1. **SASEとはどんな概念か？誕生の背景とアーキテクチャの考え方**

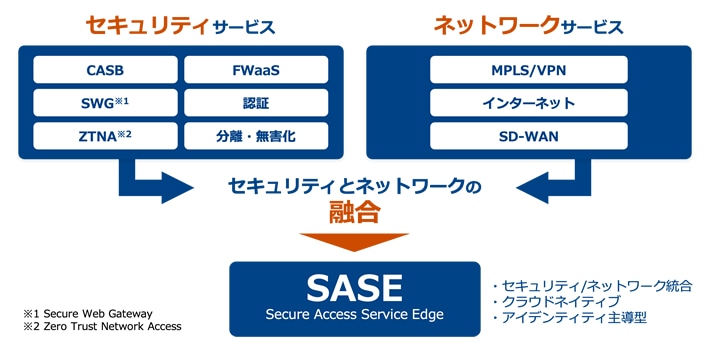
企業の情報セキュリティやIT環境に携わる中で、最近目にする機会が増えたのが「SASE」（Secure Access Service Edge）という考え方です。

SASEとは、IT環境におけるセキュリティ機能とネットワーク機能を1つのクラウドサービスに統合させるという、新たなセキュリティフレームワークの考え方です。  
企業のデジタルトランスフォーメーション推進に欠かせない概念とされるSASEについて、この記事ではアーキテクチャやメリット、懸念事項といった視点から解説していきます。

* [SASEの定義](https://www.ntt.com/business/lp/sase.html?utm_source=pocket_mylist#p1)
* [SASEの概念が生まれた背景](https://www.ntt.com/business/lp/sase.html?utm_source=pocket_mylist#p2)
  + ビジネスにおけるネットワーク利用の現状
  + ゼロトラストとの違い
* [SASEの基本的なアーキテクチャ](https://www.ntt.com/business/lp/sase.html?utm_source=pocket_mylist#p3)
* [SASE導入のメリットと懸念事項](https://www.ntt.com/business/lp/sase.html?utm_source=pocket_mylist#p4)
  + 導入メリット
  + 懸念事項

1. **SASEの定義**

SASEとは、これまで個々に存在していたセキュリティサービスとネットワークサービスを一体にしたネットワークセキュリティの概念です。

図1

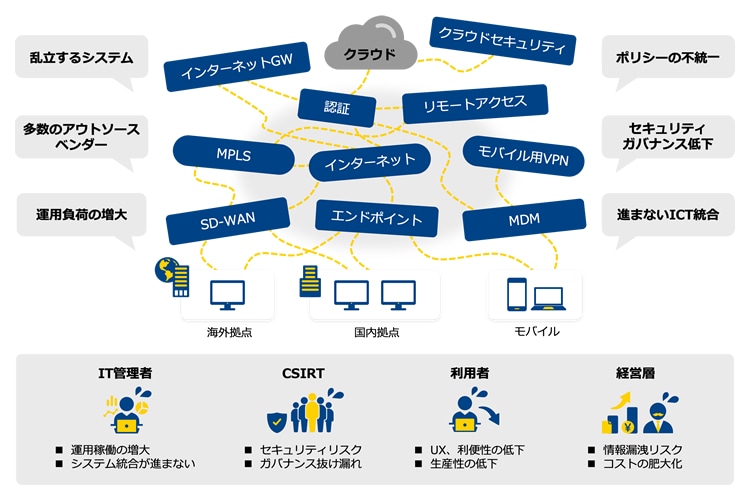
1. **SASEの概念が生まれた背景**

SASEは2019年に初めて提唱された、まだ新しい考え方です。まずはこの概念が生まれた背景について見ていきましょう。

今までのセキュリティやネットワークのアーキテクチャ（構成）は、1つの課題に対して1つのアーキテクチャという形が主流でした。

例えば、社員のPCからのインターネット利用を想定したセキュリティ対策や、リモートワーク環境からクラウドサーバーへのアクセスなど、1つの目的に対して1つのシステムを構築することがこれまでは一般的でした。

その結果、セキュリティやネットワークのシステム全体がツギハギのような形になり、管理・運用コスト増加や接続遅延といったユーザーの利便性低下などが課題になり始めています（図2参照）。

