kaspersky

「Kaspersky Threat Data Feeds」のご紹介
～最新の脅威インテリジェンスを活用したセキュリティ対策強化～

2023年9月22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

Kaspersky Threat Data Feeds：サービス概要

Kaspersky
Threat Data Feeds

・**IOCと実用的なコンテキスト情報をJSON形式で提供**

-信頼性の高いさまざまなソースから情報を収集

-脅威データフィードの精度を高めるための当社技術を活用した分析・アナリストによる検証

・**用途や分野ごとに特化したさまざまな脅威データフィードから必要なものを選択して導入可能**

-悪意のあるURL・ハッシュ値・IPアドレスなどIoCごとに分類された脅威データフィード

-pDNSレコードセット、ICS向け、Suricata用、CASB用など特定の分野に特化した脅威データフィード

・**お客様の既存環境にあわせた導入方法が選択可能**

-ログ照合ツール「Kaspersky CyberTrace」の導入 / SIEM連携用アプリケーションの導入 / TAXIIサービスを仲介した
ダウンロード　など

kaspersky

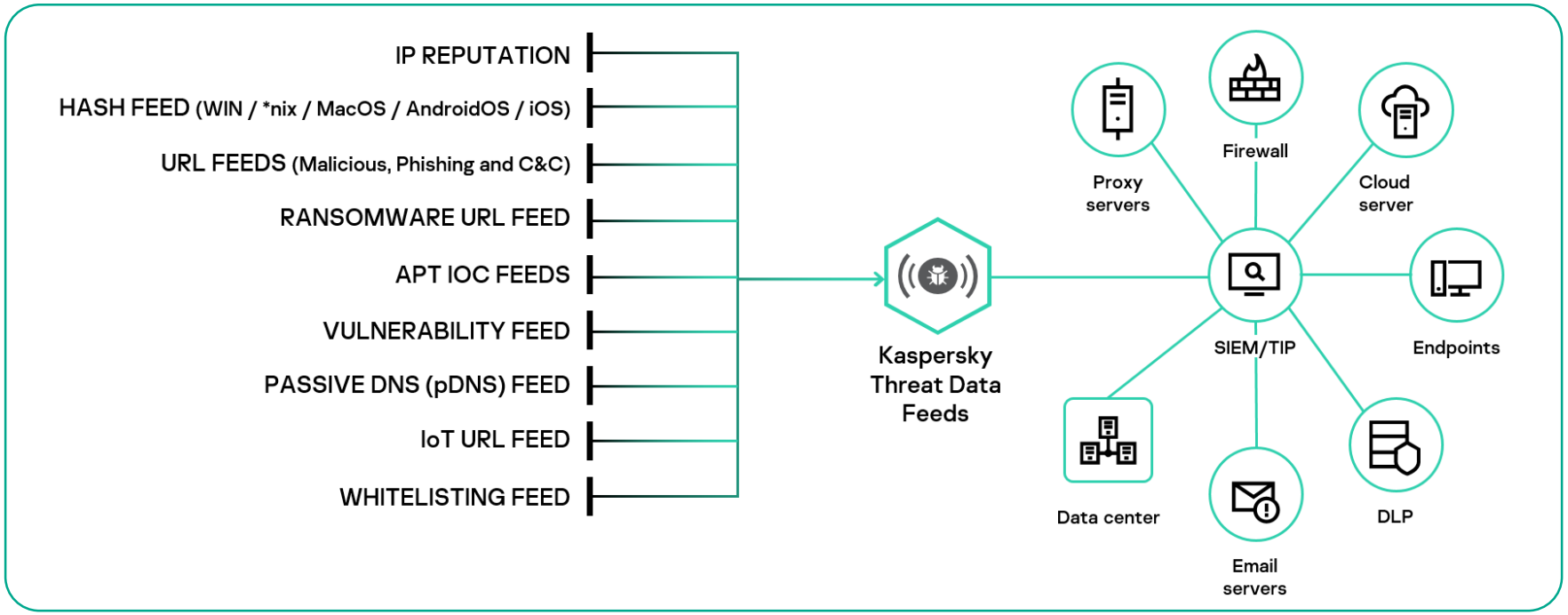
Kaspersky Threat Data Feeds とは

Kaspersky
Threat Data Feeds

高品質なIOCとコンテキスト情報を提供

・Kaspersky Threat Data FeedsはIOCと実用的なコンテキスト情報をJSON形式で提供します。
脅威データフィードは様々な脅威情報に特化した複数のフィードで構成され、各フィードの情報からグローバルな知見を得て、
攻撃者の戦術・テクニック・手順を深く理解することが可能です。

