
一般消費者のリテラシー向上に関する調査

IPA 1. 調査背景・検討概要

- ソフトウェア製品の脆弱性対処に関して製品開発者が望ましい対処と開示等を行った場合でも、一般消費者のセキュリティに関するリテラシーが低い場合は、脆弱性対処がなされている製品が選定されない。また、安全な製品利用(適切な設定やパッチ適用など)がされていない状況にある。これにより、脆弱性が放置された状態で利用されているソフトウェア製品が多数存在すると推察する。
- このため、一般消費者が安全なソフトウェア製品等を選定するための確認事項、及び、ソフトウェア製品等を購入後に安全に利用するために必要な対応事項を検討する。

「ソフトウェア製品の脆弱性対処促進に関する調査」
「ソフトウェア製品を購入後に安全に利用するために必要な対応事項の調査」

(1) 一般消費者向けガイドの作成

一般消費者向けガイド
(安全なソフトウェア製品の選定)

一般消費者向けガイド
(ソフトウェア製品購入後の安全な利用)

(1)についての意見聴取

(2) ヒアリング調査

(製品開発者、セキュリティ有識者、
業界団体「量販店、ECサイト、販売協会 等6社)

(アウトプット) 普及手段と効果測定方法、普及促進資料

IPA 2.一般消費者向けガイドの作成

- 一般消費者が安全なソフトウェア製品を選定するための確認事項について「**一般消費者向けガイド（安全なソフトウェア製品の選定）**」として取り纏める。
- ソフトウェア製品購入後に安全に利用するために必要な対応事項についての調査結果を踏まえ、「**一般消費者向けガイド（ソフトウェア製品購入後の安全な利用）**」として取り纏める。
- 「一般消費者向けガイド」の作成にあたり、以下の事項について考慮する。
 - 一般消費者にとって分かり易い内容で作成する
 - 一般消費者に手に取って頂ける様に、全体構成やイラスト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行うことを前提として資料を作成する

[成果物]

- ・「**一般消費者向けガイド（安全なソフトウェア製品の選定）**」
 - ＜構成案＞
 - 安全なソフトウェア製品を選定する意義
 - ソフトウェア製品選定／購入時に最低限確認すべき項目とその理由
 - 確認場所／確認方法
 - チェックリスト（別紙）
- ・「**一般消費者向けガイド（ソフトウェア製品購入後の安全な利用）**」
 - ＜構成案＞
 - ソフトウェア製品購入後にセキュリティを維持する意義
 - ソフトウェア製品購入後に最低限実施すべき項目とその理由
 - 実施方法
 - チェックリスト（別紙）

IPA 3.ヒアリング調査（1） 調査目的・概要

- 「一般消費者向けガイド（安全なソフトウェア製品の選定）」、「一般消費者向けガイド（ソフトウェア製品購入後の安全な利用）」の普及手段(普及に協力頂ける他組織の調査、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。
- 「一般消費者向けガイド（安全なソフトウェア製品の選定）」、「一般消費者向けガイド（ソフトウェア製品購入後の安全な利用）」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。
- ヒアリングを実施するために、「**ヒアリング対象者向けの主旨説明**」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を取り纏めた資料「**ヒアリング調査結果**」を作成する。
- 普及に必要な資料「**普及促進資料**」を作成する。

[成果物]
普及促進資料

IPA 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「量販店、ECサイト、販売協会 等」） 【ヒアリング候補（案）】 ＜製品開発者＞ ＜セキュリティ有識者＞ ＜業界団体（量販店、ECサイト、販売協会）＞
実施時期	2019年12月
調査項目	<ul style="list-style-type: none">• 一般消費者向けガイドの内容の妥当性• 効果的な普及手段• 業界団体による活用方法案• 業界団体による普及・活用における課題とその解決方法 等

3. ヒアリング調査（3）普及手段と効果測定方法 （1/2）

■ 「一般消費者向けガイド」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	量販店	ECサイト	販売協会	公的機関	教育機関
普及対象	<ul style="list-style-type: none"> 販売員 製品購入者 	<ul style="list-style-type: none"> 製品購入者 	<ul style="list-style-type: none"> 製品購入者 協会加盟者 	<ul style="list-style-type: none"> 製品購入者 	<ul style="list-style-type: none"> 学生(製品購入者)
場所	<ul style="list-style-type: none"> 店頭 	<ul style="list-style-type: none"> Webサイト (電子ファイル掲載) 	<ul style="list-style-type: none"> カタログ、パンフレット Webサイト (電子ファイル掲載) 	<ul style="list-style-type: none"> 受付事務所 	<ul style="list-style-type: none"> 各校
方法	<ul style="list-style-type: none"> 設置 配布 掲示 	<ul style="list-style-type: none"> 掲載 	<ul style="list-style-type: none"> 配布（カタログ・パンフレット送付時同封） 掲載 	<ul style="list-style-type: none"> 設置 配布 掲示 	<ul style="list-style-type: none"> 掲示板での掲載 パンフの配布 ガイドの配布
媒体	<ul style="list-style-type: none"> 紙媒体 	<ul style="list-style-type: none"> 電子ファイル 	<ul style="list-style-type: none"> 紙媒体 電子ファイル 	<ul style="list-style-type: none"> 紙媒体 	<ul style="list-style-type: none"> 電子ファイル 紙媒体
効果測定手法	<ul style="list-style-type: none"> 量販店へのヒアリング調査 量販店を通じた販売員へのアンケート調査 	<ul style="list-style-type: none"> ダウンロード数 	<ul style="list-style-type: none"> 配布数 ダウンロード数 	<ul style="list-style-type: none"> 公的機関へのヒアリング調査 公的機関を通じた配布者へのアンケート調査 	<ul style="list-style-type: none"> 配布数の調査

