NRI Secure Insight 2019

企業における情報セキュリティ実態調査

Since 2002

NRI SECURE

NRI Secure Insight 2019

企業における情報セキュリティ実態調査
Since 2002

「企業における情報セキュリティ実態調査」は、NRI セキュアテクノロジーズが毎年実施している企業の情報セキュリティに関する取り組みの実態調査です。2002年度から過去16回毎年実施してきた「企業における情報セキュリティ実態調査」での知見を活かし、17年目の今年は日本、アメリカ、シンガポールを対象とした調査を実施した結果、各国企業のセキュリティに対する意識の違いが浮き彫りになりました。本報告書の作成にあたり、アンケートにご回答頂いた皆様に深く感謝いたします。
ご協力ありがとうございました。

NRI SECURE

EXECUTIVE SUMMARY

調査概要

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状況を明らかにする
- 企業の情報システム / 情報セキュリティ関連業務に携わる方へ有益な参考情報を提供する

調査対象

- 日本、アメリカ、シンガポール企業の情報システム / 情報セキュリティ担当者

調査期間

- 日本：2019/1/15～2019/2/28、アメリカ・シンガポール：2018/12/3～2018/12/14

回答いただいた企業数

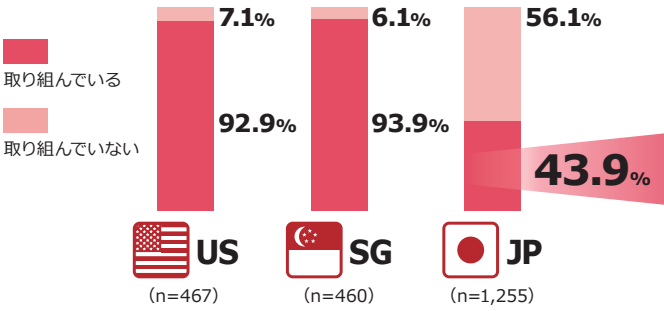
- 計 2,807 社（日本：1,794 社、アメリカ：509 社、シンガポール：504 社）

※ 米：アメリカ、星：シンガポール
※ 特に明記していない限り、調査ベースは全回答者（日本 1,794 社、アメリカ 509 社、シンガポール 504 社）

デジタルセキュリティ

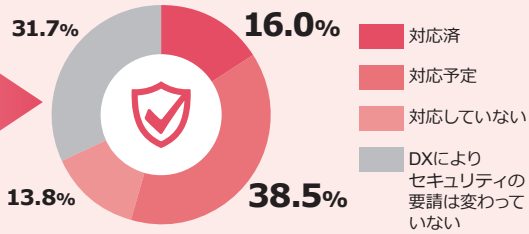
☑ 米/星の90%以上がDX※に取り組んでいる一方で、日本は50%を下回っている
☑ DXに取り組んでいる日本企業の半数以上は、DXに関わるセキュリティに対応している

DXに取り組んでいる企業



※ ビジネスモデルの変革や創造に寄与する高度なIT活用の取り組み

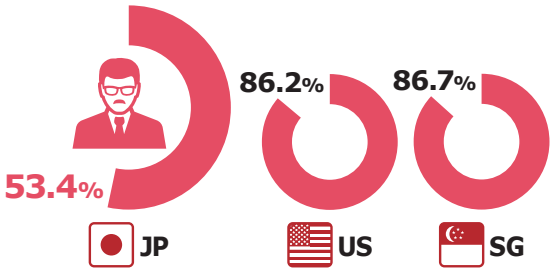
DXに関わるセキュリティに対応している日本企業（n=551）



セキュリティマネジメント

☑ 日本はCISOの設置率が米/星と比較して低い
☑ 日本の25%以上がGDPRの対応状況が「わからない」と回答、まずは対応要否を確認したい

CISO※を設置している企業



※ 最高情報セキュリティ責任者

GDPR※の対応状況

	わからない	未対応	対応中・検討中	対応済
JP	25.3%	16.4%	16.3%	8.5%
US	7.3%	7.9%	51.2%	21.3%
SG	6.5%	10.7%	55.0%	18.8%

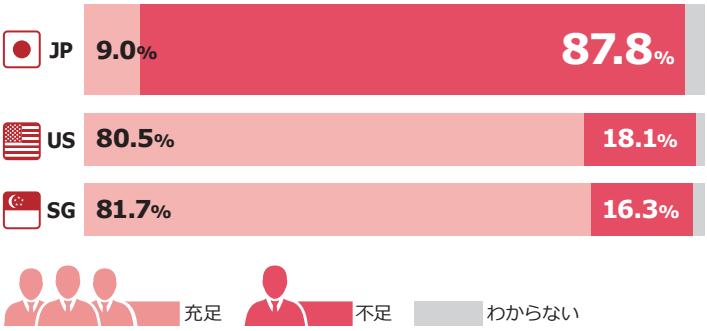
（対応不要を除く）

※ EU一般データ保護規則（GDPR: General Data Protection Regulation ）
欧州経済領域の個人データ保護を目的とした管理規則

セキュリティ人材

☑ 日本は米/星と比較して圧倒的に人材不足を訴えている
☑ セキュリティ戦略・企画を策定できる人材の育成が課題の1つか

セキュリティ対策に従事する人材の充足状況



日本企業で不足している人材 (n=1,575)

1位	セキュリティ戦略・企画を策定する人
2位	セキュリティリスクを評価・監査する人
3位	ログを監視・分析する人

セキュリティ対策

☑ 対策実施のきっかけ1位は、日本は自社のセキュリティインシデントであり、米/星は経営層の指示であった
☑ 担当者として最も対応に困っていることは、日本は対策実施・有事対応が、米/星は情報収集・共有が上位となった

セキュリティ対策の実施のきっかけや理由

1位 自社のセキュリティインシデント	1位 経営層のトップダウン指示
JP	US SG

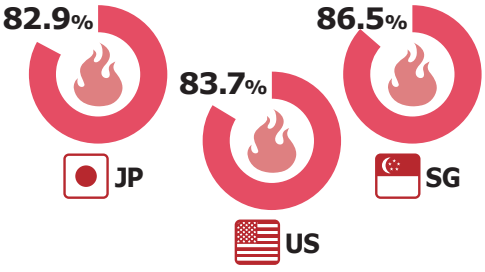
セキュリティ担当者として最も対応に困っていること

	JP	US	SG
1位	自社セキュリティ対策の遅れ（最新技術・動向の未反映）	セキュリティ対策のトレンド・他社動向の把握	
2位	セキュリティインシデント発生時の緊急対応	セキュリティ脅威・事故に関する情報収集と関係者共有	
3位	サイバー攻撃の高度化への対応	サイバー攻撃の高度化への対応	セキュリティインシデント発生時の緊急対応

脅威・事故

☑ 各国の80%以上で、過去1年間にセキュリティインシデント※が発生している
☑ 発生したセキュリティインシデントの内訳としては、日本ではヒューマンエラーが、米/星ではサイバー攻撃が上位となった

過去1年間にセキュリティインシデントが発生した企業



発生したセキュリティインシデントの内訳

	JP	US	SG
1位	メール等の誤送信・ご配送	DoS / DDoS攻撃	
2位	情報機器等の紛失・置き忘れ・破損	Webアプリの脆弱性攻撃	
3位	マルウェア感染	システム基盤への脆弱性攻撃	リスト型アカウントハッキング

※ サイバー攻撃、内部不正、あるいはヒューマンエラー等により発生した事件・事故

CONTENTS

Investigation result

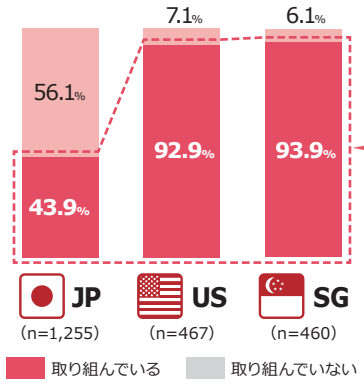
調査結果

CATEGORY

- デジタルセキュリティ
- セキュリティマネジメント
- セキュリティ人材
- セキュリティ対策
- 脅威・事故

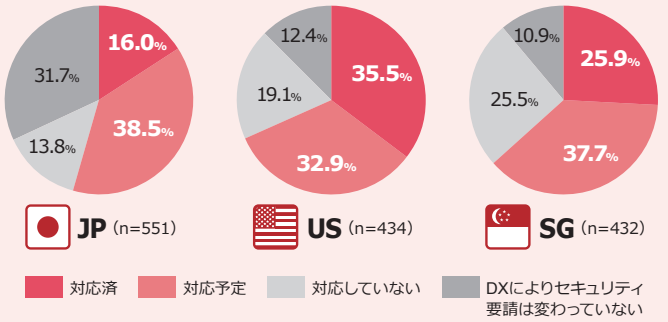
日本は米/星と比較して、DXの取り組みが進んでおらず、DXに関わるセキュリティ対応を現行の延長で捉えている企業が多い

DX※に取り組んでいる企業



※ ビジネスモデルの変革や創造に寄与する高度なIT活用の取り組み

DXに関わるセキュリティに対応している企業



- 米/星の90%以上がDXに取り組んでいる一方で、日本では約44%にとどまっている。
- DXに取り組んでいる日本企業の内、約32%が「DXによりセキュリティの要請は変わっていない」と回答しており、DXに関わるセキュリティ対応を現行の延長として捉えている割合が米/星と比べて高い。DXに取り組む企業においては、DX推進の影響分析やリスク評価を通じてセキュリティ要請のアップデート要否を組織的に判断し、必要に応じて対応することが望ましい。

各国のDXの取り組みを進めるにあたっての阻害要因TOP5

あてはまるものすべて選択

	JP (n=1,794)		US (n=509)		SG (n=504)	
1位	技術を実装する人員やリソースの確保やスキル	39.2%	新技術に対する理解	42.4%	ビジネス現場の理解	40.5%
2位	予算配分や投資判断	33.3%	ビジネス現場の理解	36.9%	技術を実装する人員やリソースの確保やスキル	39.9%
3位	新技術に対する理解	28.0%	技術を実装する人員やリソースの確保やスキル	34.2%	新技術に対する理解	38.3%
4位	組織的な対応、トップの理解	26.0%	予算配分や投資判断	26.3%	予算配分や投資判断	31.0%
5位	ビジネス現場の理解	25.1%	組織的な対応、トップの理解	23.0%	組織的な対応、トップの理解	21.2%

※ 他選択肢：情報セキュリティに係る対応/課題はない/その他

- 各国のTOP3には「新技術に対する理解」と「技術力を持つ人員の確保」が入り、DXを具現化するためのナレッジやスキルの価値が高いことが考えられる。
- 日本の阻害要因の2位は「予算配分や投資判断」であり、企業の現場はDXに取り組む際に、限られた予算や人員でDXを推進しながら、セキュリティにも配慮する必要がある。このような状況下においてはDXの取り組みを低コストで立ち上げ、リスクを小さく取りながら仮説検証を繰り返すことが現実解になるだろう。しかし、これはDX推進速度の鈍化を招きかねない。
- 日本におけるDXの取り組みをセキュリティ対応を含めて進展させるためには、経営層のDXに対する理解および適切な予算確保・投資判断が欠かせない。

