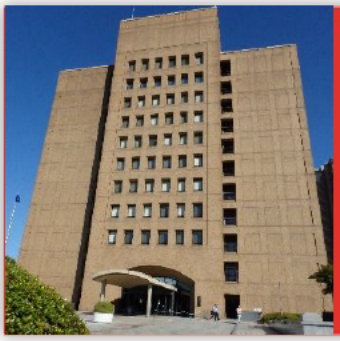
導入事例

徳島県様
「徳島発！『サイバー攻撃対策強化』実証実験」



全国トップレベルの光ファイバー網を有し、全国のIT企業の
サテライトオフィスを誘致するなどIT先進県として知られる。
2018年1月より「『サイバー攻撃対策強化』実証実験」を開始し、
FFRI yaraiを県庁総合サービスネットワーク計5,200台に導入済み

徳島県は、光ファイバー全県域普及・世帯当たりの総延長全国1位（2012年徳島県調査）、教室の無線LAN整備率全国1位（2015年文部科学省調査）等、他自治体に先んじたIT利活用が注目されています。電子行政推進課では徳島県庁内の電子化、全庁システムを所管し、サイバーセキュリティに関しては"徳島県からいかなる情報も漏らさない、そのための方法を考える"方針で活動しています。2018年1月より「徳島発！『サイバー攻撃対策強化』実証実験」（※1）をＦＦＲＩセキュリティと共同で行い、自治体の環境に適したセキュリティモデルの構築を目指しています。

※1　関連プレスリリース　https://ssl4.eir-parts.net/doc/3692/ir_material11/85394/00.pdf

導入の背景

「三層からなる対策」実施後の懸念点の解消

日本年金機構の個人情報流出事件を受け、2015年11月、総務省から地方自治体の情報セキュリティに係る抜本的な対策として、各都道府県・市町村に「三層からなる対策」（※2）の要請があり、徳島県でも県のシステムに合わせて「三層からなる対策」をマイナンバー施行に間に合わせるよう約2年弱で行いましたが、いくつか懸念点が残っていました。

LGWAN系およびインターネット系では、ネットワーク分離後のファイル受け渡しの際にすべての種類のファイルのサニタイズ（無害化）が不可能である点が挙がりました。また、USBメモリ等で横展開する未知マルウェアが持ち込まれた場合、既存のセキュリティ対策では対応しきれないという課題もありました。

「海外製サニタイズソフトを使っていましたが、国産ソフトのファイルまで完全にサニタイズするのは困難でした。また、どうしてもUSBメモリを使用しなければいけない業務には特定のUSBメモリのみ使用できるよう制限を掛けていますが、未知マルウェアが持ち込まれる可能性があるため感染被害発生の不安がありました」(山住氏)

インターネット系ではセキュリティ対策を施した自治体セキュリティクラウドに接続し、仮想端末(仮想ブラウザ)を使ったインターネット仮想化を行っていますが、未知のマルウェアの侵入や脆弱性攻撃による被害発生の可能性がゼロではありませんでした。

「侵入を検知した場合に仮想端末なら端末イメージごと即削除ができますが、物理端末ではそうはいきません。業務上物理端末が必要な部署もあるため、マルウェア感染後の対応が課題となっていました」(山住氏)

FFRI yaraiを利用した自治体向けセキュリティ対策として、「徳島発！『サイバー攻撃対策強化』実証実験」の話があがったのはその頃のことでした。

※2　自治体の庁内ネットワークシステムを（1）マイナンバー利用事務系、（2）LGWAN（総合行政ネットワーク）接続系、（3）インターネット接続系に３分割し、扱う情報の秘匿性に即したセキュリティ強度を確保する方策

導入の経緯

ネットワーク分離でも使える
振る舞い検知製品
純国産の安心感

FFRI yaraiがインターネットにつながっていないLGWAN系・マイナンバー系でも機能する振る舞い検知製品であり、純国産である安心感も今回の実証実験の実施につながりました。

「「三層からなる対策」の数年前に電子行政推進課が事務局を務める県内イベントで同じ徳島県出身でサイバーセキュリティ専門家でもあるＦＦＲＩセキュリティ代表・鵜飼さんにご講演いただきました。その当時からオフライン環境でも機能する振る舞い検知製品で純国産のFFRI yaraiの優位性は知っていたので、今回FFRI yaraiを採用することに不安はありませんでした」(山住氏)

