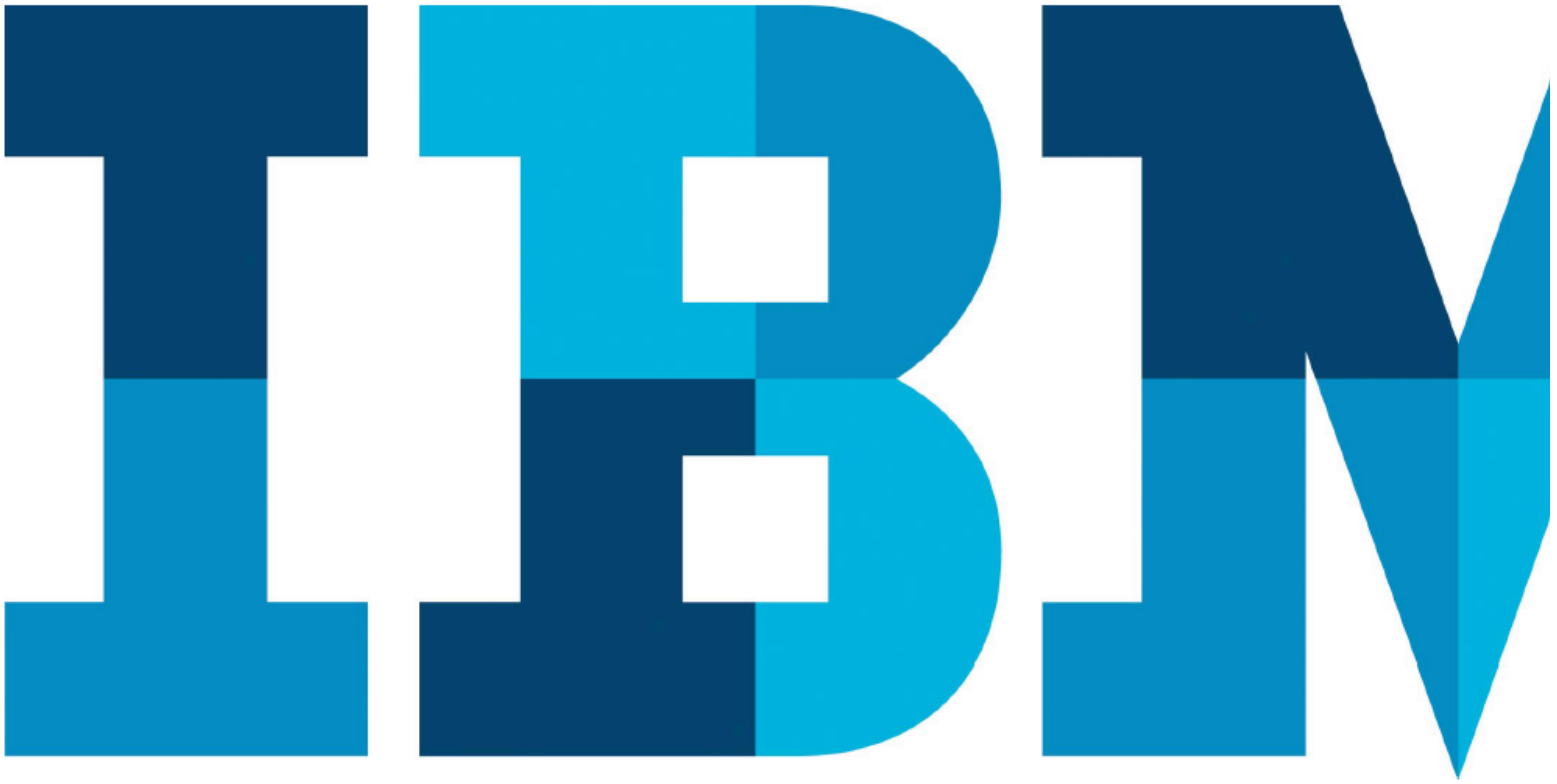
IBM Analytics

クラウドとオンプレミスのデータを保護するには

適切なガバナンスの実施により、
ハイブリッド環境の情報を保護する方法



IBM

目次

はじめに: 新たな環境ではガバナンスが不可欠な要素となる

クラウド・ベースのデータは、業界において競合他社を凌駕できる能力を獲得し維持しようとする企業にとって、膨大な情報を獲得できる可能性を意味します。しかし、「情報ガバナンスとクラウドの真実」で説明したように、ほとんどの企業はレガシーのオンプレミス・データならびに第三者によるクラウド・ベースのデータおよび Hadoop テクノロジーとその他のオープンソース・テクノロジーのデータの突き合せを行う課題に直面することになります。ユーザーが重要な意思決定を行うための知見を求めてアクセスするのが、このような「ハイブリッド」環境なのです。

一般的に、綿密な計画を立てなければハイブリッド環境は増大していくため、常に増大を続けるデータ・ストアを管理することがよりいっそう困難になります。しかしながら、この混乱状態を制御する方法があります。他の問題と同様に、まず問題の特性を理解する必要があります。重要なのはデータそのものであり、データのソースとデータを管理するために使用されるシステムの重要性は二の次です。最重要課題としてデータに加えデータから得られる情報の管理に取り組むと、その他の課題はスピーディーに解決します。

4 つの柱

