

MANAGED SERVICE

SASE運用支援サービス

導入後こそが本番。

SASE環境を安全・安定に維持し、使い続けるためのマネージドサービス

対応SASE製品

Zscaler

Netskope

監視・ヘルス管理 / ポリシー運用 / インシデント対応 / 海外拠点对応

アドバンジ日本株式会社

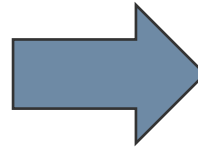
Advange Japan Co.,Ltd

なぜSASEは「導入後」が本番なのか

SASE導入により、運用の対象はネットワーク中心から、ユーザー・アプリケーション・アクセス制御中心へと大きく変わります。

従来のネットワーク運用

- 回線・機器の死活監視
- 拠点ネットワークの保守
- 障害箇所は物理構成から特定
- 変更は機器単位・拠点単位



SASE導入後の運用

- ポリシー・例外申請の継続管理
- ID／認証連携とユーザー権限管理
- ログを横断した多段の原因切り分け
- クラウド側とオンプレ側の同時把握

通信経路とセキュリティ制御が集約されるぶん、可視化・標準化の効果は大きくなります。一方で、複数システムにまたがる事象の切り分けとログ調査は運用負荷が高くなりやすい領域です。この領域を継続的に支えることが、SASE投資の効果を維持する鍵になります。

導入後に生じる5つの運用課題

SASE運用の現場で、実際にご相談をいただくことの多い課題です。

1

切り分けが複雑になる

端末・ネットワーク・SASE基盤・DNS・認証・クラウド側と、原因候補が多層にまたがる。

2

問い合わせが特定の担当に集中する

「サイトが見えない」「社内接続できない」が日々発生し、情報システム部門の工数を圧迫する。

3

ポリシーが業務の変化に追いつかない

人事異動・SaaS追加・拠点新設に設定更新が追いつかず、過剰許可や業務影響が生じる。

4

海外拠点で言語・時差の壁がある

現地ITからの一次情報が整理されず、ベンダーへの英語問い合わせも滞留しやすい。

5

ベンダー窓口の使いこなしが難しい

どの情報を添えて起票すれば早く解決するかが定まらず、往復が増える。

対応が遅れると、起こりうること

SASEは「設定して終わり」にすると、時間の経過とともに導入時の状態から乖離していきます。

起こりえる事象	考えられる影響
退職者アカウントが残ったまま	意図しないアクセスが発生するリスク
ポリシーが業務の変化に追いつかない	業務アプリへのアクセスに支障が出る可能性
SSL復号の除外リストが古いまま	一部の脅威を見逃してしまう可能性
コネクタが片系のまま復旧されない	障害時に社内システムへのアクセスが停止するリスク
クライアントが旧バージョンのまま	既知の脆弱性が残り続ける可能性
SIEMへのログ転送が途絶したまま	インシデントの検知が遅れる可能性
新拠点がポリシー適用外のまま	その拠点だけカバレッジに空白が生じる