3. ヒアリング調査（3）普及手段と効果測定方法 （2/2）

- IPAにおける「一般消費者向けガイド」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。
- 費用対効果なども考慮して取捨選択の上、より効果的な手段を実施予定。
- 実施に際しての具体的な方法は、関係部門と相談・調整予定

	ITメディア系 Webサイト	IPAが参加する イベント・セミナー	IPA インターネット 安全教室	IPA セキュリティプレゼンター	SNS (Facebook, Twitter) メール配信
普及対象	<ul style="list-style-type: none"> 小売り事業者 一般消費者 	<ul style="list-style-type: none"> 一般消費者(製品利用者) 	<ul style="list-style-type: none"> 教育機関 一般消費者 	一般消費者(セキュリティに関心がある人)	<ul style="list-style-type: none"> IPAフォロアー(セキュリティに関心がある人)
場所	<ul style="list-style-type: none"> Webサイト 	<ul style="list-style-type: none"> イベント会場 	<ul style="list-style-type: none"> Webサイト 各都道府県の安全教室 	<ul style="list-style-type: none"> 全国各地のプレゼンター 	<ul style="list-style-type: none"> SNS メール
方法	<ul style="list-style-type: none"> 寄稿 ガイドの掲載 	<ul style="list-style-type: none"> パンフの配布 ガイドの配布 	<ul style="list-style-type: none"> 教材への取り込み パンフの配布 ガイドの配布 	<ul style="list-style-type: none"> パンフの配布 ガイドの配布 	<ul style="list-style-type: none"> 告知文とリンク掲載
媒体	<ul style="list-style-type: none"> 電子ファイル 	<ul style="list-style-type: none"> 紙媒体 	<ul style="list-style-type: none"> 紙媒体 電子ファイル 	<ul style="list-style-type: none"> 紙媒体 	<ul style="list-style-type: none"> SNS メール
効果測定 手法	<ul style="list-style-type: none"> アクセス数をヒアリング ダウンロード数の調査 	<ul style="list-style-type: none"> 配布数の調査 	<ul style="list-style-type: none"> ダウンロード数の調査 配布者へのアンケート 	<ul style="list-style-type: none"> 配布数の調査 ダウンロード数の調査 	<ul style="list-style-type: none"> いいねの件数 メール配信数

4.一般消費者向けガイド (安全なソフトウェア製品の選定) 骨子案

- 「一般消費者向けガイド (安全なソフトウェア製品の選定) 」 (骨子案) において採り上げる項目は、以下の通り。選定時に確認可能な内容とし、一般消費者が安全な製品を選定可能とする。

＜一般消費者向けガイド (安全なソフトウェア製品の選定) 骨子案＞

1. 安全なソフトウェア製品を選定する意義
2. ソフトウェア製品選定／購入時に最低限確認すべき項目とその理由
 - ① セキュリティサポート方針が記載されているか
 - ② 脆弱性対策情報に関する通知を行うことが記載されているか
 - ③ 情報開示の場所・方法やユーザへの通知元が記載されているか
 - ④ 脆弱性報告の受付窓口が記載されているか
3. 確認場所／確認方法

チェックリスト (別紙)

「製品開発者向けガイド」のうち、開示を勧める内容を反映

＜製品開発者向けガイド (骨子) ＞

1. 脆弱性対処・公表の意義
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 ユーザに対して脆弱性対策情報に関する通知を行うこと
 - ④ 不完全なアップデート時の対応を行うこと
 - ⑤ 初期パスワードを設定しないこと
 - ＜製品の開発＞
 - ＜脆弱性発見時の対処＞
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
5. 対応状況の望ましい開示方法

4.一般消費者向けガイド (ソフトウェア製品購入後の安全な利用) 骨子案

- 「一般消費者向けガイド（ソフトウェア製品購入後の安全な利用）」（骨子案）において採り上げる項目は、以下の通り。利用時に認識・実施可能な内容とし、一般消費者による製品の安全な利用を可能とする。

＜一般消費者向けガイド (ソフトウェア製品購入後の安全な利用) 骨子案＞

1. ソフトウェア製品購入後にセキュリティを維持する意義
 2. ソフトウェア製品購入後に最低限実施すべき項目とその理由
 - ① セキュアな通信を確保すること
 - ② 初期パスワードを設定しないこと
 - ③ 情報開示、あるいは通知される脆弱性対策情報を確認すること
 3. 実施方法
- チェックリスト（別紙）

「製品開発者向けガイド」のうち、
利用者が購入後に留意する
点を反映

＜製品開発者向けガイド（骨子）＞

1. 脆弱性対処・公表の意義
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 ユーザに対して脆弱性対策情報に関する通知を行うこと
 - ④ 不完全なアップデート時の対応を行うこと
 - ⑤ 初期パスワードを設定しないこと
 - ＜製品の開発＞
 - ＜脆弱性発見時の対処＞
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
5. 対応状況の望ましい開示方法