Verona

中小企業の
ゼロトラスト戦略

「導入企業の
半分が失敗
する」
とされる
要因と
対策とは？

AMIYA

中小企業の
ゼロトラスト戦略

「導入企業の半分が失敗する」とされる要因と対策とは？

Index

はじめに

テレワークの普及により顕在化されたセキュリティ課題と従来型セキュリティモデルの限界

従来の境界防御型セキュリティに対し、「すべてを信頼しない」セキュリティ対策として注目を集めるゼロトラスト。テレワークやクラウドサービスの普及により、信頼できる領域か否かの「境界」が曖昧となった近年、ゼロトラストの考え方は重要度を増しており、大手企業を中心に、ゼロトラストの思想に沿ったサイバーセキュリティ対策が進んできています。

しかしその一方で、「ゼロトラスト」は概念的で理解しにくいことから、国内で注目されてから4年が経った今も、中堅・中小企業の多くでシフトできていないのが実情です。
サイバー攻撃のターゲットは、機密情報を多数保有する官公庁や大手企業だけではありません。
中堅・中小企業の被害も連日ニュースに取り上げられています。
このように、企業規模に関わらずいかなる企業もセキュリティ対策をおろそかにできない状況ですが、では、予算やリソースの限られている中堅・中小企業が「ゼロトラスト」に取り組むためには、どうしたらよいでのでしょうか。

本資料では、従来の境界防御の延長としてゼロトラストを考えることで、概念的になりがちなゼロトラストの本質を紐解き、中堅・中小企業がゼロトラストに取り組む際に、課題となるポイントと、その対策についてご紹介します。

「ゼロトラスト」誕生の背景

「ゼロトラスト」とは、従来のセキュリティモデルである境界防御型に代わる、新しいセキュリティの考え方です。境界防御型とは、「敵はローカルネットワークの外に存在し、内にはいない」という考え方がベースとなり、主に、インターネットとローカルの境界に対して、FW、UTM、プロキシ、メールセキュリティなどのセキュリティ対策を実施するものでした。対して「ゼロトラスト」は「敵はどこにでもいる」という前提で、インターネットやローカルネットワークを区別せず、「すべての場所でセキュリティ対策を実施するべき」という考え方です。

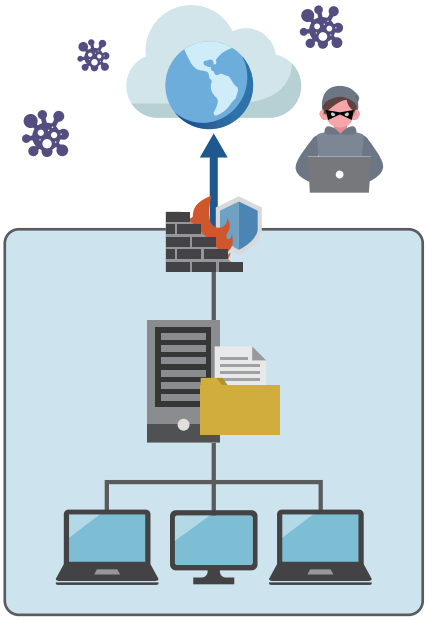
ではなぜ、「ゼロトラスト」という概念は誕生し、注目を集めるようになったのでしょうか？

従来のセキュリティモデル

（境界防御モデル）

「敵は外にいる」という考え方

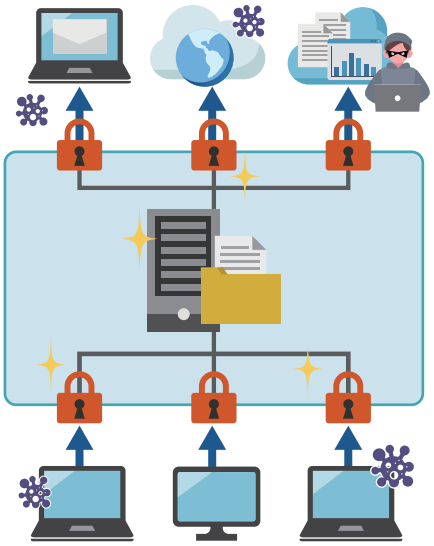
信頼できる部分・できない部分に切り分け、
その「境界」にセキュリティ対策を実施



ゼロトラスト

「敵はどこにもいる」という考え方

誰も、何も信頼せず、全てのアクセスを検証し、
必要なセキュリティ対策を実施



クラウドシフトと働き方の変化

「ゼロトラスト」の考え方が注目される大きな要因として「クラウドシフトと働き方の変化」があげられます。

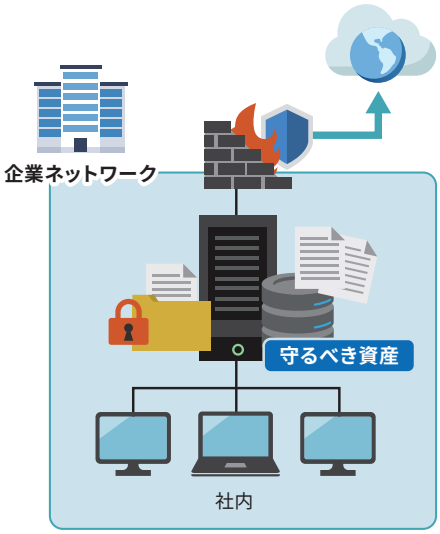
近年、業務システムのクラウド化やテレワークの普及により、私たちの働き方は大きく変化しました。SaaS、PaaS、IaaSなどのクラウド型サービス利用が浸透し、テレワーク用のノートPCやスマートフォンなど、一人当たりが所有するモバイルデバイスも増加しています。

DX推進が叫ばれる中、業務効率化や生産性向上のためにクラウドシフトは欠かせません。しかしその一方で、守るべきデータやデバイスが分散されることによる新たな「セキュリティリスク」が問題視されています。

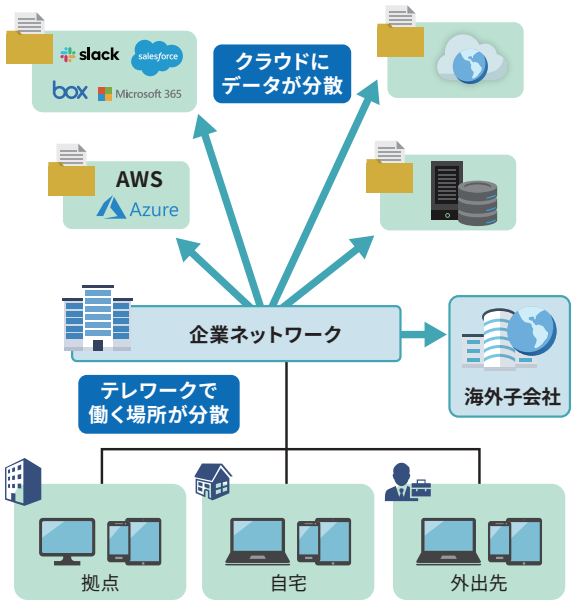
クラウド利用や社外での業務活動が一般的になると、ファイアウォールで隔てていた「社内」と「社外」という境界にのみ対策を集中させていた、従来の境界防御型のセキュリティ対策では不十分となってしまいました。

