Verona

これだけはやっておきたい

SaaS クラウドセキュリティ

AMIYA

Index

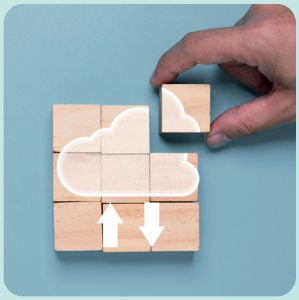
はじめに：広がるクラウド利用 ―― 2
SaaSのセキュリティリスク ―― 3
責任共有モデル ―― 4
これだけはやっておきたい5つの対策 ―― 5
総務省：
「クラウドサービス利用・提供における適切な設定のためのガイドライン」 ―― 8
セキュアなクラウドアクセスを実現：クラウドゼロトラスト「Verona」 ―― 9
「Verona」のクラウドアクセス ―― 10
不正アクセス防止機能が満載！ ―― 11
カンタン3STEP導入 ―― 12
おわりに：SaaSには適切な対策を ―― 13

はじめに
広がるクラウド利用

クラウドサービスの利用が広がりを見せています。
総務省「令和3年通信利用動向調査」によると、2021年時点でクラウドサービスを一部でも利用している企業の割合は70.4%に上っており、多くの企業が主要なシステムをオンプレミス環境からクラウド環境へ移行しています。読者の皆様も、業務でクラウドサービスを利用している方が多いのではないでしょうか。

クラウドサービスとは、ネットワークに接続されたコンピューター資源（計算能力、記録装置、情報システム等）を、ネットワークを介して必要なときに必要な分だけ利用できるようなサービスを指します。オンプレミス環境とは異なり、サーバ等を企業自ら保有し、構築・運用する必要がないため、導入が簡単、運用・管理の負担が軽減できる、システムの拡張がしやすい、等のメリットがあります。

クラウドサービスのメリット



導入が簡単

運用・管理の負担軽減

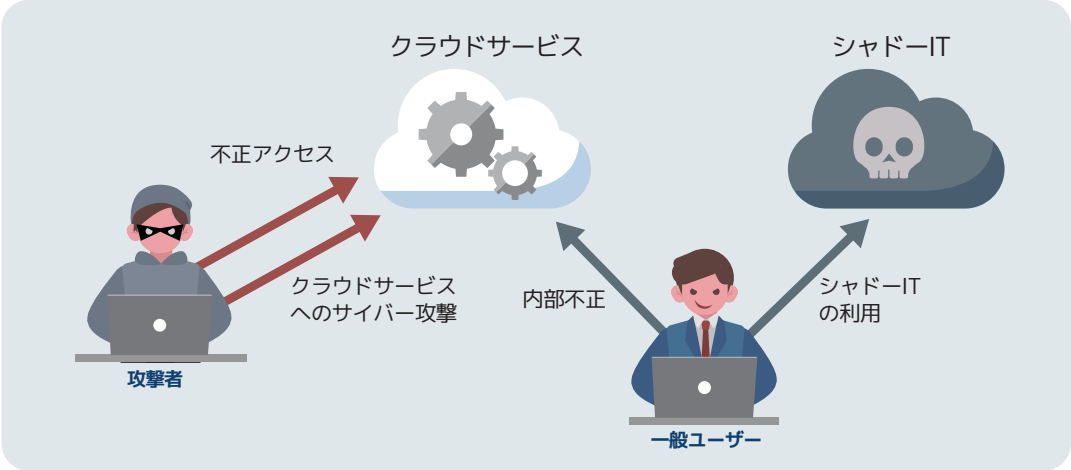
拡張しやすい

クラウドサービスの中でも、特に普及しているのが「SaaS」でしょう。SaaSは、「Software as a Service」の略で、電子メールや文書作成等のソフトウェア（アプリケーション）レベルの機能を提供するサービスです。利用者は、インターネット環境さえあれば、ソフトウェアが提供する各機能をすぐに利用できるため、大変便利で手軽なサービスです。しかし、これらのメリットがある一方で、SaaSを利用するには必ずインターネットを経由するため、利用には不正アクセスや情報漏えいなどのセキュリティリスクが常に隣にあります。

それでは、クラウドサービスを安全に利用するために、わたしたちはどのような対策をすればよいのでしょうか。本書では、クラウドサービスの中でもSaaSに絞り、「SaaSを利用したいが、セキュリティに不安がある」「SaaSを利用しているが、どのような対策をすればよいかわからない」といった悩みをもつ読者向けに、SaaSのセキュリティリスクと、安全に利用するための対策をわかりやすく解説していきます。本書がSaaSのセキュリティ対策の参考となれば幸いです。

