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

「セキュリティ人材育成は、新たなステージへ！」

～セキュリティ人材に求められる役割の変化とSecBoK2019～

NPO日本ネットワークセキュリティ協会 教育部会 部会長

平山　敏弘

１．セキュリティ人材不足の現状

本当に足りない人材は？

セキュリティ人材不足　20万人？

日本経済新聞

2016年6月4日（土）

Web刊　速報　ビジネスリーダー　マーケット　テクノロジー　アジア　スポーツ　マネー・ライフ

全て　経済　企業　国際　政治　株・金融　スポーツ　社会　ニュース18時　その他ジャンル▼

速報＞経済＞記事

サイバー防衛で20万人不足　経産省調べ、20年に

2016/5/19 0:04｜日本経済新聞　電子版

小 中 大　保存　リプリント　▼共有

経済産業省は、サイバー攻撃などに対処できるセキュリティーの専門人材が2020年に20万人近く不足するとの調査結果をまとめた。人工知能（AI）など最先端のIT（情報技術）に関わる人員も約5万人足りなくなる見通し。官民を挙げた人材育成が急務になる。

調査は企業へのアンケートやIT産業の就職・離職率、市場規模の統計などから、経産省が推計した。ITを主力とする企業だけでなく、自動車や電力など産業界全体で…

＜電子版トップ　＜速報トップ

