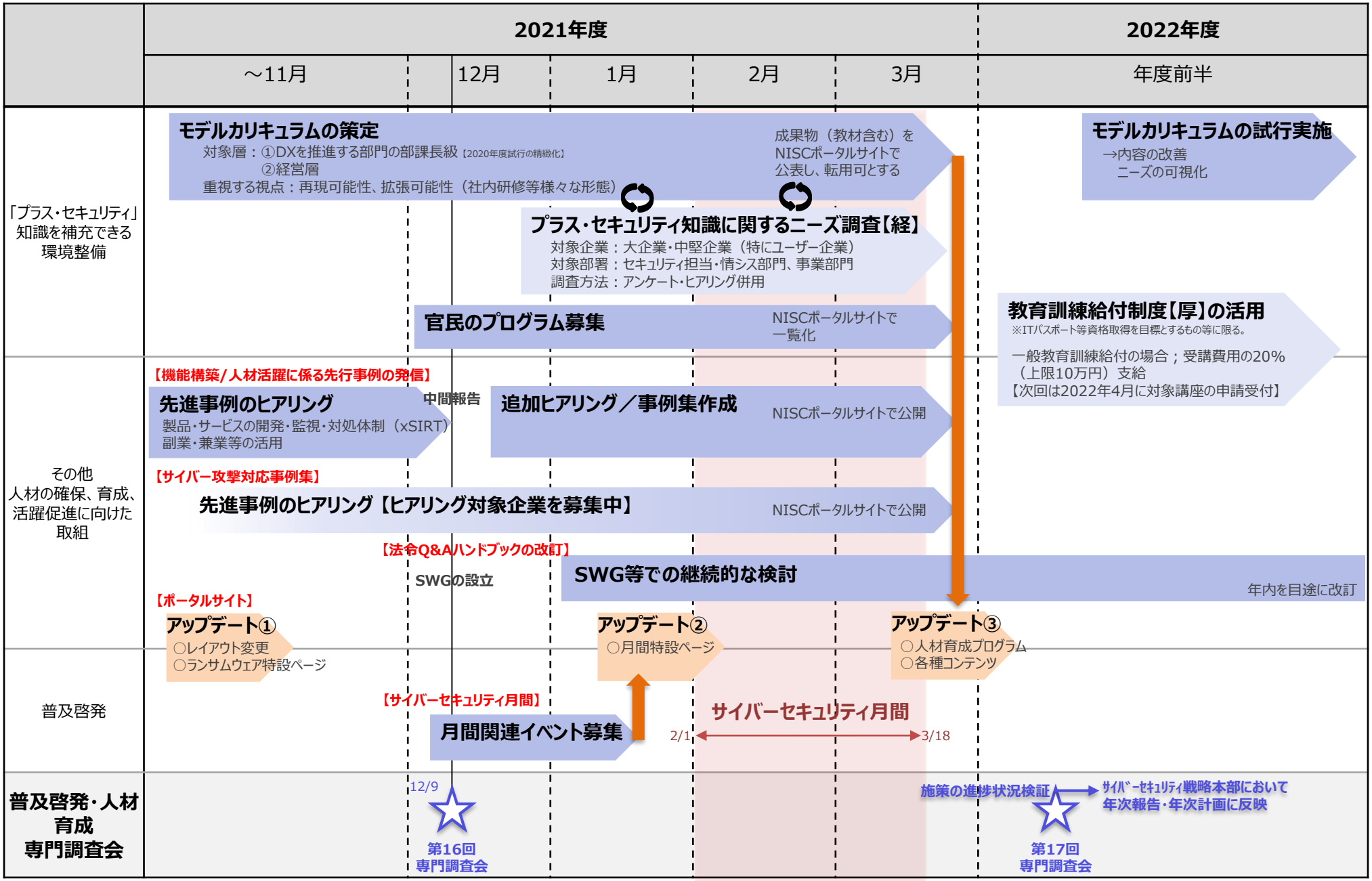
NISC National center of Incident readiness and Strategy for Cybersecurity