企業がクラウド・ソースから抽出した情報のセキュリティーと信頼性を確保したうえで、クラウドによる財務上のメリットを実現するにはどうすればいいのでしょうか。その答えはガバナンスにあります。

ハイブリッド情報を適切に制御するには、IT 部門と ビジネス部門はいくつかの重要施策を実施する必要がありあます。

1. **情報の意味に関して広範な合意があること** (ビジネス部門が必要とする情報に関する共通のポリシーとわかりやすいルールおよび情報の処理方法に関するメタデータを含む)。
2. **保有する情報資産の保守と監視に関して明確な合意があること** (オンプレミス・システムでデータを管理するためのオペレーショナル・データの品質に関するルールなど)。
3. **戦略的な情報資産のセキュア化と保護のための全社的なプラクティスと部門別のプラクティスを実施すること** (役割ごとの情報へのアクセス・ルールの規定、情報の共有と第三者からの機密情報の保護に関するルールの作成など)。
4. **全社的なデータ統合戦略を実施すること** (ライフサイクルの管理、データの流れと戦略情報への加工の明文化、継続的な情報の管理に関する計画など)。

このようなコンポーネントは、ハイブリッド環境における情報ガバナンスの基盤となります。いずれの場合も、施策を成功に導くには、プロセスに関する要因、組織的な要因、技術的な要因を組み合わせる必要があります。このような柱を設定できれば、企業はスピーディーに自信を持って柔軟にプロジェクトを進めることができます。

