資料４

WG２（経営・人材・国際）の方向性について

経済産業省

商務情報政策局

サイバーセキュリティ課

１．WG２（経営･人材･国際）の目的･ねらい

２．経営

３．人材

４．国際

WG２（経営・人材・国際）設置の目的・ねらい

- 産業サイバーセキュリティ研究会で整理した政策の方向性のうち、４． 基盤の整備のうち、①経営者の意識喚起、②多様なサイバーセキュリティ人材の育成を中心に検討。これに加え、サイバーセキュリティ分野の「国際協力基盤の整備」に関する施策を検討。

サイバーセキュリティ政策の方向性

1．産業政策と連動した政策展開

① 重要インフラの対策強化
－情報共有体制強化　等

② IoTの進展を踏まえたサプライチェーン毎の対策強化 (Industry by industry)
－防衛関係、自動車、電力、スマートホーム等の分野別検討と技術開発・実証の推進

③ 中小企業のサイバーセキュリティ対策強化

2．国際ハーモナイゼーション

① 日米欧間での相互承認の仕組みの構築
② 民間主体の産業活動をゆがめる独自ルールの広がり阻止

3．サイバーセキュリティビジネスの創出支援

① 産業サイバーセキュリティシステムを海外に展開
② サービス認定創設、政府調達などの活用

4．基盤の整備

① 経営者の意識喚起
② 多様なサイバーセキュリティ人材の育成（ICSCoE等）
③ サイバーセキュリティへの過少投資解決策の検討

情報セキュリティ10大脅威2018

- 2017年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案のトップ10をIPAが公表（2018年1月）。
- 従業員への注意喚起・意識向上やセキュリティ人材の確保等、対策のための経営層の理解が必要となる脅威が増加。

順位	内容	昨年順位
1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位
3位	ビジネスメール詐欺	ランク外
4位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
5位	セキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	3位
7位	IoT機器の脆弱性の顕在化	8位
8位	内部不正による情報漏えい	5位
9位	サービス妨害攻撃によるサービスの停止	4位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	9位

ビジネスメール詐欺（3位）
巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の悪用した口座へ送金される詐欺の手口。

セキュリティ人材不足（5位）
脅威の増大、巧妙化に対応するためのセキュリティの知識、技術を有する人材が圧倒的に不足。

１．WG２（経営･人材･国際）の目的･ねらい

２．経営

３．人材

４．国際

（１）経営者の意識の現状
（２）サイバーセキュリティ経営ガイドライン
（３）経営者の意識改革に向けた対策案

セキュリティに関する経営層の関わり

- 海外と比較すると日本の企業は情報セキュリティに関する意思決定において経営層の関わりが薄い。

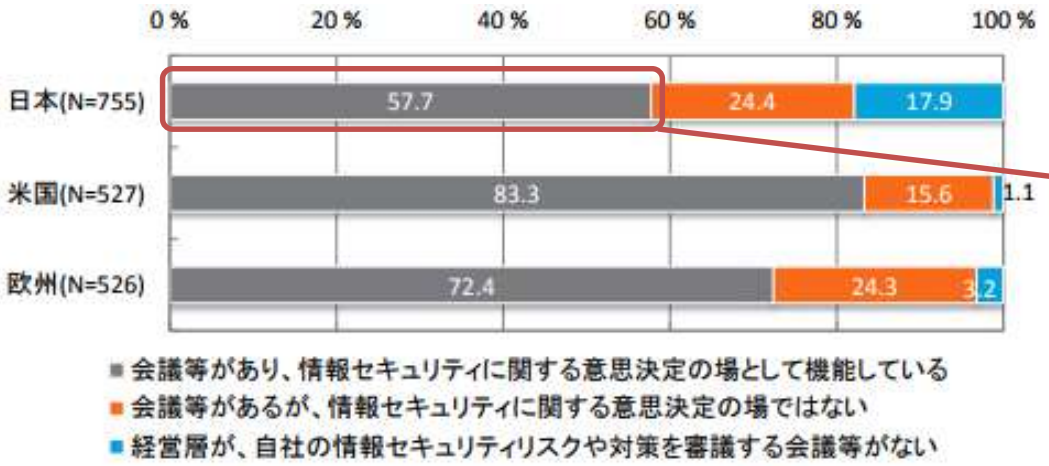


図 5.3-2 経営層の情報セキュリティに対する関与

経営層が積極的にセキュリティに関与している企業は6割弱

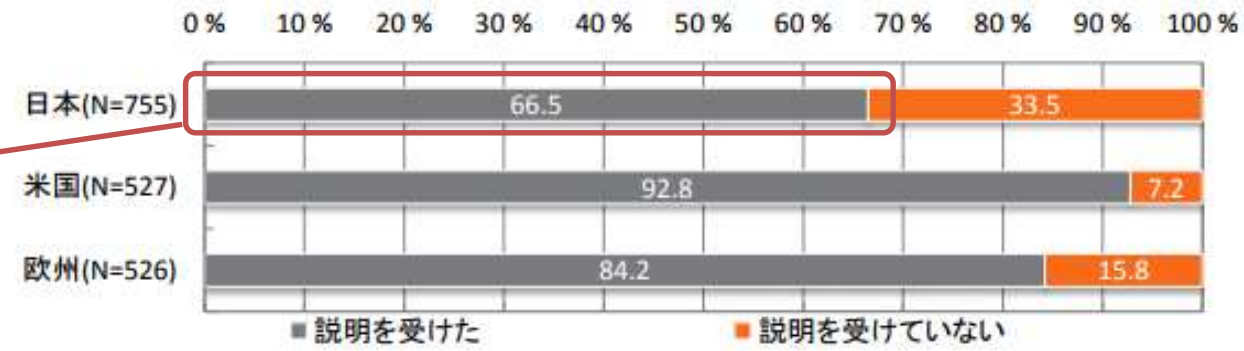


図 5.3-1 経営層または上司からの説明状況

セキュリティが経営上のリスクの1つであることを上司から説明を受けている企業は7割弱
（米国は9割強）

出典：企業のCISOやCSIRTに関する実態調査2017(IPA)

セキュリティ対策に関する責任者（CISO等）の設置状況

- 欧米ではCISOは経営層、又は経営層直下に設置されており、スピード感を持った対応を実施できている。一方で、日本企業は情報システム部門のトップをCISOに任命しているケースが多く、ボトムアップで対策が取られている。

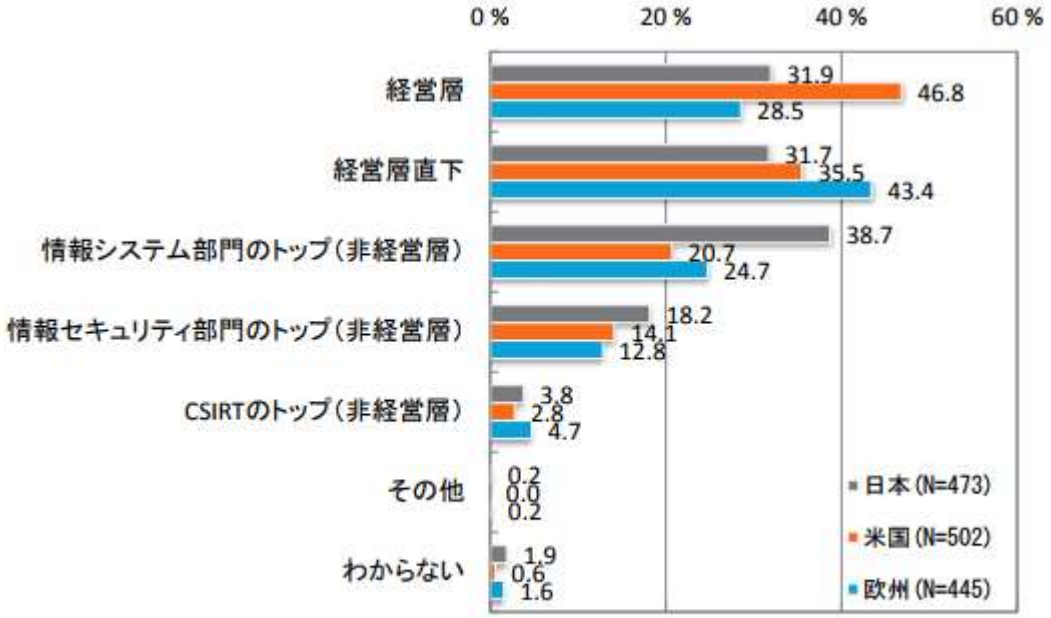


図 5.6-3　CISO 等の組織内の位置づけ

出典：企業のCISOやCSIRTに関する実態調査2017(IPA)

【現場の声】(経済産業省ヒアリングによる)

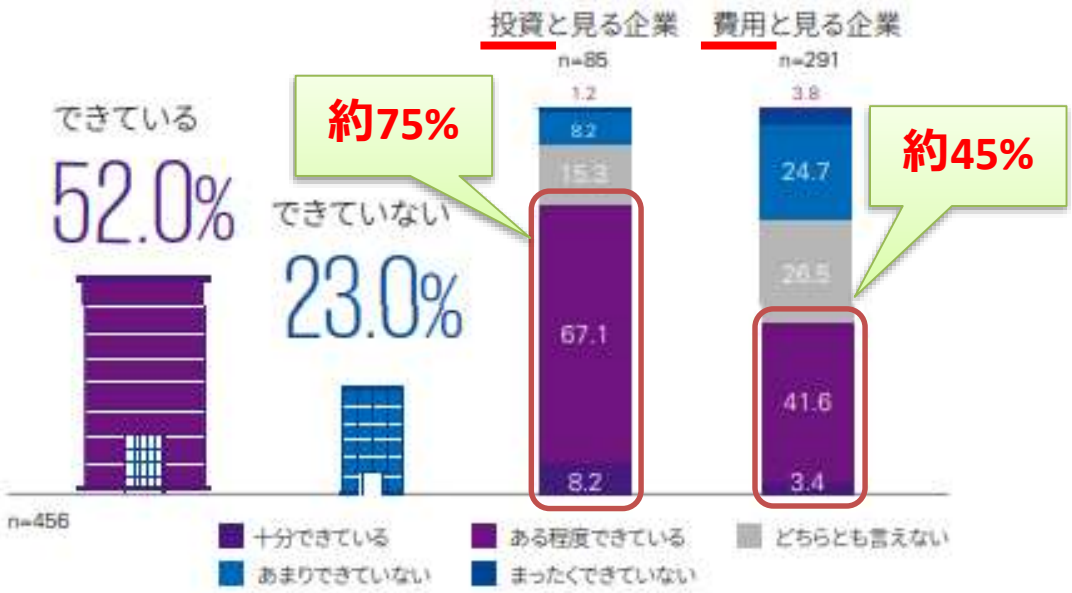
- 経営層が積極的な関与をしていないため、セキュリティ担当者が会社から評価されにくい
- 企業のセキュリティ担当者はモチベーションが上がらない

➡ セキュリティ人材を育成する上でも経営層が積極的に関与し、会社から評価される体制が必要

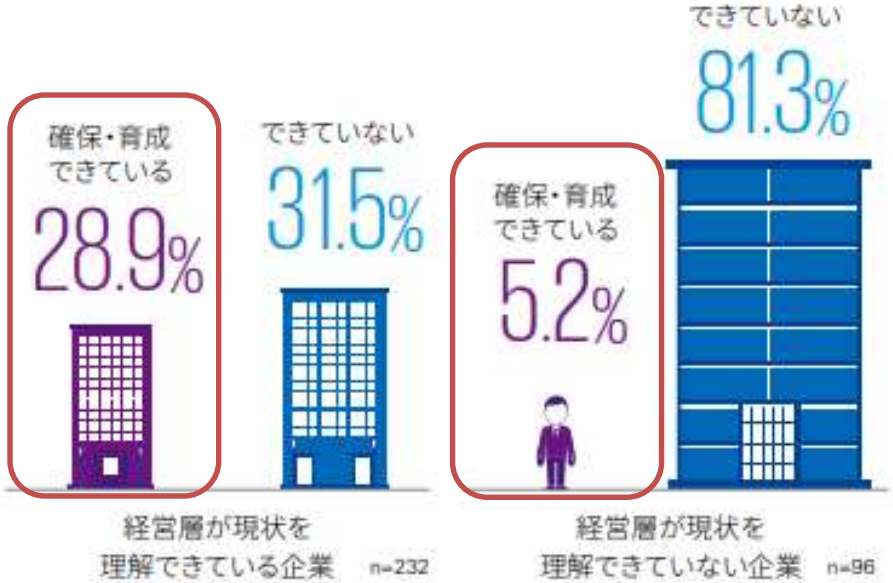
経営層の意識に見るリソースの確保状況

- 経営層がセキュリティに対して積極的に関与している企業は予算、人材をともに確保している割合が高い。

必要なセキュリティ予算の確保状況



必要な人材の確保・育成の状況



出典：サイバーセキュリティサーベイ2017（KPMGコンサルティング）

経営層の意識の現状に関するまとめ

- 日本は欧米と比べてセキュリティに対する経営層の関与が低い。

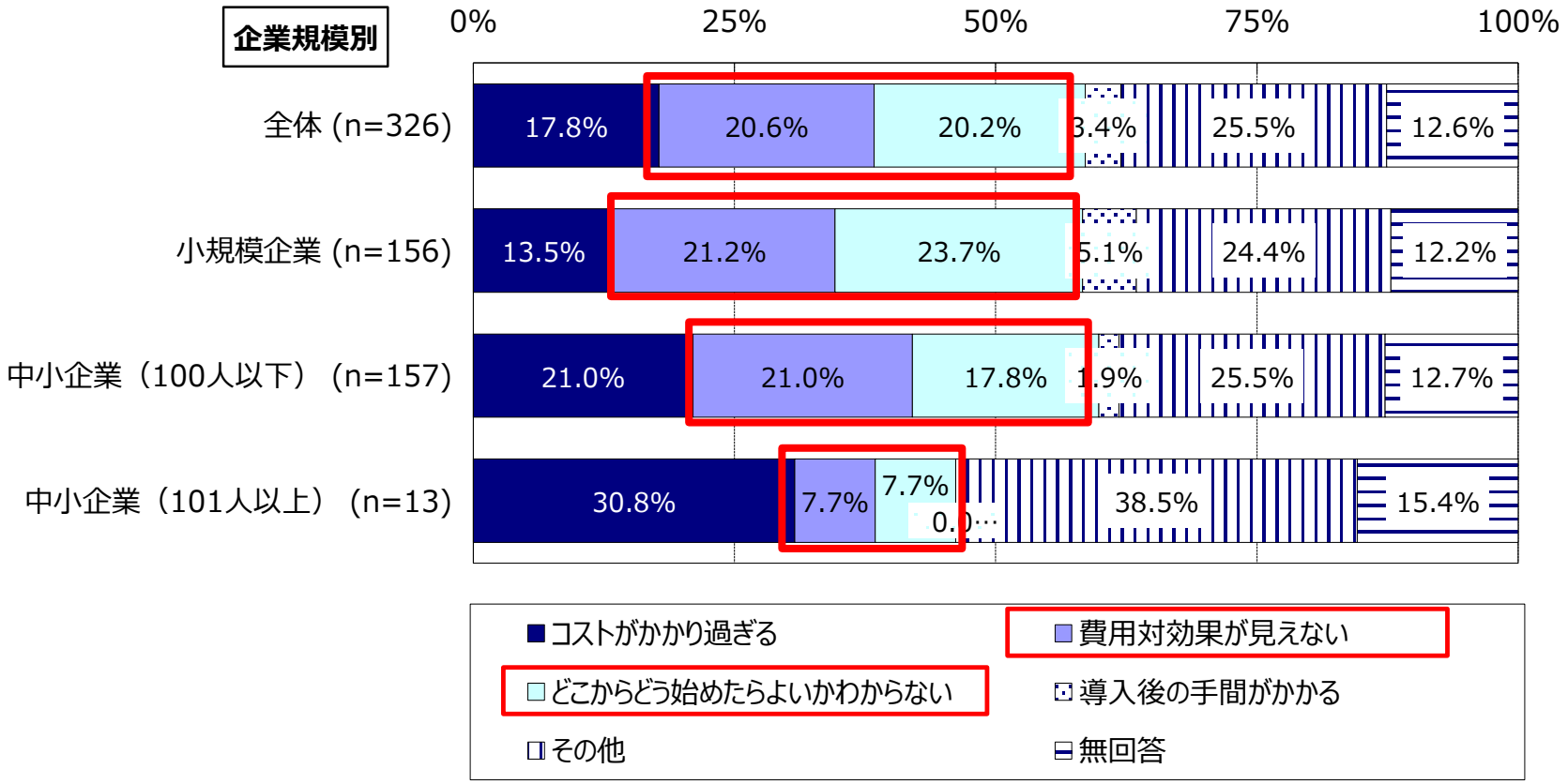
- 経営層のセキュリティに対する意識が高いほどＩＴ戦略を重視しており、成長にも関係している可能性がある。