資料2

# 普及啓発・人材育成に係る取組状況について（報告）

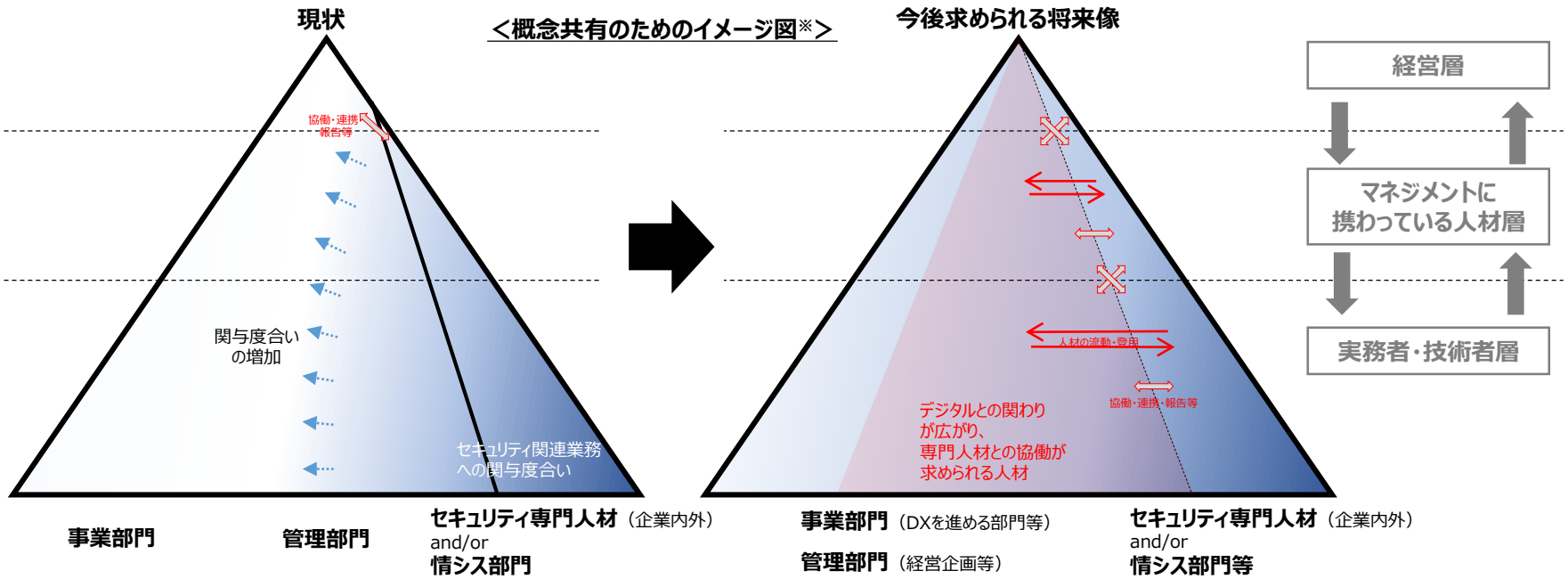
令和3年12月

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


2021年度
2022年度
～11月
12月
1月
2月
3月
年度前半
「プラス・セキュリティ」知識を補充できる環境整備
その他人材の確保、育成、活躍促進に向けた取組
普及啓発
普及啓発・人材育成専門調査会
モデルカリキュラムの策定
対象層：①DXを推進する部門の部課長級【2020年度試行の精緻化】
②経営層
重視する視点：再現可能性、拡張可能性（社内研修等様々な形態）
成果物（教材含む）をNISCポータルサイトで公表し、転用可とする
モデルカリキュラムの試行実施
→内容の改善
ニーズの可視化
プラス・セキュリティ知識に関するニーズ調査【経】
対象企業：大企業・中堅企業（特にユーザー企業）
対象部署：セキュリティ担当・情シス部門、事業部門
調査方法：アンケート・ヒアリング併用
官民のプログラム募集
NISCポータルサイトで一覧化
教育訓練給付制度【厚】の活用
※ITパスポート等資格取得を目標とするもの等に限る。
一般教育訓練給付の場合；受講費用の20%（上限10万円）支給
【次回は2022年4月に対象講座の申請受付】
【機能構築/人材活躍に係る先行事例の発信】
先進事例のヒアリング
製品・サービスの開発・監視・対処体制（xSIRT）
副業・兼業等の活用
中間報告
追加ヒアリング／事例集作成
NISCポータルサイトで公開
【サイバー攻撃対応事例集】
先進事例のヒアリング【ヒアリング対象企業を募集中】
NISCポータルサイトで公開
【法令Q&Aハンドブックの改訂】
SWGの設立
SWG等での継続的な検討
年内を目途に改訂
【ポータルサイト】
アップデート①
○レイアウト変更
○ランサムウェア特設ページ
アップデート②
○月間特設ページ
アップデート③
○人材育成プログラム
○各種コンテンツ
【サイバーセキュリティ月間】
月間関連イベント募集
サイバーセキュリティ月間
2/1
3/18
12/9
第16回専門調査会
施策の進捗状況検証
サイバーセキュリティ戦略本部において年次報告・年次計画に反映
第17回専門調査会

# 「プラス・セキュリティ」知識を補充できる環境整備

- 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、必ずしも現時点でITやセキュリティに関する専門知識や業務経験を有していない様々な人材も、あらゆる場面で企業内外のセキュリティ専門人材との協働が求められることが想定される。
- こうした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を、「プラス・セキュリティ」知識と整理し、「サイバーセキュリティ戦略」に位置づけ。
- 「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。需要・供給双方の顕在化に繋がる取組を両面で行い、市場の形成発展を促していく。