その結果求められたのが、「内外の区別をせず、アクセスがあったもの全てを信用（トラスト）せずに検証する」というゼロトラストの考え方です。

守るべき資産は企業ネットワーク内に



守るべき資産があちこちに



境界防御型セキュリティの限界と近年のサイバー攻撃

前述した背景をもとに生まれたゼロトラストですが、「企業ネットワークへの侵入を前提とした対策」という観点では、近年の巧妙化したサイバー攻撃に対しても有効です。

サイバー攻撃の代表とされるランサムウェアは、ひと昔前まで、ばらまき型メールや悪意のある Webページから不特定多数に配布するなど「端末」を狙うものでした。感染した端末は暗号化され、端末内に保存されていたデータが使えなくなるという事態になります。しかし裏を返せばそれは、「被害範囲が感染端末に限定される」という状況でした。

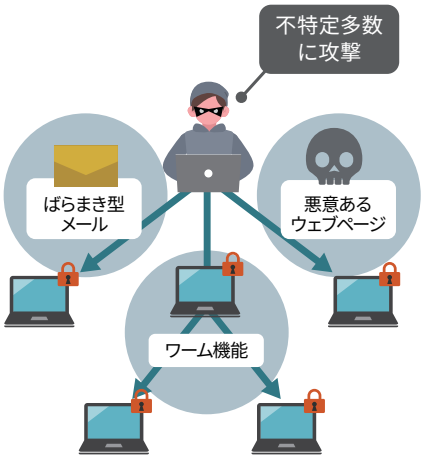
一方、最近のランサムウェアが狙うのは端末だけではなく「企業ネットワーク内のすべて」です。一度ローカルネットワークに侵入されてしまったが最後、Active Directoryなどのドメインコントローラーの奪取を糸口に、グループポリシーを活用して、そのドメイン配下の端末に一斉にランサムウェアを配布・実行させます。結果、ローカルネットワーク内のITシステムの大半が、短時間で一気に暗号化されてしまいます。

従来の境界防御型セキュリティは、あくまで入口のセキュリティ対策です。ローカルネットワークには対策を施していないため、侵入されてしまった場合被害が大きくなる傾向にあります。一方ゼロトラストの考え方であれば、万が一侵入された場合にも二重三重の対策が講じられていることになり、被害を最小限に抑えることができます。

その結果求められたのが、「内外の区別をせず、アクセスがあったもの全てを信用（トラスト）せずに検証する」というゼロトラストの考え方です。

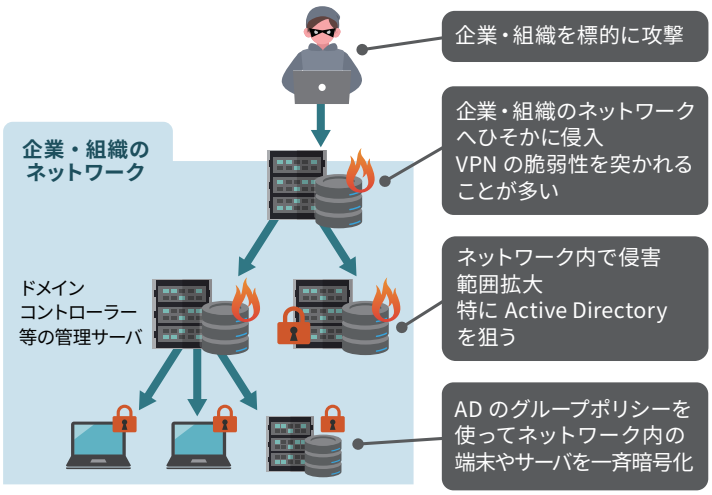
従来のランサムウェア攻撃

被害は感染デバイスのみ。
事業継続リスクとしては限定的。



新たなランサムウェア攻撃

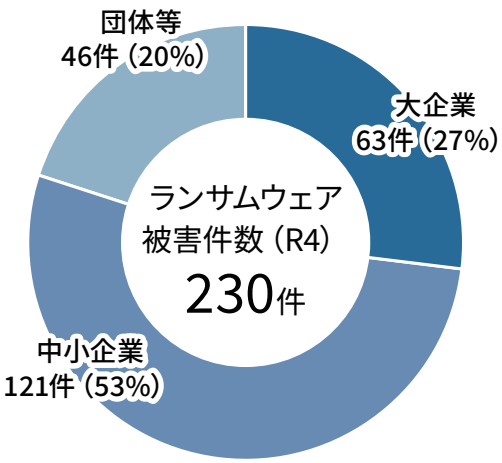
ITシステム全体が停止。
事業継続を揺るがすリスク。



境界防御型セキュリティの限界と近年のサイバー攻撃

企業規模を問わず、被害はより広範囲に

企業規模別 報告件数



ランサムウェア被害の企業・団体等の規模別報告件数
出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」

ランサムウェアの被害事業継続を揺るがすリスク

製造業　2022年9月

サーバーにランサムウェアとみられる不正アクセス攻撃を受けた。調査の結果、従業員情報、取引先の個人情報、株主情報の**約6,000件の個人情報**が外部に漏えい。
さらに部品や海外顧客情報などの機密情報が漏えいした。

輸送業　2022年8月

従業員のPCがランサムウェアに感染していることが発覚。速やかにサーバのネットワークを遮断し、調査を開始した結果、**グループ会社ネットワークへの不正アクセス**が行われたのち、データが**ランサムウェアにより暗号化**されて、使用できない状態になっていた。明確な情報漏えいの有無及びその範囲は判明していない。

サービス業　2022年8月

メールやファイルサーバにアクセスできない障害が発生。社内ネットワークを停止して調査をしたところ、**ランサムウェアによる攻撃**と判明。被害範囲および侵入経路の特定などを調査中。

米NISTによるゼロトラストの考え方

ここまで、ゼロトラストがどういう狙いをもって誕生したかを解説してきました。
ここからはより具体的に、ゼロトラストの考え方について深堀りしていきましょう。

下記は、アメリカのNISTが提唱するゼロトラストの考え方です。7つのポイントで構成されているので、一つずつご紹介します。

1 守るべき資産を把握する
全てのコンピュータとコンピューティングサービスはリソースと見なす

ゼロトラストでは、企業内のすべてのコンピュータやコンピューティングサービスをセキュリティ上のリソースとして扱います。保護すべき資産を把握し、それらのリソースを守るための適切な手段を選択する必要があります。

