NRI Secure Insight 2023

企業における情報セキュリティ実態調査　Since 2002

NRIセキュアテクノロジーズ株式会社

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20回実施してきた「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、21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 2023」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1,657社、アメリカ540社、オーストラリア586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：2023/8/1-2023/9/29 • アメリカ、オーストラリア：2023/9/8-2023/9/29
回答いただいた企業数	計 2,783社（日本：1,657社、アメリカ：540社、オーストラリア：586社）

セキュリティマネジメント

ソリューションの導入状況

JP n=1,657

前年度比 +8.9pt

	EDR※1	NDR※1	XDR※1
対応実施済み	27.8%	11.9%	6.5%
検討・検証中	34.3%	41.1%	36.6%

セキュリティ対策

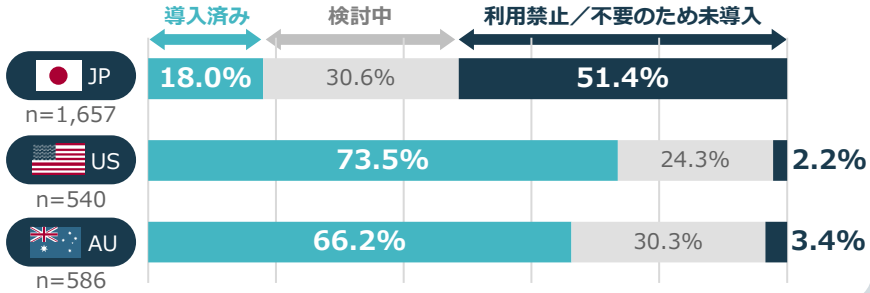
DMARC 実施率

JP n=1,657

未対応・わからない率 約74%　検討中 約13%　実施済み※2 13%

生成AI

生成AIの導入状況

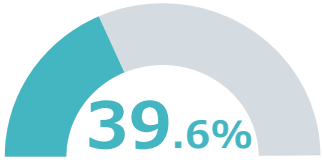


※1 E = Endpoint、N = Network、X = EXtended / DR = Detection and Response
※2 None (なにもしない)、Quarantine (検疫)、Reject (拒否)のいずれかを実施している回答割合

サプライチェーン

経済安全保障推進法に関連し、セキュリティの強化を意識している割合

JP n=1,657



サプライチェーンのセキュリティ統制状況

JP n=1,657

SBOM※3を利用中／検証中と回答した企業の割合

JP n=1,657 **3.2%**

US n=540 **82.1%**

AU n=586 **77.4%**

※3 Software Bill of Materials（ソフトウェア部品表）

CONTENTS

調査結果

1 セキュリティマネジメント 5

2 サプライチェーン 11

3 セキュリティ対策 19

4 生成AI 23

回答者属性 27

調査方法 28

制作委員 29

調査結果

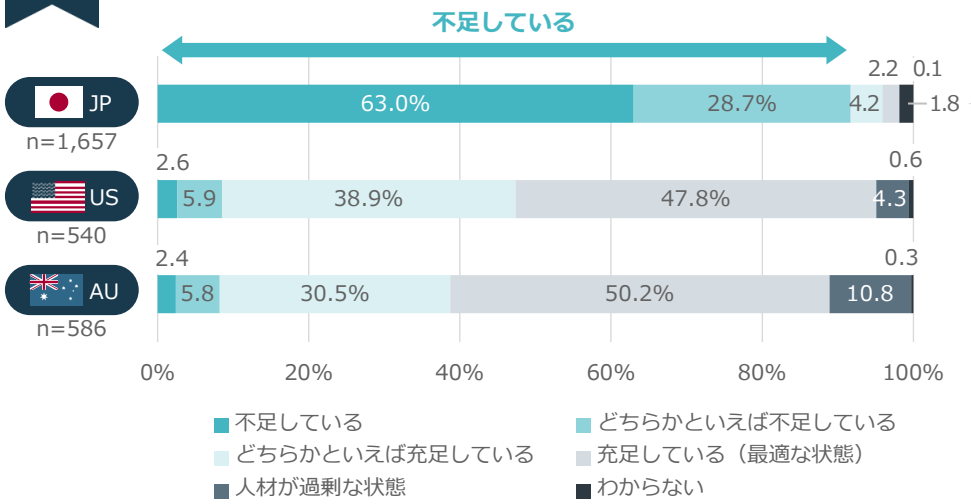
CATEGORY

1. セキュリティマネジメント
2. サプライチェーン
3. セキュリティ対策
4. 生成AI

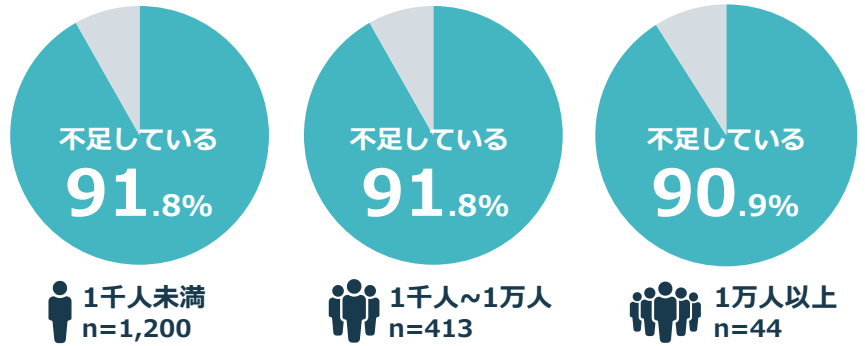
1 セキュリティ人材

日本では約9割の企業でセキュリティ人材が不足しており、直近10年で同様の傾向
日本企業のセキュリティ人材不足は、企業規模によらない共通の課題

セキュリティ人材の充足状況



JP 従業員数別



※ 不足している：「不足している」「どちらかといえば不足している」のいずれかを回答

Key Results

セキュリティ人材が不足していると回答

JP 約90%

1千人未満 ＝ 1千人~1万人 ＝ 1万人以上

Key Insights

- 日本では約9割がセキュリティ人材が不足していると回答しており、慢性的な人材不足の傾向が10年以上続いている。企業規模による回答の差は見られず、日本企業の共通的な課題であることを示す結果となった。
- 少子高齢化の進行により、日本の生産年齢人口は減少している。また、DXの進展により、企業におけるセキュリティリスクは多様化・深刻化しており、セキュリティ人材の希少価値はさらに増している。
- セキュリティ人材不足を解消するために、人材の獲得・育成は依然として有効な打ち手であるが、その数は有限である。解消を後押しする補完策・代替策の検討や実践が欠かせない。

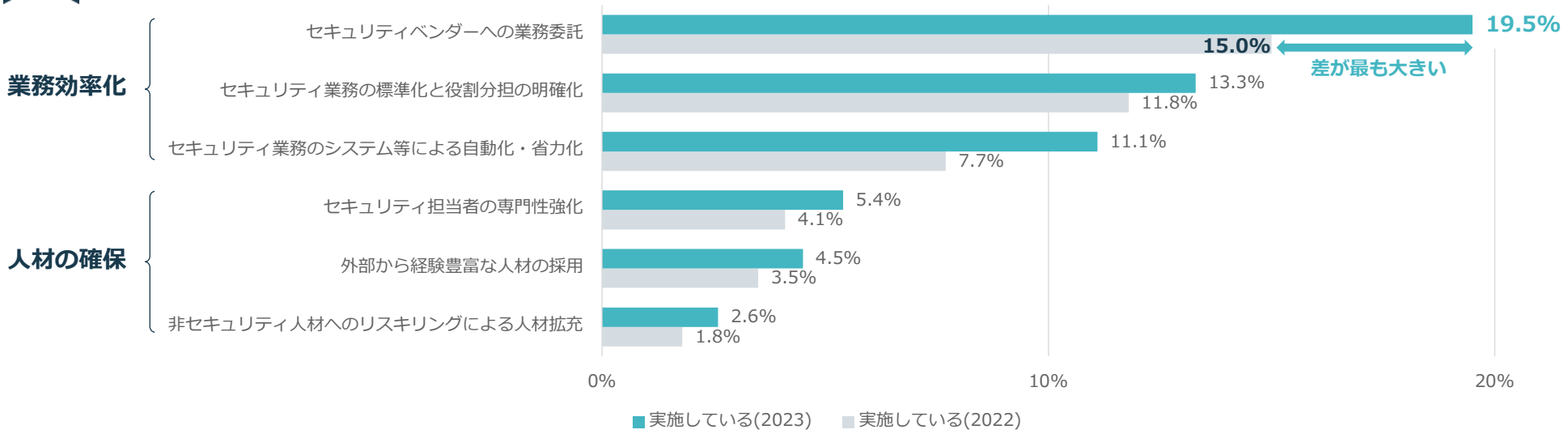
1 セキュリティ人材不足を補う施策

人材不足を補う施策として業務委託の実施率が最も高いが、2割弱に留まっている
サステナブルなセキュリティ活動に向けて、複数施策の計画・実行が求められる

「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=1,520

※ 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のみ対象



Key Results

増加した施策（前年度比）

No.1	セキュリティベンダーへの業務委託	+4pt
No.2	セキュリティ業務のシステム等による自動化・省力化	+3pt

Key Insights

- 「セキュリティベンダーへの業務委託」はセキュリティ業務を効率的・効果的に実施する上で有効な選択肢であるが、サステナブルなセキュリティ活動を実現するためには、セキュリティ人材の確保やセキュリティ業務の効率化などの複数施策をバランスよく実践していくことが求められる。
- 実施率が最も高い業務委託の回答が2割弱に留まっている理由は、セキュリティ関連予算の不足や現場が常時繁忙で検討や実行の時間が取れないことなどが原因と推察する。人材不足の真の解消には、経営主導の積極的な予算確保などの配慮や現場の後押しが欠かせない。

1 セキュリティ担当者の困りごと

企業規模により順位は異なるが、困りごとの背景にサイバー脅威の影響がうかがえる
規模が大きい企業ほどサプライチェーン統制が必要であり、人材不足に拍車をかける

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 従業員数別

※ 最大3つの複数選択可

	1千人未満 n=1,200	1千人～1万人 n=413	1万人以上 n=44
1位	39.5% セキュリティインシデント発生時の緊急対応	43.1% セキュリティ人材の育成	50.0% セキュリティ人材の育成
2位	37.3% サイバー攻撃の高度化への対応	41.2% セキュリティインシデント発生時の緊急対応	43.2% 業務委託先や取引先のセキュリティ統制・管理
3位	36.5% セキュリティ人材の育成	33.9% グループ会社・国内外拠点のセキュリティ統制・管理	29.5% サイバー攻撃の高度化への対応
4位	34.0% 自社セキュリティ対策の遅れ（最新技術・動向の未反映）	31.2% 自社セキュリティ対策の遅れ（最新技術・動向の未反映）	27.3% セキュリティインシデント発生時の緊急対応
5位	19.6% セキュリティ脅威・事故に関する情報収集と関係者共有	31.0% サイバー攻撃の高度化への対応	25.0% 自社セキュリティ対策の遅れ（最新技術・動向の未反映）

