External Supplier Control Obligation

情報とサイバーセキュリティ(ICS)

2021 年 10 月付け第 11.0 版

管理エリア/対象	管理内容	本件が重要である理由
1.情報/サイバーセキュリティガバナンス、フレームワーク	サプライヤーは、業界ベストプラクティスユーザーNIST、ISO/IEC 27001、ITIL、COBIT を含む現在の業界最高のプログラム）および適用される業界要件に従って、情報およびサイバーセキュリティガバナンスのための確立された一貫した業界標準フレームワークを持っていなければなりません。これによりサプライヤーは、そのプロセス、技術および物理的環境を保護する手段または対策を持てるようになります。適切に体系化された、全社規模の情報ガバナンスプログラムでは、可用性、完全性および機密性という核となる概念が、情報の損失、中断または破損のリスクを軽減または低減させるように設計された適切な管理によってサポートされていることを確実にしなければならず、サプライヤーは、Barclays のサービスを保護するために、Barclays の要件管理が適切に実施され、効率的に運用されるようにしなければなりません。 セキュリティガバナンスフレームワークは、資産とデータを不正な紛失、悪用、アクセス、開示、改ざん、破壊から保護するための事務的、組織的、技術的、物理的な保護措置を含めて、策定、文書化、承認、実施されなければなりません。 セキュリティプログラムには以下が含まれる必要がありますが、これらに限定されません。 • 情報とサイバーセキュリティの方針および標準の実施の有効性を効果的に策定・実施・継続測定する方針、手続および標準的なプログラム。 • セキュリティに対する説明責任と啓発の文化を育成するために、明確なリーダーシップ構造、上申の仕組み、経営陣の監視機能を備えた包括的なセキュリティプログラム。 • 組織全体で承認・伝達される、方針、手順、およびプロセス。 • 情報およびサイバーセキュリティの方針および手順/基準は、定期的に（年 1 回以上、または重大な変更があった場合）見直すものとし、現在のサイバーセキュリティの慣行および進化し続ける脅威の状況に合わせて適応させるようにします。	この原則が守られない場合は、Barclays またはそのサプライヤーは、情報/サイバーセキュリティを適切に監視していない可能性があり、適切な実施を実証できない場合があります。強固なセキュリティガバナンスフレームワークは、組織全体のセキュリティに対する意識を向上させます。

	• サプライヤーは、重要なビジネス環境、情報、セキュリティーシステムを適切に備え、それを有能な個人に割り当てて、情報とセキュリティシステムに対して社員それぞれが説明責任を負うようにするものとします。 • サプライヤーは、社内外のパートナーと連携し、有効なセキュリティ戦略とフレームワークを実施、管理、監督し、社員の役割と責任を調整・手配するものとします。 • サプライヤーは、組織をあらゆる脅威（サイバーセキュリティを含む）から保護するために、安全なインフラと管理のフレームワークを導入する必要があります。 • 少なくとも年に 1 度、独自に専門家による見直しと評価を行い、確立された方針、基準、手順、およびコンプライアンス義務の不適合に組織が対処できるようにするものとします。 **合併、買収、その他の所有権の変更があった場合には、サプライヤーは、法的に可能な限り速やかに Barclays に書面により通知するものとします。**	
2.サイバーリスク管理	サプライヤーは、サプライヤーが管理する環境全体の進化し続けるセキュリティリスクを効果的に評価、低減、監視するセキュリティリスクマネジメントプログラムを構築するものとします。 リスクマネジメントプログラムには以下が含まれる必要がありますが、これらに限定されません。 • サプライヤーは、適切な運営機関（取締役会またはその委員会など）によって承認されたセキュリティリスクマネジメントのフレームワークを備えている必要があります。これは、事業戦略やリスクマネジメントのフレームワーク全体に採用されている必要があります。 • リスクフレームワークに沿って、正式なリスク評価は、少なくとも年に 1 度、または計画された間隔で実施されるものとし、また、例えば、インシデントまたはそれに関連した教訓など何らかの事案（情報システムの変更に関連して）に対応し、定性的かつ定量的な方法を用いて、特定されたすべてのリスクの発生見込みと影響を判断する必要があります。固有リスクおよび残存リスクに関連する発生見込みおよび影響は、すべてのリス	このような管理が実施されない場合、サプライヤーは、セキュリティリスクを管理するための適切な対策を実施していることを証明できない可能性があります。

	クカテゴリー（監査結果、脅威と脆弱性の分析、規制遵守など）を考慮し、独自に決定するものとします。
	• リスク評価の結果を考慮し、セキュリティリスクに対する適切な対応方法を選択するものとします。
	• セキュリティリスクへの対応計画を策定し、適切な資質を有し、責任のある社員を通じたリスク受容基準を策定するものとします。そのような基準にはこれらのデータの機密性と業務上の重要性が含まれますが、これらに限定されるものではありません。
	• サプライヤーは、リスクに優先順位を付けて防護策を講じることにより、特定の状況下におけるリスクを確実に最小化または排除するものとします。
	• リスクは受容レベルにまで低減するものとします。リスク基準に基づく許容レベルは、解決に合理的に必要な時間および利害関係者の承認に従って構築し、文書化するものとします。
	• データガバナンス要件に関するリスク評価については、以下の点を考慮する必要があります。
	  ○ データを分類し、不正使用、情報漏洩、アクセス、紛失、破壊、変更、改ざんから保護する。
	  ○ アプリケーション、データベース、サーバー、ネットワークインフラストラクチャ間で機密データがどこに保存され、転送されているかを確認する。
	  ○ 定義された保管期間および使用期間経過後の破棄に関する要件を遵守する。
	• サプライヤーは、セキュリティに関連したセキュリティリスク評価を少なくとも年 1 度実施し、状況に応じてより頻繁に実施することを検討するものとします。
	
	サプライヤーは、Barclays のデータおよび/または Barclays に提供するサービスに影響を与える可能性のある重大なリスクを低減または排除できない場合は、その記録を作成し、Barclays に通知するものとします。	

3.役割と責任	サプライヤーは、Barclays へのサービス提供に携わるすべての個人が本文書の Barclays の管理要件を認識し、遵守することを確実にする責任を負います。Barclays の管理要件については、サプライヤーは、Barclays の管理要件を管理するため、ならびに Barclays のサービスを保護するために、適切な専門家チームおよび/または適切なスキルを持ち定義された役割と責任を有する人員が配置され、効果的に運用されるようにしなければなりません。 サプライヤーは、管理要件の対象となるすべてのセキュリティ領域に対する役割と責任を定義し、連絡調整を行わなければならなりません。これらは定期的に（少なくとも 12 か月に 1 回）見直さなければならず、サプライヤーの運営モデルまたは業務に重大な変更があった場合には、その都度見直さなければなりません。主な役割には、情報/サイバーセキュリティに責任を負う上級役員を含むものとします。 サプライヤーの従業員/スタッフが、本基準および関連する方針ならびに基準の管理要件をよく理解し、遵守させるようにするのはサプライヤーの責任となります。サプライヤーは、Barclays と連携して行動するための上申のための窓口担当者を任命するものとします。	役割と責任に関する明確な定義は、情報およびサイバーセキュリティ SCO の実施をサポートします。
4.許可される使用	サプライヤーは、許容される使用要件を作成、公表し、サプライヤーの社員（組織のシステムを利用する請負業者や第三者のユーザーを含む）に自らの責任を通知するものとします。 以下の内容を考慮するものとします： • インターネットの使用 • SaaS（サービスとしてのソフトウェア）の使用 • パブリックコードリポジトリの使用 • ブラウザベースのプラグインとフリーウェア/シェアウェアの使用 • ソーシャルメディアの使用 • 会社 E メールの使用 • インスタントメッセージの使用	許容される使用要件は、情報資産を保護する管理環境をサポートします。

	• サプライヤーにより提供されるIT機器の使用 • サプライヤーにより提供されないIT機器の使用（自分自身の機器の持ち込みなど） • ポータブル/取り外し可能なストレージ機器の使用 • Barclaysの情報資産を取り扱い、保存し、保管する際の責任 • データ漏えい経路のアウトプット、および • 上記項目の誤用および/またはそのような誤用から生じるあらゆる違法で、有害で、または攻撃的な結果のリスクおよび結果。 サプライヤーは、許容できる使用要件に確実に従うための適切な手順を講じるものとします。	
5.教育と意識向上	サプライヤーは、組織のシステムを利用するすべての従業員、請負業者、および第三者のユーザーを対象としたセキュリティ教育および意識向上のためのトレーニングプログラムを構築し、必要に応じて参加を義務付けるものとします。Barclaysのデータ/情報にアクセスできるすべての個人は、会社に関連する専門的能力に関連して、適切な教育および啓発訓練を受け、技術的および組織的な手順、プロセス、および方針についての最新情報を定期的に取得するものとします。教育、トレーニングおよび意識向上のレベルは、参加者の役職に見合ったものでなければならず、適切な学習管理プラットフォームに記録するものとします。 サプライヤーは、その管理下にあるすべての社員に対し、業界ベストプラクティスとBのデータ保護を含む必須のセキュリティ情報トレーニング（進化し続ける脅威と業界固有のリスクに対処するために継続的に更新）を、入社後1カ月以内に実施し、少なくとも年1回は更新しなければなりません。必要であれば以下の内容を含む必要があります。 特権アクセス許可を持つ者や、機密性の高い事業に携わる者などの高リスクグループ（特権ユーザー、上級役員、情報とサイバーセキュリティ担当者、第三者の利害関係者を含む）は、各役割と責任に応じて、情報とサイバーセキュリティの状況別意識向上トレーニングを受けるものとします。適宜このトレーニングは外部の第三者専門家が実施するものとします。	教育と意識向上は、本スケジュール内のその他すべての管理を支援します。 この原則が実施されない場合、関係する社員は、サイバーリスクおよび攻撃ベクトルに関する認識を持たず、攻撃を検知または防止することができなくなります。

6.セキュリティーインシデント管理	サプライヤーは、サプライヤー環境におけるセキュリティインシデントを効果的に検証し、効率的に上申を行って、封じ込め、是正するセキュリティインシデント管理フレームワークを構築するものとします。 サプライヤーは、社員の役割、上申のしくみ、およびインシデント対処/管理のフェーズを定義した、既知のセキュリティリスク/インシデントの各カテゴリーのための、書面によるインシデント対応計画を備えている必要があります。 • インシデントの検証 - さまざまなデータソースを活用し、会社全体で統一されたインシデント検証プロセスを確立し、セキュリティーインシデントを効果的に検証する（これは、サプライヤが IT 環境全体で有効かつ適切な監視および検出メカニズムを備えていることを前提とします）。 • インシデントの分類 - 検証されたインシデントをすべてのイベントの種類に応じて効果的かつ迅速に分類するインシデント分類プロセスを構築する。 • インシデントの上申 - インシデントを（分類に応じて）適切な利害関係者、説明責任のある担当者、または適宜外部の専門家に上申するための適切な仕組みを構築し、迅速なインシデント対応を可能にしておく。 • インシデントの封じ込め - 人、プロセス、およびテクノロジーの能力を活用し、攻撃経路を迅速かつ効果的に特定し、環境内のセキュリティインシデントを封じ込める。 • 是正 - スタッフ、プロセス、テクノロジー機能を活用し、環境から発生するセキュリティ上の脅威や構成要素を迅速かつ効果的に是正する。効果的な是正により、将来、同様の性質の攻撃に対して確実に対処できるようになる。 サプライヤーは、現在および過去の検出・対処実績から得られた教訓を取り入れ、可能な限りインシデント対応措置が改善されるように努めるものとします。 サプライヤーは、サイバーセキュリティーインシデントに対応できるように、インシデント対応チームとプロセスに対し、少なくとも年に 1 度テストを実施するものとします。	インシデント管理および対応プロセスは、インシデントを速やかに解決し、エスカレートすることを防止するためのものです。

	• シミュレーションおよび試験では、Barclays がセキュリティインシデントの影響について通知を受けることを実証しなければならず、こうした実証は、そのようなインシデントの場合に適切な担当者に連絡する能力があることをサプライヤーが証明することによって行う必要があります。 • 連絡手段 - サプライヤーは、セキュリティ上の問題が発生した場合に、Barclays と連携して行動するための窓口担当者を任命するものとします。サプライヤーは、時間外の連絡先、電話番号などを含め、窓口担当者の連絡先詳細に変更があった場合は Barclays に通知するものとします。 **連絡先詳細には、名前、会社内での責任、役割、メールアドレス、電話番号を含めるものとします。** サプライヤーは（また、該当する場合には、その下請業者のいずれかが）、Barclays へのサービスもしくは Barclays の情報/データへのサービスに影響を与えるか、または影響を与える可能性があると疑われるインシデントに気付いた場合、合理的な期間内に、またいかなる場合でも、サプライヤーがセキュリティインシデントに気付いた時点から**2 時間**以内に、Barclays に通知するものとします。 データ侵害の疑いがある、またはデータ侵害が判明している場合（偶発的または違法な破壊、損失、改変、権限のない開示、または個人データへのアクセスにつながるセキュリティ違反を含む）、サプライヤーは、そのようなインシデントに気付いた時点から合理的な期間内に、またいかなる場合もサプライヤーがそのようなインシデントに気付いた時点から**2 時間**以内に、Barclays に通知するものとします。 上記のような初期の通知に加えて、サプライヤーは、Barclays へのサービスもしくは Barclays の情報/データに影響を与えるインシデントに気付いてから**24 時間**以内に、Barclays に報告書を提出するものとします。報告書には以下を含めるものとします： • サプライヤーがセキュリティ・インシデントに気付いた日時	

