



Nomura Research Institute Group

NEWS RELEASE

2022年12月13日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、日・米・豪の3か国で 「企業における情報セキュリティ実態調査 2022」を実施

～ CISO の設置が約4割にとどまる日本。新規セキュリティ予算は増加傾向 ～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、社長：柿木 彰、以下「NRI セキュア」）は、2022年7月から9月にかけて、日本、アメリカ、オーストラリア3か国の企業計2,877社を対象に、情報セキュリティに関する実態調査を実施しました。この調査は、2002年度から毎年実施しており、今回で20回目となります。

調査で明らかになったのは、おもに以下の3点です。

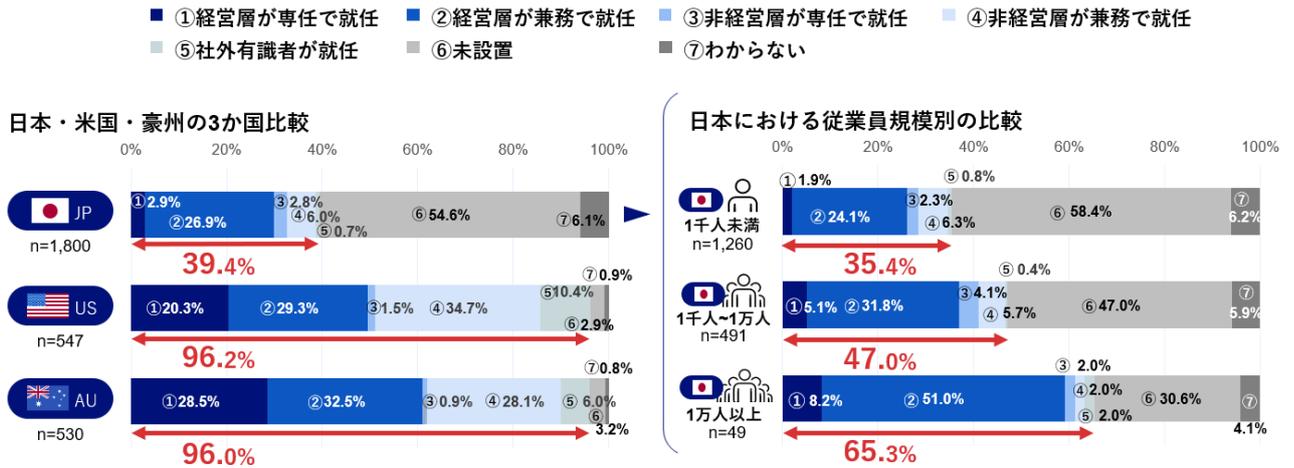
■ CISO の設置割合が約4割にとどまる日本企業（米・豪は9割以上）

サイバーセキュリティへの対策は企業が果たすべき社会的責任であり、経営者としての責務です。セキュリティ対策の整備が十分に進んでいる組織において、重要な役割を果たしているのが、経営とセキュリティ担当者をつなぎ、有効な対策の立案から実践に至るまでの責任を負う「CISO（最高情報セキュリティ責任者）」の存在です。

CISO を設置している企業の割合は、日本では全体の39.4%であり、アメリカの96.2%やオーストラリアの96.0%と比べて大幅に低い結果となりました。日本企業において従業員規模別に見ると、従業員が1万人以上の企業でも、CISO の設置割合は65.3%にとどまっています（図1）。