時代の要請を反映するように、クラウド対応、運用業務効率化、端末脅威のリモート対応などに関心が集まる

日本企業における先進的なセキュリティソリューション導入および導入検討状況

JP (n=1,794)

			導入済みまたは検討中	導入済・利用している	検討中・関心がある	未検討・関心がない	知らない
1位	CASB	ユーザーのクラウド利用の可視化や制御 (Cloud Access Security Broker)	46.6%	4.6%	42.0%	25.1%	28.2%
2位	SOAR	セキュリティ運用の自動化及び効率化技術 (Security Orchestration, Automation and Response)	41.3%	4.8%	36.5%	27.3%	31.4%
3位	EDR	遠隔地からの端末脅威探索、アラート、インシデント時の隔離や分析の実施 (Endpoint detection and response)	38.8%	5.4%	33.4%	30.6%	30.7%
4位	UEBA	ユーザ行動に関わるログの統合分析とアラート (User and Entity Behavior Analytics)	33.1%	7.0%	26.1%	30.3%	36.6%
5位	WebAuthn	パスワードを不要とする認証	26.5%	2.1%	24.4%	35.2%	38.4%
6位	TLPT	脅威ベースのペネトレーションテスト (Threat-Led Penetration Test)	26.3%	3.4%	22.9%	35.2%	38.5%
7位	ゼロトラスト	境界防御を前提としないセキュリティ対策	24.4%	1.2%	23.2%	34.2%	41.3%
8位	DevSecOps	セキュリティチェックの継続的開発運用プロセスへの組み込み	20.2%	1.3%	18.9%	38.1%	41.7%
9位	RASP	アプリケーション稼働環境に組み込み異常検出・防御する仕組み (Runtime Application Self Protection)	19.2%	1.3%	17.9%	37.6%	43.2%
10位	DAST	アプリケーションセキュリティの動的テスト (Dynamic Application Security Testing)	18.1%	1.8%	16.3%	38.9%	43.0%
11位	IAST	アプリ稼働環境へのセキュリティテストの組み込み (Interactive Application Security Testing)	17.1%	1.3%	15.8%	39.1%	43.9%
12位	SAST	ソースコード解析ツール等によるアプリセキュリティの静的テスト (Static Application Security Testing)	16.9%	1.7%	15.2%	40.9%	42.3%

- 1位のCASBは、DXの進展によりクラウドサービスの業務利用が増えていることが背景にある。クラウドサービス全般は利用開始までの障壁が低いことがメリットであるが、その反面、「サービスの内容やリスクを十分に確認せずに利用する」、「意図しない設定のままで利用する」、「機密度の高い業務情報を取り扱う」ことに起因したインシデントの増加が導入意欲の高まりの一因と考えられる。
- 2位のSOARは、セキュリティ人材の不足に悩んでいる企業が多い中、日々増えるセキュリティアラートへの対応や業務を自動化することで、限られたリソースを効率的に活用しつつインシデントへの対応力を強化する手段として有用である。また、業務の自動化は単なるリソース不足の対応策ではなく、従業員の生産性や創造性を向上させ、単純作業の連続から来るストレスの軽減などのメリットをもたらす側面がある点も考慮したい。
- また、多様な働き方を許容・奨励する時代背景を踏まえて、企業がテレワーク導入を検討・推進するにあたり、従業員が自宅や社外などで業務利用するモバイルPCに対する脅威やインシデント発生時の迅速な対応の難しさという課題がある。それらの課題に対して、3位のEDRは、IT・セキュリティ担当者が遠隔から迅速かつ安全に対応できる手段として注目されている。
- 8位から12位は、いずれも開発プロセスにおけるスピードとセキュリティの両立を実現し、DXを促進するセキュリティソリューションである。DXの進展は利用者に対して、サービスの選択肢と乗り換えの容易性をもたらす。DXサービスの提供者は、利用者のサービスに対する興味や体験を向上させるために、俊敏かつ柔軟な開発スタイル（Agile/DevOps）を志向しているため、セキュリティ品質を担保するプロセス自体をボトルネックにしない取り組みが重要である。

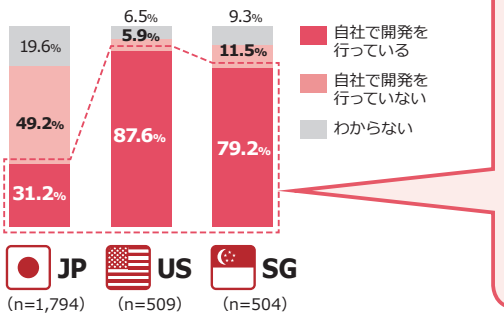
先進的なセキュリティソリューションに対するDX観点での分類

DX1.0 - 業務プロセス・インフラ変革に寄与するDX	DX2.0 – ビジネスモデルそのものを変革するDX
CASB、SOAR、EDR、UEBA、WebAuthn、TLPT、ゼロトラスト	SOAR、UEBA、WebAuthn、TLPT、DevSecOps、RASP、DAST、IAST、SAST

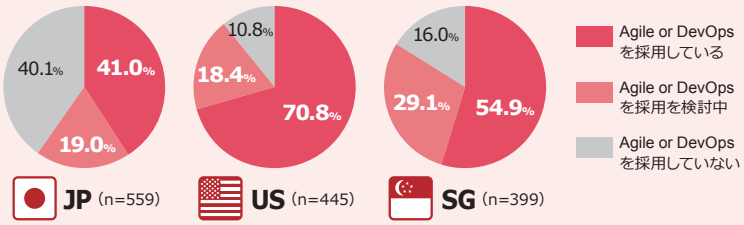
上記の12個のソリューションをDXの観点で分類し順位に着目すると、日本においては、DX1.0に資する新たな課題解決ソリューションの導入が先行している。DX2.0を促進させるセキュリティソリューションの導入は「検討中・関心がある」の回答も一定数いることがら今後進んでいくものと考えられる。

自社で開発を行う企業の40%以上がAgile/DevOpsを採用し、DXの取り組みやセキュアな開発にも積極的

３カ国の開発体制比較

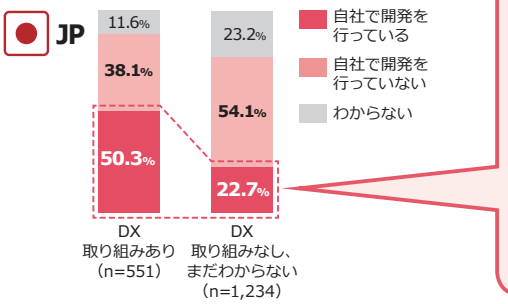


３カ国の自社開発企業のAgile型開発またはDevOpsの採用状況

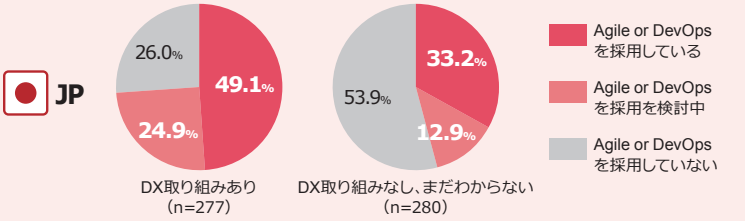


- 日本では自社で開発を行っている企業は30%程度にとどまった。自社で開発を実施している企業のうち、アジャイルもしくはDevOpsを開発プロセスに採用または採用検討中の企業は、日本では60%であり、米/星の80%以上と比較すると遅れをとっている。

日本企業のDX取り組みと開発体制



DX取り組み別の自社開発企業のAgile型開発またはDevOpsの採用状況



- DX取り組み企業の50%が自社開発し、そのうち70%強がアジャイルやDevOpsの採用に前向きである一方、DX取り組みのない企業は自社開発が約20%で、その開発・運用形態はアジャイル・DevOps未採用企業が優勢である。
- システム特性やビジネスの目標、環境により最適な開発・運用形態は異なり、依然としてウォーターフォールモデルが適している場合もある。一方、不確実性の高いDXでは事業そのものをアジャイル（機敏）に変化へと対応させていくことが求められ、それらのビジネス要求を実現する開発・運用形態が不可欠である。DXに取り組むアジャイル型の開発、内製も含めた開発体制の見直しは、デジタル事業における選択肢を増やすことにつながる。
- なお、自社開発と外部への委託開発を併用するケースも多いと考えられる。世にあるサービスや専門家のリソースを活用しつつも、事業の中核は自社で開発することが、DXの事業リスクをコントロールしつつ他社との差別化を図るうえで重要である。

日本企業における開発形態で実施率の差が大きかったセキュアな開発に係る実施状況

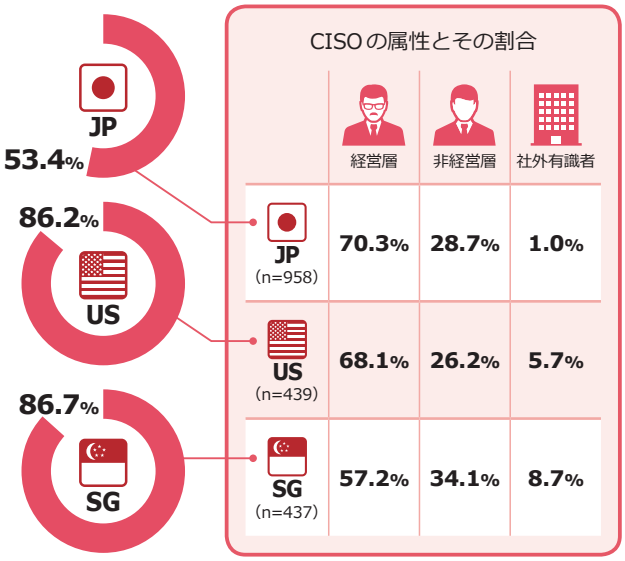
JP	実施率の差異	Agile/DevOpsを採用している日本企業の実施率（n=201）	自社開発は行っているがAgile/DevOpsを採用していない日本企業の実施率（n=208）
脆弱性チェック*2	1位 33.3pt	60.7%	27.4%
セキュアコーディングガイドライン*3	2位 19.6pt	54.2%	34.6%
セキュリティ設計レビュー*1	3位 17.8pt	85.1%	67.3%

＊1: システム設計時にセキュリティレビューを実行するようルールを定め実施している。 ＊2: システムリリース時、および定期的にソースコードをレビュー、あるいはスキャンツールを利用して脆弱性を発見している。 ＊3: セキュアコーディングガイドラインを定めている。

