7ZL-03

長崎のデータ連携基盤を利用したWebサイト作成時のセキュリティ実施事項のベストプラクティスの提案

志方　里穂†　　小林　信博†

長崎県立大学†

1　はじめに

近年、ICT を活用して生活の質の向上や新たな価値創出による経済循環の促進、社会課題の解決を図るスマートシティが大きな注目を集めている。スマートシティの特徴として、様々な主体が様々なデータを連携・共有することが求められる。長崎県は新サービスの創出による生産性の向上、地域活性化を図ることを目的とした「つながる長崎」データ連携基盤[2]を提供している。一方、総務省は安心・安全に新サービスを創出するために「スマートシティセキュリティガイドライン（第 2 版）[1]」を公表している。しかし、セキュリティ対策に不慣れな人が見ると実施方法や手順についてイメージしづらいと考えられる。

本論文では、スマートシティセキュリティガイドラインをセキュリティについての知識が少ない人でもイメージしやすいようにセキュリティ対策実施事項を具体的にマニュアル化することで安心・安全に新サービスを創出することを実現するとともに、参考事例としてのベストプラクティスを提案する。

2　「つながる長崎」データ連携基盤

「つながる長崎」データ連携基盤とは、長崎県が令和４年から提供しているデータ連携基盤である。これは、行政・民間が有する様々なデータの集積・共有・活用を可能とするデータ連携基盤を利活用するものである。「つながる長崎」では、以下の機能・サービスを提供している。

（1）ながさきデータマップ

データを地図上に表示し提供するサービスで、申請不要で誰でも利用可能。

（2）ながさき API カタログサイト

データを公開 API として提供するサービスで、「ながさき API カタログサイト利用申請フォーム」から利用申請する必要がある。

（3）ながさきデータ公開環境

データを可視化・分析可能な情報として提供するサービスで誰でも利用可能。

3　現状の問題、課題と解決策

まず、本論文の対象者及び想定するシナリオについて記述する。

（1）対象者

セキュリティ専門家の居ない企業に勤める、Web サイトなどのシステムは構築出来るが、セキュリティ対策については不慣れで実際にどうすればセキュリティ対策が出来るか、何から始めれば良いか分からない人 。

（2）想定するシナリオ

対象者がながさき API カタログサイトと連携したスマートシティの新サービス(＝スマートシティガイドラインに沿った新たな Web システム)の開発を企業の中で任されている状態。

（3）現状の問題

スマートシティセキュリティガイドラインやその中に記載されている「スマートシティセキュリティガイドライン導入チェックシート」はセキュリティに不慣れな対象者にとってはセキュリティの専門用語が多く、実施方法、実施手順についてイメージしづらく、対象者がスマートシティセキュリティガイドラインを参照しながらセキュリティ対策を行うには不十分であると考える。

（4）課題

対象者でもセキュリティ対策が行えるようスマートシティセキュリティガイドラインに記載されている実施事項をさらに具体的にまとめる必要がある。また実施方法や実施手順などについてまとめたマニュアル、そして、スマートシティセキュリティガイドライン導入チェックシートについても既存の実施事項を詳細に分けたチェックシートを作成する必要があると考える。さらに、新サービスを創出する際にスマートシティセキュリティガイドラインに則った対策の実施が出来るようにする必要があると考える。

（5）解決策

対象者が一人でもセキュリティ対策を実施

Proposal of best practices for security practices when creating websites using Nagasaki's data federation infrastructure.
† Riho Shikata, Nobuhiro Kobayashi. University of Nagasaki

Copyright ©2023 Information Processing Society of Japan.
All Rights Reserved.

出来るようにし、かつスマートシティセキュリティガイドラインに沿った新サービスが構築出来るようにするためマニュアルを作成する。マニュアルには、スマートシティセキュリティガイドラインに記載されている実施事項に基づき、実施方法や実施手順について、具体的に実施した際のスクリーンショットや図、表を用いて説明を記載する。

4　ベストプラクティス

スマートシティセキュリティガイドラインに記載されている実施事項に基づいたベストプラクティスの一例として、今回は地図上に観光地を表示する Web サイトを構築した。

本論文では、Web サイト開発の流れである基本設計、開発、テスト、公開の 4 つの段階のうち、今回は外部に公開しないため開発段階とテストを対象としている。作成方法は以下の通り。

1：スマートシティセキュリティガイドラインに沿ってセキュリティ対策を実施する
2：ながさき API カタログサイトを用いて Web サイトを作成しながら 3 を実施する
3：実施事項、内容、手順を図や表、写真を用いてマニュアルにまとめる

スマートシティのカテゴリにはガバナンス、サービス、都市 OS、アセットの 4 つがあるが、本論文ではながさき API カタログサイトを用いて新たな Web サイトを構築するので、サービスに該当する。また、スマートシティの新サービスということでもあるため、スマートシティ特有のセキュリティ対策についてもマニュアルに記載している。

（1）マニュアルの実施項目

スマートシティセキュリティガイドラインのサービスの実施項目とスマートシティ特有のセキュリティ対策の実施項目は以下の通りである。

＜サービス＞
①サービス個別でのリスクアセスメントの実施
②外部からの攻撃等を防ぐセキュリティ対策
③セキュリティインシデント発生の未然防止のためのセキュリティ対策
④インシデント発生時に備えたセキュリティ対策

＜スマートシティ特有のセキュリティ対策＞
①適切なサプライチェーン
②インシデント対応時の連携
③データ連携時のセキュリティ

（2）マニュアルの内容　（サービス）

サービスのカテゴリでは、守るべき機能や資産を特定すること、Web サイトのセキュリティを検討し実装することが求められる。マニュアルでは、以下について実際に実施した際の図や表、写真を用いて記載している。

・リスクアセスメントの実施方法や手順
・リスクアセスメント報告書
・WAF の実装方法
・セキュリティテストや脆弱性診断の方法や手順について

（3）マニュアルの内容　（スマートシティ特有のセキュリティ対策）

一主体だけではスマートシティ全体のセキュリティを確保することは難しいため、関係主体全体によるセキュリティ対策が必要となる。マニュアルでは、以下について実際に実施した際の図や表、写真を用いて記載している。

・サプライチェーンリスクの特定方法や対策の検討方法
・ハードウェア・ソフトウェアの選定基準
・インシデント発生時の対応体制や連絡体制

（作成したマニュアルは下記の URL より参照可）
http://apply.sun.ac.jp/internalweb/index.php?user=s&dept=security&year=4

5　考察

本論文では、対象者のような人でもセキュリティ対策が行えるようにマニュアルとチェックシートを作成した。その結果、セキュリティ対策の実施項目が 24 項目から 54 項目となった。リスクアセスメントを実施するという項目では、参考資料や実施手順について例を挙げながら説明しており、具体的な実施方法の知識や経験が無くても、例を見ながら行えば実施出来るようになっている。しかし、リスクに対する対処法などは基本的なセキュリティ知識が必要となるため、基本的なセキュリティ知識を学べる機会やツールが必要であると分かった。

また IDS,IPS の構築の項目では、自力で対策するには高度なセキュリティ知識が必要な為、セキュリティサービス事業者が提供する既存のサービスを利用することも必要であるということが明らかになった。

参考文献

[1]総務省　スマートシティセキュリティガイドライン(第 2 版)　2021 年 6 月
[2]長崎県「つながる長崎」データ連携基盤（ながさきデータマップ他）. https://www.pref.nagasaki.jp/bunrui/shigoto-sangyo/johoka-it/link-nagasaki/index.html, (参照 2022-11-20).

Copyright ©2023 Information Processing Society of Japan.
All Rights Reserved.