

情報セキュリティ資格保有者のあり方

- ISEPAでの活動を通しての考察 -

2010年2月15日(月)
ISEPA運営委員 / スキルWGリーダー
衣川 俊章

アジェンダ

- ・ ISEPAのご紹介
- ・ 高度情報セキュリティ人材の定義
- ・ 高度情報セキュリティ人材育成・活用の現状と課題
- ・ 資格の有効活用
- ・ 今後に向けての提言

情報セキュリティ教育事業者連絡会 (ISEPA)の紹介

和文 情報セキュリティ教育事業者連絡会
英文 Information Security Education Providers Association
略称 ISEPA
URL <http://www.jnsa.org/isepa/>
設立 2007年10月1日

- ・ 情報セキュリティ人材育成を通して、より豊かな情報社会に貢献する
- ・ 情報セキュリティ教育事業者が協業することにより、情報セキュリティ人材育成に関わる情報を広く社会に発信するとともに、人材育成の拡大に向けた様々な取り組みを推進する
- ・ 教育機関とも連携し有益なコンテンツの共同利用などを検討する

ISEPAが目指すもの

- ・ 分かりやすい教育体系・資格制度の公開
- ・ 求められるセキュリティ人材の安定育成への挑戦
- ・ 情報セキュリティ人材による社会貢献のサポート
- ・ まだ見ぬ後輩達がセキュリティ業界に夢を持てる環境構築への挑戦

NISC
内閣官房
情報セキュリティ
センター

総務省

経済産業省

広報、後援、
講師派遣等
各種支援
オブザーブ

情報セキュリティ教育事業者連絡会

参加団体

ISACA、(ISC)2、インフォセック、SANSジャパン、
NTTコムチェオ、NTT - LS、CompTIA、SEA/J、
KKC情報システム、ソフトピア、JASA、ラック、
ひょうご情報教育機構、RHC、CISCO、SAAJ、JTP

活動内容(案)

普及活動、情報共有・各種提携・共通領域の策定
分野/レベル別教育・コンサル・資格者育成/登録
ケーススタディの蓄積 教材作成

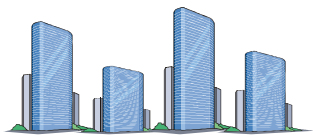
事務局：
JNSA

教育機関

情報セキュリティ大学院大学
カーネギーメロン大学日本校
工学院大学
サイバー大学
東京電機大学 等

情報共有・後援等依頼中
アドバイザー協力要請

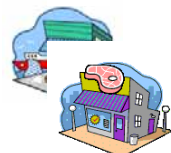
人材育成計画の支援
人材の紹介・斡旋



政府機関・地方公共団体

企業

有資格者による
バーチャルコンサル
(簡易相談)



中小企業

人材育成セミナー
カテゴリ別セミナー
(CISO、担当者等)
資格取得相談



セキュリティ人材候補

情報共有
講師候補・育成
キャリア登録



高度セキュリティ人材

「高度情報セキュリティ人材」の定義

「高度ICT人材」

(2) 我が国において求められる高度ICT人材像(育成目標とするICT人材像)

<中略>

社会、経済等の諸課題について、自ら発掘し、ICTを活用して解決できる人材

(職種イメージ:非ICT企業(ストラテジスト等)、ICT企業(コンサルタント等))

高度、複雑で、大規模なプロジェクトを適切に遂行するためのコミュニケーション能力とリーダーシップを有する人材

(職種イメージ:プロジェクトマネージャ等)

諸課題解決を実行するため新たなICT製品・技術(アプリケーション、データベース、ネットワーク、各種プログラム等)を開発等できる人材

(職種イメージ:ICT企業(ITアーキテクト、組み込みソフトウェア・ソフトウェアエンジニアリング等スペシャリスト等)、非ICT企業(ISアーキテクト、アプリケーションデザイナー・システムデザイナー等スペシャリスト))

ハード・ソフトに関わらず多様な汎用のICT製品・技術を組み合わせ、ネットワークやシステムの構築ができる人材

(職種イメージ:ICT企業(ITアーキテクト、組み込みソフトウェアスペシャリスト等)、非ICT企業(ISアーキテクト等))

海外のICT人材と適切なコミュニケーションを取り、業務を遂行できる人材

(職種イメージ:プロジェクトマネージャ、ブリッジSE等)

ICTの利活用により大きな社会的インパクトや高い経済的な付加価値を創造できる人材

(職種イメージ:非ICT企業(CIO、ストラテジスト等)、ICT企業(CIO、コンサルタント等))

「高度ICT人材育成に関する研究会報告書 - 我が国を支える高度ICT人材の自律的な育成メカニズムの構築に向けて - 」～ 総務省、平成20年5月

「高度デジタル人財」

高度デジタル人財について

デジタル技術は、パソコン、携帯端末、自動車、家電、産業機器等から産業・行政・社会の基幹システムに至るまで活用され、個人の生活や企業・行政等の活動に欠かせないものとなっており、経済社会全体を支えている。これを支える人財が、**デジタル技術を理解し・活用し、高い付加価値を創造できる高度デジタル人財**であり、具体的には以下のような人財をいう。

