Nomura Research Institute Group

NEWS RELEASE

2020 年 12 月 15 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、「企業における情報セキュリティ実態調査 2020」を実施

～ 日本企業の DX とテレワークが加速するも、セキュリティが課題であることが浮き彫りに ～

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：小田島 潤、以下「NRI セキュア」）は、2020 年 7 月から 9 月にかけ、日本、アメリカ、オーストラリア 3 か国の企業を対象に、「企業における情報セキュリティ実態調査 2020」を実施しました。合計 2,260 社から得た回答を集計・分析した結果を、「NRI Secure Insight 2020」として本日発表します。この調査は、2002 年度から毎年実施しており、今回で 18 回目となります。

今回の調査で明らかになったのは、おもに以下の 3 点です。

1. DX 推進に伴い、セキュリティ対策の見直しを実施している日本企業は約 2 割

デジタルトランスフォーメーション（DX）を取り組むにあたっての阻害要因について尋ねたところ、日米豪 3 か国で、「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」を挙げた企業がそれぞれ 4～5 割を占め、最も多い結果となりました。また、「情報セキュリティへの対応」も、日本で 32.4%（2 番目）、米国で 26.5%（3 番目）、豪州で 25.6%（3 番目）と多く、企業風土や組織構造とともに、大きな阻害要因になっていることがうかがえます（表 1）。

DX 推進にあたり、「自社のセキュリティ戦略やルール、プロセスを見直しているか」を尋ねると、日本では「検討中」と答えた企業が 59.0%と最も多く、「一部実施」および「実施済」はあわせて 21.7%に留まりました（図 1）。一方、米豪では 7 割を超える企業が「一部実施」「実施済」と回答しており、日本企業の対応の遅れが明らかになりました。日本企業は、セキュリティへの対応を課題と認識してはいるものの、実際は不十分な対策のまま DX を進めてしまっている可能性が高いと考えられます。

2. 約半数の日本企業が、新型コロナウイルス感染症拡大以降にテレワークを開始

日本企業で「COVID-19 以前より、テレワークを実施していた」と答えた割合は 20.9%で、「COVID-19 以降に実施し始めた」が 52.1%でした。（図 2）。また、テレワークに伴うセキュリティへの対応状況につ

いては、「セキュリティ要件を把握し、対策を行っている」（56.5%）が最も多かった一方、「要件を把握しているが、対策を行えていない」（31.1%）、「要件を把握していない」（8.0%）という回答もありました（図3）。

以上から、新型コロナウイルス感染症拡大を受けて、ビジネスを継続するためにテレワークが急速に広がったものの、テレワーク実施企業の約 4 割においては、テレワークのためのセキュリティ対策が追い付いていないことがわかります。

3. 日本企業のサプライチェーンのセキュリティ対策は、委託先企業や国外向けで課題

日本では、国内関連子会社に対しては 71.0%、国外関連子会社に対しては 57.0%の企業が、セキュリティ対策状況を把握していると回答しました。米豪の企業についてみると、国内・国外関連子会社のいずれに関しても把握している割合が 8 割前後と、日本よりも高くなっています（図 4）。ビジネスパートナーや委託先企業に対してのセキュリティ統制状況についても、米豪では 8 割以上の企業がセキュリティ統制を実施しているのに対して、日本で実施している企業は、国内で 51.9%、国外に対しては 35.2%に留まる結果となりました（図 5）。

日本のグローバル企業においても、サプライチェーンに起因したセキュリティインシデント（事件・事案）が近年相次いで発生していますが、以上の結果からパートナーや委託先企業に対するセキュリティ統制の強化が必要であることがわかります。

この調査結果の詳細は、次の Web サイトから入手いただけます。

https://www.nri-secure.co.jp/download/insight2020-report

2020 年は、新型コロナウイルス感染症の拡大防止策や緊急事態宣言等により多くの企業活動が制限される年になりましたが、DX の機運は継続して高まっています。新たな社会環境（ニューノーマル）のなか、クラウドサービスの活用や企業間のコラボレーションもますます進展しており、デジタルサービスやテレワーク、サプライチェーンを狙うサイバー攻撃も国内外で多数発生しています。

今回の調査では、日本企業は DX、テレワーク、サプライチェーンのいずれの領域においても、セキュリティ対策が十分とは言えず、取り組み強化の必要性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。

【ニュースリリースに関するお問い合わせ先】

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 2020」
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：2020 年 7 月 1 日～9 月 18 日 アメリカ、オーストラリア：2020 年 8 月 1 日～9 月 18 日
調査方法	Web によるアンケート
対象企業	日本：株式上場企業または従業員数 350 人以上の企業 アメリカ、オーストラリア：従業員数 500 人以上の企業
回答企業数	日本：1,222 社、アメリカ：523 社、オーストラリア：515 社