※ 他選択肢：セキュリティ業務の状況・進捗に関する経営層への報告 ／ セキュリティ対策のトレンド・他社動向の把握 ／ 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

IPA情報セキュリティ10大脅威※が上位の困りごとに影響と予想

- 10大脅威の1位 ランサムウェア
  - セキュリティインシデント発生時の緊急対応
  - サイバー攻撃の高度化への対応
- 10大脅威の2位 サプライチェーン攻撃
  - グループ会社・国内外拠点のセキュリティ統制・管理
  - 業務委託先や取引先のセキュリティ統制・管理

Key Insights

- 従業員数が1千人以上の企業では、人材育成とグループ会社や委託先の統制・管理に関する困りごとが上位にある。IPAの10大脅威の2位であるサプライチェーン攻撃に対応する一方で人材不足に拍車がかかっていると推察する。
- 1千人未満の企業の1位・2位にあるように、セキュリティの事前対策と事後対応への意識が高まっている。
- サプライチェーン攻撃では、規模の小さい企業も狙われるため、グループ会社や委託元からの統制は広範囲に及ぶ。1千人未満の企業は、その要請に対応することでセキュリティ意識がさらに高まることが予想される。

※参考　IPA『情報セキュリティ10大脅威 2023』
https://www.ipa.go.jp/security/10threats/10threats2023.html

1 セキュリティ対策の新しいソリューション

サイバー攻撃・被害の増加やテレワークの浸透などを背景にEDRの導入が普及
EDRの導入が進むほど、運用の高度化および負荷軽減のためにXDRの注目が高まる

ソリューションの導入状況

JP n=1,657

			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	遠隔での端末内潜伏脅威探索(スレットハンティング)とNW隔離、フォレンジック対応	62.0%	27.8%	10.6	23.7%	23.4%	14.6
2位	NDR	組織内のネットワーク上の通信内容の監視・脅威検出	53.0%	11.9	9.1	32.0%	28.3%	18.6
3位	CASB	クラウド利用の可視化・制御	44.6%	6.7	7.9	30.0%	32.7%	22.7%
4位	XDR	複数のセキュリティレイヤーにわたる一元的な脅威の検知、調査、対応	43.1%	6.5	8.2	28.4%	34.1%	22.8%
5位	IDaaS	クラウド型ID・アクセス管理	40.8%	8.3	7.4	25.1%	35.2%	24.0%
6位	SOAR	セキュリティアラート等への対応自動化	39.1%	5.3	5.2	28.6%	35.6%	25.3%
7位	UEBA	ユーザ行動に関わるログの統合分析とアラート	37.0%	8.4	5.2	23.4	35.7%	27.3%
8位	CSPM	クラウドセキュリティ態勢管理	31.3%	3.1	3.9	24.3	39.9%	28.8%
9位	SSPM	SaaSのセキュリティ態勢管理	29.1%	1.8	4.1	23.2	41.2%	29.8%
10位	TLPT	脅威ベースのペネトレーションテスト	27.3%	4.5	4.0	18.8	43.0%	29.7%
11位	VRM	ベンダーリスクの継続的な管理	22.3%	1.6	2.5	18.2	48.1%	29.6%

Key Results

EDR導入済み

2022年 18.9% → 2023年 27.8%

XDR※を導入済み、検証中または検討中

約43%

EDR普及に伴う運用負荷の増加が背景

※ EXtended Detection and Response

Key Insights

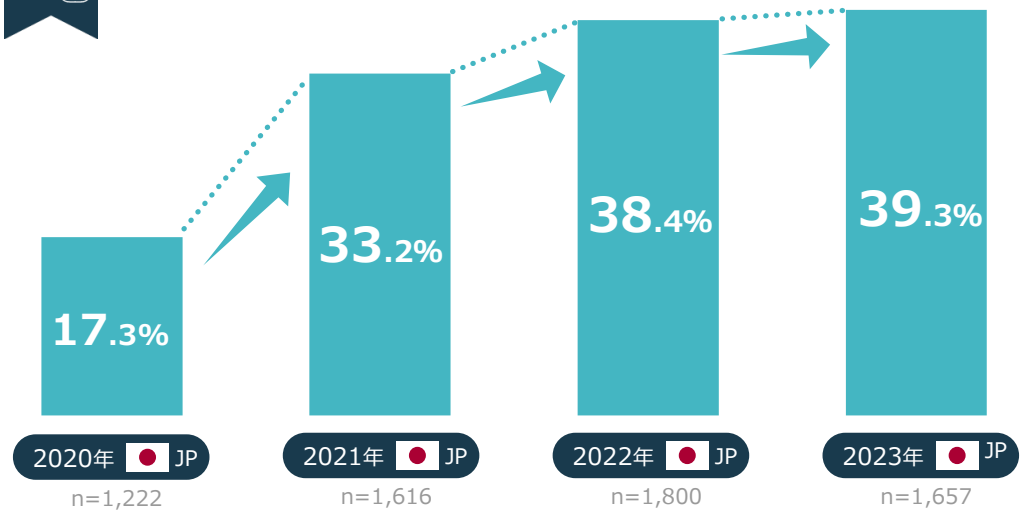
- Emotetの流行やランサムウェアによる攻撃の増加、テレワークを前提にしたセキュリティ体制を背景に、日本のEDR導入率が上昇している。一方で、EDR運用負荷の増大という新たな課題を抱えている。
- 社内ネットワークの膨大な通信に対して、異常を検知・対応するNDRの導入・検討率が高い。その背景は、近年増加傾向にあるVPN機器やリモートデスクトップ経由の侵入等に対応することが一因と推察される。
- EDRの運用負荷の高まりに対応するため、EDRとNDRを包括し、複数のセキュリティレイヤーからの情報を基に自動で検知・対応するXDRの導入・検討が進むと予想される。

セキュリティ用語解説：XDR https://www.nri-secure.co.jp/glossary/xdr

1 サイバー保険

サイバー保険の加入率は毎年上昇傾向にあったが、2023年は横ばい傾向に変化
加入理由の1位から、サプライチェーン攻撃への警戒や関心がうかがえる

サイバー保険加入率の推移



サイバー保険への加入理由

JP n=652

※ 最大3つの複数選択可

1位	67.6%	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
3位	28.2%	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）／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／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／トップダウンの指示があったため／など

Key Results

サイバー保険の加入率は横ばい

38.4% 2022年 → 39.3% 2023年

サイバー保険の加入理由3年連続1位

67.6% 自社の対応だけでは被害を防ぎきれない

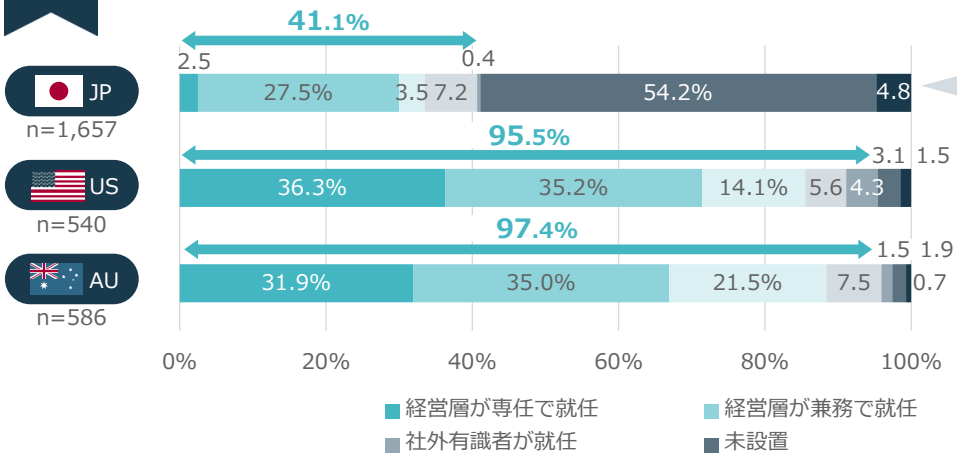
Key Insights

- サイバー保険の加入率は2022年まで年々上昇していたが、2023年の加入率は、ほぼ横ばいの結果となった。その理由として、サイバー保険がリスク移転のセキュリティ対策として浸透し、サイバー保険を必要と考える企業の導入が一巡したことが要因として考えられる。
- サイバー保険への加入理由は自社の対応だけでは防ぎきれないためと回答した企業が多く、サプライチェーン攻撃など自社以外を起点としたサイバーリスクへの懸念があると推察する。
- セキュリティ事故は初動対応が遅れるほど、被害の拡大に直結する。サイバー攻撃のリスクや被害の影響を考慮し、事後対応に不安を抱える企業ほど、サイバー保険の加入に適している。

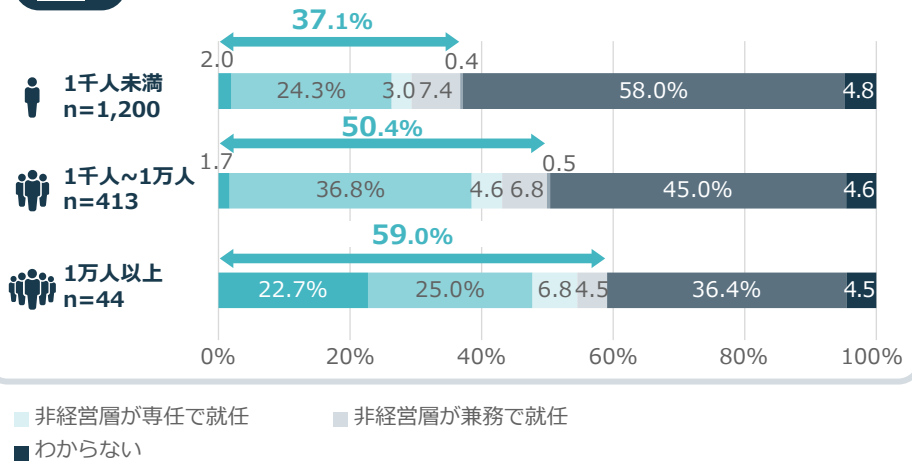
1 セキュリティの専門人材

日本のCISO設置割合は約4割であるが、従業員規模が多いほどに割合は増加傾向
未設置の企業はCISOをチームとして立上げ、時間をかけて整備する発想が望まれる

CISO（情報セキュリティを統括する人材）の設置状況



JP 従業員数別



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60%

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、資質と能力を網羅的に満たす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割に留まっている要因と考えられる。
- 未設置の企業は、CISOにスーパーマンを1人任命しようとするのではなく、 CISOをチームとして立ち上げ、時間をかけて整備・強化していく選択肢もある。そのためには、自社におけるセキュリティ業務の棚卸しを行い、役割とアサインを再定義することから始めたい。
- CISO設置企業においても、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。経営トップがCISOを支え、執行に必要な権限とリソースを与えることが不可欠である。

