地域におけるサイバーセキュリティ向上の取り組みと地方シンクタンクの役割
～KIIS サイバーセキュリティ研究会の活動から～

一般財団法人関西情報センター　主席研究員　石橋 裕基

1. はじめに（現状認識）

1.1.　サイバーセキュリティを取り巻く全般的な動向

標的型攻撃やランサムウェア、それにビジネスメール詐欺など、サイバーセキュリティは今や企業のビジネスに直結する大きなリスクとなっている。業務の妨害や機密情報の窃取、金銭の獲得などを狙った各種の攻撃はますます巧妙化している。

また昨今では、企業の取引関係や製品に内蔵された部品に潜む脅威、いわゆるサプライチェーンリスクも顕在化している。大阪商工会議所（2019）による調査では、大企業との取引を行っている中小企業 118 社のうち、30 社において何らかの攻撃を受けたことがあると回答している[1]。大企業においては相当程度のセキュリティ対策が講じられていたとしても、関連会社やビジネス上の取引を行っている企業には中小規模のところも少なくない。リソースが相対的に少ない中小企業においては、そもそも「自らがサイバー攻撃の対象になる」と想定していないところや、セキュリティへの不安を感じていたとしても「何から手を付けていいのかがわからない」と考える企業も多く、対策が後手に回っているケースも散見される。

加えて、昨今のコロナ禍においては、接触を避けるために急遽テレワーク等の導入に踏み切った、あるいはテレワークの範囲を大幅に拡大した企業等も多い。機器やシステムの整備を急ぐあまり、対策を講じておくべき脆弱性が放置され、それをきっかけに重要なネットワーク接続情報が窃取され闇市場に公開されるという事案も発生した[2]。非接触・オンライン化の流れは今後スタンダードになっていくと想定されることから、これまで以上にセキュリティ対策を強化していく必要がある。

1.2.　地域におけるセキュリティ人材の不足

こういったセキュリティ対策を具体的に講じるのは、最終的には「人」である。IoT や AI 等の第四次産業革命関連技術の登場により、サイバーセキュリティに対するニーズが今後ますます増大する一方で、経済産業省（2016）では、2020 年時点では全国で 19.3 万人のセキュリティ人材が不足するとの試算を示した[3]。サイバーセキュリティを担う人材の発掘・育成にいかに取り組むかが我が国全体の喫緊の課題となっているが、大企業の本社機能や

---

[1] 「サプライチェーンにおける取引先のサイバーセキュリティー対策等に関する調査結果」（大阪商工会議所、2019.5.10）。

[2] 「VPN、突かれた欠陥　サイバー攻撃、900 組織の接続情報流出」（朝日新聞、2020.8.26 付）等。

[3] 「IT 人材の最新動向と将来推計に関する調査結果」（経済産業省、2016.6.10）。

IT 系企業が首都圏に集積していることを考えると、このセキュリティ人材の不足はとりわけ「地方」において深刻であると言える。たとえ地方の中小企業であっても、重要な産業のサプライチェーンに組み込まれていることが多く、これらの企業におけるセキュリティ対策の弱さが、我が国全体の社会経済における脆弱性につながる恐れがある。いわゆる「桶の理論」、あるいは「the strength of a chain is in the weakest link（鎖の強度は最も弱い環で決まる）」ということわざ等に示される状況である。今後のセキュリティ人材確保に向けた取り組みは、とりわけ首都圏以外の地方、中小企業等において重点的に推進される必要がある。

図 1. 情報セキュリティ人材の不足数推計
経済産業省「IT 人材の最新動向と将来推計に関する調査結果」（2016.6.10）より抜粋

また、首都圏以外の地域では、サイバーセキュリティに関する最新情報に触れる機会も絶対的に少ないのが現状である。セキュリティをテーマとした展示会やシンポジウム等は首都圏・大都市圏を中心に展開されることが多く、地方の企業にとっては様々な情報を得るために、さらなる追加コストが必要となっている。サイバーセキュリティを取り巻く技術は日進月歩であり、様々な攻撃や犯罪の手口などが日々生み出されている。セキュリティ担当者が適切な取り組みを進める上では最新のサイバーセキュリティ情報が欠かせないが、地方においては、そもそもセキュリティ対策に取り組む人材の絶対数が少ないことに加え、それらの担当者が的確な対応を取るために必要な情報を得るためのハードルも高いと言わざるを得ない。

