経済安全保障・サイバー攻撃対策セミナー

官民一体で危機意識を共有

日本の企業や研究機関にとって、技術情報流出やサイバー攻撃は、もはや「対岸の火事」ではない。諸外国からターゲットにされ、組織の規模や合法・非合法を問わず狙われるリスクがある。早期の対策が急務となる中、日刊工業新聞社とモノづくり日本会議は1月22日、警視庁の協力を得て「経済安全保障・サイバー攻撃対策セミナー」を開いた。技術情報流出の実態や具体的な防衛策を紹介し、官民一体で危機意識を共有。対策の早期普及と組織内への浸透の重要性をあらためて浮き彫りにした。

「経済安全保障・サイバー攻撃対策セミナー」は、リアルとオンラインのハイブリッドで実施。大企業、中小企業関係者ら約50人が参加し、講師の言葉に熱心に耳を傾けた。昨今の相次ぐ情報流出事件も踏まえ、〝自分事〟と捉えている様子が見て取れた。

警視庁久松警察署署長の林勝彦警視があいさつし、「安全保障の思想が経済・技術分野にも広がっている今、流出した技術情報により、企業の競争力が失われるだけでなく、他国での軍事転用により、日本の安全保障上のリスクにもなる」と警鐘を鳴らした。

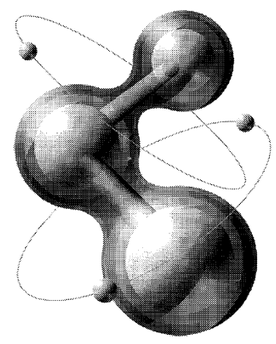
その後、「技術流出の現状と対策―リスクマネジメント」をテーマに、経済安全保障に関する警視庁プロジェクトチーム管理官の那須周警視が登壇。

また「サイバー攻撃の情勢と対策」と題して警視庁サイバー攻撃対策センター副所長の後藤太作警視、「特殊詐欺の現状と対策」と題して警視庁匿名・流動型犯罪グループ対策本部防犯対策担当管理官の佐藤孝重警視が講演した。

警察庁の東京都警察情報通信部による「標的型メール攻撃の実演」もあり、その巧妙な手口に肝を冷やし、聴講者もあらためて警戒を強めたようだ。

同セミナーは、背景にAI（人工知能）や量子技術といった革新的技術の台頭をはじめ、宇宙・サイバー領域の安全保障上の重要性が増している状況がある。中堅・中小企業も含めたすべての組織が情報流出のリスクに直面する中、具体的な手口を把握し、官民一体で防御力を高める重要性を再確認する場となった。


企業も含む全ての組織が情報流出のリスクに直面している（イメージ）


モノづくり日本会議
超モノづくりへの挑戦

技術流出の現状と対策～リスクマネジメント

トレーサビリティー確保を

経済安全保障に関するプロジェクトチーム管理官
那須 周 警視

「ドベネックの桶」という言葉がある。長さの違う板で作った桶に満ちた水が板の短い部分から流れ出ることに転じて、情報も対策レベルが低い部分から流出する。どれほど高い板が後ろ側にあっても、弱い箇所から漏れ出てしまう。サイバー攻撃は件数こそ少ないが、起きた際のハレーションが大きい。2025年に攻撃を受けた国内企業もあり、完全復旧に時間を要した。

経済安全保障上、「懸念国」と呼ばれる国がある。例えばA国は西側諸国に破壊工作や情報窃取、影響工作などをしている。B国は金銭獲得、情報窃取が目的の暗号資産関係のアクセスなどが特徴だ。C国は台湾、米国、日本などの軍事企業、先端技術関連企業、政府関連組織に、経済安全保障上の情報内容の窃取を行っている。国への警戒は必要だが、従業員やスタッフにも多様な国の人がいる。共に働く仲間という点で差別的な行いをしないように求める。

図利加害目的で営業秘密を不正に取得・使用・開示する行為は、不正競争防止法違反に該当する。営業秘密とは秘密管理性、有用性と非公知性が三つ重なったものだけが認められる。有用性とは文字通り使える情報。非公知性は公開されていない情報。秘密管理性とは、アクセス権の制限や、施錠できる同じ場所への保管など、秘密として管理をしていると外形上わかるようにすることだ。これにより不正競争防止法の保護が得られ、裁判で有利に働く。

ポイントはモノの製造から販売まで管理する「トレーサビリティー」の確保、トレーサビリティーの意思と能力があることの組織内への周知、関係者への研修を通じた指導・教養、定期的あるいは随時行う監査、関係機関との連携だ。狙われる可能性に対して適度の憂い、心配をすることが重要になる。

