NRI Secure Insight 2020

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 2020

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 17 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、18 年目の今年は日本、アメリカ、オーストラリア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。

- 本アンケート調査は、NRI セキュアテクノロジーズ株式会社が、企業や公的機関におけるセキュリティ対策の推進を支援することを目的として、自主的な活動として行っているものです。
- 本アンケート調査の生データは提供いたしかねます。
-
- 内容の一部を転載・引用される場合には、出所として弊社名および調査の名称「NRI Secure Insight 2020」を併記した上で、弊社までお知らせ下さい。 ・電子メール：info@nri-secure.co.jp
- 今回のアンケートにおける回答企業数 n は日本 1,222 社、アメリカ 523 社、オーストラリア 515 社、です。
- 以下の行為はご遠慮ください。
  ・データの一部または全部を改変すること ・本報告書を販売・出版すること ・出所を明記せずに転載・引用を行うこと

NRI SECURE

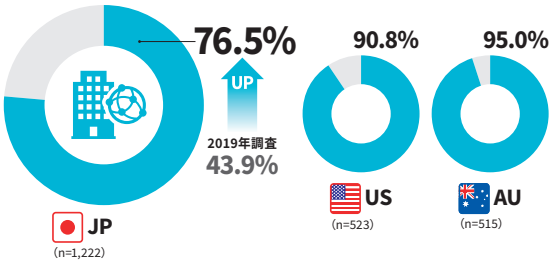
EXECUTIVE SUMMARY

※ 米：アメリカ、豪：オーストラリア
※ 特に明記していない限り、調査ベースは全回答者（日本 1,222 社、アメリカ 523 社、オーストラリア 515 社）

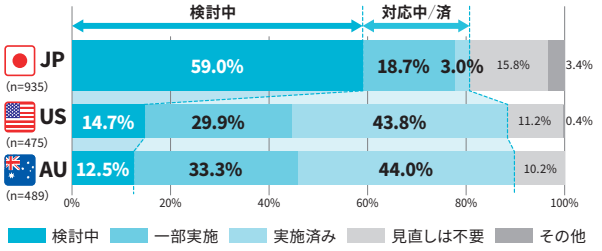
デジタルトランスフォーメーション

- 日本は昨年と比べて DX に取り組んでいる企業が大幅に増加した
- 日本は米 / 豪と比較して DX に伴うセキュリティへの取り組みが遅れている

DX に取組んでいる企業



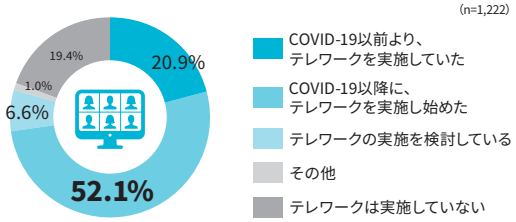
DX に伴うセキュリティ戦略の見直し状況



- 日本は約 50% の企業が COVID-19 以降にテレワークを実施し始めた
- テレワークの実施に伴い、セキュリティへの対応まで行った企業は半数強にとどまった

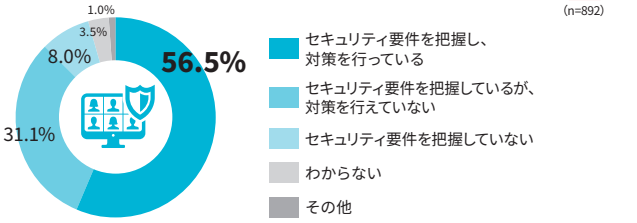
テレワークの実施状況

JP (n=1,222)



テレワーク実施に伴うセキュリティへの対応状況

JP (n=892)



セキュリティマネジメント

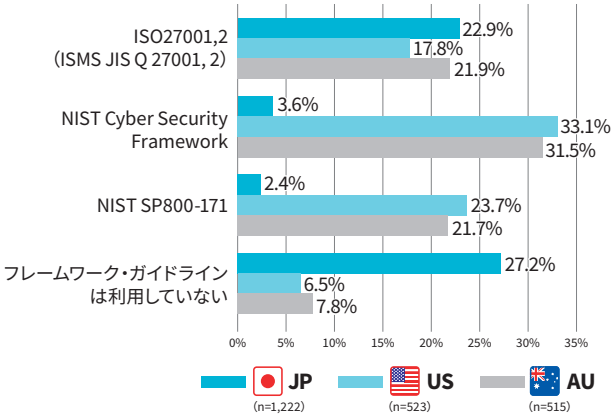
- 日本はセキュリティ関連予算を維持ないし増額する意向の企業が多い
- 日本は依然として ISO ベースのセキュリティ対策を選択する企業が多い

COVID-19 によるセキュリティ関連予算の昨年度比

	JP (n=1,059)	US (n=510)	AU (n=499)
1位	55.9% セキュリティ関連予算に変化はない	27.3% COVID-19 とは関係なく、セキュリティ関連予算は減額した、または減額する見込み	37.5% COVID-19 によって、セキュリティ関連予算は増額した、または増額する見込み
2位	17.6%	26.7%	22.2% COVID-19 とは関係なく、セキュリティ関連予算は減額した、または減額する見込み
	COVID-19 によって、セキュリティ関連予算は増額した、または増額する見込み		
3位	14.0% COVID-19 とは関係なく、セキュリティ関連予算は増額した、または増額する見込み	22.7%	18.8%
		COVID-19 によって、セキュリティ関連予算は減額した、または減額する見込み	

増加　変化なし　減少

ガイドラインの活用状況



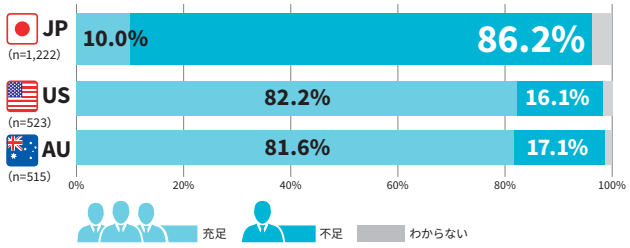
調査概要

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、オーストラリア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：2020/7/1 ～ 2020/9/18、アメリカ・オーストラリア：2020/8/1 ～ 2020/9/18
回答いただいた企業数	● 計 2,260 社（日本：1,222 社、アメリカ：523 社、オーストラリア：515 社）

セキュリティ人材

- 日本は米 / 豪と比較して圧倒的に人材不足を訴えている
- 日本では、セキュリティ戦略・企画をリードする人材が最も不足している

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

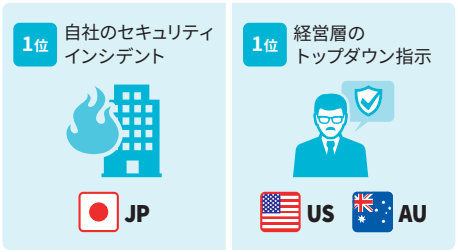
JP

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

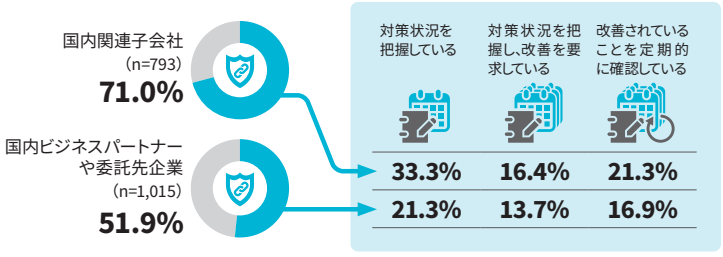
- 対策実施のきっかけ1位は、日本は自社のセキュリティインシデントであり、米 / 豪は経営層の指示であった
- 日本企業は国内関連子会社で7割強、国内委託先企業で5割強、セキュリティ対策状況を把握している

セキュリティ対策の実施のきっかけや理由



サプライチェーンに対するセキュリティ統制実施状況

JP



脅威・事故

- 2020 年は標的型メール攻撃などのサイバー攻撃による事件・事故の順位が上がった

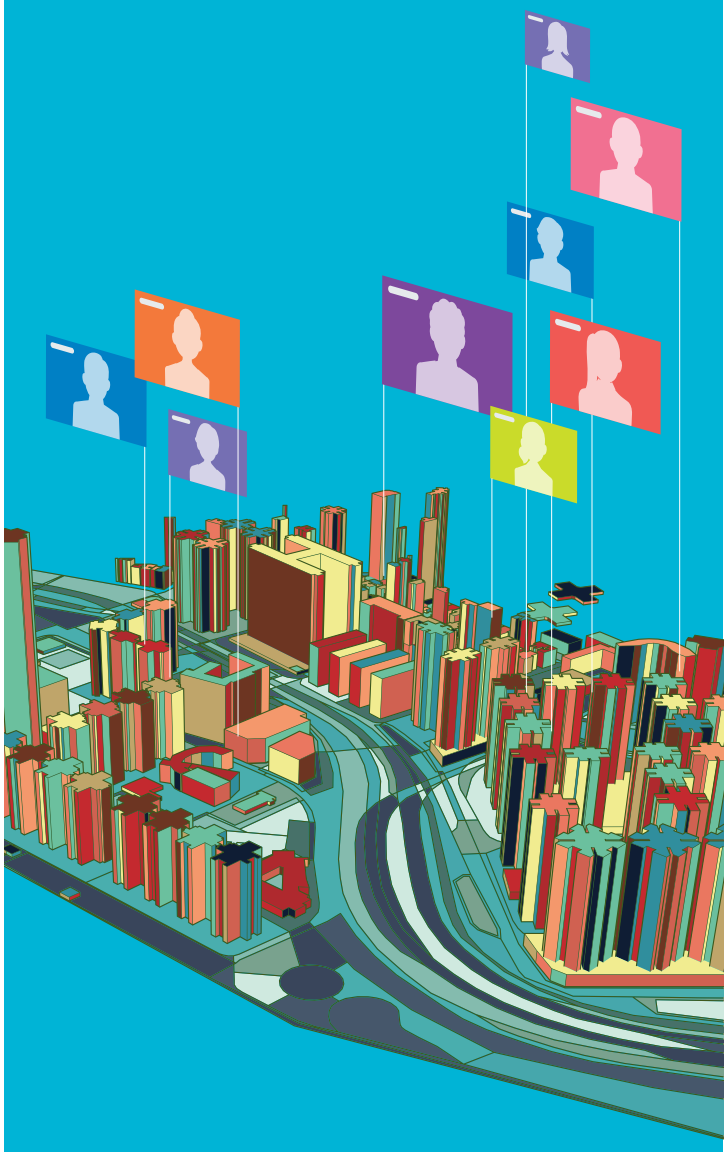
日本の過去 1 年で発生した事件・事故（昨年との比較）

JP

2019年 (n=1,794)		2020年 (n=1,222)	
1位	電子メール、FAX、郵便物等の誤送信・誤配送	1位	電子メール、FAX、郵便物等の誤送信・誤配送
2位	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	2位	標的型メール攻撃
3位	マルウェア感染	3位	マルウェア感染
4位	システム設定ミス、誤操作	4位	情報機器・外部記憶媒体の紛失・置き忘れ・棄損
5位	標的型メール攻撃	5位	システム設定ミス、誤操作

