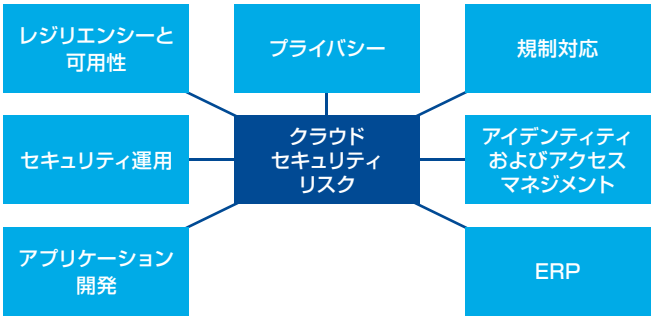
Deloitte.

クラウド・アシュアランス
何が「信用」の鍵となるのか

クラウドにはさまざまなセキュリティリスクが存在します

クラウドコンピューティングが企業ITとして浸透していくにつれて、企業はこれまでにない経営環境の変化に直面します。クラウドサービスの利用に対する不安を取り除き、顧客からの信用を勝ち取るために、情報セキュリティを始めとする技術的リスクへの対応に加えて、より大局的な視点から、企業は何を選択できるでしょうか。



サービス提供会社と利用者それぞれのリスク

クラウドサービス提供会社の視点

クラウドサービス提供会社は、データ所有者と同じ責任や説明責任を持たないかもしれませんが、それでも顧客のために、クラウドにあるデータを管理し、保護することについて、重大なリスクを引き受けています。

クラウドリスクに対する信用

プロバイダーの責任の具体例
- セキュリティ運用
- レジリエンシー
- 可用性

クラウド・アシュアランス

利用者の責任の具体例
- プライバシー
- アプリケーション開発

クラウドサービスの利用者の視点

クラウドサービスの利用者は、データ資産をアウトソースすることが出来ますが、これらの資産に関する責任や説明責任をアウトソースすることは出来ません。

クラウドに関するアシュアランスの形態

使用許諾契約書／サービス内容合意書	使用許諾契約書とサービス内容合意書は、運用上の要求事項を満たす上で非常に優れています。何が期待され、何を探し求めているのかを理解することは顧客の要求に答えるための鍵となるでしょう。
国際標準化機構 ISO27001認証	ISO27001情報セキュリティ管理システムの認証は、優れたセキュリティが実践されている事を第三者機関による認証によって明らかにする方法です。
サービス・オーガニゼーション・コントロール報告書 (SOC1 - SSAE16)*	SOC1-SSAE16報告書は、財務報告に関連するプロセスやデータをクラウド提供会社に預けている顧客から要求されるでしょう。
サービス・オーガニゼーション・コントロール報告書 (SOC2/3)	セキュリティ、可用性、処理のインテグリティー、機密保持、またはプライバシーに関連するサービス・オーガニゼーション・コントロール報告書 — 米国公認会計士協会（AICPA）によるこの新しい報告書形態は、SOC報告書に、SAS70/SSAE16で求められている従来の財務監査の範囲を超えて、クラウド採用上の幾つかのキーリスク障壁を緩和するためのリスク領域を含んでいます。

*過去SAS70として知られていたもの

トーマツ.

SOC2の概要(内部統制の新報告書)

SOC2とは

サービス・オーガニゼーション・コントロール2(SOC2)は、サービス・オーガニゼーション(クラウド事業者等のサービス提供会社)の統制のセキュリティ、可用性、処理のインテグリティー、機密保持、およびプライバシーについて、サービス監査人が意見表明する事を認めた米国公認会計士協会(AICPA)の基準を利用して提供される、新しい内部統制の仕組みです。

更にSOC2は、客観性のある論拠を柔軟に取り入れる事を認めており、具体例として、サービス内容合意書、米国国立標準技術研究所フレームワーク、公共産業の標準規格に順ずる基準(例、医療保険の相互運用性と説明責任に関する法律(HIPAA)、ユーティリティーフレームワーク)があります。SOC2は2011年の夏から導入されました。

SOC2は財務報告以外のビジネス分野をカバーする為に、US-SOX等の規制領域、またはその他の非規制領域に対しても適用することができます。報告書は、依頼者からの要望を満たす為の処理のコントロールやシステムに重点を置いて明示され、依頼者やその他の利害関係者に提供されます。

