第278回NRIメディアフォーラム

セキュリティが経営戦略になる時代

企業における情報セキュリティ実態調査2019

セキュリティコンサルタント　名部井 康博

NRIセキュアテクノロジーズ株式会社
GRCデジタルプラットフォーム部

2019年7月18日

NRI NRIセキュアテクノロジーズ

Share the Next Values!

01 調査概要

02 調査結果

03 総括

01. 調査概要

日本 / アメリカ / シンガポール の企業における情報セキュリティ実態調査

■ 目的

- 日本 / アメリカ / シンガポールの企業における、情報セキュリティに対する取り組みを明らかにする
- 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に、有益な参考情報を提供する

■ 調査期間

- 日本：2019/1/15 ~ 2019/2/28
- アメリカ / シンガポール：2018/12/3 ~ 2018/12/14

■ 調査方法

- Webによるアンケート

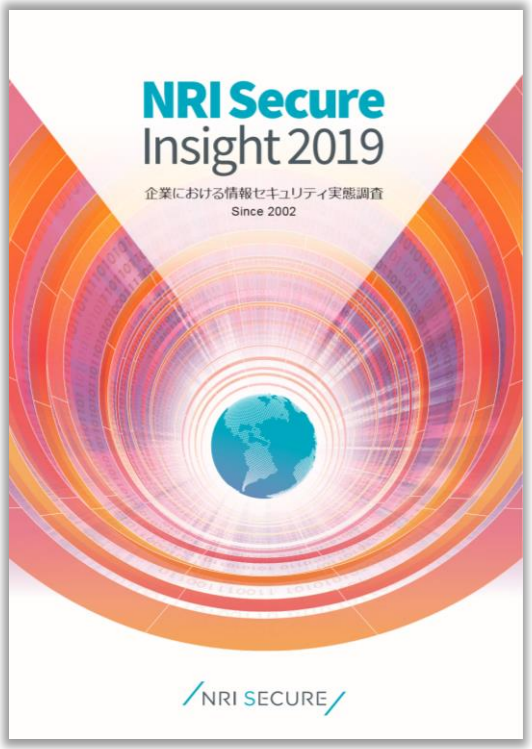
■ 調査対象

- 日本 / アメリカ / シンガポール の企業の情報システム / 情報セキュリティ担当者

■ 回答数

- 日本：1,794社 / アメリカ：509社 / シンガポール：504社

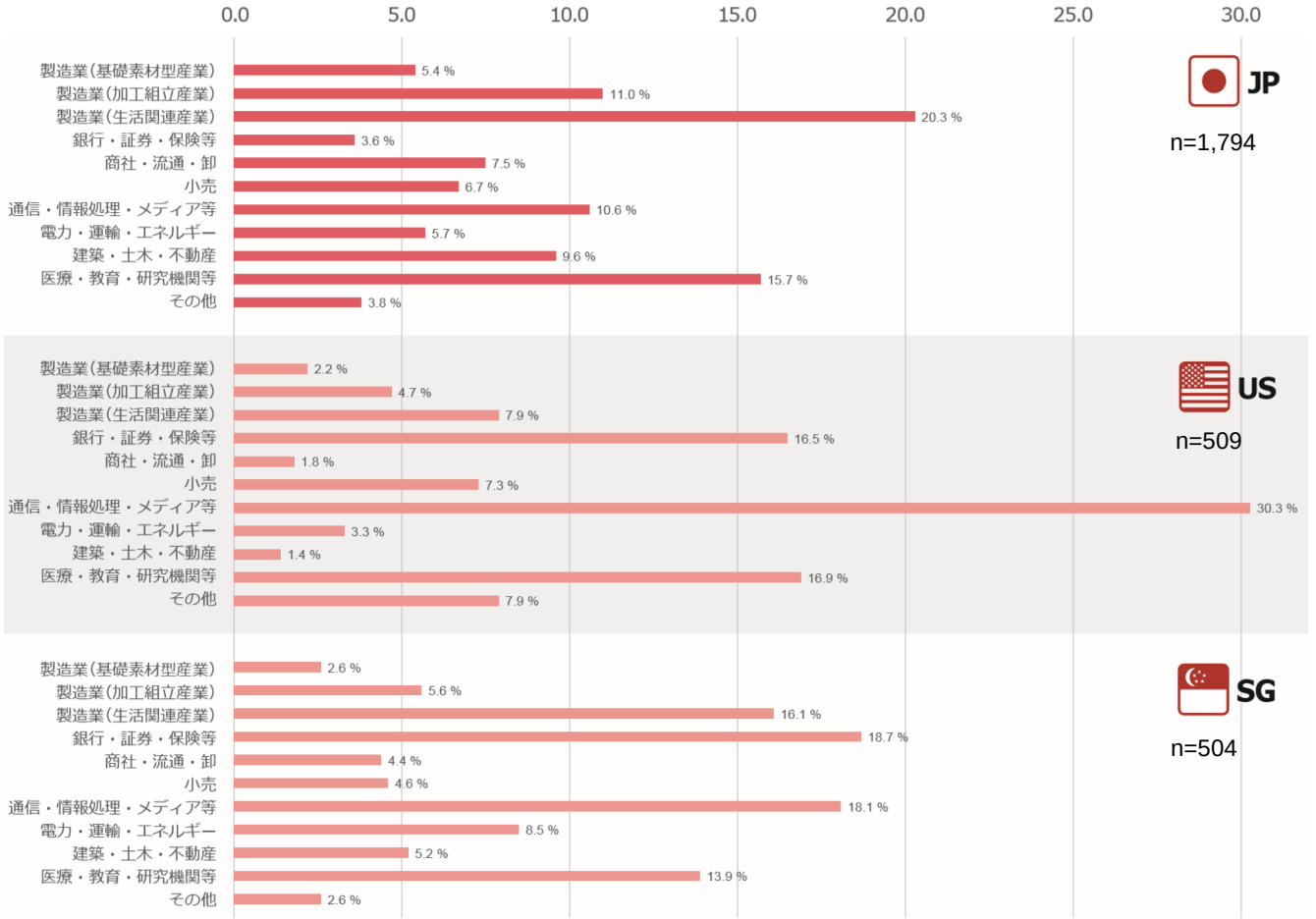
（参考：過去の調査における日本の回答数　2018年版: 107社、2017年版: 671社、2015年版: 665社）



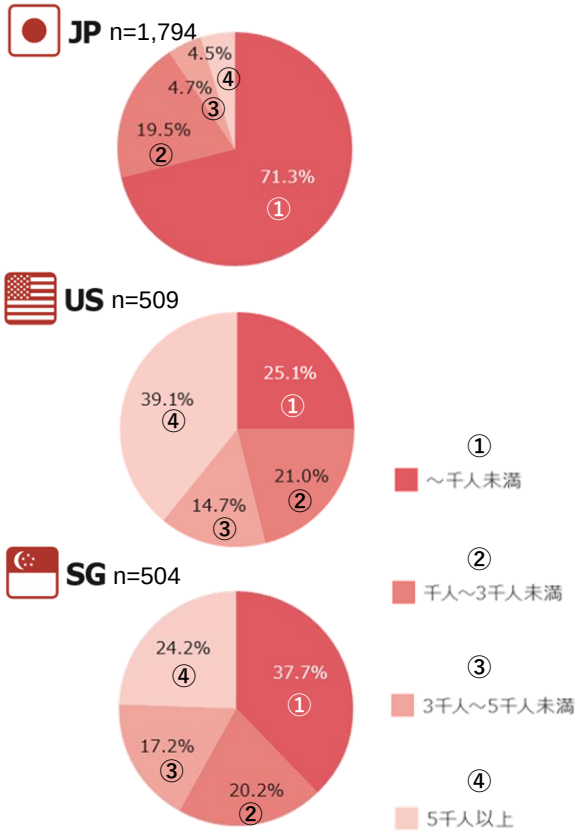
01 調査概要

回答企業の内訳

回答企業の業種



回答企業の従業員数



※ 回答企業の業種を以下のように分類

- 製造業(基礎素材型産業):紙・パルプ、化学、鉄鋼・金属
- 製造業(加工組立産業):機械・精密機器、電気機器、自動車製造業
- 製造業(生活関連産業):食品、繊維・アパレル、医薬、その他の製造業
- 銀行・証券・保険等:銀行、証券、保険、その他金融
- 通信・情報処理・メディア等:コンサルティング・シンクタンク、マスコミ・出版・印刷・広告、情報処理・ソフトウェア・SI、ISP・CATV・x DSL事業、通信・放送
- 電力・運輸・エネルギー:電力、石油・ガス、鉄道・航空、運輸
- 建設・土木・不動産:建設・土木・不動産、農林水産漁業・鉱業
- 医療・教育・研究機関等:医療、福祉、教育・研究機関、その他のサービス業

