Proven
Intelligence.
Guided Defense.

Kaspersky for Security Operations Center

kaspersky

効果的なセキュリティオペレーションセンター（SOC）の実現への課題

企業はより積極的に保護に取り組むようになりましたが、同時に犯罪組織も、企業によるセキュリティの壁を突破するために、さらに巧妙なテクニックを考案し続けています。サイバー攻撃がもたらす極めて高い対価に惹かれ、未発見のセキュリティの不具合を積極的に探して標的にするサイバー犯罪組織は増えるばかりです。多くの企業はこのような環境で、セキュリティ問題の発生時に対処するためのセキュリティオペレーションセンター（SOC）を設立し、迅速な対応を行い、断固とした解決策を打ち出そうとしています。

Kaspersky の 2018 年企業 IT セキュリティリスク調査（Corporate IT Security Risks Survey）での主な調査結果：

- データ侵害コストの増加率は 20 % 超。データ侵害の財務上の影響は、大企業で平均 123 万ドル（2017 年から 24 % 増加）。
- 侵害の発生後のインフラ強化には、大企業で平均 193,000 ドルの費用が発生（2017 年の 132,000 ドルから 46 % 以上増加）。
- 一方、平均的なセキュリティ予算はあらゆる規模の企業で増加。大企業が現在サイバーセキュリティにかける費用は平均 890 万ドル。
- 前年までと比較すると、グローバルな脅威の発生率は上昇傾向：

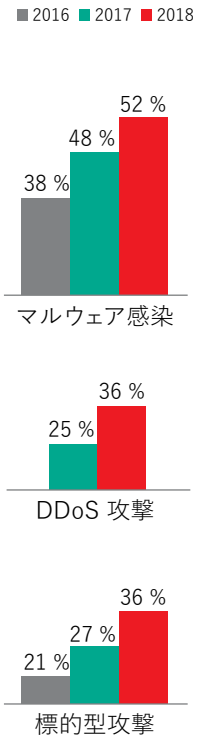


図 1:
グローバルな脅威の遭遇率

SOC は脅威を継続的に監視、分析するため、およびサイバーセキュリティインシデントを軽減、防止するための一元化された部門である

今日のサイバー脅威はかつてないほど大量に発生し、複雑化、深刻化しています。プロセスの文書化や基本的な技術の導入、監視および対応を行う専門チームの設立は、始まりの一歩に過ぎません。変わり続ける脅威の情勢に応じて継続的に適応し発展することを怠れば、SOC の有効性は損なわれるでしょう。

Gartner の「アダプティブ・セキュリティ・アーキテクチャ」モデルによると、現在の脅威を取り巻く環境でサイバー犯罪に正しく立ち向かうためには、SOC チームが効果的に脅威を予測、防止、検知し、脅威に対応できる必要があります。

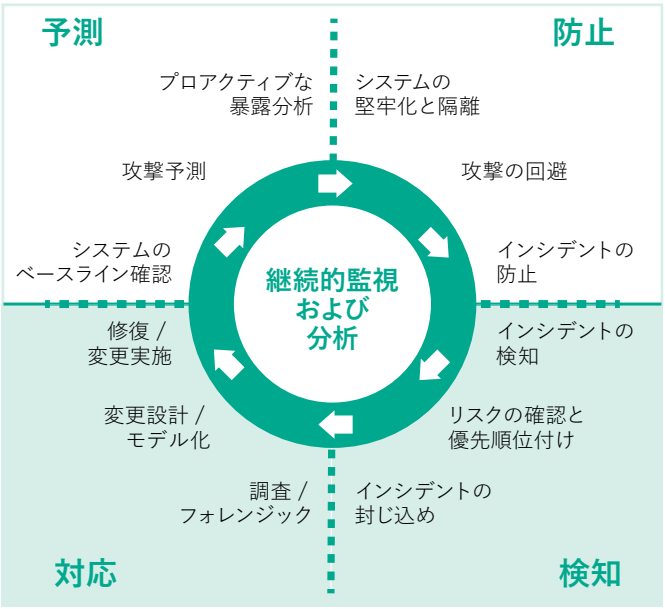
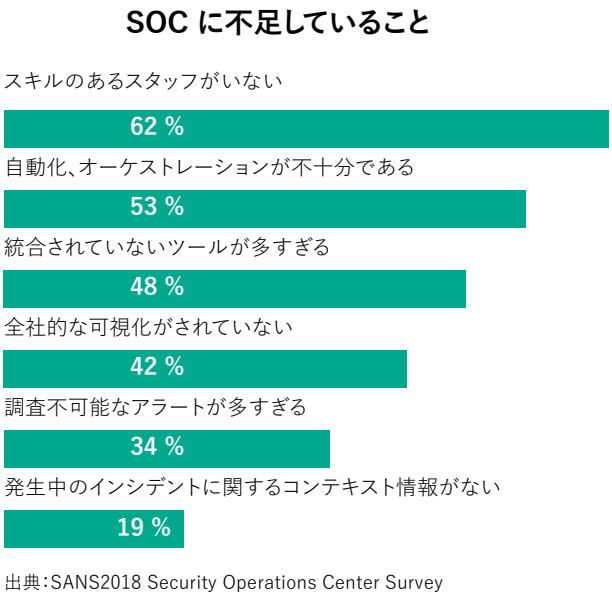


図 2:
Gartner、『Designing an Adaptive Security Architecture for Protection From Advanced Attacks』、2014 年 2 月

「セキュリティオペレーションセンターはインテリジェンスを目指して設計する必要があり、コンテキスト認識およびインテリジェンス主導になるための適応型セキュリティアーキテクチャを採用する必要があります。セキュリティリーダーは、インテリジェンス主導の SOC で最新の脅威から保護するためのツール、プロセス、戦略をどのように利用するかを理解する必要があります」

Gartner、『The Five Characteristics of an Intelligence-Driven Security Operations Center』、2015 年 11 月

社内に SOC を設置した企業を対象とした『SANS 2018 Security Operations Center』調査では、効果的で安定した SOC を実現するまでに数多くの障壁があることがわかっています。



出典：SANS2018 Security Operations Center Survey

図 3：
SOC に不足していること

スキルのあるスタッフがいない

IT セキュリティスタッフが全体的に足りないために、SOC は適切なスキルと経験の不足という特有の問題に直面しています。SOC チームには、マルウェア分析、デジタルフォレンジック、インシデント対応などの分野の知識や経験を有する、高い技能を持つ希少な技術者が必要になります。SIEM（セキュリティ情報およびイベント管理）システムのデータを正しく解釈し、汎用のデータストリームから重要な情報を特定して抽出し、関連付けルールを微調整して、受信した情報にコンテキスト情報を追加できるのが、彼らのような専門家です。 複雑な脅威への対応においてアナリストの専門知識が不十分で、しかもコンテキスト情報を利用したインシデントの適切な範囲設定や調査の仕方について知識が不足していると、具体的な脅威への最適な対応の決定が一層難しくなり、その結果企業に損害をもたらしかねません。

自動化が不十分である

SOC の有効性を損ねる問題は他にもあります。それは自動化が不十分であることです。今日、多くのアナリストが、必要かつ重要だけれども自動化できる定型業務に多くの時間を費やしています。これらの手動タスクを自動化することで、アナリストの貴重な労働時間を短縮して、それにより負荷が減ることで、本当に複雑なインシデントの分析と対応に集中するための時間を増やすことができます。

統合されていない

互いに統合されていない専門ツールがあまりにも多いことが、調査回答者の 48 % にとっての懸念事項になっています。そのために、アナリストは異なるツールやコンソールを切り替えなければならず、時間が無駄になるほか、ミスが起きる可能性も高くなります。追加の保護ツールおよび自動化ツールを導入するときには、それらのツールと既存のソリューションの統合方法やツール同士の統合方法を考慮することが重要です。

アラートが多すぎる

情報セキュリティツールは、SIEM システムに接続する重要なビジネスアプリケーションとともに、毎日確認が必要になる大量のアラートを生成します。しかし、このような情報過多の状態になると、多くのアラートが未処理のままになります。実際、全アラートの約 50 % は調査されていません。一方で、誤検知率は 60 ～ 80 % になる場合もあります。これらの事実から、真の潜在的な脅威を特定しようとすることは、アナリストにとって干し草の山から針を探すようなものに感じられるでしょう。深刻なインシデントが見過ごされるのも無理はありません。

全社的な可視化がされていない

SOC が大量のデータに圧倒され、多くの場合は限定されたシステムを監視対象とすることで範囲を制限しようします。しかし、このアプローチには、インフラの全体像を把握できないという問題があります。これは、「全社的な可視化がされていない」という別の問題につながります。
たとえば、エンドポイントが SIEM システム内のログのソースとして使われることは稀です。その理由の一部として、コストがかかり過ぎることや誤検知数が多くなることが挙げられます。しかし、エンドポイントは攻撃者の主な標的です。ワークステーションやサーバーは、企業 IT インフラへの攻撃の侵入口としてもっとも一般的であり、エンドポイントのデータ（プロセス、プログラム、モジュール、ファイル、自動実行ファイル、ネットワーク接続など）はインシデント調査にとって不可欠なものになります。それに加えて、新しい TLS 1.3 プロトコルの登場により、エンドポイントでのテレメトリ分析の価値が大幅に高まっています。エンドポイントのデータへのアクセスが重要である理由が明確になっているのです。

有効なコンテキスト情報がない

攻撃者の動機、戦術、テクニック、手順を理解しなければ、SOC の技術者が調査対象となるインシデントを適切に優先順位付けできなくなる恐れがあり、そのために技術者がすべての調査を同時に行ったり、決断ができず動きが取れなくなる可能性もあります。インシデントを情報に基づいて適切に優先順位付けしなければ、処理すべきアラートが多すぎて、ただでさえ負担の多い SOC チームへのストレスがさらに増え、業務が非効率になり、対応により長い時間がかかるようになります。その結果、大量のアラートに苦慮することになり、しかも、不正確な調査結果の割合も高くなります。SOC が入手する情報を脅威インテリジェンスのデータと比較することで、インシデントの適切な優先順位付けと効果的な調査に必要となるコンテキスト情報を得ることができます。

主な構成要素

この業界に認められたアプローチを持続していくには、以下の主な構成要素と、明確に定義されたプロセスおよび関連するテクノロジーをともに配備する必要があります：

- **ナレッジマネージメント：**巧妙化する攻撃を阻止し、その対応に成功するには、デジタルフォレンジック、マルウェア分析、インシデント対応について担当者（SOC チームメンバー）が十分に訓練を受けている必要があります。
- **高度な検知、対応技術：**より詳細な分析と迅速なインシデント対応を可能にするため、複雑な脅威や標的型攻撃を想定します。
- **脅威インテリジェンス：**以下のような関連性の高い信頼できるソースから収集した脅威インテリジェンスが、新しい脅威を迅速に検知するために不可欠です：
  - 内部の脅威に関するデータ
  - オープンソースのインテリジェンス（OSINT）
  - 業界固有のコミュニティ（FS-ISAC など）
  - 各業界の CERT
  - プライベートコミュニティ
  - マルウェア対策のグローバルベンダー
  - 脅威インテリジェンス専門プロバイダー
- **脅威ハンティング：**ファイアウォール、IPS/IDS、SIEM などの従来のセキュリティシステムでは検知されない脅威をプロアクティブに検索します。
- **インシデントの調査と対応能力：**損害を抑え、修復コストを削減するために必要です。
- **侵入テストとレッドチーム演習：**改善が不可欠となる脆弱な部分を迅速に特定します。

これらの構成要素のそれぞれが等しく重要で、個別の検討が必要です。

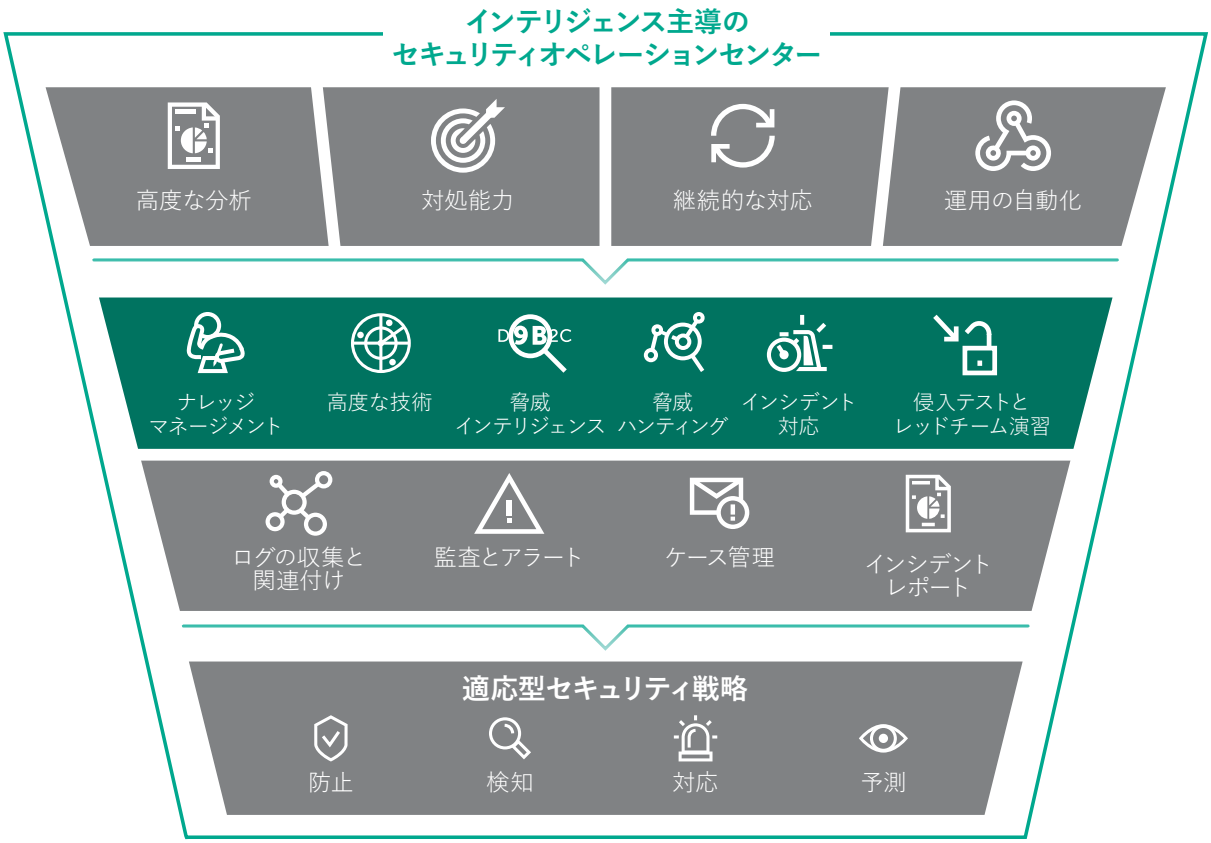


図 4：
SOC の主な構成要素

ナレッジマネージメント

SOC は、大量のデータを分析し、さらなる調査が必要かを識別することのできる、実践的な知識や専門知識を持つ人材プールです。

予算が少なければ、SOC の人材獲得が難しくなります。現在の市場では、十分な訓練を受けたサイバーセキュリティの専門家が不足しているため、採用や雇用のコストが増大しています。

効果的な SOC チームメンバーには、以下の能力が必要です：

- 散らばったデータのかけらから全体像をまとめることのできる探求心
- 高いレベルのストレスに耐えながら集中力を維持できる力
- IT とサイバーセキュリティに関する適切な一般知識（実戦的経験が豊富にあることが好ましい）

外部からの採用でも社内での募集でも、SOC のそれぞれの役割を担う人材を獲得しようとした場合に、求めているスキルを「最初から」持っているチームメンバーを見つけることは簡単ではありません。現在のスキルセットと必要なスキルセットの差を縮めるためだけでなく、変わり続けるセキュリティ技術や常に進化する脅威を取り巻く環境に対処できる知識をチームメンバーが備えるためにも、継続的なトレーニングが不可欠です。

以下の表は、一般的な SOC の役割とその責務について例を示したものです。お客様のサービスポートフォリオと範囲によって、SOC に関連する役割とそのスタッフ数は変わってきます。

小規模な SOC では 1 人のスタッフが複数の役割を担う一方で、大規模な SOC チームでは 1 つの役割を 2 人以上のスタッフで担当する方がよい場合があります。

ロール	説明	説明
	Core	
ティア 1 アナリスト	トリアージ専門技術者	• インシデントの登録と割り当て • セキュリティインシデントの分類、検証、優先順位付け • セキュリティセンサーの正常性の監視（該当する場合） • ティア 2 アナリストの作業に必要となるデータの収集
ティア 2 アナリスト	インシデント対処担当者	• インシデントの調査と対応 • 封じ込めと修復の作業に関する助言 • インシデント対応の調整とサポート • ティア 1 アナリストの作業の定期的レビュー
マルウェアアナリスト	非常に巧妙な脅威へのインシデント対応では、マルウェアサンプルのリバースエンジニアリングやアーティファクトに対する高度なフォレンジック分析が必要になります。 マルウェアのリバースエンジニアリングを実行し、インシデント対応活動のための価値ある結果を生み出すことが、マルウェアアナリストの主な責務です。	• 静的、動的な詳細マルウェア分析 • マルウェアサンプルのリバースエンジニアリング • コンピューターインシデントおよび標的型攻撃の調査への参加 • IOC の収集
デジタルフォレンジックアナリスト	非常に巧妙な脅威へのインシデント対応では、マルウェアサンプルのリバースエンジニアリングやアーティファクトに対する高度なフォレンジック分析が必要になります。必要に応じて、法に則ってフォレンジック形跡を収集し分析しなければなりません。 インシデント対応活動中にフォレンジック形跡を収集、分析することがデジタルフォレンジックアナリストの主な責務です。	• デジタル形跡の収集と分析 • コンピューターインシデントおよび標的型攻撃の調査への参加 • OS、アプリケーション、メモリ、ネットワークフォレンジック分析 • IOC の収集
脅威インテリジェンスアナリスト	SOC の規模が十分に拡大したら、社内の脅威インテリジェンス担当部署に専門の役割を割り当てるのが合理的です。 脅威インテリジェンスのエキスパートは、さまざまなソース（分析レポート、OSINT、過去の経験など）から脅威インテリジェンスを分析し、SOC チームにとって価値ある結果（TTP、IOC、分析）を生み出す責務を担います。	• オープンソースの脅威インテリジェンスの収集と分析 • ベンダーによる脅威インテリジェンス分析レポートの分析、解析 • TI ソースからの TTP および IOC の収集 • 脅威データフィードの分類、優先順位付け、検証 • さまざまな関係者向けの脅威インテリジェンス分析レポートの作成 • SOC チームおよび外部パートナー向けの関連する分析の生成 • お客様との脅威フィードおよび IOC の共有
SOC システム管理者	SOC システム管理者は、SOC 領域の運用と維持（O&M）を担当します。	• SOC IT インフラストラクチャの O&M • SOC インフラストラクチャの正常性監視 • スクリプト作成、自動化 • SOC インフラストラクチャおよびツールのドキュメント作成