グローバルに競争していくためにも、経営戦略にセキュリティを積極的に位置づけて取組を進めることが求められる。

（参考）中小企業におけるリソースの確保状況

- 費用対効果の測定ができない、何を実施すればよいのかを判断できないことから、セキュリティに関するリソースの確保に消極的。

Q5-4　情報セキュリティ対策に関する投資が含まれていない理由は何ですか。（○は1つ）
※回答者：Q5-2で「2.含まれていない」と回答



出典：2016年度中小企業における情報セキュリティ対策の実態調査（IPA）

（１）経営者の意識の現状

（２）サイバーセキュリティ経営ガイドライン

（３）経営者の意識改革に向けた対策案

サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
平成28年12月8日改訂（Ver.1.1）
平成29年11月16日改訂（Ver2.0）

- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドラインを公表

１．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

２．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築

（１）組織全体での対策方針の策定
（２）方針を実装するための体制の構築
（３）予算・人材等のリソース確保

リスクの特定と対策の実装

（４）リスクを洗い出し、計画の策定
（５）リスクへの対応
（６）PDCAの実施

インシデントに備えた体制構築

（７）緊急対応体制の構築
（８）復旧体制の構築

サプライチェーンセキュリティ

（９）サプライチェーンセキュリティの確保

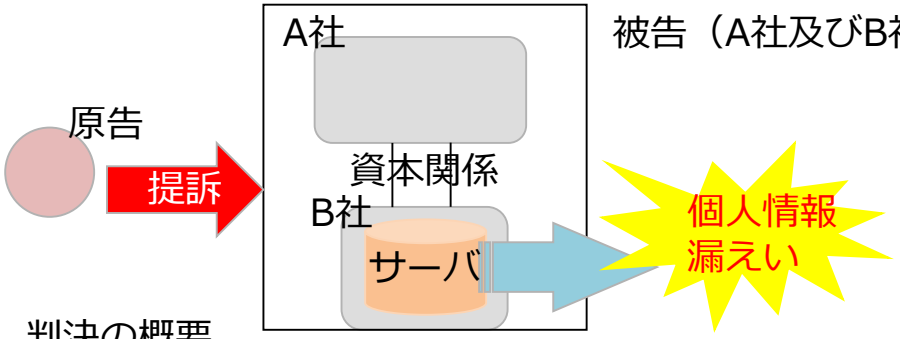
関係者とのコミュニケーション

（10）情報共有活動への参加

（参考）サイバー攻撃等により発生した情報漏えいに対する訴訟事件

- サイバー攻撃やアクセス権限の不備により個人情報が漏えいした場合、被害者や委託企業から損害賠償を求める訴えがされる可能性があり、現実に判決も出ている。

被害者から提訴された事案
大阪高裁平成18年(ネ)1704号
平成19年6月21日判決

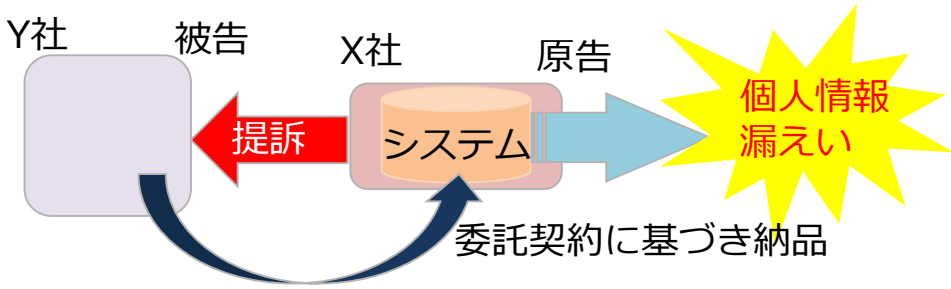


判決の概要
- 被告が管理するサーバに職員が不正にアクセスを行い原告の個人情報が漏えい。
- 個人情報の漏えいにより被告の受けた精神的苦痛に対して、1人あたり6,000円の損害賠償責任が認められた。

ポイント
- 被害者1人あたり500円の金券を交付していたが、それでは不十分として合計で6,000円の慰謝料を認めた。
- 個人情報について直接管理を行っていた子会社だけでなく、親会社についても管理責任を認めて損害賠償責任を認めた。

（出典）裁判所判例（大阪高裁平成18年（ネ）１７０４号）
http://www.courts.go.jp/app/files/hanrei_jp/228/033228_hanrei.pdf

委託元企業から提訴された事案
東京地裁平成23年(ワ)32060号
平成26年1月23日判決



判決の概要
- 被告が原告の委託を受けて納品した商品受注システムが攻撃を受け、顧客のクレッジトカード情報が漏えい。
- 被告に対して、委託契約の債務不履行に基く損害賠償（約2,200万円）が認められた。

ポイント
- 契約締結時に、経済産業省やIPAから脆弱性に対する注意喚起情報が示されており、被告は対策を行う義務を負っていたが対応しなかった（重過失）。
- 原告も被告からシステム改修提案を受けていたにも関わらず放置した（3割の過失相殺）。

（出典）東京地方裁判所判決／平成23年（ワ）第３２０６０号
http://www.softic.or.jp/semi/2014/5_141113/op.pdf

（参考）経営者が認識すべき３原則（サイバーセキュリティ経営の３原則）

① 経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、**リーダーシップによって対策を進める**ことが必要。

② 自社は勿論のこと、**系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策**が必要

③ **平時及び緊急時のいずれにおいても**、サイバーセキュリティリスクや対策、対応に係る情報の開示など、**関係者との適切なコミュニケーション**が必要

（参考）経営者がCISO等に指示をすべき１０の重要事項 －全体像－

経営者

【３原則】
１．経営者のリーダーシップが重要
２．自社以外（ビジネスパートナー等）にも配慮
３．平時からのコミュニケーション・情報共有

ACT

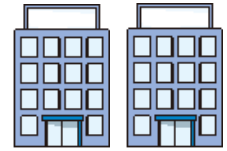
指示

報告

①サイバーセキュリティ対応方針策定

PLAN

内外に宣言・開示



ステークホルダー
（株主、顧客、取引先等）

②リスク管理体制の構築

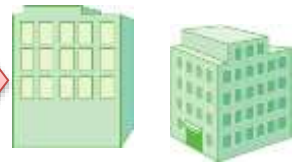
サイバーセキュリティリスク管理体制

◆経営リスク委員会等
他の体制と整合
（ex.内部統制、災害対策）

CISO等の担当幹部

③資源(予算、人材等)の確保

⑨サプライチェーンセキュリティ対策



ビジネスパートナー

DO

セキュリティ担当、CSIRT等

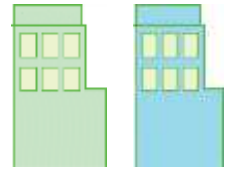
④リスクの把握と対応計画策定

⑤保護対策(防御・検知・分析)の実施

⑦緊急対応体制の整備

⑧復旧体制の整備

⑩情報共有活動への参加



情報共有団体・コミュニティ

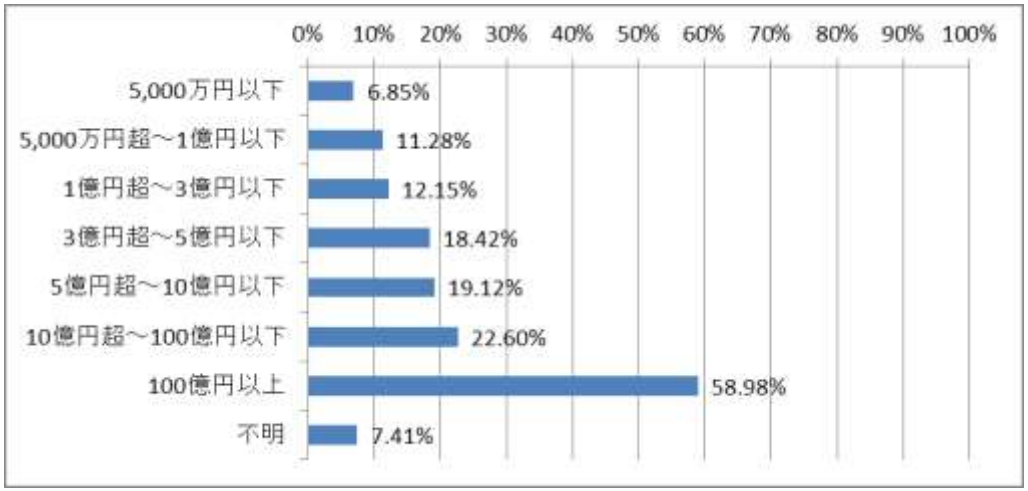
CHECK

⑥PDCAの実施

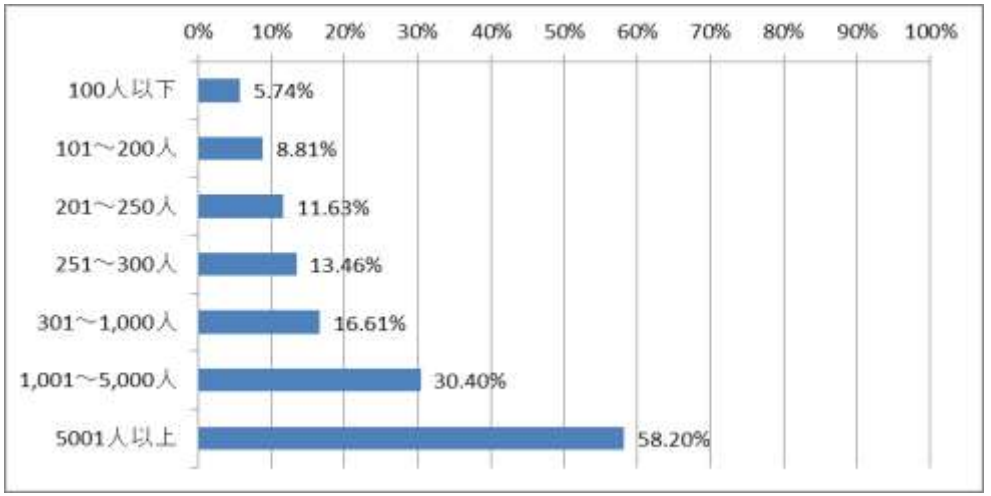
企業におけるサイバーセキュリティ経営ガイドラインの活用状況

- 策定後1年の状況によると、企業規模が大きくなるにつれて経営ガイドラインの実施率が高くなっている。
- 2016度には約55%の企業がガイドラインを参照しており、認知度は広まってきている。

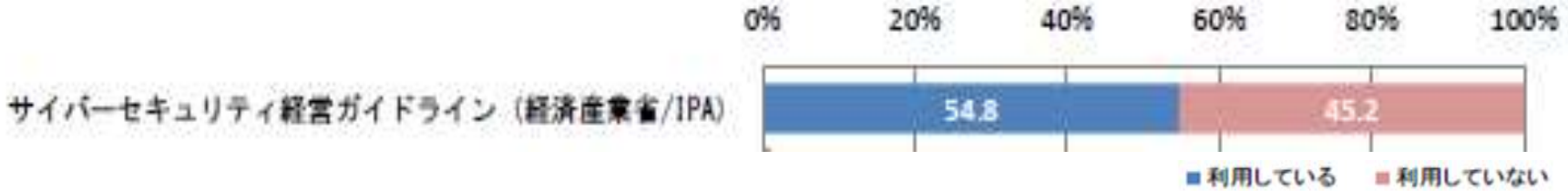
経営ガイドラインの参照状況（資本金別）（*1）



経営ガイドラインの参照状況（従業員数別）（*1）



経営ガイドラインの参照状況（2016年度）（*2）

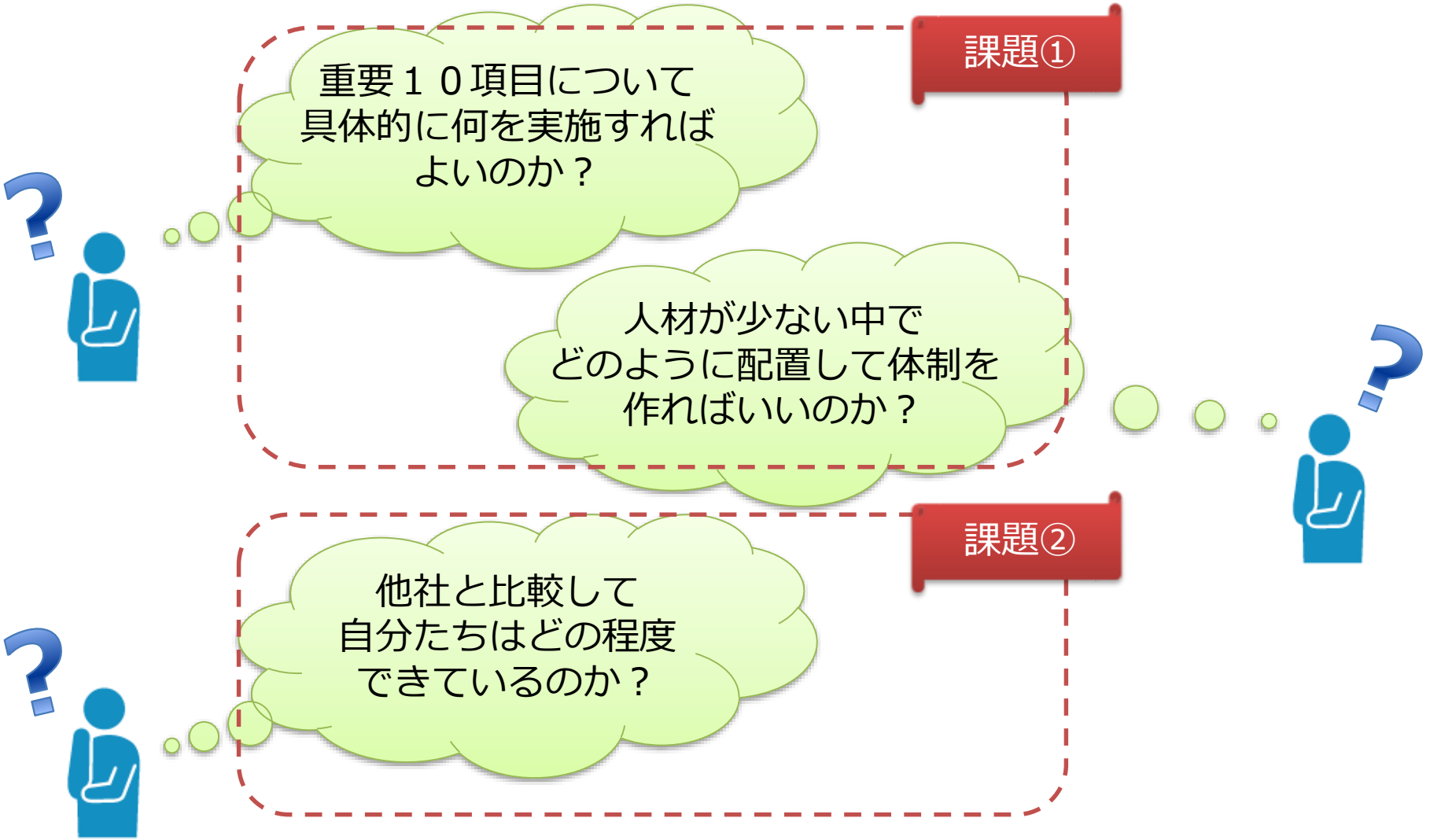


(*1)平成28年度我が国におけるデータ駆動型社会に係る基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書（経済産業省）のデータを元に作成　http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H28_report.pdf

