KASPERSKY lab

カスペルスキーのセキュリティインテリジェンスサービス

2015 年

今日のサイバー犯罪に国境はなく、技術レベルも急速に高まっており、攻撃は巧妙になる一方です。Kaspersky Lab のミッションは、あらゆる種類のサイバー攻撃から世界を守ることです。これを実現するために、そしてインターネットを安全に使用できるようにするために、脅威に関する情報をリアルタイムで共有することが不可欠です。データとネットワークを効果的に保護し続けるための中核を成すのは、情報へのタイムリーなアクセスです。

Kaspersky Lab 会長兼最高経営責任者（CEO）
ユージン・カスペルスキー（Eugene Kaspersky）

はじめに

日々出現するサイバー攻撃は常に新しいもので、それぞれ見え方は異なり、攻撃経路もさまざまです。

1 つのソリューションですべてを保護することは不可能です。しかし、ビッグデータの世界において、危険が潜む可能性のある場所を知ることが、最新の脅威に対抗するための大きな力となります。

ビジネスマネージャーには、目下の脅威から組織を保護し、今後数年に待ち受ける危険を予測するという責任が課せられています。これには、スマートな方法で既知の脅威から業務を保護するだけでなく、一定の戦略的なセキュリティインテリジェンスが必要になりますが、これを社内で開発するだけのリソースを持っている企業はほとんどありません。

Kaspersky Lab は、事業に長期的な成功をもたらすには、長く続く関係が必要であると理解しています。

Kaspersky Lab は有益なビジネスパートナーとして、さまざまなチャネルを通じてお客様チームと常に最新情報を共有できるようにしています。幅広い提供手段を通じて、お客様のセキュリティオペレーションセンター（SOC）や IT セキュリティチームが、あらゆるオンライン脅威からいつでも組織を保護できる状態にあるように支援します。

カスペルスキー製品を使用していないお客様も、Kaspersky Lab のセキュリティインテリジェンスサービスによるメリットを活用していただけます。

他とは一線を画すセキュリティ

当社の DNA に組み込まれた世界有数のセキュリティインテリジェンスが、Kaspersky Lab のすべての行動に影響を及ぼし、市場でもっとも強力なアンチマルウェア保護の提供を可能にします。

CEO のユージン・カスペルスキー（Eugene Kaspersky）を筆頭に、組織全体が**テクノロジー主導型の企業**です。

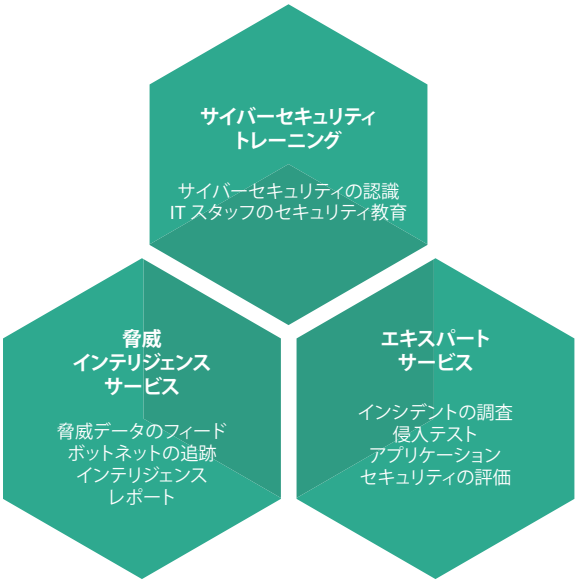
グローバルな研究および分析チーム（GReAT）は、IT セキュリティエキスパートからなる精鋭集団であり、世界でもっとも危険なマルウェア脅威と標的型攻撃を多数発見するための道を開いてきました。

世界でもっとも評判の高いセキュリティ組織と警察機関（インターポール、ユーロポール、CERT、ロンドン市警察を含む）が、カスペルスキーの支援を積極的に求めてきました。

Kaspersky Lab は、中核をなす技術をすべて社内で開発し、完成させているため、その製品とインテリジェンスは必然的により信頼性が高く効率的です。

もっとも広く評価されている業界アナリスト（Gartner、Forrester Research、International Data Corporation（IDC）を含む）によって、Kaspersky Lab は、多数の主要な IT セキュリティカテゴリでリーダーとして評価されています。

130 を超える OEM（Microsoft、Cisco、Blue Coat、Juniper Networks、Alcatel Lucent を含む）がその製品およびサービスで、カスペルスキーのテクノロジーを使用しています。