新しいテクノロジーやイノベーションを創造できる人財

ユーザー企業等のCIO に代表される、デジタル技術のみならず、経営や業務改革など幅広い知識と知見を有する人財

大規模・複雑化する情報システム・ソフトウェアを構築するためのアーキテクチャやシステム設計力を有する人財

難度の高い情報システム・ソフトウェアを使いやすく、高信頼なものとして実現に導くプロジェクトマネジメント能力を有する人財

高度なソフトウェアエンジニアリング能力を有する人財

高度な知識を持った情報セキュリティ人財

デジタル技術と業務の両方に精通し、新しい事業・サービスを創造できる人財

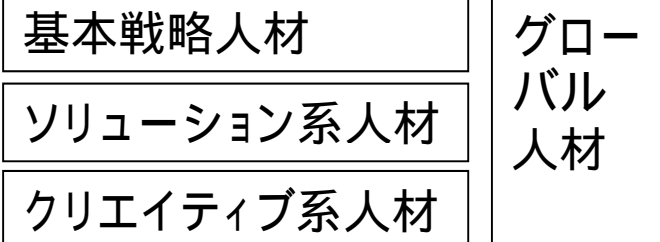
いずれの人財も英語を活用可能で、国際的にも通用する力量を持つ。

「i-Japan 戦略2015～国民主役の「デジタル安心・活力社会」の実現を目指して」～内閣官房 IT 戦略の今後の在り方に関する専門調査会、平成21年6月30日

「高度IT人材」

- ・ 今後の我が国がめざすべき高度IT人材は、**経営における付加価値を創造する基本戦略系人材**、**信頼性や生産性の向上を実現するソリューション系人材**、**技術イノベーションを創造するクリエイション系人材**の3つに大別され、どの分野においても、グローバルに活躍できる人材が求められる。
- ・ 今後のIT人材像
 - ・ **構造変化に対応し、変革をリードできる人材**が必要

ITと経営の融合
ITアーキテクチャの変貌
グローバル標準化



「高度IT人材を目指して」～総務省 産業構造審議会、情報経済分科会情報サービス・ソフトウェア小委員会
人材育成ワーキンググループ報告書案 平成19年4月

高度情報セキュリティ人材育成・活用 の現状と課題

日本政府の取り組み

我が国の成長力・競争力の強化を図るため、情報通信分野の専門的人材を育成する研修事業に対し、当該事業に必要な経費の一部を助成すること目的に「**情報通信人材研修事業支援制度**」を実施している。また、企業等における戦略的情報化を担う人材を育成するため、**実践的育成手法であるPBL (Project Based Learning) 教材 (情報セキュリティマネジメント分野を含む。)**を開発している。加えて、横須賀テレコムリサーチパークにおいて、**情報セキュリティ技術も対象にした「YRP情報通信技術研修**」に取り組むなど、情報通信分野の人材育成に取り組んできているところであるが、より一層の取組の強化が期待される。

「高度ICT人材育成に関する研究会報告書 - 我が国を支える高度ICT人材の自律的な育成メカニズムの構築に向けて -」～総務省、平成20年5月

日本政府の取り組み

1. **高度IT人材の具体像(キャリアとスキル)の可視化、共有化**
 - ・めざすべき高度IT人材像を、基本戦略系、ソリューション系、クリエイション系に区分し、必要なスキルを明確化
 - ・人材キャリアを7段階に区分し、ミドルレベル(3段階)までは、情報処理技術者試験の合否によりレベルを判定
2. **実践的かつ先端的な人材育成手法の確立、実践**
 - ・ソフトウェア工学手法、モデリング手法等、実践的かつ先端的なソフトウェア開発・管理手法を確立、普及
 - ・大学等において、ダブル・メジャー教育(文系or理系+IT)を推進
 - ・創造性に富んだ優れた人材(天才クリエイター)を早期発掘するとともに、その起業を支援
3. **客観性の高い人材評価メカニズムの構築**
 - ・情報処理技術者試験と人材スキル標準の統合により、客観的な人材評価メカニズムを構築
 - ・情報処理技術者試験において、広く社会人一般に求められる基礎的な知識を問うエントリー試験を創設
4. **我が国発の人材育成・評価システムの国際展開**
 - ・アジア統一IT試験の拡充強化を図るとともに、アジア諸国におけるIT人材育成を支援
 - ・プロジェクト・マネジメント手法やソフトウェア技術者認証方法、組込み人材育成手法の国際標準化を推進
5. **高度IT人材育成のための推進体制づくり**
 - ・高度IT人材育成のロードマップと行動計画の策定、高度IT人材育成手法の開発を行う**産学官協議会**を設置
 - ・ストラテジストやアーキテクトなど、各専門分野の高度IT人材による**自立的なコミュニティ活動を支援**
 - ・企業の若手幹部技術者候補を対象とし、最先端のIT教育を英語で行うITスーパー学校の創設を検討

