

「セキュリティ知識分野(SecBoK)人材スキルマップ2016年版」概要

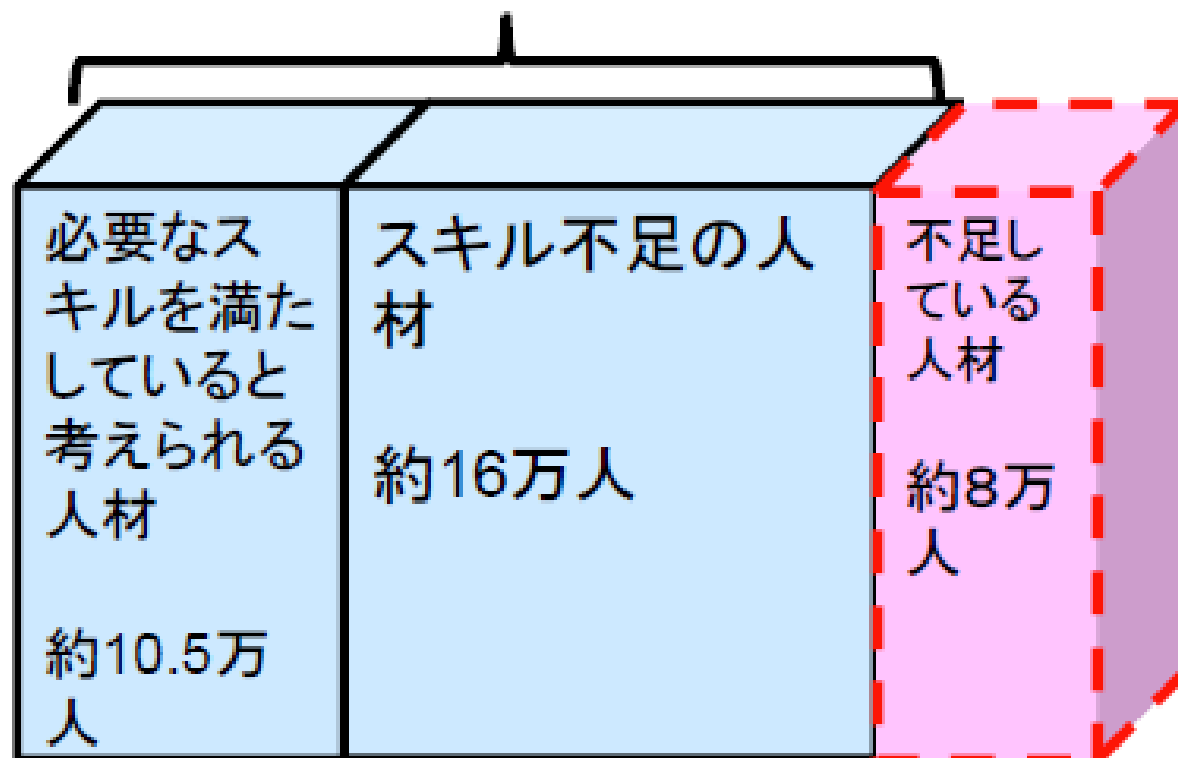
～現在最も必要とされる人材にスコープして公開～

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. 不足する情報セキュリティ技術者
本当に足りないのは誰？

1.1 誰が足りない？ 何が足りない？

国内のユーザー企業において
情報セキュリティに従事する技術者
約26.5万人



IPAの試算によれば、国内のユーザー企業において、情報セキュリティ人材は大幅に不足(約8万人の不足)。

＜IPA試算「情報セキュリティ人材育成に関する基礎調査」の人材不足数に関する追加分析による。H24調査→H26追加分析。＞

1.2 どこで足りない？ どの業界(業種)で足りない？ **JNSA**

約8万人の業種別内訳

業種	(人)
農林業・水産業・鉱業	256
建設・土木・工業	2,764
電子部品・デバイス・電子回路製造業	1,403
情報通信機械器具製造業	605
電気機械器具製造業	1,159
その他製造業	15,853
電気・ガス・熱供給・水道業	81
通信業	683
情報サービス業	1,885
その他の情報通信業	1,717
運輸・郵便業	6,719
卸売業・小売業	14,480
金融業・保険業	4,957
不動産業・物品賃貸業	1,547
学術研究・専門技術者	1,014
宿泊業・飲食サービス業	3,535
生活関連サービス業・娯楽業	3,301
教育・学習支援業	2,084
医療・福祉	8,473
複合サービス業	614
その他サービス業	8,462
計	81,590

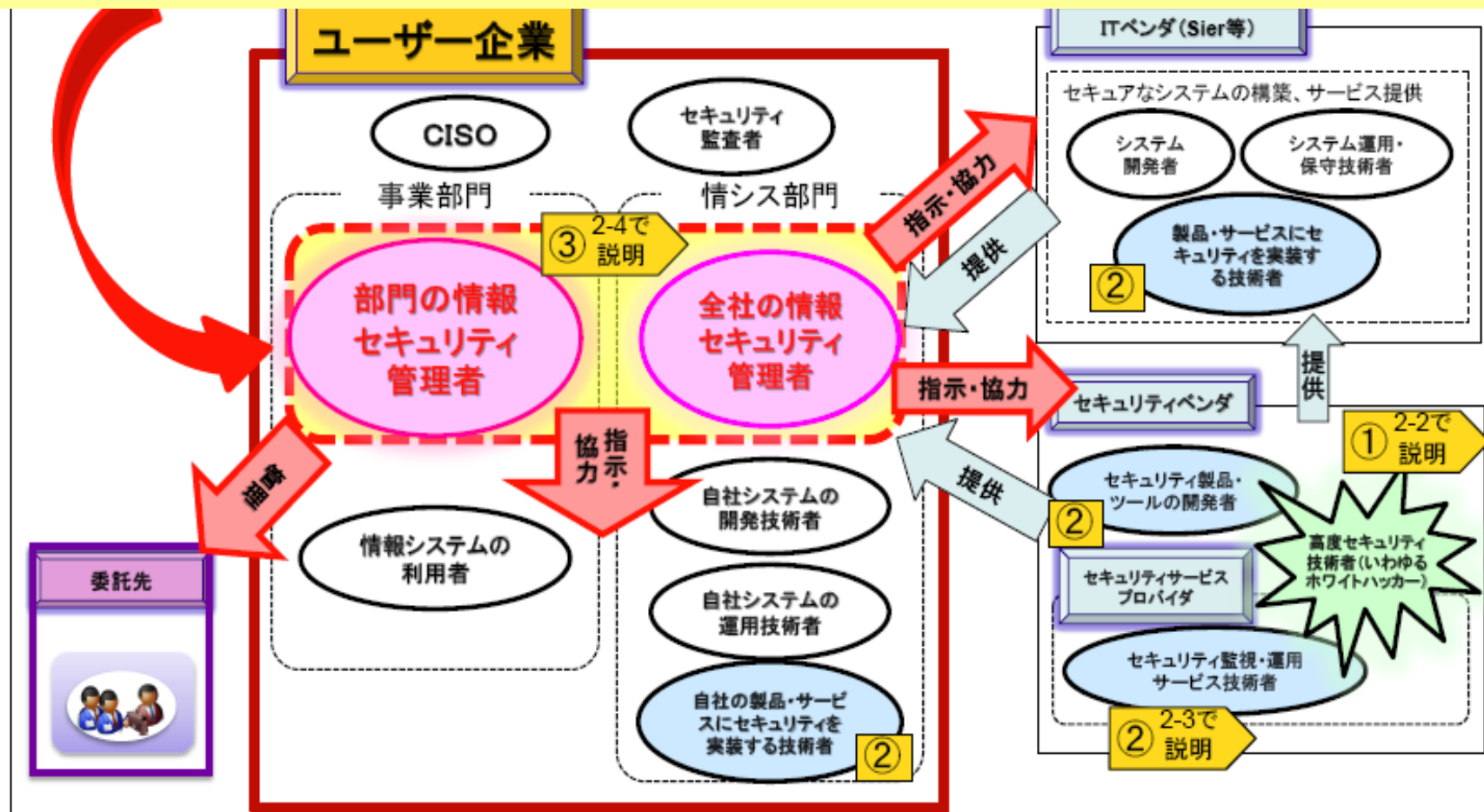
特に情報関連以外の製造業や卸売業・小売業、医療・福祉等のユーザ業種における人材不足が顕著。