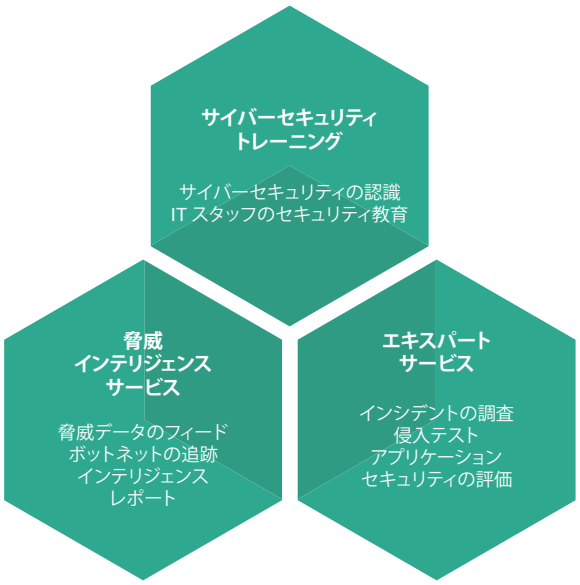


サイバーセキュリティトレーニング

Kaspersky Lab が持つサイバーセキュリティの知識、経験、知恵を活かした、革新的トレーニングプログラム

絶えず増加と発展を続ける脅威に直面する企業にとって、サイバーセキュリティの認識と教育は不可欠な要素となりました。セキュリティ関連の従業員は、効果的な脅威の管理および軽減戦略の主要要素となる高度なセキュリティテクニックに精通する必要があり、その他すべての従業員は、危険とその回避方法に対する基本的な認識を持つ必要があります。

Kaspersky Lab のサイバーセキュリティトレーニングコースは、インフラストラクチャと知的財産の効果的な保護を目指すすべての組織に向けて開発されています。すべてのトレーニングコースは英語で提供されます。



コース内容

	IT 部門以外の認識	IT セキュリティ部門の教育	
従業員	オンライントレーニングプラットフォーム	レベル 1 - 初心者	中核となるセキュリティの基礎 基本的な IT 知識
			ラボを使用した実用的なセキュリティの基礎 基本的な IT 知識
ラインマネージャー	CYBERSAFETY GAMES	レベル 2 - 中級者	デジタルフォレンジック システム管理者スキルが必要
			マルウェア分析とリバースエンジニアリング プログラミングスキルが必要
ビジネスマネージャー	サイバーセキュリティに関する文化の評価	レベル 3 - 上級者	高度なデジタルフォレンジック 高度なシステム管理者スキルが必要
			高度なマルウェア分析とリバースエンジニアリング アセンブラスキルが必要

サイバーセキュリティの認識力の向上

コンピューターまたはモバイルデバイスを業務に使うすべての従業員および管理職に向けた、対話型自習式オンライントレーニングモジュールとサイバーセキュリティゲームによるオンサイトトレーニング

全サイバーインシデントの約 80% は、人為的ミスによって引き起こされています。企業はサイバーセキュリティの認識プログラムに多額のコストをかけていますが、その結果に満足しているCISO はほとんどいません。何が間違っているのでしょうか。

ほとんどのサイバーセキュリティ認識トレーニングは、過剰に長く、技術的で、基本的にネガティブです。これでは人々の中核的な強みとなる意思決定の行動基準と学習能力を活かすことにならず、結果的に効果のないトレーニングになります。

組織は、セキュリティ認識への投資に対する定量化可能な価値ある利益をもたらす、より洗練された行動支援アプローチ（企業文化の養成など）を求めています。

Kaspersky Lab が提供するサイバーセキュリティ認識コースの特長は以下のとおりです:

- 安全な業務遂行方法への取り組みを促し、「誰もがサイバーセキュリティに配慮しているから、私もそうしよう」と思える企業環境を構築することで、従業員の行動を変えます。
- 動機付けのアプローチと、ゲーミフィケーションによる学習手法、攻撃のシミュレーション、サイバーセキュリティスキルに関する詳細な対話型トレーニングを組み合わせて提供します。

トレーニングの仕組み

包括的でありながら分かりやすいトレーニング	トレーニングでは、データ漏洩が発生する仕組みからインターネットベースのマルウェア攻撃や安全なソーシャルネットワーキングまで、一連の簡単な演習を通じて、幅広いセキュリティ課題について学習します。 集団力学、対話型モジュール、マンガ、ゲーミフィケーションといった学習手法を利用して、魅力的な学習プロセスを可能にします。
継続的な動機付け	ゲーミフィケーションや競争によって学習しやすい機会を提供し、その後、攻撃をシミュレートしたオンライン演習や評価、トレーニングキャンペーンによって、年間を通して再度トレーニングを実施します。
認識の改革	Kaspersky Lab は、サイバー犯罪者にとって一番の標的は人間であり、機械ではないことを伝えます。従業員がよりセキュリティ意識の高い方法で業務に取り組むことで、攻撃の被害者になったり、自分自身や職場を攻撃にさらしたりしないように防止する方法を紹介します。
サイバーセキュリティに配慮する企業文化の養成	Kaspersky Lab は、経営陣がセキュリティの提唱者となることを目指します。サイバーセキュリティが習性となるような文化を確立するための最善の方法は、IT による押し付けではなく、経営陣が本気で取り組み、手本となることです。
前向きで協力的なトレーニング	セキュリティに配慮した行動が業務効率に良い影響を与え、IT セキュリティチームを含む社内の別部門との効果的な連携を促すことを実証します。
行動の測定	従業員のスキルを測定するツールに加えて、日常業務でのサイバーセキュリティに対する姿勢を分析する企業レベルの評価サービスを提供します。

