isepa 情報セキュリティ教育事業者連絡会
Information Security Education Providers Association

「情報セキュリティ人財アーキテクチャー」について

情報セキュリティ教育事業者連絡会
スキルWGリーダー
(ISC)2ジャパン　代表
衣川　俊章

情報セキュリティ教育事業者連絡会(ISEPA)概要

名称と目的

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/

- 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

情報セキュリティ教育事業者連絡会
Information Security Education Providers Association

NISC

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ー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

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
情報セキュリティ大学院大学
工学院大学
サイバー大学
東京電機大学　等

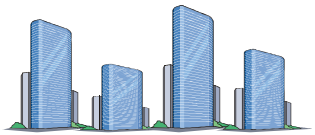
情報共有・後援等依頼中
アドバイザー協力要請

人材育成計画の支援
人材の紹介・斡旋

有資格者による
バーチャルコンサル
（簡易相談）

人財育成セミナー
カテゴリ別セミナー
（CISO、担当者等）
資格取得相談

情報共有
講師候補・育成
キャリア登録



政府機関・地方公共団体

企業

中小企業

セキュリティ人材候補

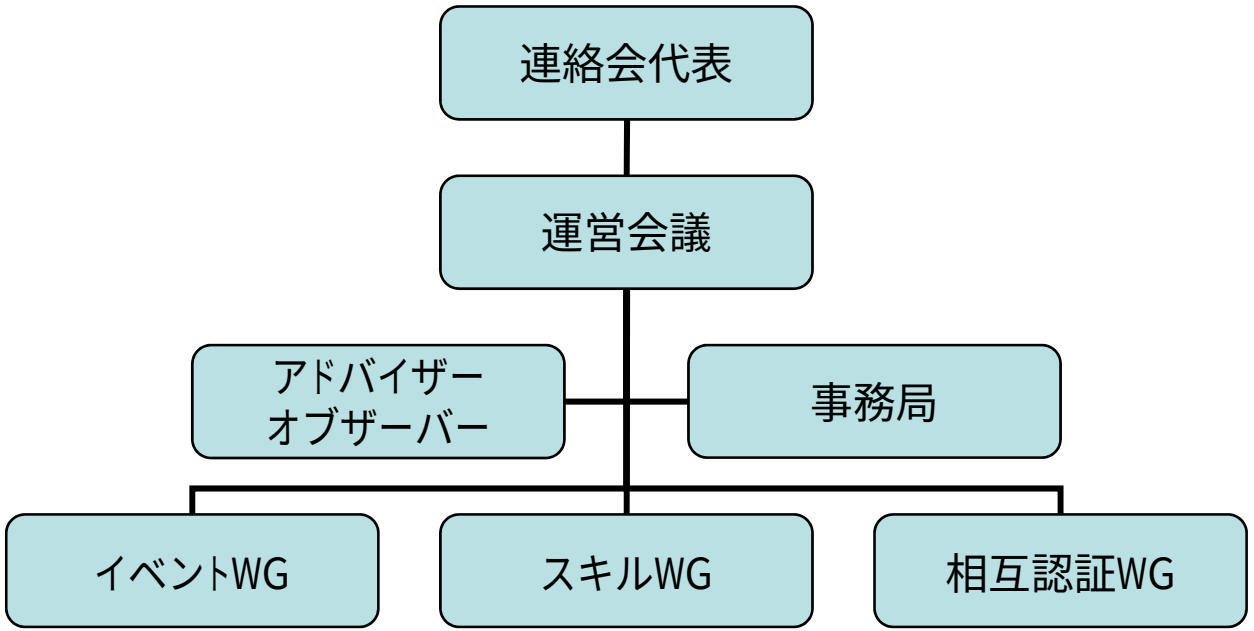
高度セキュリティ人材

参加組織

2008年2月23日現在

会員		オブザーバー
(ISC)2 Japan	NPO 日本セキュリティ監査協会 (JASA)	内閣官房情報セキュリティセンター
ISACA東京支部	(財)ひょうご情報教育機構 (カーネギーメロン大学日本校)	総務省　情報通信政策局
㈱インフォセック	㈱ラック	経済産業省 商務情報政策局
NRIセキュアテクノロジーズ㈱ (SANS JAPAN事務局)	リコーヒューマンクリエイツ㈱	独立行政法人 情報処理推進機構　(IPA)
NTTコムチェオ㈱	NPO 日本セキュリティネットワーク協会 (JNSA)	(財) 日本情報処理開発協会　(JIPDEC)
NTTラーニングシステムズ㈱		(財) インターネット協会　(IAjapan)
㈱ケーケーシー情報システム		ISSA (Information Systems Security Association) 東京支部
CompTIA Japan		
SEA/J		
(財)ソフトピアジャパン		

運営体制



連絡会が目指すもの

- 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

「情報セキュリティ人財アーキテクチャー」概要

「情報セキュリティ人財アーキテクチャー」策定の目的

- 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すこと
  - 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財アーキテクチャー」に込められた意味

