kaspersky

Kaspersky Anti Targeted Attack

2025年07月01日
株式会社カスペルスキー
セールスエンジニアリング本部

V1.0

Kaspersky Anti Targeted Attack（KATA）とは?

kaspersky

高度なネットワークおよびエンドポイントの検知・インシデントレスポンス・予防的な脅威の探索を組み合わせた包括的な標的型攻撃対策を実現
NDR/EDR機能により、管理の一元化とリアルタイムの可視化し、すべての主要な攻撃侵入ポイントを完全に制御

- ✓ 複数のセンサによるITインフラ全体の脅威状況の可視化と異常な挙動の検知
- ✓ 機械学習・サンドボックスによる脅威検出と直観的なレスポンス機能
- ✓ プロアクティブな脅威ハンティングやフォレンジックをサポートする相関分析・Yaraルール・遡及分析機能

Copyright © 2025 Kaspersky Lab. All rights reserved.

KATA ｜ 特徴

kaspersky

■高度な脅威検出

セントラルノードによる機械学習・KSNによるレピュテーション確認・サンドボックスによる動的分析を組み合わせ、標的型攻撃をはじめとする高度な脅威を検出

■多層的なセキュリティ分析

ネットワーク・メール・Webトラフィック・エンドポイントなど複数のソースからイベントを収集し、攻撃の全体像を可視化

■インシデント対応支援

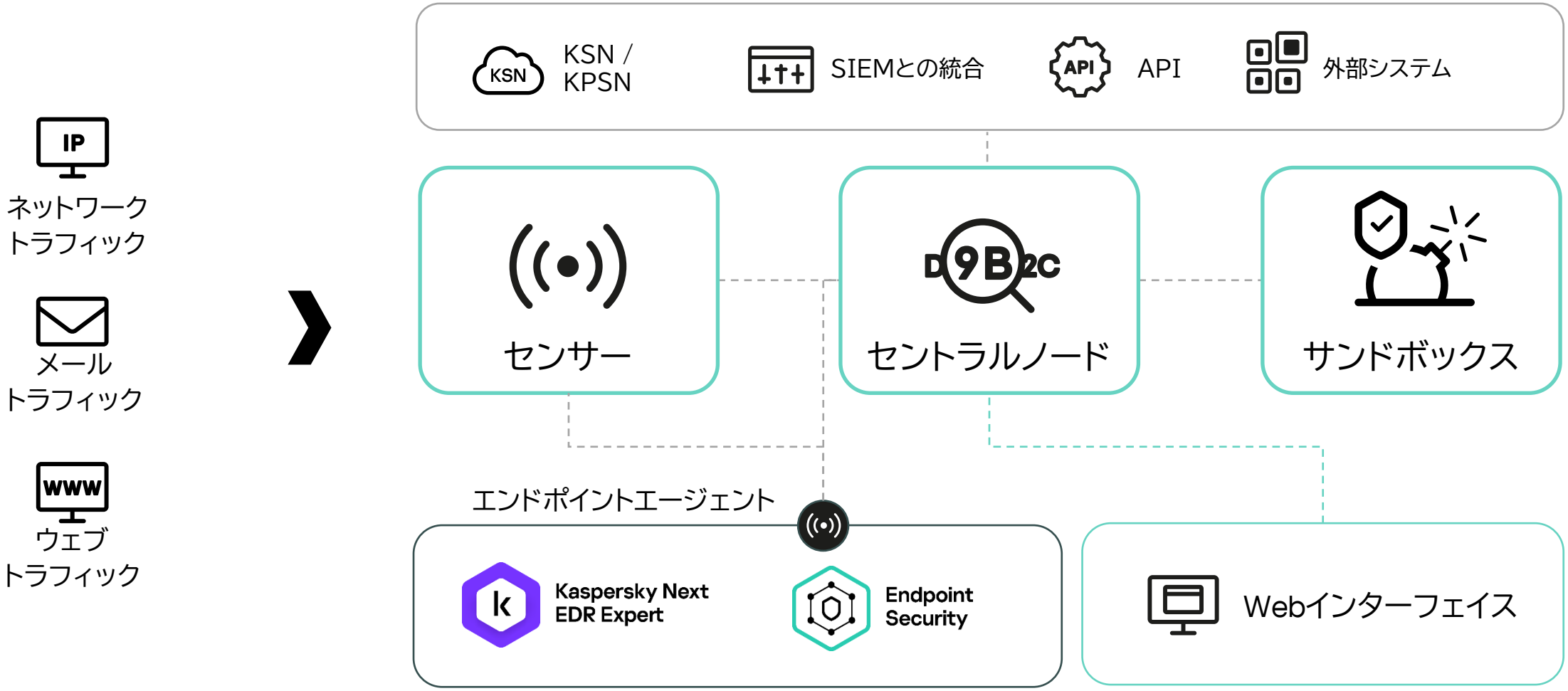
相関分析によって、脅威の起点・経路・影響範囲を明確にし、自動・手動によるレスポンス機能で迅速な対応・封じ込めをサポート

