第325回NRIメディアフォーラム

ビジネスもセキュリティも拡がる時代
キーワードは３つのeXtend（拡張）

企業における情報セキュリティ実態調査2021

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プラットフォーム部

2022年2月8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

I. ゼロトラストセキュリティ
II. セキュリティマネジメント
III. セキュリティ人材
IV. セキュリティ対策
V. 脅威・事故

03 総括

※ゼロトラストセキュリティ：社内外のネットワーク環境における、従来の「境界」の概念を捨て去り、守るべき情報資産にアクセスするものはすべて信用せずに検証することで、情報資産への脅威を防ぐという、セキュリティの新しい考え方

01. 調査概要

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：2021/10/11 ~ 2021/11/26
- アメリカ / オーストラリア：2021/10/25 ~ 2021/11/5

■ 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

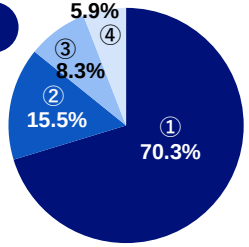
- 日本：1,616社 / アメリカ：511社 / オーストラリア：526社

回答企業の内訳

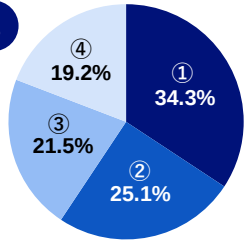
回答企業の従業員数

- ①~千人未満
- ②千人~2千人未満
- ③2千人~5千人未満
- ④5千人以上

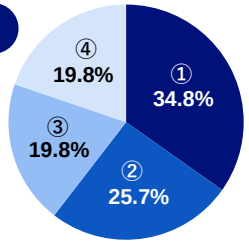
JP
n=1,616



US
n=511

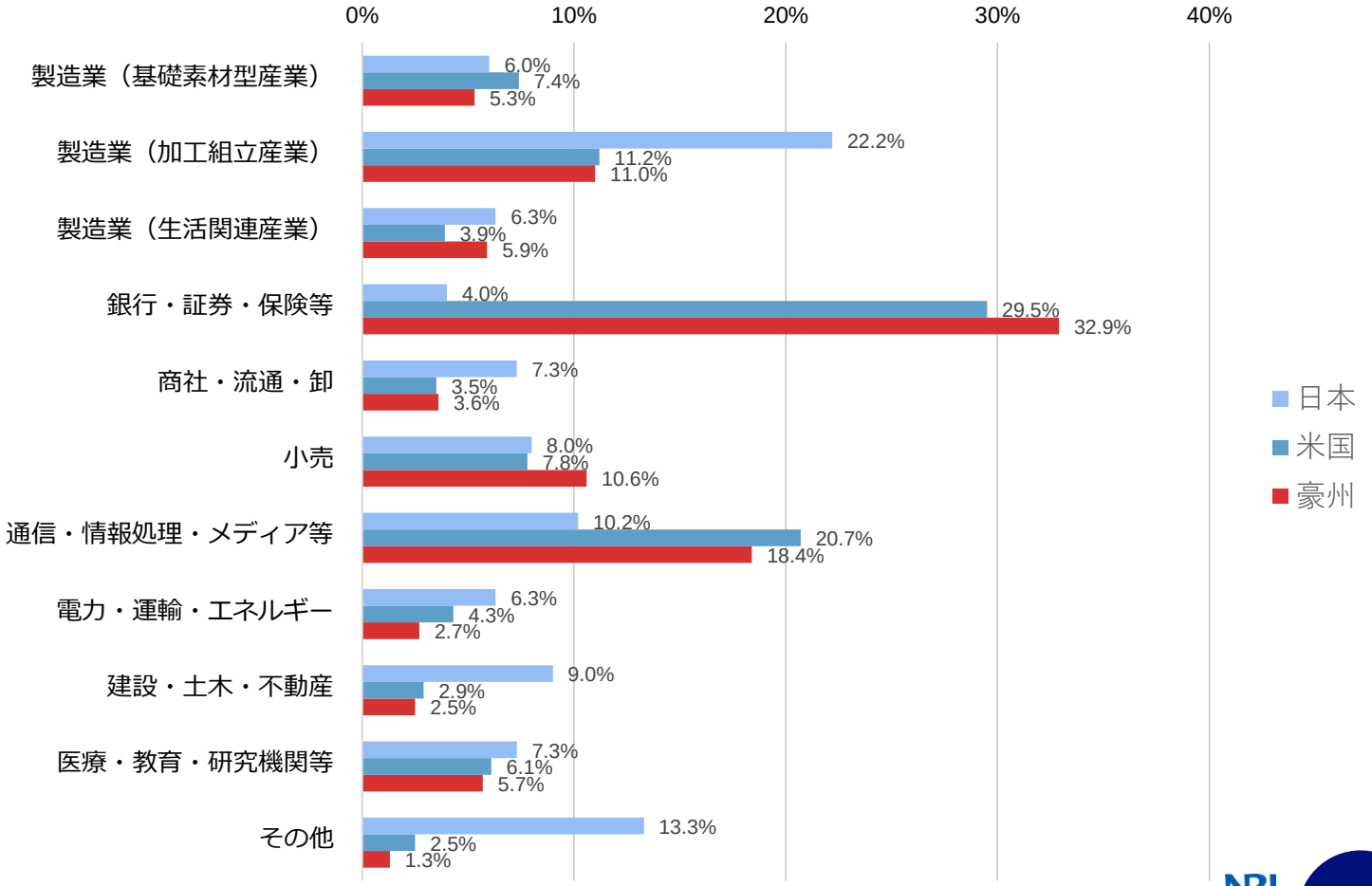


AU
n=526



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）：金属、化学、紙・パルプ、その他素材・素材加工品
- 製造業（加工組立産業）：機械・電気製品、輸送機器・部品製造、その他製品製造
- 製造業（生活関連産業）：バイオ・医薬品、繊維・アパレル、食品
- 銀行・証券・保険等：銀行、証券、保険、その他の金融
- 通信・情報処理・メディア等：システム・ソフトウェア開発、通信、メディア・広告、その他情報処理
- 電力・運輸・エネルギー：鉄道・航空、運輸、エネルギー
- 建設・土木・不動産：建設、不動産
- 医療・教育・医療、飲食、教育、法人サービス、消費者サービス



