資料 1-5

ソフトウェア製品の脆弱性対処促進に関する調査

1. 調査背景・検討概要

- ソフトウェア製品の脆弱性対処について、製品開発者としての責務（望ましい対処）であることを認識させるべく普及啓発を実施しているが、中小規模の製品開発者ではリソース不足等の理由により網羅的に対処することは困難な場合がある。
- 一般消費者向け製品は価格や機能ばかりが競争要素となっており、製品開発者が望ましい対処をしても一般消費者によるソフトウェア製品選定の動機づけや競争要素とならないため、脆弱性対処が製品開発者の利益に繋がり辛い。このことから、脆弱性対処への予算が充てられず対処が促進されない状況にあると推測される。
- このため、最低限の対処を促進するために望ましい対処の優先度付けを行い、最低限必要なもののみを抽出するとともに、望ましい対処を実施するための体制や手順、想定されうる課題への対処方法をこれまでの脆弱性研究会での調査結果も踏まえて検討する。さらに、望ましい対処をしているソフトウェア製品が一般消費者から評価されるために対処状況を開示(アピール)する方法を検討する。

（1）文献／事例の調査

（2）ヒアリング調査
（製品開発者**（中小規模）**、セキュリティ有識者、業界団体　等6社）

(1)(2)の調査結果を基に作成

（3）製品開発者向けガイドの作成

（アウトプット）製品開発者における望ましい脆弱性対処・公表に関する調査報告書、普及手段と効果測定方法、普及促進資料

2.文献／事例の調査（1/3）

- 製品開発者による脆弱性対処に関して、望ましい対処項目およびその開示方法について、文献/事例の調査結果やこれまでの脆弱性研究会報告書を踏まえて、**「製品開発者における望ましい脆弱性対処・公表に関する調査結果報告書」**として取り纏める。
- 下記の検討結果を調査結果報告書に含める。
  - 望ましい対処項目の優先度、および、望ましい対処項目の開示方法
  - 望ましい対処を実施するための体制や手順、想定されうる課題への対処法

[成果物]
製品開発者における望ましい脆弱性対処・公表に関する調査結果報告書

[調査対象と件数]
これまでの脆弱性研究会での調査結果を踏まえ、下記のような文献を10件以上調査する。
- ISO等の世界標準規格
- 国内外の政府機関・セキュリティ団体が公開する資料
- 業界団体が公開する資料
- 国内外の製品開発者による望ましい脆弱性対処と開示事例　等

[調査項目]
- 望ましい対処項目および優先度
- 望ましい対処を実施するための体制や手順
- 望ましい対処項目の対応状況の開示方法
- 望ましい対処項目を実施する上での阻害要因・課題
- 望ましい対処を阻害する想定課題への対処方法
- 望ましい対処項目が実施できない場合の代替策

2.文献／事例の調査（2/3）

■ 文献調査対象（案）は以下の通り。

	文献名	記載内容
1	SP 800-40 ver.3 Creating a Patch and Vulnerability Management Program	パッチおよび脆弱性管理プログラムの策定
2	NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks（2019）	IoT機器により生じるサイバーセキュリティとプライバシーリスクを軽減するための対策例
3	IOTSF（IoT Security Foundation） IoTSF Vulnerability Disclosure Best Practice Guidelines	脆弱性開示のベストプラクティス
4	NIST Small Business Information Security: The Fundamentals	中小企業向けサイバーセキュリティ対策 ※利用者の観点から開発者への要求事項を抽出
5	NISTIR 8259 (DRAFT) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers	IoT機器のセキュリティに関するベースライン、考え方、根拠
6	CARNEGIE MELLON UNIVERSITY The CERT® Guide to Coordinated Vulnerability Disclosure	脆弱性発見時の望ましい報告内容
7	UK DCMS Code of Practice for consumer IoT security	消費者向けIoTセキュリティに関する13項目のベストプラクティス
8	ETSI TS 103 645 CYBER Cyber Security for Consumer Internet of Things	IoT機器の最低限のセキュリティ要件

2.文献／事例の調査（3/3）

■ （続）

	文献名	記載内容
9	経済産業省「サイバーフィジカルセキュリティ対策フレームワーク」	セキュリティの観点から、バリュークリエイションプロセスにおけるリスク源を整理するためのモデル（三層構造と6つの構成要素）
10	IPA「つながる世界の開発指針」	IoT製品の開発者が開発時に考慮すべきリスクや対策
11	IPA「IoT開発におけるセキュリティ設計の手引き」	IoT機器およびその使用環境で想定されるセキュリティ脅威と対策
12	IPA「つながる世界のセーフティ＆セキュリティ設計入門」	経営者への啓発、現場の技術者へのセーフティ設計・セキュリティ設計の入門ガイド
13	IoT推進コンソーシアム・総務省・経済産業 「IoTセキュリティガイドラインver1.0」	IoT機器やシステム、サービスについて、セキュリティ確保の観点から求められる基本的な取組
14	IPA「IoT製品・サービス脆弱性対応ガイド」	経営者・管理者向け、企業が実施すべきIoT脆弱性対策のポイント
15	CSAJ セキュリティ委員会 制度WG プロダクト脆弱性対策・対応成熟度シートVersion 1.0	25のフレームワークを元にした成熟度

3.ヒアリング調査（1）調査目的・概要

- 文献調査結果を踏まえて、後述する「製品開発者向けガイド」の普及手段(普及に協力頂ける他組織、掲載場所、掲載方法、媒体等)および効果測定方法について検討し、検討結果を資料**「普及手段と効果測定方法」**として取り纏める。
- 「製品開発者向けガイド」および「普及手段と効果測定方法」についてのヒアリング調査を実施する上での具体的な実施時期、対象者、調査項目について**「ヒアリング実施概要」**として資料を取り纏める。
- ヒアリング調査を実施するために、**「ヒアリング対象者向け主旨説明」**資料を作成する。

