AMIYA

警察庁・日本政府観光庁含む
600以上の組織が被害に!

2020年大規模流出事件から読み解く VPNを狙うサイバー攻撃 撃退法

目次

- 2020年8月、大規模なVPN認証番号流出事件が発生 …… 1
- コロナ禍、テレワークの普及と共に進んだリモートアクセスVPNの導入 …… 2
- VPN機器の脆弱性が続々とターゲットに… …… 3
- リモートアクセスＶＰＮは諸刃の剣？ …… 4
- 有効な対策
  - 対策① セキュリティパッチの適用を徹底 …… 5
  - 対策② 多要素認証で第二、第三の防御を …… 6
- 考えたり、作ったりせずに、もう既にある仕組みを使おう！ …… 7
- 選ばれる理由
  - 運用サポートまで任せられる …… 8
  - クライアント証明書認証を標準搭載 …… 9
  - ダイナミックポートコントロール機能 …… 10
- 様々なセキュリティ機能 …… 11
- コストも魅力の要因 …… 11
- 導入から稼働まで簡単3ステップ …… 12
- Veronaには、こんな機能が …… 13
- 導入事例 [ホーチキ株式会社] …… 14
- SaaS連携も …… 14
- 最善の策は、既にある仕組みを利用すること …… 15

2020年8月、大規模なVPN認証番号流出事件が発生

2020年8月、警察庁・日本政府観光庁含む600以上の組織が被害にあう大規模なVPN認証番号流出事件が発生しました。安全なリモートアクセスのために導入したはずのVPNが、なぜサイバー攻撃の標的となってしまったのでしょうか？

本ホワイトペーパーでは、今回の事件の原因を紐解くと共に、VPNの特性を理解し、本来の目的である安全なリモートアクセス環境を構築/維持するにはどのような点に留意する必要があるのか詳しく紹介したいと思います。

600超の組織にサイバー攻撃　テレワーク機器の欠陥悪用

2020/12/1(火) 6:00 配信 3

KYODO

VPN狙うサイバー攻撃

テレワークや遠隔操作に使われる情報機器の欠陥が悪用され、少なくとも607の国内企業や行政機関などがサイバー攻撃を受けていたことが30日、専門家への取材で分かった。警察庁や日本政府観光局、岐阜県庁、リクルート、札幌大などで被害が判明。多くがID、パスワードなどの認証情報を盗まれていた。

この機器は外部からネットワーク内部に安全に接続するために利用され「VPN（仮想私設網）」と呼ばれる。新型コロナウイルス流行で利用が増えている。問題のVPNは米フォーティネット社製で、欠陥が放置されている機器は世界で約5万台あり、うち1割超の約5400台が日本関連だった。

↑（Yahoo!ニュース　2020/12/1(火) 6:00配信）
共同通信「600超の組織にサイバー攻撃　テレワーク機器の欠陥悪用」
https://news.yahoo.co.jp/articles/5c798d2d31cc66a3063ccf2bae1a7b4226ab5129

在宅勤務の認証情報38社が流出　住友林業や日立化成など悪用恐れ

2020/8/25(火) 11:55 配信 280

KYODO

住友林業や日立化成などで在宅勤務する社員らが社内システムの利用時に必要な機器「VPN（仮想私設網）」の認証情報が、不正アクセスによって盗まれていたことが25日、情報セキュリティー専門家への取材で分かった。両社を含む38社分の認証情報がインターネット上に流出している。

VPNは新型コロナウイルスの感染拡大とともに利用が急増。第三者に悪用されると社内システムへの侵入が容易になることから、内閣サイバーセキュリティセンター（NISC）が注意を呼び掛けている。現在まで被害は確認されてないという。

↑（Yahoo!ニュース　2020/8/25(火) 11:55配信）
共同通信「在宅勤務の認証情報38社が流出　住友林業や日立化成など悪用恐れ」
https://news.yahoo.co.jp/articles/0ec3beca3dc2fb5b814f8c32423a9858361cb617