「高度IT人材を目指して」～総務省 産業構造審議会、情報経済分科会情報サービス・ソフトウェア小委員会
人材育成ワーキンググループ報告書案 平成19年4月

民間での取り組み

例えば、ISEPAには16社・団体が加盟 - 下記以外でも多数の企業が様々なレベルの教育、資格を提供している

- ・ (ISC)2 Japan
- ・ ISACA (情報システムコントロール協会) 東京支部
- ・ 株式会社 インフォセック
- ・ NRIセキュアテクノロジーズ株式会社 (SANS JAPAN事務局)
- ・ NTTラーニングシステムズ株式会社
- ・ 株式会社ケーケーシー情報システム
- ・ CompTIA (コンピュータ技術産業協会)
- ・ シスコシステムズ合同会社
- ・ SEA/J (セキュリティ・エデュケーション・アライアンス・ジャパン)
- ・ 財団法人ソフトピアジャパン
- ・ 日本サード・パーティ株式会社
- ・ NPO日本システム監査人協会
- ・ NPO日本セキュリティ監査協会 (JASA)
- ・ 財団法人ひょうご情報教育機構 (カーネギーメロン大学日本校)
- ・ 株式会社ラック
- ・ リコー・ヒューマンクリエイティブ株式会社 リコー情報セキュリティ研究センター

先導的ITスペシャリスト育成推進プログラム」とは 文部科学省が特に認定した大学院段階の高度IT人材育成プログラム

【平成19年度】（情報セキュリティ分野）

大学間や産学の壁を越え、情報セキュリティ分野での世界最高水準の人材を育成する教育拠点の形成を支援する。

実施期間：2007年度～2010年度

国公私立大学10件のうち2件(国立1, 私立1)が採択

★ 社会的ITリスク軽減のための情報セキュリティ技術者・管理者養成(IT Keys)

拠点校：奈良先端科学技術大学院大学

<http://it-keys.naist.jp/>



★ 研究と実務融合による高度情報セキュリティ人材育成プログラム(ISSスクエア)

拠点校：情報セキュリティ大学院大学

<http://iss.iisec.ac.jp/>



ISSスクエア - 人材育成ターゲット

以下のような情報セキュリティ人材の育成をターゲットにしています。

➤ 高度情報セキュリティ実践リーダー

情報セキュリティ全般の確実な知識を持ち、企業活動や国の安心・安全を確保する観点から、実社会の正確な状況認識のもとに、CIO/CISOとして組織の情報政策をリードできる人材

➤ 高度情報セキュリティ研究・開発者

情報セキュリティ全般の知識を備え、優れた基礎能力をベースに問題の本質を把握し、場当たりでない抜本的な情報セキュリティ対策や基盤技術を創出・先導できる人材

修了者には情報セキュリティ・スペシャリスト・サーティフィケート (ISS Certificate) が授与。毎年、3研究科で合計30～40名程度の高度情報セキュリティ人材育成を予定

海外での政府施策

政策面においても、日本以外の国においては、技術開発における政府資金の活用やその民間移転の仕組み、情報セキュリティ人材の育成のための施策が展開されていることが判明しました

- ・ 米国の情報セキュリティ関連政策は、
 - 連邦政府情報セキュリティマネジメント法 (FISMA3) という法律を元に、国立標準技術研究所 (NIST4) が基準やガイドラインを制定。行政管理予算局 (OMB5) が実施推進。米国会計検査院 (GAO6) と議会が報告と監査、と権限の分離が体系化されている
 - NISTの基準に基づく実施基準等は官民共同で開発、その技術が民間でも活用されることでセキュリティ対策が推進される構造がある
 - 更に、情報セキュリティに特化した奨学金制度や、政府機関での活用等、人材育成にも政策支援が行われている
- ・ 欧州においては、例えばドイツでは国立研究所の開発成果を背景にしたベンチャー起業も活発で、大学での人材育成にも注力している
- ・ 韓国では過去に国産技術の奨励策が取られ、現政権下では人材育成予算措置が取られる等、政府の積極的関与が見られる

情報セキュリティ産業の構造に関する基礎調査 ~ IPA

米国での取り組み

- ・ CIOユニバーシティ：既存の大学と協力して運営しており、CIOの持つべき能力として定義された「クリンガー・コーエン・コア・コンピタンス」に従い必要な知識を学んでいる。このコースは、単に勉強するだけではなく、最終的にCIOカウンスルによるコース終了の認定まで行う仕組みになっている

クリンガー・コーエン・コア・コンピタンス

1.0	ポリシーと組織	2.0	リーダーシップ/経営
3.0	プロセスマネジメント / 変更マネジメント	4.0	情報資源戦略 / 計画
	成果評価:モデルと手法	5.0	
6.0	プロジェクトマネジメント / プログラムマネジメント		
7.0	資産計画と投資評価	8.0	調達
9.0	電子政府/電子ビジネス / 電子商取引		
10.0	ITセキュリティ/情報の保証	11.0	技術的事項
12.0	デスクワークで使うITツール		

インドでの取り組み

IT労働力開発イニシアチブ

- ・IT業界が必要とするスキルセットを学生に獲得させるため、産業界と学界によるフォーラムを開催
- ・欧米企業も含む複数の企業によるファカルティ・トレーニングの実施
- ・特定企業と特定大学によるメンターシップ

国家IT人材スキル登録制度

- ・20以上の企業の協働による、人材DBの構築
- ・個人情報の保護に留意しつつ、第三者が認証した客観的なスキル情報の開示を可能にする制度。

競争力評価制度(産業界主導)

- ・7つの異なるスキルセットについての認定制度を試験的に創設。企業や地方政府、大学が参加。今後、参加機関の試験実施の適正性を審査の後、全国レベルの正式制度として発足。

