“DX with Cybersecurity”実践に向けた人材の確保、育成、活躍促進に係る主な政策課題と方向性

令和3年6月2日 普及啓発・人材育成専門調査会

「サイバーセキュリティに係る人材の確保、育成、活躍の促進に係る政策課題の当面の検討の進め方について」（令和2年7月31日 普及啓発・人材育成専門調査会会長）に基づき、3つの政策課題と対応する方策について検討を行ってきたところ、それらの方向性は以下の通り。

今後、この方向性を次期「サイバーセキュリティ戦略」に反映し、“DX with Cybersecurity”実践に向けた取組の推進を図るべきである。

政策課題1：サイバーセキュリティ確保のための新たな開発・監視・対処体制の構築

＜より重要となるプラクティスと人的資源・体制＞

①セキュリティ・バイ・デザイン、迅速・柔軟な開発・対処の必要性
→開発とセキュリティの一体化、部署間の協働

②製品のネット接続、デジタルサービス連携増加への対応
→組織をまたぐ連携・情報共有、より高度なリスク管理

＜実践・普及に向けた主な課題と推進方策＞

①新たな体制構築・プラクティス実践の先進事例が少ない。
→実践モデルやプラクティスの積極共有

②製品・サービスとセキュリティの両方への理解が必要。
→「プラス・セキュリティ」知識を補充できる環境整備

③経営層によるリーダーシップ発揮が不可欠。
→経営層の意識改革

人材・仕事の需要増加

双方が連関し好循環を形成

人材・仕事の供給増加

政策課題3：セキュリティ人材の活躍の促進に向けた流動性とマッチングの機会の促進

＜新たな流動モード＞

①コロナ禍を経た働き方・雇用環境の変化
→リモートワーク、副業・兼業といった柔軟な雇用形態の活用

②デジタル改革の推進（2021年9月 デジタル庁設置予定）
→政府・自治体で業務改革経験を積み、官民を行き来

＜実践・普及に向けた主な課題と推進方策＞

①新たな体制構築・プラクティス実践の先進事例が少ない。
→実践モデルやプラクティスの積極共有

②マッチングに向けて、人材の需要と供給双方の明確化が必要。
→スキルに関する共通言語化ツールの活用促進

③地域・中小企業におけるマッチングの促進
→新たな流動モードの促進、地域におけるコミュニティ形成を通じた人材のマッチング促進

政策課題2：DXに必要な「プラス・セキュリティ」知識を補充できる環境・人材育成の推進

※「プラス・セキュリティ」知識は、ITやセキュリティに関する専門知識や業務経験を必ずしも有していない人材が社内外のセキュリティ専門家と協働するにあたって必要な知識として、時宜に応じてプラスして習得すべき知識を指す。

＜プログラムの普及に向けた主な課題と推進方策＞

①潜在的に大きな需要が存在すると考えられる一方、顕在化していない。
→プログラムや研修等の受講を呼びかける取組を促す普及啓発、インセンティブ付け

②需要者からみて供給側の一定の質が確保・期待される仕組みが必要。
→先導的・基盤的なプログラム提供、趣旨に適うプログラムの積極的な発信

○経営層や事業を担う者が「プラス・セキュリティ」
→主体的に、的確な体制構築を図れる。

○開発運用や企画の人材が「プラス・セキュリティ」
→開発とセキュリティの一体化や、部署間の協働が促進される。

○経営層や事業を担う者が「プラス・セキュリティ」
→主体的に、専門家に期待する業務等を明確化し、的確なジョブディスクリプション等で採用することで、より円滑なマッチングが促進される。

政策進展の前提

経営者：サイバーセキュリティリスクに対する経営問題としての認識／対策に向けたリーダシップの発揮

添付資料

1月21日 第14回普及啓発・人材育成専門調査会資料（一部修正）

主な政策課題と検討論点

政策課題１　サイバーセキュリティ確保のための新たな開発・監視・対処体制の構築

１．１　xSIRTごとに特徴的な機能や体制等はあるか。これらの構築や普及に当たっての課題は何か。

１．２　DXに伴いデジタル・サービスが増加する際に重要となる開発・監視・対処のプラクティスとは何か。
その実現にあたっての人的資源・体制につき考慮すべきことは何か。

１．３　また、実践や普及をどのように政策的に後押ししていくか。

政策課題２　DXに必要な「プラス・セキュリティ」知識を補充できる環境・人材育成の推進

２．１　「プラス・セキュリティ」の考え方

２．２　ユーザ企業の主体的なIT 活用・DX 実施において経営・事業を担う者が「プラス・セキュリティ」
知識を補充できるよう、対象人材に応じてどのようなモデルカリキュラムが考えられるか。

２．３　カリキュラムの構築や普及をいかに政策的に後押ししていくか。

政策課題３　セキュリティ人材の活躍の促進に向けた流動性とマッチングの機会の促進

３．１　DX時代におけるIT・セキュリティ人材の流動イメージ（モード）は何か。

３．２　人材の流動性やそれぞれのモードに応じたマッチングの促進策は何か。
また、それをどのように政策的に後押ししていくか。

政策課題１

サイバーセキュリティ確保のための
新たな開発・監視・対処体制の構築

xSIRTごとの特徴的な機能

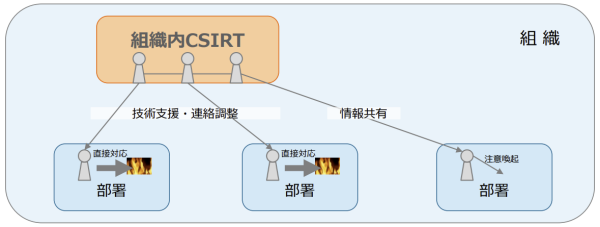
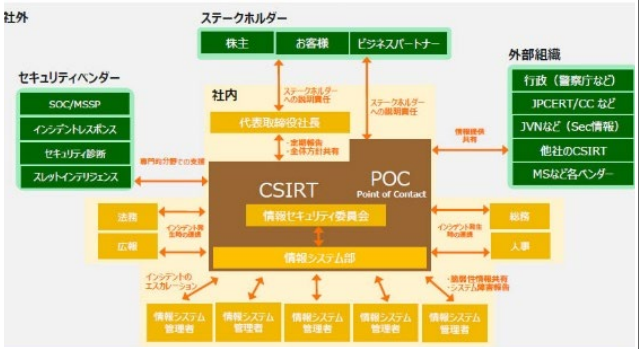
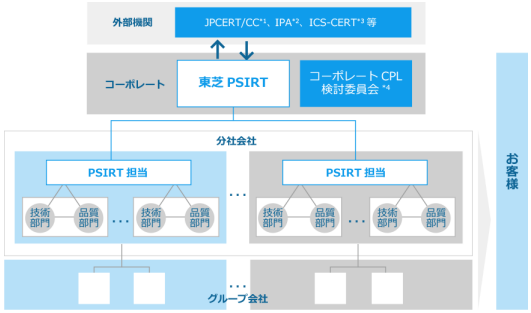
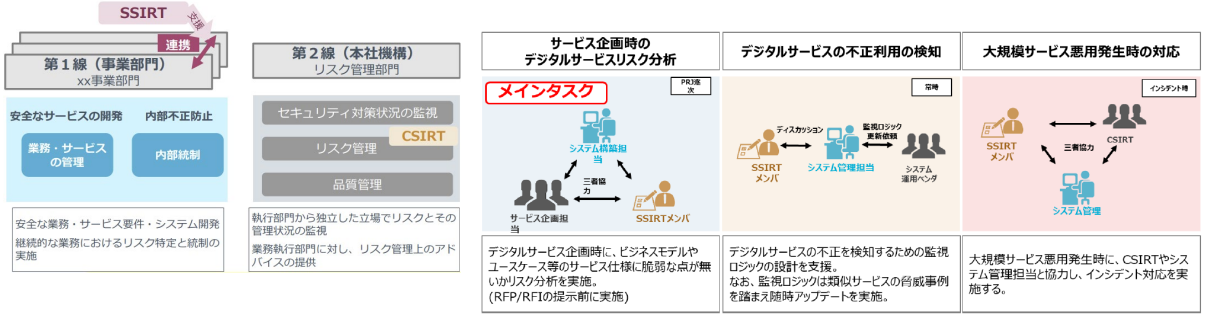
注：以下は各xSIRTと呼ばれるものの機能的な面を中心に整理を試みたものであり、企業・組織内にそれぞれ別個に体制として設ける必要性を示すものではない。体制の検討にあたっては、経済産業省の手引き[1]が示すように、近年、デジタル技術の活用の進展に伴い、全社的なリスクマネジメントが必要となってきている。

xSIRT	対象	主な活動	設置部署
CSIRT（組織内CSIRT） （Computer Security Incident Response Team）	組織内CSIRTは、組織内の業務運営に用いるコンピュータやネットワークといった情報システムの安定稼働とそこで取り扱われる情報保護を対象として、セキュリティ・インシデントに対処する。 ※全組織的なセキュリティ統括機能が設置される場合はその機能の1つとして上記を担う。	インシデントの検知や受付を経て、その原因分析や影響範囲の調査、問題への対応、復旧を行う。あるいは、そのための技術支援を関係部署に提供する。 経営層や関係部署との連絡調整や情報共有なども行う。 平常時には、パッチ適用などの脆弱性対応、従業員への普及啓発・注意喚起なども担う。	情報システム部門やIT部門と呼ばれる部署に設置されることが多い。 なお、なお、インシデントの検知や深堀分析をSOC（Security Operation Center）と呼ばれる専門組織が担い、CSIRTと連携する場合が多い。自組織CSIRTと外部の専門組織の役割分担は組織によって異なる。
PSIRT （Product Security Incident Response Team）	PSIRTは、顧客に販売されネットワークに接続された製品および顧客の安全確保・情報保護を対象として、セキュリティ・インシデントに対処する。 ここでいう製品にはハードウェア製品とソフトウェア製品がある。	インシデントの検知や受付を経て、CSIRTが設置されている場合はCSIRTと分担・連携しつつ、製品に係る原因分析や影響範囲の調査、問題への対応、復旧を行う。 更に、製品の顧客へのパッチ提供や対策支援等の脆弱性対応なども行う。 活動の際には、製品開発や品質管理を担う部署と協調することが求められる。	事業部門ごとに、製品開発や品質管理を担う部署と連携する部署として設置されることが多い。 その際、製品開発プロセスにおけるセキュリティ・バイ・デザインの管理を兼ねる場合もある。また、複数の事業部門がある場合は、全組織的に統括的なPSIRTが置かれる場合がある。
DSIRT/SSIRT （Digital Service Security Incident Response Team）	Service SIRTは、顧客が利用するデジタル・サービスの継続的提供・品質維持および顧客の資産保護・情報保護を対象として、セキュリティ・インシデントに対処する。	インシデントの検知や受付を経て、デジタル・サービスを提供する事業部門が原因分析や影響範囲の調査、問題への対応、復旧を行うが、Service SIRTは、各事業部門を横断的・俯瞰的に確認し、事業部門に対して実務的な助言・支援を行う。 主に、サービス企画時のサービスリスク分析、サービスの不正を検知する監視ロジックの設計・更新支援、大規模サービスインシデント発生時の対応が挙げられる。 全組織的なCSIRTがある場合は必要に応じ連携する。	デジタル・サービスを提供する事業部門と横並びの独立部署、もしくは、各事業部門のセキュリティ担当を集めたバーチャル組織として設置されることが多い。

※なお、製造業などにおいては自社の工場や生産ラインの安定稼働や作業員の安全確保の為に、サイバー攻撃の監視・対処を行うFSIRT(Factory Security Incident Response Team)と呼ばれる組織が生産管理部門に設置される場合もある。