さらに、収集したログ・データを対象とした遡及分析・YARAルールやIOCによる脅威検出で能動的な脅威ハンティングをサポート

Copyright © 2025 Kaspersky Lab. All rights reserved.

KATA| アーキテクチャ

kaspersky



Copyright © 2025 Kaspersky Lab. All rights reserved.

KATA| 3つのエディション

kaspersky

KATA

メール・ネットワーク・ウェブトラフィックの収集、セントラルノード・サンドボックスによる分析
ネットワークレベルでの不審なパターン・ふるまいを検知

KATA NDR Enhanced

KATAの機能に加え、エンドポイントからもネットワークテレメトリも収集、分析
ネットワーク情報の可視化・遡及分析を提供し、脅威ハンティングをサポート

KATA Ultra

KATA｜NDRの機能にEDRでの分析機能を追加、IoC/IoA・ Yaraルールによる脅威検出で
高度なサイバー攻撃の予兆を検出し、早期対応の実現をサポート

（※EDR機能の詳細はKaspersky Next EDR Expertの資料をご参照ください）

Copyright © 2025 Kaspersky Lab. All rights reserved.

KATA| 機能比較

kaspersky

	KATA	KATA NDR Enhanced	KATA Ultra
URLレピュテーション	○	○	○
サンドボックス（ネットワークレベル）	○	○	○
Yaraルール（ネットワークレベル）	○	○	○
アンチマルウェアエンジン（ネットワークレベル）	○	○	○
Cloud ML for Android（ネットワークレベル）	○	○	○
ICAP / SMTP / POP3 / API での統合	○	○	○
TLSフィンガープリント	○	○	○
ディープパケットインスペクション		○	○
IDS		○	○
ネットワークセッション、ネットワークマッピング、ネットワーク可視化		○	○
RAWファイルの保管、遡及分析		○	○
ネットワークテレメトリ分析とエンドポイント監視（Windows / Linux）		○	○
ネットワークセキュリティリスクからの保護		○	○
クロスプラットフォーム分析(Windows / Mac / Linux)			○
IoCスキャン			○
IoA			○
Yaraルール（エンドポイントレベル）			○

Copyright © 2025 Kaspersky Lab. All rights reserved.

コンポーネント紹介 ｜ センサー

kaspersky

センサー：

ネットワーク・メールトラフィック・エンドポイントエージェントがインストールされたホストからデータを受信

KSNによるURLレピュテーションチェック・IDSによる組織のインフラストラクチャに対する攻撃の兆候を検出し、さらなる分析のため、セントラルノードに転送

ネットワーク：SPAN・ERSPAN・RSPANトラフィックを受信・処理し、HTTP・HTTP/2・FTP・SMTP・SMB・NFS・DNSプロトコルオブジェクトおよびメタ情報をネットワーク接続速度最大10 Gbpsで取得