2 どこでも働けるように
ネットワークの場所に関係なく、全ての通信を保護する

現代のビジネス環境では、外部からのアクセスが必要なケースが増えており、リモートワークが一般的になっています。リモートワークやモバイルワークを含み、全ての通信を保護して初めて、企業は「どこでも働ける環境」を実現することができます。

3 割り振る権限は最小にしよう
企業リソースへのアクセスは、セッション単位で付与する

必要最小限の権限でアクセスを許可することが推奨されます。これにより、サイバー攻撃者がアクセスを得た場合でも、その攻撃者が行える悪意のある行動が最小限に抑えられ、企業に与える被害を低減することができます。

4 人、デバイスがずっと安全だと思わない
リソースへのアクセスは、クライアントID、アプリケーション、要求する資産の状態、その他の行動属性や環境属性を含めた動的ポリシーによって決定する

人やデバイスについて、常に安全であるとは限りません。人は退職時に、機密データを転職先に持っていく危険性があります。
デバイスはマルウェアが仕込まれ、悪意のある行動をするように変化することも考えられます。そのためリソースへのアクセスは、クライアントID、アプリケーション、要求する資産の状態、その他の行動属性や環境属性を含めた動的ポリシーによって決定されるべき、という考え方です。

米NISTによるゼロトラストの考え方

5 運用が大事
企業は、すべての資産の整合性とセキュリティ動作を監視し、測定する

セキュリティポリシーの遵守状況やシステムの脆弱性、不正なアクセスの試行など、さまざまな指標を監視し、リスク管理のための基準を設定します。これにより、セキュリティリスクに対する迅速な対応と、セキュリティの改善に必要なデータの収集が可能に。また、セキュリティの測定は、企業がセキュリティ戦略の成果を測定する上で不可欠な要素であり、常に最新の状態に保つことが重要です。

6 なりすましを疑う
全てのリソースの認証と認可は動的に行われ、アクセスが許可される前に厳格に実施する

アクセスに必要な認証情報を確認し、リソースへのアクセスが許可される前に厳密に認可を行う必要があります。従来のセキュリティ手法では、一度認証されたユーザーがリソースにアクセスできるよう、認証情報を保存する場合がありましたが、ゼロトラストの考え方では、アクセスごとに動的に認証と認可を行うことで、なりすまし（不正アクセス）を防ぎます。

7 終わりはない、常に改善していこう
企業は、資産やネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、それをセキュリティ対策の改善に利用する

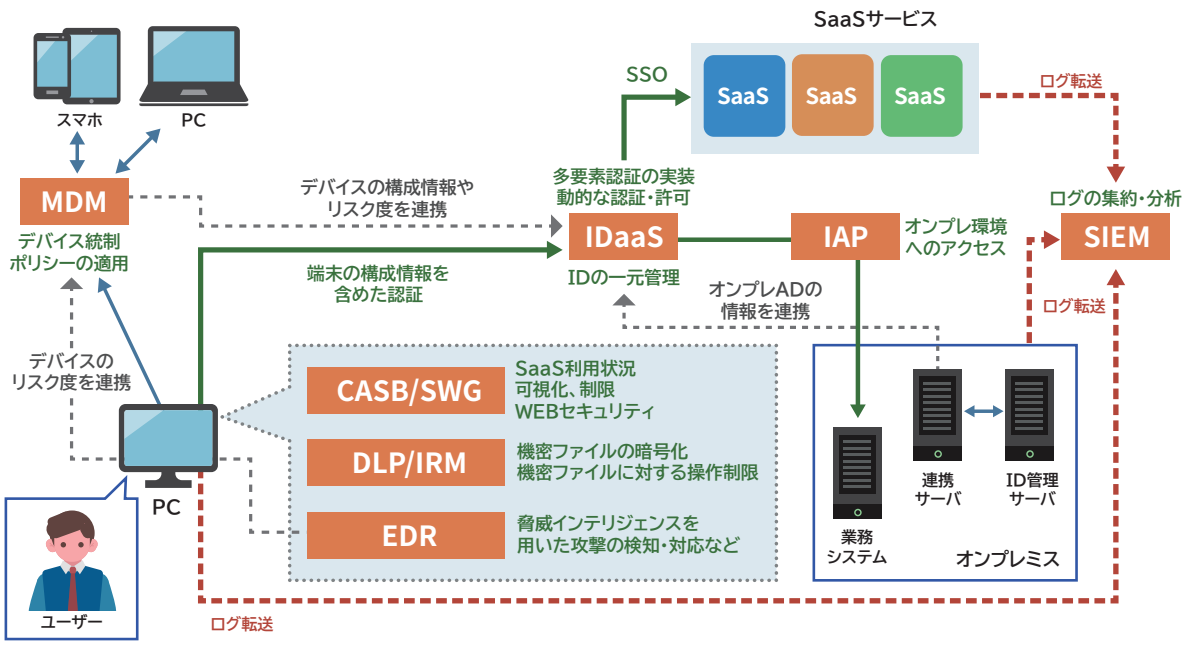
企業がどのようなリソースを持っているかや、どのようなネットワークインフラストラクチャを使っているか、通信にどのようなパターンがあるかなど、可能な限り多くの情報を収集し、その情報を分析した上で、セキュリティ対策を改善していくことが求められます。

以上がゼロトラストの7つのポイントです。
セキュリティ対策は日々進化しているため、企業の状況に応じて、適切な対策を検討する必要があります。

米NISTによるゼロトラストの考え方

ゼロトラストモデル例

グランドデザインを考える上で、参考までにサンプルを一つ挙げます。あくまでも一例であり、この形にしなければならないというわけではありません。こちらはIPAの資料の抜粋です。



IPA「ゼロトラスト移行のすすめ」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002ko3-att/000099778.pdf

まずは左下のPCの部分、ユーザー端末の対策として、CASB（従業員のクラウドサービスの利用を監視し、適切なセキュリティ対策を行うためのソリューション）、DLP（情報漏洩対策）、EDR（利用者端末において脅威を継続的に監視して対応する技術）という各アプリケーションなどの要件に応じたセキュリティ対策を施します。

左上、モバイル端末の管理に関しては、MDM（携帯端末管理）、デバイス管理のソフトウェアを利用。

SaaSサービスなどクラウドへのアクセスにはIDaaSを、またオンプレミスへのアクセスにはIAPを、それぞれ認証管理は、多要素認証でセキュアな状態を確保する構成になっています。

最後にログの管理として、一番右にSIEM（統合ログ管理ツール）を設置しています。各製品・サービスからログを取得、分析することで、インシデント発生時に原因究明ができる環境となっています。

