総務省
Ministry of Internal Affairs and Communications

総務省におけるサイバーセキュリティ分野の人材育成に関する取組について

令和２年２月２５日

総務省
サイバーセキュリティ統括官室

赤阪　晋介

「サイバーセキュリティ戦略」（平成30年7月27日 閣議決定）の全体概要

中長期的

戦略期間（2018～2021年（3年間））

1 策定の趣旨・背景

1．1． サイバー空間がもたらすパラダイムシフト（サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト）

1．2． 2015年以降の状況変化（サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会等を見据えた新たな戦略の必要性）

2 サイバー空間に係る認識

2．1． サイバー空間がもたらす恩恵

・人工知能（AI）、IoT※などサイバー空間における知見や技術、サービスが社会に定着し、既存構造を覆すイノベーションを牽引。**様々な分野で当然に利用**され、人々に豊かさをもたらしている。

※：Internet of Thingsの略

2．2． サイバー空間における脅威の深刻化

・技術等を**制御できなくなるおそれは常に内在**。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的な損失が生ずる可能性は拡大

3 本戦略の目的

3．1． **基本的な立場の堅持**

（1）基本法の目的（2）基本的な理念（「自由、公正かつ安全なサイバー空間」）（3）基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3．2． 目指すサイバーセキュリティの基本的な在り方

（1）目指す姿（**持続的発展のためのサイバーセキュリティ（「サイバーセキュリティエコシステム」）の推進**）（2）主な観点（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**）

4 目的達成のための施策

経済社会の活力の向上及び持続的発展

1．新たな価値創出を支えるサイバーセキュリティの推進

＜施策例＞・**経営層の意識改革の促進（「費用」から「投資」へ）**
・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）
・セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化

2．多様なつながりから価値を生み出すサプライチェーンの実現

＜施策例＞・**中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定**

3．安全なIoTシステムの構築

＜施策例＞・IoTシステムにおけるセキュリティの体系の整備と国際標準化
・**IoT機器の脆弱性対策モデルの構築・国際発信**

等

国民が安全で安心して暮らせる社会の実現

1．国民・社会を守るための取組

＜施策例＞・脅威に対する事前の防御（**積極的サイバー防御**）策の構築
・サイバー犯罪への対策

2．官民一体となった重要インフラの防護

＜施策例＞・安全基準等の改善・浸透（サイバーセキュリティ対策の**関係法令等における保安規制としての位置付け**）
・地方公共団体のセキュリティ強化・充実

3．政府機関等におけるセキュリティ強化・充実

＜施策例＞・**情報システムの状態のリアルタイム管理の強化**
・先端技術の活用による先取り対応への挑戦

4．大学等における安全・安心な教育・研究環境の確保

＜施策例＞・**大学等**の多様性を踏まえた対策の推進

5．2020年東京大会とその後を見据えた取組

＜施策例＞・**サイバーセキュリティ対処調整センターの構築の推進**
・成果のレガシーとしての活用

6．従来の枠を超えた情報共有・連携体制の構築

＜施策例＞・**多様な主体の情報共有・連携の推進**

7．大規模サイバー攻撃事態等への対処態勢の強化

＜施策例＞・**サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化**

等

国際社会の平和・安定及び我が国の安全保障への寄与

1．自由、公正かつ安全なサイバー空間の堅持

＜施策例＞・**自由、公正かつ安全なサイバー空間**の理念の発信
・サイバー空間における法の支配の推進

2．我が国の防御力・抑止力・状況把握力の強化

＜施策例＞・国家の**強靭性の確保**（①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策）
・サイバー攻撃に対する**抑止力の向上**（①実効的な抑止のための対応、②信頼醸成措置）
・サイバー空間の**状況把握の強化**（①関係機関の能力向上、②脅威情報連携）

3．国際協力・連携

＜施策例＞・**知見の共有・政策調整**
・事故対応等に係る国際連携の強化
・能力構築支援

等

横断的施策

人材育成・確保 ＜施策例＞**戦略マネジメント層の育成・定着**、実務者層・技術者層の育成（**高度人材**含む）、人材育成基盤の整備、**政府人材**の確保・育成の強化、国際連携の推進

研究開発の推進 ＜施策例＞実践的な研究開発の推進（**検知・防御等の能力向上、不正プログラム等の技術的検証**を行うための体制整備）、**AI等**中長期的な技術・社会の進化を視野に入れた対応

全員参加による協働 ＜施策例＞サイバーセキュリティの普及啓発に向けた**アクションプランの策定、国民への情報発信**（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

5 推進体制

本戦略の実現に向け、サイバーセキュリティ戦略本部の下、**内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化**を図るとともに、同センターが、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。**施策が着実かつ効果的に実施されるよう必要な予算の確保と執行を図る。** 等

IoT・5Gセキュリティ総合対策（2019年8月公表）

■ ICTの利活用が一層進展していく中で、5Gのサービスの開始、データ管理・流通の重要性やサプライチェーンリスクへの対応などの必要性が増大していること等を踏まえ、IoT・5G時代にふさわしいサイバーセキュリティ対策の在り方について検討し、総務省として取り組むべき課題を「IoT・5Gセキュリティ総合対策」として策定し2019年8月に公表（※）。