1.3. セキュリティコミュニティの重要性

一般に、企業におけるセキュリティ担当者は「孤軍奮闘」していると言われる。攻撃者が次々と新たな武器を生み出し、絶え間なく侵入を試みるのを水際で防ぐ役割を担っている。その中で、何も事故が起きなければ誰からも特に気にされず、逆に不幸にしてひとたび事故等が発生した場合には、様々な対応に追われる。企業内のセキュリティ担当者は数が限られており、1 名でしかも他の業務と兼務、といった状況も少なくない。

そういった担当者が組織や企業の枠を越え、交流や情報交換を行う場として「コミュニティ」での活動がある。セキュリティ関連のコミュニティには、PC 実習等を含む技術的な勉強会や各種のイベント、それにいわゆるオフ会等いろいろな形態があり、規模としても有志

による小規模な会合から、全国から数百名規模のセキュリティ関係者・有識者が集合する大規模なシンポジウムまで様々である。このような会合やイベント等に定期的に参加し、コミュニケーションを図ることで、セキュリティ担当者は人的なネットワークを日頃から維持するとともに、最新のサイバーセキュリティ情報を互いに情報共有しているのだ。地域の様々なセキュリティコミュニティは、企業等に所属するセキュリティ担当者の拠り所として極めて重要な位置を占める。

2. KIIS サイバーセキュリティ研究会

2.1. 経緯

前節で述べたセキュリティ人材の不足や地域での最新情報の不足は、京阪神を含めた関西地方においても重要な課題である。一般財団法人関西情報センター（KIIS）では、関西地域の情報化に関する各種課題解決や関連産業の振興等の諸活動を推進している中で、2015年度からサイバーセキュリティをテーマとする取り組み「KIIS サイバーセキュリティ研究会」をスタートさせた（2015 年度は試行実施、2016 年度から本格稼働）。

KIIS サイバーセキュリティ研究会は、関西地域での人材不足・情報不足を解消すべく、地域の企業・団体・大学等研究者をネットワーク化し、普及啓発や最新情報の提供等を行うものである。事業をスタートさせるにあたり、関西圏の企業に対しアンケートを実施し、サイバーセキュリティ対策を進める上でのニーズを尋ねたところ、図 2 のような結果が得られた（図の調査結果は 2017 年度実施分）。

このうち、やはり回答の上位を占めたのは「サイバー攻撃に対する最新の手口や具体的な事件・事故事例に関する情報を知りたい」「サイバー攻撃に関する技術的な情報を知りたい」といった、最新情報の提供を希望する意見であった。次いで実際に自社に対するセキュリティ診断を具体的に行ってほしいという意見があり、「自社の職員にセキュリティ関連の研修・講座を受けさせたい」という人材育成に関するニーズが見て取れた。また、先に述べたセキュリティコミュニティへの参加による情報交換を希望する声も聞かれた。研究会の活動内容を企画する上ではこれらのニーズを踏まえ、（1）サイバーセキュリティに関する定期的な最新情報提供、

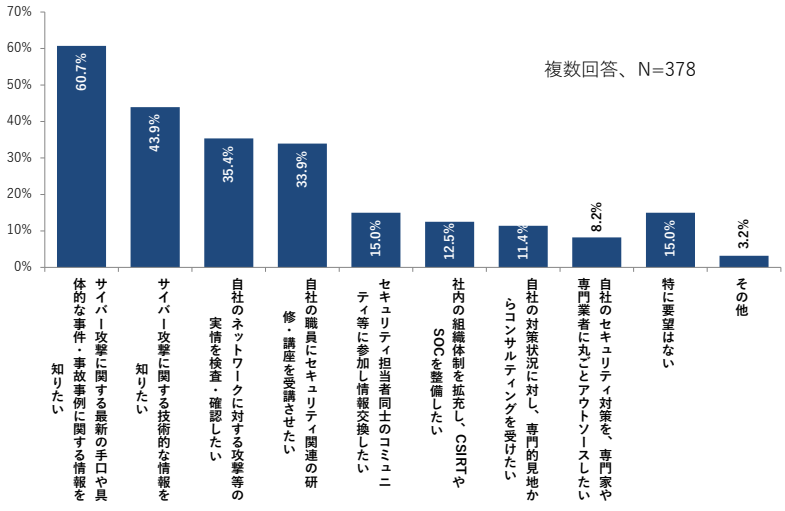

図 2. サイバーセキュリティ対策を進める上での要望
※2017 年度 e-Kansai レポート調査（一般財団法人関西情報センター）結果より抜粋

（2）セキュリティに携わる担当者によるコミュニティ醸成、（3）セキュリティ専門人材及びそれらをマネジメントする人材の育成、を事業の三本柱として推進することとした。

