第300回NRIメディアフォーラム

企業が挑むニューノーマルなセキュリティ

企業における情報セキュリティ実態調査2020

セキュリティコンサルタント　山田 真暉

NRIセキュアテクノロジーズ株式会社
GRCプラットフォーム部

2020年12月15日

NRIセキュアテクノロジーズ

Share the Next Values!

01. 調査概要

日本 / アメリカ / オーストラリア 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 / オーストラリアの企業における、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：2020/7/1 ~ 2020/9/18
- アメリカ / オーストラリア：2020/8/1 ~ 2020/9/18

■ 調査方法

- Webによるアンケート

■ 調査対象

- 日本 / アメリカ / オーストラリア 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：1,222社 / アメリカ：523社 / オーストラリア：515社

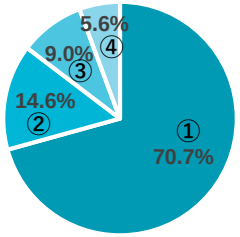
（参考：昨年の調査における日本の回答数　2019年版： 1,794社）

回答企業の内訳

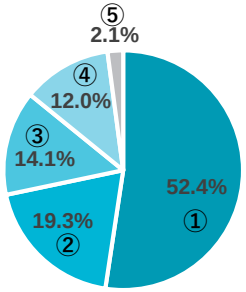
回答企業の従業員数

■ ① ~千人未満　■ ② 千人~3千人未満
■ ③ 3千人~5千人未満　■ ④ 5千人以上
■ ⑤ 不明

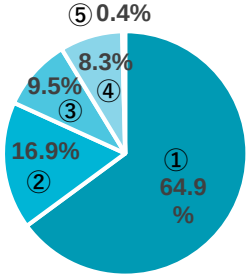
日本
n=1,222



米国
n=523

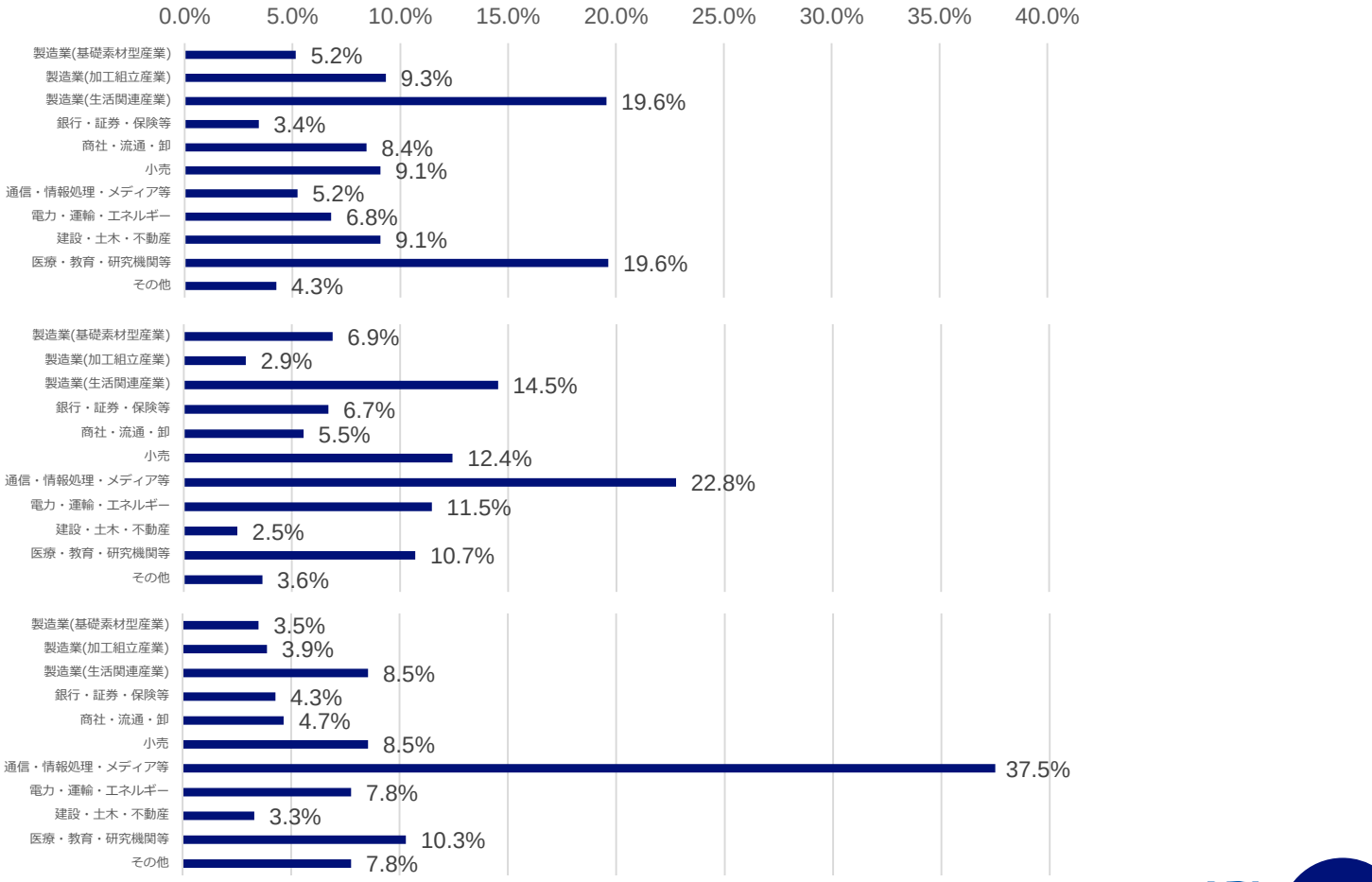


豪州
n=515



回答企業の業種

※ 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つのテーマについて調査

I. デジタルトランスフォーメーション(DX)

DXの取組みに関わるセキュリティ対応

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の充足状況

IV. セキュリティ対策