IT スタッフのセキュリティ教育

サイバーセキュリティのテーマと技術に関する幅広いカリキュラムと、基本から専門家レベルまでにわたる評価を提供します。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、可能な場合は Kaspersky Lab のローカルオフィスもしくは地域拠点で実施します。

コースは、理論的な講座とハンズオン「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、受講者の知識を確認するための評価が実施されます。

初心者から中級者、上級者までに対応

このプログラムは、セキュリティの基礎から高度なデジタルフォレンジックやマルウェア分析までにわたって、あらゆる要素を網羅しているため、組織は以下の3つの領域に関するサイバーセキュリティ知識を蓄えることができます:

- 該当テーマの基本知識
- デジタルフォレンジックとインシデント対応
- マルウェア分析とリバースエンジニアリング

サービスのメリット

レベル 1 – 中核となるセキュリティの基礎
IT とセキュリティの管理者およびマネージャー向けに、業界リーダーが実用的な IT セキュリティ対策に対する最新の考察の基本的理解を授けます。

レベル 1 – 実用的なセキュリティの基礎
最新のセキュリティ関連ツールを使用した実践的な演習を通じて、セキュリティを掘り下げて理解します。

レベル 2 ～ 3 – デジタルフォレンジック
社内のデジタルフォレンジックおよびインシデント対応チームの専門知識を強化します。

レベル 2 ～ 3 – マルウェア分析とリバースエンジニアリング
社内のマルウェア分析およびリバースエンジニアリングチームの専門知識を強化します。

ハンズオン演習

大手セキュリティベンダーのグローバルエキスパートと一緒に作業し学習することで、受講者はサイバー犯罪を検出して阻止するための「もっとも困難な局面」での経験を学ぶことができます。

プログラムの説明

テーマ	期間	獲得スキル
レベル 1 - 中核となるセキュリティの基礎		
• サイバー脅威とアンダーグラウンド市場の概要 • スパムとフィッシング、メールセキュリティ • 詐欺の防止技術 • エクスプロイト、モバイル、Advanced Persistent Threat • 公開 Web ツールを使用した調査の基本 • 職場のセキュリティ	2 日間	• セキュリティインシデントの認識と解決に向けた意思決定 • 情報セキュリティ部門の負荷の軽減 • 追加のツールにより、各従業員の作業場所のセキュリティレベルを向上 • 簡単な調査の実施 • フィッシングメールの分析 • 感染した Web サイトや偽の Web サイトの識別

テーマ	期間	獲得スキル
レベル 1 - 実用的なセキュリティの基礎		
• セキュリティの基本 • オープンソースに関する知識 • 企業ネットワークのセキュリティ • アプリケーションのセキュリティと脆弱性攻撃ブロック • DDoS 攻撃とバンキングの脅威 • 無線 LAN のセキュリティとグローバルモバイルネットワーク • バンキングとモバイルの脅威 • クラウドおよび仮想環境のセキュリティインシデント対応	5 日間	• 公開リソース、専門的検索エンジン、ソーシャルネットワークを使用した、基本的な調査の提供 • セキュリティ保護されたネットワーク境界の作成 • 基本的な侵入テストのスキル • 攻撃種類別のトラフィック調査 • 安全なソフトウェア開発の実施 • 悪意のあるコードインジェクションの識別 • 基本的なマルウェア分析とデジタルフォレンジックの実施
レベル 2 - 一般的なデジタルフォレンジック		
• デジタルフォレンジックの紹介 • ライブ応答と形跡の収集 • Windows レジストリの内部 • Windows アーチファクトの分析 • 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 • デジタル形跡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使用 • Windows OS 内のアーチファクト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用ツールおよび機器の活用
レベル 2 - 一般的なマルウェア分析とリバースエンジニアリング		
• 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則の理解 • 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 • 高速マルウェア分析の実施
レベル 3 - 高度なデジタルフォレンジック		
• 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の実施 • 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
レベル 3 - 高度なマルウェア分析とリバースエンジニアリング		
• 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 • 高度な静的および動的分析テクニック • （手動の解凍） • 難読化解除テクニック • ルートキットとブートキットの分析 • エクスプロイトの分析（.pdf、.doc、.swf など） • Windows 以外のマルウェア分析（Android、Linux、Mac OS）	5 日間	• 世界的なリバースエンジニアリングのベストプラクティスを活用 • リバースエンジニアリング対策テクニック（難読化、デバッグ対策）の認識 • ルートキットおよびブートキットに対する高度なマルウェア分析の適用 • 各種ファイルタイプに埋め込まれたエクスプロイトシェルコードの分析 • Windows 以外のマルウェアの分析