未来予測「5割が失敗するゼロトラスト」

ここまでの話で、ゼロトラストの具体的な考え方と導入にあたっての一例をご紹介しました。

ここで一つ、ゼロトラストについて衝撃的な仮説をご紹介します。

Gartner社が出した「2022〜2023年のサイバーセキュリティに関する8つの主要な仮説」の中の一節で、「2025年までに、組織の60%はゼロトラストを採用するが、その半数以上はメリットを得られず失敗する」と言われています。

それはいったいなぜでしょうか？

Gartner社の仮説

「2025年までに、組織の60%は、セキュリティの
出発点としてゼロトラストを採用する。
しかしその半数以上がゼロトラストのメリットを得られず失敗する」

Gartner「2022~2023年のサイバーセキュリティに関する8つの主要な仮説」
https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20220725

「半分が失敗する」とされる要因は、2つあると考えられます。

1 セキュリティ人材不足

ゼロトラストを導入するに際しては、最初に緻密なグランドデザインを設計する必要があります。この際に一つの壁となるのが、「社内に高度なセキュリティ知識を持った人材」が必要になる点です。

2 リソース不足

もう1つは、リソース不足。先ほどご紹介したモデルの中にもある通り、ゼロトラストを実現するためには、IDaaSやMDMなど複数のセキュリティツールが必要となります。しかしその導入には高額な費用と、緻密な運用が求められます。組織は、これらの課題を克服するために、セキュリティに関する計画的な予算の確保、専門的なサポートの利用、効果的なトレーニングと教育の提供などの方法を検討する必要があります。

以上2つの理由から、予算やリソースが限られる中堅・中小企業は特に、敷居が高いとされています。

ゼロトラストは、

「最初に緻密なグランドデザインを描くことが重要だ」

→ 高度なセキュリティ知識をもった人材が必要

「IDaaS、MDM、CASB/SWG、IAP、DLP、EDR、SIEMが必要だ」

→ ツールの導入費用が高額にさらに緻密な運用が求められる

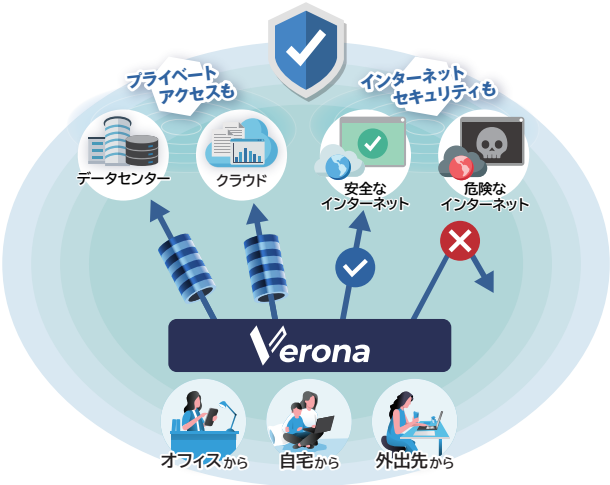
▶▶▶ 中堅・中小企業にはリソース、コスト的に難しい…

中堅・中小企業のゼロトラスト戦略
クラウド型ゼロトラスト「Verona」

中堅・中小企業がゼロトラストに乗り出すためにはまず、前述した2つの課題をクリアする必要があります。それを踏まえた上で、ここからご紹介するのは「セキュリティ人材」と「運用リソース」、両方の不足をカバーするゼロトラストソリューションで、「Verona」です。

働く場所を選ばない、ゼロトラストなネットワークセキュリティを実現

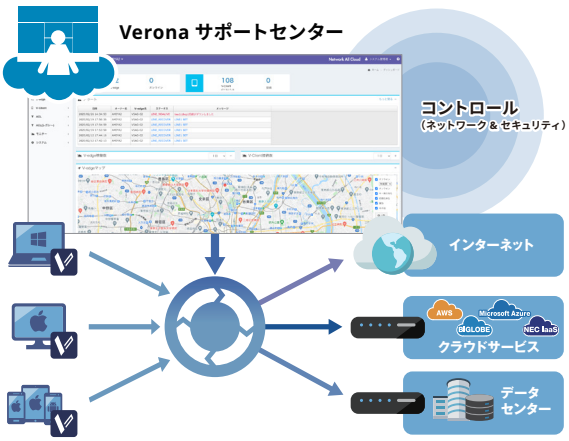
Veronaは安全なプライベートアクセスとインターネットアクセスを提供する、フルマネージドのネットワークサービスです。クラウドシフトにより需要が増えた「自宅からのリモートデスクトップ」や「外出先からMicrosoft 365などのクラウドシステムへアクセス」など、ワンクリックでセキュアに社内環境へアクセス。また、危険なインターネットアクセスをブロックする「DNSセキュリティ」により、インターネットセキュリティにも対応しています。



運用の自動化で「人材不足」と「リソース不足」を解消

「Verona」は機器の提供だけではなく、クライアント端末やVPN機器の設定管理・運用・障害時の対応までを、ネットワークのプロフェッショナルがフルマネージ。専用の管理画面から全拠点の稼働状況や設定が確認できるため、運用に手間がかかりません。

また、ファームウェア更新も自動的に対応するため、サイバー攻撃で狙われるVPN機器の脆弱性も放置されません。ゲートウェイ機器を狙ったサイバー攻撃リスクを最小化します。



安心の運用サービス

01 設定管理

初期設定/追加設定（アドレス変更、ACL設定変更など）

02 運用

アカウント管理（証明書発行/停止）、接続ログの記録/保管、ファームウェアアップデート

03 障害対応/不具合対処

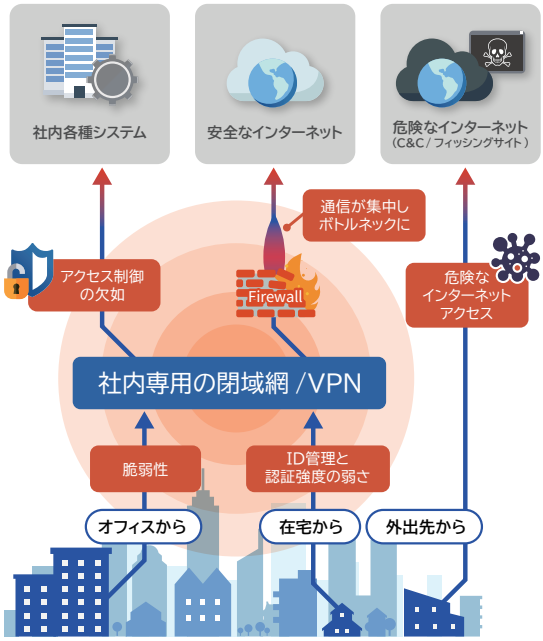
接続/遅延の問題対処、障害切り分け、機器故障時の代替機器送付（先出しセンドバック）
不具合の原因発見と対処、適切な設定指南及び代行

