# NRI Secure Insight 2018

企業における情報セキュリティ実態調査

NRI SECURE

# NRI Secure Insight 2018

企業における情報セキュリティ実態調査

「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15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、16年目の今年は初の5か国を対象としたグローバル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 2018」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107 社、アメリカ500 社、イギリス197 社、シンガポール210 社、オーストラリア96 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

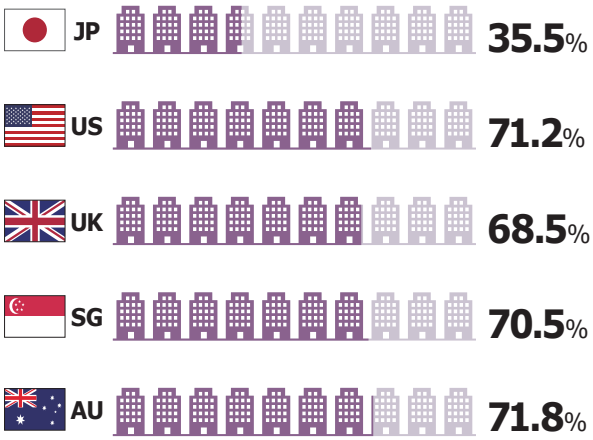
NRI SECURE

# EXECUTIVE SUMMARY

## セキュリティ経営

☑ 中長期的なセキュリティ対策実行計画にこそ経営層の旗振りが欠かせない
☑ 日本のセキュリティ経営においては、経営層と現場が一体となった対策推進が望まれる

### ◆CISO※1 を設置し、経営層が就任している割合




※1 最高情報セキュリティ責任者

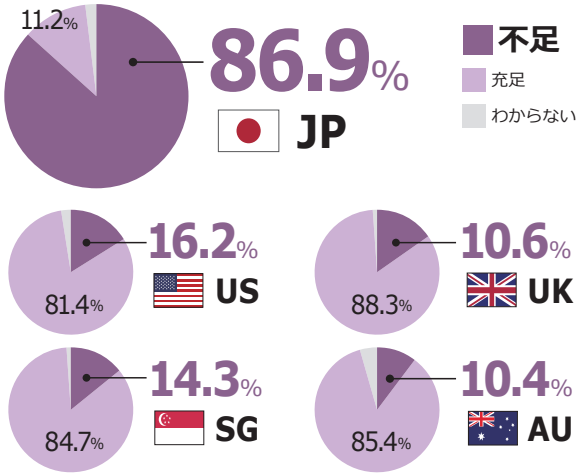
### ◆セキュリティ対策の計画スパンの差異

| | 計画策定していない | 短期計画（1年程度） | 中長期計画（3年程度） |
|---|---|---|---|
| JP | **28.9%** | **42.1%** | 25.2% |
| US | 6.0% | 38.6% | **49.0%** |
| UK | 4.0% | 27.9% | **64.0%** |
| SG | 10.0% | 37.1% | **49.1%** |
| AU | 8.3% | **50.0%** | 33.3% |

## セキュリティ人材

☑ 日本は海外4か国と比較して圧倒的に人材不足を訴えている
☑ 人材不足解消には、業務自体のあり方や人材配置の見直しが有効か

### ◆セキュリティ人材の充足状況




### ◆充足していると考える理由トップ3※1

- セキュリティ業務が自動化・省力化されている
- セキュリティ業務が標準化され、役割分担が明確
- 経験豊富なメンバで対応

※1 日本を除く4か国で理由トップ3が同一

## 調査概要

**目的**
- 日本、アメリカ、イギリス、シンガポール、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

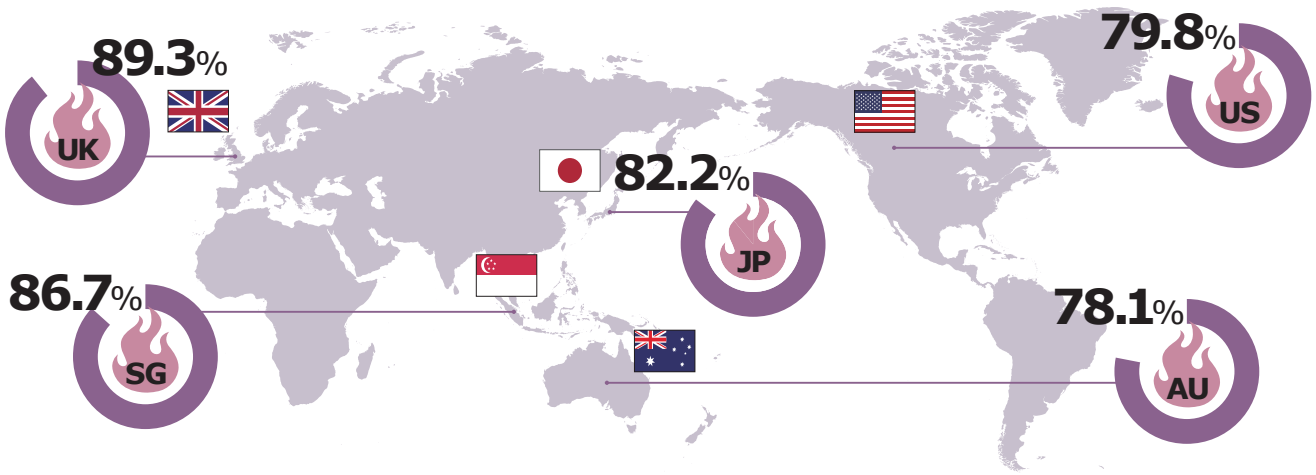
**調査対象**
- 日本、アメリカ、イギリス、シンガポール、オーストラリア企業の情報システム・情報セキュリティ担当者

**回答いただいた企業数**
- 計1,110社(日本：107社,アメリカ：500社、イギリス：197社、シンガポール：210社、オーストラリア：96社)

## 脅威・事故

☑ 調査対象国5か国の傾向が同様で、およそ8割の企業でセキュリティインシデント※1が発生している

◆過去1年に情報セキュリティインシデントが発生した企業

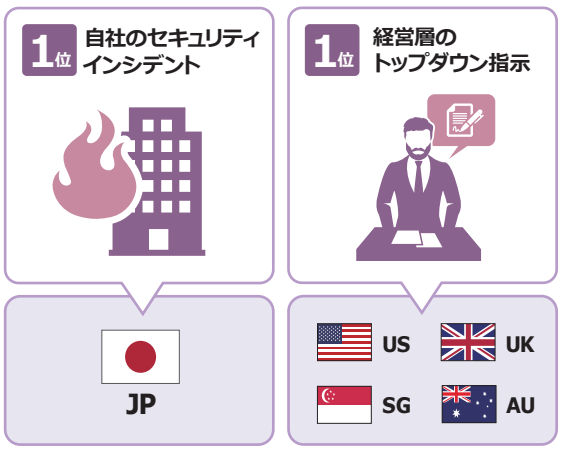



※1 サイバー攻撃、内部不正、あるいはヒューマンエラー等により発生した事件・事故を指す

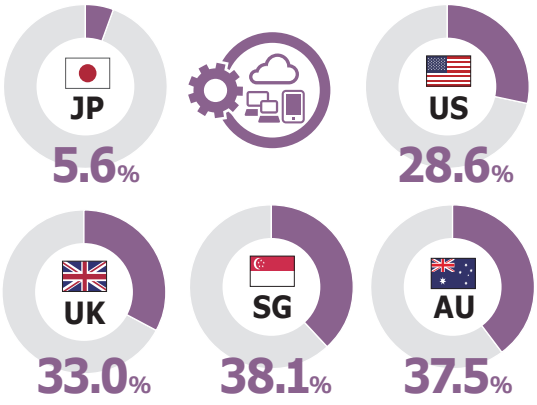
## セキュリティ対策

☑ 対策実施のきっかけ1位は日本のみが自社のセキュリティインシデント
☑ 海外4か国に比べ、日本はシャドーIT※1対策としてCASB※2等のシステム導入率が低い

◆情報セキュリティ対策の実施のきっかけや理由




◆シャドーIT 対策としてCASB等のシステムを導入している企業




※1 企業で使われる情報システムや情報機器、ソフトウェア、クラウドサービス等のうち、会社の承認なく従業員が利用しているものまたは各部門が会社の承認なく独自に導入し、情報システム部門の管理が行き届いていない情報システム

