NISC National center of Incident readiness and Strategy for Cybersecurity

資料3

人材育成等に係る取組状況について（報告）

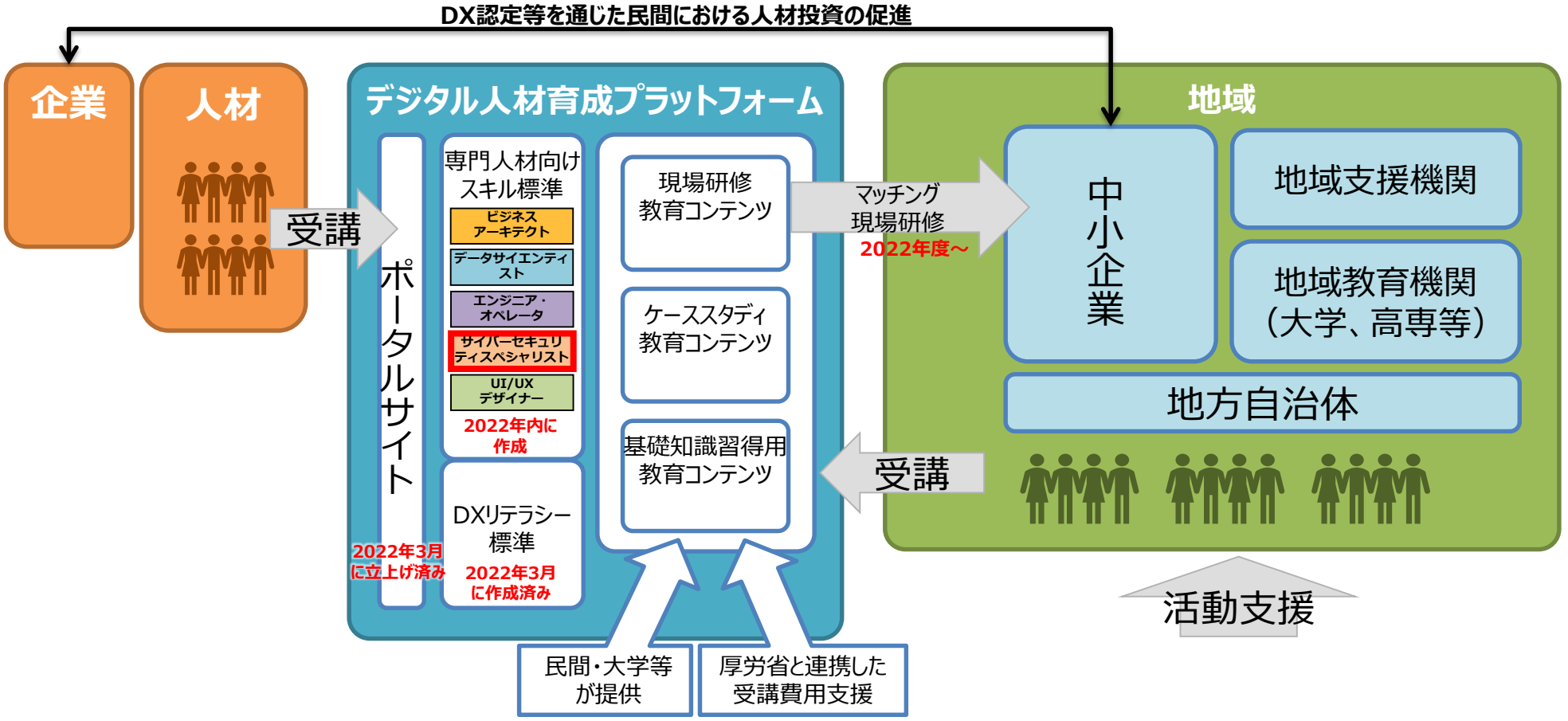
令和4年6月

内閣官房 内閣サイバーセキュリティセンター
基本戦略第1グループ

デジタル人材育成プラットフォーム

経済産業省等

- デジタル知識・能力を身に付けるためには、講義の受講等に加え、ビジネスの現場における課題解決の実践を通じた能力を磨くことが重要。
- 産業界で求められるスキル標準やそれに紐付く教育コンテンツの提示、地域の現場とのマッチング等を行う「デジタル人材育成プラットフォーム」を構築し、全国大で人材育成を行っていく。

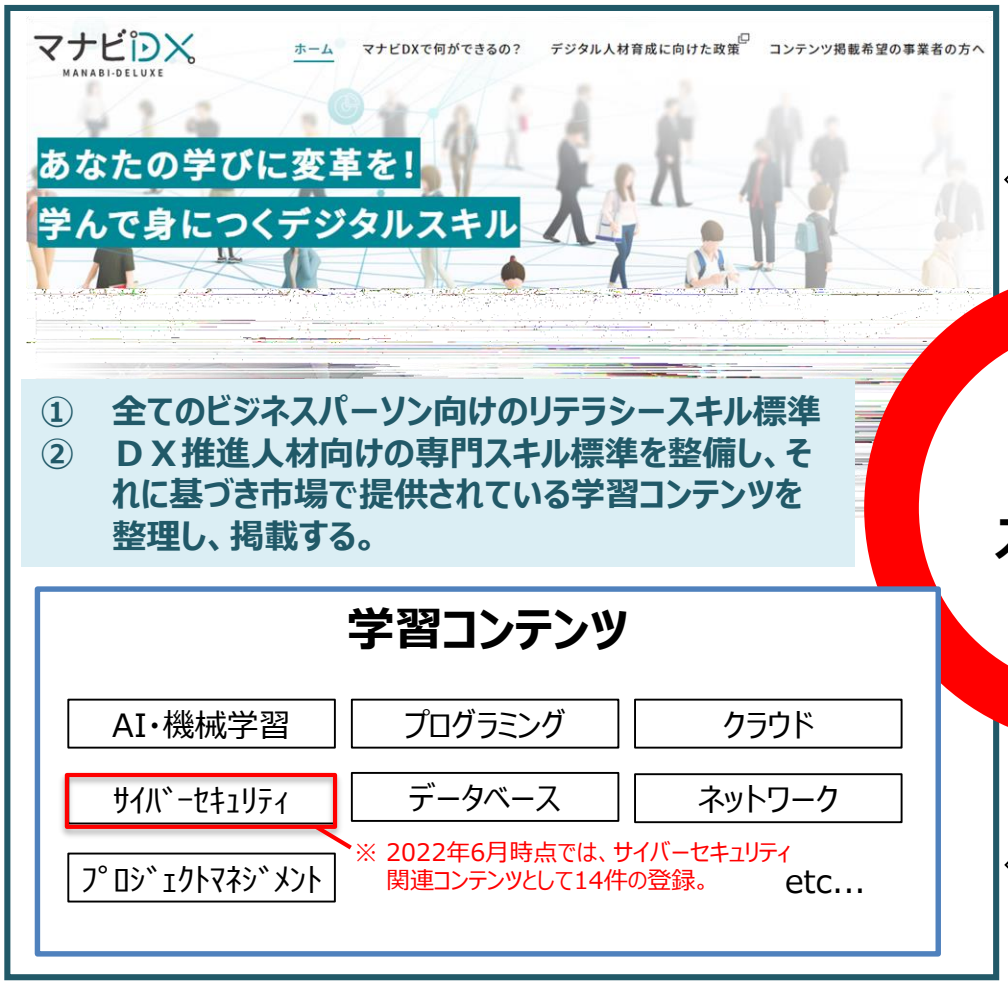


[出典] 第3回デジタル田園都市国家構想実現会議 経済産業省資料（2022年2月）を一部修正

（参考）デジタル人材育成プラットフォームにおけるポータルサイト・コンテンツ整備

経済産業省等

- スキル標準（分野・レベル）に紐付ける形で、民間や大学等が提供する様々な学習コンテンツや講座（URL等）を提示する。
- 利用者は目標の人材像に向け、デジタルスキル標準で整理された学習コンテンツを使い、学習や社内教育を行う。
- 民間事業者等は、デジタルスキル標準と紐付けされた学習コンテンツを利用者へ提供し、修了証を発行する。



