NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

SecBoKを活用したセキュリティ人材スキル可視化ガイドラインの紹介

持田 啓司
株式会社ラック／ISEPA・教育部会

§1「SecBoK2018概要」

スキル中心からタスク・ロールとの連携強化へ

NPO日本ネットワークセキュリティ協会 教育部会
SecBoK2018改訂委員会

１．SecBoK2017の活用・普及状況

SecBoKの活用状況（産・学・官）（１）

- 産業界
  - 企業における活用
    - 例：みずほフィナンシャルグループ（日経コンピュータ2017年3月16日号）
    - 他にも複数社あり
- 教育界
  - 情報系大学
    - コンピュータサイエンス授業のカリキュラム体系雛形である「J17」との連携

    「情報学を専門とする学科対象の教育カリキュラム標準の策定及び提言Cyber Security(CyS)」
    http://www.mext.go.jp/a_menu/koutou/itaku/__icsFiles/afieldfile/2018/07/30/1407590_2.pdf
  - enPiT-PRO Security
    - 社会人学び直しプロジェクトのカリキュラム体系とSecBoKが連携

    http://www.seccap.pro/#overview
  - 国立高等専門学校機構
    - 高専での取り組みである情報セキュリティ人材育成事業(K-SEC)とJNSAによる産学連携

    https://csinfo2018.kochi-ct.ac.jp/index.html

SecBoKの活用状況（産・学・官）（２）

- 行政機関
  - 文部科学省
    - 2017年6月に公表した高等教育機関向けモデル・コア・カリキュラムにおいて、産業界で用いられる指標との対応として、SecBoK及び産業横断サイバーセキュリティ人材育成検討会の人材定義リファレスとの対応関係を整理

    http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2017/06/19/1386824_001.pdf

  - 独立行政法人情報処理推進機構（IPA）
    - ITSS+（セキュリティ分野）の13種類の専門分野の策定にあたり、SecBoK及び日本シーサート協議会による役割定義との対応関係に配慮

  - 独立行政法人国際協力機構（JICA）
    - 海外国立大学でのセキュリティ専攻用のカリキュラム対系に、SecBoKを利用したいための協力要請あり

SecBoK2017での課題

- 役割定義が網羅的でない
  - 「不足感のある役割を先行的に整備」という趣旨が理解されず、“偏っている”という意見もあった
    - 「開発系のセキュリティ対策は不要なのか」など
- 知識・スキル項目がNICEフレームワークの直訳
  - NICEフレームワークとの互換性を狙っているが、利用者から見るとわかりにくいとの指摘もあり
    - NICEフレームワークの項目とSecBoK独自性の見極め
  - NICEフレームワークの課題をそのまま受け継いでいる
    - 米国における軍と政府機関で用いられているものを集めて作成しているため、役割定義やタスクや知識・スキルがMECEでなく、内容が重複していると思われる項目も多数ある
    - 用語の不統一も複数見られる

セキュリティ現場が直面している課題

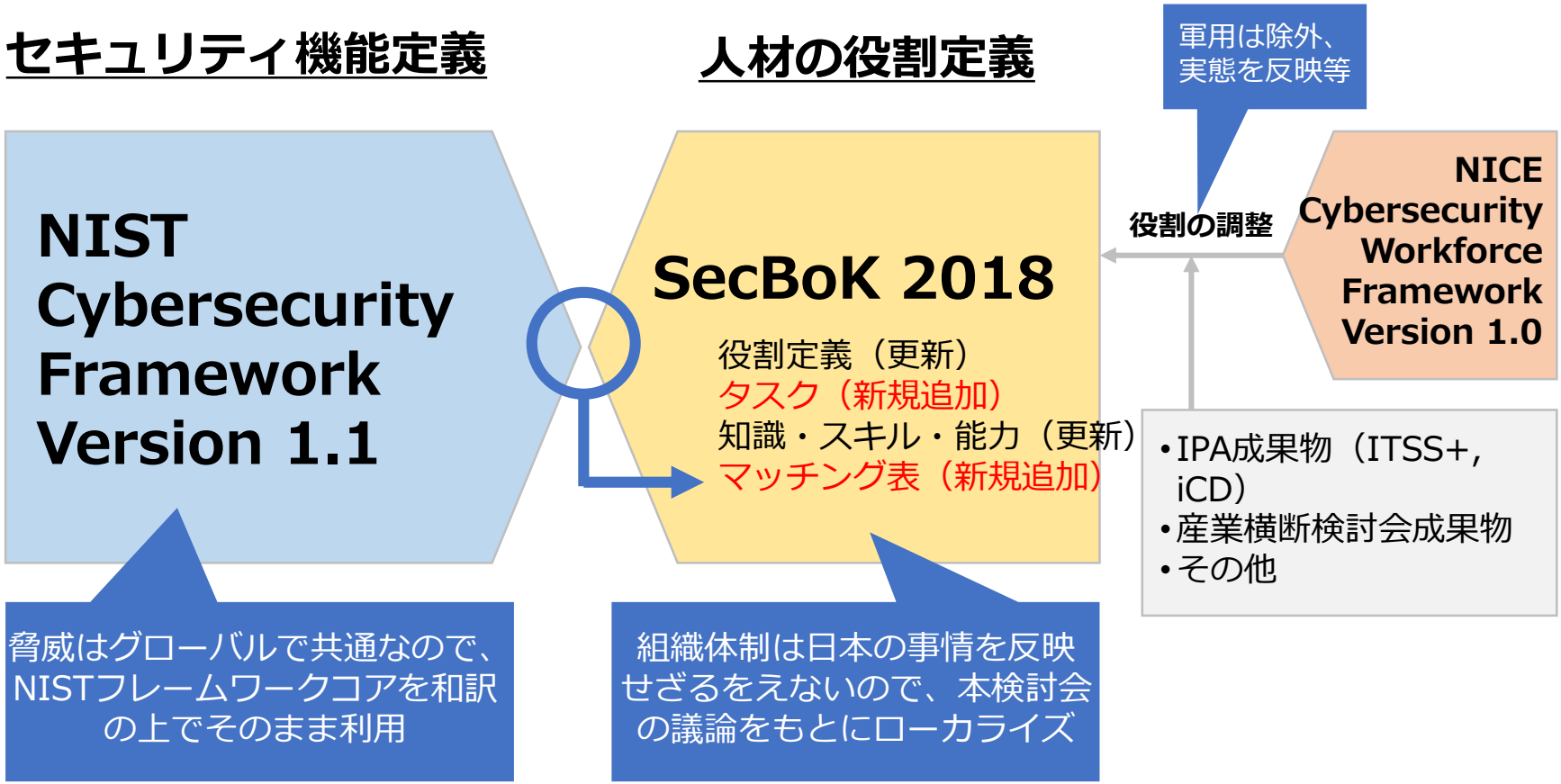
- 情報システム部門に丸投げできなくなりつつある
  - 現場事業部門が直接ベンダに委託
  - クラウド移行で情シス部門が縮小、余力がなくなっている
- 「セキュリティ人材」の多様化
  - もはや「セキュリティスペシャリスト」的な人材だけ育成すればよいわけではない
  - サイバーセキュリティに関する事業リスクをマネジメントできる人材（NISC）
- 体制は企業によってまちまち
  - SecBoKでもITSS+でも、そのまま取り込めない企業が多い
- 役割定義をそのままこなせる人材がいない
  - 「チームで対応」という建前の組織が多いが、チーム内で適切なコミュニケーションが成立しないと、１人の代替にはならない

