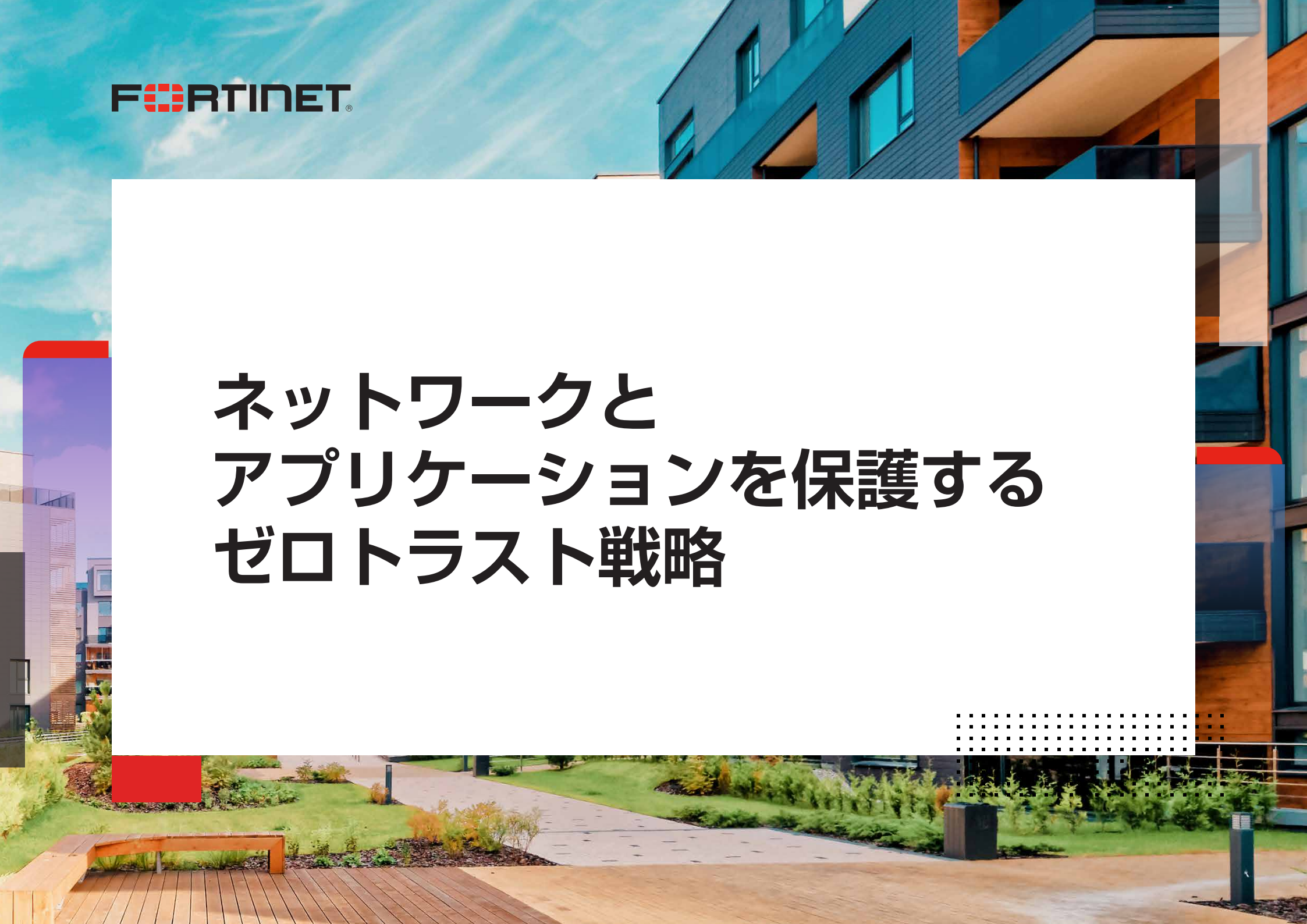

# ネットワークと
# アプリケーションを保護する
# ゼロトラスト戦略

# 目次

# 概要

企業ではデジタルイノベーション、クラウドアプリケーション、テレワークなどのイニシアチブが続けられ、ネットワークはますます複雑化と分散化が進み、「エッジ」の数は増加の一途をたどっています。また、ネットワークに接続するユーザーやデバイスが増え続けているために従来のネットワークの境界は消失し、境界ベースのセキュリティアプローチではもはや十分な保護は提供できません。