➢ DX進展の中で、特にDXを進めている事業部門や経営企画部門等において、セキュリティ関連業務との関与が増加していく。

➢ 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。）

※ 本イメージ図は、用語の考え方について強調すべき点を共有するための資料として、イメージを大まかに記した資料であり、本内容につき精緻化等を図るためものではない。

# （参考）SC3※ 産学官連携WGにおける「プラス・セキュリティ」に関するニーズ調査

| | |
|---|---|
| 件名 | 産業界が求めるプラス・セキュリティに関する調査 |
| 目的 | 特にプラス・セキュリティに着目し、産業界が求めるプラス・セキュリティの素養を調査し整理する。 |
| 期間 | 2021年度末まで |
| 調査手法 | ヒアリング調査。原則、リモート形式による。 |
| ヒアリング対象 | 大企業・中堅企業（特にユーザー企業）のセキュリティ担当部署、セキュリティ専門企業、コンサルティング会社等 |
| ヒアリング件数 | 10件程度（予定） |
| 人材スコープ | ユーザー企業におけるプラス・セキュリティ の人材層のうち、実務者・技術者層を調査対象の人材スコープとする。 |
| ヒアリング項目 | プラス・セキュリティに求められるスキル要件等に関する仮説を踏まえ、社内のセキュリティを向上する上での課題・対策・対応の優先度、及びプラス・セキュリティの推進に関する取組状況等が聞き取れるよう、既存の調査結果・公表情報等も踏まえつつヒアリング項目を作成する。 |

※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：
産業界が一丸となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策を推進していくことを目的とし、2020年11月1日に設立。
（2021年11月1日時点、96団体含む175会員。事務局:IPA）

# （参考）教育訓練給付制度

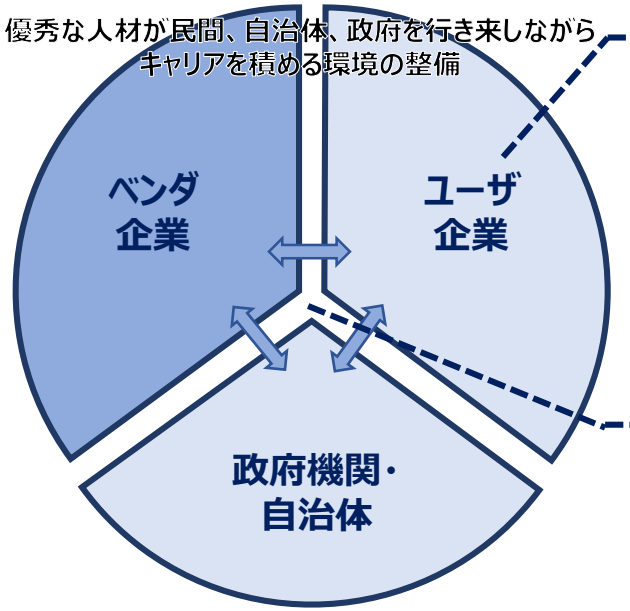
労働者が費用負担し、厚生労働大臣が指定する教育訓練を受けた場合に、その費用の一部を「教育訓練給付」として雇用保険により支援。

| | **専門実践教育訓練給付**（2014年10月制度開始）<br>**<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）<br>**<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）<br>**<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。<br>○ 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<br>＋ 雇用保険の被保険者期間３年以上<br>（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<br>＋雇用保険の被保険者期間３年以上<br>（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<br>＋ 雇用保険の被保険者期間３年以上<br>（初回の場合は１年以上） |
| 対象講座数 | 2,584講座（2021年10月時点）<br>累計新規指定講座数 4,266講座<br>※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 | 484講座（2021年10月時点） | 11,177講座（2021年10月時点） |
| 受給者数 | 23,251人（2019年度実績）／71,442人（制度開始～2019年度）<br>※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。**<br>**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**<br>受験率、合格率及び就職・在職率の実績が一定以上<br>（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）】<br>**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 文部科学省連携<br>就職・在職率の実績が一定以上<br>（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）】<br>**③ 専門職大学院**（MBA等）<br>【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）】<br>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<br>**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 文部科学省連携<br>【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】<br>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<br>**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**<br>（情報処理安全確保支援士等）※2<br>【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】<br>受験率、合格率及び就職・在職率の実績が一定以上<br>**⑥ 第四次産業革命スキル習得講座**（AI、IoT等）※4 経済産業省連携<br>就職・在職率の実績が一定以上<br>【時間が30時間以上かつ期間が2年以内】<br>**⑦ 専門職大学・専門職短期大学・専門職学科の課程**※5<br>【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】<br>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<br>※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<br>※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。**<br>**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**<br>（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）<br>※　専門実践教育訓練の①に該当するものを除く。<br>受験率、合格率及び就職・在職率の実績が一定以上<br>**② 情報通信技術に関する資格のうちITSSL２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**<br>（120時間未満のITSSレベル3を含む）<br>※　専門実践教育訓練の⑤に該当するものを除く。<br>受験率、合格率及び就職・在職率の実績が一定以上<br>**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<br>※　専門実践教育訓練の②・④に該当するものを除く。<br>就職・在職率の実績が一定以上<br>※ 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。<br>※ 講座時間・期間要件<br>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。**<br>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<br>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）<br>※ 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。<br>※ 講座時間・期間要件は原則として以下のとおり。<br>・ 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<br>・ 通信制：３ヶ月以上１年以内<br>指定講座例<br>○ 輸送・機械運転関係（大型自動車、建設機械運転等）<br>○ 医療・社会福祉・保健衛生関係（同行援助従事者研修等）<br>○ 専門的サービス関係（社会保険労務士、税理士、司法書士等）<br>○ 情報関係（プログラミング、CAD、ウェブデザイン等）<br>○ 事務関係（簿記、英語検定等）<br>○ 営業・販売・サービス関係（宅地建物取引主任者等）<br>○ 技術関係（建築施工管理技士検定、電気主任技術者等）<br>○ 製造関係（技能検定等）<br>○ 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：408講座　修了者数：4,591人
※修了者数は令和元年度実績

