Kaspersky Network Security Data Feeds

2025年10月21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

V1.1

なぜ脅威インテリジェンスが必要なのか？

kaspersky

■ 脆弱性を正確に把握し、リスク管理を行う「コンプライアンス型アプローチ」では
管理コスト・リソース・複雑性から十分な対策が難しくなった

-管理コスト：利用製品の多様化などにより、脆弱性対応の負担が増大
-リソース：　セキュリティにかけられるヒト・モノ・金・時間は有限
-複雑性：　クラウド・サプライチェーンなどの拡大で、IT環境がより複雑に

■ 「脆弱性をどう管理するか」という発想から「攻撃者の目的をいかに阻止するか」という点に
焦点を当てた「脅威ベース型アプローチ」が注目

**＝ サイバーセキュリティリスクの起点となる「脅威」を理解し、発生頻度・影響が大きいリスクに
対する具体的な脅威への対応を優先**

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Network Security Data Feeds とは

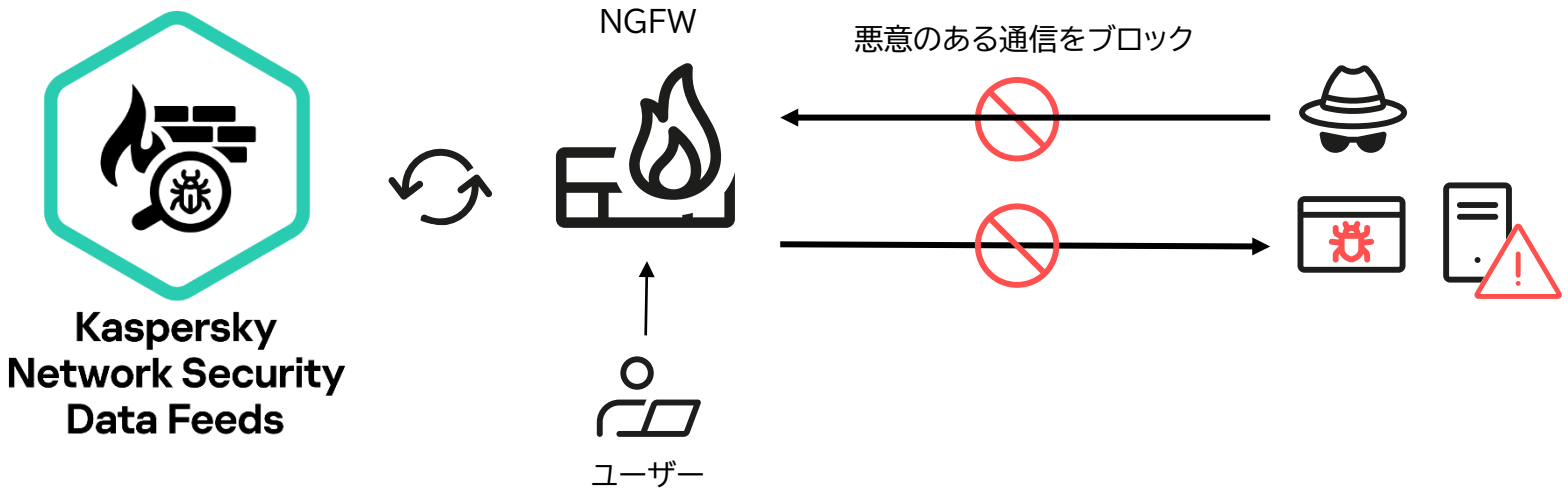
kaspersky

■Kaspersky Network Security Data Feeds：

・カスペルスキーの脅威データフィードを次世代ファイアフォール（NGFW）向けに最適化した脅威データフィードサービス

・NGFWの外部脅威データフィードとして登録することで脅威の検出力を強化

・3種類（マルウェア・ボットネット・フィッシング）のURLのルールセット(※)とC2サーバーなどの通信先IPアドレスのルールセットを提供、URL・IPアドレスそれぞれ単体での契約可能