出典

http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/it_jinzai_wg/pdf/002_03_00.pdf

1.3 今後必要となるセキュリティ人材像とは？

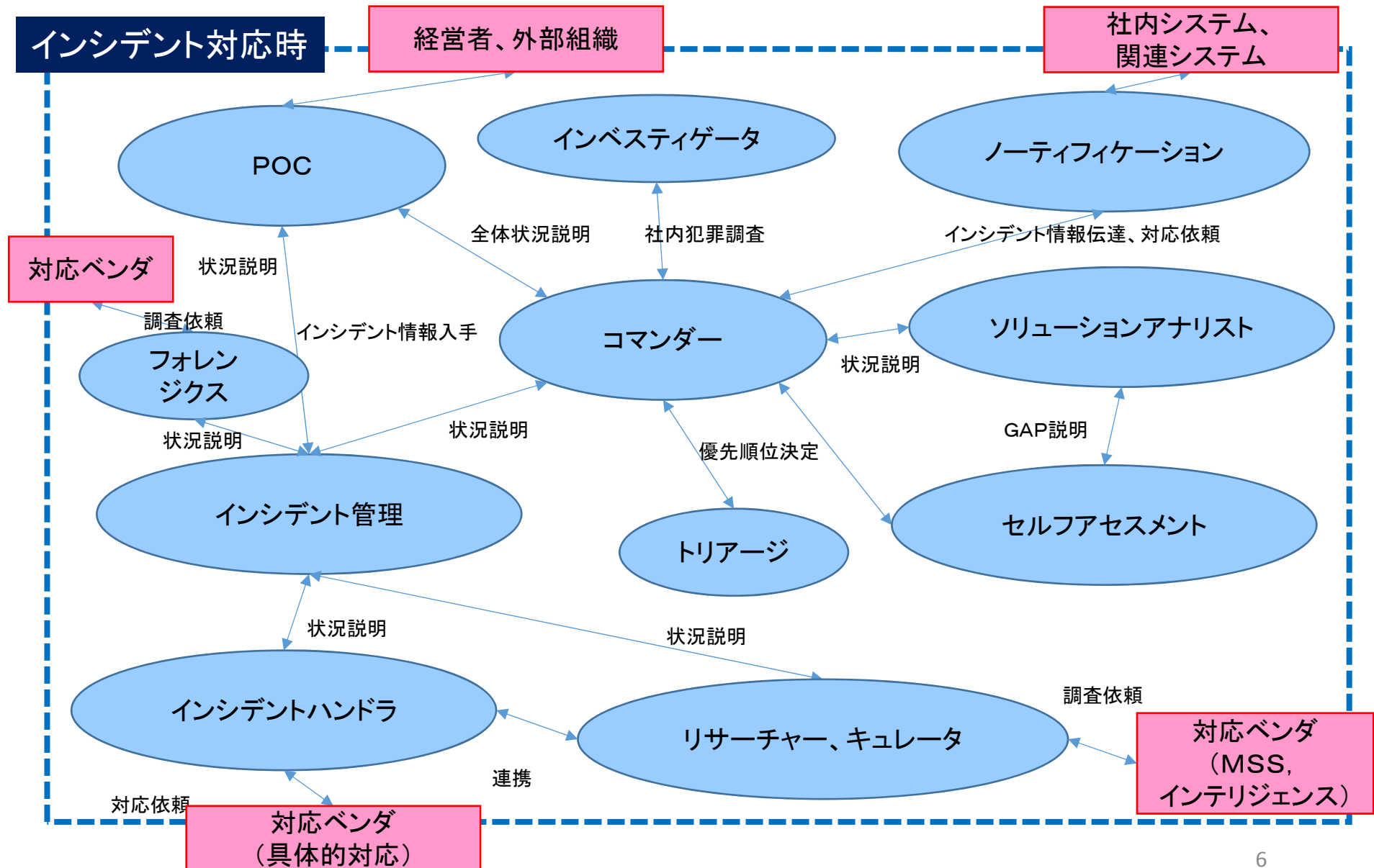
- ① ホワイトハッカーのような高度セキュリティ技術者
- ② 安全な情報システムを作るために必要なセキュリティ技術を身につけた人材
- ③ ユーザー企業において、社内セキュリティ技術者と連携して企業の情報セキュリティ確保を管理する人材。