サイバー攻撃

CONTENTS



調査結果

CATEGORY

- デジタルトランスフォーメーション
- 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

デジタルトランスフォーメーション

直近1年で、DXに取り組んでいる日本企業の割合が急上昇
一方で、DXに伴うセキュリティ戦略の見直しは足踏みしている

DX に取組んでいる企業

JP (n=1,222) **76.5%** UP 2019年調査 43.9%

US (n=523) **90.8%**

AU (n=515) **95.0%**

解説 企業におけるDXな取り組みの3分類

タイプ1 IT視点	タイプ2 マーケティング視点	タイプ3 新規事業視点
CIO	CMO	CDO
デジタルを用いた業務の効率化	デジタルマーケティングの推進	デジタル活用で新しい収益基盤を創出

DX 取組み阻害要因

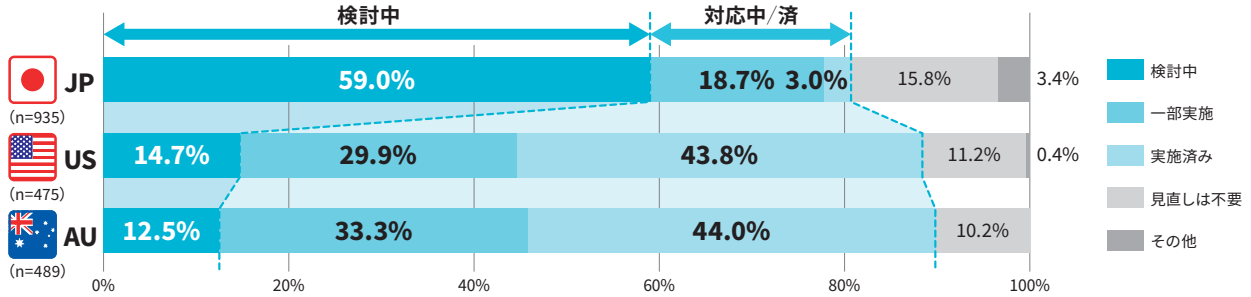
あてはまるものをすべて選択

	JP (n=935)	US (n=475)	AU (n=489)
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	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	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
2位	情報セキュリティへの対応	変化を受入れる企業風土がない	縦割りの組織構造
3位	変化を受入れる企業風土がない	情報セキュリティへの対応	情報セキュリティへの対応

- DX に取り組んでいると回答した企業が76.5%を占めるが、推進中の企業にもDX取組みの阻害要因が多数存在している。
- 各国共に「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」が1位であった。DX推進を牽引できるIT人材の価値が、グローバル規模で非常に高いことが分かる。
- 各国共に「情報セキュリティへの対応」が上位を占め、日/米では「変化を受入れる企業風土がない」が上位にランクインした。DX推進の現場では、現行のITやセキュリティポリシーをDXに即した形でアップデートすることの壁に直面している。

  企業内で、DXな新規事業を形にするためには、中長期視点での取り組みの継続が求められるが、既存事業で長年培われてきた評価指標の適用や四半期/半期での短期成果を重視する声に戸惑うケースも多い。
- 経営/IT戦略にDX推進を掲げる経営層やリーダーは、「DX人材育成に向けた積極的な投資」、「DXを促進するためのルールや評価指標のアップデートへの理解と支援」および「中長期的な成長・成果視点を持つこと」を改めて意識されたい。

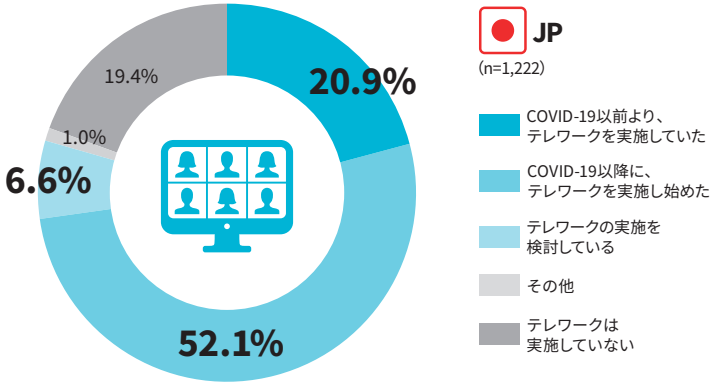
DX に伴うセキュリティ戦略の見直し状況



- 日本企業の約80%がDXに伴うセキュリティ戦略の見直しを進めており、本対応の必要性が幅広く認知されている一方で、約60%の企業は未だ検討中の段階にある。多くの日本企業において、セキュリティへの対応がDX推進のボトルネックになっている、もしくは、セキュリティ対策が不十分なままDXを進めている可能性がある。
- 検討中と回答する日本企業が多い背景として、DXを推進したくとも、オンプレミスを前提にした現行のITインフラ、境界防御を前提にした現行のセキュリティポリシーなどの制約により、見直しの影響範囲が甚大、かつ検討/対応を進めるための人材や予算が不足しており、何から手を付けて良いかわからないなどの理由が考えられる。
- DXに関するリソースやナレッジ不足という課題解決には、企業側の取り組みに加えて、企業のDXを促進する税制度優遇などの政府施策やDXに取り組む企業間の事例共有など、1企業の枠を超えた共助・公助のアクションが求められる。

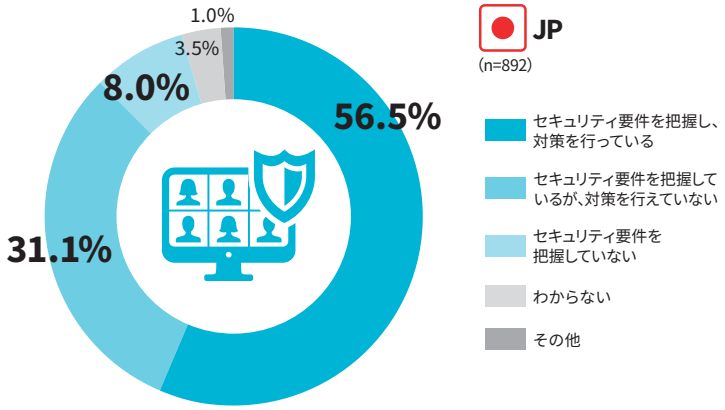
待ったなしのテレワーク緊急導入を暫定的なセキュリティ対応で進めざるを得なかった日本企業

テレワークの実施状況



- 日本において、約70%以上の企業がテレワークを実施していた。その内、COVID-19 以降にテレワークを実施し始めた割合が半数を超えている。
- COVID-19 をきっかけとして、日本企業におけるテレワーク実施率は急激に上昇したが、その一方で企業の情報システム、情報セキュリティ担当者は、テレワーク環境の急速な整備やユーザーサポートなどで、業務量が増加し、既存の業務や新規プロジェクトを延期 / 停止せざるを得ない状況であった。

テレワーク実施に伴うセキュリティへの対応状況



- ビジネス継続のため迅速なテレワークの導入を迫られ、セキュリティ対応が追い付いていない、もしくは暫定的なセキュリティ対応を取らざるを得なかった企業が多いと考えられる。
- 喫緊の対応として、リモート端末（ノート PC など）は社内ネットワークへの VPN 接続を前提とし、各端末に対して既存の境界防御型のセキュリティ対策を適用させている企業も多いと見られる。
- 2020 年 4 月の緊急事態宣言の前後で、VPN 機器や認証トークンのハードウェア調達ニーズが一気に高まり、必要数を迅速に調達できないことでテレワーク推進が計画通りに進まなかった企業も多い。VPN の管理負荷、変化への機敏な対応を考えると、ゼロトラストへのシフトも見据えたセキュリティ戦略を立てていくことが望ましい。

テレワークに関する参考情報

NRI セキュア・ブログ

【解説】テレワーク環境のリスク評価｜アーキテクチャ見直しの初めの一歩
https://www.nri-secure.co.jp/blog/consideration-of-telework-security-and-after-corona-security-architecture