講座情報検索

デジタルスキル標準

利用者（個人・企業）

必要とする人材像を目標として、デジタルスキル標準で整理された学習コンテンツを使い、学習や社内教育を行う

学習

修了証

コンテンツ掲載

学習コンテンツ提供事業者

Google
CHANGE
PEOPLE, BUSINESS, JAPAN
IPA
SHOWCASE
AVILEN
SkillUp AI
Practical Machine Learning Courses
TRAINOCATE
AIJobColle
DIVE INTO CODE
zero one
等

[出典] 経済産業省 第5回デジタル時代の人材政策に関する検討会資料（2022年3月）を一部加工

（参考）教育訓練給付制度

厚生労働省

労働者が費用負担し、厚生労働大臣が指定する教育訓練を受けた場合に、その費用の一部を「教育訓練給付」として雇用保険により支援。

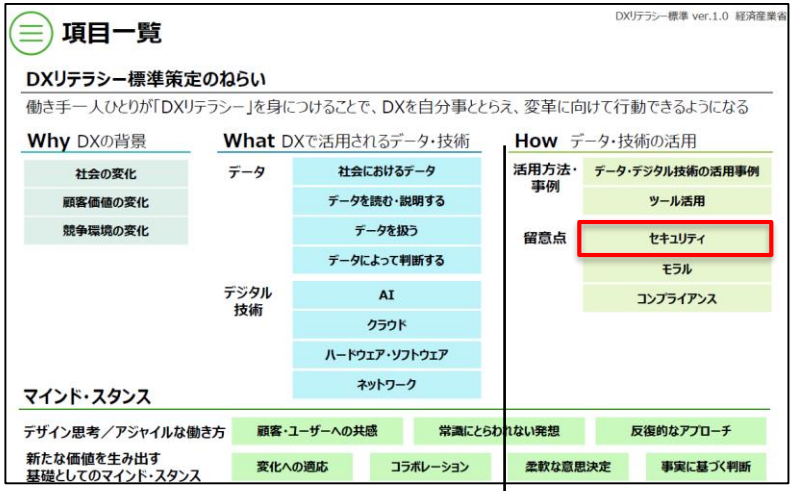
	専門実践教育訓練給付（2014年10月制度開始） **<特に労働者の中長期的キャリア形成に資する教育訓練受講を対象>**	**特定一般教育訓練給付**（2019年10月制度開始） **<特に労働者の速やかな再就職及び早期のキャリア形成に資する教育訓練受講を対象>**	**一般教育訓練給付**（1998年12月制度開始） **<左記以外の雇用の安定・就職の促進に資する教育訓練受講を対象>**
給付内容	○ 受講費用の**50%**（上限**年間40万**円）を６か月ごとに支給。 ○ 訓練修了後１年以内に、資格取得等し、就職等した場合には、受講費用の**20%**（上限**年間16万**円）を追加支給。	○ 受講費用の**40%**（上限**20万**円）を受講修了後に支給。	○ 受講費用の**20%**（上限**10万円**）を受講修了後に支給。
支給要件	在職者又は離職後１年以内（妊娠、出産、育児、疾病、負傷等で教育訓練給付の対象期間が延長された場合は最大20年以内）の者 ＋ 雇用保険の被保険者期間３年以上 （初回の場合は２年以上）	在職者又は離職後１年以内（妊娠、出産、育児、疾病、負傷等で教育訓練給付の対象期間が延長された場合は最大20年以内）の者 ＋雇用保険の被保険者期間３年以上 （初回の場合は１年以上）	在職者又は離職後１年以内（妊娠、出産、育児、疾病、負傷等で教育訓練給付の対象期間が延長された場合は最大20年以内）の者 ＋ 雇用保険の被保険者期間３年以上 （初回の場合は１年以上）
対象講座数	2,627講座（2022年４月時点） 累計新規指定講座数 4,441講座 ※平成29年４月時点の給付対象講座数に、その後新規指定された講座数を加えた数	557講座（2022年４月時点）	11,378講座（2022年４月時点）
受給者数	29,404人（2020年度実績）／100,846人（制度開始～2020年度） ※いずれも初回受給者数。	1,647人（2020年度実績）※速報値	89,011人（2020年度実績）※速報値
対象講座指定要件（講座の内容に関する主なもの）	**次の①～⑦の類型のいずれかに該当し**（【】内は講座期間・時間要件）**かつ、類型ごとの講座レベル要件を満たすものを指定。** **① 業務独占資格又は名称独占資格に係るいわゆる養成施設の課程** 受験率、合格率及び就職・在職率の実績が一定以上 （看護師・準看護師、社会福祉士の養成課程等）【原則１年以上３年以内で、かつ取得に必要な最短期間（法令上の最短期間が４年の管理栄養士の課程及び法令上の最短期間が３年の養成課程であって定時制により訓練期間が４年となるものを含む※1）】 **② 専門学校の職業実践専門課程及びキャリア形成促進プログラム**※2 就職・在職率の実績が一定以上　文部科学省連携 （商業実務、経理・簿記等）【２年（キャリア形成促進プログラムは120時間以上２年未満）】 **③ 専門職大学院**（MBA等） 【２年以内（資格取得につながるものは、３年以内で取得に必要な最短期間）】 就職・在職率、認証評価結果、定員充足率等の実績が一定以上 **④ 職業実践力育成プログラム**（子育て女性のリカレント課程、ビジネス等）※1 【正規課程：１年以上２年以内、特別の課程：時間が120時間以上かつ期間が２年以内】　文部科学省連携 就職・在職率（正規課程にあっては、就職・在職率及び定員充足率）の実績が一定以上 **⑤ 一定レベル以上の情報通信技術に関する資格取得を目標とする課程** （情報処理安全確保支援士等）※2 【時間が120時間以上（ITSSレベル相当４以上のものに限り30時間以上※3）かつ期間が２年以内】 受験率、合格率及び就職・在職率の実績が一定以上 **⑥ 第四次産業革命スキル習得講座**（AI、IoT等）※4 就職・在職率の実績が一定以上　経済産業省連携 【時間が30時間以上かつ期間が2年以内】 **⑦ 専門職大学・専門職短期大学・専門職学科の課程**※5 【専門職大学・大学の専門職学科：4年、専門職短期大学・短期大学の専門職学科：３年以内】 就職・在職率、認証評価結果、定員充足率等の実績が一定以上 ※1：2016年4月から適用　※2：2016年10月から適用　※3：2017年10月から適用 ※4：2018年4月から適用　※5：2019年4月から適用	**次の①～③の類型のいずれかに該当しかつ、類型ごとの講座レベル要件を満たすものを指定。** **① 業務独占資格、名称独占資格若しくは必置資格に係るいわゆる養成施設の課程**(※)**又はこれらの資格の取得を訓練目標とする課程等** （介護職員初任者研修、生活援助従事者研修、特定行為研修等を含む） ※　専門実践教育訓練の①に該当するものを除く。 受験率、合格率及び就職・在職率の実績が一定以上 **② 情報通信技術に関する資格のうちITSSレベル２以上の情報通信技術に関する資格取得を目標とする課程** （120時間未満のITSSレベル3を含む） ※　専門実践教育訓練の⑤に該当するものを除く。 受験率、合格率及び就職・在職率の実績が一定以上 **③ 短時間のキャリア形成促進プログラム及び職業実践力育成プログラム**　文部科学省連携 ※　専門実践教育訓練の②・④に該当するものを除く。 就職・在職率の実績が一定以上 ※ 趣味的・教養的な教育訓練、入門的・基礎的な水準の教育訓練、職業能力を評価するものとして社会一般に認知されていない免許資格・検定に係る教育訓練は、対象外。 ※ 講座時間・期間要件 通学制：期間が１ヶ月以上１年以内であり、かつ時間が50 時間以上、通信制：３ヶ月以上１年以内	**次の①又は②のいずれかに該当する教育訓練を指定。** ① **公的職業資格**又は**修士若しくは博士の学位等**の取得を訓練目標とするもの ② ①に準じ、**訓練目標が明確であり、訓練効果の客観的な測定が可能なもの**（民間職業資格の取得を訓練目標とするもの等） ※ 趣味的・教養的な教育訓練、入門的・基礎的な水準の教育訓練、職業能力を評価するものとして社会一般に認知されていない免許資格・検定に係る教育訓練は、対象外。 ※ 講座時間・期間要件は原則として以下のとおり。 ・ 通学制：期間が１ヶ月以上１年以内であり、かつ時間が50 時間以上 ・ 通信制：３ヶ月以上１年以内 指定講座例 ○ 輸送・機械運転関係（大型自動車、建設機械運転等） ○ 医療・社会福祉・保健衛生関係（同行援助従事者研修等） ○ 専門的サービス関係（社会保険労務士、税理士、司法書士等） ○ 情報関係（プログラミング、CAD、ウェブデザイン等） ○ 事務関係（簿記、英語検定等） ○ 営業・販売・サービス関係（宅地建物取引主任者等） ○ 技術関係（建築施工管理技士検定、電気主任技術者等） ○ 製造関係（技能検定等） ○ その他（大学院修士課程等）

