情シス必見

AMIYA

今のセキュリティ対策で会社を守れる？

「たまたま狙われていないだけ」から脱却する方法

Copyright @ AMIYA, Inc.

ビジネス環境の変化と企業のセキュリティ

AMIYA

デジタル化が進み続ける現代のビジネス環境において、
データや働く場所は分散化の一途を辿っています。
社内ネットワークを重点的に保護していた従来の境界型防御を見直し、時代にマッチしたセキュリティ対策を実現することは、事業の成功と存続に直結する重要な要素と言えるでしょう。

新たな働き方の普及、様々なクラウドサービスの台頭、柔軟なデータ活用は、企業の可能性を広げる一方で、新たな脅威と課題も引き起こしているのではないでしょうか。

SASE（Secure Access Service Edge）は、
このような課題への有効な解決策として注目を集めています。
ゼロトラストを実現する有力な手段ではありますが、
その導入と活用には困難さも伴います。
高額なコスト、専門的な知識を必要とする仕組みや高い運用難易度は代表的な課題ではないでしょうか。

この資料では現代のビジネスを取り巻く要素や課題を考え、
効果的な対策を実現するためにはどうすればいいのか
を解説します。

目次

01. ビジネス環境の変化と企業のセキュリティ
02. 効果的なセキュリティ対策の実施はなぜ難しいのか
03. 課題1：サイバー攻撃の対象やセキュリティ対策が必要な環境の増加
04. 課題2：人材不足とコストの問題
05. 現代のビジネス環境に対応するための「SASE」
06. SASEの必要性は意識されているが、導入に至っている企業は極一部
07. リモートワークへの課題を抱えている企業が大多数
08. 企業規模に関わらず最大の効果を発揮する「Verona SASE」
09. 専門知識や予算に不安があるなら、ぜひVerona SASEをご検討ください！

Copyright @ AMIYA, Inc.

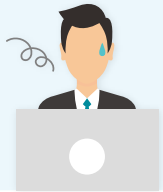
効果的なセキュリティ対策の実施はなぜ難しいのか

AMIYA

急速な変化を続けるビジネス環境において、サイバー攻撃も一段と高度化しています。
この脅威に対抗するための**専門的な人材獲得やセキュリティ対策の実施は、企業にとって重要な生命線**と言えるでしょう。
しかし、クラウド活用やテレワーク、データ活用など、環境の変化に対応し続けるセキュリティ対策は容易ではありません。

