2021

Cybersecurity INSIDERS

アプリケーション セキュリティ レポート

FORTINET®

はじめに

『2021 年アプリケーションセキュリティレポート』は、344 名のサイバーセキュリティの専門家を対象に実施された世界規模の包括的な調査に基づいて作成されました。重要な業務で使用するアプリケーションの数が急増し、DevOps によってアプリケーション更新のペースが加速された現在、組織はさまざまなセキュリティの課題に直面しています。

この調査では、多くの組織が導入と管理が容易なアプリケーションセキュリティのツールとプロセスを必要としていることが確認されました。

調査結果の要点は以下のとおりです。

- 自社のアプリケーションセキュリティについて「信頼できる」または「非常に信頼できる」と回答した組織は 43% と半数を下回り、セキュリティの最大の懸念として多くの企業が（46%）データ保護を挙げました。
- 過去にアプリケーションの感染や侵害を経験した組織は 43% でした。それに対し、3 分の 1 以上（35%）が直近の侵害の時期については「わからない」と回答しています。
- 毎月実施するソフトウェアアップデートの回数は平均で 25 回でした。脅威と脆弱性のテストを頻繁に実施することは重要ですが、コードが変更されるたびにテストを実施していたのはわずか 21% でした。
- Web アプリケーションの保護で組織が直面する障壁としては、スキルのある人材の不足が最多の 46% でした。

この重要なリサーチプロジェクトはフォーティネットの支援のもとで実施されました。

皆様の Web アプリケーション保護の参考としてこのレポートをお役立ていただけたら幸いです。ぜひご一読ください。

Holger Schulze

Holger Schulze

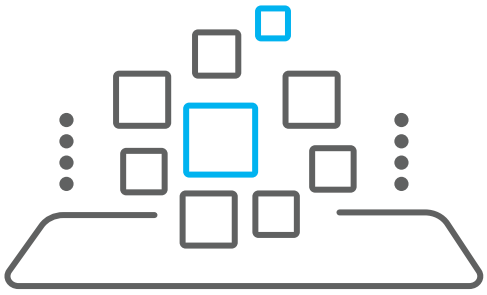
Cybersecurity Insiders 社
CEO 兼創設者

Cybersecurity
INSIDERS

アプリケーションの急増

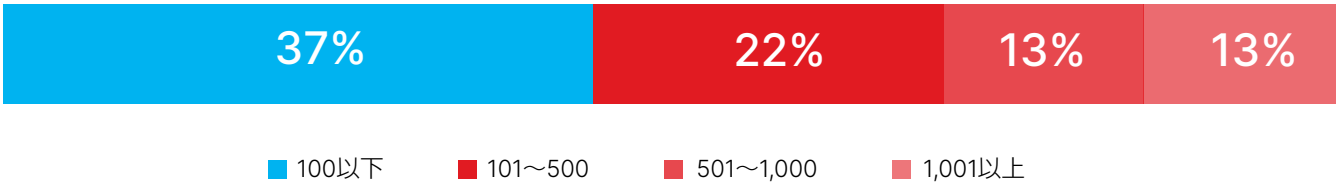
組織のアプリケーションは急速に増加し、調査回答者の半数が 100 種類以上のアプリケーションを導入していました。

▶ 御社では何種類のアプリケーションを導入していますか？



48%

の組織が100種類以上の
アプリケーションを導入*



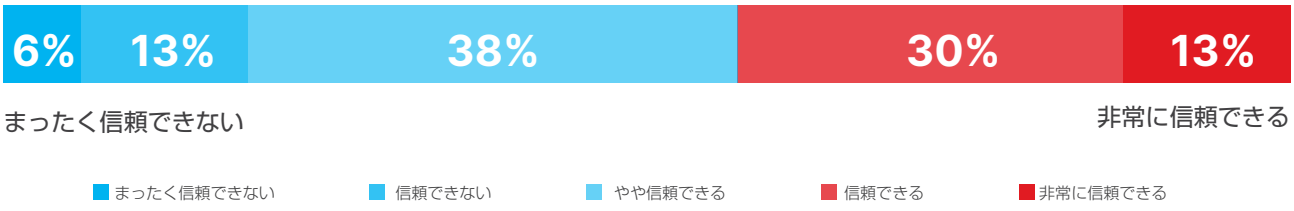
* わからない 15%

アプリケーションセキュリティの信頼性

ビジネスクリティカルな業務のために、機密性の高いデータをアプリケーションで使用する組織は増加しています。自社のアプリケーションセキュリティについて「信頼できる」または「非常に信頼できる」と回答した組織は 43% と半数を下回り、セキュリティの最大の懸念として多くの企業が（46%）データ保護を挙げました。