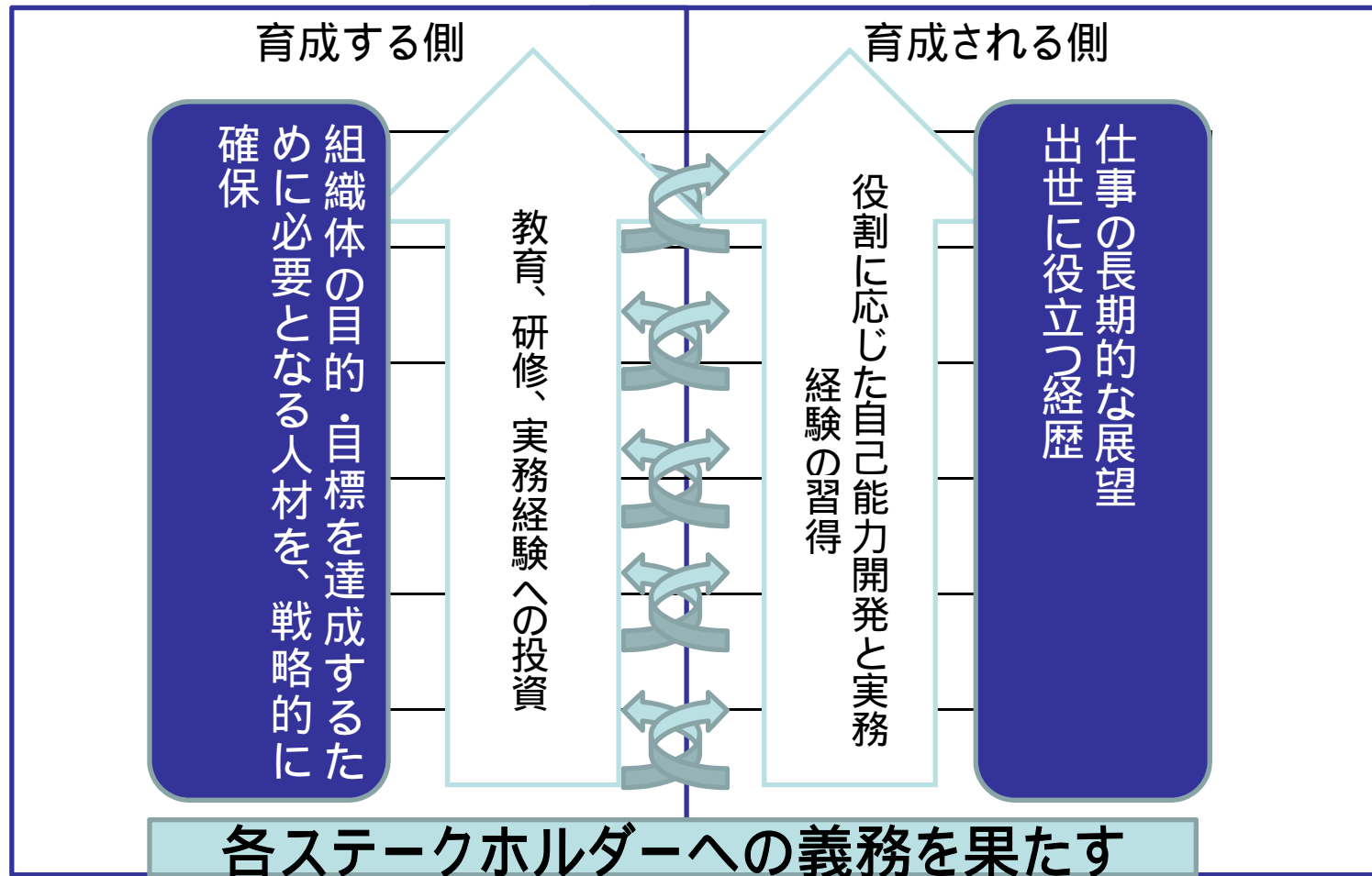
第一線マネージャ育成認証制度

- ・中堅幹部級の認証制度についても複数の企業、コンサルタント会社との連携で開始予定。

情報セキュリティ人材育成の課題

- ・ 人材育成方法が不明確
「セキュリティの人材育成方法・手法が分からない」
「教育・資格の評価の仕方が分からない」
「産学の連携不足」
- ・ 資格制度や教育が多数
「自分にはどの資格が適切か分からない」
- ・ 資格の位置づけやキャリアパス形成の共通認識の必要性
「自身の保有資格のレベル感が分からない」
「CISO / CSOになる為のパスが見えない」
「教育・資格がどうキャリアに反映されるか分からない」
「そもそもキャリアパスがあるのか」 などなど

経営戦略と人材育成戦略の融合が必要不可欠



これからの情報セキュリティ人材政策

第3章 今後3年間に取り組む重点政策

第1節 対策実施4領域における取組みの推進と政策目的の着実な実現

(1) 対策実施4領域 企業

(ウ) 企業における情報セキュリティ人材の育成・確保

情報セキュリティ人材の目指すキャリアパスを考慮に入れることも重要である。こうしたことを踏まえ、官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。また、産学連携による高度情報セキュリティ人材を育成するためのカリキュラム整備や教員強化、インターンシップの充実等に取り組むための体制を整備する。

