Nomura Research Institute Group

NEWS RELEASE

2025 年 2 月 27 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 2024」を実施

## ～ サイバー攻撃に対する組織の回復力「サイバーレジリエンス」に注目のきざし ～

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、2024 年 7 月から 10 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 2,491 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 22 回目となります。

調査で取り上げたさまざまなテーマのうち、生成 AI、ゼロトラストセキュリティ [1]、サイバーレジリエンス、セキュリティ関連予算に関する結果を、一部抜粋して紹介します。

### ■ 日本企業の生成 AI の活用率は 65.3%

生成 AI の活用用途について尋ねたところ、日本では社内の個人利用が最も多く（51.4%）、問い合わせチャットボットなどを含む顧客向けサービスで活用していると答えた割合は 6.3%にとどまりました（図 1）。一方、米・豪では社内向け業務や顧客向けサービスでの活用が多く、日本と比べて活用用途に違いがあることが浮き彫りになりました。また、「活用していない」と回答した割合から、何らかの形で活用している企業は日本では 65.3%であったのに対し、米国は 99.2%、豪州は 100%と、ほとんどの企業で生成 AI を活用していることが分かりました。

生成 AI を活用して顧客向けサービスを提供していると回答した企業に対して、生成 AI サービスの提供を検討するにあたり、懸念や課題となることについて尋ねたところ、日本では「入力可能なデータの判断」と「ルールを策定する人材の不足」と回答した企業がそれぞれ 45.7%と最も多い結果となりました（図 2）。米国では「利用コストの予測」（47.6%）、豪州は「ルールを策定する人材の不足」（44.4%）が最も多くを占め、日本ではデータの入出力に対する懸念や課題意識が強いことがうかがえました。

図 1：生成 AI の活用用途

Q.「生成 AI（ChatGPT、コード生成 AI、Azure OpenAI Service など）活用の用途について、以下の中からあてはまるものをすべてお選びください。」（複数回答）

