KASPERSKY lab

SOC POWERED BY KASPERSKY LAB

www.kaspersky.co.jp

企業が自社のセキュリティ体制を向上させても、サイバー犯罪者はそのセキュリティを突破するためのさらに洗練された技術を考案します。サイバー攻撃によって獲得できる収入はこれまでとは桁違いであることから、セキュリティ上の未知のぜい弱性を探し出し、これを標的にしようと、ますます多くのサイバー犯罪者が知力を尽くしています。

そうした中、発生し続けるセキュリティ上の問題と闘うため、また問題に迅速に対応して解決に導くため、セキュリティオペレーションセンター（SOC）の設置が加速しています。

「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重視した設計とし、状況に応じてソリューションを選択できる、包括的かつ適応型のセキュリティアーキテクチャを採用すべきです。セキュリティ部門のトップは、インテリジェンス主導の SOC が最新の脅威から組織を守るために用いることのできるツール、プロセスや戦略を理解することが必要です」

Gartner 社のレポート『The Five Characteristics of an Intelligence-Driven Security Operations Center』（2015 年 11 月）より

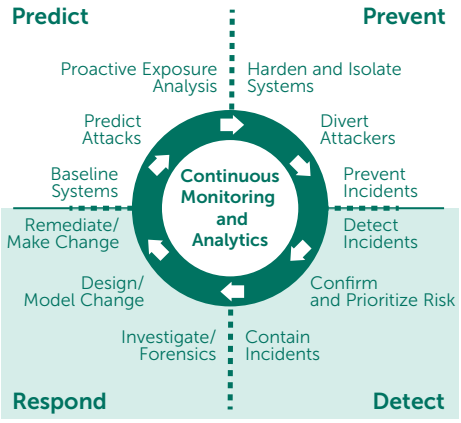
SOC は、サイバー脅威の監視と分析を継続的に実施し、セキュリティインシデントを防止、あるいはリスクを低減するための司令塔です

B2B International 社が世界 25 か国の 4,000 を超える企業を対象に最近実施した調査（2016 年）では、以下のことが明らかになっています：

- 回答者の **38 %** が過去12か月の間に**マルウェアによる重大な事象**を経験し、生産性の低下を招いた。
- **21 %** が**標的型攻撃によるデータの漏洩や損失**を経験。
- 回答者の約 40 % がこうした問題を明確な懸念事項であると指摘。
- **企業の 17 %** が過去 1 年間に **DDoS 攻撃**を複数回経験。
- **フィッシング攻撃**を経験したとの回答の **42 %** は従業員 1,000 名以上の企業であった。
- セキュリティ上の全事象の **26 %** は数週間経っても**検知されず**、外部のセキュリティ監査によって初めて発見されている。
- データ侵害を 1 度以上経験した企業の**財務インパクトは平均で 89 万 1,000 ドル**に及ぶ（新たな社内スタッフの人件費、信用格付けおよび保険料への影響、ビジネスの損失、損なわれたブランドイメージを回復するための新たな宣伝費用、外部コンサルタントの契約費用を含む）。
- 企業が被るこうした財務上の**インパクト**は、データ侵害が検知された時期によって **39 万 3,000〜110 万ドル**の開きがある – 早期検知が低コストに貢献している。
- 漏えいした顧客や従業員の個人情報の件数も、検知時期によって異なる – （現場の検知システムにより）事実上即時検知された場合で 9,000 件、1 年以上検知されなかった場合で 24 万件。

Gartner 社の「適応型セキュリティアーキテクチャ」モデルによれば、現在の脅威レベルにおいてサイバー攻撃に有効に対抗するためには、SOC チームは以下を実現しなければならないとされています：

- 予見
- 防御
- 発見
- 対処



Gartner 社のレポート『Designing an Adaptive Security Architecture for Protection From Advanced Attacks（高度な攻撃からの保護を意図した適応性のあるセキュリティアークテクチャの設計）』（2016 年 1 月）より

3 つの要素

このアプローチを追求していくには、プロセスおよび重要なテクノロジーを明確に定義することに加え、3 つの要素が必要になります。その 3 つの要素とは以下の通りです：

- **人材**（SOC チームメンバー）：ますます洗練されていく攻撃を回避し、これらに対応するための、デジタルフォレンジックおよびマルウェア分析のトレーニングを十分に受けている人材が必要です。
- **脅威インテリジェンス**：脅威を適時検知するためには、以下のようにさまざまな情報源（多いほどよい）から情報を収集することが不可欠です：
    1. 脅威に関する社内データ
    2. オープンソース（OSINT）からの情報
    3. 業界の CERT
    4. グローバルなマルウェア対策ベンダー
- **インシデントレスポンスフレームワーク**：被害を最小限に留め、復旧コストを低減するための枠組みが必要です。

