IIJ Internet Initiative Japan

Internet Week 2021

今注目の SASE 入門

～ 最近よく聞くネットワークセキュリティのクラウド化とは ～

安全をあたりまえに
wizSafe

株式会社インターネットイニシアティブ
岸 三樹夫

自己紹介

安全をあたりまえに wizSafe

岸 三樹夫

（Mikio Kishi）

株式会社インターネットイニシアティブ

セキュリティ本部

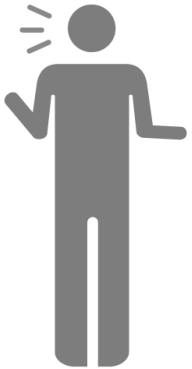
2002年入社 (20年目)

入社後、主にセキュリティサービスの
システム開発・運用・サポートなど、様々な業務を経験。
現在はセキュリティサービスの企画・開発の統括。

今、世の中で注目を集めている

サッシー（サシー）
SASE について、

中立的な立場から、その概要を解説します。



安全をあたりまえに
wizSafe

1. 今、SASE に注目が集まっている背景
2. SASE の概要
3. 世の中の SASE ソリューションの特徴・分類

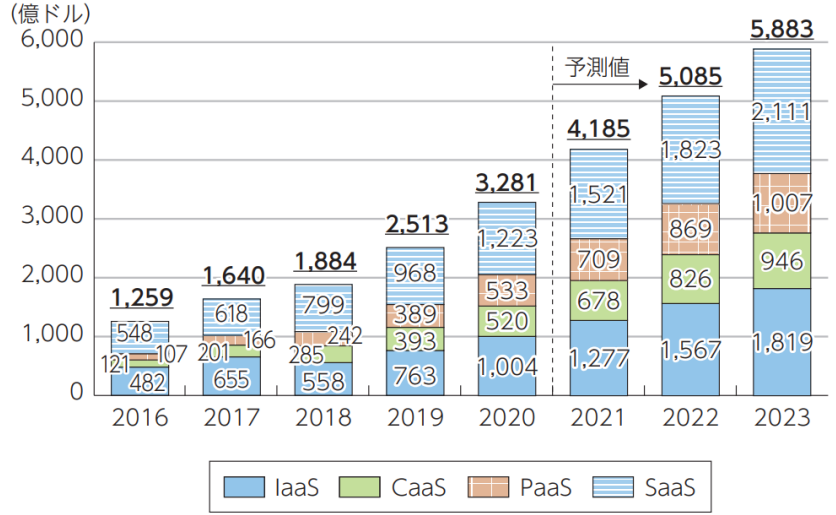
クラウドサービス利用増加による、機密情報の拡散

AWS や Azure などの IaaS、Microsoft365、Salesforce、Zoom などの SaaS 利用が進み、各法人企業の機密情報の場所がオンプレミスからクラウドへシフトしていっている。

利用するクラウドアプリケーションによっては、膨大なネットワーク帯域・コネクションリソースを必要とするものもある。

一方で、オンプレミス or クラウドのどちらかに完全にシフトできるわけではないため、双方に対して格納されている機密情報・リソースの管理が課題となっている。

図表 0-2-2-8 世界のクラウドサービス市場規模の推移及び予測（カテゴリ別）



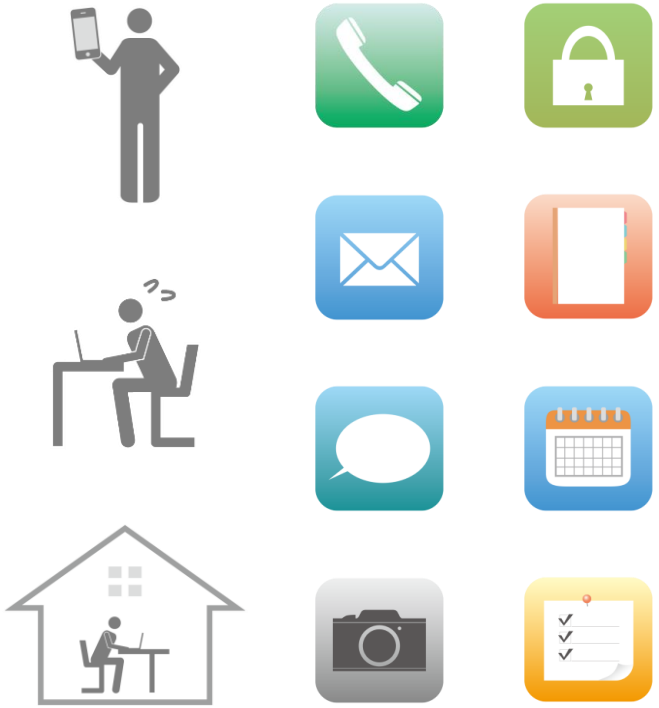
出典:「令和3年版情報通信白書」(総務省)
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf

