経済産業省

資料３

事務局説明資料

経済産業省

商務情報政策局

サイバーセキュリティ課

1．経営

2．人材

3．国際

サイバーセキュリティ経営における全体像

- 経営層向け、現場向け、中小企業向けの３つの視点で、サイバーセキュリティ経営を促進するための施策を検討。

経営層向け

サイバーセキュリティ経営ガイドラインを軸として経営者の意識向上を図るとともに、将来的にセキュリティの高い企業が投資家の評価を受けられる枠組みの構築を支援する。

現場向け

サイバーセキュリティ経営ガイドラインの実践規範となるプラクティスや、対策状況の可視化ツールの提供により対策の実行を支援する。

中小企業向け

サイバー保険との連動も検討しつつ、中小企業におけるセキュリティに関するトラブルの相談対応を支援する。

（１）経営層向けの施策

（２）現場向けの施策

（３）中小企業向けの施策

段階的なサイバーセキュリティ経営の実現

- 以下の3Stepにより、サイバーセキュリティ経営の定着を目指す。

1st Step

サイバーセキュリティ経営の明確化

- サイバーセキュリティ経営ガイドラインの普及・定着

2nd Step

サイバーセキュリティ経営の実践

- CGSガイドラインにサイバーセキュリティを反映
- IRの観点から、サイバーリスクを経営リスクとして認識・自己確認することの重要性を啓発
- 取締役会実効性評価の項目にサイバーリスクを位置づけ
- 投資家に対してもサイバーセキュリティの重要性を啓発

3rd Step

セキュリティの高い企業であることの可視化

- セキュリティの高い企業であることを投資家が評価できるようにするための、サイバーセキュリティ経営に関する情報の開示の在り方の検討

サイバーセキュリティ経営ガイドライン

前回WG資料より再掲

- 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

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

前回WG資料より再掲

- 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

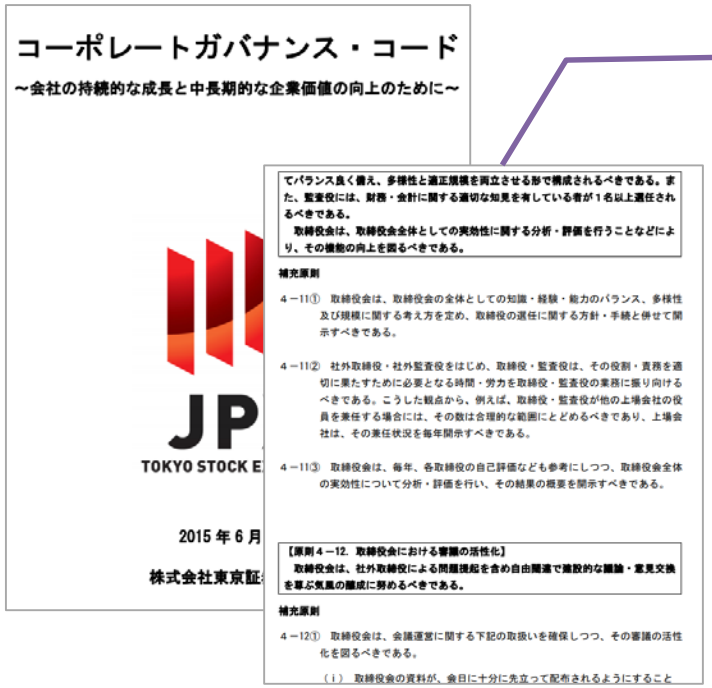
- CEO・経営陣の選解任や評価、報酬に関する**基準及びプロセスを明確化**
- 基準作成やプロセス管理のため、**社外者中心の指名・報酬委員会を設置・活用**（過半数が社外、半々なら委員長が社外）

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**

サイバーセキュリティを考慮した取締役会の実効性評価

- 経営層がサイバーセキュリティに関与していることを、投資家（株主）が確認できるようにすることが重要。（昨今、企業がセキュリティに配慮しているかどうかを投資を行う上での判断材料の一つとしている投資家が増えている）
- コーポレートガバナンス・コードでも求められている取締役会の実効性評価（原則４－１１）に、サイバーセキュリティへの関与も評価項目として組み込むことを促進。


コーポレートガバナンス・コード
～会社の持続的な成長と中長期的な企業価値の向上のために～
2015 年 6 月
株式会社東京証
てバランス良く備え、多様性と適正規模を両立させる形で構成されるべきである。また、監査役には、財務・会計に関する適切な知見を有している者が１名以上選任されるべきである。
取締役会は、取締役会全体としての実効性に関する分析・評価を行うことなどにより、その機能の向上を図るべきである。
補充原則
4－11① 取締役会は、取締役会の全体としての知識・経験・能力のバランス、多様性及び規模に関する考え方を定め、取締役の選任に関する方針・手続と併せて開示すべきである。
4－11② 社外取締役・社外監査役をはじめ、取締役・監査役は、その役割・責務を適切に果たすために必要となる時間・労力を取締役・監査役の業務に振り向けるべきである。こうした観点から、例えば、取締役・監査役が他の上場会社の役員を兼任する場合には、その数は合理的な範囲にとどめるべきであり、上場会社は、その兼任状況を毎年開示すべきである。
4－11③ 取締役会は、毎年、各取締役の自己評価なども参考にしつつ、取締役会全体の実効性について分析・評価を行い、その結果の概要を開示すべきである。
【原則４－12. 取締役会における審議の活性化】
取締役会は、社外取締役による問題提起を含め自由闊達で建設的な議論・意見交換を尊ぶ気風の醸成に努めるべきである。
補充原則
4－12① 取締役会は、会議運営に関する下記の取扱いを確保しつつ、その審議の活性化を図るべきである。
（i） 取締役会の資料が、会日に十分に先立って配布されるようにすること

コーポレートガバナンス・コード
（株式会社東京証券取引所）

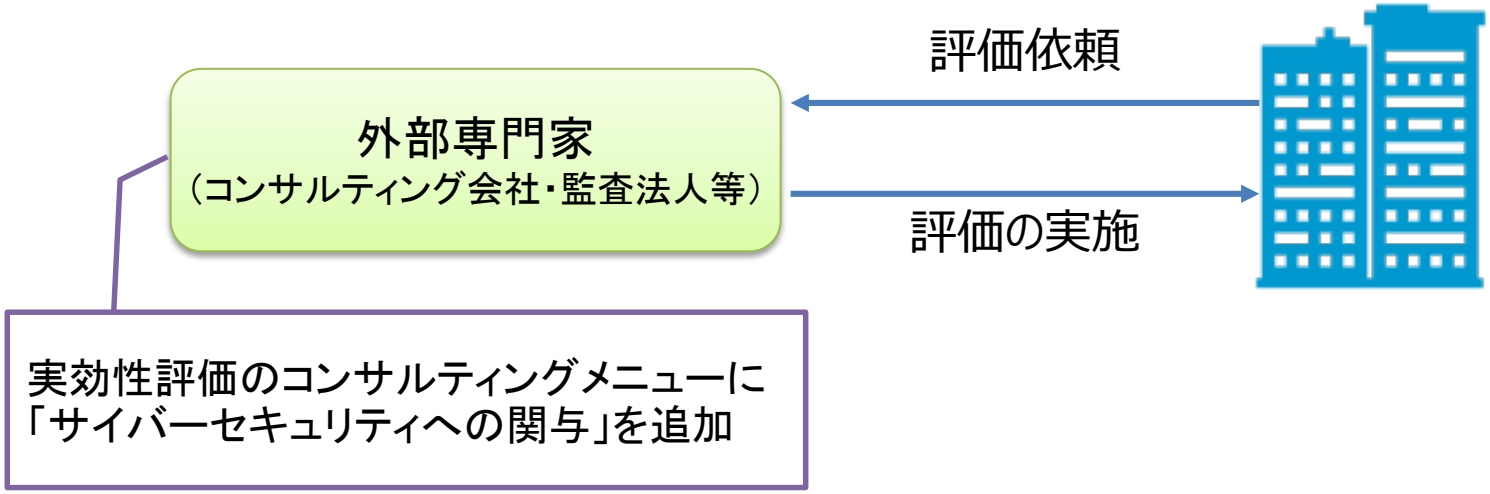
【原則４－１１．取締役会・監査役会の実効性確保のための前提条件】
（中略）
取締役会は、**取締役会全体としての実効性に関する分析・評価を行う**ことなどにより、その機能の向上を図るべきである。

補充原則
４－１１③ 取締役会は、毎年、各取締役の自己評価なども参考にしつつ、取締役会全体の実効性について分析・評価を行い、**その結果の概要を開示すべき**である。

（コーポレートガバナンス・コードより抜粋）

外部専門家との連携による実効性評価の強化

- 実効性評価の実施方法や評価項目は各企業の目指す姿によってそれぞれ定められるものの、外部の専門家による評価を実施することで、評価結果の信頼性が向上。
- **外部専門家と連携し、サイバーセキュリティへの関与状況も考慮した実効性評価を促進**するとともに、**投資家に対するサイバーセキュリティの教育を実施**。



（参考） 英国における実効性評価の位置づけ
2010年に制定された英国コーポレートガバナンス・コードにおいて、主要な上場企業（FTSE350企業）には**外部の専門家を関与させた評価を少なくとも3年ごとに実施することを要求**。

B.6.2. Evaluation of the board of FTSE 350 companies should be externally facilitated at least every three years. The external facilitator should be identified in the annual report and a statement made as to whether they have any other connection with the company.

（The UK Corporate Governance Code（Financial Reporting Council）より抜粋）

（参考）英国の投資家団体の動向

- 英国の投資家団体であるThe Investment Association（IA）とKPMGは、サイバーセキュリティに投資することを経営層に求める報告書（Building Cyber Resilience in Asset Management）を作成。
- IAはこれらの取組を支援するために、企業、規制当局、公的機関と協力してCyber Security Committeeを設立。

<u>英国の投資家は、経営層がサイバーセキュリティに関与しているかどうかを重要視</u>している。

報告書においては、「取締役会はサイバーセキュリティリスクを理解し、説明責任をはたすべき」、「サイバーセキュリティリスクはサプライチェーン全体で管理されるべき」、等について言及

