salesforce app cloud

Salesforce Shield

――金融業界に最適なセキュリティサービス

新たなセキュリティレベルで金融業界のクラウドへの移行を促進

目次

はじめに

金融サービス業界は常にプレッシャーにさらされており、収益力を強化し、変化する顧客の要求にすばやく対応することが求められます。クラウドサービスに特化した俊敏性の高い金融サービス企業とも競合しなくてはなりません。このような動向が業界内でイノベーションへの投資を促す結果となっています。そして、戦略的な資産としてのクラウドに注目が集まっているのです。クラウドを活用すれば、モバイルやソーシャルへの対応力を強化し、俊敏性を高めて、変化する顧客の要求にすばやく対応できるからです。

しかし、一部の金融サービス企業は、クラウドにおけるデータのセキュリティとプライバシーの確保、多数の規制に対応する能力に不安を抱き、導入に二の足を踏んでいます。金融サービス企業が収集する情報のほとんどは、機密情報または個人情報であり、規制の対象となっています。そのため、金融サービスにクラウドコンピューティングを導入するには、インフラストラクチャ、ネットワーク、アプリケーションのすべてのレベルにおいて、常に変化する情報セキュリティ要件を満たす必要があります。さらに、機密性の高いデータのモニタリング、監査、保護を行う Salesforce Shield のような新しい制御ツールが、コンプライアンスやガバナンスに関する取り組みを合理化し、クラウドを活用した大規模なイノベーションを推進するうえで、重要な役割を果たすことになるでしょう。

> “あるゆる利点を考慮して、クラウドへの移行を決定しました。クラウドはセキュリティと拡張性を備え、データセンターの管理や通貨、言語の違いを心配する必要もありません。機能拡張も簡単です。”
>
> The Warranty Group 社、グローバルサービスおよびアーキテクチャ担当責任者、Paul Risk 氏

第 1 章

誰もが知りたいこと
クラウドはオンプレミスのサービスを上回るセキュリティを実現できるのか

クラウドの草創期から現在にいたるまで、クラウド対オンプレミスのセキュリティを対立軸とする論争は、金融サービスや医療、ライフサイエンス、政府機関など規制の厳しい業界を中心に巻き起こってきました。ガートナー社は次のように述べています。「クラウドサービスプロバイダーがエンドユーザー組織よりもセキュリティ面で劣るという証拠は一切ありません。むしろ、パブリッククラウドを利用した大手マルチテナントサービスのほうが、オンプレミスよりも攻撃に対する耐性が高いことが明らかになっています。新規に導入する場合でも、クラウドのほうがオンプレミスよりもセキュリティ面で優れています」

金融サービス業界では、単一のリポジトリを使用して、オンラインポータルからオンデマンドで顧客情報を保存、処理、表示していますが、Salesforce のマルチテナントプラットフォームはこのしくみによく似ています。また、Salesforce のモデルでは、ユーザーのトランザクションごとに一意の識別子を付与しており、このモデルも金融機関ではなじみ深いものでしょう。ただし、金融機関では地域が異なると同じ部門においてさえも、複数の異なるデータベースを使用していることが多く、その処理方法には一貫性がありません。Salesforce では、場所や顧客とは関係なく、単一のプラットフォームを使用して、すべての顧客データを一貫した方法で保存および処理しています。

創業以来、信頼性とセキュリティは、セールスフォース・ドットコムの成功の礎となってきました。

暗号化、トークン化、マスキング、難読化といったデータの匿名化は、データセキュリティモデルの中で一定の役割を果たしています。一方、Salesforce の特徴である、一貫性のあるインフラストラクチャと多層防御のセキュリティアプローチは、異種混在の企業 IT 環境において強みを発揮します。

第 2 章

信頼性の確保

世界で最も信頼される金融サービス向け クラウドプラットフォームである理由

信頼性をセールスフォース・ドットコムはもっとも重要視しています。ほとんどのグローバル企業が、厳格なガイドラインと手法を導入して顧客データを保護していますが、当社のセキュリティ戦略にもこれらは採用され、大規模なクラウド環境に適用されています。したがって Salesforce のすべてのお客様は、信頼性を確保するためのさまざまな仕組みをプラットフォームを通じて利用できるのです。

インフラストラクチャレベル

Salesforce のデータセンターでは、強力なアクセス制御対策と物理的なセキュリティ対策が講じられており、高い安全性が確保されています。生体認証や環境制御のほか、ほぼリアルタイムの複製による障害回復、バックアップなどを導入しています。また、セキュリティを 24 時間年中無休で監視する専任チーム（CSIRT）のほか、システムの可用性とパフォーマンスを監視するチームも別に設けられています。

ネットワークレベル

Salesforce は、アクセス制御や侵入検知など、ネットワークセキュリティ対策を複数導入しています。データは、転送時に AES-256 暗号化標準で暗号化されるので、お客様はそれぞれのブラウザから当社のサービスに安全に接続できます。

