クラウドゼロトラスト Verona

＼最新！／

ランサム被害事例から学ぶ

ゼロトラストセキュリティ

【Private Access編】

2022年度版

AMIYA

Index

■ **はじめに**

VPNを標的としたランサム被害が拡大中 ・・・・・・・・・・・・・・・・・・・・・・ 2

■ **進化するランサムウェア** ・・ 3

■ **ゼロトラストとは？** ・・・・・・・・・・・・・・・・・・・

はじめに

VPNを標的としたランサム被害が拡大中

原因の多くがVPN!?

徳島県の病院や大手製粉会社、自動車部品会社など、昨今数多くの企業がランサムウェアの被害に合っています。その原因は何でしょうか？実はVPN機器の脆弱性が原因です。
VPN機器の脆弱性により社内ネットワークに侵入され、「LockBit 2.0」などのランサムウェアに感染。その結果、重要なシステムが停止し、事業継続に多大な影響を及ぼしました。

医療ISAC > 医療ISACからのお知らせ > ランサムウェア対策に関する注意喚起

ランサムウェア対策に関する注意喚起

投稿日: 2021-12-02 投稿者: SatoYasuo

既に報道等でご存知とは思いますが、徳島県の公立病院の電子カルテシステムがランサムウェアに感染し、診療が大幅に制限される事態となっております。
また本年５月には大阪府の公立病院にて、遠隔読影システムがランサムウェアに感染し、放射線画像やレポートの閲覧が不可能となる自体が生じています。

上記の２事例に共通する点として、米国Fortinet 製 Virtual Private Network(VPN)装置の脆弱性(CVE-2018-13379)からマルウエアの侵入を許した可能性が高いと報道されており、また、データのバックアップがオンラインのみであったため、バックアップデータまで暗号化されてしまった結果、復旧が非常に困難になったという状況が推定されています。

これらの事情を鑑み、医療ISACとしては一般的なサイバーセキュリティ対策に加え、以下の提言を行いますのでご参考にしていただけると幸いです。

（図1）一般社団法人 医療ISAC HP「ランサムウェア対策に関する注意喚起」　https://www.m-isac.jp/2021/12/02/recommend01/

そこで本ホワイトペーパーでは、VPNを経由したランサムウェアの特徴を解説するとともに、昨今注目のゼロトラストの概念で、プライベート（リモート）アクセスに必要なセキュリティポイントを解説していきたいと思います。

進化するランサムウェア

なぜ事業継続を揺るがすほどの被害に？

ランサムウェアの進化が要因

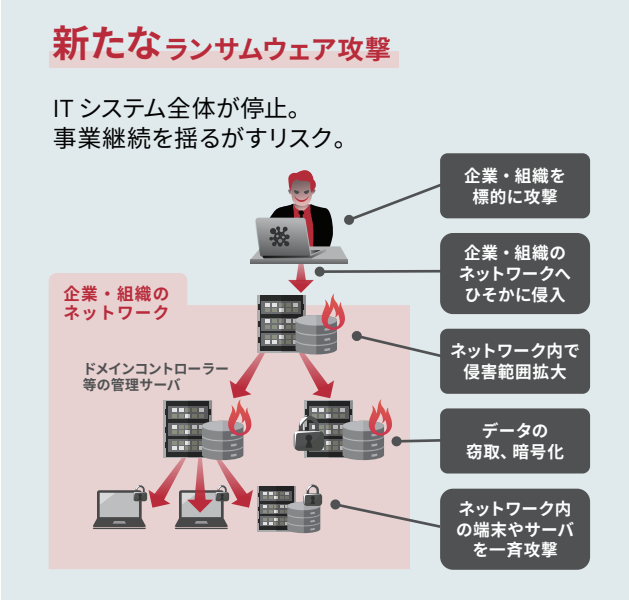
これまでもランサムウェア被害によりファイルサーバが暗号化され、事業に影響を与える事件は数多く発生していましたが、最近はその被害が事業が停止するまでに深刻化してしまっています。その要因は、ランサムウェアの進化が関係しています。

従来のランサムウェアは、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されたランサムウェアに感染させていました。こうして感染させられた端末は暗号化され、その中のデータが使えなくなる事態に。しかし逆にいうと、被害範囲は感染端末だけでした。

もちろん、ワーム機能のように感染が横展開されることもありますが、その端末をすぐにネットワークから切り離しさえできれば、そのリスクはそこまで強くはありませんでした。

一方、新たなランサムウェアの特徴です。企業ネットワークに手動で侵入したのち、Active　Directoryなどのドメインコントローラーを狙います。そして、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、ITシステムの大半が短時間で一気に暗号化。対処する暇もなく、事業継続に多大な被害を及ぼすほどの被害を受けてしまうのです。

進化するランサムウェア攻撃



企業ネットワークへの侵入経路として、VPNの脆弱性を利用

新たなランサムウェア攻撃、それは企業ネットワークへ不正侵入するところからスタートします。そして、その侵入経路に冒頭でご紹介したVPNの脆弱性が利用されるケースが多いわけです。VPN装置は言わば内部ネットワークと外部との境界線なわけですから、社内ネットワークへのアクセスポイントであるVPN機器は特に注意してセキュリティ対策を行う必要があるといえます。
そこで、ゼロトラストをキーワードにプライベートアクセスはどうあるべきなのか、次ページより解説していきます。

と、その前に…

What is Zero-Trust？

テレワークの普及に伴い、様々な環境からでも働く事ができるようになった今、これまでの“内”と“外”とを区別する事で成り立っていた境界型モデルの対策では十分なセキュリティ機能を果たせなくなりつつあります。
そこで注目を集めているのが、“すべてを信頼しない”という前提のもと対策を講じる『ゼロトラスト』の概念。NIST（米国国立標準技術研究所）発表の、ゼロトラスト・アーキテクチャによるとその概念は次のように記されています。

ゼロトラストは、
ネットワークが侵害されている場合であっても、
情報システムやサービスにおいて、
各リクエストを正確かつ最小の権限となるように
アクセス判断する際の不確実性を最小化するために
設計された概念とアイデアの集合体のことである。