セキュリティ対策状況やサプライチェーンへの対応状況

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. デジタルトランスフォーメーション

~ Digital transformation ~

- DXへの取組み状況と阻害要因
- DXに伴うセキュリティ戦略の見直し状況
- テレワーク導入率と、それに伴うセキュリティへの対応状況

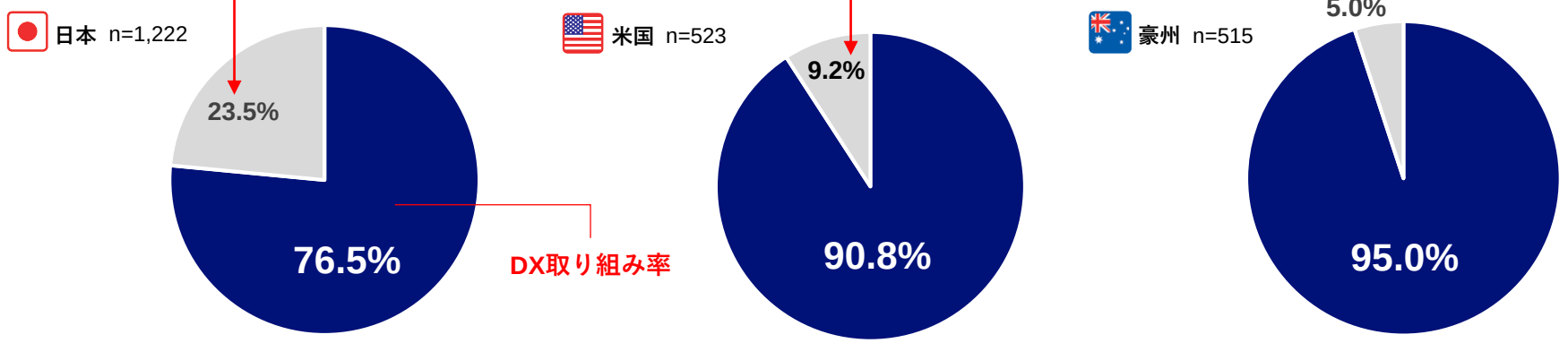
I. デジタルトランスフォーメーション：DXへの取組み状況と阻害要因

DXへの取り組み阻害要因は各国に共通事項があった
日本企業のDXへの取り組み率は76.5%

Q.デジタルトランスフォーメーションの取り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）

※「課題はない」「デジタルトランスフォーメーションには取り組んでいない」を選択した場合は、他の選択肢の回答不可とし、他は複数選択。

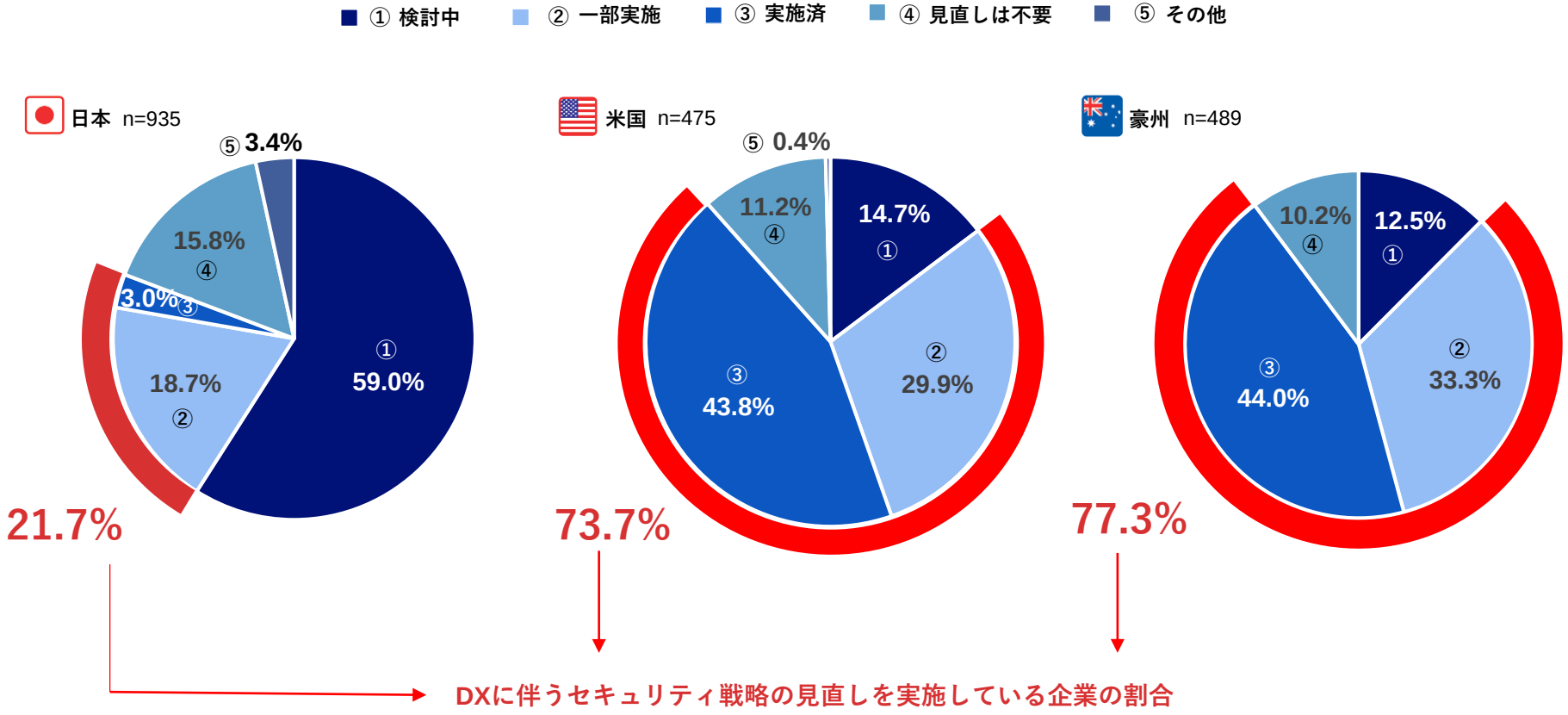
	日本 n=1,222		米国 n=523		豪州 n=515	
1位	新技術に対する理解や実装する能力を有した人員やリソースの確保	54.5%	新技術に対する理解や実装する能力を有した人員やリソースの確保	42.1%	新技術に対する理解や実装する能力を有した人員やリソースの確保	44.2%
2位	情報セキュリティへの対応	32.4%	変化を受け入れる企業風土がない	28.2%	縦割りの組織構造	26.2%
3位	変化を受け入れる企業風土がない	31.8%	情報セキュリティへの対応	26.5%	情報セキュリティへの対応	25.6%
4位	DXに対する経営の理解	28.0%	縦割りの組織構造	25.3%	変化を受け入れる企業風土がない	22.1%
5位	縦割りの組織構造	24.8%	DXに対する経営の理解	14.5%	DXに対する経営の理解	15.1%
6位	デジタルトランスフォーメーションには取り組んでいない	23.5%	デジタルトランスフォーメーションには取り組んでいない	9.2%	課題はない	12.5%
7位	課題はない	16.3%	課題はない	7.8%	デジタルトランスフォーメーションには取り組んでいない	5.0%
8位	その他	2.5%	その他	0.8%	その他	0.6%



