導入期間
最短 2週間

フルマネージドで
運用負担
ゼロ

オール
インクルーシブで
コスト減

Verona

Network All Cloud
2023年度実績
4800
社以上

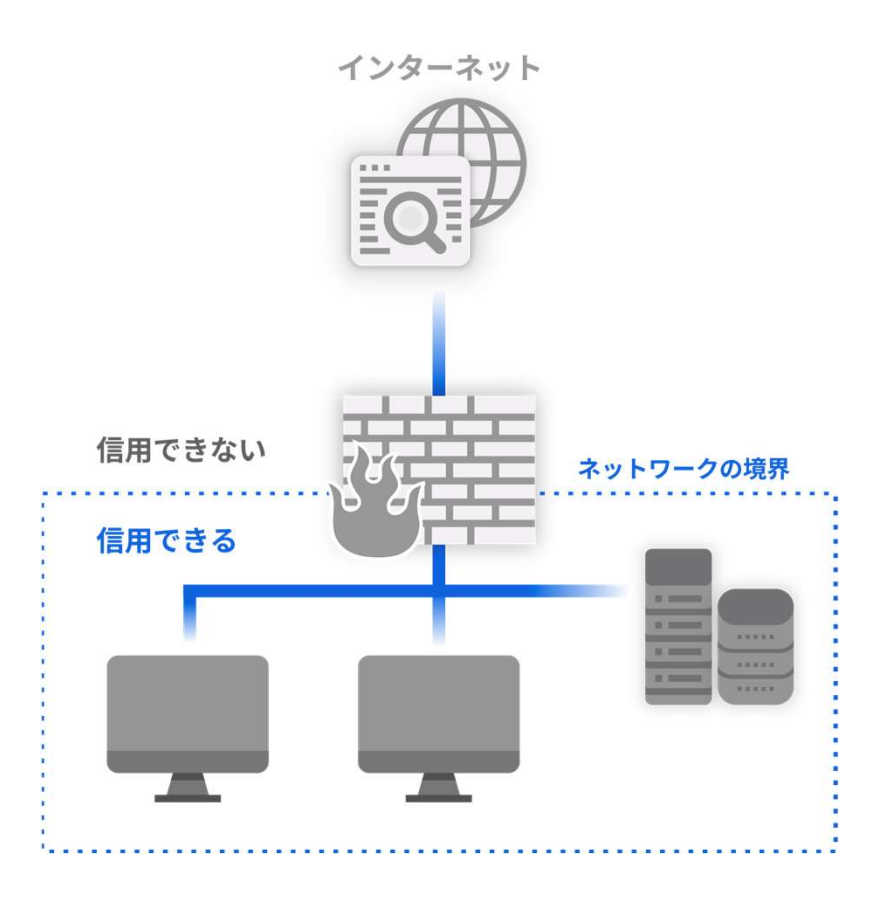
ここからはじめる
ゼロトラスト

AMIYA Ver. 10.2

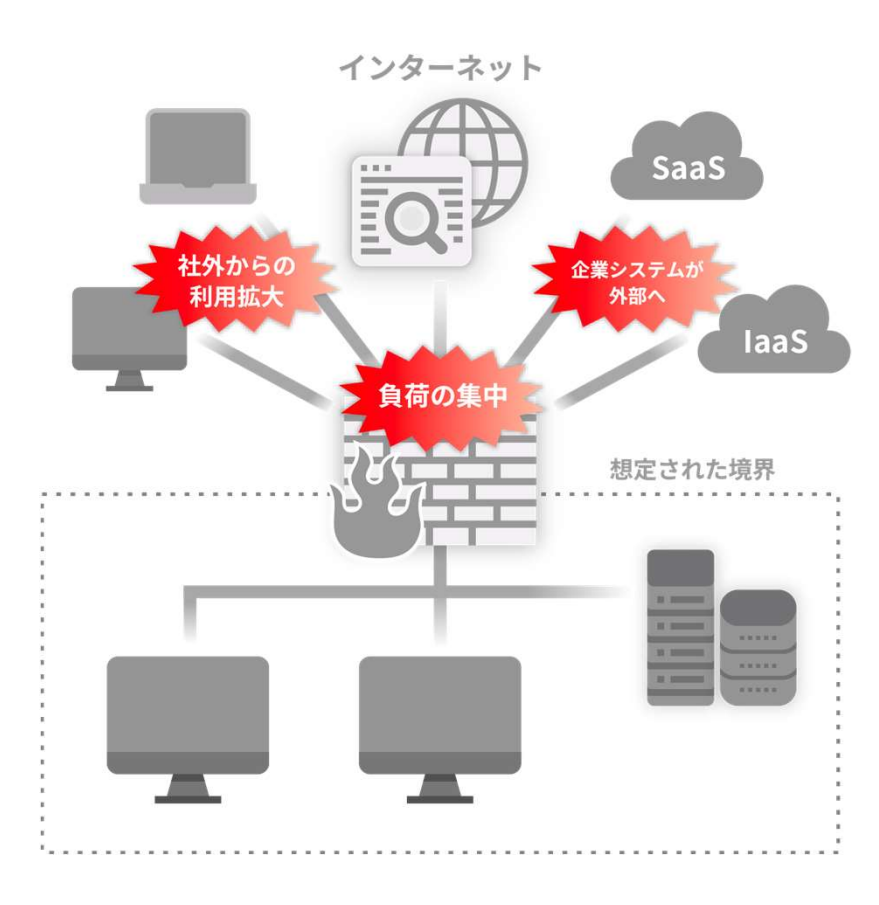
境界型防御アーキテクチャの限界

業務システムのクラウド化やテレワークの普及により、守るべきデータやデバイスが社外に分散。
社内の資産を守る従来の境界防御モデルでは、巧妙化したサイバー攻撃を前にセキュリティを担保できない。
「ゼロトラスト」の概念に則したセキュリティフレームワークが必要に。

守るべき資産は企業ネットワーク内に



守るべき資産が分散



© AMIYA Corporation

ITシステムの増大による運用負荷

運用しなければならないIT機器/システムは増加する一方で、IT人材は慢性的な不足。
ネットワークの安定運用と利便性、セキュリティの両立を達成するには多大な苦労が。

Firewall
VPN
Web proxy
ファイル
サーバー
UTM
WSUS
DNS
スイッチ
ルーター
無線LAN
Microsoft
365
AWS
Microsoft Entra ID
zoom
Google Workspace

© AMIYA Corporation

フルマネージドSASE 「Verona」という選択肢

Veronaは、ゼロトラストセキュリティを実現するフルマネージドSASEです。
働く場所を選ばない、統一された次世代ネットワークセキュリティを実現します。

© AMIYA Corporation

Veronaで実現する未来

従来の課題であったセキュリティと運用の課題を一度に解決！

ネットワーク全体を保護！

ネットワーク全体を保護！
アクセス元、アクセス先を問わない
セキュアなアクセスを実現。

運用管理を効率化

ネットワークセキュリティの
包括管理により、運用が効率化！

© AMIYA Corporation

Network All Cloudシリーズは、4,800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。

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　StylingLife　SAKURA Internet　ADERANS　MINI STOP　HOCHIKI

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

© AMIYA Corporation

Veronaのポイント1　“カンタン導入”

導入に必要な作業は、ヒアリングシートの記入だけ。
最短2週間で、カンタンにSASEを導入できます。

一般的なSASE導入プロジェクトの一例

- 既存環境の棚卸し
- 要件定義
- 既存機器のシステム変更
- 導入作業
- 受け入れテスト

6ヶ月～

半年以上の大規模プロジェクト…

Verona

ヒアリングシートを記入

網屋での
設定作業の実施

2週間

ご利用開始

お客様はヒアリングシートの記入だけ！

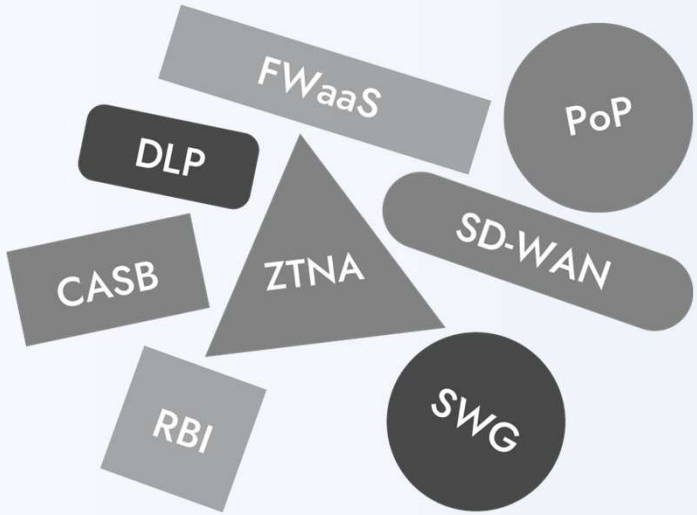
最短2週間のカンタン導入！

© AMIYA Corporation

Veronaのポイント2　“運用負荷 ゼロ”

障害対応や設定変更など、日々の運用・管理をセキュリティのプロが代行。
運用負荷なくネットワークセキュリティを運用できます。

一般的なSASE



SASEの各機能の運用・管理が煩雑。
必要以上の高機能を使いこなせない場合も。

Verona

運用・管理のすべてを行う
フルマネージドサービスでSASEの真価を発揮。

© AMIYA Corporation

Veronaのポイント3　“オールインクルーシブ”

Veronaはサービス費用に全ての費用がインクルード。
他社のSASE導入で必要となる高額なSI費用を含めた様々な費用が不要で、大幅なコスト減を実現。

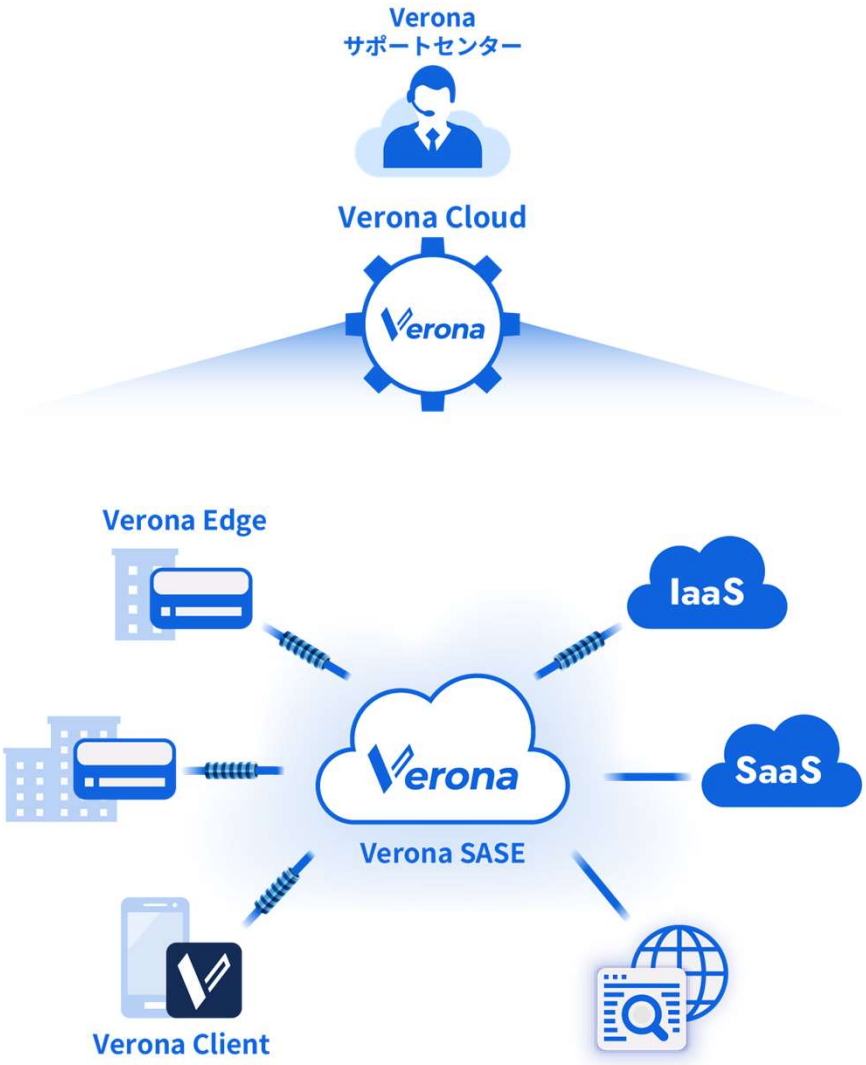
一般的なSASE導入費用

Verona

© AMIYA Corporation

Veronaの構成要素

Veronaは、ネットワーク、セキュリティ機能を提供するVerona SASE、SASEゲートウェイのVerona Edge、クライアントソフトのVerona Clientとそれらをコントロールする Verona Cloudから構成されます。



クラウドコントローラー（Verona Cloud）

Verona Client と Verona Edge、
SASEを管理
各種設定やステータス、ログ情報を
設定・確認可能
Veronaサポートセンターがコントロール

