2012 年 12 月 18 日

独立行政法人情報処理推進機構(IPA)

欧州連合(EU)における、インシデント発生状況(2011 年度)

本概要は、欧州ネットワーク情報セキュリティ庁(ENISA:European Network Information Security Agency)が発行する、"Annual Incident Reports 2011 – Analysis of the Article 13a incident reports of 2011"の抄訳となります。内容の詳細につきましては、原文をご参照ください。(※本文中のリンク先は全て英文となります)

URL:

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011

欧州連合(EU)加盟国は、年に 1 度、通信ネットワークおよび通信サービスにおけるインシデント発生状況を、欧州委員会(EC)およびENISAに報告することが枠組指令(2009/140/EC)条項13aで義務付けられている。本報告書は、これに従い各国が 2012 年春に報告した、2011 年度の深刻なインシデント 51 件について分析したものである。以下に結果を纏める。詳細については、(原文の)本文を参照こと。

インシデントの傾向

- 11 ヶ国が計 51 件の深刻なインシデントを報告し、9 ヶ国は 0 件であったと報告している。これは、これらの 9 ヶ国がインシデント報告フレームワークを導入したのが 2011 年末に近かったことが理由と思われ、翌年度(2012 年度)の報告数は、10 倍に増加するのではないかと見られる
- 最もインシデントの発生が多かったのは、携帯電話および携帯電話向けインターネットサービスで(約 60%)
- 最も多くのユーザに影響を及ぼしたのは、携帯電話および携帯電話向けインターネットサービスの障害(約 30 万ユーザ)
- 一次的要因として最も多かったのは、ハード/ソフト障害、第三者に起因する障害(サイバー攻撃は全体の 2%)
- 天災(嵐、洪水など)による障害時間の平均は 45 時間
- 天災(嵐、洪水、豪雪など)は電力供給に大きな影響を及ぼし、しばしば数時間に及ぶ停電につながる
- モバイル通信も固定通信も、電力供給への依存性が大きい。3G 基地局の電源は数時間しか保たないため、停電が長引くことで障害が発生することになる
- モバイル通信の障害要因で最も多かったのはハード/ソフト障害で、その割合は、固定通信より明らかに高い。これは、モバイル通信の方がより複雑なためか、冗長性が乏しいためか、ただ単純に固定通信に比べて利用するハード/ソフトの成熟度や信頼性が低いことなどが考えられる

以下に、分析を通じて見つかった現行制度の課題や、検討が必要な事項を纏める。

改善事項・検討事項

- 絶対値の使用: 報告の基準である「影響を受けた利用者の数」について、絶対値ではなく割合としたことで、報告数が不均衡になった(大きな国では報告が少なく、小さな国では多くなった)。絶対

値を採用し、報告数が国や当局の規模に比例するようにする

- 基準値の見直し： 現行の報告基準には曖昧であったり、ややこしいものがある。各国の対応を合わせるため、基準の数を減らしたり、シンプル化を図る
- 影響を受けるネットワークの細分化： 現行は「携帯電話」等のみの区分だか、より細分化することで、2G の方が 3G より電力供給の停止に強いなどの分析が可能となる
- 報告フォーマット： 殆どの国が、EC が推奨する Article 13a Working Group（ENISA および EU 加盟国の所轄機関（以下、「当局」）が、加盟国における条項 13a の導入について検討するワーキンググループ）のフォーマットを使用したが、別のフォーマットで報告した国もあった。そうしたケースの多くでは重要な情報が欠如していて、全体の分析に使用できなかった。各国で同一のフォーマットを使用する必要がある
- 要因の細分化： 「ハード／ソフト障害」「第三者に起因する障害」などは汎用的であり、ソフトウェア更新の不具合や他社に委託しているネットワークサービスの中断が「第三者に起因する障害」に分類されるように、電源供給の停止が「第三者に起因する障害」に分類されることもある。要因をより細分化することが望ましいと思われる
- インシデントには一定のパターンを持つものが多くある（悪天候→停電（電力供給停止）→障害発生など）。こうした連鎖についても当局の報告に含めてもらうことで、一次的要因をより明確にする助けとなると考えられる
- 条項 13a の目的はインシデントの防止だが、現時点ではインシデントと必要な対策を結びつけることができない。インシデントの報告には、当該インシデントを防げたはずの対策情報も含むべきである。これによって、当局や Article 13A Working Group が再発を防ぐのに何をすべきかより理解できるようになる

Article 13a Working Group では、活動の一環として、特定なタイプのインシデントについて話し合い、そうしたインシデントを防ぐために、当局やプロバイダ向けに技術的ガイダンスの提供が必要かどうかなども検討している。

ENISA では、2013 年春に、2012 年度のインシデントについての報告書を発行する予定である。

以上