※2 シャドーITの可視化やクラウドサービスへのアクセス制御を行うセキュリティソリューション

# CONTENTS

Investigation result

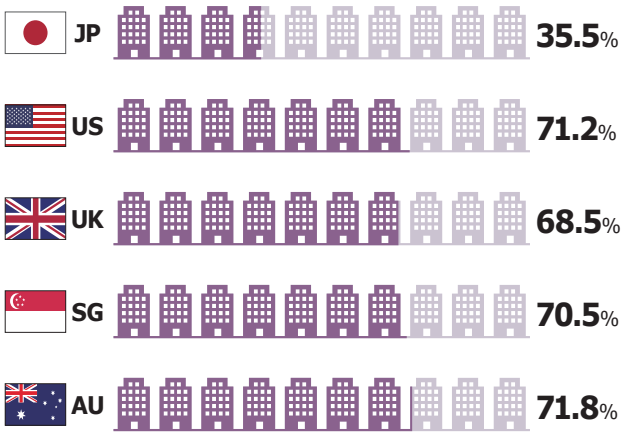
# 調査結果

**CATEGORY**

- セキュリティ経営
- セキュリティ人材
- 脅威・事故
- セキュリティ対策

# 海外４か国ではセキュリティを「経営課題」として捉えており、経営層が積極的に関与している。

## CISOを設置し、経営層が就任している割合




● CISOのポジションを専任・兼任関わらず経営層が就任している割合は、海外４か国では約70%となっており、日本では、その半数の約35%に留まっている。

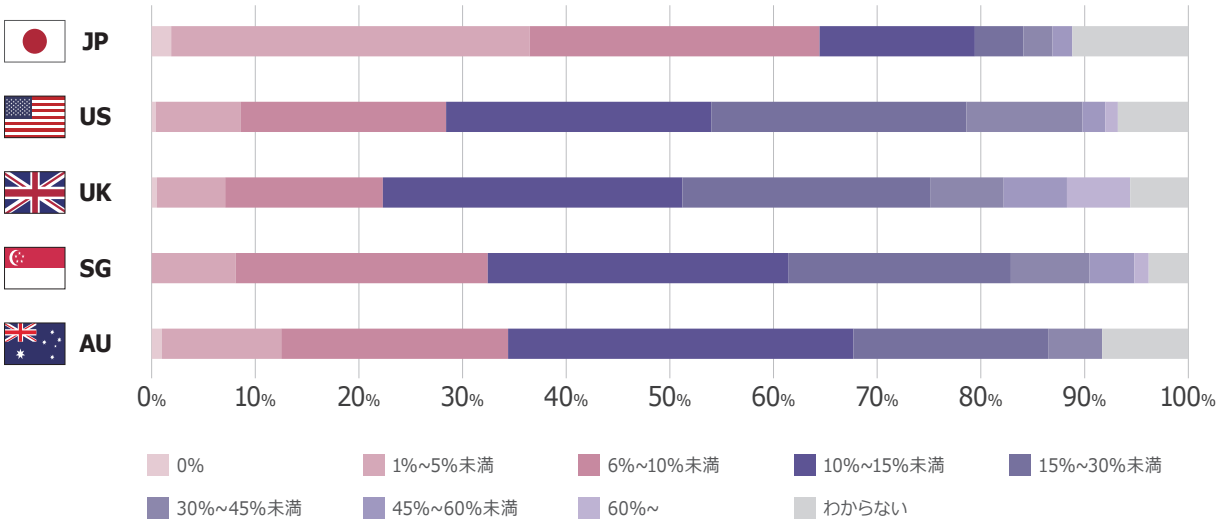
## セキュリティ対策の計画スパンの差異

| | 計画策定していない | 短期計画（1年程度） | 中長期計画（3年程度） |
|---|---|---|---|
| JP | **28.9%** | **42.1%** | 25.2% |
| US | 6.0% | 38.6% | **49.0%** |
| UK | 4.0% | 27.9% | **64.0%** |
| SG | 10.0% | 37.1% | **49.1%** |
| AU | 8.3% | **50.0%** | 33.3% |

※ 他選択肢：分からない / その他

● アメリカ、イギリス、シンガポールの3か国では、セキュリティ対策の実行計画を、3年程度の「中長期的」な視点で策定をする企業が多かった。日本、オーストラリアでは、1年程度の「短期的」な視点でセキュリティ計画を策定する企業が多く、日本企業の28.9%は計画自体を策定していないという結果となった。

## IT関連の予算に占めるセキュリティ関連予算の割合

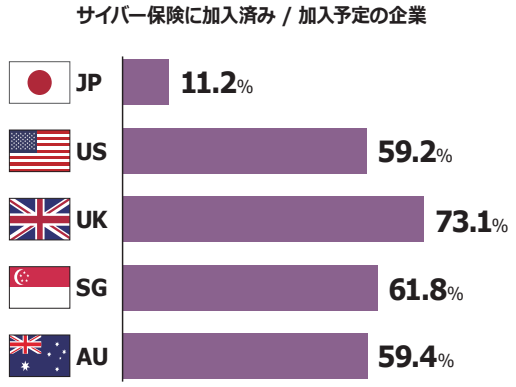



● IT関連予算に占めるセキュリティ関連予算の割合が10%以上である、と回答した日本企業は約20%程であった。海外４か国で同様の回答した企業は50%以上であった。

● 一般的に、CIOはビジネスを加速させるための「攻めの投資」を担い、CISOは情報資産を保護するための「守りの投資」を担っている。そのため、CISO設置率の高い海外企業の方が、日本企業よりもセキュリティ関連予算が多い傾向になったと考えられる。

# 海外４か国はサイバー保険の活用や、セキュリティ関連の情報開示も戦略的に実施している。

## サイバー保険の活用状況とその課題



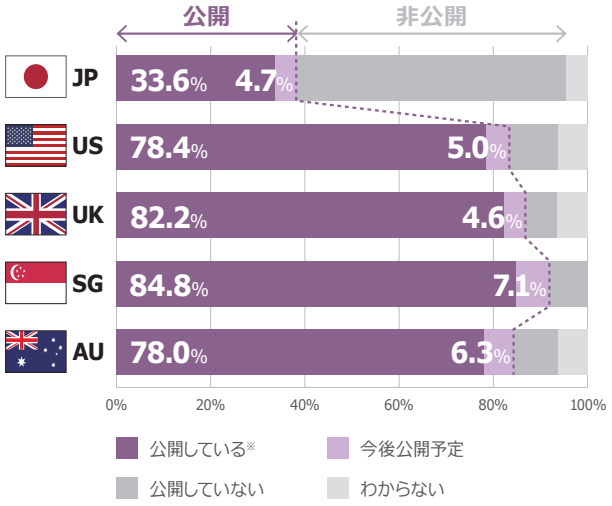

サイバー保険に対しての不満・課題

（当てはまるもの最大３つ選択）

| | JP | US | UK | SG | AU |
|---|---|---|---|---|---|
| 1位 | わからない | 補償内容の拡充 | 補償額の引き上げ | 補償額の引き上げ | 補償内容の拡充 |
| 2位 | 保険料の引き下げ | 補償額の引き上げ | 支払い条件の透明性向上 | 支払い条件の透明性向上 | 付帯サービスの拡充 |
| 3位 | 特に無し | 支払い条件の透明性向上 | 補償内容の拡充 | 補償内容の拡充 | 補償額の引き上げ |

- 「サイバー保険に加入している」および「加入予定」と回答した企業は、日本では約10%、海外４か国では約60～70%程度であった。
- サイバー保険に対しての不満・課題については、日本では「わからない」と「保険料の引き下げ」という回答が上位を占めていた。一方で、海外４か国では、「補償内容の拡充」「補償額の引き上げ」さらには「付帯サービスの拡充」等、保険に対する具体的なニーズや改善要望が上位を占めていた。
- 日本ではまだサイバー保険に対しての具体的なニーズ・課題が見えていない状況である。一方、海外４か国では、サイバー保険を活用する前提で、保険商品から得られるベネフィットを最大化させようとしているものと考えられる。

## セキュリティ対策の情報開示状況



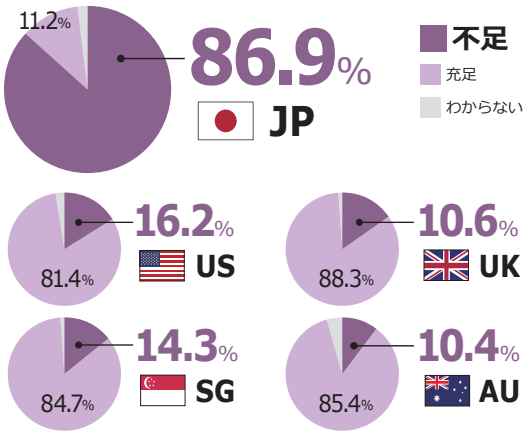

- セキュリティ対策の情報を開示する企業の割合は、日本では約40%であったが、海外４か国では約80%であった。
- 海外４か国では、サイバーセキュリティに関するリスクや、それらへの対応状況について、有価証券報告書等の中で情報開示することが義務付けられていたり、サイバーセキュリティ事故が発生した際に、当局に届け出ることが義務付けられていたりと、国のサイバーセキュリティに対しての姿勢の違いから、このような結果になっているものと考えられる。
- 日本でも総務省が、サイバーセキュリティタスクフォース内に、「情報開示分科会」を設けて、民間企業のセキュリティ対策の情報開示に関する検討を開始している。
- 今後は日本においても、企業が情報開示することで、市場を含む第三者に評価されるような仕組みが構築され、企業は諸外国並みにセキュリティに関する情報開示が求められるようになると予測される。

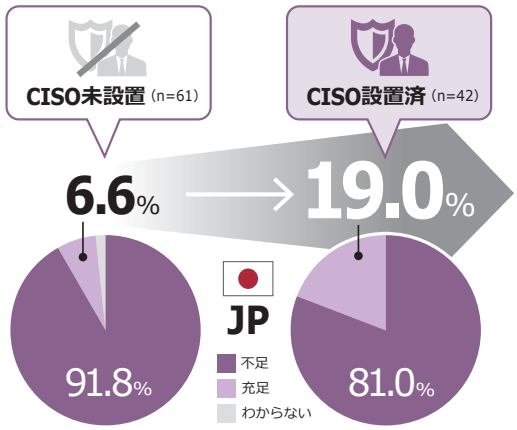
※「公開している」とみなす選択肢：
- 企業のWebサイトの情報セキュリティに特化したページ（情報セキュリティ報告書等）で公開している
- 企業のWebサイトの情報セキュリティ以外のページ（CSR、年次報告書等）で公開している
- 業界団体やISAC等のコミュニティ内で公開・共有している
- 講演会やセミナー等で紹介している、紹介したことがある

