# 「セキュリティ知識分野（SecBok）人材スキルマップ」

## ～誰を育てるのか？　どう育成するのか？～

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

# 自己紹介：NPO日本ネットワークセキュリティ協会(JNSA)
# 教育部会　部会長　平山 敏弘（ひらやま としひろ）

【活動概要】

入社以来，UNIX を中心とした以下の分野などの分散システムにおけるシステムデザインおよびシステム構築作業を数多く経験.

・ホームセキュリティシステム
・ナレッジマネジメント/メールシステム
・コンビニエンスストア情報端末システム
・Web システム，商用インターネットシステム

現在，上級 IT スペシャリストとして、クラウドコンピューティングのソリューション提案やサーバー仮想化統合および IT 基盤成熟度診断・事業継続に関するコンサルティングを中心に活動中．大規模システムにおけるシステム要求分析やシステムデザインも数多く経験.

一方，情報セキュリティや IT キャリアパスなどに関する講義を複数の大学および大学院で非常勤講師として実施するなど，産学連携教育に関する活動も実施している.

【受賞暦】

2013 年アジア太平洋情報セキュリティ・リーダーシップ・アチーブメント（ISLA）・アジアンアワード受賞

【協会・学会活動】

・経済産業省
　元情報セキュリティ人材育成指標策定事業委員会　委員
・独立行政法人　情報処理推進機構（IPA）
　新 IT スキル標準（iCD）推進協議会　委員
・NPO 日本ネットワークセキュリティ協会(JNSA)
　産学情報セキュリティ人材育成検討会　委員
・情報処理学会　学会システム WG 委員会　委員

【大学・大学院活動】

専修大学ネットワーク情報学部　兼任講師
岡山理科大学総合情報学部　非常勤講師
中央大学大学院理工学研究科　兼任講師
名古屋大学情報科学研究科/工学部　非常勤講師
産業技術大学院大学　プログラム開発委員会　委員

【大学・大学院講義実績】

「情報セキュリティ概論～便利と脅威～」　中央大学
「ビジネスモデルの変革に大きな影響を与える IT 技術」　名古屋大学・佐賀大学
「即戦力を考える」　岐阜大学
「情報リスク管理」　専修大学
「情報セキュリティ」　岡山理科大学
「ビジネスコミュニケーション」　北陸先端科学技術大学院

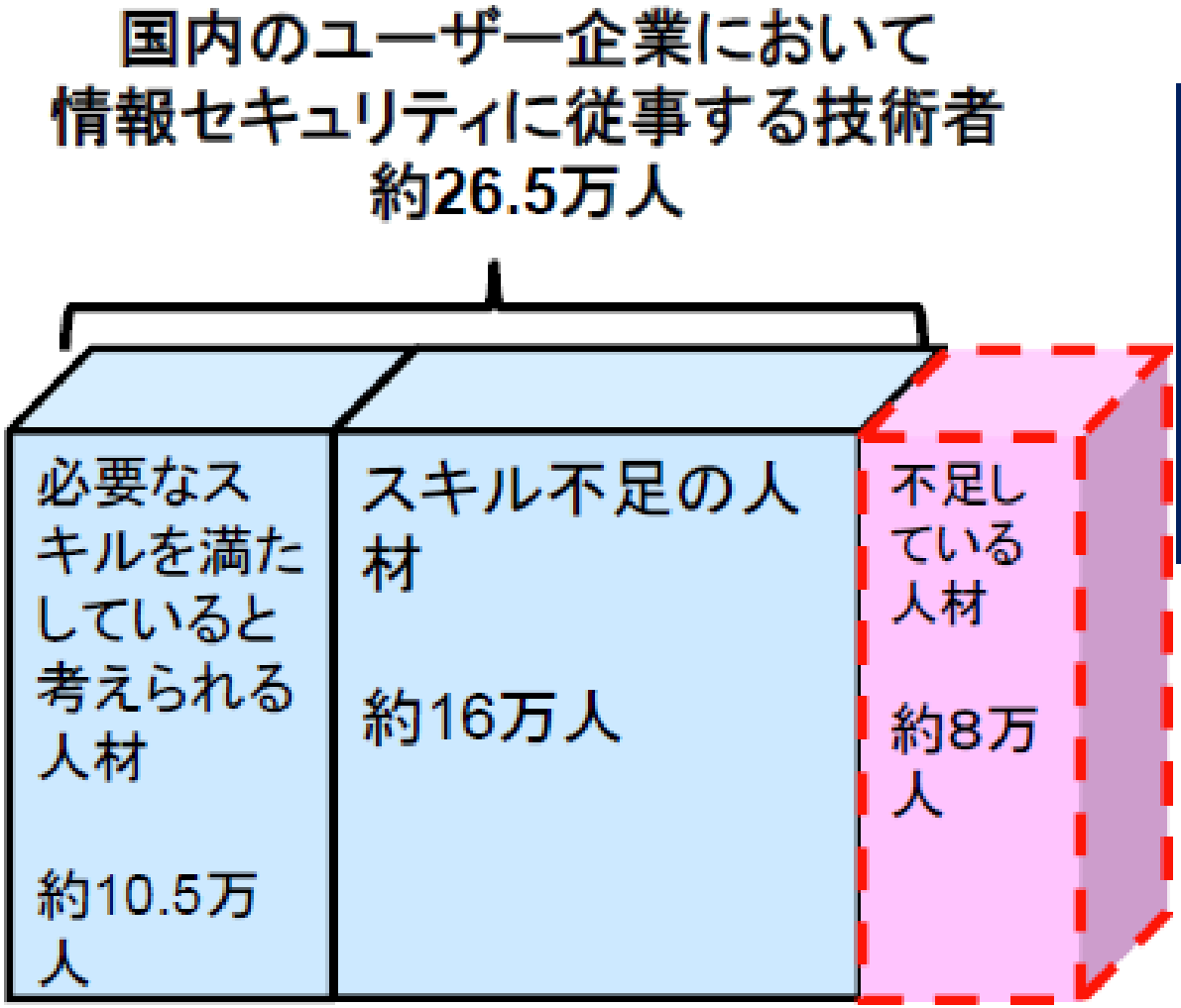
【対外発表】

「クラウド時代に求められる IT 部門の役割　～ITスキル標準からiコンピテンシ・ディクショナリ時代へ～」
　第 25 回 iSUC(全国 IBM ユーザー研究会連合会)大会