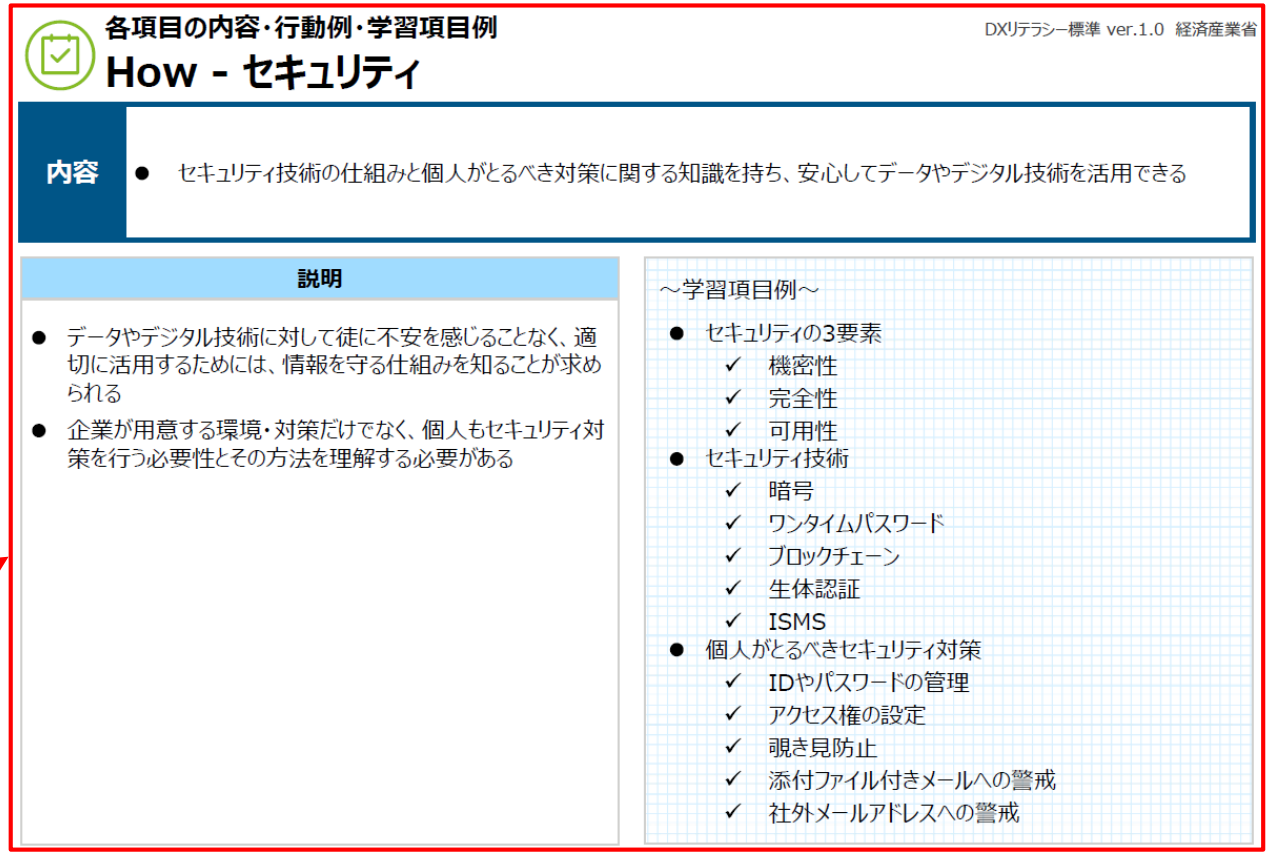
サイバーセキュリティを含む
デジタル関係講座等実績
講座数：397講座　修了者数：5,206人
※修了者数は令和２年度実績