ロール	説明	説明
SOC マネージャー	SOC マネージャーは、全体的な業務の監督とチームの管理を担当します。	• 人材管理 • 戦略管理 • SOC のロードマップと戦略の策定 • 上層部、利害関係者などへの報告 • SOC のパフォーマンスと KPI の管理
	オプション[1]	
ティア 3 アナリスト（脅威ハンター）	ティア 3 アナリストは、プロアクティブな脅威ハンティングと高度な検知ロジック開発を主に担当する、高い技能を持つエキスパートです。非常に巧妙な脅威や優先度の高いインシデントに対処するために、インシデント対応活動にも関わる可能性があります。	• 脅威ハンティング • インシデントの分析と対応（ティア 3） • 検知のロジック開発とチューニング • セキュリティ監視システムの開発 • ティア 2 アナリストの作業のレビュー
脆弱性評価エキスパート	SOC の規模が十分に拡大したら、脆弱性評価部署に専門の役割を割り当てるのが合理的です。 また、レッドチーム演習の企画、攻撃シミュレーションの実施などを行うために、攻撃側セキュリティエキスパートを配置することも重要になります。また、TTP 分析や検知ロジック開発も非常に重要です。	• 脆弱性分析、優先順位付け、レポート • 侵入テスト、レッドチーム演習 • 検知ロジックのテスト（攻撃シミュレーション）への参加
SOC セキュリティエンジニア	SOC セキュリティエンジニアは、SOC のツールのエンジニアリング、統合、開発を担当します。SOC の規模、構成、ニーズに応じて、SIEM、エンドポイントセキュリティ、その他のセキュリティエンジニアリングの詳細分野に秀でた幅広いセキュリティエンジニアでチームを構成することができます。	• 関連付けルール、ダッシュボード、レポートの作成と開発（該当する場合） • センサーのチューニングと維持管理 • セキュリティ監視システムの維持管理と開発 • スクリプト作成、自動化 • カスタムツールの開発
法務責任者	法務責任者は、コンプライアンスの観点から SOC の活動やプロセスについて責任を担います。	• SOC 業務に関する具体的な法的問題に関する助言 • 利害関係者向けの法的助言 • その他の SOC チームの法的なサポート

Kaspersky のサービス：サイバーセキュリティトレーニングサービス

脅威の検知、マルウェア調査、リバースエンジニアリング、デジタルフォレンジックなど、Kaspersky のサイバーセキュリティに関する専門知識は 20 年以上にわたって進化と発展を続けてきました。Kaspersky のエキスパートは、1 日 325,000 件のマルウェアサンプルがもたらす脅威にどう対処すれば最善であるか、および今日の変わりゆく難しいサイバーセキュリティ環境に対処するためにその知識や現場で得られた経験を企業にどう活かしていけるかをよく理解しています。

当社のセキュリティトレーニングプログラムは、Kaspersky のアンチウイルスラボの設立に携わり、現在は次世代のグローバルエキスパートを指導し意識を喚起しているセキュリティ分野の権威によって設計され、開発されました。

コースは、理論的な講座と実践的なラボの両方を含むように設計されています。各コースの修了時に、受講生に対して、得られた知識を確認するための評価が行われます。

トレーニングコースは、システム管理とプログラミングについて一般的または高度なスキルを持っている IT 関連の専門家向けです。すべてのコースは、お客様の拠点で受講形式で行うか、または、適宜 Kaspersky のローカルオフィスもしくは地域拠点で実施します。

1　これらの役割がどれほど関連するかは、SOC のサービスポートフォリオと目標によって大きく変わります。たとえば、SOC が脅威ハンティングや脆弱性管理を行わない場合、「ティア 3 アナリスト（脅威ハンター）」や「脆弱性評価エキスパート」などのチームの役割はチームにとって不要な場合があります。

テーマ	期間	獲得スキル
Windows デジタルフォレンジック		
実例に基づいたサイバー空間での標的型攻撃インシデントのシミュレーションを通じて、以下のトピックについて学習します： • デジタルフォレンジックの概要 • ライブ形式での対応と形跡の収集 • Windows マシンの事後分析 • Windows OS レジストリの内部 • Windows OS イベント • Windows OS アーティファクトの分析 • ブラウザーのアーティファクトフォレンジック • メールの分析 • SSD ディスクを使ったフォレンジックの実践 • デジタルフォレンジックラボ構築の際の推奨事項 • 各種 Windows アーティファクトを使った、新しく得たスキルの実践的テスト	5 日間	• さまざまなデジタル形跡の取得、フォレンジック用として健全な環境での対処 • Windows OS アーティファクトからのインシデントに関連する悪意のある動作の痕跡発見 • 各種 Windows アーティファクトのタイムスタンプを活用したインシデントシナリオの再現 • ブラウザーおよびメール履歴の発見と分析 • デジタルフォレンジック用ツールおよび機器の活用 • デジタルフォレンジックラボの構築プロセスの理解

テーマ	期間	獲得スキル
マルウェア分析とリバースエンジニアリング		
• IDA Pro を使った基本分析 • 一般的な仮想化ソリューションやデバッガーを使った動的分析 • 悪意のあるドキュメントの分析 • アンパック • 復号化 • シェルコードの解析 • エクスプロイトの分析 • リバースエンジニアリングのヒントとテクニック	5 日間	• OS およびアセンブリ言語についての予備知識の取得 • 静的、動的なマルウェア分析の実施とそのふるまいや機能に関する完全な理解 • マルウェア分析対策テクニック、自己保護技術、保護ソフトウェア迂回機能への対処 • スタンドアロンおよび埋め込みのシェルコードの特定とリバースエンジニアリング • PDF エクスプロイトのゼロからの分析
高度な Windows デジタルフォレンジック		
実例に基づいた標的型のサイバー攻撃インシデントのシミュレーションを通じて、以下のトピックについて学習します： • 数値算定システム • FAT ファイルシステム • NTFS ファイルシステム • 詳細な Windows フォレンジック • ファイルシステム、シャドーコピー、ファイルカービングを使ったデータおよびファイルの復元 • クラウドコンピューティングでのフォレンジックの実践 • メモリフォレンジック • ネットワークフォレンジック • タイムラインとスーパータイムラインの分析の比較 • 取得したデジタル形跡を使った、新しく得たスキルの実践的テスト	5 日間	• 詳細なファイルシステム分析の実施 • さまざまなテクニックを使った、削除されたファイルの特定と復元 • 各種ツールを使ったネットワークトラフィックの分析 • メモリダンプ内の悪意のある動作の特定と追跡 • 詳細分析に使うためのメモリ関連箇所の特定とダンプ • ファイルシステムのタイムスタンプを使ったインシデントタイムラインの再現 • インシデントシナリオの理解を深めるための、全 Windows OS アーチファクト用の単一タイムラインの作成
高度なマルウェア分析とリバースエンジニアリング		
• アンパック • 復号化 • 共通するシナリオに対する独自のデクリプタの開発 • バイトコードの逆コンパイル • コードの分解 • 逆アセンブル • 最新の APT アーキテクチャの再構成 • 典型的なコード構成要素の確認 • 暗号化、圧縮アルゴリズムの特定 • コードとデータに基づいた分類とアトリビューション • クラスと構造の再構成 • APT プラグインアーキテクチャ（最近の APT サンプルに基づく）	5 日間	• 最初のサンプルの受信から IOC による攻撃者の TTP に関する技術的説明の作成まで、最新の APT ツールキットを分析 • 実例に基づいた静的なデクリプタの作成と、その後の悪意のあるコードの詳細分析 • 通常初期のペイロード配信に使われる悪意のあるドキュメントの分析と、それらのペイロードの抽出方法の理解 • 損害の評価、正確で効果的なインシデント対応の実施
Windows インシデント対応		
実例に基づいたシミュレーション環境でインシデントが発生し、そのシナリオに沿って以下のトピックについて学習します： • インシデント対応プロセスとそのワークフローの概要 • 一般の脅威と APT の違いについて • APT サイバーキルチェーンについて • さまざまなインシデントシナリオへのインシデント対応プロセスの適用 • シミュレーション環境でのサイバーキルチェーンの活用 • 最初の対応者が行う標的マシン上でのライブ分析 • フォレンジック用として十分な形跡の取得テクニック • 事後分析およびデジタルフォレンジックの概要 • メモリフォレンジックの概要 • 正規表現と ELK を使ったログファイル分析 • サイバー脅威インテリジェンスの概要 • YARA および SNORT による不正アクセスの痕跡（IOC）の作成 • マルウェア分析とサンドボックスの概要 • ネットワークトラフィックフォレンジックの概要 • インシデント分析レポートについてのディスカッションと CSIRT 作成に関する推奨事項 • 別のシミュレーションシナリオでの、新しく得たスキルの実践的テスト	5 日間	• インシデント対応の各フェーズの理解 • サイバーインシデントへの対応中に考慮すべきこと • サイバーキルチェーンを通じたさまざまな攻撃テクニックと標的型攻撃の構造の理解 • 適切な行動による各種インシデントへの対応 • APT と他の脅威の区別 • ライブ分析ツールを使ったサイバーインシデントの確認 • ライブ分析と事後分析の違い、およびそれらを適用すべき状況に関する理解 • デジタル形跡の特定（HDD、メモリ、ネットワークトラフィック）、そのフォレンジック分析の導入 • 検知された攻撃用の YARA および SNORT IOC の記述 • ログファイル分析 • IR チームの構築に関わるプロセスの理解
Yara による効率的な脅威検知		
• Yara 構文の概要 • 高速かつ効果的なルールを作成するためのコツ • Yara 生成ツール • Yara ルールの誤検知テスト • VT での新規未検知サンプルのハンティング • 効果的な検知のための Yara 内での外部モジュール活用 • アノマリ検索 • 多数の実例 • Yara スキル向上のための演習	2 日間	• 効果的な Yara ルールを作成する • Yara ルールのテスト • 未知の脅威を発見できるレベルにまでの Yara ルールの改善

高度な検知、対応技術

今日の高度な脅威に対する保護製品は、SIEM システムと連携して、企業が効果的な新しい SOC を設立し、あるいは既存の SOC をより充実させられるものになっています。そのための手段がいくつかあります。

1 つ目の手段は可能な限りの自動化です。手動タスクの検知、分析、および対応を自動化することで、アラートのトリアージを行うアナリストが、脅威データストリームへの対処などについて分析スキルを効果的に適用するために必要になるツール、時間、ヘッドスペースを確保できます。成熟したインシデント対応および脅威ハンティングチームは、この時間をプロアクティブな脅威ハンティング、インシデントの詳細分析、複雑なインシデントへの効果的な対応を実現するための配置計画に充てることができます。

ほかにも、アナリストがインフラ全体を 360 度完全に見渡せるようにすること、関連するログを SIEM に提供すること、統合されたメタデータ、オブジェクト、判定データにすぐにアクセスできるようにすることが、上記の手段として挙げられます。これらも、侵害されたワークステーションにアクセスできない状態になった場合やデータがハッカーによって暗号化された場合でも、アナリストが効果的に作業するために役立ちます。

これらすべての手段を講じることで、SOC チームは侵入者の一連の行動を全体的により深く理解でき、また、アナリストが対処しなければならない誤検知のアラート数や、アラートの優先順位付けにかかる時間を削減することができます。

Kaspersky のソリューション：Kaspersky Sandbox

Kaspersky のポートフォリオには高度な APT 対策技術が含まれています。この技術については、多くの第三者評価機関のテストによって業界最高の検知率であることが証明されています。しかし、これらのソリューションを効果的に活用するためには、適切な経験と専門知識を持つ本格的な IT セキュリティ部門の設置が必要になります。しかし、インフラが地理的に分散されている企業では、そのような部門がない場合もあります。

そのような企業は通常、多数のワークステーション、サーバー、その他の補助装置で構成される統合 IT インフラストラクチャを備えた本社を置いています。支社は異種混在環境であることが多く、大規模な支社と、ローカルネットワークやインターネットアクセスが遅い小規模な支社で構成される場合もあります。

Kaspersky Anti Targeted Attack および Kaspersky EDR を利用すれば、本社または大規模な支社を保護することができます。セキュリティオペレーションセンターのエキスパートがこれらのツールを利用することで、複雑な脅威を完全かつ迅速に特定して撃退することができます。しかし、中規模の支社やリモートオフィスでリソースや専門知識が不足していた場合、これらのソリューションを常に利用できるとは限りません。予算に制約があり、複雑な脅威に対処できるように訓練された技術者が世界的に不足している（そのために人件費がかかる）ことが、この種のソリューションのリモートオフィスでの利用が進まない主な要因になっています。

この場合、もっとも効果的で利用しやすいアプローチは、Kaspersky Endpoint Security for Business を Kaspersky Sandbox と併用することで、複雑な脅威に対抗することです。

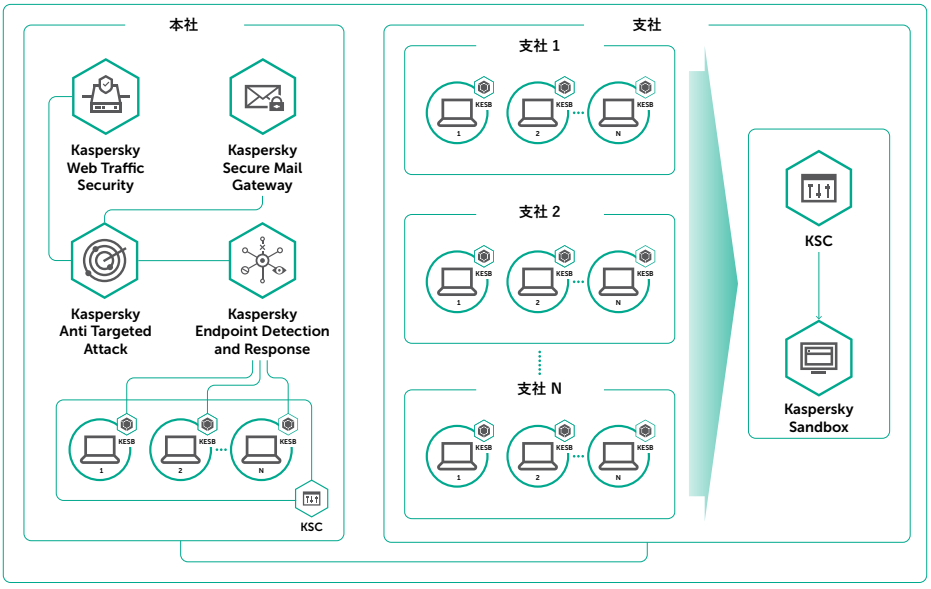


図 5：
分散ネットワークを設置する大規模組織での Kaspersky Sandbox

Kaspersky Sandbox は、既存のエンドポイント保護製品を迂回できる、増え続ける複雑な最新の脅威に対抗するための製品です。Kaspersky Sandbox により Kaspersky Endpoint Security for Business の機能を補うことで、高度な専門知識を持つ情報セキュリティアナリストがいなくても、未知のマルウェア、新しいウイルスやランサムウェア、ゼロデイエクスプロイト、その他の脅威に対するワークステーションやサーバーの保護レベルを大幅に引き上げることができます。

仕組み

Kaspersky Sandbox は、複雑な脅威や APT レベルの攻撃に対抗してきた Kaspersky のエキスパートのベストプラクティスを活用しており、Kaspersky Endpoint Security for Business と密接に統合されています。管理は、Kaspersky のポリシーベースの統合管理コンソールである Kaspersky Security Center から行います。

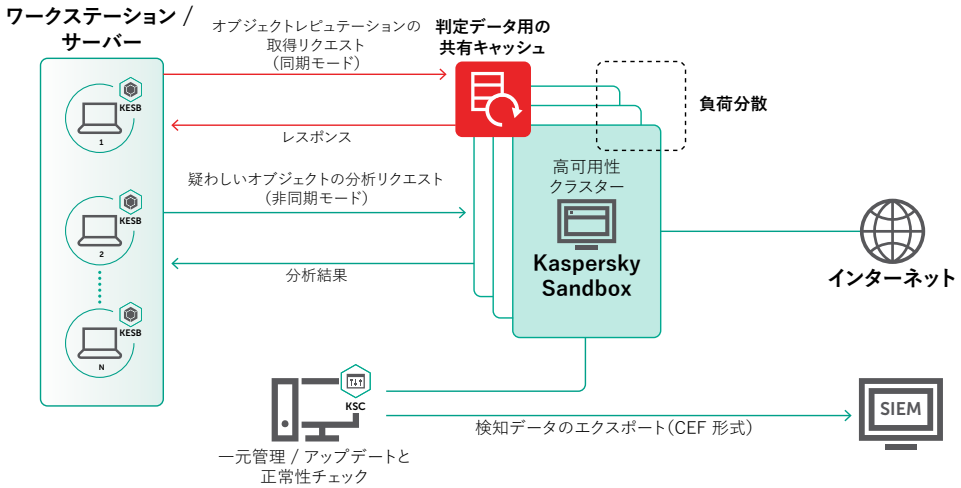


図 6:
Kaspersky Sandbox

Kaspersky Endpoint Security for Business エージェントは、Kaspersky Sandbox サーバーにある判定データ用の共有運用キャッシュから、疑わしいオブジェクトに関するデータを取得するようリクエストします。オブジェクトがすでにスキャン済みである場合、Kaspersky Endpoint Security for Business はその判定データを受信し、以下の 1 つ以上の修復オプションを適用します：