御社のアプリケーションセキュリティはどのくらい信頼できますか？

43% の組織が自社のセキュリティは信頼できる（「やや信頼できる」から「非常に信頼できる」まで）と回答しています



御社にとってアプリケーションセキュリティの最大の懸念とは何ですか？

46%
データ保護

43%
増加する
脆弱性への対応

39%
開発する
アプリケーションの
保護

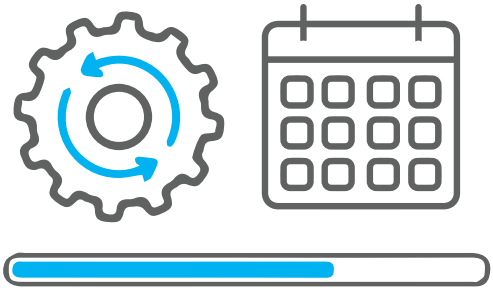
38%
脅威の検知 /
侵害の検知

クラウドアプリケーションの保護 37% | マルウェア 28% | 効果的な脅威モデルの開発 28% | モバイルアプリケーションの保護 26% | 規制 / コンプライアンス要件の遵守 26% | 高リスクの脆弱性の効果的な優先度判定と修正 25% | ビジネスアプリケーション（ERP など）の保護 23% | 顧客のセキュリティニーズと要件への対応 21% | オープンソースソフトウェアの保護 21% | 市販ソフトウェアの保護 17% | エンベデッド / IoT / ハードウェアの保護 17% | ブロックチェーンの保護 6% | わからない / その他 6%