これらの要素はすべて重要で、かつ個別に検討することができます。

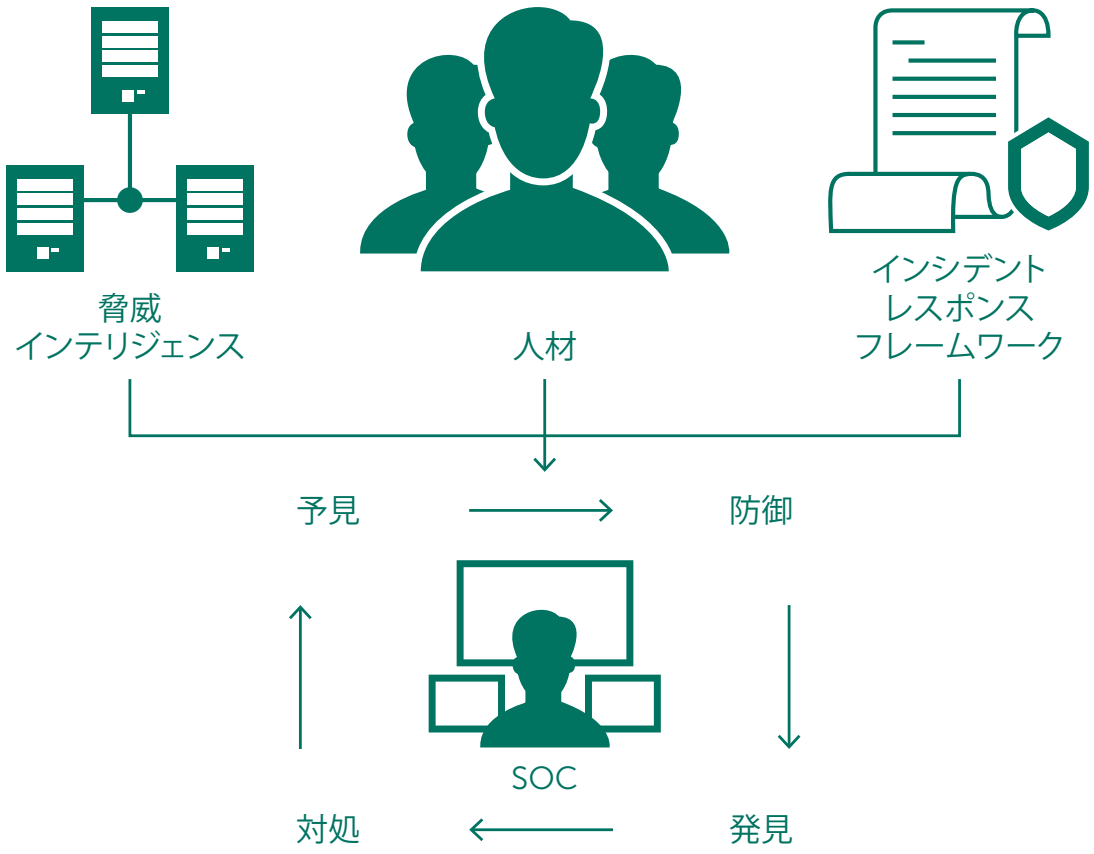


図 1：
SOC の 3 つの要素

人材

SOC には、必要なタイミングに膨大なデータを分析し、さらに調査が必要な個所を特定できるだけの、実際的な知識と高い専門性を持つメンバーからなるチームが必要です。

しかし限られた予算では、なかなか SOC に人員を割くことはできません。

また市場においても十分なトレーニングを受けたサイバーセキュリティのプロフェッショナルが不足しているため、人員採用の費用も人件費も上昇しています。

効果的な SOC 担当者の必要要件は以下の通りです：
- ちりばめられた多様で断片的なデータをつなぎ合せて全体像を構築できるような探求心があること
- 強いストレスにさらされつつも集中力を維持できること
- IT およびサイバーセキュリティに関する一般的な知識が十分にあり、できれば実務経験が豊富にあること

SOC のメンバーを社外から募集するにせよ、社内で調達するにせよ、このような必要要件を備える人材を何の秘策もなしに見つけることは簡単ではありません。メンバーのスキルを目標レベルに引き上げるためだけでなく、日々新しくなるセキュリティ技術と進化し続ける脅威に対応するために、継続的なトレーニングが必要です。

インシデント対応、デジタルフォレンジック、マルウェア分析は不可欠な能力です。

インシデント対応とデジタルフォレンジック	マルウェア分析
• インシデントに迅速かつ正確に対応 • 証拠を分析（HDD イメージ、メモリダンプ、ネットワークログ）し、インシデントの発生過程とロジックを再現 • 推定される攻撃元および侵害を受けた可能性のあるその他のシステムを特定 • 同様のインシデントの再発を防ぐため、当該インシデントの根本原因を解明	• 疑わしいソフトウェアサンプルを入手し、その機能を解析 • 実際にマルウェアなのかどうかを判定 • 当該サンプルが組織内のシステムに感染した際に考えられる影響を特定 • 解析によって得られたマルウェアの動作に基づいて、包括的な復旧計画を策定

Kaspersky Lab は以下のサービスを提供します：
サイバーセキュリティトレーニングサービス

Kaspersky Lab では17年以上にわたり、脅威検知、マルウェア研究、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、サイバーセキュリティに関する専門知識を継続的に進化・発達させてきました。当チームのエキスパートは、1 日あたり 32 万 3,000 ものマルウェアサンプルを解析し続けるすることによって得られた、脅威に対する最も効果的な方法を理解しており、その知識と現場で培った経験を、今日のサイバー空間の現実ともいえる、新しい脅威に立ち向かうお客様に提供します。

Kaspersky Lab のセキュリティトレーニングプログラムは、当社の Anti-Virus Lab の構築に関わり、グローバルに活躍する次世代の育成に携わるトップエキスパートがデザインし、開発したものです。

コースは、理論を学ぶ講座と実習「ラボ」の両方を含むように設計されています。各コースの終了時には認定試験があり、受講者の知識を検証することが可能です。

トレーニングコースは、一般的あるいは高度なシステム管理およびプログラミングスキルを備える、IT 関連専門技術者に適しています。すべてのコースは、お客様の拠点やカスペルスキーのオフィス、あるいはその他の適切な場所で開催することが可能です。

プログラムの説明

テーマ	期間	獲得スキル
デジタルフォレンジック -基礎編-		
• デジタルフォレンジック入門 • ライブレスポンスと証拠の収集 • Windows レジストリの内部 • Windows artifacts の分析 • ブラウザーのフォレンジック • メールの分析	5 日間	• デジタルフォレンジックラボの構築 • デジタルエビデンスの収集と正しい処理 • インシデントの再現とタイムスタンプの活用 • Windows OS 内の artifacts に基づく侵入形跡の発見 • 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・ツールの利用と活用テクニック
マルウェア分析とリバースエンジニアリング -基礎編-		
• マルウェア分析とリバースエンジニアリングの目標およびテクニック • Windows の内部処理、実行可能ファイル、x86 アセンブラ • 基本的な静的分析テクニック（文字列の抽出、インポート分析、PE エントリポイントの概要、自動解凍など） • 基本的な動的分析テクニック（デバッギング、監視ツール、トラフィックのインターセプトなど） • .NET、Visual Basic、Win64 ファイルの分析 • スクリプトと非 PE 分析テクニック（バッチファイル、AutoIt、Python、JScript、JavaScript、VBS）	5 日間	• マルウェア分析に適した安全な環境の構築：サンドボックスと必須ツールの導入 • Windows プログラム実行の原理 • 悪意のあるオブジェクトの解凍、デバッグ、分析と機能の識別 • スクリプトマルウェア分析による悪意のあるサイトの検出 • 表面解析の実施

テーマ	期間	獲得スキル
デジタルフォレンジック -発展編-		
• 詳細な Windows フォレンジック • データの復元 • ネットワークとクラウドのフォレンジック • メモリフォレンジック • タイムライン分析 • 実際の標的型攻撃に対するフォレンジック手法	5 日間	• 詳細なファイルシステム分析 • 削除済みファイルの復元 • ネットワークトラフィックの分析 • ダンプを使用した悪意のある動作の調査 • インシデントタイムラインの再現
マルウェア分析とリバースエンジニアリング -発展編-		
• 高度な静的分析テクニック（シェルコードの静的な分析、PE ヘッダー、TEB/PEB 構造体、さまざまな方法でパックされたコードの構文解析） • 高度な動的分析のテクニック（PE 構造、高度なマニュアルアンパッキング、完全な実行ファイルが暗号化形式にてパックされた悪意あるファイルのアンパッキング） • APT のリバースエンジニアリング（フィッシングメールから始まり、可能な限り深く侵入していく、APT 攻撃のシナリオをカバー） • プロトコル分析（暗号化された C2 の通信プロトコルの分析、トラフィックの復号方法） • ルートキットおよびブートキット分析（Ida と VMWare を使用したブートセクターのデバッグ、仮想マシン 2 台を使用したカーネルデバッグ、ルートキットサンプルの分析）	5 日間	• 対リバースエンジニアリングのトリック（難読化、アンチデバッギング）を認識しつつ、リバースエンジニアリングのベストプラクティスに沿った対応 • 高度なマルウェア分析の手法を用いたルートキットおよびブートキットの詳細解析 • さまざまなファイルタイプおよび非 Windows のマルウェアに埋め込まれたエクスプロイトシェルコードの分析

ツールは適時変更しますが、学習の基本および方法は変わりません。受講者はツール一式を受け取り、説明を受けるだけでなく、その根本的な本質と機能性も理解できるようになります。実習はすべて実際の事例をベースに実施します。

脅威インテリジェンス

SOC は、次のような機能を目的として構築されます：

- セキュリティデバイス管理、および IPS/IDS、ファイアウォール、プロキシなどネットワーク境界における予防的なセキュリティ技術の導入と運用
- セキュリティ情報イベント管理（SIEM）システムによるセキュリティイベントの監視
- インシデント時のフォレンジック調査と復旧
- 社内規定や規制（PCI-DSS など）への準拠

現在、多くの組織が自前の SOC を構築し、より高度な脅威の可視化を実現しようとしています。しかし中には、SOC を構築したものの、それまでと同じ多くの問題に直面している組織もあります。
その理由は以下の通りです：