# 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？




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？

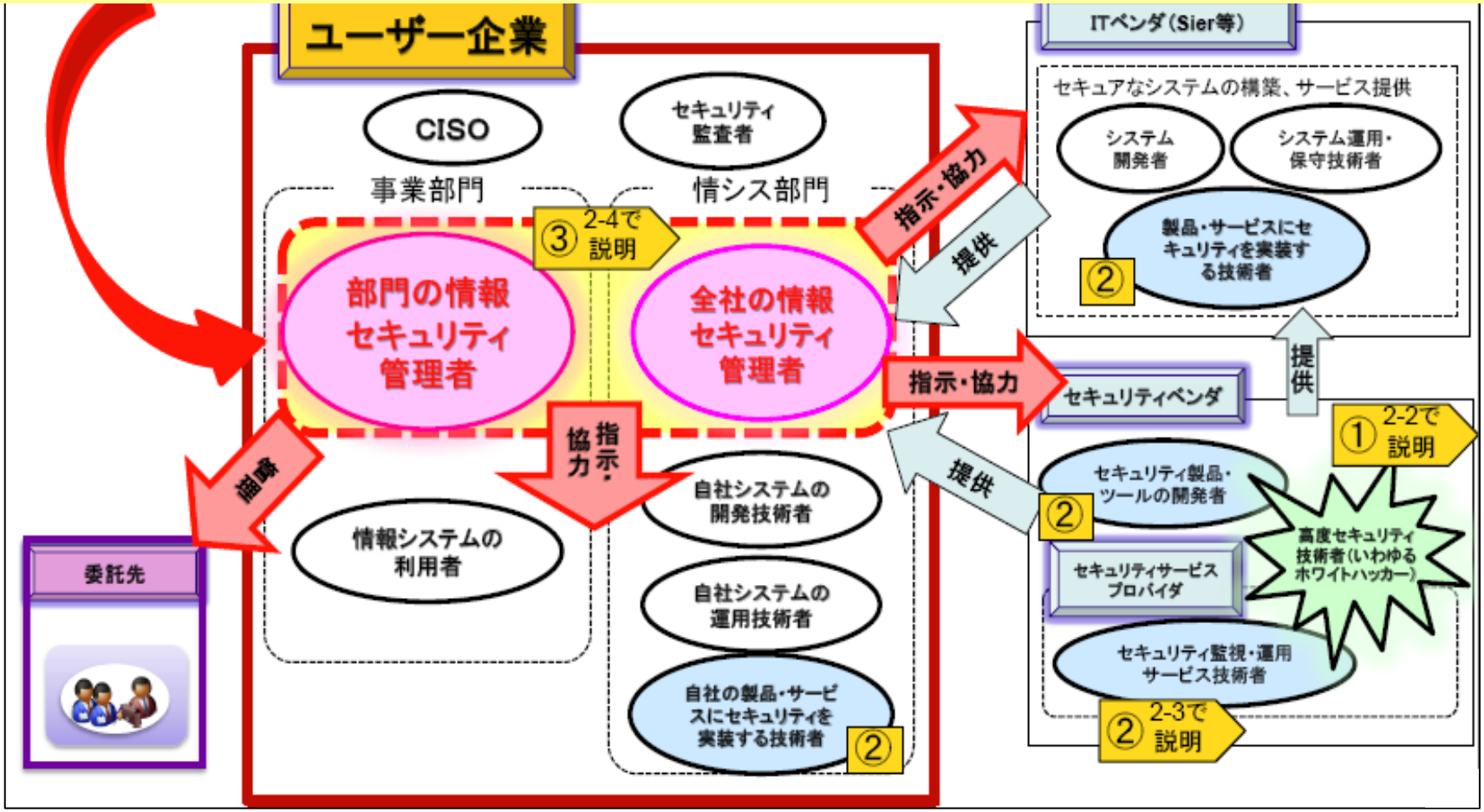
## 約8万人の業種別内訳

| 業種 | （人）<br>不足数 |
|---|---|
| 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。