5つのテーマについて調査

I. ゼロトラストセキュリティ

DX時代に適したセキュリティモデル

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

自社やサプライチェーンにおけるセキュリティの対応状況

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. ゼロトラストセキュリティ

~ Zero Trust Security ~

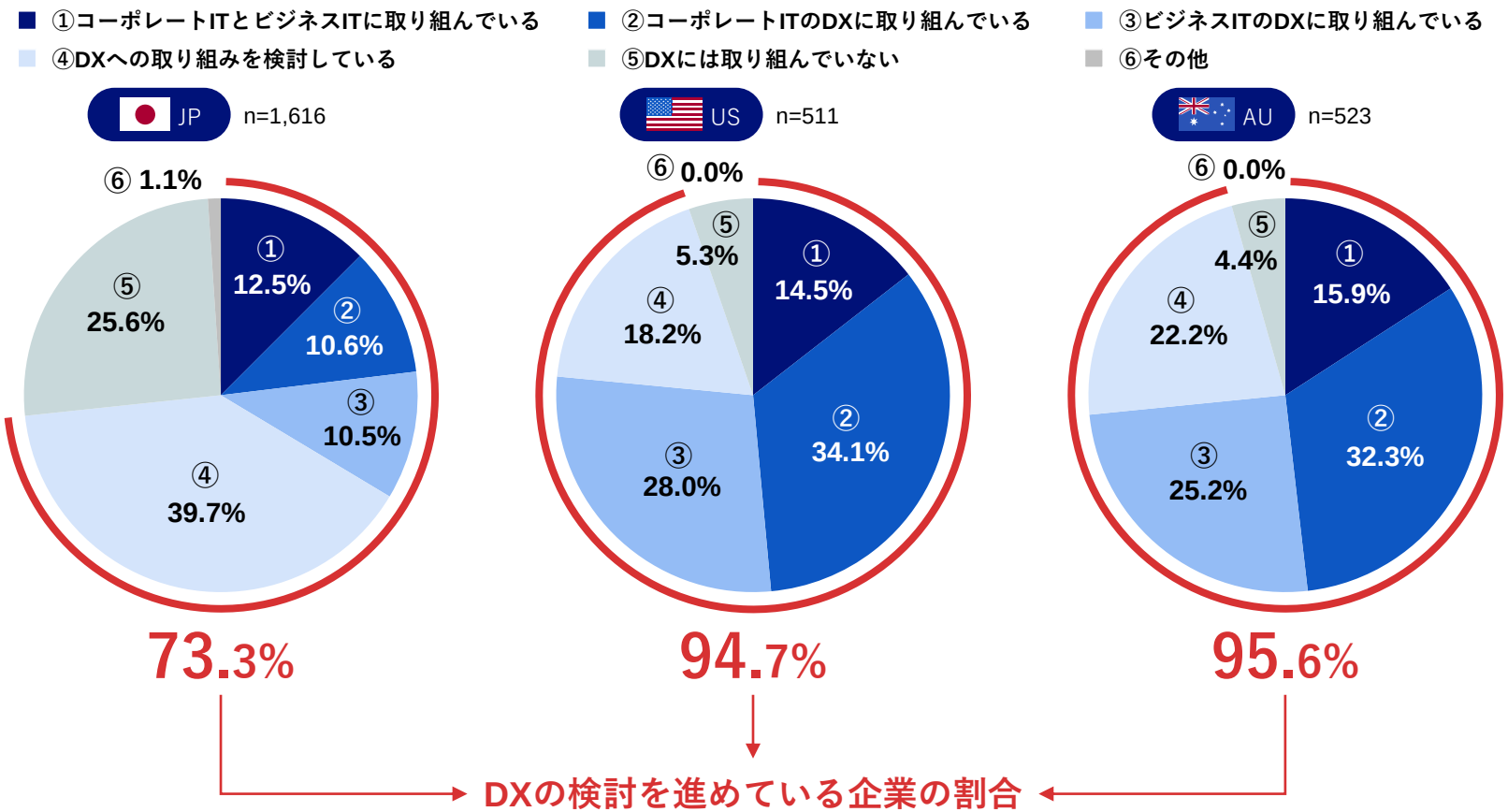
- DXへの取組み状況
- テレワーク環境における今後の構想
- ソリューションの導入状況

I. ゼロトラストセキュリティ：DXへの取組み状況

▶ DXの検討を進めている日本企業は約73%であった

Q デジタルトランスフォーメーションの取り組み状況を教えてください。

※コーポレートIT：自組織の業務プロセスで利用する内部向けのITシステム（基幹業務、経理、人事システム等）
※ビジネスIT：自組織の事業やビジネスで利用する外部向けのITシステム（オンラインショッピングサイトやスマホアプリ等