図 1：CISO（最高情報セキュリティ責任者）を設置している企業の割合
（国別および日本企業における従業員規模別）

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。 | CISO（最高情報セキュリティ責任者）



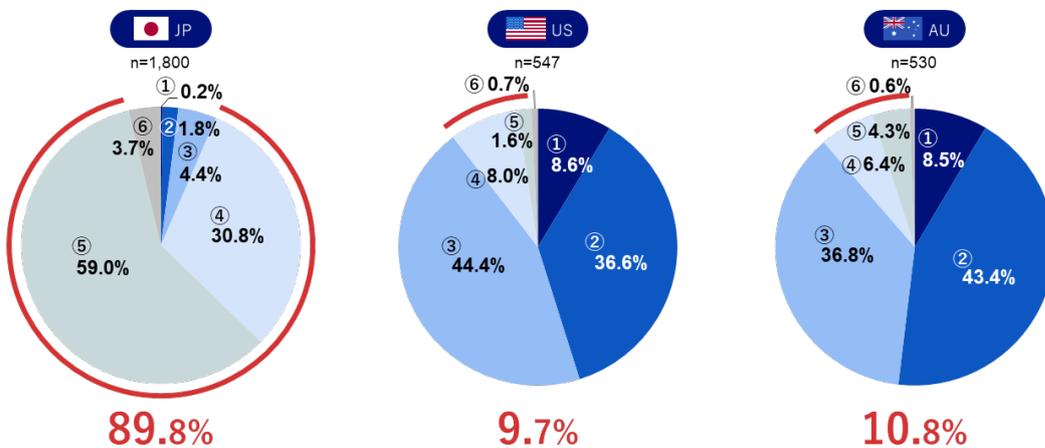
■ 日本企業の 9 割はセキュリティ人材が不足していると感じ、過去 10 年以上改善が見られない

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について、「どちらかといえば不足している」と「不足している」を合計した回答割合は、日本企業で 89.8%となり、前年度の 90.4%とほぼ同じでした（図 2）。同じ選択肢について集計したアメリカの 9.7%、オーストラリアの 10.8%と比較して、日本では圧倒的なセキュリティ人材不足の課題が浮き彫りとなっています。この状況は、例えば 2012 年度の調査においても 84.4%であったように、過去 10 年以上改善が見られていません。

図 2：セキュリティ人材の充足状況（国別）

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。

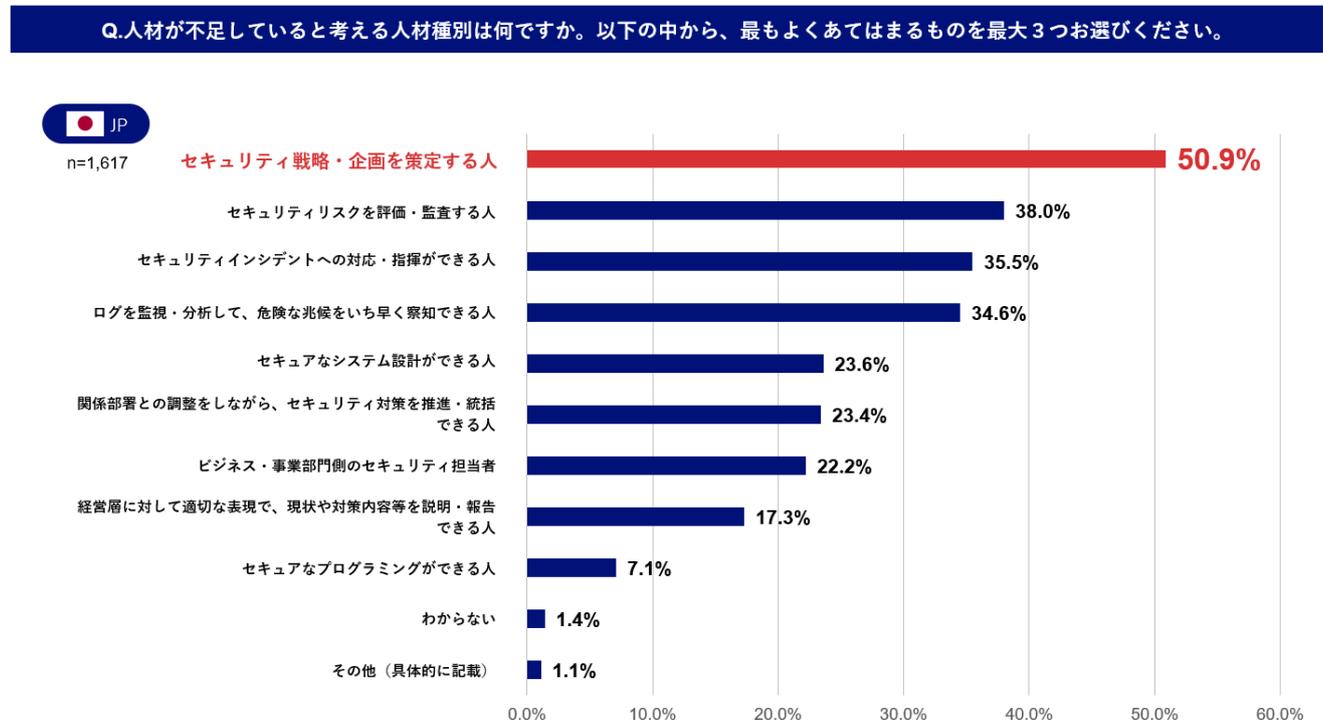
- Legend:
 ① 人材が過剰な状態 (1) ② 充足している（最適な状態） (2) ③ どちらかといえば充足している (3)
 ④ どちらかといえば不足している (4) ⑤ 不足している (5) ⑥ わからない (6)



