Nomura Research Institute Group

NEWS RELEASE

2019 年 7 月 18 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 2019」を実施

～DX の推進に向けて、セキュリティ対応の意識・行動改革が求められる日本企業～

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、2018 年 12 月から 2019 年 2 月にかけ、日本、アメリカ、シンガポールの 3 か国で、「企業における情報セキュリティ実態調査 2019」を実施しました。2,807 社から得た回答を集計・分析し、「NRI Secure Insight 2019」として本日発表します。本調査は、2002 年度から毎年実施しており、今回で 17 回目となります。

本調査で明らかとなったのは、おもに以下の 3 点です。

■ DX に取り組む日本企業は 3 割、デジタルセキュリティに対応する企業は 16.7%

DX（デジタル・トランスフォーメーション）への取り組み状況について尋ねたところ、「取り組んでいる」と回答した日本企業の割合は、30.7%でした（図 1）。取り組みを阻害する要因としては、「技術を実装する人員やリソースの確保やスキル」（39.2%）、「予算配分や投資判断」（33.3%）が最も多く挙げられています（図 2）。

DX の推進においては、複数の関係者がコラボレーションし、新しい技術や複数のクラウドサービスの活用によって、社内外の多種多様なシステムとのつながりが拡大していくことから、従来型のセキュリティ対策とは異なるセキュリティ要請への対応（デジタルセキュリティ）が求められます。「DX でセキュリティの要請が変わり、ルールや対策更新等の対応をしている」と答えた日本企業は、回答全体の 4.9%と低く、「今後対応する予定」と合わせても、16.7%にとどまりました（図 1）。

回答企業の範囲が同一ではないため比較には注意を要しますが、アメリカおよびシンガポールの調査では、いずれも 85%以上の企業が「DX に取り組んでいる」と回答し、デジタルセキュリティに対応している（予定を含む）企業の割合も、アメリカで 58.4%、シンガポールで 54.5%となりました。DX を推進して自社のビジネスを拡大させていくためには、デジタルセキュリティへの対応が不可欠であり、DX に取り組む日本企業の意識改革と早急な対応が求められます。

■ 日本企業の CISO 設置率は約半数、経営のリーダーシップ向上が課題

自社の CISO（最高情報セキュリティ責任者）について質問したところ、「設置している」と答えた企業が日本では 53.4%だったのに対して、アメリカは 86.2%、シンガポールで 86.7%でした（図 3）。また、この 1 年間で実施したセキュリティ対策について、実施のきっかけや理由を尋ねると、日本企業は、「自社でのセキュリティインシデント（事件・事故）」（33.6%）が最も多かったのに対して、他の 2 か国は「経営層のトップダウン指示」（アメリカ 55.4%、シンガポール 66.1%）がトップでした（図 4）。

日本企業は、インシデントの発生をきっかけにセキュリティ対策を実施するという、後手に回った対応が多いとみられます。DX やデジタルセキュリティなど、企業を取り巻く環境が目まぐるしく変化する中で、今後は、セキュリティ分野における経営のリーダーシップを向上させ、先を見据えた対策を打っていく必要があります。

■ 日本ではヒューマンエラーによるセキュリティの事件・事故が上位

過去 1 年間のセキュリティ関連のインシデントについて尋ねたところ、何らかの事件・事故が発生したと答えた企業の割合は、3 か国いずれも 80%以上を占めました。しかしながら事件・事故の種類別にみると、日本企業では「メールの誤送信」や「情報機器の紛失・置き忘れ」といったヒューマンエラーに起因するものが上位を占めましたが、アメリカ・シンガポールではいずれも、「DoS 攻撃／DDoS 攻撃[1]」「Web アプリケーションの脆弱性を突いた攻撃」が首位となり、3 位以降もサイバー攻撃による事件・事故が多く挙げられました（表 1）。

