資料 3-3

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. ヒアリング調査（1）調査目的・概要

■ 後述する「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。

■ 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。

■ 文献調査結果を踏まえて、「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)、およびガイドの内容がどれだけ認知（理解）されたか、適用されたかについての効果測定方法を検討し、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。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

2. 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】 ＜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～12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.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）

3.製品開発者向けガイドの作成 （2）ガイド案

■ **「製品開発者向けガイド」（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るもので、ガイドが対象とする中小規模の製品開発者が、段階的に対策を進められるよう、レベル分けの記載を行った。

ガイドの想定読者：中小規模の製品開発者（開発部門、セキュリティ担当の方）

エグゼクティブサマリ

背景・目的
想定読者
対象製品
本書の構成

I. 方針・組織
1. 全体ポリシーを定める
2. セキュリティサポート方針を明確にする
3. 製品セキュリティを維持するための体制と管理

II. 設計・開発
4. セキュリティを確保するための設計
5. アップデートを考慮した開発
6. 既知の脆弱性を解消する
7. セキュアコーディング
8. 開発環境のセキュリティを保つ
9. リリース前にテストを実施する
10. 製品と製品コンポーネントの脆弱性監視

III. リリース後の対応
11. 脆弱性の報告の受付・通知・情報開示
12. 利用者がするべき事項や利用者に委ねられたリスクを明示する

IV. 一般消費者に留意いただく事

V. 用語集

VI. 参考情報

※各項目に『①意義②実施方法・検討方法③開示方法・開示例』を追記

チェックリスト（別紙）

IPA

以下のページは非公開

4. ヒアリング調査結果

5. ヒアリング調査結果　得られた意見と対応方針