NRIセキュアテクノロジーズ

資料２-１

サイバーセキュリティ人材の育成に関する施策間連携
ワーキンググループ第2回会合

実態調査からひも解く、これからの情報セキュリティ対策のあり方

～ NRIセキュア 『企業における情報セキュリティ実態調査2017 』 から～

Share the Next Values!

2017年9月14日

NRIセキュアテクノロジーズ株式会社
事業推進部　担当部長

与儀　大輔

〒100-0004
東京都千代田区大手町1-7-2 東京サンケイビル

自己紹介

与儀 大輔，CISSP （Daisuke Yogi, CISSP）

Certified Information Systems Security Professional

- 1994年～2007年　横河電機
  2007年～2012年　ラック
  2012年　12月～　野村総合研究所
  2012年　12月～　NRIセキュアテクノロジーズ

- ＜主な対外活動及び受賞＞
  - NPO 日本ネットワークセキュリティ協会 幹事
  - 情報セキュリティ大学院大学　客員研究員
  - 2017年アジア・パシフィック
    情報セキュリティ・リーダーシップ・アチーブメント(ISLA)

JNSA

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

(ISC)² ISLA asia-pacific

- ＜政府等委員会＞
  - 情報処理推進機構 情報セキュリティ人材育成委員会　委員
  - 経済産業省　情報セキュリティ人材の育成指標等の策定　主査
  - 内閣官房情報セキュリティセンター　セキュリティ人材育成委員会　委員
  - 情報通信機構　実践的サイバー防護演習　実行委員会　推進委員

会社概要

NRI 野村総合研究所グループにおける情報セキュリティ専門の中核企業

- **本社所在地： 東京都千代田区大手町１-７-２　東京サンケイビル**
- **代表取締役社長　小田島　潤**
- **設立：　２０００年８月１日**　※サービス提供は１９９５年より開始
- **資本金：４．５億円**

- **拠点**
  - 東京　（本社）
  - 横浜　（テクニカルセンター）
  - Irvine, CA　（北米支社）
- **グループ会社**
  - 株式会社ユービーセキュア　（東京都港区）
- **社員数**　（連結）：391名　　（単体）：335名

- **資格取得者数**
  - 高度情報処理技術者　：　のべ460名　（うち情報セキュリティスペシャリスト　172名）
  - CISA(Certified Information System Auditor)　：　74名
  - CISM(Certified Information Security Manager)　：　40名
  - CISSP(Certified Information Systems Security Professionals)　：　36名
  - GIAC(Global Information Assurance Certification)　：　のべ155名

- **ＩＳＯ／ＩＥＣ 27001認証取得**

IS 75215 / ISO 27001:2013

- **サービス提供実績**
  - 官公庁、金融、流通、製造、製薬、　通信、マスコミ　等500社以上に運用サービスを提供
  - 一次的なスポットサービスを含めると2000社以上にサービス提供

（2017年6月1日現在）

事業概要

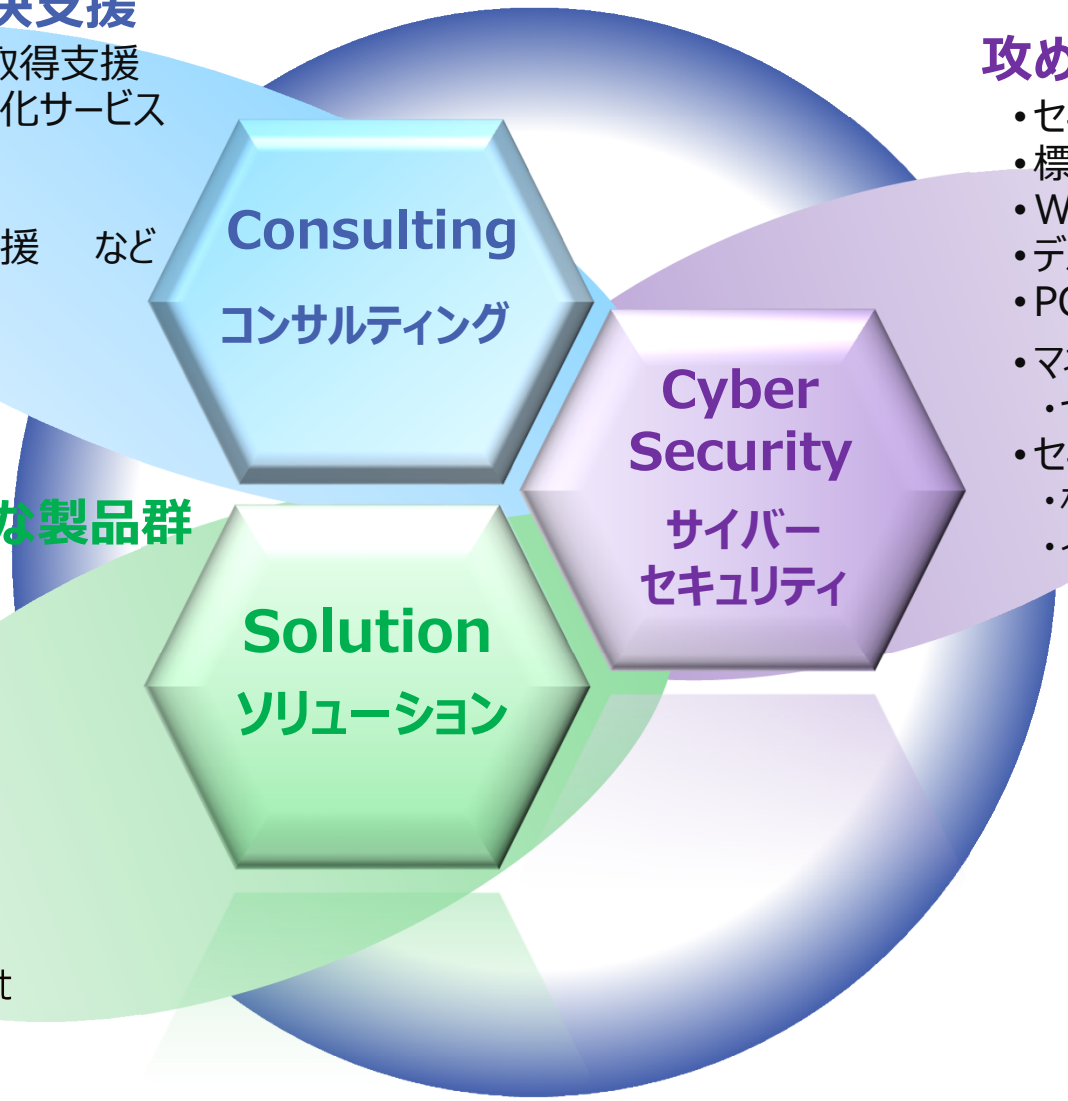
コンサルティング・サイバーセキュリティ・ソリューションのすべてを提供

高い専門性による解決支援

- PCI DSS等、各種認証取得支援
- セキュリティ対策状況可視化サービス
- CIO、CISO支援
- CSIRT構築支援
- セキュリティポリシー策定支援　など

攻めと守りのサイバー攻撃対策

- セキュリティ診断
- 標的型メール攻撃シミュレーション
- Webサイト探索棚卸し
- デバイスセキュリティ診断
- PCI DSS　ペネトレーションテスト　など
- マネージドセキュリティサービス(MSS)
  - セキュリティ機器運用監視
- セキュリティログ監視サービス
  - 相関分析監視
  - インシデントレスポンス　など



対策を実現する多様な製品群

- Access Check
- PC Check Cloud
- Cryptobin
- POSTUB
- Contents EXpert
- Uni-ID

ナビゲーション活動 -独自分析による情報発信-
国内調査2017：『企業における情報セキュリティ実態調査 2017』

目的

- 国内の大手・有力企業における
  情報セキュリティに対する取り組み状況を明らかにする
- 企業の情報システム・情報セキュリティ関連業務に携わる方へ
  有益な参考情報を提供する

時期

2016/09/05 ～ 2016/10/14

方法

郵送およびWebによるアンケート

対象

3,000社 (東証１部・２部上場企業とJASDAQ上場企業、マザーズ上場企業、地方上場企業および未上場企業で従業員の数が多い企業)
の情報システム・情報セキュリティ担当者

回答社数 (回収率)

671社 (22.4%)

https://www.nri-secure.co.jp/security/report/2016/analysis.html

ナビゲーション活動 -独自分析による情報発信-

国際比較調査：『NRI Secure Insight 2017 企業における情報セキュリティ実態調査 ～グローバル編～』

目的

3カ国（アメリカ、シンガポールおよび日本）の企業における
情報セキュリティの**対策状況の可視化**

時期

2016/11/21 ～ 2016/12/5

方法

Webによるアンケート

対象

従業員500人以上の規模のアメリカ、シンガポールの企業
※日本のデータは「企業における情報セキュリティ実態調査2017」から従業員500人以上の企業を抽出

回答社数

1,108社（500社(アメリカ)+134社(シンガポール)+474社(日本)）

https://www.nri-secure.co.jp/security/report/2016/analysis_global2017.html

目次

1. NRIセキュア 国内調査 2017
『企業における情報セキュリティ実態調査 2017』 **【FACT】**

2. NRIセキュア 国際比較調査
『NRI Secure Insight 2017 企業における情報セキュリティ実態調査 ～グローバル編～』 **【FACT】**

3. 企業をとりまく情報セキュリティの状況 **【動向把握】**

4. 情報セキュリティ対策のあり方 **【提言】**

EXECUTIVE SUMMARY

01 セキュリティ戦略
対策実施理由の１位は“自社の”セキュリティインシデント

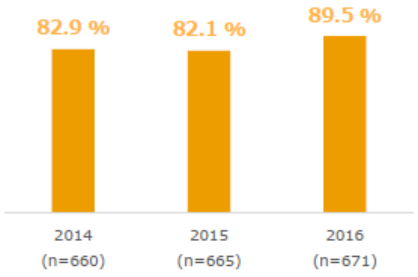
- ✓ 自社・他社を問わずセキュリティインシデントが対策実施理由の上位
- ✓ セキュリティ人材の不足傾向がより顕著に

