

「アラート疲れ」の次に来る落とし穴

～MDR/SOCは”どこまで対応してくれるか”で選ぶ～



会社概要

社名	株式会社NSD
設立	1969年4月8日(昭和44年4月8日)
資本金	72億5百万円
従業員数	4,555名(連結) (2026年3月末日時点)
業務内容	システム開発事業 (1) ITコンサルティング (2) システムの企画・設計・開発 (3) ITインフラの構築 ソリューション事業 (1) ITを利用したサービスの提供 (2) ソフトウェア・プロダクトの販売
上場取引所	東京証券取引所 プライム市場
売上高	117,813百万円 (連結) (2026年3月期)
事業所	東京(本社)、大阪、名古屋、福岡、札幌、仙台、広島



PMI®ATPロゴは、Project Management Institute, Inc. の登録商標です。



皆さんのMDR/SOC、
“対応します”の
『対応』はどこまでですか？

今日、この問いに対する
答えを持ち帰ってください。

EDR導入後に 起きたこと



検知できるようになった。
でも、**運用負荷は増えた。**

→ アラートは増えた。しかし、それを”処理する人”は増えない。

そしてMDR/SOCへ

アラート処理を任せたい。その願いから生まれたのが、MDR/SOC。



“これで安心”

→ 多くの企業が、ここで“終わり”だと思っていた。

しかし、本当の落とし穴はここではない。

“対応してくれる”
—
と思っていた。

でも、どこまで？

EDRを家の 防犯に例えると



防犯カメラ

+



侵入センサー

= EDR



POINT

“泥棒を見つけて、教えてくれる”

MDRなら 警備員が見てくれる



監視センターの警備員

あなたの代わりに
カメラ映像を見てくれる
専門家



異常を検知し、
内容を確認し、
現場に駆け付ける。

——
ここまでが
多くの人が想像するMDR。



警備員が、庭で1人の泥棒を確保。



対応完了です。
……本当に？

警備員は
帰っていく



対応完了です。

.....

「捕まえたので、対応完了です。」

え、連れて行ってくれないの？



他にも 侵入者は いるのでは？

「他の侵入者を調べるのは
別料金です。」

1人目の泥棒を捕まえても、
他の場所に別の泥棒が潜んでいるケースは、調査しなければ分からない。



割れた窓。 開いた扉。

『侵入経路調査は、
サービス対象外です。』



なぜ泥棒が入れたのか。
分からないまま、次の日も安心して暮らせるだろうか？



事件の対応は完了した。
でも、家に戻っても
本当に安全なのか分からない。」

もう家に戻って
いいですか？

『安全かどうかは、お客様でご判断ください。』



HOME

ホームセキュリティ

- ✓ 防犯カメラで「見つける」
- ✓ 警備員が「駆け付ける」
- ~~✗ 他に泥棒がいなか調べる~~
- ~~✗ 侵入経路を調べる~~
- ~~✗ 危険がなくなったか確認する~~



CYBER

サイバーセキュリティ

- ✓ EDRが「検知する」
- ✓ SOCが「アラートに対応する」
- ~~✗ 横展開する脅威を調べる~~
- ~~✗ 侵入経路・根本原因を調べる~~
- ~~✗ 「安全か」を確認する~~

問題は、"対応"という言葉の**解釈**。

"対応"という言葉 分解すると



CORE MESSAGE

"対応"は1つの言葉ではなく、**8つの工程。**



どのベンダーが、どこまでを行うのか。
ここを契約前に確認する必要がある。

あなたのMDRは、どこまで？

	① 検知	② 脅威判定	③ 封じ込め	④ 影響範囲 調査	⑤ 原因調査	⑥ 脅威排除	⑦ 復旧支援	⑧ 安全確認
 サービスA								検知・封じ込めまで
 サービスB								原因調査まで対応
 サービスC								

