NRI Secure Insight 2022

企業における情報セキュリティ実態調査

Since 2002

NRI SECURE

概要

「企業における情報セキュリティ実態調査」は、ＮＲＩセキュアテクノロジーズ株式会社が毎年実施している企業の情報セキュリティに関する取り組みの実態調査です。2002年度から過去19回毎年実施してきた「企業における情報セキュリティ実態調査」での知見を活かし、20年目の今年は日本、アメリカ、オーストラリアを対象とした調査を実施した結果、各国企業のセキュリティに対する意識や対策状況の違いが浮き彫りになりました。

本報告書の作成にあたり、アンケートにご回答いただいた皆さまに深く感謝いたします。
ご協力ありがとうございました。

- 本アンケート調査は、ＮＲＩセキュアテクノロジーズ株式会社が、企業や公的機関におけるセキュリティ対策の推進を支援することを目的として、自主的な活動として行っているものです。
- 本アンケート調査の生データは提供いたしかねます。
- 本報告書の著作権は、ＮＲＩセキュアテクノロジーズ株式会社が保有します。
- 内容の一部を転載・引用される場合には、出所として弊社名称「ＮＲＩセキュアテクノロジーズ株式会社」および調査の名称「NRI Secure Insight 2022」を併記した上で、弊社までお知らせ下さい。（電子メール：info@nri-secure.co.jp）
- 今回のアンケートにおける回答企業数 n は、日本1,800社、アメリカ547社、オーストラリア530社です。
- 以下の行為はご遠慮ください。 ＊データの一部または全部を改変すること
  ＊本報告書を販売・出版すること
  ＊出所を明記せずに転載・引用を行うこと

E XECUTIVE SUMMARY

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
調査対象	日本、アメリカ、オーストラリア企業の情報システム／情報セキュリティ担当者
調査期間	日本：2022/7/20-2022/9/25、アメリカ・オーストラリア：2022/8/15-2022/8/24
回答いただいた企業数	計 2,877社（日本：1, 800社、アメリカ：547社、オーストラリア：530社）

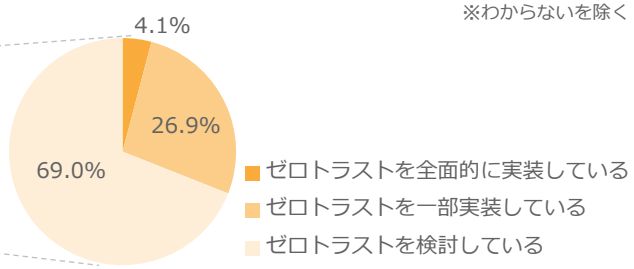
ゼロトラストセキュリティ

ゼロトラストセキュリティの採用

n=1,493 (JP)

※わからないを除く

実装・検討中と回答した割合 **51.6%**



ソリューションの導入率

n=1,800 (JP)

導入済みと回答した割合

EDR 18.9%　CASB 4.8%　IDaaS 6.8%

EDR：遠隔地からの端末脅威探索・インシデント時の隔離／分析
CASB：ユーザーのクラウド利用の可視化や制御　IDaaS：クラウド型ID・アクセス管理

セキュリティマネジメント

情報セキュリティを統括する人材の設置状況

(JP)

	1千人未満	1千人～1万人	1万人以上
CISO	37.7% (n=1,182)	50.0% (n=462)	68.1% (n=47)

CISO（Chief Information Security Officer）：最高情報セキュリティ責任者

※わからないを除く

サイバー保険への加入状況

(JP)

セキュリティ人材

人材の充足状況

n=1,800 (JP)

不足していると回答した割合

過去10年改善が見られない **89.8%**

不足している人材

n=1,617 (JP)

1位	セキュリティ戦略・企画を策定する人
2位	セキュリティリスクを評価・監査する人
3位	セキュリティインシデントへの対応・指揮ができる人

セキュリティ対策

2022年2月以降に発出したサイバー注意喚起を契機に実施したセキュリティ対策

人的対策を優先 ⟷ 技術的対策を優先

	人的対策を優先		技術的対策を優先	
	n=1,772		n=540	n=528
従業員への注意喚起や周知	67.1%			
多要素認証の有効化			41.9%	45.8%

※わからないを除く

CONTENTS

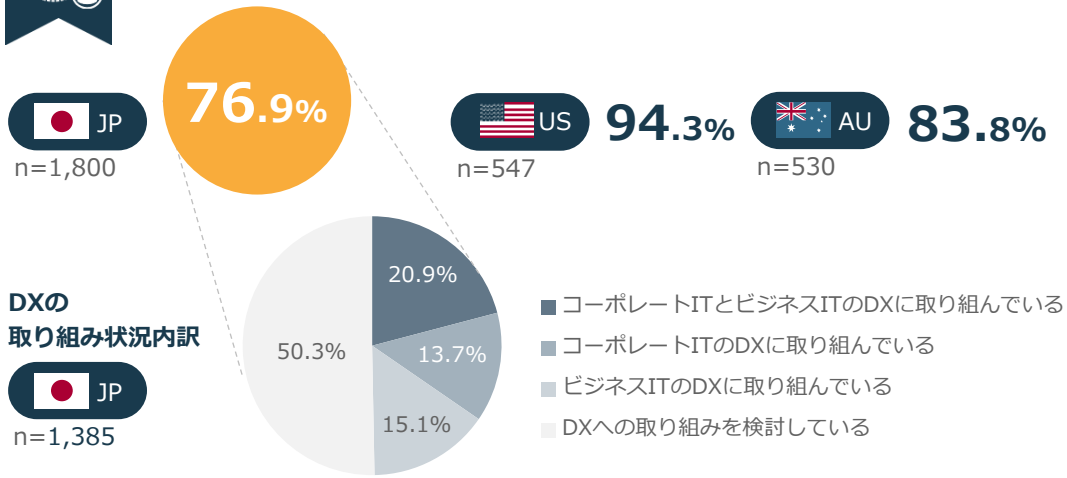
調査結果

CATEGORY

1. ゼロトラストセキュリティ
2. セキュリティマネジメント
3. セキュリティ人材
4. セキュリティ対策
5. 脅威・事故

日本の約8割がDXに取り組み、生産性向上やコスト削減に成果を感じている
今後は業務効率化に加え、製品・サービスの収益向上の実現など、DXの目的シフトが求められる

DXに取り組んでいる企業の割合



DXの取り組み成果

	JP n=689	US n=398	AU n=307
1位	48.2% 業務の生産性が向上した	46.7% 業務の生産性が向上した	50.5% 製品やサービスの売り上げが向上した
2位	34.4% 業務コストが削減された	43.0% 製品やサービスの売り上げが向上した	50.2% 業務コストが削減された
3位	27.1% 老朽化したシステムを刷新した	41.5% 業務コストが削減された	42.3% 業務の生産性が向上した

※ 他選択肢：IT/セキュリティ担当者のモチベーションが向上した／顧客からの評判や信頼が向上した／特に成果は感じられていない／その他（具体的に記載）／わからない

Key Results

DXに取り組んでいる企業割合

JP **約8割**

日本と米・豪のDX成果の違い

米豪のTop3 に**売り上げの向上**

Key Insights

- 経産省が公表したDXレポート2.2（概要）では、DXの取り組みを既存ビジネスの省力化・効率化にとどめず、既存ビジネスの付加価値向上や新規ビジネスの創発など、組織全体の収益向上にシフトすべきであると伝えている。
- その実現のために、経営層がDXビジョンや中長期的な戦略を打ち出し、人材・施策への投資を実行し、DXの効果が出るまでに時間を要することを前提とし、実行・改善を継続し続けることが欠かせない。

DXの取り組み課題

新技術を理解し、実装する能力を有するDX人材の確保は、日・米・豪における共通の課題
DX認定を取得しているなどDXの推進に積極的な企業ほど、情報セキュリティへの対応意識が高い

DXの取り組み課題

	JP n=1,800	US n=547	AU n=530
1位	60.8% 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	53.7% 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	58.5% 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
2位	41.3% 情報セキュリティへの対応	38.0% 縦割りの組織構造	48.5% 縦割りの組織構造
3位	34.3% 変化を受け入れる企業風土がない	28.7% 変化を受け入れる企業風土がない	30.0% DXに対する経営の理解

※ 他選択肢：その他（具体的に記載） ／課題はない

DX認定取得有無におけるDXの取り組み課題の差

	JP DX認定未取得 n=1,738	JP DX認定企業 n=62
1位	60.6% 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	66.1% 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
2位	40.6% 情報セキュリティへの対応	59.7% 情報セキュリティへの対応
3位	34.8% 変化を受け入れる企業風土がない	41.9% 縦割りの組織構造

19.1 Point UP

DX認定企業は、 経産省がDXや働き方改革に積極的な企業として認定した企業であり、Insight2022回答企業全体の内、62社が該当した。(2022年11月時点)

Key Results

DXの取り組み課題の1位は日・米・豪で同一

DX推進をけん引できる**人材の確保**

DX推進の積極性とセキュリティ対応の相関

+19.1pt DX認定企業の情報セキュリティ対応

Key Insights

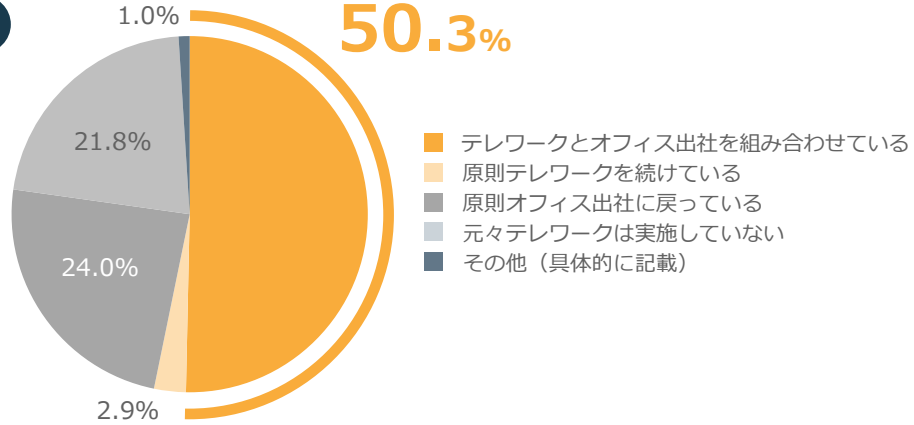
- DXを推進する人材の確保は日・米・豪の共通課題であり、人材獲得競争はさらなる激化が予想される。今後の日本企業は、当該人材から選ばれる企業となるべく競争力や企業価値を高める必要がある。DX人材への処遇改善、働きやすい環境の整備や人的資本への継続的投資が欠かせない。
- DX認定企業の方が情報セキュリティへの対応を課題と捉える割合が高い。DX認定の取得には企業イメージの向上や税制優遇などの効果だけでなく、人材のセキュリティ意識や組織のセキュリティレベルの向上にも寄与していることがうかがえる。