（１）経営層向けの施策

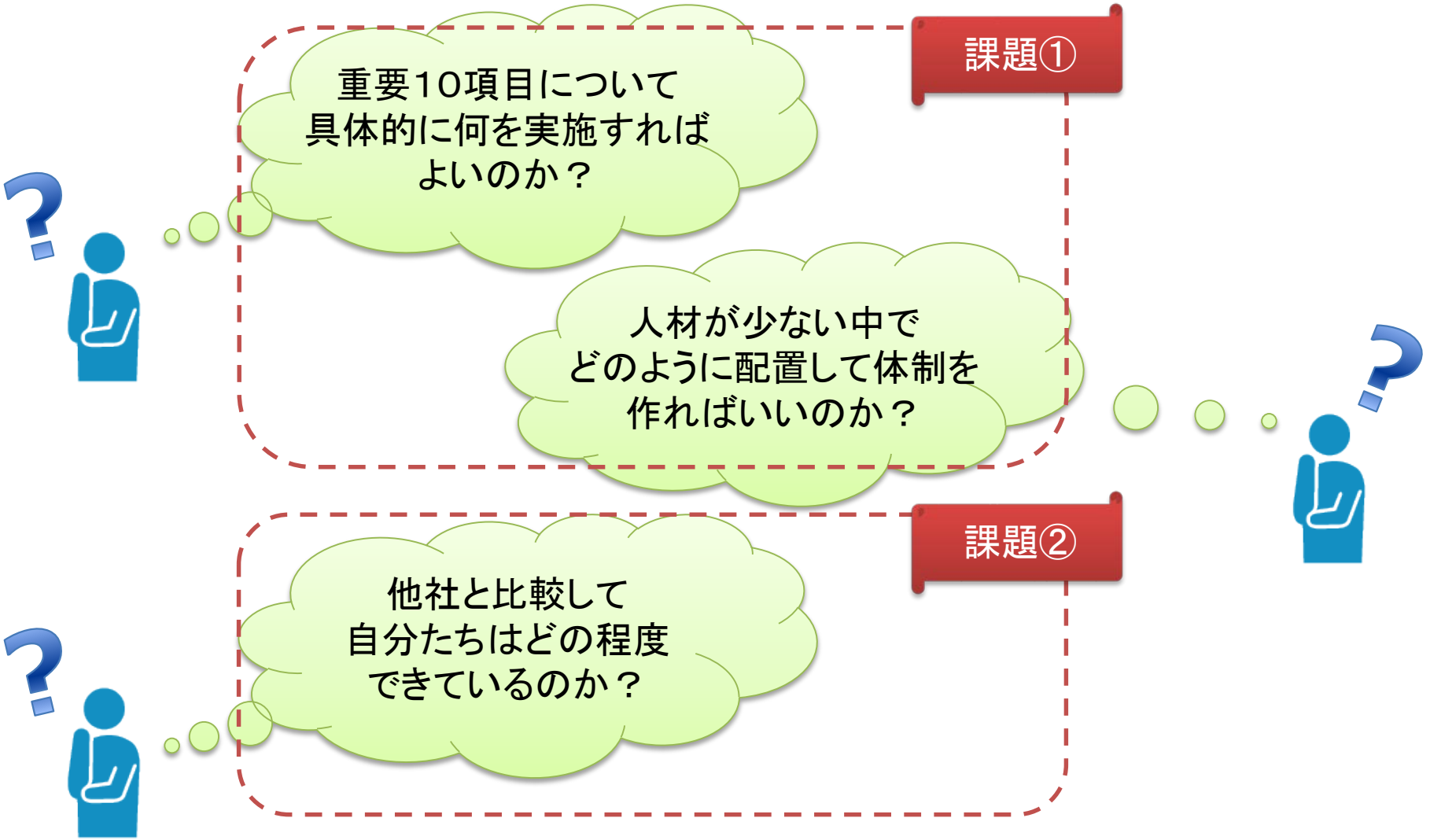
（２）現場向けの施策

（３）中小企業向けの施策

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

前回WG資料より再掲

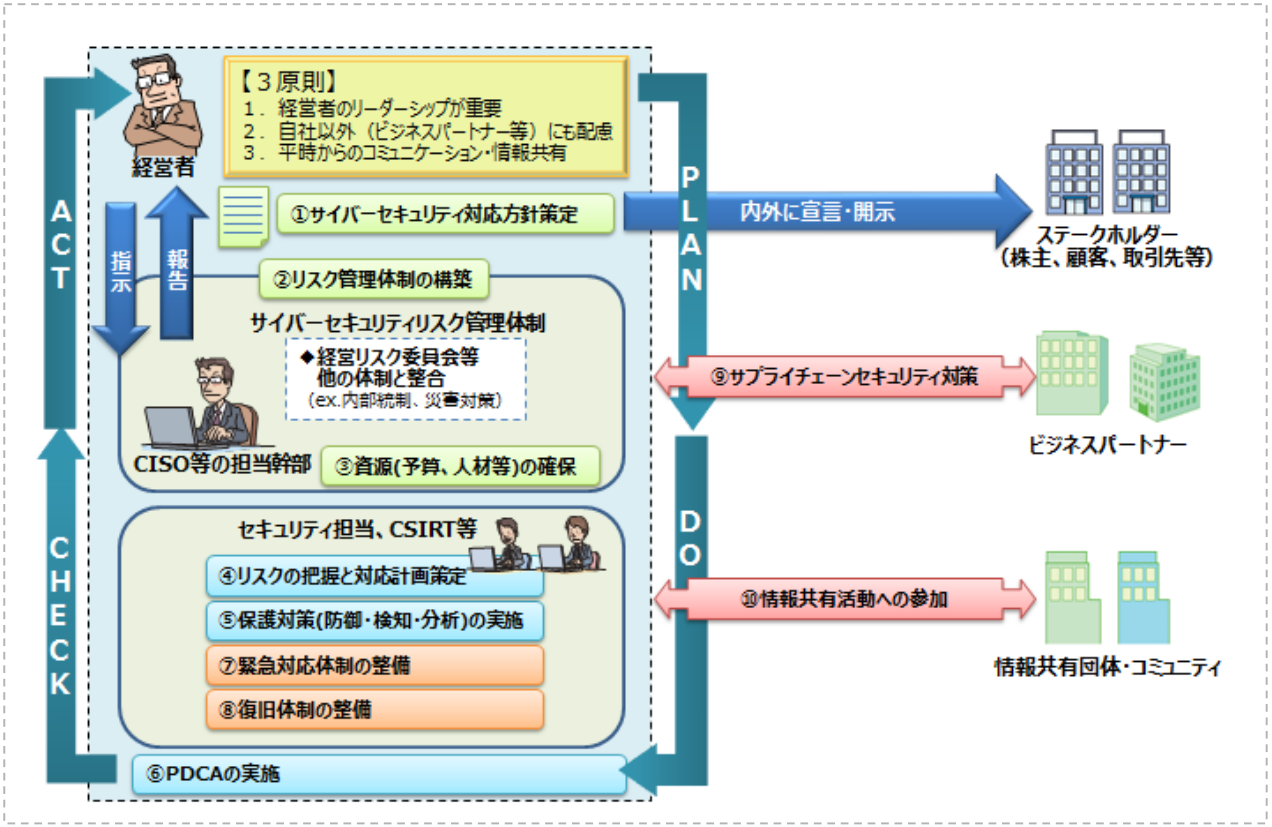
- サイバーセキュリティ経営ガイドラインの内容について認識をしている企業は増加しているものの、対策の実行へ結びつける上で課題を感じている企業も多い。



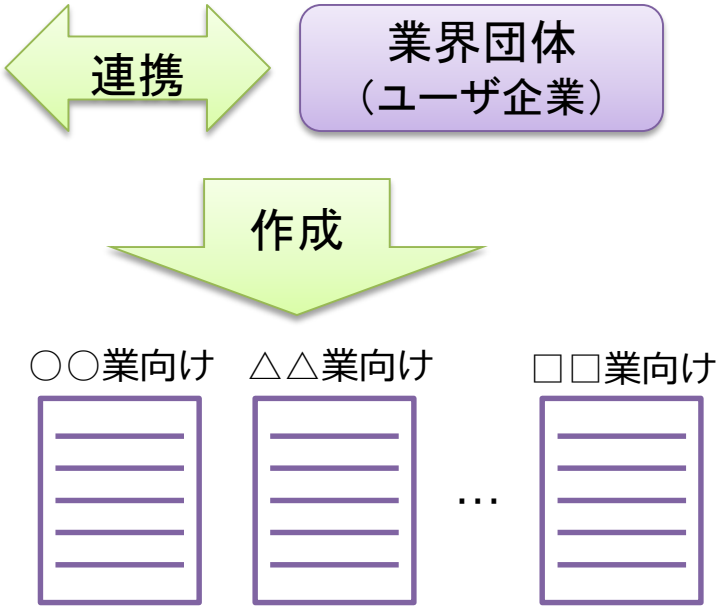
（課題①への対策案）ベストプラクティスの作成

前回WG資料より再掲

- 『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。
- **<u>組織が取り組んでいる具体的な対策事例</u>**や**<u>サイバー攻撃に関する情報共有活動事例</u>**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

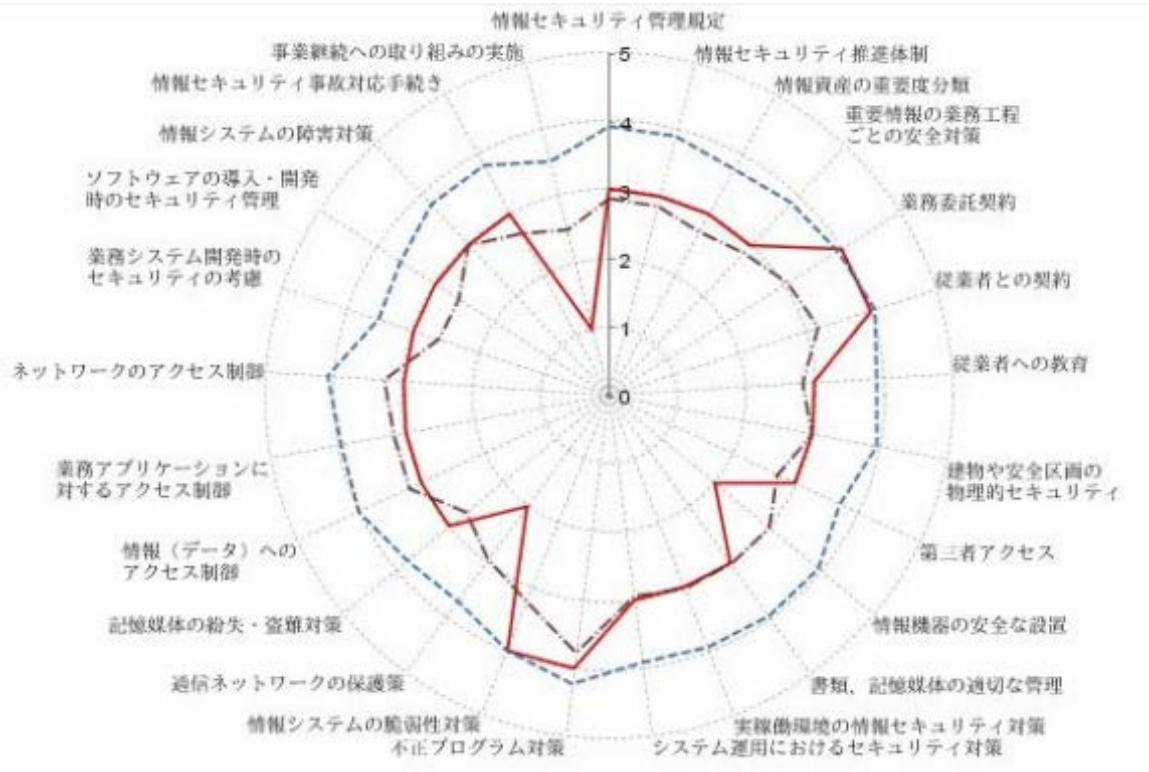


業界ごとの
ベストプラクティス

（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

前回WG資料より再掲

- 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。



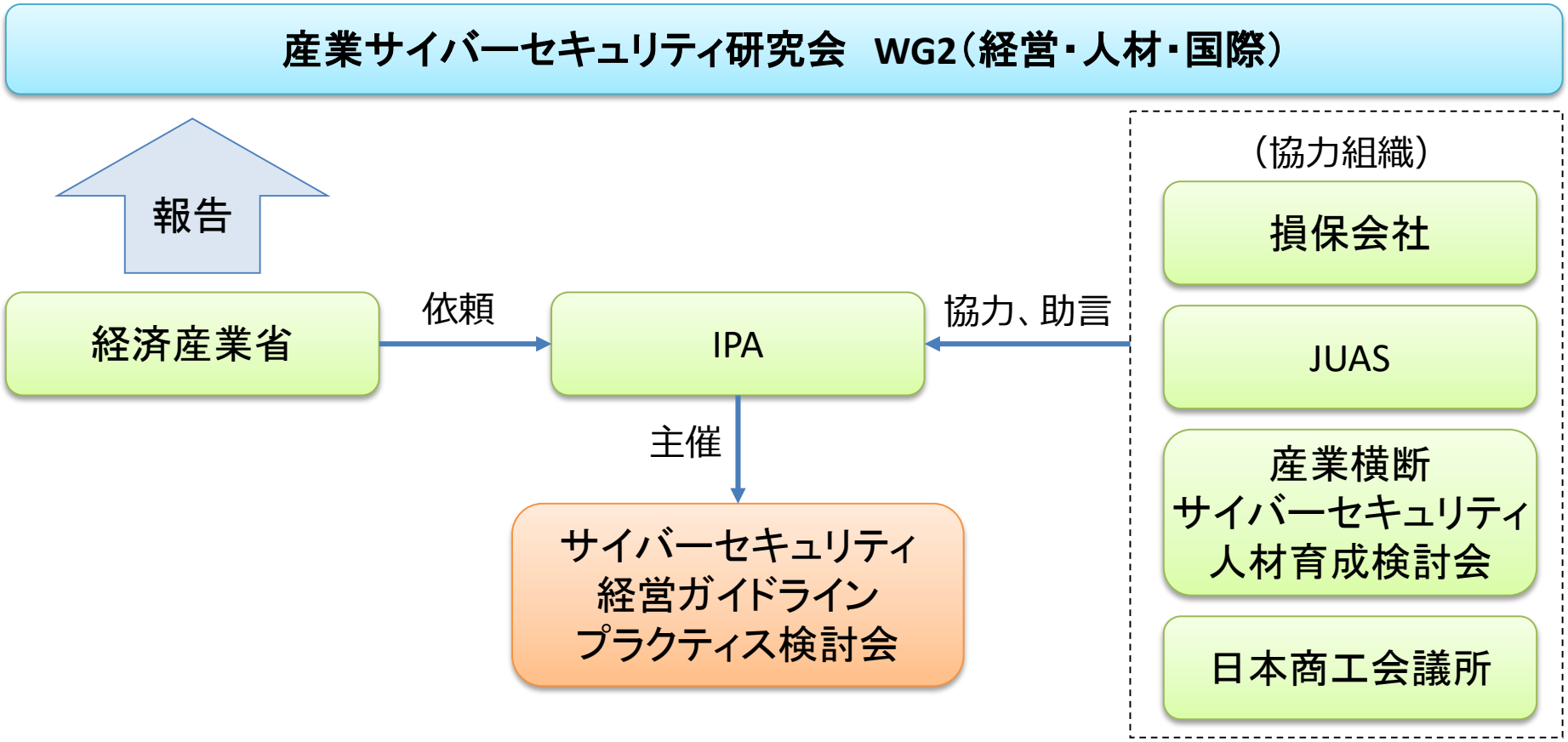
（参考）情報セキュリティ対策ベンチマーク（IPA）

サイバーセキュリティ経営ガイドラインプラクティスと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プラクティスと、セキュリティ対策の実施状況を可視化するツールを作成（平成３０年度中に公開予定）する体制をIPAにて構築。

  ＊ユーザー企業の活動の多様性を踏まえ、多数のセキュリティの実践事例を収集し、体系化する。

＜作成体制＞



米国のサイバーセキュリティ促進策との連携

- 米国の団体（Cyber Readiness Institute、CREATe Compliance等）では、中小企業におけるサイバーセキュリティへの意識の底上げを図るための各種ツールを作成。
- IPAを中心にこうした取組と連携を図りながらツールを整備。

NIST文書やISO/IEC27001等の各種規格をベースとした設問に回答

回答結果に基づき、結果を可視化

（１）経営層向けの施策

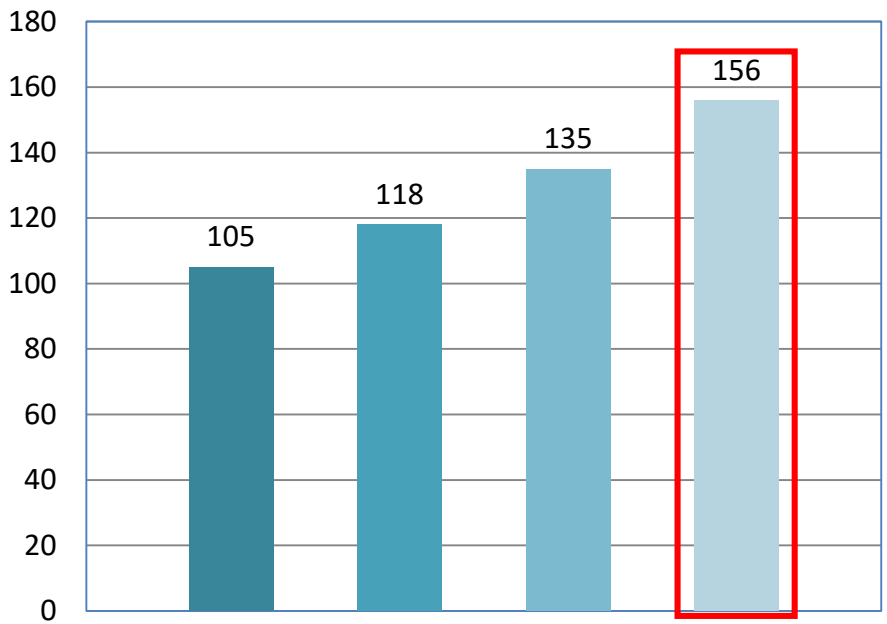
（２）現場向けの施策

（３）中小企業向けの施策

サイバー保険の状況

- 現在日本の情報セキュリティ保険市場は156億円、加入率は全体の１％以下。
- 特に中小企業では、加入メリットが認識されていないことや、費用面の課題などからほとんど加入が進んでいない状況。
- 損害保険会社では、サイバー保険の割引、商工三団体と連携した団体サイバー保険の販売などにより、中小企業へのサイバー保険普及を進めている。