■ 表 1：DX に取り組む際の阻害要因

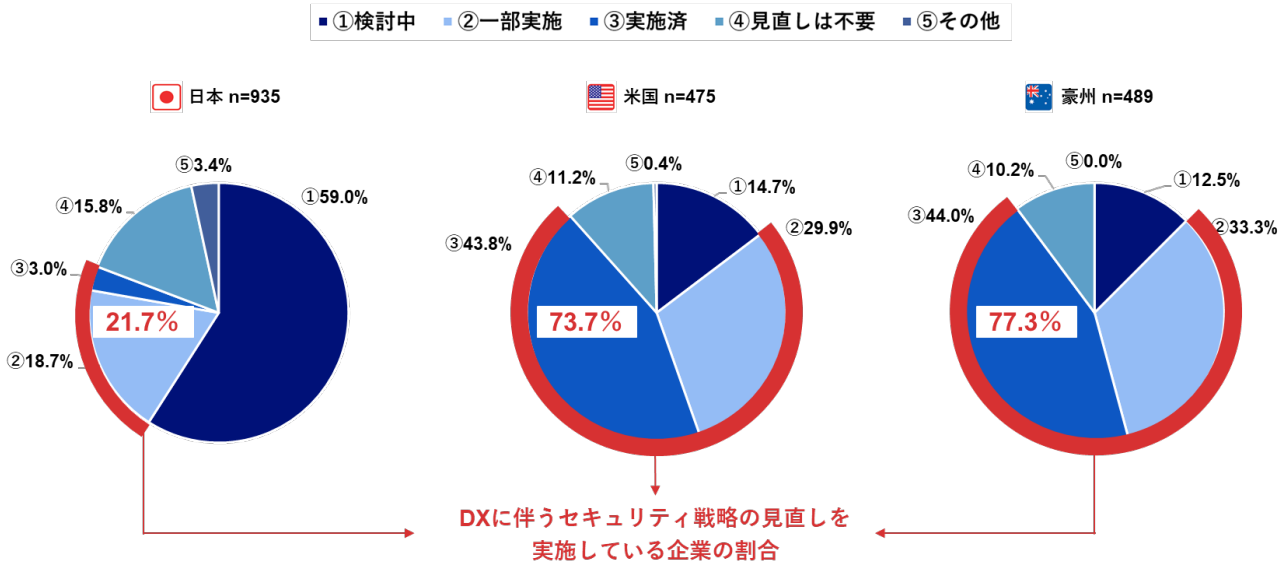
Q. デジタルトランスフォーメーションの取り組みを進めるにあたって、阻害要因はありますか。
以下の中から、あてはまるものを全てお選びください。

	日本 n=1,222		米国 n=523		豪州 n=515	
1位	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	54.5%	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	42.1%	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	44.2%
2位	情報セキュリティへの対応	32.4%	変化を受け入れる企業風土がない	28.2%	縦割りの組織構造	26.2%
3位	変化を受け入れる企業風土がない	31.8%	情報セキュリティへの対応	26.5%	情報セキュリティへの対応	25.6%
4位	DXに対する経営の理解	28.0%	縦割りの組織構造	25.3%	変化を受け入れる企業風土がない	22.1%
5位	縦割りの組織構造	24.8%	DXに対する経営の理解	14.5%	DXに対する経営の理解	15.1%
6位	デジタルトランスフォーメーションには取り組んでいない	23.5%	デジタルトランスフォーメーションには取り組んでいない	9.2%	課題はない	12.5%
7位	課題はない	16.3%	課題はない	7.8%	デジタルトランスフォーメーションには取り組んでいない	5.0%
8位	その他	2.5%	その他	0.8%	その他	0.6%

※「課題はない」「デジタルトランスフォーメーションには取り組んでいない」を選択した場合は、
他の選択肢の回答不可とし、他は複数選択。

■ 図 1：DX に伴うセキュリティ対策の見直し状況

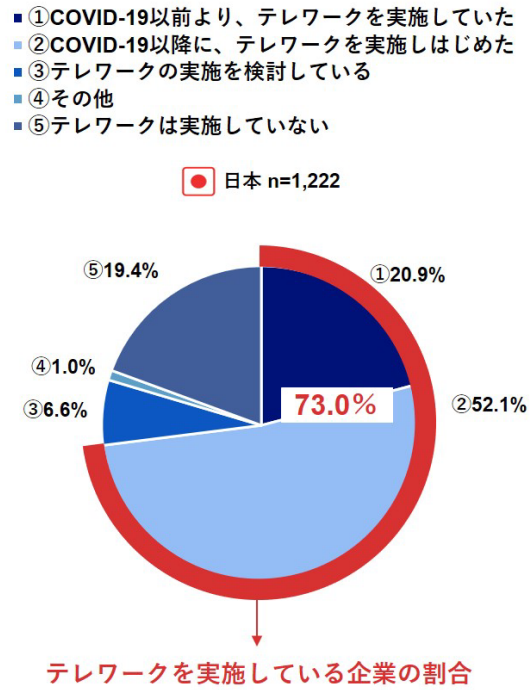
Q.デジタルトランスフォーメーションの取り組みを進めるにあたって、
自社のセキュリティ戦略やルール、プロセスの見直しを行っていますか。