"対応あり"では、サービスを比較できない。

8工程のうち、どこまでがサービス範囲なのか。明示されていない限り、比較になりません。

検知端末への対応

≠

インシデント全体への対応

WORLD A

検知端末1台だけ調べる世界



≠

WORLD B

環境全体を調べる世界



1台を止めることと、インシデントを収束させることは、違う。

いざ、インシデントが発生してみると

こんなはずじゃな
かった…

実際にあったこと

ケース1：IRは〇時間まで



契約内

例：〇時間まで



追加費用

それ以降

インシデントは
営業時間内に
収まるとは限らない。

■ 一定時間までは契約内

■ それ以降は追加費用 ——— 時間制限は、契約前に確認すべき最重要項目

真夜中にランサムウェアが発生したら、その対応も契約内か？

ケース2：横展開調査は別途

INFECTED ENVIRONMENT

PC-A

⚠ 検知
✓ 調査済み

PC-B

?
未調査

PC-C

?
未調査

SERVER

?
未調査

他にも 侵害されていないか？

→ 追加調査

(契約範囲外)

1台の調査で
"他に侵害がない"
とは、言えない。

ラテラルムーブメント — 感染は、1台では止まらない。

ケース3： 復旧判断は誰がする？

SOC

「脅威を
隔離しました。」

？

顧客

「で、もう業務を
戻していいんですか？」

REALITY

最後の判断が、自社に残る。

——派遣されたインシデントレスポンス担当が
「全部対応します」と言わなかったか。
その範囲を、契約後に知るケースが多い。

契約前と発生後の ギャップ

BEFORE 契約前のイメージ

「全部任せられる」

- ✓ 24時間365日監視
- ✓ 脅威に対応
- ✓ 専門家に対応
- ✓ 安心



AFTER インシデント発生後

「これが現実…」

- × ここから先は別料金
- × 対象端末以外は対象外
- × 原因調査はオプション
- × 安全確認は自社判断

期待と、**契約範囲**のギャップ。

—— このギャップを知らずに契約すると、インシデントは"最初の"リスクから始まる。

1台を隔離した **≠** 会社が安全になった

左：STOPPED

感染PCを隔離した状態

PC-A	✓ 隔離
PC-B	?
PC-C	?
SV	?

右：CONFIRMED SAFE

環境全体を確認、
脅威が排除された状態

PC-A	✓ 脅威排除済み
PC-B	✓ 影響なし確認
PC-C	✓ 影響なし確認
SV	✓ 影響なし確認



"止めた"だけでは、"終わった"とは限らない。

"安全"を判断するために 必要な6項目

01

攻撃対象の特定

何が何に侵入されたのか



02

影響範囲の確認

どこまで広がっているか



03

横展開の確認

他の端末・サーバーは無事か



04

侵入経路・
根本原因の確認

どう侵入を許したのか



05

脅威の排除

完全に消えたことの確認



06

業務再開判断に
必要な情報

"戻してよい"と言える根拠



MESSAGE

6項目全てが、
"はい"と
答えられないなら、
"安全"ではない。

—— どちらか分からない、ではなく、
確認して"安全"と言える状態を、
作ること。

6項目を確認してくれるサービスを、契約前に選ぶ。

MDR/SOC選定で 確認する7つの質問

Q1 IR対応に時間制限はありますか？

例：SLA時間、平日/休日、深夜帯

Q2 検知端末以外も調査しますか？

例：横展開調査、サーバー影響範囲

Q3 封じ込めは誰が実施しますか？

例：SOC側か、顧客側か、共同か

Q4 侵入経路・根本原因まで調べますか？

例：発生源の特定、ログ解析の範囲

Q5 脅威排除・復旧支援はどこまでですか？

例：マルウェア除去のみ、リストア支援まで

Q6 追加料金が発生する境界はどこですか？

例：時間、調査台数、担当者の追加

Q7 ”もう安全か”を判断するために何を提供しますか？

例：報告書、再発防止提案、業務再開サインオフ

「MDRを導入しているか」ではなく、
「有事の際、誰が、どこまでやってくれるか」を確認してください。

あなたのMDRの「対応」は、
どこまでですか？



“見つける”だけでなく、“止める・調べる・排除する”まで任せられるMDR

ソフォス株式会社 Corporate Overview

- 創業：1985年(英国オックスフォード)
- 事業内容：
 - ・ ITセキュリティソリューションの開発・販売・サポート
 - ・ 脅威解析センター「Sophos Lab」からのセキュリティサービスの提供
- 従業員数：全世界約3,500名
- 顧客数：約60万社以上(150カ国)
- 利用者数：1億ユーザー以上(150カ国)
- 売上：約1,700億円規模