■情報セキュリティ対策の実施にいたったきっかけ

1位	41.7 %	自社のセキュリティインシデント
2位	33.7 %	経営層のトップダウン指示
3位	32.0 %	他社のセキュリティインシデント事例

（n=671、複数回答）

■情報セキュリティ人材が不足している企業



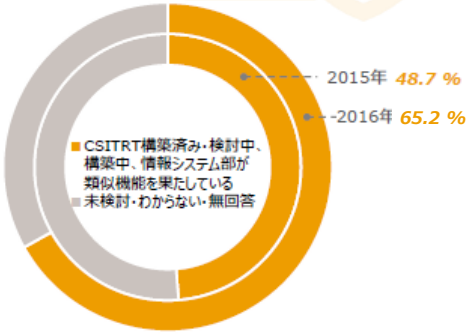
02 セキュリティ施策
サイバーセキュリティリスクの顕在化が事後対策の機運を後押し

- ✓ 標的型メール攻撃、ランサムウェアによる事件・事故が台頭
- ✓ 組織内CSIRTを構築または検討している企業が半数を突破

■過去１年間で発生した事件・事故

	2015 (n=665)	2016 (n=671)	
1位	37.1 %	35.6 %	電子メール、FAX、郵便物等の誤送信・誤配送
2位	17.3 %	34.1 %	標的型メール攻撃
3位	New	32.5 %	ランサムウェアによる金銭等の要求
4位	26.0 %	31.0 %	マルウェア感染
5位	33.7 %	28.9 %	情報機器・外部記憶媒体の紛失・置き忘れ・棄損

■組織内CSIRTの構築状況

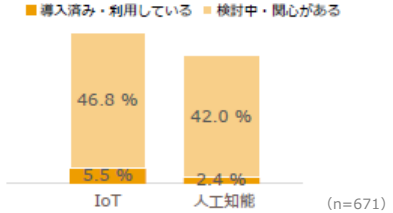


（2016年 n=671、2015年 n=665）

03 IoT・クラウド
IoTへの関心は高いが、ビジネス活用できている企業は少ない

- ✓ 新技術の関心の上位はIoTと人工知能
- ✓ 既にIoTに関する製品リリースや運用を行っている企業も存在する
- ✓ IoTに係る課題として、サイバー攻撃リスクの増大を挙げている企業が多い

■検討中・関心がある新技術



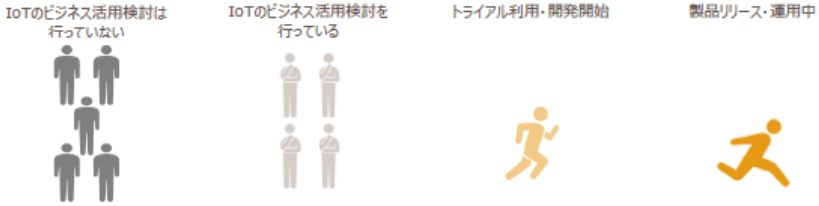
（n=671）

■IoTに係る課題認識

1位	59.8 %	IoTを活用したビジネスモデルの策定
2位	41.9 %	機器をインターネットに接続することによるサイバー攻撃リスクの増大
3位	30.2 %	IoTに関して専門性を有する技術者の確保

（n=351、複数回答）

■IoTに関する検討フェーズ



（n=351）

04 グローバル・ガバナンス
法令順守対応が国内の5.1倍となり、ずば抜けてギャップが大きい

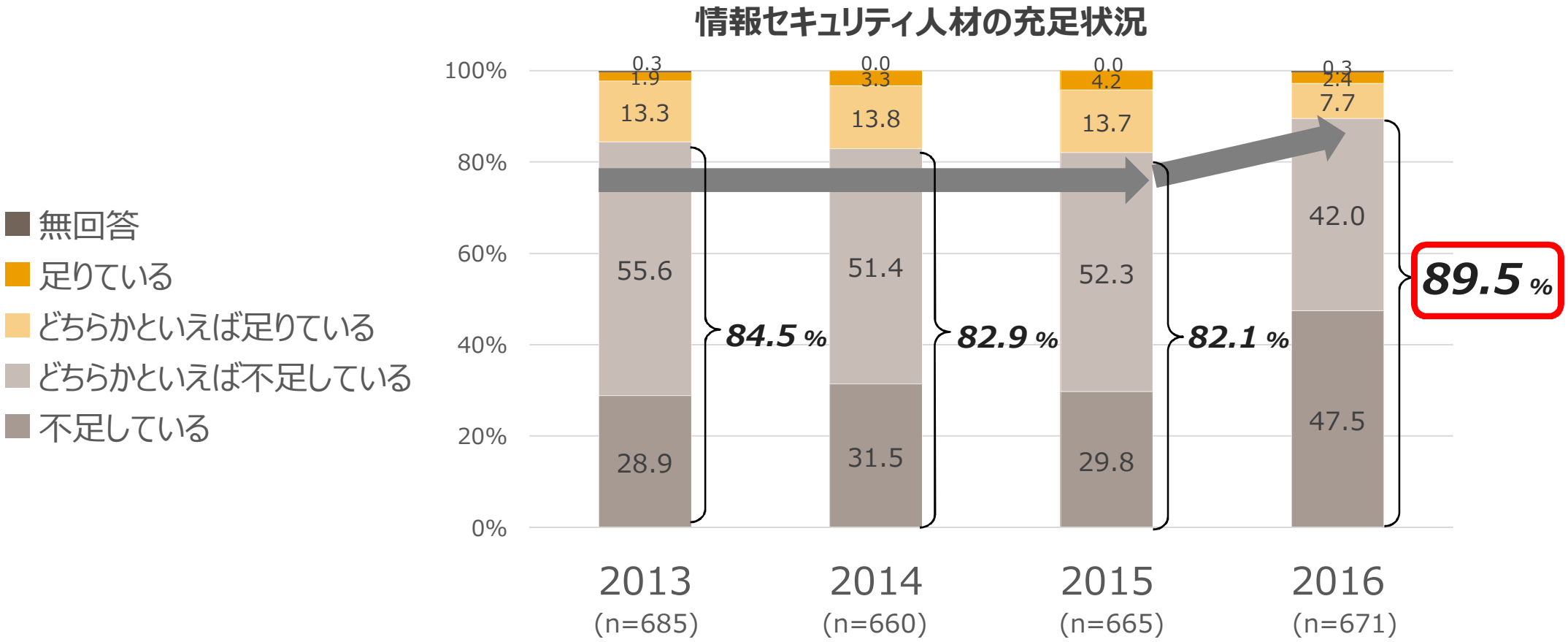
- ✓ 現地事情や物理的制約に起因する課題ほどギャップ大

■国内および海外拠点のセキュリティ統制に伴う課題　※同一標本の中で、海外の課題意識と国内の課題意識を比較

5.0倍～	5.1倍 法令遵守対応（国による法令の差異等）
	2.9倍 セキュリティルール類の整備が困難
	2.8倍 IT機器・サービスの調達・仕様の全体最適化が困難
2.5倍～	2.7倍 IT利活用のモニタリング・資産管理が困難
	2.4倍 現地との情報共有の高度化・効率化
	2.3倍 法人格が違うことにより、セキュリティ統制がきかせにくい
2.0倍～	1.9倍 M&Aや合弁化等により、セキュリティ統制がきかせにくい