その背景として、これら 2 か国の企業は日本に比べて、クラウドサービスの活用や DX への取り組みが進んでおり、インターネットへ公開しているサービスの数が多いことから、外部からの攻撃が盛んであることが考えられます。こういった傾向は、DX が進展するとともに日本でも増えていくと予想され、その対策に一層取り組む必要があります。

本調査結果の詳細は、下記の Web サイトからご入手いただけます。

https://www.secure-sketch.com/ebook-download/insight2019-report

[1] DoS 攻撃／DDoS 攻撃：DoS（Denial of Service）は、システムのサービス継続を妨害すること。DoS 攻撃のうち、攻撃元を分散させて防御を困難にした攻撃を、DDoS（分散型 DoS）攻撃と呼ぶ。

【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 2019」

調査目的：　日本、アメリカ、シンガポール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：2019 年 1 月 15 日～2 月 28 日

アメリカ・シンガポール：2018 年 12 月 3 日～12 月 14 日

調査方法：　Web によるアンケート

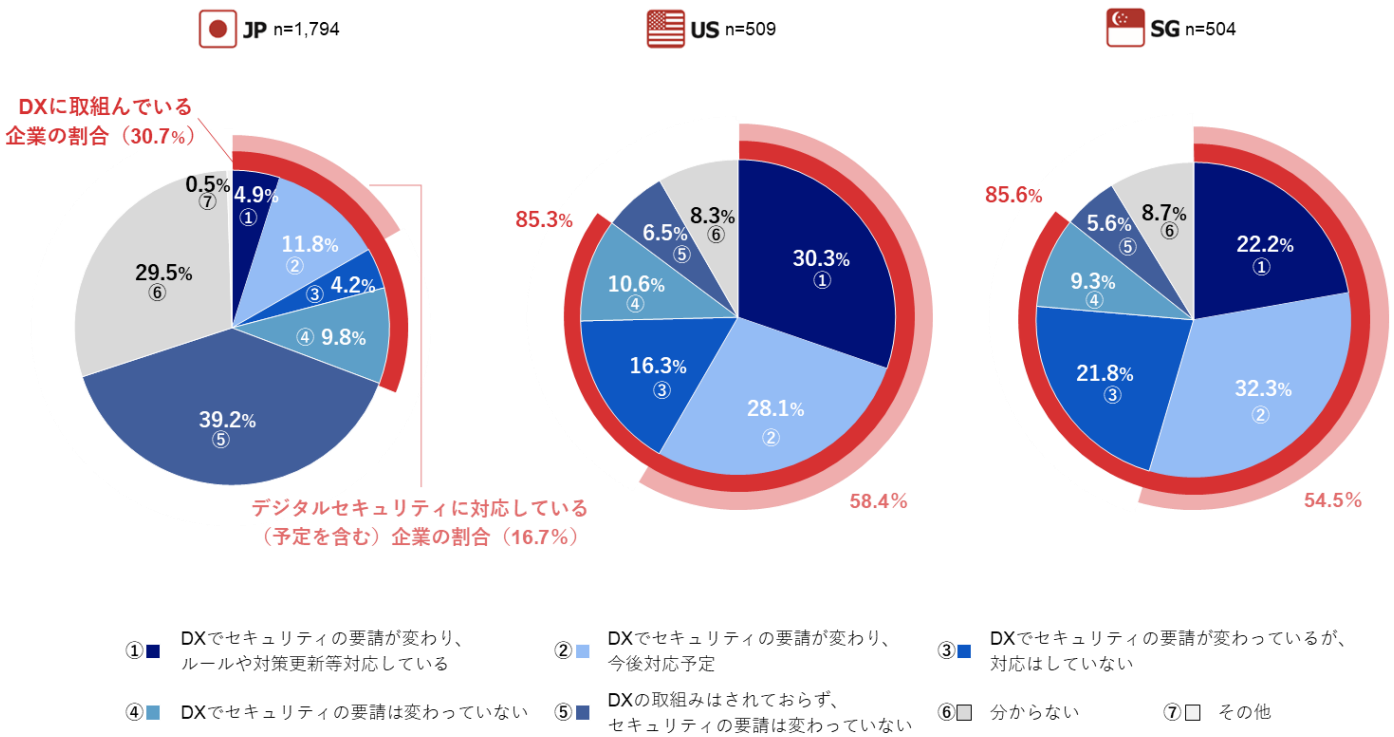
対象企業：　日本：株式上場企業または従業員数 350 人以上の企業

アメリカ・シンガポール：　従業員数 500 人以上の企業

回答企業数：日本：1,794 社、アメリカ：509 社、シンガポール：504 社