- 除去、隔離
- ユーザーへの通知
- 簡易スキャンの開始
- 検知されたオブジェクトを、管理対象ネットワーク内の他のマシンで検索

オブジェクトのレピュテーションについての判定データをキャッシュから取得できない場合、Kaspersky Endpoint Security for Business エージェントはその疑わしいファイルを Sandbox に送信して、レスポンスを待ちます。Sandbox はオブジェクトのスキャンのリクエストを受信し、この時点で、実際のインフラから隔離された環境内で、そのテストオブジェクトが実行されます。ファイルスキャンは、一般的な作業環境（オペレーティングシステムやインストール済みアプリケーション）をエミュレートし、各種ツールを配備した仮想マシン内で実行されます。オブジェクトの悪意のある意図を検知するために、ふるまい分析が実行され、アーティファクトが収集、分析されます。オブジェクトが悪意のある動作を実行している場合は、Sandbox はそのオブジェクトをマルウェアとして認識します。サンドボックス分析の実行中、オブジェクトに対して 1 つの判定が割り当てられます。

オブジェクトのエミュレートプロセスが完了すると、判定結果がリアルタイムで判定データ用の共有運用キャッシュに送信され、Kaspersky Endpoint Security for Business がインストールされている他のホストもスキャン済みオブジェクトのレピュテーションに関するデータをすぐに取得できるようになります。同じファイルを再分析する必要はありません。このアプローチによって、疑わしいオブジェクトを迅速に処理して、Kaspersky Sandbox サーバーの負荷を軽減し、脅威に対する対応のスピードと効率性を高めることができます。

Kaspersky Sandbox を利用すれば、高度な脅威の阻止に関連するタスクの大部分を自動化することで、IT セキュリティエキスパートの人件費や関連するコストを大幅に削減することができます。リソースを追加せずに高度で複雑な未知の脅威が自動でブロックされるようになり、IT セキュリティアナリストが他のタスクに集中できるようになります。

Kaspersky のソリューション：Kaspersky Anti Targeted Attack と Kaspersky Endpoint Detection and Response

ネットワークトラフィック分析用の Kaspersky Anti Targeted Attack と、エンドポイントレベルの Kaspersky Endpoint Detection and Response は、1 つの技術プラットフォームを基盤としています。このプラットフォームは多次元的な一体型のソリューションで構成され、時間のかかる形跡の収集や、脅威の痕跡の検知、分析、複雑なインシデントへの対応のプロセスに関連する定型的な手動タスクが完全に自動化されます。

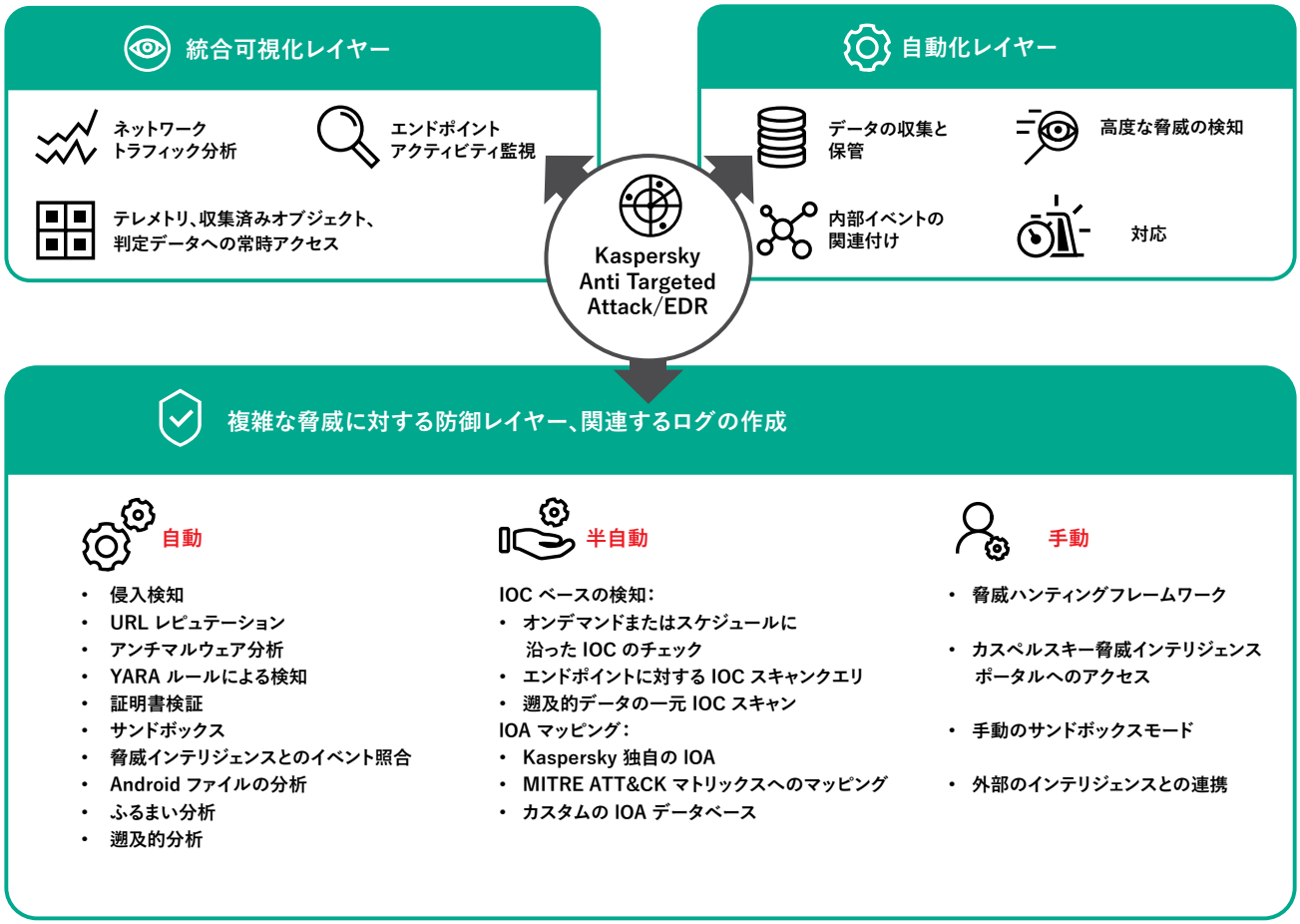


図 7:
Kaspersky Anti Targeted Attack と
Kaspersky EDR

Kaspersky のテクノロジーは、SIEM への重要なデータソースとしての役割を果たしながら、強力な自動検知機能と脅威ハンティング機能を提供します。Kaspersky Anti Targeted Attack と Kaspersky EDR には次の検知メカニズムが搭載されています。一元管理された NGAV、IOC スキャン、IOA マッピング、YARA ルール、サンドボックス、クラウドベースの ML-APK 分析、ふるまい分析、証明書チェック、遡及的分析、脅威ハンティングフレームワーク、組み込みの自動脅威インテリジェンスモジュール、および脅威インテリジェンスポータルへのアクセスです。

これにより、従来のセキュリティ対策を迂回するように設計された巧妙な脅威も検知しながら、SOC が定型的なタスクに時間を浪費したり、複数のコンソールを何度も切り替えたりせず、日常業務を効果的かつ効率的に行えるようになります。関連のないログの分析にかかるコストを避け、インシデント対応に必要な時間を大幅に削減できます。

Kaspersky Anti Targeted Attack と Kaspersky Endpoint Detection and Response の導入による効果：

- データ収集、検知、対応プロセスにおける面倒だが必要な手動タスクにアナリストが費やす時間を大幅に削減
- インシデント処理プロセスを大幅に効率化することで、リスクを大きく軽減
- 他のシステムからのログと関連付けるための新しい関連ログソースを SIEM に提供することで、コントロールの強化、効果的な調査のほか、大幅な可視化と、行動までの期間の短縮を実現
- SOC 成熟化のためのより幅広い長期的なアプローチが可能に

製品の概要:

- オンプレミスでデプロイされるため組織外部へのデータ送信はなし
- 100 以上のファイル種別の分析に対応
- 高度な回避テクニック
- ユーザーアクティビティのエミュレート
- カスタムイメージによって、幅広いオペレーティングシステムやアプリケーションにわたる脅威の分析、および実際の環境に適応される脅威のみの分析が可能
- 各プロセスを個別に分析して、疑わしい動作と関連するネットワーク接続を検知
- すべてのシステムアクティビティ、抽出されたファイル、ネットワークアクティビティ(PCAP)、視覚的なグラフを含む詳細な分析レポート
- STIX、JSON、CSV 形式でのデータのエクスポート
- Kaspersky Private Security Network との統合サポート
- 手動ファイル送信、およびシームレスな統合とセキュリティ運用自動化のための RESTful API

Kaspersky のソリューション:Research Sandbox

ファイルのふるまいに基づいてインテリジェントな判断を行うこと、およびそれと並行してプロセスメモリ、ネットワークアクティビティなどを分析することが、目標に合わせて洗練された現在の標的型脅威を理解する上で最適なアプローチです。サンドボックス技術は、ファイルサンプルの発生源を調査し、ふるまい分析に基づいて IOC を収集し、未知の悪意のあるオブジェクトを検知できる強力なツールとなります。

現代のマルウェアは、悪意のある動作の存在を知らせる可能性のあるコードを実行しないように、あらゆる策を講じています。標的のシステムに必要なパラメータが揃っていない場合、悪意のあるプログラムはほぼ確実に自らを破壊し、一切の痕跡を残しません。そのため、悪意のあるコードを実行するには、サンドボックス環境が通常のエンドユーザーのふるまいを正確に模倣できる必要があります。

Kaspersky Research Sandbox は、当社のラボ内で 10 年以上にわたって進化を遂げてきたサンドボックステクノロジーを活用して直接開発されています。この製品には、Kaspersky の継続的な脅威の研究によって明らかになったマルウェアのふるまいに関する全知識が取り込まれています。当社が毎日 350,000 件以上の新たな悪意のあるオブジェクトを検知できるのも、この製品があるからです。この強力なテクノロジーはオンプレミスで導入されるため、データの外部への送信は実行しません。

以下に、Kaspersky Research Sandbox のアーキテクチャ概要図を示します。

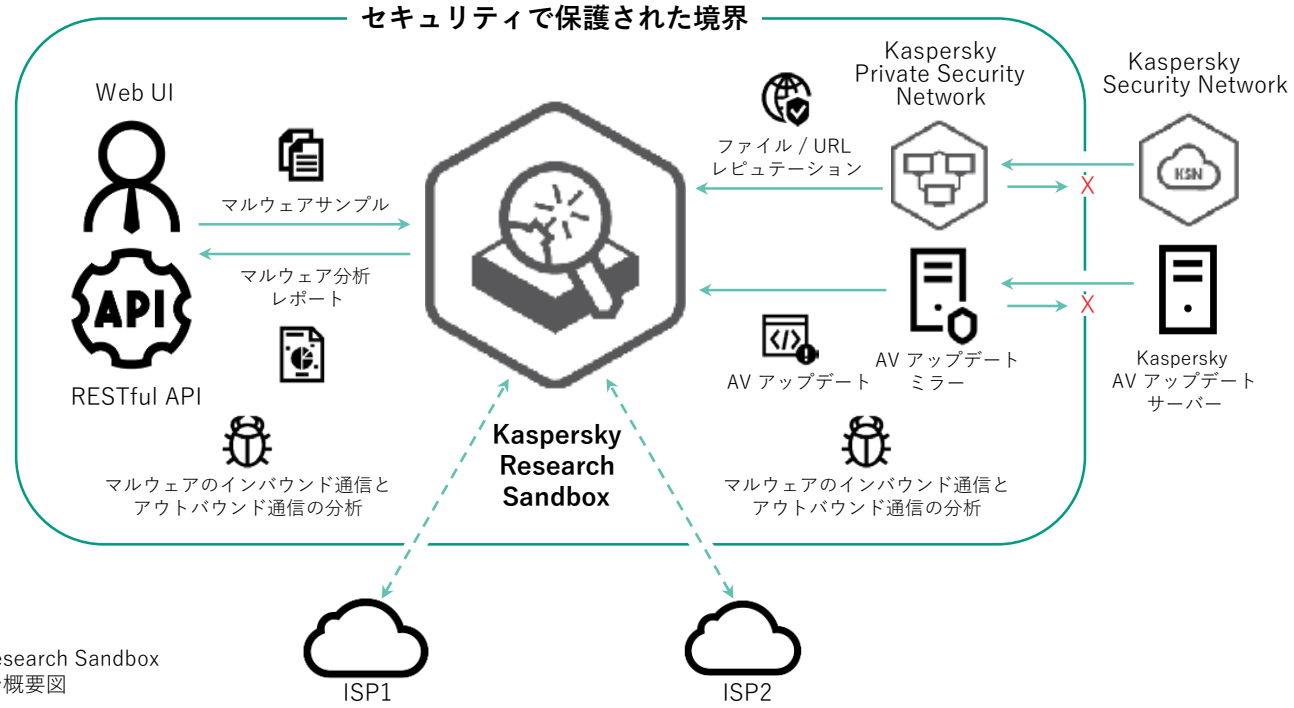


図 8:
Kaspersky Research Sandbox
アーキテクチャ概要図

Kaspersky Research Sandbox は、数ペタバイト規模の統計的データから収集した脅威インテリジェンス、ふるまい分析、信頼性の高い回避対策と、ユーザー操作のシミュレート技術を組み合わせたハイブリッドアプローチを採用しています。また、分析用のシステムのイメージをカスタマイズして実際の環境に合わせることも可能で、これにより脅威検知の精度と調査スピードを高めることができます。

分析の終了後は、分析対象サンプルのふるまいと機能に関する以下の詳細レポートが生成され、ユーザーはこのレポートを利用して適切な対応手順を定義することができます:

- **概要**:ファイルの実行結果に関する一般情報。
- **サンドボックス検知名**:ファイルの実行中に登録された検知名(AV およびふるまい)のリスト。
- **トリガーされたネットワークルール**:実行されたオブジェクトからのトラフィックの分析中にトリガーされた SNORT ネットワークルールのリスト。
- **実行マップ**:オブジェクトの動作(ファイル、プロセス、レジストリに対する操作、およびネットワークアクティビティ)の順序とそれらの間の関係をグラフィカルに表現したもの。ツリーのルートノードは実行されたオブジェクト。
- **疑わしい動作**:登録された疑わしい動作のリスト。
- **スクリーンショット**:ファイルの実行中に取得された一連のスクリーンショット。

- **読み込まれた PE イメージ**：ファイルの実行中に検知された、読み込まれた PE イメージのリスト。
- **ファイル操作**：ファイルの実行中に登録されたファイル操作のリスト。
- **レジストリ操作**：ファイルの実行中に検知された、OS レジストリに対する操作のリスト。
- **プロセス操作**：ファイルの実行中に登録された、各種プロセスによるファイルとの相互作用のリスト。
- **同期操作**：ファイルの実行中に登録された、作成済み同期オブジェクト（ミューテックス、イベント、セマフォ）の操作のリスト。
- **ダウンロードされたファイル**：ファイルの実行中にネットワークトラフィックから抽出されたファイルのリスト。
- **ドロップされたファイル**：実行されたファイルによって保存（作成または変更）されたファイルのリスト。
- **HTTPS/HTTP/DNS リクエスト**：ファイルの実行中に登録された HTTPS/HTTP/DNS リクエストのリスト。
- **ネットワークトラフィックのダンプ（PCAP）**：ネットワークアクティビティは PCAP 形式でエクスポート可能。

Kaspersky Research Sandbox は、未知の脅威を検知するための最適なツールです。他のどのソリューションよりも成熟し、高度な脅威に特化したものになっています。

製品の概要：

- 多数の APT グループやサンプルに関する要約済みデータのリポジトリにすぐにアクセス可能
- 効率的な自動または手動の脅威優先順位付けとアラートのトリアージ
- 公にされていないサイバー犯罪組織やオブジェクトを追加できる機能
- サンプルの手動アップロード、自動化されたワークフローと連携するためのオープン API
- Kaspersky Reserach Sandbox との標準での統合
- ESXi 対応
- 完全なオンプレミスデプロイオプションに対応
- 機密情報の漏洩を避けるため、すべての送信内容について完全的なプライバシーと機密性を維持

Kaspersky のソリューション：Threat Attribution Engine[1]

サイバー攻撃の規模は世界中で拡大し続けています。国家が支援するサイバー攻撃や標的型攻撃は、以前は見られなかったほど熾烈になっています。プロのサイバー犯罪組織、「ハクティビスト」、および国家支援によるサイバー攻撃グループなどが、技術的な進歩を遂げており、その多くがセキュリティチームのスキルやリソースの成長速度を上回っています。x

しかし、攻撃者は以前の攻撃のコードやテクニックを再利用することが多く、以前の攻撃から再利用された要素を識別すること、および観察された変更点や再利用の種別において一定のパターンを検知することができます。そうすることで、より迅速に防御手段を開発し、マルウェアの発生源について仮説を立て、将来の攻撃を予測し、その攻撃から防御するために準備することができます。

