6ZC-02

Web サイトを対象とした脆弱性情報ハンドリング教育プログラムの検討

藤田 佳菜子*　　大浦 優太郎　　寺田 真敏
東京電機大学

1. はじめに

インターネットの普及・発展と共に，脆弱性情報を数多く取り扱うようになった．2021 年 7 月に IPA が公開した「ソフトウェア等の脆弱性に関する取り扱い状況」[1]によれば，脆弱性の報告件数は IPA に寄せられたものだけで累計 16,000 件を超えている．

脆弱性報告の取り扱いについては，国内には官民連携で運営されている情報セキュリティ早期警戒パートナーシップと呼ばれる仕組みが存在する．しかし，2021 年 3 月に IPA が公開した「小規模ウェブサイト運営者の脆弱性対策に関する調査報告書概要」[2]では，『情報セキュリティ早期警戒パートナーシップの認知度』について，この仕組みについて聞いたことがない，または聞いたことはあるが内容はよく知らないと回答した Web サイト運営者が 8 割に上ると報告している．脆弱性は数多く報告されているものの，脆弱性情報の取り扱い方の認知度の低さは課題と言える．

本稿では，脆弱性情報の取り扱い方の普及啓発のため，Web サイトを対象とした脆弱性情報ハンドリングを体験するための教育プログラムについて報告する．教育プログラムは，脆弱性公開ポリシーの作成，脆弱性の指摘受領から対応までの体験をサポートする．

2. 国内外の脆弱性情報取り扱いの仕組み

2.1 情報セキュリティ早期警戒パートナーシップ

日本国内には IPA および JPCERT/CC が運営している情報セキュリティ早期警戒パートナーシップ[3]と呼ばれるソフトウェア製品と Web サイトの脆弱性情報の取り扱いの仕組みが存在する．Web サイトの場合，Web サイト運営者(以降，運営者)に Web サイトに存在する脆弱性の修正を促すことを目的としている．脆弱性の発見者(以降，発見者)は調整機関である IPA を通して間接的に運営者に脆弱性の存在を通知する．運営者は，IPA から受領した脆弱性情報を元に脆弱性を修正する(図 1)．また，運営者は，受領した脆弱性に関連して，Web サイトから個人情報漏洩等のインシデントを確認した場合には，その事実を一般に公表する等の措置を取らなければならないとしている．

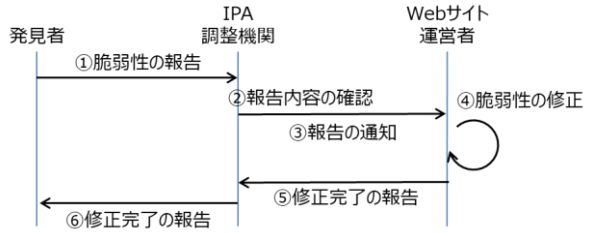

図 1　情報セキュリティ早期警戒パートナーシップにおける Web サイト脆弱性情報取り扱いフロー

2.2 VDP

アメリカ合衆国には VDP(Vulnerability Disclosure Policy，脆弱性公開ポリシー)[4]と呼ばれる脆弱性情報の取り扱いの仕組みが存在する．この仕組みは，米国国土安全保障省が政府機関に作成を義務付けたもので，政府機関と一般市民の相互協力を促し，政府機関のオンラインサービスのセキュリティを高めることを目的としている．VDP では一般の人々(発見者)が政府機関のオンラインサービスに脆弱性を発見した場合の報告手順，またそれに対する政府機関(運営者)の対応を明示しなければならない．脆弱性報の発見者は直接運営者に脆弱性を報告し，運営者は脆弱性の修正を行う(図 2)．

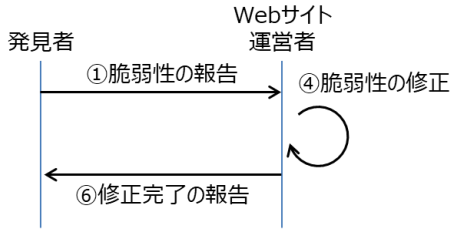

図 2　VDP における脆弱性情報取り扱いフロー

3. 脆弱性情報ハンドリング教育プログラム

第 1 章で述べた，Web サイト運営者の脆弱性情報の取り扱い方の認知度の低さという課題を解決するため，脆弱性報告(発見者側)及び対応(運営者側)の体験を通して，脆弱性情報の取り扱い方を学ぶ教育プログラムを検討した．なお，第 2 章で述べた国内外の脆弱性情報取り扱いの仕組みを踏まえ，脆弱性の報告が直接運営者に届くことを想定した教育プログラムとした．

* A Study on Vulnerability Information Handling Education Program for Web Sites
Kanako Fujita, Yutaro Oura and Masato Terada
Tokyo Denki University

3.1 教育プログラム概要

本教育プログラムは，Web サイトの運営者と脆弱性を見つけ報告する発見者の2つの視点からの体験プログラムで，講師と受講者，受講者のみの 2 人以上を想定している．図 3 の脆弱性情報取り扱いフローに沿って，運営者視点では，テンプレートを用いた脆弱性開示ポリシーの作成，通知された脆弱性情報の読み解き方を XSS(CWE-79;クロスサイトスクリプティング)など Web サイトで良く知られている脆弱性の理解を通して体験する．発見者視点では，本教育プログラム用に作成した脆弱性体験ツール[5]を使った Web サイトでの脆弱性攻撃のハンズオンや通知する脆弱性情報告の作成を体験する．