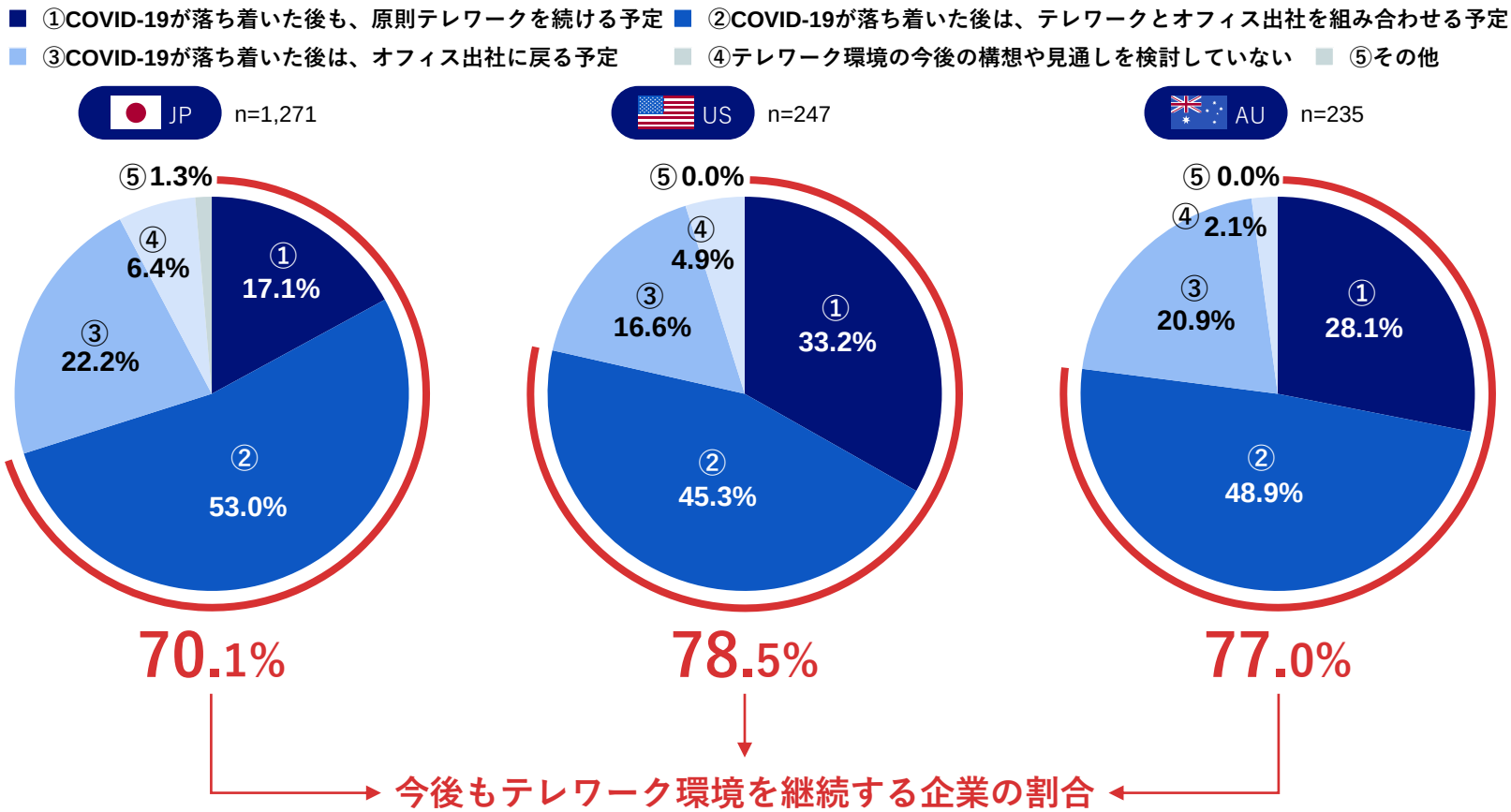
※少数の切上げ/切捨てにより、選択肢の合計値が100%にならない場合があります

I. ゼロトラストセキュリティ：テレワーク環境における今後の構想

▶ COVID-19後もテレワーク環境を維持する予定の日本企業は約70%であった

Q.テレワーク環境に関する今後の構想や見通しについて教えてください。

※「テレワークを実施している」と回答した企業が対象。

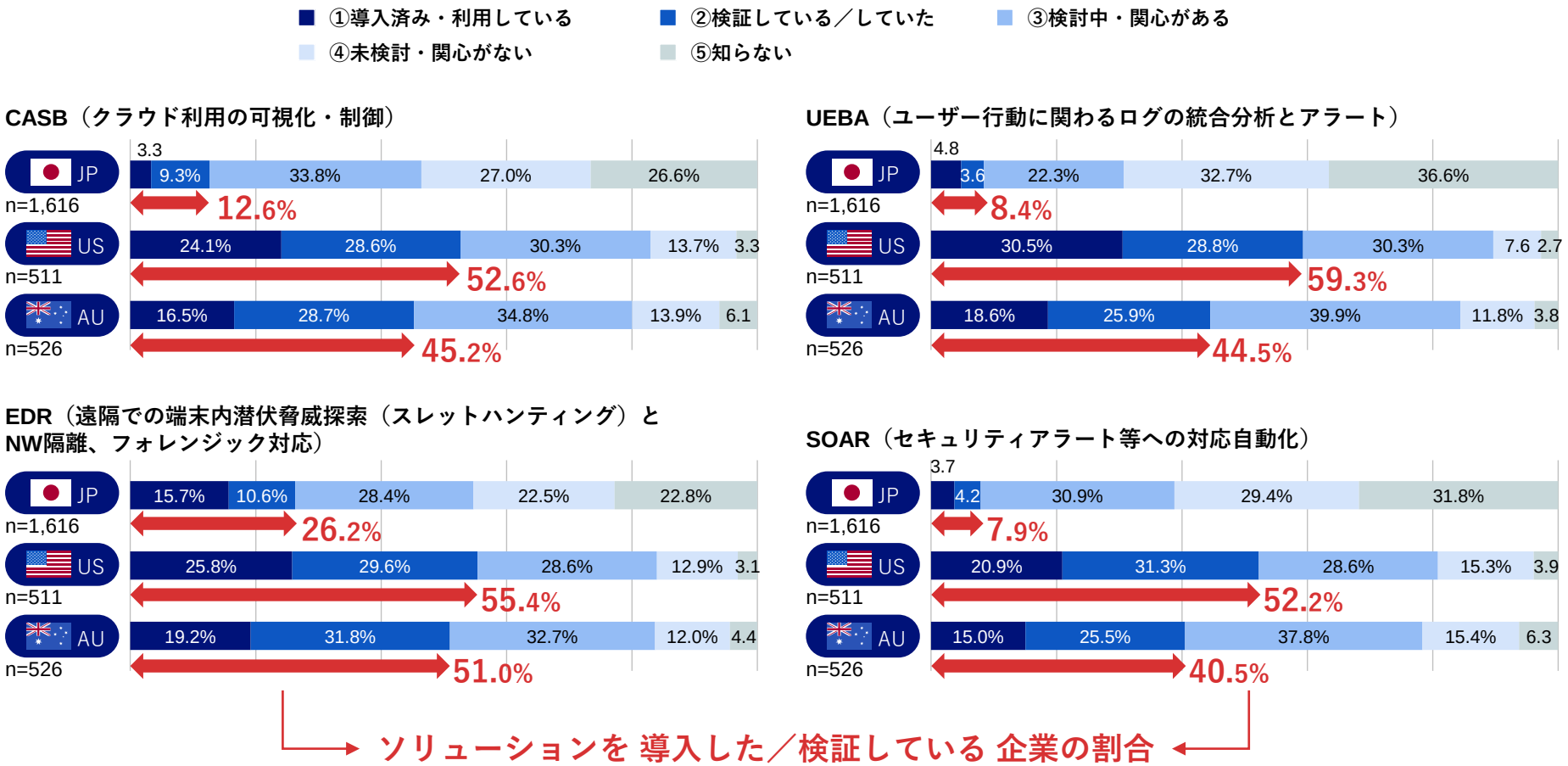


※少数の切上げ/切捨てにより、選択肢の合計値が100%にならない場合があります

I. ゼロトラストセキュリティ：ソリューションの導入状況

▶ ゼロトラストセキュリティを実現するソリューションの導入/検証を進める企業の割合は米国/豪州と比べて低い

Q.セキュリティ対策の新しいソリューションについて、お答えください。