2

解説

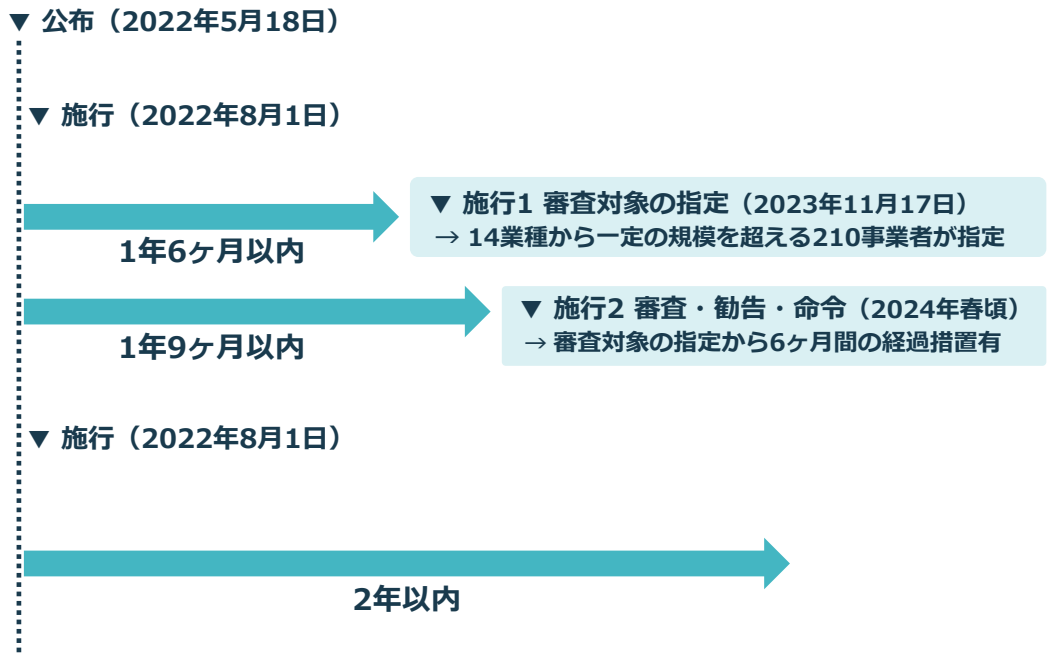
経済安全保障推進法と「第2の柱」が求める要請事項

サプライチェーン

2022年5月公布の「経済安全保障推進法」には4つの柱があり、第2の柱である「特定社会基盤役務の安定的な提供の確保」に際して、事前審査が必要となる

経済安全保障推進法における4つの柱

- **第1の柱** 重要物資の安定的な供給の確保に関する制度
- **第2の柱** 特定社会基盤役務の安定的な提供の確保に関する制度
- **第3の柱** 先端的な重要技術の開発支援に関する制度
- **第4の柱** 特許出願の非公開に関する制度



第2の柱の要請事項

Who だれが	特定社会基盤事業者は、
When どんな時に	特定社会基盤事業に関する役務の提供に際して、特定重要設備の導入及び重要維持管理等の委託を行う場合は、
What なにを	事業所管大臣が行う**事前審査**を受けなければならない

事前審査の位置づけと考慮要素

事業所管大臣が、導入等計画書に関する特定重要設備が特定妨害行為の手段として使用される恐れが大きいかどうかを審査することを指す。

- 供給者・維持管理委託先が、**外部にある主体から強い影響**をうけているか
- リスクに関する評価を自ら行い、結果に応じた**リスク管理措置**を講じているか
- 構成設備に脆弱性を指摘された例、**維持管理に対して不適切性が指摘**された例、供給者・維持管理委託先が、国際的な基準、国内の**法令の不遵守が指摘**された例
- その他、**同盟国・同志国の制裁リスト**に含まれていないか

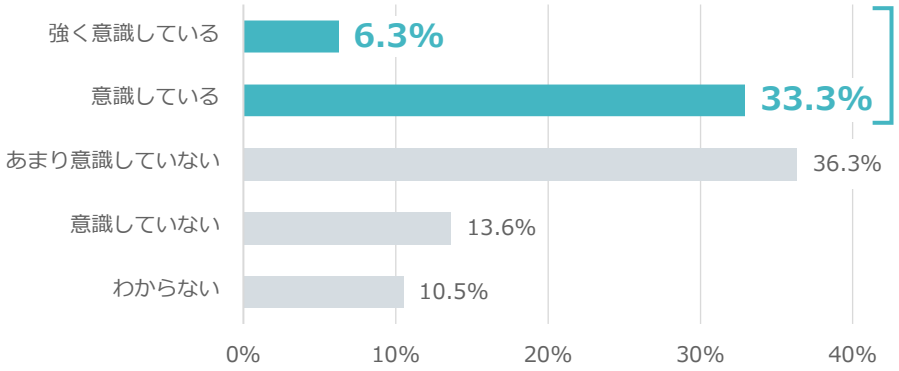
※内閣府『経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）』https://www.cao.go.jp/keizai_anzen_hosho/
を基にNRIセキュアが作成

2 経済安全保障推進法への意識

日本企業の約４割が経済安全保障推進法を意識している
特定社会基盤事業者ほど、経済安全保障推進法への関心が高い

経済安全保障推進法に関連して、サイバーを含むセキュリティの強化を意識している割合

JP n=1,657



強く意識している／意識していると回答した割合 ※1

全体 39.6%（n=1,657社）

特定社会基盤事業者 ※2	特定社会基盤事業者を除く
88.2%（n=17社）※3	39.0%（n=1,640社）

※1 日本企業に対するアンケートは、2023/8/1-2023/9/29 の期間で実施
※2 経済安全保障推進法に基づき特定社会基盤事業者の対象として指定された210の事業者
※3 サンプル数が少ないので参考値

Key Results

強く意識している／意識していると回答した割合

全体		特定社会基盤事業者
39.6%	＜	88.2%

Key Insights

- 経済安全保障推進法に関連したサイバーセキュリティ強化を「強く意識している／意識している」と回答した企業は、全体の39.6%であった。
- 一方、サンプル数が少ないので参考値ではあるが、国民生活や経済活動の基盤となるサービスを提供する特定社会基盤事業者に絞ると、88.2%の企業がセキュリティ強化を「強く意識している／意識している」と回答しており、経済安全保障推進法の対策が要請される事業者ほど、関心が高いことがうかがえる。
- 経済安全保障推進法の対象となった事業者は、2024年春以降に予定されている制度の運用開始に備えて、各省庁による具体的な制度内容の公表を継続的に注視する必要があるが、内容の公表と運用開始までの時間的な制約を考慮し、前広かつ計画的な準備が求められる。

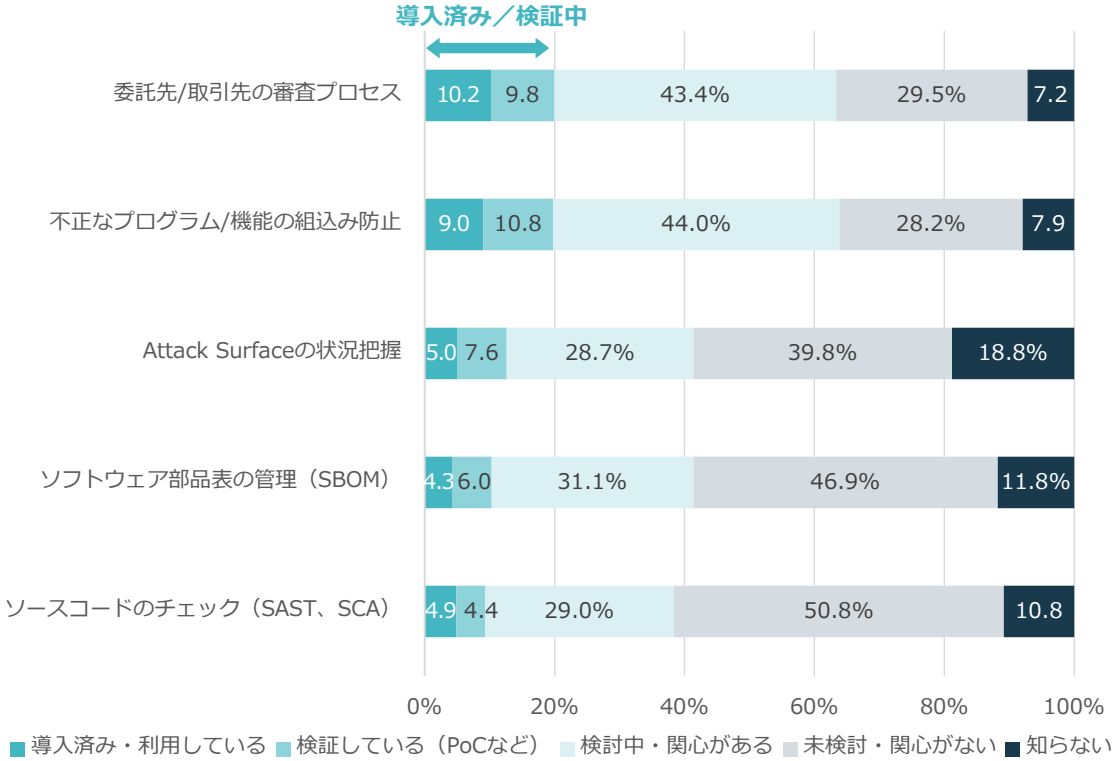
2 経済安全保障推進法を受けて強化した対策

経済安全保障推進法を受けた対策の1位は「委託先／取引先等の審査プロセス」「不正なプログラム／機能の組み込み防止」の想定対策にはバラつきがあると推察

経済安全保障推進法を受けて、強化ないし新規導入したサプライチェーンリスク対策

※ 経済安全保障推進法に関連して、セキュリティの強化を強く意識している／意識していると回答した企業のみ対象

JP n=655



セキュリティ用語解説：Attack Surface https://www.nri-secure.co.jp/glossary/attack-surface

Key Results

導入済み／検証中の対策No.1

約20% 委託先／取引先の審査プロセス

検討中の対策No.1

約45% 不正なプログラム／機能の組込み防止

Key Insights

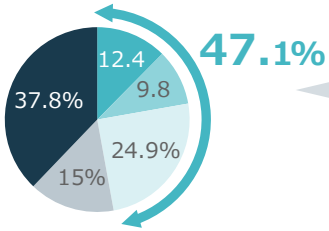
- 経済安全保障推進法を受けた対策の1位は「委託先／取引先等の審査プロセス」であった。2024年春以降に予定されている制度の本格施行に備えて、今後の法規制の動向や案内を引き続きウォッチする必要がある。
- 「不正なプログラム／機能の組込み防止」への回答は検討中が多いが、想定対策の内容にはバラつきがあると推察する。NRIセキュアとしての想定対策は、開発環境へのアクセス制御、開発用端末の外部デバイス接続遮断など、システム開発環境の整備と統制がある。
- 「Attack Surfaceの状況把握」を知らないと回答した割合が最も高い。委託先を通じた攻撃等に備え、自社に関わるサードパーティの構造を踏まえたAttack Surface（攻撃対象領域）の状況把握が求められる。