Verona で 解決

テレワーク普及で顕在化した課題

ゼロトラストの考え方が求められた最も大きな要因の一つ「働き方の変化」。
ここからは、テレワークやクラウドシフトによる働き方の変化によって、どんなセキュリティ課題が顕在化したか、そしてその課題に対して「Verona」がどうアプローチするのかを具体的に見ていきましょう。

左側の図は、一般的な境界防御のネットワークモデルです。中央に閉域網やVPNがあり、オフィスや在宅できるネットワークが構築されています。 それを中心に、社内各種システムへのアクセスや、インターネットへのアクセスを行います。



! 脆弱性

担当者不在などの要因により、放置された脆弱性がサイバー攻撃の足掛かりに。

! ID管理と認証強度の弱さ

ITシステムの増加に伴って、増加するID管理コストにより、統一されない認証方法。
IDとパスワードのみという認証強度の弱さから不正侵入被害に。

! 通信が集中しボトルネックに

通信が社内のFWを経由するため、負荷が集中し、遅延が発生。

! アクセス制御の欠如

「VPN接続できれば、ほぼフルアクセス可能」のようにアクセス制御ができていないため、一度侵入を許せば被害が拡大。

! 危険なインターネットアクセス

社外からのインターネットアクセスを制御できず、危険なWebサイトからマルウェアに感染。

このネットワークには、5つの課題があります。それぞれ解説します。

01 脆弱性

担当者不在などの理由で、VPN機器などのシステムの脆弱性が放置され、 そこをサイバー攻撃の足がかりとして利用されています。

02 ID管理と認証強度の弱さ

クラウドサービスなどの増加に伴い、管理すべきIDは急増しています。その結果、管理がしきれず放置されたIDがサイバー攻撃に利用されるという事態に。 また、認証強度にも問題があり、VPN機器のようにインターネットに公開しているシステムに対し、ID/passwordだけの認証では、総当たり攻撃などにより突破されるリスクが存在します。

03 アクセス制御の欠如

境界型防御モデルで構築された社内ネットワークは、侵入されることを前提としていません。 どのネットワークからでも全てのネットワークにアクセスできるようになっているケースがほとんどです。
その結果、一度侵入を許すと、被害は拡大することになります。

04 通信が集中しボトルネックに

社内に設置したUTMを経由することによって、安全なインターネットアクセスを実現できます。しかしテレワークによるWeb会議の増加や、クラウドサービスへのアクセスなど、インターネットへの通信量が増大し、 UTMやFWでの通信ボトルネックによる遅延が頻発するようになりました。

05 危険なインターネットアクセス

04の通信ボトルネックを回避するために、在宅時や外出先からのインターネットアクセスについては「社内のUTMを経由しない」という方法を取るとします。しかしそれでは、インターネットへのアクセスをコントロールできなくなり、場合によっては危険なwebサイトからマルウェアに感染することにつながります。

Verona で 解決

テレワーク普及で顕在化した課題

01

課題

脆弱性対応

サイバー攻撃者が真っ先に狙うのはVPNの脆弱性です。「脆弱性の放置は危険である」というのはセキュリティの基本としてありますが、業務都合や日々の業務に追われ、最新の脆弱性情報のチェックまで手がまわらず、やむを得ず放置されてしまうことが多いです。

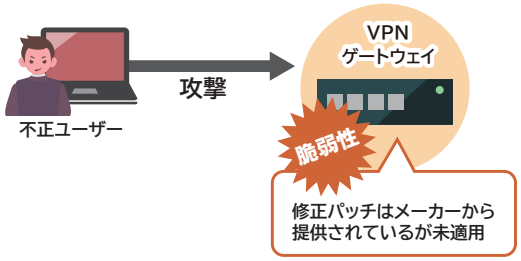
対策

Veronaの自動ファームウェア更新で脆弱性をゼロに

旧来型のVPN機器では、セキュリティ設定を行った後に自動でアップデートがかかるわけではないため、メーカーから提供されるセキュリティパッチを自分でネットワーク機に適用する必要がありました。しかし、多忙を極める情シス担当者にとって、「機器メーカーから発表されるセキュリティ情報（脆弱性の報告）を常にチェックし即座に対応する」というのは、現実的ではありません。
Veronaの場合は、Verona Cloudから自動でファームウェアがアップデートされるため、お客様が意識することなく最新のセキュリティ状態でご利用いただけます。

従来のVPN

世界中からアクセスできるＶＰＮゲートウェイ。
放置された脆弱性からランサムウェアの被害に。

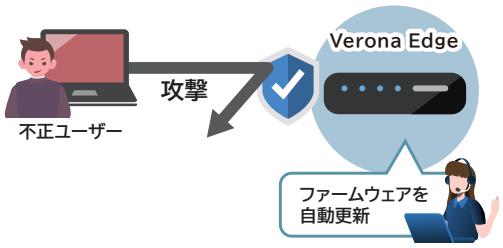


なぜ放置されやすい

- そもそも修正パッチの提供を知らない
- セキュリティパッチを適用する人員がいない
- 担当者が退職してしまった… etc

Verona

ファームウェアの更新も専門のエンジニアが随時対応。
脆弱性が放置されないため、攻撃対象になりにくい。



**定期的なファームウェア更新が
セキュリティ対策の基本中の基本**

Verona で 解決

テレワーク普及で顕在化した課題

02

課題

ID管理と認証強度の弱さ

クラウドサービスなどの増加に伴い、管理すべきIDは急増しています。その結果、管理がしきれず放置されたIDがサイバー攻撃に利用されるという事態に。また、認証強度にも問題があり、VPN機器のようにインターネットに公開しているシステムに対し、ID/passwordだけの認証では、総当たり攻撃などにより突破されるリスクが存在します。

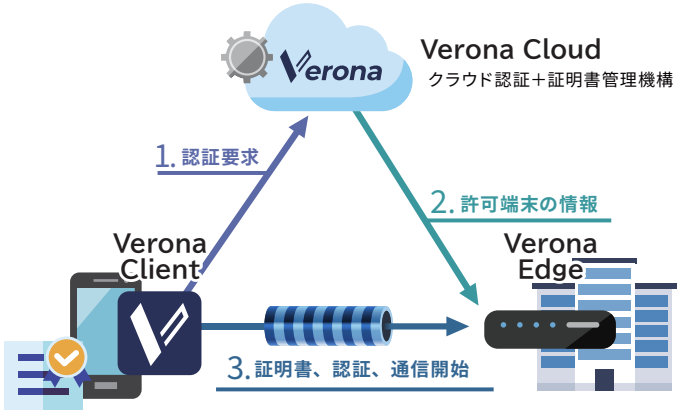
対策

❶ 証明書認証でリスクを最小限に

一般的な機器の場合、ID/パスワードだけの認証のものが多く、なりすましにより侵入される危険性が高いです。
Veronaは証明書認証とパスワード認証を組み合わせた多要素認証での接続を標準搭載。
例えば下記図の上部にある「Verona Cloud」というクラウドコントローラーに、Aさんが「社内の人間として入ってもいいですか」という確認をし、Verona CloudがOKであれば、VPN装置に「今からAさんが入ってくるので、Aさん宛だけにポートを開けて」という動的な指示が出されます。この後、Aさんの端末がVPN装置にトンネルを張り、セキュアな通信が行われます。作業が終わったらポートを閉じて、外から侵入されないようにします。