Verona SASE

ネットワーク機能、セキュリティ機能を
一つで提供

Verona Edge（SASEゲートウェイ）

拠点間の
安全なプライベートアクセスを提供する機器

Verona Client （クライアントソフト）

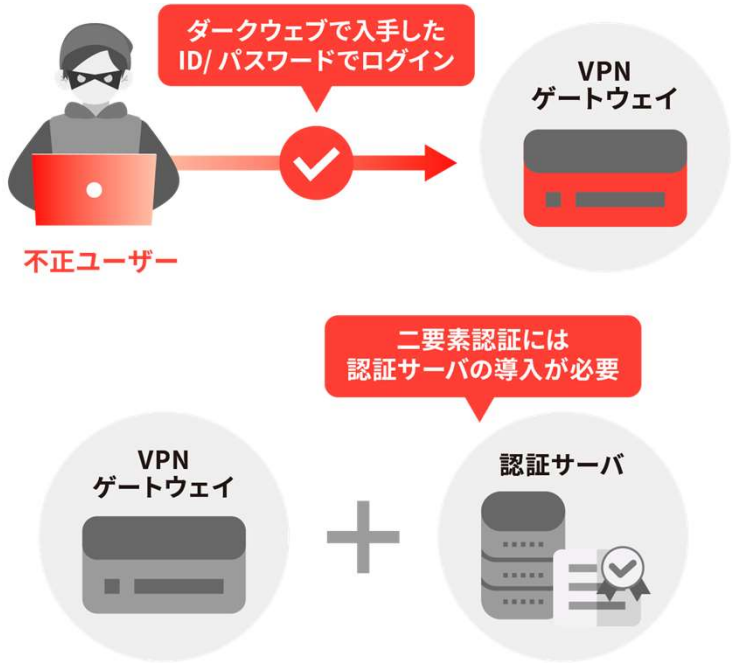
端末の安全なプライベートアクセスを提供する
ソフトウェア

© AMIYA Corporation

証明書認証による強固な認証

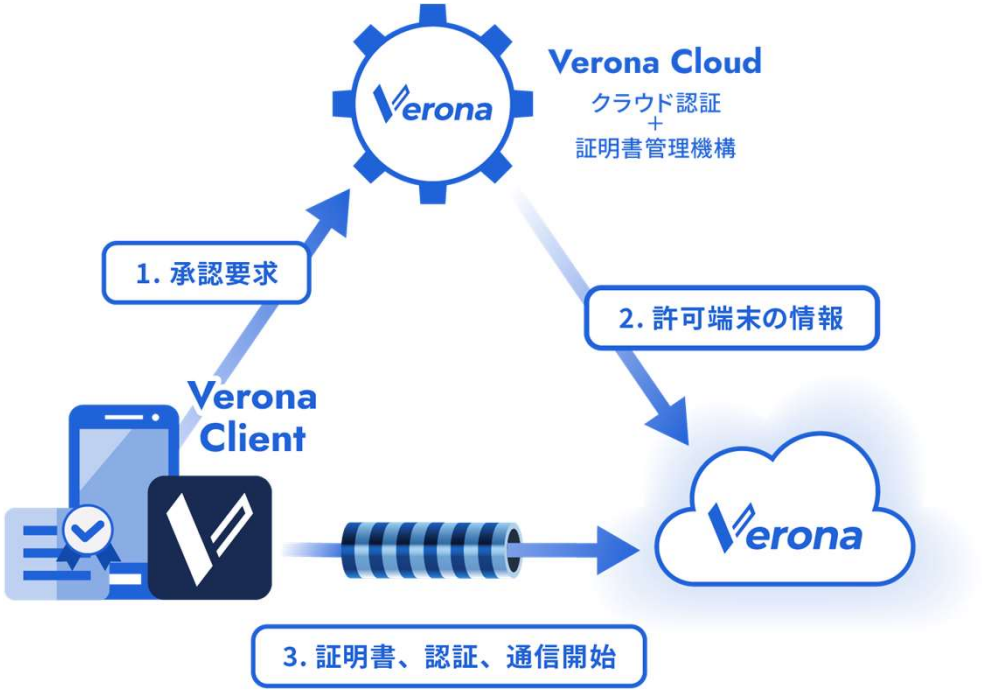
クライアント証明書をベースにした独自の認証システムで不正アクセスを防止します。

従来のVPN



ID/パスワード認証のみでは不十分。
しかし、認証強化には別途システムが必要。

Verona



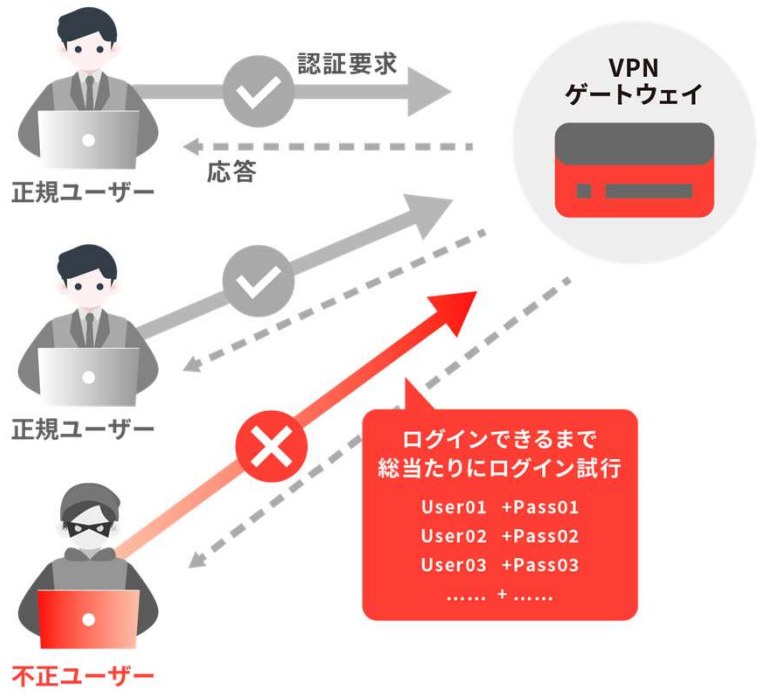
クライアント証明書認証を標準搭載。
Verona Cloudが証明書を管理。

© AMIYA Corporation

ダイナミックポートコントロール

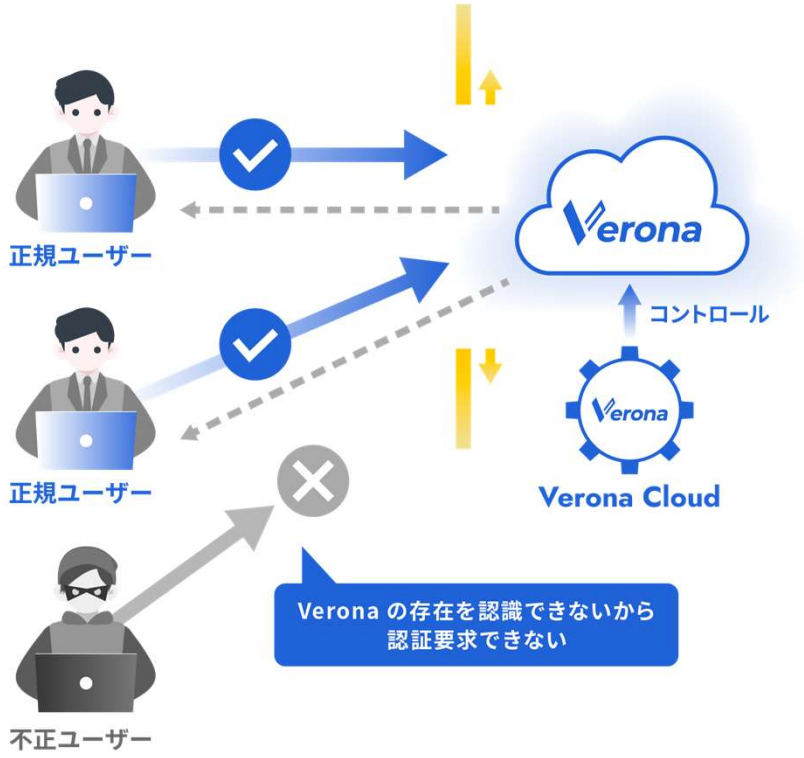
ダイナミックポートコントロール機能により、リモートアクセス環境の存在を隠し、
不正アクセスリスクを極めて最小にします。

従来のVPN



どのユーザーからの認証要求にも応答。
パスワードの総当たり攻撃で認証を突破されるリスクあり。

Verona



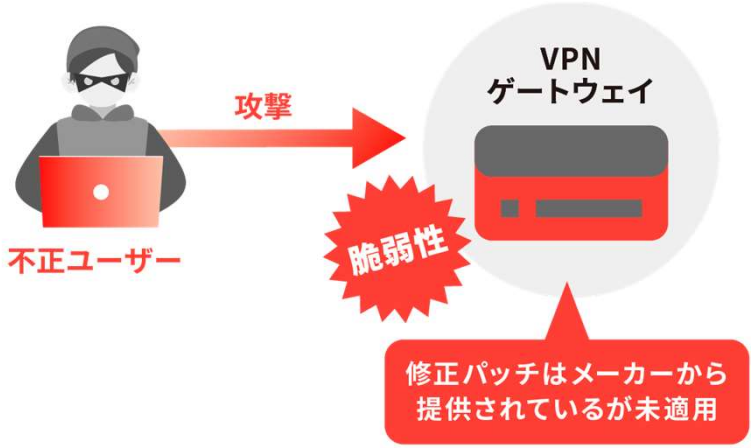
Verona Cloudと連携し、
正規ユーザーからの認証要求のみ応答。

© AMIYA Corporation

専門のエンジニアが脆弱性に対応

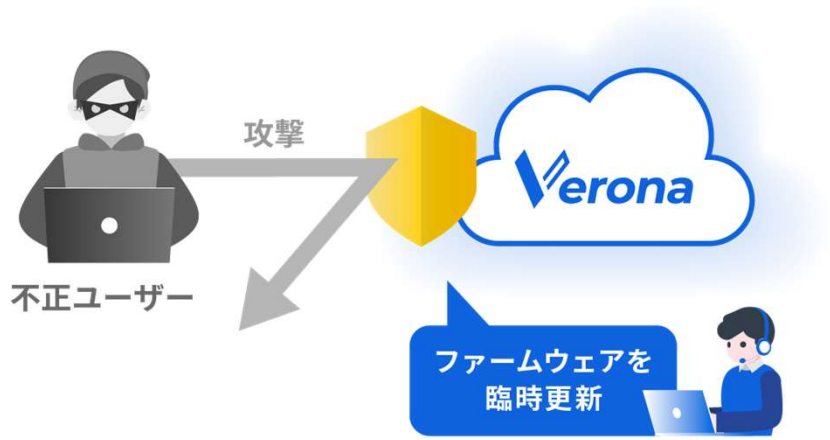
専門のエンジニアがファームウェアを随時更新します。

従来のVPN



セキュリティ強化で導入した多数の製品。
運用・管理に手が回らず、脆弱性から侵入を許してしまう。

Verona



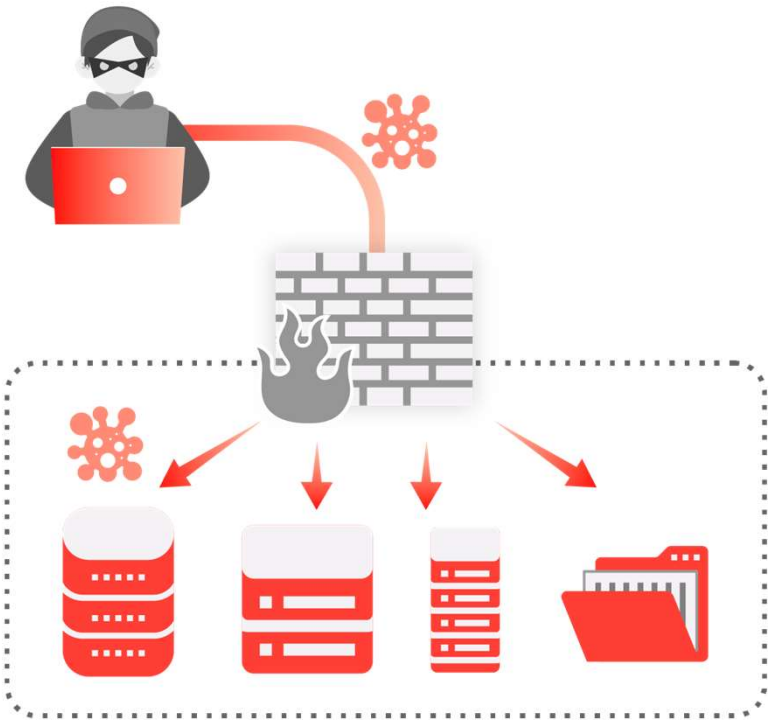
脆弱性が放置されないため、攻撃対象になりにくい。

© AMIYA Corporation

社内トラフィックも管理・監視

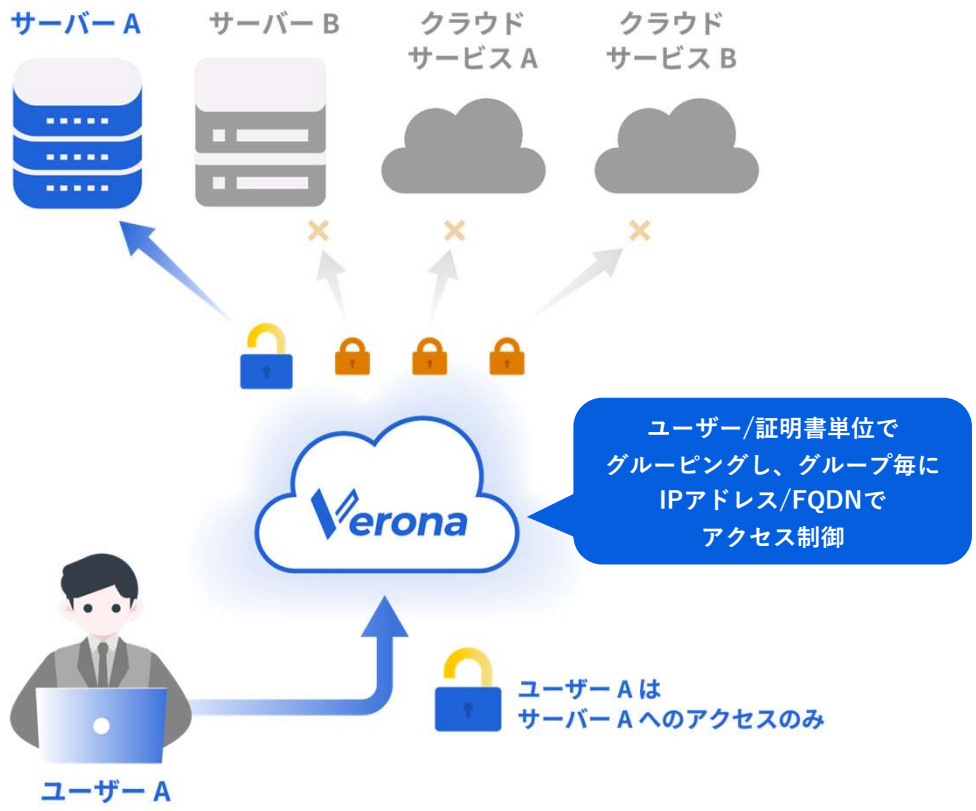
マイクロセグメンテーションにより社内もアクセス制御。
攻撃者侵入後の感染拡大を防止します。

従来のVPN



社内のアクセス制御がなされておらず、
一度侵入を許すと全システムが侵害されてしまう恐れが。

Verona



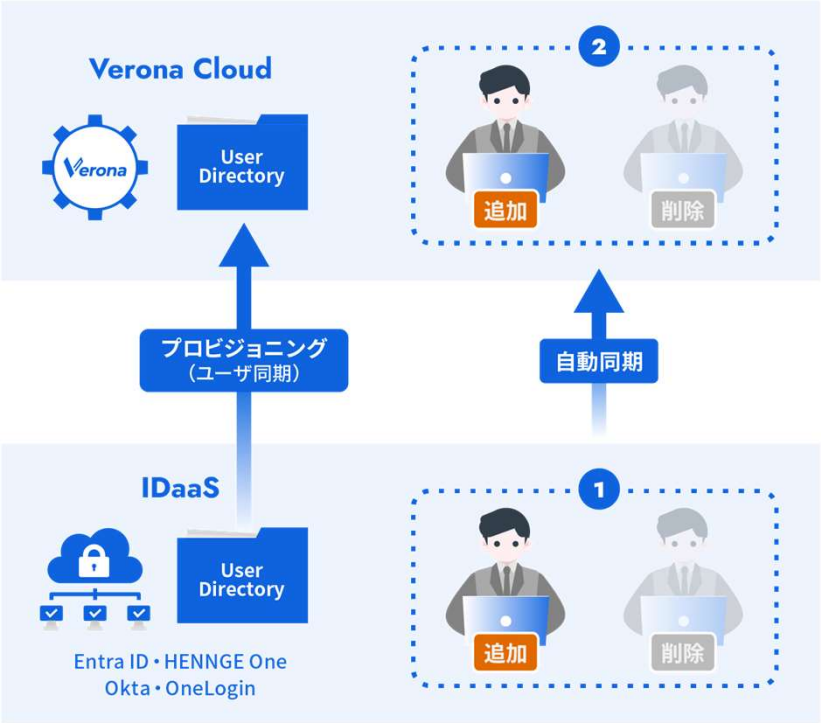
全てのネットワークアクセスを管理。
マイクロセグメンテーションにより、侵入後の感染拡大を防止。

© AMIYA Corporation

IDaaS連携でユーザ管理の効率化と認証強化

ユーザ情報を同期

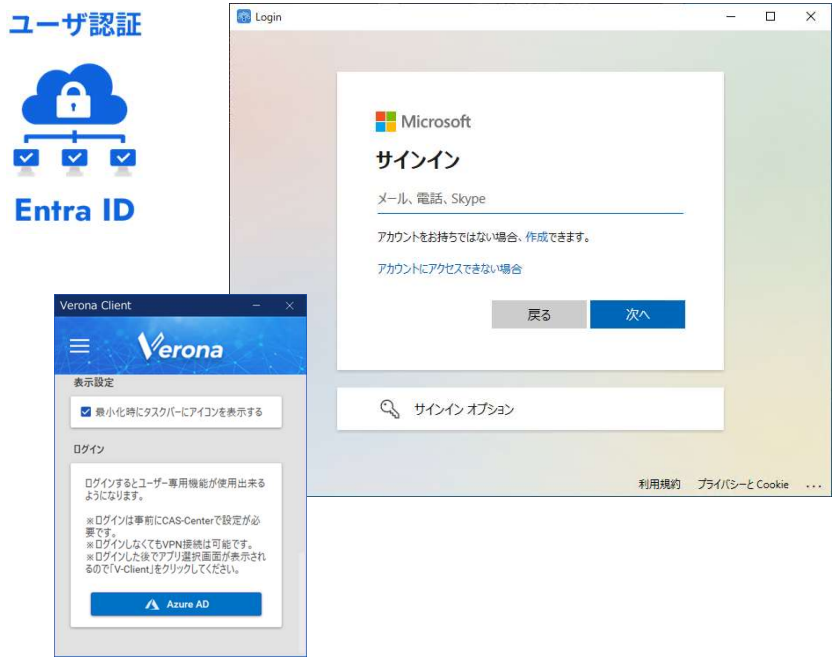
ユーザ管理をIDaaSに一本化。
ユーザ削除忘れによるセキュリティリスクを回避。



