ORACLE KPMG

Oracle and KPMG Cloud Threat Report 2020

グローバル比較で見えてきたクラウド・セキュリティの現状と今後の対策

クラウドサービスが急速に拡大している状況において、
各企業が直面しているサイバーセキュリティの課題とリスクを検証し、
ビジネスを成功に導くための重要な洞察と推奨事項を提供

［調査実施時期］
2019/12/16 – 2020/1/16

［回答数］
750社

［調査参加国］
米国、カナダ、英国、フランス、
オーストラリア、シンガポール、日本

01.

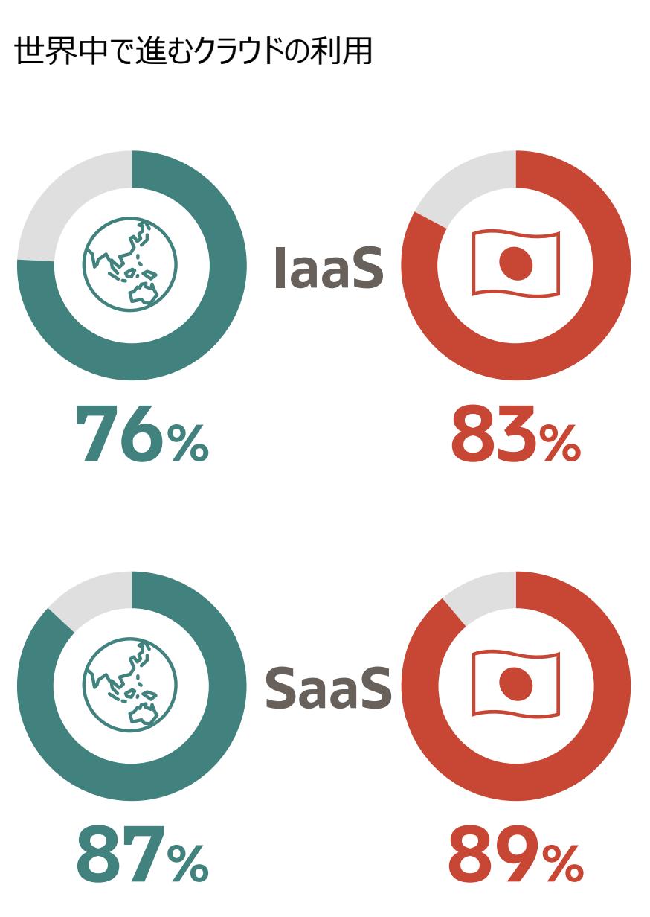
出遅れる日本企業の本格的なクラウド利用

クラウド利用は広まるも、本格的活用が進まない

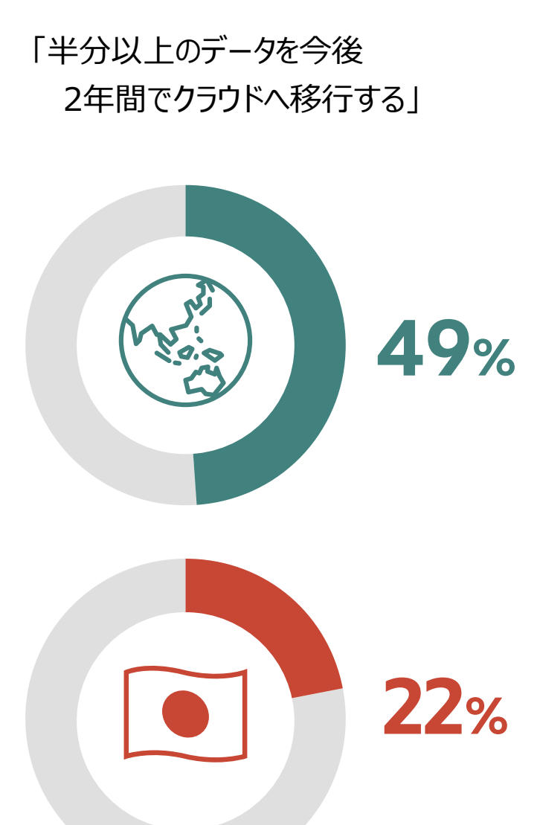
- クラウド利用は世界中で広まっている
- 本格的な活用で遅れをとっている日本企業
- クラウド・セキュリティに対する理解が深まっていない