	• 影響を受けたと思われる管轄区域 • セキュリティインシデントの種類と簡単な概要 • Barclays へのサービスおよび/または Barclays の情報/データ（該当する場合、影響を受けるデータ主体）に対する影響ならびに予想される影響 • セキュリティインシデントの状況（例えば、法医学の専門家が立ち入ったか、関係当局に通知されたか、攻撃経路がわかっているか、監視が強化されているか、封じ込めが行われているか等） • セキュリティインシデントに対する是正のために取られた、または計画された措置 • 侵害されたデータの詳細 これらのインシデントは、是正措置およびデータ対象者への通知に関するすべての最新情報と同様に、Barclays サプライヤーマネージャーおよび**Barclays チーフセキュリティオフィス（CSO）ジョイントオペレーションセンター（JOC）内の Barclays ジョイントオペレーションセンター（gcsojoc@barclays.com）に報告するものとします。** **メールの件名は「[サプライヤー名を挿入]–セキュリティインシデント–緊急の対応が必要」にしてください。インシデントが非常に緊急で、至急対応する必要がある場合は、24 時間年中無休のホットラインで JOC に連絡できます。** • イギリス： +44 330 041 5586 • アメリカ：+1 201 499 1900 • インド：+91 788 781 9890	
7.情報分類と保護	サプライヤーは、以下の構成要素を対象とするがこれらに限定されない、確立された適切な情報分類、取扱いおよび保管のフレームワーク/スキーム（業界ベストプラクティスおよび/または Barclays 要件に従う）を備えている必要があります。 • 既存および新規の Barclays の情報/データを継続的に見直し	このような要件が実施されなければ、Barclays のデータが、許可のない改変、開示、アクセス、損傷、遺失、破壊に対して脆弱となる結果をもたらし、

	• Barclays の情報/データの、正しい情報ラベルスキーマへの割り当て。 • 割り当てられた分類レベルに従った、Barclays の情報/データの安全かつ適切な取り扱いおよび保管。 • すべてのスタッフが、サプライヤー/Barclays のラベリング、保管、および取り扱い要件、および正確な情報分類を適用する方法を認識していることを確認する。 サプライヤーは、Barclays の情報ラベリングスキームおよび取り扱い要件（付録 B、表 B1 および B2）またはその代わりとなるスキームを参照し、保持および/または処理された Barclays 情報を保護および安全に管理するものとします。この要件は、Barclays に代わって保有または処理されるすべての情報資産に適用されます。	その結果、規制上および評判上の損害が発生する可能性があります。
8.IT 資産マネジメント（ハードウェアおよびソフトウェア）	サプライヤーは、資産のライフサイクルを通して効果的な資産管理プログラムを構築するものとします。資産管理は、取得から使用終了までの資産のライフサイクルを管理し、環境における全レベルの資産に対し、可視性と安全性を提供するものとします。 サプライヤーは、Barclays にサービスを提供するすべての拠点および/または地理的な場所にあるビジネス上重要な資産（サプライヤーの敷地内に設置された Barclays の機器、および/または Barclays が提供する下請け業者を含む）の完全かつ正確な目録を維持し、資産目録が最新、完全かつ正確であることを検証するため、少なくとも年に 1 回のテストを必ず実施するものとします。 資産管理プロセスは最低限、以下の条件を満たす必要があります。 • すべての情報資産およびインフラ、継続的にマッピング/更新されます。 • 情報資産とインフラはその後、分類、重要度、事業運営上の価値に基づいて保護されます。 • サプライヤーは、資産のライフサイクルを通してハードウェアの資産データの記録および継続的な保守を保証するための管理を実施するものとします。	情報資産の完全かつ正確な在庫目録は、適切な管理を徹底するために不可欠です。 この原則が実施されない場合、Barclays の資産または Barclays へのサービス提供のためにサプライヤーが使用する資産が損なわれる場合があり、これにより財務上の損失、データの損失、風評被害、規制上の非難が発生する場合があります。

	• サプライヤーは最新の資産目録を保管するものとします。 • **一次請け、二次請け、および三次請けの構造を持つサプライヤーは、最新で完全かつ正確な資産目録（すべてのエンドポイント、ネットワーク機器、RSA トークン、および／または Barclays が提供する資産を含む）を保管する必要があります。** • **サプライヤーは、Barclays のすべての資産（ハードウェアおよびソフトウェア）の照合を毎年実施し、Barclays（最高セキュリティオフィスの ECAM チーム）に証明書を提出するものとします。** • 承認されていない資産がネットワークから削除されるかまたは隔離され、かつ目録が適時に更新されることを確認する。 • Barclays のサービス提供に必要な、すべての認可されたソフトウェアの最新リストを保管する。 • 現在サポートされているソフトウェアアプリケーションまたはオペレーティングシステムのみがサポートされていること、およびベンダーのアップデートを受領することが会社の正規ソフトウェア目録に追加されることを確認する。サポートされていないソフトウェアについては、目録システム内でサポートされていない旨を表示するものとします。寿命が近づいているソフトウェアにも、目録管理システムでその旨の印を付けるものとします。 サプライヤーは、データ漏洩のリスクを排除するため、サポートされていない技術の低減、ならびに資産およびデータの使用期間満了、使用終了、および破棄のための効果的かつ効率的な手順を確実に適時に実施するものとします。	
9.物理的資産の廃棄・破壊と電子情報のデータ残存	物理的または電子的な形式で保存された Barclays の情報資産の破壊または消去は、Barclays のデータが確実に復元不可能となるよう、関連するリスクに適した安全な方法で実施される必要があります。 サプライヤーは、物理的または電子的形式のいずれかで保存された Barclays の情報資産の破棄または削除が、契約に従い、または情報セキュリティのために、法律上または規制上の目的で	情報資産を確実に破壊することにより、Barclays の情報資産にデータ違反、データ紛失または悪意ある活動が発生した場合に復元不能であることが保証されます。

	いつ適切かつ必要とされるかを継続的に評価し判断するために、有効な方針および手続きを定める必要があります。Barclays は、書面による請求により、Barclays の情報資産の破棄を求めることもできるものとします。 サプライヤーは、コンピュータによる科学的な手段でデータを復元できないよう、すべての記憶媒体から Barclays データ（バックアップ用のコピーを含む）を安全に廃棄し安全に除去/消去するため、事業プロセスと技術的手段を含む手順を構築するものとします。 Barclaysの媒体に格納されたデータは、データが復元できないようにするのに十分なレベルまで消去しなければなりません。可能であれば、セキュアワイプ、パージング、データ消去、データ破壊などの適切なデータ消去技術を使用するか、データを上書きするソフトウェアに基づいた方法、またはデータ廃棄に関する業界標準フレームワーク(NIST)を使用します。装置はすべて稼働寿命の終了時（故障や何らかの処理のために廃止された、廃棄された、または不要になった、試験または概念証明で使用されたなど）に破棄する必要があります。データ消去の処理は、再利用する機器に活用できます。 廃棄要件は、Barclays にサービスを提供するために使用されるサプライヤーの第 4 者/下請けの代理店に対しても適用されます。 ハードコピー情報の廃棄の際は、クロスカットシュレッダー（支払いカード情報を含む）を使用して少なくともP4 DIN 66399の基準までシュレッダーで破断処理するか、またはBS EN 15713:2009に準拠して焼却する必要があります。 Barclays に関しては、データの廃棄に関する証拠を保持し、監査記録、証拠、追跡を提供し、以下を含まなければなりません。 • 破壊および/または廃棄の証明（実施日および方法を含む） • 削除に関するシステム監査記録。 • データ廃棄証明。 • 廃棄を実行した担当者（廃棄の際の共同作業者、第三者、請負業者を含む）。	

	• 破壊および検証報告書を作成して、破壊/削除プロセスが成功したか失敗したかを確かめる必要があります（例えば、上書きプロセスでは、消去できなかった部分を詳細に報告する必要があります）。 サプライヤーは、業務終了時に、Barclays からの通知と承認に基づき、Barclays のデータが安全に破棄されるようにしなければなりません。	
10.境界とネットワークセキュリティ	サプライヤーは、B のサービスをサポートするサプライヤーまたはその請負業者が運用するすべての IT システムが、サプライヤー（および関連するすべての請負業者）のネットワークを経由する脅威から保護されるようにしなければなりません。サプライヤーは、セキュリティに悪影響を及ぼすデータに焦点を当て、信用レベルの異なるネットワークを介して転送される情報の流れを監視、検出、予防し、必要に応じて修正するものとします。 ネットワーク整合性メカニズムには以下が含まれる必要がありますが、これらに限定されません。 • 組織のネットワーク境界のすべての最新の目録を保管する（ネットワークアーキテクチャ/ダイアグラムを介して）。 • ネットワークの設計および実施、潜在的な脆弱性、ネットワークインフラの廃棄と更新の必要性については、少なくとも年 1 回、または変更の原因となるイベントが原因で生じた要件がある場合は、見直す必要があります。 • セキュリティの侵害を防止するため、サプライヤーネットワークへの外部接続を記録し、ファイアウォールを経由して、接続が確立される前に検証、承認される必要があります。 • サプライヤーネットワークが、徹底した防御の原則（ネットワーク分割、ファイアウォール、ネットワーク機器への物理的なアクセス制御など）を適用することで保護される。 • サプライヤーは、悪意のあるトラフィックがネットワークに侵入した場合それを検知、防止するためのネットワーク侵入防止技術を有している必要があります。 • 悪意のあるネットワーク攻撃に対処できる、境界防御層を提供する強力なネットワークファイアウォール機能を使用する。	この原則が履行されない場合、外部または内部ネットワークは、その内部サービスまたはデータにアクセスしようとする攻撃者により、弱体化されるおそれがあります。

	• インターネットのネットワークトラフィックは、不正な接続をフィルタリングするように設定されたプロキシを経由する。 • ロギングと監視が確実に有効化されている必要があります。 • ネットワーク機器は、悪意のある攻撃を防ぐために安全性が強化されている。 • デバイス管理ポート/インターフェースをユーザー・トラフィックから論理的に分離し、適切な認証制御が行われている。 • ネットワークデバイスを介した通信データの流れを許可する設定ルールはすべて、設定管理システムに登録し、ルールごとに具体的な業務上の理由を記載する。 • 不正な TCP または UDP ポートまたはアプリケーション トラフィックを介した通信を拒否し、認証されたプロトコルのみが、組織の各ネットワーク境界を越えて出入りを許可されていることを確認する。 • 信頼できる各ネットワーク境界の外部から定期的にスキャンを実施し、境界を越えてアクセスしている不正な接続を検出する。 • デバイスと管理ステーション/コンソール間の通信を確保する。 • 組織のネットワークのそれぞれの境界を通過するネットワークパケットを記録するための監視システムを設定する。 • オフィス間/クラウドサービスプロバイダー間/データセンター間のネットワーク接続を安全なプロトコルで暗号化する。サプライヤーの広域通信網（WAN）内で転送される Barclays の情報資産／データを暗号化する。 • サプライヤーは、ファイアウォール（外部ファイアウォールと内部ファイアウォール）のルールを年に 1 度見直す。 • ネットワークへのすべての無線アクセスは、セキュリティ侵害を防ぐために、承認、認証、分離、暗号化プロトコルの下に置かれるものとします。 • サプライヤーは、社内ネットワークへのアクセスが監視され、許可されている機器のみが適切なネットワークアクセス管理を通じて許可されることを確認するものとします。	

	• サプライヤーネットワークへのリモートログインアクセスの際は、多要素認証を使用する必要があります。 • サプライヤーは Barclays のサービスのためのものとは別のネットワークを持っていなければなりません。 サプライヤーは、Barclays にサービスを提供するために使用するサーバーが適切なセキュリティ管理のない、信頼できないネットワーク（インターネットに接続する場合など、ネットワークがセキュリティ境界の外にあり、事務的管理の範囲を越えるもの）に接続されないことを確認する必要があります。 データセンターまたはクラウドで Barclays の情報を運用しているサプライヤー（下請業者を含む）は、セキュリティ管理のための有効な ISO/IEC27001 および/または SOC1 または 2 認証（または同等の管理が行われていることを示す認証であり、独立監査人の報告により保証されているもの）を保有するものとします。 T2 および T3 ネットワーク - • T2 ネットワークは、ファイアウォールによってサプライヤ企業ネットワークから論理的に分離され、すべてのインバウンドおよびアウトバウンドトラフィックが制限・監視される必要があります。 • ルーティング設定は、Barclays ネットワークへの接続を確保する必要があり、他のサプライヤーネットワークにルーティングしてはなりません • Barclays エクストラネット・ゲートウェイに接続するサプライヤーのエッジルーターは、ポート、プロトコル、およびサービスの制御を制限するという構想のもとで安全に設定されていなければなりません。 　o ロギングと監視が確実に有効化されている必要があります。 *注記：この管理において使用される「ネットワーク」という用語は、サプライヤーの下請業者のネットワークを含む、サプライヤーが責任を負う Barclays 外のネットワークを指します。*	

11.サービス拒否の検知	サプライヤーは、サービス妨害（DoS）攻撃および分散サービス妨害（DDoS）攻撃を検知し、防衛する能力を備えているものとします。 サプライヤーは接続されているインターネット、または Barclays に提供されるサービスをサポートする外部チャンネルに、可用基準を保証するための十分な DoS 攻撃への保護策を設けるものとします。 サプライヤーがインターネット向けのアプリケーションを運用しており、制限付きのデータを保持している場合、または回復力カテゴリ 0 もしくは 1 のサービスをサポートしている場合、Barclays が承認しなければならない適切な技術を使用して、これを階層 7 まで保護する必要があります。	この原則が実施されない場合、Barclays とサプライヤーは、サービス拒否攻撃がその目的を達成することを阻止できない場合があります。
12.在宅勤務（リモートアクセス）	サプライヤーが管理する環境/ネットワーク内に存在している/格納されている Barclays Citrix アプリケーションおよび/または Barclays データを介した Barclays ネットワークへのリモートアクセスについて、サプライヤーまたはそのいずれかの下請業者が、Barclays のデータもしくは Barclays の個人データ、またはサプライヤーに知る必要があることを前提に供給者に提供された機密情報に、物理的な形式であるか仮想的な形式であるかを問わず、リモートでアクセス、共有、または処理される必要がある場合、特にそのスタッフが在宅勤務をしている場合、サプライヤーは、これらの手配について Barclays（最高セキュリティオフィス–ECAM チーム）の事前承認を求めるものとします。 サプライヤーは、リモートアクセスのために最低限、以下の対策が実施されていることを確認するものとします。 • サプライヤーネットワークへのリモートログインアクセスは、転送中のデータを暗号化し、多要素認証を使用する必要があります。 • Barclays ネットワークへのアクセスは、Barclays が提供する RSA トークン（ハードおよびソフト）を使用して、Barclays Citrix アプリケーションを介して行う必要があります。	リモートアクセスを管理することで、不正で安全でないデバイスが Barclays の環境にリモートで接続されていないことを確認することができます。