I. デジタルトランスフォーメーション：DXに伴うセキュリティ戦略の見直し状況

▶ 日本はDXに伴うセキュリティに対応している企業が約20%

Q.デジタルトランスフォーメーションの取り組みを進めるにあたって、自社のセキュリティ戦略やルール、プロセスの見直しを行っていますか。



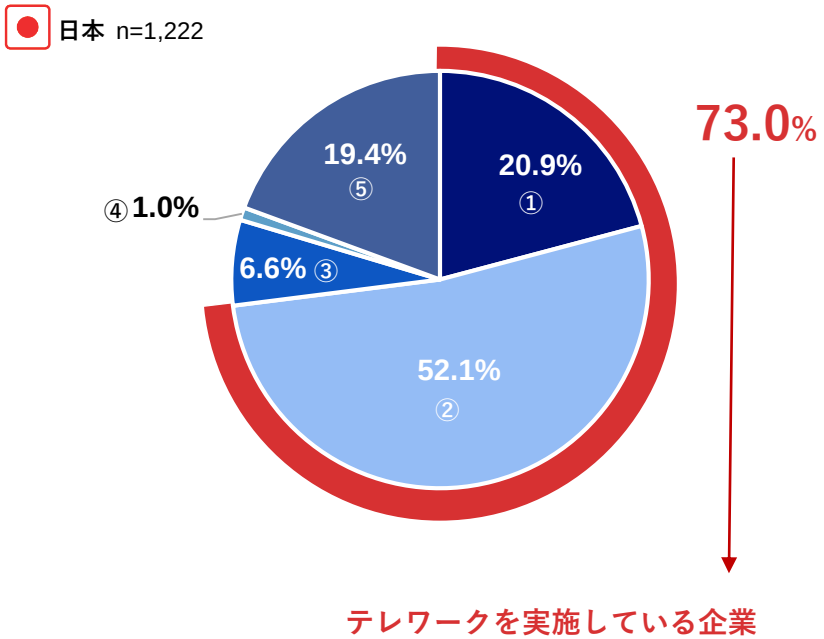
※「デジタルトランスフォーメーションには取り組んでいない」と回答した企業は除く。

I. デジタルトランスフォーメーション：テレワーク導入率と、それに伴うセキュリティへの対応状況

▶ 日本企業のテレワークの導入率は73%、テレワークに伴うセキュリティに対応している企業は約55%

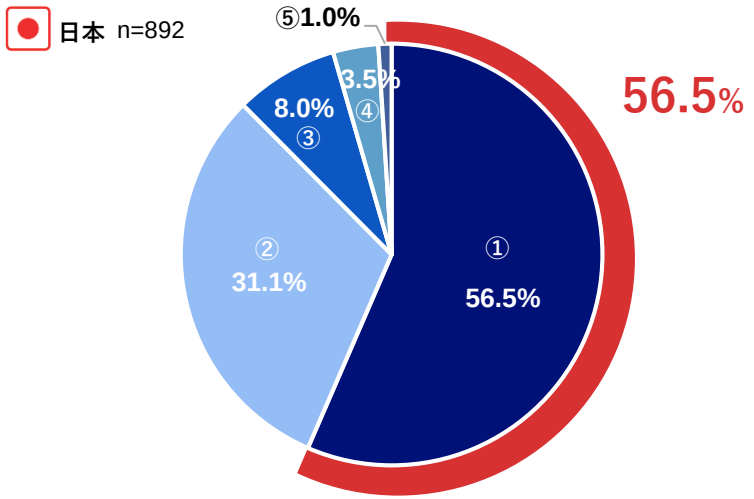
Q. テレワークの実施状況を教えてください。

■ ① COVID-19以前より、テレワークを実施していた
■ ② COVID-19以降に、テレワークを実施しはじめた
■ ③ テレワークの実施を検討している
■ ④ その他
■ ⑤ テレワークは実施していない



Q. テレワーク実施に伴う、セキュリティへの対応状況を教えてください

■ ① テレワークに伴うセキュリティ要件を把握し、対策を行っている
■ ② テレワークに伴うセキュリティ要件を把握しているが、対策を行えていない
■ ③ テレワークに伴うセキュリティ要件を把握してない
■ ④ わからない
■ ⑤ その他