コロナ禍、テレワークの普及と共に進んだリモートアクセスVPNの導入

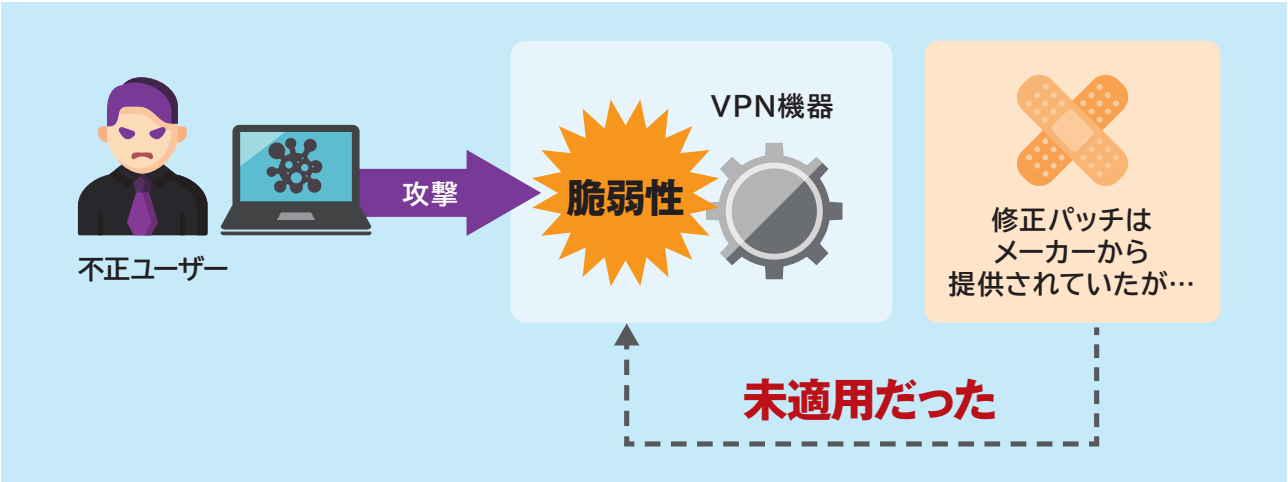
2020年、新型コロナウイルスの感染拡大の防止を目的に急速に進んだテレワーク環境の整備。多くの企業が、自宅やサテライトオフィスからでも、社内ネットワークへ安全にリモートアクセスできる環境を突如整備しなくてはならない事態となりました。
社外からのリモートアクセスを実現するにあたりいくつか方法はありますが、なかでもVPNは「セキュリティレベルが高いこと」と、「導入のしやすさ（社内ネットワークにゲートウェイを設置し、使用端末に専用ソフトウェアをインストールするだけ）」から、多くの企業が採用している方式です。
そんな中、発生したのが今回の大規模VPN認証番号流出事件。
社会的に大変大きなインパクトを与えました。

安全なリモートアクセスのためのVPN、なぜ標的に？

原因はパッチの未適用

今回の事件、社内ネットワーク側に設置されていたVPN装置に既知の脆弱性が存在し、これに修正パッチを適応しないまま放置してしまったことが主な原因でした。

メーカーは事件が発生した2020年8月の約1年半前には、この脆弱性に対応した修正パッチを提供していたものの、該当機器を利用する多くの企業でこれが適応されておらず、結果的に600以上の組織が被害にあう事態となってしまいました。



VPN機器の脆弱性が続々とターゲットに…

また、事件が報じられた2020年8月は、Pulse Secure社製品の脆弱性をターゲットとした攻撃が話題となりましたが、これを皮切りにPalo Alto Networks 社製やFortinet 社製、Citrix社製品と、大手メーカーから提供されているVPN機器の脆弱性も攻撃対象として次々とハッカーから狙われる事態となりました。

2020年にJPCERTが注意喚起を行ったVPN機器の脆弱性

Pulse Connect Secure	CVE-2019-11510 CVE-2019-11539
Palo Alto Networks	CVE-2019-1579
Fortinet	CVE-2018-13379
Citrix ADCおよびCitrix Gateway	CVE-2019-19781

いずれの脆弱性も1年以上前に、メーカーから発表されていた…

参考: JPCERTコーディネーションセンター
「複数のSSL VPN製品の脆弱性に関する注意喚起」https://www.jpcert.or.jp/at/2019/at190033.html
「複数の Citrix 製品の脆弱性（CVE-2019-19781）に関する注意喚起」https://www.jpcert.or.jp/at/2020/at200003.html

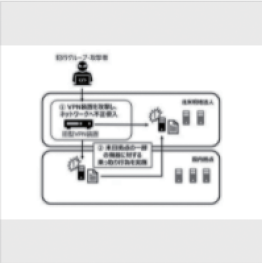
実被害も発生

VPN装置の脆弱性が狙われ、実際にサイバー攻撃被害にあってしまったケース

カプコン、不正アクセス被害の調査結果を公表　旧型VPN装置にサイバー攻撃

4/14(水) 18:29 配信 3

ITmedia NEWS



攻撃被害のイメージ図

2020年11月にカプコンが不正アクセスを受け、個人情報が流出した問題で、同社は4月13日、北米の現地法人に設置していた旧型VPN装置へのサイバー攻撃が原因とする調査結果を公表した。流出を確認した個人情報は計1万5649人。