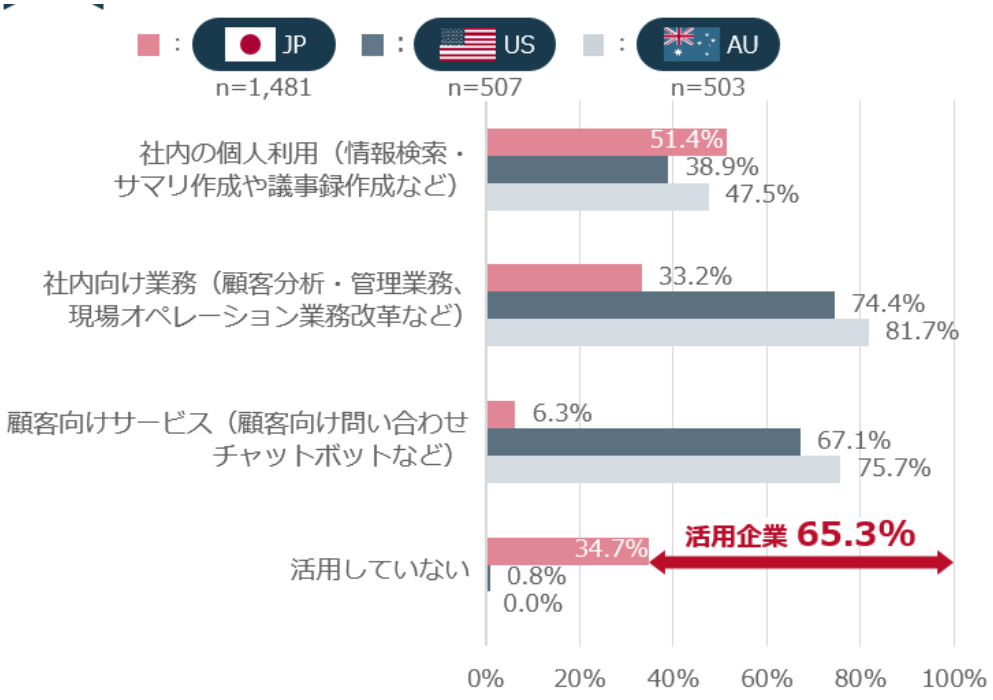



図 2：生成 AI サービスの提供を検討するにあたり懸念や課題となること

Q.「生成 AI サービスの提供を検討するにあたり、懸念や課題となることはありますか。以下の中からあてはまるものをすべて選択してください。」（複数回答）

| | JP n=94 | US n=340 | AU n=381 |
|---|---|---|---|
| 1位 | 45.7% 入力可能なデータの判断 | 47.6% 利用コストの予測 | 44.4% ルールを策定する人材の不足 |
| 2位 | 45.7% ルールを策定する人材の不足 | 47.1% | 38.8% 利用コストの予測 |
| 3位 | 39.4% 出力される結果の不安定さ | 39.1% | 36.5% 利用用途の定義 |
| 4位 | 37.2% 利用用途の定義 | 36.2% | 35.7% 自社業務に応用できる人材の不足 |
| 5位 | 36.2% 利用コストの予測 | 34.7% 入力可能なデータの判断 | 29.4% 利用可能ユーザの制御 |

※ 他選択肢：生成AI特有の攻撃（プロンプトインジェクション等）対策 ／その他（具体的に記載）

※ 生成AIを活用して顧客向けサービスを提供していると回答した企業のみ

## ■ ゼロトラストセキュリティは検討段階から実装要否を決めた段階へ

ゼロトラストセキュリティの実施状況について尋ねたところ、「ゼロトラストを全面的に実装している」または「ゼロトラストを一部実装している」と回答した日本企業の割合は、合計で 21.1%となり、2 年前の調査と比べると 7.8 ポイント増加しました（図 3）。また、「ゼロトラストを検討したが実装しなかった」と回答した割合も 9.1%と、同じく 4 ポイント増加しています。これらより、ゼロトラストを実装するかどうかを検討する段階を終えて、実装の有無を決めた企業が増えている傾向が推測できます。

さらに、VPN の使用状況を調査しました。その結果、約 8 割の日本企業が「今後も使用を継続予定」と回答した一方で、6.8%の企業が「使用停止を検討している」と回答し、2.9%は直近一年間または一年以上前に「使用を停止した」と答えました（図 4）。「使用停止を検討している」または「使用を停止した」企業に停止の理由を尋ねたところ、「ゼロトラストセキュリティ推進による脱 VPN」を選んだ割合が 62.2%と最も多くを占めました。サイバー攻撃の標的となりやすい VPN の利用をやめ、ゼロトラストセキュリティによるアクセス制御を強化する動きが広がっていることが考えられます。

図 3：日本におけるゼロトラスト実施状況

Q.「ゼロトラストの実施状況について、以下の中から最もよくあてはまるものを 1 つお選びください。」

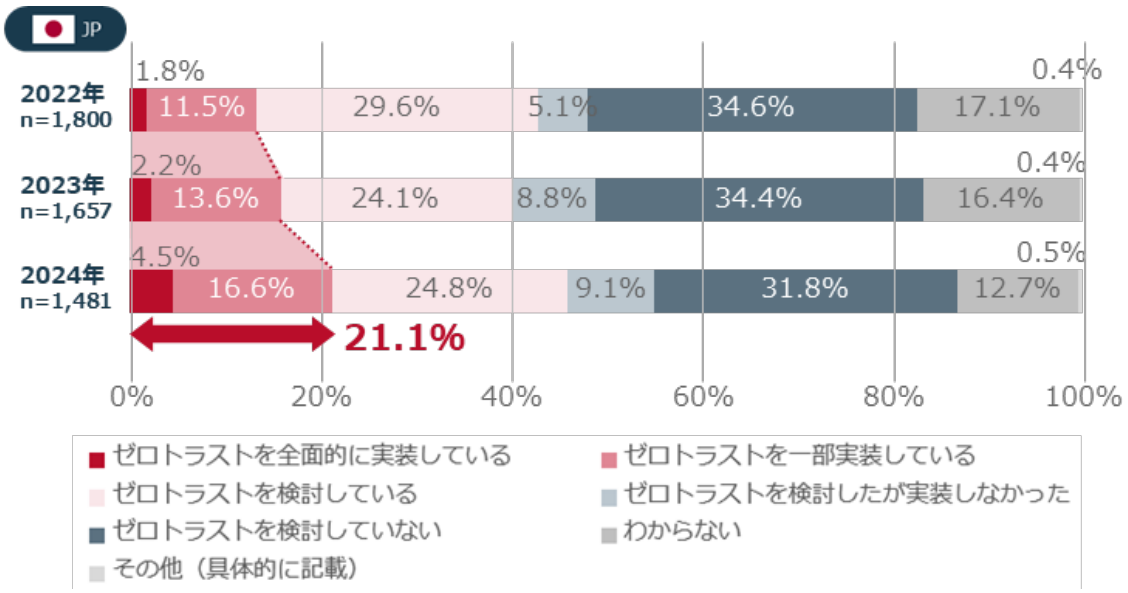
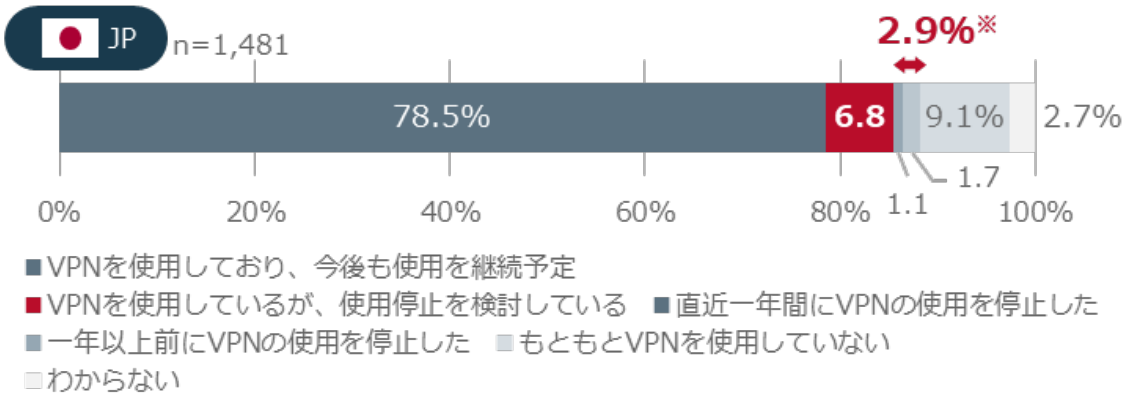


