導入事例：姫路市役所様

限りなく”100%安全”を目指す、姫路市役所のセキュリティ戦略

お客様
姫路市役所

業種・業界
官公庁・公共

地域
日本

ウォッチガード製品
WatchGuard Firebox M400
APT Blocker

巧妙化する脅威には「多層防御と標的型攻撃対策」！
統合セキュリティ性能とコストパフォーマンスが決め手

ウォッチガード・テクノロジー・ジャパン株式会社

画像：姫路市役所様 Web ページより

限りなく“100%安全”を目指す、姫路市役所のセキュリティ戦略

企業と同様、市民生活を支える自治体もサイバー攻撃の脅威と無縁ではない。攻撃の巧妙化や予算の制約を前に、実効的なセキュリティ対策をどう実現すべきか。その課題に挑んだ姫路市役所の取り組みを見ていこう。

世界文化遺産の国宝「姫路城」をはじめとする豊富な観光資源のおかげで内外から多くの観光客を集める兵庫県姫路市は、人口約53万人を数える兵庫県西部の中核都市だ。姫路市役所は2015年10月、既存システムの更改に合わせ、セキュリティのさらなる強化を目的に、セキュリティシステムを刷新した。

今や地方自治体もサイバー脅威とは無縁ではない時代だ。外部からの不正アクセスやマルウェア感染、あるいは内部犯行による情報流出など、リスクを挙げればきりがない。一方で、予算の限られた地方自治体が単独で投入できるリソースには限りがあるのも事実だ。

こうした中、姫路市役所はどのようにセキュリティを強化したのだろうか。

脅威の巧妙化を前に「全てのセキュリティ機能を」

姫路市では本庁舎の他、複数の支所や出張所なども含め、約3800人の正規職員が勤務する。同市はこれら各拠点を地域公共ネットワークによってリング状に接続。2007年に市役所近隣に建設された免震構造の「防災センター」に集約し、インターネットにつながる構成にしている。

今回、姫路市役所が取り組んだセキュリティ強化の中核となるのが、WatchGuard Technologies（以下、ウォッチガード）のセキュリティアプライアンス製品「WatchGuard Firebox M400」だ。庁内ネットワークとインターネットとを結ぶ境界部分にWatchGuard Firebox M400を導入。冗長構成を採用して高い可用性を確保するとともに、他のセキュリティ機器と併用することで、より堅牢な対策を目指した。

WatchGuard Firebox M400の導入以前は、ファイアウォール専用機と不正侵入防止システム（IPS）をインライン構成で配置し庁内ネットワークを保護してきた。ごく基本的な「多層防御」ともいえるだろう。ただし「機能ごとに別々のアプライアンスを運用する必要がある上に、標的型攻撃に代表される通り、サイバー攻撃がますます巧妙になる状況の中で不安が残っていました」と、姫路市総務局情報政策室主任の藪上憲二氏は語る。

2015年12月に迫った機器更改時期を前に、藪上氏はこうした問題意識を抱いて機器の検討を始めていた。そのタイミングで発生したのが、日本年金機構をはじめとする複数の組織を襲った標的型攻撃だった。

一連の被害の深刻さを目の当たりにし、「全てのセキュリティ機能を統合できる方がいい」（藪上氏）と考え、UTM（Unified Threat Management:統合脅威管理）アプライアンスを検討することにした。しかも標的型攻撃に用いられるマルウェアは、シグネチャベースのセキュリティ対策をすり抜ける恐れがあることから「『サンドボックス』機能も必要だと考えました」（同氏）と説明する。サンドボックスとは、実環境に影響を与えない隔離環境でファイルを実行してウイルスを検知する仕組みのことだ。

