NRIセキュアテクノロジーズ

第251回NRIメディアフォーラム：2017年3月28日(火)

企業における情報セキュリティ実態調査2017

～経営者が主導する組織横断的なセキュリティ施策が必須の時代へ～

Share the Next Values!

2017年3月28日

NRIセキュアテクノロジーズ株式会社
コンサルティング事業本部
ストラテジーコンサルティング部

セキュリティコンサルタント 金子 洋平

セキュリティコンサルタント 山本 直実

〒100-0004
東京都千代田区大手町1-7-2 東京サンケイビル

目次

1.調査概要

国内調査：2002年の開始以来、15年連続で調査を実施

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

回答数(回収率)

671社(22.4%)　※参考：昨年度 665社(22.2%)

国際比較調査：本年度より情報セキュリティ実態の国際比較調査を開始

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

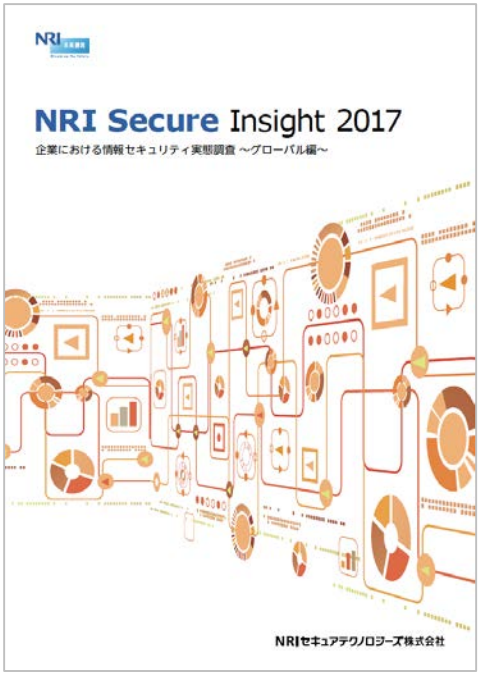
Webによるアンケート

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

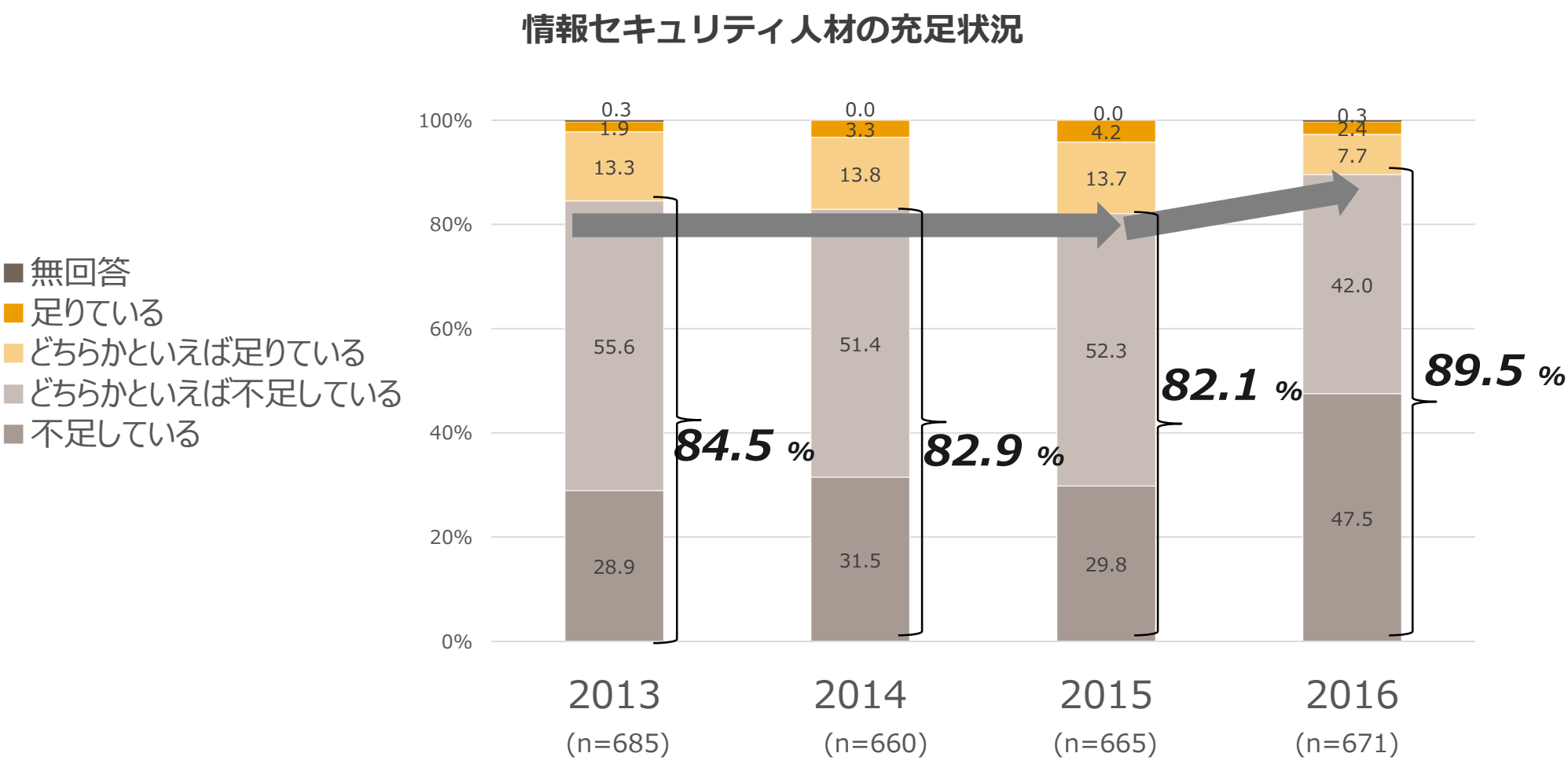
回答社数

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



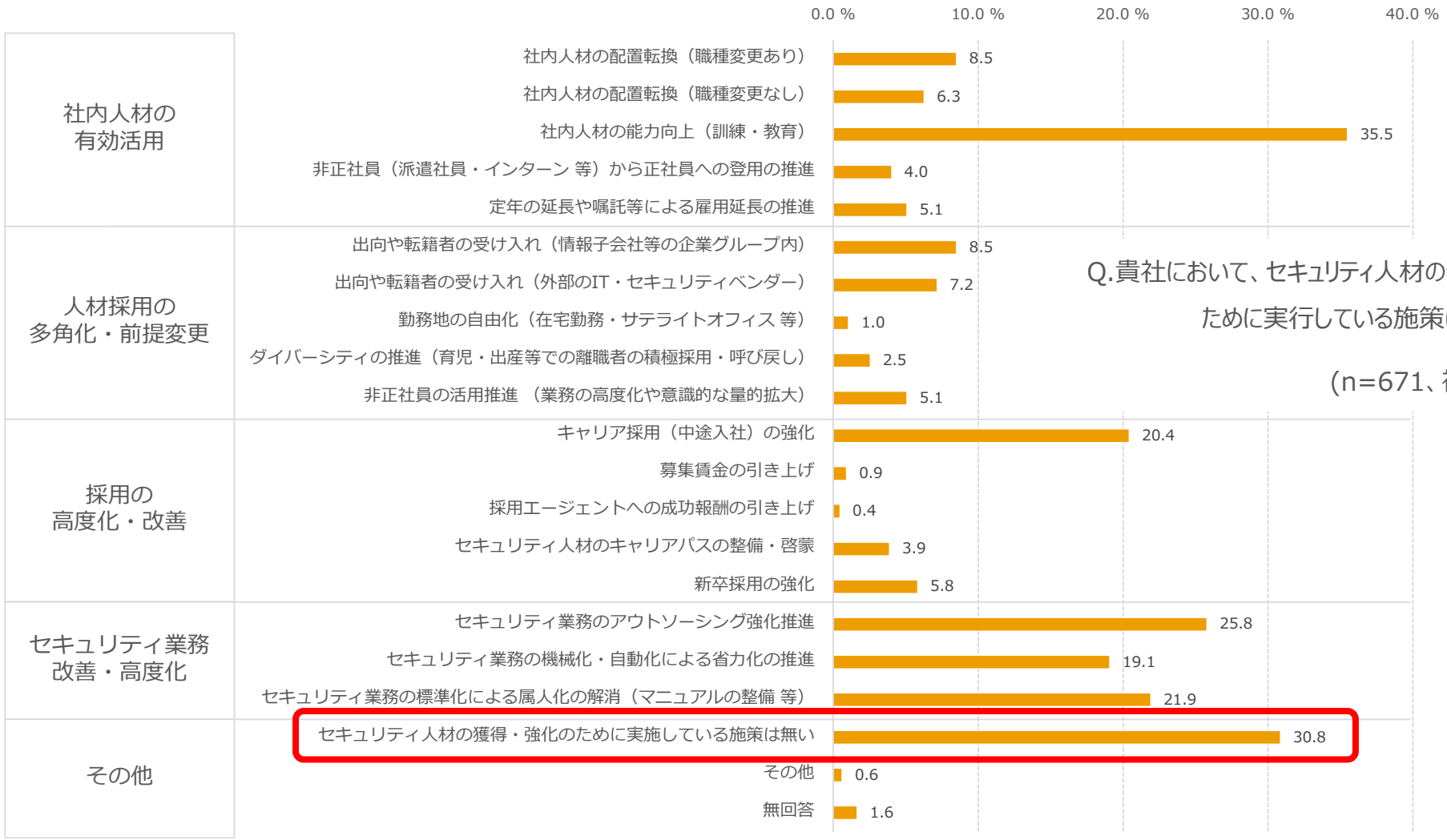
2.本年度のポイント　-国内調査-

セキュリティ人材の不足傾向がより顕著に



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獲得強化施策は3割の企業で未実施。
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

