資料36－3－1

総務省における人材育成・普及啓発等の現状と課題

令和4年3月

サイバーセキュリティタスクフォース事務局

① 人材育成

- ①－１ CYDER
- ①－２ SecHack365
- ①－３ 地域におけるセキュリティ人材育成

② 普及啓発

- ②－１ テレワークのセキュリティ
- ②－２ 無線LANのセキュリティ
- ②－３ 地域セキュリティコミュニティの形成
- ②－４ 国民のための情報セキュリティサイトの改修
- ②－５ その他の普及啓発施策

③ フィッシング対策

前回タスクフォースの振り返り

総務省におけるこれまでの取組（前回タスクフォース資料抜粋）

○CYDER

・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、2017年度から、行政機関等の実際のネットワーク環境を模した大規模仮想LAN環境を構築の上、国の機関等、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（全都道府県で年間100回、計3,000名規模。2020年度までに延べ11,413名が受講）。

・2021年度から、地理的・時間的要因等によりCYDERが受講できない者への対応としてオンラインAコース、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」の実施結果を踏まえたCコースをそれぞれ提供開始。

○SecHack365

・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、2017年度から、25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材（セキュリティイノベーター）を育成する「SecHack365」を実施（これまでに合計171名が修了）。

○地域におけるセキュリティ人材育成

・地域において、民間による雇用の受け皿創出の動きに合わせ、就業の場の確保と就業につながる研修を一体的に行い、地域における人材エコシステムの形成を図るモデル事業を実施するとともに他地域への展開の可能性を検証。

前回タスクフォースでお寄せいただいた意見（抜粋）

- ✓ 戦略マネジメント層においては技術と安全保障の両面の知識と技術が必要。総務省における法令や技術基準の改正等について、安全保障の方面の人々にも分かりやすく説明していく必要があるのではないか。（林構成員）
- ✓ 育成ターゲットとして、戦略マネジメント層・経営層が特に重要。教育プログラム受講後も最新の情報を提供する活動を検討されたい。（藤本構成員）
- ✓ 地域における人材育成エコシステムが継続的に機能し、人材が拡大再生産されるようにするにはどうするべきか。（園田構成員ほか）

① 人材育成

①－１ CYDER

①－２ SecHack365

①－３ 地域におけるセキュリティ人材育成

② 普及啓発

②－１ テレワークのセキュリティ

②－２ 無線LANのセキュリティ

②－３ 地域セキュリティコミュニティの形成

②－４ 国民のための情報セキュリティサイトの改修

②－５ その他の普及啓発施策

③ フィッシング対策

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）
2017年度以降で、延べ**13,867名**が受講
2021年度から、オンラインコースを開設するとともに、準上級コースを開設

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

⇒ 2017年度から開始し、2020年12月で事業完了
期間中に、**演習形式**で延べ**571**名、**講義形式**で延べ**1,717名**の人材を育成

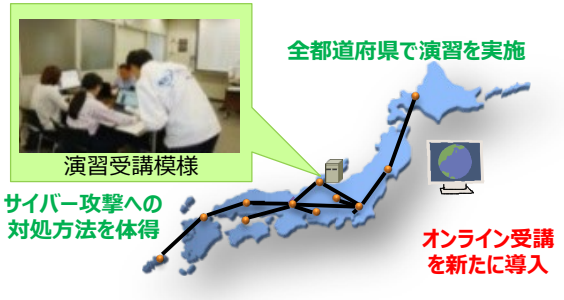
サイバーコロッセオのレガシーとして、準上級コースを制作

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

⇒ **年間50名程度**の受講者を選定し、**１年間のトレーニング**コースを実施
2017年度以降で、計**212名が修了**

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

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）

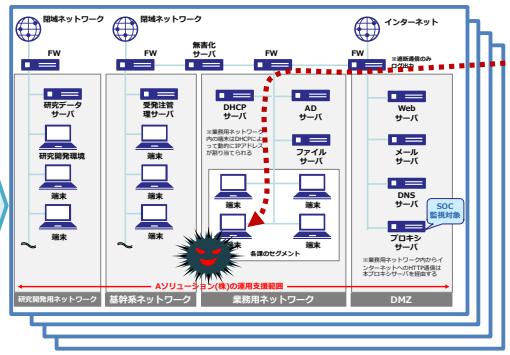
CYDER：CYber Defense Exercise with Recurrence

- 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、**外部のセキュリティ事業者の支援を受けることを前提とし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。 参加申込 → https://cyder.nict.go.jp
  ※2017年度:100回・3,009名、2018年度:107回・2,666名、2019年度:105回・3,090名、2020年度:106回・2,648名、2021年度:105回・2454名

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

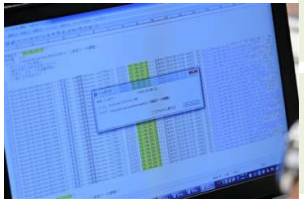
北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**



演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和３年度の実施計画

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	６８回	７月～翌年２月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国１１地域	２１回	10月～翌年２月
B-2				地方公共団体以外	東京・大阪・名古屋・福岡	１３回	翌年１月～２月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	３回	翌年１月～２月
オンラインA	ｵﾝﾗｲﾝ演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	(受講者職場等)	随時	11月～翌年２月 (6~8月に試験提供)

令和３年度から新規開設

CYDER開催スケジュール（令和3年度）

Aコース（初級）（全組織共通）

地域	開催県	開催日	
北海道	北海道	10/14 札幌	11/05 釧路
東北	青森県	9/22 青森	
	岩手県	9/14 盛岡	
	宮城県	8/17 仙台	10/26 仙台
	秋田県	10/22 秋田	
	山形県	10/01 山形	
	福島県	10/08 郡山	
関東	茨城県	10/19 水戸	
	栃木県	9/17 宇都宮	
	群馬県	7/27 前橋	
	埼玉県	8/20 さいたま	
	千葉県	9/14 習志野	
	東京都	7/20 東京	9/22 東京
		10/13 東京	10/21 東京
		11/10 東京	12/09 東京
		1/21 東京	1/27 東京
		2/02 東京	2/09 東京
		2/16 東京	
	神奈川県	10/05 横浜	1/28 横浜
	山梨県	9/07 甲府	
信越	新潟県	9/17 新潟	
	長野県	8/24 松本	11/12 佐久
北陸	富山県	11/19 富山	
	石川県	8/31 金沢	
	福井県	11/09 福井	
東海	岐阜県	10/15 岐阜	
	静岡県	11/17 静岡	
	愛知県	7/30 名古屋	10/29 名古屋
		12/03 名古屋	
	三重県	8/05 津	

地域	開催県	開催日	
近畿	滋賀県	12/10 大津	
	京都府	8/27 京都	
	大阪府	8/03 大阪	9/10 大阪
		10/22 大阪	12/14 大阪
	兵庫県	9/03 神戸	
	奈良県	12/03 橿原	
	和歌山県	11/02 和歌山	
中国	鳥取県	11/16 倉吉	
	島根県	11/05 浜田	
	岡山県	10/12 岡山	
	広島県	10/01 広島	1/14 福山
	山口県	12/17 山口	
四国	徳島県	12/07 徳島	
	香川県	12/17 高松	
	愛媛県	1/18 松山	
	高知県	11/10 高知	
九州	福岡県	9/29 福岡	1/25 福岡
	佐賀県	11/02 佐賀	
	長崎県	10/07 長崎	
	熊本県	10/05 熊本	
	大分県	11/19 大分	
	宮崎県	1/12 宮崎	
	鹿児島県	11/26 鹿児島	
沖縄	沖縄県	10/29 那覇	

B-1コース（中級）（地公体向け）

開催地域	開催日	
北海道	11/25 札幌	
東北	11/25 仙台	12/22 盛岡
関東	10/14 東京	11/11 東京
	1/14 東京	2/17 東京
信越	12/24 新潟	
北陸	11/30 金沢	
東海	10/19 名古屋	1/25 名古屋
近畿	10/26 大阪	11/16 大阪
	12/21 大阪	2/04 大阪
中国	1/19 岡山	2/09 広島
四国	2/15 松山	
九州	12/14 熊本	2/15 福岡
沖縄	2/04 那覇	

B-2コース（中級）（国・重要インフラ）

開催地域	開催日	
関東	1/13 東京	1/20 東京
	1/26 東京	1/28 東京
	2/01 東京	2/03 東京
	2/08 東京	2/10 東京
	2/18 東京	2/25 東京
東海	2/01 名古屋	
近畿	1/21 大阪	
九州	2/10 福岡	

Cコース（準上級）（全組織共通）

開催地域	開催日			
関東	1/18 ~19	東京	2/21 ~22	東京
	2/24 ~25	東京		

オンラインAコース（初級）（全組織共通）

オンラインにより受講可能なコースを2021(令和３)年11月９日～翌2022(令和４)年３月４日まで提供
※開講に先立ち、オープンβによる試行を６月中旬から８月にかけて実施

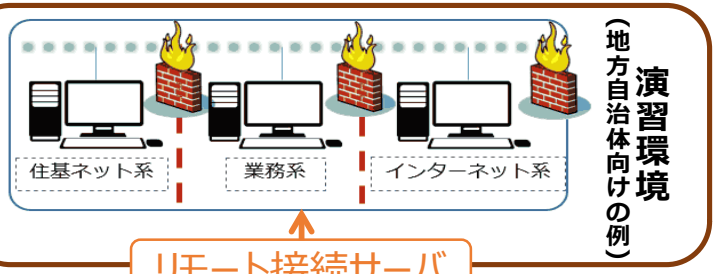
CYDERオンラインコースの実施

- **感染症拡大防止対策**として、また、**地理的・時間的要因**等によりCYDERが受講できない方への最低限の対応として、**オンライン受講環境**を**整備**。
- 自組織のパソコンの**Webブラウザから演習環境に接続**し、**eラーニング方式**により演習を**受講**。
- 2021年８月まで試験提供を実施し、改修を加えた上で、**同年11月から正式提供**。