# 企業・組織内での機能構築 / 人材の流動性・マッチングの促進

- デジタル化進展に伴い新たに必要となるセキュリティに係る人材・仕事の需要・供給の好循環の形成、ひいてはDX with Cybersecurityの実現に向けて、企業・組織内での機能構築、人材の流動性・マッチングの観点から、セキュリティ人材が活躍できるような環境整備を進める。
- 特に、設計・開発から運用・監視、対処に係る体制・機能（xSIRT）や、人材の流動性・マッチングの促進に資する副業・兼業の活用等、新たなプラクティスの普及に向けて、先進事例の収集・整備を図る。




※ IT企業に所属する情報処理・通信に携わる人材の割合を諸外国比較すると、日本は72.0%と突出して高い。一方、日本以外の国は概ね5割以下であり、中でも米国は34.6%。（出典：IPA「IT人材白書2017」）

**企業・組織内での機能構築の促進**

業務のデジタル化に留まらない、社業そのもの（製品・サービス）のデジタル化の進展

ネットワークに接続された製品や、デジタルサービスを対象とした、設計・開発から運用・監視、対処に係る体制・機能（xSIRT）の必要性

**人材の流動性・マッチングの促進**

IT・セキュリティ人材の偏在※

業種やセクター、地域に限定されないデジタル化の広がりにより、リソース不足に直面

地域制約・時間制約にとらわれない、リモートワークや副業・兼業等の形態の活用可能性

**（A）新たなプラクティスの普及に向けた取組**

**a. 先進事例の収集・NISCポータルサイトでの発信**

→ 今後、年度内を目途に、新たなプラクティスを促進する材料となるよう、事例集として整備し、ポータルサイトで公表。（なお、企業名不開示を希望する場合は柔軟に対応。）

b. 手引き資料等の活用促進（必要に応じ改訂）

**（B）人材のマッチング促進**

a. 学び直しの機会の提供（教育訓練給付制度等）

b. 地域SECUNITYの形成促進等

# （参考）政府機関における人材の確保・育成

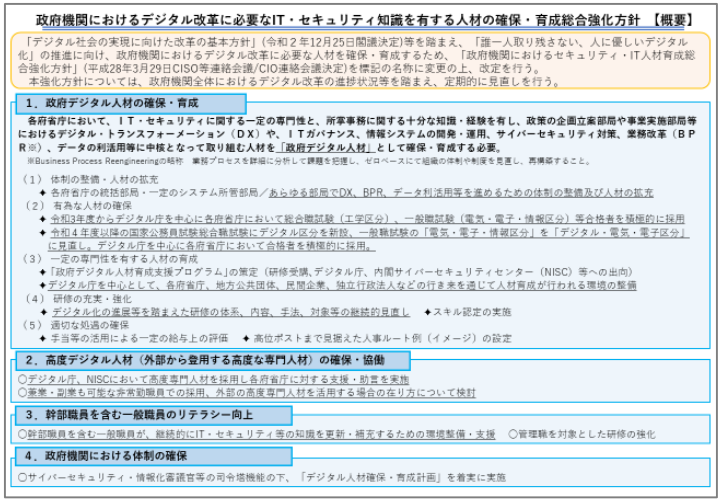
- 本年7月に策定した「政府機関における（中略）人材の確保・育成総合強化方針」に基づき、各府省庁において、政府部内での専門人材の育成や高度専門人材の確保に向けた取組を強化する。
- 特にNISCでは、人材の流動化促進や人材育成の観点から、専門職種ごとに必要な能力や資格等の整理（人材モデルの定義）等を進めており、各府省庁に提供するなど活用に向けた検討を進める。

