関西サイバーセキュリティ・ネットワークの取組
（関西SEC-net）

2020年２月

関西サイバーセキュリティ・ネットワーク事務局

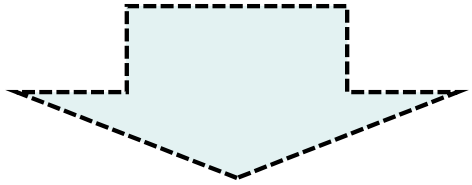
（近畿経済産業局、近畿総合通信局、一般財団法人関西情報センター）

１．関西SEC-netの発足

1-1. 問題意識

＜背景＞

- IoTやAI等の第四次産業革命関連技術の登場により、あらゆる産業分野においてIT利活用が不可欠になる一方で、企業や団体等が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は多様化。
- 近年は社会インフラ・産業基盤に物理的なダメージを与えるサイバー攻撃のリスクが増大し、海外においては既に他国家等からなされるサイバー攻撃により、社会インフラ・産業基盤の安全が脅かされる事案も発生。
- 政府は、2018年7月、「サイバーセキュリティ戦略」（新戦略） を閣議決定し、サイバーセキュリティの基本的な在り方として、実空間との一体化が進展しているサイバー空間の持続的な発展を目指す（「サイバーセキュリティエコシステム」の実現）という方針を掲げ、3つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進する方針。



サイバーセキュリティの重要性は今後ますます高まっていくと考えられる中、地方においても様々な課題が浮き彫りに。

＜地方におけるサイバーセキュリティに関する課題例＞

（１）人材の発掘・育成及び裾野拡大

（２）情報伝達及び機運醸成

（３）情報共有及び中小企業における対策の実装

1-2. 課題①　人材の発掘・育成及び裾野拡大

- サイバーセキュリティに対するニーズが増大する一方、労働人口の減少が見込まれる中、いかに十分なサイバーセキュリティ人材を育成し確保できるかは、日本の産業全体にとって重要な課題。しかし、サイバーセキュリティ人材の育成・確保は、質的・量的いずれの観点からも容易ではなく、**地方においては一層厳しい状況。**

（１）人材育成する側の人材不足問題

- 社会人の学び直しを含めた、サイバーセキュリティ人材育成の機会は、首都圏に集中。地方においては、大学・大学院におけるサイバーセキュリティ分野の専門家は特に限られており、特定の教員の負担が増大。また、企業内で人材育成するための人的リソースやノウハウ不足が指摘。

（２）人材育成のターゲットをどこに定めるか問題

- 実社会で発生する予測不可能なインシデント等に対しては、原理原則に立ち返りながら、現実的な解決策を導くことができるサイバーセキュリティ人材の存在がますます重要。大学・大学院での教育のほか、民間団体や企業内での研修等が様々実施されている中、全体のカバレッジとして不足がないか、また補完し合うことができる体系になっているか。

（３）人材受入れ側の受入体制問題／受皿不足問題

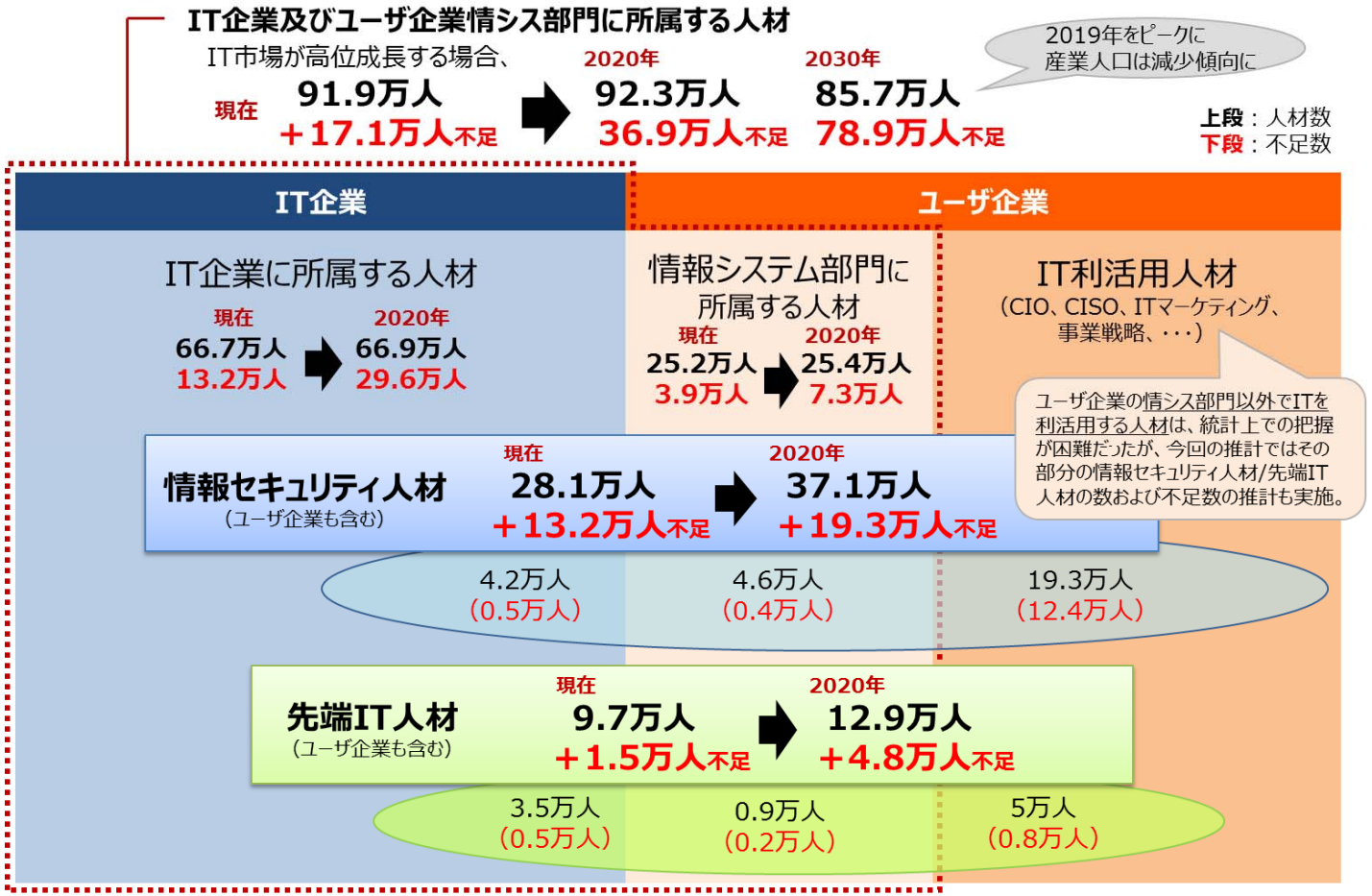
- 地方でサイバーセキュリティ分野を学んだ学生の多くは、首都圏で就職する傾向があり、地方の企業にとって、情報セキュリティの素養を持った学生をリクルートすることは容易ではない。また企業では、サイバーセキュリティ人材のキャリアパスや処遇等が十分整備されておらず、人材育成と当該人材の流出懸念が常に隣り合わせ。