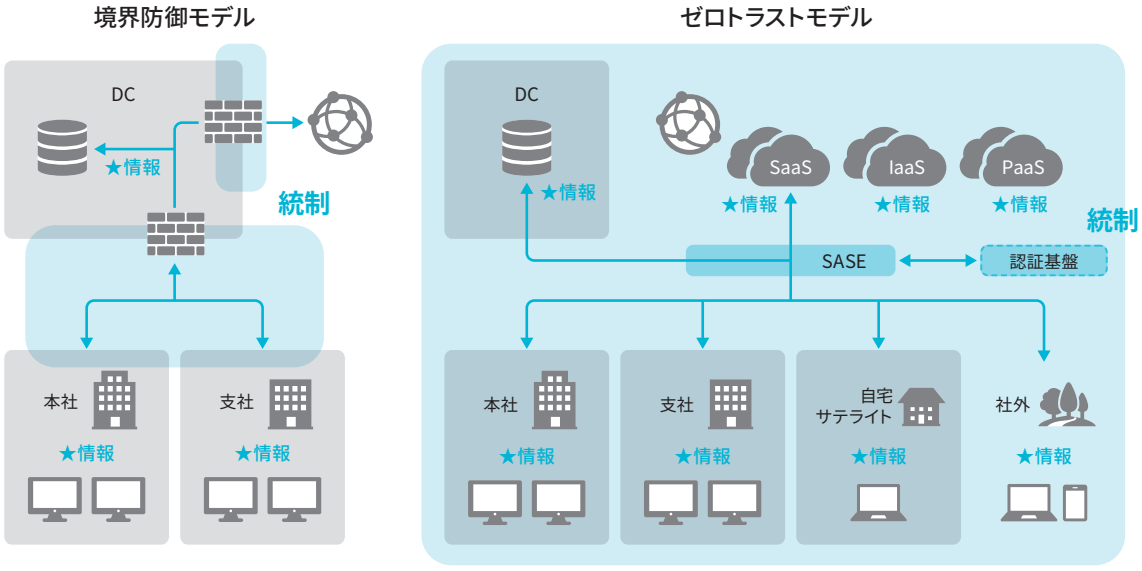
NRI セキュア・お知らせ

総務省「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）」公表のお知らせ
https://www.nri-secure.co.jp/news/2020/0916

解説

COVID-19で明確になった境界防御型モデルの限界とDX時代における理想的なセキュリティ対応のアプローチ

企業のDXを支えるセキュリティのニューノーマル：ゼロトラストモデル



- 従来の境界防御型のセキュリティモデルでは、情報資産は全て社内ネットワーク等の境界内に存在することを前提とし、その境界を出入りする通信に対して統制を効かせることで、セキュリティを担保してきた。しかし、ビジネス推進のためのクラウドサービス活用やワークスタイル変革のためのテレワーク対応など、企業のDXが進むにつれて、「情報資産は全て境界内に存在する」という前提が崩れ始めた。
- そこでゼロトラストモデルという考え方が登場した。ゼロトラストモデルでは、境界の内と外という考えに捉われず、常に全ての通信を必ず確認し、厳密なアクセス管理を徹底する。あらゆるサービス/情報/デバイス/人が連携する今後のDX時代において、ゼロトラストモデルは、セキュリティにおけるニューノーマルとなりうる考え方である。

ゼロトラストに関する参考情報

NRIセキュア・ブログ

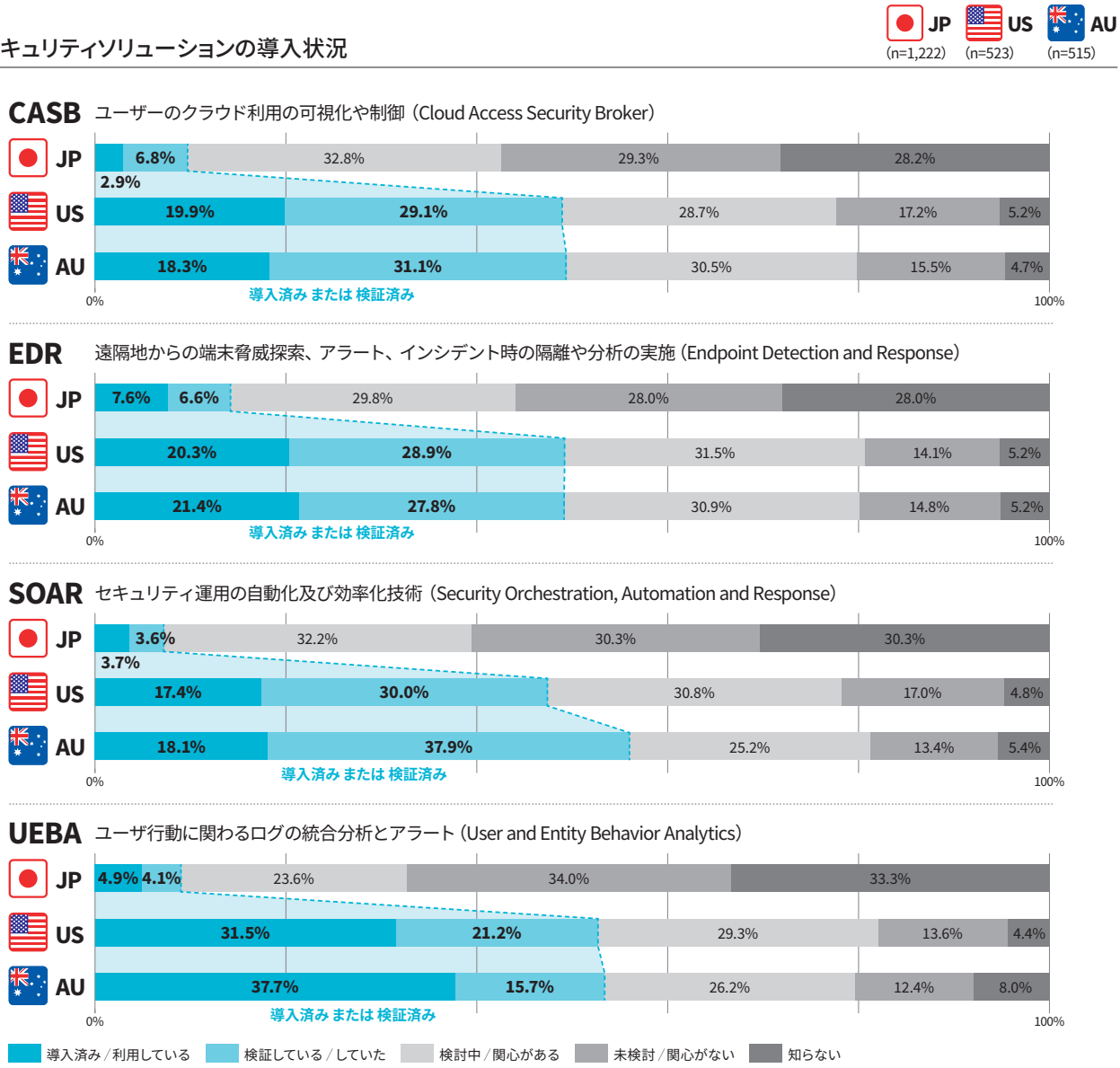
「ゼロトラスト」が働き方を変える～次世代のセキュリティモデル～
https://www.nri-secure.co.jp/blog/zero-trust-security-model

ゼロトラストネットワークアクセス（ZTNA）とは？「脱VPN」の最有力ソリューションを解説
https://www.nri-secure.co.jp/blog/explanation-of-zero-trust-network-access

ゼロトラスト入門｜テレワーク環境から始める新時代のセキュリティ対策
https://www.nri-secure.co.jp/blog/benefits-of-introducing-a-zero-trust-model-in-telework

DXやゼロトラストモデルを支えるセキュリティソリューション
日本企業における認知や浸透には更なる時間を要する状況

セキュリティソリューションの導入状況



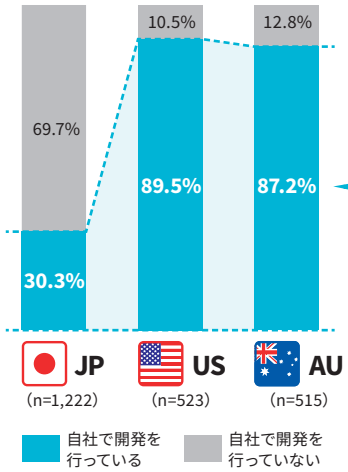
解説 セキュリティソリューションの略称と読み方

CASB （キャスビ）	EDR （イーディーアール）	SOAR （ソアー）	UEBA （ユーイービーエー）

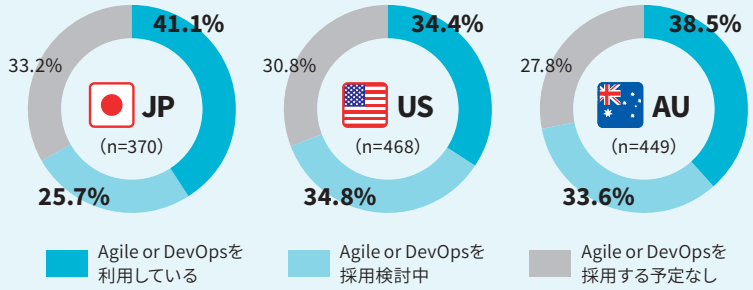
- クラウドサービスには様々なメリットがある一方で、企業内で未許可のクラウドサービス利用（シャドーIT）の把握や機密情報アップロードの制御、など業務利用する上で気を付けるべきポイントは多い。クラウドサービスを安全に運用するための1つの手段として、CASBの導入を検討したい。
- テレワーク環境においては、従業員が社外で利用するモバイルPCへのセキュリティ統制が課題となる。遠隔地の端末のセキュリティも担保できるEDRの導入も検討したい。
- ゼロトラストモデルにおいては、セキュリティ上の監視対象が増大するため、脅威情報の収集・検知・検知後の対応などを、積極的に効率化していくことが望ましい。新規事業の創発や既存プロセスの変革などのDX活動にリソースを投入するためにも、SOAR等のソリューション活用によって定型的なセキュリティ運用を可能な限り自動化することを検討したい。
- 複数のサービスを組み合わせて業務を行う状況下で不審な動きを早急に検知するために各サービスの利用状況をユーザ個々人やリソース1つ1つの振舞いで監視する手段として、UEBAの活用余地がある。