情報セキュリティ保険市場



（出典）JNSA 2015年度情報セキュリティ市場調査報告書

サイバー保険の販売

損保ジャパン日本興亜　東京海上日動　三井住友海上 MS&AD INSURANCE GROUP

大手三社が販売

保険料割引

セキュリティ対策を実施していることを自己宣言した中小企業にSECRUTIY ACTIONマークを付与。マークを取得した企業の保険料を割引。

サイバー保険の付帯サービス

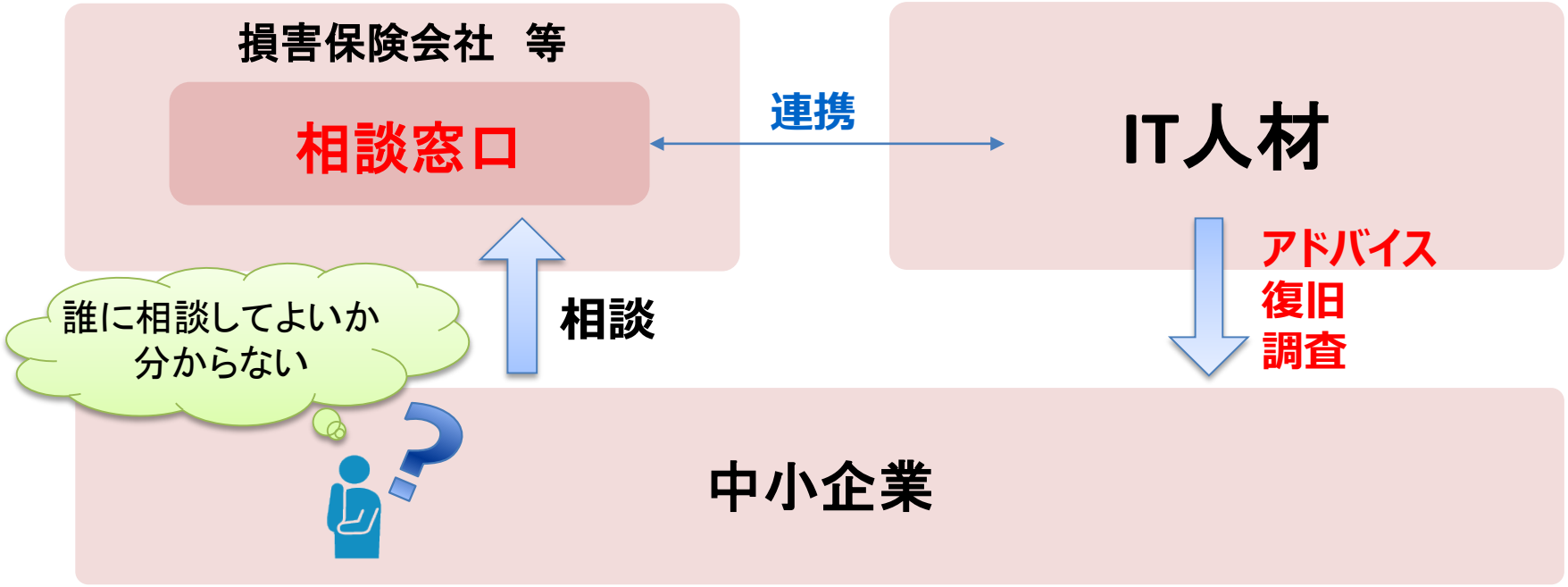
・サイバーリスクニュースやセミナーなど情報提供
・セキュリティ管理体制の簡易リスク診断
・サイバーリスクに関する教育支援ツール提供

商工三団体との連携

団体制度を活用したサイバー保険の販売による、
中小企業のサイバー保険販売促進

中小企業向けサイバーセキュリティ支援体制の整備

- 前述のベストプラクティスや可視化ツールによりセキュリティ対策を実施しても、サイバー攻撃による被害を100%防ぐのは困難。
- 特に中小企業については、事案発生したと思われる時に相談できる身近な窓口へのニーズが高い。
- このような相談窓口を整備し、サイバー保険やIT人材との連動も検討することにより、中小企業のセキュリティ強化を図ることが必要ではないか。



1．経営

2．人材

3．国際

（１）セキュリティ人材活用モデルの構築

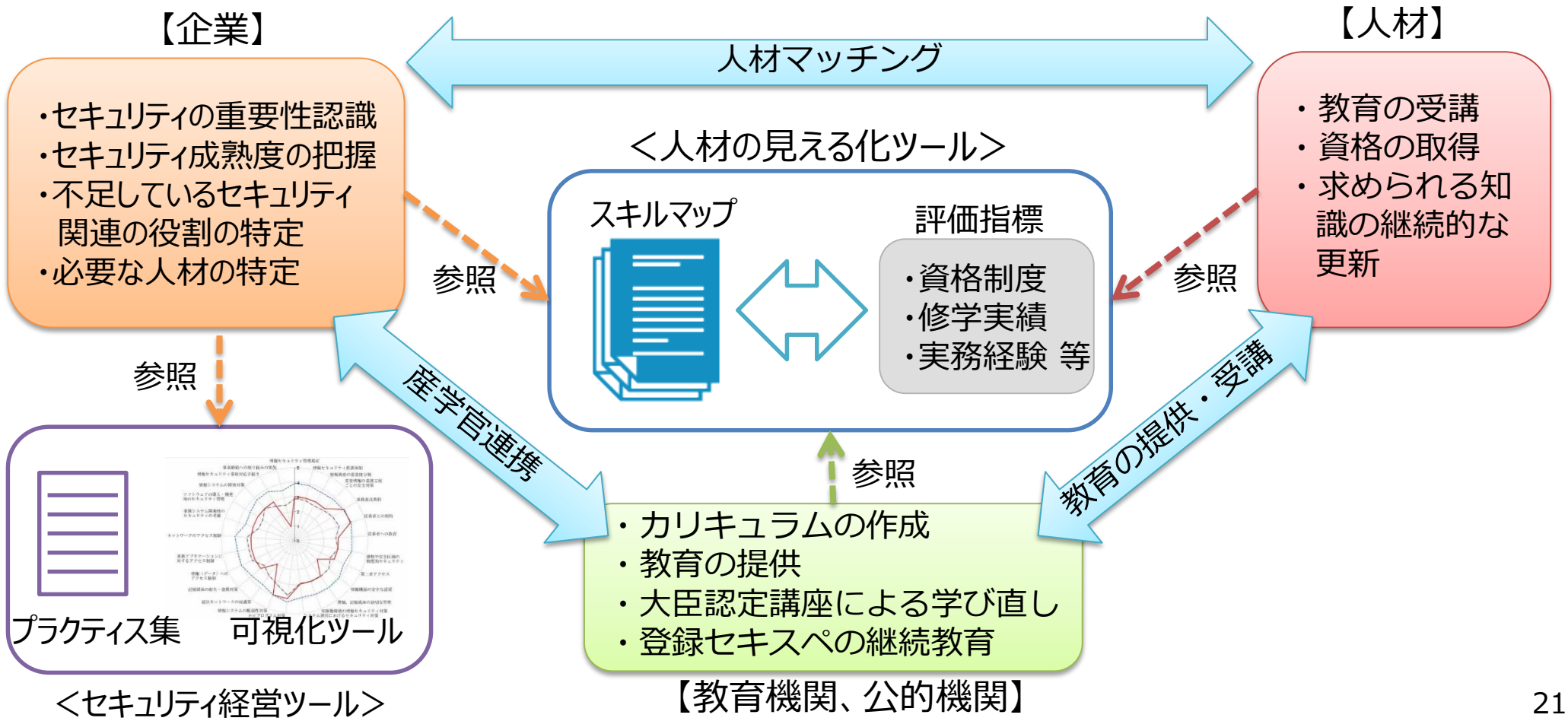
（２）戦略マネジメント層の育成

（３）リテラシー教育の強化

（４）産学官連携の促進

セキュリティ人材活用モデル

- 適切なサイバーセキュリティ経営の実現を目指す企業に求められるスキルを持つセキュリティ人材をマッチングするモデルの構築を目指す。
- これにより、ニーズの高いスキルを持つセキュリティ人材の最適な活用、処遇改善につなげ、流動化に対応できるセキュリティ人材市場を実現。



セキュリティ人材活用モデルの構築に向けた課題

- セキュリティ人材活用モデルの構築に向けては、以下のような課題があるのではないか。

採用までのプロセス（企業目線）	現実の状況・課題	想定される対策
経営者がサイバーセキュリティの重要性を認識	・経営者のサイバーセキュリティへの意識が低い	<経営者の意識喚起> ・サイバーセキュリティ経営GL ・CGSガイドライン ・取締役会実効性評価
自社に不足しているサイバーセキュリティ関連の役割の特定	・不足している役割が分からない ・セキュリティ経営の成熟度と人材雇用の関係が不明確	<自社の取組状況の可視化> ・ベストプラクティス集 ・セキュリティ対策可視化ツール ・人材戦略と成熟度の関係整理
自社に不足している役割を満たす人材のスキルの特定	・不足している役割を満たす人材のスキルが分からない	<役割とスキルのマッチング> ・役割毎のスキルマップの作成（既に複数のスキルマップが存在）
自社に不足しているスキルを満たす資格、修学実績、実務経験等を特定	・不足しているスキルを満たす資格、修学実績、実務経験等の基準が分からない	<スキルと指標のマッチング> ・スキルマップと資格、修学実績、実務経験等のマッチング
特定した資格等を保有する人材を労働市場から採用	・必要な人材が労働市場にいない	<スキルと人材のマッチング> ・スキルマップに応じた人材育成の強化 ・産学官連携の強化 ・キャリアパスの明確化

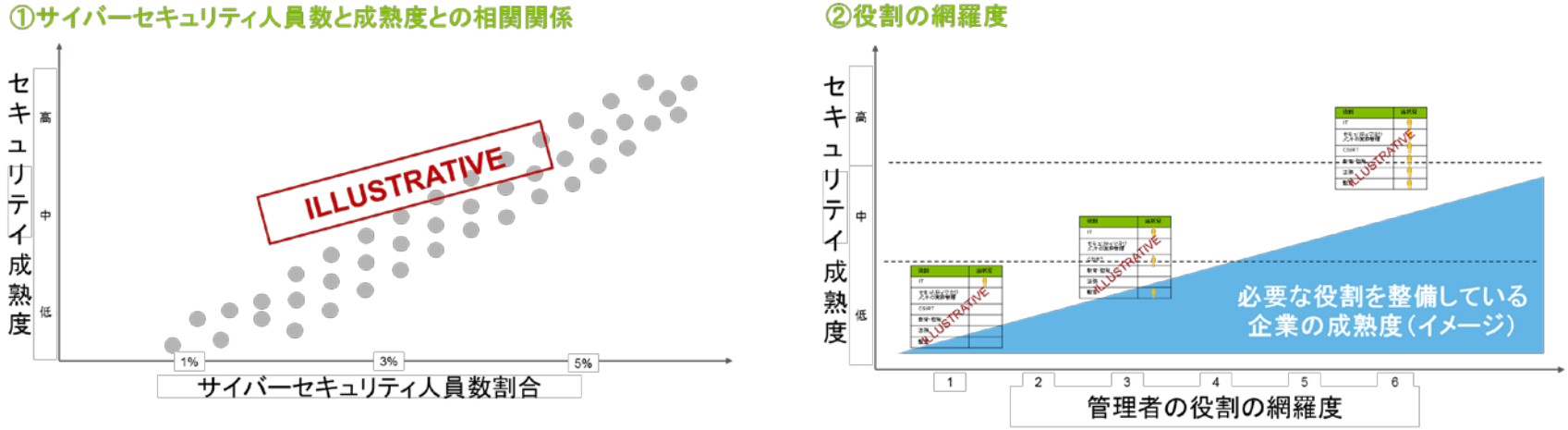
セキュリティ人材活用モデルの構築に向けた海外調査のねらい

- ①企業の人材戦略とセキュリティ経営成熟度の関係の考察、②人材のスキルマップと指標（資格、修学実績、実務経験）の関係整理を目的として、英米の状況調査を実施

①企業の人材戦略とセキュリティ経営成熟度の関係の考察

- セキュリティ担当人材の保有割合と成熟度のレベルには一定の関係があることが考えられる。
- セキュリティ関連事項のカバレッジの広さと成熟度のレベルには一定の関係があることが考えられる。

＜想定する仮説＞



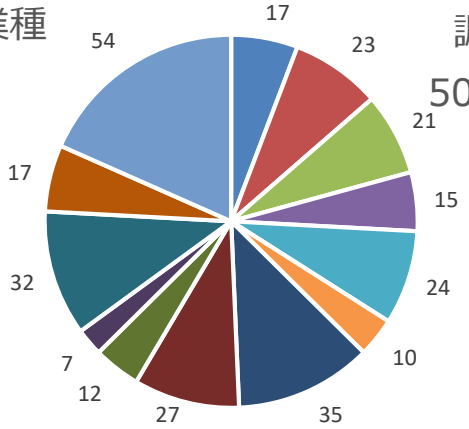
②人材のスキルマップと指標（資格、修学実績、実務経験）の関係整理

- 英米の企業が各役割の人材を雇用するに際して重視する指標を調査

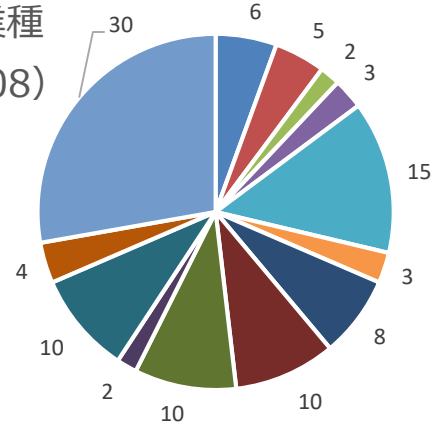
海外調査の概要

- 英米の企業500社程度に選択式アンケート調査を実施。有効回答は294社。
- 主な調査項目は以下のとおり。
  - サイバーセキュリティ関連人員数、セキュリティ成熟度（簡易なモデルによるもの）、サイバーセキュリティに関わる役職の設置状況、各役職を採用する際に重視する要素（資格、修学実績、実務経験）
  - なお、サイバーセキュリティに関わる役割については、産業横断サイバーセキュリティ人材育成検討会作成の「産業横断人材定義リファレンス」の定義に従った。