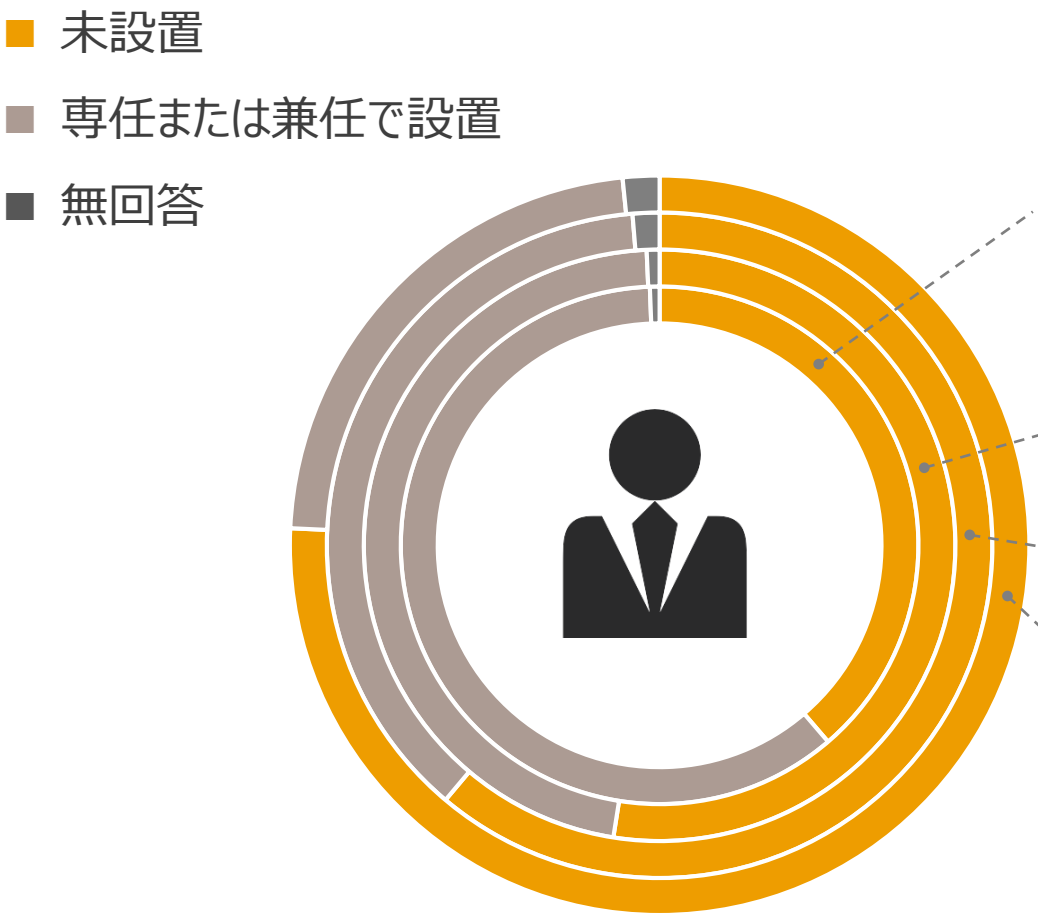


Q.貴社において、セキュリティ人材の獲得・強化のために実行している施策はありますか。

(n=671、複数回答)

国内調査_01　セキュリティ人材

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



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 %

CRO（最高リスク責任者）
61.1 %

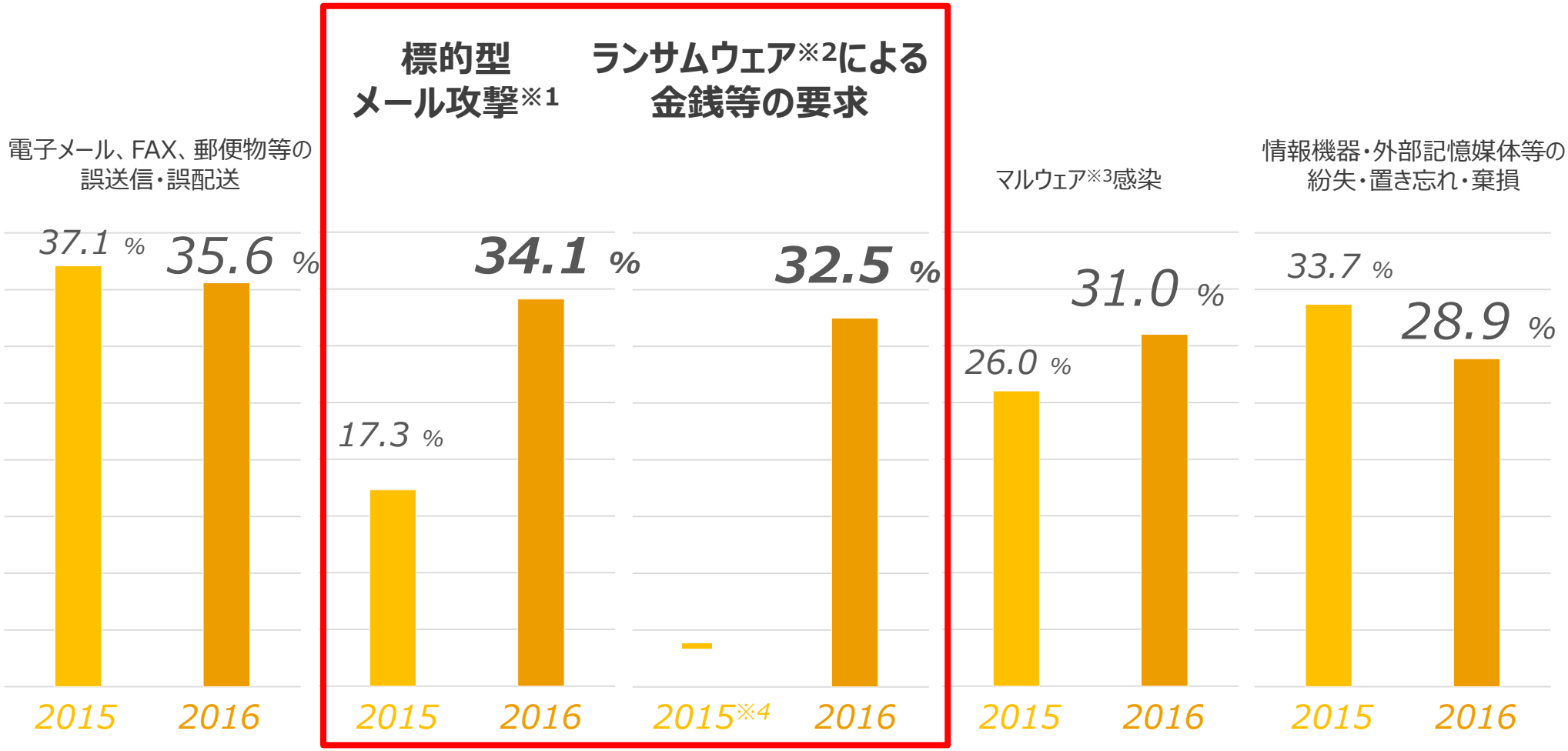
CTO（最高技術責任者）
75.7 %

[参考]2015年度（n=660）
CISO未設置：53.4%

Q.情報セキュリティおよび、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)