クラウドの利用は世界中で広まっているが、本格的なクラウド活用が進まない日本

世界中で進むクラウドの利用



「半分以上のデータを今後
2年間でクラウドへ移行する」

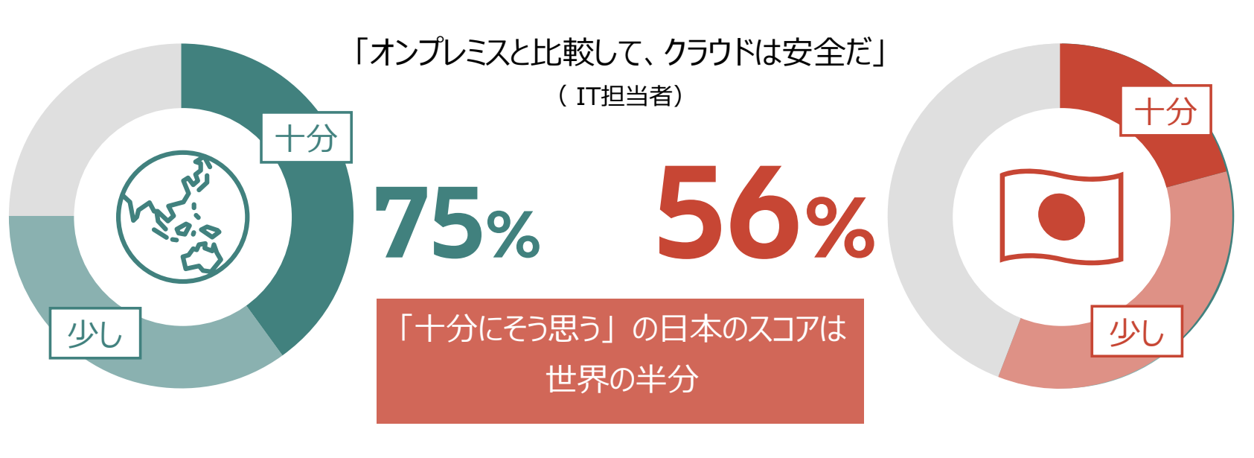


世界中で、90パーセント近い企業はSaaS、80パーセント近い企業がIaaSを利用しています。クラウド利用は広がっていますが…
今後2年間でデータの半分以上をクラウドへ移行する予定と回答した企業は、世界のトレンドの半分以下にとどまり、日本では特に本格的なクラウド活用が進んでいないようです。
その差はどこから来るのでしょう。

クラウドのセキュリティに対する理解は深まっておらず、グローバルと大きな開き

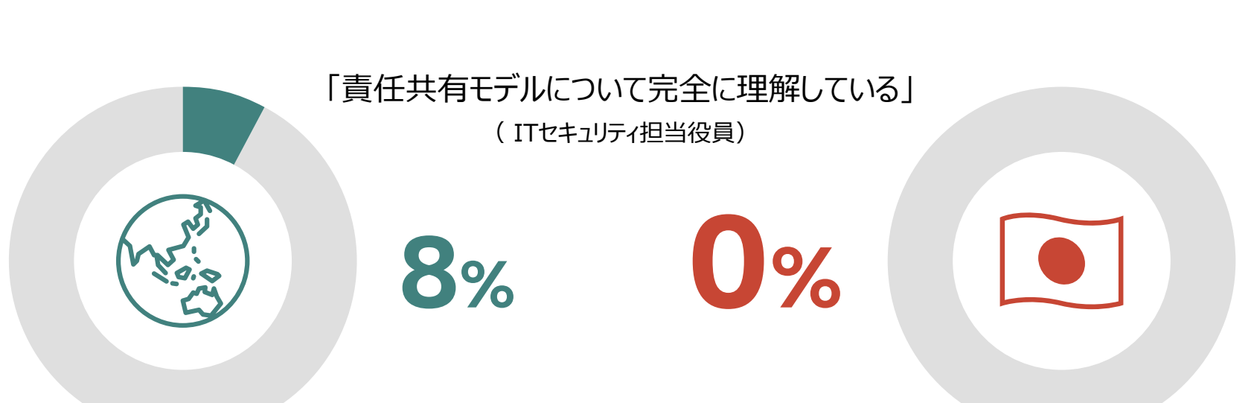
クラウドが安全であると認識する企業が、グローバルでは75パーセントに達する一方で、日本企業では56パーセントにとどまります。特に、十分と安全だと認識する企業はグローバルの半分にとどまります。
まだ多くの日本企業がクラウドは安全性でないと考えているようです。
「責任共有モデル」の完全理解度は世界でも低いものの、日本企業ではほとんど理解が進んでいません。

「オンプレミスと比較して、クラウドは安全だ」
（ IT担当者）



「十分にそう思う」の日本のスコアは世界の半分

「責任共有モデルについて完全に理解している」
（ ITセキュリティ担当役員）



02.