（国内 n=671、海外 n=377）

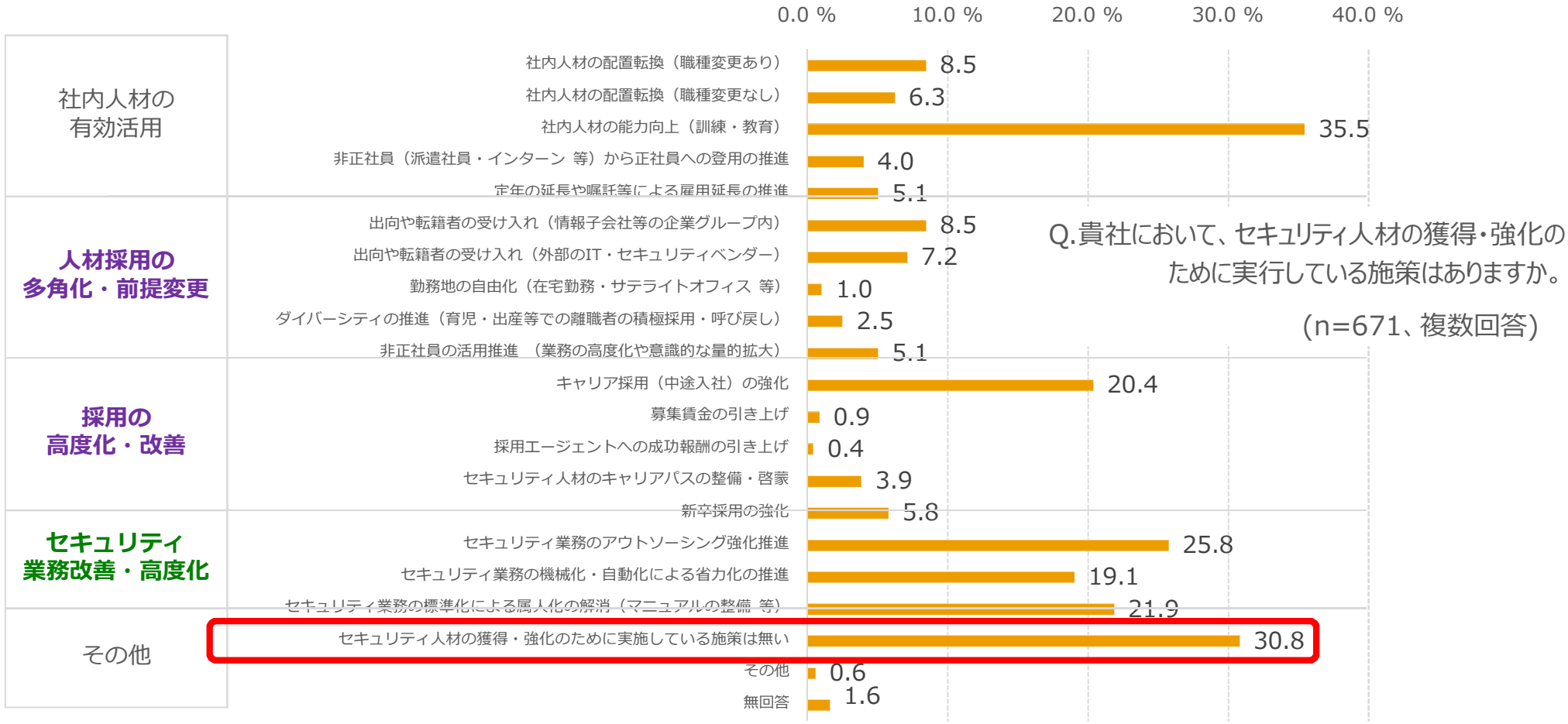
セキュリティ人材
情報セキュリティ人材の充足状況



Q.貴社の情報セキュリティの管理や、社内システムのセキュリティ対策に従事する人材の充足状況はいかがですか。

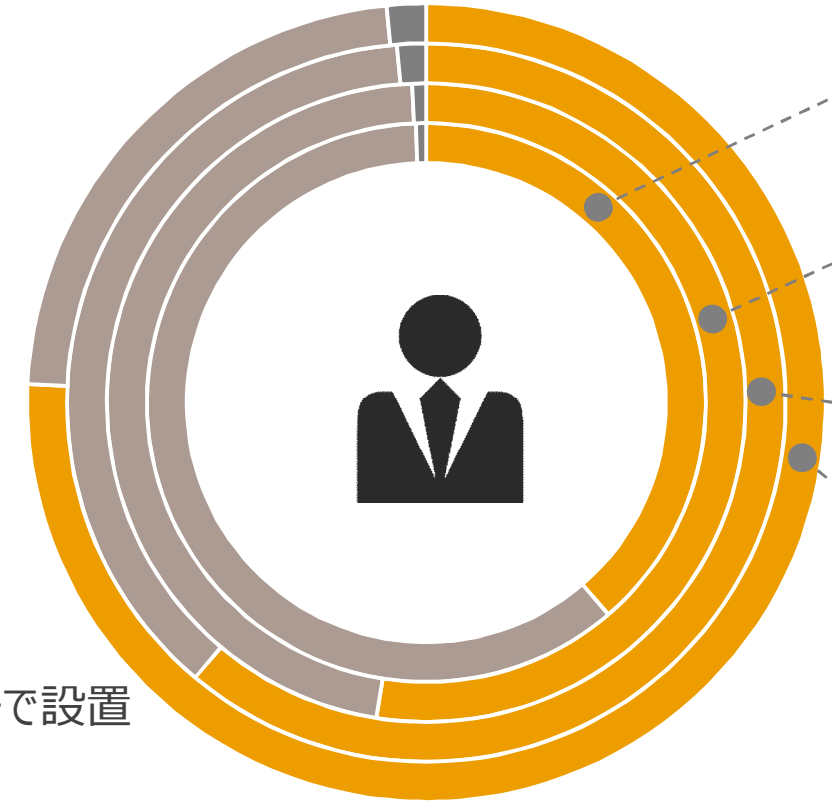
- **セキュリティ人材の不足傾向がより顕著に。 9割近くの企業で人材不足**
- **昨今のセキュリティ脅威の深刻化で、業務量の増加 & 仕事の質の向上が求められる**

セキュリティ人材
情報セキュリティ人材の獲得・強化の実効策



- 人材不足対策として**業務改善**の実施率は高いが、**人材採用施策**の実施率は低い傾向
- 約3割の企業で、セキュリティ人材の獲得・強化の施策は未実施(労力を捻出できず)

セキュリティ人材
情報セキュリティを統括する人材の設置状況



CIO（最高情報システム責任者）
38.7 %

CISO（最高情報セキュリティ責任者）
52.5 % が未設置

CRO（最高リスク責任者）
61.1 %

CTO（最高技術責任者）
75.7 %

- 未設置
- 専任または兼任で設置
- 無回答

Q.情報システムおよび、情報セキュリティを統括する人材の設置状況はいかがですか。(n=671)

[参考]2015年度（n=660）
CISO未設置：53.4%

■ **最高情報セキュリティ責任者（CISO）は、半数以上の企業で未設置**
→ 情報セキュリティにおける意思決定の遅延や、統率力・一貫性に懸念

1. NRIセキュア 国内調査 2017
『企業における情報セキュリティ実態調査 2017』 【FACT】

2. NRIセキュア 国際比較調査
『NRI Secure Insight 2017 企業における情報セキュリティ実態調査 ～グローバル編～』 **【FACT】**

3. 企業をとりまく情報セキュリティの状況 【動向把握】

4. 情報セキュリティ対策のあり方 【提言】

EXECUTIVE SUMMARY

調査概要

目 的

- アメリカ、シンガポール、日本の企業における情報セキュリティに対する取り組み状況を明らかにする
- 企業の情報システム・情報セキュリティ関連業務に携わる方へ有益な参考情報を提供する

調査対象

- 従業員規模 500 人以上のアメリカ、シンガポール、日本企業の情報システム・情報セキュリティ担当者

回答いただいた企業数

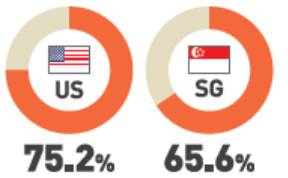
- 計 1108 社 (アメリカ :500 社、シンガポール :134 社、日本 :474 社)

サイバー保険

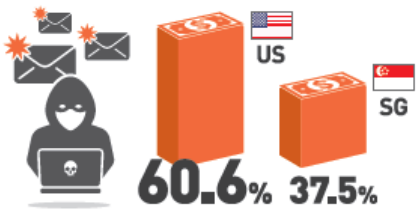
過去 1 年のサイバー保険加入状況

ビジネスメール詐欺

過去 1 年間で金銭詐取を目的とした送金指示等の不正なメールをユーザが受信した企業



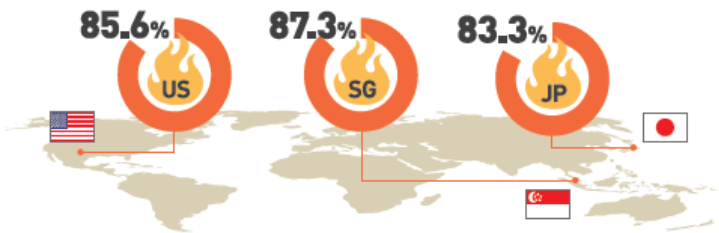
過去 1 年間でビジネスメール詐欺 (BEC※1) により金銭被害に遭った企業※2 (US=376、SG=88)



※1 ビジネスメール詐欺の略称。経営幹部や経理担当、取引先の実在する人物を騙り、金銭を騙し取る詐欺の手口のこと
※2 回答した企業は金銭詐取を目的とした送金指示等の不正なメールをユーザが受信した企業

セキュリティインシデント

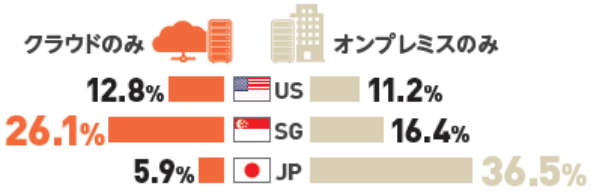
過去 1 年に情報セキュリティインシデント※1 が発生した企業



※1 サイバー攻撃、内部不正、あるいはヒューマンエラー等により発生した事件・事故を指す

クラウド

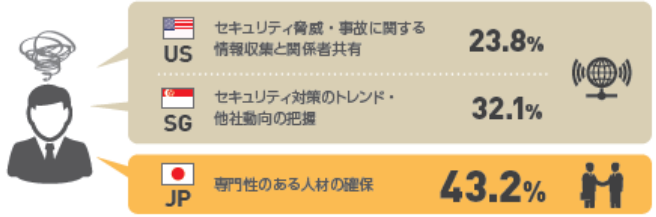
使用する情報システムがクラウドのみ / オンプレミスのみの企業※1



※1 上記グラフはクラウドのみ / オンプレミスのみを使用する企業のデータのみ表しており、クラウド・オンプレミス両方を使用している企業、及びクラウド・オンプレミスのどちらも利用していない企業のデータは含まない
なお、「情報システム」は顧客向けシステム、基幹業務システム、情報システムを指し、「クラウド」は IaaS、PaaS、及び SaaS を指す

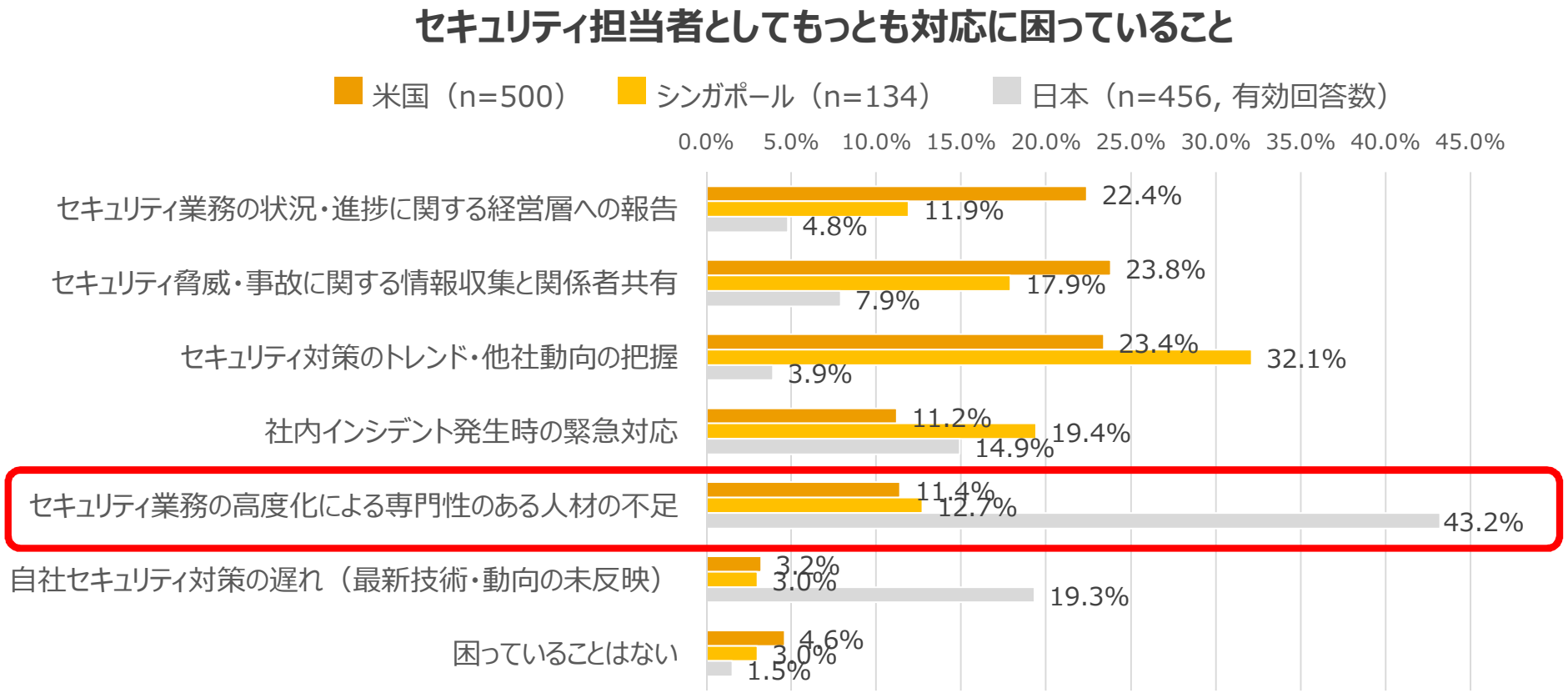
人 材

情報セキュリティ担当者が最も対応に困っていること



専門性の高い人材の確保はアメリカ、シンガポールにおいて 4 位であった (US : 11.4%、SG : 12.7%)