クライアント証明書認証を標準搭載

脆弱ポイントになりかねないリモートアクセスVPN。
クライアント証明書をベースにした独自の認証システムで
不正アクセスを防止します。



なぜ証明書認証が必要なのか

ID/パスワード認証は世界中から攻撃の標的に。
個人情報や機密情報の漏えい、悪用に繋がるリスクも高い。証明書認証であれば、証明書をインストールしたデバイスのみにアクセスを限定。
攻撃されるリスクを最小限に抑える事が可能。

Verona で 解決

テレワーク普及で顕在化した課題

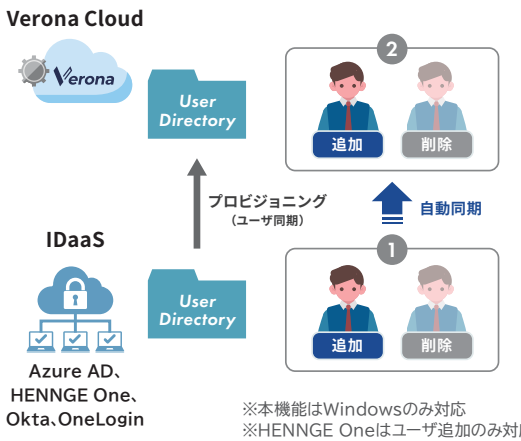
02

❷ IDaaS連携でユーザ管理の効率化と認証強化

ユーザーIDの管理は情シス担当者の手間になりますが、入退職者の管理をおろそかにしてしまうと、退職した方のIDで不正侵入されるなどのリスクが生じます。
Veronaでは、増減するユーザー情報を効率的に管理できます。IDaaS連携機能により、VPN装置のID管理とAzureAD（Microsoft Azureのクラウドベースのユーザー管理サービス）などのID管理を統一することができるため、AzureAD側だけを見ていれば、自動的にVeronaにアカウント連携ができるシングルサインオンが実現できます。

ユーザー情報を同期

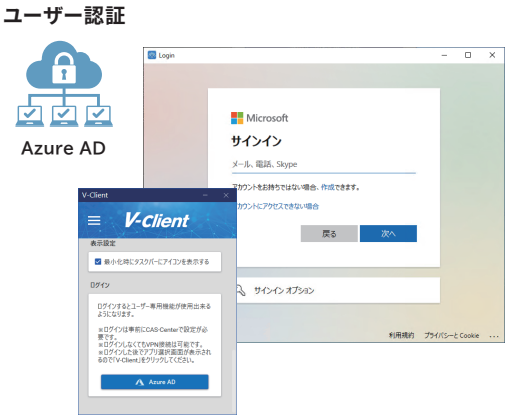
ユーザー管理をIDaaSに一本化。
ユーザー削除忘れによるセキュリティリスクを回避。



※本機能はWindowsのみ対応
※HENNGE Oneはユーザ追加のみ対応

シングルサインオン

IDaaSアカウントでのユーザー認証と
証明書によるデバイス認証で強固な二要素認証を実現。



※本機能はWindowsのみ対応

IDaaS連携で証明書配布をカンタンに！

ユーザ側から証明書配布の申請フローが可能なため、3ステップで、安全かつカンタンに証明書を配布できます。

※管理者による手動承認だけでなく、自動承認も可能

Verona で解決

テレワーク普及で顕在化した課題

03

課題

アクセス制御の欠如

境界型防御モデルで構築された社内ネットワークは、侵入されることを前提としていません。どのネットワークからでも全てのネットワークにアクセスできるようになっているケースがほとんどです。その結果、一度侵入を許すと、被害は拡大することになります。

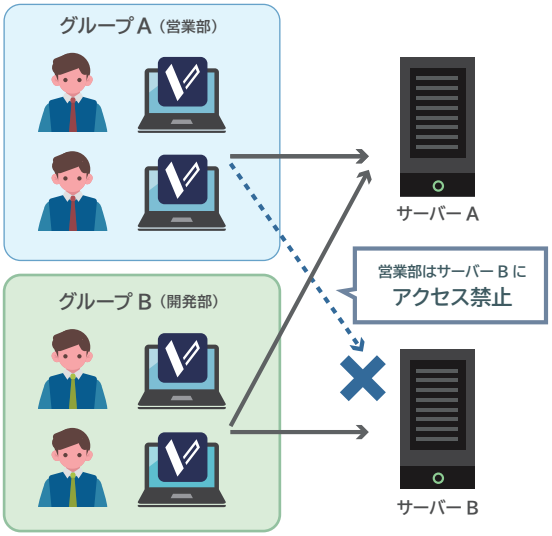
対策

緻密なアクセス制限で被害を最小化

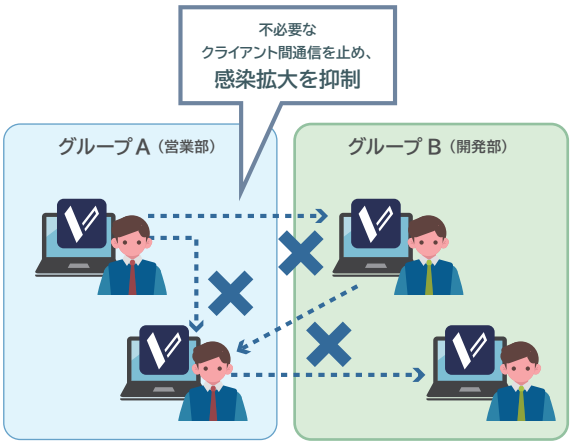
「Verona」なら、細かくアクセス権を設定することで被害を最小限に抑えることができます。例えば、下記の図では営業部と開発部を一例として挙げていますが、相互通信が必要な対象に対してのみアクセス制御を設定しています。

これにより、万が一営業部のメンバーが感染してしまった場合でも、被害は営業部内にとどまり、開発部まで及ぶことはありません。

グルーピング



アクセス制御



Verona で 解決

テレワーク普及で顕在化した課題

04

課題

通信が集中しボトルネックに

社内に設置したUTMを経由することによって、安全なインターネットアクセスを実現することができます。しかし、テレワークによるWeb会議の増加や、クラウドサービスへのアクセスなど、インターネットへの通信量が増大し、UTMやFWでの通信ボトルネックによる遅延が頻発するように。