平成27年3月 経済産業省情報処理振興課「情報セキュリティ分野の人材ニーズについて」より抜粋

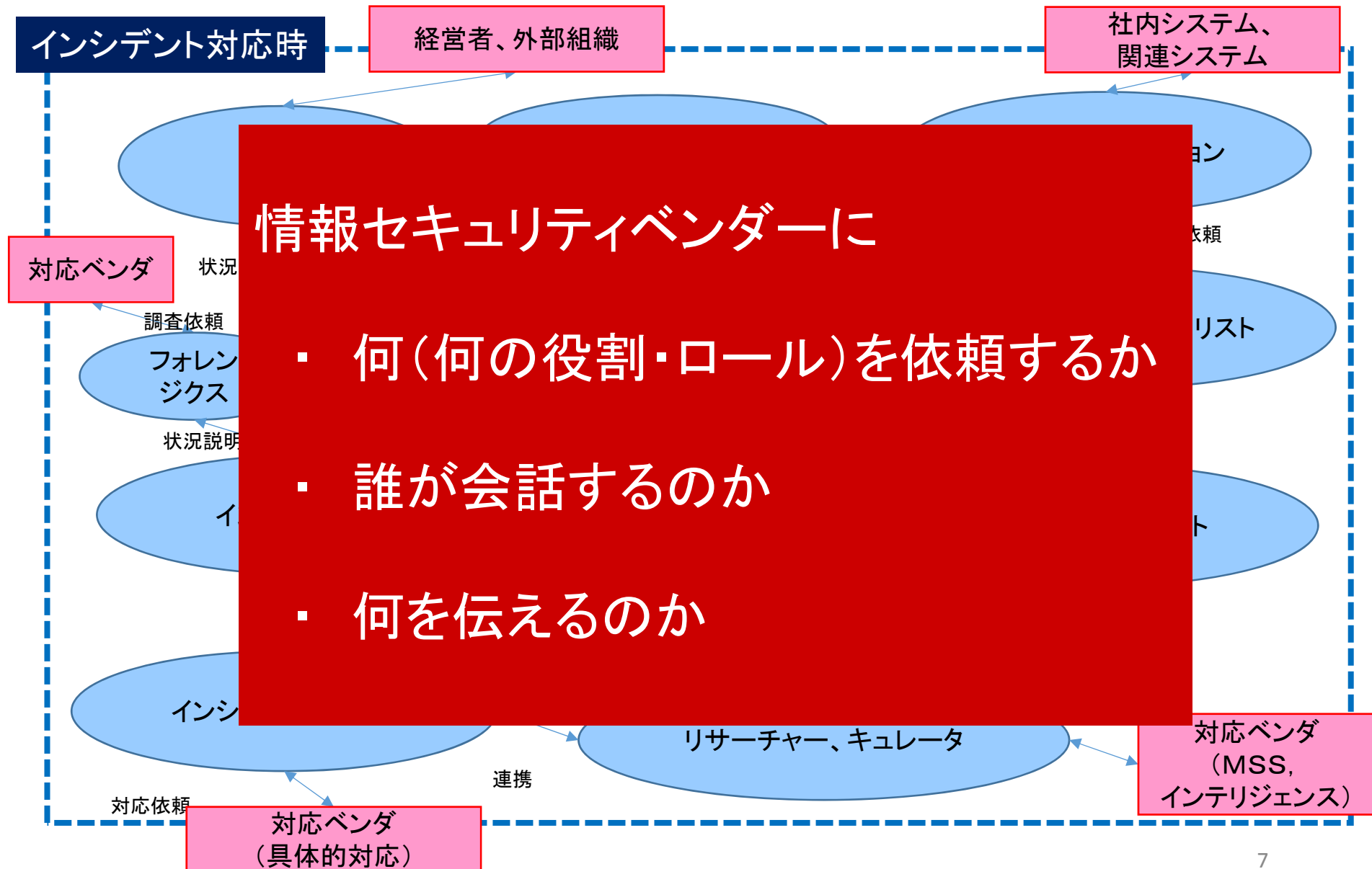
1.4 ユーザー企業内情報セキュリティ技術者の役割と関連部門

(参考) 日本シーサート協議会(NCA)における情報セキュリティ人材のタスク整理図



1.4 ユーザー企業内情報セキュリティ技術者の役割と関連部門

(参考) 日本シーサート協議会(NCA)における情報セキュリティ人材のタスク整理図



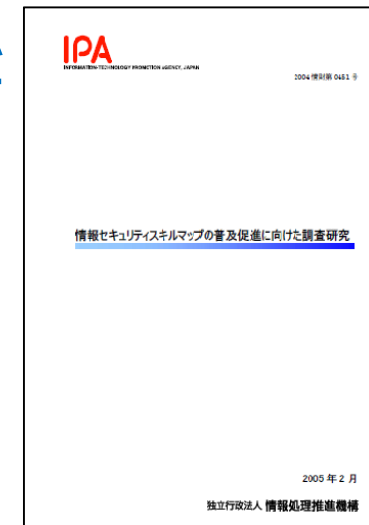
2. 何を学ぶのか？

情報セキュリティ知識分野
SecBoK (Security Body of Knowledge)
の登場

2.1 情報セキュリティ人材育成 取り組み経緯(1) **JNSA**

1) IPA様からの依頼で、2004年/2005年(修正版)と情報セキュリティスキルマップを作成

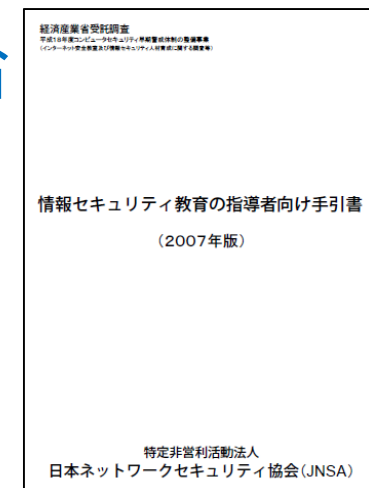
http://www.ipa.go.jp/security/fy15/reports/skillmap/documents/skillmap_2003.pdf
http://www.ipa.go.jp/security/fy16/reports/skillmap/documents/skillmap_2004.pdf



2) JNSAよりSecBoKとして名称変更し、経済産業省様受託事業のアウトプットとして公開

「情報セキュリティ教育の指導者向け手引書(2007年版)」内にある知識分野がSecBoKそのもの(P.40-P67)

<http://www.jnsa.org/result/2007/edu/materials/071111/tebiki2007.pdf>



2.2 情報セキュリティ人材育成 取り組み経緯(2) **JNSA**

3) ISEPA より、「情報セキュリティ人材アーキテクチャガイドブック」を公開

ISEPA（情報セキュリティ教育事業者連絡会）より、
2009年に人材育成ガイドを公開

http://www.jnsa.org/isepa/images/outputs/jinzai_arch_2009.pdf



4) SecBokを参考に、2009年に以下の「情報セキュリティプロフェッショナル教科書」出版

<http://ascii.asciimw.jp/books/books/detail/978-4-04-867782-0.shtml>



2.3 現行SecBoK:職種分類

情報セキュリティ人材アーキテクチャ職種別・人材育成マップ



職種	定義
1 プリセールスエンジニア	セキュリティ製品導入を検討する企業に対し、どのような環境なら顧客の要望が実現可能なのか製品・サービスに関する技術的知識を持って営業活動を支援する
2 セールスコンサルタント	顧客システムの現状の把握および課題点の調査し、顧客の状況に合わせて、適用範囲が広範囲な製品・ソリューション対策/提案をする
3 テクニカルコンサルタント	情報セキュリティに関する経験値が高く、技術的見地からのアドバイスやレビューを行う
4 セキュリティアーキテクト(製品・ソリューション)	セキュリティ製品・ソリューション開発の設計、及び管理
5 セキュリティアーキテクト(コンサル)	セキュリティ確保、情報漏洩防止等におけるコンサルティング・設計・実装および支援業務
6 セキュリティエンジニア(要求定義)	セキュリティ・ソリューションに関する要求定義を行う
7 セキュリティエンジニア(企画・設計)	セキュリティ・ソリューションの企画・設計・最新技術調査、製品評価
8 セキュリティエンジニア(基盤)	セキュリティ・システムの基盤部分(OS・ネットワーク)の全体設計・運用設計・方式設計、開発
9 セキュリティエンジニア(アプリ)	アプリケーションの開発フェーズにおいてセキュリティの確保を行う
10 セキュリティエンジニア(DB)	DBMSを構成要素とするシステムを対象に、セキュリティの確保を行う
11 QAマネージャー	品質保証業務及びそのプロセス改善業務。製品品質に関する顧客窓口業務。開発チームに対する品質保証啓蒙活動
12 QAエンジニア	ソフトウェア開発および開発プロジェクトに対し、品質保証全般のテストを実施。
13 セキュリティテスター	ソースコード解析や脆弱性の洗い出し
14 プログラマー	仕様書や設計書に従って、セキュアプログラミングの知識を持ってプログラムを作る。
15 プロジェクトマネージャー	プロジェクトの計画と実行に於いて総合的な責任を持つ。期日までに成果物を完成させる。
16 セキュリティシステムアドミニストレーター	システムに対するセキュリティ対策を整備し、運用管理を行う
17 オペレーター	提供しているサービスの運用・監視を行う。 ネットワーク監視。ヘルプデスク。サービスシステム維持管理等
18 セキュリティアナリスト	各種ログを分析し、インシデントを抽出し、予兆を発見し、対策を提示
19 フォレンジックアナリスト	証拠証拠の分析を行い、証拠保全、証拠開示手続きも行う
20 インシデントハンドラー(プロダクト)	プロダクトに確認された脆弱性の分析と関係部署との調整をおこなう
21 インシデントハンドラー(組織)	攻撃発生時のインシデント分析及び対応と関係部署との調整をおこなう
22 フィールドエンジニア	顧客現場で、セキュリティシステム構築に伴う、システム機器の設置から設定保守・修繕を行う
23 プライバシーオフィサー	企業・団体内の個人情報保護体制の構築、運用、改善を行う
24 プライバシースペシャリスト	企業の個人情報保護に関して、規定作成から意識向上施策実施までを担当する
25 CSO/CISO/CIAO	情報資産保護を経営の観点から意思決定をし、指揮をとり、組織の情報資産保護の責任をとる
26 CSO/CISO/CIAO補佐	CSO/CISO/CIAOの業務を補佐し、経営陣の意思を現場に浸透させ、施策がきちんと実行されるかを監視する
27 セキュリティプロダクトオーナー	セキュリティ製品の企画から保守にいたるまで製品に関わる全責任をとる
28 セキュリティサービスオーナー	セキュリティサービスの企画から保守にいたるまでサービスに関わる全責任をとる
29 セキュリティコンサルタント(マネジメント)	情報セキュリティ戦略立案から、情報資産の管理・運用方法の策定までに関し、顧客の問題解決を支援する。
30 セキュリティアドバイザー	情報セキュリティ全般に関してのアドバイスを行う
31 セキュリティストラテジスト	企業の経営戦略実現にむけて、セキュリティを活用した基本戦略を策定、提案、推進する
32 セキュリティ監査人	情報セキュリティ監査制度に対する知識と経験を有するとともに、実証された能力として、監査計画を立案し、監査計画に基づいて監査を実施し、報告書を作成し、監査結果を被監査主体に報告する