【画像】カプコンのオフィス（出典：公式ページ）

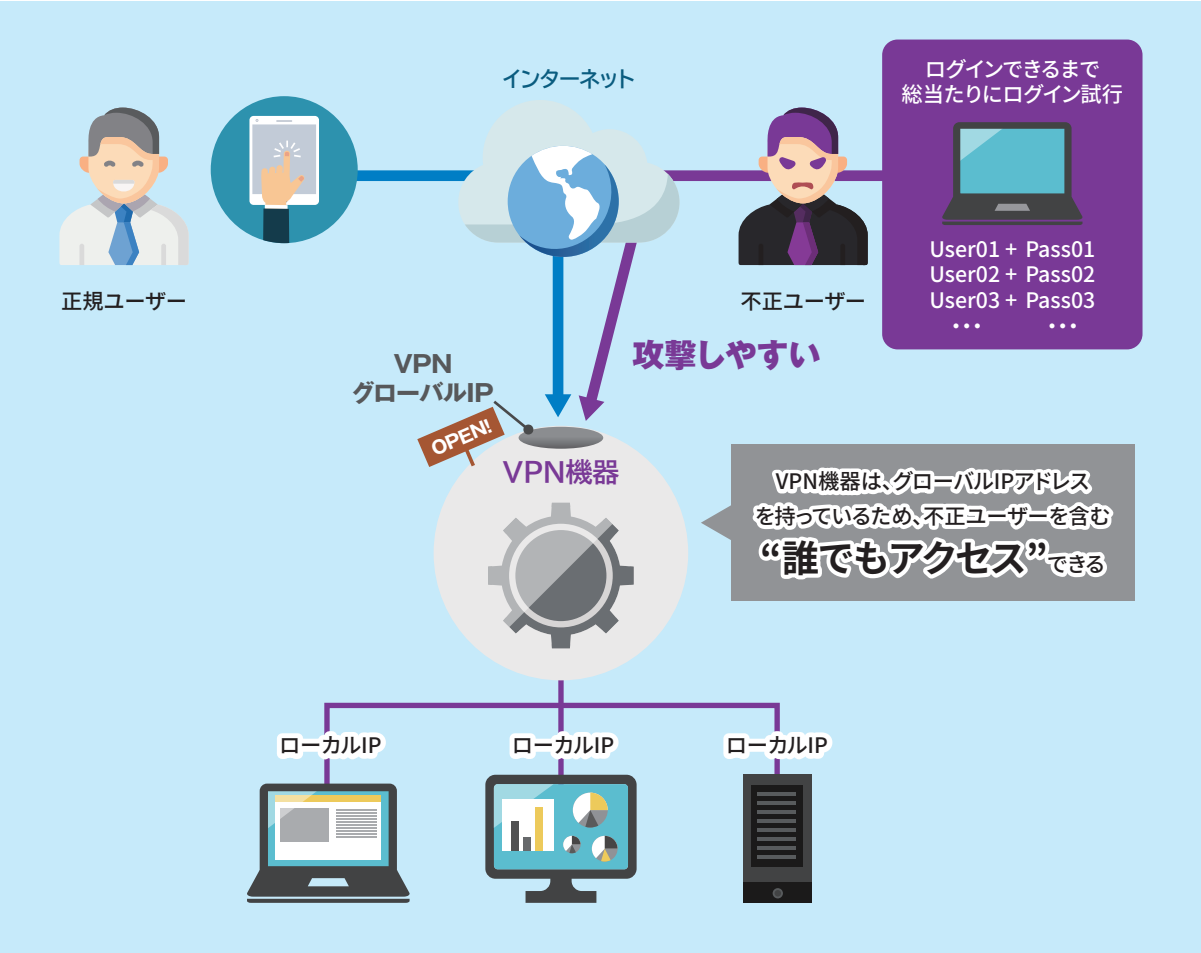
調査結果によると20年10月、北米の現地法人

↑（ITmedia NEWS　4/14(水) 18:29配信）
ITmedia NEWS「カプコン、不正アクセス被害の調査結果を公表　旧型VPN装置にサイバー攻撃」
https://news.yahoo.co.jp/articles/8c696ddc2ed4242c01db1d32b562a4bc862466c9

脆弱性とパッチ提供の状況を把握し、すぐに適応を!

リモートアクセスVPNは諸刃の剣？

VPNの最大の特徴はその名(Virtual Private Network)の通り、インターネット空間上に仮想の専用ラインを構築できるところにあります。この仮想専用ライン内を通って通信が行われるようになることから、「どこからでも安全にアクセスできる環境」が実現するのですが、これを実装するのに欠かせないのがVPNルータの存在。
このVPNルータはゲートウェイとして機能するためにグローバルIPを保有しており、インターネット上でリモートアクセスをする際に必要な特定のポートを、常時開放しています。
すなわちこれは、正規ユーザーのみならず不正ユーザーを含む“誰もが”VPN機器にアクセスできる状態と言えます。



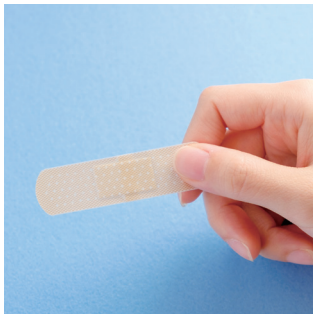
今回の事件ではVPNルータの脆弱性をついて攻撃されてしまいましたが、脆弱性がなくとも、攻撃者はログインできるまで総当たりにログインを試行することができるため注意が必要です。

VPNだからといって安心はできない

有効な対策法

リモートアクセスVPNに存在する、様々な危険性が見えてきたところでここからは、有効な対策法を述べていきたいと思います。

対策① セキュリティパッチの適用を徹底

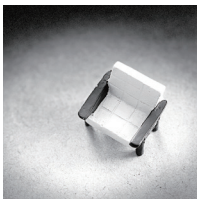


まずは、基本的なことですがセキュリティパッチの適用を徹底しセキュリティーホールをそのままにしないこと。とはいえ、これはもはや誰もが知っている当然のルール。では、なぜ今回の事件のように多くの企業がセキュリティパッチの適用を徹底できず脆弱性を放置してしまうのでしょうか。

