LGWAN対応の次世代セキュリティ

カスペルスキーは、LGWAN-ASPを無償で提供しています。

エンドポイントセキュリティだけでなく、ハイブリッドクラウド環境向け
セキュリティ、メールセキュリティへの定義ファイル更新を可能にします。

■ 費用

LGWAN-ASP利用費用　無償

※カスペルスキーのセキュリティ製品のライセンス費用は別途かかります。

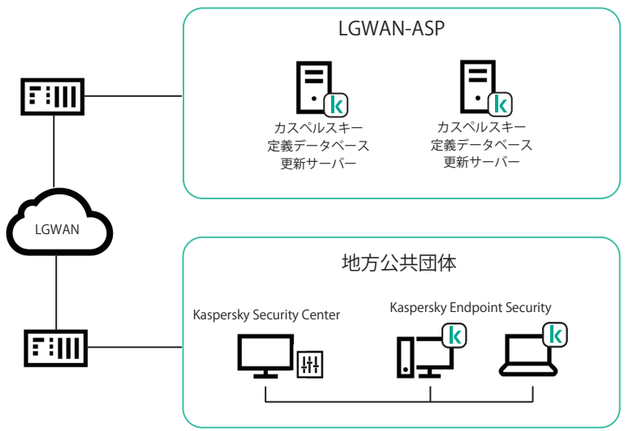
■ 利用可能な製品

- Kaspersky Endpoint Security for Business (Windows、Mac、Linux、Android)
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway

ご利用につきましては、お問い合わせ先までご連絡ください。
接続に必要な手続きをお送りいたします。

kaspersky　BRING ON THE FUTURE

LGWAN-ASP概念図



1. Kaspersky Security Center* が、更新サーバーに対して定義データベース取得をリクエスト
2. 取得した最新の定義データベースを、配下のKaspersky Endpoint Security for Business利用ユーザーへ配信

* マルチプラットフォーム (PC、サーバー、モバイルおよび仮想環境)のセキュリティを一元管理するためのツール

お問い合わせ先

株式会社カスペルスキー

TEL: 03-3526-8530　Mail: jp-sales@kaspersky.com

LGWAN-ASP定義データベース配信サービスの詳細はこちらをご覧ください。
https://kasperskylabs.jp/biz/lgwan.html

kaspersky

企業活性、地方創生、イノベーション
月刊事業構想
PROJECT DESIGN
より抜粋

東京都立川市
LGWAN対応で情報セキュリティを強化

複雑化する
サイバー攻撃から
庁内情報を守る

東京都立川市　LGWAN対応で情報セキュリティを強化

「未知の脅威」から庁内情報を守る

サイバー攻撃が高度化・複雑化している中で、立川市はウイルス対策製品をリプレースし、カスペルスキー製品を導入した。製品の選定にあたっては、未知の脅威にも対応できる保護性能や、LGWAN環境でも運用しやすく、高いレベルで情報セキュリティを維持・向上できることが決め手となった。

自治体に求められる強固な情報セキュリティ

東京・多摩地域の中心都市であり、JRの駅周辺には多くの商業施設やオフィスが集積する立川市。人口約18万人の暮らしを支える立川市役所では、情報化政策を展開するにあたっての基本方針として、「ICTマネジメント」と「情報セキュリティ」の2つを柱に掲げている。

マイナンバーなど高度な個人情報を扱う自治体には、強固な情報セキュリティが求められる。総務省が打ち出した方針により、現在、各自治体では住民基本台帳や税、社会保障などの情報を扱う基幹系システムと外部のインターネットが分離されている。マイナンバー等の情報連携に活用されるLGWAN（エルジーワン、地方公共団体の庁内LANを相互に接続する行政専用のネットワーク）もインターネットから切り離され、外部からの脅威に対する情報セキュリティを高めるとともに、情報流出への対策も徹底されている。

立川市役所では、約1500台のクライアント端末にカスペルスキー製品を導入。2019年3月から運用を開始している

浜野創太
立川市 情報推進課 推進係

立川市も国の方針や複雑化するリスクに対応し、情報セキュリティの向上に取り組んできた。情報資産を保護・管理する庁内システムやマネジメントを随時見直していく中で、2019年3月に運用を開始したのが、カスペルスキーのセキュリティ製品『Kaspersky Endpoint Security for Business（KESB）』だ。