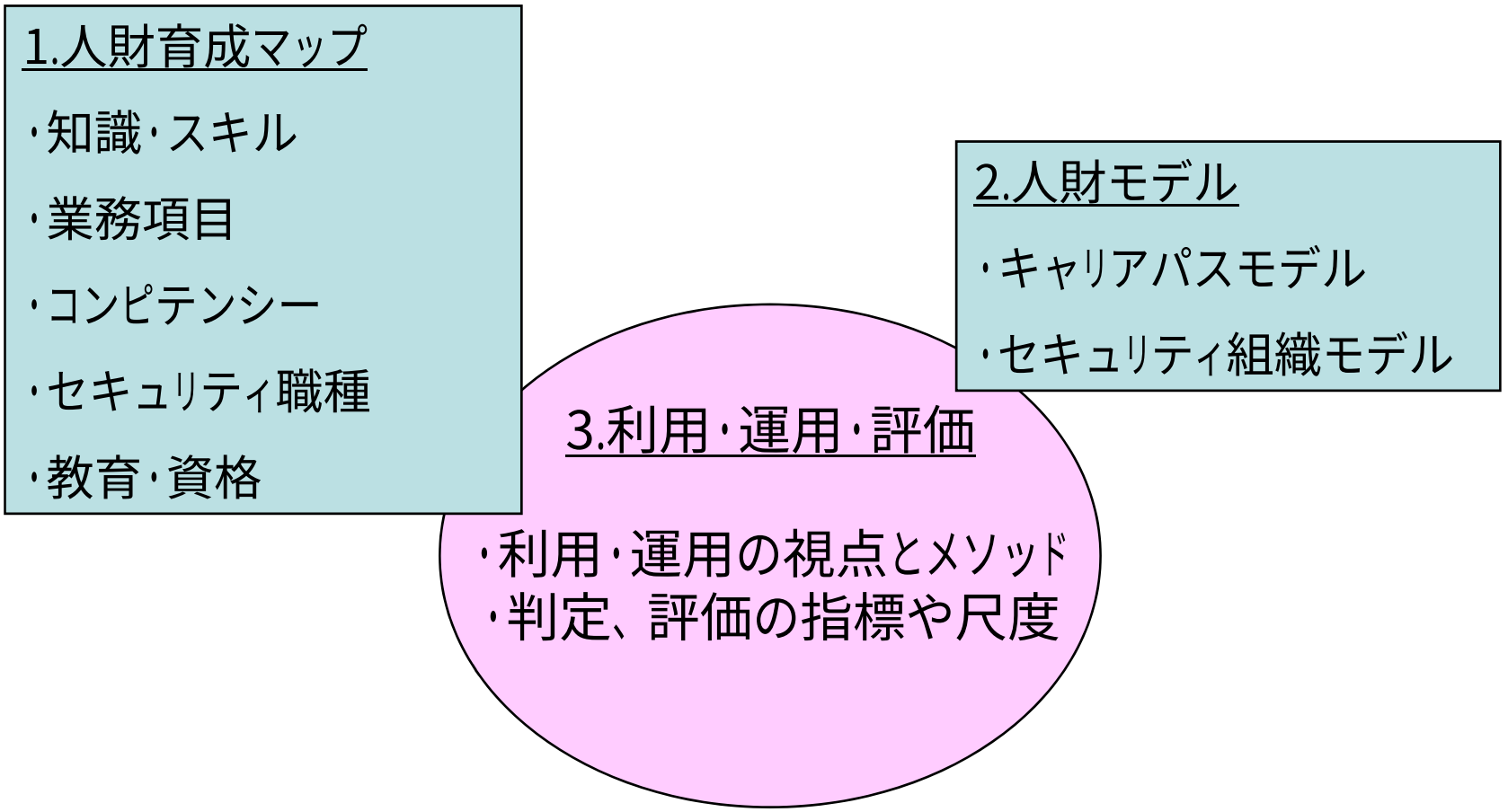
- 「人財」：

組織において「人」は、「技術」「特許」などと同じ「知的財産」であるべき、という考えから「人財」とした。

- 「アーキテクチャー」：

あるべき姿を構築・維持するための枠組み・方法論である「EA」の情報セキュリティ人材版を目指す、という方針から「アーキテクチャー」とした。

セキュリティ人財アーキテクチャー全体概要図



「人財育成マップ」と「人財モデル」

セキュリティ人財アーキテクチャ全体概要図

これらを関連付けて示す事により、人財育成への具体的な指標を示す

1.人財育成マップ

・知識・スキル

・業務項目

・コンピテンシー

・セキュリティ職種

・教育・資格

2.人財モデル

・キャリアパスモデル

・セキュリティ組織モデル

3.利用・運用・評価

・利用・運用の視点とメソッド
・判定、評価の指標や尺度

知識・スキル

●JNSA作成の「セキュリティ知識分野（SecBoK）」の 中分類までを参照

	分野名		分野名
1	情報セキュリティマネジメント	12	**PKI（Public Key Infrastructure）**
2	ネットワークインフラセキュリティ	13	暗号
3	アプリケーションセキュリティ	14	電子署名
4	OSセキュリティ	15	攻撃手法
5	ファイアーウォール	16	コンプライアンス
6	侵入検知（IDS/IPS）	17	セキュリティプロトコル
7	不正プログラム	18	事業継続・災害復旧計画
8	セキュアプログラミング技法	19	情報セキュリティ監査
9	セキュリティ運用	20	フォレンジック
10	コンテンツセキュリティ	21	物理セキュリティ
11	認証		

業務項目

- 情報セキュリティ業務を遂行するのに必要な項目を、以下のリファレンスより抽出　→　日本国の目指している物との整合性をとった

- 内閣官房情報セキュリティセンター：
  1．第一次情報セキュリティ基本計画
  2．セキュアジャパン2007
  3．人材育成・資格制度体系化専門委員会報告書
- 総務省：
  4．u-Japan政策パッケージ
- 経産省：
  5．グローバル情報セキュリティ戦略
  6．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

コンピテンシー

- 情報セキュリティ業務を遂行するのに必要なヒューマンコンピテンシーを、以下のリファレンスより策定
  - 国家公務員採用1種試験　着眼点別評価段階と行動例

積極性[意欲・行動力]		経験学習力[課題の認識・経験の適用]	
	自らの考えを積極的に伝えようとしているか		自己の経験から学んだものを現在に適用しているか
	考え方が前向きで向上心があるか		自己や組織の状況と課題を的確に認識しているか
	目標を高く設定し、率先してことに当ろうとしているか		優先度や重要度を明確にして目標や活動計画を立てているか
	困難なことにもチャレンジしようとする姿勢が見られるか		他者から学んだものを自己の行動・経験に適用しているか
社会性[他者理解・関係構築力]		自己統制[情緒安定性・統制力]	
	相手の考えや感情に理解を示しているか		落ち着いており、安定感があるか
	異なる価値観にも理解を示しているか		ストレスに前向きに対応しているか
	組織や集団のメンバーと信頼関係が築けるか		環境や状況の変化に柔軟に対応できるか
	組織の目的達成と活性化に貢献しているか		自己を客観視し、場に応じて統制することができるか
信頼感[責任感・達成力]		コミュニケーション力[表現力・説得力]	
	相手や課題を選ばずに誠実に対応しようとしているか		相手の話の趣旨を理解し、的確に応答しているか
	公務に対する気構え、使命感はあるか		話の内容に一貫性があり、わかりやすく簡潔か
	自らの行動、決定に責任を持とうとしているか		話し方に熱意・説得力があるか
	困難な課題にも最後まで取り組んで結果を出しているか		話題や説明材料を効果的に使っているか