加えて、研究会の活動内容を専門的見地から指導いただくため、神戸大学大学院工学研究科の森井昌克教授を研究会座長として招聘することとした。森井教授は電気通信・暗号理論の専門家で、早くからサイバーセキュリティ分野の学術研究を進めるとともに、企業や警察等団体にも積極的に協力し、普及啓発の活動も行っている。これらの幅広い社会的活動により、極めて広範な人的ネットワークを有している。

また、研究会立ち上げ時点においては、財団にはサイバーセキュリティ関連の人的・組織的ネットワークはほとんど存在していなかった。最新のサイバーセキュリティ関連情報を入手するためには、中央省庁や民間の専門研究機関等との連携が欠かせない。そこで、内閣官房内閣サイバーセキュリティセンター（NISC）や一般社団法人 JPCERT コーディネーションセンター、独立行政法人情報通信研究機構（NICT）、独立行政法人情報処理推進機構（IPA）等の公的研究機関に加え、株式会社ラック、日本電信電話株式会社等民間研究機関にも協力を要請し、関西地域でのサイバーセキュリティ普及啓発活動に際して情報提供や事業連携ができる体制を新たに構築した。

2.2. 活動内容

研究会の組織体制を整えた上で、具体的な事業実施フェーズに入った。KIIS サイバーセキュリティ研究会事業の概要及び具体的な活動例については以下のとおりである。

（1）サイバーセキュリティセミナー（最新情報提供）

サイバーセキュリティに関する様々なトピックスを選定し、技術情報や社会動向、その時々の最新情報を広く普及するセミナーを開催する。「サイバーセキュリティ」は非常に裾野が広い概念であり、技術分野・領域も多岐にわたる。ターゲットやポイントを絞った情報提供を行わないと、本当に情報を伝えたい対象を見誤る可能性もある。様々な関心を持つ人がいることを想定して、開催回数を増やし（年 5 回程度）、他の団体等との連携開催等も行って、幅広い層に的確なテーマでの情報提供を行うことを心がけている。

表 1. これまでのサイバーセキュリティセミナー開催テーマ（抜粋）

日付	テーマ ＜共催機関＞
2015.12.15	組織における情報セキュリティ緊急対応体制のあり方
2016.02.04	経営課題としてのサイバーセキュリティ
2016.03.22	制御システム・IoT のセキュリティ
2016.08.09	ビジネスを脅かすサイバー攻撃最新動向
2016.10.06	サーバ監視最前線
2017.02.06	身近な脅威『内部不正』
2017.12.19	海外ビジネス展開とサイバーセキュリティ対策＜JPCERT コーディネーションセンターとの共催＞
2018.05.18	狙われる IoT 機器とビジネス化するサイバー攻撃＜組込みシステム産業振興機構との共催＞
2018.09.26	企業における個人情報保護と GDPR（EU 一般データ保護規則）対応について
2019.03.25	セキュリティ最新技術研究解説アカデミックセミナー
2019.07.16	安心・安全のソフトウェア創出社会に向けて～セキュアなソフトウェア開発に関する指針と取り組み実態～ ＜Software ISAC との共催＞

（2）セキュリティ最新情報解説サロン（セキュリティ担当者のコミュニティ醸成）

セキュリティ担当者は組織内で孤立しがちであることから、企業同士の情報交換や連携を進めるためには、担当者間で顔の見える関係を作り、企業や団体の枠を越え、セキュリティ担当者がざっくばらんに意見交換できるコミュニティを醸成することが重要である。

セキュリティ最新情報解説サロンでは、一定の秘密保持の条件のもとで、各界で著名な専門家から「ここだけの話」を提供してもらい、フランクなディスカッションを行う活動を展開している。また、よりコミュニケーションを深めるため、座学だけの会合ではなく、最新のセキュリティ施設や研修機関、研究機関等への見学会等も合わせて企画・実施している。