※［1］、［3］、その他の資料を参照して事務局にて作成。

xSIRTごとの特徴的な体制

xSIRT	体制例	規模感
CSIRT（組織内CSIRT）	 （出典）組織内CSIRTの役割とその範囲、JPCERT/CC （2015年11月18日） https://www.jpcert.or.jp/csirt_material/files/02_role_of_csirt20151126.pdf  （出典）「CSIRT」の構築・運用のポイントとは？、マイナビニュース（2019年2月14日） https://news.mynavi.jp/article/20190214-770901/	• 大きな組織では、数名から十数名の人員を配置することが多くみられる。一方、ユーザ企業では組織によっては他の業務と兼務となる場合が多くみられる。 ・各部署にセキュリティ対応力が備わっている場合、問題に直接対応する必要がないため、組織内CSIRTの規模は小さくなる。
PSIRT	 *1:Japan Computer Emergency Response Team / Coordination Center *2:Information-technology Promotion Agency Japan *3:Industrial Control Systems Cyber Emergency Response Team *4:CPL:CL（契約に基づく品質保証責任）とPL（製造物責任）を合わせた略称 （出典）東芝 PSIRT、株式会社 東芝（2020年11月30日確認） https://www.toshiba.co.jp/security/psirt	• 事業部門毎にPSIRTが設置され、それぞれに数名の人員を配置することがみられるが、組織によっては他の業務と兼務となる場合もある。 • 全組織的に統括的なPSIRTでは、事業部門とは別途、数名程度配置することがみられる。
DSIRT/SSIRT	 （出典）普及啓発・人材育成専門調査会 第13回会合「資料3 DXサービスに必要なセキュリティ対策（ＮＲＩセキュアテクノロジーズ株式会社 説明資料）」（2020年7月31日）	• 一部の先進的な取組を行う企業で設置がみられる。 • 顧客に提供するデジタル・サービスが複数でも類似する場合には、人員の増加は少ないと考えられる。

※ [1]、[3]、その他の資料を参照して事務局にて作成。

機能構築や普及にあたっての課題

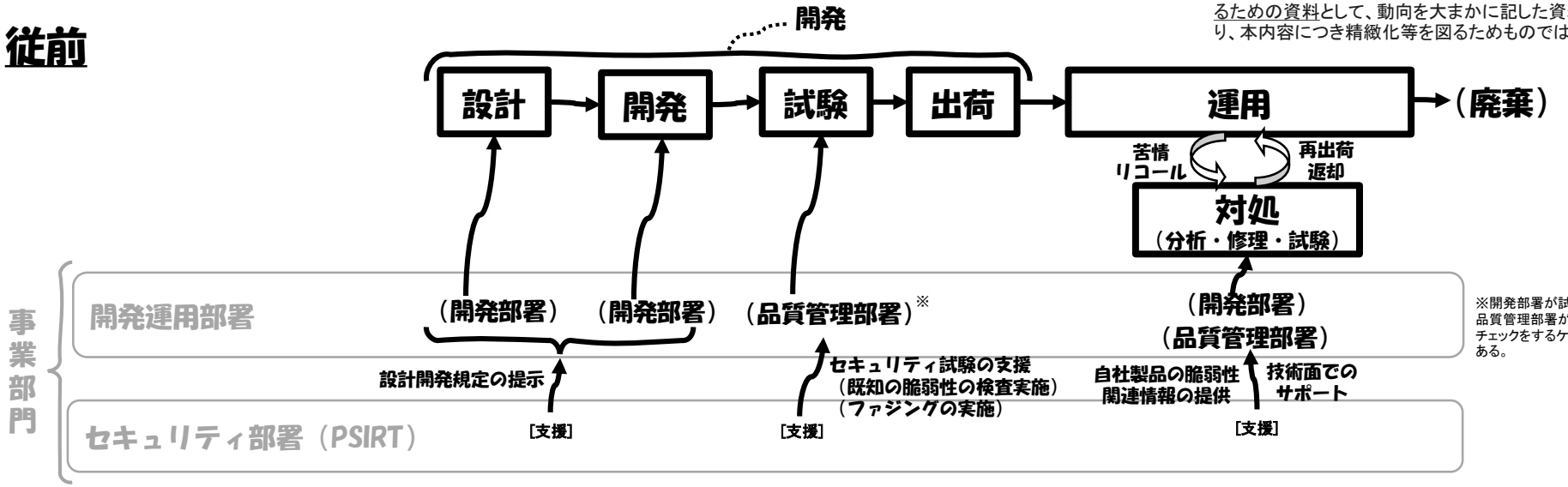
xSIRT	機能構築にあたっての課題	普及にあたっての課題
CSIRT （組織内CSIRT）	（CSIRTの機能構築に関しては多くの事例や参考情報がある。） ※ 機能構築にあたっては、経済産業省の手引き[1]や日本シーサート協議会のスターターキット[2]、JNSAらのセキュリティ対応組織の教科書[3]などが参考となる。	1） ユーザ企業を中心にIT・セキュリティ人材への不足感がある。また、中小企業など経営リソース（資金、人）に限りのある場合がある。
PSIRT	1） 事業部門とIT・セキュリティの両方の知識を備えた人材は極めて少なく、確保が困難。 2） 部品のサプライヤとの間で、セキュリティ確保のための連携体制の構築が必要。	1） 事業部門とIT・セキュリティの両方の知識を備えた人材は極めて少なく、確保が困難。[再掲]
DSIRT/ SSIRT	1） 広範囲に渡るサービスリスク分析などこれまでよりも高度なリスク管理業務を行う専門的知見・人材の蓄積が少ない。 2） 複数の異なる事業部門や他の組織の提供するサービスとの連携におけるセキュリティ・インシデントに対処する連携体制の構築が必要。 ※ CSIRTや既存部署とのすみ分け・役割分担の整理に留意が必要。	1） 広範囲に渡るサービスリスク分析などこれまでよりも高度なリスク管理業務を行う専門的知見・人材の蓄積が少ない。[再掲] 2） デジタルサービスの普及やサービス間連携の増加の一方で、参照できるDSIRT/SSIRT導入事例はまだ少ない。 3） 事業部門横断的な組織・調整機能が必要なため、経営層や経営企画部門が問題意識をもって取り組むことが不可欠。

※ [1]サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き、経済産業省（2020年9月30日）
[2] CSIRTスタータキット Ver2.0、日本シーサート協議会（2011年8月1日）
[3] セキュリティ対応組織（SOC/CSIRT）の教科書 ～機能・役割・人材スキル・成熟度～ 第2.1版、日本ネットワークセキュリティ協会（JNSA）、日本セキュリティオペレーション事業者協議会（ISOG-J）（2018年3月30日）

DXやデジタル技術の活用が進展する際にPSIRTに関連する開発・監視・対処プラクティスはどう変わるか。その動向を踏まえ、今後の人的資源・体制につき考慮すべきことは何か。

※今後の人的資源・体制につき考慮すべき点を議論するための資料として、動向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のものではない。

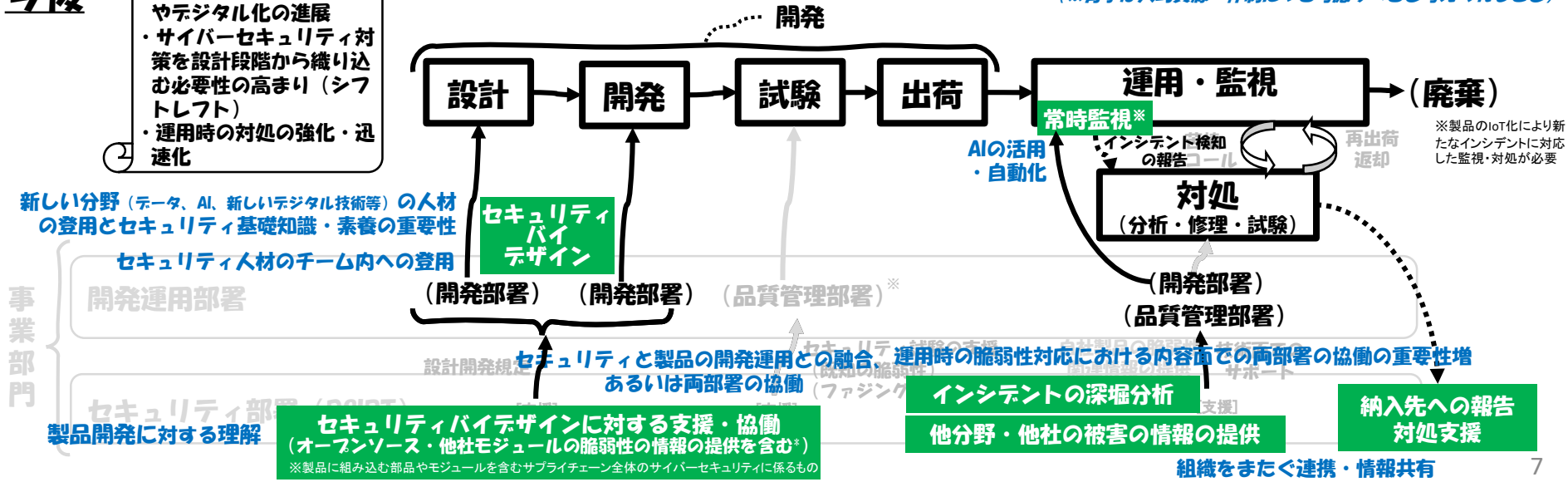
従前



今後

（今後起きうること）
- 製品のネットワーク接続やデジタル化の進展
- サイバーセキュリティ対策を設計段階から織り込む必要性の高まり（シフトレフト）
- 運用時の対処の強化・迅速化

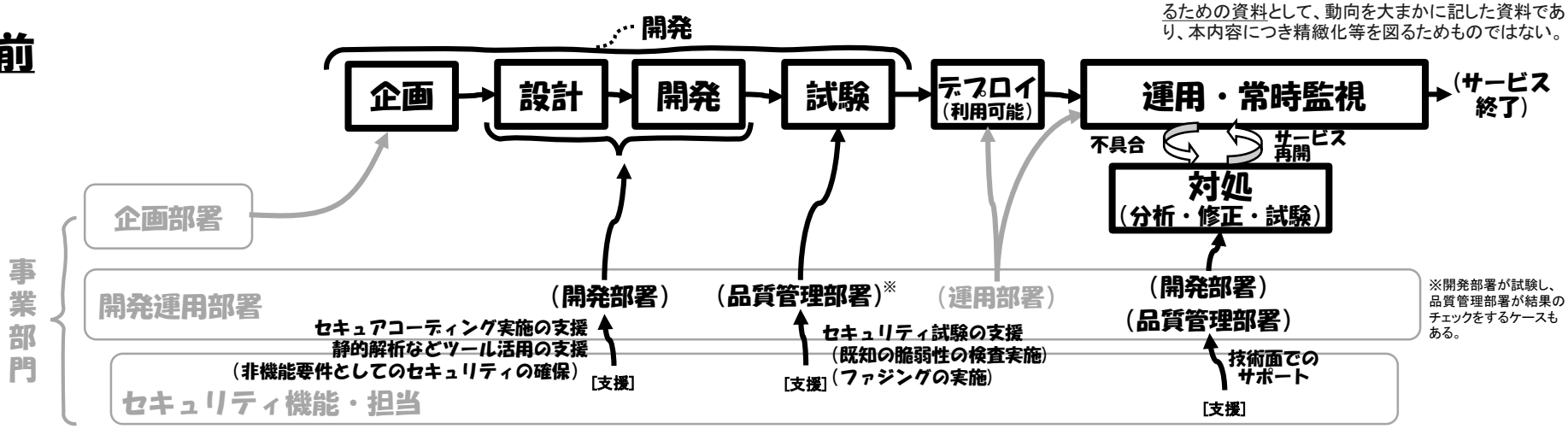
（※緑は重要性が増すと考えられるプラクティス）
（※青字は人的資源・体制につき考慮すべきと考えられること）



DXやデジタル技術の活用が進展する際にデジタル・サービスに関連する開発・監視・対処のプラクティスはどう変わるか。その動向を踏まえ、今後の人的資源・体制につき考慮すべきことは何か。

※今後の人的資源・体制につき考慮すべき点を議論するための資料として、動向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。