テレワークとセキュリティ

テレワークとオフィス出社を組み合わせたハイブリッドな働き方が主流となる
攻撃対象領域の観点で、VPN機器やリモートデスクトップの脆弱性対応や定期的な見直しが重要

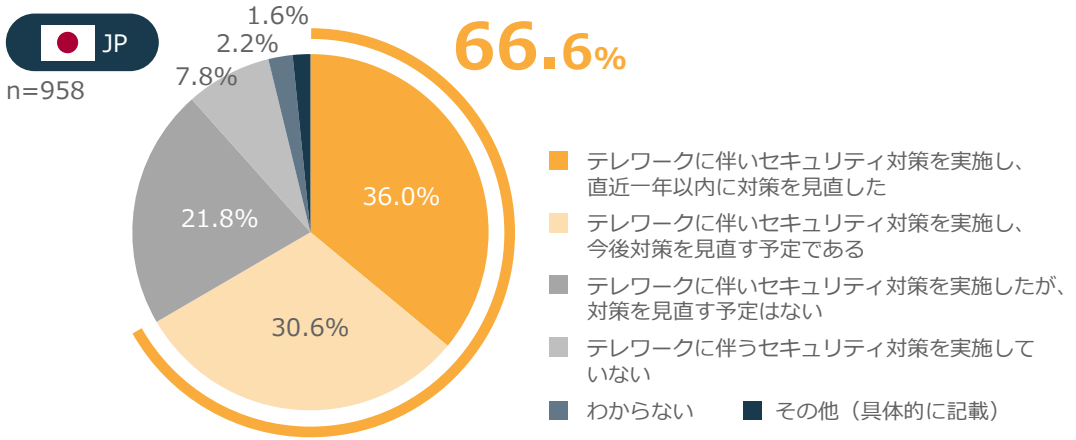
テレワークの実施状況

JP
n=1,800



テレワーク実施に伴うセキュリティ要件への対応状況

JP
n=958



Key Results

ニューノーマルな働き方

約50% テレワークとオフィス出社のハイブリッド

テレワークに潜むリスクと対策

約67% セキュリティ対策の実施＋今後見直し予定

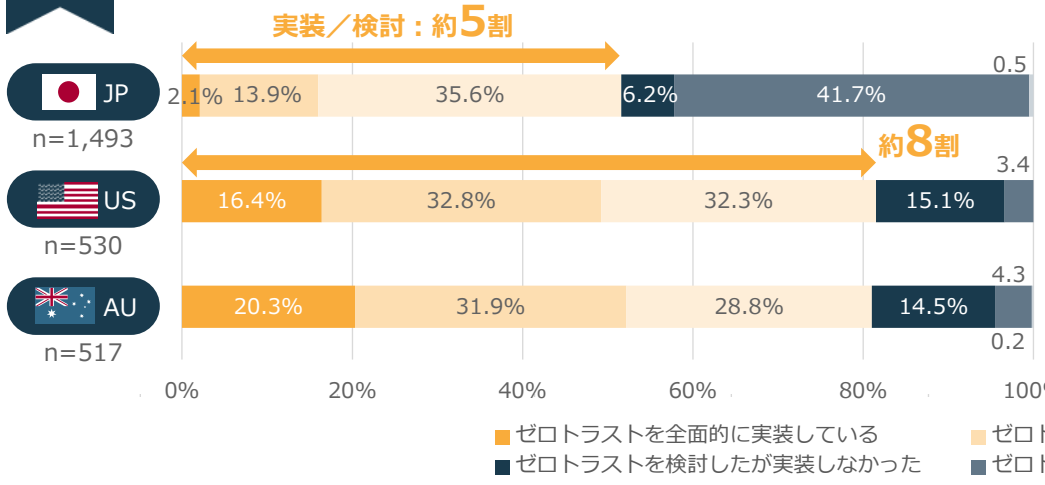
Key Insights

- 従業員の意思や希望に合わせた柔軟な働き方を採用する企業が増えている。時間や場所に縛られない業務環境を整備することは、従業員の生産性を高めるだけでなく、帰属意識や企業ブランド力が高まる効果も見込まれ、優秀な人材の獲得やエンゲージメント向上にもつながる。
- VPN機器やリモートデスクトップの脆弱性を狙った不正アクセスやランサムウェア攻撃が多発しているため、アタックサーフェス（攻撃対象領域）に対して、網羅的な観点（NIST Cyber Security Frameworkが推奨する、特定・防御・検知・対応・復旧など）での見直しが求められる。

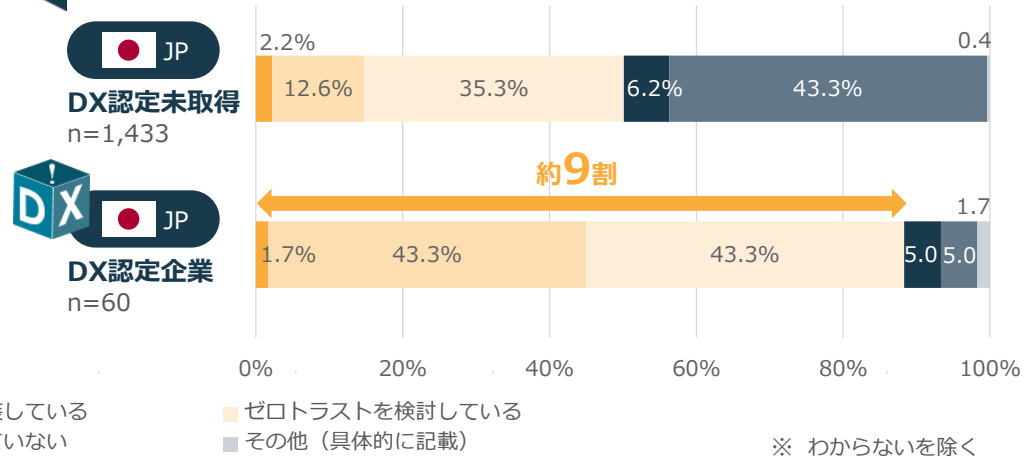
ゼロトラストセキュリティ

日本は、米・豪と比較してゼロトラストセキュリティの実装／検討割合が低い
社内外の環境変化を踏まえて、自社のセキュリティ戦略や思想を今一度見直すことが望まれる

ゼロトラストセキュリティの採用



DX認定企業におけるゼロトラストセキュリティの採用



※ わからないを除く

Key Results

ゼロトラストセキュリティの実装／検討企業

JP 約5割　US AU 約8割

DX推進の積極性とゼロトラストの相関

約9割 DX認定企業のゼロトラスト実装／検討

Key Insights

- 従来の境界防御からゼロトラストセキュリティへの転換には、多くの検討コストを要するが、この変革はセキュリティレベルのみならず、従業員の生産性・利便性を大きく向上させ得る。
- 米・豪に比べて日本の実装／検討企業が少ないのは、既存の業務環境でも企業活動が継続できている上、その投資対効果が過少に見積もられており、必要性・緊急性が十分に理解されていないことが原因と推察される。
- 多様なクラウドサービスの活用や働き方の変容などを踏まえて、自社のセキュリティ関する戦略や思想を、既存の座組や制約に捉われることなく、今一度見直すことを推奨する。

ゼロトラストを実現するソリューション

働き方の変化や頻発するインシデントを背景にEDRが一般化
クラウド関連はIDaaSやCASBが続伸、クラウド設定不備のチェックに発展の兆候あり

ソリューションの導入状況

JP n=1,800

			導入済み、検証中または検討中	導入済み・利用している	検証している／していた	検討中・関心がある	未検討・関心がない	知らない
1位	EDR	遠隔地からの端末脅威探索、アラート、インシデント時の隔離や分析 (Endpoint Detection and Response)	57.6%	18.9%	12.8%	25.9%	22.9%	19.4%
2位	CASB	ユーザーのクラウド利用の可視化や制御 (Cloud Access Security Broker)	44.4%	4.8%	9.4%	30.2%	30.8%	24.8%
3位	IDaaS	クラウド型ID・アクセス管理 (Identity as a Service)	42.4%	6.8%	7.1%	28.5%	31.8%	25.8%
4位	SOAR	セキュリティ運用の自動化及び効率化技術 (Security Orchestration, Automation and Response)	40.3%	4.1%	6.1%	30.1%	32.0%	27.8%
5位	脅威インテリジェンス	ダークウェブ監視および攻撃予兆・フィッシング・偽アプリ等の外部脅威情報の可視化・対策	38.2%	4.8%	5.3%	28.1%	35.2%	26.6%
6位	UEBA	ユーザー行動に関わるログの統合分析とアラート (User and Entity Behavior Analytics)	35.5%	6.3%	5.7%	23.5%	35.2%	29.4%
7位	CSPM	クラウドセキュリティ態勢管理 (Cloud Security Posture Management)	31.4%	2.0%	3.8%	25.6%	37.3%	31.3%
8位	SSPM	SaaSのセキュリティ態勢管理 (SaaS Security Posture Management)	27.5%	1.4%	3.6%	22.5%	39.4%	33.1%
9位	TLPT	脅威ベースのペネトレーションテスト (Threat-Led Penetration Testing)	26.4%	2.3%	4.7%	19.4%	39.5%	34.1%

Key Results

EDRエンドポイント対応

約58% が導入済み、検証・検討中

クラウド関連対策ソリューション導入

3位 2位 7位 8位
IDaaS・CASB > CSPM > SSPM

Key Insights

- EDRは端末上で実行されるマルウェアの挙動の監視、端末の動作ログの収集と分析、フォレンジック調査を支援する。日本の導入率は約19%と他のソリューションと比べて高い。防御だけでなく、インシデントの早期検知や対応・復旧が求められるEmotetの流行やランサムウェアによる攻撃の増加、テレワーク前提の対策として導入が進んでいる。
- クラウド関連では、クラウド前提のID管理（IDaaS）や、クラウド利用状況の可視化（CASB）の導入や検討が進む。加えて新たな対策ソリューションとしてクラウドのセキュリティ態勢管理（CSPM、SSPM）の検討企業も3割弱いる。該当製品は成長分野で、現時点では導入企業は限られているが、クラウド設定不備に起因する事故に鑑みて、今後も製品導入検討が進むと考えられる。

2 セキュリティの専門人材

日本はCISOの設置割合が約4割にとどまるが、従業員規模が多いほど設置割合は高まる
未設置の企業は、CISOをチームとして立上げ、時間をかけて整備していく発想が望まれる