※少数の切上げ/切捨てにより、選択肢の合計値が100%にならない場合があります

II. セキュリティマネジメント

~ Security Management ~

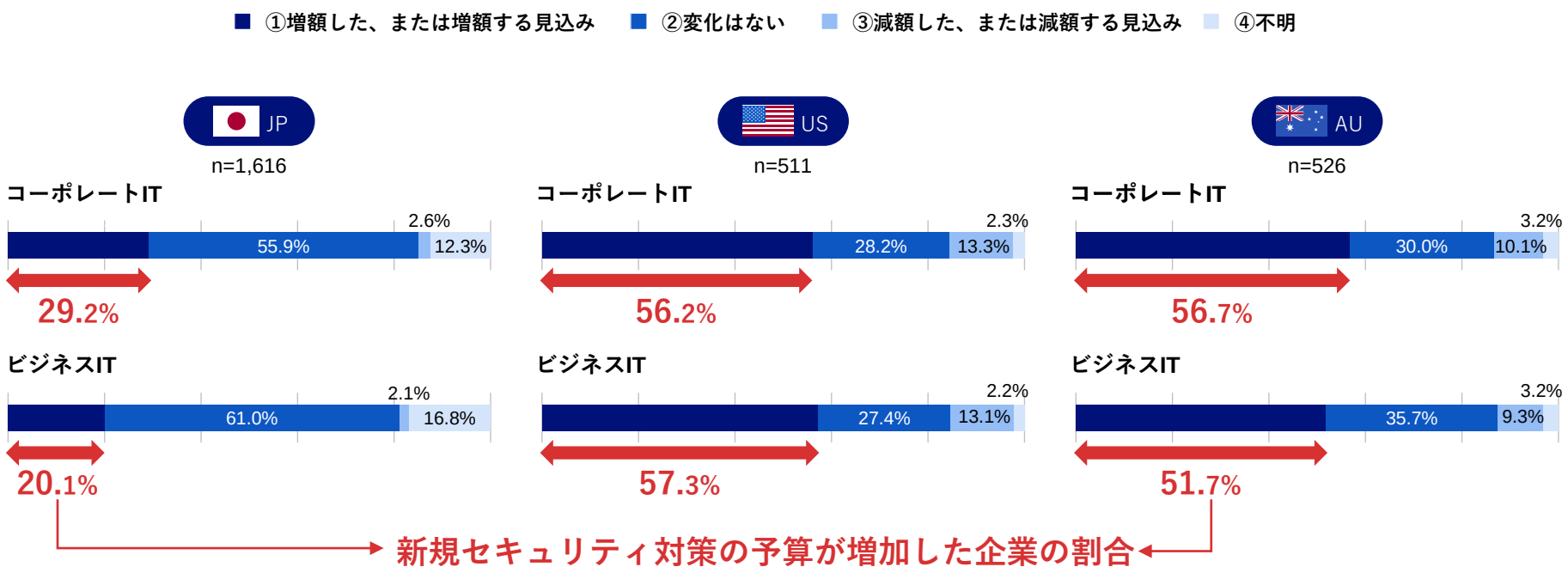
- 新規セキュリティ対策への投資状況
- 統括人材の設置状況

II. セキュリティマネジメント：新規セキュリティ対策への投資状況

▶ 約半数の日本企業において新規セキュリティ対策への投資額は昨年度から横ばい

Q.情報セキュリティ関連予算のうち新規セキュリティ対策に投資する予算は昨年度と比べて変化はありますか？

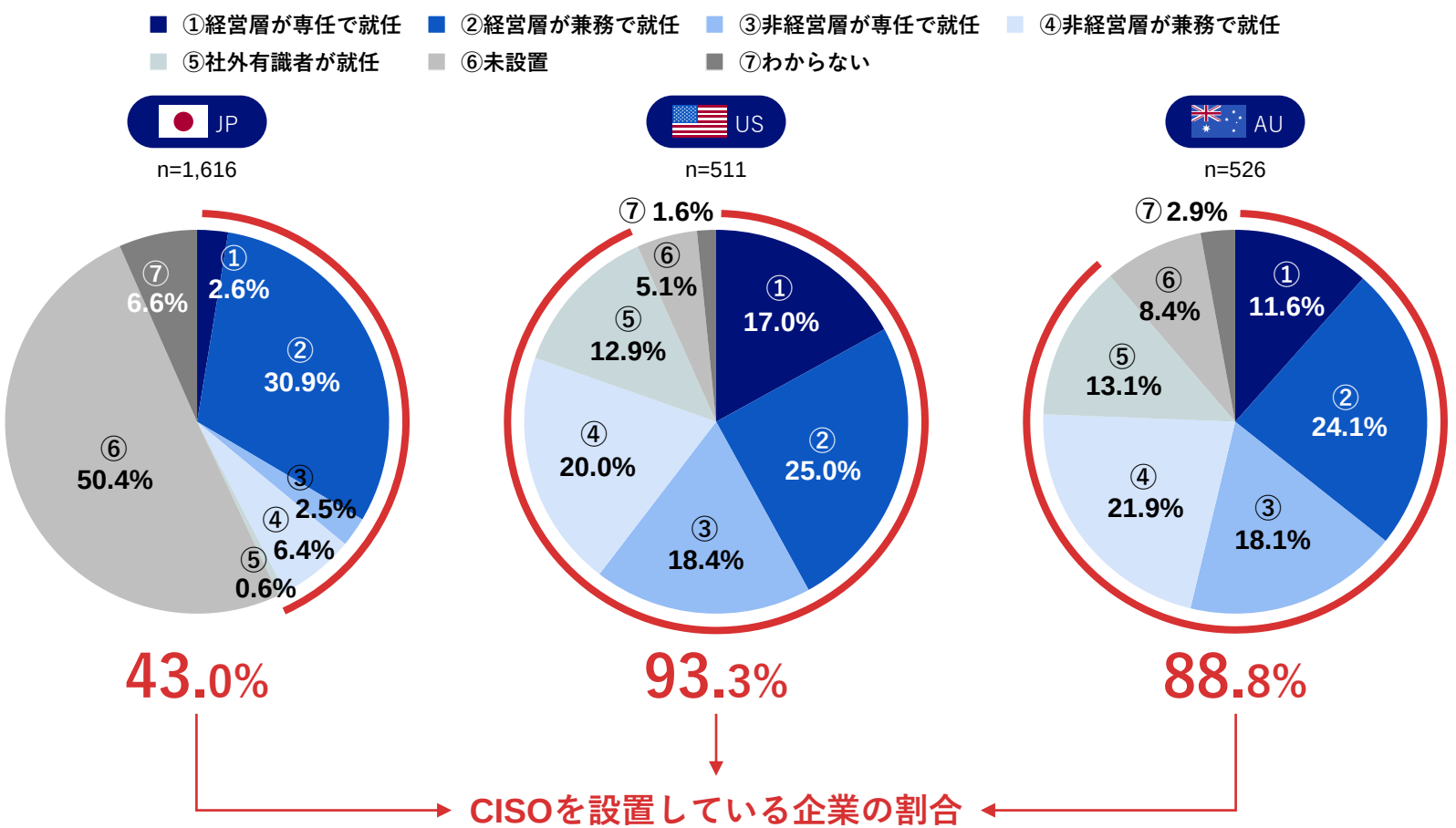
※コーポレートIT：自組織の業務プロセスで利用する内部向けのITシステム（基幹業務、経理、人事システム等）
※ビジネスIT：自組織の事業やビジネスで利用する外部向けのITシステム（オンラインショッピングサイトやスマホアプリ等