5つの分野にわたる調査

I. デジタルセキュリティ

DX（ビジネスモデルの変革や創造に寄与する高度なIT活用）の取組みに関わるセキュリティ要請への対応

II. セキュリティマネジメント

セキュリティ対策を推進するための組織体制

III. セキュリティ人材

セキュリティ業務を遂行する人材

IV. セキュリティ対策

セキュリティ対策の導入状況や導入計画

V. 脅威・事故

発生したインシデント（事件・事故）

02. 調査結果

I. デジタルセキュリティ

~ Digital Security ~

- DXへの取組み状況
- DXへの取組みの阻害要因
- DXに関するセキュリティの対応状況
- 先進的なセキュリティ対策の導入状況

I. デジタルセキュリティ：DXへの取組み状況

▶ 日本企業は、他2カ国に比べてDXへの取組みが遅れている

Q. 一般的に「デジタル変革・デジタルトランスフォーメーション（以下、DX）」と呼ばれるビジネスでの高度なIT活用の取組みは進んでいますか。また、それらの取組みによって情報セキュリティに対する変化はありますか。

①■ DXでセキュリティの要請が変わり、ルールや対策更新等対応している

②■ DXでセキュリティの要請が変わり、今後対応予定

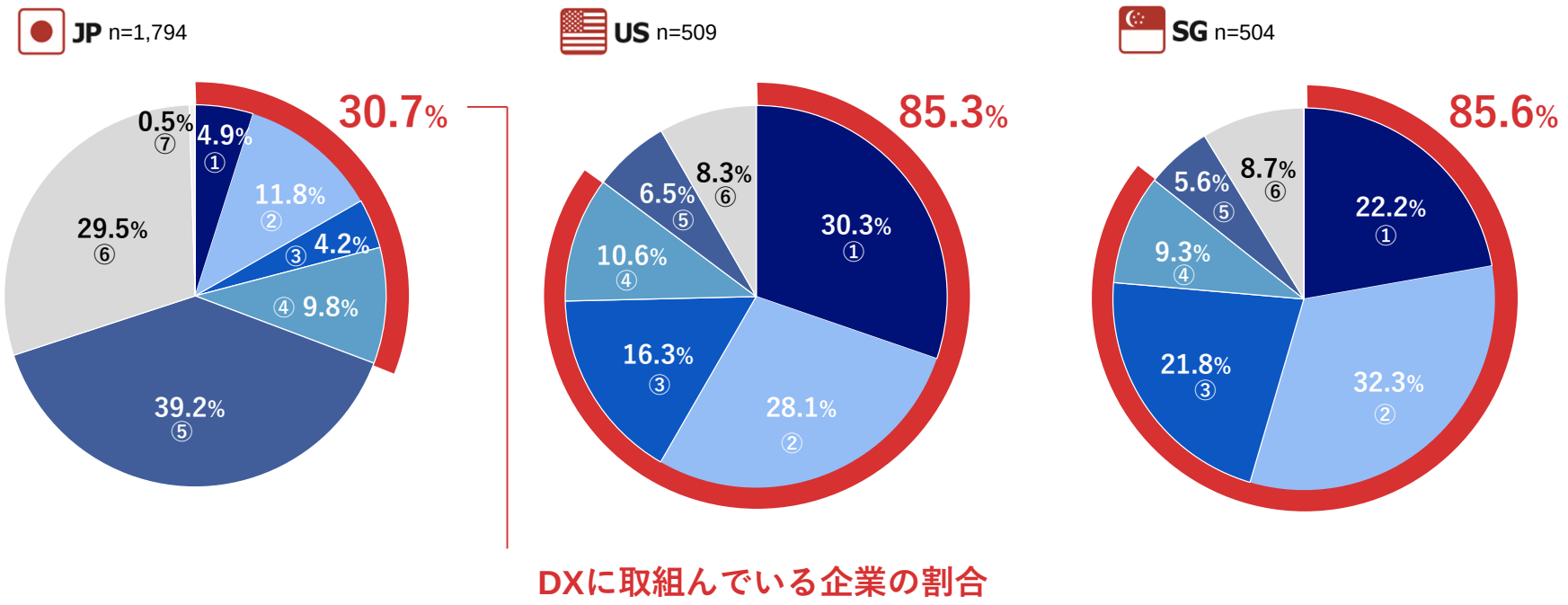
③■ DXでセキュリティの要請が変わっているが、対応はしていない

④■ DXでセキュリティの要請は変わっていない

⑤■ DXの取組みはされておらず、セキュリティの要請は変わっていない

⑥■ 分からない

⑦ その他

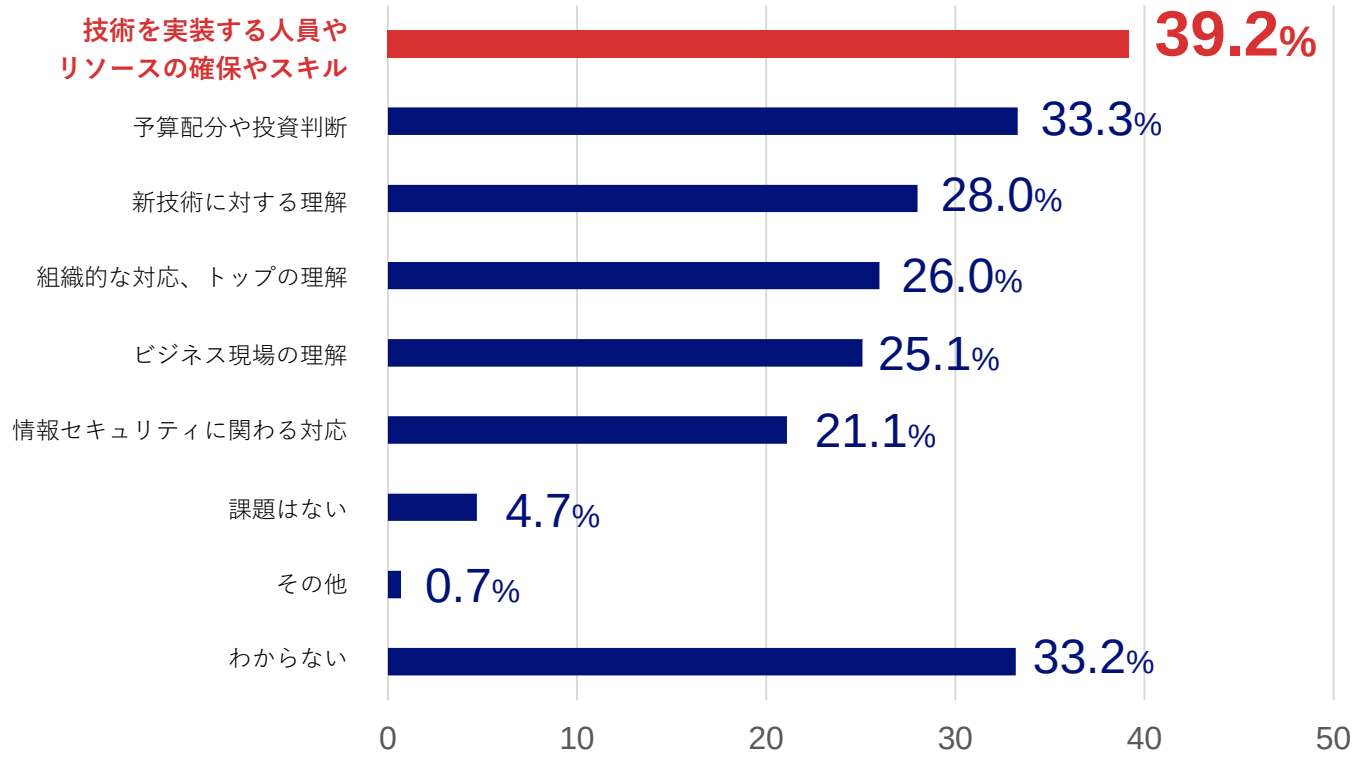


DXに取組んでいる企業の割合

I. デジタルセキュリティ：DXへの取組みの阻害要因

▶ 日本企業では、「スキルやナレッジを持つ人員確保」がDXの取組みを推進するうえでの課題

Q. デジタルトランスフォーメーションの取組みを進めるにあたって、阻害要因はありますか。（あてはまるものを全て選択）



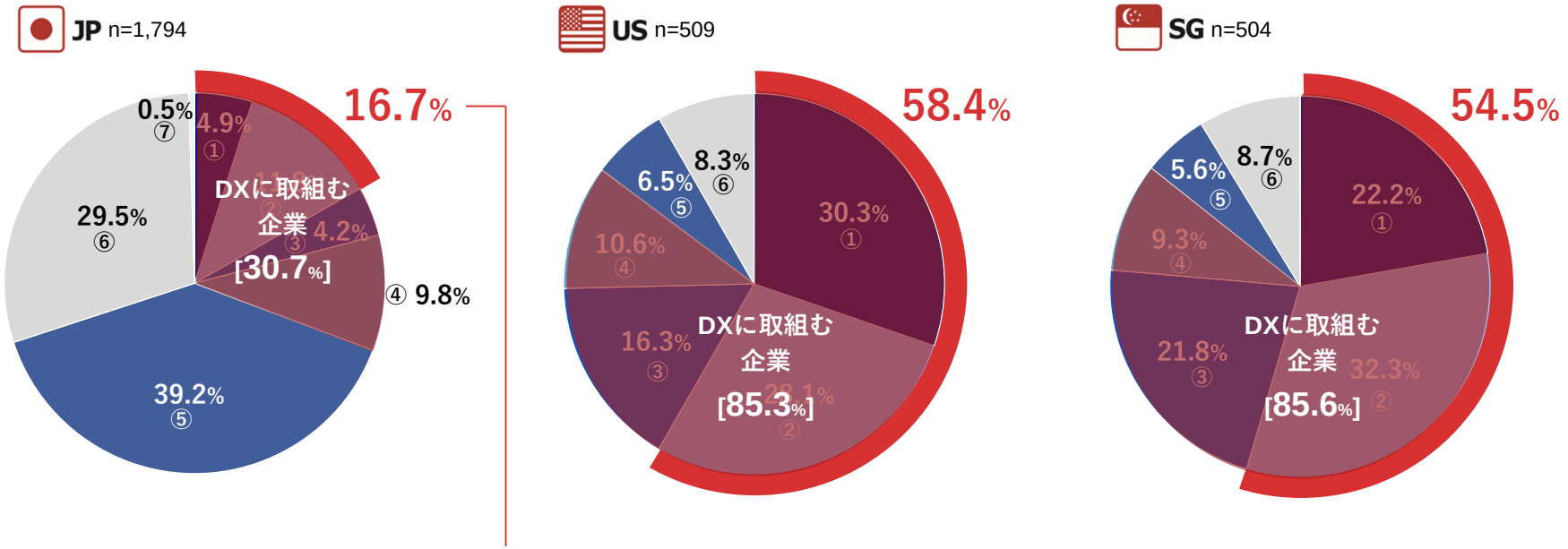
再掲

I. デジタルセキュリティ：DXへの取組み状況

▶ DXに取組む企業の半数以上は、DXに関するセキュリティにも対応している

Q. 一般的に「デジタル変革・デジタルトランスフォーメーション（以下、DX）」と呼ばれるビジネスでの高度なIT活用の取組みは進んでいますか。また、それらの取組みによって情報セキュリティに対する変化はありますか。

①■ DXでセキュリティの要請が変わり、ルールや対策更新等対応している
②■ DXでセキュリティの要請が変わり、今後対応予定
③■ DXでセキュリティの要請が変わっているが、対応はしていない
④■ DXでセキュリティの要請は変わっていない
⑤■ DXの取組みはされておらず、セキュリティの要請は変わっていない
⑥ 分からない
⑦ その他

