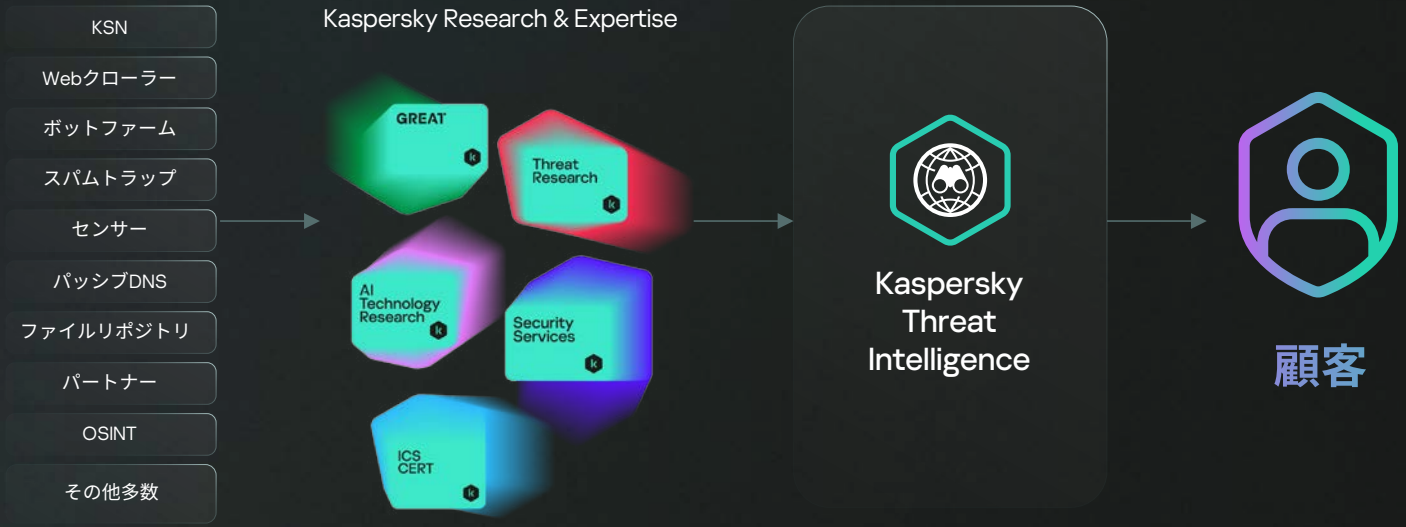
Kaspersky Threat Intelligence

攻撃者の機先を制する

kaspersky

Kaspersky Threat Intelligenceの情報源



Kaspersky Threat Intelligenceは、世界トップクラスのアナリストやリサーチャーが収集した多岐にわたる情報へのアクセスを可能にし、今日のサイバー脅威に組織が効果的に対処できるよう支援します。

世界各国の脅威に関する唯一無二の専門知識と知見に基づく脅威インテリジェンス

いずれのセンターも、Kaspersky のソリューションとサービスに貢献しています

● 脅威リサーチ　● インシデント調査

Kaspersky グローバル調査分析チーム

- 複雑な脅威の調査：APT、サイバースパイ活動、世界的規模のサイバー脅威被害など。
- 未来志向のセキュリティ技術
- 巧妙な金融サイバー犯罪に関する調査

Kaspersky 脅威リサーチ

- マルウェア対策リサーチ
- コンテンツフィルタリングリサーチ
- SSDLC（セキュアソフトウェア開発ライフサイクル）とセキュア・バイ・デザインに基づく方法論

Kaspersky AI技術リサーチ

- AIのサイバーセキュリティ
- 生成AIのリサーチ
- AIを活用した脅威検知 / ソリューション

Kaspersky セキュリティサービス

- MDR
- インシデントレスポンス
- セキュリティ評価
- SOCコンサルティング
- デジタルフットプリントインテリジェンス

Kaspersky ICS CERT

- 重要インフラの脅威分析
- ICS脆弱性に関するリサーチと評価
- 技術関連団体、分析、標準

Kaspersky Threat Intelligenceの注目すべきポイント

当社は、サイバー脅威の調査における高度な知識、豊富な経験と、サイバーセキュリティのあらゆる側面に関する他社にはない見識を兼ね備えています。その結果、当社は世界各地の企業から信頼されるパートナー、およびインターポールや数多くのCERT組織から高く評価される提携先としての地位を確立しています。