# 1.3　今後必要となるセキュリティ人材像とは？

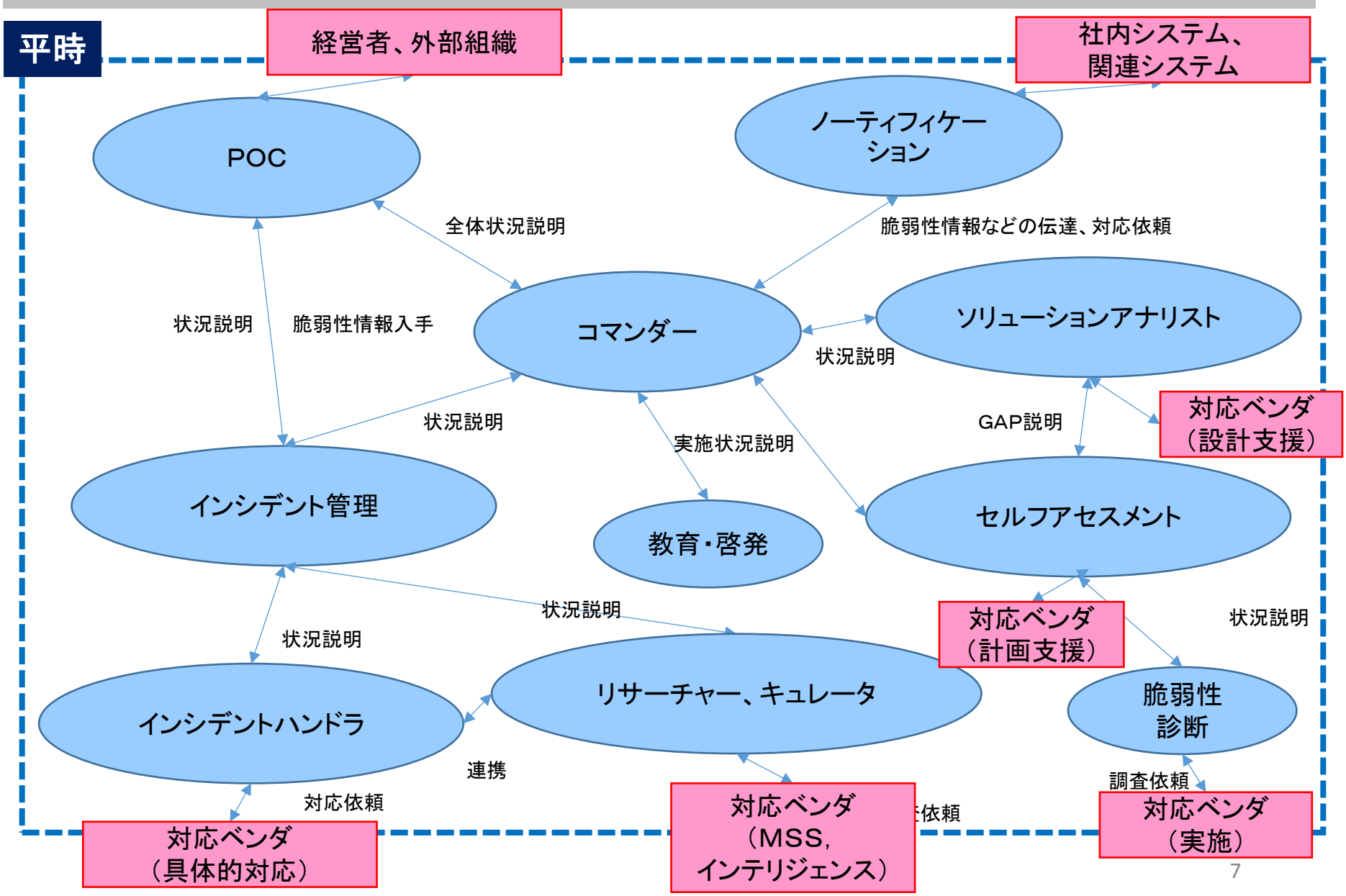
①ホワイトハッカーのような高度セキュリティ技術者
②安全な情報システムを作るために必要なセキュリティ技術を身につけた人材
③ユーザー企業において、社内セキュリティ技術者と連携して企業の情報セキュリティ確保を管理する人材。