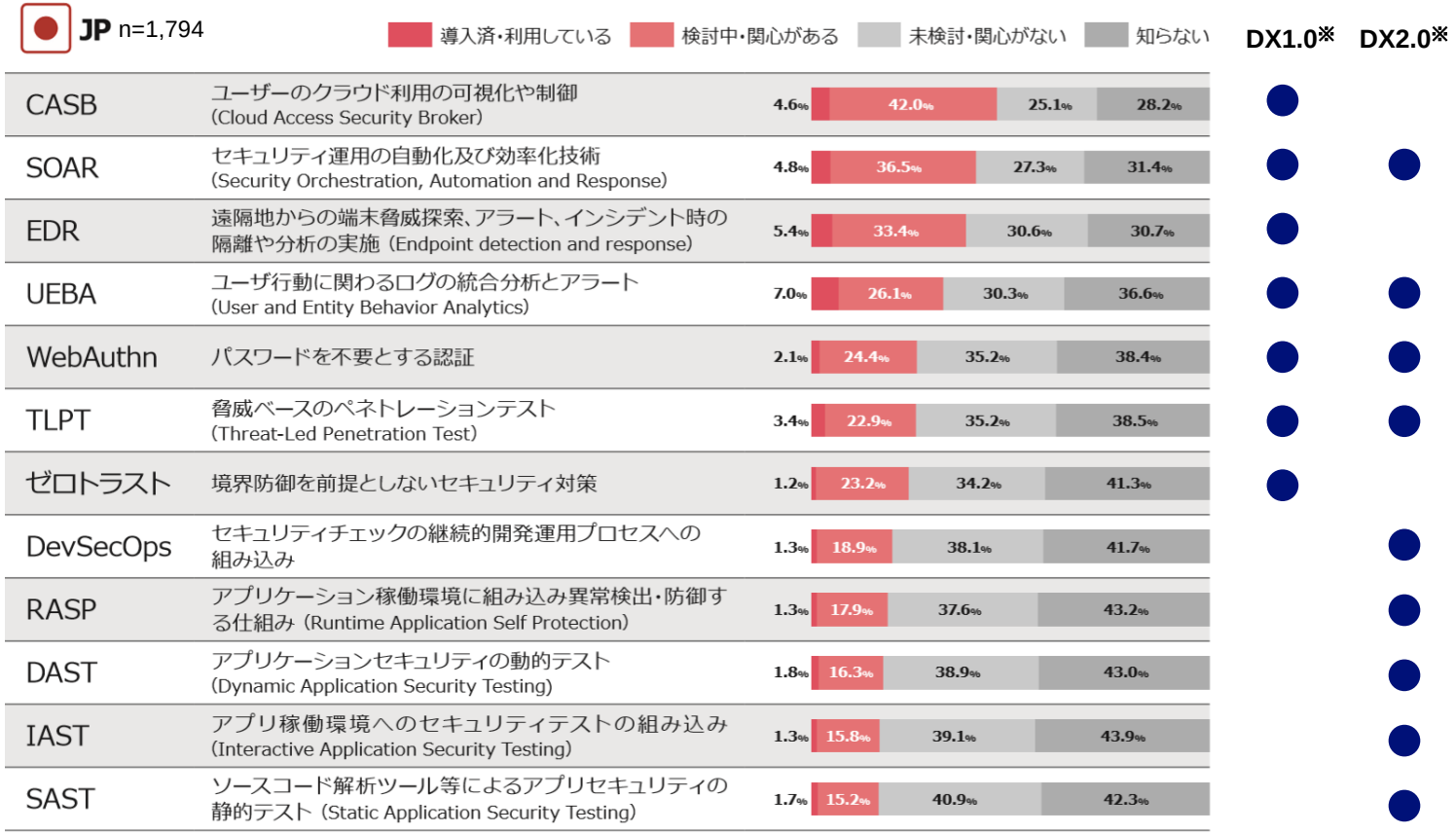


DXに取組んでいる企業のうち、DXに関するセキュリティにも対応している企業の割合

I. デジタルセキュリティ：先進的なセキュリティソリューションの導入状況

▶ 日本企業において、DXに関わる先進的なソリューションの導入率は低い

Q. 導入済みまたは関心のあるセキュリティ対策の新技術についてお答えください。



※DX1.0: プロセス変革、DX2.0: ビジネス変革

II. セキュリティマネジメント

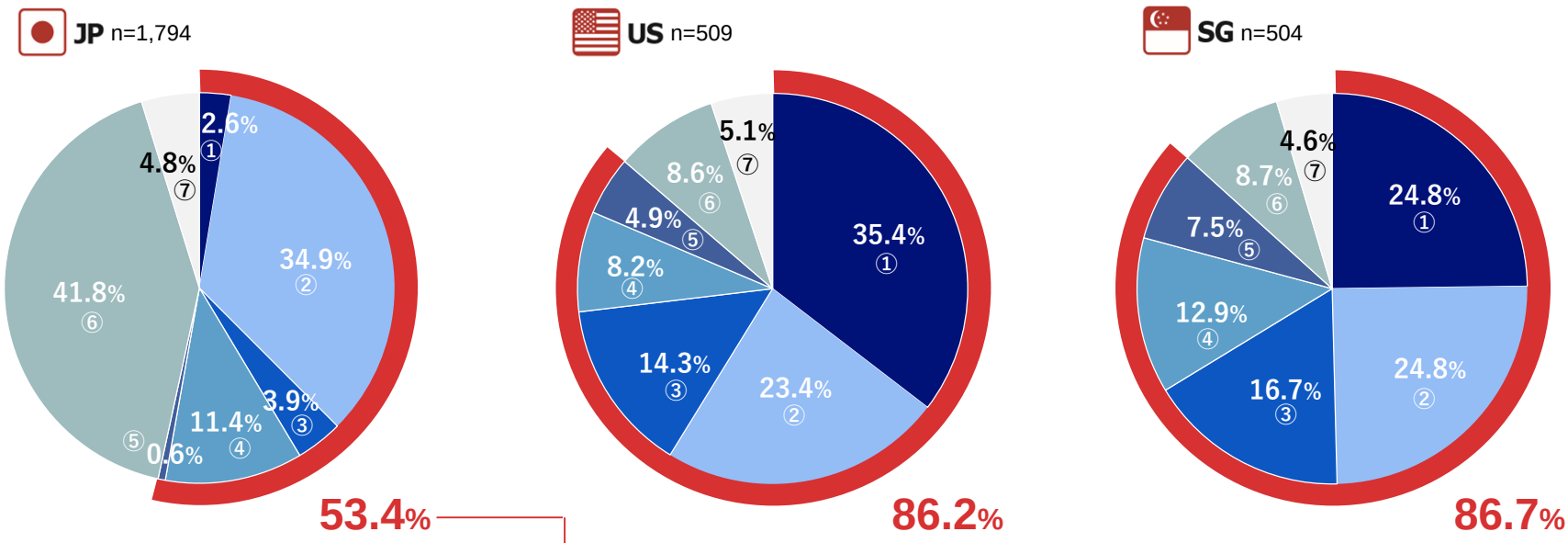
~ Security Management ~

- CISOの設置状況
- セキュリティ関連予算
- GDPRへの対応状況

日本企業のCISO設置率は約50%だが、他2カ国は約85%

Q. CISO（最高情報セキュリティ責任者）の設置状況についてお答えください。

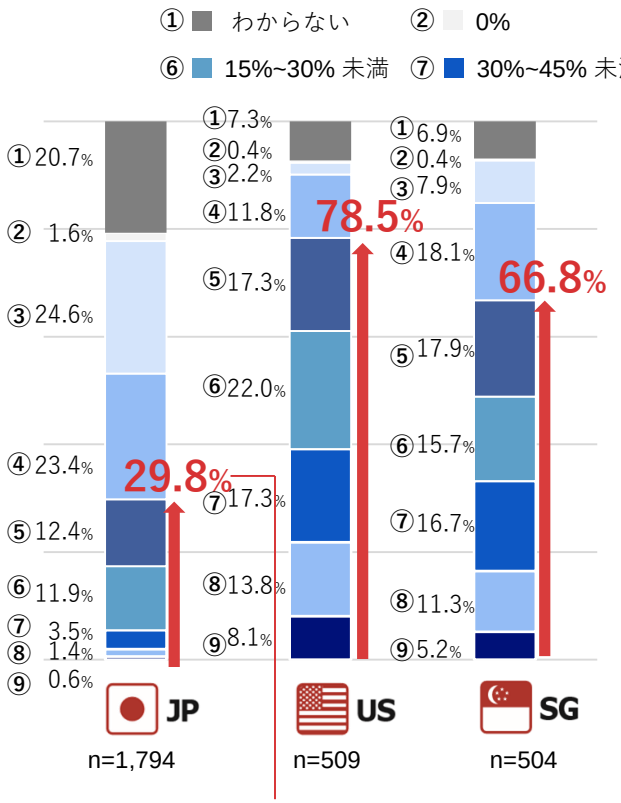
