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）

2022 年 10 月付け第 12.0 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）	電子的、機械的、またはデジタルアクセス管理は、Barclays の契約に関連する活動を行うすべての敷地内に配置され、管理される必要があります。セキュリティシステムはすべて、法的および規制要件に従って設置、運用、保守される必要があります。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。 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。 施設や制限付きエリア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、解雇、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。 サプライヤーまたは下請業者が、物理的または仮想的な形式で、その性質上制限されている Barclays の情報（知る必要がある場合に限ってサプライヤーに提供される個人データまたは機密情報を含む）にアクセス、保存、または処理する際に遠隔操作が必要な場合、サプライヤーは、このデータへのアクセスを許可する前に、Barclays とのこれらの取り決めを承認しなければなりません。	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.侵入者検知システム・防犯カメラ（TC 5.2）	不適切なアクセスや犯罪行為を抑止、検知、監視、特定するために、侵入者検知システム（IDS）や防犯カメラを導入する必要があります。設備は、各場所のセキュリティリスク評価により特定された物理的なセキュリティ上の脅威に比例して配置されなければなりません。すべてのカメラシステムおよびIDSは、最新の業界標準（国際標準化機構（ISO）、システムおよび組織管理（SOC）、一般的な法規制上の要件、現在のメーカーの仕様など）に従って導入、運用および維持される必要があります。 IDSおよびセキュリティカメラの警報を効果的に監視および管理するための手順を定める必要があります。セキュリティシステムへのアクセスは、権限のある担当者に制限されている必要があります。	侵入者検知システムと防犯カメラは、不正アクセスから敷地を保護し、資産のセキュリティを確保するための多段階管理の一部です。これらのシステムが有効に設置・運用・監視・保守されていないと、Barclaysの資産およびデータを含む敷地や建物への不正アクセスのリスクがあり、不正アクセスが適時に発見されない可能性があります。
3.データセンター、ホール、通信設備（TC 5.3）	単独型、共同設置型、およびサードパーティーのデータセンター、クラウドプロバイダー、データホールおよび通信設備（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、Barclaysの資産やデータへの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。すべてのデータセンターでは、データホールその他すべての重要なエリアの境界、構築、および整合性を有効に保護するため、技術的、物理的、人手による管理、および施設固有の手順を多段階で実施する必要があります。管理には、防犯カメラ、侵入者検知システム、入退室管理および警備員などが含まれますが、これらに限定されません。 設置場所が共有されている場合は、個別分離を中心とした効果的なセキュリティを導入する必要があります。	これにより、データセンター、データホール、および同様の重要な場所に保管されているBarclaysの資産またはデータを、制限されたスペースへの不正アクセスによる損失、損傷、または盗難のリスクから保護することができます。

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。