Kaspersky Threat Attribution Engine は、当社の Global Research and Analysis Team が調査した APT の脅威に関する非常に大規模なリポジトリに基づいてセキュリティチーム向けに提供される、他社にはないマルウェア分析ツールです。新しい攻撃を既知の APT マルウェア、過去の標的型攻撃、ハッカーグループにすぐに関連付けることができます。深刻度の低いインシデントの中から高リスクの脅威を見つけて、適切なタイミングで保護対策を適用することで、攻撃者がシステム内に足掛かりを作ることを阻止できます。

1　2020 年第 2 四半期にリリース予定

仕組み

Kaspersky Threat Attribution Engine は、マルウェアの「遺伝的性質」(すなわち、元のファイルをリバースエンジニアリングした表現)を分析し、以前に調査された APT サンプルとのコードの類似性と関連付けられたサイバー犯罪組織を自動的に探し出します。分析対象のファイルの「遺伝子」(すなわち、抽出されたコード文字列)を、APT マルウェアサンプルデータベースと比較して、マルウェアの発生源、サイバー犯罪組織、および既知の APT サンプルとのファイルの類似性についてレポートを作成します。また、公にされていないサイバー犯罪組織やオブジェクトをデータベースに追加することもできます。リバースエンジニアリング分析の自動化によって、マルウェア分析とインシデント対応にかかる時間を大幅に短縮して、脅威の優先順位付けを迅速に行うことができます。

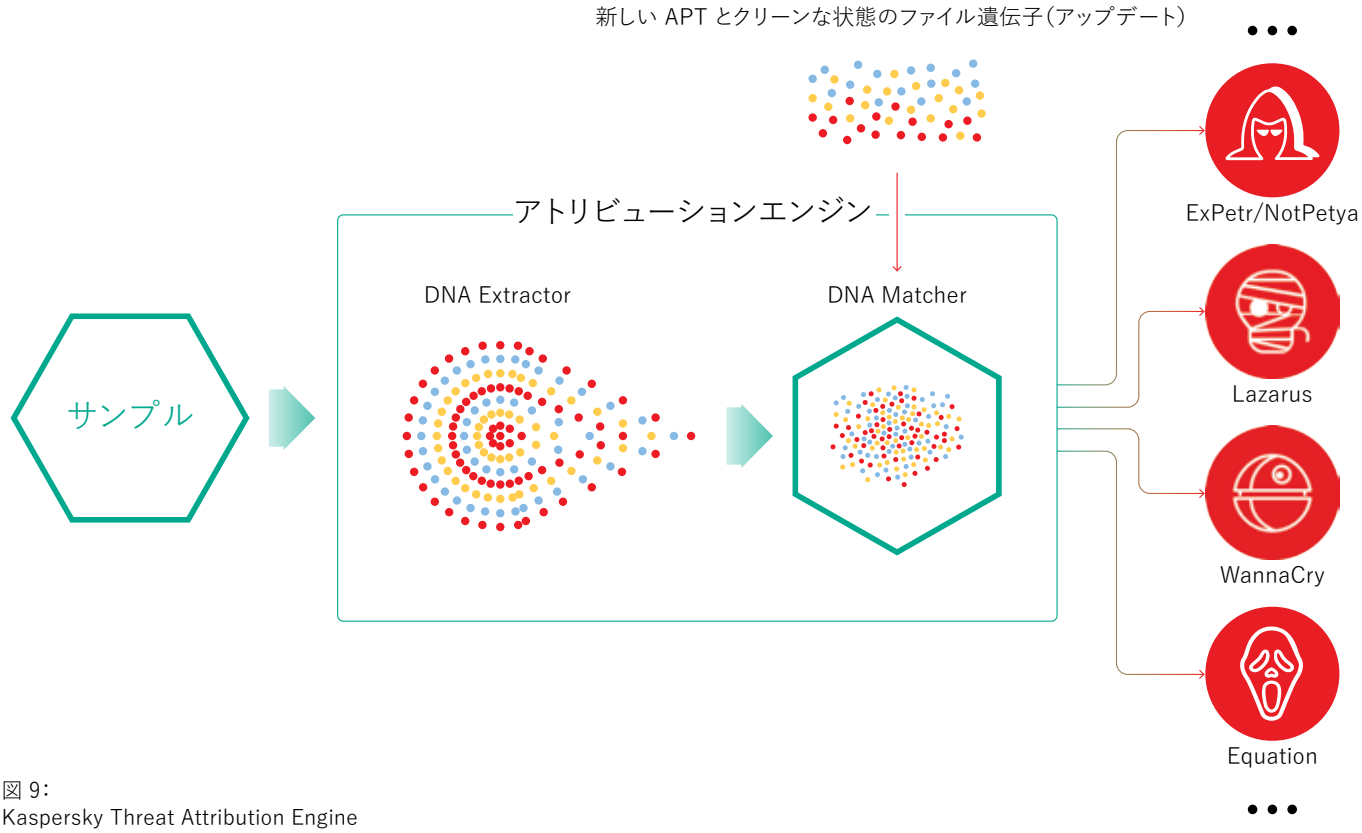


図 9:
Kaspersky Threat Attribution Engine

まず、Kaspersky Threat Attribution Engine が特定の基準に一致する関連コード文字列(「遺伝子」)を抽出します。重要な点として、最終的なゲノムデータベースには 10 000 を超える遺伝子が格納されます。次に、Kaspersky の 20 年以上にわたる調査によって収集された 30 億以上のサンプルからレピュテーションスコアを計算し、すべての「良」、「不良」の「遺伝子型」(代表的な遺伝子グループ)を示します。最後に、サンプルの遺伝子型とコードのアトリビューションを明らかにして、ユーザーがマルウェアの発生源とその作成者の候補について洞察できるようにします。

Kaspersky Attribution Engine によって、セキュリティ運用が以下のように改善されます:

- ファイルから既知の APT グループを迅速に特定し、サイバーインシデントの背景にある動機、手法、ツールを明らかにする。
- お客様が攻撃の標的であるのか、攻撃に巻き込まれたのかを即座に評価して、適切な封じ込めおよび対応手順を設定できるようにする。
- カスペルスキー APT インテリジェンスレポートに示される APT ファミリーに関する実用的な脅威インテリジェンスに従って、効果的かつ迅速に脅威を軽減する。[2]

2 カスペルスキー APT インテリジェンスレポートの購読サービスは別途購入していただく必要があります

脅威インテリジェンス

SOC は従来、以下の業務を行うための部門でした：

- セキュリティデバイス管理、境界部の維持管理、予防的なセキュリティ技術（IPS/IDS、ファイアウォール、プロキシなど）の適用
- SIEM（セキュリティ情報およびイベント管理）システムによるセキュリティイベントの監視
- インシデント対応と修復
- 内部規則または規制へのコンプライアンス（PCI-DSS など）

現在では、多くの組織が独自の SOC を設置することで、脅威の可視化を進めようと取り組んでいます。しかし、すでに SOC を設置した一部の組織は、以前と同じ問題の多くに直面しています。それにはさまざまな理由があります：

- 優先順位付けの質が良くない。1 日に何千もの重要度の低いセキュリティアラートを受信し分析しているために、本当に重要な脅威が埋もれてしまっている。
- 関連するサイバー犯罪組織の TTP（戦術、テクニック、手順）を正しく理解せずにインシデントの修復措置を行っているために、高度な攻撃を見過ごしている。
- インシデントに対して事後対応型のアプローチをとっており、組織内で未発見のまま活動を続けている脅威をプロアクティブに「ハンティング」していない。
- 現在の脅威の情勢について戦略的に見渡しておらず、同種企業に対する攻撃や利用可能な対策について意識していない。
- ビジネスプロセスに対するセキュリティ侵害関連のリスクを、技術者ではない取締役に伝えることが難しいために、特定のセキュリティ技術に対して社内の十分な投資を引き出せないという問題がある。

これらの検討課題に基づいてセキュリティ部門のリーダーにアドバイスできることは、インテリジェンス主導の SOC というアプローチに従うことです。SOC を効果的に運用するためには、脅威を取り巻く環境における変化の広がりに合わせて、新しいテクノロジーやコントロールを継続的に取り入れる必要があります。

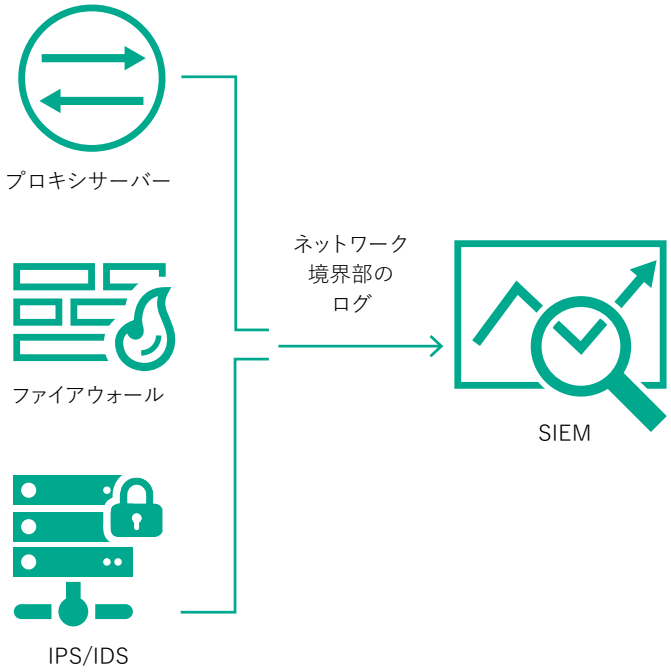


図 10：
従来の SOC

ガートナーによる脅威インテリジェンスの定義：「資産に対する既存または新規の脅威や危険に関する、コンテキスト、メカニズム、痕跡、予想される影響、実用的なアドバイスを含む、形跡に基づいた知識であり、その主体によるその脅威や危険への対応に関する意思決定のための根拠として利用可能なもの」

Gartner、『How Gartner Defines Threat Intelligence』

内部の脅威に関するデータを外部の信頼できるソース（OSINT、マルウェア対策のグローバルベンダーなど）から収集した情報と組み合わせることで、攻撃テクニックやその痕跡の可能性について把握できます。それにより、特定の組織を対象とした汎用的な攻撃や高度な攻撃に対抗するための効率的な防御戦略を策定できるようになります。

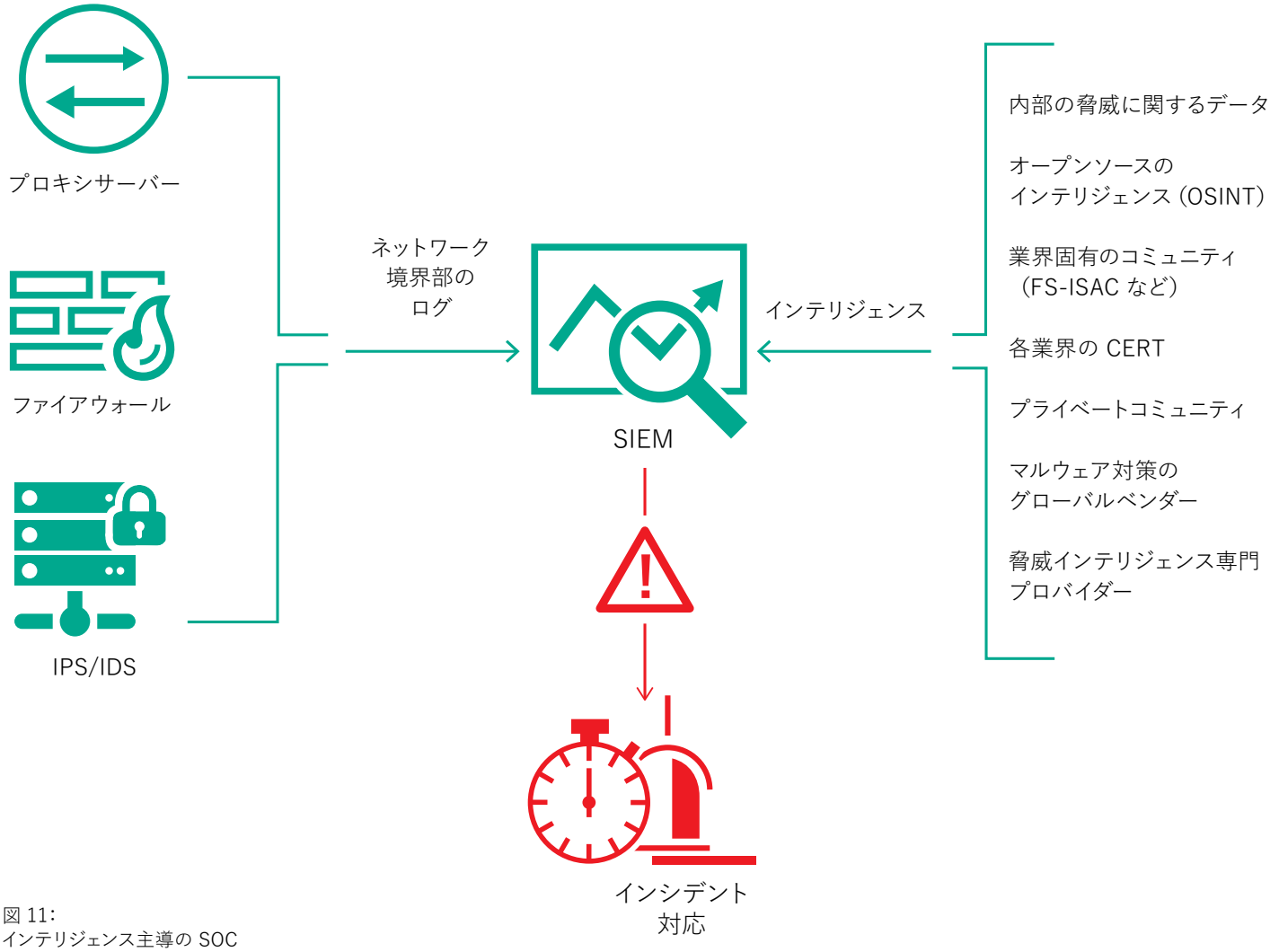


図 11：
インテリジェンス主導の SOC

インテリジェンスの提供元は慎重に選ぶ必要があります。

利用するインテリジェンスの品質と、そのインテリジェンスに基づいて行われる意思決定の有効性には直接的な相関関係があります。

利用するインテリジェンスが関連性の薄いもの、不正確なもの、または業界やビジネス目標に合わないものである場合や、脅威情報をすぐに受信できない場合、組織の意思決定の質が大きく損なわれる可能性があります。

コンテキスト情報のない一次的なデータでは、SOC チームが効果的に業務を行うために必要な関連情報を得ることができません。たとえば、ある特定の URL が悪意のあるものだと知る場合と、それがエクスプロイトや特定の種別のマルウェアをホストする目的で利用されているという情報も知る場合とでは、状況はかなり異なってきます。このような追加のインテリジェンスレイヤーによって、セキュリティエキスパートはインシデントの調査時に注意すべき点を把握できるのです。

さまざまな商用の脅威インテリジェンスサービスを評価するための共通の基準はまだ存在しませんが、その評価において念頭に置くべきことがいくつかあります：

- グローバルな範囲のインテリジェンスを探しましょう。攻撃に国境はありません。ラテンアメリカの一企業を標的とする攻撃が欧州から開始される場合もあれば、その逆の場合もあります。そのベンダーは情報を世界中から入手し、一見関係のないアクティビティをまとまりのある攻撃活動として表現していますか。この種のインテリジェンスが適切な行動につながります。

- 長期的なセキュリティ計画策定の情報を得るために、以下のようなより戦略的なコンテンツを探し求めている場合：
  - 攻撃傾向の概要
  - 攻撃者が利用するテクニックと手法
  - 動機
  - アトリビューションなど

  その場合は、関係する地域または業界において、複雑な脅威を継続的に発見し調査してきた実績のある脅威インテリジェンスプロバイダーを探しましょう。そのプロバイダーが顧客企業の特性に合わせて調査できるかという点も重要です。
- コンテキスト情報によって、データからインテリジェンスが生まれます。コンテキスト情報のない脅威の痕跡に価値はありません。「なぜこれが重要なのか」という重要な質問に答えるための支援ができるプロバイダーを探し出す必要があります。関係に関するコンテキスト情報（例：特定のファイルのダウンロード元となった検知済み IP アドレスまたは URL に関連するドメイン）があればさらに価値が高まり、インシデント調査を迅速化し、ネットワーク内で新しく発見した関連の不正アクセスの痕跡（IOC）を明らかにすることで、より質の高いインシデントの「スコープ設定」も可能になります。
- 何らかのセキュリティコントロールをすでに配備しており、関連するプロセスを定義している企業の場合は、すでに利用中の既知のツールから脅威インテリジェンスを利用できることが重要です。そのため、脅威インテリジェンスを既存のセキュリティ運用にスムーズに統合するのを支援するための配信方法、統合メカニズム、および形式について確認してください。

サービスの概要

- データフィードは、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されます（Kaspersky Security Network は、200 を超える国と地域の数千万のエンドユーザーを対象として、インターネットの全トラフィックのうち、かなりの割合のトラフィックを把握しています）。そのため、高い検知率と精度を実現しています。
- 各データフィード内のすべてのレコードに実用的なコンテキスト情報（脅威名、タイムスタンプ、地理位置情報、感染した Web リソースの解決済み IP アドレス、ハッシュ値、知名度など）が付加されます。コンテキスト情報によって「より広い視野」が得られ、その後の検証や、幅広いデータの利用法が可能になります。データをコンテキスト情報とともに考察することで、「誰が」、「何を」、「どこで」、「いつ」という疑問に答えることが簡単になり、その結果、攻撃者を特定して、特に自社を保護する迅速な意思決定を下して行動に移すことができます。
- 単純な軽量の配布形式（JSON、CSV、OpenIOC、STIX）であり HTTPS や任意の配信手法によって配信されるため、フィードをセキュリティソリューションに容易に統合できます。
- 脅威インテリジェンスは耐障害性の高いインフラストラクチャによって生成、監視されており、継続的可用性と一貫したパフォーマンスが確保されています。
- HP ArcSight、IBM QRadar、Splunk などのソリューションとすぐに統合できます。