メール：POP3（S）およびSMTP経由でメールサーバーに接続、メールのコピーを受信・処理

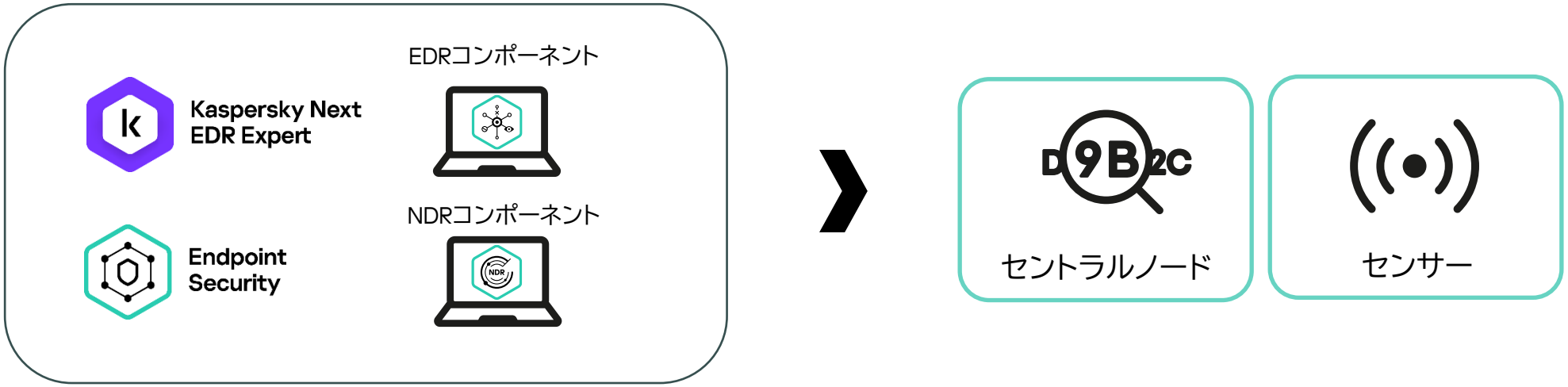
ウェブ：ICAP経由でプロキシサーバーに接続、HTTPおよびFTPトラフィックを受信・処理、プロキシサーバーでトラフィックの復号化が設定されている場合、HTTPSも処理

Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ エンドポイントエージェント

kaspersky

・エンドポイントエージェント：PC・サーバー・仮想マシンからテレメトリを収集し、
センサーおよびセントラルノードに送信
カスペルスキーのEPPの場合、NDR・EDRコンポーネントが
EPPに組込み済み
カスペルスキー以外のEPPの場合、エンドポイントエージェントを
インストールすることで統合可能



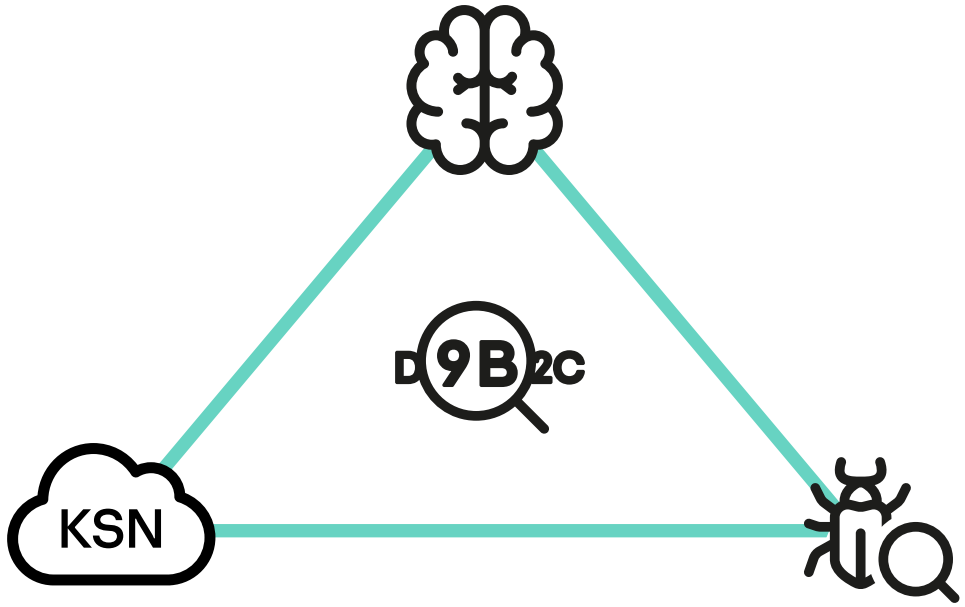
Copyright © 2025 Kaspersky Lab. All rights reserved.