２．改訂の方向案

NICE Cybersecurity Workforce Framework

- NIST SP800-181として標準化（2017年8月）
  - 旧版はパンフレットのような様式の文書しかなかった
  - Excel版もリリース（2018年1月）
- ７カテゴリのタスクとスキルを網羅
  - 旧版では分析（Analyze）と収集と運用（Collect & Operate）の両カテゴリについては「独自かつ高度に特殊」という理由で提供されず
  - 用語が整理された（information assurance → cybersecurity 等）
- 専門領域の整理
  - 政府機関や民間サービスにおけるサイバーセキュリティに関する役割（Work Role）を52種類定義し、それぞれのタスクとタスクをこなす上で必要となる知識・スキル・能力（KSA）を整理

SecBoK2018改訂の方法性
セキュリティ機能定義と役割定義の分析



3．SecBoK2018概要

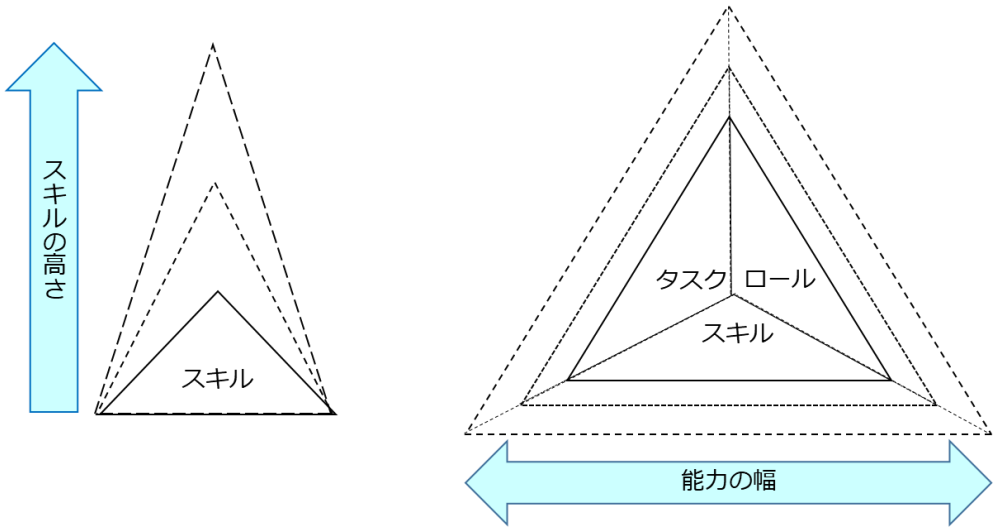
セキュリティ人材育成の考え方の変化
スキル中心からタスク・ロールとの連携強化へ

従来の考え方

セキュリティスキルの習得こそがセキュリティ人材の育成につながるとの考えより、セキュリティスキル向上の施策が次々と実施

新たな考え方

Society5.0などのITを利活用して社会を変えようとの時代の流れにおいては、セキュリティスキルの習得が目的ではなく、何ができるというタスクの考え方が必要



左図は従来のスキル育成中心のイメージであるが、近年は右図のように三角形全体が大きくなるように**スキル・タスク・ロール**の幅が広がる育成が必要となる

SecBoK2018の特長（１）
NIST SP800-181との連携１

NIST SP800-181の約1000強のスキル項目とSecBoK2018の16ロールとの連携を実施

役割（ロール）

スキル項目

セキュリティ知識分野（SecBoK）人材スキルマップ2018年版 全体整理表

<ロール毎の必須知識・スキル>

1 前提スキル（職務遂行の前提として有しておくべき知識・スキル）
2 必須スキル（職務遂行の実施に際して必要となる知識・スキル）
3 参考スキル（職務遂行に際して必須ではないが、あると望ましい知識・スキル）
※「前提スキル」と「必須スキル」の関係
前提スキルを有する人材を確保し、必須スキルに関する教育・トレーニングを行うと、当該職務を担うことができる人材となる

<知識・スキルのレベル>

L 低（概ね経験3年未満でも対応可能）
M 中（経験3年以上または関連する演習・トレーニング受講者なら対応可能）
H 高（経験10年以上または高度な研修受講を前提とする専門実務経験者または「突出した人材」なら対応可能）
P ペンティング（情報収集・インテリジェンスに関するもの。今回はレベル付けの対象外）

	KSA-ID	新旧別	旧ID	分野	大項目	中項目	レベル	小項目	CISO	POC	ノーティフィケーション	コマンダー、トリアージ	インシデントマネージャー、インシデントハンドラー	キュレーター	リサーチャー	セルフアセスメント・ソリューションアナリスト	脆弱性診断士	教育・啓発	フォレンジックエンジニア	インベスティゲーター	リーガルアドバイザー	IT企画部門	ITシステム部門	情報セキュリティ監査人
1	K0052	旧NICEに類似項あり	75	00基礎	1数物情報学		L	数学に関する知識（例：対数、三角法、線形代数、微積分、統計、操作解析）								3								
2	K0030	旧NICEに類似項あり	42	00基礎	2計算機・通信工学		L	コンピュータアーキテクチャ（例：回路基板、プロセッサ、チップ及びコンピュータハードウェア）に適用される電気工学に関する知識																	
3	K0036	旧NICEと同一	52	00基礎	2計算機・通信工学		L	マンマシンインタラクションの原理に関する知識						1		1								
4	K0055	旧NICEと同一	78	00基礎	2計算機・通信工学		L	マイクロプロセッサに関する知識																
5	K0061	旧NICEとほぼ同一	92	00基礎	2計算機・通信工学		L	ネットワーク上でトラフィックがどのように流れるか（例： TCP/IP、OSI、ITIL現行版）に関する知識	2		1		1		1	1	1		1				1	
6	K0108	旧NICEに類似項あり	261	00基礎	2計算機・通信工学		L	通信メディアの基本概念、用語及び幅広い範囲での運用に関する知識（コンピュータと電話のネットワーク、衛星、ファイバ、無線）						3									1	
7	K0109	旧NICEに類似項あり	264	00基礎	2計算機・通信工学		L	多様な構成要素と周辺機器の機能を含む、物理的なコンピュータの構成要素とアーキテクチャに関する知識（例：CPU、ネットワークインターフェースカード、データストレージ）の機能を含む、物理的なコンピュータコンポーネントとアーキテクチャに関する知識						1	1			1	1					
8	K0113	旧NICEとほぼ同一	278	00基礎	2計算機・通信工学		L	さまざまな種類のネットワーク通信に関する知識（例：LAN、WAN、MAN、WLAN、WWAN）		2		1	1	1	1								1	
9	K0114	旧NICEとほぼ同一	281	00基礎	2計算機・通信工学		L	電子デバイスに関する知識（例：コンピュータシステム/コンポーネント、アクセス制御デバイス、デジタルカメラ、デジタルスキャナ、電子オーガナイザ、ハードドライブ、メモリカード、モデム、ネットワークコンポーネント、ネットワークアプライアンス、ネットワークホームコントロールデバイス、プリンタ、リムーバブルストレージデバイス、電話機、複写機、ファクシミリなど）											3					
10	K0138	旧NICEに類似項あり	903	00基礎	2計算機・通信工学		L	Wi-Fiに関する知識				1	1			1							1	
11	K0395	旧NICEとほぼ同一	22	00基礎	2計算機・通信工学		L	コンピュータネットワークの基礎に関する知識（ネットワークの基本的なコンピュータコンポーネント、ネットワークの種類など）						1	1		1		1					1
12	K0491	新規	—	00基礎	2計算機・通信工学		L	ネットワークとインターネット通信に関する知識（すなわち、デバイス、デバイス構成、ハードウェア、ソフトウェア、アプリケーション、ポート/プロトコル、アドレッシング、ネットワークアーキテクチャとインフラストラクチャ、ルーティング、オペレーティングシステムなど）					1	1	1	1	1		1				1	1	1
13	K0516	新規	—	00基礎	2計算機・通信工学		L	ハブ、スイッチ、ルータ、ファイアウォールなどを含む物理的および論理的なネットワークデバイスおよびインフラストラクチャに関する知識					1	1	1	1	1		1			1	1	1
14	K0555	新規	—	00基礎	2計算機・通信工学		L	TCP/IPネットワーキングプロトコルに関する知識					1	1	1	1	1		1			1	1	1
15	K0556	新規	—	00基礎	2計算機・通信工学		L	通信の基礎に関する知識					1	1	1	1	1		1			1	1	1
16	K0015	旧NICEと同一	21	00基礎	3ソフトウェア		L	計算機アルゴリズムに関する知識						1	1	1	1		1					
17	K0016	旧NICEに類似項あり	23	00基礎	3ソフトウェア		L	コンピュータプログラミングの原則に関する知識						1	1	1	1		1					
18	K0060	旧NICEと同一	90	00基礎	3ソフトウェア		L	オペレーティングシステムに関する知識			2	1	1	1	1	1	1	1	1					1
19	K0068	旧NICEと同一	102	00基礎	3ソフトウェア		L	プログラミング言語の構造とロジックに関する知識						1	1	1	1		1					