Kaspersky のソリューション：脅威データフィード

Kaspersky は、絶えず更新される脅威データフィードを提供することで、SOC チームにサイバー脅威のリスクと予想される影響について通知します。この情報により、脅威を効果的に緩和し、攻撃が始まる前でも攻撃から保護することができます。

フィードの説明

- **IP レピュテーションフィード**：疑わしいホストや悪意のあるホストを対象とした IP アドレスとコンテキスト情報のセット。
- **悪意のある URL**：悪意のあるリンクと Web サイトを含む URL のセット。マスキングされたレコードまたはマスキングされていないレコードを利用できます。
- **フィッシング URL**：Kaspersky がフィッシングサイトとして識別した URL のセット。マスキングされたレコードまたはマスキングされていないレコードを利用できます。
- **ボットネットの C&C URL**：ボットネットのコマンド & コントロール（C&C）サーバーと関連する悪意あるオブジェクトの URL のセット。
- **ランサムウェア URL フィード**：ランサムウェアオブジェクトをホストするリンクまたはランサムウェアオブジェクトからアクセスされるリンクを対象とします。
- **脆弱性データフィード**：セキュリティ脆弱性と、関連する脅威インテリジェンスのセット（脆弱なアプリケーションやエクスプロイトのハッシュ値、タイムスタンプ、CVE、パッチなど）。
- **APT IOC フィード**：APT 攻撃を実行するために利用される悪意のあるドメイン、ホスト、IP アドレス、ファイルを対象とします。
- **パッシブ DNS（pDNS）フィード**：ドメインを対応する IP アドレスに DNS 解決した結果を含むレコードのセット。
- **IoT URL フィード**：IoT デバイスに感染するマルウェアのダウンロードに使われた Web サイトを対象とします。
- **ホワイトリストデータフィード**：サードパーティの製品およびサービスについての正規ソフトウェアに関する体系的知識を提供するファイルハッシュ値のセット。
- **悪意のあるハッシュフィード**：もっとも危険かつ蔓延している新しいマルウェアを対象とします。
- **モバイル向けの悪意のあるハッシュフィード**：モバイルプラットフォームに感染する悪意あるオブジェクトを検知するためのファイルハッシュ値のセット。
- **P-SMS 型トロイの木馬フィード**：モバイルユーザーへの高額請求や、攻撃者による SMS メッセージの盗用、削除、応答を可能にする SMS 型トロイの木馬を検知するためのコンテキストとトロイの木馬のハッシュ値のセット。
- **モバイルボットネットの C&C URL**：モバイルボットネットの C&C サーバーを対象としたコンテキストと URL のセット。

Kaspersky のソリューション：Kaspersky CyberTrace

SOCのティア 1 アナリストが毎日処理するセキュリティアラートの数は急増しています。これほどの量のデータを分析しながら、アラートの優先順位付け、トリアージ、検証を効果的に行うのはほぼ不可能になりました。多数のセキュリティ製品からあまりにも多くの点滅信号が送られるため、大量のアラートが雑音の中に埋もれて、アナリストが疲れ果てています。セキュリティデータを集計して関連するアラームを対応付ける SIEM、ログ管理ツール、セキュリティ分析ツールは、追加調査を必要とするアラートの数を削減するのにいずれも役立ちますが、ティア 1 の技術者が過剰な負担を強いられる状況は変わりません。

効果的なアラートのトリアージと分析の実現

SOCは、マシンリーダブルな最新の脅威インテリジェンスを SIEM システムなどの既存のセキュリティコントロールと統合することで、初期のトリアージプロセスを自動化することができます。また同時に、調査が必要なアラートまたは詳細調査や対応のためにインシデント対応（IR）チームにエスカレーションする必要のあるアラートを迅速に特定するための十分なコンテキスト情報をティア 1 の技術者に提供できます。しかし、脅威データフィードの数や利用可能な脅威インテリジェンスの提供元が増え続けているために、どの情報が自社に関連があるかを判断するのが難しくなっています。脅威インテリジェンスはさまざまな異なる形式で提供され、大量の不正アクセスの痕跡（IOC）情報が含まれているため、SIEM やネットワークセキュリティコントロールがそれらの情報を取り込むのも困難な状況です。

Kaspersky CyberTrace は、脅威インテリジェンスの融合および分析ツールであり、脅威データフィードと SIEM ソリューションのシームレスな統合を可能にして、アナリストが既存のセキュリティ運用ワークフローで脅威インテリジェンスをより効果的に活用できるようにします。ユーザーが利用する可能性のある形式（JSON、STIX、XML、CSV 形式）のあらゆる脅威インテリジェンスフィード（Kaspersky、他ベンダー、OSINT からの脅威インテリジェンスフィードまたはカスタムのフィード）と統合されます。また、多数の SIEM ソリューションやログソースとすぐに統合可能です。Kaspersky CyberTrace では、ログを脅威インテリジェンスフィードと自動的に照合することで、リアルタイムの「状況認識」が可能になり、ティア 1 のアナリストが迅速かつより良い情報を得た上で意思決定できるようになります。

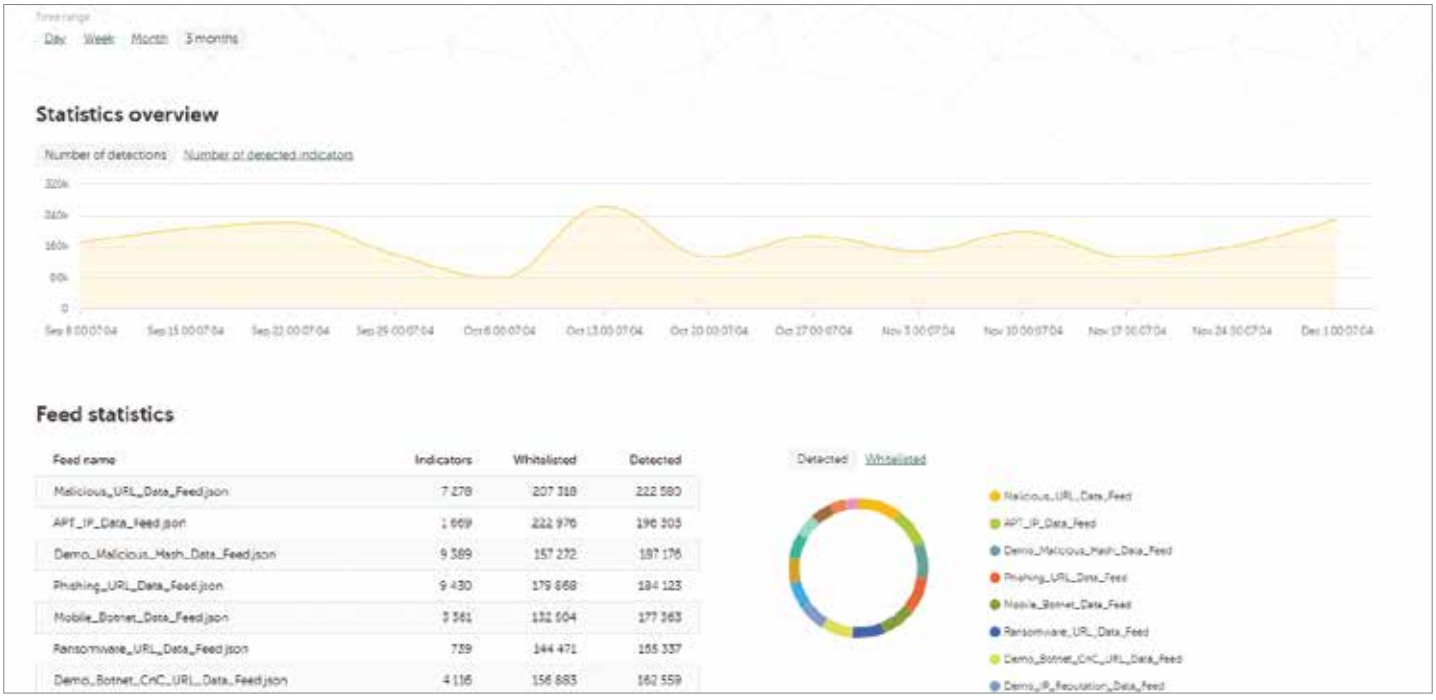


図 12：
Kaspersky CyberTrace の統計データ

Kaspersky CyberTrace は、効果的なアラートのトリアージと初期対応を行うために脅威インテリジェンスを運用できるようにするための以下の一連のツールを提供します：

- Kaspersky からのデモ用の脅威データフィードと OSINT フィードはすぐに利用可能
- 脅威の検知に関するデータを視覚化して管理するための、幅広い SIEM ソリューション用の SIEM コネクタ
- 統合されたフィードの有効性を測定するためのフィード利用統計データ
- 詳細な脅威調査のための痕跡（ハッシュ値、IP アドレス、ドメイン、URL）のオンデマンド検索
- データを視覚化し、設定、フィード管理、ログ解析ルール、ブラックリスト、ホワイトリストにアクセスするための Web ユーザーインターフェイス

- フィードの高度なフィルタリング（脅威の種別、地理位置情報、知名度、タイムスタンプなどの痕跡のそれぞれについて提供されるコンテキスト情報に基づく）およびログイベント（カスタムの条件に基づく）
- 他のシステム（ファイアウォール、ネットワーク IDS、ホスト IDS、カスタムツール）との統合のためにデータフィードと一致した検索結果を CSV 形式にエクスポートする機能
- ログおよびファイルの一括スキャン
- Windows および Linux プラットフォーム用のコマンドラインインターフェイス
- スタンドアロンモード（Kaspersky CyberTrace が SIEM と統合されない状態で、ネットワーキングデバイスなどの各種ソースのログを受信して解析するモード）
- インターネットからの隔離を必要とする DMZ サポートシナリオでのインストール

このツールは、受信したデータの解析と照合を内部で処理するため、SIEM のワークロードが大幅に削減されます。Kaspersky CyberTrace は受信したログやイベントを解析し、その結果のデータを即座にフィードと照合して、脅威検知に関する独自のアラートを生成します。このソリューションの統合に関するアーキテクチャ概要を以下の図に示します：

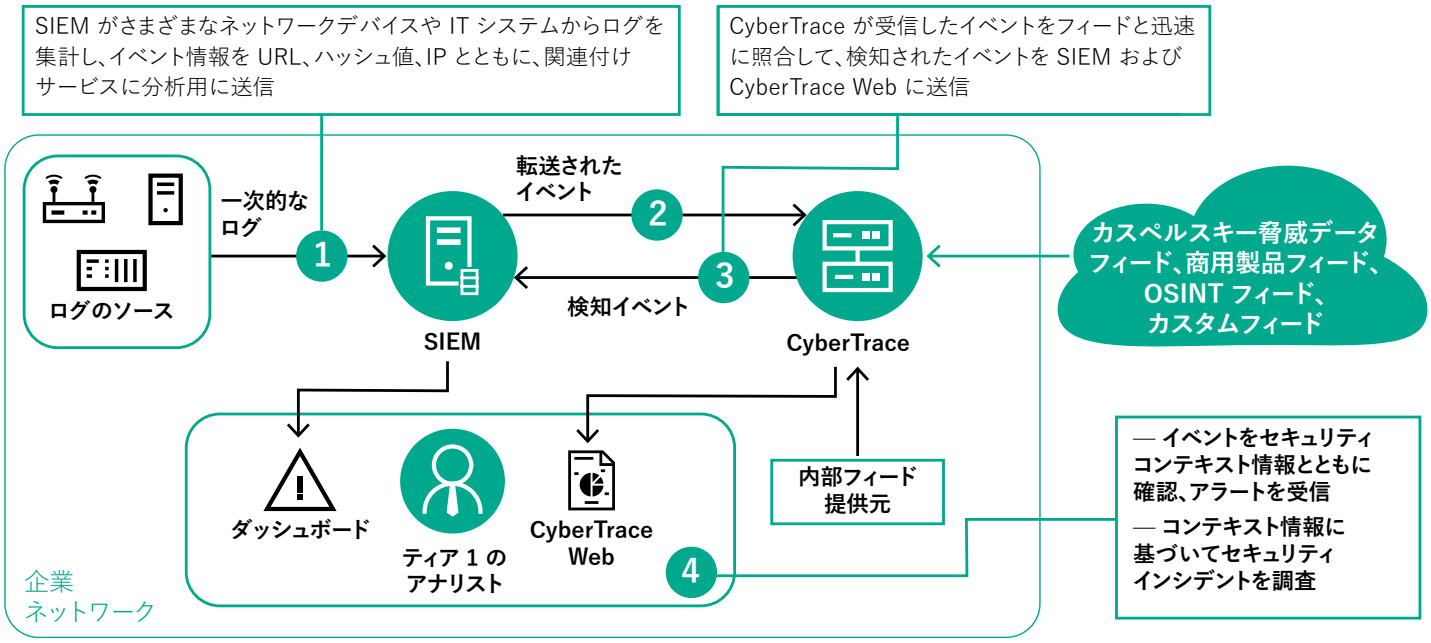


図 13：
Kaspersky CyberTrace の統合スキーム

Kaspersky は Kaspersky CyberTrace との統合が可能な、以下のような常に更新される脅威データフィードも提供しています。脅威データフィードを利用することで、世界中の脅威を可視化し、サイバー脅威を迅速に検知し、セキュリティアラートの優先順位付けを行い、情報セキュリティインシデントに効果的に対応できるようになります：

- IP レピュテーションフィード：疑わしいホストや悪意のあるホストによる異なるカテゴリを対象とした IP アドレスとコンテキスト情報のセット。
- 悪意のある URL およびフィッシング URL フィード：悪意のあるフィッシングリンクおよびフィッシングサイトを対象とします。
- ボットネット C&C URL フィード：デスクトップボットネット C&C サーバーおよび関連する悪意のあるオブジェクトを対象とします。
- モバイルボットネット C&C URL フィード：モバイルボットネット C&C サーバーを対象とします。
- ランサムウェア URL フィード：ランサムウェアオブジェクトをホストするリンクまたはランサムウェアオブジェクトからアクセスされるリンクを対象とします。
- APT IOC フィード：APT 攻撃を実行するために利用される悪意のあるドメイン、ホスト、IP アドレス、ファイルを対象とします。
- パッシブ DNS（pDNS）フィード：ドメインを対応する IP アドレスに DNS 解決した結果を含むレコードのセット[3]。
- IoT URL フィード：IoT デバイスに感染するマルウェアのダウンロードに使われた Web サイトを対象とします[4]。
- 悪意のあるハッシュフィード：もっとも危険かつ蔓延している新しいマルウェアを対象とします。
- モバイル向けの悪意のあるハッシュフィード：Android および iOS 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対象とします。
- P-SMS 型トロイの木馬フィード：SMS メッセージの盗用、削除、応答や、モバイルユーザーへの高額請求を可能にする SMS 型トロイの木馬を対象とします。
- ホワイトリストデータフィード：サードパーティの製品およびサービスについての正規ソフトウェアに関する体系的知識を提供します。

3　統合機能は 2019 年にサポートされる予定

4　統合機能は 2019 年にサポートされる予定

データフィードは、Kaspersky Security Network と、当社とサイバー脅威に関するデータを自ら共有している世界中の 1 億以上のユーザー、当社独自の Web クローラー、ボットネット監視システム（すべての既知のボットネットおよびその標的とアクティビティを 24 時間 365 日監視するシステム）、スパムトラップ、脅威調査チーム、信頼できるパートナーなどの信頼性の高い異種混在のソースを融合して、そこから集積されます。

次に、集積されたすべてのデータがリアルタイムで慎重に調査され、複数の前処理手法によってふるい分けされます。その手法として、統計的な基準、Kaspersky のエキスパートシステム（サンドボックス、ヒューリスティックエンジン、マルチスキャナー、近似ツール、ふるまいプロファイリングなど）、アナリストによる検証、ホワイトリスト検証などが利用されます。

各データフィード内のすべてのレコードに実用的で充実したコンテキスト情報（脅威スコア、地理位置情報、脅威名、タイムスタンプ、感染した Web リソースの解決済み IP アドレス、ハッシュ値、知名度など）が付加されます。