# セキュリティ人材

## 日本はセキュリティ人材が圧倒的に不足している。
## 不足解消には人材拡充だけでなく、業務見直しも有効か。

### セキュリティ人材の充足状況




- 海外４か国に比べて日本は圧倒的に人材不足を訴えている。弊社の調査によると日本企業はここ数年変わらず８割以上の企業が人材不足を訴えており※、回復傾向が見られない。

※ NRIセキュア「情報セキュリティに関する実態調査2017（調査対象年度：2014,2015,2016）」

- 日本企業において、CISO設置済/未設置の企業でセキュリティ人材充足状況の差異を分析したところ、CISO未設置企業の方が人材不足を強く訴える結果となった。人材不足解消のためには、CISOのリーダーシップ発揮が有効であると考えられる。

### 充足していると考える理由

（当てはまるもの全て選択）

| | US (n=407) | UK (n=174) | SG (n=178) | AU (n=82) |
|---|---|---|---|---|
| 1位 | 47.9% セキュリティ業務が標準化され、役割分担が明確 | 49.4% セキュリティ業務が標準化され、役割分担が明確 | 54.5% セキュリティ業務が自動化・省力化されている | 53.7% セキュリティ業務が自動化・省力化されている |
| 2位 | 47.2% 経験豊富なメンバで対応 | 48.3% 経験豊富なメンバで対応 | 47.2% セキュリティ業務が標準化され、役割分担が明確 | 43.9% 経験豊富なメンバで対応 |
| 3位 | 39.1% セキュリティ業務が自動化・省力化されている | 42.0% セキュリティ業務が自動化・省力化されている | 47.2% 経験豊富なメンバで対応 | 41.5% セキュリティ業務が標準化され、役割分担が明確 |

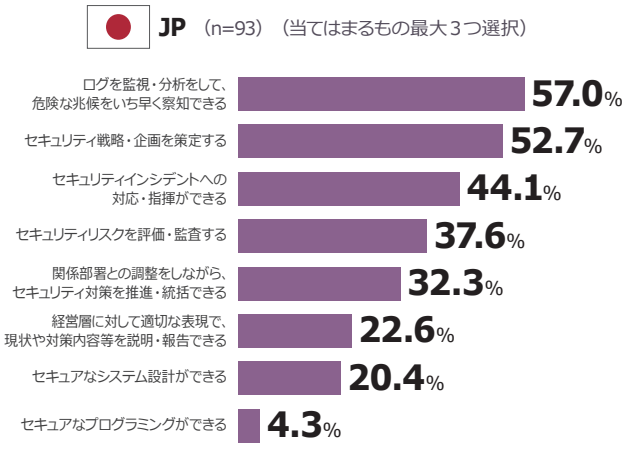
※ 他選択肢：セキュリティ業務量が少ない ／ セキュリティ業務を外部委託している ／ 外部から経験豊富な人材を採用 ／ 社内/グループ内異動で人材を補充

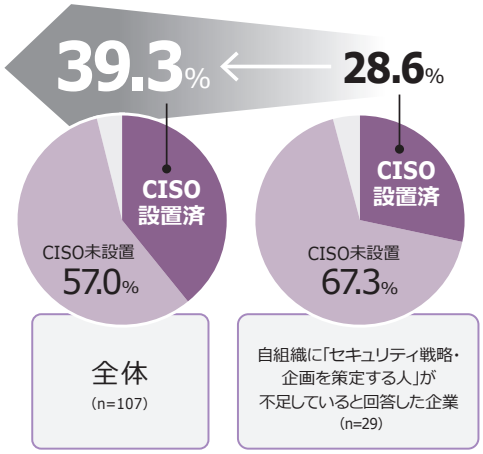
- 海外４か国の「セキュリティ人材が充足している」と回答した企業において、「充足していると考える理由」に対する回答トップ３は同一の内容であった。“人員を増やすための施策”よりも、「業務の標準化」や「業務の自動化・省力化」などにより、“業務を効率的に遂行するための施策”を積極的に行っていることが、セキュリティ人材の充足度に強い影響を与えていることがうかがえる。

- 日本企業においても、「人材不足＝人員の補充」という施策を講ずるだけでなく、業務自体のあり方を見直すこともセキュリティ人材不足の状況を改善するための一手となり得ると考えられる。

# 日本企業はCISO主導で中長期的な人材育成戦略を策定し、必要なキャリアパス整備に取り組むことが重要である。

## 自組織に不足していると考える人材種別




- ログ監視や分析は完全自動化が難しいながらも、機械化・省力化が見込まれる分野なので、自組織人材の育成強化だけではなく、アウトソースの検討も望ましい。
- 一方、セキュリティ戦略・企画の策定は自組織の人材で対応することが求められる。経営目線でセキュリティを考えられる人材の確保は引き続き強化すべきである。
- セキュリティ戦略・企画策定する人材の不足状況をCISO設置済/未設置の差異で分析したところ、戦略・企画を策定する人材が足りないと回答した企業の方が、全体と比べて10pt程度、CISOの設置率が低くなる傾向にあった。
- セキュリティ戦略・企画を策定する上でCISOが果たす役割は大きく、現場部門のみで戦略・企画を策定していくことが難しい状況であると考えられる。

## 人材育成・教育に係る課題

（当てはまるもの全て選択）

| | JP | US | UK | SG | AU |
|---|---|---|---|---|---|
| 1位 | キャリアパス不足 | 37.8% 教育実施の時間の捻出 | 44.2% 専門性の蓄積・継承が困難 | 58.1% 専門性の蓄積・継承が困難 | 43.8% 教育実施の時間の捻出 |
| 2位 | 46.7% 教育実施の時間の捻出 | 37.4% 専門性の蓄積・継承が困難 | 37.1% 教育実施の時間の捻出 | 49.5% 教育実施の時間の捻出 | 38.5% 教育実施の予算の確保 |
| 3位 | 38.3% 能力・スキル要件が不明 | 31.8% 教育実施の予算の確保 | 31.5% 能力・スキル要件が不明 | 43.8% 能力・スキル要件が不明 | 33.3% 専門性の蓄積・継承が困難 |

68.2%

- 日本が突出してキャリアパス不足を訴える結果となった。海外諸国と比べて平均勤続年数が長い日本においては、キャリアアップの道筋が見えないことは要員のモチベーション低下等を引き起こす可能性があるので、キャリアパス整備に取り組むべきである。
- その際は、闇雲に取り組むのではなく、CISO相当の人材が人材育成戦略の全体像を描き、自社の事業特性や今後の経営戦略を踏まえて必要な人材を中長期的に育成していくことが重要である。

# 標的型攻撃、ランサムウェアが５か国全てで恐れられる脅威。内部不正などの社内のリスク意識には差異あり。

## 自社で最も脅威となる事象

（当てはまるもの最大３つ選択）

| | JP | US | UK | SG | AU |
|---|---|---|---|---|---|
| 標的型攻撃による情報漏えい | 1位 66.4% | 1位 45.8% | 1位 48.7% | 1位 54.8% | 1位 44.8% |
| ランサムウェアによる被害（情報消失、金銭被害） | 2位 57.9% | 2位 38.2% | 2位 40.6% | 2位 48.1% | 2位 38.5% |
| 内部不正による被害 情報漏えいや業務停止 | 3位 52.3% | 4位 25.2% | 7位 21.8% | 5位 22.9% | 3位 30.2% |
| ビジネスメール詐欺（BEC）による金銭被害 | 4位 21.5% | 5位 23.8% | 4位 31.5% | 3位 35.2% | 7位 19.8% |
| 情報機器、社員証等の置き忘れ、棄損による情報漏えい | 5位 20.6% | 8位 18.4% | 9位 6.6% | 10位 9.5% | 10位 6.3% |
| メールの誤送信・誤配信 | 6位 19.6% | 10位 8.2% | 10位 6.1% | 9位 10.6% | 9位 9.4% |
| サービス妨害攻撃（DDoS攻撃等）によるサービス停止 | 7位 15.0% | 3位 34.6% | 3位 36.5% | 3位 35.2% | 3位 30.2% |
| 退職者、転職者による在職時に利用していた情報の使用 | 8位 12.1% | 9位 18.0% | 8位 15.7% | 8位 16.2% | 8位 14.6% |
| Webサイトの改ざん | 9位 7.5% | 7位 19.2% | 6位 23.4% | 6位 22.4% | 5位 29.2% |
| 自社Webサービスへのリスト型アカウントハッキング被害 | 10位 3.7% | 6位 22.4% | 5位 25.4% | 6位 22.4% | 6位 22.9% |