SaaSのセキュリティリスク

まず、SaaS利用のセキュリティリスクについて紹介します。



1. 不正アクセス

インターネットを経由して利用するため、外部からの不正アクセスのリスクがあります。適切な設定を施さないと、悪意のある第三者に不正アクセスされ、機密情報が盗まれたり、マルウェアを仕込まれたりといったインシデントにつながります。

2. 内部不正

企業内部にもリスクがあります。適切な閲覧制限がなされていないと、悪意を持ったユーザーが業務外で機密情報にアクセスし、外部に流出させてしまう恐れがあります。

3. シャドーITの利用

また、悪意はなくとも、社員が未許可のSaaS(シャドーIT)を用いて業務を行うことにもリスクがあります。
社内の適切なセキュリティチェックを受けていないシャドーITを利用することで、そこから攻撃者の不正アクセスを受け、情報が漏えいしたり、マルウェアに感染したりする可能性があります。

4. クラウドサービスへのサイバー攻撃

利用しているSaaSがサイバー攻撃を受けるリスクもあります。SaaSがサイバー攻撃を受けると、正常にサービスを利用できなくなったり、預けていた機密情報が流出してしまったりする恐れがあります。

実際に起こった被害事例

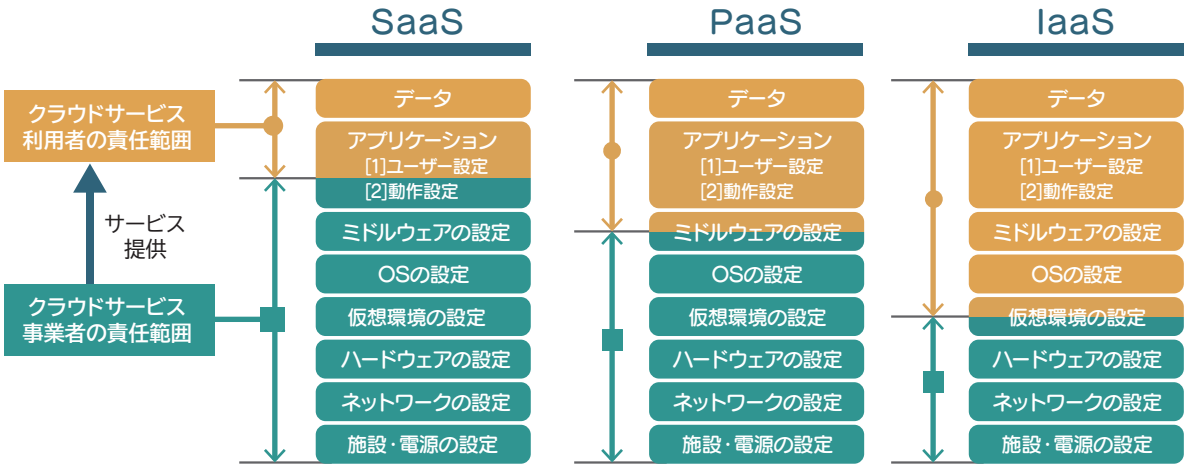
2023年6月、社労士向けクラウドサービスを手掛ける企業がランサムウェアによるサイバー攻撃を受け、サービス提供用のサーバが暗号化された。
これにより、サービスを導入する社労士法人や民間企業からは、個人情報漏えいにつながった可能性があるとの発表が相次いでいる。
2023年8月、本書執筆時点で未だ完全復旧はできておらず、約3400ものユーザーが通常サービスを利用できていない状況が続いている。

SaaS利用の大前提
責任共有モデル

SaaSを利用する上で、これらのリスクを回避するために理解しておくべき大前提が、「責任共有モデル」です。「責任共有モデル」とは、クラウドサービスの情報セキュリティを高めるには、クラウドサービス事業者とクラウドサービス利用者が協力して、クラウドサービスに対する責任を共有する必要がある、という考え方です。ただし、このモデルにおいて、事業者と利用者の責任範囲・内容は一律ではなく、クラウドサービスの内容や利用環境などで異なるため、利用者は責任分界をよく確認した上で、適切な対策を施す必要があります。

以下では、この責任共有モデルのもと、各クラウドサービス（SaaS/PaaS/IaaS）における一般的な責任分界を示しています。ご覧の通り、SaaSのセキュリティ対策は事業者側の比重が大きいことが特徴です。しかしながら、利用者側も、データとユーザ設定（利用者アカウントや業務データの設定）に関してはセキュリティ対策の責任を負う必要があります。