脅威のインテリジェンスサービス

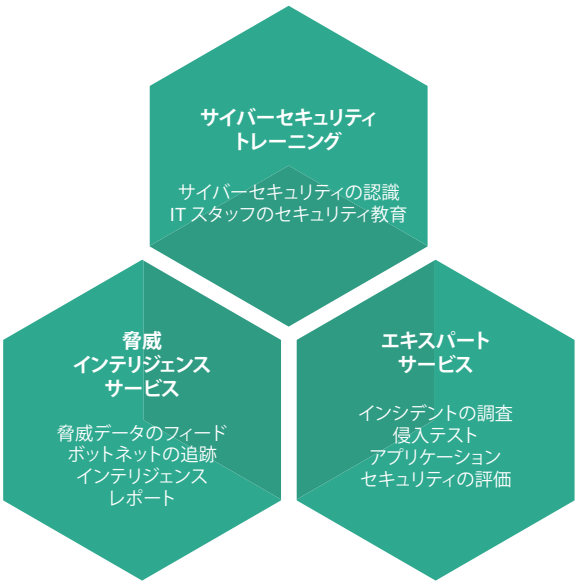
絶えず進化し続ける IT セキュリティの脅威を追跡、分析、解釈、軽減する作業には、非常に大きな労力が必要です。あらゆるセクターの企業で、IT セキュリティの脅威に付随するリスクへの対処に必要な最新情報と適切なデータが不足しています。

Kaspersky Lab のセキュリティ脅威のインテリジェンスサービスを利用することで、お客様は、世界有数の研究者とアナリストのチームが提供する、脅威を緩和するために必要なインテリジェンスにアクセスできます。

サイバーセキュリティのあらゆる側面に関する知識、経験、奥深い情報により、Kaspersky Lab は世界有数の警察機関および政府機関（インターポール、主要 CERT を含む）からパートナーとして信頼されています。このインテリジェンスを、お客様の組織で活用していただけます。

Kaspersky Lab が提供する脅威のインテリジェンスサービスには以下が含まれます:

- 脅威データのフィード
- ボットネットの追跡
- APT インテリジェンスレポート



脅威データフィード提供サービス

絶えず更新される包括的なデータを通じて、サイバー脅威と標的型攻撃に対する知見を提供することで、SIEM、ファイアウォール、IPS/IDS、APT 対策、サンドボックス / シミュレーション技術を含む既存のネットワーク防御ソリューションを強化します。

過去数年でマルウェア群とその変種は急増しており、Kaspersky Lab は現在、1 日あたり約 325,000 種類の新しいマルウェアサンプルを検知しています。これらの脅威からエンドポイントを守るために、ほとんどの組織は、アンチマルウェアソリューションや侵入防止システム、脅威検知システムなどの従来の保護対策を導入しています。変化の急速な環境では、サイバーセキュリティが常にサイバー犯罪の 1 歩先を行くことが求められており、従来のソリューションは、脅威に関する最新情報へアクセスして強化する必要があります。

Kaspersky Lab が提供する脅威データのフィードは、既存のセキュリティ情報およびイベント管理（SIEM）システムに統合することで、追加の保護層を提供することを目的としています。脅威データのフィードを統合することで、たとえば、各種ネットワークデバイスから SIEM に送信されるログを Kaspersky Lab から受け取った URL フィードと関連付けることができます。HP ArcSight SIEM への接続が含まれており、Splunk と QRadar 向けのコネクタも提供されています。

ユースケースおよびサービスのメリット

Kaspersky Lab が提供する脅威データのフィードによるメリットは以下のとおりです:

- 有害な URL に関するデータを活用することで、SIEM ソリューションを補強各種ネットワークデバイス（ユーザーの PC、ネットワークプロキシ、ファイアウォール、その他のサービス）から SIEM に送信されるログを介して、マルウェア、フィッシング、ボットネットの C&C URL に関する情報が SIEM に届けられる
- 絶えず更新される脅威の情報を通じて、ファイアウォール、IPS/IDS、SIEM ソリューション、APT 対策、サンドボックス / シミュレーション技術、UTM アプライアンスなどの主要ネットワーク防御ソリューションを強化
- 脅威に関する有意義な情報と標的型攻撃の背景にある考えをセキュリティチームに提供することで、お客様のフォレンジック機能を改善
- お客様の調査の支援。有害な URL と悪意のあるファイルの MD5 ハッシュ値に関する情報は、脅威調査プロジェクトに貢献する有益な情報

Kaspersky Lab は、3 種類の脅威データフィードを提供しています:

1. 悪意のある URL とマスク
2. 悪意のあるオブジェクトデータベースの MD5 ハッシュ値
3. モバイルスレッドのフィード

フィードの説明

悪意のある URL - 悪意のあるリンクと Web サイトを含む URL。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使用できます。
フィッシング URL – Kaspersky Lab がフィッシングサイトとして識別した URL。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使用できます。
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。
マルウェアハッシュ値（ITW） – KSN が持つインテリジェンスを通じて提供されたもっとも危険かつまん延しているマルウェアを対象とした、ファイルハッシュ値と対応する分類。
マルウェアハッシュ値（UDS） – Kaspersky Lab のクラウド技術を使い、ファイルのメタデータと統計情報に基づいて（オブジェクト自体を保持せずに）検知されたファイルハッシュ値（UDS は緊急検知システムの意）。これにより、その他の手法では検知されない新たな（ゼロデイの）悪意あるオブジェクトを識別できます。
モバイルマルウェアハッシュ値 – 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を検知するためのファイルハッシュ値。
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。
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。

ボットネットの追跡サービス

顧客と評判を脅かすボットネットを特定するための、エキスパートによる監視および通知サービス

多くのネットワーク攻撃はボットネットを使って組織化されています。このような攻撃は通りがかりのインターネットユーザーを対象とする場合もありますが、多くの場合、特定の組織のオンライン顧客が標的となります。

Kaspersky Lab のエキスパートソリューションはボットネットの動作を追跡して、個々のオンライン決済システムやバンキングシステムのユーザーに関連する脅威を迅速に(20 分未満で)通知します。お客様はこの情報を使用し、目下の脅威について、顧客やセキュリティサービスプロバイダ、警察機関に通知および助言することができます。Kaspersky Lab のボットネット追跡サービスを使用して、組織の評判と顧客を保護しましょう。

ユースケースおよびサービスのメリット

- オンラインユーザーを標的としたボットネットがもたらす脅威についての事前警告により、常に攻撃の一歩先を行くことができます。
- オンラインユーザーを狙うボットネットのコマンド & コントロールサーバーの URL 一覧を識別することで、CERT または警察機関に要請を送ってこれらをブロックすることができます。
- 攻撃の性質を理解することで、オンラインバンキングまたは決済キャビネットの機能を強化できます。
- オンラインユーザーの教育を通じて、攻撃に使用されるソーシャルエンジニアリングの認識と被害の防止を可能にします。

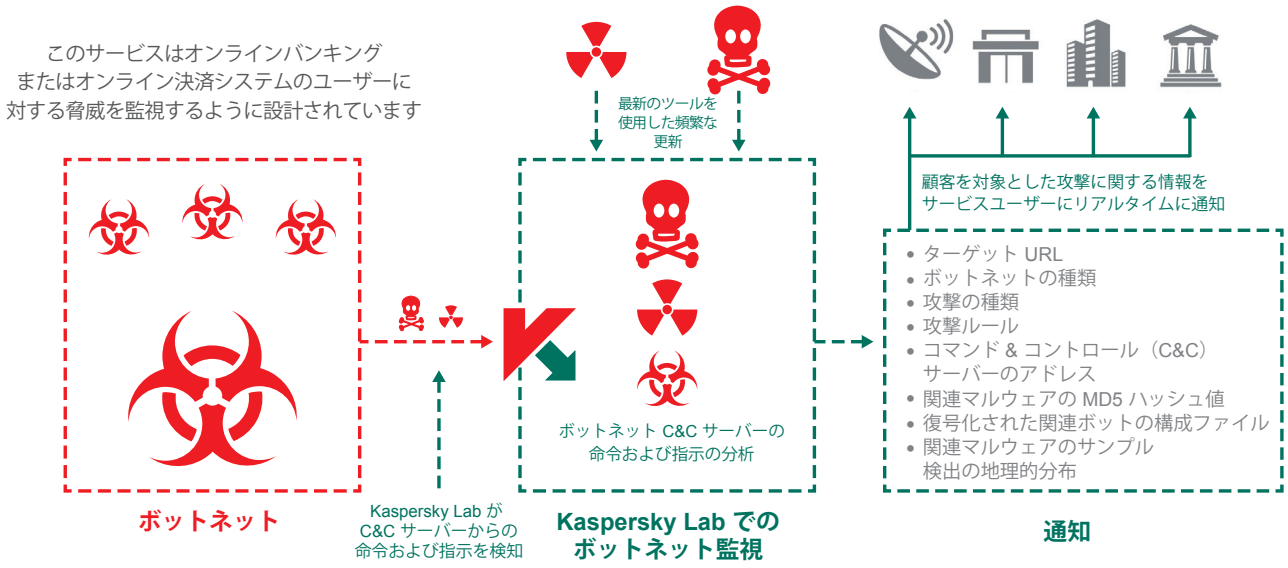
リアルタイムの情報提供による対策:

このサービスは、Kaspersky Lab が監視するボットネット内のキーワードを追跡して、一致したブランド名に関する情報を含む、個別化された通知をサブスクリプションとして提供します。通知はメールまたは RSS を介して、HTML あるいは JSON 形式で提供されます。通知に含まれる内容は以下のとおりです:

- **ターゲット URL** – ボットマルウェアは、ユーザーがターゲット組織の URL にアクセスするのを待ってから攻撃を開始するように設計されています。
- **ボットネットの種類** – 顧客のトランザクションを危険にさらすためにサイバー犯罪者が、どのようなマルウェアの脅威を利用しているのかを正確に識別します。例には、Zeus、SpyEye、Citadel が含まれます。
- **攻撃の種類** – サイバー犯罪者がマルウェアを使用する目的を特定します。例には、Web データインジェクション、画面ワイプ、ビデオキャプチャ、フィッシング URL への転送が含まれます。
- **攻撃ルール** – Web コードインジェクションでどのルールが使用されているかを特定します。例には、HTML リクエスト(GET または POST)、インジェクション前のデータまたは Web ページ、インジェクション後のデータまたは Web ページがあります。
- **コマンド & コントロール(C&C)サーバーのアドレス** – インターネットサービスプロバイダに問題のサーバーを通知して、迅速に脅威を解消できるようにします。
- **関連マルウェアの MD5 ハッシュ値** – マルウェアの検証に使用するハッシュサムを提供します。
- **復号化された関連ボットの構成ファイル** – ターゲット URLの完全なリストを特定します。
- **関連マルウェアのサンプル** – ボットネット攻撃のリバース解析やデジタル科学分析に使用します。
- **検出の地理的分布(上位 10か国)** – 世界中から取得したマルウェアサンプルの統計データを提供します。

ボットネットの追跡:アーキテクチャ

C&C サーバーから



Kaspersky Lab のソリューションには、各種のサービス内容と監視対象 URL 数に応じて、標準版とプレミアム版があります。お客様に適したパッケージを確認するには、カスペルスキーまたは再販業者にお問い合わせください。

サブスクリプションレベルとサービス内容

プレミアム版

メールまたは JSON 形式での通知 — **監視対象 URL 数:10**

- 復号化された関連ボットの構成ファイル
- 関連マルウェアのサンプル（要望に応じて）
- 関連マルウェアサンプルの検出に対する地理的分布

標準版

メール形式での通知 — **監視対象 URL 数:5**

- ターゲット URL（ボットプログラムがユーザーを狙っている URL の特定）
- ボットネットの種類（Zeus、SpyEye、Citadel、Kins など）
- 攻撃の種類
- 攻撃ルール:Web データインジェクション、URL、画面、ビデオキャプチャなど
- C&C アドレス
- 関連マルウェアの MD5 ハッシュ値

「APT」インテリジェンスレポート

注目度の高いサイバースパイキャンペーンの認識と知識を高める、包括的かつ実用的な Kaspersky Lab のレポート

インテリジェンスレポートで提供される情報とツールを活用すると、新しい脅威と脆弱性に素早く対応できるため、既知の経路からの攻撃をブロックし、先進の攻撃による損害を軽減し、セキュリティ戦略を強化することができます。

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 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 Lab のインテリジェンスレポートを通じて、誰よりも早く、詳しい情報を手に入れましょう。

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技術データを含むカスペルスキー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 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、サイバー犯罪者と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、ただちにお客様に警告を送ります。また、お客様は、企業のセキュリティ戦略にとって強力な研究および分析コンポーネントとなる、Kaspersky Lab の完全な APT レポートデータベース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メリット:

- **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。
- **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、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**:標準形式(openIOC、STIX など)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(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。

注 - サブスクリプションの制限事項

本サービスのレポートに含まれる情報の機密性と固有性により、レポートのサブスクリプションは信用ある政府、公共団体、民間団体に限定することが義務付けられています。

「専用」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。

お客様専用のカスペルスキー脅威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 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、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 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、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 Lab のサービスを使用し始めるためにインフラストラクチャ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。

エキスパートサービス

Kaspersky Lab のエキスパートサービスは文字どおり、社内のエキスパートが提供するサービスです。Kaspersky Lab のエキスパートの多くは、各自が世界的な権威であり、その知識と経験が、セキュリティインテリジェンスの世界的リーダーとしてのカスペルスキーの評判を支えています。

まったく同じ IT インフラストラクチャは存在せず、また、もっとも攻撃力の高いサイバー脅威は、個々の組織に潜む特定の脆弱性を悪用するように個別設計されているため、Kaspersky Lab のエキスパートサービスも目的に特化した個別サービスとなっています。以降に記載するサービスによりプロフェッショナルツールキットが構成されます。お客様と協業していく中で、これらのサービスの一部（またはすべて）を、必要に応じて部分的または全体として適用します。