2 サプライチェーン統制状況

グループ会社数や従業員数が大きいほど、サプライチェーン統制が進んでいる
委託先への統制は、対象数の多さやつながりの複雑さなどの難しい課題が存在する

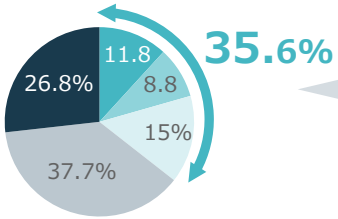
国内関係会社／グループ会社の統制状況

JP n=1,657

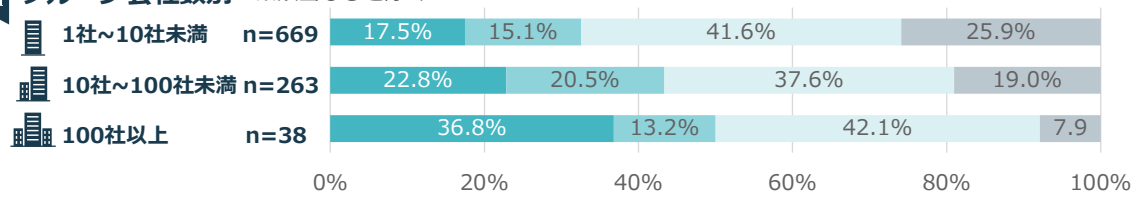


国内パートナー／委託先の統制状況

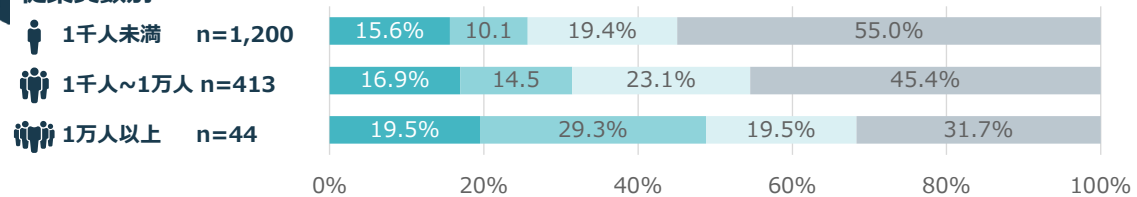
JP n=1,657



グループ会社数別 ※該当なしを除く



従業員数別 ※該当なしを除く



■ 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

Key Results

企業のセキュリティ統制状況

国内関係会社		国内委託先
47.1%	＞	35.6%

Key Insights

- グループ会社数や従業員数が大きい企業ほど、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、サプライチェーンリスクへの意識が高いことがうかがえる。
- 関係会社への統制が約47%であることに比べ、委託先への統制状況が約36%に留まっている。その背景として、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り、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あると考えられる。
- 関係会社・グループ会社は、親会社と同じセキュリティルールや対策の実践が求められる傾向があるのに比べ、委託先の対策状況は異なる。DX前提の時代、委託先とのITのつながりが常時かつ複雑になっていることから、委託先のセキュリティ対策状況を効率的に統制することが求められる。

セキュリティ用語解説：サプライチェーン攻撃 https://www.nri-secure.co.jp/glossary/supply-chain-attack

2 サプライチェーンにおけるセキュリティ課題

脅威の高まりや経済安保の流れで、サプライチェーン周辺の人材不足感は高まる
セキュリティ対応の初手は対象の把握だが、約3~4割の企業が課題と感じている

サプライチェーンに対するセキュリティ対応における課題

JP グループ会社数別

※ 複数選択可

	1社～10社未満 n=989	10社～100社未満 n=322	100社以上 n=50
1位	33.6% セキュリティ対応のリソースが自社向けで手一杯	42.9%	36.0% サプライチェーンの対象数（拠点や取引先）が多い
2位	27.8% **サプライチェーンとして管理すべき対象の全体像を把握できていない**	36.3%	34.0% セキュリティ対応のリソースが自社向けで手一杯
3位	27.6% 特になし	32.0% サプライチェーンの対象数（拠点や取引先）が多い	32.0% **サプライチェーンとして管理すべき対象の全体像を把握できていない**
4位	26.8% 何から手をつければよいか分からない	31.7% サプライチェーン管理向けのセキュリティ予算を確保できない（本社・自社向けの対策予算がメイン）	26.0%
5位	23.7% サプライチェーン管理向けのセキュリティ予算を確保できない（本社・自社向けの対策予算がメイン）	23.9% 何から手をつければよいか分からない	24.0% 特になし
6位	18.5% サプライチェーンの対象数（拠点や取引先）が多い	19.3% 特になし	20.0% アンケートでセキュリティ対策状況を確認しているが、実効性の観点で不安がある
7位	14.2% アンケートでセキュリティ対策状況を確認しているが、実効性の観点で不安がある	15.8%	18.0% 何から手をつければよいか分からない

※ 他選択肢：取引先や委託先からセキュリティ対応の理解・協力を得られない ／ アンケートでセキュリティ対策状況を確認しているが、確認内容を更新できていない ／ その他（具体的に記載）
※ グループ会社数が0社の企業を除く

Key Results

全体像を把握できていない割合

約30~40%

サプライチェーンとして管理すべき対象の全体像を把握できていない

大規模企業の課題No.1

36%

サプライチェーンの対象数（拠点や取引先）が多い

Key Insights

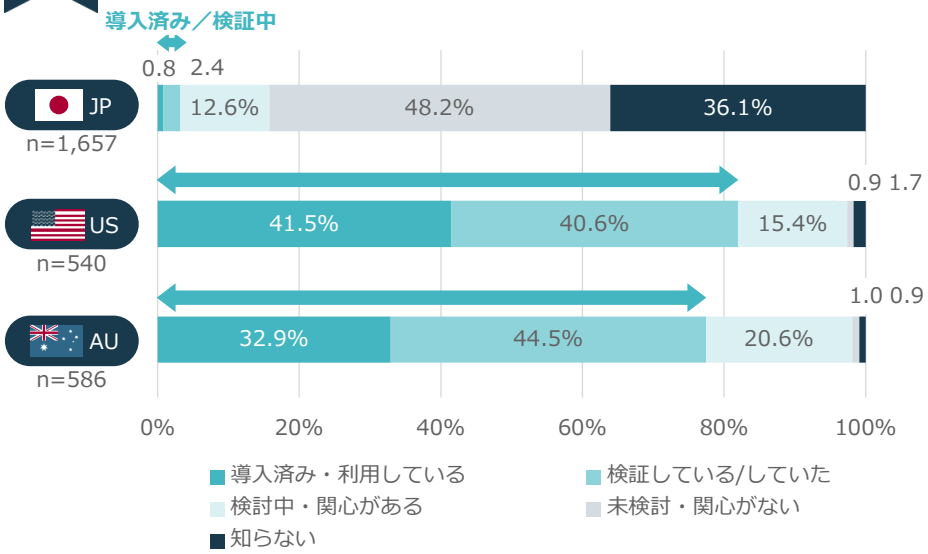
- サイバー脅威の高まりや経済安保の流れを受けて、サプライチェーンの重要性が増している一方、企業規模を問わず3~4割でサプライチェーンの全体像を把握できていない。委託関係の定期把握は統制の肝と言える。
- DXが進展し、クラウドやAPIの利活用も進んでいるため、大企業のサプライチェーン対象数は増加傾向にある。対象が多いという課題への効率的な対応策として、VRM（Vendor Risk Management）などが求められる。
- 中・小規模の企業は、サプライチェーンの管理体制を整備する必要性は感じているが、予算確保や人材不足などで対応が難しい状況と考えられる。