## 「政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保・育成総合強化方針」＜抜粋＞

（令和3年7月6日 サイバーセキュリティ対策推進会議(CISO等連絡会議)・各府省情報化統括責任者(CIO)連絡会議 決定）


政府機関におけるデジタル改革に必要な
ＩＴ・セキュリティ知識を有する
人材の確保・育成総合強化方針

令和３年７月６日
サイバーセキュリティ対策推進会議（ＣＩＳＯ等連絡会議）
各府省情報化統括責任者（ＣＩＯ）連絡会議


政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保・育成総合強化方針 【概要】

「デジタル社会の実現に向けた改革の基本方針」（令和２年12月25日閣議決定）等を踏まえ、「誰一人取り残さない、人に優しいデジタル化」の推進に向け、政府機関におけるデジタル改革に必要な人材を確保・育成するため、「政府機関におけるセキュリティ・IT人材育成総合強化方針」（平成28年3月29日CISO等連絡会議/CIO連絡会議決定）を標記の名称に変更の上、改定を行う。
本強化方針については、政府機関全体におけるデジタル改革の進捗状況等を踏まえ、定期的に見直しを行う。

1．政府デジタル人材の確保・育成

各府省庁において、ＩＴ・セキュリティに関する一定の専門性と、所掌事務に関する十分な知識・経験を有し、政策の企画立案部局や事業実施部局等におけるデジタル・トランスフォーメーション（ＤＸ）や、ＩＴガバナンス、情報システムの開発・運用、サイバーセキュリティ対策、業務改革（ＢＰＲ※）、データの利活用等に中核となって取り組む人材を「政府デジタル人材」として確保・育成する必要がある。
※Business Process Reengineeringの略称　業務プロセスを詳細に分析して課題を抽出し、ゼロベースにて組織の体制や制度を見直し、再構築すること。

（１）体制の整備・人材の拡充
- 各府省庁の統括部局・一定のシステム所管部局／あらゆる部局でDX、BPR、データ利活用等を進めるための体制の整備及び人材の拡充

（２）有為な人材の確保
- 令和3年度からデジタル庁を中心に各府省庁において総合職試験（工学区分）、一般職試験（電気・電子・情報区分）等合格者を積極的に採用
- 令和４年度以降の国家公務員試験総合職試験にデジタル区分を新設、一般職試験の「電気・電子・情報区分」を「デジタル・電気・電子区分」に見直し。デジタル庁を中心に各府省庁において合格者を積極的に採用。

（３）一定の専門性を有する人材の育成
- 「政府デジタル人材育成支援プログラム」の策定（研修受講、デジタル庁、内閣サイバーセキュリティセンター（NISC）等への出向）
- デジタル庁を中心として、各府省庁、地方公共団体、民間企業、独立行政法人などの行き来を通じて人材育成が行われる環境の醸成

（４）研修の充実・強化
- デジタル化の進展等を踏まえた研修の体系、内容、手法、対象等の継続的見直し　✦スキル認定の実施

（５）適切な処遇の確保
- 手当等の活用による一定の給与上の評価　✦高位ポストまで見据えた人事ルート例（イメージ）の設定

2．高度デジタル人材（外部から登用する高度な専門人材）の確保・協働

○デジタル庁、NISCにおいて高度専門人材を採用し各府省庁に対する支援・助言を実施
○兼業・副業も可能な非常勤職員での採用、外部の高度専門人材を活用する場合の在り方について検討

3．幹部職員を含む一般職員のリテラシー向上

○幹部職員を含む一般職員が、継続的にIT・セキュリティ等の知識を更新・補充するための環境整備・支援　○管理職を対象とした研修の強化

4．政府機関における体制の確保

○サイバーセキュリティ・情報化審議官等の司令塔機能の下、「デジタル人材確保・育成計画」を着実に実施

### １．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、ＩＴ・セキュリティに関する一定の専門性と、所掌事務に関する十分な知識・経験を有し、政策の企画立案部局や事業実施部局等におけるデジタル・トランスフォーメーション（ＤＸ）や、ＩＴガバナンス、情報システムの開発・運用、サイバーセキュリティ対策、業務改革（ＢＰＲ）、データの利活用等に中核となって取り組む人材を「政府デジタル人材」として確保・育成する必要がある。

（３） 一定の専門性を有する人材の育成

デジタル庁を中心として、各府省庁、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。

人材の流動化促進や人材育成のための取組として、内部監査やＣＳＩＲＴ等の専門職種ごとに必要な能力や資格等について整理した結果を各府省庁へ提供するなど、活用に向けた検討を進める。