図 4：日本における VPN の使用状況

Q.「あなたの会社では現在 VPN を使用していますか？以下の中から最もよくあてはまるものを 1 つ選択してください。」




※各選択肢の小数点以下の値の四捨五入の関係で、合計値とずれが生じています。

## ■ サイバーレジリエンスへの注目度は規模が大きい企業ほど高い

近年、「サイバーレジリエンス」が注目を集めています。サイバーレジリエンスとは、サイバー攻撃に対する組織の対応力と回復力を指し、有事の際にもビジネスの継続性を維持して被害の影響を最小限に抑える能力を指します。今回の調査では、サイバーレジリエンスの理解度やその実践状況について尋ねました。「サイバーレジリエンスを理解している」と回答した日本企業の割合は全体では 24.7%でしたが、そのうち従業員規模が 1 万人以上の企業では、80.0%を占めました（図 5）。規模が大きい企業ほど、アタックサーフェス（攻撃対象領域）が広く、サプライチェーンリスクへの関心が高まることから、サイバーレジリエンスへの注目も高くなっていると考えられます。

「サイバーレジリエンスを理解し、実践している」と回答した企業に対して、具体的な取り組み内容を尋ねたところ、「訓練、教育の実施」（71.2%）、「技術的対策の強化（検知、対応、復旧）」（61.0%）が上位に挙がりました（図 6）。訓練や教育は従来多くの企業で実施されてきたため、最も多い回答を得ましたが、サイバー攻撃の検知、対応、復旧にかかる技術的対策を強化するという選択肢が二番目に多かった背景には、サイバー攻撃から守る対策だけではなく、攻撃の検知と対応および自社で被害が発生した際の復旧に至るまでが、事業活動の継続において重要視されていることが推測されます。