いずれも「大きな障害」ではなく、日常の小さな未対応の積み重ねから生じます。

サービス全体像 — 8つの運用領域

日常監視から設定変更、インシデント対応、レポート、ライフサイクル管理までを一括してお引き受けします。

01

監視・ヘルス管理

クラウド基盤・コネクタ・クライアント接続率・ログ転送の稼働監視

02

ポリシー・設定管理

URLフィルタ／SaaS制御／SSL復号／ZTNA権限の変更対応

03

ユーザー・デバイス管理

入退社・組織変更に伴うアカウント／グループ／端末の管理

04

インシデント対応

重大度に応じた初動・調査・復旧・報告

05

変更管理

申請から影響評価・承認・実施・記録までの標準フロー運営

06

レポート・可視化

日次ステータスから月次レポート・四半期レビューまで

07

セキュリティ運用

脅威イベント分析・シャドーIT可視化・SIEM連携

08

ライフサイクル管理

製品アップデート追従・設定棚卸し・最適化提案

監視・ヘルス管理 / ポリシー・設定管理

「壊れていないか」を継続的に見ること、「業務に合っているか」を継続的に整えること。運用の土台となる2領域です。

01 監視・ヘルス管理

クラウド基盤監視

SASEクラウドの稼働状況・インシデント情報を定期確認

コネクタ監視

各拠点の中継サーバーの死活・冗長構成を確認

クライアント接続率監視

全ユーザー・拠点の接続状態を日次確認、急減時にアラート

通信品質監視

エンドユーザー体感の品質指標を監視し、低下時に調査着手

ログ転送監視

SIEMへの転送状態を日次確認、途絶時は検知・復旧対応

02 ポリシー・設定管理

URLフィルタリング管理

許可／ブロックリストの追加・変更、カテゴリ調整

SaaSアプリ制御管理

許可・ブロック・読み取り専用制御の変更対応

SSL復号管理

除外リストの追加・管理、証明書エラーへの対応

ファイアウォール／経路制御

IP・ポート単位のルール、バイパス設定の最適化

ZTNAアクセス権限管理

ユーザー・グループ別のアクセス権限の変更対応

ユーザー・デバイス管理 / 変更管理

人と端末の変化に追従し、設定変更は影響評価と承認を伴う標準フローで実施します。

03 ユーザー・デバイス管理

アカウント管理

入退社・組織変更に伴う追加／削除

グループ管理

作成・変更とポリシー紐付けの更新

クライアント版数管理

新版の情報収集・検証・段階的展開

クライアント配布

新規端末・拠点への配布、MDM設定管理

コネクタ保守

ソフト／OS更新対応、冗長構成の維持

05 変更管理 — 3つの区分と実施フロー

軽微な変更

例：許可／ブロックリスト登録、グループ変更

お客様が変更申請



当社が影響評価・実施



完了をご報告

重大な変更

例：ポリシー体系変更、SSL復号範囲変更、拠点追加

当社が変更案・影響評価



お客様が最終承認



実施・確認結果を報告

緊急変更

例：インシデント対応に伴う即時変更

当社が即時実施



実施後すみやかに報告



翌営業日に事後レビュー

インシデント対応 — 重大度に応じた対応方針

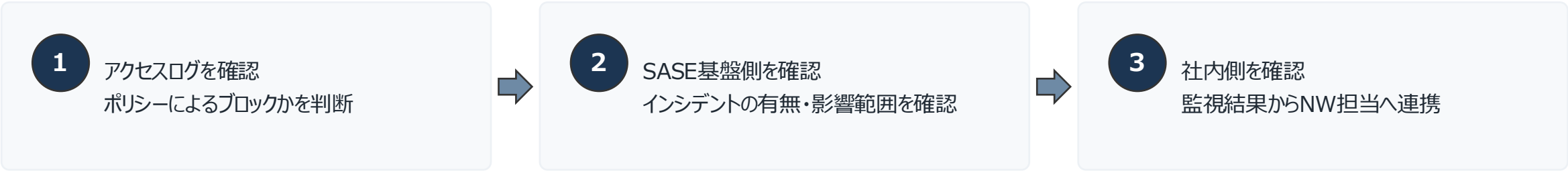
影響範囲に応じて重大度を定義し、初動・エスカレーション・報告の基準をあらかじめ明文化します。（下記は標準的な区分の例です）

最優先	高	中	低
全拠点で通信不可等、業務全体に影響 - 即時に一次対応を開始 - ご担当者へ即時ご連絡 - 製品ベンダーへ同時起票	一部拠点のサービス断、侵害の疑い - 一次～二次対応を実施 - 対応経過を随時ご報告 - 必要に応じ緊急変更を実施	一部ユーザーへの影響、設定起因の不具合 - 調査と暫定対処を実施 - 定期報告のなかでご共有 - 恒久対策を別途ご提案	個別の問い合わせ、軽微な設定確認 - 翌営業日を目安に着手 - 対応完了後に記録 - 月次レポートへ集約

初動目標時間・対応時間帯・報告期限などの具体的なサービスレベルは、お客様の環境・拠点構成・ご要望をふまえて個別に設定いたします。標準（平日日中）／拡張（早朝・夜間）／24時間365日の3形態からお選びいただけます。

障害時の一次切り分け — 3つの領域を決まった順序で

「Webが見えない」「社内接続できない」を、ポリシーによるブロックか、基盤側の障害か、社内側の問題かへ切り分けます。



領域 1	SASE基盤（クラウド側）	稼働状況・インシデント情報をリアルタイムに確認。異常時はベンダーへの確認により障害有無と影響範囲を特定し、原因を切り分けます。
領域 2	コネクタ（中継サーバー）	死活監視・リソース監視により、停止や閾値超過の際にアラートを発報。運用チームが速やかに復旧対応を行います。
領域 3	社内システム／ネットワーク	業務システム・トンネル・拠点ルータの監視結果からイントラ側の障害有無を確認し、ネットワーク担当へエスケーションします。

他製品・既存環境との切り分け

SASE単独では完結しない事象こそ、運用負荷が高くなります。関連する構成要素を順序立てて確認し、責任分界を明確にします。

確認対象	確認内容
端末・ネットワーク	他端末・他ネットワークで再現するか
SASEクライアント	クライアント状態・ログ・バイパス設定
ファイアウォール・回線	FWログと通信経路
DNS	名前解決の可否
ID基盤・認証	認証基盤の障害情報・認証ログ
証明書・SSL	証明書エラーやSSL復号の影響有無
EDR	EDRによる通信遮断・隔離の有無
VPN・クラウド側	経路有無での再現性、事業者の障害情報