責任共有モデル



クラウドサービスの分類

クラウドサービスは、クラウドサービス事業者が利用者に提供する資源の範囲によって、SaaS・PaaS・IaaSという分類があります。

① SaaS
（Software as a Service）

電子メールや文書作成等のソフトウェア（アプリケーション）レベルの機能を提供するサービスです。利用者はソフトウェアが提供する各機能をすぐに利用できます。

② PaaS
（Platform as a Service）

データベースや開発フレームワーク等のアプリケーションを開発・実行するためのプラットフォームレベルの機能を提供するサービスです。
利用者はプラットフォームが提供する各種機能を使って、必要なアプリケーションを開発する必要があります。

③ IaaS
（Infrastructure as a Service）

サーバやストレージ等のハードウェアレベルの資源を提供するサービスです。
利用者は、提供されたハードウェアを利用するため、OSをはじめとする必要なソフトウェアを自力で導入する必要があります。

これだけはやっておきたい5つの対策

以上の前提のもと、安全にクラウドサービスを利用するには、どのような対策を実施すればよいのでしょうか。
これだけはやっておきたい、5つの対策を紹介します。

1. 信頼できるSaaSの選定

責任分界を理解した上で、自組織に合ったSaaSを選定しましょう。SaaSにおけるセキュリティ対策は、事業者の比重が大きいからこそ、必ず、信頼できるSaaS事業者やSaaSを選定することが重要です。信頼性の高い事業者・サービスを選定するために、以下の点を確認するとよいでしょう。

- ISO/IEC 27017、ISMAP（日本）、FedRAMP（米国）などの認証を取得しているか。
- 利用実績数や事例は信頼に足るものか。
- サービスの稼働率やこれまでの障害発生状況。
- 事業者がログデータを利用者に提供できるか等、有事の際の事業者のサポート体制は十分か。
- データの保管やバックアップ体制は明示さているか。
- 適切な情報開示が行われているか。

実施しないと
こんなリスクが…

- 使用しているSaaSがサイバー攻撃を受けて機密情報が流出。

2. アクセス管理

SaaSにアクセスできるユーザや端末を制限しましょう。
SaaSにアクセスできるユーザの範囲を定め、IPアドレス制限などを実施します。

その上で、認証の強度は高くしましょう。
以下を徹底することで、不正アクセスリスクを低減させることができます。

- パスワードはなるべく文字数を増やす。
- パスワードに大文字、小文字、数字、記号を織り交ぜる。
- 認証情報を複数人で共有しない。
- 認証情報を複数サービスで使いまわさない。
- 端末に認証情報を記録しない。
- 使用していない認証情報は削除する。
- 多要素認証を設定する。

特に、管理者や特権アカウントの管理においては、アカウント数を最小限に留める、多要素認証を必須とする、アカウント利用の際には複数人でのチェックを行う、などの対策が必要です。

実施しないとこんなリスクが…

- 攻撃者の総当たり攻撃により不正アクセス。
- 退職者の認証情報を攻撃者が不正利用。

3. アカウント管理

SaaSにアクセスできる人の中でも、利用できる機能や閲覧できるデータなどを段階分けし、適切に管理しましょう。アカウントの棚卸を定期的に行い、最小権限の原則のもと、役割分担（閲覧のみ、設定可能、アカウント作成可能、など）を徹底します。特に、ゲストユーザーについては、不要な情報公開を割けるため、必要最小限の権限としましょう。

実施しないとこんなリスクが…

- ゲストユーザが誤って機密情報にアクセス。

4. ログ管理

ログを適切に管理しましょう。ロギングの設定は、デフォルトでオフとなっているSaaSが多いため、確実に設定を行う必要があります。設定により、異常が起きたらアラートを発報できるようなサービスも存在します。また、適切な期間ログを保存し、監査やインシデントの事後調査等に利用できる体制を整えておくことも重要です。

実施しないとこんなリスクが…

- 不正アクセスを受けていることに気が付かない。
- ログが保存されておらず、異常時の解析ができない。

5. SaaS利用ルールの徹底

適切な対策を施しても、利用者が適切に利用しなければ、元も子もありません。クラウドサービス利用における社内の基本方針やルールを明確にし、文書化しましょう。また、クラウドサービスにはどんなセキュリティリスクがあるのか、適切に利用しないと実際にどんなインシデントにつながるのか、利用者に周知することも重要です。その上で、組織のルール外で利用されているSaaS（シャドーIT）を発見し、取り締まりましょう。クラウドサービスの利用状況を可視化し、制御できるツールとして、CASBなどの導入も検討するとよいでしょう。