コンポーネント紹介 ｜ セントラルノード

kaspersky

・セントラルノード：「**アンチマルウェアエンジン**」と「**標的型攻撃アナライザー**」で構成される
テレメトリの分析基盤

・機械学習を搭載した標的型攻撃アナライザー・アンチマルウェアエンジン・クラウドベースの脅威情報基盤「Kaspersky Security Network（KSN）」から提供される情報を組み合わせて詳細に分析



Copyright © 2025 Kaspersky Lab. All rights reserved.

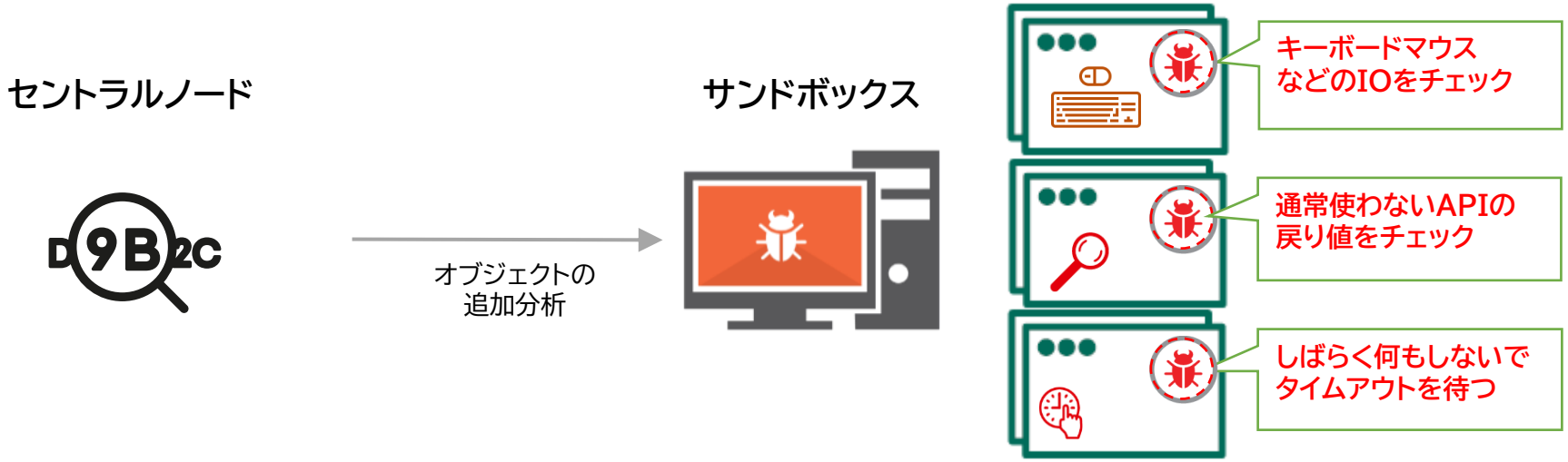
コンポーネント紹介 ｜ サンドボックス

kaspersky

・疑わしいオブジェクトを仮想マシンで実行し、システム関数呼び出しのログ、他のプロセスやファイルとのやり取り、ネットワーク活動、URL、ダンプ、ドロップされたオブジェクト、生成されたトラフィックなどを収集し、悪意のある活動を検出

