SB Technology

導入事例

長崎県

導入サービス　CSIRT 構築支援サービス

プロフィール

所在地	長崎県長崎市尾上町3-1
設立	1871年（明治4年）11月
従業員数	4,087名 （一般行政部門 2018年4月現在）
事業概要	長崎県の行政
URL	https://www.pref.nagasaki.jp/

長崎県
総務部 情報政策課
課長
山崎 敏朗氏

長崎県
総務部 情報政策課
情報基盤班
課長補佐
里脇 太市氏

長崎県
総務部 情報政策課
情報基盤班
主事
溝上 朝洋氏

「自治体情報セキュリティクラウドと密に連携した インシデント対応にあたる『長崎県 CSIRT』を構築できました」

導入のポイント

- 自治体情報セキュリティクラウドと連携した CSIRT を構築
- SBT のノウハウを基に実行性のある CSIRT が完成
- インシデント発生時の適切な対応を実現

抱えていた課題、解決したかったこと

サイバー攻撃によるインシデント対応の強化を目指した長崎県

2018年1月、長崎魚市跡地に竣工した新庁舎へ移転した長崎県庁。情報企画の調整・推進や情報システムの開発・運用管理などを担当する長崎県情報政策課では、新庁舎の完成に前後してさまざまな施策に取り組んでいた。

「2015年12月の総務省通知に従い、長崎県では庁内ネットワークとインターネット環境の分離、特定個人情報取扱領域からの情報持ち出し禁止措置、県市町のインターネット接続点を集約してセキュリティ対策を強化する『長崎県自治体情報セキュリティクラウド』の構築といったセキュリティ対策を進めてきました。そうした中、セキュリティインシデントの対応について改めて評価したところ、これまでの対応では十分でないことが明らかになりました」

これまで長崎県で発生したセキュリティインシデントは、職員の事務処理ミスによるものがいくつかあったという。そうした職員の過失によるインシデントについては、過去の事例を参考にある程度の対応はできていたそうだ。

「しかし、サイバー攻撃によるインシデントについては、これまで運よく被害が生じていなかったこともあり、発生した場合にどのように関係者と情報を共有し、どのように対応する必要があるかといった行動基準が体系化できていませんでした。そのため、インシデントに直面した際には、担当職員と関係者が都度判断・対応せざるを得ないという状況でした。また、セキュリティ担当者は数年ごとに入れ替わるため、インシデント対応のノウハウが蓄積されないことも課題でした」

- セキュリティインシデント対応が不十分だったことが明らかに
- インシデント発生時の行動基準が体系化されていない
- 担当職員と関係者がその場その場で判断・対応せざるを得ない状況

導入の経緯

自治体情報セキュリティクラウドと連携した CSIRT の構築が可能な SBT を選定

こうしたインシデント対応の課題を解決するために、長崎県ではセキュリティポリシーの改定作業に着手した。

「2018年に総務省の『地方公共団体における情報セキュリティポリシーに関するガイドライン』が改定され、長崎県も本ガイドラインを参照してセキュリティポリシーやその下位規定に該当するセキュリティ実施手順などを見直すことにしました。この改定に盛り込むために、セキュリティポリシーの策定と併せて進めることにしたのが、インシデント対応にあたる組織「長崎県 CSIRT（Computer Security Incident Response Team）」を構築することでした」

長崎県 CSIRT を構築するにあたり、長崎県がまず提案を依頼したのがソフトバンク・テクノロジー（SBT）だった。

「SBT へ長崎県自治体情報セキュリティクラウドの構築と運用を委託しており、県や市町の安全なインターネット利用のため、セキュリティ機器最適化のためのチューニングや通信記録の監視・分析（マネージドセキュリティサービス）を行っていただいています。そのため、SBT のセキュリティ対応力・技術力について高く評価しており、CSIRT との連携も考慮したインシデント対応の監視・分析が可能だと判断し、選定しました」

- セキュリティポリシーの改定と併せて CSIRT の構築に着手
- 自治体情報セキュリティクラウドの構築・運用を委託している SBT に提案を依頼

ソフトバンク・テクノロジーの評価ポイント

SBT が持つ CSIRT フレームワークを基に、長崎県の要件・実情に合わせ CSIRT を構築

長崎県では、2018年10月に CSIRT の構築を開始。県が策定したセキュリティポリシー、インシデント対応時に連携が必要な組織の概要などの情報を SBT へ共有するとともに、SBT に対して CSIRT の構築に必要な要件整理、および他自治体の CSIRT に関する情報収集を依頼した。その後、SBT の持つ CSIRT フレームワークを長崎県の要件に合わせてローカライズし、実態に沿った組織構築のためにロールプレイングを実施して完成度を高めていったという。

「SBT とは、これまでも自治体情報セキュリティクラウドを通じて円滑なコミュニケーションが取れていたこともあり、長崎県の実情を反映した CSIRT の完成形が提示されたことを高く評価しています。SBT から提供された参考情報も、必要な情報が端的にまとめられており、長崎県のインシデント対応に不足する部分や必要な対策を明確に認識することができました」

- SBT が持つ CSIRT フレームワークを要件に合わせてローカライズ
- 実情を反映した CSIRT の完成形が提示されたことを高く評価

導入効果と今後の展望

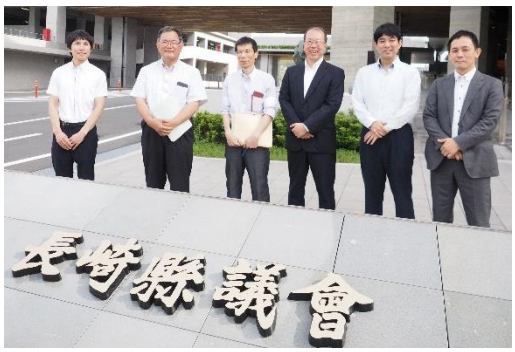
インシデント発生時の適切な対応と迅速な収束が可能に

長崎県 CSIRT の構築が完了したのは、2019年1月のこと。導入後にも職員の事務処理ミスによるセキュリティインシデントが発生しているが、これまでの対応と異なって、確立された処理フローに基づく適切なインシデント対応が可能になったという。

「これまで検知しきれていなかった、不審メールの受信といったインシデントの予兆と思われる事象も分かるようになり、インシデント発生時の対応だけでなく、インシデントの早期把握や予防という観点からもセキュリティの向上を実感しています。それに加え、従来はあいまいだったインシデント時に連携すべき所管がはっきりし、情報共有の漏れや連携不足による無駄な事務手続きを削減するという効果が得られています」

今後は長崎県内各市町にも CSIRT 運用で培ったノウハウを共有し、長崎県全体がセキュアな自治体となるように取り組む方針だという。

また、外部の CSIRT とも連携を図りながら、継続的に発展できる運用を目指す考えだ。



ソフトバンク・テクノロジー株式会社
山田 晋也、小林 青己、井野 一義（写真右より）

- 確立された処理フローに基づく適切なインシデント対応が可能に
- インシデントの早期把握や予防の観点からセキュリティの向上を実感
- 情報共有の漏れや連携不足による無駄な事務手続きを削減

お客様窓口
SBテクノロジー株式会社
〒160-0022
東京都新宿区新宿 6丁目27番30号 新宿イーストサイドスクエア 17階
TEL ：03-6892-3154
E-MAIL ：sbt-ipsol@tech.softbank.co.jp
企業情報：https://www.softbanktech.co.jp/