サイバーリスクの脅威などテーマに

大阪代協　2018年大阪代協オープンセミナーを開催


参加者で満席となったセミナー会場

大阪代協（山中尚会長）は、8月24日14時から、大阪市中央区の大阪損保会館で「サイバーリスクの脅威とソリューションの提供」をテーマに2018年大阪代協オープンセミナーを開催した。セミナーでは、サイバーリスクとその被害の実情とともに、これに対してどのようにセキュリティ対策を講じていくかが紹介され、会員をはじめとする参加者161名が熱心に耳を傾けた。

約4割の法人が重大被害
中小企業の平均損害額1億円超


山中会長

セミナーの開催に先立ち、山中会長が「大阪代協は、保険代理店の持続的な発展を実現させたい、という強い想いを抱き、保険業界の発展そして広く社会に貢献したいと考えている。オープンセミナーはその一環として定期的に実施している活動の一つである。今回は『サイバーリスク』をテーマとしたが、これにはサイバーリスクの実態を知ること、そして新しいリスクへの対応という二つの目的がある。自動車保険はいずれ縮小することが避けられない。世の中の動きや出来事を敏感に察知し、新たなリスクを認識するとともに、その対策をお客様に提案できるようにならなければならない。本セミナーを有意義な時間としていただきたい」と挨拶した。

セミナーの第1部PART1では、トレンドマイクロ㈱業種営業推進グループ金融担当シニアマネージャーの今泉智氏が「企業を無差別に襲うサイバーリスクの実情」をテーマに講演を行った。

同氏は、国内でのサイバー攻撃被害は極めて深刻な状況にあり、約4割の法人組織がセキュリティインシデントによる重大な被害を経験していると報告。その被害額は年間平均2億3177万円、中小企業の被害額も平均1億円を超えているとし、最近は中小企業が狙われる傾向にあると指摘した。同社が2017年に行った集計では、98%の法人組織で広く一般を狙う攻撃のセキュリティリスクを確認し、71%で標的型サイバー攻撃の疑いがあったとし、とくに遠隔操作ツールを利用したRATによる活動は26%に及んでいると説明した。

また、最近は新しいサイバー攻撃が次々と登場し、とりわけ感染したパソコンを強制的にロック（端末ロック型）したり、パソコン内のファイルを暗号化（暗号化型）したりした上で、元に戻すことと引き換えに身代金を要求する不正プログラム『ランサムウェア』は脅威であると説明。2018年に入って攻撃総数は減っているものの、小規模な攻撃にシフトしており、万一攻撃を感染した場合には「お金を支払っても暗号が解かれないケースもあり、決して相手の要求に従ってはならない」と強調した。

その他、所有者の知らないところで仮想通貨発掘（マイニング）が行われるコインマイナーや高額の金銭を法人からだまし取るビジネスメール（BEC）、2018年第1四半期で137万件強と過去最大規模に増加しているフィッシング詐欺、不正アプリや不正サイト、配達業者の通知を偽装した詐欺サイトを活用したスマートフォンを狙ったサイバー攻撃など、手口が巧妙化していると述べた。

こうしたサイバー攻撃に対して、同氏は、まずランサムウェアやコインマイナー、ビジネスメール詐欺対策として、①使っているソフトは常に最新の状態にする、②差出人に見覚えがない、添付ファイル等に矛盾がある不審メールに注意する、③アドレスバーに表示されているURLが正しいか注意する、④不審な兆候が現れたらすぐにシステムサポートデスクに連絡することとし、また、スマートフォンを狙うサイバー脅威の対策として、①Androidやiosを最新バージョンにアップデートする、②公式アプリストア等のみ利用する、③攻撃の手口を知り、サイトのURLをチェックするなどの注意を心がけることだと紹介した。

常にサイバー攻撃があることを念頭に事前対策を!!