- インシデントの優先順位付けが的確ではないため、日々発生する何千もの重要ではないセキュリティアラートの分析作業の中に、真に重要な脅威が埋もれ、放置されている。
- 攻撃者の TTP（戦術、手法、手順）を正確に理解しないままインシデントからの復旧を行うため、先進的な攻撃を見落としている。
- 適切な脅威データが不足しているため、検出漏れが生じている。
- 組織内にすでに存在する未発見の脅威を積極的に「狩り出す」のではなく、インシデントが発生してから対処する受動的なアプローチになっている。
- 直面している今日の脅威の全体像について戦略的な視点がない、あるいは他社が受けている攻撃や対策について把握できていない。
- セキュリティ侵害によるビジネスのリスクを経営陣に伝えることが難しいため、セキュリティ技術に十分な予算を獲得できない。

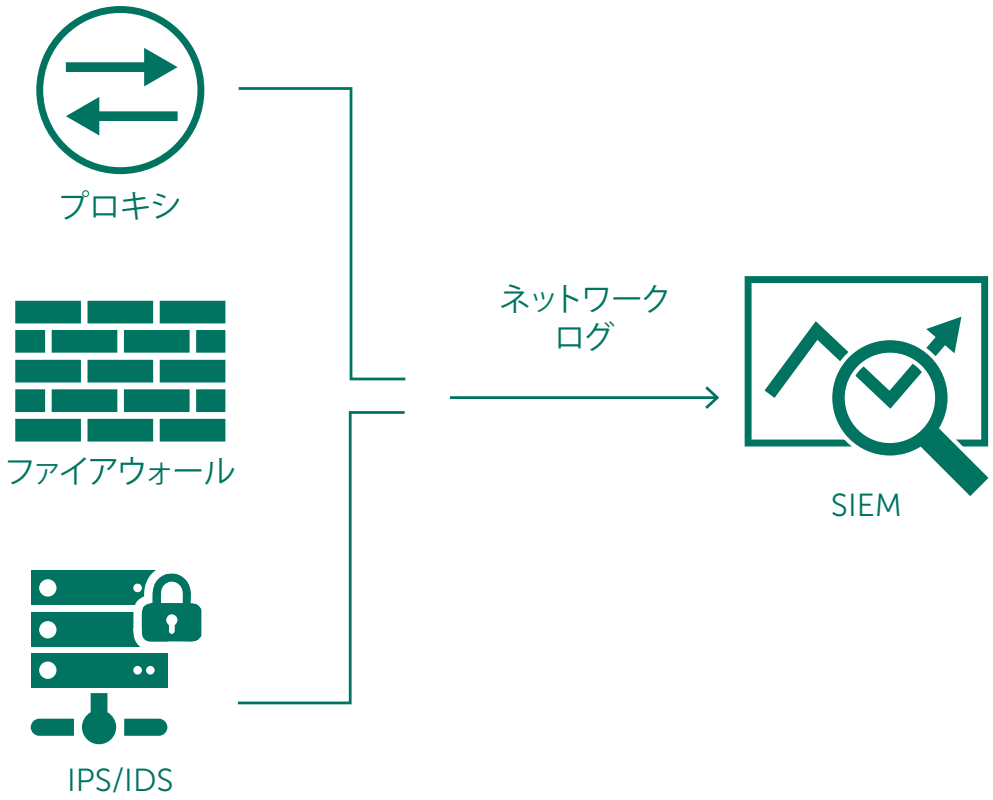


図 2：
一般的な SOC

Gartner 社は脅威インテリジェンスを以下のように定義しています：
「資産の保全に対する既存あるいは新しい脅威や危険に関する裏付けのある知識で、属性や前後関係、メカニズム、インジケーター、推測される影響、実用的なアドバイスなどを含み、その脅威や危険への対策を意思決定するための情報源となり得るもの」

Gartner 社のレポート『How Gartner Defines Threat Intelligence（Gartner が定義する脅威インテリジェンス）』（2016 年 2 月）より

このような問題を考慮すると、セキュリティ部門のトップが選択すべき賢明なアプローチは、インテリジェンス主導の SOC ということになります。効果的な SOC を実現するには、現在の大きく変化し続ける脅威に対応できるよう、常に新しい技術と管理手法を取り入れていく必要があります。

脅威に関する社内データとさまざまな情報源（OSINT やグローバルなマルウェア対策ベンダーなど）から収集した情報を合わせることで、攻撃に使用されるテクニックと攻撃の兆候を把握できるようになります。そしてこれが、一般的な攻撃に加えて特定の組織を標的とする先進的な標的型攻撃に対して効果的な防衛戦略を構築することにつながるのです。

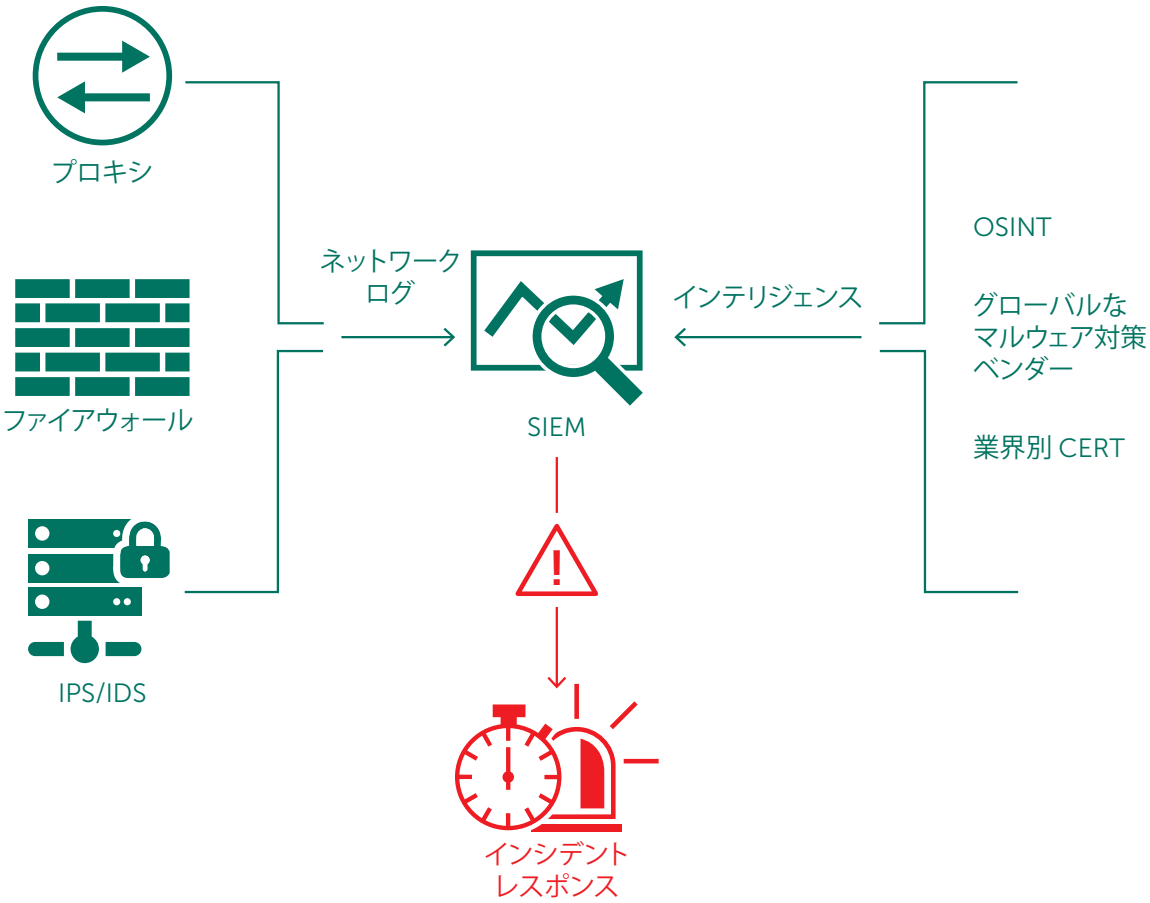


図 3：
インテリジェンス主導の SOC

インテリジェンスの情報源は慎重に選択する必要があります。採用するインテリジェンスの質と、それを基に下す意思決定の効果の間には、直接的な相関関係があるからです。不適切あるいは不正確であったり、業界やビジネス目標に沿わなかったりする情報を基にしてしまうと、また脅威に関する情報をタイムリーに取得できないと、意思決定の質は著しく低下してしまう可能性があります。