SecBoK2018の特長（１）
NIST SP800-181との連携２

	役割（ロール）	役割定義（ユーザ企業におけるおもな役割）	NICE定義のロール名		NICEにおけるロールの定義
1	CISO（最高情報セキュリティ責任者）	社内の情報セキュリティを統括する。セキュリティ確保の観点から、CIO（最高情報セキュリティ責任者）、CFO（最高財務責任者）と必要に応じて対峙する。	1	許可権限者	組織の業務（ミッション、機能、イメージ、評判を含む）、組織資産、個人、その他の組織、国家に許容可能なレベルで情報システムを運用する責任を正式に負う権限を持つ上級管理職または役員。
			27	幹部のサイバーリーダシップ	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
			31	IT投資/ポートフォリオ管理者	ミッションと企業の優先度に関する全体的なニーズに合わせたIT投資のポートフォリオを管理する。
2	POC（Point of Contact）	社外向けではJPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口、社内向けではIT部門調整担当社内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、それぞれ情報連携を行う。		（対応ロールなし）	
3	ノーティフィケーション	組織内を調整し、社内各関連部署への情報発信を行う。社内システムに影響を及ぼす場合にはIT部門と調整を行う。		（対応ロールなし）	
4	コマンダー	自社で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関してはCISOや経営層との情報連携を行う。また、CISOや経営者が意思決定する際の支援を行う。	27	幹部のサイバーリーダシップ	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
4	トリアージ	事象に対する対応における優先順位を決定する。	27	幹部のサイバーリーダシップ	組織のサイバーおよびサイバー関連の資源及び/又は運用に関する意思決定を行うとともに、ビジョンと方向性を確立する。
5	インシデントマネージャー	インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。	35	防衛インシデント対応者	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
5	インシデントハンドラー	インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。	35	防衛インシデント対応者	ネットワーク環境またはエンクレーブ内のサイバーインシデントを調査、分析、および対応する。
6	キュレーター	リサーチャーの収集した情報を分析し、その情報を自社に適用すべきかの選定を行う。リサーチャーと合わせてSOC（セキュリティオペレーションセンター）とすることが多い。	37	脅威/警告アナリスト	高度にダイナミックなオペレーティング環境の状況を把握するためのサイバー指標を開発する。サイバー脅威/警告評価を収集、処理、分析、および普及させる。
7	リサーチャー	セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。収集のみで分析はしない。	33	サイバー防衛アナリスト	さまざまなサイバー防御ツール（IDSのアラート、ファイアウォール、ネットワークトラフィックログなど）から収集したデータを使用して、脅威を緩和する目的で環境内で発生するイベントを分析する。
8	セルフアセスメント	自社の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とTobe像のFit&Gapからリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、改善計画に反映する。	18	システムセキュリティアナリスト	システムセキュリティの統合、テスト、運用、保守の分析と開発を担当する。
8	ソリューションアナリスト	平常時にはリスクアセスメントを行う。インシデント対応時には脆弱性の分析、影響の調査等に対応する。	18	システムセキュリティアナリスト	システムセキュリティの統合、テスト、運用、保守の分析と開発を担当する。
9	脆弱性診断士	ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。	36	脆弱性診断アナリスト	ネットワーク環境内のシステムとネットワークの評価を実施し、それらのシステム/ネットワークが受け入れ可能な構成、特殊又はローカルなポリシーから逸脱している場所を特定する。既知の脆弱性に対する多層防御アーキテクチャの有効性を評価する。
10	教育・啓発	社内のリテラシーの向上、底上げのための教育及び啓発活動を行う。	21	サイバー教育カリキュラム開発者	教育上の必要に基づき、サイバーセキュリティを対象とする訓練・教育に関するコース、手法及び技術について開発、立案、調整及び評価する。
			22	サイバーセキュリティインストラクター	サイバーセキュリティ領域における要員の訓練または教育を開発及び主導する。
			25	サイバーセキュリティ要員の育成者・管	サイバー空間の人材、人材、訓練、教育の要件をサポートし、サイバー関連のポリシー、原則、教材、編成、教育訓練の要件に対する変化を扱うためのサイバー空間を対象とする労働力の計画、戦略、指針を開発する。
11	フォレンジックエンジニア	システム的な鑑識、精密検査、解析、報告を行う。悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。	51	法執行フォレンジックアナリスト	サイバー侵入事件に関連するデジタルメディアとログを含めるために、ドキュメンタリーまたは物理的証拠を確立するコンピュータベースの犯罪に関する詳細な調査を実施する。
			52	防衛フォレンジックアナリスト	デジタル証拠を分析し、コンピュータセキュリティインシデントを調査し、システム/ネットワークの脆弱性緩和を支援する有益な情報を導き出す。
12	インベスティゲーター	外部からの犯罪、内部犯罪を捜査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象を絞っていくことが要求される。	50	サイバー犯罪捜査員	制御され、文書化された分析および調査技術を使用して、証拠を特定、収集、調査、および保存する。
13	リーガルアドバイザー	システムにおいてコンプライアンス及び法的観点から遵守すべき内容に関する橋渡しを行う。	19	サイバーリーガルアドバイザー	サイバー法に関するトピックについて、法的な助言や勧告を行う。
14	ＩＴ企画部門	社内のIT利用に関する企画・立案を行う。必要に応じて、ITの利用状況の調査・分析等を行う。	26	サイバーセキュリティ対策方針・戦略の	組織のサイバーセキュリティに関するイニシアチブおよび規制遵守をサポートし、それと整合するようなサイバーセキュリティ計画、戦略、およびポリシーを策定し維持する。
			29	ITプロジェクトマネージャー	情報技術関連プロジェクトを直接管理する。
15	ITシステム部門	社内のITプロジェクトを推進するとともに、アプリケーションシステムの設計、構築、運用、保守等を担当する。	16	ネットワーク運用スペシャリスト	ハードウェアおよび仮想環境を含む、ネットワークサービス/システムの計画、実装、および運用を行う。
			17	システムアドミニストレータ	システムまたはシステムにおける特定のコンポーネントの設定および保守（例：ハードウェアおよびソフトウェアのインストール、構成、更新、ユーザーアカウントの確立および管理、バックアップおよびリカバリタスクの監督または実施、運用上および技術上のセキュリティ管理の実装、組織のセキュリティポリシーと手順への準拠）に関する責任を負う。
			23	情報システムセキュリティ管理者	プログラム、組織、システム等におけるサイバーセキュリティ対策に責任を負う。
			24	通信セキュリティ管理者	組織の通信リソースまたは暗号鍵管理システムの鍵を管理する。
			34	サイバー防衛インフラサポートスペシャ	インフラストラクチャのハードウェアとソフトウェアをテスト、実装、展開、保守、管理する。
16	情報セキュリティ監査人	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。	32	ITプログラム監査者	標準への準拠状況を判断するため、ITプログラムまたはその個々の構成要素を評価する。