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

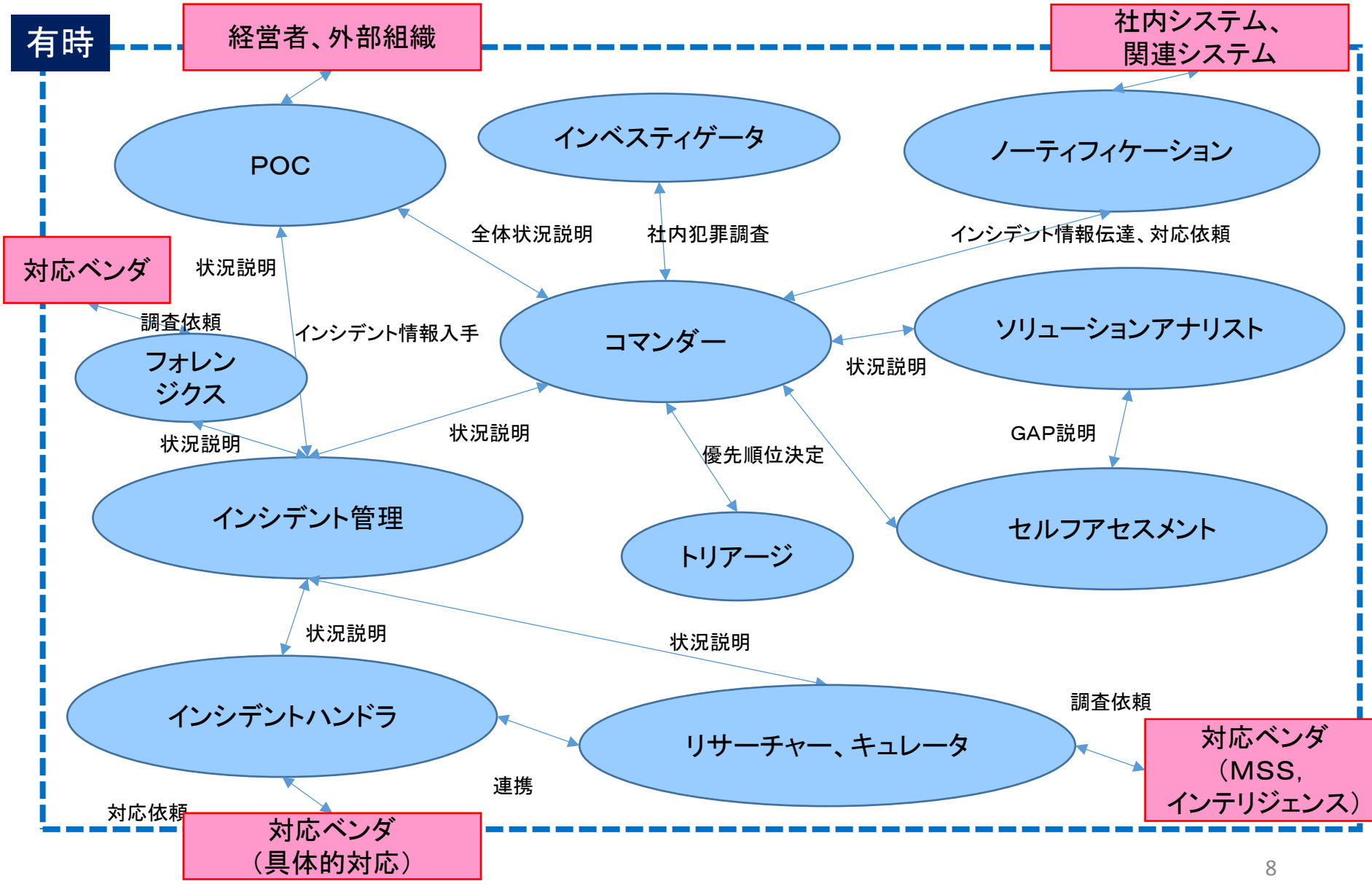
# 1.4　ユーザー企業内情報セキュリティ技術者の役割と関連部門

（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



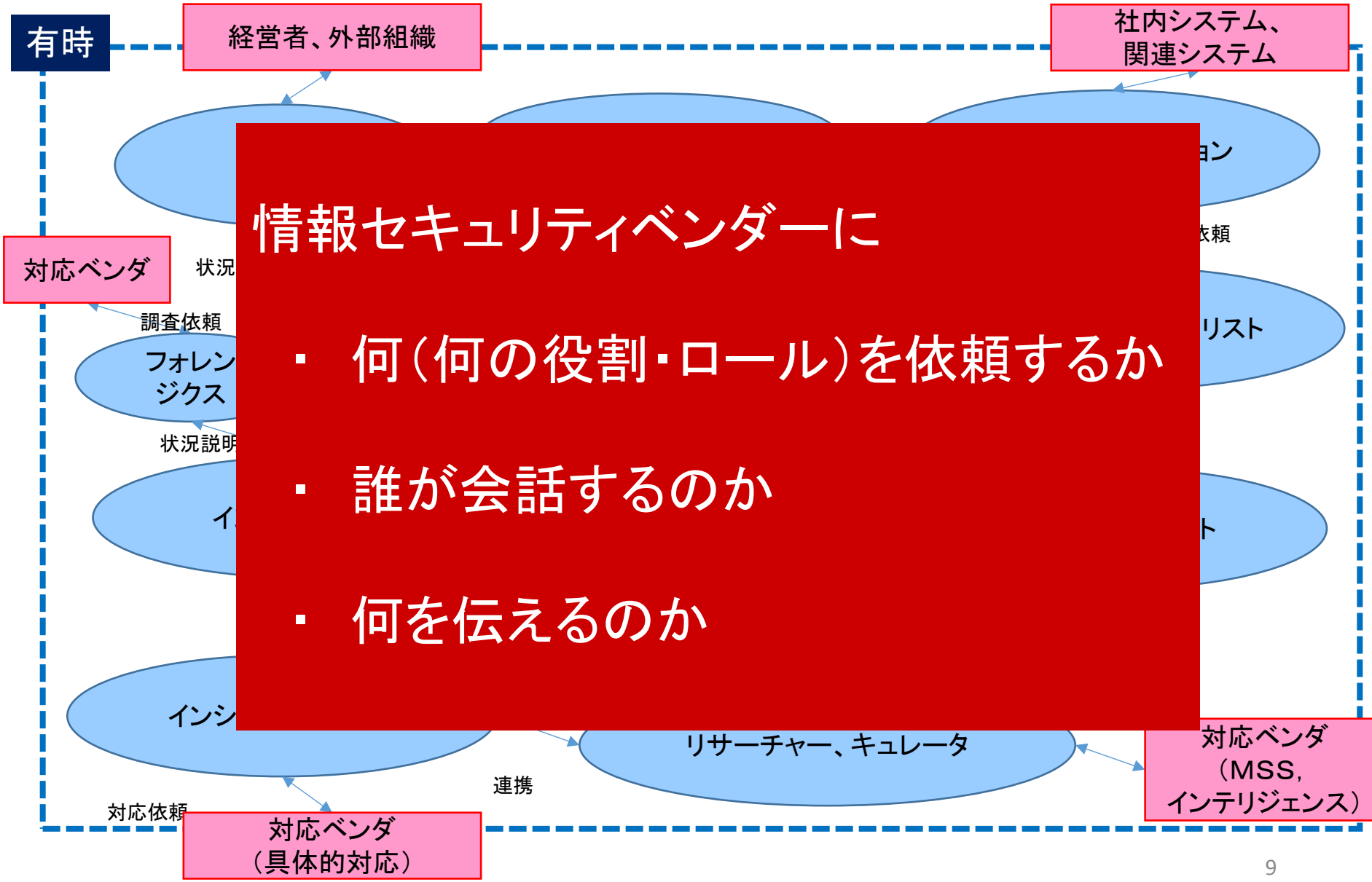
# 1.5　ユーザー企業内情報セキュリティ技術者の役割と関連部門

（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



# 1.6　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



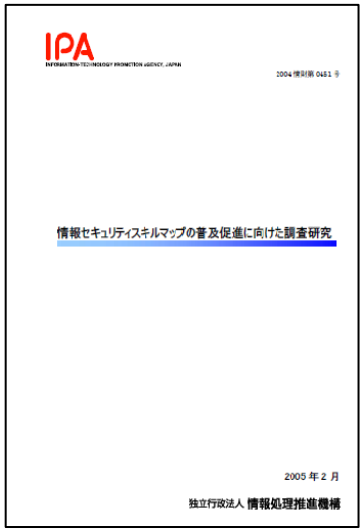
# ２．何を学ぶのか？

# 情報セキュリティ知識項目 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）

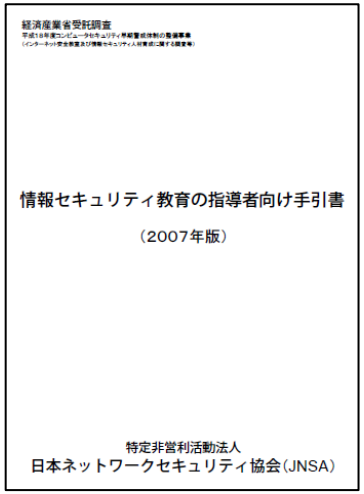
## 1）　IPA様からの依頼で、2004年/2005年（修正版）と情報セキュリティスキルマップを作成

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）」内にある知識項目が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)

## 3） ISEPA より、「情報セキュリティ人財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財アーキテクチャ職種別・人材育成マップ

JNSA

| | 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問題点の調査し、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。<br>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 | 証拠証跡の分析を行い、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処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・修理を行う |
| 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（マネージメント） | 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と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）

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項目（SecBok）** | **JNSA** |

# 2.7 JNSA教育部会 2015年度SecBoK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．セキュリティ知識項目（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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 平常時とインシデント発生時の区別。<br>• 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。 |

# 3.2　SecBoK2016への改訂方針

## 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るべきである

# 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。

# 3.4　米国 NICE Frameworkのカテゴリー

NICE Cybersecurity Workfoce 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 種類のカテゴリで分類

| | カテゴリ | カテゴリの定義 | 専門領域の例 |
|---|---|---|---|
| I | セキュアな供給<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>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）

## インシデントハンドラー
インシデントの現場監督・ベンダとの連携

## 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
社内内偵

## 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
脆弱性を悪用した攻撃が実際に有効であることを検証し、社内・社外への説明

## 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、脆弱性対応

# ４．どの様に使うのか？

## SecBoK利用例

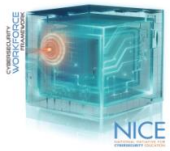
# 4.1　ユーザー企業も対象としたSecBoK2016

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項目（SecBoK）2016を公開（近日公開予定）

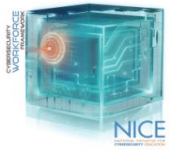
ITスキル標準
（ITSS）

受託情報システム開発や
パッケージソフトウェア開発等を担う
ITベンダー等の「IT提供側」のIT人材向け

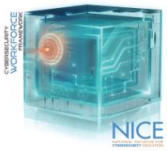

従来のSecBoK




セキュリティベンダー企業向け




ITベンダー企業向け



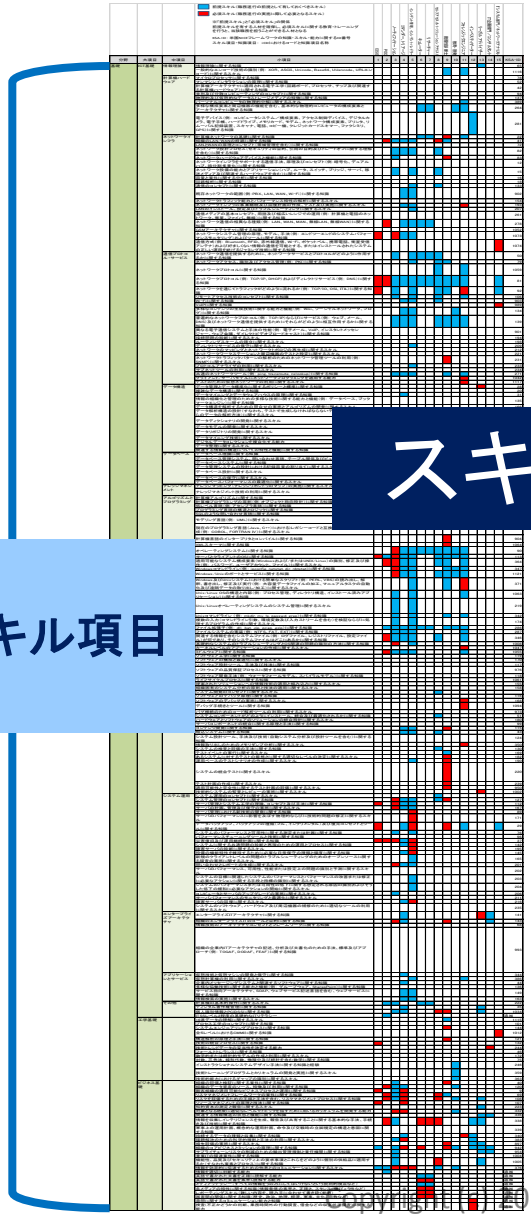

ユーザー企業向け

SecBok2016対象範囲

# 4.2 各ロールとNICEフレームワークの対応づけ案

| 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） | ITセキュリティ部門 | |
| 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 | トリアージ | 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 | 15 | インシデントレスポンス | | インシデントハンドラー |
| i | リサーチャー | 14 | 計算機ネットワーク防御分析 | | マルウェアアナリスト |
| 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 |
| 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 |
| 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）