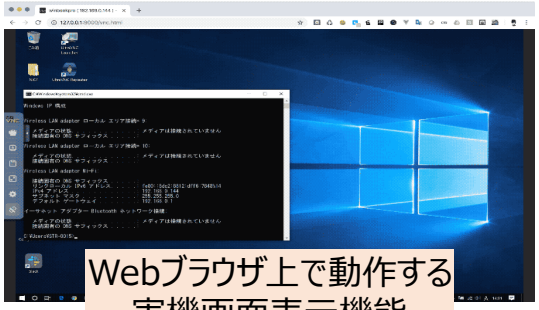
※実施期間: 2021年11月9日～2022年３月４日

- **641名**が受講修了、**771名**が申込（令和３年度）。

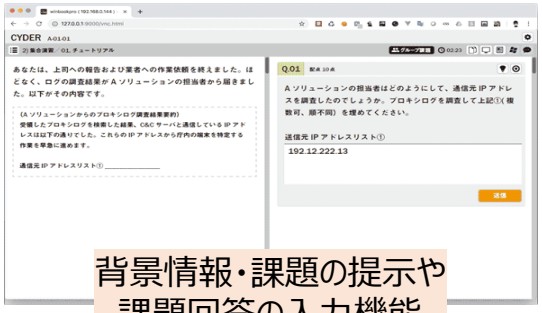
NICT内の大規模計算環境



自身のPC上の**Webブラウザ**において**遠隔受講機能**を利用可能



Webブラウザ上で動作する実機画面表示機能



背景情報・課題の提示や課題回答の入力機能

解説表示機能やチュートリアル表示機能

サイバーコロッセオの知見を活用したCYDER Cコースの実施

- 2020年度まで実施した「サイバーコロッセオ」のレガシー(遺産)のうち中級A, Bを、CYDERのCコース(準上級)として、2022年1月、2月に計３回開催
- コロッセオでは1日間で提供していたコースを2日間に延長し、演習スケジュールに余裕を持たせることで、受講者がしっかりと技術を習熟できるように工夫
- **72名**が受講修了、**109名**が申込（令和３年度）。

コースの具体的内容

1回目: Web系を主とした攻撃と対処【2022年1月】

脆弱性のあるWebサイトへの攻撃や攻撃ツールを利用した攻撃体験と攻撃解析を通じて防御方法の検討を行う。

- Web系への攻撃を学ぶ
- 自チームから他チームを攻撃
- 各種攻撃ログの調査や分析を行う
  - ✓他チームの受講者が行った攻撃を解析
  - ✓受講者の攻撃以前に用意しておいた攻撃痕跡を解析

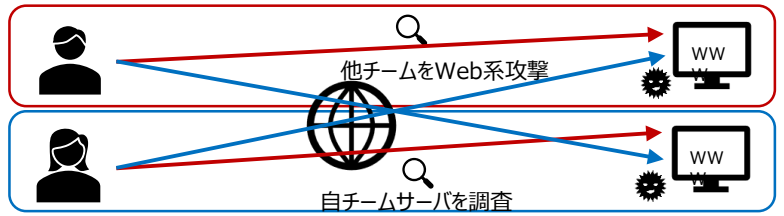
2, 3回目: パケット解析を主とした攻撃と対処【2022年2月】

外部公開サーバ経由での侵害を発端とする1つの大規模なインシデントを解き明かす。

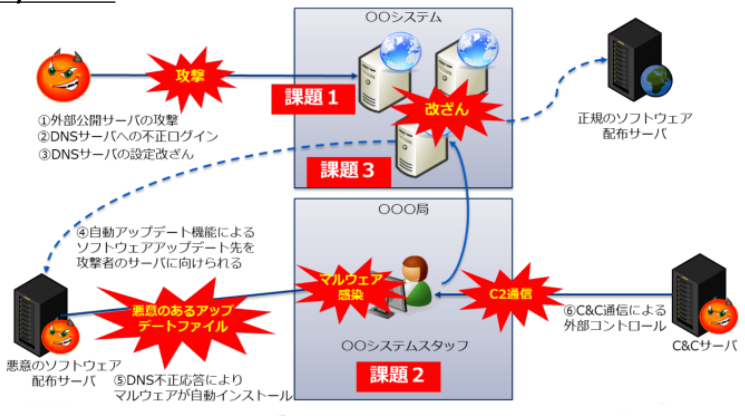
- 外部公開サーバへの侵害(サーバログ調査)
- クライアント端末のマルウェア感染
  - ✓Proxyログ解析
  - ✓ネットワークパケット解析
- 被疑サーバの調査

コース内容のイメージ

１回目



２, 3回目



CYDER開催スケジュール（令和4年度）（案）

Aコース（初級）（全組織共通）　計64回

地域	開催県	開催日	
北海道	北海道	8/23 札幌	10/7 帯広
東北	青森県	8/26 青森	
	岩手県	10/12 盛岡	
	宮城県	7/22 仙台	10/14 仙台
	秋田県	8/30 秋田	
	山形県	9/6 山形	
	福島県	9/15 郡山	
関東	茨城県	7/20 水戸	
	栃木県	9/9 宇都宮	
	群馬県	10/4 前橋	
	埼玉県	7/26 さいたま	
	千葉県	10/19 千葉	
	東京都	7/12 東京	8/5 東京
		9/13 東京	10/18 東京
		11/30 東京	12/07 東京
		1/17 東京	
	神奈川県	8/25 横浜	1/25 小田原
	山梨県	9/30 甲府	
信越	新潟県	9/2 新潟	
	長野県	7/29 長野	9/21 塩尻
北陸	富山県	10/7 富山	
	石川県	8/2 金沢	
	福井県	9/16 福井	
東海	岐阜県	10/12 岐阜	
	静岡県	8/9 静岡	
	愛知県	7/27 名古屋	9/27 名古屋
		12/08 名古屋	
	三重県	10/28 津	

地域	開催県	開催日	
近畿	滋賀県	8/4 大津	
	京都府	10/14 京都	
	大阪府	7/29 大阪	9/13 大阪
		11/8 大阪	12/13 大阪
	兵庫県	11/1 神戸	
	奈良県	11/18 奈良	
	和歌山県	10/25 和歌山	
中国	鳥取県	10/25 倉吉	
	島根県	10/18 出雲	
	岡山県	9/6 岡山	
	広島県	8/26 広島	11/8 広島
	山口県	8/9 山口	
四国	徳島県	10/28 徳島	
	香川県	9/9 高松	
	愛媛県	8/2 松山	
	高知県	10/21 高知	
九州	福岡県	8/23 福岡	2/7 福岡
	佐賀県	11/11 佐賀	
	長崎県	9/2 長崎	
	熊本県	8/30 熊本	
	大分県	8/5 大分	
	宮崎県	9/30 宮崎	
	鹿児島県	9/27 鹿児島	
沖縄	沖縄県	9/21 那覇	

B-1コース（中級）（地公体向け）　計20回

開催地域	開催日	
北海道	11/2 札幌	
東北	11/09 盛岡	11/17 仙台
関東	10/13 東京	12/1 東京
	12/8 東京	1/24 東京
信越	11/25 長野	
北陸	11/29 金沢	
東海	11/2 名古屋	12/9 名古屋
近畿	10/21 大阪	11/25 大阪
	12/14 大阪	
中国	11/15 岡山	11/22 広島
四国	11/11 高松	
九州	11/22 福岡	11/29 熊本
沖縄	11/16 那覇	

B-2コース（中級）（国・重要インフラ）　計13回

開催地域	開催日	
関東	1/12 東京	1/20 東京
	1/25 東京	1/27 未定
	1/27 東京	1/31 東京
	2/2 東京	2/7 東京
	2/10 東京	2/15 東京
近畿	1/31 大阪	2/14 大阪
東海	2/3 名古屋	

※九州地区（福岡）は、受講ニーズが低いため廃止

Cコース（準上級）（全組織共通）　計３回

開催地域	開催日	
関東	10/26~27	東京
	12/13~14	東京
	2/8~9	東京

オンラインコース（全組織共通）

オンラインにより受講可能なコースを時期を分けて開催
　第1期（5月中旬～7月中旬を予定）　　第2期（翌年1月～2月を予定）

出前CYDER及びCYDERサテライトの導入

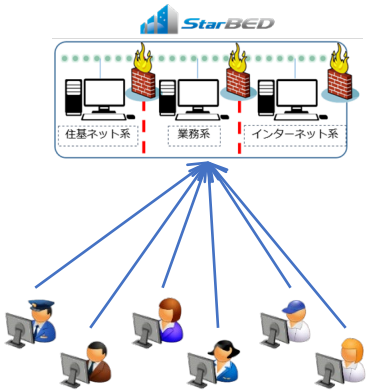
CYDER 集合演習【30人／回】

- 各会場に講師・補助者を手配して、実機演習環境を準備した上で実施

＋

CYDER オンライン演習

- 形態
  - ✓個人単位での遠隔接続による実機演習
  - ✓録画済み教材
  - ✓機材は受講者手配
- R3年度から本格実施



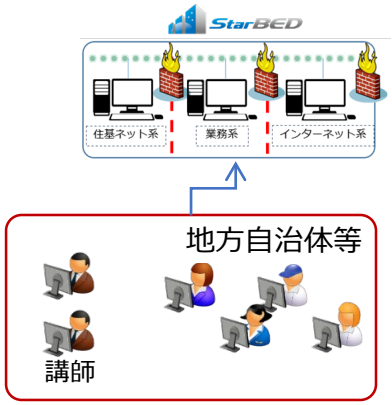
新規実施予定

小規模・柔軟化

出前CYDER【10 人／カ所】

2ヶ所

- ✓**未受講自治体の解消**にフォーカス
- ✓ 地方自治体等での遠隔接続による実機演習
- ✓ 講師が現地指導にてサポート
- ✓ 自治体等の受講者需要に応じて臨機応変に開催
- ✓ 機材貸与も選択可能

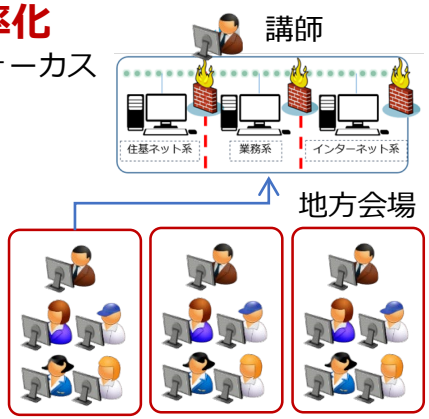


高効率化

CYDERサテライト

1ヶ所

- ✓**集合演習費用の効率化**（実施費用低廉化）にフォーカス
- ✓ サテライト会場からの遠隔接続による実機演習
- ✓ 講師は中央に、遠隔会場には補助者が支援
- ✓ ボトルネックの講師を柔軟に活用
- ✓ 機材貸与も選択可能