セキュリティ人材が「不足している」と感じている企業の割合

セキュリティ人材が不足していると感じる日本企業に対して、不足している人材の種別を調査したところ、「セキュリティ戦略・企画を策定する人」が最も多く 50.9%、続いて「セキュリティリスクを評価・監査する人」が 38.0%となり、マネジメント層の不足が結果に表れています（図 3、3 つまでの複数回答）。

図 3：日本企業で不足しているセキュリティ人材の種別



これらの結果を踏まえると多くの日本企業においては、セキュリティ担当者が自社のセキュリティ戦略立案からリスク評価、インシデント（事件・事案）対応に至るまで、さまざまな業務をこなしている状況が推察できます。長年続く人材不足の問題を本質的に解決するためには、CISO を中心に経営層が一体となって人材と技術のバランスの取れたセキュリティ業務の推進体制を早急に整備すべきであると NRI セキュアは考えます。

具体的には、セキュリティ担当者が今実施している業務を棚卸し、今後のサイバー攻撃の動向や想定リスクを踏まえて、自社にとって適切なセキュリティ業務内容と人材のスキルを明確に定義する必要があります。業務内容に応じた育成支援やリスクリングなど、人材育成にこれまで以上の積極的な投資が伴うことも予想されます。また人手に依存しがちなセキュリティ設計や業務プロセスを抜本的に見直し、セキュリティ確保の観点から、業務の定型化や標準化、ツールやシステム等による自動化・効率化を同時に進めることが有効です。