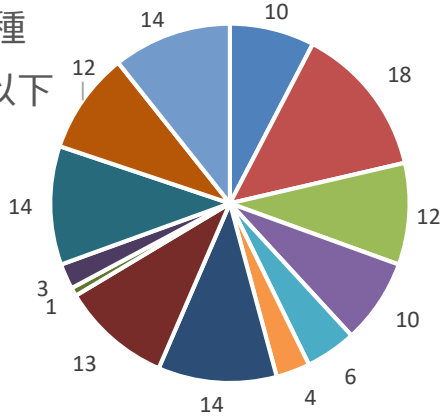
調査対象企業の業種
総数（n=294）



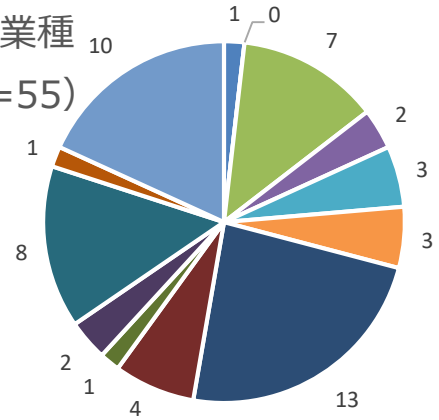
調査対象企業の業種
500名未満（n=108）

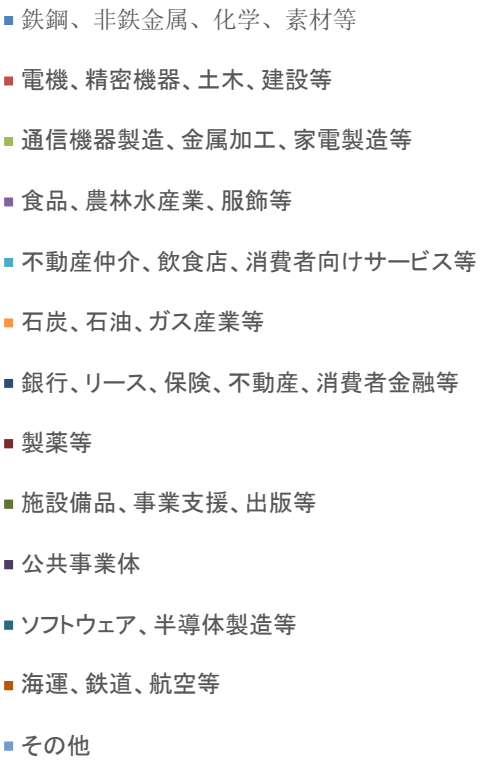


調査対象企業の業種
500名以上5000名以下
（n=131）



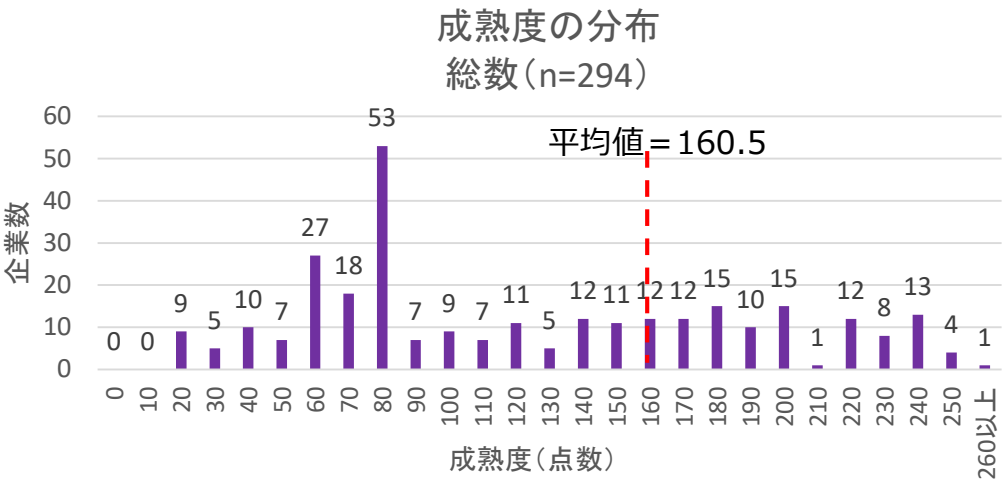
調査対象企業の業種
5001名以上（n=55）

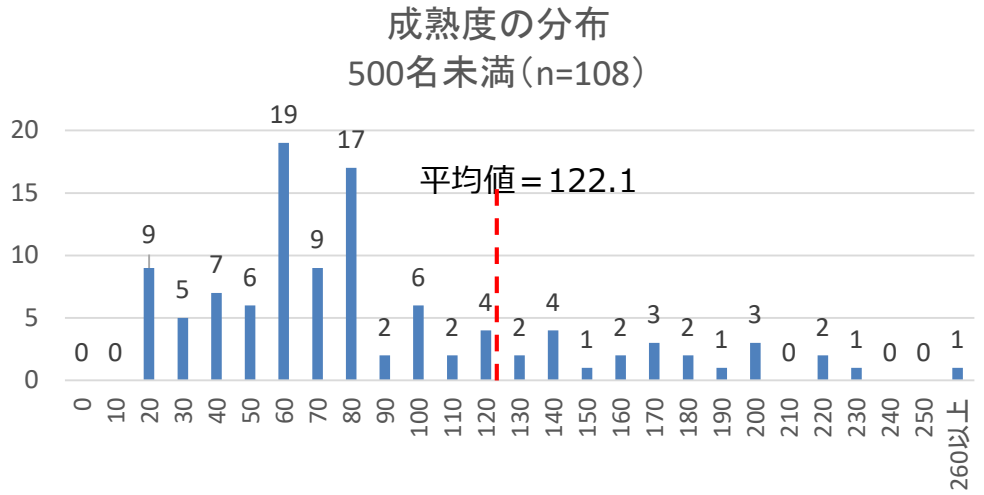


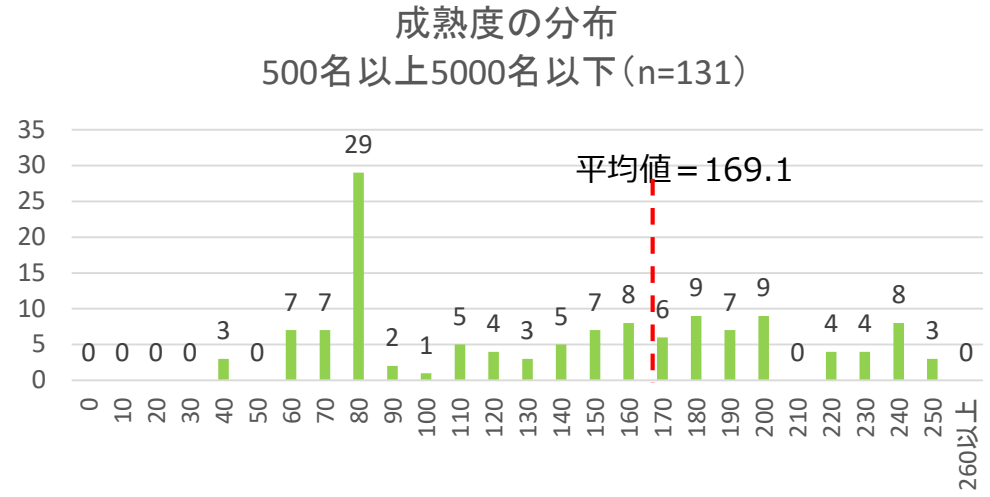


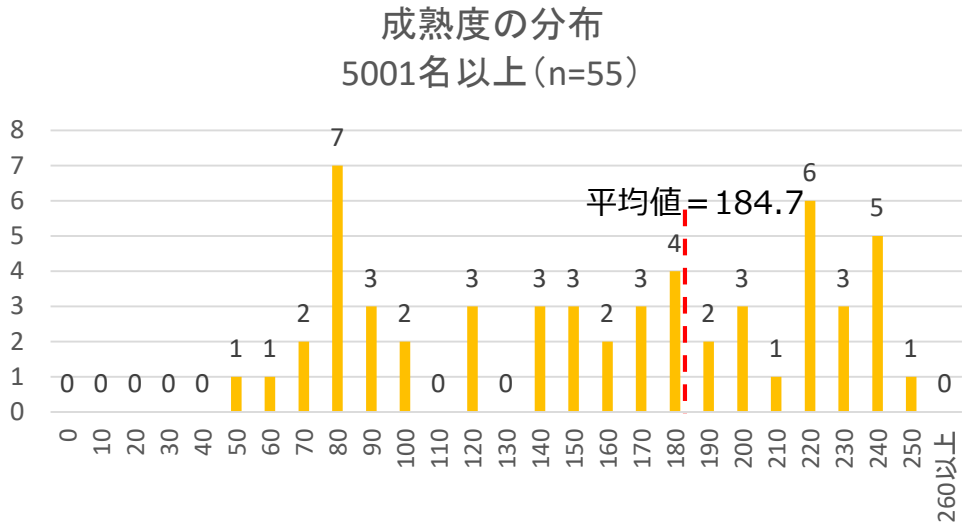
成熟度の分布状況

- 企業規模が大きいほど成熟度が高い傾向が見られる。



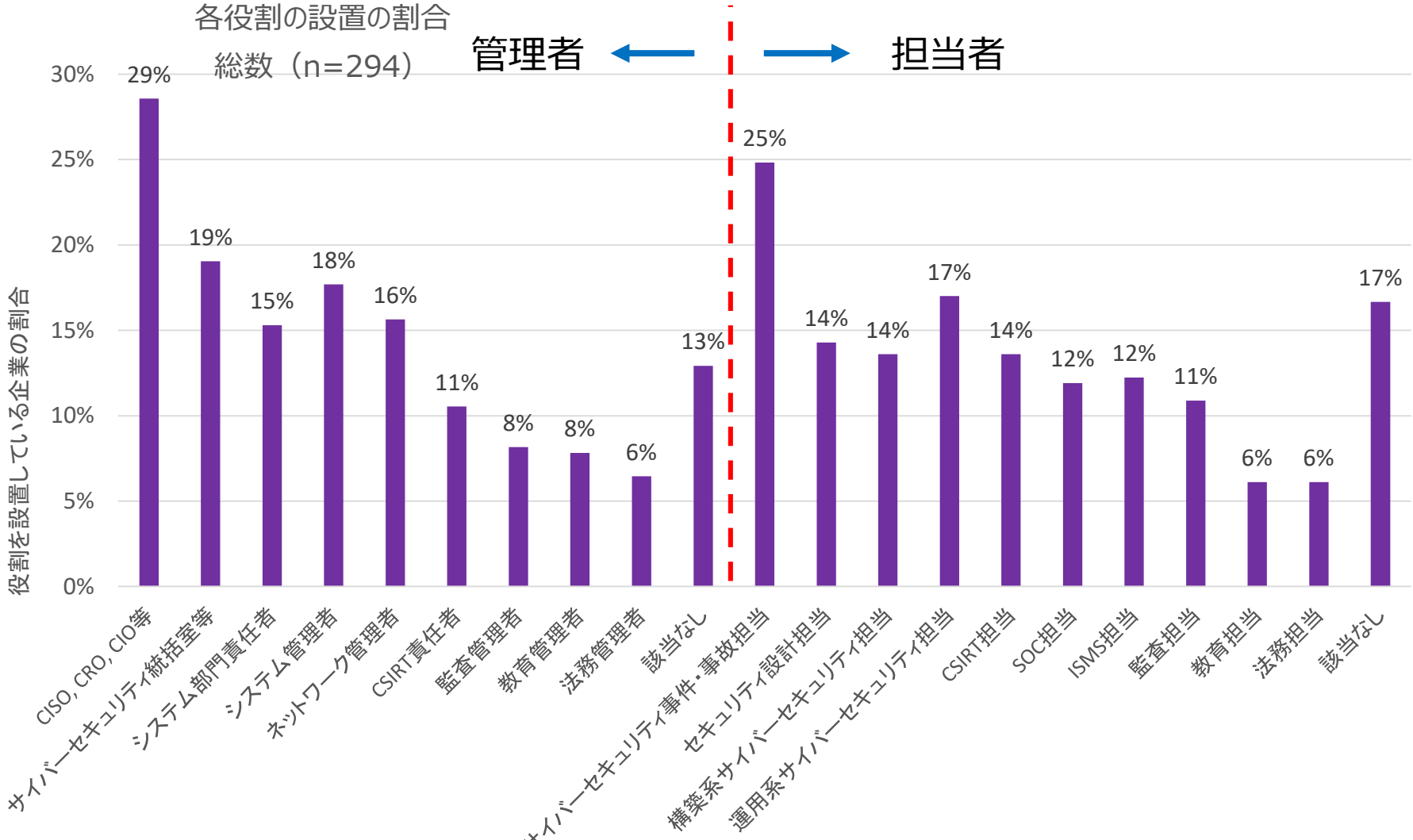




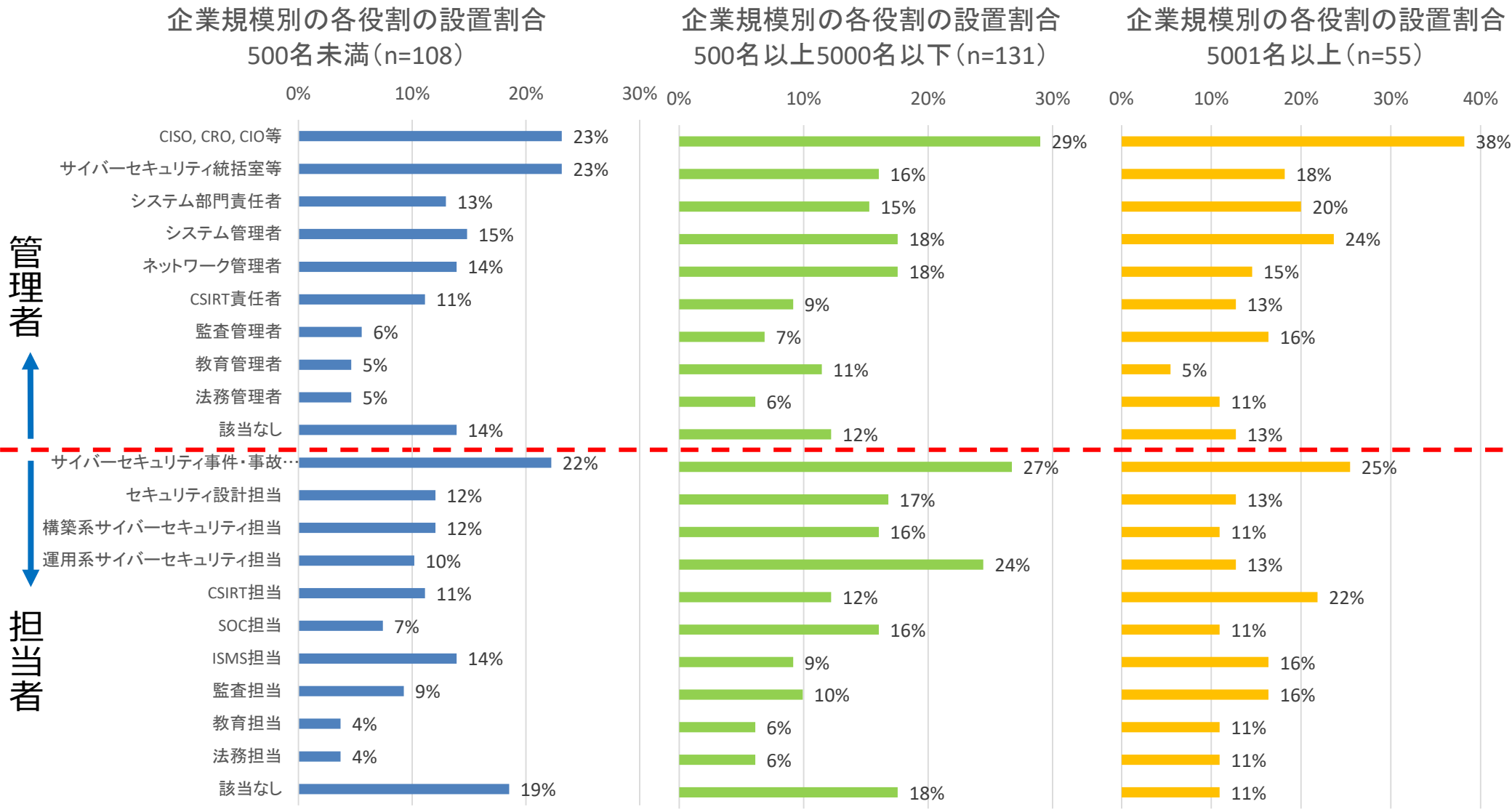


サイバーセキュリティ関連の役割の設置割合

- サイバーセキュリティ関連の役割については、産業横断サイバーセキュリティ人材育成検討会作成の「産業横断人材定義リファレンス」の１３種に、監査管理者、教育管理者、法務管理者、監査担当、教育担当、法務担当の６種を追加した計１９種で実施した。

