

セキュリティガイドシリーズ #01

EDR導入 選び方ガイド



セキュリティガイドシリーズ #01

EDR導入 選び方ガイド

目次

1. EDRの導入のメリット

- ① EPPで防げなかった攻撃をリアルタイムで検知
- ② インシデント対応を効率化・迅速化できる
- ③ セキュリティ状況の見える化

2. EDRの主要な機能

- ① 検知
- ② 隔離
- ③ 調査・復旧

3. EDR製品の選び方、ポイント

- ① 検知・分析の正確性
- ② 調査・復旧のサポート機能
- ③ 機能の拡張性
- * 【注目】自動修復機能

今、世界で注目されているEDRとは？

MERIT

メリット

EDR（Endpoint Detection and Response／エンドポイントの検知と対応）は、組織のセキュリティ対策を強化するための重要なツールです。EDRを導入することで得られるメリットについてご紹介いたします。



MERIT

メリット

①EPPで防げなかった攻撃をリアルタイムで検知

EDRはエンドポイント上での異常な動作やパターンを監視し、これまでの攻撃履歴や行動分析をもとに、未知の脅威を特定するソリューションです。

従来の「EPP」は、既知の脅威に対しては高い効果を発揮するものの、新たに発見された**未知のマルウェア**や**持続的標的型脅威（APT）**への対応は難しい場合がありますが、**EDRを導入することで、これらの高度な攻撃をリアルタイムで検知**できるようになります。

例）通常の業務時間外に行われる大量のデータ転送や、許可されていないアプリケーションの実行など、EPPでは見逃されがちな異常をリアルタイムで捕捉



検知した脅威に対して即座にアラートを発することで、**初期対応や攻撃の進行を阻止するための対策を講じやすくなります。**

※ EPP（Endpoint Protection Platform／エンドポイント保護プラットフォーム）



MERIT

メリット

②インシデント対応を効率化・迅速化できる

インシデントとは、事故が発生する恐れのある状況を意味します。従来の手法でインシデント対応を行う場合、**ログの分析や原因特定に多大な時間と労力を要しますが、EDRを導入することで、このプロセスを大幅に効率化・迅速化**できます。

例) EDRは攻撃者の侵入経路や攻撃の進行状況を詳細に追跡し、被害範囲を正確に把握。これにより、適切な封じ込め戦略を迅速に実行し、攻撃の拡大を防ぐことが可能。

さらに、EDRには自動応答機能が備わっており、特定の条件下で自動的に隔離やシャットダウンなどの対応を実行するので、**人手を介さずに初期対応を迅速に行うことで、被害の拡大防止**につながります。

また、EDRは他のセキュリティツールと連携することもできるので、より総合的なセキュリティ対策を構築できます。

例) SIEMシステムやファイアウォール、ウイルス対策ソフトウェアと統合することで、全体的なセキュリティ態勢を強化し、脅威に対する多層的な防御を実現。

※ SIEM (Security Information and Event Management)

MERIT

メリット

③セキュリティ状況の見える化

EDRは、組織全体のセキュリティ状況を可視化するためのツールとしても機能します。エンドポイント上で発生したすべてのイベントを詳細に記録し、それらをダッシュボード上で視覚的に表示します。



攻撃の兆候や異常な活動を一目で確認できるため、**潜在的な攻撃を早期に発見し、被害を最小限に抑えやすくなります。**



また、セキュリティ管理の一元化が可能となり、複数のエンドポイントからのデータを一括して監視・管理することができます。これにより、セキュリティチームは**異なるシステムやデバイス間の整合性を確保しやすくなり、迅速かつ効果的な対応が可能**になります。



このほか、レポート機能が充実したEDR製品を利用することで、セキュリティポリシーの改善点や新たな脅威に対する対応策を見出すことができ、**組織全体のセキュリティレベルを継続的に向上させることが可能**です。