・サンドボックス回避機能を持つマルウェアへの対応を実現、最新の回避手法に対抗するためにモジュールを随時配信

・解析環境：Windows XP・7・10、CentOS 7.8、Astra Linux 1.7をサポート

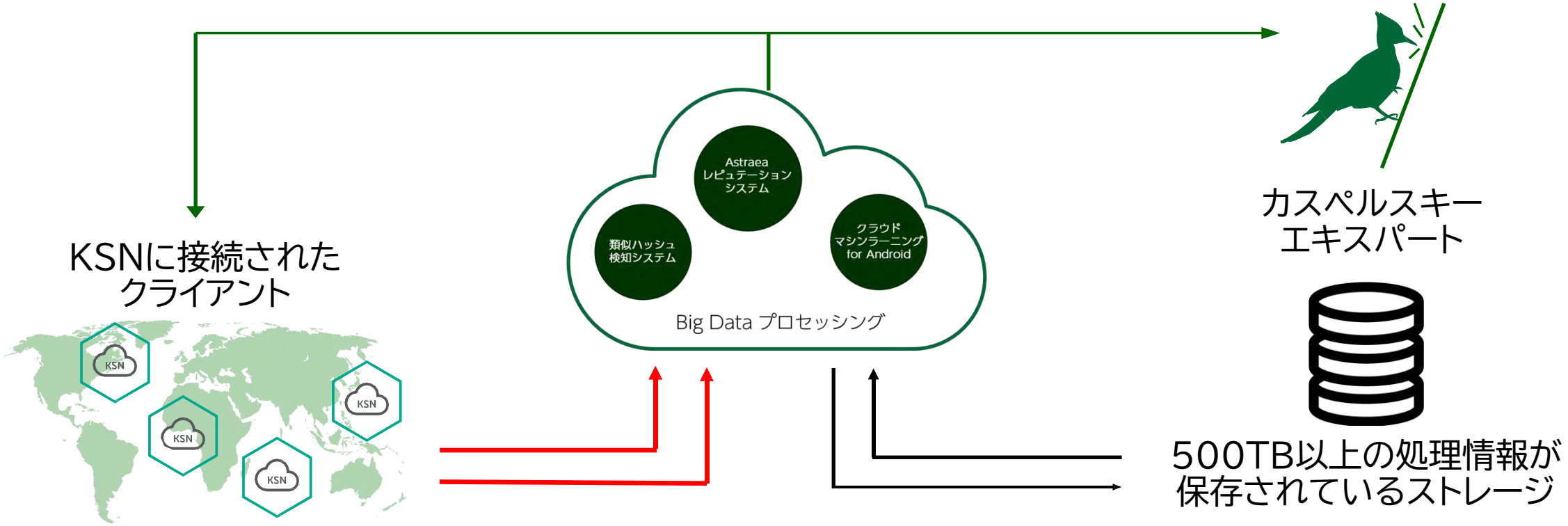


Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ KSN

kaspersky

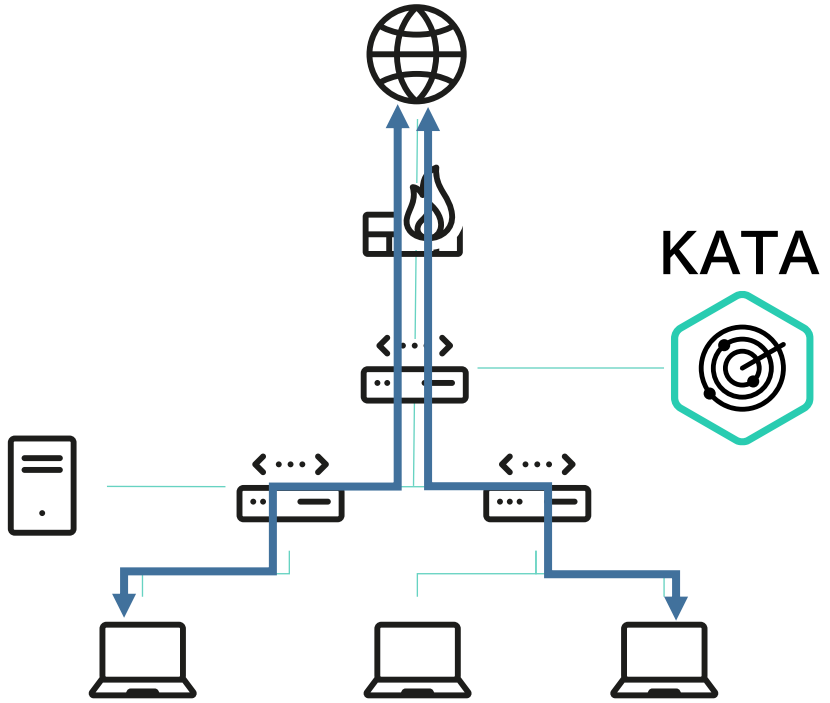
・カスペルスキー製品利用の数百万のお客様の同意を得た上でサイバーセキュリティ関連情報を収集
収集された情報を基に脅威に即座に判断・対応
高度で未知のマルウェアの検知・誤検知の低減・新たな脅威への応答時間の大幅な短縮を実現