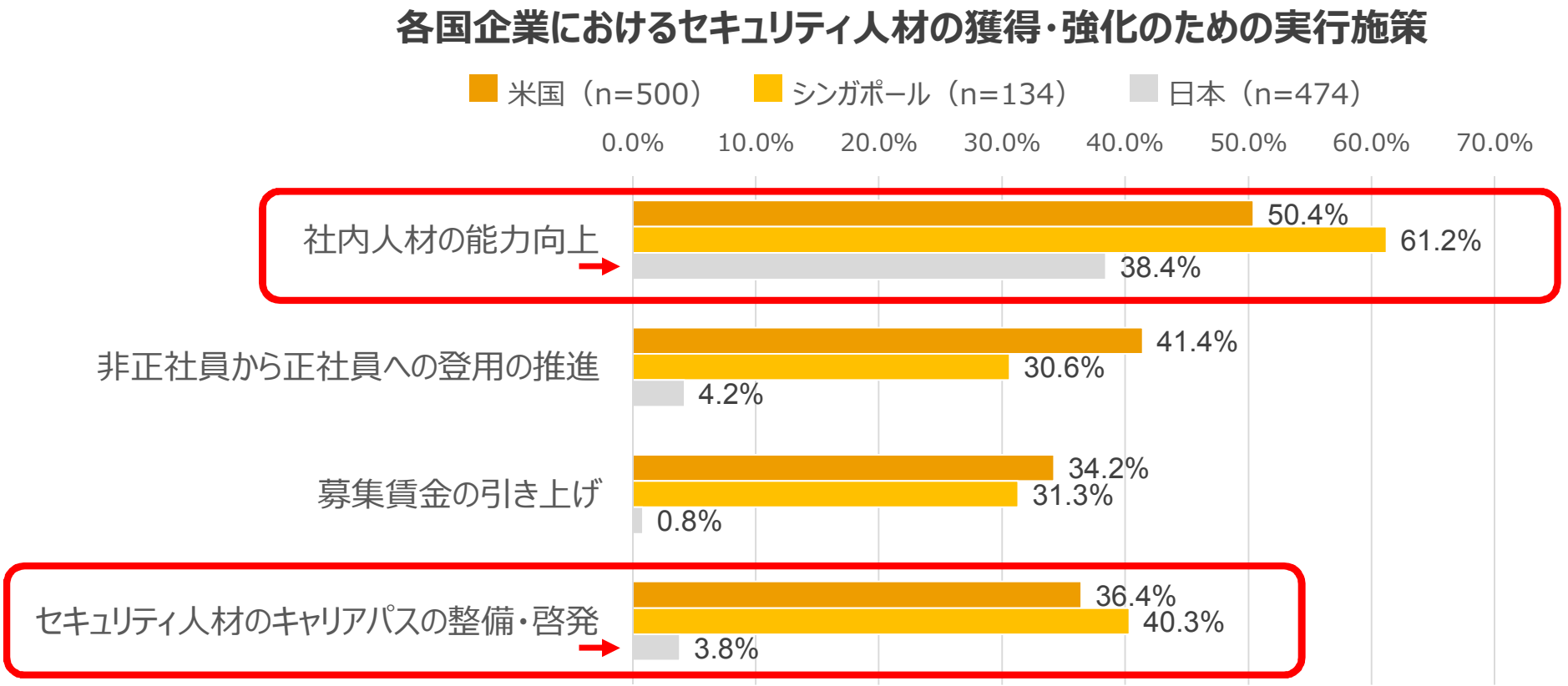
セキュリティ人材
セキュリティ担当者が困っていることの国別差異



Q.企業のセキュリティ担当者として、もっとも対応に困っていることは何ですか。

- **日本企業は「人材不足」が顕著**
- **米国/シンガポール企業は、より具体的な「セキュリティ業務内容」にシフト**

セキュリティ人材
セキュリティ人材を獲得・強化する施策の実施状況



Q.貴社において、セキュリティ人材の獲得・強化のために実行している施策はありますか。

■ **セキュリティ人材の獲得・強化策として、日本は「社内人材の能力向上」に偏重**
→ キャリアパス整備・啓発も含め、他の施策とのバランシングが肝要

1. NRIセキュア 国内調査 2017
『企業における情報セキュリティ実態調査 2017』 【FACT】

2. NRIセキュア 国際比較調査
『NRI Secure Insight 2017 企業における情報セキュリティ実態調査 ～グローバル編～』 【FACT】

3. 企業をとりまく情報セキュリティの状況 【動向把握】

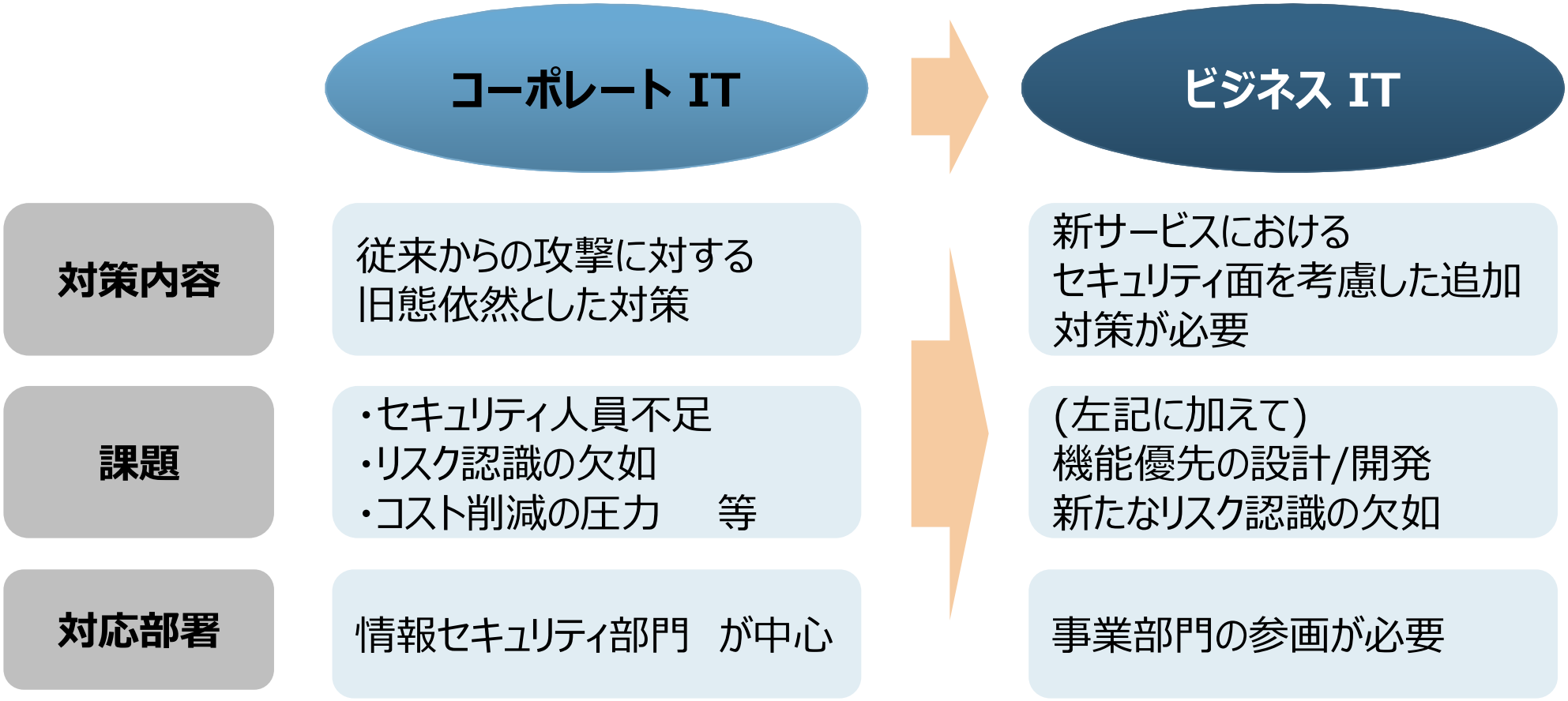
4. 情報セキュリティ対策のあり方 【提言】

自社の課題解決とビジネス拡大を支えるセキュリティ　　【内部要因】
コーポレートITからビジネスITへ

■コーポレートIT から　ビジネスIT へのシフトに伴い、セキュリティ対策にも変化

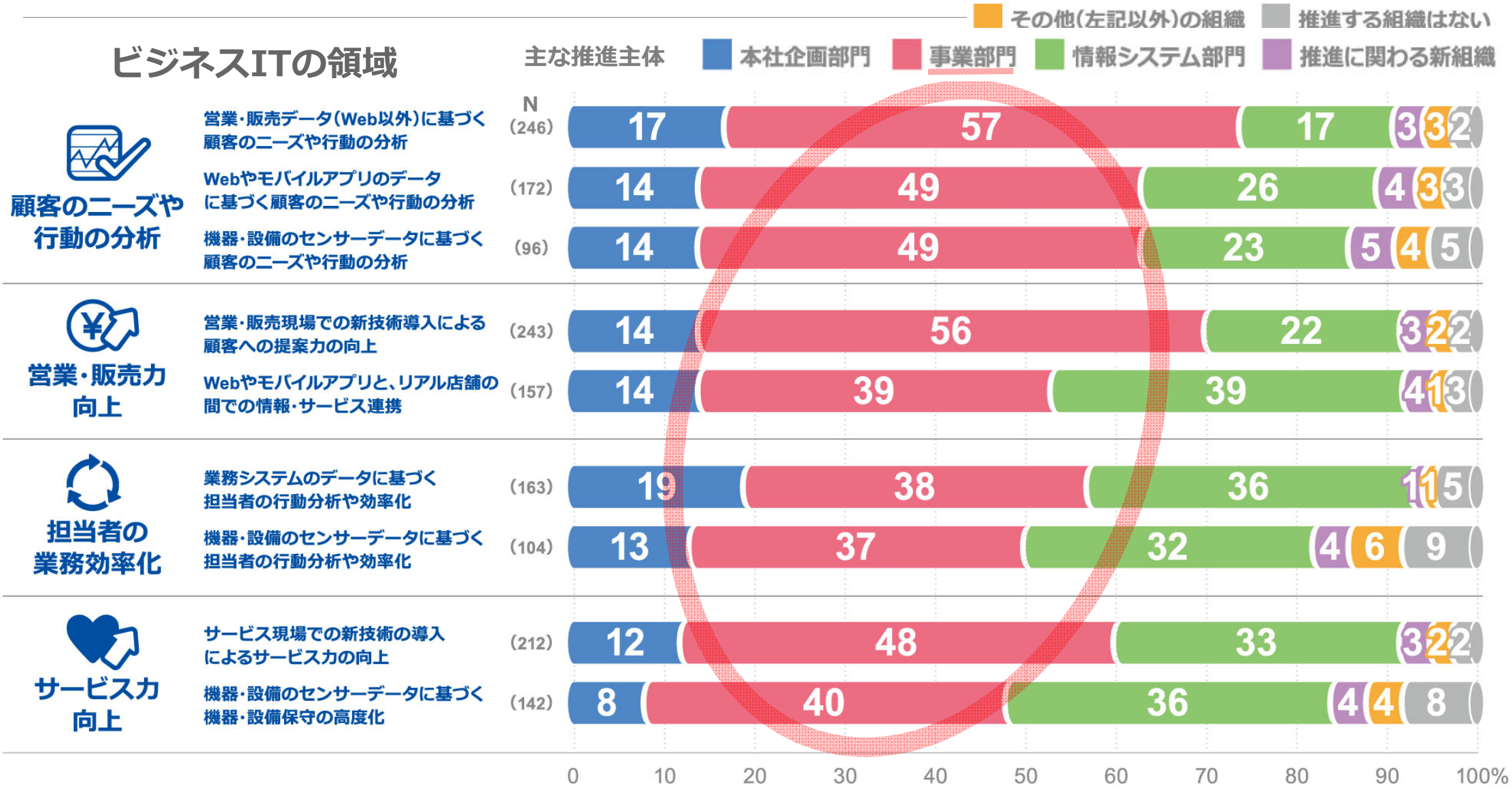
■ビジネス領域を拡大するにあったっては、(従来とは違った)セキュリティ対策を十分固める必要あり

■情報セキュリティ部門だけでなく、事業部門も参画し、対策検討。セキュリティ対策が差別化ポイントに