※Kaspersky Threat Data Feeds – Network Security URLを契約することで3つのURLのルールセットが利用可能

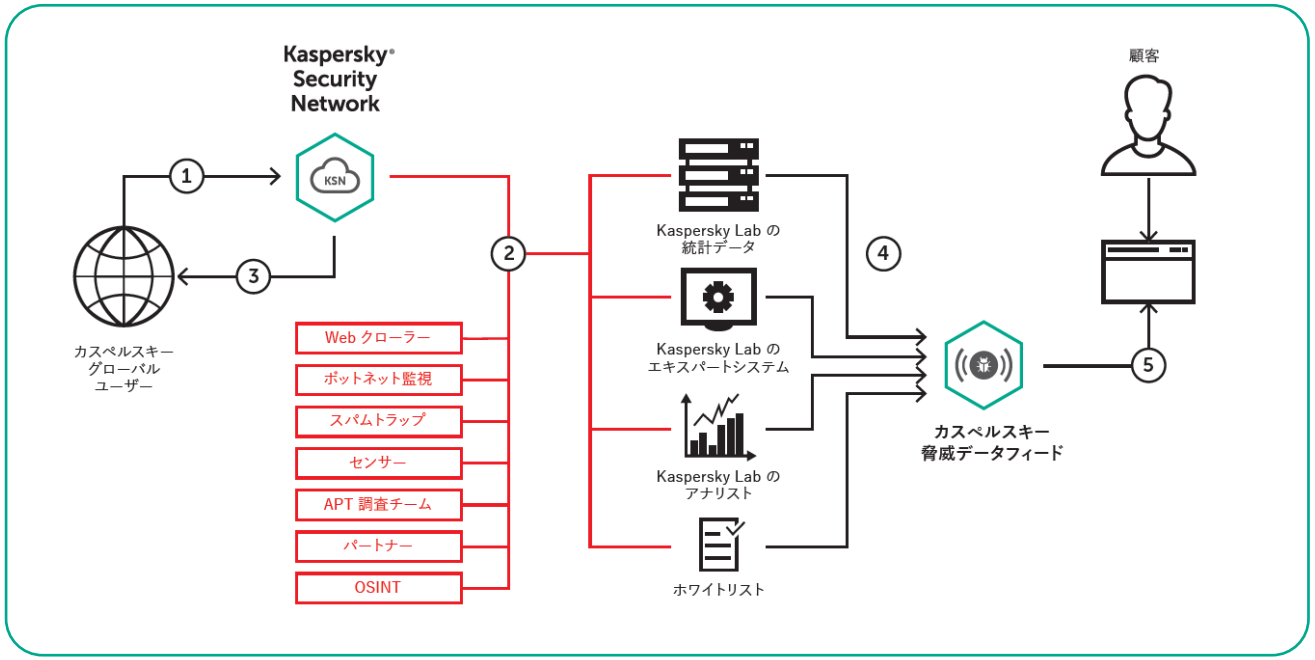
Copyright © 2025 Kaspersky Lab. All rights reserved.

脅威インテリジェンスのソース

kaspersky

・カスペルスキーの脅威インテリジェンスは、Kaspersky Security Network、独自のウェブクローラー、ボットネット監視サービス（ボットネットとそのターゲットおよび活動を 24 時間 365 日監視）、スパムトラップ、リサーチチーム、パートナー及び当社が収集した悪意あるオブジェクトに関するその他の過去データなど、信頼性の高い各種のソースから収集

・収集された情報を統計分析、サンドボックス・ヒューリスティックエンジン・機械学習などのエキスパートシステム、アナリストによる検証、ホワイトリストなど、さまざまな技術を用いて「リアルタイム」で分析することで、**誤検知の少ない高品質な脅威データフィード**を提供



Copyright © 2025 Kaspersky Lab. All rights reserved.