このサービスの第一の目的は、エキスパートアドバイザーとしてお客様と一対一で協力することで、お客様がリスクを評価し、セキュリティを強化して、将来的な脅威を緩和できるように支援することです。

エキスパートサービスには以下が含まれます:

- インシデントの調査
- 侵入テスト
- アプリケーションセキュリティの評価

インシデントの調査サービス

デジタルフォレンジック - マルウェア分析

個別化されたインシデント調査を通じて、お客様が IT セキュリティインシデントを識別し、解決するための支援を行います。

企業ネットワークに対するサイバー攻撃の危険性は増す一方です。これらの攻撃は、犯罪者が選んだ標的に固有の脆弱性を悪用するように個別設計されており、しばしば、機密情報または知的財産の盗用や破棄、業務への悪影響、産業設備の損傷、金銭の盗難を引き起こします。

このように巧妙かつ周到な攻撃から企業を守る対策は、ますます複雑になっています。組織が実際に攻撃されているかどうかを明確にすることすら難しい場合もあります。

Kaspersky Lab のインシデント調査サービスは、脅威の詳しい分析を提供し、インシデントの解決に向けた適切な手順を助言することで、組織が防御戦略を策定できるように支援します。

サービスのメリット

Kaspersky Lab のインシデント調査サービスを利用すると、お客様は当面のセキュリティ問題を解決し、マルウェアの動作とそれによる結果を理解し、修正策をアドバイスできるようになります。また、以下の間接的なメリットもあります:

- サイバー感染によって生じる問題の解決コストを削減
- 感染した PC から流出する可能性のある機密情報の漏洩を阻止
- 感染による業務プロセスへの損害に起因する評判低下リスクを軽減
- 感染によって障害の発生した PC を正常な状態に復旧

Kaspersky Lab の調査は、デジタルフォレンジックとマルウェア分析に関する実用的な専門知識を持つ、経験豊かなアナリストによって実施されます。調査が完了すると、サイバー調査の完全な結果と修正手順の提案を含む詳細なレポートが提供されます。

デジタルフォレンジック

デジタルフォレンジックは、インシデントを詳しく描写することを目指した調査サービスです。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、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、ネットワークトレース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、形跡を集めてインシデントの概要をまとめます。Kaspersky Lab 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、修正手順を含む詳細レポートを提供します。

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、組織に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と脅威の動作および目的(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。
- **修正シナリオ**: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。

提供方法

Kaspersky Lab の調査サービスを利用する方法には以下があります:

- 合意済みのインシデント数に基づく定額制
- 個々のインシデントへの対応

侵入テストサービス

潜在的なサイバー攻撃から IT インフラストラクチャ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情報システム、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。

IT とセキュリティの専門家が、すべてのネットワークコンポーネントを侵入者から保護しながら、正規ユーザーが十分に使用できるようにするために賢明に取り組んでいても、1つの脆弱性のせいで、情報システムを乗っ取ろうと画策するサイバー犯罪者に入り口が開かれる場合があります。

侵入テストは、悪意のあるサイバー犯罪者が企業ネットワークのセキュリティ制御をすり抜けて、重要システムの高い権限を得ようとするような、潜在的な攻撃シナリオを対象とした現実的なデモです。

Kaspersky Lab の侵入テストサービスは、インフラストラクチャ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、修正措置と改善点を提案します。

Kaspersky Lab の侵入テストを使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 インフラストラクチャに応じて、以下のいずれか(またはすべて)の侵入テスト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 Lab のエキスパートがお客様の拠点を訪問して、WiFi セキュリティ管理の状況を分析

侵入テストの範囲には IT インフラストラクチャのどの部分を含めることもできますが、ネットワーク全体か最大の区分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。

侵入テストの結果

侵入テストサービスの目的は、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。これには、以下が含まれます:

- 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更新が適用されていない旧式のハードウェアおよびソフトウェアバージョンの使用による脆弱性
- 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、推奨される修正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。

侵入テストに対する KASPERSKY LAB のアプローチ

侵入テスト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うえで、Kaspersky Lab のセキュリティエキスパートによって厳密に制御、実行されます。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:

- 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。

アプリケーションセキュリティの評価サービス

企業アプリケーションを社内で開発する場合も、サードパーティから購入する場合も、1つのコーディングエラーから攻撃に対する脆弱性が生み出され、相当な金銭的損害や評判の低下につながる可能性があります。また、新しい脆弱性が、ソフトウェアの更新や安全性を欠いたコンポーネント構成によってアプリケーション・ライフサイクル中に生じたり、新しい攻撃手法によってもたらされたりする場合もあります。