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

日米豪の3か国比較

CISO（Chief Information Security Officer）：最高情報セキュリティ責任者

	JP	US	AU
CISO	41.9% (n=1,691)	**97.0% (n=542)**	**96.8% (n=526)**
CIO	45.2% (n=1,696)	96.9% (n=543)	97.3% (n=527)
CDO	17.2% (n=1,648)	94.8% (n=534)	94.7% (n=525)

※ わからないを除く

JP 日本の従業員規模別比較

	1千人未満	1千人～1万人	1万人以上
CISO	37.7% (n=1,182)	50.0% (n=462)	**68.1% (n=47)**
CIO	40.0% (n=1,185)	54.7% (n=464)	80.9% (n=47)
CDO	15.4% (n=1,159)	20.4% (n=447)	33.3% (n=42)

※ わからないを除く

Key Results

CISOの設置状況

US AU 約97%

従業員1万人以上の日本企業 CISOの設置状況

JP 約68%

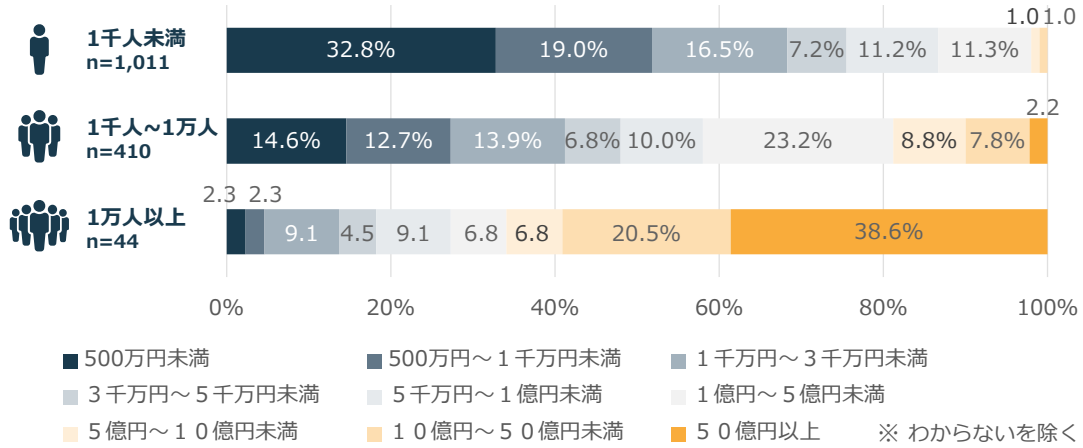
Key Insights

- CISOには「セキュリティの知識・技術」、「戦略・会計などのビジネススキル」、「リーダーシップと意思決定力」、「コミュニケーションスキル」など、多様な資質・能力が求められる。企業内で適任人材を見つけにくいことが、日本のCISO設置割合が約4割に留まる背景と考えられる。
- 未設置の企業は、CISOにスーパーマンを任命しようとするのではなく、チームとして立上げ、時間をかけて整備していく発想が望ましい。そのためには、自社におけるセキュリティ業務を棚卸しを行い、役割とアサインを再定義することから始めたい。
- CISO設置企業では、CISOが抱える孤独や立場上のプレッシャーに伴う機能不全、離職が課題となる。経営がCISOを支え、執行に必要な権限とリソースの付与が欠かせない。

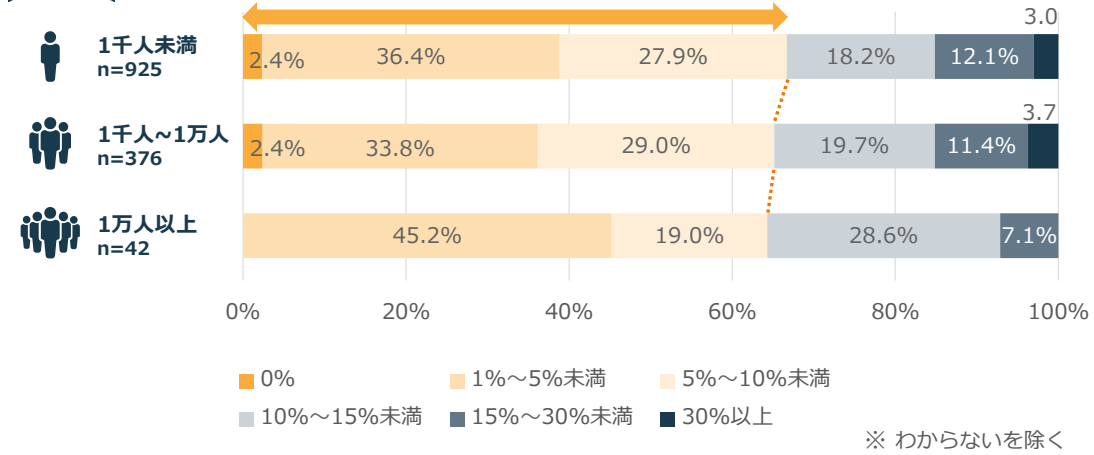
IT/セキュリティ関連予算

日本のセキュリティ関連予算の割合は、従業員規模を問わず、約7割において10%未満
米・豪のセキュリティ関連予算の10%未満の回答割合は3割前後であり、比率が大きく異なる

IT関連予算 JP



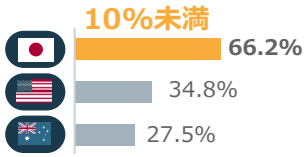
IT関連予算に占めるセキュリティ関連予算の割合 JP



Key Results

IT関連予算に占めるセキュリティ予算割合

10%未満の企業が 約7割



※米豪：3割前後

Key Insights

- セキュリティ対策には人的・物理的・技術的などの分野があるが、日本企業の多くはセキュリティ担当者のスキルと運用を重視し、従業員への注意喚起により行動を促すなど人的対策の割合が高い傾向がある（P24を参照）。一方、米・豪は技術的対策の優先度が高いことが、セキュリティ予算比率の明確な差の背景にあると考えられる。
- DXの進展と共にIT利活用の範囲は広がり、サイバーセキュリティの脅威は増す。生産年齢人口の減少によるセキュリティ人材不足も深刻なため、人的対策の比重が高いセキュリティ戦略は限界に差し掛かっている。今後は、時代の要請に応じた対策の見直しとそれに伴う予算確保が望まれる。

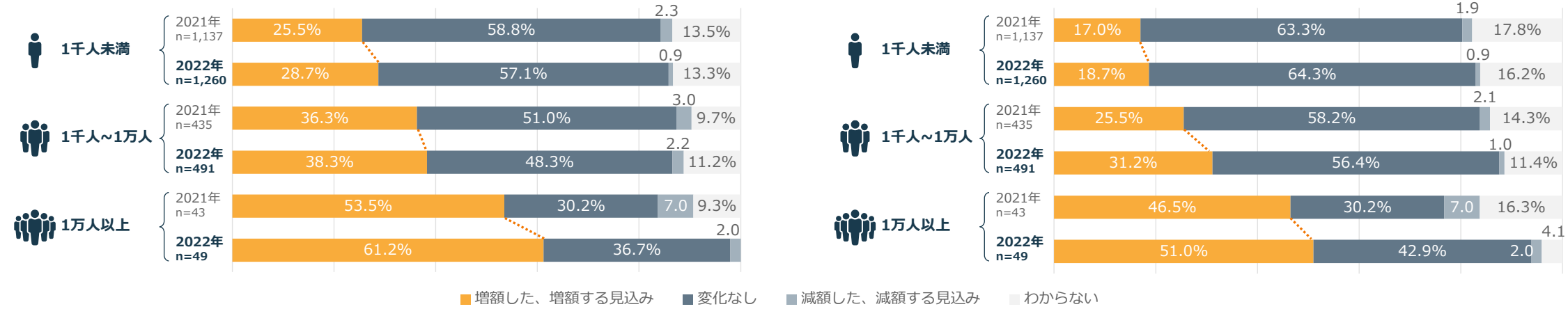
新規セキュリティ対策への投資予算

新規セキュリティ対策への投資予算は、従業員規模やIT用途によらず、2021年と比べ増加傾向
従業員規模が大きい企業ほど増額回答の割合が多いのは、攻撃対象領域の広がりとの相関と推察

前年度と比較した
新規セキュリティ対策に投資する予算の増減

JP

※1 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）
※2 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）



Key Results

新規セキュリティ予算の経年比較

2021年 ＜ **2022年**

従業員規模と新規予算の相関

従業員規模が大きいほど**増額回答が多い**

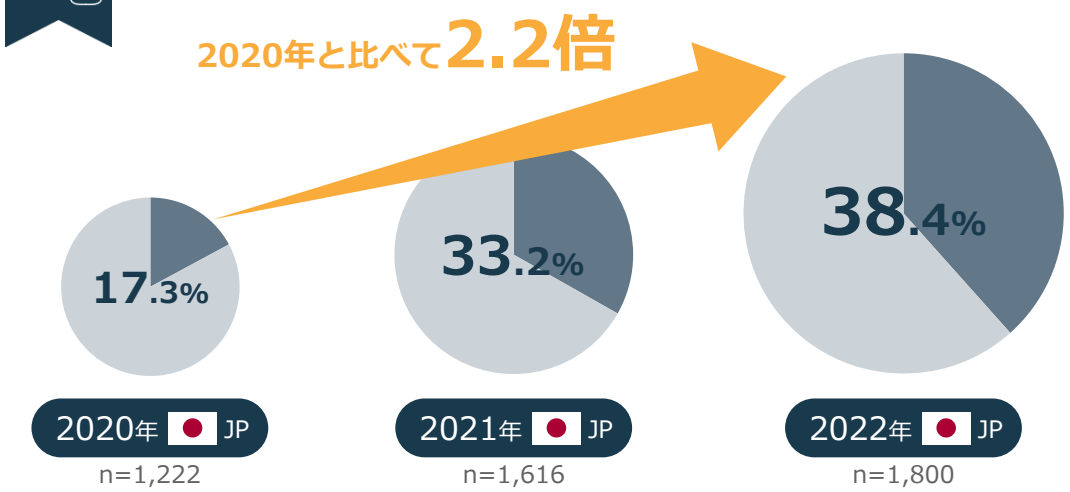
Key Insights

- 2022年の日本は円安が進み、世界全体で景気後退が発生するリスクへの関心が高まったが、新規セキュリティ対策への投資予算は2021年と比べて増加した。2022年2月以降の国際情勢を踏まえたサイバー脅威の高まりや頻発するセキュリティ事故が要因と考えられる。
- 従業員規模が大きい企業ほど増額回答の割合が多いのは、規模が大きい企業ほど、事業をグローバルに展開し、DXも進み、アタックサーフェス（攻撃対象領域）が広がったことで、サプライチェーン全体で攻撃対象領域を定義・管理する必要に迫られたことが一因と考えられる。