(*2)出典：企業のCISOやCSIRTに関する実態調査2017(IPA)

サイバーセキュリティ経営ガイドラインの定着における課題

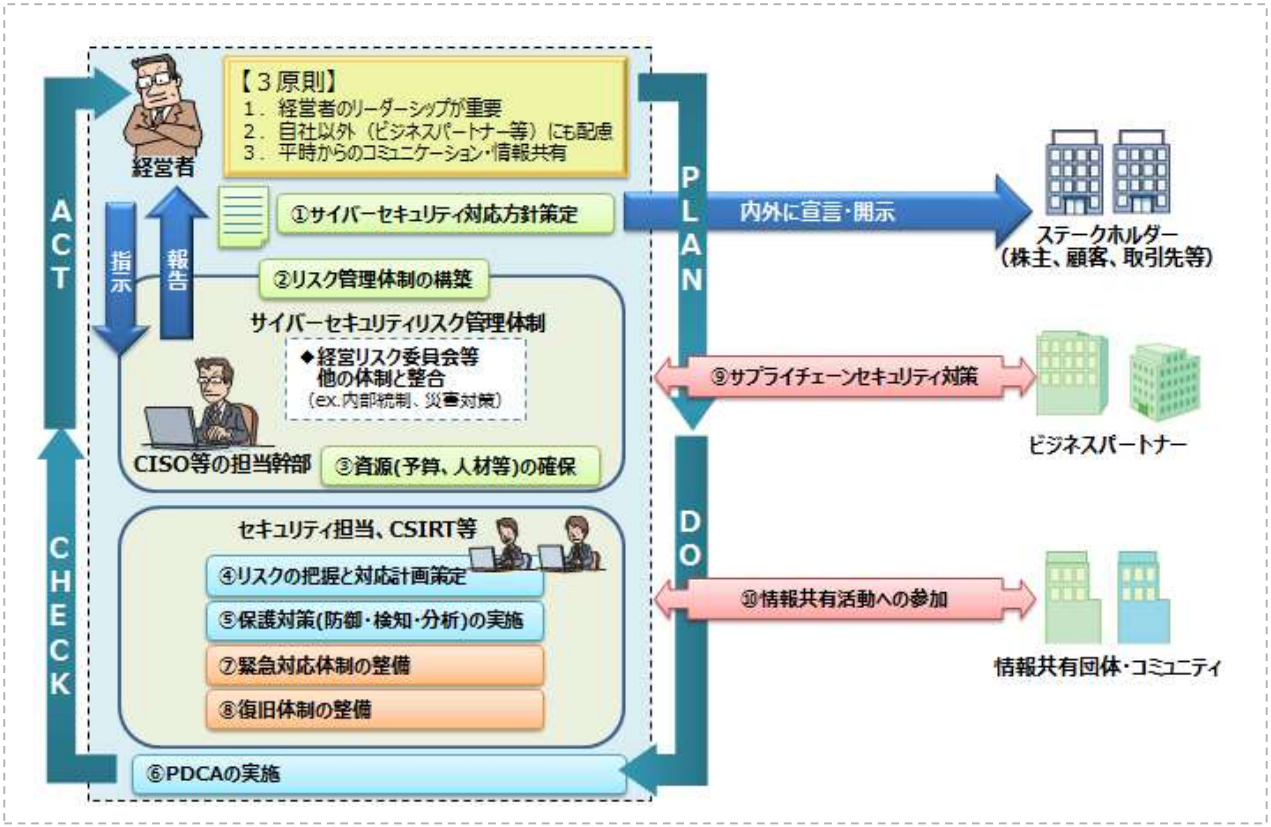
- サイバーセキュリティ経営ガイドラインの内容について認識をしている企業は増加しているものの、対策の実行へ結びつける上で課題を感じている企業も多い。



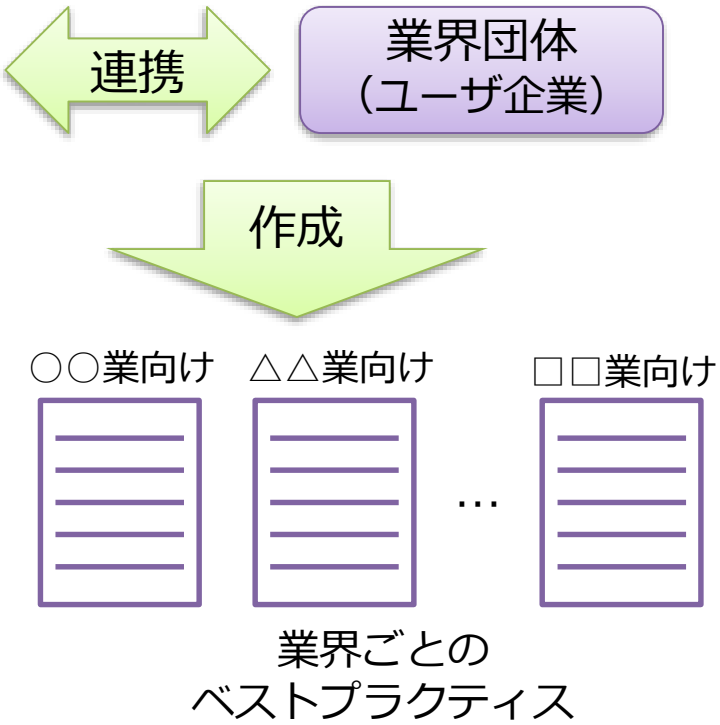
（１）経営者の意識の現状
（２）サイバーセキュリティ経営ガイドライン
（３）経営者の意識改革に向けた対策案

（課題①への対策案）ベストプラクティスの作成

- 『サイバーセキュリティ経営ガイドライン』の実践的な定着を図るために、業界、規模毎のベストプラクティスを作成。
- **組織が取り組んでいる具体的な対策事例**や**サイバー攻撃に関する情報共有活動事例**等を示すことで、組織の対策強化を期待。

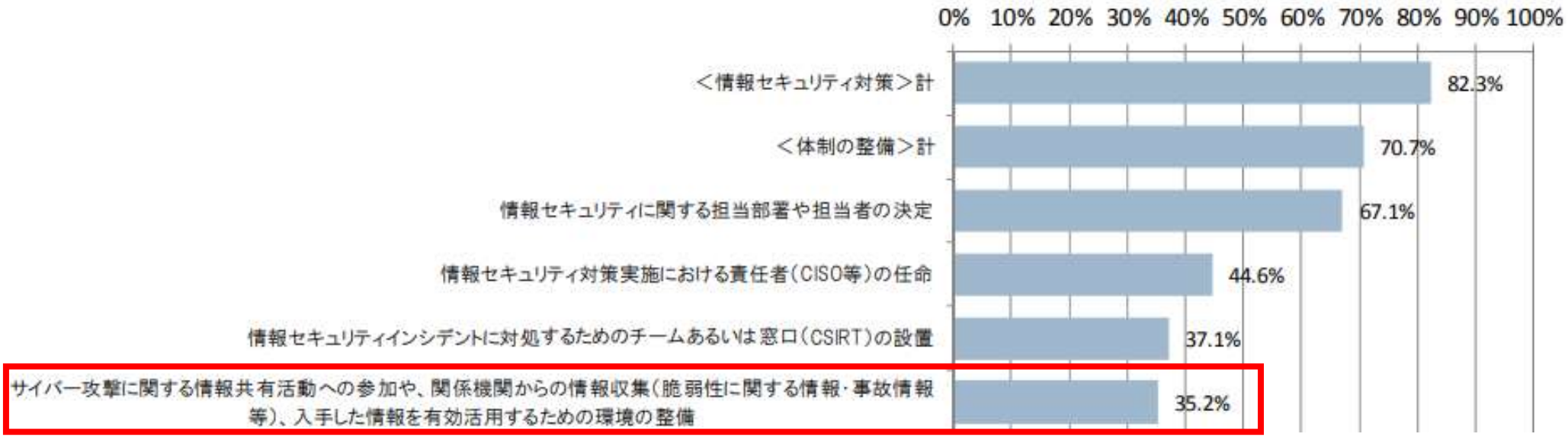


サイバーセキュリティ経営ガイドライン



（参考）情報共有活動の取組状況

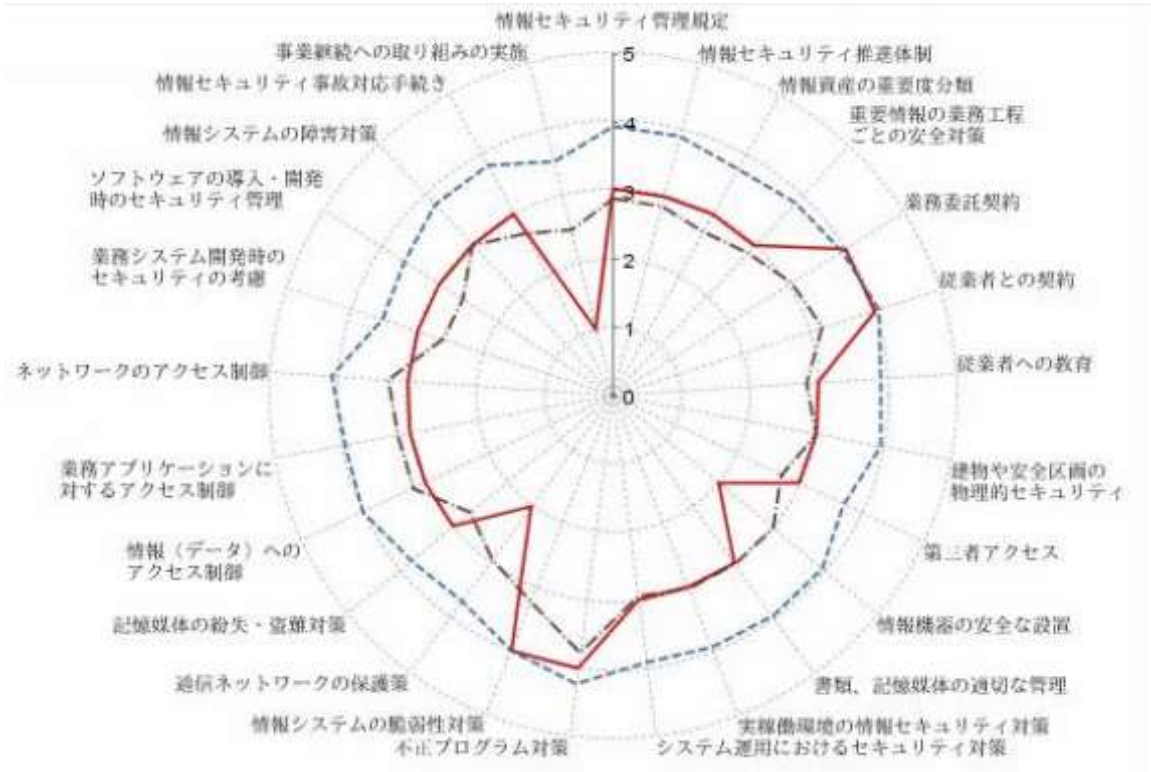
- サイバー攻撃の巧妙化に伴い、個社だけでサイバー攻撃に対抗するのは困難。
- 他社のサイバー攻撃に関する情報を収集するのみでなく、自社へのサイバー攻撃に関する情報も提供するといった**情報共有活動を積極的に行うことによって、社会全体としてサイバー攻撃に対抗することが重要**。
- 一方で、情報共有活動を実施しているのは約35%程度にとどまる。



(*)平成28年度我が国におけるデータ駆動型社会に係る基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書（経済産業省）のデータを元に作成
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H28_report.pdf

（課題②への対策案）セキュリティ対策の可視化ツールの作成

- サイバーセキュリティ経営ガイドラインの項目をベースとして、可視化ツールを作成。
- 業界ごとに平均値を出すことによって、企業がどこまで対策を実施するかの目安として活用できることを期待。



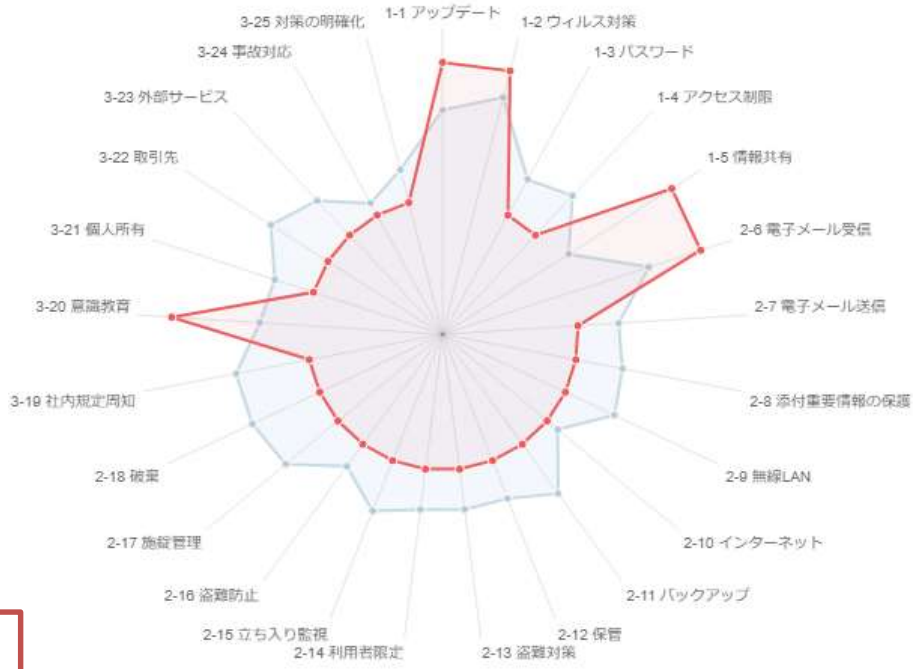
（参考）情報セキュリティ対策ベンチマーク（IPA）

（参考）（中小企業向け）5分でできる！自社診断

- 中小企業向けにはIPAが中小企業の情報セキュリティ対策ガイドラインを公開。
- 当該ガイドラインの付録「5分でできる！自社診断」（25のチェック項目）に基づき対策状況の可視化、及び業界平均との比較等が可能。

5分でできる！自社診断

基本的対策（5問）
（パスワード設定、ウイルス対策ソフトの導入等）
従業員としての対策（13問）
（無線LAN設定、不審メール対策等）
組織としての対策（7問）
（BYOD対策、クラウド利用対策等）



情報セキュリティ対策支援サイト（IPA）

企業経営におけるサイバーセキュリティの位置付け強化

- 企業の経営にとって、サイバーセキュリティは重要なリスク管理の一部であり、グループ内企業におけるセキュリティ確保も含め、適切な体制整備が必要。
- また、中小企業をはじめとする取引先も含め、サプライチェーン全体でセキュリティ意識を向上していくことも重要。
- コーポレート・ガバナンス・システムに関する議論において、「守り」のリスク管理の一環としてサイバーセキュリティ対策を位置付けることについて検討が必要ではないか。