世界各地の脅威への対応力と、多数の攻撃が発生する地域における脅威のリサーチを長年継続してきた経験

Kasperskyのエキスパートによる継続的な貢献

IT/OTセグメント向けの脅威インテリジェンス

Kaspersky Threat Intelligenceの注目すべきポイント

当社が把握、監視している脅威アクターや活動の数：

300以上

脅威アクター

500以上

キャンペーン

200以上

年間に発行する非公開レポート

170000以上

レポートに関連するIoC

2500以上

レポートに関連するYARAルール

脅威インテリジェンスのデータレベル

戦術性

セキュリティ運用とインシデントレスポンスをサポートする、低レベルで有効期間が極めて短い情報。戦術的インテリジェンスの例としては、新たに発見された攻撃行為に関するIOCが挙げられます。

ロール：

SOCアナリスト

システム：

SIEM　NGFW　SOAR　IPS　IDS

プロセス：

脅威ハンティング　監視

実用性

このレベルには通常、キャンペーンや高次のTTPに関するデータが含まれます。特定のアクターの属性、敵対者の能力や意図に関する情報が含まれる場合があります。

ロール：

SOC L3アナリスト　DFIRアナリスト　IRアナリスト

システム：

SIEM　NTA　TIP　EDR / XDR

プロセス：

インシデントレスポンス　脅威ハンティング

戦略性

このレベルは、リスク評価、リソース配分、組織戦略に関する重大な意思決定を行う経営幹部や取締役会をサポートします。この情報には、トレンド、アクターの動機、およびその分類が含まれます。

ロール：

CISO　CTO　CIO　CEO

プロセス：

IS戦略の構築　アウェアネスの喚起

脅威インテリジェンスの配信形式

機械可読型の脅威インテリジェンス

Kaspersky Threat Data Feeds

30種類以上の脅威データフィードは、多様なニーズに焦点を当てています。ITとOTの双方をカバーし、TIプラットフォームに対応しています

対人可読型の脅威インテリジェンス

Kaspersky Threat Intelligence Portal

ITおよびOT環境向けのKaspersky Threat Intelligenceポートフォリオの主要部分。Kaspersky Threat Intelligence Portal経由で一元的にアクセス可能です。

脅威インテリジェンスをエキスパートがサポート

Kaspersky Takedown Service

Kaspersky Ask the Analyst

経験豊富なエキスパートによる専門的なガイダンス

Kaspersky Threat Intelligence

機械可読型の
脅威インテリジェンス

- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

脅威インテリジェンスを
エキスパートがサポート

- Kaspersky Takedown Service
- Kaspersky Ask the Analyst

Kaspersky
Threat Intelligence

- 戦術性
- 実用性
- 戦略性

○ これらが利用可能なポータル

Kaspersky
Threat Intelligence
Portal

対人可読型の
脅威インテリジェンス

- Kaspersky Threat Lookup
- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Analysis
  - Sandbox
  - Attribution
  - Similarity
- Kaspersky Threat Intelligence Reporting
  - APT
  - クライムウェア
  - ICS
- Kaspersky Threat Infrastructure Tracking

Kaspersky Threat Data Feeds

複雑な設定が不要な30種類以上の脅威データフィードを多様なタスク向けに用意

組織のニーズに合わせた脅威データフィードを利用可能。

- 戦術的なTI
- 実用的なTI

一般的な脅威データフィード

- 悪意のあるURL
- ランサムウェアURL
- フィッシングURL
- ボットネットC&C URL
- モバイルボットネットC&C URL
- 悪意のあるハッシュ
- 悪意のあるハッシュ（モバイル）
- IPレピュテーション
- IoTのURL
- ICSのハッシュ
- APTのハッシュ
- APTのIP
- APTのURL
- クライムウェアのハッシュ
- クライムウェアのURL