セキュリティ職種

- セキュリティ職とは　ー　情報セキュリティに係る人材
- 各種情報セキュリティ政策文書と調査により、ISEPAスキルWGが策定
  → 各職種にISEPAとしての定義を当てはめている

1	プリセールスエンジニア	17	オペレーター
2	セールスコンサルタント	18	セキュリティアナリスト
3	テクニカルコンサルタント	19	フォレンジックアナリスト
4	セキュリティエンジニア（要求定義）	20	インシデントハンドラー（プロダクト）
5	セキュリティアーキテクト（製品・ソリューション）	21	インシデントハンドラー（組織）
6	セキュリティアーキテクト(コンサル)	22	フィールドエンジニア
7	セキュリティエンジニア(企画・設計)	23	プライバシーオフィサー
8	セキュリティエンジニア(基盤)	24	プライバシースペシャリスト
9	セキュリティエンジニア(アプリ)	25	CSO/CISO/CIAO
10	セキュリティエンジニア（DB）	26	CSO/CISO/CIAO補佐
11	QAマネージャー	27	セキュリティプロダクトオーナー
12	QAエンジニア	28	セキュリティサービスオーナー
13	セキュリティテスター	29	セキュリティコンサルタント(マネージメント)
14	プログラマー	30	セキュリティアドバイザー
15	プロジェクトマネージャー	31	セキュリティストラテジスト
16	セキュリティシステムアドミニストレーター	32	セキュリティ監査人

セキュリティ教育・資格

- 日本市場に現存するセキュリティ関連教育・資格を職種毎に特定していく。
  - まずは、ISEPA加盟団体・企業のものをマッピングした
  - 各職種で、レベル感の違う教育・資格が混在しているが、これは同一職種内での経験年数や職責などの違いによって、必要とされるレベルが存在するという前提でマッピングしているため

セキュリティ教育・資格リスト

提供団体・企業名	コース・資格名	対象記号	提供団体・企業名	コース・資格名	対象記号
ISACA	CISA	CISA	SANS	GIAC Security Essentials Certification	GSEC
	CISM	CISM		GIAC Certified Penetration Tester	GPEN
(ISC)2	CISSP	CISSP		GIAC Certified Firewall Analyst	GCFW
	SSCP	SSCP		GIAC Systems and Network Auditor	GSNA
NTTラーニングシステムズ	情報セキュリティ専門家養成講座	LS-0		GIAC Certified Incident Handler	GCIH
ひょうご情報教育機構	カーネギーメロン大学日本校	CMU		GIAC Certified Windows Security Administrator	GCWN
	情報セキュリティ育成プログラム－ベーシックコース	Hyogo-B		GIAC Certified UNIX Security Administrator	GCUX
	情報セキュリティ育成プログラム－アドバンスドコース	Hyogo-A		GIAC Securing Oracle Certification	GSOC
CompTIA	Security+	CTIA		GIAC Secure Software Programmer-Java	GSSP-J
SEA/J	情報セキュリティ技術認定　基礎コース	SEAJ-B		GIAC Secure Software Programmer-C	GSSP-C
	情報セキュリティ技術認定　応用コース・テクニカル	SEAJ-T		GIAC Certified Project Manager Certification	GCPM
	情報セキュリティ技術認定　応用コース・マネージメント	SEAJ-M		GIAC Certified Intrusion Analyst	GCIA
シスコシステムズ	CCSP	CCSP		GIAC Reverse Engineering Malware	GREM
	CCIEセキュリティトラック	CCIE-Sec		GIAC Certified Forensics Analyst	GCFA
	CCNAセキュリティトラック	CCNA-Sec		GIAC Security Leadership Certification	GSLC
ソフトピアジャパン	セキュリティマネージメントコース	SPIA-M		GIAC Certified Incident Manager	GCIM
	セキュリティテクニカルコース	SPIA-T		GIAC Certified ISO-17799 Specialist	G7799
	インシデントレスポンス実践コース	SPIA-IR		SEC301：Intro to Information Security	SANS-SEC301
日本セキュリティ監査協会	公認情報セキュリティ監査人	CAIS		SEC401：SANS Security Essentials	SANS-SEC401
JASA				SEC501：Advanced Security Essentials	SANS-SEC501
LAC	情報セキュリティマネジメントシステム	LAC-B1		SEC502：Perimeter Protection In-Depth	SANS-SEC502
	情報セキュリティ監査	LAC-B2		SEC503：Intrusion Detection In-Depth	SANS-SEC503
	内部統制と情報セキュリティ	LAC-B3		SEC504：Hacker Techniques, Exploits and Incident Handling	SANS-SEC504
	法と倫理	LAC-B4		SEC505：Securing Windows	SANS-SEC505
	セキュリティアーキテクチャ	LAC-B5		SEC506：Securing Unix/Linux	SANS-SEC506
	不正アクセス対策	LAC-B6		SEC508：Computer Forensics, Investigation, and Response	SANS-SEC508
	ネットワークインフラセキュリティ	LAC-B7		SEC509：Securing Oracle	SANS-SEC509
	ネットワークセキュリティ(ファイアウォールと侵入検知)	LAC-B8		SEC560：Network Penetration Testing and Ethical Hacking	SANS-SEC560
	ネットワークセキュリティ(セキュリティプロトコル)	LAC-B9		SEC601：Reverse-Engineering Malware: The Essentials of Malware Analysis	SANS-SEC601
	OSセキュリティ	LAC-B10		SEC610：Reverse-Engineering Malware: Malware Analysis Tools and Techniques	SANS-SEC610
	不正プログラミング対策	LAC-B11		SEC709：Developing Exploits for Penetration Testers and Security Researchers	SANS-SEC709
	セキュアプログラミングとセキュアアプリケーション開発	LAC-B12		AUD429：IT Security Audit Essentials	SANS-AUD429
	暗号・電子署名	LAC-B13		AUD507：Auditing Networks, Perimeters & Systems	SANS-AUD507
	PKI・認証技術	LAC-B14		DEV304：Software Security Awareness	SANS-DEV304
	物理セキュリティ	LAC-B15		DEV319：Intro to Web Application Security	SANS-DEV319
	インシデントレスポンス	LAC-B16		DEV422：Web Application Security Essentials	SANS-DEV422
	デジタルフォレンジック	LAC-B17		DEV534：Java Security Source Code Review	SANS-DEV534
	事業継続概要	LAC-B18		DEV536：Secure Coding for PCI Compliance	SANS-DEV536
	Webアプリケーションセキュリティ講座	LAC-B19		DEV538：Web Application Pentesting Hands-On Immersion	SANS-DEV538
	データベースセキュリティの現状とあるべき姿	LAC-B20		DEV541：Secure Coding in Java/JEE	SANS-DEV541
	インシデントレスポンス(ハンズオン)	LAC-C1		DEV544：Secure Coding in .NET	SANS-DEV544
	フォレンジック(ハンズオン)	LAC-C2		DEV545：Secure Coding in PHP	SANS-DEV545
	マルウェア現況分析	LAC-C3		DEV548：Secure Coding in C	SANS-DEV548
リコーヒューマンクリエイツ	プライバシーマーク審査員研修	RC-P1		MGT411：SANS 17799/27001 Security & Audit Framework	SANS-MGT411
	プライバシーマーク制度とJISQ15001入門解説	RC-P2		MGT504：Hacking for Managers	SANS-MGT504
	演習で学ぶJISQ15001:2006規格解説	RC-P3		MGT512：SANS Security Leadership Essentials For Managers	SANS-MGT512
	演習で学ぶプライバシーマーク・リスク分析	RC-P4		MGT525：Project Management and Effective Communications for Security Professionals and Managers	SANS-MGT525
	演習で学ぶプライバシーマーク・内部規定	RC-P5			
	演習で学ぶプライバシーマーク・内部監査	RC-P6			
	プライバシーマーク更新審査に向けた「新JIS対応」	RC-P7			
	プライバシーマーク取得のための「ラピッドコンサルティング講座」	RC-P8			
	ISMS審査員研修	RC-27K-1			
	ISMS審査員資格更新のための実践集中コース	RC-27K-2			
	はじめて学ぶISO27001	RC-27K-3			
	リスク分析を中心に学ぶISO27001	RC-27K-4			
	演習で学ぶISO27001内部監査	RC-27K-5			
	経営者のための必修情報セキュリティ	RC-27K-6			
	ISO27100認証取得のための「ラピッドコンサルティング講座」	RC-27K-7			

