兵庫県
Hyogo Prefecture

統合型FortiSandboxと複数のFortiGateを閉域網で連携させ県と外郭団体間の高度なセキュリティ対策モデルを実現

サイバー攻撃の脅威が増すなか、兵庫県では県の外郭団体（密接関連公社）の情報セキュリティ対策を強化。県内各地に分散する密接関連公社にフォーティネットのUTM/次世代ファイアウォール「FortiGate」を導入するとともに、県庁データセンターにサンドボックス「FortiSandbox」を設置し、FortiGateから送られる未知のマルウェアなど不審なファイルを一元的に解析・防御する仕組みとして「公社等情報セキュリティ基盤」を構築している。その狙いを兵庫県の情報セキュリティを担当する情報企画課システム管理室のキーパーソンに聞いた。

導入・構築のポイント

(1)FortiGateとFortiSandboxを連携させ、標的型攻撃や未知のマルウェアを一元的に解析・防御

(2)不正アクセスの検知・防止や、脅威の兆候把握のためのログ取得が可能なFortiGateを導入

(3)自治体情報セキュリティクラウドに適用可能な、公社等の情報セキュリティ基盤のモデルを構築

兵庫県

県　庁　兵庫県神戸市中央区下山手通5-10-1
面　積　8,400km^2
人　口　約552万人(2015年10月推計)

北は日本海に面し、南は瀬戸内海から淡路島を介して太平洋へと続いている。県域の情報基盤として、本庁と地方機関を結ぶ県庁WANや、県と県内市町を接続する総合行政ネットワークなど、効率的なネットワークの基盤として兵庫情報ハイウェイを整備・運用している。

兵庫県
企画県民部
情報企画課
システム管理室
室長
津川 誠司氏

兵庫県
企画県民部
情報企画課
システム管理室
システム運用班長
前田 晃氏

密接関連公社のWeb閲覧制限や標的型攻撃対策が課題に

特定の組織・団体を狙った標的型攻撃の被害が後を絶たない。中でも、職員のパソコンが外部から不正アクセスされ、大量の個人情報が流出した日本年金機構に対する標的型攻撃は記憶に新しい。

兵庫県では、個人情報や機密情報を適切に管理するため、兵庫県情報セキュリティ対策指針に基づき、情報セキュリティの確保に努めてきたが、県の外郭団体のセキュリティ対策が課題になっていた。「国の特殊法人である日本年金機構の事案ではありませんが、比較的セキュリティ対策が手薄になりがちな外郭団体が狙われることもあります。兵庫県には多くの外郭団体がありますが、中でも県の出資比率が高い32の密接関連公社を対象に、Web閲覧や標的型攻撃に対するセキュリティを強化する必要がありました」と、企画県民部 情報企画課 システム管理室室長の津川誠司氏は説明する。