● 直近で留意すべき事項

1 5Gのサービス開始に伴う新たなリスク

- ✓ 仮想化、ソフトウェア化、モバイルエッジコンピューティング
- ✓ 産業用途でのIoT機器の設置・運用

2 サプライチェーンリスクの管理の重要性

- ✓ ICTの製品・サービスの製造・流通過程でのリスク
- ✓ 委託先が踏み台となって攻撃を受けるケース

3 Society5.0の実現に向けたデータの流通・管理の重要性

- ✓ クラウドサービスやスマートシティなどのセキュリティの確保の重要性
- ✓ トラストサービスの必要性

4 サイバーセキュリティにおけるAI利活用の重要性

- ✓ AIの活用が進展する中で、特にAIを利活用したサイバーセキュリティ対策を促進することが必要

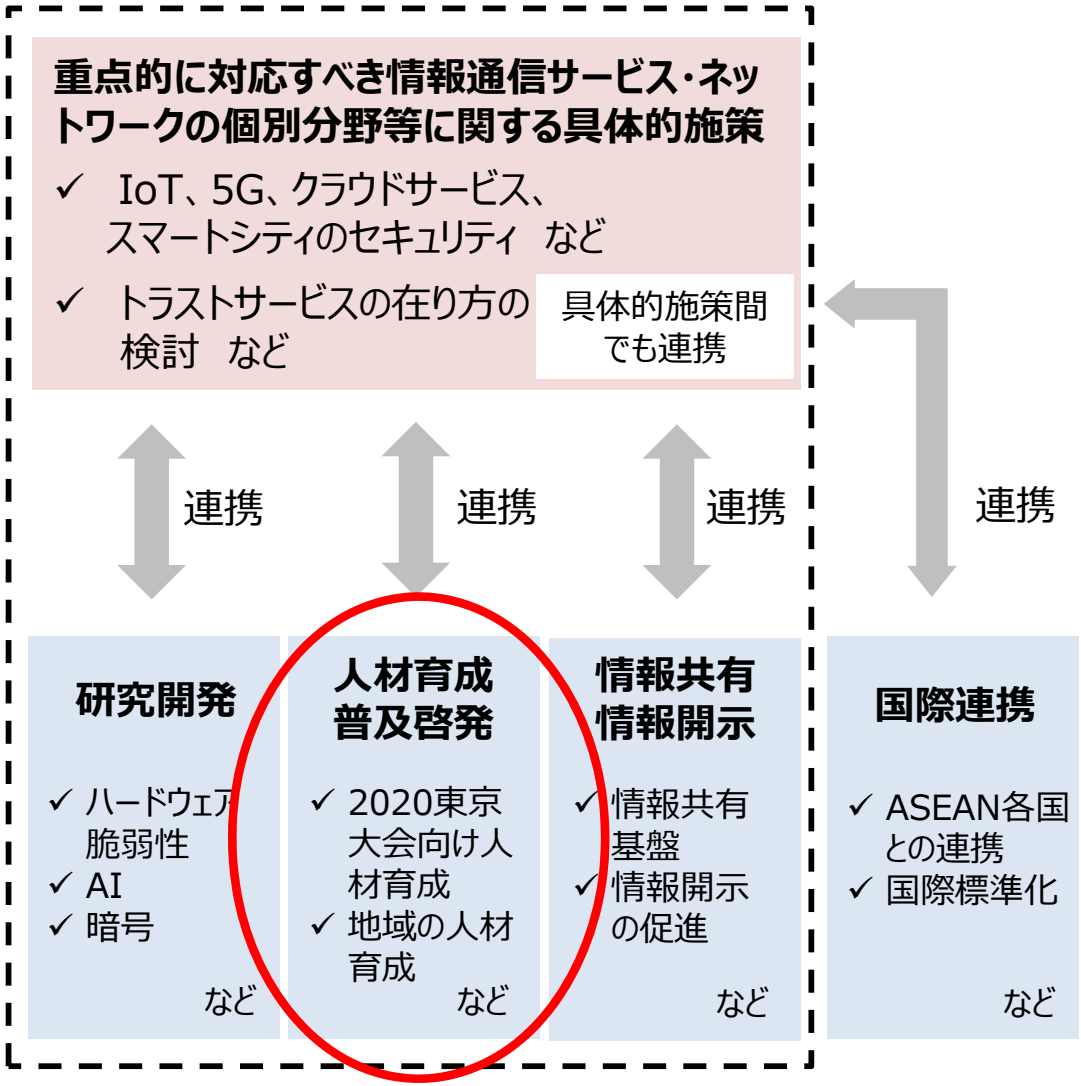
5 大規模な量子コンピュータの実用化の可能性

- ✓ 将来の大規模な量子コンピュータの実用化の可能性を踏まえ、現時点から新たな推奨暗号の在り方について検討の必要性

6 大規模な国際イベント等の開催

- ✓ ラグビーワールドカップや東京オリンピック・パラリンピック大会の円滑な実施、及びその後も見据え、対策の着実な実施が必要

● IoT・5Gセキュリティ総合対策の枠組み



（※）これに先立ち、2017年（平成29年）には、IoT機器・システムのセキュリティ等の確保を主眼においた「IoTセキュリティ総合対策」を策定・公表

我が国のサイバーセキュリティ強化に向け早期に取り組むべき事項［緊急提言］の概要

■ サイバーセキュリティタスクフォースにおける「IoT・5Gセキュリティ総合対策」の策定・公表後の議論を踏まえ、2020年７月より開催される2020年東京大会に向けた対処として早急に取り組むべき事項を整理・公表
（2020年１月28日）

1 IoT機器のセキュリティ対策の拡充

- ✓ 脆弱な状態にあるIoT機器について注意喚起方法の一層の改善を図ることが必要
- ✓ 重要施設に設置されているIoT機器に対して新たに注意喚起を実施することが必要

2 地方公共団体向け実践的サイバー防御演習（CYDER）の繰り上げ実施等

- ✓ 2020年東京大会前に未受講の地方公共団体を中心としてCYDERの集中的な受講機会を設けることが必要
- ✓ CYDERのオンライン受講を早期に開始することが必要

3 サイバーセキュリティに関する情報共有体制の強化

- ✓ 個人情報などの流出が疑われる時点で、速やかにインシデントに関する情報の公表を検討することが望ましい
- ✓ 類似の被害の拡大を防ぐ観点から、インシデントに関する情報の共有を速やかに行うことが求められる
- ✓ 先行的に始まったISACの知見やノウハウの展開を通じて、重要インフラ分野等におけるISACの立ち上げを促進することが必要

4 公衆無線LANのセキュリティ対策

- ✓ 公衆無線LANサービスの利用者及び提供者に対し、公衆無線LANのセキュリティ対策の状況や自ら講じるべきセキュリティ対策の周知を強化するため、ガイドラインを年度内に改定し、ホテル、病院、学校等への周知を強化することが必要

5 制度的枠組みの改善

- ✓ サイバーセキュリティ対策等の法令への位置づけや、官民のガイドラインや基準について周知し、対応の強化を呼びかけていくことが必要
- ✓ 放送設備のサイバーセキュリティ確保に関する省令改正を速やかに実施することが必要
- ✓ 各地方公共団体における情報セキュリティ対策及び緊急時連絡体制の確保等の徹底を図ることが必要

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

➢ 巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月より、情報通信研究機構（ＮＩＣＴ）の「ナショナルサイバートレーニングセンター」において演習等を実施。

CYDER（サイダー）

国・地方公共団体・独法・重要インフラ事業者等を対象とした実践的サイバー防御演習

⇒ 年間100回、計3,000名規模で実施（１日コース＆全都道府県で開催）
令和２年度からは、攻防型の準上級コースや、オンライン受講を新設予定

cyber colosseo（サイバーコロッセオ）

2020年東京大会関連組織のセキュリティ担当者等を対象とした実践的サイバー演習

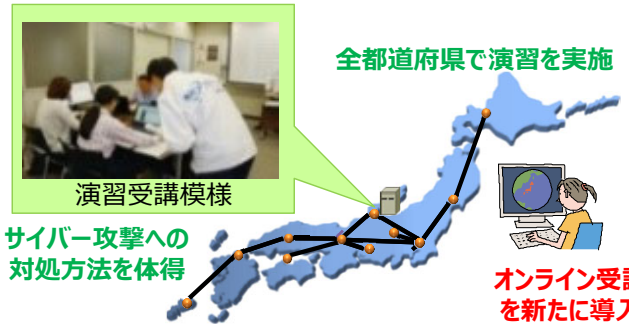
⇒ 平成29年度は延べ74名、平成30年度は延べ137名が受講
今年度は延べ最大400名規模で実施予定（令和２年度も大会直前まで実施予定）