2.4 現行SecBoK スキルマップ大分類



項番	大分類	
1	情報セキュリティマネジメント	
2	ネットワークインフラセキュリティ	
3	アプリケーションセキュリティ	Web
		電子メール
		DNS (Domain Name System)
4	OS セキュリティ	Unix
		Windows
		セキュアOS
5	ファイアーウォール	
6	侵入検知	
7	ウイルス	
8	セキュアプログラミング技法	
9	セキュリティ運用	
10	コンテンツセキュリティ	
11	認証	
12	PKI(Public Key Infrastructure)	
13	暗号	
14	電子署名	
15	不正アクセス手法	
16	法令・規格	

中分類以下に
約600の小分
類スキル項目
から構成され
ている

2.5 IPAより、2015年6月に、「iCD2015」が発表



参照 http://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/icd.html

国際的な競争が高まる中、近年ではクラウド・モバイル・SNSなど新たなITサービスやITインフラが台頭し、企業を取り巻くビジネス環境は刻一刻と変化しています。そのためIPAでは、これらの環境変化に対応したIT人材を育成可能とするため、人材育成の枠組みを整備し活用促進を図ることで、産業界における人材育成を支援してきました。

IPAが提供する「i コンピテンシ ディクショナリ」(以下、iCD)は、企業においてITを利活用するビジネスに求められる業務(タスク)と、それを支えるIT人材の能力や素養(スキル)を「タスクディクショナリ」、「スキルディクショナリ」として体系化したもので、企業は経営戦略などの目的に応じた人材育成に利用することができます。

IPAは、2014年7月31日にiCDの試用版を公開しましたが、パブリックコメントや産業界における実証実験などを踏まえ、この度、正式版となる「i コンピテンシ ディクショナリ2015」(以下、iCD2015)を公開しました。

今回公開したiCD2015では、試用版における知識体系などの見直しに加え、“**情報セキュリティ**”、“攻めのIT”など新時代に必要な人材育成に対応したタスク・スキルを追加しています。

2.6 スキルディクショナリ(セキュリティ知識体系) **JNSA**

スキル標準、情報処理技術者試験の知識項目に加え、情報専門学科におけるカリキュラム標準、主要知識体系を参考としている。**SecBoKの追加**

スキルディクショナリ

- メソドロジ
- テクノロジ
- 関連知識

洗い出した約11000知識項目を

3 カテゴリ
78 分類
423 スキル項目
8234 知識項目
の独自体系に整理したもの

名称	発行団体
情報処理技術者試験 午前の出題範囲 (知識体系)	情報処理推進機構 (IPA)
共通キャリア・スキルフレームワーク (第一版・追補版) (CCSF) 知識体系	情報処理推進機構 (IPA)
ITスキル標準 (ITSS) V3 2011	情報処理推進機構 (IPA)
ITスペシャリスト育成ハンドブック2008年度改訂版	情報処理推進機構 (IPA)
情報システムユーザースキル標準 (UISS) Ver.2.2	情報処理推進機構 (IPA)
組込みスキル標準 (ETSS) 2008	情報処理推進機構 (IPA)
情報専門学科におけるカリキュラム標準 (J07)	情報処理学会
ビジネスアナリシス知識体系ガイド (BABOK) 第1.2版	International Institute of Business Analysis (IIBA)
要求工学知識体系 (REBOK) 第1版	情報サービス産業協会 (JISA)
Strategy and Analysis Body Of Knowledge (SABOK)	日本ITストラテジスト協会
ソフトウェア工学知識体系ガイド (SWEBOK) 2004	IEEE/ACM
プロジェクトマネジメント知識体系ガイド (PMBOK) 第4版	Project Management Institute (PMI)
ITIL (Information Technology Infrastructure Library) V3	itSMF Japan
ソフトウェア品質知識体系ガイド (SQuBOK) Ver1.0	日本科学技術連盟
データ管理知識体系ガイド (DMBOK) 第1版	DAMAインターナショナル
(ISC) ² 公式CISSP CBK	(ISC) ² Japan

情報セキュリティ知識分野 (SecBok)

JNSA

2.7 SecBoK改訂関連活動



1) SecBoKの見直しおよびアップデート

現在のSecBok内容は、2004年に作成し、その後アップデートを重ねて2009年時点の内容が公開されているが、その後のアップデートが行われていない。

現在のユーザー企業における情報セキュリティ人材不足やクラウド時代などに対応できるようなアップデートが必要と考えて、2015年度に改訂活動を実施。

2) 他協会および団体様に対してのSecBoK普及&利用促進活動

2009年よりアップデートが実施されていなかったのは、情報セキュリティ業界外への普及に問題があった点もあるため、今回のiコンピテンシ・ディクショナリ対応化に伴い、SecBokに関して、情報セキュリティ業界内にとどまらず、その他の外部協会および団体様への普及活動や情報共有活動を検討。

3. セキュリティ知識分野(SecBoK)2016

3.1 SecBoK改訂の方向性



分類	SecBoK改訂委員会での指摘事項および方針
職種	• ISEPAの32職種は多過ぎる。 • セキュリティシステムにフォーカスした上で、どのような業務・プレイヤーがいるかに絞って整理すると少なくできるのではないか。 • ビジネスモデルや業務内容に応じて、「ここにはこのような職種の人が必要」という形でまとめるとよい。
知識項目の分類	• 現行のスキルマップはベンダに偏り過ぎている。 • 新しい概念の取り込み(クラウド、仮想化、グリッド、SDNなど)が必要。 • ユーザ向け、ベンダ向けという分類ではなく、職種やタスクをベースに整理することで、企業にとらわれずに整理することができる。
考慮点	• あまり細かいものは一般企業では受け入れてもらえない。 • 組織のミッションやビジョンを組織モデルに落とし込めるように。 • 平常時とインシデント発生時の区別。 • 自社で担当するか、外部委託するか、両方に対応できるようにする。
進め方	• 「ベンダと対話できる人材」など、現在不足している職種・人材像を明らかにした上で、そうした人材の育成に役立つ成果物を検討したい。