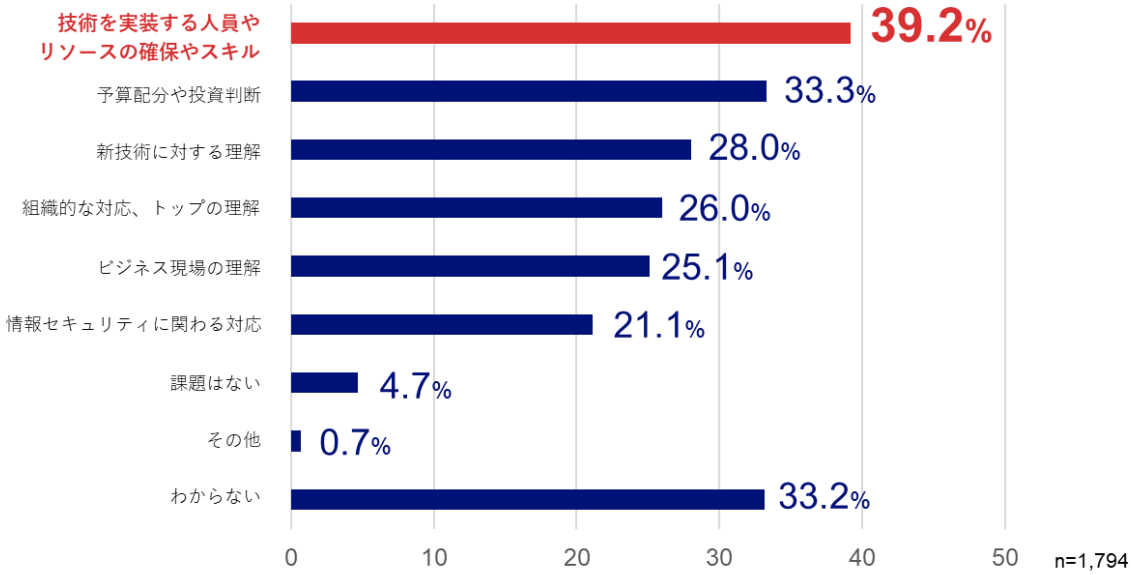
（日本は相対的に規模の小さい企業も対象に加えていることに留意）

■ 図 1：DX への取り組みおよびそれに伴うセキュリティ対応



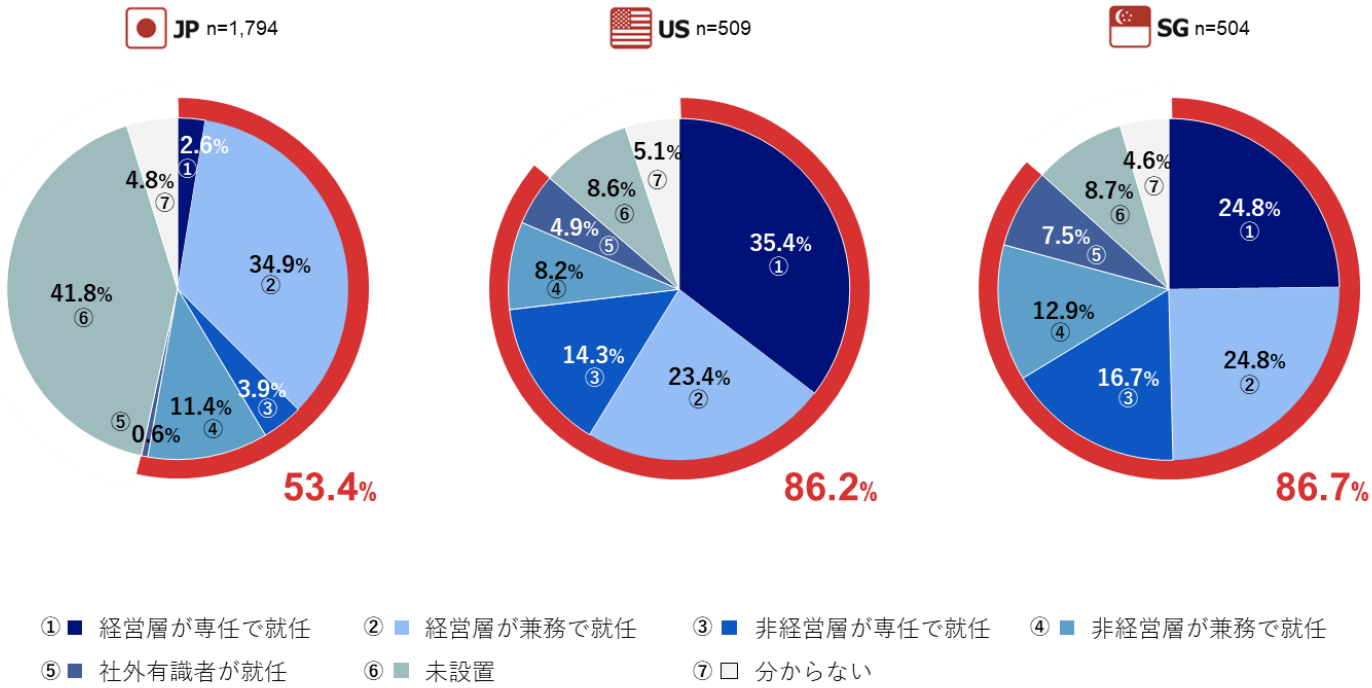
Q. 一般的に“デジタル変革・デジタルトランスフォーメーション”と呼ばれるビジネスでの高度なIT活用の取組みは進んでいますか。また、それらの取組みによって情報セキュリティに対する変化はありますか。

■ 図 2：日本企業が DX に取り組む際の阻害要因



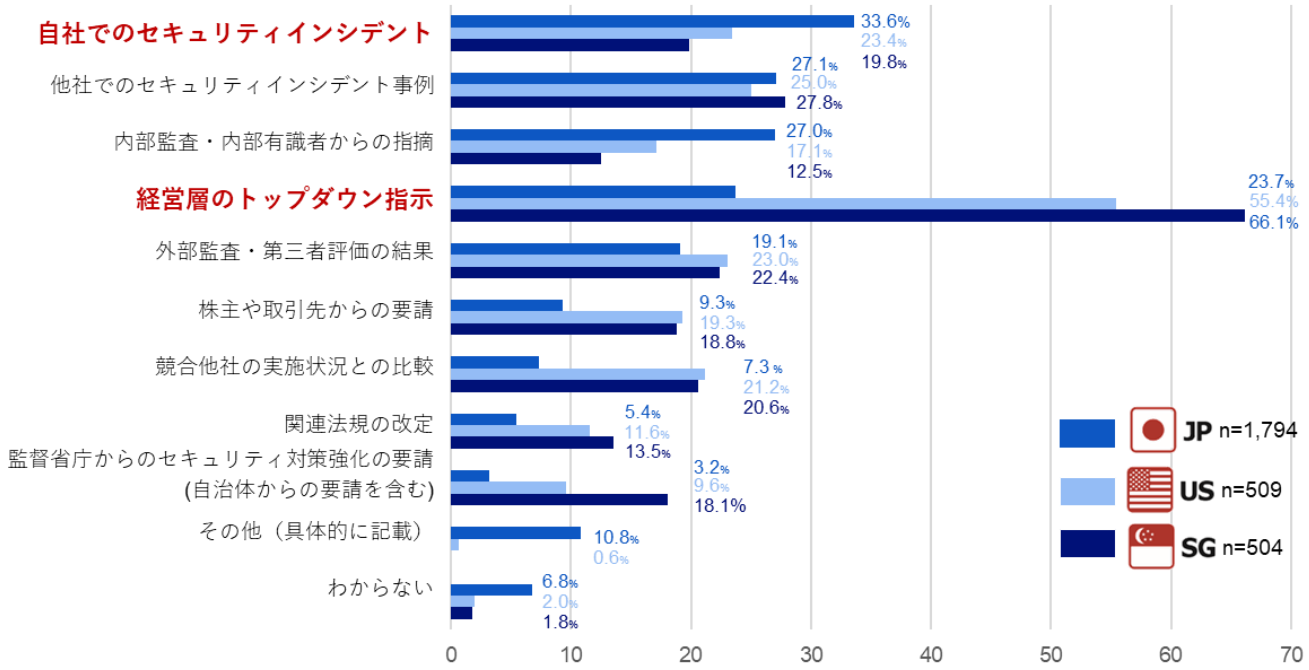
Q. デジタルトランスフォーメーションの取組みを進めるにあたって、阻害要因はありますか。（あてはまるものを全て選択）