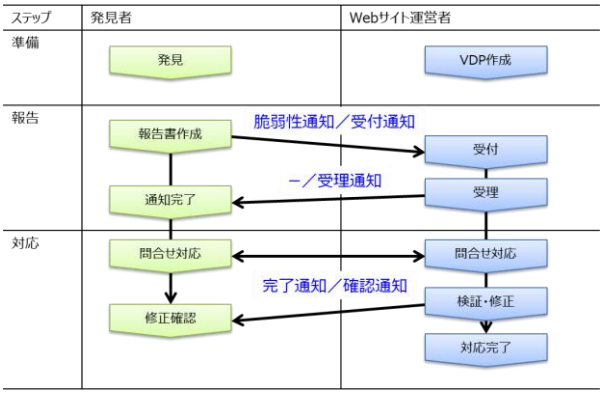

図 3　教育プログラムにおける
脆弱性情報取り扱いフロー

3.2 運営者ならびに発見者視点での体験項目

教育プログラムにおける運営者ならびに発見者視点での体験項目を表 1，表 2 に示す．

3.3 VDP 作成

各体験項目では，実施する上での留意点がある．ここでは，体験項目のうち，教育素材[6][7]の準備が完了している VDP 作成を実施する上での留意点を示す．

- VDP テンプレートの読み込み
  脆弱性公開ポリシーを作成する上での必要項目や用語等を確認し不明点をなくす．
- 必要項目を記載した VDP の作成
  適用範囲，許可する調査方法及び法的措置の追求，報告書の提出先・作成要件，対応期間，連絡先等の必要項目を記載した VDP を作成する．
- 必要項目を記載できる報告フォームの作成
  脆弱性の発見日や種類，再現方法，発見者の連絡先等の必要項目を記載できる報告フォームを作成する．

4. まとめ

本稿では Web サイトの運営者および発見者視点で脆弱性情報の取り扱い方の学習支援，及び普及啓発を目的として，Web サイトを対象とした脆弱性情報ハンドリング教育プログラムについて検討した．

本教育プログラムでは，発見者から運営者に直接脆弱性情報の報告があったと想定し，脆弱性情報の取り扱い方を体験する．特徴は，Web サイトの運営者と脆弱性を発見し報告する発見者とに視点を分け，脆弱性公開ポリシーの作成，脆弱性の指摘受領から対応までの体験をサポートするところにある．

今後，検討した脆弱性ハンドリング教育プログラムの体験項目の具体化を進めていく．

表 1　運営者視点の体験項目

体験項目	内容
VDP 作成	脆弱性公開ポリシーを作成する(3.3 章参照).
受付	事前に用意した通知用脆弱性情報を報告フォームで受け付け，受付を通知する.
受理	通知された脆弱性情報が，次の条件を満たしているか否か判断する．満たしている場合には報告受理を通知する. ● 報告フォームの項目が十分に記述されている. ● 脆弱性情報であり，既に報告されている脆弱性情報ではない.
問合せ対応	発見者に適宜状況を報告する.
検証・修正	報告された脆弱性について，報告内容に沿って，脆弱性が存在するかを検証する.
対応完了	修正内容について発見者に確認をとり，対応を完了する.

表 2　発見者視点の体験項目

体験項目	内容
発見	OWASP Top10 の脆弱性を資料と，脆弱性体験ツールによるハンズオンを通して理解する[5].
報告書作成	VDP を読み，報告先や報告要件を確認した後，事前に用意した通知用脆弱性情報を用いて報告書を作成する.
問合せ対応	運営者に適宜状況を確認する.
修正確認	脆弱性体験ツールによるハンズオンを通して修正により脆弱性が発動しないことを確認する.

参考文献

[1] IPA，“ソフトウェア等の脆弱性関連情報に関する届け出状況[2021 年題四半期(4 月～6 月)]”，https://www.ipa.go.jp/security/vuln/report/vuln2021q2.html ， 2021 年 10 月参照
[2] IPA，“小規模ウェブサイト運営者の脆弱性対策に関する調査報告書概要”，https://www.ipa.go.jp/files/000089536.pdf ， 2021 年 12 月参照
[3] IPA，“情報セキュリティ早期警戒パートナーシップガイドライン”，https://www.ipa.go.jp/security/ciadr/partnership_guide.html ,2021 年 10 月参照
[4] 米国安全保障省，“Bending Operational Directive 20-01”,https://cyber.dhs.gov/bod/20-01/ ,2021 年 10 月参照
[5] 大浦優太郎・藤田佳菜子・寺田真敏“脆弱性情報ハンドリング教育プログラムにおける Web サイト脆弱性体験ツールの検討”，情報処理学会第 84 回全国大会,2022 年
[6] 情報セキュリティ研究室，“Vulnerability Disclosure Policy, https://www.isl.im.dendai.ac.jp/vulnerability-disclosure-policy/ ， 2022 年 1 月参照
[7] 情報セキュリティ研究室，“脆弱性情報報告フォーム”，https://www.isl.im.dendai.ac.jp/vulnerability-disclosure-policy/report-form.html ,2022 年 1 月参照