① 人材育成

①－１ CYDER

①－２ SecHack365

①－３ 地域におけるセキュリティ人材育成

② 普及啓発

②－１ テレワークのセキュリティ

②－２ 無線LANのセキュリティ

②－３ 地域セキュリティコミュニティの形成

②－４ 国民のための情報セキュリティサイトの改修

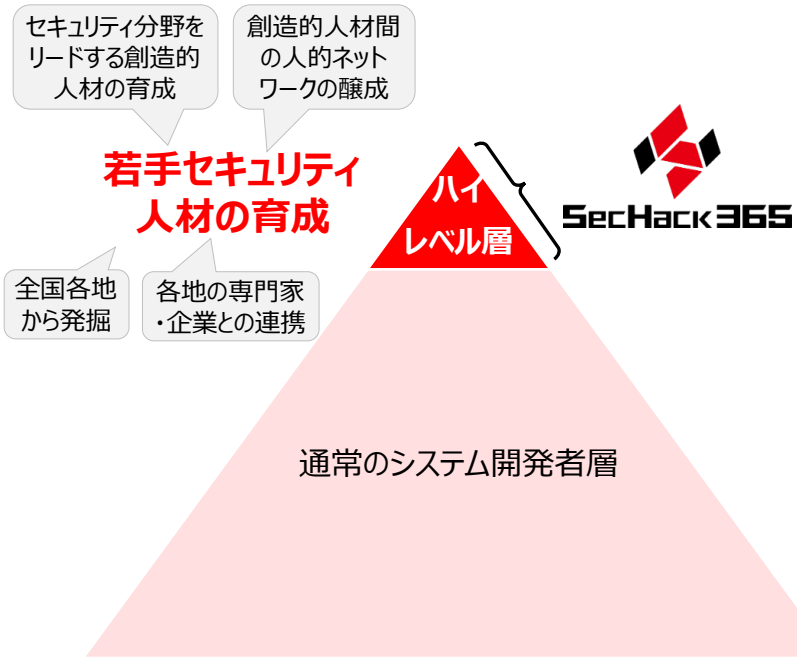
②－５ その他の普及啓発施策

③ フィッシング対策

SecHack365

- 日本国内に居住する**25歳以下の若手ICT人材を対象**として、新たなセキュリティ対処技術を生み出しうる**最先端のセキュリティ人材（セキュリティイノベーター）**を育成。
- NICTの持つサイバーセキュリティの研究資産を活用し、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。**
  （2017年度:39名, 2018年度:46名, 2019年度:45名, 2020年度:41名, 2021年度:41名, 合計212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。



年６回の集合研修（座学講座等）、
成果発表会・OB交流会＋通年の遠隔開発実習
の組合せによる総合的な人材育成プログラム

（参考）SecHack365の実施内容:コース制

SecHack365内コース

- 受講生の個性に対応するため、セキュリティイノベーターになるための異なるアプローチとして複数のコースを開講している。トレーナーの専門性や強みの活用にもつなげている。
- 各コースは、それぞれのアプローチにて重視する素養を問う募集課題を出題する。受講生は応募時の提出課題によってコースを選択する。
- 各コースはコース別に活動する。1～2週間に1回のオンラインミーティングや個別相談を実施して、受講生の作品づくりを支援・指導する。

表現駆動コース：解決したい課題や提案したいものを重視して、発表や試作など他者に表現して伝えることを通じた磨き上げに取り組む。協創や創発のためにグループ開発での作品づくりを求める。

学習駆動コース：開発や制作にすでに取り組んでいる者を対象にして、自分のやりたいことに取り組ませる。作り上げる以外の他の技術的要素の学習と付加要素として加えることを重視する。

開発駆動コース：トレーナーの専門性に基づいたテーマを受け入れて、まず考えていることの開発と完成を重視する。完成に向けての開発や完成してからの発展的な開発について、技術的な観点の指導を与える。

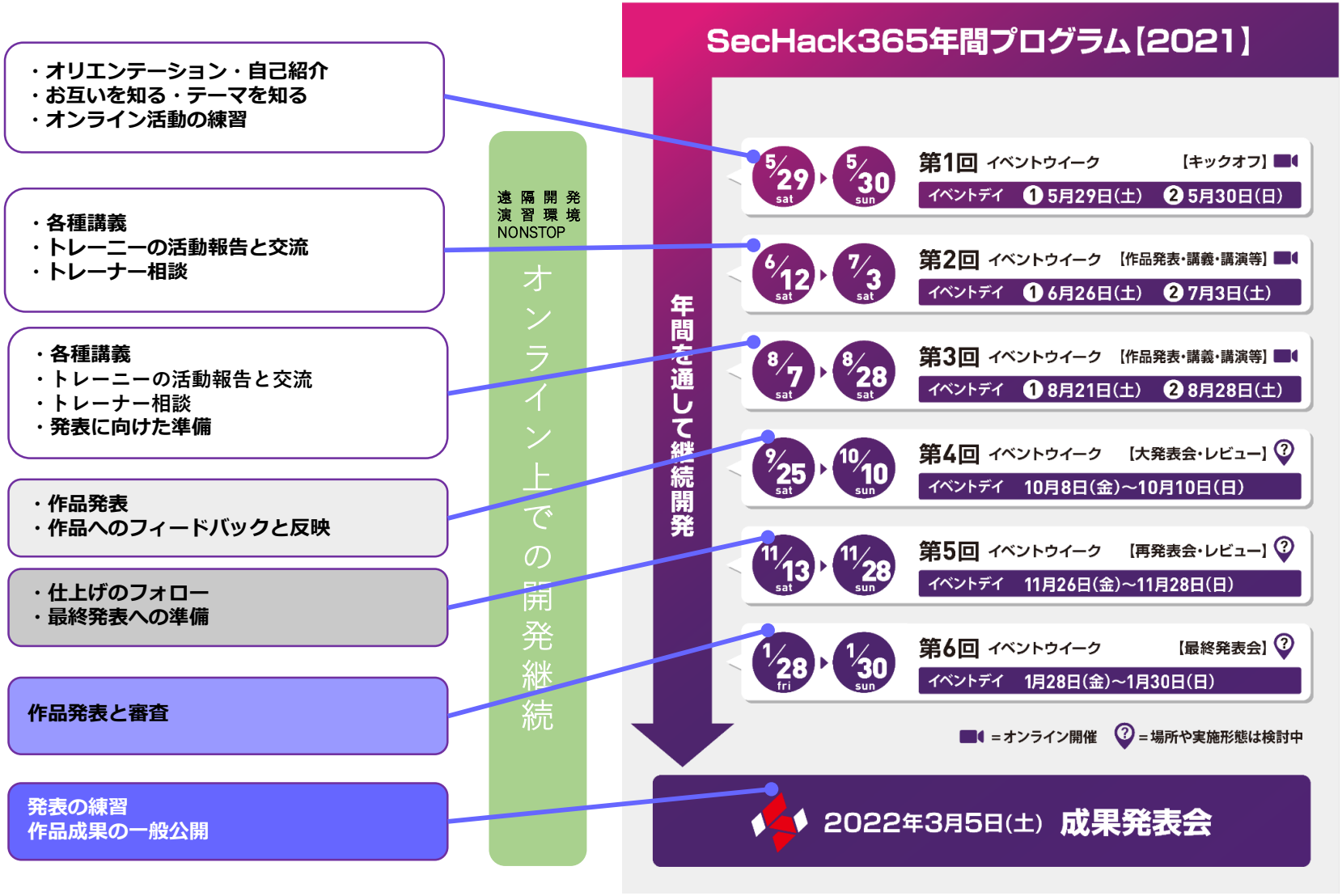
思索駆動コース：受講生には議論や対話と、問題に対する深い思索を求める。受講生が最も重要と考える課題を見出して、効果的な解決方法の実現に取り組む。

研究駆動コース：研究的手法に基づいて、セキュリティ上の課題の抜本的な解決やユニークな研究成果の達成に取り組む。先行研究や技術との差異を明確にして、研究成果とそのデモを求める。

全員共通の内容：

- 発表：自分の取り組む作品内容や活動内容についての発表とレビューの機会を与える
- 講義：継続力を身につけるための習慣化、アイデア発想、技術者倫理などの土台スキルを養成する
- 講演：セキュリティ開発・実務の方やアジャイル開発など、外部の方からの知識伝授の機会を与える
- 交流：受講生やトレーナーたちでの協創や相談のため、自己紹介や議論・対話のイベントを実施する

SecHack365の年間スケジュール（令和3年度）



SecHack365 成果発表会

- 2021年度の受講生41名のうち、優秀修了生を６名選定。

2021年度 優秀修了生成果

題名	概要
開発環境に馴染むWeb アプリ向けFuzzingツール SecHackFuzz	Webアプリ開発向けにFuzzingという脆弱性検知手法を用いたツールを作成した。Webアプリ開発工程にて簡単に利用できる工夫や、脆弱性探索の時間を減少させる工夫を施した。
キーボード打鍵音による 入力推定攻撃とその対策	キーボードの打鍵音から入力内容を推定する攻撃について、日本語として考えられる入力パターンを用いた精度向上の脅威の発見と対策方法を研究開発した。
GeneSlimeMold_分散型ゲノム情報 利活用システム	将来のゲノム情報の利用を想定して、個人の持つゲノム情報を保護して適正な利用を可能とするプラットフォームを提案した。
Seknot あなただけの暗号資産で新しい世界を	誰もが暗号トークンを発行して利用できる、ブロックチェーン技術を用いたプラットフォームを開発した。SH365内で利用できるデモサービスを開発した。
Rune ~CPUの特権命令をユーザープログラムへ安全に公開するための仕組み~	RISC-V CPUのセキュリティ特権命令をユーザープログラムへ安全に公開するRune という仕組みを開発した。Runeを使ったサンドボックスを実装した。
ソフトウェアルーターCURONOSの開発	TCP/IP機能を実装した自作OSを開発して、BGP対応ソフトウェアルータをゼロから実現した。中継時のパケット処理などの柔軟な制御などの機能も提供する。

2021年度成果発表会資料より総務省作成

SecHack365 令和4年度実施計画(案)

- 過去２年間のオンライン実施の結果を踏まえて、集団研修としての協創や交流の強化を目指しつつ、オンライン実施のノウハウも取り入れて、集合形式とオンライン形式を組み合わせた形での実施を検討。
- 実施内容や実施規模は従来通り、25歳以下の40名を対象に1年間のハッカソンを実施。
  通年でのオンライン指導、集合イベントを4回、オンラインイベントを2回、成果発表会を1回、Returnsを1回の実施を予定。コロナウィルスの蔓延状況に応じて、集合イベントはオンライン実施へと切り替える。

令和４年度の実施スケジュール（検討中）

	形式	時期	内容
募集	ー	４月中	応募の受付、合格者の審査と確定
第1回イベント	オンライン	(P)	オリエンテーション、キックオフ
第2回イベント	集合	(P)	初顔合わせ、活動状況の把握と助言
第3回イベント	集合	(P)	活動支援・インプット
Returns	オンラインの方向	９月頃	修了生向けイベント
第4回イベント	オンライン	(P)	作品発表・レビュー
第5回イベント	集合	(P)	作品発表、最終発表への準備
第6回イベント	集合	(P)	最終発表・審査
成果発表会	集合の方向	翌年３月頃	事業成果の発表会