※ 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、５か国全てで、「標的型攻撃による情報漏えい」が１位、「ランサムウェアによる被害」が２位に挙がっている。
- 2017年はランサムウェアによる攻撃が世界的に報道され、引き続き標的型攻撃による情報漏えいも各国で話題に挙がっていることから、世界共通のセキュリティ脅威として認識されている状況がうかがえる。
- 日本の３位は「内部不正による被害」であり、日本企業のおよそ２社に１社が脅威と考えている。順位ではオーストラリアも上位に挙がっているが、割合では４社に１社程度であり、日本企業と比較して脅威認識が低いといえる。国内の脅威認識の高さは、過去大きく報道された情報漏えい事件が影響していることも考えられる。
- 一方で日本企業では、「サービス妨害攻撃（DDoS）」、「Webサイトの改ざん」や「自社Webサービスへのリスト型アカウントハッキング被害」等のサイバー攻撃の脅威認識は低い。その理由として、日本企業は内部不正への脅威認識が高いことや、攻撃対象となるサービスを自社で利用・提供していないケースが海外４か国と比べ多いこと等が考えられる。

# 日本では「ヒューマンエラー」による事故が多く、海外４か国ではマルウェア等の「サイバー攻撃」による事故が多い。

## 過去１年で発生した事件・事故

（当てはまるもの全て選択）

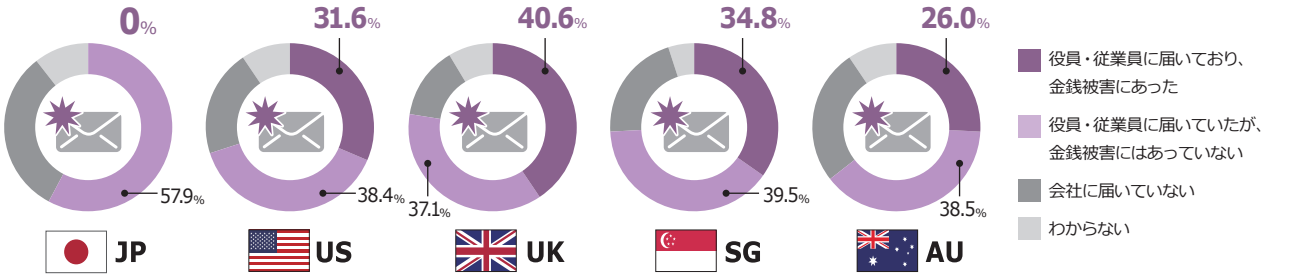
| | JP | US | UK | SG | AU |
|---|---|---|---|---|---|
| 1位 | 電子メール、FAX、郵便物等の誤送信・誤配送 | マルウェア感染 | システム基盤の脆弱性を突いた攻撃 | マルウェア感染 | マルウェア感染 |
| 2位 | 情報機器・外部記憶媒体の紛失・置き忘れ・棄損 | DoS攻撃／DDoS攻撃【※1】 | DoS攻撃／DDoS攻撃【※1】 | システム基盤の脆弱性を突いた攻撃 | システム基盤の脆弱性を突いた攻撃 |
| 3位 | マルウェア感染 | システム基盤の脆弱性を突いた攻撃 | Webアプリケーションの脆弱性を突いた攻撃 | Webアプリケーションの脆弱性を突いた攻撃 | 情報機器、電子記憶媒体、紙媒体等の盗難 |
| 4位 | 標的型メール攻撃【※3】 | Webアプリケーションの脆弱性を突いた攻撃 | 標的型メール攻撃【※3】 | DoS攻撃／DDoS攻撃【※1】 | 特になし |
| 5位 | ランサムウェアによる金銭等の要求【※4】 | 標的型メール攻撃【※3】 | マルウェア感染 | 自社サービスへのリスト型アカウントハッキング【※2】 | Webアプリケーション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 | 自社サービスへのリスト型アカウントハッキング【※2】 | 自社サービスへのリスト型アカウントハッキング【※2】 | 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 | 自社サービスへのリスト型アカウントハッキング【※2】 |
| 7位 | システム設定ミス、誤操作 | 特になし | 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 | 電子メール、FAX、郵便物等の誤送信・誤配送 | DoS攻撃／DDoS攻撃【※1】 |
| 8位 | 特になし | 情報機器、電子記憶媒体、紙媒体等の盗難 | 情報機器、電子記憶媒体、紙媒体等の盗難 | 標的型メール攻撃【※3】 | 電子メール、FAX、郵便物等の誤送信・誤配送 |

ヒューマンエラー
サイバー攻撃
盗難

【※1】DoS攻撃はDenial of Service attackの略。ネットワーク経由で大量のパケットの送信や不正な入力をし、サービスを停止に追い込む攻撃。DDoS攻撃はDistributed Denial of Service attackの略。ネットワーク上に分散したコンピュータを踏み台として行うDoS攻撃。
【※2】複数のサービスで同一IDとパスワードを設定していることを悪用し、パスワード流出したサービスのパスワードリストで他のサービスへの不正アクセスを行う攻撃。
【※3】特定の企業や組織を狙い、巧妙に偽装されたメールを送り、マルウェアに感染させることで情報を漏えいさせる攻撃。
【※4】PC上のデータやシステムへのアクセスを制限し、その制限の解除に金銭を要求するマルウェア。
＊ 回答選択肢のうち、以下の項目についてはいずれの国も9位以下のため本表には掲載していない。
「退職者、転職者による在職時に利用していた情報の使用」「データ通信、音声通信等の盗聴・傍受」「水飲み場型攻撃」「業務アクセスが可能な一般ユーザによる不正アクセスや持出」「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」「ショルダーハックによる盗み見」「Web（SNS、掲示板等）への重要情報のアップロード」

- 過去１年で発生した事件・事故として、海外４カ国では、脅威認識として上位に挙がった「マルウェア感染」などのサイバー攻撃が多く、日本は「誤送信」や「設定ミス」などのヒューマンエラー関連の事象が上位に挙がっていることが特徴的である。５か国共通で脅威認識として上位に挙がったランサムウェアは日本のみ５位にランクインした。
- 一方で海外４か国と比較して日本では「システム基盤やWebアプリケーションなどへのサイバー攻撃」が発生したと回答した企業が少ない。これは所有システム数や事故に対する認識の違い等が影響していると考えられる。加えて、これらのサイバー攻撃はランサムウェア感染と比較すると気づきにくいため、被害に気づいていない企業が存在する可能性もある。

## ビジネスＥメール詐欺



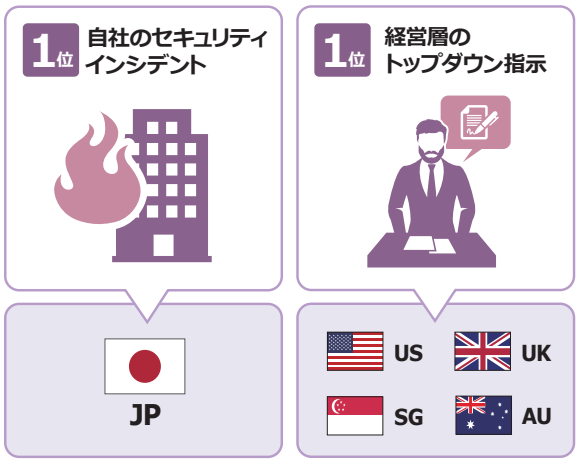

- 今回の調査対象の日本企業においては、半数以上の企業でビジネスＥメール詐欺と思われるメールを受信しているが、金銭被害が発生したという回答はなかった。ビジネスＥメール詐欺に関する攻撃の成功有無は、攻撃者にとっての言語障壁も関係していると考えられる。
- 日本企業では、海外グループ会社や海外取引に関わる被害事例が報道されている。IT側の技術的な対策だけでは、ビジネスＥメール詐欺の検知・対応は困難であるため、ビジネス部門やコーポレート部門も含めた企業グループ全体でのチェック機能が必要である。

# セキュリティ対策

## 海外４か国は経営層のトップダウンにより対策を進め、定期的な評価や有事に備えた体制構築も実施している。

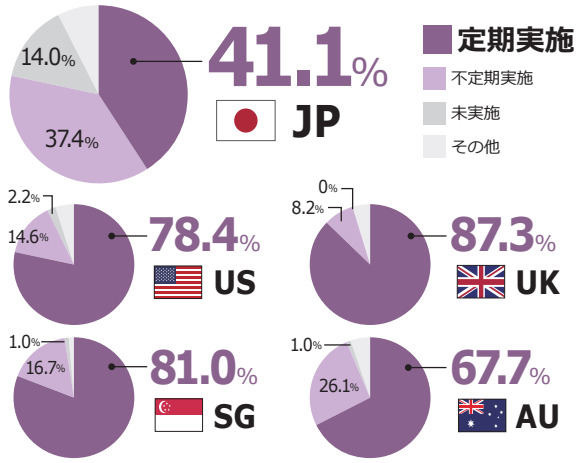
### 情報セキュリティ対策実施のきっかけや理由

（当てはまるもの最大３つ選択）



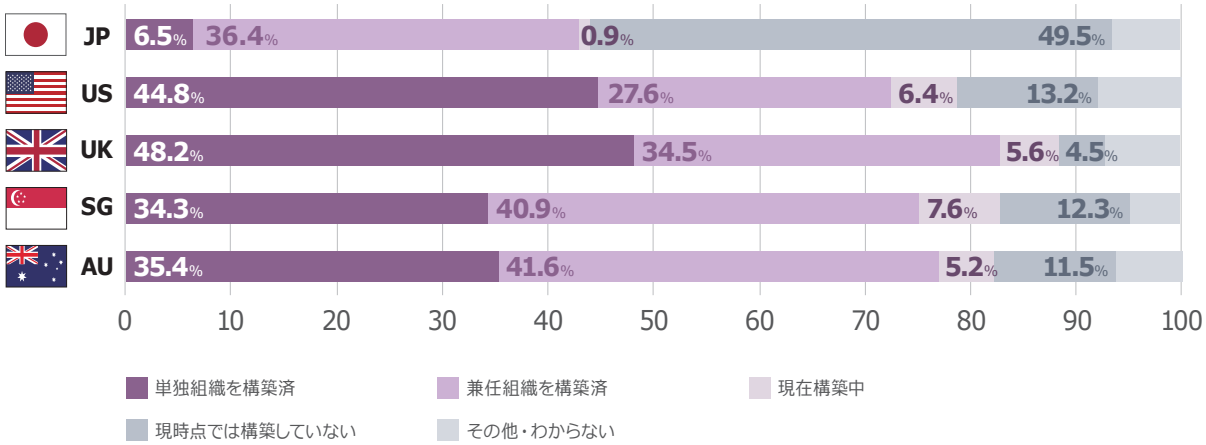

- 海外４か国の１位は共通して「経営層のトップダウン指示」であった。日本の１位は「自社のセキュリティインシデント」であり、”インシデントが発生してから対応する” というイベントドリブン型な企業の割合が高かった。