	• サプライヤーは、Barclays が提供するすべての RSA トークン（ハードおよびソフト）の目録、およびトークン（ハードトークン）の割り当て・使用・応答の確認および監視を含む管理プロセスを維持するものとします。 • サプライヤーは、リモートワークを依頼された個人の記録とその理由を保持するものとします。 • **サプライヤーは、すべてのリモートユーザーの照合を四半期ベースで実施し、Barclays（最高セキュリティオフィスの ECAM チーム）に証明書を提供するものとします。** • Barclays は、認証情報が一定期間使用されていない場合（使用されていない期間は 1 ヶ月を超えないもの）、直ちに認証情報を無効化します。 • サプライヤーは、Barclays の情報システムをリモートで接続するために使用されるエンドポイントが安全に、かつベストプラクティス（パッチレベル、マルウェア対策のステータス、エンドポイント検出および応答 EDR ソリューション、記録など）に従って設定されていることを確認する必要があります。 • Barclays の Citrix アプリケーションを介してリモート印刷にアクセスが可能なサービスは、Barclays（最高セキュリティオフィスの ECAM チーム）の承認と認証を受けている必要があります。サプライヤーは記録を保管し、四半期に 1 度調整を行うものとします。 • **個人所有のデバイス（BYOD）による、サプライヤが管理する環境（サプライヤのスタッフ、コンサルタント、臨時スタッフ、請負業者、マネージドサービス・パートナーなどを含むがこれらに限定されない）内に存在している/格納されている Barclays の環境および/または Barclays のデータへのアクセスを許可してはなりません。** エンドポイント（ノート PC/デスクトップ PC）のアクセス許可が Barclays の Citrix アプリケーション経由でインターネットを介して Barclays のネットワークに付与される場合、サプライヤーは、エンドポイントのセキュリティーおよびオペレーティングシステムの適合性を検証するため、Barclays が提供するエンドポイント分析 (EPA) ツールをインストールするものとし、エンドポイント分析の検査に合格した機器のみが Barclays の Citrix アプリケーション経由で Barclays のネットワークへのリモートアク	

<table>
<tr><td></td><td>セスを許可されます。サプライヤーが EPA ツールをインストールまたは使用できない場合は、Barclays のサプライヤーマネージャーに連絡する必要があります。

注意：Barclays は、アクセスが不要になった旨の通知（従業員の雇用終了、プロジェクトの再配置など）を受けた場合、24 時間以内に認証情報を無効化します。</td><td></td></tr>
<tr><td>13.セキュリティログの管理</td><td>サプライヤーは、アプリケーション、ネットワーク機器、データベース、エンドポイント、セキュリティー機器、インフラ、ならびにサーバーを含む主要な IT システムおよびプロセスが、ベストプラクティスおよびガイダンスに従って、必要なログを生成していることを確認する、確立された監査およびログ管理フレームワークを備えていることを確実にする必要があります。そのような記録は、サプライヤーが適切にかつ一元的な方法で保管し、少なくとも 12 か月間、または下記のカテゴリーに基づいて適正かつ合理的に保管するものとします。

<table>
<tr><th>分類</th><th>影響の少ないシステム/サービス</th><th>影響が中程度のシステム/サービス</th><th>影響の大きいシステム/サービス</th></tr>
<tr><td>ログの保管</td><td>3 ヶ月</td><td>6 ヶ月</td><td>12 ヶ月</td></tr>
</table>

セキュリティログ管理プロセスは最低限、以下の条件を満たす必要があります。

• サプライヤーは、ログ管理の方針と手順を確立するものとします。
• サプライヤーは、ログ管理インフラストラクチャを構築し、保持するものとします。
• サプライヤーは、ログ管理に携わる個人およびチームの役割と責任を定義するものとします。
• 攻撃の監視、検出、把握、復旧のため、イベントの監査ログを収集、管理、分析する。
• システムログにイベント発生源、日付、ユーザー、タイムスタンプ、送信元アドレス、宛先アドレス、その他の有効な要素などの詳細情報を含めることを可能にする。
• イベントログの例は以下の通りです。</td><td>この管理が実施されない場合、サプライヤーは、サービスやデータの不正使用や悪意のある使用を合理的な期間内に検出し、対応することができなくなります。</td></tr>
</table>

	○ IDS/IPS、ルータ、ファイアウォール、ウェブプロキシ、リモートアクセスソフトウェア（VPN）、認証サーバー、アプリケーション、データベースログ ○ 成功したログイン、失敗したログイン（間違ったユーザーID やパスワードなど）、ユーザーアカウントの作成、変更、削除 ○ 設定変更のログ。 • 適切な業界ベストプラクティスのログを有効にする必要があるビジネスアプリケーションおよび技術的なインフラストラクチャシステムに関連する Barclays のサービス（外部委託されているものやクラウドにあるものを含む） • セキュリティ関連のイベントログの分析（正規化、集計、相関関係を含む） • イベントログのタイムスタンプを共通の信頼できるソースに同期する • セキュリティ関連のイベントログの保護（暗号化、MFA、アクセス制御、バックアップなどによる）。 • 特定された問題を修正し、サイバーセキュリティーインシデントに迅速かつ効果的に対応するために必要な措置を取る。 • ログの相関や分析のための SIEM（「セキュリティ情報とイベント管理」）やログ分析ツールの導入。 • 内部および外部ソースを含む複数のソースからの異常活動、ネットワークおよびシステムアラート、関連イベントおよびサイバー脅威インテリジェンスのリアルタイムの一元的集計および相関を実行するためのツールを必要に応じて導入し、多面的なサイバー攻撃をより的確に検出、防止する。 記録される主要イベントとは、Barclays へのサービスの守秘性、完全性および可用性に影響を与える可能性があるイベント、および、サプライヤーのシステムに関連して発生する重大なインシデント、および/またはアクセス権違反の特定または調査に役に立つイベントを意味します。	

14.マルウェア対策	業界ベストプラクティスに従ってサプライヤーは、マルウェアが実行されるのを IT 環境全体で防ぐために、方針と手順を構築し、業務プロセスと技術的な対策を実施する必要があります。 サプライヤーは、サービスの中断やセキュリティ侵害を防ぐために、適用されるすべての IT 資産にマルウェア対策が常に適用されていることを確認するものとします。 マルウェア対策は、以下を有する、または含むものとしますがこれらに限定されません。 • マルウェア対策ソフトウェアを集中管理し、会社の IT 環境を継続的に監視し、防御する。 • 組織のマルウェア対策ソフトウェアにより、業界ベストプラクティスに従って、定期的にスキャンエンジンとシグネチャデータベースが更新されていることを確認する。 • すべてのマルウェア検出イベントを企業のマルウェア対策管理ツールおよびイベントログサーバーに送信し、分析と警告を行う。 • サプライヤーは、モバイルマルウェア対策および、Barclays またはサプライヤーのネットワークに接続して Barclays のデータにアクセスしようとしているモバイルデバイスに対する攻撃を防止するための適切な管理を実施するものとします。 • 潜在的な脆弱性や必要なアップデートについて必要な議論を行うためのプロセスが、定期的な会議やフォーラム（月単位など）といった形で用意されている必要があります。是正のための措置は、優先順位をつけて、適時に実施されるものとします。実施された報告、フォーラムおよび是正措置の記録は保管するものとします。 注意マルウェア対策には、不正なモバイルコード、ウイルス、スパイウェア、キーロガーソフトウェア、ボットネット、ワーム、トロイの木馬など（ただしこれらに限定されない）の検出を含める必要があります。	アンチマルウェアソリューションは、Barclays の情報資産を悪意のあるコードから保護するために不可欠です。
15.セキュア設定標準	サプライヤーは、確立されたフレームワークを備え、すべての構成可能なシステム/ネットワーク機器が、業界慣習（NIST、SANS、CIS など）に従って安全に構成されていなければなりません。	標準ビルド管理は、情報資産を不正アクセスから守る上で役立ちます。

	構成標準プロセスは、以下をカバーする必要がありますが、これらに限定されるものではありません。 • 認定されたすべてのネットワーク機器、オペレーティングシステム、アプリケーション、およびサーバについて、ベストプラクティスのセキュリティ設定標準を実施できるよう、方針、手順、社内対策、およびツールを確立する。 • ベースラインのセキュリティ基準への違反が速やかに是正されるよう、定期的に（年に 1 度）チェックを実施する。適切なチェックおよび監視を行い、ビルド/デバイスの完全性が維持されていることを確認する。 • システムおよびネットワーク機器が、セキュリティ原則（ポート、プロトコルおよびサービスの制御を制限する、不正なソフトウェアを使用しない、不必要なユーザーアカウントを削除および無効にする、デフォルトのアカウントパスワードを変更する、不要なソフトウェアを削除するなどの概念) に従って機能するように構成されている 。 構成管理が、すべての資産クラスにわたって安全な構成基準を管理し、構成の変更や逸脱を検出し、警告し、効果的に対応することを確認する。	変更の許可を徹底する標準ビルドおよび管理への準拠は、Barclays の情報資産の保護を確実にする上で役立ちます。
16.エンドポイントセキュリティ	サプライヤーは、Barclays のネットワークへのアクセス、または Barclays の情報資産/データへのアクセス/処理に使用されるエンドポイントには、あらゆる悪意ある攻撃に対する強固な防御策を設けられていることを確認するものとします。 業界ベストプラクティスが実施される必要があり、エンドポイントのセキュリティビルドには以下が必要ですが、これらに限定されるものではありません。 • ディスクの暗号化。 • 不要なソフトウェア/サービス/ポートをすべて無効にする。 • ローカルユーザーの管理者権限アクセスを無効にする。	この管理が実施されない場合、Barclays とサプライヤーのネットワークとエンドポイントはサイバー攻撃に対して脆弱となる場合があります。

	• サプライヤーの社員がデフォルトのサービスパック、システムパーティション、デフォルトサービスなどの基本設定を変更することは許可されません。 • Barclays のデータを外部メディアにコピーできないようにするため、USB ポートを無効にする必要があります。 • 最新のアンチウイルスシグネチャとセキュリティパッチにで更新を実施する。 • 切り取り、コピー & ペーストをしない、スクリーンショットを撮らないことにより情報漏えい対策を行う。 • デフォルトでは、プリンターへのアクセスを無効にする • サプライヤーは、google ドライブ、Dropbox、iCloud など、インターネット上で情報を保存する機能を持つソーシャルネットワークサイト、ウェブメールサービス、およびウェブサイトにアクセスできる権限を制限するものとします。 • Barclays の情報資産/データの共有/転送は、インスタントメッセージツール/ソフトウェアを使用して無効にする。 • 悪意があると識別された不正なソフトウェアを検出し、不正なソフトウェアのインストールを防止する機能とプロセス。 注意リムーバブルメディア/ポータブルデバイスはデフォルトで無効にし、業務上必要な理由がある場合のみ有効にするものとします。 サプライヤーは、組織が承認した構成基準に基づいて、企業内のすべてのシステムの画像またはテンプレートのセキュリティを管理するものとします。新しく導入されたシステムや既存のシステムが危険にさらされた場合は、それらの画像またはテンプレートのいずれかを使用して画像化するものとします。 エンドポイント（ノート PC/デスクトップ PC）のアクセス許可が Barclays の Citrix アプリケーション経由でインターネットを介して Barclays のネットワークに付与される場合、サプライヤーは、エンドポイントのセキュリティーおよびオペレーティングシステムの適合性を検証するため、Barclays が提供するエンドポイント分析 (EPA) ツールをインストールするものとし、エンドポイント分析の検査に合格し	

	た機器のみが Barclays の Citrix アプリケーション経由で Barclays のネットワークへのリモートアクセスを許可されます。サプライヤーが EPA ツールをインストールまたは使用できない場合は、Barclays のサプライヤーマネージャーに連絡する必要があります。 Mobile devices used for Barclays Services - 1. サプライヤーは、ライフサイクル全体を通じて、Barclays の機密情報にアクセスし、機密情報を取り扱うモバイルデバイスを安全に管理・運用するためのモバイルデバイス管理（MDM）を活用し、データ漏えいのリスクを軽減するものとします。 2. サプライヤーは、モバイルデバイスにリモートロックやリモート消去の機能が搭載されていることを確認し、デバイスの紛失や盗難にあったり、危険にさらされたりした場合に情報を保護するものとします。 3. モバイルデバイスのデータを暗号化する（Barclays のデータ）。	

17.データ漏えい防止	サプライヤーは、以下のデータ漏えいルート（ただしこれらに限定されない）を含む不適切なデータ漏えいの防止を確実にするためのフレームワークを確立するものとします。
	• 内部ネットワーク/サプライヤーネットワークを越えた、外部への情報の不正な転送
	  ○ E メール
	  ○ インターネット/ウェブゲートウェイ（オンラインストレージ、ウェブメールを含む）
	  ○ DNS
	• ポータブル電子メディア（ノート PC 上の電子情報、モバイルデバイス、ポータブルメディアを含む）上の Barclays 情報資産の損失または盗難。
	• ポータブルメディアへの情報の無許可での転送。
	• 第三者（第四者または下請業者）との安全でない情報交換。
	• 情報の不適切な印刷または複写。
		Barclays の情報が、アクセスを許可された人員のみに制限されること（守秘）、許可のない変更が防止されること（完全性）、必要な際に取得され、提示されること（可用性）を確実にするために、適切な管理が効果的に運用されることが必須です。
		このような要件が実施されない場合、Barclays の機密情報が、許可のない改変、開示、アクセス、損傷、紛失、破壊の危険にさらされる可能性があ