① 経営層が専任で就任　② 経営層が兼務で就任　③ 非経営層が専任で就任　④ 非経営層が兼務で就任
⑤ 社外有識者が就任　⑥ 未設置　⑦ 分からない



CISOを設置している企業の割合

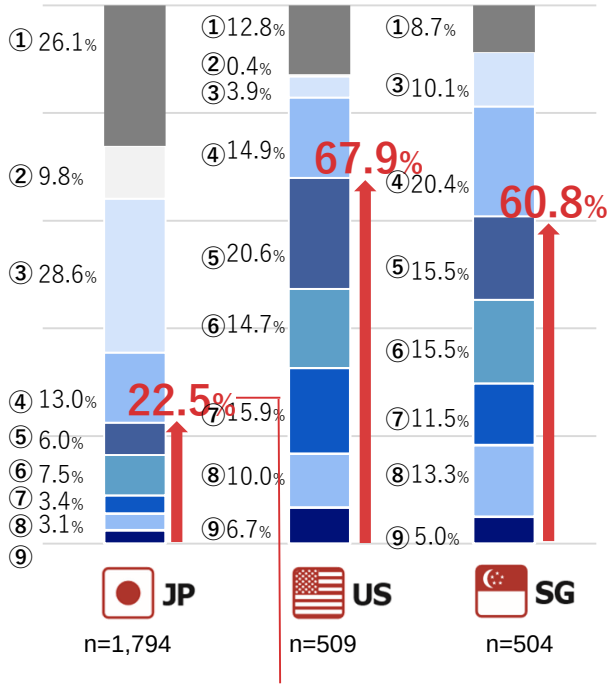
▶ 日本企業は他2カ国と比較して、セキュリティ予算及び新規対策導入予算が少ない

Q. IT関連予算に対する情報セキュリティ関連予算の割合はどの程度を見込んいますか。



IT予算のうち、情報セキュリティ予算を
10%以上計上している企業の割合

Q. 情報セキュリティ関連予算の中で、新規対策導入に利用する費用の割合はどの程度を見込んでいますか。



情報セキュリティ予算のうち、
新規対策導入予算を10%以上計上している企業の割合

II. セキュリティマネジメント：GDPR※への対応状況

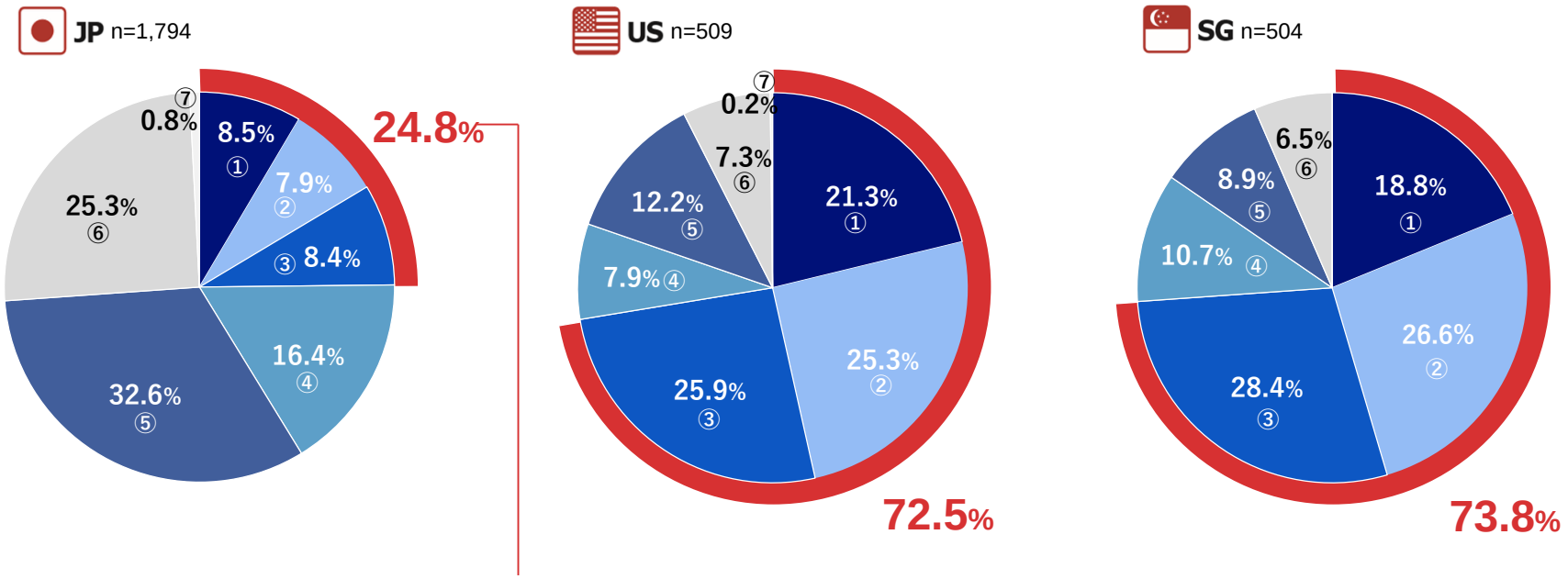
※EU一般データ保護規則(GDPR: General Data Protection Regulation)
欧州経済領域の個人データ保護を目的とした管理規則