（４）人材育成される側－人材受入れ側のコミュニケーション機会不足問題

- 学生は、自らの能力を評価してくれる企業への就職や、自らのキャリアパスの不透明性の払拭等に関心。一方、人材受入れ側又は人材輩出側でもある企業にとっては、学生の能力評価や、自社が求める人材像に即した社員教育の実施等に関心。双方のコミュニケーション機会は必ずしも多くはなく、ミスマッチが発生している可能性。

（参考）IT人材及びサイバーセキュリティ人材の不足

- 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。経産省の試算では、IT企業及びユーザー企業（産業界全体）におけるサイバーセキュリティ人材は、2020年には不足数が19.3万人に拡大すると推計。



※**サイバーセキュリティ人材とは**、情報セキュリティに関わる業務上の役割として**以下の分類の業務を行う人材**を指す。

①統括的情報セキュリティ管理者
組織全体の情報セキュリティ対策を統括・管理する人材。
②部署内情報セキュリティ管理者
統括的情報セキュリティ管理者の指示のもとで部署内の情報セキュリティ対策の実施を主導する人材。
③開発系業務従事者
情報セキュリティ対策製品・サービス等の設計、開発関連業務に従事する人材。
④運用系業務従事者
監視・インシデント対応等のサービス提供に関する業務に従事する人材。
⑤検査・監査系業務従事者
分析、検査、監査等のサービス提供に関する業務に従事する人材。
⑥コンサルティング系業務従事者
情報セキュリティマネジメント関連サービスの提供に関する業務に従事する人材。

出典：経済産業省（2016）「IT人材の最新動向と将来推計に関する調査結果」

（参考）全国におけるサイバーセキュリティ人材育成関連の取組例

機関等名	主な取組	ターゲット
IPA （独）情報処理推進機構 【経産省】	○平成29年4月、ICSCoE（産業サイバーセキュリティセンター）設置。社会インフラ・産業基盤事業者において、自社システムのリスクに対し、必要なセキュリティ対策を判断できる人材の育成。 ○平成29年度は、幅広い業界から研修生を受入れ、国内外の大学や研究機関、企業と連携し、実践的な演習・対策立案等の1年程度のトレーニングを実施。受講者約80名。【受講費用：300万円】	社会人 （将来、企業などの経営層と現場担当者を繋ぐ中核人材を担う方）
NICT （国研）情報通信研究機構 【総務省】	○平成29年4月、NICTにナショナルサイバートレーニングセンターを設置。ハイレベルな若手セキュリティイノベーター（革新的研究・開発者）を育成する1年間の能力開発事業「SecHack365」を実施。平成29年度受講者：47名（応募者：358名）。【受講費用：50万円（学生無料）】	学生 若手社会人 （25歳以下）
enPiT (Education Network for Practical Information Technologies) 【文科省】	○産学連携による課題解決型学習（PBL）等の実践的な教育の推進により、社会人の学び直しを含め、大学等における情報技術人材の育成強化を目指す（平成30年度予算：8億円）。 ○これまで、平成24年度～28年度はenPiT（大学院生向け）、平成28年度～32年度はenPiT2（学部生向け）として、クラウドコンピューティング分野、セキュリティ分野、組込みシステム分野等を対象に人材育成を実施。 ○平成30年度からは、enPiT-Proの、情報科学技術分野の社会人向け実践教育プログラムを、産業界・複数大学の協働により開発実施予定（平成29年度に全国で5件採択され、うちサイバーセキュリティ人材育成案件は1件）。履修可能期間2年間、受講者10名程度。【受講費用（8単位）：15万円（入学金3万円含む）】	【enPiT】 大学院生 【enPiT2】 学部生 【enPiT-Pro】 社会人
情報セキュリティ大学院大学 （IISEC） 【ProSec】	○平成16年に開学した、日本初の情報セキュリティ専門の大学院大学（横浜）。様々な大学院・研究機関と協定を締結して、大学間ネットワークを活用した学習機会・研究機会を提供。産学連携にも積極的に取り組む。 ○1年制及び2年制のコースがあり、修士課程は1学年40名程度、うち8割が社会人学生。（2016年度末までに修士339名、博士30名輩出）。【年間受講費用：150万円（入学金30万円含）】 ○enPiT-Pro事業として、情報セキュリティプロ人材育成短期集中プログラム（ProSec）として3コースを実施。各コース修了者には、学校教育法に基づく履修証明制度により「ProSec-X履修証明書」を授与。各コース5ヶ月、定員若干名。【コース受講費用：36～46万円】	大学院生 社会人
慶応義塾大学 【ProSec】	○平成28年11月、慶應義塾大学が国内外の10数大学に呼びかけ、サイバー脅威に対応するための世界初の国際連携組織「INCS-CoE（インクス・シーオーイー）」を設立。国内外の大学間で学術交流協定締結や国際シンポジウムの開催など実施。	研究者
東京電機大学	○昭和24年大学、昭和33年大学院設立。学外の研究機関と連携して大学院生の研究指導を行う「連携大学院方式」を導入し、研究領域の多様化と研究内容の拡大を図っている。 ○平成19年度の学校教育法の改正により、大学等における「履修証明制度」が創設されたことを受け、社会人向け履修証明プログラム「国際化サイバーセキュリティ学特別コース（CySec）」（大学院修士課程レベル）を開学。情報セキュリティ技術領域の先端教育に加え、経営・運営・監査等も先導可能な高度専門家を養成。年間入学定員30名。【受講費用：約25万円／7科目】	社会人（Cysec）

