドメインをまたがるシステムとなる可能性があり、これらは車両制御通信バスとインターネットとの通信が可能なものです。

F-Secure が複数の自動車メーカーおよび自動車部品メーカーのプロジェクトに参加して、ローカルやリモートからの攻撃に対する耐久性を検証した結果、車両用の CAN バス（制御用通信バス）にリモートから不正アクセス可能なケースが少なくないことが分かりました。

弊社は関連するあらゆるレイヤーに精通することにより、実践的なリスク緩和策と長期的な設計向上を顧客へ提案してきました。これにより、仮にインフォテインメントユニットに不正アクセスが発生した場合でも最悪の事態を避けられるよう、内部コンポーネント間の分離が確保されるようにしました。

カーシェアリング

NFC カードやモバイルフォンの Bluetooth を利用したキーレスのカーシェアリングシステムの普及に伴い、車両の攻撃対象となり得る領域が大幅に拡大しました。また、自動車メーカーでは扱っていないサードパーティ製の装置が取り付けられる可能性も増大しています。

F-Secure では複数のクライアントに対して、特定の車両（最悪の場合はすべての車両）への不正アクセスを許可してしまう NFC / インターネットベースの、あるいは物理攻撃から保護するためのセキュリティ対策を支援しました。

車載ブラックボックス

現在、多くの保険会社が車載テレマティクス（ブラックボックス）の導入を推奨することで、GPS や速度情報を顧客別に正確に割り出す形で保険料の割引を図っています。

保険会社がアドオン機能などを自社開発することはほとんどなく、サードパーティからの提供に依存しているため、セキュリティを適切に検証するための技術的な専門知識が不足していることが少なくありません。

こうした製品の品質はさまざまではあるものの、市場の大きさを考えると、十分にセキュリティが確保されていない製品が多く出回っている可能性があります。

F-Secure では複数のクライアントに対し、不適切な車載ブラックボックスを特定する支援を製品選定の段階から行ってきました。また、すでに導入済みのユニットを徹底的に評価することで、深刻なセキュリティの脆弱性への対処も行いました。

車載ブラックボックスが正常に動作することは、ドライバーの安全や保険会社に対する評価はもとより、改ざんや誤使用による保険金支払の負担を避ける意味でも非常に重要です。

交通情報チャンネル（TMS）

F-Secure は、交通情報チャンネル（TMS: Traffic Message Channel）の国内全体への導入を成功に導きました。これにより警察や輸送管理責任者は、事故や渋滞のリアルタイムな情報を提供できるようになりました。

F-Secure の幅広いスキルにより、イベントを容易に入力できる Web アプリケーションをはじめ、RDS エンコーダ、全国をカバーする衛星ナビゲーションシステムに信号を送信する FM 送信機に至るまで、インフラ全体をカバーする開発に貢献しました。

ハードウェアダイオード

安全性が極めて重視される領域（航空管制など）を、それ以外の領域（飛行中のエンターテイメントなど）の管理と適切に分離できるかどうかは、その分離をどれだけ物理層に近い部分で実施できるかにかかっています。レイヤーによっては必ず相互接続が必要になるので、データを一方向だけに流れるようにするデータダイオードを採用することで、セキュリティレベルの低い領域のデータがクリティカルな領域に流れ込まないようにして保護を確立します。

F-Secure は、データダイオードの設計や実装内容についての検証を複数のプロジェクトで行い、データを一方向に流し続けることで得られるメリットを担保してきました。

データダイオードの実装範囲は、初歩的な電子接続（またはその欠如）から、より複雑なカスタム論理回路（FPGA ベースなど）にまで及びます。

アビオニクスの分野ではハードウェアダイオードの採用は一般的であるため、F-Secure はアプリケーションの認証プロセスの前段階において、開発者が問題を修正できるようにサポートいたしました。

また自動車産業のクライアントの例では、インターネットに接続されている「機能豊富な」組み込みシステムを車両制御通信バスから切り離すなど、航空電子機器システムに適用されるものと同様の厳しい原則の導入を支援しました。

脆弱なセキュリティ計画に対する防御戦略として、データダイオードを設置したり、適切な導入を計画して統合を実装することは、最悪のシナリオに対する緩和策となるだけでなく、自社では対応が困難なセキュリティ障害に対する顧客の法的責任を保護するためにも不可欠となります。