国内調査_02　高度なサイバー攻撃への対策

標的型メール攻撃やランサムウェア等の事件事故が急速に台頭



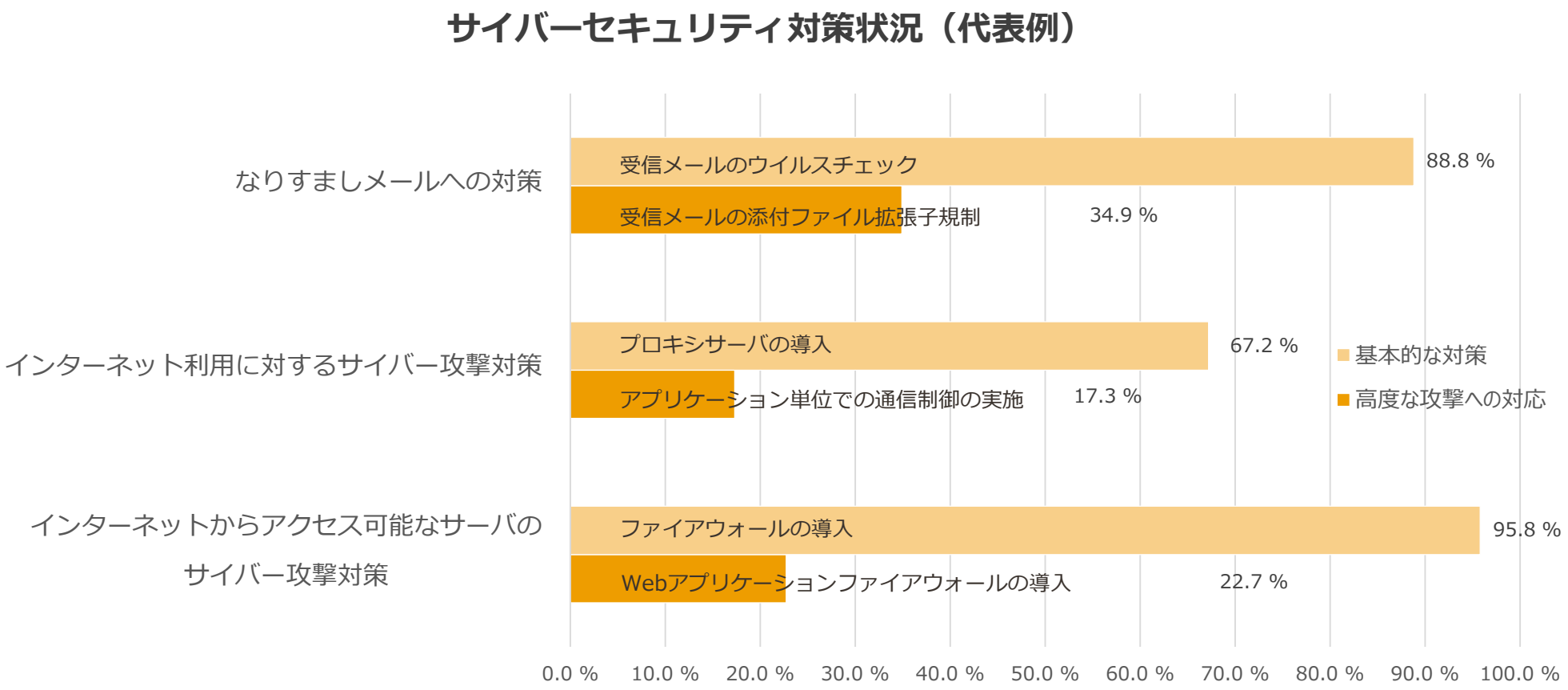
Q.過去1年間で発生した、情報セキュリティに関する事件・事故はありますか。

(2015：n=660、2016：n=671、複数回答)

※1　特定の企業や組織を狙い、巧妙に偽装されたメールを送り、マルウェアに感染させることで情報を漏洩させる攻撃
※2　PC上のデータやシステムへのアクセスを制限し、その制限の解除に金銭を要求するマルウェア
※3　コンピュータウィルスやワーム等、悪意のある不正なソフトウェアの総称
※4　2016年度調査から実施

国内調査_02　高度なサイバー攻撃への対策

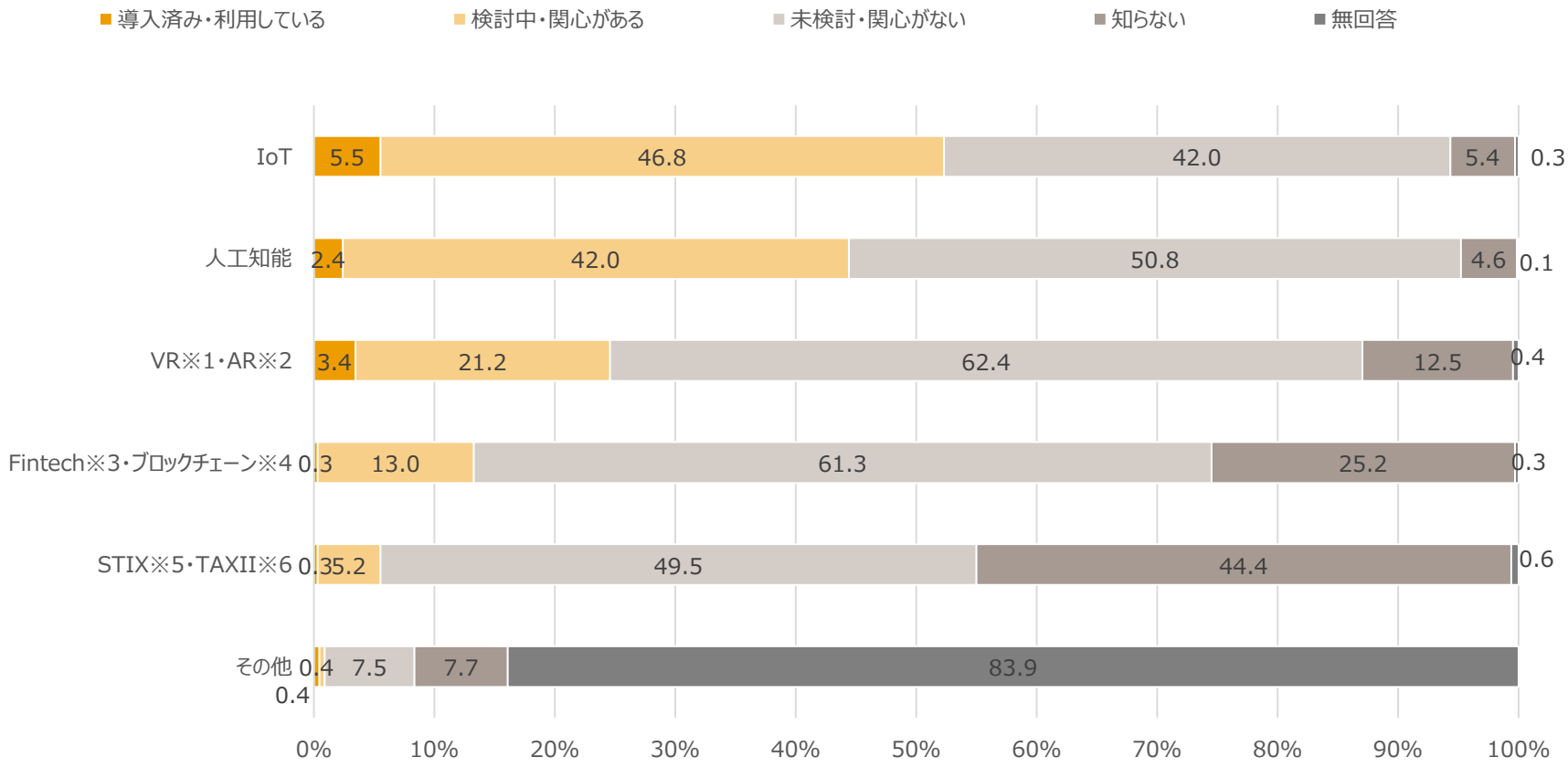
基本的な対策は実施できているが、高度な攻撃への対応に遅れ



Q.「インターネットからのサイバー攻撃、Webやメール利用 等」に関する対応・対策状況はいかがですか。(n=671、複数回答)

国内調査_03 IoTのセキュリティ

新技術の中で、約半数の企業がIoTを利用している/関心がある

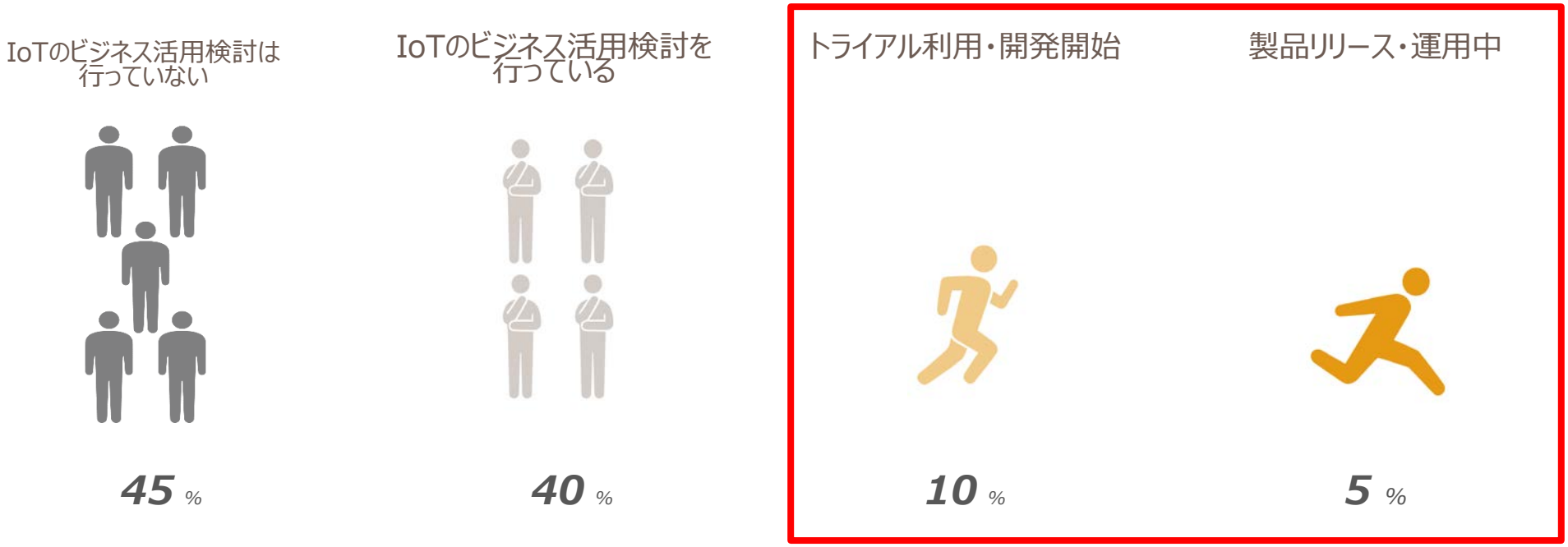


Q.新技術の導入・検討状況はいかがですか。(n=671)