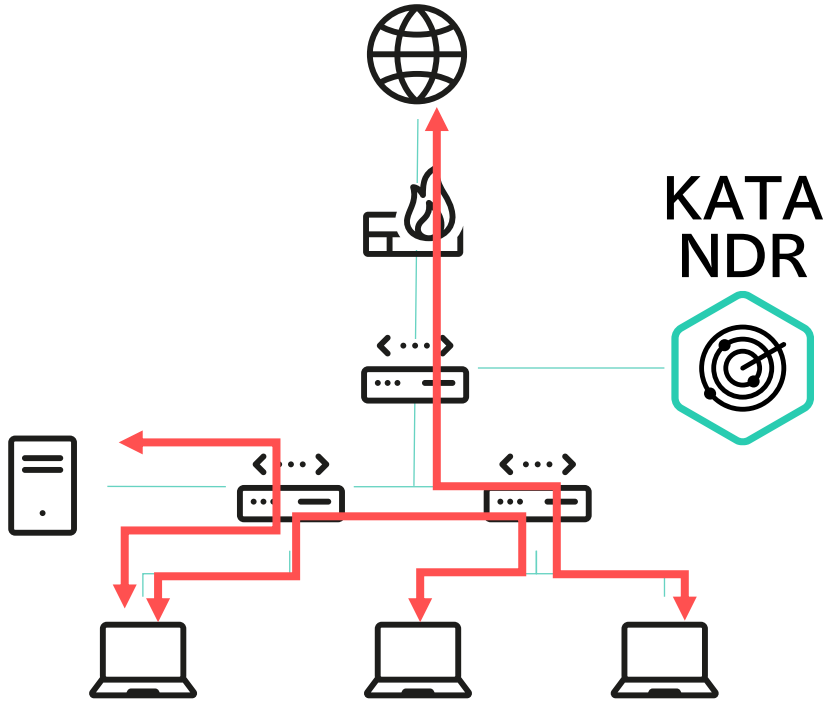


Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ IDS

KATA: KATAと連携するNW機器を通るネットワークトラフィックを分析
KATA NDR:クライアントからもデータを収集することでKATAと連携するNW機器を
通らないトラフィックの分析も実現