コンプライアンス

Salesforce は、ISO 27001、SSAE 16/ISAE 3402 SOC 1、SOC 2、SOC 3、FedRAMP、PCI-DSS、TÜV Rheinland Certified Cloud Service などの主要な国際業界標準に準拠しています。

透明性

プラットフォームの信頼性を担保するうえで、透明性は不可欠な要素です。そのため、公開 Web サイト https://trust.salesforce.com/trust/jp/ では、当社システムのパフォーマンスとインシデントに関する情報を公開しています。お客様は、当社データセンター内のインスタンスのアップタイムと応答時間を確認できます。データセンターは、マルチテナントで、地理的に分散しており、フェイルオーバーが多重に設定されています。

アプリケーションレベル

利用する環境の規模に関係なく、アプリケーションレベルのセキュリティを確保するための詳細な設定が可能です。シングルサインオン、厳格なパスワードポリシー、ロールベースおよびプロファイルベースのアクセス制御など、ユーザーがデータにアクセスする方法、場所、タイミング、使用するデバイスについて、個々の項目レベルで詳細に設定できます。

“決済テクノロジーのトップ企業として世界各国でサービスを提供する当社は、連邦政府や国際的なコンプライアンス基準が定める厳格な規定を遵守しています。Salesforce Shield によってアプリにもさまざまなコンプライアンス機能を組み込むことが可能になり、よりお客様のニーズに沿ったサービスを提供できるようになりました。”

ファーストデータ社、技術部門上級副社長、Steve Petrevski 氏

第 3 章

Salesforce Shield
信頼できる高いセキュリティレベルの実現

企業がクラウドに保存するデータの量は増加しており、適切な管理手法とポリシーの適用によってデータへのアクセスを管理することが、これまで以上に重要になっています。このような状況のなかで、コンプライアンスとガバナンスに複雑な要件を持つ企業に対し、当社プラットフォームのセキュリティをさらに強化するために提供するのが Salesforce Shield です。Salesforce Shield では、クラウドデータのガバナンスとコンプライアンスについて、ライフサイクル全体の管理に不可欠な 3 つのサービスを提供しています。

監視と予防

イベントモニタリング

インテリジェンスを使用して、データの不正な使用を検出および防止します。

- ユーザー操作の記録
- リアルタイムのアラート
- 予防機能

Salesforce 上に構築されたすべてのアプリケーションを対象に、詳細な利用状況を確認できます。誰が、いつ、どこから重要なビジネスデータにアクセスしているのかを把握できるだけでなく、利用パターンを分析することもできるほか、操作に対するアラートを送ったり、操作のブロックをリアルタイムに実行したりするなどのセキュリティポリシーを実装することも可能です。

予防と保護

暗号化機能

データへのアクセスを制御します。

- 保管されている機密データの暗号化
- 暗号化キーの管理

Salesforce はクラウドとエンドユーザーとの間の通信をすべて暗号化しますが、一部の規制や社内ポリシーによっては、PII[1] などの機密データについて、その保管中もさらに保護が必要になることがあります。Salesforce Platform の暗号化を利用すれば、保管されているデータとファイルをワンクリックで暗号化できます。暗号化した後でも、検索やワークフロー、入力規則などの重要なアプリケーション機能は影響を受けません。

保持と監査

項目監査証跡

データを保持して完全性と可監査性を確保します。

- 最長 10 年間のデータ保持と
  アーカイブポリシー
- クエリベースでの項目履歴の取得

金融サービス業界では、規制を遵守するために、顧客の財務データに対する変更内容を一定期間にわたり適切に保持する必要があります。項目監査証跡は、フォレンジックに必要となる監査証跡の作成に利用できるように、最長 10 年分の履歴を保持します。企業はデータ保持ポリシーを定義でき、指定したスケジュールに沿ってデータを自動的に削除できます。これによって、規制の対象となるデータのライフサイクルをカテゴリごとに自動管理できるようになります。

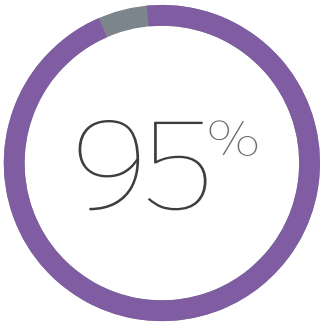
[1] PII - Personally Identifiable Information の略。個人を特定できる情報のこと

“

金融サービスを提供する企業として、当社は大きな責任を負っています。機密情報であるお客様の PII データを大量に保管しているのです。規制に準拠するために、膨大な数のデータポイントを詳しく確認し、管理しなければなりませんが、Shield のおかげでコンプライアンスに関する業務が簡素化され、事業の中核をなす業務にリソースを集約できるようになりました。

LendingPoint 社、CTO、Franck Fatras 氏

”