・データフィードの情報は世界中から収集された調査結果に基づいてリアルタイムで自動的に生成し、誤検知を削減する為に
フィードリリース前に大量のテストとフィルターを適用しているため、高い検知率と精度を実現します。
ログ解析やフォレンジック対応など様々な用途に活用することで、お客様のインシデント対応能力を改善、強化します。



kaspersky

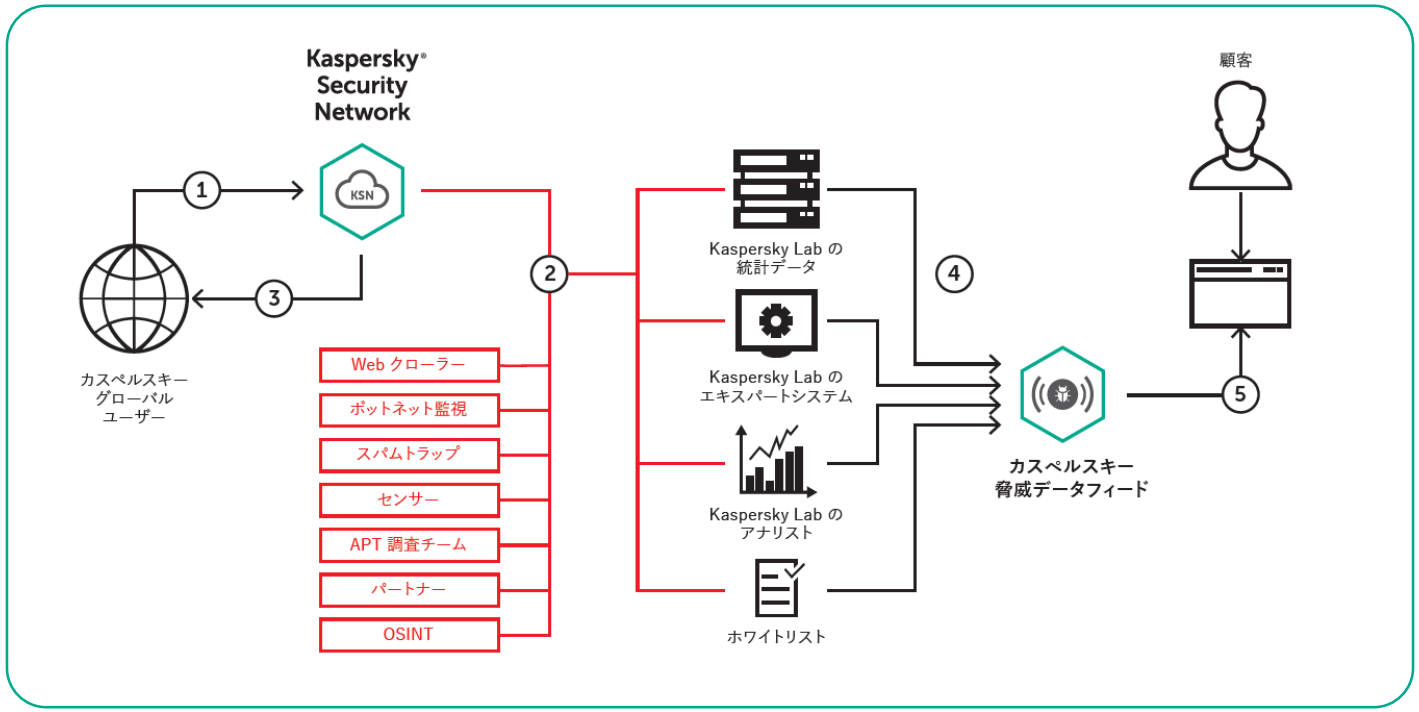
脅威インテリジェンスのソース

Kaspersky
Threat Data Feeds

高品質なサービスを提供するための取り組み

・脅威インテリジェンスは、Kaspersky Security Network（KSN）、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

・収集された情報は、統計分析や 当社のサンドボックス・ヒューリスティックエンジン・マシンラーニングといった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



kaspersky

脅威データフィード構成

Kaspersky
Threat Data Feeds

様々な脅威情報に特化した脅威データフィード

脅威データフィード名	フィードに含まれる情報
Malicious URL Feed	悪意のあるリンクやウェブサイトを含むコンテキストを持つURLマスクのセット
Phishing URL feed	フィッシング・リンクやウェブサイトを含むコンテキストを持つURLマスクのセット
Botnet C&C URL Feed	デスクトップ・ボットネットのC&Cサーバーや関連する悪意のあるオブジェクトを含むURLマスクのセット
Malicious Hash Feed	最も危険で広く普及している新興のマルウェアに対応するコンテキストを持つファイルハッシュのセット
Mobile Malicious Hash Feed	AndroidおよびiPhoneのモバイルプラットフォームに感染する悪意のあるオブジェクトを検出するために対応するコンテキストを持つファイルハッシュのセット
Mobile Botnet C&C URL Feed	モバイル・ボットネットのC&Cサーバのコンテキストを含むURLのセット
IP Reputation Feed	疑わしいホストや悪意のあるホストのさまざまなカテゴリを示すコンテキストを持つIPアドレスのセット
Ransomware URL feed	ランサムウェアのリンクやWebサイトを含むURL、ドメイン、ホストのセット
IoT URL Data Feed	IoTデバイスに感染するマルウェアのホスティングに使用されるサイトのコンテキストを含むURLセット・マルウェアのハッシュ値も提供
Vulnerability Data Feed	関連するサイバー脅威情報(脆弱なアプリケーション/エクスプロイトのハッシュ・タイムスタンプ・CVE・パッチなど)を含むセキュリティ脆弱性のセット