Kaspersky Threat Data Feeds

SIEM、SOAR/IRP、TIP、EDR/XDR

TIプラットフォーム

各種の脅威インテリジェンスフィードをすぐに運用可能にし、SIEMのワークロードを軽減

Kaspersky CyberTrace

特定の脅威データフィード

Kaspersky Network Security データフィード	Suricata ルールフィード	Sigmaルール データフィード	YARAルール データフィード	脆弱性情報のフィード	オープンソースソフトウェアの脅威データフィード
NGFW	IDS / IPS	SIEM / EDR	YARA-スキャナー	SBOM /CMDB	OSA / CSA / ASOC

Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligenceへのアクセスを、統一されたユーザーインターフェイスとAPIで一元化して提供します。複数のサービスが連携し、相互のリッチ化と強化を実現しています。Kasperskyのサイバー脅威に関する専門知識と知識をすべて1か所に集約することで、独自のデータ処理および標準化技術を使用して特定の組織に関連する脅威を監視することが可能になります。また、マルウェアサンプルとその属性を調査できるようになります。

- 戦術的なTI
- 実用的なTI
- 戦略的なTI

Kaspersky Threat Intelligence Portal（無料版）

Kaspersky Threat Intelligence Portal 上の脅威の状況

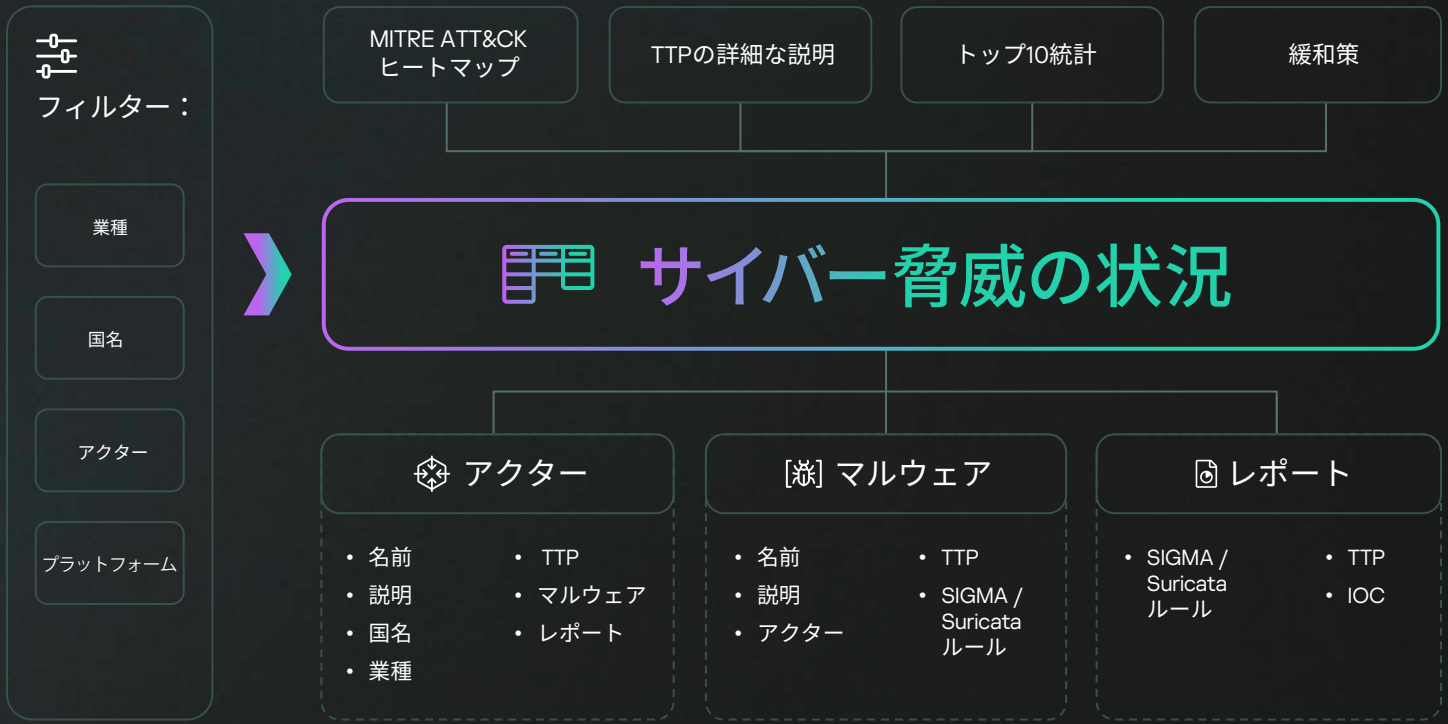
地域および業界に特有の脅威インテリジェンスにより、組織が直面する脅威を正確に把握

