2015 年 10 月 30 日
独立行政法人情報処理推進機構（IPA）

ENISA “Cyber Europe 2014” 実施報告書（公開版）概要

本概要は、欧州ネットワーク情報セキュリティ機関（ENISA）発行の“*ENISA CE2014 After Action Report –Public Version*”の概訳となります。内容の詳細につきましては、原文をご確認ください。
URL：
https://www.enisa.europa.eu/media/press-releases/stronger-together-enisa-releases-cyber-europe-2014-after-action-report

Cyber Europe（CE）は、欧州連合（EU）加盟国 28 ヶ国および欧州自由貿易連合（EFTA）加盟国 4 ヶ国の計 32 ヶ国が、欧州全体に影響を及ぼす可能性のある大規模なサイバーインシデントに対し、協調・連携して対応に当たるために行っている演習である。2010 年、2012 年に続き行われた CE 2014 は、2014 年から 2015 年にかけ、3 つのフェーズに分けて実施された。

◆ CE 2014 の目的

1. 各国のサイバーインシデント対応担当機関間における、注意喚起、協力、情報共有のテスト
2. 各国国内における、重要インフラサービスの緊急時対応計画および対応力をテストする機会の提供
3. 官民・民民で発生する、複数かつ並行して行われる情報交換がもたらす影響の検証
4. 重要インフラサービスで発生したサイバーインシデントに対する、技術的、運用的、政治的対応レベルの「エスカレーション（段階的引き上げ）」および「ディエスカレーション（段階的引き下げ）」の検証
5. 大規模なサイバーインシデントに伴う広報対応（public affairs handling）の検証

◆ 3 つのフェーズと参加国／参加者

CE2014 では、危機管理における対応レベルごとの課題により効率的・効果的に取り組むため、演習自体を「フェーズ 1 ： 技術レベル」「フェーズ 2 ： 運用レベル」「フェーズ 3 ： 戦略レベル」の 3 フェーズに分けて行った。

- フェーズ 1 － 技術レベル ： 2014 年 4 月 28 日～30 日（49 時間）
  29 ヶ国から、各国官民 CERT の技術的専門家らが参加。インシデント検知、分析、被害軽減、情報交換を実施
- フェーズ 2 － 運用レベル ： 2014 年 10 月 30 日（10 時間）
  26 カ国から 269 組織、841 人が参加。関係者、機関、国間での共通認識および協力の確立、短期解決策の検討等を実施
- フェーズ 3 － 戦略レベル ： 2015 年 2 月 25 日
  20 ヶ国から 58 人が参加。状況の共通認識に基づく意志決定、長期的解決策に係る政策を議論。なお、戦略レベルでの演習の実施は今回（CE 2014）が初めてとなる

◆ 演習シナリオ

CE2014 は、以下のシナリオに基づき実施された：

ウィンドファームや太陽光発電道路などのグリーンテクノロジーの発展にあてる税源として、EU では加盟国におけるエネルギー資源の輸入に関する規制を提案。反対勢力は真の目的は経済危機の真っ只中にも係らず増税するためだと非難し、規制の影響を受ける国々も自国の発展を妨げようとする地政学的権益操作だと批判。大規模な反対活動にも係らず EU 加盟国による交渉は進み、関連情報の窃取やエネルギー市場の不安定化を狙い、EU 加盟国に対するサイバー攻撃が行われるようになる。

→ フェーズ 1（技術レベル演習）はこの段階を想定

サイバー攻撃をよそに、法案は可決されていく。このため、EU 加盟国を恐怖に陥れ、法案の成立を妨げようとする大規模なサイバー攻撃が続くようになる。ゼロデイ脆弱性を悪用した高度な攻撃が見られるようになり、様々な重要インフラ事業者や多数のオンラインサービスに対して攻撃が行われるようになる。

→ フェーズ 2（運用レベル演習）はこの段階を想定

状況は更に悪化し、厳冬の最中に複数のエネルギー事業者がサイバー攻撃によって深刻な被害を受け、市民の間で不安が高まる。

→ フェーズ 3（戦略レベル演習）はこの段階を想定

◆ 結果・所見

- 欧州における各レベル（技術、運用、戦略）での既存の協力・連携体制を確認・評価する良い機会となった
- 演習では国際レベルで多数の多角的なやり取りが発生し、地域（欧州）レベルでの協力・連携の重要性が改めて浮き彫りになった
- 演習中の状況認識や協力・連携に、EU Standard Operational Procedures（EU-SOP）[1] およびコミュニケーションツールが非常に役に立った。これらの手順やツールに慣れ親しんでおくことで、より迅速な対応が可能になる
- 大多数の参加者が、初めての試みであった戦略レベルの演習を有用と感じた
- 技術レベル演習の参加者の 98%が、次回も参加したいと回答した
- Cyber Exercise Platform（CEP）[2]が、演習の計画や実施、評価に有力なツールであることが確認できた
- CE 2014 のような大規模演習は複雑なプロジェクトであり、計画や準備に長い時間（2 年以上）が掛かるほか、ENISA および加盟国からの貴重な人材（専門家）の寄与が必要となる

[1] EU、FETA、ENISA が協力して策定した、多国間に跨る大規模なサイバー危機への対処にあたっての各国における危機管理計画および手順の策定に関するガイドライン
https://www.enisa.europa.eu/media/press-releases/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa

[2] ENISA が開発した演習プラットフォーム。今後の演習に向けて拡充中

◆ 提言

1. CE だけでなく、実際にサイバー危機が発生した場合のあらゆる EU レベルでの協力・連携は、既存の加盟国間の「関係」の上に成り立つ。ENISA および加盟国は、継続的な信頼の維持・発展に努めること
2. ENISA および加盟国は、現在および将来的な強力・連携の枠組みも考慮に入れ、サイバー危機の際の協力・連携を深める運用手順の発展に努め、国民の保護や航空分野における協力・連携同様の成熟度を目指すこと
3. ENISA および加盟国は、各国の活動および地域（欧州）としての活動の更なる統合を図ること
4. ENISA は、今後の CE について、より有用な経験と影響をもたらすため、トレーニングだけでなく小規模演習・大規模演習を盛り込んだプログラムを計画すること
5. ENISA は、サイバー演習コミュニティの発展を促し、演習計画者および参加者により豊かな経験を提供するほか、各国や地域（欧州）での演習を支援するべく、CEP の拡充を進めること

以上