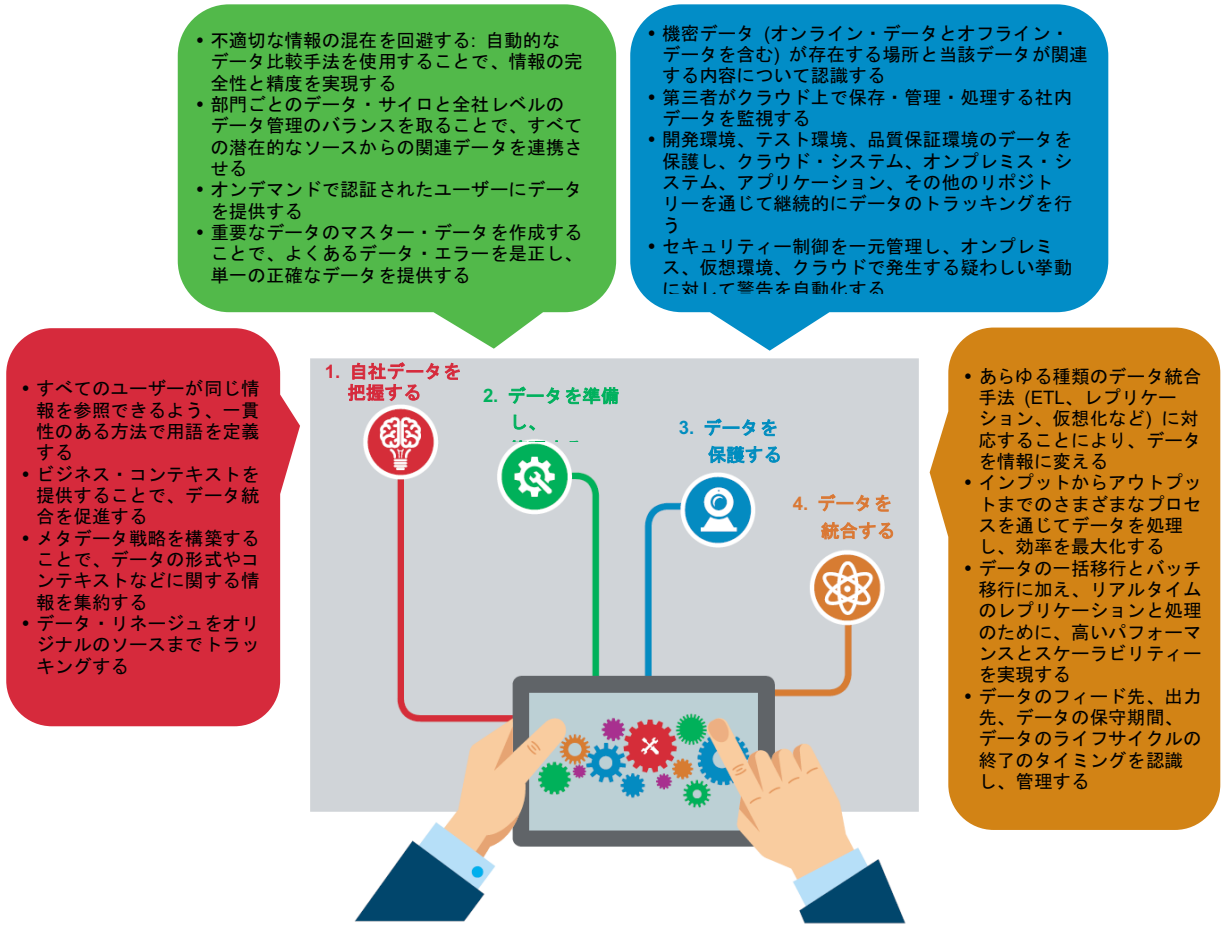
本 e-book は、3 つ目の柱である「ハイブリッド環境でデータを保護すること」について解説します。

戦略情報を制御する

ハイブリッド環境を採用したからといって、IT 戦略が完全に実現したわけではありません。実際には、クラウド環境の要素はビジネスの優先課題に合わせて迅速に進化します。しかし、クラウド・ベースのソースからのデータの比率が小さくても、IT 部門はデータの統合とセキュリティーに関する計画を持つ必要があります、IT 部門は、データがどこに存在する場合でも、企業があらゆるデータとデータの処理によって生まれる情報を制御できるよう支援しなければなりません。

ハイブリッド・インフラと分散コンピューティングは、戦略的な情報資産を構築するという最終目標を達成する手段に過ぎません。この基本的なコンセプトを採用すると、IT 部門が対応すべきことが明確になり、さらに重要なことに、IT 部門がより効果的にビジネス・ユーザーと連携するにはどうすべきかがはっきりとします。

以下のアイコンにカーソルを置くと、ハイブリッド環境で情報の適切なガバナンスを行うための重要ポイントを確認できます。



ハイブリッド環境でデータを保護する: 今後の課題

データ容量が爆発的に増大しテクノロジーが急速に変化する現代においては、あらゆる環境でデータの制御が困難になっています。クラウド環境が従来のデータ保護機能 (これまでのセキュリティー戦略で主要な役割を果たしたファイアウォールなど) の及ばないロケーションでデータを生成し、移動するなか、この課題はさらに複雑化します。IDC の調査結果によると、73% の企業が、社内の IT ポリシーやセキュリティー・ポリシーに準拠せずにクラウド・サービスまたはクラウド・アプリケーションが使用されたケースが少なくとも 1 度あったと回答しました[1]。ほとんどの場合、このような新規のクラウド実装環境が既存のエンタープライズ IT インフラに追加され、ハイブリッド環境を構成しています (図 1 を参照)