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…

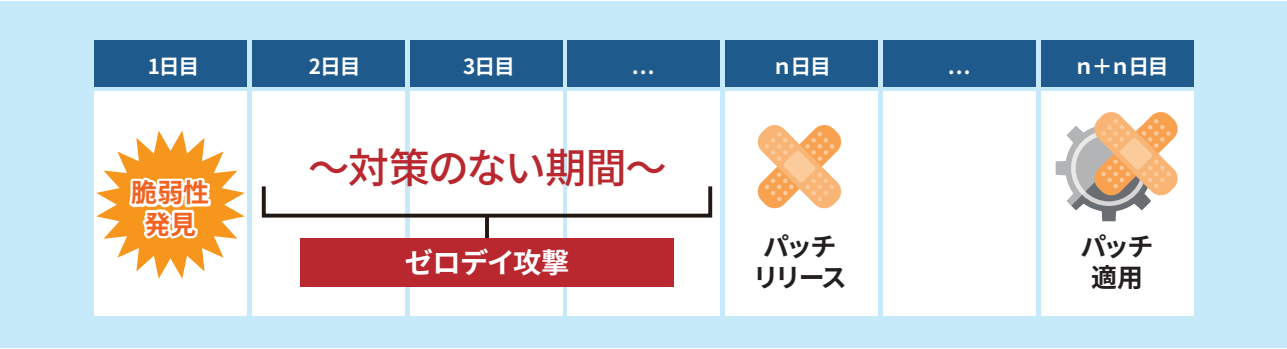


近年、クラウド化、デジタルトランスフォーメーション（DX）、IoTなど、経営戦略の中でIT活用はますます重要度を増しており、これに比例して情報システム部門の負担増が深刻な問題となっています。

IT活用戦略を進めながら、イレギュラーに発生する障害対応も行わなければならない彼らに、「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できるようにせよ」というのは、とても現実的なことではありません。

努力で乗り切ろうにも、ゼロデイ攻撃には無力…

そもそも、いくらセキュリティパッチの適応を徹底したとしても、脆弱性が発覚しメーカーから修正パッチがリリースされるまでの間に攻撃を受けてしまう可能性もあります（これをゼロデイ攻撃と言います）から、これには努力の対応も無力です。



現実問題、属人的な運用管理には限界がある

有効な対策法

対策② 多要素認証で第二、第三の防御を

そこで次の砦となるのが、多要素認証。
たとえID認証の情報が漏えいしたとしても、第二・第三の防御壁となり
社内システムへの侵入を防ぐことが可能です。

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

もし2要素の認証をしていれば

▶ たとえIDとパスワードが流出しても、2要素目で認証が通らないから大丈夫

様々な認証が存在しますが、お勧めはデバイス認証の併用です。
従業員の私物端末からのアクセスを回避できますので、悪意ある従業員が内部の情報を持ち出してしまうといった万が一の事態に備えることが可能です。
また、たとえ悪意はなくとも私物デバイスはセキュリティ対策が不十分なケースが多くウイルス感染していてそこから情報が流出してしまうことも十分考えられます。

おすすめのデバイス認証なら

このように多要素認証により第二、第三の防御壁を構築することの重要性については、お判り頂けたことと思います。
しかし、当然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が出たりと、労力だけでなくコストもかさみます。

現実問題、多要素認証は運用&コストの課題が

だから! 考えたり、作ったりせずに、もう既にある仕組みを使おう！

クラウド型+フルマネージド付きのサービス

VeronaはVPN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すべてオールインワンで提供するサービス。
社内システムへワンクリックでつながるセキュアなリモートアクセス環境をすぐに構築することが可能です。

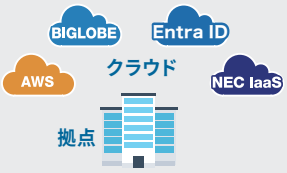
クライアントソフト（Verona Client）

専用リモートアクセスソフトを提供
マルチデバイス対応
ワンクリックカンタン接続

＋

プライベートアクセスゲートウェイ（Verona Edge）

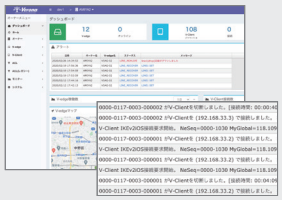
専用ゲートウェイ（Verona Edge）を提供
拠点・クラウドに設置可能



＋

クラウドコントローラー（Verona Cloud）

構築なしで管理画面が利用可能。
社員への証明書発行などもラクラク



3,700社を超える実績

Veronaはセキュリティを重視する法人企業へ
多数導入されています。

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

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

病院
イムス三芳総合病院様
大手病院グループに
拠点展開

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

選ばれる理由

1

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

▶ 面倒な証明書管理や修正パッチ適応に追われる必要はもうない！

不具合の対処や設定変更作業の代行までやる

例えば

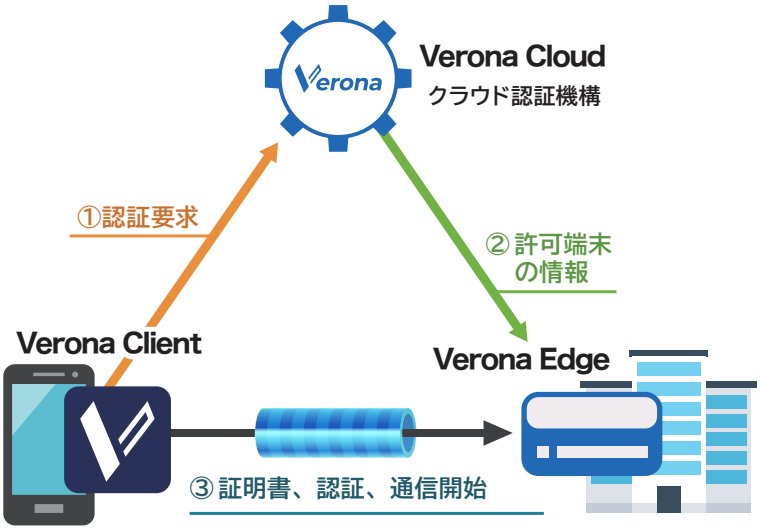
「Bサーバには営業部アクセスNG、開発部はA、Bサーバ両方アクセスOKにしたい」
さて…どうやって？とりあえずサポートに聞いてみよう！