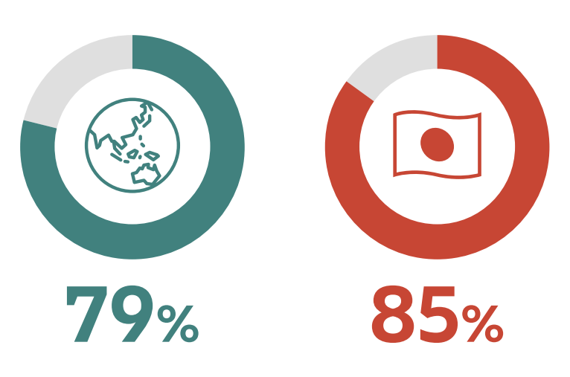
日本企業におけるクラウド・セキュリティの現状

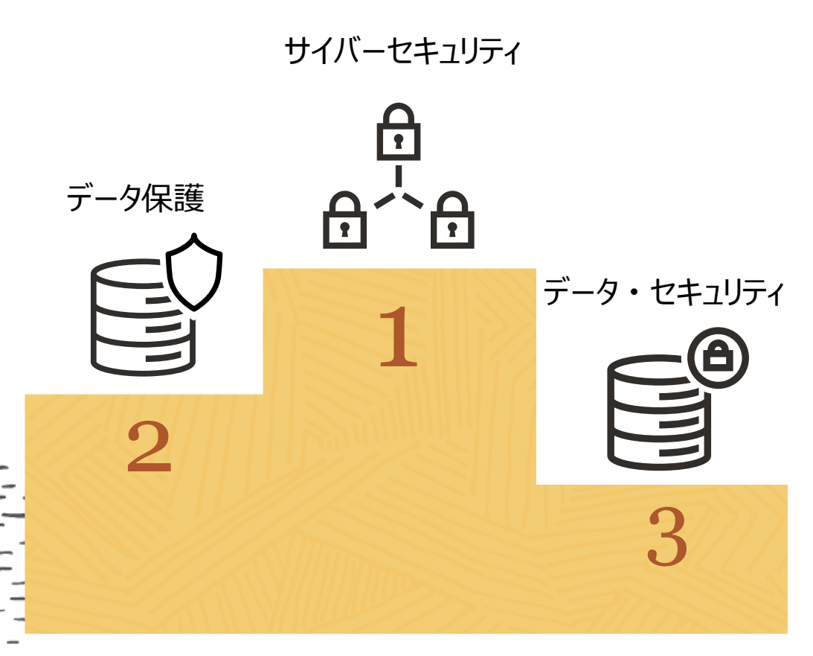
広がり続けるクラウド利用、安全に利用するための準備は万全か？

- 全世界で重視されているデータ・セキュリティ
- 場当たり的な対応を重ねてきたこれまでのセキュリティ・アプローチ
- ３つの視点で考える、クラウド利用を前提にしたセキュリティモデルへ

クラウドのセキュリティ対策において、データ・セキュリティ対策が重視されている

「他企業で最近発生したデータ侵害によって
自社のデータ保護への関心が増した」





日本のIT担当者が多くの時間を割いているデータ・セキュリティ

クラウドの利用が広がっている一方で、安全に利用するための準備が整っておらず、他企業で発生したインシデントが自社のデータ保護への関心を高める契機になっています。
IT担当者は、業務の多くの時間をデータ・セキュリティに割いています。