ガートナー社によると、2020 年までにクラウドで発生するセキュリティのトラブルの 95% は、顧客側の要因によるものであると予測されています。

『Clouds Are Secure: Are You Using Them Securely?』、Jay Heiser 著、2015 年 9 月 22 日

salesforce app cloud

第 4 章

イベントモニタリング
ユーザー操作の可視化

金融サービスに携わる企業には、ユーザーによる機密データへのアクセスを可視化することが求められます。データの漏洩を確認するために必要な情報はすべてログに記録されていますが、実際に脅威を特定するには、膨大な量のログデータを解析しなければなりません。

言い換えれば、問題にすばやく対応するには、不審な利用パターンを特定するための、簡単に使える利用状況ログが必要になるということです。

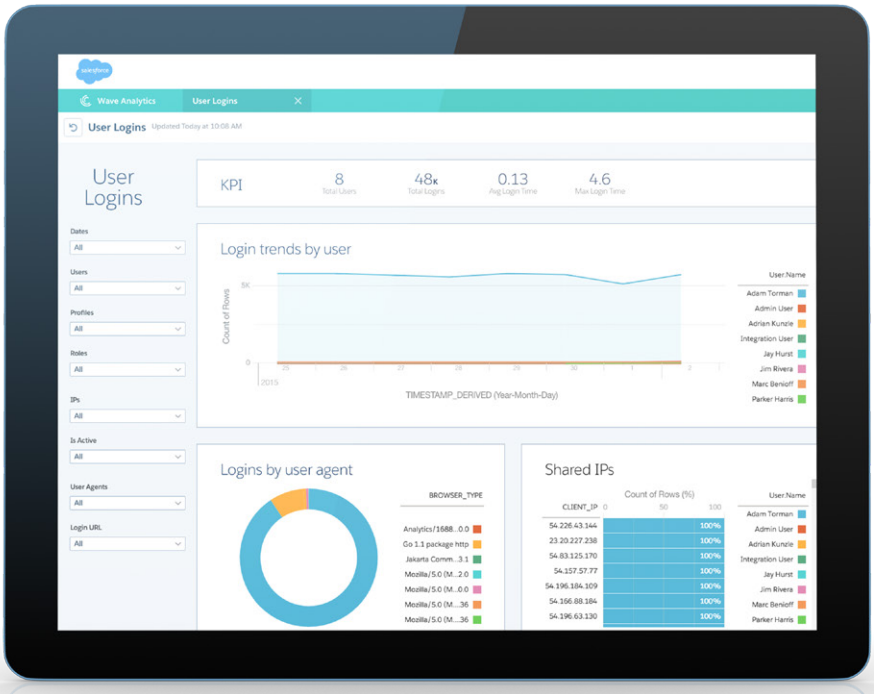
イベントモニタリング機能によって、利用状況に関する一連のログから、有用な情報を読み取ることができます。

イベントモニタリング機能を利用すれば、ユーザーが、どのデータに、どこからアクセスしているか、そのデータをどのように操作しているかを、詳しく知ることができます。

金融サービス企業の場合、記録対象の操作として一般的にはページやリストの印刷、レコードの編集や作成、所有権の変更やリストの更新、あるいは、富裕層の顧客データのエクスポートなどが考えられます。

ニーズに応じた柔軟な利用が可能

データプレゼンテーション層に求める内容は企業ごとに異なりますが、イベントモニタリングでは、コンプライアンス上重要なデータに API 経由で簡単にアクセスできるので、Splunk や New Relic、FairWarning、Salesforce Wave Analytics など、任意のツールでイベントを分析およびビジュアル化することが可能になります。



