National center of Incident readiness and Strategy for Cybersecurity

資料4

「サイバーセキュリティ人材育成総合強化方針（仮称）」に向けた検討事項について

2015年12月14日

内閣サイバーセキュリティセンター（NISC）

http://www.nisc.go.jp/

「サイバーセキュリティ人材育成総合強化方針（仮称）」について

【目的】

日本年金機構における情報流出事案をはじめ、サイバーセキュリティの問題は甚大化・深刻化している。一方、サイバーセキュリティに係る専門人材の質的量的不足、経営層の意識改革は十分とは言えない状況。

こうした中、「新・情報セキュリティ人材育成プログラム」（平成２６年５月情報セキュリティ政策会議決定）や「サイバーセキュリティ戦略」（平成２７年９月閣議決定）の考えを踏まえつつ、喫緊の課題に対し、特に重点的に進めるべき施策を総合的かつ強力に推進することで、サイバーセキュリティ人材の育成を加速化する。

【検討のスケジュール】

○「日本再興戦略」改訂2015（平成２７年６月閣議決定）では「サイバーセキュリティ人材育成総合強化方針（仮称）」を本年度中に策定と記載。

○「普及啓発・人材育成専門調査会」を２回開催し、平成２７年度中に専門調査会として決定し、その後のサイバーセキュリティ戦略本部に報告、としたスケジュールを想定。

「サイバーセキュリティ人材育成総合強化方針（仮称）」に関する政府決定文書

○「日本再興戦略」改訂2015（平成27年6月閣議決定）の記載

4．世界最高水準のIT社会の実現

イ） 人材育成

顕在化・深刻化しているセキュリティリスクや、急速な技術革新とともに高度化するサイバー攻撃への対策を確かなものとするためには、それを支える人材の育成が急務である。このため、初等中等教育段階からのプログラミングや情報モラルに関する教育を充実させる。また、高等教育機関において、大学等における実践教育ネットワークの構築に向けた取組、国立高等専門学校におけるセキュリティ教育プログラムの開発を推進するとともに、産業界と連携した実践的なセキュリティ教育の普及等を図る。（中略）2020年東京オリンピック・パラリンピック競技大会の開催も見据え、高度な実践的人材の育成を強化する。このため、産学官の協力体制構築に向け、緊密な連携や情報共有の促進に加え、実践的なサイバー演習環境をクラウド環境で整備する。（中略）これらを含め、人材育成に係る施策を総合的に推進するため、本年度中に「サイバーセキュリティ人材育成総合強化方針（仮称）」を策定する。

○サイバーセキュリティ戦略（平成27年9月閣議決定）の記載

5．4．2 人材の育成・確保

情報通信技術が広く国民全体に拡大・浸透し、社会の基盤となっており、連接融合情報社会においては、サイバーセキュリティは、同分野の専門家はもちろん、一般的な情報通信技術者、ひいてはIoTシステムの利用者に至るまで、程度に差はあるものの様々な層の人材に必須の素養である。しかし、例えば、国内でサイバーセキュリティに関する業務に従事する技術者は現在、質的にも量的にも圧倒的に不足している という現実に鑑みても、人材育成は喫緊の課題である。そこで、以下のとおり、サイバーセキュリティや関係する分野に係る教育の充実、突出した能力を有する人材の発掘・育成・確保、人材が将来にわたって活躍し続けるための環境整備等に取り組む。また、これらを含め、人材育成に係る施策を総合的かつ強力に推進するための方針を策定する。