※テレワークを実施中の企業のみ回答。

II. セキュリティマネジメント

~ Security Management ~

- セキュリティ関連予算
- セキュリティガイドラインの利用状況

▶ 日本はセキュリティ関連予算に変化がない企業が約50%、増額傾向が約30%

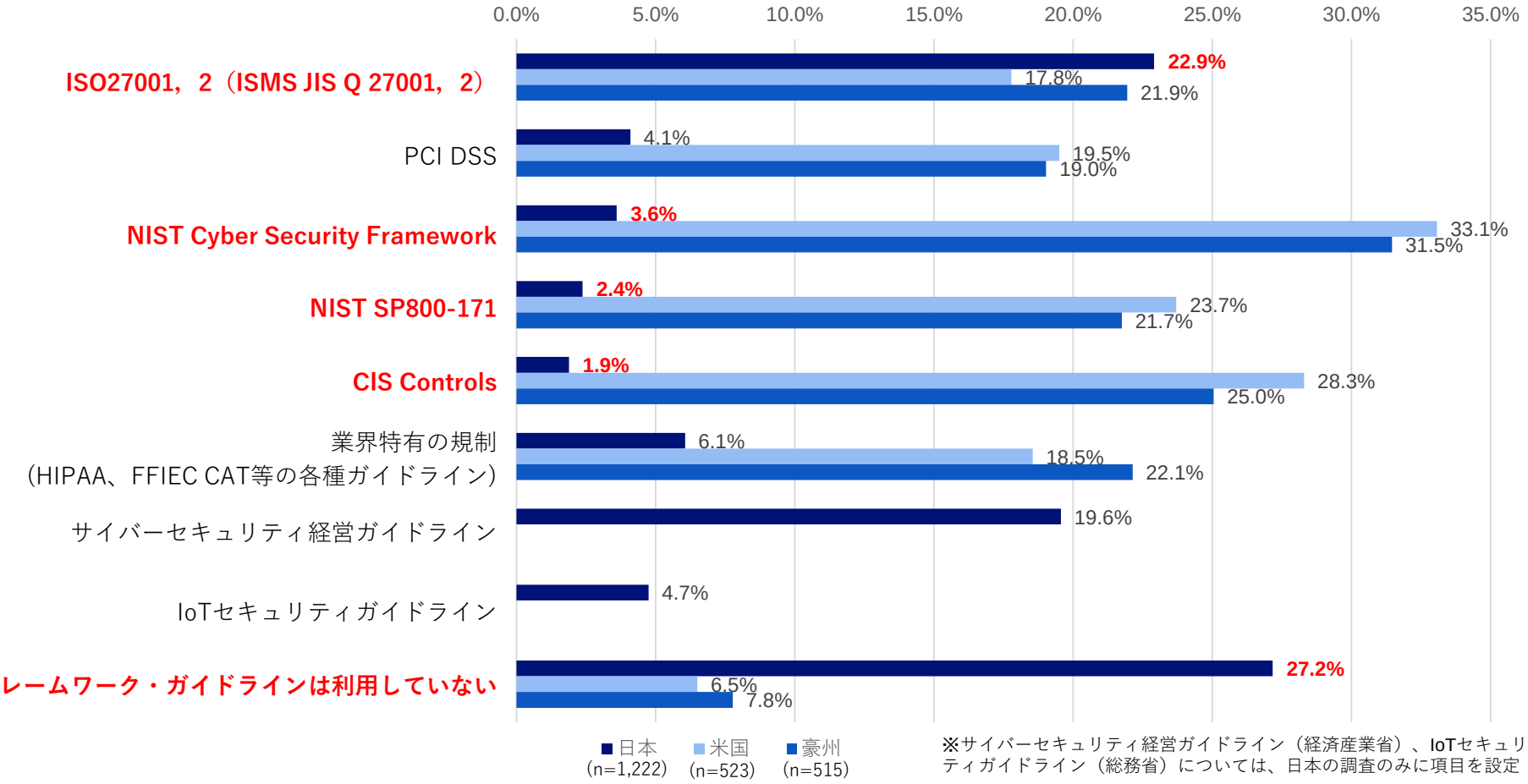
増加　変化なし　減少

Q. IT関連予算に対する情報セキュリティ関連予算は昨年度と比べて変化はありますか。

	日本 n=1,222	米国 n=523	豪州 n=515
1位	セキュリティ関連予算に変化はない **48.4%**	COVID-19とは関係なく、セキュリティ関連予算は減額した、または減額する見込み **26.6%**	COVID-19によって、セキュリティ関連予算は増額した、または増額する見込み **36.3%**
2位	COVID-19によって、セキュリティ関連予算は増額した、または増額する見込み **15.2%**	**26.0%**	COVID-19とは関係なく、セキュリティ関連予算は減額した、または減額する見込み **21.6%**
3位	わからない **13.3%**	COVID-19によって、セキュリティ関連予算は減額した、または減額する見込み **22.2%**	**18.3%**
4位	COVID-19とは関係なく、セキュリティ関連予算は増額した、または増額する見込み **12.1%**	**14.1%**	**10.9%**
5位	COVID-19によって、セキュリティ関連予算は減額した、または減額する見込み **8.3%**	セキュリティ関連予算に変化はない **8.6%**	**9.9%**
6位	COVID-19とは関係なく、セキュリティ関連予算は減額した、または減額する見込み **2.5%**	わからない **2.5%**	**3.1%**

▶ 日本企業が利用するガイドラインには特徴があった

Q.情報セキュリティに係る戦略策定や自社・グループのルール・ガイドライン策定の際に利用するフレームワーク、ガイドラインを教えてください。(あてはまるものを全て選択)



※サイバーセキュリティ経営ガイドライン（経済産業省）、IoTセキュリティガイドライン（総務省）については、日本の調査のみに項目を設定

III. セキュリティ人材

~ Human Resources ~

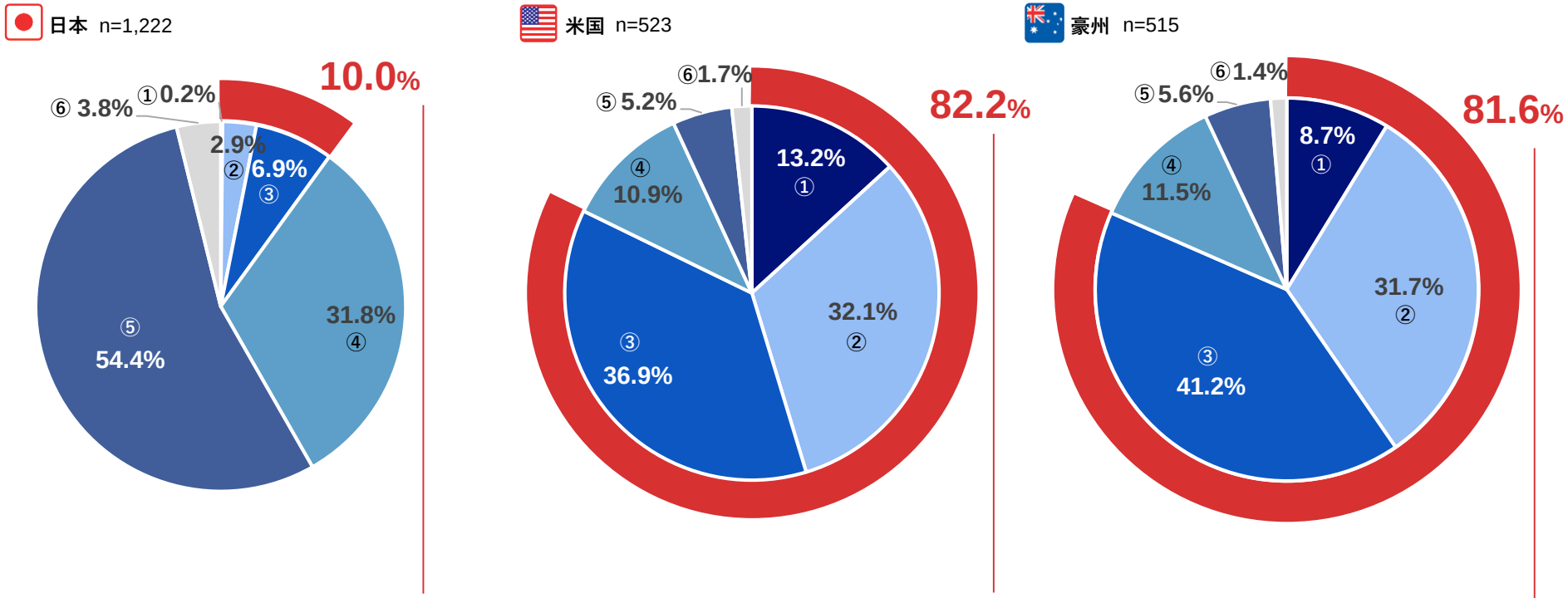
- セキュリティ人材の充足状況
- 充足していると考える理由
- 不足してる人材の種別

