2013 年 9 月 19 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(2012 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 2012 – Analysis of the Article 13a incident reports of 2012"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-2012

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 2013 年春に報告した、2012 年度の深刻なインシデント 79 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を参照のこと。

1. 報告基準の変更

過去 2 年間、加盟国はインシデント報告においてテクニカルガイドライン 1.0 を使用していたが、昨年末、ENISA は 2013 年の報告に使用する報告基準およびインシデント報告フォーマットを改訂した。2013 年 1 月より、加盟国はインシデント報告においてテクニカルガイドライン 2.0 を使用している。

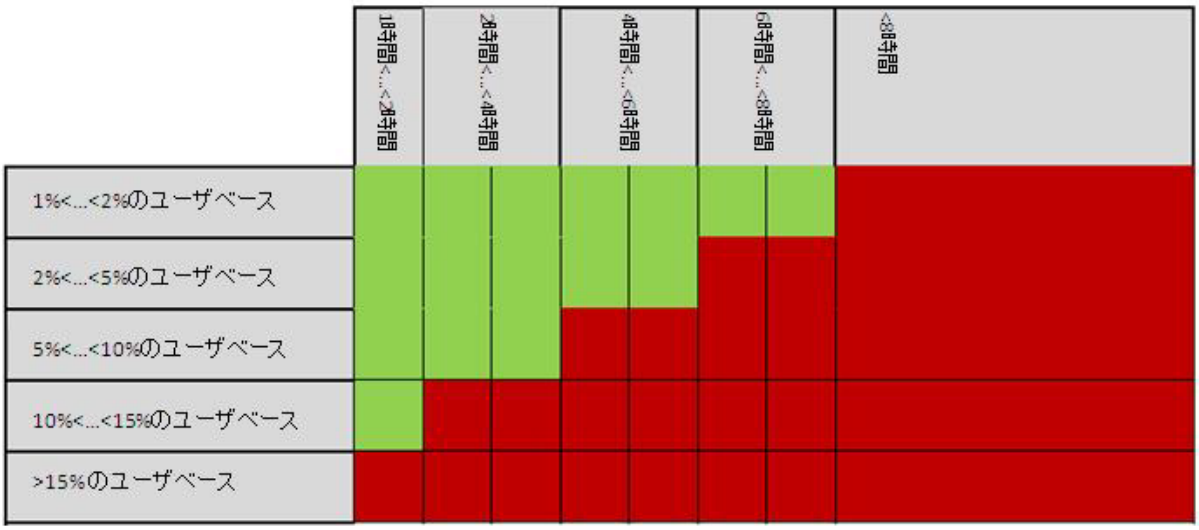
以下に主な変更点を記す。

1-1 報告基準

年次報告は、固定通信サービス(電話、インターネット)およびモバイル通信サービス(電話、インターネット)について、影響を受けたユーザ数(当該サービスの各国の総ユーザ数における割合)およびインシデントの継続時間に基づくものとする。加盟国は以下の状況に該当する場合に報告を行う。

- インシデントが 1 時間以上継続、および影響を受けたユーザの割合が 15%以上の場合
- インシデントが 2 時間以上継続、および影響を受けたユーザの割合が 10%以上の場合
- インシデントが 4 時間以上継続、および影響を受けたユーザの割合が 5%以上の場合
- インシデントが 6 時間以上継続、および影響を受けたユーザの割合が 2%以上の場合
- インシデントが 8 時間以上継続、および影響を受けたユーザの割合が 1%以上の場合

※ 基準に達さなかったインシデントについても、報告することは可能



＜表で見る影響を受けたユーザの割合およびインシデント継続時間の組み合わせを基にした年次報告基準＞

報告基準の変更の詳細については、以下のテクニカルガイドライン 2.0 を参照のこと。

テクニカルガイドライン 2.0
https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

1-2 報告フォーマット

2012 年春、欧州委員会(EC)は 2011 年のインシデントに関して第一回目の年次報告を行うことで EU 加盟国と合意した。合意内容には、ENISA が作成し、条項 13a の Expert Group が承認した報告フォーマットを使用することが含まれていた。当初は、条項 13a のインシデント報告ガイドラインに基づき電子フォーマットが使用されていたが、2012 年秋に、ENISA にてオンラインインシデント報告ツール（CIRAS）を整備し、それまで電子メールで処理していた報告形態を刷新した。

2. インシデントの概要

本報告は、2012 年に発生したインシデントについて纏めている。

- EU 全 28 ヶ国が本プロジェクトに参加。18 ヶ国が合計 79 件の深刻なインシデントを報告し、9 ヶ国は 0 件、1 ヶ国はインシデント報告を行わなかった
- インシデントの影響を最も受けたのは、モバイル通信サービス（携帯、インターネット）であった。また、最も多くのユーザに影響を及ぼしたのも、モバイル通信サービス（携帯、インターネット）のインシデントであった（1 インシデントにつき約 180 万ユーザ）。これは、モバイル通信サービスの高い普及率に一致する傾向
- インシデントの 37%で、112 番（110/119 番のような緊急電話）に影響が発生した
- 一時的要因で最も多かったのはシステム障害で、詳細原因としてはハードウェア／ソフトウェア障害が最も多く、その中ではハードウェアの故障が最多、次がソフトウェアのバグであった

- 第三者に起因するインシデント（多くは停電）では、平均約 280 万の接続（IPA 注：1 人のユーザが複数サービスに接続していることもあるため、接続数でカウント）に影響が出た
- インシデントの継続時間が最も長かったのは、天災（嵐、豪雪等）によるインシデントで、平均約 36 時間だった
- インシデントにより最も影響を受けたのは、スイッチおよび HLR（ホームロケーションレジスタ：ユーザ情報を管理するデータベース）などのネットワーク機器だった

＜2011 年度からの変化＞

- インシデントの一次的要因で最も多かったのは、システム障害（2011 年 47%、2012 年 76%）。悪意ある行為は、2011 年は 6%、2012 年は 8%
- インシデントの平均継続時間では、最長は自然現象（2011 年平均 45 時間、2012 年平均 36 時間）
- 一次的要因毎の影響を受けたユーザ接続の平均数は、最多は第三者に起因する障害（20111 年 364 件、2012 年 2,808 件）。悪意ある行為は、2011 年は 13 件、2012 年は 1,528 件（影響を受けたユーザ接続の数が 2012 年に激増した理由は不詳）
- サービス毎のインシデントの原因の詳細では、サイバー攻撃が、固定インターネットサービス・モバイルインターネットサービスともに 2011 年は 5 件前後。2012 年は、固定インターネットサービスで 20 件、モバイルインターネットで 13 件（IPA 注：グラフ上明確な数値の記載がないため、12 件または 14 件の可能性あり）。固定インターネットサービスでは、サイバー攻撃は 2 番目に高い原因

3. インシデントの事例

報告を受けたインシデントの例を以下に挙げる。

- 一連の分散型サービス妨害（DDoS）攻撃により、プロバイダのドメインネームサービスが標的にされた。このため、最大 250 万人のモバイルインターネットユーザが 1、2 時間に渡り影響を受けた。攻撃者の IP アドレスを突き止めてブロックし、ロードバランサ（負荷分散装置）を再起動して復旧させた後、類似の攻撃に備え、DNS サーバの追加入、ファイアウォールの設定変更、ハードウェアの拡張等の対策を行った
- インターネットプロバイダの元職員が、約 1 万人が利用する固定インターネット回線に使われているスイッチングシステムに放火した。スイッチを交換することで解決したが、復旧に約 36 時間掛かった

Article 13a Working Group では、活動の一環として、特定の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、2014 年夏に、2013 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