### ２．高度デジタル人材（外部から登用する高度な専門人材）の確保・協働

セキュリティについては、ＮＩＳＣにおいて、民間の特に高度な専門人材を特定任期付職員等の制度を活用して採用し、監査を通じ各府省庁のサイバーセキュリティ対策を支援する。また、企画・立案段階からのセキュリティ確保のため、政府情報システムについて、必要に応じてセキュリティに関する助言を行う。外部の高度専門人材の有する知識・経験を政府機関において活用するため、利害関係や職務遂行への支障に配慮の上、兼業・副業も可能な非常勤職員での採用についても検討する。また、採用に当たり、ＩＴスキルに関する民間の評価基準を活用する等の工夫等といった外部の高度専門人材を活用する場合の在り方についても検討を進める。

# （参考）製品・サービスの開発・監視・対処体制（xSIRT）に係るヒアリング結果概要

**9事業者：**電気機器、通信、IT、小売、自動車部品、デジタルサービス、クラウド 等　（中小企業含む）

## 機能構築の経緯

**＜きっかけ＞**
- 概ね①自社でのインシデント発生、②自社の新しいデジタルサービスの供用開始、③脅威動向を踏まえた対応に類別。（自動車部品では規制対応も）
- 一部では、設立にあたり経営層のリーダーシップが発揮された事例も。（全社部門への位置づけ等）

**＜参考事例＞**
- 2017年以前は各社手探りでの対応か、外部コンサルの支援の下で設立。
- 2018年以降、FIRST「PSIRT Service Framework」※が参照されている例もみられるが、初見ではハードルが高く、背景知識が必要との声も。（自動車部品では米国AUTO-ISAC「Best Practice Guides」を参考にされるなど、業界ごとの動きもあり。）

※ FIRST(Forum of Incident Response and Security Teams) が発行する支援ガイド(2018年7月にver.1.0発行)。2019年11月にJPCERT/CC・Software ISACが共同して日本語版を作成。

## 組織上の位置づけ

**＜組織名称＞**
- SIRTという名称を掲げていないケース、デジタルサービスを対象としてもPSIRTと呼称するケース、PSIRTとDSIRTが並列するケースなど様々。

**＜組織階層＞**
- 各事業部門・製品部門ごとに設置されるケースと、全社部門に設置されるケースとに類別。
- 前者では、特に製造系でそうした部門の特徴や権限が色濃く、それらの品質管理部署が兼務し、事業所階層でも設置されている場合が多い。

**＜所掌事務＞**
- 脆弱性対処に特化しているケースと、企画・開発プロセスへの関与も含まれるケースに類別。また、こうした機能を複数の部署で分担するケースも。

※ FIRSTのFrameworkでは、脆弱性対処を中心に、Discovery / Triage / Remediation / Disclosureのプロセス別に事務を記述。

## 開発プロセスへの関与（特筆すべき事例）

○SSIRTが決済サービスのリスクマネジメントを行う一環として、銀行決済の仕組みに踏み込んでリスク評価を行うこともあり得る。[通信]

○グループ会社の新規サービスをすべてHDで集約してレビューしている。[小売]

○アジャイル開発の場合、開発側に過度な負担がかからないよう、段階的に対応を依頼し、最終段階ですべてが対応されるよう管理している。[デジタルサービス]

○スプリントごとにレビューを行い、指摘は次のスプリントで修正する。[クラウド]

※ FIRSTのFrameworkでは、Stakeholder Managementの一部としてセキュア開発ライフサイクル(SDL)への参加を位置づけも、具体の方法論に関する記述はない。

## 脆弱性対処（特筆すべき事例）

○Discovery：脆弱性発見者に報酬を支払うバグバウンティ制度を実施。また、年に1回外部へテストを依頼して脆弱性の発見に努めている。[クラウド]

○Triage：Excelの台帳管理を廃止し、ソフトウェア構成（Software Bill of Materials：SBOM)をシステム上で管理し、自動収集した脆弱性情報とマッチング。[電機]

○Remediation：製品によってサプライチェーンの中での位置づけが異なるため、各事業部門ごとの各サプライヤーの担当者との繋がりを重視。[自動車部品]

○Disclosure：外部テストでみつかった脆弱性は、経営層や営業サイドが懸念を持つことがあるが、漏れなく情報公開を行っている。[クラウド]

## 人材確保等

**＜求める要素＞**・自社サービス仕様への理解、サービス間の相関の整理能力、脅威情報の収集能力、社内外との調整能力など様々。スキルセットの整理が必要との声も。

**＜中小の課題＞**・中小企業では追加人員確保が難しいため負荷の軽減が重要。パッケージサービス導入や取引先からの確認フォーマットの普及を進めてほしいとの声も。

※ FIRSTのFrameworkでは、PSIRTに必要なトレーニングとして、脆弱性対処を念頭に技術・コミュニケーション・プロセス・タスクツールと整理。具体スキルの記述はなし。