▶ 日本企業は米/豪と比べて圧倒的に人材不足を訴えている

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

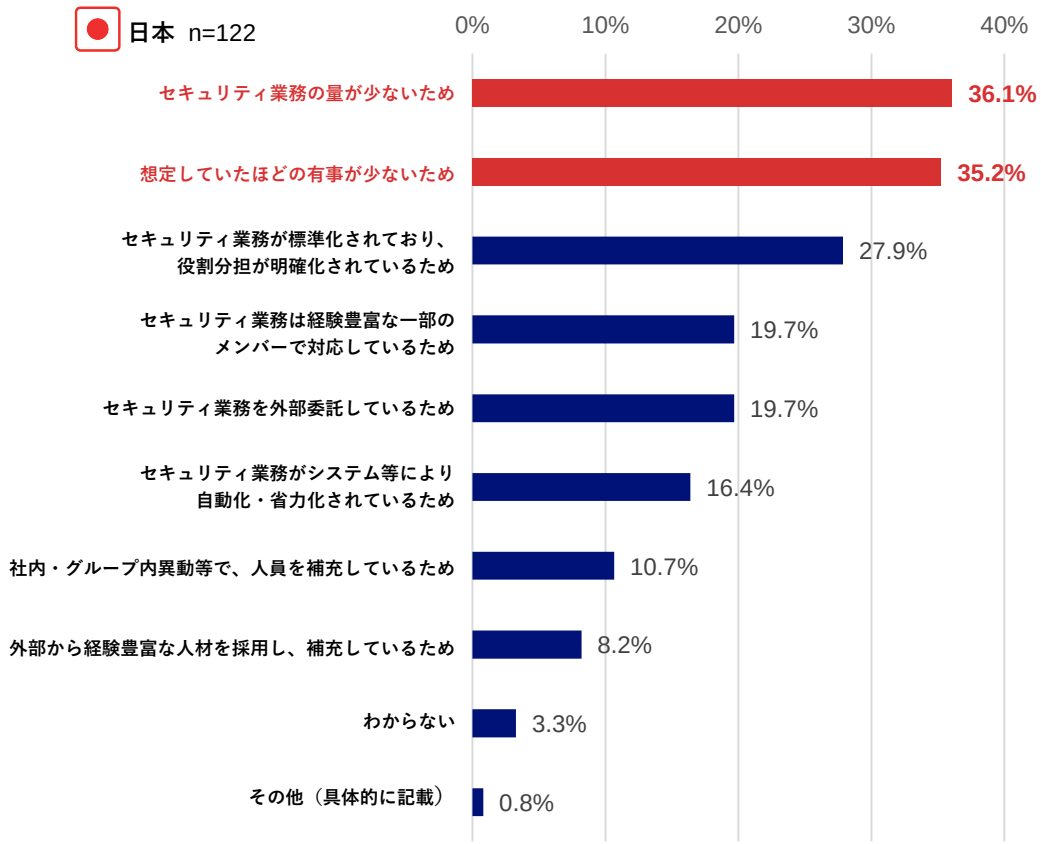


セキュリティ人材が「充足している」と感じている企業の割合

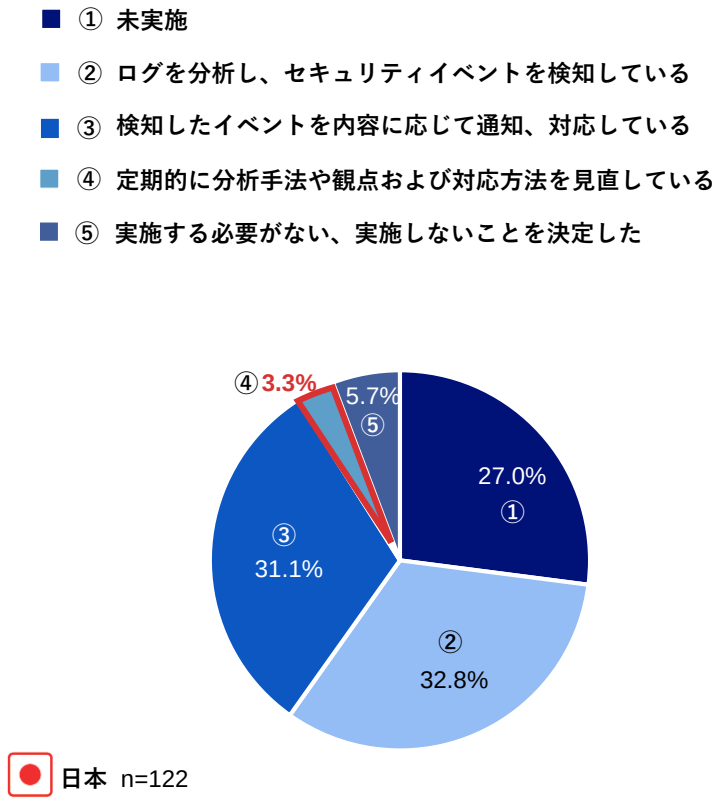
III. セキュリティ人材：充足していると考える理由

▶ 「充足している」と考える理由の見直しが求められる

Q. 人材が充足していると考える理由は何ですか。
（あてはまるものを最大３つ選択）



Q.ログを分析し、不審な挙動があった場合は担当者に通知するなどの対応をしていますか。

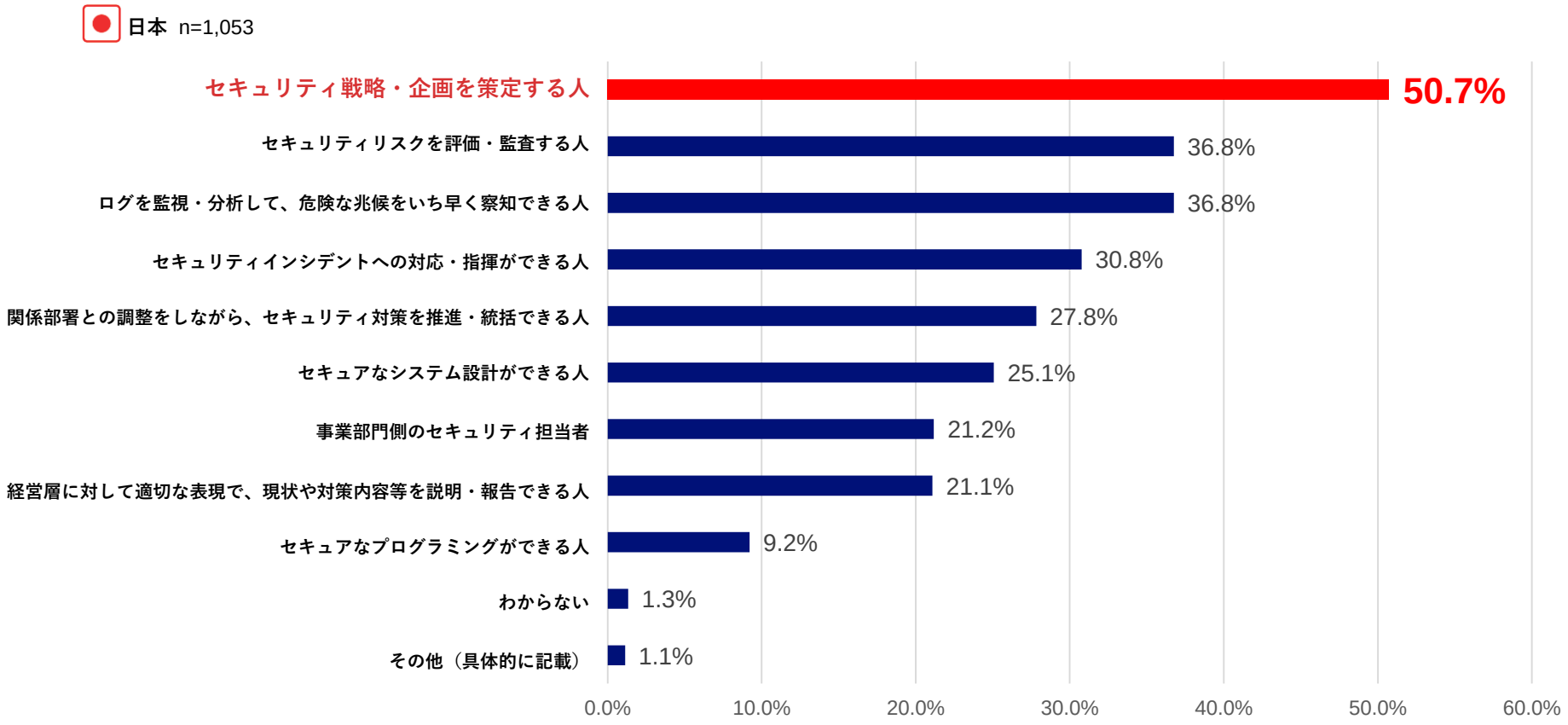


※セキュリティ人材が、「人材が過剰な状態」「充足している」「どちらかと言えば充足している」と回答した企業が対象