18.データセキュリティ	サプライヤーは、Barclays の情報資産/データが、暗号化、データへのアクセスのための安全な手段、完全性の保護、データ損失防止技術を組み合わせることにより、サプライヤーの保管場所またはネットワーク上に保管されているデータが適切にセキュリティ確保されていることを確認するものとします。個人データを含む Barclays の情報資産/データへのアクセスを制限し、そのアクセスを安全なものにするために、適切に配慮することが重要です。 データセキュリティプロトコルでは以下がカバーされる必要がありますが、これらに限定されません。 1. サプライヤーには、適用されるすべてのデータ保護法を常に遵守する義務があります。 2. サービスにおいて地理的に分散している（物理的および仮想的な）アプリケーションおよびインフラストラクチャのネットワークおよびシステムコンポーネント内に（恒久的または一時的に）保存されているデータ、および/または第三者と共有されているデータの目録作成、文書化、およびデータフローを維持するために、方針と手順を定め、それを裏付ける業務プロセス/全社的措置と技術的施策を実施する。 3. サプライヤーが保存、処理、または送信したすべての機密/極秘情報（Barclays の情報資産/データ）の目録を保持する。 4. 機密/極秘情報（Barclays の情報資産/データ）が適切に分類され、保護されていることを確実にするために、データ分類基準を確立する。 5. すべての Barclays のデータが、情報の分類および保護の基準に基づいて分類され、識別表示されていることを確認する。 6. 休止中データの保護 a. 不正アクセスによる機密情報の悪用を防ぐため最低限、保存データを暗号化する。 7. データベース活動の監視 a. データベースへのアクセスと活動を監視および記録し、悪意のある活動を迅速かつ効果的に特定する。 8. 使用中データの保護	り、法的・規制上の制裁、風評被害、または、事業の損失/混乱を招く場合があります。

	a. 機密情報の閲覧および使用がアクセス管理機能によって管理され、機密情報が悪用されないよう保護されていることを確認する。 b. データマスキングおよび難読化技術を使用して、使用中の機密データを不注意による開示や悪意のある悪用から効果的に保護する。 9. 転送中データの保護 a. 強力な暗号化機能を使用して、転送中のデータを確実に保護する。 b. 転送中データの暗号化は、通常、Transport または Payload（メッセージまたは選択フィールド）の暗号化を使用して行われます。Transport の暗号化メカニズムには、以下が含まれますが、これらに限定されません。 • トランスポート層セキュリティ(TLS)（プロトコルと暗号の使用/不使用など、最新の暗号化に関する業界ベストプラクティスに従う） • セキュア・トンネリング (IPsec) • セキュアシェル (SSH) c. トランスポート・セキュリティプロトコルは、アルゴリズムとキー長の両方のエンドポイントが強力なオプションをサポートしている場合、より弱いアルゴリズムや、より短いキー長による干渉を防ぐよう構成されている必要があります。 10. データバックアップ – a. Barclays と合意した要件に準拠し情報が十分にバックアップされ復元可能である（また、合理的な時間内に復元できる）ことを保証するための規定を設ける。 b. バックアップが、保存時、およびネットワークへの移動時、物理的なセキュリティまたは暗号化によって適切に保護されていることを確認する。これにはリモートバックアップ、クラウドサービスが含まれます。 c. すべての Barclays のデータが定期的に自動バックアップされていることを確認する。	

19.アプリケーションソフトウェアのセキュリティ	サプライヤーは、安全なコーディング慣行を使用し、安全な環境においてアプリケーションを開発するものとします。 Barclays が使用する、または Barclays へのサービスをサポートするために使用されるアプリケーションをサプライヤーが開発する場合、開発プロセスにおいてセキュリティ侵害を防止し、コードの脆弱性を特定して改善するための、セキュア開発のフレームワークを確立するものとします。 アプリケーションソフトウェアセキュリティは、以下をカバーする必要がありますが、これらに限定されるものではありません。	アプリケーション開発を保護するための制御により、アプリケーションの展開中にセキュリティを確保することができます。

	• セキュリティー脆弱性およびサービスの中断を防止するとともに、既知の脆弱性を防御するため、業界ベストプラクティスに従い、セキュアコーディング標準が適用され、採用されていることを確認する。 • プログラミング言語に適した安全なコーディング手法を確立する。 • 開発はすべて非本番環境で行う。 • 本番システムと非本番システムには個別の環境を用意する。開発者が、監視されていない状態で本番環境にアクセスできないようにする。 • 本番環境と非本番環境での業務範囲を分離する。 • システムがセキュア開発のための業界ベストプラクティス（OWASP など）に沿って開発されている。 • コードは安全に保管され、品質保証の対象となる。 • テストが終了し、本番環境に移行した後は、コードを不正な変更から適切に保護する。 • サプライヤーが開発したソフトウェアには、信頼できる最新のサードパーティ製部品のみを使用する。 • 静的および動的解析ツールを使用して、安全なコーディング手法に従っているかどうかを検証する。 • サプライヤーは、実データ（個人データを含む）が非本番環境で使用されないことを確認するものとします。 • アプリケーションとプログラミングインタフェース（API）は、業界ベストプラクティス（例：ウェブアプリケーションのための OWASP）に従って設計、開発、導入、テストするものとします。 サプライヤーは、ウェブアプリケーション上のすべてのトラフィックを点検する最新かつ共通のウェブアプリケーションファイアウォール（WAF）を導入することによって、ウェブアプリケーションを保護するものとします。ウェブベースではないアプリケーションの場合、特定のアプリケーションタイプでそのようなツールを使用できる場合は、特定のアプリケーションファイアウォールを導入するものとします。トラフィックが暗号化されている場合、デバイスも暗号化されているか、分析前にトラフィックを復号化で	

	きるようになっている必要があります。いずれのオプションも適切でない場合は、ホストベースのウェブアプリケーションファイアウォールを導入するものとします。	
20.ローカルアクセスマネジメント（LAM）	情報へのアクセスは制限され、知る必要、最低限の特権、職務分離の原則を慎重に考慮するものとします。情報資産所有者は、誰が、どのようなアクセスを持つかの決定に責任を持ちます。 • 知る必要の原則とは、社員は自らの許可されている職務を遂行するために知る必要のある情報にのみアクセスできることです。 例えば、社員が英国を本拠にした顧客のみを取り扱うのであれば、米国を本拠とする顧客に関係する情報を「知る必要」はありません。 • 最小限の権限原則とは、社員は自らの許可されている職務を遂行するために知る必要のある最低レベルの特権のみを持つことです。 例えば、社員が顧客の住所を見る必要があるものの、それを変更する必要がない場合、必要とする「最小限の権限」は読み取り/書き込みアクセスではなく、読み取りのみのアクセスを与えられるべきです。 • 職務の分離原則とは、エラーと詐欺を防ぐために、どのような職務においても、少なくとも 2 名の個人が別々の部分に責任を負うことです。例えば、アカウント作成をリクエストする社員は、そのリクエストを承認する人であってはなりません。 サプライヤーは、個人情報へのアクセスが適切に管理され、サービスを提供するためにアクセスを必要とする者に限定されていることを確実にしなければなりません。 アクセス管理プロセスは、業界ベストプラクティスに従って定義され、以下を含むものとします。 • サプライヤーは、アクセス管理プロセスおよび決定事項が文書化され、すべての IT システム（Barclays の情報資産を保存または処理するもの）に適用されることを確認し、実施の際には、新入社員/異動者/離職者/リモートアクセスする社員に対する適切な管理を実行するものとします。	適切な LAM 管理は、情報資産を不正な使用から守る上で役立ちます。 アクセスマネジメント管理は、承認されたユーザーのみが情報資産にアクセスできることを確認する上で役立ちます。

	• 承認には、アクセスの許可、変更、取消のプロセスに、許可される権限に相当する承認のレベルが含まれることを確実にするために、管理が確立されなければなりません。 • アクセス管理プロセスに、検証を識別するための適切なメカニズムが含まれることを確実にするために、管理が確立されることが必須です。 • 各アカウントは、そのアカウントを使用して行う活動に責任を負う 1 名の個人に関連付けられている必要があります。 • アクセスの再認証 - アクセス許可がその目的にかなっていることを確認するために、少なくとも 12 か月に 1 度見直しを行うための体制を確立するものとします。 • すべての特権アクセス許可は、少なくとも 6 か月ごとにレビューされることが必須であり、特権アクセス要求には適切な管理が実施されなければなりません。	

	• 異動者管理 – 異動日から 24 時間以内にアクセスを修正/削除する（適切な記録は残す）。 • 離職者管理 - Barclays にサービスを提供するために使用されたすべての論理アクセスは、離職日から 24 時間以内に削除する（適切な記録は残す）。 • リモートアクセス - リモートアクセスの管理は、Barclays（最高セキュリティオフィスの ECAM チーム）が合意したメカニズムを通してのみ許可されるものとし、リモートアクセスは多要素認証を使用するものとします。 • 認証 - 適切なパスワードの長さと複雑さ、パスワードの変更頻度、多要素認証、パスワード認証情報の安全な管理、その他の管理は、業界のベストプラクティスに従うものとします。 • 休眠アカウント - 連続して 60 日以上使用されていない休眠アカウントは一時停止/無効にする（適切な記録は残す）。 • 対話型アカウントのパスワードは最低でも 90 日に 1 度変更される必要があり、それ以前の 12 パスワードとは異なるものである必要があります。 • 特権アカウントは、使用後に毎回変更され、少なくとも 90 日に 1 度変更されるものとします。 • 対話型アカウントは、最大 5 回連続して失敗するか、または業界ベストプラクティスで定められている場合はそれ以下の回数失敗した場合は無効にする必要があります。	
21.脆弱性管理	サプライヤーは、サプライヤーが所有または管理するアプリケーション、インフラストラクチャ・ネットワーク、およびシステム・コンポーネント内の脆弱性を効果的に監視し適時に検出し、修正するための方針と手順を確立し、それを支えるプロセス/全社的措置、おｙび技術的対策を実施して、実施されたセキュリティ対策が効率的であることを確認するものとします。 脆弱性管理は、以下をカバーする必要がありますが、これらに限定されるものではありません。	この管理が実施されない場合、攻撃者がシステム内の脆弱性を利用しサイバー攻撃を行う場合があり、規制上または風評上の損害が発生する恐れがあります。

- 監視、報告書作成、上申、および是正のための役割、責任、および説明責任が定義されている。
- 脆弱性を調査するための適切なツールおよびインフラストラクチャ。
- 脆弱性調査をルーティンベースで（業界ベストプラクティスに従って定期的に）実施し、環境内のすべての資産クラスの既知および未知の脆弱性を効果的に特定する。
- リスクの活用-発見された脆弱性の修正に優先順位をつけるための評価プロセス。
- 環境内のすべての資産クラスにわたる脆弱性の修正を迅速かつ効果的に検証する脆弱性改善検証プロセスを確立する。
- 脆弱性が悪用されるリスクを低減するために、強力な修正活動とパッチ管理を通じて、脆弱性に効果的に対処することを確認する（業界ベストプラクティスに従って適時に実施される是正措置）。
- 継続的に脆弱性調査を行い、その結果を定期的に比較し、適時に脆弱性が修正されていることを確認する。

サプライヤー向けに、Barclays に代わってインフラ/アプリケーションの **ホスティング** に関連するサービスを提供するものとします。

- サプライヤーは、重大/高いに該当する脆弱性が発見された場合、直ちに Barclays に通知しなければなりません。
- サプライヤーは、以下の表に従って、または Barclays（最高セキュリティオフィスの ECAM チーム）との合意に基づいて、脆弱性を是正しなければなりません。

優先順位	評価	閉鎖日数（最大）
P1	重大	15
P2	高い	30

	<table><tr><td>P3</td><td>中程度</td><td>60</td></tr><tr><td>P4</td><td>低い</td><td>180</td></tr><tr><td>P5</td><td>参考</td><td>360</td></tr></table> サプライヤーが提供するホスティングインフラストラクチャ/ウェブアプリケーションに重大な影響を与えることのある、すべてのセキュリティ問題や脆弱性について、サプライヤーがリスク受け入れを決定したものについては、速やかに Barclays に連絡/通知し、Barclays（最高セキュリティオフィスの ECAM チーム）と書面で合意するものとします。	
22.パッチ管理	サプライヤーは、セキュリティパッチの必要性を監視/追跡し、サプライヤーの環境/資産全体を管理するためにセキュリティ修正プログラムを導入するため、確立された方針および手順、業務プロセス/全社的措置、ならびに実施済みの技術的措置を備えているものとします。 サプライヤーは、システム/資産/ネットワーク/アプリケーションに最新のセキュリティパッチが適時にかつ業界のベストプラクティスに従って適用され、以下の事項が確実に行われていることを確認するものとします。 • サプライヤーは、本番システムにパッチを移行させる前に、目標となる本番システムの構成を正確に表すシステム上のすべてのパッチをテストし、パッチ適用後にパッチを適用したサービスの動作の妥当性を検証するものとします。パッチが適用できない場合は、適切な対策を講じる必要があります。 • サービス中断およびセキュリティー違反を防止するため、すべての主要な IT 変更は、実施前にログを取り、テストし、承認済みの堅固な変更管理プロセスによる承認を受けるものとします。	この管理が実施されない場合、消費者データが損なわれたり、サービスの損失、または、他の悪意ある行為を可能にする、セキュリティ上の問題に対してサービスが脆弱になる可能性があります。