ソフトウェアのアップデート

組織内で毎月実施するソフトウェアアップデートの回数について質問しました。
その結果、毎月平均で約 25 回ソフトウェアアップデートを実施していました。

ソフトウェアアップデートは毎月平均何回実施していますか？

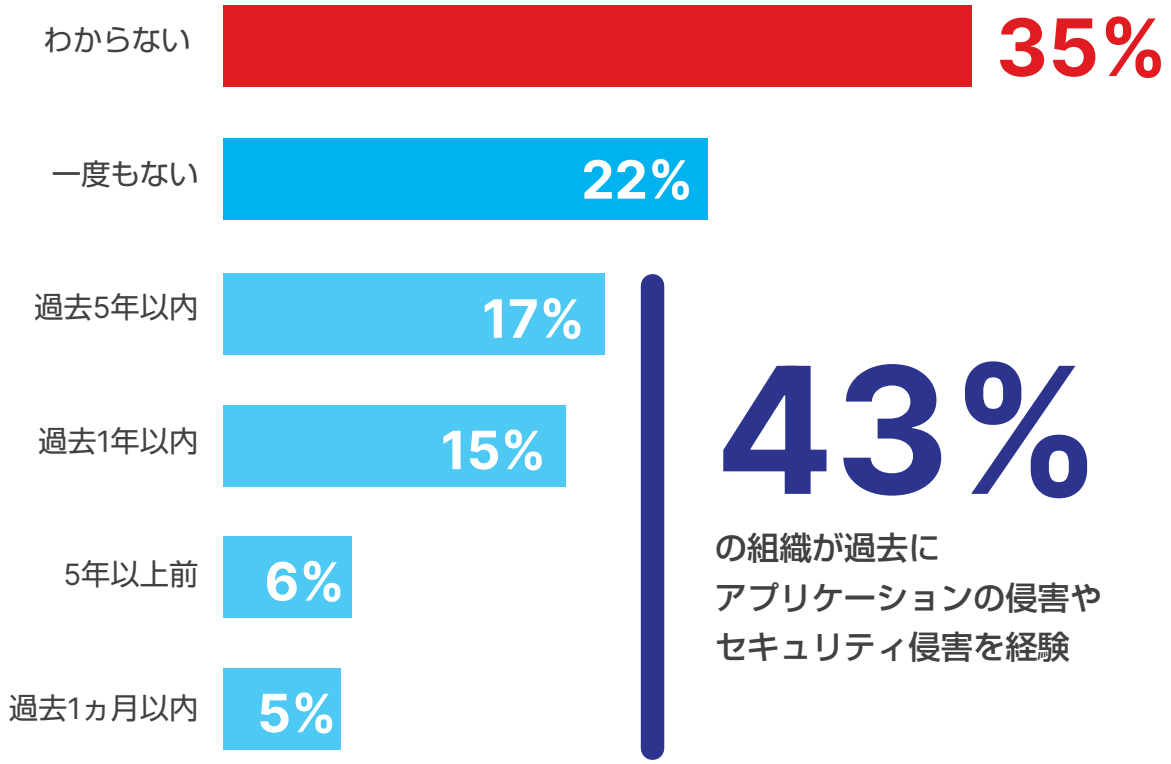


25回 ソフトウェア
アップデートを
毎月実施（平均）

アプリケーションへの侵害

回答者の 43% が過去にアプリケーションへの侵害または攻撃を経験しています。それに対し、3 分の 1 以上（35%）が直近の侵害の時期については「わからない」と回答しています。ただし、これにはツールとプロセスの問題である場合と単に回答者が確認していない場合が含まれます。

御社のアプリケーションが最後に侵害されたのはいつですか？



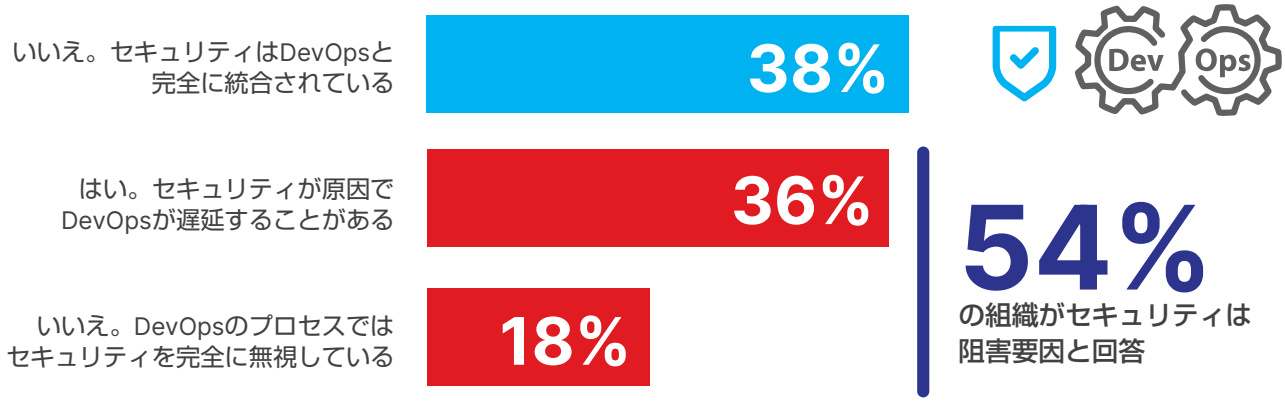
43%

の組織が過去に
アプリケーションの侵害や
セキュリティ侵害を経験

セキュリティと DevOps

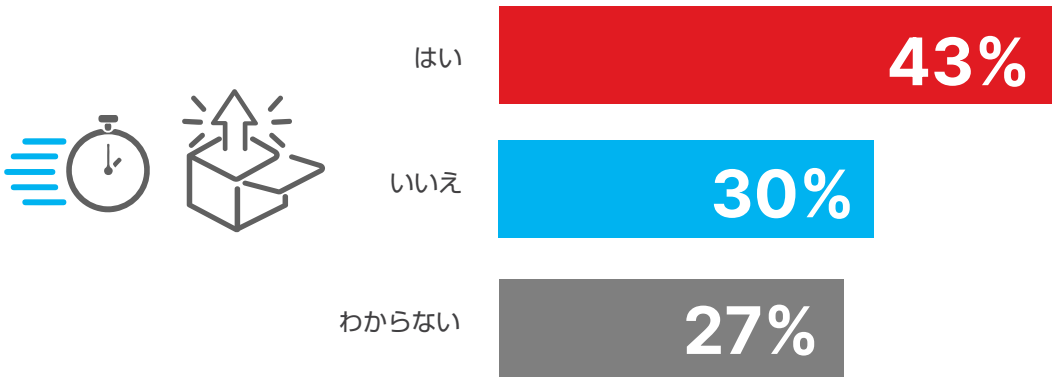
調査結果から、セキュリティチームと開発チームの連携が多くの組織の課題になっていることがわかります。組織の 54% がセキュリティを阻害要因とみなし、43% がアプリケーションを優先するためにセキュリティを犠牲にすることがあると回答しています。