何の疑いもなくデバイスやユーザーを信頼してしまうと、企業のデータ、アプリケーション、知的財産が危険にさらされます。CISO はこれまでの信頼を中心に構築したオープンネットワークからゼロトラストモデルへと基本的なパラダイムを移行する必要があります。このゼロトラスト戦略では、デバイス、ユーザー、エンドポイント、クラウド、SaaS（Software-as-a-Service）、インフラストラクチャのすべてが保護されるように、分散したネットワークにまたがる厳密なアクセス制御が必要になります。

フォーティネットは、ネットワークとアプリケーションへのアクセスを求めるすべてのユーザーとデバイスを特定して分類することが可能な、緊密に統合されたセキュリティソリューションを提供しています。

# はじめに

リモートワーカー、マルチクラウドアーキテクチャ、デジタルイノベーションに対応したネットワークへと移行する企業が増えていますが、それに合わせてセキュリティに対するアプローチも変更する必要があります。今日の組織は場所を問わず、さまざまなクラウドサービスや企業のリソースへの安全で信頼できるアクセスを確立する必要があります。

従来のセキュリティモデルは、ネットワーク内のユーザーやデバイスはすべて信頼できるという前提に基づいて機能していました。しかし、デバイスやユーザーを無条件で信頼すると、故意、過失いずれでも、1 台または 1 人が侵害されると組織全体にリスクが及びます。

BYOD（私的デバイスの活用）や IoT（モノのインターネット）の増加によってアクセスポイントとエンドポイントのデバイスが急増し、従来のネットワーク境界は消失しました。エッジのセキュリティチェックポイントを迂回した攻撃者、マルウェア、感染したデバイスは多くの場合、内部のネットワークに自由にアクセスできます。

このゼロトラストアプローチは、固有の信頼に基づいて構築されたオープンネットワークの基本的なパラダイムを、ユーザーやデバイスが信頼できないという前提のセキュリティモデルへと移行させ、ユーザーとデバイスがアクセスを許可されているかどうか検証されていない場合、いかなるトランザクションに対しても信頼を与えることはありません。また、その戦略にはネットワークの内外のユーザーとデバイスを識別、認証、および監視する厳格なネットワークアクセス制御が必要です。

ネットワーク境界内のユーザーでも信頼しないゼロトラストセキュリティモデルに移行した組織はわずか 15% です [1]。

## 効果的な ZTA 戦略の鍵

現在のネットワークには動的なエッジが幅広く分散し、一時的なエッジも珍しくありません。オフラインになるデバイスが多いため、リスクと信頼性を継続的に評価することはますます困難になっています。ネットワークへの接続と切断を繰り返すユーザーやデバイスの信頼性を確認する方法がないため、セキュリティの責任者はネットワーク上のすべてのデバイスを感染している可能性があるものとして対応する必要があります。また、すべてのユーザーが故意、過失いずれでも、重要なリソースにリスクをもたらす可能性があります。

効果的なゼロトラストアクセス（ZTA）戦略では、ユーザーやデバイスは基本的に信頼しないということを前提に、ネットワークへの接続とアプリケーションへのアクセスを処理します。ユーザーやデバイスのアクセス権を確認せずにトランザクションを許可することはありません。ZTA モデルを導入する場合、以下の 3 つの要件に対応している必要があります。

### 1. ネットワーク上のすべてのデバイスを特定できること

アプリケーションとデバイスの増加によってネットワークの境界が拡大し、管理と保護が必要なエッジは数十億に及ぶことさえあります。そのため、NAC（ネットワークアクセス制御）ツールによってネットワーク環境を可視化する必要があります。

### 2. ネットワークにアクセスするすべてのユーザーを特定できること

効果的な ZTA 戦略を策定するには、すべてのユーザーと組織におけるロールを特定することが重要です。ゼロトラストモデルでは、ロールや業務に必要なリソースへのアクセスのみをユーザーに許可する「最小特権アクセスのポリシー」が焦点になります。