### セキュリティ対策評価の実施状況




- 海外４か国は各国65%以上の企業が定期的に対策評価を実施しているが、日本は約40%であった。また、評価未実施と回答した企業も14%に上った。
- インシデント発生後に対応する場合でも、定期的な評価により自社の現状を把握できているか否かで対応のスピードと正確性に大きな差が生じる可能性が高い。

### CSIRTの構築状況

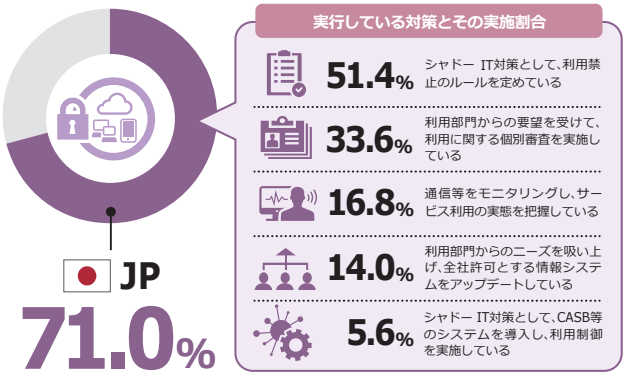



- 海外４か国企業の40%前後がCSIRTを単独組織で構築しており、兼任組織も含めれば70%以上の企業がCSIRTを構築済という結果となった。
- 日本企業の単独組織での構築率は6.5%と、海外４か国と比べると低い結果となった。また、現時点では構築していない企業は49.5%であり、2社中１社はCSIRTを構築していない実態が明らかとなった。
- “情報セキュリティ対策実施のきっかけや理由” の分析結果を踏まえると、日本は「インシデント発生を起因として対策を実施するが、次のインシデント発生に備えた体制作りはできていない」という企業が多いのではないかと考えられる。

# 日本のセキュリティ担当者はインシデント対応に疲弊気味。最新技術の活用などで業務の効率化を目指すべき。

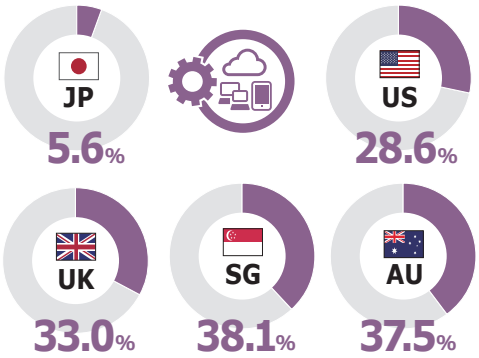
## シャドーIT対策を実施している企業

（当てはまるもの全て選択）




- 日本企業の70%以上がシャドーIT対策を実施している。
- 一方で、通信等のモニタリングやシステムによる利用制御の実施割合は低く、ルールや利用プロセスの整備により対策を行う企業の割合が高いことが明らかとなった。

## シャドーIT対策としてCASB等のシステムを導入している企業




- 日本企業におけるCASB等導入率は海外4か国企業と比較すると低く、5%程度の導入率であった。
- 働き方改革やビジネスのデジタル化に伴いシャドーITの脅威が増す中で、CASB等のシステム導入をシャドーIT対策の一つの選択肢として検討することが望ましい。

## 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 | UK | SG | AU |
|---|---|---|---|---|---|
| 1位 | セキュリティインシデント発生時の緊急対応 | セキュリティ対策のトレンド・他社動向の把握 | セキュリティ対策のトレンド・他社動向の把握 | セキュリティ対策のトレンド・他社動向の把握 | セキュリティ対策のトレンド・他社動向の把握 |
| 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） | 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 | セキュリティ脅威・事故に関する情報収集と関係者共有 | セキュリティ脅威・事故に関する情報収集と関係者共有<br>セキュリティインシデント発生時の緊急対応 |
| 3位 | グループ会社・国内外拠点のセキュリティ統制・管理<br>サイバー攻撃の高度化への対応 | セキュリティ脅威・事故に関する情報収集と関係者共有 | セキュリティ業務の状況・進捗に関する経営層への報告 | セキュリティインシデント発生時の緊急対応 | サイバー攻撃の高度化への対応 |

※ 他選択肢：その他 ／ 困っていることはない

- 日本の1位は「セキュリティインシデント発生時の緊急対応」であった。前頁の”CSIRTの構築状況”で分析した通り、日本企業のCSIRT構築率は海外4か国企業と比べると低く、故に5か国で唯一困っていることの1位になったと考えられる。
- 一方で、CSIRT構築率が日本より高いアメリカ・シンガポール・オーストラリアの上位にも「セキュリティインシデント発生時の緊急対応」が選ばれている。また、海外4か国上位の「セキュリティ脅威・事故に関する情報収集と関係者共有」はCSIRTの平時の活動における悩みであると推察される。日本企業もCSIRTを構築して終わりではなく、有効に機能させるための運営方法まで確立することが望ましい。
- 海外4か国の1位は共通して「セキュリティ対策のトレンド・他社動向の把握」であった。業界のトレンドを把握することでセキュリティ業務効率化のヒントを得られる可能性があるため、コミュニティなどを活用したトレンド把握に努めることは有用であると考える。

Secure SketCH


Cross analysis result

# Secure SketCHとの クロス分析結果

## Secure SketCH とは

NRIセキュアが提供するセキュリティ対策実行支援プラットフォームサービスです。企業のセキュリティ対策状況を「見える化」し、戦略的な対策実行をサポートします。

詳細は以下をご参照ください。
**https://www.secure-sketch.com/**

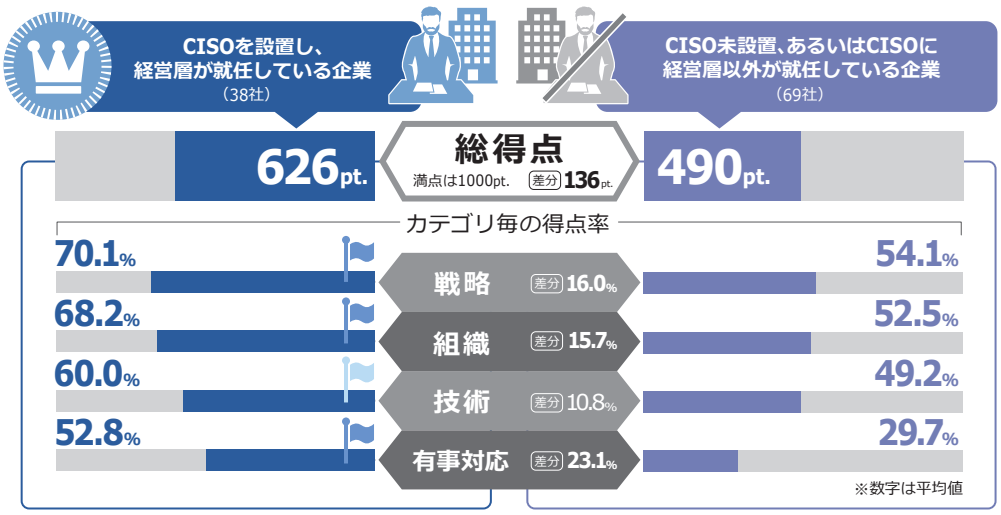
### ● クロス分析概要

アンケートの回答と、Secure SketCHのデータを突き合わせて、日本企業に関する更なる分析を行った結果を記載します。

**Secure SketCHのデータ：**
日本企業107社（アンケートの調査対象と同様）

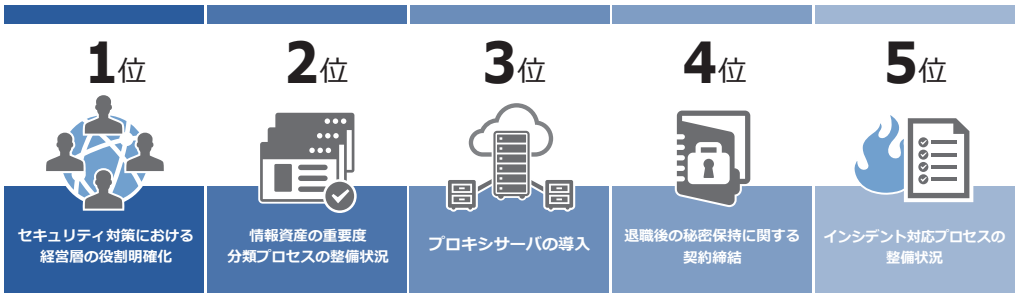
# 経営層がセキュリティに関与することで、企業のセキュリティ対策レベルの向上が期待できる。