セキュリティ用語解説：VRM https://www.nri-secure.co.jp/glossary/vrm

2 SBOM（ソフトウェア部品表）の導入状況と解説

日本のSBOM導入率は低いが、経済安全保障推進法の具体策としての普及に期待

SBOMの導入状況



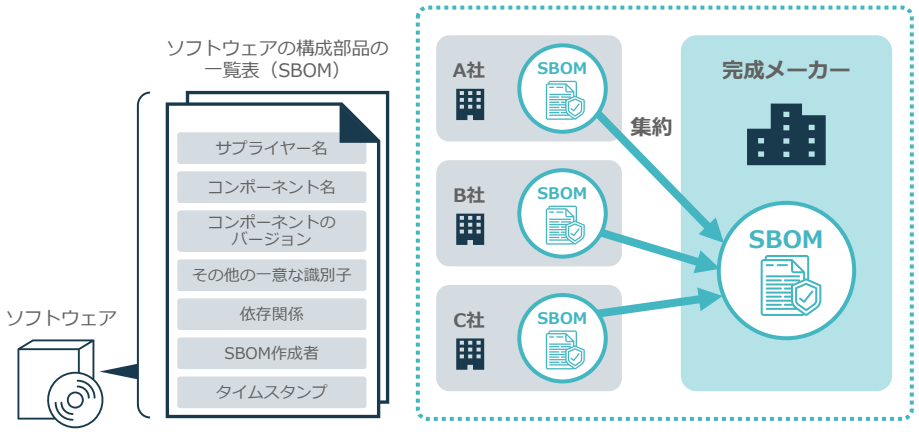
Key Results

SBOMを利用中／検証中と回答した企業の割合

JP **3.2%** → US **82.1%** AU **77.4%**

セキュリティ用語解説：SBOM https://www.nri-secure.co.jp/glossary/sbom

SBOM（Software Bill of Materials）



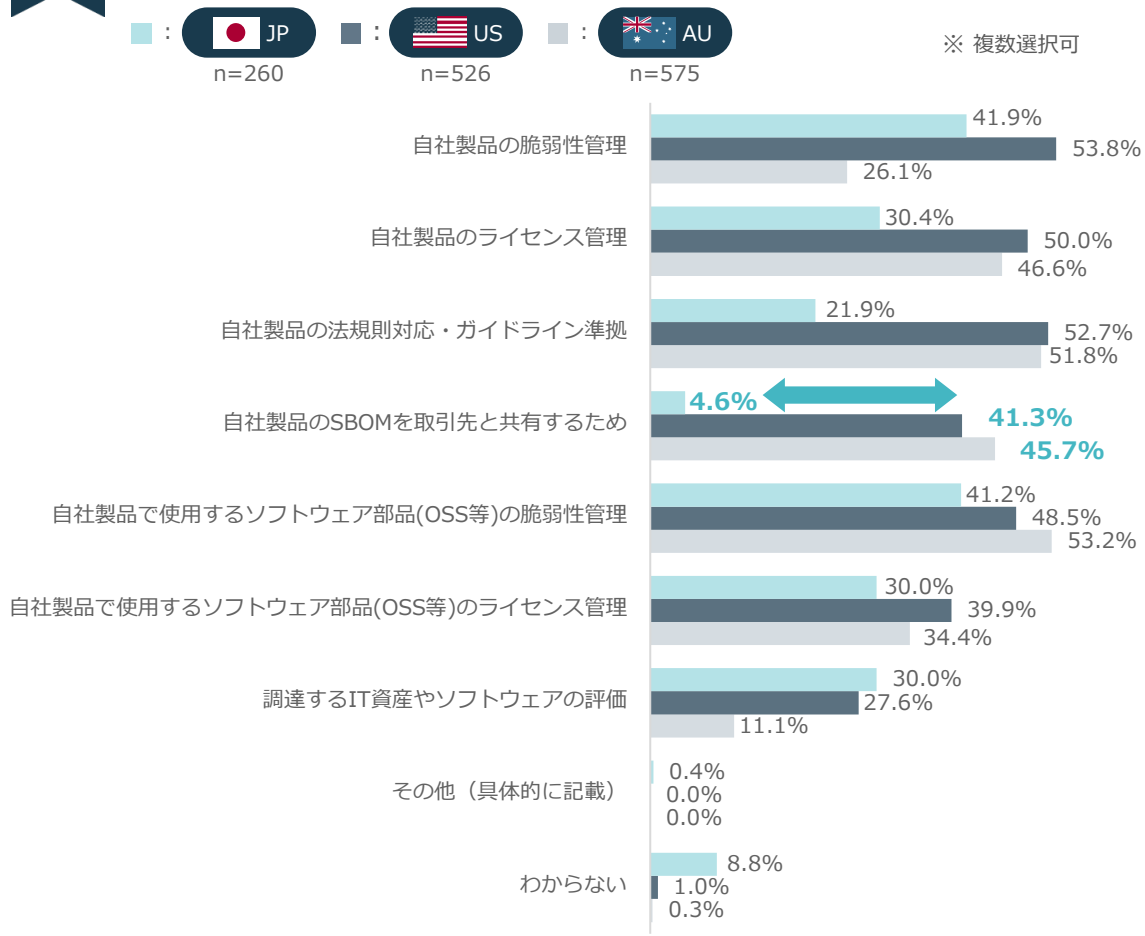
- SBOM（Software Bill of Materials、ソフトウェア部品表）は、ソフトウェアを構築するために使用される様々なコンポーネントの一覧表であり、OSS（Open Source Software）のライセンス管理や脆弱性管理、ソフトウェアサプライチェーンリスク管理等の用途で利用されている。
- 2021年5月に発出された米国大統領令（EO14028）において、政府調達におけるSBOM活用の検討指示が明記されたことをきっかけに、SBOMが急速に普及しつつある。
- 日本での導入は少ないが、2023年7月に、経産省より『ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引』が公開されるなど、企業によるSBOM活用を推進するための施策が行われており、今後の普及が期待される。

2 SBOM（ソフトウェア部品表）の導入／検討の目的

日本のSBOMの導入は、米・豪と比較してまだ進んでいない
米・豪と同様に、今後は取引先からSBOMを要求されることが増えると予想される

SBOM導入／検討の目的

※ SBOMを導入済み・検証している・検討中と回答した企業のみ対象



Key Results

日本と米豪の差 No.1

取引先とのSBOM共有

JP **4.6%** ⇔ US **41.3%** AU **45.7%**

Key Insights

- SBOMの導入が進んでいる米・豪において、導入の目的の約半数は取引先とのSBOMの共有となっている。すでに多数の企業がソフトウェアの調達要件においてSBOMを要求するようになっており、このトレンドは経済安保の流れを受けて、日本でも盛んになっていくことが考えられる。
- SBOMの導入を義務化する法規や、ガイドラインの対象となる製造業をはじめとする企業を中心に、日本でも取引先へSBOMを要求するようになっていくことが予想される。それに伴い、それらの企業のサプライヤにあたる企業においてもSBOMの導入／検討が今後進んでいくと思われる。

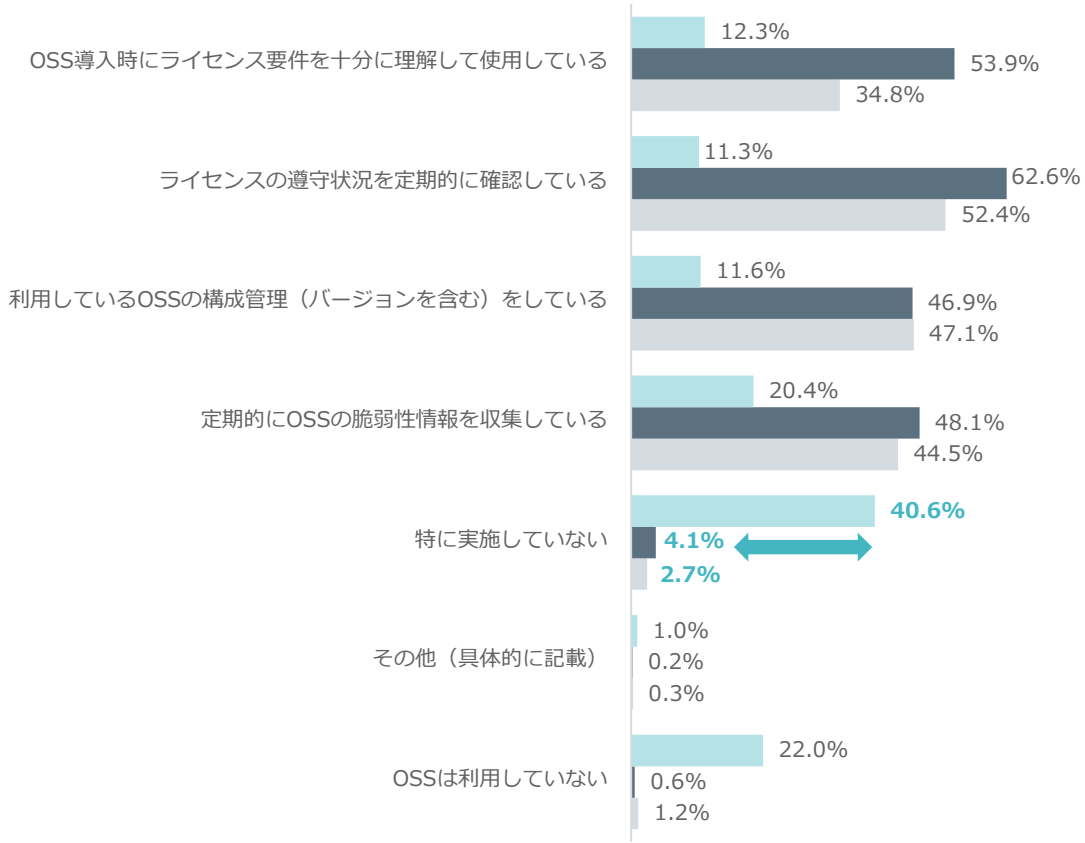
2 OSS（Open Source Software）のリスク対策

米・豪では約半数の企業がOSSの脆弱性やライセンスのリスク対策を実施
日本でもOSSの利活用が進むことを踏まえて、組織的なガバナンス強化が必要

自社で利用しているOSSのリスクに対して実施している対策

JP n=1,657　US n=540　AU n=586

※ 複数選択可



Key Results

日本企業のOSSのリスク対策の現状

JP **約40%** 特に実施していない

Key Insights

- 日本では「特に実施していない」の回答率が最も高いが、今日のソフトウェアに1つ以上の既知OSS脆弱性が含まれる割合は8割以上という調査結果※もあり、OSSのリスク対策は喫緊の課題であると言える。
- 米・豪では約半数の企業が脆弱性情報の収集やライセンスの遵守状況の確認といった対策を行っており、OSSのリスク対策を積極的に進めている状況が分かる。
- 今後より一層OSSの利活用が進む中で、リスク対策を含めた組織的なガバナンスの強化を進めていくことが望ましい。日本でもOSPO（オープンソースプログラムオフィス）を設置する企業も登場している。

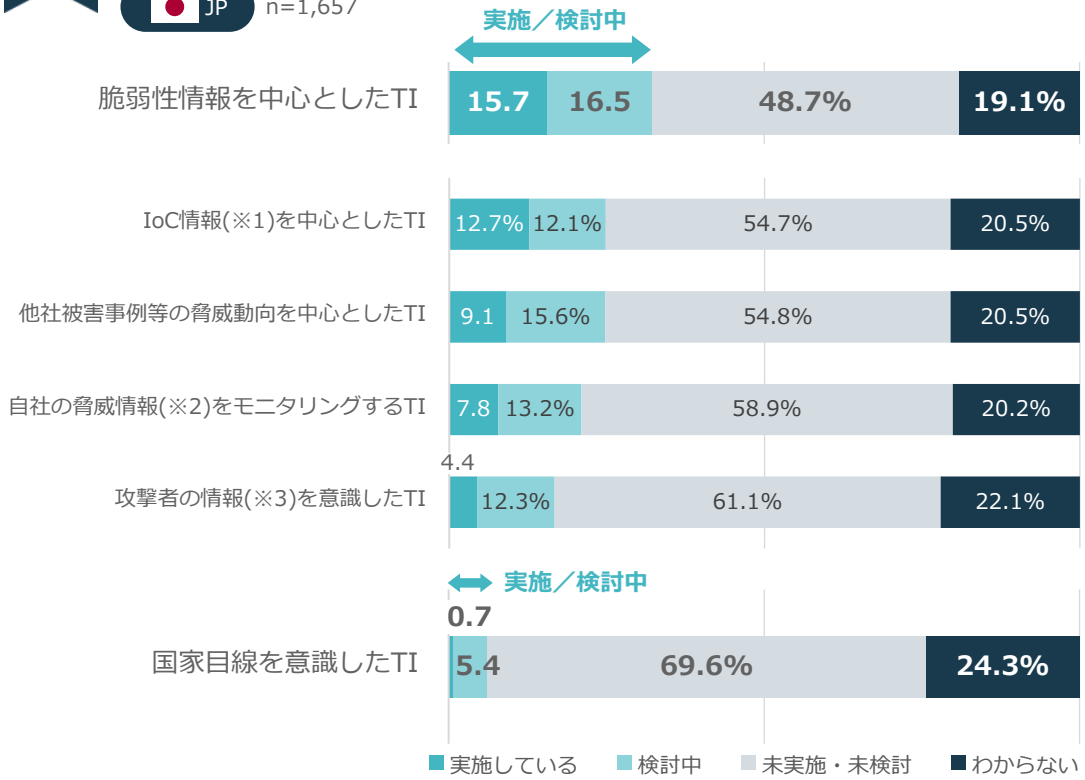
※ 出所　日本シノプシス合同会社 『2023年 オープンソース・セキュリティ＆リスク分析レポート』https://www.synopsys.com/ja-jp/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