▶ 日本において、GDPRへの対応を進める企業は約25%、対応不要と判断する企業が約33%

Q. GDPRへの対応状況はいかがですか。

①■ 対応済みである　②■ 現在、対応中である　③■ 現在、対応を検討している　④■ 将来的に対応が必要だが、現時点では検討していない

⑤■ GDPRの対象となるデータを保持していないため、対応は必要ない　⑥■ 分からない　⑦■ その他



GDPRへの対応を進めている企業の割合

III. セキュリティ人材

~ Human Resources~

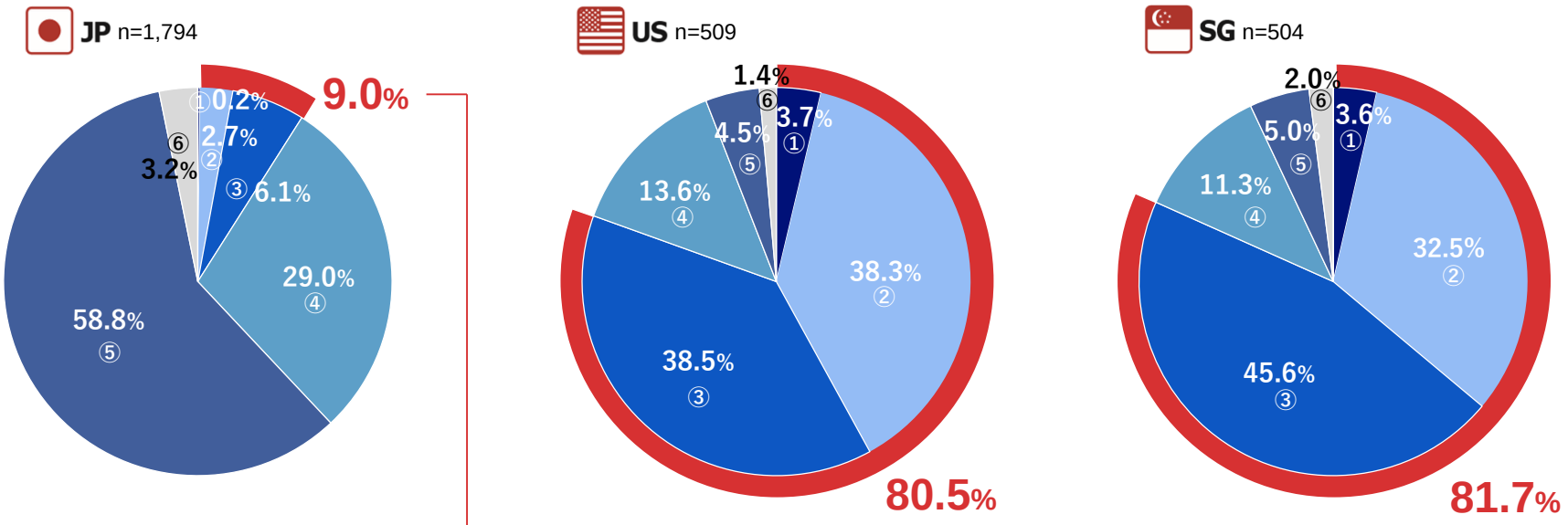
- セキュリティ人材の充足状況
- 不足している人材の種別
- 育成・教育における課題