セキュリティ人材不足は、嘘？

日本経済新聞
2019年3月25日（月）

トップ　経済・政治　ビジネス　マーケット　テクノロジー　国際・アジア　スポーツ　社会

ストーリー　速報　朝刊・夕刊

セキュリティー人材、消えた「19万人不足」

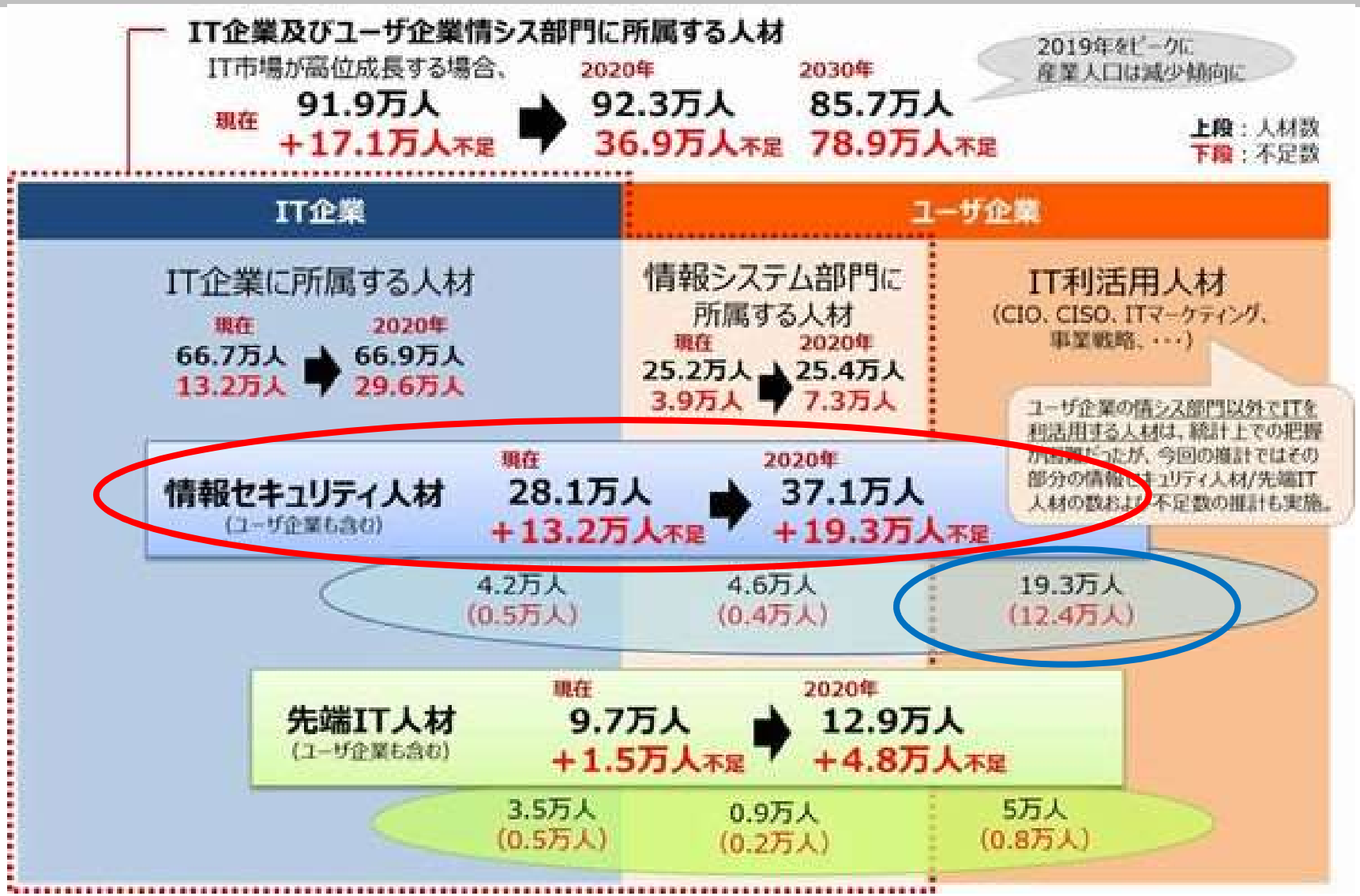
コラム（ビジネス）

2018/8/28 6:30 | 日本経済新聞　電子版

保存　共有　その他

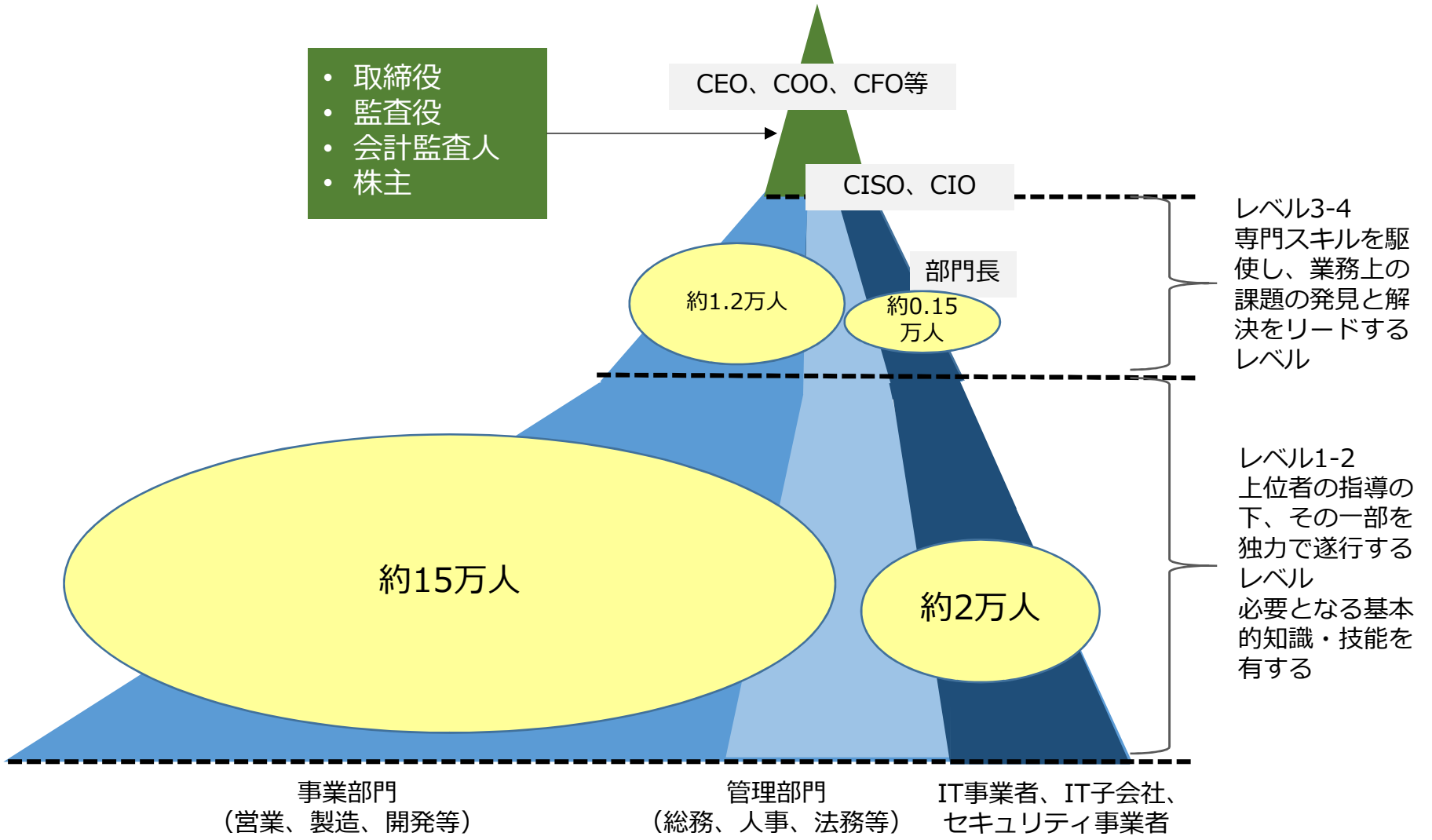
サイバー攻撃の増加を背景に、情報セキュリティー人材の不足を指摘する声が多い。経済産業省の2016年の調査では「20年に国内で19万3000人が不足する」と予測したほどだ。だがサイバー防衛の現場からは「不足感はない」との反論が多い。背景には「理想的な状況」を想定して必要な人材数を割り出した経産省と、実務の大部分を外部に委託している一般企業との「食い違い」があった。

本当に足りない人材は？
ここの数値にも注目を



出典　http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

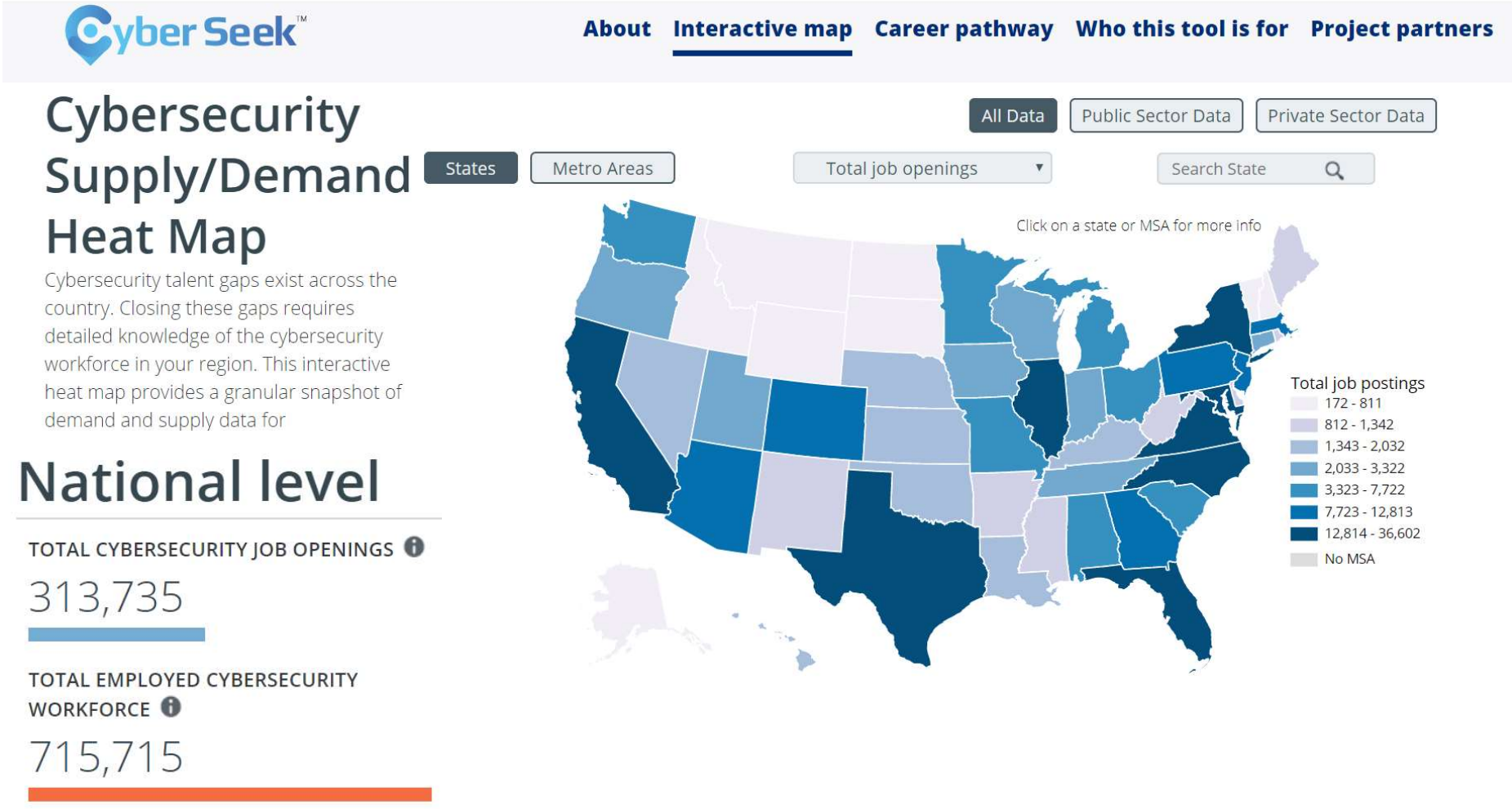
セキュリティ人材不足数をマッピングしてみると
「＋（プラス）セキュリティ人材」不足への対応