ツールの多さ、場当たり的なセキュリティ・アプローチと設定ミス

利用しているサイバーセキュリティ製品

設定ミスによるデータ損失の発生

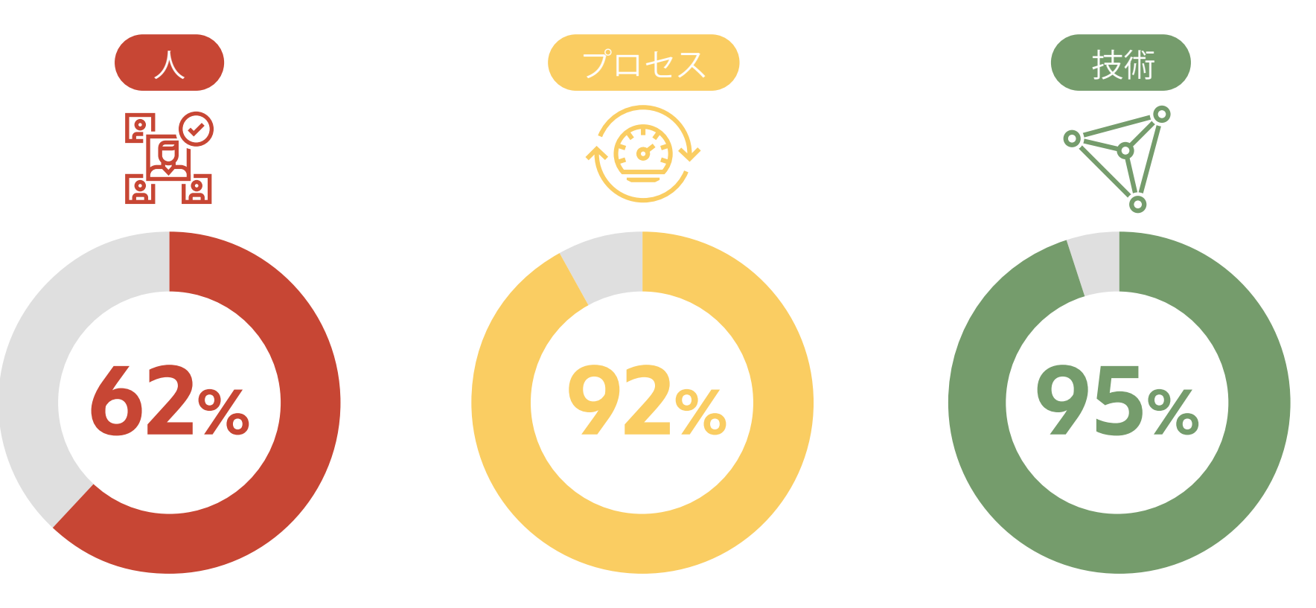
パッチワークのように多数の異なるサイバーセキュリティ製品を組み合わせて利用してきた結果、それらの設定が誤っているケースもあり、セキュリティ対策において苦戦を強いられています。

セキュリティにおける最大の課題は、設定です。
グローバルの51パーセントの企業は、設定ミスによりデータ損失が発生しています。日本においても、42パーセントに上ります。

今こそクラウド利用を前提としたセキュリティモデルの構築を

顕在化しているクラウド・セキュリティの課題を解決するには、クラウド利用を前提としたセキュリティ対策に取り組む必要があります。
技術を有する人材の採用に加え、AIの活用、拡大するデジタル世界の脅威に対応するためのプロセス、テクノロジーの3つの視点で絶え間ない向上が必要です。

3つの視点での取り組むべきセキュリティモデルの構築



「クラウド・セキュリティのスキルを有するCISOを採用した、または採用予定」

「今後3年間でパッチ適用処理の自動化を採用」

「不正、マルウェア、設定ミスなどへの対策強化のため、今後3年でAI/MLを活用」

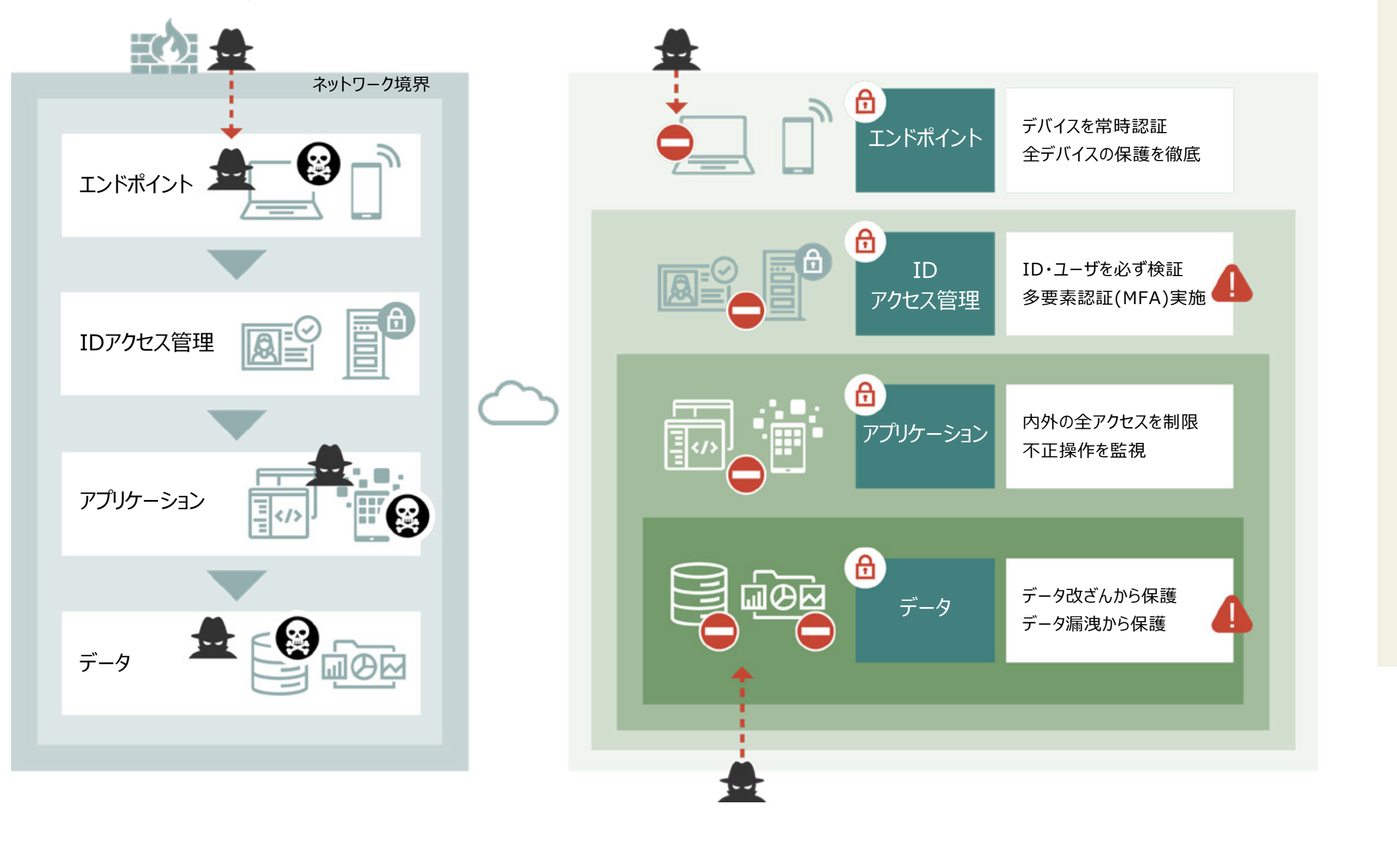
03.