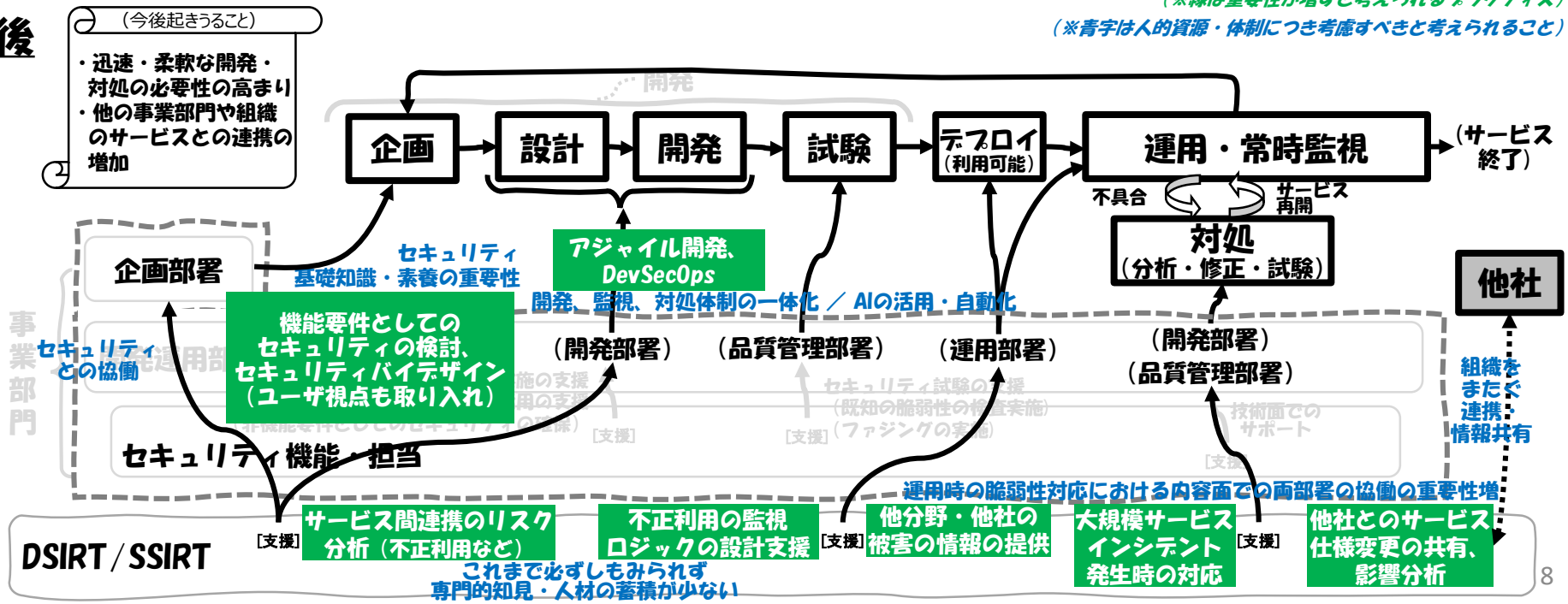
従前



※開発部署が試験し、品質管理部署が結果のチェックをするケースもある。

今後

（※緑は重要性が増すと考えられるプラクティス）
（※青字は人的資源・体制につき考慮すべきと考えられること）



実践・普及に向けた課題（まとめ：SIRT、DSIRT/SSIRT）

＜課題群と方向性（イメージ）＞

①新たな体制構築・プラクティス実践に関する蓄積が少ない　→　モデルやプラクティスの積極共有[次頁以降参照]

②製品・サービスとセキュリティの両方への理解　→　「プラス・セキュリティ」知識の補充できる環境[政策課題２]

③サイバーセキュリティリスクに対する経営問題としての認識／対策に向けたリーダシップの発揮（意識改革）

xSIRT	機能構築にあたっての課題	普及にあたっての課題	DX時代のプラクティス実践に向けた人的資源・体制に係る考慮点
PSIRT	1）事業部門とIT・セキュリティの両方の知識を備えた人材は極めて少なく、確保が困難。 2）部品のサプライヤとの間で、セキュリティ確保のための連携体制の構築が必要。	1）事業部門とIT・セキュリティの両方の知識を備えた人材は極めて少なく、確保が困難。[再掲]	1）新しい分野（データ、AI、新しいデジタル技術等）の人材の登用とセキュリティ基礎知識・素養の重要性 2）セキュリティと製品の開発運用との融合、あるいは部署間（特に開発運用部署とセキュリティ部署）の連携・協働 ←①セキュリティ部署における製品開発に対する理解 ②セキュリティ人材の開発運用部署チーム内への登用 3）納入先等他社との組織をまたいだ連携・情報共有
DSIRT/ SSIRT	1）広範囲に渡るサービスリスク分析などこれまでよりも高度なリスク管理業務を行う専門的知見・人材の蓄積が少ない。 2）複数の異なる事業部門や他の組織の提供するサービスとの連携におけるセキュリティ・インシデントに対処する連携体制の構築が必要。 ※ CSIRTや既存部署とのすみ分け・役割分担の整理に留意が必要。	1）広範囲に渡るサービスリスク分析などこれまでよりも高度なリスク管理業務を行う専門的知見・人材の蓄積が少ない。[再掲] 2）デジタルサービスの普及やサービス間連携の増加の一方で、参照できるDSIRT/SSIRT導入事例はまだ少ない。 3）事業部門横断的な組織・調整機能が必要なため、経営層や経営企画部門が問題意識をもって取り組むことが不可欠。	1）開発・監視・対処プロセスの一体化 2）部署間（特に企画部署、開発運用部署におけるセキュリティ機能・担当、DSIRT/ SSIRT機能を担う組織）の連携・協働 ←セキュリティ基礎知識・素養の重要性 3）サービス連携を行う他社との組織をまたいだ連携・情報共有

モデルやプラクティスの発信

①経済産業省「手引き」（※）に、以上で整理したモデルやプラクティスを記載。

（※）サイバーセキュリティ経営ガイドライン Ver2.0 付録 F　サイバーセキュリティ体制構築・人材確保の手引き、経済産業省（2020年9月30日）。
なお、所要の措置の対象となる「DX認定制度」の認定基準の1つとして、「サイバーセキュリティ経営ガイドライン等に基づき対策を行っていること」が確認できることが規定されている。本「手引き」資料は「サイバーセキュリティ経営ガイドライン」の一部を実践するための参考資料と位置付けられている。

②経営層の関与の下で体制構築を進めていくためには、実際に被害を受けた事例の共有を通じて、サイバーセキュリティリスクに対する経営問題としての認識し、対策に向けたリーダシップの発揮してもらうとともに、経験を通じて得られた気づきを共有し対策の底上げや体制構築等に還元してもらうことが重要。

→このため、セミナーを通じた普及啓発活動に取り組むとともに、こうした被害事例に関する「生」の情報は、企業の経営情報や機微情報に触れる可能性があることから、クローズな場で事例の共有・抽出を図り、内容を集約した事例集を作成していく。

③こうしたモデルやプラクティスが反映された「手引き」、「ナレッジ集」といった基礎的マテリアルに加え、DX時代に即したプラクティスを実践するPSIRT、DSIRT/SSIRT構築に関する好事例の収集を行い、当面、関係省庁との連携の下、「NISC普及啓発・人材育成ポータルサイト」等を活用し、共有を図る。

＜「NISC普及啓発・人材育成ポータルサイト」への掲載事項（イメージ）＞

	政策課題１	政策課題２	政策課題３
基礎的マテリアル	・「手引き」 ・事例集【今後作成】	・「プラス・セキュリティ」モデルカリキュラムに関する資料	・スキル等の共通言語化ツール（JTAG、ITSS+等）
先行事例	・DX時代に対応したPSIRTやDSIRT/SSIRT構築事例	・「プラス・セキュリティ」講座	・新たな流動モード事例

政策課題２

DXに必要な「プラス・セキュリティ」知識を補充できる環境・人材育成の推進

問題意識

〇今後、経済社会のデジタル化に伴い、サービスやプロセスのDXが加速的に進展していくことが想定される中で、経営層や経営企画部門を含め、専門部署ではない部署においても、サイバーセキュリティリスクを全社的な問題としての認識し、自律的に対策が実施されることが求められる。

〇対策実施に当たっては、例えば経営者では、

- どんなシステム・情報資産が自社を支えているか？（デジタル化・ネット活用が進む自社の業務・製品・サービスやサプライチェーンを含む。）
- それらが止まると業務にどのような／どれくらいの範囲で支障が生じるのか？
- 情報漏えいすると、どのような損害が生じるのか？

といった自社の状況の把握から始めることが考えられるが、そうした初歩の取組から具体的な対策の実施に至るまで、その過程でセキュリティ専門人材とのコミュニケーションは欠かせない営為となる。

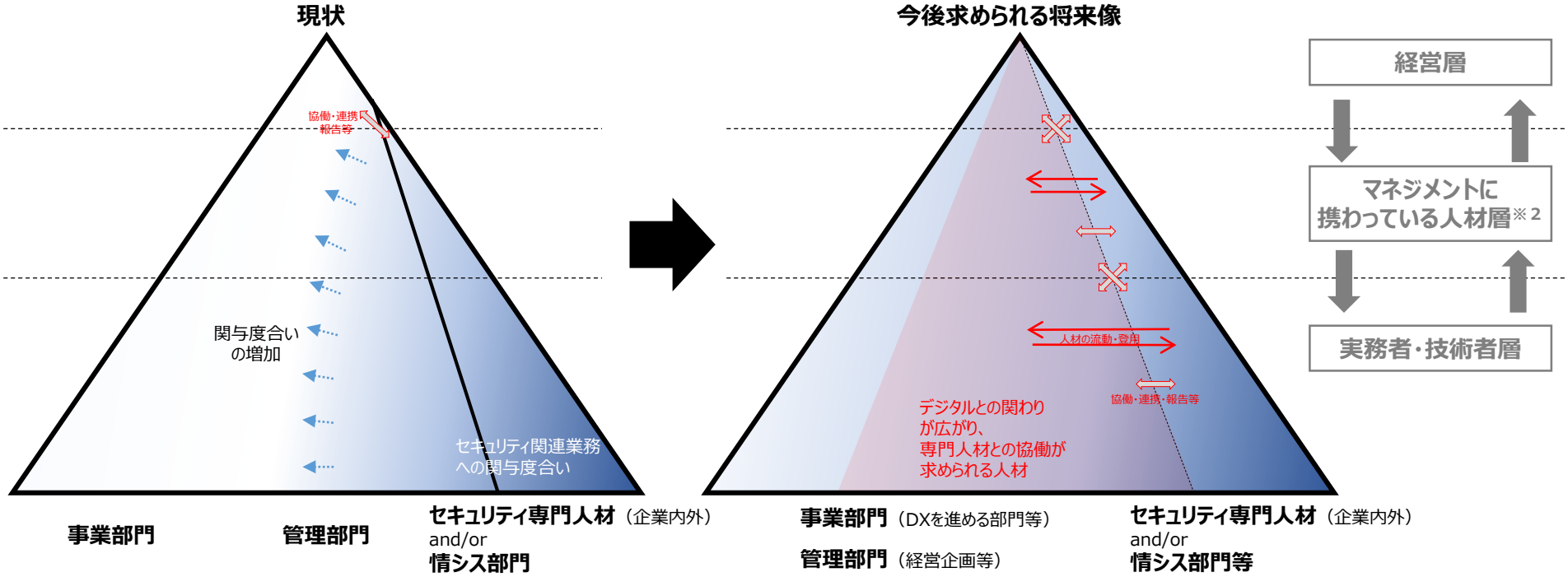
〇一方で、サイバーセキュリティの確保は全社的な課題ではなく、情シス部門又はセキュリティ担当で対処すべき課題と捉えられていないだろうか？

「プラス・セキュリティ」知識の考え方①

○今後は、（経営者やマネジメントに携わっている人材層をはじめとして）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にも、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、ここでは「プラス・セキュリティ」知識と呼ぶ。

＜概念共有のためのイメージ図※1＞



- 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。）

※1　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のものではない。
※2　現行の「サイバーセキュリティ戦略」（2018年7月27日閣議決定）によれば、こうした人材層において、「経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材」が「戦略マネジメント層」と定義されている。

「プラス・セキュリティ」知識の考え方②

○こうした協働はあらゆる部門・人材層において想定されるが、経営企画部門や事業部門のマネジメントに携わっている人材（部課長級など）を例にとれば、「プラス・セキュリティ」知識を補充する取組は、従来取り組まれてきた「戦略マネジメント層の確保・育成」のためのアプローチの１つとして捉えることもできる。

＜セキュリティ専門人材との協働例＞

① デジタルシステムストラテジー
- 「セキュリティ統括」と連携：次期デジタル戦略立案時のセキュリティ体制検討

② デジタルプロダクト開発
- 「セキュリティ統括」と連携：開発環境の更新に関する協議
- 「脆弱性診断・ペネトレーションテスト」と連携：テスト時の脆弱性診断実施
- 「セキュリティ調査分析・研究開発」と連携：脆弱性情報の共有