図 5：サイバーレジリエンスを理解・実践している日本企業の割合

Q.「サイバーレジリエンスについて、以下の中から、最もよくあてはまるものを 1 つお選びください。」

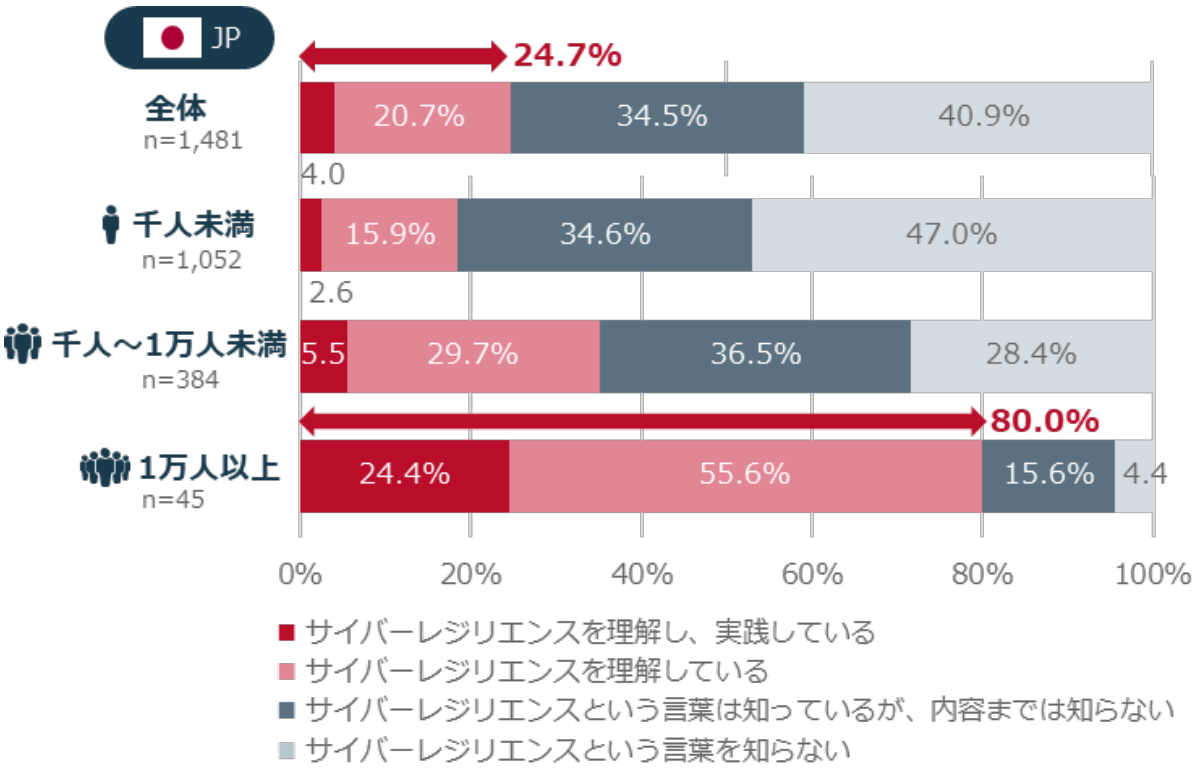
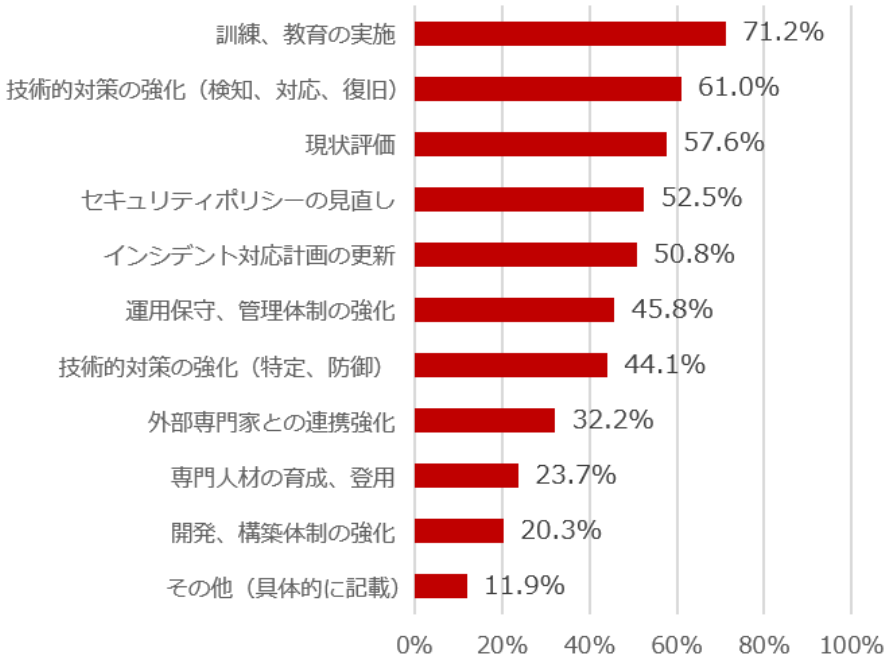



図 6：サイバーレジリエンスの実践に向けた取り組み

Q.「サイバーレジリエンス実践の取り組みについて、以下の中からあてはまるものをすべてお選びください。」（「サイバーレジリエンスを理解し、実践している」と回答した日本企業のみ (n=59)、複数回答）

