



Nomura Research Institute Group

## NEWS RELEASE

2024年1月25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 2023」を実施

～ 生成 AI サービスの導入率で、米・豪の約7割に対し日本は約2割 ～

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：建脇 俊一、以下「NRI セキュア」）は、2023年8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2,783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年度から実施しており、今回で21回目となります。

おもな調査結果は次のとおりです。

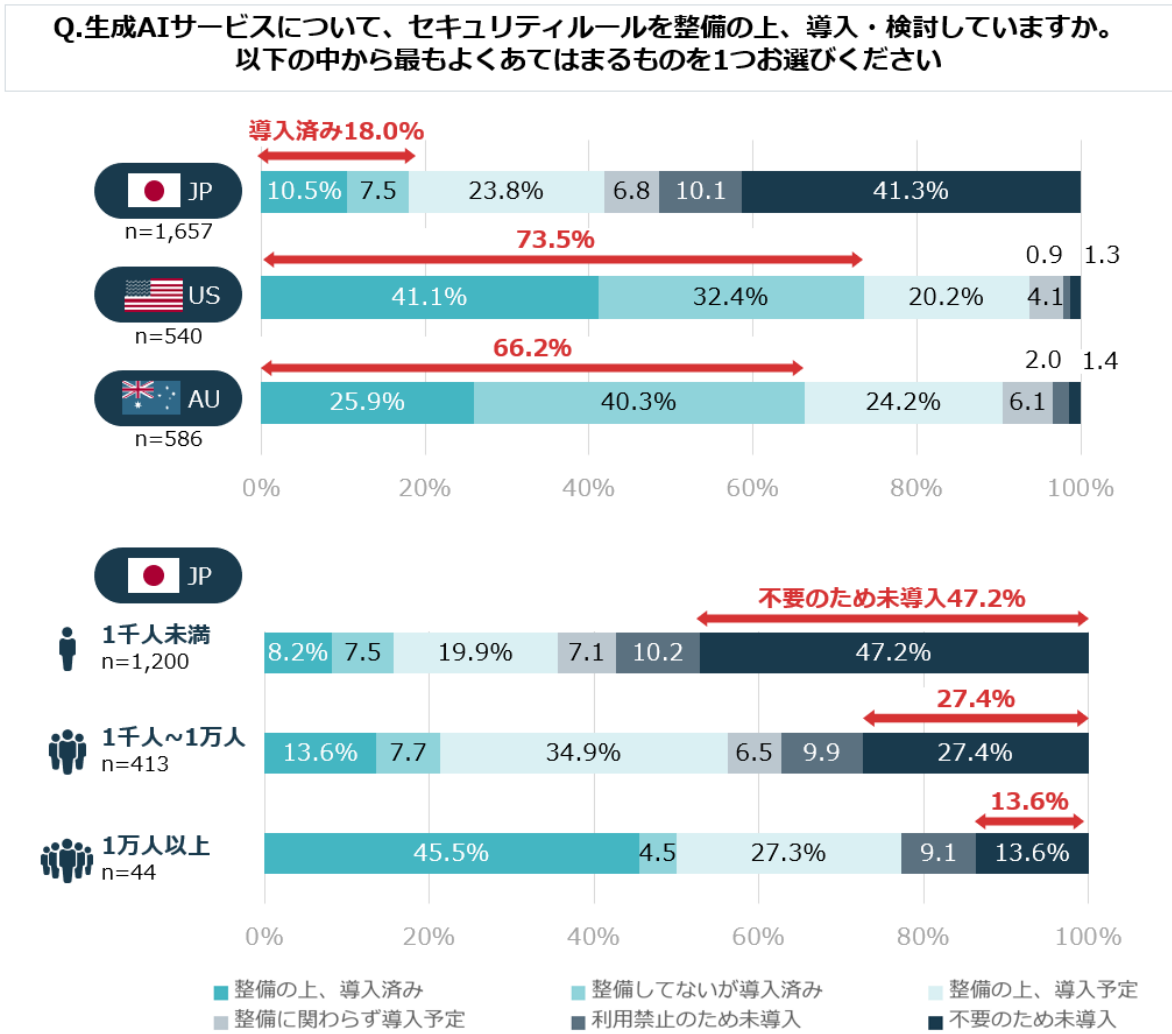
## ■ 生成 AI サービスの導入率が約2割にとどまる日本企業

### 1. 導入状況

生成 AI サービスの導入状況について、セキュリティルールを「整備の上、導入済み」または「整備していないが導入済み」と回答した割合は、日本では合計18.0%でした（従業員1万人以上の日本企業では50%）。同じ選択肢で比較した結果、アメリカは73.5%、オーストラリアは66.2%と、いずれも日本と比べ生成 AI サービスの導入率が高いことがわかります（図1）。