姫路市役所の藪上氏

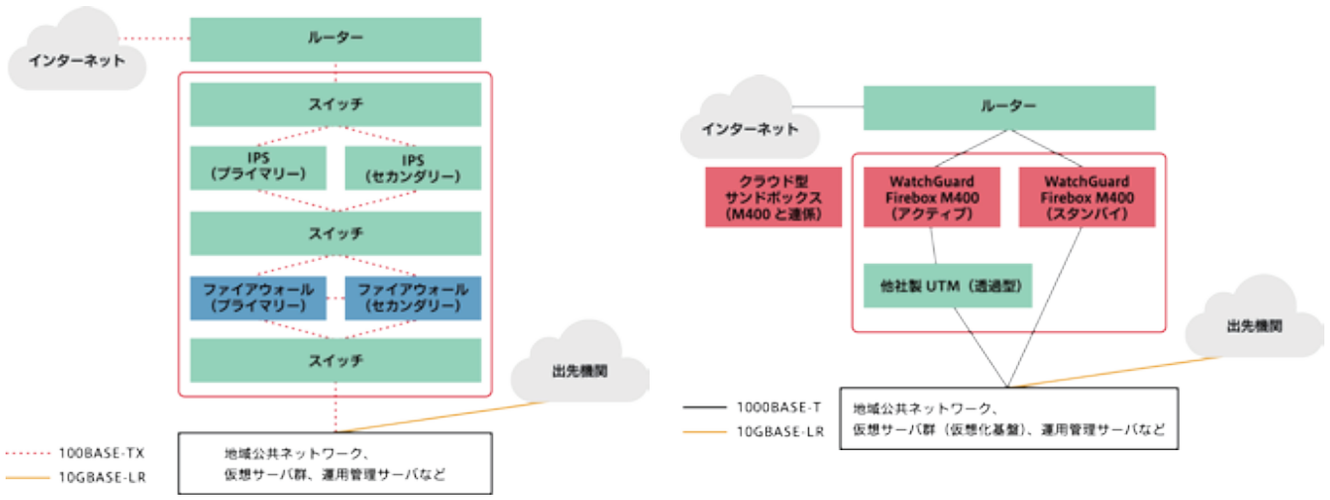
姫路市役所

UTM機能全体の性能とコストパフォーマンスが決め手

こうした観点で複数のUTM製品を検討した結果、最終的に選んだのがWatchGuard Firebox M400だった。パケットフィルタリングにはじまり、IPSやWebフィルタリング、スパム対策、ウイルス対策、アプリケーション制御といった複数の機能を1つの筐体に統合したアプライアンス製品だ。不正なパケットの侵入を水際で食い止めるとともに、LANからインターネットの不審なサーバへのアクセスを防ぐ。複数のシグネチャベースのセキュリティ機能に加え、ウォッチガードが長年にわたって蓄積してきたレピュテーションデータベースを活用することで、効率的な防御を実現する。

ウォッチガードではこうした一連のセキュリティ機能を、優れたセキュリティ技術を持つパートナー企業との協力に基づいて“ベストオブブリード”の形で搭載している。その最新例が、標的型攻撃対策製品を開発するLastlineのサンドボックス機能と連係する「WatchGuard APT Blocker」だ。姫路市役所がWatchGuard Firebox M400を選択した理由の1つも、このサンドボックス機能の存在にあったという。

加えて並列処理を実現するマルチプロセッシングエンジンにより、全てのセキュリティ機能を高速に処理できることもポイントだった。「ファイアウォール機能だけが速くても意味はありません。WatchGuard Firebox M400は全ての機能を有効にした状態のパフォーマンスを示す『UTMスループット』が



WatchGuard Firebox M400の導入前（左）と導入後（右）のネットワークセキュリティシステム

高く、エンドユーザーに悪影響を与えずに導入できると考えました」（藪上氏）

何より大きな決め手は、優れたコストパフォーマンスだ。同様の性能を備えた競合他社の製品と比べて安価で、しかも標準機能のライセンスで冗長化構成（アクティブ／スタンバイ）を取ることができる。「コストパフォーマンスで言えば差は数倍。『限られた予算の中で最大限の対策をしたい』というわれわれのニーズに最も合致していました」と藪上氏は振り返る。

こうした理由から姫路市役所はWatchGuard Firebox M400の採用を決定。富士ゼロックス兵庫ならびに鳥取県情報センターの支援を受けて導入作業を進め、予定を3カ月前倒しし、運用を開始した。

リソースをうまく使い継続的なセキュリティ強化に取り組む

姫路市役所で情報システムの導入や運用を担当する総務局情報政策室では2015年度、藪上氏も含めた主に4人の担当者が市の情報系システムを運用してきた。今回の更改に併せ、教育委員会のネットワークも市役所のネットワークに一本化したので、インターネットに接続するクライアントPCが約1万5000台規模に上る大規模システムを運用することになる。「これだけの数になると、クライアントの管理が教育委員会と分かれていることもあり、たった1件のパッチでも全端末に速やかに適用するのは難しい」と藪上氏は語る。ときにはIPS、ときにはWebフィルタリングといった具合にUTMの各機能を有効に活用し、セキュリティと利便性とのバランスを取りながら対策に取り組んでいると説明する。