① 人材育成

①－１ CYDER

①－２ SecHack365

①－３ 地域におけるセキュリティ人材育成

② 普及啓発

②－１ テレワークのセキュリティ

②－２ 無線LANのセキュリティ

②－３ 地域セキュリティコミュニティの形成

②－４ 国民のための情報セキュリティサイトの改修

②－５ その他の普及啓発施策

③ フィッシング対策

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

気付きの機会がない → 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 → 悪循環

２．組織体制の不足

何をすればよいかわからない → 専門人材を雇用できない → 対策が進まない → 悪循環

３．就業機会の不足

雇用の受け皿がない → 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更に不足 → 悪循環

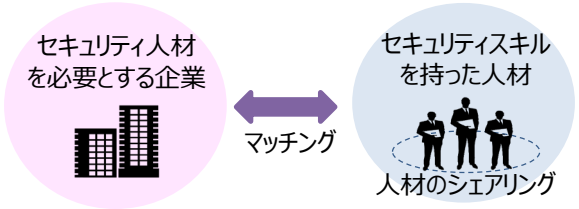
１．地域のセキュリティリーダーの育成

中部地方にて実施
→2019年度でモデル事業終了

○ **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
→2019年度でモデル事業終了

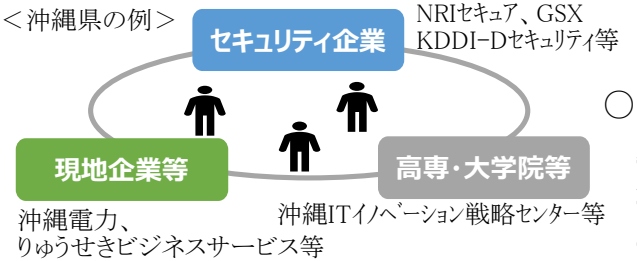


○ 県や広域エリアにおいて、複数の中小企業等が**セキュリティ専門家をシェアできるようにマッチング**。

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
→2020年度以降も継続して実施中

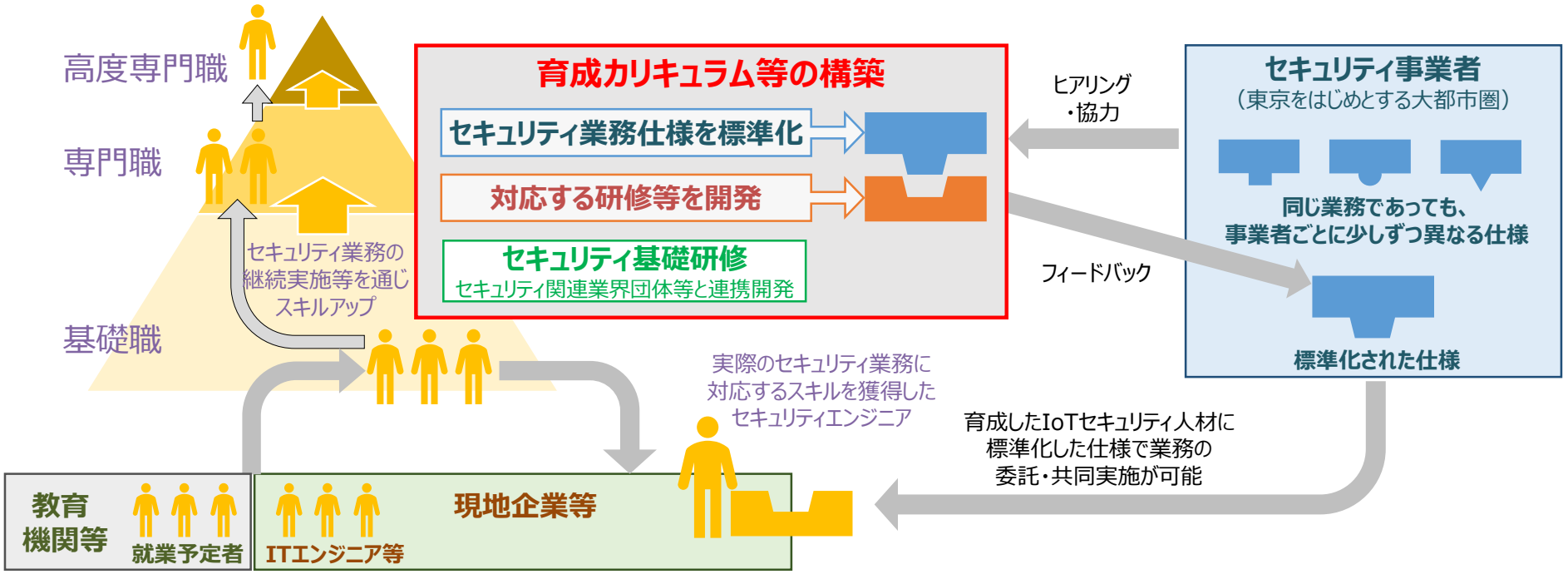
＜沖縄県の例＞



○ 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**。

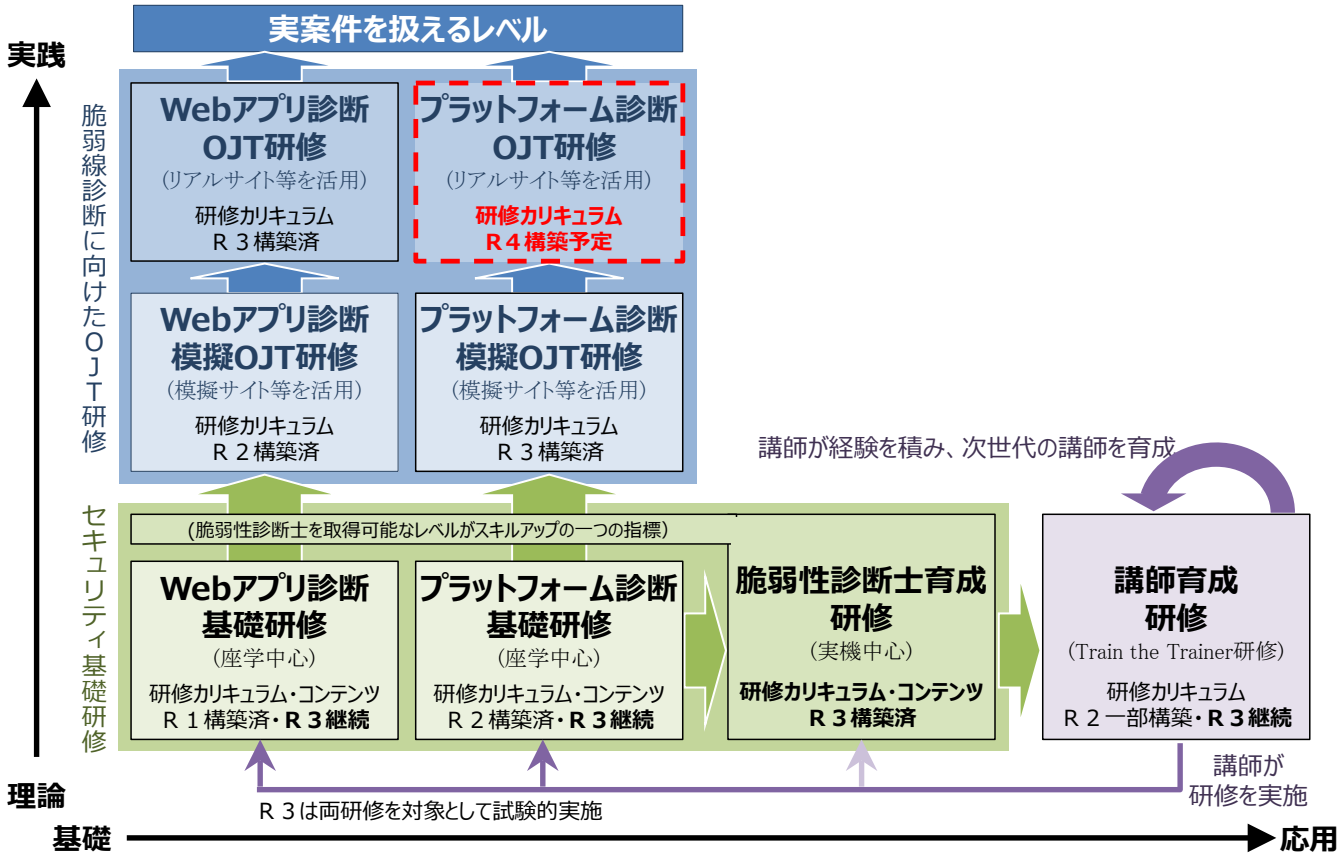
地域におけるIoTセキュリティ人材の確保

- **地域コミュニティにおいてIoTセキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築。**
  - ✓ セキュリティ事業者ごとに異なる業務仕様を、業務ごとに標準化し、対応する研修等を開発。
  - ✓ 地方を拠点に、現地のITエンジニアや若年層に集中的に研修等を提供し、業務遂行できるスキルを身につけたIoT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。
- **エコシステム構築に必要となる、育成カリキュラム等の育成モデルを構築する。**



地域におけるセキュリティ人材のエコシステムの形成（令和４年度実施案）

- エコシステム構築に必要となる育成カリキュラムは、令和２年度までで基礎的な骨格ができ、令和３年度では自走に向けたカリキュラム構築を行った。
- 令和４年度は、以下を実施予定。
  - ・カリキュラム未実施部分を完結させ、沖縄県でのエコシステム自走を本格化
  - ・他地域展開に向け、要件整理及び展開を容易にするための本事業のパッケージ化等の検討



論点

人材育成

○ CYDER未受講自治体の解消及び繰り返し受講の定着に向けて、他に取り組むべきことはあるか。

○ SecHack365の取組方向性として、さらに検討すべき点はあるか。

○ 地域におけるサイバーセキュリティ人材の育成が自律的に進むように、さらに取り組むべきことはあるか。

① 人材育成

- ①－１ CYDER
- ①－２ SecHack365
- ①－３ 地域におけるセキュリティ人材育成

② 普及啓発

- ②－１ テレワークのセキュリティ
- ②－２ 無線LANのセキュリティ
- ②－３ 地域セキュリティコミュニティの形成
- ②－４ 国民のための情報セキュリティサイトの改修
- ②－５ その他の普及啓発施策

③ フィッシング対策

前回タスクフォースの振り返り

前回タスクフォース資料（抜粋）

○テレワークのセキュリティ

・「テレワークセキュリティガイドライン」（2004年に初版を策定）について、テレワークを取り巻く環境やセキュリティ動向の変化に対応するため、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」とともに、2021年5月に第5版として改定。

○無線LANのセキュリティ

・2015年に策定した「Wi-Fi利用者向け簡易マニュアル」及び「Wi-Fi提供者向けセキュリティ対策の手引き」について、新たな無線LAN規格の登場等を踏まえ、2020年5月に改定。