属性や前後関係のないデータでは、SOC チームは十分に効果を発揮できません。例えば、ある URL が悪質であることを把握していることと、それに加えてその URL があるエクスプロイトや特定のタイプのマルウェアをホストしていることをも把握していることには大きな違いがあります。こうした階層構造をもつインテリジェンスによって、組織のセキュリティエキスパートは感染した機器を見つけるために何を探せばよいかを把握することができます。

外部の脅威インテリジェンス情報源に必要なこと:

- グローバル規模の情報を有し、幅広い攻撃を把握していること
- 新しい脅威インジケーターを早期に特定した実績を持つプロバイダーであること
- 属性や前後関係などの付加情報が豊富で、すぐに活用できること
- 既存のセキュリティ管理システムと簡単に統合できるフォーマットおよびメカニズムを提供できること

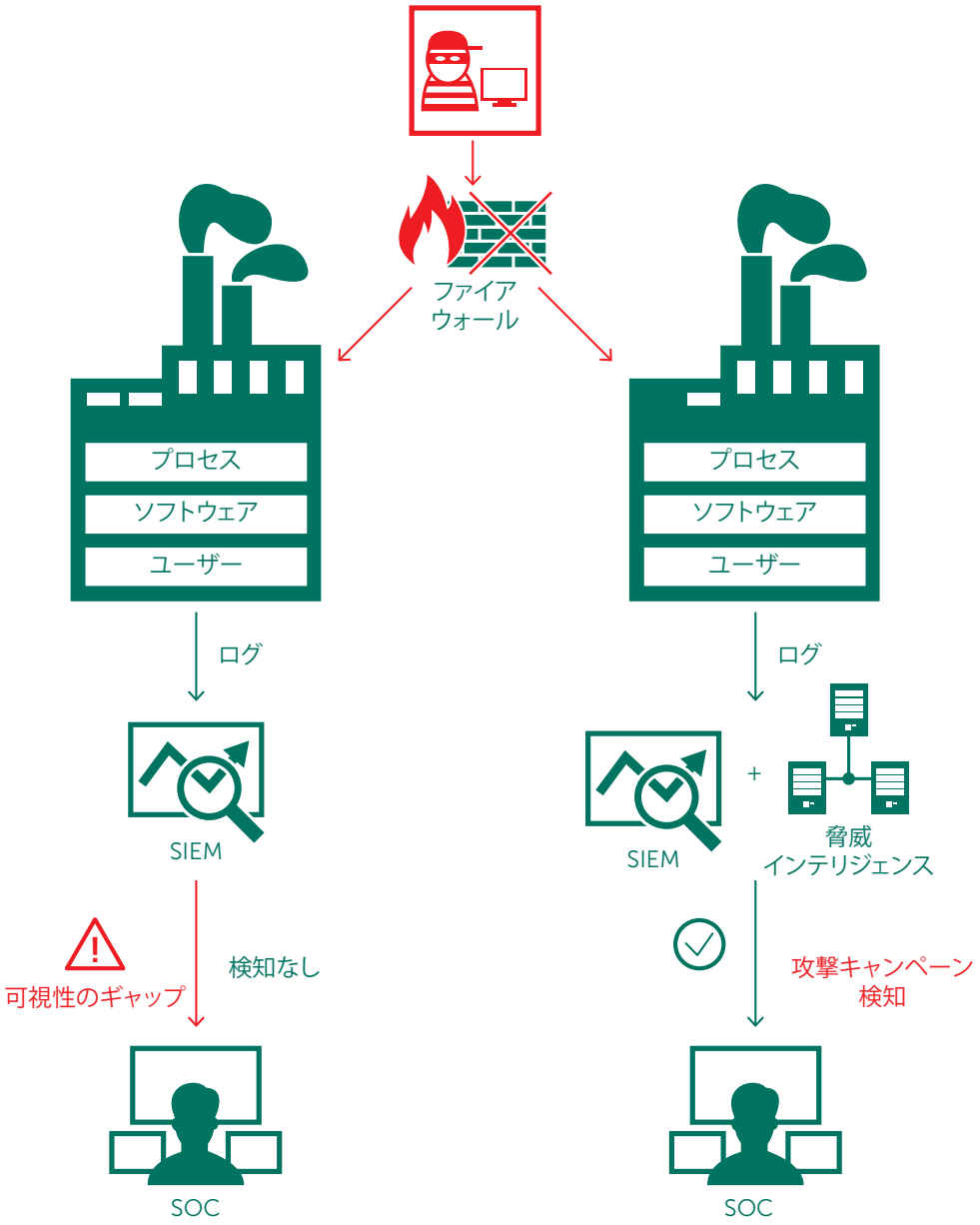


図 4:
脅威インテリジェンスのモデル

Kaspersky Lab は以下のサービスを提供します：
脅威データベース提供サービス

Kaspersky Lab では、常に最新の脅威インテリジェンスデータを提供することで、お客様の SOC チームにサイバー脅威のリスクとその影響について通知し、脅威をより効果的に軽減できるよう、また攻撃をそれらが実行される以前に回避できるよう、支援します。

フィードの説明

IP レピュテーション — 悪意のある、もしくは疑わしい IP アドレス。(マルウェアホスト、スパム送信元、Tor-Exit-Node 、ボットネット C&C 、アノニマイザー、フィッシング、ポートスキャナーなどを含む)

悪意のある URL — 悪意のあるリンクとサイトを含む URL。

フィッシング URL — フィッシングサイトの URL。

ボットネット C&C URL — ボットネットのコマンド & コントロール(C&C)サーバーの URL およびその C&C に関係する悪意あるオブジェクトのハッシュ値。

ホワイトリスト — 正規ソフトウェアに関する体系的な知識に基づいて蓄積された、サードパーティのソリューションやサービスで使用される正規ソフトウェアのハッシュ値。

マルウェアのハッシュ値 — マルウェアのハッシュ値。(流行中あるいは最新の危険度の高いマルウェアをカバー)

モバイル向けのマルウェアのハッシュ値 — 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のハッシュ値。