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

IV. セキュリティ対策

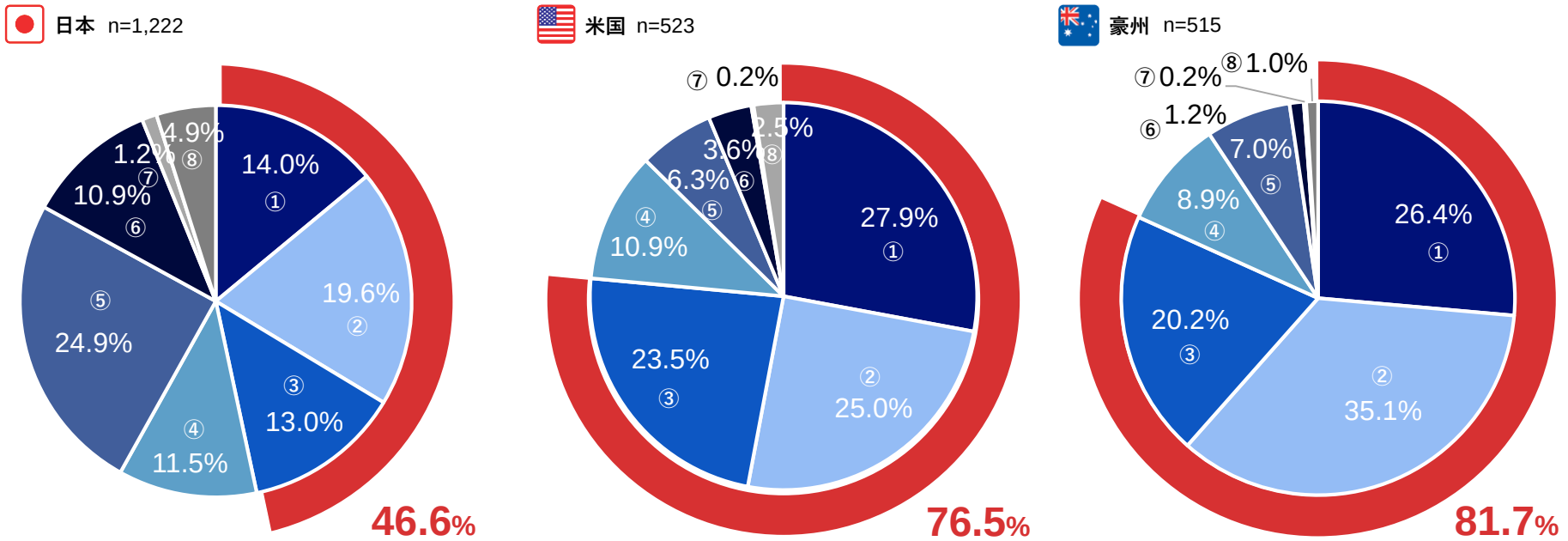
~ Security Measures ~

- セキュリティ対策状況の把握
- サプライチェーンにおけるセキュリティ対策状況

▶ 日本企業は他2ヶ国と比較して、セキュリティ対策評価を定期的に実施している割合が低い

Q.定期的にセキュリティ対策の実施状況を評価し、足りていない対策を把握していますか。

① セキュリティベンダや監査法人などの第三者評価を定期的に実施している
② 自己評価を定期的に実施している
③ 第三者評価および自己評価をいずれも定期的に実施している
④ 今後定期的に評価を実施する予定である
⑤ 不定期に評価を実施している
⑥ いずれも実施する予定はない
⑦ その他（具体的に記載）
⑧ わからない