セキュリティが原因で御社の DevOps などの手法による開発が遅延することはありますか？*



* その他 8%

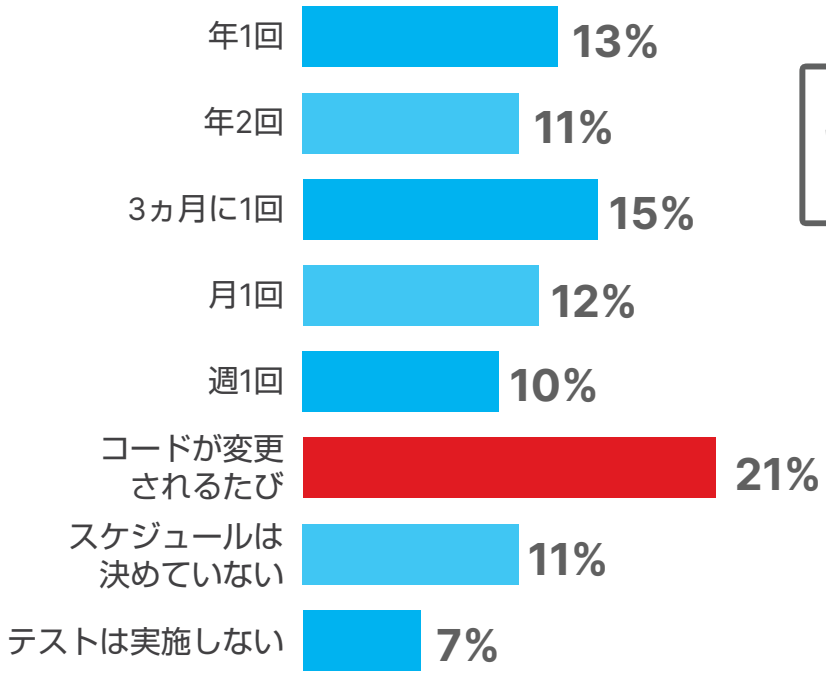
リリースを急ぐために、組織内のアプリケーション開発者が安全なコーディングの手順とプロセスを怠ってしまう事はありますか?

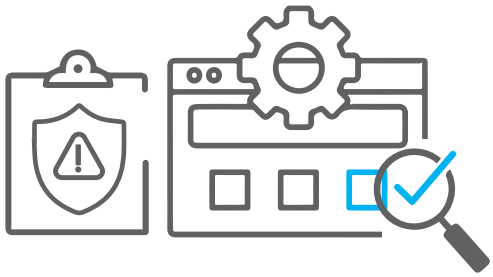


脆弱性のテスト

毎月実施するソフトウェアアップデートの回数は平均で 25 回でした。脅威と脆弱性のテストを頻繁に実施することは重要ですが、コードが変更されるたびにテストを実施している組織はわずか 21% で、多くの組織が自動化したツールやプロセスさえあれば回避できるリスクを放置していました。

どのくらいの頻度でアプリケーションの脅威と脆弱性をテストしていますか？





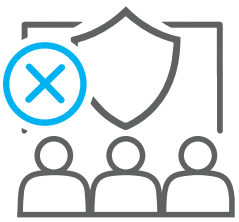
セキュリティの障壁

アプリケーションの保護で組織が直面する障壁としては、スキルのある人材の不足が最多の 46% でした。人材不足はこれまでも障壁になってきましたが、解決には時間がかかるでしょう。人材不足を補うには、これまで手作業に頼っていたセキュリティ関連の作業を自動化するツールやプロセスに投資する必要があります。

