

MANAGED SERVICE

EDR運用支援サービス

導入したEDRを、確実に機能する状態へ。

導入状況・稼働・除外設定・バージョン・ポリシーを継続確認し、是正まで支援します。

対応EDR製品

**Microsoft Defender
for Endpoint**

CrowdStrike

Tanium

その他のEDR製品もご相談いただけます。

アドバンジ日本株式会社

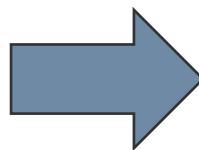
Advange Japan Co.,Ltd

EDRの保護状態は、導入した時点がピーク

端末、業務、例外設定、製品バージョンは導入後も変化し続けます。運用を止めると、保護は静かに弱まっていきます。

導入直後の状態

- 対象端末に一斉展開されている
- ポリシーが統一されている
- 除外設定は最小限
- 全端末が最新バージョン



運用しない場合の1年後

- 新規端末・サーバーに導入漏れ
- 停止したエージェントが放置される
- 業務都合の除外が積み上がる
- 旧バージョンの端末が残存する

EDRは「入れたかどうか」ではなく「いま全端末で機能しているか」で価値が決まります。導入状況・稼働・除外・バージョン・ポリシーを定期的を確認し、差分を是正し続けることが、投資した保護水準を維持する唯一の方法です。

EDR導入後に生まれる、4つの運用ギャップ°

保護状態を維持するには、導入後の定期的な確認と是正が欠かせません。

01

未導入・停止端末

新規端末やサーバーへの導入漏れ、エージェント停止により、監視対象外の端末が発生する。

02

長期化した除外設定

業務影響を避けるために追加した例外が見直されず、検査されない範囲が残り続ける。

03

バージョン・ポリシーの差異

更新の遅れや設定差異により、一部の端末で必要な保護機能を利用できない状態になる。

04

検知後の確認・対処

利用者、端末用途、業務影響が分からず、アラートの判断と初動対応に時間がかかる。

対応が遅れると、起こりうること

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。

起こりえる事象	考えられる影響
新規端末にEDRが導入されないまま	その端末だけ検知・遮断が働かない
停止したエージェントが気づかれない	監視対象から外れた端末が残り続ける
業務都合で追加した除外が残り続ける	検査されない範囲がじわじわ広がる
一部端末が旧バージョンのまま	新しい検知・防御機能を利用できない
部門ごとにポリシーがばらつく	同じ脅威でも端末により結果が変わる
誤検知が放置され通知に慣れてしまう	本当に対応すべきアラートを見落とす
検知時に利用者・端末用途が分からない	初動判断と関係者への連絡に時間がかかる