○地域セキュリティコミュニティの形成

・2019年度以降、各地域における、民間企業、行政機関、教育機関、関係団体等による地域セキュリティコミュニティ（SECUNITY）の形成を促すとともに、セキュリティ意識啓発・対応能力向上のためのセミナーやサイバーインシデント対応演習の実施などを支援。

○国民のための情報セキュリティサイトの改修

・情報セキュリティに関する周知啓発を目的として運用している「国民のための情報セキュリティサイト」について、最新のセキュリティ動向に対応した内容に刷新するべく、改修を実施し、2022年春頃に公開予定。

前回タスクフォースでお寄せいただいた意見（抜粋）

✓ 防御策の普及啓発については多くの施策があるが、起きてしまった後どうするのかという点の普及啓発についてはどうなのか。（篠田構成員）

✓ 社内で自宅のテレワーク用機器のIPアドレスを調べて入力し、脆弱性を調査する取組を展開しているが、（社員に）IPアドレスを調べてもらう時点で大変な困難を感じた。（セキュリティ対策において、）技術的あるいは概念的に可能なことと、現場で実用可能なことは若干違うと思う。実用化できる対策や教育を考えられたらよい。（宇佐美構成員）

✓ 中央省庁でまとめられた知識体系が、省庁を分断してバラバラに出ている状況があると認識している。これを1つの知識体系にして、双方向のプラットフォームとしてポータルサイト化し、現場の近くで普及啓発するところへ提供したり、あるいは双方向の助言等を行えるようにすると良いのではないか。現在総務省が運営している「国民のための情報セキュリティサイト」は一方通行で、国民からの声をリアルタイムに拾っていないような印象であるので、改善を検討できると良い。（名和構成員）

① 人材育成

- ①－１ CYDER
- ①－２ SecHack365
- ①－３ 地域におけるセキュリティ人材育成

② 普及啓発

- **②－１ テレワークのセキュリティ**
- ②－２ 無線LANのセキュリティ
- ②－３ 地域セキュリティコミュニティの形成
- ②－４ 国民のための情報セキュリティサイトの改修
- ②－５ その他の普及啓発施策

③ フィッシング対策

テレワークにおけるセキュリティ対策の推進

- 総務省では従来から「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示してきた。
  → テレワークを取り巻く環境やセキュリティ動向の変化に対応するため**2021年５月**に**全面的に改定**
- ガイドラインを補完するものとして、セキュリティの専任担当がいないような中小企業等においても、テレワークを実施する際に**最低限のセキュリティ**を**確実に確保**してもらうための**チェックリスト**についても策定。

公表URL　https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークセキュリティガイドライン
（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４版

- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、
理解や検討が難しい場合

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)
（2021年５月　第２版）　2020年９月初版

中小企業等に向け**最低限のセキュリティを確実に確保**してもらうためのものに限定

【想定読者像】
- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能

テレワークで活用される代表的なソフトについて、**設定解説資料**を作成し、具体的な設定を解説
【設定解説資料の対象】
CiscoWebexMeetings／Microsoft Teams／Zoom／Windows／Mac／iOS／Android／LanScope An／Exchange Online／Gmail／Teams_chat／LINE／OneDrive／Googleドライブ／Dropbox／YAMAHA VPNルータ／CiscoASA／Windowsリモートデスクトップ接続／Chromeリモートデスクトップ／Microsoft Defender／ウイルスバスターービジネスセキュリティサービス

① 人材育成

- ①－１ CYDER
- ①－２ SecHack365
- ①－３ 地域におけるセキュリティ人材育成

② 普及啓発

- ②－１ テレワークのセキュリティ
- **②－２ 無線LANのセキュリティ**
- ②－３ 地域セキュリティコミュニティの形成
- ②－４ 国民のための情報セキュリティサイトの改修
- ②－５ その他の普及啓発施策

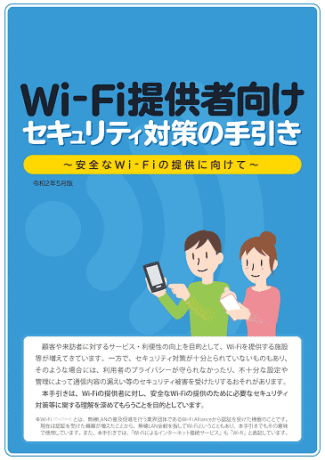
③ フィッシング対策

無線LANのセキュリティガイドライン

- 総務省では、無線LANの利用者・提供者向けにガイドラインを作成しており、周知啓発に活用。
- 新技術や最新のセキュリティ動向に対応するため、内容を見直し2020年５月に改定版を公表。
- 改定版については、Wi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に幅広く周知。
  https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

「Wi-Fi利用者向け 簡易マニュアル」のポイント

- ✓ セキュリティ対策の訴求点を明確にするため、**セキュリティ対策のポイント**を**整理**
  - ① 接続する**アクセスポイント**を**よく確認**（偽アクセスポイント対策として接続URL等を確認）
  - ② 正しい**URL**で**HTTPS通信**をしているか**確認**（Wi-Fi暗号化等に関わらず通信内容を保護）
  - ③ 自宅に設置している**機器の設定**を**確認**（管理用パスワードの変更やファームウェアアップデート等）
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**



「Wi-Fi提供者向け セキュリティ対策の手引き」のポイント

- ✓ ガイドラインの対象者の明確化（**自店利用者のみへ提供する者も対象**）
- ✓ 近年懸念されている**偽アクセスポイント対策**（認証画面のURLの周知等）を追記
- ✓ 暗号化のための**パスフレーズを公開**している場合解読の**リスクが高まる**ことを明示
- ✓ 状況に応じたセキュリティ対策の選択と**利用者への周知**が必要であることを明確化
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

無線LAN(Wi-Fi)の利用に関する周知啓発

- 総務省では、無線LANの利用者のセキュリティ対策に関する周知啓発を継続的に実施。
- 令和元年度以降、**オンライン動画講座**を開講するとともに、**ショートムービー**を作成し**SNSを通じて周知。**

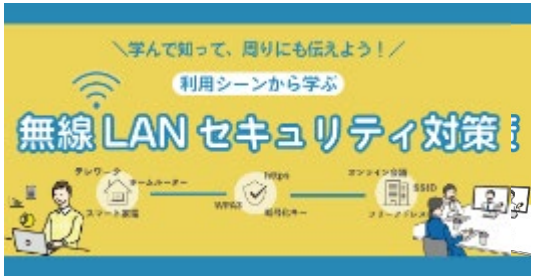
オンライン動画講座

- ✓ 無線LAN利用時のリスクや、適切なセキュリティ対策を**有識者が動画により説明**
- ✓ オンライン講座プラットフォーム「gacco」にて配信
  https://gacco.org/wifi-security/
  ①「これだけは知っておきたい 無線LANセキュリティ対策」（開講期間:2/1～3/25）
  ②「学んで知って周りにも伝えよう 無線LANセキュリティ対策」（開講期間:3/7～3/25） ※追加開講
- ✓ 2022年3月18日現在、合計2130名が受講登録
  （前年度は3,161名：2021.2.12～3.24）

①「これだけは知っておきたい 無線LANセキュリティ対策」

第１回：もっとつながる・使える公衆無線LAN <Wi-Fiの技術>
第２回：とっても危険！「野良Wi-Fi」
第３回：そのWi-Fi、本物ですか？
第４回：さまざまな公衆無線LANサービスを知ろう
第５回：Wi-Fiの接続と暗号化の仕組み
第６回：安全なWeb利用の方法
第７回：自分で重要な通信内容を守る
第８回：より安全・安心にWi-Fiを使うために
第９回：Wi-Fi規格の最新動向
第10回：無線LAN利用時に注意すべき３つのポイント
第11回：提供者視点からみた無線LANセキュリティ

②「学んで知って周りにも伝えよう 無線LANセキュリティ対策」



第１回：こんなにある無線LAN（Wi-Fi）
第２回：Wi-Fiはこうやってつながっている
第３回：Wi-Fiのここに気をつけよう ～自宅での設置編～
第４回：Wi-Fiのここに気をつけよう ～自宅での利用編～
第５回：Wi-Fiのここに気をつけよう ～オフィスでの利用編～
第６回：Wi-Fiのここに気をつけよう ～外出先での利用編～
（新規）
第７回：さまざまな公衆無線LANサービスを知ろう
第８回：安全なWeb利用の方法
第９回：Wi-Fiの接続と暗号化の仕組み
第10回：Wi-Fi規格の最新動向
第11回：無線LAN利用時に注意すべき３つのポイント
第12回：提供者視点からみた無線LANセキュリティ

SNSを用いた周知啓発

- ✓ 無線LANのセキュリティ周知啓発に関し、20秒程度の動画コンテンツを配信（全７種）
  ※うち２種類は３月１日から追加配信
- ✓ SNSを通じて配信するとともに、動画クリック時に上記オンライン動画講座にリンクすることにより誘導
  （Instagram、Facebook）
- ✓ 2022年２月１日～３月25日に配信し、3月18日現在226万インプレッション（３万クリック）
  ※前年度は216万インプレッション（3.3万クリック）（2021.2.12～3.23）

＜動画例：あなたの自宅のWi-Fiセキュリティは大丈夫？＞

① 人材育成

- ①－１ CYDER
- ①－２ SecHack365
- ①－３ 地域におけるセキュリティ人材育成

② 普及啓発

- ②－１ テレワークのセキュリティ
- ②－２ 無線LANのセキュリティ
- **②－３ 地域セキュリティコミュニティの形成**
- ②－４ 国民のための情報セキュリティサイトの改修
- ②－５ その他の普及啓発施策

③ フィッシング対策

地域に根付いたセキュリティコミュニティ（地域SECUNITY）の形成促進

➢ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ（地域SECUNITY（セキュニティ））の形成の促進を図る。

【令和４年度予算：地域セキュリティコミュニティ強化支援事業（0.4億円）】

● 全国規模で事業展開する企業に比べ、地域の企業や地方公共団体などについては、有効なサイバーセキュリティ対策をとるための人材育成・普及啓発の機会や情報共有の枠組みなどが不足しているおそれ。

➡

● 地域の企業や地方公共団体については、各者とも単独で有効なサイバーセキュリティ対策をとることは困難であり、地域レベルでのコミュニティを形成して情報共有等を強化する必要がある。

地域に根付いたセキュリティコミュニティ

セキュリティ関連の情報共有

定期的なセミナーや演習等の実施

セキュリティコミュニティの形成の促進

● ①当該地域における大手事業者、②業界団体（地方支部など）、③都道府県警、④サイバーセキュリティ関係事業者・機関、⑤地方公共団体、⑥有識者などによる地域のサイバーセキュリティ向上のための推進体制を構築する。なお、情報共有体制がすでに存在している地域においては、既存の体制を活用していくことが望ましい。