NIST SP800-181の52ロールのうち、関連のあるロールをピックアップし、SecBoK2018の16ロールとの連携を実施

SecBoK2018の特長（２）
NISTサイバーセキュリティフレームワーク(CSF)との連携

機能の一意の識別子	機能
ID	特定 (Identify)
PR	防御 (Protect)
DE	検知 (Detect)
RS	対応 (Respond)
RC	復旧 (Recover)

業務遂行能力(タスク)と知識項目との連携を新たに提示

下記は、検知（DE）の一例

知識（スキル）項目

			基礎	セキュリティ基礎	セキュリティガバナンス	セキュリティマネジメント	セキュリティネットワーク	セキュリティシステム	セキュアシステム設計構築	セキュリティ運用	暗号・認証・署名	サイバー攻撃手法	情報収集インテリジェンス	デジタルフォレンジクス	サイバー捜査	セキュリティ人材育成	法・制度・準標	関連領域（Hは無 ICT	工学	ビジネス
検知（DE）	異常とイベント（DE.AE）：異常な活動を検知し、イベントがもたらす可能性のある影響を把握している。	DE.AE-1：ネットワーク運用のベースラインと、ユーザとシステム間の予測されるデータの流れを特定し、管理している。	●	●		L	H			M	L	M					L	L		
		DE.AE-2：攻撃の標的と手法を理解するために、検知したイベントを分析している。	●	●		L	H	H	M	H	M	H		L	L		L	L	L	L
		DE.AE-3：イベントデータを複数の情報源やセンサーから収集し、相互に関連付けている。	●	●		L	H	M	M	H	M	H		L	L		L	L	L	L
		DE.AE-4：イベントがもたらす影響を特定している。	●	●		L	H	H	H	H	M	H		L	L		L	L	L	L
		DE.AE-5：インシデント警告の閾値を定めている。	●	●	L	M	H	H	M	H	M	H		L	L		M	L	L	M
	セキュリティの継続的なモニタリング（DE.CM）：サイバーセキュリティイベントを検知し、保護対策の有効性を検証するために、情報システムと資産をモニタリングしている。	DE.CM-1：発生する可能性のあるサイバーセキュリティイベントを検知できるよう、ネットワークをモニタリングしている。	●	●		L	M	M		M		H						L		L
		DE.CM-2：発生する可能性のあるサイバーセキュリティイベントを検知できるよう、物理環境をモニタリングしている。	●	●		L	M	M		M		H						L		L
		DE.CM-3：発生する可能性のあるサイバーセキュリティイベントを検知できるよう、個人の活動をモニタリングしている。	●	●		L	M	M		M		M		L	L			L	L	M
		DE.CM-4：悪質なコードを検出できる。	●	●			H	H		M		H		L	L			L	L	L
		DE.CM-5：悪質なモバイルコードを検出できる。	●	●			H	H		M		H		L	L			L	L	L
		DE.CM-6：発生する可能性のあるサイバーセキュリティイベントを検知できるよう、外部サービスプロバイダの活動をモニタリングしている。	●	●		M	M	L		H		H						L	L	L
		DE.CM-7：権限のない従業員、接続、デバイス、ソフトウェアのモニタリングを実施している。	●	●		M	L	L		H		M		L	L			L	L	L
		DE.CM-8：脆弱性スキャンを実施している。	●	●			M	M		M		H		L				L	L	
	検知プロセス（DE.DP）：異常なイベントを検知するための検知プロセスおよび手順を維持し、テストしている。	DE.DP-1：説明責任を果たせるよう、検知に関する役割と責任を明確に定義している。	●	●	L	H	M	M	L	H	L	H		L			M	L	L	L
		DE.DP-2：検知活動は必要なすべての要求事項を満たしている。	●	●		H				H		H		L			M	L	L	L
		DE.DP-3：検知プロセスをテストしている。	●	●		M	H	H	M	H	L	H		L			M	L	L	L
		DE.DP-4：イベント検知情報を伝達している。	●	●	L	H				M		M					L	L	L	M
		DE.DP-5：検知プロセスを継続的に改善している。	●	●		H				M		M					L	L	L	M

SecBoK2018の特長（３）

参考資料：NICEが定める人材とタスクの一覧

NICE（NIST SP800-181）が定める各ロールを担う人材が行うべきタスクの一覧を日本語化し公開

システムアーキテクチャ Systems Architecture (ARC)	SP-ARC-001 エンタープライズアーキテクト Enterprise Architect	T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、適切なフェールオーバー/代替サイト要件、バックアップ要件、システム復旧/復元のためのマテリアルサポート性要件を含む適切な災害復旧と運用要件の継続性を、システム要件が確実に識別するようにする。
		T0084	安全な構成管理プロセスを採用する。
		T0090	取得または開発されたシステムとアーキテクチャが、組織のサイバーセキュリティアーキテクチャガイドラインと一貫していることを確認する。
		T0108	組織のステークホルダーと連携して重要なビジネス機能を特定し、優先順位を付ける。
		T0196	プロジェクト費用、設計コンセプト、または設計変更に関するアドバイスを提供する。
		T0205	リスク管理フレームワークのプロセス活動および関連する文書（例えば、システムライフサイクルサポート計画、運用の概念、運用手順、および保守トレーニング資料）を入力する。
		T0307	候補アーキテクチャの分析、セキュリティサービスの割り当て、セキュリティメカニズムの選択を行う。
		T0314	システムセキュリティコンテキスト、予備システムセキュリティコンセプト（CONOPS）を開発し、適用可能なサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義する。
		T0328	セキュリティアーキテクチャと設計を評価して、取得文書に含まれる要件に応じて提案または提供されるセキュリティ設計とアーキテクチャの妥当性を判断する。
		T0338	アーキテクチャ開発プロセスを記述する詳細な機能仕様を記述する。
		T0427	アーキテクチャを計画するためのユーザーのニーズと要件を分析する。
		T0440	致命的な障害イベントが発生した後、システムの一部または全部を復旧するために必要なシステム機能やビジネス機能をキャプチャして統合する。
		T0448	ユーザーのニーズを満たすために必要なエンタープライズアーキテクチャまたはシステムコンポーネントを開発する。
		T0473	必要に応じてすべての定義およびアーキテクチャ活動を文書化して更新する。
		T0517	セキュリティアーキテクチャのギャップの特定に関する結果を統合する。
		T0521	企業のコンポーネントを統合して整列させるための実装戦略を立てる。
		T0542	提案された機能を技術要件に変換する。
		T0555	システム間の新しいシステムまたは新しいインターフェースの実装が、セキュリティーの姿勢を含むがこれに限定されない現在の環境およびターゲット環境にどのように影響するかを文書化する。
		T0557	サイバースペースに関連するキー管理機能を統合する。
	SP-ARC-002 セキュリティアーキテクト Security Architect	T0050	致命的な障害イベントが発生した後、システムの一部または全部を復旧するために必要なシステム機能またはビジネス機能を定義し、優先順位を付ける。
		T0051	重要なシステム機能に基づいて適切なレベルのシステム可用性を定義し、適切なフェールオーバー/代替サイト要件、バックアップ要件、システム復旧/復元のためのマテリアルサポート性要件を含む適切な災害復旧と運用要件の継続性を、システム要件が確実に識別するようにする。
		T0071	主に政府組織に適用される複数の分類レベルのデータ（UNCLASSIFIED、SECRET、およびTOP SECRETなど）の処理のための、複数レベルのセキュリティ要件または要件を備えたシステムおよびネットワークのサイバーセキュリティ設計の開発/統合。
		T0082	取得ライフサイクル全体にわたる組織の情報セキュリティ、サイバーセキュリティアーキテクチャ、およびシステムセキュリティエンジニアリング要件の文書化と処理を行う。
		T0084	安全な構成管理プロセスを採用する。
		T0090	取得または開発されたシステムとアーキテクチャが、組織のサイバーセキュリティアーキテクチャガイドラインと一貫していることを確認する。
		T0108	組織のステークホルダーと連携して重要なビジネス機能を特定し、優先順位を付ける。
		T0177	セキュリティレビューを実行し、セキュリティアーキテクチャのギャップを特定し、セキュリティリスク管理計画を策定する。
		T0196	プロジェクト費用、設計コンセプト、または設計変更に関するアドバイスを提供する。
		T0203	業務声明やその他の適切な調達文書に含めるべきセキュリティ要件に関する情報を提供する。
		T0205	リスク管理フレームワークのプロセス活動および関連する文書（例えば、システムライフサイクルサポート計画、運用の概念、運用手順、および保守トレーニング資料）を入力する。
		T0268	新しいシステムの実装またはシステム間の新しいインターフェイスが現在の環境のセキュリティの姿勢にどのように影響するかを定義し、文書化する。
		T0307	候補アーキテクチャの分析、セキュリティサービスの割り当て、セキュリティメカニズムの選択を行う。
		T0314	システムセキュリティコンテキスト、予備システムセキュリティコンセプト（CONOPS）を開発し、適用可能なサイバーセキュリティ要件に従ってベースラインシステムセキュリティ要件を定義する。
		T0328	セキュリティアーキテクチャと設計を評価して、取得文書に含まれる要件に応じて提案または提供されるセキュリティ設計とアーキテクチャの妥当性を判断する。
		T0338	アーキテクチャ開発プロセスを記述する詳細な機能仕様を記述する。
		T0427	アーキテクチャを計画するためのユーザーのニーズと要件を分析する。
		T0448	ユーザーのニーズを満たすために必要なエンタープライズアーキテクチャまたはシステムコンポーネントを開発する。
		T0473	必要に応じてすべての定義およびアーキテクチャ活動を文書化して更新する。
		T0484	情報システムとネットワークおよび文書の保護ニーズ（すなわち、セキュリティ制御）を適切に決定する。
		T0542	提案された機能を技術要件に変換する。
		T0556	サイバースペースに関連するセキュリティ管理機能を評価し、設計する。