また、技術者向けの情報セキュリティに係るモデルキャリア開発計画の策定や専門家コミュニティへの支援を進めることで、広く企業の情報セキュリティを担うことのできる人材の育成・確保に取り組む。

出展：「第2次情報セキュリティ基本計画」より抜粋 ～ 内閣官房情報セキュリティセンター (NISC)

これからの情報セキュリティ人材政策

第1章 第1次情報セキュリティ基本計画(2006～2008年度)に基づく取組みと評価について
第2節 第1次基本計画の3年間(2006～2008年度)を通じた施策の取組みと評価
(1) 施策の取組みによる社会的変化に関する評価・分析・課題

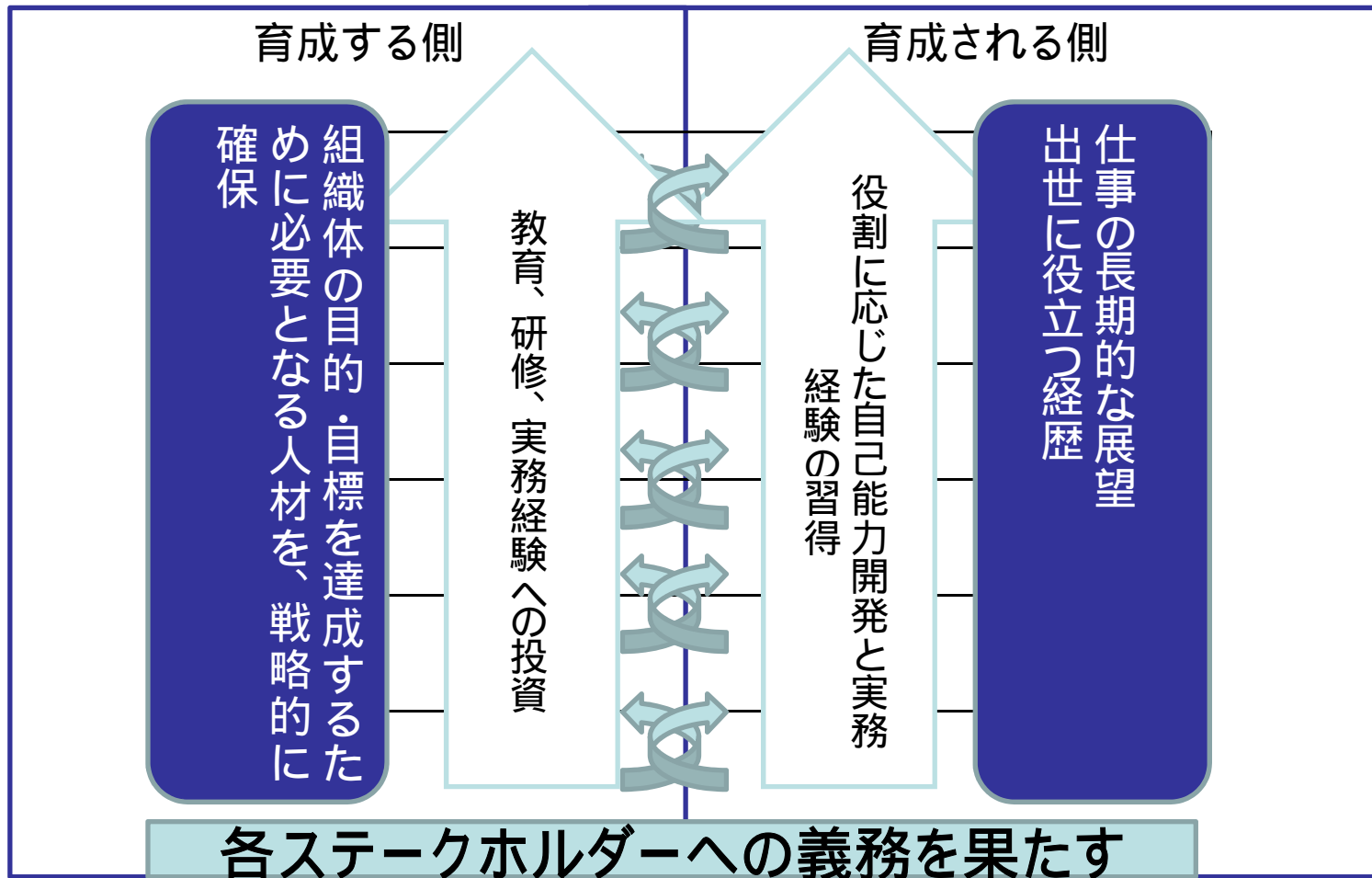
情報セキュリティ人材の育成・確保
(中略)

現在情報セキュリティに携わる人材の一部からは、自らのキャリアパスを明確に描くことができないといった不安の声も上がっている。今後は情報セキュリティ人材を必要とするいわゆる需要側と情報セキュリティ人材を供給する側だけでなく、情報セキュリティ人材そのものからのニーズに着目した施策検討も必要になるものと考えられる。

出展:「セキュア・ジャパン2009」より抜粋 ～ 内閣官房情報セキュリティセンター(NISC)