SecHack365（セックハック365）

25歳以下の若手セキュリティイノベーターの育成

⇒ 平成29年度は39名、平成30年度は46名が1年間のコースを修了
今年度は46名を受講者として選定（令和２年度も50名程度の受講者を選定予定）

新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発



実事案に対処可能な人材育成
CYDER

攻防側コースを新設
ノウハウを活用

高度な攻撃に対処可能な人材育成
サイバーコロッセオ

ハイレベル層の人材育成
SecHack365

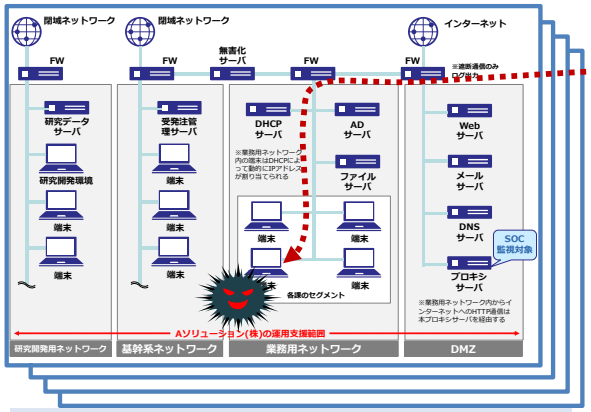
実践的サイバー防御演習（CYDER）

CYDER：CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**(**CYDER**)を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回**・計**3,000名規模**で実施。
  ※平成29年度は、年間100回・3,009名が受講。平成30年度は、年間107回・2,666名が受講。

演習のイメージ

NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した**最新の演習シナリオ**をコースごとに用意。



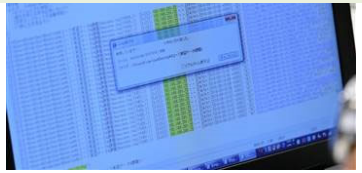
実際の**大規模LANを模した環境**を、**受講チームごと**に専用環境として**構築**

擬似攻撃者

NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用

演習実施模様
専門の指導員による補助

機材・データを使用して**本番同様の作業**を実施



インシデント（事案）対処能力の向上

令和２年度の実施計画（調整中）

コース	受講対象組織	対象者	開催地	開催回数	実施時期
A-1コース（初級）	地方公共団体	システムの運用担当者（システムの利用者レベルを含む）	４７都道府県	２０回程度	４月下旬～７月
A-2コース（初級）	全組織共通			４０回	７月以降
B-1コース（中級）	地方公共団体	セキュリティ管理業務を主導する立場の者	全国１１地域	２０回	秋以降
B-2コース（中級）	国の機関等、重要インフラ事業者等		東京・大阪・名古屋	１５回	秋以降

オリパラ前に未受講自治体に集中実施

緊急提言本文　CYDER関係部分抜粋

（１）地方公共団体向け実践的サイバー防御演習（CYDER）の繰り上げ実施等

ア　背景と課題

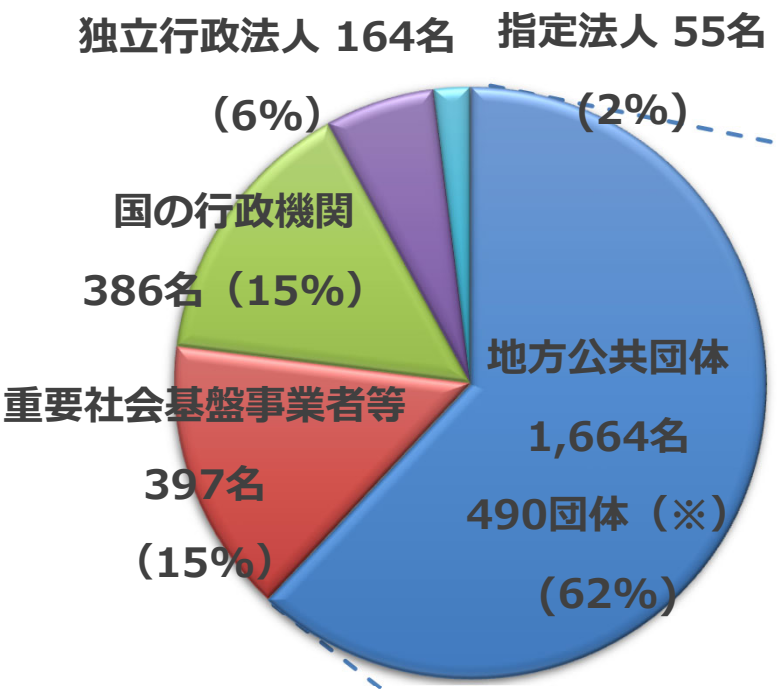
④　国の行政機関等についてはCYDERの未受講数が過去３年間で急速に減少し、ほぼ全ての機関が受講しているところである。一方、国と同様に個人情報をはじめとする重要な情報を取り扱う地方公共団体については、開催日程の同一地域内での分散化や、県庁等所在地以外での演習の実施といった受講しやすい環境を整える取組を行ってきたものの、**依然として半数近くの地方公共団体が未受講の状況**である。

イ　とるべき対策

②　**都道府県ごとにCYDER未受講の地方公共団体を対象とした受講計画を作成**した上で、当該地方公共団体を念頭においた**集中的な受講機会を2020年度第１四半期に設ける**ことが望ましい。その際には、地方公共団体に加えて、人材育成に課題を抱える地域の関係者においても可能な限り対象を広げていくことが求められる。