2 サイバー保険

サイバー保険の加入率は、直近3年間で2.2倍の大幅上昇
ランサムウェア攻撃や国際情勢の変化に伴う脅威の増加、個人情報保護法の改定が要因か

サイバー保険への加入状況



サイバー保険への加入理由

	JP 2021年 n=537	JP 2022年 n=691
1位	65.0% 自社の対応だけでは被害を防ぎきれない可能性があるため	65.3% 自社の対応だけでは被害を防ぎきれない可能性があるため
2位	31.7% 事故発生時の見舞金等、支払う可能性がある金銭を補うため	33.7% 事故発生時の見舞金等、支払う可能性がある金銭を補うため
3位	25.9% 事故発生時に迅速に対応するためのコストを捻出したいため	26.0% 補償内容に対し、保険料が妥当だと感じたため

※ 他選択肢：付帯サービスに魅力を感じたため（具体的な付帯サービスを記載）／残留セキュリティリスクも適切に管理していることを株主・取引先にアピールするため／取引先や業務委託元等から加入の要請があったため／トップダウン指示があったため／法制度改正等による処罰や制裁金が厳しくなっているため／関連企業、同業他社が加入しているため／セキュリティリスクの高いビジネスを立ち上げたため／サイバーセキュリティ経営ガイドラインで加入を推奨する記載があるため／情報漏えいなど、セキュリティ事件・事故のニュースを見聞きする機会が増えたため／DX化に伴い取り扱う情報やサービスが増えたため／その他（具体的に記載）

Key Results

サイバー保険の加入率の大幅上昇

2.2倍（2020年⇒2022年）

サイバー保険加入理由2年連続1位

約65% 自社の対応だけでは被害を防ぎきれない

Key Insights

- 直近3年間の加入率の伸びには、ランサムウェア攻撃による被害リスクの増加、2022年2月以降のサイバーリスクの増大、2022年4月の個人情報保護法の改正による規制の厳格化等が背景にあると推察する。
- サイバー保険の加入が増え、セキュリティ事故の発生割合も高まっていることから、保険会社が課す加入条件や補償内容が厳しくなることが想定される。自社やサプライチェーンにおよぶサイバーリスクの影響度や発生可能性を考慮し、リスク移転の観点でサイバー保険を検討する必要はあるが、引き続き自社やサプライチェーン全体のセキュリティ対策を怠ってはならない。

3 セキュリティ担当者の困りごと

日本は、増加するセキュリティ業務に対応できる人材の育成に課題がある
米・豪は攻撃を未然に防ぐため、セキュリティ脅威動向・トレンドに関する情報収集を実施

企業のセキュリティ担当者として、最も対応に困っている事項

	JP n=1,800	US n=547	AU n=530
1位	44.4% セキュリティ人材の育成	43.7% セキュリティ対策のトレンド・他社動向の把握	49.8%
2位	35.9% サイバー攻撃の高度化への対応	41.0% セキュリティ脅威・事故に関する情報収集と関係者共有	48.5%
3位	33.8%	25.0% セキュリティインシデント発生時の緊急対応	31.7%
4位	32.0% 自社セキュリティ対策の遅れ（最新技術・動向の未反映）	24.7% セキュリティ業務の状況・進捗に関する経営層への報告	29.6%
5位	17.1% グループ会社・国内外拠点のセキュリティ統制・管理	23.8% サイバー攻撃の高度化への対応	22.8%

※ 他選択肢：業務委託先や取引先のセキュリティ統制・管理／テレワーク環境におけるセキュリティの確保／DX化に伴うデジタルサービスのリスク分析・把握／その他（具体的に記載）／困っていることはない

Key Results

セキュリティ人材の育成が課題であると回答

JP 約44%

日本と米・豪の課題の違い

人的リソース JP ⟷ US AU 攻撃の未然防止に向けた取り組み

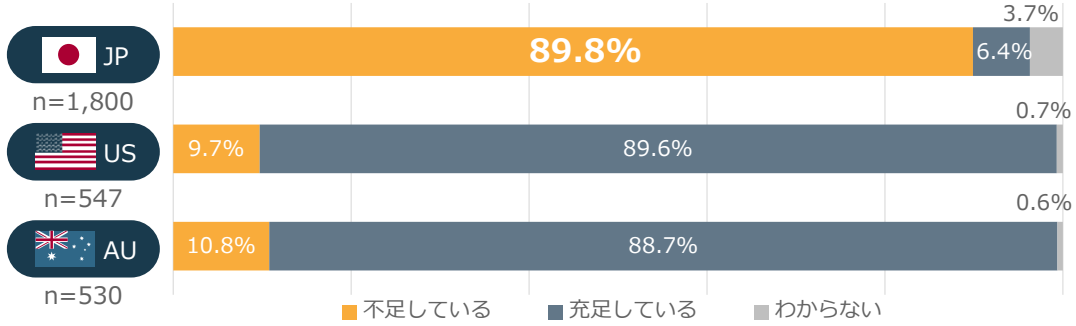
Key Insights

- セキュリティ人材育成が1位の背景には、高度化する攻撃への事前/事後対応（2,3位）、技術動向への追従（4位）といった外部要因に加え、セキュリティ統制の範囲拡大（5位）が要因となり、セキュリティ関連業務が増加していることで人材不足に拍車がかかっていることにある。
- 自社に必要なセキュリティスキルと量を明確に定義し、資格取得支援・専門能力開発プログラムの整備やリスキリングなど、人材育成により積極的な投資が求められる。人的資本経営の推進は、セキュリティの観点でも重要となる。
- 米・豪では、セキュリティ対策のトレンドや脅威・事故など、社外動向やコミュニティの共有情報を基に、強化すべきセキュリティ対策を先回りして実装することの重要性が十分認識されていると推察する。

セキュリティ人材の充足状況と不足理由

日本の約9割の企業はセキュリティ人材の不足に悩んでいる
現場の担当者はマネジメント層不在により、戦略立案から対策実行まで兼務していると推察

セキュリティ対策に従事する人材の充足状況



※ 不足している：「どちらかといえば不足している」「不足している」のいずれかを回答
※ 充足している：「人材が過剰な状態」「充足している（最適な状態）」「どちらかといえば充足している」のいずれかを回答

「不足している」と回答した企業における、不足している人材種別

	JP n=1,617	US n=53	AU n=57
1位	50.9% セキュリティ戦略・企画を策定する人	56.6% 経営層に対して適切な表現で、現状や対策内容等を説明・報告できる人	52.6%
2位	38.0% セキュリティリスクを評価・監視する人	28.3%	40.4% 関係部署との調整をしながら、セキュリティ対策を推進・統括できる人
3位	35.5% セキュリティインシデントへの対応・指揮ができる人	26.4%	29.8% セキュアなシステム設計ができる人
4位	34.6% ログを監視・分析して、危険な兆候をいち早く察知できる人	24.5% 関係部署との調整をしながら、セキュリティ対策を推進・統括できる人	28.1% セキュリティリスクを評価・監査する人
5位	23.6% セキュアなシステム設計ができる人	18.9% セキュアなプログラミングができる人	21.1% セキュアなプログラミングができる人

※ 他選択肢：ビジネス・事業部門側のセキュリティ担当者／その他（具体的に記載）／わからない

Key Results

セキュリティ人材が不足していると回答

JP **約90%** 過去10年、同様の傾向
※米・豪は正反対

日本で不足している人材種別

JP **約5割** **マネジメント層（戦略・企画の策定）**

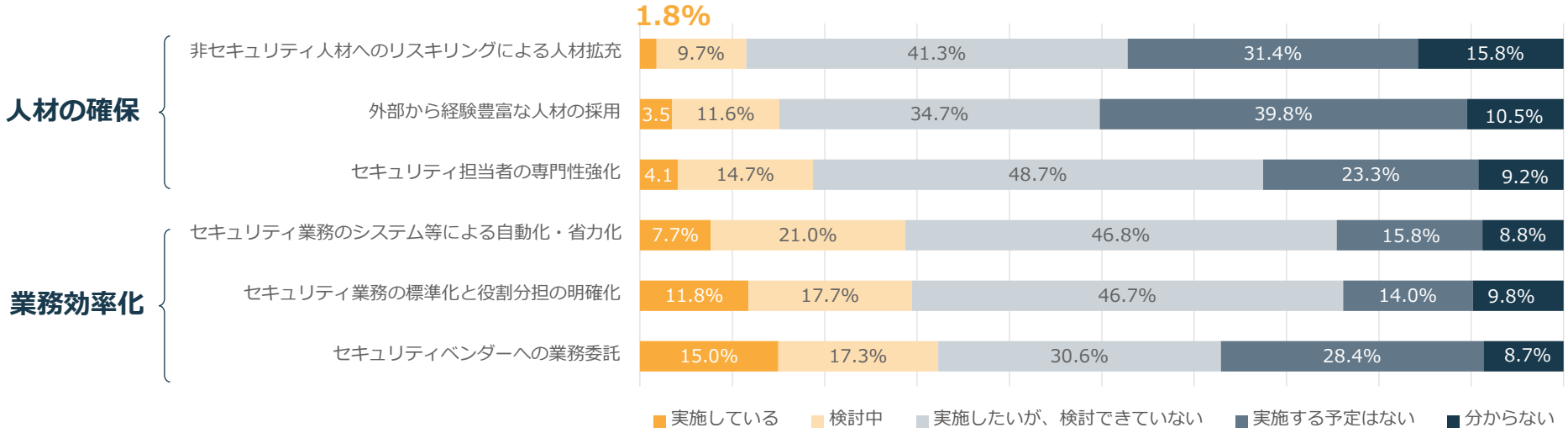
Key Insights

- 日本の約9割はセキュリティ人材が不足していると感じ、過去10年以上改善がみられていない。特にセキュリティ戦略・企画を策定する人材が不足しており、現場の担当者が日々の対策実行や運用業務だけでなく、マネジメント層の不在により戦略・企画も兼務せざるを得ない状況が推察できる。
- セキュリティ担当者が戦略立案から対策実行まで、すべてを実施することは困難である。セキュリティ戦略は、CISOが経営者と一体となって、経営戦略やセキュリティ予算・人材スキルなどの内部環境を踏まえ、セキュリティ動向といった外部環境も捉えて、推進することが望ましい。

3 セキュリティ人材不足を補う施策

人材不足が問題となる一方「人材の確保」や「業務効率化」への施策実施率は低い
不足感の解消には、CISOと経営層が一体となり、多面的な施策実行と継続的な改善を徹底すべき