FUNCTION

機能

EDRの主要な機能として、「検知」「隔離」「調査・復旧」があげられます。それぞれの詳細についてご紹介いたします。



FUNCTION

機能

①検知

EDRの「検知」機能は、エンドポイント上での**異常な行動や脅威の兆候をリアルタイムで把握**するための機能です。具体的には、以下のような状況で動作します。



✓ 異常なプロセスの起動

通常業務では実行されない不審なプロセスが起動した場合、EDRはそのプロセスの振る舞いを監視し、異常が検知されるとアラートを発します。

例) 通常のアプリケーションが予期しないファイルアクセスやネットワーク通信を行った場合など



✓ 不正なファイルの操作

正規のソフトウェアによるファイル操作とは異なった、疑わしいファイルの作成や変更が行われた場合の検知も可能です。

例) マルウェアがシステムファイルを改ざんしようとする場合など



✓ ネットワーク通信の異常

エンドポイントが通常のトラフィックとは異なる通信を行っている場合にも検知し、警告を発します。

例) 外部サーバーへの異常なデータ転送など

これらの検知機能により、**従来のセキュリティ対策では見逃しがちな脅威を早期に発見し、迅速な対応が可能**になります。

FUNCTION

機能

② 隔離

EDRの「隔離」機能は、**検知された脅威からシステムやネットワークを保護**するための措置です。具体的な動作は、以下の通りです。



✓ 感染したエンドポイントの隔離

マルウェアや攻撃者によって危険な動作が検知された場合、EDRはそのエンドポイントをネットワークから切り離し、他のシステムやデータへのアクセスを遮断します。これにより、感染の拡大を防ぎます。

例) マルウェアに感染したコンピュータをネットワークから自動的に切り離す



✓ 疑わしいプロセスやファイルの隔離

疑わしいプロセスやファイルが発見された場合、それらを一時的に隔離し、システムの他の部分への影響を防ぎます。

例) 悪意のあるファイルがシステム内で拡散する前に、そのファイルを隔離して安全な状態を保つ

隔離機能は、**被害の拡大を防ぎ、組織のセキュリティを保護するために重要な役割**を果たします。

FUNCTION

機能

③調査・復旧

「調査・復旧」機能は、**インシデント発生後の対応を迅速に行う**ための機能です。
具体的な動作として、以下があげられます。



✓ インシデントの調査

EDRはエンドポイント上のログや活動データを収集し、攻撃の詳細を調査します。

例) 感染したファイルや攻撃の発端・進行状況、影響範囲の特定



✓ 復旧作業の支援

インシデントが解決された後には、システムを元の状態に戻すためのツールや手順を提供します。

例) マルウェアの除去後の、影響を受けた設定やファイルの復旧支援
(感染したファイルの削除や修復、設定のリセット)



✓ 再発防止のための分析

調査の結果に基づき、再発防止のための改善策を提案します。これには、新たなセキュリティポリシーの策定や、脅威に対する対策の強化が含まれます。

例) 攻撃のパターンを分析し、同様の攻撃に対する防御策を強化するためのインサイトを提供する

調査・復旧機能により、**インシデント対応の迅速化・効果化につながるほか、同様の問題の再発防止にも寄与**します。

FUNCTION

機能

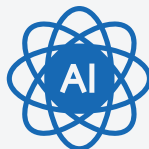
【注目】 自動修復機能

最新のEDRの機能で注目されているのが自動修復機能です。これは、サイバー攻撃によるシステム侵害やデータの損傷を自動的に修復できる素晴らしい機能です。



✓ 迅速な修復とロールバック

自動修復機能ではインシデントを検知した際、書き換えられたレジストリや改ざんされたファイルを、ストーリーラインなどの特許技術に沿って、変更されたファイルのみVSSを元に自動で修復。さらに、改ざんされたファイルを修復すべきか人が判断する必要がないので、詳しい方がいなくても運用することができます。



✓ AIによる自動化対応

AIを活用して攻撃をリアルタイムで検知・分析し、感染したファイルやプロセスを自動的に修復します。これにより、脅威に対する対応スピードが飛躍的に向上し、平均修復時間（MTTR）の短縮を実現します



✓ 多層防御と自動復元

AI、ふるまい検知、シグネチャ検知など、複数のアプローチによりエンドポイントを保護し、万一に攻撃が成功してしまった場合でも、システムのシャドーコピーを使用して即座に復元する機能が備わっています。