- MITRE ATT&CKのアラインメント
- Kasperskyの継続的なリサーチに基づくリアルタイムでのアップデート
- 敵対者とソフトウェアのプロファイルを自動入力
- 検知ルールのリポジトリ

400,000件以上の

当社が毎日検知する悪意のあるファイル

脅威の状況 – その仕組み


フィルター：
業種
国名
アクター
プラットフォーム
MITRE ATT&CK ヒートマップ
TTPの詳細な説明
トップ10統計
緩和策
サイバー脅威の状況
アクター
名前
説明
国名
業種
TTP
マルウェア
レポート
マルウェア
名前
説明
アクター
TTP
SIGMA / Suricata ルール
レポート
SIGMA / Suricata ルール
TTP
IOC

Kaspersky Threat Intelligence をエキスパートがサポート

Kaspersky Ask the Analyst

- 実用的なTI
- 戦略的なTI

Kaspersky Ask the Analystは、当社の脅威インテリジェンスのポートフォリオを拡張するサービスです。貴社が直面しているか関心がある特定の脅威に関するガイダンスや知見をリクエストすることができます。

案件ごとにKaspersky の主要リサーチャーグループへのアクセスを可能にし、問題解決をサポートします。このサ ービスでは、エキスパート間の総合的な情報交換により、当社独自の知識とリソースを活用して、貴社の 既 存の対応能力を強力に補強します。