出典：各機関HP等公開情報より近畿経済産業局作成

（参考）関西におけるサイバーセキュリティ人材育成関連の講座・取組例

機関等名	主な取組
兵庫県立大学大学院	○兵庫県立大学とカーネギーメロン大学とのダブルディグリー・プログラム。兵庫県立大学大学院応用情報科学研究科博士前期課程に入学し、その在学中にカーネギーメロン大学の修士課程をあわせて履修することにより、計２年間で両大学の学位を同時に取得し、世界最先端の情報セキュリティに関する知識と技能を修得することができる。定員10名。【2年間学費：約878万円】 http://www.cmuj.jp/
立命館大学大学院	○情報理工学研究科博士課程前期課程・後期課程では、社会人入試を実施。募集人数若干名。 http://www.ritsumei.ac.jp/gsise/
神戸大学大学院	○工学研究科では、大学院入試の際に社会人特別選抜を実施。募集人数若干名。 http://www.eng.kobe-u.ac.jp/admission/social.html
和歌山大学 【ProSec】	○enPiT-Pro事業（文部科学省）の、情報セキュリティプロ人材育成短期集中プログラム（ProSec）として演習を中心とした２コース（インシデントレスポンス実践メインコース、インシデントレスポンス実践クイックコース）を実施。2019年度は定員若干名。【受講費用：(クイック)69,120円、(メイン) 入学料:10,000円、必須科目：69,120 円、選択科目 14,400 円/単位）】 http://www.wakayama-u.ac.jp/dtier/prosec/
大阪大学 【ProSec】	○ProSec事業として、「安全なデータ利活用のためのプロフェッショナル人材育成コース」を実施。社会人と大学院生とが学びの場を共有し、短期集中合宿やグループワークを通して、セキュリティ技術の習得を通して、リーダーシップ力やチームマネジメント力も習得。2019年度は定員若干名。【受講費用：入学金28,200円、授業料14,400円/単位】 https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/pro-sec/index-jp.html
（一財）関西情報センター（KIIS） 【Reスキル】	○サイバーセキュリティ研究会を主宰し、企業や組織がビジネスを推進する上で必要となる技術や制度について、すぐに役立つ実践的な内容の研修コース「セキュリティ人材育成プログラム」（セキュリティ担当人材コース、マネジメント人材コース）を開講。経済産業省「第四次産業革命スキル習得講座認定制度」（通称：「Reスキル講座」）の認定取得。講義及び実習合わせて10回。1コース3ヶ月程度、受講者数約20名。【受講費用：10万円／人】 https://secure.kiis.or.jp/cybersecurity/program.html
総サイLT実行委員会 【コミュニティ】	○サイバーセキュリティ関係者のコミュニティ。サイバーセキュリティに関する意見交換会「総関西サイバーセキュリティLT大会」を偶数月の第2水曜日に開催。現在700名を越える登録者がおり、毎回100名以上の参加者がいる。
OWASP Kansai 【コミュニティ】	○OWASP KansaiはWebアプリケーションのセキュリティ向上を目指す非営利団体であるOWASPの関西地域でのLocal Chapter。定期的にChapter Meeting / OWASP Nightと称した勉強会を開催。
tktkセキュリティ勉強会 【コミュニティ】	○情報セキュリティの知識及び技術向上に加え、人と人との繋がりを持つ場として勉強会を開催。対象者は、情報セキュリティに関心がある方であれば、誰でも参加可能。