人財育成マップ策定プロセス

- 業務項目ー知識･スキルの紐付け
  - 実務遂行に絶対必要な知識･スキルと知っている必要はあるが、業務遂行上絶対必要ではない知識･スキルの両方を紐付けした
- 職種ー業務項目の紐付け
  - 各職種の定義をした上で、その定義に従って、必須業務項目をリストアップし、それに加えて各職種で出来るべき業務項目を列挙
- 職種ー教育･資格の紐付け
  - 既存の教育のアジェンダ、資格の必要知識分類を、知識･スキルの各項目に当てはめた
- コンピテンシー
  - セキュリティ職種毎に異なるスキルという事より、前提条件としてのスキルと判断した

人財育成マップ策定プロセス

業務項目	スキル
A	1,2,3
B	3,4,5
C	1,4,7,8

職種	業務項目
ア	A
イ	B,C
ウ	B,E,F

スキル	教育	資格
1,2,3	a,b,c	i,j
1-5,7,8	a-c, d,e,f	i,j,k
3-5,9,10	c-f,g,h	j,l,m.n

職種	業務項目	スキル
ア	A	1,2,3
イ	B,C	1-5,7,8
ウ	B,E,F	3- 5,9,10

人財育成マップ

コンピテンシー（共通項目）				
職種	業務項目	スキル	教育	資格
ア	A	1,2,3	a,b,c	i,j
イ	B,C	1-5,7,8	a-c, d,e,f	i,j,k
ウ	D,E,F	3-5,9,10	c-f,g,h	j,l,m.n