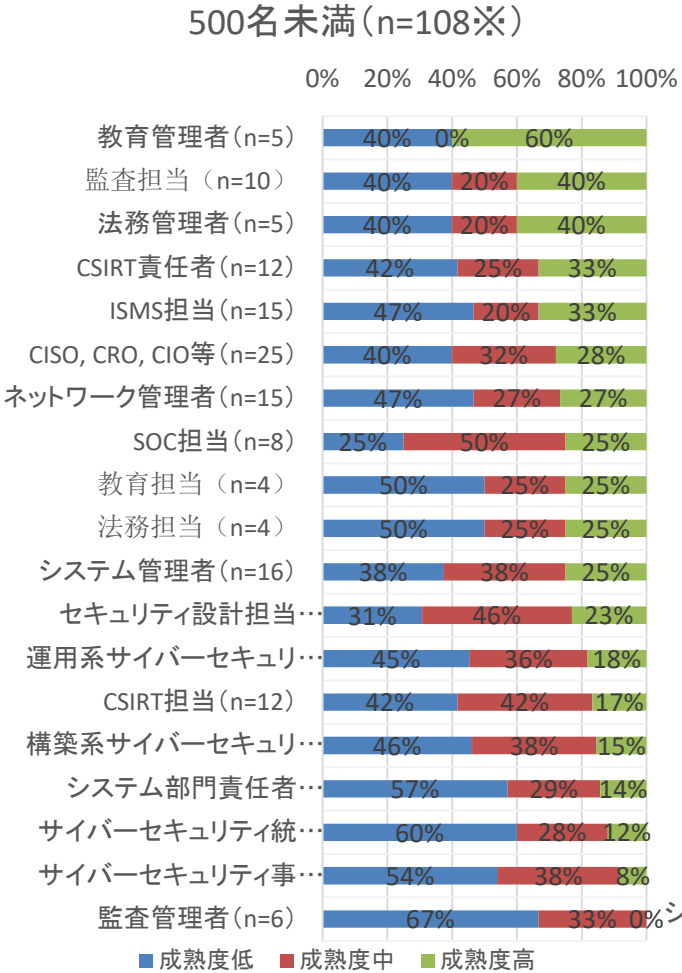


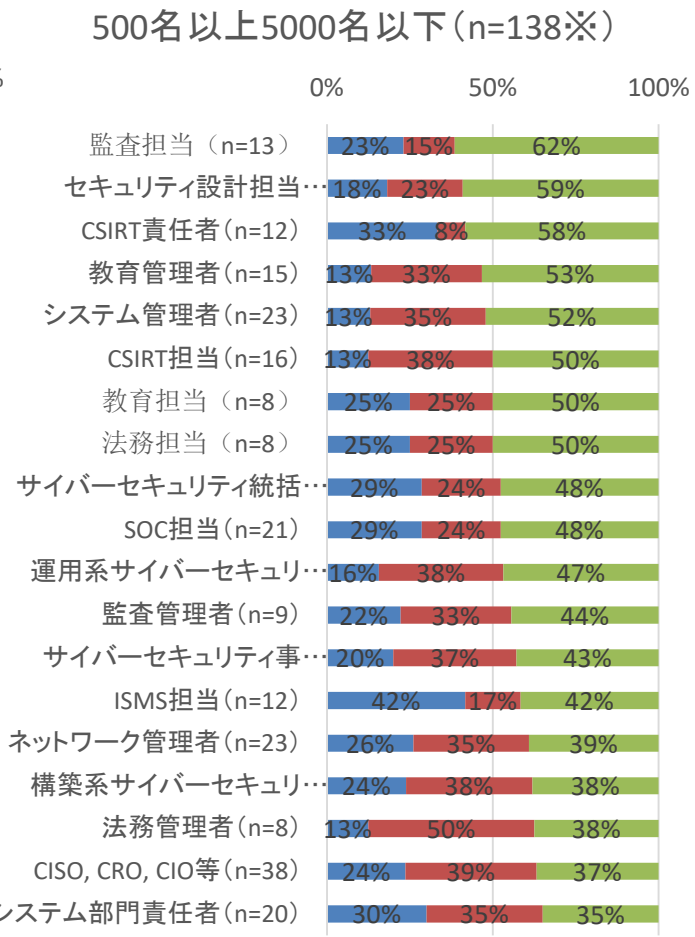
企業規模別の各役割の設置割合

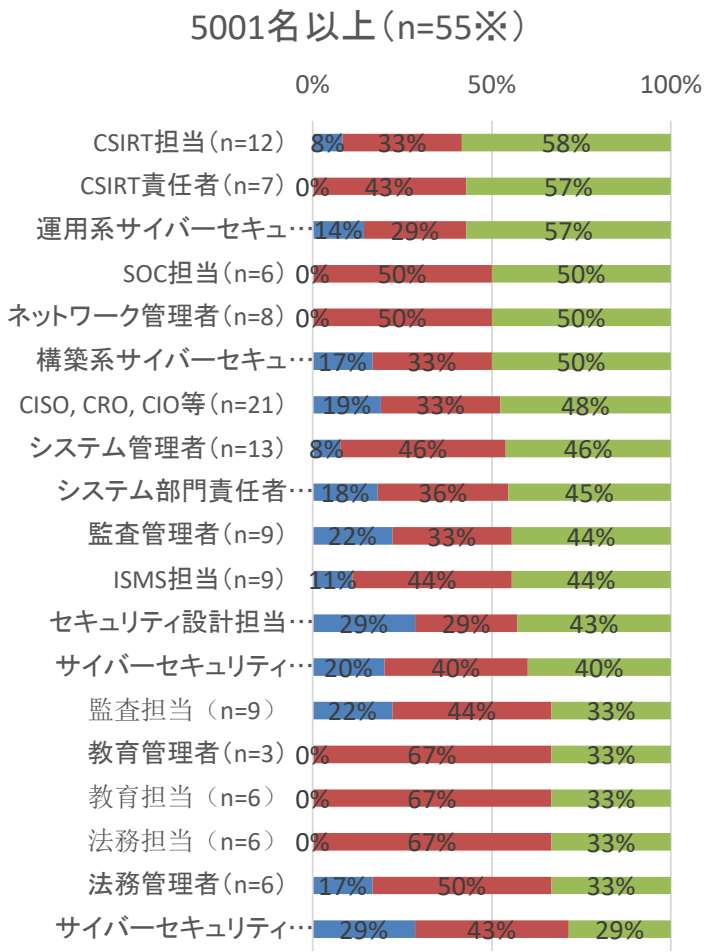


企業規模別の各役割の設置と成熟度の関係

- 小規模企業(500名未満)については、従業員への教育が成熟度の高度化につながっている可能性がある。
- 中規模企業(500-5000名)については、監査担当やセキュリティ設計担当などを設置し、セキュリティ体制の構築に取り組んでいることが成熟度の高度化につながっている可能性がある。
- 大規模企業(5001名以上)については、CSIRTやSOCなどのインシデント対応体制の構築が成熟度の高度化につながっている可能性がある。



