Sec33-01_SASE(Secure Access Service Edge)の概念整理の概念整理

1. 概要

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ある「SASE」（Secure Access Service Edge）という考え方について概念を紹介する。

参考資料

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

https://www.ntt.com/business/lp/sase.html

SASE（Secure Access Service Edge）とは？仕組みやメリットについて徹底解説

https://cybersecurity-jp.com/column/35849

1分で分かるかも？「SASE（サシー）」～ DXに必要なセキュリティー ～

https://www.uniadex.co.jp/annex/security/blog/detail/20200309_sase.html

ゼロトラストの実現とSASE（Secure Access Service Edge）について

https://jpn.nec.com/cybersecurity/blog/201106/index.html

改版履歴

2022年2月10日 改版

2022年1月31日 初版

2. 従来型のセキュリティ対策

境界防御モデル（ペリメータモデル）

境界型セキュリティ」として『境界線（ペリメータ）で内側と外側を遮断して、外部からの攻撃や内部からの情報流出を防止しようとする考え方。

境界型セキュリティでは、「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提となる。防御対象の中心はネットワーク。』と定義

「境界防御モデル」を実現するソリューションはファイアウォールやVPN（Virtual Private Network）、プロキシサーバ、IDS（不正侵入検知システム）やIPS（不正侵入防御システム）など

3. 新しい概念でのセキュリティ対策

「ゼロトラスト」

2010年に米国のフォレスター・リサーチ社（Forrester Research, Inc.）のジョン・キンダーバーグ（John Kindervag）氏により提唱された概念

「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方。

「ゼロトラスト」はコンセプトであり、定義や実現方法は世界中の様々なベンダやセキュリティ企業によって検討が進められ、多種多様な定義や実現方法が存在する

参考資料

「SP800-207 Zero Trust Architecture」（NIST）

https://csrc.nist.gov/publications/detail/sp/800-207/final

「DXレポート
～ITシステム「2025年の崖」の克服とDXの本格的な展開～」（METI)

https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/20180907_report.html

「政府情報システムにおけるゼロトラスト適用に向けた考え方」（政府CIO）

https://cio.go.jp/dp2020_03

4. ユーザーの利便性や運用の最適化までを含めたセキュリティ対策

クラウド時代の新しいネットワークとセキュリティのフレームワーク

テレワークが急速に普及しつつある現在、センター拠点を中心とした従来のネットワークセキュリティアーキテクチャは限界を迎える

ネットワークセキュリティアーキテクチャは限界を迎える

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

個々人の働き方に合わせた快適なインターネット接続を実現するため、いつでもどこからでも接続できる「ネットワーク機能」と、接続の安全性を確保できる「ネットワークセキュリティ」をまとめて提供する

SASE（Secure Access Service Edge）とは

2019年8月に米国のガートナー社（Gartner, Inc.）が公開した「The Future of Network Security Is in the Cloud」で提唱された新たなネットワークセキュリティモデル

The Future of Network Security Is in the Cloud

https://start.paloaltonetworks.com/gartner-report-roadmap-for-sase-convergence.html

包括的なWAN機能と包括的なネットワークセキュリティ機能を組み合わせることで、デジタル企業の動的なセキュアアクセスニーズをサポートする新たな製品。

ネットワーク機能（Network as a Service）とネットワークセキュリティ機能（Network Security as a Service）をクラウド上で組み合わせることにより、オールインワンにサービスを提供するモデル

全てのアプリケーションがデータセンタではなくクラウドプラットフォームに統合

クラウドを前提としたセキュリティー設計であり、自社のデータセンターですらクラウドサービスの一つとして取り扱うというコンセプト

SASEが掲げる2つの重要なコンセプト

デジタル変革を進めるには、自社のデータセンターも一つのクラウドサービスとして捉えクラウドを前提としたセキュリティー設計にするべき

アイデンティティこそがセキュリティーポリシーをかける重要な要素になる。

「デジタルアイデンティティ」

個人の属性情報が電子化され、現実社会における「実体としての人」をデジタル社会における「データとしての人」として存在させる

「アイデンティティ・セキュリティ」

所属や職責、雇用形態などのユーザプロファイルによって、閲覧、変更などの細かいアクセス権限や有効期間などを効率的に管理する

解説

最小特権の原則（PoLP）を用いて、アクセス権を許可、保護、管理する

ネットワーク内の全てのアイデンティティは、業務に必要な最小限のアクセス権しか持たない

職務権限とユーザーの役割に基づいて許可を制限することで、ユーザーがアクセスしてはいけない情報にアクセスして、不注意から、あるいは故意にその情報を用いて何かをするリスクを軽減

組織全体に渡る可視性および一貫性を同じレベルに維持しながら、すべてのアプリケーション、システム、データ、そしてクラウドサービスのアカウント、役割、権限の管理および統制を可能にする

DcX（データセントリックトランスフォーメーション）とは

DXよりも言葉の意味を少し狭めた、データのやりとりや分析・活用を核とした取り組み

「Edge」とは

「Edge」とは、セキュリティサービスの提供者の接続拠点やユーザー企業の各拠点の出入口に設置するデバイスを指す。

SASEの機能

ネットワーク：SD-WAN（Software-Defined WAN、ソフトウェア定義のWAN）

既存の物理回線の上に仮想的なWANを構築し、通信の監視や制御を実現するサービス

輻輳や遅延を防ぐ

セキュリティ機能：ZTNA（ゼロトラストネットワークアクセス）

ゼロトラストの考え方に基づくネットワークアクセス環境を提供するサービス

通信のたびに使用しているネットワーク、デバイスの状態などについて認証

セキュリティ機能：CASB（Cloud Access Security Broker）

「可視化」「コンプライアンス」「データセキュリティ」「脅威防御」で構成

利用者が怪しいクラウドサービスを使い、セキュリティインシデントが発生する事を防止

セキュリティ機能：
FWaaS（Firewall as a Service、クラウド型ファイアウォール）

クラウド上でファイアウォール機能を提供。URLフィルタリングに加え、IPS、アプリケーション制御などの機能を備えた次世代ファイアウォール（NGFW）を含む

セキュリティ機能：SWG（Secure Web Gateway）

WEB通信の可視化やアプリケーション制御を行うことにより、外部への安全な接続方法を提供する

特にクラウドに特化したものをCloud SWGと呼ぶ

参考資料

ゼロトラストの実現とSASE（Secure Access Service Edge）について

https://jpn.nec.com/cybersecurity/blog/201106/index.html

1分で分かるかも？「SASE（サシー）」～ DXに必要なセキュリティー ～

https://www.uniadex.co.jp/annex/security/blog/detail/20200309_sase.html

SASE（Secure Access Service Edge）とは？仕組みやメリットについて徹底解説

https://cybersecurity-jp.com/column/35849

【初心者向け】SASEとは？仕組み・メリット・おすすめサービスを紹介

https://www.nttpc.co.jp/column/network/sase.html

デジタルアイデンティティ入門｜DXに不可欠な重要概念を解説

https://www.nri-secure.co.jp/blog/digital-identity

New SASE Report from Gartner

https://start.paloaltonetworks.com/gartner-report-roadmap-for-sase-convergence.html

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

https://www.ntt.com/business/lp/sase.html?utm_source=pocket_mylist