※少数の切上げ/切捨てにより、選択肢の合計値が100%にならない場合があります

▶ 米国/豪州と比較すると日本企業のCISO設置率は低い

Q.情報システムおよび情報セキュリティを統括する人材の設置状況についてお答えください。



※少数の切上げ/切捨てにより、選択肢の合計値が100%にならない場合があります

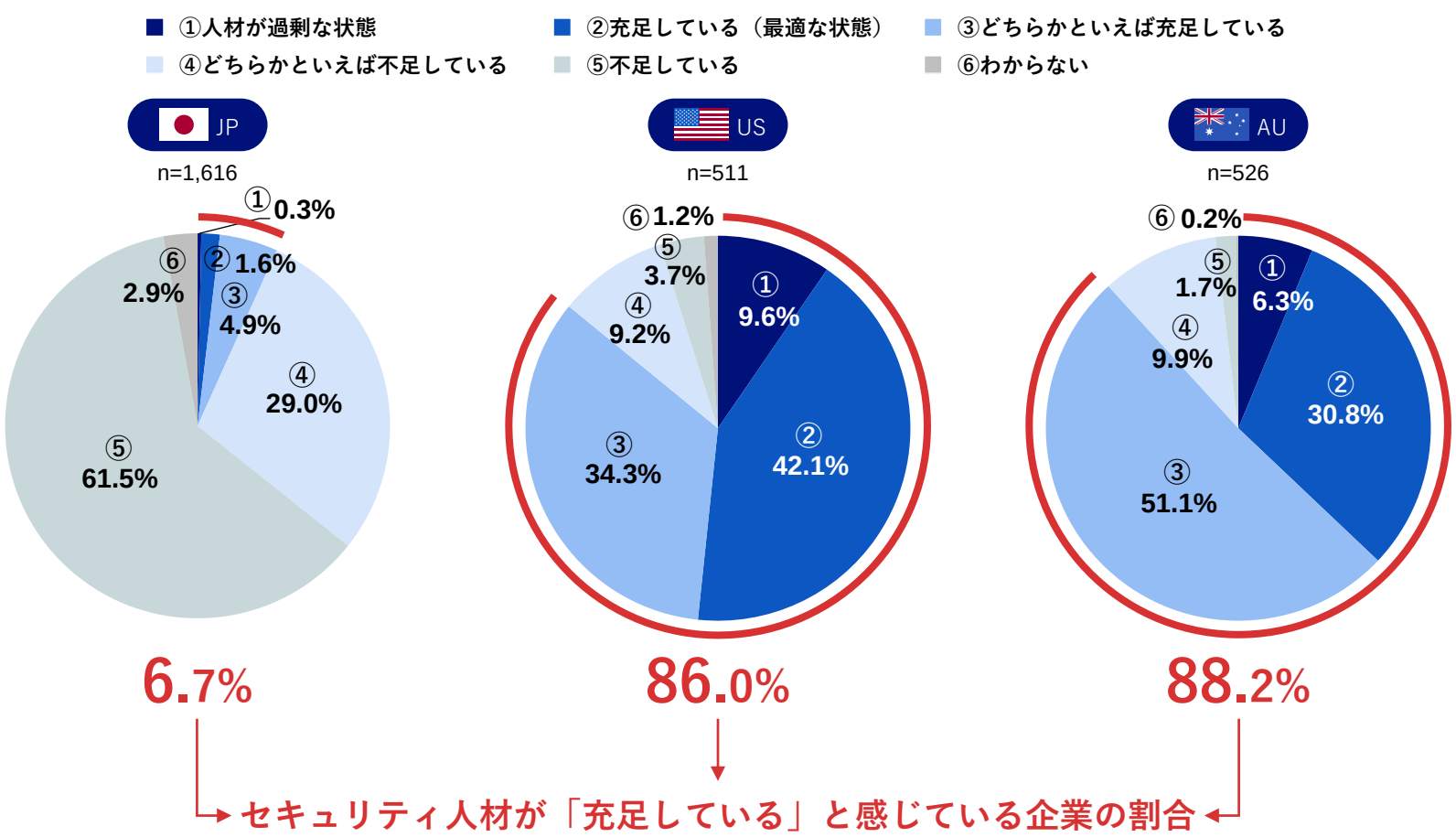
III. セキュリティ人材

~ Human Resources ~

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

▶ 日本企業は米国/豪州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。



※少数の切上げ/切捨てにより、選択肢の合計値が100%にならない場合があります

III. セキュリティ人材：不足している人材種別

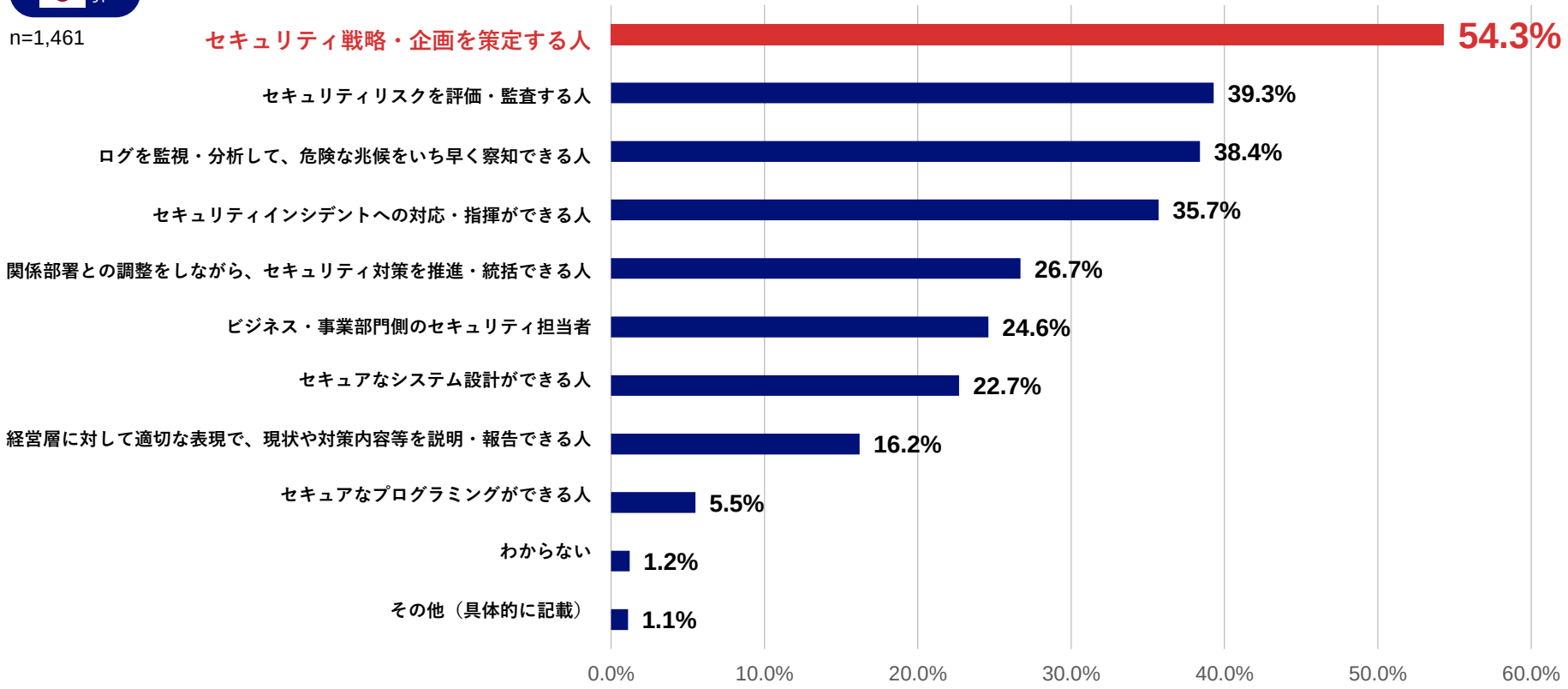
▶ 不足する人材種別として「セキュリティ戦略・企画を策定する人」が１位であった

Q.人材が不足していると考える人材種別は何ですか。以下の中から、最もよくあてはまるものを最大３つお選びください。

※ 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

JP

n=1,461



III. セキュリティ人材：充足していると考える理由

▶ 充足している理由として業務の「標準化」や「自動化」が上位にランクインした

Q. 人材が充足していると考える理由は何ですか。以下の中から、最もよくあてはまるものを最大３つお選びください。

※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

	JP n=109		US n=439		AU n=464	
1位	セキュリティ業務が標準化されており、役割分担が明確化されているため	33.9%	セキュリティ業務がシステム等により自動化・省力化されているため	35.8%	セキュリティ業務がシステム等により自動化・省力化されているため	35.3%
2位	想定していたほどの有事が少ないため	32.1%	セキュリティ業務が標準化されており、役割分担が明確化されているため	33.3%	想定していたほどの有事が少ないため	32.8%