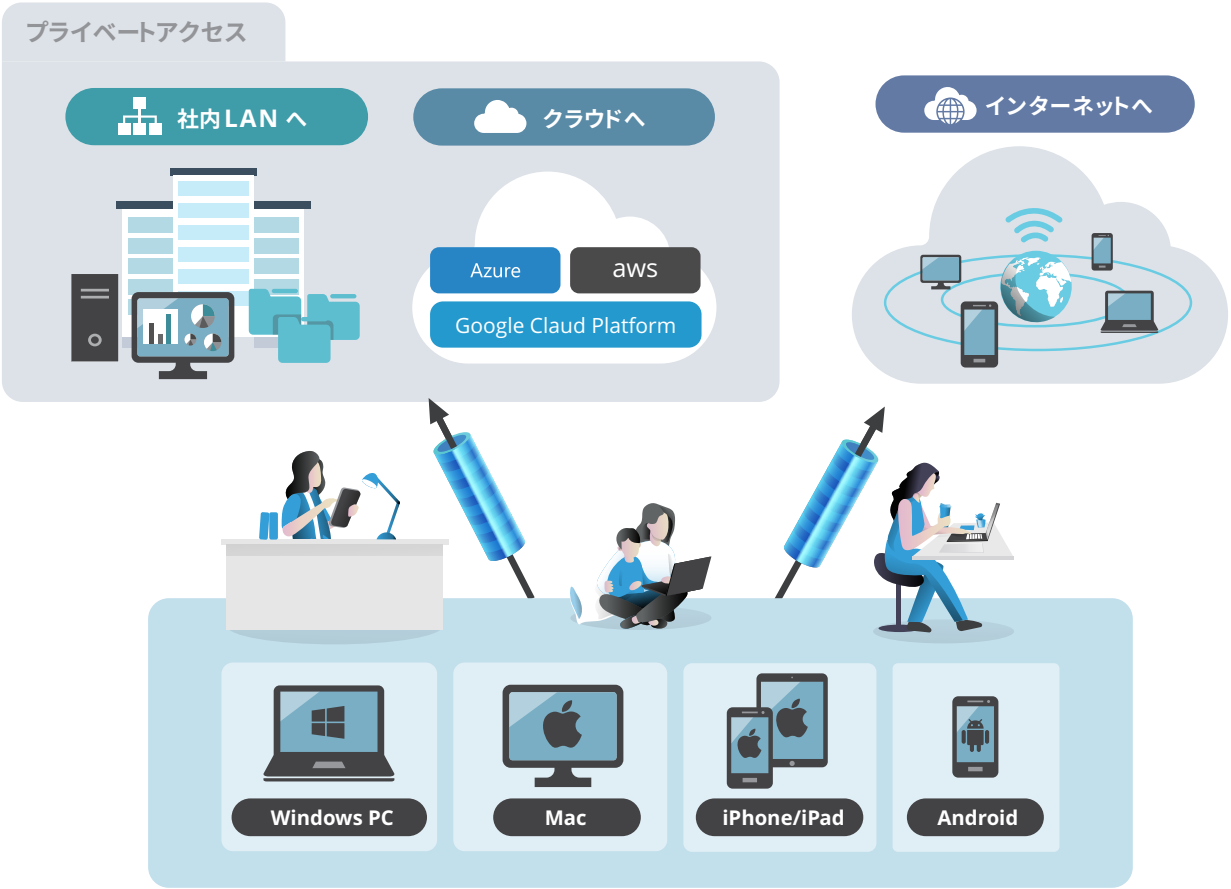
※NIST SP800-207（日本語訳）より抜粋

NIST 「ゼロトラストの原則」

1. すべてのデータソースとコンピューティングサービスをリソースとみなす
2. ネットワークの場所に関係なく、すべての通信を保護する
3. 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
4. リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、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り決定する
5. 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
6. すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する
7. 資産、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、
8. セキュリティ態勢の改善に利用する

※NIST SP800-207（日本語訳）より抜粋

このゼロトラストの概念をかみ砕いて具体的に考えてみると、“ゼロトラスト”なネットワーク環境を構築するにあたり、肝となるのはずばり2経路。プライベートアクセスとインターネットアクセスです。



そして、今回のテーマであるプライベートアクセスにフォーカスしてゼロトラスト実現の為のポイントをまとめたものがこちら。

ゼロトラストなプライベートアクセスを実現する
4つのポイント

Point1 ユーザーの一元管理

Point2 認証の強化

Point3 マイクロセグメンテーション（権限の最小化）

Point4 脆弱性管理

次頁からはこの4つのポイントを、具体的にご紹介していきます。

ゼロトラストなプライベートアクセスへ

Point1 ユーザーの一元管理

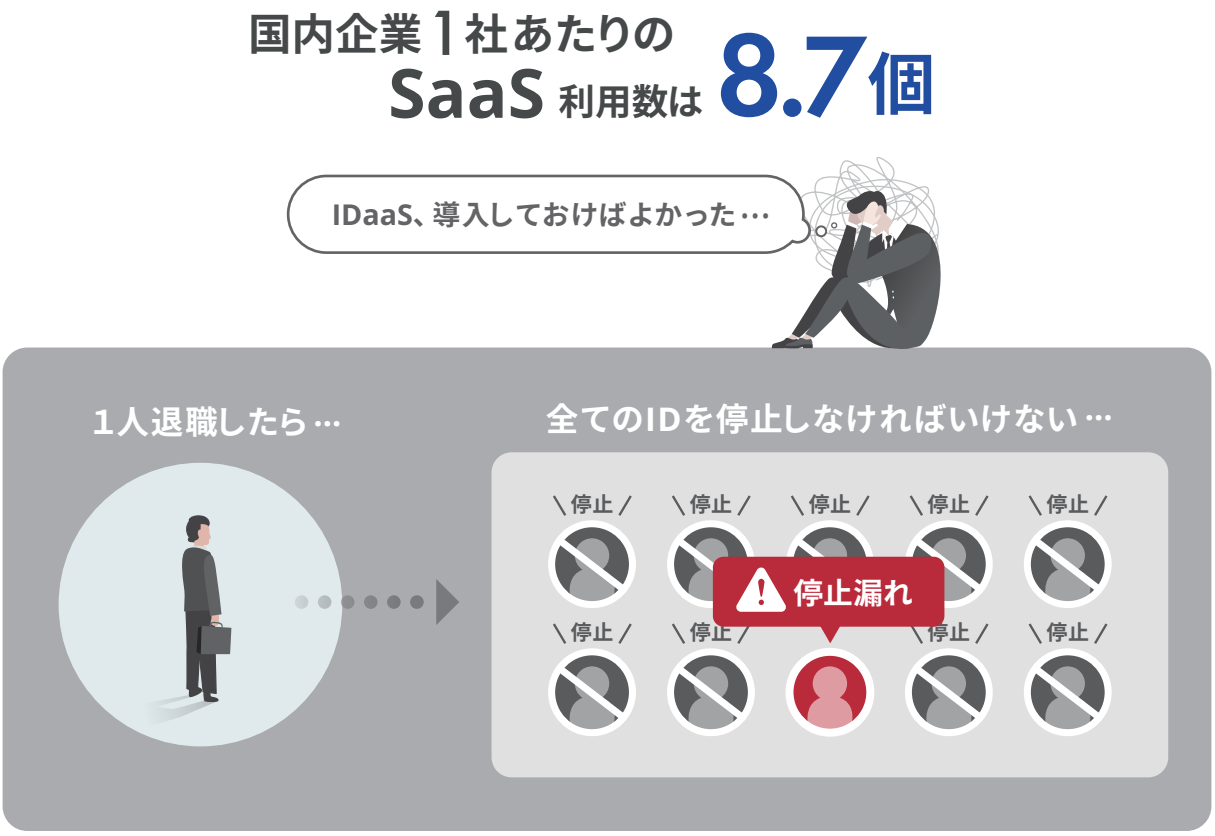
昨今の多様な働き方を実現する理由の一つとしてあげられるのが、サービスとしてのソフトウェア(SaaS)の普及。
インターネット環境さえあればどこからでもサービスを利用できるので、非常に便利です。しかしその便利さの反面、課題となっているのがプラットフォームへログインする時の認証として使用されているIDの管理問題。

