EPP/EDRを再定義するSentinelOne

オンプレ環境からAI活用時代まで守る新しい選択肢

東京エレクトロン デバイス株式会社
CN技術本部
カスタマーサクセスデザイン部
小方　滋雪

本セッションの流れ

01 近年の脅威の動向

02 SentinelOneの自律型EDR

03 閉域網環境でも実現する自律型EDR運用

04 東京エレクトロンデバイスによる支援体制

05 まとめ/引き継ぎ

© Tokyo Electron Device LTD. All Rights Reserved.

近年の脅威動向

© Tokyo Electron Device LTD. All Rights Reserved.

IPA2026から見る最新の脅威傾向

IPA 2026｜組織向け脅威ランキング（上位5位）

順位	組織向け脅威	前年順位
1位	ランサム攻撃による被害	前年1位
2位	サプライチェーンや委託先を狙った攻撃	前年2位
3位	AI の利用をめぐるサイバーリスク	NEW
4位	システムの脆弱性を悪用した攻撃	前年3位
5位	機密情報を狙った標的型攻撃	前年5位

出典：IPA「情報セキュリティ10大脅威 2026」組織編（2026年1月29日）
https://www.ipa.go.jp/security/10threats/10threats2026.html

攻撃者もAIを使う時代

AI 利用をめぐるリスクが上位に初選出

IPA 2026では、組織向け脅威の3位に「AIの利用をめぐるサイバーリスク」が初選出。攻撃・防御の両面でAI活用を前提にした見直しが必要。

最初に狙われ、侵入後の展開を許してしまう接点がエンドポイント

© Tokyo Electron Device LTD. All Rights Reserved.

AIで変わったのは「攻撃手法」ではなく「攻撃工程の自律化」

英国政府のAI安全研究機関AISIによる、Claude Mythos Previewの企業ネットワーク攻撃シミュレーション（TLO）評価より。

従来

攻撃者（人）が判断しながら、1つずつ段階的に進める

偵察 → 人が判断 → 脆弱性探索 → 人が判断 → 悪用 → 人が判断 → 横展開 → 人が判断 → ネットワーク掌握

AI時代

目標の指示

初期アクセス

AIが調査・判断しながら連続実行

偵察 → 脆弱性探索 → 悪用 → 横展開 → ネットワーク掌握

AISIによるAIサイバー能力評価

AIに目的と初期アクセスを与え、
企業ネットワーク攻撃をどこまで自律的に進められるかを評価

TLO 32段階
企業ネットワークへの攻撃シナリオ

3/10回
最後の段階まで攻撃を完遂

平均 22/32段階
途中で止まった試行も含め、平均で約7割まで到達

⚠ 攻撃者が工程ごとに判断していた攻撃が、AIによって**複数工程にまたがって自律的・連続的に進むように**

脆弱性を修正する	アクセスを適切に制御	エンドポイントを保護

AI時代だからこそ、基本対策を確実に

© Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス

脆弱性対策だけでは防ぎきれない ― 侵入後を止める備えが必要

DBIR 2026が示す、EPP / EDRが必要な理由

① 侵入される

31%

脆弱性悪用が
初期アクセス経路

脆弱性悪用は、侵害の主要な入口

パッチは重要

② 修正が間に合わない

26%

CISA KEV掲載脆弱性の
完全修正率

43日

完全修正までの
中央値

重要な脆弱性でも、修正には時間がかかる

修正待ちの間にも
攻撃は起こり得る

③ 被害が拡大する

48%

侵害にランサムウェアが関与

侵入後の横展開・暗号化を止める備えが必要

「侵入を防ぐ」だけでなく、「侵入されても早く見つけて止める」対策が必要

パッチ適用は必須。ただし、すべてを即日修正できる前提ではなく、攻撃を前提に検知・封じ込めるレイヤーが必要。

脆弱性対策・アクセス制御 ＋ EPP / EDRによる検知・封じ込め

© Tokyo Electron Device LTD. All Rights Reserved.

AI時代の自律型エンドポイント防御

ポイントは「検知」だけではなく、
調査・判断・対処までの時間を短くすること



SentinelOneなら、AIによる検知・判断・対処の自動化で、攻撃の高速化に対抗可能

高い防御・検知力

第三者評価で示される
高い防御・検知力

いつでもゼロタイムで保護

AI

自律型AIにより
オフラインでも
即時検知で保護

脅威排除の自動化

AI

検出・駆除・復旧などの
初動対応を自動化

© Tokyo Electron Device LTD. All Rights Reserved.

SentinelOneの自律型EDR

© Tokyo Electron Device LTD. All Rights Reserved.

SentinelOneの会社概要



設 立	2013年1月
C E O	Tomer Weingarten
従 業 員	2,900人超(2026年1月31日時点)
本 社	米国カリフォルニア州マウンテン・ビュー
開発拠点	イスラエル、インド、チェコ共和国を中心にグローバル展開
製 品	Singularity Platform
顧 客	Fortune 500の約5分の1、Global 2000の数百社を保護
上 場	2021年6月30日ニューヨーク証券取引所

- サイバーセキュリティに加え、AIの強みが評価
- サイバーセキュリティ関連企業としては過去最大額でのIPO

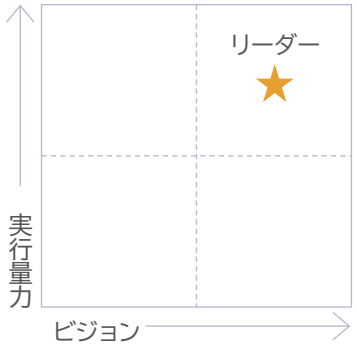
Copyright © Tokyo Electron Device LTD. All Rights Reserved.

SentinelOneの第三者評価

某リサーチ会社　市場調査レポート

6年連続
Leader（2026年）

- 2021-2026年版エンドポイント保護プラットフォーム分野マジッククアドラントの**リーダー**
- クリティカルケイパビリティの**すべての顧客タイプで最高スコア**



某リサーチ会社 カスタマーレポート（実利用者評価）

4.9 / 5
総合レーティング

- EDRで**最高スコア獲得**
- エンドポイント保護プラットフォームとエンドポイント検知と対応ソリューションで**4.9/5**のレーティング
- **96%** のお客様がSentinelOneを推奨