選ばれる理由

2

クライアント証明書認証を標準搭載

今回の事件のように、脆弱ポイントにもなりかねないリモートアクセスVPN。
Veronaなら、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できます。



▶ 安心の認証をストレスなく実現

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 Console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。

選ばれる理由

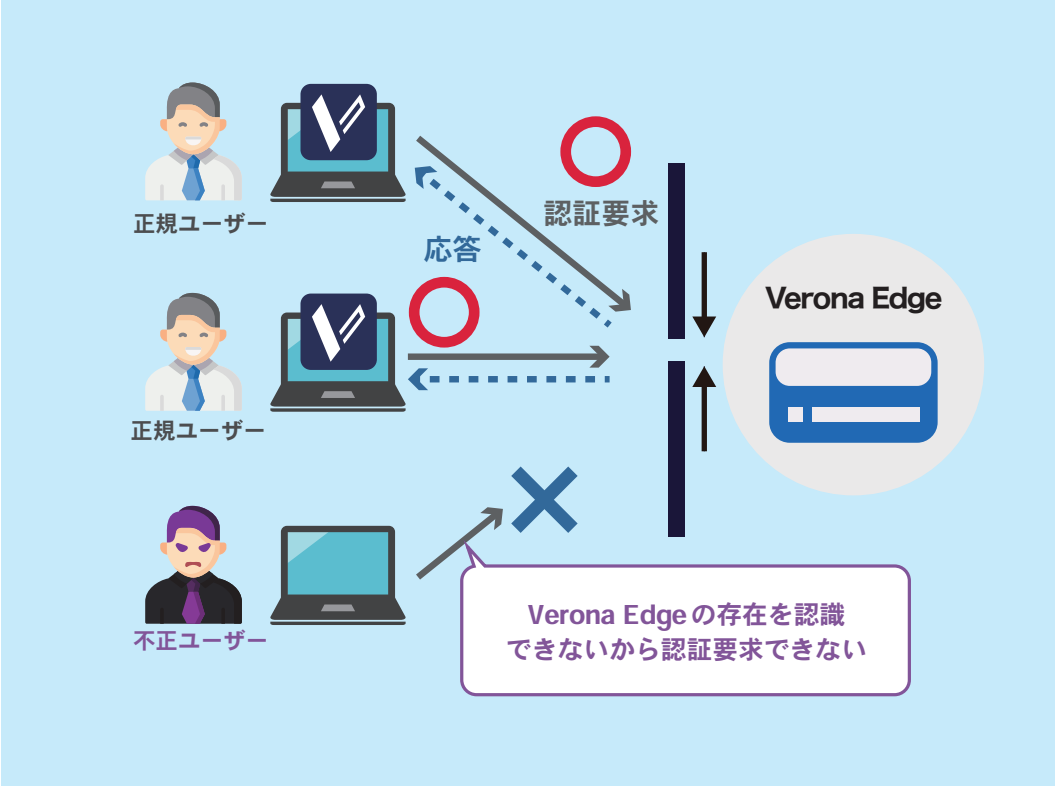
3

ダイナミックポートコントロール機能

Veronaには正規ユーザーからの認証要求のみに応答可能な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。

