SecDogo Digest

第 3 号

2025 年 3 月 7 日　金曜日

意見交換会

意見交換会が愛媛大学生協食堂で開催されました。愛媛県庁から菅副知事にご来賓のご挨拶を頂き、四国総合通信局の中澤局長にご挨拶を頂きました。

中澤局長

菅副知事

会場

テーマ１

「サイバーセキュリティお助け隊セッション」というテーマで、以下のパネリストによるナイトセッションが開催されました。

パネリスト

我満　英樹　氏（セントラル警備保障株式会社）

佐藤　栄城　氏（独立行政法人情報処理推進機構(IPA)セキュリティセンター）

関原　優　氏（三井物産セキュアディレクション株式会社）

野田　幹希　氏（大阪商工会議所　経営情報センター）

藤田　優　氏（ラディックス株式会社）

本セッションのテーマである「サイバーセキュリティお助け隊サービス」は、中小企業がサイバー攻撃の脅威から身を守るために設計された包括的なセキュリティ支援サービスです。2021 年度に正式にブランド化され、現在 35 の事業者が提供しており、専門知識がなくても導入・運用できる仕組みが整えられています。

コーディネーターの 森井 昌克 氏が進行を務め、まず独立行政法人情報処理推進機構（以下、IPA）の 佐藤 栄城 氏は、サイバーセキュリティに関して人材や予算が限られている中小企業を支援するため、「見守り・駆付け・保険」の仕組みが重要であると述べられました。24 時間 365 日の監視体制が導入されており、年々導入件数が増加して 24 年度においては約 9,000 件の導入実績があり、医療や自動車業界を含む様々な分野で活用されています。

続いて、我満 英樹 氏が、中小企業向けに低価格で SOC（セキュリティオペレーションセンター）監視を提供する取り組みについて紹介されました。警備会社のパトロール員による駆け付けやコールセンター「サイバーガード」との連携を特徴としています。フィジカルセキュリティと IT セキュリティの統合により、大手 IT 企業では対応しきれない領域をカバーしている点が強調されました。また、少子高齢化による将来的な警備会社の在り方についても言及されました。さらに、中小企業向けのサイバー対策は IT 導入補助金を活用するケースが多いものの、ネットワーク構成図を持っていない企業も多いことが課題です。

関原 優 氏は、「お助け隊」の認知度の低さや紹介の機会の不足、費用面の課題について言及されました。特に、地域セキュリティとの連携による顧客の発掘や、PR 宣伝の強化が必要であると指摘されました。小規模企業でも導入しやすくするための補助金制度の改善や、サービス導入による付加価値の創出が求められます。

藤田 優 氏は、「お助け隊」サービスを活用した IT 導入補助金の申請支援について説明されまし

た。補助金のターゲットはベンチャー企業や中小企業であり、採択率の高さが特徴です。また、申請企業側の課題として、担当者の突然の退職によるアカウント情報の管理不足や、建築業の企業が法務・税務手続きの時間を確保できない点が挙げられました。また、申請手続きが煩雑であることも問題視されました。

野田 幹希 氏は、NEC と連携した取り組みを紹介されました。中小企業は、規模や知識の有無にかかわらず、セキュリティ対策が不可欠です。しかし、現在の市場は未成熟であり、事業自体では赤字になっています。

また、セキュリティ対策の導入促進のため、IPA によるセミナー開催支援や講演者の派遣が求められます。中小企業の多くはセキュリティをコストと捉えてしまい、積極的に導入する意識が低いため、DX と組み合わせて推進することが有効です。価格設定に関して、最低売価が限界に近く、販売側の利益が少ないため、積極的に販売しにくい現状が指摘されました。

コミュニティの活用によるセキュリティ人材の育成や、ビジネスが持続的に回る仕組みの構築が重要です。「お助け隊」は現状バランスが取れておらず課題があります。特に、サプライチェーンの中小企業をどのように守るかが重要なテーマとして挙げられました。