kaspersky

脅威データフィード構成

Kaspersky
Threat Data Feeds

様々な脅威情報に特化した脅威データフィード

脅威データフィード名	フィードに含まれる情報
pDNS Data Feed	実用的なコンテキストで強化された対応するIPアドレスへのドメインのDNS解決の結果を含むレコードのセット
ICS Hashes Feed	産業用制御システムのインフラストラクチャ(ICS)を攻撃するために使用される悪意のあるオブジェクトに対応するコンテキストを持つファイル・ハッシュのセット
ICS Vulnerability Feed	産業用制御システム(ICS)およびICSネットワークに統合された一般的なITシステムにおけるセキュリティ脆弱性の集合体
Suricata Rules Data Feed	APT、ボットネットC&C、ランサムウェアなどさまざまな脅威を検出するSuricata IDSルール
Cloud Access Security Broker Feed	クラウドサービスのドメインをカバーするマスクのセット
New Open Source Software Threats Data Feed	脆弱性が存在するオープンソースソフトウェアのバージョン・ダウンロード元、受ける可能性のある攻撃手法のセット
New Industrial OVAL Data Feed for Windows	産業用制御システムに利用されるソフトウェアに存在する脆弱性を検出するための脅威データフィード

kaspersky

各脅威データフィードの特徴

Kaspersky
Threat Data Feeds

各脅威データフィードに含まれるIoCと実用的なコンテキスト情報

Malicious URL Feed:

悪意のあるドメイン、IPアドレス、Kasperskyの検知名、関連するオブジェクトのハッシュ値など

Phishing URL Feed:

悪意のあるドメイン、IPアドレス、フィッシングキット、盗まれるデータタイプ、標的の組織、攻撃タイプなど

Botnet C&C URL Feed:

悪意のあるドメイン、IPアドレス、Kasperskyの検知名、C&Cサーバーと通信するボットのハッシュ値など

Malicious Hash Feed:

悪意のあるオブジェクトのハッシュ値(MD5、SHA-1、SHA-256)、ホストされているサーバーのIPアドレス、URLなど

Mobile Malicious Hash Feed:

悪意のあるオブジェクトのハッシュ値(MD5、SHA-256)、流行度、Kasperskyの検知名、遭遇が確認された地域など

Mobile Botnet C&C URL Feed:

悪意のあるドメイン、IPアドレス、Kasperskyの検知名、関連するオブジェクトのハッシュ値など

kaspersky

各脅威データフィードの特徴

Kaspersky
Threat Data Feeds

各脅威データフィードに含まれるIoCと実用的なコンテキスト情報

IP Reputation Feed：

悪意のあるIPアドレスおよび位置情報、脅威スコア、流行度、遭遇が確認された地域、関連するオブジェクトのハッシュ値など

Ransomware URL Feed:

悪意のあるドメイン、IPアドレス、流行度、遭遇が確認された地域、対象のランサムウェアに関連するオブジェクトのハッシュ値など

IoT URL Data Feed

悪意のあるドメイン、プロトコル、ポート番号、遭遇が確認された地域、関連するオブジェクトのハッシュ値など

Vulnerability Data Feed

ベンダー名、影響のある製品およびバージョン、解決方法、修正用パッチのバージョン・リリース日・ダウンロード先、CVE番号など

pDNS Data Feed

レコードに関連するFQDN、レコードタイプ（A/NS/CNAMEなど）、過去1時間に解決された回数など

ICS Hashes Feed

悪意のあるオブジェクトのハッシュ値（MD5、SHA-1、SHA-256）、ホストされているサーバーのIPアドレス、URLなど

kaspersky

各脅威データフィードの特徴

Kaspersky
Threat Data Feeds

各脅威データフィードに含まれるIoCと実用的なコンテキスト情報

ICS Vulnerability Feed

ベンダー名、影響のある製品およびバージョン、解決方法、修正用パッチのバージョン・リリース日・ダウンロード先、CVE番号など

Suricata Rules Data Feed

APT / Botnet C&C / Crimeware / DNSトンネリング / ランサムウェア / エクスプロイト / ハックツール / マイナーなどの脅威をブロックするためのルール

Cloud Access Security Broker Feed

URL、サービス名、サービスのカテゴリ(ファイル共有/メッセンジャー/ソーシャルメディア/メール)など

New Open Source Software Threat Data Feed

脆弱性が存在するオープンソースソフトウェア名・バージョンおよびダウンロード元/受ける可能性のある攻撃手法/推奨バージョンなど

New Industrial OVAL Data Feed for Windows

脆弱性が存在するソフトウェア・製品名およびバージョン / CVSS / 脆弱性に関連するNVD(NISTが運営する脆弱性データベース)のリンクなど

kaspersky

マスク

Kaspersky
Threat Data Feeds

精度の高い検知を実現するためのマッチングルール

・URLベースの脅威データフィードにはマッチングルールの値が入力されるフィールド”mask”が含まれます。
maskの値ごとにマッチングすべき対象が異なり、このマッチングルールによって誤検知の少ない精度の高い検知を実現します。

<マッチングルール例>

-ルール1：第2レベルドメイン

レコードサンプル：domain.com

検知対象：ドメイン自体、すべてのサブドメインとそのすべてのコンテンツ

検知対象例：domain.com/folder、www2.a.domain.com、www2.a.domain.com/index.php

検知対象外：どのレベルのドメインでもない、部分文字列としてドメインを含むリンク

検知対象外例：google.com/search?q=a.domain.com/1.exe

-ルール2：フォルダー/ファイルを含むドメイン

レコードサンプル： domain.com/script.php

検知対象：マスクに正確に一致するリンクと、その後に「/」記号（スラッシュ）、ファイルまたはフォルダーの名前が続くリンク

検知対象例：domain.com/script.php、domain.com/script.php/subfolder、domain.com/script.php/file.exe