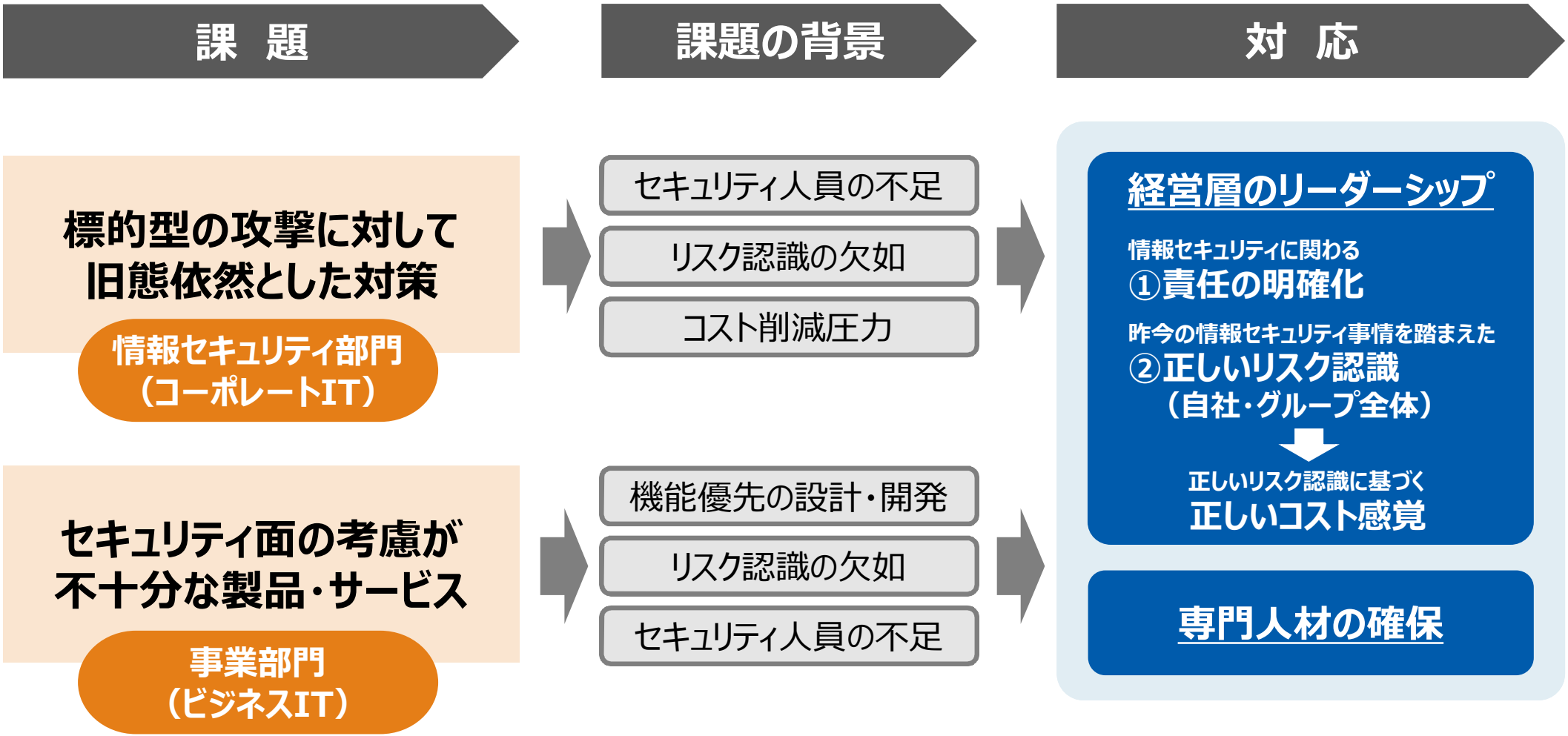
3. 企業をとりまく情報セキュリティの状況 【動向把握】

ビジネスITの領域は、ビジネス部門が主体となっている企業が多い



出所) 野村総合研究所 「2015年度IT活用実態調査」

第３章まとめ



1. NRIセキュア 国内調査 2017
『企業における情報セキュリティ実態調査 2017』 【FACT】

2. NRIセキュア 国際比較調査
『NRI Secure Insight 2017 企業における情報セキュリティ実態調査 ～グローバル編～』 【FACT】

3. 企業をとりまく情報セキュリティの状況 【動向把握】

4. 情報セキュリティ対策のあり方 【提言】

本章のポイント

■ 経営層のリーダシップ

- 情報セキュリティ対策は経営問題であると認識した上で、情報セキュリティ担当役員(CISO)を軸とした管理体制を構築し、全社横断的な取り組みを。

■ 専門人材の育成・確保

- 情報セキュリティ人材の育成・確保は、計画的に進める必要があり、まずは必要な業務の中で内製化(社内人員)とアウトソースの方針決めから。

■ Security By Design

- 特にIoT製品やネットビジネスにおいては、開発の初期段階からセキュリティを考慮して、対策を「組み込んでおく」ことが重要。

■ リスクマネジメント

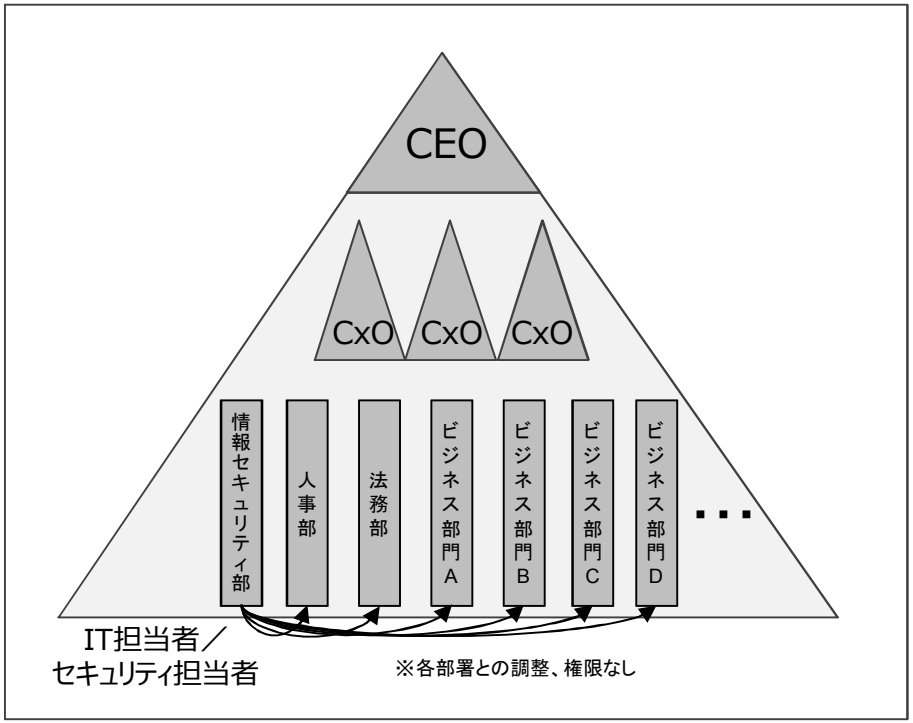
- つまるところ、リスクマネジメント。リスクの合理的管理とその説明責任を負うこと。
  場合によっては、対策を行わない（リスク保有）という経営判断もあり。
  リスクをきちんと認識した上で、多層防御を意識してバランスの良いセキュリティ対策を。