「ふるまい検知」で未知の脅威に備える

「巧妙にウイルスを仕込んだ標的型攻撃や、不特定多数にばら撒かれるランサムウェアなど、サイバー攻撃は高度化・複雑化しています。これまでにないタイプの攻撃も増える中で、未知の脅威に対応するためにKESBを導入しました。立川市の正規職員は1071名（2019年4月1日時点）。約1500台のクライアント端末にKESBを導入しています」

情報セキュリティ、「組織」の10大脅威（2019）

1位	標的型攻撃による被害
2位	ビジネスメール詐欺による被害
3位	ランサムウェアによる被害
4位	サプライチェーンの弱点を悪用した攻撃の高まり
5位	内部不正による情報漏えい
6位	サービス妨害攻撃によるサービスの停止
7位	インターネットサービスからの個人情報の窃取
8位	IoT機器の脆弱性の顕在化
9位	脆弱性対策情報の公開に伴う悪用増加
10位	不注意による情報漏えい

出典:IPA（独立行政法人 情報処理推進機構）

そう語るのは、立川市情報推進課推進係・浜野創太氏だ。立川市では、2018年にPC端末のリプレースを実施。その機会に合わせて、ウイルス対策製品の見直しを行った。

複数の製品が候補となる中でKESBを選んだ決め手の1つは、「ふるまい検知」だったという。ふるまい検知とは、ウイルス定義データベースだけに頼らず、組織内のプログラムを常時監視し、疑わしいふるまいをしているプログラムを「ウイルスの可能性がある」と自動的に判定してブロックし、感染を防ぐ機能だ。

「ふるまい検知ならば、感染してからそれを隔離するのではなく、怪しいプログラムを事前に検知してリスクを未然に防ぐことができます。未知の脅威に対応するには、ふるまい検知を備えた製品が必要だと考えていました。その中でも、KESBが最もコストパフォーマンスに優れていると判断しました」

立川市が以前使っていたウイルス対策製品では、アラートが出ることはほとんどなかったという。それがKESBの導入後、クライアント端末からのアラートが一気に増えた。従来の製品では見逃されていたリスクもKESBは検知しているのだ。カスペルスキーの技術力の高さは世界的に認められており、同社の製品は世界中の企業や重要インフラ、政府機関に導入され、4億人以上のユーザー、27万以上の企業・組織で利用されている。

立川市情報推進課では安全性の向上と効率的な管理の両立を図るために、セキュリティポリシーを見直しながらKESBを運用している。導入から約半年、特に業務の中断や組織内の混乱を伴うこともなく、安心して運用ができているという。

「職員はセキュリティ品が新しくなったことを意識することなく、日々の業務に励んでいます」

KESBは、管理者が単一の管理コンソールで庁内のセキュリティ情報をすべて把握・管理できるようになっている。セキュリティポリシーの設定や、それを庁内のすべてのクライアント端末に適用するのも容易であり、運用の負荷を軽減する仕組みになっている。

LGWANへの対応も導入の決め手に

立川市はLGWANに接続するPC端末にKESBを導入しているが、ふるまい検知とともに、カスペルスキーが無償で提供しているLGWAN-ASPによる定義データベース配信サービスも導入の決め手になったという。

「行政内に閉じたネットワークで利用しますから、定義データベースの更新のためにインターネットにつなぐようなシステムでは、運用がしづらいと考えました。LGWAN環境において、最新の定義データベースを配信するサービスがあることもKESBを選んだ理由の1つです」

また、立川市はKESBのデバイスコントロール機能を活用し、職員がUSBメモリを端末に接続すると自動的にスキャンするように設定している。

「以前のウイルス対策製品では、職員が手動でスキャンする仕組みでした。庁内のルール上、USBメモリを利用する時は、まずLANケーブルを取り外してから端末にUSBメモリを接続するという決まりになっていますが、人の努力に頼るだけでなくシステム面でも対策を講じています」

情報セキュリティにおいては、脆弱な部分が1ヵ所でもあると、そこをついて脅威が侵入して被害を及ぼす恐れがある。立川市はKESBをはじめ、数々の仕組みで情報資産の保護と管理に万全を期しているが、人的対策にも力を注いでいる。

「職員一人ひとりがリスクをきちんと認識して対応できるように、集合研修やeラーニングを行っています。今後も、情報セキュリティ意識の維持・向上に努めていきます」

高度化・複雑化しているサイバー攻撃から大切な情報資産を守り、市民の生活を支える。立川市は組織的・体系的な施策で情報セキュリティに継続的に取り組んでいる。 J