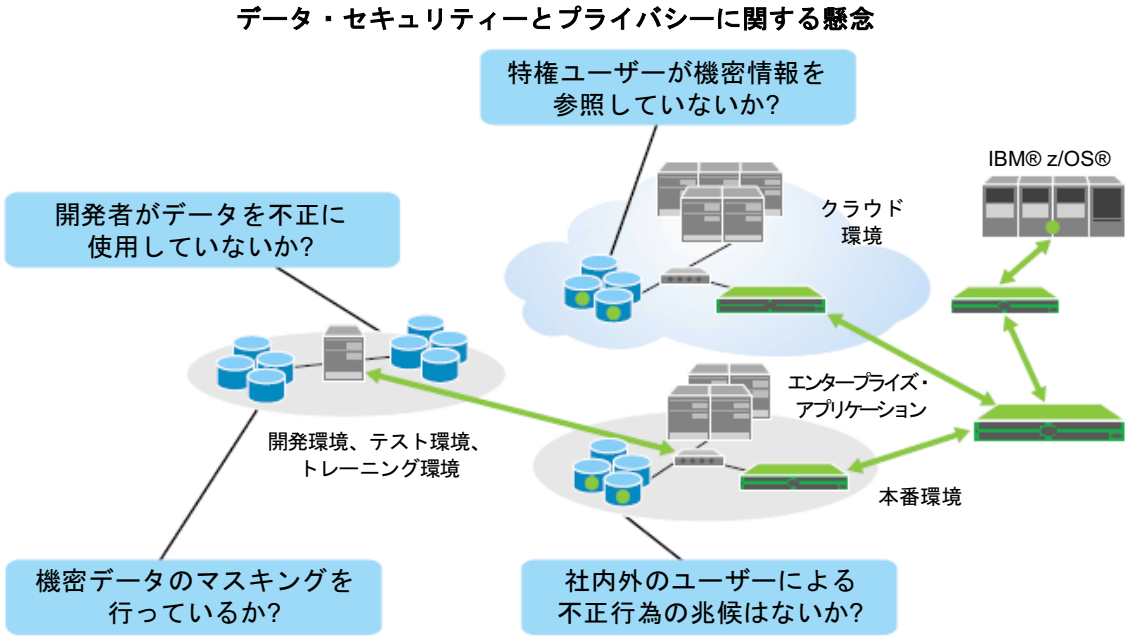


図 1. 企業はあらゆる環境 (テスト環境、本番環境、オンプレミス環境、クラウド環境を含む) に存在するデータを保護しなければなりません。

セキュリティー担当者とガバナンス担当者が懸念を抱いているのはどうしてでしょうか。どのようなリスクがあるのでしょうか。オンプレミスとクラウドでセキュリティー対策が至急必要となるいくつかの要因があります。

クラウド・セキュリティーに関する懸念が企業にとって非常に深刻な問題となっている

回答者の **70%** は、セキュリティーがクラウド・コンピューティングの実装を阻んでいると感じています

クラウド・コンピューティングのセキュリティーに関する 5 大懸念
データ・セキュリティー: 41%
アクセスと制御: 35%
監査とコンプライアンス: 32%
データの制御: 26%
セキュリティー・モデルとツールセット: 18%

出典: IDG Enterprise, 2013; 451 Research, “Cloud Computing - Wave 6,” 2014.