P-SMS 型トロイの木馬のハッシュ値 — ユーザーへの高額請求や SMS メッセージの盗用、削除、不正応答を可能にする SMS 型トロイの木馬のハッシュ値。

モバイルボットネットの C&C URL — モバイルのボットネット C&C サーバーの URL。

サービスの特徴

- 脅威データベースは、世界中で特定されたデータ(Kaspersky Security Network は 200 か国以上に及ぶ数千万のエンドユーザーをカバーし、全インターネットトラフィックの相当部分を可視化しています)に基づいて、リアルタイムで自動生成されており、高い検出率と正確性を誇っています。
- 提供されるそれぞれのデータベースのレコードにはすべて、実用的な付加情報(脅威名、タイムスタンプ、地域情報、感染した Web リソースの名前解決後の IP アドレス、ハッシュ値、感染数など)が付随されています。データに付加情報があると、さらなる検証ができ、またそのデータの活用度も広がるため、「より大きな全体像」を把握することができます。周辺情報と総合することで、そのデータは、攻撃元の特定に必要な、誰が、どこで、いつ、何をといった疑問への答えも見つかりやすくなり、タイムリーな意思決定と、組織を保護するための具体的な行動が促進されます。
- 情報を、HTTP または個別の配信方法を使ってシンプルで軽い一般的なファイル形式(JSON、CSV、OpenIoC、STIX)にて提供することにより、提供されるデータを容易にセキュリティソリューションに統合することが可能です。
- 脅威インテリジェンスは耐障害性の高いインフラにて生成・監視されるため、連続可用性と一貫性のあるパフォーマンスが保証されます。
- Splunk、Infoscience Logstorage、HP ArcSight、IBM QRadar などにも簡単に統合可能です。

脅威情報ルックアップサービス

カスペルスキー脅威情報ルックアップサービスは、サイバー脅威に関して Kaspersky Lab が収集し蓄積し続けるすべてのデータとそれらの間にある相互関係を検索し、閲覧することのできる Web サービスプラットフォームとして提供するものです。その目的は、お客様の SOC チームに可能な限り多くのデータを提供し、組織に影響が及ぶ前にサイバー攻撃を回避することにあります。このプラットフォームでは、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、ふるまいデータ、WHOIS データ、DNS データなどに関し、最新かつ詳細な脅威インテリジェンスを検索することができます。グローバルな最新の脅威に関する情報を提供することによって、組織の保護とインシデント対応能力の強化を支援します。

サービスの特徴

- 信頼できる情報：カスペルスキー脅威情報ルックアップサービスの主な特徴として、脅威インテリジェンスの信頼性が高く、さらにそこに実用的な付加情報が付随していることが挙げられます。カスペルスキー製品は第三者評価機関による比較テスト[1] においてトップを走っており、最高の検知率と極めて低い誤検知率がセキュリティインテリジェンスの比類のない質の高さを実証しています。
- 高いリアルタイム性：脅威インテリジェンスは、Kaspersky Security Network のサポートにより世界中から集められたデータをベースをもとに、「リアルタイム」で自動生成されています。
- 脅威ハンティング：先を見越した防御、発見、対処を行うことで、攻撃の影響を最小化しかつ攻撃頻度を低減します。可能な限り早い段階から攻撃を追跡し、積極的に排除します。脅威の発見が早いほど、ダメージも小さく、復旧期間も短く、ネットワークオペレーションを早期に通常状態に戻すことができます。
- 豊富なデータ：脅威情報ルックアップサービスから提供される脅威インテリジェンスは、ハッシュ値、URL、IP、WHOIS、pDNS、GeoIP、ファイル属性、統計的データ、ふるまいデータ、ダウンロード・チェイン、タイムスタンプなど、さまざまなデータタイプを幅広くカバーしています。組織が直面するセキュリティ脅威は広大な範囲に及びますが、こうした豊富なデータが提供されることで、その調査が可能になります。
- いつでも利用可能：脅威インテリジェンスは耐障害性の高いインフラにて生成・監視されるため、連続可用性と一貫性のあるパフォーマンスが保証されます。
- セキュリティのエキスパートによる継続的なレビュー：Kaspersky Lab に在籍する世界のセキュリティアナリスト、Global Research & Analysis Team (GReAT) の世界的に著名なエキスパート、最先端の研究開発チームなど、数百名に及ぶセキュリティ専門家が、価値ある実世界の脅威インテリジェンスの生成に尽力しています。
- 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で実行することで、未知の脅威を検知し、すべての動作を検証するとともに、分かりやすいレポートを生成します。

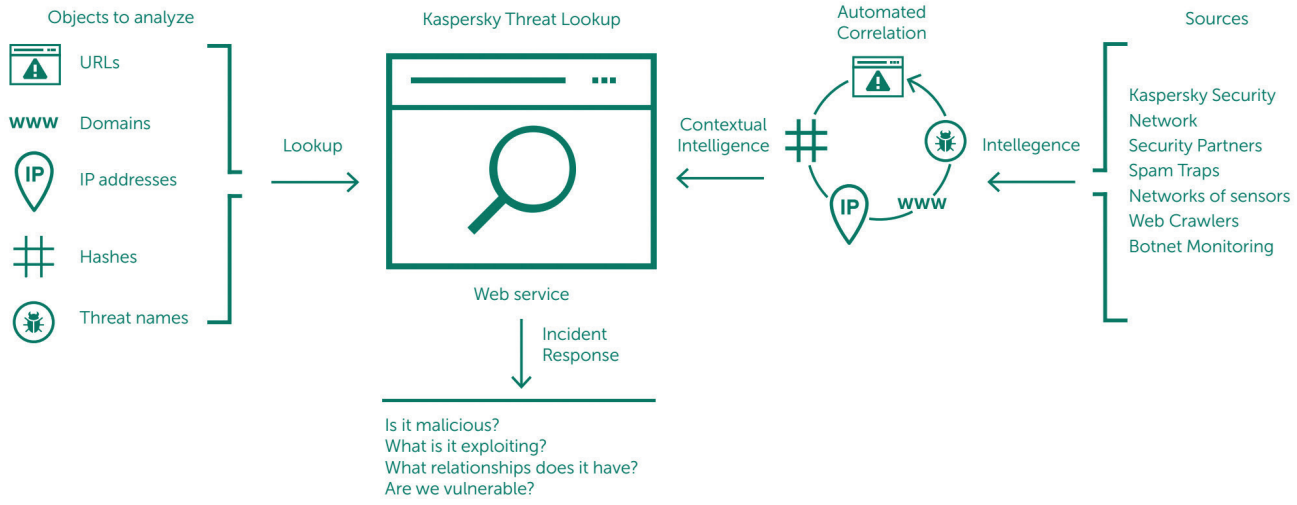
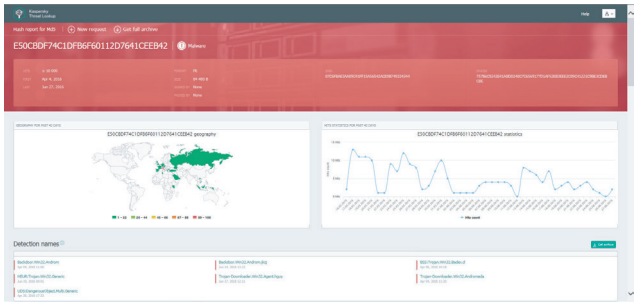
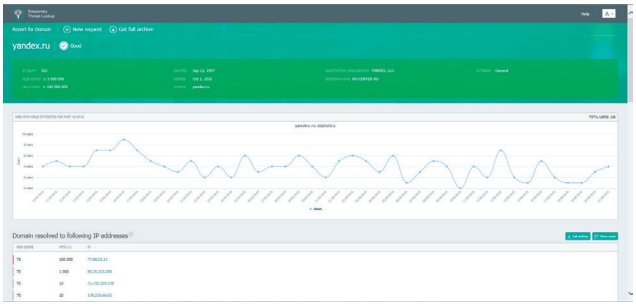