検知対象外：サブドメインのコンテンツや他のフォルダーのコンテンツ

検知対象外例：domain.com/script.php?p1=1&p2=2、www2.domain.com/script.php

kaspersky

マスク：処理方法

Kaspersky
Threat Data Feeds

精度の高い検知を実現するためのマッチングルール

・URLベースの脅威データフィードを使用する場合、maskの値によってマッチングルールが異なるため、maskの値を考慮した照合を行う必要があります。

<mask処理方法パターン>

-パターン1：脅威データフィードと統合するSIEM側で判定ロジックを設定

->マッチングルールの詳細についてはカスペルスキーが提供する「脅威データフィード導入ガイド」をご参照ください。

-パターン2：Kaspersky CyberTraceを利用 （12ページ参照）

->CyberTraceはマスク処理を自動で行うため、SIEM側での判定ロジックの設定が必要ありません。

-パターン3：そのまま照合に利用可能なIOCを提供するExact Feedを使用（9ページ参照）

kaspersky

Exact Feed

Kaspersky
Threat Data Feeds

マスク(マッチングルール)の考慮が必要ないDataFeed

・Kasperskyから提供されるURLベースの脅威データフィードはマスク(マッチングルール)を考慮する必要がありますが、SIEM、FW、SWGやマスク判定のロジックの実装が困難なプラットフォームにもData Feedを統合できるようにマスクを考慮する必要がなく、そのまま照合に利用可能な状態でIOCを提供する脅威データフィードも提供しています。

・Exact Feedには従来のコンテキスト情報に加え、URL・ドメイン自体やドメイン内の特定のコンテンツ、オブジェクトといった情報が含まれます。

脅威データフィード名	フィードに含まれる情報
Malicious URL Exact Feed	悪意のあるリンクやウェブサイトを含むコンテキストを持つURLマスクのセット
Phishing URL Exact feed	フィッシング・リンクやウェブサイトを含むコンテキストを持つURLマスクのセット
Botnet C&C URL Exact Feed	デスクトップ・ボットネットのC&Cサーバーや関連する悪意のあるオブジェクトを含むURLマスクのセット

kaspersky

APT Data Feeds

Kaspersky
Threat Data Feeds

・APT Data FeedsはAPT Intelligence ReportingのマスターIoCファイルの情報から生成されます。

・APT Data Feedsには、4つの脅威データフィードが含まれます。

脅威データフィード名	フィードに含まれる情報
APT URL Feed	悪意のあるAPTキャンペーンで使用されるインフラストラクチャの一部であるドメインのセット
APT IP Feed	悪意のあるAPTキャンペーンで使用されるインフラストラクチャの一部であるIPアドレスのセット
APT Hash Feed	APTアクターがAPTキャンペーンを行う際に使用する悪意のあるアーティファクトをカバーするハッシュのセット
APT YARA Feed	APTアクターが使用するマルウェアファミリーを検出し、ハントするためのYARAルールのセット

・各脅威データフィードに含まれる情報は以下の通りです。

APT URL Feed:

APTキャンペーンに関連するURL、APT攻撃の影響を受ける国および業界、APT攻撃を実行する攻撃グループなど

APT IP Feed:

APTキャンペーンに関連するIPアドレス、APT攻撃の影響を受ける国および業界、APT攻撃を実行する攻撃グループなど

APT Hash Feed:

APTキャンペーンに関連する悪意のあるオブジェクトのMD5ハッシュ値、APT攻撃の影響を受ける国および業界、APT攻撃を実行する攻撃グループなど

kaspersky

New Crimeware Feeds

Kaspersky
Threat Data Feeds

・Crimeware FeedsはCrimeware Intelligence ReportingのマスターIoCファイルの情報から生成されます。

・Crimeware Feedsには、3つの脅威データフィードが含まれます。

脅威データフィード名	フィードに含まれる情報
Crimeware URL Feed	クライムウェアキャンペーン(主に金銭を目的としたサイバー攻撃)で使用されるインフラストラクチャの一部であるドメインのセット
Crimeware Hash Feed	クライムウェアキャンペーンで使用する悪意のあるアーティファクトをカバーするハッシュのセット
Crimeware YARA Feed	クライムウェアキャンペーンで使用するマルウェアファミリーを検出し、ハントするためのYARAルールのセット

・各脅威データフィードに含まれる情報は以下の通りです。

Crimeware URL Feed:

クライムウェアキャンペーンに関連するURL、攻撃の影響を受ける国および業界、クライムウェア攻撃を実行する攻撃グループなど

Crimeware Hash Feed:

クライムウェアキャンペーンに関連する悪意のあるオブジェクトのMD5ハッシュ値、攻撃の影響を受ける国および業界、
クライムウェア攻撃を実行する攻撃グループなど

kaspersky

提供方法

提供方法

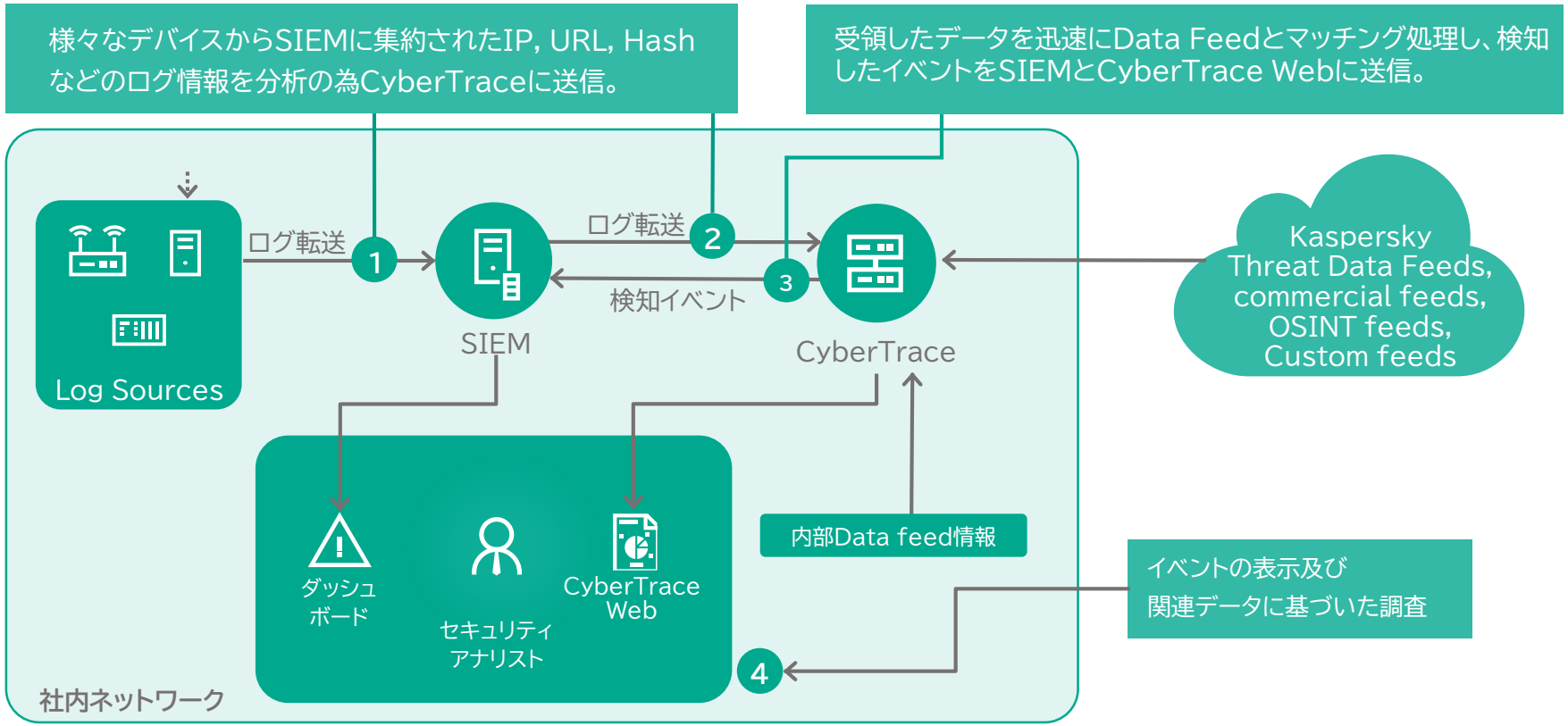
Kaspersky
Threat Data Feeds

提供方法1：脅威インテリジェンス融合・分析ツール「Kaspersky CyberTrace」を導入

CyberTraceを導入することでお客様環境のSIEMが集約したログとThreat Data Feedsの脅威情報を自動的に照合し、リアルタイムな「状況認識」を実現し、運用者のインシデント対応の負担を軽減することが可能です。