出典：各機関HP等公開情報より近畿経済産業局作成

（参考）その他サイバーセキュリティ人材育成関連の講座・取組例（関西開催行事あり）

機関等名	主な取組
IPA （独）情報処理推進機構	○2017年4月、ICSCoE（産業サイバーセキュリティセンター）を設置。社会インフラ・産業基盤事業者において、自社システムのリスクに対し、必要なセキュリティ対策を判断できる人材を育成。 ＜中核人材育成プログラム＞ https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ1年程度のトレーニングを実施。3ヶ月程度の初歩的なレベル合わせからハイレベルな卒業プロジェクトまで実施。※2019年度（第3期）は、2019年7月～2020年6月に実施中。定員約80名。【受講料：300万円】 ＜責任者向けプログラム：業界別サイバーレジリエンス強化演習＞（CyberREX） https://www.ipa.go.jp/icscoe/program/short/specific_industries/index.html 部門責任者層が、業界別のシナリオによる実践的演習の形式で、企業が直面するサイバーリスクへの対応について学ぶ機会を提供。※2019年度は大阪においても9月に開催。定員約30名。【受講料：8万円】 ＜実務者向けプログラム：制御システム向けサイバーセキュリティ演習＞ https://www.ipa.go.jp/icscoe/program/short/icssec/index.html 模擬プロセス制御ネットワークを使用して、機器の不正な制御に使用されるサイバー攻撃や対応策による防御を体験し、制御システムのセキュリティについてより深く理解する実践的な内容。※2019年度は大阪においても9月に開催済。定員約20名。【受講料：18万円】
NICT （国研）情報通信研究機構	○平成29年4月、NICTにナショナルサイバートレーニングセンターを設置。長年のサイバーセキュリティに関する研究で得られた技術的知見等を最大限に活用することにより実践的なサイバートレーニングを企画・推進。 ＜実践的サイバー防御演習「CYDER」＞ https://cyder.nict.go.jp/ サイバーセキュリティ基本法に規定される国の行政機関、地方公共団体、独立行政法人、重要社会基盤事業者等を対象として、実践的なサイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）を実施。2018年度からは民間企業や大学等も受講可。※2019年度は全国47都道府県において100回程度開催。【受講料：7万円】（ただし、国の行政機関等、地方公共団体に所属されている方は無料） ＜若手セキュリティイノベーター育成プログラム：SecHack365＞ https://sechack365.nict.go.jp/ 25 歳以下の学生や社会人から公募選抜する受講者を対象に、サイバーセキュリティに関するソフトウェア開発や研究、実験、発表を一年間継続してモノづくりをする機会を提供する長期ハッカソン。※2019年度定員約40名（応募者：295名）。【受講料：約50万円（学生については全額補助）】

出典：各機関HP等公開情報より近畿経済産業局作成

1-2. 課題②　情報伝達及び機運醸成

- サイバーセキュリティについての情報が、**地方の企業には必ずしも行き届いていない**という状況が見られ、このいわば**「サイバーセキュリティのラストワンマイル」**に情報が行き着くよう配慮し、取組を推進することが必要。

（１）地方の企業が情報をキャッチしやすい仕組みが限定的

・官民から数多く提供される情報が、より効果的・効率的に地方の個人や企業等に行き渡るつながりをつくるため、官民の関係者間のみならず、大学・高専や地域において活動するコミュニティとも、実質を伴う連携強化が必要。

（２）メディア等を通じた情報発信頻度が限定的

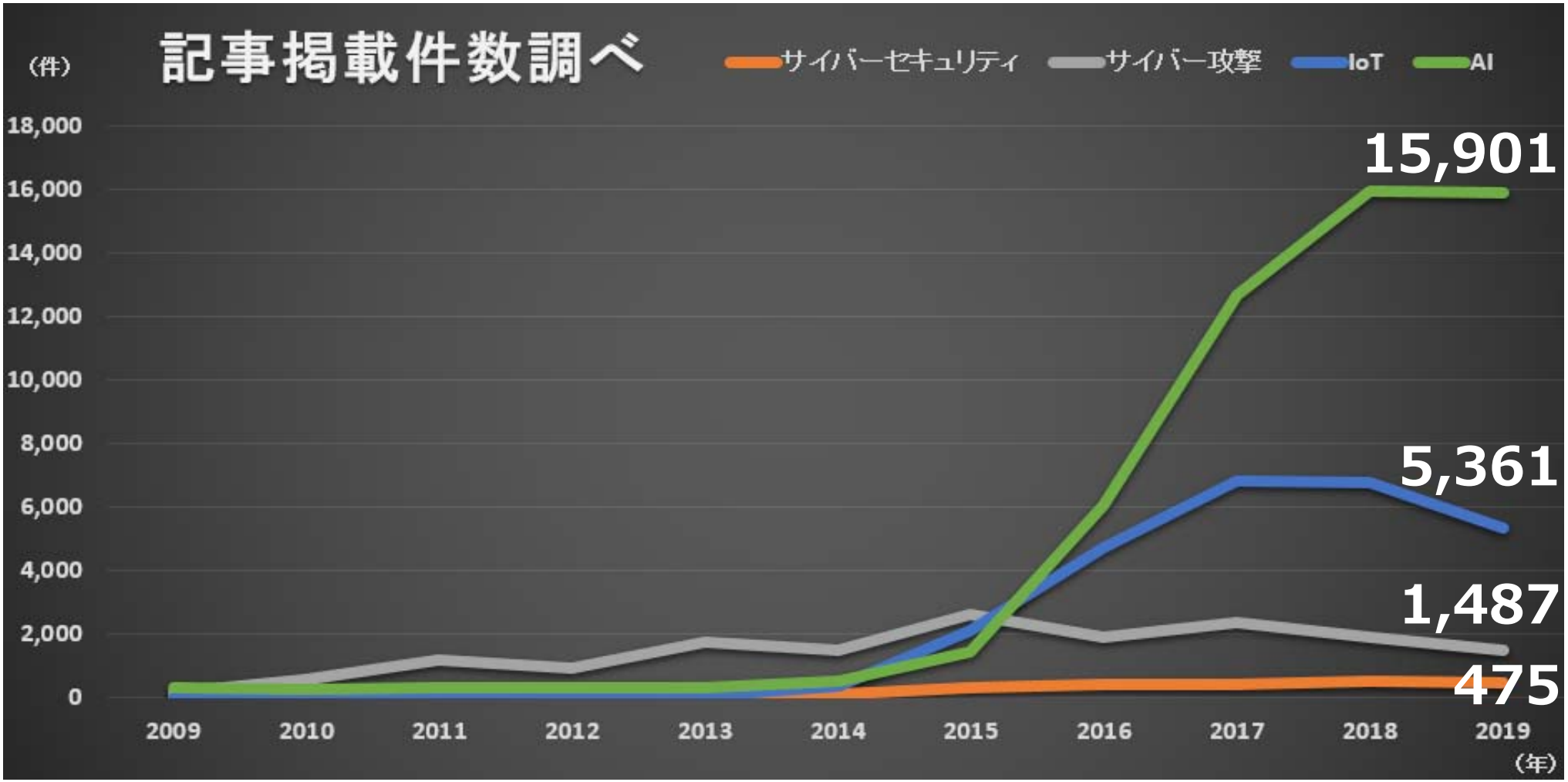
・サイバーセキュリティについては、脅威情報や対応策、企業等の取組事例、国や自治体の施策等に関する最新情報を、タイムリーかつ分かりやすく、そして広く伝えるため、意識的にPR（パブリック・リレーションズ）に取り組むことが必要。