＜参考＞「コーポレート・ガバナンス・システムに関する実務指針（CGSガイドライン）」（平成29年3月）の内容

1. 形骸化した取締役会の経営機能・監督機能の強化

- **中長期の経営戦略**、**経営トップの後継者計画**の審議・策定
- 個別業務の執行決定は対象を絞り込み、CEO以下の**執行部門に権限委譲**

2. 社外取締役は数合わせでなく、経営経験等の特性を重視

- 人選理由を後付けで考えるのではなく、最初に必要な社外取締役の**資質、役割を決定した上で人選**
- 社外取締役のうち**少なくとも１名は企業経営経験者**を選任（逆に、経営経験者は他社の社外取を積極的に引受け）

3. 役員人事プロセスの客観性向上とシステム化

- CEO・経営陣の選解任や評価、報酬に関する**基準及びプロセスを明確化**
- 基準作成やプロセス管理のため、**社外者中心の指名・報酬委員会を設置・活用**（過半数が社外、半々なら委員長が社外）

4. CEOのリーダーシップ強化のための環境整備

- 取締役会機能強化により、CEOから各部門（事業部、海外・地域拠点等）への**トップダウンをやりやすく**
- **退任CEOが相談役・顧問**に就任する際の**役割・処遇の明確化**
- 退任CEOの就任慣行に係る積極的な**情報開示**

グループガバナンスに関する論点（案）（１）

第２期CGS研究会
第１回事務局資料より抜粋
＊赤字吹き出し・下線は本WG事務局により追記

「グループガバナンス」とは

○連結子会社を含む企業グループ経営において、グループ全体としての企業価値向上のための設計・管理等の仕組み。
○「守り」（内部統制、リスク管理、コンプライアンス等）と「攻め」（企業理念・経営ビジョン、業績目標管理、インセンティブ報酬等）は両輪であり、「守り」があっての「攻め」。
○経営資源の「選択と集中」を図るため、事業ポートフォリオの機動的な組換え（最適化）もその一環。

「守り」の「リスク管理」の一環としてサイバーセキュリティ対策を明確に位置付けることが必要ではないか

主な論点（案）

○グループ全体の企業価値向上のために、「攻め」と「守り」（※）の両面で、どのようなグループ設計及び管理（事業ポートフォリオマネジメントを含む）の在り方が考えられるか。
（※）法的リスクにとどまらず、ブランド価値やレピュテーションリスクを含む。

○その際、権限移譲（遠心力）と統合管理（求心力）をどうバランスさせ、子会社の自律性とグループとしての全体最適の追求という２つの要請にどう対応するか。
- 権限移譲（分権化）⇔ 一元的管理／子会社の経営責任（集権化）
- 意思決定の迅速性 ⇔ グループ管理の実効性
- 多様性・自律性・創意工夫 ⇔ スケールメリット・コスト効率性

○業種・業態や市場環境等の多様性を踏まえ、複数のパターン化が考えられるか。

次ページにつづく

グループガバナンスに関する論点（案）（２）

第２期CGS研究会
第１回事務局資料より抜粋
＊赤字吹き出し・下線は本WG事務局により追記

前ページからつづく

（１）グループの設計(※)の考え方について

（※）親会社の形態（事業会社／ホールディングス）や、グループ構成（コーポレート部門／事業部門、カンパニー制、上場子会社／完全子会社等）について

– 別法人とする企業経営上の意義
– 親と子の機関設計とコーポレートガバナンスの仕組みとその関係性の在り方（指名・報酬委員会の設置等）
– 事業ポートフォリオや組織構造の柔軟性の確保

（２）グループ管理(※)の具体的実務の在り方について

（※）「企業集団としての内部統制システムの構築」を含む。

– 各種規程の策定と子会社への適用関係と遵守の担保手段（子会社統治の根拠となるルール、共通化と個別化等）
– 事前承認・報告の基準設定と運用（子会社の規模・属性・業務内容等に応じた取扱い区分等）
– 子会社におけるコンプライアンスの確保（平時における不正・違法行為の予防・把握と、有事の際の対応）
– 人事（役員・従業員）・報酬設計（KPI、インセンティブ報酬等）の在り方（親会社としての管理と子会社としてのモチベーション）
– 上場子会社の扱いについて（利益相反問題への対応等）
– 海外子会社について（M&A後のPMIの在り方、各国法制への対応等）

「グループ管理」の一環として
サイバーセキュリティ対策を明確に
位置付けることが必要ではないか

（３）事業ポートフォリオ・マネジメントの在り方について

– 事業ポートフォリオに関する方針（コア分野の考え方等）
– 見直し基準の在り方（収益性・成長性等に関する指標の立て方、基準を置くことの意義等）
– 見直しプロセスの在り方（子会社ごとの評価プロセス、取締役会での議論、子会社の取締役会の役割等）

ベストプラクティスの収集・整理・分析（共通要素の抽出等）を通じて、企業グループごとの多様性に配慮しつつ、グループガバナンスの望ましい在り方に関する実務指針のとりまとめを目指す。

企業経営のためのサイバーセキュリティの考え方（１）

参考：(NISC)セキュリティマインドを持った企業経営ＷＧ

企業が自発的に行うサイバーセキュリティの取組が促進されるよう、企業経営のためのサイバーセキュリティに係る基本的考え方とともに、経営層に期待される“認識”や経営戦略を企画する人材層に向けた実装のためのツールを示す。

※普及啓発・人材育成専門調査会の下に設置された、「セキュリティマインドを持った企業経営ワーキンググループ」（主査：林紘一郎 情報セキュリティ大学院大学教授）を通じ、検討を実施。

基本方針　　ーサイバーセキュリティは、より積極的な経営への「投資」へー

グローバルな競争環境の変化

- ITの発展によるビジネスの変革が、消費者向けのビジネスから企業間取引へと拡大
- サイバー空間と実空間の融合がさらに進み、チャンスもリスクも一層増大

サイバーセキュリティをやむを得ない「費用」でなく、積極的な経営への「投資」と位置づけ、企業としての「挑戦」と、それに付随する「責任」として取り組むことが期待される

I.基本的考え方

二つの基本的認識

＜①挑戦＞

サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。

＜②責任＞

全てがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる。

三つの留意事項

＜①情報発信による社会的評価の向上＞

- 「セキュリティ品質」を高め、品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。
- そのような取組に係る姿勢や方針を情報発信することが重要。

＜②リスクの一項目としてのサイバーセキュリティ＞

- 提供する機能やサービスを全うする（機能保証）という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。
- 経営層のリーダーシップが必要。

＜③サプライチェーン全体でのサイバーセキュリティの確保＞

- サプライチェーンの一部の対策が不十分な場合でも、自社の重要情報が流出するおそれあり。
- 一企業のみでの対策には限界があるため、関係者間での情報共有活動への参加等が必要。

企業経営のためのサイバーセキュリティの考え方（２）

参考：(NISC)セキュリティマインドを持った企業経営ＷＧ

II.企業の視点別の取組

企業が投資すべき対象や経営リスクは様々であり、各企業の人的・金銭的資源にも限りがあることから、ITの利活用やサイバーセキュリティへの取組において、各企業の事業規模のみならず、その認識の違いなどを踏まえて取り組んでいく必要がある。

ITの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に競争力強化に活用しようとしている企業

（積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）

【経営者に期待される認識】
- 積極的なITの利活用を推進する中で、製品やサービスの「セキュリティ品質」を一層高め、自社のブランド価値の向上につなげるべく、システムの基盤におけるセキュリティの向上、情報・データの保護、製品等の安全品質向上に取り組む。
- 様々な関係者との協働が重要であるため、情報提供に主体的に取り組む。
- 決して現存する標準や取り組みなどに満足することなく、実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、変革していく存在となることが期待される。

【実装に向けたツール】
- IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等）
- 自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信

IT・セキュリティをビジネスの基盤として捉えている企業

（IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置づけていない企業）

【経営者に期待される認識】
- 経営者のリーダーシップによって、社会的責任としてのサイバーセキュリティ対策に取り組む。
- サプライチェーンやビジネスパートナー、委託先を含めた対策を行う。
- 平時・緊急時のいずれにおいても、情報開示などの適切なコミュニケーションを行う。

【実装に向けたツール】
- サイバーセキュリティ経営ガイドライン
- 企業等がセキュリティ対策に取り組む上での保険等のリスク管理手法の活用
- サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信

自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業

（主に中小企業等でセキュリティの専門組織を保持することが困難な企業）

【経営者に期待される認識】
- サプライチェーンを通じて中小企業等の役割はますます重要となる中、消費者や取引先との信頼関係醸成の観点から経営者自らサイバーセキュリティ対策に関心を持ち、取り組む。
- 外部の能力や知見を活用しつつ、効率的に進める方策を検討する。

【実装に向けたツール】
- 効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等）
- サイバーセキュリティに関する相談窓口やセミナー、地域の相談員等の活用