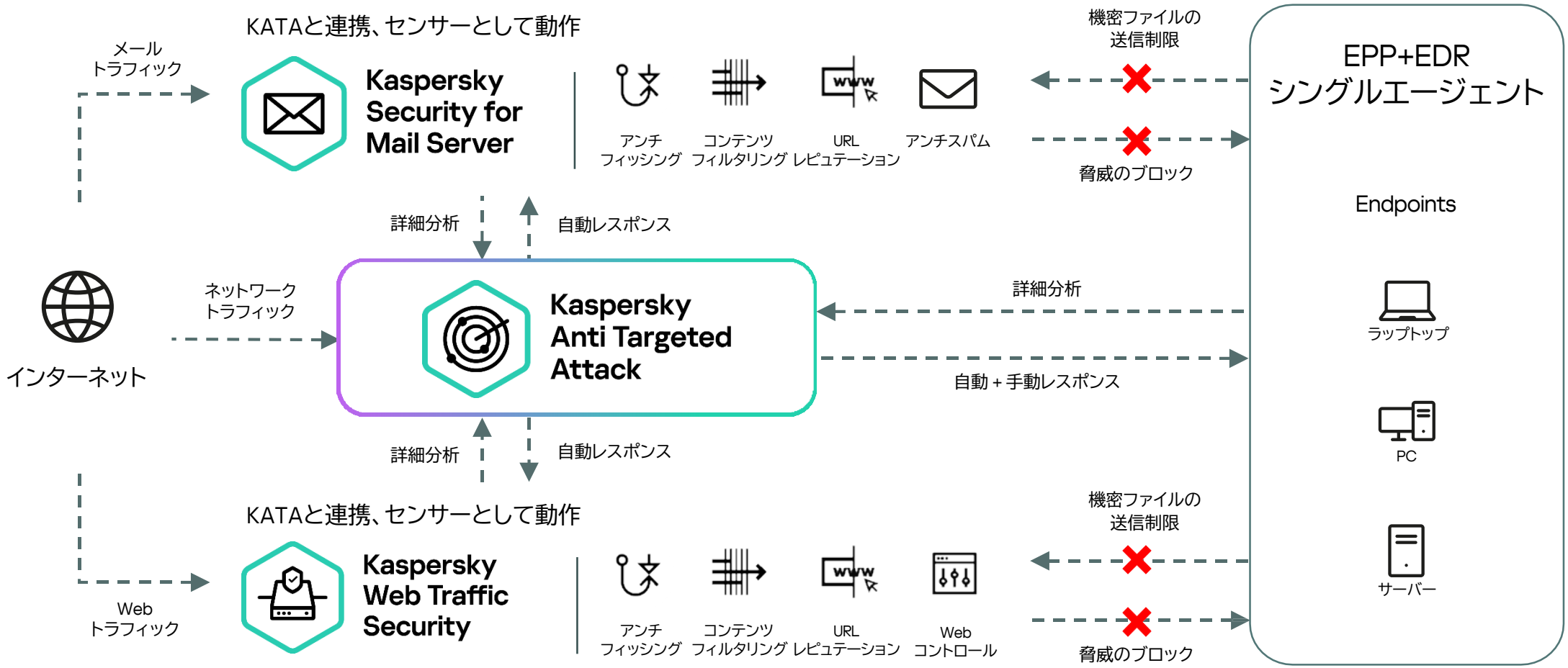


Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ カスペルスキー製品との統合

kaspersky

・カスペルスキーのゲートウェイ製品と統合、センサーとして動作



Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ ふるまい検知

kaspersky

セントラルノードによるふるまい検知でネットワークレベルでの不審なアクティビティを検出

＜検知例＞

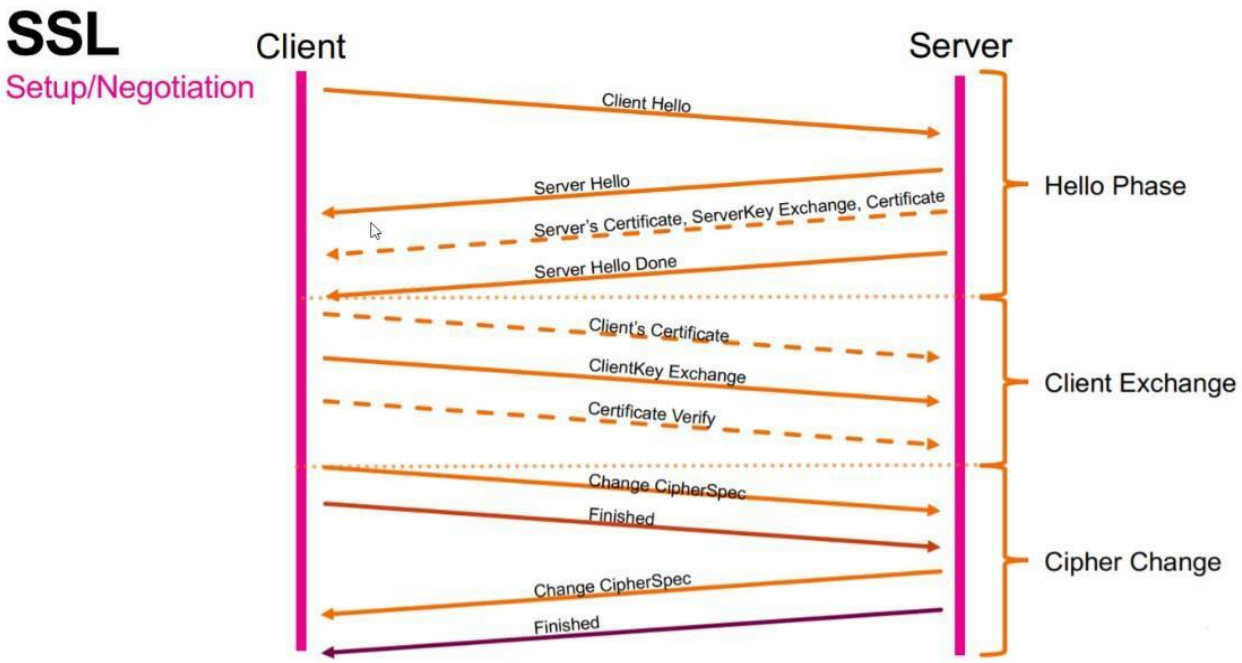
・DC同期
・DNSトンネリング
・ICMPトンネリング
・ブルートフォース攻撃（HTTP、FTP、SSH、SNMP、RDP、Kerberos）
・Kerberoasting
・不審なファイル読み書き動作

Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ TLSフィンガープリント

kaspersky

・TLSハンドシェイクのHelloフェーズから情報を抽出してハッシュ化、IDSルールと照合し脅威を検出

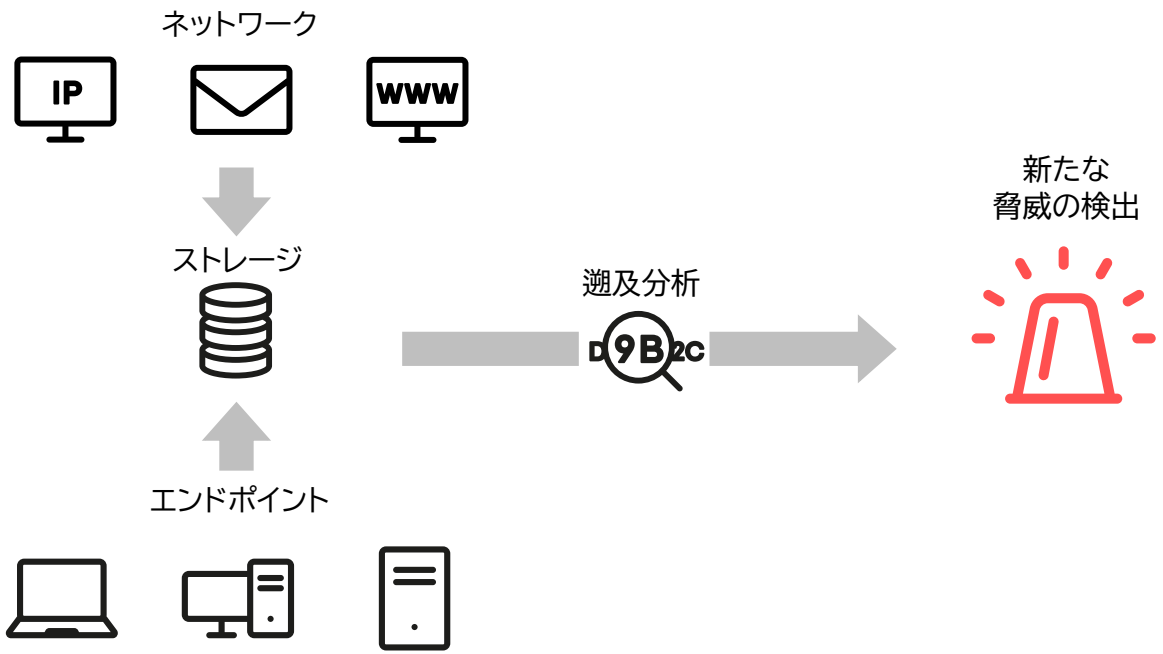


Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ ログの保存・遡及分析

kaspersky

・テレメトリ/オブジェクトを自動収集し、ストレージに保存
サイバー攻撃による暗号化などアクセス不能な状態になった場合でも、調査・分析に必要なデータへのアクセスを提供
さらに、保存されたデータを対象に新たなIoCをトリガーとした遡及分析をサポート



Copyright © 2025 Kaspersky Lab. All rights reserved.

kaspersky