サイバー脅威からの防御を妨げる障壁となっているのは以下のどれですか？

46%

スキルのある
人材の不足

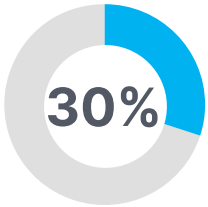


43%

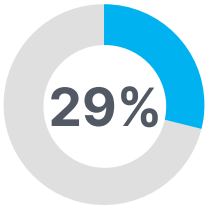
社員の
セキュリティに対する
意識の低さ

39%

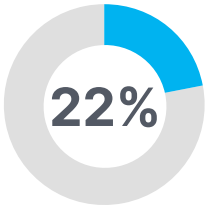
予算の不足



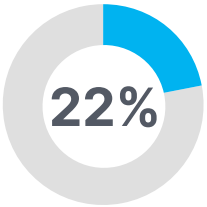
部門間の
コラボレーションの
不足



経営幹部の
支援 / 認識の不足



過剰な
データの分析



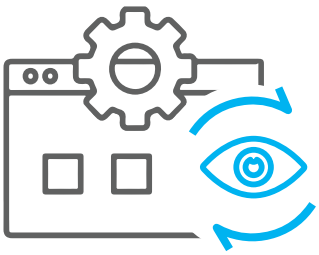
セキュリティ
ソリューションの
不十分な統合 /
相互運用性

リスクに基づいて脆弱性の優先度を判定する機能の不足 21% | 効果的なソリューションへの投資の不足 20% | セキュリティツールからの情況に関する情報の不足 14% | 追加投資の不足 13% | なし 7% | わからない / その他 10%

アプリケーションの監視

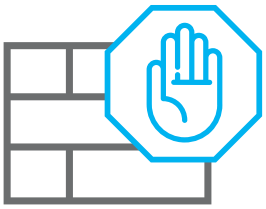
半数の組織（50%）は脅威インテリジェンスを収集して対応するために、アプリケーションを積極的に監視しています。セキュリティの問題を監視する方法はさまざまですが、Web アプリケーションセキュリティとしては Web アプリケーションファイアウォール（WAF）を使用している組織が多く見られました（43%）。

アプリケーションセキュリティの問題はどのように監視していますか？



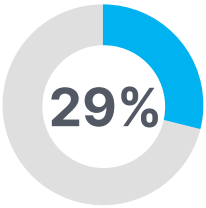
50%

アプリケーションを積極的に
監視して脅威インテリジェンスの
収集 / 脅威に対応している

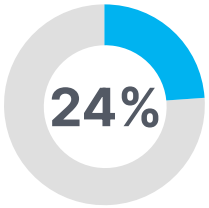


43%

Webアプリケーション
ファイアウォール（WAF）で
アプリケーションを保護している



インシデントや潜在的な脆弱性の情報
を開発チームや設計チームと共有する
フィードバックループがある



アプリケーションの
導入時にコード署名
を使用している

わからない / その他 17% | 上記のいずれでもない 11%

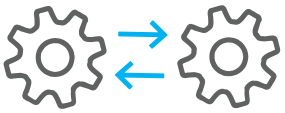
選択の基準

アプリケーションセキュリティソリューションを購入する際の最も重要な基準についての質問では、価格設定という回答が最も多く見られました（54%）。その次が統合の容易さでした（53%）。前述の人材不足を含め、今後もこれらのリソース不足が解消されなければ、セキュリティの強化と効率化のために自動化や WAF などのプラットフォームを導入する組織は増加すると予測されます。

アプリケーションセキュリティのツールやサービスを選択する場合、最も重要な基準は何ですか?

54%

価格 /
ライセンス料

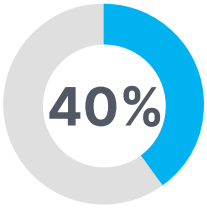


53%

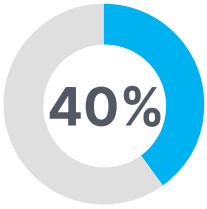
統合の容易さ

42%

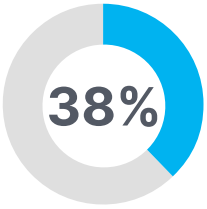
拡張性



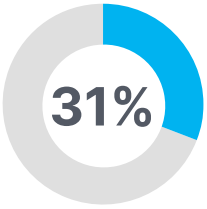
操作の容易さ



正確さ



機能の豊富さ



エンタープライズ
クラスのサポート

信頼性（定評のあるベンダー）29% | 導入から実稼働までにかかる時間 18% | SaaS のオプション 16% | わからない / その他 11%

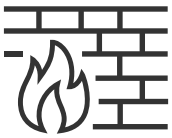
API のワークロード

回答者の 46% は、クラウドベースの WAF などのソリューションを使用してオンプレミスとクラウドの両方を保護しています。ただし、セキュリティソリューションが進化したため、調査に回答したサイバーセキュリティの専門家の 79% がクラウドベースのオプションと、API の保護機能を備えた最新のソリューションを必要としています。これらの最新機能を導入することで、リソースの制約が緩和され、柔軟性が向上するだけでなく、アプリケーション全体の保護も強化されます。

