製品のセキュリティと完全性に対するフォーティネットの取り組み

フォーティネットのアプローチ

製品設計のライフサイクルの安全性を、設計から製品寿命に至るまでの各段階で確保

製品の初期段階の構想からセキュリティを組み込み

製品開発ライフサイクルのすべての段階、社内外で、堅牢な製品セキュリティ精査を導入

透明性の高いインシデント対応計画に従って迅速な修復を実施

お客様とのパートナーシップによって、透明性のある情報とフィードバックを共有

業界と協力し、すべてのお客様にメリットのある、より強力な標準を開発して実装

当社の取り組み

フォーティネットは、お客様の安全を第一に考え、製品ライフサイクルのあらゆる段階で強固なセキュリティによってお客様を保護し、ポリシーとプロセスの継続的な改善を最も重視しています。

代表的なサイバーセキュリティベンダーとしてのフォーティネットの使命は、人材、デバイス、データをどこでも安全に保護することです。フォーティネットソリューションは 730,000 社以上のお客様に信頼していただいており、導入実績、特許の取得数、検証件数では業界トップを誇ります。フォーティネットは、世界で最もクリティカルな国家レベルのインフラストラクチャの保護の一端を担い、サプライチェーンの堅牢なセキュリティがお客様にとって重要であることを認識しています。当社は、製品の設計、開発、製造、配送、サポートの各プロセスにおいて、製品のセキュリティと完全性を保護するための包括的なアプローチの導入に取り組んでいます。

フォーティネットのセキュアな製品開発ライフサイクルポリシー（SPDLC）

フォーティネットの既存の製品開発プロセスは、「セキュアバイデザイン」と「セキュアバイデフォルト」の原則に則って、製品開発ライフサイクルの全段階で製品のセキュリティを徹底して監査し、構想から製品寿命に至るまで各製品のセキュリティを確保しています。以下のような取り組みを実施しています。

- 独自のネットワーク、コンテンツプロセッサ、SOC（システム オン チップ）アプリケーション固有集積回路（ASIC）を自社開発
- 米国とカナダを中心に研究開発を実施
- NIST SP 800-161 に準拠し、厳密な選択と適格性を確認した製造パートナーとともに信頼性の高いサプライヤープログラムを運用
- セキュアな開発のベストプラクティス（NIST SP 800-53、800-161、および 800-218、EO 14028、英国電気通信セキュリティ法など）に準拠
- 機能を損なう可能性のあるマルウェアおよび / または不正なコンポーネントを防止する技術的な対策の実施
- 脅威のモデル化を採用することで、初期段階からセキュリティを製品に組み込み、深いレベルでの防御を適用してリスク軽減を支援
- 当社の厳格なセキュリティ製品テストを採用しています。これには、当社のビルドプロセスに組み込まれた静的アプリケーションセキュリティテスト（SAST）やソフトウェア構成分析、動的アプリケーションセキュリティテスト（DAST）、脆弱性スキャン、各リリース前のファジングのほか、当社の専任セキュリティ技術者による侵入テストや手動コード監査などのツールと手法を採用しています。
- 独立した第三者機関による侵入テストを定期的に実行
- NIST FIPS 140-2、NIAP Common Criteria NDcPP / EAL4+ など第三者機関の製品品質基準によって検証

フォーティネットの脆弱性開示ポリシー

フォーティネットの製品開発プロセスでは、社内外を問わず、製品開発ライフサイクルのすべての段階で、堅牢な製品セキュリティ精査を導入しています。フォーティネットの製品セキュリティインシデントレスポンスチーム（PSIRT）は、フォーティネット製品のセキュリティ標準の維持管理を担当し、業界でトップクラスの強固な PSIRT プログラムを運用しています。フォーティネットの積極的、透過的、責任ある脆弱性公開を重視する企業文化では、米国のサイバーセキュリティ・インフラセキュリティ庁（CISA）など、政府機関が支持するベストプラクティスを順守しています。これは、お客様を保護する取り組みを実証する当社の数ある方法の 1 つです。

~80%

2023 年に発見されたフォーティネット脆弱性の約 80%が、厳格な監査プロセスによって社内で特定

2023 年に発見されたフォーティネットの脆弱性の約 80% は、当社の厳格な監査プロセスを通じて社内で特定されたものであり、お客様にはこれをご理解いただき安心していただいています。このような積極的アプローチによって、不正なエクスプロイトが発生する前に修正プログラムを開発し、実装することが可能になります。

フォーティネットは、お客様や独立したセキュリティリサーチャー、コンサルタント、同業組織、その他のベンダーと協力し、当社の PSIRT ミッションを遂行しています。このようなコミュニケーションを通じて報告された問題点は適切に処理され、解決されたすべての問題点は、発見場所が社内か社外かにかかわらず、毎月第 2 火曜日に公開の毎月の脆弱性アドバイザリなどで、透明性と責任をもって公表されています。

脆弱性を責任ある透明性を持って開示することで、お客様の資産を効果的に保護するために必要な情報をお客様に提供しています。お客様の保護は当社の最優先事項であり、お客様が組織のセキュリティに関して情報に基づいたリスクベースの意思決定を行えるように支援しています。

責任ある徹底的な透明性の実現

フォーティネットは、セキュリティに対するお客様の意識が高まっており、組織がサプライヤーを選定する際には、自社のネットワークに導入する会社と製品を安心して選択する必要があることを理解しています。フォーティネットは、リスクベースの意思決定に必要な情報を提供するために、透明性を備えた責任ある PSIRT プログラムを運営しています。

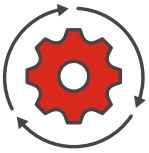
- フォーティネット内部で発見されたすべての問題を含む、公開されている PSIRT ポリシーとアドバイザリ
- 140-2/3、CC EAL4+、CC NDcPP、SOC2 など、独立したさまざまな製品セキュリティ認証
- ソフトウェア部品表（SBOM）の作成など、国家のサイバーセキュリティ向上に関する大統領令の順守

第三者機関の製品の認定については、フォーティネットセキュリティと信頼を参照してください。

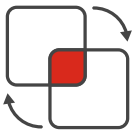
制御機能による減災

即時アップグレードを常に選択できるとは限りませんが、フォーティネットは可能な限り、以下のような補正的な制御機能を提供しています。

仮想パッチ
フォーティネットの管理下にあるデバイスの社外向けインタフェースに仮想パッチを自動的に適用し、アップグレードプロセスを制御しながら、ただちにリスクを軽減



自動アップグレード
ローエンドのシステムには、デフォルトのポリシー設定によるアップグレードを実施し、常に最新パッチへのアップグレードを実行



回避策
構成の変更によって潜在的リスクを減災

ハードウェアとファイルシステムの完全性チェック
BIOS のハードウェア信頼チェーンと FortiSP5 ASIC によるセキュアブート機能

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