表 2. セキュリティ最新情報解説サロン実施状況

日付	テーマ	講師（所属）※出講当時のもの
2016.11.16	サイバー・インテリジェンス	伊東 寛 氏（経済産業省）
2016.12.05	韓国サイバーセキュリティ事情	趙 章恩 氏（東京大学）
2017.01.31	我が国のサイバーセキュリティ対策の現況と事例研究	山内 智生 氏（内閣サイバーセキュリティセンター）
2017.02.21	もしも社長がセキュリティ対策を聞いてきたら	蔵本 雄一 氏（日本マイクロソフト株式会社）
2017.07.20	情報爆発時代、今見直す企業の情報セキュリティ	丸山 司郎 氏（株式会社ベネッセインフォシェル）
2017.09.12	脆弱な IoT 機器の現状、その対策と国際標準化	中尾 康二 氏（独立行政法人情報通信研究機構）
2017.11.28	そろそろセキュリティガバナンスを考えませんか？	丸山 満彦 氏（デロイトトーマツリスクサービス）
2018.01.12	【サロン特別編】最新サイバーセキュリティ施設見学会	＜詳細非公表＞
2018.03.27	セキュリティ人材育成とキャリアパス	砂原 秀樹 氏（慶應義塾大学）
2018.06.29	リスクマネジメントと危機管理のためのデータ復旧～サイバーテロ（実演）、社内不正、データ消失事故災害～	下垣内 太 氏（大阪データ復旧株式会社）
2018.08.29	Fintech と仮想通貨の現状とサイバーセキュリティの課題	岩下 直行 氏（京都大学）
2018.10.18	【サロン特別編】イスラエルのサイバーセキュリティ訓練を集中的に学ぶ～体験型実践演習トライアル～	大日本印刷株式会社
2019.03.26	戦いの歴史から学ぶこれからのサイバーセキュリティ	伊東 寛 氏（ファイア・アイ株式会社）
2019.05.20	混沌とするサイバーセキュリティ対策の現状と対策の本質	鵜飼 裕司 氏（株式会社 FFRI）
2019.07.01	モノづくりとコトづくりの融合～コネクテッドカー＆自動運転をセキュリティ視点とビジネス視点で考える～	蔵本 雄一 氏（合同会社 White Motion）
2019.09.11	フェイクニュース対策は誰がする？	藤代 裕之 氏（法政大学）
2019.11.29	安心・安全な Society 5.0 の実現に向けて～プライバシー保護データ解析技術の現在～	盛合 志帆 氏（独立行政法人情報通信研究機構）
2020.03.24	【サロン特別編】最新サイバーセキュリティ施設見学会	※新型コロナウイルス感染拡大の影響で中止
2020.06.26	新型コロナパンデミックとサイバーセキュリティ経営	下村 正洋 氏（NPO 日本ネットワークセキュリティ協会）

（3）セキュリティ人材育成プログラム（技術・知識の向上）

企業内でセキュリティ対策を担当する人材は今後ますます不足すると見込まれる。先に述べたように、関西圏を含めた地方での人材不足はより深刻である。研究会では、企業で活躍するセキュリティ人材の裾野拡大・底上げに資するべく、ビジネス実務にすぐに役立つセキュリティ技術や知識、関連ノウハウ等を提供する、最先端の講師を集めた人材育成コースを開発し提供している。

コースは「セキュリティ担当人材コース」と「マネジメント人材コース」の 2 種類を設け、企業内での業務への携わり方によって選択可能としている。前者は PC 実習を含め技術