コンプライアンス

データの存在する場所にかかわらず、機密データのタイプを見極め、オンプレミスとクラウドでのこのデータの使用に関する一貫性のあるポリシーを設定する必要があります。**データがどこに存在し、どのような領域の情報が存在し、データが社内でどのように連携しているのか理解することが重要です。**

この理解があれば、データのセキュア化と保護を行い、サーベンス・オクスリー法、PCI データ・セキュリティー・スタンダード (PCI DSS)、連邦情報セキュリティー・マネジメント法 (FISMA)、経済的および臨床的健全性のための医療情報技術に関する法律 (HITECH) などの法令への遵守を実現するための適切なポリシーを定義することができます。遵守が求められる法令の数と種類は増大を続ける一方で、データがクラウドへと移行するなか、企業は説明責任を求められています。

データ侵害

機密データに対する脅威は遍在しています。悪意のあるハッカーは機密データに簡単にアクセスできる方法を求めています。会社に不満を持つ従業員が意図的にビジネス上の秘密と顧客情報を漏えいする場合があります。ポリシーに準拠せず、適切に許可が設定されないと、データ漏えい事故につながりかねません。しかも、ファイアウォールや IPS デバイスのような従来型の境界を防御する機能では十分な抑止力を発揮することはできません。

物理環境、仮想環境、クラウド環境で社内外からの攻撃からデータを保護しなければなりません。ベストプラクティスとしては、エラーとアクセス権の乱用を防止するために「ユーザーに付与する特権を最小限に抑える」ことが必要です。**クラウドで発生している状況と特権ユーザーの行動の両方を把握できるよう、データ・セキュリティー・ソリューションを活用した複数階層の防御を設定する必要があります。**

プライバシー

もう 1 つの課題は、機密情報にアクセスする際に正当なビジネス上の理由を求めることです。例えば、医師は症状と予後に関する情報を必要とするものの、請求担当者は患者の保険番号と請求先住所を必要とします。ビジネス・ニーズを満たし、知る必要のある人にのみデータを提供したうえで、適切なデータの保護を行うことは非常に困難なことです。**機密データは構造化データのデータベースと非構造化データのファイル・システムの両方に存在するため、このようなインスタンスのすべてを監視しなければなりません。**

生産性

セキュリティー・ポリシーとプライバシー・ポリシーはビジネス業務を促進すべきであり、妨害することがあってはなりません。**このようなポリシーを毎日の業務に組み込み、ユーザーの生産性を下げることのないよう、クラウド環境でシームレスに機能させる必要があります。**例えば、アプリケーション・テストを効率化するために多くのプライベート・クラウドが設定されています。機密データをマスキングすると、テストの結果に悪影響を及ぼすことなく、このような環境でデータ漏えいによるセキュリティー・リスクを下げることができます。

脆弱性

データベースが脆弱性を示すケースは膨大にあり、ハッカーは入り込むチャンスがあればどんな小さなきっかけでも悪用しようとします。あらゆる角度から脆弱性を把握し、脆弱性に対応する手法を確立する必要があります。**よく見られるデータベースの脆弱性としては、パッチが古いこと、設定ミス、デフォルトのシステム設定が挙げられます。**データベース・サーバーが仮想化する現在、このような脆弱性はさらに複雑化しています。

現代の企業は、エンタープライズ・データを保護しコンプライアンスを実現するためのさまざまなセキュリティー・テクノロジーを備えています。クラウド活用を開始すると、データ・セキュリティーのスケーラビリティーが課題となります。最も頻繁に使用されるデータ・セキュリティー・ソリューションの 1 つである暗号化も、このような課題に直面することがあります。一部の暗号化手法は特定のハードウェアやネットワークのリソースと紐付いています。クラウド環境では、ネットワークやインフラに依存することはできません。

場合によっては、アプリケーションのテストや開発のためにクラウドを活用して、定期的に新規のデータベースの構築や解除を行っているかもしれません。このようなデータベースは動的に構築されるため、データの保護が必要です。クラウド環境のためのスケーラブルなデータ・セキュリティー手法を設定すると、新規に構築されたデータベースを自動的に検出し、含まれるデータを自動的に分類・保護・監視できます。