- ヒアリング調査を実施し、**「ヒアリング調査結果」**の資料を作成する。
- ヒアリング調査結果を踏まえ、**「普及手段と効果測定方法」**の資料を見直す。普及啓発に必要な資料**「普及促進資料」**を作成する。

[成果物]
普及促進資料

3. ヒアリング調査（2）ヒアリング実施概要

■ ヒアリング実施概要は以下の通り。

調査対象	ヒアリング6件以上 （製品開発者、セキュリティ有識者、業界団体　等） 【ヒアリング候補（案）】 ＜製品開発者（中小規模）＞ ＜セキュリティ有識者＞ ＜業界団体＞
実施時期	2019年11月
調査項目	• 「製品開発者向けガイド」の内容の妥当性 • 望ましい対処ができない理由、課題 • 課題の解決方法 • 望ましい対処項目の対応状況の開示方法 • 効果的な普及手段　等

3. ヒアリング調査（3）普及手段と効果測定方法

■ 「製品開発者向けガイド」の普及手段および効果測定方法（案）については以下の通り。

普及に協力いただける他組織	業界団体	SIer・製品ベンダ	セミナー・研修事業者	セキュリティベンダ	ITメディア系Webサイト	IPAが参加するイベント・セミナー
普及対象	• 製品開発者（会員）	• 製品開発者（取引先）	• 製品開発者（受講者）	• 製品開発者（サービス提供者）	• 製品開発者	• 製品開発者
場所	• Webサイト（電子ファイル掲載） • イベント等	• 調達時	• セミナー・研修	• セキュリティサービス提供時	• Webサイト	• イベント会場
方法	• ガイドの掲載 • ガイドの配布・紹介	• ガイドの提示	• ガイドの配布	• ガイドの配布	• 寄稿 • ガイドの掲載	• パンフの配布 • ガイドの配布
媒体	• 電子ファイル • 紙媒体	• 電子ファイル • 紙媒体	• 紙媒体	• 紙媒体	• 電子ファイル	• 紙媒体
効果測定手法	• ダウンロード数 • 会員向けアンケート調査	• 配布数	• 事業者向けヒアリング調査 • 受講生向けアンケート調査	• 事業者向けヒアリング調査	• アクセス数をヒアリング • ダウンロード数の調査	• 配布数の調査

4.製品開発者向けガイドの作成（1）調査目的・概要

- 調査結果を基にして、**「製品開発者向けガイド（骨子）」**を作成する。
- ヒアリング調査を結果を踏まえ、「製品開発者向けガイド（骨子）」を見直し、**「製品開発者向けガイド」**として取り纏める。
- 「製品開発者向けガイド」の作成にあたり、以下の事項について考慮する。
  - 製品開発者にとって分かり易い内容で作成する
  - 表紙等についてはデザインに配慮して作成する
  - ウェブページでの公表及び、冊子化しての配布等をすることを前提として資料を作成する
- 分量は最大20ページ程度（チェックリスト含む）とする。

[成果物]
製品開発者向けガイド

[製品開発者向けガイドに関する構成案]
脆弱性対処・公表の意義
最低限実施すべき項目とその理由
最低限実施すべき項目が実施できない場合の代替策（ノウハウ等）
実施に際して必要な体制や手順
実施を阻害する要因／課題
課題への対処方法
望ましい対処項目の対応状況の開示方法
チェックリスト（別紙）

4.製品開発者向けガイドの作成 （2）ガイド骨子案（1/2）

■ **「製品開発者向けガイド（骨子）」（案）**において採り上げる項目は、文献調査において選定した文献に記載があり、ガイドの対象とする中小規模の製品開発者にとって有用な項目とする。

ガイドの目的・想定読者：中小規模の製品開発者（開発部門、セキュリティ担当の方）

1. 脆弱性対処・公表の意義

① 脆弱性対処を行わない場合のリスク
② 脆弱性対処の必要性・意義

2. 最低限実施すべき項目とその理由

＜製品の機能・要件＞
① セキュアな通信を確保すること
② アップデートデータ等の完全性を検証すること
③ ユーザに対して通知を行うこと
④ 不完全なアップデート時の対応を行うこと（フェールオーバー、初期化等）
⑤ 初期パスワードを設定しないこと

＜製品の開発＞
① 新たに脆弱性を作り込まないこと
② 既知の脆弱性を解消すること
③ 調達した部品の脆弱性を管理すること

＜脆弱性発見時の対処＞
① 脆弱性が発見された時の対策を検討すること
② パッチリリースの管理計画を検討すること

［コラム］最低限実施すべき項目が実施できない場合の代替策（ノウハウ等）

4.製品開発者向けガイドの作成
（2）ガイド骨子案（2/2）

3. 実施に際して必要な体制・手順

① 体制

a. セキュリティサポート方針を明確にすること
b. 内部のステークホルダ管理を行うこと
c. 運用・保守体制を整備・維持すること
d. 脆弱性報告の受付窓口を作ること
e. 情報開示やユーザへの通知体制を整備すること
f. 継続的に脆弱性対策情報の収集を行うこと

② 手順

4. 脆弱性対処の課題と対処方法

① コスト
② 人材
③ 保守

5. 対応状況の望ましい開示方法

① 内容
② タイミング
③ 対象
④ チャネル

チェックリスト（別紙）