ただしWatchGuard Firebox M400に関して言えば、導入後の管理負荷はほとんどないという。通常の管理業務は、専用の統合管理ツール「WSM（WatchGuard System Manager）」を利用している。「Webベースのインタフェースでは、操作時の画面読み込みに時間がかかることも少なくありません。これに対しクライアントアプリケーションであるWSMは画面表示がスムーズで、設定や更新作業を素早く実行できます」（藪上氏）。

少ない手間で安定運用を実現するために、機器のリモート死活監視やレポート作成を提供するマネージドセキュリティサービス「MSXサービス」（提供:コムネットシステム）を鳥取県情報センター経由で利用している。また1カ月で約4億件に上るログ解析を効率化するために、より専門的な知識が要求されるアラートの解析については外部のSOC（Security Operation Center）サービスを活用。こうした工夫で捻出したリソースを、情報化計画の推進や新たなセキュリティ施策といった部分に効果的に投じている。

マイナンバー（社会保障と税の共通番号）制度のスタートと昨今の標的型攻撃の被害を受け、総務省は「新たな自治体情報セキュリティ対策の抜本的強化に向けて」と題する報告書を公開し、地方自治体における情報セキュリティ対策の抜本的強化策を求めている。姫路市役所もこれを踏まえ、総合行政ネットワーク（LGWAN）接続系とインターネット接続系の分離に取り組む他、2要素認証における顔認証の活用をはじめとしたセキュリティ強化に継続的に取り組んでいく計画だ。

セキュリティ強化においては「人」も重要な要素となる。姫路市では管理職も含めた全職員に対するEラーニングを定期的に実施し、セキュリティに関する基本的な知識を伝えている。ただし最も弱い部分が人であるのも事実だ。最悪の事態が発生しないよう、継続してできる限りの対策に取り組んでいくという。

攻撃の巧妙化によって全ての攻撃を防ぐのは困難になり、「事故は発生するもの」という前提に立った事後対応の必要性が指摘されるようになった。ただし、それは予防をないがしろにしていいという意味ではない。「侵入を100%防ぐことは不可能かもしれませんが、守らないというわけにはいきません。100%が難しいなら多層防御により99.99%を防いでいく、そして防げなかったものでも速やかに検知し、対策を取って最悪の事態を防いでいくという姿勢で、できる限りの策を講じていくことが大事です」と藪上氏も意気込む。WatchGuard Firebox M400は、そんな姫路市の防御を強力に支援している。

※この記事は、TechTargetジャパン（http://techtarget.itmedia.co.jp/）に2016年5月に掲載されたコンテンツを再構成したものです。
http://techtarget.itmedia.co.jp/tt/news/1605/17/news03.html

標的型攻撃対策も統合する先進のセキュリティ対策
セキュリティ・パフォーマンス・コストのバランス

	Firebox T Series			Firebox M Series	
	小規模オフィス・分散拠点向け			中規模エンタープライズ規模向け	
					
モデル	T10/T10-W	T30/T30-W	T50/T50-W	M400	M500
スループットと接続					
推奨ユーザー数（プロキシ/FW利用時）	10/20	15/30	35/50	150/300	300/500
FWスループット	400Mbps	620Mbps	1.2Gbps	8Gbps	8Gbps
VPNスループット	100Mbps	150Mbps	270Mbps	4.4Gbps	5.3Gbps
AVスループット	120Mbps	180Mbps	235Mbps	2.5Gbps	3.2Gbps
IPSスループット	160Mbps	240Mbps	410Mbps	4Gbps	5.5Gbps
UTMスループット	90Mbps	135Mbps	165Mbps	1.4Gbps	1.7Gbps
インターフェイス 10/100/1000	3	5	7	8（2SFP含む）	8（2SFP含む）
I/Oインターフェイス	1Serial/1USB	1Serial/1USB	1Serial/1USB	1Serial/2USB	1Serial/2USB
ノード数（LAN IPｓ）	制限なし	制限なし	制限なし	制限なし	制限なし
同時接続（双方向）	50,000	200,000	300,000	3,800,000	9,200,000
VLANサポート	10	50	75	300	500
認証ユーザー数	200	500	500	制限なし	制限なし
VPNトンネル数					
Branch Office VPN	5	40	50	100	500
モバイル VPN IPSec（標準/最大）	5	25	50	150	500
モバイル VPN SSL /L2TP	5	25	50	150	500

T10-W/T30-W/T50-W：無線LAN アンテナ内蔵モデル

お問合せ：

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 CR神谷町ビル5階 Tel:03.5797.7205 Fax:03.5797.7207
http://www.watchguard.co.jp info-jp@watchguard.com