## 「セキュリティへの経営層の関与」と「Secure SketCHの評価結果」の関連性




- 経営層がセキュリティに関与する企業の方が、そうでない企業と比較して、セキュリティ対策全体のスコア、並びに全カテゴリでの得点率が高いという結果であった。特に平均総得点は136pt.もの差がついている。
- カテゴリ毎の実施率では、「技術」が10.8%で比較的差が小さく、「有事対応」「戦略」「組織」がそれぞれ23.1%、16.0%、15.7%と差が大きくなった。
- 「技術」に関する対策は、現場主導でもある程度実行可能であることに対して、「有事対応」や「戦略」のカテゴリについては、体制作りやポリシー整備等、組織横断的な施策になること多い。
- したがって、人的リソースの再配置や、トップダウンでの指示が必要なケースが多く、経営層が関与している企業の方が、効率的・効果的に施策が推進できているものと考えられる。

## セキュリティに経営層が関与している / していない企業間で、Secure SketCHの得点率の差が大きかった対策



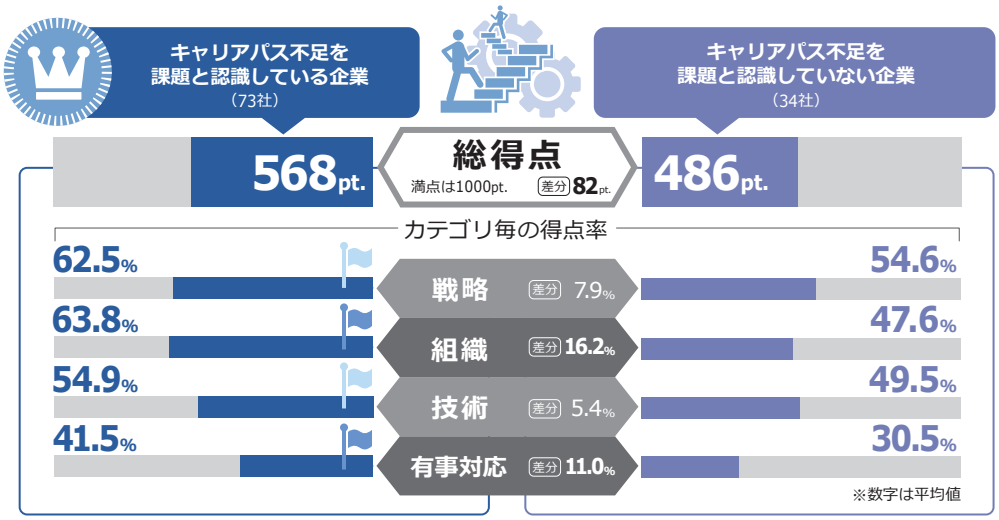

- 「セキュリティ対策における経営層の役割明確化」が1位となった。セキュリティに対して、経営層が関与し業務を統括している企業では、経営層も含めたエスカレーションフローや役割分担が定義されていることが多い。

  経営層がリーダーシップを発揮して、セキュリティ対策を推進していく、あるいは迅速な有事対応をしていくためには、現場部門のみならず経営層も含めた、役割の明確化が欠かせない。
- 次に、「情報資産の重要度分類プロセスの整備状況」が続いた。情報資産を重要度別に分類する際は、全社に点在する情報資産にどのようなものがあるのか、そして、それらが漏えいしてしまった場合に、どのようなインパクトがあるか、などを考慮する必要がある。

  全社的にこれらの施策を推進するためには、自社の事業を俯瞰できる高い視点からの分析が必要であり、経営層の関与が結果に影響したものと推測される。

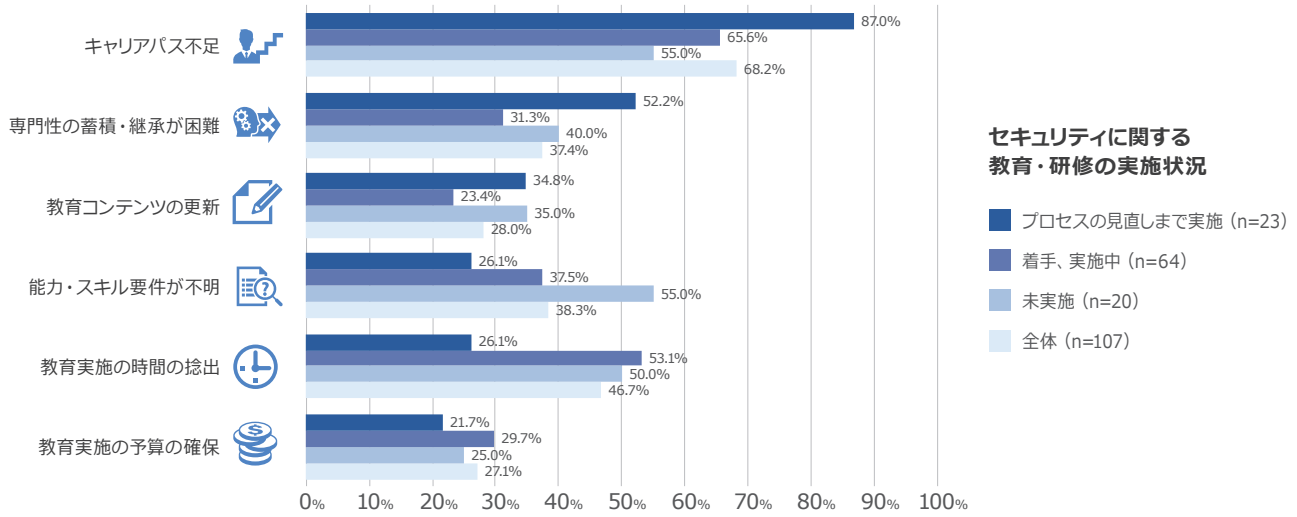
# セキュリティ人材不足状況の打破には、各社が現状を正確に把握し、解消のための施策を見極める必要がある。

## 「キャリアパス不足が課題」と「Secure SketCHの評価結果」の関連性




- キャリアパス不足を課題と認識している企業が、していない企業に比べて全体的にスコアが高い結果となった。なかでも、人材育成の実施状況等を問う「組織」のカテゴリでは得点率で15%以上という差がついた。
- キャリアパス不足が課題と認識している企業の方がスコアが低くなることを当初予想していた。そうではなく、キャリアパス不足に課題を感じ、セキュリティ人材の待遇改善に取り組もうとしている企業こそ、その他対策も同様に取り組んでいると考えられる。

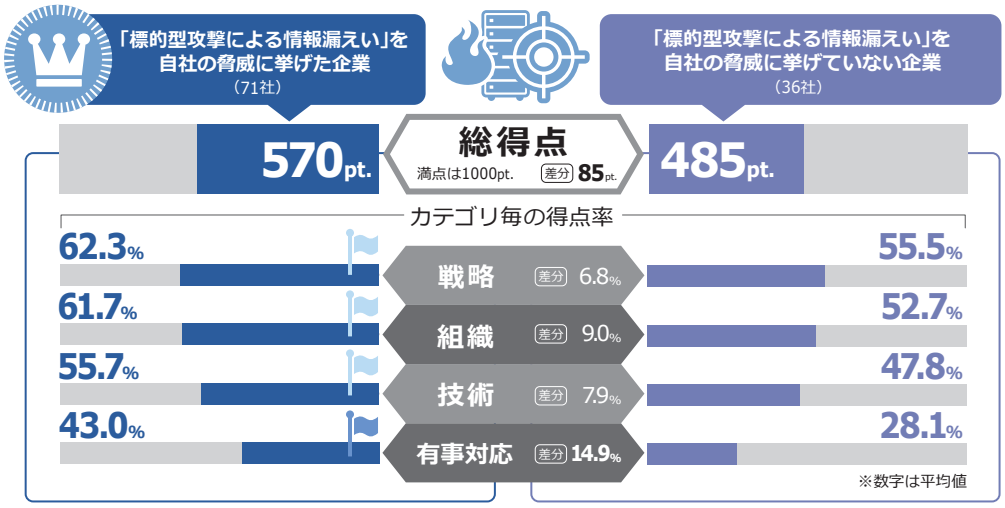
## 「人材育成・教育に係る課題」と「セキュリティに関する教育・研修の実施状況」の関連性




- 「人材育成・教育に係る課題」を「セキュリティに関する教育・研修の実施状況」別に分析した結果、教育のプロセスが成熟している企業こそキャリアパス不足を強く訴える結果となった。
- まだ教育プロセスが未実施な企業においては、キャリアパス不足に加え、スキル要件の定義や時間捻出も課題と感じており、教育実施以前の制度設計が求められる。