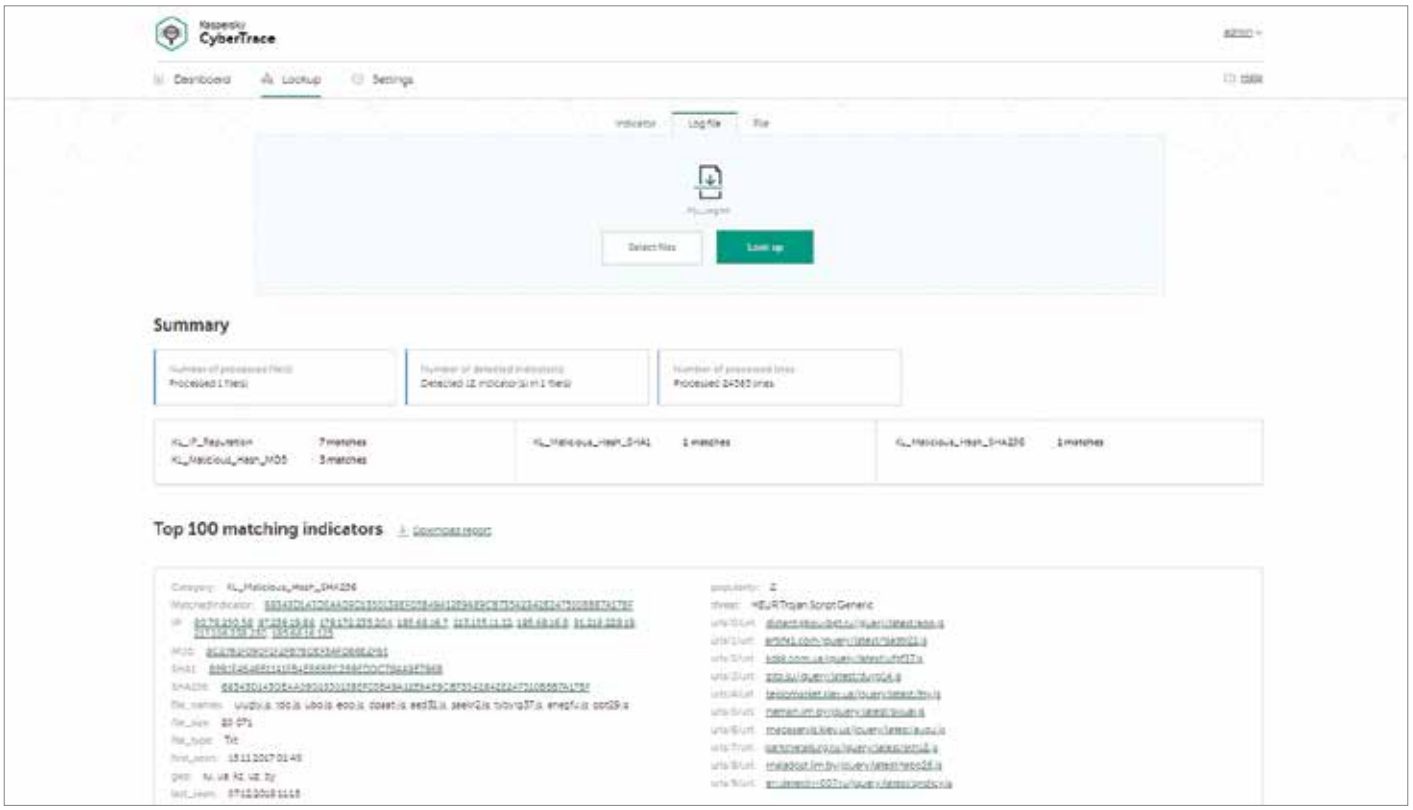


図 14：
Kaspersky Threat Data Feedsの
コンテキスト情報

このコンテキスト情報によって「より広い視野」が得られ、その後の検証や、幅広いデータの利用法が可能になります。データをコンテキスト情報とともに考察することで、「誰が、何を、どこで、いつ」という疑問に答えることが簡単になり、その結果、攻撃者を特定して、適切な意思決定を下すことができます。

Kaspersky CyberTrace と Kaspersky Threat Data Feeds は個別に利用できますが、併用することで脅威検知能力を大幅に強化することができ、セキュリティ運用においてサイバー脅威のグローバルな動向を把握できるようになります。Kaspersky CyberTrace と Kaspersky Threat Data Feeds によって、セキュリティオペレーションセンターのアナリストは以下のことを実行できるようになります：

- 大量のセキュリティアラートを効果的に抽出し、優先順位を付ける
- トリアージと初期対応プロセスの質を高め、迅速化する
- 企業にとって重大なアラートを即座に特定し、IR チームにエスカレートすべき問題について、より良い情報を得た上で意思決定する
- インテリジェンス主導のプロアクティブ防御を行う

Kaspersky のソリューション：カスペルスキー脅威インテリジェンスポータル（Threat LookupとCloud Sandbox）

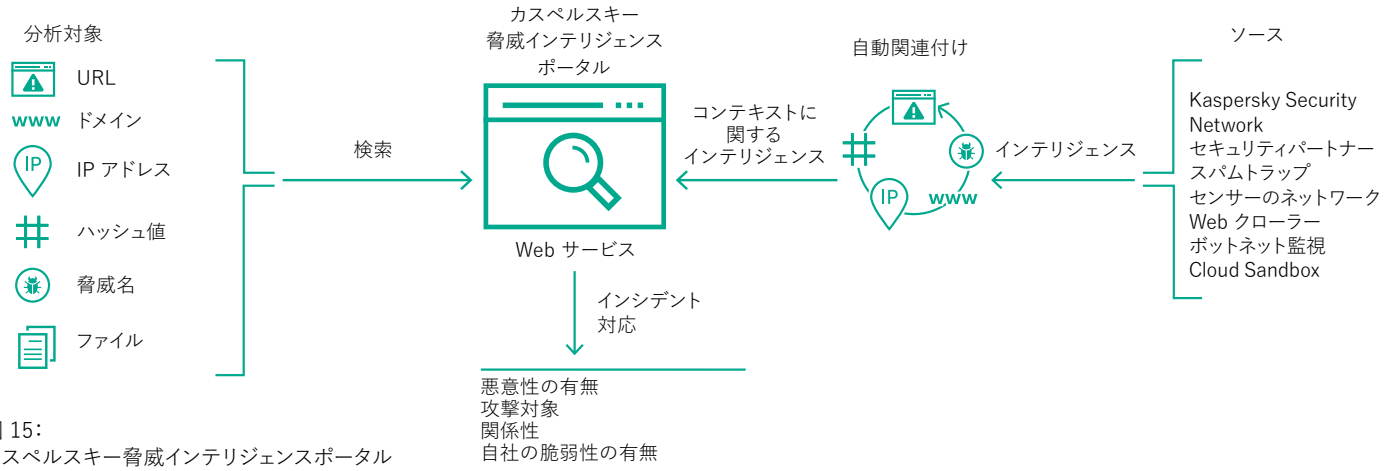


図 15：
カスペルスキー脅威インテリジェンスポータル

サービスの概要

- **信頼できるインテリジェンス：**カスペルスキー脅威インテリジェンスポータルの主な特徴として、脅威インテリジェンスデータの信頼性が高く、実用的なコンテキスト情報が付属していることが挙げられます。カスペルスキー製品はアンチマルウェアテスト[5]の分野でトップの評価を獲得しており、セキュリティインテリジェンスデータの比類のない質の高さが最高水準の検知率と極めて低い誤検知率によって実証されています。
- **脅威ハンティング：**先を見越した予防、検知、対処を行うことで、攻撃の影響や頻度を最小限に抑えることができます。可能な限り早期に攻撃を追跡し、積極的に排除します。脅威の発見が早いほど与えられるダメージも小さく、速やかに修復して、ネットワーク運用を通常状態に戻すことができます。
- **サンドボックス分析：**疑わしいオブジェクトを安全な環境内で実行することで未知の脅威を検知します。脅威のふるまいとアーティファクトの全体像をわかりやすいレポートで確認できます。
- **さまざまなエクスポートフォーマット：**不正アクセスの痕跡（IOC）や実用的なコンテキスト情報を、広範に利用され系統化された機械判読可能な共有フォーマット（STIX、OpenIOC、JSON、Yara、Snortのほか CSV にも対応）にエクスポートできるため、脅威インテリジェンスの十分な活用、運用ワークフローの自動化、SIEM などのセキュリティ管理システムへの統合が可能です。
- **使いやすい Web インターフェイス、RESTful API：**このサービスは、Web インターフェイス（Webブラウザー）経由で手動モードで利用することも、簡潔な RESTful API 経由でアクセスすることもできます。

カスペルスキー脅威インテリジェンスポータルは、サイバー脅威に関して Kaspersky が収集し続けているすべてのデータとそれらの間にある相互関係を単一の強力な Web サービスにまとめたものです。お客様の SOC チームに対して、影響を受ける前にサイバー攻撃を防止できるよう、可能な限り多くのデータを提供することを目的としています。ポータルが URL、ドメイン、IP アドレス、ファイルハッシュ値、脅威名、統計的データまたはふるまいデータ、WHOIS データ、DNS データ、ファイル属性、地理位置情報データ、ダウンロードチェーン、タイムスタンプなどに関する最新の脅威インテリジェンスの詳細情報を引き出すものであるのに対して、クラウドサンドボックスは、その知識を、分析対象サンプルによって生成された IOC に関連付けるものです。その結果、新しい脅威のグローバルな動向を把握し、組織の保護とインシデント対応能力の強化に役立てることができます。

カスペルスキー脅威インテリジェンスポータルによって提供される脅威インテリジェンスは耐障害性の高いインフラストラクチャによってリアルタイムで生成、監視されており、継続的可用性と一貫したパフォーマンスが確保されています。世界中のセキュリティアナリスト、世界的に著名な GReAT チームや最先端の研究開発チームのセキュリティエキスパートなど、数百人に及ぶ専門家が、実態に即した価値ある脅威インテリジェンスの生成に携わっています。

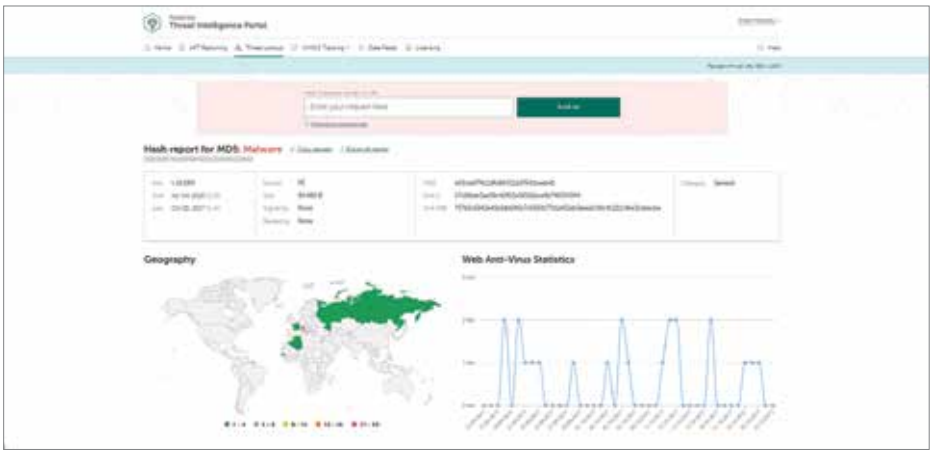


図 16：
カスペルスキー脅威インテリジェンスポータル

5 http://www.kaspersky.com/top3

Kaspersky のソリューション：APT インテリジェンスレポート

発見されるすべての Advanced Persistent Threat（APT）が即座に報告されるわけではなく、多くは公表されないままになります。APT に関する詳細かつ実用的な Kaspersky のインテリジェンスレポートを通じて、誰よりも早く最新の調査結果を手に入れましょう。

Kaspersky の調査

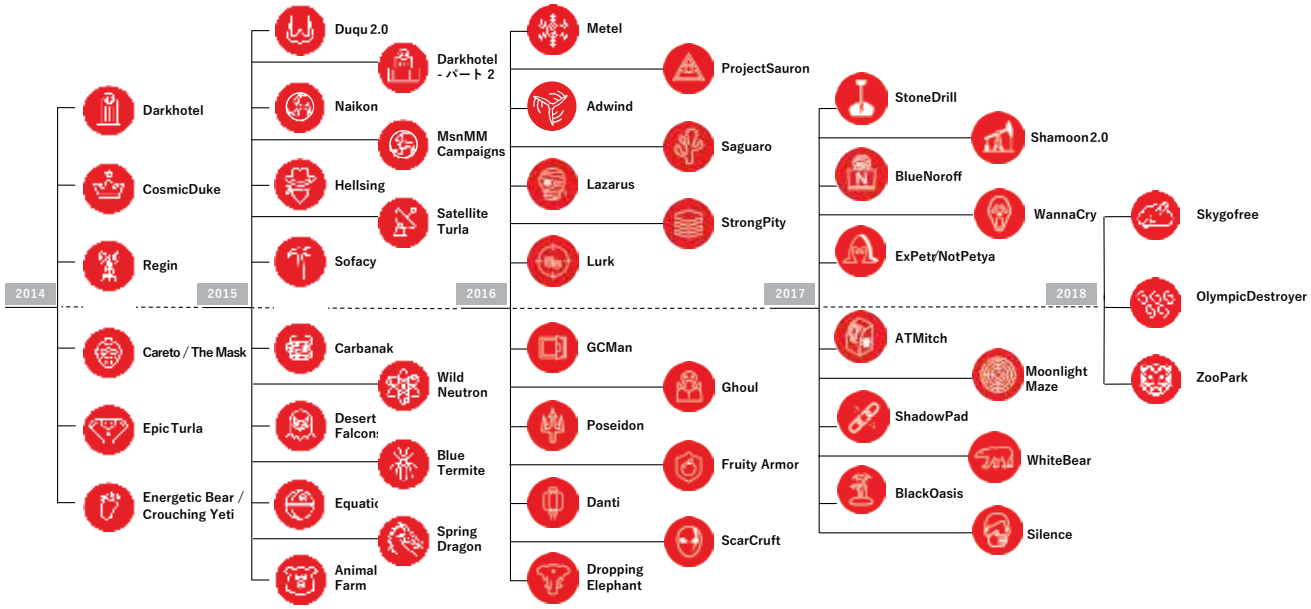


図 17：
Kaspersky が過去に公開した APT 調査

サービスの概要

- 専用アクセス：最先端の脅威に関する技術的な情報を、公開前の調査段階で入手できます。2017 年には 100 以上の APT レポートが発行されました。
- 非公開の APT 情報：注目を集めるすべての脅威が公開の対象となるわけではありません。攻撃を受けた組織やデータの機密性、脆弱性解消プロセスの性質、または関連する警察の活動が原因となって、公開されない脅威もあります。しかし、カスペルスキー APT インテリジェンスレポートの利用者には、すべての脅威が報告されます。
- 詳細な関連情報：OpenIOC 形式で提供される不正アクセスの痕跡（IOC）の広範なリストを含むテクニカルデータに加えて、Yara ルールへのアクセスを提供します。
- 継続的な APT 活動の監視：実用的なインテリジェンスに調査段階でアクセスできます（APT 分類、IOC、C&C インフラストラクチャに関する情報）。
- 遡及的分析：サブスクリプション期間中はずっと、以前に発行されたすべてのプライベートレポートにアクセスできます。

カスペルスキー APT インテリジェンスレポートの利用者は、発見されたすべての APT に関して、幅広い形式で提供される完全なテクニカルデータを含む Kaspersky の調査および発見結果に継続的にアクセスできます。これには、公開されることのない脅威もすべて含まれています。Kaspersky のエキスパートは、業界でもっとも高いスキルと実績を持つ APT 発見者であり、サイバー犯罪者グループが戦術を変更した場合は、ただちにお客様に警告を送ります。さらに、お客様は、企業のセキュリティ戦略にとってより一層の強力な研究および分析コンポーネントとなる、Kaspersky の APT レポートデータベース全体にアクセスできます。

SOC エキスパートにとってこのレポートのもっとも実用的な箇所は、不正アクセスの痕跡（IOC）です。この構造化された情報は、後続の特定の自動化ツールで利用するためのものであり、インフラストラクチャの感染の兆候を確認するために役立ちます。

すべてのレポートは Web インターフェイスで参照するか、RESTful API 経由でアクセスできます。

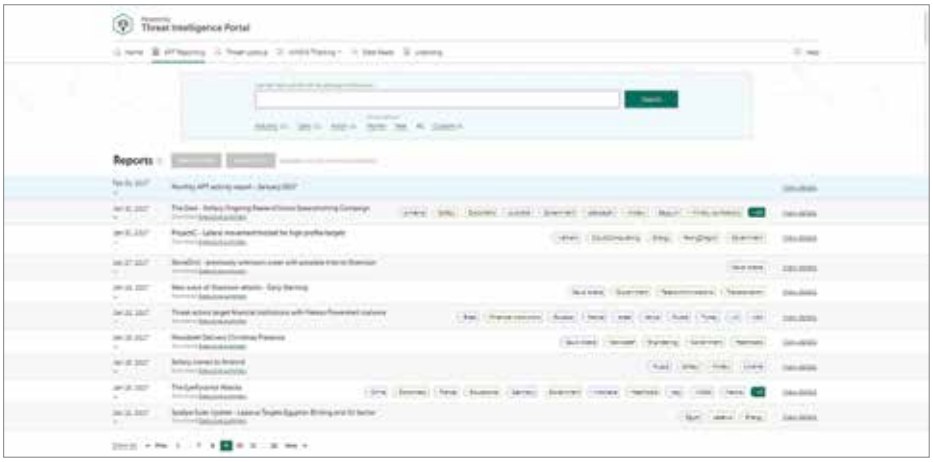


図 18：
APT インテリジェンスレポート

Kaspersky のソリューション：個別インテリジェンスレポート

お客様専用の脅威インテリジェンスレポート

組織に攻撃を仕掛けるためにもっとも有効な方法は何でしょうか。標的を絞った攻撃者は、どのような経路と情報を利用できるでしょうか。すでに攻撃が開始されているか、または攻撃の脅威にさらされつつあるでしょうか。

個別インテリジェンスレポートは、これらの疑問に答えるだけにとどまりません。Kaspersky のエキスパートが現在の攻撃状況を総合的につなぎ合わせて、悪用可能な弱点を特定し、過去 / 現在 / 将来の攻撃の痕跡を明らかにします。

お客様は提供される固有の情報を活用して、サイバー犯罪者の一番の標的として特定された領域を重視した防御戦略を策定し、迅速かつ正確な行動で侵入者を撃退し、攻撃が成功するリスクを最小限に抑えることができます。

オープンソースインテリジェンス（OSINT）や、Kaspersky のエキスパートシステムおよびデータベースによる詳細分析、アンダーグラウンドのサイバー犯罪ネットワークに関する知識を利用して開発されたインテリジェンスレポートは、以下の領域を対象としています：