図 5:
Kaspersky Threat Lookup

1 http://www.kaspersky.co.jp/top3

- 幅広いエクスポート形式：IOC（侵害インジケーター）や実用的な付加情報を、STIX、OpenIOC、JSON、Yara、Snort、さらには CSV といった、広く普及し、より体系化された読み込み可能な共有フォーマットにてエクスポートすることができるため、脅威インテリジェンスの利点を余すことなく活用でき、オペレーションワークフローを自動化したり、SIEM などのセキュリティ管理システムに統合したりすることができます。
- 使いやすいウェブインターフェースまたは RESTful API：ウェブインターフェース（ウェブブラウザー経由）を使ってマニュアルモードにてサービスを利用することも、シンプルな RESTful API 経由でアクセスすることも可能です。





APT インテリジェンスレポートサービス

発見されるすべての APT 攻撃 (Advanced Persistent Threat) が即座に報告されるわけではなく、多くは公表されません。APT に関する、Kaspersky Lab 独自の、詳細かつ実用的なインテリジェンスレポートを通じて、誰よりも早く、最新のリサーチ結果を入手することができます。

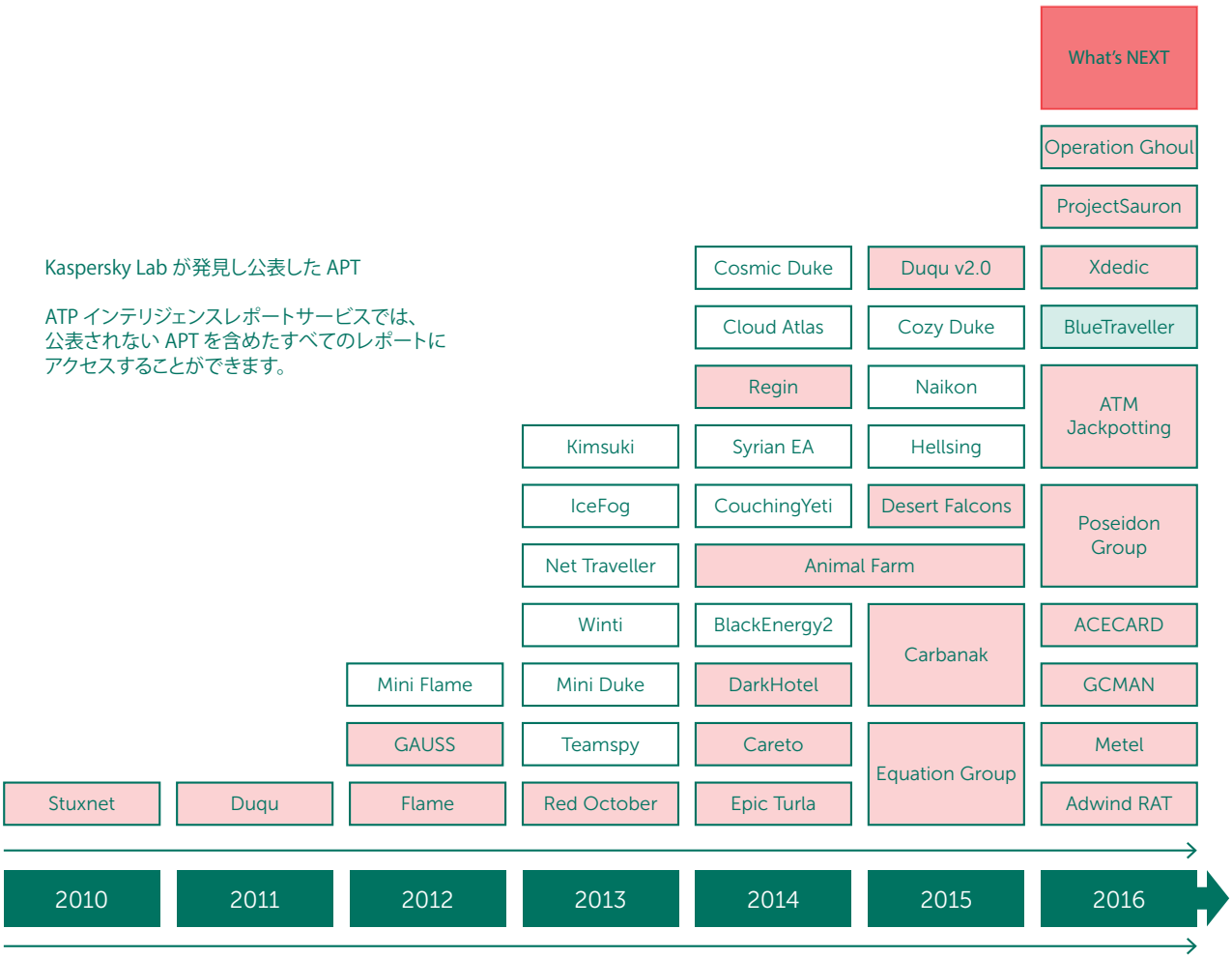


図 6:
Kaspersky Lab が発見した APT

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、Kapersky Lab が発見し調査したすべての APT に関する解析結果に継続的にアクセスすることができます。それぞれの APT 毎に解析された完全な技術データが様々なフォーマットで提供されるとともに、公開されることのない脅威もすべて含まれています。Kaspersky Lab 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、サイバー犯罪者やサイバーテロリストのグループが戦術を変更した場合は、ただちに警告を送ります。さらに利用者は、組織のセキュリティ戦略を検討するにあたって強力な分析ツールとなる、Kaspersky Lab の APT レポートデータベースにフルアクセスすることができます。

サービスの特徴

- 専用アクセス：最先端の、また現在進行中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。
- 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。被害を受けた組織やデータの機密性、関連するぜい弱性やその解消に関する状況、また関係する捜査機関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。
- 詳細な関連技術情報：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技術データ、サンプル、ツールに加えて、Yara ルールへのアクセスを提供します。
- 継続的な APT キャンペーンの監視：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（発生分布、IOC、C&C インフラストラクチャに関する情報）。
- 遡及分析：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。

実際的な見地から、IOC は、SOC エキスパートのレポートの中でも最も実用的な部分であるといえます。こうした整理された情報は、特定の自動化ツールと合わせて利用できるよう提供され、組織のインフラにおける感染の兆候を確認するために活用されることになります。
すべてのレポートは、下図に示す通り、APT インテリジェンスポータル経由で提供されます。