SOPHOS MDR が選ばれる “3つのPoint”

Point 01

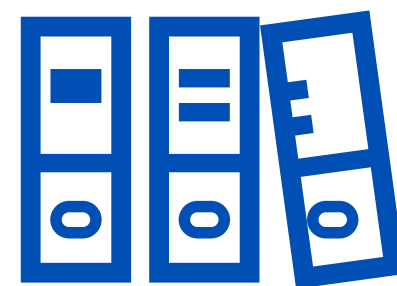
24時間365日の対応



ベンダーが昼夜問わず、検出～駆除含めた
対応を行うサービス

Point 02

インシデントレスポンス



時間無制限でデータ収集・解析から
影響範囲の特定及び復旧までを行うサービス

Point 03

補償



万が一の暗号化被害に対しての
金額面での補償が含まれたサービス

他社のMDRサービスとの大きな違い

	 SOPHOS	他社
サービス提供時間	24時間365日 同じサービスを提供	平日日中のみ 人による調査対応時間が制限
対応内容	検知、調査、対応(脅威の除去)までを 24時間365日実施	アラートのみで端末隔離 調査は平日のみ 脅威の除去は顧客で実施
検知・調査・対応完了時間	検知、調査、対応まで平均38分	1時間以内の調査開始や 平日日中の調査のみの記載で 完了時間は未掲載
最小契約ライセンス	1ライセンス (端末1台、サーバー1台からOK)	300ライセンス以上
対象製品	EDRだけでなく、その他の危機のアラートを 含めた分析、調査が可能	EDRが導入されたサーバー、 端末のみ

他社は対象範囲や日時で内容が異なり、SOPHOSは同じサービスを提供可能！

SOPHOS



Sophos XDR



Sophos Endpoint



Sophos Firewall



Sophos Cloud



Sophos NDR



Sophos Email

Endpoint

Microsoft CrowdStrike
SentinelOne TrendMicro
Symantec BlackBerry

Firewall

Paloalto Fortinet
CheckPoint F5
Cisco(Meraki)
SonicWall WatchGuard
Forcepoint Barracuda

Identity

Microsoft Okta
Duo ManageEngine
Cisco(ISE) auth0

Email

Microsoft Proofpoint
Mimecast Google

Productivity

Microsoft
Google

Network

Darktrace Vectra
Canary Cisco(Umbrella)
Skyhigh Secutec
Zscaler

Cloud

Microsoft AWS
Google Cloud Orca

Backup / Recovery

Veeam
Acronis

SOPHOSなら 1ライセンスから契約可能！

＼ こんな企業様におすすめです ／

自社のユーザー規模に合わせて契約したい

セキュリティを強固にする必要がある一部の部署のみ導入したい

重要な端末のみ導入したい

各サービスをトライアル感覚で試してみたい



NSDはSOPHOS社認定のプラチナパートナーです。
セキュリティに関するお悩みお気軽にご相談ください。

株式会社NSD 市場開拓事業部

☎ お電話でのお問い合わせ

(東京) 03-3257-1141

(大阪) 06-6442-1329

平日09:00-17:00

✉ メールでのお問い合わせ

products@nsd.co.jp

会社名、氏名、お電話番号、メールアドレスを
ご記入の上、お問い合わせください。

<https://www.products.nsd.co.jp/service/sophos>

当社のホームページでも資料請求・お問い合わせができます。

ご清聴ありがとうございました。