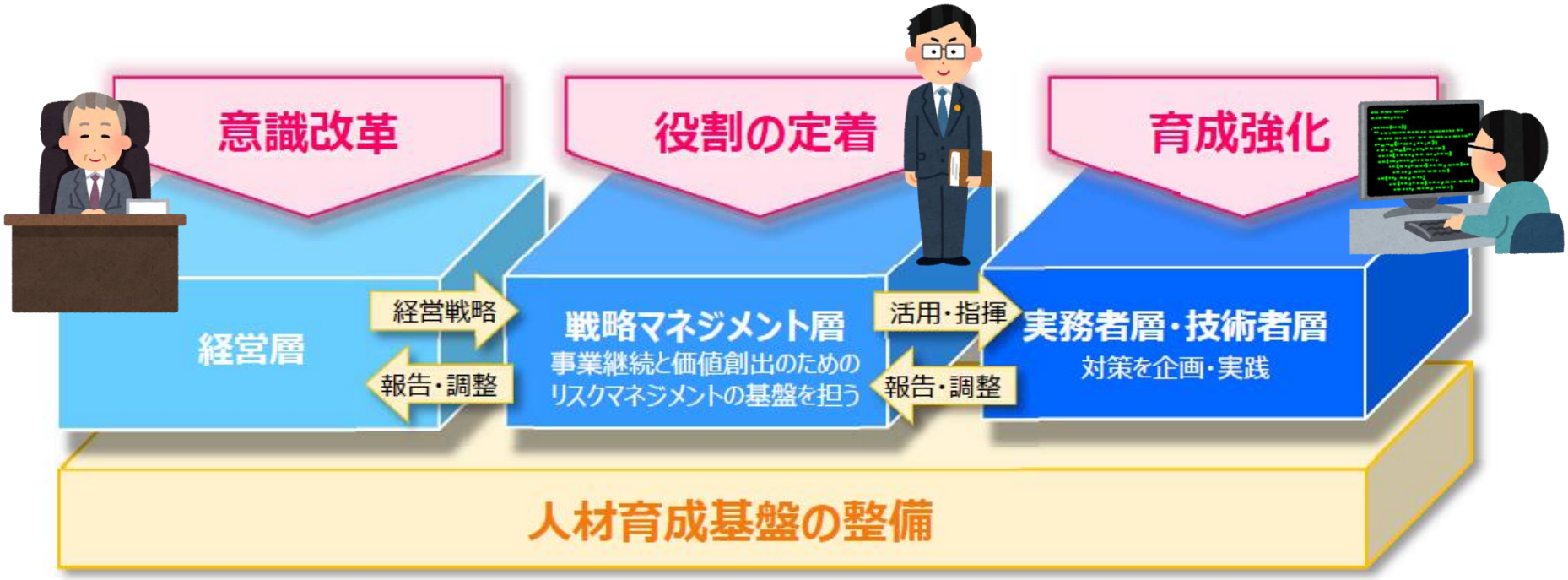
§2「セキュリティ人材の課題」

人材育成視点での現状の課題

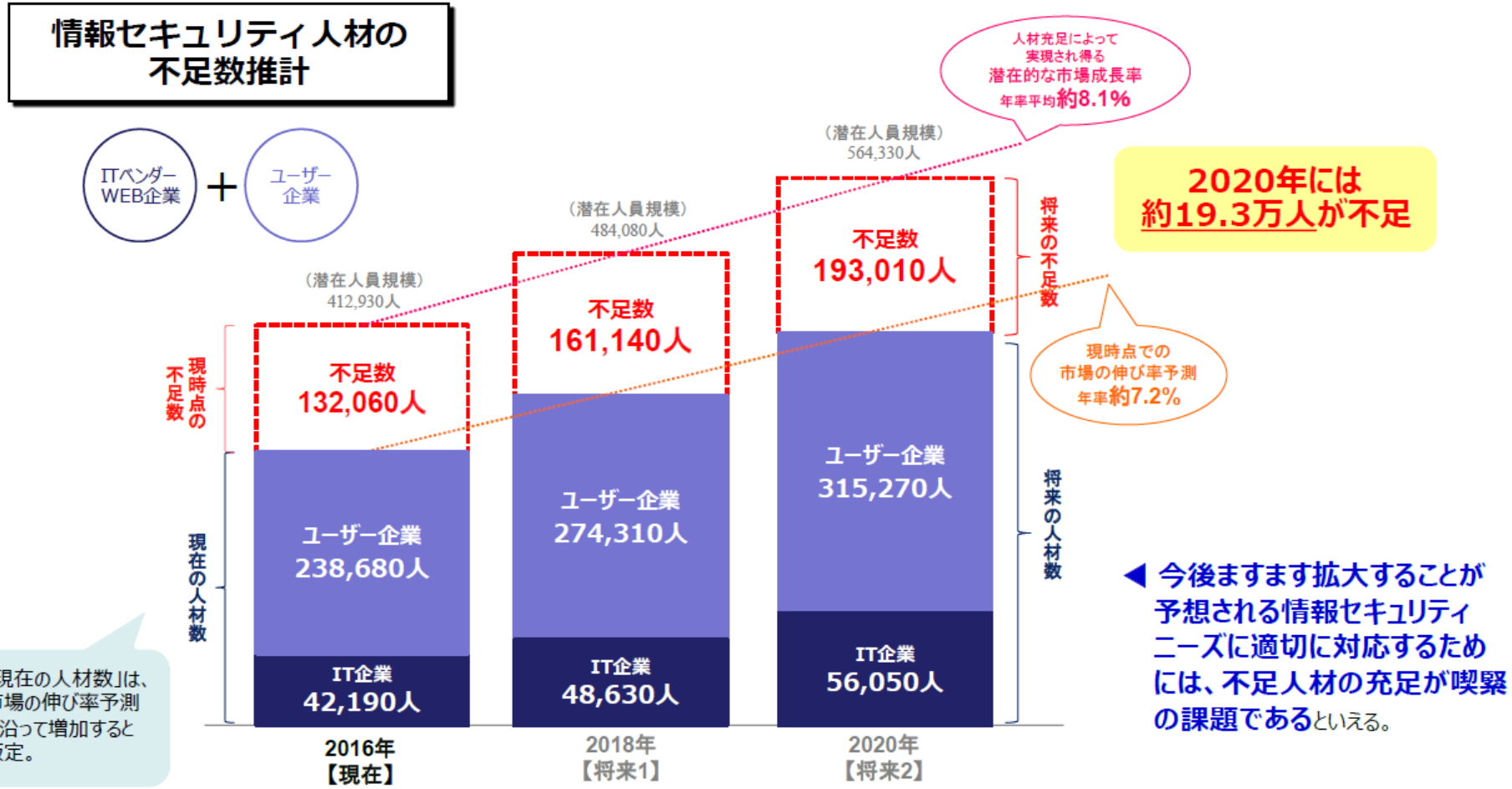
情報セキュリティ教育事業者連絡会（ISEPA）

叫ばれ続ける人材不足

- NISC サイバーセキュリティ戦略(閣議決定)
  平成30年7月27日
  - 各省庁施策で必要人材を育成
- しかし、ハイエンドな技術者育成が注目されがち



2020年には19万人が不足!?



出典：IT ベンチャー等によるイノベーション促進のための人材育成・確保モデル事業
事業報告書 第2部「今後のIT 人材需給推計モデル構築等 編」平成28年3月

不足数推計を逆算してみた

	現在 ＜2016年＞	将来1 ＜2018年＞	将来2 ＜2020年＞	2020年 不足数内訳
ITベンダー＋WEB企業	42,190	48,630	56,050	29,134
ユーザー企業	238,680	274,310	315,270	163,876