これらの領域における必要な保証は、5つのSOC2 Trust原則の1つ、またはそれ以上により提供されます。

Security	物理的、または理論的な承認されていないアクセスや占有に対するセキュリティ
Availability of operations	運用の可用性
Processing integrity	タイムリーな処理と正確で完全さを含む処理のインテグリティ
Confidentiality of information	情報の機密保持
Privacy	AICPAのTrust原則や組織のプライバシーポリシー(例、個人情報や機密データ)、またはその他の規則に従っているプライバシー

SOC2は構造や一般的なアプローチにおいて、タイプ1またはタイプ2の報告書をオプションとして含んでいる従来のSAS70報告書(現在のSOC1)と似たものになります。タイプ1は統制のデザインのみをカバーし、タイプ2はデザインと運用の有効性をカバーします。

SOC2の適用例とデロイトの強み

対象	適用例		デロイトの強み
全業界	サービス・オーガニゼーション(受託会社)	SOC2の適用範囲はとても広く、事実上全てのインダストリーや事業部門に活用することが出来ます。 SOC2は、受託会社が効果的な内部統制を適用している事について、依頼者やその他利害関係者に対し、保証を提供する事を認めています。	デロイトは過去のSAS70報告書や内部統制サービスにおけるマーケット・リーダーの一つとして認知されています。当法人は、立ち上げ時間を削減するために、深く業界に精通し、経験を有する専門的なリスクと統制の実務スペシャリストを擁しています。
Cloud Computing	クラウドサービス提供会社	依頼者が安心してクラウド提供会社に極秘データや重要なコンピューティングを委託することが出来るように、クラウドサービス提供会社は、全てのSOC2 Trust原則の内部統制が有効である事に対する保証を提供する必要があります。 SOC2報告書は、依頼者の信用を築く方法とさまざまなインダストリーの規制や基準に対する適合性を説明できます。例:米国における医療保険の相互運用性と説明責任に関する法律(HIPAA)、高度先端技術(HITECH)、グラム・リーチ・ブライリー法(GLBA)、連邦情報セキュリティ・マネジメント法(FISMA)。	デロイトは、最も要求の厳しいクラウドの依頼者と最大のクラウド提供会社へのサービス提供経験によって、多くのクラウドコンピューティングに対する能力を有しています。 当法人は、セキュリティ、プライバシー、および内部統制サービスにおけるリーダーです。当法人の強力な保証業務におけるブランド力は、当法人を、クラウド提供会社から最初に選ばれるSOC2サービス提供者に位置付けています。
Power & Utilities	電力およびユーティリティー業界	電力およびユーティリティー事業会社は、SOC2を利用することによりさまざまな規制機関の要件、インダストリーの概要、および北米電力信頼性評議会の定める重要インフラ保護基準(NERC CIP)などの基準、スマートグリッド(次世代送電線):米国標準技術研究所　IR 7628-スマートグリッド・サイバーセキュリティに関するガイドライン、スマートメーター(AMI)-SEC System Security Requirement、および米国の各州で求められるプライバシーに対するコンプライアンスを明らかにすることができます。	デロイトは、深いインダストリー経験と共に、ユーティリティー業界の保証分野において代表的なビック4ファームの一つに位置付けられています。当法人はスマートグリッド周辺の重要な資格を有しており、その事が当法人を当サービスにおけるマーケットリーダーにしています。
FISMA	米国連邦政府ガイドライン	米国連邦政府とのビジネスを行うことを契約または計画している企業は、米国連邦情報セキュリティ・マネジメント法(FISMA)で要求されているコントロールを満たしている事を示す為にSOC2を活用することができます。 SOC2報告書は、他の政府機関、契約者やその他の情報源により管理または提供されているものを含む政府機関の資産や運用をサポートしている情報セキュリティの統制が文書化され、それを政府機関が保持している事に対して保証を提供します。	デロイトは、米国連邦情報セキュリティ・マネジメント法(FISMA)の評価管理やFISMAのプログラムの構築に習熟しており、商業部門や連邦政府に対する経験豊富なスタッフと重要な資格を擁しています。

国内ネットワーク

www.tohmatsu.com/ers

有限責任監査法人トーマツ

東　京　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1112
大　阪　〒541-0042　大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング　Tel:06-4560-6021
名古屋　〒450-8530　愛知県名古屋市中村区名駅3-13-5 名古屋ダイヤビルディング3号館　Tel:052-565-5517
福　岡　〒810-0001　福岡県福岡市中央区天神1-4-2 エルガーラ　Tel:092-751-1517

デロイト トーマツ リスクサービス株式会社

本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1300