### 3. ネットワーク内外の資産を保護できること

効果的な ZTA 戦略ではエンドポイントの可視性を向上させて、オフラインのデバイスも保護します。モバイルデバイスとリモートワークが増加し、ユーザーの不注意によってデバイスや企業のリソースが脅威にさらされる可能性が高まっています。他の接続サービスを利用すると、ウイルスやマルウェアに感染するリスクが増加し、その後に企業のネットワークに接続すると、企業のリソースを感染させるリスクも増加します。

**エンドポイントに対する攻撃の頻度は増加傾向にあり、検知は困難になっています。**
**回答者の 68% が過去 12 ヵ月間で攻撃の頻度が増加したと回答しています [2]。**

# フォーティネットのゼロトラストソリューション

ZTA の導入のためフォーティネットでは、セキュリティソリューションの緊密な統合により、ネットワークとアプリケーションへのアクセスを求めるすべてのユーザーとデバイスを特定して分類できます。また、内部のセキュリティポリシーに対するユーザーとデバイスのコンプライアンスを評価し、自動的に制御対象に割り当ててネットワークの内外で継続的に監視できます。さらに、フォーティネットは、従来の ZTA ネットワークアクセスをアプリケーションごとの利用にまで拡張したゼロトラストネットワークアクセス（ZTNA）も提供しています。これにより、システム管理者は、誰がネットワーク上にいるのかだけでなく、どのアプリケーションを現在使用しているのかまで把握することができ、トランザクションや使用状況が常に監視 / 検査されます。

### 1. エンドポイントのアクセス制御

エンドポイントは多くの場合、最初の侵害や攻撃の標的になります。実際、最近の調査によると、攻撃の 30% はエンドポイントにインストールしたマルウェアを利用しています [3]。フォーティネットは可視化、制御、プロアクティブな防御を組み合わせることによってエンドポイントのセキュリティを強化します。また、エンドポイントのリスクの検出、監視、評価によって、エンドポイントのコンプライアンスを担保し、リスクを軽減すると同時に外部への情報漏洩を抑制します。フォーティネットの FortiClient エンドポイントアクセスソリューションには以下のような特長があります。

- スプリットトンネリングと SASE（Secure Access Service Edge）により、安全性の低いネットワーク接続を暗号化してセキュリティを強化
- デバイスの OS とアプリケーション、既知の脆弱性、パッチ、セキュリティのステータスなど、エンドポイントのセキュリティテレメトリデータを継続的に提供
- セキュアな接続を簡素化する ZTNA リモートアクセスをサポートし、ユーザーやアプリケーションの場所を問わず、アプリケーションへのシームレスなアクセスを実現

## 2. アイデンティティ / アクセス管理

今日の企業のアイデンティティ環境はネットワークデバイス、サーバー、ディレクトリサービス、クラウドアプリケーションなどのさまざまな記録システムで構成されています。これらのシステムに存在するアイデンティティの管理は管理者にとって大きな負担となっており、ユーザー、管理者、アプリケーション開発者にも悪影響が及ぶ可能性があります。また、現在、大規模な被害をもたらしているセキュリティ侵害は、ユーザーアカウントとパスワードの悪用から始まることが多いため、ユーザーに過剰なアクセス権を許可すると被害はますます拡大します。セキュリティ侵害を最小限に抑えるには、すべてのシステムとアプリケーションのアイデンティティの認証を安全かつ効果的に管理することが重要です。フォーティネットのアイデンティティ / アクセス管理（IAM）ソリューションでは以下が可能になります。

- ログイン、多要素認証（MFA）、証明書によってアイデンティティを確立（継続的なコンテキストによる認証も追加可能）
- 認証ソースからのロールベースの情報を特権アクセスに使用
- ロールベースの最小特権アクセスポリシーの開発と適用
- シングルサインオン（SSO）のサポートによるセキュリティ強化、ユーザーのコンプライアンスと利用の促進
- デバイスとユーザーの ZTNA 接続を、個々のアプリケーションでセッションごとに検証

### 3. ネットワークアクセス制御

ネットワークアクセス制御は、今日のように攻撃対象が拡大を続ける情況下でも保護を可能にするゼロトラストネットワークアクセスソリューションです。FortiNAC を使用することで、ポリシーの適用と動的な制御に必要なネットワーク環境の可視化も可能になります。また、ネットワークの内外を問わず侵害されたデバイスや異常なアクティビティにも自動で対応できます。FortiNAC の主な機能は以下のとおりです。