Kaspersky Lab のアプリケーションセキュリティ評価サービスは、大規模なクラウドベースソリューションや ERP システム、オンラインバンキング、その他の固有ビジネスアプリケーションから、各種プラットフォーム（iOS、Android など）上の組み込みアプリケーションとモバイルアプリケーションにいたるまでの、あらゆる種類のアプリケーションに含まれる脆弱性を発見します。

Kaspersky Lab のエキスパートは、国際的なベストプラクティスに実際の知識と経験を組み合わせて、お客様の組織を脅威にさらす可能性のあるセキュリティ上の不具合を検出します。対象となる脅威の例を以下に挙げます:

- 機密データの流用
- データとシステムの変更および侵入
- サービス妨害攻撃の開始
- 詐欺行為の企て

Kaspersky Lab の推奨に従って、アプリケーション内で発見された脆弱性を解消することで、攻撃を防止できます。

サービスのメリット

Kaspersky Lab のアプリケーションセキュリティ評価サービスが提供するメリットは以下のとおりです:

- **アプリケーションへの攻撃に利用される脆弱性を事前に検知、解消する**ことで、財政、業務、評判に損害が及ぶことを防止します。
- 問題の解決にかなりの中断とコストがかかるユーザー環境に進む前に、アプリケーションが開発またはテスト段階にある時点で脆弱性を突き止めることで、**修正コストを節約**します。
- **セキュリティ保護されたアプリケーションの作成と維持に貢献する**、安全なソフトウェア開発ライフサイクル（S-SDLC）をサポートします。
- **アプリケーションセキュリティを対象とした**政府、業界、社内の標準（PCI DSS、HIPAA など）に準拠します。

サービスの範囲とオプション

評価対象となるアプリケーションには、公式 Web サイトと、組み込みおよびモバイルアプリケーションを含むビジネスアプリケーション（標準またはクラウドベース）が含まれます。

サービスはお客様のニーズやアプリケーションの特性に合わせて調整され、以下を含めることができます:

- **ブラックボックステスト** – 外部攻撃のエミュレート
- **グレーボックステスト** – さまざまなプロファイルを持つ正規ユーザーのエミュレート
- **ホワイトボックステスト** – ソースコードを含むアプリケーションへの全面的アクセスによる分析（発見できる脆弱性の数という面でもっとも効果的）
- **アプリケーションファイアウォールの有効性評価** – ファイアウォール保護を有効化および無効化した状態でアプリケーションをテストして脆弱性を検出し、潜在的なエクスプロイトがブロックされているかどうかを検証

評価結果

Kaspersky Lab のアプリケーションセキュリティ評価サービスで認識される可能性のある脆弱性は以下のとおりです:

- 多要素認証を含む認証と認可の不具合
- 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)
- 詐欺につながる論理的脆弱性
- 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)
- 脆弱な暗号化の使用
- クライアントサーバー通信での脆弱性
- 安全性を欠いたデータの保管または転送(決済システムでの PAN マスキングの欠如など)
- セッション攻撃につながるものを含む構成の不具合
- 機密情報の漏洩
- 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

結果は最終レポートで提供され、評価のプロセス、結果、発見された脆弱性、推奨される修正方法に関する詳しい技術情報と、経営への影響をまとめ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。

アプリケーションのセキュリティ評価に対する KASPERSKY LAB のアプローチ

アプリケーションのセキュリティ評価は、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うえで、Kaspersky Lab のセキュリティエキスパートによって、手動方式と自動化ツールを利用した方式の両方で実施されます。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:

- Web Application Security Consortium(WASC)Threat Classification
- Open Web Application Security Project(OWASP)Testing Guide
- OWASP Mobile Security Testing Guide
- お客様の事業と地域に応じたその他の標準

プロジェクトチームのメンバーは、各種のプラットフォーム、プログラミング言語、フレームワーク、脆弱性、攻撃手法を含むセキュリティ分野に関する、最新で深い実践的知識を持つ経験豊かな専門家です。主要な国際カンファレンスでの講演実績があり、Oracle、Google、Apple、Facebook、PayPal を含む大手のアプリケーションおよびクラウドサービスベンダーに対して、セキュリティアドバイザリサービスを提供しています。

提供方法:

セキュリティ評価サービスの種類、対象となるシステムの特性、作業条件に対するお客様要件に応じて、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。ほとんどの場合はリモートで実施されます。


Twitter.com/
kaspersky_japan


Facebook.com/
KasperskyLabsJapan


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

パートナー検索
http://www.kaspersky.co.jp/partners

本書に記載した製品およびサービスの詳細について、また、これらのサービスを組織のセキュリティに適用する方法については、intelligence@kaspersky.com までメールでお問い合わせください。

契約条件（作業範囲、スケジュール、ローカルサービスの利用可能性、提供言語、コストを含むがこれに限定されない）は、地域ごとに異なる可能性があります。

セキュリティインテリジェンスサービスカタログ 2015 年 8 月

KASPERSKY lab