的な内容にフォーカスし、後者は運用や監査、リスクマネジメント等に特化した内容としている。

表 3. セキュリティ人材育成プログラム　2019 年度のカリキュラム

ｺｰｽ	No	タイトル	講師（講師所属）
セキュリティ担当人材コース	a-01	サイバーセキュリティ人材育成とスキル	小熊 慶一郎 氏（(ISC)2）
	a-02	情報セキュリティの基本とリスクマネジメント	富田 一成 氏（株式会社ラック）
	a-03	情報セキュリティの基本とリスクマネジメント【演習】	長谷川 長一 氏（株式会社ラック）
	a-04	Web アプリケーション脆弱性診断ハンズオン	田所 成久 氏（株式会社神戸デジタル・ラボ）
	a-05	Web アプリケーションの脅威と脆弱性	はせがわ ようすけ 氏（株式会社セキュアスカイ・テクノロジー）
	a-06	DFIR（デジタルフォレンジックとインシデントレスポンス）の入門と体験	マシス・ザッカリー 氏（株式会社神戸デジタル・ラボ）
	a-07	サイバーセキュリティの管理と法	金子 啓子 氏（大阪経済大学）
	a-08	暗号と認証（１）	白石 善明 氏（神戸大学大学院）
	a-09	暗号と認証（２）	白石 善明 氏（神戸大学大学院）
	a-10	情報セキュリティの運用と組織	嶋倉 文裕 氏（NPO 日本ネットワークセキュリティ協会）
マネジメント人材コース	b-01	サイバーセキュリティ人材育成とスキル	小熊 慶一郎 氏（(ISC)2）
	b-02	情報セキュリティの基本とリスクマネジメント	富田 一成 氏（株式会社ラック）
	b-03	情報セキュリティの基本とリスクマネジメント【演習】	長谷川 長一 氏（株式会社ラック）
	b-04	リスク分析からの対策立案、予算化計画	近藤 伸明 氏（株式会社神戸デジタル・ラボ）
	b-05	Web アプリケーションの脅威と脆弱性	はせがわ ようすけ 氏（株式会社セキュアスカイ・テクノロジー）
	b-06	サイバーセキュリティ技術概論	森井 昌克 氏（神戸大学大学院）
	b-07	サイバーセキュリティの管理と法	金子 啓子 氏（大阪経済大学）
	b-08	情報セキュリティの運用と組織	嶋倉 文裕 氏（NPO 日本ネットワークセキュリティ協会）
	b-09	情報セキュリティの運用と組織【演習】	長谷川 長一 氏（株式会社ラック）
	b-10	CSIRT 構築・運用	洞田 慎一 氏（一般社団法人 JPCERT コーディネーションセンター）

2.3.　人的ネットワークのさらなる拡大

上記のようなセミナー企画や研修プログラム開発にあたっては、講師や情報提供者となりうる有識者との人的ネットワークが必要不可欠である。筆者がもともと有していた人脈では到底足りず、研究会立ち上げ以降に、座長の森井教授からの紹介等により、全国のセキュリティ関係者・有識者とのネットワークづくりに注力した。先に述べたように、サイバーセキュリティに関係するメンバーが一堂に会する大規模イベントや、各地域で行われているセキュリティ勉強会等が日々開催されている。こういった全国的なイベントや会合に筆者自らが参加し、人と会うことを心がけ、有識者との交流や意見交換を図ることで、徐々にではあるが芋づる式にネットワークを拡大することができた。このことにより、途切れることなく研究会活動を企画・実施できた。

またこういった全国的なセキュリティコミュニティへの参加を続け、担当者等と話を進めるうち、関西圏において精力的に活動するコミュニティや勉強会主催者との関係も次第に強固なものとなってきた。関西地域には、様々な個人のモチベーションやマインドに応じ、多様なコミュニティが存在する。しかもいくつものコミュニティを行き来する交流人材も多数おり、そういったキーパーソンとの連携のもとで、研究会活動への参加の裾野を広

げ、周知の範囲を拡大することができた。

表 4. これまでに訪問した主なセキュリティイベント・コミュニティ等

全国規模のサイバーセキュリティ関連イベント	関西地域を拠点とする主なセキュリティコミュニティ
● サイバー犯罪に関する白浜シンポジウム（和歌山県） ● サイバーセキュリティシンポジウム道後（愛媛県） ● 情報セキュリティワークショップ in 越後湯沢（新潟県） ● 九州サイバーセキュリティシンポジウム（大分県） ● サイバー防衛シンポジウム熱海（静岡県）等	● 総関西サイバーセキュリティ LT 大会 ● OWASP Kansai ● tktk セキュリティ勉強会 ● 子供とネットを考える会 ● 神戸脆弱性診断の会 ● 一般社団法人情報セキュリティ関西研究所　等