（３）セキュリティを経営課題として位置づける問題意識が限定的

・大企業から中小企業まで、サイバーセキュリティが、価値創造や危機管理の観点から不可欠なものであり、経営課題そのものであるという認識を持って、企業経営者がサイバーセキュリティ対策に取り組むことが必要。

記事掲載件数（Connected Industries におけるキーワード）

- サイバーセキュリティのメディア掲載は、他のキーワードに比べて低調であり、情報が地域に行き届いていない。



■手　　法：日経テレコンにてキーワード記事検索
■期　　間：2009年1月1日～2019年12月31日
■対　　象：新聞（全国5紙）（朝日、毎日、読売、産経、日経）、
新聞（産業・経済）（日経産業、日刊工業、フジサンケイ、日経MJ、日経ヴェリタス）
ビジネス週刊誌（日経ビジネス、週刊ダイヤモンド、週刊東洋経済、週刊エコノミスト、プレジデント）

1-2. 課題③　情報共有及び中小企業における対策の実装

- **サプライチェーン全体としてのサイバーセキュリティをいかに確保するか**という点が今後ますます重要。
- 例えば、セキュリティ対策が十分でない**中小企業が踏み台となって、自社のみならず取引先までサイバー攻撃の影響が拡大**するという懸念が広がっている。こうした中小企業を含めた事業者が実際に対策を行いやすくするために、理想論ではなく、現実的に実施可能な対策をいかに着実に講じていくかという視点が必要。

（1）中小企業は自社も攻撃対象となっていることの認識が不足

・まさか自社がサイバー攻撃を受けるとは考えていない中小企業は多い。しかし昨今では、取引先も含めてセキュリティを確保していることが重要であり、自社が対策をしていないことで委託元に迷惑をかけてしまう可能性や、セキュリティ要件を満たさない事業者、製品、サービスはグローバルサプライチェーンからはじき出される可能性も指摘。

（2）中小企業がセキュリティに割けるリソースは限定的

・中小企業及び小規模企業においては、限られた人員や予算の中で日々多くの業務をこなさなければならない中で、日々アップデートされるサイバー攻撃の脅威等について情報収集し、自社で対策を講じることは容易ではないという現状を認識した上で、現実的にどのような対策が可能かを検討することが必要。

（参考）中小企業に対するサイバー攻撃の実態調査【大阪商工会議所】

中小企業におけるサイバー攻撃対策に関するアンケート調査結果（2017年6月）
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf

○有効回答数：関西の中小企業や団体など 315社
○ポイント：
・現在実施している**セキュリティー対策で十分でないと思っている企業が約7割（68%）**。
・十分ではないと思っている理由は、**情報セキュリティに経費がかけられない（60%）、専門人材がいないのでわからない（48%）**。
・情報セキュリティの担当者がいないと回答した企業が過半数。担当者がいても専任担当者(4%)ではなく、**業務の兼任（44%）の担当者**。
・**情報セキュリティにかける経費として、8割弱（79%）の企業が年間50万円以下**。

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対策等に関する調査結果（2019年5月）
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190510sc.pdf

○有効回答数：全国の従業員100人以上の企業　118社
○ポイント：
・**大企業・中堅企業の約７割（68%）**は、「仕入・外注・委託先（買い先）」「販売・受注・受託先（売り先）」におけるサイバーセキュリティやサイバー攻撃被害について**「あまり把握していない」**。
・**「取引先がサイバー攻撃被害を受け、それが自社に及んだ経験」がある企業は4社に1社（25%）**。その結果、**「情報漏洩」（5社）、システムダウン（3社）、データ損壊（3社）など実害も**出ている。

