

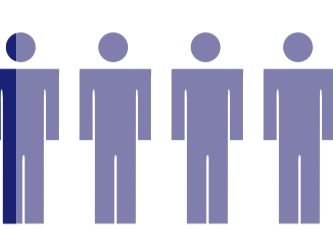
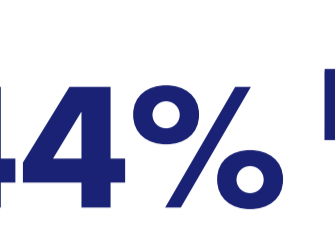
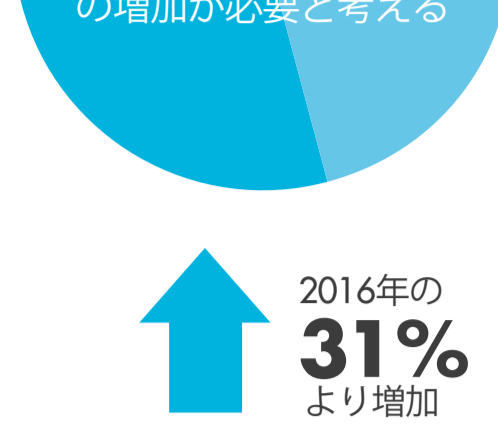
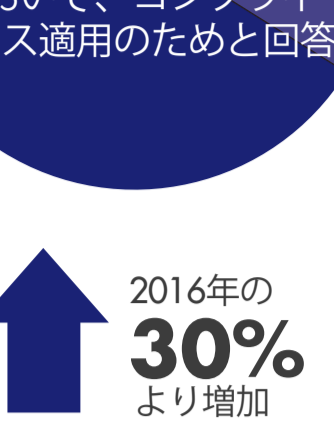
2017年は個人情報の保護がITセキュリティのキーワード

改正個人情報保護法施行が迫る中、企業はコンプライアンス要件への適用を優先しITセキュリティに対する予算を増強。

「個人情報保護法のようなプライバシーに関する法規は要件が多くなり得るが、企業はコンプライアンス要件に準拠するために暗号化とBYOKの利用を検討すべきであり、特に機密データをクラウド環境や他の先進的な環境に保存する場合はさらにその必要性が高まる。」

451リサーチ社の情報セキュリティ分野の主任調査分析官ガレット・ベッカー

ITセキュリティ予算に対するウエイトは、コンプライアンスへの適用が66%と最優先に。昨年の30%から倍増。



44% 昨年はコンプライアンス要件への適用がデータ漏洩防止に「極めて有効」と考える回答者は44%にとどまる

企業のITセキュリティに対する予算の増額率はライバル国より小さい

グローバル

73%



日本

54%



アメリカ

75%



ドイツ

79%



ブラジル

85%



オーストラリア

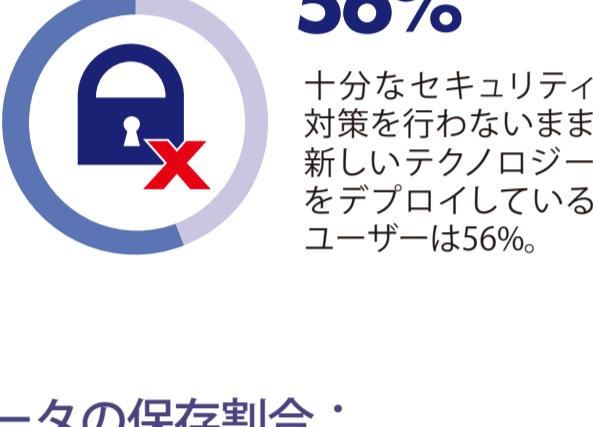
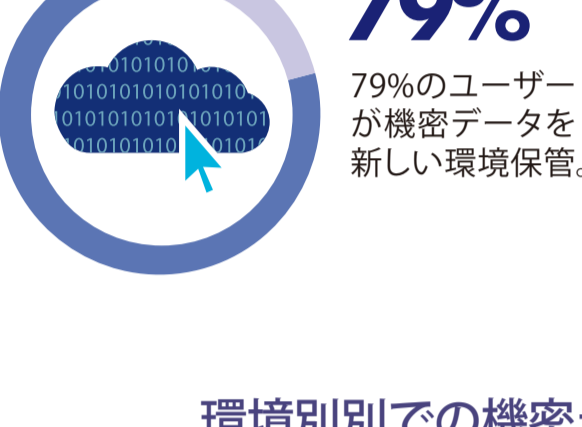
64%