セキュリティ人財アーキテクチャ全体概要図

1.人財育成マップ

・知識・スキル

・業務項目

・コンピテンシー

・セキュリティ職種

・教育・資格

2.人財モデル

・キャリアパスモデル

・セキュリティ組織モデル

3.利用・運用・評価

・利用・運用の視点とメソッド
・判定、評価の指標や尺度

人財モデル

「キャリアパス」モデル

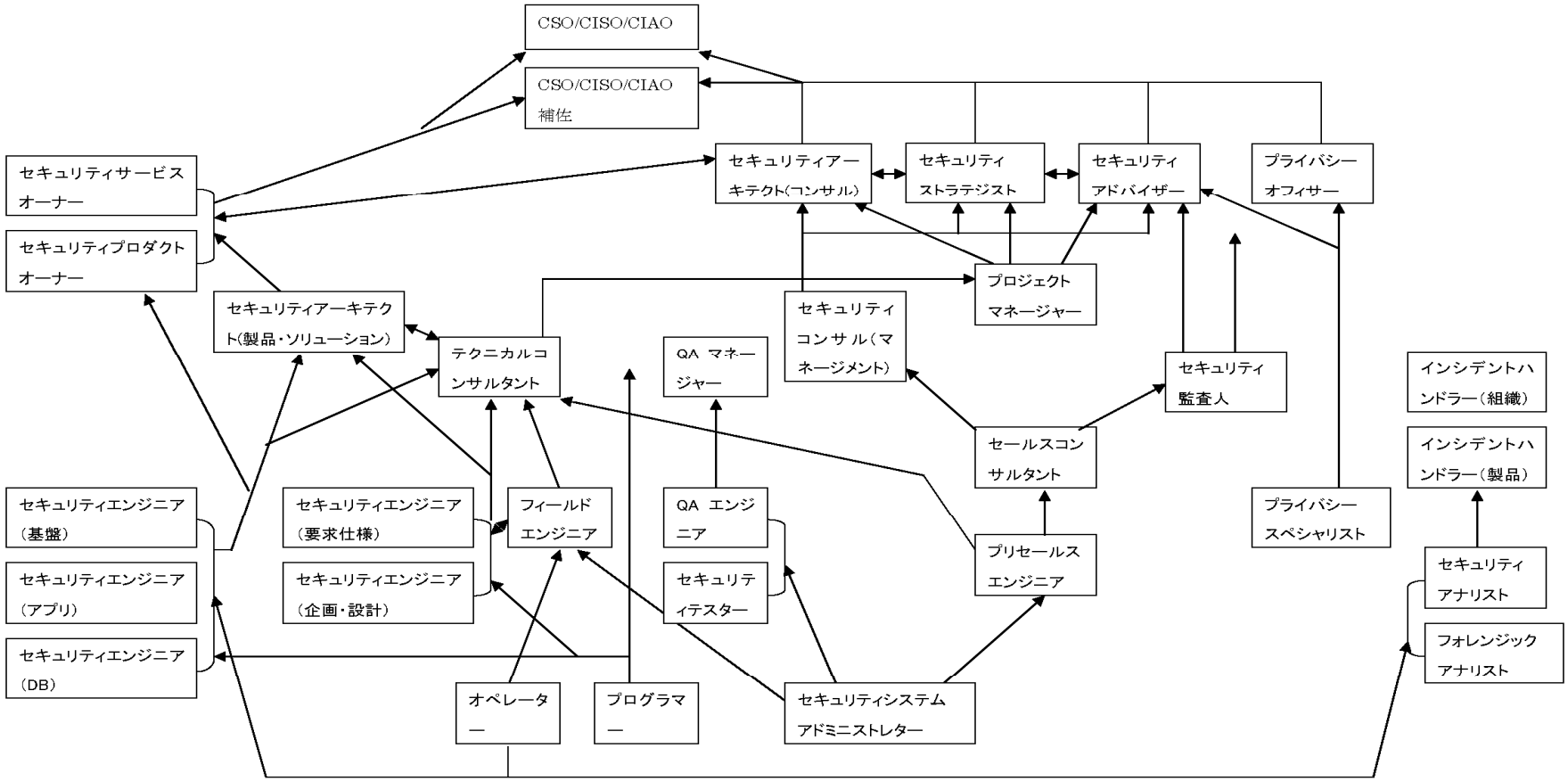
- 情報セキュリティにおけるキャリアパスの事例を作成し、育成側、育成される側の双方にとっての道しるべとする

「セキュリティ組織モデル」

- 組織やプロジェクト遂行において必要なる、人材を「職種」「業務項目」で特定し、いくつかのモデルケースを提示し、ケース毎の必要人材群を特定化する

★今回は、数例の提示となるが、徐々に増やし、改定を重ねていくことで、活用の幅を広げていく

キャリアパス モデル　ー　ToBeモデル



★各職種の業務項目の相関性をベースに、レベル感も入れ込んで作成

セキュリティ組織モデル

- 組織構成において、必要とされる人材群を特定した。これを具体的な組織策定への参考としてもらいたい
- 職種名に拘るというより、そういう業務実行をする人材が必要で、それはどういうスキル・知識を持っているべきかを参照してもらいたい
- 以下の3組織をモデルケースとして提示

  - 企業内CSIRT
  - セキュリティシステム開発プロジェクト
  - 企業内情報セキュリティ機能

＊上記のケースを自社内のみ、アウトソースする、大・中小企業における違いなどを事例として提示してあります

組織モデル　－　企業内CSIRT

★理想モデル

CSIRTチーム

CSO/CISO補佐（室長）
プライバシーオフィサー
オペレーター
セキュリティアナリスト
フォレンジックアナリスト
インシデントハンドラー（プロダクト）
インシデントハンドラー（組織）

★社内責任範囲別

経営企画

CSO/CISO補佐（室長）
プライバシーオフィサー

CSIRTチーム

オペレーター
セキュリティアナリスト
フォレンジックアナリスト
インシデントハンドラー（プロダクト）
インシデントハンドラー（組織）

組織モデル　ー
セキュリティシステム開発プロジェクト

★自社モデル

開発プロジェクトチーム

プロダクトオーナー
(またはサービスオーナー)
セキュリティアーキテクト
(製品・ソリューション)
プロジェクトマネージャー
セキュリティエンジニア (企画・設計)
セキュリティエンジニア (要求定義)
セキュリティエンジニア (基盤)
セキュリティエンジニア (アプリ)
セキュリティエンジニア (DB)
プログラマー
QAマネージャー
QAエンジニア
セキュリティテスター

★アウトソースモデル

開発プロジェクトチーム

プロダクトオーナー
(またはサービスオーナー)
セキュリティアーキテクト
(製品・ソリューション)
プロジェクトマネージャー
セキュリティエンジニア (企画・設計)
セキュリティエンジニア (要求定義)

開発委託先ベンダー

セキュリティエンジニア (基盤)
セキュリティエンジニア (アプリ)
セキュリティエンジニア (DB)
プログラマー
QAマネージャー
QAエンジニア
セキュリティテスター

組織モデル
ー　企業内情報セキュリティ機能

★自社完結モデル

統括部門

CSO/CISO
CSO/CISO補佐
プライバシーオフィサー
プライバシースペシャリスト

企画・設計チーム

セキュリティストラテジスト
セキュリティエンジニア（企画・設計）

運用チーム

セキュリティシステムアドミニストレーター
オペレーター
セキュリティアナリスト
フォレンジックアナリスト
インシデントハンドラー（組織）

開発チーム

プロジェクトマネージャー
セキュリティアーキテクト
（製品・ソリューション）
セキュリティエンジニア（要求定義）
セキュリティエンジニア（基盤）
セキュリティエンジニア（アプリ）
セキュリティエンジニア（DB）
プログラマー
QAマネージャー
QAエンジニア
セキュリティテスター