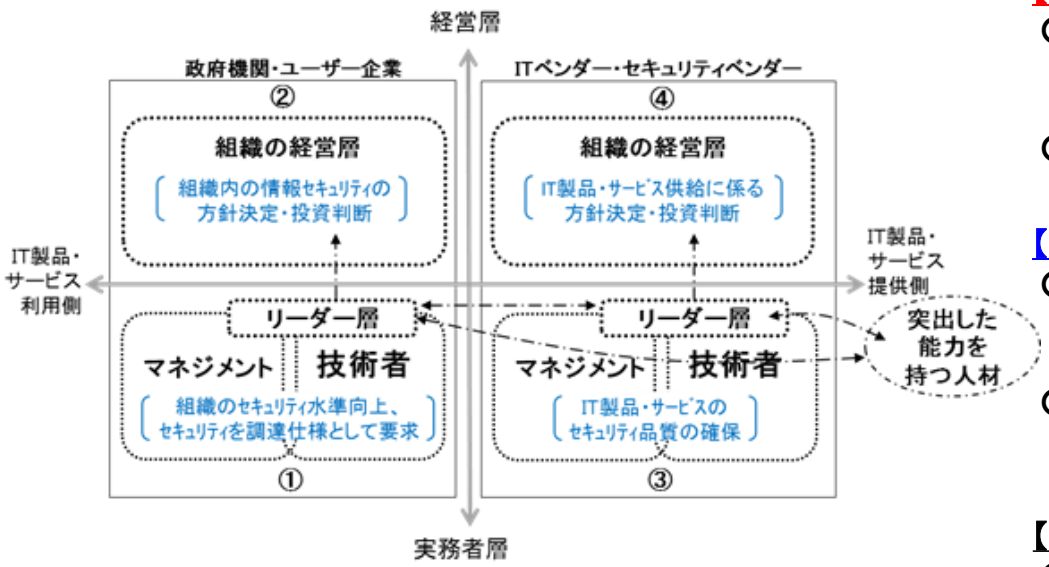
○サイバーセキュリティ2015（平成27年9月サイバーセキュリティ戦略本部決定）の記載

4．2 人材の育成・確保

（イ）内閣官房において、人材育成に係る施策を総合的に推進するため、「サイバーセキュリティ人材育成総合強化方針（仮称）」を策定する。

新・人材育成プログラムを踏まえ各種取組①

新・情報セキュリティ人材育成プログラムにおいては、IT製品・サービスの提供側・利用側、経営層、実務者層の４象限に分け、それぞれの領域において、情報セキュリティに関して求められる項目を示した上で、人材の供給（育成・発掘）だけでなくその需要（雇用等）にも施策を講じて「人材の好循環」を形成することを目標としたところ。



施策の対象分類

「新・情報セキュリティ人材育成プログラム」より抜粋

【人材の供給】

- 政府機関・ユーザー企業等が、「利用側の実務者層」（①）に、どのような対策が必要かを判断し実行する能力を身につけさせることが必要。
- 「提供側の実務者層」（③）は、利用側の顕在的・潜在的要求に応えるレベルの能力を身につけることが必要。

【人材の需要】

- 「利用側の経営層」（②）は、情報セキュリティを自組織の経営戦略として認識し、①を適切な処遇で登用することが必要。
- 「提供側の経営層」（④）は、必要なサービス・製品の開発・供給の戦略に基づき、③を適切な処遇で登用することが必要。

【各場面を行き来して活躍する牽引役】

- 牽引役として突出した能力を持つ人材が、実務者層のリーダー層、経営層と実務者層との間のコミュニケーション役、提供側と利用側の橋渡し役などとして、各場面を行き来して活躍することが必要。

新・人材育成プログラムを踏まえた各種取組②

新・人材育成プログラムを踏まえ、以下のような各種施策を推進

（1）経営層の意識改革
・経済団体等の場を活用して、企業等の経営層に対し、経営戦略の一部としてのサイバーセキュリティ対策について意識啓発を実施。（内閣官房）
・企業経営者を対象にしたサイバーセキュリティ経営ガイドラインの策定。（経済産業省）

（2）必須能力としての情報セキュリティ
・官公庁や企業等組織における実践的サイバー防御演習（CYDER）の基盤の強化及び拡充。（総務省）
・複数の大学や産学の連携によるサイバーセキュリティに係る実践的な演習を推進する体制の構築。（文部科学省）
・サイバーセキュリティに従事する者の実践的な能力を適時適切に評価するための資格登録・更新制度の検討。（経済産業省）

（3）高度な専門性及び突出した能力を有する人材の発掘・育成、グローバル水準の人材の育成
・若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材の創出を目的とした「セキュリティ・キャンプ」の実施。（経済産業省）
・攻撃・防御両者の視点を含むセキュリティの総合力を試すセキュリティコンテストの支援。（経済産業省）

（4）政府機関等における人材育成
・政府機関におけるサイバー攻撃に係る対処要員の能力及び連携の強化を図るための訓練・演習を実施。（内閣官房）
・政府職員のインシデント・ハンドリング能力等を向上させていくため、総務省事業（CYDER）を活用し、2014年度にサイバー攻撃対処能力を競うNATIONAL 318(CYBER) EKIDENを実施。（内閣官房及び総務省）