企業

- どのような攻撃をされるのか予想がつかない…
- セキュリティ人材がいない…
- セキュリティにかけられる予算は限られている…



- 社外にも保存される機密情報
- 自宅やコワーキングスペースで業務を行なうテレワーカー
- 様々な分析基盤上で活用されるデータ

攻撃者

- 社外の環境はセキュリティが甘いかもしれない
- テレワーカーの端末を狙ってみよう
- このクラウドサービスの脆弱性を突けば機密情報を奪取できる

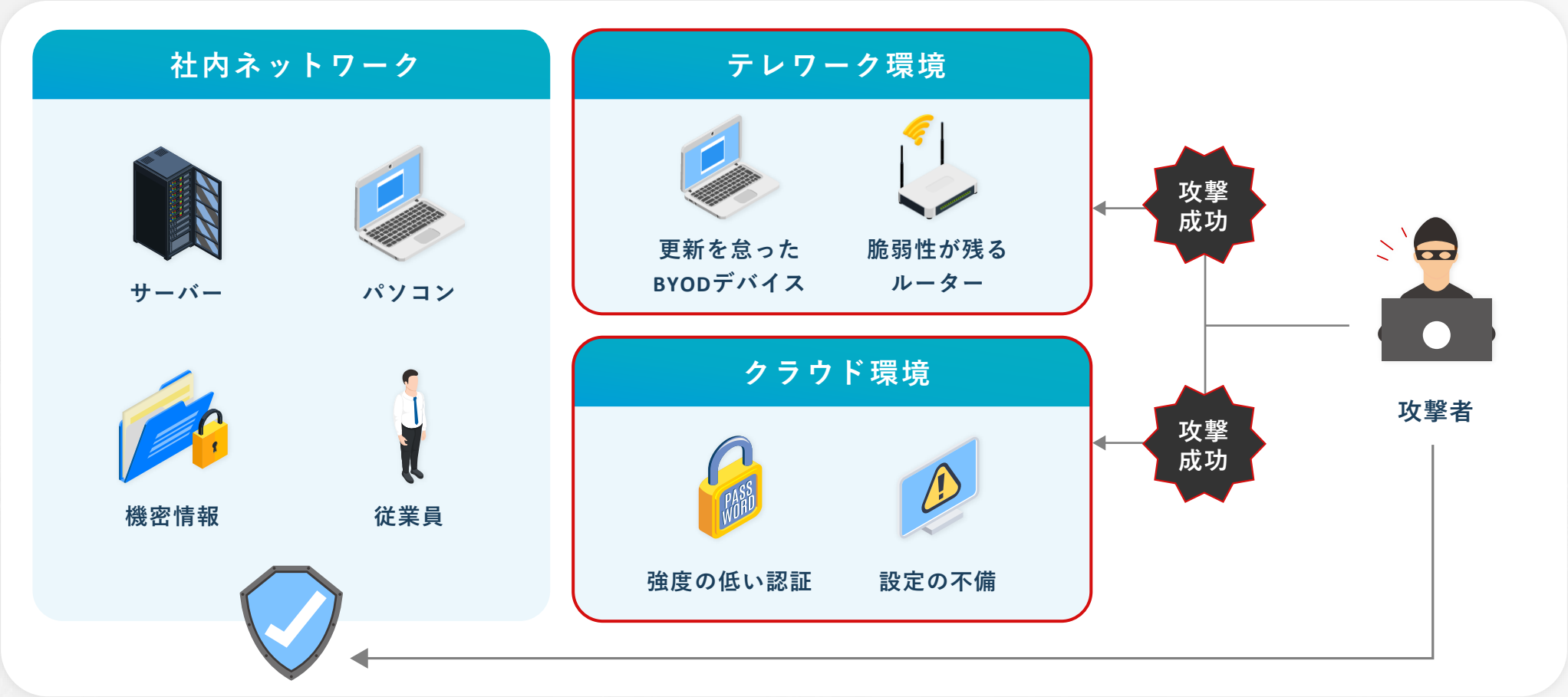
人材や予算が潤沢ではない企業にとって、
様々な脅威に対して効果的な防御を行なうことは困難を極めます。

Copyright @ AMIYA, Inc.

課題1 サイバー攻撃の対象やセキュリティ対策が必要な環境の増加

AMIYA

ビジネス環境の変化は、利便性や生産性の向上をもたらしました。
しかし、それによりクラッカーが**攻撃できる対象や手法の増加**、企業の**セキュリティに不足が生じるケース**も散見されます。



適切なセキュリティ対策を実現できない状況では、
たまたま標的になっていないだけで、狙われたら重大なセキュリティ事故が発生してしまう
という状況になりかねません。

Copyright @ AMIYA, Inc.

課題2 人材不足とコストの問題

AMIYA

前述の課題に対し、企業としてやるべきことは**必要なセキュリティ対策を適切に実施する**ことでしょう。
しかし、実際に行なうことは困難である企業が多いのではないでしょうか。