<table>
<tr><td></td><td>

- サプライヤーは、パッチが本番環境と災害復旧（DR）環境に反映されていることを確認するものとします。

</td><td></td></tr>
<tr><td>23.脅威シミュレーション/ペネトレーションテスト/IT セキュリティ評価</td><td>

サプライヤーは、Barclays に提供するサービスに関連する、災害復旧サイトおよびウェブアプリケーションを含む IT インフラを対象とする IT セキュリティ評価/脅威シミュレーションを実施するため、独立の、適格なセキュリティプロバイダーと契約するものとします。

これは、サイバー攻撃により Barclays データの機密性の違反に利用される恐れのある脆弱性を特定するために、少なくとも年に一度実施するものとします。すべての脆弱性は、解決のために、優先順位を付けて追跡しなければなりません。テストは、業界ベストプラクティスに沿って実施するものとします。

サプライヤー向けに、Barclays に代わってインフラ/アプリケーションの **ホスティング** に関連するサービスを提供するものとします。

- Barclays の主要活動の中断を防ぐため、サプライヤーは Barclays とセキュリティ評価の対象範囲について、特に開始日と終了日/時間について通知し、合意を得るものとします。
- リスク許容と決定されたすべての問題は、Barclays（最高セキュリティオフィスの ECAM チーム）に伝達され、合意を得るものとします。
- **サプライヤーは、最新のセキュリティ評価報告書を年に一度、Barclays（最高セキュリティオフィスの ECAM チーム）に提供するものとします。**
- サプライヤーは、重大/高いに該当する脆弱性が発見された場合、直ちに Barclays に通知しなければなりません。
- サプライヤーは、以下の表に従って、または Barclays（最高セキュリティオフィスの ECAM チーム）との合意に基づいて、脆弱性を是正しなければなりません。

優先順位	評価	閉鎖日数（最大）

</td><td>

この管理が実施されない場合、サプライヤーは、直面するサイバー脅威および防衛策の適切性と強度を評価することができない場合があります。

Barclays の情報が曝露され、および/または、サービスの損失が発生する可能性があり、規制上または風評上の損害が発生する恐れがあります。

</td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>
<table>
<tr><td>P1</td><td>重大</td><td>15</td></tr>
<tr><td>P2</td><td>高い</td><td>30</td></tr>
<tr><td>P3</td><td>中程度</td><td>60</td></tr>
<tr><td>P4</td><td>低い</td><td>180</td></tr>
<tr><td>P5</td><td>参考</td><td>360</td></tr>
</table>
</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24.暗号</td>
<td colspan="3">

暗号化の根拠 - サプライヤーは、暗号化技術を利用する根拠を文書化し、目的に合致しているかどうかを確認するものとします。
暗号化ライフサイクル管理手順書 - サプライヤーは、暗号化キー管理のためのキー生成、アップロード、配布から廃棄までのエンドツーエンドのプロセスを詳細に説明した暗号化ライフサイクル管理手順書を文書化し、管理するものとします。
マニュアル操作による承認 - サプライヤーは、キーおよび電子証明書に関する、人による管理イベント（新しいキーおよび証明書の登録および生成を含む）のすべてが適切なレベルで承認され、承認の記録が保持されることを確認するものとします。
デジタルによる承認 - サプライヤーは、すべての証明書が承認・審査を受けた認証局（CA）により発行されていることを確認するものとします。また、技術的に認証局の証明を受けることが不可能な場合、およびキーの完全性・真正性を確保して適時に失効・更新を行うために手動での管理が必須となる場合のみ、自己署名による証明書が利用可能であることを確認するものとします。
キーの生成と暗号化期間 - サプライヤーは、すべてのキーを、認証されたハードウェア、または暗号論的擬似乱数生成器（CSPRNG）ソフトウェアを使用してランダムに生成する必要があります。

</td>
<td>最新かつ適切な暗号保護とアルゴリズムは、Barclays の情報資産の継続的な保護を保証します。</td>
</tr>
</table>

	○ サプライヤーは、それによってすべてのキーが更新または無効化されるまでの限定および定義された暗号期間のライフタイムでのみ機能することを確認するものとします。これは、アメリカ国立標準技術研究所 (NIST) および該当する業界ベストプラクティスにも合致している必要があります。 • キーストレージの保護 - サプライヤーは、秘密/非公開の暗号キーが以下の形態でのみ存在することを確認するものとします。 ○ ハードウェアで認証されたセキュリティデバイス/モジュールの暗号境界の形態。 ○ 暗号化された形式で、別の確立されたキーまたはパスワードから派生したキーの形態。 ○ 別々の保管・管理グループに分割された各構成部分の形態。 ○ HSM の保護に必要でない限り、暗号化処理の期間はホストメモリで構築される。 • サプライヤーは、ハイリスクキーについては、キーが HSM のメモリの境界内で生成され、保持されることを確認するものとします。これには以下が含まれます。 ○ HSM が義務化されている規制サービスのキー。 ○ 公的な認証局が Barclays を代表する証明書。 ○ Barclays n のサービスを保護する証明書の交付に使用されるルート証明書、交付証明書、失効証明書、RA（登録局）証明書の各証明書。 ○ キー、認証情報、または PII データの集約されたリポジトリを保護するキー。 • キーのバックアップと保管 - サプライヤーは、キーが破損したり、復元が必要になった場合にサービスが中断されないようにするため、すべてのキーのバックアップを保管するものとします。バックアップへのアクセスは、知識分離、二重管理された安全な場所のみで行われるよう制限されるものとします。キーのバックアップには、使用中のキーと同等以上の強力な暗号化保護を使用するものとします。 • 目録 - サプライヤーは、Barclays に提供するサービスで使用する暗号化された完全かつ最新の目録（万一の事故発生時に被害を防止するために、サプライヤーが管理するすべての暗号キー、電子証明書、暗号化ソフトウェア、暗号化ハードウェアを詳細に記述したもの）を保	

	管するものとします。少なくとも四半期に 1 度見直しを行い、Barclays に提供された目録に署名することで証明されたものとします。目録には、必要に応じて以下を含めるものとします。 ○ IT サポートチーム ○ 関連の資産 ○ アルゴリズム、キー長、環境、キー階層、認証局、指紋、キーの保存・保護、技術的・運用上の目的。 • 機能目的と運用目的 - キーは、機能および運用の単一の目的を有するものとし、複数のサービス間で共有したり、Barclays のサービスの範囲を超えて共有してはなりません。 • 監査証跡 - サプライヤーは、すべてのキーおよび証明書のライフサイクル管理イベントについて、少なくとも四半期に 1 度監査可能な記録見直しを実施し、その証拠（不正使用を検知するために、キーの生成、配布、アップロード、破壊を含むすべてのキーの完全な管理を実証するもの）を保管するものとします。 • ハードウェア - サプライヤーは、ハードウェアデバイスを安全な場所に保管し、キーのライフサイクル全体で監査証跡を保持して、暗号デバイスの保管チェーンが危険にさらされないようにするものとします。この証跡は四半期に 1 度見直しを行うものとします。 ○ サプライヤーは、暗号ハードウェアが少なくとも FIPS140-2 レベル 2 の認証を受け、物理的セキュリティおよび暗号キー管理または PCI HSM のレベル 3 を達成していることを確認するものとします。サプライヤーは、個人または顧客がオフサイトで保管しているキーを保管するための許容可能なハードウェアとして、チップベースのスマートカードまたは FIPS 認定の電子トークンを許可することができます。 • キーの危殆化 - サプライヤーは、危殆化したキーの更新に関する情報が漏えいを防ぐため、キーの危殆化対策計画を維持・監視し、危殆化したキーとは別に更新キーが生成されるようにするものとします。危殆化インシデントが発生した場合は **Barclays チーフセキュリティオフィス（CSO）ジョイントオペレーションセンター（JOC）**（gcsojoc@barclays.com）に報告するものとします。	

	• 強力なアルゴリズムとキー - サプライヤーは、使用されているアルゴリズムとキー長が、アメリカ国立標準技術研究所 (NIST) および該当業界の要件に準拠していることを確認するものとします。	
25.クラウドコンピューティング	サプライヤーは、Barclays のサービスに使用されるクラウドサービスが、機密性、完全性および可用性という核となる概念を保護し、Barclays のサービスを保護するためにセキュリティ管理が実施され、効果的に運用されていることを確実にするため、明確に定義されたセキュリティ管理フレームワークを備えていなければなりません。サプライヤーは、クラウド技術のあらゆる使用について安全を確保するため、確立されたセキュリティ対策を講じるために、ISO/IEC 27017 もしくは 27001 または SOC 2 もしくは類似のクラウドセキュリティフレームワークまたは業界ベストプラクティスの認証を取得するものとします。 クラウドサービスプロバイダーが、最新版のクラウドセキュリティアライアンスであるクラウドコントロールマトリクス (CCM) に相当する適切な管理を含むベストプラクティスの認定を受けていることを確認するものとします。 サプライヤーは、クラウド内の個人データを含む Barclays の情報資産/データに関連するデータセキュリティ管理を確実に実施する責任を負っており、クラウドサービスプロバイダの CSP は、クラウドサービスのセキュリティに責任を負っています。サプライヤーは、データ侵害を含むいかなるセキュリティインシデントからも自らを保護するために、セキュリティコントロールの実施の構成と監視について引き続き責任を負います。 サプライヤーは、Barclays の情報および Barclays が利用するサービスへの権限のない個人のアクセス機会を最低限にすることで機密性、完全性、可用性およびアクセス性を保護できるようにするため、クラウド共有責任モデルを含む、提供されるサービスのすべての側面にわたってセキュリティ対策を実施しなければなりません。クラウド管理は、以下のデプロイメントモデル (IaaS/PaaS/SaaS) を含むものとしますがこれらに限定されません。	このクラウド管理が実施されない場合、Barclays のデータは危害を受ける可能性があり、規制上または、Barclays に対する風評被害を招くおそれがあります。

	• ガバナンスと説明責任の仕組み • ID およびアクセス管理 • ネットワークセキュリティ（接続性を含む） • データセキュリティ（転送/休止/保存） • 暗号作成、暗号化、およびキー管理 - CEK • 記録と監視 • 視覚化 • サービスの分離 Barclays へ提供されるサービスの一環としてクラウドに保存されている、個人データを含む Barclays の情報資産/データは、Barclays（最高セキュリティオフィスの ECAM チーム）の承認を受けている必要があります。 機密データ（個人データおよび制限付きデータ） がクラウドサービスプロバイダーによって保持されている場合、サプライヤーは Barclays に対し、そのようなデータが保持される場所、データゾーンおよびフェイルオーバー（障害迂回）用のデータゾーンを提供するものとします。	
26.銀行専用スペース（BDS）	正式な銀行専用スペース（BDS）が要求されるサービスには、特定の BDS 用物理的および技術的要件を設けるものとします。（BDS はサービス要件である場合、管理要件が適用されます。） BDS の種類の違いは以下の通りです。 ティア 1（ファーストクラス） - IT インフラストラクチャ全体が、Barclays に管理される LAN、WAN、デスクトップが Barclays 専用のスペースを有するサプライヤーの敷地内に提供されることで、Barclays によって管理されます。	この管理が履行されない場合、適切な物理的および技術的管理が設けられず、サービスの遅延または中断、または、サイバーセキュリティ違反/セキュリティインシデントの発生を招く可能性があります。

	ティア 2（ビジネスクラス） - IT インフラ全体が **サプライヤー** によって管理され、Barclays のエクストラネットゲートウェイに接続されます。LAN、WAN、デスクトップ機器はサプライヤーが所有し、管理します。 ティア 3（エコノミークラス） – IT インフラ全体は **サプライヤー** によって管理され、Barclays のインターネットゲートウェイに接続されます。LAN、WAN、デスクトップ機器はサプライヤーが所有し、管理します。	
26.1 BDS - 物理的分離	占有される物理的エリアは、Barclays 専用とし、他の会社/ベンダーと共有させることはできません。論理的にも物理的にも分離されていることが必要です。	
26.2 BDS - Physical Access Control	• サプライヤーは、サービスが提供される BDS へのアクセス方法と認証をカバーする物理的なアクセス手順を有している必要があります。 • BDS エリアへの出入りを制限し、物理的なアクセス管理のしくみによって監視し、許可された担当者のみがアクセスを許可されていることを確認するものとします。 • 施設内の BDS エリアにアクセスするには、承認された電子アクセスカードが必要です。 • サプライヤーは、許可された個人にのみ BDS アクセスが提供されていることを確認するため、四半期に 1 度チェックを実施するものとします。例外は徹底的に調査して解決するものとします。 • 離職者や移動者のアクセス権は、24 時間以内に削除するものとします（適切な記録は残す）。 • 警備員を配置して BDS 内を定期的に巡回し、不正アクセスや不正行為の疑いの活動を効率的に特定するものとします。 • BDS へのアクセスには、以下を含むセキュリティ自動管理を運用するものとします： 認証されたスタッフの場合: o 常時見ることができる写真付き ID バッジ o 近接カードリーダーを配置 o アンチパスバックメカニズムを有効化 • サプライヤーは、メンテナンスや清掃を目的とした BDS エリアへの物理的なアクセス権を持つ第三者を含む、外部スタッフの管理と監視のためのプロセスと手順を実施するものとします。	