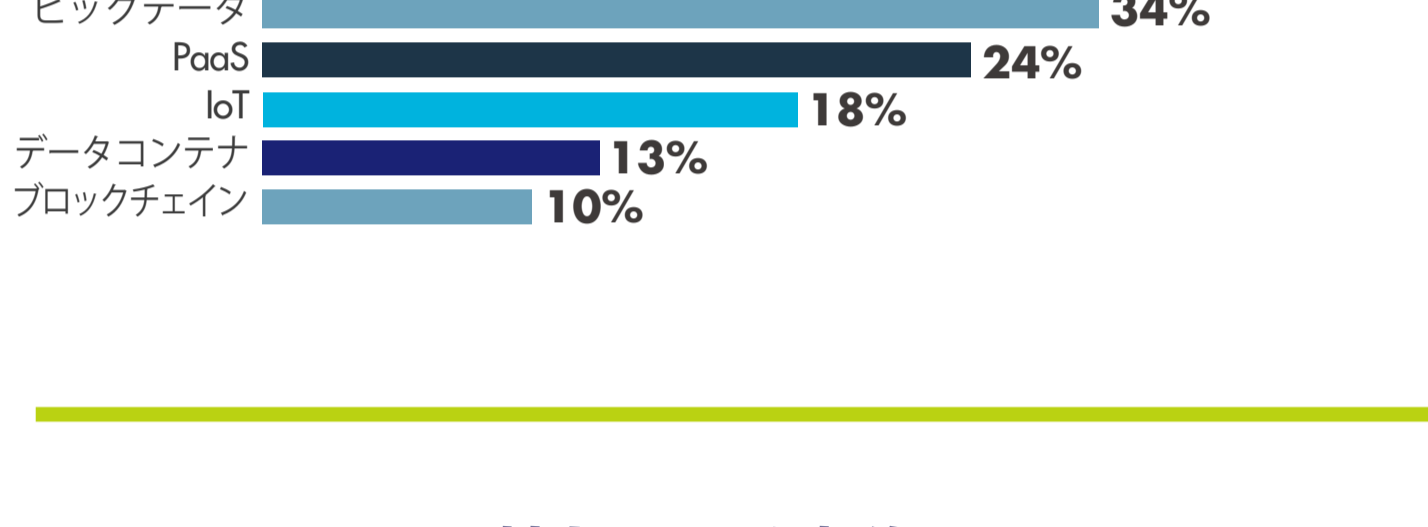
新しい環境での利用が増加 – 課題が大きく

「クラウド、ビッグデータ、Internet of Things (IoT)、データコンテナ環境の利用はいずれも積極的に受け入れられており、それらはかつてのビジネスの基本原則を一気に根底から覆す可能性を秘めている。」

451リサーチ社の情報セキュリティ分野の主任調査分析官ガレット・ベッカー



環境別での機密データの保存割合：



ITセキュリティに対する誤った投資 data-at-restへの投資は有効と評価されつつも減少している

「企業は過去に有効だったソリューションに対して依然として投資を続けているが、それらは必ずしも今日のデータ漏洩対策に最も有効であるとは言えない。」

451リサーチ社の情報セキュリティ分野の主任調査分析官、ガレット・ベッカー

ITセキュリティ対策に対する予算の増額率およびデータ保護が有効と考える割合

保存データ防御

27% (ITセキュリティ上の懸念への対応)

63% (データ保護の有効率)

ネットワーク

52% (ITセキュリティ上の懸念への対応)

61% (データ保護の有効率)

伝送データ防御

30% (ITセキュリティ上の懸念への対応)

55% (データ保護の有効率)

エンドポイント/モバイル

28% (ITセキュリティ上の懸念への対応)

52% (データ保護の有効率)

解析/相関分析ツール

24% (ITセキュリティ上の懸念への対応)