VPN環境の整備

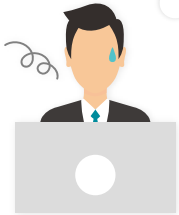
ゼロトラスト

IAM、シングルサインオン

デバイス保護

強度の高い認証

機密情報保護



担当者

やるべきことは山積み…
しかし予算も人材も余裕はなく、現実的にできることは限られている…

人材不足や高額なコストといった課題に直面しており、
あるべき姿が見えていてもそれを実現することは非常に困難です。

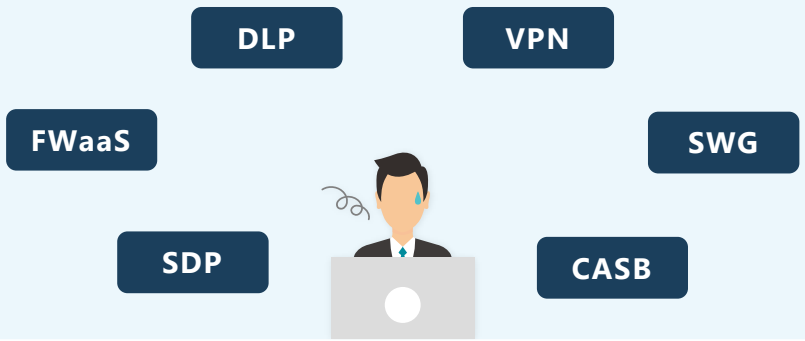
Copyright @ AMIYA, Inc.

現代のビジネス環境に対応するための「SASE」

AMIYA

高度化するサイバー攻撃や分散するデータへの有効なアプローチとして、**ゼロトラスト**が提唱されています。
全ての通信を監視・検証し、脅威に対処できるため、現代のビジネス環境にマッチしていると言えるでしょう。
また、ゼロトラストに必要な要素をパッケージングしたシステムとして**SASE**が存在します。

ゼロトラスト



様々な要素の選定・設計が必要

SASE

ゼロトラストの要素がパッケージングされ、
個別要素の選定が不要

SASEでゼロトラストを実現しやすくなるものの、高度なセキュリティ知識や高額な予算は必要。
そのため、誰でもSASEを活用できるとは言えない。

実際に企業で働く情シスの方々は、
このような状況をどのように意識しているのでしょうか。

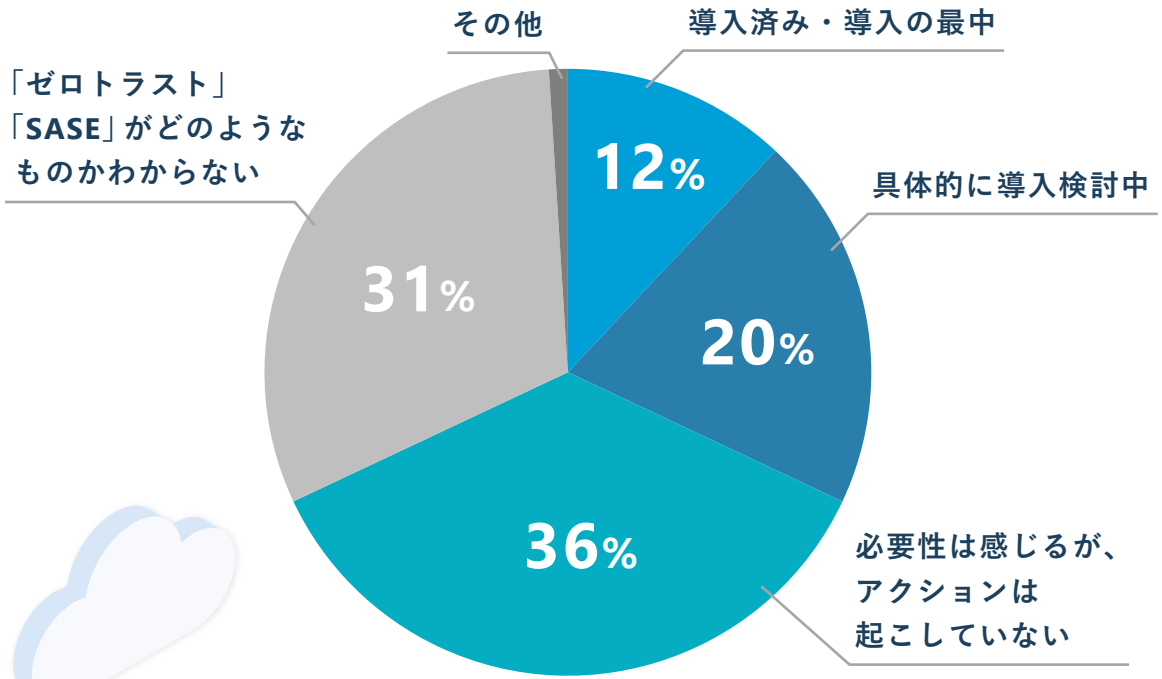
Copyright @ AMIYA, Inc.