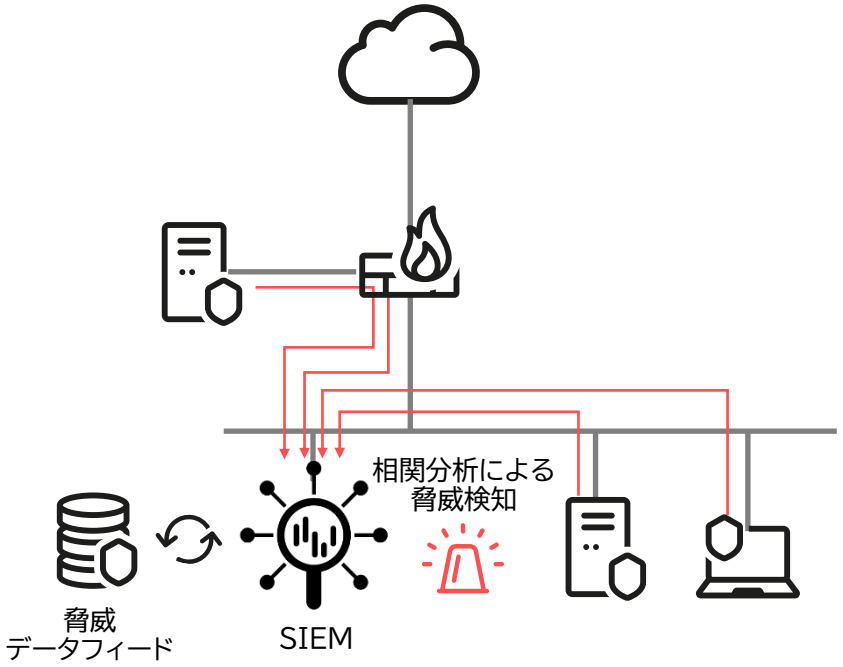
NGFWと脅威インテリジェンスを統合するメリット

kaspersky

■ SIEMのない環境でも脅威の検出力を強化

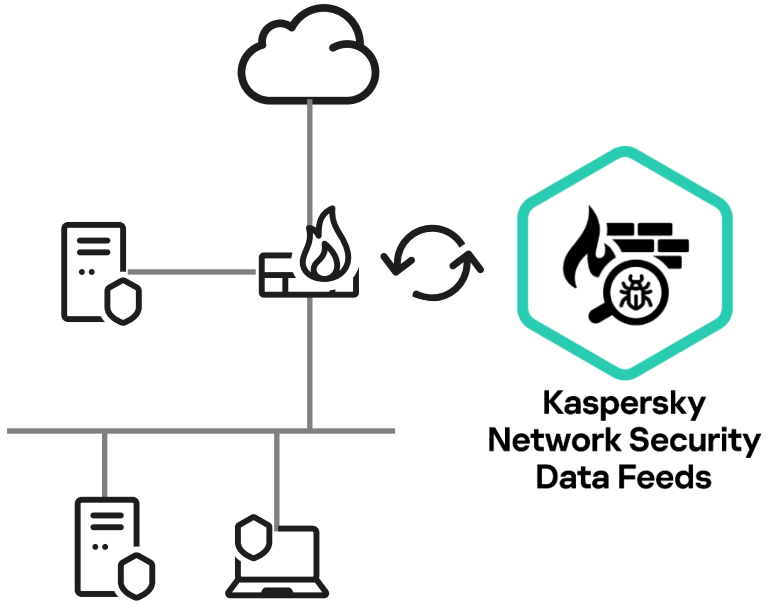
<SIEM環境>

SIEMへの情報集約・脅威データフィード連携による
脅威インテリジェンス統合で脅威を検出



<SIEM無し環境>

カスペルスキーの脅威データフィードなら、
SIEMが無い環境でも脅威インテリジェンス統合を実現



Copyright © 2025 Kaspersky Lab. All rights reserved.