セキュリティ監査人

組織モデル
ー　企業内情報セキュリティ機能

★アウトソースモデル（大企業）ー開発＆運用（監視、インシデントハンドリング）を委託

統括部門

CSO/CISO
CSO/CISO補佐
プライバシーオフィサー
プライバシースペシャリスト
セキュリティ監査人

企画・設計チーム

セキュリティストラテジスト
セキュリティエンジニア（企画・設計）

運用チーム

セキュリティシステムアドミニストレーター
オペレーター

セキュリティベンダー

開発チーム

プロジェクトマネージャー
セキュリティアーキテクト（製品・ソリューション）
セキュリティエンジニア（要求定義）
セキュリティエンジニア（基盤）
セキュリティエンジニア（アプリ）
セキュリティエンジニア（DB）
プログラマー
QAマネージャー
QAエンジニア
セキュリティテスター

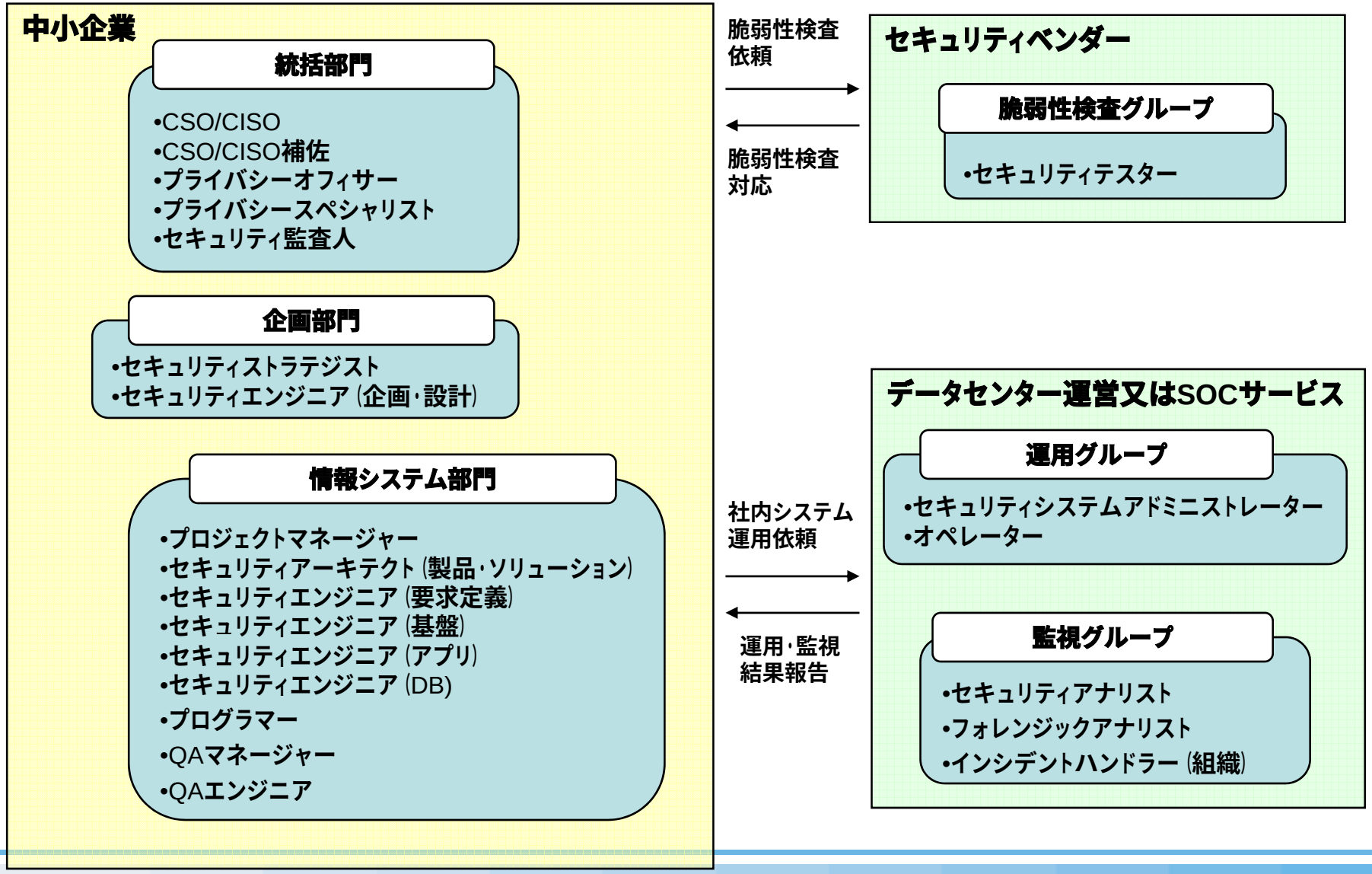
SOCサービス企業

運用チーム

セキュリティアナリスト
フォレンジックアナリスト
インシデントハンドラー（組織）

