オラクルとKPMGによるクラウドの脅威レポート（概要）

独自調査から分かった世界の動向、日本企業が抱える課題とは

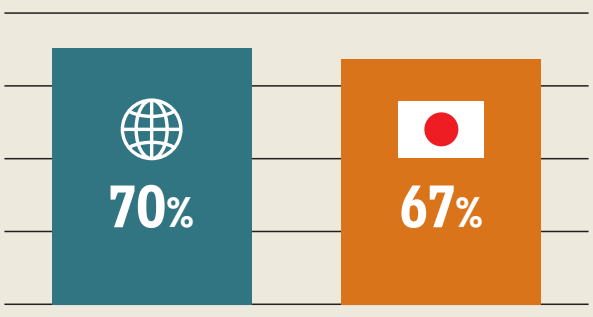
KPMGコンサルティングと日本オラクルは、オラクル・コーポレーションとKPMGが共同で実施したクラウドセキュリティに関する意識調査「Oracle and KPMG Cloud Threat Report 2019」を発行しました。「Oracle and KPMG Cloud Threat Report 2019」および日本オラクルで行った日本での調査から、クラウドへの現状認識と利用において日本は世界と同水準にあるものの、ガバナンスとセキュリティ対策へのアクションで遅れを取る日本企業の実態が明らかになりました。ここではその実態を裏付けるデータの一部をご紹介します。

共通の課題1 ｜ もはやクラウドは欠かせないビジネス基盤に
共通の課題2 ｜ 高まるセキュリティポリシー違反への懸念
日本の課題1 ｜ データ分析によるインシデントの検出
日本の課題2 ｜ セキュリティ対策における機械学習の活用
日本の課題3 ｜ 自動パッチ管理への取り組み

共通の課題1 ｜ もはやクラウドは欠かせないビジネス基盤に

世界の70%、日本の67%の企業がクラウドサービスのビジネスにおける重要性は高まっていると回答しています。
事実、クラウド上に機密データが保存されていると回答した企業は、世界で97%、日本でも88%に上ります。

クラウドはビジネスにとってより重要になっている

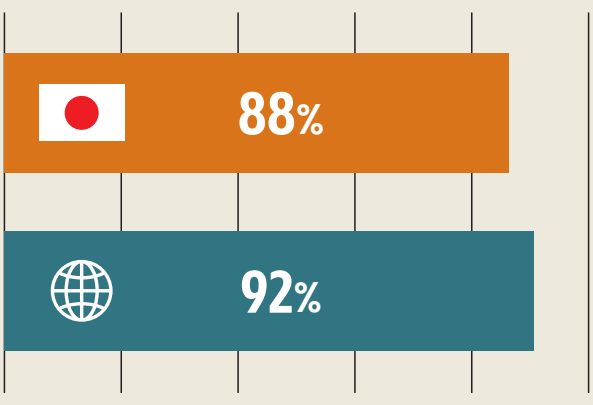


機密データの保存にクラウドを利用している

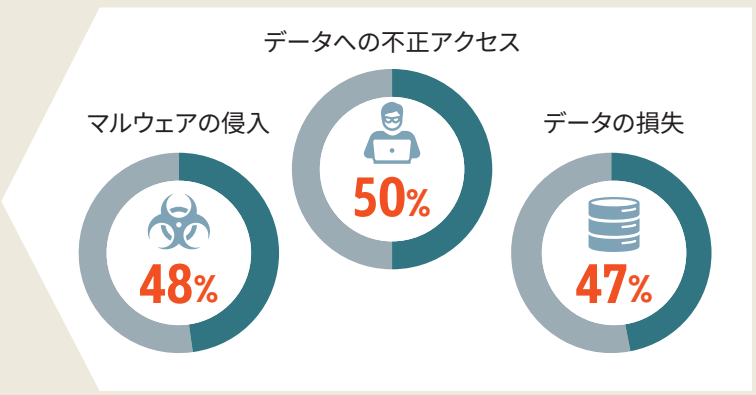
共通の課題2 ｜ 高まるセキュリティポリシー違反への懸念

クラウドの利用が拡大する一方で、ポリシー違反に対する懸念を抱く企業は世界で92%、日本で88%とむしろ深刻化しています。
その懸念が大げさでないことは、ポリシー違反に起因するセキュリティ・インシデントを多くの企業が経験していることからも明らかです。