- リリースサイクルの早いAgile/DevOpsを採用した企業では、ツール利用を含む脆弱性の検出・チェックの導入で従来の開発手法を採用した企業との差が顕著である。
- 事業の変化に対応できる俊敏な開発組織として、多くのビジネス要求にこたえるための設計やレビューに時間を使うため、セキュア開発の標準化・自動化の組み込みが今後も浸透していくことが期待される。

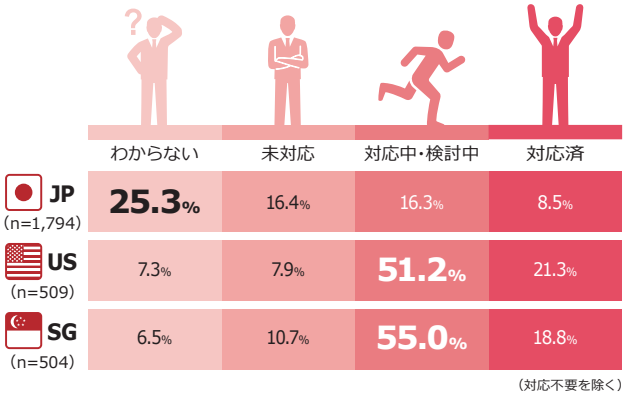
米/星に比べてGDPR対応が進んでいない日本、コンプライアンス推進にはCISOの関与が必要か

CISOを設置している企業



- 米/星ともに85%以上の企業でCISOを設置している。日本は50%台にとどまっている。
- CISOの属性内訳を見てみると、日本は経営層が就任している割合が一番高い。米/星の結果からも読み取れる通り、社外有識者の就任という選択肢もある。

GDPRの対応状況



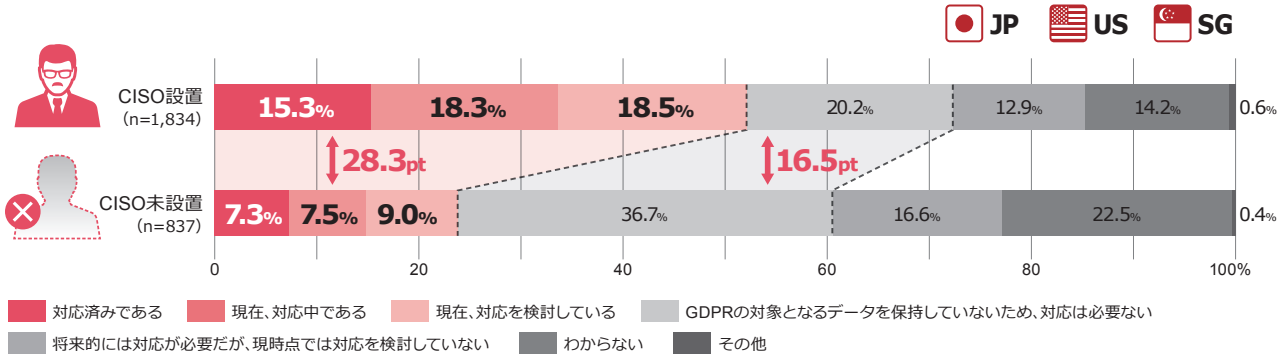
(対応不要を除く)

※ EU一般データ保護規則(GDPR: General Data Protection Regulation)欧州経済領域の個人データ保護を目的とした管理規則。
※ 他選択肢:「対象となるデータを保有していないため、対応不要」、「その他」

- 米/星は対応済、対応中・検討中が70%以上であるが、日本は25%程度にとどまった。一方、同程度の企業が「わからない」を選択しており、対応状況を把握できていないことがわかった。コンプライアンス違反で賠償責任なども問われる可能性もあるので、早急な確認が必要。

CISO有無別GDPR対応状況

※ CISO設置有無を「わからない」と答えた企業は除く。

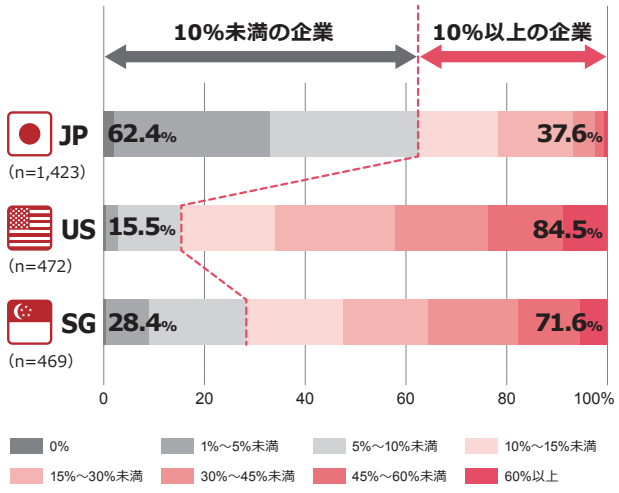


- GDPR対応状況をCISO有無別に3ヶ国合算して分析すると、CISOがいる企業の方が、いない企業に比べて「対応済・対応中・検討中」と答えた割合が約30pt高い。この結果から、CISOの関与・リーダーシップは、GDPR対応の進展に良い影響をもたらしていると考えられる。
- CISOがいない企業の方が「対応不要」と回答した割合が約16pt高かった。GDPRの保護対象となる個人データは多岐に渡るので、「対応不要」と回答した企業も"本当に対応不要なのか"、他に考慮漏れがないかを今一度確認したい。
- ある時点で「対応不要」と明確に判断した企業においても、定期的に個人データの棚卸することが望ましい。その際、経営戦略・事業戦略を踏まえて、現状だけでなく、今後取り扱う個人データの棚卸しを実施し、GDPRを含む各種コンプライアンスへの対応要否を前広に判断・対応することが重要である。

予算と人材の適切な採配には CISOのリーダーシップの発揮が求められる

IT関連の予算に占めるセキュリティ予算の割合

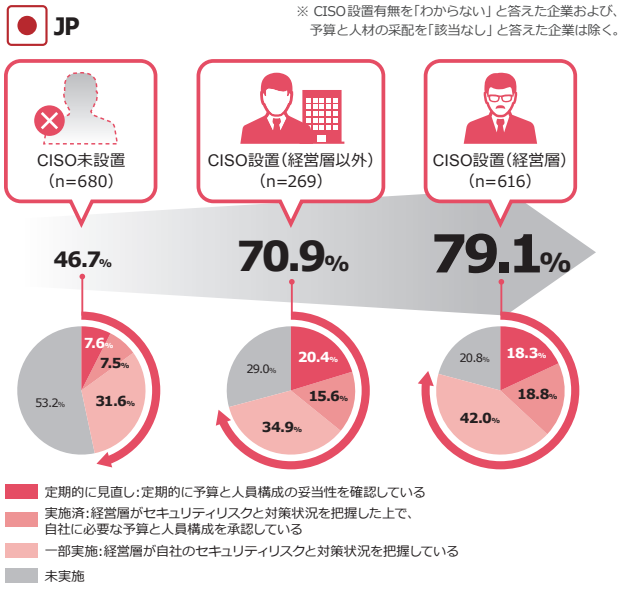
※ IT関連予算に占めるセキュリティ予算の割合を「わからない」と答えた企業は除く



- IT関連予算に占めるセキュリティ関連予算の割合が10%以上であると回答した日本企業は40%を下回った。同様の回答をした米国企業は80%以上、星国企業は70%以上であった。
- 米/星では、CISO設置企業が85%以上で、CISOの存在がセキュリティ予算獲得に良い影響を与えているとも考えられる。

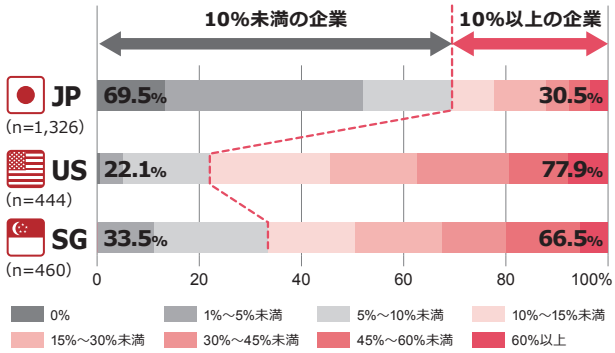
日本企業におけるCISO設置別の予算と人員の採配

※ CISO設置有無を「わからない」と答えた企業および、予算と人材の採配を「該当なし」と答えた企業は除く。



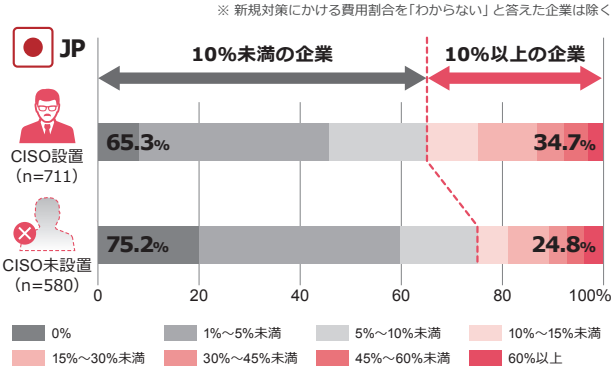
- 「経営層が自社のセキュリティリスクと対策状況を把握したうえで、自社に必要な予算と人員構成を承認しているかどうか」はCISO設置有無により実施率に差が出た。
- CISO設置企業でも、経営層の関与度合いで実施率に差が出た。自社の経営層がCISOに就任している方が予算確保の必要性が認識しやすくなり、効率的な予算と人材採配が可能になることが伺える。

セキュリティ予算に占める新規対策にかける費用の割合



- セキュリティ予算のうち、新規対策にかける費用の割合が10%以上と回答した日本企業は約30%だった。米では70%以上、星では60%以上であった。
- 日本企業では10%以上の企業が新規対策費用を割り当てていない(0%)と回答している。対策の遅れや陳腐化が自社の情報セキュリティ負債とならないように、予算策定前にリスク評価や対策の見直しを実施して、新規対策費用の割当要否を確認することが重要である。

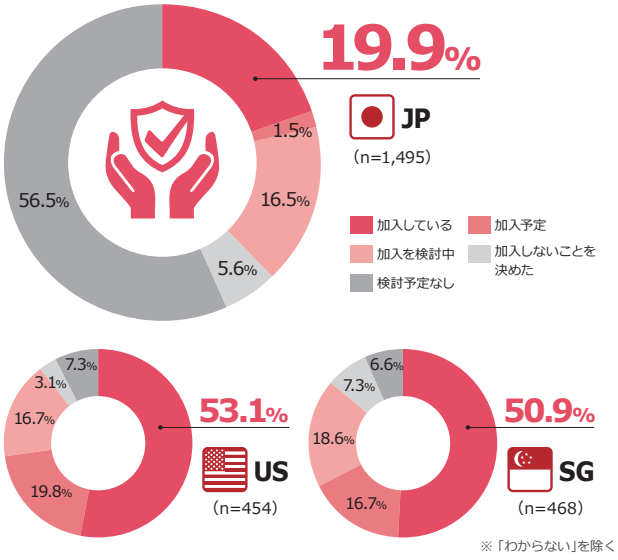
※ 新規対策にかける費用割合を「わからない」と答えた企業は除く



- CISO設置の有無によって、新規対策に割り当てる費用の割合が10%以上と回答した日本企業の割合は約10ptの差がついた。
- 従来のセキュリティ対策の高度化も必要だが、日々脅威が進化する中で、新しい対策の導入も検討すべきである。セキュリティ予算は、CISO相当の人材が経営・事業戦略を踏まえた上で、投資額とリスクのバランスをとりながら、適切な予算判断・策定することが望ましい。