これらの最新機能によって被害の拡大を防ぎ、システムのダウンタイムを最小限に抑えることが可能となります。

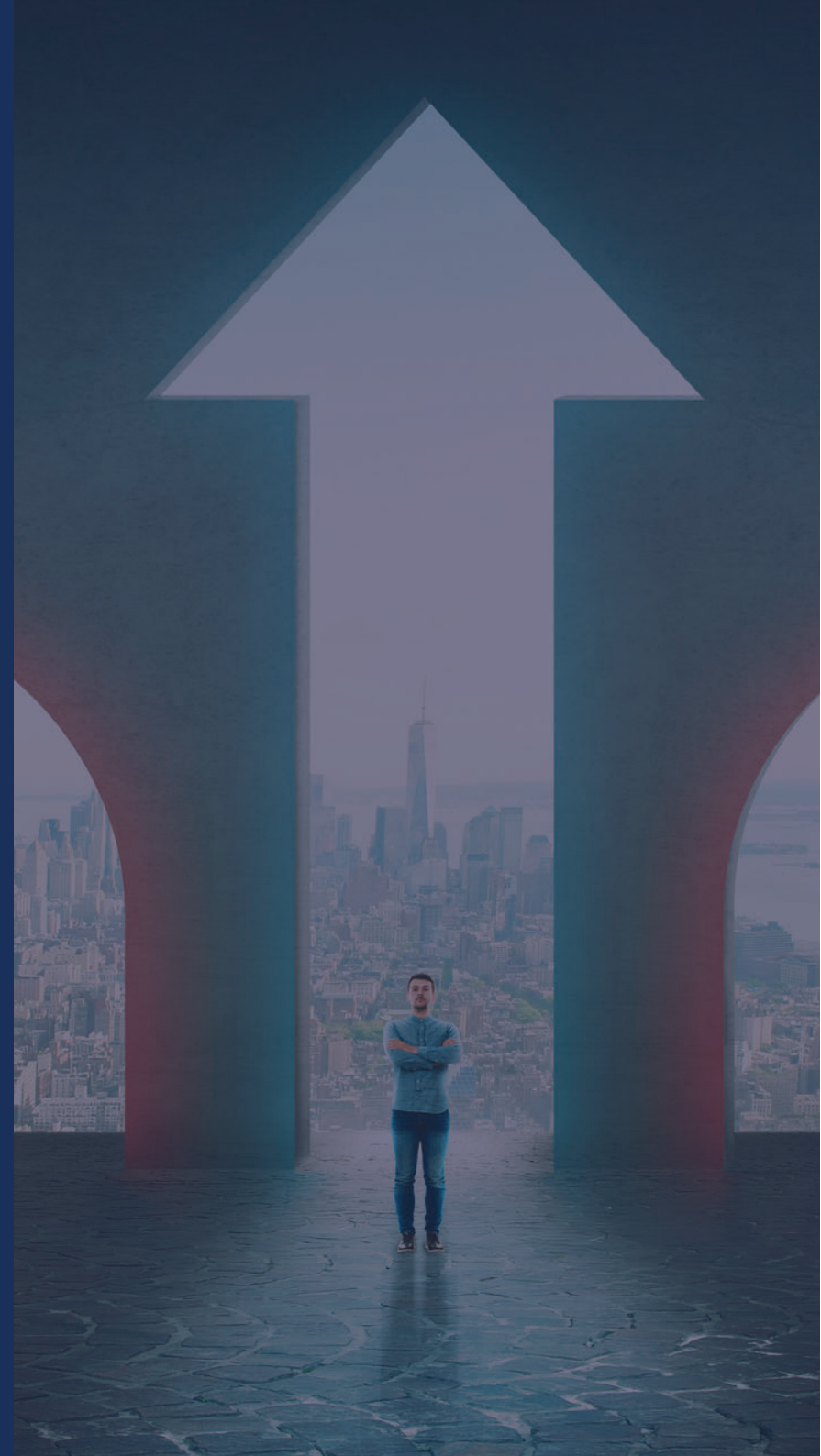
※ MTTR（Mean Time To Repair / Recovery）＝ 平均修理時間