3位	セキュリティ業務の量が少ないため	31.2%	想定していたほどの有事が少ないため	33.0%	セキュリティ業務は経験豊富な一部のメンバーで対応しているため	31.3%
4位	セキュリティ業務は経験豊富な一部のメンバーで対応しているため	19.3%	セキュリティ業務の量が少ないため	31.4%	セキュリティ業務の量が少ないため	28.9%
5位	セキュリティ業務がシステム等により自動化・省力化されているため	14.7%	セキュリティ業務は経験豊富な一部のメンバーで対応しているため	29.8%	セキュリティ業務を外部委託しているため	21.6%
6位	セキュリティ業務を外部委託しているため	12.8%	社内のセキュリティ人材を育成する仕組みを整備しているため	24.1%	セキュリティ業務が標準化されており、役割分担が明確化されているため	21.3%
7位	社内・グループ内異動等で、人員を補充しているため	10.1%	セキュリティ業務を外部委託しているため	19.1%	外部から経験豊富な人材を採用し、補充しているため	19.2%
8位	社内のセキュリティ人材を育成する仕組みを整備しているため	5.5%	外部から経験豊富な人材を採用し、補充しているため	18.7%	社内のセキュリティ人材を育成する仕組みを整備しているため	16.6%
9位	外部から経験豊富な人材を採用し、補充しているため	2.8%	社内・グループ内異動等で、人員を補充しているため	8.0%	社内・グループ内異動等で、人員を補充しているため	9.3%
10位	その他（具体的に記載）	2.8%	わからない	0.7%	わからない	0.9%
11位	わからない	1.8%	その他（具体的に記載）	0.0%	その他（具体的に記載）	0.2%

IV. セキュリティ対策

~ Security Measures ~

- セキュリティ対策実施のきっかけ
- サプライチェーン管理

IV. セキュリティ対策：セキュリティ対策実施のきっかけ

▶ 日本では「他社でのセキュリティインシデント事例」、米国/豪州では「経営層のトップダウン指示」が１位であった

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何ですか。以下の中から、最もよくあてはまるものを最大３つお選びください。

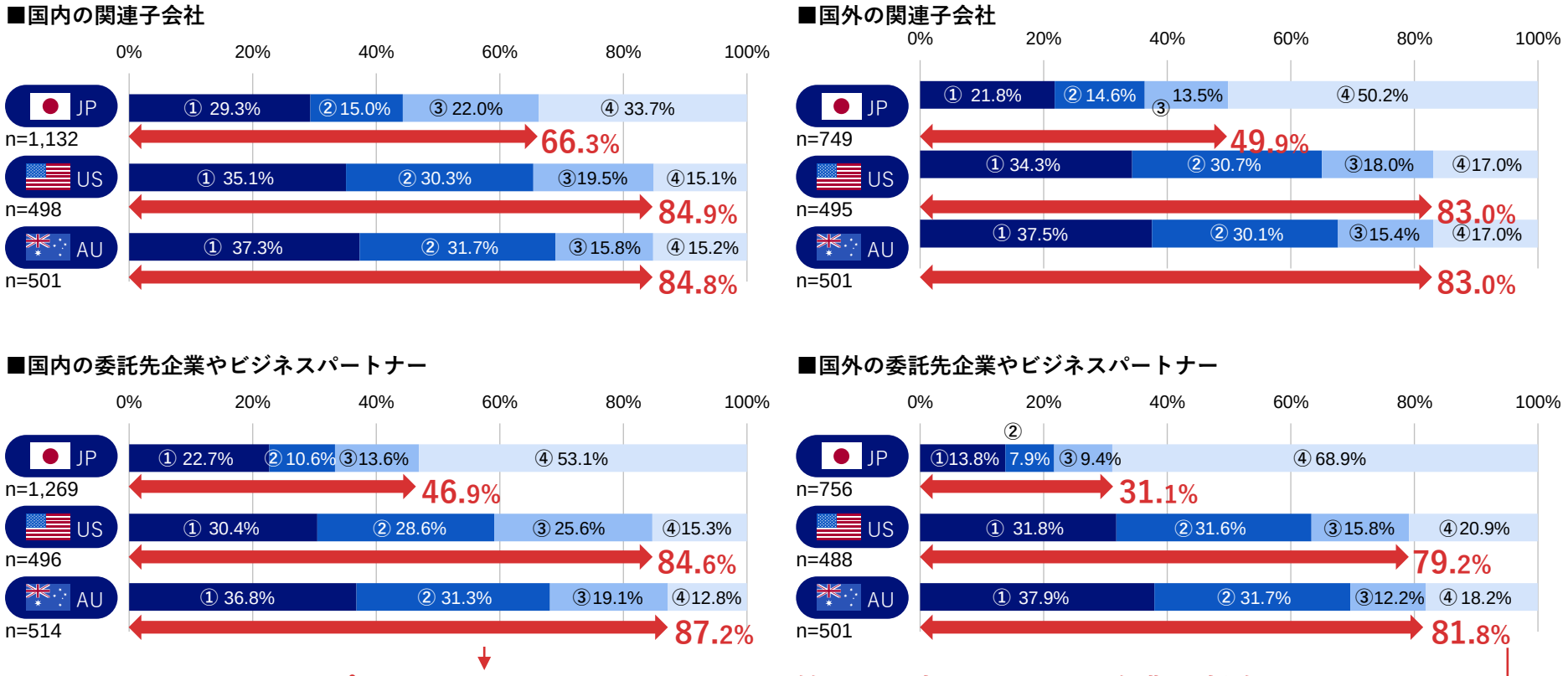