日本はサイバー保険加入とガイドラインの活用に遅れが見える
自社の状況に応じてこれらの活用を積極的に検討したい

保険加入状況



※「わからない」を除く

保険加入理由

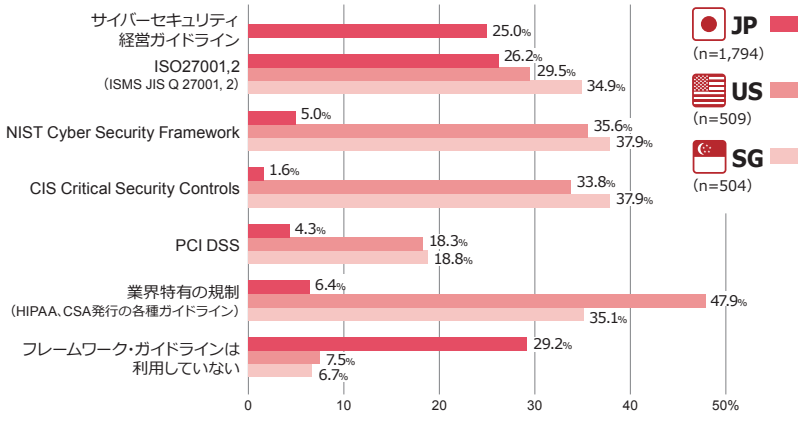
あてはまるもの最大3つ選択

	JP (n=321)	US (n=331)	SG (n=316)
1位	54.2% 自社の対応だけでは被害を防ぎきれない可能性があるため	44.4% 補償内容に対し、保険料が妥当だと感じたため	54.7%
2位	36.8% 事故発生時の見舞金等、支払う可能性がある金銭を補うため	41.4% 自社の対応だけでは被害を防ぎきれない可能性があるため	37.3%
3位	35.5% 補償内容に対し、保険料が妥当だと感じたため	23.3% 残留セキュリティリスクも適切に管理していることを株主・取引先にアピールするため	20.3%
4位	22.7% 事故発生時に迅速に対応するためのコストを捻出したいため	22.4%	19.6%
5位	12.1% トップダウン指示があったため	14.2% 事故発生時の見舞金等、支払う可能性がある金銭を補うため	15.8% 法制度改正等による罰が厳しくなっているため

- 加入予定も入れると、米/星ともに70%近い企業が保険加入に意欲がある一方、日本では20%程度に留まっている。
- 米国に比べると日本でサイバー保険商品ができたのは新しく、いまだ普及段階にあると考えられる。また、米/星では1位だった「保険料の妥当性」は日本では3位だった。保険料が高いか、あるいは事故発生時の被害額の算出が妥当にできていない可能性がある。
- 保険会社は保険料の妥当性を的確にPRすることや付帯サービスの拡充が求められる。
- 各国共に「自社の対応だけでは被害を防ぎきれない可能性がある」の回答が保険加入理由の上位に来ており、事故が起こる前提で万が一の被害を考慮する必要性を認識できていることが伺える。
- 米/星の保険加入理由3位にある通り、保険加入は社外ステークホルダーへのアピールにも利用できることを日本企業は意識したい。
- また、経済産業省がサイバーセキュリティ経営ガイドラインver.2.0で保険加入をリスク移転の1つの手段として推奨しているように、日本企業はリスクコントロールの1つの手段として保険加入を検討するべきである。

参考ガイドライン

あてはまるものすべて選択



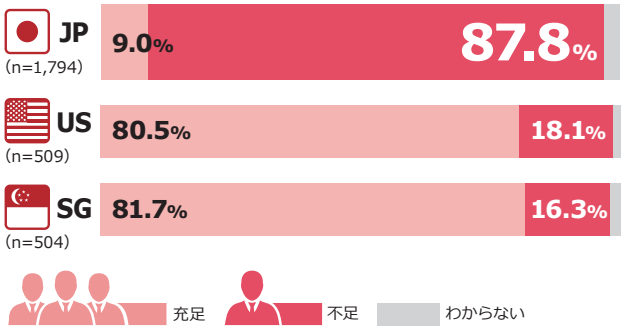
※「サイバーセキュリティ経営ガイドライン」は日本の経済産業省が発行するガイドラインのため、日本のみ選択肢に追加

- 米/星は30%程度、あるいはそれ以上の企業で各種セキュリティガイドラインを参考にしている。米国では、業界特有の規制に関するガイドラインも参考にしている。
- 日本はISOおよびサイバーセキュリティ経営ガイドラインが多く参照されている一方、ガイドラインを利用していないという企業が約30%と一番多かった。
- 技術寄り、組織対策寄り、といったようにガイドラインにも特徴があるので、自社に合ったガイドラインを参考にしたい。また、ガイドラインは脅威動向を受けて内容が更新されるので、定期的に更新内容を確認することを推奨する。

日本だけが圧倒的に人材が不足している
根本的な解決には業務の「標準化」や「自動化」が必須

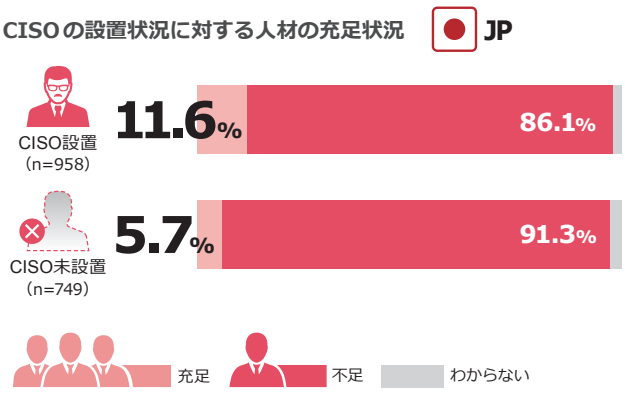
人材の充足状況

セキュリティ対策に従事する人材の充足状況



- 米/星の約80%が充足していると回答する一方で、日本は圧倒的な人材不足の状況にある。これは直近9年の弊社の調査結果でも同様であった。
- 日本の外部環境において、少子高齢化による労働人口の減少と新卒・キャリア採用の難易度が高まっている。企業がセキュリティ業務の継続性を維持するためには、人が対応する業務量を必要最小化することが望ましい。

CISOの設置状況に対する人材の充足状況



- 日本において、CISOを設置している企業は設置していない企業と比較して、人材が充足していると回答する割合が高かった。
- CISOに相当する組織の上位層が、人材不足を経営課題として認識し、課題解決に取り組むことが求められる。課題を解決するためには業務の再定義、既存ルールの変更、アウトソース活用への方針変更などの意思決定・合意形成を伴うため、CISO・経営層の関与が欠かせない。

充足していると考える理由

あてはまるもの最大3つ選択

「充足している」と回答した企業における、充足していると考える理由

	JP (n=161)	US (n=410)	SG (n=412)
1位	想定よりも有事対応が少ない	セキュリティ業務が標準化され、役割分担が明確	セキュリティ業務が自動化・省力化されている
2位	セキュリティ業務の量が少ない	想定よりも有事対応が少ないため	想定よりも有事対応が少ない
3位	セキュリティ業務が標準化され、役割分担が明確	経験豊富なメンバーで対応	セキュリティ業務が標準化され、役割分担が明確
4位	経験豊富なメンバーで対応	セキュリティ業務が自動化・省力化されている	セキュリティ業務の量が少ない
5位	セキュリティ業務を外部委託している	外部から経験豊富な人材を採用している	経験豊富なメンバーで対応

※ その他の選択肢：社内・グループ内の異動で人員を補充 / その他 / わからない

- 人材が充足していると回答した理由において、日本の1位・2位は「想定よりも有事対応が少ない」・「セキュリティ業務の量が少ない」という回答であった。安全・安心の観点からは望ましい回答であるも、有事が発生した際に適切な判断・対応ができるように平時から訓練を行うことが望ましい。
- 米では「セキュリティ業務が標準化され、役割分担が明確」、星では「セキュリティ業務が自動化・省力化されている」が1位となった。人材不足に悩む日本企業は、不足している人材を補充するだけでなく、より少ない人材でセキュリティ業務を継続的に回せるように、業務の量・プロセスの見直しやツール導入により、標準化・自動化を徹底することが求められる。
- セキュリティの現場が業務の標準化や自動化を進めたいと考えても、自社の慣習やポリシーに抵触することや、当初に見込んでいない予算が必要になる可能性もある。そのため、業務課題の理解や内部での議論・合意形成をCISOがリードするなど、リーダーシップの発揮が欠かせない。

セキュリティ業務を棚卸したうえで、人材を育成する、アウトソースする、など適切な選択をすることが望ましい

不足している人材の種別

あてはまるもの最大3つ選択

「不足している」と回答した企業における、不足していると考えるセキュリティ人材の種別

	JP (n=1,575)	US (n=92)	SG (n=82)
1位	セキュリティ戦略・企画を策定する人	ログを監視・分析する人	経営層に現状や対策内容等を説明する人
2位	セキュリティリスクを評価・監査する人	セキュアなシステム設計する人	セキュアなシステム設計する人
3位	ログを監視・分析する人	セキュリティリスクを評価・監査する人	ログを監視・分析する人
4位	インシデントへの対応・指揮をする人	関係部署と調整しつつ、対策を推進・統括する人	セキュリティリスクを評価・監査する人
5位	関係部署と調整しつつ、対策を推進・統括する人	経営層に現状や対策内容等を説明する人	セキュリティ戦略・企画を策定する人

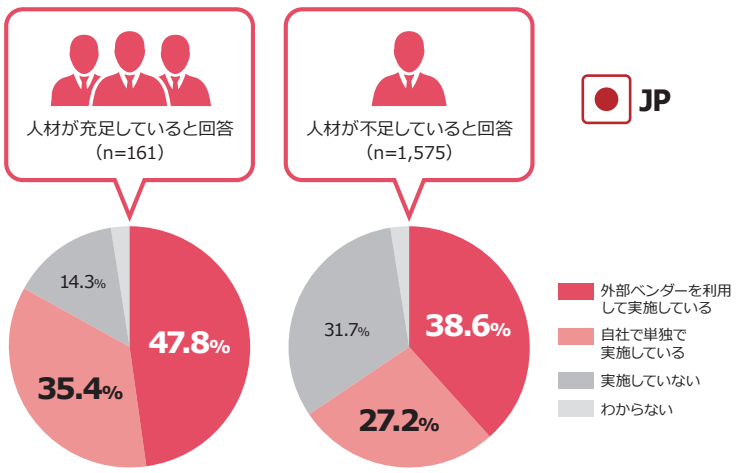
※ その他の選択肢：セキュアなプログラミングができる人 / 事業部門側のセキュリティ担当者 / その他 / わからない

