宮崎市

市の機密情報を取扱う各職員のノート PC を保護する包括的なセキュリティ体制を構築



宮崎市役所

宮崎市は、九州の東南端に位置する宮崎県の県庁所在地であり、中核市として人口 399,243 人、187,222 世帯を擁しています（2022 年 12 月 1 日現在）。宮崎市役所は宮崎市の中央を流れる大淀川の河畔にあり、本庁舎は客船を模したイメージで建築されました。2022 年に新市長就任を契機に、「市役所改革推進ビジョン」と「デジタルチャレンジ宣言」を策定し、「職員一人ひとりが行政のプロとして誇りと情熱を持ち、市民の幸せのために全力を尽くします。」という経営理念を掲げています。

課題

昨今、中小企業のセキュリティ対策が遅々として進んでいないことが問題視されていますが、行政の場合、セキュリティは言うに及ばす、IT 化の推進も予算と人材の都合上滞っていると言われています。こうした状況の中でも、宮崎市役所では積極的に IT 化とセキュリティ対策を進めてきており、セキュリティ対策の一環として導入していたアンチウイルスソフトが更新のタイミングを迎えようとしていました。また同時に、三層に分離されているネットワーク環境について、より利便性の高い新たなネットワークモデルへの検討も開始されたところでした。

「高いセキュリティレベルを維持しつつ、ネットワークの利便性を最大限に向上させるためには、エンドポイントセキュリティの強化が必須と考え、EDR の導入を検討することとなりました」と宮崎市役所の宮崎市 総務部 情報政策課 DX 推進室 松浦 裕（まつうら ゆたか）氏は述べています。導入する際の要件としては、EPP（エンドポイント保護プラットフォーム）や EDR（エンドポイント検知／レスポンス）といったエンドポイントのセキュリティ機能が充実していること、設定・導入が容易であり、運用管理もしやすいこと、管理コンソールが日本語化されていること、脅威ハンティングなどの高度なセキュリティサービスが提供されていること、そして宮崎市の分離されたネットワーク環境でも、単一の管理コンソールで運用管理が行えること、といったことが挙げられました。

ソリューション

宮崎市役所では、先の要件に沿ってベンダー各社の製品を実際の環境で評価を繰り返した結果、ウォッチガードの「WatchGuard EPDR」が最も適していると判断し、採用に至りました。宮崎市 総務部 情報政策課 情報政策係 中平 翔太（なかひら しょうた）氏は、「ウォッチガードのエンドポイントセキュリティ製品には、エンドポイントを保護するプラットフォームの『WatchGuard EPP』、およびエンドポイントの感染を検知し、レスポンスする『WatchGuard EDR』がありますが、今回導入したのは、より包括的なセキュリティ体制を実現するべく、両製品の機能を併せ持ち、さらに高機能のオプションも利用できる WatchGuard EPDR を導入することにしました」と説明しています。

導入

WatchGuard EPDR の導入は 2022 年 7 月に決定し、ライセンス納品後、EPP ／ EDR の各種設定やインストーラの作成はわずか数日で完了しました。続けて 3,500 台に及ぶ PC 端末への導入展開は数週間かけて実施されました。「ウォッチガードの手厚いサポートにより、導入作業は順調に進めることができました」と宮崎市 総務部 情報政策課 情報政策係 上谷 政嗣（うえたに まさつぐ）氏は回想しています。