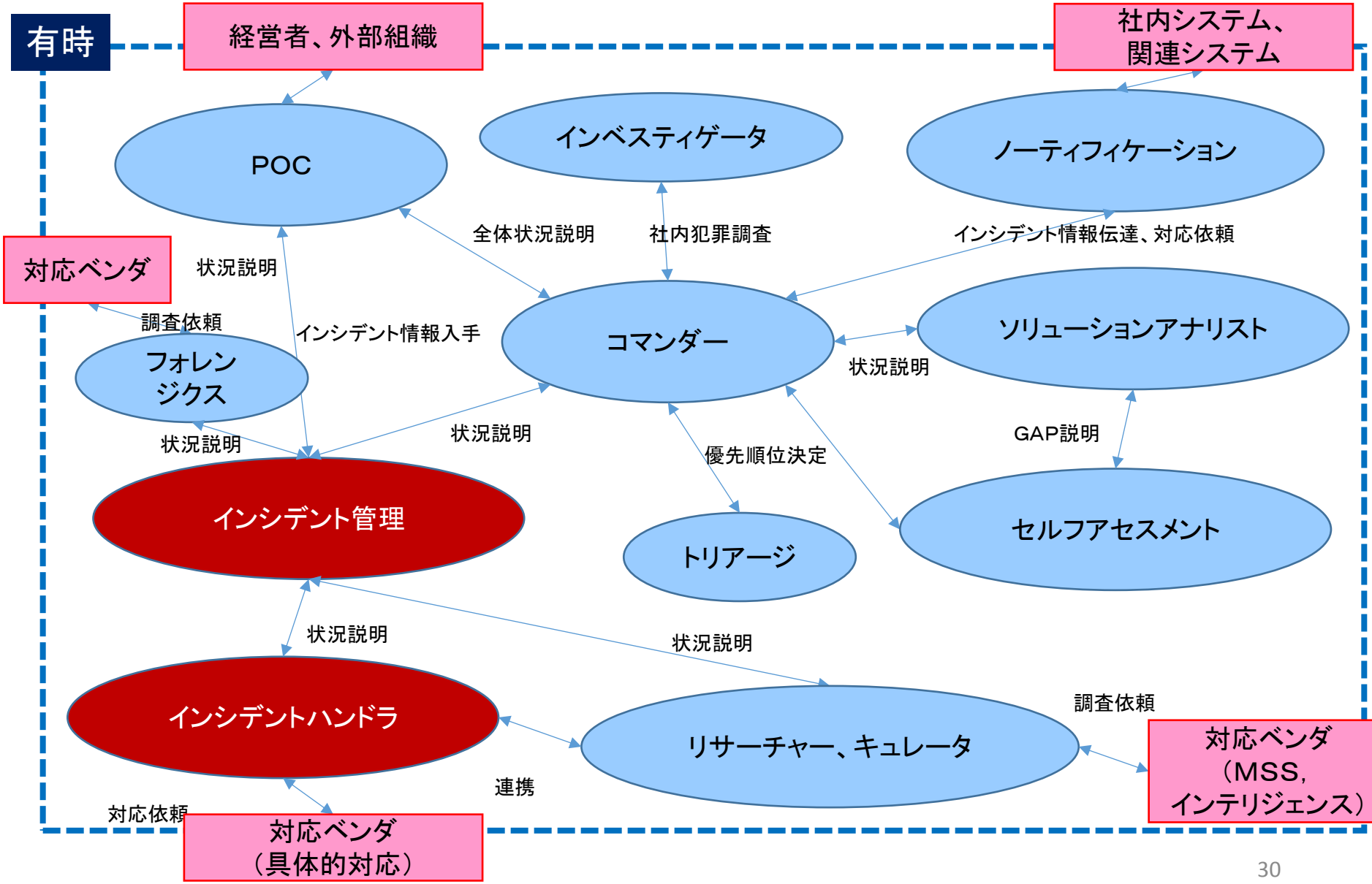
400弱のスキル項目

スキル項目

役割・ロール

15の役割（ロール）に分類

# 4.4 インシデントハンドラ・インシデント管理技術者育成活用例



# 4.5　NICEフレームワーク　スキル項目とのマッピング例

前提スキル（職務遂行の前提として有しておくべきスキル）

必須スキル（職務遂行の実施に際して必要となるスキル）

※「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

KSA-ID：米国NICEフレームワークの知識・スキル・能力に関するID番号
スキル項目・知識項目：　iCDにおけるコードと知識項目名称

| 分野 | 大項目 | 中項目 | 小項目 | 1 CISO | 2 POC | 3 ノーティフィケーション | 4 コマンダー、トリアージ | 5 インシデント管理、インシデントハンドラー | 6 キュレーター | 7 リサーチャー | 8 セルフアセスメント・ソリューションアナリスト | 9 脆弱性診断士 | 10 教育・啓発 | 11 フォレンジックエンジニア | 12 インベスティゲーター | 13 リーガルアドバイザー | 14 IT企画部門／コンサルタント | 15 ITシステム部門／ネットワークアナリスト | KSA-ID |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 基礎 | ICT基礎 | システム運用 | システム運用のコンセプトに関するスキル | | | | | | | | ■ | | | | | | | | |
| | | | システム管理のコンセプトに関する知識 | | | ■ | ■ | ■ | | | ■ | ■ | | | | | | | 127 |
| | | | サーバ管理とシステム工学の理論、コンセプト及び手法に関する知識 | ■ | | ■ | ■ | ■ | | | | | | | | | | | 112 |
| | | | サーバの計画、管理及び保守の実施に関するスキル | | | ■ | ■ | ■ | | | | | | | | | | | 167 |
| | | | サーバ管理における新技術の開発に関する知識 | | | | | ■ | | | | | | | | | | | 89 |
| | | | サーバのパフォーマンスに影響を及ぼす物理的ならびに技術的問題の修正に関するスキル | | | | | ■ | | | | | | | | | | | 171 |
| | | | 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 | ■ | | | ■ | ■ | | | | ■ | | ■ | | | | ■ | 29 |
| | | | システムのパフォーマンスと可用性に関する測定または計器に関する知識 | | | ■ | | ■ | | | | | | | | | | | 76 |
| | | | パフォーマンスチューニングツールと技術に関する知識 | | | | | | | | | | | | | | | | 96 |
| | | | 災害復旧及び運用継続計画に関する知識 | ■ | ■ | ■ | ■ | ■ | | | | | | | | | | | 37 |
| | | | システムに関する共通問題の診断と再現のための運用とプロセスに関する知識 | | | | ■ | ■ | | | | | | | | | | | 142 |
| | | | 障害サ | | | | | ■ | | | | | | | | | | | 195 |
| | | | 設備の | | | | ■ | ■ | | | | | | | | | | | 145 |
| | | | 新規の のオープンソースに関する調査の実施に関するスキル | | | | | ■ | | | | | | | | | | | 165 |
| | | | 問い合わせとレポートの生成に関するスキル | | | ■ | ■ | ■ | | | | | | | | | | | 201 |
| | | | サーバのパフォーマンス、可用性、性能または設定上の問題の識別と予測に関するスキル | | | | | | | | | | | | | | | | 202 |
| | | | システムの目標に関連したシステムのパフォーマンスとパフォーマンスの改善または修正に必要なアクションに関する手段と指標の識別に関するスキル | | | | | ■ | | | | | | | | | | | 203 |