人材数合計（実在人材数）	280,870	322,940	371,320	―――
不足人材数	132,060	161,140	193,010	―――
潜在人員規模（必要人材数）	412,930	484,080	564,330	―――

■ ITベンダー＋WEB企業

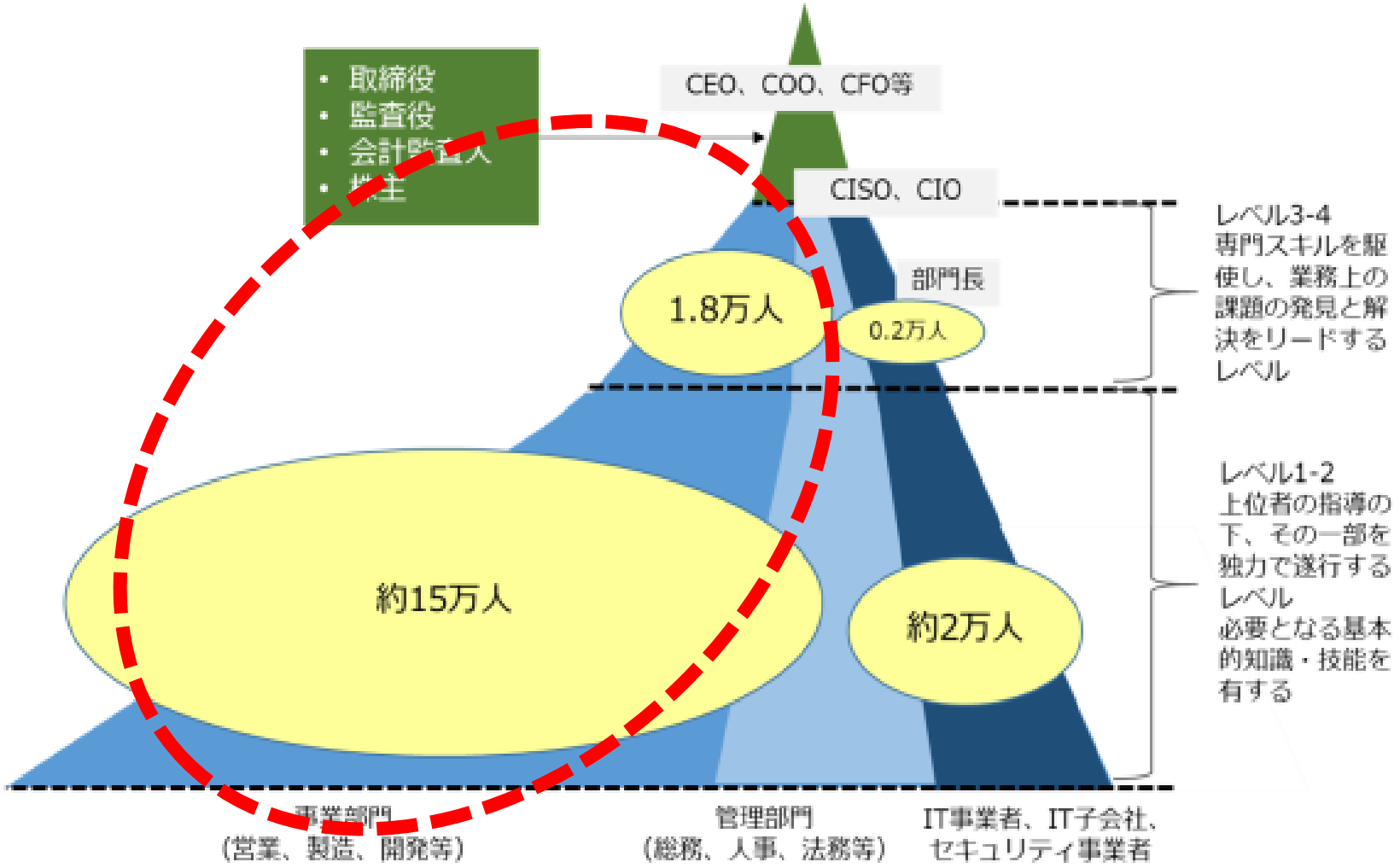
29,134人の 不足状況別内訳	危機的	無理すれば回る	理想には 不安	ちょうどよい	不要/不明
業務別平均	3.83%	14.30%	23.78%	21.97%	36.12%
換算率	0.5	0.3	0.2	0	0
換算不足見込み数	5,093	11,400	12,641	0	0

■ ユーザー企業

163,876人の 不足状況別内訳	危機的	無理すれば回る	理想には 不安	ちょうどよい	不要/不明
業務別平均	3.83%	14.30%	23.78%	21.97%	36.12%
換算率	0.5	0.3	0.2	0	0
換算不足見込み数	28,650	64,125	71,101	0	0