3 脅威インテリジェンスの活用の実施・検討状況

日々のセキュリティ対策に活用しやすい脅威インテリジェンスの利用が進んでいる
未実施・未検討の企業は、TIに関する情報収集やPoC等でのTI活用の体験が必要

脅威インテリジェンス（TI: Threat Intelligence）の活用の実施・検討状況

JP n=1,657



※1 不正IPアドレス、悪性ドメイン等
※2 クレデンシャル漏洩、フィッシング関連、ダークウェブ上の自社情報調査等
※3 攻撃手法・動機・標的

NRIセキュアブログ https://www.nri-secure.co.jp/blog/effectiveness-of-threat-intelligence

Key Results

実施・検討率 No.1

脆弱性情報を中心としたTI **約32%**

最も低い実施・検討率

国家目線を意識したTI **約6%**

Key Insights

- 脆弱性情報、他社被害事例等のTIは話題になりやすく、TIとして活用イメージが浮かびやすいことから、実施・検討率が高いと考えられる。
- 「国家目線を意識したTI」の実施・検討率は低いが、この理由はTIで国家が関与するサイバー攻撃の兆候などを把握しても、それを自組織の対策イメージまで落とし込めないためと考えられる。これらの情報の重要性と有効性を理解するためには、TIに関する情報収集やPoC等を通じ実際にTIに触れることが重要である。
- セキュリティ対策の成熟度が高い企業では、IoC情報を中心としたTIを、SIEM（セキュリティ情報イベント管理）に連携するなど、TI情報をセキュリティの防御や検知に利用していることが予想される。

セキュリティ用語解説：SIEM https://www.nri-secure.co.jp/glossary/siem

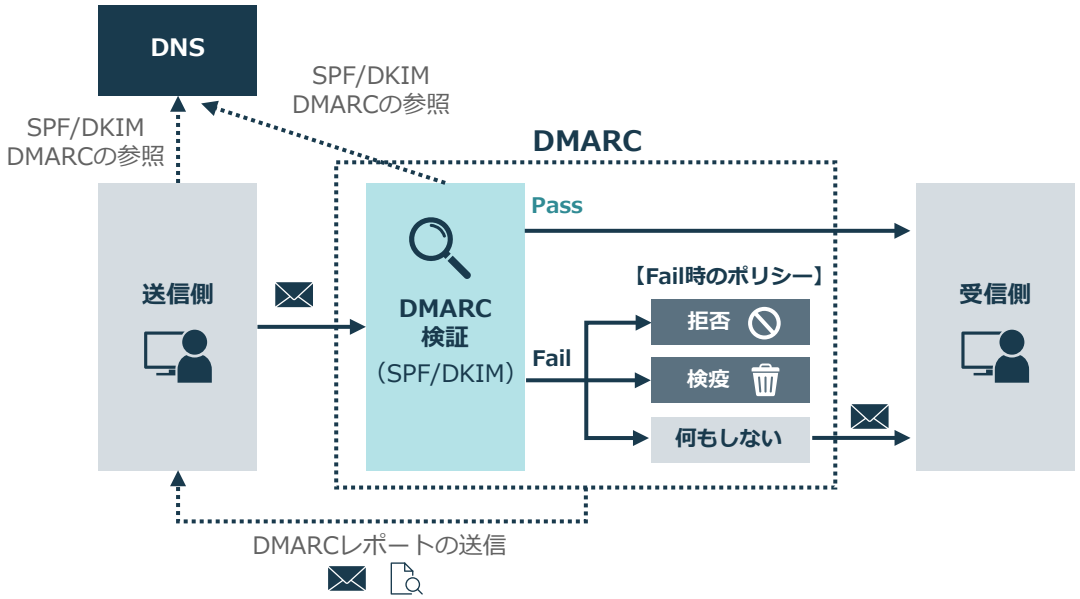
3

解説

DMARC

偽装メール対策であるDMARCは、政府のセキュリティ統一基準に明記されたことをきっかけに注目が高まっている

DMARC (Domain-based Message Authentication, Reporting and Conformance)



DMARCポリシー

Reject（拒否）
DMARC認証に失敗したメールを拒否するよう求めるポリシー

Quarantine（検疫）
DMARC認証に失敗したメールを疑わしいメールとして扱うよう求めるポリシー

None（何もしない）
DMARC認証に失敗したメールでも受け入れ、監視のみするポリシー

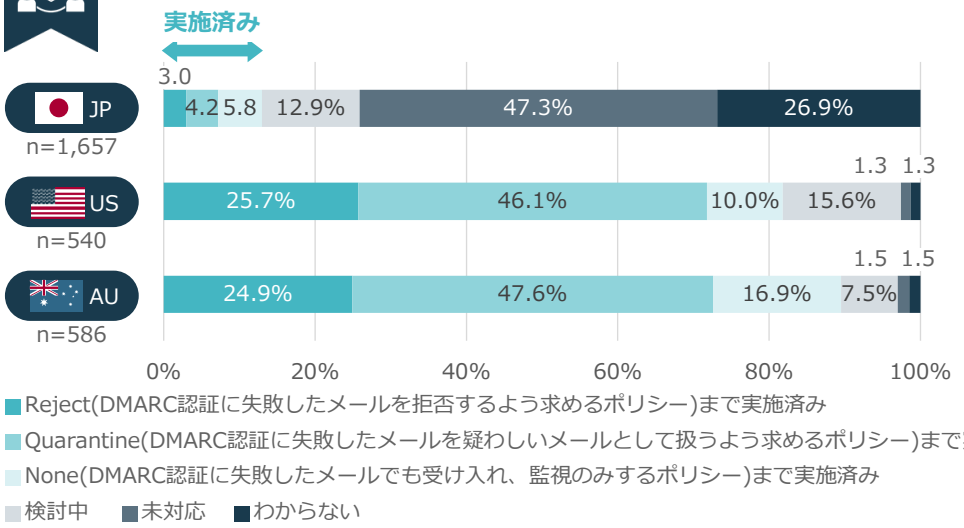
- DMARCとは、メールに表示された送信元（ヘッダーFrom）ドメインから正規に送信されたメールであるかどうかを認証する、送信ドメイン認証技術であり、自社ドメインを偽装したメールから受信者を保護する。
- ヘッダーFromのドメインによってSPFまたは DKIMの認証に成功した場合、DMARCの認証成功となる。DMARCでは認証に失敗した場合のメールの扱いを、送信ドメイン所有者側がReject（拒否） 、Quarantine（検疫）、 None（何もしない）のいずれかに指定することができる。また、送信ドメイン所有者側はDMARCの判定結果についての情報をレポートとして受け取り、可視化することができます。
- 2023年度に改定された政府のセキュリティ統一基準に、偽装メール対策としてDMARCが明記されたことを理由に注目が高まっており、今後、日本でも導入が進むと予想される。

セキュリティ用語解説：DMARC https://www.nri-secure.co.jp/glossary/dmarc　**NRIセキュア ブログ** https://www.nri-secure.co.jp/blog/how-to-dmarc

3 DMARC・BIMIの実施状況

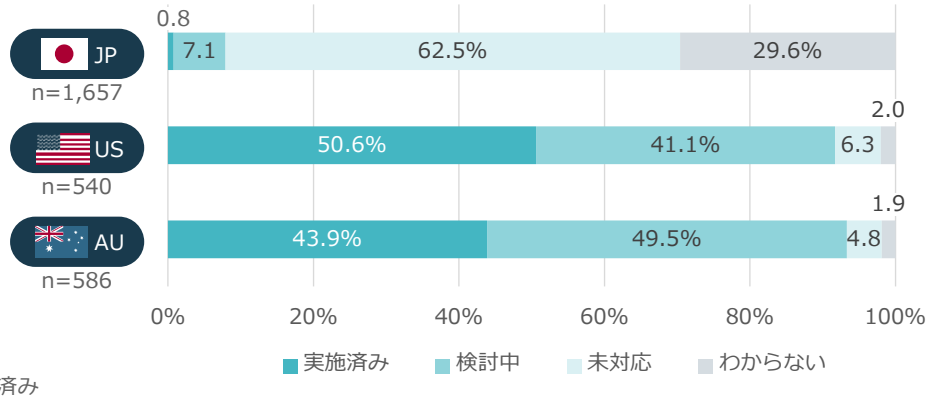
日本ではDMARCの実施が求められる機会が増加しており、今後の導入が進むと予想
DMARC対応の成熟には時間がかかるので、早期着手と中長期的な推進が望ましい

DMARCの実施・検討状況



BIMI※の実施・検討状況

※ Brand Indicators for Message Identification



セキュリティ用語解説：BIMI
https://www.nri-secure.co.jp/glossary/bimi

Key Results

未対応・わからない率

JP 約74%

DMARC 実施率の３カ国比較

JP 13%

US 約82%

AU 約90%

Key Insights

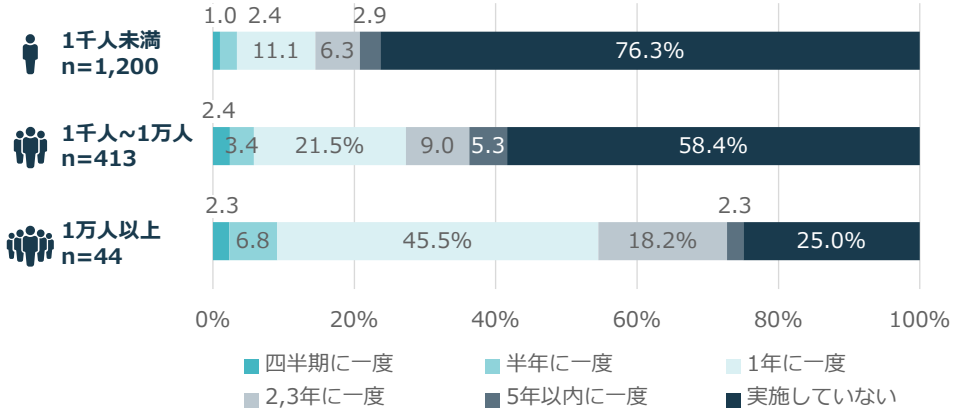
- 米豪のDMARC導入割合が高い理由は、国家機関でDMARC実施が義務付けられ、導入に関するガイドラインが公表されるなど、DMARC実施が推奨されていることが考えられる。
- 日本では、クレジットカード会社へのDMARC実施要請や令和5年政府統一基準へのDMARC実施明記など、DMARC実施が求められることが増えており、DMARCの導入が進むと考えられる。未対応の企業は、Noneポリシーでの導入は影響なく実施できるのでまずはそこから導入し、その上でQuarantine／Rejectに進んでいくことが望ましい。
- BIMI導入には、DMARCポリシーがQuarantine／Rejectである必要がある。前提条件が整っていないため、必然的に日本ではBIMI対応も進んでいない。