（参考）スキル標準の整備

経済産業省

■ DXリテラシー標準：2022年3月 経済産業省策定





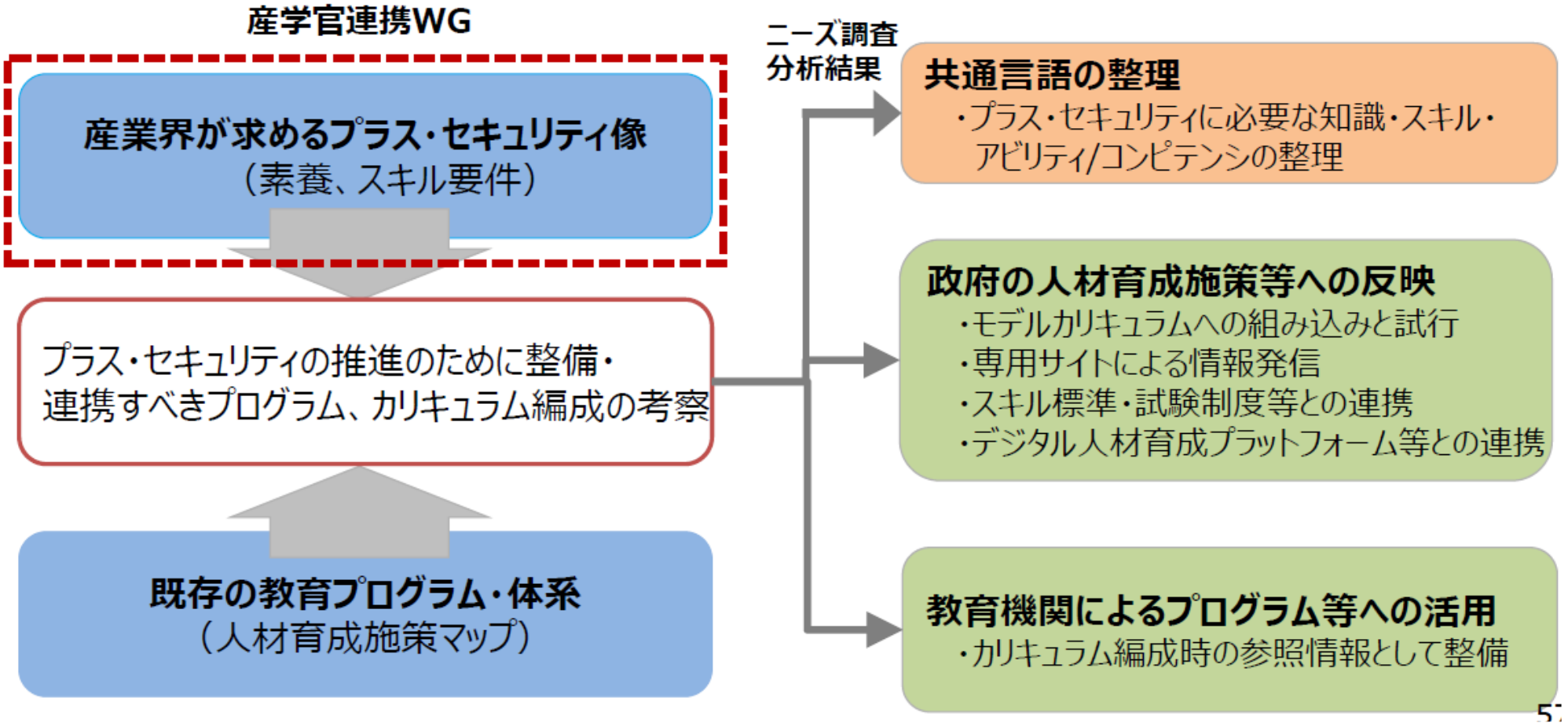
[出典] DXリテラシー標準 ver.1.0（2022年3月 経済産業省）

■ DX推進人材（サイバーセキュリティスペシャリスト）標準：2022年中に策定予定（経済産業省）

プラス・セキュリティ知識補充の推進とスキル標準等との関係

NISC・経済産業省

- 産業界主導の枠組みであるSC3（サプライチェーン・サイバーセキュリティ・コンソーシアム）の下に立ち上げられた産学官連携ワーキンググループにおいて、プラス・セキュリティの推進について検討。
- NISC・経産省で連携し、デジタル人材育成プラットフォームに関する取組との連携等に取り組む。

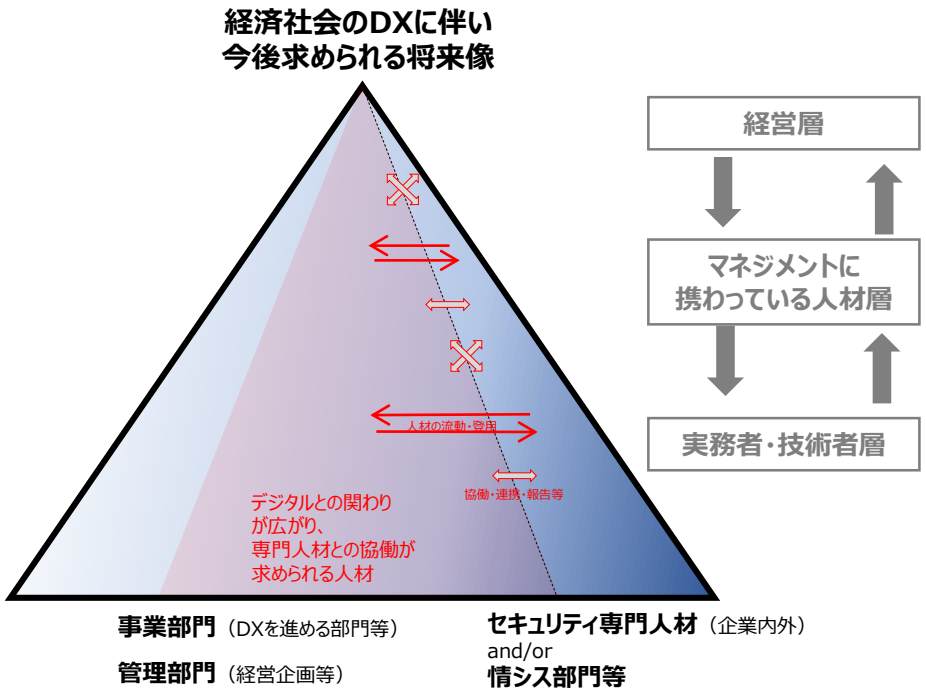


[出典] 経済産業省 産業サイバーセキュリティ研究会 第8回ワーキンググループ2（経営・人材・国際）資料（2022年3月）

プラス・セキュリティ知識補充プログラム カリキュラム例の策定

NISC

- 業務、製品・サービスのデジタル化が進展する中で、今後は、経営層やDXを進める部門でマネジメントに携わる人材層などで、「プラス・セキュリティ知識」が必要となる場面が増えると想定される。
- プラス・セキュリティ知識を補充するプログラムは、潜在的な需要が大きいと考えられる一方、市場形成が不十分であるため、民間教育事業者等の参考となるようなカリキュラム例を作成・公開。



➢ 様々な人材層・部門において、専門人材との協働が求められる。
（協働のためには、互いの領域への相互理解が前提となる。）

■ プラス・セキュリティ知識：

セキュリティ専門人材との協働を行うに当たって必要となる知識として、時宜に応じてプラスして習得すべき知識

（参考）米国での事例 ※日本ではこうしたプログラムは僅少

Cyber-Risk Oversight Certificate

概要:

- 全米取締役協会（NACD）がカーネギーメロン大学の協力を得てオンラインで提供している取締役向けサイバーリスク管理に関する概説的コース
- 最終試験に合格することで履修証明の取得が可能
- NACD Director's Handbook on Cyber Risk Oversight の事前参照を推奨
- 時間：16時間（最終試験を含む、オンラインで都合のよい時間に受講可）
- 価格：非会員$4,495- 会員$3,995-