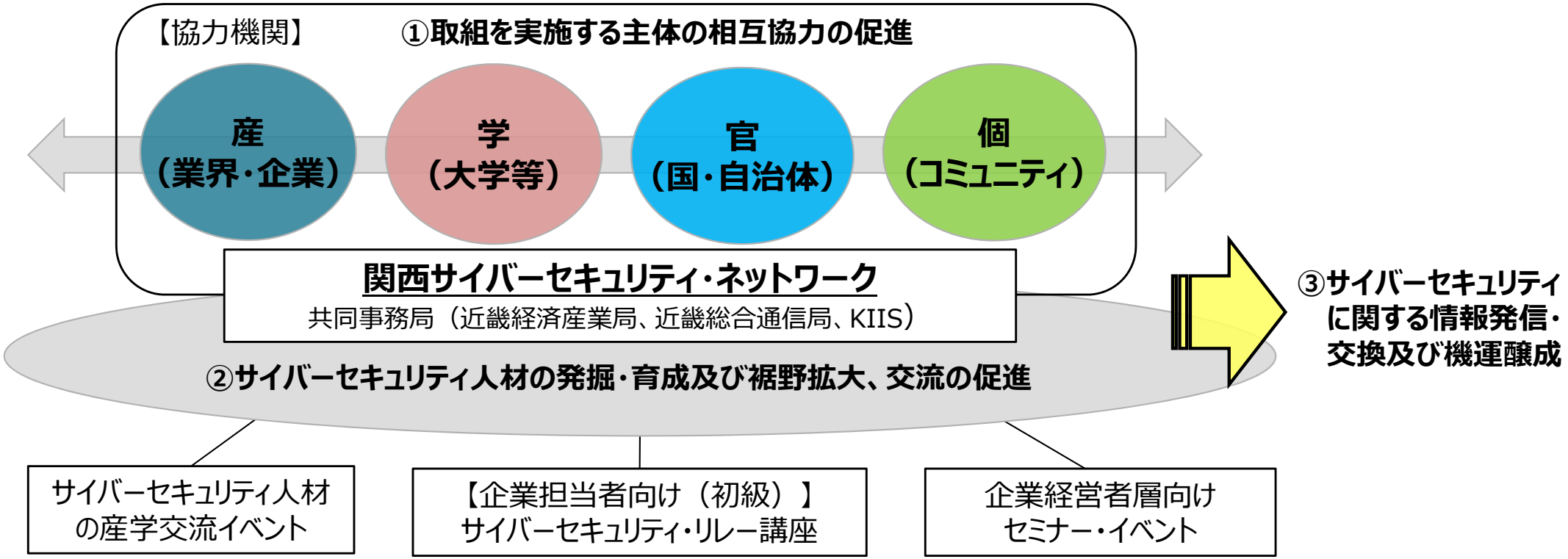
平成30年度中小企業に対するサイバー攻撃実情調査（報告）　（2019年7月）
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190703cyber.pdf

○協力企業数：大阪市内を中心とした多種多業種の中小企業 30社
○ポイント：
・**30社すべてにおいて何等かの不正な通信があった旨を示すアラート（警告）の記録（ログ）**があった。
・アラートのログを分析した結果、脆弱性（弱点）やポート（出入口）を狙って攻撃されている事例から、外部から社内の端末をリモート操作されているなど、大きく3つの種類のサイバー攻撃の実態が複数企業に対して確認された。
・**今回のほとんどの協力企業では何等かのウィルス対策ソフトの導入ならびに運用がされていた**。

出典：大阪商工会議所プレスリリースより抜粋

1-3. 取組方針

- 2018年10月、近畿経済産業局、近畿総合通信局、(一財)関西情報センター(KIIS)が共同事務局となり、サイバーセキュリティ分野における関西の産学官等の相互協力を促進するため、「関西サイバーセキュリティ・ネットワーク」（関西SEC-net）を発足。
- 関西におけるセキュリティの推進基盤として、人材発掘・育成、情報交換、機運醸成の場を提供。サイバーセキュリティで重要な、「知る」ための取組を進める。



※原則として、産学官個の各主体が実施していない領域の取組を補完的に実施する

1-4. 関西サイバーセキュリティ・ネットワーク体制

【協力機関】 ※平成30年10月17日発足時（40機関）より順次拡大中。　（順不同）62機関（令和元年12月1日時点）

カテゴリ		主な機関等
産	業界団体・経済団体	関西経済連合会、関西経済同友会、大阪商工会議所、神戸商工会議所、京都商工会議所、関西ものづくりIoT推進連絡会議関係団体（18団体：IT・電気計測器・電子電機・電子部品）、近畿情報通信協議会、日本ネットワークセキュリティ協会（JNSA）西日本支部、ISACA（情報システムコントロール協会）大阪支部、産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）
	セキュリティベンダー	神戸デジタル・ラボ、ファイア・アイ、ラック、エムオーテックス、大日本印刷、日本シノプス
	情報通信企業	NTT西日本、オージス総研、NEC、富士通、日立製作所、さくらインターネット、ケー・エス・ディー、日商エレクトロニクス、NTTデータ先端技術、さくらケーシーエス
	ユーザー企業	パナソニック、関西電力、大阪ガス、西日本旅客鉄道、ダイキン工業、日本放送協会大阪放送局、毎日放送、朝日放送テレビ、関西テレビ、読売テレビ放送
	その他企業	NHKテクノロジーズ大阪総支社、双日インシュアランス、SOMPリスクマネジメント、トーマツ、
学	大学・大学院	神戸大学、兵庫県立大学、和歌山大学、大阪経済大学、立命館大学情報理工学部上原研究室、奈良先端科学技術大学院大学サイバーレジリエンス構成学研究室、近畿大学
	研究機関	産業技術総合研究所（AIST）、情報通信研究機構（NICT）
	その他	OCA大阪デザイン＆IT専門学校
官	国関係機関	内閣官房内閣サイバーセキュリティセンター（NISC）、情報処理推進機構（IPA）
	自治体	大阪府、兵庫県、滋賀県、大阪市、神戸市、堺市、京都市
個	セキュリティコミュニティ	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