切り分けの適用例

- クラウドメールに接続できない

端末・NW → SASE → DNS → ID基盤
- ZTNA経由で社内接続できない

クライアント → DNS → FW → ゲートウェイ
- 業務サイトがブロックされる

Webフィルタ → SSL復号 → IP制限 → EDR
- 他ベンダー領域が原因の場合も、調査結果を添えて連携します。

レポート・可視化 — 現状が見える状態を保つ

日々の稼働状況から中長期のロードマップまで、意思決定に必要な粒度で定期的にご報告します。

日次	日次ステータス	監視結果・インシデント有無・接続率・異常イベント
週次	週次サマリー	週間のインシデント状況・変更実施内容・拠点別ヘルス
月次	月次運用レポート	KPI実績・変更管理台帳・インシデントサマリー・翌月予定
月次	セキュリティ／利用状況レポート	ブロック統計・脅威検知・リスクユーザー・シャドーIT
四半期	四半期レビュー（QBR）	セキュリティ体制の評価・改善提案・ロードマップのご提示

報告内容・頻度・提出期限は、お客様の会議体に合わせて調整いたします。

運用体制モデル

お客様のIT部門、当社の運用チーム、海外現地IT、製品ベンダーの役割と連携経路をあらかじめ定義します。（構成例）



大規模グローバル環境での運用実績

日本の大手製造業のお客様において、Netskope基盤のSASEを含むセキュリティ基盤の設計・展開・運用を担っています。

100,000+ 対象ユーザー数 国内外拠点	110,000 管理端末数（台） グローバル横断	4 統合運用製品領域 SOC／EDR／UEM／SASE	7×24 セキュリティ監視体制 多言語サポート
---	---	--	--

- 主要SASE製品に対応

Zscaler・Netskopeいずれの環境でも、設計・展開・運用をご支援します。
- 大規模グローバル運用の実績

国内外拠点を横断する、大規模かつ複雑なセキュリティ基盤の運用実績。
- マルチプロダクトの統合運用力

SOC・EDR・UEM・SASEを連携させた多層防御体制をワンストップで運用。
- 継続的な品質改善提案力

運用から得た知見を蓄積し、セキュリティ体制の高度化を提案・実現。

運用品質を高める4つの取り組み

定常対応を回すだけでなく、問い合わせそのものを減らし、対応時間を短くする改善活動を継続します。

1

Runbookの整備

代表的な障害・問い合わせごとに、初動からクローズまでの標準手順を明文化。

2

受付テンプレート・切り分け表

受付時に必要な情報を網羅したテンプレートと一次切り分け表を現地ITにも展開。

3

重大度定義とエスカレーション基準

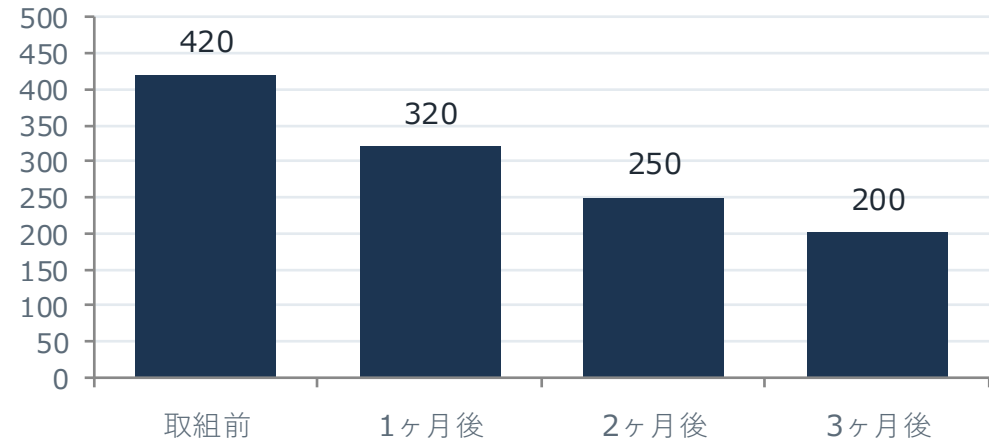
重大度を定義し、優先度に応じた対応・連絡基準を明文化。

4

定例レビューとFAQ化

問い合わせ内容を定期レビューし、よくある事例をFAQとして蓄積・公開。

改善効果の一例（ある大手企業様での実績）



1件あたりの対応時間

短縮

同一原因の再発率

低減

現地ITのエスカレーション

減少

※効果は環境・体制により異なります。

ご提供形態

Zscaler・Netskopeいずれの環境にも対応。拠点構成・業務時間・ご予算に応じて対応時間帯と範囲を組み合わせます。

標準

平日日中

- 監視・ヘルス管理
- ポリシー・設定管理
- ユーザー・デバイス管理
- インシデント対応・変更管理
- レポート・可視化

拡張

早朝・夜間まで対応

- 標準の全範囲
- 対応時間帯の拡張
- 重大度に応じた時間外初動
- 海外拠点の時差考慮

グローバル

24時間365日

- 拡張の全範囲
- 多言語（日本語／英語）対応
- セキュリティ運用（SOC連携）
- 四半期レビュー（QBR）

SASE運用のご相談を承っています

現在の運用体制の棚卸しから、部分的な運用のお引き受けまで対応いたします。

アドバンジ日本株式会社

〒163-0722 東京都新宿区西新宿2-7-1 新宿第一生命ビル22階
TEL 03-6908-6908 / FAX 03-6304-5370

sales@advange.co.jp