実施しないとこんなリスクが…

- 適切なセキュリティ設定が施されていないシャドーITからマルウェアに感染。

総務省
「クラウドサービス利用・提供における適切な設定のためのガイドライン」

これまで、これだけはやっておきたい5つの対策を紹介しましたが、他にも実施を推奨されている対策は多くあります。それらを文書化したものが、総務省の「クラウドサービス利用・提供における適切な設定のためのガイドライン」です。ガイドラインでは、クラウドサービスの設定不備によるセキュリティインシデントが発生しないよう、安全安心なクラウドサービスの利用・提供を目的として、利用者と事業者双方が認識しておくべき事柄や、具体的なリスクと対策法について、詳しく解説されています。クラウドセキュリティの必読書と言える内容なので、一読することをおすすめします。
このガイドラインの中で、SaaSのセキュリティ対策として確実に実施すべきとして記載されているものが、「アクセス管理」です。

> “管理者アカウントには多要素認証を必須にする等の設定を確実に行うほか、組織の要件に応じてユーザアカウントのIPアドレス制限など各種設定を確実に行う必要がある。”
>
> 総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン」p.48
> https://www.soumu.go.jp/main_content/000843318.pdf

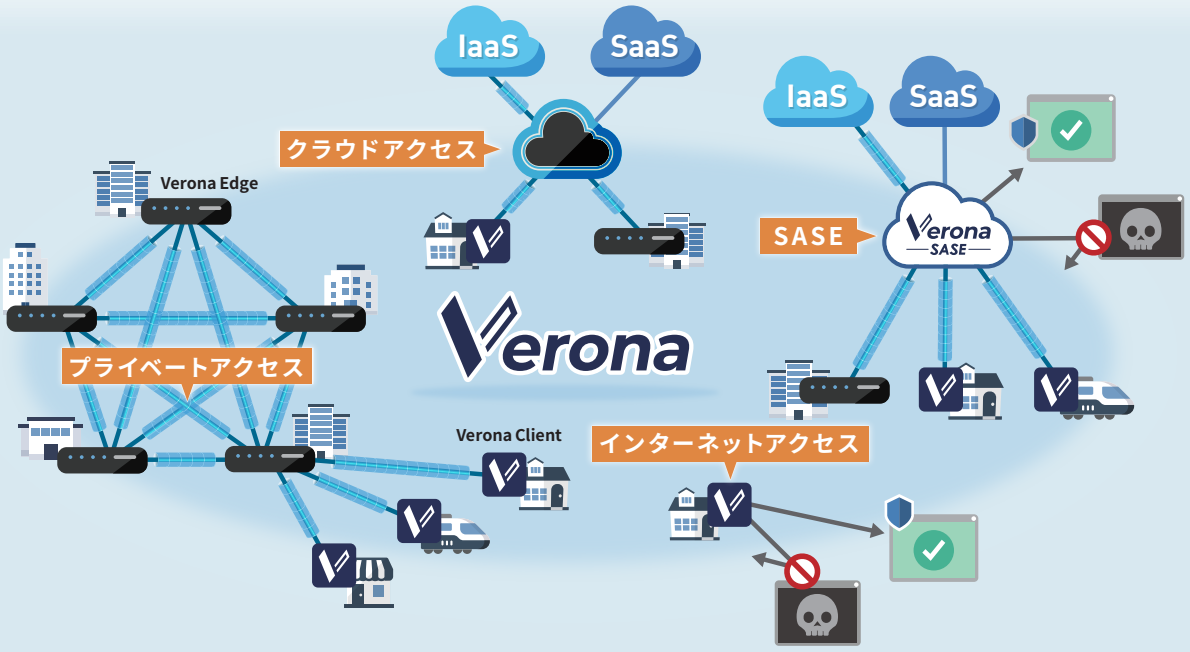
SaaSの認証強化とアクセス制限を行わないと、どんな端末・ユーザからでも、認証さえ突破できれば、社内で利用しているSaaSにアクセスできてしまいます。そのため、悪意のある第三者が容易にSaaSに不正アクセスできてしまいます。