日本では自社開発がDX推進に与える影響が大きい
セキュアな開発をするための対策が求められる

3ヶ国の開発体制比較



3ヶ国の自社開発企業のAgile型開発またはDevOpsの採用状況

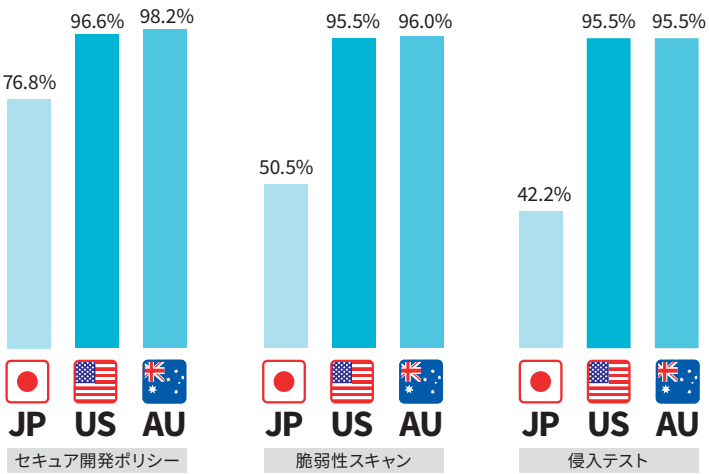


- 日本で自社開発を行っている企業は30%にとどまり、米 / 豪と比較して約60pt近く低い結果となった。対して、Agile型開発またはDevOpsの採用状況は41.1%と3ヶ国で最も高かった。
- 企業におけるDXの取り組みは、下記の3タイプに大別できるが

  タイプ1　デジタルを用いた業務の効率化（CIO視点）
  タイプ2　デジタルマーケティングの推進（CMO視点）
  タイプ3　デジタル活用で新しい収益基盤を生み出す（新規事業視点）

  タイプ1/2よりも、タイプ3の取り組みにおいて、自社開発を行い、Agile や DevOps を採用しているケースが多いことが考えられる。
  新規事業はその特性上、不確実性が高く、プロトタイプに対する顧客フィードバックから常に学び、迅速なアップデートや継続的な仮説検証を必要なことから、Agile や DevOps の特性との相性の良さが伺える。
- 日本で自社開発を行っていないという回答が多い背景としては、日本企業の多くは社内にIT/ 開発人材が少なく、SI ベンダーへの依存度が高い状況などが考えられる。DX成功の鍵は、ビジネスとDevSecOpsの関係性がより近く・深くなることにあるため、今後は日本においても、DXの進展に伴い、自社で開発を行う割合が高まっていくことが予想される。

自社開発をしている日本企業において他国と実施率の差が大きかったセキュリティ対策



- 開発に係わるセキュリティ対策として、日本は侵入テスト、脆弱性スキャンの実施率が米 / 豪よりも約40pt以上下回った。
- 今後、DXのさらなる推進のために、自社で開発を行う日本企業が増加すると予想される。DXをセキュリティが担保された状態で成功させるためには、セキュアな開発プロセスを標準化し、自社開発におけるセキュリティレベルを底上げすることが求められる。

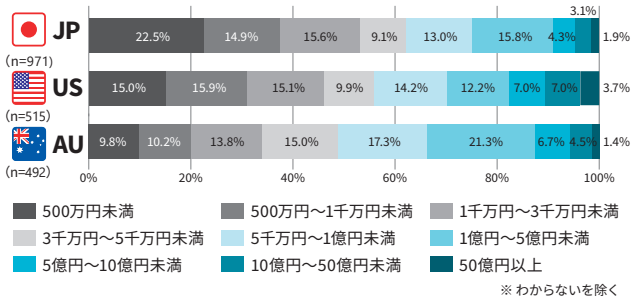
JP (n=370)　US (n=468)　AU (n=449)

※脆弱性スキャン：自動ツールや手動テストを用いて脆弱性の存在を確認する
侵入テスト（ペネトレーションテスト）：現実のサイバー攻撃を模してテストし、攻撃者の目的の達成可否や影響範囲を確認する

セキュリティマネジメント

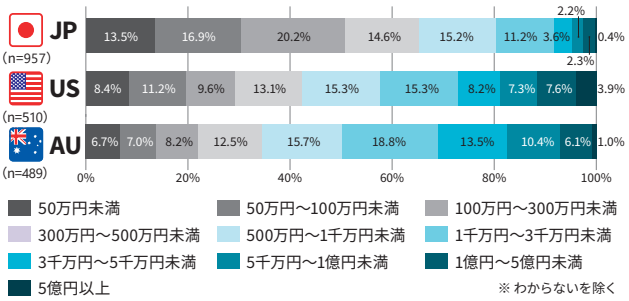
米/豪と比較すると、日本のセキュリティ関連予算額は少ない
一方で、日本のセキュリティ関連予算を昨年度と比べると維持ないし増額の見通し

IT 関連予算



※ わからないを除く

セキュリティ関連予算



※ わからないを除く

- 日本の IT 関連予算およびセキュリティ関連予算は、米 / 豪と比較して、予算額が少ない。
- 金額レンジのギャップに着目すると、セキュリティ関連予算額の方が各国における割当ギャップが大きい。

COVID-19 によるセキュリティ関連予算の昨年度比

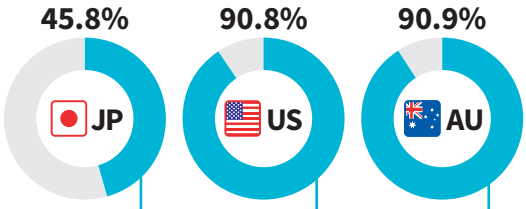
	JP (n=1,059)	US (n=510)	AU (n=499)
1位	55.9% セキュリティ関連予算に変化はない	27.3% COVID-19 とは関係なく、セキュリティ関連予算は減額した、または減額する見込み	37.5% COVID-19 によって、セキュリティ関連予算は増額した、または増額する見込み
2位	17.6% COVID-19 によって、セキュリティ関連予算は増額した、または増額する見込み	26.7%	22.2% COVID-19 とは関係なく、セキュリティ関連予算は減額した、または減額する見込み
3位	14.0% COVID-19 とは関係なく、セキュリティ関連予算は増額した、または増額する見込み	22.7% COVID-19 によって、セキュリティ関連予算は減額した、または減額する見込み	18.8%
4位	9.6% COVID-19 によって、セキュリティ関連予算は減額した、または減額する見込み	14.5% COVID-19 とは関係なく、セキュリティ関連予算は増額した、または増額する見込み	11.2%
5位	2.9% COVID-19 とは関係なく、セキュリティ関連予算は減額した、または減額する見込み	8.8% セキュリティ関連予算に変化はない	10.2%

※ わからないを除く

増加　変化なし　減少

- 日本は、米 / 豪とは異なり、セキュリティ関連予算に変化がないと回答した企業が最も多かった。
- 日本企業のセキュリティ関連予算の増減については、COVID-19 の影響を問わず、増額すると回答した企業が 2 位、3 位を占め、減額すると回答した企業よりも多かった。
- 日本は、今後の事業環境の変化や変化に伴う想定リスクを踏まえて、セキュリティ関連予算の見直しを検討すべき。

CISO を設置している企業



CISO の属性とその割合

	JP (n=1,059)	US (n=510)	AU (n=499)
経営層	75.2%	49.8%	55.9%
非経営層	23.0%	38.6%	33.6%
社外有識者	1.8%	11.6%	10.5%

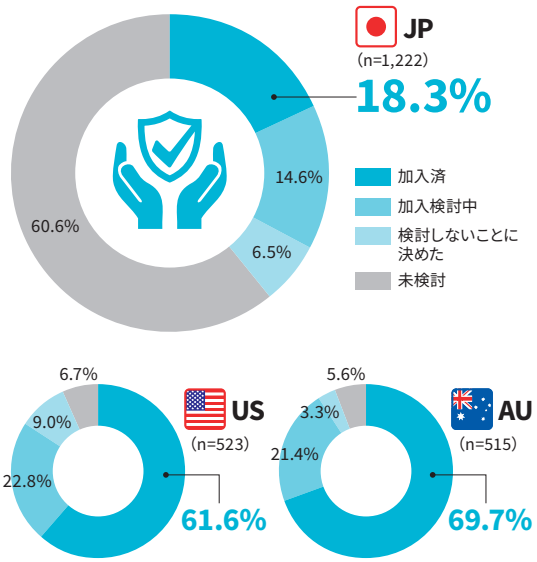
※ わからないを除く

- 米 / 豪ともに 90% 以上の企業で CISO を設置しているところ、日本は約 45% 程度にとどまっている。
- CISO の属性内訳をみてみると、3ヶ国とも経営層が就任している割合は一番高い結果となったが、日本と米 / 豪では社外有識者の採用率に差が出た。

セキュリティマネジメント

サイバー保険の加入を検討することで自社の事業特性やリスクの解像度が高まる
人材不足に悩む企業ほど、ガイドラインのベストプラクティス参照が有益

サイバー保険の加入状況



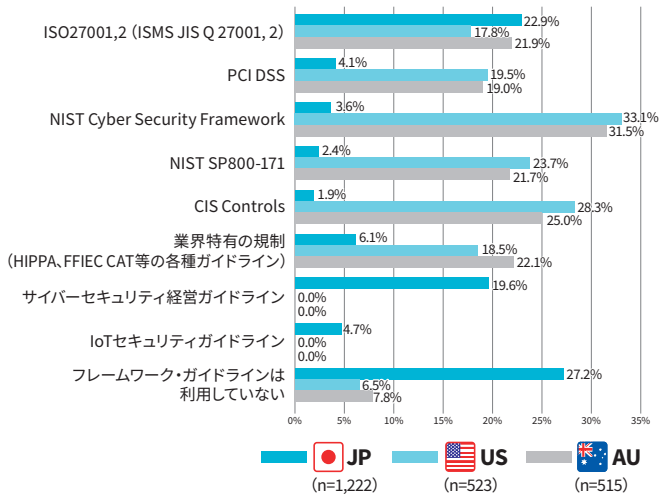
保険加入理由

	JP (n=224)	US (n=322)	AU (n=359)
1位	40.2% 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	48.1% 補償内容に対し、保険料が妥当だと感じたため	44.0% 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
2位	30.8% 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	44.4% 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	43.7% 補償内容に対し、保険料が妥当だと感じたため
3位	27.7% 補償内容に対し、保険料が妥当だと感じたため	22.0% 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	22.3%
4位	16.5%	19.3% 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	20.1%
5位	6.7% トップダウン指示があったため	14.9% 取引先や業務委託元等から加入の要請があったため	18.4%