SASEの必要性は意識されているが、導入に至っている企業は極一部

AMIYA

企業の情シス担当者は、どの程度**SASE**を意識しているのでしょうか。

Q 近年注目されている「ゼロトラストセキュリティ」を実現する選択肢として「SASE」がありますが、どの程度意識していますか？



調査概要

調査対象：全国23～60歳の企業に勤める情シス
調査手法：インターネットリサーチ
調査期間：2023年5月
回答数：300名

POINT

SASEを活用できている企業は全体の12%に留まります。
未導入企業のうち56%はSASEを意識していますが、導入には至っていません。

SASEの導入は一部の企業に留まりますが、これからのセキュリティとして一定の注目を集めています。専門知識が求められるケースが多く、使いやすいSASEがまだ少ないことも一因と考えられるのではないでしょうか。

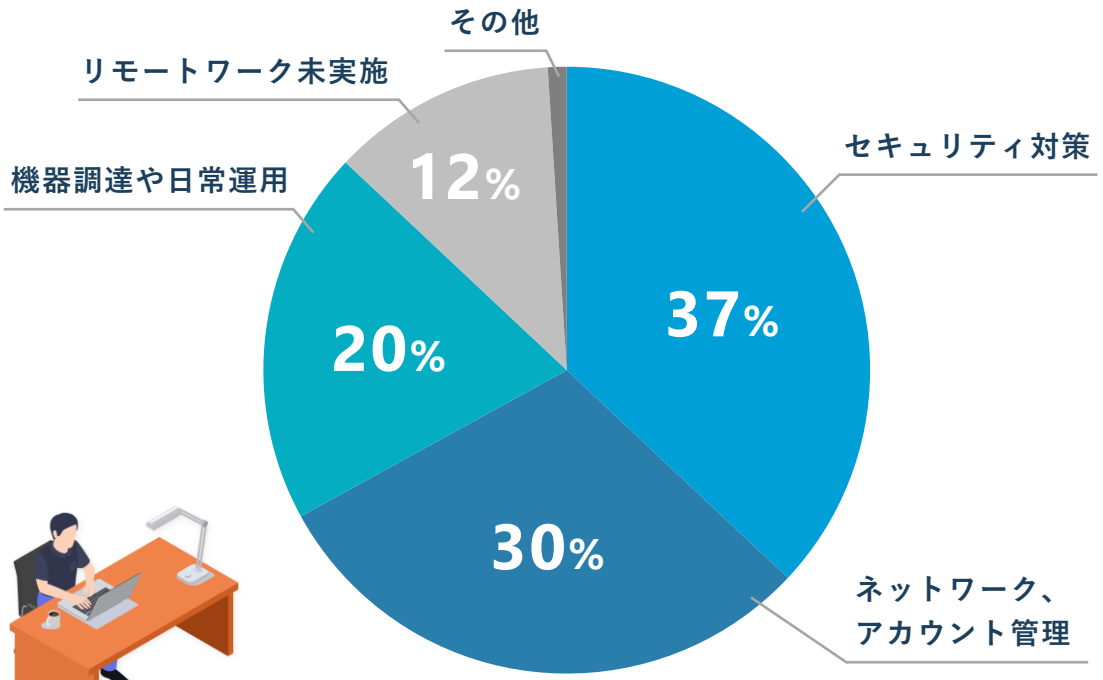
Copyright @ AMIYA, Inc.