● 地域の企業等向けに①定期的なセミナーやインシデント演習の実施、②セキュリティ関連の情報共有の枠組みなどを構築。

各地域におけるセキュリティコミュニティ

➢ 令和３年度内に、全11地域において、セキュリティコミュニティの設立が完了。

関西サイバーセキュリティ・ネットワーク

【事務局】近畿総合通信局、近畿経済産業局、(一財)関西情報センター（2018年10月設立）

北陸サイバーセキュリティ連絡会

【事務局】北陸総合通信局（2020年3月設立）

北海道地域情報セキュリティ連絡会（HAISL）

【事務局】北海道総合通信局、北海道経済産業局、北海道警察本部（2014年9月 設立）

中国地域サイバーセキュリティ連絡会

【事務局】中国総合通信局、中国経済産業局（2020年10月設立）

東北地域サイバーセキュリティ連絡会

【事務局】東北総合通信局、東北経済産業局（2021年10月設立）

関東サイバーセキュリティ連絡会

【事務局】関東総合通信局、関東経済産業局（2021年3月設立）

九州・沖縄地域情報セキュリティ推進連絡会議

【事務局】九州総合通信局、九州経済産業局（2012年5月設立）

信越サイバーセキュリティ連絡会

【事務局】信越総合通信局、関東経済産業局（2022年1月設立）

沖縄サイバーセキュリティネットワーク

【事務局】内閣府沖縄総合事務局、沖縄総合通信事務所、沖縄県警察本部（2015年3月設立）

サイバーセキュリティシンポジウム道後

【事務局】（一社）テレコムサービス協会四国支部、四国総合通信局（共催）、他複数団体が共催（2012年10月設立）

東海サイバーセキュリティ連絡会

【事務局】東海総合通信局、中部経済産業局（2020年8月設立）

総務省によるセキュリティコミュニティへの支援

- 令和３年度において、各地域からの要望を踏まえ、サイバーセキュリティに関するセミナー（14回）、インシデント対応演習（９回）、若年層向けCTF（２回）の開催を支援。
  ※年間で、セミナーを957名、インシデント対応演習を268名、若年層CTFを53名が受講。
- 令和４年度も、引き続き、このようなイベントの開催を支援するとともに、地域のセキュリティコミュニティによる先進的な取組の支援も検討。

＜支援内容＞

支援項目	支援内容
●サイバーセキュリティに関するセミナーの開催	• 地域で開催するセミナーの運営補助 （会場費、講師謝金などの必要経費は総務省（請負事業者）が負担）
●インシデント対応演習の開催 ※インシデント対応演習：インシデント発生時における一次対応や情報連携についてグループワークを行う。	• インシデント対応演習の企画・内容検討 • インシデント対応演習の開催に係る支援全般
●若年層向けCTFの開催 ※CTF：Capture The Flagの略で、ゲーム形式でセキュリティの実践的技能を競うコンテストを行う。	• 若年層を中心としたサイバーセキュリティ初学者向けのCTFの企画・運営

※このほか、セキュリティコミュニティにおけるメールマガジンによる配信を想定したコンテンツ作成、サイバーセキュリティ普及啓発のためのケーブルテレビ番組制作（富山地域）を実施。

（参考）令和３年度の開催状況（地方局独自開催分含む）

➢ 令和３年度、総務省の支援で、各地域において、25件のセミナーやインシデント対応演習等を開催（このほか、地方局独自開催で８件のセミナーを開催）。

管区	イベント名	形式	実施形態	場所	開催時期（予定）	本省の支援
北海道	サイバーセキュリティフォーラム北海道2022	セミナー	オンライン	ー	令和４年３月３日	有
	HAISL人材育成プロジェクト(若手向け勉強会)	セミナー	オンライン	ー	令和３年５月～令和４年２月（計５回）	有 (5回目のみ)
	サイバーインシデント演習	演習	オンライン	ー	令和４年３月10日	有
東北	東北地域サイバーセキュリティセミナー	セミナー	オンライン	ー	令和３年12月15日	有
	サイバーインシデント演習in東北	演習	オンライン	ー	令和４年２月22日	有
	サイバーインシデント演習in東北	演習	オンライン	ー	令和４年３月２日	有
関東	サイバーインシデント演習in関東	演習	オンライン	ー	令和３年12月１日	有
	関東サイバーセキュリティセミナー	セミナー	オンライン	ー	令和４年２月18日	無
信越	セキュリティセミナー	セミナー	ハイブリッド	新潟	令和４年２月18日	無
	サイバーセキュリティセミナー2022	セミナー	オンライン	ー	令和４年２月24日	無
	サイバーインシデント演習	演習	オンライン	ー	令和４年３月17日	有
北陸	若年層向けCTFワークショップ	CTF	ハイブリッド	鯖江	令和４年１月29日	有
	『ビジネス』を護るサイバーセキュリティデイズ	セミナー	ハイブリッド	金沢	令和４年２月24日	有
東海	東海サイバーセキュリティ連絡会	セミナー	実地	名古屋	令和３年７月29日	有
	サイバーインシデント演習in東海	演習	実地	名古屋	令和３年11月11日	有
	サイバーセキュリティセミナー2022	セミナー	オンライン	ー	令和４年２月４日	有
近畿	サイバーインシデント演習	演習	オンライン	ー	令和４年１月21日	有
	サイバーセキュリティカフェ	セミナー	ハイブリッド	奈良	令和３年11月15日（１回目）	有
	サイバーセキュリティカフェ	セミナー	ハイブリッド	豊岡	令和４年１月18日（２回目）	有
	サイバーセキュリティセミナー	セミナー	ハイブリッド	大阪	令和４年３月９日	有
	若年層向けCTFワークショップ	CTF	ハイブリッド	大阪	令和４年３月17日	有
中国	サイバーセキュリティセミナー	セミナー	オンライン	ー	令和３年11月12日	有
	サイバーインシデント演習in松江	演習	実地	松江	令和３年12月８日	有
	サイバーセキュリティ連絡会交流セミナー	セミナー	オンライン	ー	令和４年２月22日	有
四国	サイバーインシデント演習in四国	演習	オンライン	ー	令和４年２月９日	有
	セキュリティ対策セミナー	セミナー	ハイブリッド	高松	令和４年３月３日	有
九州	サイバーセキュリティ・カレッジin熊本2022	セミナー	ハイブリッド	益城	令和４年２月10日	無
沖縄	サイバーセキュリティセミナー	セミナー	オンライン	ー	令和３年11月25日	有
	サイバーセキュリティ月間セミナー	セミナー	オンライン	ー	令和４年２月17日	有

各地域コミュニティにおける主な取組

北海道ブロック

◇若手人材育成

・学生や青年層向けに、サイバーセキュリティに関する知見や技術を教授し、将来のセキュリティリーダー、ホワイトハッカーになり得る人材の発掘と育成を目的としたプロジェクトとして、SC４Y（Security College for Youth）を公立千歳科学技術大学で開催。

近畿ブロック

◇地方都市におけるイベント

・地域の企業、団体等の方を対象にサイバー攻撃の現状や対策など「サイバーセキュリティ」に関するミニ講演と素朴な疑問や相談を気軽にできるよう“座談会”的な地域密着型のイベントを開催（奈良、豊岡）

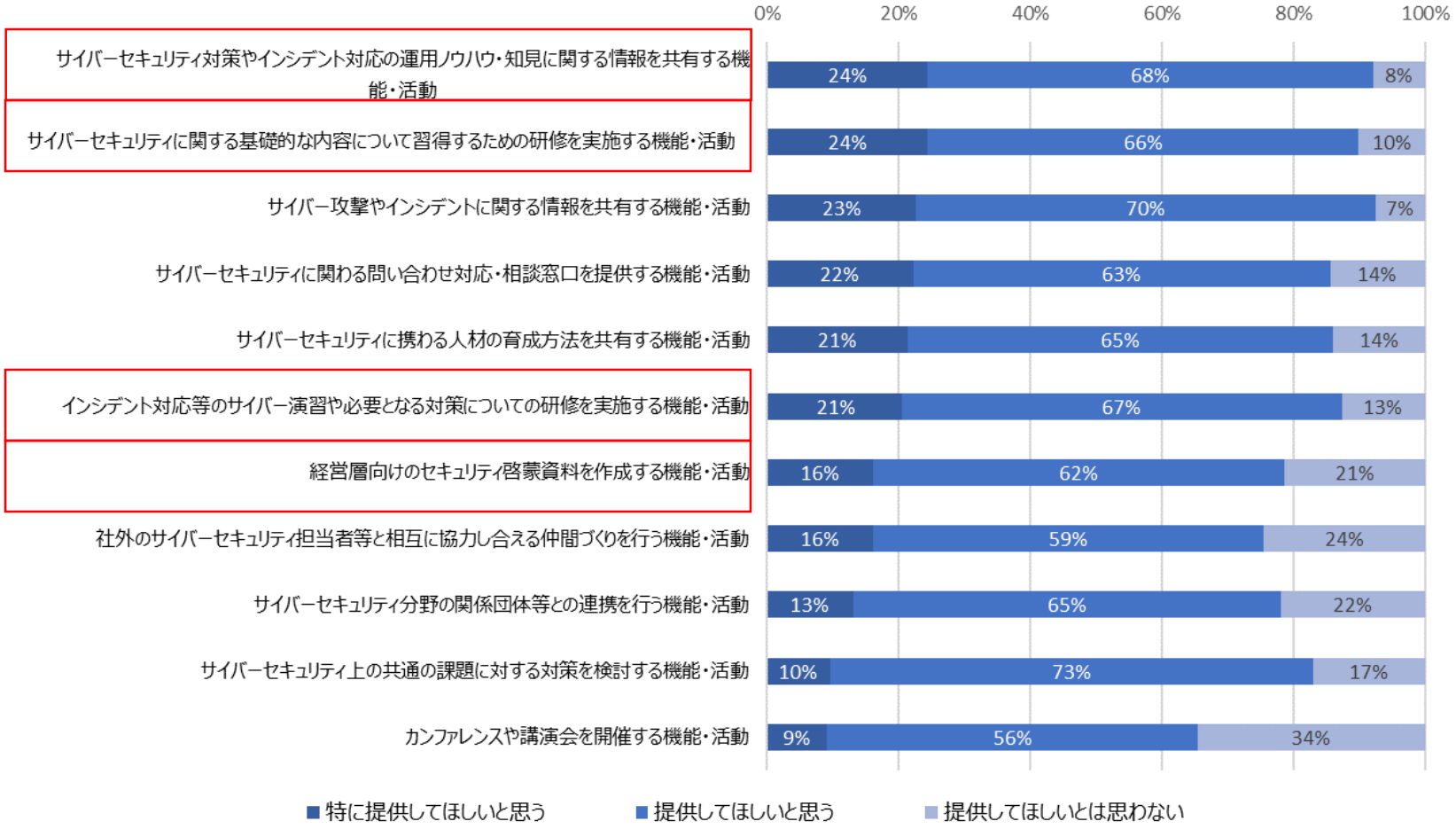
北陸ブロック

◇CTF（Capture The Flag）の開催

・地域の若年層等を対象として、サイバーセキュリティに興味を持ち、セキュリティエンジニアになるためのスキルアップに向けた知識の習得等を目的として、楽しみながらサイバーセキュリティを学ぶ競技を中心とするイベントを開催（鯖江）