- 各国のTOP3に「ログを監視・分析する人」が入っている。サイバー攻撃の高度化による脅威の高まりは世界的な課題であるため、セキュリティ監視人材の価値が高まっている。ログの監視・分析は高度な専門性を有するので、外部のSOCサービスなど、社外リソースの活用が有効な選択肢となる。
- 日本では「セキュリティ戦略・企画を策定する人」が不足人材の1位であった。セキュリティ戦略・企画の担当には、自社のビジネスを理解している社内人材を任命する。そして、戦略・企画の方向性を定めるためのセキュリティリスクの評価・監査（2位）においては、外部ベンダーの活用を選択肢にいれて検討することが望ましい。
- セキュリティ業務を最適化するべく、業務全体の棚卸し・見直しの実施を推奨する。各業務に必要なスキルを把握し、戦略的に経験やナレッジを社内に蓄積すべきかを判断し、各業務の内製化やソーシング戦略を決定する。加えて、現場の業務支援に資するツール導入を同時検討することも、効率化をもたらすために重要である。

セキュリティ業務のアウトソース状況

- 日本において、人材が充足している企業と不足している企業で、「セキュリティリスク評価・監査」業務のアウトソース状況を比較したところ、「充足」と回答した企業は「不足」と回答した企業よりも、外部ベンダーを利用して実施している割合が約10pt高く、セキュリティリスク評価を実施していない割合は約15pt低い。
- 企業がセキュリティ業務をアウトソースするのには、「人員の頭数の不足」、「人員のスキル不足」、「人員を育成するためのナレッジを得る」、「自社で実施するよりコストが安い」、「その分野の経験・スキルが自社には不要」、「第三者視点の中立的な意見・評価が必要」など、様々な理由がある。直近のセキュリティ業務の遂行を考慮するだけでなく、3年程度の中期的な視点でセキュリティの業務設計と人材育成を計画することが重要である。

人材の充足 / 不足に対するセキュリティリスク評価のアウトソース状況

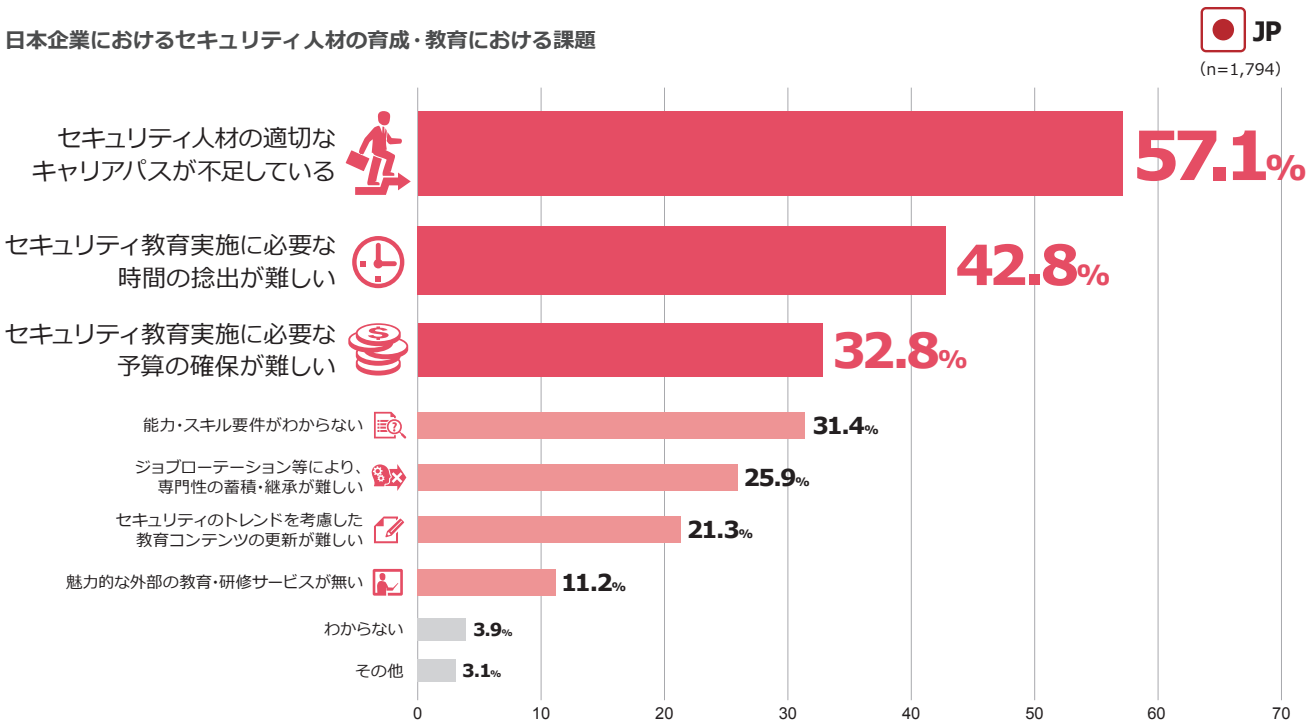


日本におけるセキュリティ人材育成のポイントは「キャリアパスの整備」と「必要なスキルの整理」

セキュリティ人材の育成・教育における課題

あてはまるもの最大3つ選択

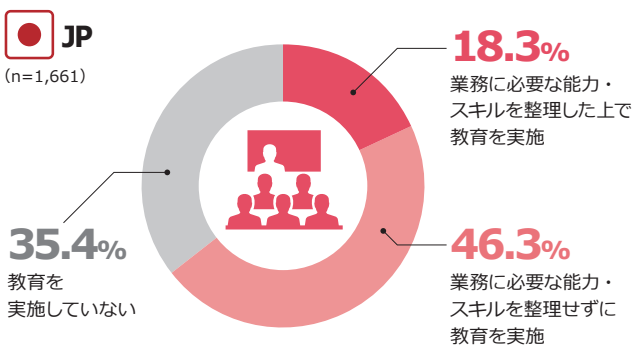
日本企業におけるセキュリティ人材の育成・教育における課題



- 「セキュリティ人材の適切なキャリアパスが不足している」という課題が上位なのは例年と同様であるが、昨今ではDXの更なる進展により、セキュリティ人材に求められる知識・技術分野が広がっているため、キャリアパス設計の難易度アップに拍車をかけていると考えられる。
- CISOに経営層が就任している企業は、セキュリティマネジメント人材のキャリアパスにおける象徴的な観点で優位性がある。
- キャリアパスの不足を感じる企業は、セキュリティ業務全体の棚卸し・見直しを行い、各業務の対応方針（内製化やアウトソースなど）を定める過程で、自社人材が担当する領域、習得するスキルやナレッジを定義することを推奨する。

セキュリティ人材の育成・教育の実施状況

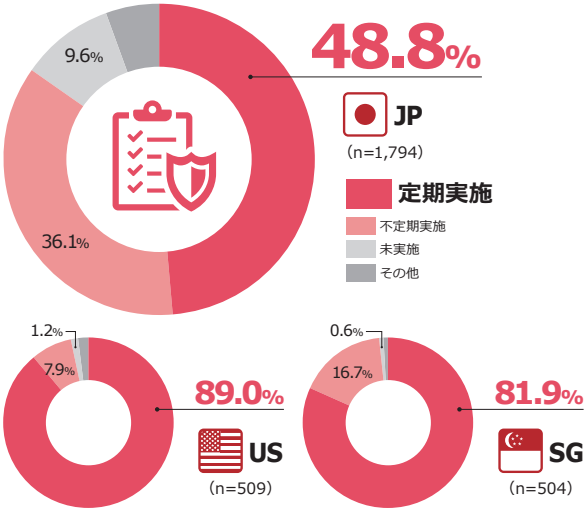
日本企業におけるセキュリティ人材育成の実施状況



- セキュリティ人材の育成を実施している日本企業は、60%以上であるが、業務に必要な能力・スキルを整理した上で実施している企業は、全体の20%に満たない。
- 育成における課題の上位であったリソース（時間・予算）不足を解消するためには、効率的・効果的な育成方法が求められる。そのためにも、自社の業務に求められる能力を整理し、その能力を習得するのに最適なカリキュラムを組むことが大切である。
- 求められる能力の整理が難しい場合は、社内におけるセキュリティ業務を整理した上で、社外の専門家に相談する等の対応を検討したい。

対策計画は策定後、適宜見直すことが重要
見直しのためには、定期的な評価を組織の慣習にすべき

セキュリティ対策評価の実施状況



- セキュリティ対策評価を定期的に実施する企業の割合は、米が約90%、星が約80%である一方、日本は50%に満たない結果となった。海外ではリスク評価を徹底し、評価結果に応じた合理的・効率的な対策を重視する考え方が根付いていることが背景として考えられる。
- 人間ドックを定期的に受診することと同様に、セキュリティ対策評価も定期的な取り組みとして継続し、自社の現状や対策優先ポイントの把握・更新をし続けることが望ましい。

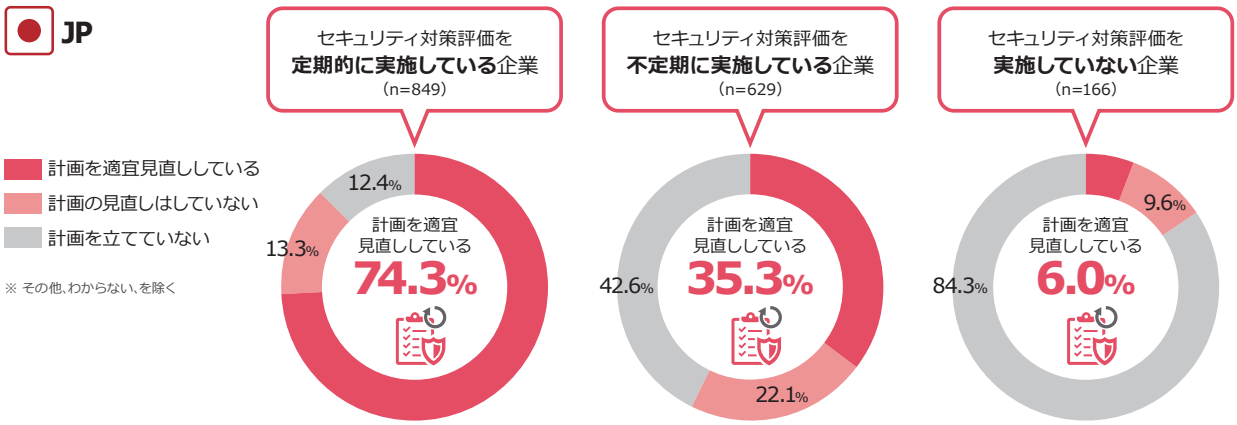
セキュリティ対策の計画スパンの差異

	計画策定していない	短期計画（1年程度）見直しはしていない	短期計画（1年程度）適宜見直ししている	中長期計画（3年程度）見直しはしていない	中長期計画（3年程度）適宜見直ししている
JP (n=1,794)	**29.8%**	9.6%	**30.4%**	5.7%	18.1%
US (n=509)	4.2%	2.2%	19.6%	14.3%	**56.2%**
SG (n=504)	6.0%	6.2%	16.5%	18.5%	**49.6%**