参考資料：米国のセキュリティ人材求人状況
海外でもこんなにもセキュリティの仕事が

米国のCyberSeekというサイトでは、セキュリティの求人数が「見える化」されており、30万件以上の求人募集がある状況である。

CyberSeek　https://www.cyberseek.org/heatmap.html



２．セキュリティが経営課題と言われる背景

世界経済フォーラム（WEF:World Economic Forum）

世界経済フォーラム（WEF:World Economic Forum）

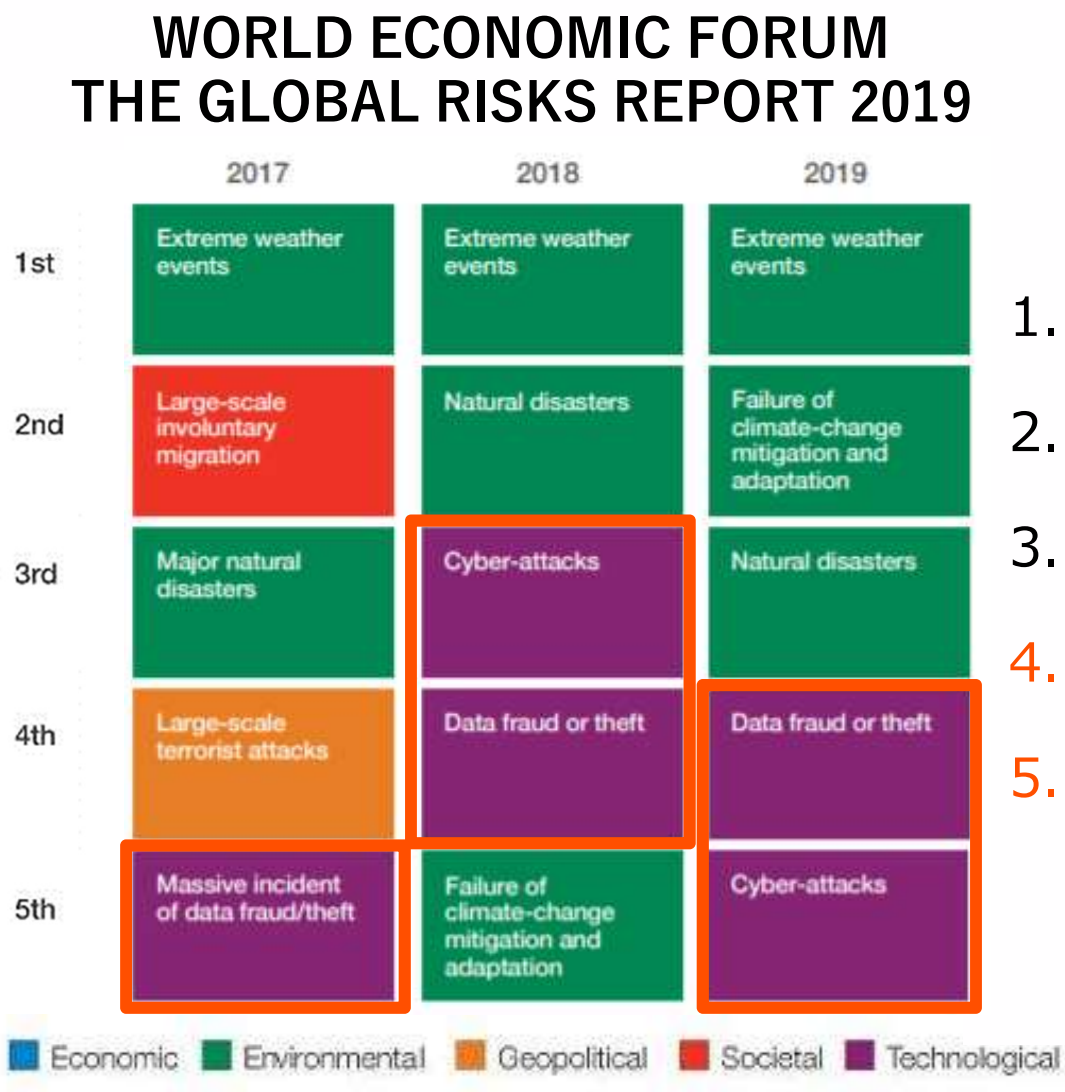
「WEF」は、官民両セクターの協力を通じて世界情勢の改善に取り組む国際機関で、1971年に非営利財団として設立されました。スイスのジュネーブに本部を置き、特定の利害と結びつくことのない、独立した公正な組織です。当フォーラムは、最高水準のガバナンスを維持し、またグローバルな公益のために起業家精神を発揮することに全力を尽くしており、モラルと知的誠実さを行動指針の核として掲げています。

政界、ビジネス界、および社会における
その他の主要なリーダーと連携し、世界、
地域、産業のアジェンダを形成します。

ダボス会議

「ダボス会議」は、WEFが毎年1月に、スイス東部の保養地ダボスで開催する年次総会です。この会議では毎年、世界を代表する政治家や実業家が一堂に会し、世界経済や環境問題など幅広いテーマで討議しますが、各界から注目され、世界に強い影響力を持っています。日本からも首相や著名な経済学者などが参加しています。

なぜセキュリティ人材は足りない？
世界中の経済界でもサイバーセキュリティの重要性



グローバルリスクTOP5

1. 異常気象
2. 気候変動緩和・適応への失敗
3. 自然災害
4. データ詐欺・データ盗難
5. サイバー攻撃

サイバー犯罪の与える経済へのインパクト

約63兆円/年

GLOBAL CYBER CRIME IMPACT

0.8%

OF GLOBAL GDP

出典：CSIS（Center for Strategic and International Studies）&McAfee
共同調査レポート「Economic Impact of Cybercrime - No Slowing Down」