▶ 日本企業は圧倒的にセキュリティ人材の不足を訴えている

Q. 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。

① ■ 人材が過剰な状態　② ■ 充足している（最適な状態）　③ ■ どちらかといえば充足している

④ ■ どちらかといえば不足している　⑤ ■ 不足している　⑥ ■ わからない

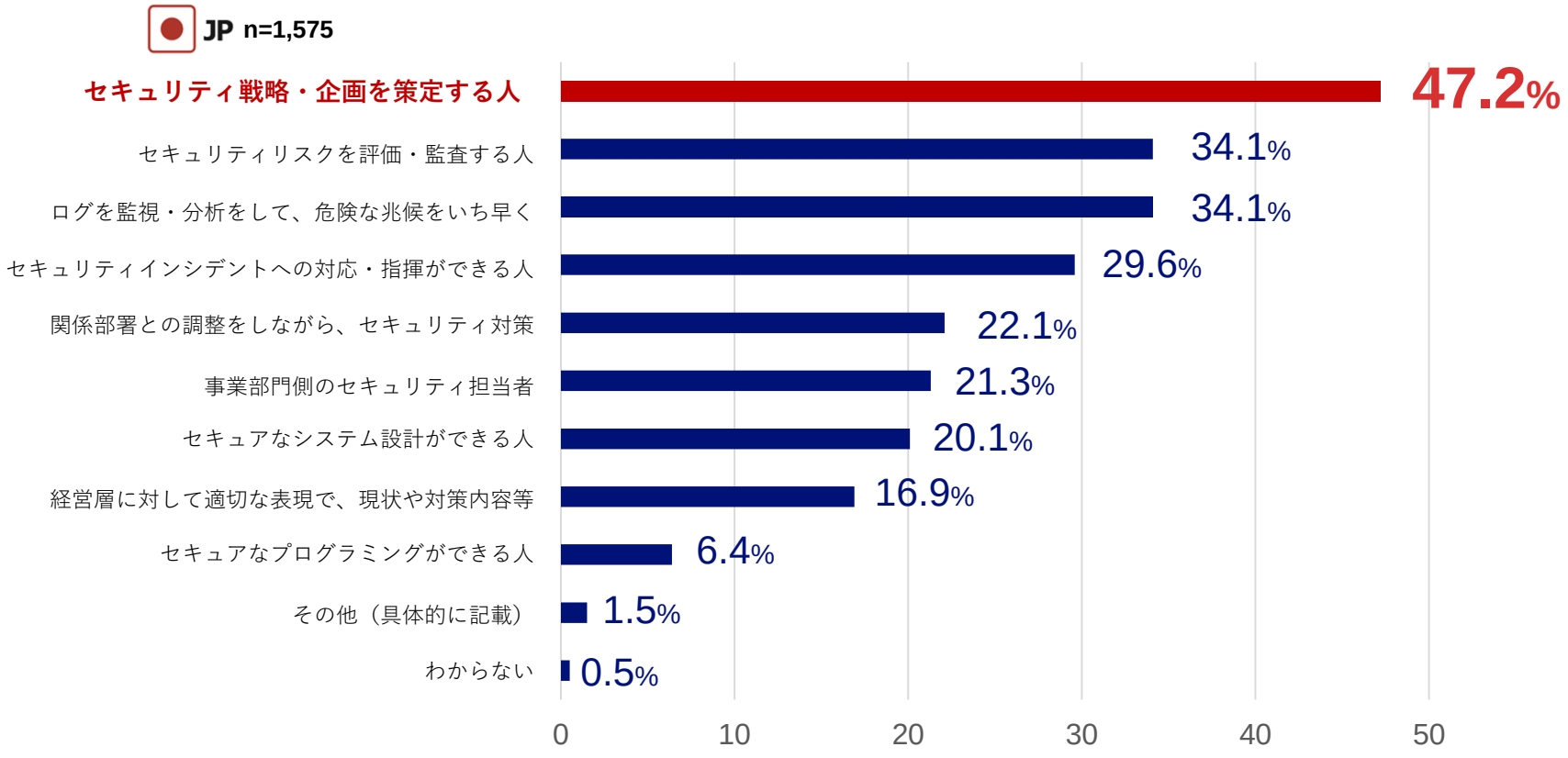


セキュリティ人材が「充足している」と感じている企業の割合

III. セキュリティ人材：不足している人材の種別

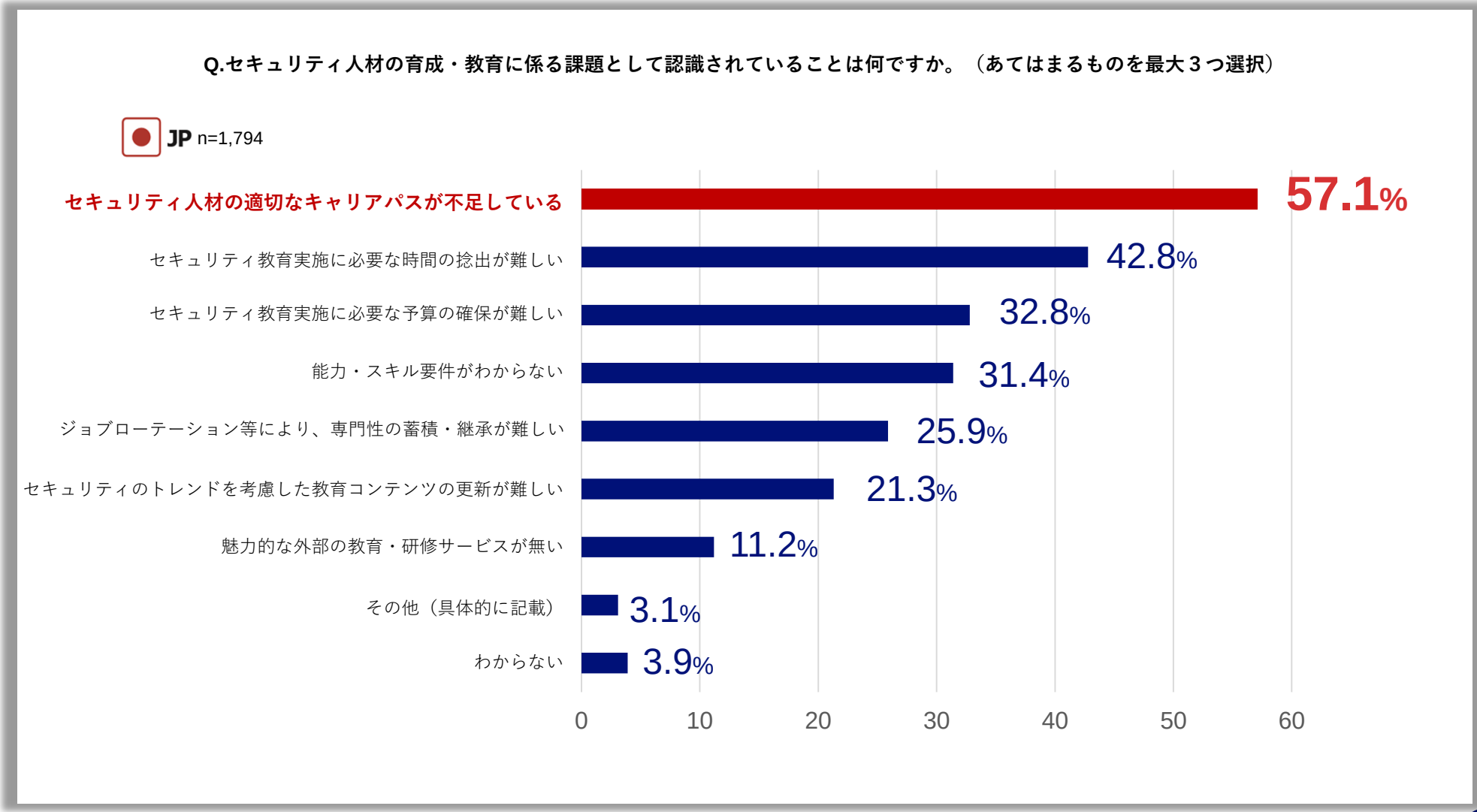
▶ 日本企業において、「セキュリティ戦略・企画を策定する人」が不足人材のTOP

Q. 人材が不足していると考える人材種別は何ですか。（あてはまるものを最大３つ選択）



※ セキュリティ人材が 「不足している」 「どちらかといえば不足している」 と回答した企業が対象

▶ 日本企業において、「キャリアパスの整備」がセキュリティ人材育成における課題のTOP



IV. セキュリティ対策

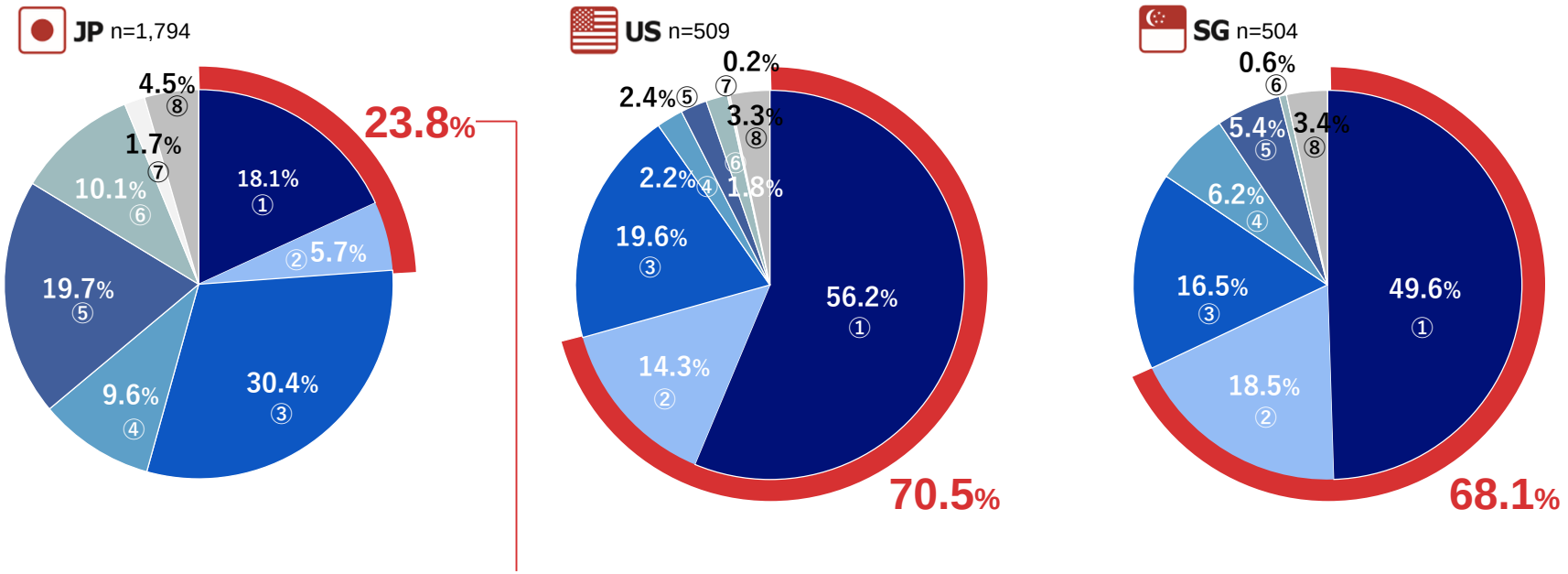
~ Security Measures~

- セキュリティ対策実行計画の策定状況
- セキュリティ対策実施のきっかけ
- CSIRTの構築状況

日本企業は他2カ国と比較して、中長期の実行計画を立てる割合が小さい