また、日本においては、従業員規模を問わずおよそ1割の企業が「利用禁止のため未導入」と回答していますが、アメリカ0.9%、オーストラリア2.0%と比べ割合が高く、生成 AI サービスの導入に対する日本企業の慎重な姿勢がうかがえます。さらに、従業員数が1千人未満の企業では、「不要のため未導入」という回答が半数近くを占めており、生成 AI サービスの必要性を感じていない日本企業が多く存在する傾向が見受けられます。

図 1：生成 AI サービスのルール整備と導入の状況（国別および日本企業における従業員規模別）

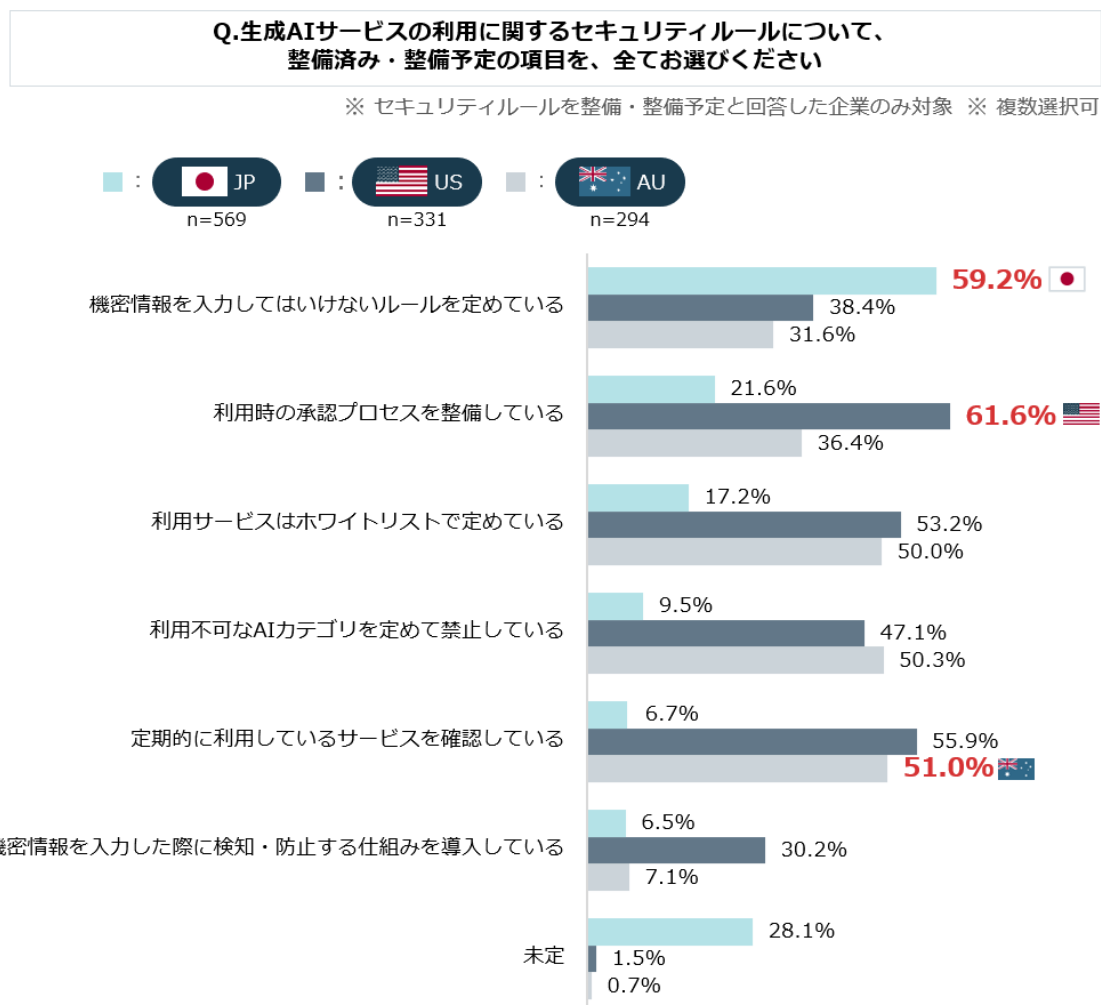


## 2. 生成 AI サービスの利用に関するセキュリティルール

生成 AI サービスの利用に関するセキュリティルールを「整備の上、導入済み」「整備の上、導入予定」と回答した企業に対して、どのようなルールを整備または整備予定かについて複数回答で尋ねたところ、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」という回答の割合が 59.2%と最も多く、アメリカの 38.4%、オーストラリアの 31.6%を上回りました（図 2）。