- サイバー保険加入済の企業は米国・豪州で60%以上なのに対し、日本では20%程度にとどまっている。日本企業では未検討の割合が60%以上を占めているため、事業特性を踏まえた上での有用性やリスク移転という選択肢を選ぶことによる期待効果を検討することが求められる。
- 保険加入理由として、日本では「見舞金支払いへの充当」という理由が2位に来ているのが特徴的である。米/豪ではほぼ同一の理由が選ばれたが、3位に「株主・取引先にアピールするため」が占めているのは、日本との明確な差である。

参考ガイドライン

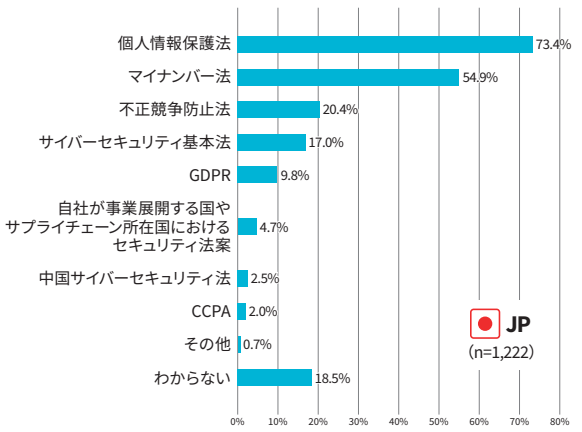
あてはまるものをすべて選択



- 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で、ガイドラインを利用してない企業が約30%と多かった。
- 自社の事業特性やセキュリティ課題を踏まえた上で、複数の国内外ガイドラインを参照することで、セキュリティ対策の抜け漏れ防止や効率・効果的な対策選定に繋げることが期待できる。

セキュリティ関連法令の対応状況

あてはまるものをすべて選択

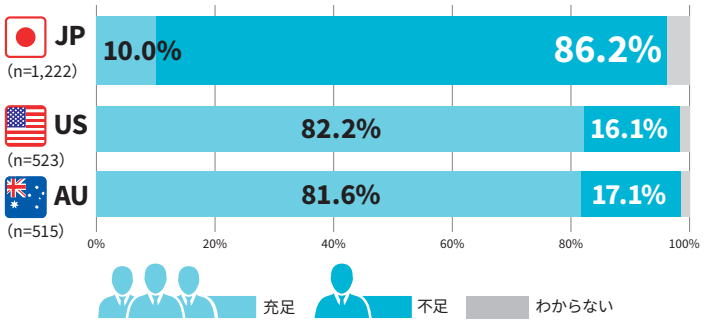


- 2020年6月に改正個人情報保護法が公布された。公布後、2年以内に施行予定のため、企業には期限を意識した計画的な対応が求められる。
- 日本企業は、GDPR、CCPAなどの国外法令への準拠要否を判断するために、事業やサービスの提供範囲を把握し、自社に関係があるかを把握することが肝要である。

セキュリティ人材

過去10年間と同様、日本だけが圧倒的に人材が不足している
人材が充足している企業においても、サイバー攻撃の検知状況は要確認

セキュリティ対策に従事する人材の充足状況



- 米・豪の80%以上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10年間の調査でも同様であった。
- 日本では少子高齢化による労働人口の減少とDXの進展というトレンドを受けて、IT・セキュリティ人材の希少価値が更に高まっている。
- 企業がセキュリティ業務の継続性を維持・向上するためには、人が対応する業務の量を必要最小化することで、業務環境やルール・プロセスを絶えずアップデートすることが欠かせない。

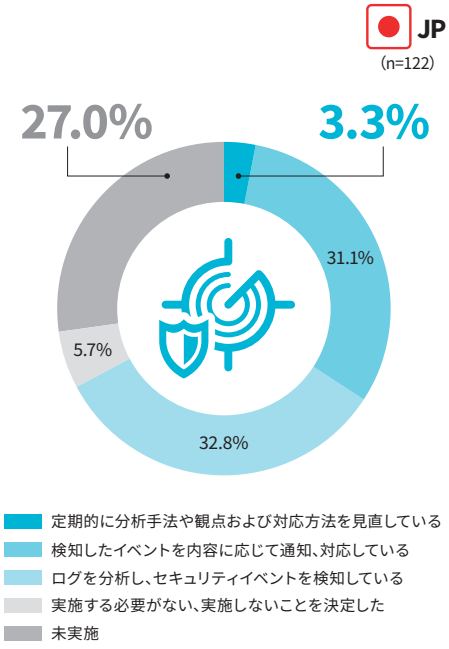
充足していると考える理由

あてはまるものを最大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=122)	US (n=430)	AU (n=420)
1位	セキュリティ業務の量が少ない	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
2位	想定よりも有事対応が少ないため	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
3位	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標準化され役割分担が明確	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	想定よりも有事対応が少ないため	セキュリティ業務が自動化・省力化されている
5位	セキュリティ業務を外部委託している	経験豊富なメンバーで対応	経験豊富なメンバーで対応

サイバー攻撃の検知状況



- 充足理由としては、各国に共通してセキュリティ業務量が少ない、想定よりも有事対応が少ないという回答が上位を占めている。そんな状況下においても、各企業は有事が発生した際に適切かつ迅速な判断ができるように、平時から有事に備えて訓練をしておく必要がある。
- 人材が充足していると回答した日本企業の「サイバー攻撃の検知状況」を見てみると、多くの企業が検知している結果であったが、27.0%は未実施で、定期的に検知状況を見直している企業は3.3%に留まった。企業のセキュリティインシデント事例では、被害発覚後に詳細調査を行うと、サイバー攻撃者が数年前に侵入しており、巧妙な侵入・侵害に気づけていなかったというケースも多数見られる。そうならないためにも、定期的に検知状況の見直しまで行うことが望ましい。
- セキュリティ人材の不足に悩む日本企業は、不足人材の採用・補充だけを行うのではなく、セキュリティ業務を継続的かつ効率的に回せるように、業務を自動化・標準化することで肝要である。

セキュリティ人材

不足人材は、セキュリティ教育・アウトソースなどの取り組みでカバー
足りない高度専門能力を補う手段として、副業などの選択肢に注目が集まる

不足している人材の種別

あてはまるものを最大3つ選択

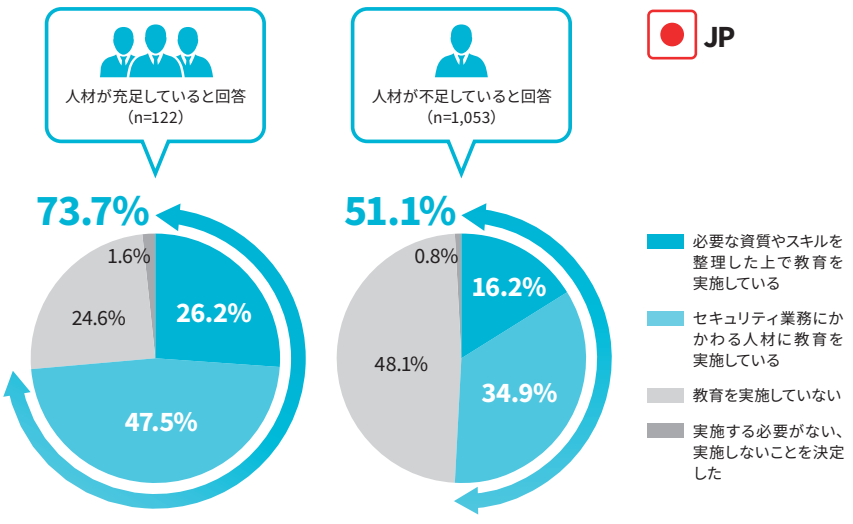
不足していると回答した企業における、不足している人材種別TOP5

	JP (n=1,053)	US (n=84)	AU (n=88)
1位	セキュリティ戦略・企画を策定する人	経営層に現状や対策内容等を説明する人	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	セキュリティリスクを評価・監査する人	セキュリティ戦略・企画を策定する人
3位	ログを監視・分析する人	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
4位	インシデントへの対応・指揮ができる人	セキュリティ戦略・企画を策定する人	セキュアなシステム設計する人
5位	関係部署と調整しつつ、対策を推進・統括する人	セキュアなプログラミングができる人	セキュリティインシデントへの対応・指揮ができる人

- 日本の1位は「セキュリティ戦略・企画を策定する人」で、2位は「セキュリティリスクを評価・監査する人」だった。DX機運の高まり、ゼロトラストモデルへのシフト、テレワークの緊急導入など、セキュリティ戦略を描ける人材や変化に伴うセキュリティリスクを把握できる人材の価値が一層高まっている。
- 各セキュリティ業務の特性を見極め、社内の人材を充てて育てる、アウトソースする、ツール導入で現場を支援する等、適切な選択を迅速に継続し続けることが重要である。
- 過去10年間続いてきたセキュリティ人材不足の解消には、これまでの前提条件や慣習を根本から見直す必要がある。
- 今後は、IT・セキュリティ分野においても、副業人材の受入れや自社人材の副業を許可する流れになると考えられる。そのため、就業規則を見直し、多様な能力・経験の獲得を促進する制度の策定が望まれる。