（参考）

自然災害のGDPに対する影響

国内大震災事例

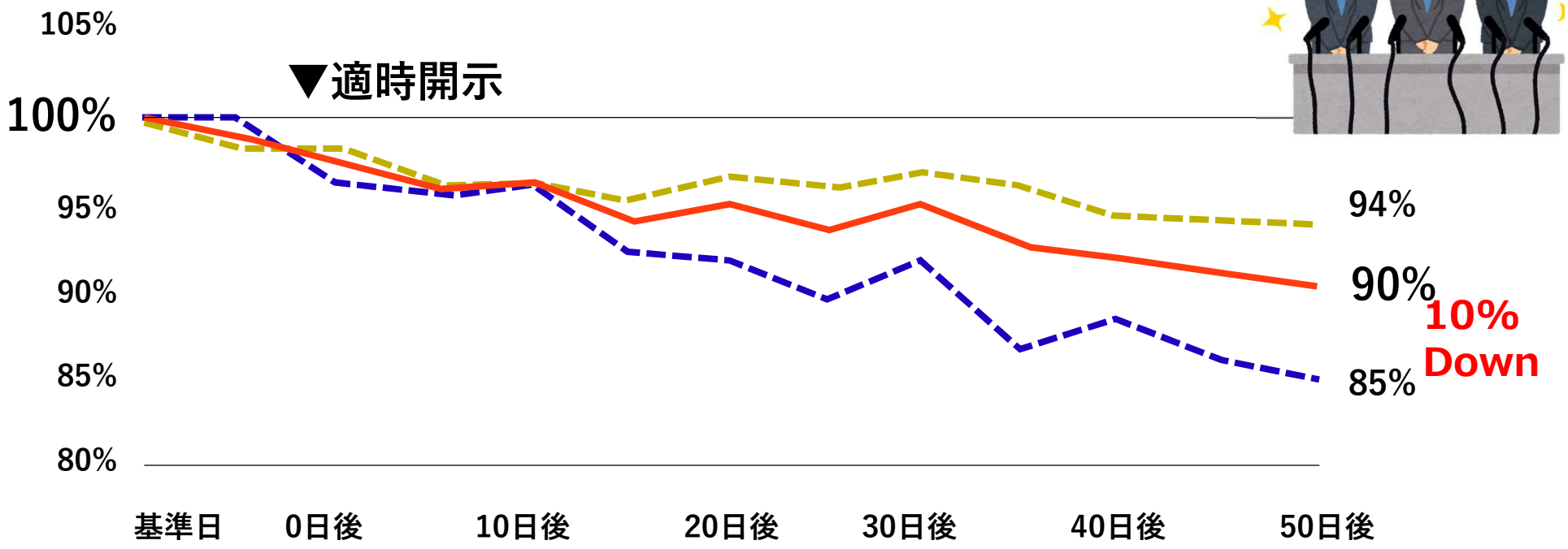
阪神・淡路大震災（1.9%）

東日本大震災（3.5%）

出典：内閣府「交通事故の被害・損失の経済的分析に関する調査結果」
内閣府「平成27年版 防災白書　近年の自然災害による被害額のGDP比」

謝罪だけでは済まない
セキュリティインシデントの企業に与える影響

セキュリティ事故適時開示後の株価傾向（日本企業）



2018 JCIC 取締役会で議論するためのサイバーリスクの数値化モデル ～サイバーリスクの金額換算に関する調査～

- 東証一部
- 平均
- 東証一部以外の上場企業

N=18

サイバーリスク指標モデル
（年商1000億円企業における社内報告資料の例）

		想定すべき損失額	算出根拠
直接被害	個人情報漏えいによる金銭被害	▲80億円	JNSA一人当たり損害賠償額より算出 （基礎情報価値×機微情報度×本人特定容易度×社会的責任度×事後対応評価×顧客数≒80億円）
	ビジネス停止による機会損失	5営業日あたり ▲20億円	社内ヒアリングより算出 （1日あたりの生産量×商品単価≒2億円） （1日あたりのECサイト売上≒2億円）
	法令違反による制裁金	▲40億円	EUデータ保護指令（GDPR）の制裁金 （全世界の売上高の4%≒40億円）
	事故対応費用	▲0.6億円	過去事例や業者ヒアリングにより算出 （調査費用、データ復旧費用、応急処置費用等）
間接被害	純利益への影響	▲10.5億円	JCIC調査実績より算出 （前期純利益50億円×21%≒10.5億円）
	時価総額への影響	▲300億円	JCIC調査実績より算出 （時価総額3000億円×10%≒300億円）

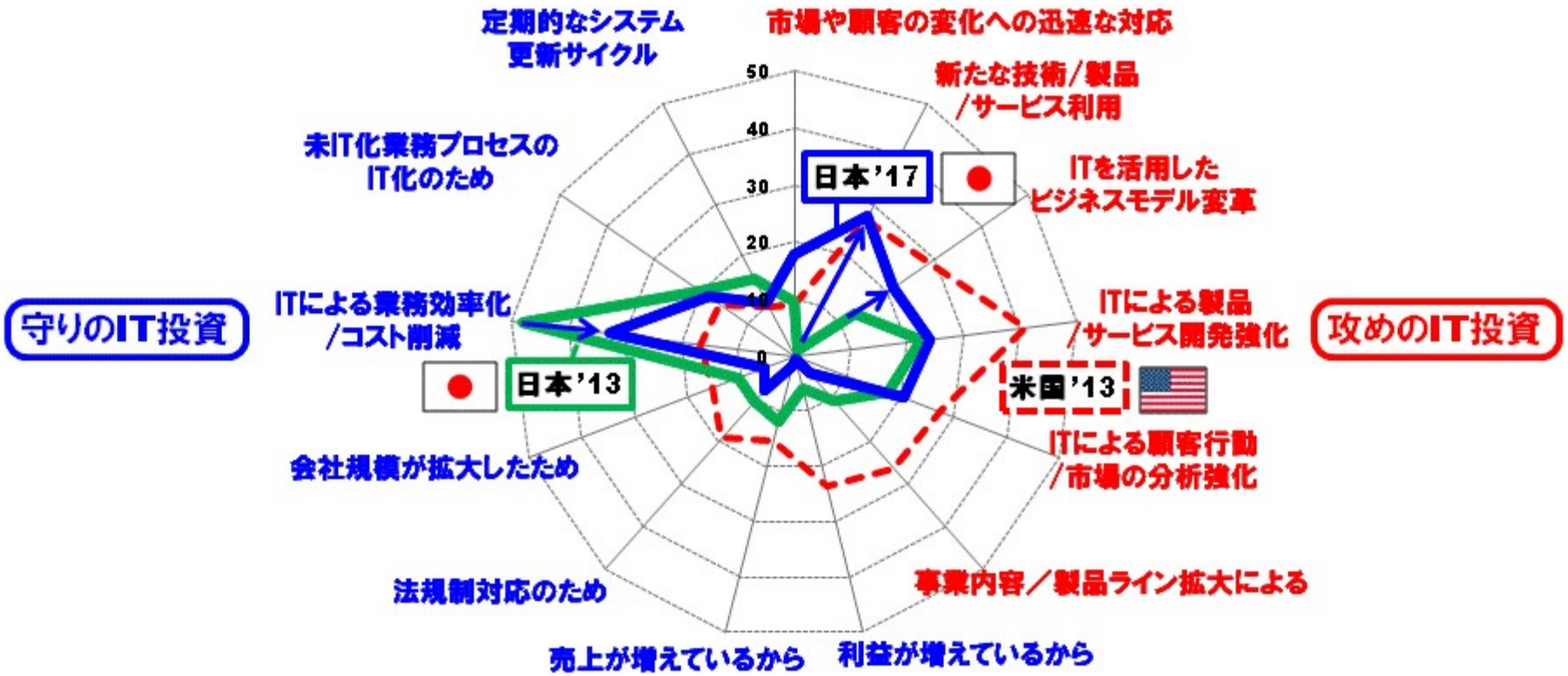
出典：JCIC「取締役会で議論するためのサイバーリスクの数値化モデル」サイバーリスク指標モデル