１．ＷＧ２（経営･人材･国際）の目的･ねらい

２．経営

３．人材

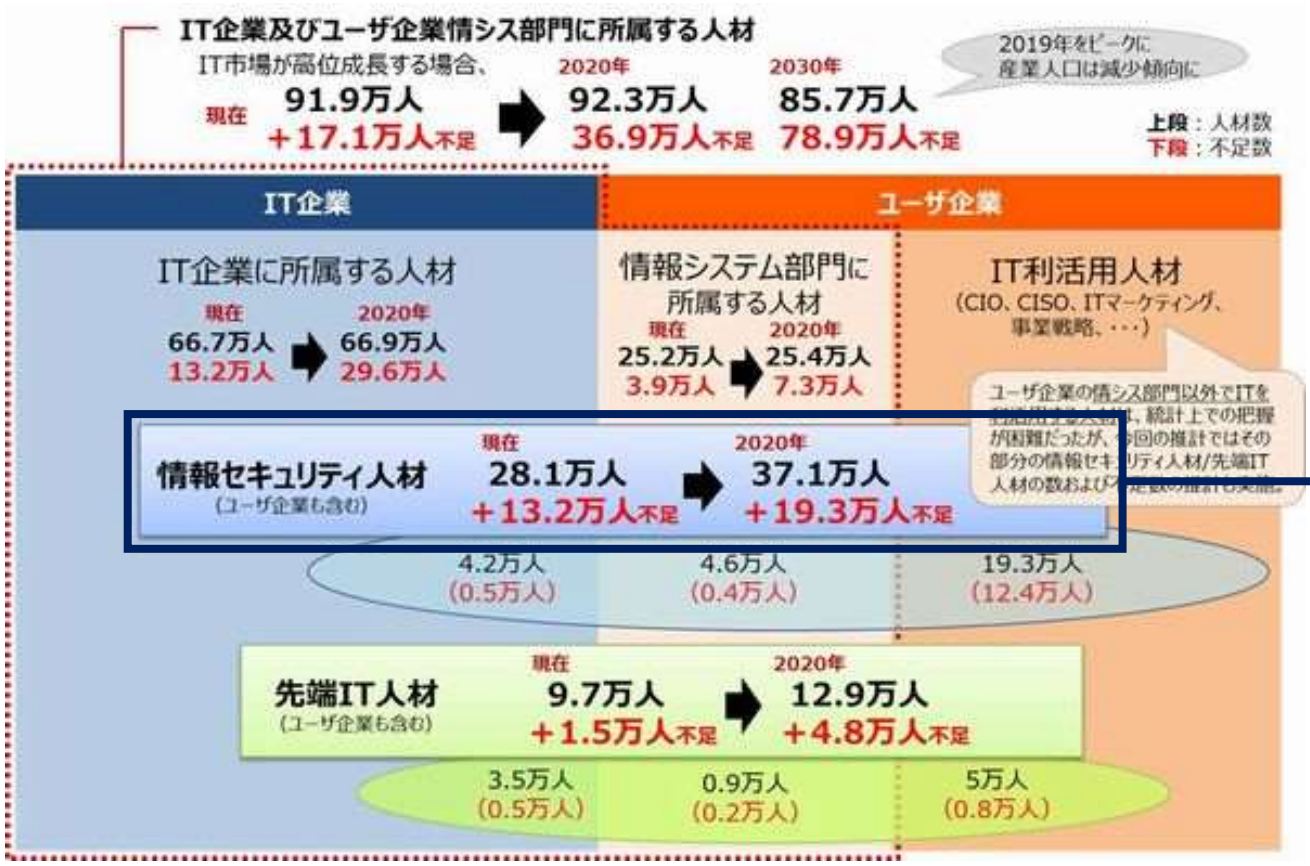
４．国際

（１）セキュリティ人材をめぐる状況
（２）セキュリティ人材育成政策の現状
（３）今後のセキュリティ人材育成政策の方向性

日本のサイバーセキュリティ人材の需要

- 情報セキュリティ人材は、現在13.2万人不足、特にユーザー企業で大きな不足感。

IT・データ人材の需給に関する推計



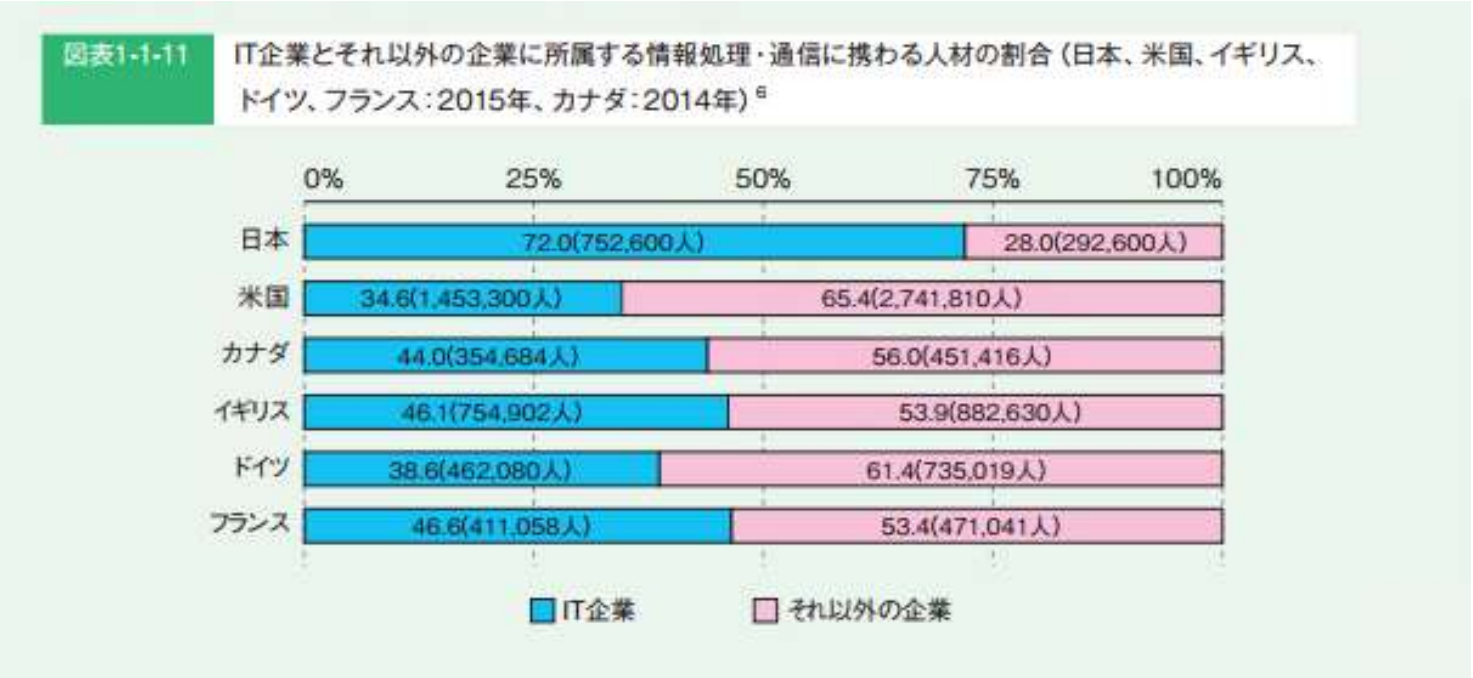
海外の知見も習得する高度な人材
全体の1～2割

セキュリティ人材
50万人超（37.1万人＋19.3万人）
（2020年時点）

（資料）経済産業省平成26年度補正先端課題に対応したベンチャー事業化支援等事業「IT人材の最新動向と将来推計に関する調査結果（報告書概要版）」より

IT人材の所属企業（IT企業／その他の企業）

- 日本では、IT人材の７０％超はIT企業に在籍しており、各国と比較すると、ベンダーとユーザーのバランスが大きく異なる。

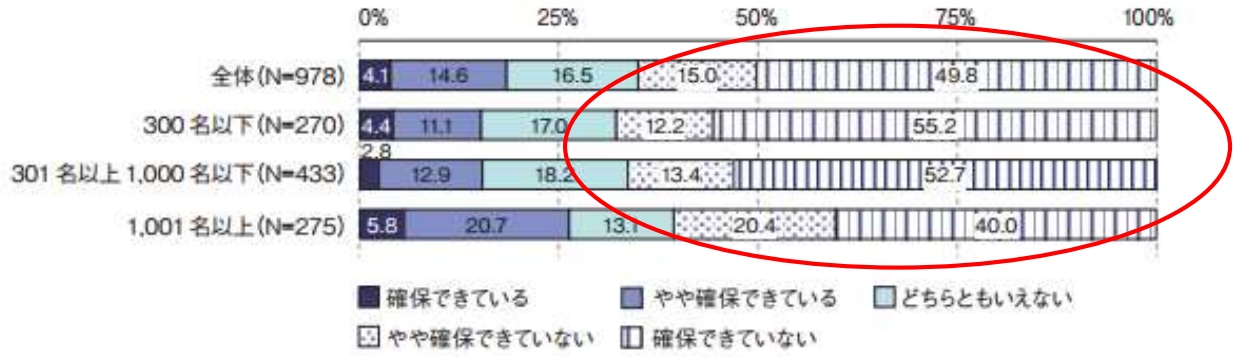


【出所】IT人材白書2017（IPA）

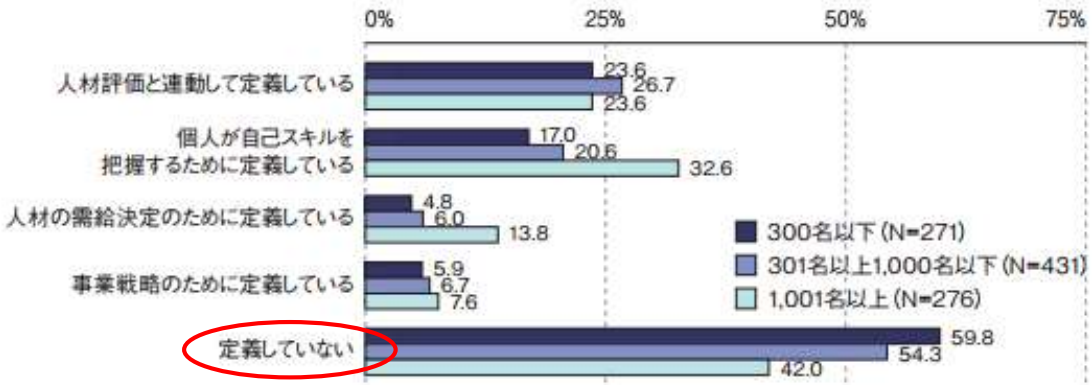
ユーザー企業におけるセキュリティ専門技術者の確保の状況

- ユーザー企業では、セキュリティ専門技術者を確保できていない。
- また、IT人材に求められるスキルの定義も進んでいない。

図表3-2-32　ユーザー企業の情報セキュリティ専門技術者の確保状況【従業員規模別】　無回答を除く



図表3-2-29　ユーザー企業のスキル定義の目的【従業員規模別】[11]　その他、無回答を除く

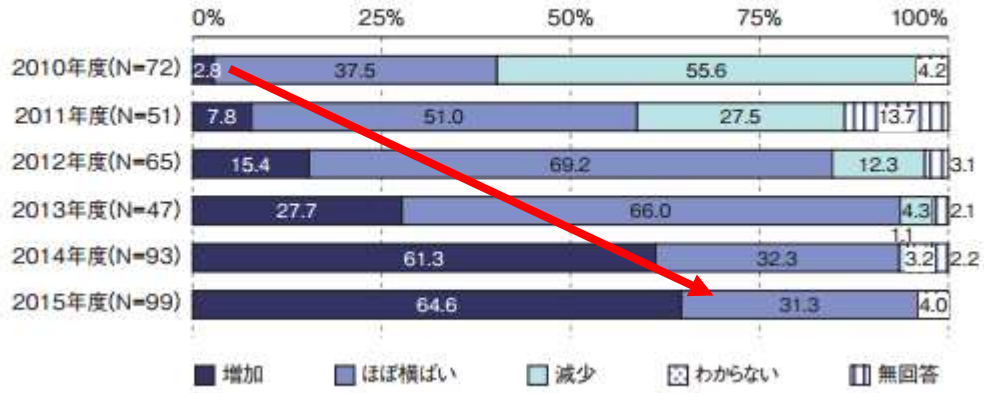


【出所】IT人材白書2017（IPA）

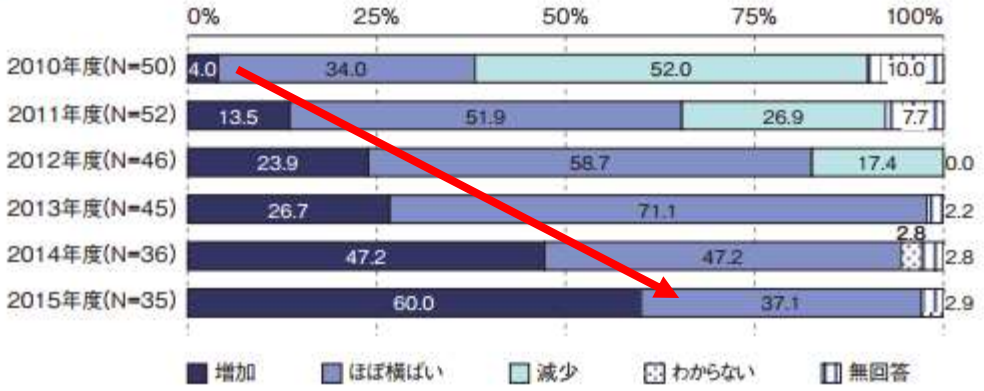
情報系学科の大学学部・高等専門学校卒業生に対する企業の需要

- ユーザー企業の情報系学科の大学学部・高等専門学校卒業生に対する企業の需要は大幅に拡大。

図表4-1-4 大学学部の卒業生に対する企業の需要の変化【2010年度~2015年度】



図表4-1-8 高等専門学校の卒業生に対する企業の需要の変化【2010年度~2015年度】

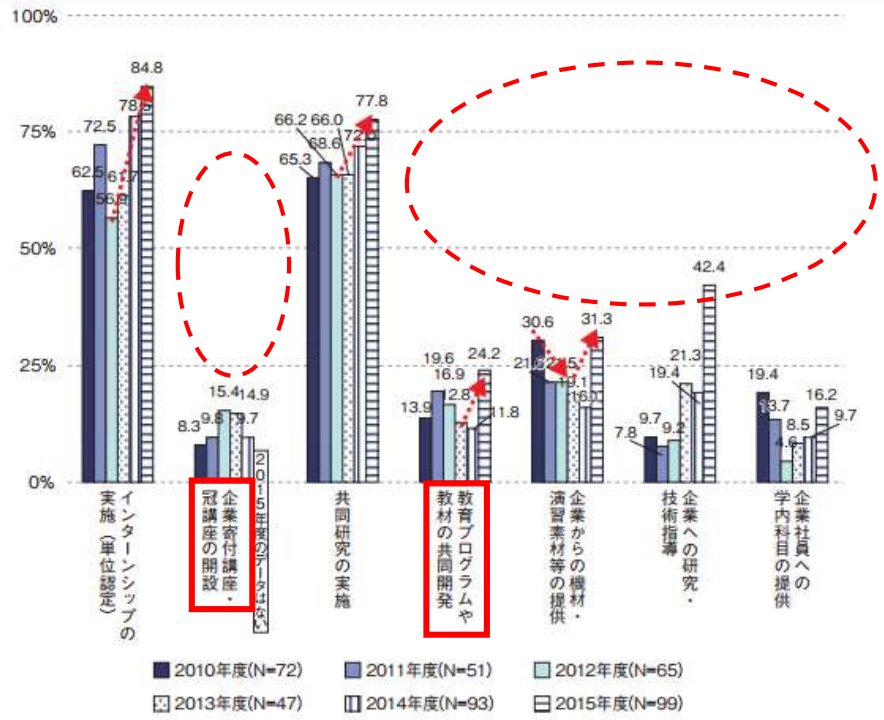


【出所】IT人材白書2017（IPA）

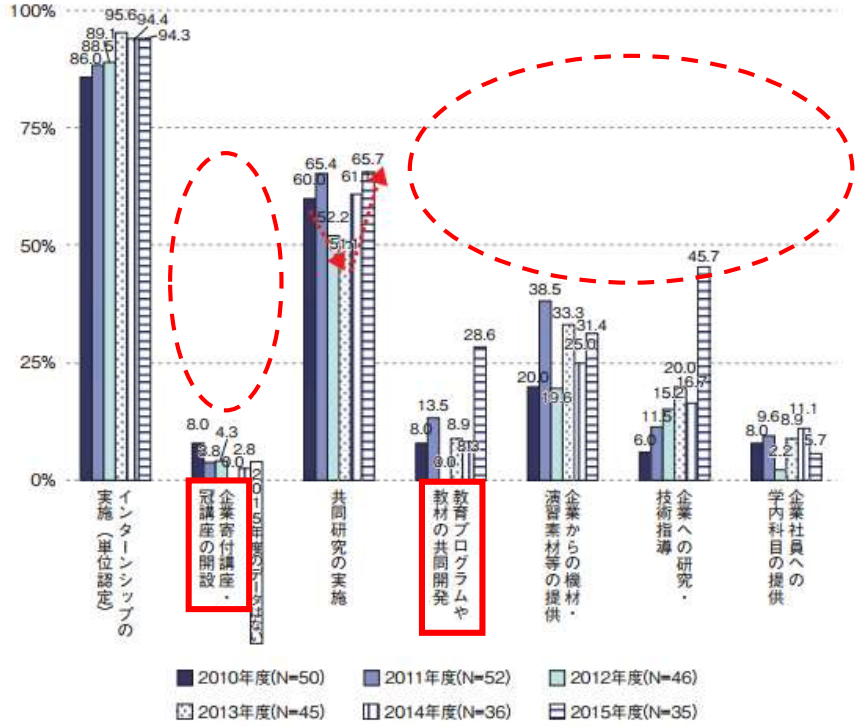
情報系学科の大学学部・高等専門学校における産学連携の取組

- 情報系学科の大学学部・高等専門学校における産学連携の取組は拡大傾向ではあるものの、拡大の余地あり。
- 大学の教育プログラムへの貢献など、教育に対する貢献も低調。

図表4-1-6 大学学部の産学連携で実施している取り組み【2010年度~2015年度】[4] 無回答を除く



図表4-1-10 高等専門学校の産学連携で実施している取り組み【2010年度~2015年度】[7] 無回答を除く

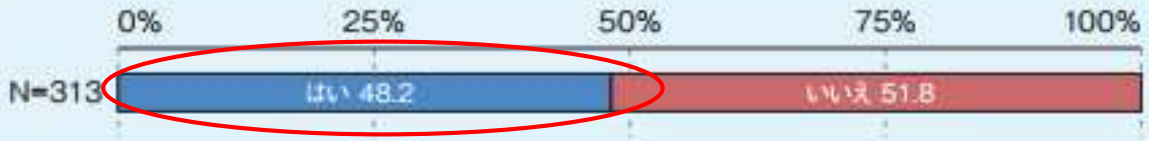


【出所】IT人材白書2017（IPA）

米国の組織における大学との連携・協業状況

- 米国においては、半数近い組織がサイバーセキュリティトレーニングプログラム開発のために大学との連携・協業を実施しており、大学との連携に積極的に関与。

図表2-2-31 米国の組織におけるサイバーセキュリティトレーニングプログラム開発のための大学との連携・協業状況



【出所】IT人材白書2017（IPA）

（１）セキュリティ人材をめぐる状況

（２）セキュリティ人材育成政策の現状

（３）今後のセキュリティ人材育成政策の方向性

サイバーセキュリティ人材育成の検討の方向性（案）

参考：(NISC)サイバーセキュリティ人材の育成に関する施策間連携ＷＧ

- IoT、ビッグデータ、AIの進展により「経済のサービス化」は不可避。これに伴い、企業におけるIT利活用も**CIT(コーポレートIT)**から**BIT(ビジネスIT)**へ主軸が移行。
- 企業においては、BITを前提としたビジネス戦略の推進及びリスクマネジメントの確保に当たり、サイバーセキュリティの重要性が増大。このような環境変化に対応したセキュリティ人材の育成・確保が必要。

経営層
（取締役会・経営企画部門）
・ビジネス戦略の企画・立案、事業投資判断
・リスクマネジメント

＜求められる役割＞
- ビジネス戦略及びリスクマネジメントの一要素として、サイバーセキュリティを位置づけ、企業経営に組み込む
- 情報システム部門のみならず、事業部門等に必要なセキュリティ人材を配置

＜問題・課題＞
- サイバーセキュリティの重要性に対する意識が希薄
- ITの問題をシステム部門任せにする傾向
- 中小企業においては、とりわけ人材確保が困難

戦略マネジメント機能（※）
（事業部門等の各業務部門）
・ビジネス等の企画・設計、運営、評価
※名称については、別途検討。

事業部門A　事業部門B　総務部門　経理部門　広報部門　・・・・
BIT　CIT

＜求められる役割＞
- 事業分野に関する能力・経験に加え、戦略マネジメント機能の遂行に必要となるセキュリティ知識・スキル、ITに係る基本的知識等を習得
- 事業に関するセキュリティリスクが事業利益・企業価値に与える影響を把握・分析し、経営層に適確に説明
- サプライチェーンを意識しつつ、セキュリティ要件を含めてシステム部門を指揮
- セキュリティ問題について他の部門とチームとして連携

＜問題・課題＞
- 戦略マネジメント機能の遂行に必要となるセキュリティ知識・スキル、ITに係る基本的知識等の習得
- 戦略マネジメント機能を担う人材の育成・確保に係るプロセスの確立

システム担当
・システム化の企画・開発　・ソフトウェアの要件定義

＜求められる役割＞
（システム担当）
- 各業務部門とコミュニケーションを取りつつ、システム化に係るセキュリティの要件定義を実施

（システム構築担当）
- セキュリティが確保されたプログラミングを実践
- ペネトレーションテスト、脆弱性検査、インシデント対応

＜問題・課題＞
- セキュリティ知識・スキルのみならず、それらを支えるITに係る基本的知識等の習得
- キャリアパスの明確化

システム構築・運用担当
（子会社・外部委託含む）
・プログラミング、システム構築　・システム運用テスト
・システム管理・運用

＜主な検討事項＞

企業経営WG
- ✓ 経営層の意識改革促進のための具体的方策の在り方
- ✓ リスクマネジメント確保のための組織体制の在り方
- ✓ 中小企業におけるセキュリティ確保の方策
- ✓ 産学官連携の在り方・具体的方策

等

施策間連携WG
- ✓ 各層別の人材像やキャリアパスの明確化
  - ・特に、各部門におけるセキュリティを含めた戦略マネジメント機能を担う人材
  - ・高度人材の定義、位置付けの整理
- ✓ セキュリティ人材育成の前提となる基本的知識の明確化及び各層別のカリキュラム（短期・中長期）策定
- ✓ 各層別のカリキュラムを意識した各省施策に関する全体像の整理、連携策の検討
- ✓ 教材R&Dの推進
- ✓ 産学官連携の在り方・具体的方策