※1 仮想現実（Virtual Reality）。完全な3D空間を現実ように体験できる
※2 拡張現実（Augmented Reality）。現実世界に情報を付加する
※3 主にITを活用した新たな金融サービスやその提供企業のことを含めて意味する
※4 ビットコインなどの分散型暗号通貨を支えるコアの技術
※5 Structured Threat Information eXpression。サイバー攻撃を特徴付ける事象などを取り込んだサイバー攻撃活動に関連する項目を記述するための技術仕様
※6 Trusted Automated eXchange of Indicator Information。サイバー攻撃に関連する脅威情報を交換するための技術仕様

IoT関連で、「トライアル利用・開発開始」以降のフェーズに進んでいる企業は15％

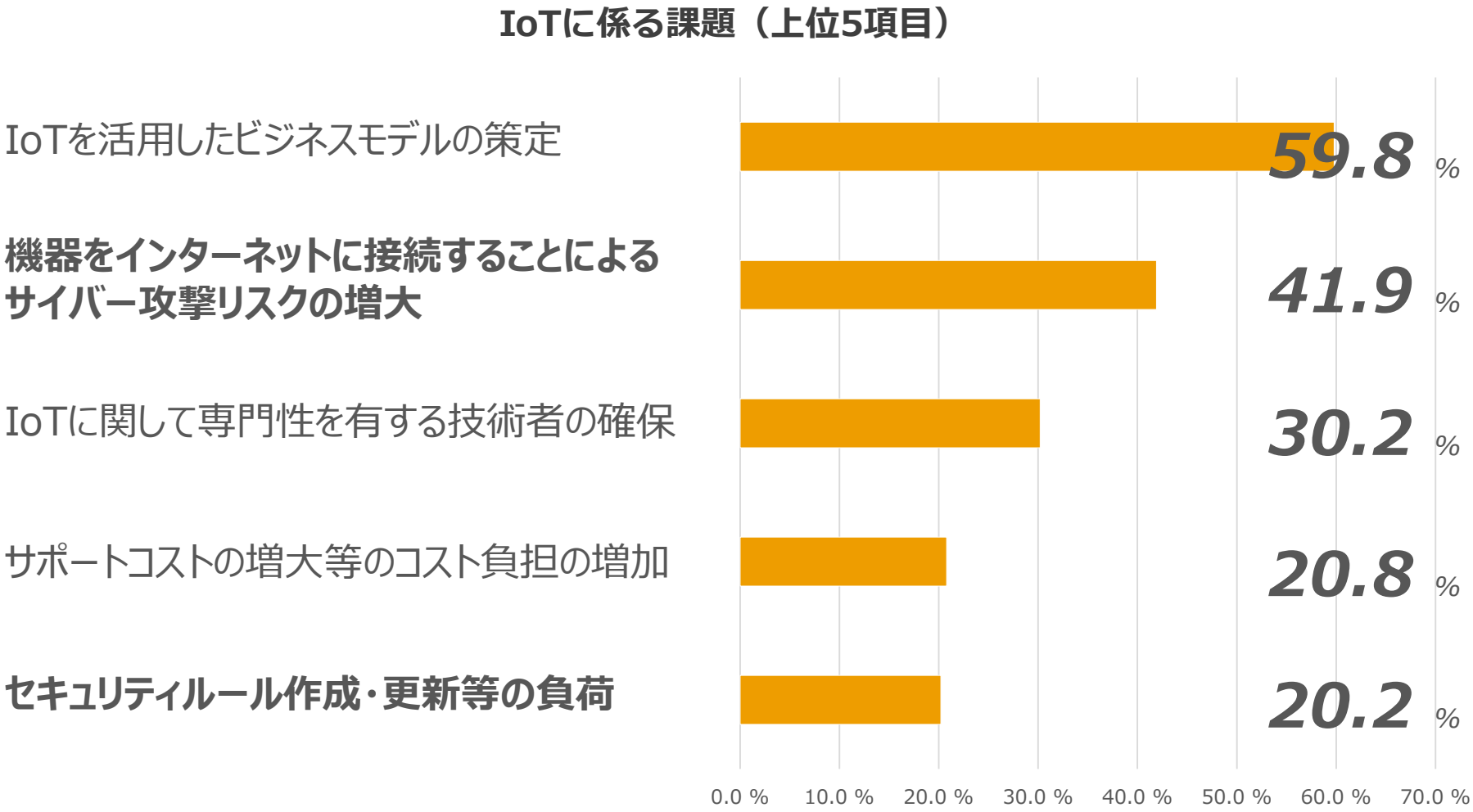
IoTに関する検討・利用フェーズ



Q.貴社内においてIoTに関する検討がどのフェーズにあるかお教えください。(n=351、IoTを「導入済み・利用している」「検討中・関心がある」と回答した企業)

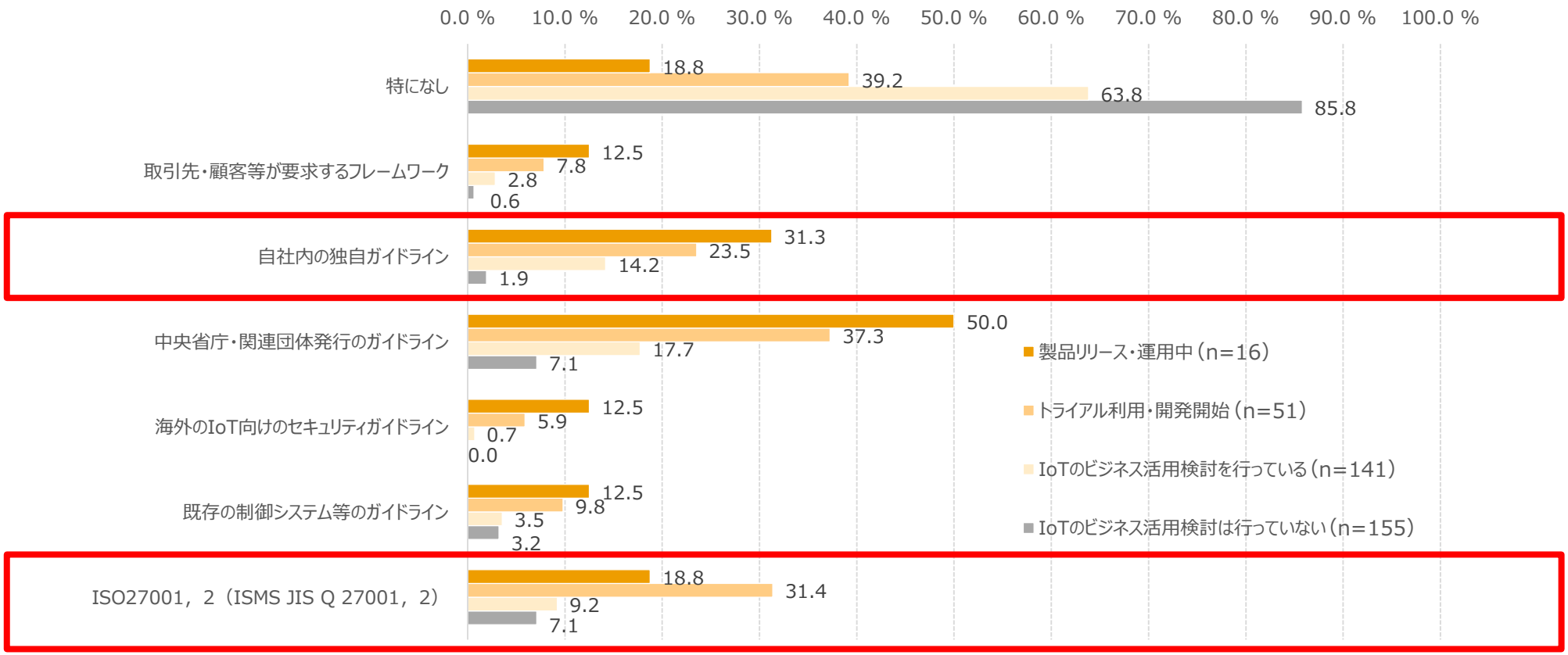
国内調査_03 IoTのセキュリティ

「サイバー攻撃リスクの増大」をIoTの課題として挙げる企業は4割強と多い



Q.IoTに係る課題として認識されていることは何ですか。(n=351、 IoTを「導入済み・利用している」「検討中・関心がある」と回答した企業、複数回答)