26.3 BDS - ビデオによる監視	• 不正アクセスや悪質な活動を効果的に検知し、調査するために、BDS エリアのビデオ監視を実施するものとします。 • BDS エリアのすべての出入り口はビデオ監視するものとします。 • 悪意のある活動を捉え、調査に役立てるため、防犯カメラを適切に配置し、常に鮮明で識別可能な画像が得られるようにします。 サプライヤーは、関連する CCTV 画面を変更、削除、または「偶然見てしまう」ことを防ぐため、記録された CCTV の映像を 30 日間保存し、すべての CCTV の記録とレコーダーを安全に配置するものとします。また、録画へのアクセスは、権限のある個人にのみ制御、制限するものとします。
26.4 BDS - Barclays のネットワークおよび Barclays 認証へのアクセス トークン	• 個々のユーザーは、Barclays が提供する多要素認証トークンを使用して、BDS から Barclays のネットワークへの認証のみを行うものとします。 • サプライヤーは、Barclays の認証トークンを提供された個人の記録を保持し、四半期に 1 度その照合を行うものとします。 • Barclays は、アクセスが不要になった旨の通知（従業員の雇用終了、プロジェクトの再配置など）を受けた場合、24 時間以内に認証情報を無効化します。 • Barclays は、認証情報が一定期間使用されていない場合（使用されていない期間は 1 ヶ月を超えないもの）、直ちに認証情報を無効化します。 • Barclays の Citrix アプリケーションを介してリモート印刷にアクセスが可能なサービスは、Barclays（最高セキュリティオフィスの ECAM チーム）の承認と認証を受けている必要があります。サプライヤーは記録を保管し、四半期に 1 度調整を行うものとします。 コントロール - 12 を参照。在宅勤務（リモートアクセス）
26.5 BDS - オフィス外サポート	BDS 環境へのリモートアクセスは、デフォルトでは、オフィス時間外/営業時間外/リモートワークのサポートは提供されません。すべてのリモートアクセスは、関係する Barclays チーム（チーフ・セキュリティ・オフィス-ECAM チームを含む）による承認を受けるものとします。
26.6 BDS - ネットワークセキュリティー	• 組織のネットワーク境界のすべての最新の目録を保管する（ネットワークアーキテクチャ/ダイアグラムを介して）。 • ネットワークの設計と実施は、少なくとも年に 1 度見直す必要があります。 • BDS ネットワークは、ファイアウォールによってサプライヤ企業ネットワークから論理的に分離され、すべてのインバウンドおよびアウトバウンドトラフィックが制限・監視される必要があります。

	• ルーティング設定は、Barclays ネットワークへの接続を確保する必要があり、他のサプライヤーネットワークにルーティングしてはなりません • Barclays エクストラネット・ゲートウェイに接続するサプライヤーのエッジルーターは、ポート、プロトコル、およびサービスの制御を制限するという構想のもとで安全に設定されていなければなりません。 　　o　ロギングと監視が確実に有効化されている必要があります。 • BDS ネットワークは、アクセスが監視され、許可されている機器のみが適切なネットワークアクセス管理を通じて許可されることを確認するものとします。 コントロール - 10 を参照。境界とネットワークセキュリティ
26.7 BDS – ワイヤレスネットワーク	Barclays にサービスを提供するためには、Barclays のネットワークセグメントで無線ネットワークを無効にする必要があります。
26.8 BDS - エンドポイントセキュリティ	データセンターまたはクラウドで Barclays 情報を運用するサプライヤー（下請業者を含む）は、セキュリティ管理のための業界ベストプラクティス認証を取得する必要があります。 業界のベストプラクティスを導入する必要があります。また、BDS エンドポイント機器のセキュリティビルドには以下のものが必要ですが、これらに限定されるものではありません。 • ディスクの暗号化 • 不要なソフトウェア/サービス/ポートをすべて無効にする • ローカルユーザーの管理者権限アクセスを無効にする • サプライヤーの社員がデフォルトのサービスパック、デフォルトサービスなどの基本設定を変更することを許可しない • Barclays のデータを外部メディアにコピーできないよう、USB ポートを無効にする • 最新のアンチウイルスシグネチャとセキュリティパッチで更新を実施する • 切り取り、コピー & ペーストをしない、スクリーンショットを撮らないことにより情報漏えい対策を行う • デフォルトでは、プリンターへのアクセスを無効にする • Barclays の情報資産/データの共有/転送は、インスタントメッセージツール/ソフトウェアを使用して無効にする • 悪意があると識別された不正なソフトウェアを検出し、不正なソフトウェアのインストールを防止する機能とプロセスを備える

	コントロール - 16 を参照。エンドポイントセキュリティ	

26.9 BDS - E メールとインターネット	• ネットワーク接続性は、BDS ネットワーク上の E メールやインターネット活動を制限するよう、安全に設定される必要があります。
	• サプライヤーは、google ドライブ、Dropbox、iCloud のような、インターネット上で情報を保存する機能を持つソーシャルネットワークサイト、ウェブメールサービス、およびウェブサイトにアクセスできる権限を制限するものとします。
	• Barclays データの BDS ネットワーク外への無断転送があった場合、データ漏えいから保護するものとします。
	  • E メール
	  • インターネット/ウェブゲートウェイ（オンラインストレージ、ウェブメールを含む）
	• ネットワークベースの URL フィルタを設置し、サプライヤー組織内またはインターネット上のウェブサイトにのみ接続できるようシステムの機能を制限するものとします。
	• すべての添付ファイルやウェブサイトへのアップロード機能をブロックします。
	• フルサポートされているウェブブラウザと E メールクライアントのみが許可されていることを確認します。	

26.10 BDS - BYOD/個人所有のデバイス	**個人のデバイス/BYOD からの Barclays の環境および/または Barclays データへのアクセスを許可してはなりません**	
視察の権利	サプライヤーは、Barclays による少なくとも 10 営業日前の書面による通知により、サプライヤーがその義務へのコンプライアンスを果たしているかを審査するため、サプライヤーまたは下請業者が役務に使用しているサプライヤーシステムの開発、テスト、改良、保全のために使用する現場または技術に対し、Barclays がセキュリティ審査を実施することを許可するものとします。 サプライヤーは、Barclays が年に 1 度、またはセキュリティーインシデント後即時に視察を実施することを許可するものとします。 視察中に Barclays により特定された管理の非遵守については、Barclays によるリスク評価が行われ、Barclays は改善期間を特定するものとします。サプライヤーは、それを受け、期間内に必要な改善を完了するものとします。	これが合意されない場合、サプライヤーはこれらのセキュリティ義務に対するコンプライアンスの完全な保証を与えることができなくなります。

	サプライヤーは、Barclays から合理的に要求された視察に関するすべてのサポートを提供し、視察中に提出された書類に記入し、Barclays に返却するものとします。	

付属書 A：用語集

定義	
アカウント	それによって、IT システムへのアクセスが論理アクセスコントロールを使用して管理される、一連の認証情報（例えば、ユーザーIDとパスワード）。
バックアップ	バックアップまたはバックアッププロセスとは、追加コピーがデータ損失イベント後にオリジナルの回復に使用できるよう、データの複製を作成することを指す。
銀行専用スペース	銀行専用スペース（BDS)とは、サービスを実行または提供するサプライヤーグループメンバーまたは Barclays 専属の下請業者の所有または管理する施設を意味する。
業界ベストプラクティス	市場をリードするベストプラクティス、プロセス、標準、認定を使用して、Barclays に提供されるサービスと同一または類似のサービスの提供に従事できる高度なスキルおよび経験があり、ならびに市場をリードする専門組織が合理的に期待する程度の技能と配慮を行使すること。
BYOD	個人所有のデバイス
暗号	機密性、データ完全性および/または認証などの目標を達成するため、データに適用することのできる技法およびアルゴリズムを開発する数学的理論の適用。
サイバーセキュリティ	コンピュータシステム、ネットワーク、プログラム、デバイス、およびデータをデジタル攻撃から保護するための技術、プロセス、コントロール、および組織的手段の適用のこと。これには、ハードウェア、ソフトウェア、またはデータの不正な開示、破壊、紛失、改変、盗難、または損傷が含まれます（ただし、これらに限定されません）。
データ	事実、概念または指示を記憶媒体に記録し、自動手段で通信、検索および処理を行い、人間が理解可能な情報として提示されたもの。
サービス妨害（攻撃）	その意図されたユーザーがコンピューターリソースを使用できないようにする試み。
破棄/削除	情報を復元できないようにする、上書き、削除または物理的な破壊行為。
ECAM	サプライヤーのセキュリティ姿勢を評価する外部のサイバー保証・監視チーム。
暗号化	不正リーダーにより理解できない意味のない形式にメッセージ（データ、音声、または動画）を変換すること。 プレーンテキスト形式から暗号形式に変換すること。
HSM	ハードウェアセキュリティモジュールのこと。暗号化処理の高速化など、安全な暗号キーの生成・保存・利用を実現する専用デバイス。
情報資産	その情報の守秘性、整合性、可用性要求の観点から価値があると考えられる、あらゆる情報。あるいは その組織にとっての価値を有する単一またはグループの情報
情報資産の所有者	資産の分類と、それが適正に取り扱われることを保証する責任を負う組織内の個人。

最小限の権限	ユーザーまたはアカウントがビジネス上の役割を履行できるようにする最低レベルのアクセス/許可。
ネットワークデバイス/ネットワーク機器	ネットワークに接続され、ネットワークを管理、サポート、または管理するために使用される IT 機器。 ルーター、スイッチ、ファイアウォール、ロードバランサが含まれるが、これらに限定されない。
悪意のあるコード	IT システム、デバイス、またはアプリケーションのセキュリティ方針を迂回することを意図して書かれたソフトウェア。例としては、コンピューターウィルス、トロイの木馬、ワームなどがある。
多要素認証 (MFA)	2 つ以上の異なる認証技術が要求される認証。 例としてはセキュリティトークンの使用があり、認証の成功は、個人が保有するもの（すなわちセキュリティトークン）かつユーザーが知っているもの（すなわちセキュリティトークン暗証番号）に依拠する。
個人データ	識別された又は識別可能な自然人（「データ主体」）に関連するあらゆる情報。識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子などの識別子、またはその自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的同一性に特有の 1 つ以上の要因を参照することによって、直接的または間接的に識別可能な自然人のことを指します。
特権アクセス	ユーザー、プロセス、またはコンピュータに対し、特別な（標準より上の）アクセス、権限、または機能が割り当てられること。
特権アカウント	特定の IT システムに対して高レベルの管理を提供するアカウントのこと。これらのアカウントは通常、IT システムのシステムメンテナンス、セキュリティ管理、または、構成変更のために使用される。 例として、「管理者」、「ルート」、uid=0 の Unix アカウント、サポートアカウント、セキュリティ管理アカウント、システム管理アカウント、ローカル管理者アカウントなどがある。
リモートアクセス	権限のあるユーザーが離れた場所から会社のネットワークおよびシステムにアクセスできるようにするために使用される技術および手法。
システム	この文書の文脈において、システムとは、人員、手順、IT 機器およびソフトウェアを指す。この複合体の要素は、与えられたタスクを行うため、または特定の目的、サポートまたはミッションに関する要件を達成するために意図された運用環境またはサポート環境において共に使用される。
必須事項	この定義は、その意味合いを十分に理解し、慎重に評価することを意味します。
セキュリティーインシデント	セキュリティインシデントは、以下を含むがこれに限定されないイベントと定義されます。 • （失敗または成功にかかわらず）システムまたはそのデータへの不正アクセスを試みること。 • 望まれていないサービスの中断または拒否。 • データの処理または保存のためのシステムの不正使用。

	• 所有者の知識、指示、または同意なくシステムのハードウェア、ファームウェア、またはソフトウェアの特性を変更すること。 • データへの不正アクセスにつながるアプリケーションの脆弱性。

付属書 B：Barclays 情報ラベリングスキーム

表 B1：Barclays 情報ラベリングスキーム

ラベル	定義	例
秘密	情報は、エンタープライズリスク管理枠組み（ERMF）の下で「最重要」と評価され（財務または非財務）、その不正な開示が Barclays にマイナスの影響を及ぼす場合、**秘密**として分類されるものとします。 この情報は特定の対象者に制限され、作成者の許可なしにさらに配布してはなりません。対象者には情報所有者の明示的な許可を受けた社外の受取人が含まれる場合があります。	• 吸収合併または買収可能性の情報 • 戦略的な計画情報 – ビジネスと組織 • 特定の情報セキュリティの設定に関する情報 • 特定の監査所見およびレポート • 執行委員会議事録 • 認証または本人確認および検証（ID&V）詳細 – 顧客/取引先および社員 • 大量のカードホルダー情報 • 利益予測または年度決算結果（一般公開前） • 正式な機密保持契約（NDA）で対象となっている項目
社内秘	想定されている受取人が Barclays の認証された社員であるか、Barclays と有効な契約を締結した特定の対象者に限定された Barclays マネージドサービスプロバイダー（MSP）のみである場合、情報は**社内秘**として機密情報に分類されるものとします。 エンタープライズリスク管理枠組み（ERMF）の下で「重要」または「関係者外秘」と評価される情報（財務または非財務）は、不正に開示された場合 Barclays に悪い影響を及ぼす場合があります。 この情報は一般的な配布を意図していませんが、知る必要の原則に従って受取人は転送または共有することができます。	• 戦略および予算 • 成績評価 • スタッフの報酬および個人情報。 • 脆弱性評価
社外秘	想定されている受取人が Barclays の認証された社員であるか、Barclays と有効な契約を締結した特定の対象者に限定された Barclays マネージドサービスプロバイダー（MSP）、または情報の所有者によって承認された外部の	• 新製品計画 • 依頼人契約書 • 法的契約書

	関係者のみである場合、情報は**社外秘**として機密情報に分類されるものとします。 エンタープライズリスク管理枠組み（ERMF）の下で「重要」または「限定」と評価される情報（財務または非財務）は、不正に開示された場合 Barclays にマイナスの影響を及ぼす場合があります。 この情報は一般的な配布を意図していませんが、知る必要の原則に従って受取人は転送または共有することができます。	• 外部への送信を目的とした個人・少数顧客・取引先情報 • 顧客/取引先への通信。 • 新情報を提供する新しい発行物（目論見書、募集要項など） • 最終調査報告書 • Barclays 外へ非公開の重大な情報（MNPI） • 全調査報告書 • 特定のマーケティング資料 • 市場解説 • 監査所見およびレポート
制限なし	情報は、一般配布を目的としているか、または配布されても組織に悪影響を与えない場合、「制限なし」に分類されるものとします。	• マーケティング資料 • 出版物 • 公示 • 求人広告 • Barclays に影響を及ぼさない情報

