kaspersky BRING ON THE FUTURE

Kaspersky® Web Traffic Security

Web ベースの脅威に対する戦略的防御

Kaspersky Web Traffic Security は、企業の IT ネットワークをインターネット上の危険から保護すると同時に、データ漏洩のリスクを軽減し、インターネットの使用を統制して生産性を向上させます。幅広い機能を備え、汎用性と応答性に優れたこのアプリケーションを使用することで、企業のさまざまなシナリオを迅速かつ効果的に保護することができます。Kaspersky Web Traffic Security は、Kaspersky Security for Internet Gateway のコアコンポーネントであり、インフラストラクチャ全体を保護する Kaspersky の企業向け総合セキュリティソリューションの重要な構成要素です。

特長

- 多層防御によるマルウェア対策とフィッシング対策
- ゼロアワー脅威に対する保護
- コンテンツフィルタリング
- ランサムウェアのブロック
- Web コントロール
- 高負荷ネットワークに対応できる高い拡張性
- Kaspersky Security Network が入手したグローバルな脅威インテリジェンスの活用
- 管理と Web 利用へのロールベースのアクセス
- Microsoft Active Directory のサポート
- MSP や分散型の事業部門に対応したマルチテナント機能
- スタンドアロンアプリケーションまたはすぐに使用できるアプライアンスで提供
- AWS および Azure パブリッククラウドで使用可能
- Kaspersky Anti Targeted Attack との統合による自動対応

主な利点

保護と制御の組み合わせにより感染リスクを軽減

侵入してくる脅威をゲートウェイレベルでブロックすることでエンドポイントへの到達を阻止し、ソーシャルエンジニアリングを利用した脅威や脆弱性悪用のリスクを軽減します。また、インターネットリソースの利用を管理および制限することにより、ユーザーのミスが原因のインシデントやシャドー IT のまん延を最小限に抑えます。

企業ゲートウェイの保護効果を強化

業界最高レベルの保護技術を備え、優れた検知率と極めて低い誤検知率を実現するこのアプリケーションを、Kaspersky 製品ファミリーに統合できます。または、現在ご使用中の Web ゲートウェイ対策のパフォーマンスを大幅に強化する目的で、このアプリケーションを使用することもできます。

さまざまな要件に対応

ニーズと企業の構造に合わせてスケーリングし、階層的な展開、複数ノードとマルチテナント管理、およびロールベースのアクセス制御と委任をサポートします。スリム化された構成オプションにより、通信事業者などの環境で広範な帯域幅を処理できます。

スタンドアロンアプリとソフトウェアアプライアンス	構成済みの独自のプロキシサーバーを含む一体型のソフトウェアアプライアンスを選択してデプロイを簡素化することも、スタンドアロンアプリとして既存のシステムにインストールするように選択することもできます。どちらの場合も、最小限の手間で済みます

機能

データサイエンスを活用した多層型の脅威保護および制御

Kaspersky の次世代型アンチマルウェア保護および制御には、以下を含む複数のプロアクティブなセキュリティ層が組み込まれています。

アンチマルウェア

機械学習を活用したプロアクティブな検知、分析、およびフィルタリング技術による、業界で実証された保護で、スパイウェア、金融機関を狙ったトロイの木馬、ランサムウェア、マイナー、ワイパーなどのマルウェアの脅威を特定し、ブロックします。

新たな脅威をリアルタイムで検知

Kaspersky Security Network のインフラストラクチャは、世界中の数千万人ものユーザーと世界トップレベルの調査から入手した最新のインテリジェンスを駆使し、潜在的な脅威が発生した場合には、極めて低い誤検知率でリアルタイムに検知します。

サンドボックスでのエミュレーション

安全なエミュレーション環境で添付ファイルを実行、解析し、極めて高度で難読化されたマルウェアからも保護します。

スクリプトの検知

エンドポイントに送信される一見無害なファイルにマルウェアを埋め込むスクリプトや、Web ベースのドライブバイ攻撃に使用されるスクリプトを識別して、対処します。

レピュテーションベースのフィルタリング

絶えず更新される Kaspersky Security Network のクラウドデータベースから提供されるファイルとアドレスのレピュテーションに基づいて、詳細な分析を必要とせずに、不審なまたは望ましくないファイルとインターネットリソースをブロックできます。

高度なフィッシング対策

検知モデルはクラウドベースの保護をサポートしており、画像や言語のチェック、特定のスクリプトなど 1,000 を超える基準を使用したニューラルネットワークをベースとする分析と、世界中から入手した悪意のあるフィッシング URL や IP アドレスに関するデータを組み合わせることで、既知、未知、およびゼロアワーのオンラインフィッシングから保護します。