さらに、データ・セキュリティーのために開発した自社構築ツール (データ・マスキング・ルーチンやデータベース・アクティビティーの監視スクリプトなど) の活用も検討する必要があります。その際、仮想データベースで起動させるためにコーディングの変更が必要になったらどうでしょうか。このような自社構築ソリューションをアップデートするために多額の投資が必要になることでしょう。理想を言えば、新規のデータベースを追加するたびに既存のツールを変更しなくてもいいよう、手作業の処理を伴うことなくセキュリティーのプロセスと手続きを実行する必要があります。

つまり、ハイブリッド環境のファブリックに直接データ・セキュリティーを組み込む必要があります。しかし、整然と取りこぼしなくこれを実現するにはどうすればいいのでしょうか。

データ・セキュリティーに関する包括的な方策を実施する

包括的なデータ・セキュリティー戦略を設定すると、企業が保有するすべてのデータ (データの存在する場所とデータの使用段階を問わない) に対する 360 度のセキュリティーを実現できます。戦略に基づきハイブリッド環境全体でセキュリティー制御を一元管理し、データ管理者がセキュリティー管理者や監査担当者となることのないよう、業務分掌を実現する必要があります。

ハイブリッド環境のための堅固なデータ・セキュリティー戦略にはいくつかの主要な要素が含まれます。

機密データが存在する場所を把握する。
当初は、ほとんどの企業はすべての機密データが使用されている場所を把握できていると感じています。しかし、インフラの複雑化により、新規のデータベース、ウェアハウス、さらにはアプリケーションに機密性の高いデータを誤ってロードしているかどうか把握することが困難になります。企業が把握できない機密データは間違って分類したデータベース・テーブルやサンドボックス・環境に隠れていることが多く、恐ろしいリスクを生み出します。ディスカバリーを行うツールを活用すると、Infrastructure-as-a-Service (IaaS) タイプのクラウド・データベース内であっても機密データの検出と分類を行うことができます。

機密データを保護する。機密データ (構造化データ、非構造化データ、オンライン・データ、オフライン・データを包含する) を保護する最適な方法を 1 つに絞ることはできません。ビジネス要件とセキュリティー・パラメーターに基づき、いくつかのオプションを検討する必要があります。適切なソリューションを特定するには、まず以下の問いに答える必要があります。

- どのような種類のデータを保護する必要があるのか (構造化データか、それとも非構造化データか)。両方のニーズを満たすソリューションは存在するのか。
- 機密データをクラウドに保存する必要があるのか。ある場合、オンプレミス環境とクラウド環境の両方に保存することになるのか。このような環境でデータを共有しなければならないのか。
- データをクラウドに送信する前に、機密性を排除することはできるか。データをマスキングすることで、現実のデータではあるものの架空の結果を提供できることがあります。
- 満たさなければならない暗号化規格はあるのか。多くの法令では特定の暗号化規格が必要となる。
- ソリューションのスケーラビリティーにより、現在の要件を満たすだけでなく、ハイブリッド環境やさらにはビッグデータ環境に対応する将来のニーズを満たすことができるか。ハードウェアの暗号化や自社構築のソリューションでは、この点で課題が発生する場合がある。

確実かつ継続的にデータ・アクセスを監視する。
マスキングや暗号化などのデータの匿名化手法はデータ保護に役立つ実績のある手法です。しかし、この手法も許可ユーザーや特権ユーザーに対しては限界があります。例えば、暗号化がセキュリティー確保の唯一の手段である場合、特権ユーザーは機密情報に既にアクセスでき (暗号データへの鍵を持つ)、その行為は通常問題があるとは見なされません。このリスクを抑えるには、データ資産そのものをリアルタイムで監視することで疑わしい行動 (特権ユーザーの行動を含む) の特定と阻止をリアルタイムで行う必要があります。この手法を採用すると、許可ユーザーにシームレスに機密データにアクセスさせたうえで、異常な使用が発生した時点でセキュリティー・ポリシーを実施することができます。