遅れる日本のリモートワーク環境向けセキュリティ対策

リモートワーク環境へのクラウド・セキュリティ対策が急務

- リモートワークの拡大に伴い、多層防御の考え方が必要に
- クラウド利用を前提にした、全てのアクセスを検査するゼロ・トラスト・セキュリティが重要に
- 境界防御偏重の日本は、IDアクセス管理とデータ・セキュリティに遅れ。対策が急務

リモートワークの拡大に伴い、多層防御が重要に

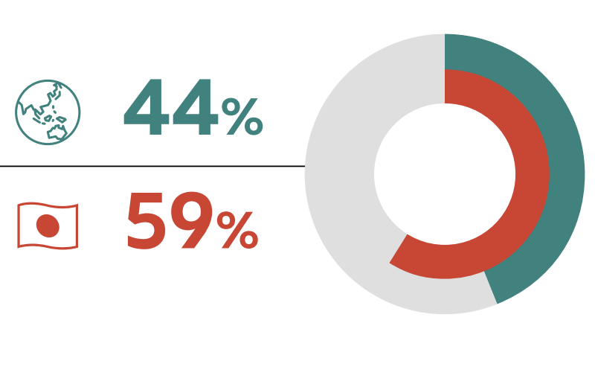


リモートワークを推進するためには、従来の境界防御型セキュリティから、全てのアクセスを検査するゼロ・トラスト・セキュリティの考え方への転換が重要になります。
そのためにはネットワークに依存しない、「エンドポイント」「IDアクセス管理」「アプリケーション」「データ」各層での守るべき情報を中心とした多層防御が必要となりますが、日本においては、境界防御に偏っていることがわかりました。
特に、IDアクセス管理とデータ・セキュリティ対策がグローバルより遅れているため対策が急務となっています。

対策が急務！遅れる日本企業のIDアクセス管理とデータ・セキュリティ

日本企業のセキュリティ対策は、境界防御に偏っているのが実状です。
日本企業においては、IDアクセス管理、データ・セキュリティに関する設定ミスが多くなっています。
また、クラウド上のデータ管理不備により、グローバルより多くのデータ損失が発生しています。
設定ミスによるデータ漏洩の脅威にさらされており、対策は急務です。

ネットワークベースのセキュリティ対策で脅威を検知



発見された設定ミス：グローバルと差が大きい TOP3

1	45%	過剰な権限付与
2	40%	セキュリティグループの誤設定
3	32%	機密情報が暗号化されていない

クラウド上のデータ損失原因 TOP 3

1	51%	機密区分の誤設定
2	43%	外部委託先へ機微情報を共有
3	37%	データが暗号化されていなかった

ORACLE KPMG