MITRE ATT&CK

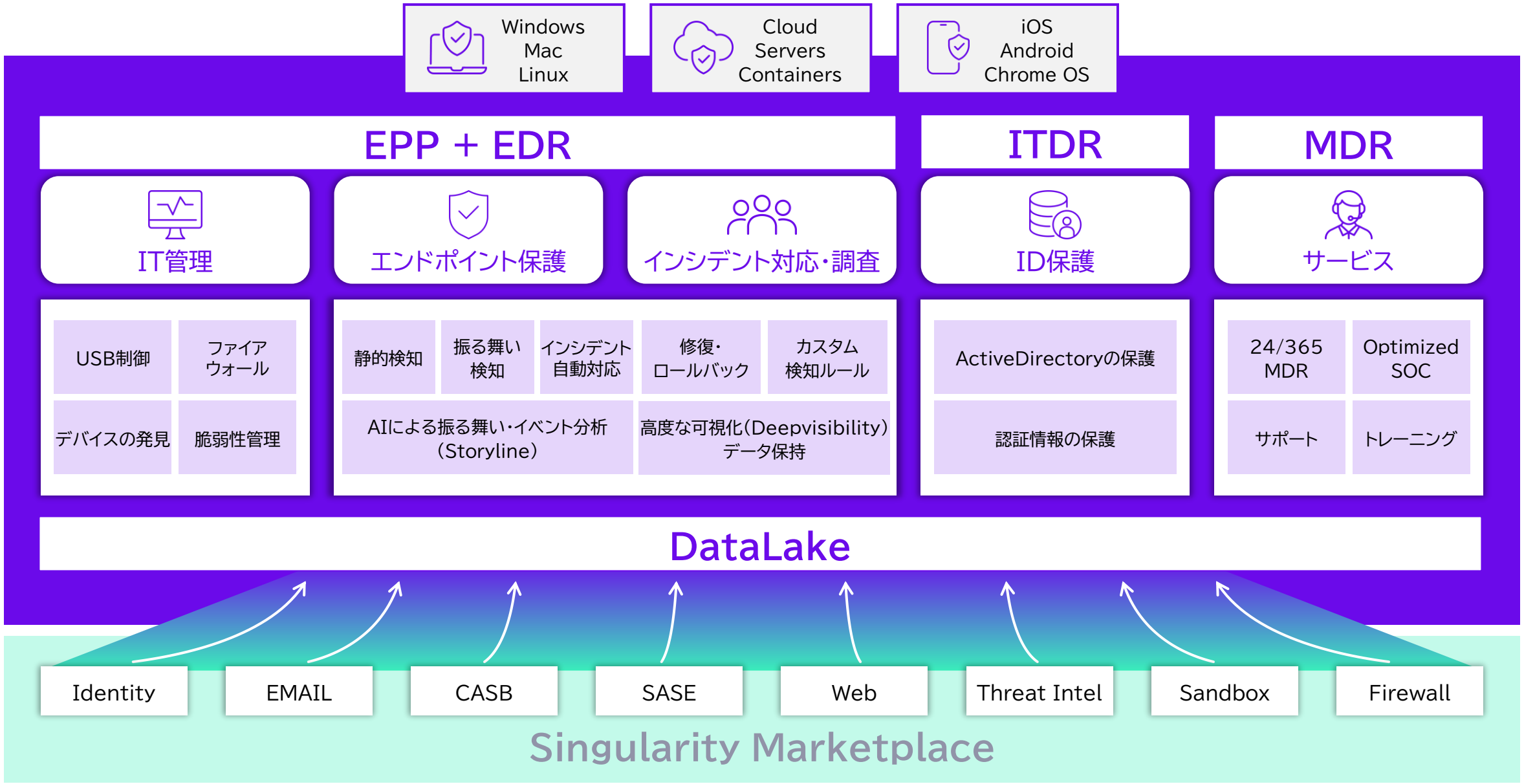
100%
検知率（2024年）

- 記録的なATT＆CK評価結果
- アナリティック検知**最多2年間連続**
- 検知漏れ**ゼロ**
- 100%を可視性
- 遅延**ゼロ**、設定変更**ゼロ**

様々な機関が高く評価

© Tokyo Electron Device LTD. All Rights Reserved.

Singularity Platform の全体イメージ



© Tokyo Electron Device LTD. All Rights Reserved.

SentinelOne概要

- 必要に応じて入力
- 必要に応じて入力
- 必要に応じて入力

© Tokyo Electron Device LTD. All Rights Reserved.

SentinelOneの特徴

- パターンマッチングもNGAV・EPPもEDRもワンエージェントで提供
- 既知・未知のファイルベースのマルウェアに対応

- 対象のプロセス・ファイルは自動停止/自動隔離
- 対象の端末をネットワークから自動隔離も可能

- ひとまずの脅威が取り除かれた状態で調査可能
- 多様な調査ツール



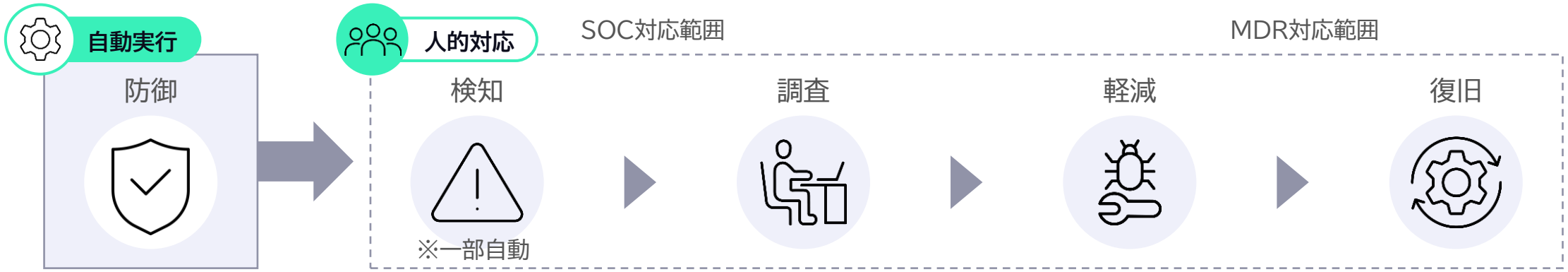
- ファイルレスなど、様々なマルウェアの振る舞いを検知
- エンドポイントのAIが検知
- オンラインはもちろんオフラインでも即時検知
- リアルタイムにコンテキスト化

- マルウェアでの汚染箇所を自動で完全復旧
- ランサムウェアに暗号化されたファイルを自動でロールバック

© Tokyo Electron Device LTD. All Rights Reserved.

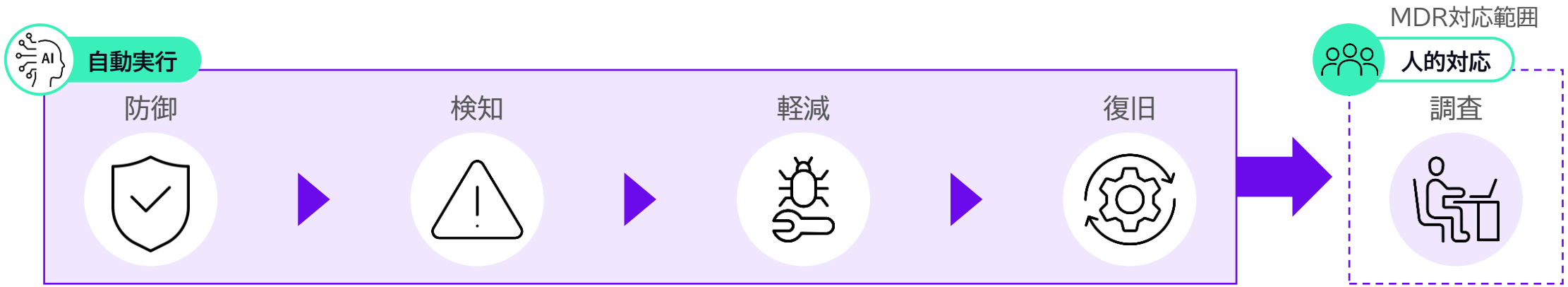
SentinelOneと他EDR製品との違い

他社EDR製品



未知のマルウェア対策は、人的対応による対処の遅れと対応漏れにより被害が拡大

SentinelOne



自動的にインシデントへ対応し、人手に頼らない自律型防御をAIで実現

© Tokyo Electron Device LTD. All Rights Reserved.

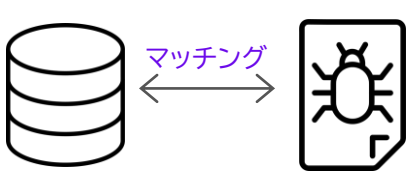
防御・検知

SentinelOneは、複数の検知エンジンで防御・検知にも強い

実行前のマルウェア対策

パターンマッチング

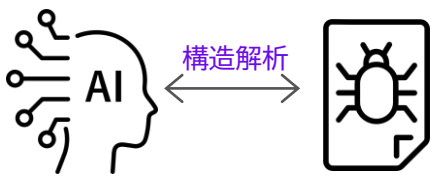
レピュテーションエンジン



既知のマルウェアに対する
シグネチャ方式の
パターンマッチング

NGAV・EPP

Static AIエンジン

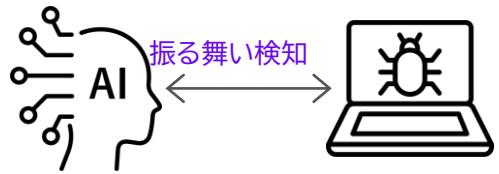


未知のマルウェアに対する
ファイルの構造解析

実行中のマルウェア対策

Active EDR

Behavioral AI エンジン



ユーザーレベル・カーネルレベルの
振る舞いをエンドポイントのIが
検知して防御するEDR

© Tokyo Electron Device LTD. All Rights Reserved.