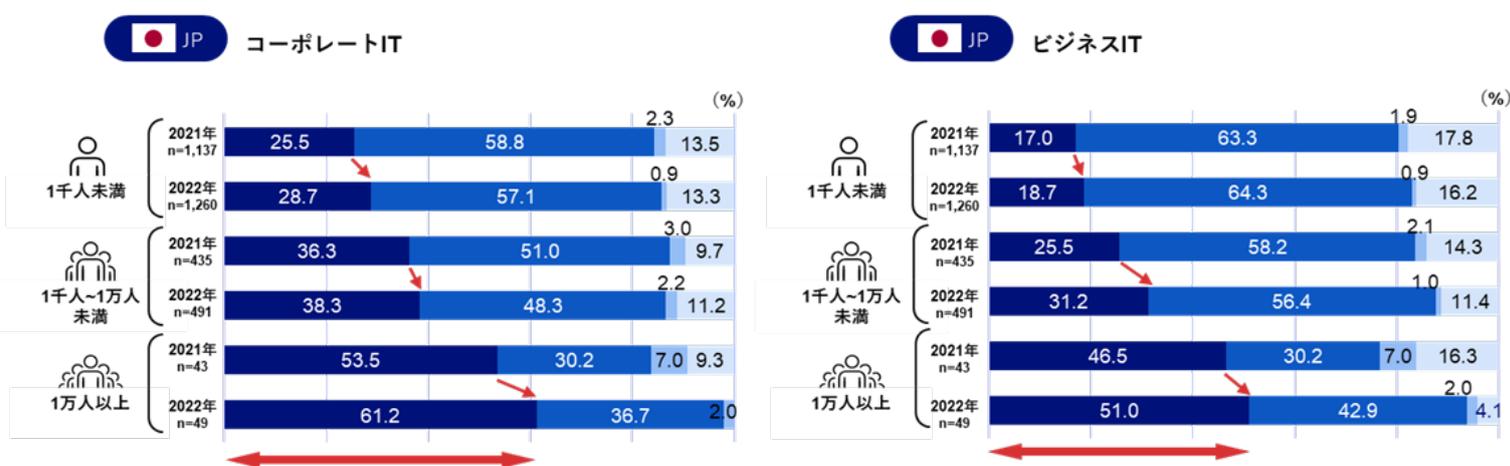
■ 新規セキュリティ対策への投資予算は、2021 年度よりも増加

日本企業が新規のセキュリティ対策に投資する予算について、前年度との変化を尋ねたところ、2021 年度の調査と比べて「増加した、または増加する見込み」と回答した割合が高い結果となりました。この傾向は、自社の情報システムのうち、コーポレート IT¹およびビジネス IT²のどちらの用途にも見られ、また従業員規模が大きい企業ほど、「増加」とする回答の割合が高くなっています（図 4）。

図 4：日本企業における新規セキュリティ対策の予算の変化（情報システムの用途別、従業員規模別に前年度調査結果と対比）

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？

■ ①増額した、または増額する見込み ■ ②変化はない ■ ③減額した、または減額する見込み ■ ④不明



新規セキュリティ対策の予算が増加した企業の割合

2022 年の日本では、ウィズコロナの状況下で円安が進み、世界的に物価の高騰や景気後退が発生するリスクへの関心が高まりました。その中で、新規セキュリティ対策への投資予算が前年度と比べて増加傾向にある理由としては、2022 年 2 月以降の国際情勢を踏まえたサイバー攻撃による脅威の高まりや、頻発するセキュリティ事故、DX（デジタル・トランスフォーメーション）推進や IT 利活用に伴うアタックサーフェス（攻撃対象領域）拡大への対策が迫られたことが挙げられます。

「企業における情報セキュリティ実態調査 2022」の詳細は、「NRI Secure Insight 2022」として、2023 年 1 月をめどに、NRI セキュアのホームページにて公開する予定です³。NRI セキュアは調査結果を踏まえて、今後も企業・組織の情報セキュリティ対策を支援し、安全・安心な情報システム環境と社会の実現に貢献していきます。

¹ 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情報システム（基幹業務、経理、人事システム等）

² 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情報システム（オンラインショッピングサイトやスマホアプリ等）

3 公開時期は予告なく変更する可能性があります。

【ニュースリリースに関するお問い合わせ】

NRI セキュアテクノロジーズ株式会社 広報担当

TEL : 03-6706-0622 E-mail : info@nri-secure.co.jp

【ご参考】

■ 調査概要

調査名	「企業における情報セキュリティ実態調査 2022」
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とともに、企業の情報システムおよび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。
調査時期	日本：2022年7月20日～9月25日 アメリカ、オーストラリア：2022年8月15日～8月24日
調査方法	Webによるアンケート
回答企業数と従業員規模別の内訳	日本：1,800社（千人未満：70.0%、千人～1万人未満：27.3%、1万人以上：2.7%） アメリカ：547社（千人未満：29.3%、千人～1万人未満：60.3%、1万人以上：10.4%） オーストラリア：530社（千人未満：25.3%、千人～1万人未満：69.4%、1万人以上：5.3%）

※本文中に掲載した単一回答のパーセンテージについては、小数点以下の値の切り上げ・切り捨てにより、各選択肢の回答割合の合計値が100%にならない場合があります。