# （参考）副業・兼業の活用等に係るヒアリング結果概要

**5組織 / 6名：**自治体DX、教育委員会、教育機関、デジタルサービス（副業元：製造業、監査法人、セキュリティベンダ、省庁）

**副業・兼業の形態**　※ケースによって大きく幅があることに留意

＜契約形態＞ ・謝金支払い（役職の委嘱等を行うケースとそうでないケースと両方）、個人との委託契約に類別。（雇用契約は今回のヒアリングではなし。）
・副業元でも副業・兼業が容認されており、柔軟に勤務時間を設定できる契約形態となっているケースが多かった。一方で、副業・兼業の開始を機に契約を見直したケースも。

＜業務割当＞ ・上記で謝金支払いの場合はアドバイザー的な業務となる傾向がある一方、委託契約の場合はプロジェクト推進を任されているケースも。

＜勤務形態＞ ・今回のヒアリングではいずれも週1回勤務。勤務日・時間を固定するケースと柔軟に設定するケースといずれもあり。

＜情報管理＞ ・誓約書の提出、機密資料はweb会議の投影のみ、副業・兼業者には社内システムにアクセスできる範囲を制限する、など。

| | 利点 | 課題 |
|---|---|---|
| ＜副業・兼業先の企業・組織＞ | ○通常では採用できない第一線で活躍する人材を採用できた。<br>→副業・兼業者の知見を社内に蓄積するなど、組織内の人員（教育機関であれば生徒）にとって大きな刺激となった。<br>○地方でも、全国から人材の募集があった。<br>○柔軟な対応が可能なため、女性や転勤を嫌がる人の志望者が増えた。 | ○個人情報やセキュリティの根幹に関わるような内容については副業・兼業者のアクセス可能範囲を慎重に検討しなければならない。<br>○[公的機関のケース]癒着と捉えられかねないため、安全を期して、副業・兼業人材が入札業務に携わらないという線引きをした。ただ、これにより副業・兼業人材に依頼できる業務も限られる場合がある。 |
| ＜副業・兼業元の企業・組織＞ | ○副業先の方が取組が先進的な場合、その経験が還元された。<br>○[本業業務と直接関連、取引関係はないケース]利益相反に注意する必要があるが、両面の業務を知れたため直接的なシナジーがあった。<br>○採用イベント等で自らの副業・兼業について話すと学生からの関心が高く、優秀な人材の採用にも繋がると考えられる。 | ○現在採用している雇用契約の形態や職種によって対応できない場合があるため、現在の先行事例がそのまま横展開できるとは限らない。<br>○自分が初めての副業・兼業ケースのため、他職員への影響から、副業・兼業を認めていることを積極的に公表したがらなかった。 |
| ＜副業・兼業人材＞ | ○現在の職務を継続しつつ、実践的なスキルアップができる。<br>○転職となると、サラリーの変化や居住環境を変えたりなどハードルが高かったため、副業・兼業は中間的な手段として有用だった。 | ○副業・兼業業務の準備のため、割り当てられた時間に収まりきらないことがままあり、工夫が必要。<br>○テレワーク勤務が中心であることもあり、大人数の会議などで他部署との接点を作ることが難しく、工夫が必要。 |

**セキュリティ関係業務との親和性**

○時間の融通が利きやすく、幅広い知見や経験、人脈がモノをいう多くの業務は、副業・兼業によりむしろ本業へのフィードバックも考えられ、なじみやすい。
○機密性が高い業務は、業務内容そのものを外部に話せないため、業務の独自性が強く応用が利きづらく、また本業の企業・組織の理解を得づらい傾向がある。
○常時対応が必要なSOC等の監視・検知・対応業務は副業・兼業に適さないと考えられる。
○インシデントハンドリング業務でも、本業の企業・組織が柔軟な勤務形態であれば、十分に両立可能である。

# サイバー被害対応事例集の作成

- 昨今のランサムウェア被害をはじめ、当事者からサイバー攻撃被害の実情が公表されないことが多く、サイバー攻撃を受けた際の経験が共有され難い状況。他方で、一部の企業からは積極的に知見の共有を図りたいとの意見も寄せられているところ、事例集の作成を検討してきた。【6/2 前回調査会にて報告のとおり】
- 現在、サイバー攻撃を受けた様々な企業・組織に対してヒアリングを実施中。個社が特定されないよう情報の匿名化を行った上で、年度末を目途に事例集を作成・公表する予定。