	JP n=1,616		US n=511		AU n=526	
1位	他社でのセキュリティインシデント事例	27.6%	経営層のトップダウン指示	54.8%	経営層のトップダウン指示	52.7%
2位	自社でのセキュリティインシデント	25.6%	他社でのセキュリティインシデント事例	25.0%	他社でのセキュリティインシデント事例	25.3%
3位	経営層のトップダウン指示	21.6%	株主や取引先からの要請	24.5%	株主や取引先からの要請	22.1%
4位	COVID-19に伴うテレワーク対応	19.0%	競合他社の実施状況との比較	21.3%	競合他社の実施状況との比較	19.4%
5位	内部監査・内部有識者からの指摘	18.8%	自社でのセキュリティインシデント	19.8%	監督省庁からのセキュリティ対策強化の要請（自治体からの要請）	18.8%
6位	外部監査・第三者評価の結果	15.7%	監督省庁からのセキュリティ対策強化の要請（自治体からの要請）	19.4%	自社でのセキュリティインシデント	18.8%
7位	DX化推進に伴う対応	14.3%	持株会社や親会社からの要請	17.2%	外部監査・第三者評価の結果	18.8%
8位	持株会社や親会社からの要請	10.8%	内部監査・内部有識者からの指摘	16.0%	持株会社や親会社からの要請	17.1%
9位	その他（具体的に記載）	8.2%	外部監査・第三者評価の結果	15.3%	内部監査・内部有識者からの指摘	16.5%
10位	株主や取引先からの要請	7.9%	COVID-19に伴うテレワーク対応	13.1%	COVID-19に伴うテレワーク対応	15.0%
11位	わからない	5.7%	DX化推進に伴う対応	5.3%	関連法規の改定（具体的な関連法規を記載）	5.1%
12位	競合他社の実施状況との比較	4.7%	関連法規の改定（具体的な関連法規を記載）	3.3%	DX化推進に伴う対応	4.6%
13位	東京2020大会に伴う対応	3.4%	わからない	1.4%	わからない	2.1%
14位	関連法規の改定（具体的な関連法規を記載）	2.1%	東京2020大会に伴う対応	0.0%	その他（具体的に記載）	0.2%
15位	監督省庁からのセキュリティ対策強化の要請（自治体からの要請）	1.6%	その他（具体的に記載）	0.0%	東京2020大会に伴う対応	0.0%