スマートフォンを含めた利用デバイスの多様化

企業における利用デバイスは多様化している。
（PC、スマートフォン、タブレットなど）

多様化したデバイスは使われ方も様々であり、
それぞれのユースケースを想定する必要がある。

対応するデバイス毎にセキュリティの脅威からの
対処方法やリスクが異なるため、対応に割く労力
が大きく、必要十分な対応がしきれていない

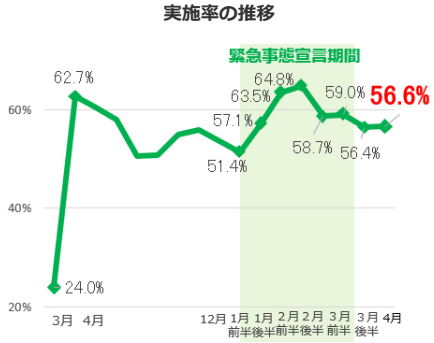


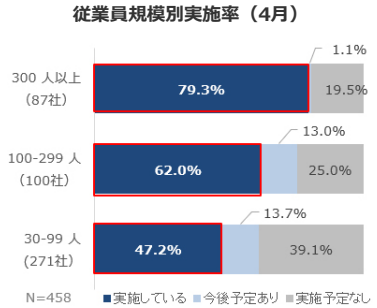
働き方改革や COVID-19 によるテレワークの普及拡大

働き方改革や COVID-19 によって、
テレワークがドラスティックに浸透した。
（緊急事態宣言期間は**企業の約半数がテレワークを実施**）

自宅等のオフィス外で業務を実施する社員が増え、
社内インフラでは想定していなかった課題が発生。

業務・事業継続を最優先として、セキュリティ
レベル低下を許容している企業も見受けられる。





出典:「テレワーク実施率調査結果（2021年5月）」（東京都 産業労働局）
https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/05/07/10.html

その背景により見え隠れする多くの課題

安全をあたりまえに wizSafe

エンドユーザの利便性低下

オフィスと自宅で使えるツール/システムが異なるため、認証の仕方などが変わり使い勝手に影響が出てくる。
また、データセンターを経由するなどトラフィックの折り返しが発生し、通信遅延が発生する。

セキュリティポリシの複雑化・運用コストの増加

オンプレミス/クラウドを問わず、ありとあらゆる箇所でセキュリティポリシのチェックが発生することや、
様々な種類のネットワーク機器・システムをメンテナンスする必要があり、システム管理コストが増加する。

セキュリティレベルの低下

オフィスで業務をする前提のネットワークシステム環境でリモートワークを実施すると、セキュリティ機能の
一部が適用されない、もしくはできないことを妥協する状況に陥るため、マルウェアの感染や不正アクセス、
内部犯行による情報漏洩などのセキュリティリスクが高くなる。