（参考）地域のセキュリティコミュニティへの期待

➢ 地域のセキュリティコミュニティにおいて提供してほしい機能・活動として、「インシデント対応の運用ノウハウ・知見に関する情報共有」、「基礎的な内容を習得するための研修」などが上位を占める。



【出典】地域の経営層及び戦略マネジメント層等を対象としたインシデント演習を実施するにあたっての事前調査（総務省委託調査、2021年11月） ※対象は地域セキュリティコミュニティに参加する229事業者。

① 人材育成

- ①－１ CYDER
- ①－２ SecHack365
- ①－３ 地域におけるセキュリティ人材育成

② 普及啓発

- ②－１ テレワークのセキュリティ
- ②－２ 無線LANのセキュリティ
- ②－３ 地域セキュリティコミュニティの形成
- **②－４ 国民のための情報セキュリティサイトの改修**
- ②－５ その他の普及啓発施策

③ フィッシング対策

国民のための情報セキュリティサイトの改修

- 総務省は、国民のための情報セキュリティサイトを運用し、情報セキュリティに関する周知啓発を実施。
- 2020年度においても**約130万件のアクセス**があり、多くの国民が閲覧。
  （ https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/ ）
- 内容の最終更新が2013年4月のため、情報が老朽化しており、最新のセキュリティ動向に対応した内容に刷新するべく、2021年度に改修を行う。

改修の進め方

●コンテンツの現行化

・サイバーセキュリティに関する知見（技術を含む）を有する者、サイバーセキュリティ事業者の意見を代表する者（業界団体等）、消費者団体関係者等へのヒアリングを実施。
・内容が老朽化している点、新たに追加すべき点（テレワーク時のセキュリティ等）をとりまとめ。

●レビューの実施

・改定案の全頁を対象として、テクニカルレビュー及び消費者目線レビューを実施。

●公開中WEBサイトの刷新

・CMS対応化、あわせてスマートフォン・タブレットからの閲覧用ページの作成検討。

反映

改修・公開

スケジュール

- **2022年春頃公開予定**

① 人材育成

- ①－１ CYDER
- ①－２ SecHack365
- ①－３ 地域におけるセキュリティ人材育成

② 普及啓発

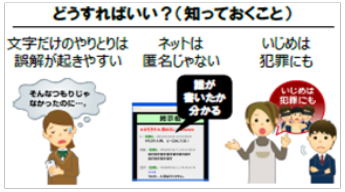
- ②－１ テレワークのセキュリティ
- ②－２ 無線LANのセキュリティ
- ②－３ 地域セキュリティコミュニティの形成
- ②－４ 国民のための情報セキュリティサイトの改修
- **②－５ その他の普及啓発施策**

③ フィッシング対策

eネットキャラバン

- 子どもたちのインターネットの安全な利用に係る普及啓発を目的に、児童・生徒、保護者・教職員等に対する学校等の現場での無料の「出前講座」を、情報通信分野等の企業・団体と総務省・文部科学省が協力して全国で開催。
- 2020年度は、1,208件の講座を実施し、約14万人が受講。（2006年度開始以来の実績：23,791件、のべ約382万人）

実施主体	一般財団法人マルチメディア振興センター（ＦＭＭＣ）
協力団体	通信事業者等の民間企業（486社）、公益法人等（20団体）、政府（総務省及び文部科学省）、自治体（59団体）、その他（61団体）　＊企業等がCSRとして講師を派遣。（認定講師数：5,445名）
対象者	小学生（小３～小６）、中学生、高校生、保護者、教職員等
講座内容	ネット依存、ネットいじめ（誹謗中傷含む）、不確かな情報の拡散、ネット誘引（誘い出し・なりすまし）、ネット詐欺、著作権の侵害等のトラブル事例を用いて、予防策等を啓発。
受講方法	従来は集合形式のみだったが、受講方法の選択肢を拡大。2020年11月にFMMCが報道発表。同年12月に総務省・文部科学省の連名で全国に周知文書を発出。 ＊校内の放送設備やWeb会議システムを利用した講座、リモート講座、ビデオオンデマンド講座。

① ネット依存		② ネット いじめ		③ 不確かな 情報の 拡散	
④ 誘い出し・ なりすまし		⑤ 個人情報 漏洩		⑥ ネット詐欺	
⑦ 著作権・ 肖像権					

（2022年２月末時点）

デジタル活用支援推進事業

- 民間企業や地方公共団体等と連携し、デジタル活用に不安のある高齢者等の解消に向けて、オンラインによる行政手続等のスマートフォンの利用方法に対する助言・相談等の対応支援を行う「講習会」を、全国で実施中。
  （総務省「デジタル活用支援推進事業」：2021年度は携帯ショップ等を中心に約2,000箇所超）
- 現在、総務省とNISCにおいて、サイバーセキュリティの普及啓発の観点から、本事業との連携を検討中。

携帯キャリア等（都市部等）

令和３年度～
講習会(全国展開型)

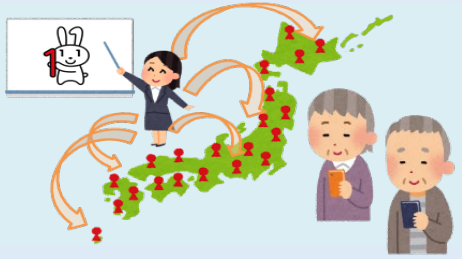
講習会等を行う拠点を全国に有しており、当該拠点で支援を実施する主体（携帯ショップを想定）

地域に根差した支援（地方）

令和３年度～
講習会(地域連携型)

地方公共団体と連携して、公民館等の公共的な場所で支援を実施する主体（地元ICT企業、社会福祉協議会等）

令和4年度～
デジタル活用支援推進事業講師の派遣



地域の担い手となる、高度なスキルを有するデジタル活用支援推進事業の講師を育成し、携帯ショップがない市町村など津々浦々に講師を派遣して支援を実施

＜2021年度事業における講座の例＞

基本講座（スマートフォンの基本的な利用） ※全国展開型では各社の既存のスマホ教室等の取組で補完できることから対象外	応用講座（スマートフォンによる行政手続等）
① 電源の入れ方、ボタンの操作方法	① マイナンバーカードの申請方法
② 電話のかけ方、カメラの使い方	② マイナポータルの活用方法
③ アプリのインストール方法	③ マイナポイントの予約・申込方法
④ インターネットの利用方法	④ e-Taxの利用方法
⑤ メールの利用方法	⑤ オンライン診療の利用方法
⑥ 地図アプリの利用方法	⑥ 地域におけるオンライン行政手続の実施方法
⑦ SNS・コミュニケーションアプリの利用方法	⑦ 新型コロナワクチン接種証明書アプリを用いた接種証明書の発行方法

サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会　第16回会合（令和３年12月９日）　資料２より一部編集

論点

普及啓発

○地域セキュリティコミュニティについて、現在は、セミナーやインシデント対応演習を開催する役割を担っているが、今後どのような役割の拡大を期待するか。

○ 子ども・高齢者向けのサイバーセキュリティ普及啓発に向けて、最近の動向を踏まえ、どのような施策を実施すべきか。

① 人材育成

①－１ CYDER

①－２ SecHack365

①－３ 地域におけるセキュリティ人材育成

② 普及啓発

②－１ テレワークのセキュリティ

②－２ 無線LANのセキュリティ

②－３ 地域セキュリティコミュニティの形成

②－４ 国民のための情報セキュリティサイトの改修

②－５ その他の普及啓発施策

③ フィッシング対策

前回タスクフォースの振り返り

前回タスクフォースでお寄せいただいた意見（抜粋）

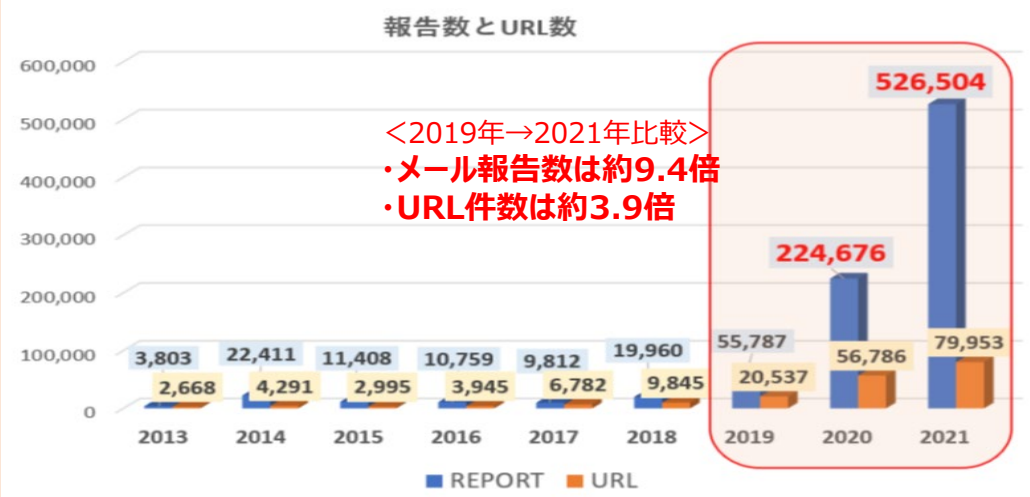
- ✓フィッシングの対象が移り変わり、これまで（フィッシングに悪用された）経験がなかったようなカード会社等が盛んに狙われている。また、ボットを使ったバルクメールという形で同じURLから多数のメールが出されるケースも見られる。（岡村構成員）
- ✓フィッシングの注意喚起のための情報発信について、届出件数だけに着目するのではなく、現状が正しく伝わるようにすべき。（辻構成員）
- ✓フィッシング被害の報告については、自動化するなどわかりやすくするべきではないか。また、報告の質・量が上がれば、セーフブラウジングへのインプットも考慮できるのではないか。（篠田構成員）
- ✓国際的なCERT間の連携によるフィッシングサイトのテイクダウンを進めることも重要。（岡村構成員）
- ✓セーフブラウジングについて、ブロッキングの基準は各ブラウザ企業の基準に依存している。政府にフィッシングサイトのデータが集まっているのであれば、それをブラウザ企業に提供することも一案ではないか。（篠田構成員）
- ✓社内のフィッシングメール訓練に引っかかった社員を対象に講習会を開催したが、こうやれば通常のメールとフィッシングメールを区別できるということがはっきりと言えないので、一般的に気をつけましょうといった精神論で終わってしまうところが非常に難しいと痛感した。（宇佐美構成員）