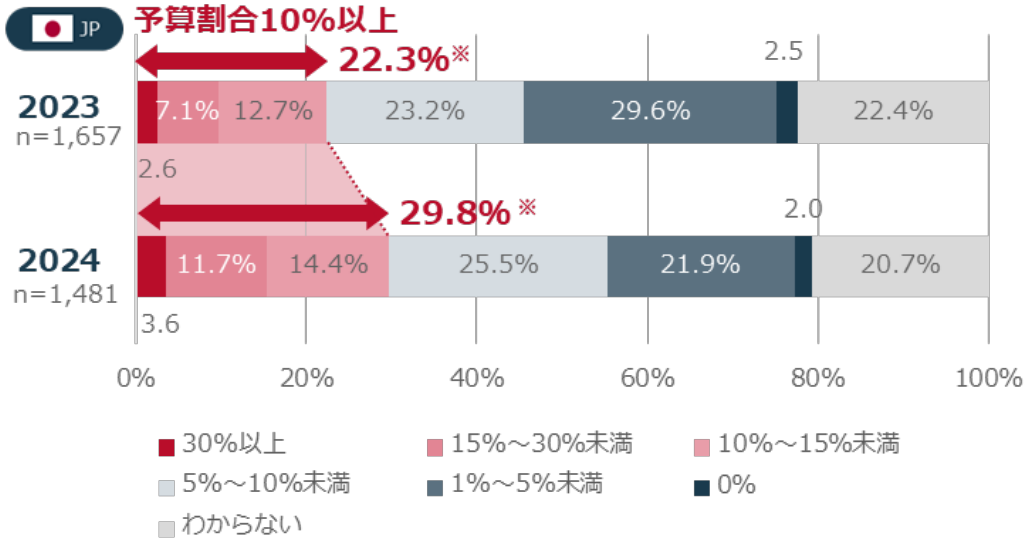


## ■ IT 関連予算に占めるセキュリティ関連予算の割合が増加

IT 関連予算のうちセキュリティ関連予算が占める割合についても尋ねました。その結果、2023 年度の調査では 10%以上を占めると回答した日本企業は全体の 22.3%だったのに対して、2024 年度の調査では 29.8%と 7.5 ポイント増加しました（図 7）。背景には、多発するランサムウェア攻撃への対策などで、セキュリティ施策に投資する動きが拡大していることが影響していると考えられます。

図 7：IT 関連予算に占めるセキュリティ関連予算の割合

Q.「IT 関連予算に対する情報セキュリティ関連予算の割合は、どの程度を見込んでいますか。以下の中から、最もよくあてはまるものを 1 つお選びください。」




※各選択肢の小数点以下の値の四捨五入の関係で、合計値とずれが生じています。

今回の調査では、ゼロトラストセキュリティの実装要否を決めた企業が増えていることに加えて、規模の大きい企業ほどサイバーレジリエンスへの注目度が高いことが明らかになりました。背景には、企業の関心がサイバー攻撃からの防御にとどまらず、攻撃を受けた際の復旧までを視野に入れた、組織としての対応力を志向してきていることがうかがえます。昨今のサプライチェーン統制の広がりにより、セキュリティ対策の強化が企業規模を問わず求められるようになる中、サイバーレジリエンスについても、今後理解や取り組みが進んでいくと NRI セキュアでは考えています。また、DX 推進と生成 AI の活用に伴う新たなセキュリティリスクが登場し、社会的に注目を集めるセキュリティインシデントも増加していることを踏まえると、IT 関連予算の中でセキュリティ関連予算が占める割合は、今後も増加する可能性が高いと予測しています。

「企業における情報セキュリティ実態調査 2024」の詳細なレポートは、次の Web サイトから入手できます。

https://www.nri-secure.co.jp/download/insight2024-report

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。

## 【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 2024」 |
| 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：2024 年 7 月 23 日～2024 年 9 月 20 日<br>• アメリカ、オーストラリア：2024 年 10 月 15 日～2024 年 10 月 28 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：1,481 社<br>（千人未満：71.0%、千人～5 千人未満：22.9%、5 千人以上：6.1%）<br>• アメリカ：507 社<br>（千人未満：67.1%、千人～5 千人未満：26.4%、5 千人以上：6.5%）<br>• オーストラリア：503 社<br>（千人未満：65.6%、千人～5 千人未満：29.1%、5 千人以上：5.4%） |

※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。

[1] 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、サイバーセキュリティの考え方です。

**【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