検討初期段階ではISO27000の利用は多いが、「製品リリース・運用中」では割合が下がる段階が進むにつれて「自社内の独自ガイドライン」の利用割合は顕著に増加



Q.IoTに係るセキュリティについて、参照しているセキュリティガイドラインはありますか。

（ IoTを「導入済み・利用している」「検討中・関心がある」と回答した企業、複数回答）

1. ９割近くの企業でセキュリティ人材は不足しているものの、
人材強化・獲得施策は**３割の企業で未実施**

2. 新しいタイプの高度な攻撃が台頭しているが、
対応する高度な対策の**実施率は低い**

3. IoTの課題としてサイバー攻撃を挙げている企業は多い。
また、IoT先行企業では自社独自のセキュリティガイドラインを策定している割合も多い

組織横断的な情報セキュリティ戦略を推進する人材による施策が必要である

1. セキュリティ人材の不足解消には、以下の対応が重要
   - セキュリティ部門だけでなく、**人事部門・ビジネス部門などと連携**した、組織を横断した施策の推進
   - CISO（最高情報セキュリティ責任者）やその責任を担う指揮官の設置

2. セキュリティ対策については、昨今の高度な攻撃に対応するための定期的な見直しや設定変更等による、**対策の高度化**が重要。
   それらを円滑に行うためにも、セキュリティ統括の設置は必須

3. IoTシステムのセキュリティ担保のためには、**情報セキュリティ部門がビジネス部門と連携し、**自社のIoTビジネスの特性に合った自社独自のガイドラインの作成が必要。そのためにも部門間をつなぐ組織・役割を設置し、風通しの良い組織を作ることが重要