資格の有効活用

経営戦略と人材育成戦略の融合が必要不可欠



資格保有の効果

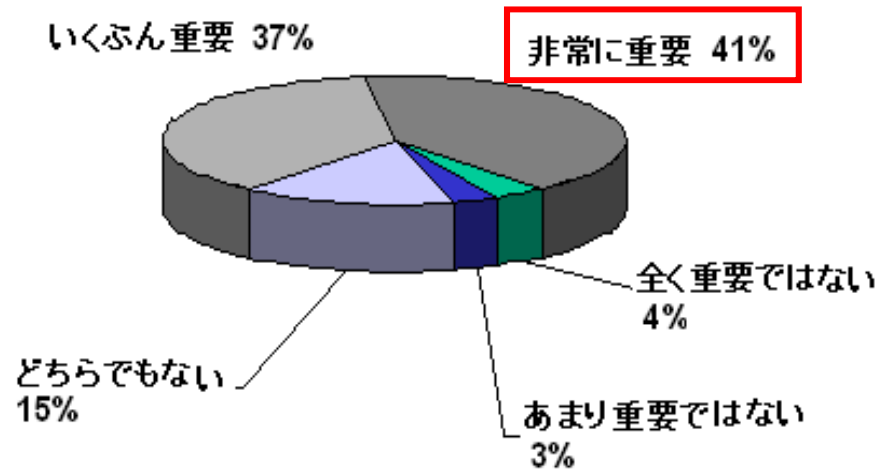
立場	期待される効果
情報セキュリティの業務を実施する側	情報セキュリティ人材を目指す個人にとって:目標の自己設定や評価ができる 情報セキュリティ人材を育成する組織にとって:実効性が高い人材の育成、評価や管理ができる
情報セキュリティの業務を委託する側	業務を委託する際に、要件に合った適切な人材を要求・調達できる

情報セキュリティ人材の育成・活用・管理のための、実効的かつ相対的な指標を示せる

資格に求められる要件

客観性	保有者の知識、スキルを客観的に判断できる共通知識分野体系
適切	定期的な共通知識分野アップデートなどを通じ、その時々で市場で使える人材を認定
実務経験	実務経験を通じた情報セキュリティ実践の証明
厳格な認定プロセス	共通知識分野の理解度を測る試験と実務経験の裏づけとなる推薦と監査プロセス
国際的	世界に認められた共通知識分野をベースとしている
維持更新	認定を維持するための継続的教育・訓練を義務付けている

資格保有の重要性は？ - 組織側から見た時



理由 ()内は昨年の調査結果

- ・ 能力の裏づけ
71%(67%)
- ・ 企業ポリシー
67%(33%)
- ・ 仕事の質の確保
61%(59%)
- ・ 規制上
44%(27%)
- ・ 企業イメージ・評価
44%(N/A)
- ・ 法的要素
36%(21%)

- 「非常に重要」が、2007年から8%アップ。
- 能力の裏づけとして、資格の保有が最重要。それに加え、企業ポリシーとして資格保有が重要と考える企業が急激に増加。

活用のキーポイント - 個人にとって

- ・ 資格取得 - インプットの有効性の証明
- ・ 業務においてのアウトプットが必要 - 業務経験・経歴などで実証

- ・ 上記2つが揃って始めて「高度人材」と呼べる
 - 資格取得はある意味、スタート地点
- ・ キャリアパスとの結びつけ

結果として、「自分力」アップ！

活用のキーポイント - 組織にとって

人事評価との連携

- ・ 段階ごとでの評価指標としての資格導入
- ・ プラス業務経験を経て、その上に行くための指標としての資格
- ・ 評価に際しては、保有資格 + 業務経験の双方をバランス良く
- ・ インセンティブの導入も重要な要素

結果として、「組織力」の向上！

米国国防総省 Directive 8570.1 必須資格一覧

IAT Level I		IAT Level II		IAT Level III	
A+ Network+ SSCP		GSEC Security+ SCNP SSCP		CISA CISSP <i>(or Associate)</i> GSE SCNA	
IAM Level I		IAM Level II		IAM Level III	
GISF GSLC Security+		GSLC CISM CISSP <i>(or Associate)</i>		GSLC CISM CISSP <i>(or Associate)</i>	
CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND-SP Manager	
GCIA	SSCP	GCIH CSIH	CISA GSNA	CISSP-ISSMP CISM	
IASAE I		IASAE II		IASAE III	
CISSP <i>(or Associate)</i>		CISSP <i>(or Associate)</i>		ISSEP ISSAP	