防御・検知

実行前のマルウェア対策

ファイルベースのマルウェアに対する静的解析

既知・未知のファイルベースの
マルウェアに対する複数の検知エンジン

既知のマルウェア

レピュテーションエンジン

既知のマルウェアに対する、
シグネチャ方式のパターンマッチング

未知のマルウェア

Static AIエンジン

未知のマルウェアに対する、
ファイルの構造解析

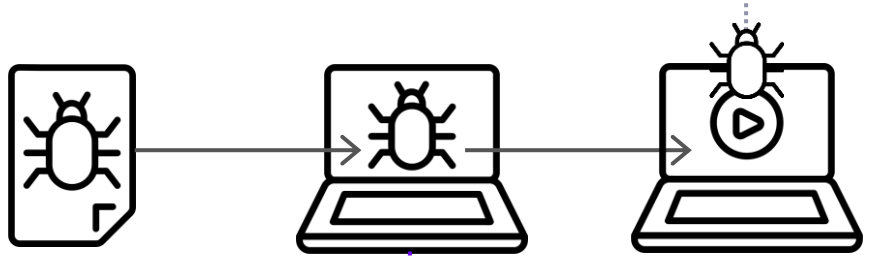
AI

ハードディスクへの書き込みタイミングで即時スキャン

あるタイミングでスキャンすると、マルウェアは
動いていないが存在している、という状況がありうる

通常の検知エンジン

ファイルが実行されたタイミングでスキャン



SentinelOneの検知エンジン

ハードディスクに書き込まれたタイミングで即時スキャン開始

© Tokyo Electron Device LTD. All Rights Reserved.

防御・検知　実行中のマルウェア対策

振る舞い検知エンジン ユーザーレベル・カーネルレベル

- 振る舞いをエンドポイントのAIが検知して防御するEDR
- ユーザーレベルのみならずカーネルレベルでの振る舞いも検知

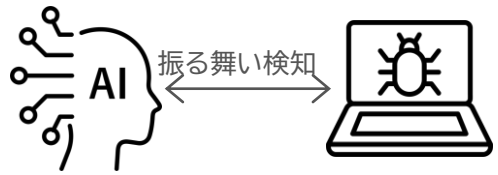
高い防御力

- Storyline機能でプロセス毎の振る舞いを詳細かつ体系的にトレース
- エモテットのようなマクロや、パワーシェルを使用したファイルレス攻撃も効果的に検知

いつでもリアルタイムで保護

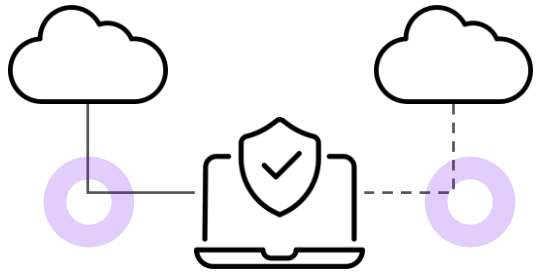
- エンドポイントにEDRのAI検知エンジンを搭載
- オンライン・オフラインでも同等の検知・対処を実現

Behavioral AI エンジン



Active EDR　ユーザーレベル・カーネルレベル





オンライン対応　オフライン対応

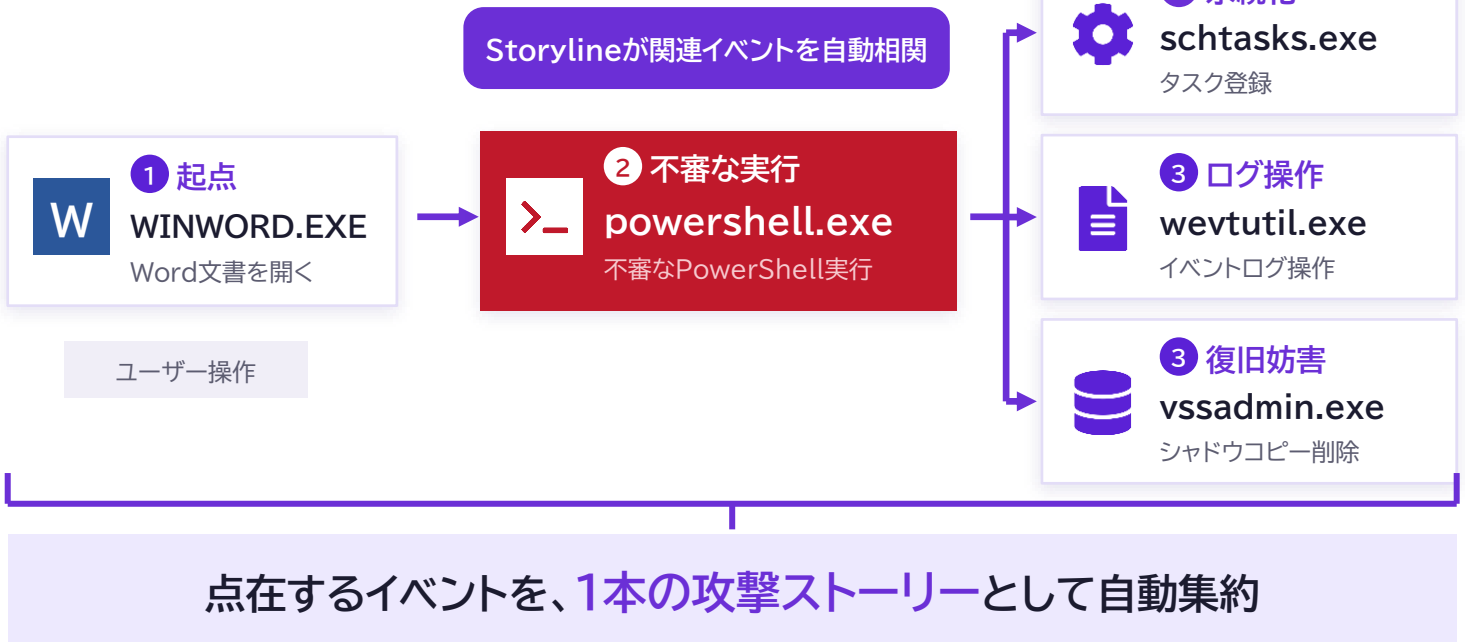
© Tokyo Electron Device LTD. All Rights Reserved.