等

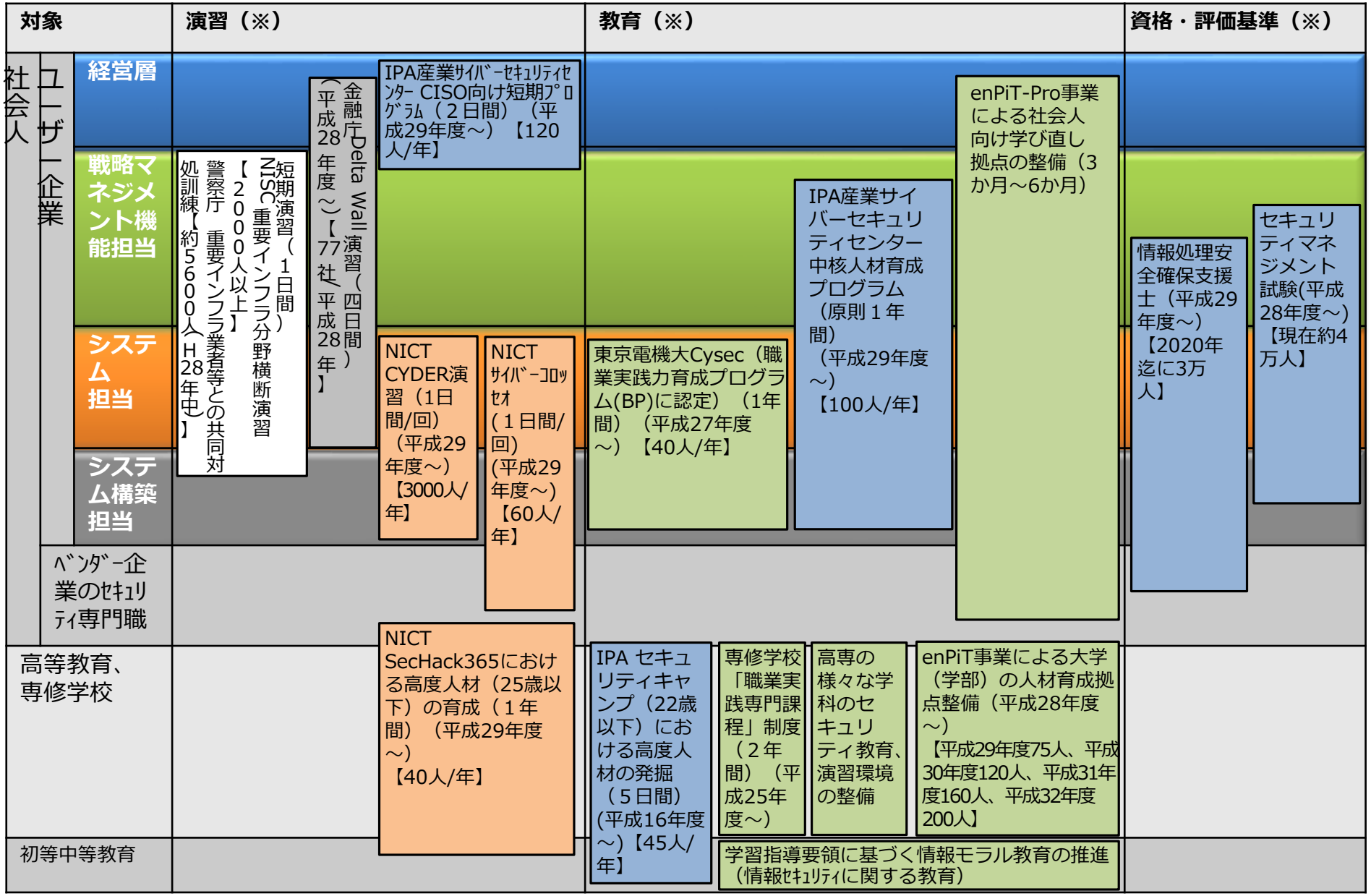
＜その他の検討事項＞
- サイバーセキュリティの目標人数・不足人数に関するデータ等の整理
- 諸外国の取組状況　等

次期「サイバーセキュリティ戦略」への反映

各省庁の人材育成施策に関する全体像（イメージ）

参考：(NISC)サイバーセキュリティ人材の育成に関する施策間連携ＷＧ

総務省　文科省　経産省　金融庁　その他

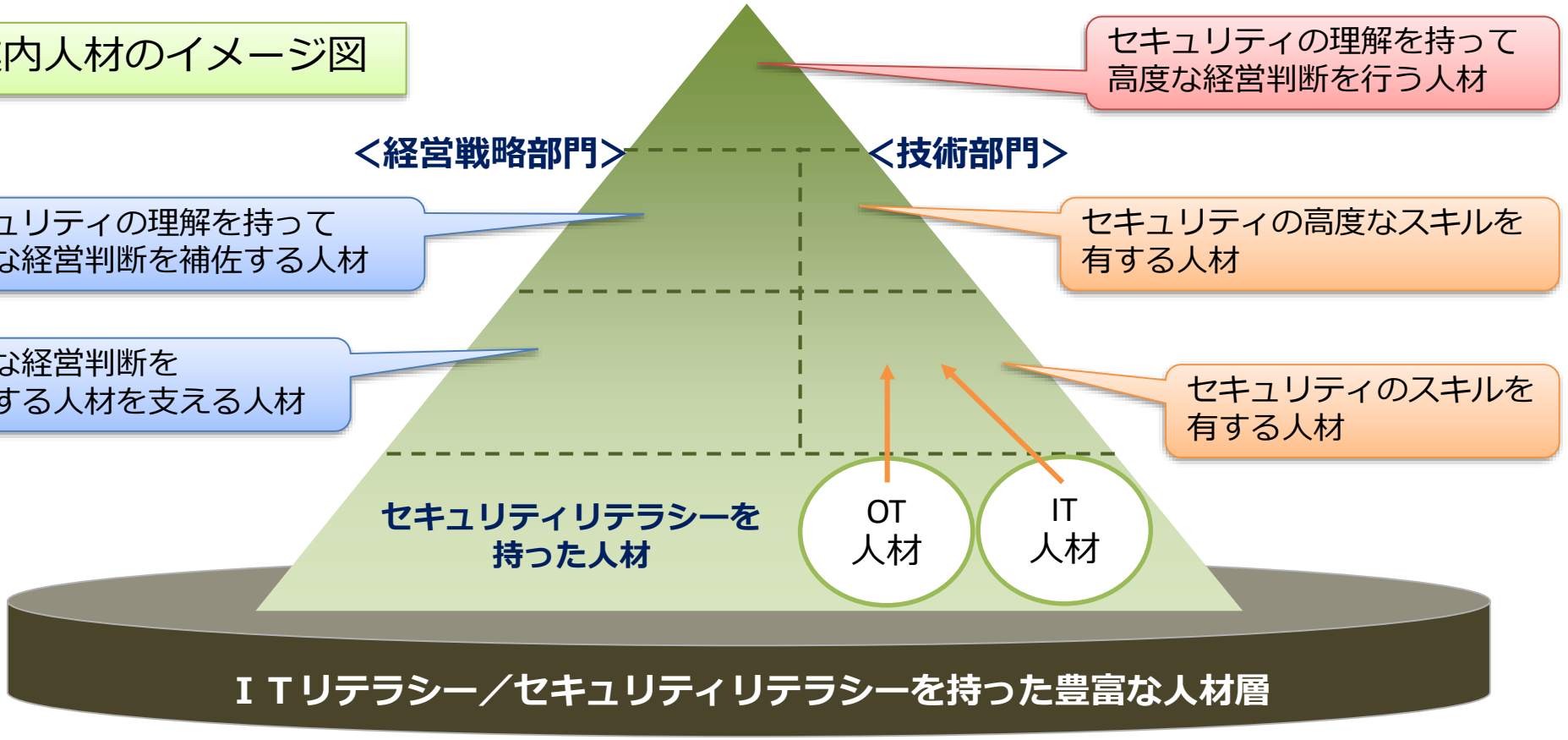


※演習、教育、資格・評価基準の分類については、サイバーセキュリティ人材育成総合強化方針（平成28年3月31日サイバーセキュリティ戦略本部決定）に基づくもの。各施策は、その中心となる内容に基づいて分類。

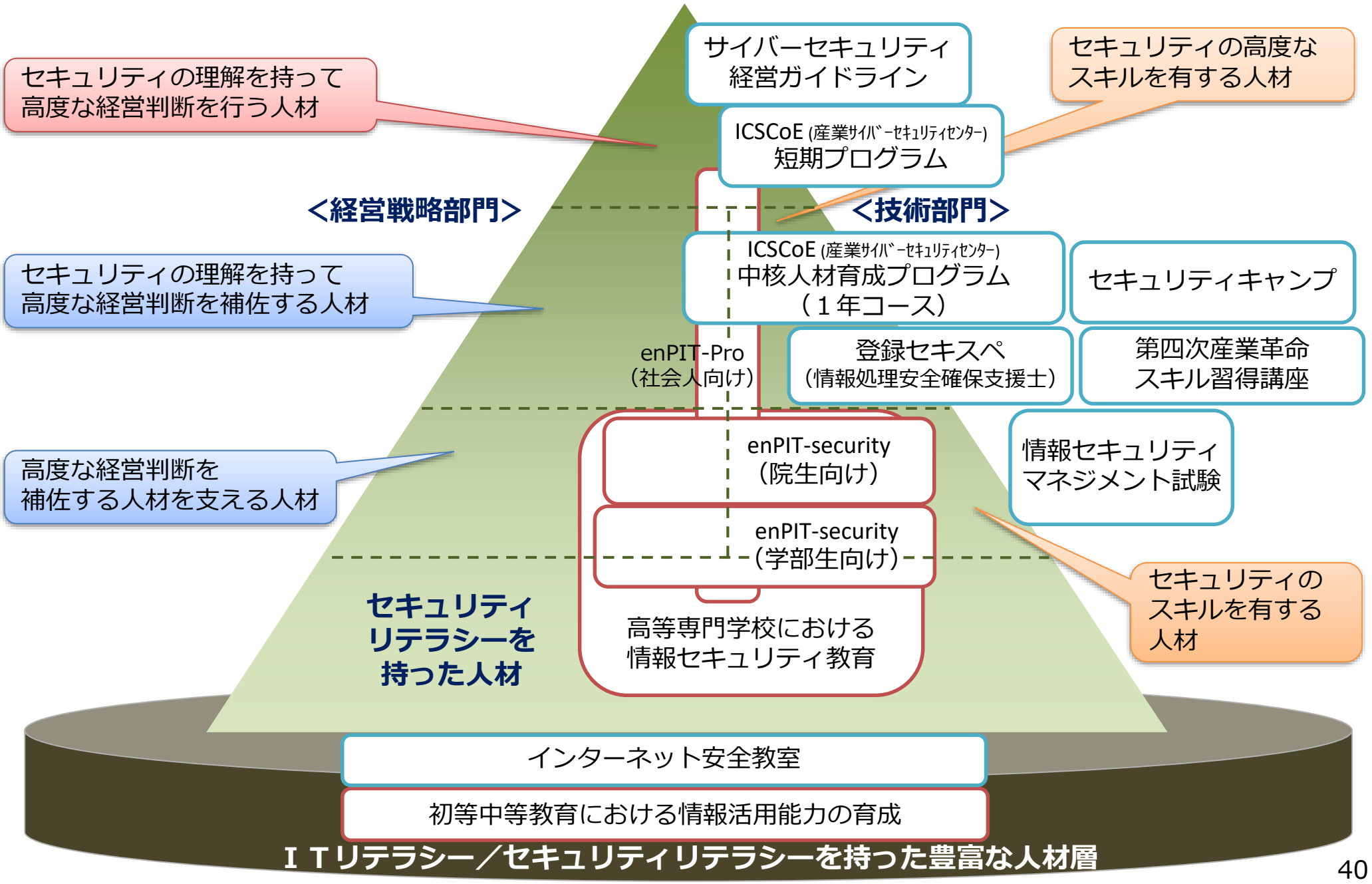
育成すべき人材について（イメージ）

- セキュリティ人材の育成に当たっては、ＩＴリテラシー／セキュリティリテラシー（IT／セキュリティの基礎的な素養）を持った豊富な人材層が必要。
- セキュリティリテラシーやITの基本的知識を持つ人材の育成によって、ベースとなる人材層の拡大を図るとともに、高度なセキュリティスキルを持つ人材の育成、セキュリティリテラシーを持つ戦略マネジメント部門の育成に取り組んでいく。
- また、制御系に対する脅威なども増加する中で、OT人材をセキュリティ対応に活用するなどにより、セキュリティ人材の確保を進めることが重要。

企業内人材のイメージ図



既存の人材育成施策のターゲット（イメージ）



産業サイバーセキュリティセンター（ICSCoE）

- 2017年4月、IPAに産業サイバーセキュリティセンターを設置
- 電力、ガス、鉄鋼、石油、化学、自動車、鉄道、ビル、空港、放送、通信、住宅等の各業界60社以上から約80名の研修生を受け入れ、実践的な演習・対策立案等のトレーニングを行う。
- 2017年9月、米国・国土安全保障省（DHS）及びICS-CERTから専門家を招聘し、「産業分野におけるサイバーセキュリティの日米共同演習」を実施
- 2017年11月、イスラエルから複数の有識者を招聘し、世界の最新動向を踏まえた特別講義の開催

- **IT系・制御系に精通した専門人材の育成**
- **模擬プラントを用いた対策立案**
- **実際の制御システムの安全性・信頼性検証等**
- **攻撃情報の調査・分析**

現場を指揮・指導するリーダーを育成

模擬プラント全景

機械製造設備プラント

発電模擬プラント

セキュリティ・キャンプ

- 2004年から開始し、若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材を創出。
- 民間企業と一丸となって、倫理面も含めたセキュリティ技術と、最新ノウハウを、第一線の技術者から伝授する場を創出。これまで累計で６６３名が受講。
- 地方におけるセキュリティ・キャンプ（地方大会）により、セキュリティ人材の裾野と輪を拡大。

セキュリティ・キャンプ卒業生の例

清水郁美さん
2015年修了（15歳）

米国ラスベガスで開催される世界最大のハッカーの祭典「DEFCON(デフコン)。その目玉イベントのハッカー大会において、８位入賞を果たした。

SECCON　（セキュリティ・コンテスト）について

- SECCON（SECurity CONtest）とは、2012年度から開催されている、実験ネットワーク内で行う擬似的な攻防戦などを通じてセキュリティ技術を競うコンテスト。
- 2016年には世界99カ国、4,349人、2017年には世界102カ国、4,347人が予選参加する日本最大の国際競技大会に成長。

■SECCON2016
1位　CyKor(韓国)
2位　PwnPineappleApplePwn(韓国)
3位　eee（中国）
4位　２１７（台湾）
5位　binja（日本）

■SECCON2017
1位　CyKor（韓国）
2位　PPP（米国）
3位　dododo（日本）
4位　HITCON（台湾）
5位　２１７（台湾）

情報処理安全確保支援士（登録セキスペ）制度

- 情報セキュリティの専門人材の識別を容易にし、専門人材へのアクセスを確保するため、国家資格「情報処理安全確保支援士」（通称：登録セキスペ）制度を創設。
- 2020年までに登録者3万人超を目指す。

◆ 政府機関や企業等のサイバーセキュリティ対策を強化するため、専門人材を見える化し、活用できる環境を整備することが必要

➡ **情報処理安全支援士の名称の独占使用**

➡ **登録簿整備**

◆ 技術進歩等が早いサイバーセキュリティ分野においては、知識等が陳腐化するおそれ

➡ **講習の受講を義務化**

➡ **更新制の導入**

◆ 民間企業等が安心して人材を活用できるようにするには、専門人材に厳格な秘密保持が確保されていることが必要

➡ **業務上知り得た秘密の保持義務を措置**

情報処理安全確保支援士
（登録セキスペ）

2016年

10月21日　情報処理の促進に関する法律改正法施行

2017年

4月　1日　第1回登録により、4,172名の登録セキスペが誕生

4月16日　第1回試験実施（25,130名応募）

6月21日　第1回試験合格発表 (2,822名合格)