クラウドベースの WAF を使用してオンプレミスとクラウドの両方を保護していますか？

46% がクラウドベースのWAFで
オンプレミスとクラウドを保護

WAF によって API ワークロードを識別して保護することは重要ですか？

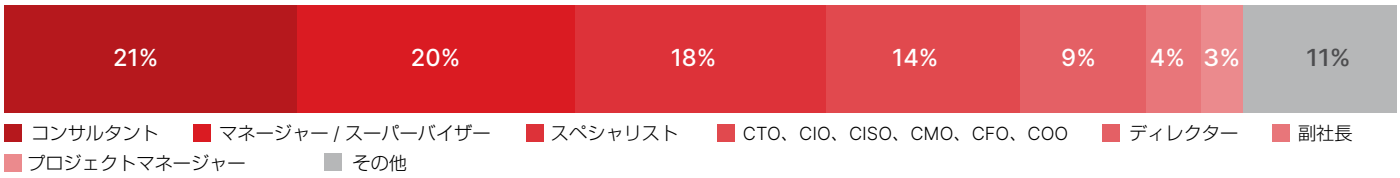


79% の組織がWAFによってAPIワークロードを認識して
保護することは重要であると回答しています

調査の手法と回答者

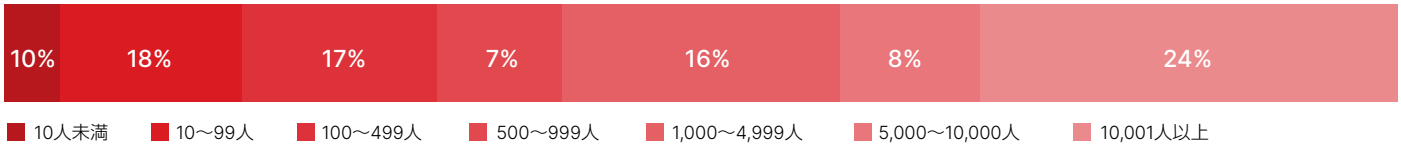
『2021 年アプリケーションセキュリティレポート』はアプリケーションセキュリティの最新の動向、主な課題、ソリューションなどを理解するために、344 人のサイバーセキュリティの専門家を対象に 2021 年 7 月に実施された世界規模の包括的オンライン調査の結果に基づいて作成されました。回答者は技術部門の幹部からマネージャー、IT セキュリティ担当者までと幅広く、業種と規模も多様性を考慮して調整しています。

職位

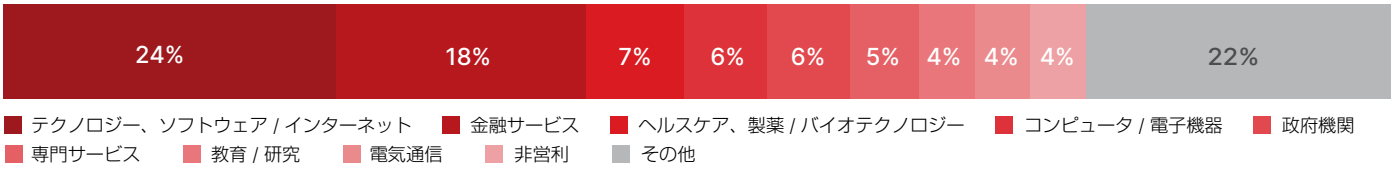


部門

組織の規模



業種



サイバーセキュリティソリューションの世界的リーダーで、幅広い適用領域で（Broad）システム連携し（Integrated）自動化された（Automated）ソリューションを提供するフォーティネット（Fortinet®、NASDAQ: FTNT）は、世界中の大企業、サービスプロバイダー、政府機関を守っています。フォーティネットは、拡大するアタックサーフェス（攻撃対象領域）に対するシームレスな保護とインテリジェンスを提供し、外部との明確な境界が消滅したネットワークでの、増え続けるパフォーマンスの条件に応じるパワーで、現在もまた将来も、お客様に貢献します。ネットワーク上でも、アプリケーションやクラウド、またはモバイル環境であっても、妥協することなく、極めて重大なセキュリティ上の問題に対応するセキュリティを提供できるのはフォーティネットのセキュリティ ファブリックのアーキテクチャだけです。フォーティネットは世界で最も多くのセキュリティアプライアンスを出荷し、世界500,000 以上のお客様がビジネスを守るためにフォーティネットに信頼を寄せています。

www.fortinet.com/jp

フォーティネットジャパン株式会社

〒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

Report-Cybersecurity-Insiders-Application-Security-202110-R1