第 4 章

金融サービス業界における モニタリングのニーズ

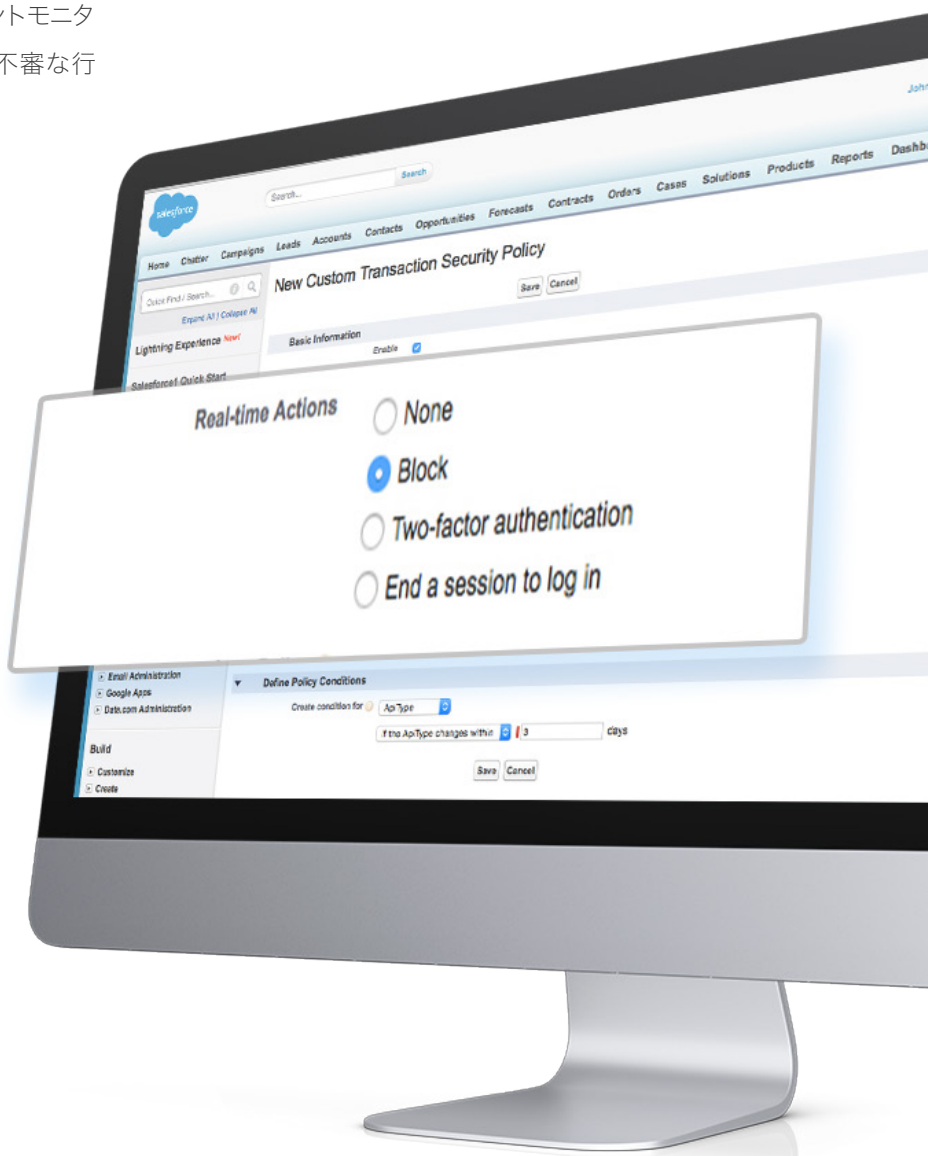
業界の規制

イベントモニタリングによって、COSO フレームワークが推奨する方法で、ユーザーの操作を簡単に監視できるようになります。また、SOX や FFIEC、PCI などの規制への準拠も容易になります。

サーベンス・オクスリー法では、不正行為のリスクと統制対策を評価するよう企業に求めており、通常このような場合、データの盗難や消失につながるおそれのあるシナリオを想定する必要があります。イベントモニタリング機能では、ダッシュボードを構成して不審な行動を簡単に検出することが可能です。

一方、FFIEC によるセキュリティ規制では、機密リソースへのユーザーのアクセスならびに、セキュリティイベント発生時のアラートを、記録、監視するよう銀行に求めています。イベントモニタリング機能では、操作が行われた時刻と場所 (IP アドレス)、ある操作とそれに続く一連の操作などを記録し、わかりやすく表示することができます。

イベントモニタリングは、
問題の対策につながる
情報を提供するだけでなく、
その情報にもとづいて、
アラートを送信したり
アクションを自動化したり
できます。



salesforce app cloud

内部のリスクとガバナンス

金融サービスを提供する企業には、操作ログの監視を高度に自動化してセキュリティリスクに対応することが求められています。

銀行は誰がデータを閲覧、ダウンロードしているかを監視することで、顧客のデータを保護することができます。

ハッカーが利用者のアカウント情報を盗み出して不正ログインを行った場合でも、イベントモニタリングを行っていれば、銀行は詳しい調査を行うことができます。また、データの消失やその前兆となる不審な操作を分析できるだけでなく、融資手続きなどの複雑なワークフローにおけるお客様とのやりとりを監視して利用パターンを把握し、プロセスの改善につなげることも可能です。

また、ウェルスマネジメントを行う企業であれば、担当者の行う操作を記録することで、レポートやリスト、ファイルに含まれる競合クライアントのデータを保護して、他社にデータが漏れるリスクを軽減することができます。