Verona

Verona Cloudと連携し、正規ユーザーからの認証要求のみ応答
不正ユーザーはVerona Edgeの存在を認識できません

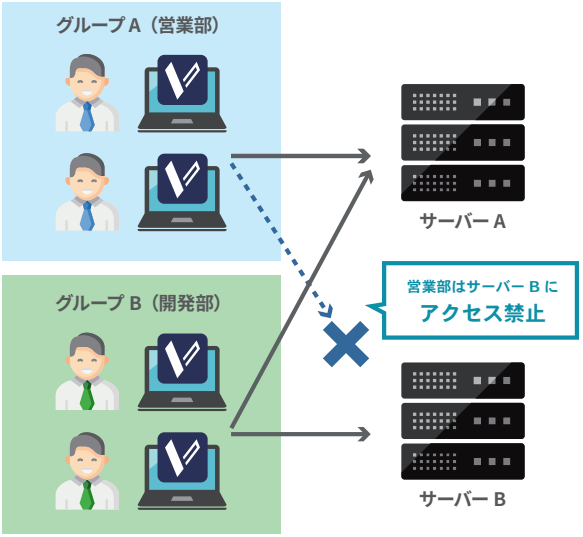


▶ ダイナミックポートコントロール機能で攻撃を回避

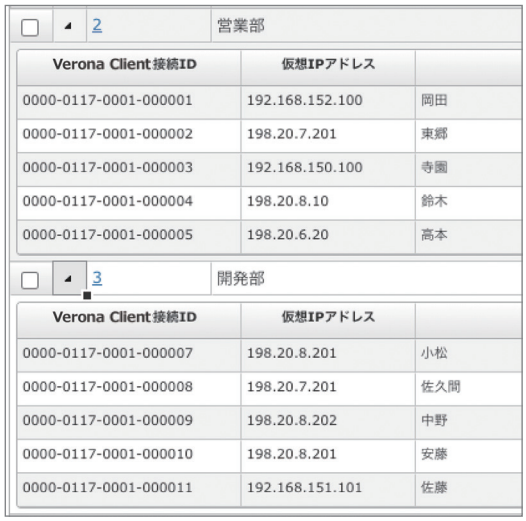
まだある 様々なセキュリティ機能

■グルーピングとアクセス制御

セキュリティ対策として、ユーザーごとのアクセス制御は必須機能。証明書（ユーザー）をグルーピングし、それぞれのグループにアクセス制御を設定できます。



管理画面



2 営業部

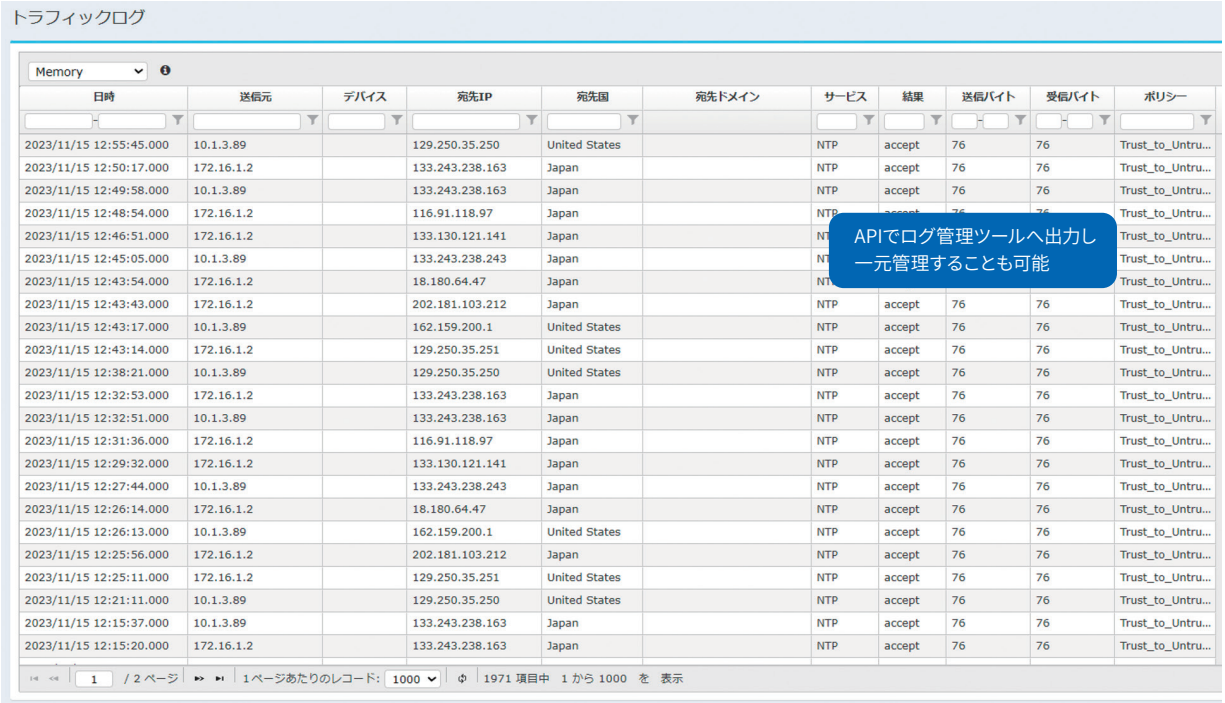
Verona Client接続ID	仮想IPアドレス	
0000-0117-0001-000001	192.168.152.100	岡田
0000-0117-0001-000002	198.20.7.201	東郷
0000-0117-0001-000003	192.168.150.100	寺園
0000-0117-0001-000004	198.20.8.10	鈴木
0000-0117-0001-000005	198.20.6.20	高本

3 開発部

Verona 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

■ログで履歴をしっかり記録

万一のとき、ログが不正の証跡に。ポリシーによって許可・拒否された通信のログ（トラフィックログ）や、リモートアクセス端末の接続切断ログ（システムログ）、各種設定を確認できます。