実践的サイバー防御演習（CYDER）の受講実績（2018年度）

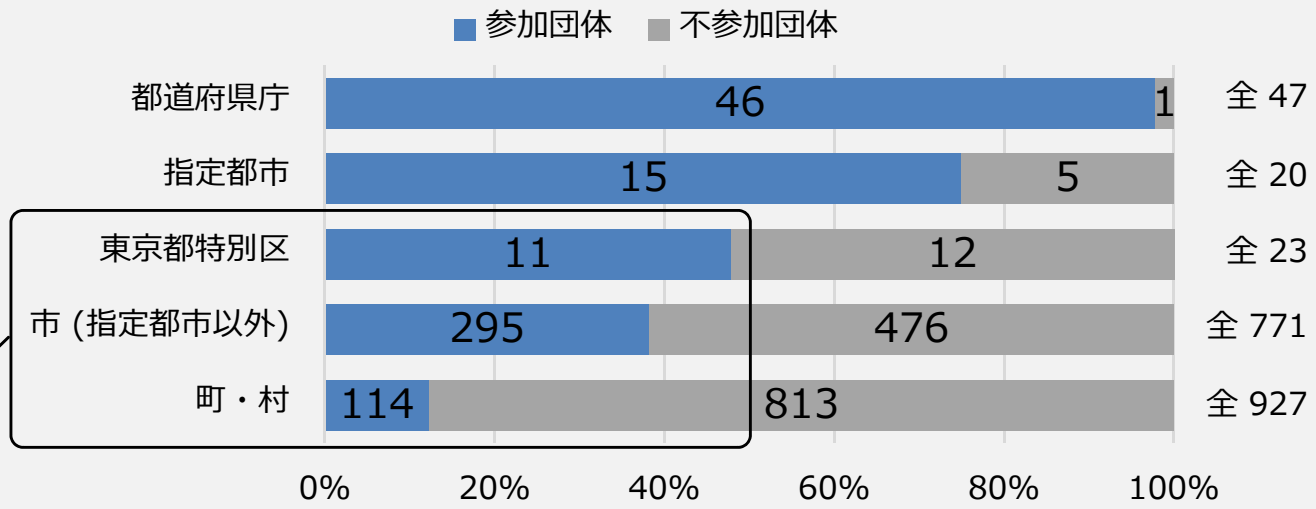
① 組織別の受講者数（全コース総数2,666名）



（※）地方公共団体481団体に加え、医療広域連合等９団体が受講

東京都特別区及び市は
半数以下であり、
町・村は12%

②地方公共団体（全1,788団体中481団体が受講）



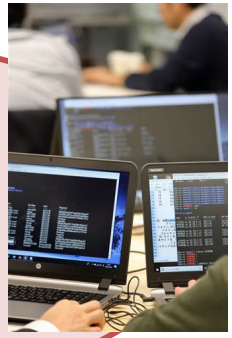
2020年東京大会に向けた実践的サイバー演習（サイバーコロッセオ）

- 近年さらに高度化・多様化するサイバー攻撃に備え、2020年東京オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象**とした、**高度な攻撃に対処可能な人材の育成**を行う実践的サイバー演習「**サイバーコロッセオ**」を平成30年２月から本格的に実施。
- 実機演習を伴う**コロッセオ演習**を補完する形で、演習時以外にも学習可能な**学習コンテンツ**を提供するとともに、**講義演習形式**によりセキュリティ関係の知識や技能を学ぶ**コロッセオカレッジ**を開設。
- **コロッセオ演習**として、**令和元年度は**、初・中級コース各125名、準上級コース150名の**計400名**、**令和２年度は**、大会直前までに初・中級コース各50名、準上級コース75名の**計175名**を予定。（人数は延べ受講定員数）

イメージ図

コロッセオ演習

実機演習を伴っての演習
（攻防型演習を含む）



- 大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を忠実に再現した、仮想のネットワーク環境を構築
- 仮想のネットワーク環境上で、東京2020大会時に想定されるサイバー攻撃を擬似的に発生させ、攻撃・防御手法の検証及び訓練を実施