第 4 章

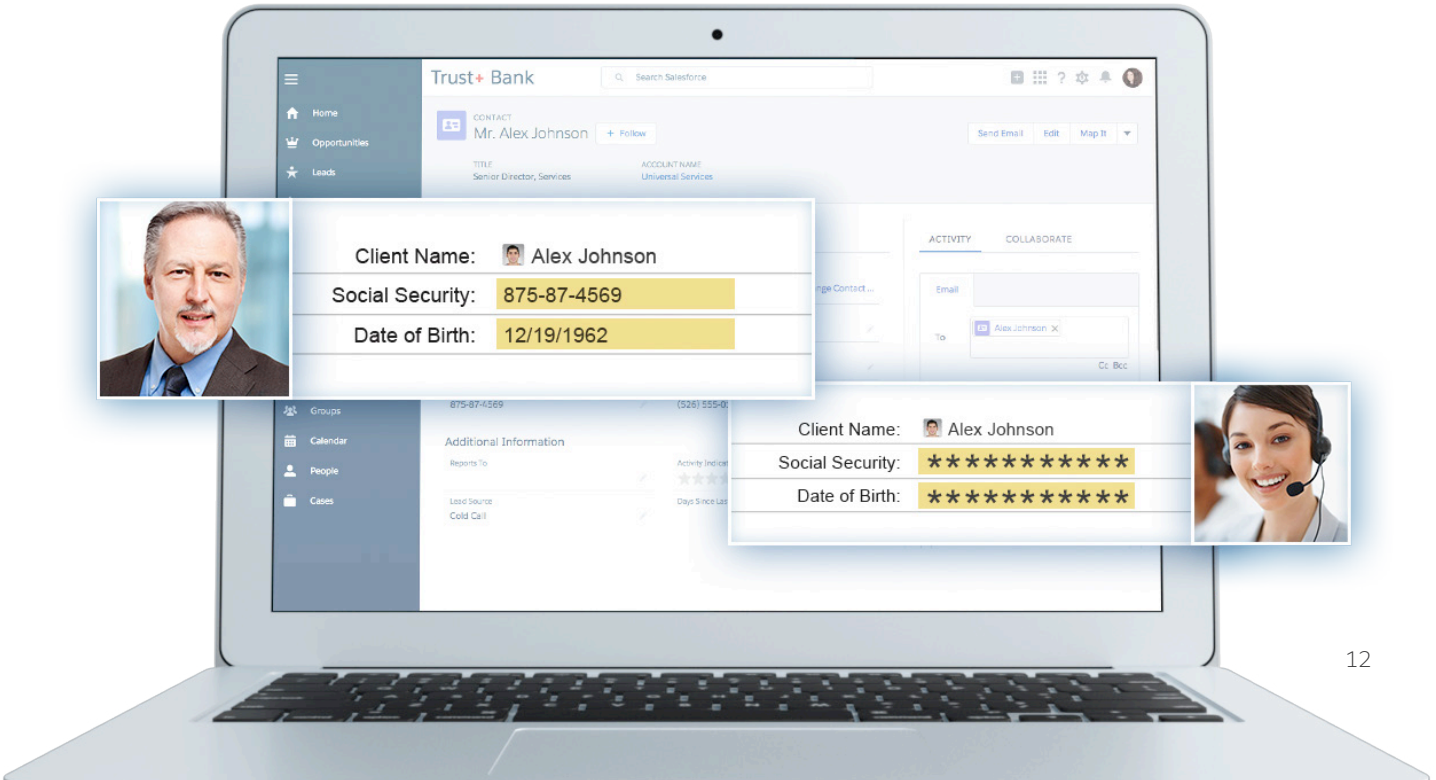
暗号化機能

機能性はそのままに PII データを暗号化

Salesforce は、通信データの暗号化などによって、お客様のデータを強力に守っています。しかし、金融サービス業界で Salesforce の採用が広がった結果、追加の保護要件を満たす必要のある機密データが、大量にクラウドに保管されるようになりました。これらのデータに適用される要件には、クレジットカードに関する情報を保護する PCI DSS や、SOX/J-SOX、NCUA、GLBA のほか、データプライバシーおよびデータレジデンシーに関する法律などがあります。こうした規制によって、データの保管場所を問わず、機密データを保護する必要が生じています。ほとんどの規制では暗号化を具体的な要件として定めてはいませんが、お客様は Salesforce Shield の暗号化機能を導入して、レベルの高いコンプライアンスを確保しています。

暗号化機能によって、入力項目や、ファイル、添付ファイルの機密データを暗号化して保管できます。

データはデータベースのメタデータ層で暗号化されるので、グローバル検索や入力規則といった Salesforce の主要なアプリケーション機能は、暗号化されているデータに対しても機能します。暗号化機能はプラットフォームにネイティブに組み込まれており、ワンクリックで設定できます。