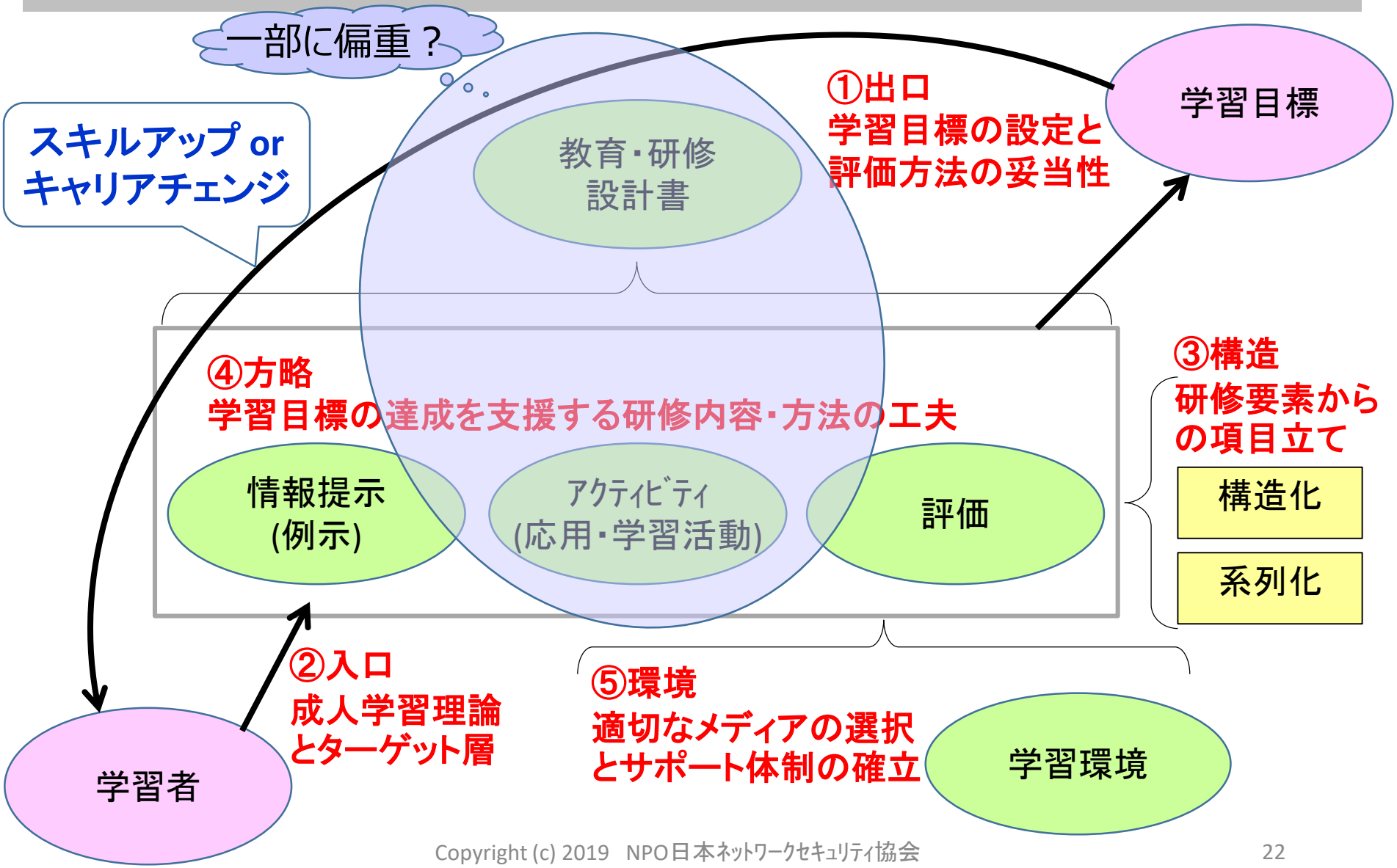
※ 報告書記載内容に基づいて持田が逆算したものですので正確ではありません。

不足推計イメージ



出典：JCICレポート「セキュリティ人材不足の真実と今なすべき対策とは」

ID視点の育成サイクルと現状課題



§3「課題解決のためのJTAG」

人材の現状調査とスキル可視化による課題解決の一考察

情報セキュリティ教育事業者連絡会（ISEPA）

関係事業者が垣根を超えて！ JTAG

- 競合の枠を超えて、国内事業者(J)がTAGを組み、セキュリティ人材の適切な育成、適職認定を行うことで、必要セキュリティ業務への適材適所の配置を行う。
  - 効率的な人材育成
    - スキル見える化と不足スキル学習
  - 必要業務の整理
    - 適材適所の明確化で適職への配置
  - 市場価値の認定
    - キャリアパス(育成・配置計画)、報酬への反映
- 参加企業数：52社

をJNSAが推進する意義

① 認定ツールによる実力の可視化で、業務遂行に不足するスキルの研修受講を促進

研修ニーズ拡大 ⇒ セキュリティ業務へのキャリアチェンジ支援 → 教育事業の売上アップ

② 人材育成施策の社会人対象領域の受け皿機能

学から産へのセキュリティ人材輩出増加 ⇒ 活躍の場拡大支援 → 業界への採用増加

③ 多様なスキルを一元的に把握できるタレントマネジメントツールとして活用

セキュリティ業務へのキャリアチェンジ増加 ⇒ 活躍の場拡大支援 → 業界への採用増加・社内適正評価

国の施策・社会全体のサイバーセキュリティを牽引する立場としての役割

JTAG活動 #1

JNSA

人材不足は本当か？

自組織のセキュリティ業務担当者に
聞いてみた

セキュリティ業務を担う人材の現状調査報告書公開（11月2日）

https://www.jnsa.org/isepa/outputs/research.html

現状調査報告書

- 調査の目的
  - セキュリティ業務の担当者や責任者の方の知見やノウハウの共有を行うとともに、セキュリティ業務に携わる方が事前に何を学習および経験しておけば、より円滑にその業務を担うことができるのかを示唆することで、セキュリティ業務に携わる人材の素養を高めるための情報共有を行う。
- 調査期間
  - 2018年 6月 ～ 2018年 10月
- 調査対象企業/調査対象人数
  - 12社 / 25名
- ヒヤリング対象者
  - 自社内のセキュリティ対策の維持・向上を担当している方
- 調査実施方法
  - 担当者への対面インタビュー

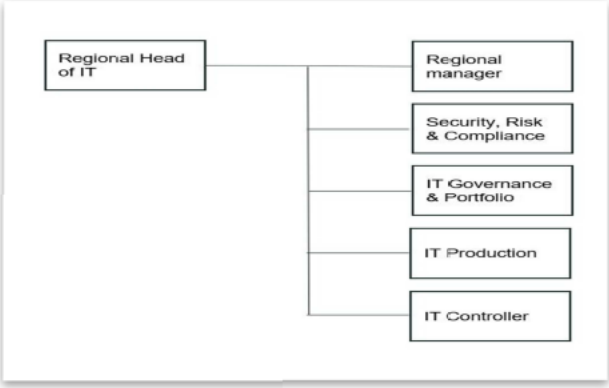
インタビュー項目

1.業務内容の把握
1.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
1.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
1.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
1.4.「セキュリティ業務」を行う環境（体制）
2.経験談
2.1.「セキュリティ業務」を実施していて苦労した経験
2.2.「セキュリティ業務」をしていてよかった経験
2.3.「セキュリティ業務」をしていて悩んだ経験
2.4.「セキュリティ業務」に着任しての処遇変化
2.5.自社のセキュリティ維持向上に効果が出たという取り組み
3.キャリアパス
3.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)
3.2.「セキュリティ業務」前に行っていた業務内容
3.3.「セキュリティ業務」についたことによるキャリア（観）への影響

報告書イメージ

2.1. ケース 1（人材サービス関連：自社内セキュリティ担当）
2.1.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：個人



組織図
業種
人材サービス関連

企業規模

社員数	3000名
システム要員数（内務）	35名
システム要員数（外部委託・派遣）	27名

（インタビュー当時の人数）

2.1.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容

内部統制、監査対応がメインの業務となるが、顧客からくる個人情報保護に関係する質問への対応もしている。主にやっていることとしては、アカウントレビューやログレビューなどになる。部署内にはインシデントレスポンスやバルネラビリティ（脆弱性）チェックを担当している人もいる。さらに、個人情報保護法などに関係する対応は法務部がしている場合もある。