兵庫県
企画県民部
情報企画課
システム管理室
システム運用班
北村 尚志氏

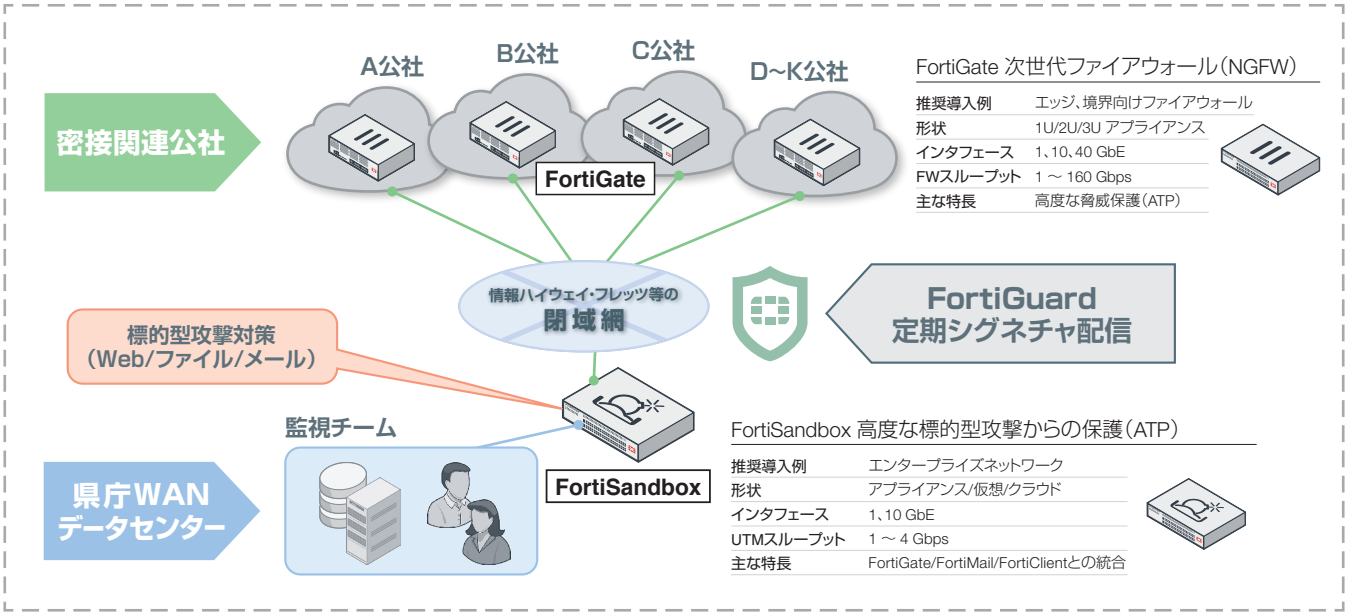
兵庫県
企画県民部
情報企画課
システム管理室
システム運用班
松原 裕樹氏

業務外のインターネット閲覧など情報セキュリティの課題を抽出

従来から密接関連公社はそれぞれ独自にファイアウォールなどのセキュリティ対策を行っていたが、システム管理室では情報セキュリティ上の課題を洗い出すため、アンケートとヒアリングによる事前調査を実施している。回答30団体のうち、(1)「システム管理者を設置していない」団体は15（50%)、(2)「セキュリティポリシーを策定していない」24（80%)、(3)「インターネットの閲覧制限がない」26（87%)、(4)「職員のインターネット閲覧ログがない」26（87%)、(5)「標的型攻撃対策システムを導入していない」30（100%）という調査結果が出た。

例えばインターネット閲覧制限がない密接関連公社の場合、職員が悪意のあるWebサイトを閲覧してマルウェアに感染し、機密情報が流出するリスクがある。業務時間内に業務外のインターネットを閲覧していたとしても、インターネット閲覧ログを取得していない場合は職務専念義務の管理ができないうえ、問題が発生した時に原因究明が困難なことに加え、「ログで状況を確認できなければ外部に対して説明責任を果たせません」(津川氏)。

「そこで、密接関連公社向けのサンドボックスとUTMの要件を定義し、費用対効果を勘案しながら、公社等情報セキュリティ基盤の構築に向けて製品を検討したのです」とシステム管理室の北村尚志氏は話す。



要件から絞り込んだ結果、FortiGateとFortiSandboxを選択

公社等情報セキュリティ基盤は、密接関連公社と県庁WANを兵庫情報ハイウェイまたは通信事業者の閉域網サービスで結び、密接関連公社が新たに導入するUTMが検知した不審なファイルを県庁データセンターに設置するサンドボックスで一元的に分析し、自動的に必要な対策が打てる仕組みだ。

そして、サンドボックスはセキュリティの観点から、外部でデータを解析するクラウド型サービスではなく、アプライアンス型で複数デバイスと連携可能なオンプレミスの運用が可能な製品とした。また、UTMはファイアウォールやアンチウイルス、侵入検知／防御(IPS)などのセキュリティ機能のほか、事前調査で課題となっていたWeb閲覧制限が行えるWebフィルタリングと閲覧ログが取得できるWebプロキシ機能が要件となった。

これらを要件に数社の製品を比較・検討した結果、フォーティネットのサンドボックス「FortiSandbox 1000D」及びUTM/次世代ファイアウォール「FortiGate 100D/200D」(密接関連公社の規模によって選択)の採用を決定した。「費用対効果や要件、各製品ベンダーとの会話から製品を絞り込んだ結果、フォーティネット製品を選択しました。特にFortiGateとFortiSandboxの組み合わせは、コストパフォーマンスに優れていて、高機能なソリューションを安価に導入することができました」と津川氏は話す。密接関連公社のシステム管理体制や費用対効果を勘案し、職員が40人以上の団体は公社等情報セキュリティ基盤の利用、40人未満の団体はプロバイダが提供する標的型攻撃対策サービスの利用を可能にしている。

そして、2015年12月から公社等情報セキュリティ基盤の運用を開始。FortiSandboxの導入効果について、津川氏は「脅威の有無を可視化でき、必要な対策を講じられることです。また、FortiGateは日本語に対応しているなど、操作性や運用性に優れていると思います」と評価する。そして、北村氏は「標的型攻撃や未知のマルウェアの脅威が増える中、FortiSandboxで一元的に脅威を可視化できるのは助かります」と話す。

「導入を検討中の公社の相談に乗りながら、基盤の導入を支援していきます」とシステム管理室 システム運用班長の前田晃氏は今後の取り組みを話す。また、「基盤の導入後、脅威に適切に対応するためには運用が大切です。脅威検出のアラートメール通知後の公社側での対応や職員のセキュリティ意識を含め、サポートしていきます」とシステム管理室の松原裕樹氏は述べる。外郭団体のセキュリティ対策の強化は、兵庫県の取り組みが参考になるだろう。

FORTINET
フォーティネットジャパン株式会社
www.fortinet.co.jp/contact

お問い合わせ