1. ユーザー企業での利活用対応

日本国内において情報セキュリティ人材が大幅に不足していると指摘されているユーザー企業での活用に対応できるものにすべきである

2. 世界基準への対応

JNSAだけの認識ではなく、公に認知されているフレームワークを取り入れるべきである

3. 組織・ビジネスへの対応

あまり細かくなり過ぎず、かつ実際の業務フローや組織モデルを想定できるものにすべきである

3.3 他のフレームワーク

NICE: National Initiative for Cybersecurity Education とは



<http://csrc.nist.gov/nice/>

米国ではNIST (National Institute of Standards and Technology)で策定された、NICEフレームワークをベースにした各省庁での人材育成計画の策定が進むと想定されている。

フレームワークでは、サイバーセキュリティ領域を7つの大分類として整理している。



CYBERSECURITY
WORKFORCE
FRAMEWORK

3.4 米国 NICE Frameworkのカテゴリー



NICE Cybersecurity Workforce Framework では、サイバーセキュリティに関するタスクと知識を下表の7 種類のカテゴリーで分類

	カテゴリー	カテゴリーの定義	専門領域の例
I	セキュアな供給 Security Provision	システム開発の各過程に関わる、セキュアなIT システムの概念化、設計及び構築についての専門領域	システム要件検討、システム開発、ソフトウェア保証とセキュリティエンジニアリング、システムセキュリティアーキテクチャ、試験と評価、技術研究開発、情報保証コンプライアンス
II	運用・保守 Operate and Maintain	効果的かつ効率的なIT システムの性能とセキュリティを確保するために必要なサポート、アドミニストレーション及び保守に関する専門領域	システム・アドミニストレーション、ネットワークサービス、システムセキュリティ分析、カスタマーサービスと技術サポート、データ・アドミニストレーション、ナレッジマネジメント
III	守備・防衛 Protect and defend	内部のIT システムやネットワークへの脅威の識別、分析及び緩和に関する専門領域	脆弱性アセスメントと管理、インシデントレスポンス、計算機ネットワーク防御(CND)分析、計算機ネットワーク防御(CND)インフラ支援
IV	捜査 Investigate	IT システム、ネットワーク及びデジタルエビデンスに関するサイバー事象及び/または犯罪についての専門領域	捜査、デジタル・フォレンジック
V	運用・情報収集 Collect and Operate	情報活動に用いられるサイバーセキュリティ情報の情報の高度な収集に関する専門領域	情報収集オペレーション、サイバーオペレーション計画、サイバーオペレーション
VI	分析 Analyze	入手したサイバーセキュリティ情報が情報活動に有効かどうかを決定するための、高度なレビューと評価に関する専門領域	脅威分析、エクスプロイト分析、ターゲット、全情報源のインテリジェンス
VII	監督と開発 Oversight and Development	他者がサイバーセキュリティ活動を効率的に実施できるようなサポートに関する専門領域	法的助言と弁護、教育と訓練、戦略策定とポリシー開発、情報システムセキュリティオペレーション(ISSO)、最高情報セキュリティ責任(CISO)

<http://csrc.nist.gov/nice/framework/documents/NICE-Cybersecurity-Workforce-Framework-Summary-Booklet.pdf>

3.5 役割・ロール(セキュリティ専門家集団)



マルウェア アナリスト



侵入したマルウェアや使われたエクスプロイトを安全に解析し、攻撃手法の解明や対策手法の考案を行う。またシステム・ネットワーク上に残された痕跡から未知のマルウェアの検出も行える人物

フォレンジック アナリスト



インシデント時にシステム・ネットワーク上の証拠を発見、適切に証拠保全する人物

ペネトレーショ ンテスター



最新の攻撃手法を熟知し、対策方法を提案する。必要に応じて、システム・ネットワークに脆弱性が検査を計画し適切に行える人物

インシデント ハンドラー



インシデント時に素早く対応し、システム・ネットワーク運用者および管理者と連携して、対策を行い安全に復旧を行える人物

ネットワーク アナリスト



システム・ネットワークの運用、管理を行う。インシデント時の初期対応も行える人物

プロフェッショナル セールス



組織に必要なセキュリティ対策を検討、提案する上で必要な基礎知識・スキルを持ち、ビジネス戦略的観点から最適なソリューションを提案できる人物

3.6 役割・ロール(ITシステムを作る人たち)



コンサルタント

顧客ニーズを把握し、提案。顧客満足度に責任を持つ人物



プロジェクト マネジャー

業務要件、IT要件を把握し要件を定義し、プロジェクトに責任を持つ人物



ITスペシャリスト

基盤システムの設計、構築、運用、保守する人物。



アプリケーション スペシャリスト

アプリケーションシステムの設計、構築、運用、保守する人物



3.7 役割・ロール(ITを利用する人たち)



インシデントマネージャー インシデントハンドラー

インシデントの現場監督・ベンダとの連携・インシデントの処理



キュレーター・リサーチャー

インシデントの情報収集、運用しているセキュリティセンサ異常値の発見、影響分析



インベスティゲーター

外部からの犯罪、内部犯罪を捜査



リーガルアドバイザー

法律・法令に基づく支援



コマンダー・トリアージ

セキュリティ全体統括者



フォレンジックエンジニア

インシデントの原因究明や証拠発見などを行うための電子情報の分析



POC

外部との連絡窓口となり、情報連携を行う。社内窓口として社内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報連携を行う