3. 地域での活動の発展

3.1. 関西サイバーセキュリティ・ネットワーク（関西 SEC-net）の設立

KIIS サイバーセキュリティ研究会の活動が確立し、コミュニティとの行き来による人的ネットワークが拡大していく中で、関西地域でのサイバーセキュリティ関連の活動が活発であるとの評価が次第に高まってきた。さらなる活動範囲の拡大や事業展開の活性化を図るためには、行政面での政策的支援が有効であると考えられた。こういった考え方のもと、2018 年 10 月、経済産業省近畿経済産業局、総務省近畿総合通信局、それに一般財団法人関西情報センターが共同事務局となり「関西サイバーセキュリティ・ネットワーク（関西 SEC-net）」を立ち上げた。これは関西においてサイバーセキュリティに携わる業界や企業（産）、国や自治体（官）、大学等研究者（学）、コミュニティ（民あるいは個）が連携し、地域でのサイバーセキュリティの重要性についての認識醸成や、サイバーセキュリティの向上に資する人材の発掘・育成の円滑化を図る連携プロジェクトである。発足に際しては関西地域の主要な業界団体・経済団体、セキュリティベンダ、情報通信企業、大学・大学院、研究機関、自治体、セキュリティコミュニティ等 40 機関が協力機関として名を連ねた。

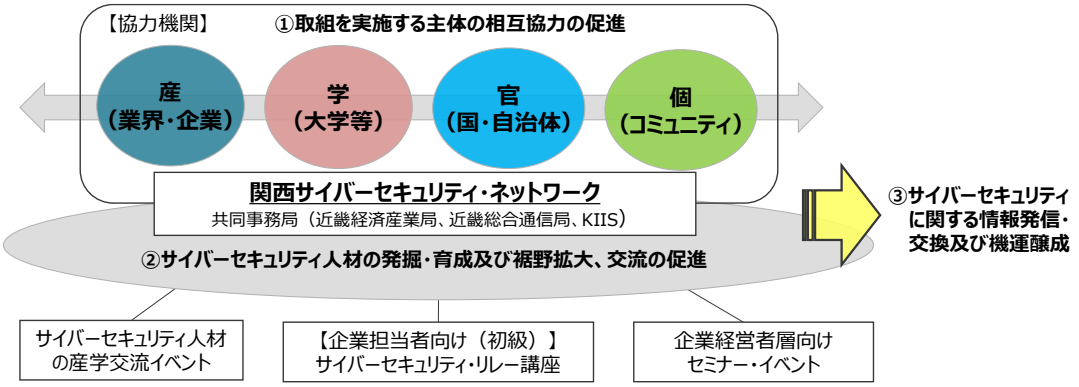

図 3. 関西サイバーセキュリティ・ネットワークの概要

3.2. 活動内容と派生効果

関西サイバーセキュリティ・ネットワークでは、様々な機関との連携により、セキュリティに関する最新情報を提供するセミナー等を展開するとともに、地域に特化した形での交

流イベントも企画し、推進している。2019 年度には京阪神地区でそれぞれ地域にゆかりのある大学研究者、セキュリティベンダ、地元産業界等が連携したセキュリティイベントを実施したのに続き、2020 年度には福井県の企業を対象としたフォーラムを開催した。特に福井ではこれまで大規模なサイバーセキュリティイベントは開催されていなかったが、本イベント等をきっかけとして、新たに地元企業が主導するコミュニティが立ち上がる見通しである。

表 5. 関西サイバーセキュリティ・ネットワークの主な活動実績

日付	イベント
2018.11.12	関西サイバーセキュリティ・ネットワーク キックオフフォーラム
2018.11.29~ 2019.01.28	企業担当者向け（初級）サイバーセキュリティ・リレー講座
2019.02.08	平成 30 年度情報セキュリティ＆危機管理セミナー
2019.07.19	産業サイバーセキュリティ対策関連施策説明会
2019.07.22~ 2019.07.30	サイバーセキュリティソリューション地域別講座 ［京都／大阪／神戸］～中小企業のセキュリティソリューション＆脅威情報の目利き力習得編～
2019.08.28~ 2019.09.26	第 2 回企業担当者向け（初級）サイバーセキュリティ・リレー講座
2020.01.31	中小企業等向け「業種横断的」セキュリティ戦略セミナー
2020.02.03~ 2020.03.18	「地域のキーパーソンに聞く、経営課題としてのセキュリティ」毎日原稿配信 ～60 秒で読める！サイバーセキュリティ対策の勘所～
2020.07.31	情報セキュリティ・マネジメントセミナー
2020.08.03	サイバーセキュリティフォーラム in 福井
2020.08.20~ 2020.09.29	第 3 回企業担当者向け（初級）サイバーセキュリティ・リレー講座

なお、これらの活動は、2019 年度・2020 年度については、一部を経済産業省「地域企業イノベーション支援事業」及び「中小企業サイバーセキュリティ対策促進事業」の枠組みで実施している。