このような多大なリスクを回避するためには、認証強化とアクセス制限は必須のセキュリティ対策と言えます。

セキュアなクラウドアクセスを実現
クラウドゼロトラスト「Verona」

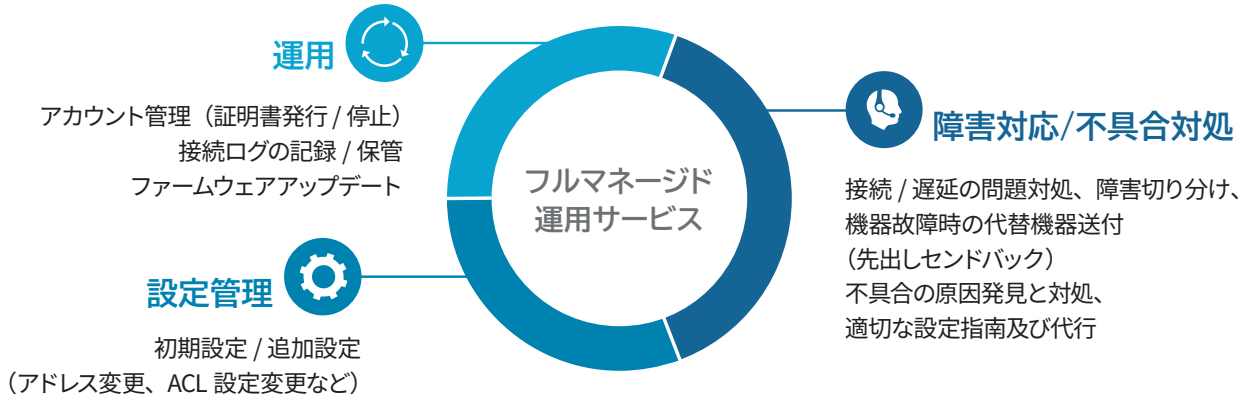
網屋の「Verona」なら、クラウドサービスへの認証強化とアクセス制限により、安全にクラウドサービスを利用することができます。