日本企業における人材の充足状況別、セキュリティ教育状況

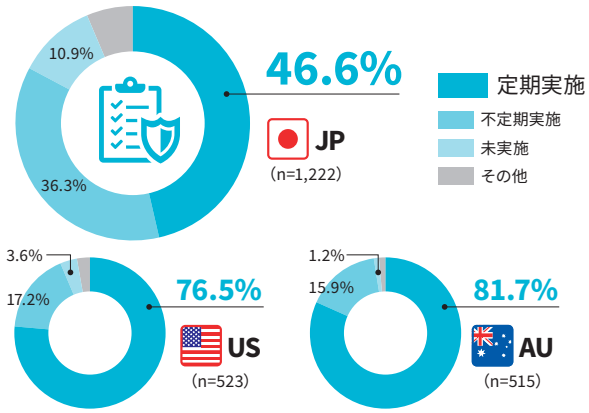
- 日本のセキュリティ人材充足企業と不足企業で、セキュリティ教育の実施状況を比較したところ、「充足」と回答した企業は、教育を実施していると回答した割合が約25pt高かった。
- セキュリティ人材不足を解消するために、社内異動や配置変更で新たなセキュリティ人材を設置する際には、早期立上げを支援するためのセキュリティ教育が有効である。
- テレワークが標準となる時代において、IT/セキュリティ部門はその実践をリードする立場になるため、テレワークと相性が良いオンラインの教育機会を整備するなど、セキュリティ教育自体のDX化が欠かせない。



セキュリティ対策

日本企業の経営層のリーダーシップ発揮割合が向上
COVID-19に伴い対策が急務であった影響か

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75%、豪が約80% である一方、日本は50% 以下であった。
- 日本も不定期を含めると約80% の企業が評価を実施しているが、評価や現状の見直しもセキュリティ対策の重要なマイルストーンとして捉え、定期的に実施することが大切である。
- 専門家による第三者評価とツールなどを用いた自己評価の双方のメリットを踏まえ、自社に適した手法で実施することが望ましい。

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=1,222)	**30.7%**	8.3%	**28.4%**	7.8%	16.2%
US (n=523)	9.6%	11.7%	24.3%	20.1%	**32.5%**
AU (n=515)	10.6%	6.4%	23.1%	22.7%	**35.3%**

※ その他の選択肢：わからない / その他

- 日本は「短期的」、米 / 豪は「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。
- 日本は計画未策定企業の割合が約30% と、米 / 豪に比べ高い。
- 効果的なセキュリティ対策推進のためには、自社に適した実行計画を中長期的な視点で策定し、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。

情報セキュリティ対策実施のきっかけや理由

あてはまるものを最大3つ選択

	JP (n=1,222)	US (n=523)	AU (n=515)
1位	自社でのセキュリティインシデント **30.7%**	経営層のトップダウン指示 **56.4%**	経営層のトップダウン指示 **61.4%**
2位	経営層のトップダウン指示 **23.4%** UP 昨年4位からランクアップ	他社でのセキュリティインシデント **22.2%**	他社でのセキュリティインシデント **23.7%**
3位	他社でのセキュリティインシデント **23.2%**	自社でのセキュリティインシデント **19.3%**	自社でのセキュリティインシデント **19.8%**

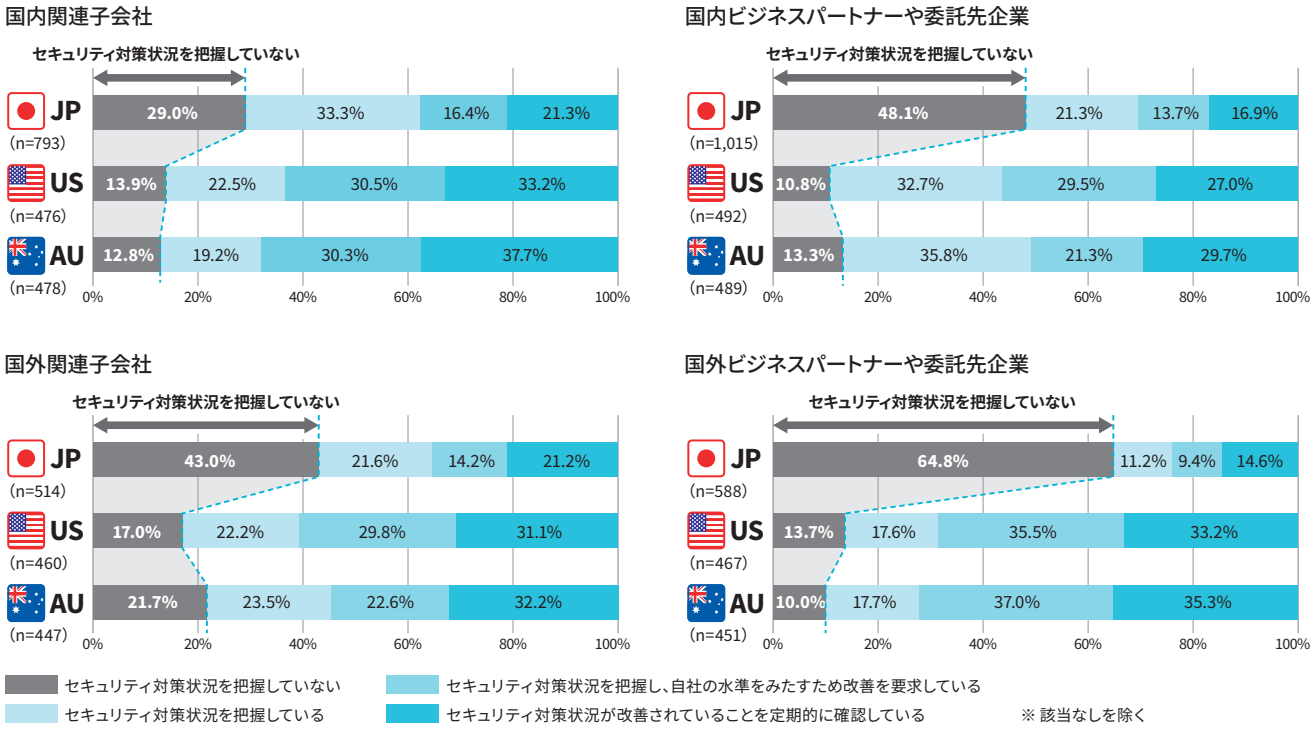
※ 他選択肢：監督省庁からのセキュリティ対策強化の要請 /関連法規の改定 /株主や取引先からの要請 /持株会社や親会社からの要請 / 競合他社の実施状況との比較 / 外部監査・第三者評価の結果 内部監査・内部有識者からの指摘 / COVID-19に伴うテレワーク対応 / 国際的なイベント開催に伴う対応 / DX化推進に伴う対応 / その他 / わからない

- 米 / 豪の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。
- 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。米 / 豪と比較すると、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ることが多いと考えられる。
- 一方で日本の「経営層のトップダウン指示」は昨年調査の4位から2位にランクアップしており、「COVID-19に伴うテレワーク対応」の割合は20.3% で4位となった。COVID-19 による影響から、IT・セキュリティ戦略が待ったなしの状態となり例年に比べ経営層がリーダーシップを発揮した、あるいは経営層の協力を得やすかったのではないかと推察する。

セキュリティ対策

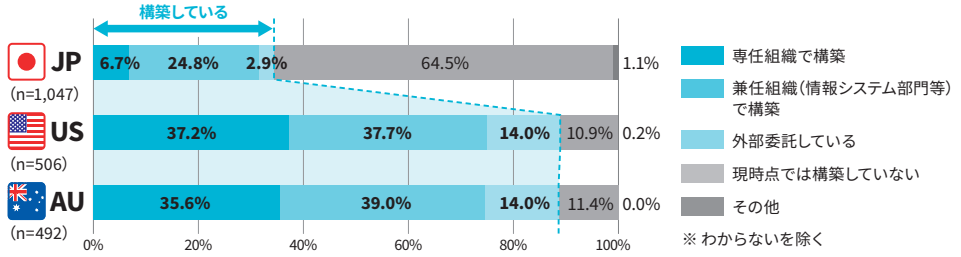
日本のセキュリティ統制は範囲拡大と要請のレベルアップの双方が求められる
まずは統制範囲を委託先企業や国外企業に広げていくことが望ましい

サプライチェーンに対するセキュリティ統制



- 米/豪と比較すると低いものの、日本企業の約70%が国内関連子会社のセキュリティ対策状況を把握している。
  近年、サプライチェーン攻撃を起因としたインシデントが多数発生していることや、国や政府機関が発行するガイドラインにおいて、サプライチェーンを意識した対策の重要性が言及されていることから、多くの日本企業が国内関連子会社のセキュリティ対策状況の把握に取り組んでいるものと推察する。
- 国内よりも国外、関連子会社よりもビジネスパートナーや委託先企業に対する統制割合が低いのは、企業間の関係性に対する配慮や言語の壁などに加え、セキュリティ予算の割当てが相対的に自社や国内に割かれやすいことが原因と考えられる。
- セキュリティ対策状況を把握している場合でも、日本は米/豪と比べて、関連子会社や委託先企業に改善を求める割合が少ない。米国では、サードパーティーリスクの最小化を目的に、VRM（ベンダーリスクマネジメント）という考え方が浸透しており、VRMプラットフォームを活用するユースケースが多く見られる。
- VRMプラットフォームを用いることで、統制元の企業は国内・国外を問わず、関連子会社や委託先企業のセキュリティ実態を把握しやすくなる。また、一過性ではなく、サプライチェーンを継続的に評価することが可能になるため、改善要請や改善状況の確認がしやすくなる。今後、日本でもVRMのコンセプトが浸透していくことを期待したい。

CSIRTの構築状況



- CSIRTの構築形態を見てみると、日本企業は兼任組織が中心であるものの、米/豪は専任組織と兼任組織での構築がほぼ同割合であり、日本に比べ外部ベンダにアウトソースしている企業の割合も高い結果となった。