3 ペネトレーションテストの実施状況

大手企業ほどテストの実施頻度が高いのはセキュリティ投資効果の確認のためと推測
ペネトレーションテスト実施のきっかけは、自発的な動機が上位を占めている

ペネトレーションテストの実施頻度

JP 従業員数別



ペネトレーションテスト実施のきっかけ

JP n=489

※ ペネトレーションテストの実施頻度を四半期に一度／半年に一度／1年に一度／2,3年に一度／5年以内に一度と回答した企業のみ対象

※ 複数選択可

1位	64.8%	セキュリティレベル向上の一環
2位	29.9%	年次計画に基づく実施
3位	19.4%	自社のセキュリティインシデント
4位	10.6%	他社のセキュリティインシデント
5位	7.0%	その他（具体的に記載）
6位	3.7%	監督省庁の要請

Key Results

従業員数1万人以上の実施率

約75%

自発的な実施が大半

監督省庁の要請		セキュリティレベル向上の一環
約3.7%	＜	約64.8%

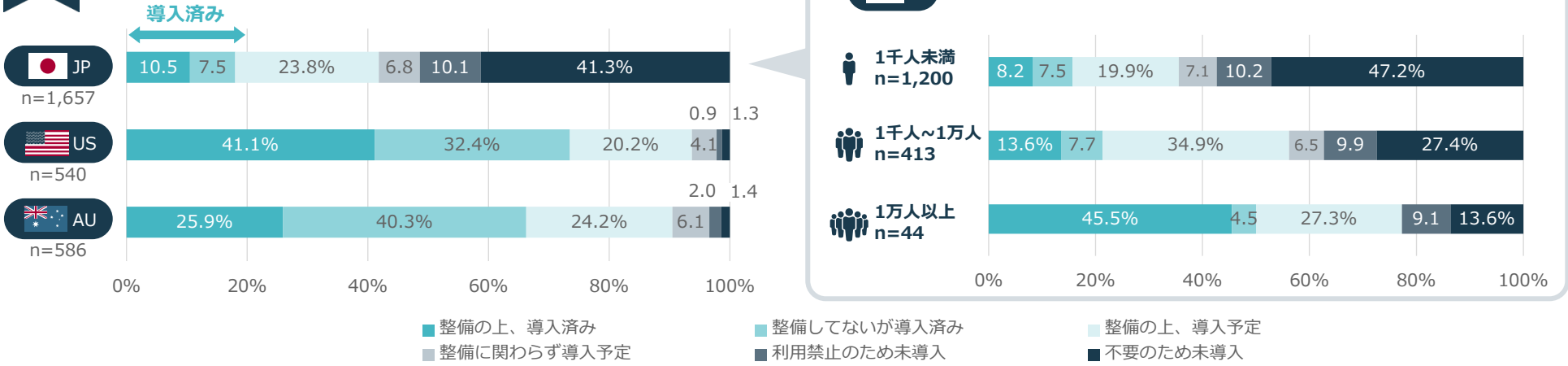
Key Insights

- 従業員別にみると、従業員数が多いほどペネトレーションテストの実施率は高い。一般に企業規模とセキュリティ投資額には相関があるため、現場の視点では対策有効性（抜け漏れ）の確認、経営の視点ではセキュリティ投資効果を確認していると推測される。
- 実施のきっかけについては自発的な動機（「セキュリティレベル向上の一環」「年次計画に基づく実施」）が多数を占めていた。現時点においては「監督省庁からの要請」を受ける対象が少なく、その他に複数含まれる「親会社からの指示」「顧客からの指示」のような外的要因もまだ少ないと推測される。

4 生成AIの導入状況

日本ではルールを整備した上で、生成AIを導入する方針の企業が多い
日本と米豪では、新しい技術の導入とルール整備に対する優先度の違いがうかがえる

生成AIのルール整備と導入状況



Key Results

生成AI導入率の差

JP **18%** ＜ US **約74%** AU **約66%**

不要のため未導入

JP **41.3%**

Key Insights

- 米豪では、ルールの整備に関わらず導入割合が高く、約7割である。一方、日本の従業員数1万人以上の企業では、50%が生成AIを導入しているが、そのほとんどがルールを整備の上導入しており、ルールを「整備の上、導入予定」と回答している。米豪との新しい技術の導入とそのルールの整備に対する、優先度の違いがうかがえる。
- 日本では従業員規模を問わず、「利用禁止のため未導入」と回答した企業が約10%あるが、今後、企業での導入実績が増加するにつれ、減少すると予想される。
- 日本の従業員数が千人未満の会社では、「不要のため未導入」という回答が半数近い。ユースケースを想定できない企業が多いと思われるが、試してみる姿勢が必要とも考えられる。

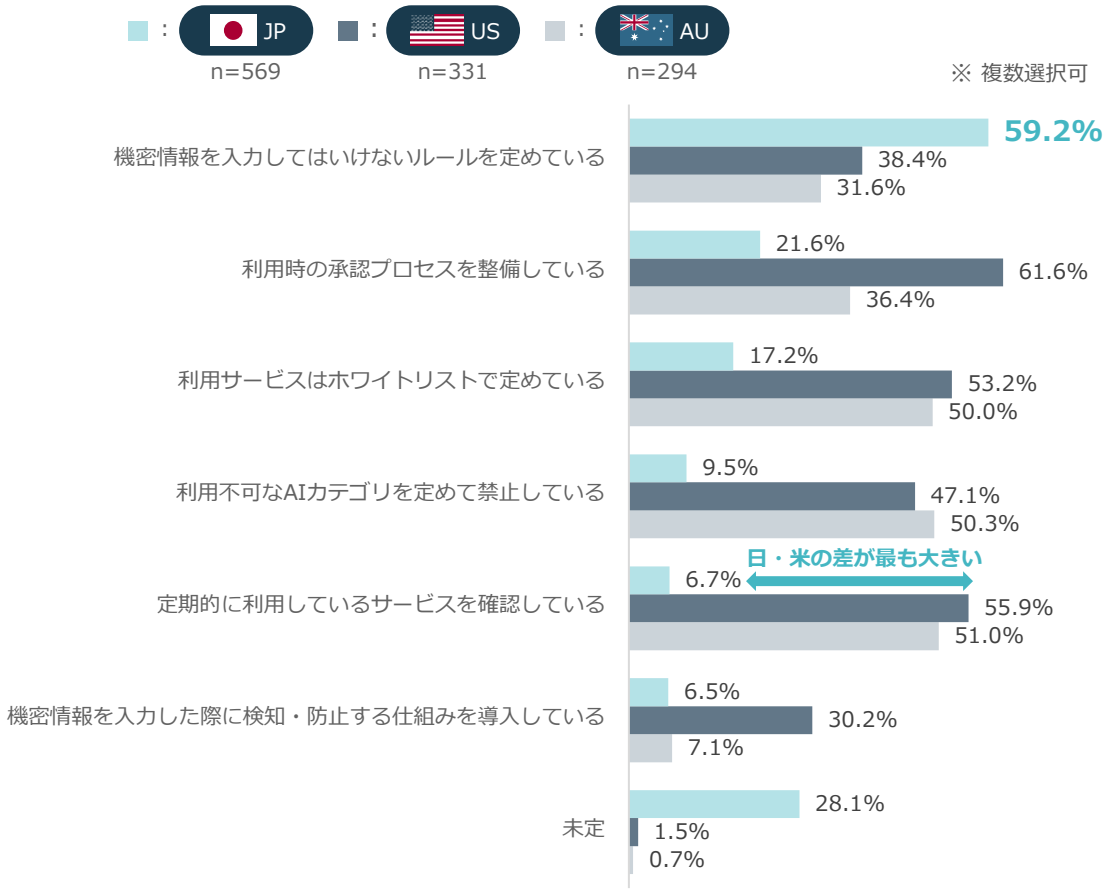
NRIセキュア ブログ https://www.nri-secure.co.jp/blog/generative-ai-security