2.本年度のポイント　-国際比較調査-

国際比較調査：本年度より情報セキュリティ実態の国際比較調査を開始（再掲）

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

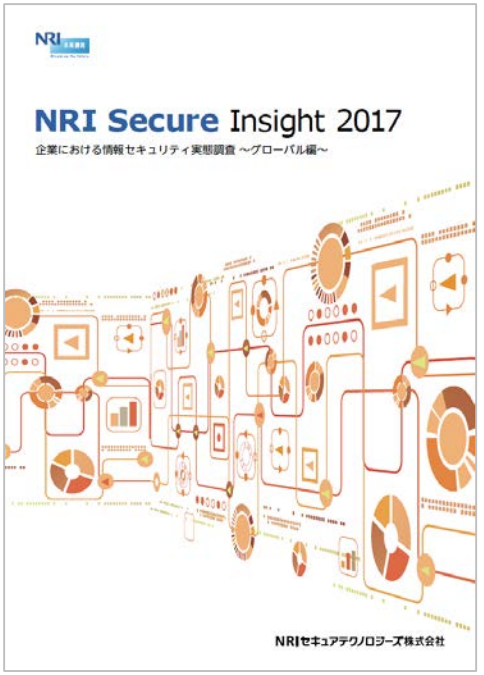
Webによるアンケート

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

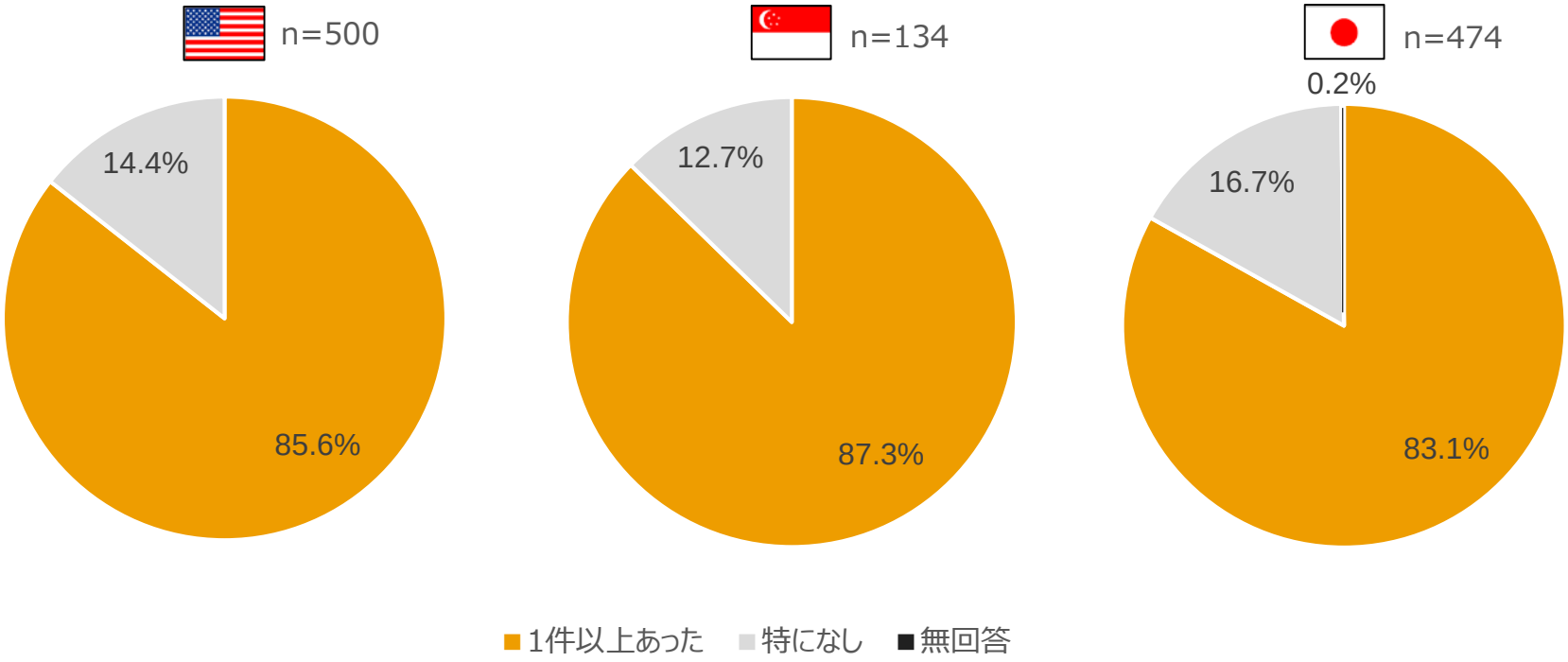
回答社数

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



過去1年でセキュリティ事件・事故を経験した企業は各国とも8割に上る

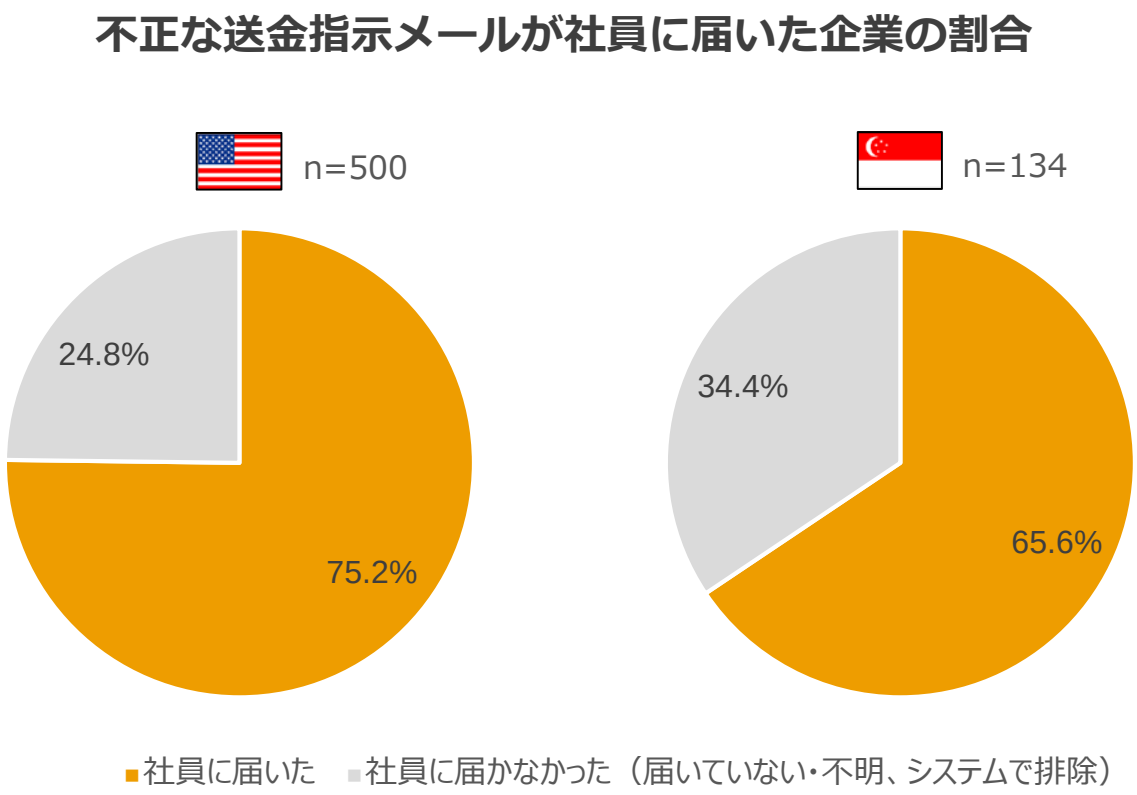
過去1年で情報セキュリティに関する事件・事故があった企業割合



Q.過去1年間で発生した情報セキュリティに関する事件・事故※はありますか。

※サイバー攻撃、ヒューマンエラー、内部不正等の原因により発生した事件・事故

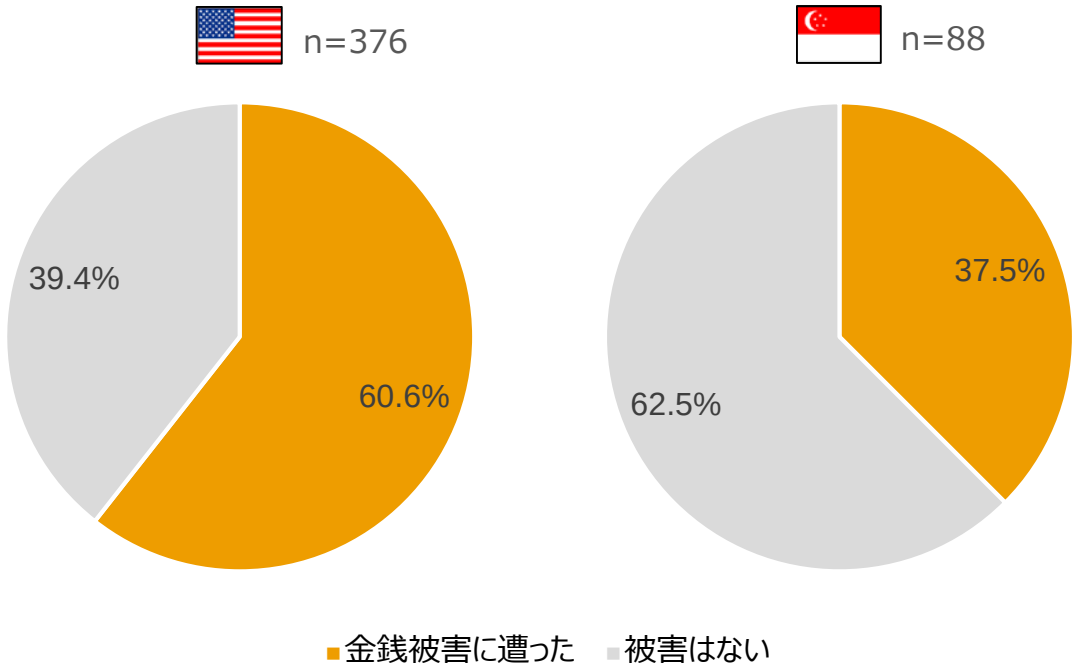
7割前後の米国・シンガポール企業に「送金指示メール」や「金銭の詐取を目的としたメール」が社員に届いたと回答



