



## サマリー

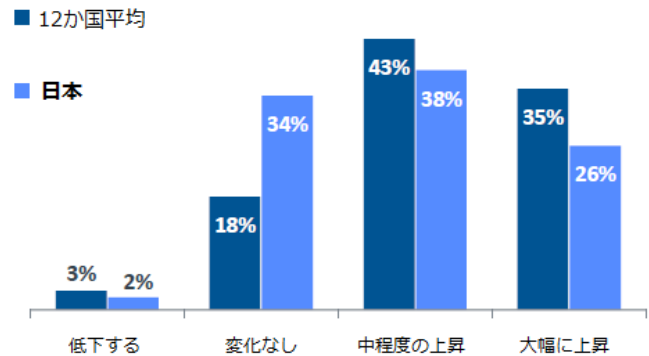
IT セキュリティの重要性はますます高まっています。本調査で対象となる 12 か国全体を見た場合、セキュリティを担当するマネージャ 10 人中約 8 人が、今後 2 年間に於けるセキュリティの重要性はさらに上昇すると予測しています（79% - 中程度に上昇 + 大幅に上昇の合計）。大幅に上昇すると予測した回答者は特に、マチュアリングエコノミー（経済が成熟過程にある市場）に多く見られ（86%）、マチュアエコノミー（経済が成熟している市場）をしのご結果となりました（68%）。日本では、企業の 3 分の 2 近くが、IT セキュリティの重要性の上昇を予測しています（64%）。

IT は常に変化することから、組織の大部分はセキュリティへの取り組み方を変えざるを得ません。日本も他国同様に「IT オペレーションの変化」がセキュリティの取り組みを見直す最大の要因となっています。これは企業のクラウドへの移行や、モビリティ戦略の実施が影響しています。

また、「企業内部のセキュリティ違反」もセキュリティを見直す大きな要因となっています。さらには、調査対象の国全体を見た際、4 分の 3 近くが、過去 12 か月間に少なくとも一度のセキュリティ違反/インシデント（内部または外部による）を経験していることが分かりました（73%）。

## サイバーセキュリティの重要性

2年後の状況を予測



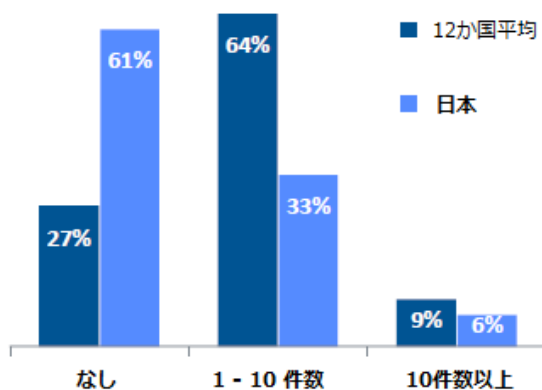
64%

今後2年間に於いて、  
日本の企業ではセキュリティが大いに重要視されます



## セキュリティ違反の発生件数

過去12か月



## サイバーセキュリティへの取り組みを見直すきっかけとなった要因とは？

※日本企業間のデータ

1. IT オペレーションの変化（クラウド、モビリティなど）
2. 企業内部のセキュリティ違反やインシデント
3. 他社で発生したセキュリティ違反の報告
4. 外部第三者により発見された脆弱性
5. トレーニング/認定資格による知識の習得から

※マチュアリング/マチュアエコノミーのカテゴリについては最終頁に記載しています。

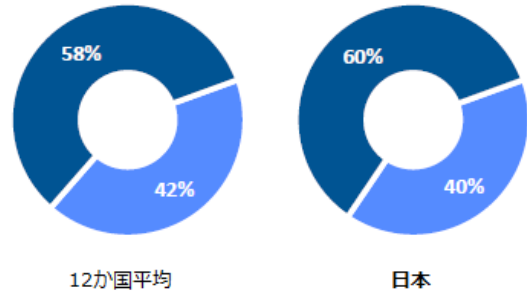


日本企業の10社中4社は、少なくとも1度のセキュリティインシデントを経験しており、5分の1をわずかに上回る企業では、重要な違反に分類される違反を経験しています。多くの企業では、「人為的エラー」が、セキュリティ違反の要因となっており、特に経済が成熟過程にあるマチュアリングエコノミーの企業で多く見られます（64%）。日本においても、2年前の調査結果からの上昇が見られ、半数以上（59%）が、人為的エラーを根本要因としています。

良いニュースは、調査では、10社中9社が何らかのセキュリティトレーニングを導入している点です。新入社員オリエンテーション、継続的なトレーニングプログラム、ランダムに実施されるセキュリティ監査、オンラインコースなどにより、従業員のセキュリティ知識の獲得または改善を行っています（92% 全体のデータ vs. 86% 日本のデータ）。また、大半のマネージャは、ITセキュリティトレーニングで得た知識を確実にするため、トレーニング後の試験実施が重要と回答しています。さらに、マチュアリングエコノミーの企業では、ITセキュリティ認定資格が非常に有効と回答しています（49% vs. 25% マチュアエコノミーの回答）。日本では、3分の2近くのマネージャが、「セキュリティに関連した知識/スキルを評価する」または「志願者を評価する」などの点において、ITセキュリティ認定資格は、非常に有効（13%）または有効（47%）と回答しています。