（参考）カリキュラム例の構成

NISC

	A. 経営層向け	B. 部課長級向け
目標	● サイバーセキュリティが自社のコーポレートリスクに与える影響の把握 ● 影響を踏まえた自社のセキュリティ体制構築・投資の決定・指示 ● インシデント発生時の適切な経営判断・指示	● サイバーリスクが自部署に与える影響理解 ● 自部署で実施されている対策の現状理解 ● 上記の経営層への報告 社内外とのコミュニケーション
時間設定	7.5時間（集合講習3時間＋オンデマンド4.5時間（うち必須3時間））	11時間（集合講習4.5時間＋オンデマンド6.5時間（うち必須5.5時間））
留意点	● 経営会議及び対外対応として実際に起こり得るケースから逆算。 ● 各コマのインプット項目では、部課長級向けから内容を限定・変更。	● 部署内会議やベンダー管理で実際に起こり得るケースから逆算。 ● 既存のスキル等フレームワーク（SP800-181等）と紐付けを実施。
1.基礎知識	①デジタルインフラの基本（30分）◇ ②デジタル技術の基盤とリスク（30分）◇ ③デジタル環境のコストと運用責任（30分）◇	①デジタルインフラ入門（20分）◇ ②サイバーセキュリティに関する用語の意味（20分）◇ ③デジタル環境の管理や責任に関するキーワード（20分）◇ ①デジタルインフラの要点（30分）◆ ②デジタル技術の基盤とリスク（30分）◆ ③デジタル環境のコストと運用責任（30分）◆
2.脅威と対策	①サイバー攻撃手法とそのトレンド（30分）◆ ②脅威への対策（30分）◆ ③事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーション等）（30分）★	①サイバー攻撃手法とそのトレンド（30分）◆ ②脅威への対策（30分）◆ ③事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーション等）（30分）★ ④演習1：脅威と対策における“悪い見本”から学ぶ（60分）★
3.投資	①コーポレートリスクとしてのサイバーセキュリティ（コンプライアンスを含む）（30分）◆ ②体制構築・人材確保（30分）◆ ③演習1：各種対策の費用、損失想定、確率値から必要な投資を検討（70分）★	①サイバーセキュリティのリスクマネジメントの特徴（30分）◆ ②対策における費用と損失の考え方（30分）◆ ③リスクマネジメントのケーススタディ（30分）★ ④演習2：自部署リスクとその対応策を洗い出し、リスク管理部門等へ説明（60分）★
4.SHとの関係	①インシデント対応における経営層の役割（30分）◆ ②通常時の備えと情報開示の在り方（30分）◆ ③インシデント対応と情報開示の事例から学ぶ（30分）★ ④演習2：インシデント発生時の模擬記者会見（50分）★	①インシデント対応プロセスとその準備（30分）◆ ②通常時の備えとインシデント情報の取扱上のポイント（30分）◆ ③インシデント対応と情報開示の事例から学ぶ（30分）★ ④演習3：インシデント発生時の社内外連絡（60分）★
5.関係法令	–	①サイバーセキュリティに関する国内法令とその読み方（20分）◆ ②サイバーセキュリティに関する基準・規格等（20分）◆ ③サイバーセキュリティに関するガイドライン等（20分）◆

★：集合講習での開催が推奨されるもの（受講必須）
◆：オンライン・オンデマンド形式での実施を想定（受講**必須**）
◇：オンライン・オンデマンド形式での実施を想定（受講**任意**）

（参考）カリキュラム例とDX人材に関するスキル標準との関係性

■ 「デジタル人材育成プラットフォーム」との連携等の観点から、2022年3月に策定された「DXリテラシー標準」との関係性を整理（いずれの項目も含む）。今後策定される各専門人材向けスキル標準との関係も整理。

NISC プラス・セキュリティ知識補充講座 カリキュラム例	経済産業省 DXリテラシー標準 セキュリティ関連項目 学習項目例		
	セキュリティの3要素	セキュリティ技術	個人がとるべきセキュリティ対策
1.基礎知識 ○サイバーセキュリティに関する用語の意味 • ソフトウェア開発と脆弱性 • インターネットの仕組み • デジタルのリスクに関する諸概念 ○デジタル技術の基盤とリスク • ソフトウェア開発と脆弱性 • デジタルリスクとその対策	機密性、完全性、可用性	暗号、ブロックチェーン ワンタイムパスワード、 生体認証、ISMS	
2.脅威と対策 ○脅威への対策 • 対策の基本的な考え方 • 対策実施上の留意点			IDやパスワードの管理、アクセス権の設定 覗き見防止 添付ファイル付きメール・社外メールアドレスへの警戒

（参考）カリキュラム例とSP800-181との関係性

NISC

■ 人材育成施策への活用や国際協調等の観点から、米国NISTが策定する、サイバーセキュリティ人材に係るフレームワークであるSP800-181との関係性を整理。

■ **SP800-181**：

○米国NIST（国立標準技術研究所）において策定された、サイバーセキュリティに関する業務の性質を共有し、人材育成施策等の開発に活用されることを目的に、個別のタスクの遂行に必要な知識（Knowledge）、スキル（Skill）、能力（Ability）を記述する参照構造。

NISC プラス・セキュリティ知識補充講座 カリキュラム例	**SP800-181において各Role※求められる知識・スキル・能力（一部例）**
1.基礎知識	[K0006]サイバーセキュリティの喪失による特定の運用上の影響に関する知識 [K0044]（機密性、完全性、可用性、認証、否認防止に関連する）サイバーセキュリティとプライバシーの原則と組織の要件に関する知識
2.脅威と対策	[K0147]新たに出現したセキュリティ問題、リスク及び脆弱性に関する知識 [S0358]テクノロジーインフラの進化を意識し続けるスキル
3.投資	[K0154]サプライチェーンリスクマネジメントの標準、プロセス及びプラクティスに関する知識 [S0147]サイバーセキュリティの原則と教義に基づいたセキュリティ管理策を評価するスキル（例：CIS CSC、NIST SP 800-53、サイバーセキュリティフレームワークなど）
4.ステークホルダーとの関係	[A0077]他の組織の機能やサポート活動とサイバーセキュリティ業務とを調整する能力
5.関係法令	[K0003]サイバーセキュリティとプライバシーに関する法律、規制、政策及び倫理に関する知識

※「デジタル化を推進する部門のマネジメントを担う部課長級」が担う役割と類似要素を含む以下のWork Roleに求められる知識・スキル・能力を抽出。

許可権限者(Authorizing Official/Designating Representative)　セキュリティ管理策査定者(Security Control Assessor)　幹部によるサイバーリーダーシップ(Executive Cyber Leadership (EXL))
事業計画マネージャー(Program Manager)　ITプロジェクトマネージャー(Information Technology Project Manager)　ITポートフォリオ管理者(IT Investment / Portfolio Manager)

国際連携の取組

- 5月に開催された日米豪印首脳会談において、能力構築や「サイバーセキュリティ・デイ」について協力を確認。
- 各国と協調しつつ、国内においても必要な対応を検討していく。

■2022年5月24日(火) 日米豪印首脳会合 共同声明【抜粋】

Cybersecurity

In an increasingly digital world with sophisticated cyber threats we recognize an urgent need to take a collective approach to enhancing cybersecurity. To deliver on the Quad Leaders' vision for a free and open Indo-Pacific, we commit to improving the defense of our nations' critical infrastructure by sharing threat information, identifying and evaluating potential risks in supply chains for digitally enabled products and services, and aligning baseline software security standards for government procurement, leveraging our collective purchasing power to improve the broader software development ecosystem so that all users can benefit. **The Quad partners will coordinate capacity building programs in the Indo-Pacific region under the Quad Cybersecurity Partnership**, and **will initiate the first-ever Quad Cybersecurity Day to help individual internet users across our nations, the Indo-Pacific region, and beyond to better protect themselves from cyber threats**.