Q.過去1年間の間、貴社に偽の送金指示メール・金銭の詐取を目的としたメールが届きましたか。

米国では不正な送金指示メールをユーザーが受信した企業のうち半数以上が金銭被害に遭ったと回答

不正な送金指示メールをユーザーが受信した企業のうち、金銭被害に遭った企業割合

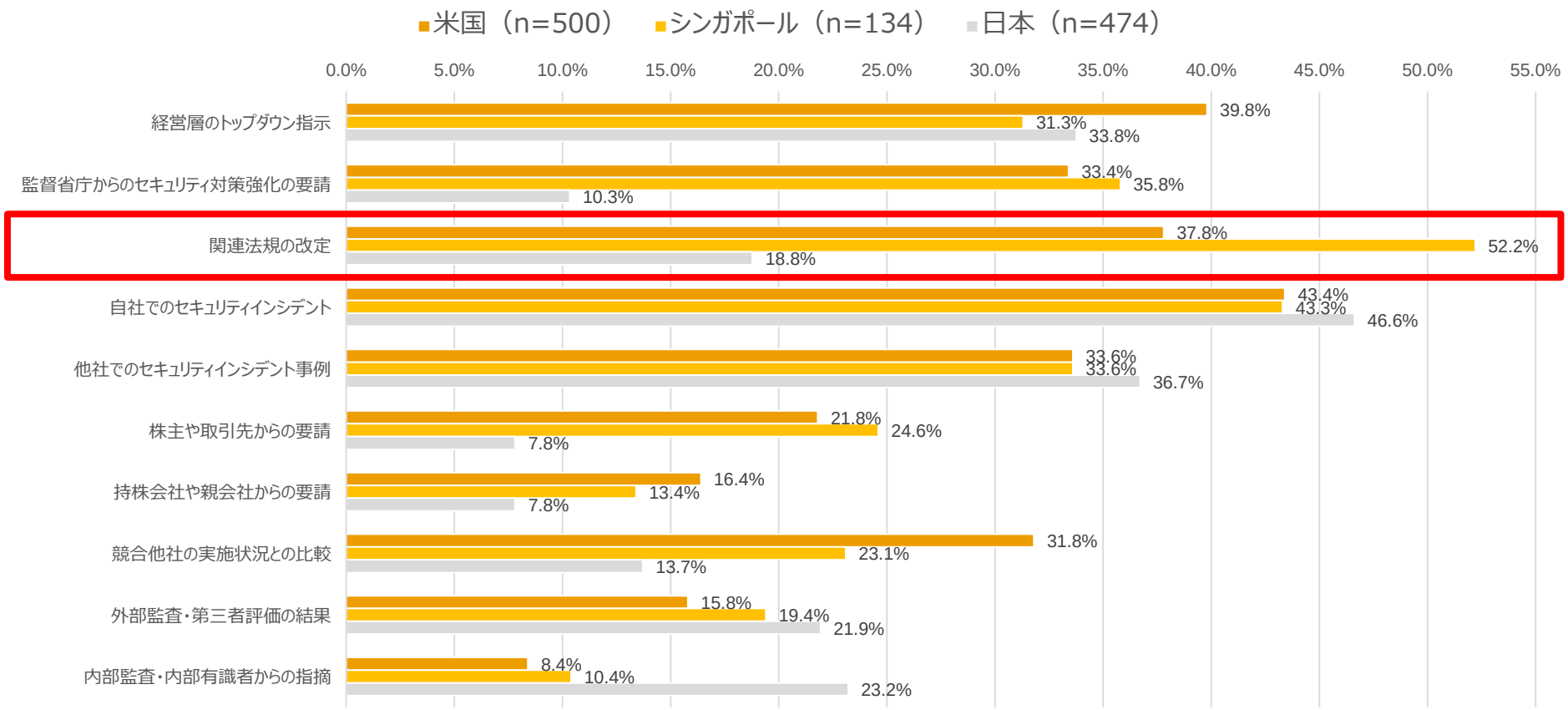


Q.偽の送金指示メール・金銭の詐取を目的としたメールによる被害を受けましたか。

（過去1年間の間、偽の送金指示メール・金銭の詐取を目的としたメールがユーザーに届いた企業に限定）

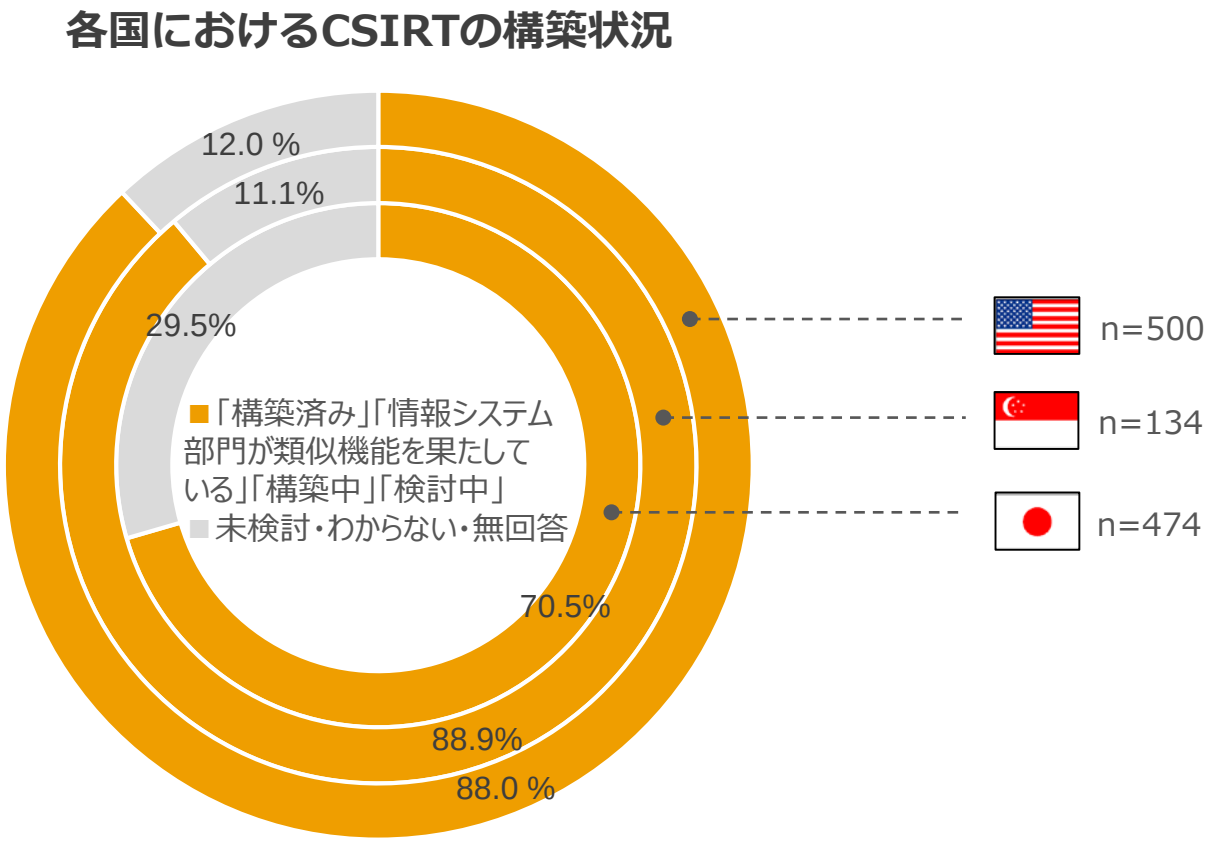
「関連法規の改定」をきっかけとして、情報セキュリティ対策を実施する企業が多い

情報セキュリティ対策の実施に至った理由/きっかけ



Q.情報セキュリティ対策の実施にいたった理由やきっかけは何ですか。（複数回答）

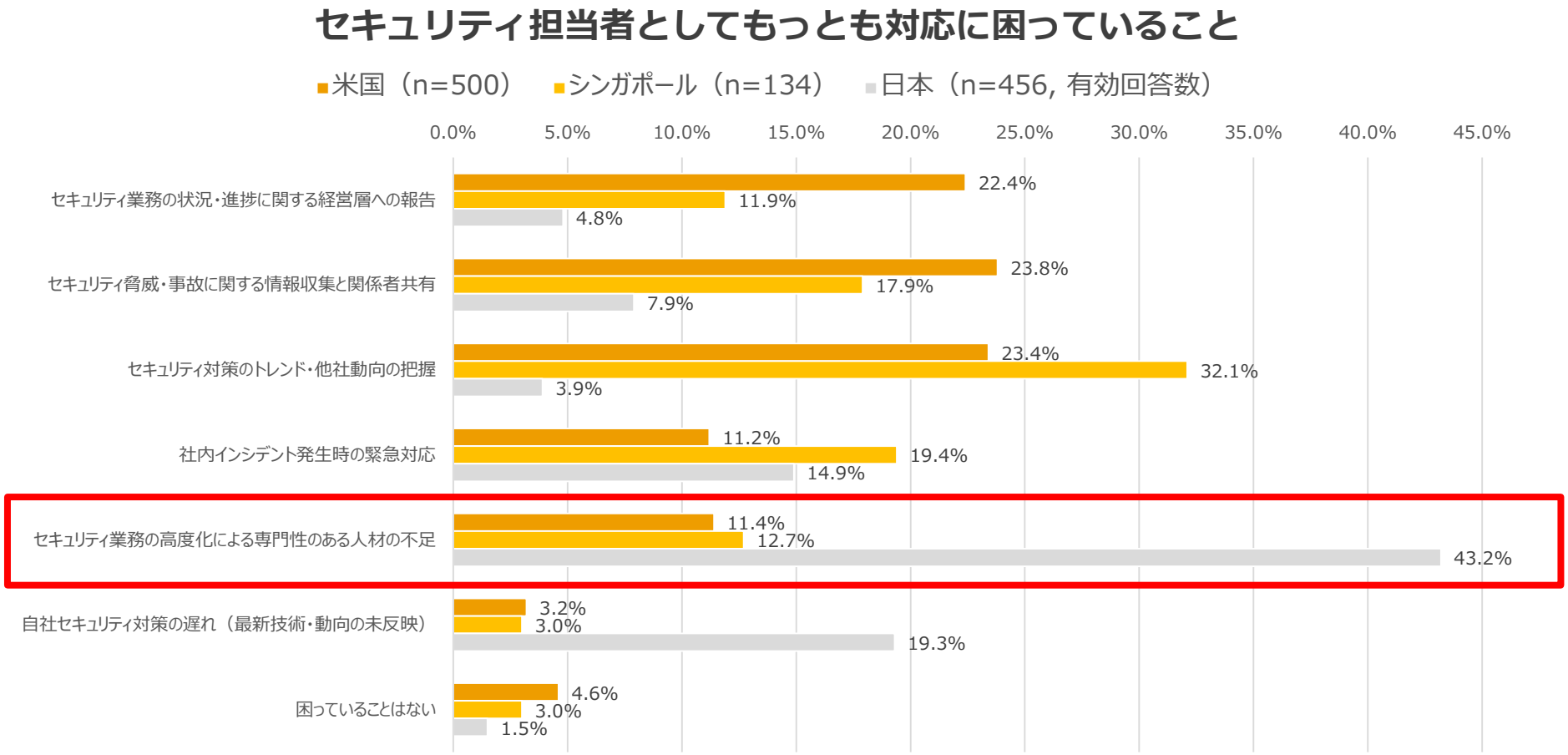
日本ではCSIRTの構築率が他の2カ国と比べ未だ低い



Q.組織内CSIRT※の構築状況はいかがですか。

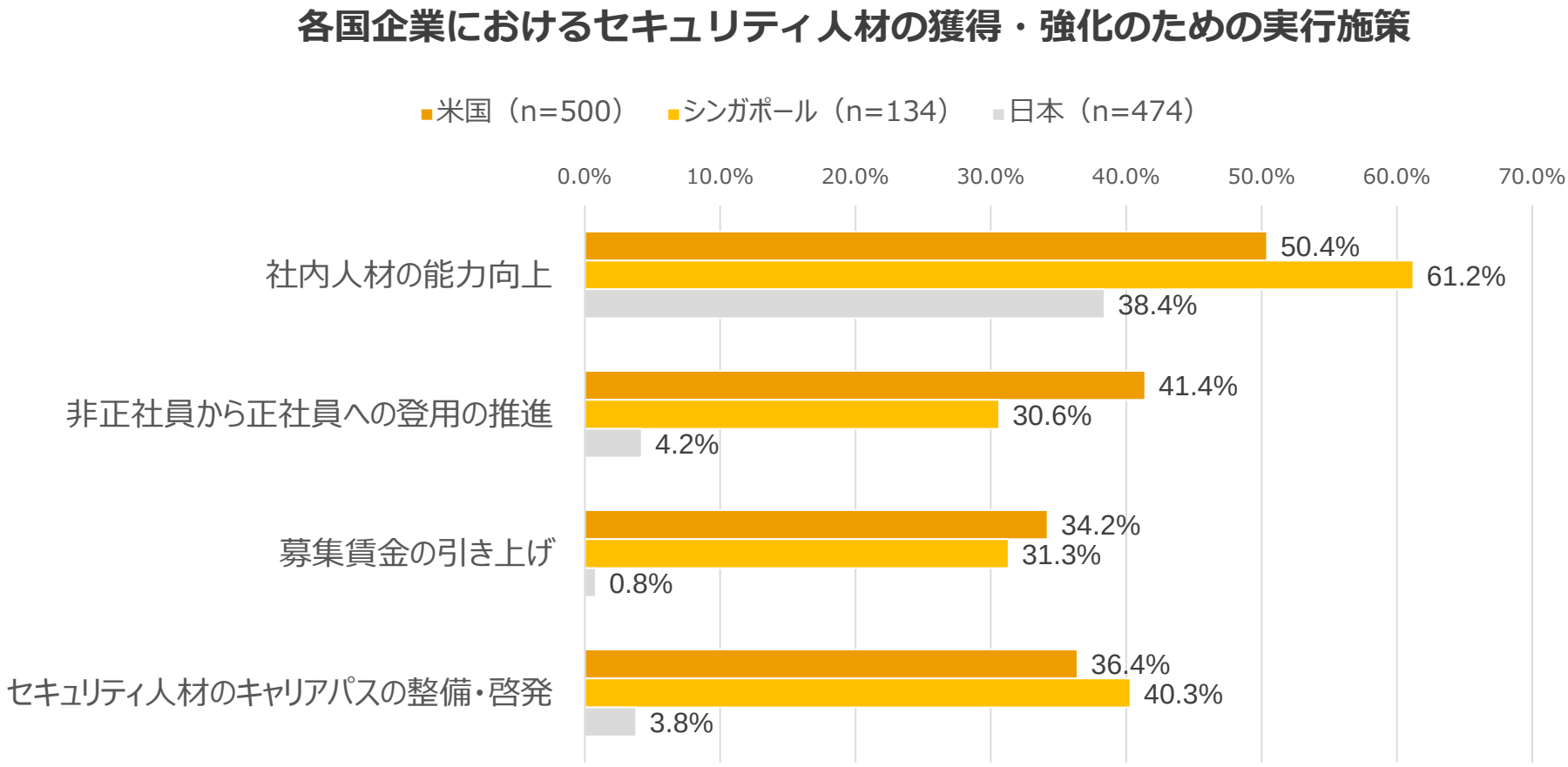
※ Computer Security Incident Response Team。コンピュータセキュリティインシデント対応組織の総称。決まった形はなく、内部／外部環境・制約等を鑑みて構築される。

他の2カ国と比べ日本企業は人材不足が顕著



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。

日本は既存人材の能力向上施策の割合が高いが具体的なキャリアパス整備は行っていない。また、人材の採用強化施策は実施割合が低い



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。

1. 米国では不正な送金指示メールを受け取った企業のうち
   半数以上が金銭被害に遭ったと回答

2. 「関連法規の改定」をきっかけとして、
   情報セキュリティ対策を実施する米国、シンガポール企業が多い

3. 日本は他2カ国に比べ、既存人材の能力向上施策の割合が高い
   が、具体的なキャリアパス整備は行っていない。
   また、人材の採用強化施策は実施割合が低い