SaaSサービスのみならず、ID/パスワード情報の取扱いは、セキュリティの観点からみて当然、十分に注意する必要があります。しかし、先日とある企業が発表した調査結果(※)によると、2020年の国内企業1社あたりのSaaSサービス利用数は8.7個だったそうです。

つまり、単純に考えて1企業当たり従業員数×8.7個のアカウント管理が必要な時代になってしまったという事。

これだけ多くのIDを抜け漏れ無く管理するのは大変な作業ですから、一元的な管理を実現するIDaaS(Identity as a Service)の活用をお勧めします。

（※）メタップス：「コロナ期のSaaS導入変化でふり返る2020年」SaaS利用実態調査レポートより
https://www.metapscloud.com/report_20201229.html



人の管理は抜け漏れが生じる、前提で…
ID管理は、IDaaSで一元管理すべし

ゼロトラストなプライベートアクセスへ

Point2 認証の強化

続いて二つ目のポイントとなるのが認証の強化です。IDaaSを活用しID管理も徹底した上で、万が一認証情報が情報が漏えいしても、第二・第三の防御壁となるよう、複数認証システムを使用することをお勧めします。

認証システム例

知識認証	所有物認証	生体認証
本人だけが知る知識	**本人の所有物**	**本人の身体的特徴**
ex: パスワード、PINコード	ex: クライアント証明書、スマホのSMS、ワンタイムパスワード	ex: 指紋、顔、静脈、虹彩

認証情報は流出する、前提で... 複数認証システムを採用すべし

様々な認証システム、何がおすすめ?

お勧めはデバイス認証の併用です。　セキュリティの手薄な私物端末を踏み台とした攻撃も、内部犯行による情報漏えいも防ぐことが可能です。

しかしここで問題が・・・
多要素認証によるセキュリティ強化の重要性は理解いただけたと思いますが、認証システムを増やせば増やすほどその運用は複雑になっていくもの。そのうえ認証システム用のサーバを別途構築する必要もあり、労力だけでなく コストも嵩みます。