ハードウェアセキュリティモジュール

暗号鍵などの復号情報の内容を従来のサーバで扱うことにより、さまざまなインフラやクラウドプロバイダ、および利用している会社自体へ流出してしまうのを避けるため、HSM はセキュリティに関する認識が高いサービスプロバイダの間で広く普及しています。

これはデータへの不正アクセスがあった場合に責任の重大性を把握できるとともに、すべての機密情報を完全に暗号化する最初のステップとしても優れた手段だと言えます。

F-Secure では HSM を利用するクライアントに対し、HSM の適切な設定をサポートします。不適切な論理回路やプロセスにより、HSM の外部にデータや機密情報を漏出させるようなミスの発生を回避できるようにしました。また、クライアントが運用要件に合致するよう正しく HSM を導入し、それが高度な攻撃にも耐えられるかどうかの確認もしています。

さらに HSM のハードウェアおよびファームウェアメーカーとも連携し、メーカーが HSM 製品を市場に投入する前に、製品の悪用やハードウェア攻撃に対して適切に機能するように開発のサポートも実施しております。

ARM® TrustZone®

従来の TPM とは対照的に、ARM TrustZone（TZ）テクノロジーを効果的に活用するための支援を通じて、開発者はドメインを「安全」な領域と「通常」の領域に分割し、信頼性に優れたプラットフォームモジュールのカスタム開発ができます。これは CPU コアに限定することなく、SoC コンポーネント全体を通じて反映されます。

このテクノロジーは当初、DRM 保護向けにモバイルフォンで広く採用されてきたものですが、安全性が重視されるタスクと、安全性が不十分である可能性がある「高度な」アプリケーションを単一の CPU 上で混在した形で稼働させることができるため、自動車産業でもその利用が急速に広まりつつあります。

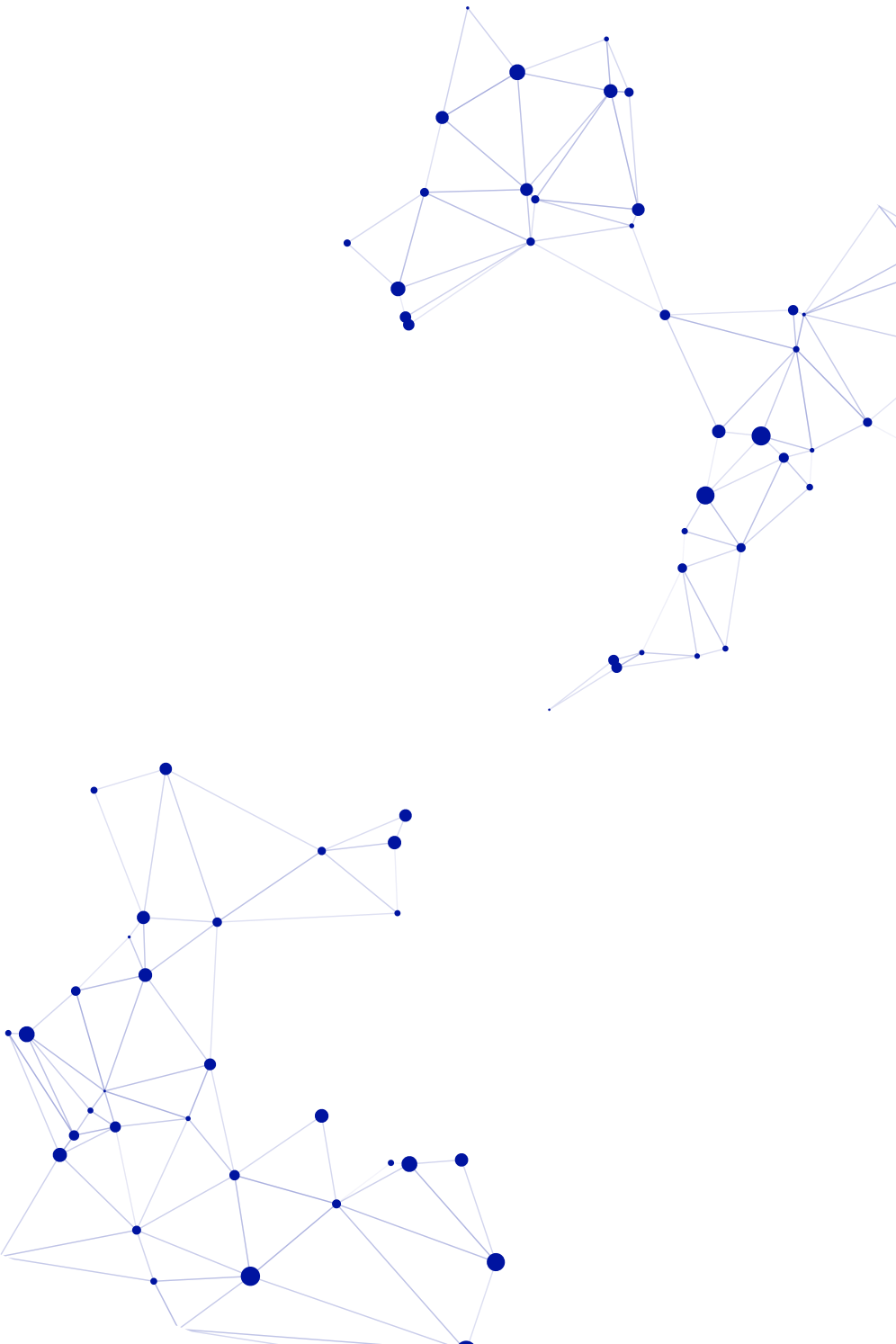
F-Secure は TZ の効果的かつセキュアな導入に向けて、検証や設計、トレーニングを提供してきました。このタスクには内部のハードウェアレイアウトに関する専門知識が求められ、場合によってはクライアント製品だけでは特定の機能的・セキュリティ面での目標達成が困難であることをアドバイスしてきました。