対策

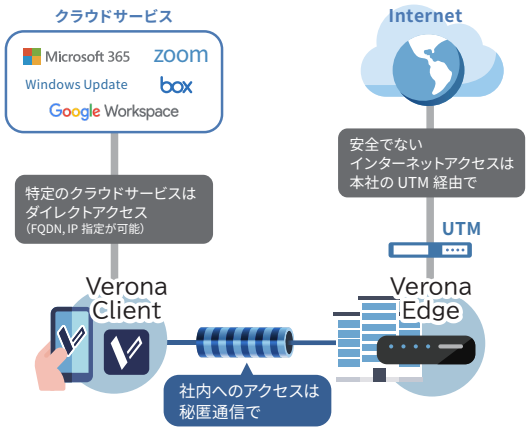
経路選択と負荷分散でボトルネックを解消

「Verona」には、通信負荷の集中を解消する「ローカルブレイクアウト機能」と「ロードバランス機能」が搭載されており、VPN 機器の負荷を軽減・分散することができます。

「ローカルブレイクアウト機能」は、特定のクラウドサービスへダイレクトにアクセスさせることができる機能です。重要データのやりとりなど社内へのアクセスにはVPN通信を行い、オフィス外からのWeb会議やMicrosoft 365などへは直接アクセスさせるなど、使い分けることによりオフィスの回線負荷を軽減します。
「ロードバランス機能」は同時接続台数が多い時に自動でロードバランシングする機能です。Veronaは100名規模から5,000名規模までさまざまな規模の企業に使われておりますが、徐々にスケールアップできる構成となっています。最初から高額な機器を購入する必要はなく、100人や200人ずつ増やしていただくことができます。また、同時接続台数が多い時は、負荷分散が自動で行われる機能も搭載されています。

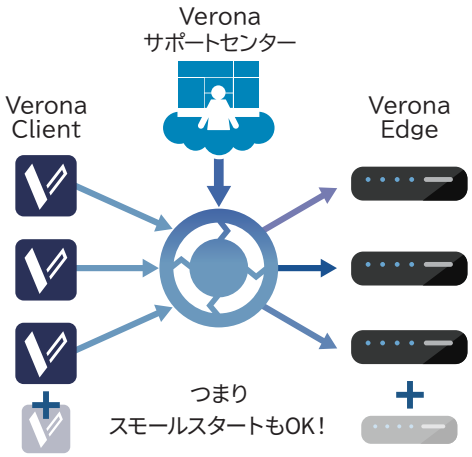
ローカルブレイクアウト

特定のクラウドサービスはダイレクトにアクセスさせることで
オフィスの回線負荷を軽減。



ロードバランス

同時接続台数が多いときは、
接続数に応じて自動的にロードバランシング。
規模の拡大によるスケールアウトが容易です。



Verona で 解決

テレワーク普及で顕在化した課題

05

課題

危険なインターネットアクセス

通信ボトルネックを回避するために、在宅時や外出先からのインターネットアクセスを「社内のUTMを経由させない」という方法を選択した場合、インターネットへのアクセスをコントロールできなくなり、危険なwebサイトからマルウェアに感染する可能性があります。

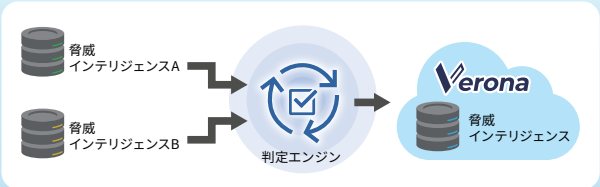
対策

危険なサイトやサーバ情報を蓄積した「脅威インテリジェンス」

「Verona」のDNSセキュリティは独自の脅威インテリジェンスデータベースを保有しており、VPNを使用しない状態でも安全なインターネットアクセスを実現します。
URL単位での綿密なアクセス制御が可能な「プロキシ型」のwebフィルタリングでは、webの通信しかブロックできません。しかし「DNS型」であるVeronaのフィルタリング機能であれば、Webの通信に限らず、あらゆる通信をフィルタリングできるため、ランサムウェアを代表するC&Cサーバを利用した危険な通信など、幅広い悪性の通信を遮断することができるため、サイバー攻撃対策としても有効です。

独自の脅威インテリジェンス

独自エンジンにより収集した200万以上のレピュテーション情報をベースに、独自の脅威インテリジェンスを構築。
迅速なアップデート対応により、既知・未知を意識することなく高精度な検知を実現します。



有害ドメインへのアクセスをブロック

Veronaが選ばれる3つの理由

1 クラウドだから オールインワン

ゲートウェイやクライアントソフト、それをマネージするVerona Cloudを
オールインワンで提供。また、障害対応やテクニカルサポートだけでなく、
初期設定や導入後の設定変更も含む運用サポートも対応します。

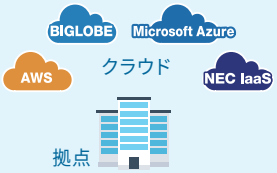
クライアントソフト（Verona Client）

プライベートアクセス、
DNSセキュリティをこれ一つで

＋

プライベートアクセス ゲートウェイ（Verona Edge）

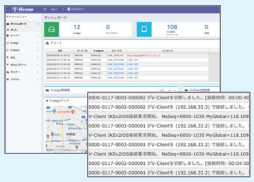
ハードウェア版、ソフトウェア版、
クラウドゲートウェイ版を用意



＋

クラウドコントローラー（Verona Cloud）

クラウドでシステムをフルコントロール。
構築無しで管理画面も利用可能。



運用サポートまで任せられる

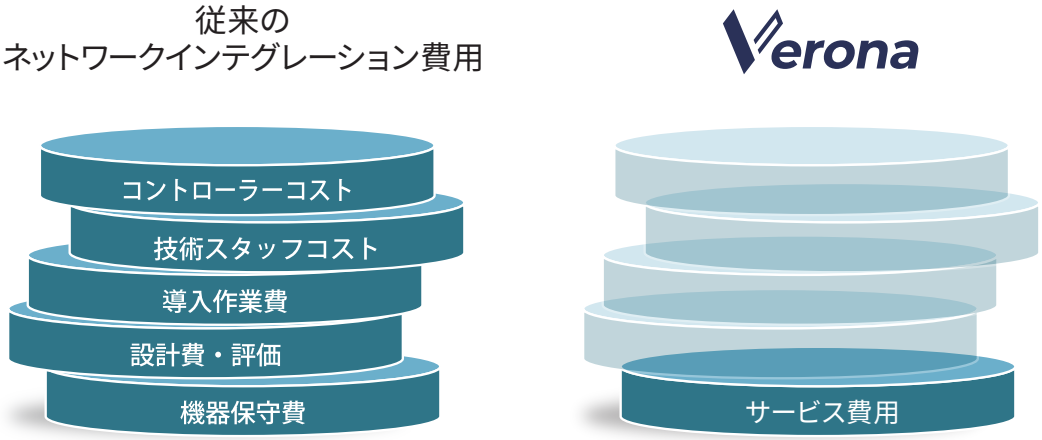
障害対応やテクニカルサポートだけでなく、
初期設定や導入後の設定変更も含む運用サポートまでご提供。