トラフィックログ

Memory

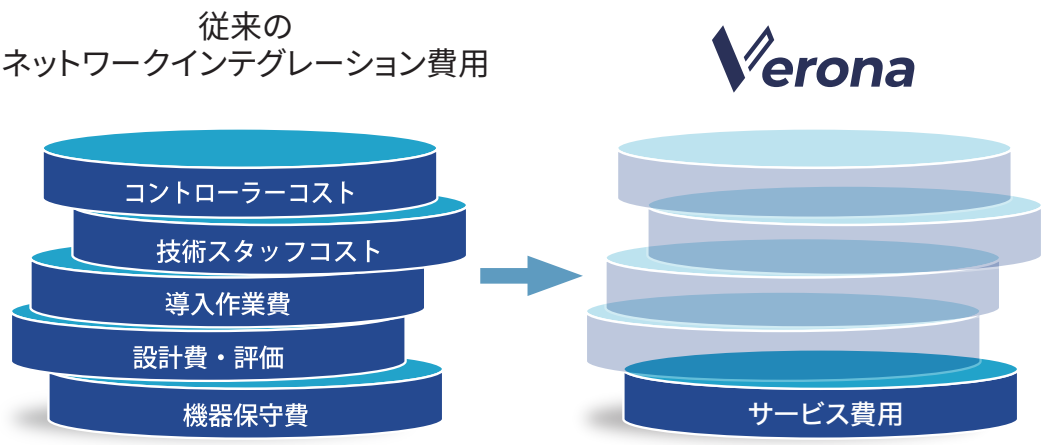
日時	送信元	デバイス	宛先IP	宛先国	宛先ドメイン	サービス	結果	送信バイト	受信バイト	ポリシー
2023/11/15 12:55:45.000	10.1.3.89		129.250.35.250	United States		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:50:17.000	172.16.1.2		133.243.238.163	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:49:58.000	10.1.3.89		133.243.238.163	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:48:54.000	172.16.1.2		116.91.118.97	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:46:51.000	172.16.1.2		133.130.121.141	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:45:05.000	10.1.3.89		133.243.238.243	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:43:54.000	172.16.1.2		18.180.64.47	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:43:43.000	172.16.1.2		202.181.103.212	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:43:17.000	10.1.3.89		162.159.200.1	United States		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:43:14.000	172.16.1.2		129.250.35.251	United States		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:38:21.000	10.1.3.89		129.250.35.250	United States		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:32:53.000	172.16.1.2		133.243.238.163	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:32:51.000	10.1.3.89		133.243.238.163	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:31:36.000	172.16.1.2		116.91.118.97	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:29:32.000	172.16.1.2		133.130.121.141	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:27:44.000	10.1.3.89		133.243.238.243	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:26:14.000	172.16.1.2		18.180.64.47	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:26:13.000	10.1.3.89		162.159.200.1	United States		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:25:56.000	172.16.1.2		202.181.103.212	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:25:11.000	172.16.1.2		129.250.35.251	United States		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:21:11.000	10.1.3.89		129.250.35.250	United States		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:15:37.000	10.1.3.89		133.243.238.163	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:15:20.000	172.16.1.2		133.243.238.163	Japan		NTP	accept	76	76	Trust_to_Untru...

1 / 2 ページ　1ページあたりのレコード: 1000　1971 項目中　1 から 1000　を　表示

APIでログ管理ツールへ出力し一元管理することも可能

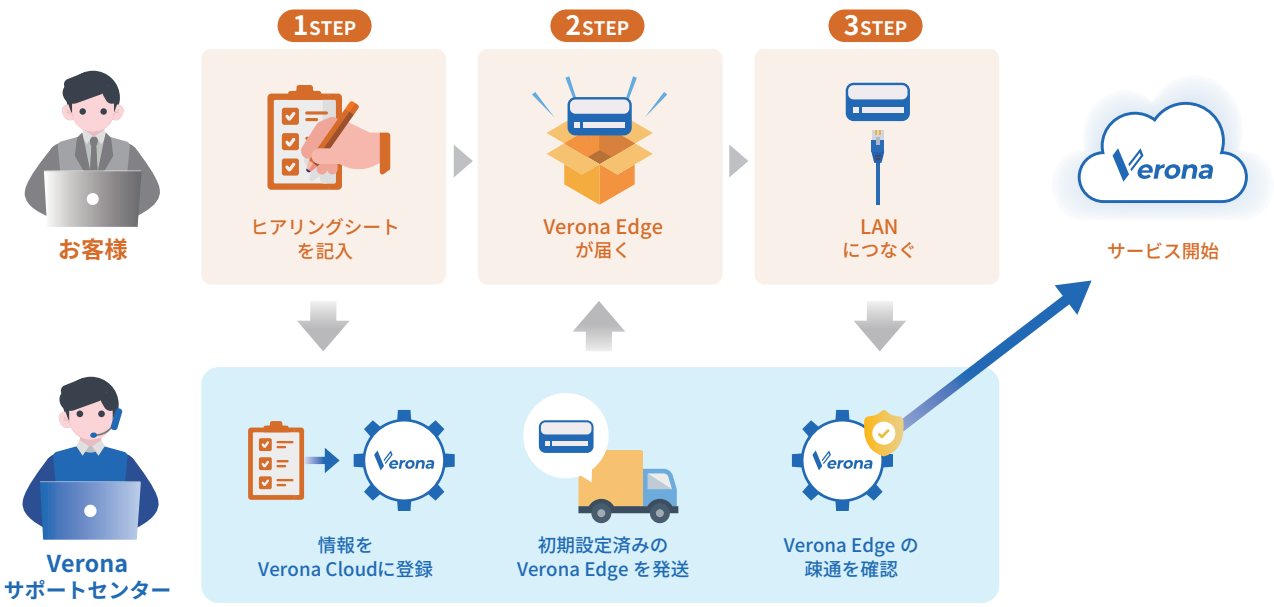
コストも魅力の要因

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、「〇〇は別途請求」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

また、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。



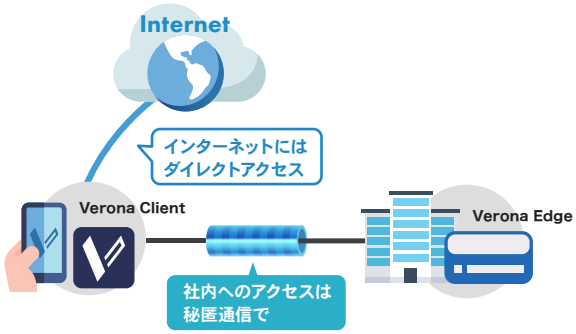
さらに! Veronaには、こんな機能が

■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、スプリットトンネル機能とロードバランス機能で、VPN機器の負荷を軽減・分散します。