③ デジタルプロダクト運用
- 「セキュリティ統括」と連携：新規に利用するクラウドアプリのアクセス制御方法協議
- 「セキュリティ監査」と連携：監査指摘事項への対応方法の協議

④ 経営リスクマネジメント
- 「セキュリティ統括」と連携：サイバーセキュリティ保険加入に関する協議

⑤ 法務
- 「セキュリティ統括」と連携：法規改正への対応方針協議

⑥ 事業ドメイン（戦略・企画・調達）
- 「セキュリティ統括」と連携：新規サービスに伴うサイバー関連リスクの評価

⑦ 事業ドメイン（生産現場・事業所管理）
- 「セキュリティ統括」と連携：インシデント発生に備えた訓練の共同実施

（出典）サイバーセキュリティ経営ガイドライン　付録F サイバーセキュリティ体制構築・人材確保の手引き（令和２年９月30日）
経産省、http://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf

＜戦略マネジメント層の確保・育成との関係性＞

＜想定されるキャリアパス＞

「戦略マネジメント層」を担う人材については、経営企画部門や事業部門等のマネジメントラインにおいて、キャリアパスを歩み、現時点でそれらの部門におけるマネジメントに携わっている人材を想定している。そういった人材が、様々な課題に対するマネジメントを行う中の一つの要素として、サイバーセキュリティ関連のリスクに起因する経営・事業上の脅威に対するマネジメントも行うことが期待される。なお、（一般的に伝統的な企業によく見られる傾向として、）事業部門等を含めたサイバーセキュリティのマネジメントに関し、IT 部門（情報システム部門）やリスクマネジメント部門が一括して担当するケースがある。その場合においては、少なくとも経営企画部門や各事業部門との緊密な連携・コミュニケーションや、それらの部門に対するガバナンスの確保が必要である。さらに、IT 部門（情報システム部門）やリスクマネジメント部門の当該人材は、その部門のみの経験ではなく、経営企画部門や事業部門の経験を有していることが望ましい。

→前段と後段で両面のアプローチが記述されている。
「プラス・セキュリティ」知識を補充する取組は前段のアプローチと位置付けられる。

（出典）サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書（平成30年５月31日）
https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf

カリキュラムのモデル化

○内外のセキュリティ専門人材と協働するために必要となる知識は、部門・人材層等によって異なるため、「プラス・セキュリティ」知識は一意に体系化される性質のものではないが、知識を提供するプログラムが広く普及していくためには一定のモデル化が必要である。

○このため、まずは、今後デジタル化が進んでいく中で特に需要が高まると考えられる、「DXを推進する部門の責任者あるいは主要な役割を担う管理職」（※）を対象層としてモデルカリキュラム開発を試行。

（※）DX経営推進者・DX事業推進者等、部課長級であって、必ずしも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方を念頭。

○特に、NISCにおいては、過去に整理された「戦略マネジメント層」向けのモデルカリキュラムと対応し、コンピュータ・情報通信ネットワーク・インターネット・サイバーセキュリティに関する知識のうち、DX推進の中で専門家との協働に当たって、最低限必要で役に立つと考えられる基礎知識の整理作業を行った。※1/21 普及啓発・人材育成専門調査会 参考資料2-1参照

<戦略マネジメント層育成モデルカリキュラム(2018年)>

目的		企業等における事業戦略の企画・立案責任者が、事業戦略そのものに必要なサイバーセキュリティ対策を組み込む（例えば、セキュリティを考慮したビジネス設計や適切な外部委託）ために求められる、専門ベンダーとのコミュニケーションやリスク評価及び対応体制の構築のための知識・スキルを習得する。	
前提知識・経験		企業等において事業やプロジェクトの管理経験を有する者。IT リテラシーは一般ユーザーレベルで可。企業経営に近い部署や業務の経験を有することが望ましい。	
	スクーリング内容	説明	実施方法
第1回	サイバー空間を理解するための基礎知識（基礎知識がある場合にはスキップしてもかまわない）	サイバーセキュリティの全体像を把握するとともに、サイバーセキュリティ上のリスクを理解するために必要となる、以下の基礎知識を理解することで、サイバーセキュリティの専門家とのコミュニケーションに必要なリテラシーを習得する。 (1) 人類と IT（脳木通信から5G、量子コンピューティングまで） (2) サイバー空間と社会（国家、政治、企業、テクノロジー、国民） (3) コンピュータ理論（OS を中心に）、情報通信ネットワーク理論 (4) インターネットの基本原理（ウェブ、電子メール、e コマース、クラウド） (5) サイバーセキュリティの要素技術（暗号と電子署名、認証、アクセス制御）	予習 2 時間 講義 90 分 宿題 2 時間
第2回	サイバー空間における脅威と対策	サイバー空間における主要な脅威を事業上のリスクとして適切に把握することができるよう、脅威及び脆弱性とその対策に関する以下の事項について学ぶ。 (1) 脅威の関係主体（利用者過失、犯罪組織等） (2) 不正・悪用の歴史・トレンドと考え方、犯罪心理 (3) 脅威と対策に関する情報収集の考え方と方法論・基本動作 (4) 脅威のトレンド（サイバーセキュリティに関わる過去の主要な事故やトラブル） (5) 脆弱性と対策（脆弱性の原理と対策方法、性能や利便性とのトレードオフ）	予習 2 時間 講義 90 分 （場合によっては、90×2分） 宿題 2 時間
第3回	サイバーセキュリティに関連する法令・規格・諸制度	サイバーセキュリティ確保のために事業者が遵守すべき事項や、効果的な対策実現のために参照すべき制度等について学ぶ。 (1) 法令・規格・諸制度対応の考え方と方法論・基本動作 (2) 関連法令（不正アクセス禁止法、不正競争防止法、個人情報保護法、EU 一般データ保護規則（GDPR）等） (3) 規格・標準・ガイドライン（ISO 31000、ISO/IEC 27000 シリーズ、SP-800.171 等） (4) その他（クラウドサービスにおける約款、サイバーセキュリティ保険、インターネットの関係機関）	予習 2 時間 講義 90 分 宿題 2 時間
第4回	サイバーセキュリティに関連するリスクマネジメントの方法	リスクマネジメントを行う上でのサイバーセキュリティ分野の特殊性について認識した上で、リスクを許容レベル以下に抑制するための方法について、グループワークによる演習を通じて学ぶ。 (1) リスクマネジメントの基本的考え方と方法論・基本動作 (2) サイバーセキュリティリスクに関連するリスクの評価方法 (3) (2)で評価したリスクについての低減、回避、保有、移転の方法 (4) 体制構築（組織内での連絡・共有体制の整備・維持、外部専門家の活用等） (5) インシデント対応プロセス（異常検知、サービス停止の判断、復旧、メディア対応等）	予習 2 時間 講義 30 分+ 演習 60 分 宿題 2 時間
第5回	企業価値向上とサイバーセキュリティ	事業において IT が担う役割が大きな企業ほど、サイバーセキュリティ対策を含めた形で適切にリスク管理されたサービスを提供することが企業価値の向上につながることを認識し、サイバーセキュリティ対策があらかじめ組み込まれた事業戦略を企画立案するための方法について、グループワークによる演習を通じて学ぶ。 (1) 企業価値とサイバーセキュリティの基本的考え方と方法論・基本動作 (2) 企業価値への影響を考慮した費用対効果分析に基づくサイバーセキュリティ投資の考え方 (3) セキュリティ品質とブランド戦略・顧客との信頼醸成 (4) セキュリティ対策の証明と情報発信	予習 2 時間 講義 30 分+ 演習 60 分 宿題 2 時間

最低限必要で役に立つと考えられる基礎知識を体系化

作業①：DX推進に際し活用が想定される場面から逆算し、どのような状態を目指すかを整理した。

↓

作業②：実務目線からIT 初心者に必要な知識が整理された「IT パスポートシラバス」を参照し、ｉ：詳細な目標とｉｉ：予め理解することが望ましいと考えられる基礎概念を整理した。

【詳細は1/21 普及啓発・人材育成専門調査会参考資料2-2等を参照】

↓

情報セキュリティ大学院大学において実施されたプログラム（試行カリキュラム）において、上記の作業結果を参考にしていただいた。

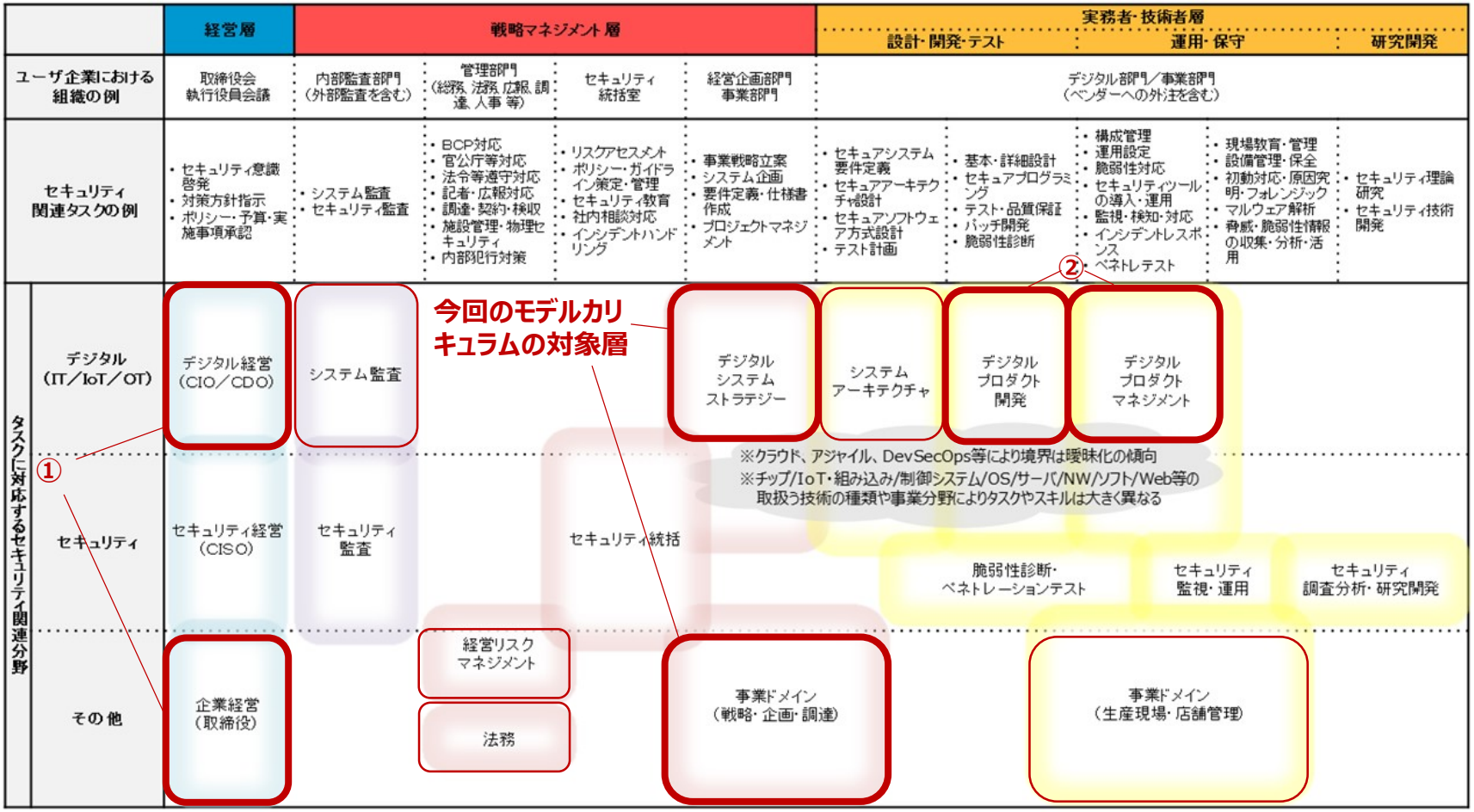
【詳細は1/21 普及啓発・人材育成専門調査会資料1-7を参照】

※（出典）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「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ 報告書」（2018年5月）

プログラムの普及促進策①

○さらに、今回の試行をベースとして、部課長級向けのカリキュラムの改善に加え、今後需要が高まっていくと思われる他の人材層に向けた取組の進展も期待される。（また、次世代の人材育成においても念頭に置く必要がある。）