組織内のクラウド・ポリシー違反への懸念がある



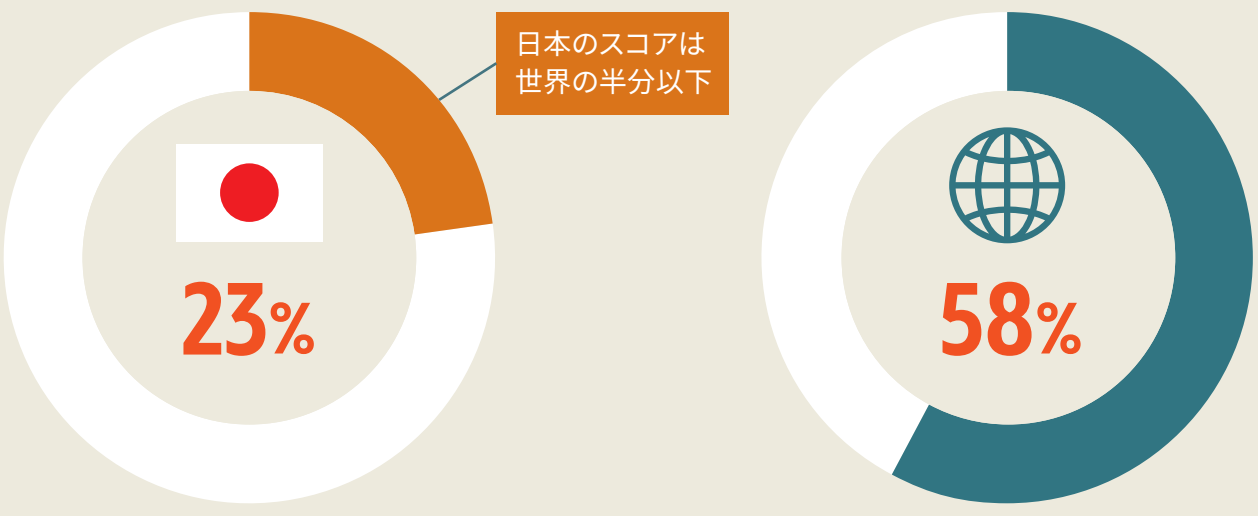
ポリシー違反に起因するインシデントの発生率



日本の課題1 ｜ データ分析によるインシデントの検出

セキュリティ・インシデントに素早く対応するには、データ分析による検出が不可欠です。
世界の半数以上（58%）の企業は、4割以上のデータを分析できていると回答したのに対し、日本のそれは23%に過ぎません。

収集したセキュリティイベントやテレメトリデータの4割以上を分析している



日本の課題2 ｜ セキュリティ対策における機械学習の活用

とどまるところを知らないサイバー攻撃の高度化に対抗するため、セキュリティ対策に機械学習を導入する動きが加速しています。
ただし、世界の企業の73%がすでに機械学習を導入しているのに対し、日本企業の導入率は47%と遅れをとっています。

セキュリティ対策に機械学習技術を導入している

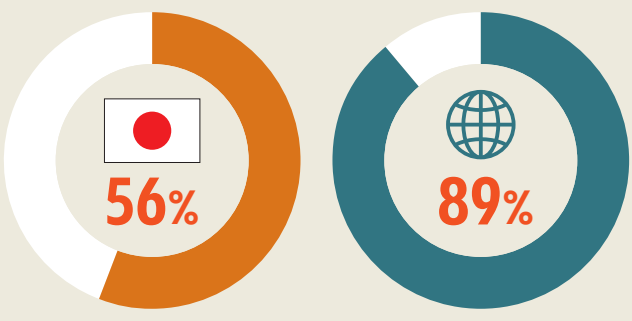
セキュリティ対策で機械学習に期待する効果

1. セキュリティアラートの調査
2. 精度の向上と誤検知の減少
3. シグニチャ検知技術の排除
4. 未知のゼロデイ攻撃の検知
5. 若手アナリストへの支援

日本の課題3 ｜ 自動パッチ管理への取り組み

脆弱性対策の基本は、今も昔も速やかなパッチ適用です。しかし、サービスの中断を嫌って、あるいは脆弱性情報のチェックに手が回らず、パッチの適用が遅れて被害を受けるケースが後を絶ちません。そうした被害を回避や運用を効率化するために、自動パッチ管理に取り組む企業は、世界では89%に上りますが、日本では約半数（56%）に留まります。

自動パッチ管理を導入済み・導入計画がある



自動パッチ管理を導入済み・導入計画した理由

1. 運用の効率化
2. 脆弱性対策
3. SLA※を満たすため
4. 過去の失敗の教訓から

※SLA：サービス品質保証

サマリー

クラウドセキュリティの動向	日本企業の課題
クラウドガバナンスのさらなる強化	●クラウドサービスの利用管理 ●安全な構成の維持
セキュリティインシデント検知	●セキュリティイベントデータの検知・分析の強化 ●セキュリティイベント監視における機械学習の活用
自動化によるセキュリティ運用の改善	●パッチ管理・脆弱性管理への対策

クラウドセキュリティソリューションをより詳しく！

日本オラクル株式会社
〒107-0061 東京都港区北青山2-5-8 オラクル青山センター
oracle.com/jp
お問い合わせ窓口
Oracle Digital
TEL 0120-155-096
URL oracle.com/jp/contact-us