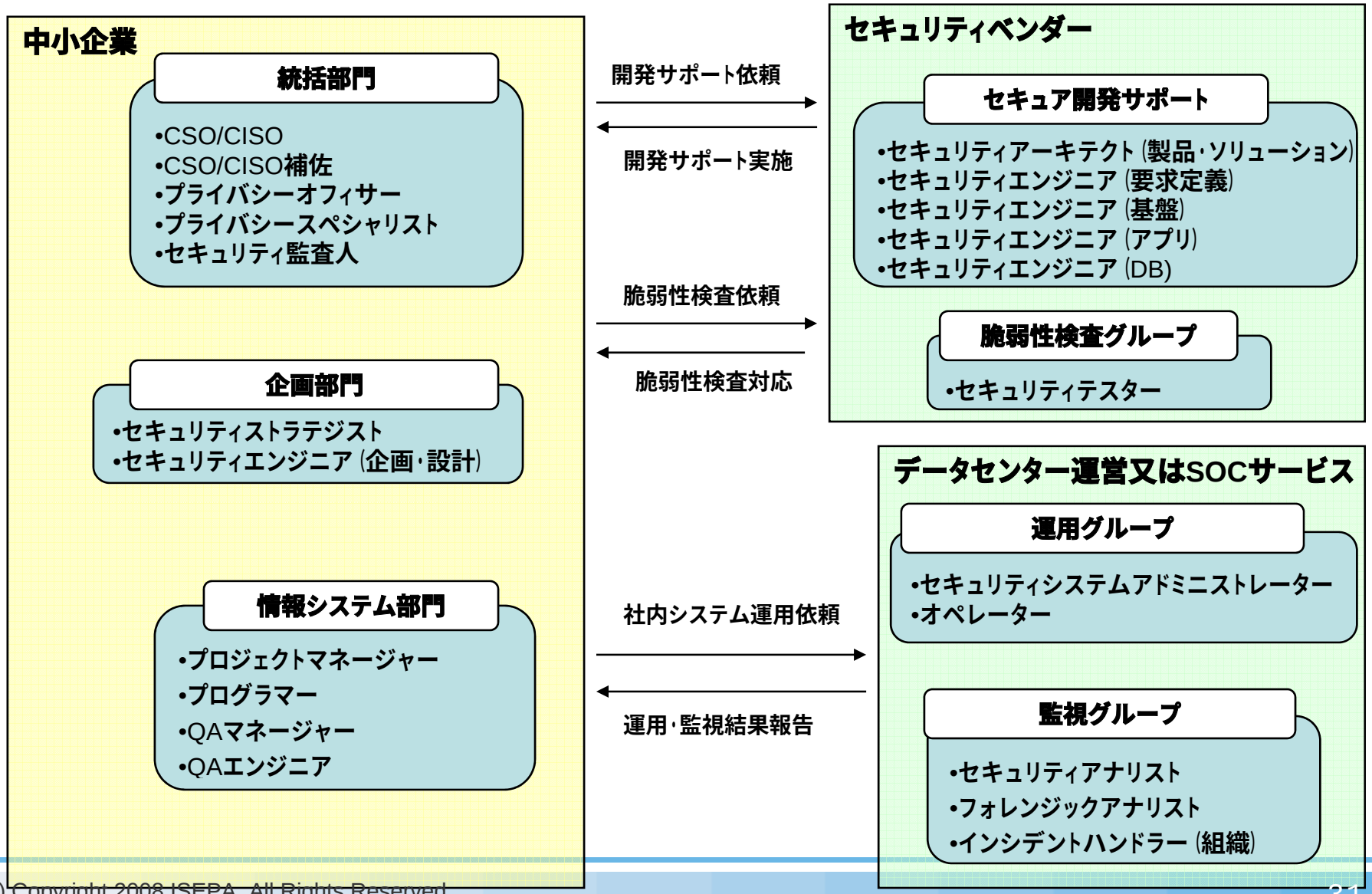
組織モデル
ー　企業内情報セキュリティ機能

★アウトソースモデルー検査･運用･監視を委託



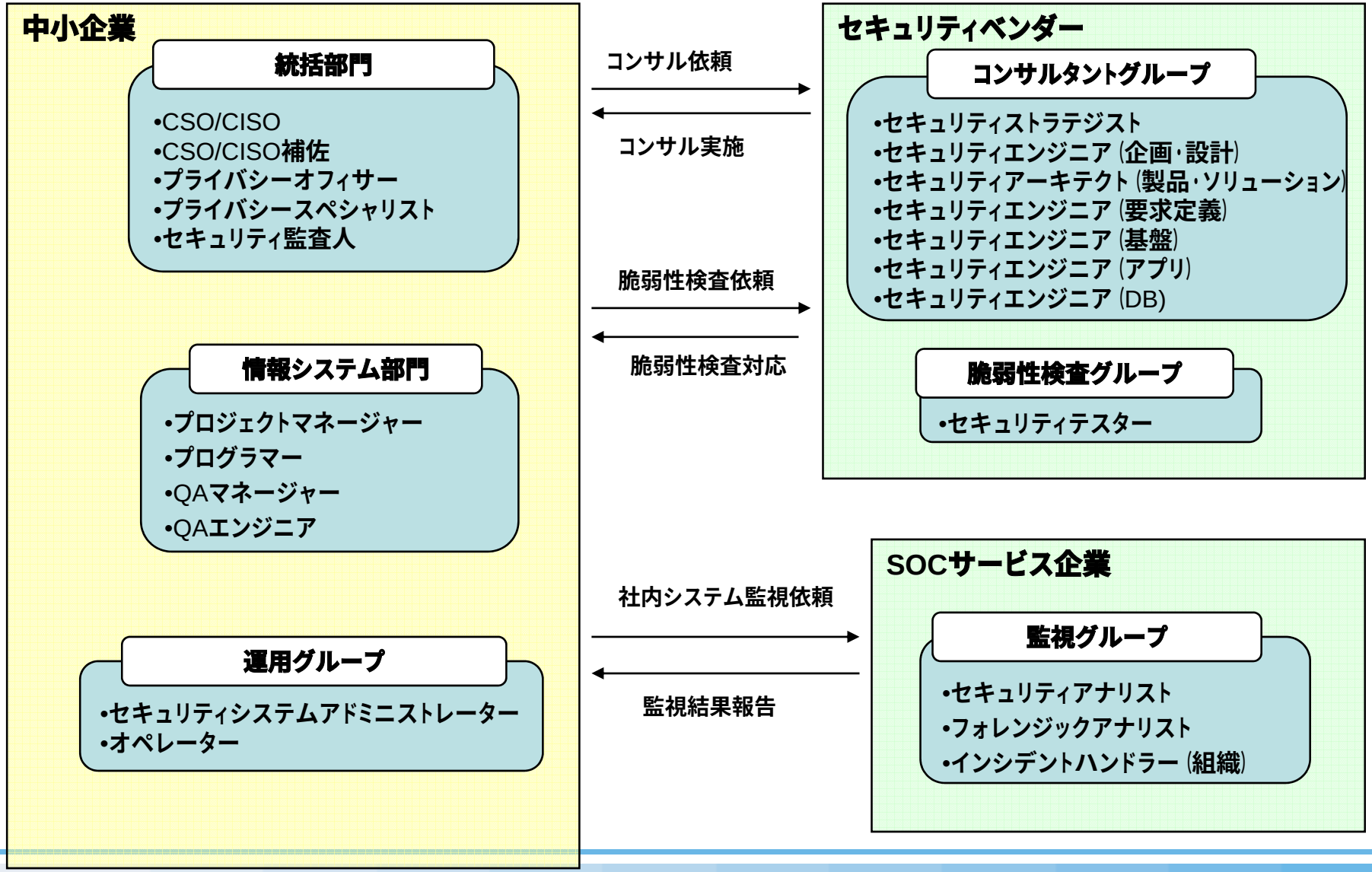
組織モデル
ー　企業内情報セキュリティ機能

★アウトソースモデル（中小企業）ー開発サポート・検査・運用・監視を委託



組織モデル
ー　企業内情報セキュリティ機能

★アウトソースモデル（中小企業）ー企画、構築、検査、監視までを委託



方法論：利用・運用・評価

セキュリティ人財アーキテクチャ全体概要図

1.人財育成マップ

・知識・スキル

・業務項目

・コンピテンシー

・セキュリティ職種

・教育・資格

2.人財モデル

・キャリアパスモデル

・セキュリティ組織モデル

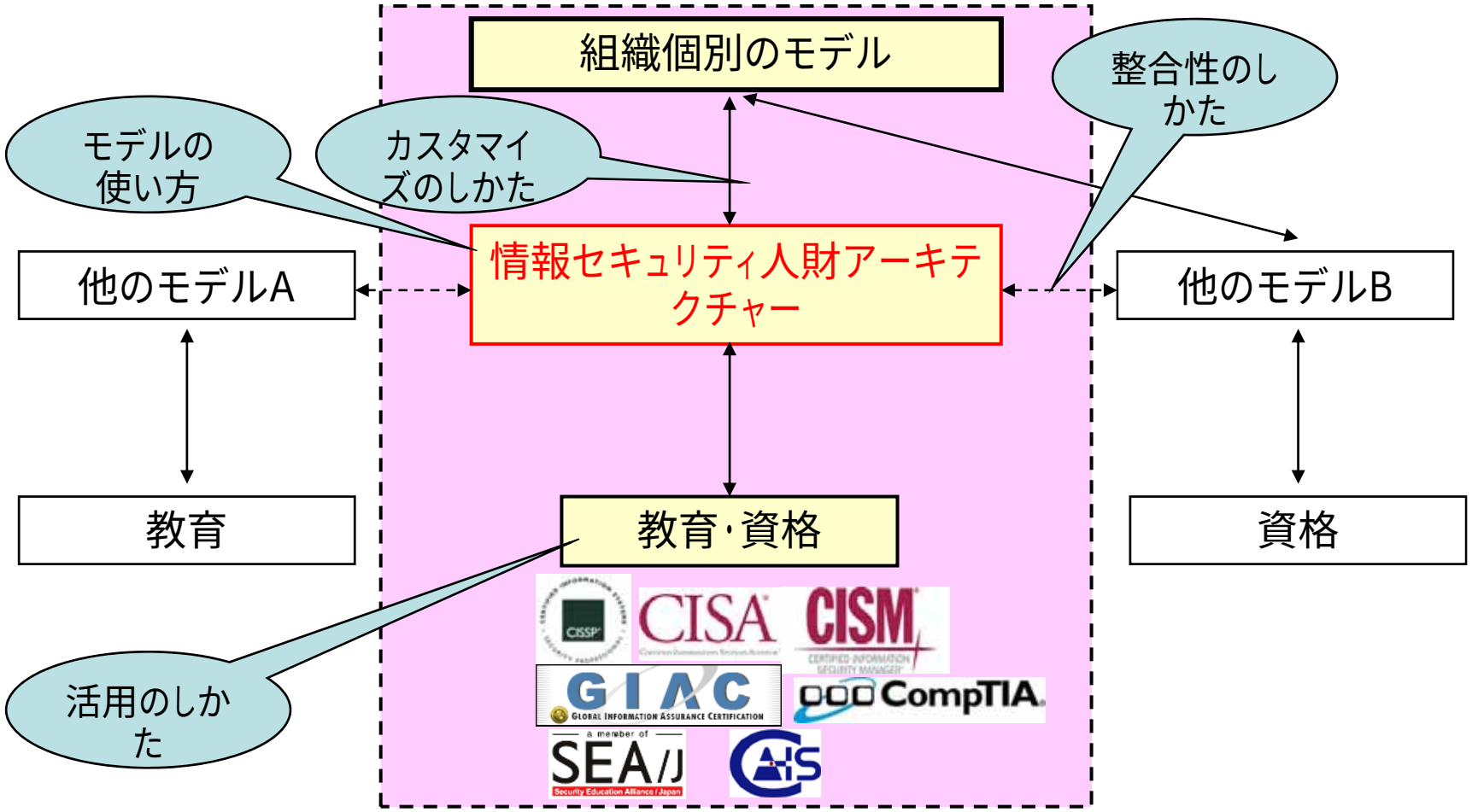
3.利用・運用・評価

・利用・運用の視点とメソッド
・判定、評価の指標や尺度

方法論：利用・運用・評価

- 「人財育成マップ」「人財モデル」を使って、どのように実際の人材の育成や維持・管理をしていくのか、その利用・運用・評価（レベルの判定）の方法論をモデル、ガイド(指針・手引き)として示す。
  - 想定される利用者（それぞれの視点と目的で利活用できるもの）
    - 人材を目指すもの
    - 育成や管理をするもの／人材を使う（委託・発注）もの
  - 何のために使うのか
  - どう使うのか

方法論のイメージ



今後の活動

「情報セキュリティ人財アーキテクチャー」の今後

- 定期的なアップデートの実施
- 現状とのギャップ分析
- 事例集や活用ガイドの作成
- 他のモデル（ITSS等）との互換性の実現

など

「理論」と「実証」を繰り返し、より良いものにしていく・・・

その他の活動予定（計画・検討中）

- 実証実験
  - 「スター育成プロジェクト」の継続、第2期開始へ
  - 「情報セキュリティ人財アーキテクチャー」実証実験組織の募集と支援
  - 「学」との連携（キャリア教育の始まりは、いつ？）
- 調査研究
  - IT業界以外のモデルや事例
  - 海外のモデルや事例

Thank you.