※ VSS（ボリュームシャドーコピー）

SELECTION POINT

選び方のポイント

EDR製品を選定する際は、次で紹介する3つのポイントに注目することで、自組織のセキュリティニーズに最適な製品を選ぶことができます。



SELECTION POINT

選び方のポイント

①検知・分析の正確性

EDR製品の検知・分析機能の正確性は、その製品が**脅威を正確に把握し、適切な対応ができるかどうか**を決定づける要素です。具体的には、以下の点に注目すると良いでしょう。



✓ 脅威の検知能力

EDRがどの程度の精度で脅威を検知できるかが重要です。例えば、従来のウイルス対策ソフトウェアでは検知できなかった新たなマルウェアや高度な持続的脅威（APT）に対応できるかどうかを確認しましょう。



✓ 誤検知の少なさ

EDRが正確に脅威を識別し、誤検知を最小限に抑えられるかどうかも重要なポイントです。過剰なアラートが発生すると、セキュリティチームの効率が低下するため、製品の評価にあたっては誤検知率の低さも確認することをおすすめします。

SELECTION POINT

選び方のポイント

②調査・復旧のサポート機能

調査・復旧のサポート機能は、**インシデント発生後の対応を迅速かつ効果的に行う**ために必要な機能です。EDR製品を選定する際には、以下の点を確認しましょう。



✓ 調査ツールの詳細度

EDRが提供する調査ツールの性能を確認します。例えば、攻撃の経路を追跡するための詳細なタイムライン機能や、感染したファイルやプロセスの詳細なログを提供しているEDR製品の場合、セキュリティチームは迅速にインシデントの根本原因を特定し、適切な対応策を講じることができます。



✓ 復旧機能の充実度

インシデント後にシステムを元の状態に戻すための機能も重要です。自動で感染ファイルを隔離し、その後の復旧プロセスを支援する機能を持っているEDR製品であるかどうかを確認すると良いでしょう。

SELECTION POINT

選び方のポイント

③機能の拡張性

EDR製品の機能の拡張性を確認することで、**将来的なニーズに対応できるかどうかを判断**できます。以下のポイントに注目しましょう。

✓ 追加機能のサポート



EDR製品が提供する基本機能に加えて、必要に応じて追加機能を導入できるかどうかを確認することが重要です。例えば、脅威インテリジェンスやエンドポイントの脆弱性管理といった追加機能をオプションで提供し、セキュリティニーズの変化に柔軟に対応できる製品は、拡張性が高い製品であると評価できます。

✓ 統合の容易さ



他のセキュリティツールやシステムとの統合が、どの程度容易かも選定ポイントとなります。SIEMシステムや他のセキュリティ製品と統合できるかどうかを確認することがポイントです。

これらのポイントを考慮しながら、**自社や自組織のセキュリティニーズに最適なEDR製品を選定**することで、セキュリティ対策の強化と効率的な運用を実現できます。

※ SIEM（Security Information and Event Management）

今、世界で注目されているEDRとは？

導入企業 8,000 社 を超える 注目のEDRの資料を取り寄せませんか？

- 世界で8,000社超の導入実績
- 日本国内1,000社超の導入実績
- ガートナーで「Leader」に選出
- EDR検知性テスト「3年連続トップクラス」
- EDR製品で唯一「自動修復機能」を搭載
- 分析能力が最も優れているEDRと最高評価

 SentinelOne™ ご紹介資料

資料を無料でご提供中

株式会社 電算システム
クラウドインテグレーション事業部
プラットフォームソリューション部

2つの入手方法からお選びいただけます

資料を無料でご提供中

1 PDFでご覧の方
(クリックでフォームへ)

CLICK HERE

2 QRコードでアクセス



《 35ページの詳しい解説資料 》

※資料の内容・ボリュームは変更となる場合がございます

CONTACT

お問い合わせ

EDRをはじめセキュリティに関する
ご質問・ご相談がございましたら、
お気軽にお問い合わせください。



株式会社電算システム

岐阜本社

〒501-6196 岐阜県岐阜市日置江1丁目58番地
TEL: 058-279-3481

東京本社

〒104-0032 東京都中央区八丁堀2丁目20番8号
八丁堀綜通ビル
TEL: 03-3206-1780

名古屋支社

〒460-0003 名古屋市中区錦3丁目1番1号
十六銀行名古屋ビル12階
TEL: 052-961-3690



idc-neta@densan-s.co.jp



www.dsk-idc.jp