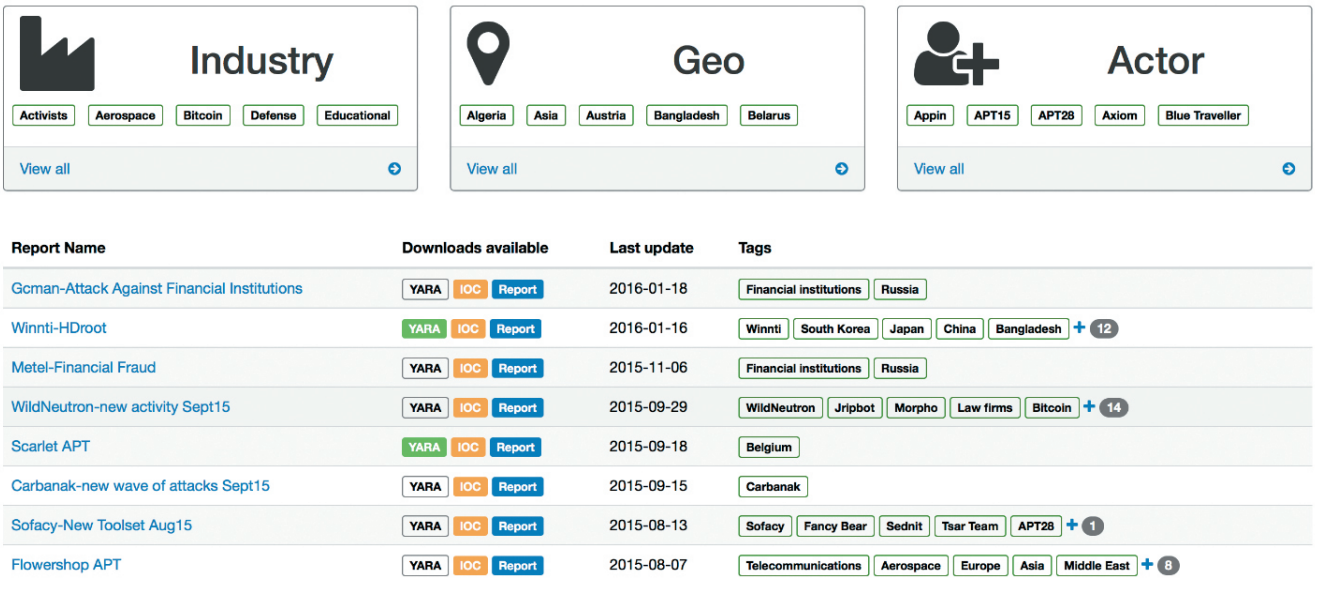


図 7:
APT インテリジェンスレポートポータル

個別インテリジェンスレポートサービス

お客様専用の脅威レポート

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。

カスペルスキー個別インテリジェンスレポートサービスによって提供される、お客様専用の脅威レポートは、これらの疑問に答えるだけにとどまりません。Kaspersky Lab 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、攻撃者が侵害することのできる組織の弱点を特定するとともに、過去と現在の攻撃の痕跡と計画されている攻撃に関する情報を提供します。

お客様はこのユニークな洞察を活用して、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 Lab 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用して作成される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、攻撃の対象となり得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、およびネットワーク上の疑わしい動きを識別、監視、分析します。
- **サードパーティーへの攻撃**：お客様の顧客、パートナー、サービス利用者を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用さ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、あるいはたとえば不誠実な従業員（インサイダー）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見つけた場合、有効な修正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

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、お客様側では一切の準備、作業は発生いたしません。

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。

国に特化した脅威レポート

国のサイバーセキュリティには、その国のすべての主要機関および団体の保護が包括されます。政府機関に対する APT（Advanced Persistent Threat）は国家の安全保障に影響を与え得るものであり、製造、運輸、通信、金融をはじめとする重要産業に対するサイバー攻撃は、財務的損失や生産事故、ネットワーク通信の遮断、国民の不信感といった国家レベルの重大な問題を引き起こす可能性があります。

しかしマルウェア攻撃およびハッカー攻撃における現在表出している攻撃と現在の動向を総体的に把握することができれば、防御戦略をサイバー犯罪者の主要標的として特定されるエリアに集中させ、それにより侵入者を迅速かつ正確に撃退し、攻撃成功のリスクを最小限に留めることができます。

国に特化した脅威レポートは、オープンソースインテリジェンス（OSINT）や、Kaspersky Lab 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などを駆使して構築されたもので、以下の領域をカバーしています：

- **攻撃経路の識別**：外部から利用でき、攻撃の対象となり得る国の重要な IT リソース（政府の脆弱なアプリケーション、通信機器、SCADE や PLC といった産業用制御システムのコンポーネント、ATM など）を特定し、その状況を分析します。
- **マルウェアおよびサイバー攻撃の追跡分析**：国に関係する APT キャンペーン、活動中または非活動中のマルウェアサンプル、過去または現在のボットネット動作、その他の重要な脅威を、カスペルスキー独自の内部監視リソースから得られるデータを基に特定し、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監視することで、ハッカーが特定の組織を念頭に攻撃を計画しているかどうかを突き止めます。さらに、組織や機関へのリスクになり得る重要なアカウント侵害も特定します（例えば、Ashley Madison: 不正アクセスを受けた不倫サイトに政府機関の職員のアカウントがあった場合、それが脅迫に使われることもあります）。

カスペルスキー脅威インテリジェンスレポートは、調査対象となる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。本サービスは、非侵入型のネットワーク偵察手法、ならびにオープンソースおよびアクセスを限定したリソースから取得できる情報の分析をベースとしています。

本サービスで提供されるレポートには、国の各産業および機関に対する重要な脅威の説明に加え、詳細な技術分析結果に関する追加情報が含まれます。レポートは暗号化されたメールメッセージにて提供されます。

本サービスは、単発のプロジェクトとして提供することも、契約に基づく定期サービス（例：四半期ごと）として提供することも可能です。

カスペルスキーの脅威インテリジェンスのソースについて

脅威インテリジェンスは、Kaspersky Security Network（KSN）、当社独自のウェブクローラー、当社の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、および約 20 年をかけて Kaspersky Lab 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されています。収集された情報は、統計的基準や Kaspersky Lab 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、類似性発見用ツール、動作プロファイリング、マシンラーニングなど）、アナリストによる検証、ホワイトリストによる認証など、さまざまな前処理テクニックを用いて、「リアルタイム」で慎重に調査および精査されます。

適切なスキルを有し、トレーニングを受けた人員を配置し、信頼できるソースから取得した脅威インテリジェンスを既存のセキュリティ管理システムと統合できたら、次はインシデント対応について検討します。