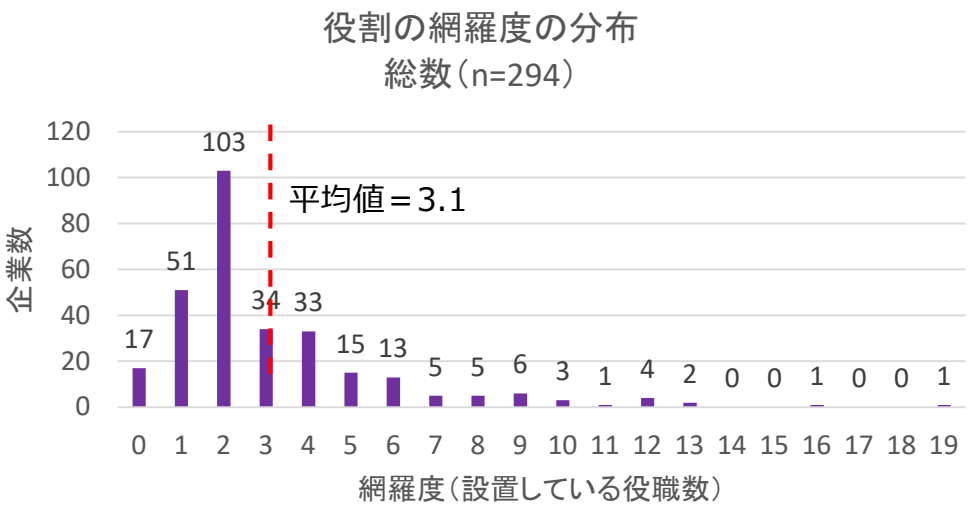


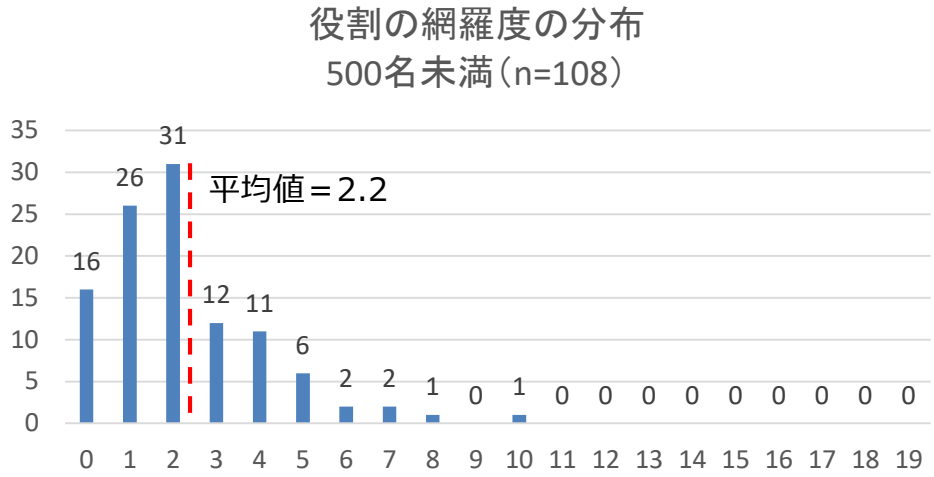


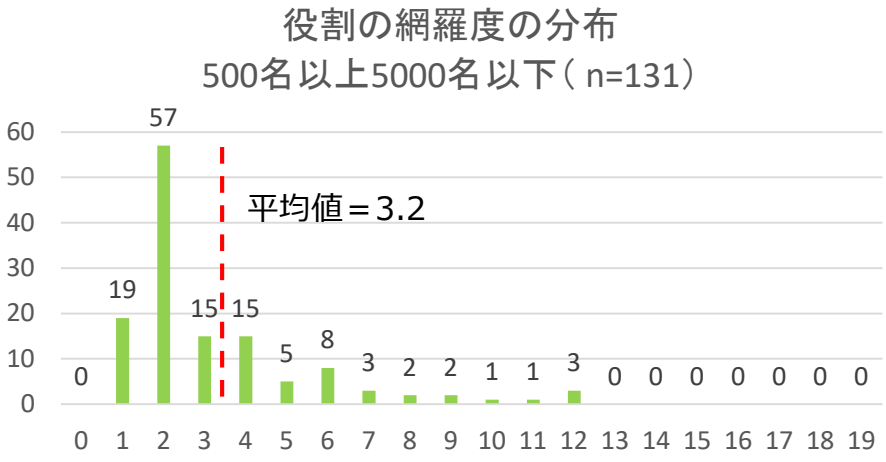
※複数回答可なので合計数は一致しない

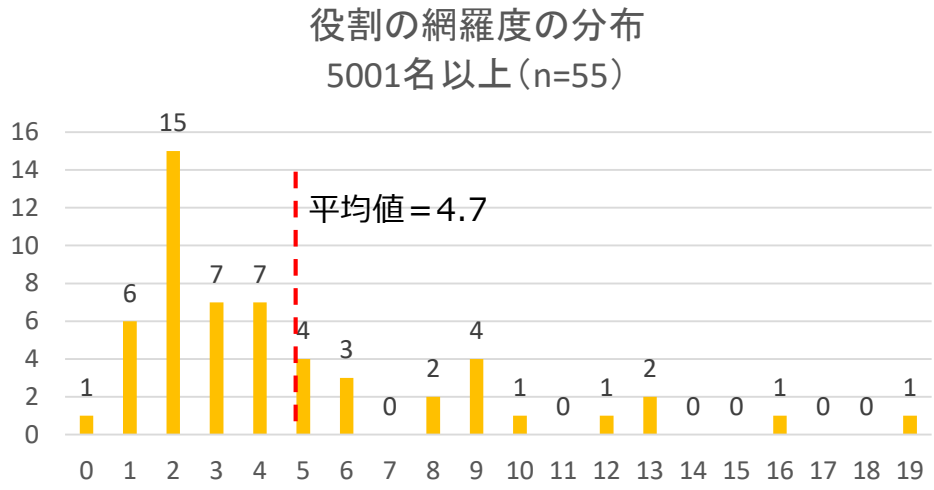
役割の網羅度（設置している役職数）

- 企業規模が大きいほど網羅度が高い傾向が見られる。



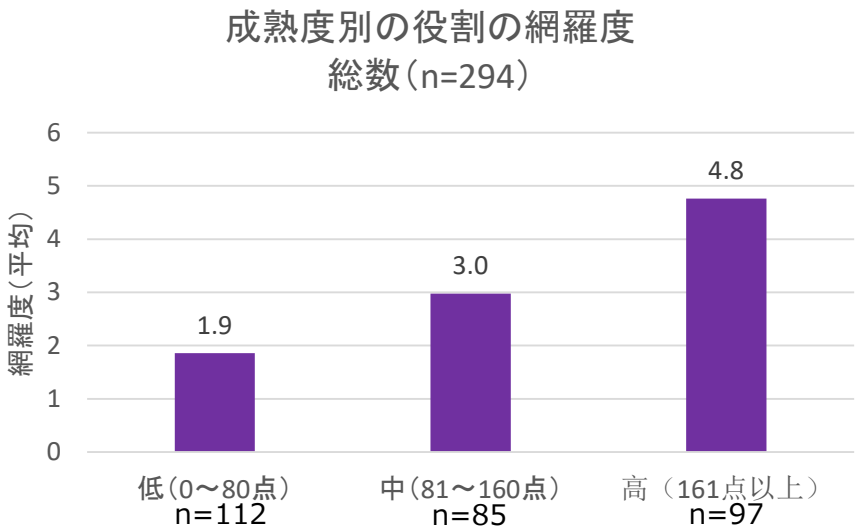


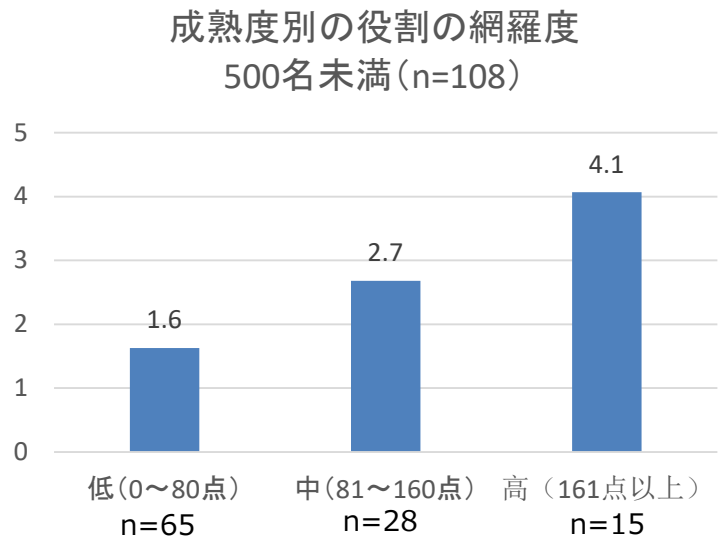


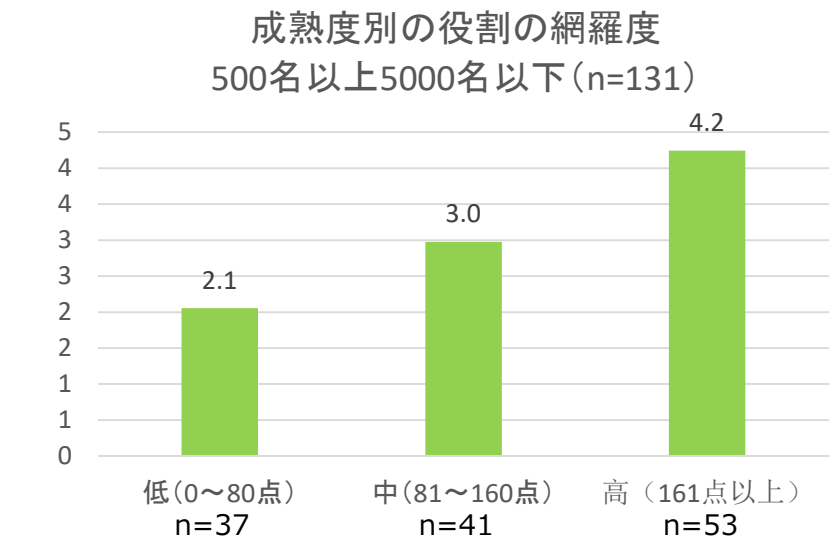


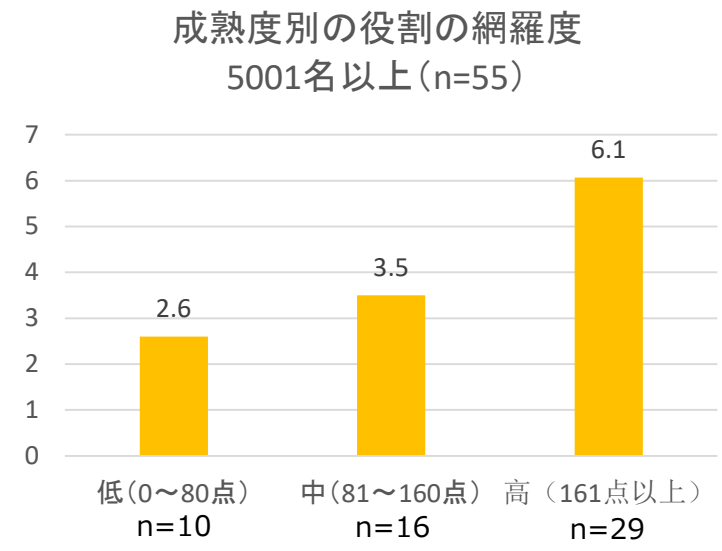
成熟度別の役割の網羅度

- 成熟度が高い企業ほど役割の網羅度が高い傾向が見られる。

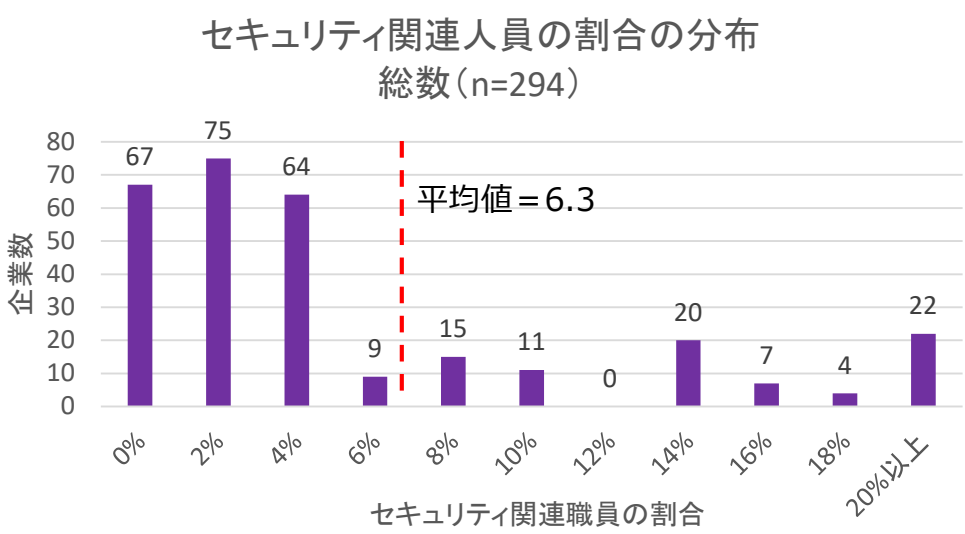


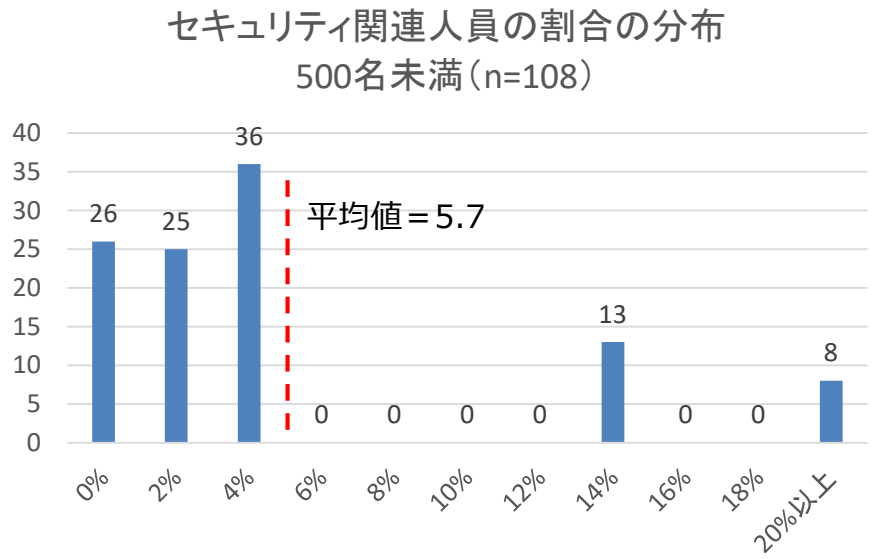


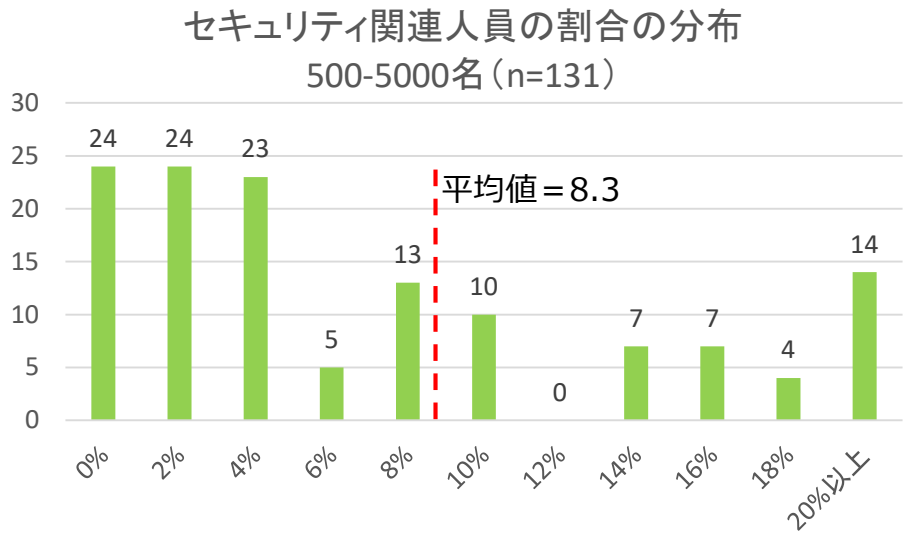


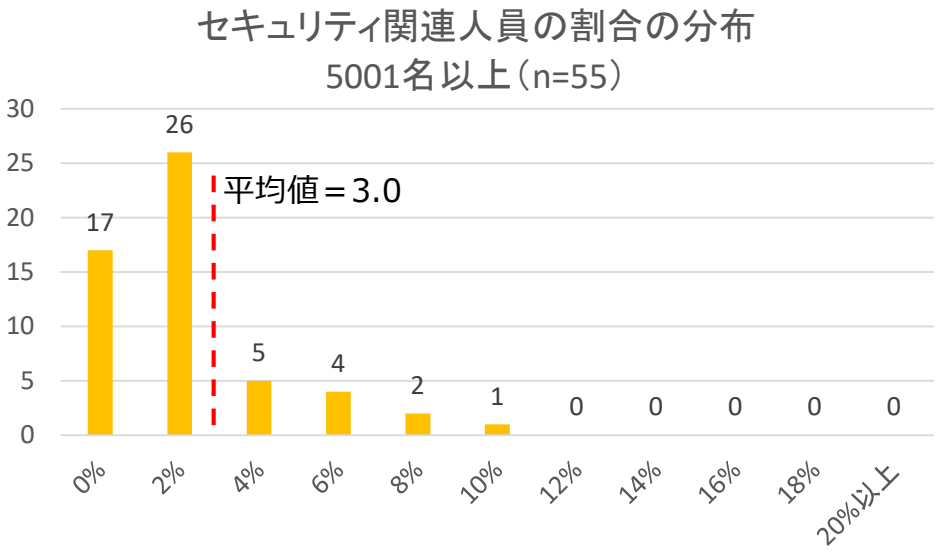


セキュリティ関連職員の割合



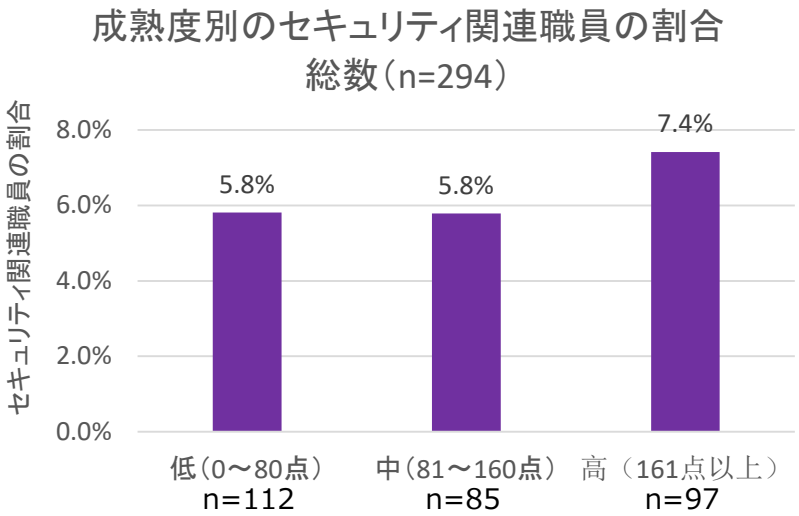


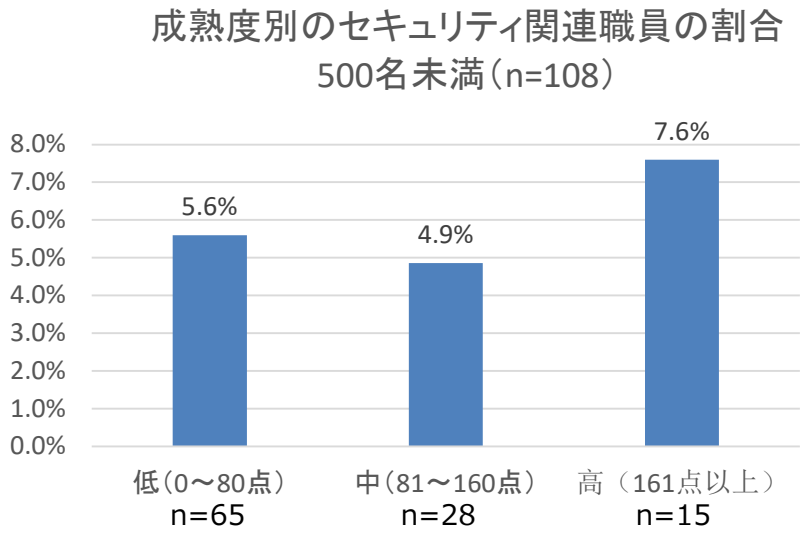