※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

IDaaS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

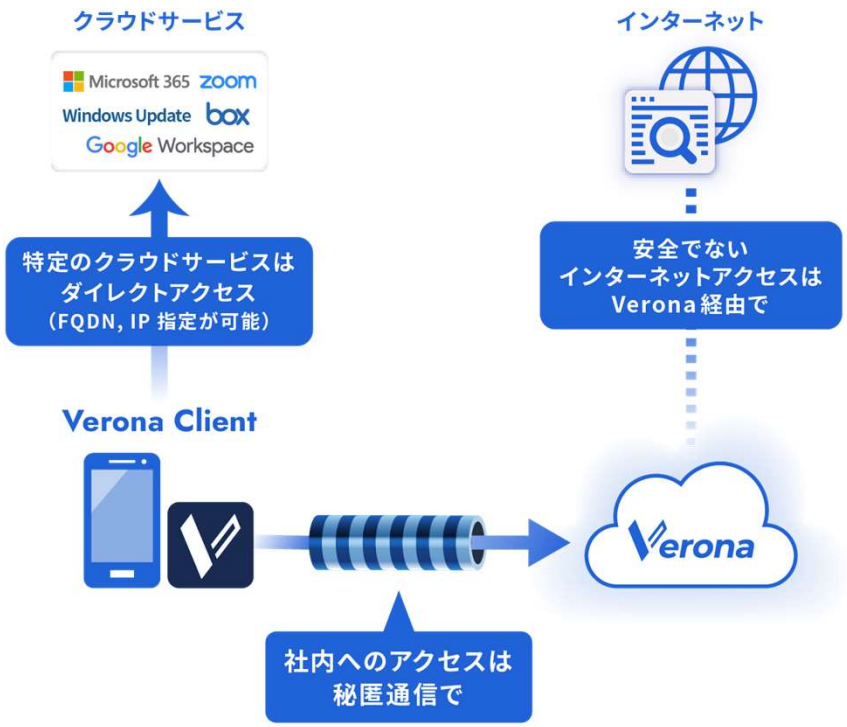
© AMIYA Corporation

最適な経路選択と負荷分散で通信ひっ迫を解消

オンプレミスのゲートウェイに回線が集中し、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、回線負荷を軽減・分散します。

ローカルブレイクアウト

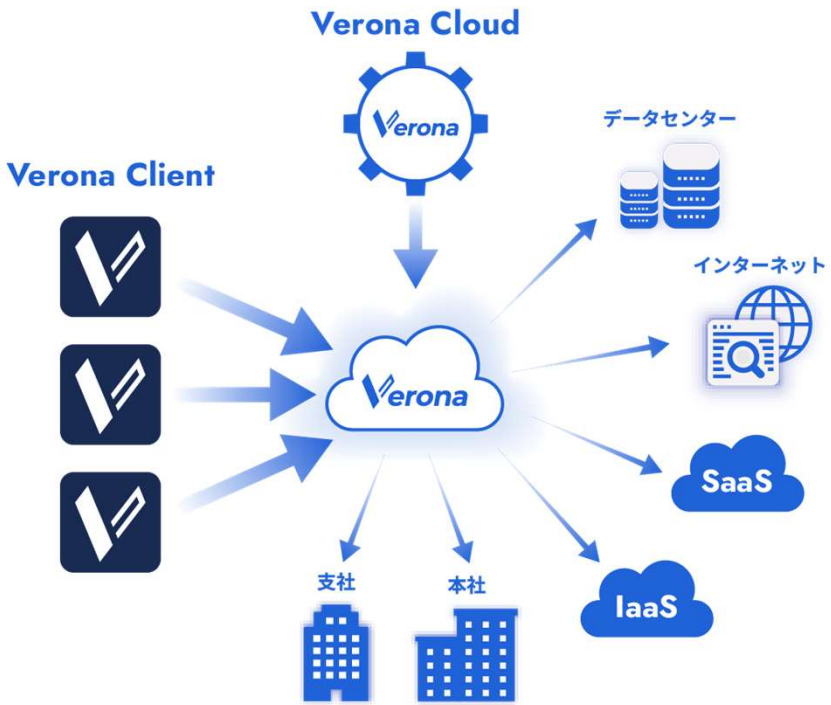
特定のクラウドサービスはダイレクトにアクセスさせることで
Veronaの回線負荷を軽減。



※本機能はWindowsのみ対応

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。



© AMIYA Corporation

包括的なセキュリティ対策を一つで

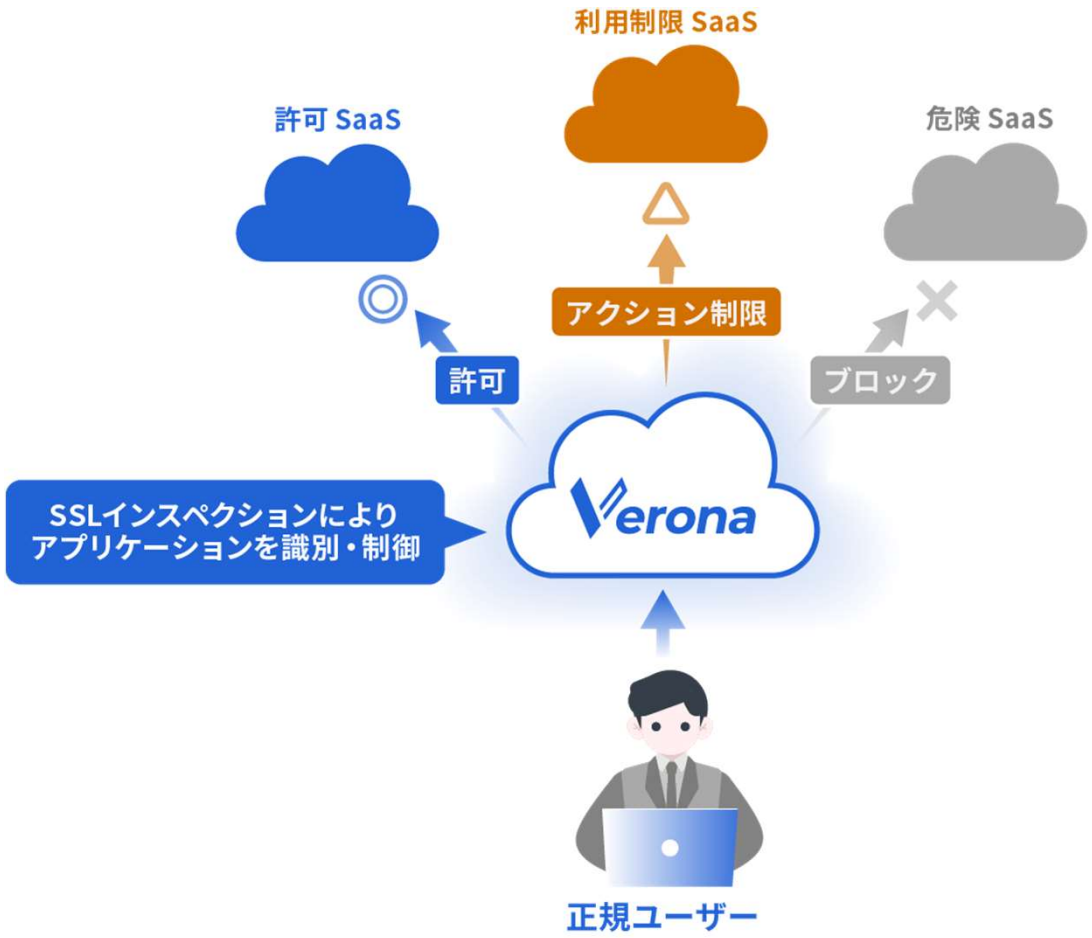
以下のすべてのセキュリティ機能をVeronaひとつで提供可能です。

© AMIYA Corporation

包括的なセキュリティ対策を一つで

クラウドセキュリティ：アプリケーションコントロール

アプリケーションの可視化・制御ができます。業務に必要なアプリケーションのみアクセスを許可したり、
情報漏洩の危険性があるアプリケーションの使用や、業務に無関係なアプリケーションの使用を禁止することができます。



4800以上のアプリケーションコントロールリスト

リストの例）
・Microsoft Teams
・Microsoft.Teams_File.Download
・Microsoft.Teams_File.Upnload
・Microsoft.Teams_Post
・Google Drive
・Google.Drive_File.Download
・Google.Drive_File.Upload
・Google.Drive_File.Sharing　　など

なぜアプリケーションの可視化・制御が必要なのか？

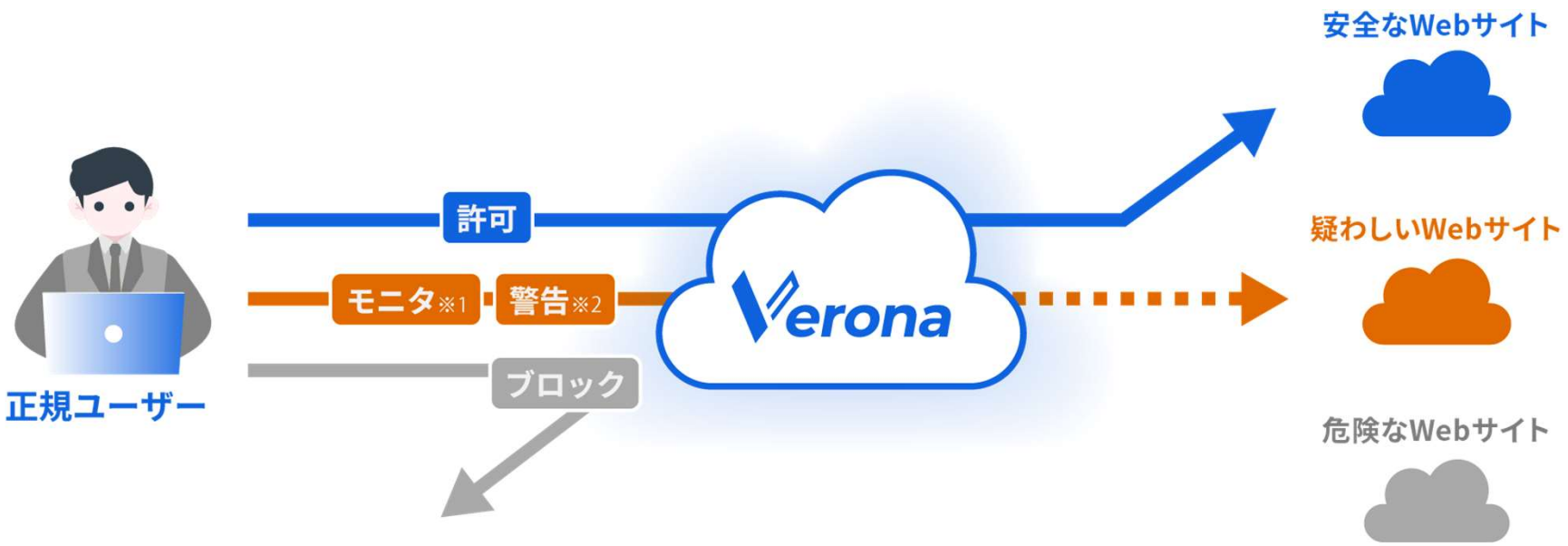
- 危険なアプリケーションの利用やシャドーITによる危険な通信（マルウェア感染や情報漏えい）を発見し、ブロックするため
- ユーザのアプリケーションの使用状況を把握することで、適切なアプリ管理により帯域を確保するため

© AMIYA Corporation

包括的なセキュリティ対策を一つで

Webセキュリティ①　URLフィルタリング

91のカテゴリに基づいてWebサイトへアクセスを監視、制御できます。
業務に不必要なサイトや危険なサイトへのアクセスをブロックすることで、マルウェア感染や情報漏えいを防ぎます。



URLフィルタリングにできること

ホワイトリスト/ブラックリスト設定により
個別のURLを許可/ブロック

数十億のWebサイトを分類したカテゴリに基づき
許可/ブロック

※1：通信を許可するが、アクセスコンテンツを含めログに出力。
※2：利用者のWeb画面上に警告メッセージを表示し注意喚起。

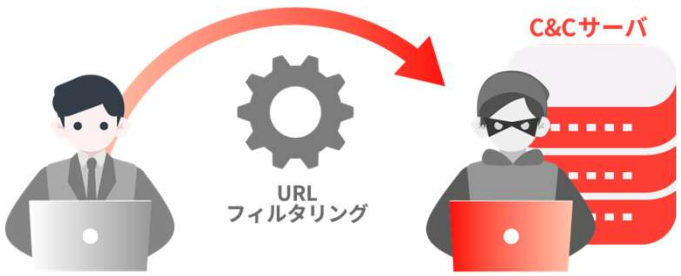
© AMIYA Corporation

包括的なセキュリティ対策を一つで

Webセキュリティ②　DNSセキュリティ

DNSレイヤーでのフィルタリングにより、プロトコルに依らない全ての通信をチェック。
マルウェアによる不正なDNS要求など、URLフィルタリングでは制御できないアクセスも制御できます。

URLフィルタリングのみ



Web系の通信以外をフィルタリングできず
危険なアクセスを許してしまう。

DNSセキュリティ

**URLフィルタリングを通過する悪性通信からも保護。
防御をさらに強固に。**

DNSトンネリング攻撃の防止にも！

DNSクエリを監視し、不正なクエリをブロックできるため、DNSクエリを悪用してC&Cサーバとの接続を確立するDNSトンネリング攻撃にも効果的！

ローカルブレイクアウトのセキュリティにも！

ローカルブレイクアウト時のWebフィルタリングとしても有効！インターネットへの直接アクセスでボトルネックが発生しにくい！

© AMIYA Corporation

包括的なセキュリティ対策を一つで

アンチウイルス・アンチスパム

高度な脅威検知エンジンにより、新たな脅威や進化する脅威にも対応し、ファイルベースの攻撃を防止します。

マルウェアの侵入経路に最も使用されるメール。
スパムメールの大幅な削減により、メール攻撃のリスクを抑制します。

ウイルスやスパイウェアなど、コンテンツレベルの脅威を検知・ブロックし、ネットワークを保護。メール添付された危険なファイルの実行等のリスクから保護します。

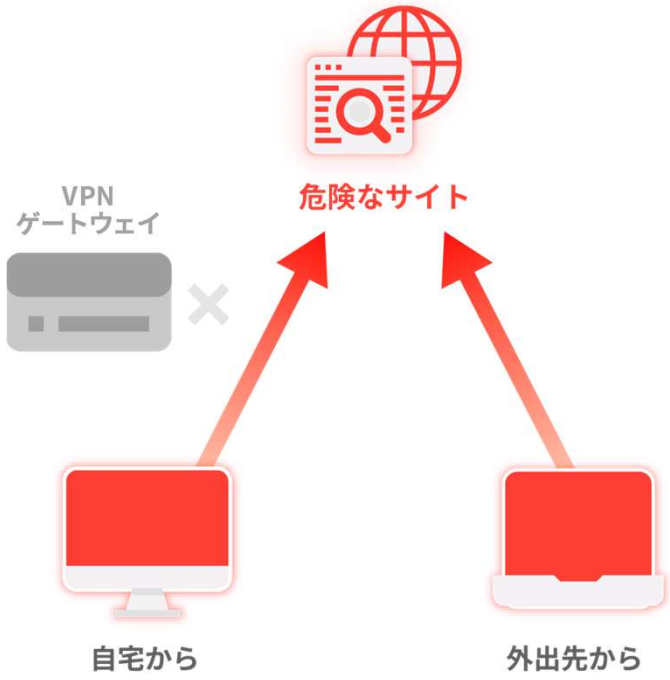
※Fortinet社の脅威検知エンジンを使用しています

© AMIYA Corporation

インターネットアクセスを常時制御

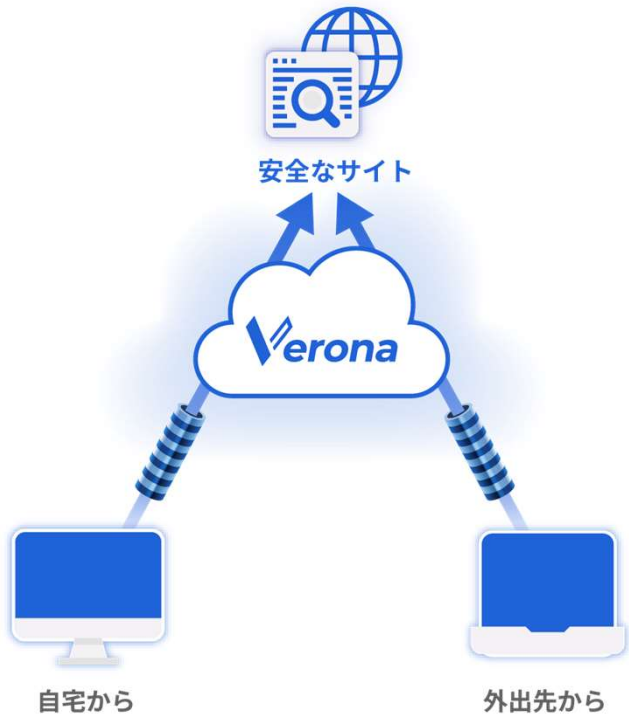
Verona SASEへの常時接続で、インターネットアクセスを常時制御。
社外から危険なサイトにアクセスしてしまうリスクから守ります。