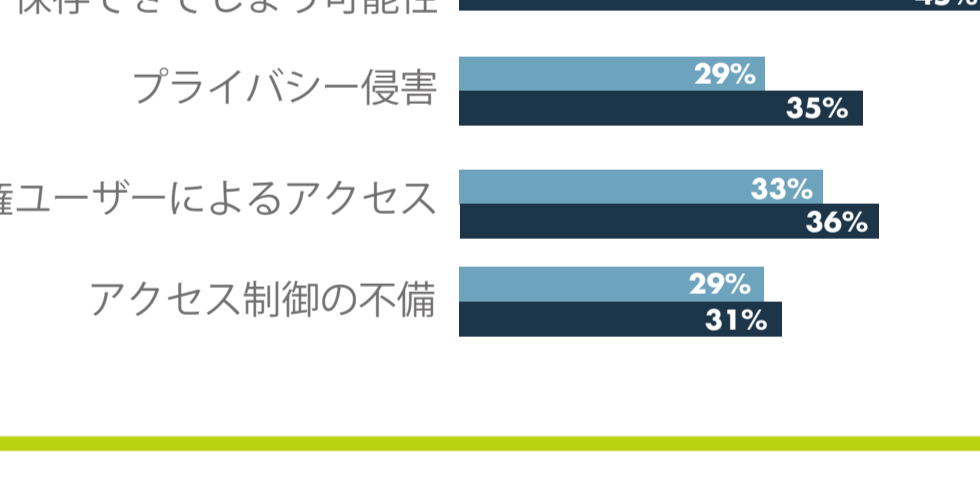
50% (データ保護の有効率)

日本では35%が、世界では47%が、機密データをビッグデータ環境で使用

「ビッグデータは世界的に極めて大きな成長を見せている。企業は、そのビッグデータが企業にとってどれだけの潜在的な価値があるのかを見極めるように、そのデータの機密性やどのように保護されるべきかといった見極めに取り組み始めている。」

451リサーチ社の情報セキュリティ分野の主任調査分析官、ガレット・ベッカー

ビッグデータにおけるデータセキュリティ上の主な懸念事項



先進的なテクノロジーによる暗号化によってデジタル・トランスフォーメーションが可能に

クラウド

暗号化がクラウドの導入時の懸念を排除

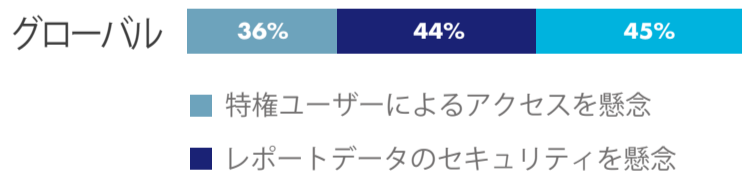
ビッグデータ

暗号化がセキュリティ上の主な懸念を軽減

49% Japan

61% Global

企業自身による鍵を用いたクラウド環境でのデータ暗号化の割合



IoT

利用用途拡大のために必要となる主要な技術

コンテナ

導入を増やすには暗号化を用いた対策が必要と回答した割合

日本

39%

41%

グローバル

56%

55%

■ データの暗号化

■ 認証やID管理

45% 日本

53% グローバル

何をすべきなのか

1 ITセキュリティツールセットに対する優先度の見直し

クラウドとSaaSにより、レガシーなITセキュリティモデルは終わりを告げた。全ての環境に対して、暗号化によるデータ保護とアクセス制御が必要。

サービスベースのソリューションとプラットフォームの採用。自動化はコストの削減や一元管理をもたらす。

2 データの可視化と分類

機密データの保存場所を可視化。特にクラウド、ビッグデータ、コンテナ、IoT

3 コンプライアンス要件のチェックだけでは不十分

コンプライアンスの先を見据えた、暗号化とBYOKの利用。特にクラウドおよび新しい環境への対策。

4 暗号化とアクセス制御

暗号化の対象は、ラップトップ、デスクトップだけでは不十分。

データセンター：ファイルとアプリケーションレベルの暗号化およびアクセス制御。

コンテナ：コンテナおよび内在するストレージ上での暗号化とデータへのアクセス制御。

クラウド：暗号化と鍵管理を企業自身で行い、BYOKによりSaaS、PaaS、IaaSの安全を確保する。

IoT：脅威を減らすためには、デバイス上の格納データやバックエンドシステム、送信データの暗号化だけでなく、安全なデバイスIDと認証を使用することが重要。

ビッグデータ：ビッグデータ環境での暗号化とアクセス制御。

クリックしてレポートをダウンロード

フォローをどうぞ