学習コンテンツ

コロッセオ演習当日
以外でも学習可能な
コンテンツを提供

コロッセオカレッジ

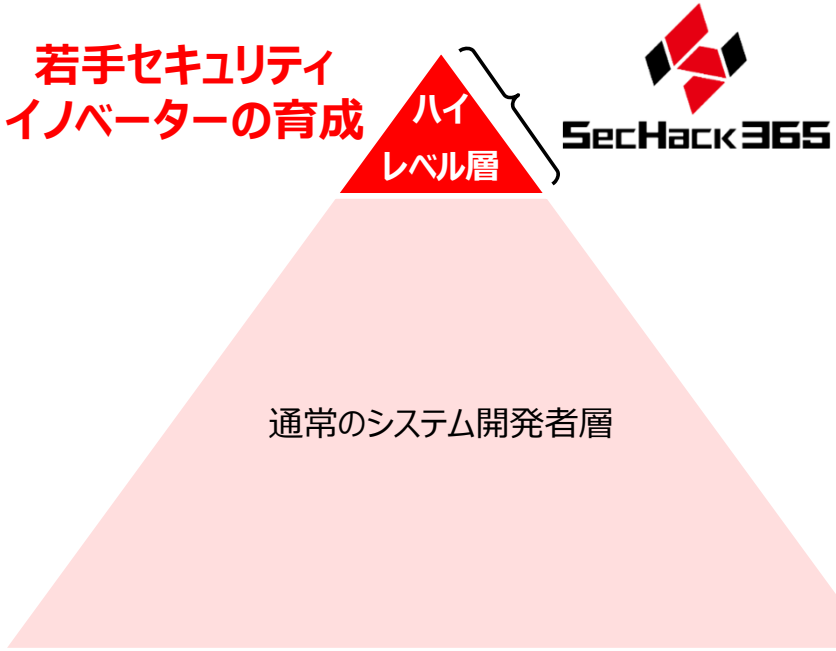
講義演習形式により
セキュリティ関係の
知識や技能を学習

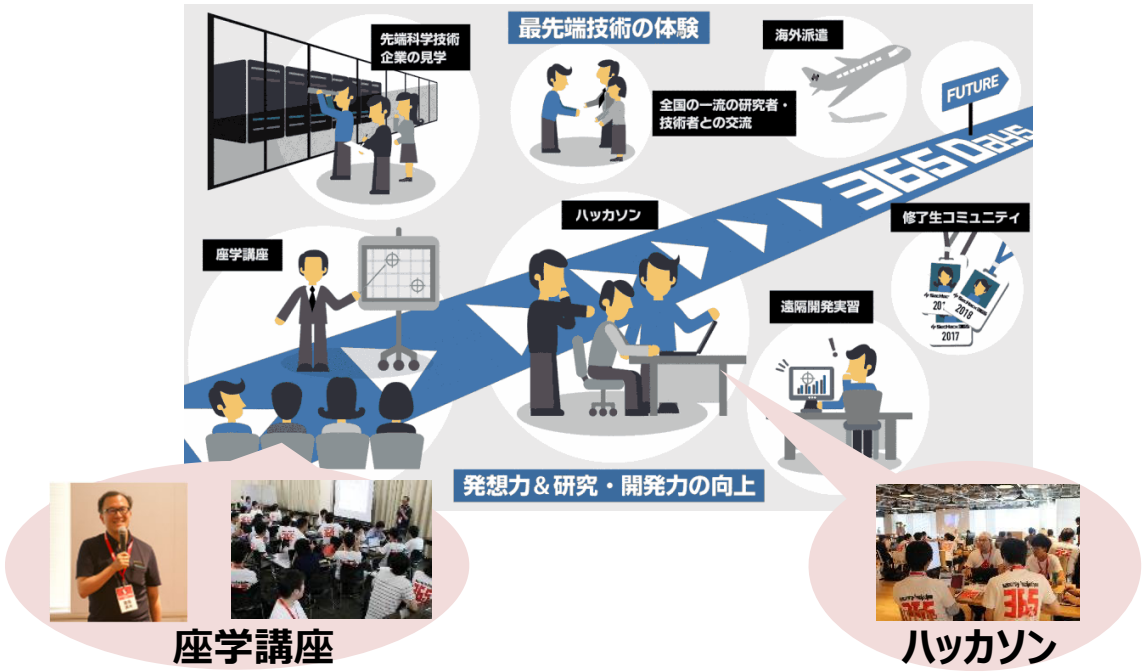
2020年東京オリンピック・パラリンピック競技大会のサイバーセキュリティを確保

SecHack365

- **未来のサイバーセキュリティ研究者・起業家の創出**に向けて、NICTの持つサイバーセキュリティの研究資産を活用し、**若年層のICT人材を対象**に実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、**第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導**。
- 対象者は、日本国内に居住する**25歳以下の若手ICT人材**（2017年度は39名、2018年度は46名が修了）。
- 受講者は、NICTの有する遠隔開発環境※を活用し、**年中どこからでも遠隔開発実習が可能**。また、集合イベントとして、**座学講座（研究倫理）**や**ハッカソン等**を実施。

※ NONSTOP（NICTER Open Network Security Test-out Platform）では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができ、NONSTOP内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組むことが可能。





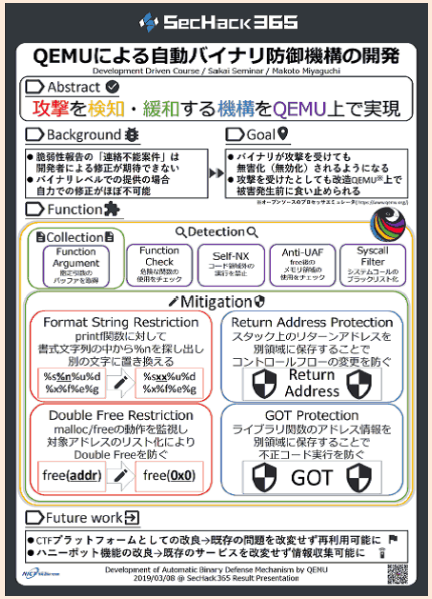
通年の遠隔開発実習＋年６回の集合研修（座学講座・ハッカソン等）の組合せによる総合的な人材育成プログラム

SecHack365の主な成果（例）

〈2018年度の優秀修了生の成果〉

題名	概要
QEMUによる 自動バイナリ防御機構の開発	プログラムの脆弱性が適時に修正されない場合に備え、攻撃者の典型的な挙動を検知し、無効化する仮想環境（QEMU）を構築し、攻撃を受けても被害発生前に食い止めることを目指した。
NFCとWebUSBを用いた Webアプリ用認証システム	WebUSB（Web を通じたUSB デバイスへのアクセス）とNFCカードリーダー（Suicaなどの近距離無線通信規格）を用い、Webブラウザでの ICカード認証の機構を製作。
Exgdb ～GDBを用いた 動的なバイナリ解析の効率化～	CTF(Capture The Flag：コンピューターのハッキング技術を競うコンテスト）において、より効率的に利用できるGDB（プログラムの不具合の原因を調べるためのツール）を開発。
安心・安全なSNS	近年増加するSNSトラブルに着目し、SNSを安全に使えるよう、個人情報に関係する画像や文章を分析し、投稿する前に警告するソフトウェアを開発。
セキュリティ機能を持つ 組込み向けハイパーバイザの開発	組込み向けハイパーバイザ（1台の機器で複数の仮想OSを動かせるソフトウェア）について、セキュリティ機能の実装に関する開発。
CanSatをはじめよう	CanSat（カンサット：飲料水の缶サイズの小型の模擬人工衛星）の初心者向けの標準的な機能を搭載したハードウェアキットと開発を学習できるサポートWebページを開発。

QEMUによる
自動バイナリ防御機構の開発



（概要）

プログラムの脆弱性が適時に修正されない場合に備え、攻撃者の典型的な挙動を検知し、無効化する仮想環境（QEMU）を構築し、攻撃を受けても被害発生前に食い止めることを目指す。

地域におけるサイバーセキュリティ人材育成

- サイバーセキュリティ人材は、地方においては首都圏以上に不足している状況。これを踏まえ、総務省では、「サイバーセキュリティタスクフォース・人材育成分科会」において課題と対応方策の検討を実施。
- 2019年６月に「第１次取りまとめ」を公表するとともに、地域のコミュニティや企業、教育機関等と連携して新たなスキームによる人材育成の方策を実証するためのモデル事業を2019年10月から実施。