（5）教育機関における情報通信技術教育の充実等
・学習指導要領を踏まえながら、児童生徒の発達段階に応じた情報活用の実践力、情報の科学的な理解、情報社会に参画する態度を培う教育を一層推進。（文部科学省）
・高等専門学校におけるセキュリティ教育の強化のための施策として、企業等のニーズを踏まえた技術者のセキュリティ教育に必要な教材・教育プログラム開発。（文部科学省）

今後重点的に取り組んでいく主な施策

これまでのサイバーセキュリティ人材育成の取組を加速化するために平成２８年度においては以下に掲げる施策を推進していってはどうか。

1. 「費用」から「投資」への経営層の意識改革

2. 政府機関及び企業等で必要なセキュリティ人材の育成・確保

3. 突出した能力を有した人材の発掘・育成・確保

4. 情報セキュリティ関係の政府専門家の育成体制の構築

1.「費用」から「投資」への経営層の意識改革

政府における議論

◆*サイバーセキュリティ戦略（平成27年9月4日閣議決定）*

５．１．２　セキュリティマインドを持った企業経営の推進

（１）経営層の意識改革

（前略）サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成のための官民が一体となった啓発活動を実施する。（後略）

（２）経営能力を高めるサイバーセキュリティ人材の育成

（前略）経営層の示す経営方針を理解し、サイバーセキュリティに係るビジョンの提示や、実務者層との間のコミュニケーションの支援を行う橋渡し人材層の育成を推進する。（後略）

５．４．２　人材の育成・確保

（４）人材が将来にわたって活躍し続けるための環境整備

（前略）サイバーセキュリティに従事する者の実践的な能力を適時適切に評価できる資格制度の創設や組織において業務に必要となる標準的なスキルの基準の整備により能力の可視化を図る。（後略）

取組概要

サイバーセキュリティの確保はもとより、新たなビジネスの創出等のためにも、セキュリティリスクの把握や経営資源に係る投資判断を適切に行い、製品・サービスへのセキュリティ機能の実装の推進、セキュリティ人材の育成、組織能力の向上等を図ることは重要。そのため、サイバーセキュリティに関する取組を、市場や出資者といったステークホルダーから正当に評価して頂くためのガイドラインを策定。また、技術革新が著しいため、最新の知識・技能を継続して保持することを評価する手法として、資格制度を活用し、能力を可視化。

具体的な施策例

✓　サイバーセキュリティ経営ガイドラインの策定【経済産業省】
✓　サイバーセキュリティを担う人材の資格登録・更新制度導入【経済産業省】

2. 政府機関及び企業等で必要なセキュリティ人材の育成・確保（参考2）

政府における議論

◆*サイバーセキュリティ戦略（平成27年9月4日閣議決定）*

５．４．２　人材の育成・確保

（１）高等教育段階や職業能力開発における社会ニーズに合った人材の育成

今後社会で活躍できる高度な専門人材については、産学官がより一層有機的に連携し社会のニーズに合った人材を量・質の両面から効果的に育成していくことが必要である。大学院、大学、高等専門学校等の高等教育機関においては、サイバーセキュリティに係る理論・基礎の習得と演習を通じた実践力の強化に向けた取組を推進する。（後略）

（５）組織力を高めるための人材育成

組織全体としての能力を効果的・効率的に向上させていくためには、異なる組織同士で切磋琢磨する環境を整備するとともに、個々の組織についてその実践的な能力や課題について具体的に把握できるようにしていくことが重要となる。このため、組織のサイバー攻撃対処に必要な能力を体系化するとともに、それらの能力を向上させるための実践的演習の取組を充実させる。（後略）

取組概要

あらゆるモノがネットワークに接続され始めている中、サイバーセキュリティに関する知識は、専門家のみならず、様々な層の人材に必要。そのため、高等教育、さらには企業において、サイバーセキュリティに係る人材を育成。また、大規模なサイバー攻撃等への対処能力の向上を図るため、ログ分析等の技術的な対応やチーム単位での迅速なインシデント対応を習得できるような実践的サイバー防御演習に係る体制を強化。なお、日本年金機構の事案やマイナンバーの導入を踏まえ、演習の対象を独立行政法人、特殊法人及び地方公共団体等へ拡大。