「不足している」と回答した企業のセキュリティ人材不足を補う施策の実施状況　JP　n=1,617



Key Results

人材不足を補う施策の実施率

人材の確保：5%以下　　**業務効率化：15%以下**

非セキュリティ人材へのリスキリング

1.8% のみ実施している

Key Insights

- 日本の約9割が人材不足を感じる一方で、人材の確保や業務効率化などの実施率は、いずれも10%程度であり、施策が後手に回っている。長年続いているセキュリティ人材不足の本質的な解決には、CISOを中心に経営層が一体となり、各施策の多面的な実行と継続的な改善の徹底が欠かせない。
- 近年注目される非セキュリティ人材へのリスキリングや、自らの業務遂行にあたり必要かつ十分なセキュリティ対策を実現できる人材（プラス・セキュリティ）の育成など、セキュリティの基礎教育の重要性が高まっていることも視野に入れたい。

セキュリティ人材の充足理由

米・豪は「業務の自動化・省力化」が上位の理由に
日本は現状の業務を整理し、定型化・標準化、ツールやシステム等による自動化に備えたい

「充足している」と回答した企業のセキュリティ人材充足理由

	JP n=116	US n=490	AU n=470
1位	32.8% セキュリティ業務の量が少ないため	36.5% 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	50.9% 想定していたほどの有事が少ないため
2位	31.9% 想定していたほどの有事が少ないため	34.1% 想定していたほどの有事が少ないため	40.6% 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
3位	25.9% 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	32.7% 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	36.0% セキュリティ業務の量が少ないため
4位	22.4% 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	31.0% 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	31.9% 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
5位	19.0% セキュリティ業務を外部委託しているため	27.3% セキュリティ業務の量が少ないため	26.6% 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

※ 他選択肢：外部から経験豊富な人材を採用し、補充しているため／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／社内・グループ内異動等で、人員を補充しているため／その他（具体的に記載）／わからない

Key Results

米・豪の人材充足理由

US AU 約40% 業務の自動化・省力化

Key Insights

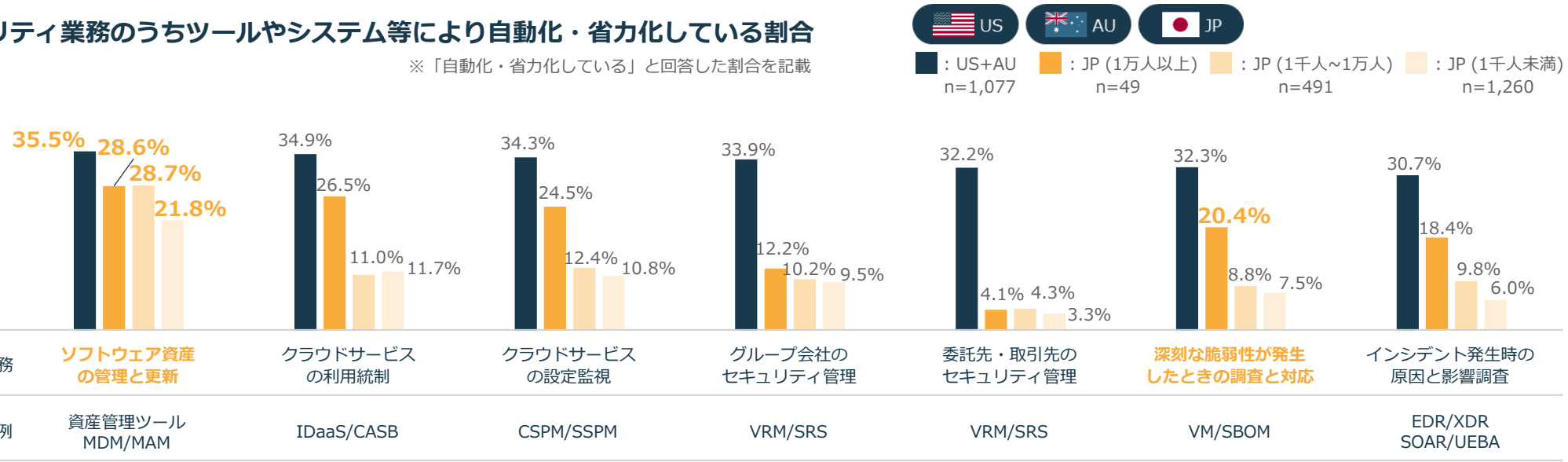
- 米・豪ではCISOなどが、人材戦略を明確にすることで、トップダウンで自動化・省力化を図っていると推察される。
- 更に米・豪ではジョブ型雇用が主流であり、自社で賄うべきセキュリティ業務が整理されているため、自動化・省力化すべき業務の精査が容易である。こうした背景が日本の結果との差異を生んでいると推察される。
- 人材不足に悩む日本企業は、一足飛びに自動化・省力化を目指す必要はなく、まずは現状のセキュリティ業務の棚卸しから始めたい。そのうえで自社に必要な各業務に対し、フローやマニュアルの定型化・標準化、システムやツール導入による自動化などに取り組むことが望ましい。
- 業務の自動化は人的リソース不足の解消や生産性向上に留まらず、ルーチンワークによるモチベーション低下や手作業による人為的ミスの低減なども期待される。こうした従業員が享受できるメリットについても押さえておきたい。

3 セキュリティ業務の自動化・省力化

日・米・豪ともに、ソフトウェア資産の管理と更新の自動化・省力化率が最も高い
深刻な脆弱性が発生したときの影響調査・対応における効率化の必要性が増している

セキュリティ業務のうちツールやシステム等により自動化・省力化している割合

※「自動化・省力化している」と回答した割合を記載



Key Results

自動化・省力化が最も進む業務

JP US AU ソフトウェア資産の管理と更新

深刻な脆弱性が発生時の調査対応

JP 1万人以上 **約20%** 自動化・省力化している

Key Insights

- 日・米・豪ともに「ソフトウェア資産の管理と更新」の自動化率の高さから、ニューノーマルかつ多様な働き方の採用に伴う業務端末などの社外持ち出しに備え、IT資産の可視化並びにOS設定・パッチの適用などを自動で実施したい需要の高まりがうかがえる。
- Log4Shell（2021年12月公開）のような深刻な脆弱性の発生時には、多くの企業において影響範囲の調査に多くの労力を要した。脆弱性検知や影響度の可視化、パッチの適用を自動サポートするVM(Vulnerability-Management) やソフトウェアの構成情報を一元的に管理し、脆弱性の迅速な調査をもたらすSBOM(Software Bill of Materials)の導入が、今後進むと予想する。

4 セキュリティ対策を実施するきっかけ

日本も米・豪のように、経営層がリーダーシップ発揮しプロアクティブに対策推進すべき
株主や取引先に対し、自社のリスクや対策状況・人的資本を開示する流れが一層強まると予想

直近1年に実施したセキュリティ対策の実施のきっかけや理由

	JP n=1,656	US n=524	AU n=524
1位	35.0% 他社でのセキュリティインシデント事例	55.3% 経営層のトップダウン指示	46.6% 経営層のトップダウン指示
2位	33.0% テレワークなど働き方の変化に伴う対応	23.1% 競合他社の実施状況との比較	33.6% 他社でのセキュリティインシデント事例
3位	29.3% 自社でのセキュリティインシデント	22.9% 他社でのセキュリティインシデント事例	32.3% 株主や取引先からの要請
4位	20.2% 経営層のトップダウン指示	20.4% 株主や取引先からの要請	23.7% 持株会社や親会社からの要請
5位	14.7% 内部監査・内部有識者からの指摘	19.3% 外部監査・第三者評価の結果	21.2% 自社でのセキュリティインシデント

※ 他選択肢：DX化推進に伴う対応／昨今の国際情勢を踏まえた監督省庁からの注意喚起／関連法規の改定（具体的な関連法規を記載）／監督省庁からのセキュリティ対策強化の要請（自治体からの要請を含む）（具体的な要請内容を記載）／その他（具体的に記載）

※ わからないを除く

Key Results

リアクティブな日本、プロアクティブな米・豪

経営層のトップダウン指示

JP 約20% ▶ US AU 50%前後

評価する時代から評価される時代へ

株主や取引先からの要請

US 約20% AU 約32%

Key Insights

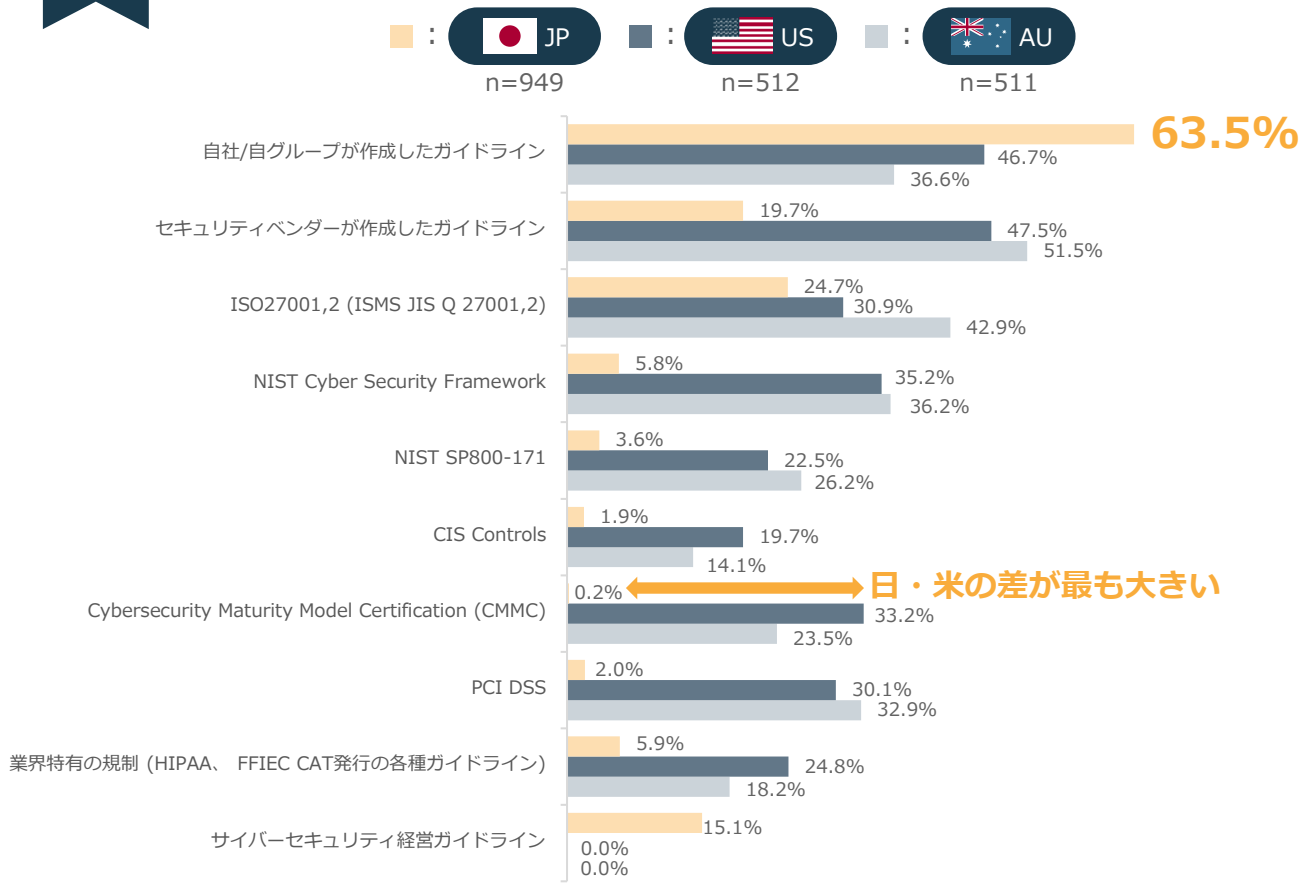
- 米・豪では、セキュリティリスクが顕在化する前にCISOがリーダーシップを発揮し、経営層からのトップダウン指示で推進できるセキュリティ体制があることがうかがえる。
- ESG投資の拡大に伴い、株主やステークホルダーに対し、自社のリスクや対応方針を盛り込んだ非財務情報、セキュリティ人的資本などの積極的な情報開示がより一層求められると予見する。
- 委託先・取引先からの要請に応じ、自社を評価する時代から、サプライチェーンの枠組みで、社外・外部からも評価される時代へと差し掛かっていることを意識したい。