○例えば、政策課題１でとりあげたように、①経営層：意識改革とあわせてDXに対応した体制構築を担える人材、②製品開発・品質管理部門：PSIRTを担う人材で潜在的な需要があり、体系的な整理が必要。



□「プラス・セキュリティ」知識が必要となり得る分野

（出典）サイバーセキュリティ経営ガイドライン　付録F サイバーセキュリティ体制構築・人材確保の手引き（令和２年９月30日）
経産省、http://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf

プログラムの普及促進策②

○量的な広がりを生むためには市場が形成され需要と供給が相応して増加していくことが望ましいが、その初期段階においては、需要の喚起に加え、需要者からみて一定の質が確保・期待される仕組みづくりが重要ではないか。

○海外の事例を参考に、当面、関係省庁との連携の下、NISC「普及啓発・人材育成ポータルサイト」を活用し、基礎的なマテリアルとあわせ、官民で行われる「プラス・セキュリティ」講座の掲載を積極的に行うことを検討。

＜「NISC普及啓発・人材育成ポータルサイト」への掲載事項（イメージ）＞

	政策課題１	政策課題２	政策課題３
基礎的マテリアル	・「手引き」 ・事例集【今後作成】	・「プラス・セキュリティ」モデルカリキュラムに関する資料	・スキル等の共通言語化ツール（JTAG、ITSS+等）
先行事例	・DX時代に対応したPSIRTやDSIRT/SSIRT構築事例	・「プラス・セキュリティ」講座	・新たな流動モード事例

政策課題３

セキュリティ人材の活躍の促進に向けた流動性とマッチングの機会の促進

IT・セキュリティ人材の流動ごとにみられる特徴と動向

主な流動	キャリア形成の特徴	現在の動向等
①人材のベンダー企業間の流動 ※右の分析に当たっては、ベンダー企業については、セキュリティベンダーを念頭に置いて記載を行っている。ITベンダー、NWベンダーなどで右の特徴や動向にはバリエーションが存在し得る。	・自らの技術力や専門性を高めることで業界での地位を高める。（なお、エンジニアからコンサルといった職種を移行したキャリア形成も考えられる。）	・トップ人材を中心に流動が多くみられる。【有識者意見】 ・JNSAによるJTAGや、IPAによるITSS+をはじめ、スキルを可視化するためのツールが官民で整備されつつある。 ※中長期的には、AIやRPA等を活用した自動化等により、監視・運用などの特定の職種でベンダー企業からの人材流動が生まれる可能性がある。
②人材のユーザ企業・組織への流動	・DXを主体的に推進するユーザ企業において、ベンダー企業等で培った専門性を実際に活用し、経験を高める。	・ベンダー企業に比し、ユーザ企業における人材不足感は大きい。 ・今後ユーザ企業におけるDX進展の中で更に不足感は拡大していくものと考えられる。
特に地域・中小企業	・上記に加え、地元・地域課題への貢献といった動機が考えられる。	・地理的制約により、大都市圏に集中しがちな人材を獲得することが難しい。 ・規模的制約により、専任の人材を配置することや、どのような人材が必要かの明確化が難しい。
特に 政府・自治体	・行政のデジタル改革業務に携わることで、多様な人脈の形成や、今後様々なDXの現場で必要となる業務改革の経験を獲得し、後の活躍の幅を広げる。	・行政のデジタル化やデジタル庁の設立等の動きにともない、政府・自治体での専門人材のニーズが増えることが想定される。

※このほか、③ユーザ企業からベンダー企業へのUターンや、④ユーザ企業同士の流動も考えられるが、こうした流動は、②ベンダー企業からユーザ企業への流動が広がれば、波及して増加する側面もあると考えられる。

DX推進の対応方法・人材確保の選択肢

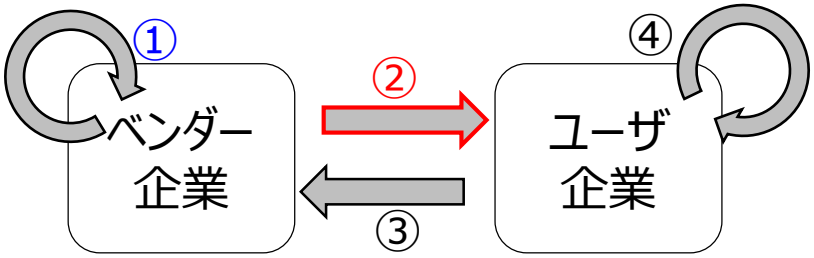
○ユーザ企業におけるシステムの開発は外部委託が主流であったが、DX推進にあたってはユーザ企業の主体的な取り組みが重要であるとの観点から、人材育成や即戦力となる専門人材を中途採用や副業・兼業等により外部から登用することも重要な選択肢となり得る。

対応方法・人材確保の選択肢		特徴	動向
自社対応	人材育成	・社内にノウハウを蓄積できる。 ・自社の業務をよく理解した人材を育てることができる。 ・育成には時間がかかるため、中長期的な計画に基づき確保していく必要がある。	・これからDXに取り組む企業にとっては、育成計画の策定が課題となる。核となる人物を外部から採用することで推進しているケースがみられる。
	中途採用 ※副業・兼業を経て、中途採用となるケースもあり得る。	・即戦力となる人材の確保が可能であり、自社内にはないスキルを直ぐに活用したい場合に有効である。 ・既存の組織にない多様な視点・ノウハウ・人脈の確保等による新たな発想やイノベーションを期待できる。 ・ジョブ型雇用への移行や、俸給等の見直しにもあわせて取り組むことが定着につながる。 ・一度に多くの要員を獲得することは困難である。	・デジタル化を推進している企業ほど中途採用を積極的にしている傾向がある。 ・DXを推進する上で核となる人材として獲得し、社内の人材育成やプロジェクトの推進を担うといった活用がみられる。 ・リモートワークの普及等もあり、地域・中小企業でも獲得しやすくなっていると想定される。 ・人材側の副業・兼業の関心は高くなっており、目的も仕事内容を重視している傾向がある。
	特に副業・兼業	・専門人材側も応募しやすく、比較的優秀な人材の確保が期待できる。 ・複数の業務を掛け持ちすることから、作業を依頼できる時間に制約が生まれる。 ・機密保持の観点から、依頼しづらい業務もあるとの声も。	
外部委託		・特定の期間のみ必要な業務であったり、専門人材を多く必要とする業務については、外部に委託する方が効率的な場合がある。 ・社内へのノウハウの蓄積ができない。	・リソース状況に応じて外部委託を活用することは有益であるが、全てを委託せず、戦略・方針の立案や意思決定は自社要員で実施することが肝要となる。

DX時代におけるIT・セキュリティ人材の流動モード

○①人材のベンダー企業間への流動では、JTAGやITSS＋など、スキルの共通言語化ツールが活用され、トップ人材に留まらない動きとなることが期待される。

○②人材のユーザ企業・組織への流動は、IT・セキュリティ人材がベンダー企業に固定化・偏在している現状、DXの取組の広がりや他のセクターへの波及効果を踏まえ、以下のような新たな流動モードを念頭に置き重点的に取り組まれるべき。



流動の波及イメージ

① 人材のベンダー企業間の流動

現状①は一定程度進展。
②の動きも少しずつ表れ始めている。

② 人材のユーザ企業・組織への流動

③ ユーザ企業からベンダー企業

ユーザ企業で培った経験を基に、ベンダー企業で活かすことで、活躍することを目的とした流動。

④ ユーザ企業間

ユーザ企業で培った経験を基に、ユーザ企業を渡り歩きながら活躍することを目的とした流動。

新たな流動モード（例）

a. リモートワーク、副業・兼業といった新たな働き方・雇用形態の活用

○コロナ禍を経て浸透・定着しつつあるリモートワークは、地理的な制約を克服し得る。

○また、今後、副業・兼業といった雇用形態も広がっていくと想定される中、地域・中小企業への流動に向けて、双方のハードルは更に下がっていくと想定される。

○副業・兼業を認める企業にとっても、自社では獲得できない経験や知識の還元や、柔軟な職務環境の実現により更なる優秀な人材の獲得へのアピールも期待できる。

b. 行政のデジタル化を成長の機会としたキャリアモデル

○デジタル庁の創設やそれに伴うマイナンバーカード普及の本格化等に伴い、今後、政府・自治体ともにIT・セキュリティ人材への需要は高まる見込み。

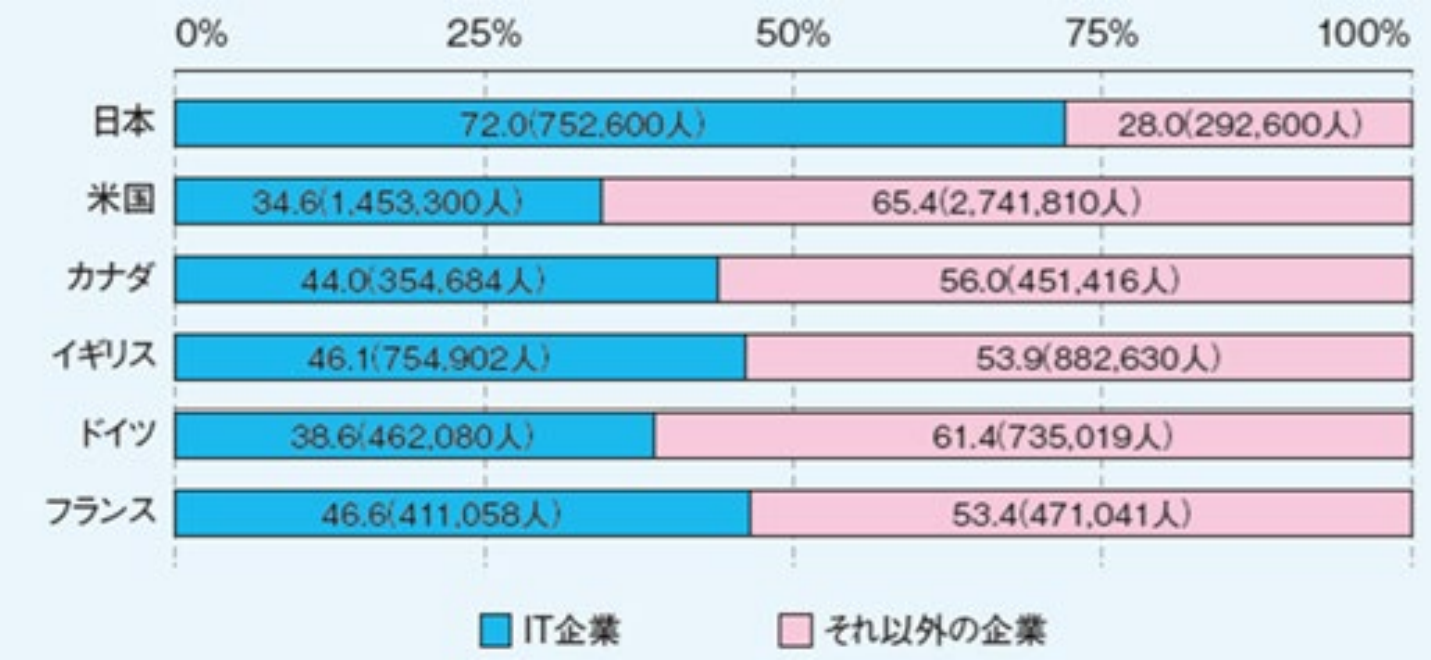
○こうした改革業務に携わることで、多様な人脈の形成や、今後様々なDXの現場で必要となる業務改革の経験を獲得することができ、ユーザ企業での活躍や起業等の更なるキャリアアップを目指すことも想定される。

このほか、DX進展の中での新たなデジタルサービス開発や、生産現場へのIoTの浸透による生産管理の現場など、幅広い領域でIT・セキュリティ人材の活躍の場が広がると考えられる。

（参考）IT人材の所在に関する国際比較

○IT企業に所属する情報処理・通信に携わる人材の割合を比較すると、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%）

＜日米、欧州等のIT企業・IT企業以外の企業における情報処理・通信に携わる人材の割合＞



（出典）独立行政法人情報処理推進機構「IT人材白書2017」 https://www.ipa.go.jp/files/000059087.pdf

---

※上記の出典等：

○日本：2015年国勢調査結果（I T企業として扱った業種は、「ソフトウェア業」、「情報処理・提供サービス業」、「インターネット附随サービス業」。情報処理・通信に携わる人材として扱った職種は、「システムコンサルタント・設計者」、「ソフトウェア作成者」、「その他の情報処理・通信技術者」）