ISEPAの取り組み

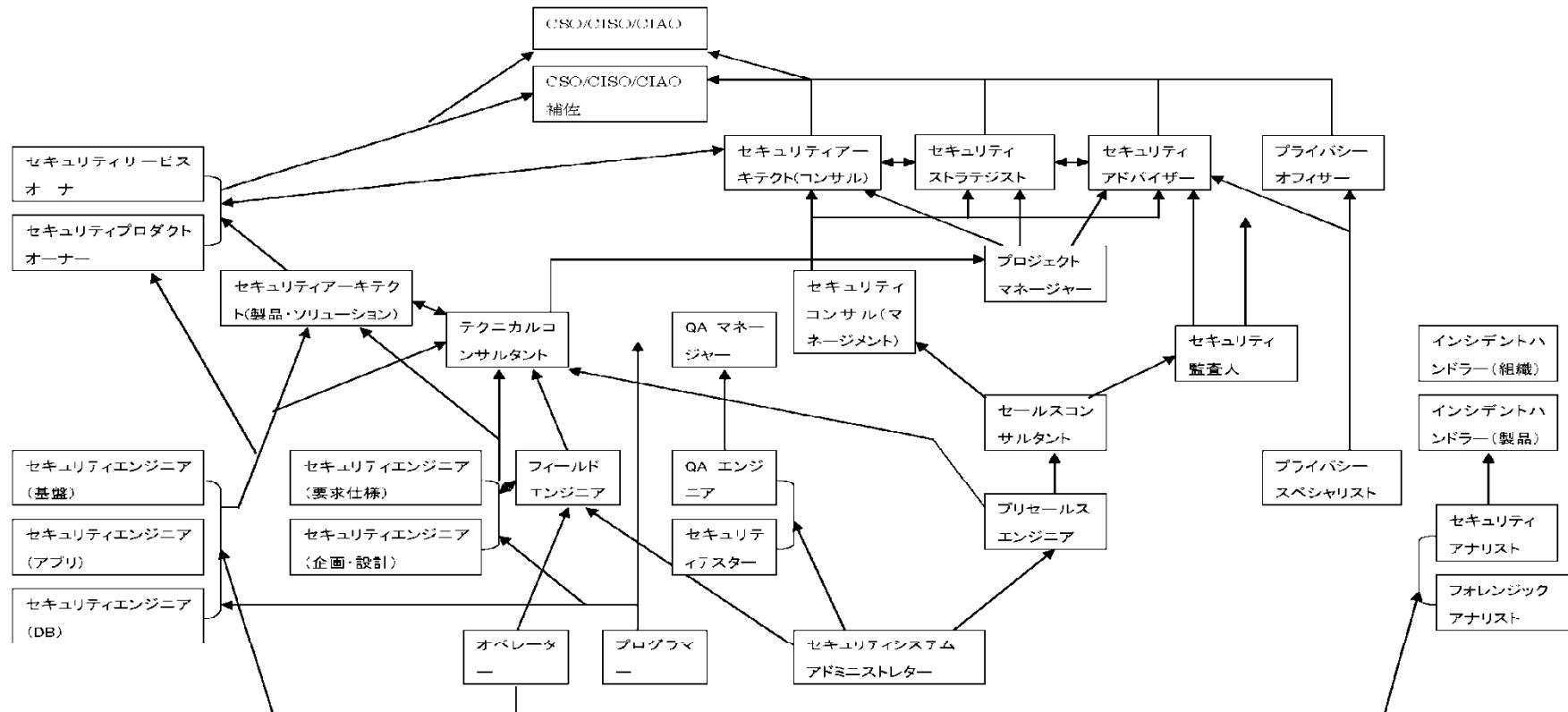
- ・ アーキテクチャガイドの開発
 - 人財育成マップ 業務・スキル・知識と教育・資格の紐付け
 - キャリアパス 高度人材への道筋としての指標
 - 組織モデル 組織における必要人材の特定
- ・ 人材調査
 - 資格保有者 & 非保有者の現状把握
 - 取得推進に留まらず、利活用についての問題点を浮き彫りにし、将来への方向性を見出す基礎材料とする

人財育成マップ

職種名	セキュリティコンサルタント(マネージメント)		
定義	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。	所属企業・部署グループ	サービス・製品提供組織 営業
職務項目	スキル・知識		
必須職務:	必須:		
単一の技術や基礎に依存する事のリスクを改善できる	知識項目 情報セキュリティマネジメント	大分類 マネジメント概論	中分類 セキュリティマネジメントの基本
情報セキュリティに関する共通化された物を使用して要求仕様を作成できる			マネジメントプロセス
相互依存性解析の成果を踏まえた情報セキュリティ基準等が検討できること			関連知識
災害発生時における対応等、横断的な取り組みと整合性の確保・連携について検討ができること			セキュリティポリシー
情報セキュリティ管理も重視した標準的な情報サービスマネジメントの導入ができること			リスク分析
情報セキュリティ管理の活用を促進できること	コンプライアンス	コンプライアンス	基準 規格・基準・指針・ガイドライン等(国内)
事業継続マネジメント(BCM)			規格・基準・指針・ガイドライン等(国際)
オフショア・アウトソーシングに関連する固有リスクを把握できること			
情報システムの一元的把握ができること(参照される情報が整理されている)	実践:		
各業務・システムの最適化ができること	知識項目	大分類	中分類
IT障害、リスクについての分析と改善			
CSIRTに対する情報提供体制の構築と確立			
事故、災害や攻撃に対して、事前に考えられる対策を十分に施せる			
情報セキュリティに関する取り組みについて全体としての整合性が確保できること			
実施可能職務:			
サイバー攻撃等に関する脅威/影響度の分析・対処能力を向上させるための機材選定ができること			
適切な暗号化及び電波の範囲設定等の対策			
各利用者の環境に応じた対策の優先度に関する意思決定を支援するツール等の作成ができること			
ビジネスプロセス、Webサービス、外部委託先を対象とした情報セキュリティ評価			
情報セキュリティ対策実施状況を確認する為の標準フォーマットの検討ができること			
情報セキュリティ対策の手引きの作成ができること			
個人情報保護、営業機密管理			
インシデント対応			
教育			
CMU, SPIA-M, LAC-B5-18, RC-27K-1,2,3,4,5,6,7, CMU, SANS-SEC401, MG1411, IS-ISMS, ISMSAudit, BCM, BCMAudit			
資格			
CISA, CISSP, SEAJ-M, CAIS, SANS-GSEC, SANS-G7799			