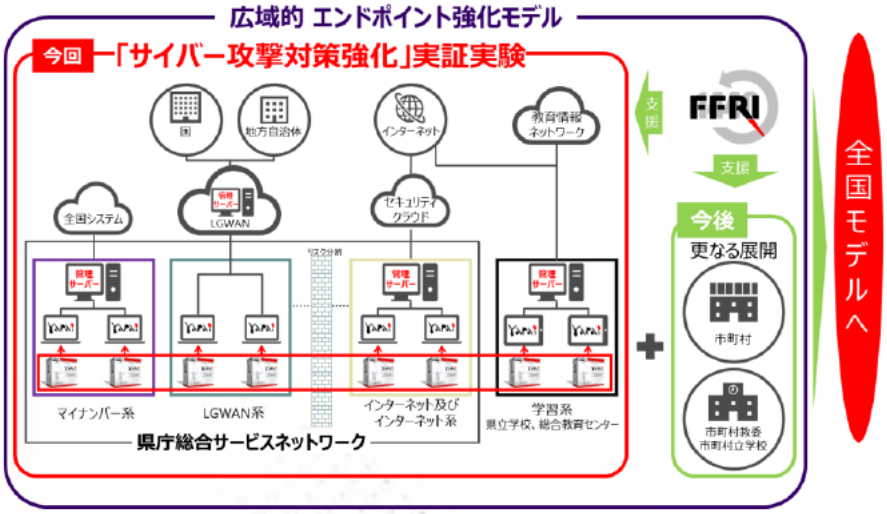
導入の効果

FFRI yaraiをインストールして
すぐにウイルス対策ソフトで
検知不可な不審ファイルを検知

FFRI yaraiは、県庁総合サービスネットワーク5,200台（インターネット系210台、LGWAN系4,700台、マイナンバー系290台）へ導入し、現在も問題なく安定稼働しています。FFRI yaraiはインストール後、評価（検出モードでログをチェック→ホワイトリスト作成）モード→通常（ブロック）モードと、段階的に運用を開始することができます。徳島県では現在検出モードを適用しています。

「インストール後すぐに検出モードで全ファイルスキャンをした際に、ネットワーク分離前から潜んでいた、ウイルス対策ソフトでは検知できなかった不審なダウンローダーが検知されたことに、まず導入効果を感じました。また、振る舞い検知の強みである未知マルウェアの検知力に対して、過検出による運用負荷を導入前に懸念していましたが、実際には県独自のソフト等の過検知はありましたが、数は多くなく、ホワイトリスト登録も面倒ではありませんでした。検知したファイルはＦＦＲＩセキュリティに詳細な分析と丁寧な対応をしていただいているので安心して利用できます」（山住氏）

徳島発！『サイバー攻撃対策強化』実証実験
概念図



今後の展望

実証実験をモデルとして展開し、
他自治体のセキュリティレベル引き上げ
にも貢献

電子行政推進課では2019年度末までに庁内全端末のWindows 10移行計画や現在LGWAN系のみ利用しているLGWAN-ASP(※3)をインターネット系にも拡張した一括管理も進め、さらなるエンドポイントのセキュリティレベルと利便性の向上に取り組んでいます。今後は教育情報ネットワークの学習系(県立高校5校、総合教育センター）600台へのFFRI yarai導入も予定されています。

「今回の実証実験をモデルとして展開することで他の自治体のセキュリティレベル引き上げにも貢献したいと考えています」(山住氏)

※3　LGWAN上で提供されるASPサービス

徳島県経営戦略部 電子行政推進課 情報セキュリティ担当室長 山住健治氏

製品・サービスについてのお問い合わせは
株式会社ＦＦＲＩセキュリティ
〒100-0005
東京都千代田区丸の内3-3-1　新東京ビル2階
TEL：03-6277-1811　E-mail：sales@ffri.jp
本製品に関する情報はインターネットでもご覧いただけます。
https://www.ffri.jp/

2018年10月現在