○米国：職業雇用統計（IT企業として扱った業種は、「511200 Software Publishers」、「518200 Data Processing, Hosting, and Related Services」、「541500 Computer Systems Design and Related Services」。情報処理・通信に携わる人材として扱った職種は、「11-3020 Computer and Information Systems Managers」、「15-1100 Computer Occupations」）

○カナダ：カナダ情報局（Statistics Canada　http://www.statcan.gc.ca）のデータを基にICTCが作成（出典元「Digital Economy Annual Review 2015」）、情報処理・通信に携わる人材の職種、IT企業として扱った業種は米国の基準に準拠。

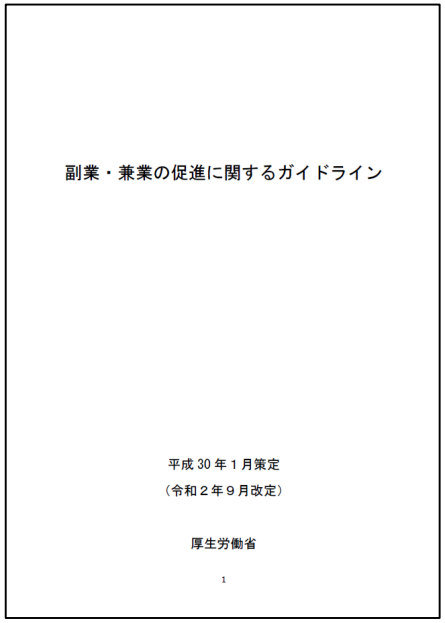
○イギリス、ドイツ、フランス：EU統計局（Eurostat）が保有する労働力調査（EU LFS）の結果を調査会社であるempiricaが入手し分析したものを利用

流動促進に向けた環境整備（兼業・副業）

○「成長戦略実行計画」（令和２年12月１日閣議決定）においても「兼業・副業の定着を通じて転職が活性化することは、日本の組織全体に好影響を与える」とされており、我が国の経済成長の観点からも「兼業・副業」は政府全体としての重要な政策課題として位置づけられている。

○従来、「兼業・副業」を認めるに当たっては、労働時間管理のあり方が論点になっていたが、本年9月に厚生労働省がガイドラインを改訂し、「労働時間の自己申告制を設け、申告漏れや虚偽申告の場合には、兼業先での超過労働によって上限時間を超過したとしても、本業の企業は責任を問われない」ことを明確化。今後、ガイドラインの分かりやすいパンフレットや、労働時間の申告の際に活用できる様式の丁寧な周知等を図っていくこととされている。

※本ガイドラインでは、副業・兼業の場合に留意する点として、安全配慮義務、秘密保持義務、競合避止義務、誠実義務にも触れられているが、本業側への利益誘導の防止や利益相反への懸念といった声もある。



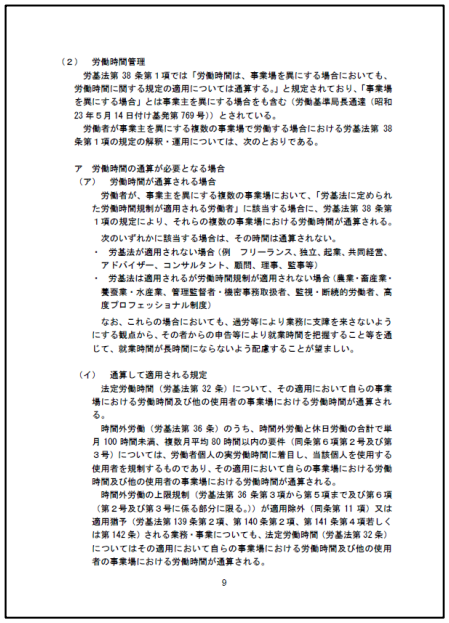
副業・兼業の促進に関するガイドライン

平成 30 年１月策定

（令和２年９月改定）

厚生労働省

1



（２） 労働時間管理

労基法第 38 条第１項では「労働時間は、事業場を異にする場合においても、労働時間に関する規定の適用については通算する。」と規定されており、「事業場を異にする場合」とは事業主を異にする場合をも含む（労働基準局長通達（昭和23 年５月 14 日付け基発第 769 号））とされている。

労働者が事業主を異にする複数の事業場で労働する場合における労基法第 38 条第１項の規定の解釈・運用については、次のとおりである。

ア 労働時間の通算が必要となる場合

（ア） 労働時間が通算される場合

労働者が、事業主を異にする複数の事業場において、「労基法に定められた労働時間規制が適用される労働者」に該当する場合に、労基法第 38 条第１項の規定により、それらの複数の事業場における労働時間が通算される。

次のいずれかに該当する場合は、その時間は通算されない。

・ 労基法が適用されない場合（例 フリーランス、独立、起業、共同経営、アドバイザー、コンサルタント、顧問、理事、監事等）

・ 労基法は適用されるが労働時間規制が適用されない場合（農業・畜産業・養蚕業・水産業、管理監督者・機密事務取扱者、監視・断続的労働者、高度プロフェッショナル制度）

なお、これらの場合においても、過労等により業務に支障を来さないようにする観点から、その者からの申告等により就業時間を把握すること等を通じて、就業時間が長時間にならないよう配慮することが望ましい。

（イ） 通算して適用される規定

法定労働時間（労基法第 32 条）について、その適用において自らの事業場における労働時間及び他の使用者の事業場における労働時間が通算される。

時間外労働（労基法第 36 条）のうち、時間外労働と休日労働の合計で単月 100 時間未満、複数月平均 80 時間以内の要件（同条第６項第２号及び第３号）については、労働者個人の実労働時間に着目し、当該個人を使用する使用者を規制するものであり、その適用において自らの事業場における労働時間及び他の使用者の事業場における労働時間が通算される。

時間外労働の上限規制（労基法第 36 条第３項から第５項まで及び第６項（第２号及び第３号に係る部分に限る。））が適用除外（同条第 11 項）又は適用猶予（労基法第 139 条第２項、第 140 条第２項、第 141 条第４項若しくは第 142 条）される業務・事業についても、法定労働時間（労基法第 32 条）についてはその適用において自らの事業場における労働時間及び他の使用者の事業場における労働時間が通算される。

9

↓ ガイドラインには、労働者、企業双方のメリットや留意点も明確に示されている。

【労働者】

メリット：

① 離職せずとも別の仕事に就くことが可能となり、スキルや経験を得ることで、労働者が主体的にキャリアを形成することができる。

② 本業の所得を活かして、自分がやりたいことに挑戦でき、自己実現を追求することができる。

③ 所得が増加する。

④ 本業を続けつつ、よりリスクの小さい形で将来の起業・転職に向けた準備・試行ができる。

留意点：

① 就業時間が長くなる可能性があるため、労働者自身による就業時間や健康の管理も一定程度必要である。

② 職務専念義務、秘密保持義務、競業避止義務を意識することが必要である。

③ １週間の所定労働時間が短い業務を複数行う場合には、雇用保険等の適用がない場合があることに留意が必要である。

【企業】

メリット：

① 労働者が社内では得られない知識・スキルを獲得することができる。

② 労働者の自律性・自主性を促すことができる。

③ 優秀な人材の獲得・流出の防止ができ、競争力が向上する。

④ 労働者が社外から新たな知識・情報や人脈を入れることで、事業機会の拡大につながる。

留意点：

① 必要な就業時間の把握・管理や健康管理への対応、職務専念義務、秘密保持義務、競業避止義務をどう確保するかという懸念への対応が必要である。

（出典）厚生労働省 「副業・兼業の促進に関するガイドライン」 （平成 30 年１月策定 （令和２年９月１日改定） ）
https://www.mhlw.go.jp/file/06-Seisakujouhou-11200000-Roudoukijunkyoku/0000192844.pdf

流動促進に向けた環境整備（政府のデジタル化）

○政府のデジタル社会の実現に向けた改革の基本方針において、政府におけるデジタル人材の確保に関して、「民間、自治体、政府を行き来しながらキャリアを積める環境を整備」と言及されており、今後、具体的な検討が進められる中で、官民の高度外部人材の交流が活発化することが期待される。

（７）デジタル人材の確保

デジタル庁を含め政府部門においてデジタル改革を牽引していく人材を確保するため、ITスキルに係る民間の評価基準活用により採用を円滑に進める等、優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境を整備する。

令和３年度前半に「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）」を改定し、デジタル人材の採用計画や育成・キャリアパスの策定のための基本的な考え方、研修の充実・強化方策を新たに示すとともに、この改定を踏まえ、各府省において「セキュリティ・IT人材確保・育成計画」についても、速やかに改定することとする。

また、デジタル人材の採用について、採用募集活動を強化し、令和３年度から、デジタル庁を中心に各府省において国家公務員採用試験の総合職試験（工学区分）や一般職試験（電気・電子・情報区分）等の合格者の積極的な採用に努めるとともに、民間企業等における実務経験を有する人材を確保するため経験者採用試験を活用するものとする。

あわせて、国家公務員採用試験について、令和４年度以降の実施に向けて総合職試験に新たな区分（「デジタル」（仮称））を設けることや、出題などに関する検討を人事院に要請する。

これらにより、行政と民間のデジタル人材が効果的に連携して業務を進める組織文化を醸成する。

（出典）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）
※赤字の下線は事務局にて付記

流動促進に向けた環境整備（自治体のDX推進）

○自治体DX推進計画において、自治体におけるデジタル人材の確保に関して、現在CIO補佐官への外部人材の任用が少ない状況の中、外部人材の活用のニーズがあることから、市町村のCIO補佐官等への外部人材の任用等を支援が検討されている。

地方自治体のデジタル化に向けた人材確保の必要性

○　CIO補佐官はCIOのマネジメントを専門的知見から補佐する役割を担うが、現在、外部デジタル専門人材を任用している市町村はほとんどない。また、今後のデジタル化を進めていくため、外部から専門人材を招き、登用したいというニーズがある。

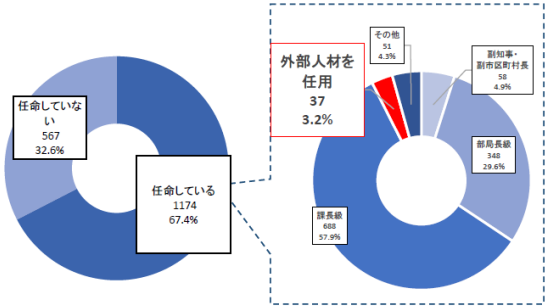
外部人材CIO補佐官設置市町村（37団体／1741団体）

※現行制度（任期付職員、特別職非常勤職員）の活用により民間のデジタル人材の柔軟な任用が可能

○　また、自治体の情報化担当職員の確保・育成も課題となっている。

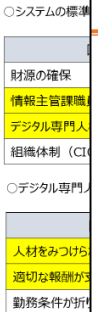
（※情報化担当職員が5人以下の市町村が6割以上）

・CIO補佐官の任命状況（市区町村）



出典：総務省「自治体情報管理概要」（2019年3月）

・市町村へのアンケート



出典：総務省「デジタル専門

地方自治体のデジタル人材の確保・育成のための支援（案）

【外部人材の確保】

プロパー職員が担うことが多いCIOを補佐するCIO補佐官等を想定。高度なデジタル知識を有していることが期待される。

○ **デジタル庁・総務省・都道府県が連携**して市町村のCIO補佐官等の外部人材任用等を支援

（複数市町村での兼務等を想定）

・デジタル庁　：デジタル庁人材と自治体向け人材を同時にリクルーティング、人材のレベル維持
・総務省　　：デジタル庁・企業の協力のもと都道府県へ人材紹介
・都道府県　：地域の人材の掘り起こし、市町村のニーズの調整