- すべてのデバイスの脆弱性の特定、分析、スキャン
- 継続的なネットワーク制御
- ネットワークアクセスを必要な範囲に制限するポリシーの策定と適用
- 自動レスポンスとネットワークオーケストレーション

### 4. アプリケーションアクセス制御

ゼロトラストモデルではアプリケーションアクセスはセッションごとに制御し、各ユーザーとデバイスの接続がリモートであるか自社のネットワークであるかを確認する必要があります。

また、アプリケーションへのアクセスは個人のロールに関連付けて、ユーザーが必要なアプリケーションのみを使用するようにします。アプリケーションはオンプレミスサーバー、プライベートクラウド、またはパブリッククラウドで提供しますが、ZTA メカニズムを使用して制御します。ZTA はネットワークに対するロールベースのアクセス制御を可能にし、ZTNA はユーザーによるアプリケーションへのアクセスを仲介します。フォーティネットの ZTA ソリューションを使用することにより、アプリケーションアクセス制御は SASE サービス、オンプレミスのアプライアンスや仮想マシン（VM）のファイアウォールなど、さまざまな展開シナリオで利用できます。その主な機能は以下のとおりです。

- 各アプリケーションセッションのユーザーとデバイスの検証
- アプリケーションへのユーザーアクセスのポリシーに基づいた制御
- ユーザーの場所を問わないアプリケーションアクセスポリシーの適用
- ユーザーと ZTNA プロキシポイント間の安全な自動接続の確立
- ファイアウォール、VM ファイアウォール、SASE サービスとの連携

安全性の低い家庭用ネットワークで接続する社員が企業のネットワークにもたらす脅威から保護するには、ゼロトラストモデルなどのより優れたアプローチが必要であることを多くの企業が痛感しています[4]。

## フォーティネット ZTA フレームワークの主なメリット

セキュリティの効果を向上させるには、セキュリティの境界のみに限定した保護から、エッジ、ユーザー、システム、デバイス、重要なアプリケーションに分散しているデータの保護へと移行する必要があります。フォーティネットのプラットフォームでは、デバイス、ユーザー、エンドポイント、クラウド、SaaS、インフラストラクチャに対応した包括的な可視化と保護が提供されます。フォーティネットのゼロトラストソリューションの主なメリットは以下のとおりです。

- アプリケーションやユーザーの場所を問わず、アプリケーションにアクセスするユーザーを完全かつ継続的に制御
- ネットワークに接続しているユーザーおよびデバイスの完全かつ継続的な制御
- オンプレミスでもクラウドでも、ローカルエリアネットワーク、広域ネットワーク、リモートトンネルで同様に機能するフォーティネット セキュリティ ファブリックを活用した ZTA と ZTNA の統合ソリューション
- 1 社のベンダーで実現する完全な統合ソリューション

# まとめ

急速に拡大するネットワークセキュリティ業界で数十年の経験を持つフォーティネットはアプリケーションへのアクセス、ネットワーク上のユーザー、ネットワーク上のデバイス、オフラインのユーザーとデバイスという 4 つの重要な要素の可視化と制御を効果的に実現するゼロトラストソリューションを提供しています。

[1]「2019 Zero Trust Adoption Report」、Cybersecurity Insiders、2019 年 11 月（英語）：https://www.cybersecurity-insiders.com/portfolio/2019-zero-trust-adoption-report/

[2]「The state of endpoint security risk: it's skyrocketing」、Larry Ponemon 著、Ponemon Sullivan Privacy Report、2020 年 5 月（英語）：https://ponemonsullivanreport.com/2020/05/the-state-of-endpoint-security-risk-its-skyrocketing/

[3]「2020 Data Breach Investigations Report」、Verizon、2020 年（英語）：https://www.verizon.com/business/resources/reports/dbir/

[4]「フォーティネットグローバル脅威レポート 2020 年上半期版」、FortiGuard Labs、2020 年 8 月：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ja_jp/TR-20H1.pdf

**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



EB-Zero-Trust-Strategies-202109-R1