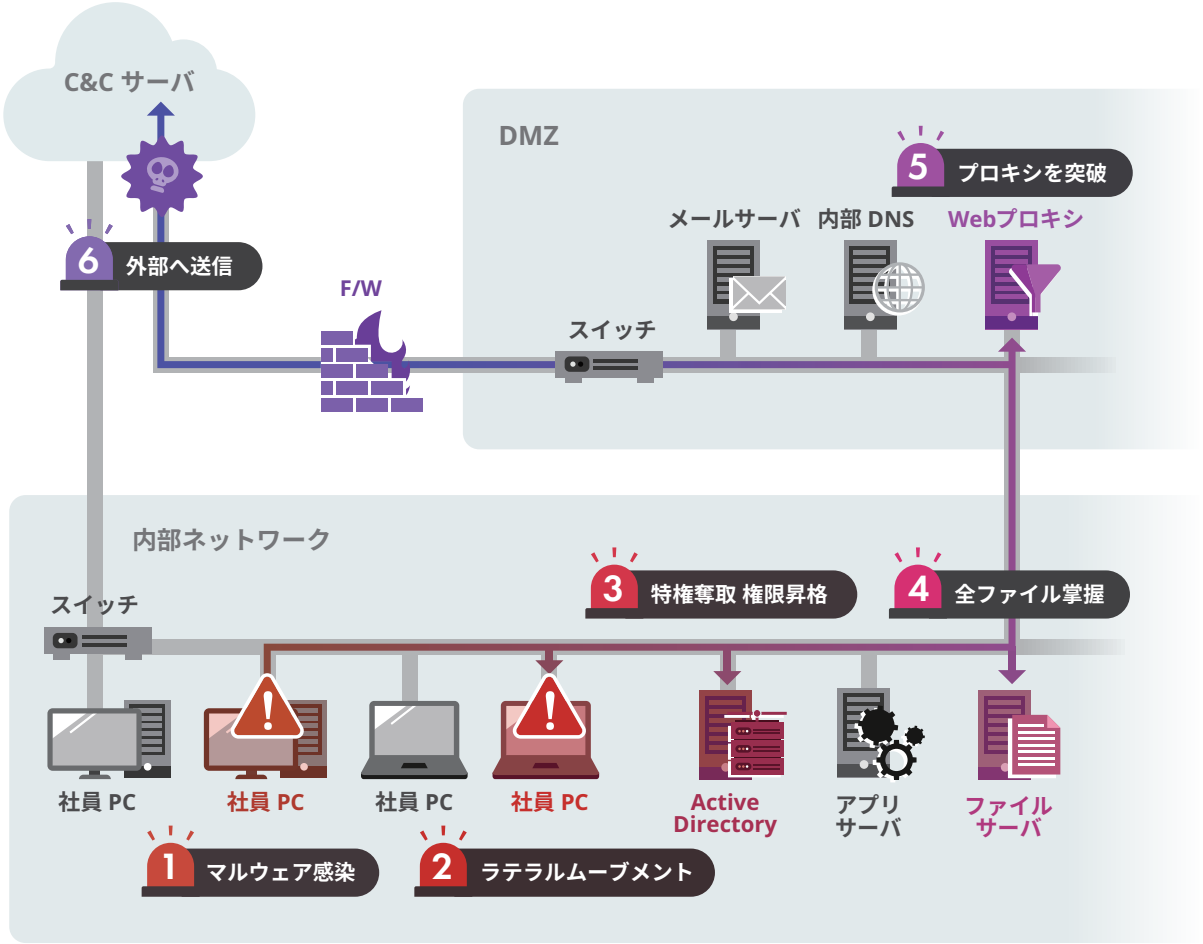
→ 多要素認証導入は、運用・コストが課題

ゼロトラストなプライベートアクセスへ

Point3 マイクロセグメンテーション（権限の最小化）

そして3つ目のポイントがこちら。
マイクロセグメンテーション（権限の最小化）です。下の図は、一般的な攻撃者の侵入後のパターンを図式化したもの。マルウェア感染に成功すると、攻撃者はラテラルムーブメントといって水平方向への移動を開始し、内部の偵察やより強い権限をもつアカウントの捜索を開始します。つまり万が一社内ネットワークへ侵入されたとしても、マイクロセグメンテーションで権限を必要最低限にしておけば、この水平方向の攻撃を最小限に抑えることが可能となります。

攻撃者のパターン



必要な通信のみを許可する、特に同一のセグメント間通信に注意

侵入は成功し横展開される、前提で…
権限を最小化。必要な通信だけ解放すべし

ゼロトラストなプライベートアクセスへ

Point4 脆弱性管理

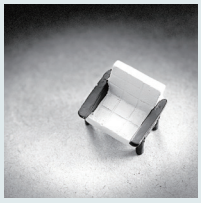
最後に、これはNIST によるゼロトラストの定義や原則には記述はないですが、冒頭でご紹介した通り、昨今被害を受けている企業の多くがVPNの脆弱性を突かれていま。そのため、脆弱性管理の徹底は非常に重要なポイントであると言えます。

とは言え、【脆弱性の放置は危険】などという事は、もはや誰もが知っているセキュリティの基本事項。にもかかわらず、なぜ多くの企業がセキュリティパッチの適用を徹底できないのでしょうか。下の図は放置される主な理由を紹介したものです。これらの理由から考えるに、属人的ではない仕組みを取り入れる必要があるのではないかと我々は考えます。

なぜ放置されやすい？

パッチ適応が放置されてしまう主な理由

- 業務の都合上、すぐには機器を止められない…
- セキュリティパッチの適用係を決めていなかった…
- 長年の担当者が退職…。引継げていなかった…



→ **属人的でない管理が要**

深刻化を極める、IT人材不足問題

昨今「ひとり情シス」や、専任担当者がいない「ゼロ情シス」などというワードが取りざたされるほど、IT人材不足が深刻化しています。しかし、ゼロトラスト対応も、DX推進も、クラウド化も…と情シスの課題は山積み。

そんな彼らに「メーカー発表のセキュリティ情報（脆弱性の報告）を常にチェックし即対応せよ」などと言うのは、とても現実的とは言えません。

脆弱性は放置されがち、という前提で…
マネージメント付きサービスを活用すべし

フルマネージド付き

クラウドゼロトラスト「Verona」で、即ゼロトラスト対応

Veronaはゼロトラストなプライベートアクセスを提供する、フルマネージド付きのクラウドVPNサービスです。専用機器も、リモートアクセスソフトも、それをマネージするクラウド管理センターもオールインワンでご提供しています。

クラウドゼロトラスト
Verona

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

Windows PC / Mac　iPhone / iPad / Android

＋

プライベートアクセスゲートウェイ（Verona Edge）

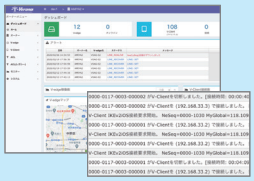
ハードウェア版、ソフトウェア版、クラウドゲートウェイ版を用意

BIGLOBE　Microsoft Azure　AWS　クラウド　NEC IaaS　拠点

＋

クラウド管理センター（Verona Cloud）

構築なしで管理画面が利用可能。ユーザ管理、設定管理もラクラク



2,900社を超える実績

セキュリティを重視する法人企業へ多数供給しています。

Network All Cloud 2021年度実績 2900社以上

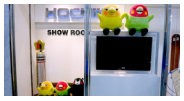
外食店舗　**松屋フーズ様**
1,000 店舗へスピード導入

オフィス　**ファインドスター様**
10 数社のグループ企業オフィスに

事務所　**熊谷組様**
300 店舗超の
サテライト工事事務所をクラウド化

学校　**板橋中央看護専門学校様**
授業のタブレット利用
に学校インフラをクラウド化

テレワーク　**ホーチキ様**
2,000 名のテレワーク環境に



モール店舗　**リクルート様**
90 拠点以上の
スーモカウンターに全国展開

市進教育グループ　SAKURA Internet　StylingLife　ADERANS　MINI STOP　DCS

JISA AWARDS WINNER 2020

支える技術**[amigram]**は、
情報サービス産業協会（JISA）で『**JISA Awards 2020**』を受賞

選ばれる4つの理由

選ばれる理由 その1
IDaaS連携

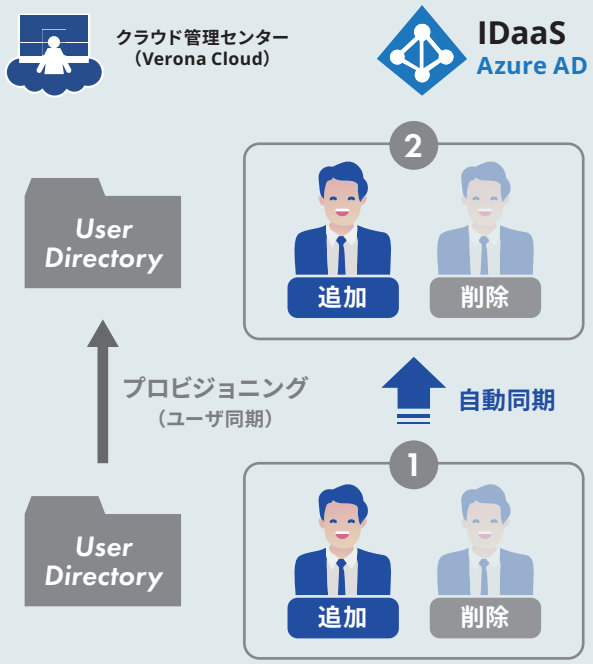
Veronaは、IDaaS（AzureAD）と連携をしています。
AzureAD側で登録/削除された情報は、Verona側でも自動で連携されますので、アカウントの削除漏れなどにより生じるセキュリティリスクを回避することが可能です。