リモートワークへの課題を抱えている企業が大多数

AMIYA

一定の浸透を見せるリモートワークによるIT環境の変化や課題について、情シス担当者はどのように考えているのでしょうか。

Q 近年のリモートワークの普及により、IT環境にどのような課題が生じていますか？



※調査概要は前ページと同様

POINT

なんらかの課題が生じている企業は全体の87%、課題がない13%のうち12%はリモートワーク未実施であり、ほとんどの企業にセキュリティの課題が生じていました。

社内ネットワークを守れば安全であった以前と比較し、守るべきデータやデバイスの分散、増加が一因と考えられます。
ゼロトラスト（SASE）はこのような課題にも有効ですが、前ページの通りまだ浸透したとは言えない状態です。

リモートワークの課題を解決するためには、セキュリティ人材の獲得や、適切なセキュリティシステムの活用が重要です。しかし、そもそもの人材不足や予算の都合もあり、対応が後手になってしまう企業も多いのではないでしょうか。

Copyright @ AMIYA, Inc.

企業規模に関わらず最大の効果を発揮する「Verona SASE」

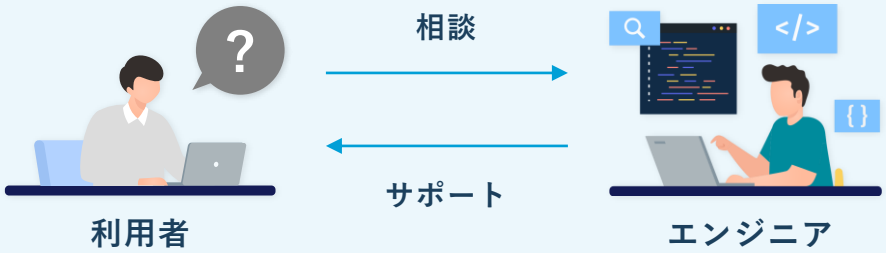
AMIYA

Verona SASEは、現代の**ビジネス環境にマッチしたゼロトラストセキュリティを実現**するためのSASEサービスです。
専門家による運用代行と、多くのケースで専門家を雇用するよりも**低いコスト**を実現しています。

専門性を持ったエンジニアによる運用サポート

Verona SASE環境

VPN　SWG　CASB　FWaaS



運用負担や要求知識を最小限に抑えます！

専門家を雇用するよりも低コスト

	ベーシック	スタンダード	ハイスペック
ユーザー数	～100	～500	～1000
初期費用	50,000円	50,000円	50,000円
サービス費用（月額）	210,000円	400,000円	600,000円

※1000ユーザー以上でも個別カスタム可能

専門家の雇用モデル
月額：800,000円／別途システム導入費用

専門家より低コストでSASE導入・運用を実現！

Verona SASEにより、
「コストや十分なスキルを持った人材の不足」といった課題を解消することが期待できます。

Copyright @ AMIYA, Inc.

専門知識や予算に不安があるなら、ぜひVerona SASEをご検討ください！

AMIYA

Verona SASE

堅牢なセキュリティ環境を低コストで実現できるVerona SASEは、
企業規模にマッチしたサイジングで無理なく導入できるSASEサービスです。

セキュリティシステム導入のハードルとなる**コスト**や**専門知識**の課題をクリアし、
様々な企業で堅牢なセキュリティ環境を実現することができます。

Verona SASEの特徴

セキュリティプロフェッショナルによる運用サポート

規模に合わせられる低コストなSASE環境

より詳しいサービス情報はこちら

株式会社網屋
ネットワークセキュリティ事業部

03-6822-9995
（ダイヤルイン）

infra-sales@amiya.co.jp

Copyright @ AMIYA, Inc.