ネットワークを集約した境界型防御のセキュリティ対策では限界

安全をあたりまえに
wizSafe

1. 今、SASE に注目が集まっている背景

2. SASE の概要

3. 世の中の SASE ソリューションの特徴・分類

SASE とは？

あらゆる環境のユーザ／デバイスが、

クラウドサービスや情報資産に安全にアクセスできるように、

本社やデータセンターに通信を集約する従来の方法から、

クラウドサービスへの経路上で

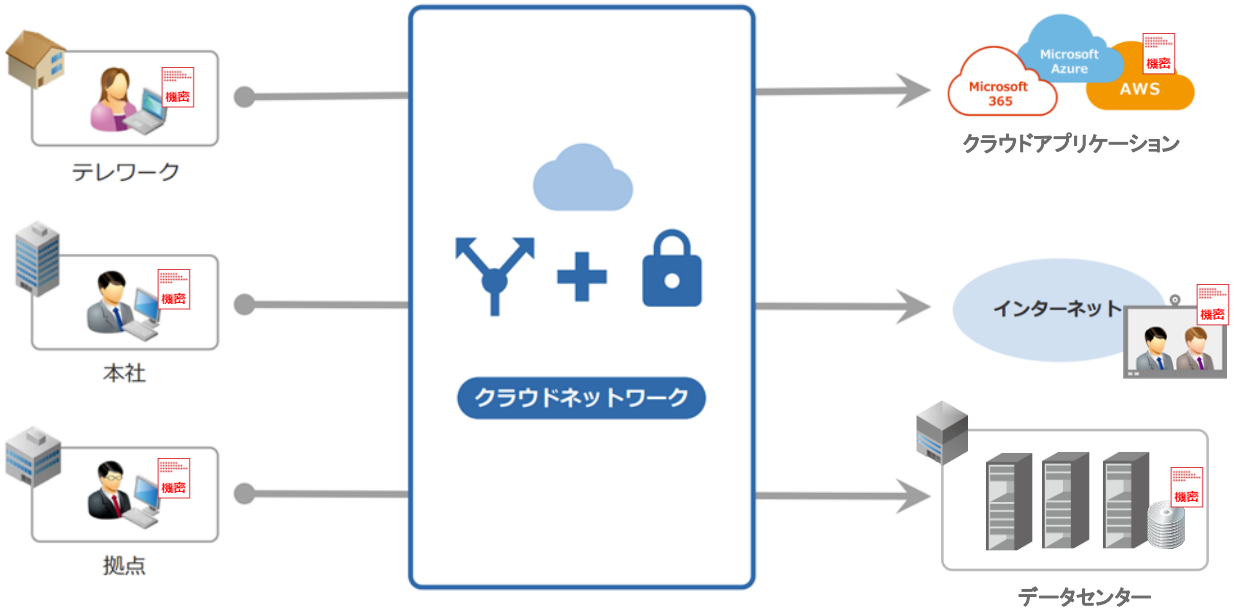
ネットワーク制御とセキュリティ統制を行う方式 のこと。

- ガートナー社が2019年8月に提唱したネットワークセキュリティのコンセプト
- SASE = Secure Access Service Edge の略
  「サッシー」「サシー」とよばれることが多い
- 2024年までに企業の40%が SASE の導入を計画すると言われている

SASE とは？

安全をあたりまえに wizSafe

あらゆる環境から繋がり、安全なネットワークへ



場所・デバイスを
問わずアクセス可能

クラウド上で提供される
ネットワークセキュリティと一元管理

情報資産に
適切にアクセス

SASE の概念

安全をあたりまえに wizSafe

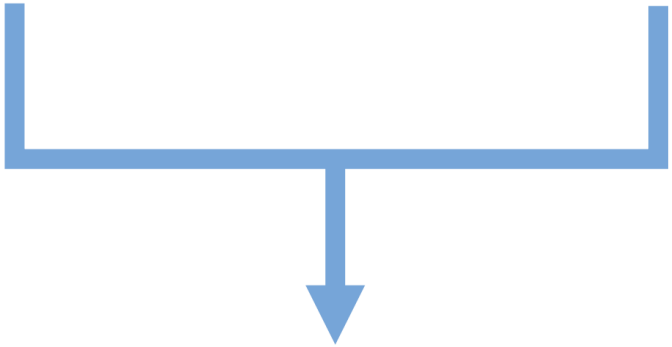
ネットワーク&セキュリティを、包括的にクラウド提供

Network as a service

- SD-WAN
- Carriers
- CDN
- WAN Optimization
- Network as a service
- Bandwidth Aggregators
- Networking Vendors