３．セキュリティの変化

「守り」から「攻め（積極的）」へ

「守りのIT投資」から「攻めのIT投資」へ

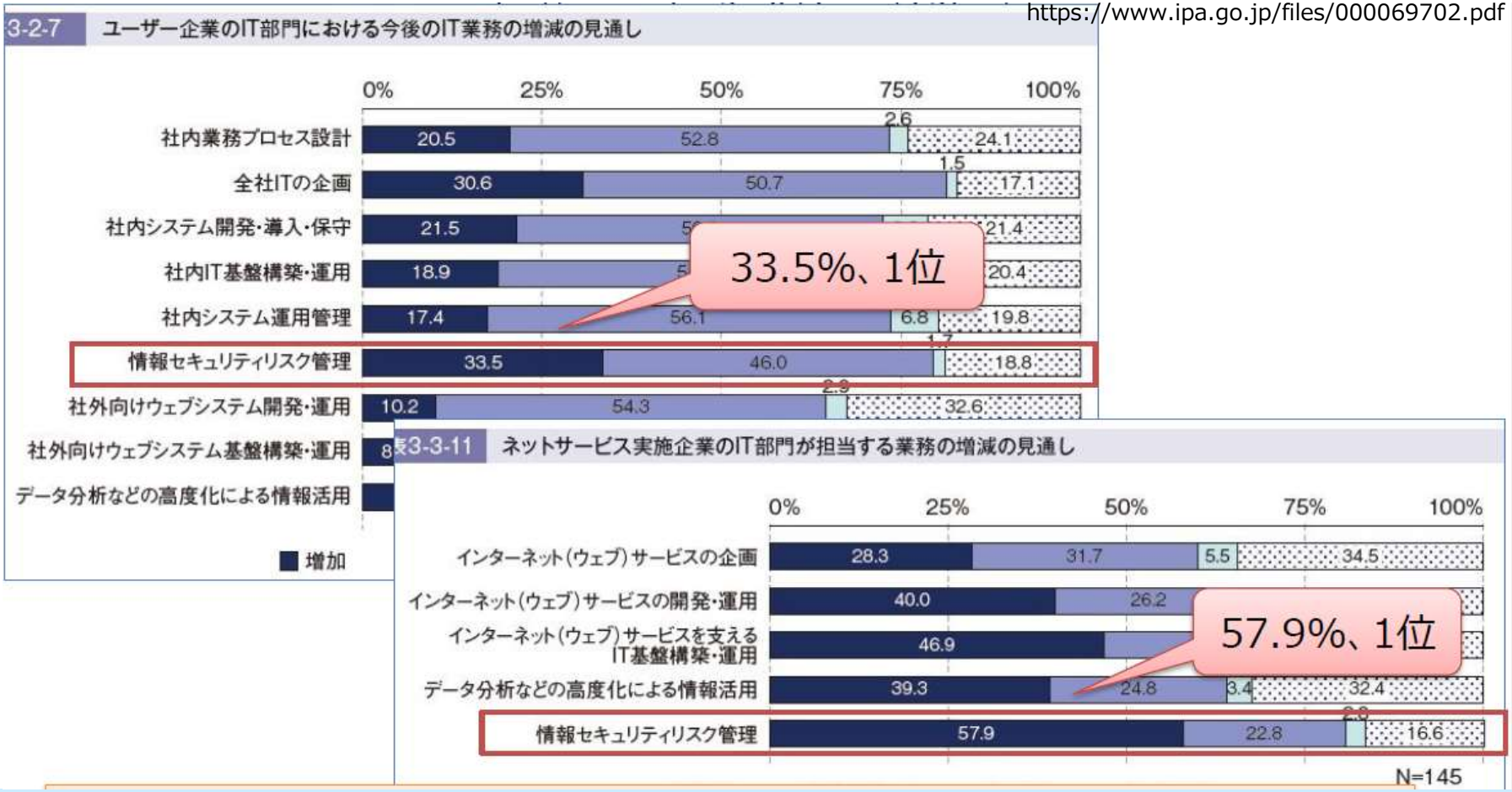
「作る」から「創る」へ、「必要なもの」から「意味あるもの」への変化



出典：JEITA『2017 年 国内企業の「IT経営」に関する調査結果　https://www.jeita.or.jp/japanese/exhibit/2018/0116.pdf

経営へのIT依存度が高まる程、
セキュリティの重要性も高まる傾向へ

出典：IPA「いま求められるセキュリティ人材確保のために」より
https://www.ipa.go.jp/files/000069702.pdf



「情報セキュリティリスク管理業務が増加する見通し」では、ネットサービス企業とユーザ企業では意識が違う（6割⇔3割）。ネットサービス企業は情報セキュリティに対する危機感が、ユーザ企業と比較して高い
→**経営のIT依存度の違い**と考えられる
→今後、**DX化などにより経営のIT依存度が高まる**と、ユーザ企業でも高まる可能性が

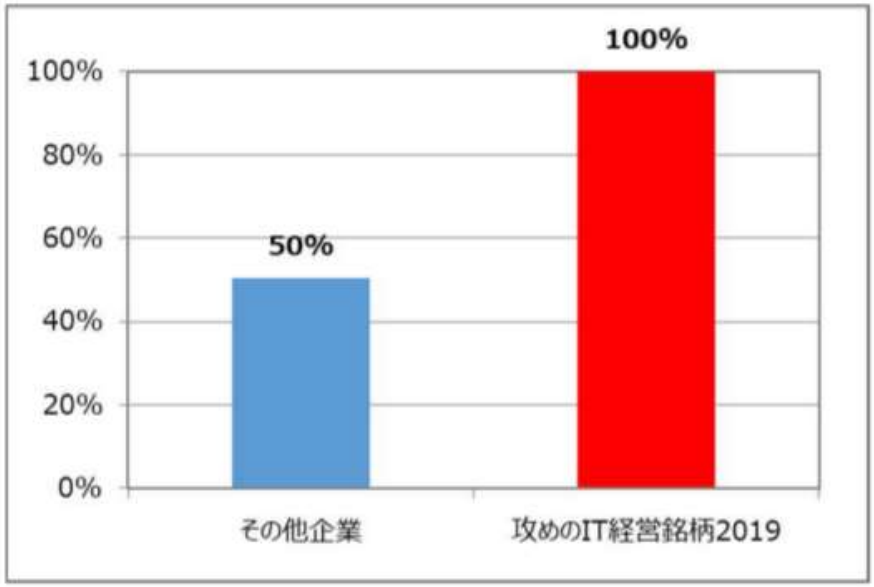
攻めのIT経営銘柄
攻めのIT経営を支える基盤的取組

「攻めのIT銘柄」とは
経済産業省が、我が国企業の戦略的IT利活用の促進に向けた取組の一環として、東京証券取引所と共同で、中長期的な企業価値の向上や競争力の強化のために、経営革新、収益水準・生産性の向上をもたらす積極的なIT利活用に取り組んでいる企業を、「攻めのIT経営銘柄」として選定しています。

（大きな差が出ている取組）

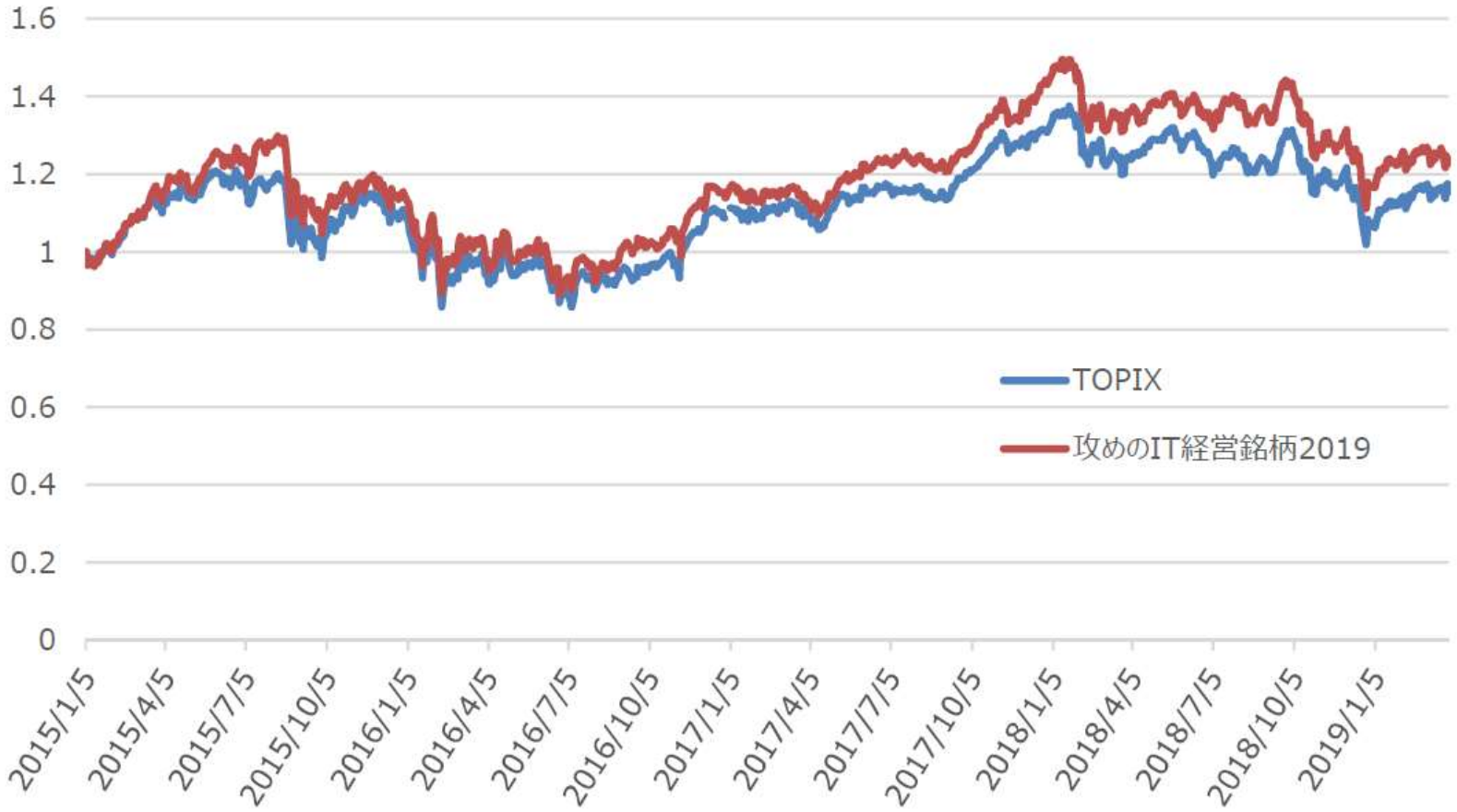
- **情報セキュリティリスクとして守るべき情報を特定し、リスクに対応するための計画（システム的・人的）を策定するとともに、防御のための仕組み・体制を構築している**