図2

こうした状況は人的コスト増加だけでなく、セキュリティリスクを増大させる可能性もあります。複数のシステムが同時に走る環境では、システムごとのポリシーが統一しづらく、それが外部からの侵入の穴をつくることにつながってしまいます。

また、外部からの侵入を防ぐためにシステムごとにその場しのぎの対策をしてしまうと、トラブルが発生した際に、問題の原因がどのシステムにあるか特定しづらくなるデメリットもあります。例えばマルウェアが侵入したことは判明したものの、端末一台だけなのか、どんな情報が盗まれたのかなど、影響の範囲を調査するのに膨大な時間を要してしまうといったケースが該当します。

セキュリティや利便性を向上するためのシステムやサービスを導入すればするほど潜在的なリスクが増し、管理も複雑化する状況を解決する概念として、SASEが提唱されました。

1. **ビジネスにおけるネットワーク利用の現状**

近年の潮流として、企業のネットワークはVPNのような専用回線だけではなくインターネット回線も併用する傾向にあります。

1つの理由はVPNの運用コストです。セキュリティの面ではVPNを導入するメリットがありますが、事業規模などの面で導入が難しいケースも現実にはあるでしょう。

また、接続する先もオンプレミスからクラウドを利用することが増えていたり、業務で利用するアプリケーションもインターネット上にあるものが増えています。

加えて、2020年は新型コロナウイルスという社会的な要因で都市部や大企業を中心にリモートワークが急速に広まりました。これにより、自宅やサテライトオフィスで働く社員のネットワーク環境としてインターネットを使うことが増えている背景もあります。

ただし昨今はインターネット利用をする上でセキュリティの脅威がどんどん高度化しています。また、製品ごとに得意な機能、不得意な機能があることから「1つの製品を入れれば問題に対処できる」という状況ではなくなっています。そのため、セキュリティの安全を確保するために、必要最小限の製品を組み合わせ、そこからのログを適切に分析する人材や部門（SOC=Security Operation Center）が求められています。

1. **ゼロトラストとの違い**

SASEと同じく、最近ネットワークセキュリティの中で注目されるキーワードとして、ゼロトラストがあります。

ゼロトラストとは、も2010年代に入って登場したセキュリティにおける概念です。

認証なしには何も信用しない（ゼロトラスト）という前提に立ち、「適切な認証を受けた端末とそのユーザーだけが、許可されたデータやアプリケーションにアクセスできる」というゼロトラストの概念は、非常に注目されています。

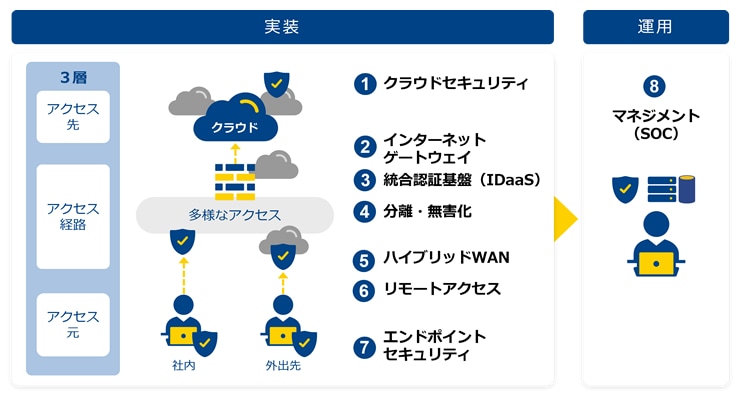
SASEは、このゼロトラストを含むセキュリティ対策の考え方に加え、ユーザーの利便性や運用の最適化までを含めた概念です。

なお、SASEは具体的なソリューションであることに対して、ゼロトラストはあくまでセキュリティを構築する上での考え方である、という違いもあります。

1. **SASEのアーキテクチャ例**

ここからは、弊社が提供している「[SASEソリューション](https://www.ntt.com/business/solutions/cloud-based-ict-infrastructure/sase-solution.html)」を例に、SASEの具体的なアーキテクチャについて紹介していきます。