10月　1日　第2回登録　新たに2,822名が登録

10月15日　第2回試験実施(23,452名応募)

12月20日　第2回試験合格発表（2,767名合格）

第四次産業革命スキル習得講座認定制度（概要）

Reスキル講座

● ＩＴ・データを中心とした将来の成長が強く見込まれ、雇用創出に貢献する分野において、社会人が高度な専門性を身に付けキャリアアップを図る、専門的・実践的な教育訓練講座を経済産業大臣が認定する。

※ 厚生労働省が定める一定の要件を満たし、厚生労働大臣の指定を受けた講座は「専門実践教育訓練給付」の対象となる。

■講座の要件

- ✓ 育成する職業、能力・スキル、訓練の内容を公表
- ✓ 必要な実務知識、技術、技能を公表
- ✓ 実習、実技、演習又は発表などが含まれる実践的な講座がカリキュラムの半分以上
- ✓ 審査、試験等により訓練の成果を評価
- ✓ 社会人が受けやすい工夫（e-ラーニング等）
- ✓ 事後評価の仕組みを構築　等

■実施機関の要件

- ✓ 継続的・安定的に遂行できること（講座の実績・財務状況等）
- ✓ 組織体制や設備、講師等を有すること
- ✓ 欠格要件等に該当しないこと　等

■認定の期間

- ✓ 適用の日から３年間

■対象分野・目標

※IT技術の基礎・初級は対象としない。

(1) IT（IT業界）

- 新技術・システム
  - ① クラウド、ＩｏＴ、ＡＩ、データサイエンス　等
    - 開発手法：デジタルビジネス開発（デザイン思考、サービス企画、データ分析、アジャイル等）との組み合わせも想定
- 高度技術
  - ② ネットワーク、**セキュリティ**　等

(2) 産業界のＩＴ利活用

- 自動車（モデルベース開発）　等

（目標） ＩＴＳＳレベル４相当を目指す

※ **ＩＰＡ等からの専門的な助言を踏まえ、外部専門家による審査を経て認定を行う**

（参考）第四次産業革命スキル習得講座（第１回認定）

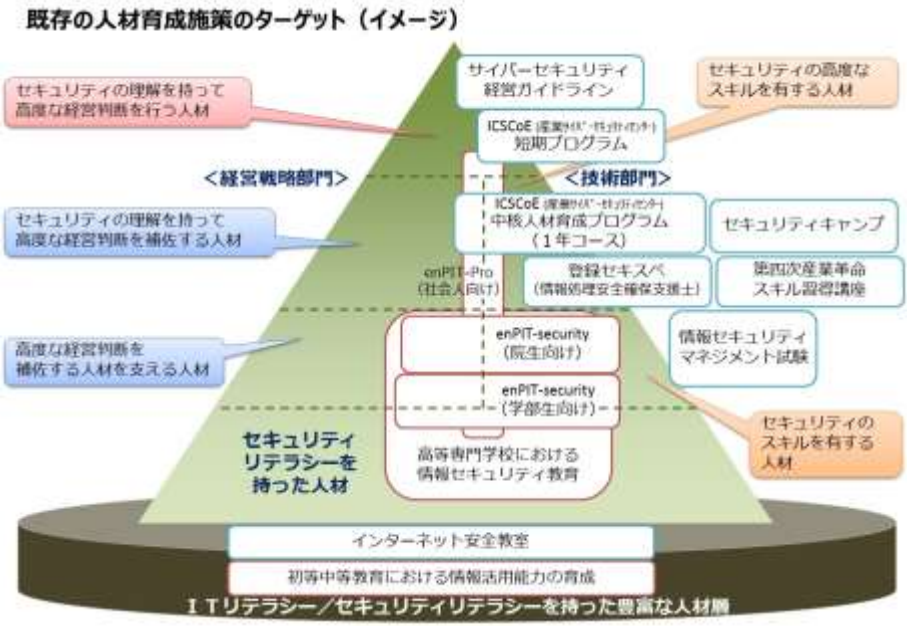
Reスキル講座

ＡＩ（４講座）	
株式会社チェンジ	「AI活用コンサルタント」育成トレーニング　～AIer 育成プログラム～
株式会社ウチダ人材開発センタ	ＡＩ活用講座
日本マイクロソフト株式会社	ディープラーニングハンズオンセミナー
株式会社富士通ラーニングメディア	Fujitsu Digital Business College／AI・データ分析を活用するイノベーター
ＩｏＴ（１講座）	
株式会社ウチダ人材開発センタ	ＩｏＴ活用講座　上級編
クラウド（４講座）	
デジタルハリウッド株式会社	ジーズアカデミーTOKYO　LABコース
NECマネジメントパートナー株式会社	クラウド基盤構築とクラウドサービス適用検討 -Microsoft Azure編-
株式会社ITプレナーズジャパン・アジアパシフィック	ICT利活用コース　～クラウドサービスマネジメント～
株式会社富士通ラーニングメディア	デジタルビジネス創出人材育成コース
データサイエンス（７講座）	
株式会社ｅｆｔａｘ	データ分析教育講座　白・茶・黒帯編
株式会社ブレインパッド	データサイエンティスト入門研修
株式会社ブレインパッド	データサイエンティスト入門研修（アドバンスド）
株式会社アイ・ラーニング	データサイエンティスト育成講座
株式会社チェンジ	データサイエンティスト養成コース
株式会社日立インフォメーションアカデミー	データ利活用技術者育成講座
フューチャー株式会社	データサイエンティスト養成講座
セキュリティ（６講座）	
株式会社アイ・ラーニング	日本IBM　CSIRT研修
NECマネジメントパートナー株式会社	情報セキュリティ技術者養成講座
シーティーシー・テクノロジー株式会社	セキュリティエンジニア養成講座
株式会社ラック	実践！デジタル・フォレンジック完全マスター
株式会社ラック	実践！マルウェア解析完全マスター
ネットワンシステムズ株式会社	CSIRT能力向上研修
自動車（モデルベース開発）（１講座）	
公益財団法人ひろしま産業振興機構	モデルベース開発プロセス研修

（１）セキュリティ人材をめぐる状況
（２）セキュリティ人材育成政策の現状
（３）今後のセキュリティ人材育成政策の方向性

セキュリティ人材育成における課題

- **<u>セキュリティニーズに対応する人材マッチングのためのセキュリティ人材像の明確化</u>**
  - セキュリティ人材に求める役割、役割に応じたスキル、スキルを測る指標が必ずしも明確化されていない。
- **<u>サイバーリスクを理解する経営層・経営企画担当層の育成</u>**
  - サイバーセキュリティは経営層が当然に認識すべきリスクの１つ。Society5.0の実現に向けて次期経営層・経営企画担当層のサイバーセキュリティ教育は喫緊の課題。
- **<u>産学官連携推進</u>**
  - 産学官それぞれがセキュリティ人材の育成に取り組んでいる中、厚みのある人材層形成のためには、これらを有機的に結び付けることが必要。



＜産業界に期待する役割＞

- ✓ 産業の魅力向上
- ✓ 流動性向上により高付加価値領域への人材配置
- ✓ 高い競争力の実現
  - → 企業収益の確保
  - → 優秀な情報技術者に対する高い処遇という好循環の実現

【文部科学省作成資料より抜粋】

産業サイバーセキュリティ政策（人材関係）の推進体制の考え方（案）

1．経営企画の幹部候補へのサイバーセキュリティ教育

次世代経営人材育成
- 戦略的経営人材の育成支援

【IPA】ICSCoE短期コースの活用

2．セキュリティ人材の可視化・育成

人材評価モデルの具体化
（原案年度内）
- 海外におけるセキュリティ人材に求める要件、評価指標の整理　→　モデル化
- セキュリティ人材保有とセキュリティ成熟度の関係

人材可視化モデル
- スキルセットの整理
- 登録ｾｷｽﾍﾟ等の資格との連動
- 専門人材の評価・可視化モデルの提示

【産業横断人材育成検討会】
セキュリティスキル標準の整理

【NISC】ｻｲﾊﾞｰｾｷｭﾘﾃｨ人材育成に関する施策間連携ＷＧにおける検討

【IPA】
・ICSCoE中核人材育成プログラム
・資格（セキスペ等）の提供

3．サイバーセキュリティリテラシー、ITリテラシー

座間事件対応「インターネット上の有害環境から若者を守るための対策」
- （教室等）草の根啓蒙活動

【IPA】インターネット安全教室

＜産学官連携促進＞

- 可視化モデル策定時の連携
- ICSCoEの活用
- 拠点高専等への専門講師派遣などによる集中支援
- 産業界とのマッチング

ビジネススクール

enPIT-Pro

enPIT-security

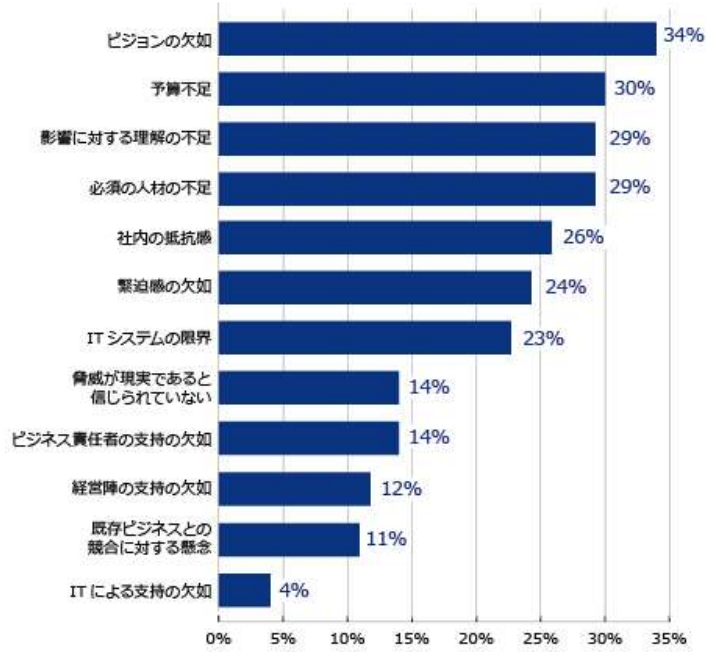
大学工学部教育

高等専門学校

デジタル化時代における経営人材の育成

- 世界的にデジタル化が進展する中で、日本企業のデジタル・トランスフォーメーションが急務。
- 国際的な競争に勝ち抜くため、デジタル革命に立ち向かう戦略性を備えた、次世代の経営人材を集中的に育成するプログラムを産学官連携して構築することを検討。
- その取組の中で、**サイバーセキュリティのリテラシーについても、身につけるべき要素として位置付けていく**。

デジタルディスラプションへの対応における障壁



（出所）KPMG（2015）「グローバルCIO調査レポート」

プログラム案

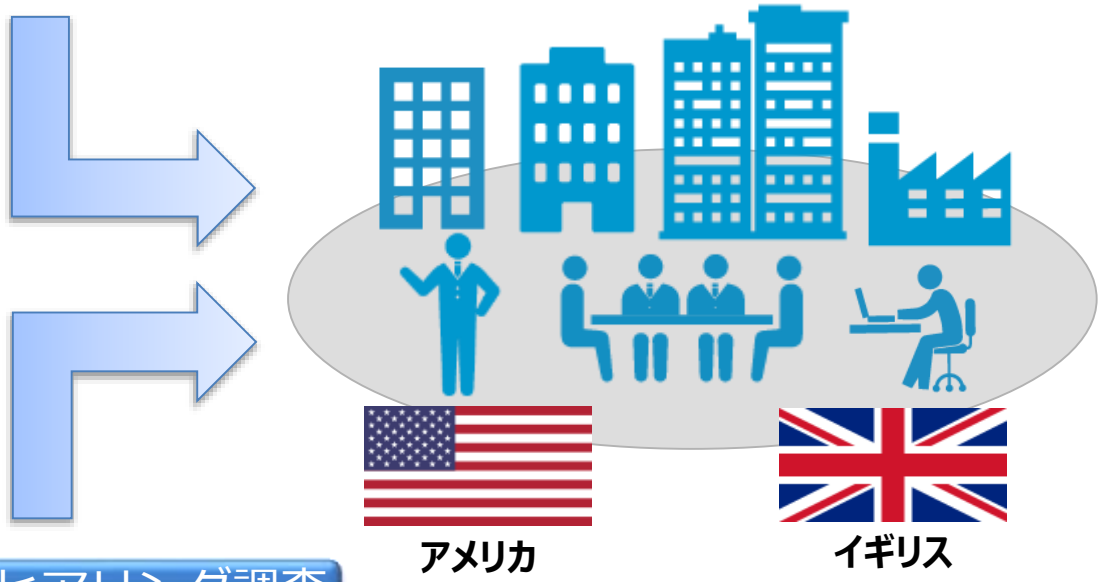
対象	・30代後半～40代の社会人 ・所属組織で次世代の経営を担うことを期待される方 ・現在も経営トップへのアドバイスが期待される方
身につけるべき要素	・戦略的発想 ・デジタル革命を踏まえた、ITを活用した戦略構築 ・**サイバーセキュリティのリテラシー** ・企業や業種をこえた横連携、ネットワーク形成

海外調査（概要）

- ①確保すべきセキュリティ人材のスキルセットとセキュリティ人材の評価指標、②セキュリティ人材の保有状況とセキュリティ成熟度の関係について、下記の海外調査を実施中。

アンケート調査

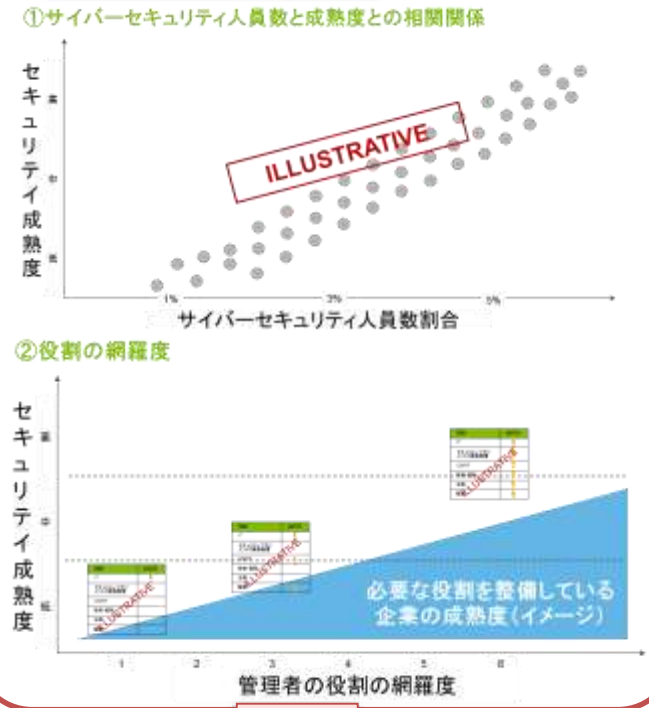
- 求めるセキュリティ人材の要件、評価指標等を調査
- 海外企業のセキュリティ成熟度測定



ヒアリング調査

- CISO及び経営層にヒアリング調査を実施
- 人材のキャリアプランや雇用方針など具体的な内容を調査

成果イメージ



調査結果から得られた傾向をもとに

- ユーザー企業で保有すべき人材の定義・評価指標を検討
- 人材保有状況における企業の評価指標を検討

（参考）既存のスキルモデル

■産業横断サイバーセキュリティ人材育成検討会

- ✓ サイバーセキュリティの各種課題において、最初に問題となる「人材の確保（育成と雇用）」について、企業が互いに協力して取り組むため、産業界の自主的な取組として、「産業横断サイバーセキュリティ人材育成検討会」を設立。
- ✓ 2016年9月に第一期の成果報告として、「産業横断人材定義リファレンス」を作成。**ユーザー企業において必要な情報システムセキュリティの機能とスキルセット**をまとめて公開。
- ✓ 現在、産業横断サイバーセキュリティ人材育成検討会は、一般社団法人サイバーリスク情報センターに設置され、取組を継続。