4．情報セキュリティ対策のあり方　【提言】

経営層のリーダーシップ
情報セキュリティの管理体制

＜現在の情報セキュリティ管理体制＞

情報セキュリティ部などが情報セキュリティを主管し、他部署とは施策ごとに調整

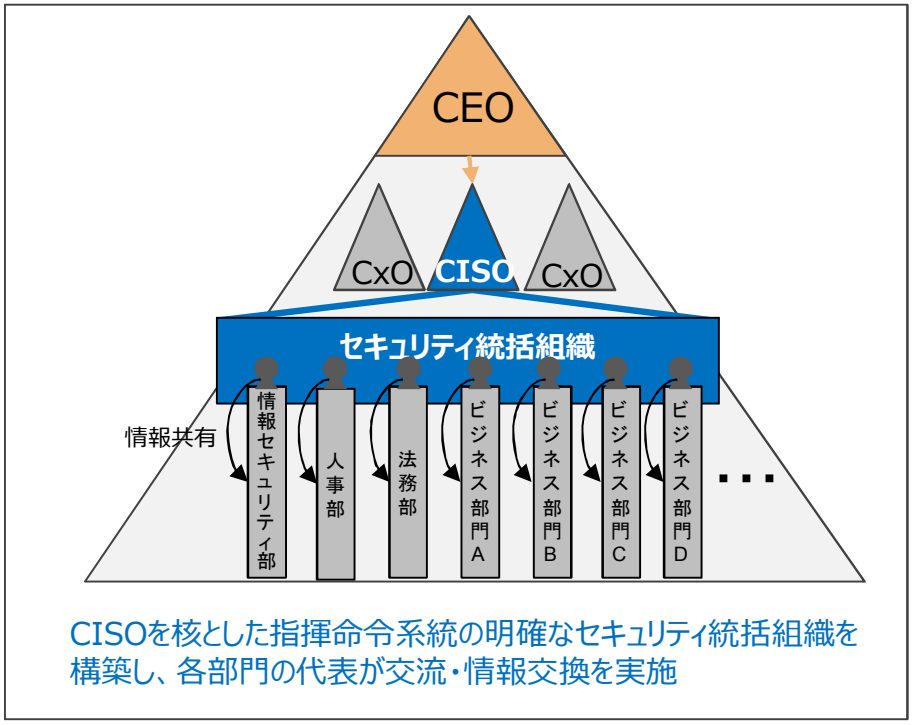


課題

- セキュリティ人材の確保などの部署横断的な連携に時間がかかってしまう
- セキュリティ対策状況の全体を把握できておらず、定期確認をしていないため、高度な攻撃に対応できていない可能性がある
- ビジネス部門で情報セキュリティ活用の機運が高まっているが、ノウハウ共有ができない、セキュリティを担保できない懸念がある

＜今後目指すべき情報セキュリティ管理体制＞

セキュリティ経営実現のためCEOとCISOが協調し
セキュリティ施策を横串で束ねる組織を設置



CISOを核とした指揮命令系統の明確なセキュリティ統括組織を構築し、各部門の代表が交流・情報交換を実施

効果

- 部署横断的な施策を担当役員（CISO）のリーダーシップの下、実施可能
- 自社のセキュリティ戦略に沿った網羅的かつ高度化されたセキュリティ対策が可能
- 情報セキュリティ部門で培ったノウハウの活用やセキュリティ対策のできていない製品のリリースなどを防げる可能性がある

専門人材の育成・確保
人材育成の５ステップ

必要な社内人員の決定
Step 1

セキュリティ関連業務を洗い出し、内製化か社外委託かを選別

（次ページ参照）

スキル棚卸
Step 2

業務に必要なスキルの棚卸

システム・セキュリティ関連スキル
- セキュリティ要件の定義
- セキュアデザイン
- セキュアコーディング
- 脆弱性診断の結果の理解

基盤関連スキル
- ネットワーク・システム構築
- ネットワーク・システム運用

CSIRTメンバー
- インシデント対応能力
- フォレンジック能力
- サイバーインテリジェンス関連スキル

フレームワーク化
Step 3

キャリアパス、ローテーション等既存育成計画に組み入れ

フレームワーク・ツール
- キャリアパス
- 職務・ポジション
- 育成計画
- ローテーション

研修プログラム選定
Step 4

社内、社外の研修プログラムの選定

選定の6つのポイント
- 業務に適合した内容
- 体系立った内容
- 実践的な内容
- 復習可能な教材
- 定評、実績ある研修
- 評価・測定可能な研修

スキルの可視化
Step 5

推奨資格等スキルの可視化

国内資格
- 情報処理技術者試験
- 情報処理安全確保支援士
- 情報セキュリティ監査人

等

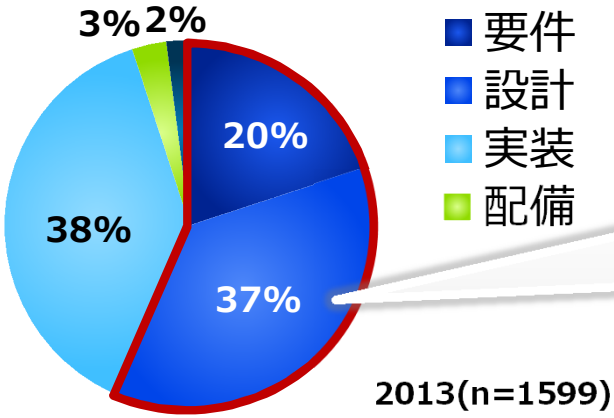
グローバル資格
- GIAC
- CISSP
- CISA、CISM

等

Security By Design
開発の初期の段階からセキュリティの考慮が必要

アプリケーションの開発工程別 支援アプローチ

開発フェーズ別の脆弱性発見割合

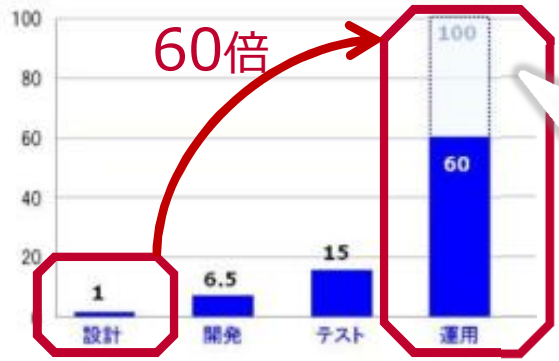


2013(n=1599)

診断で発見された
脆弱性の半数以上が、
要件定義・設計フェーズ
で作り込まれていた

出所）NRIセキュア Webサイトのセキュリティ診断：傾向分析レポート2014より
(同一の問題を個別のWebサイトで検出した場合は、複数回カウント)

開発フェーズ別の脆弱性修正費用



脆弱性の
修正費用比較

リリース後では、
設計時での 60倍

出所）Kevin Soo Hoo他 “Tangible ROI through Secure Software Engineering”
Secure Business Quarterly FOURTH QUARTER 2001

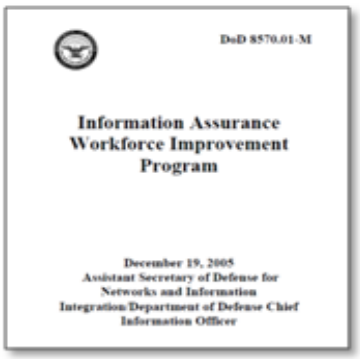
4. 情報セキュリティ対策のあり方 【提言】

- **サイバーセキュリティのリスクは、今日では企業経営を揺るがしかねない問題となっている**
  - 「今」の状況に対応するのではなく、将来を見据えた対策が必要
- **ITが、コーポレートITからビジネスITに比重を移す中、事業部門のセキュリティ対応が重要になる**
  - 特にIoT製品やネットビジネスでは、初期の段階からセキュリティの考慮が必要
- **経営層が、サイバーセキュリティについての自身の責任とリスクを認識することが肝要である**
  - セキュリティ専門人材は５ステップで計画的に確保
  - CISSPなど資格による人材の可視化も重要

参考資料　海外情報及びセキュリティ資格の概要

U.S. DEPARTMENT OF DEFENSE

US DoD Directicve 8570.1M



IAT Level I	IAT Level II	IAT Level III
A+ Network+ **SSCP**	GSEC Security+ **SSCP**	CASP CISA **CISSP (or Associate)** GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+	**CAP** CASP CISM **CISSP (or Associate)** GSLC	GSLC CISM **CISSP (or Associate)**

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND-SP Manager
CEH GCIA GCIH	CEH **SSCP**	CEH CSIH GCFA GCIH	CEH CISA GSNA	CISM **CISSP-ISSMP**

IASAE I	IASAE II	IASAE III
CASP **CISSP (or Associate)** **CSSLP**	CASP **CISSP (or Associate)** **CSSLP**	**CISSP-ISSAP** **CISSP-ISSEP**

Level I: 0～4年程度の業務経験
Level II: 5年から10年程度
Level III: 10年以上

米国国防総省（The U.S. Department of Defense: DoD）は、効果的にDoDの情報、情報システム、情報インフラを守るため、職員、兵役メンバー、請負業者、DODシステムに特権アクセスをもつユーザーなどすべての情報保証を必要とする人材に対し、「DoD Directive 8570.1M（米国国防総省指令8570.1M ）」を要求しています。
（資格取得義務化）
対象は職員のみならず納入業者にも拡大しています。
納入業者は有資格者が必要人数いなければ、政府のプロジェクトに参加できません。

IAT(Information Assurance Technical)
IAM (Information Assurance Management)
CND (Computer Network Defense)
CNDSP (Computer Network Defense Service Provider)
IASAE (Information Assurance System Architect and Engineer)

※黄色字：(ISC)2提供資格
※GXXX：SANS提供資格
※XX+：CompTIA提供資格

National Initiative for Cybersecurity Education

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

米国ではNIST (National Institute of Standards and Technology)で策定された、NICE (National Initiative for Cybersecurity Education)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