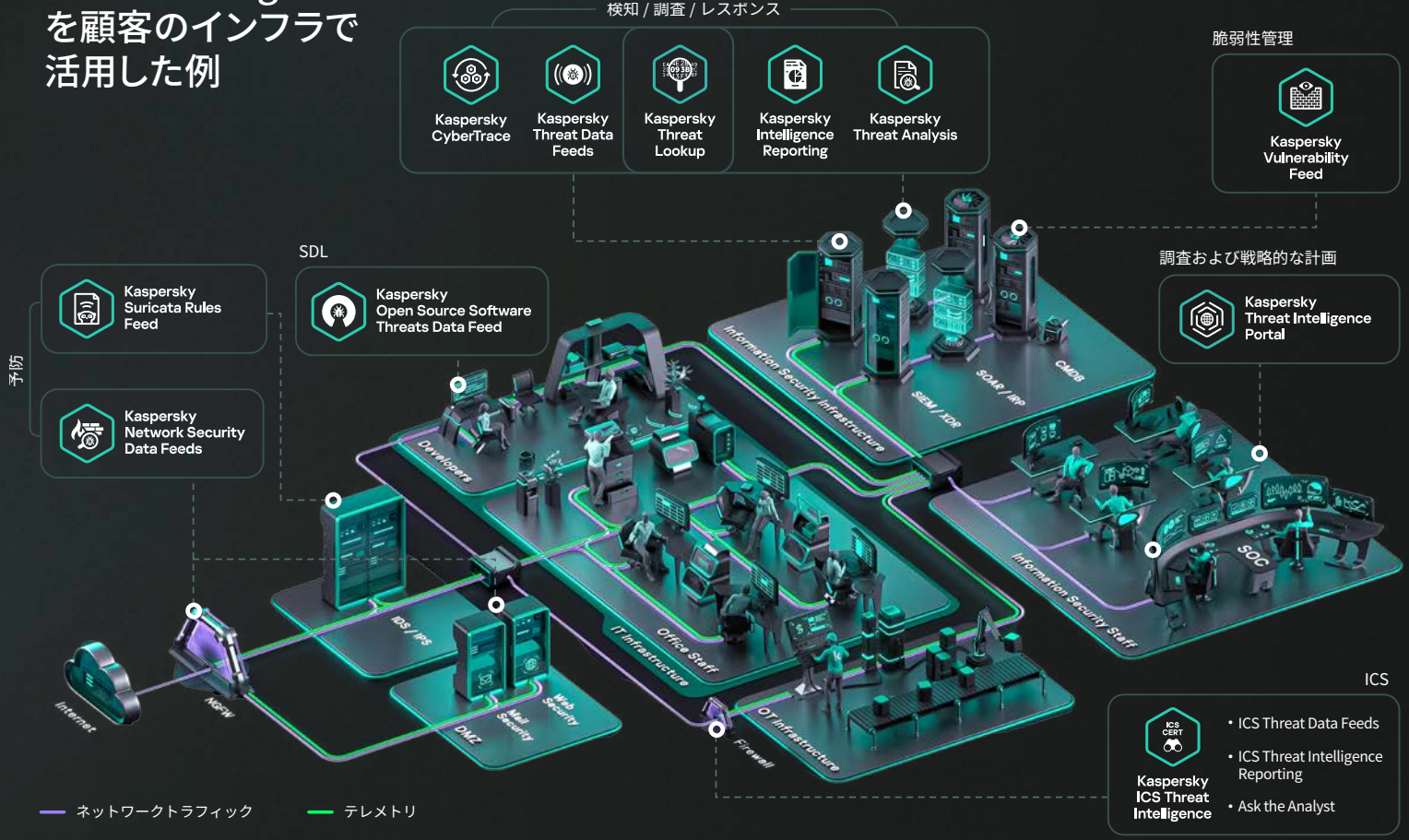
Kaspersky Takedown Service

- 実用的なTI

Kaspersky Takedown Service は、ブランドやビジネスが損害を受ける前に、悪意のあるフィッシングドメインがもたらす脅威による影響をいち早く緩和します。当社はドメインの分析において豊富な経験を有しており、悪意のあるドメインであることの証明に必要となるすべての証拠を収集する方法を熟知しています。テイクダウン管理は当社にお任せください。

このサービスは、国際組織および国や地域の法執行機関と協力して、世界中で提供されています。

Kaspersky Threat Intelligence を顧客のインフラで活用した例



Kaspersky Threat Intelligence Industrial により提供されるサービス

機械可読型の脅威インテリジェンス

Kaspersky Threat Data Feeds

産業用サイバーセキュリティの脅威と脆弱性に関する機械可読のデータ

Kaspersky ICS Hashes Data Feed
Kaspersky ICS Vulnerability Data Feed
Kaspersky ICS Vulnerability Data Feed（OVAL 形式）

対人可読型の脅威インテリジェンス

Kaspersky ICS Intelligence Reporting

産業用サイバーセキュリティの脅威と脆弱性に関する定期的な公開情報を、Kaspersky Threat Intelligence Portalで閲覧できます

脅威インテリジェンスとエキスパートのサポート

Kaspersky Ask the Analyst

産業用サイバーセキュリティの脅威や脆弱性、脅威の統計、脅威の状況、業界標準などに関して、Kaspersky ICS CERTのエキスパートに直接相談し、個別の状況に合わせたアドバイスを得ることができます

● 戦術性　● 実用的なTI　● 戦略的なTI

Kaspersky Threat Intelligenceを選ぶ理由

トップクラスのTIサービスとして
業界のアナリストに評価されています

Frost & Sullivan、Quadrant Knowledge Solutions、Forrester、IDC など、多種多様かつグローバルな各種調査会社の企業のアナリストにより検証済み。

数多くの信頼性が高い独自の情報源から
信頼性が高いTIを生成

当社のKaspersky Security Networkインフラは、1億個以上のセンサーを200か国に配置して、悪意のあるファイルと正規のファイル、ダークウェブ、継続的なTHとIR活動、Webクローラー、スパムトラップなどに関する最大のレポジトリを包括しています。

IT/OTの専門知識の分野で定評がある
エキスパート

GReATチームやICS-CERTなどの5か所のエキスパートセンターから、200人以上の認定エキスパートが世界中に配置されています。また、20種類以上の言語に対応しています。Kasperskyのエキスパートは、StuxnetやWannaCry、Operation Triangulationなど、最も悪名高い脅威を常に誰よりも早く発見してきました。