Storyline　点在するイベントを、1本の攻撃ストーリーへ

個々のイベントを自動で関連付け、攻撃の全体像をリアルタイムに可視化。検知・防御・修復までを一気通貫で支援します。

攻撃の全体像をつなぐ　Storyline

関連するプロセスやイベントを自動相関し
1本の攻撃ストーリーとして可視化



01 アラート集約

関連する検知を1つにまとめ、
個別アラートを追う負荷を軽減

02 即時の自動対応

オンライン・オフラインを問わず、検知した脅威に対し、
停止・隔離などのレスポンスを即時に実行

03 インシデントに合わせた復旧

影響範囲を把握し、Remediate / Rollback
などの復旧対応につなげる

04 調査の効率化

一連の攻撃をStorylineで可視化し、
原因や影響範囲を素早く把握

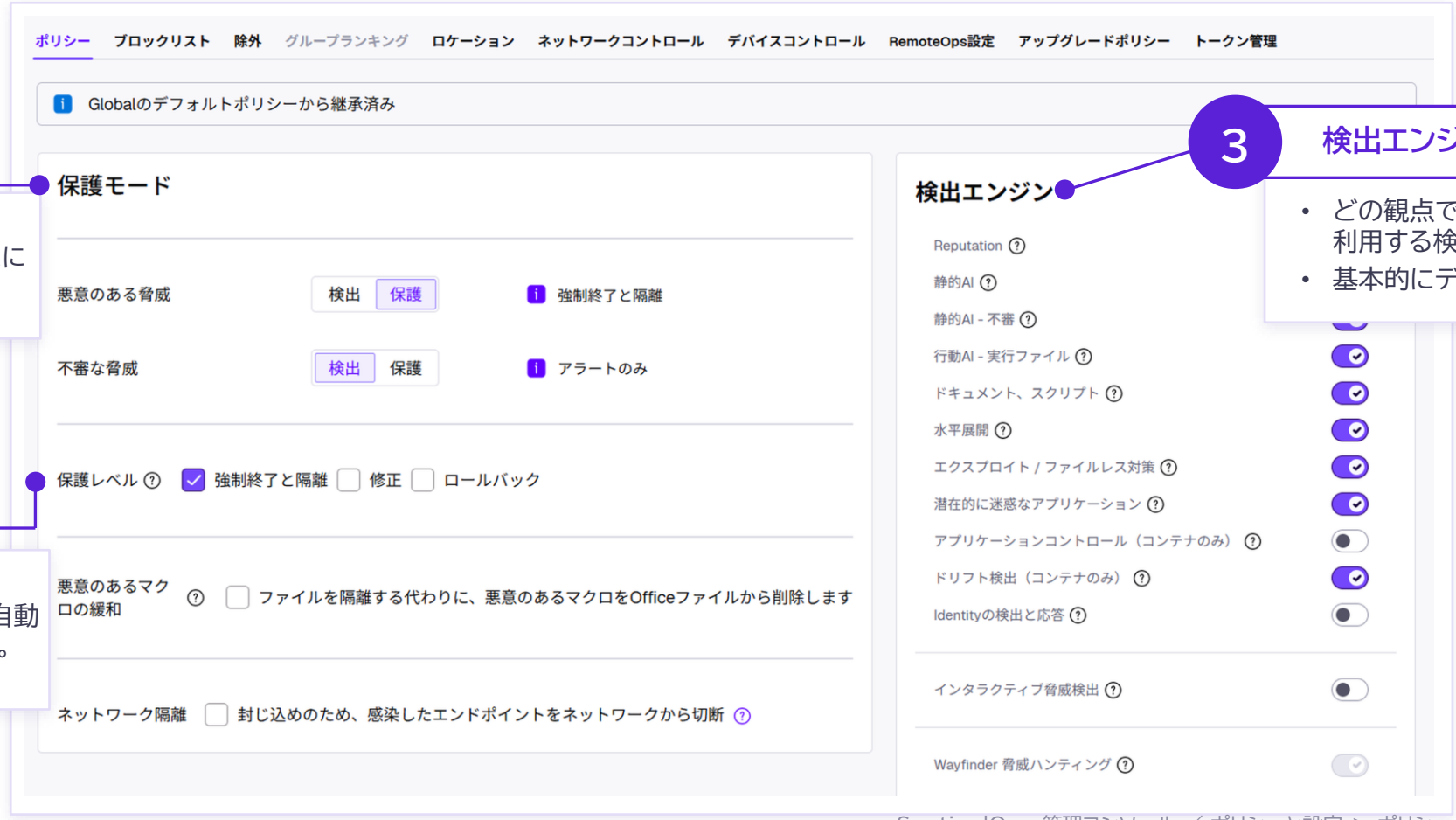
Storylineで攻撃を「見える化」し、「止める」「戻す」までつなげる

© Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス

シンプルな設定画面

高度な検知・分析はAIで自動化されるため、管理者はシンプルなポリシー設定で運用できます。



SentinelOne 管理コンソール ／ ポリシーと設定 > ポリシー

1 保護モード

「悪意のある脅威」「不審な脅威」ごとに検出のみ／保護を選択

2 保護レベル

「保護モード」適用の際、どこまで自動対処するか、検知後の対応を選択。

3 検出エンジン

- どの観点で脅威を検知するか、利用する検出ロジックを設定
- 基本的にデフォルト設定での運用

複雑なルールを細かく作り込むのではなく、必要な保護方針をシンプルに設計

© Tokyo Electron Device LTD. All Rights Reserved.

軽減・復旧

SentinelOneは防御・検知だけでなく、自動的にダメージを軽減し、復旧も自動

一般的な場合

他のEDRベンダーなら

1分で検知
＋10分で調査
＋60分で復旧

人的対応

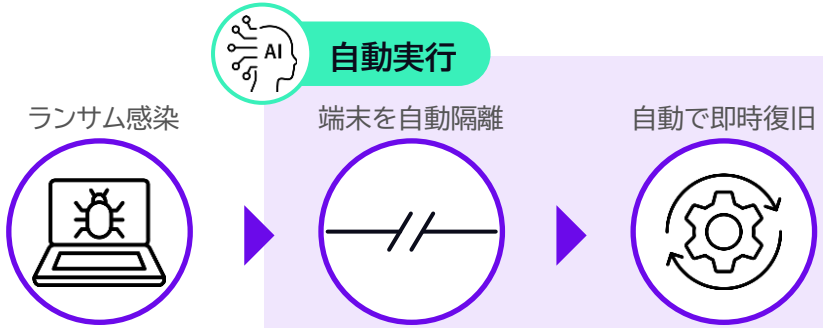


SentinelOne

自動対応・自律型なので

0分で検知
＋**0分**で調査
＋**0分**で復旧

自動実行



- 特別な知識やスキル不要
- インシデント対応が即時完了

人的対応が不要で、自動で即時復旧！

© Tokyo Electron Device LTD. All Rights Reserved.

軽減　実行中のマルウェア対策

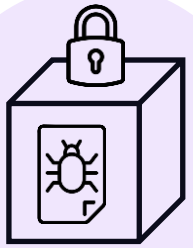
自動的に対応することで、自律的にダメージを軽減

プロセスの停止



怪しい挙動を示した
プロセスを
自動的に強制停止

ファイル隔離



被疑ファイルを
特定ディレクトリへ
自動的に強制隔離し暗号化

ネットワーク隔離

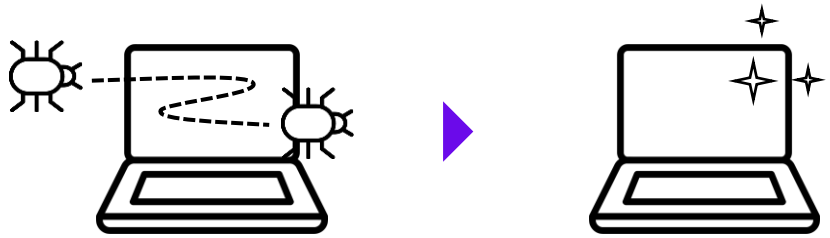


端末を、自動的に
ネットワーク隔離

© Tokyo Electron Device LTD. All Rights Reserved.

復旧 マルウェア実行後

マルウェアでの汚染箇所を自動で完全復旧

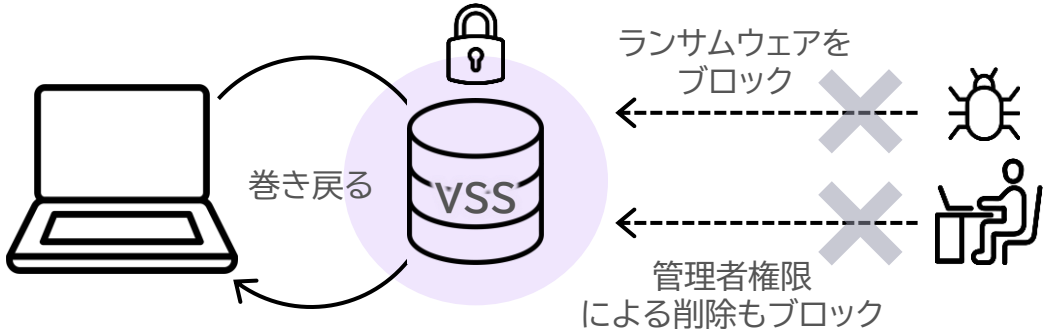


Remediate

- 攻撃途中の侵入段階で汚染された箇所を、自動で完全に復旧
- マルウェア実行により書き込まれた一時ファイルやスケジュールタスク、レジストリ設定などを自動で完全復旧

Windows対応　　macOS対応

ランサムウェアによる暗号化ファイルを自動でロールバック



Rollback

- 4時間ごとにVSSのスナップショットを作成
- ランサムウェアによるVSSの破壊を未然に防止
- 管理者権限での削除に対してもプロテクト

Windows対応

© Tokyo Electron Device LTD. All Rights Reserved.