※ その他の選択肢：わからない / その他

- 日本は「短期的」、米/星は「中長期的」な視点で計画を策定している企業の割合が高かった。また、日本の「短期的」と「中長期的」合わせた計画の見直し率は約50%という結果となった。
- 効果的、かつ実現性の高いセキュリティ対策推進のためには、自社の現状や世の中の動向を踏まえ、目指すべきレベルや対策実行計画を適宜見直すことが大切である。

「対策評価の実施状況」と「対策計画の見直し実施率」の関連性



- セキュリティ対策評価を定期的に実施している企業の約75%は、セキュリティ対策の実行計画を適宜見直ししている結果となった。計画の見直しを行うために、あるいは計画の見直しとセットで現状の評価・把握を実施している企業が多いと考えられる。
- セキュリティ対策評価を実施していない企業の約85%は、実行計画も策定していないという結果となった。まずは一度セキュリティ対策評価を実施し、自社の現状や課題を正確に把握した後、セキュリティ対策のトレンドやベストプラクティスを踏まえ、自社に適した実行計画を策定することが望ましい。

日本は経営層のリーダーシップ発揮により、対策の遅れを挽回することが重要

情報セキュリティ対策実施のきっかけや理由

あてはまるもの最大3つ選択

	JP (n=1,794)	US (n=509)	SG (n=504)
1位	自社でのセキュリティインシデント 33.6%	経営層のトップダウン指示 55.4%	経営層のトップダウン指示 66.1%
2位	他社でのセキュリティインシデント 27.1%	他社でのセキュリティインシデント 25.0%	他社でのセキュリティインシデント 27.8%
3位	内部監査・内部有識者からの指摘 27.0%	自社でのセキュリティインシデント 23.4%	外部監査・第三者評価の結果 22.4%

※ 他選択肢:株主や取引先からの要請 / 関連法規の改定 / 監督省庁からのセキュリティ対策の要請

- 米/星の1位は共通して「経営層のトップダウン指示」であり、経営層がリーダーシップを発揮し、セキュリティ対策を実施する企業の割合が高かった。なお、日本の「経営層のトップダウン指示」の割合は23.7%で4位であった。
- 日本の1位は「自社でのセキュリティインシデント」で、発見した事象に対する事後的な対応である。日本企業のセキュリティ対策実施の位置づけは依然「コスト」であり、インシデントが発生したことでようやく経営層が対策の必要性を認識したといったケースが多いのではないかと考えられる。
- なお、各国共に2位は共通して「他社でのセキュリティインシデント」であった。対策のきっかけとなる外的要因として、他社のセキュリティインシデントが最も影響を与えていることがわかる。

情報セキュリティ担当者として、最も対応に困っていること

あてはまるもの最大3つ選択

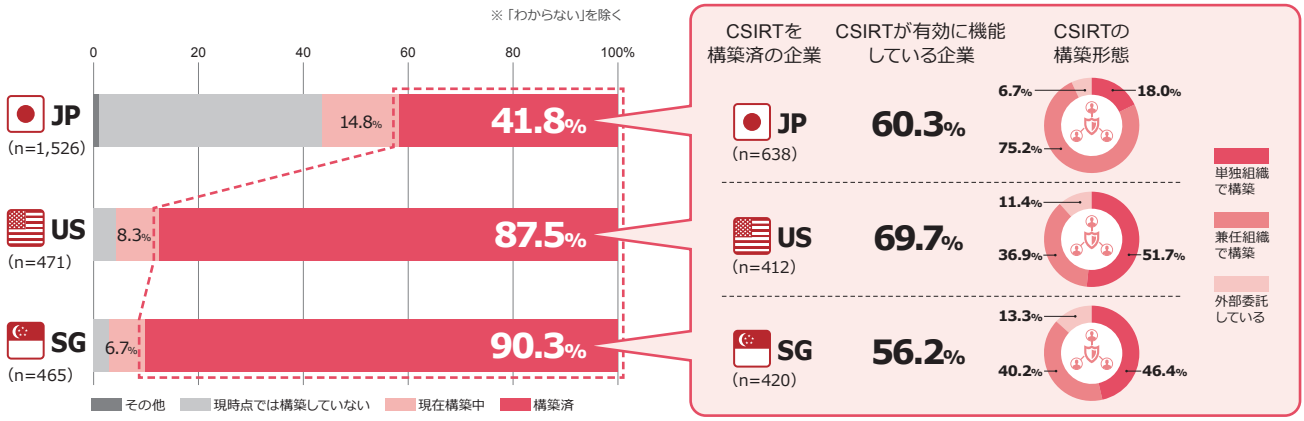
	JP (n=1,794)	US (n=509)	SG (n=504)
1位	自社セキュリティ対策の遅れ(最新技術・動向の未反映) 42.2%	セキュリティ対策のトレンド・他社動向の把握 38.3%	セキュリティ対策のトレンド・他社動向の把握 39.9%
2位	セキュリティインシデント発生時の緊急対応 41.9%	セキュリティ脅威・事故に関する情報収集と関係者共有 30.6%	セキュリティ脅威・事故に関する情報収集と関係者共有 36.3%
3位	サイバー攻撃の高度化への対応 38.7%	サイバー攻撃の高度化への対応 27.3%	セキュリティインシデント発生時の緊急対応 32.5%

※ 他選択肢:セキュリティ業務の状況・進捗に関する経営層への報告 / 国際的なイベント開催に伴うサイバー攻撃の増加 / グループ会社・国内外拠点のセキュリティ統制・管理 / 困っていることはない

- 日本は、自社セキュリティ対策の遅れが1位となった。予算配分や投資判断において経営層のリーダーシップが発揮されない場合、対策の計画・推進が円滑に進まず、セキュリティ担当者が日々の業務遂行で手一杯になってしまうことが考えられる。
- 米/星は、セキュリティのトレンドや他社動向、事故事例等の情報収集と関係者共有が上位となった。米/星では自社のセキュリティ対策を検討するにあたり経営層へのインプットとしてこれらの情報を必要としていると考えられるが、膨大にある情報の中から自社に適用すべき情報を選択・抽出することの難しさが伺える。
- 日本企業の困りごとは対策の遅れやインシデント対応といった目先の対応に起因することが目立った一方、米/星企業の困りごとは最新情報の収集や周知といった先を見据えた対応に起因することが多く、常に新しい環境に適応しようとする姿勢が見受けられる。

日本のCSIRT構築率は約40%であり、米/星の約90%と比べると大きく遅れている

CSIRTの構築状況



- 日本企業のCSIRT構築率は約40%であり、米/星の約90%と比べると低い結果となった。一方、CSIRT構築済企業のうち、CSIRTが有効に機能していると回答した企業の割合は、CSIRT構築率と比較すると3ヶ国間の差が少なかった。
- 各国共にCSIRTが有効に機能している割合が約60%に留まっているのは、CSIRTを構築することが目的となっており、本質的に必要な手順整備やセキュリティ対策機器導入が後回しになっている可能性が考えられる。枠組みとしてのCSIRTを構築するだけでなく、実務目線での支援が有効性を高める。実務をフォローするセキュリティ対策(SOAR)の導入やCSIRT構成員の訓練が必要である。
- CSIRT構築済企業の構築形態を見てみると、日本企業は兼任組織が中心、米企業は専任組織が中心、星企業は専任・兼任組織の割合がほぼ同じであった。兼任組織はインシデントの際に組織横断的なコミュニケーションが取りやすい一方、指揮系統があいまいになりやすい。兼任組織が中心の日本においては、緊急時に適切な指示系統で動けるようCISOを巻き込んだ訓練を平時から実施しておくことが重要である。
- 外部委託も含め、CSIRTの構築形態に正解はなく、組織文化やリソースを踏まえて自社に適した形態で構築することが望ましい。重要なのは、CSIRTの果たすべき役割の明確化や、適切な権限付与により、有効に運用できるCSIRTを組織することである。

CSIRT運営に関する課題

あてはまるもの最大3つ選択

	JP (n=1,794)	US (n=509)	SG (n=504)
1位	運営人員数の不足 44.3%	運営人員のスキル不足 27.7%	運営人員のスキル不足 34.3%
2位	運営人員のスキル不足 39.1%	運営人員数の不足 22.4%	運営人員のモチベーション維持 27.8%
3位	運営予算の不足 18.5%	運営人員のモチベーション維持 20.6%	運営人員の労務環境 21.4%

※ 他選択肢：運営人員数の過剰 / 経営層への報告方法・頻度の整理 / 脆弱性情報の収集・判断方法の整理 / 既存のシステム障害対応手順との整合性確保 / 既存の社内組織との役割分担の整理 / インシデント発生時の社外対応 / インシデントの影響度判断・対応方法の整理 / 監視体制(SOC等)との連携 / 内製する機能と外部委託する機能の整理 / 取り扱う脅威・リスクの整理 / 課題はない

- 日本は人材・スキル・予算の3つの不足が上位となった。CSIRT運用は高度かつ対応範囲が多岐にわたるため、自前のリソースのみでCSIRTを運営する方向から転換し、「自社で主体的に実施する業務」と「アウトソースする業務」を明確に選別することが望ましい。
- 米/星も日本同様にスキル不足が課題となっている一方、モチベーション維持や労務環境など、業務環境に関する課題が上位だった。CSIRTは有事の際には有効性が認められるが、平時の際には必要性が経営層から理解されにくい。そのため、自身の評価が適切でないと感じることが、モチベーションの維持を難しくしている要因の一つである可能性がある。その際、評価や処遇の改善にばかり目が向きがちだが、CSIRT業務の遂行環境において、自動化によるストレス軽減や繰り返し業務からの脱却など、省力化や効率化によって、より生産的かつ健全な環境作りを経営層が理解・支援することも、CSIRT要員のES・ロイヤリティ向上に必要である。