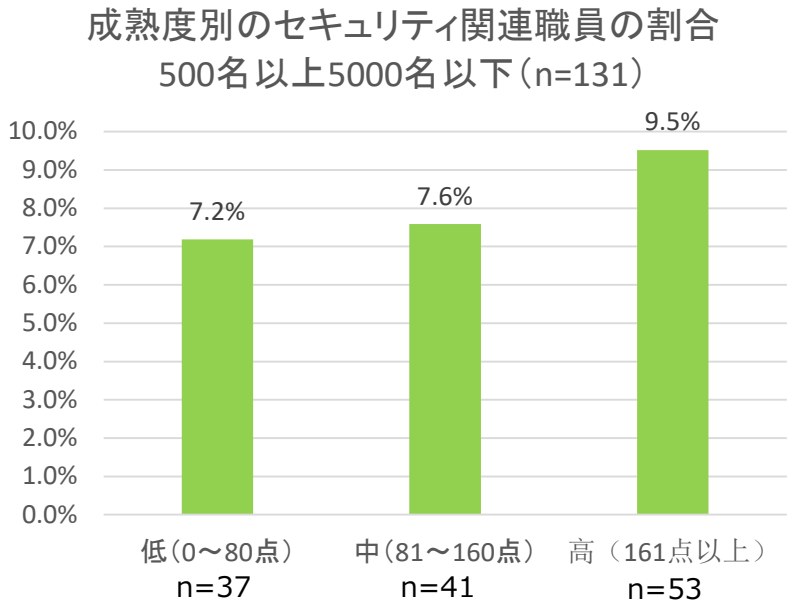


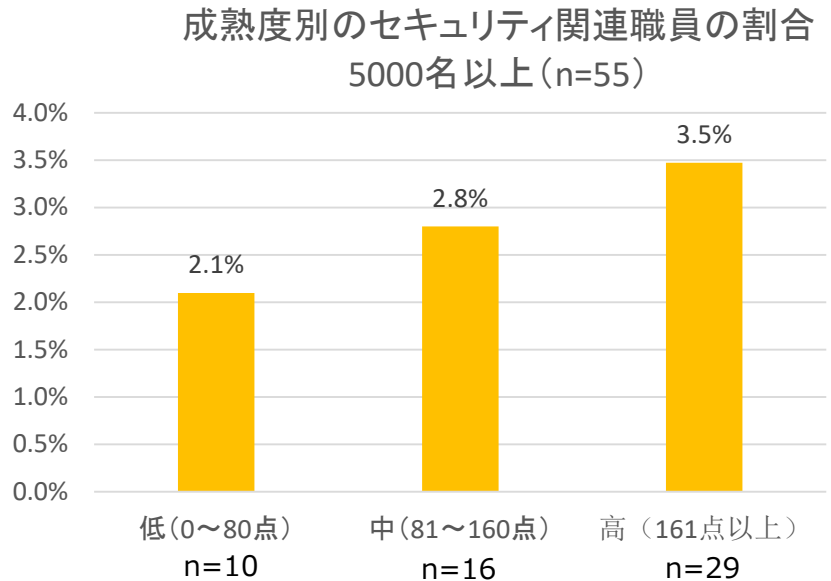
成熟度別のセキュリティ関連職員の割合

- 成熟度が高い企業ほどセキュリティ関連職員の割合が高い傾向が見られる。

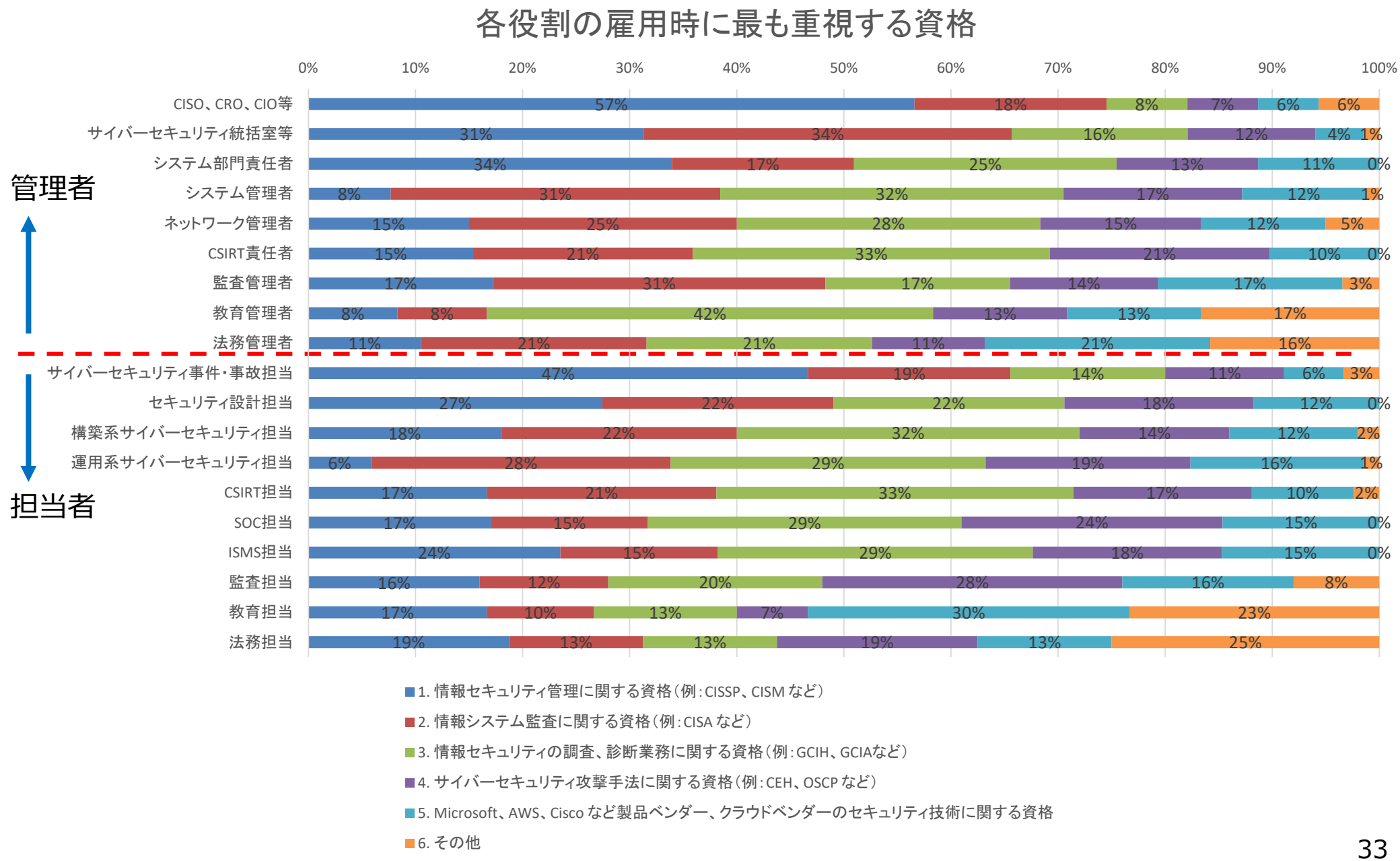




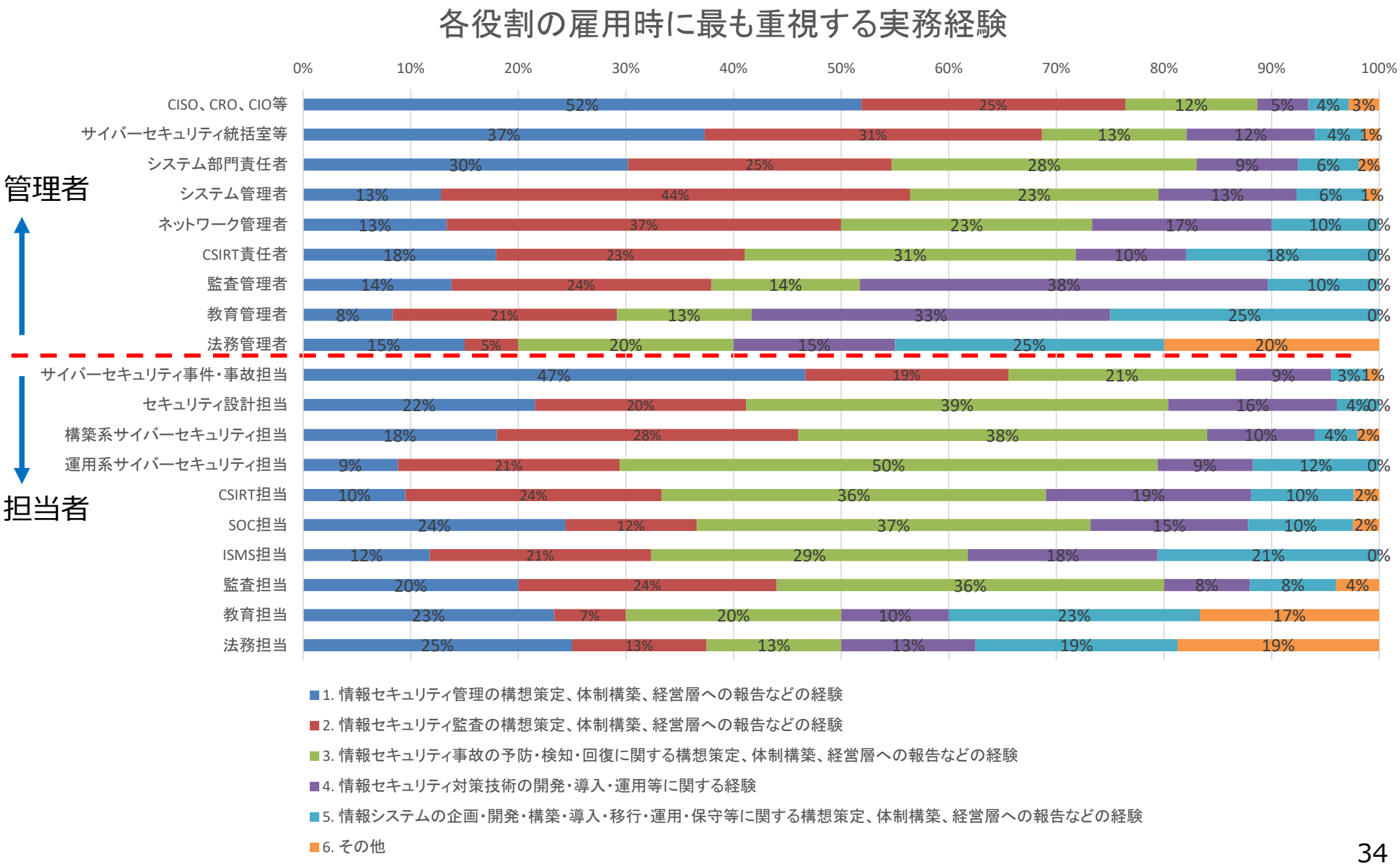




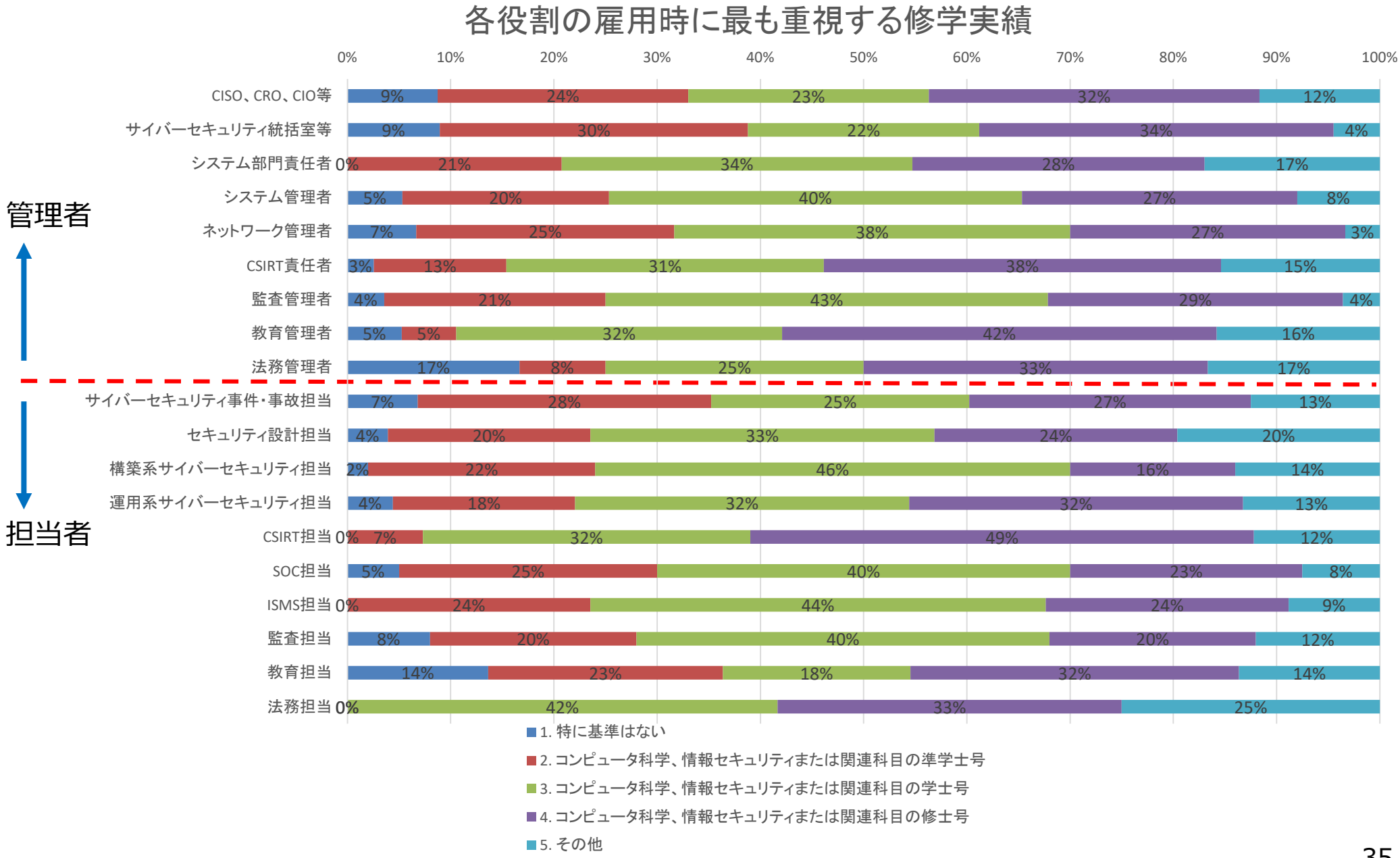
各役割を雇用するに際して重視する事項（資格）



各役割を雇用するに際して重視する事項（実務経験）



各役割を雇用するに際して重視する事項（修学実績）



企業の人材戦略とセキュリティ経営成熟度との関係に係る考察

＜役割の網羅度と成熟度との関係＞

- **成熟度の高い企業は網羅度が高い**傾向が見られた。

＜特定の役割の設置と成熟度との関係＞

- **小規模企業**については、**従業員への教育が成熟度の高度化**につながっている可能性。
- **中規模企業**については、監査担当やセキュリティ設計担当などを設置し、**セキュリティ体制の構築に取り組んでいることが成熟度の高度化**につながっている可能性。
- **大規模企業**については、CSIRTやSOCなどの**インシデント対応体制の構築が成熟度の高度化**につながっている可能性。
- セキュリティ人材活用モデルの構築に向けては、企業規模別・業種別等の更なる分析によって特定の役割の設置と成熟度の相関関係を把握することが必要。