従来のVPN



都度、手動で接続。
社外からのインターネットアクセスを制御できない。

Verona



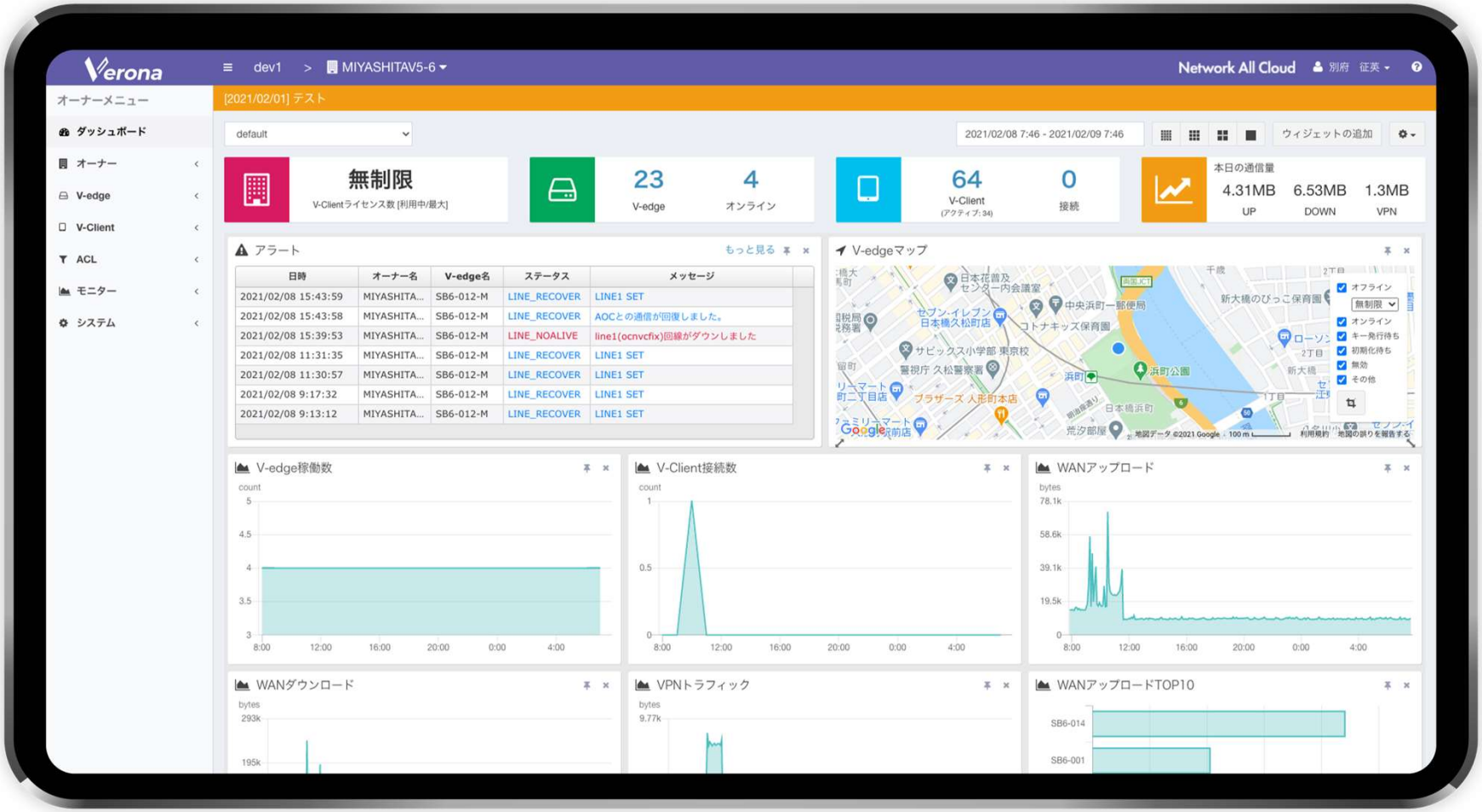
常時接続の強制が可能。
いつでもどこでもインターネットアクセスを安全に。

※本機能はWindowsのみに対応

© AMIYA Corporation

Verona Cloud Consoleで運用・管理をシンプルに

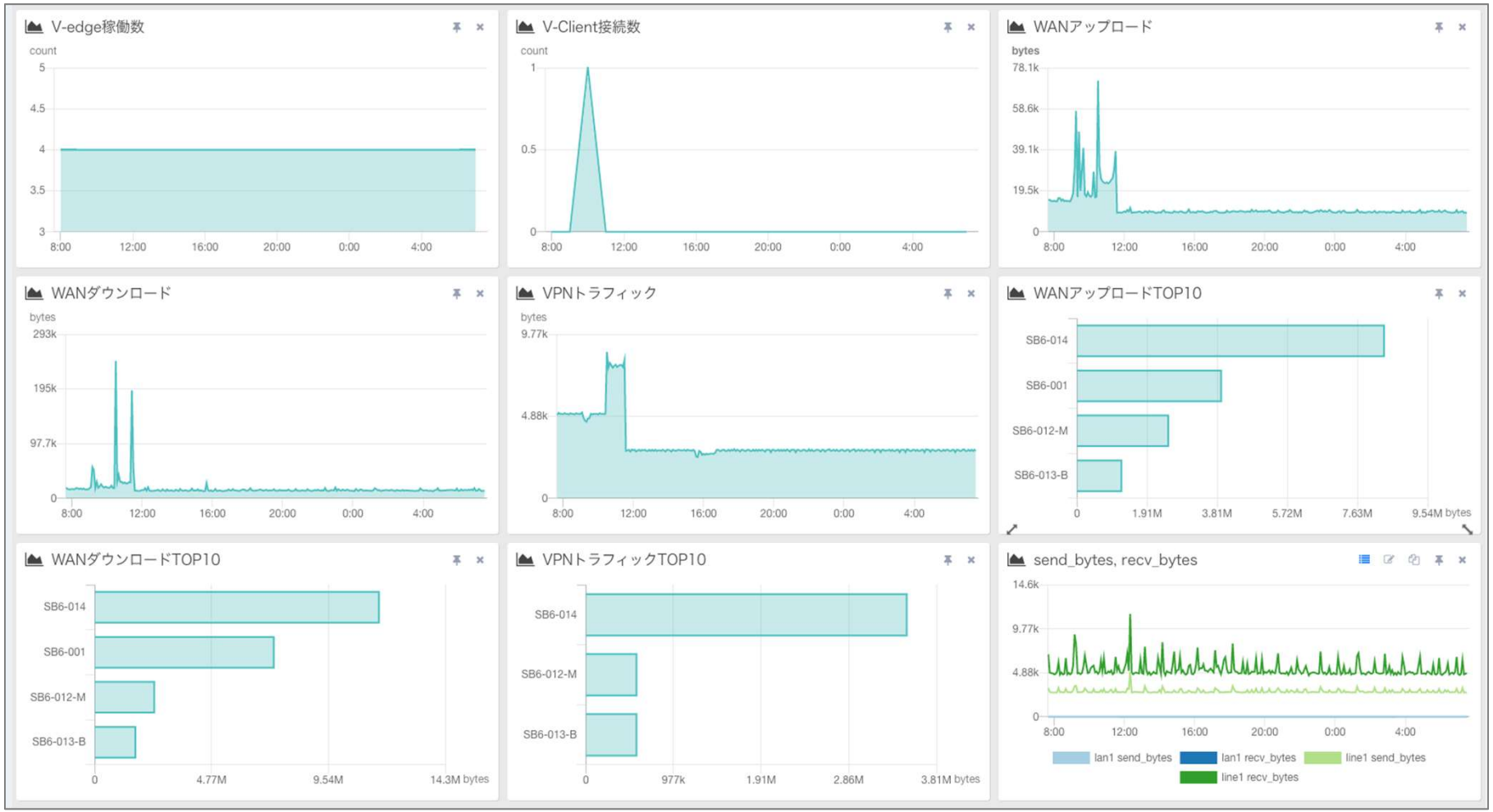
Veronaのあらゆるステータス情報をひとつに集約。
リモート拠点やテレワーク中のクライアントまで、スムーズに状況を把握できます。



© AMIYA Corporation

高負荷、遅延の発生箇所を特定

Verona Edge稼働数、Verona Client接続数、そして各インターフェースの通信量をグラフ化。
「東京本社の特定時間に通信量が多い」など高負荷の発生箇所を特定し、改善方法を導きます。



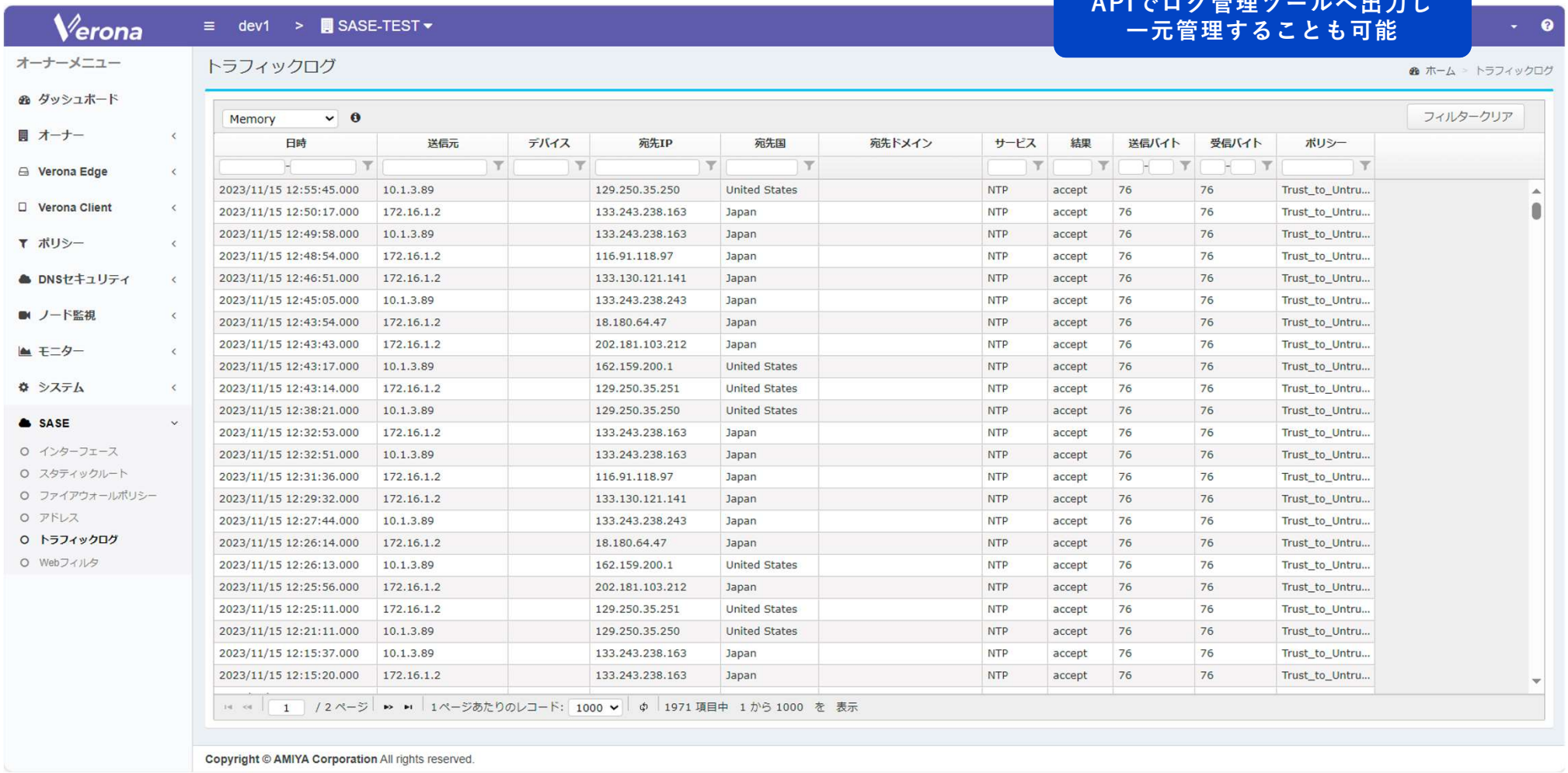
© AMIYA Corporation

Verona Cloud Console

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。

APIでログ管理ツールへ出力し一元管理することも可能



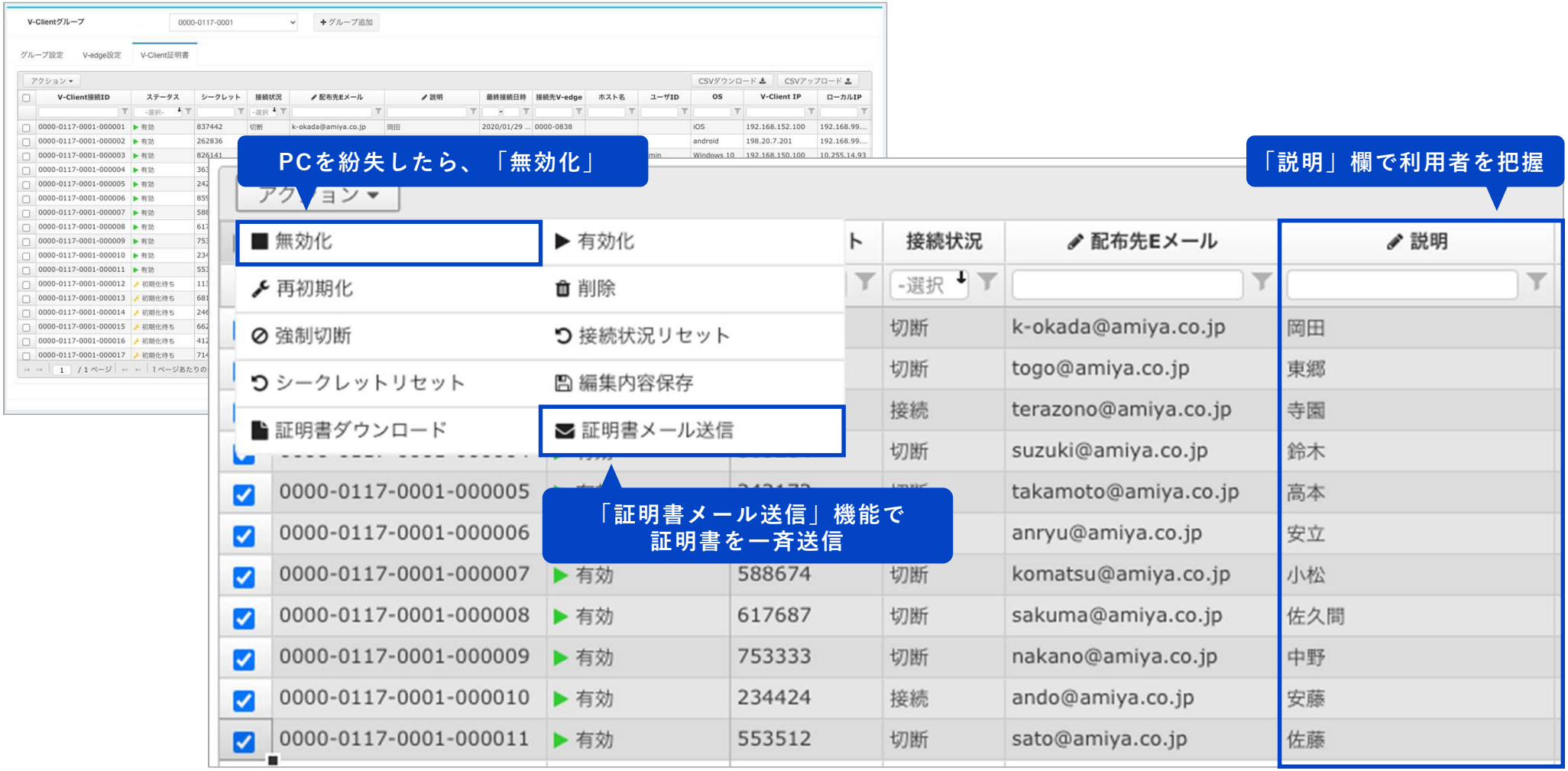
日時	送信元	デバイス	宛先IP	宛先国	宛先ドメイン	サービス	結果	送信バイト	受信バイト	ポリシー
2023/11/15 12:55:45.000	10.1.3.89		129.250.35.250	United States		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:50:17.000	172.16.1.2		133.243.238.163	Japan		NTP	accept	76	76	Trust_to_Untru...
2023/11/15 12:49:58.000	10.1.3.89		133.243.238.163	Japan		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...