具体的な施策例

- ✓ SIP（戦略的イノベーション創造プログラム）の枠組みにおける重要インフラ等におけるサイバーセキュリティ人材育成【内閣府】
- ✓ 実践的サイバー防御演習（CYDER）の実施【総務省】
- ✓ 数千人規模の仮想ネットワーク環境を実現できる大規模設備やネットワークセキュリティに関する幅広い知見を有する国立研究開発法人情報通信研究機構（NICT）が、それらを活用して継続的・安定的に実践的サイバー防御演習を実施できるよう措置【総務省】
- ✓ enPiT（情報技術人材育成のための実践教育ネットワーク形成事業）の枠組み等を活用した、複数の大学間や産学の連携によるサイバーセキュリティに係る実践的な演習の推進【文部科学省】

3. 突出した能力を有した人材の発掘・育成・確保

（参考3）

政府における議論

◆*サイバーセキュリティ戦略（平成27年9月4日閣議決定）*
５．４．２　人材の育成・確保
（３）突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保
　突出した能力を有する人材の発掘・確保も引き続き行っていく。（中略）サイバーセキュリティがグローバルな課題となっていることに鑑みれば、こうした突出した能力を有する人材はグローバル水準の能力を備える必要がある。つまり、国境を意識することなく十分に活躍できる人材の育成が不可欠である。（後略）

取組概要

　突出した能力を持つ人材は、通常の教育では育成が難しい。このような人材に対しての取組は、その能力に着目した発掘や、国内外の優秀な技術者等と切磋琢磨して能力の開花に結び付く場を設けることが重要である。このため、例えばサイバー攻撃に対する対処法（防御手法、攻撃手法も含む。）の研究を通じ、自ら考え、対策を検討できる能力の育成を推進するとともに、海外からの参加者を集めた競技イベントの実施、人材間のネットワーク形成等の取組を充実させるなど、政府として積極的に措置を講ずる。

具体的な施策例

✓２０２０年東京オリンピック・パラリンピック競技大会を見据え、本大会関連システムの模擬も可能な大規模演習基盤を構築・運用し、より高度な専門性及び突出した能力を有するセキュリティ人材の育成に対する支援を実施【総務省】
✓学術情報ネットワーク（SINET）上のリアルなサイバー攻撃データを活用した、攻撃の状況を俯瞰・判断するシミュレーション演習等【文部科学省】
✓セキュリティキャンプ、未踏人材等の各種施策の実施【経済産業省】
✓セキュリティの競技イベントである「ＳＥＣＣＯＮ」やグローバルレベルのセキュリティの国際会議の実施【民間事業】

4. 情報セキュリティ関係の政府専門家の育成

（参考4）

NISC

政府における議論

◆*サイバーセキュリティ戦略（平成27年9月4日閣議決定）*

５．２．３　政府機関を守るための取組

（２）しなやかな組織的対応能力の強化

（前略）組織的対応の要は人であることから、幹部を含む職員全体のサイバーセキュリティに関する素養の向上を確実なものとするよう取り組む。また、資格等を個人の能力を客観的に示す指標の一つとして活用しつつ、各機関における対応能力強化のけん引役となるセキュリティ人材の育成・確保を図る。

６．推進体制

大規模なサイバー攻撃等の事象への対処に際し、政府機関、独立行政法人、セキュリティ事業者等が協力して対処する体制を確立するとともに、大規模なサイバー攻撃への対処や人材育成のための実践的な演習・訓練などの面において、産学官が緊密に協力し、一定の知見等を有する者と積極的な連携を図る。

（中略）政府において専門性にふさわしい処遇等により高度なセキュリティ人材を登用するなど、実行可能なものは直ちに実施するとともに、新たな制度の整備が必要と認められる場合については、遅滞なく所要の措置を講じる。

取組概要

政府機関等に対するサイバー攻撃の高度化・巧妙化やITに関する製品・サービスの多機能化・多様化を始めとした社会環境の変容が一層加速化されることが想定されるなど、政府機関等においては、既に顕在化している脅威や課題はもとより、未知の脅威等に直面した場合であっても柔軟かつ迅速に対応できるよう、体制の構築・整備・強化を図る。