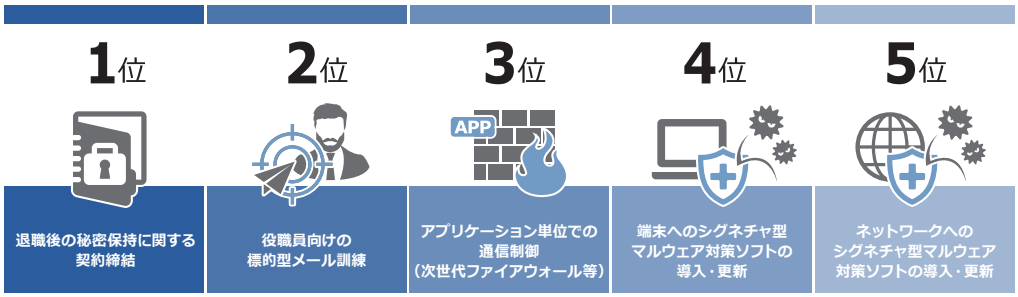
# 標的型攻撃を脅威と考える企業は特に「有事対応」を強化すべき。攻撃されることは前提であり、被害を最小限にする対策が必要である。

## 「標的型攻撃による情報漏えいを脅威と挙げた／挙げていない」と「Secure SketCHの評価結果」の関連性




● 「標的型攻撃による情報漏えい」を自社の脅威に挙げた企業が、そうでない企業と比較して、セキュリティ対策全体のスコア並びに、全カテゴリでの得点率が高いという結果であった。カテゴリごとでは特に有事対応に14.9%の差がついている。

## 標的型攻撃による情報漏えいを脅威に挙げている／挙げていない企業間で、実施率の差が大きかった対策

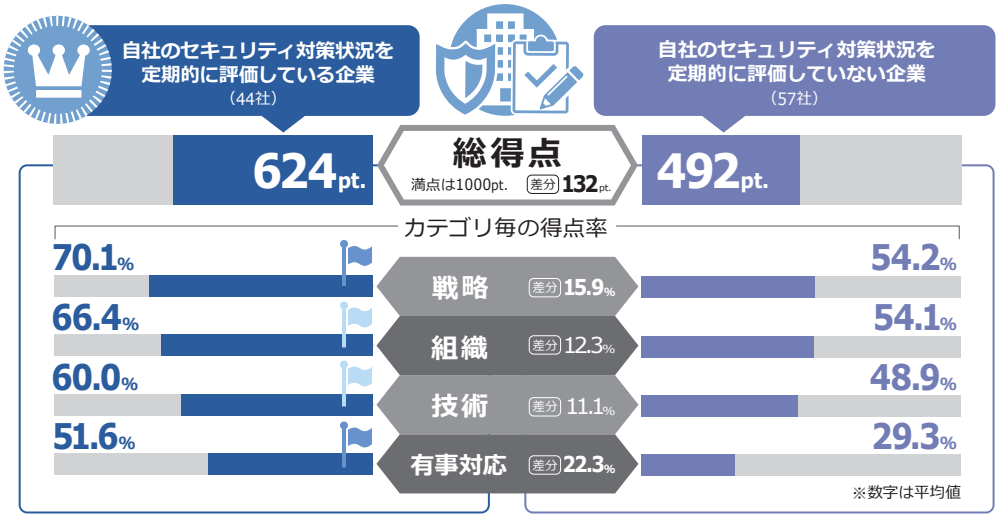



● 標的型攻撃による情報漏えいを脅威に挙げている／挙げていない企業間で実施率の差が大きかった対策を分析すると、標的型攻撃の過程で攻撃手段としてもちいられることの多い「標的型メール」による被害を低減するための役職員向けの標的型メール訓練や、ネットワークを経由した端末遠隔操作や情報の漏えいを防ぐための通信制御、そして端末・ネットワークでのマルウェア対策ソフト導入などの技術的対策が実施されていることがわかる。

● 昨今の標的型攻撃ではOS標準のコマンドや正規のアプリを利用してエンドポイントを不正に操作し、情報の持ち出し等を行うケースもある。また、痕跡を残さない攻撃も増加し、仮に攻撃を防ぐことができなかった場合の被害調査や説明責任を果たすことが難しいこともある。標的型攻撃による情報漏えいを脅威として認識する企業においては、攻撃を防ぐ対策に加えて、マルウェア感染を想定した端末ログ取得・制御機能などの攻撃による被害を最小限に抑える対策も有効と考える。

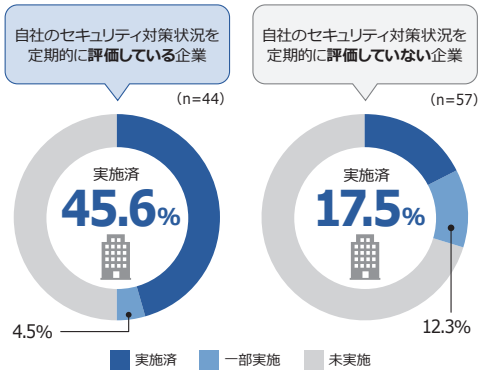
# セキュリティにおける経営層の役割を明確化する企業は、定期的な評価により対策レベルを向上させている。

## 「対策評価の実施状況」と「Secure SketCHの評価結果」の関連性



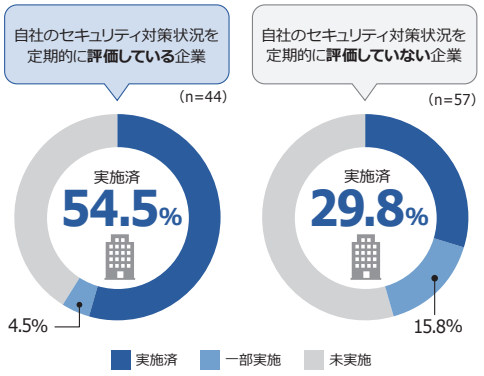

- 自社のセキュリティ対策状況を定期的に評価している企業が、していない企業に比べて全体的にスコアが高い結果となった。なかでも、「戦略」と「有事対応」のカテゴリでは得点率で15%以上という差がついた。
- 自社のセキュリティ対策状況を定期的に評価することはセキュリティ戦略を策定する上で重要であり、「戦略」カテゴリ全般の得点率が高くなったと考えられる。
- 定期的な評価を実施していない企業の「戦略」と「有事対応」の得点率は2倍近い差が生じており、局所的な対策実施となっていないか懸念が残る。全体的なセキュリティレベルの底上げには、自社の対策状況の把握が有効であると考える。

## 「セキュリティにおける経営層の役割明確化」の状況




- 定期的な評価を実施している企業の方が、経営層の役割を明確化し、経営層がセキュリティ業務に積極的に関与している割合が高かった。セキュリティに関与する経営層に対し現状を適宜報告するため、あるいは、経営層主導で策定されたセキュリティ中長期計画に含まれるため、定期的な評価を行う企業が多いのではないかと推察する。

## 「事業特性を踏まえたセキュリティリスクの特定」の状況




- 定期的な評価を実施している企業の方が、事業特性を踏まえたセキュリティリスクを特定している割合が高かった。定期評価を実施する企業の半数以上は、自社のビジネス形態・特性を考慮したセキュリティリスクの特定を行うことで、定期評価の有効性を高めている。