【共同事務局】　近畿経済産業局、近畿総合通信局、一般財団法人関西情報センター（KIIS）

２．2019年度の主な取組

主な取組項目

【　】＝連携する主な協力機関

1. 人材の発掘・育成及び裾野拡大

＜座学／演習／産学交流＞

・サイバーセキュリティ・リレー講座（初級者向け）【大学】
・制御システム向けサイバーセキュリティ演習（制御システム実務者向け）【IPA】
・業界別サイバーレジリエンス強化演習（部門責任者向け）【IPA】
・セキュリティ・ミニキャンプ（若者向け）【高専、IPA、ミニキャンプ協議会】

2. 情報伝達及び機運醸成

＜イベント／PR＞

・サプライチェーンにおけるサイバーセキュリティを語りあうシンポジウム【IPA】
・産業サイバーセキュリティ対策関連説明会【IPA、JPCERT/CC】
・サイバーセキュリティソリューション地域別講座（中小企業向け）【企業・地域関係機関】
・企業経営者または実務者向けイベント 【商工会議所、経済団体、業界団体】

3. 情報共有及び中小企業における対策の実装

＜経済産業省／総務省／IPA／NICT施策の地方展開＞

・サイバーセキュリティお助け隊 【大阪商工会議所、IPA】
・中小企業の情報セキュリティ対策ガイドライン 【IPA】
・セキュリティ対策自己宣言「SECURITY ACTION」【IPA】
・実践的サイバー防御演習「CYDER」【NICT】
・IoT機器調査及び利用者への注意喚起の取組「NOTICE」【NICT】

2-1. 人材の発掘・育成及び裾野拡大

●第2回サイバーセキュリティ・リレー講座（初級者向け）
～サイバーセキュリティの基礎＆心得習得編～

企業でこれからサイバーセキュリティを担う担当者（初級者）に対し、様々な事案に柔軟に対応できるセキュリティ分野のセンスや専門性の土台を身につけることを目的に、関西を代表する研究者8名による集中講座を実施。（全8回）

日程	テーマ	講師
8/28	フォレンジック技術	上原　哲太郎　氏 立命館大学　情報理工学部　教授
9/3	AIとサイバーセキュリティ	申　吉浩　氏 兵庫県立大学大学院　応用情報科学研究科 特任教授
9/5	暗号技術に基づくサイバーセキュリティ	五十部　孝典　氏 兵庫県立大学大学院　応用情報科学研究科　准教授
9/10	ネットワーク運用とそのセキュリティ対策	川橋　裕　（他名：泉　裕）　氏 和歌山大学　学術情報センター　講師
9/12	情報セキュリティリスクマネジメントにおける人材育成の考え方	猪俣　敦夫　氏 大阪大学　情報セキュリティ本部　教授
9/17	サイバーセキュリティマネジメント	金子　啓子　氏 大阪経済大学　経営学部　准教授
9/24	サイバーフィジカルシステムにおけるセキュリティ	森　彰　氏 産業技術総合研究所　サイバーフィジカルセキュリティ研究センター　ソフトウェアアナリティクス研究グループ長
9/26	システムの脆弱性、無線LANセキュリティ	森井　昌克　氏 神戸大学大学院　工学研究科　教授

【実績】
・日程：2019年8月28日～
　　2019年9月26日
・時間：各回120分（16:30～18:30）
・会場：KIIS会議室（大阪市内）
・対象：企業でのサイバーセキュリティを担当者（初級者）で、今後専門性を高めていきたい意欲のある方
・受講者数：118名
・受講修了証交付者数：82名

※受講修了証：
原則7回以上講義に出席し、一定水準以上の理解が認められる場合（各回講義後に簡単なテストを出題し理解度を確認）、事務局から受講修了証を授与。


受講修了証

株式会社 ×××
×× ×× 殿

貴殿は下記の連続講座を受講し、講座内容に対し十分な理解を得られたものと認めます。

記

講座名：【企業担当者向け（初級）】
サイバーセキュリティ・リレー講座
講座期間：平成３０年１１月～平成３１年１月

平成 31 年 1 月 28 日
関西サイバーセキュリティ・ネットワーク事務局

2-2. 情報伝達及び機運醸成

●サイバーセキュリティソリューション地域別講座（中小企業向け）
～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～

サプライチェーンセキュリティ対策の必要性が高まる中、中小企業が複数のサービスを比較し、そのポイントを見極める目利き力の習得を目指す講座を地域別に開催。
（京都、大阪、神戸にて開催）

●大阪会場　（共催: 大阪商工会議所　※来場者82名）

【モデレーター】大阪大学　猪俣教授
【パネリスト】エムオーテックス(株)、西日本電信電話(株)、日本電気(株)、(株)日立システムズ、富士通(株)、大阪商工会議所

●京都会場　（共催: Ksisnet、京都商工会議所、一般社団法人京都府情報産業協会　※来場者48名）

【モデレーター】立命館大学　上原教授
【パネリスト】アイマトリックス(株)、アドソル日進(株)、カゴヤ・ジャパン(株)、京セラコミュニケーションシステム(株)、ISACA大阪支部

●神戸会場　（共催: 神戸商工会議所　※来場者54名）

【モデレーター】神戸大学大学院　森井教授
【パネリスト】(株)FFRI、(株)神戸デジタル・ラボ、(株)さくらケーシーエス、NRIセキュアテクノロジーズ株、日本ネットワークセキュリティ協会（JNSA）西日本支部