4 評価に用いるセキュリティガイドライン

日本は独自に作成したガイドラインやチェックリストをベースに評価を実施
セキュリティ評価の共通の物差しとして、公的機関が作成したガイドラインの活用検討が望まれる

セキュリティ評価を実施している企業が参考にするセキュリティガイドライン

※ セキュリティ評価を実施していると回答した企業のみ対象



Key Results

日本企業が参考にするガイドライン

JP **約64%** 自組織が作成したガイドライン

日本と米国の差 No.1

Cybersecurity Maturity Model Certification (CMMC)

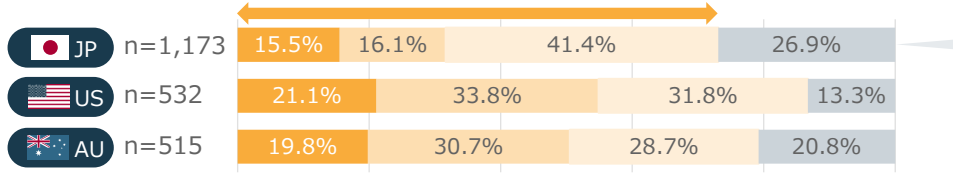
Key Insights

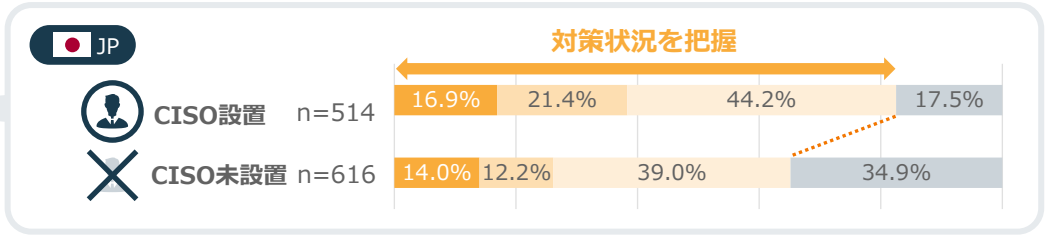
- 自組織が作成したガイドラインを活用することで、自社の実態に即した評価ができる一方、事業環境の変化や脅威動向の変化に伴い、ポリシーの見直しや項目の更新などの対応に負荷がかかることが推察される。
- 取引先や委託先を選定する際に、セキュリティ対策状況が評価される事例が増える中で、公的機関が作成した各種ガイドラインの活用を検討したい。共通の物差しで双方ともに評価可能となり、人材不足に悩む企業にとって、評価業務の効率化にも繋がると考えられる。
- 日本においても防衛省のサイバーセキュリティ調達基準の元となるNIST SP800-171や、サプライチェーンのセキュリティ対策に対応するCMMC等の採用が今後ますます進むと予想される。

4 サプライチェーンのセキュリティ（グループ管理）

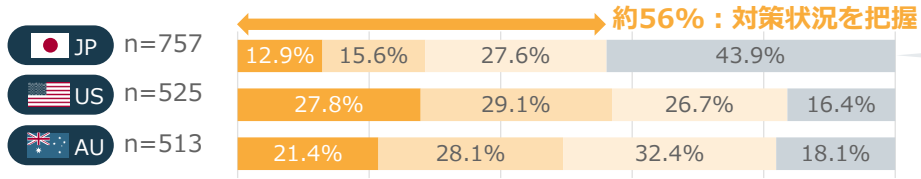
子会社・グループ会社の統制として、国内・国外ともに半数以上が対策状況を把握
日本国外は４割が対策を把握できておらず、新たな打ち手が求められる

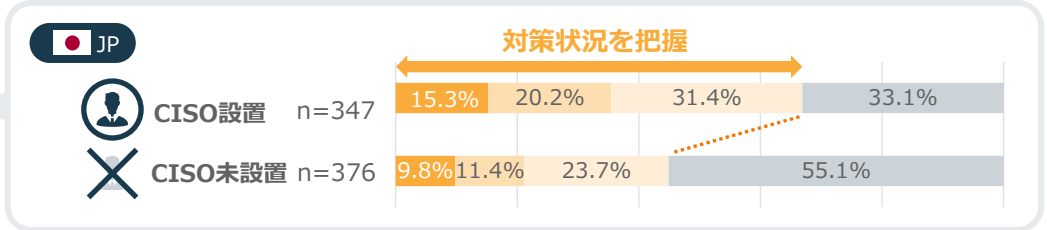
国内関連子会社／グループ会社への統制状況





国外関連子会社／グループ会社への統制状況





■ 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
■ セキュリティ対策状況を把握している
■ セキュリティ対策状況を把握していない
※ 該当なしを除く

Key Results

日本企業のグループ統制状況（国内／国外）

約73% 約56%

米・豪におけるグループ会社の統制状況

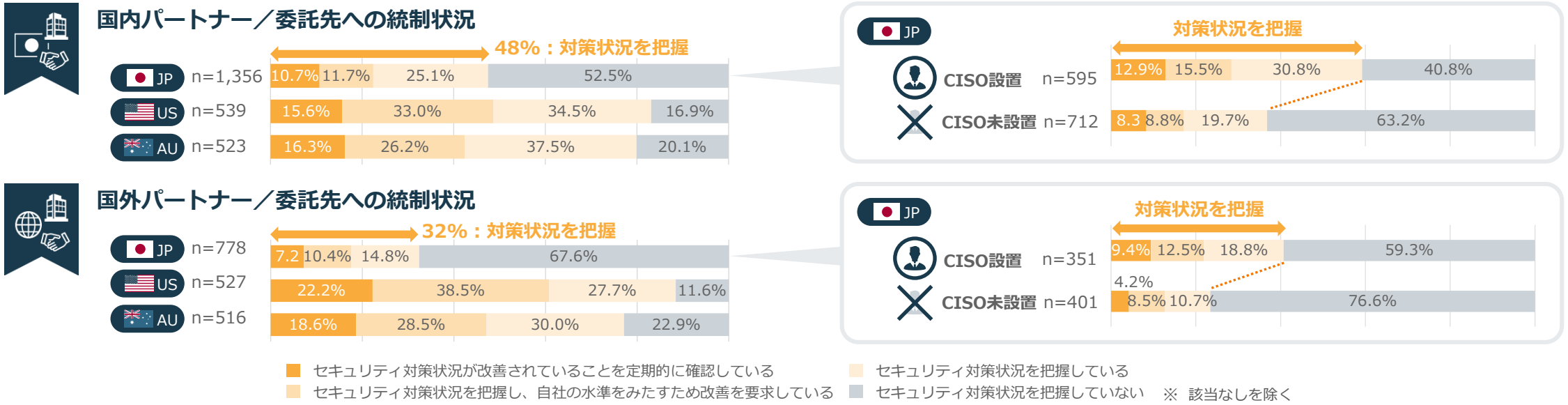
US AU 80%以上

Key Insights

- 国外への統制は、NIST Cyber Security Frameworkなど、グローバルガイドラインの活用やグローバルガイドラインを参照した自社ルールの作成が要求事項の妥当性説明に有用である。
- 加えて、ASM（アタックサーフェス管理）や SRS（セキュリティレーティングサービス）などインターネット上の公開情報や攻撃者視点より得られるセキュリティの格付け評価、それにより検出された具体的な課題と改善案の提示を組み合わせることが、人手の労力を削減しつつ、世界中のグループ会社に対する合理的なセキュリティ統制と対策推進への有効な打ち手となる。

4 サプライチェーンのセキュリティ（委託先管理）

日本では、国内/国外の委託先を問わず、セキュリティ対策状況の把握比率が半数以下に留まる
米・豪で、対策状況の把握比率が8割を超えているのは、VRMツールの活用が理由と推察



Key Results

日本企業の委託先統制状況（国内／国外）

約48% 約32%

米・豪における委託先の統制状況

US AU 80%以上

Key Insights

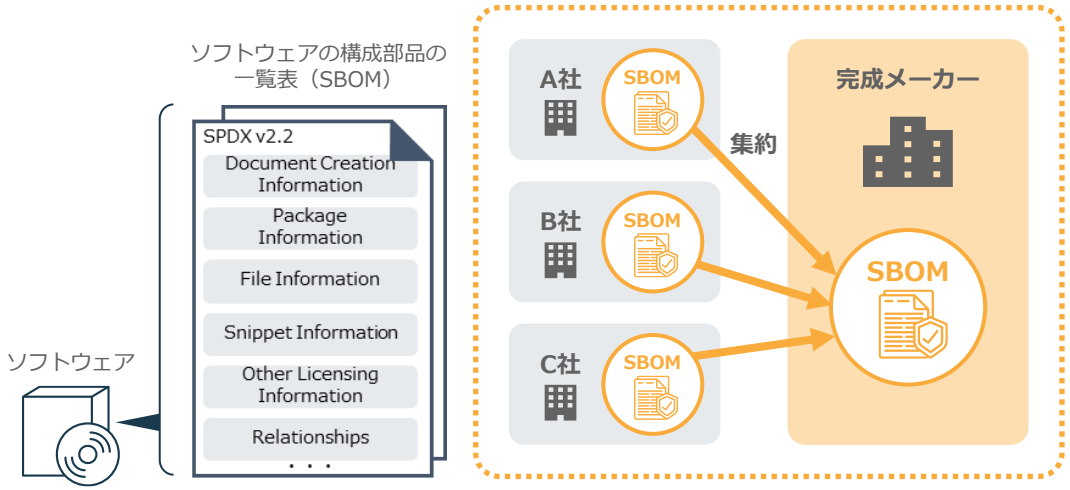
- 日本企業において委託先への統制状況が半数以下に留まっている理由として、対応人材や予算の不足、委託先管理の対象数の多さや複雑さ、委託先は別法人であることから委託元として状況を把握した後の改善活動の促進・関与が難しいことなどが背景にあると考えられる。
- 米・豪で委託先の対策状況の把握比率が80%以上となっているのは、大量の委託先管理を効率的かつ継続的に実現するために、VRM（ベンダーリスクマネジメント）ツールの活用が進んでいることが一因と考えられる。今後、日本でもVRM活用が進んでいくことが予想される。