そして、いったんサイバー攻撃の被害を受けると、その調査や復旧・再発防止の対応に高額な費用がかかるといった経済的な損害、精神的な苦痛を受けるだけでなく、その間の業務縮小を余儀なくされること、お客様や取引先からの信用失墜・離反といった影響は計り知れないと述べた。

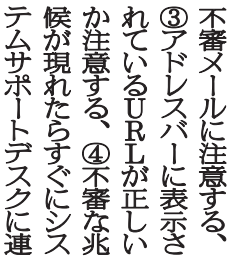
こうした被害に遭いにくくするためには、①便利と危険は背中合わせであり、使用しているパソコン等の機能・状態と合わせ、どこにどんな脅威があるかを把握しておくリスク感性を磨いておく（己を知る）、②常にサイバー攻撃に遭っている認識を持ってサイバー攻撃の特徴や保険のカバー範囲を知っておく（相手を知る）、③技術（セキュリティ対策機器などの仕組みの導入）・プロセス（役員を含めた社内態勢の整備）・人（定期的な訓練・教育の実施）といった仕組みを整え守ることが重要だとし、一度自社での取組みを確認してほしいと訴えた。

セキュリティに限界　サイバー保険で対応

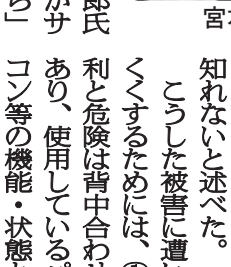
第2部では、大阪代協副会長の佐野誠美氏がコーディネーター、第1部で講師を務めた今泉氏、宮本氏に加え、損保ジャパン日本興亜コマーシャルビジネス業務部関西グループのグループリーダーである池田明浩氏、三井住友海上新種保険部関西新種保険チームのチーム長である奥村洋氏がパネラーとなり、パネルディスカッション「サイバーリスクに対する防衛策とお客様に提供できるソリューション」が行われた。

サイバー攻撃の対策として、「情報セキュリティの3大要素である『機密性』『完全性』『可用性』を高めると同時に、技、組織・ルール、人の3つの仕組みで守ること。とくに教育が重要」（宮本氏）、「常にサイバー攻撃下にあることを念頭に置き、代理店はトップダウンで取り組むこと」（池田氏）、「サイバー攻撃による事故は常に発生していることを前提に、事前対策をしておくこと」（奥村氏）、「ウイルス感染した者が悪者扱いにされる雰囲気では、それが対応の遅れの原因になる。すぐに報告できる態勢を整えておくこと。そして、セキュリティ知識を高めておくこと。さらに、セキュリティウェアには限界があるのでサイバー保険に加入しておくこと」（今泉氏）といった意見が出された。

また、個人情報漏えい保険より補償範囲が拡大された各社のサイバー保険の特徴や留意点、付帯サービスなどが紹介される中で、サイバーセキュリティ事故対応費用に関する補償限度額が1億円程度と高額に設定されている背景について、「不正アクセス等の確定後、原因調査に関する費用はパソコン1台当たり150万円程度かかる。これが複数台になることや、さらにサーバー等まで範囲が広がるとその費用は相当なものになる。それほどにサイバーセキュリティ事故ではお金がかかる」とその損失の大きさが紹介された。


池田氏


宮本氏


奥村氏


佐野氏

フィッシング詐欺は過去最大規模に


今泉氏

被害者が加害者になることも
経済的な損失、信用失墜に

続いて行われたセミナーPart2では、東京海上日動IT企画部・リスク管理グループグループリーダーの宮本寿郎氏が「もし保険代理店がサイバー攻撃を受けたら」と題し講演を行った。

同氏は、サイバー攻撃に遭うキッカケとして、①迷惑メールやWebサイトの改ざん・侵入といった外部からの攻撃、②悪意あるWebサイトへのアクセスやビジネスeメール詐欺、退職者ID利用といった内部の不適切な行為、③委託先がサイバー攻撃に遭うといった委託先でのリスクを挙げ、これによって端末がマルウェアに感染し情報の漏えいや詐取につながると説明。また、その一方で、感染したマルウェアに気づかずにお客様や取引先に拡散するといった、加害者となる可能性を秘めていると警告した。