■IPA スキル標準（ITSS＋）

- ✓ IPAで作成しているITスキル標準（ITSS）に加えるかたちで、専門分野の更なる具体化が求められる「セキュリティ領域」について、新スキル標準の策定に先行し“ITSS+”（プラス）として過渡的に取りまとめを行い、公開。
- ✓ ITSS+は、主に従来ITSSが対象としている情報サービスの提供やユーザ企業のIS部門に関わっている**既存の人材が「セキュリティ領域」や「データサイエンス領域」のスキル強化を図るための“学び直し”の指針として活用**されることを想定。

■JNSA セキュリティ知識分野（SecBoK）人材スキルマップ

- ✓ JNSAにおいて、**情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキルを体系的に整理**した「情報セキュリティスキルマップ」の作成を継続実施。
- ✓ IPAのITSS＋の発表を受け、この人材定義マップとの連携を前提としてリバイスを実施。

インターネット安全教室

- インターネットの安全利用に関する基礎知識（パスワード管理、ウイルス対策等）を学習できるセミナー「インターネット安全教室」を全国各地の関係団体等と協力して実施。
- 座間市の事件を受けて、教育内容の充実、教育対象の拡充を予定。

インターネット安全教室

IPA

講師トレーニング
を実施

**全国のNPO法人、大学等
（共催団体）**

講師の派遣

全国でインターネット安全教室を開催

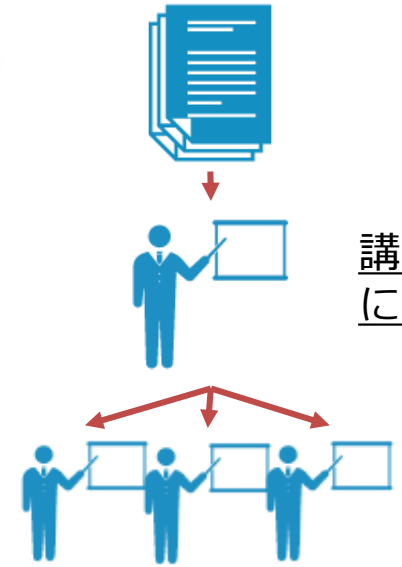
座間市の事件を受けた対応

- **教育内容の充実**

  ー座間市の事件を受けて平成30年度より
  SNSに関する内容を追加

- **教育対象の拡充**

  ー教育現場を対象としたインターネット安全教室の開催



教育現場のニーズを
調査・分析

講師トレーニング用資料
にSNSに関する内容を反映

講師が教材に反映

１．ＷＧ２（経営･人材･国際）の目的･ねらい

２．経営

３．人材

４．国際

サイバーセキュリティの強化に向けた国際連携基盤の構築、整備

達成すべきゴール（イメージ）

- 二国間サイバー協議（米、EU、英、独、仏、イスラエル、エストニア、豪州等）及び多国間における議論を通じた各国との政府間レベルの**信頼醸成の基盤の構築**
- 各国との産業間対話の強化による**サイバーセキュリティに関する共通認識の形成**
- 産業サイバーセキュリティセンター（ICSCoE）を活用した海外との**人材交流、育成基盤の構築**
- 官民連携した二国間・多国間対話及び相互承認システムの構築を通じた安全な**サプライチェーンセキュリティ確保のための基盤の構築**
- ASEAN等への人材育成支援などのキャパシティビルディングを通じた円滑な企業活動のための環境基盤の構築、**国際的なルールメイキングにおける支持者の獲得**

アメリカ

- 様々な政策対話を行う中、アメリカと日本の制御システムセキュリティ分野における知見を生かした**日米連携での人材育成**まで協力を拡大
- 日米産業間での**知見の共有、信頼醸成の構築**を支援

- **日米共同演習（Step1）（2017年9月@東京）**
  - 国土安全保障省（DHS）/ ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)から専門家7名を産業サイバーセキュリティセンター（ICSCoE）に招聘し、「産業分野におけるサイバーセキュリティの日米共同演習」を実施。
- **日米共同演習（Step2）（2018年2月@アイダホ国立研究所）**
  - ICSCoEの生徒2名をアイダホ国立研究所（INL）に派遣し、ICS-CERTが提供する301演習を5日間受講。
- **日米共同演習（Step3）（2018年9月@東京）**
  - DHS/ICS-CERTとICSCoEが共同で、産業分野におけるサイバーセキュリティ演習をASEAN、豪州、NZからの参加者も含めて実施。
- **Track 1.5の準備会合（2018年2月@DC）**
  - 日米の民間事業者が集まり、情報共有の促進、知見の共有。

日米共同演習(2017.9)

欧州（EU 、ドイツ）

- Cybersecurity ACT、ICT Certification等**ルール作りから始める欧州との制度調和**

【EU】

- **日EUICT対話＆サイバーセキュリティ認証に関する専門家会合の立ち上げ（2017年10月）**

➢ ICT 製品の確認・認証のあり方について情報交換をする専門会合の立ち上げを合意

【ドイツ】

- **産業サイバーセキュリティに関する日独共同文書の発出（2017年3月@ベルリンG20会合）**

➢ 産業サイバーセキュリティ分野の検討論点や日独間での今後の協力方針等を記載した日独共同文書（Common Position Paper）をドイツPI4.0とRRIで発出。

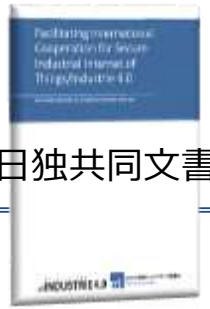
＊ドイツPI4.0：Plattform Industrie 4.0　ドイツのインダストリー4.0を推進する官民一体の団体。ドイツ連邦経済エネルギー大臣と連邦教育科学大臣が最高責任者。

＊RRI：ロボット革命イニシアティブ協議会。「ロボット新戦略」（2015年2月10日日本経済再生本部決定）に基づき、同戦略に掲げられた「ロボット革命」を推進するために、民間主導で設立された組織的プラットフォーム。

- **Securing Global Industrial Value Networks （2018年5月@ベルリン）**

➢ ドイツ経済エネルギー省主催の会議において、ドイツPI4とRRIがサプライチェーンサイバーセキュリティに関する日独共同文書を発出すべく準備中。

ドイツG20会合（2017年3月）



日独共同文書

イスラエル

● **イスラエルの持つ強み**を、日本の技術向上・人材育成・新たなビジネスチャンスに繋げていく。

●世界で最もサイバー攻撃を受けていると言われる国

●実戦に基づいた不断の更新を続ける防御技術・ノウハウ

8200 יחידה

● **日・イスラエル経済省庁間サイバーセキュリティ協力覚書（MOC）（2017年5月署名）**
  - イスラエル国家サイバー本部（INCD）を含むイスラエル政府との協力の土台

● **産業サイバーセキュリティセンター（ICSCoE）を通じた協力**
  - 世界の最新動向に基づく特別講義や演習を実施

● **イスラエル民間セクターが擁する製品・サービス・経験を知る機会の提供**
  - 官民サイバーセキュリティワークショップの開催（2017年11月）
  - サイバーテック東京への後援（2017年11月）

ASEAN

- 日本へのサイバー攻撃の起点・踏み台となり得るASEAN地域に対して、重要インフラ防護をはじめとした**キャパシティビルディング支援を実施**。
- **セキュリティ産業にとって有望な市場**であるASEAN諸国において、**人材育成や制度設計の支援**を通じて日本企業の活動を側面支援。
- 同時に、データ保護主義など民間主体の産業活動をゆがめる独自ルール形成の動きが地域全体に波及することを防ぐため、**国際的なルールメイキングにおける日本の方針への理解と支持拡大**を目指す。

- **日ASEANサイバーセキュリティ政策会議**
  - NISC、総務省とともに、重要インフラ防護のためのガイドラインの作成を支援。
  - オペレーションの専門家を対象とした机上演習やワークショップを実施。
  - 毎年開催されるWGの場で、TPP三原則の重要性やリスクベースアプローチの有効性について啓発。

- **AOTSを通じたASEAN向け能力構築支援**
  - ASEAN加盟国のうち８か国を対象に海外産業人材育成協会（AOTS）を通じた研修を実施。（2012－2016年度）

- **AOTSを通じた対ベトナム電力セキュリティ研修**
  - 電力制御システムに関するセキュリティ規制策定能力向上支援（2017年度）
- **日米共同アウトリーチ（2018年9月@東京）【日米共同演習（Step3）の再掲】**

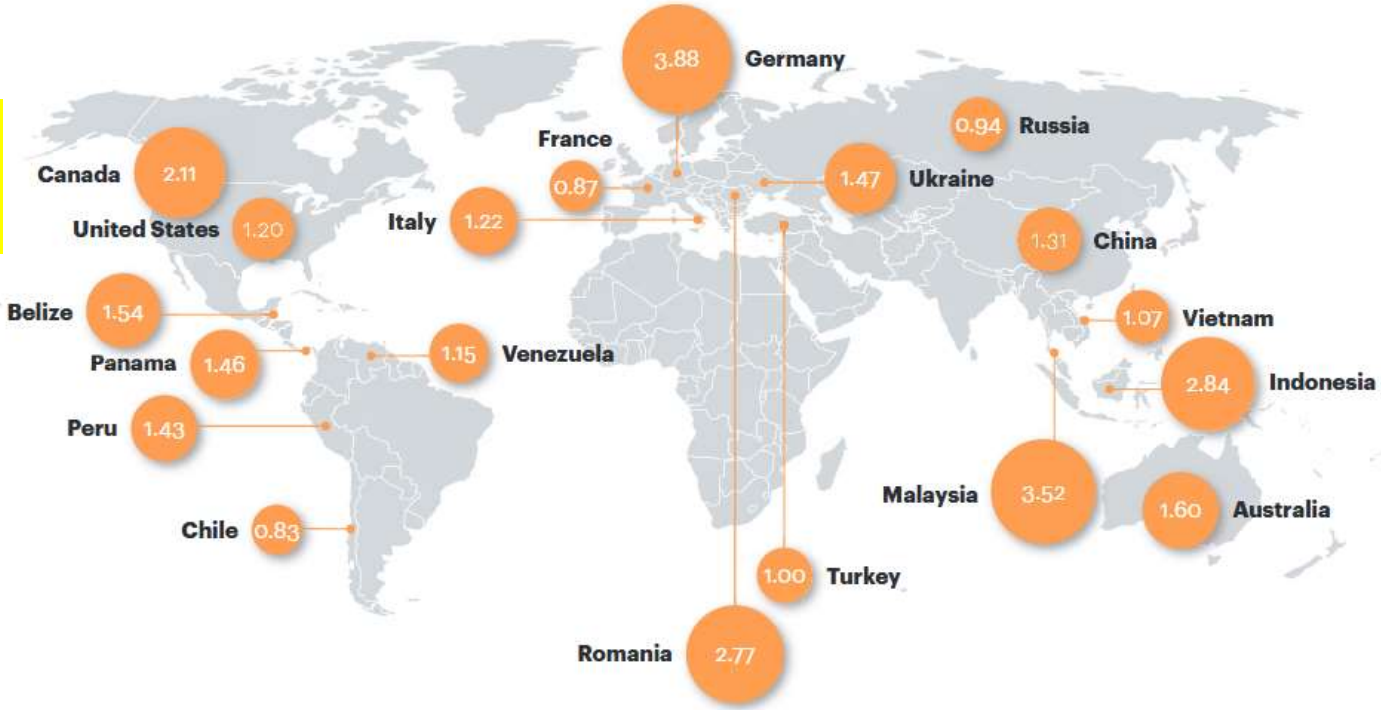
- DHS/ICS-CERTとICSCoEが共同で、産業分野におけるサイバーセキュリティ演習をASEAN、豪州、NZからの参加者も含めて実施。

ASEANにおける状況

参考：第１回WG１（制度・技術・標準化）において配布

- **ASEAN諸国は、サイバー攻撃の活動拠点となっている。**
  - マレーシア、インドネシア、ベトナムは、遮断された不正なWEB活動の起点となっている比率が高く、マルウェアの攻撃に悪用されている。
  - ベトナムは、2015年12月から2016年11月までの間に、168万個のIPアドレスの遮断を記録した。さらに、2016年に発生したIoT機器に対する攻撃の起点に悪用された数が世界で5番目に多かった。

Blocked suspicious Web activity, by country of origin (expected ratio = 1.0)



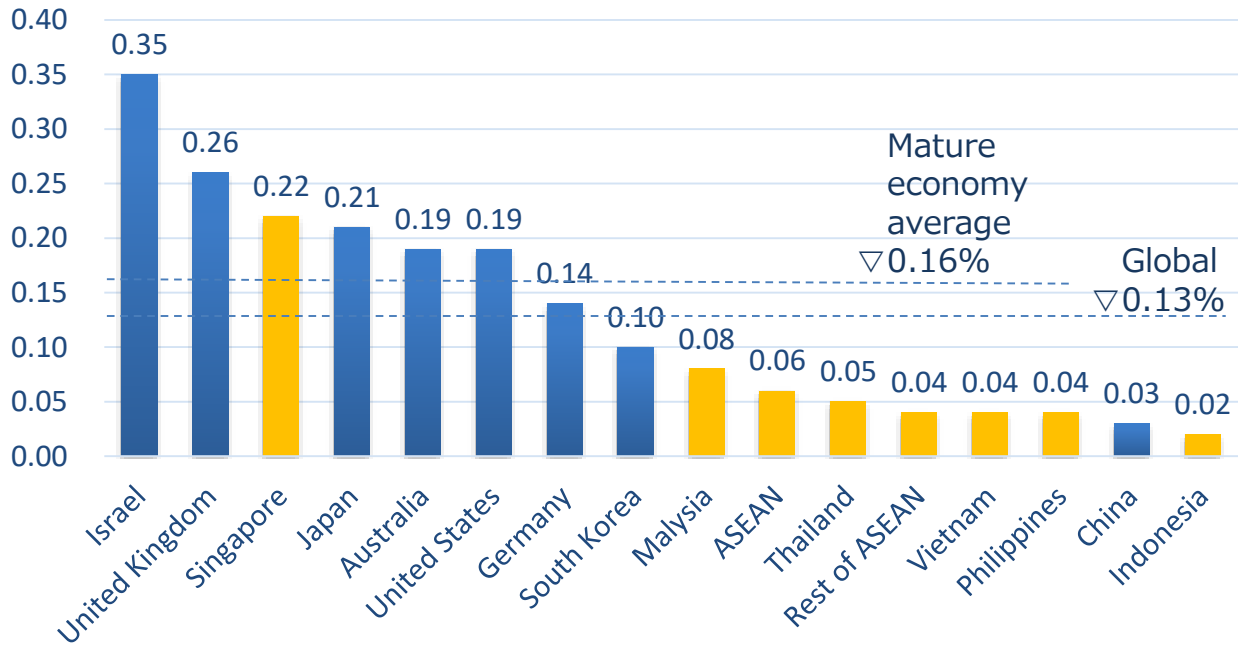
出典：「A.T. Kearney, “Cybersecurity in ASEAN—An Urgent Call to Action”」より引用

ASEANにおける状況

参考：第１回WG１（制度・技術・標準化）において配布

- **サイバーセキュリティに対するポリシーが不十分。**
  - **ASEAN地域におけるサイバーレジリエンスは、一般的に低いという評価 （特に、ポリシー、ガバナンス、サイバーセキュリティ能力）。**
  - **産業界もリスクを過少評価しており、結果として、サイバーセキュリティに対する投資が不足しているという指摘あり。**

Cybersecurity spending (% of GDP for 2017)



出典：「A.T. Kearney, “Cybersecurity in ASEAN—An Urgent Call to Action”」より引用