SecDogo Digest 第 2 号

2025 年 3 月 7 日 金曜日

特別講演

「サイバーインテリジェンスが事業継続にもたらすもの」というテーマで 軍司 祐介 氏（株式会社マキナレコード 代表取締役）による特別講演が開催されました。

軍司 祐介 氏

講演では主にサイバーインテリジェンスの重要性について述べられました。ネットワークの重要インフラ化に伴う攻撃の増加により、企業に対する攻撃も増加しています。そのため、セキュリティ施策が事業継続に直結します。そレラを踏まえた上で、今までのセキュリティ施策には限界と課題があり、サイバーインテリジェンスが必要であることが語られました。

企業でサイバーインテリジェンスに取り組む専門のチームを作り、セキュリティ戦略の意思決定を支援することで、セキュリティチームの価値を増やすことができると述べられました。

最後に、株式会社マキナレコードが提供するインテリジェンスに関する支援内容が説明されました。インテリジェンスに関して、コンサルティング、トレーニング、サービス導入など支援が可能であるとのことです。

パネルディスカッション

「インシデント対応の現実と理想：ベストプラクティスを求めて」というテーマで以下のパネリ

ストによるパネルディスカッションが開催されました。

コーディネーター

佐藤 公信 氏　（国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所

サイバーセキュリティネクサス 主任研究員）

パネリスト

間下 義暁 氏（国立研究開発法人宇宙航空研究開発機構 JAXA-CSIRT 副 CSIRT 長）

マキロイ 七重 氏（最高検察庁刑事部先端犯罪検察ユニット（JPEC）事務取扱検事）

小川 久仁子 氏（個人情報保護委員会 事務局 審議官）

全体写真

佐藤 公信 氏

間下 義暁 氏

マキロイ 七重 氏

小川 久仁子 氏

本パネルディスカッションでは、インシデント対応を義務化する際のバランスの取り方や、実際のインシデント対応時に望まれること、あるいは避けるべきこと、そして今後のインシデントへの備えについて、被害組織の視点（JAXA）、捜査機関の視点（検察庁）、および個人情報保護の視点（総務省）の三方向から議論されました。

はじめに各パネリストの経歴が紹介され、その後、各組織の立場からインシデント対応に関する具体的な課題や望ましい対応について意見が交わされました。

被害組織の立場から間下義暁氏（JAXA）は、インシデント対応における情報共有の重要性が述べられました。特に、セカンドオピニオンやサードオピニオンの収集、関係機関（警察、内閣サイバーセキュリティセンター(NISC)、IPA、JPCERT、専門家、英国国家犯罪対策庁(NCA)）との積極的な情報共有が対応を迅速かつ的確にする鍵であると述べられました。間下氏は、JAXA が実際に約 9 か月間継続して情報共有を行ったことで、多様な視点から有益な情報が得られ、効果的な対応に繋がったとのことです。一方で、多様な機関から繰り返し同じ説明を求められることが被害組織にとって大きな負担となることから、あらかじめ明確なコミュニケーション体制や相互理解のある信頼関係を構築する必要性も指摘されました。

捜査機関の立場からマキロイ七重氏（最高検察庁）は、迅速かつ正確な証拠収集が重要であり、具体的な対応策として早期の警察への通報、データ保全、時系列表の作成、被害状況の証拠保全などを推奨されました。特に、現場の写真撮影など客観的でわかりやすい証拠の確保が有効であると述べられました。また、インシデント発生時には、証拠品自体を操作しないこと、稼働中の端末の再起動や電源オフ、ウイルス対策ソフトによるフルスキャン、ネットワーク機器の再起動などは証拠価値を著しく損なう可能性があるため非推奨とされました。一方で、復旧を急ぐ必要がある場合もあり、復旧作業と証拠収集のバランスを慎重に取るべきことも説明されました。

さらに、小川久仁子氏（総務省）は、個人情報に関するインシデント対応に伴う法的義務、特に個人情報漏洩の報告義務について解説されました。漏洩事案に対する速やかな速報、確報（60 日以内の報告）が求められますが、現実問題として短期間で完全な報告が難しいこともあります。フォレンジックレポートがあれば個人情報保護委員会が適切に解釈してくれる可能性も示唆されました。

最後に、各パネリストは、関係機関との日頃のコミュニケーションや、インシデント発生時に迅速に対応するための平時からの準備・情報共有の重要性を改めて確認しました。また、捜査機関に提出するためのネットワーク構成図やシステム設計書などの資料を日常的に管理・更新しておくことがインシデント発生時の混乱を防ぐために重要と述べられました。