なお前述の通り、現段階ではSASEは複数の製品を組み合わせることが前提になっているため、企業ごとの事情によって適切なアーキテクチャが違うことを覚えておいてください。

図3

まず、SASEには中心となるクラウドサービス（セキュリティプラットフォーム）が存在し、アクセス元のユーザーはこれを経由してWebなどに接続します（図3-②、⑤、⑥）。

この形式により、IaaSやSaaSに低遅延かつ安全にアクセスできるメリットが存在します。

Webサイトやクラウドサービスに接続する際、今まではVPN経由がメインでしたが、SD-WANやリモートアクセスを導入することでインターネット経由でも繋げられるようになります（図3-⑤、⑥）。この時、アクセス元でのセキュリティリスクをより軽減するための対策を行います（図3-⑦）。

また、クラウドサービスが安全に使えるものなのかどうかを検証するために、CASB（Cloud Access Security Broker）という機能も欠かせません（図3-①）。

さらに、クラウドプロキシーや分離無害化サービスを利用することで、安全なURLにアクセスできているかをチェックしたり、ウイルス感染を防止します（図3-②）。

次に、統合認証基盤によって適切なユーザーの利用か適切な情報アクセス権限になっているかなどを管理します（図3-③）。そして、クラウドプロキシーやエンドポイントセキュリティのログをSOCが相関分析して不正アクセスを検知し、通信遮断や端末隔離などの対応を実施することで、SASEソリューションのアーキテクチャが完成します（図3-⑧）。

1. **SASE導入のメリットと懸念事項**

これまでのネットワークセキュリティやシステム利用の課題を解決する目的で生まれたSASEですが、改めてそのメリットについてまとめてみます。合わせて、導入前に知っておくべき点についてもご紹介します。

1. **導入メリット**

SASE導入により発生する業務レベルでのメリットは次のようなポイントが挙げられます。

* ゼロトラスト実現によるセキュリティ強化
* 働き方改革に対応したネットワーク環境の実現
* 業務の生産性向上
* 運用の一元化による負担減

また、こうしたことを実現した結果として、SASE導入によって企業価値の向上に寄与します。

企業評価の軸としてESG（Environmental, Social, Governance）が注目されています。このESGへの取り組みのうち、ガバナンスには企業としてのセキュリティ対策も含まれています。

特に昨今は、情報漏えいによる企業の信頼性や市場からの評価が下がることも少なくありません。こうしたリスクへの対策をしていることが投資家をはじめ、求職者や取引先、顧客といった社会へのメッセージとなり、企業価値の向上につながります。

1. **導入前に知っておくべきこと**

SASE導入にはデメリット自体はないものの、事前に知っておくべきことが2つあります。

1つは、SASEを実現するための「単一のクラウドサービス」が現時点では存在しないことが挙げられます。

セキュリティやネットワークサービスごとに、それぞれ機能の違いがあるため、自社の要件に応じて製品の組み合わせや構成を考える必要があります。

もう1つは、SASE導入の仕方です。既存のシステムのアーキテクチャすべてを一斉に切り替えることは、現実を考えると良い方法だといえないことがほとんどです。

まずは理想的なシステム構成を考えると同時に、入念な移行計画も同時に検討することがSASE導入前に必要なステップです。

加えて、導入後のことにも事前に検討しておきましょう。クラウドを一元的に運用するには、社内に専門人材を抱えるか、適切なアウトソース先を見つけることが必要になります。

1. **最後に**

SASEは現代のネットワーク利用や、セキュリティにまつわる環境に対応した新しい概念です。

用途ごとに混在するシステムの数が増え、運用や管理が複雑化している状況は、業務面のデメリットだけでなく、セキュリティの潜在的なリスクも抱えることにもなります。

SASEを導入することにより、一元化されたセキュリティ管理を実現し、業務効率や管理コストの向上、そしてその結果による企業価値アップにもつながります。

最初のステップとして、自社に必要なネットワーク環境・セキュリティ環境の要件を洗い出すことから始めてみてください。

[](https://dm.ntt.com/jp_inq_1385_01reg)

* [](https://www.ntt.com/business/solutions/cloud-based-ict-infrastructure/sase-solution.html)
* [](https://www.ntt.com/business/lp/sase-movie.html)