© AMIYA Corporation

Verona Cloud Console

証明書管理をWebでラクラク

PC紛失時の接続拒否、PCリプレイス時の証明書の入替え/配布などが、
コントローラを構築することなく、Web上からSaaSで管理できます。



© AMIYA Corporation

セキュリティにこだわった運用体制

Verona

Veronaの運用体制は、クラウドセキュリティに関する国際規格である、ISO/IEC 27017認証を取得。
高度なセキュリティ要件を満たしたサービスで、安心してサービスをご利用いただけます。

ISMS取得の運用体制

bsi ISO/IEC 27017 Cloud Security Management CERTIFIED

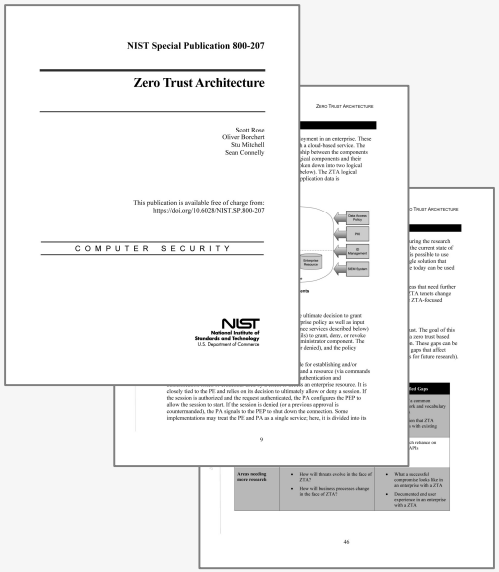
CLOUD 774562

ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 27001 MANAGEMENT SYSTEMS CERTIFICATION BODY / bsi / isms-AC ISMS ISR004

IS 502082 / ISO 27001

NIST SP800-207に準拠

NIST SP800-207
「ゼロトラスト・アーキテクチャ」



https://doi.org/10.6028/NIST.SP.800-207

JISA Awards 2020

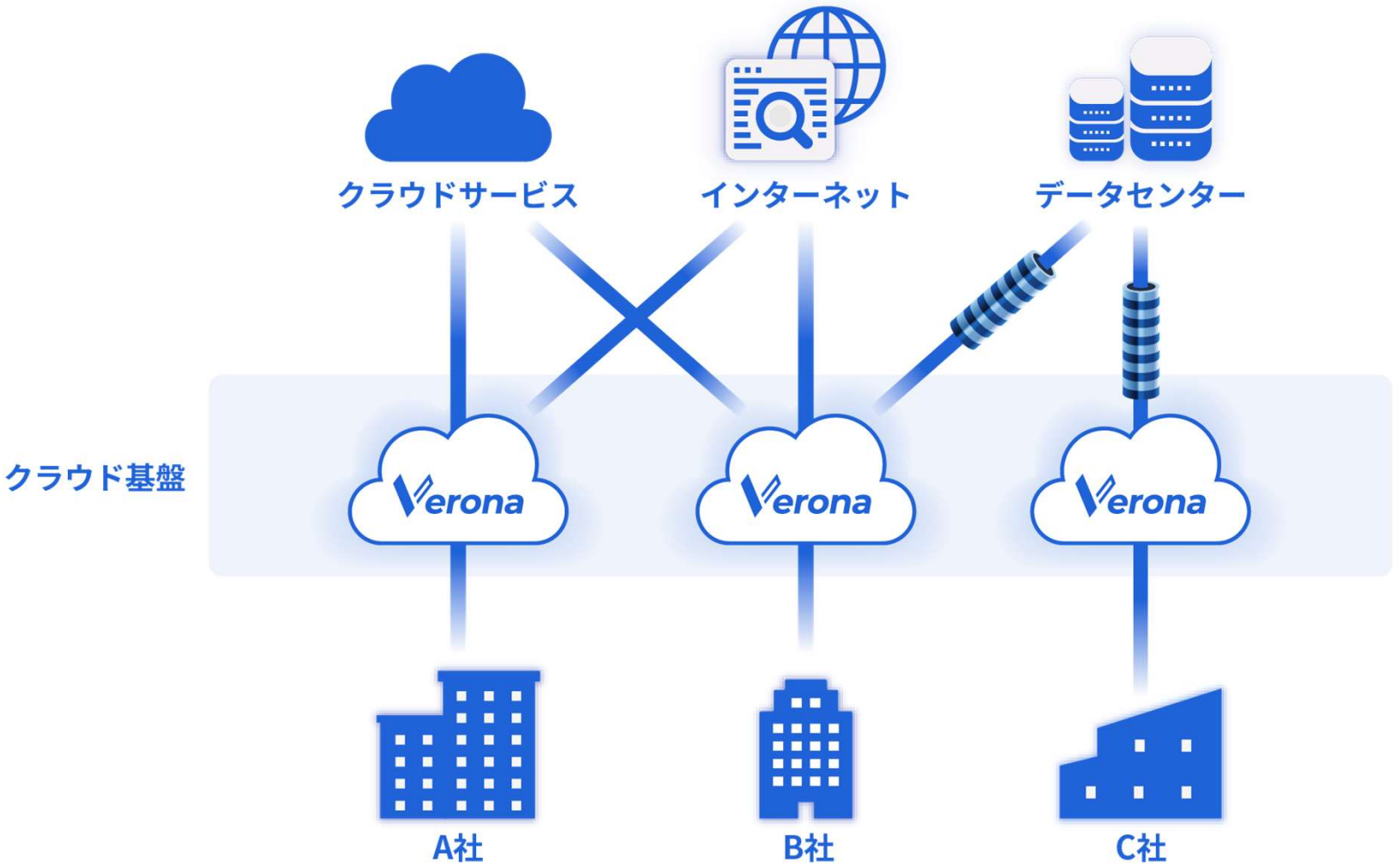
JISA AWARDS WINNER 2020

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

© AMIYA Corporation

安心の個別テナント

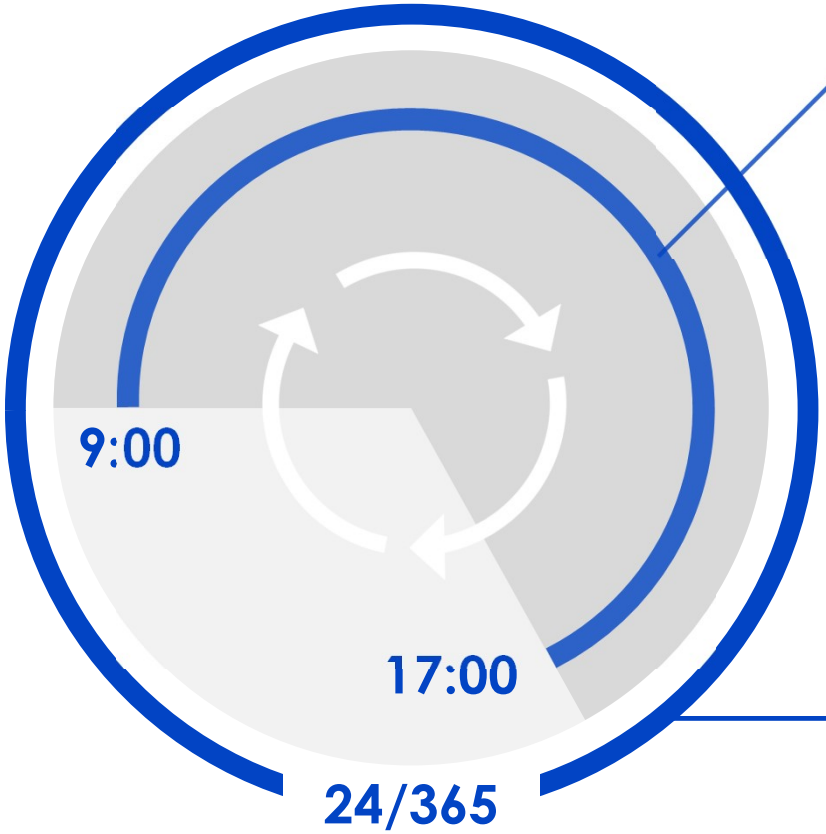
クラウド基盤上に、お客様ごとの個別テナントを作成し、固定のGIPを付与。
他のお客様と環境が分離されるため、セキュリティ面も安心です。



© AMIYA Corporation

サポート体制

サポート対応時間



通常サポート

- エンジニアサポート
- 故障機交換
  ※先出しセンドバック
- 障害対応・原因分析
- 機器設定変更対応

24/365オプション

- 夜間/休日の
  カスタマーサポート
- ファームウェアの
  自動更新

※電話・メール対応のみ
※24/365の詳細は別紙案内を参照

© AMIYA Corporation

導入事例

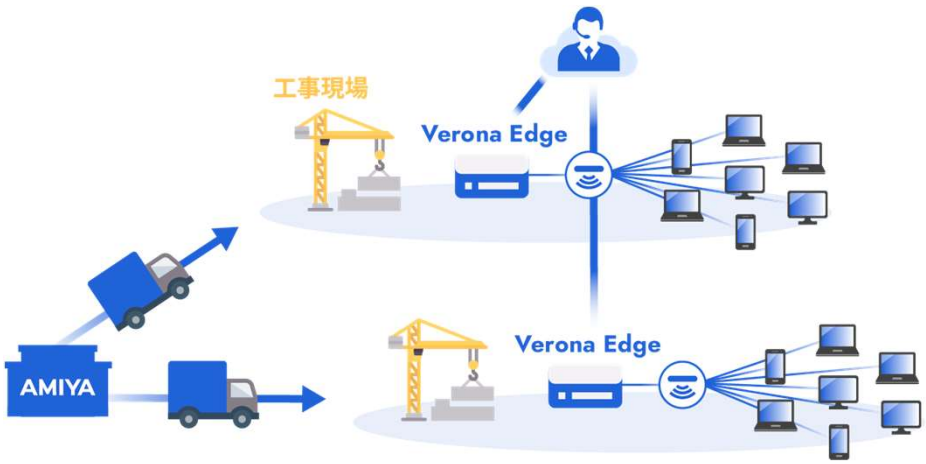
拠点間VPN

株式会社 熊谷組

人と地球の未来を考える 熊谷組

300超の拠点のITインフラを全てクラウドから遠隔管理

課題	導入効果
有期的な拠点のITシステムの整備が大変。	設置・撤去のしやすさで、有期的なITインフラの整備が楽に。
300を超える拠点のITシステムの運用に手が回らない。	無線LAN・ルータのすべてをクラウドから遠隔管理。
管理のアウトソースでコストがかさむのが心配。	リソース・労力の観点からしても納得のコストパフォーマンス。



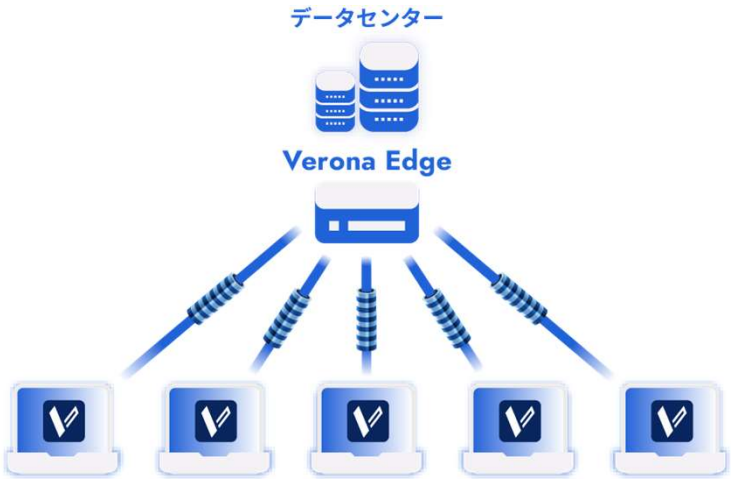
リモートアクセスVPN

ホーチキ 株式会社

HOCHIKI

2週間で2000人のテレワーク環境を整備
導入後も運用サービスで安心

課題	導入効果
コロナで全社員テレワークになり、環境整備が急務に。	2週間で申し込みから利用まで完了。
ID・Passwordの認証では、セキュリティレベルが…	クライアント証明書認証で高セキュリティ。
急なシステム導入で、運用が懸念。	運用サービス付きだから安心。



© AMIYA Corporation

導入事例

リモートアクセスVPN（オンプレサーバーなし）

株式会社マクアケ
Makuake,Inc.