一方、アメリカでは「利用時の承認プロセスを整備している」（61.6%）、オーストラリアでは「定期的に利用しているサービスを確認している」（51.0%）がそれぞれ最も多くなりました。今後普及が見込まれる生成 AI サービスの利用においては、ユーザの判断に頼ったルールを整備するだけでなく、監視・統制システムなどの仕組みを用いて利用環境を整えることも重要です。

図 2：生成 AI サービスの利用に関する整備済み・整備予定のセキュリティルール（国別）



### ■ 偽装メール対策「DMARC」の実施率は日本の約 1 割に対し米・豪では 8 割台

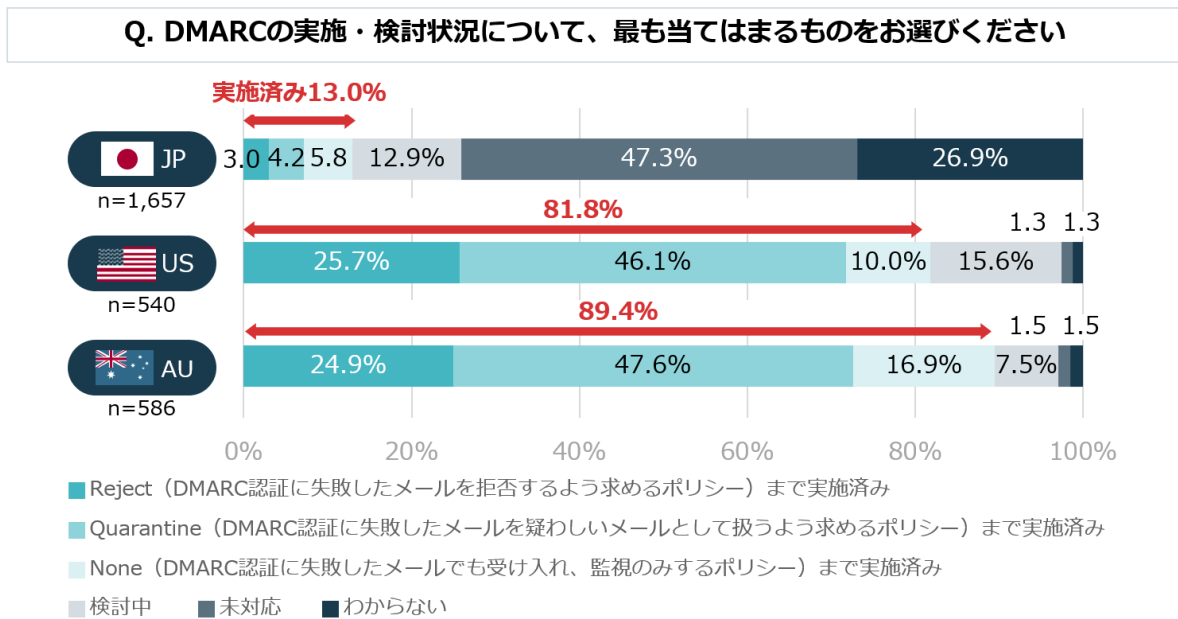
DMARC (Domain-based Message Authentication, Reporting and Conformance) とは、電子メールの送信元ドメインをもとに、正規に送信されたメールであるかどうかを認証する技術のことで、自社ドメインを偽装した悪意のあるメールから受信者を保護することを目的として、全世界で採用が進んでいます。

今回の調査では、DMARC 実施段階を、「Reject (拒否) / Quarantine (検疫) / None (何もしない)」の 3 つに分類した上で、「DMARC の実施・検討状況」について尋ねました。その結果、いずれかの形で DMARC を「実施済み」と回答した企業は、日本 13.0%、アメリカ 81.8%、オーストラリア 89.4%で、日本企業の DMARC 実施度合いが大幅に低い状況にあります (図 3)。

企業の DMARC 実施割合が高い米・豪においては、政府主導で DMARC の実施が推進されています。日本でも、2023 年 2 月に経済産業省、警察庁および総務省がクレジットカード会社に対して、DMARC 実施を要請<sup>1</sup>したほか、同年 7 月には「政府機関等のサイバーセキュリティ対策のための統一基準群」<sup>2</sup>において、偽装メール対策として DMARC が明記されました。さらに、2023 年 11 月に Google から発表された