Q. リスクに対する具体的なセキュリティ対策の実施計画を立てていますか。

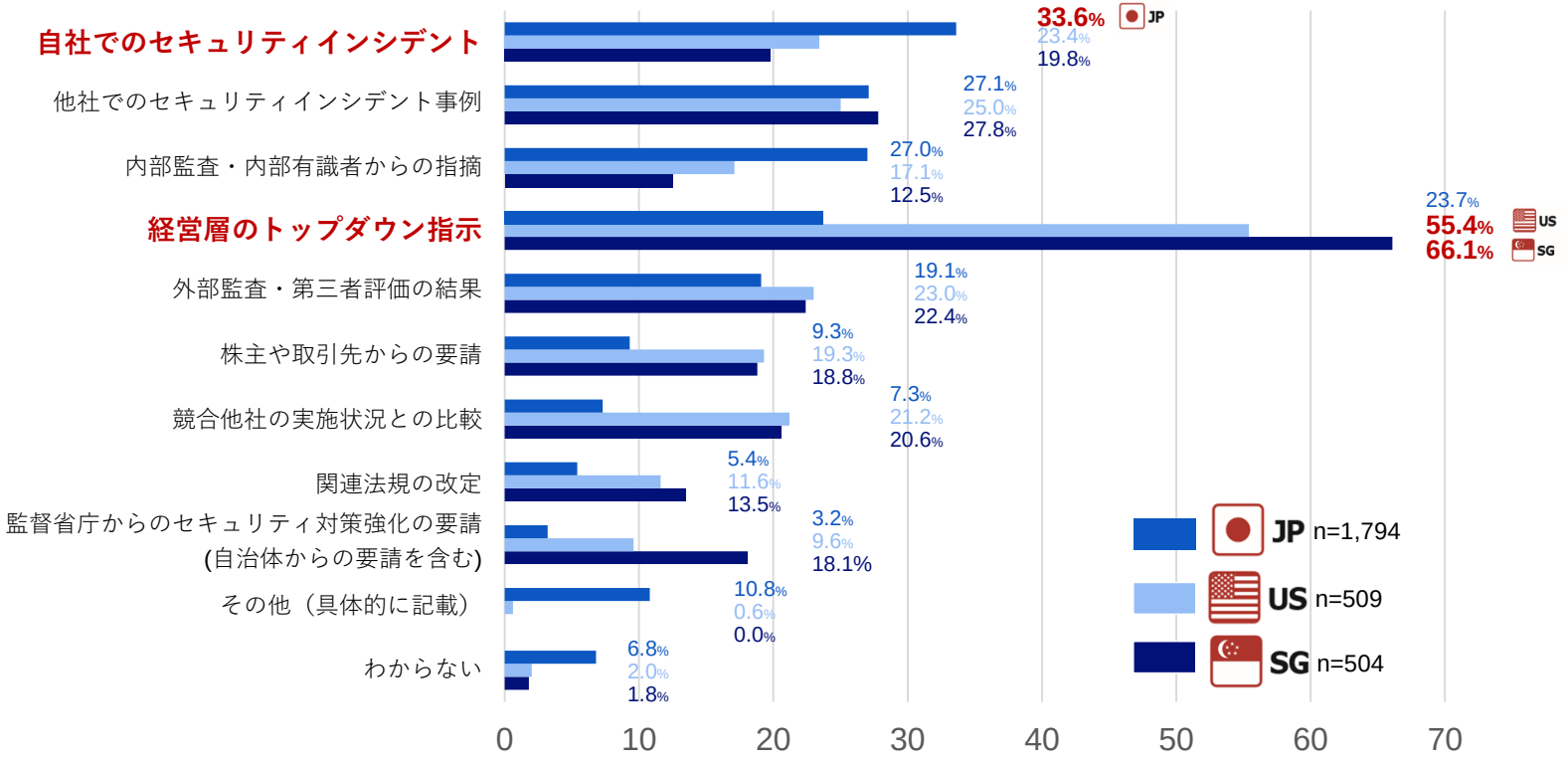
① 中長期（3年程度）計画をたて、年単位で適宜見直ししている
② 中長期計画を立てているが、見直ししていない
③ 直近1年以内の計画を立て、適宜見直ししている
④ 直近1年以内の計画を立てているが、見直ししていない
⑤ 今後計画を立てる予定である
⑥ 計画を立てる予定はない
⑦ その他
⑧ 分からない



中長期(3年程度)の計画を立てている企業の割合

日本企業における対策実施のきっかけは、自社でのインシデント発生がTOP

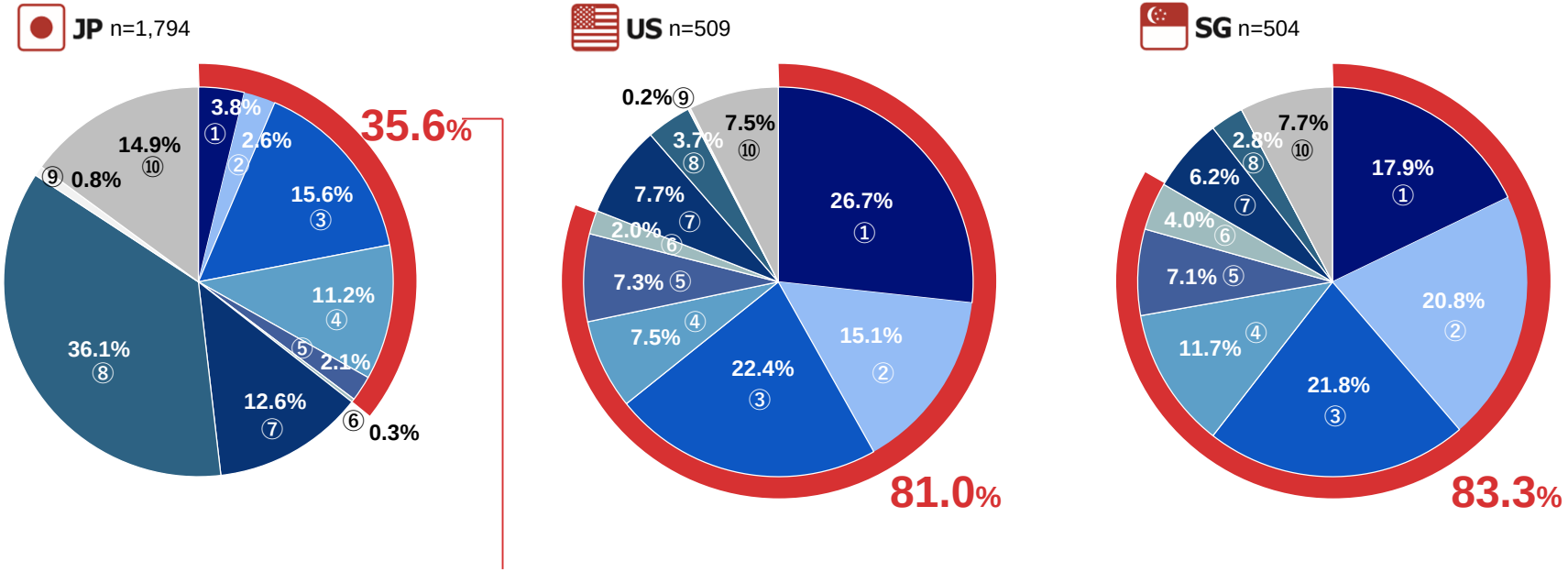
Q. 直近1年に実施した情報セキュリティ対策の実施のきっかけや理由はなんですか。（あてはまるものを最大3つ選択）



▶ 日本企業は他2カ国と比較して、CSIRTの構築が遅れている

Q. CSIRTの構築状況はいかがですか。

① 専任組織を構築済みで、有効に機能している
② 専任組織を構築済みだが、有効に機能していない
③ 兼任組織が類似機能を果たしており、有効に機能している
④ 兼任組織が類似機能を果たしているが、有効に機能していない
⑤ CSIRT運営は外部の業者に委託しており、有効に機能している
⑥ CSIRT運営は外部の業者に委託しているが、有効に機能していていない
⑦ 現在、検討中もしくは構築中である
⑧ 検討していない
⑨ その他
⑩ わからない