１．研修リーダーの不在

気づきの機会がない
悪循環
研修があっても参加者が少ない
地方で研修が開催されない

２．組織体制の不足

何をすればよいかわからない
悪循環
専門人材を雇用できない
対策が進まない

３．就業機会の不足

雇用の受け皿がない
悪循環
地域の若年層がセキュリティ人材を目指さない
地域におけるセキュリティ人材がさらに不足

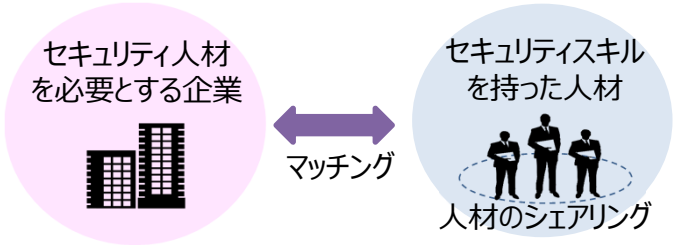
１．地域のセキュリティリーダーの育成

愛知県を中心に実施

○ **地域のコミュニティ活動を活性化し、中核としてリードする人材を育成**。

２．地域でのセキュリティ人材のシェアリング

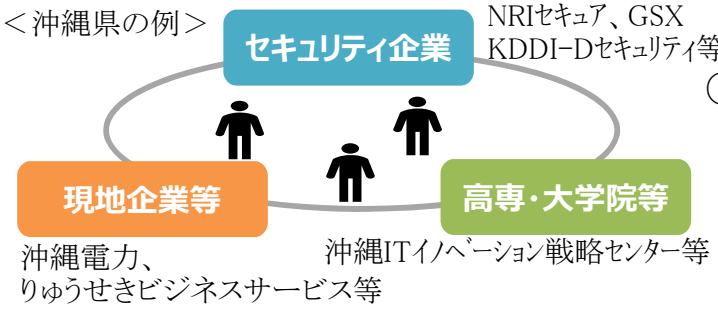
関西地方にて実施



○ 県や広域エリアにおいて、複数の中小企業等が**セキュリティ専門家をシェアできるようにマッチング**。

３．地域におけるセキュリティ人材のエコシステムの形成

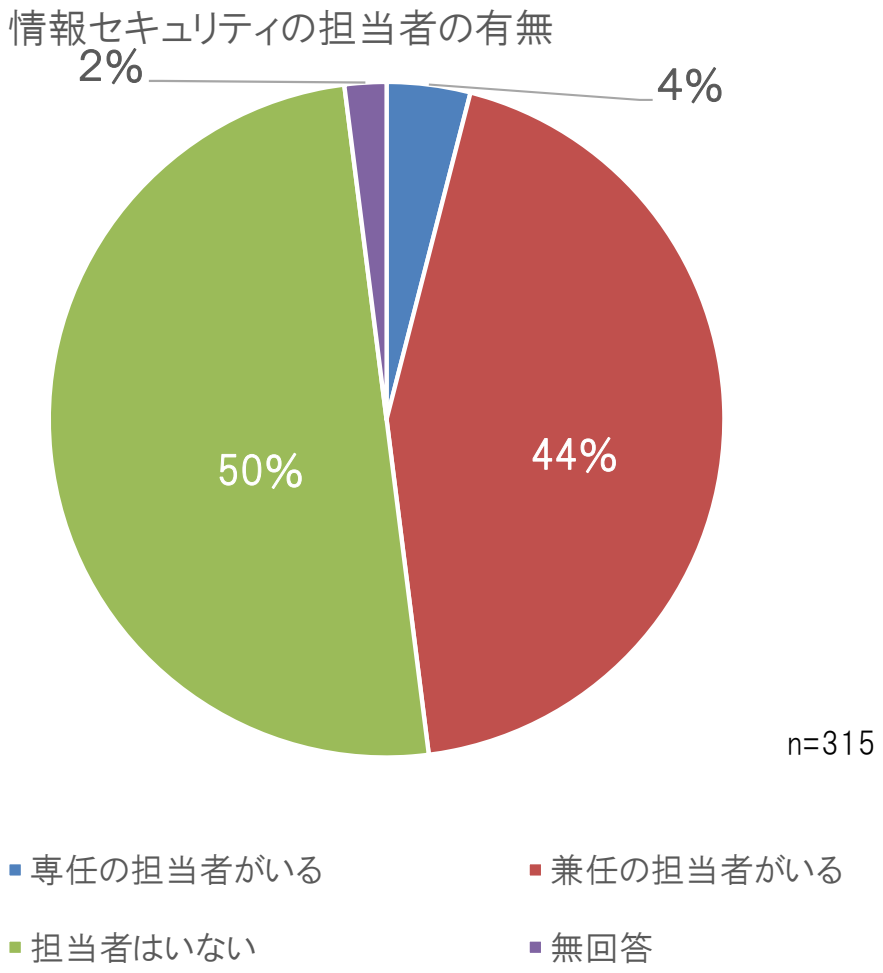
沖縄にて実施



○ 地域の企業や教育機関と連携し、就業の場の確保と**就業につながる研修を行うことで、地域のセキュリティ人材のエコシステムを形成**。

情報セキュリティの担当者の有無

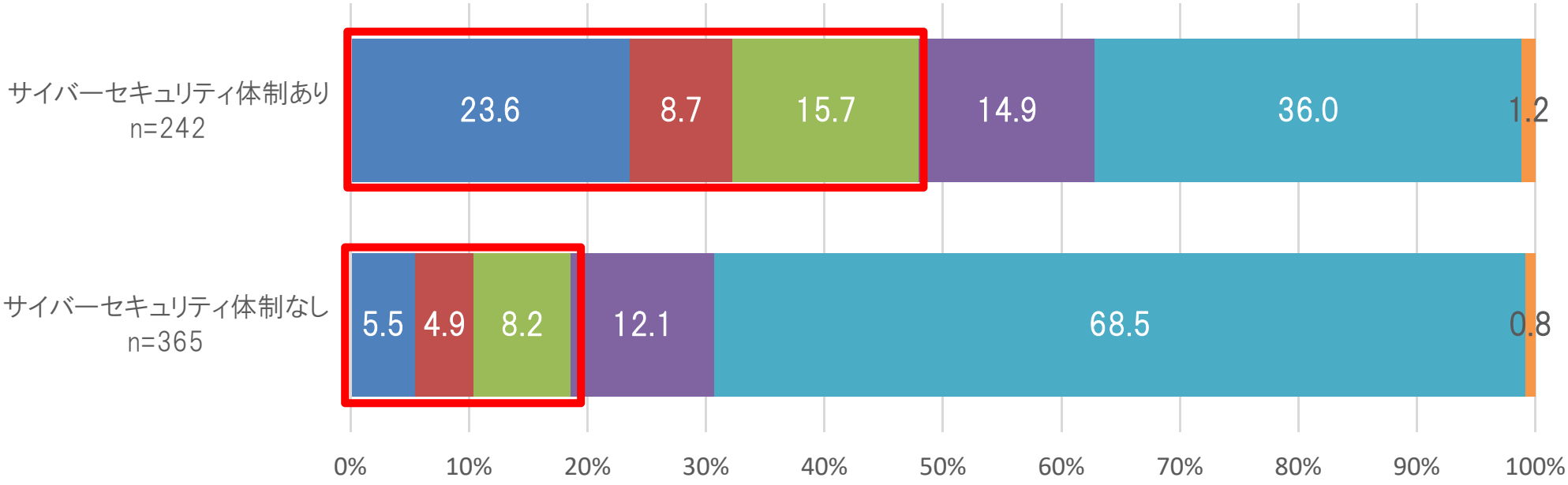
○　中小企業の過半数で、情報セキュリティ担当者がいない。担当者がいる場合でも、4割が他の業務との兼任。



出典：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」（2017年6月）をもとに総務省作成
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf

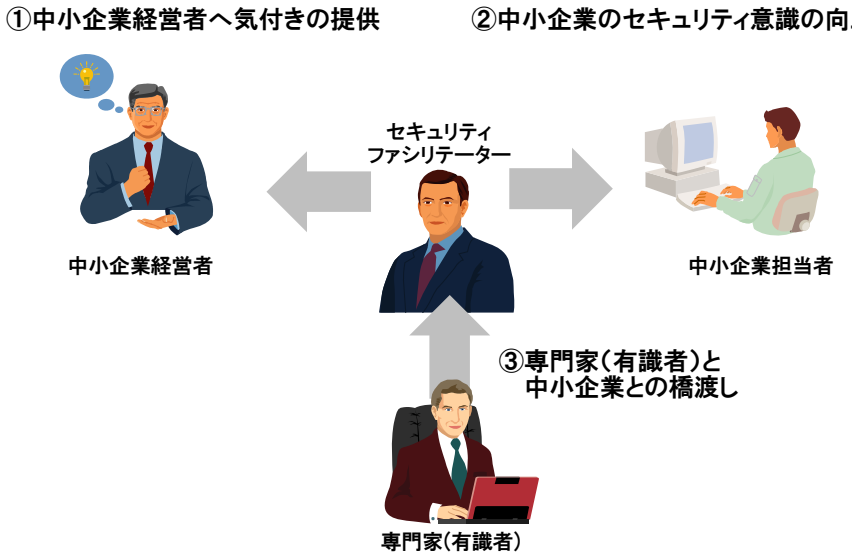
セキュリティ・インシデント発生時の訓練実施状況

○　サイバーセキュリティ体制の有無で比較すると、体制のある組織・企業では、「訓練を実施している（IT以外の部門も参加）」、「訓練を実施している（IT部門のみ）」、「訓練を一部実施している」の合計が48.0%と半数近い。一方、体制が無い場合には、同合計が18.6%となっており、30ポイント近い差が出ている。



出典：MS&ADインターリスク総研「企業の情報セキュリティ対策に関する実態調査報告書」（2018年12月）をもとに総務省作成

地域のセキュリティリーダー（ファシリテーター）の育成



セキュリティファシリテーター
に求められるスキル

中小企業に必要な セキュリティ知識	
中小企業経営者 との コネクション	モチベーション ・意義あり

研修	内容	対象	時間
セキュリティファシリテーターの役割と必要な基礎スキル研修	• セキュリティファシリテーターとしての役割や必要なセキュリティ基礎知識を学びます。 • セキュリティファシリテーターが、中小企業の抱える問題を引き出すスキルを学びます。	すべてのセキュリティファシリテーター	3時間
IoT等のセキュリティ対策の重要性を意識づける**研修**	• IoT化による中小企業等のメリットを学びます。 • IoT化に伴い考えるべきセキュリティ対策とセキュリティ対策の不備による被害について学びます。 • 中小企業等にとってセキュリティ対策がメリットとなる事がわかるセキュリティ対策支援制度を学びます。 • ビデオコンテンツを活用し、研修内容を効果的に学びます。	中小企業の経営者と会話するセキュリティファシリテーター	3時間
サイバー攻撃の最新脅威等を学ぶ**研修**	• サイバー攻撃事の最新脅威を学びます。 • ビデオコンテンツを活用し、研修内容を効果的に学びます。	中小企業の担当者と会話するセキュリティファシリテーター	3時間
ロールプレイ**研修**	• 中小企業等が抱える問題の課題解決方法をロールプレイ演習を通して学びます。 • コミュニティ形成を目的とした意見交換会を実施します。	すべてのセキュリティファシリテーター	3時間

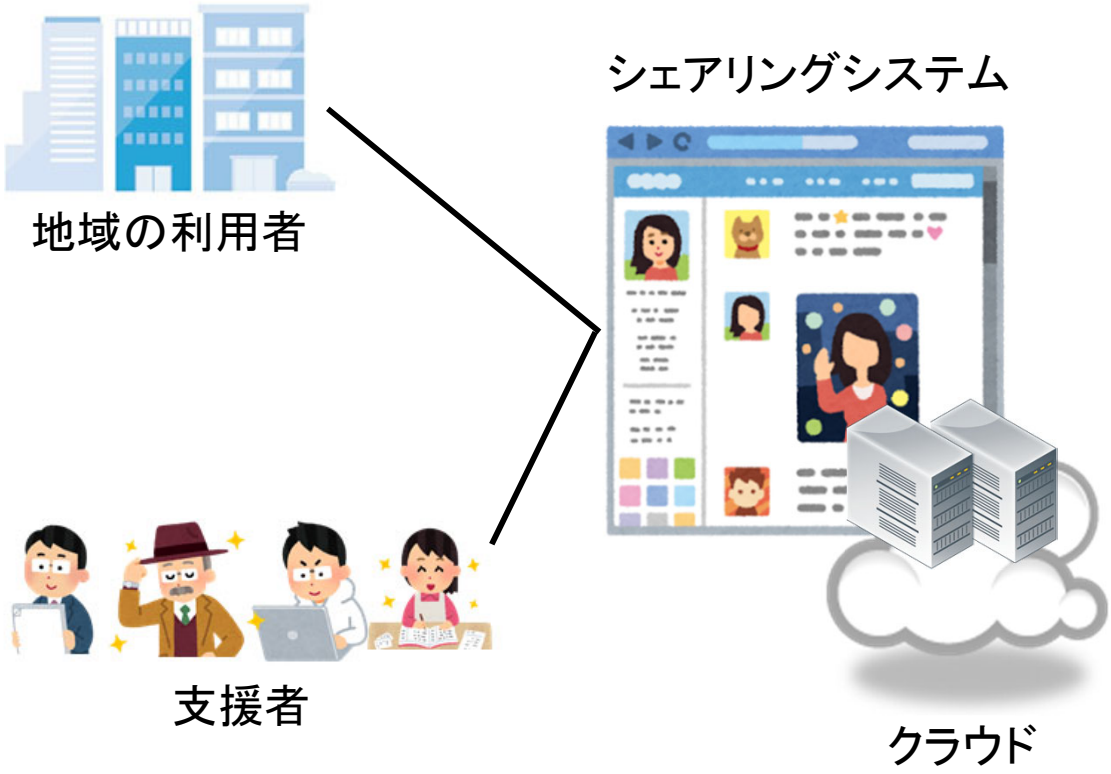
愛知県を中心に実施（(株)日立製作所が受託）

地域でのセキュリティ人材のシェアリング

- 利用者が地域のセキュリティ人材（支援者）をシェアするシステムをクラウド上に構築
- シェアリングシステムを通じて、利用者が抱える情報セキュリティの課題と、支援者のセキュリティスキルを組み合わせることで、組織が抱える情報セキュリティ上の課題解決を支援