デジタル化が進む米/星では「サイバー攻撃」、日本では「ヒューマンエラー」によるセキュリティインシデントが上位

過去１年で発生した事件・事故

あてはまるものすべて選択

	JP (n=1,794) 82.9%	US (n=509) 83.7%	SG (n=504) 86.5%
1位	電子メール、FAX、郵便物等の誤送信・誤配送	DoS攻撃／DDoS攻撃	DoS攻撃／DDoS攻撃
2位	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	Webアプリケーションの脆弱性を突いた攻撃	Webアプリケーションの脆弱性を突いた攻撃
3位	マルウェア感染	システム基盤の脆弱性を突いた攻撃	自社サービスへのリスト型アカウントハッキング
4位	システム設定ミス、誤操作	自社サービスへのリスト型アカウントハッキング	標的型メール攻撃
5位	標的型メール攻撃	マルウェア感染	システム基盤の脆弱性を突いた攻撃
6位	社員証、業務書類等物品の紛失・置き忘れ・棄損	標的型メール攻撃	マルウェア感染
7位	情報機器、電子記憶媒体、紙媒体等の盗難・紛失	水飲み場型攻撃	水飲み場型攻撃
8位	ランサムウェア	ランサムウェア	情報機器・外部記憶媒体の紛失・置き忘れ・棄損
9位	その他	電子メール、FAX、郵便物等の誤送信・誤配送	ランサムウェア
10位	DoS攻撃／DDoS攻撃	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	システム管理者等による不正アクセスや持出

ヒューマンエラー　サイバー攻撃　過去一年で事件・事故が発生した企業の割合

- 各国の約80%の企業で、過去一年間にセキュリティの事件・事故が発生しており、引き続き、企業には事故発生を前提とした継続的なセキュリティ対策の推進が求められる。日本は例年と変わらず、メールの誤送信や紛失・置き忘れ等のヒューマンエラーが上位を占めている。
- ヒューマンエラーによるセキュリティインシデントを個人の責任とせず、ヒューマンエラーは起こる前提として捉え、組織としてどのように、抑制・防止・予防・検知・回復の観点で対策するかが重要である。そのためには、メール一本足になりがちなコミュニケーションツールをチャットにシフトする、FAXや郵便を電子ファイル交換サービスへシフトするなど、いわゆるDX1.0の意識的な推進も有効な選択肢となる。
- 一方、米/星の企業では「DoS攻撃/DDoS攻撃」や「Webアプリケーションへの脆弱性を突いた攻撃」といったサイバー攻撃によるセキュリティインシデントが上位に挙がった。日本企業より、クラウドサービスの活用やデジタル化(DX)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が考えられる。
- 米/星の企業では、メールの誤送信や紛失・置き忘れ等のヒューマンエラーを日本のように厳密にセキュリティインシデントとしてカウントしていない可能性も考えられる。また、性悪説・性弱説の考え方を踏まえて、ヒューマンエラーが発生しない/しにくい仕組み・プロセスを選択していることが伺える。

標的型攻撃による情報漏洩が各国共に最たる脅威である
加えて日本は「社内からの脅威」を上位にあげた

自社で最も脅威となる事象

あてはまるものを最大3つ選択

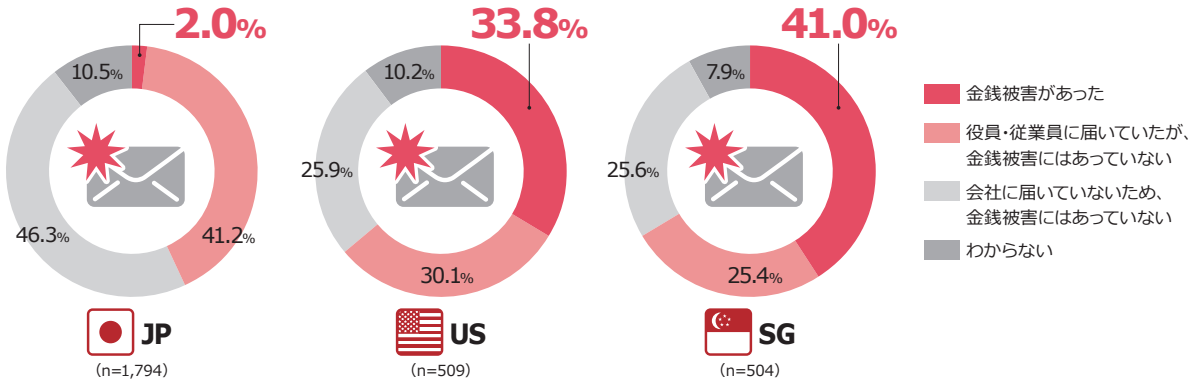
	JP (n=1,794)	US (n=509)	SG (n=504)
標的型攻撃による情報漏洩	1位 55.5%	1位 35.6%	1位 38.7%
内部不正による被害（情報漏洩、業務停止）	2位 51.7%	8位 12.2%	5位 18.5%
ランサムウェアによる被害（情報消失、金銭被害）	3位 47.9%	3位 30.3%	4位 33.7%
メールの誤送信・誤配信	4位 28.3%	9位 10.2%	8位 10.7%
情報機器・社員証等の置き忘れ、棄損による情報漏洩	5位 21.7%	6位 12.6%	9位 9.5%
退職者・転職者による在職時に利用していた情報の使用	6位 20.7%	7位 12.4%	7位 14.7%
ビジネスメール詐欺（BEC）による金銭被害	7位 15.5%	4位 23.6%	2位 37.1%
サービス妨害攻撃（DDoS攻撃等）によるサービス停止	8位 14.9%	2位 32.8%	3位 35.7%
自社Webサービスへのリスト型アカウントハッキング	9位 12.3%	5位 19.4%	6位 17.1%

※ 回答選択肢「その他」「わからない」を除く

- 自社において最も脅威となる事象は、各国共に「標的型攻撃による情報漏洩」が1位となった。また、2017年に各種メディアで大きく採り上げられた「ランサムウェアによる被害」は、日/米では3位、星では4位となり、依然として各国の企業の脅威となっている。
- 日本の特徴は、2位が「内部不正による被害」である点にある。社会において、情報漏洩が最もインパクトの強いインシデントと捉えられていることが背景にあると考えられる。サイバー攻撃ほどの発生件数はないが、内部不正は顕在化すると、漏洩件数が大きく、さらに企業にとって機密性が高い情報が漏洩するケースが多い。
- また、日本では2位の「内部不正による被害」や4位の「メールの誤送信」といった組織内の従業員・関係者に起因する、いわゆる社内発の脅威が高い順位となったのも特徴的だと言える。システム管理やメール送受信は、日々の業務遂行に欠かせない内容であることから、脅威の顕在化を予防・牽制すべく、メール誤送信防止の仕組み、管理者の特権IDに対する統制やモニタリングなどを業務プロセスに組み込むことが望ましい。
- 一方、米/星の特徴は、日本では順位が低かった「ビジネスメール詐欺（BEC）による金銭被害」や「サービス妨害攻撃（DDoS攻撃等）によるサービス停止」が上位となったことが挙げられる。

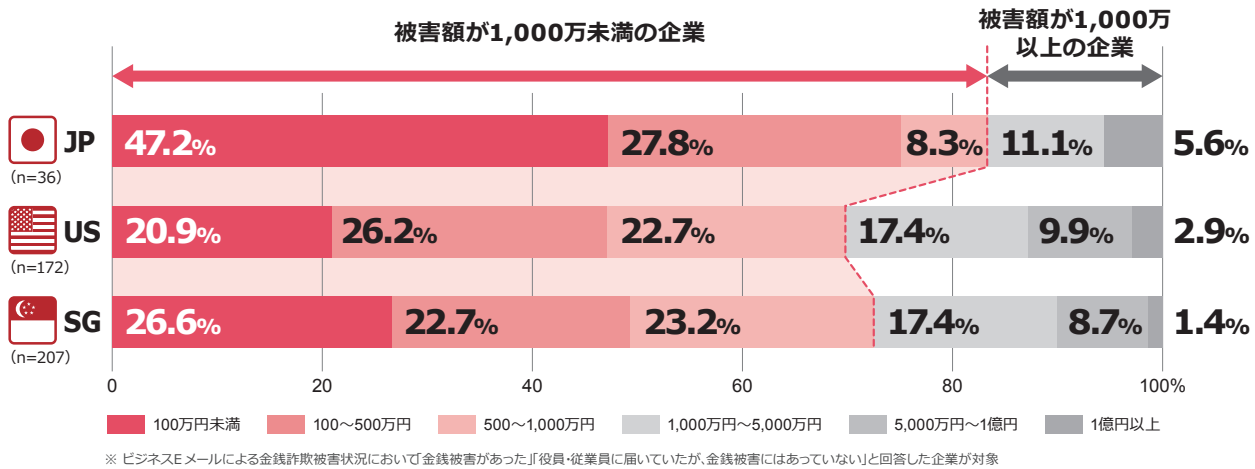
米/星ではビジネスメールによる金銭詐欺被害が多く発生
日本は極少であるが、充分注意し対策していく必要あり

ビジネスEメールによる金銭詐欺被害状況



- 米/星の企業は、ビジネスメール詐欺で被害が発生した割合が30～40%である一方、日本企業では、被害が発生した企業はわずか2%という結果で、大きな差が生じた。その背景として、米/星は60%以上の企業に詐欺メールが届いているのに対して、日本企業には40%程度しか届いていない点が挙げられる。
- また米/星では、メールを受け取った企業の2社に1社が金銭被害にあっていて、攻撃成功率が日本と比較して高い。これは、詐欺メールは海外の攻撃者によるものが多く、文面が日本語の場合は不自然な表現になるケースが多いため、攻撃メールであることを見破りやすいからだと推察される。
- 日本企業は金銭被害にあった割合が少ないものの、近年では特に海外に子会社・関連会社を持つ日系グローバル企業において、メール盗聴から巧妙に取引先に犯人がなりすまし、偽の請求書を送りつけられて、金銭詐欺に遭った事例も報告されているため、充分注意をしていく必要がある。日本企業は、海外のグループ会社が利用しているメールサービスの種別に留意したい。クラウド型のメールサービスの場合は、認証の設定強化・見直しに然るべき配慮・対応を徹底することが望ましい。

ビジネスEメールによる金銭詐欺被害総額の割合



※ ビジネスEメールによる金銭詐欺被害状況において「金銭被害があった」「役員・従業員に届いていたが、金銭被害にはあっていない」と回答した企業が対象

- ビジネスメールによる金銭詐欺被害総額は、1,000万円以下が米/星では約70%、日本では約80%を占めていた。一方、1億円以上の金銭被害を受けている企業も数%ではあるが存在した。
- ビジネスメール詐欺は、ウイルスや危険なURLなどが含まれていないため、従来のウイルス対策やスパムメール対策等では防ぐことができない。そのため、メール盗聴によるなりすまし対策、入金処理を2重3重でチェックするなどの業務フロー整備、従業員の教育や訓練等を徹底し、大きな被害が発生する前に水際で食い止めることが求められる。