CSIRTを構築済みである企業の割合

V. 脅威・事故

~ Threats & Incidents ~

- 過去1年間で発生したインシデント
- ビジネスメール詐欺の被害状況

V. 脅威・事故：過去1年間で発生したインシデント (22項目中の上位10項目)

▶ 日本企業では、ヒューマンエラーに起因するインシデントが上位にランクイン

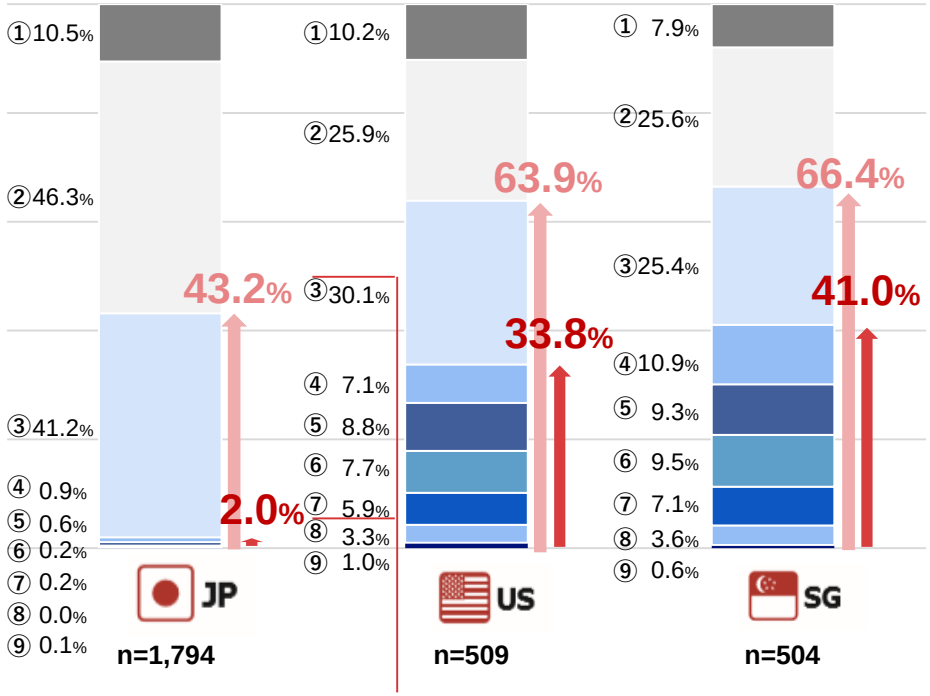
Q.過去1年間で発生した情報セキュリティに関する事件・事故はありますか。（あてはまるものを全て選択）

	ヒューマンエラー	JP n=1,794		US n=509		SG n=504	
1位	電子メール、FAX,郵便物等の誤送信・誤配信	29.4%		DoS攻撃／DDoS攻撃	30.6%	DoS攻撃／DDoS攻撃	36.5%
2位	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	22.6%		Webアプリケーションの脆弱性を突いた攻撃	29.9%	Webアプリケーションの脆弱性を突いた攻撃	29.6%
3位	マルウェア感染	22.5%		システム基盤の脆弱性を突いた攻撃	23.4%	自社サービスへのリスト型アカウントハッキング	25.8%
4位	システム設定ミス、誤操作	19.8%		自社サービスへのリスト型アカウントハッキング	21.8%	標的型メール攻撃	20.4%
5位	標的型メール攻撃	17.9%		マルウェア感染	19.8%	システム基盤の脆弱性を突いた攻撃	19.8%
6位	社員証、業務書類等物品の紛失・置き忘れ・棄損	16.9%		標的型メール攻撃	18.1%	マルウェア感染	17.3%
7位	情報機器、電子記憶媒体、紙媒体等の盗難・紛失	15.1%		水飲み場型攻撃	11.2%	水飲み場型攻撃	11.7%
8位	ランサムウェアによる金銭等の要求	11.6%		ランサムウェアによる金銭等の要求	9.0%	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	9.7%
9位	DoS攻撃／DDoS攻撃	6.5%		電子メール、FAX、郵便物等の誤送信・誤配送	8.3%	ランサムウェアによる金銭等の要求	8.5%
10位	退職者、転職者による在職時に利用していた情報の使用	4.0%		情報機器・外部記憶媒体の紛失・置き忘れ・棄損	7.5%	システム管理者（特権ユーザ）等による不正アクセスや持出	8.5%

V. 脅威・事故：ビジネスメール詐欺（BEC）の被害状況

▶ 日本企業において、金銭詐欺等のメールを受け取った割合は約40%、金銭被害は約2%

Q. 過去1年間で、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、金銭被害にあいましたか。



① わからない
② 会社に届いていないため、金銭被害にはあっていない
③ 役員・従業員に届いていたが、金銭被害にはあっていない
④ 金銭被害総額が、100万円未満
⑤ 金銭被害総額が、100万円～500万円未満
⑥ 金銭被害総額が、500万円～1000万円未満
⑦ 金銭被害総額が、1000万円～5000万円未満
⑧ 金銭被害総額が、5000万円～1億円未満
⑨ 金銭被害総額が、1億円以上（具体的に記載）

※アメリカとシンガポールにおいては 「$」 および 「SG$」 表記で調査

・ビジネスメール詐欺の攻撃メールを受け取った企業の割合
・実際に金銭被害にあった企業の割合

03. 総括

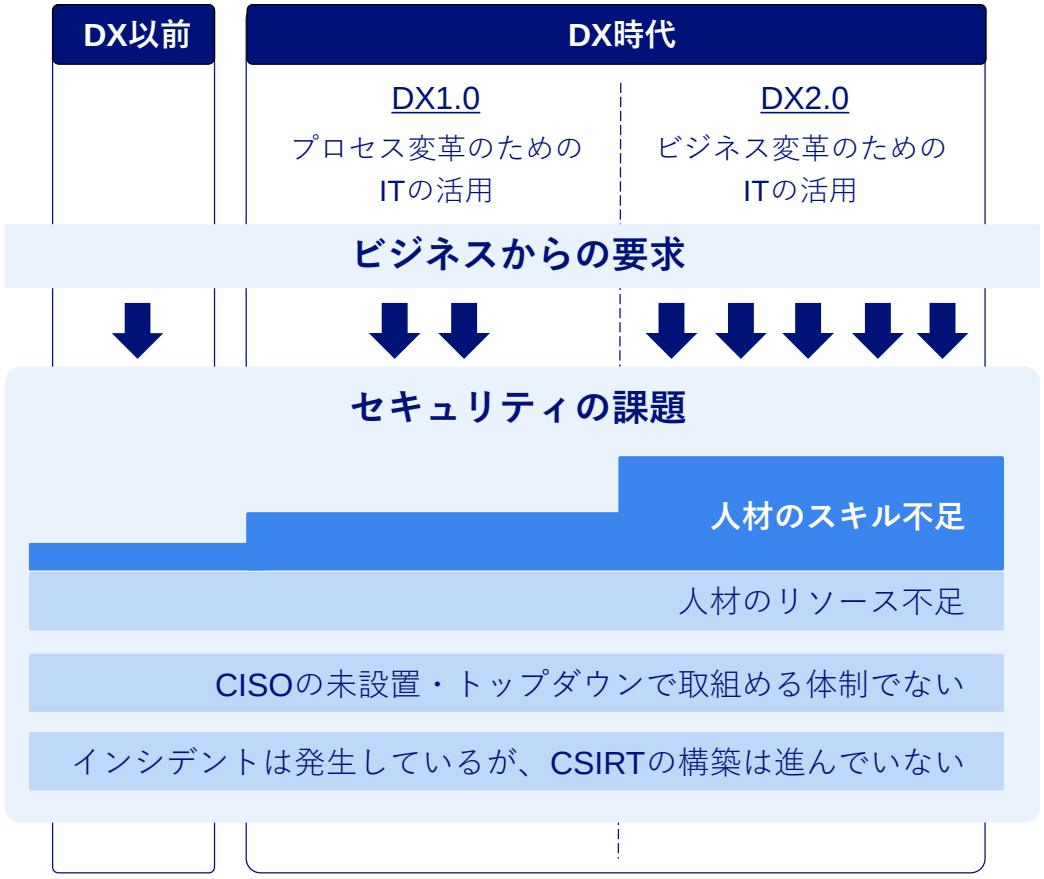
調査結果のまとめ

デジタルセキュリティ **~ Digital Security ~**	DX推進とDXのセキュリティ対策において、人員のスキル不足が課題
セキュリティマネジメント **~ Security Management ~**	CISOの設置率が低い / セキュリティに関する予算が少ない
セキュリティ人材 **~ Human Resources ~**	人材不足 / キャリアパスの未整備
セキュリティ対策 **~ Security Measures ~**	対策のきっかけは事故等の後追い / CSIRTの構築が遅れている
脅威・事故 **~ Threats & Incidents ~**	一定割合でインシデントが発生

提言

DX時代では、ビジネスのスピードと安全性の両立が必須
セキュリティを経営戦略として捉え、CISO主導によるセキュリティ事業の最適化が必要

人材のスキル不足が招く
セキュリティの遅れがビジネスの阻害要因に



セキュリティを経営戦略と捉えた
セキュリティ事業の最適化

CISOを設置
セキュリティにトップダウンで取組みつつ
ビジネス部門とも連携を図る

プロセス（Process）

ルール・体制の見直し
「全ての業務を自社の人手で実施する」
という発想から脱却

技術（Technology）

支援ツールの導入
セキュリティ対策だけでなく
業務を支援するツールも導入

人（People）

DXセキュリティ人材の育成
DX時代に求められるスキルを
習得するための機会の提供


Share the Next Values!