表 B2：Barclays 情報ラベリングスキーム – 取り扱い要件

*** システムセキュリティ設定情報、監査所見、および個人情報は、無許可の開示がビジネスに及ぼす影響により、社内秘または秘密のいずれかに分類される場合があります

ライフサイクル段階	秘密	社内秘	社外秘
作成および導入	• 資産には情報資産所有者を割り当てることが必須。	• 資産には情報資産所有者を割り当てることが必須。	• 資産には情報資産所有者を割り当てることが必須。
保存	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所に保管してはなりません。	• 資産（物理または電子）は、公共エリア（訪問者が監視されずにアクセスすることが可能なサプライヤー施設内の公共エリアを含む）に保管してはなりません。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所に保管してはなりません。

	• 保管中の電子資産は、許可を受けない人物がアクセスできる重大なリスクがある場合は、暗号化または適切な補償管理によって保護することが必須です。 • Barclays のデータ、アイデンティティ、および/または名声を保護するために使用されるすべてのプライベート鍵は、FIPS 140-2 レベル 3 以上の証明書付きハードウェアセキュリティモジュール（HSM）により保護されるものとします。	• 情報は、訪問者が監視されることなくアクセスが可能な施設内の公共エリアに放置してはなりません。	• 保管中の電子資産は、許可を受けない人物がアクセスできる重大なリスクがある場合は、暗号化または適切な補償管理によって保護することが必須です。
アクセスおよび使用	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所で作業したり、無人状態で放置してはなりません。 資産は、適切な管理が確立されている場合のみ作業可能です（覗き見防止フィルムなど）。 • 印刷される資産は、印刷セキュリティツールを使用して印刷するものとします。 • 電子資産は、適切な論理的アクセス管理により保護するものとします。	• 資産（物理または電子）は、施設外の公共エリアに放置してはなりません。 • 資産（物理または電子）は、訪問者が監視されることなくアクセスが可能な施設内の公共エリアに放置してはなりません。 • 電子資産は、必要に応じ、適切な論理的アクセス管理により保護するものとします。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所で作業したり、無人状態で放置してはなりません。 資産は、適切な管理が確立されている場合のみ作業可能です（覗き見防止フィルムなど）。 • 印刷された資産は、速やかにプリンターから回収するものとします。 それが不可能な場合は、印刷セキュリティツールを使用するものとします。 • 電子資産は、適切な論理的アクセス管理により保護するものとします。
共有	• 紙印刷された資産には、全ページに明確な情報ラベルを付けるものとします。	• 紙印刷された資産には、明確な情報ラベルを貼るものとします。 ラベルは、最低でもタイトルページに貼るものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。	• 紙印刷された資産には、明確な情報ラベルを貼るものとします。 ラベルは、最低でもタイトルページに貼るものとします。 • 紙印刷された資産が入っている封筒には、表面に明確な情報ラベルを貼るものとします。

	• 紙印刷された資産が入っている封筒には、表面に明確な情報ラベルを貼り、開封明示シールを貼るものとします。 それらは配布前に、ラベルのない別の封筒に入れるものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。 複数ページの電子文書のコピーには、全ページに明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。 • 資産は、情報資産の所有者により受信を個別に許可された人員のみに配布するものとします。 • 資産はファックスで送信してはなりません。 • 電子資産を社内ネットワーク外に転送する場合は、承認済みの暗号保護メカニズムを使用して暗号化するものとします。 • 電子資産の流通管理を維持するものとします。	• 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。	• 電子資産には、明確な情報ラベルを付けるものとします。 複数ページの電子文書のコピーには、全ページに明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。 • 資産は、それを受け取るためのビジネス上のニーズがある人員のみに配布するものとします。 • 資産は、受信者がその資産をすぐに回収できることを送信者が確認していない限り、ファックスで送信してはなりません。 • 電子資産を社内ネットワーク外に転送する場合は、承認済みの暗号保護メカニズムを使用して暗号化するものとします。
アーカイブ化と処分	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。

	• 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。 • 秘密電子資産が保存されていたメディアは、処分の前または処分中に、適切に機密情報を分離するものとします。	• 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。	• 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。

銀行秘密

銀行秘密法域（スイス/モナコ）のみを対象とした追加管理

管理エリア/対象	管理内容	本件が重要である理由
1. 役割と責任	サプライヤーは、クライアント識別データ（以下「CID」）の取扱いに関する役割、責任および説明責任を定義し、それを伝達しなければなりません。サプライヤーのオペレーティングモデル（またはビジネス）に重大な変更が行われた後、あるいは少なくとも年に 1 度、サプライヤーは CID の役割、責任、および説明責任に焦点を当てた文書を見直し、それらを適切な銀行秘密法域に配布するものとします。 主な役割には、CID 関連の全活動の保護と監視に責任を持つ上級役員を含めるものとします（CID の定義については付属書 A を参照してください）。知る必要性の原則に基づき、CID にアクセスするスタッフの数を最小限に抑えるものとします。	役割と責任に関する明確な定義は、外部サプライヤー管理義務スケジュールの実施をサポートします。

2. CID 違反報告	CID に影響を与える違反の報告、管理を徹底するため、文書化された管理、プロセス、手順を設けるものとします。 取り扱い要件（表 B2 に定義される）に違反があった場合は、サプライヤーが対応し、直ちに（遅くとも 24 時間以内に）銀行秘密に対応する Barclays の組織に報告するものとします。CID を含むイベントの適時な取り扱いと通常の報告のためのインシデント対応プロセスを確立し、定期的にテストするものとします。 サプライヤーは、インシデント後に特定された改善措置が、改善計画（是正措置、責任者、実施日）に基づいて対処され、対応する銀行秘密法域と共有され、合意を得ていることを確認するものとします。是正措置は、サプライヤーによって適時に実施される必要があります。 外部のサプライヤーがコンサルティングサービスを提供しており、そのサプライヤーの従業員がデータ損失防止インシデントを引き起こした場合、当行は、その旨をサプライヤーに通知し、必要に応じて従業員の交代を要請する権利を有します。	インシデント対応プロセスは、インシデントを速やかに解決し、エスカレートすることを防止するためのものです。 CID に影響を及ぼす違反は Barclays に深刻な風評被害を与える可能性があり、スイスまたはモナコにおける罰金および銀行業ライセンスの喪失に至る場合があります。
3. 教育と意識向上	CID へのアクセスを持つ、および/またはそれらを取り扱うサプライヤーの社員は、規制に何らかの変更があった後、または少なくとも年に 1 回は CID 銀行秘密要件をカバーするトレーニングを完了するものとします。 サプライヤーは、サプライヤーの新社員全員（CID へのアクセスを持ち、および/またはそれを取り扱う）が、CID に関する自らの責任を確実に理解するよう合理的な期間内（約 3ヶ月）にトレーニングを完了するものとします。 サプライヤーはトレーニングを完了した社員を記録するものとします。 * トレーニングが想定されるコンテンツに関する指導を提供する銀行秘密法域。	教育と意識向上は、本スケジュール内のその他すべての管理を支援します。

4. 情報のラベリングスキーム	***適宜****、サプライヤーは、銀行秘密法域に代わって保有または処理される全ての情報に対して、Barclays 情報ラベリングスキーム（付属書 E の表 E1）または銀行秘密法域と合意した代替スキームを適用するものとします。 CID データの取り扱い要件は付属書 E の表 E2 に記載されています。 *「**適宜**」とは、関連コストに対しラベル付けのメリットが見合う場合を意味します。例えば、文書のラベル付けは、それを行うことにより法的な改ざん防止要件に違反する場合には不適切です。*	情報資産の完全かつ正確な在庫目録は、適切な管理を徹底するために不可欠です。
5. クラウドコンピューティング/外部ストレージ	当該法域向けのサービスの一貫として使用される CID のクラウドコンピューティングおよび/または外部ストレージ（銀行秘密法域外またはサプライヤーインフラストラクチャ外のサーバー）のすべての使用は、対応する関連の現地チーム（チーフ・セキュリティ・オフィス、コンプライアンス部、法務部を含む）により承認される必要があり、高リスクプロファイルに関する CID 情報を保護するため、対応する銀行業秘密取引法域で適用される法律および規制に従って管理を実施するものとします。	この原則が適切に実施されない場合、保護される顧客データ（CID）が損なわれ、法的および規制上の制裁または風評被害が発生する恐れがあります。

付属書 C：用語集

** 取引先特定データは、スイスとモナコにおいて効力を発揮する銀行秘密法により特別データとなっています。そのため、ここにリストされている管理は上記に挙げられているものを補完するものです。

条件	定義
CID	取引先特定データ
CIS	サイバーおよび情報セキュリティ
サプライヤー社員	正規社員としてサプライヤーに直接割り当てられている個人、または限られた期間サプライヤーにサービスを提供する個人（コンサルタントなど）
資産	その組織にとっての価値を有する単一またはグループの情報
システム	この文書の文脈において、システムとは、人員、手順、IT 機器およびソフトウェアを指す。この複合体の要素は、与えられたタスクを行うため、または特定の目的、サポートまたはミッションに関する要件を達成するために意図された運用環境またはサポート環境において共に使用される。
ユーザー	高レベルの権限を持たず、Barclays が所有するシステムに対するアクセス権を付与されているサプライヤーの社員、コンサルタント、請負業者または派遣社員に割り当てられるアカウント。

付属書 D：取引先特定データの定義

直接 CID（DCID）は一意の識別子（取引先が所有する）として定義することができる。これはそのまま、およびそれ自体で、Barclays 銀行アプリケーションにあるデータにアクセスすることなく取引先を特定できる。これは曖昧であってはならず、解釈されるものではなく、名、姓、会社名、署名、ソーシャルネットワーク ID などの情報を含むことがある。直接 CID とは銀行の所有または作成によらない取引先データを指す。

間接 CID（ICID）は 3 つのレベルに分かれている

- L1 ICID は、銀行アプリケーションやその他の**第三者アプリケーション**へのアクセスが提供される場合に、顧客を一意の識別子（銀行が所有）として定義することができるものです。識別子は曖昧であってはならず、解釈されるものではなく、アカウント番号、IBAN コード、クレジットカード番号などの識別子を含むことがある。
- L2 ICID は、別の情報と組み合わせることで、取引先特定を推定できる情報（取引先が所有）と定義される。この情報はそれ自体では取引先の特定に使用できないものの、他の情報と併せて取引先の特定に使用することができる。L2 ICID は DCID と同じ厳格さで保護および管理される必要がある。
- L3 ICID は一意の、ただし匿名化された識別子（銀行が所有）であり、銀行アプリケーションへのアクセスが提供される場合、取引先を特定できるものとして定義される。L1 ICID との違いは銀行秘密ではなく社外限の情報分類であることであり、同じ管理を受けないことを意味する。

分類方法の概要については図 1 CID 決定木を参照してください。

直接および間接 L1 ICID は銀行外の人物と共有してはならず、いかなる時も知る必要の原則を尊重する必要があります。L2 ICID は知る必要ベースで共有することができるが、その他の CID 情報と併せて共有してはなりません。CID の複数の情報を共有することで、潜在的に取引先の身元を明かすような「有害な組み合わせ」を生み出す可能性があります。当社は少なくとも 2 つの L2 ICID をはじめ、有害な組み合わせを定義しています。L3 ICID は銀行秘密レベル情報として分類されていないため共有が可能です。ただし、同一の識別子を繰り返し使用することで、取引先の身元を明かすのに十分な L2 ICID データが収集されることになる恐れがない場合に限られます。

情報分類	銀行秘密			社内秘
分類	直接 CID（DCID）	間接 CID（ICID）		
		間接 (L1)	潜在的に間接 (L2)	非個人的識別子 (L3)
情報の種類	取引先名	コンテナ番号/コンテナ ID	出生地	CID ホスティング/処理アプリケーションの厳密な内部識別子
	会社名	MACC（Avaloq コンテナ ID 下のマネーアカウント）番号	生年月日	動的識別子
	アカウント明細	SDS ID	国籍	CRM 当事者役割 ID
	署名	IBAN	敬称	社外コンテナ ID
	ソーシャルネットワーク ID	e バンキングのログオン詳細	家族の状況	
	パスポート番号	貸し金庫番号	郵便番号	
	電話番号	クレジットカード番号	富の状況	
	メールアドレス	SWIFT メッセージ	大型ポジション/取引価値	
	役職または PEP タイトル	取引先社内 ID	最後の顧客訪問	
	アーチスト名		言語	
	IP アドレス		性	
	FAX 番号		CC 期限日	

			一次連絡先	
			出生地	
			アカウント開設日	

例： 社外の人（スイス／モナコにいる第三者を含む）またはスイス/モナコあるいはその他の国（例えば英国）にある別の関連会社/子会社における社内の同僚にメールを送信したり、文書を共有する場合