ログの解析・照合はCyberTrace内部で処理される為、お客様SIEMへ負荷を増やすことなく導入が可能です。

（詳細はKaspersky CyberTraceの資料をご参照ください）



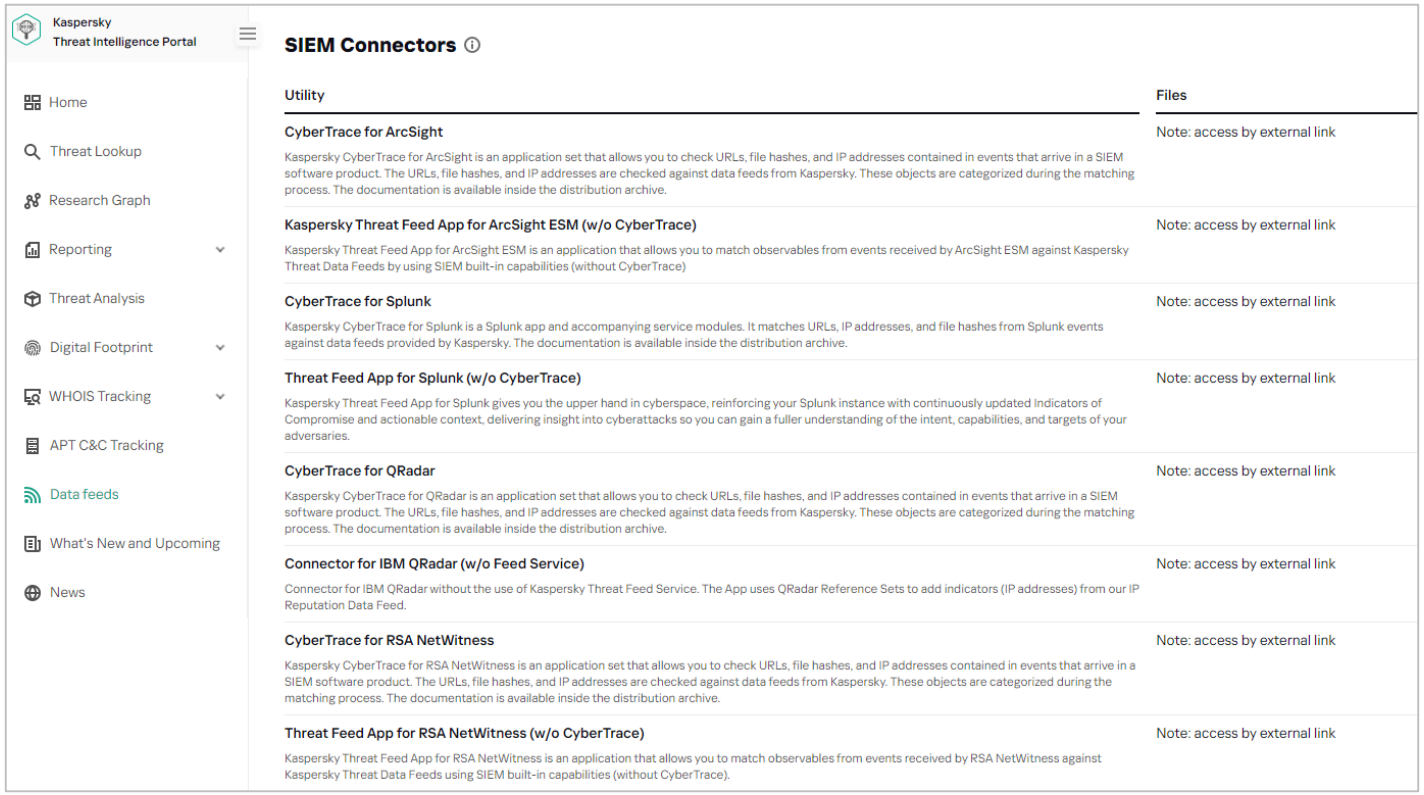
kaspersky

提供方法

Kaspersky
Threat Data Feeds

提供方法2：SIEM連携用のアプリケーションを使用

Kaspersky提供のアプリケーションを使用することで、お客様環境のSIEMへ直接データフィードを取り込み可能です。
（アプリケーションはポータルサイト「Kaspersky Threat Intelligence Portal」からダウンロード可能）



Kaspersky Threat Intelligence Portal内　Threat Data Feeds画面

kaspersky

提供方法

Kaspersky
Threat Data Feeds

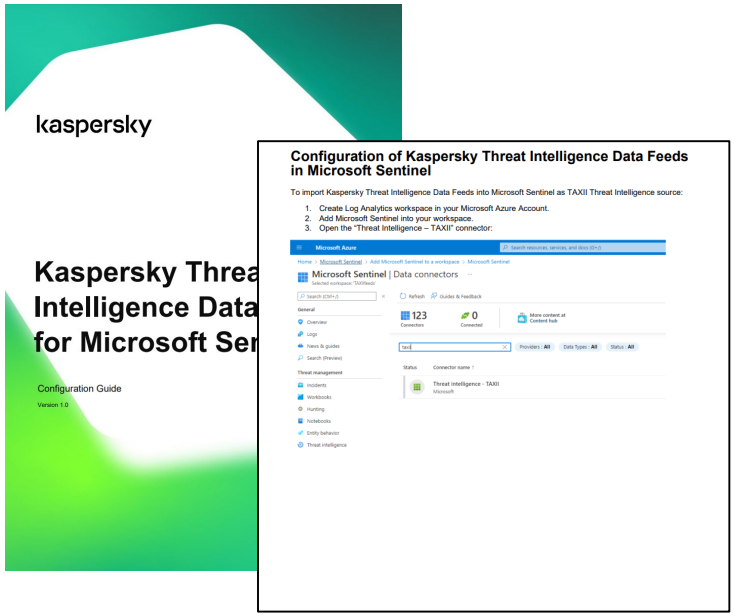
提供方法3：TAXIIサービスを仲介したデータフィードの取得

・TAXIIプロトロルを使用して、STIX形式の脅威データフィードのダウンロードが可能です。（STIX　1.0/1.1、2.0、2.1に対応）

・脅威データフィードはすべての情報を提供する通常のデータフィードとブロック対象のインジケーターのみ記載された軽量版の2種類から選択可能です。

New

・TAXIIデータコネクタを使用して、Microsoft SentinelでKaspersky Threat Data Feedsの脅威インテリジェンスサービスが取得可能になりました。