※新たに、市町村が外部人材を雇用する場合の経費について特別交付税措置（措置率0.5）を講じる。

【内部人材の育成】

プロパー職員を想定。基本的なデジタル知識を有していることが期待される。

○**デジタル庁・総務省が連携**して以下の取組を実施

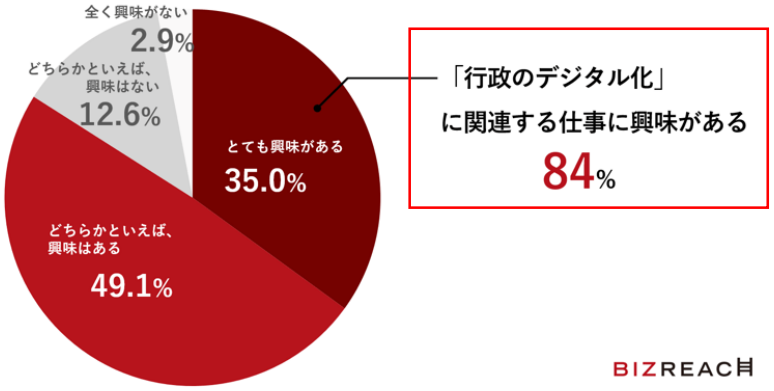
・自治体のデジタル担当職員とデジタル庁との対話を促進するため、オンラインでのデジタル化に関する意見交換の仕組みである**「共創プラットフォーム」**を創設
・デジタル担当職員に対するデジタル庁等の**研修**
・自治体のデジタル担当職員の**デジタル庁への出向**等のキャリアパスを通じたデジタル人材としての育成

（出典）総務書「自治体ＤＸ推進計画概要」　（令和2年12月25日）
※赤字の下線は事務局にて付記

（参考）行政のデジタル化への関心

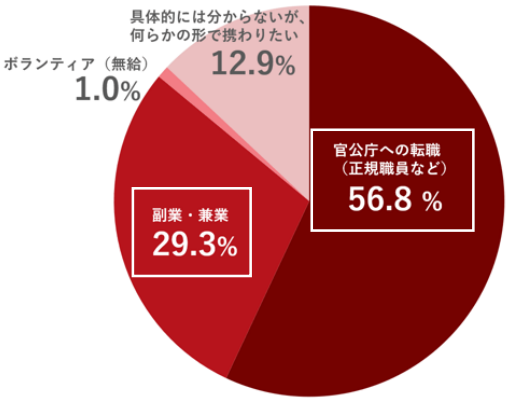
即戦力の民間デジタル人材にアンケート
約8割が官公庁の仕事に興味あり、うち約3割が「副業・兼業」を希望

Q.「行政のデジタル化」に関連した仕事に興味はありますか？ （n=578）



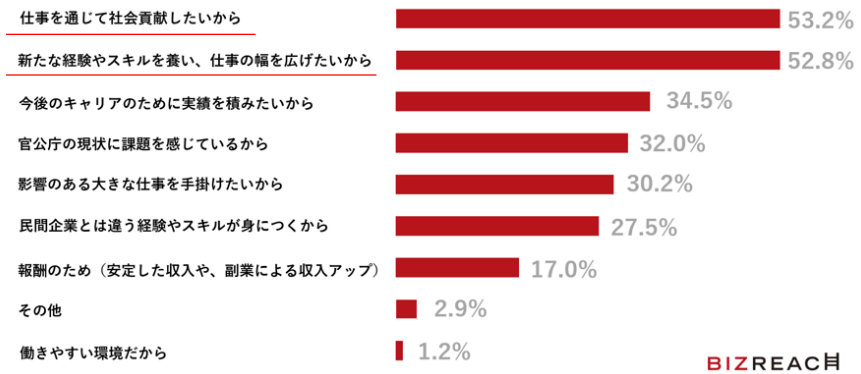
BIZREACH

Q.「行政のデジタル化」の仕事にはいくつかの雇用形態の可能性がありますが、ご自身がお仕事をされるとしたら、検討するものはどれですか？ （n=488）



BIZREACH

Q.「行政のデジタル化」に関連した仕事に興味がある理由を具体的に教えてください
（複数回答、最大3つ選択）（n=487）



BIZREACH

（出典）株式会社ビズリーチ「即戦力の民間デジタル人材にアンケート約8割が官公庁の仕事に興味あり、うち約3割が「副業・兼業」を希望」
※枠囲み、赤字の下線は事務局にて付記
https://www.bizreach.co.jp/pressroom/pressrelease/2020/1207.html

マッチング促進策

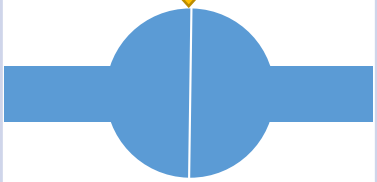
- 異なるセクター間のマッチングにおいては、需要の明確化、供給の質の明確化は大前提。特に、需給双方で、ITSS＋やJTAGをはじめ、官民で整備されてきたセキュリティに係るスキルの共通言語化ツールの活用を進めるべきではないか。
- 加えて、新たな流動モードでは、事例やつながりが少ないためにマッチングに向けた障壁が高くなるおそれがあるところ、こうした課題への対応が必要ではないか。
  （→具体的には、積極的なプラクティスの共有や地域におけるコミュニティ形成を政策的に推進することが考えられる。）

新たな流動モードにおけるマッチングの障壁

② 経験もなく具体的なイメージがわかず実現するにはハードルが高いと思われる

③ 人材、企業・組織が知り合う場がない

マッチングの機会創出



人材側の視点

① 自分の能力を示すためにスキルの明確化が必要

プログラムの活用が期待

大学等の教育機関、民間企業
様々なリカレントプログラムの提供

受入企業・組織側の視点

① 組織内の人材の能力や必要となる人材像を把握して、採用すべき人材像やジョブディスクリプションを明確化することが必要

※ このためには、採用を推進する経営層及び戦略マネジメント層における「プラス・セキュリティ」「プラス・IT」知識が非常に重要となる。

有機的な連携が期待

供給の質の明確化　　**需要の明確化**

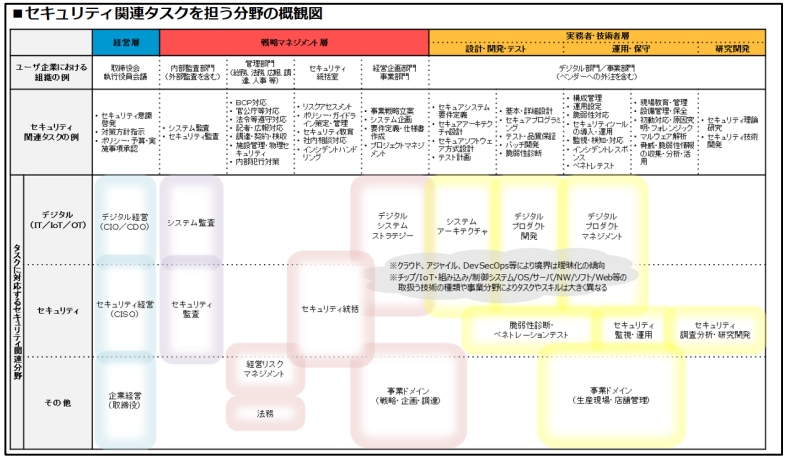
＜マッチング促進の今後の方向性（イメージ）＞

① → スキルの共有言語化ツール（ITSS＋、JTAG等）の活用促進
② → 流動モードに対応したマッチング事例（プラクティス）の積極共有
③ → 地域におけるコミュニティ形成の政策的推進

NISC「普及啓発・人材育成ポータルサイト」の活用

（参考）官民で整備されているスキルの共通言語化ツールの例

ITSS+「セキュリティ領域」



■分野とセキュリティ関連タスク等との対応

区分	分野名	セキュリティ関連タスクの例	担当部署／機能の例（青字は社外ベンダー等）
経営層	デジタル	セキュリティ意識啓発、対策方針の指示、セキュリティポリシー・予算・対策案施事項の承認 等	経営者、経営層（CISOを含む）
経営層	セキュリティ		
経営層	その他		
戦略マネジメント層	デジタル	システム監査	システム監査、報告・助言 等	監査部門 ITベンダー・監査法人（システム監査サービス）
戦略マネジメント層	デジタル	デジタルシステムストラテジー	デジタル事業戦略立案、システム企画、要件定義・仕様書作成、プロジェクトマネジメント 等	経営企画部門、IT企画部門、IT・デジタル部門の企画機能 IT/セキュリティコンサルタント
戦略マネジメント層	セキュリティ	セキュリティ監査	セキュリティ監査、報告・助言 等	監査部門 セキュリティベンダー・監査法人（セキュリティ監査サービス）
戦略マネジメント層	セキュリティ	セキュリティ統括	セキュリティ教育・普及啓発、セキュリティ関連の講義・講演、セキュリティリスクアセスメント、セキュリティポリシー・ガイドラインの策定・管理・周知、警報・喜ぶ等対応、社内相談対応、インシデントハンドリング 等	セキュリティ専門部門、CSIRT セキュリティ委員会 IT・デジタル部門のセキュリティ対策機能
戦略マネジメント層	その他	経営リスクマネジメント	経営リスクマネジメント、BCP／危機管理対応、サイバーセキュリティ保険検討、記者・広報対応、施設管理・物理セキュリティ、内部犯行対策 等	総務部門（リスク管理部門を含む） 経営企画部署、総務部署等のリスクマネジメント機能
戦略マネジメント層	その他	法務	デジタル関連法令対応、コンプライアンス対応、契約管理 等	法務部門、総務部門の法務担当
戦略マネジメント層	その他	事業ドメイン（戦略・企画・調達）	事業特有のリスクの洗い出し、事業特性に応じたセキュリティ対応、サプライチェーン管理 等	事業部門の企画機能 事業戦略コンサルタント
実務者・技術者層	デジタル	デジタルシステムアーキテクチャ	セキュアシステム要件定義、セキュアシステムアーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画 等	IT・デジタル部門の設計機能、IT子会社 IT/OTベンダー
実務者・技術者層	デジタル	デジタルプロダクト開発	基本設計、詳細設計、セキュアプログラミング、テスト・品質保証、パッチ開発 等	IT・デジタル部門の開発・保守機能、IT子会社 IT/OTベンダー
実務者・技術者層	デジタル	デジタルプロダクト運用	構成管理、運用設定、利用者管理、サポート・ヘルプデスク、脆弱性対策・対応、インシデントレスポンス 等	IT・デジタル部門の運用機能、IT子会社 IT/OT/セキュリティベンダー
実務者・技術者層	セキュリティ	脆弱性診断・ペネトレーションテスト	脆弱性診断、ペネトレーションテスト 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（脆弱性診断サービス）
実務者・技術者層	セキュリティ	セキュリティ監視・運用	セキュリティ製品・サービスの導入・運用、セキュリティ監視・検知・対応、インシデントレスポンス、連絡受付 等	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（セキュリティ監視・運用サービス）
実務者・技術者層	セキュリティ	セキュリティ調査分析・研究開発	サイバー攻撃捜査、原因究明・フォレンジック、マルウェア解析、脅威・脆弱性情報の収集・分析・活用、セキュリティ理論・技術の研究開発、セキュリティ市場動向調査 等	CSIRT/IT・デジタル部門のリサーチ機能、IT子会社 セキュリティベンダー（デジタルフォレンジックサービス）
実務者・技術者層	その他	事業ドメイン（生産現場・事業所管理）	現場教育・管理、設備管理・保全、QC活動、初動対応 等	運転、保全、計装、品質管理関連部署、PSIRT OT/セキュリティベンダー

（出典）情報処理推進機構（IPA）「ITSS+「セキュリティ領域」改訂版」
（2020年10月2日公開）
https://www.ipa.go.jp/files/000058688.xlsx

JTAG

図 19　サンプルプロファイルとスキルチャート例

このような比較により、個人および組織・企業において次のような活用を想定している。
個人：
- 自己のスキルレベル・特定の業務における遂行能力の把握
- 目指す業務とのギャップ把握
- 目指す業務に向けた方策把握
- 求人や特定のセキュリティ業務とのマッチ度把握

企業・組織
- 所属メンバーのスキルレベル・特定の業務における遂行能力の把握
- 組織の能力レベル把握・人材ポートフォリオ作成
- 求人と応募者のマッチ度把握

（出典）　情報セキュリティ教育事業者連絡会（ISEPA）
セキュリティ業務を担う人材のスキル可視化施策の考察～プラス・セキュリティ人材の可視化に向けて～＜1.0版＞
（2019年10月30日掲載）
https://www.jnsa.org/isepa/images/outputs/JTAGreport2019.pdf

（参考）NISC「普及啓発・人材育成ポータルサイト」の活用イメージ

○人材のマッチングに当たって必要な「スキルの共通言語化ツール」といった基礎的マテリアルに加え、特にこれまであまりみられなかった新たな流動モードに関する好事例の収集を行い、当面、関係省庁との連携の下、NISC「普及啓発・人材育成ポータルサイト」を活用し、官民で行われる「プラス・セキュリティ」講座の掲載を行うことを検討。