コンテンツフィルタリング

ファイル名、拡張子、種類（形式認識機能を使用して、拡張子を偽装したファイルを検出）、サイズ、MIME タイプ（動画、画像など）、ハッシュ値などのパラメータに基づき、潜在的な問題がある、または無関係な種類のファイルの送信を禁止できます。

Web 管理

管理者は、事前定義されたカテゴリまたは独自のリストに基づき、Web リソースへのアクセスをブロックするルールを作成することで、リスクを軽減すると同時に、インターネットでユーザーの作業の妨げとなる要素を排除することができます。必要に応じて「デフォルトで拒否」シナリオを導入し、ユーザーやグループの作業には必要がない Web リソースへのアクセスを制限できます。

配置オプション

スタンドアロンアプリ[1] を選択して現在ご使用のシステムに統合するか、すぐに使用できるソフトウェアアプライアンスを選択してデプロイを簡素化できます。

ソフトウェアアプライアンスのオプションには、以下の特長があります。

- 一体型で設定が容易：構成済みのプロキシサーバーが含まれるため、Secure Web Gateway（SWG）のデプロイに必要なすべての設定がわずか数クリックで完了します。
- 管理：アプライアンスの Web インターフェイスには、組み込まれたプロキシサーバーを管理するために必要なものがすべて含まれているため、コマンドラインベースの構成プロセスの手間がありません。
- トラフィック監視がすぐ可能：いわゆる「SSL/TLS バンピング」が事前に構成されているため、いくつかの簡単な管理アクションを実行するだけで、暗号化された Web トラフィックの保護を開始できます。
- パブリッククラウドで使用可能：特にクラウドベースのインフラストラクチャに対応したワークロードイメージが含まれるため、Microsoft Azure および AWS パブリッククラウドですぐにデプロイできるイメージを使用できます。

スタンドアロンアプリでは、以下が可能です。

- リソースを効率的に活用： ワークロードを完全に分離する必要はありません。このアプリを、他のアプリと一緒に複数の機能を持つサーバーにインストールできます。
- 既存の構成と緊密に統合： 複雑な環境では、他のゲートウェイコンポーネントとは別にセキュリティアプリをインストールおよび構成できると、より優れた効率性が実現します。

柔軟性と統合

適応性に優れ、ほぼ無限にスケーリング可能な Kaspersky Web Traffic Security は、現在ご使用の IT インフラストラクチャにすぐに統合できるように設計されています。

ICAP に対応したシステムのセキュリティ

プロキシサーバーだけでなく、ICAP プロトコルをサポートするすべてのデバイスでトラフィックが保護されます。これには、ネットワークアタッチストレージ（NAS）や、内部のセキュリティソリューションでは保護されないその他のシステムが含まれます。

Kaspersky Anti Targeted Attack との双方向の統合

Kaspersky が提供する標的型攻撃検知の強力なプラットフォームと API ベースで統合することで、高度な脅威の詳細分析に追加のコンテキストが提供されると同時に、インターネット上の攻撃コンポーネントや攻撃者によるコマンドの送信、別のペイロードの展開、窃取したデータの取り出しなどのアクティビティが自動的にブロックされます。

SIEM との統合

広く使用されている syslog とともに、共通イベント形式（CEF）で情報がエクスポートされるため、セキュリティ情報およびイベント管理（SIEM）システムのコンテンツが充実します。

マネージドサービスプロバイダーに最適

強力な Web ゲートウェイ保護サービスにより、以下の機能を使用して、顧客に代わって簡単に管理できます。

- マルチテナント機能：サービスを提供する顧客ごとに専用のエリア（「ワークスペース」）を割り当てて、必要に応じて「グローバル」ポリシーと「ローカル」ポリシーを組み合わせることで、顧客を個別に管理できます。
- ロールベースのアクセス制御：特定のワークスペースで、サービスを提供する顧客ごとに適切なレベルの制御を設定できます。
- サブスクリプションベースのライセンスにより、毎月のサービス料金および予算管理のモデルが補完されます。（2020年4月以降提供予定）

簡便な管理

Kaspersky Web Traffic Security は、柔軟で使いやすい管理システムを提供します。

一元管理のコンソール

単一の Web インターフェイスの使用により、優れた可視性と管理の容易性を実現し、プロキシやストレージを含む、ICAP に対応したすべてのシステムのセキュリティを管理します。

利便性の高いダッシュボード

ゲートウェイレベルで企業セキュリティの現在の状況を評価するために必要なすべてのものが単一のダッシュボードにまとめられているため、迅速な対応が求められるイベントも含めて、状況の全容を速やかに把握できます。