情報セキュリティリスクとして守るべき情報を特定し、リスクに対応するための計画（システム的・人的）を策定するとともに、防御のための仕組み・体制を構築している



攻めのIT投資の成果例（運用パフォーマンスの試算）
攻め（積極的な）のセキュリティ投資の意味

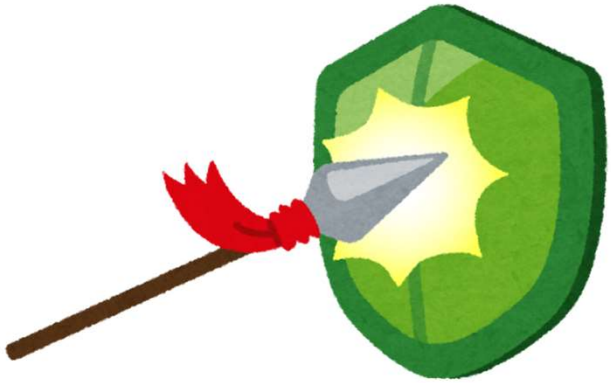
「攻めのIT経営銘柄2019」選定企業を構成銘柄として、各銘柄に等金額投資した際の運用パフォーマンスを試算し（2015年1月初を起点とし各社に対し等金額投資をした場合の評価額の推移）、参考としてTOPIX平均株価の推移との比較が掲載されています。
「攻めのIT経営銘柄2019」は、試算期間全体で見ると、TOPIX平均以上（10-20%Up）の株価上昇率となっており、高いパフォーマンスを示しています。



デジタル時代に求められるセキュリティ人材への役割（ブレーキは何のために必要）

守りのセキュリティ（盾と矛）

攻めとスピードのセキュリティ



３．求められるセキュリティ関連人材

求められる人材と役割の変化

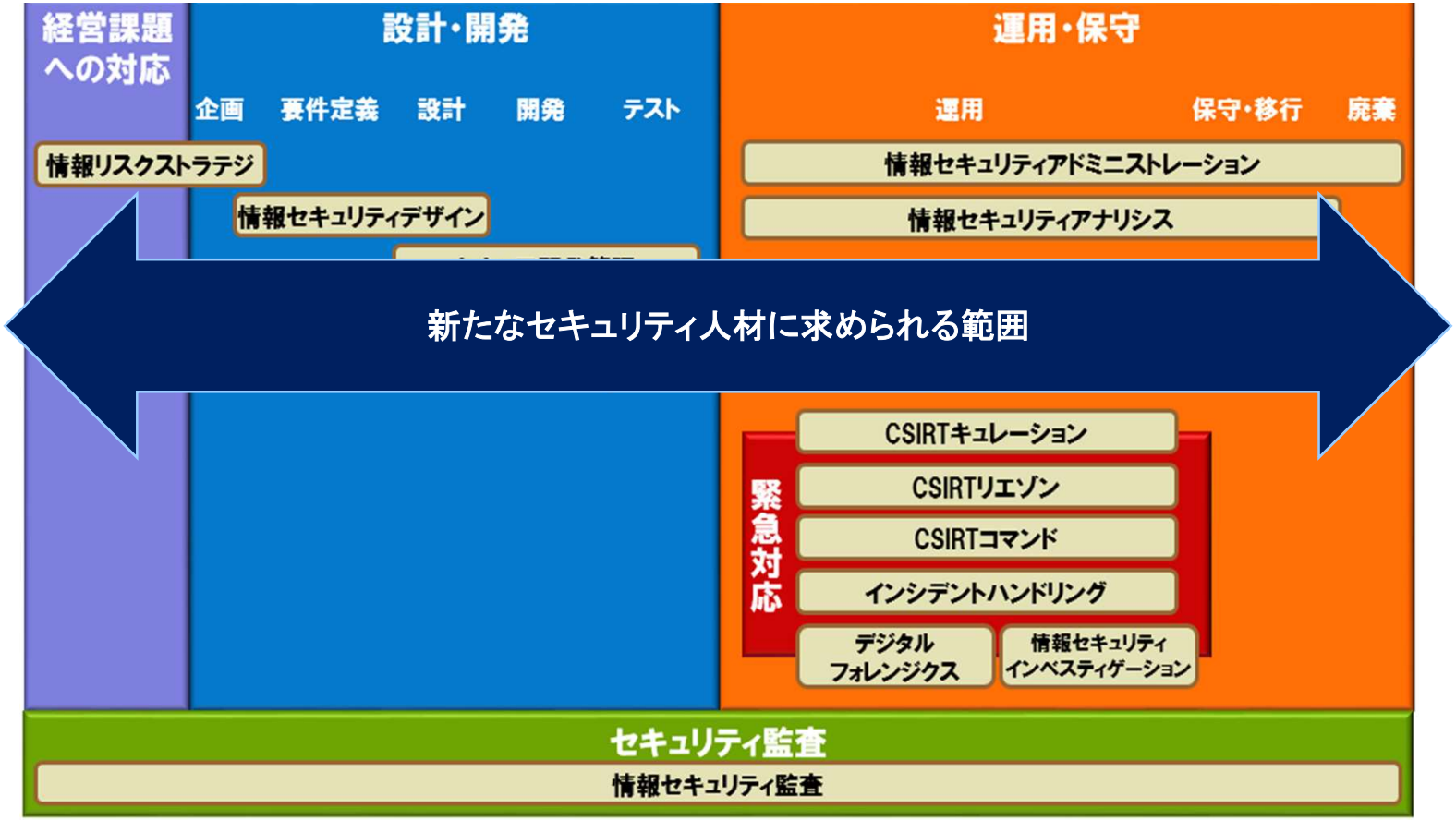
国ではどんな人材育成施策が取られているのか

参照http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_2/pdf/001_04_00.pdf

情報処理安全確保支援士とITSS+ロールとの関係

情報処理安全確保支援士の想定業務

サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、
サイバーセキュリティ対策の調査・分析・評価や
その結果に基づく指導・助言を行う。