2.1.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容

業務の区切りは明確に分けられない場合が多い。プロジェクトに参加し、要件定義などの際に、セキュリティ観点からのアドバイスを行うなどを現在行っている。

調査結果考察（概要）

- インタビュー対象者はCSIRT所属を除けば、**各部署業務に付随するセキュリティ業務にあたっている**方達。中には部内でセキュリティ担当を置いているという場合や、部の業務範疇のセキュリティ業務だけ外部へ委託しているといったケースも見られた。
- 処遇面で見ると**専門性が反映された評価基準にはなっていない**企業がほとんどである。各部署がセキュリティ業務の要素を担う場合では、部署の仕事の範疇とみられていると思われる。
- 今回の調査では時代背景や業務命令といった形で、**本来業務に加えてセキュリティ業務に携わる**きっかけを得ている場合が多かった。また、他部署との**積極的な配置転換は行われていなかった**。
- 人材の流動化や今後の人材確保を考えた場合、採用や育成、キャリア開発などについて**引き続き検討していく必要**がある。

調査活動スケジュール

活動へのご協力のお願い

- セキュリティ関連スタッフへのインタビューをお受けいただける組織を募集中！
  - お受けいただける組織の方は、JTAG事務局まで次のメールまでご連絡ください（JNSA内 jtag-sec@jnsa.org）
  - その後の詳細は直接ご連絡します

JTAG活動 #2

担当者のスキルは十分か？

セキュリティ業務に必要な知識やスキルの可視化ガイドラインを作ってみた

セキュリティスキル可視化ガイドライン β版で公開

可視化のための評価要素

評価要素の入力①

- 個人の主観によるブレをなくすため、事実（資格と業務経験）を重視したポイント計算方法を採用
- 各カテゴリの入力
  - ① 基本情報入力
  - ② 保有資格入力
  - ③ 業務経験入力（経験年数とセキュリティ関連度）

【手順①：基本情報入力】

氏名　（任意）	伊勢羽太郎
勤務先（任意）	ISEPA
役職　（任意）	係長
担当業務 (必須選択)	SOC
業務経験年数　（必須）	30
入力日　YYYY/MM/DD	2019/1/15

メールアドレス（任意）	
部門　（任意）	JTAG

担当業務 (自由書式)	
マネージメント年数	20

評価要素の入力②

【手順②：保有資格入力】

資格名称		保有資格
セキュリティ関連資格	ITパスポート試験	◎
	情報セキュリティマネジメント試験	◎
	システムアーキテクト試験	
	プロジェクトマネージャ試験	
	ネットワークスペシャリスト試験	
	データベーススペシャリスト試験	
	ITサービスマネージャ試験	
	エンベデッドシステムスペシャリスト	
	システム監査技術者試験	
	情報処理安全確保支援士試験	◎
	応用情報技術者試験	
	基本情報技術者試験	
	EnCE(（EnCase Certified	
	SSCP	
	CISSP	◎
	CompTIA security+	
	CompTIA CSA+	

評価要素の入力③

セキュリティ専門業務ではないが、関連する仕事を経験し、それなりに知識やスキルやノウハウなど持っている“プラス・セキュリティ人材”を評価するポイントとして、業務経験を指標に盛り込む。自己申告では判断しかねるスキルレベルを客観的に算出。

【手順③：業務経験入力】

業務/職務/役割			経験年数	セキュリティに関する関連%
	アプリケーションシステム（アプリ系）	企画・要件定義		
		設計		
		開発		
		構築		
		運用		
	ネットワークシステム	企画・要件定義	3	50%
		設計	3	50%
		開発		
		構築		
		運用（機器保守含む）	5	50%
		企画・要件定義		

非IT系の業務(一般事務・営業・人事・法務など)も業務経験として入力

評価結果表示

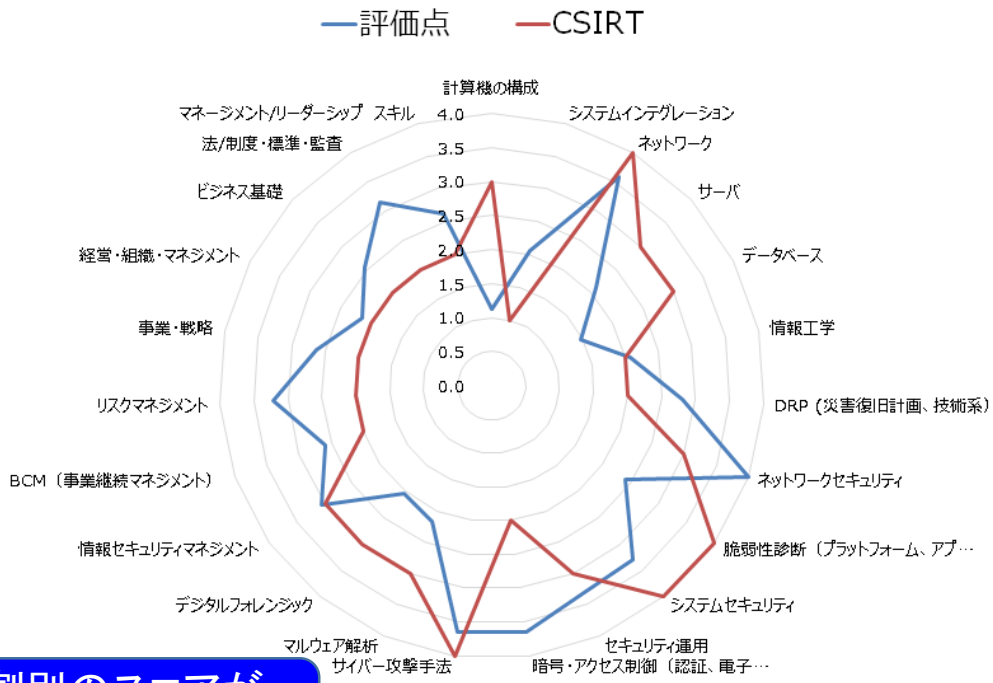
- 保有資格と業務経験から各スキルを**自動でポイント化**
- 可視化は合否ではなく、（TOEICのような）**スコア制**
- 点数とレーダーチャートで表現し、役割への**マッチ度**を測定

役割を表示

伊勢羽 太郎

CSIRT		←目標業務	
	評価点	CSIRT	重要評価ポイント
計算機の構成	1.1	3.0	
システムインテグレーション	2.1	1.0	
ネットワーク	3.6	4.0	★
サーバ	2.1	3.0	
データベース	1.5	3.0	
情報工学	2.1	2.0	
DRP（災害復旧計画、技術系）	2.8	2.0	
ネットワークセキュリティ	4.0	3.0	★
脆弱性診断（プラットフォーム、アプリ等共通）	2.4	4.0	★
システムセキュリティ	3.3	4.0	★
セキュリティ運用	3.3	3.0	
暗号・アクセス制御（認証、電子署名等）	3.7	2.0	
サイバー攻撃手法	3.7	4.0	★
マルウェア解析	2.2	3.0	★
デジタルフォレンジック	2.1	3.0	★
情報セキュリティマネジメント	3.1	3.0	
BCM（事業継続マネジメント）	2.6	2.0	
リスクマネジメント	3.2	2.0	
事業・戦略	2.6	2.0	
経営・組織・マネジメント	2.2	2.0	
ビジネス基礎	2.6	2.0	
法/制度・標準・監査	3.2	2.0	
マネージメント/リーダーシップ スキル	2.6	2.0	

マッチ度 重要項目のみ	85.4%
マッチ度 重要項目＋非重要(上限100%)	88.9%



役割別のスコアがマッチ度として表示

可視化ガイドライン活動スケジュール

活動へのご協力のお願い

- β版による適合度チェックのトライアル募集中！
  - お受けいただける方は、JTAG事務局まで次のメールまでご連絡ください
    （JNSA内 jtag-sec@jnsa.org）
  - チェック項目の入力フォーマットを事務局より希望者に送付
  - 希望者はチェック項目への入力を行い、事務局に送付
  - 事務局で適合度報告書を作成し返送
  - 報告書の内容について必要に応じて事務局にコメント返送

JNSA

JNSA