Security as a service

- Network Security
- CASB
- Cloud SWG
- ZTNA / VPN
- WAAPaaS
- DNS
- RBI



Secure Access Service Edge

SASE の機能群「SWG (Secure Web Gateway)」

安全をあたりまえに wizSafe

Web（HTTP/HTTPS）に関するアクセス制御および可視化

プロキシ機能
HTTPS のヘッダ・リクエスト等を制限する

URL フィルタリング
業務上必要のない分野のアクセスを制限・禁止

アプリケーション識別
業務上必要のないアプリケーションのアクセスを制御/禁止

アンチウイルス
ウイルス・マルウェアの検知・駆除

サンドボックス
未知のマルウェアの検知・駆除

SASE の機能群「CASB (Cloud Access Security Broker)」

安全をあたりまえに wizSafe

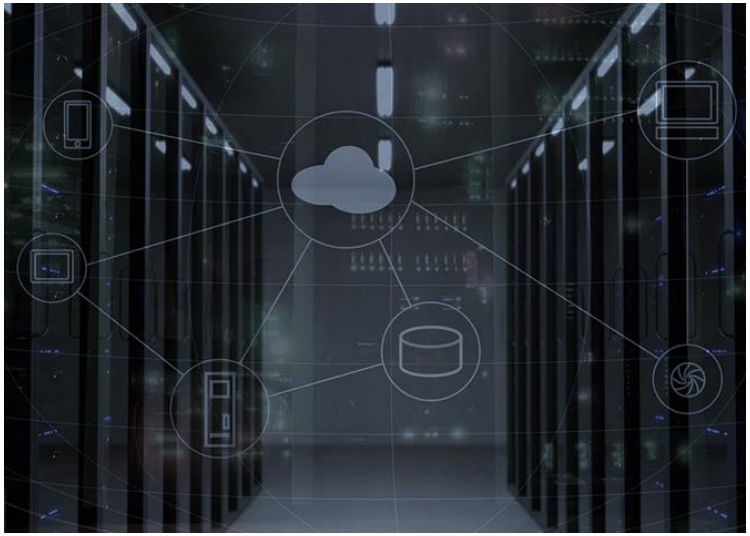
クラウドサービス・アプリケーションに対するアクセス制御および可視化

クラウドサービスの利用状況の可視化と分析
業務上不要なクラウドサービスを制限/禁止、リスクを評価

クラウドサービスの制御
定義したセキュリティポリシに基づきアクセスを制御

DLP
機密情報の定義とその情報漏洩の検知

脅威防御
クラウドサービスに潜む脅威を防御



SASE の機能群「FWaaS (Firewall as a Service)」

安全をあたりまえに wizSafe

ファイアウォール機能をベースとしたネットワークセキュリティ制御

NGFW (Next Generation Firewall)