- 攻撃経路の識別：外部から利用でき、攻撃の対象となりうるネットワーク上の重要コンポーネント（ATM、モバイル技術を使ったビデオ監視などのシステム、従業員のソーシャルネットワークプロファイルと個人用メールアカウントなど）を特定し、その状況を分析します。
- マルウェアとサイバー攻撃の追跡分析：お客様の組織を標的とするマルウェアサンプル（活動中 / 非活動中）、過去または現在のボットネット動作、ネットワークベースの疑わしい動作のすべてを識別、監視、分析します。
- 第三者による攻撃：お客様の顧客、パートナー、サービス利用者を明確に標的とした脅威やボットネット動作がある場合、感染システムが攻撃に使われる可能性があるため、その痕跡を確認します。
- 情報漏洩：アンダーグラウンドのオンラインフォーラムやコミュニティを慎重に監視することで、ハッカーがお客様を念頭に置いた攻撃計画を話し合っているか、たとえば不誠実な従業員が情報を売買しているかどうかを突き止めます。
- 現在の攻撃ステータス：APT 攻撃は、何年にもわたって気付かれることなく継続される場合があります。お客様のインフラストラクチャに影響を与えている現在の攻撃を検知した場合、有効な修復手順をアドバイスします。

クイックスタート - リソース不要の使いやすさ

パラメータ（お客様専用レポート用）とデータ形式がいったん決まったら、Kaspersky のサービスを使い始めるためにインフラを追加する必要はありません。

カスペルスキー脅威インテリジェンスレポートは、ネットワークリソースを含むリソースの整合性と可用性にまったく影響を与えません。

各国固有の脅威インテリジェンスレポート

国家のサイバーセキュリティは、そのすべての主要機関および組織の保護により成り立ちます。政府当局への APT（Advanced Persistent Threat）は国家の安全に影響を及ぼします。製造、輸送、通信、銀行、その他の中枢産業に対してサイバー攻撃が行われれば、財務的損失、製造工程での事故、ネットワーク通信障害、一般市民の不満など、国全体にとって大きなダメージになる可能性もあります。

国を標的としたマルウェアやハッカーの攻撃について、現在の攻撃対象領域と傾向を大まかに知っておくことで、サイバー犯罪者の第一の標的とされる領域を重視した防御戦略を策定し、迅速かつ正確な行動によって侵入者を撃退し、攻撃が成功するリスクを最小限に抑えることができます。

オープンソースインテリジェンス（OSINT）や、Kaspersky のエキスパートシステムおよびデータベースによる詳細分析、アンダーグラウンドのサイバー犯罪ネットワークに関する知識を使って作成された各国固有の脅威レポートは、以下の領域を対象としています：

- **攻撃経路の識別：**政府の脆弱なアプリケーション、通信機器、産業用制御システムのコンポーネント（SCADA、PLC など）、ATM など、外部からアクセス可能な国の重要 IT リソースを特定して、そのステータスを分析します。

- **マルウェアとサイバー攻撃の追跡分析:**APT 活動、マルウェアサンプル(活動中 / 非活動中)、過去または現在のボットネット動作、国を標的としたその他の重大な脅威を、Kaspersky 独自の内部監視リソースのデータに基づいて識別、分析します。

- **情報漏洩:**アンダーグラウンドのフォーラムやオンラインコミュニティを秘密裏に監視することで、ハッカーが特定組織を念頭に置いた攻撃計画を話し合っているかを突き止めます。また、標的の組織や機関にとってリスクになりうる、重大なアカウント侵害についても明らかにします(たとえば、不倫サイト「Ashley Madison」で情報が漏洩した政府職員のアカウント。この情報は脅迫に利用される恐れがあります)。

カスペルスキー脅威インテリジェンスレポートは、調査対象のネットワークリソースの整合性と可用性にまったく影響を与えません。このサービスは、ネットワークを阻害しない偵察手法と、オープンソースで入手できる情報の分析、およびアクセスが制限されているリソースに基づいています。

このサービスでは最終的に、それぞれの国営産業や国家機関にとって重大な脅威に関する説明、および詳しい技術分析結果に関する追加情報を含むレポートが提供されます。レポートは暗号化されたメールメッセージによって配信されます。

当サービスは、一度のプロジェクトとして、またはサブスクリプションに基づいて定期的(例:四半期ごと)に利用できます。

カスペルスキー脅威インテリジェンスの提供元に関する詳細

脅威インテリジェンスは、Kaspersky Security Network(KSN)、当社独自の Web クローラー、ボットネット監視システム(ボットネットおよびその標的とアクティビティを 24 時間 365 日監視するシステム)、スパムトラップ、調査チーム、パートナー、Kaspersky が約 20 年にわたって収集した悪意のあるオブジェクトに関するその他の履歴データなどの信頼性の高い異種混在のソースを融合して、そこから集積されます。次に、集積されたすべてのデータがリアルタイムで慎重に調査され、複数の前処理手法によってふるい分けされます。その手法として、統計的な基準、Kaspersky のエキスパートシステム(サンドボックス、ヒューリスティックエンジン、近似ツール、ふるまいプロファイリングなど)、アナリストによる検証、ホワイトリスト検証などが利用されます。

適切なスキルを持ち訓練を受けた担当者を配置し、脅威インテリジェンスを信頼できるソースから収集して既存のセキュリティコントロール内に導入すれば、次に検討すべきことはインシデント対応です。

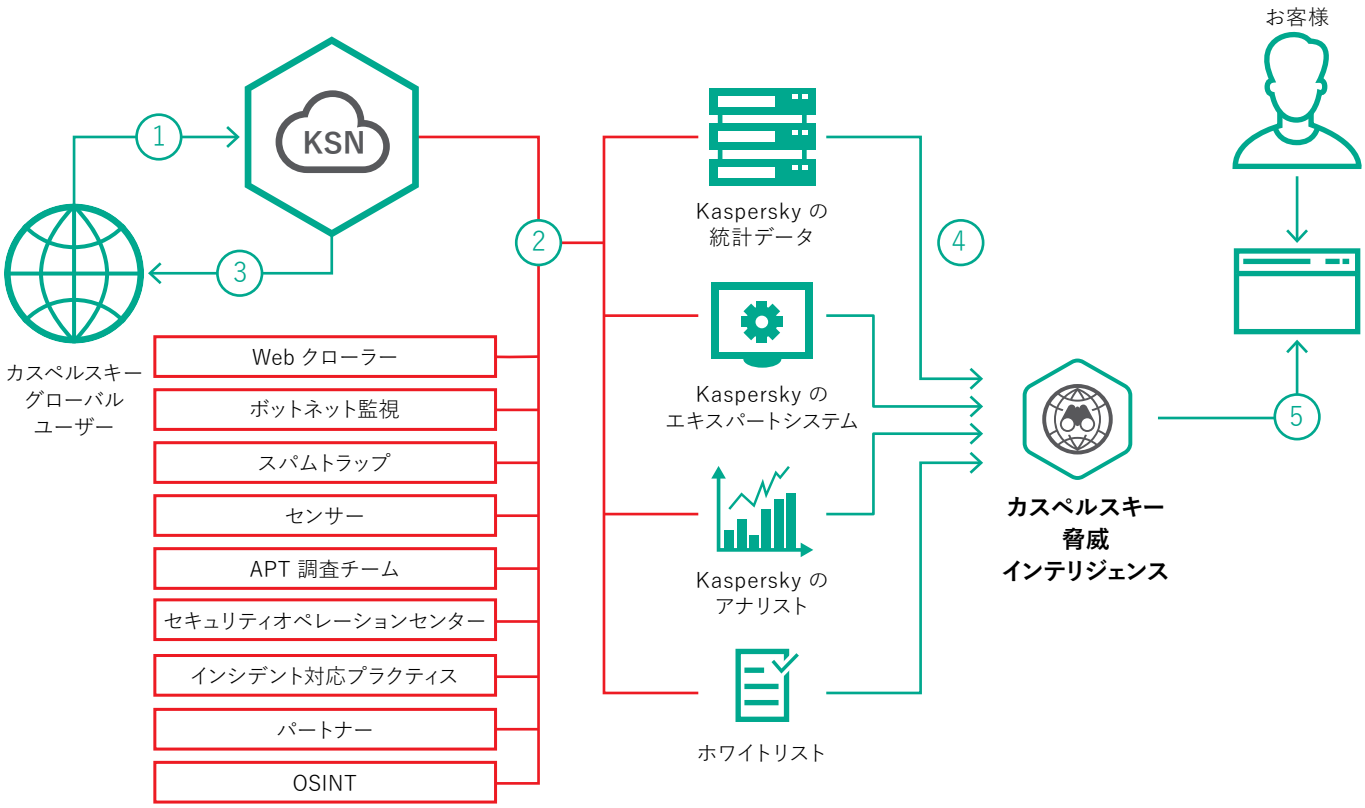


図 19:
カスペルスキー脅威インテリジェンスの提供元

脅威ハンティング

脅威ハンティングも毎日の SOC の業務における重要な要素です。これ自体は新しい考え方ではありません。未知の高度な脅威を検知できるかは、自動化されたルールやシグネチャベース検知のメカニズムよりも、セキュリティアナリストの現場での忍耐強い努力にかかっています。

最新の攻撃は、標的が利用できる保護ツールについて考慮した上で、自動検知および防止システムを迂回するように開発されています。この種の攻撃はソフトウェアを一切利用せずに実行されることが多く、攻撃者の操作は IT セキュリティや情報セキュリティの責任者が行う操作とほとんど見分けがつきません。最近の攻撃で利用されているテクニックの一例を以下で説明します：

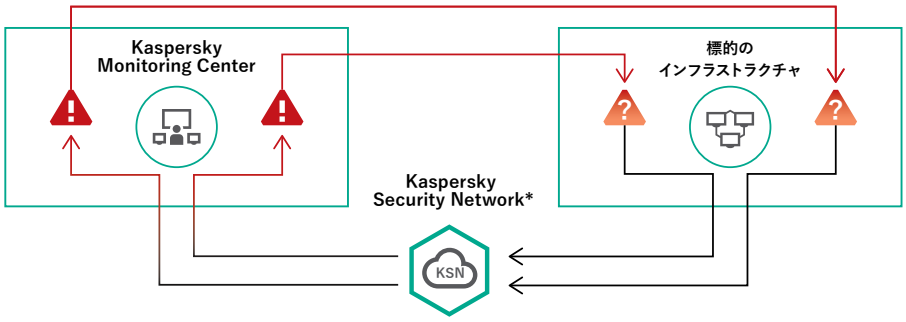
- デジタルフォレンジックを妨害するツールの利用（例：ハードディスク上のアーティ　ファクトを確実に削除する、コンピューターのメモリ内のみで攻撃を実施する）
- IT 部門や情報セキュリティ部門が日常的に利用する正規のツールの利用
- 多段階攻撃（前段階までの痕跡を確実に削除する）
- 専門家チームによる対話型操作（侵入テスト中に利用される方法に類似）

この種の攻撃は、標的の資産が侵害されるまでは検知できず、そのタイミングで初めて、悪意のある操作の存在を示す疑わしいふるまいが検知されます。脅威ハンティングは、初期の侵害の発生後に攻撃を検知できます。重要なのは、意思決定の最終段階でプロのアナリストを関わらせることです。一連のイベント分析の最中に人が関わることで、自動による脅威検知ロジックの弱い点を補うことができます。さらに、侵入テストのような攻撃で、攻撃側に人が関わっている場合、自動技術を迂回するという点ではその人が有利であることは間違いありません。そのため、人のアナリストがいることが、この種の攻撃に耐えるための唯一の手段になります。

ただし、脅威の自動検知および防止ツールも、サイバー脅威ハンティングも、単独ではここ最近の脅威スペクトラム全体に対して万全ではありません。侵害が発生する前に従来型の検知および防止ツールを配備し、さらに侵害が発生した後に、自動ツールでは発見されなかった新たな脅威を探し出す反復型のプロセスを組み合わせることが有効な手段になります。

Kaspersky のソリューション：Kaspersky Managed Protection

Kaspersky Managed Protection サービスは Kaspersky Endpoint Security と Kaspersky Anti Targeted Attack Platform のユーザーに提供される完全マネージドサービスであり、独自の幅広く高度な技術的手段によって、お客様の組織に対する標的型攻撃を検知し、阻止します。このサービスには、Kaspersky のエキスパートによる 24 時間の監視、およびサイバー脅威データの継続的分析が含まれており、重要な情報システムを標的とした既知、新規両方のサイバースパイ活動およびサイバー犯罪活動をリアルタイムで検知します。



*隔離されたインフラストラクチャの場合は Kaspersky Private Security Network

図 20：
Kaspersky Managed Protection

サービスのメリット

- 高速で効率的な検知によって、より迅速で効果的な緩和と修復が可能になります。
- 疑わしい動作を明確、即座に特定し分類できるため、時間のかかる誤検知が発生しません。
- セキュリティコストの総額を削減します。自社内に各種専門家を雇用しトレーニングする必要がありません。
- もっとも複雑で革新的な非マルウェアの脅威に対しても常に保護されているという安心が手に入ります。
- 攻撃者、その動機、手法、ツール、潜在的な損害について洞察し、十分な情報を得た上で効果的な保護戦略を策定することができます。

サービスの概要

- 24 時間 365 日の監視と、お客様専用の Kaspersky エキスパートによる「クラッキングチーム」のサポートを受けながら、幅広い技術者のスキルと現在も発展中の脅威インテリジェンスを利用して、標的型攻撃とマルウェアから継続的に高いレベルで保護します。
- 非マルウェア攻撃、未知のツールが関係する攻撃、ゼロデイ脆弱性を利用した攻撃を、迅速かつ正確に検知します。
- 検知された脅威からは、アンチウイルスの定義データベースの自動アップデートによって迅速に保護します。
- お客様に対してサイバー犯罪組織が利用した手法な技術を含め、インシデントの遡及的分析と脅威ハンティングを行います。
- 統合アプローチ：Kaspersky のポートフォリオには、準備、検知、調査、データ分析、自動保護という標的型攻撃からの保護サイクル全体を導入するために必要なすべての技術とサービスが含まれています。

インシデントの調査と対応

フォレンジックおよびインシデント対応では、かなりの社内リソースをほぼ事前の通知なしに割り当てる必要があります。サイバー脅威に立ち向かうための実務経験を積んだ豊富な知識を持つ技術者が、悪意のある活動を識別、隔離、ブロックするためにすばやく行動する必要があります。結果の重大性や修復コストを最小限に抑えるには、スピードが肝心です。

このレベルの専門知識をすぐに習得することは、安定した SOC チームであっても難しいものです。高度な攻撃をその場で阻止できる十分な社内リソースのある組織は多くありません。さらに、国家支援による複雑な脅威や APT などのケースもあり、その場合 SOC チームには、関係する APT グループが利用している固有のアプローチや戦術に関する専門知識が不足しています。

これらのケースでは、サードパーティのインシデント対応ベンダーやコンサルティング企業と協力する方が費用効果と生産性の面で優れている場合があります。それらの企業では、十分な情報に基づいた迅速な対応をする態勢が整っているからです。

包括的なインシデント対応フレームワークには以下の項目が含まれる必要があります：

- **インシデントの特定**
  初期インシデント分析および感染したシステムの隔離
- **痕跡の収集**
  インシデントの種別に応じて、必要な痕跡を入手するために各種ソースを確実に調査
- **フォレンジック分析（必要に応じて）**
  この段階で、インシデントの詳細なイメージを確立可能
- **マルウェア分析（必要に応じて）**
  対象のマルウェアの能力について把握
- **修復計画**
  問題の根本原因と悪意のあるコードのすべての痕跡を除去するための計画策定
- **知識獲得**
  既存のセキュリティコントロールの見直し、更新により、同様のインシデントを予防

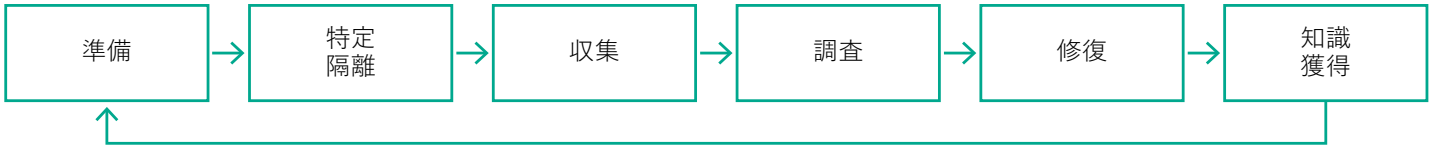


図 21：
インシデント対応フレームワーク

Kaspersky のソリューション：Incident Response Services

Incident Response Services は、インシデント調査サイクル全体を対象とした当社のプレミアムサービスです。オンサイトでの形跡の収集から、他の不正アクセスの痕跡（IOC）の特定、修復計画の準備、お客様の組織に対する脅威の根絶までを対応します。Kaspersky の調査は、経験豊かなサイバー侵入検知アナリスト / 調査担当者が実施します。デジタルフォレンジックとマルウェア分析における当社のグローバルな専門知識のすべてが、お客様のセキュリティインシデントの解決に向けて集結します。

このサービスでは、以下の目標の達成を目指します：

- 侵害されたリソースの特定
- 脅威の隔離
- 攻撃の拡散の阻止
- 痕跡の発見と収集
- 痕跡の分析、インシデントの時系列とロジックの再現
- 攻撃に使われたマルウェアの分析（マルウェアが発見された場合）
- 攻撃元、その他の侵害されている可能性のあるシステムの明確化（可能な場合）
- ツールの支援を受けた IT インフラストラクチャのスキャンによる侵害の兆候の明確化
- 社内ネットワークと外部リソース間の外部向け接続の分析による、疑わしいものの検知（コマンドアンドコントロールサーバーの可能性など）
- 脅威の除去
- 今後とり得る修復措置の推奨

お客様独自のインシデント対応チームの有無に応じて、Kaspersky のエキスパートが調査サイクル全体を実施することも、侵害されたマシンの特定、隔離と脅威の拡散防止、またはマルウェア分析やデジタルフォレンジックのみを実施することもできます。

マルウェア分析

マルウェア分析の目的は、組織を標的とした特定のマルウェアファイルのふるまいと目的を完全に理解することです。Kaspersky のエキスパートは、提供されたマルウェアサンプルを徹底的に分析し、以下の内容を含む詳細レポートを作成します：