■ 図 3：CISO を設置している企業の割合



Q. CISO（最高情報セキュリティ責任者）の設置状況についてお答えください。

■ 図 4：過去 1 年間で実施したセキュリティ対策のきっかけ



Q. 直近1年に実施した情報セキュリティ対策の実施のきっかけや理由はなんですか。（あてはまるものを最大3つ選択）

■ 表 1：過去 1 年間で発生したセキュリティ事件・事故（22 項目中上位 10 項目）

ヒューマンエラー	JP n=1,794		US n=509		SG n=504	
1位	**電子メール、FAX,郵便物等の誤送信・誤配信**	**29.4%**	DoS攻撃／DDoS攻撃	30.6%	DoS攻撃／DDoS攻撃	36.5%
2位	**情報機器・外部記憶媒体の紛失・置き忘れ・棄損**	**22.6%**	Webアプリケーションの脆弱性を突いた攻撃	29.9%	Webアプリケーションの脆弱性を突いた攻撃	29.6%
3位	マルウェア感染	22.5%	システム基盤の脆弱性を突いた攻撃	23.4%	自社サービスへのリスト型アカウントハッキング	25.8%
4位	**システム設定ミス、誤操作**	**19.8%**	自社サービスへのリスト型アカウントハッキング	21.8%	標的型メール攻撃	20.4%
5位	標的型メール攻撃	17.9%	マルウェア感染	19.8%	システム基盤の脆弱性を突いた攻撃	19.8%
6位	**社員証、業務書類等物品の紛失・置き忘れ・棄損**	**16.9%**	標的型メール攻撃	18.1%	マルウェア感染	17.3%
7位	**情報機器、電子記憶媒体、紙媒体等の盗難・紛失**	**15.1%**	水飲み場型攻撃	11.2%	水飲み場型攻撃	11.7%
8位	ランサムウェアによる金銭等の要求	11.6%	ランサムウェアによる金銭等の要求	9.0%	**情報機器・外部記憶媒体の紛失・置き忘れ・棄損**	**9.7%**
9位	DoS攻撃／DDoS攻撃	6.5%	**電子メール、FAX、郵便物等の誤送信・誤配送**	**8.3%**	ランサムウェアによる金銭等の要求	8.5%
10位	退職者、転職者による在職時に利用していた情報の使用	4.0%	**情報機器・外部記憶媒体の紛失・置き忘れ・棄損**	**7.5%**	システム管理者（特権ユーザ）等による不正アクセスや持出	8.5%

Q.過去1年間で発生した情報セキュリティに関する事件・事故はありますか。（あてはまるものを全て選択）