4 生成AI利用に関するセキュリティルール

日本では、生成AI利用における機密情報入力に対する警戒が大きい
今後は、生成AIの利用状況の監視・分析を行うなどのシステム的な統制が必要

整備済み・整備予定の生成AIサービスの利用に関するセキュリティルール

※ セキュリティルールを整備・整備予定と回答した企業のみ対象



Key Results

日本が唯一、米豪を上回った回答

JP 約60% **機密情報**を入力してはいけないルール

日本と米国の差 No.1

定期的に利用しているサービスを確認している

JP → 8倍 US

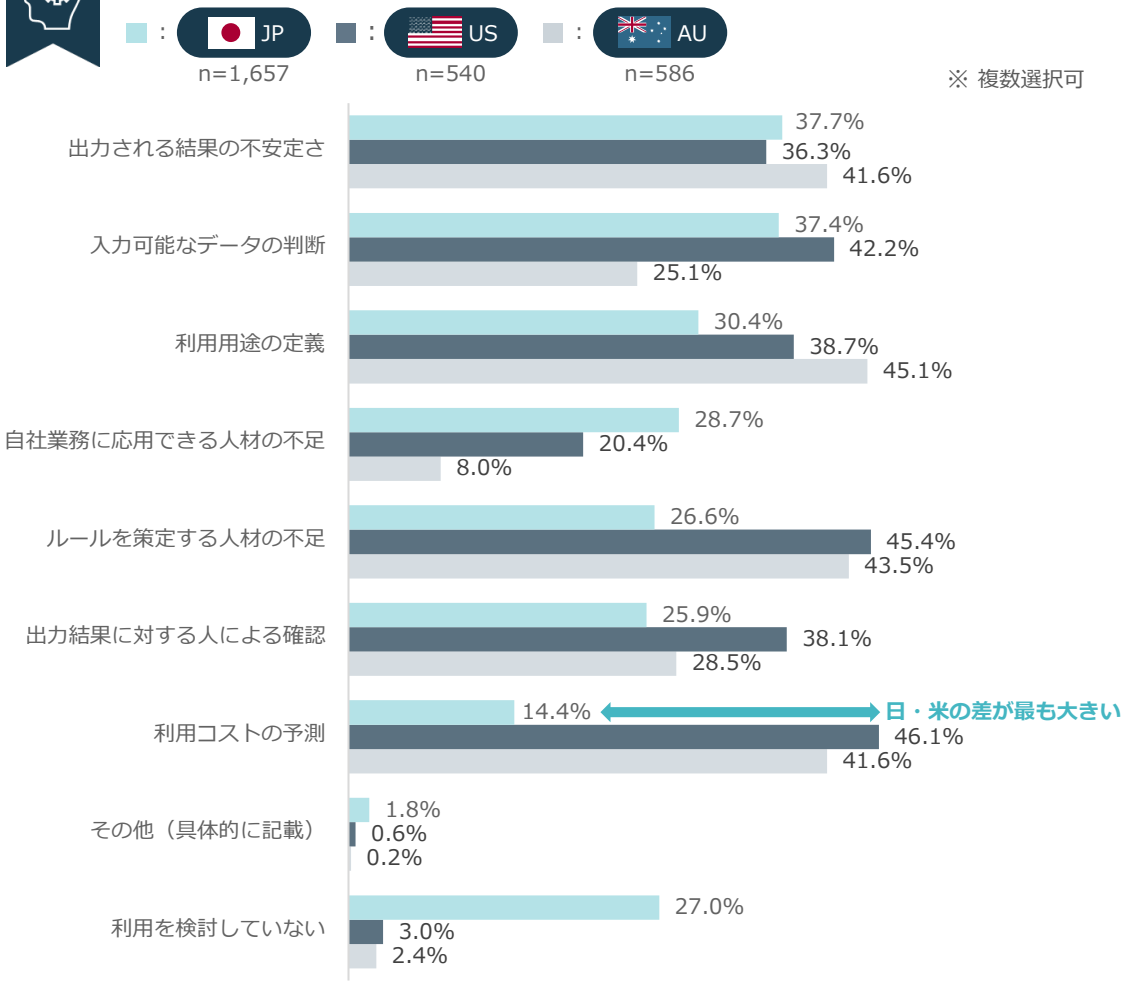
Key Insights

- 日本では「機密情報を入力してはいけないルールを定めている」と回答した企業の割合が米豪を上回り、日本企業の生成AIに対する慎重な姿勢が見られる。
- 一方、米豪では機密情報の入力検知や、CASBなどを用いた定期的な利用サービスの確認等、システム的に統制していこうとする姿勢がうかがえる。
- 様々な利用が普及すると予想されるAIサービスのセキュリティルールでは、従業員へのリテラシだけに頼るのではなく、利用状況の監視・分析を行うなどシステム的な統制が求められる。
- 日本では未定の回答が約3割であり、ルールを整備したいが具体的な策定にいたっていない企業が多い。

4 生成AI利用の課題

日本では、生成AIの導入に遅れがあるため「利用コストの予測」が後回しの状況
生成AI利用への慎重さが「自社業務に応用できる人材の不足」に拍車をかけている

生成AIサービスの利用を検討するにあたり、懸念や課題となること



Key Results

日本と米国の差　No.1

利用コストの予測

JP **14.4%** ⇔ US **約46%**　AU **約42%**

日本が米豪よりも課題と感じていること

自社業務に応用できる人材の不足

JP **28.7%** ＞ US **約20%**　AU **8%**

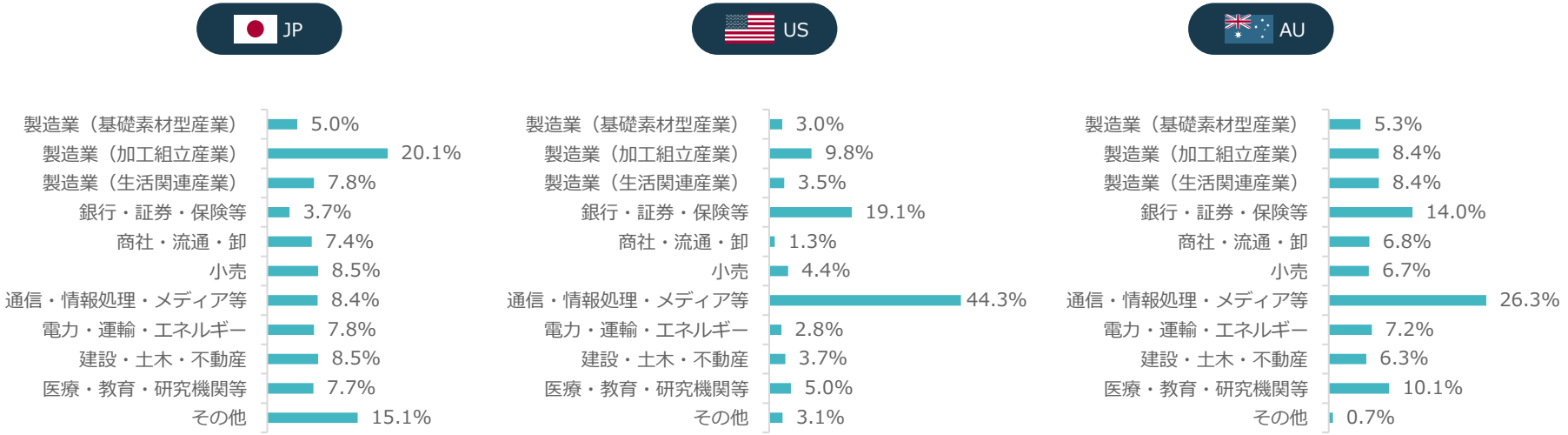
Key Insights

- 日本では「利用コストの予測」と回答した割合が、米豪に比べて大幅に低いが、これは懸念や課題とならない訳ではなく、まだそこまでの検討段階に至っていないだけと思われる。今後、日本での生成AI活用が進むにつれて、コストを意識する企業が増えていく。
- 米豪では、セキュリティ人材は充足している一方で、AI利用に関しては「ルールを策定する人材の不足」を懸念・課題と回答した企業が多く、AI人材の獲得競争のさらなる高まりが予想される。

回答者属性

回答企業数：合計2,783社（JP 1,657社、US 540社、AU 586社）

回答いただいた企業の業種



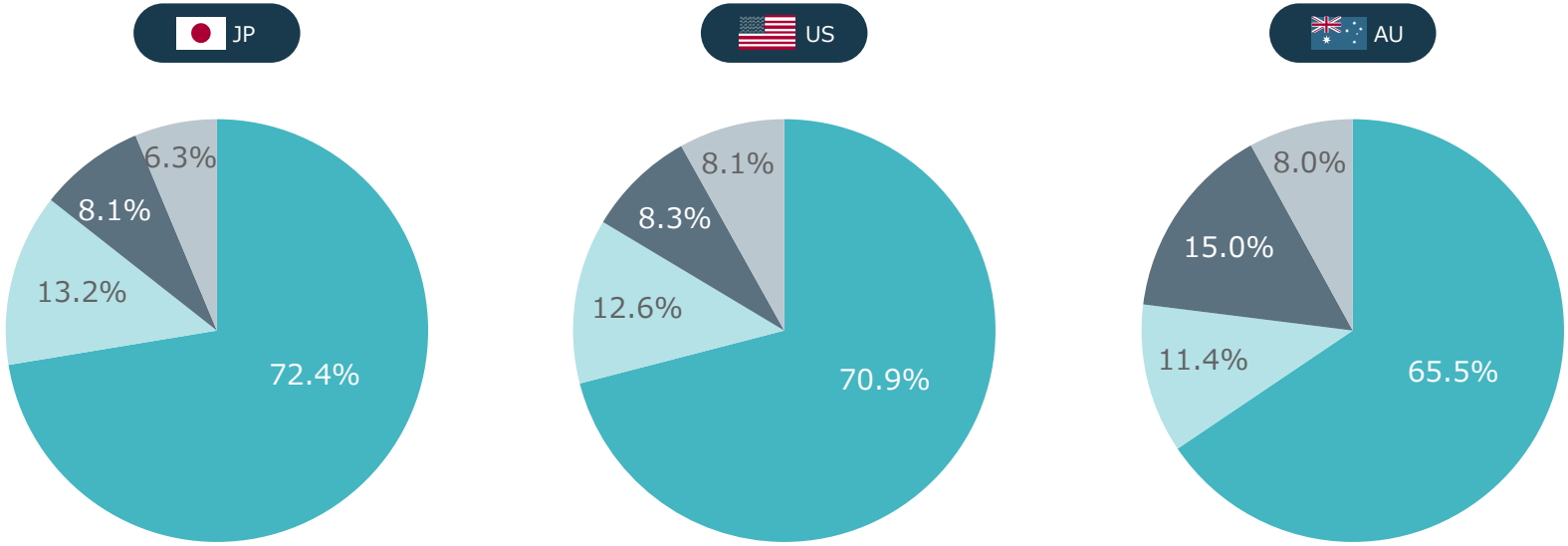
※ 回答企業の業種を以下のように分類

- 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2,783社（JP 1,657社、US 540社、AU 586社）

回答いただいた企業の従業員数・回答者の所属



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　：2023年8月1日～2023年9月29日 アメリカ、オーストラリア：2023年9月8日～2023年9月29日 注：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 2023　制作委員会
企画	松本 彩花
執筆	山田 真暉　　薮内 俊平　　中土井 洋平太
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　岡 博文　野口 大輔 藤井 秀之　大杉 周平　沖 真也　Deen De Silva 高梨 素良　奥村 哲平　稲垣 俊　市川 智史 遠藤 良二　大塚 淳平　半田 伸太郎　下山 洋一 斉藤 弘之　境 文也　藤井 貴弘　代田 晃基 延 優介　田中 悠一郎　松舘 拓也　大上 進也 渡部 惣　日下部 美弥子　大野 勝紀　西 はる菜
監修	足立 道拡　　川崎 聡太　　大高 ともり

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
サイバー セキュリティハブ大阪	〒530-0005 大阪府大阪市北区中之島3-2-4 中之島フェスティバルタワー・ウエスト
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：731名　単体：619名 ※2023年10月現在延べ人数

資格取得者数

110名 CISA
（公認情報システム監査人）

115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）

320名 GIAC
（Global Information Assurance Certification）

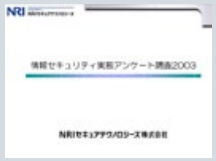
※ 2023年10月現在、延べ人数

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

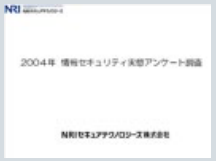
NRIセキュアテクノロジーズは情報セキュリティ実態調査を**21年**にわたり実施し、
のべ**23,780社から回答**を収集してきました。

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

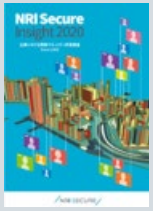
2015年：665社

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

2023年：2,783社
(内訳)
日本：1,657社
海外：1,126社

NRI Secure Insight 2023

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/insight2023-report

NRI SECURE

9213 0108 02 2312