資料３－２

2019 年度 情報システム等の脆弱性情報の取扱いに関する研究会 第 2 回会合 開催結果概要

●日時: 2019 年 11 月 22 日(金)15:00 ～ 17:00
●場所: 文京グリーンコート センターオフィス 15 階 委員会室 1,2,3
●出席者(敬称略):
座長: 土居
委員: 歌代、垣内、北澤、栗田、柴﨑、下村、高木、高橋、谷川、西嶋、山崎
オブザーバ: METI 奥家課長、津國課長補佐;CSAJ 戸島;JPCERT/CC 宮地、椎木、高橋、石川、伊藤
事務局: IPA 富田理事長、江口理事、瓜生、桑名、渡辺、土屋、板橋、木曽田、田中、井上、唐亀
MRI 村野、江連、小川、朱、平林

●決定事項:
- 第 1 回会合の開催結果概要について委員より承認を得た。
- 本年度の研究会の活動内容について、本会合の議論を踏まえて引き続き進めることで決定した。

●主な論点:

1. 前回会合の確認について

事務局から、資料 2-2 に基づき前回会合における検討について説明の後、以下の補足を行った。議事結果概要については委員より承認を得た。
- IPA で意識調査をしており、今年度も 12 月上旬から中旬にかけて、脆弱性に関する設問を入れて実施予定。ウェブ調査で、PC・スマートフォンユーザ計 1 万人の一般消費者が対象。2 月頃に意識調査結果が公開。

2. ソフトウェア製品の脆弱性対処促進に関する調査について

事務局から、資料 2-3～資料 2-6 に基づきソフトウェア製品の脆弱性対処促進に関する調査について説明の後、委員から以下の意見を頂いた。
- エグゼクティブサマリやグローサリー付け、理解を得るようにした方がよい。
- 製品開発者ガイドについては、製品分野によって要求事項が異なることを考慮すべき。
  - 分野/機能でマトリックスの作成等を検討する。
- この分野は技術革新が激しく仕様要求は古くなりやすいため、一般論としてベースラインポリシーを記載し方向感が捉えられるようにする。あわせて、調査文献の制定背景を踏まえて例として使えるものを例示する。
- ヒアリングの結果、中小企業の製品開発者においてガイドに記載する対策が難しいという意見があったが、技術的・本質的に困難という理由が無い限り、やらなければならない技術的に正しいプラクティスを記載すべき。
- ガイドの項目の対応状況に関する表彰もしたらどうか。

3. 一般消費者のリテラシー向上に関する調査について

事務局から、資料 2-7～資料 2-9 に基づき一般消費者のリテラシー向上に関する調査について説明の後、委員から以下の意見を頂いた。
- デザインは検討してほしい。
  - 現在は骨子のため、今後デザインを考慮予定である。
- 一般消費者が理解できる表現を用いて簡単かつ簡潔としつつ、もう少し説明したほうが親切である。
- 運用ガイドには、まずアップデートを「定期的に」実施するということが書かれているべき。
- アップデートの重要性を理解してもらうため、アップデートしないとどうなるかを書くべき。
- 運用ガイドについては、今まで買った機器を確認し、必要に応じて買い替えてほしいこともあるのでは。
- 一般消費者が購入前にマニュアルを確認しないと思われるため、簡単に確認でくる方法(店員に聞く等)を記載する。
- 初めは、消費者のうち気にする人たちにフォーカスし、メッセージを伝えた方がよい。
- 開発者向けガイドに対応する事項を入れるべきでは無いか。
  また、一般消費者が製品開発者の取り組み状況を分かるような対策として以下の意見もでた。

- 売り場に製品毎のガイドの対応状況が表示されたり、ウェブですぐに確認できるようになっているとよい。
- 製品に認証マークを掲示する案も挙がったが、マークが何を保証しているかが明確でないと一般消費者が混乱するため、一般消費者がリスクを理解し対策を講じるように、本質を啓発すべきとの意見があった。
- 売る側のサポートも必要である。
- しっかり対策しているメーカー2・3 社の良い例を示してはどうか。
- 対策を行っている日本企業の強みを活かせる仕組みがあるとよい。

4. サポート終了製品のパートナーシップにおける取扱いに関する調査について

事務局から、資料 2-10 に基づきサポート終了製品のパートナーシップにおける取扱いに関する調査について説明の後、委員から以下の意見を頂いた。

- EoL の場合、優先情報提供では製品の利用停止が案内されるが、メーカーがパッチを作れるなら通常の優先情報提供と同様に対策情報が提供される。
  - EoL の場合、優先情報提供の条件「対策が作成後」に該当しないため、優先情報提供できないのではないか。
- EoL と利用中止の旨だけを公表した場合、脆弱性情報を伏せていたとしても、IPA が公表したことにより、脆弱性届出があったことが推察される恐れがある。
- 告示では、優先情報提供の条件として「製品開発者と協議」の記載があり、連絡不能開発者の場合は開発者から優先情報提供の了承が得られないため、優先情報提供ができない。
- 「協議」には伝達は必須だが合意までは必須でないのではないか。
  - 告示の「協議」という概念に「合意」が含まれるならば、告示の改正が必要ではないか。
- 開発者の同意が必要なのは何故か、本質的な理由に立ち返る必要があるのでは。
- 利用者との契約があるため、メーカーとしても使うなとは言いづらいが、第三者が使うなと言ってくれればメーカーとしてもありがたいのではないか。

5. スケジュールについて

事務局から、資料 2-11 に基づきスケジュールについて説明の後、以下日時で委員から了承を頂いた。

- 第 3 回研究会は 12 月 25 日(水)13:30-15:30

以上