| | | | システムのパフォーマンスまたは可用性の低下に関する想定される原因の識別およびそうした低下の緩和に必要なアクションの開始に関するスキル | | | | | ■ | | | | | | | | | | | 204 |
| | | | コンピュータとサーバのアップグレードの実施に関するスキル | | | ■ | | | | | | | | | | | | | 206 |
| | | | サーバパフォーマンスのモニタリングと最適化に関するスキル | | | | | | | | | | | | | | | | 211 |
| | | | 障害サーバの回復に関するスキル | | | | ■ | ■ | | | | | | | | | | | 216 |
| | | | システムのソフトウェア、ハードウェア及び周辺機器の補修のために適切なツールの利用に関するスキル | | | | | | | | | | | | | | | | 235 |

**400弱のスキル項目**

# 4.6 スキルマップ案 （インシデント管理・ハンドラー例）

| 分野 | 大項目 | 中項目 | 小項目 | 前提スキル | 必須スキル | KSA-ID |
|---|---|---|---|---|---|---|
| 基礎 | ICT基礎 | 情報理論 | 情報理論に関する知識 | | | 65 |
| | | | 一般的なエンコード技術の識別（例： XOR、ASCII、Unicode、Base64、UUencode、URLエンコード）に関するスキル | | | 1116 |
| | | 計算機ハードウェア | マイクロプロセッサに関する知識 | | | 78 |
| | | | マンマシンインタラクションの原理に関する知識 | | | 52 |
| | | | 計算機アーキテクチャに適用される電子工学（回路ボード、プロセッサ、チップ及び関連する計算機ハードウェア）に関する知識 | | | 42 |
| | | | 並列及び分散コンピューティングのコンセプトに関する知識 | | | 94 |
| | | | 物理的及び仮想的なデータストレージメディアの特徴に関する知識 | | | 137 |
| | | | パーソナルコンピュータの物理的分解に関するスキル | | | 389 |
| | | | 多様な構成要素と周辺機器の機能を含む、基本的な物理的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 | | | 264 |
| | | | 電子デバイス（例： コンピュータシステム／構成要素、アクセス制御デバイス、<br>メラ、電子手帳、ハードドライブ、メモリカード、モデム、ネットワーク構成要素、<br>ムーバル記録装置、スキャナ、電話、コピー機、クレジットカードスキマー、ファ<br>GPS）に関する知識 | | | |
| | | ネットワークインフラ | 計算機ネットワークの基礎に関する知識 | | | |
| | | | 組織のLAN/WANの経路に関する知識 | ● | | 41 |
| | | | LANとWANの原理とコンセプト（帯域管理を含む）に関する知識 | | | 72 |
| | | | ネットワーク設計プロセス（セキュリティの目的、引用の目的及びトレードオフに関する理解を含む）に関する知識 | ● | | 82 |
| | | | ネットワークハードウェアデバイスと機能に関する知識 | | | 83 |
| | | | ネットワークインフラをサポートする通信手法、原理及びコンセプト（例：暗号化、デュアルハブ、時分割多重化）に関する知識 | | | 12 |
| | | | ネットワーク設備の能力とアプリケーション（ハブ、ルータ、スイッチ、ブリッジ、サーバ、移送メディア及び関連するハードウェアを含む）に関する知識 | ● | | 15 |
| | | | 容量と要件に関する分析に関する知識 | | | 16 |
| | | | 回路解析に関する知識 | | | 18 |
| | | | 通信のコンセプトに関する知識 | ● | | 133 |
| | | | 既存ネットワークの範囲（例：PBX、LAN、WAN、Wi-Fi）に関する知識 | ● | | 902 |

15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連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