サイバーセキュリティ　（仮訳）

高度なサイバー脅威が存在し、ますますデジタル化する世界において、我々は、サイバーセキュリティを強化するために共同のアプローチをとることが急務であることを認識する。自由で開かれたインド太平洋という日米豪印のリーダーのビジョンを実現するために、我々は、脅威情報の共有を通じて各国の重要インフラ防護を強化すること、デジタル対応の製品・サービスのサプライチェーンにおける潜在的リスクを特定・評価すること、及びソフトウェア開発エコシステム全体を強化して全てのユーザーが便益を感じられるよう我々の共同の購買力を活かして政府調達における基本的なソフトウェアセキュリティ基準を整合させることにコミットする。日米豪印パートナーは、**日米豪印サイバーセキュリティ・パートナーシップの下、インド太平洋地域における能力構築プログラムについて協調**し、**日米豪印各国、インド太平洋地域及びそれ以外の地域の一人一人のインターネットユーザーがサイバー脅威からより防御できるよう、初めて日米豪印サイバーセキュリティ・デイを開始する予定である。**

■対応例

- ✓ 関係国間で、必要となるスキルに関する「共通要素」を特定し、官民の人材育成プログラムにも活用する。
- ✓ 関係省庁、教育機関、民間企業などの官民の様々な主体に対して、参画を促す。

CYNEX：サイバーセキュリティ統合知的・人材育成基盤（人材育成基盤のオープン化）

総務省

- CYNEX：サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学官の結節点として開放する取組。
- その一環として、演習シナリオ・システムをオープン化し、民間事業者や教育機関等による事業を促進。

[出典] 総務省 第36回サイバーセキュリティタスクフォース資料（2022年3月）

多様な人材の育成・活躍促進に向けた取組の方向性

NISC

- 脅威の巧妙化・複雑化を踏まえ、男女や学歴等によらない多様な視点や優れた発想を取り入れつつ、実践的な対処能力を持つ人材の育成・活躍促進が急務。
- 以下のような、「働くことに困難さを抱えた方」を対象にした、サイバーセキュリティに係るスキル習得のための支援プログラムなど、今後、こうしたモデルの横展開に向けた検討を進める。

■ **R-PAC (Reskilling Program Against the Covid-19)**：厚生労働省 新型コロナウイルス感染症セーフティネット強化交付金事業
（実施団体：認定NPO法人 育て上げネット、協力団体：デジタルハーツ、Microsoft Global Skills Initiative）

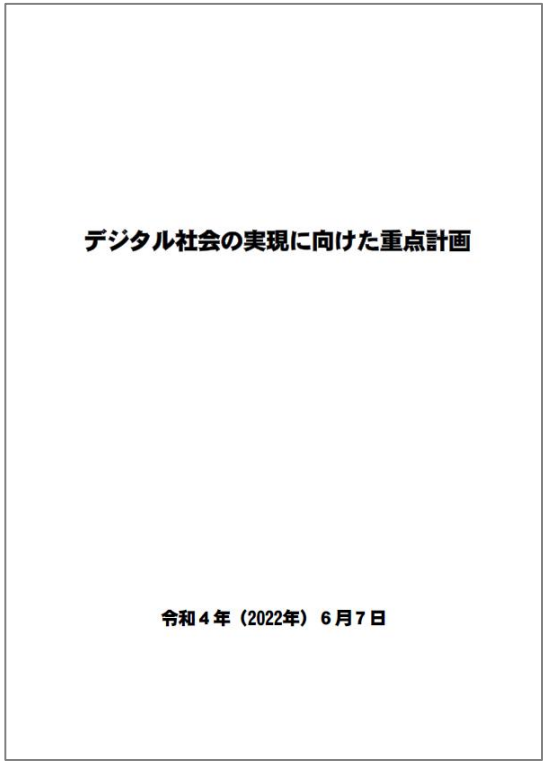
⇒ 計約1,000名が参加し、うち約800名がサイバーセキュリティ基礎・応用講座に参加

政府機関におけるデジタル人材の確保・育成に向けた取組

デジタル庁・NISC

- デジタル庁、NISC等において、各府省庁の取組支援の一環として、デジタル化の進展等を踏まえて必要となる能力を整理し、その育成のために必要となる研修の体系・内容・手法・対象等の継続的な見直しを実施。
- 具体的には、①既存の研修を整理し所定の資格試験の合格をもって研修修了に代える仕組みの創設や、②スキル認定において、所定の資格試験の合格を認定要件にすることにより組織の垣根を超えて比較可能な仕組みとすること等を検討する。

「デジタル社会の実現に向けた重点計画」＜抜粋＞（令和4年6月7日 閣議決定）



第６　６．（２）② ウ ｉ）　政府デジタル人材（部内育成の専門人材）の確保・育成

各府省庁において、政府デジタル人材を確保・育成するため、次の取組を推進する。

- 各府省庁の統括部局、一定のシステム 所管部局の体制を整備し、人材を拡充するとともに、あらゆる部局でDXや業務改革（BPR）、データ利活用等を進めるために必要な人材を広く活用できるよう、体制を整備し、人材の拡充を行う。
- 令和４年度（2022年度）以降の国家公務員採用試験にから新設等された総合職試験の「デジタル」区分及び一般職試験の「デジタル・電気・電子」区分について、デジタル庁を中心に各府省庁において合格者の積極的な採用に努めるとともに、啓発活動・人材確保活動を通じて積極的な広報を実施する。
- 各府省庁において、「デジタル人材確保・育成計画」の一環として、研修受講、出向、スキル認定等に係る具体的な目標を設定した「政府デジタル人材育成支援プログラム」を策定・改定し、人材の適切な育成について明記する。
- デジタル庁、NISC等は、各府省庁が策定・改定する上記計画やプログラムに基づく人材の確保・育成を支援する。特に、デジタル化の進展等を踏まえて必要となる能力を整理し、その育成のために必要となる研修の体系・内容・手法・対象等の継続的な見直しを行う。
- 具体的には、より客観的で一貫性のある人材の育成を目指し、既存の研修を整理し所定の資格試験の合格をもって研修修了に代える仕組みの創設やデジタル化の進展を踏まえた研修の提供、スキル認定においては、所定の資格試験の合格を認定要件にすることにより、組織の垣根を超えて比較可能な仕組みとすることや、課室長級職員のスキルについても認定対象とすることを検討する。その際、これまでの政府デジタル人材育成の経緯、状況も踏まえ、経過措置についても検討を進める。【追加】
- 政府デジタル人材に対する適切な処遇の確保のため、手当等を活用し、一定の給与上の評価を行うとともに、「デジタル人材確保・育成計画」の中で、出向等の機会を捉えた昇任等も含め、高位のポストまでを見据えた人事ルート例（イメージ）を設定する。

上記の取組に加え、デジタル庁を中心として、国、地方公共団体、民間企業、独立行政法人など、組織の垣根を超えた人材の行き来や、デジタル庁と各府省庁等の職員が一体的にシステムの開発・運用等を行うことを通じて人材の育成が行われるような環境の整備を行う。