EDR無効化(回避)対策 — 手法とSentinelOneの標準対策

攻撃者はEDRそのものを止めにきます。SentinelOneは主要な無効化手口に対し、標準で有効な防御を備えています。

BYOVD
Bring Your Own Vulnerable Driver

攻撃

脆弱性のある正規(署名付き)ドライバを持ち込み、OSのカーネル領域へ不正アクセス。EDR自体を停止させる。

SentinelOneの対策

「不審なドライバのブロック」機能(標準でON)により、署名の有無に関わらず検知・ブロック。

BYOI
Bring Your Own Installer

攻撃

正規インストーラーを悪用してローカルで更新を実行。更新中の一時停止を狙いプロセスを強制終了し保護を無効化。

SentinelOneの対策

原則ローカル更新を許容しない。ローカルアップグレード認証で管理コンソール承認制に(必要時のみ一時許可)。

不正停止・改変・アンインストール
Tampering / Uninstall

攻撃

管理者権限でのアンインストールや、エージェントの不正な停止・改変を狙い、保護を無効化。

SentinelOneの対策

アンチタンパー(改ざん防止)で保護。削除・停止には承認またはパスフレーズが必須。標準ON。

いずれも標準機能で対応可能。 BYOI対策のローカルアップグレード認証は既存環境では既定オフのため、運用に合わせた有効化を推奨します。

© Tokyo Electron Device LTD. All Rights Reserved.

ライセンス別機能

workstation
server

攻撃ステージ	機能	Core	Control	Complete
実行前対応	レピュテーションエンジン	✓	✓	✓
	Static AI エンジン	✓	✓	✓
実行中対応	Behavioral AI エンジン	✓	✓	✓
	ドキュメント、スクリプト攻撃	✓	✓	✓
	ファイルレス、脆弱性攻撃	✓	✓	✓
	ラテラルムーブメント	✓	✓	✓
	ネットワーク隔離	✓	✓	✓
実行後対応	修復・ロールバック	✓	✓	✓
	攻撃時のストーリーライン	✓	✓	✓
	リモートシェル		✓	✓
and More	ファイアウォール制御		✓	✓
	デバイス制御		✓	✓
	アプリケーション管理(脆弱性診断)		✓	✓
	常時ログ収集			✓
	SIEM(14日間、10 GB/日)			✓
	Purple AI(調査支援機能)			✓

Core

- 基本的なEPP/EDR機能
  (防御、検知、軽減、復旧)

Control

- リモートシェル
- デバイス制御
- ファイアウォール管理
- アプリケーション管理(脆弱性診断)

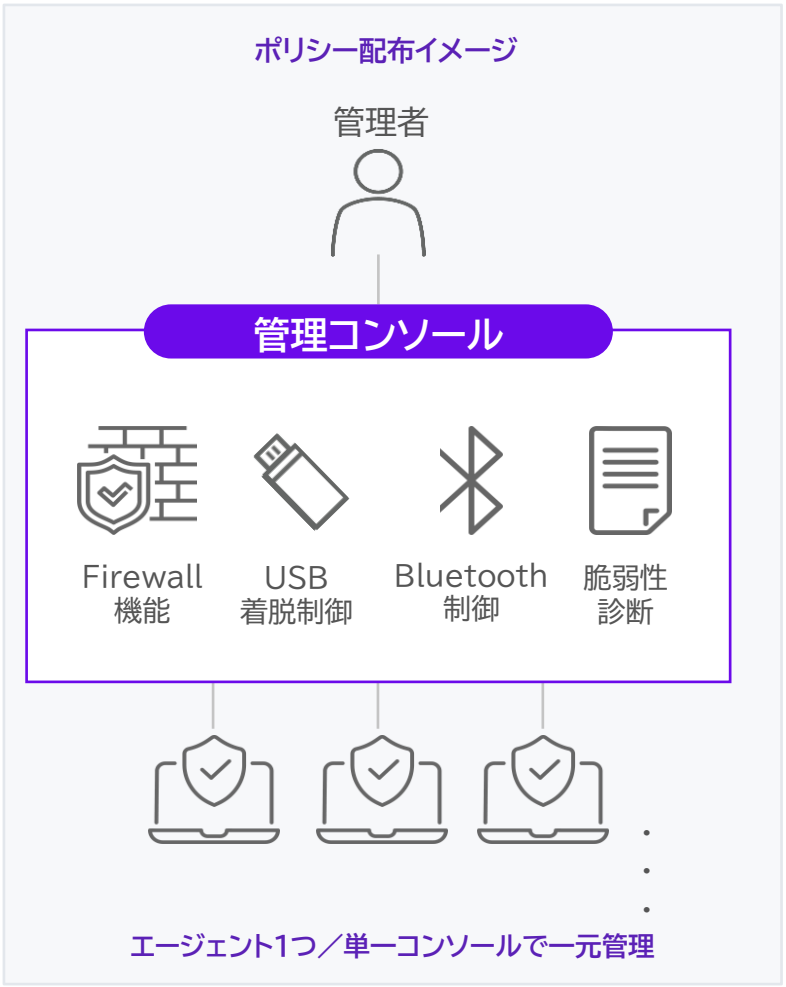
Complete

- 常時ログ収集
- SIEM(14日間、10 GB/日)
- カスタムアラート
- Purple AI(調査支援機能)

© Tokyo Electron Device LTD. All Rights Reserved.

Control アドオン機能

管理コンソールからポリシーを配布し、端末・通信・資産の一括制御が可能です。



Remote Shell

現場に行かず、その場で調査・修復

- 管理コンソールからPowerShell/Bashを直接実行
- EDR検知の直後にそのまま調査まで一気通貫

デバイス制御機能

USB等の周辺機器をきめ細かく統制

- 部署/ユーザー単位で許可・禁止を一元管理
- USB・Bluetooth・Thunderboltまで対象
- 利用状況をアクティビティログで確認可能

Firewall機能

端末単位の通信制御を一元化

- IP／ポート／プロトコルによる通信制御
- FQDN／URLベースの通信制御
- Location Awarenessによる Firewallポリシーの自動切り替えに対応

アプリケーション管理

アプリと脆弱性を可視化

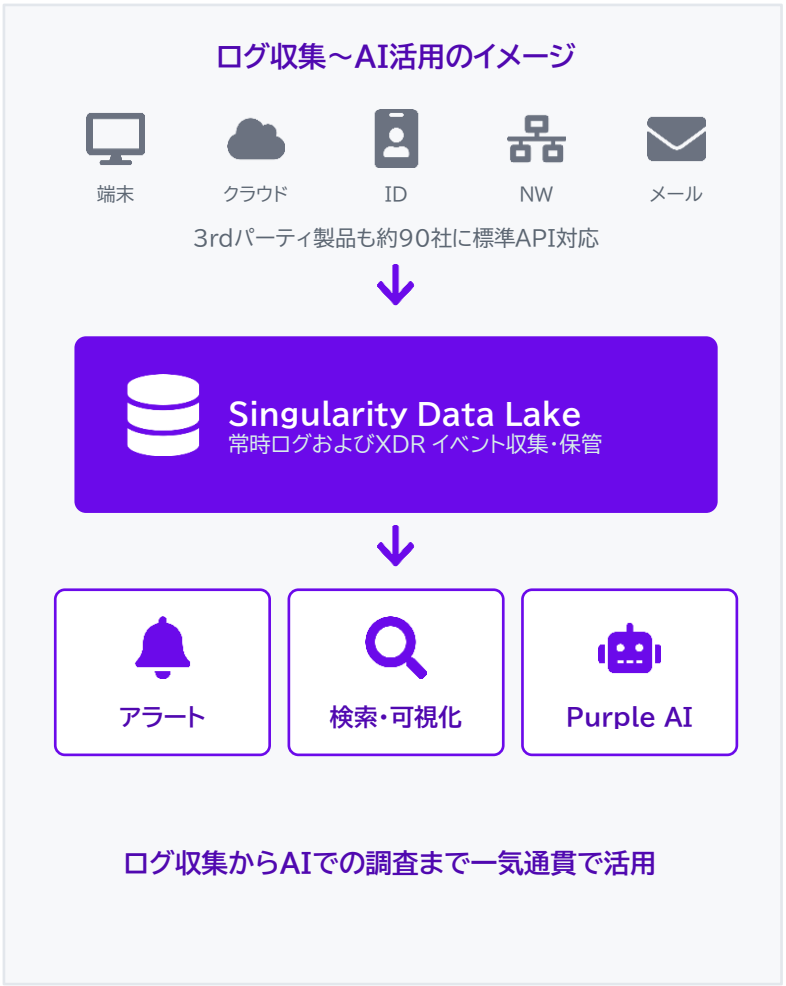
- アプリケーションの棚卸しとMITREのCVE情報を照合
- 優先度付けで効率的なパッチ運用を支援

© Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス

Complete アドオン機能

ログを常時収集・蓄積・AIで活用。EDRを“検知と復旧”から、事後調査・SIEM運用まで拡張します。



常時ログ収集

端末の全アクティビティを常時記録

- エンドポイントの全アクティビティを可視化・検索可能
- EDR検知後の「なぜ・どこまで・何が起きたか」を即座に把握可能
- 標準14日間保存（拡張可能）

SIEM

各種ログを取り込み、横断検索

- インデックスを生成しない高速なSIEM
- 3rdパーティー製品ログの取り込み（標準14日／10GB per day）
- インシデント発生時は、ログを横断的に調査

カスタムアラート

自社環境に即した検知ルールを追加

- EDR/XDRのログをもとに、自社環境にフィットした検知ルールを追加
- 標準テンプレートをベースに、しきい値や条件だけを調整して利用可能

Purple AI

クエリなしで高度な調査

- 自然言語での質問をクエリに自動変換し検索・要約
- インシデントのアラート内容を日本語で自動要約

→ Complete機能詳細はp〇以降

© Tokyo Electron Device LTD. All Rights Reserved.

SentinelOne サポートOS

Windows
- Windows 8.1, 10, 11, 11 23H2, 11 24H2, 11 25H2,365
- Windows Server 2012 R2, 2016, 2019, 2022, 2025
- Windows Storage Server 2012 R2, 2016, 2022
- Windows Server Core 2016, 2019, 2022, 2025
- Windows Server IoT 2019/2022/2025(いずれも64-bit対応)

Editions
Home, Pro, Pro for Workstations, Enterprise, Education, Pro Education, Enterprise LTSC, Embedded, Windows 10 IoT Enterprise

Windows Legacy Plus OS
- Windows 7 SP1 (32/64-bit), POSReady 7
- Windows 8 (32/64-bit), Windows 8.1 (32-bit), Windows 10 (32-bit)
- Windows Server 2012 (not R2) (32/64-bit)
- Windows Storage Server / Server Core 2012 (not R2) (32/64-bit)
- Windows Server 2008 R2 SP1 (32/64-bit)

Windows Legacy OS
- Windows XP SP2 (64-bit), XP SP3 (32/64-bit)
- Windows Vista SP2 (32/64-bit)
- Windows Server 2003 SP2, R2 SP2 (32/64-bit)
- Windows Server 2008 SP2 (not R2) (32/64-bit)
- Windows Embedded POSReady 2009

macOS
- 13.0-13.7.8(Ventura), 14.0-14.8.5(Sonoma), 15.0–15.6, 15.6.1, 15.7.1, 15.7.2, 15.7.5–15.7.8(Sequoia)
- 26.0-26.5.1(Tahoe)

Linux (64-bit)
- CentOS:6.4–6.10, 7.0–7.9, 8.0–8.5 / CentOS Stream:9
- RHEL:6.4–6.10, 7.0–7.9, 8.0–8.10, 9.0–9.8, 10.0–10.2
- Ubuntu:14.04, 16.04, 18.04, 20.04.6, 22.04, 22.04.5, 24.04.1–24.04.4
- Oracle Linux:6.9–6.10, 7.0–7.9, 8.0–8.10, 9.1-3,9.5-7, 10.0–10.1
- Amazon Linux:Amazon Linux 2, AMI 2017–2018, Amazon Linux 2023, 2023.1, 2023.3, 2023.5-10,2023.12
- SUSE Linux Enterprise Server:11 SP4, 12.0–12.5, 15.0–15.7
- Fedora:35, 36, 37, 38, 39, 40, 41, 42
- Debian:8, 9, 10.0–10.13, 11.0–11.11, 12.0–12.14, 13.0–13.5
- AlmaLinux:8.4–8.8, 8.10, 9.0–9.8, 10.0–10.2
- Rocky Linux:8.4–8.8, 8.10, 9.0–9.7, 10.0–10.1
- Scientific Linux:6, 7
- Virtuozzo:7
- CloudLinux Shared:v6, v8(※Container 非対応)
- Miracle Linux:8, 9

Virtual Environments
- Citrix XenApp / XenDesktop
- Microsoft Hyper-V
- Oracle VirtualBox
- VMware vSphere / Workstation / Fusion / Horizon

※2026年7月7日時点

© Tokyo Electron Device LTD. All Rights Reserved.

閉域網環境でも実現する
自律型EDR運用

© Tokyo Electron Device LTD. All Rights Reserved.

工場・OT環境が抱えるセキュリティ課題

「外部とつながらない」だけでは防ぎ切れず、侵入後の検知・封じ込めにも制約が残る

現場に残る4つの制約

1 閉域網でも侵入経路が残る

USBメモリ、保守PC、更新媒体など、物理的な接点からの侵入を完全には防げない

2 レガシーOSが残存

設備依存により、OS更新やパッチ適用を容易に進められない

3 OS内部の脅威が見えにくい

設備やネットワークは監視していても、不審なプロセスやマルウェアの振る舞いまでは把握できない

4 生産設備を止められない

24時間稼働などにより、調査・隔離・再起動に使える時間が限られる

制約が重なることで生じるリスク

侵入に気づくまで時間がかかり、初動が遅れやすい

- 端末内部で進行する不審な挙動を捉えにくい
- 侵入後の横展開・感染拡大を止めるまでに時間がかかる
- 対応が遅れるほど、生産停止や復旧長期化のリスクが高まる

求められるのは、閉域・レガシー環境でも「端末自身で見つけ、封じ込められる」対策

© Tokyo Electron Device LTD. All Rights Reserved.

閉域網環境でも実現する自律型EDR運用

クラウド接続に依存せず、端末上で侵入の検知から封じ込め・復旧までを継続

製造現場の制約

工場・OT環境

1. **閉域網でも侵入経路が残る**
   USB・保守PC・更新媒体など
2. **レガシーOS／パッチ制約**
   設備依存で更改が困難
3. **OS内部の脅威が見えにくい**
   プロセスの振る舞いまで監視できていない
4. **生産設備を止められない**
   初動対応にかけられる時間が限られる

