2025 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 3 回会合 開催結果概要

●日時: 2026 年 2 月 16 日(月)13:00 ～ 15:00
●場所: 文京グリーンコートセンターオフィス 17 階貸会議室 A
●出席者(敬称略):
座長:土居
委員:歌代、垣内、北澤、木谷、下村、新、鈴木、高木、高橋、谷川、中尾、中野、森田、山崎
オブザーバ:MIC 田中、入谷
JPCERT/CC 洞田、石川、阿部、桑原
事務局:NCO 伊藤企画官、澤村
METI 武尾課長、薄羽、関戸
IPA 清水理事、酒井、川口、渡辺、板橋、北爪、夏目、大久保、唐亀
NRI 山本、平岩、山口

●主な論点:

1. 第 2 回会合の振り返りについて

事務局から、資料 3-2 に基づき第 2 回会合の振り返りについて説明し、委員から以下の意見を頂いた。
- 開催結果概要では、会合において実施することとなったこと、決定したことがわかるような書き方にすることが望ましい。
- サイバー対処能力強化法の施行に伴う告示・ガイドライン改正は、スピード感を持って検討を行う必要がある。

2. サイバー対処能力強化法の施行に伴う告示改正状況の説明について

事務局から告示改正に関する進捗状況について説明を行った。

3. 製品開発者向けガイド(案)について

事務局から、資料 3-3 に基づき製品開発者向けガイド(案)について説明し、土居座長、委員から以下の意見を頂いた。
- EU の CRA 対応などでは第三者認証が重要になる。また、脆弱性の発見との関連で、第三者認証機関が脆弱性を発見する場合の対応も調査検討すべきである。
- ISO/IEC 29147(脆弱性の開示)や、ISO/IEC 30111(脆弱性対処プロセス)の内容を参考にして、記載内容を充実すべきである。
- IoT 機器については法令上の規制が既に存在している。そのような法令要件への対応について、ガイドのスコープとの関係で整理するのがよい。
- 「安全」という言葉が多く使われているが、セーフティとの区別の観点から用語を整理すべきである。
- 経営層が果たすべき役割について、何をすべきかがほとんど記載されていない。経営層が果たすべき役割に関する記載をガイドの最初に記載すべきである。
- SI 事業者や、小売・卸売事業者のような製品開発者と製品利用者の間に立つ事業者の位置づけを整理し、それらの事業者に関連する課題があることを記載する必要がある。
- 本ガイドの定義と、告示の定義が異なる部分については、混乱を避けるため、それぞれの関係を適切に説明する必要がある。告示では、製品開発者の定義に、ソフトウェア製品を頒布する者等も含まれるが、本ガイドでは、製品開発者の定義に含まれないことを記載すべきである。
- 製品開発者と製品利用者が協働して脆弱性に対処し、対応品質を高めていく上で、利用規約やユーザーマニュアルといったソフトウェア自体の付帯物が重要となる。ガイドの中でも言及すべきである。

4. 製品利用者向けガイド(案)について

事務局から、資料 3-4 に基づき製品利用者向けガイド(案)について説明し、土居座長、委員から以下の意見を頂いた。
- 中小企業が実施するには難しい内容のものが多い。大企業を想定しているのであれば、そのように想定読者に追記すべきである。また、想定読者を大規模の企業に限定しないのであれば、網羅的な対応を求めるのではなく、読者の所属する企業の規模や、リソースに応じて実施できるところから検討・対応を開始することと明記することが望ましい。

- 中小企業については、IPA が別途提供する中小企業向けコンテンツにおいて対応する。本ガイドは、比較的規模や体力のある企業を対象とする想定であるので、その旨をガイドで明示する形で修正する。

・ 製品利用者向けガイドはスコープが広すぎる印象である。脆弱性対処に関する部分だけに焦点を当てた内容にすることが望ましい。
  - ソフトウェア・システムのライフサイクル全体を通じて脆弱性対処が必要であることを示すものとするため、広いスコープとすることを想定している。
・ 製品開発者と製品利用者の責任分界に関与しないのであれば、そのように明記した方がよい。
・ 法令上、契約内容にセキュリティ要件が明示されていない場合や、サポート内容が明示されていない場合等において問題が生じることが多いとの認識である。製品利用者側が契約でセキュリティ要件やサポート内容を明確にすることで、問題を回避し、セキュリティを担保できる場合があることを記載すべきである。
・ 製品利用者が、ソフトウェアだけではなく、ソフトウェアに付帯する利用規約、ユーザーマニュアルの内容や、契約内容について事前に確認し、製品開発者が想定しない使い方をしないことを求める内容を記載すべきである。
・ クラウドサービスでの暗号化消去については、クラウドサービス事業者ごとに状況が異なることを踏まえ、実態に沿った内容にするのが望ましい。

5. 情報システム等の脆弱性情報の取扱いに関する調査の報告書(案)について

事務局から、資料 3-5 に基づき情報システム等の脆弱性情報の取扱いに関する調査の報告書(案)について説明し、委員から以下の意見を頂いた。

・ 業界ごとに脆弱性管理に関するセキュリティ基準やガイドラインが作成されており、今後も増加することが想定される。そのような基準等と今回作成するガイドの整合性を確認することも重要である。

6. その他

事務局から、来年度の研究会の実施時期について説明した。

以上