※ITスペシャリスト（セキュリティ）は、ITスキル標準及びiコンピテンシ・ディクショナリにおいて定義されている

４．SecBoK2019の改定ポイント

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

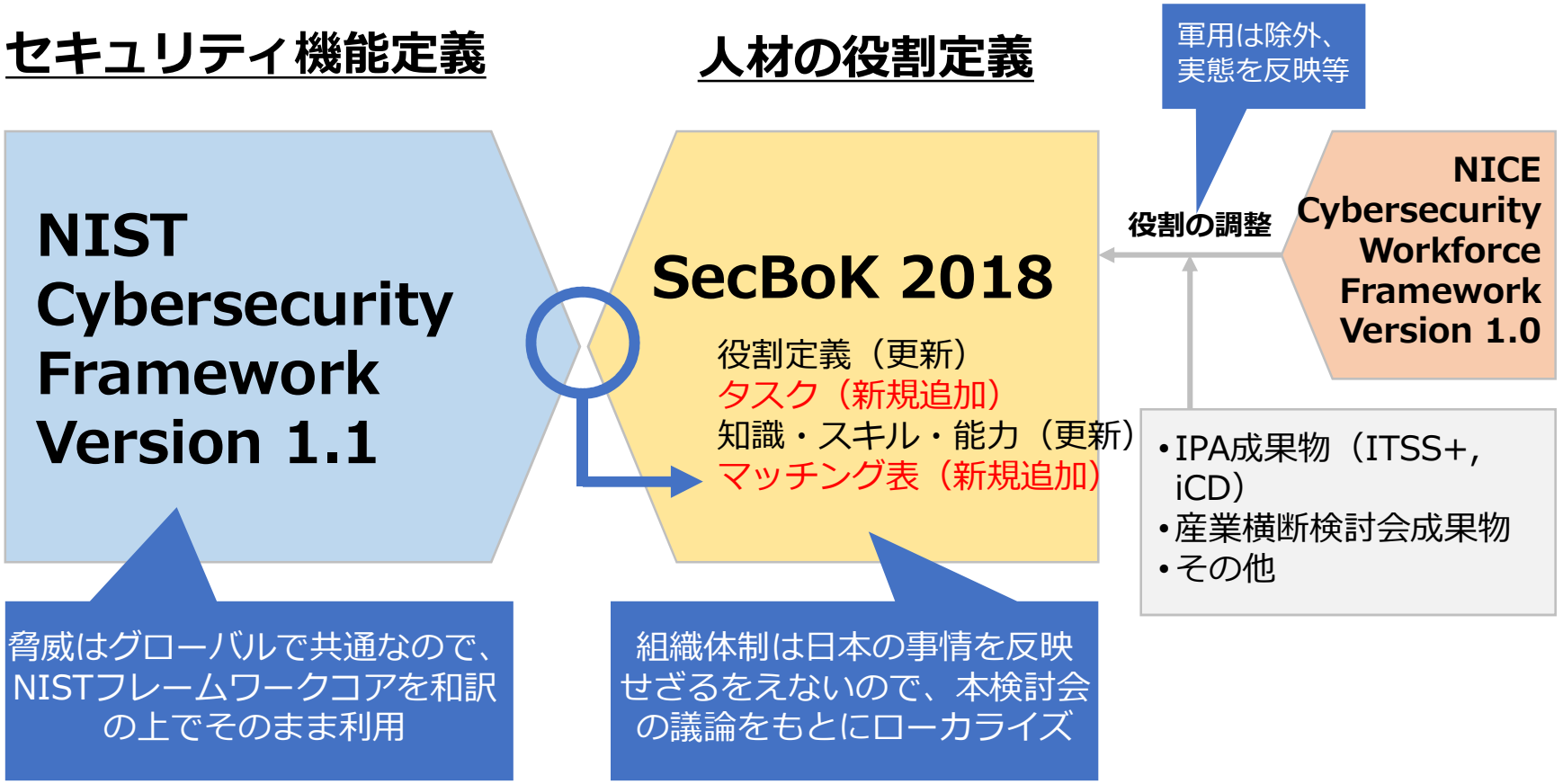
セキュリティ現場が直面している課題

- 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（専門人材）」だけ育成すればよいわけではない　→　**プラス・セキュリティ人材の重要性　高**
  - 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

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改定の方法性
セキュリティ機能定義と役割定義の分析



5．SecBoK2019概要

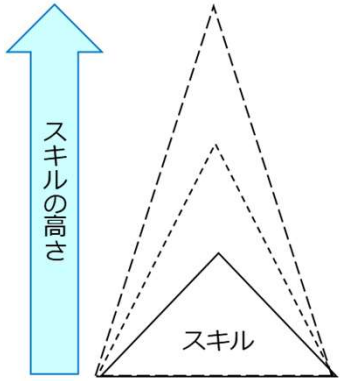
セキュリティ人材育成の考え方の変化
スキル中心からタスク・ロールとの連携強化へ

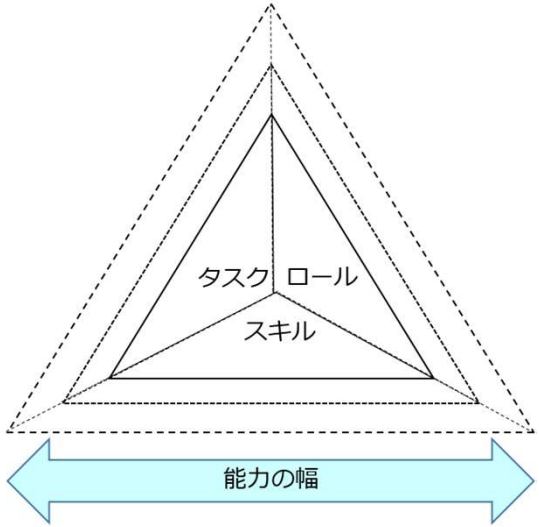
従来の考え方

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（日本で使いやすいように、カテゴリー変更や、基礎・総論などの項目分けなどを独自に実施）

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（２）
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リ	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（３）
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・標準	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（４）
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。

教育界（情報系大学）適用事例
コンピュータサイエンスカリキュラム標準（J17）

情報専門学科カリキュラム標準（J07）とは、日本の情報専門教育の状況に対応した見直しを行い、コンピュータ科学（CS） 情報システム（IS）コンピュータエンジニアリング（CE）ソフトウェアエンジニアリング（SE） インフォメーションテクノロジ（IT）一般情報処理教育（GE）についてまとめたカリキュラム標準で、2017年に見直しされJ17が公表されている。

分野｜大項目｜中項目	CS	IS	CE	SE	IT	GE	CyS ICT 基礎	CyS セキュリティ基礎	CyS セキュリティ専門
基礎｜ICT 基礎｜情報理論	●			●	●	●	●		
基礎｜ICT 基礎｜計算機ハードウェア	●	●		▲	●		●		
基礎｜ICT 基礎｜ネットワークインフラ	●	●		▲	●	●	●		
基礎｜ICT 基礎｜通信プロトコル・サービス	●	●		▲	●	●	●		
基礎｜ICT 基礎｜データ構造	●	●		▲	▲		●		
基礎｜ICT 基礎｜データベース	●	●		▲	●	●	●		
基礎｜ICT 基礎｜ナレッジマネジメント	●	●		▲	▲	●	●		
基礎｜ICT 基礎｜アルゴリズムとプログラミング	●			●	●	●	●		
基礎｜ICT 基礎｜オペレーティングシステム	●	●		▲	●	●	●		
基礎｜ICT 基礎｜ソフトウェア	●	●		●	●	●	●		
基礎｜ICT 基礎｜システム開発	●			●	●	●	●		
基礎｜ICT 基礎｜システム運用	▲	●		▲	●	●	●		