## 人為的エラーは、セキュリティリスクの大きな要因に

■ 人為的エラー ■ 技術的エラー

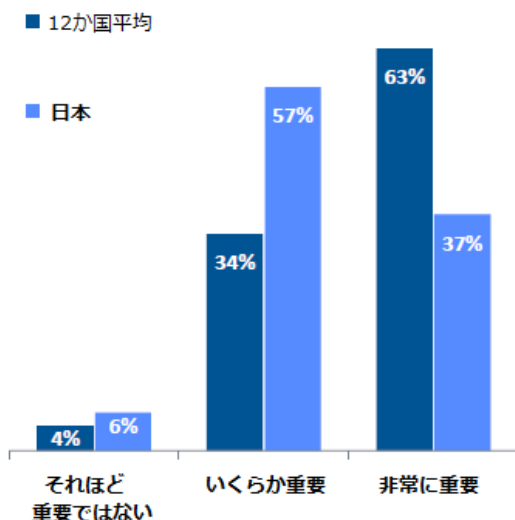


## 人為的なサイバーセキュリティエラーが発生してしまう主要因とは？

※日本企業間のデータ

1. 全体的な不注意
2. 新たな脅威を把握できていない
3. 故意によるセキュリティ機能の無効化
4. 脅威を管理するためのリソースが不十分/時間が取れない
5. ネットワーク、サーバー、その他インフラに関するセキュリティ知識の欠如
6. エンドユーザーによるセキュリティポリシーや手順の不履行

## サイバーセキュリティトレーニング後の試験実施の重要性



60%

モバイル関連のセキュリティインシデントを経験したことのある日本企業の割合

上位インシデントには、デバイスの紛失、データポリシー違反、モバイルフィッシング攻撃など





## 調査方法

CompTIA International Trends in Cybersecurity (サイバーセキュリティの国際的な傾向) 調査は、対象となった 12 か国での IT セキュリティにまつわる行動、テクニック、機会に関する定量的情報を収集し共有するために実施されました。詳しい情報はこちらよりご覧いただけます。

<https://www.comptia.org/internationalsecurity>

1,509 名の IT およびビジネスエグゼクティブが、2016 年 1 月から 2 月に実施されたオンラインアンケートに参加。本調査は信頼度 95% で、プラスマイナス 2.5% のサンプリング誤差としています。

CompTIA は、Marketing Research Association のメンバーで、調査のベストプラクティスや倫理が記されたガイドラインを順守しています。

CompTIA は本調査の全ての内容に責任を負うものとしてます。調査に関するいかなる質問は CompTIA Research and Market Intelligence のスタッフまでお問合せください。 [research@comptia.org](mailto:research@comptia.org)

## 調査参加者の役職と割合

- 22% エグゼクティブマネージメント (CEO, プレジデント, オーナー他)
- 23% シニアマネージメント - IT 部門 (CIO, CSO, VP 他)
- 10% ミドルマネージメント - IT 部門 (ディレクタ, VP 他)
- 11% スタッフレベル - IT 部門
- 21% シニアマネージメント - ビジネス部門 (CFO, VP 他)
- 6% ミドルマネージメント - ビジネス部門 (ディレクタ, チームリード)
- 8% IT コンサルタント

## 調査参加者のプロフィール

### 企業サイズ

- 5% ミクロ企業 (従業員数 5~9)
- 34% 小規模企業 (従業員数 10~99)
- 30% 中規模企業 (従業員数 100~499)
- 30% 大規模企業 (従業員数 500 以上)

### 業種

- 20% 情報テクノロジー (IT)
- 14% 製造業 (IT 関連以外)
- 11% プロフェッショナルサービス (IT 関連以外)
- 10% 小売業/卸売業 (IT 関連以外)
- 6% ヘルスケア/医療
- 8% 金融/銀行/保険
- 2% メディア/出版/娯楽
- 3% 行政 (連邦、州、自治体)
- 7% AMTUC (農業、鉱業、交通、公益事業、建設)
- 6% 教育
- 3% 接客業
- 9% その他

### 参加国

- 参加数 マチュアリングエコノミー (経済が成熟過程にある市場)**
- 126 ブラジル
  - 131 インド
  - 125 マレーシア
  - 126 メキシコ
  - 125 南アフリカ
  - 125 タイ
  - 126 アラブ首長国連邦 計 884

- 参加数 マチュアエコノミー (経済が成熟している市場)**
- 125 オーストラリア
  - 125 カナダ
  - 125 ドイツ
  - 125 日本
  - 125 UK 計 625

調査参加合計数 1,509