ノーティフィケーション

社内関連部署への連絡



セルフアセスメント・

ソリューションアナリスト

リスクアセスメント、セキュリティ戦略の策定・推進

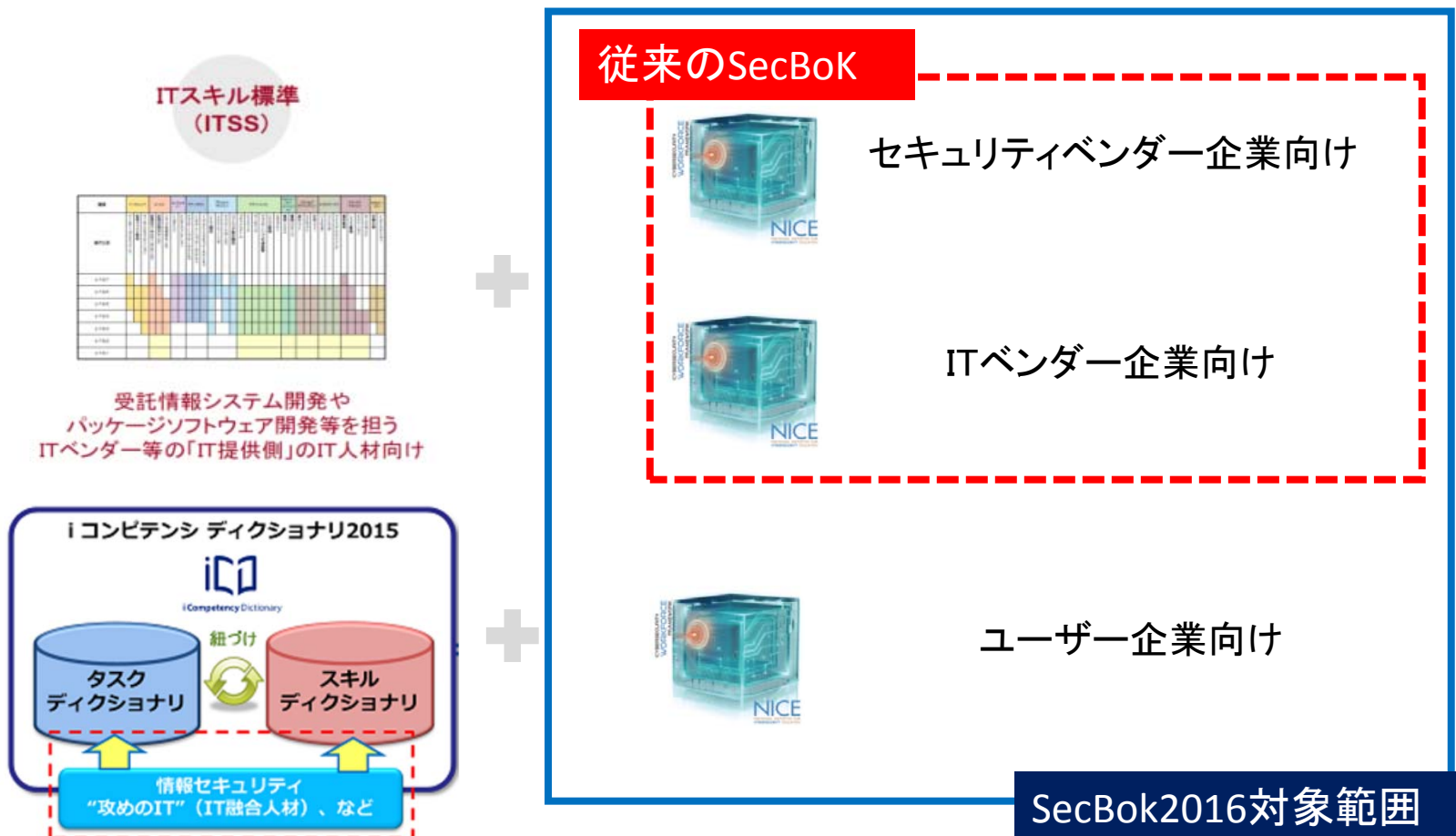


4. どの様に使うのか？

SecBoK利用例

4.1 ユーザー企業も対象としたSecBoK2016

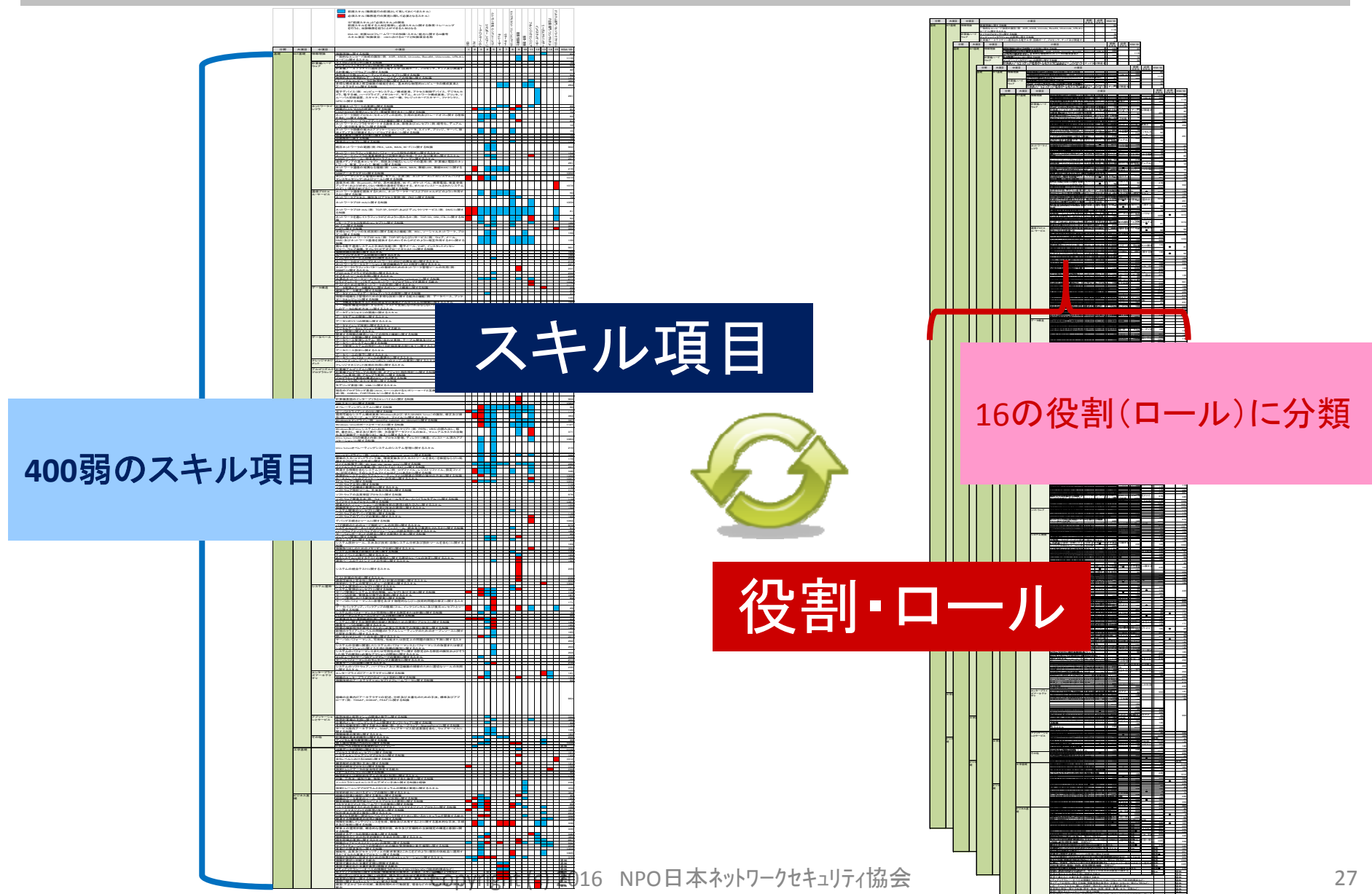
IT全般を対象にするiコンピテンシ・ディクショナリ2015(旧ITスキル標準)に、セキュリティから考えた世界基準レベルのフレームワーク「NICE」の要素をプラスして、情報セキュリティ知識分野(SecBoK)2016を本日公開



