External Supplier Control Obligations

物理的セキュリティー

2021 年 10 月付け第 11.0 版

管理対象	管理内容	本件が重要である理由
1.セキュリティリスク評価	サプライヤーは、物理的セキュリティ管理措置およびプロセスを特定、審査、実施するために、セキュリティリスク評価を確実に実施しなければなりません。評価は、現在構成されている脅威のプロファイルと、サイトに影響を与える可能性のある新たな問題の両方を軽減するため、適切な経験を積んだ者または有資格者によって完了されなければならず、物理的セキュリティ管理の適切性と有効性を考慮しなければなりません。リスク評価活動の頻度は、その場所の目的や重要度に応じたものでなければなりません。Barclays の手順（データセンターなど）の実施に重要なサイトは、少なくとも年に 1 度は評価されることが期待されます。 セキュリティリスク評価の調査結果は文書化し、行動計画を策定しなければならず、特定された問題・リスクについては責任者を割り当て、結論に至るまで追跡するものとします。 重要な発見事項はすべて、発見から 10 営業日以内に Barclays に報告するものとします。	セキュリティリスク評価は、サプライヤーの物理的なセキュリティ環境、管理、プロセス、および現状の有効性を正確に評価するための重要な要件です。これにより、新規または既存の脆弱性や管理のギャップを特定し、Barclays の資産の損失もしくは損害、またはそれに伴う風評被害もしくは規制上の罰金・問責のリスクを軽減することができます。
2.アクセス管理	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、管理されるものとします。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。 システムへのアクセスは権限のある担当者に制限される必要があり、キーとその組み合わせへのアクセスは厳重に管理・制御するものとします。 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ものとします。アクセス認証情報	効果的なアクセス管理は、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に必要な多段階管理の一部です。 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。

	は、サプライヤーのアクセス管理手順に沿って管理するものとします。 アクセス認証情報は、適切な承認を受けた上で発行されるものとします。 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ものとします。 敷地または制限区域へのアクセスの必要がなくなった場合は、通知があってから 24 時間以内にアクセス認証情報を無効化するものとします。 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。	
3.侵入者検知システム・防犯カメラ	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で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、規定の業界標準に従って設置、運用、保守されなければなりません。 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・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。
4.セキュリティ担当者	各場所の物理的なセキュリティ上の脅威に応じ、セキュリティ担当者を配置する必要があります。 すべてのセキュリティ担当者（サプライヤー、家主、外部サプライヤーに雇用されているかどうかに関わらず）は、現地法に基づき、認定された資格を持つサービスプロバイダーを通じて雇用または契約するものとします。セキュリティ担当者は、その役割と責任に見合ったセキュリティトレーニングを受けるものとします。実施されたすべてのト	セキュリティ担当者は、不正アクセスから敷地を保護し、資産の安全性を確保するための多段階管理の一部です。 セキュリティ担当者が現行のセキュリティ上の脅威に沿って配置され、適切なトレーニングを受けていない場合、Barclays の資産およびデータを含む場所への不正アクセスが発生する可能性があります。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。

	レーニングを記録し、すべてのセキュリティ担当者のトレーニング記録を保管するものとします。	
5.セキュリティーインシデント管理および応答レベル	サプライヤーは、セキュリティーインシデントを管理し、必要に応じて調査を実施するための手順を備えている必要があります。Barclays の資産が影響を受けた場合、インシデントは 48 時間以内に Barclays に報告し、現実的に可能な限り速やかに、ただし事件発生から 10 営業日以内に正式な報告と調査の詳細を通知する必要があります。 これには、必要に応じて、現地の法律や規制に沿ったアクセスコントロールデータや防犯カメラの画像が含まれます。	この要件が実施されない場合は、Barclays は、サプライヤーがセキュリティーインシデントを管理するための手順を適切にしっかりと文書化しているとの確証を得ることができない可能性があります。このことは、インシデントの後不適切な措置が取られ、Barclays の資産およびデータの損失または損害および関連する名声の毀損、および/または、法定の罰金または非難のリスクを増大させる原因となる可能性があります。
6.輸送	サプライヤーは、Barclays のすべての資産およびデータが、移送される資産およびデータの価値（財務的損害および風評被害の観点から）およびそれらが移送される脅威環境に見合った適切な管理が行われており、安全に移送されていることを確認するものとします。	これにより、サプライヤーの敷地および/または Barclays の敷地間で移送中の Barclays の資産またはデータを保護し、損失、盗難、損害、およびそれに伴う風評被害および/または規制当局の罰金/問責のリスクを低減することができます。
7.データセンターとデータホール	すべてのスタンドアローン、共同運用、サードパーティのデータセンター、クラウドプロバイダー、データホールは、Barclays の資産およびデータへの不正アクセス、盗難、損害を防ぐために有効にセキュリティ保護されるものとします。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ものとします。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。	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。