テーマ２

「やってる？脅威インテリジェンスを用いたサイバー攻撃対策」というテーマで以下の座長によるナイトセッションが開催されました。

座長

北條孝佳氏（西村あさひ法律事務所・外国法共同事業　パートナー弁護士）

鳥越真理子氏（楽天フィンテック CSIRT・Senior Cyber Threat Hunter）

本セッションはアンケート調査やクイズを交えながら進行されました。参加者へのアンケート結果から、脅威インテリジェンス（CTI）の必要性は認識されつつも、「未実施・未検討」と回答する割合が多く、CTI 活用が十分に浸透していない現状が確認されました。

CTI を活用する意義として、脅威の検知、迅速なインシデント対応、コミュニティ全体のセキュリティレベル向上があります。CTI 活用の基本的プロセスは、「計画・定義」「収集」「処理・翻訳」「分析・評価」「配布・フィードバック」を繰り返す循環型プロセスであることが述べられていました。

金融庁の「サイバーセキュリティガイドライン」に基づいた具体的な活用事例として、脆弱性管理、脅威ハンティング、フィッシング対策などが紹介されました。アンケートやクイズを用いた参加者との双方向的なやりとりを通じて、脆弱性情報や攻撃者情報、被害情報の総合的検討の重要性やシステム構成情報を活用した効率的な対応方法が示され、会場との活発な意見交換が行われました。

テーマ３

「サイバーセキュリティ業界の未来と果たすべき役割」というテーマで以下の座長によるナイトセッションが開催されました。

座長

鵜飼裕司氏（株式会社　FFRI セキュリティ）

森達哉氏（早稲田大学理工学術院・教授）

このセッションでは、サイバー安全保障や産業、研究等について、そのあるべき姿を民間企業、学校関係者等様々な視点をもつ観客で議論が行われました。

セッション冒頭で、座長から２つの話題が提示されました。森氏からは、「人材育成、産学連携、海外大学の状況」についての説明がされました。海外と比較すると、トップカンファレンスでの採択が微増に留まっている国内の R&D の現状について述べられました。そして、官民学が連携し、行き来しやすくすることが日本にとって有効なアプローチではないかと述べられました。鵜飼氏からは、「民間のサイバーセキュリティベンダーの現状と産業界の課題」についての説明がされました。北米と比較するとグローバル展開に弱いという国内のサイバーセキュリティ産業の現状・課題について述べられました。これらの話題について、会場からは積極的に意見があり、活発に議論されていました。

テーマ４

「サイバー攻撃のリアル?現実のインシデントでどう対応したのか／せざるを得なかったのか」というテーマで以下の座長によるナイトセッションが開催されました。

座長

北尾辰也氏（日本シーサート協議会専門委員／国土交通省最高情報セキュリティアドバイザー）

SecDogo Digest, サイバーセキュリティシンポジウム道後 2025

ランサムウェア攻撃において、リークサイトでは盗まれた情報が公開されることがあり、一度漏洩した個人情報を取り戻すことは現実的に不可能です。このような現状を踏まえ、攻撃発生時にはシステムの封じ込めを行い、侵入経路を特定、影響範囲の特定と回復といった対策を取ることで、被害が広がることを最小限にして、重要なところは守り、事業継続を最優先に考えることが行われます。

封じ込めの事例がいくつか紹介され、意思決定や封じこめが早ければ被害が軽減されることが説明されました。会場の参加者からは、封じ込めに上手くいったケース、対応において実際に起こったエピソード、などが紹介されました。

侵入経路の特定では、現実のシステムでは侵入経路の候補が多く調査に時間がかかってしまうため、ログの取得・保全が基本であるということが説明されました。一方で、ログが取れていないこともあり、特定できず推測に終わります。事例では、特定が分かりやすかったケース、ネットワークの見直しを行った例が紹介されました。

影響範囲の特定とクリーンナップ・回復では、システムや機器の「正常性」の証明が難しく時間がかかります。影響範囲の特定を迅速に行うには、影響範囲の特定のノウハウを訓練・蓄積すること、ファストフォレンジックツールの活用が考えられると説明されました。

現実のインシデントは教科書通りにはいかないという言葉やログの重要性が印象に残りました。会場は満席で立ち見の方もおられ、参加者が発言する機会や質疑応答の時間が多くあり、双方向の議論が活発に行われました。