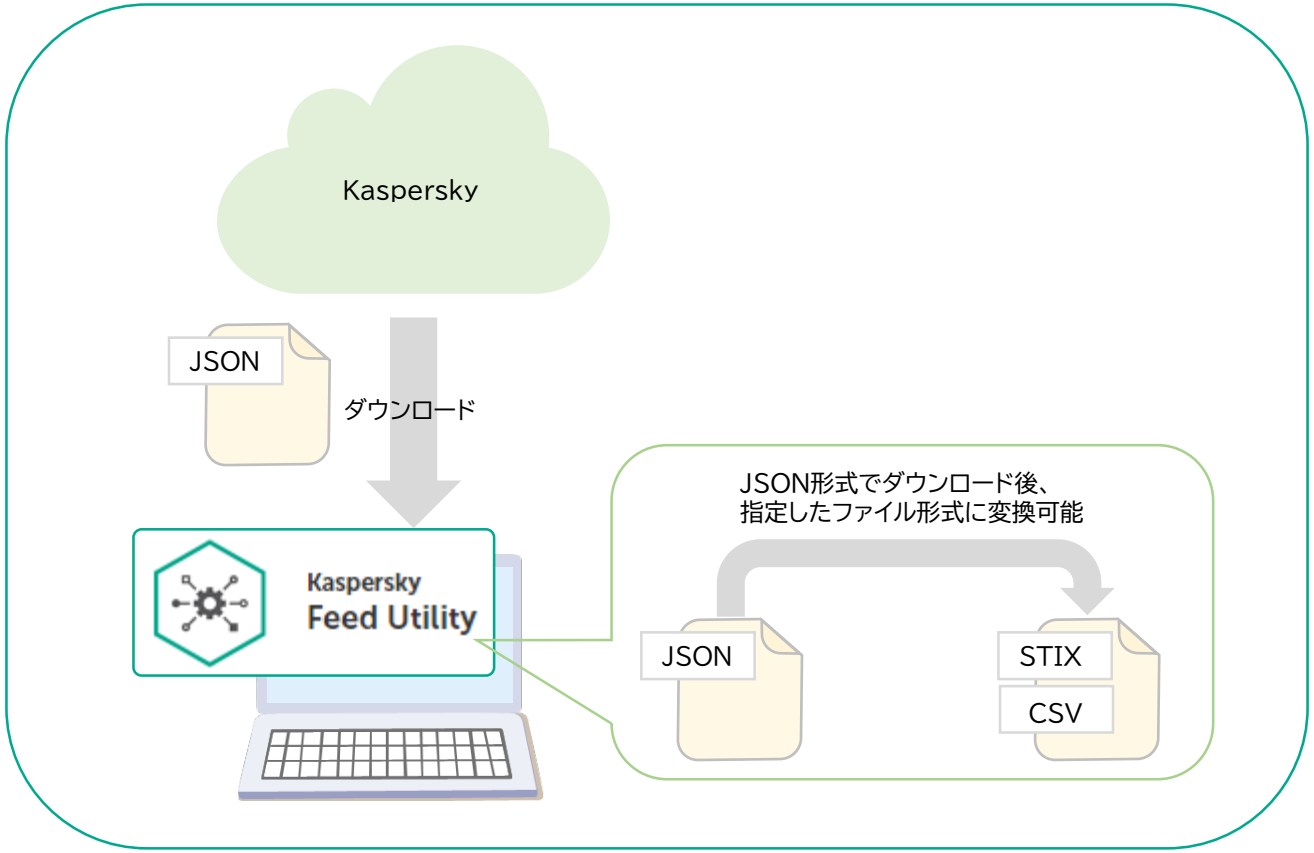
kaspersky

提供方法

Kaspersky
Threat Data Feeds

提供方法4：データフィードダウンロード用ツール「Kaspersky Feed Utility」を使用

本ツールを使用することでファイル形式の変換（JSON形式→STIX/OpenIOC/CSV/TXTへの変換が可能）や、
条件を満たすオブジェクトのみをダウンロードするようフィルター設定をすることが可能です。