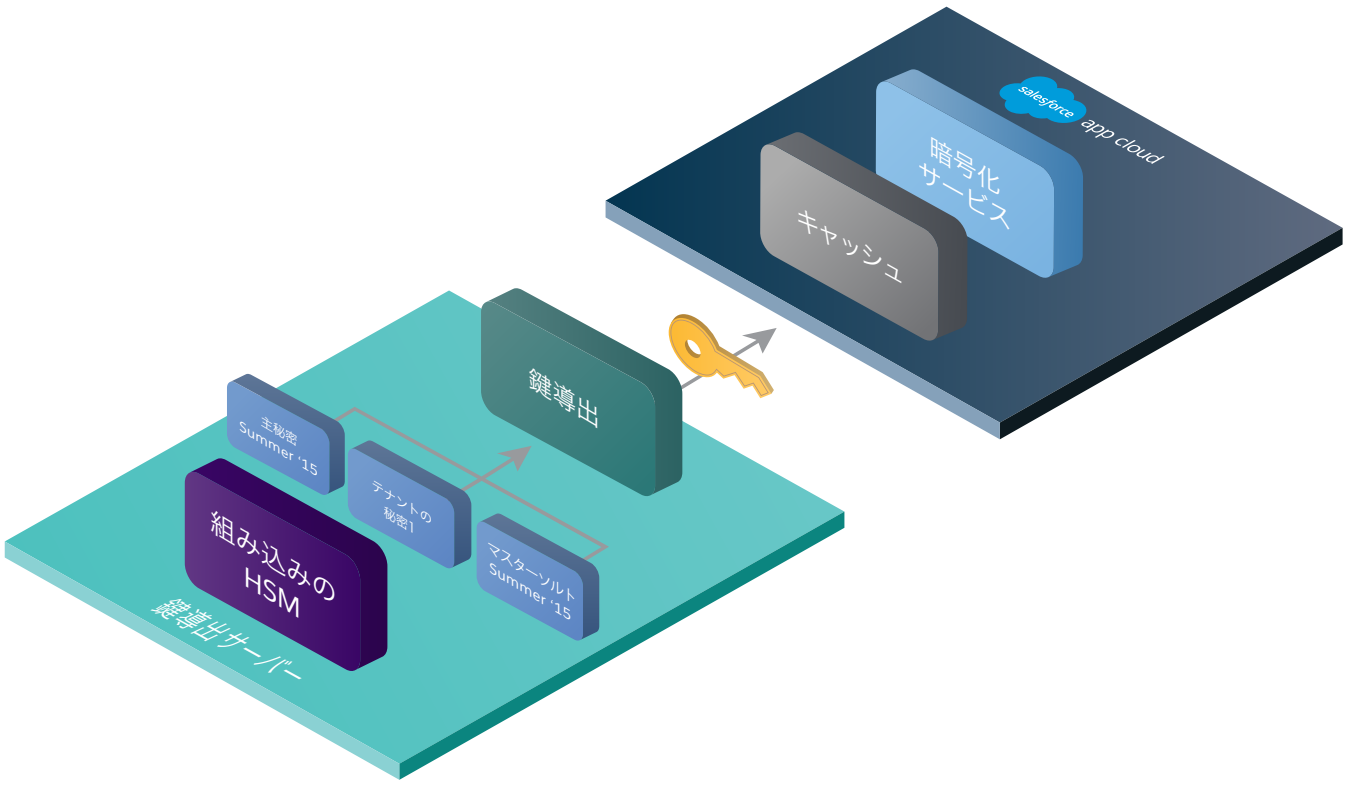
第 4 章

シンプルな宣言型ユーザーインターフェースを支える洗練されたエンジン

Salesforce Shield の暗号化機能では、業界標準の FIPS 認定 4096 ビット RSA 非対称鍵と 256 ビット AES 対称鍵が暗号解読ブロックチェーン（CBC）モードで使用されています。これらの鍵の一意の組み合わせと、リリースごとの Salesforce の主秘密のローテーションによって、ユーザーに固有の 256 ビット長の派生データ暗号化鍵が生成されます。データの暗号化と復号には、この鍵が使用されます。これらの鍵の生成に使用される個々の秘密は、固有の順番で、さらに断片化、ラップ、ラップ解除されて強力な職掌分散が実現し、堅牢な鍵管理モデルとなります。

Salesforce Platform の暗号化の詳細はこちらから。

ホワイトペーパーをダウンロード（英語）



第 4 章

保管されているデータの暗号化ニーズ

あらゆる国の多様な金融サービス企業が、規制を遵守するだけでなく、セキュリティを強化するために、保管しているデータを暗号化したいと考えています。銀行では特に社会保障番号、クレジットカード番号、口座番号、氏名などの NPPI/PII データの保管に注意を払っています。データの暗号化を推し進めるべき理由は次の 3 つです。

1 業界の規制

PCI 規制では、保管しているクレジットカードのデータを暗号化するよう求めています。画像や PDF などのドキュメントにクレジットカードのデータが記載されている場合は、ドキュメントも暗号化する必要があります。FFIEC（米国連邦金融機関検査協議会）では、金融機関が包括的なデータインベントリと適切なデータ分類プロセスを整備していることが不可欠であるとしています。また、PII などの顧客データへのアクセスが、ID とアクセスの確実な管理によって適切に制限されることも重視しています。一方、マルチテナントクラウドでは、複数の顧客がネットワークリソースを共有するため、暗号化を通じたデータ保護の必要性が高まっています。

2 内部ポリシー

金融サービス企業では、内部ユーザーによる悪用から顧客の機密データを保護するケースがあります。たとえば、富裕層や著名人に資産管理サービスを提供している企業では、これら顧客の情報を暗号化して身元を隠し、一部のユーザーだけにデータのアクセスを許可するといったことが考えられます。

