外部サプライヤー管理義務

物理的セキュリティー（技術的管理）

2024 年 10 月付け第 14.0 版

管理対象	管理内容	本件が重要である理由
1.アクセス管理（TC 5.1）	アクセス管理ルールは、保護区域のすべてに対して定義され、正式に承認された手順でサポートされ、責任が定義されている必要があります。 保護区域は、電子的、機械的、またはデジタル的アクセス管理を使用して、適切なエントリーコントロールとアクセスポイントによって保護する必要があります。 電子アクセス制御システムへの論理的および管理的アクセスは、権限を持つ者に制限する必要があり、物理的キーおよび組み合わせへのアクセスは厳重に管理および制御する必要があります。アクセス許可の付与、修正、取り消しを含む、資格情報/キー/組み合せ所有者の監査証跡を維持する必要があります。 不正アクセスのリスクを軽減するため、アクセス認証情報はすべて有効に管理する必要があります。アクセス認証情報は、サプライヤーのアクセス管理手順に沿って管理する必要があります。 一意のアクセス認証情報は、適切な承認を受けた場合に限り発行される必要があります。 制限区域へのアクセス認証情報はすべて、適切な頻度で再認証する必要があります。 施設や制限区域へのアクセスが不要になった場合、アクセス認証情報は、該当する事業単位または機能から当該従業員の要件変更（役割または責任の変更、雇用の終了など）を知らせる通知を受けてから 24 時間以内に、アクセス認証情報の管理を担当する機能によって無効化される必要があります。	効果的なアクセス制御システムとアクセス管理プロセスおよび手順を維持することは、不正アクセスから施設を保護し、資産のセキュリティを確保するために必要な階層的に組み合わされた管理の重要な要素です。有効なアクセス管理が行われていない場合、認可されていない人がサプライヤーの敷地や敷地内の制限区域に侵入するリスクがあります。これにより、Barclays 資産の損失や損害が発生し、それによる金銭的損失またはそれに伴う風評被害、および/または規制上の罰金・問責のリスクが高まる可能性があります。

2. 境界、建物、場所のセキュリティ（TC 5.2）	セキュリティ境界は、情報やその他の関連資産を収容している区域を保護するため、定義され、実装される必要があり、また、特定され、予測されるリスクおよび脅威環境に見合ったものである必要があります。オフィス、部屋、施設のための物理的セキュリティ（アクセス管理システム、セキュリティカメラ、侵入検知システム、その他の適切な技術的管理を含む）は、現在の脅威レベルおよび予想される脅威レベルに基づいて、リスクベースのアプローチで設計・実装され、実施されるビジネスプロセスおよび情報・資産の価値に見合ったものでなければなりません。 保護区域で作業するためのセキュリティプロセスを設計し、実装する必要があります。紙やリムーバブルストレージメディアに関する明確なデスクルールと、情報処理施設に関する明確な画面ルールを定義し、適切に実施する必要があります。 単独型、共同設置型、サードパーティのデータセンターに加えて、クラウドプロバイダー、データホール、通信設備（サーバールーム、単独型通信キャビネットを含む）はすべて、バークレイズの資産やデータに対する不正なアクセスや盗難、損害を防ぐために効果的に保護する必要があります。設置場所が共有されている場合は、個別分離と監視を実行するための効果的なセキュリティ管理を導入する必要があります。	これにより、制限されている場所への不正アクセスにより発生する、データセンター、データホール、サプライヤーの施設（サプライヤーが維持するものとサードパーティの両方）に保管されているバークレイズの資産またはデータを、損失、損傷、または盗難のリスクから保護することができます。
3.インフラストラクチャおよび資産に対する物理的な脅威からの保護（TC 5.3）	インフラストラクチャおよび資産に対する物理的な脅威に対する保護は、セキュリティカメラ、侵入者検知システム、および/または現在の脅威環境と予想される脅威環境に適したその他の階層型セキュリティ管理の導入を通じて設計および実装する必要があります。施設は、無許可の物理的アクセスがないか、継続的に監視する必要があります 機器は安全に設置され、保護されている必要があります。電源、データ、またはサポート情報サービスを伝送するケーブルは、物理的な傍受、干渉、損傷のいずれからも保護する必要があります。セキュリティ機器およびインストールは、製造元の要件に従ってインストールおよび維持し、	現在の脅威および予想される脅威に見合った物理的セキュリティ管理を導入し、運用することで、不正アクセス、盗難、または意図的な損傷による施設および資産への影響を抑えたり、防止したりすることができます。

	情報の可用性、完全性、機密性を確保するために監視する必要があります。 オフサイトに保持されているバークレイズの資産は、保管時および輸送時に保護する必要があります。 情報の可用性、完全性、機密性を確保するために、機器を適切かつ一般的な業界標準に合わせて設置および維持する必要があります。セキュリティシステムすべての設置および操作は、現在の法的要件および規制要件に準拠する必要があります。 配送エリアと搬入エリアが存在する場合は、それらを適切に管理し、運営施設から隔離することで、未承認のアクセスおよび未検証の配達物から派生する恐れのある脅威を防止する必要があります。	

本標準は、以下の標準と併せて読み、その範囲として特定された管理を適用する必要があります。

サードパーティーのサービスプロバイダーの管理義務（TPSPCO）、管理要件 - 情報、サイバーおよび物理的セキュリティ、テクノロジー、復旧計画、データプライバシー、データ管理、PCI DSS および EUDA。