▶ 日本は米国/豪州と比較してサプライチェーンへ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。

※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が対象

■ ①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
■ ②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
■ ③セキュリティ対策状況を把握している
■ ④セキュリティ対策状況を把握していない



※少数の切上げ/切捨てにより、選択肢の合計値が100%にならない場合があります

V. 脅威・事故

~ Threats & Incidents ~

■ 過去1年間で発生したインシデント

V. 脅威・事故：過去1年間で発生したインシデント

▶ 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。以下の中から、あてはまるものを全てお選びください。

サイバー攻撃

※過去1年間でセキュリティインシデントを経験した企業が対象
※25個の選択肢のうち上位10個を抜粋

	JP 2021年 n=1,616		US n=511		AU n=526	
1位	特になし	41.5%	DoS攻撃／DDoS攻撃	49.5%	DoS攻撃／DDoS攻撃	46.6%
2位	電子メール、FAX等の誤送信	25.2%	Webアプリケーションの脆弱性を突いた攻撃	39.9%	Webアプリケーションの脆弱性を突いた攻撃	35.7%
3位	標的型メール攻撃	14.9%	システム基盤（ミドルウェア、OSプラットフォーム等）の脆弱性を突いた攻撃	30.3%	自社サービスへのリスト型アカウントハッキング	24.5%
4位	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	14.5%	自社サービスへのリスト型アカウントハッキング	21.7%	システム基盤（ミドルウェア、OSプラットフォーム等）の脆弱性を突いた攻撃	21.1%
5位	マルウェア感染	11.9%	標的型メール攻撃	21.5%	標的型メール攻撃	19.2%
6位	社員証、業務書類等物品の紛失・置き忘れ・棄損	11.4%	水飲み場型攻撃	12.5%	マルウェア感染	13.7%
7位	システム設定ミス、誤操作	10.6%	ランサムウェア	12.5%	ランサムウェア	12.5%
8位	情報機器、電子記憶媒体、紙媒体等の盗難・紛失	9.0%	マルウェア感染	11.2%	水飲み場型攻撃	12.2%
9位	DoS攻撃／DDoS攻撃	6.1%	業務アクセスが可能な一般ユーザによる不正アクセスや持出	10.4%	情報機器、電子記憶媒体、紙媒体等の盗難・紛失	11.2%
10位	ランサムウェア	5.3%	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	10.2%	業務アクセスが可能な一般ユーザによる不正アクセスや持出	9.5%

03. 総括

調査結果のまとめ

JP

ゼロトラストセキュリティ **~ Zero Trust Security ~**	DXの検討は進んでいるが新規ソリューションの導入は遅れている
セキュリティマネジメント **~ Security Management ~**	新規セキュリティ対策への投資額は昨年度からほぼ横ばい
セキュリティ人材 **~ Human Resources ~**	特にセキュリティ戦略や企画を策定する人材が不足している
セキュリティ対策 **~ Security Measures ~**	サプライチェーンリスクへの統制は遅れている
脅威・事故 **~ Threats & Incidents ~**	標的型攻撃を含むサイバー攻撃の脅威が存在

拡がり続けるビジネス環境にセキュリティを適応するために、企業には **3つの eXtend (拡張)** が必要。

高度化するサイバー攻撃
二重脅迫型ランサムウェア、サプライチェーン攻撃など

セキュリティ
↓
拡がりへの適応

ビジネス環境 → 拡がり続けている

対象	自社	▶ 関連会社、取引先、委託先、海外
執務	オフィス	▶ テレワーク、ワーケーション
技術	オンプレミス	▶ クラウド、ゼロトラスト、API

1 最高責任者（CxO）の拡張
CDO・CISOの設置＆育成
外部CISO　リスキル　ステークホルダーへの発信

2 戦略の視野を拡張
部分から全体戦略へのシフト
xSIRT　xDR　リスク移転

eXtend
（拡張）

3 拡張の阻害要因を解消
既存の習慣・惰性をアンラーニング
継ぎはぎ　人前提　受動的


Share the Next Values!