交通サイバーセキュリティの連携強化に向けて

～総括ディスカッション～

情報セキュリティ大学院大学
サイバーセキュリティ戦略本部員
内閣府 SIP プログラムディレクタ（PD）
後藤　厚宏

本日のご講演

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 名和　利男様：ウクライナ情勢で発生した「重要インフラサービス」へのサイバー攻撃のレビューと得るべき教訓
- 髙杉 典弘様：重要インフラのサイバーセキュリティ対策に係る国土交通省の取り組みについて
- 平永敬一郎様：CASEに向けたサイバーセキュリティの取り組み
- 斉藤 宗一郎様：サイバー攻撃の脅威に備えるために経営層がなすべきこと―セキュリティ体制の構築に向けた取組からの示唆―

いくつかのキーワード

情報セキュリティから
サイバーセキュリティへ

組織全体での対応

KPIからKRIへ

経営者自らが「対策のあり方」を大きく変革

製品の安心・安全確保（PSIRT）

セキュリティはビジネス課題（経営課題）

Q1：事業継続停止による被害の連鎖は？

■ サイバー攻撃によるサプライチェーン寸断による経済活動への悪影響

■ Colonial社の石油パイプライン事案：重要インフラがサイバー攻撃で停止による社会経済全体への負のインパクト

Q2　サイバー防御の「公助」の在り方は？

- 日本の自助・共助・公助
  - 共助：分野横断での「協力・協同」の重要性（⇒ISAC）
  - 公助：重要インフラ14分野にまたがる情報共有や訓練の支援
- 米国 CIRCIA 3月に立法化（CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022）
  - 2022/9月～11月 RFI 具体的な制度策定・制度運用についての意見募集
  - “These reports will allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims.” 「インシデント報告の見返りとして、CISAがサイバー攻撃の被害者（インフラ事業＋利用者）への即時支援」

Q3：ソフトウエアサプライチェーン対策は？

- 米国 2022/9/1 “NSA, CISA, ODNI Release Software Supply Chain Guidance for Developers”
  - ソフトウエア開発者向けのSoftware Supply Chain対策の指南書　⇒　連邦政府Software Supply Chainの危機感
- 欧州 2022/9/8 “Proposal for Cyber Resilience Act”
  - IoT類を含むネットワークに接続される機器類への規制強化

Q4：本日のテーマ

■ 安全保障環境の変化やDXの進展等を踏まえた経営層の役割は？

ご質問・
コメント・
アドバイス
をお願いします

ありがとうございました