Makuake

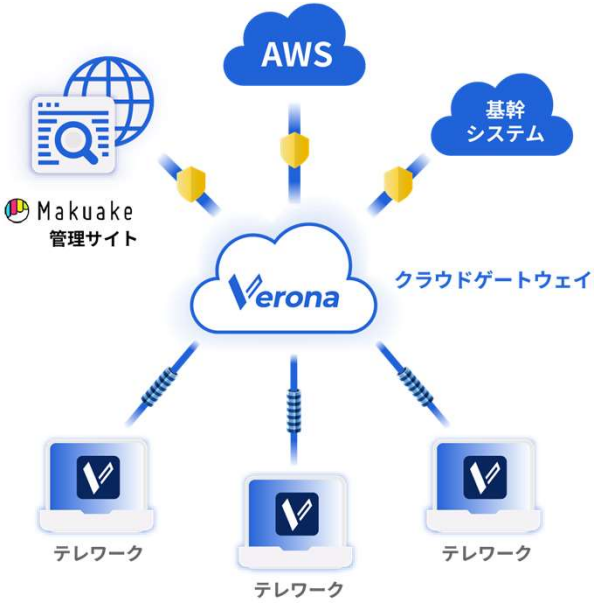
ハードウェアレス網を構築。テレワークのネットワーク環境を快適に

課題

- 使用人数が多く、速度が遅い。
- システムのハードウェア管理をしたくない。
- 今までのVPN機器は、セットアップが大変。

導入効果

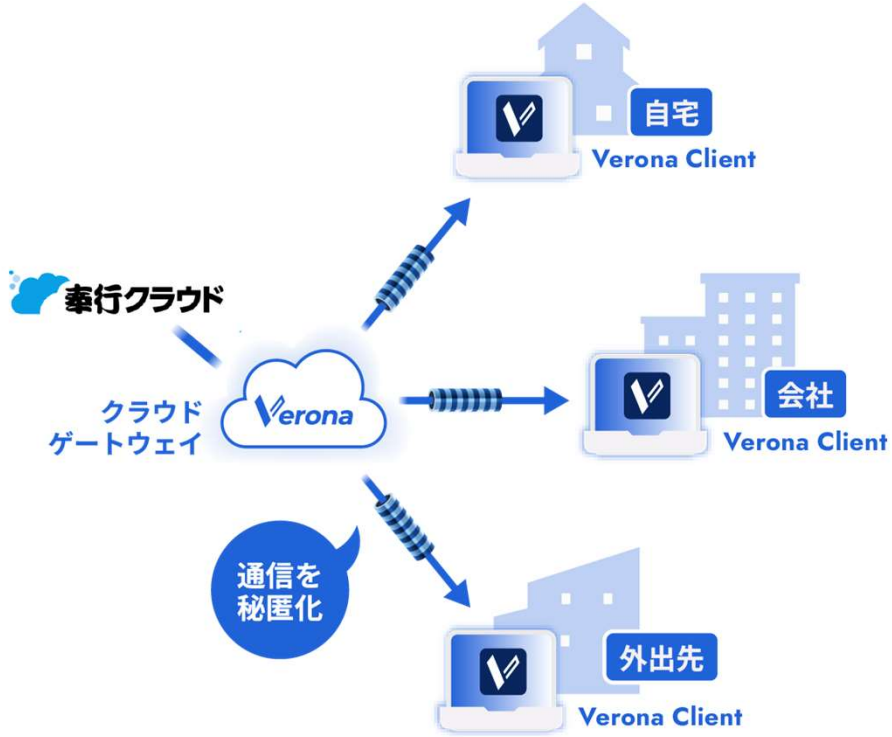
- Veronaへ全て切り替わって、ネットワークが快適になった。
- ハードウェアレスで管理不要になった。
- カンタン３ステップで完了。



SaaS 連携

オービックビジネスコンサルタント（OBC）様

奉行クラウド × Verona



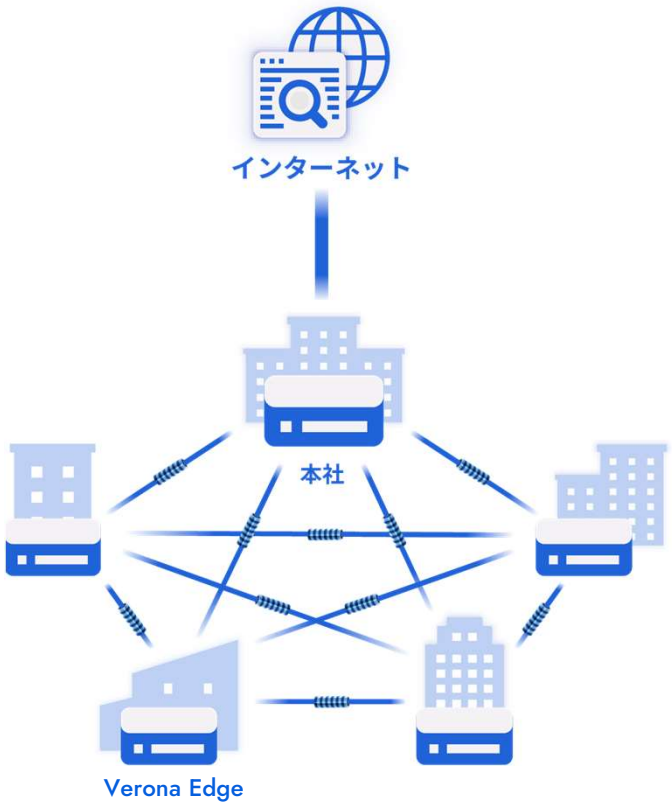
クライアント証明書をインストールしたデバイスのみ
『奉行クラウド』『OBCクラウドサービス』を利用開始

© AMIYA Corporation

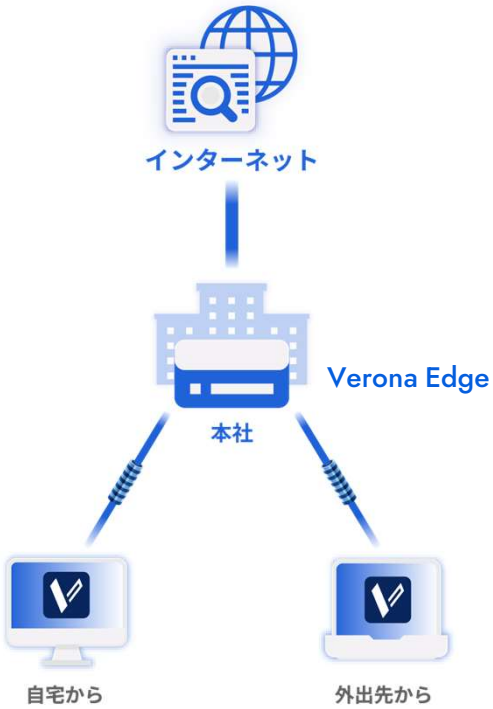
Verona構成例

目的に合わせてメニューをご提案いたします。

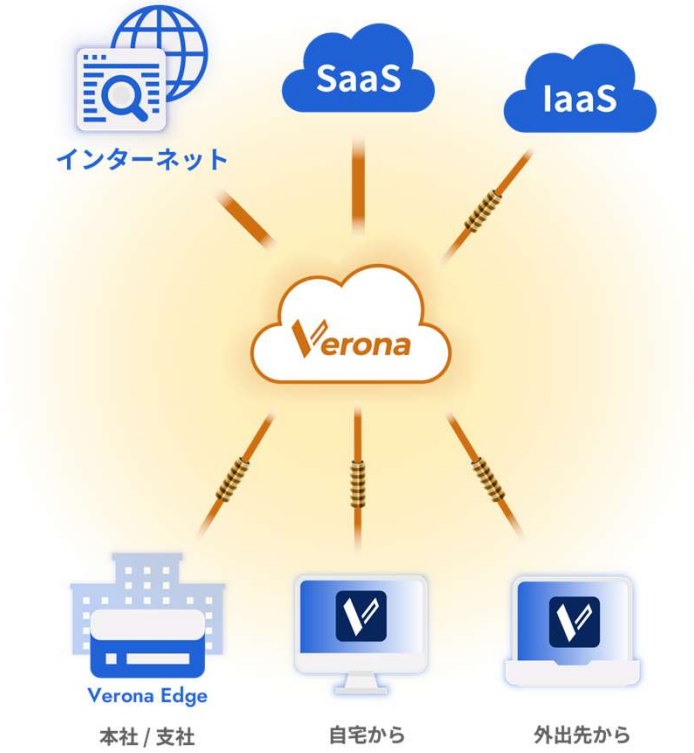
拠点間VPN



リモートアクセスVPN



Verona SASE



© AMIYA Corporation

Verona SASE ラインナップ

お客様のご利用規模に合わせて3つのタイプからご選択いただけます。
また、1000人以上規模でご利用の場合は、ご自由に「カスタム」が可能です。

	ベーシック	スタンダード	ハイスペック	カスタム
ユーザー数	100ユーザー未満	100-500ユーザー	500-1000ユーザー	1000ユーザー～
クライアントソフト Verona Client ライセンス数	100	300	500	-

※クライアントソフト Verona Clientは有償でライセンス追加可能です。　※拠点側ゲートウェイ Verona Edgeをご利用の場合は別途費用がかかります。

© AMIYA Corporation

Verona Edge ラインナップ

	ベーシックタイプ	スタンダードタイプ	ハイスペックタイプ	ソフトウェアタイプ	クラウド ゲートウェイタイプ	
VPNスループット	120Mbps	120Mbps	950Mbps	システム環境に依存	100Mbps ※回線速度に依存	200Mbps ※回線速度に依存
FWスループット	500Mbps	500Mbps	1Gbps	システム環境に依存	100Mbps ※回線速度に依存	200Mbps ※回線速度に依存
Verona Client 推奨同時接続数	10	100	200	100	100	100
Verona Client ライセンス発行上限数	10	無制限	無制限	無制限	無制限	無制限

© AMIYA Corporation

プロフェッショナルサービス

ご要望を丁寧にヒアリングし、セキュアなSASE環境の構築をご支援いたします。

ご支援内容

- **ご要望のヒアリング**
- **既存環境の調査** ※1
  - Configの確認
  - 既存構成図の確認　等

→

- **SASE環境構築支援**
  - NW設計のコンサルティング
  - ヒアリングに基づいた各種ポリシー設定

※ オンサイトでの作業はサービス範囲外です。　※1　対応ベンダーはYAMAHA、Cisco、Fortigate等

© AMIYA Corporation

無料トライアル受付中！

Veronaのすべての機能を最大30日間無料でお試しいただけます。

ヒアリングシートの記入のみでご利用開始！

ヒアリングシートのご記入	最短2週間 AMIYA 構築作業を実施	最大30日間 無料トライアル	約2週間 AMIYA 本番移行作業を実施	ご利用開始!

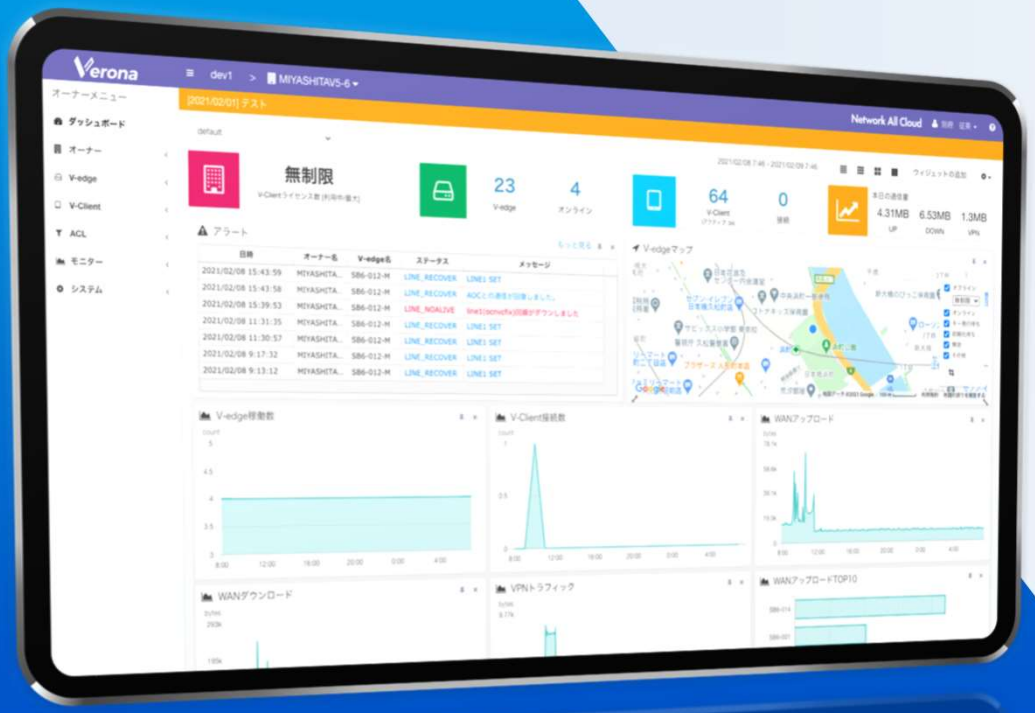
各段階にてネットワークセキュリティのプロが手厚くサポート

今すぐお申込み

※ご利用サービスによってトライアル期間が異なります。
※トライアル期間が終了すると環境がリセットされるため、本番環境への引き継ぎをご希望の場合はトライアル期間内にご契約ください。