「Verona」は、ゼロトラストを実現するクラウド管理型ゼロトラストサービスです。場所を選ばない、統一されたネットワークセキュリティを実現することができます。



Verona のポイント
フルマネージドの運用サービス

障害対応やテクニカルサポートだけでなく、脆弱性対応や日々の設定変更のすべてに対応。
運用負荷なくネットワークセキュリティを実現できます。

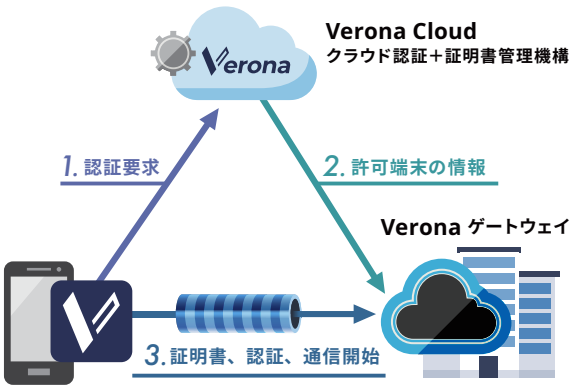


セキュアなクラウドアクセスを実現
クラウドゼロトラスト「Verona」

「Verona」のクラウドアクセス

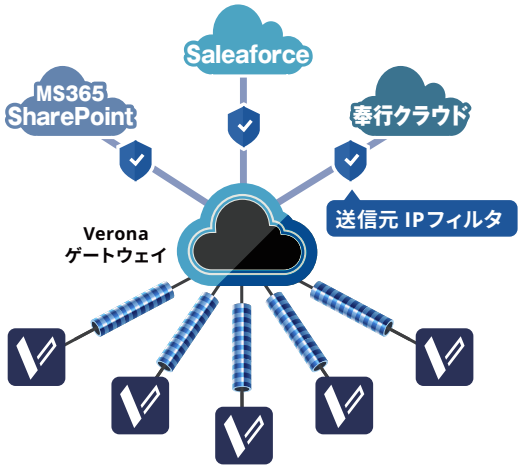
証明書認証

証明書認証をベースにした独自の認証システム。
強固な認証で不正アクセスを防止。



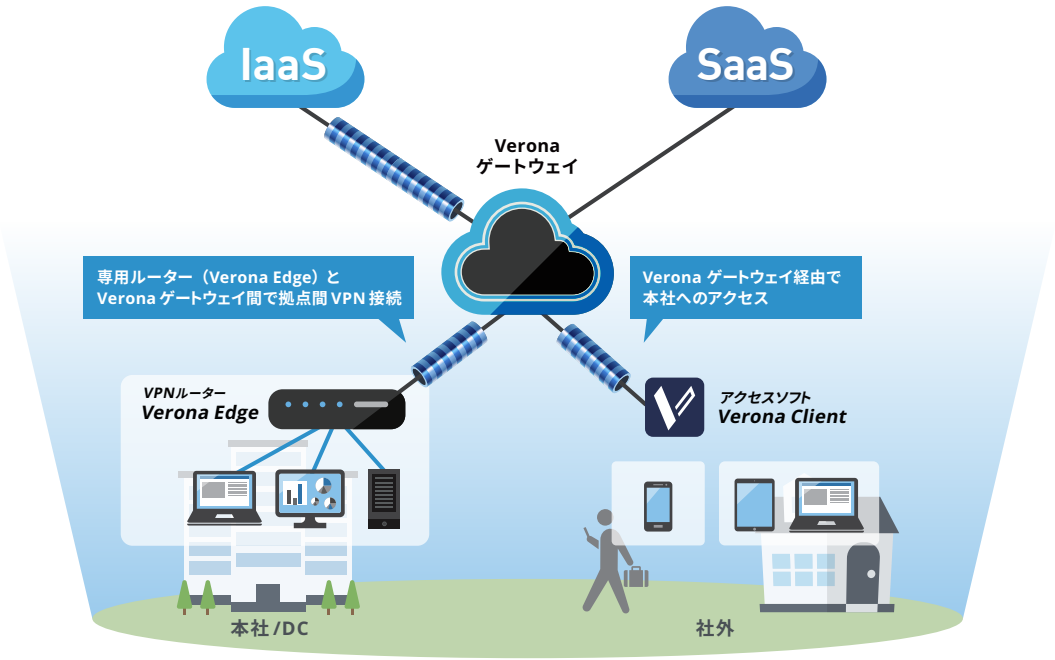
IPアドレス制限

SaaSへの接続元グローバルIPを制限し、VPNゲートウェイを経由したセキュアなSaaSアクセスを実現します。



社内アクセスとクラウドアクセスの両立も可能！

専用の拠点側ゲートウェイ（Verona Edge）、Verona ゲートウェイの併用により、一つのクライアントソフト（Verona Client）から、社内やIaaSへのVPN接続も、SaaSへのセキュアなアクセスも実現できます。