**<u>また、ヒアリングにご協力いただける企業・組織が周辺にいれば、ぜひお話を伺わせていただきたい。</u>**

**＜主なヒアリング項目＞**

・事例の背景

・サイバー攻撃の検知までの経緯

・サイバー攻撃への具体的な対応（対応に当たった当該組織の各部門の役割分担を含む）

・サイバー攻撃に至った原因

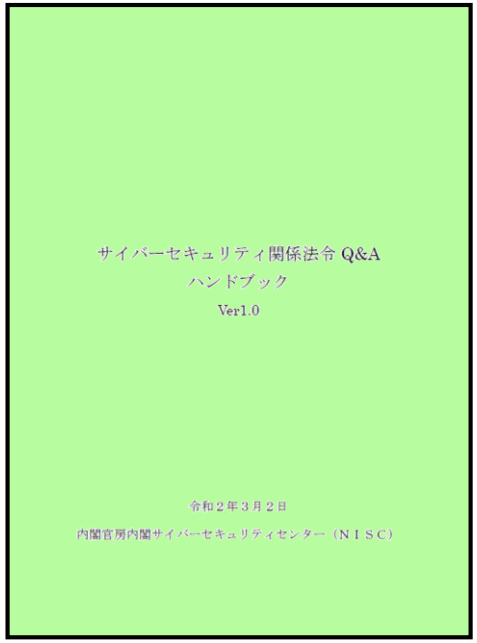
・再発に備えた対策

・得られた気付き・教訓

※ 以上について、技術的側面のみならず、サイバー攻撃を受けての事業判断や体制構築、人材確保等の組織マネジメント面での示唆を含む。

# 「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

- 「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。
- 間もなく策定から2年が経過することから、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来年中の改訂を検討しており、策定に向けたサブワーキンググループを設置したい。【詳細は資料3】




**＜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）

**＜想定される主な考慮要素の例＞**

- サイバーセキュリティ戦略（2021年）
- デジタル社会形成基本法（2021年）
- 個人情報保護法改正（2020年、2021年）
- テレワーク関係
- 電子契約関係
- NIS指令、NIS2指令等の海外法令

**＋活用シーンを想定した読みやすさ等の工夫**

# サイバーセキュリティ・ポータルサイトの活用促進

- サイバーセキュリティに係る関係機関の取組の一元化を目的として、2020年7月より試行運用し、2021年9月より本格運用を開始。【9月は月間約1万PV】
- 今後、民間事業者による人材育成プログラムを含め、定期的に取組をアップデート（本年は12月1日より募集開始）するとともに、時宜に応じて、政策推進に資するコンテンツ（ランサムウェアに対する注意喚起等）を特集化。


施策の目的や、自身の年齢層・所属から検索し、探したい施策にたどり着きやすいインターフェースを設定


**ランサムウェア特設ページ(STOP! RANSOMWARE)**
関係機関における取組を一覧化。

# 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）

### 講習会(全国展開型)

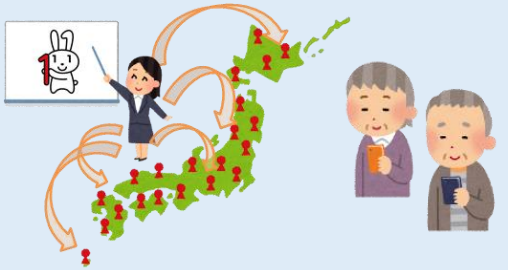
講習会等を行う拠点を全国に有しており、当該拠点で支援を実施する主体（携帯キャリア・携帯ショップを想定）

## 地域に根差した支援（地方）

### 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、シルバー人材センター等）

### 令和4年度 デジタル活用支援員派遣



地域の担い手となる、高度なスキルを有する「デジタル活用支援員」を育成し、津々浦々に支援員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）<br>※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 | |

# サイバーセキュリティ分野における多様な人材の活躍に向けて

- 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育成・活躍促進が急務。
- そのためには、(1)採用需要の喚起、(2)潜在層へのアプローチ、(3)活躍の場の拡大を一体的に進める必要。「サイバーセキュリティ戦略」を踏まえ、今後、官民で取組を具体化していく。

## (1) 採用需要の喚起

○政府機関におけるサイバーセキュリティ人材確保強化
例）デジタル庁、自衛隊・警察等における専門人材確保

○情報処理安全確保支援士等の資格制度の活用
例）「デジタルガバナンス・コード」で会社での取得奨励を「望ましい取組」として位置づけ

## (2) 潜在層（女性、ニート・引きこもり等）へのアプローチ

○多様な人材の活躍事例の発信

○若年層向け人材育成プログラムの門戸開放
例）SecHack365（学生・社会人以外も対象）

○職業訓練制度との連携
例）サイバーセキュリティに関する内容を含む職業訓練の拡充

**一体的推進**

## (3) 活躍の場の拡大

○製品・サービスの信頼性確保に向けた検証ビジネスの発展
例） 検証事業者の信頼性可視化に向けた検討