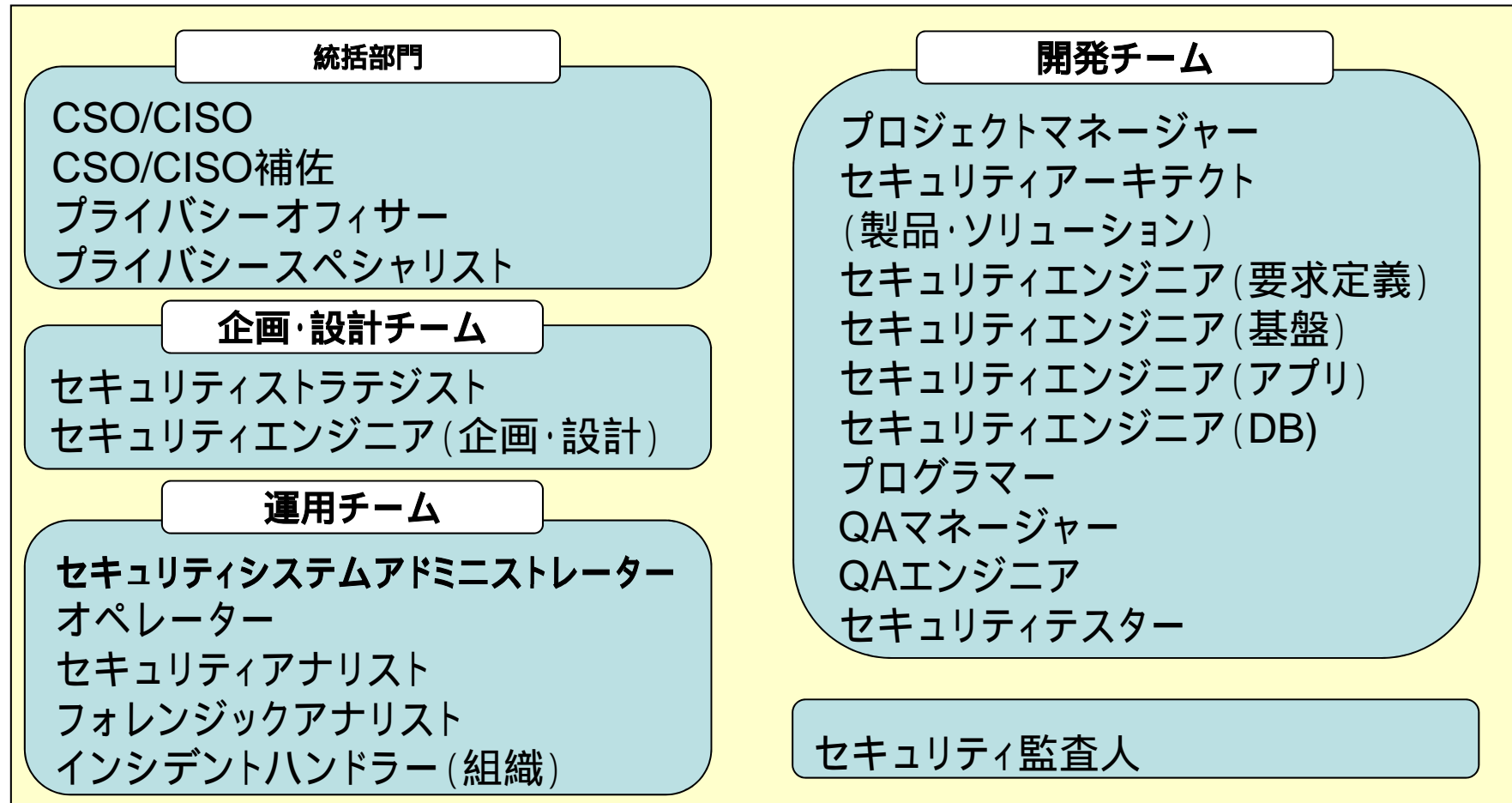
職種 → 職種の定義
業務内容 → 必要とされるスキル・知識
スキル・知識 → スキル・知識習得に有効な教育・資格

キャリアパス To-beモデル



組織モデル - 企業内情報セキュリティ機能

自社完結モデル



人材調査概要

- ・ 対象：
 - ITセキュリティ業務従事の社会人(一般企業、ベンダー、行政機関)及び学生(専門学校生含む)
 - *メインにしたいのは、非資格保有者の社会人、学生
- ・ 調査内容：
 - 資格認知度
 - 資格非保有の理由、もしくは失効者はそうなってしまった理由
 - 取得予定者への動機、準備や取得への障害
 - 取得予定資格の取得優先順位とその理由
 - 非セキュリティ資格保有の現状

今後に向けての提言

- ・ 雇用主、従業員、委託先の中で「必要な人材像」「人材育成・評価手法」「資格活用」の認識について共有することが重要
- ・ 資格の有効活用においては、「資格維持」に対して個人の努力だけではなく、組織としての支援策の確立が不可欠

ご清聴、まことにありがとうございました