「導入済み」と「保護されている」は同じではありません。差分を定期的に見つけ、是正する仕組みが必要です。

サービス全体像 — 6つの運用領域

現在の製品、エディション、構成、社内体制を確認し、必要な運用項目から段階的に引き継ぎます。

01

導入率・稼働状況

正常・停止・旧バージョン・未導入に分類し、対応対象と進捗を管理

02

除外設定管理

申請理由・対象・期限・承認を記録し、不要になった例外を定期確認

03

エージェント更新

影響確認、検証、段階展開、未更新端末のフォローまでを管理

04

ポリシー管理

端末用途や部門に応じて、保護設定と業務影響のバランスを調整

05

検知チューニング

誤検知・重複通知・優先度を確認し、対応対象と判断基準を明確化

06

問い合わせ・障害対応

エージェント不調、誤ブロック、更新失敗を切り分け、利用者対応まで

導入率・稼働状況管理 / 除外設定管理

「どの端末が保護されていないか」を毎月特定し、「なぜ検査されない範囲があるか」を管理下に置きます。

01 導入率・稼働状況管理

端末台帳との突合

資産台帳とEDR管理コンソールを定期照合

状態の分類

正常／停止／旧版／未導入に分類し対応対象を特定

未導入端末への展開

導入手順のご案内、代行導入、完了確認

停止端末の是正

原因確認、再導入、利用者へのご案内

導入率の可視化

部門別・拠点別の推移を月次でご報告

02 除外設定管理

申請受付と記録

理由・対象・期限・承認者を台帳に記録

影響評価

除外による検査範囲への影響を事前に確認

期限管理

期限到来時に継続要否を確認し、可否を判断

定期棚卸し

不要になった除外を抽出し、削除をご提案

リスクの可視化

除外件数と対象範囲を月次でご報告

エージェント更新 / ポリシー管理

更新は業務影響を見ながら段階的に。ポリシーは端末用途と業務のバランスを見て調整します。

04 ポリシー管理

用途別ポリシー設計

端末用途・部門に応じた保護設定

業務影響の調整

保護強度と業務効率のバランス確認

設定差異の是正

意図しない差異を抽出し統一

変更管理

申請・影響評価・承認・実施の記録

定期レビュー

製品機能の追加に合わせて見直し

03 エージェント更新 — 段階展開の流れ

確認・検証

リリース内容と既存環境への影響を確認

リリース情報の確認



影響評価



検証環境で確認

段階展開

影響の小さい範囲から順に適用

パイロット部門



一般部門へ拡大



全社展開

フォロー

取り残された端末を確実に拾う

未更新端末の抽出



個別に是正対応



完了確認・報告

検知チューニング / 問い合わせ・障害対応

アラートを「見るべきもの」に絞り込み、利用者からの問い合わせは一次対応から引き受けます。

05 検知チューニング

検知傾向のレビュー

週次・月次で検知内容と件数を確認

誤検知の切り分け

業務起因かを確認し、除外可否を判断

重複通知の整理

同一原因の通知をまとめ、通知先を調整

優先度の定義

対応対象と判断基準を明文化

変更内容の記録

チューニング結果と根拠を台帳化

06 問い合わせ・障害対応

エージェント不調

起動しない・通信しない等の切り分け

誤ブロック対応

業務アプリのブロック解除判断と手順

更新失敗

失敗原因の特定と再実行

端末交換・再導入

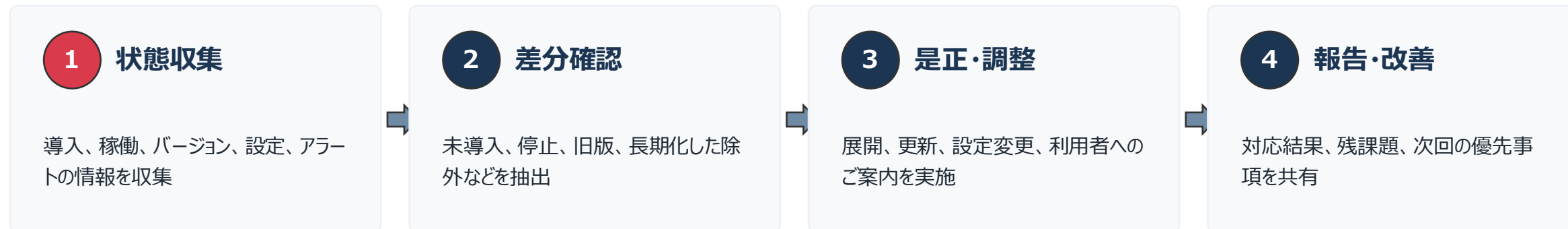
キッティング時の導入確認と登録整理

利用者へのご案内

作業依頼、状況連絡、完了報告

運用プロセス — 月次の状態確認を、是正と改善につなげる

端末台帳とEDRの情報を照合して対応対象を特定し、優先順位と承認範囲に基づいて是正します。



役割分担

変更承認、端末情報の提供、実施権限、連絡経路をあらかじめ明確化します。

多言語・海外拠点

現地IT担当者と利用者への確認・ご案内・調整を、日本語／英語で支援します。

SOC連携

24時間365日の監視、判断、端末隔離を含む体制の設計にも対応します。

アラート対応の流れ

検知そのものより、「誰の、何に使う端末で、業務にどう影響するか」を素早く確定させることが初動を決めます。

1 アラート受領

検知内容・重大度・対象端末を確認

2 トリージ

既知の誤検知か、対応要否を判断

3 端末・利用者の特定

台帳と突合し、所属・用途・所在を確認

4 業務影響の確認

隔離した場合の影響をご担当者と確認

5 対処

隔離・駆除・除外判断を実施

6 記録・報告

対応内容と再発防止策を記録し共有