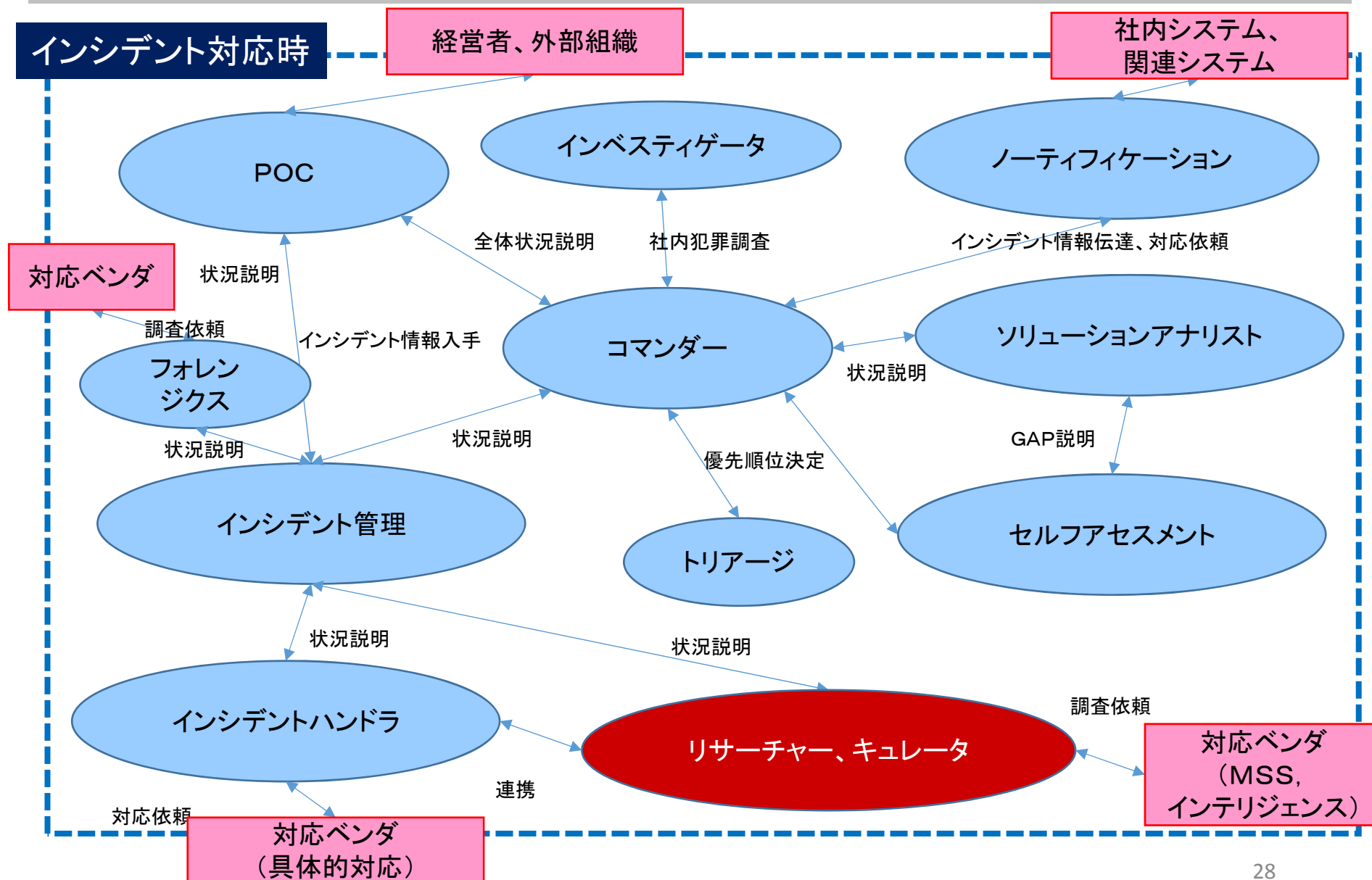
4.2 各ロールとNICEフレームワークの対応づけ例

NCAによるロール定義		NICEの専門分野		ユーザ企業職種	セキュリティベンダ職種
a	CISO	23	セキュリティプログラム管理(CISO)	(役員)	
b	POC		(なし)		
c	ノーティフィケーション		(なし)		
d	コマンダー	21	情報システムセキュリティ運用(ISSO)		
e	トリアーger	21	情報システムセキュリティ運用(ISSO)		
f	インシデント管理	15	インシデントレスポンス		インシデントハンドラー
g	インシデントハンドラー	15	インシデントレスポンス		インシデントハンドラー
h	キュレーター	14 15	計算機ネットワーク防御分析 情報保障コンプライアンス		SOCアナリスト
i	リサーチャー	14	計算機ネットワーク防御分析	ITセキュリティ部門	SOCアナリスト
j	ソリューションアナリスト	13	システムセキュリティ分析		マルウェアアナリスト/ プロフェッショナルセールス
k	セルフアセスメント	13	システムセキュリティ分析		マルウェアアナリスト/ コンサルタント
l	脆弱性診断	17	脆弱性アセスメントと管理		ペネトレーションテスター
m	教育・啓発	20	教育と訓練		(教育サービス)
n	フォレンジックス	18	デジタルフォレンジック		フォレンジックアナリスト
o	インベスティゲータ	19	捜査		フォレンジックアナリスト
p	(なし)	22	法的助言と弁護	(法務部門)	(弁護士)
q	(なし)	24	戦略策定とポリシー開発	(IT企画部門)	コンサルタント
r	(なし)	16	計算機ネットワーク防御インフラサポート	ITシステム部門	ネットワークアナリスト

4.3 SecBoK2016構成(スキルと役割・ロール)



(参考)日本シーサート協議会(NCA)における情報セキュリティ人材のタスク整理図



4.5 リサーチャー・キュレーター募集例



【サンプル】XX-CSIRT担当者募集

出典：日本シーサート協議会 CSIRT人材SWG
「CSIRT人材の定義と確保(Ver.1.0)」

<http://www.nca.gr.jp/imgs/recruit-hr20151116.pdf>

募集件名	【急募】CSIRT担当者(リサーチャー、キュレーター)
採用数	若干名
職務内容(ロール)	セキュリティログを確認し、特異点を見つけて担当にエスカレーションしてください。高齢者、第二新卒歓迎！ 典型的な職務内容(ロール)： <u>PCオペレーション</u> ヒューマンスキル： <u>緻密な作業が得意な方。会話が苦手な方も可。</u>
必要な経験、能力、資格	経験： <u>サーバ、NW構築・運用経験</u> 能力： <u>PC、Linux操作一般</u> 資格： <u>特に規定なし</u>
あると望ましい経験、能力、資格	経験： <u>サーバログ、FWログ等のログ分析経験</u> 能力： <u>持久力、集中力</u> 資格： <u>特になし</u>
導入教育	ログの分析の仕方を要領書を基に教育します。
休日・休暇	週休2日制、短時間勤務、シフト勤務も要相談。
備考	成長産業！企業のリスク回避につながる注目の仕事です！

4.6 NICEフレームワーク スキル項目とのマッピング例

分野	大項目	中項目	KSA-ID	小項目	CISO	POC	ノードファイケーション	コマンド・トリージ	インシデント管理・インシデ	リサーチヤー	リサーチヤー	脆弱性診断士	教育啓発	フォレンジックエンジニア	インベストイゲーター	リーガルアドバイザー	コンサルタント	ネットワークアナリスト	情報セキュリティ監査人
セキュリティ基礎	総論		64	情報セキュリティシステム工学の原理に関する知識															
			63	機密性、完全性、可用性、認証及び否認防止に関連する情報保証の原理と組織要件に関する知識															
			55	情報またはデータの利用、処理、蓄積及び移送に関連するリスクを管理するために用いられる情報保証の原理に関する知識															
			70	情報技術のセキュリティ原理と手法(例:ファイアウォール、非武装地帯、暗号化)に関する知識															
			77	標準に基づいたセキュリティ能力を用いた、情報技術のセキュリティ評価、観測、検知及び対応に関する現在の産業界の手法に															
			156	機密性、完全性及び可用性の原則の適用に関するスキル															
			302	ハードウェア、OS及びネットワーク技術を調査することの意味に関する知識															
			320	サイバーセキュリティ問題に関する外部組織と学術機関に関する知識															
セキュリティガバナンス	総論		952	出現するセキュリティ問題、リスク及び脆弱性に関する知識															
			38	組織の企業情報セキュリティアーキテクチャシステムに関する知識															
			300	インテリジェンスの報告原理、方針、手続き及び手段(報告書式、報告基準(例:要件と優先順位)、拡散の実践および法執行機関ならびに制約に関する知識															
			965	組織のリスク受容および/またはリスク管理のアプローチに関する知識															