・Firewall 基本機能

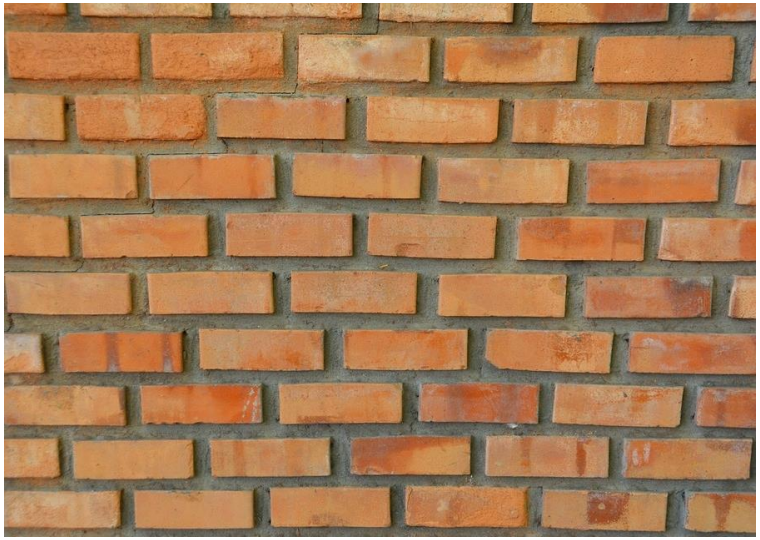
（ステートフルインスペクション）

・アンチウイルス機能

・ネットワークサンドボックス機能

・IPS/IDS機能

・アプリケーション識別機能



SASE の機能群「Network as a Service」

安全をあたりまえに wizSafe

ネットワークエンジニアリング機能の提供

SD-WAN (Software-Designed Wide Area Network)
各WAN拠点にあるネットワークデバイスを一元的に管理

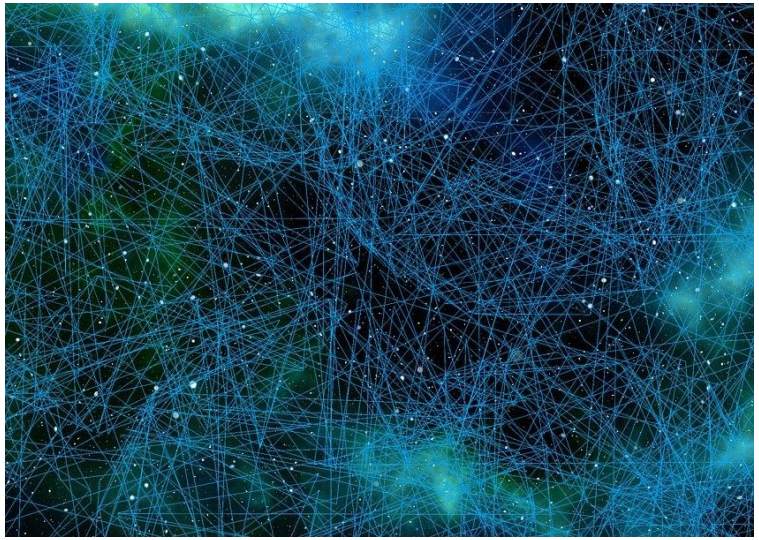
WAN最適化
WAN を流れるトラフィックの速度と効率性を高める

帯域制御
ある基準に基づき、トラフィックの帯域や速度を制限する

リモートアクセス

ルーティング

IPv6



SASE の機能群「ZTNA (Zero Trust Network Access)」

安全をあたりまえに wizSafe

ゼロトラストの概念を取り入れた認証・認可のネットワークアクセス方式

「ゼロトラスト」は2010年に米国のフォレスター・リサーチ社の
ジョン・キンダーバーグ（John Kindervag）氏により提唱された概念。

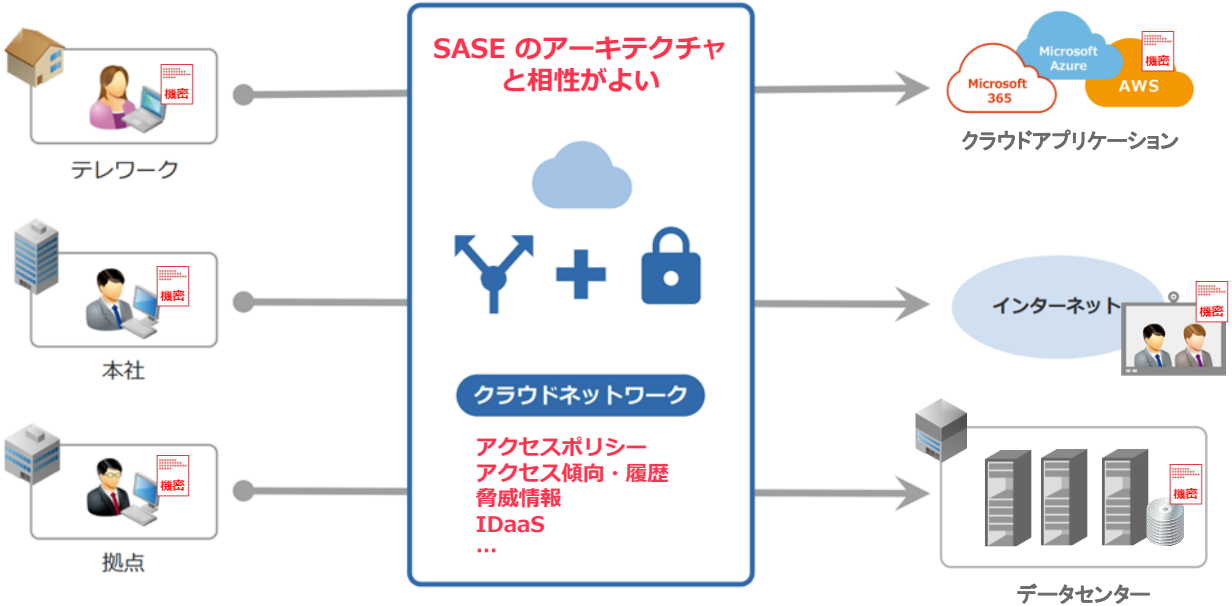
「ゼロトラスト」は社内ネットワークであっても全てのアクセスを信頼しない
性悪説のアプローチであり、実装仕様ではなくコンセプトである。