初動を早くする3つの前提

端末台帳の鮮度

所属・用途・利用者が最新であること

隔離の判断基準

誰が、どの条件で隔離を決めるかの事前合意

連絡経路

夜間・海外拠点を含む到達可能な連絡先

対応製品と対応範囲

製品ごとの管理機能と既存の運用ルールを確認し、お客様と当社の役割、対応権限、SOCとの連携範囲を定義します。

Microsoft Defender for Endpoint

- オンボーディング状況の管理
- センサー状態の監視と是正
- ポリシー・除外設定の管理
- アラート確認とチューニング
- Intune・Entra ID連携の運用

CrowdStrike

- センサーの展開・稼働管理
- 防御ポリシーの設定と調整
- 除外設定の管理・棚卸し
- 検知内容の確認とチューニング
- センサー版数の段階更新

Tanium

- 端末情報の可視化と台帳突合
- 対象端末の把握と配布管理
- 未導入・停止端末の抽出と是正
- ソフトウェア・パッチ配布の管理
- 検知・対処は導入モジュールに依存

その他のEDR製品もご相談いただけます。製品・エディション・契約機能・既存構成を確認したうえで、対応可否と運用範囲をご案内します。Taniumは端末の可視化・管理を中心とした運用支援となり、検知・対処の範囲は導入モジュールにより異なります。

EDR運用支援とSOC／MDRの役割分担

EDR運用支援は「保護状態を維持する」役割、SOCは「24時間365日、検知して判断する」役割です。単独でもご利用いただけます。

業務	お客様	EDR運用支援（当社）	SOC／MDR
24時間365日の監視・脅威検知	－	－	●
アラートの一次判断・エスカレーション	－	○	●
端末・利用者・用途の特定	○	●	－
業務影響の確認と隔離可否の判断	●	○	○
端末隔離・駆除の実施	－	○	●
除外設定・ポリシーの変更	○	●	－
導入率・稼働状況の維持と是正	－	●	－
月次報告・改善提案	○	●	○

●：主担当 ○：支援・確認 －：範囲外

SOCはオプションです。ご契約済みの場合は既存SOCとの連携を設計します。

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）



EDR運用主管の役割

保護状態の品質管理／是正の優先順位づけ／改善提案／お客様との窓口

EDR運用担当の役割

状態収集・差分抽出／展開・更新・設定変更／問い合わせ対応／ベンダー調整

月次レポートの構成 / ご提供形態

「いま何台が保護されていないか」「なぜそうなっているか」「次に何をするか」が毎月分かる状態にします。

月次レポートに含まれる項目

導入率・稼働状況サマリー	部門別・拠点別の推移
未対応端末リストと進捗	対象・原因・対応予定
除外設定の一覧と期限	件数・対象範囲・棚卸し結果
バージョン分布	旧版端末の割合と更新計画
検知・アラートサマリー	件数、傾向、対応結果
チューニング実施内容	変更点と判断根拠
残課題と次月の優先事項	改善提案を含む

ご提供形態

標準 平日日中

月次の状態確認・是正・報告と、問い合わせ対応まで。

拡張 早朝・夜間まで対応

標準の全範囲に加え、時間外の初動対応と海外拠点の時差考慮。

グローバル 24時間365日／SOC連携

拡張の全範囲に加え、多言語対応、SOC連携、四半期レビュー。

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、EDR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。

110,000

管理端末数（台）

グローバル横断

100,000+

対象ユーザー数

国内外拠点

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

- 複数のEDR製品に対応

既存のEDR環境をそのまま活かし、必要な運用項目から段階的に引き継ぎます。

- 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。

- 海外拠点を含む多言語対応

現地IT担当者と利用者への確認・案内・調整まで日本語／英語で支援します。

現在のEDR保護状態を、確認してみませんか。

未導入・停止端末、バージョン、除外設定、運用体制を確認しご提案します。

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

※ Microsoft、Defender、CrowdStrike、Taniumは各社の商標または登録商標です。