脅威イベントの管理

イベントを中心に据えたアプローチを使用して脅威分析の結果を出力し、活動をリアルタイムに表示します。インターネット上でのユーザーの振る舞いも分析します。

柔軟なルール設定

柔軟で使いやすいルール設定システムにより、ゲートウェイセキュリティを容易にきめ細かく管理できます。

Active Directory との統合

ロールベースのアクセスルールとセキュリティポリシーの設定や継続的な同期が、ネットワークやインフラストラクチャに反映されます。

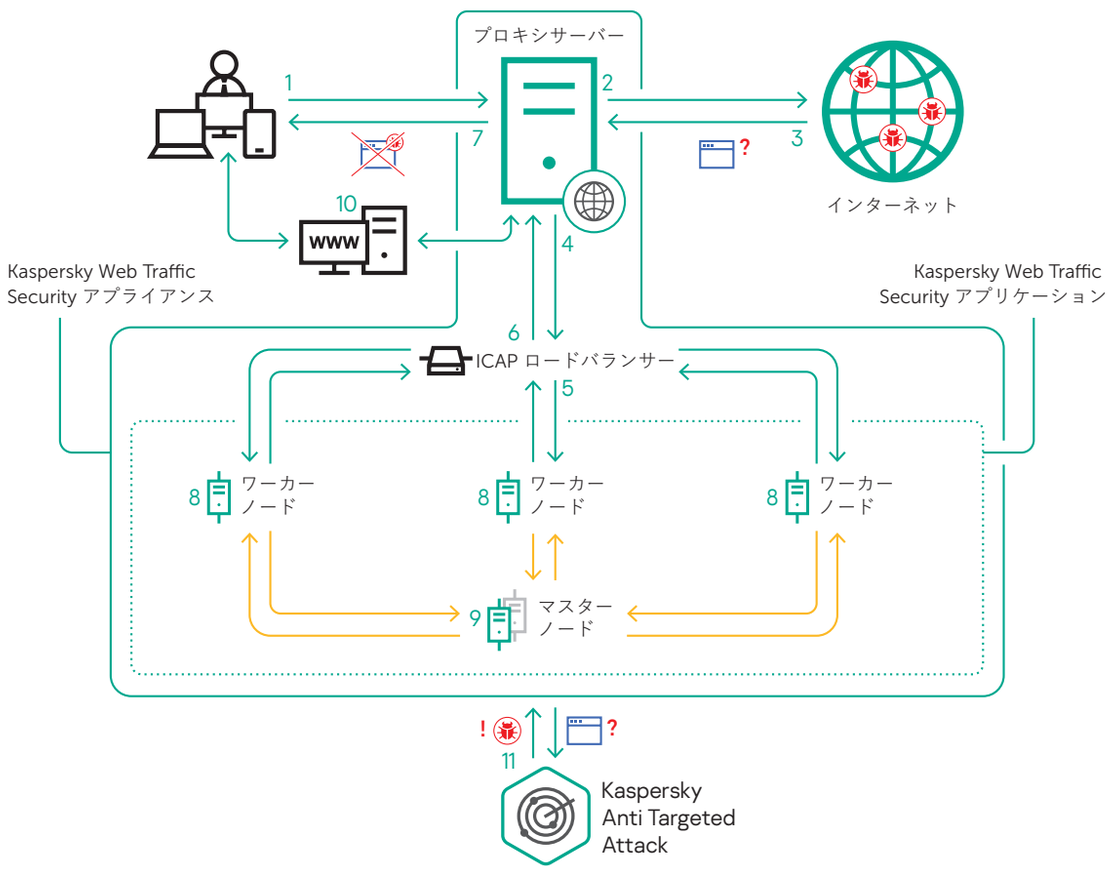
ロールベースのアクセス制御（RBAC）

さまざまな管理ロールを定義して、それぞれに割り当てる権限と制限を区別することができます。これにより、内部でタスクを委任したり、サービスを提供する顧客に適切なレベルの制御を設定したりすることができます。

マルチテナント機能

事業部門や顧客ごとに専用のエリア（「ワークスペース」）を割り当てて、必要に応じて「グローバル」ポリシーと「ローカル」ポリシーを組み合わせることで、個別に管理できます。