クラウド接続や停止を前提にしにくい

SentinelOneによる対応



運用上の価値

ON-PREMISES

閉域網内で一元管理

オンプレミス管理サーバー構成
インターネット非接続環境に対応

LEGACY OS SUPPORT

レガシー環境にも幅広く対応

レガシーOSを含む幅広いOSをサポート
既存設備を活かしながらEDRを導入

AUTOMATED RESPONSE

検知から復旧まで自動化

不審な振る舞いをリアルタイムに検知
人的対応を待たず被害拡大を抑制

「侵入させない」だけではなく、「**侵入されても早期に見つけて止める**」セキュリティへ

© Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス

東京エレクトロンデバイスによる支援体制

© Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロンデバイスが選ばれる理由

SentinelOne

2022年から開始のAPJパートナーアワード

JAPAN Partner of the Year



連続受賞

長い歴史

- 2018年SentinelOne社と販売代理店契約を締結
- 最古参のディストリビューター

豊富な導入実績

- 国内実績200社、22万ライセンス以上
- 製造業、小売、金融、IT、物流などの多種多様な業種でご支援

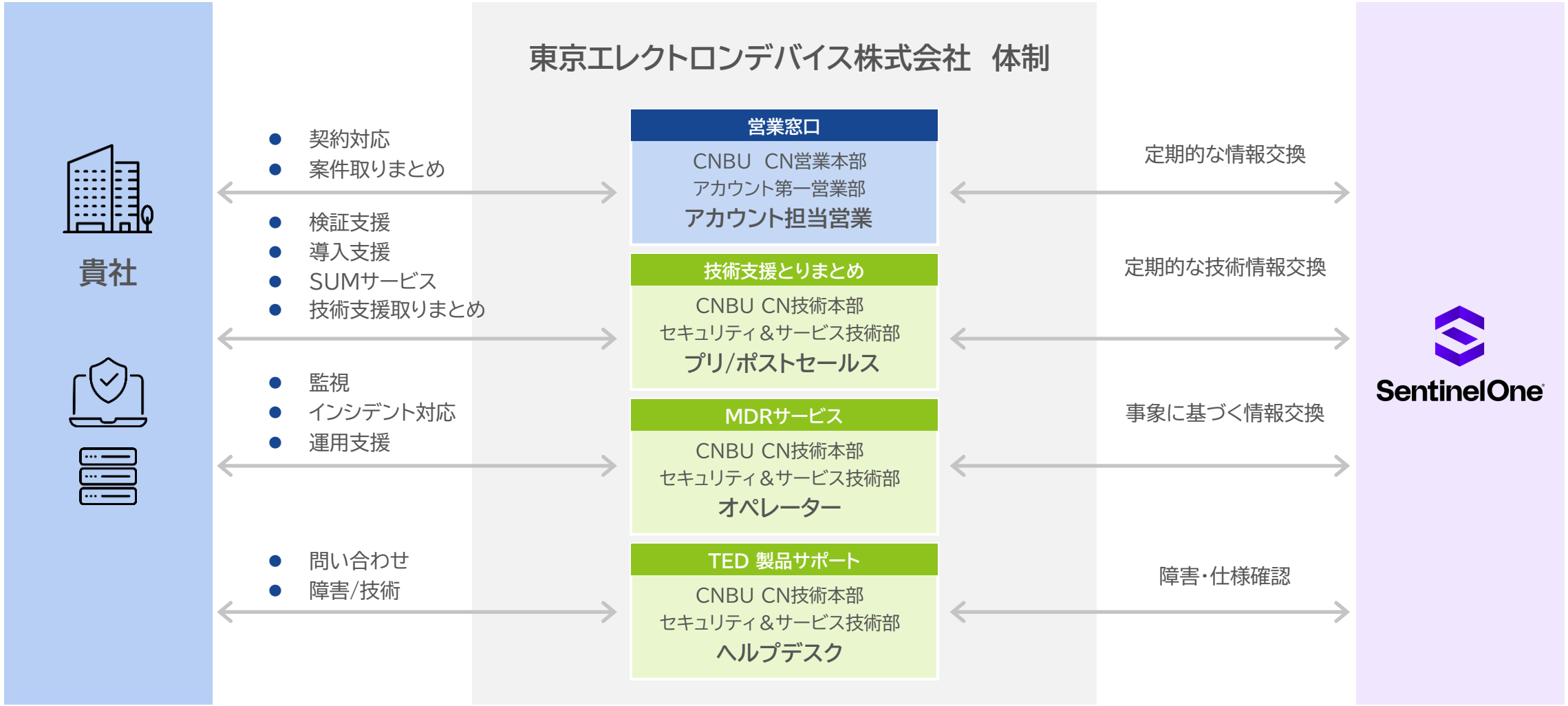
充実したサポート

- 検証から導入までを専任SEがサポート
- 約20名体制でサポート
- 国内顧客の需要に合わせたTED独自のMDR(MS1)サービスを提供
- 弊社独自の日本語マニュアルを提供
- サポートポータルにてお問い合わせを管理
- ナレッジページの提供

長い歴史と豊富な導入実績に基づいた充実したサポート

© Tokyo Electron Device LTD. All Rights Reserved.

ご支援体制



© Tokyo Electron Device LTD. All Rights Reserved.

各フェーズにおける技術支援サービス

導入フェーズ

導入支援

基本設計～導入までの技術支援

導入支援サービス

トレーニング

運用最適化、インシデント管理・対応方法のトレーニング

基本運用トレーニングサービス

インシデント管理・対応トレーニング

運用フェーズ

ヘルプデスク

SLAに準じた、技術QA、トラブル対応の支援

ヘルプデスクサービス

※ 製品サブスクリプション
ライセンスに含まれます

カスタマーサクセス

運用フェーズにおける各種課題解決をスポットで支援

カスタマーサクセスサービス

定例会サービス

定例会にて機能アップデート情報、運用ナレッジの提供や各種課題解決を支援

定例会サービス

TED-SOC SOCサービス

セキュリティ監視・運用サービス、お客様のニーズに応じた複数のサービスプラン

フルマネージドサービス

インシデントレスポンスサービス

オプティマイズドサービス

《オプション》

XDR統合セキュリティサービス

スレットハンティングサービス

DFIRサービス

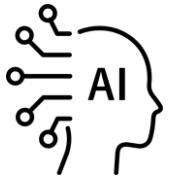
多彩なメニューから、お客様のご要望に応じた技術支援サービスをご選択いただけます

© Tokyo Electron Device LTD. All Rights Reserved.

まとめ

© Tokyo Electron Device LTD. All Rights Reserved.

まとめ　SentinelOneが選ばれる理由



AIで即時防御

脅威を端末上で自動判定し、
検知から封じ込めまでを高速化。
初動対応の遅れを防ぎ、被害拡大を抑制。



攻撃全体を一目で把握

Storylineが個々のイベントを自動相関し、
攻撃の流れを可視化。
原因や影響範囲をすばやく特定できます。

検知・調査・防御・復旧までを自動化する自律型セキュリティプラットフォーム



被害を抑え、早期復旧

検知・隔離だけでなく、
修復・ロールバックまで一気通貫で対応。
復旧時間を短縮し、業務継続性を高めます。



レガシー環境まで一元保護

Windows／macOS／Linuxに加え、
古いOSにも幅広く対応。
更改が難しい環境も同一基盤で保護。

© Tokyo Electron Device LTD. All Rights Reserved.

EPP/EDRを再定義する SentinelOne オンプレ環境からAI活用時代まで守る新しい選択肢（後半戦）

2026年10月14日

東京エレクトロン デバイス株式会社

斉藤 慎也

ここからのお話し

- 守るべき対象を変えます

端末・サーバーを守るお話し　⇒　AIの“利用・開発・接続先”を守るお話し

今まで



端末・サーバーを守る

- ウイルス対策・EDR・ファイアウォール
- “持ち込ませない／実行させない”防御

これから



AIの利用・開発・接続先を守る

- 生成AIの利用・AIコード開発・自社AIアプリ
- Agentic AI と外部ツール／MCP接続先

従来のエンドポイント対策だけでは”捉えにくい”領域が急拡大。

Device LTD. All Rights Reserved.
©

そのAI 既に会社で利用されていませんか？

管理・開発・人事・法務・経理・営業 — 生成AIは組織のあらゆる部門で日常的に使われています

経営・管理

戦略立案・資料作成

開発

コード生成・レビュー

人事

文書作成・面接準備

法務

契約チェック・要約

経理

集計・問い合わせ対応

営業

提案書・メール作成

AIを使うリスクは「従業員のAI利用」から

© Device LTD. All Rights Reserved.

その利用、”見えないまま”だとどうでしょうか？

把握できないまま利用が先行すると、、、

見えていないAI利用 = リスクの起点

- 全社の生成AI利用状況
- シャドーAI（無許可ツール）
- ポリシー違反アラート
- アクティブユーザー / 入力内容

可視化すべき観点 — 誰が・いつ・何を入力したか

機密データ（個人情報など） の検出・追跡

話題（犯罪・政治など） の検出・追跡

Secrets（APIキーなど） の検出・追跡

可視化できない状態では、選択肢は”禁止”か”放置”の二択になりがち。

© Device LTD. All Rights Reserved.

放置した場合のリスクとは？

AIリスクは利用者の不注意だけでなく、サービス側の設定不備でも顕在
攻撃面は”AIの構造そのもの”に



ユーザー

入力ミス（利用者起因）

エンジニアが ChatGPT にソースコードを入力し、機密情報の漏えいが問題化。利用者の不注意が直接の引き金に。



AIアプリケーション

基盤露出（サービス側）

認証なしのDB露出により、チャット履歴・APIキー・バックエンド情報が外部に流出。設定不備が原因に。



EchoLeak（ゼロクリック）

細工したメールを M365 Copilot が解釈し、社内データが“クリック不要”で外部流出しうる間接プロンプトインジェクション。(ユーザー操作不要)

いっそのこと禁止に・・・

© Tokyo Electron Device LTD. All Rights Reserved.