3 地域による要件

国際的な業務展開も、クラウドデータにおける必要な保護レベルを引き上げる重要な要因となりえます。たとえば、一部のアジアまたはヨーロッパ市場に拠点を展開する銀行では、現地の厳格な規制に対応するために、保管しているデータの暗号化を規制で明確に指示していない場合でも、データの暗号化を選択することがありえます。

第 4 章

Salesforce の暗号化導入のベストプラクティス

まずは Salesforce に標準で搭載されている各種アクセス管理機能を利用してみましょう。次に、プラットフォームレベルの暗号化を導入します。プラットフォームレベルの暗号化が既存のセキュリティ層を覆い、多層防御アプローチによって、保管されているデータが保護されます。

暗号化を有効にする前に、データのライフサイクル管理全体を見直して、内部の情報セキュリティガイドラインと原則に従い、各データ要素の定義、カタログ作成、分類を行う必要があります。

データが保管または処理される場所に関係なく、データに対するセキュリティアプローチを統一することで、暗号化が必要なデータが明確となります。

すべてのデータを暗号化の対象にするのではなく、暗号化の適用範囲を十分に検討し、規制や法律によって保管時に暗号化を必要とするデータ要素を絞り込む必要があります。暗号化が不要な入力項目やオブジェクトのデータについては、暗号化しない形式で保管し、拡張機能を引き続き利用できるようにするべきです。

第 4 章

項目監査証跡

フォレンジック監査証跡による、データの整合性の強化

PII や顧客担当者による操作、通信の内容など、金融サービスで扱うデータの多くには、フォレンジックに必要な監査証跡を保持するよう求める規制が課せられており、監査人が特定のイベントに関連するデータの状態をすぐに把握できることが重要です。

すべての顧客によって生成されるデータは膨大な量となり、監査データの保持および管理はますます困難になっています。一体、項目レベルの監査データは何年間保管するべきなのでしょうか。監査を実施する必要が生じた場合に、履歴データに簡単にアクセスすることはできるのでしょうか。企業には、項目レベルの監査証跡データの保持を簡素化するツールが必要です。

項目監査証跡機能を使用すれば、任意の日付のデータの状態と値をいつでも確認できます。

項目監査証跡機能では、特定の入力項目の値が時間の経過とともにどのように変化したかを完全に記録できます。Salesforce のお客様は、最長 10 年、1 オブジェクトあたり 60 項目まで、項目レベルのデータ保持ポリシーを設定できます。項目監査証跡機能はビッグデータに対応したバックエンドを基盤としているため、きわめて高い拡張性があり、即座に監査データにアクセスできます。

また、Salesforce Wave Analytics や Splunk などの分析ソリューションを活用すれば、監査履歴を可視化、分析して、有用な情報を得ることが可能です。

第 4 章

金融サービス業界における監査証跡のニーズ

金融サービス業では、変更追跡を容易に監査できるようにして、顧客データの整合性を確保する必要があります。このようなコンプライアンスやガバナンスの要件に対応するうえで、項目監査証跡機能が役立ちます。例を以下に挙げます。

業界の規制

数々の規制の存在によって、銀行は、顧客の氏名、住所、メールアドレス、電話番号、通信設定などの主要なビジネス要素（KBE）に対する変更を監査し続けることが必要になっています。PCI では、変更されたテーブルとオブジェクト、変更された入力項目の名前、変更の種類（挿入、更新、削除）、変更前後の値などを追跡することを銀行に求めています。項目監査証跡機能を使用すれば、こういったデータの保持とアーカイブを自動化できます。さらに、リアルタイム API やバッチ API から項目監査データを利用できるようにすれば、監査手続きを合理化することも可能です。必要なレポートを簡単に作成できるようになり、フォレンジック分析チームとインシデント対応チームの両方でデータを利用することもできます。

内部統制ポリシー

項目監査証跡機能の主な用途は、データの整合性確保と、社内インシデント対応です。たとえば、ウェルスマネジメントサービスを提供する企業の場合、項目監査証跡機能によって、AUM（運用資産額）や勘定残高、手数料、コミッションなどの主要な金融データに対する変更内容を監査して、不適切な変更や不正な行動を検出することができます。

さらに、不正な操作や人的ミスによって破損したデータを復元するといったリスク対策やガバナンスの用途にも利用できます。

ユーザープロファイルや役割、権限、グループなどのシステム管理項目とセキュリティ関連項目に対する変更内容を監査すれば、ソーシャルエンジニアリングの検出と防止も可能となり、セキュリティ担当者は、管理者などのシステムユーザーによる疑わしい操作を把握できます。

第 4 章

Salesforce Shield
銀行での使用事例

- 権限を使用して、カード保有者データへのアクセスを制限 (Salesforce のすべてのお客様が使用可能)。または、データを暗号化して保管することでセキュリティを強化
- 画像や PDF などのドキュメント内に保管されているクレジットカードのデータを暗号化し、機密データへのアクセスをさらに制限
- 項目監査証跡機能を使用して、氏名や住所、メールアドレス、電話番号、通信設定などの主要なビジネス要素 (KBE) に対する変更内容を監査
- 抵当書類を暗号化し、ファイルへのアクセスを管理することで、顧客の PII データを保護