JNSA

教育プログラム

IT技術者

タスクディクショナリと
ロール(役割）を参照して設定

教育機関

| 分類 | | 概要 | 知識項目 |
|---|---|---|---|
| （システム）ソフトウェアの基礎技術 | ソフトウェア構築の基礎知識 | システム開発に携わるうえでの基礎知識を修得。また、開発工程の全体像における自身の作業やその前後との関連・・・ | 外部標準の利用、形式構築法（formal construction methods）、言語の構築法、視覚的構築法、多様性の予測（汎化、実験法、局所化）、妥当性確認の組込み、複雑さの減少（複雑さの除去、複雑さの自動化、複雑さの局所化） |
| | プログラミング | プログラムを作成するにあたり必要な基本文法（変数、配列、演算子、制御文など）について学習。Java言語を使用した例題プログラムを用いて・・・ | APIプログラミング、API環境におけるデバッグ、CORBA、DCOM、DTD,XMLスキーマ、RML、XMLドキュメントの構文解析、XPath、XSL、XSLT、アプリケーションとスクリプト言語、アルゴリズムとデータ構造、アルゴリズムと問題解決、イベント駆動プログラミング、イベント駆動型プログラミング、イベント処理時の競合管理、イベント処理手法、イベント伝播、インタフェース、 |
| | オープンソースソフトウェア | Linux上でApache、MySQL、PHPを利用し、データベースアクセスを行うWebアプリケーションをプログラミング実習を通して実際に構築することにより、その具体的技術を習得。・・・ | LAMP/LAPP、OSSの種類と特徴、OSSの利用・活用と考慮点（安全性、信頼性他）、UNIX系OS、オープンソースコミュニティ、オープンソースライブラリ、動向 |
| （システム）ソフトウェアの構築技術 | システム開発のアプローチ | 集中処理方式、クライアントサーバ処理方式、Webシステムなどの処理方式や、ウォーターフォール、反復型開発などのプロセスモデル、構造化、オブジェクト指向などの開発方法論（UP2 (2) UML、 | エンドユーザ開発のシステム、オブジェクト指向開発技術（ボトムアップ設計、再利用の支援）、システムエンジニアリングの考察、システムの構成要素としてのソフトウェア、システム開発アプローチの選択、システム開発のライフサイクル：ソフトウェアのライフサイクルモデル（反復による強化、フェーズ分け開発、スパイラル、ウォーターフォール）、システム開発モデル |

タスクディクショナリ

連係

スキルディショナリ
と連係

| 大分類 | 中分類 | 小分類 |
|---|---|---|
| | | |

1. 育成に必要なスキルの明確化
2. ベンダーへの依頼明確化
3. ベンダー対応窓口の明確化
4. 人材募集時のスキル明確化
5. 各種資格との連係スキル明確化

スキルディショナリと
知識項目を相互参照

| スキルカテゴリ | スキル分類 | スキル項目 | 知識項目 |
|---|---|---|---|
| テクノロジ | （システム）ソフトウェアの基礎技術 | ソフトウェア構築の基礎知識 | 外部標準の利用、形式構築法（formal construction methods）、言語の構築法、視覚的構築法、多様性の予測（汎化、実験法、局所化）、妥当性確認の組込み、構 |
| | | ソフトウェア設計の基礎知識 | イベントに関する制御と処理、インタフェースと実現の分離、エラーおよび例外処理、フォールトトレランス、カプセル化/情報隠蔽、永続性、十分性、完全性および原始 |
| | | プログラミング | APIプログラミング、API環境におけるデバッグ、CORBA、DCOM、DTD,XMLスキーマ、RML、XMLドキュメントの構文解析、XPath、XSL、XSLT、アプリケーションとスクリプト言語、アルゴリズムとデータ構造、アルゴリズムと問題解決、イベント駆動プログラミング、イベント駆動型プログラミング、イベント処理時の競合管理、イベント処理手法、イベント伝播、インタフェース、ウェブサービスとドキュメント、オブジェクト指向設計、カプセル化/情報隠蔽、クラス、サブクラス、継承、クロスブラウザと関連ツール、 |
| | | オープンソースソフトウェア | LAMP/LAPP、OSSの種類と特徴、OSSの利用・活用と考慮点（安全性、信頼性他）、UNIX系OS、オープンソース |
| | （システム）ソフトウェアの構築技術 | システム開発の概念と方法論 | オブジェクト指向方法論、ソフトウェア工学のプロセスとプログラム、データモデリング（例:ERD図、正規形）、データ指向方法論、プロセス指向方法論、モデル化の概念、行動指向（イベントモデリング）方法論、組織のモデル、 |
| | | システム開発のアプローチ | エンドユーザ開発のシステム、オブジェクト指向開発技術（ボトムアップ設計、再利用の支援）、システムエンジニアリングの考察、システムの構成要素としてのソフトウェア、システム開発アプローチの選択、システム開発のライフサイクル：ソフトウェアのライフサイクルモデル（反復による強化、フェーズ分け開発、スパイラル、ウォーターフォール）、システム開発モデル（例:SDLC、プロトタイピング）、システム設計の方式とツール、ソフトウェアの生成方式とツール（スクラッチからの設計と、 |
| | | | OFD, E-R図, UML, アーキテクチャモデル, シェルスクリプトの設計に関する知識, システム運用管理方式に関する知識, システム機能定義に関する知識, システム |

スキルディクショナリ

情報処理技術者
試験

SecBoK2016
（情報セキュリティ知識項目）

JNSA

情報セキュリティ教育事業者
・ベンダー試験

| 分類 | | 資格試験 | | |
|---|---|---|---|---|
| | | 情報処理技術者試験 | 情報セキュリティマネジメント試験 | 初級シスアド試験 |
| （システム）ソフトウェアの基礎技術 | ソフトウェア構築の基礎知識 | ◎ | | |
| | プログラミング | ◎ | | |
| | オープンソースソフトウェア | | ◎ | |
| （システム）ソフトウェアの構築技術 | システム開発のアプローチ | | ○ | |

# SecBoK：

Coming Soon


# ありがとうございました！