# サイバー事故対応の最新知識習得

## 「サイバー保険 事故発生から収束まで」テーマにセミナー

東京代協

東京代協は9月12日、「サイバー保険　事故発生から収束まで」をテーマにセミナーを開催した。顧客にサイバー事故のリスクを伝えられるように、サイバー事故対応の最新の知識を習得しようというもの。大手企業や行政機関にサイバーセキュリティサービスを提供する株式会社ラックの谷川賞二郎氏と、内山鑑定事務所サイバー鑑定チームの平野翔士氏が講師となり、サイバー事故発生から収束までの具体例、事故の賠償や費用といった損害について解説した。損保会館（東京都千代田区）とオンラインのハイブリッドで行われ、多くの関係者が聴講した。

### 重要なエビデンス収集
### 必要資料・記録保持の共通認識を

IPA（独立行政法人情報処理推進機構）の「情報セキュリティ10大脅威2023」によると、「ランサムウエアによる被害」「サプライチェーンの弱点を悪用した攻撃」が組織の2大脅威であることが分かった。しかし、「重要な情報は持っていない」等の認識や費用等の面から、十分な対策を講じていない中小企業が見受けられる。サイバーリスクは大企業だけでなく中小企業も多く標的となっており、決して他人事ではない。


谷川氏

第1部では谷川氏が事故発生時に行われるフォレンジック調査・分析と一連の対応、身代金要求型といわれるランサムウエアの被害実態等を自社のサービスや知見とともに解説した。

フォレンジック調査は、侵入原因の痕跡調査・侵害による影響調査・被害範囲の痕跡調査・情報漏洩の痕跡調査を実施するもの。谷川氏は、「ログがないとフォレンジック調査はできない」として、保険代理店が顧客にサイバー保険の説明する上で覚えておいてほしい初動保全対応を説明。まず、ログの消失を防ぐために対象端末の電源を落とさない（再起動させない）こと。ただし、ランサムウエアに感染した場合は、操作が不能になるため早急に電源を落とす必要があるという。また、他の端末やネットワークから隔離するためにLANケーブルの抜線・無線LANからの切断・Wi Fiの切断、メモリー上のイメージコピーやHDD上のログ保全、フォレンジック調査会社への連絡を挙げ、ログが変わってしまうためワイルススキャンを控えることも注意喚起した。

同氏は、同社サービスとして提供している「サイバー119」の出動件数や出動事由等を紹介し、コロナ禍で普及したテレワーク環境におけるVPN機器経由でのサイバー攻撃被害も増加していると指摘。実例を挙げながら、ランサムウエアの攻撃手口や通常のバックアップとランサムウエア対策のバックアップの違い等を解説した。

最後にランサムウエア対策として、身代金は絶対に払わないこと、感染しても復元する仕組みを構築しておくことが重要だと強調。予防策として、怪しいファイルやメールを開かない等のセキュリティリテラシー向上で被害拡大を防止できること、システム・運用面においては未知のマルウエアも検知できる対策ソフトの導入やバックアップの仕組みの構築、OSやアプリの最新バージョンアップ等のほか、事後対応の観点からサイバー保険加入は重要だと訴えた。


平野氏

第2部では平野氏がサイバー保険の事故対応の概観、初動対応のポイントを解説した。サイバー保険の補償対象となる一般的な事故として、①他人の情報漏洩またはその恐れ②ITユーザー業務に起因する他人の損失等の発生③被保険者のコンピューターシステムに対するサイバー攻撃④サイバー攻撃の恐れ―が挙げられる。サイバー事故は物損事故のように視認できないため、事故の情報、事故・被害発生の裏付けや事故対応内容の詳細・費用の支出の証明（見積書、請求書、支払帳票等）、内容や範囲の妥当性、金額の妥当性といった資料が有責判断・損害認定の際に必要だ。このためにも適切な情報収集、事故の発生事実や損害の立証といったエビデンスの収集がポイントとなってくる。平野氏はこれらの点を踏まえ、攻撃対象とされるコンピューターシステムの範囲や管理体制、インシデント対応時の関係者相関図を示しながら、具体的な対応の流れを説明した。

サイバー保険は火災や新種事案と基本的には同じだが、インシデント対応と並行して保険対応を求められることが多く、費用を保険で賄うことが前提となっているため対応の着手前に保険の認定可否・認定金額等の回答を求められることが多いという。こうしたことから保険代理店は、被保険者から事故疑いの一報があった際には、なりすましメール等の不審なメールや被保険者のネットワークにあるマルウエア検知記録や端末管理台帳といった全体のネットワーク構成のほか、保険金支払対象であればベンダーの提案書、委託契約書、見積書や補足資料等を用意するようアドバイスすることが必要だと指摘した。また同氏は、有責判断や損害認定に必要な資料を一覧で紹介し、「必要資料は多いが、初動対応時に保険金請求に必要な資料や記録保持の共通認識を持つことで、その後の保険対応がスムーズになる」と語り、初動対応の重要性と円滑なコミュニケーションの必要性を呼びかけた。

新日本保険新聞
（損保版）
第１～４月曜日発行
発行所　新日本保険新聞社
大阪市西区靱本町１丁目５－15
（郵便番号550-0004）
電話　(06) 6225－0550（代表）
FAX　(06) 6225－0551（専用）
購読料　１か月2420円
（消費税、送料込み）