- サンプルの特性：サンプルについて簡単に説明し、マルウェアの分類について判定します。
- マルウェアの詳しい説明：マルウェアサンプルの役割と脅威のふるまいおよび目的（IOC を含む）を詳しく分析し、その活動を無害化するために必要な情報を提供します。
- 修復シナリオ：この種別の脅威から組織を完全に保護するための手段を提案します。

デジタルフォレンジック

前述のとおり、調査中に何らかのマルウェアが発見された場合、デジタルフォレンジックにマルウェア分析を含めることができます。Kaspersky のエキスパートは、HDD イメージ、メモリダンプ、ネットワークトレースなどを利用して形跡をつなぎ合わせ、何が起きているのかを正確に理解します。その結果として、詳細なインシデントの説明を提供します。お客様は最初に、形跡を収集しインシデントの概要をまとめます。Kaspersky はインシデントの症状を分析し、マルウェアバイナリ（ある場合）を特定し、マルウェア分析を実施して、修復手順を含む詳細レポートを提供します。

提供方法

Kaspersky Incident Response Services で利用できるオプションは以下のとおりです：

- 定額制
- 個々のインシデントへの対応

いずれのオプションも、Kaspersky のエキスパートがインシデントの解決にかける時間に基づいて計算されます。その時間については、契約前にお客様と協議の上、決定されます。お客様は、必要と思われる作業時間を含めることも、個々のケースに合わせて Kaspersky のエキスパートが推奨する時間に従うこともできます。

侵入テストとレッドチーム演習

サイバー攻撃から IT インフラを完全に守ることは、すべての組織にとって継続的な課題ですが、数千名の従業員と数百の IT システム、世界各地に拠点を持つ大企業にとってはなおさら重要です。セキュリティ体制を強化するためにエキスパートが推奨していることは、Web アプリケーションのセキュリティ、脆弱なソフトウェアの迅速なアップデート、パスワードによる保護、ファイアウォールのルール設定に対して特に注意を払うことです。また、IT インフラ（アプリケーションを含む）の定期的なセキュリティ評価を実施することも非常に重要です。

情報リソースの侵害を完全に防止することは、大規模なネットワークでは極めて難しく、ゼロデイ脆弱性を使って攻撃が開始された場合、それは不可能にもなります。このために、情報セキュリティインシデントをできるだけ早く検知するためのあらゆる対策を講じることが不可欠です。攻撃の早い段階でサイバー犯罪組織の活動を迅速に検知してすぐに対応することが、あらゆる損害を防ぐ、または大幅に軽減することにつながります。お客様がセキュリティ評価、脆弱性管理、情報セキュリティインシデントの検知についての安定したプロセスを配備した成熟した企業である場合は、レッドチーム演習タイプのテストを実施することを検討してください。このテストでは、スキルの高い攻撃者が最大限のステルス性で活動する場合にインフラがどの程度保護されるかを調査します。実態に即した状況での攻撃の特定と対応について、IT セキュリティチームをトレーニングすることもできます。

Kaspersky のソリューション：Penetration Testing

Kaspersky Penetration Testingは、インフラに含まれるセキュリティ上の不具合に関する詳しい情報を提供し、脆弱性を明らかにして、攻撃の形態別に生じうる結果を分析します。また、現在のセキュリティ対策の有効性を評価し、修復措置と改善点を提案します。

Penetration Testingを利用するメリットは以下のとおりです：

- ネットワーク内の顕著な弱点を識別することで、お客様が全面的に十分な情報に基づいて、将来的なリスクを軽減するためにどこに注意と予算を集中させるかを決定できるように支援します。
- サイバー攻撃によって財政、業務、評判に損害が及ぶことを防止するため、脆弱性を事前に発見および修正することで、攻撃の開始を予防します。
- この形式でのセキュリティ評価を必要とする政府、業界、社内の標準（クレジットカード業界のデータセキュリティ標準（PCI DSS）など）に準拠します。

サービスの範囲とオプション

お客様の要件と IT インフラに応じて、以下のいずれか（またはすべて）のサービスを利用できます：

- 外部侵入テスト：インターネットを介して、お客様のシステムに関する予備知識のない「攻撃者」によって実施されるセキュリティ評価
- 内部侵入テスト：オフィスに物理的にアクセスできるだけの訪問者や、システムアクセスが制限された請負業者などの、内部攻撃者に基づくシナリオ
- ソーシャルエンジニアリングテスト：フィッシング、メール内の悪意ある偽リンク、疑わしい添付ファイルなどの、ソーシャルエンジニアリング攻撃のエミュレートによる、従業員のセキュリティ認識に対する評価
- 無線ネットワークのセキュリティ評価：Kaspersky のエキスパートによる実地での WiFi セキュリティコントロールの分析

侵入テストの範囲には IT インフラのどの部分をも含めることができますが、ネットワーク全体か、少なくとも最大のセグメントを対象とすることを強く推奨します。潜在的な侵入者と同じ条件のもとで分析することで、より意味のあるテスト結果が得られます。

サービスの概要

このサービスの目的は、重要なネットワークコンポーネントへの不正アクセスを獲得するために悪用可能なセキュリティ上の弱点を明らかにすることです。以下のような弱点が含まれます：

- 脆弱なネットワークアーキテクチャ、不十分なネットワーク保護
- ネットワークトラフィックのインターセプトやリダイレクトにつながる脆弱性
- 各種サービスでの不十分な認証と認可
- 不十分なユーザー認証情報
- ユーザー権限が過剰などの設定の不具合
- アプリケーションコード内のエラーがもたらす脆弱性（コードインジェクション、パストラバーサル、クライアント側の脆弱性など）
- 最新のセキュリティアップデートが適用されていない旧バージョンのハードウェアおよびソフトウェアの利用による脆弱性
- 情報の漏洩

結果は最終レポートで提供され、テストのプロセス、結果、発見された脆弱性、推奨される修復方法に関する詳しい技術情報と、テスト結果のまとめと攻撃経路を示したエグゼクティブサマリーが含まれます。必要に応じて、技術チームまたは経営陣向けのビデオとプレゼンテーションを提供します。

Penetration Testingに対する Kaspersky のアプローチ

Penetration Testing は本物のハッカー攻撃をエミュレートするものですが、これらのテストは、お客様のシステムが持つ機密性、整合性、可用性を十分に考慮した上で、Kaspersky のセキュリティエキスパートによって厳密に制御、実行されるので安心です。また、以下を含む国際的な標準とベストプラクティスに厳密に従って実施されますのでご安心ください：

- Penetration Testing Execution Standard（PTES）
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual（OSSTMM）
- Information Systems Security Assessment Framework（ISSAF）
- Web Application Security Consortium（WASC）Threat Classification
- Open Web Application Security Project（OWASP）Testing Guide
- Common Vulnerability Scoring System（CVSS）

プロジェクトチームのメンバーは、この分野に関する最新で深い実践的知識を持つ、経験豊かな専門家であり、Oracle、Google、Apple、Microsoft、Facebook、PayPal、Siemens、SAP をはじめとする業界リーダーからセキュリティアドバイザとして認められています。

提供方法

セキュリティ評価サービスの種類、システムの特性、業務方法に応じて、セキュリティ評価サービスはリモートまたはオンサイトで提供されます。ほとんどのサービスはリモートで実施可能で、内部侵入テストも VPN アクセス経由で実施できますが、一部のサービス（無線ネットワークのセキュリティ評価など）はオンサイトでの実施が必要です。

Kaspersky のソリューション：レッドチーム演習

このサービスには以下の内容が含まれます：

- **脅威インテリジェンス：**このサービスはまず、お客様の既知の脅威とブルーチームの経験に関するディスカッションから始まります。その目的は、非常に重要なビジネス資産を特定し、企業の防御上の TTP に合わせてプロジェクトの納品物をどのようにカスタマイズできるかについて把握することです。ただし、このディスカッションで Kaspersky が標的のリソースに関する情報提供を依頼することはありません。レッドチームは、実際の攻撃者が行うように、独立した情報収集活動も実施するためです。この情報収集フェーズには、公開されている情報（オープンソースのインテリジェンス）の分析と、アンダーグラウンドコミュニティで入手できるデータの分析が含まれます。

- **攻撃者の行動のシミュレーション：**この段階は、「脅威インテリジェンス」段階の結果を踏まえて、攻撃シナリオとツールを準備することから始まります。この準備には、お客様の環境で使われているシステムの新しい脆弱性を明らかにするための詳細調査、お客様のセキュリティシステムを迂回することを目指したカスタムツールの開発、スピアフィッシング攻撃の準備が含まれます。準備が完了すると、Kaspersky は積極的な「攻撃者の行動のシミュレーション」フェーズを実行します。これらのテストには、場合によって以下の内容が含まれます：

  - 受動的な情報収集
  - ポートスキャン、利用可能なサービスの特定、特定のサービス（DNS、メール）への手動リクエストなどの積極的な情報収集（ネットワークの探索）
  - 外部の脆弱性のスキャンと分析
  - Web アプリケーションセキュリティ（自動、手動の両方のアプローチを利用）による以下の脆弱性の特定：

    – コードインジェクション（SQL インジェクション、OS コマンディングなど）
    – クライアント側の脆弱性（クロスサイトスクリプティング、クロスサイトリクエストフォージェリなど）
    – 認証、認可における不具合
    – 危険なデータの保管
    – WASC Threat Classification v2.0 と OWASP Top 10 に記載された、脅威につながるその他の Web アプリケーションの脆弱性

- 手動の脆弱性分析（認証機能のないリソースの特定、重要な公開情報、不十分なアクセスコントロールなど）
- 認証情報の推測
- ソーシャルエンジニアリングテスト
- 発見した 1 つ以上の脆弱性の利用と権限昇格（可能な場合）

- 取得した権限と上記に挙げたテクニックを使った攻撃の開発(サービスプロバイダーが LAN または重要なネットワークリソース(Active Directory ドメインコントローラ、ビジネスシステム、DBMS など)にアクセスするか、テスト中に利用可能なすべての攻撃手法を試行するまで)

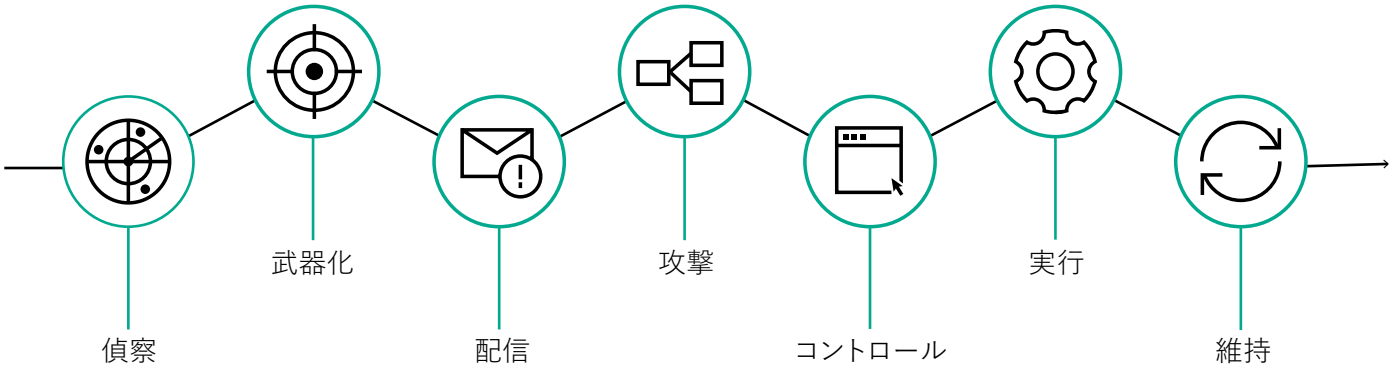


図 22:
攻撃者の行動のシミュレーション

上記のテストは、あらかじめ準備しておいたお客様専用のシナリオに従って、ブルーチームからの検知を回避するための特殊なテクニックを利用しながら実行されます。レッドチームがすべての目標を達成したら、ブルーチームが演習に関われるように、インシデントの検知と対応をトリガーする操作がレッドチームによって実行されます。

- **レポートの作成:** この段階では、Kaspersky が「攻撃者の行動のシミュレーション」の結果を分析し、攻撃の詳細説明(タイムスタンプ、不正アクセスの痕跡(IOC)を含む)と推奨事項を示したレポートを作成します。
- **テスト結果の概要:** プロジェクトの結果、検知や阻止ができなかった理由、防御面で実施可能な改善点を話し合うために、お客様のブルーチームと共同の評価後のワークショップを設けることができます。

アプローチと方法論

レッドチーム演習には、実際のハッカーによる攻撃と共通する点が多く、お客様の現在の保護対策について有効性を評価することができます。しかし、ハッカーの攻撃とは異なり、このサービスは Kaspersky の経験豊かなセキュリティエキスパートが、システムの機密性、整合性、可用性に十分に注意を払い、以下の**国際的な標準とベストプラクティス**に厳密に従って実施します。

- Penetration Testing Execution Standard(PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual(OSSTMM)
- Information Systems Security Assessment Framework(ISSAF)
- Web Application Security Consortium(WASC)Threat Classification
- Open Web Application Security Project(OWASP)Testing Guide
- Common Vulnerability Scoring System(CVSS)
- お客様の事業と地域に応じたその他の標準

分析は自動ツールを利用するほか、エキスパートによって手動で行われます。以下のセキュリティ評価ツールが状況に応じて利用される可能性があります:

- 情報収集ツール(Maltego、theHarvester 他)
- 各種汎用スキャナーおよび専用スキャナー(NMap、MaxPatrol、Nessus、Acunetics WVS、nbtscan 他)
- 複合型セキュリティ評価ソリューション(Kali Linux)
- 認証情報推測ツール(Hydra、ncrack、Bruter 他)
- Web アプリケーションセキュリティ評価用の専用ソリューション(OWASP dirbuster、BurpSuite、ProxyStrike、Mozilla Firefox 用各種プラグイン)
- ネットワークトラフィック分析ツール(Wireshark、Cain and Abel)
- 認証情報の抽出および管理ツール(Mimikatz、WCE、pwdump 他)
- 攻撃の種別に応じた専用ツール(Yersinia、Loki、Responder、SIPVicious 他)
- 逆アセンブル、デバッグツール(IDA Pro、OllyDbg)
- その他、サービスプロバイダーによって開発された制限付きアクセスエクスプロイト、カスタムエクスプロイトツール

レッドチーム演習を法に則って安全に実施するために、お客様はプロジェクトに関するすべてのコミュニケーション用の連絡先（代表者）情報を提供する必要があります。このコミュニケーションには、対象範囲の協議、アクセスの問題の解決、実行中の作業の確認などが含まれます。代表者は、メールアドレスがお客様のドメイン名（サードパーティの中間企業ではなく）に属している正社員である必要があります。

お客様の インシデント対応のリソースの機密性、整合性、可用性を維持することを、Kaspersky はもっとも重視しています。Kaspersky のエキスパートは、お客様の環境に損害が及ぶことがないよう、必要なあらゆる安全対策を講じます。このプロジェクトに関連するすべての技術的な機密情報（重要なデータ、認証情報、評価の結果など）は、強力な暗号化を使って保管、転送されます。プロジェクトの完了後、ご要望に応じてこれらの機密情報を削除することも可能です。

Kaspersky のエキスパートチームのメンバーはセキュリティ評価の経験豊かな専門家であり、この分野に深い知識があり、常にスキル向上を図っています。メンバーはセキュリティ調査の面で、Oracle、Google、Apple、Microsoft、Facebook、PayPal、Siemens、SAP などの業界リーダーから認められています（プロジェクトチームの説明についてはセクション 7 を参照してください）。プロジェクトのチームメンバーの経歴については、提案書に添付されています。

成果

このサービスの利用後に受け取るレポートには以下の内容が含まれます：

- 識別された防御能力に関するまとめと改善のための推奨事項
- 検知された脆弱性の詳細説明（重大度レベル、脆弱性への攻撃の複雑さ、脆弱なシステムに対する影響の可能性、脆弱性の存在の形跡（ある場合）など）
- 分析のための活動の詳細説明（タイムスタンプ、不正アクセスの痕跡（IOC）を含む）と防御チーム側の改善点
- 脆弱性を除去するための推奨事項
- インシデント対応プロセスの改善に関する推奨事項
- 特定された防止、検知の問題の緩和に関する推奨事項

Kaspersky のレッドチーム演習サービスは、お客様の監視能力およびインシデント対応手順の有効性を評価するために役立ちます。

Kaspersky を選ぶ理由

- インターポールや CERT など世界中の法執行機関とのパートナーシップ
- 世界中の何百万ものサイバー脅威をリアルタイムで監視する、クラウドベースのツール
- あらゆるインターネットの脅威を分析、把握しているグローバルチーム
- 脅威インテリジェンスとテクノロジーリーダーシップに重点を置いた、世界最大の独立系セキュリティソフトウェア企業
- 他のどのベンダーよりも多くの第三者評価機関によるマルウェア検知テストで、疑う余地のないトップ企業として選出
- Gartner、Forrester、IDC による「リーダー」評価の獲得

Kaspersky について

Kaspersky は、世界最大の非上場のエンドポイント保護ソリューションベンダーです。全世界でエンドポイントユーザー向けセキュリティソリューションベンダーのトップ 4 にランクインしています。Kaspersky は 21 年以上にわたり、IT セキュリティ市場のイノベーターであり続けており、効果的なデジタルセキュリティソリューションを大企業、中小企業、コンシューマ向けに提供しています。Kaspersky は現在、英国で登記された持ち株会社も含め、世界中のおよそ 200 の国と地域で営業活動を行っており、全世界で 4 億人を超えるユーザーを保護しています。

サイバー脅威に関する最新情報：www.securelist.com
IT セキュリティに関する最新情報：business.kaspersky.com/

www.kaspersky.co.jp

kaspersky BRING ON THE FUTURE

PMM-1048-201911