Kaspersky Web Traffic Security のアーキテクチャ



1. ユーザーが、企業のプロキシサーバーを通じて（http(s)、ftp 経由）インターネットの情報をリクエストします。
2. プロキシサーバーはリクエストされた Web リソースを検索します。
3. リクエストされたリソースがプロキシに送信されます。
4. プロキシサーバーはロードバランサーを通じて、ICAP を使用するシステムにオブジェクトを送信します。
5. 検査のため、ロードバランサー* はワーカーノードを選択してオブジェクトを送信します。
6. ワーカーノードは判断結果をプロキシサーバーに返します。
7. プロキシサーバーは、安全であることが実証された Web ページとオブジェクト、および検出された脅威に関する判断結果をユーザーに送信します。
8. ワーカーノードは、トラフィック処理ルールに基づいてオブジェクトをスキャンするために、ICAP サーバーとして機能します。デフォルトのルールには、アンチマルウェアとアンチフィッシングの検査が含まれます。URL 分類とコンテンツフィルタリングも使用できます。
9. 中央の（マスター）ノードは、イベントデータの収集と管理を担います。設定の管理に使用する Kaspersky Web インターフェイスをホストするほか、セキュリティイベントとシステム正常性をリアルタイムに監視するダッシュボードも提供します。
10. Windows ドメインコントローラは、Kerberos または NTLM を通じて、プロキシサーバー上でユーザー認証やデバイス認証を行います。
11. 高度な分析の結果は、高度な脅威の要素をブロックするために使用されます。

ハードウェアとソフトウェアの要件

Kaspersky Web Traffic Security 6.1 スタンドアロンアプリケーションのハードウェア最小要件
- CPU：Intel Broadwell 以降、8 コア
- RAM：16 GB
- 8 GB 以上のスワップ用空き領域
- アプリケーションのインストールおよび一時ファイルとログファイルの保存用としてハードドライブ上に 200 GB の空き領域

Kaspersky Web Traffic Security 6.1 スタンドアロンアプリケーションのソフトウェア最小要件
- Squid バージョン 3.5.x または 3.6 以降
- Ubuntu 18.04.2 LTS
- CentOS 7.6
- RHEL 7.6、8
- Debian 10
- SLES 15
- Apache バージョン 2.2 または 2.4 以降

Kaspersky Web Traffic Security の Web インターフェイスを実行するには、次のいずれかのブラウザーをコンピューターにインストールする必要があります
- Mozilla Firefox 67 以降
- Microsoft Internet Explorer 11 以降
- Microsoft Edge 44 以降
- Google Chrome バージョン 75 以降

その他の要件
- Ngnix バージョン 1.10.3、1.12.2、または 1.14.0
- 負荷分散用に、Haproxy バージョン 1.5（個別に構成する必要があります）

LDAP 統合の用途で求められる Windows Server のエディション
- Windows 2012 R2 Standard
- Windows 2016 Standard
- Windows 2019 Standard

Secure Web Gateway 一体型アプライアンスのハードウェア最小要件
- CPU：Intel Broadwell 以降、8 コア
- RAM：16 GB
- HDD：200 GB

Kaspersky Web Traffic Security 6.1 セキュア Web ゲートウェイソフトウェアアプライアンス（仮想プラットフォーム）のソフトウェア最小要件
- VMware ESXi 6.5 Update 2/6.7 Update 1
- Microsoft Hyper-V Server 2016/2019

Secure Web Gateway アプライアンスの Web インターフェイスを実行するには、次のいずれかのブラウザーをコンピューターにインストールする必要があります
- Mozilla Firefox 67 以降
- Microsoft Internet Explorer 11 以降
- Microsoft Edge 44 以降
- Google Chrome バージョン 75 以降

その他の要件
- 負荷分散用に、Haproxy バージョン 1.5（個別に構成する必要があります）

株式会社カスペルスキー

製品情報：

www.kaspersky.co.jp/small-to-medium-business-security/proxy-web-traffic

ご購入相談窓口：

jp-sales@kaspersky.com

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
中小規模企業向け IT セキュリティ：kaspersky.com/business
大企業向け IT セキュリティ：kaspersky.com/enterprise

www.kaspersky.co.jp

2019 AO Kaspersky Lab.All rights reserved.
登録商標およびサービスマークは、それぞれの所有者に属しています。

購入方法

Kaspersky Web Traffic Security は、次の製品やソリューションで有効化されるアプリケーションです。

- **Kaspersky Security for Internet Gateway**

Kaspersky は、実証された独立した企業で、透明性が確保されています。Kaspersky は、テクノロジーによって私たちのより良い生活、より安全な世界の構築に取り組んでいます。そのため Kaspersky は、テクノロジーがもたらす無限の機会をすべての人がすべての場所で享受できるよう、そのテクノロジーを守ります。より安全な未来に向けて、サイバーセキュリティを実現します。

詳しくはこちら：kaspersky.co.jp/transparency

Proven.
Transparent.
Independent.