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

President Barack Obama, 29 May 2009

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

mework

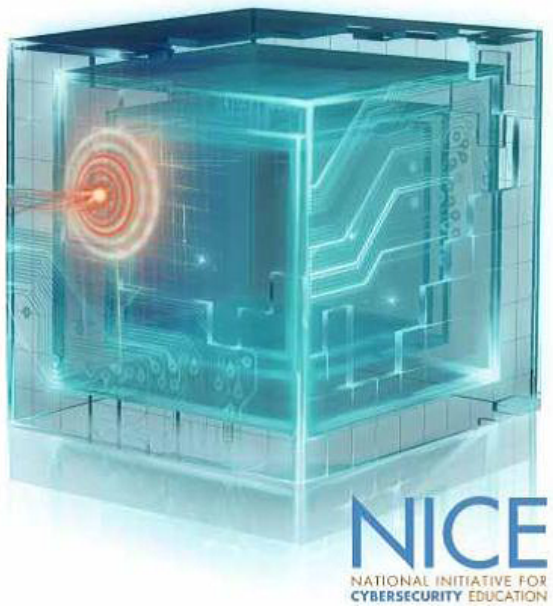
NICE Cybersecurity Workfoce Framework では、サイバーセキュリティに関するタスクと知識を下表の7 種類のカテゴリで分類

	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 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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

NICE　７大分類と31タスク

Security Provision **セキュアな供給**	Information Assurance Compliance 情報保証 コンプライアンス	Software Assurance and Security Engineering ソフトウェア保証と エンジニアリング	Systems Development システム開発	Systems Requirements Planning システム要件計画	System Security Architecture システム　セキュリティ　アーキテクチャ	Technology Research and Development 技術研究開発	Test and Evaluation 試験と評価
Operate & Maintain **運用・保守**	Customer & Tech Support カスタマーサービスと 技術サポート	Data Administration データ管理	Knowledge Mgt ナレッジマネジメント	Network Services ネットワークサービス	System Administration システム アドミニストレーション	Systems Security Analysis システム セキュリティ分析	
Protect & Defend **守備・防衛**	Computer Network Defense（CND） Analysis コンピューター ネットワーク防御分析	CND Infrastructure Support コンピューターネット ワーク防御インフラ支援	Incident Response インシデントレスポンス	Vulnerability Assessment & Mgt 脆弱性アセスメントと管理			
Analyze **分析**	All-source Intelligence 全情報源の諜報活動	Exploitation Analysis エクスプロイト分析	Targets ターゲット	Cyber Threat Analysis 脅威分析			
Collect& Operate **情報収集・運用**	Collection Operations 情報収集オペレーション	Cyber Operations サイバーオペレーション	Cyber Operational Planning サイバーオペレーション計画				
Oversight & Development **監督と開発**	Education & Training 教育と訓練	Information Systems Security Operations 情報システムセキュリティオペレーション	Legal Advice & Advocacy 法的助言と弁護	Security Program Management（CISO） セキュリティ プログラム管理	Strategic Planning & Policy Development 戦略的な計画とポリシー策定		
Investigate **捜査**	Digital Forensics デジタルフォレンジック	Investigation 捜査					



世界のCISSP人数から見た日本の現状

グローバルセキュリティ３大資格
(ISC)2：CISSP
ISACA：CISA
SANS：GIAC

世界のCISSP	117,765人
日本	1,815人
米国	76,858人
韓国	2,745人
香港	1,501人
シンガポール	1,629人
オーストラリア	2,122人

2017年7月17日現在

米国に比べ明らかに少ない　1/65

- 米国政府は積極的にセキュリティ民間資格取得を政府職員に必須・推奨として採用し教育受講費用、資格取得費用を予算化している
- 約30,000人の政府機関職員が取得
- NICEフレームワークで人材育成のフレームワークを明確化

日本においての問題点

- 経営者のセキュリティ教育に対する理解不足
- 政府機関職員は予算不足、定期ローテーションにより資格取得までに至らない
（除く警察庁・防衛省）
- セキュリティ人材のキャリアパス不足

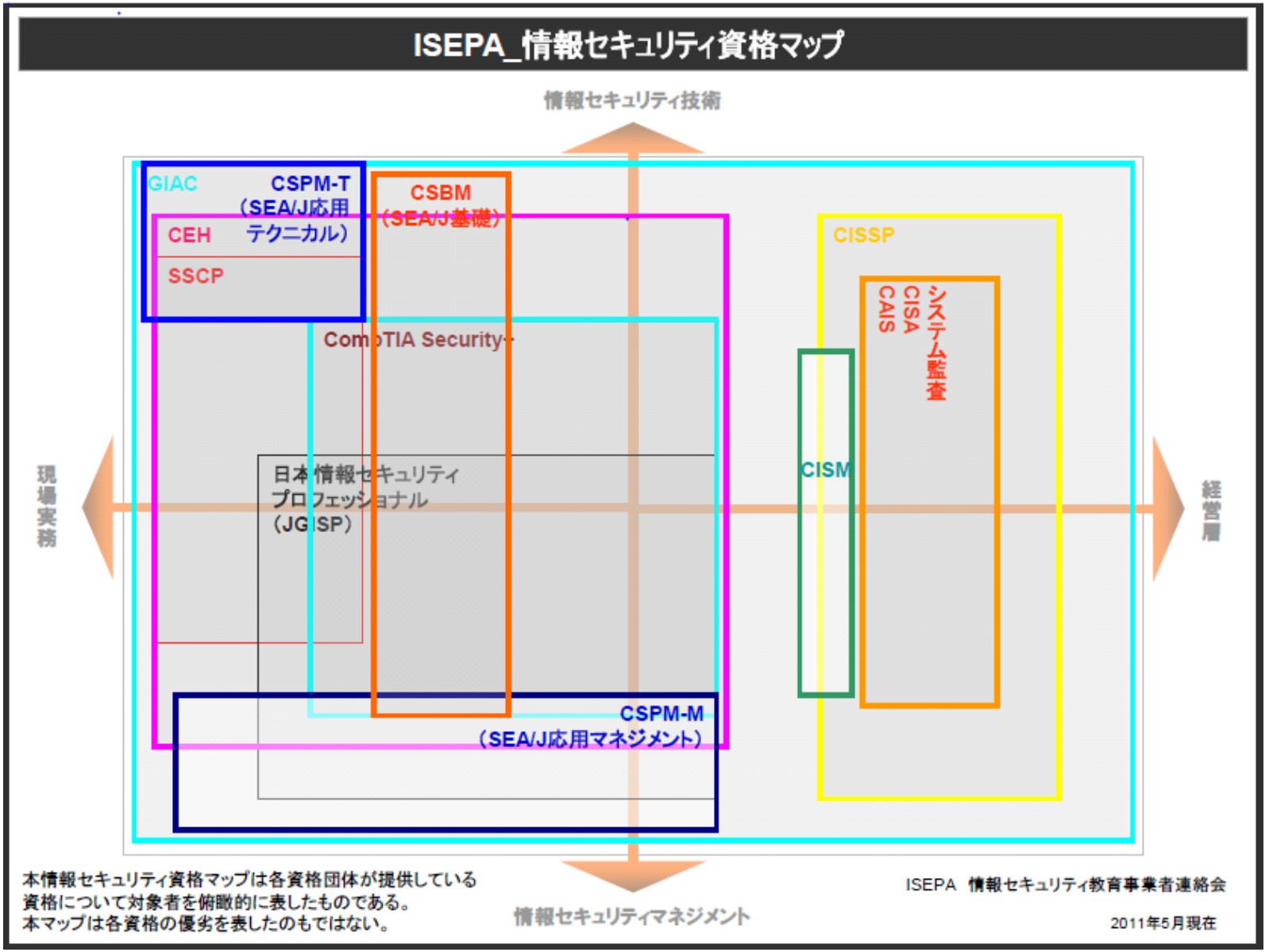
出所(ISC2)Japan
CISSPは(ISC)2が認証する情報セキュリティ専門家の資格です。
https://www.isc2.org/japan/cissp_about.html

主要国におけるCISSPの人数推移

	2010	2011	2012	2013	2014	2015	2016	2017
日本	1,204	1,219	1,249	1,284	1,350	1,475	1,607	1,834
韓国	2,486	2,691	2,853	2,910	2,811	2,706	2,698	2,756
香港	1,299	1,302	1,347	1,376	1,396	1,423	1,437	1,526
中国	466	516	572	741	877	1,153	1,353	1,538
シンガポール	1,023	1,083	1,131	1,182	1,262	1,372	1,493	1,638
オーストラリア	1,599	1,697	1,790	1,836	1,942	1,981	2,229	2,395
インド	1,183	1,290	1,431	1,521	1,616	1,756	1,805	1,945
イギリス	3,489	3,809	4,143	4,459	4,822	5,294	5,742	6,184
アメリカ	45,172	50,440	55,170	59,137	63,269	68,097	73,195	77,495
世界のCISSP	71,176	78,459	85,218	90,934	97,000	104,292	111,774	118,803