また、シングルサインオンにも対応。AzureADアカウントで使用しているユーザ認証(ID/パスワード)を使いつつ、Verona標準認証のクライアント証明書認証も同時に実行。2要素による強固な認証システムを、ストレスなく実現できるのが特徴です。

ユーザ情報を同期

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

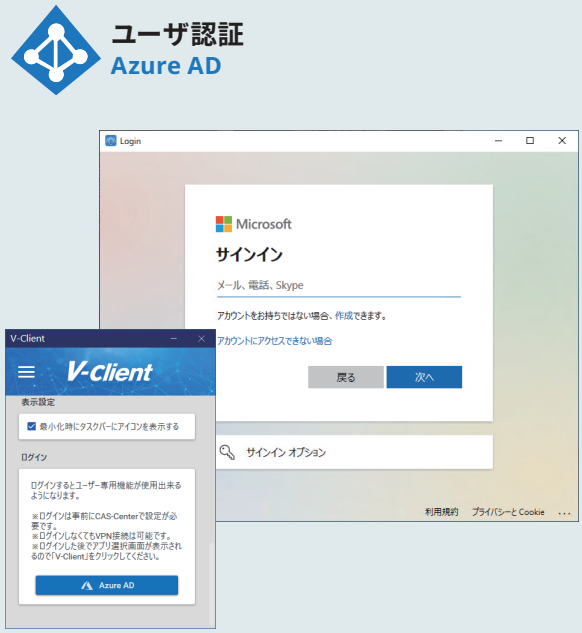
※本機能はWindowsのみ対応
※HENNGE Oneはユーザ追加のみ対応



シングルサインオン

AzureADアカウントでのユーザ認証と
証明書によるデバイス認証で強固な2要素認証を実現。

※本機能はWindowsのみ対応



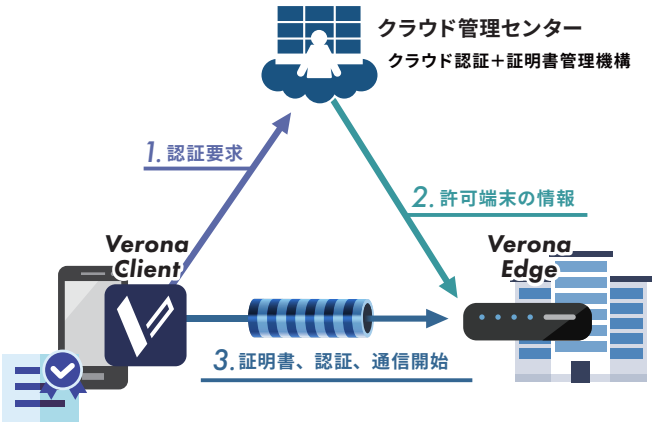
Veronaは、IDaaS（AzureAD）と連携、シングルサインオンにも対応

選ばれる4つの理由

選ばれる理由 その2
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プライベートアクセスですが、Veronaは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を採用しており、不正アクセスを防止できるのが特徴です。

証明書認証とは、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する認証システムです。許可された端末以外からはアクセスが出来ないため、たとえID/パスワード情報が漏えいしてしまったとしても、この認証が第二の防御壁として働いてくれます。



証明書管理はWebでラクラク

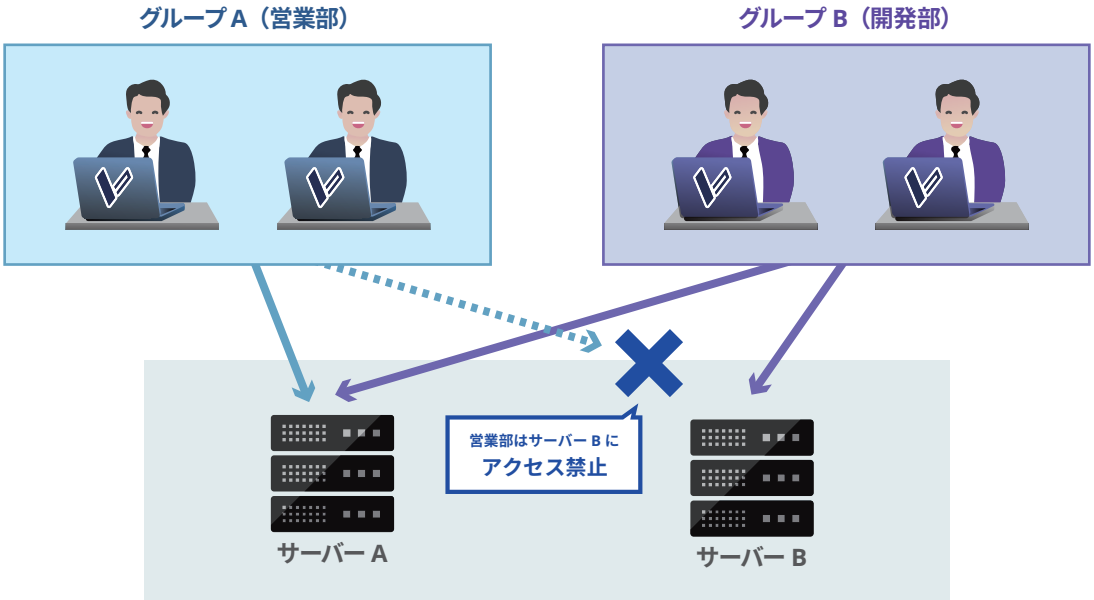
Veronaは、証明書の管理などができるVerona CloudをSaaSとして提供しています。
そのため、コントローラーの構築や証明書認証基盤の構築をすることなく、PC紛失時の接続拒否や、PCリプレイス時の証明書の入替え/配布などをWebから簡単に行う事が可能です。

Veronaなら、手間もコストもかけずに多要素認証を実現

選ばれる4つの理由

選ばれる理由 その3
マイクロセグメンテーション機能

Veronaは、証明書認証で使用している証明書をグルーピングし、それぞれグループ毎にアクセス制限をかけることが可能です。
下図のように管理画面内からいつでも設定/反映できるため、その運用が簡単なのも魅力の一つ。



管理画面イメージ

2	営業部	
V-Client接続ID	仮想IPアドレス	
0000-0117-0001-000001	192.168.152.100	岡田
0000-0117-0001-000002	198.20.7.201	東郷
0000-0117-0001-000003	192.168.150.100	寺園
0000-0117-0001-000004	198.20.8.10	鈴木
0000-0117-0001-000005	198.20.6.20	高本

3	開発部	
V-Client接続ID	仮想IPアドレス	
0000-0117-0001-000007	198.20.8.201	小松
0000-0117-0001-000008	198.20.7.201	佐久間
0000-0117-0001-000009	198.20.8.202	中野
0000-0117-0001-000010	198.20.8.201	安藤
0000-0117-0001-000011	192.168.151.101	佐藤