サイバー攻撃を受けた組織における対応事例集

NISC

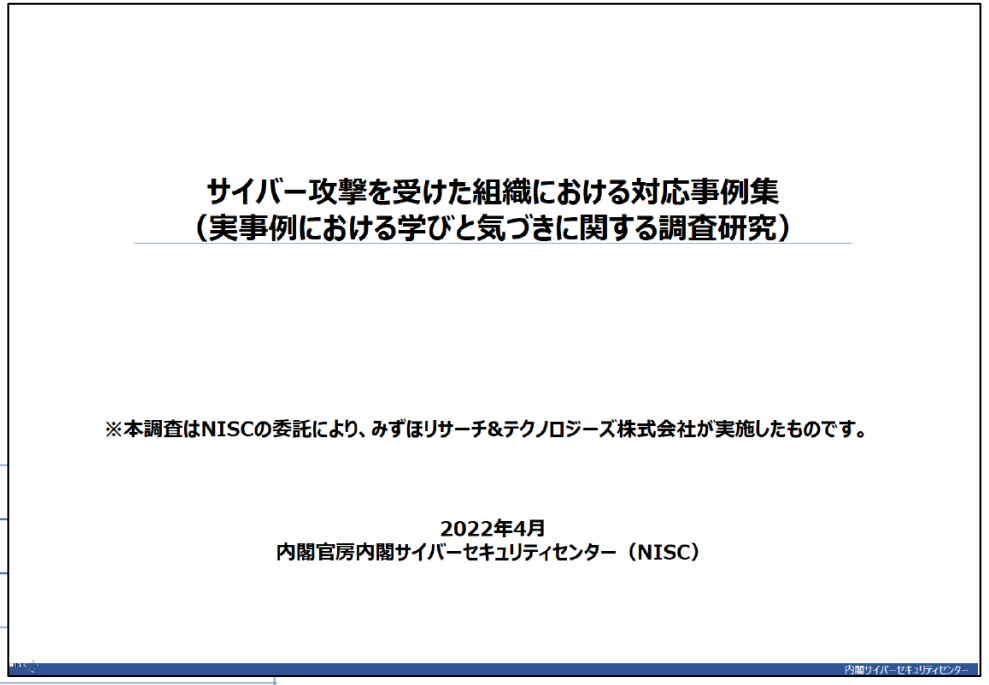
- サイバー攻撃を受けた企業や研究機関などの協力の下、これら組織が実際に講じたインシデント対応や、体制強化、人材確保等について、事例調査を実施。
- これらの実例を様々な組織でのサイバーセキュリティ対策の検討のヒントとしていただくべく、得られた教訓や気づきを含め、本年4月に事例集として公開。

■想定利用シーン

- ✓ 経営層の方が、様々な組織の取組を概観し、経営課題としてのサイバー攻撃対処への理解を深める
- ✓ 戦略マネジメント層の方が、予算確保等、経営層と現場をつなぐ工夫に活用する
- ✓ 現場でインシデント対処やセキュリティ対策の実装に携わる実務者・技術者の方が、サイバーセキュリティ対策の検討のヒントを得る

■ 調査事例

ケース１　Webホスティングサービスの改ざんに関する調査研究
ケース２　グローバルな企業グループでのランサムウェア感染に関する調査研究
ケース３　多数の国内拠点を有する企業のランサムウェア感染に関する調査研究
ケース４　サプライチェーンを介した標的型メール攻撃に関する調査研究
ケース５　開発中のクラウドサービスへの不正アクセスに関する調査研究
ケース６　グループ会社を経由した高度標的型攻撃に関する調査研究
ケース７　学術研究機関のセキュリティ体制に関する調査研究
ケース８　利用中の外部サービスを介した組織内への不正アクセスに関する調査研究
ケース９　インターネットを経由した社内システムへの不正アクセスに関する調査研究（その１）
ケース10　インターネットを経由した社内システムへの不正アクセスに関する調査研究（その２）



（参考）対応事例集の掲載情報の例

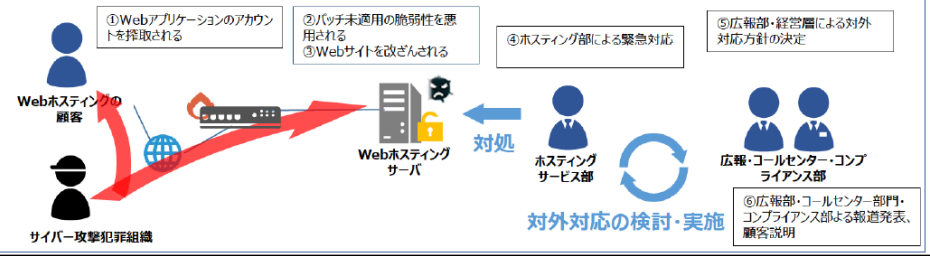
NISC

ケース1	Webホスティングサービスの改ざんに関する調査研究	想定読者	基本的取組み	組織属性	ホスティングサービス企業	要因	パッチ未適用

1．概要

- 本事例のA社は、Webホスティングサービスを提供している。
- サービス利用顧客が独自に導入したWebアプリケーションに対して、攻撃者になりすましログインされた後、Webサーバーが稼働するOSの脆弱性を悪用され、Webホスティングサービス上のコンテンツを改ざんされた。
- ホスティングサービスであることから、顧客が導入するWebアプリケーションのセキュリティ対策に関与することが困難であった。また、侵入されたWebサーバのOSには、既知の脆弱性が存在していたが、顧客サービスへの影響を考慮して、パッチ適用を見合わせていた。
- 攻撃の発覚後、ホスティングサービス部による迅速な不正ファイル削除、影響確認作業、広報部による広報活動等により、甚大な顧客被害、経営被害には至らなかった。

2．状況



3．時系列（組織毎の検知・分析・対処）

日時	①経営層	②広報・コンプライアンス部・コールセンター	③ホスティングサービス部
1日目（休）	• Webホスティングサービスの特定顧客が独自に導入したWebアプリケーションのアカウントに正規アカウントで不正ログインされた後、WebサーバーのOSの脆弱性を悪用され、不正なファイルがWebサーバー上に設置される		
1日目（休）夜間			• 運用担当者が、不正なファイルがWebサーバー上に設置されていることを確認 • 攻撃元からのアクセスを遮断 • 攻撃者が配置したファイル削除を開始
2日目（休）早朝			• 攻撃者が配置したファイルの削除完了 • 不正利用されたWebアプリケーションのアカウント停止 • 解析により、該当Webサーバーの正常性、顧客利用環境への影響を確認
3日目	• リスクが高い問題との認識に至り、全社的な問題に格上げし、役員会議にて取り扱いを協議	• コールセンターでの顧客問合わせへの対応 • マスコミからの問合わせへの対応 • 広報部門、コンプライアンス部門にて、サービス事業者としての告知タイミング、告知内容、公表範囲、メディアからの質問への回答方針を検討し、役員承認を得る	
		• JPCERT/CCから問い合わせ	
			• ホスティングサービスの利用顧客に、状況をメール連絡
5日目		• コンプライアンス部、広報部、ホスティングサービス部で対外発表対応を調整	
		• 不正アクセス被害とその対処が完了したことを対外発表 • JPCERT/CCに対応状況を回答	
7日目		• 不正アクセスの詳細を対外発表	

4．まとめ

背景・国内外の状況

- 本事象で悪用されたWebアプリケーションは、オープンソースソフトウェアであり、世界中のWebサイトで幅広く利用されているため、攻撃者の攻撃対象となりやすく、攻撃は、頻繁に行われている。
- 本件で悪用されたOSの脆弱性は、公知の脆弱性であり、設定の不備といった人的なものではない。