具体的な施策例

- ✓ 幹部を含めた組織的対応体制の構築・整備・強化
- ✓ サイバー攻撃に係る事態の把握・対処機能の強化

など、政府内にて、具体的な体制を検討中。【内閣官房を中心に各府省庁】

新たな「サイバーセキュリティ戦略」について（全体構成）　【別添1】

1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会（連融情報社会）**」が到来、同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「**経済社会の活力の向上及び持続的発展**」、「**国民が安全で安心して暮らせる社会の実現**」、「**国際社会の平和・安定及び我が国の安全保障**」に寄与する。

3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

- **安全なIoTシステムの創出**
  安全なIoT活用による新産業創出
- **セキュリティマインドを持った企業経営の推進**
  経営層の意識改革、組織内体制の整備
- **セキュリティに係るビジネス環境の整備**
  ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

- **国民・社会を守るための取組**
  事業者の取組促進、普及啓発、サイバー犯罪対策
- **重要インフラを守るための取組**
  防護対象の継続的見直し、情報共有の活性化
- **政府機関を守るための取組**
  攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

- **我が国の安全の確保**
  警察・自衛隊等のサイバー対処能力強化
- **国際社会の平和・安定**
  国際的な「法の支配」確立、信頼醸成推進
- **世界各国との協力・連携**
  米国・ASEANを始めとする諸国との協力・連携

横断的施策

- **研究開発の推進**
  攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発
- **人材の育成・確保**
  ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

「サイバーセキュリティ戦略」のうち人材育成・確保に関する取組部分の概要抜粋

■セキュリティマインドを持った企業経営の推進

- 企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築(経営ガイドライン等の発信含む)
- 経営層と実務者層との間のコミュニケーション支援を行う橋渡し人材層の育成
- 民民間・官民間における脅威・インシデント情報の共有網の拡充

▲ 合宿形式で知識・技能を学ぶセキュリティキャンプ

■人材の育成・確保

- 他分野の知識も併せ持つハイブリッド型人材の育成促進
- 高等教育等における産学官連携の推進・実践的演習の充実
- 人材育成のための実践的な演習の取組を推進
- 初等中等教育段階からの教育の充実
  (論理的思考力やモノの基礎的動作原理の理解促進、教員の指導力向上に向けた研修等の改善・充実)
- サイバー演習環境のクラウド環境における整備、産学官共同による教材開発の支援
- 国際的競技イベント等を通じたグローバル水準の高度人材の発掘・確保
- 実践的能力を評価する資格制度の創設、標準的なスキルの基準の整備等の推進

▲ 58ヶ国が参加したセキュリティコンテスト
(2014年度)

▲ 実践的サイバー防御演習 (CYDER)
(2015年度)

「新・情報セキュリティ人材育成プログラム」の概要について　【別添3】

サイバーセキュリティ戦略（平成25年）で示された課題

情報セキュリティに係るリスクの深刻化に対応するためには、

○**人材の量的不足の解消**に向け 積極的な取組が必要であるとともに、教育だけでは得られない**突出した能力を有する人材の確保**も大きな課題。

○そのためには、**社会全体で育成し活用するための仕組み**が必要。

人材の量的・質的不足

情報セキュリティ従事者 約26.5万人

うち質的不足 約16万人

さらに量的不足 約8万人

⇒これら人材の雇用の受け皿も不可欠

IT人材106万人（SE80万人）　*IPA調べ

取組の方針

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成する。

【需要】経営層の意識改革

○**組織の経営層**

・経営層の意識改革を促し、情報セキュリティを経営戦略として認識させるための取組を推進。

・製品・サービス調達における情報セキュリティの要件化等を通じ、投資意欲を喚起して、人材の需要を創出。

○**実務者層のリーダー層**

・経営戦略の視点から情報セキュリティの課題や方向性を考え、経営層と実務者層の橋渡しができる能力を育成。

【供給】人材の「量的拡大」と「質的向上」

○**IT技術者等**に、情報セキュリティを必須能力として位置付け、訓練・演習教材等の作成や能力評価基準・資格のあり方の検討を進める。

○**高度な専門性及び突出した能力を有する人材**の発掘・育成を推進するとともに、実社会での活躍を促進。

○**グローバル水準の人材**の育成に向け、国際的な体験や情報共有を通じて人材が研鑽を積む環境を構築。

○**政府機関**は自ら率先して、情報セキュリティ上のリスクに対応できる職員の採用・育成や研修・訓練等を強化。

○**教育機関**（初等中等教育機関含む）の実践的なIT教育を充実させるとともに、情報セキュリティに関する教員養成を推進。