コンプライアンスの達成により、監査に合格する。
コンプライアンス目標を達成することが困難になり、時間を要することがあります監査の不合格や罰金を避けるには、適用される法令が課す厳しい要件を満たすために特に設定された包括的なソリューションを追求する必要があります。このソリューションはビジネス成長と法令の変化の両方に対応できる拡張性を持たなければなりません。さらに、コンプライアンス・プロセスを合理化できるよう監査報告機能とサインオフ機能も備える必要があります。

また、異常なネットワーク・アクティビティーなどの疑わしい動きを管理者に警告するための手法も必要です。これに加え、クラウド環境とハイブリッド環境を支えるデータ・セキュリティー・プロセスはクラウド上のデータを継続的にトラッキングし、アプリケーション、データベース、ウェアハウス、ファイル・シェアを通じて誰がデータにアクセスしているのか解明する必要があります。

IBM が提供するデータ・セキュリティー・ソリューション

データ・セキュリティー・ソリューションを選択する際には、IT インフラ全体を通じてスケーラビリティーが高く統合機能を提供するソリューションを選択し、外部からの悪意のある攻撃、不正行為、不正アクセス、内部ユーザーの違反行為から物理環境、仮想環境、クラウド環境を保護する必要があります。このようなソリューションは特別なセットアップ、設定、追加の費用を伴うことなく、ハイブリッド環境で機能しなければなりません。

このような手法はデータ・セキュリティーとプライバシーを実現する効果的なプラットフォームを提供し、専門性の高いデータ・セキュリティー・リソースの削減を通じてコスト削減を実現し、セキュリティーとプライバシーに関するセルフサービス・オプションを通じて俊敏性と柔軟性を改善します。

IBM Security ソリューションと IBM Information Integration and Governance ソリューションは、以下の機能を提供することでクラウド・セキュリティー戦略を支えます。

- 仮想データベース・アクティビティーの監視、データベースの脆弱性評価、データ・リダクション、データ暗号化の機能
- クラウド上のデータのディスカバリーと分類の自動化機能
- クラウド・リソースに対して最も機密性の低いアクセスを実現する静的・動的なデータ・マスキング機能
- クラウド環境でコンプライアンスを実現できるよう、さまざまな法令に合わせてカスタマイズ可能な監査報告とコンプライアンス報告の機能
- 物理環境、仮想環境、クラウド環境の混在環境でセキュリティー制御を一元管理・自動化する機能

次のステップ: クラウド・ガバナンスの検討をさらに続ける

クラウド・ベースのデータ・サービスと処理サービスはビジネス・ユーザーにとって必須のビジネス・チャンスをもたらし、IT 部門は社内のオンプレミスのトランザクション・システムとレポーティング・システムの一貫性を管理する役割を負います。ハイブリッド環境のためのガバナンス・ポリシーの作成は、将来時点で検討すべきことではありません。今すぐに検討する必要があります。

本 e-book は、ハイブリッド環境の効果的なガバナンスのために必要な 4 つの柱の 1 つであるハイブリッド環境におけるデータの保護について解説しました。**他の柱について詳しく確認するには、本シリーズに含まれる以下の e-book をダウンロードしてください。**

- 情報ガバナンスとクラウドの現状
- 自社のデータを把握するには
- ハイブリッド環境のためにデータ統合とライフサイクル管理の戦略を開発するには
- データを準備し、管理するには

IBM のガバナンスに関するソートリーダーシップと関連テクノロジーに関する詳細情報が必要な場合は、以下の Web サイトにアクセスしてください。

- **ibm.com**/software/data/information-integration-governance
- **ibm.com**/analytics/us/en/technology/agile/

IBM グローバル・ファイナンシングはさまざまな支払いオプションを提供することにより、お客様がビジネスを成長させるために必要なテクノロジーの取得をサポートします。IBM は、IT 製品と IT サービスの取得から廃棄に至るまでのライフサイクル全体の管理を提供します。より詳細な情報は、**ibm.com**/financing で確認いただけます。

日本アイ・ビー・エム株式会社
ソフトウェア・グループ

〒103-8510
東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
2016 年 7 月

[1] IDC. 2013 U.S. Cloud Security Survey.Doc #242836.September 2013.

IMM14176-JPJA-01