セキュアなクラウドアクセスを実現
クラウドゼロトラスト「Verona」

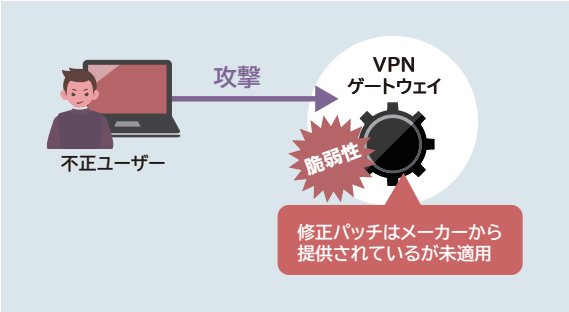
不正アクセス防止機能が満載！

「Veronaゲートウェイ」には、証明書認証とIPアドレス制限の他にも、充実の不正アクセス防止機能が実装されています。

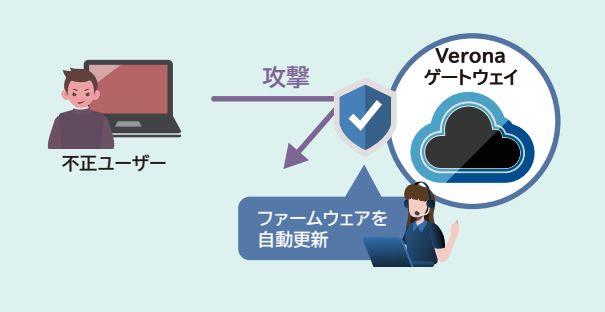
自動ファームウェアアップデート

脆弱性に即時対応する自動ファームウェア更新。
脆弱性が放置されないため、攻撃対象になりにくい。

従来のVPN



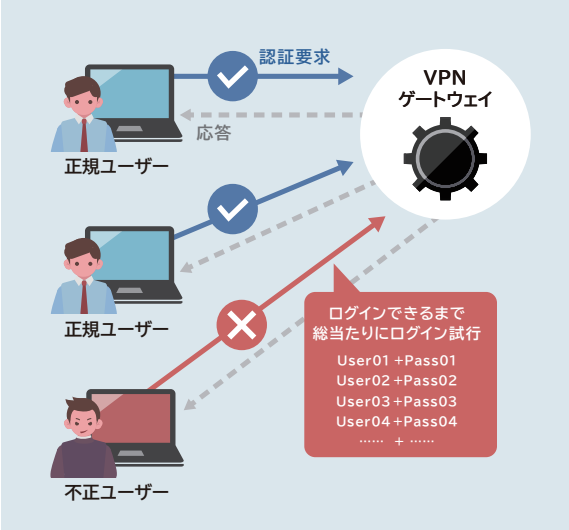
Verona



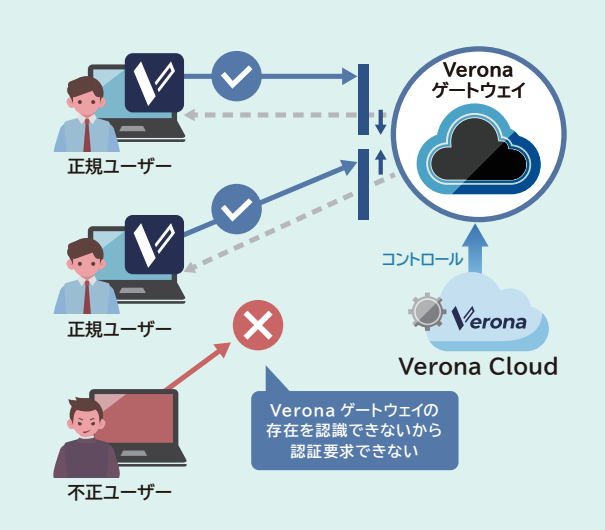
ダイナミックポートコントロール

正規ユーザからの認証要求のみにVPNゲートウェイのポートが開放。
VPNアクセス環境の存在自体を隠し、不正アクセスを防ぎます。

従来のVPN

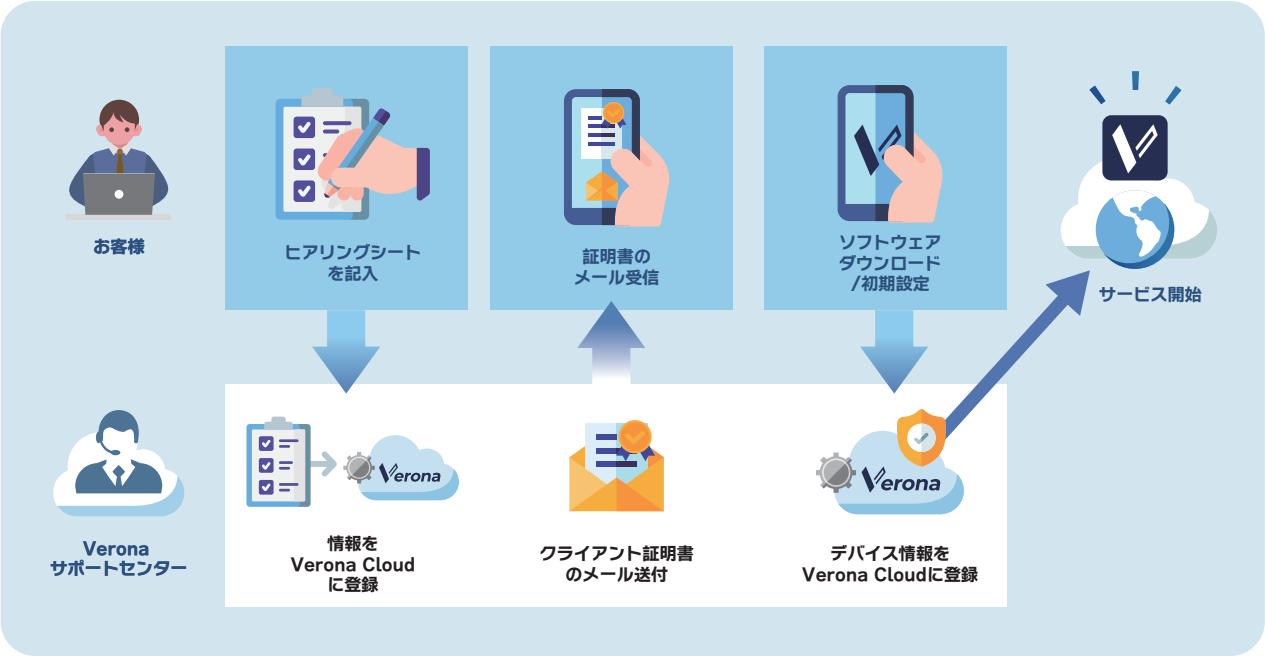


Verona



セキュアなクラウドアクセスを実現
クラウドゼロトラスト「Verona」

カンタン3STEP導入

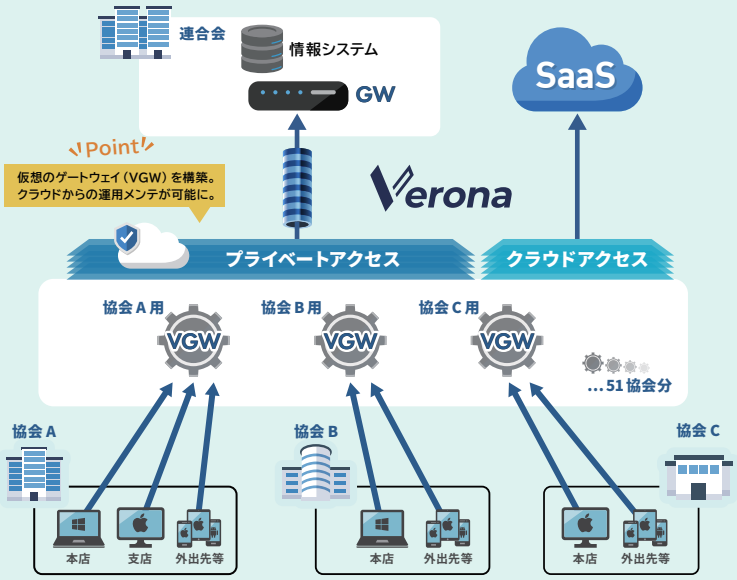


導入事例

一般社団法人
全国信用保証協会連合会

協会ごとにVeronaゲートウェイを採用
各拠点の要件に適合した大規模プライベートアクセス網を構築

- 環境の異なるシステムをつなぐVPNを、既存環境に変更なく導入することに成功。
- 協会ごとに51個のVeronaゲートウェイを構築することで、各協会の要件を満たす。
- クラウドUTMやDNSセキュリティも併せた導入で、クラウドアクセスも、インターネットアクセスもセキュアに。
- 万全なサポート体制で、各協会からの直接の障害問い合わせにも対応可能に。



おわりに
SaaSには適切な対策を

本書では、クラウドサービスの中でもSaaS利用のセキュリティリスクと、安全に利用するためのセキュリティ対策を紹介してきました。