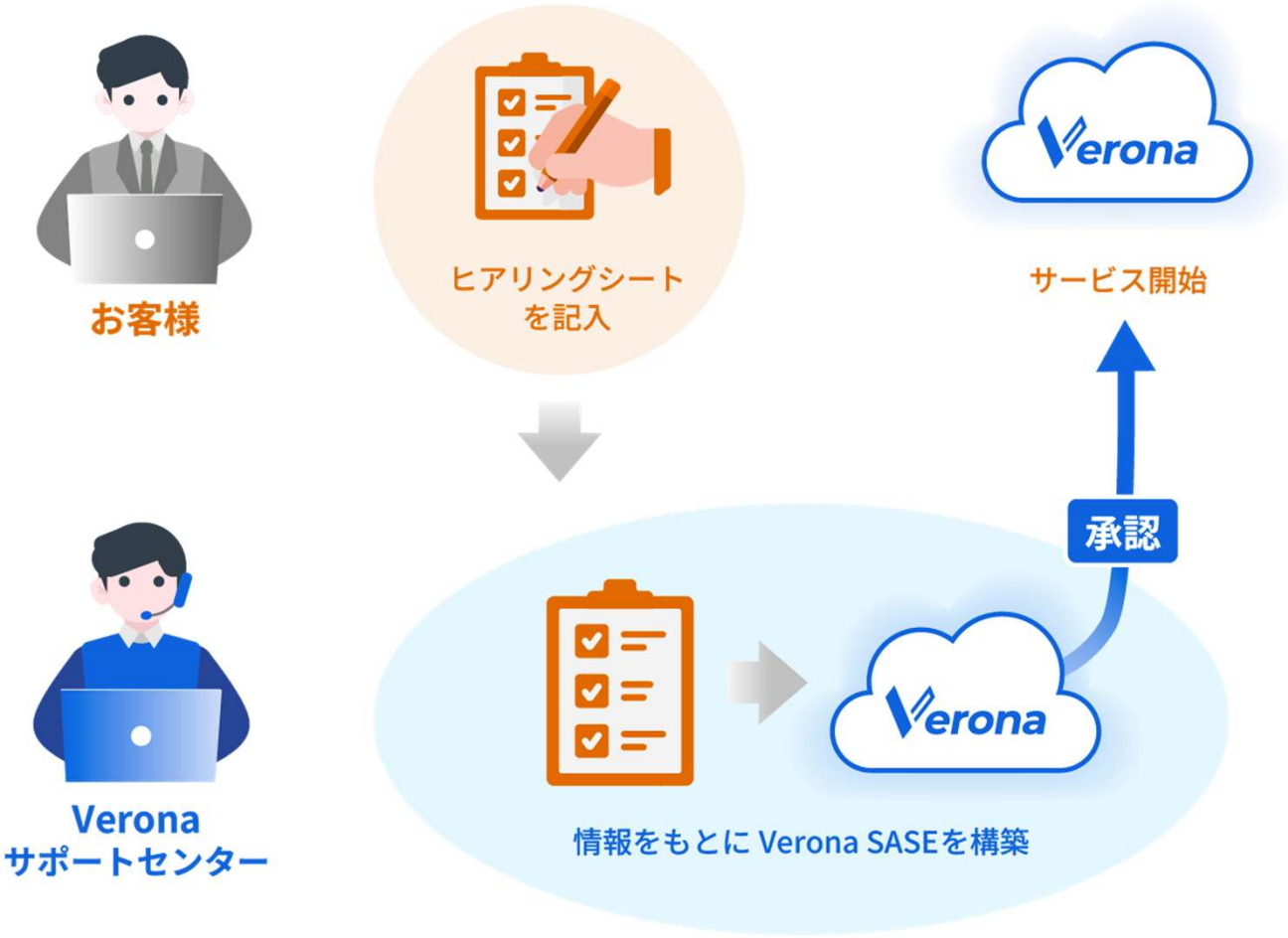
© AMIYA Corporation

Verona


Verona
dev1
MIYASHITAV5-6
Network All Cloud
無制限
23
4
64
0
4.31MB
6.53MB
1.3MB

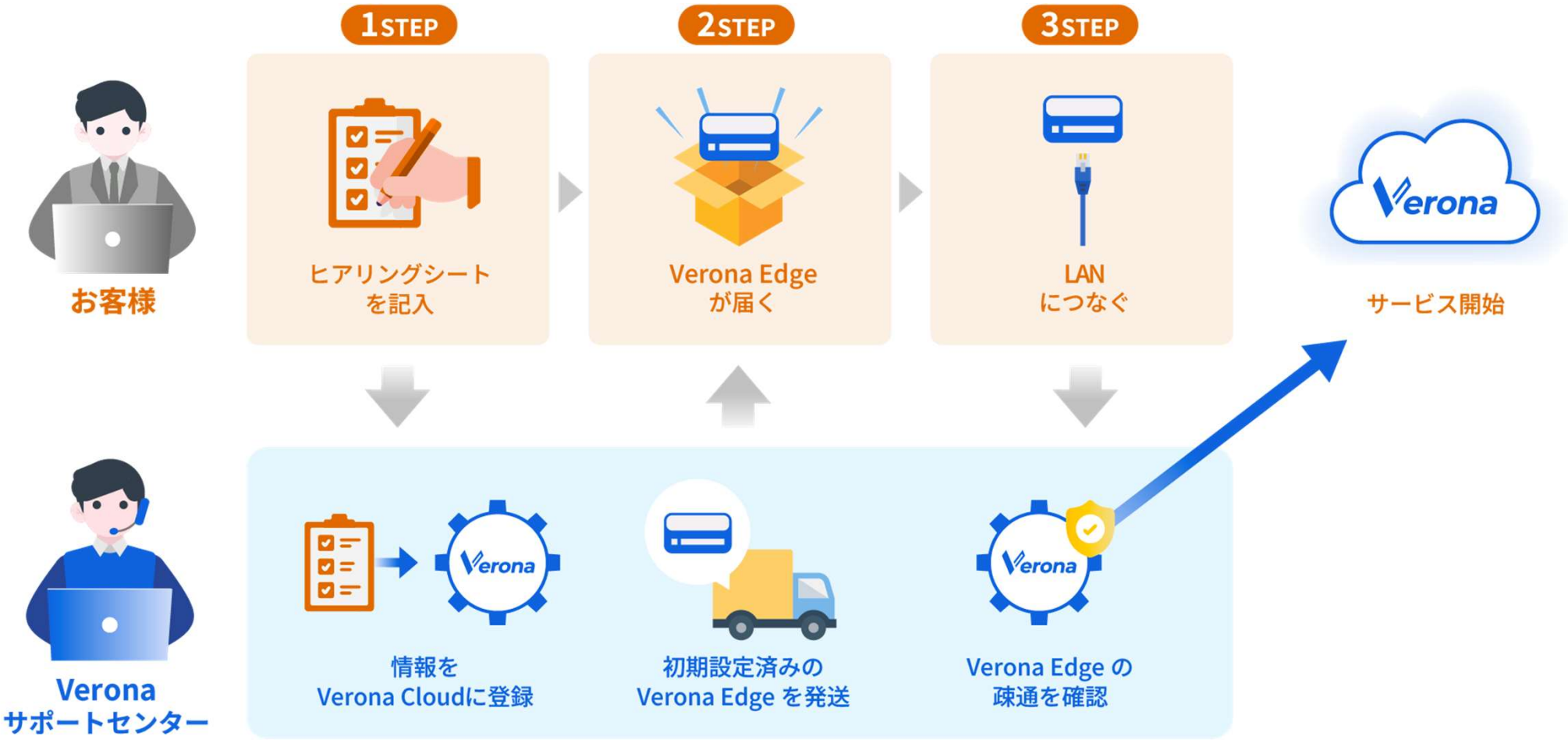
参考資料

Verona SASE導入ステップ



© AMIYA Corporation

Verona Edge（SASEゲートウェイ）導入ステップ



※ネットワーク構成によっては、上位FWの設定変更が必要です。

© AMIYA Corporation

Verona Client（クライアントソフト）導入ステップ

© AMIYA Corporation

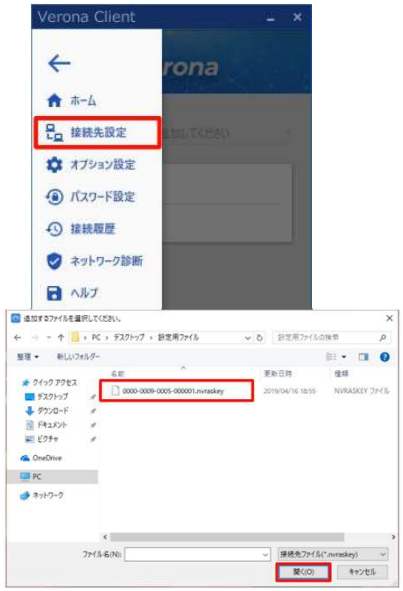
Verona Clientのインストールと初期設定

STEP 1

Verona Clientを
インストール

STEP 2

接続先の設定
証明書の登録



STEP 3

シークレット
(数字６桁)を入力

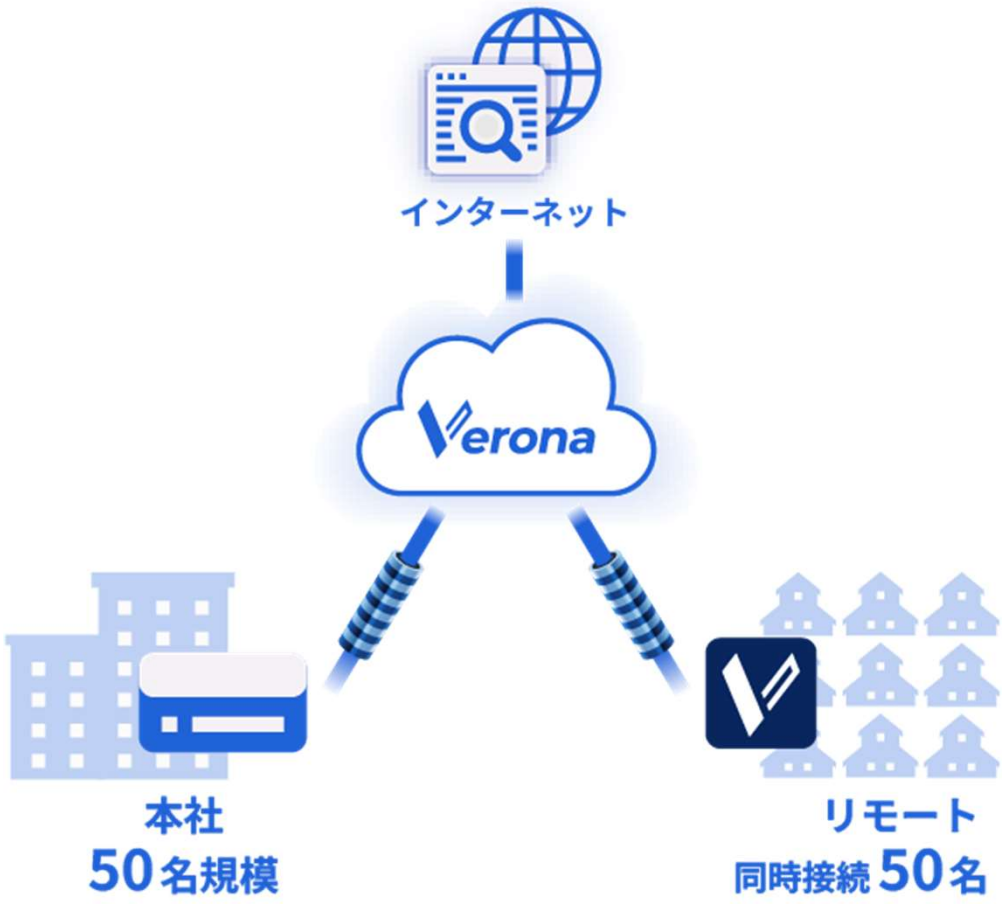
STEP 4

「接続」をクリックして
利用開始

© AMIYA Corporation

選定基準

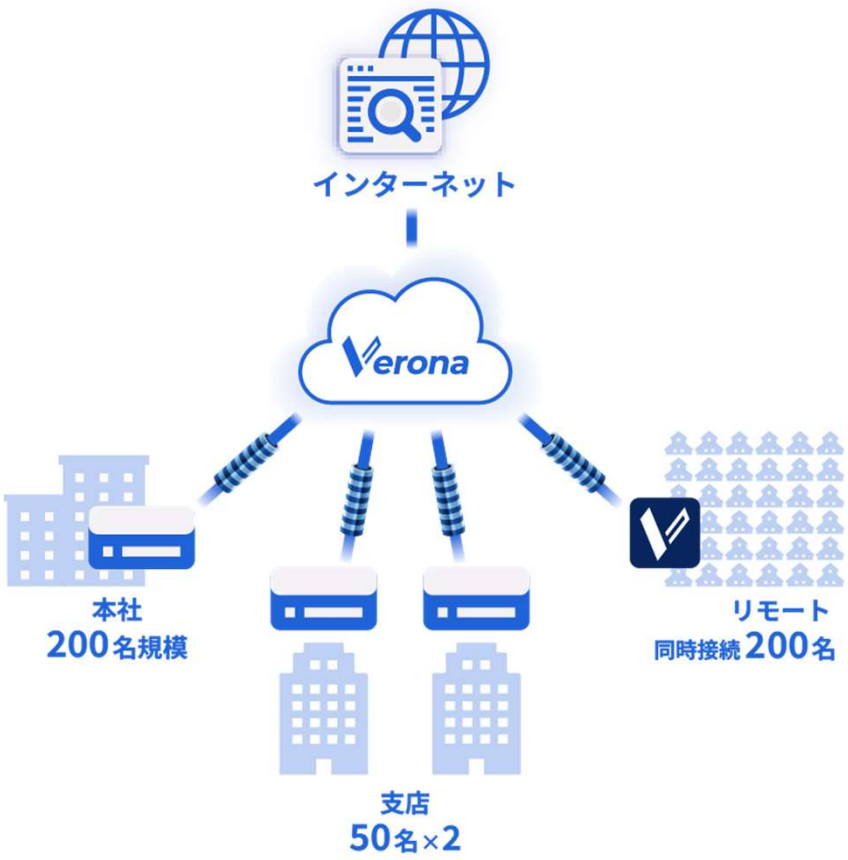
ベーシック



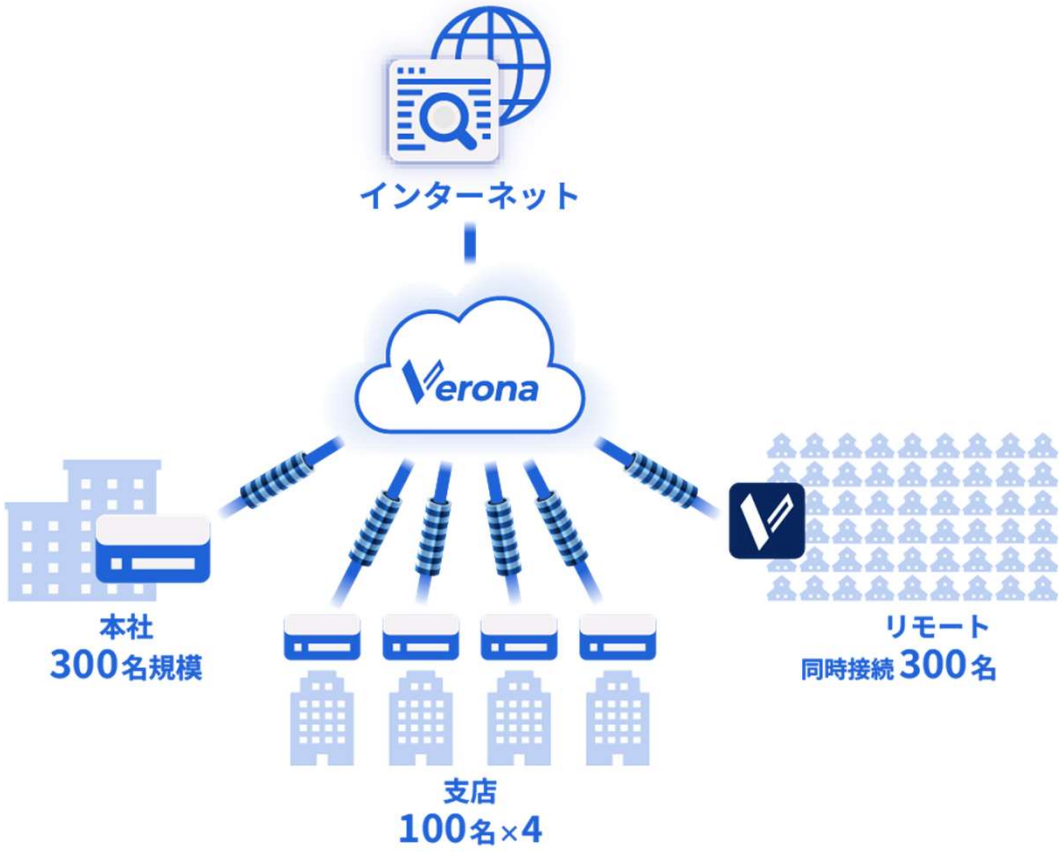
© AMIYA Corporation

選定基準

スタンダード

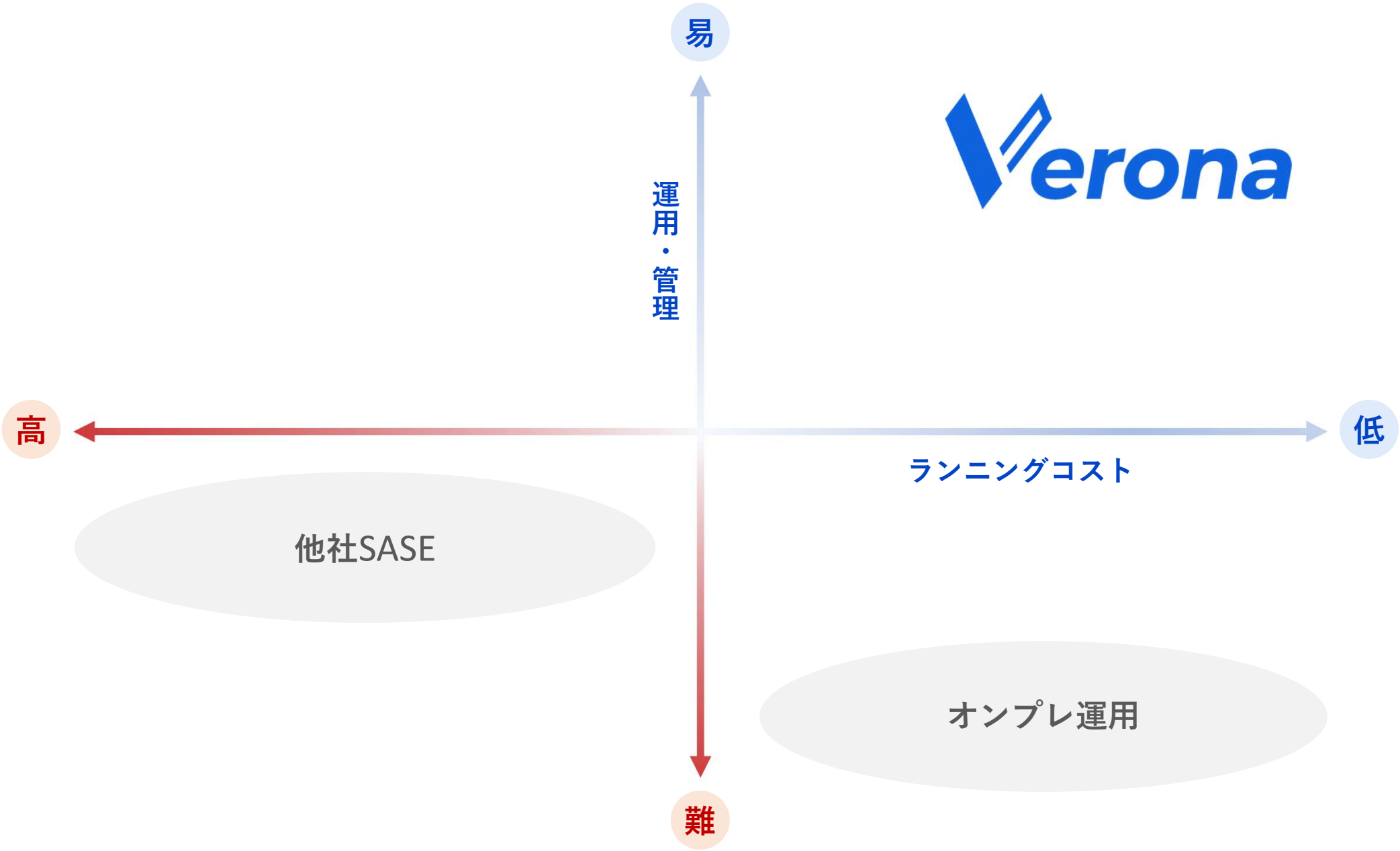


ハイスペック



© AMIYA Corporation

Veronaの位置づけ



© AMIYA Corporation

SASE競合比較

	Verona SASE	P社	Z社	C社	I社
概要	・導入前の初期設定から、導入後のメンテナンス、設定変更、障害対応までを遠隔でサポート ・機能を最低限に絞り、低コストで手軽に導入・運用可能	・XDRと連携して最高レベルの防御・検知・対処が可能 ・CASBやASMなど、様々なコンポーネントが連携可能	・プロキシベースでの制御により、既存のネットワーク環境への影響を極小化 ・ユーザ単位のライセンス体系により、帯域管理が不要	・使いやすい直感的な管理画面から、一貫したポリシーを簡単に適用可能 ・SASEの多様な機能を一つのプラットフォームで統合	・モバイル回線と自動接続機能の活用で、WANの高速展開を実現 ・仮想化された豊富な機能（NFV）との連携により、企業ネットワークの柔軟な拡張が可能
導入	◎ ・お客様作業はヒアリングシートの記入のみ ・初期設定は網屋で実施 ・初申し込み後最短２週間で導入完了	× ・POVの実施や構築作業など、導入完了までに半年以上を要する ・ベンダーによる構築作業に別途費用が発生する	× ・POVの実施や構築作業など、導入完了までに半年以上を要する ・ベンダーによる構築作業に別途費用が発生する	× ・POVの実施や構築作業など、導入完了までに半年以上を要する ・ベンダーによる構築作業に別途費用が発生する	△ ・初期設定はI社で実施 ・申し込みから機器送付まで約20-40営業日を要する
運用サポート	◎ ・電話・メール受付（オプションで24/365） ・メンテナンス、設定変更、障害対応までを遠隔でトータルサポート	△ ベンダーに依存	△ ベンダーに依存	△ ベンダーに依存	△ ・電話・メール受付（24/365） ・ヘルプデスクが各キャリア・メーカー保守業者と連携してサポート
ログ保管	◎ ・オプションで１年間のログ保管可能 ・ALogとの連携で任意の期間保管可能	◎ P社製品との連携で任意の期間保管可能	×	△ 最大6ヶ月保管可能	×
費用	◎ デバイス数に応じた３つのプランから選択 ・初期費用：50,000円～ ・月額費用：210,000円～	× ユースケース、エディションなどあらゆる要素の組み合わせ ※価格はベンダーに依存する	× 要件に応じた3つのプランから選択 ユーザー単位の課金 ※価格はベンダーに依存する	× 地域・帯域を選択 各機能は追加課金 ※価格はベンダーに依存する	△ ・初期費用：350,000円 ・月額費用：300,000円～（ネットワーク機能のみ）
導入する主な企業層	**運用負荷を抑えたい中小企業中心**	セキュリティ要件の高い大企業中心	運用要員の少ない中~大企業中心	グローバル展開する大企業中心	多拠点展開する中~大企業中心

© AMIYA Corporation

動作環境

Verona Client 動作環境

ソフトウェアをクライアント端末にインストールすることで、リモートアクセスが利用できるようになります。
クライアント端末ごとの動作要件は以下のとおりです。
※PCへのインストールにはOSの管理者権限が必要です。

Windows / Mac

OS	Windows 10 (32ビット版/64ビット版) Windows 11 (64ビット版) macOS (12.x、13.x、14.x)
動作環境	for Windows メモリ：1GB 以上（推奨） ディスク：200MB以上の空き容量を確保 for Mac メモリ：2G以上(推奨) ディスク：インストール先でドライブに600M以上空きがあること ※PCへのインストールにはOSの管理者権限が必要です。 ※ARM版Windows10は非対応となります。 ※Apple M1チップ搭載のMacに対応しています。

iPhone / iPad

OS	iOS 14.x、15.x、16.x iPadOS 14.x、15.x、16.x