1. 取引先名

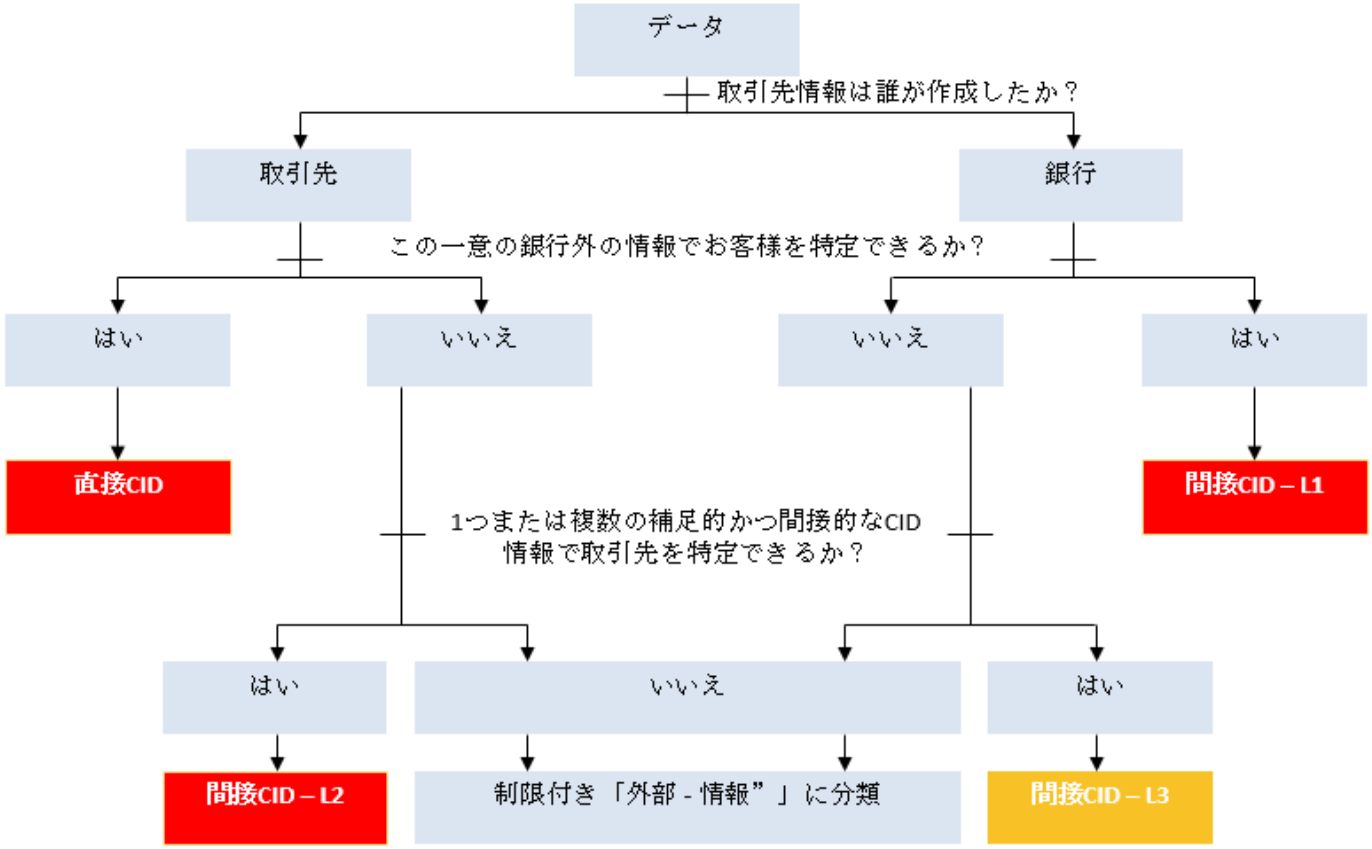
   (DCID) = 銀行秘密違反

2. コンテナ ID

   (L1 ICID) = 銀行秘密違反

3. 富の状況 + 国籍

(L2 ICID) + (L2 ICID) = 銀行秘密違反


データ
取引先情報は誰が作成したか？
取引先
銀行
この一意の銀行外の情報でお客様を特定できるか？
はい
いいえ
いいえ
はい
直接CID
間接CID – L1
1つまたは複数の補足的かつ間接的なCID
情報で取引先を特定できるか？
はい
いいえ
はい
間接CID – L2
制限付き「外部 - 情報”」に分類
間接CID – L3

付属書 E：Barclays 情報ラベリングスキーム

表 E1： Barclays 情報ラベリングスキーム

** 銀行秘密ラベルは銀行秘密法域に特有のものです。

ラベル	定義	例
銀行秘密	スイス、直接または間接取引先特定データ（CID）に関係する情報。「銀行秘密」分類は、直接または間接取引先特定データに関係する情報に適用されます。そのため、所有する法域にある場合でも全社員によるアクセスは不適切なものとなります。 この情報へのアクセスは、自らの正式な職務または契約上の責任を果たすために知る必要がある者のみに限定されます。 そのような情報実体の社内、社外での不正開示やアクセスまたは共有は、それが社内および社外で不正な人員により開示された場合、重大な影響を及ぼすことがあり、刑事訴訟に至ることもあり、罰金や銀行業ライセンスの喪失などの民事および行政上の結果を招くことがあります。	• 取引先名 • 取引先住所 • 署名 • 取引先の IP アドレス（詳細は付属書 D に記載）

ラベル	定義	例
秘密	情報は、エンタープライズリスク管理枠組み（ERMF）の下で「最重要」と評価され（財務または非財務）、その不正な開示が	• 吸収合併または買収可能性の情報。 • 戦略的な計画情報 – ビジネスと組織。 • 特定の情報セキュリティの設定に関する情報。

	Barclays にマイナスの影響を及ぼす場合、秘密として分類されるものとします。 この情報は特定の対象者に制限され、作成者の許可なしにさらに配布してはなりません。対象者には情報所有者の明示的な許可を受けた社外の受取人が含まれる場合があります。	• 特定の監査所見およびレポート。 • 執行委員会議事録。 • 認証または本人確認および検証（ID&V）詳細– 顧客/取引先および社員。 • 大量のカードホルダー情報。 • 利益予測または年度決算結果（一般公開前）。 • 正式な機密保持契約（NDA）で対象となっている項目。
社内秘	想定されている受取人が Barclays の認証された社員および有効な契約を締結しており、特定の対象者に限定されている Barclays マネージドサービスプロバイダー（MSP）のみである場合、情報は社内秘として分類されるものとします。 エンタープライズリスク管理枠組み（ERMF）の下で「重要」または「限定」と評価される情報（財務または非財務）は、不正に開示された場合 Barclays にマイナスの影響を及ぼす場合があります。 この情報は一般的な配布を意図していませんが、知る必要の原則に従って受取人は転送または共有することができます。	• 戦略および予算。 • 成績評価。 • スタッフの報酬および個人情報。 • 脆弱性評価。 • 監査所見およびレポート。
社外秘	想定されている受取人が Barclays の認定社員および有効な契約下にある Barclays マネージドサービスプロバイダー（MSP）であり、情報が特定の対象者または情報所有者が許可している外部関係者に制限されている場合、情報は社外秘として分類される必要があります。	• 新製品計画。 • 取引先契約書。 • 法的契約書。 • 社外への送付が意図される個々の/低量の顧客/取引先情報。

	エンタープライズリスク管理枠組み（ERMF）の下で「重要」または「限定」と評価される情報（財務または非財務）は、不正に開示された場合 Barclays にマイナスの影響を及ぼす場合があります。 この情報は一般的な配布を意図していませんが、知る必要の原則に従って受取人は転送または共有することができます。	• 顧客/取引先への通信。 • 資料を提供する新しい発行物（例えば、目論見書、公募メモ）。 • 最終検索文書。 • Barclays 外の重大な非公開情報（MNPI）。 • 全調査報告書 • 特定のマーケティング資料。 • 市場解説。
制限なし	一般配布が意図されているか、あるいは配布された場合に組織に影響を及ぼさない情報。	• マーケティング資料。 • 出版物。 • 公示。 • 求人広告。 • Barclays に影響を及ぼさない情報。

表 E2： 情報ラベリングスキーム– 取り扱い要件

** 規制要件通りに機密性を確保するための CID データの特定取り扱い要件

ライフサイクル段階	銀行秘密要件
作成と **ラベル付け**	「社外秘」による、および • 資産には CID 所有者を割り当てることが必須。

保存	「社外秘」による、および • 資産は、特定のビジネスニーズ、規制当局または社外監査人による明示的な要請がない限り、リムーバブルメディアのみに保存する必要があります。 • 大量の銀行秘密情報資産はポータブルデバイス/メディア上に保存してはなりません。 詳しい情報は、サイバーおよび情報セキュリティチーム（以下 CIS という）にお問い合わせください。 • 資産（物理的または電子的）は、知る必要または所有する必要の原則に従い、許可を受けない人物が表示またはアクセスできる場所に保管してはなりません。 • 資産（物理的または電子的）の保管のため、クリアデスクおよびデスクトップのロックなどの安全な職場慣行に従う必要があります。 • リムーバブルメディア上の情報資産は、それが明示的に必要とされる限りにおいて保管のために使用され、使用中でないときにはロックして保存します。 • アドホックデータのポータブルデバイス/メディアへの転送には、データ所有者、コンプライアンスおよび CIS の承認が必要です。
アクセスおよび使用	「社外秘」による、および • 資産は、CID 所有者（または代理人）からの正式な許可なしにオフサイト（Barclays の施設）で削除/閲覧されることがあってはなりません。 • 資産は、CID 所有者（または代理人）および取引先からの正式な許可なしに（権利放棄/限られた委任権）、取引先の記帳法域外で削除/閲覧されてはなりません。 • 物理的資産を現場外に持ち出す際には、ショルダーサーフィンが可能とならないよう、安全なリモート業務慣行に従う必要があります。
	• 不正な人物が、ビジネスアプリケーションへの制限されたアクセスの使用を通じて CID を含む電子資産を観察したり、またはこれにアクセスできないよう徹底します。
共有	「社外秘」による、および • 資産は「知る必要の原則」に従ってのみ配布され、かつ発信元の銀行秘密法域の情報システムおよび社員の範囲内とする必要があります。 • リムーバブルメディアを使用してアドホックベースで転送される資産については、情報資産所有者と CIS の承認が必要です。

	• 電子的通信は転送中は暗号化されるものとします。 • 郵便により送付される資産（紙印刷されたもの）は、受領確認を必要とするサービスを使って配達されるものとします。 • 資産は、「知る必要の原則」に従ってのみ配布するものとします。
アーカイブと処分	「社外秘」による

*** システムセキュリティ設定情報、監査所見、および個人情報は、無許可の開示がビジネスに及ぼす影響により、社内秘または秘密のいずれかに分類される場合があります

ライフサイクル段階	社内秘	社外秘	秘密
作成および導入	• 資産には情報資産所有者を割り当てることが必須。	• 資産には情報資産所有者を割り当てることが必須。	• 資産には情報資産所有者を割り当てることが必須。

保存	• 資産（物理または電子）は、公共エリア（訪問者が監視されずにアクセスすることが可能なサプライヤー施設内の公共エリアを含む）に保管してはなりません。 • 情報は、訪問者が監視されることなくアクセスが可能な施設内の公共エリアに放置してはなりません。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所に保管してはなりません。 • 保管中の電子資産は、許可を受けない人物がアクセスできる重大なリスクがある場合は、暗号化または適切な補償管理によって保護することが必須です。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所に保管してはなりません。 • 保管中の電子資産は、許可を受けない人物がアクセスできる重大なリスクがある場合は、暗号化または適切な補償管理によって保護することが必須です。 • Barclays のデータ、アイデンティティ、および/または名声を保護するために使用されるすべてのプライベート鍵は、FIPS 140-2 レベル 3 以上の証明書付きハードウェアセキュリティモジュール（HSM）により保護されるものとします。
アクセスおよび使用	• 資産（物理または電子）は、施設外の公共エリアに放置してはなりません。 • 資産（物理または電子）は、訪問者が監視されることなくアクセスが可能な施設内の公共エリアに放置してはなりません。 • 電子資産は、必要に応じ、適切な論理的アクセス管理により保護するものとします。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所で作業したり、無人状態で放置してはなりません。資産は、適切な管理が確立されている場合のみ作業可能です（覗き見防止フィルムなど）。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所で作業したり、無人状態で放置してはなりません。資産は、適切な管理が確立されている場合のみ作業可能です（覗き見防止フィルムなど）。

		• 印刷された資産は、速やかにプリンターから回収するものとします。それが不可能な場合は、印刷セキュリティツールを使用するものとします。 • 電子資産は、適切な論理的アクセス管理により保護するものとします。	• 印刷される資産は、印刷セキュリティツールを使用して印刷するものとします。 • 電子資産は、適切な論理的アクセス管理により保護するものとします。
共有	• 紙印刷された資産には、明確な情報ラベルを貼るものとします。 ラベルは、最低でもタイトルページに貼るものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。	• 紙印刷された資産には、明確な情報ラベルを貼るものとします。 ラベルは、最低でもタイトルページに貼るものとします。 • 紙印刷された資産が入っている封筒には、表面に明確な情報ラベルを貼るものとします • 電子資産には、明確な情報ラベルを付けるものとします。 複数ページの電子文書のコピーには、全ページに明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。	• 紙印刷された資産には、全ページに明確な情報ラベルを付けるものとします。 • 紙印刷された資産が入っている封筒には、表面に明確な情報ラベルを貼り、開封明示シールを貼るものとします。 それらは配布前に、ラベルのない別の封筒に入れるものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。 複数ページの電子文書のコピーには、全ページに明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。

		• 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。 • 資産は、それを受け取るためのビジネス上のニーズがある人員のみに配布するものとします。 • 資産は、受信者がその資産をすぐに回収できることを送信者が確認していない限り、ファックスで送信してはなりません。 • 電子資産を社内ネットワーク外に転送する場合は、承認済みの暗号保護メカニズムを使用して暗号化するものとします。	• 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。 • 資産は、情報資産の所有者により受信を個別に許可された人員のみに配布するものとします。 • 資産はファックスで送信してはなりません。 • 電子資産を社内ネットワーク外に転送する場合は、承認済みの暗号保護メカニズムを使用して暗号化するものとします。 • 電子資産の流通管理を維持するものとします。
アーカイブ化と処分	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。 • 秘密電子資産が保存されていたメディアは、処分の前または処分中に、適切に機密情報を分離するものとします。