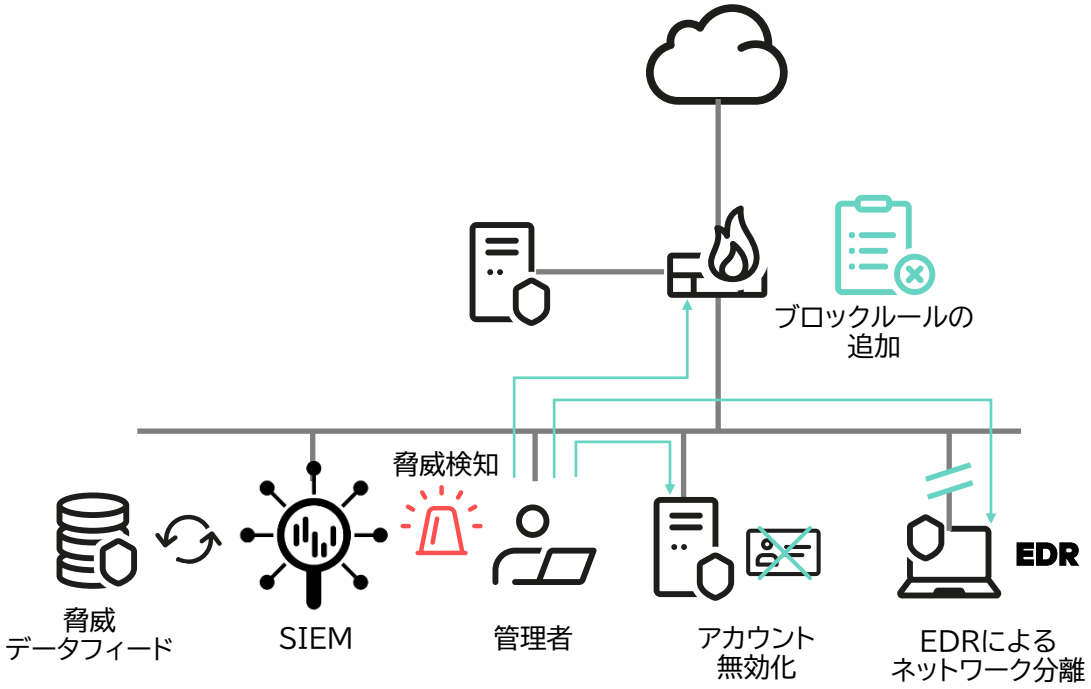
NGFWと脅威インテリジェンスを統合するメリット

kaspersky

■「能動的」なセキュリティ体制の実現

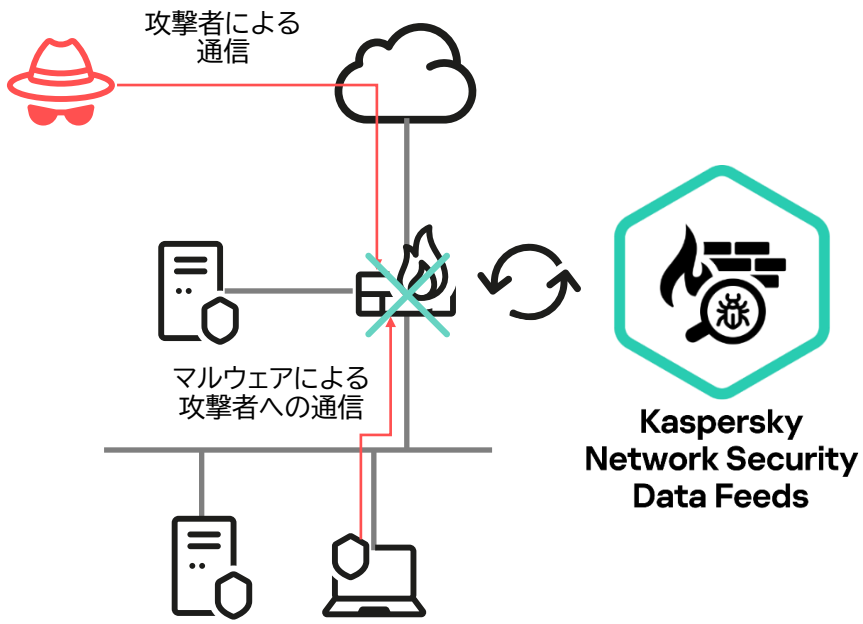
<SIEM+脅威インテリジェンスの場合>

SIEMでの分析で脅威を検出、FW・PC・ADなどで
脅威に対する柔軟な対応が可能
一方、運用の実現・即時性の確保にはリソースが必要



<NGFW+脅威インテリジェンスの場合>

NGFWに脅威インテリジェンスを統合することで
悪意のある通信を即時ブロック



Copyright © 2025 Kaspersky Lab. All rights reserved.

NGFWと脅威インテリジェンスを統合するメリット

kaspersky

■ ブラックリスト運用の工数削減

<無償の情報源(OSINT)を活用する場合>

IpC共有プラットフォームやセキュリティベンダーの
公開情報からの脅威情報の収集、信頼性などの検証、
製品への適用など、多くのプロセスが必要

<Kaspersky Network Security Data Feedsの場合>

カスペルスキーが提供する脅威データフィードと
利用中のNGFWの連携のみ
データの検証はカスペルスキーで実施済み

Copyright © 2025 Kaspersky Lab. All rights reserved.

サポート対象

kaspersky

ベンター名	サポート対象
Cisco	Cisco Firepower Management Center バージョン 6.2.3 以上で稼働するすべての NFGW （Threat Intelligence Director モジュール）
Fortinet	以下を含むFortiOS バージョン 6.0 以上を搭載したすべての FortiGate NGFW FG-30/50/70/90/120G、FG-40/60/70/80/100F FG-200/400/600/1000/1800/2600F、FG-200/900G FG-3000/3200/3500/3700/4200/4400/4800/6300/6001/6500/7081/7121F
Paloalto	PA-220, VM-50, VM-50 (Lite), VM 100, VM-1000-HV PA-850, PA-820, PA-3200 series PA-5200, PA-7000 series
CheckPoint	Gaia OS バージョン R81.20 Titan 以上を搭載したすべての Check Point ファイアウォール
Sophos	SFOS バージョン 21 以上を搭載したすべての Sophos ファイアウォール
Broadcom	Edge SWG (ProxySG) SG-Enterprise クラス — SGOS 7.4 SWG Edition 以上

Copyright © 2025 Kaspersky Lab. All rights reserved.

kaspersky