400弱のスキル項目

4.7 スキルマップ案（キュレター例）

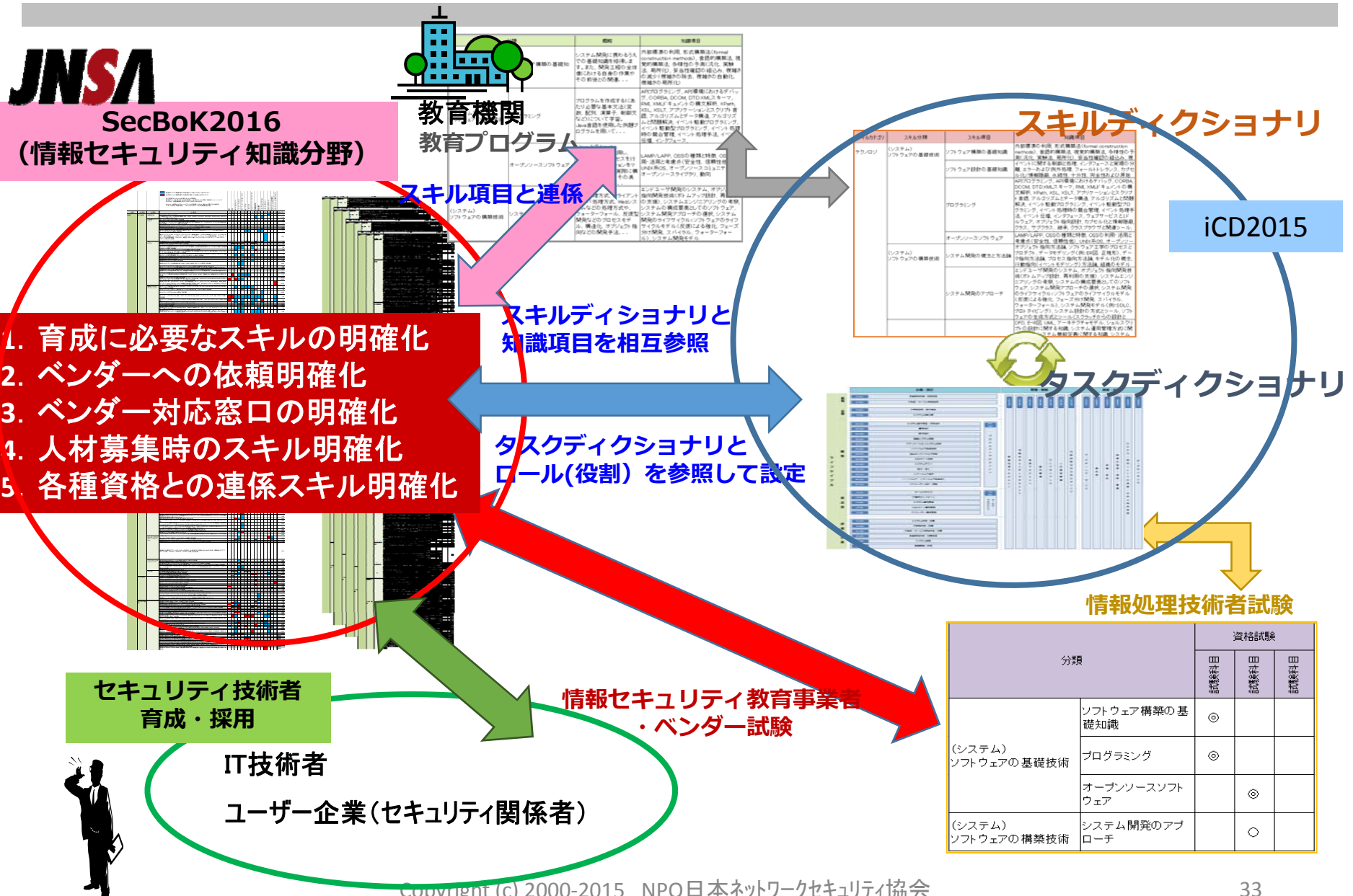


分野	大項目	中項目	KSA-ID	小項目
基礎	ICT基礎	通信プロトコル・サービス	50	ネットワーク通信を提供するために、ネットワークサービスとプロトコルがどのように作用するかに関する知識
			81	ネットワークプロトコル(例: TCP/IP, DHCP)およびディレクトリサービス(例: DNS)に関する知識
		システム運用	29	データバックアップ、バックアップの種類(フル、インクリメンタル)及び復元コンセプトとツールに関する知識
	ビジネス基礎		897	損失評価の実施に関するスキル
セキュリティマネジメント	総論		984	計算機ネットワーク防御のポリシー、手続きおよび規制に関する知識
ネットワークセキュリティ	総論		893	ネットワーク通信のセキュア化に関するスキル
			150	何がネットワーク攻撃及び脅威と脆弱性の双方への関係を構成するかに関する知識
			1072	トポロジー、プロトコル、構成要素及び原理を含むネットワークセキュリティアーキテクチャのコンセプト(例: 真相防御のアプリケーション)に関する知識
	トラフィック解析		87	ネットワークトラフィック解析手法に関する知識
			93	パケットレベル解析に関する知識
システムセキュリティ	総論		66	侵入検知技術を通じたホスト及びネットワークベースの侵入を検知するための侵入検知手法と技術に関する知識
			105	システムとアプリケーションのセキュリティ上の脅威と脆弱性(例: バッファオーバーフロー、モバイルコード、クロスサイトスクリプティング、PL/SQ及びインジェクション、競合状態、秘密の通信路、リプレイ、リターン指向攻撃、悪意のコード)に関する知識
	総論		1033	基本的なシステム管理、ネットワーク及びOSのハードニングに関する知識
セキュリティシステム設計・構築	インシデント対応		60	インシデントのカテゴリ、インシデントレスポンス及び応答のタイムラインに関する知識
			61	インシデントレスポンスとハンドリングの方法論に関する知識
	その他		923	セキュリティイベントの関連ツールに関する知識
サイバー攻撃手法	総論		1069	一般的な攻撃ステージ(例: フットプリンティング及びスキャン、列挙、アクセス権取得、特権の昇格、追跡回避)に関する知識
			895	脆弱性の種類と関連する攻撃の認知とカテゴリ化に関するスキル
			153	マルウェアの取扱いに関するスキル
	マルウェア		896	マルウェアからのネットワークの保護に関するスキル
			1029	マルウェア解析のコンセプトと手法に関する知識
	その他		991	攻撃クラスの相違(例: 受動的、能動的、内部、近接、分散)に関する知識
			992	運用上の脅威環境の違い(例: 第一世代(スクリプトキディ)、第二世代(非政府機関による支援)、第三世代(政府機関による支援)に関する知識
			217	標準の運用手続きまたは国内標準に関する証拠の完全性の維持に関するスキル
デジタルフォレンジック	総論		217	標準の運用手続きまたは国内標準に関する証拠の完全性の維持に関するスキル
レンジック			217	標準の運用手続きまたは国内標準に関する証拠の完全性の維持に関するスキル
レンジック			217	標準の運用手続きまたは国内標準に関する証拠の完全性の維持に関するスキル
レンジック			217	標準の運用手続きまたは国内標準に関する証拠の完全性の維持に関するスキル

16の役割(ロール)に分類

5. SecBoKのiコンピテンシ・ディクショナリ との関係による有効利用案

5.1 SecBoK採用によるメリットとその運用



SecBoK: **Security** **Body** **of** **Knowledge**