発生と検知、エスカレーションと役割分担、対応

- 「２.状況」、「３.時系列」を参照

サイバー攻撃による影響

- Webホスティングサービスの複数顧客のサイト（数千社）に、不正なファイルが配置されたことで、Webサイトの改ざんが発生した。

発生原因と根本原因の深堀り

- 悪用された脆弱性は、OSの既知の脆弱性である。
  - A社が**パッチを適用していれば**、本事象の発生は防止できた可能性が高い
- ホスティングサービス部門においても、原則としてセキュリティパッチ適用が定められているが、現場担当者にパッチ適用判断の裁量が与えられていた。**パッチ適用に関わる作業負担を軽減**できることもあり、各担当者は、当該パッチの緊急度が高くないと判断し、**パッチ適用を見送っていた**。
- 組織としても、**パッチ適用による顧客の利用環境への悪影響を懸念**しており、現サーバにパッチを適用するのではなく、脆弱性を解消した新しいホスティング環境を構築し、顧客に移行を打診していた。しかしながら、**契約上は移行の定めがなく**、新環境への顧客移行が進んでいない状況であった。

被害軽減に寄与した対策

- ホスティングサービス部門では、顧客の誤操作による意図しないコンテンツ改変事象に関する運用手順書を整備済であったため、インシデントによるコンテンツ改変自体への技術的対策を迅速に実施できた。手順書が整備されていなかった場合には、システムの復旧に多大な時間を要したと想定される。

4．まとめ

得られた気付き・教訓

- 脆弱性およびリスク管理が属人的であり、組織として対処する必要があり、対策した。
  - 組織としての脆弱性の対処基準を定めた。
  - 脆弱性情報を社内で共有・展開し、リスク認識を共有した。
- 24h×365d稼働を原則とするWebホスティングサービスのパッチ適用に関して、顧客との事前合意が必要であり、対策した。
  - パッチ適用運用に伴うサービス停止時間を含め、**SLAを明確化**した。
- インシデント発生時には、ホスティングサービス部門による判断と対処が中心となっていたため、全社的なインシデントへの対応体制を強化した。
  - 他サービス部門や管理部門を交えた**組織横断的な、インシデント対応体制を整備**した。
- 経営層と現場担当者とのコミュニケーション不足を改善した。
  - **経営層への報告を定例化**することで、経営層が現状および課題を的確に把握すると共に、現場担当者が経営層の意思決定に基づき迅速にセキュリティ対策に取り組むことができる。
  - セキュリティインシデントを経験し、経営へのインパクトが非常に大きいとの認識に至り、サービス維持よりもセキュリティを重視するように経営層の意識が変化した。
- 実務で利用するために**十分な詳細度で定義されたインシデント対応手順**に基づき、対処するように体制を再整備した。
  - サイバーセキュリティ基本動作を啓蒙、励行する。
  - **部門横断で、演習等を通じてインシデント対処体制を確立**する。

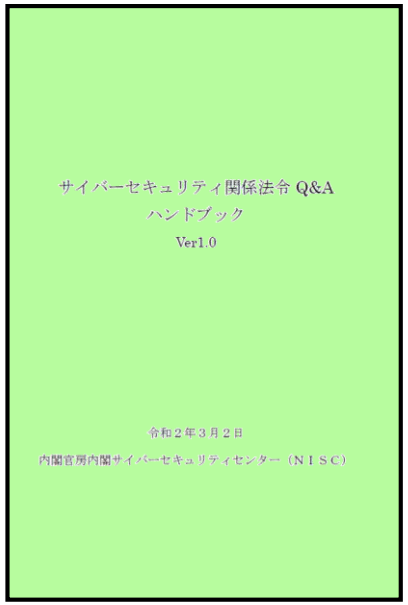
今後の課題

- **運用担当者のパッチ適用に関する作業負荷を低減**し、迅速なパッチ適用やセキュリティリスク分析を実施できる環境整備に取り組む方針である。
- **セキュリティインシデントの対応現場は、各社のノウハウ**そのものであり、インシデント対応にあたって最後に**頼る（は）人材**である。人材確保が難しい状況にあるが、**自社で確保**するように検討を進めている。
- 他部門では、**ISMS認証**を取得済であり、セキュリティマネジメントシステムを有効活用したいが、部門毎にセキュリティ運用の実態が異なっており、組織や手続きの整備と統合を**段階的に進める**よう検討している。
- 高度なサイバー攻撃への対処のために、更なる環境整備が必要である。
  - ログの効率的な取得、分析を属人管理から組織的管理とするため、**様々な機器のログの統合分析**、AIの利用をはじめとするツール選定が課題である。
  - **不審な動きの可視化**の必要性を認識しているが、**不審なふるまいの定義**などが課題である。
- 利用者責任範囲とセキュリティリスクを顧客に周知することが難しく、顧客の獲得と維持が難しくなることを懸念している。**セキュリティリスクを非常に低く認識している顧客に対して、丁寧な説明**とニーズにマッチしたサービスの提供を検討する方針である。

「サイバーセキュリティ関係法令Q&Aハンドブック」の改訂

NISC

- 「サイバーセキュリティ関係法令Q&Aハンドブック」は、サイバーセキュリティに関連する法令について、最新の内容を網羅的に整理し、それぞれの事項について解説を付したドキュメントとして、2020年3月に策定。
- 策定から2年超が経過したことから、①最新の内容へのアップデート、②企業の法務部門等での活用促進を目的として、昨年12月に設置した「サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ」において改訂の検討を行っており、2022年夏頃に改訂版を公表予定。



＜主なトピックス＞

1. **サイバーセキュリティ基本法関連**
2. **会社法関連**（内部統制システム等）
3. **個人情報保護法関連**
4. **不正競争防止法関連**
5. **労働法関連**（秘密保持・競業禁止等）
6. **情報通信ネットワーク関連**（IoT関連を含む）
7. **契約関連**（電子署名、システム開発、クラウド等）
8. **資格等**（情報処理安全確保支援士等）
9. **その他各論**（リバースエンジニアリング、暗号、情報共有等）
10. **インシデント対応関連**（デジタルフォレンジックを含む）
11. **刑事実体法**（サイバー犯罪等）
12. **海外法令**（GDPR等）

＜主な更新項目（案）＞

- サイバーセキュリティインシデント発生時の当局等対応
- 個人情報保護法関連（改正を踏まえた対応）
- テレワークにおけるセキュリティ
- 認証に関する法令について
- データの消去、データが記録された機器・電子媒体の廃棄
- ランサムウェア対応（データのバックアップ等）
- インシデント対応における費用負担及びサイバー保険
- 海外サイバーセキュリティ法令

＜参考＞「サイバーセキュリティ戦略」（令和3年9月28日閣議決定）**【抜粋】**

4．4．2　人材の確保、育成、活躍促進

（1）「DX with Cybersecurity」に必要な人材に係る環境整備

①「プラス・セキュリティ」知識を補充できる環境整備

対策推進に向けた専門人材との協働等に資するよう、**法令への理解を深めるツール等の活用促進**を図る。

デジタル活用支援推進事業との連携

- 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やサービスの利用方法等に対する助言・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に関する講座の追加に向けて検討中。

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（携帯キャリア・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