01	設定管理	初期設定/追加設定（アドレス変更、ACL設定変更など）
02	運用	証明書発行/停止、接続ログの記録/保管、ファームウェアアップデート
03	障害対応/不具合対処	接続/遅延の問題対処、障害切り分け、機器故障時の代替機器送付（先出しセンドバック） 不具合の原因発見と対処、適切な設定指南及び代行

Veronaが選ばれる3つの理由

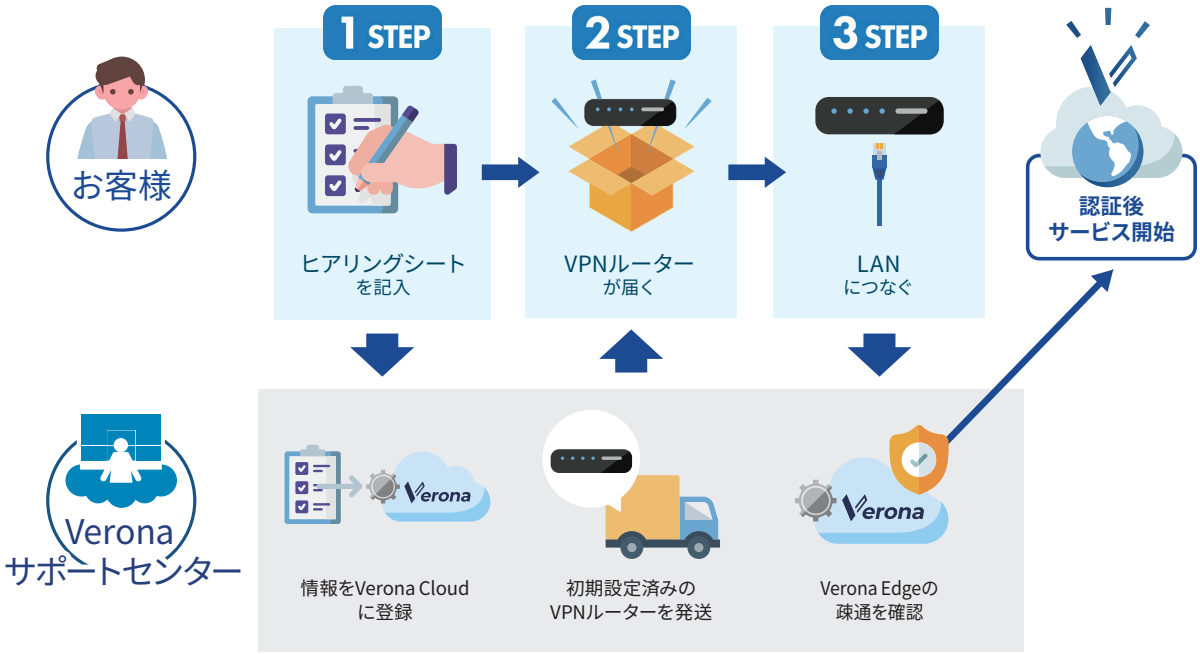
2 圧倒的 コストパフォーマンス

Veronaは、サービス費にすべての費用がインクルードされた価格設定。従来のネットワーク機器購入時に発生していた、「●●は別途請求」という事がありません。

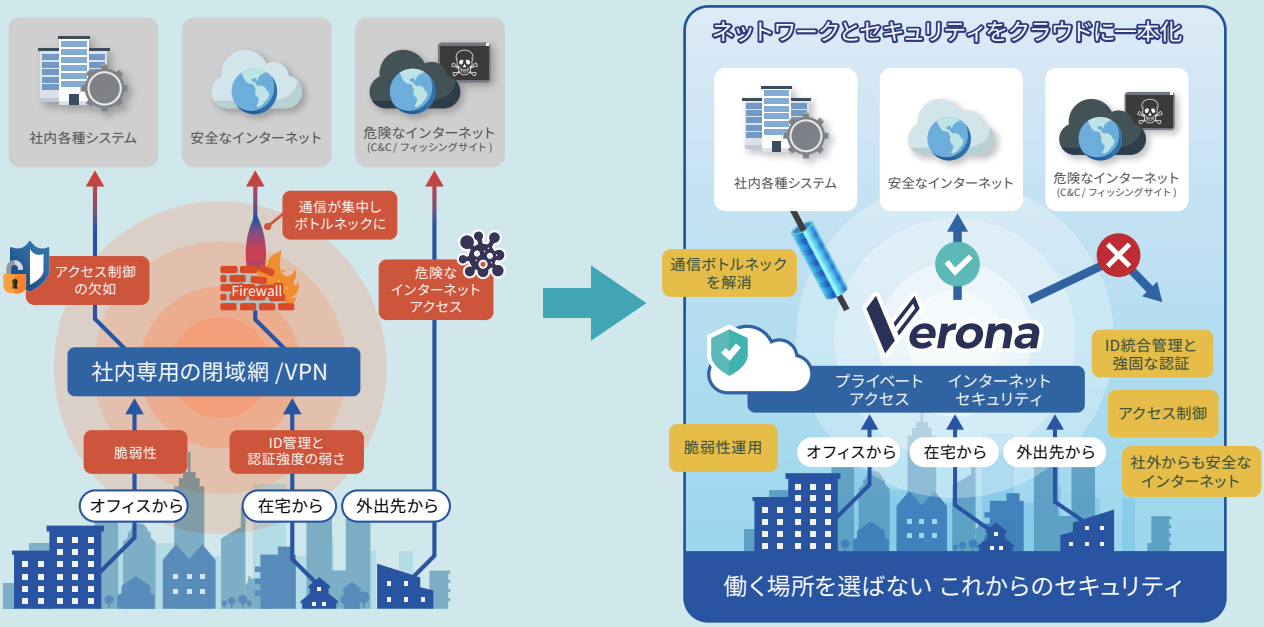


3 導入までの かんたん3ステップ

Veronaは、導入も至って簡単。ヒアリングシートに記入すれば、機器と証明書が届くので、あとは接続・設定するだけで構築が完了します。



ゼロトラストの実現に向けて、Verona という選択



お問い合わせ先

株式会社網屋　ネットワークセキュリティ事業部

TEL **03-6822-9995**　E-mail **infra-sales@amiya.co.jp**

詳しい製品概要資料はこちら ＞

開発元

株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998

https://www.amiya.co.jp/