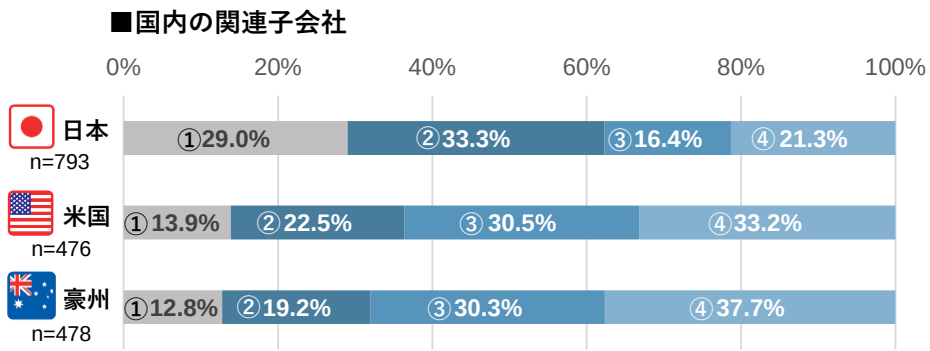


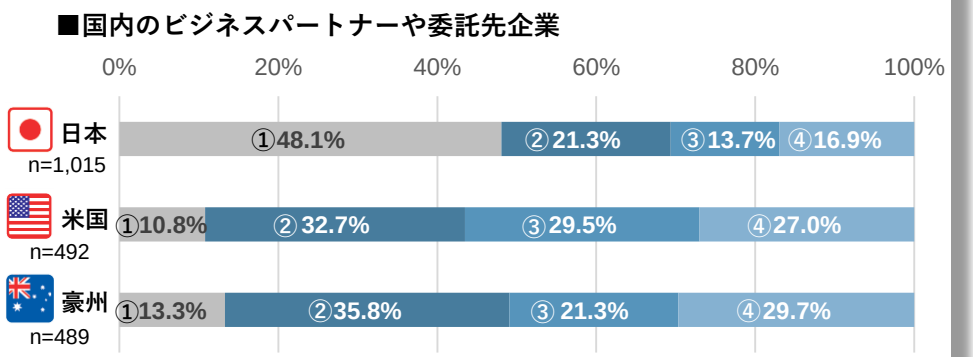
IV. セキュリティ対策：サプライチェーンにおけるセキュリティ対応状況

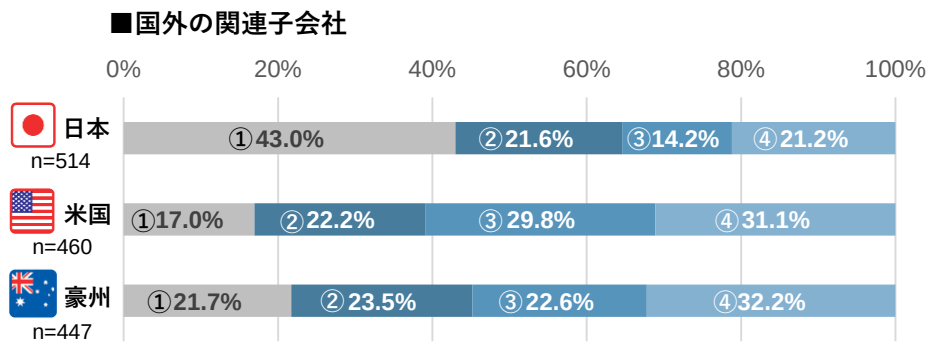
▶ 日本企業は他2ヶ国と比較して、サプライチェーンのセキュリティ対策が遅れている

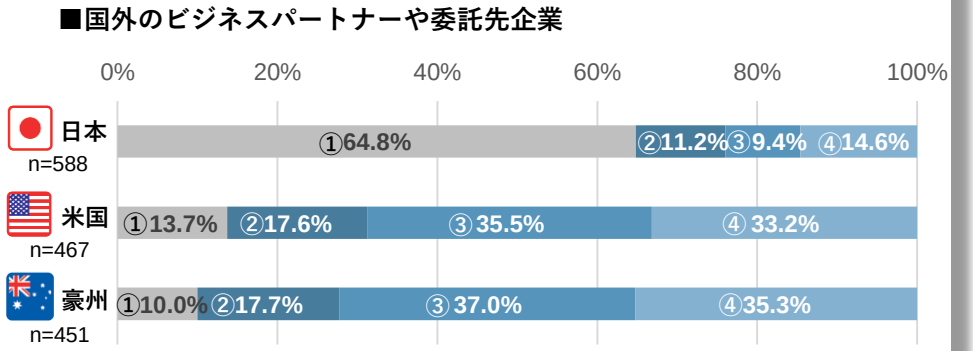
Q.サプライチェーンにおけるセキュリティの対応状況についてお答えください。

① セキュリティ対策状況を把握していない　② セキュリティ対策状況を把握している
③ セキュリティ対策状況を把握し、自社の水準をみたすため改善を要求している　④ セキュリティ対策状況が改善されていることを定期的に確認している









※セキュリティ統制の対象となる、関連子会社、ビジネスパートナーと委託先企業が存在する企業のみ回答。

V. 脅威・事故

~ Threats & Incidents ~

- 過去1年間で発生したインシデント
- 最も脅威と感じる事象

各国共通してサイバー攻撃によるインシデントが多くランクイン

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）

サイバー攻撃	日本 n=1,222		米国 n=523		豪州 n=515	
1位	特に無し	40.8%	DoS攻撃／DDoS攻撃	41.3%	DoS攻撃／DDoS攻撃	36.3%
2位	電子メール、FAX,郵便物等の誤送信・誤配信	21.9%	Webアプリケーションの脆弱性を突いた攻撃	37.7%	Webアプリケーションの脆弱性を突いた攻撃	31.8%
3位	標的型メール攻撃	16.3%	システム基盤の脆弱性を突いた攻撃	23.5%	自社サービスへのリスト型アカウントハッキング	25.4%
4位	マルウェア感染	14.4%	自社サービスへのリスト型アカウントハッキング	22.0%	標的型メール攻撃	18.8%
5位	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	13.7%	標的型メール攻撃	16.1%	システム基盤の脆弱性を突いた攻撃	18.6%
6位	システム設定ミス、誤操作	12.1%	水飲み場型攻撃	11.7%	マルウェア感染	14.6%
7位	社員証、業務書類等物品の紛失・置き忘れ・棄損	10.2%	ランサムウェアによる金銭等の要求	11.1%	特に無し	13.6%
8位	情報機器、電子記憶媒体、紙媒体等の盗難・紛失	10.1%	マルウェア感染	9.8%	水飲み場型攻撃	12.2%
9位	ランサムウェアによる金銭等の要求	6.2%	データ通信、音声通信等の盗聴・傍受	9.6%	ランサムウェアによる金銭等の要求	11.3%
10位	DoS攻撃／DDoS攻撃	4.2%	システム設定ミス、誤操作	9.4%	廃棄された電子記憶媒体等からのデータ復元による情報漏えい	10.1%