人材に必要となるスキルについては、セキュリティ知識分野(SecBoK)人材スキルマップを参考とした。カリキュラムモデルに必要となる教えるべき知識項目の整理するため、サイバーセキュリティのカリキュラム作成の際に参考として、SecBoK人材スキルマップにおける各情報専門教育項目をカバーする範囲 の専門レベル を対象としたレベル分けを整理した。

ASEAN諸国におけるSecBoK利活用 インドネシアおよびベトナムでの事例

独立行政法人国際協力機構（JICA）において、SecBoKを利用したセキュリティ人材育成プロジェクトが実施されている。

インドネシア：サイバーセキュリティ人材育成プロジェクト

https://www2.jica.go.jp/ja/evaluation/pdf/2018_1701288_1_s.pdf

【プロジェクト概要】
インドネシア最高峰の大学の一つであるインドネシア大学におい てプロフェッショナル（実務者）向けサイバーセキュリティ教育システムを立 上げることで、重要情報インフラ分野を中心とする民間機関や政府に対してサイバーセキュリ ティ人材を持続的に供給する。
【事業概要】
本事業は、インドネシア国において、セキュリティ知識分野（SecBoK）人材スキルマップに準拠するプロフェッショナル人材育成のためのサイバーセキュリティプログラムをインドネシア大学内に立上げ、諸外国のサイバーセキュリティ人材も巻込みながら、同大学におけるサイバーセキュリティ人材の育成システム強化を図り、民間機関・政府のサイバーセキュリティ対応能力強化に寄与するもの。

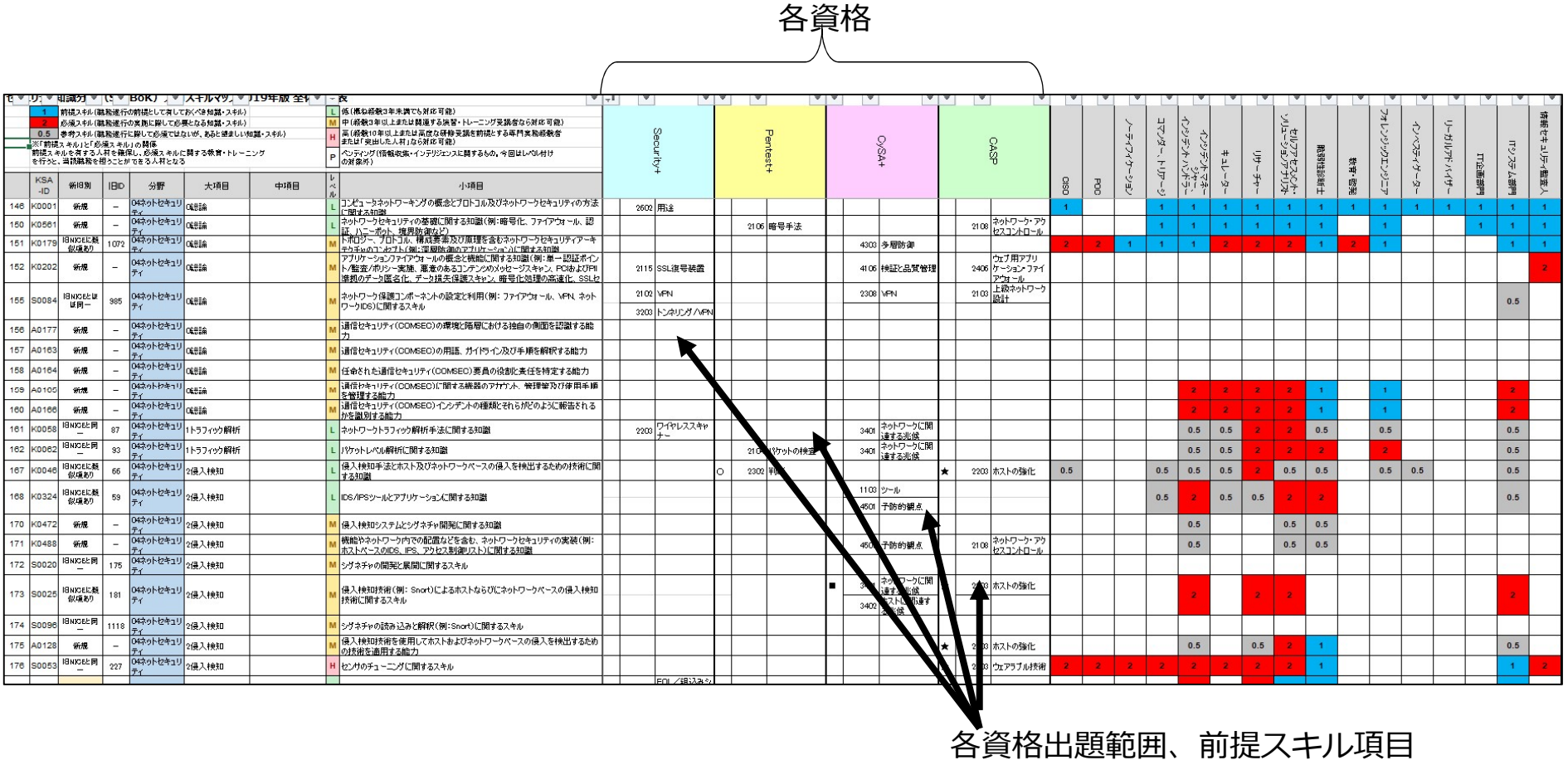
ベトナム：サイバーセキュリティに関する能力向上プロジェクト（キャリア開発計画）

https://www2.jica.go.jp/ja/announce/pdf/20190424_190086_4_02.pdf

【プロジェクト概要】
ベトナム情報通信省より「サイバーセキュリティに関する能力向上プロジェクト」実施の要請がなされた。要請された内容は、政府サイバーセキ ュリティ人材の能力向上、政府情報ネットワークをサイバー攻撃から守る機材・技術 の供与、サイバーセキュリティ啓発活動などとなっている。
【活動概要】
SecBoK のフレームワークに定義された役割（ロール）のうち必要とされるものを明らかにし、それぞれの職員のキャリア開発計画を策定する。またSecBoK のフレームワークに定義された役割（ロール）のうち優先度の高いもの研修コースを計画・実施する

資格との連携事例
CompTIAセキュリティ関連資格とSecBoKスキル

ベンダーニュートラルなIT資格団体であるCompTIAにおいて、各資格で問われているスキル項目とSecBoKスキル項目とのマッピングを実施。これにより資格ホルダーがどのセキュリティロールに適合度が高いかなどか可視化され、個人の育成計画だけでなく部門や組織の体制作りや部門全体の育成などに有用となる。



まとめ
セキュリティ人材育成　Go to the next stage！

１．人材不足は真実か？
　人材不足は真実だが、求められる人材が変化している

２．人材不足は、オリンピック・パラリンピックまでではオリンピックに関係ない米国でもセキュリティ人材不足は深刻である

３．なぜセキュリティは経営問題なのか
　サイバーセキュリティ被害は深刻であり、世界的経済において大きなリスク

４．わが社にはセキュリティは関係ない
　今後の企業生き残りをかけたDX化への対応において、セキュリティは必須

５．SecBoKって、セキュリティ企業にしか関係なのでは
　セキュリティ専門人材はもちろん、プラス・セキュリティ人材育成にも有用

６．セキュリティ人材育成の新たなステージとは
　従来のセキュリティ専門人材に対するスキル中心の育成方法から、**「セキュリティスキルを持って何ができるか」**といったタスクの考えや、事業部門やユーザ企業においてもセキュリティが必要となる**「プラス・セキュリティ人材」**育成も必要