78%

サイバーセキュリティに関する銀行の評判を重視するお客様 [1]

57%

サイバーセキュリティ上での脅威の巧妙化が進んでいると述べている銀行管理職 [1]

56%

セキュリティインシデント対応をさまたげる要因として、エンドユーザーによる機密データへのアクセスを十分に把握できていない点を挙げている企業 [2]

[1] CDW Research、『In Cybersecurity We Trust?』、2014 年 8 月
[2] Ponemon Institute、『The Second Annual Study on Data Breach Preparedness』、2014 年 9 月

第 4 章

Salesforce Shield

ウェルスマネジメントでの使用事例

- 富裕層や著名人の顧客の情報を暗号化し、身元を保護
- 顧客のデータに、いつどこから誰がアクセスし、どのような操作をしたかといったアクセスの状況を監視
- 顧客のポートフォリオと資産の所有権に対する変更の証跡を保持
- 代理人の助言により発生した変更の監査証跡を保持
- AUM（運用資産額）や勘定残高、料金、手数料などの主要な金融データに対する変更内容を監査
- 適切なデータ変更と不適切なデータ変更を区別して、監視、検出。不正な行動を監視、検出

55%

資産管理サービスを提供している企業のうち、クラウドデータ（リスク）管理の質に満足している企業 [1]

31%

セキュリティイベントの管理テクノロジーを備えている企業 [2]

60%

ウェルスマネジメントサービスを提供するグローバル企業のうち、2015 年の主要な問題をサイバーセキュリティであると述べている企業 [3]

[1] EY、『Risk management for wealth and asset management』、2014 年
[2] Ponemon Institute、『The Second Annual Study on Data Breach Preparedness』、2014 年 9 月
[3] Cerulli Associates Europe、2015 年 2 月のレポート

第 4 章

Salesforce Shield
保険業での使用事例

- 被保険者に関する機密情報へのアクセスを監視および制御（アラートとアクション）
- 追加のセキュリティ対策として、PII や PHI などの被保険者の機密情報を暗号化
- 被保険者の記録に対する変更内容を保存するためのポリシーを定義して、監査に対応
- 代理人による、顧客の口座データと関連レポートの使用状況を監視し、疑わしい使用パターンにはアラートで通知
- 顧客対応部門がインシデントデータに対して行った変更を保存するためのポリシーを定義
- インシデントケースに関連する機密データを暗号化

86%

今後 3 年間にセキュリティ予算が増加すると見込んでいる保険業者 [1]

81%

サイバーセキュリティ上の脅威の巧妙化が進んでいると考えている保険業者 [1]

72%

クラウド上のセキュリティリスクを軽減するためのポリシーと手順を整備している保険業者 [1]

[1] 米ニューヨーク州金融サービス局（NYDFS）による調査、『Report on Cyber Security in the Insurance Sector』、2015 年 2 月

salesforce app cloud

まとめ

金融サービス業界のセキュリティニーズを満たすクラウドの実現

今日、サービスの利用者が銀行業に求めるのは、Uber にみられるような、個々の状況に即したオンデマンドのユーザー体験です。そして、企業がこのようなユーザー体験を実現するうえで、クラウドが重要な役割を果たしています。データの可能性を閉じ込めたまま今と同じサービスの提供を続けていくのか。それとも、クラウドを活用して、モバイルやソーシャル、そしてインターネットに接続された無数のデバイスを対象にサービスの品質を高め、ロイヤリティプログラムを強化し、状況に即したリアルタイムのユーザー体験を提供していくのか。いま、金融サービス業界の CIO はこれまで以上にその選択を迫られています。

Salesforce を利用している金融サービス業界のお客様は、営業やマーケティングだけでなく、サービスや日々の業務管理にいたるまで当社サービスを利用しています。その結果、当社のクラウドに保管される PII などの機密データは、かつてないほどに増加しています。16 年間にわたってプラットフォームの信頼性を強化し続けた結果、当社のセキュリティ機能はほとんどの企業が自前で用意できる機能を上回っています。したがって、考えるべきは Salesforce のクラウドの安全性ではなく、クラウド上のデータへのアクセスをどのように効率的に管理、制御するかということです。

Salesforce Shield は、金融サービス業界のお客様がより多くのビジネスプロセスとデータをクラウドに移行するうえで、欠かせないセキュリティサービスを提供します。使用状況の分析から、最適なポリシーの策定、機密データの保護強化にいたるまでサポートを行い、イノベーションの推進とより迅速な顧客対応の実現に向けて、リソースの集約を可能にします。

Salesforce Shield をもっと詳しく

WEB ページへ

Salesforce Shield に関するお問い合わせ

お問い合わせ