セキュリティ対策

日本企業が困っていることの1位はインシデント発生時の緊急対応
Emotetの流行やDX・テレワークの進展による影響が背景か

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

あてはまるものを最大3つ選択

	JP (n=1,222)	US (n=523)	AU (n=515)
1位	セキュリティインシデント発生時の緊急対応 42.0%	セキュリティ対策のトレンド・他社動向の把握 38.2%	セキュリティ脅威・事故に関する情報収集と関係者共有 35.7%
2位	自社セキュリティ対策の遅れ（最新技術・動向の未反映） 40.8%	セキュリティ脅威・事故に関する情報収集と関係者共有 35.2%	セキュリティ対策のトレンド・他社動向の把握 34.4%
3位	サイバー攻撃の高度化への対応 38.2%	セキュリティ業務の状況・進捗に関する経営層への報告 27.3%	セキュリティインシデント発生時の緊急対応 29.1%

※ 他選択肢：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 / テレワーク環境におけるセキュリティの確保 / その他 / 困っていることはない

- 日本は、セキュリティインシデント発生時の緊急対応が1位となった。CSIRTの未設置企業の割合が高いことや、日本でも多くの被害事例が発生したEmotetによる影響、あるいはCOVID-19で加速化したテレワーク環境への移行に伴い、既存のインシデント対応プロセスの限界や制約に苦労したことなどが原因と考えられる。
- 日本の2位は「自社セキュリティ対策の遅れ」である。2020年にDXおよびテレワークが急激に進展した一方で、日本企業のIT/セキュリティ担当者の多くは、既存のITインフラやセキュリティポリシーに基づく境界型防御モデルに構造的な限界を感じていることが背景にあると考えられる。
- 企業の経営層やリーダーは、DXのトレンドを捉え、柔軟かつ俊敏なIT/セキュリティ環境を自社にて実現することが欠かせない。ゼロトラストモデルへのパラダイムシフトを経営計画における必要不可欠な構成要素と捉え、セキュリティ変革への投資を決断し、現場のセキュリティ変革を理解・支援することが重要である。

困りごとを解消するための情報収集手段

あてはまるものをすべて選択

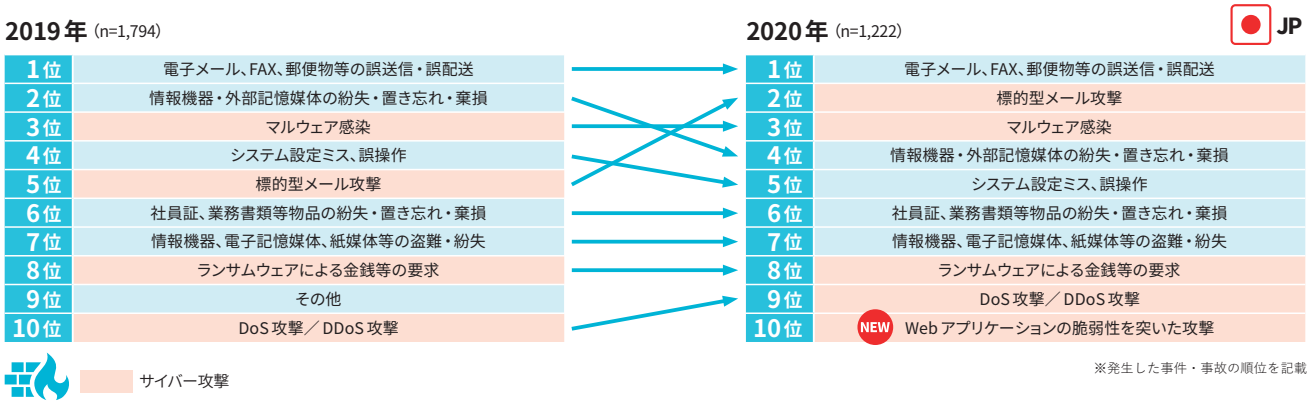
	有志の勉強会やコミュニティに参加	セキュリティベンダに問い合わせ・調査依頼	公的機関発行の情報を参照	所属する業界団体（ISAC等）に問い合わせ	インターネット記事、新聞記事を参照
JP (n=1,222)	12.9%	42.7%	27.0%	6.2%	61.5%
US (n=523)	34.4%	46.7%	28.9%	25.6%	13.2%
AU (n=515)	35.7%	47.2%	34.0%	26.4%	12.8%

- 情報セキュリティ担当者として対応に困った際、解消のための手段としてセキュリティベンダに問い合わせを行う割合は日/米/豪でほぼ差がなかった。
- 一方、インターネット記事や新聞記事を参照すると回答した割合は日本企業が圧倒的に高かった。米/豪の担当者も日頃の情報収集としてはインターネット記事を参照していると考えられるが、困りごとを迅速かつ適切に解消するための情報収集は、勉強会への参加や業界団体への問い合わせを積極的に活用していることが伺える。
- 日本は欧米と比較して情報の収集元として新聞を参照する文化が根強い。新聞による情報収集は引き続き行いつつも、COVID-19以降、頻繁に開催されているオンライン勉強会やウェビナーへの参加などを通じた新たな情報収集手段も取り入れていくことが望ましい。

日本はサイバー攻撃の事件・事故が増加傾向に
2021年以降、これまでのセキュリティ対策の定石を見直す機運が高まる

日本で過去1年で発生した事件・事故 昨年との比較

あてはまるものをすべて選択



※発生した事件・事故の順位を記載

- 日本企業では、電子メール、FAX、郵便物などの誤送信・誤配送が1位だが、その内訳はCOVID-19の影響を受けているものと考えられる。テレワーク環境下で、企業間のドキュメントや契約書などのやり取りを電子化する機会が増えた。郵便物の総量が減る一方で、メールに電子ファイルを添付する機会は減らず、メールの誤送信に繋がりうる機会と環境は例年以上だったことが考えられる。今後、「暗号化ファイルのウイルスチェックすり抜けの防止」や「メール添付ファイルのクラウドストレージへの置き換え」など、これまでのセキュリティ対策の定石であった対応の見直しが、産官学の枠組みで、適宜検討・実施されていくことが予想される。
- 標的型メール攻撃が2位に上昇した。2019年後半に話題となったメールを介した巧妙なマルウェアEmotetの攻撃が、2020年に入ってから再び活発になったことと、その時期に日本企業の多くがテレワーク環境であったことも一因と考えられる。メールを介したマルウェアへの感染を防ぐためには、組織内へ注意喚起、ソフトウェアの適宜アップデートなど従業員でできる対策と、マルウェア付きのメール検知、エンドポイントのセキュリティ強化および効率的なインシデント対応を実現するためのEDRの導入など、幅広く対策していくことが望ましい。
- Webアプリケーションの脆弱性を突いた攻撃が新しく10位にランクインした。DXの進展に伴い、企業においてWebアプリケーションサービスの提供・活用が進む一方で、適切な対策がなされていないままにリリースされているケースもあると見られる。

過去1年で発生した事件・事故（2020年の3ヶ国比較）

あてはまるものをすべて選択

	JP (n=1,222)	US (n=523)	AU (n=515)
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	標的型メール攻撃	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（ミドルウェア、OSプラットフォーム等）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	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	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	システム設定ミス、誤操作	標的型メール攻撃	システム基盤（ミドルウェア、OSプラットフォーム等）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	水飲み場型攻撃	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	ランサムウェアによる金銭等の要求	水飲み場型攻撃
8位	ランサムウェアによる金銭等の要求	マルウェア感染	ランサムウェアによる金銭等の要求
9位	DoS攻撃／DDoS攻撃	データ通信、音声通信等の盗聴・傍受	廃棄された電子記憶媒体等からのデータ復元による情報漏えい
10位	Webアプリケーションの脆弱性を突いた攻撃	システム設定ミス、誤操作	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

サイバー攻撃

※発生した事件・事故の順位を記載

- 日本はヒューマンエラーが上位を占めるが、米/豪の海外企業はDoS/DDoS攻撃や脆弱性を突いた攻撃などのサイバー攻撃が、1位から8位までの上位を占めた。
- 日本ではCOVID-19による影響を受け、テレワークへの環境移行が進んだ。政府によるデジタル庁新設の流れを受け、新しいテクノロジーやクラウド活用をベースにしたデジタル化が、より勢いを増して推進されていくことが考えられる。一方で、サイバー攻撃の被害を受ける可能性や被害発生時の影響も大きくなるため、攻守のバランスに留意しながら、時代の要請に適応したセキュリティ対策を実践・継続していく必要がある。

標的型攻撃による情報漏えい、ランサムウェア被害を各国が脅威と警戒
一方で、日本では内部不正を脅威と捉える傾向が高い

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=1,222)		US (n=523)		AU (n=515)	
1位	標的型攻撃による情報漏えい	54.3%	ランサムウェアによる被害（情報消失、金銭被害）	25.4%	標的型攻撃による情報漏えい	27.8%
2位	ランサムウェアによる被害（情報消失、金銭被害）	52.7%	サービス妨害攻撃（DDoS攻撃等）によるサービス停止	24.7%	ランサムウェアによる被害（情報消失、金銭被害）	25.8%
3位	内部不正による被害（情報漏えい、業務停止）	46.1%	標的型攻撃による情報漏えい	24.3%	ビジネスメール詐欺（BEC）による金銭被害	21.6%
4位	メールの誤送信・誤配信	25.3%	ビジネスメール詐欺（BEC）による金銭被害	22.9%	サービス妨害攻撃（DDoS攻撃等）によるサービス停止	21.4%
5位	ビジネスメール詐欺（BEC）による金銭被害	18.6%	自社Webサービスへのリスト型アカウントハッキングによる被害（情報漏えい、サービス停止）	18.0%	Webサイトの改ざん	21.0%
6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	17.8%	Webサイトの改ざん	16.6%	自社Webサービスへのリスト型アカウントハッキングによる被害（情報漏えい、サービス停止）	15.9%
7位	情報機器、社員証等の置き忘れ、棄損による情報漏えい	13.9%	内部不正による被害（情報漏えい、業務停止）	11.5%	メールの誤送信・誤配信	15.3%
8位	サービス妨害攻撃（DDoS攻撃等）によるサービス停止	11.8%	顧客向けに提供している自社製品のセキュリティ侵害	10.5%	情報機器、社員証等の置き忘れ、棄損による情報漏えい	14.4%
9位	Webサイトの改ざん	8.1%	メールの誤送信・誤配信	9.9%	退職者、転職者による在職時に利用していた情報の使用	12.4%
10位	SaaS（ストレージサービス、チャット、web会議ツール等）利用からの情報漏えい	7.7%	SaaS（ストレージサービス、チャット、web会議ツール等）利用からの情報漏えい	9.0%	内部不正による被害（情報漏えい、業務停止）	11.7%