世界的な業務展開

当社は、多くの攻撃が開始される地域（ロシア/CIS、中国など）に確固としたビジネス基盤を確立しています。これにより、あらゆる国の組織に対して、精査済みの脅威インテリジェンスを収集、分析、配信するという、他にはない事業上の優位性を有しています。

唯一無二の経験を積み重ねた
マルウェア検知技術

AVベンダーとして最大規模（受賞歴のある製品を最も多く展開）を誇る当社は、独自の脅威検知技術を使用して、毎日何百万もの新しいマルウェアサンプルを処理しています。

他社にはないAPT調査の経験

当社は、数百ものAPTアクターとキャンペーンを追跡し、毎年200件以上の詳細なTI戦略レポートを公表しています。また、70,000件以上のサンプルを含む業界最大のAPTファイルコレクションを所有しています。

AIを活用したTIにより、検知、レスポンス、脅威のレポートを強化

AIと機械学習により、実用的な分析結果の抽出、カスタムレポートの生成、分析の自動化が可能になり、時間とリソースを大幅に節約できます。

堅牢さとセキュリティを兼備したベンダー

当社のインフラは耐障害性と透明性が高く、高水準のSLAと監視機能を実装し、SDLCの方法論を使用して構築しています。また、独立系第三者機関による定期的な評価（SOC 2 Type 2またはISO 27001）も実施されています。

成功事例の公開

私たちの顧客が直面している脅威を申し分のない形で可視化してくれるソリューションです。アラート発生時、何が起きているのか、そこから何を学ぶことができるのか、その全体像を把握するためには、信頼性が高く参照可能な情報と、それに付随するすべてのデータが不可欠です。

Paul Colwell氏
（CyberGuard Technologies）

CyberGuard Technologies

事例を読む

Kasperskyは多くの場合、新種の脅威が出現した時、ソフトウェアメーカーがその存在に気づくよりも先に、その存在を特定しています。

Kasperskyの専門知識は、私たちがまだ知らない陰に潜む新しい脅威について詳しく教えてくれます。単に既出のニュースを再利用して並べ、読んだところで結局何も新しい知見を得られないような、ありがちなサービスとは一線を画しています。

Juan Andres Guerrero Saade氏
リサーチャー（Chronicle Security）

chronicle

事例を読む

Kasperskyのソリューションの機能は予想以上にすばらしいものです。また、私たちが必要とするものに対しても、真摯に向き合う姿勢がありました。製品とその背後で働く人々に対する信頼が得られ、よりセキュアな ネットワークを実現することができました。

Rashid AlNahlawi氏
ITセキュリティコンサルタント
（カタールオリンピック委員会）

قطر
QATAR

事例を読む

Kaspersky Threat Intelligenceが実現するメリット

脅威を事前に特定して防止

Kaspersky Threat Intelligenceにより、最新の脅威や脆弱性に関する情報を常に入手し、攻撃が発生する前に事前対応型の保護対策を講じることができます。

脅威検知の能力を強化

Kaspersky Threat Intelligenceは、最新の脅威インテリジェンスにより既存のセキュリティソリューションを強化し、高度な脅威を検知してブロックする能力を大幅に向上させます。

インシデントレスポンスの改善

Kaspersky Threat Intelligenceは、新たに発生した脅威やセキュリティ侵害インジケーターに関する情報をリアルタイムで提供するため、インシデントへの対応のスピードと効率性が向上します。

デジタルフットプリントの可視化

Kaspersky Threat Intelligenceは、攻撃や侵害に対して脆弱な可能性のある資産を含む、組織のデジタルフットプリントを総合的に可視化します。

社内の専門知識をリッチ化

Kasperskyのエキスパートチームは、業界で最も経験豊富で尊敬を集めるリサーチャー集団です。その豊富な知識と専門性の高いスキルにより、顧客の情報セキュリティチームを支援します。

規制および標準への準拠

すべての企業は、それぞれの業界における各種の規制や標準に従う必要があります。Kaspersky Threat Intelligenceは、こうした要件の充足を支援し、コンプライアンスをサポートします。

ありがとう
ございました

Kaspersky Threat Intelligence Portal –
最新鋭のサイバーセキュリティナレッジベース

Kaspersky Threat Intelligence Portal

詳細はこちら

デモのご依頼はこちら