Veronaには、便利なマイクロセグメンテーション機能が搭載

選ばれる4つの理由

選ばれる理由 その4
フルマネージド付サービスだから安心

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

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）

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

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は、運用管理付。脆弱性管理もお任せできる

不具合の対処や設定変更作業の代行までやる

例えば…

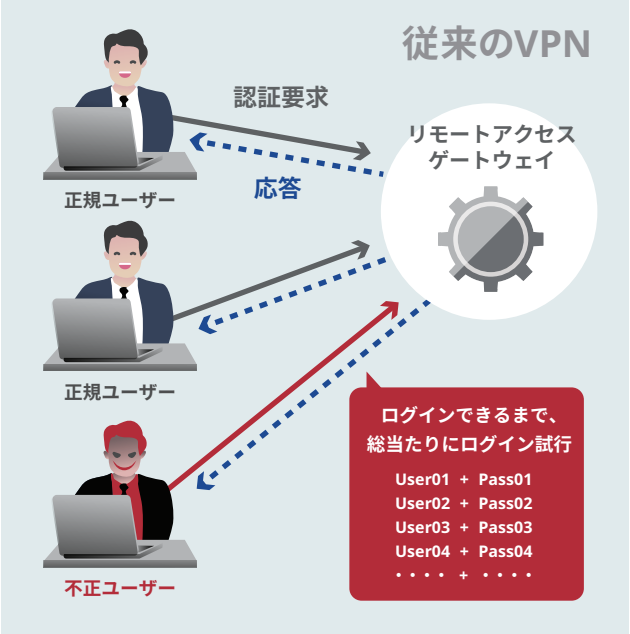
「Bサーバには営業部アクセスNG、開発部はA、Bサーバ両方アクセスOKにしたい」
さて…どうやって？ とりあえずサポートに聞いてみよう！

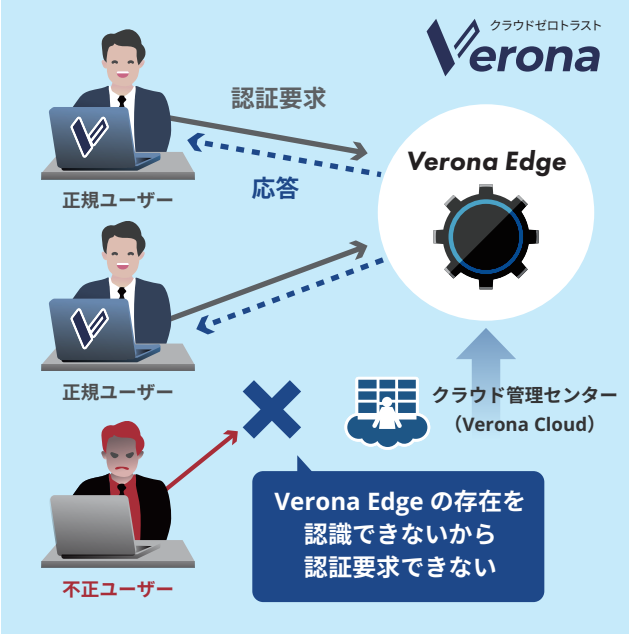
まだある！

様々なセキュリティ機能

ダイナミックポートコントロール

Veronaには、正規ユーザーからの認証要求にのみ応答するダイナミックポートコントロール機能が搭載されています。
これにより、VPNの特性上仕方ないとされていたリスク（不正ユーザーからの認証要求にも応答してしまう）を極めて最小に抑えることが可能です。





ログで履歴をしっかり記録

万一のとき、不正の証跡となるログの存在。
Veronaなら、リモートアクセス端末の接続切断ログや、取得したIPアドレス、アクセス制御などの各種設定を確認できます。

でも、使い勝手が悪くちゃ意味がない

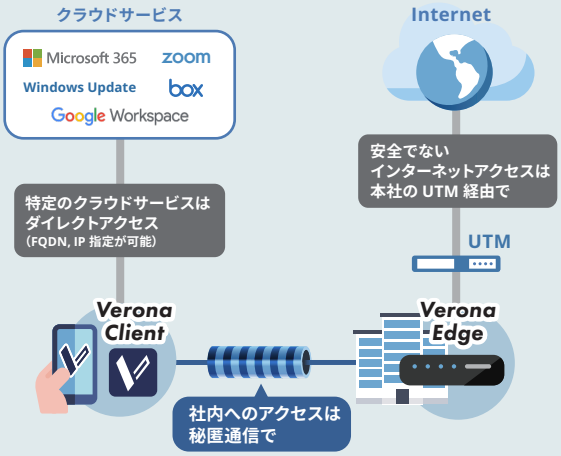
Veronaには、こんな機能が

経路選択と負荷分散

リモートからの通信が集中するVPN機器はボトルネックになることも。
Veronaなら、ローカルブレイクアウト機能とロードバランス機能で、ゲートウェイ機器の負荷を軽減・分散します。