※「デジタルトランスフォーメーションには取り組んでいない」と回答した企業は除く。

■ 図 2：日本企業のテレワーク実施状況

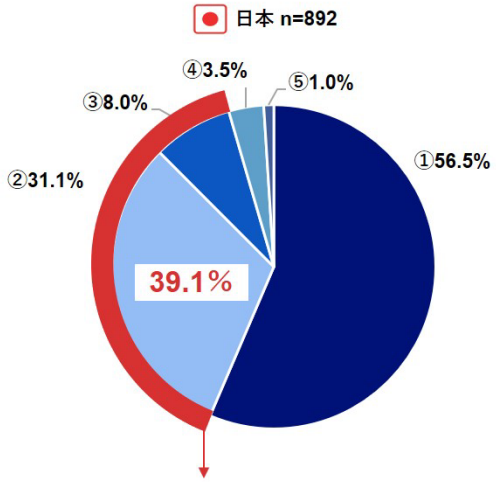
Q. テレワークの実施状況を教えてください。



■ 図 3：日本企業のテレワーク実施に伴うセキュリティへの対応状況

Q. テレワーク実施に伴う、セキュリティへの対応状況を教えてください

- ①テレワークに伴うセキュリティ要件を把握し、対策を行っている
- ②テレワークに伴うセキュリティ要件を把握しているが、対策を行えていない
- ③テレワークに伴うセキュリティ要件を把握してない
- ④わからない
- ⑤その他



テレワークを実施している企業のうち、
テレワークのセキュリティ対策を行えていない企業の割合

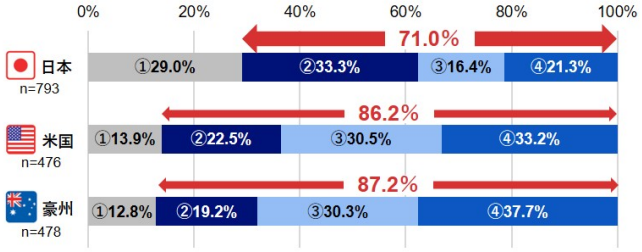
※テレワークを実施中の企業のみ回答。

■ 図 4：サプライチェーンに対するセキュリティ統制（関連子会社）

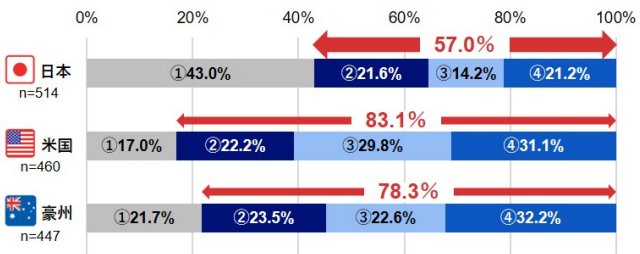
Q.サプライチェーンにおけるセキュリティの対応状況についてお答えください。

- ①セキュリティ対策状況を把握していない
- ②セキュリティ対策状況を把握している
- ③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
- ④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

● 国内の関連子会社



● 国外の関連子会社



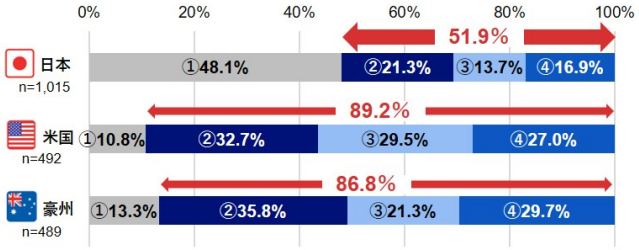
※セキュリティ統制の対象となる、関連子会社が存在する企業のみ回答。

■ 図 5：サプライチェーンに対するセキュリティ統制（パートナー・委託先）

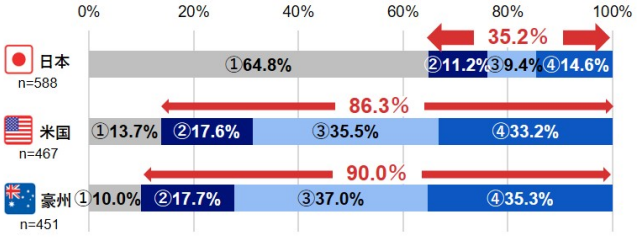
Q.サプライチェーンにおけるセキュリティの対応状況についてお答えください。

■①セキュリティ対策状況を把握していない　■③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
■②セキュリティ対策状況を把握している　■④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

● 国内のビジネスパートナーや委託先企業



● 国外のビジネスパートナーや委託先企業



※セキュリティ統制の対象となる、ビジネスパートナーと委託先企業が存在する企業のみ回答。