サイバー攻撃

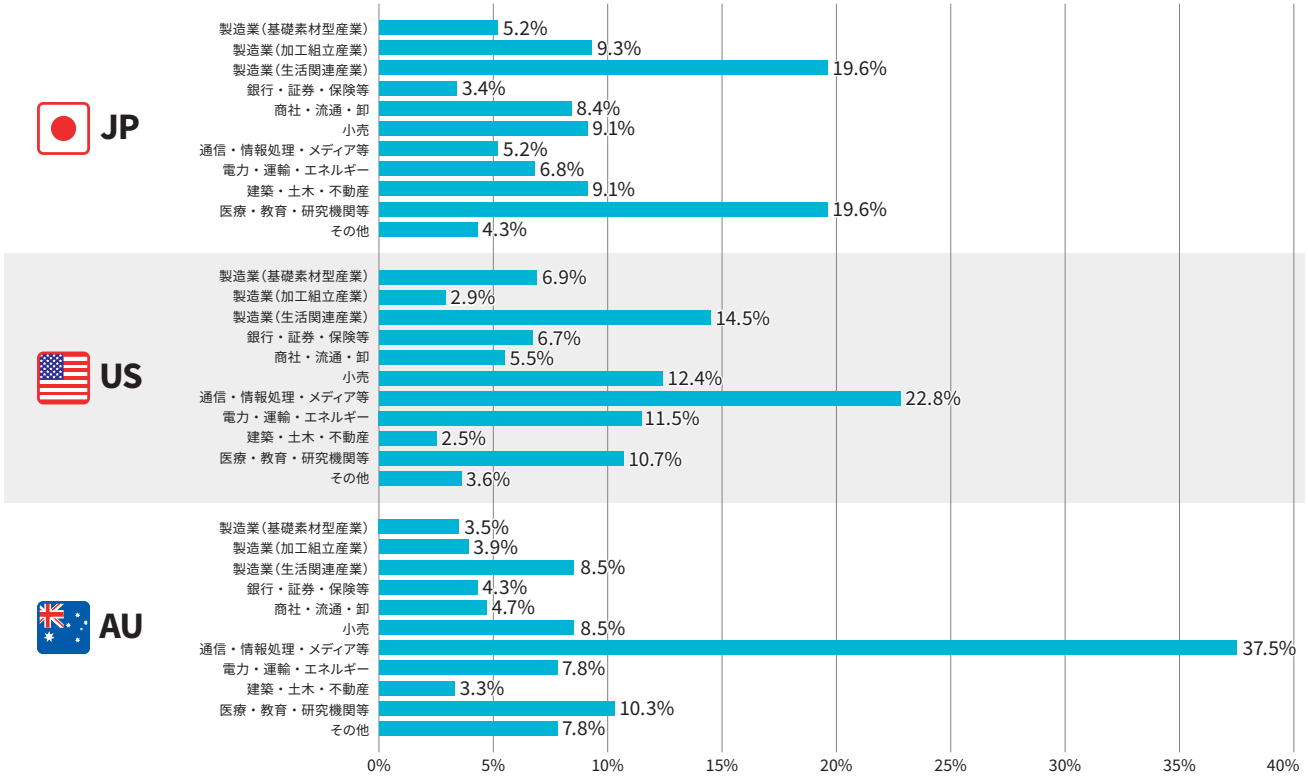
- 自社で最も脅威となる事象は、3ヶ国共に「標的型攻撃による情報漏えい」、「ランサムウェアによる被害」が上位となった。Emotetや身代金要求型のランサムウェアの世界的な流行と被害事例などが背景にあると考えられる。
- 日本の特徴は、3位の「内部不正による被害」、4位の「メールの誤送信」といった企業や組織内部の人に起因する脅威の順位が高い点にある。内部不正による被害が顕在化した場合、システム管理者などの高権限を悪用されるため、大量のデータ漏えいに繋がる可能性が高い。また、COVID-19によりテレワークが業務遂行の第一選択肢になったことで、メール送信における宛先確認や上長承認などのプロセスを緩和する可能性が高く、その影響が懸念される。
- 日/米の10位は、「SaaS利用からの情報漏えい」になった。政府が提唱するクラウド・バイ・デフォルトの原則やCOVID-19の影響によるテレワーク環境への急激な進展により、企業によるWeb会議やチャットの利用が盛んになった一方で、セキュリティへの不安が増したことが背景にあるものと考えられる。
- 米/豪は日本と比較して「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」が上位を占め、「内部不正による被害」などの人に起因する脅威は下位であった。

回答者属性

回答企業社数：合計 2,260 社（JP 1,222 社、US 523 社、AU 515 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



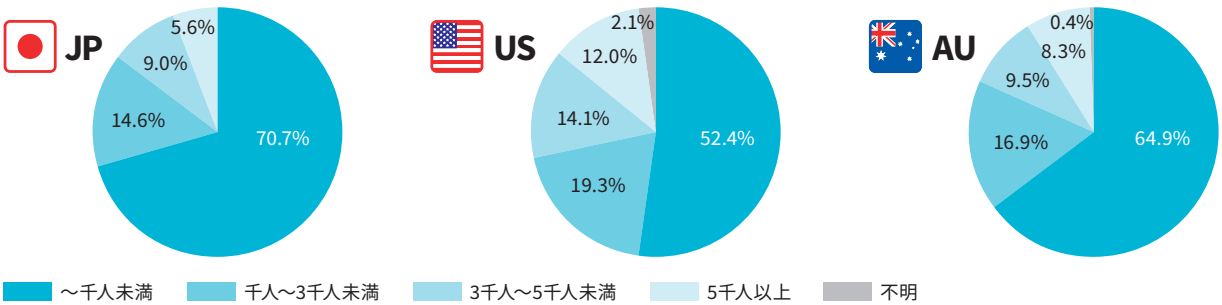
※ 回答企業の業種を以下のように分類

- 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・xDSL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。



調査方法

調査方法

日本、アメリカ、オーストラリア：
Web によるアンケート

調査対象

日本、アメリカ、オーストラリア：
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：2020/ 7 / 1 ～ 2020/ 9 / 18
アメリカ、オーストラリア：2020/ 8 / 1 ～ 2020/ 9 / 18

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 2020　制作委員会		
企画	山田 真暉		
執筆	神野 宰平 名部井 康博	森 茉莉香 永谷 知也	山田 智隆
アドバイザー	観堂 剛太郎 京山 剛大 渡部 惣 鳥越 真理子 小坂 充	菅谷 光啓 稲田 憲昭 石井 晋也 川谷内 直樹 高橋 静香	佐藤 健 木内 雄章 新井ちづる 浅水 喬大
監修	足立 道拡	川崎 聡太	

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
横浜ベイオフィス	〒221-0056 神奈川県横浜市神奈川区金港町 1-7 横浜ダイヤビルディング
北米支社	26 Executive Park Suite 150 Irvine CA 92614 U.S.A.
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	連結：548 名　単体：465 名

（2020 年 10 月現在）

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
18 年に渡り実施しています

18 年間の調査を通じ、のべ
14,837 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
  - SOC／CSIRT 構築運用支援サービス市場
  - OT セキュリティ構築運用支援サービス市場
  - セキュリティ監査サービス市場標的型攻撃メール訓練サービス市場
  - セキュリティ情報配信サービス市場

＊1 ITR「ITR Market View：アイデンティティ／アクセス管理市場 2020」2019 年度ベンダー別売上金額　＊2 ITR「ITR Market View：コラボレーション市場 2020」2019 年度ベンダー別売上金額　＊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 2019」2018 年度ベンダー別売上金額

情報セキュリティ格付 10 年連続最高ランク

- 情報セキュリティ格付最高ランク 10 年連続獲得（クリプト便）
  （格付機関：株式会社アイ・エス・レーティング、2011～2020 年）

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
  4 年連続受賞（2017 年～2020 年）

グローバル　グローバル市場における実績から IT 調査会社資料に掲載

Gartner

- 「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サービス」[*4]

＊4 “Market Guide for Digital Forensics and Incident Response Services” Brian Reed & Toby Bussa (11Dec2019)（ガートナー免責条項）ガートナーは、ガートナー・リサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高のレーティング又はその他の評価を得たベンダーのみを選択するようにテクノロジーユーザーに助言するものではありません。ガートナー・リサーチの発行物は、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、一切の責任を負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」[*5]
- 「The Forrester WaveTM：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」[*6]
- 「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」[*7]
- 「クリプトカレンシーのセキュリティ」[*8]

＊5 Forrester “Vendor Landscape: Global Managed Security Services, 2017”　＊6 Forrester “The Forrester Wave™: Emerging Managed Security Services Providers (MSSPs), Q3 2018”　＊7 Forrester “Now Tech: Managed Security Services in Asia Pacific, Q4 2020, Forrester’s Overview of 35 Managed Security Service Providers”　＊8 Forrester “The Security Of Cryptocurrencies”

資格取得者数

100 名 **CISA**（公認情報システム監査人）	**75 名** **CISM**（公認情報セキュリティマネージャー）
59 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）	**220 名** **GIAC**（Global Information Assurance Certification）

*2020 年 10 月現在

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