とはいえ”一律禁止”では守れません

一律禁止

- 業務効率が下がる
- 現場が別のAIへ移る
- 利用実態がさらに見えなくなる

閉じるだけではリスクも見えない

安全に使い続ける

- 利用状況を把握する
- 機密情報を守る
- リスクに応じて制御する

“見える化”して、必要なところだけを止める

これを実現できるのが・・・ Prompt: A SentinelOne Company です。

© Tokyo Electron Device LTD. All Rights Reserved.

Prompt Security

Prompt:

A SentinelOne Company

会社概要

Prompt Security AIセキュリティ

生成AIの利用・開発・アプリ・エージェントを守る

- 2023年設立 / イスラエル・2025年 SentinelOne が買収
- GenAI / Agentic AI セキュリティ戦略の中核

↑ 買収

SentinelOne 基盤セキュリティ

AIネイティブな統合セキュリティプラットフォーム企業

- 2013年設立 / 米国カリフォルニア州・NYSE上場
- Endpoint・Cloud・Identity・Data を統合保護

AI利用 / 開発 / Agentic AI / 自社AI を包括的に保護

Prompt for Employees
（従業員向け）

どこを保護するか
従業員による生成AI利用

保護ポイント
- シャドーAIの可視化(約13,000種類の生成AIに対応)

Prompt for AI Code Assistant
（開発者向け）

どこを保護するか
AIコードアシスタント利用工程

保護ポイント
- コード内の機密情報・PII・IP保護

Prompt for Agentic AI
（エージェンティックAI向け）

どこを保護するか
AIエージェントとMCP連携

保護ポイント
- MCP活動の可視化や危険なMCP・不正エージェント検知

Prompt for Homegrown Applications
（自社開発アプリ向け）

どこを保護するか
自社AIアプリの入出力と接続先

保護ポイント
- 不適切なAI応答、アプリ悪用、過剰課金リスクへの対策

シャドーAI・データ漏洩などのリスクを横断的に防ぐ。
AIを安全に利用するための統合セキュリティプラットフォーム

Device LTD. All Rights Reserved.

“アプローチの違い”を3つの視点で

①柔軟な導入形態

②保護ポイント

③直観的なGUI

© Tokyo Electron Device LTD. All Rights Reserved.

違い ①柔軟な導入形態 – 単品で買えます

既存のEDR／SASEを変えずに、Prompt Security だけを導入可能

Prompt Security	EDRメーカー製品	SASEメーカー製品
✓ 単体での購入が可能	✗ EDRの同時購入が必須	✗ SASE／Proxy の同時購入が必須
✓ 250ライセンスから（要相談）	✗ 5,000ライセンスから	✗ 最低購入数は非公開
✓ 既存EDR／SASEを変えず導入可能	✗ 別メーカーのEDR利用時は導入不可	✗ 別メーカーのSASE利用時は導入不可
✓ 段階的に拡大（スモールスタート可）	✗ スモールスタート不可	✗ スモールスタート不可

まずは小さくはじめて、効果を見ながら広げる

ron Device LTD. All Rights Reserved.

違い ②保護ポイントは“端末側”

経路依存の対策では取りこぼす。Prompt は端末側で横断的にカバー

Prompt Security — 端末側で横断カバー

- ブラウザ経由の生成AI
- デスクトップ版の生成AIアプリ
- ローカルLLM
- 主要ブラウザに対応（Chrome / Edge / Safari / Firefox ほか）

EDRメーカー製品

ブラウザ経由の生成AI のみ（Safari非対応の場合も）

SASEメーカー製品

自社のSASEを経由するトラフィックのみ

端末に近いからこそ取得できる情報が豊富

ron Device LTD. All Rights Reserved.

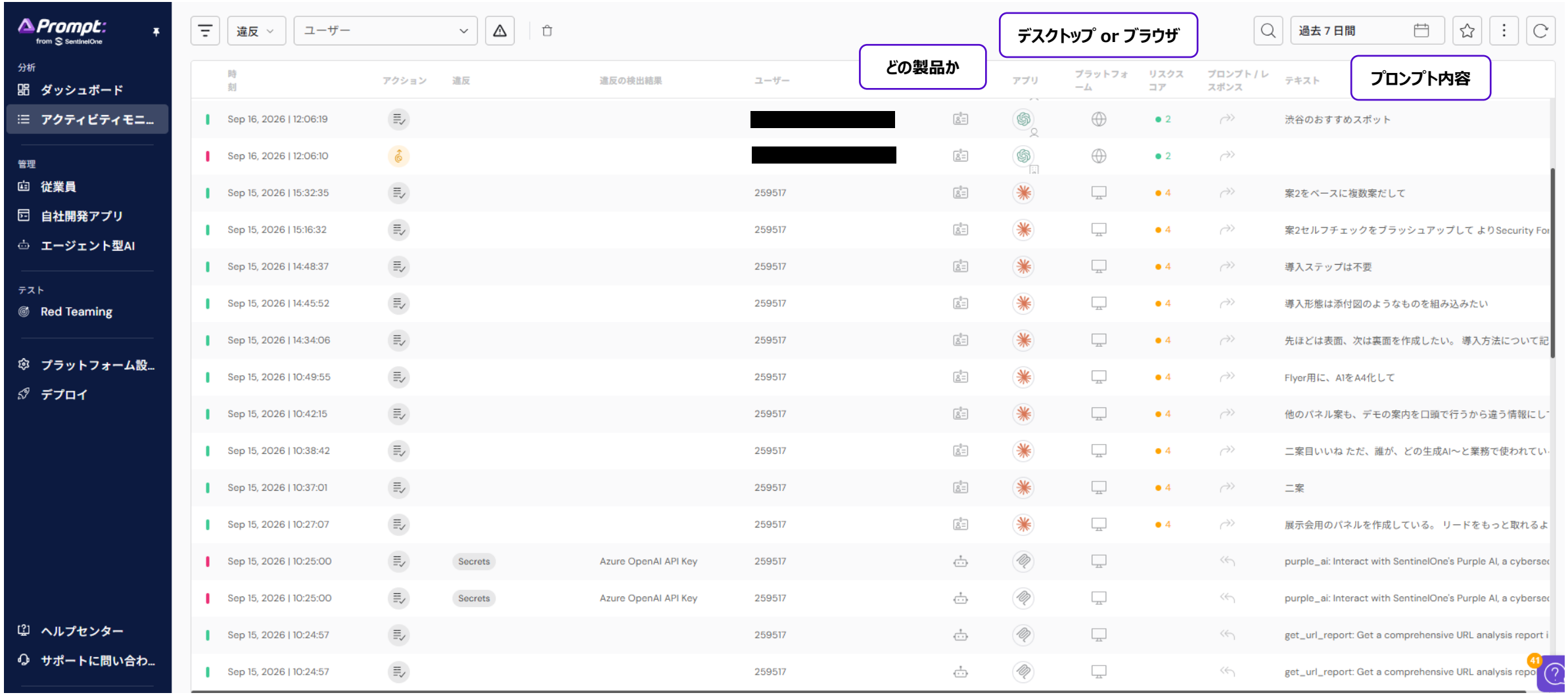
違い ③直観的なGUI



企業内での生成AI利用率の資料や、監査ツールとしても活用可能

ron Device LTD. All Rights Reserved.

参考 プロンプトがこんなに・・・



© Tokyo Electron Device LTD. All Rights Reserved.

まとめ –必要なのは”見える化・制御・教育”の一体運用

技術対策と運用、そして人を一体で回すことで、AIリスクを継続的に抑えられます



見える化

機密データ / シークレット検出・トピック単位の把握・利用状況のログ／警告



制御

ユーザー / アプリ別ルール・個人アカウント／アップロード制御・自動匿名化



教育

従業員トレーニング・未受講者の利用ブロック・リスク意識の定着

AIを安全に利用するためのガードレール整備を進めてみませんか？

ron Device LTD. All Rights Reserved.

東京エレクトロン デバイス