Verona Client 入手方法	Apple App Storeより アプリケーション Verona Client（無料）をダウンロード

Android / Chromebook

OS	Android 9.x、10.x、11.x、12.x、13.x Chrome OS バージョン 62 以降
Verona Client 入手方法	Google Playより アプリケーション Verona Client（無料）をダウンロード

© AMIYA Corporation

動作環境

Verona Edge タイプ別動作環境比較

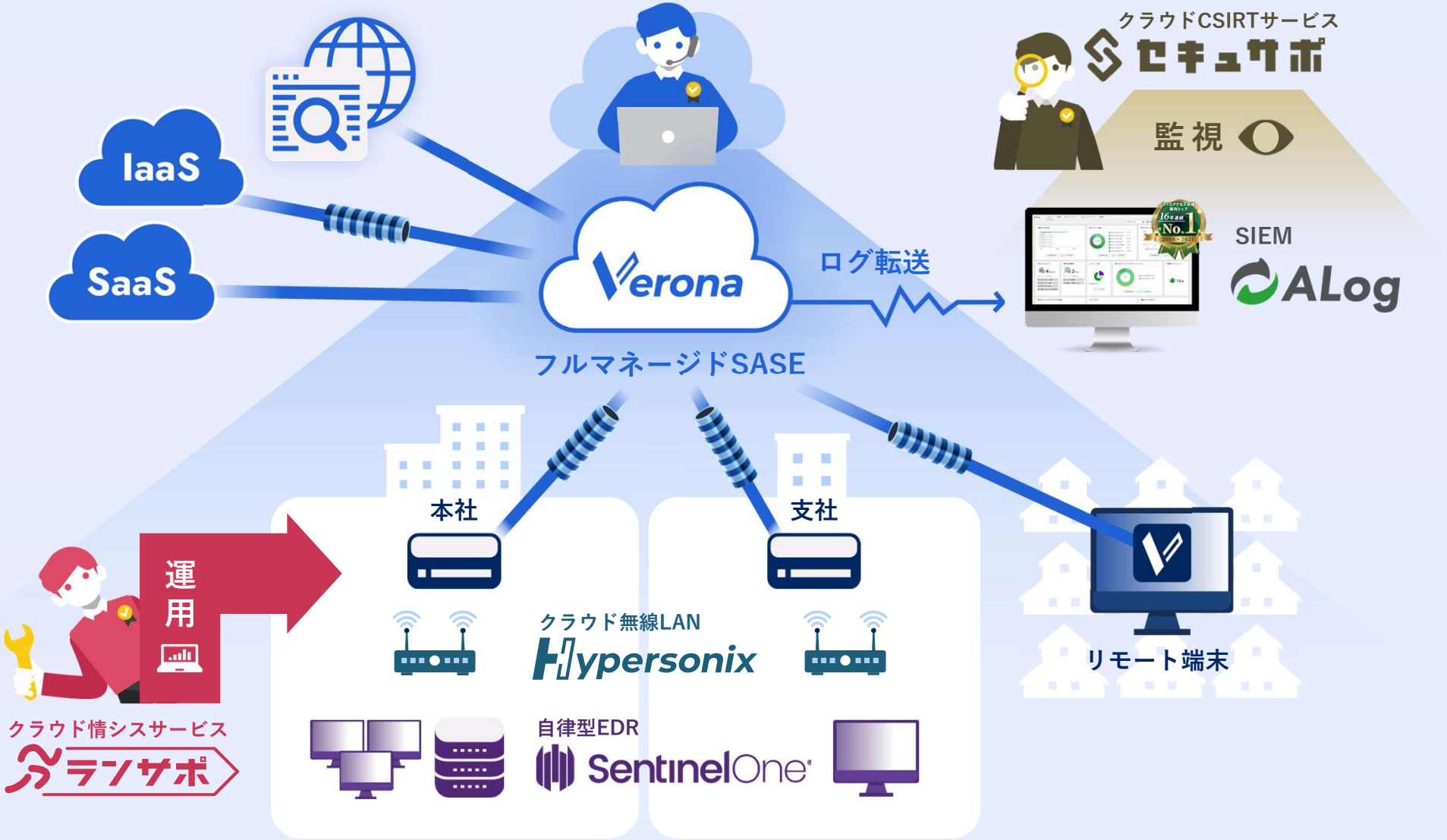
	ベーシックタイプ	スタンダードタイプ	ハイスペックタイプ	ソフトウェアタイプ	クラウド ゲートウェイタイプ
VPNスループット	120Mbps	120Mbps	950Mbps	システム環境に依存	100Mbps or 200Mbps ※回線速度に依存
FWスループット	500Mbps	500Mbps	1Gbps	システム環境に依存	100Mbps or 200Mbps ※回線速度に依存
筐体サイズ(cm)	幅16.5×奥行10.55×高さ4.3	幅16.5×奥行10.55×高さ4.3	幅43.5×奥行30×高さ4.4	-	-
利用規模	小、中規模拠点 （10～50名程度）	本社/データセンター （50名～200名程度）	サービス事業	クラウド、仮想基盤	ハードウェアレス
Verona Client 推奨同時接続数	10	100	200	100	100
Verona Client ライセンス発行上限数	10	無制限	無制限	無制限	無制限

■ ソフトウェアタイプの最低システム要件は、CPU：2core / メモリ：2GB / ストレージ：8GBとなります。

© AMIYA Corporation

網屋で実現するゼロトラスト

ゼロトラストの実現には、ネットワーク全体の監視と健全な運用が不可欠。
Veronaと網屋サービスとの連携でセキュリティを拡張。トータルセキュリティを実現します。

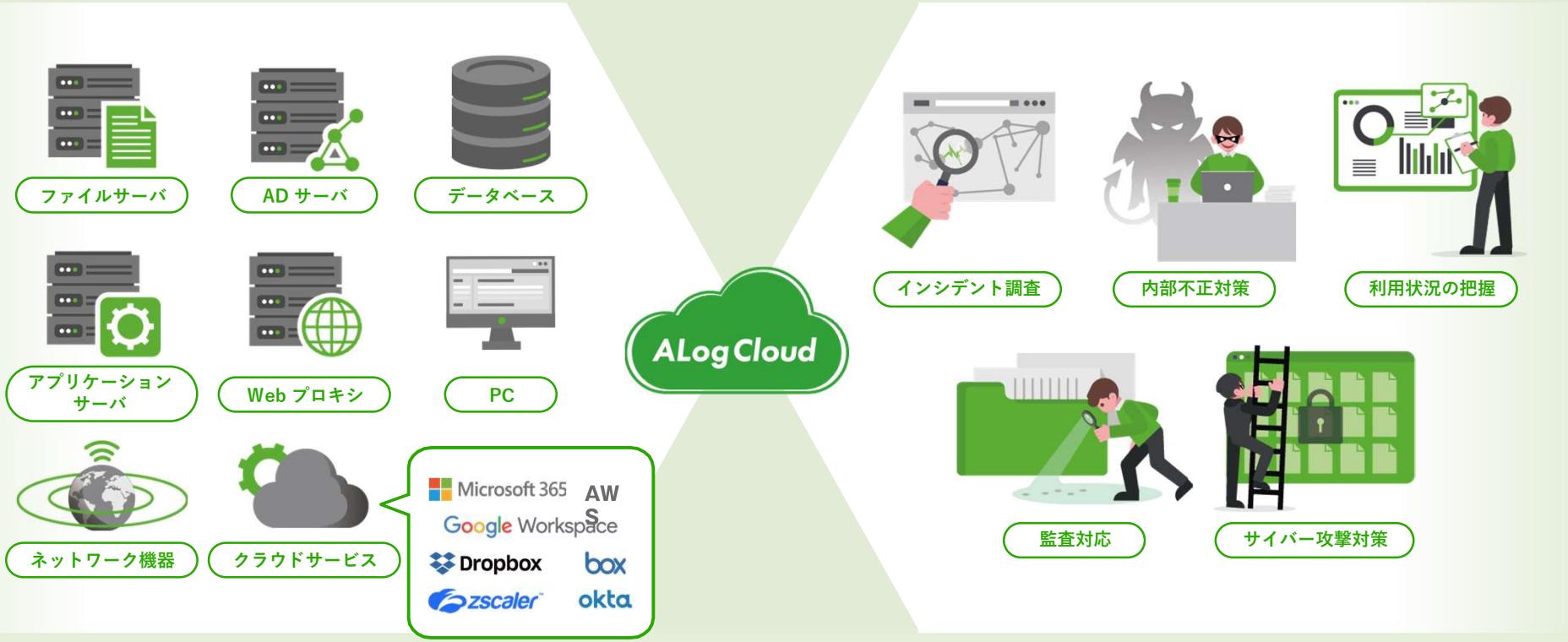


© AMIYA Corporation

システム監視なら

ALog Cloud

サイバー攻撃はあらゆるシステムが標的に。
サイバー攻撃の検知と対応には、ログを活用したシステム全体の監視が必要です。
ALog Cloudは、あらゆるITシステムのログを一元管理して自動監視。
専門知識やノウハウがなくても、誰でもカンタンにログを活用できます。



© AMIYA Corporation

システム運用なら

ランサポ

IT資産を守るには、健全なITシステムの運用が重要。
「ランサポ」は、情報システム業務全般を月額固定料金でトータルサポート。
システム運用やトラブル対応、セキュリティ対策支援など経験豊富なエンジニアが伴走。
低コストかつハイパフォーマンスなクラウド情シスサービスです。

以下のすべてに月額固定で対応します。

サーバ、ネットワークの運用/監視業務
ドキュメント整備・更新、死活監視、保守管理、月次レポート

障害/トラブル対応
サーバ、ネットワーク、クラウド、PCなどに対する問い合わせ対応及び障害対応

定型業務代行
アクセス権申請対応、アカウント管理ポリシー管理、設定変更など

PCマスターイメージ作成
PCマスターイメージの作成・定期更新

年間計画の作成支援
次年度の予算やロードマップ作成を支援

BCP関連支援
リスクレベルに応じたBCP対策を支援

クラウド移行支援
最適なクラウドの選定や移行方法などを支援

セキュリティ対策支援
今後のセキュリティ対策をアドバイス

© AMIYA Corporation

Hypersonix camera

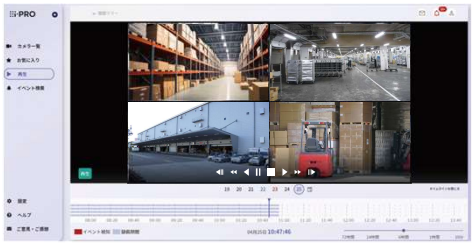
- 高性能クラウドカメラを
  ワンパッケージでご提供！
- もちろんHypersonixならではの
  安心の運用サービスつき！

Hypersonix camera のここがスゴイ！

1 高画質で識別性が向上！

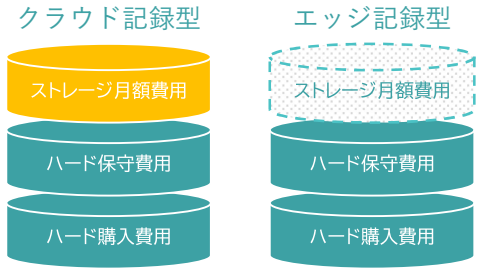
フルHD（200万画素）の鮮明な画像

2 どこからでも簡単に映像を確認！



スピーディーに検索。
スマホからも確認可能！

3 エッジ記録型でコストを削減！



クラウド利用料がかさまない！

© AMIYA Corporation

AMIYA

網屋はセキュリティの製品やサービスを開発・製造・販売する総合セキュリティプロバイダとして、お客様のセキュリティの課題を幅広くワンストップでご支援致します。

ログ管理

ALog

複雑なログをわかりやすく管理。AIと高度な分析機能で効果の見えるログ管理を実現。

クラウドCSIRTサービス

セキュサポ

当社のセキュリティ専門チームがお客様の環境全体を監視し、ランサムウェア攻撃をはじめとした一連のサイバー攻撃への対策を包括代行

脆弱性診断サービス

セキュリティ監査サービス

クラウドネットワークインフラ

Network All Cloud®

煩わしいネットワーク構築や、導入後の運用や障害対応までをクラウド上のサポートセンターが代行。

サイバーセキュリティトレーニング

経営層から一般社員、エンジニアまで網羅的なサイバーセキュリティトレーニングで組織のセキュリティレベル向上をサポート

© AMIYA Corporation

創造する時間を生み出す、
クラウド型ネットワークインフラ

Network All Cloud®

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 （ダイヤルイン）
E-Mail:infra-sales@amiya.co.jp

AMIYA

© AMIYA Corporation