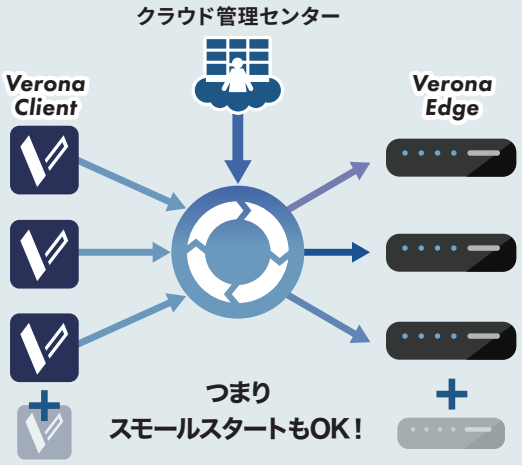
ローカルブレイクアウト

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。

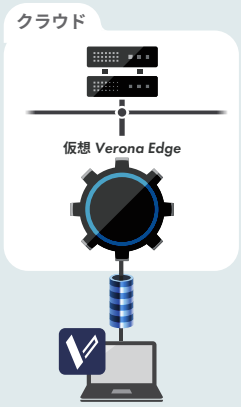


クラウドアクセスも

Veronaは、クラウドサービスへのプライベートアクセスもサポート。
ソフトウェアタイプとクラウドゲートウェイタイプの2つの方式を選択できます。

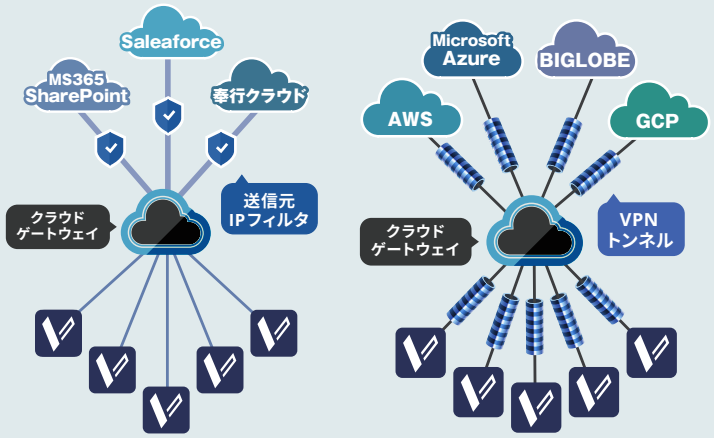
ソフトウェアタイプ

ソフトウェア版のVerona Edgeを
お客様クラウド内に構築。
冗長構成や多拠点接続に最適



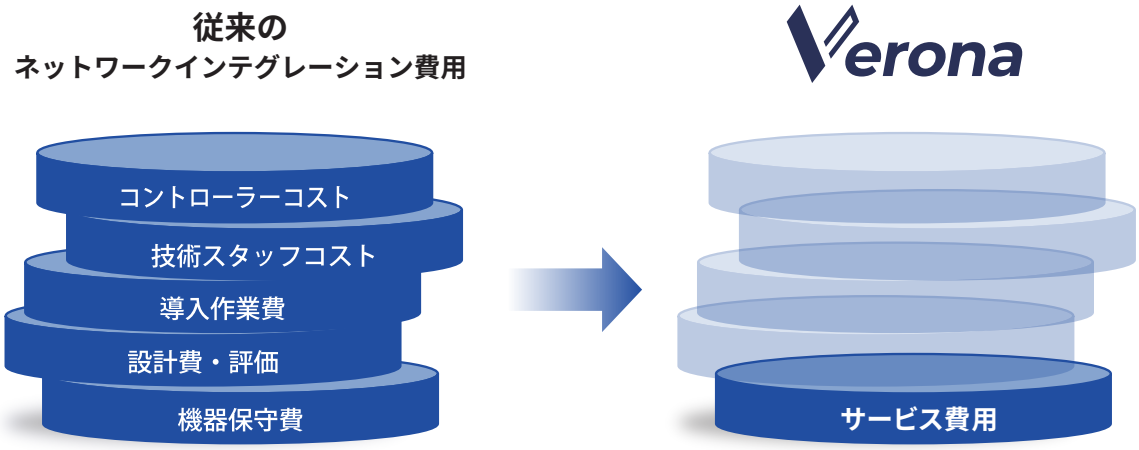
クラウドゲートウェイタイプ

クラウドゲートウェイを経由してプライベートアクセス



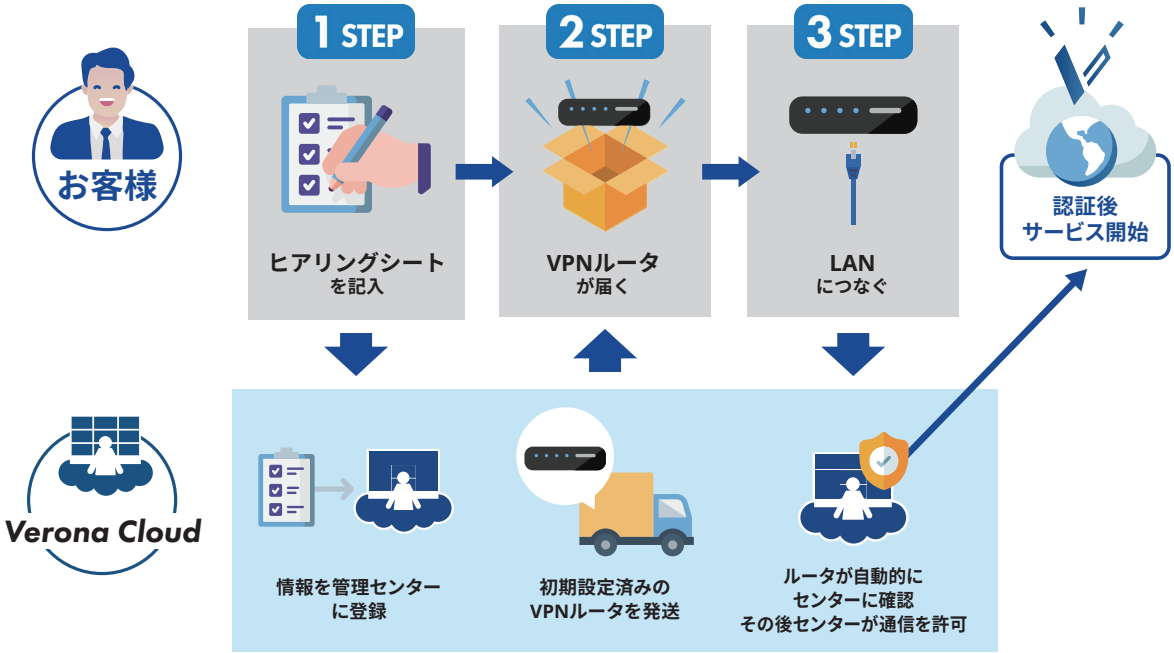
コストも魅力の要因

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。



導入から稼働まで簡単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。



導入事例

ホーチキ株式会社 様

リモートアクセス
2,000ライセンス

業種

総合防災メーカー

従業員数

単独 1,356名
連結 2,105名
（2020年3月31日現在）

情報システム部
IT推進課 課長
鈴木 智 様

Veronaを利用してみていかがですか？

セキュリティ面と運用面にも満足しています。
セキュリティ面は、強固とされるクライアント証明書を含めた2要素認証なのでより安心できます。運用面でも、死活監視をお任せでき、問い合わせしても結構レスポンスが早いので、社員の負荷が上がらず助かっています。