＜セキュリティ関連職員の割合と成熟度との関係＞

- **成熟度の高い企業はセキュリティ関連職員の割合が高い**傾向が見られた。

（１）セキュリティ人材活用モデルの構築

（２）戦略マネジメント層の育成

（３）リテラシー教育の強化

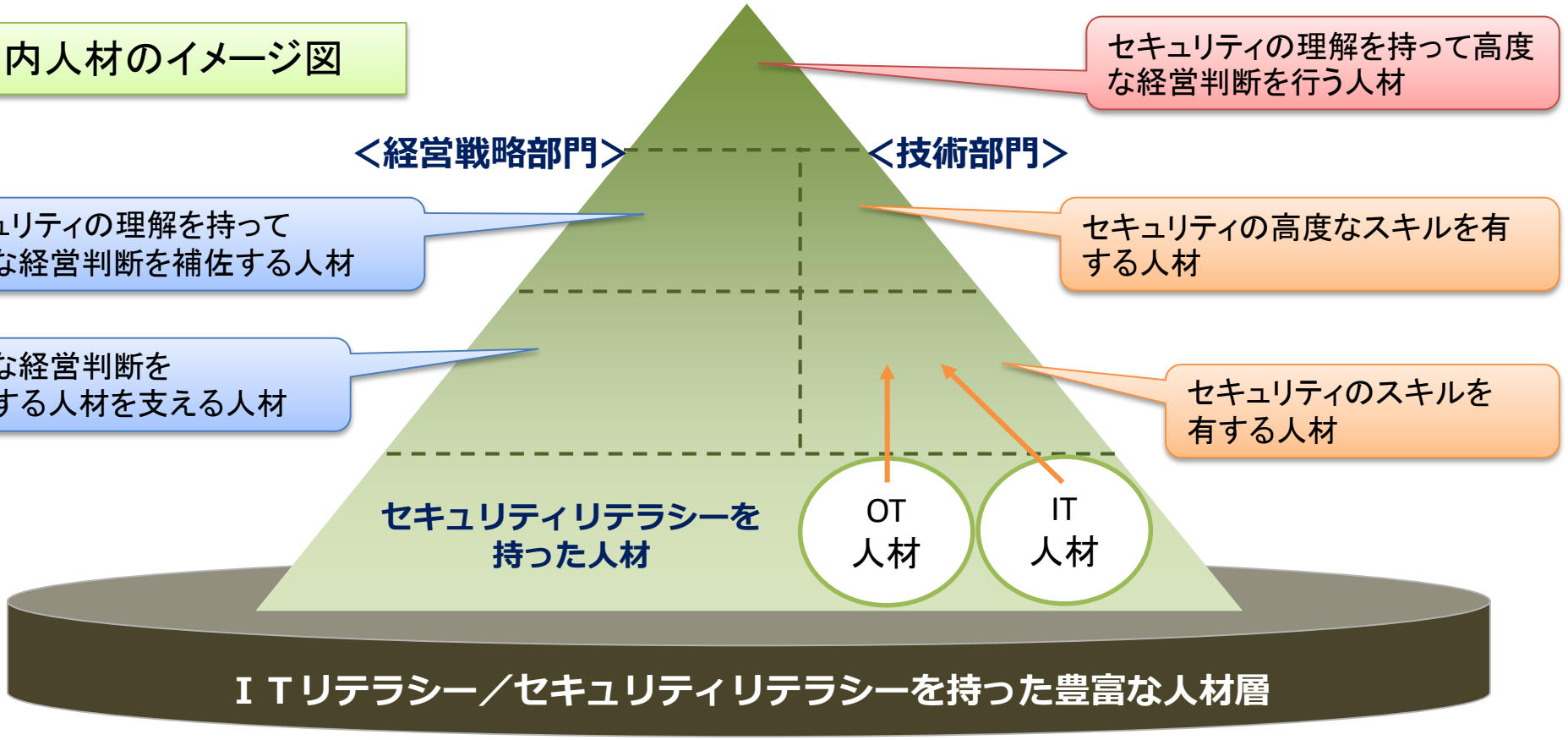
（４）産学官連携の促進

戦略マネジメント層の育成

- 第１回WGにおいては、セキュリティの理解を持って高度な経営判断を補佐する人材の育成が不足しているとの意見があった。
- NISCにおいて実施している「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」においては、「戦略マネジメント層」としてその育成の必要性を強調。

＜第１回WG２資料より抜粋

企業内人材のイメージ図



デジタル化時代における経営人材の育成

- 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し、2018年秋よりプログラムを開始予定。
- プログラムの中に、経営視点で見たサイバーセキュリティ対策について考える契機とするための講義も実施予定。

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 スキル・ノウハウ	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
カリキュラム	経営戦略・知識経営等のコアコース 世界の先進的IT戦略の集中講義 **サイバーセキュリティ・個人情報保護等の講義** デジタル経営の特別講義
期間	2018年秋～

戦略マネジメント人材の育成（産業サイバーセキュリティセンター）

- IPA産業サイバーセキュリティセンターにおいて、幅広いバックグラウンドや実務経験を持つ受講者を対象に、CISOや戦略マネジメント機能を担う人材に必要なセキュリティ対策に関するトレーニングを行うプログラムを2018年秋から開始。
- プログラムの内容については、NISCが「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」において取りまとめているモデルカリキュラム等も踏まえつつ検討。
- 具体的には、CISOや経営層が遭遇する困難な事例を材料とするケーススタディ演習の形式で実施することを検討中。

対象	• 各業界、各社において今後セキュリティ対策の中核を担うことが期待される方（同センター「中核人材育成プログラム」の受講者） • 現在CISOやその補佐として、セキュリティ対策についての経営層への直接の助言や意思決定を行う立場にある方
身につけるスキル・ノウハウ	• サイバーセキュリティに関するコミュニケーションや調整、実施体制とその運営に必要な知識・スキル • サイバーセキュリティリスクへの対応策（技術的な対応策、マネジメントによる対応策、それを提供する事業者を含む）に関する知識・スキル • サイバーセキュリティインシデントに関わる緊急時対応　等
期間	2018年11月～2019年1月頃にかけて数回にわたって実施（予定）

（１）セキュリティ人材活用モデルの構築

（２）戦略マネジメント層の育成

（３）リテラシー教育の強化

（４）産学官連携の促進

リテラシー教育の拡充（インターネット安全教室の拡張）

- 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）を学習するセミナー「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。
- 座間市の事件を踏まえ、教育内容の充実、教育対象の拡充を実施

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

＜2月＞
教育現場のニーズを調査・分析し、
**SNSに関する内容を含む
講師用トレーニング教材を作成**

＜5月＞
講師トレーニングを実施

＜6月以降＞
教育委員会への講師派遣

（１）セキュリティ人材活用モデルの構築

（２）戦略マネジメント層の育成

（３）リテラシー教育の強化

（４）産学官連携の促進

セキュリティ人材育成における課題

- セキュリティ人材の育成に関して、それぞれの主体が以下のような問題意識・課題を抱えているのではないか。

・スキルマップに沿った人材育成が不十分
・修学実績とスキルマップの関係が不明確

【企業】

・セキュリティ人材のキャリアパスが不明確
・セキュリティ教育を受ける機会が不足

【人材】

・スキルマップを参照しても教育カリキュラムの作成は困難
・企業のOJTで教育すべき部分と、学が担うべき部分の役割分担が不明確
・セキュリティ教育を行うことのできる人材が不足

【教育機関、公的機関】

産学官連携の強化

- 産学官の共通認識醸成、連携の強化に向けて、産業界、学術界などが中心となって以下のような事項を具体的に検討し、産学官連携強化の具体化を図ることが必要。

	問題意識・課題（例）	産学官連携により検討が必要なメニュー（例）
企業	・スキルマップに沿った人材育成が不十分	・産学官の役割分担の整理
	・修学実績とスキルマップの関係が不明確	・学として育成する人材像の明確化、スキルマップとの関係整理
教育機関	・スキルマップを参照しても教育カリキュラムの作成は困難	・教育カリキュラム策定を見据えたスキルマップの簡素化
	・企業のOJTで教育すべき部分と、学が担うべき部分の役割分担が不明確	・学として育成する人材像の明確化 ・産としての人材育成方針の検討 ・スキルマップとの関係整理
	・セキュリティ教育を行うことのできる人材が不足	・産業界、公的機関による高専、大学の“先生”のトレーニング ・高専、大学に対する講師派遣 ・シニア人材プールの検討
人材	・セキュリティ人材のキャリアパスが不明確	・産・学のマッチング強化
	・セキュリティ教育を受ける機会が不足	・産業界による寄附講座開設 ・IPA等の公的機関の教育カリキュラム、設備利用 ・大臣認定講座による学び直し

１．経営

２．人材

３．国際

マルチ・バイを通じた国際協調への取り組み

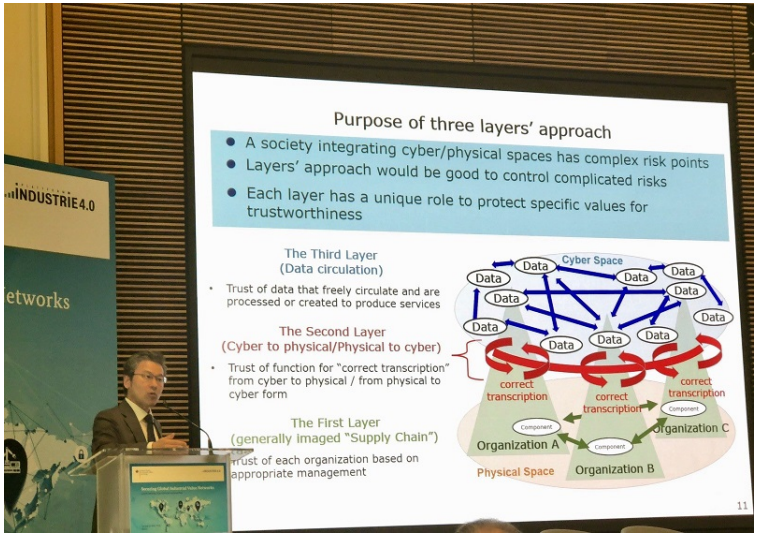
- パブリックコメントを実施中（日本語・英語両方）の**「サイバー・フィジカル・セキュリティ対策フレームワーク」**を軸に、各国のステークホルダーと議論、マルチの会議で紹介し、サイバー・フィジカル・セキュリティに関する共通の認識を醸成。
- **安全なサプライチェーンの実現**には関係する者の信頼性の確保について、各国と意見交換。

【ドイツ】

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

➢ ドイツを中心とした各国の官民の関係者にむけて、Society5.0時代のサイバーセキュリティについてフレームワークや標準化活動等、日本の取組を説明。

➢ 日独連携の取組の成果として、2017年に引き続き2018年5月に産業サイバーセキュリティに関する共同ポジションペーパーを発出。カンファレンスの講演内で日独双方から披露・解説。



マルチ・バイを通じた国際協調への取り組み

【EU・OECD】

- **<u>日EUデータエコノミー対話 政府間会合（2018年4月@東京）</u>**

➢ EUでサイバーセキュリティを所掌する通信総局（DG CONNECT）へフレームワークを紹介。
日欧は協調してセキュリティに関する国際的なルール構築に当たっていくとの認識を共有。

- **<u>OECD／CDEP（デジタル経済政策委員会）会合（2018年5月@パリ）</u>**

➢ セキュリティ・プライバシーに関する作業部会（SPDE）にてフレームワークを紹介。

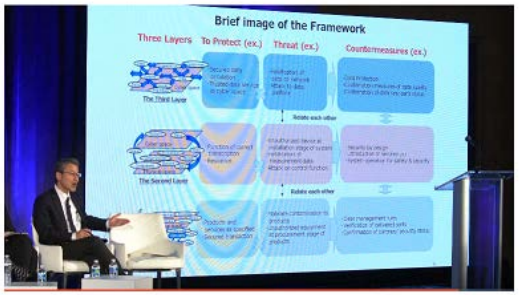
【APEC】

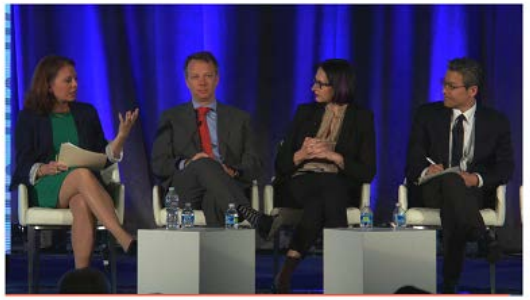
➢ APEC TEL57（第57回電気通信・情報作業部会）に際して、フレームワークを紹介（予定）。

【アメリカ】

- **TecGlobal （米国商工会議所主催）（2018年４月@ワシントン）**

➢ 国土安全保障省、アメリカ民間企業等に、現在日本で検討を進めているフレームワークについて、基本的な考え方や検討状況を共有し、お互いのサイバーセキュリティの取組を協調しながら進めていく環境を整備。



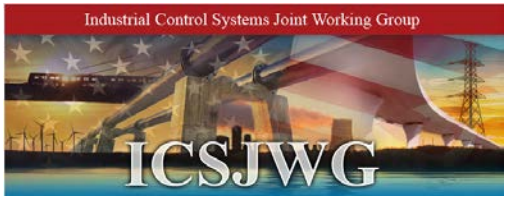


米国商工会議所のHPより引用

- **Industrial Control Systems Joint Working Group (ICSJWG)**

（2018年４月@アルバカーキ）

➢ 米国国土安全保障省(DHS）傘下の国家サイバーセキュリティ通信総合センター（NCCIC）が、重要インフラ防護に向けて官民関係者の連携を深めるべく、関係者で情報共有を図る会議において「サイバー・フィジカル・セキュリティ対策フレームワーク」を初めとする経産省のサイバーセキュリティ政策について紹介。



【ASEAN】

- **第2回日・ASEANサイバーセキュリティWG（2018年５月@インドネシア・バリ）**

➢ 情報セキュリティ分野において、我が国とASEAN諸国との国際的な連携・取組を強化することを目指す会議において、日本のサプライチェーンセキュリティの取組、フレームワークについて紹介。域内の情報セキュリティ水準向上のための意識啓発を実施。

➢ 日米共同演習（次ページ参照）への参加を呼びかけ。

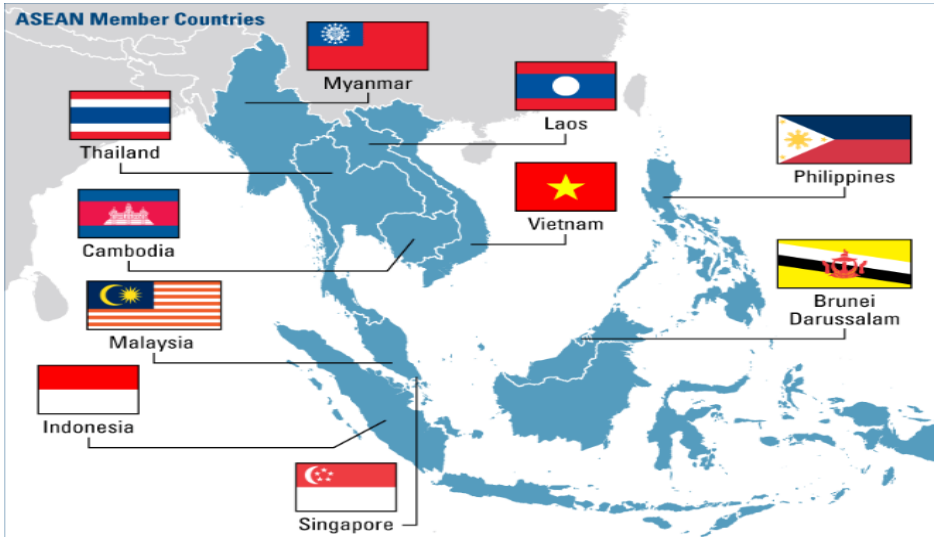
日米でASEAN等へのアウトリーチ

- ASEAN等アジア太平洋地域の各国に対して、日米が共同で、**産業分野におけるサイバーセキュリティ演習を継続的に実施**することを合意（2018年4月）

- **日米共同演習　（毎年9月に東京で開催）**

➢ 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。

➢ DHS/ICS-CERTの協力を得ながら、日本独自の演習カリキュラムを策定。



- **301演習への派遣　（毎年２月にアイダホ国立研究所に派遣）**

➢ ICS-CERTが実施する301演習（Blue&Red)の受講枠を確保。

➢ ICSCoEの優秀な生徒をアイダホ国立研究所（INL)に派遣し、301演習を受講。