サイバー攻撃の情勢と対策

適切な管理と対応訓練が重要

サイバー攻撃対策センター副所長
後藤 太作 警視

警察庁が検知するサイバー空間の不審なアクセスは、2017年は1日当たり約1890件だったが、24年には1日当たり約9520件と増加している。不審なアクセスとは、端末のIPアドレスや、サービスを行うポートとそのポートに対する脆弱性の有無の確認等、攻撃の準備と考えられる。約9520件のうち約99%が海外からのアクセスで、その攻撃への対策も情報流出防止のためには重要だ。

サイバー攻撃には社会機能を麻痺させる「サイバーテロ」やサイバー空間における諜報活動の「サイバーエスピオナージ（サイバーインテリジェンス）」があり、特に問題なのは「APT攻撃」だ。「Advanced Persistent Threat」の略で、「高度で執拗な脅威」を意味する。国家を背景に攻撃するグループが存在し、入念な調査と準備をして持続的かつ高度なサイバー攻撃を行い、情報窃取や各種システムの機能停止等を企てる。

対策として、ランサムウエアにはネットワーク機器等へのパッチ等の適用、アクセス制限、認証情報の適切な管理等がある。ネットワークの監視や電子メール等に対する警戒、データ等のバックアップ取得も有効だ。

機密情報を狙う標的型メール攻撃には従業員の意識を高めることが重要だ。不審メールへの注意力の向上や手口の周知に加えて、システム管理者への連絡等の対応が取れるようにするための訓練や研修も望ましい。

サイバー空間の安全と安心に向けて、皆さまから受け取る被害情報も、日本全体のサイバーセキュリティーを確保するためには重要だ。被害に遭ったと思料される場合は警察署に相談してもらいたい。サイバー攻撃対策センターが「X（旧ツイッター）」で発信するサイバー攻撃対策に関する情報も活用してほしい。

特殊詐欺の現状と対策

周囲の気づきが防止の一助に

匿名・流動型犯罪グループ対策本部防犯対策担当管理官
佐藤 孝重 警視

2024年度の特殊詐欺と投資ロマンス詐欺を合わせた被害額は約2000億を超え、過去最悪の被害額となった。25年度も被害は深刻化している。この潤沢な犯罪収益資金を使い、犯行グループはさらに人手を集めて規模を拡大している。

電話を利用して金をだまし取る特殊詐欺の犯行グループは、闇雲に電話をかけているパターンと、何らかの名簿に沿って電話をかけているパターンがある。

匿名・流動型犯罪グループ対策本部では、ウェブサイトで特殊詐欺の手口と対策を紹介している。手口としては、警察を名乗る者が電話越しに「あなたに逮捕状が出ている」などと脅しをかけ、被害者の金を騙し取るなどのケースがある。

犯行グループの電話は約8割が国際電話番号を利用している。「＋」から始まる電話番号で、続く2桁の数字は国番号だが、どの国に偏っているというわけではない。国際電話の番号には注意が必要だ。警視庁は、該当の電話を自動でシャットアウトするアプリを作った。

特殊詐欺の電話は、大半が昼間の、従業員が働いている場で携帯電話にかかってくる。偽警察官は相手を1人にするため、使用されていない会議室や個室、会社付近のカラオケボックスなどにも誘導をしてくる。同僚や部下が電話をしながら時間休を求めたり、会議室にこもろうとしている状況にあったら、一声かけてほしい。周囲から見れば詐欺と分かるが、本人は通話から騙され始めており、言われるがままになって気づくことが難しい。

警察が金の振り込みを求めることや、スマートフォンを使って逮捕状を見せて「あなたを逮捕する」などと電話することはあり得ない。周りが気づいてあげることが防止につながる。企業が一丸となって、1人でも被害に遭わないようにしてもらいたい。

開会あいさつ

警視庁久松警察署署長
林 勝彦 警視

スパイ工作への備え 「See」「Stop」「Share」

近年、地政学上のリスクがクローズアップされ、国際的な産業競争も激化し、日本企業の高度な技術情報が外国にも狙われている。従業員の転職時の情報の持ち出しや、取引先による漏洩など、国内だけでなく、外国との間でも起こりうるリスクとなっている。サイバー攻撃やスパイ工作により情報が盗まれ、国外に流出するリスクも顕在化しているほか、通常の経済活動でも技術情報が狙われる場面がある。スパイ工作への備えとして〝三つのS〟を紹介する。

まず一つ目は「See」、相手をよく見ること。普段のビジネスシーンと異なる場面で会った相手は、所属や連絡先などの情報をよく確認してほしい。二つ目は「Stop」、立ち止まって考えること。不特定多数の目に触れる場所に個人情報を記載する際は、立ち止まって慎重になる必要がある。三つ目は「Share」、共有する、相談することだ。さきいなことでも上司や同僚に共有、相談することが大切だ。見知らぬ人からの接触や不審な働きかけがあった場合、相談することで冷静になり、共有することで周りの人が標的になることも防止できる。不審に思うことがあれば、ぜひ警察に相談してほしい。