情報セキュリティ担当部署だけでなく、全社として対応していく必要がある

1. 英語圏で流行し、今後日本でも増えていくと思われる「ビジネスメール詐欺」に代表される高度な攻撃に対抗するためには、**全社ITリテラシの向上**が不可欠。
それをトップダウンでリードする人材が必要である

2. 国内・海外の法令に対応していくためには**法務や広報等の他部署との密な連携**が肝要。個々の部で対応を進めるよりも指揮官のもと、横連携出来る組織が望ましい

3. 専門性のある人材の獲得のためには、担当部署内に留まらず
人事部との連携を図り、**全社としての人材獲得を目指すべき。**
また、人事部のサポートや獲得した人材の維持のための施策を経営層を含め検討する必要がある

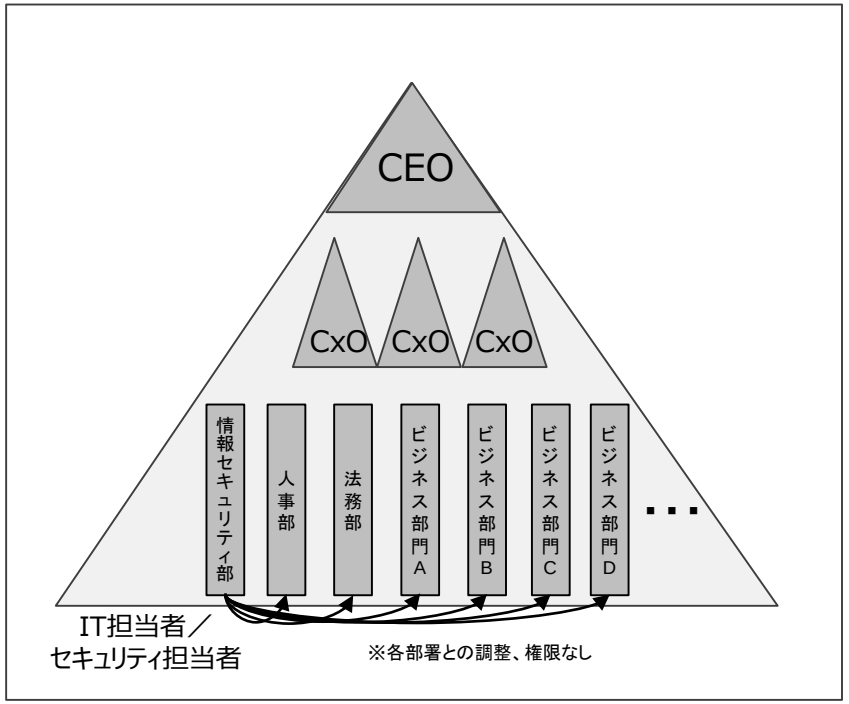
3.総括

3.総括

セキュリティの課題は経営層を中心に全社的な課題として認識し、推進すべきである

＜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

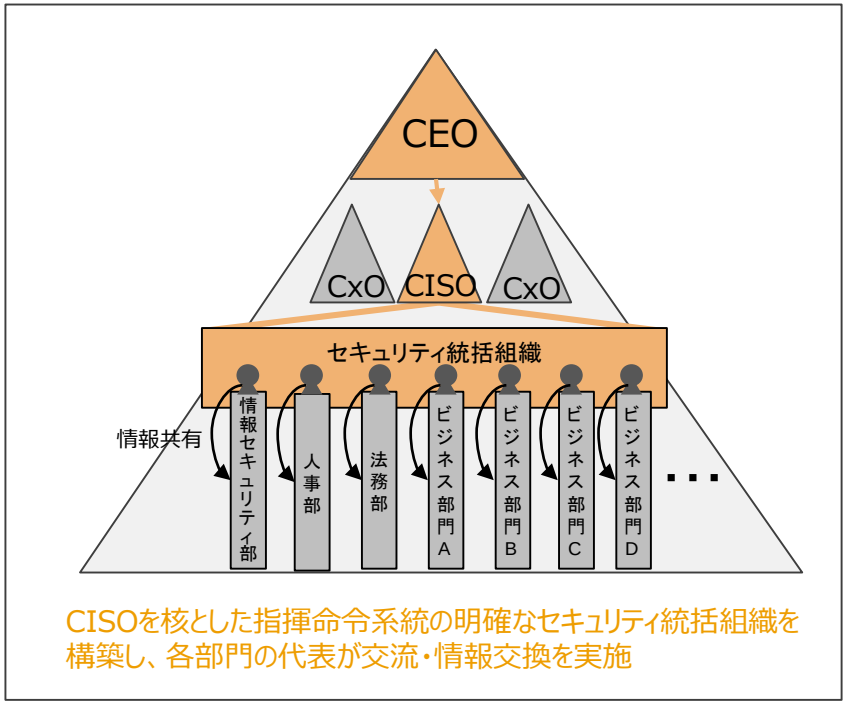


課題

- 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



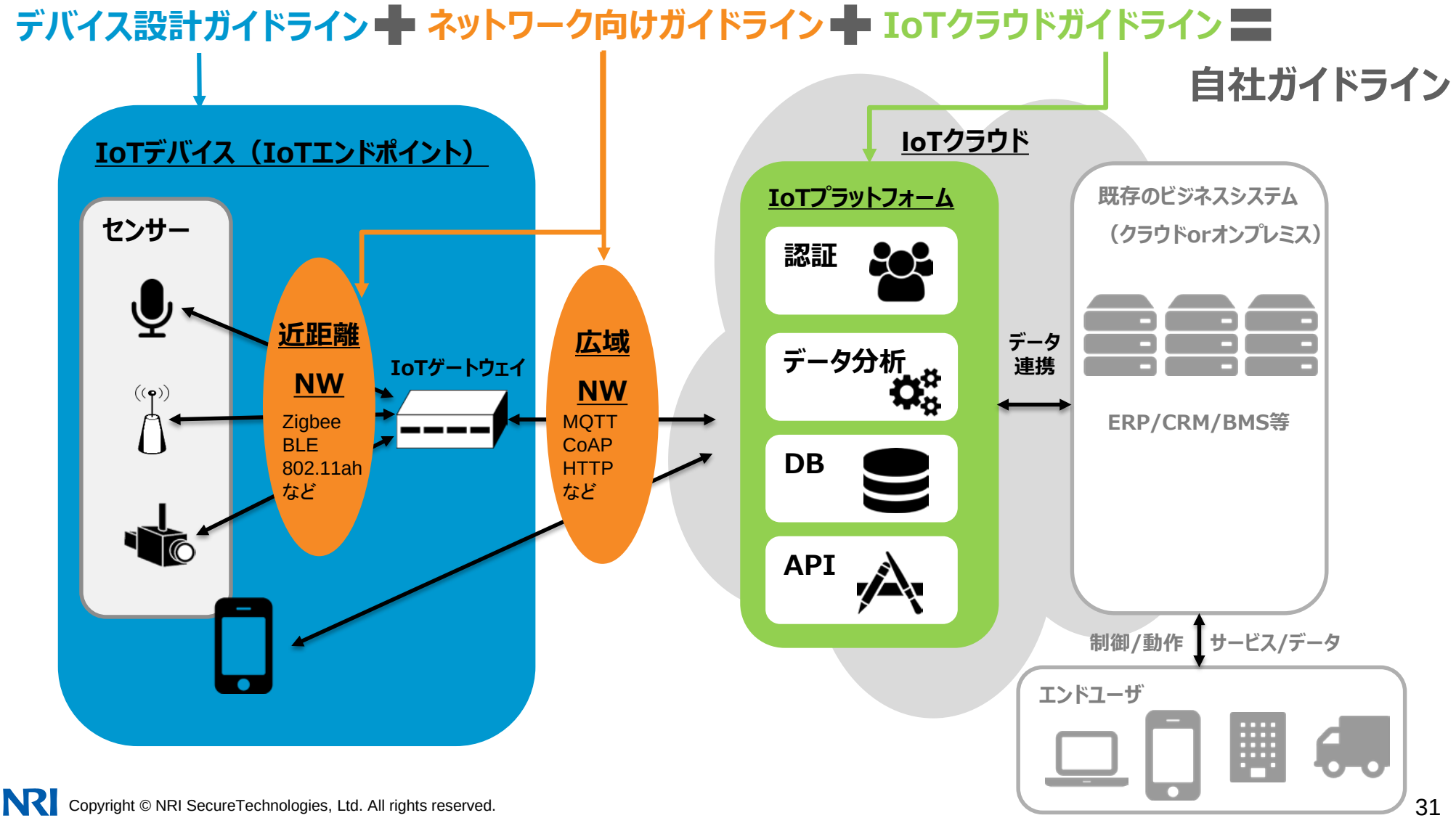
CISOを核とした指揮命令系統の明確なセキュリティ統括組織を構築し、各部門の代表が交流・情報交換を実施

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

4.ご参考

IoTセキュリティは自社のIoTシステム構成に沿ったIoTガイドラインを組み合わせた自社ガイドラインの策定が必要



NRIセキュアテクノロジーズ

NRI SecureTechnologies