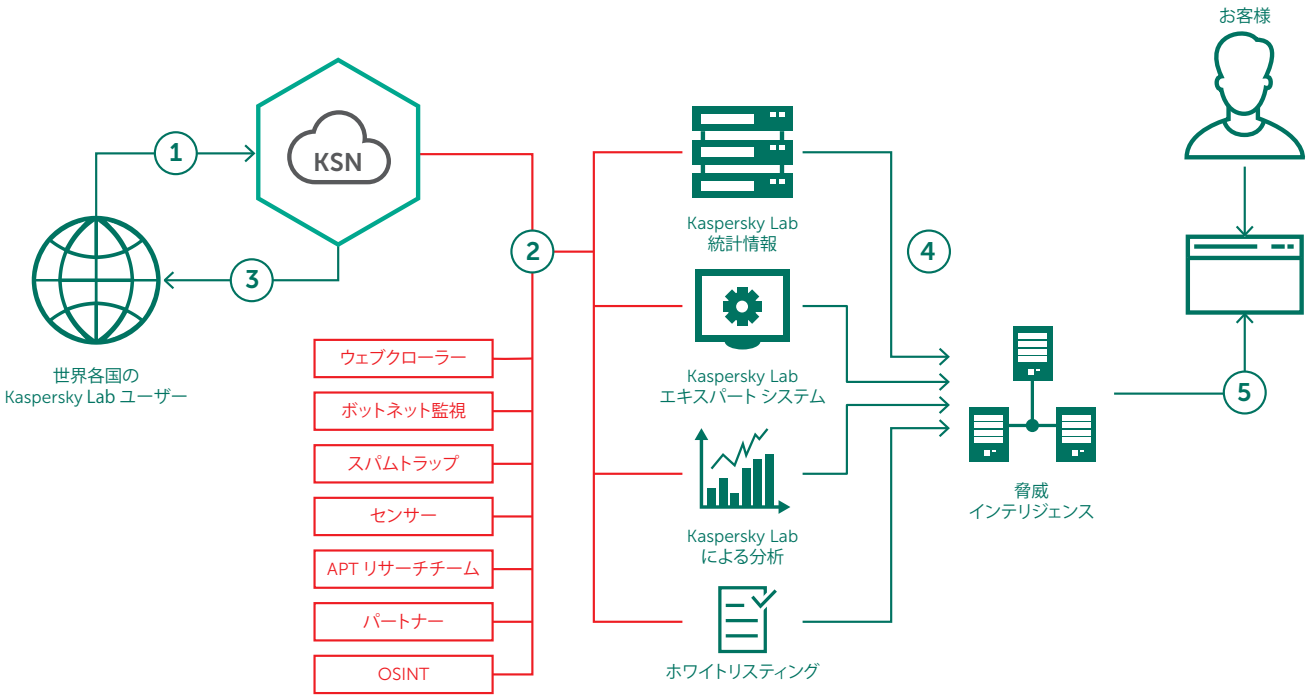


図 8：
Kaspersky Lab の脅威インテリジェンスのソース

インシデント対応のフレームワーク

フォレンジックおよびインシデント対応を効果的に実施するには、社内の相当数のリソースを即座に配置できる備えが必要です。またサイバー攻撃に対応した幅広い実務経験を有する、知識の豊富なスペシャリストが、悪意ある攻撃を迅速に特定し、隔離し、ブロックする必要があります。攻撃による影響と復旧コストを最小限に抑えるには、迅速な対応が不可欠です。

こうした高度な専門知識を短期間で習得することは、経験豊富な SOC チームをもってしても難しい場合があります。最先端の攻撃をその場で食い止められるだけの、十分な社内リソースを持つ組織はほんの一握りでしょう。さらに、国家がサポートする複雑な脅威や APT に直面した場合、そうした APT 攻撃で用いられる特定の手法や戦術に関する専門知識を SOC チームが持ち合わせていない、といったことも考えられます。

こうしたケースでは、十分な情報に基づく迅速な対応が可能な、社外のインシデント対応ベンダーやコンサルタントと協調することが、コスト効率の面でも生産性の面でも効果的であると考えられます。

包括的なインシデント対応フレームワークには、以下が必要です：

- **インシデントの特定**
  最初のインシデント分析と感染したシステムの隔離が必要です。
- **証拠の取得**
  必要な証拠を取得するための調査対象ソースは、インシデントのタイプにより異なります。
- **フォレンジック分析**
  この段階では、インシデントの詳細な全体像を描きます。
- **マルウェア分析**
  関与したマルウェアの動作や機能を理解します。
- **復旧計画**
  問題の根本的要因とマルウェアを駆除するための計画を策定します。
- **再発防止**
  それまでのセキュリティ対策を見直し、同様のインシデントの再発を防ぐための改善を行います。

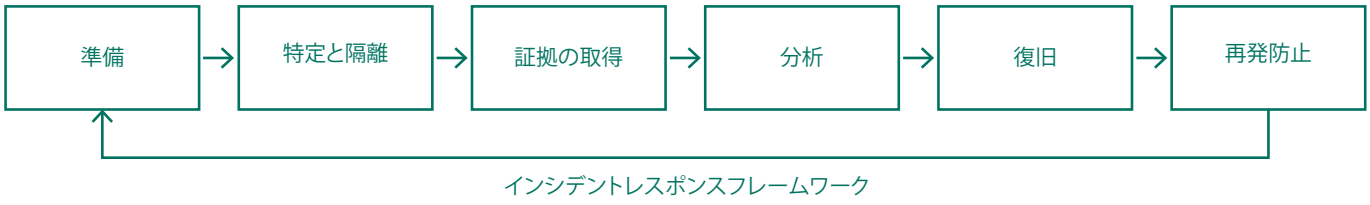


図 9：
インシデント対応のフレームワーク

Kaspersky Lab は以下のサービスを提供します：
インシデント対応サービス

インシデント対応は Kaspersky Lab のプレミアムサービスで、オンサイトでの証拠の収集から、侵害を示すさらなる兆候の特定や復旧計画の策定、さらには脅威の完全な排除まで、インシデント調査の全サイクルをカバーしています。Kaspersky Lab の調査は、経験豊富なアナリストと調査員が担当します。Kaspersky Lab では、お客様のセキュリティインシデントを解決するために、デジタルフォレンジックおよびマルウェア分析におけるグローバルレベルの専門性をフル活用します。

このサービスは以下の項目を目標に実施します：

- 侵害を受けたリソースの特定
- 脅威の隔離
- 拡大と拡散の回避
- 証拠の発見と収集
- 証拠の分析ならびにインシデントのタイムラインとロジックの再現
- 攻撃に使用されたマルウェア（何らかのマルウェアが検出された場合）の分析
- 攻撃元および侵害された可能性のあるその他のシステムの特定
- 侵害の痕跡を発見するためのツールを用いた IT インフラのスキャン
- コマンド＆コントロールサーバーなど攻撃に関与したリソースを特定するため、お客様のネットワークから外部への通信の分析
- 脅威の排除
- さらなる改善対策を提言

お客様にインシデント対応チームが存在するかどうかによって、侵害された機器を特定、隔離して脅威の拡散を防ぐインシデント対応の全てのサイクルを実施させるか、マルウェア分析やデジタルフォレンジックのみを依頼するのかを選択することができます。

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動作と目的を完全に理解することです。Kaspersky Lab のエキスパートは、お客様より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、マルウェアの分類を決定します。
- マルウェアの詳しい説明：マルウェアサンプルの役割、動作、目的ならびに IOC 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。
- 駆除シナリオ：この種別の脅威から組織を完全に駆除、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 Lab のエキスパートは、HDD イメージ、メモリダンプ、ネットワークログなどを使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。そうして、インシデントの詳細な解明につなげます。お客様にはまず、形跡を集め、インシデントの概要を提供していただきます。Kaspersky Lab はインシデントの状況を分析し、マルウェアバイナリを特定し、マルウェア分析を実施して、修正手順を含む詳細レポートを提供します。

提供方法

Kaspersky Lab のインシデントレスポンスサービスは、次のいずれかの方法で提供されます：

- 年間サブスクリプションでの提供
- 個別インシデント毎の提供

詳細はカスペルスキーの営業員にお問い合わせください。

KASPERSKY LAB が選ばれる理由

- インターポールや CERT といった国際的な法執行機関とのパートナーシップ
- 世界中の数百万ものサイバー脅威をリアルタイムで監視できる、クラウドベースのツール
- あらゆる種類のインターネット脅威を分析し把握しているグローバルチーム

なぜなら Kaspersky Lab とは以下のような企業だからです：

- 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特化した、世界最大の独立系セキュリティソフトウェア企業
- どのベンダーよりも多くの独立機関テストに参加し、最も高い評価を得る業界のリーダー
- Gartner 社、Forrester 社、IDC 社がリーダーとして認知

Kaspersky Lab について

Kaspersky Lab は、世界最大の株式非公開のエンドポイント保護ソリューションベンダーです。同社は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 Lab は 18 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、消費者向けに提供しています。Kaspersky Lab は現在、英国に持ち株会社を登録し、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。

https://twitter.com/
kaspersky_japan

https://www.facebook.
com/KasperskyLabsJapan

http://www.youtube.
com/KasperskyJapan/

株式会社 カスペルスキー
www.kaspersky.co.jp

インターネットセキュリティに関する情報：
www.securelist.com

株式会社カスペルスキー
BD-KSIS-SOC-201612-001