【解説】注目のサプライチェーンリスク管理ソリューション

SBOM（Software Bill of Materials）

■SBOMを利用中／検証中と回答した企業の割合

JP 3.3% n=1,800　US 52.3% n=547　AU 60.2% n=530



VRM（Vendor Risk Management）

■VRMを利用中／検証中と回答した企業の割合

JP 4.4% n=1,800　US 58.5% n=547　AU 63.8% n=530

- SBOM(Software Bill of Materials)は、製品に含まれるソフトウェアを構成するコンポーネントの一覧表であり、OSS(Open Source Software)のライセンス管理、脆弱性の管理や迅速な調査、ソフトウェアサプライチェーンリスク管理等の用途で利用されている。
- 2021年5月に発出された米国大統領令（EO14028）において、政府調達におけるSBOM活用の検討指示が明記されたことをきっかけに、SBOMが急速に普及しつつある。日本でも経産省により、産業分野ごとのSBOM導入に向けた議論や実証実験が始まっている。

- VRM(Vendor Risk Management)は、企業が取引先や委託先の製品・サービスが、規制・財務・オペレーションの面で負の影響を発生させないようにするためのリスク管理プロセスである。近年、サプライチェーン攻撃やランサムウェア攻撃などのサイバーリスクが高まっていることから、セキュリティ観点でのVRM確立が喫緊の課題になっている。
- グローバル化が進むビジネス環境では、自社のリソースだけでビジネスは完結せず、委託先・取引先が増え続けていることから、統制業務の効率化や継続的評価の実現のため、VRMツールへの注目が高まっている。

国際情勢を踏まえたサイバー注意喚起

同じ危機に際して、人的対策を重視する日本と、技術的な対策を進める米・豪の意識差が明確に
従業員の意識や行動に期待する対策だけでなく、技術的なセキュリティ対策の強化が欠かせない

2022年2月以降に発出したサイバー注意喚起を契機に実施したセキュリティ対策

※ 各国では昨今の国際情勢を踏まえ、2022年2月以降、各種公的機関よりセキュリティ対策の注意喚起が発出された。

リスク低減のための措置

	アカウントの棚卸しやパスワードの見直し	多要素認証の有効化	情報資産の保有状況と機器構成の把握	脆弱性の把握とパッチの適用	クラウドサービスの設定の見直し	従業員への注意喚起や周知
JP n=1,772	28.6%	15.2%	18.0%	30.3%	9.4%	**67.1%**
US n=540	30.6%	**41.9%**	39.8%	33.0%	**25.4%**	35.2%
AU n=528	29.7%	**45.8%**	44.9%	34.5%	**19.5%**	29.7%

インシデントの早期検知

	ログの監視体制の強化	自社に関わる認証情報の流出有無などの確認
JP n=1,772	18.3%	1.9%
US n=540	20.9%	**15.4%**
AU n=528	15.3%	**9.1%**

インシデント発生時の適切な対処・回復

	データのバックアップの実施方法や復旧手順の見直し	インシデント発生時の組織体制の見直しや整備
JP n=1,772	17.9%	17.7%
US n=540	22.0%	15.9%
AU n=528	14.6%	15.9%

※ わからないを除外

Key Results

日本が最も実施した対策

JP 約67% 従業員への注意喚起

日本と米豪の対策意識の差異

人的対策（注意喚起） JP ⟷ US AU 技術的対策（多要素認証、クラウドの設定見直し etc）

Key Insights

- 日本では「従業員への注意喚起や周知」の実施率が最も高く、人的対策を優先する意識が高い。企業と従業員を危機から守るためには、具体的な対策内容や技術的な仕組みの提供が必須であり、注意喚起のみでの効果は期待できない。
- 米・豪では「多要素認証の有効化」や「クラウドサービスの設定見直し」など技術的対策の優先度が高い。また「自社に関わる認証情報の流出有無などの確認」の日本との差異が大きく、サイバー攻撃への警戒感、並びに危機に対する当事者意識の高さがうかがえる。
- 今後さらに増加しうるサイバー脅威やセキュリティ人材不足である情勢を踏まえて、人的対策のみならず、自社のセキュリティの総点検並びに技術的対策の実施を推奨する。

セキュリティ専門組織の構築状況

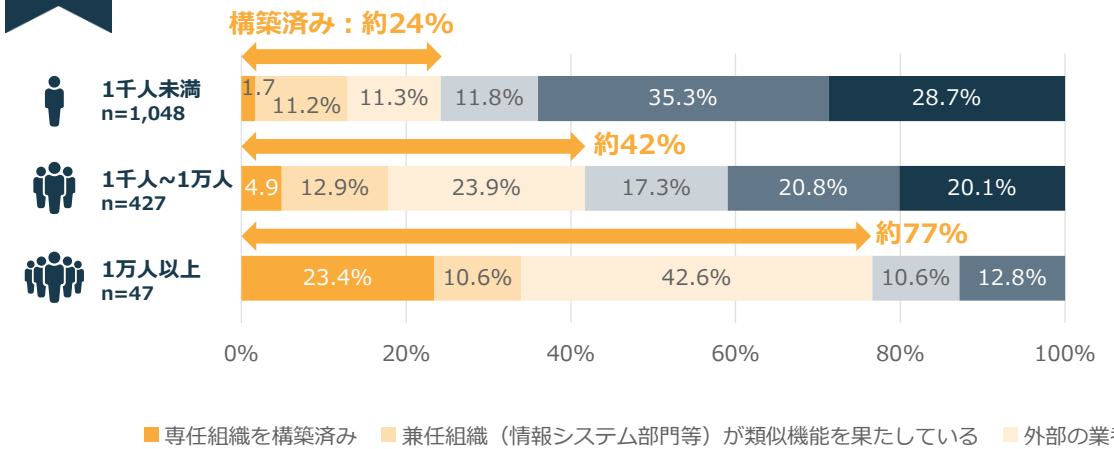
従業員規模が大きい企業ほど、SOC・CSIRTを構築している割合が高い
DXやゼロトラストの進展と共に、セキュリティ専門組織も進化していく

PSIRT※1の構築率
8.7% (n=1,401)
※1:Product SIRT

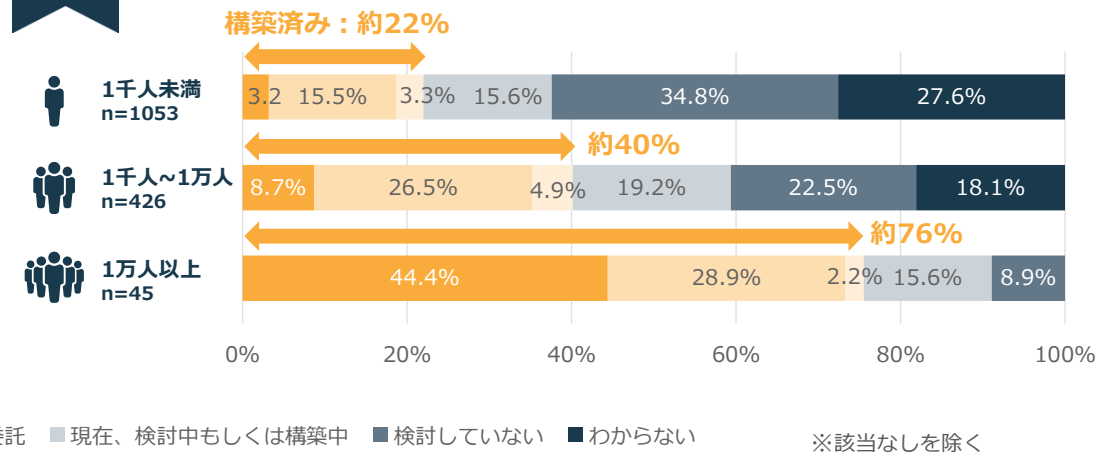
SSIRT※2の構築率
7.3% (n=1,401)
※2:Service SIRT

JP ※該当なしを除く

SOCの構築状況 JP



CSIRTの構築状況 JP



■専任組織を構築済み ■兼任組織（情報システム部門等）が類似機能を果たしている ■外部の業者に委託 ■現在、検討中もしくは構築中 ■検討していない ■わからない

※該当なしを除く

Key Results

SOCを構築する企業割合

1千人未満：**約24%**
1千人~1万人：**約42%**
1万人以上：**約77%**

CSIRTを構築する企業割合

1千人未満：**約22%**
1千人~1万人：**約40%**
1万人以上：**約76%**

Key Insights

- 従業員規模が大きい企業ほど、事業を国内・海外に展開し、アタックサーフェス（攻撃対象領域）が広がっていることから、単体・グループにてSOCやCSIRTを構築している割合が高い。
- DXやテレワークの進展を受け、ゼロトラストモデルを採用する企業が増えている。今後のSOCやCSIRTは、企業規模を問わず、24時間365日攻撃を受けることを前提に進化していく。
- 高度専門性が必要なことから、大企業ではPrivate SOCをセキュリティベンダーと共同運営する選択肢がある。中堅・中小企業ではクラウドとSaaSのセキュリティ機能を組み合わせたSOCが主流になっていくことが今後予想される。

発生したセキュリティ事件／事故

企業規模を問わず、大企業ほど標的型メール攻撃やランサムウェアが増加
中堅・中小企業は、サイバー攻撃を検知できてない可能性が高い点が課題

過去1年間で発生したセキュリティ事件／事故

JP

	1千人未満 n=1,260	1千人～1万人 n=491	1万人以上 n=49
1位	**56.3%** 特になし	42.2% 標的型メール攻撃	**46.9%** 標的型メール攻撃
2位	26.3% 標的型メール攻撃	**36.0%** 特になし	36.7% マルウェア感染
3位	11.1% マルウェア感染	21.6% マルウェア感染	**22.4%** 特になし
4位	5.2% ランサムウェア	7.3% ランサムウェア	**20.4%** ランサムウェア
5位	3.7% DoS攻撃／DDoS攻撃	6.1% DoS攻撃／DDoS攻撃	18.4% DoS攻撃／DDoS攻撃
6位	3.4% Webアプリケーションの脆弱性を突いた攻撃	5.3% 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	16.3% 退職者、転職者による不正アクセスや持出
7位	2.7% わからない	4.9% Webアプリケーションの脆弱性を突いた攻撃	12.2% サプライチェーン攻撃
8位	2.5% 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	3.7% サプライチェーン攻撃	10.2% 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

