

## パネルディスカッション

テーマ「あらためて考えるインシデントに備えて我々は何をしないといけないのか?」について、コーディネータ 佐藤公信 氏 (NICT)、パネリスト 今佑輔 氏 (一般社団法人ソフトウェア協会)、萩原健太 氏 (一般社団法人日本シーサート協議会)、竹原一駿 氏 (香川大学) によるパネルディスカッションが開催されました。



(左から) 佐藤公信 氏、萩原健太 氏、今佑輔 氏、竹原一駿 氏

アイスブレイクではインシデント対応を乗り越えるための栄養ドリンクやサプリなど話で盛り上がった。インシデントがおきる現場での問題点は、システムの複雑性による構成図の不在、組織内の責任の所在の不備などである。構成図がないことで初動の遅れや対応に差が出てしまうことが登壇所の経験を交えて説明された。対策としては、構成図の作成や更新、セキュリティ人材の育成、セキュリティポリシーの整備などがある。インシデントを防ぐための基本的考え方は、開けたら閉める (ポート)、使ったら片づける (アカウント)、動かしたら管理する (サービス)、といった、

セキュリティの基本の徹底が大事であり、各地域でセキュリティ人材を育成していくことが大切だとまとめられた。

## 日本シノプシス合同会社 presents 特別講演

テーマ「日本のサイバーセキュリティ政策と自動車、医療機器などの国際的なサイバーセキュリティ規制の社会への影響を考える」について、松岡正人氏（日本シノプシス合同会社）による特別講演が開催されました。



松岡正人 氏

アプリケーションセキュリティの重要性について議論された。安全な製品の重要性、脆弱性による攻撃の危険性、サイバーインシデントがビジネスリスクのトップに位置することなどが説明された。高品質なソフトウェア開発の重要性が強調され、セキュリティ対策とソフトウェアサプライチェーンリスク管理についても言及された。さらに、あらゆるデジタル製品にサイバーセキュリティ対策を義務付ける欧州連合（EU）の「欧州サイバーレジリエンス法（EU Cyber Resilience Act : CRA）」を通じてアプリケーションセキュリティ対策のアプローチが提案された。セキュアな開発の実践、開発環境のセキュリティ対策、脆弱性管理、SBOM 管理の重要性について語られた。