顧客
宮崎市

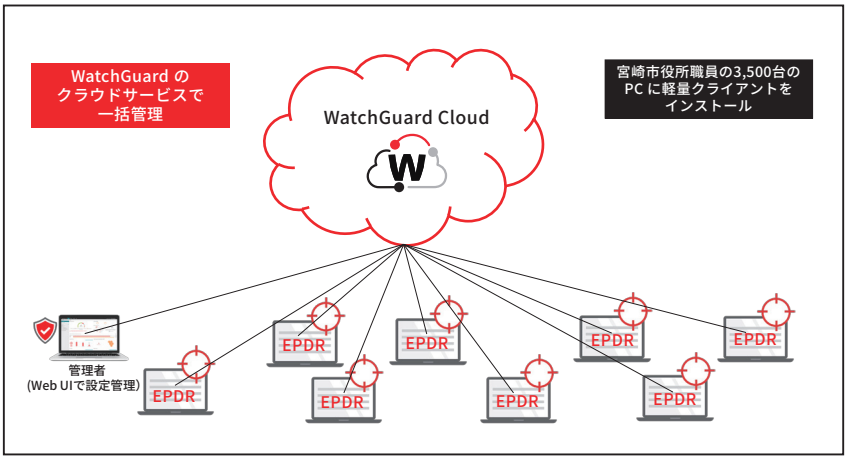
ユーザ数
3,500
ライセンス

業種
公共

地域
宮崎県

導入製品
WatchGuard
EPDR

導入時期
2022年7月



WatchGuard EPDR の導入イメージ



宮崎市 総務部
情報政策課 DX 推進室
松浦裕 氏



宮崎市 総務部
情報政策課 情報政策係
中平翔太 氏



宮崎市 総務部
情報政策課 情報政策係
上谷政嗣 氏

効果

今回、宮崎市役所で WatchGuard EPDR を導入したことで、総じてエンドポイント（PC 端末）のセキュリティを強化することができました。各 PC にはそれぞれエージェントソフトがインストールされていますが、軽量であり、１つのエージェントで EPP と EDR の両機能が動作していることから、PC 端末のリソース負荷を気にしなくてもよく、さらにオンプレミスの管理サーバは不要で、全てクラウド上で管理されています。ウォッチガードのクラウドプラットフォーム「WatchGuard Cloud」の管理コンソールから EPP ／ EDR を一元的に管理できるため、運用負荷を最小限に止めることができます。

「EPDR がインストールされていない PC 端末が自動的に管理コンソールに表示されるため、導入展開に役立ちました。また、管理コンソールが完全に日本語化されており、直感的で操作しやすく、レポート等も充実しています」（上谷氏）。また、WatchGuard EPDR 独自のゼロトラストアプリケーションサービス機能により、PC 端末上のプロセスは 100% 調査されており、究極の「デフォルト Deny」体制を築くことができるため、未知の脅威の実行を高精度で制御でき、セキュリティを非常に高いレベルで維持できています。また、製品に標準で搭載されている「脅威ハンティングサービス」も WatchGuard EPDR を選択した理由の１つとなっています。悪意のある行動をリアルタイムで監視し、攻撃の兆候を早期に検知して対応することができます。さらに、Web フィルタリング機能や USB デバイスの利用制御機能などが標準装備されており、今後リモートワーク端末などのセキュリティ対策として有効活用できます。



宮崎市役所

今後

宮崎市役所では今後「パッチの適用管理と USB デバイス等の利用制御も視野に入れています。」（中平氏）。サイバー攻撃による被害の多くは、古いバージョンのソフトウェアの利用や、セキュリティパッチが未適用の場合に生じる脆弱性を突かれることが原因となっています。このため、PC 端末の脆弱性管理が非常に重要になります。こうした状況の対策として、WatchGuard EPDR にはオプション機能として WatchGuard Patch Management（パッチ管理）が用意されており、宮崎市役所では今後導入を検討しています。同製品は EPDR と同一のエージェントソフトで動作が可能であり、Windows だけでなく、サードパーティのアプリケーションの脆弱性も管理できます。パッチを適用する際の対応優先順位付けが自動化され、管理コンソールから緊急パッチを全 PC 端末にプッシュインストールするなどの操作もシンプルに行うことができます。

【WatchGuard Technologies について】

WatchGuard® Technologies, Inc. は、統合型サイバーセキュリティにおけるグローバルリーダーです。ウォッチガードの Unified Security Platform®（統合型セキュリティプラットフォーム）は、マネージドサービスプロバイダー向けに独自に設計されており、世界トップクラスのセキュリティを提供することで、ビジネスのスケールとスピード、および運用効率の向上に貢献しています。17,000 社を超えるセキュリティのリセラーやサービスプロバイダと提携しており、25 万社以上の顧客を保護しています。ウォッチガードの実績豊富な製品とサービスは、ネットワークセキュリティとインテリジェンス、高度なエンドポイント保護、多要素認証、セキュア Wi-Fi で構成されています。これらの製品では、包括的なセキュリティ、ナレッジの共有、明快さと制御、運用の整合性、自動化という、セキュリティプラットフォームに不可欠な 5 つの要素を提供しています。同社はワシントン州シアトルに本社を置き、北米、欧州、アジア太平洋地域、ラテンアメリカにオフィスを構えています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多彩なパートナーを通じて、国内で拡大する多様なセキュリティニーズに応えるソリューションを提供しています。詳細は https://www.watchguard.co.jp をご覧下さい。

ウォッチガード・テクノロジー・ジャパン株式会社
〒 106-0041 東京都港区麻布台 1-11-9 BPR プレイス神谷町 5 階
TEL：03-5797-7205　EMAIL：jpnsales@watchguard.com www.watchguard.co.jp

© 2023 WatchGuard Technologies, Inc. All rights reserved. WatchGuard、WatchGuard ロゴ、Firebox は、米国および／またはその他の国における WatchGuard Technologies, Inc. の登録商標です。その他の商標は各社に帰属します。（2023 年 1 月作成）