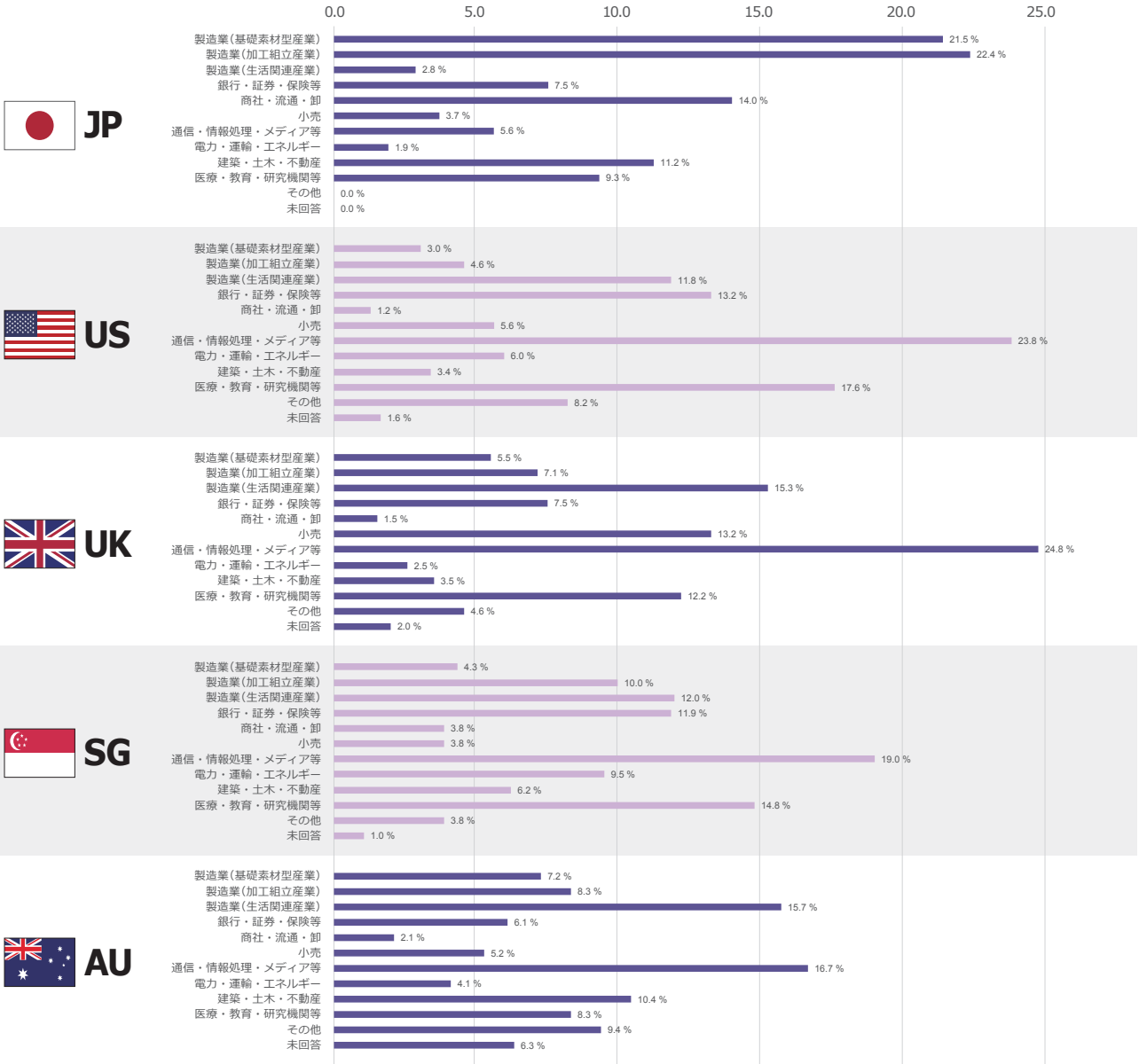
# 回答者属性

**回答企業社数：**合計 1,110社（JP 107社、US 500社、UK 197社、SG 210社、AU 96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・上場/未上場・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

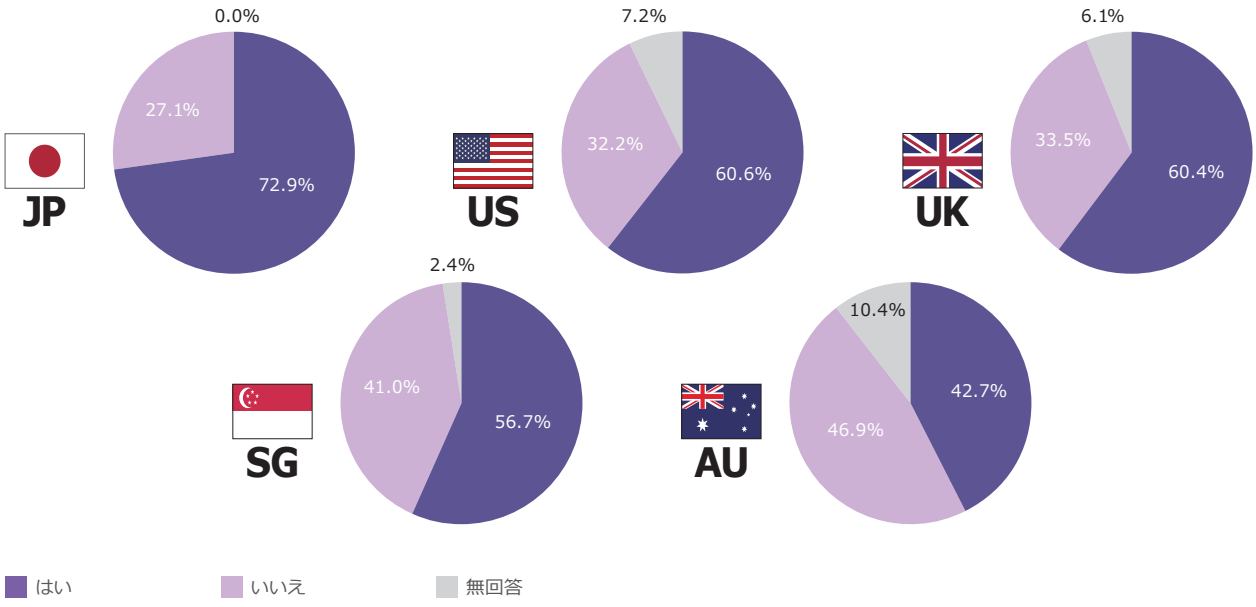
- 製造業（基礎素材型産業）：紙・パルプ、化学、鉄鋼・金属
- 製造業（加工組立産業）：機械・精密機器、電気機器、自動車製造業
- 製造業（生活関連産業）：食品、繊維・アパレル、医薬、その他の製造業
- 銀行・証券・保険等：銀行、証券、保険、その他金融
- 通信・情報処理・メディア等：コンサルティング・シンクタンク、マスコミ・出版・印刷・広告、情報処理・ソフトウェア・SI、ISP・CATV・x DSL事業、通信・放送
- 電力・運輸・エネルギー：電力、石油・ガス、鉄道・航空、運輸
- 建設・土木・不動産：建設・土木・不動産、農林水産漁業・鉱業
- 医療・教育・研究機関等：医療、福祉、教育・研究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

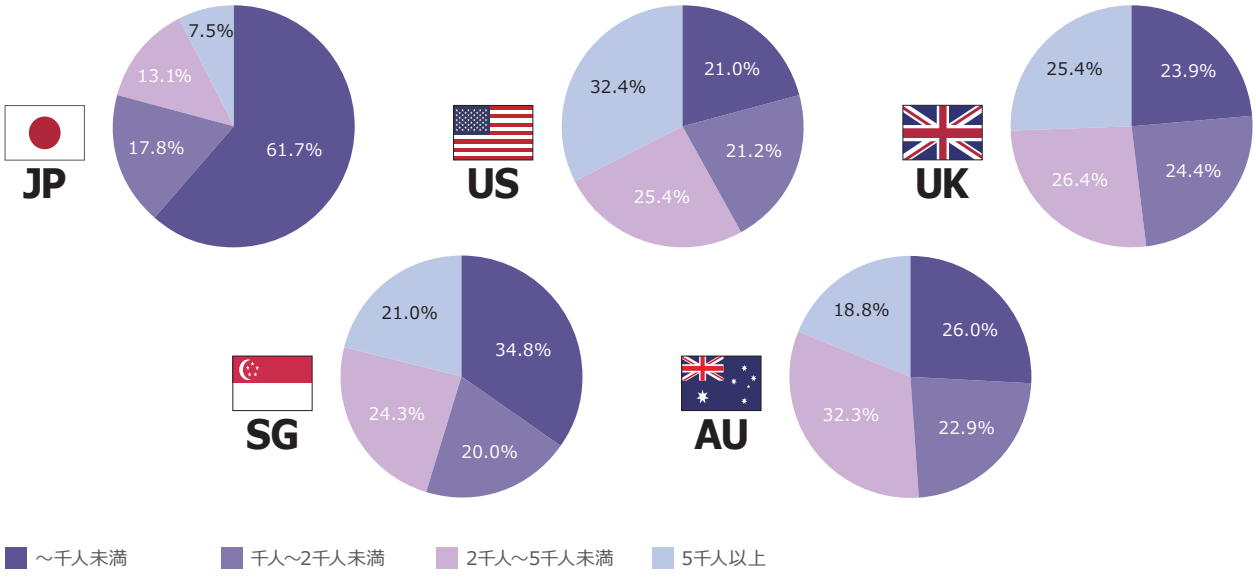
## 回答いただいた企業の上場割合

貴社は株式上場していますか。以下の中から当てはまるものを１つお選びください。




## 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、イギリス、シンガポール、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、イギリス、シンガポール、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

## 調査時期

**日本 ：** 2018/3/14 ～ 2018/3/29

**アメリカ、イギリス、シンガポール、オーストラリア：**
2017/12/6 ～ 2017/12/22

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。
- 特に明記していない限り、調査ベースは全回答者（日本 107 社、アメリカ 500 社、イギリス 197 社、シンガポール 210 社、オーストラリア 96 社）です。

**お問い合わせ先**
info@nri-secure.co.jp

# PROJECT MEMBER

## 制作委員

| | | | |
|---|---|---|---|
| **制 作** | NRI Secure Insight 2018<br>制作委員会 | | |
| **執 筆** | 山田 智隆 | | |
| **企 画** | 渡部 惣 | 川崎 聡太 | 森 茉莉香 |
| | 山本 直実 | 名部井 康博 | |
| **アドバイザー** | 菅谷 光啓 | 山口 雅史 | 十川 基 |
| | 金子 洋平 | 正田 真教 | |
| **監 修** | 足立 道拡 | | |

# 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<br>TEL（代表）：03-6706-0500 |
| **北米支社** | 26 Executive Park Suite 150 Irvine CA 92614 U.S.A.<br>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** | 385 名 |

（2018 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日本において
**16**年に渡り実施しています

16 年間の調査を通じ、のべ
**9,770** 社の回答
をいただきました

## 資格取得者数※
（社員数：385 名）

| | |
|---|---|
| **87** 名 **CISA**（公認情報システム監査人） | **43** 名 **CISM**（公認情報セキュリティマネージャー） |
| **38** 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） | のべ **185** 名 **GIAC**（Global Information Assurance Certification） |

*2018/04/01 時点

## サービス概要


NRI セキュアテクノロジーズはマネジメントとテクノロジーの両面から、お客様の信頼出来るパートナーとして情報セキュリティに関するあらゆる脅威に立ち向かいます。

グローバルにサービスとソリューションを提供しています。

## サービスの主要提供先

- 金 融
- 製 造
- IT・通信
- 官公庁
- 製 薬
- マスコミ

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