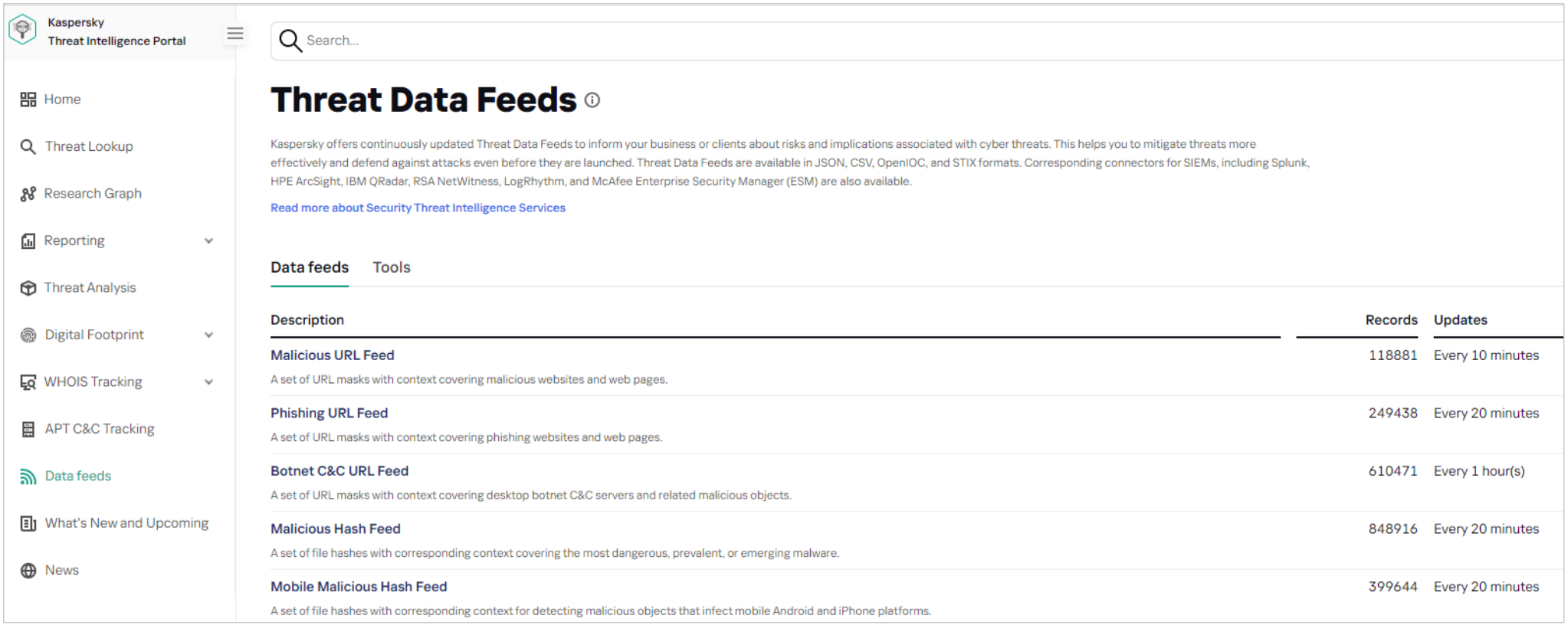
kaspersky

提供方法

Kaspersky
Threat Data Feeds

提供方法5：脅威インテリジェンスサービス用ポータル「Kaspersky Threat Intelligence Portal」から直接ダウンロード

ダウンロードした脅威情報をお客様環境のUTMアプライアンスやファイアウォール等のネットワーク機器のポリシーに登録することで悪意のあるURLや感染端末のC&Cサーバとの通信をブロック可能です。



Kaspersky Threat Intelligence Portal内 Threat Data Feeds画面

活用例

活用例

Kaspersky
Threat Data Feeds

詳細情報を基に効果の高いインシデント調査を実施

① インターネットアクセスログと脅威データフィードを照合

（対象：Malicious URL Feed、Phishing URL Feed Botnet C&C URL Feed、Ransomware URL Feed、
IP Reputation Feed、CyberTrace）

-プロキシやネットワーク機器で取得した、従業員がアクセスしたWebログと上記URL系脅威データフィードを照合

-SIEMでインターネットアクセスログを収集している場合、CyberTraceとSIEMを統合することで効率の良い照合が可能

→別サービス**「Threat Lookup」**で検知したURLを検索することで、URLにアクセスしたことでダウンロードされる可能性のあるファイルのハッシュ値などの詳細情報を取得、さらに効率の良いインシデント調査を実現

② DNSブロッキングに脅威データフィードを活用

（対象：Malicious URL Feed、Phishing URL Feed Botnet C&C URL Feed、Ransomware URL Feed）

-DNSキャッシュサーバーと上記URL系脅威データフィードを照合し、怪しいWebページへのアクセスをブロック

kaspersky

活用例

Kaspersky
Threat Data Feeds

詳細情報を基に効果の高いインシデント調査を実施

③ ファイアウォールのログの分析に脅威データフィードを活用

（対象：IP Reputation Feed、Botnet C&C URL Feed）

-Webサーバーのログに記録されるTor exitノードからのアクセスの検知

-Webサーバーから送信される悪意のあるC&Cサーバーへのアウトバウンドトラフィックの検知

→Botnet C&C URL Feedに含まれる地理情報や流行度、関連するファイルのハッシュ値といったコンテキスト情報を活用してボットネットの活動を特定

④SIEMと脅威データフィードを統合し、セキュリティを強化

（対象：全ての脅威データフィード、CyberTrace）

-SMTPログとIP Reputation Feedを照合することで、事業や顧客のいない国にある信頼できないIPアドレスからのトラフィックを検知

-EDRで収集したファイルのハッシュ値とMalicious Hashes Feedを照合し、エンドポイントに存在する悪意のあるオブジェクトを検知

→ Malicious Hashes Feedに含まれるIPアドレス、URLを活用してその他端末で怪しい通信が発生していないかをさらに調査

→検知したオブジェクトを別サービス「**Threat Lookup**」で検索することで、該当のオブジェクトの潜伏先やダウンロード元、アクセス先といった情報が確認可能（＝インシデント対応の効率化を支援）

kaspersky

活用例

Kaspersky
Threat Data Feeds

詳細情報を基に効果の高いインシデント調査を実施

⑤パッシブDNS情報の活用

（対象：pDNS Data Feed）

-DNS名前解決の履歴を蓄積したデータセットであるパッシブDNSの情報を活用することで、以下のような脅威ハンティングが可能

1.攻撃時のDNS情報を参照した調査：

攻撃者は調査を困難にするため、1つのグローバルIPに多数のドメインを割り当て、頻繁に切り替えるように細工

->検知時点と調査時点では攻撃元IPに紐づくドメインが異なるため、正しく調査することが出来ない

パッシブDNSに蓄積された情報なら攻撃時点のDNS情報を参照することが出来るため、検知時点の性格なドメイン情報を取得して調査・分析することが可能

2.悪意のあるアクティビティの防止：

ネームサーバーが悪意のあるものとして判定されている場合、pDNS Data Feedの情報からネームサーバーによってホストされているゾーンやドメイン名の識別が可能

⑥トラフィックの分類に脅威データフィードを活用

（対象：CASB（Cloud Access Security Broker）Feed）

-トラフィックのURLとCASB Feedのインジケーターを照合することで、どのカテゴリのどのクラウドサービスがアドレス指定されているか分類可能

kaspersky

kaspersky