出所：(ISC)2　2017年8月現在

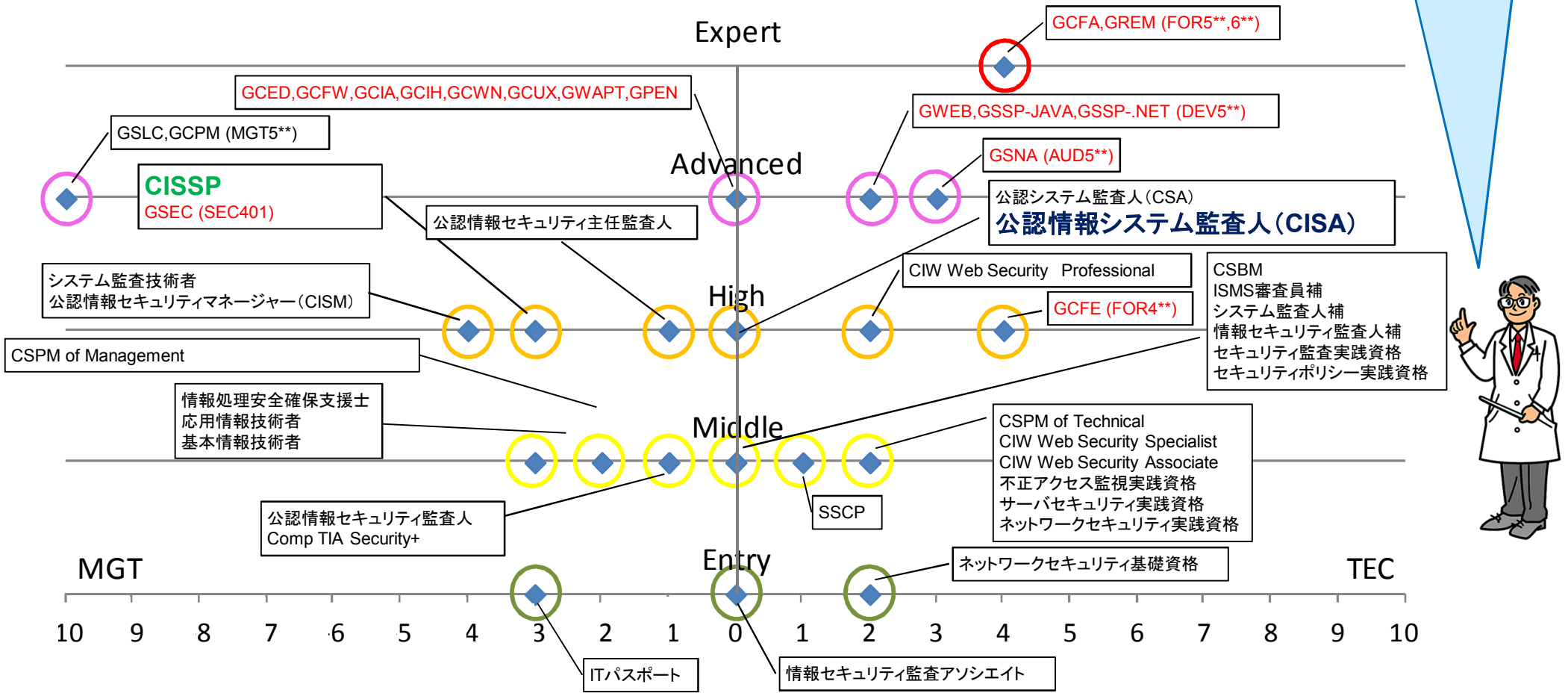
セキュリティ資格情報



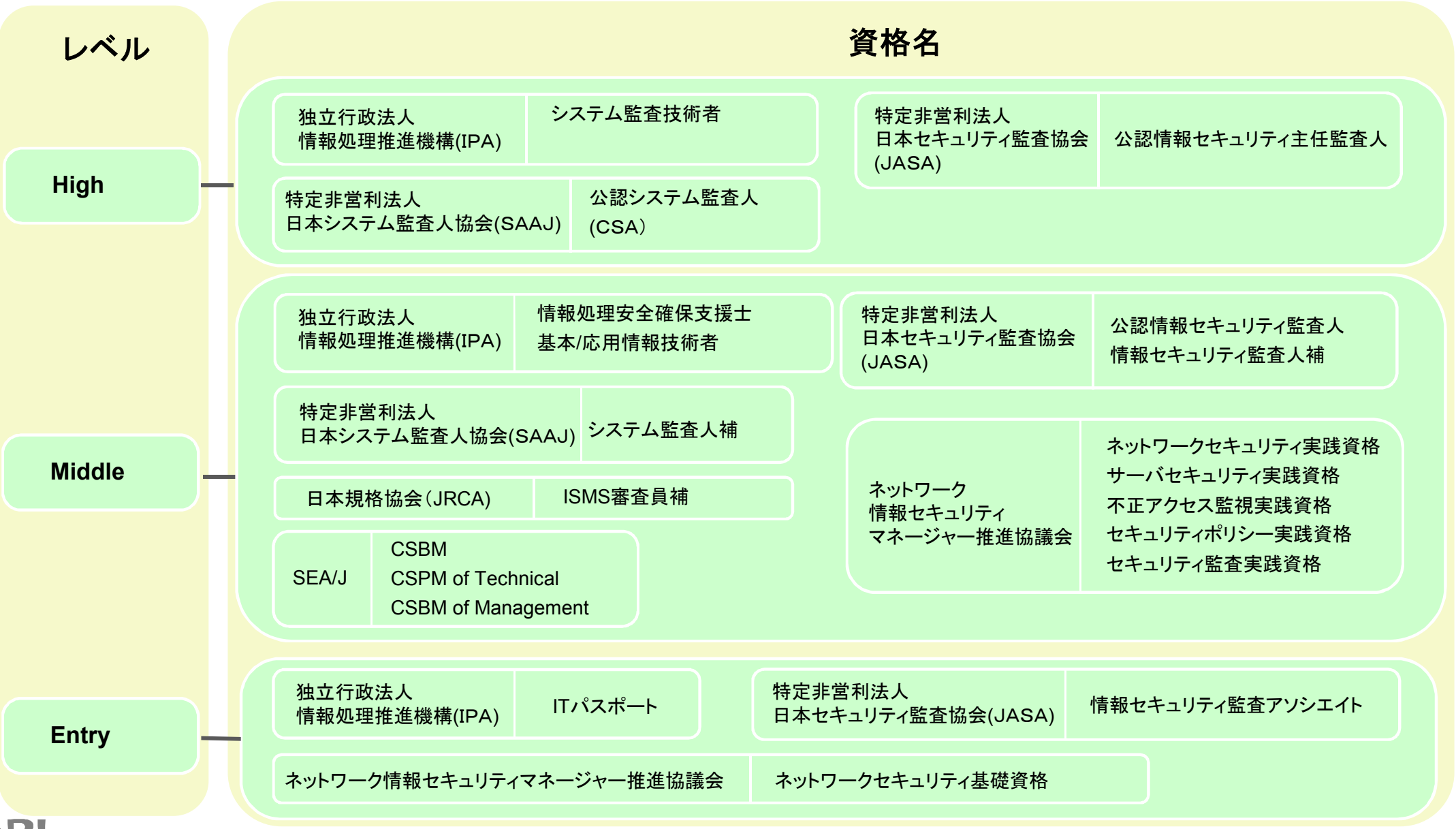
出所ISEPA http://www.jnsa.org/isepa/images/outputs/lisence-map.pdf

情報セキュリティ認定・資格レベルマップ

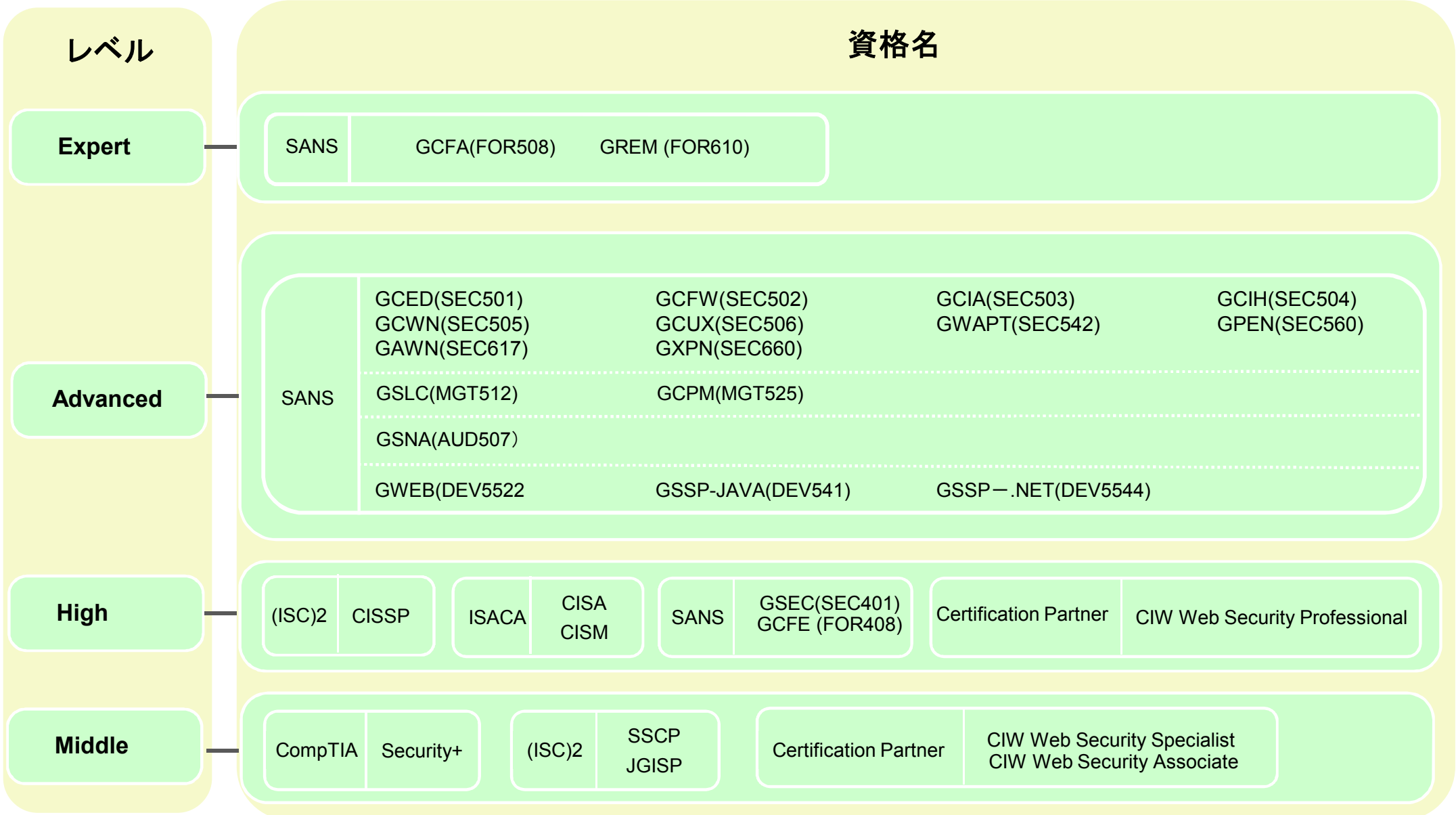
グローバルセキュリティ3大資格
(ISC)2 : CISSP
ISACA : CISA
SANS : GIAC



国内資格のレベルマップ



グローバル資格のレベルマップ



サイバーセキュリティ強化には
プロフェッショナルが必要だ！

NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ
NRI SecureTechnologies