▶ 各国共通して標的型攻撃、ランサムウェアによる被害を脅威と感じている

Q.情報セキュリティに関する脅威について、対策実施状況に関わらず、自社で最も脅威となる事象は何ですか。
（あてはまるものを最大３つ選択）

	日本 n=1,222		米国 n=523		豪州 n=515	
1位	標的型攻撃による情報漏えい	54.3%	ランサムウェアによる被害(情報消失、金銭被害)	25.4%	標的型攻撃による情報漏えい	27.8%
2位	ランサムウェアによる被害(情報消失、金銭被害)	52.7%	サービス妨害攻撃(DDoS攻撃等)によるサービス停止	24.7%	ランサムウェアによる被害(情報消失、金銭被害)	25.8%
3位	内部不正による被害(情報漏えい、業務停止)	46.1%	標的型攻撃による情報漏えい	24.3%	ビジネスメール詐欺(BEC)による金銭被害	21.6%
4位	メールの誤送信・誤配信	25.3%	ビジネスメール詐欺(BEC)による金銭被害	22.9%	サービス妨害攻撃(DDoS攻撃等)によるサービス停止	21.4%
5位	ビジネスメール詐欺(BEC)による金銭被害	18.6%	自社Webサービスへのリスト型アカウントハッキングによる被害(情報漏えい、サービス停止)	18.0%	Webサイトの改ざん	21.0%
6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	17.8%	Webサイトの改ざん	16.6%	自社Webサービスへのリスト型アカウントハッキングによる被害(情報漏えい、サービス停止)	15.9%
7位	情報機器、社員証等の置き忘れ、棄損による情報漏えい	13.9%	内部不正による被害(情報漏えい、業務停止)	11.5%	メールの誤送信・誤配信	15.3%
8位	サービス妨害攻撃(DDoS攻撃等)によるサービス停止	11.8%	顧客向けに提供している自社製品のセキュリティ侵害	10.5%	情報機器、社員証等の置き忘れ、棄損による情報漏えい	14.4%
9位	Webサイトの改ざん	8.1%	メールの誤送信・誤配信	9.9%	退所者、転職者に利用していた情報の使用	12.4%
10位	SaaS(ストレージサービス、チャット、web会議ツール等)利用からの情報漏えい	7.7%	SaaS(ストレージサービス、チャット、web会議ツール等)利用からの情報漏えい	9.0%	内部不正による被害(情報漏えい、業務停止)	11.7%

03. 総括

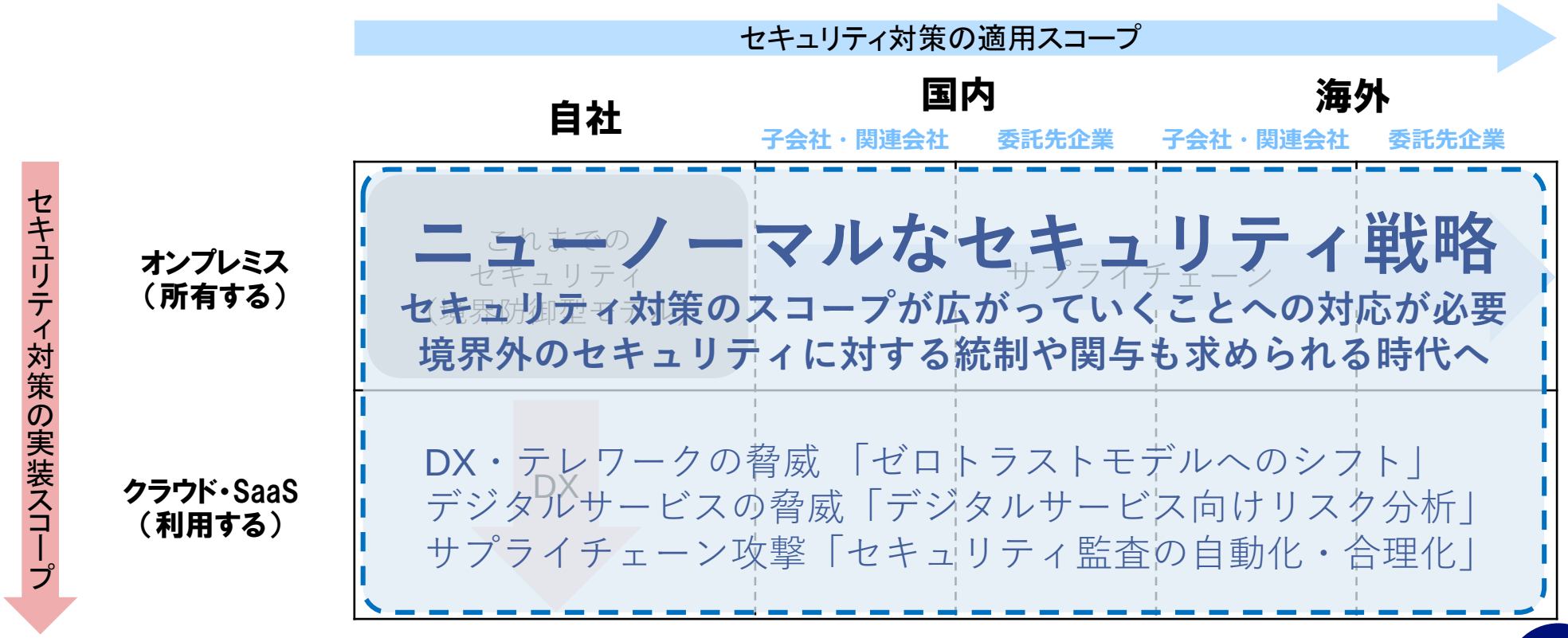
調査結果のまとめ

デジタルトランスフォーメーション ~ Digital Transformation ~	DXに伴うセキュリティの対応状況が遅れている
セキュリティマネジメント ~ Security Management ~	セキュリティ予算は維持ないし増額の傾向にある
セキュリティ人材 ~ Human Resources ~	人材不足の根本的な解消には、これまでの前提や慣習の見直しが必要
セキュリティ対策 ~ Security Measures ~	サプライチェーンにおけるセキュリティ対応状況が遅れている
脅威・事故 ~ Threats & Incidents ~	標的型攻撃、ランサムウェアを脅威と感じている

03 総括

DX時代の企業は、IT利活用やセキュリティ脅威のトレンドを踏まえた上で、セキュリティ戦略を再考すべき

これまで	2020年のセキュリティ脅威	これから
企業がコントロール可能なオンプレミスに境界を作り境界内で、セキュリティを担保	**絶え間ないサプライチェーン攻撃** ラテラルムーブメントで本社におよぶ脅威 **DXの進展に伴うセキュリティ事故** デジタルサービスでの金銭被害や情報漏えい **COVID-19で一気に広まったテレワーク** 自宅などオフィス外でのインシデント対応	2021年以降も、サプライチェーンを狙うサイバー攻撃やDX・テレワークの進展に伴うセキュリティ脅威は増す




Share the Next Values!