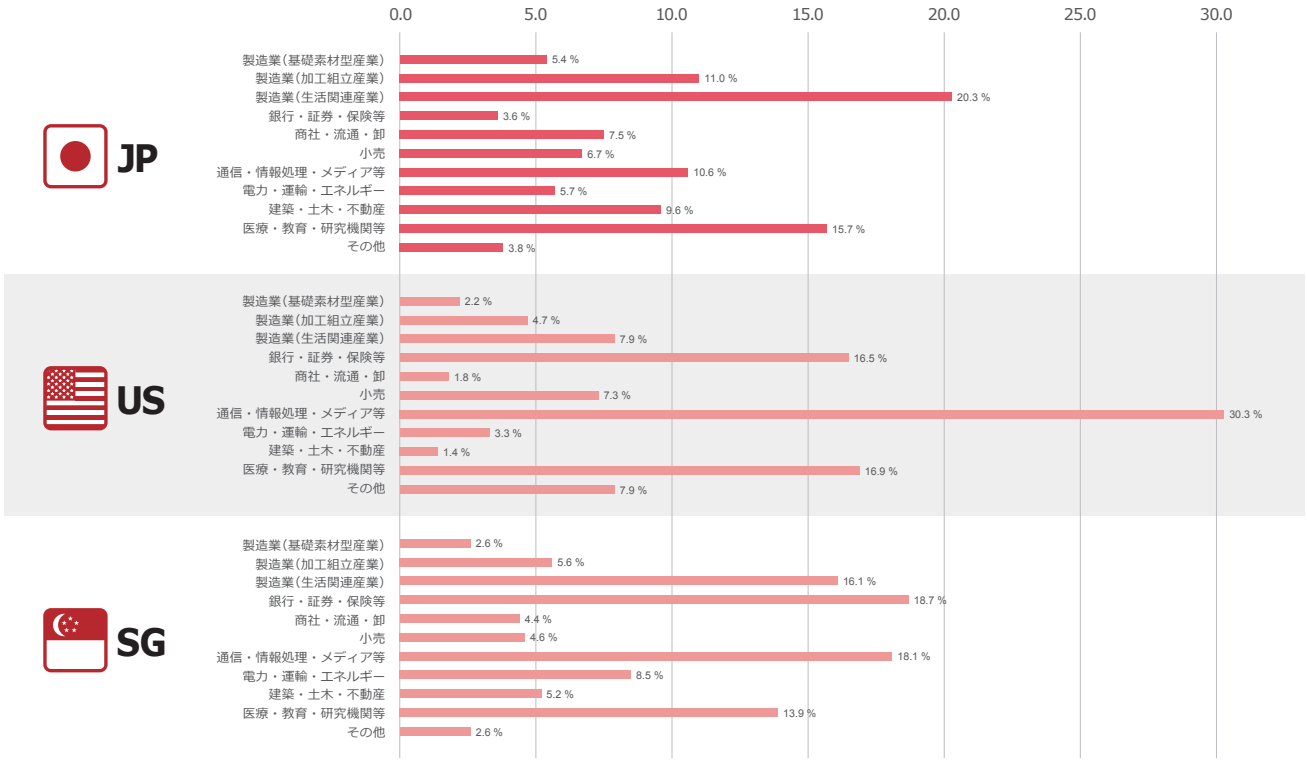
回答者属性

回答企業社数：合計 2,807社（JP 1,794社、US 509社、SG 504社）
日本企業向けのアンケートにおける調査対象企業の業種・従業員数は外部の企業情報データベースから取得

回答いただいた企業の業種・所属部署

■ 業 種

貴社の業種をお教えください。以下の中から当てはまるものを１つお選びください。



※ 回答企業の業種を以下のように分類

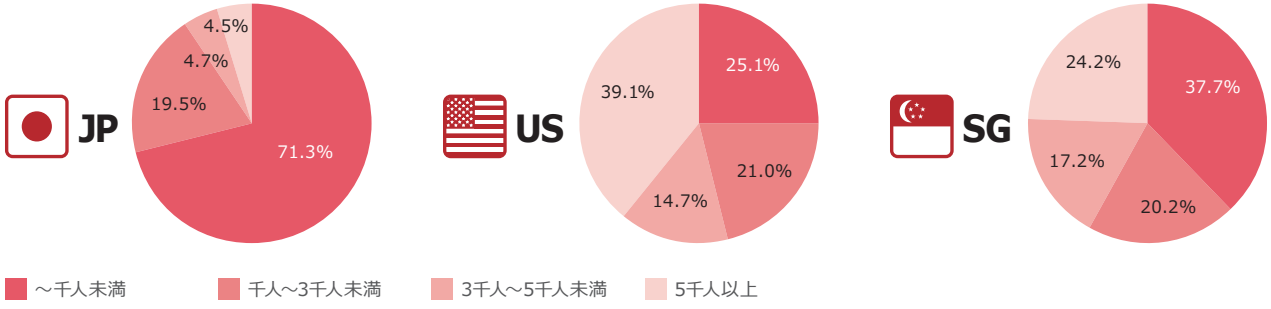
- ■ 製造業（基礎素材型産業）：紙・パルプ、化学、鉄鋼・金属
- ■ 製造業（加工組立産業）：機械・精密機器、電気機器、自動車製造業
- ■ 製造業（生活関連産業）：食品、繊維・アパレル、医薬、その他の製造業
- ■ 銀行・証券・保険等：銀行、証券、保険、その他金融
- ■ 通信・情報処理・メディア等：コンサルティング・シンクタンク、マスコミ・出版・印刷・広告、情報処理・ソフトウェア・SI、ISP・CATV・x DSL事業、通信・放送
- ■ 電力・運輸・エネルギー：電力、石油・ガス、鉄道・航空、運輸
- ■ 建設・土木・不動産：建設・土木・不動産、農林水産漁業・鉱業
- ■ 医療・教育・研究機関等：医療、福祉、教育・研究機関、その他のサービス業

■ 所属部署

調査対象国全てにおいて、回答者の主な所属部署は情報システム部、情報セキュリティ部等のIT 業務に携わる部署であった

回答いただいた企業の従業員数

貴社の従業員数はいかがですか。以下の中から当てはまるものを１つお選びください。



Survey method

調査方法

調査方法

日本、アメリカ、シンガポール： Web によるアンケート

調査対象

日本、アメリカ、シンガポール： 企業の情報システム・情報セキュリティ担当者

調査期間

日本 ： 2019/1/15 ~ 2019/2/28

アメリカ、シンガポール： 2018/12/3 ~ 2018/12/14

注：

- 「把握していない」「不明」という回答や無回答の除外、パーセンテージの切り上げ等により、全ての数字の合計値が100%にならない場合があります。

お問い合わせ先
info@nri-secure.co.jp

PROJECT MEMBER

制 作 委 員

制作	NRI Secure Insight 2019　制作委員会
企画	名部井 康博
執筆	川崎 聡太　神野 幸平　森 茉莉香 山田 智隆　山田 真暉
アドバイザー	観堂 剛太郎　菅谷 光啓　佐藤 健 稲田 憲昭　山口 雅史　十川 基 宇佐見 彰浩　高見澤 涼　齋藤 大地 長谷川 ちひろ
監修	足立 道拡　渡部 惣

CORPORATE DATA

会社情報

会社名	ＮＲＩ セキュアテクノロジーズ株式会社
英語表記	NRI SecureTechnologies, Ltd.
本 社	〒100-0004 東京都千代田区大手町 1-7-2 東京サンケイビル TEL（代表）：03-6706-0500
北米支社	26 Executive Park Suite 150 Irvine CA 92614 U.S.A. TEL：+1-949-537-2957
代表取締役社長	小田島 潤
設 立	2000 年 8 月 1 日
資本金	4.5 億円
株 主	株式会社野村総合研究所
社員数	479 名

（2019 年 4 月 1 日現在）

NRIセキュアテクノロジーズについて

NRIセキュアテクノロジーズは
情報セキュリティ実態調査を
17年に渡り実施しています

17年間の調査を通じ、のべ
12,577社の回答
をいただきました

評価・実績

日本　業界のパイオニアであり トップベンダーとして様々な実績・評価

マーケットシェア No.1

- 特権ID管理市場*1
  （SecureCube / Access Check、Cloud Auditor by Access Check）
- IDM／IAM市場*1（Uni-ID Libra）
- ユーザー間ファイル転送市場*2（クリプト便）
- サイバーセキュリティコンサルティングサービス市場*3
  - セキュリティコンサルティング・プランニングサービス市場
  - セキュリティ脆弱性診断・検査サービス市場
  - CSMS／PSIRT／IoTセキュリティ構築運用支援サービス市場
  - CSIRT構築運用支援サービス市場
  - 標的型攻撃メール訓練サービス市場
  - セキュリティ監査サービス市場
  - セキュリティ情報配信サービス市場
  - SOC構築運用支援サービス市場

＊1 ITR「ITR Market View：アイデンティティ／アクセス管理市場 2018」2017 年度ベンダー別売上金額（2018 年 11 月発行）/ ＊2 ITR「ITR Market View：ファイル共有・転送市場 2017」2016 年度ベンダー別売上金額（2017 年 9 月発行）/ ＊3 ITR「ITR Market View：サイバー・セキュリティ・コンサルティング・サービス市場 2018」2017 年度ベンダー別売上金額（2018 年 6 月発行）

情報セキュリティ格付8年連続最高ランク

- クリプト便：情報セキュリティ格付最高ランクを2011年より8年連続獲得（格付機関：株式会社アイ・エス・レーティング）

Frost & Sullivan

- ジャパンマネージドセキュリティサービス プロバイダーオブザイヤー2年連続受賞（2017年、2018年）

グローバル　グローバル市場においても実績を重ね、Gartner、Forresterの資料に掲載

Gartner

- 「Magic Quadrant：特権アクセス管理」*4
- 「Market Guide：デジタルフォレンジック調査／インシデントレスポンス」*5

＊4 Gartner “Magic Quadrant for Privileged Access Management” Felix Gaehtgens et al.（03Dec2018）/ ＊5 Gartner “Market Guide for Digital Forensics and Incident Response Services” Brian Reed & Toby Bussa（04Dec2018）（ガートナー免責事項）ガートナーは、ガートナー・リサーチの見解を表したものであり、事実を表現したものではありません。ガートナーは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の保証を行うものではありません。）

Forrester

- 「Vendor Landscape：グローバル マネージドセキュリティサービス」*6
- 「The Forrester Wave™：エマージング マネージドセキュリティサービス プロバイダー」*7
- 「Now Tech：アジアパシフィックマネージドセキュリティサービス」*8

＊6 Forrester “Vendor Landscape : Global Managed Security Services, 2017” / ＊7 Forrester “The Forrester Wave™ : Emerging Managed Security Services Providers (MSSPs), Q3 2018” / ＊8 Forrester “Now Tech : Managed Security Services in Asia Pacific, Q1 2019, Forrester Overview of 19 Managed Security Service Providers”

資格取得者数（社員数：479名）

88名 **CISA**（公認情報システム監査人）	52名 **CISM**（公認情報セキュリティマネージャー）
45名 **CISSP**（情報システム・セキュリティ・プロフェッショナル認定資格）	193名 **GIAC**（Global Information Assurance Certification）

*2019/4/1 時点

NRI SECURE

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル
https://www.nri-secure.co.jp