ZTNA はそれを実践した上で、オンプレミスやクラウド上の情報資産・
リソースへの安全かつ便利なアクセスを実現する機能。

境界を全く意識せず（信用もしない）、常にリソースにアクセスする毎に
認証/認可が実施される。（社内ネットワークは安全という点でVPNとは異なる）

SASE の機能群「ZTNA のポイント」

場所・デバイスに関わらず、適切な認証・認可を実施するのが ZTNA の本質



どの場所・どんなデバイスを使っても、信用はしない

通信を常に監視しつつ、適切なタイミングで認証・認可処理を実施

情報資産に適切にアクセス

ここがポイント！

SASE 導入によるメリット

利便性の向上

場所・デバイスによらず、どこからでも共通の機能が使えるため、エンドユーザにシンプルで使いやすい環境を提供できる。

結果として、それぞれが業務に集中することができる。

セキュリティポリシの統一・運用コストの削減

オンプレミスのハードウェアが最小限にでき、システムバージョンアップの作業等も不要になるため運用コストが削減できる。

また、海外拠点を含めて、場所やデバイスを統合した運用/ポリシを構築できるためセキュリティレベルの向上が期待できる。

また、複雑に機能・機器が絡み合ったオンプレミスシステムのトラブルシュートからも解放され運用がシンプルになる。

パフォーマンスの向上

オンプレミス構成が主の場合、複数のネットワーク機器が組み合わさった複雑なネットワーク構成になっているケースが多い。

SASEの利用により、ネットワーク構成/経路がシンプルになり、不必要な折り返しや帯域によるボトルネックも軽減されるため、

結果としてパフォーマンスが向上する。

安全をあたりまえに
wizSafe

1. 今、SASE に注目が集まっている背景

2. SASE の概要

3. 世の中の SASE ソリューションの特徴・分類

現在の SASE ソリューションの状況

現時点で SASE の機能を
すべて実装しているサービスはまだない と言われている。

実際に SASE を導入していくにあたっては、
それぞれのサービスで得意・不得意があり、
その 特徴を把握すること が重要。

今回はその中で特徴的な傾向を説明する。

SASE ソリューション比較

	SWG（Secure Web Gateway） サービス派生型	Firewall サービス派生型	ネットワーク サービス派生型
概要	SWG を提供しているサービスの 延長線上としての SASE ソリューション	Firewall を提供しているサービスの 延長線上としての SASE ソリューション	ネットワークを提供しているサービスの 延長線上としての SASE ソリューション
特長	SWG に関する機能は充実しており、Web に関するセキュリティ機能は非常に強い。	Firewall 機能をベースに全体的に機能としてバランスが取れている。	SD-WAN を含めたネットワーク機能に強みがある。
注意点	Web(HTTP/HTTPS)以外の通信制御ができないため、Web 以外の通信制御は別の対応が必要になる。	Web (HTTP/HTTPS)通信に特化したセキュリティ機能が不足しているため、Web 通信の制御は別の対応が必要になる。	高度なセキュリティ機能は実装されていないため、高度なセキュリティ機能を利用したい場合は別の対応が必要になる

SASE ソリューション導入時の注意点

安全をあたりまえに wizSafe

SASE は万能薬ではない。いざ導入してみると問題が発生することもある。

出口のＩＰアドレスを共用することに問題はないか？

出口のグローバルIPアドレスが複数顧客で共用されていたり、
動的に変わる可能性がある。

契約上リソースに上限はないか？

クラウドサービスとはいえ膨大なトラフィックを送ると、
パフォーマンス遅延が発生する場合がある。

SASE への集中管理がゆえの課題はないか？

全トラフィックがそこに集まることにより障害時の影響が大きい。
また、悪意のある者に狙われる対象にもなりうる。

必要な機能・拡張性を有しているか？

導入しようとしたときに「こんなはずではなかった」とならないように、それぞれのソリューションの特徴を把握していくことが非常に大事。とくに ZTNA はその傾向が強い。また、既存環境からの移行を踏まえた選定も非常に必要

最後に

SASE (Secure Access Service Edeg) について
概要と特徴を説明してきました。

SASE を導入することによる
メリットのイメージをつかめたのではないかなと思います。

一方で、現実的に導入していくには、各ソリューションの
特徴をつかんでいくと同時に注意すべき事項もあります。

SASE 検討時の参考に活用していただければ幸いです。

wizSafe

安全をあたりまえに