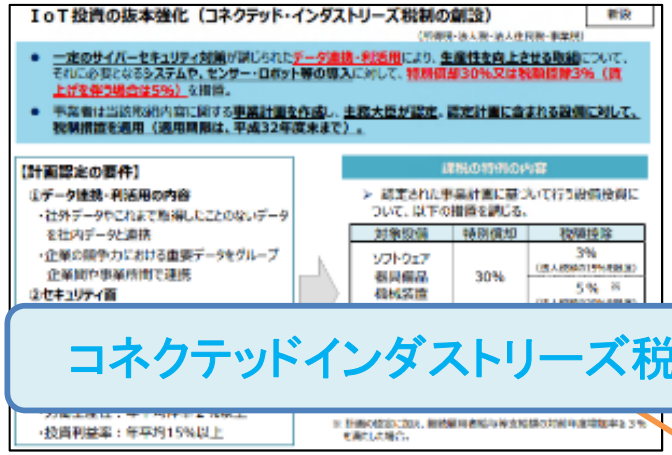
2-3. 情報共有及び中小企業における対策の実装

●経済産業省／総務省／IPA／NICT施策の地方展開

・サイバーセキュリティお助け隊
・中小企業の情報セキュリティ対策ガイドライン
・セキュリティ対策自己宣言「SECURITY ACTION」 など

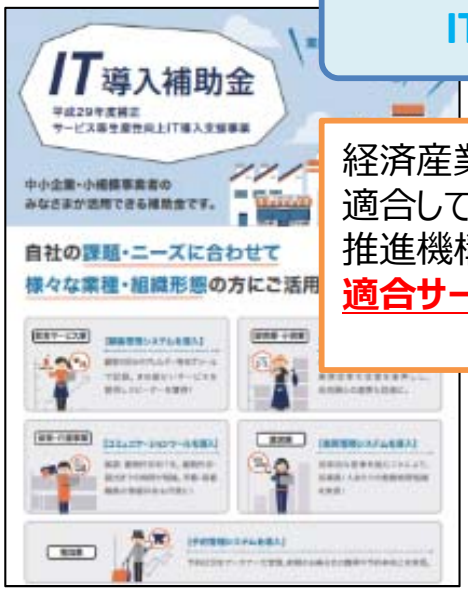
【基準を満たした情報セキュリティサービスの利用促進】

情報セキュリティサービスの利用を促進するため、政府調達や、税制・補助金における「情報セキュリティサービス基準適合サービスリスト」の推奨を実施。



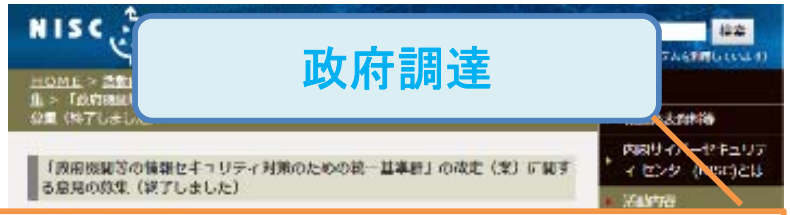
コネクテッドインダストリーズ税制

セキュリティ監視・運用サービスを利用する場合、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した**「情報セキュリティサービス基準適合サービスリスト」に記載があるサービスを利用している**。
～「認定申請書記入方法」より抜粋
※情報セキュリティ監査、脆弱性診断についても同様に記載。



IT導入補助金

経済産業省が公開している「情報セキュリティサービス基準」に適合しているサービスのリストとして、独立行政法人情報処理推進機構（IPA）が公表する**「情報セキュリティサービス基準適合サービスリスト」を参照することが望ましい。**
～「ITツール登録要領」より抜粋



政府調達

経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた 企業を記載した**「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監査サービスに係る部分）を活用**するほか、（中略）～参照することも考えられる。
～「政府機関等の対策基準策定のためのガイドライン」より抜粋

2-4. 2020年「サイバーセキュリティ月間」（2月1日～3月18日）の取組

■ 政府では、重点的かつ効果的にサイバーセキュリティに対する取組を推進するため、2010年より、**毎年2月1日から3月18日**を**「サイバーセキュリティ月間」**に設定。各種啓発主体と連携し、サイバーセキュリティに関する普及啓発活動を集中的に実施します。

■ 近畿経済産業局、近畿総合通信局、一般財団法人関西情報センターでは、関西SEC-net協力機関等と連携し、関西ならではの企画を実施します。

（主な取組例）

●60秒で読める！【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～】

関西を拠点とする有識者、企業の経営層、団体及びコミュニティ主宰者に対して「経営課題としてのセキュリティ」をテーマにインタビューを行った内容を、60秒で読むことができる記事に編集し、2020年サイバーセキュリティ月間の間、毎日1記事ずつ配信します。【合計31回】（土日祝日は除く。）
https://www.kansai.meti.go.jp/2-7it/k-cybersecurity-network/interview2020/keyperson.html

※本記事は経済産業省公式Twitterでも、期間中の平日夕方に当局HPのリンクをキーメッセージを添えて毎日発信中です。 ＜経済産業省公式Twitter「@meti_NIPPON」＞

●サイバーセキュリティフォーラム＆ミートアップin福井 ～IoT/AI時代に、地域全員でサイバーセキュリティを考える～

福井県内におけるサイバーセキュリティの取組機運向上及び域内関係者間のつながりを深めることを目的に、福井県で実施するサイバーセキュリティ分野の取組としては、過去最大規模のイベントを開催します。

日　程： 令和2年3月2日（月曜日） 13時30分～19時00分　（於：福井市内）
主　催： 関西サイバーセキュリティ・ネットワーク事務局、北陸総合通信局、福井県
定　員： 150名程度
対象者： 福井県内の企業、団体、有識者、行政、メディア関係者、本テーマに関心を有する福井にゆかりのある方等
申　込： https://secure.kiis.or.jp/KCSN/200302fukuiforum/