フィッシングの動向

前回タスクフォース資料35-1を更新

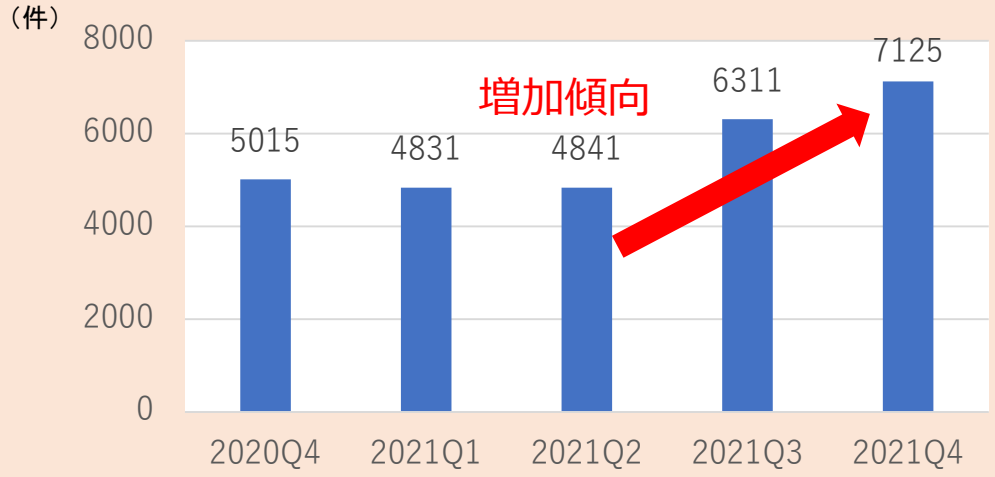
フィッシングメールの報告数とフィッシングサイトURL数

出典：フィッシング対策協議会



フィッシングサイトに関するインシデントの報告件数

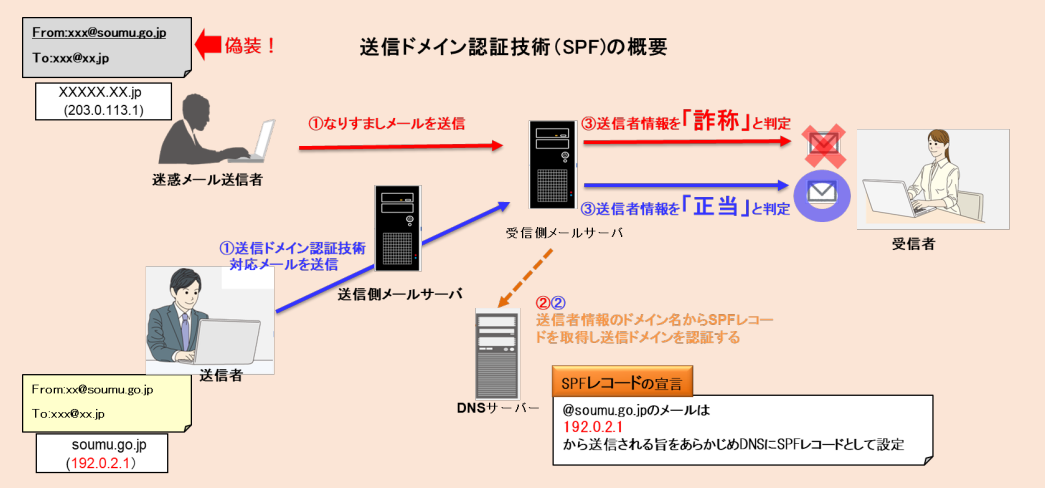
出典：JPCERT/CC インシデント報告対応レポート



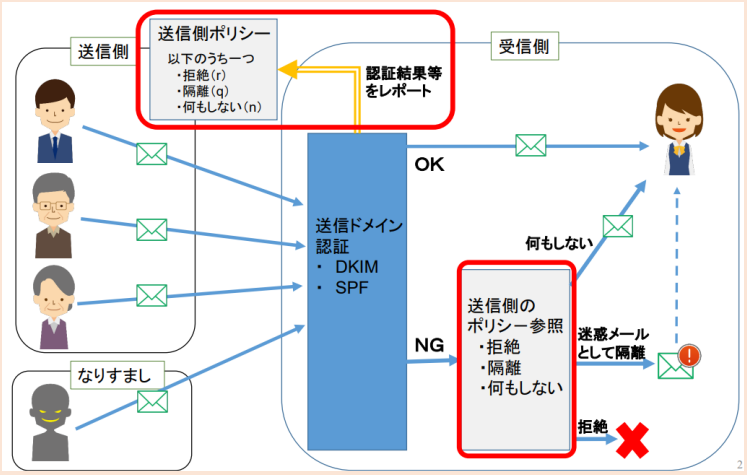
送信ドメイン認証技術の普及に向けた取組

- フィッシングメールを含む迷惑メール送信者は、受信者にメールを開いてもらうために有名なサイトからの送信に見せかけたり、送信者を特定しづらくするため、自前のサーバー等から直接迷惑メールを送信する際、ドメインを詐称して送信することが多い。
- 受信側で後者の詐称を検出できるようにするのが送信ドメイン認証技術(SPF※1、DKIM※2、DMARC※3)であり、これらの導入により、詐称と判断されたメールは受信しない等の対策が可能となる。
- 総務省では、これらの技術について法的に整理の上、留意点を公表※4し、導入を促進している。
- また、来年度より中小ISPにおける送信ドメイン認証技術の導入実証※5も予定している。

SPFの仕組み



DMARCの仕組み

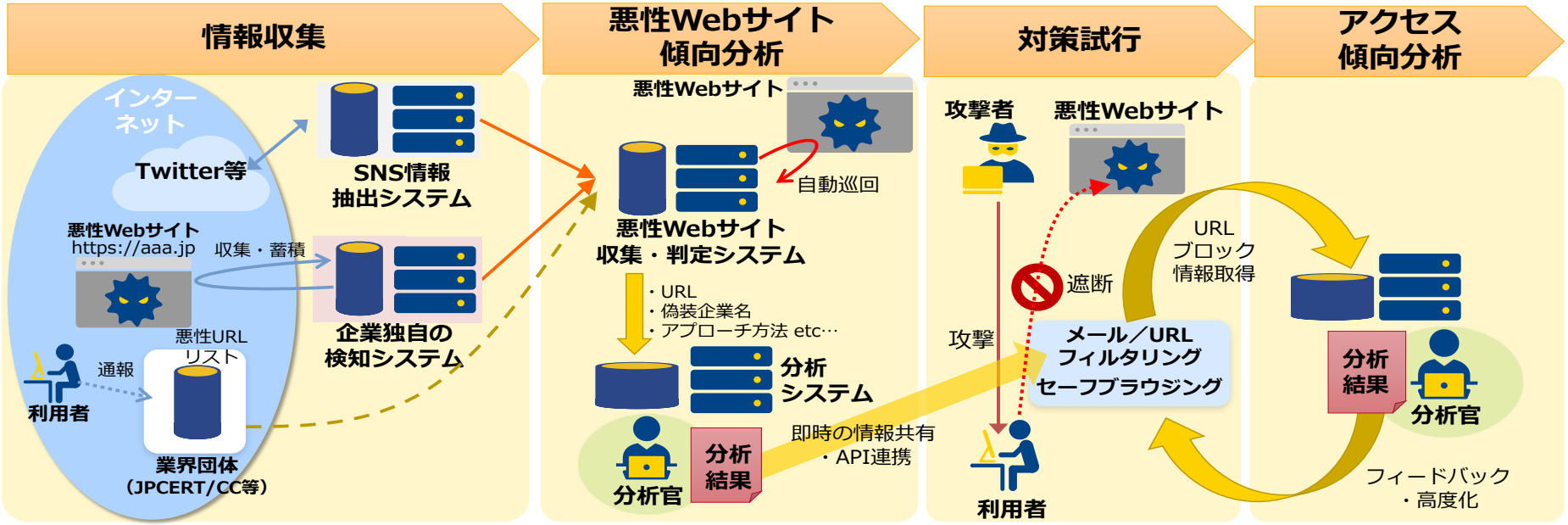


※1　SPF（Sender Policy Framework）：送信側のメールサーバーのIPアドレスをDNSで宣言することにより、ネットワーク的に認証を実施する技術。
※2　DKIM（DomainKeys Identified Mail）：送信側のメールサーバーで作成した電子署名により認証する技術。
※3　DMARC(Domain-based Message Authentication, Reporting, and Conformance):SPF・DKIMの認証結果を利用し総合的に送信ドメイン認証を行う技術。
※4　「受信側における送信ドメイン認証技術導入に関する法的な留意点」：https://www.soumu.go.jp/main_content/000499986.pdf
「DMARC導入に関する法的な留意点」：https://www.soumu.go.jp/main_content/000495390.pdf
※5　中小ISP等の通信ネットワークを実証環境として選定し、技術的課題の解決策や運用者に求められるスキルの取得ノウハウ等を分析してガイドラインを策定することを想定。

悪性Webサイトの検知技術・共有手法の実証（令和3年度補正予算施策）

- 総務省では、令和４年度より、悪性Webサイト（フィッシングサイト等）の検知技術及び共有手法の有効性を検証する実証事業を行う。
- 事業の詳細は以下のとおり。

- SNS等に投稿された情報、企業独自の悪性Webサイト検知システムにより収集・蓄積された情報及び利用者により通報された情報等をもとに、自動巡回による機械的処理を活用して悪性Webサイト情報の収集・分析を行い、検知技術の有効性及び課題を整理する。
- 悪性Webサイトの検知結果及び傾向分析結果を活用し、サービス提供者側からの継続的な対策を講じるための必要事項を整理する。
- 以上の整理結果を踏まえ、偽装サイト検知手法のガイドライン策定等による各種企業へのノウハウの普及、業界団体を通じた悪性Webサイトの削除要請への貢献、迷惑メール/URLフィルタリング・セーフブラウジングサービス等を提供する企業への情報提供を通じて、サービス提供者側の悪性Webサイト対策の強化を図る。



論点

フィッシング対策

○ フィッシング対策協議会からの御報告や最近のフィッシングの急増等の現状も踏まえ、今後、総務省として、どのような取組を実施すべきか。