＜「NISC普及啓発・人材育成ポータルサイト」への掲載事項（イメージ）＞

	政策課題１	政策課題２	政策課題３
基礎的マテリアル	・「手引き」 ・事例集【今後作成】	・「プラス・セキュリティ」モデルカリキュラムに関する資料	・スキル等の共通言語化ツール （JTAG、ITSS+等）
先行事例	・DSIRT/SSIRT構築事例	・「プラス・セキュリティ」講座	・新たな流動モード事例

参考資料１

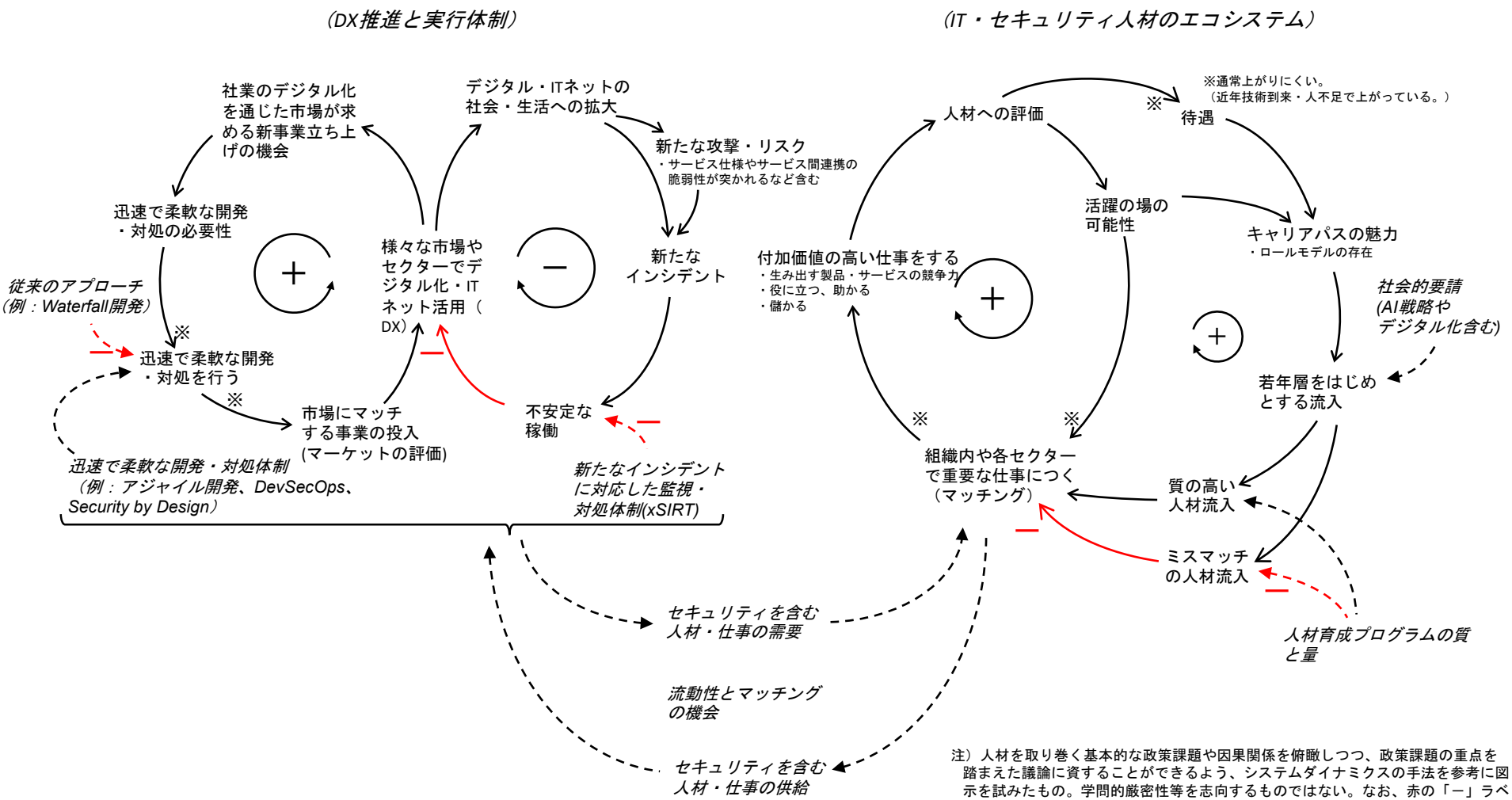
政策議論のための補助フレームワーク

サイバーセキュリティに係る人材の確保、育成、活躍の促進

（政策議論のための補助フレームワーク）

DX with Cybersecurity の推進

（日本でDXが進み、セキュリティが保たれること、あるいは同時推進）



注）人材を取り巻く基本的な政策課題や因果関係を俯瞰しつつ、政策課題の重点を踏まえた議論に資することができるよう、システムダイナミクスの手法を参考に図示を試みたもの。学問的厳密性等を志向するものではない。なお、赤の「－」ラベルの矢印は負の因果関係を示す。また、「＋」とあるループは正のフィードバックループまたは増強ループ、「－」は負のフィードバックループまたは平衡ループと呼ばれる。「※」は因果に複雑さや遠さが含まれる関係を試みに示し、点線はループの外からの入力をイメージしている。

（参考１）

従来の構図

○ ユーザ企業にとってITは人ごとで丸投げ

○ 丸投げを受けるベンダーと多重下請け構造

- ー 社内のシステム・ソフト
- ー 会社・部門毎のカスタマイズや複雑化したシステムの維持
- ー 付加価値が高くない
- ー 下請けの専門人材が人月工数で仕事
- ー ユーザ企業の内部にノウハウが蓄積しにくい

○ メンバーシップ型雇用

DXを実現する構図
（＝図のサイクルを回す構図）

○ ユーザ企業の主体的なIT活用とDX実施

○ ユーザ企業の主体性と専門ベンダーを使う意識

- ー 社業を担い顧客価値を生み出すシステム・ソフト
- ー 事業（社業）の自社ならではの基幹部分のコンピテンシーをシステム・ソフトで実現
- ー 付加価値が高い
- ー 専門人材の能力発揮
- ー 蓄積したノウハウを活かし更に発展・改善

○ ジョブ型雇用

鍵と考えられるもの

・ユーザ企業におけるIT・セキュリティ人材の活躍　（前ページの推進）

・ユーザ企業においてDX経営・事業を担う者が「＋IT」「＋セキュリティ」知識を補充できる環境　（併せて推進する必要あり）

（参考２）

○なぜサイバーセキュリティ政策の観点からも、DX推進を重視するのか。

・重要かつ構造的な政策課題（ユーザ企業における人材不足や次世代にとってのキャリアの魅力等）をwin-winで解決できる可能性があるため。

・相当数の企業は、それぞれが置かれた競争環境やウィズコロナでDXを進めると考えられ、何にせよ、DXに伴うセキュリティ政策課題を検討する必要があるため。

・業界や業界内によってDXの進展に差が出ると、セキュリティの差になり得るが、サイバーセキュリティ政策上、それは望ましくないため。（攻撃者は弱いところを狙うため）

サイバーセキュリティに係る人材の確保、育成、活躍の促進

（政策議論のための補助フレームワーク）
※経営層・戦略マネジメント層を加えた全体像と政策インプット

DX with Cybersecurity の推進

経営層

【経産省】
・サイバーセキュリティ経営ガイドライン（2017,ver.2.0）
＋ガイドライン実践のためのプラクティス（2020.6）
＋ガイドライン実践状況の可視化ツール（2020.3, β版）

「＋IT」「＋セキュリティ」知識

戦略マネジメント層

戦略マネジメント層の育成・定着

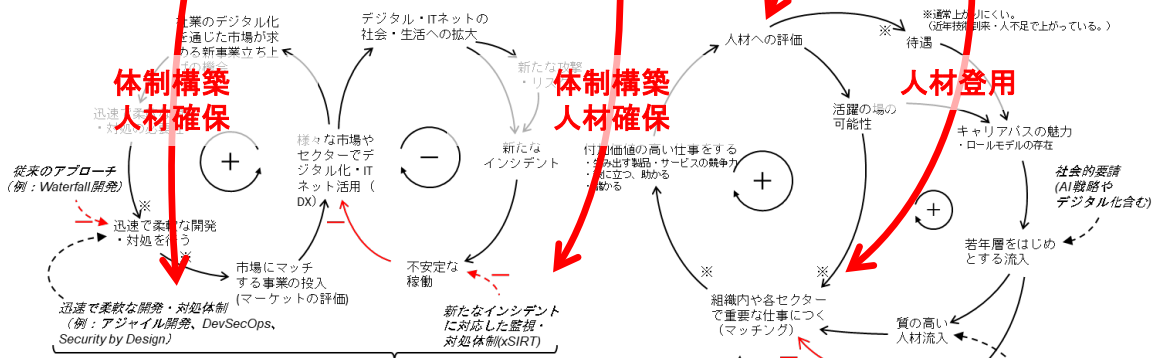
【経産省】
・戦略マネジメント層育成教育
2018～
IPA産業サイバーセキュリティセンター（ICSCoE）
東京工業大学CUMOT

評価

体制構築
人材確保

体制構築
人材確保

人材登用



実務者層・技術者層

【経産省】
・セキュリティ人材活躍モデルの構築（役割定義の共通言語化等）
・情報処理安全確保支援士（登録セキスペ）制度

・各省が施策を実施

参考資料２

「サイバーセキュリティに係る人材の確保、育成、活躍の促進に係る政策課題の当面の検討の進め方について」

（令和2年7月31日 普及啓発・人材育成専門調査会会長）

サイバーセキュリティに係る人材の確保、育成、活躍の促進に係る政策課題の 当面の検討の進め方について

令和２年７月３１日
普及啓発・人材育成専門調査会会長

１．趣旨

● デジタルトランスフォーメーション（DX）の進展が予想される中、DXと同時にサイバーセキュリティ対策を組み込んでいくこと（DX with Cybersecurity）が求められている。また、新型コロナウイルス感染症への対応を契機に、新たなデジタル技術の活用は更に重要になってくると考えられる。こうした中、新たなサイバーセキュリティ戦略の策定を見据え、この１年、本専門調査会において、DX時代におけるサイバーセキュリティ人材の確保、育成、活躍の促進に係る政策課題について検討を進めることが重要と考える。

● これまでの本部会合や本専門調査会の議論を踏まえつつ、主な政策課題を事務局と抽出してきたところ、現時点で以下の３つが挙げられる。当面、これらについて、本専門調査会での議論・検討を深めたい。それ以外の課題が抽出されれば、随時あるいは合わせて議論・検討を行うこととする。

２．検討を深めるべき主な政策課題

● サイバーセキュリティ確保のための新たな開発・監視・対処体制の構築
　DXでは、セキュリティを組み込んだ迅速で柔軟な事業・製品・サービスの開発体制が必要になるとともに、デジタル化やIT・ネット活用の社会・生活への拡大に伴う新たなインシデントへの対応が求められると考えられる。そこで、この新たな開発体制や監視・対処体制の構築や普及に向けた方策について検討する。

【アドバイザ委員：鎌田委員、蔵本委員】

● DXに必要な「プラス・セキュリティ」知識を補充できる環境・人材育成の推進
　DXでは、ユーザ企業の主体的なIT活用とDX実施が必要になると考えられる。そこで、DXに関わる経営・事業を担う者が「プラス・セキュリティ」知識を補充できる環境や人材育成を推進するための方策について検討する。

【アドバイザ委員：藤本委員、三浦委員】

● サイバーセキュリティ人材の活躍の促進に向けた流動性とマッチングの機会の促進
　様々な分野で DX with Securityの進展が予想される一方、いわゆるユーザ企業においてIT・セキュリティ人材が不足し、ベンダー、大企業、都市圏に偏重しているとの指摘がある。セキュリティ人材の活躍の場を広げ、キャリアパスの魅力を高めるとともに、流動性とマッチングの機会が促進されるための方策について検討する。

【アドバイザ委員：志済委員、下村委員】

※アドバイザ委員：政策課題の検討を深めるため、事務局が行う専門調査会の資料等の準備やとりまとめ草案作成への協力・助言、外部専門家を交えた予備的な議論への参画等の役割を担い、専門調査会での議論・検討を促進する。