

# 金融サービスのデータ保護とセキュリティ

知っておくべき重要なポイント

金融サービス機関ではクラウド化が進んでいます。その一方で規制当局は、特にデータに関して、企業が業務中断に適応し、回復できるかどうかを精査しています。

懸念される主な規制の動向には、データプライバシーやサイバーセキュリティに関するものに加えて、ヨーロッパの金融機関内およびヨーロッパの金融機関とビジネスを行っている企業を対象とした GDPR と Schrems II が含まれます。

## データプライバシー

金融サービス企業は規制当局から、重要な情報資産とその基盤となるインフラストラクチャを特定するよう求められています。また、これらの情報資産が銀行の重大な業務にとって重要であることを踏まえ、サイバーセキュリティへの取り組みを優先する必要があります。

### リモートアクセス、迅速な導入、および帯域幅の拡張に関する考慮事項：

**リスクの軽減：**テクノロジーやアプリケーションの中断や侵害に関連する潜在的なリスクを事前に計算します。

**管理：**リモート資産の使用、管理者ユーザー、およびアプリケーション開発を含むプロセスを定義、文書化、および展開します。

**ICT パートナiership：**長期的なリモートアクセスに対応するための正しい姿勢を維持するために、サイバーセキュリティを含む ICT チームを定期的にアップデートします。

サイバーインシデントの発生後に重要な情報の完全性を維持するための計画を策定し、重要な情報資産の脅威プロファイルを定期的に評価することが不可欠です。また、定期的に脆弱性をテストし、ICT 関連のリスクに対するレジリエンスを確保することも重要です。

## サイバーセキュリティ

サイバー攻撃はますます高度化しているだけでなく、デジタル化、相互接続性、サードパーティーへの依存の高まりによって、個々の機関だけでなく市場全体を混乱させる可能性が高くなっています。

企業のレジリエンスを維持し、向上させることは、組織がお客様や規制当局との信頼を築くための新しい方法です。

テクノロジー資産は最新の状態に維持し、パッチを適用して、

### 欧州中央銀行の金融市場インフラに対する期待水準：

**進化：**サイバーリスクを特定、管理、緩和するために必要不可欠な能力が確立され、進化し、維持します。実践のパフォーマンスを監視・管理します。

**進歩：**これまでのレベルに加えて、部門全体を統合し、時間の経過とともに改善された、より高度なツールを実装して、先を見越してサイバーリスクを管理します。

**革新的：**これまでのレベルに加えて、FMI とより広範なエコシステムの人、プロセス、テクノロジーのイノベーションを推進して、サイバーリスクを管理し、サイバーレジリエンスを強化します。これには、新しいコントロールとツールの開発、または新しい情報共有グループの作成が必要になる場合があります。

新しいサイバー脅威や既存のサイバー脅威、サポート対象外のテクノロジーを軽減する必要があります。技術的負債に対処するためには、大規模な変更プログラムを確立する必要があるかもしれません。

## Schrems II

この裁定は、主にデータ主権と、PIIの保管/格納場所の管理に関するものです。米国への個人データの転送に関しては、米国のプライバシーシールドフレームワークを認定する十分性のある取り決めが行われていました。欧州司法裁判所が2020年7月に下したこの判決は、プライバシーシールドの妥当性を事実上排除し、米国とEU間のデータ転送に不確実性をもたらしめるものです。

### 欧州データ保護委員会は、越境移転と移転先の第三国を評価するための6つのステップを設定しています。

- 移転元に移転を知らせる
- 移転に使用する移転ツールを確認する
- 第三国の法律または慣習法が移転に対するセーフガードの有効性に影響を及ぼす可能性があるかどうかを評価する
- データ移転に関して、データ保護レベルをEUの基準と本質的に同等レベルにまで引き上げるための措置を特定し採用する
- これらの補足措置を採用するための正式な手続き上の手順を踏む
- 適切な間隔をあけて再評価し、データ移転に影響する可能性のある変化を監視する

英国はEUから離脱したため、Schrems IIは英国に直接影響を及ぼすようには思われなくても、英国はEUから「金メッキ」規制を受ける傾向があります。彼らは、EUの裁定から逸脱したくないかもしれませんが、またはEUの慣行法から逸脱しているように見えるかもしれません。

## GDPR

EUの個人データ保護法は、世界中の企業に影響を与えるもので、2018年に施行されました。GDPRは、個人を特定できる情報(PII)を使用して企業ができていないことを示しています。

PIIには以下の項目が含まれます(ただし、これらに限定されません)。

|         |              |
|---------|--------------|
| 名前      | ソーシャルメディアの使用 |
| 電話番号    | 位置情報         |
| 住所      | 健康に関する記録     |
| 生年月日    | 人種           |
| 銀行口座    | 宗教           |
| パスポート番号 | 支持する政党       |

個人データの紛失、盗難、破壊、変更につながるすべてのインシデントはデータ侵害と見なされ、最大2,000万ユーロ(2,300万ドル)または企業の全世界年間売上高の4%の制裁金が科せられる可能性があります。

## 必要なアクションとは？

デジタルファーストが標準的な運用モデルになるため、データの保護とセキュリティは、将来のグローバルな金融サービス機関にとって大きな懸念事項です。データの取り扱いに影響を与える新しい規制があっても、最小限の混乱で対応できるよう、柔軟性が今後の成功の重要な要素となるでしょう。新しいハイブリッドおよびマルチクラウドインフラストラクチャは、究極の柔軟性をもたらすでしょう。複数のクラウドプロバイダー間でデータを移行し、ワークロードを移動させることができるようになります。また、必要に応じてオンプレミスに戻すことも可能です。データの移動は、混乱を最小限に抑えながら、迅速に行うことができます。

## テラデータについて

テラデータは、コネクテッド・マルチクラウド・データプラットフォームを提供する企業です。テラデータのエンタープライズアナリティクスは、ビジネスのあらゆる課題を解決します。大規模な混合データワークロードを今、そして将来も処理できる柔軟性を実現するのは、テラデータだけです。Teradata Vantage アーキテクチャは、クラウドネイティブで、as-a-service で提供され、オープンなエコシステム上に構築されています。こうした設計上の特徴により、Vantage はマルチクラウド環境でコストパフォーマンスを最適化するための理想的なプラットフォームとなっています。詳しくは、[Teradata.jp](https://www.teradata.jp) をご覧ください。

17095 Via Del Campo, San Diego, CA 92127 Teradata.jp

Teradata および Teradata のロゴは、Teradata Corporation およびその関連会社の米国およびその他の国における登録商標です。テラデータは、新しいテクノロジーやコンポーネントの登場に合わせて製品を改善し続けています。そのためテラデータは各種仕様を事前の通知なく変更できる権利を留保します。地域や市場によっては、本書に記載されている機能、仕様、動作の一部を利用できない場合があります。詳細については、テラデータの営業担当者、または [www.teradata.jp](https://www.teradata.jp) よりお問い合わせください。

© 2021 Teradata Corporation All Rights Reserved. Produced in U.S.A. 01.22



teradata.