TZ の導入・運用はコストの浪費につながることが多く、セキュリティと安全性を担保しながらコスト削減目標を達成するためには、これらの分野における早い段階からのコンサルティングが極めて重要です。

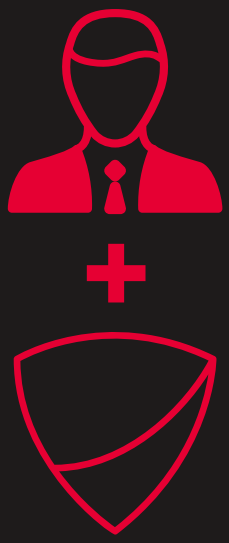
正しい専門知識をもとに TZ テクノロジーを活用すれば、部品の点数が減り、製造コストの大幅な節約が期待できます。

専門分野

- 車両バス（CAN バス、LIN バスなど）
- 小範囲および広範囲 RF プロトコル（RKE、RKI、RDS-TMC、GPS など）
- HSM 導入（CSE、CSE2、SHE、Evita など）
- インフォテインメント接続システム（セルラー、Wi-Fi、Bluetooth、USB など）
- セキュアブート（Freescale/NXP HAB、Intel TEE など）
- アーキテクチャ CPU コア隔離（ARM® TrustZone®、Intel TEE など）
- ベンダー固有セキュリティ／セーフティ／ロックステップコア（Infineon、Freescale/NXP, Atmel）
- 外部暗号化プロセッサ（Infineon smartcards、Atmel cryptochips など）



エフセキュアについて



人＋マシン

高度な攻撃をどのようにして検出しますか？
最先端の分析技術と機械学習技術を活用していますか。

しかしそれだけでは足りません。
攻撃者の立場になって考える必要があります。

エフセキュアのセキュリティ専門家は、
他のどの企業よりも多くヨーロッパのサイバー犯罪現場の捜査に協力しています。

エフセキュアの専門家が、
サイバー攻撃のランドスケープを正確に把握していますので、
常に最新の脅威対策の知見を活用することができます。

エフセキュアは、 1988 年フィンランドで設立されて以来、
サイバーセキュリティのイノベーションを推進しています。

ヘルシンキとクアラルンプールにセキュリティラボを有し、
世界 25 ヶ国のオフィスを通じて 100 ヶ国以上でビジネスを展開しています。

今日のサイバーセキュリティ製品で必需品と考えられている多くの重要なセキュリティ機能は、
当社のヘルシンキのセキュリティラボで開発されたものです。

また、 当社は、 業界の中のビジョナリーとして、
エンタープライズレベルの企業向けサイバーセキュリティ製品とサービスを提供し、
世界中のユーザーの安心を提供しています。

エフセキュアは 1988 年に設立され、 NASDAQ OMX Helsinki Ltd に上場しています。

エフセキュア株式会社
〒105-0004
東京都港区新橋 2-2-9 KDX 新橋ビル 2F
Tel. 03-4578-7710
E-mail: japan@f-secure.co.jp

お問い合わせ先

2019.07 JP 1000

f-secure.com/consulting