SaaSは便利である反面、適切なセキュリティ対策を施さないと、多大なリスクにさらされることとなります。

しかし、適切な対策を実装することで、多くのリスクを回避することができます。
ぜひ、本書で紹介したセキュリティ対策を実施し、安全にSaaSを利用してください。

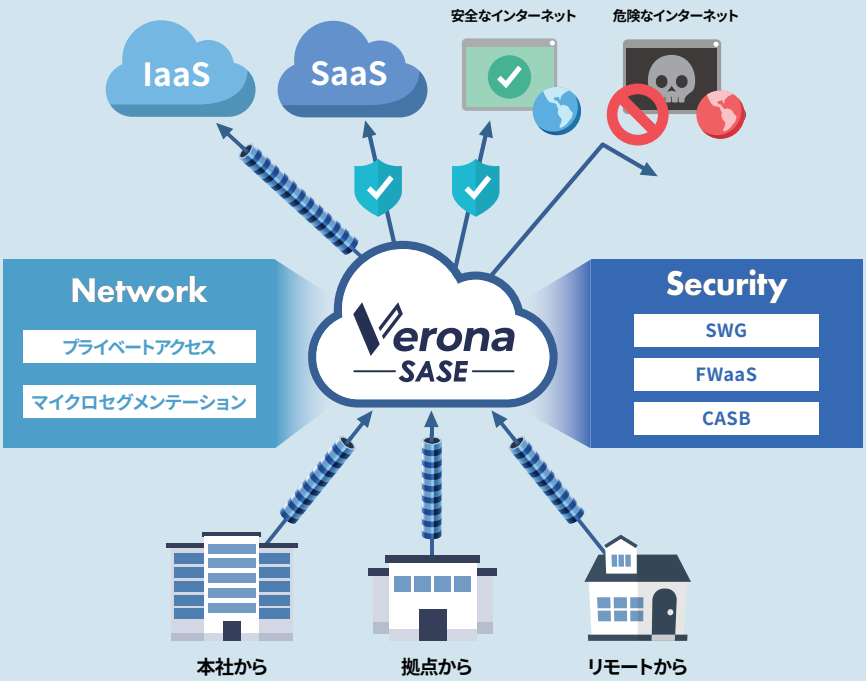
ネットワーク全体のセキュリティ強化に
ここから始めるゼロトラスト Verona SASE

近年では、クラウドサービスと共にテレワークも普及したことにより、守るべき資産が社外に分散し、従来の境界型防御モデルでは資産を守り切れなくなったことから、「ゼロトラスト」の概念が重要視されています。
「ゼロトラスト」とは、アクセス先・アクセス元に関係なくすべての通信を信用せずに、ネットワーク全体を保護するセキュリティ対策を実施する考え方のことです。

そこでご紹介するのが、網屋の「Verona SASE」です。
Verona SASEは、中堅・中小企業のゼロトラスト実現のハードルとなる人材とコストの課題を解消し、誰でも手軽に導入・運用できるSASEです。

SASEの概念をベースに必要な機能を絞り、シンプルな構成とすることで、専門知識不要の使いやすさと低価格を実現しました。Veronaシリーズの最大の特徴と言えるフルマネージドの運用サービスで、導入・運用負荷を最大限軽減しています。

Verona SASEなら、万全のクラウドセキュリティを実装できます。アプリケーションコントロールによりクラウドサービスをアプリケーションレベルで可視化・制御し、シャドーITの対策を可能とするのみならず、URLフィルタリングやアンチウイルスにより、インターネット経由でのサイバー攻撃の脅威からネットワーク全体を保護します。



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/

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。