また、関西サイバーセキュリティ・ネットワークのような産官学民連携の枠組みが立ち上がったことで、他省庁におけるサイバーセキュリティ関連施策の実証プロジェクト等が関西地域で展開されることが増えた。厚生労働省「平成 31 年度教育訓練プログラム開発事業（1 年開発コース）・IT/IoT セキュリティ人材育成プログラムの開発」や、総務省「セキュリティ人材シェアリングモデル事業」等である。関西でのセキュリティコミュニティの活動の盛り上がりが、国の政策を誘導する形となり、さらなる事業集積を生む結果となっている。

4. 活動の評価と今後の展望

KIIS サイバーセキュリティ研究会、関西サイバーセキュリティ・ネットワークともに今後も継続して事業を展開していく予定であるが、現段階で一旦の評価を行っておく。

事業開始当初は、財団には一部の調査業務実績を除き、サイバーセキュリティ関連での技術ノウハウや人的ネットワークはほとんど有していなかった。研究会座長を依頼した森井教授のアドバイスのもと、情報を足で稼ぎ、活動を積極化させることでネットワークは大幅に拡大し、地域の既存コミュニティとの連携も深まった。もともと関西にはサイバーセキュリティ分野での研究者やコミュニティが豊富であったことも、それらを連携・集約させるこ

との効果につながったと考えられる。またこういった活動を継続的に行うことで、他地域からも注目を集めるようになり、省庁横断型のプロジェクトに発展するとともに、多くの政策を関西に誘導する素地ができた。国がサイバーセキュリティ面で展開する各種施策とも軌を一に、いわば、サイバーセキュリティに関する一定のムーブメントを関西にもたらすことができたと考えている。

一方で課題は残る。地域での機運は高まりつつあるとしても、情報を届けられている先はまだ十分ではない。そもそもセキュリティに関心を持たず、自分ごととして捉えていない個人や企業は未だ多数残っている。一部の「意識の高い」企業だけが取り組みを行ったとしても、先に述べた「桶の理論」のように、弱いところから事故や被害は起きるものである。地域での全般的なセキュリティレベル底上げにつなげるべく、継続的に事業を進めていく必要がある。また今後は、実際に活動によって地域のセキュリティレベルが具体的にどれだけ向上したか、何らかの形で把握していくことが重要であろう。

ところで、研究会やネットワークにおける具体的な活動は、セミナーを始めとした普及啓発や人材育成、研修事業が中心である。地域に根差したシンクタンクがこういった活動を展開することで、国や関連団体等との繋がりを強固にすることができ、事業の継続性も確保できた。シンクタンクの社会的使命は、リサーチ・政策提言にとどまらず、それが実行・実践されるところまでチェックを行い、ときに伴走型として事業運営に携わることにある。地域でのサイバーセキュリティ向上に向けた取り組みを進める上では、人的ネットワークを駆使し、産官学民等地域の様々な主体が連携することが極めて重要であることは先にも述べた。これまで草の根的に発生してきた勉強会等コミュニティの活動をさらに横連携させ、地域全体での機運醸成が欠かせないが、そのためには、地域のコーディネータ役あるいは事務局役となって、認知度向上・合意形成・実施体制づくり等を進めていく、シンクタンクの本質的な活動が極めて有効である。

昨今、企業がデジタル技術を用いてビジネスのありようを変革していく「デジタルトランスフォーメーション（DX)」の重要性が叫ばれている。With コロナ社会を生き抜くためにも、また地域経済の発展のためにも、あらゆる組織がデジタル化を推進し、既存のビジネスのあり方を変革していく必要がある。その一方で、車の両輪としてサイバーセキュリティが確保されていなければ、DX の出鼻はくじかれ、今後の経済社会の発展が危ぶまれることになる。サイバーセキュリティは技術的に専門性が高い領域であるため、これまでは大手の SIer や専門ベンダ等によるビジネスベースでの取り組みが中心であった。しかし、地域でのセキュリティレベルの底上げや機運醸成のためには、本稿で述べたとおり、地域での人的ネットワークの確保及びコミュニティ活動の活性化が重要な施策となりうる。地方シンクタンクは人と人とをつなぎ、地域のコーディネータ役となることができるとともに、他地域との連携を進めることも有効な手段となりうるであろう。これからの地方シンクタンクが果たすべき役割は非常に大きいと考える。