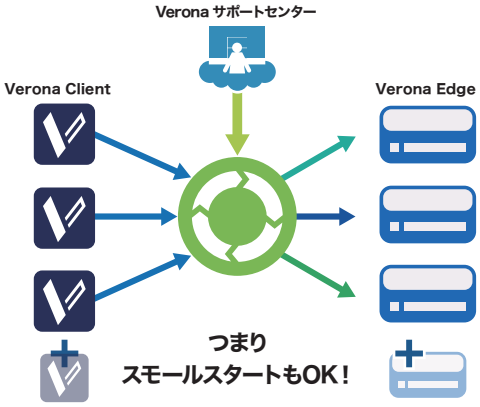
スプリットトンネル

インターネット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。

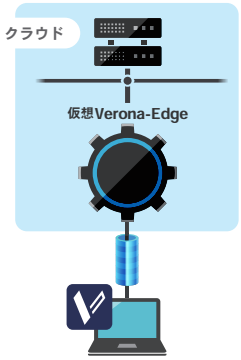


■クラウドアクセスも

クラウドサービスへのリモートアクセスVPNもサポート。
仮想Verona Edge方式とクラウドゲートウェイ接続方式
（Verona Client）の2つの方式を選択できます。

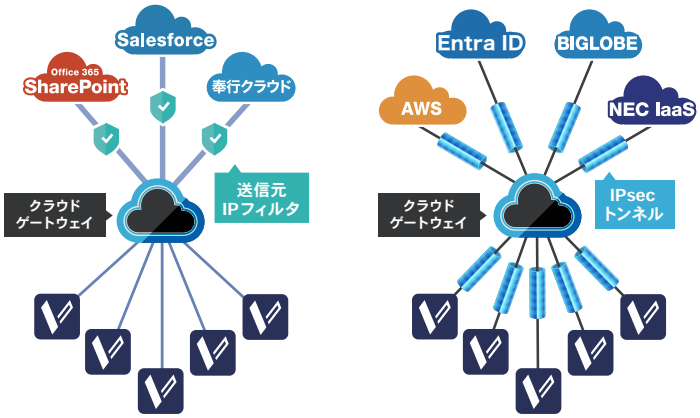
仮想Verona Edge方式

ソフトウェア版のVerona Edgeをクラウド内に
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接続方式

Verona Clientのクラウドゲートウェイを経由してリモートアクセス



導入事例

HOCHIKI ホーチキ株式会社様

リモートアクセス：1,300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名3月31日現在）

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に環境整備が急務に
- 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

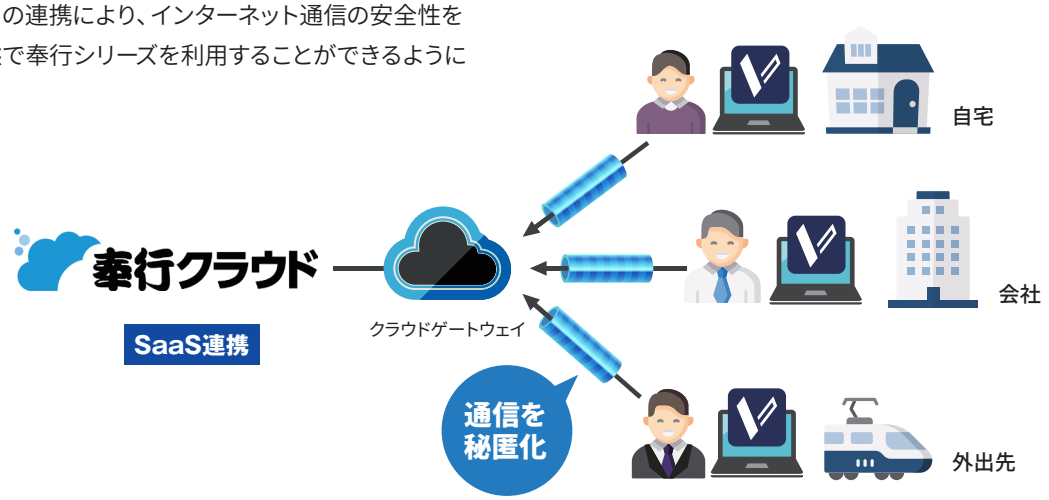
- 2週間で申し込みから利用まで完了安心
- クライアント証明書認証で高セキュリティ
- 運用サービス付きだから安心

SaaS連携も

奉行クラウド × Verona

オービックビジネスコンサルタント（OBC）様

『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。



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 最善の策は、既にある仕組みを利用すること

運用問題を解決する

修正パッチ適用など、専門的運用は
自力ではやりづらい

Veronaなら、運用サポートまで任せられる
証明書管理や修正パッチ適応に追われる必要はもうない！

脆弱な認証を使わない

内外の門扉となるVPNは、多要素認証が必須

Veronaなら、パスワードとクライアント証明書
による2要素認証でハイセキュア

VPNの特性に対処する

不正ユーザーを含む“誰でも
”VPN機器にアクセスできてしまう

Veronaなら、ダイナミックポートコントロール機能で
VPN機器を狙った攻撃を回避

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 ＞

販売代理店
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: 03-6822-9995
https://www.amiya.co.jp/

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。