調査検討会の構成員

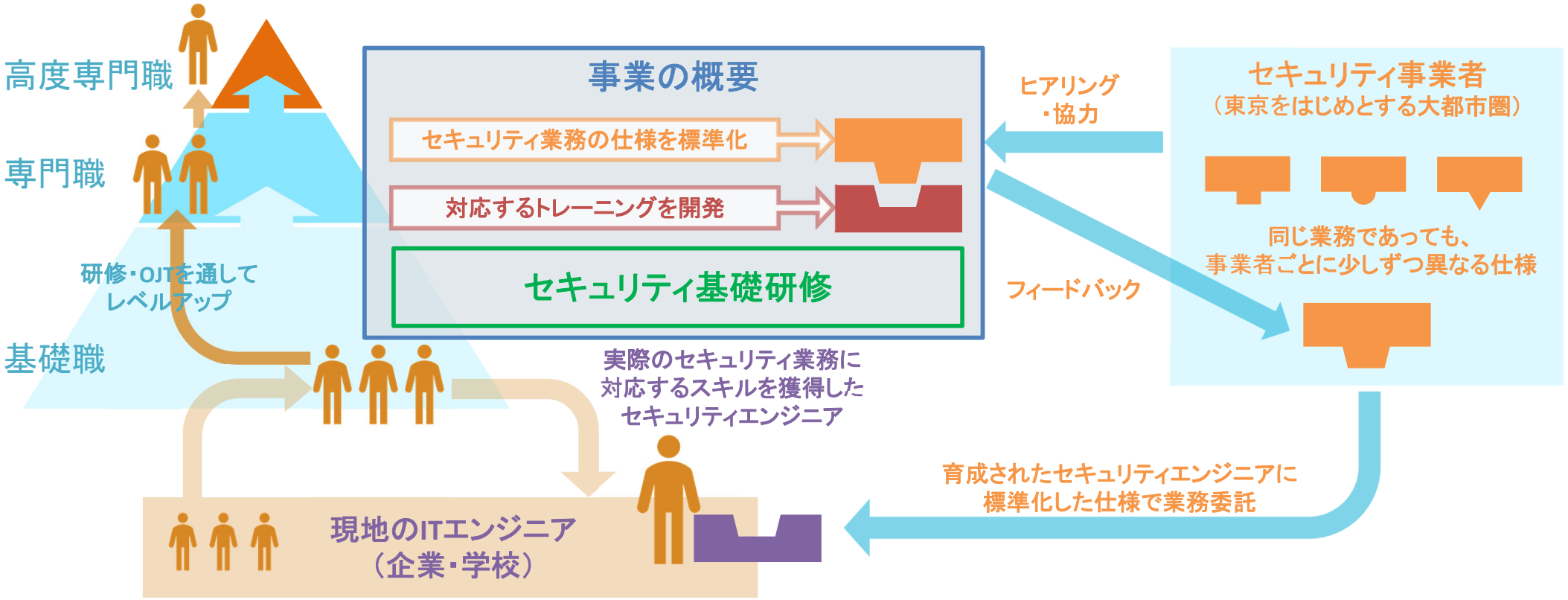
氏名（敬称略）	所属
森井　昌克（座長）	神戸大学
池田　耕作	（株）オージス総研
石橋　裕基	一般財団法人関西情報センター
窪田　敏明	（株）神戸デジタル・ラボ
嶋倉　文裕	NPO 日本ネットワークセキュリティ協会
竹中　篤	一般財団法人関西情報センター
谷本　重和	（株）アシックス
古川　佳和	大阪商工会議所



関西地方にて実施（グローバルセキュリティエキスパート(株)が受託）

地域におけるセキュリティ人材のエコシステムの形成

- セキュリティ事業者ごとに異なる業務仕様を、業務毎に標準化し、対応するトレーニングを開発
- 地方を拠点に、現地のITエンジニアに集中的にトレーニングを提供し、業務遂行できるスキルを身につけたセキュリティエンジニアを育成
- セキュリティ事業者は、標準化した業務仕様に基づき業務委託が可能



沖縄にて実施（NRIセキュアテクノロジーズ(株)が受託）

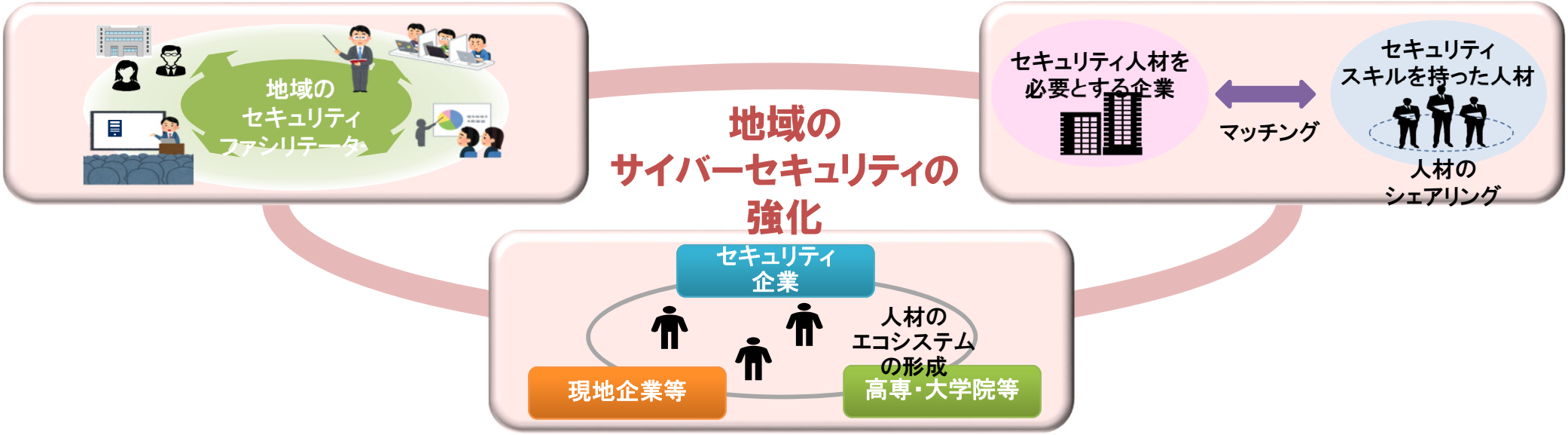
むすび

○ Society5.0がもたらすメリットを地域が享受するためには、その基盤として地域におけるセキュリティ活動の活性化が不可欠である。

○ 具体的には、

- 地域におけるセキュリティファシリテーターの育成の取組を通じて、地域全体で面的にサイバーセキュリティの関心を高めること
- サイバーセキュリティに関心を持った個別の中小企業等が専門家や専門組織を地域でシェアしながら、効率的に活用する仕組みの構築
- それぞれの地域で活動を支える人材が育つエコシステムの形成

が求められる。



○ セキュリティ対策においては、自助、共助、公助のバランスが求められる中で、地域における共助が全体を繋ぐ要となり得る。

ご清聴ありがとうございました。