※ 他選択肢：水飲み場型攻撃／リスト型アカウントハッキング／クラウドサービス（IaaS/PaaS/SaaS）の設定ミスによる情報漏えい／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／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／その他（具体的に記載）

Key Results

「特になし」を回答

1千人未満の企業の **約56%**

従業員1万人以上の企業被害

約47% 標的型メール攻撃　**約20%** ランサムウェア

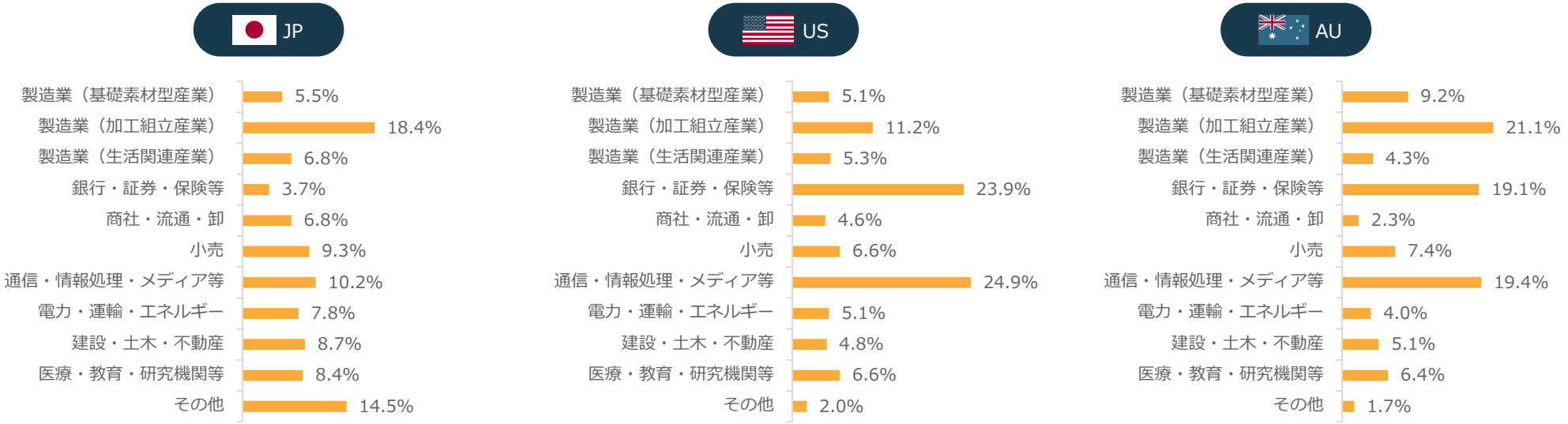
Key Insights

- 企業の従業員規模が小さくなるにつれ、「特になし」の回答率が増加している。SOC・CSIRTといったセキュリティ対応態勢を整備していない中小企業では、インシデント自体を検知できていない可能性が高い。
- 2022年は、取引先や委託先のランサムウェア感染をきっかけとして、その被害がサプライチェーンに影響を及ぼすケースが多かった。
- 2023年も、標的型メール攻撃やランサムウェアは引き続き猛威を振るうことが予想される。人的対策に加え、EDRやCASBなどのゼロトラストを強化する技術的対策がより求められる。

回答者属性

回答企業数：合計2,877社（JP 1,800社、US 547社、AU 530社）
日本企業向けのアンケートにおける調査対象企業の業種・従業員数は外部の企業情報データベースから取得

回答いただいた企業の業種



※ 回答企業の業種を以下のように分類

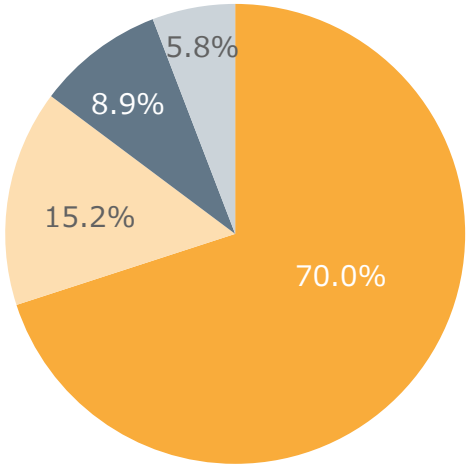
- 製造業（基礎素材型産業）：金属、化学、紙・パルプ、その他素材・素材加工品
- 製造業（加工組立産業）：機械・電気製品、輸送機器・部品製造、その他製品製造
- 製造業（生活関連産業）：バイオ・医薬品、繊維・アパレル、食品
- 銀行・証券・保険等： 銀行、証券、保険、その他金融
- 通信・情報処理・メディア等：システム・ソフトウェア開発、通信、メディア・広告、その他情報処理
- 電力・運輸・エネルギー：鉄道・航空、運輸、エネルギー
- 建設・土木・不動産：建設、不動産
- 医療・教育・研究機関等：医療、飲食、教育、法人サービス、消費者サービス

回答者属性

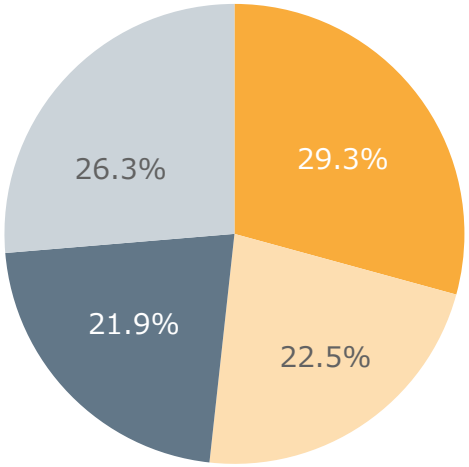
回答企業数：合計2,877社（JP 1,800社、US 547社、AU 530社）
日本企業向けのアンケートにおける調査対象企業の業種・従業員数は外部の企業情報データベースから取得

回答いただいた企業の従業員数・回答者の所属

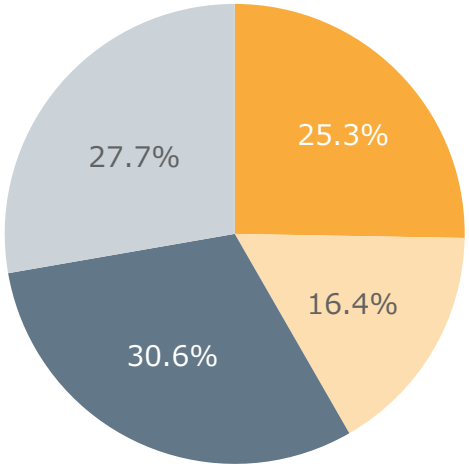
JP



US



AU



- ～千人未満
- 千人～2千人未満
- 2千～5千人未満
- 5千人以上

回答いただいた担当者の所属部署

調査対象国全てにおいて、回答者の主な所属部署は情報システム部、情報セキュリティ部等のIT業務に携わる部署であった

調査方法

調査方法	WEBによるアンケート
調査対象	企業の情報システム・情報セキュリティ担当者
調査期間	日本　：2022年7月20日～2022年9月25日 アメリカ、オーストラリア：2022年8月15日～2022年8月24日 注：「把握していない」「不明」という回答や無回答の除外、パーセンテージの切り上げ等により、選択肢の合計値が100%にならない場合があります

お問い合せ先

info@nri-secure.co.jp

制作委員

制作	NRI Secure Insight 2022　制作委員会
企画	薮内 俊平
執筆	山田 真暉　松本 彩花
アドバイザー	池田 泰徳　佐藤 健　観堂 剛太郎 石井 晋也　稲田 憲昭　西田 助宏 渡部 惣　遠藤 良二　長谷川 剛 延 優介　半田 伸太郎　名部井 康博 日下部 美弥子　大野 勝紀　月岡 稚恵　西 はる菜
監修	足立 道拡　川崎 聡太　大高 ともり
名誉監督	菅谷 光啓

RIセキュアテクノロジーズについて

会社名	NRIセキュアテクノロジーズ株式会社
英語表記	NRI SecureTechnologies, Ltd.
本社	〒100-0004 東京都千代田区大手町 1-7-2 東京サンケイビル
横浜ベイ オフィス	〒221-0056 神奈川県横浜市神奈川区金港町 1-7 横浜ダイヤビルディング
北米支社	26 Executive Park Suite 150 Irvine CA 92614 U.S.A.
代表取締役社長	建脇 俊一
設 立	2000年8月1日
資本金	4.5億円
株 主	株式会社野村総合研究所
社員数	連結：642名　単体：525名 ※2022年10月現在延べ人数

資格取得者数

105名 CISA
（公認情報システム監査人）

95名 CISSP
（情報システム・セキュリティ・プロフェッショナル認定資格）

80名 CISM
（公認情報セキュリティマネージャー）

304名 GIAC
（Global Information Assurance Certification）

※2022年10月現在、延べ人数

RI Secure Insight （企業における情報セキュリティ実態調査）

NRIセキュアテクノロジーズは情報セキュリティ実態調査を**20年**にわたり実施し、のべ**20,367社から回答**を収集してきました。

2002年：249社

2003年：280社

2004年：235社

2005年：447社

2006年：449社

2007年：688社

2008年：785社

2009年：804社

2010年：702社

2011年：599社

2012年：741社

2013年：685社

2014年：660社

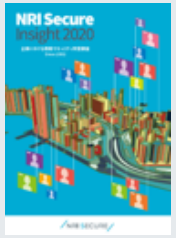
2015年：665社

2017年：1,301社
(内訳)
日本：667社
海外：634社

2018年：1,110社
(内訳)
日本：107社
海外：1,003社

2019年：2,807社
(内訳)
日本：1,794社
海外：1,013社

2020年：2,260社
(内訳)
日本：1,222社
海外：1,038社



2021年：2,653社
(内訳)
日本：1,616社
海外：1,037社

2022年：2,877社
(内訳)
日本：1,800社　海外：1,077社

new

NRI SECURE

NRI Secure Insight 2022

企業における情報セキュリティ実態調査

Since 2002

本資料のダウンロードはこちら

https://www.nri-secure.co.jp/download/insight2022-report

NRIセキュアテクノロジーズ株式会社