課題

- コロナで全社員テレワーク環境整備が急務に
- ID/Passwordの認証ではセキュリティレベルが…
- 急なシステム導入運用が懸念

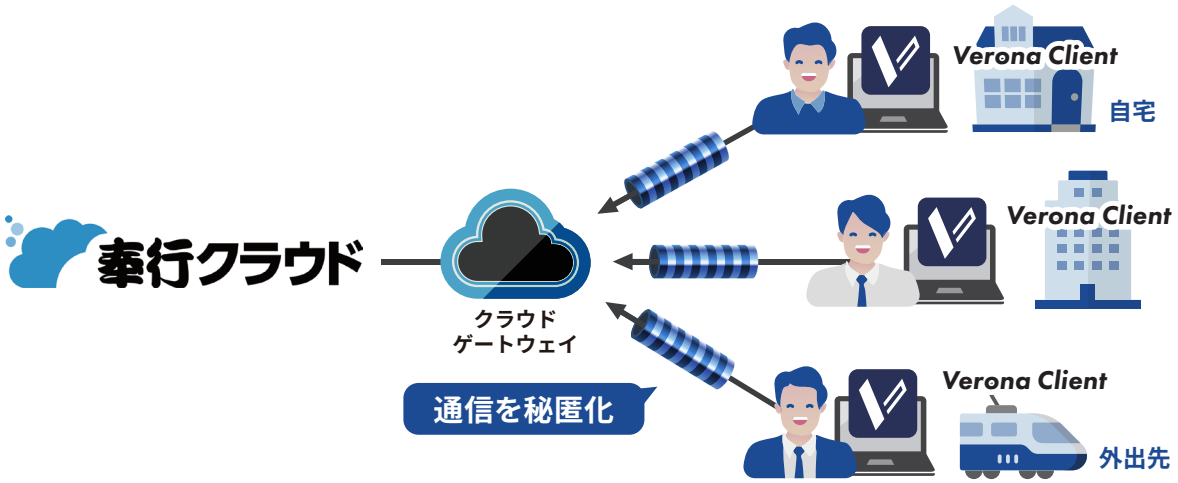
導入効果

- ☑ 2週間で申し込みから利用まで完了
- ☑ クライアント証明書認証で高セキュリティ
- ☑ 運用サービス付きだから安心

オービックビジネスコンサルタント（OBC）様

SaaS連携も

『Verona』との連携により、インターネット通信の安全性を確保した状態で奉行シリーズを利用することができるようになりました。



奉行クラウド × Verona

クライアント証明書をインストールしたデバイスのみ
『奉行クラウド』『OBCクラウドサービス』を利用開始

まとめ

1 人の管理は抜け漏れが生じる、前提で…
ID管理は、IDaaSで一元管理すべし
→ Veronaは、IDaaS（AzureAD）と連携、シングルサインオンにも対応

2 認証情報は流出する、前提で…
複数認証システムを採用すべし
→ Veronaなら、手間もコストもかけずに多要素認証を実現

3 侵入は成功し横展開される、前提で…
権限を最小化。必要な通信だけ解放すべし
→ Veronaには、便利なマイクロセグメンテーション機能が搭載

4 脆弱性は放置されがち、という前提で…
マネージメント付きサービスを活用すべし
→ Veronaは、運用管理付。脆弱性管理もお任せできる

クラウドゼロトラスト Verona なら、

速攻でゼロトラストなプライベートアクセス環境を構築できる

詳しい製品のご紹介、評価版のご依頼は以下にお問い合わせください。

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

AMIYA 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/

Veronaは株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、著作権の侵害になります。

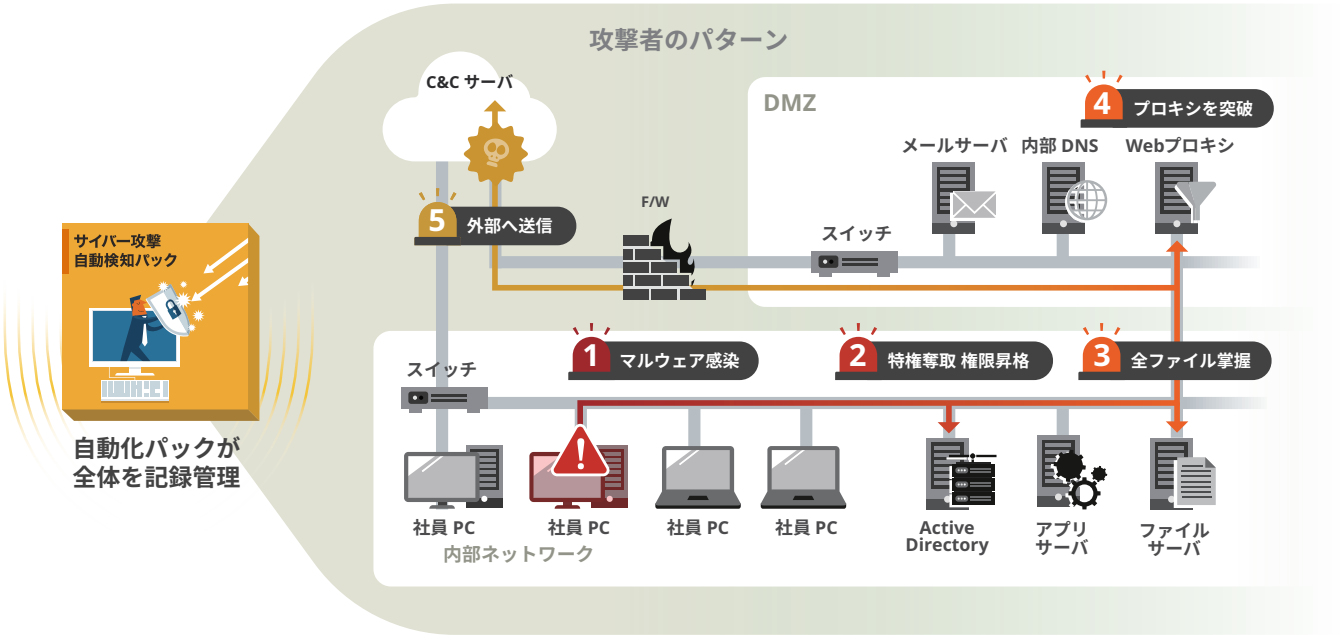
念には念を

サイバー攻撃対策に万全はない

巧妙化する標的型攻撃。もはや侵入の完全制御は不可能な時代。
最善の対策は、侵入される事を前提にした体制まで整えること。

ALog サイバー攻撃自動検知パック

ALogはITシステムを包括的に記録管理するログデータマネジメントソリューション。
サイバー攻撃の自動検知に特化した定義済みのテンプレートパックが用意されており、難しい事前設計なくして誰でもカンタンに「侵入のスピード察知」と「感染源のスピード隔離」が実現できるようになります。



詳細はこちらのホワイトペーパーで

**サイバー攻撃監視はカンタンに自動化できないのか？
専門知識不要、コスト不要の徹底自動化ガイド
[2022年最新版]**

ダウンロードはこちら ›