「メール送信者のガイドライン」では、メール送信を行う事業者に対して DMARC 対応を求めるなど、今後日本でも DMARC 実施が進むとみられます。

図 3：DMARC の実施・検討状況（国別）

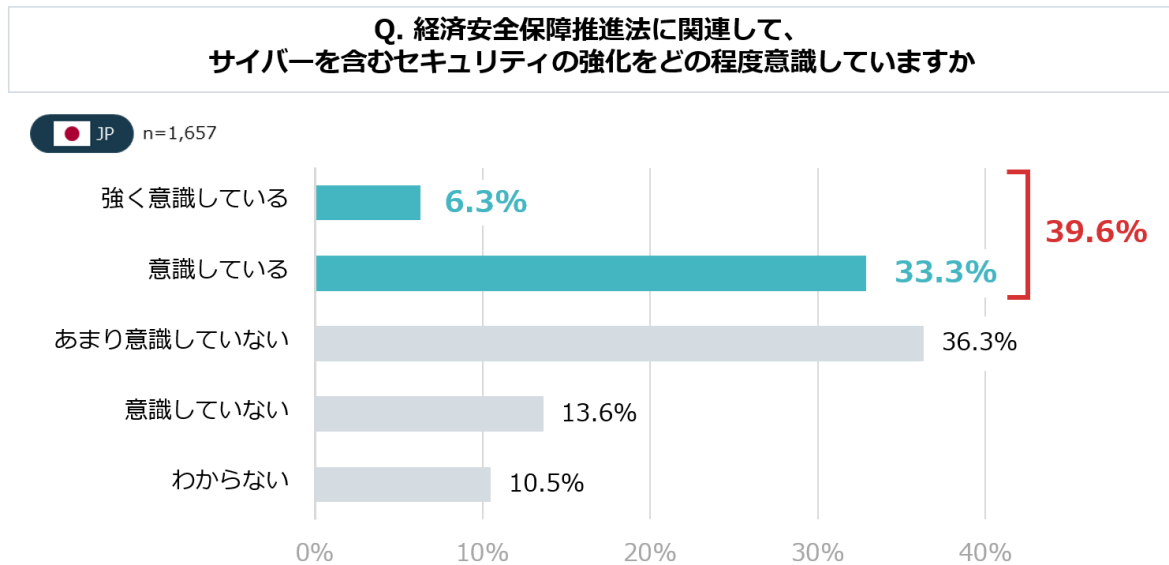


### ■ 特定社会基盤事業者に限らず、日本企業の約4割が経済安全保障推進法をうけてセキュリティ強化を意識

2022年にわが国で成立した経済安全保障推進法<sup>3</sup>に関連して、サイバー分野を含むセキュリティの強化を意識しているかどうかを日本企業に尋ねたところ、「強く意識している」「意識している」と回答した割合は、全体の39.6%となりました（図4）。

そのうち、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」に指定された企業に絞ると、88.2%の企業（17社中15社）がセキュリティ強化を「強く意識している」「意識している」と答えました。全体の傾向と比べると、特定社会基盤事業者は経済安全保障推進法に関連してセキュリティ強化をより意識しています。

図 4：経済安全保障推進法に関連して、サイバー分野を含むセキュリティの強化を意識している日本企業の割合



「企業における情報セキュリティ実態調査 2023」の詳細なレポートは、次の Web サイトから入手いただけます。

<https://www.nri-secure.co.jp/download/insight2023-report>

今回の調査で、生成 AI のセキュリティ、DMARC などの領域において米・豪と比べた際に、日本企業の取り組みの遅れが浮き彫りになりました。NRI セキュアは、今回の調査結果を踏まえ、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 経済産業省、警察庁及び総務省は、クレジットカード番号等の不正利用の原因となるフィッシング被害が増加していることに鑑み、クレジットカード会社等に対し、送信ドメイン認証技術（DMARC）の導入をはじめとするフィッシング対策の強化を要請しました（出所：経済産業省「クレジットカード会社等に対するフィッシング対策の強化を要請しました」2023年2月1日）。
- 2 政府機関等のサイバーセキュリティ対策のための統一基準群：サイバーセキュリティ基本法に基づき内閣に設置されるサイバーセキュリティ戦略本部は、令和5年7月4日に「政府機関等のサイバーセキュリティ対策のための統一基準群」の令和5年度版を公開しました。
- 3 経済安全保障推進法：国際情勢の複雑化、社会経済構造の変化等に伴い、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基本方針を策定するとともに、安全保障の確保に関する経済施策として、(1) 重要物資の安定的な供給の確保、(2) 基幹インフラ役務の安定的な提供の確保、(3) 先端的重要技術の開発支援、(4) 特許出願の非公開に関する4つの制度を創設することを目的として、2022年5月に成立した法律です。

**【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 2023」
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	<ul style="list-style-type: none"><li>日本：2023年8月1日～2023年9月29日</li><li>アメリカ、オーストラリア：2023年9月8日～2023年9月29日</li></ul>
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	<ul style="list-style-type: none"><li>日本：1,657社 (千人未満：72.4%、千人～5千人未満：21.3%、5千人以上：6.3%)</li><li>アメリカ：540社 (千人未満：70.9%、千人～5千人未満：20.9%、5千人以上：8.1%)</li><li>オーストラリア：586社 (千人未満：65.5%、千人～5千人未満：26.4%、5千人以上：8.0%)</li></ul>

※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。