外部サプライヤー管理義務

情報とサイバーセキュリティ(ICS)

2020 年 10 月付け第 10.0 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、情報とサイバーセキュリティのガバナンスのための確立され一貫した業界標準のセキュリティフレームワークを備え、人々、プロセス、技術環境、情報/サイバーセキュリティ管理の状況を理解し、主要な業界標準（NIST、ISO/IEC 27001 など）または適用される業界要件に従って、サイバー攻撃の脅威からサプライヤーを保護するセキュリティプログラムを設けるものとします。 セキュリティガバナンスフレームワークとは、資産とデータを紛失、悪用、不正アクセス、開示、改ざん、破壊から保護するための事務的、技術的、物理的な保護手段を含むものであり、これは策定、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、情報とサイバーセキュリティの方針、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と経営陣の監督下にある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、適切な情報セキュリティとサイバーセキュリティの方針と手順。 • 情報とサイバーセキュリティの方針と手順/基準を定期的に（年 1 回以上、または重大な変更があった場合）見直すものとします。 • サプライヤーは、重要なビジネス環境、情報、システムを適切に備え、それを有能な個人に割り当てることで、情報とシステムに対して社員がそれぞれが責任を負っていることを確認するものとします。 • 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。 • 少なくとも年に 1 度、独自に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。**	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。

2.情報/サイバーセキュリティリスク管理	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情報とサイバーセキュリティの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。 • リスク評価の結果には、セキュリティポリシー、常に最新の手順、基準、管理を含め、必要に応じてそれらが適切かつ有効であるとともに、業界のベストプラクティスに沿ったものが必要です。 • リスク評価の結果を考慮し、情報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。 • 情報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。 • サプライヤーは、リスクに優先順位を付け対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、アクセス、紛失、破壊、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、情報/サイバー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	文書化された方針および標準はリスク管理とガバナンスのために必須の要素です。これらは、情報/サイバーリスク管理に必要な管理に対する経営陣の見解を定めます。 この原則が履行されない場合、Barclays の情報が不当に公開され、および/またはサービスの損失が発生する可能性があり、法律上および規制上の制裁、または、名声の毀損を招く場合があります。

	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 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、Barclays に通知するものとします。**	
3.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 • 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う際の責任、および • データ漏えい経路のアウトプット。 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。	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。
4.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、適切な啓発訓練を受け、組織の手順、プロセス、およびポリシーについての最新情報を定期的に取得するものとします。トレーニングおよび意識時向上のレベルは、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、すべての社員に対し、サイバーセキュリティのベストプラクティスおよび Barclays データの保護を	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。

	含むセキュリティ情報に関する必須のトレーニングを入社後 1 ヶ月以内に受講させ、少なくとも年に 1 度は更新していることを確認するものとします。必要に応じて、以下の内容を含む必要があります。 システムへの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ハイリスクグループ（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。	
5.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ーインシデントを効果的に検証し、インシデントを封じ込め・除去・低減するサイバーセキュリティーインシデント管理の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、社員の役割およびインシデントへの対処/管理のフェーズを定義した、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と。 • インシデントの分類 - 迅速なインシデント対応措置を取ることができるよう、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。 • インシデント封じ込め - 人、プロセス、テクノロジーの能力を活用し、環境内のセキュリティーインシデントを迅速かつ効果的に封じ込める。 • 脅威の除去/緩和 - 人、プロセス、テクノロジーの能力を活用し、セキュリティ上の脅威およびその構成要素を環境から迅速かつ効果的に除去/低減する。 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。 • テストには、適切な人員に連絡を取ることができることを証明することによる Barclays への通知能力の検証を含むものとします。 • 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	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。

	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、電話番号以下を含めるものとします。** サプライヤーは、Barclays へのサービスまたは Barclays の情報/データに影響を与えるインシデントが発生した場合、インシデントが発覚してから合理的な時間内に、またいかなる場合でもサプライヤーが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場合、またはデータ侵害の発生が発覚した場合、ベンダーは、影響を受ける国のデータ保護要件に従い、かかるインシデントがあった旨を Barclays に通知するものとします。 サプライヤーは、Barclays に提供するサービスまたは Barclays の情報・データに影響を与えるインシデントについて、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： • 日付と時刻 • 発生場所 • インシデントの種類 • 影響 • 現在の状況 • 影響の低減または対応措置 これらのインシデントは、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。	
6.情報分類と保護	サプライヤーは、以下を含む、確立された適切な情報分類および取り扱いのフレームワークまたはプログラム（業界の最良慣行および/または Barclays 要件に従う）を備えている必要があります。 • 正しい情報ラベルスキームの割り当て。 • 割り当てられた分類レベルに従った、情報の安全な取り扱い。 • すべてのスタッフが、サプライヤー/Barclays のラベリングと取り扱い要件、および正確な情報分類を正しく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	Barclays の秘密情報が、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ければ、

	その代わりとなるスキームを参照し、保持または処理された 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。	Barclays の秘密情報が、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、法制上の制裁、名声の毀損、または、ビジネスの遺失/損壊を招く場合があります。
7.資産管理（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（サプライヤーまたはベンダーの下請業者の敷地内で運用される、または Barclays が提供する Barclays 機器を含む）の完全かつ正確な目録を保管し、情報資産の目録が最新、完全、正確であることを確認するため、少なくとも年に 1 度のテストを実施するものとします。 資産管理プロセスは、以下の条件を満たす必要があります。 • 情報資産とインフラが分類、重要度、事業運営上の価値に基づいて保護される。 • 将来的に情報を保存または処理できるよう、すべての技術資産の正確かつ最新の目録を管理する。目録には、会社のネットワークに接続されているかどうかを問わず、すべての資産を含むものとします（Barclays のサービスに固有）。 • **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（デスクトップ、ラップトップ、ネットワーク機器、RSA トークン、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。** • 不正な資産がネットワークから削除されるか、隔離されるか、インベントリが適時に更新される。 • 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。 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	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。

	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実施するものとします。	
8.物理的および論理的情報の破壊/削除/処分	物理的または電子的形態で保管された Barclays の情報資産は、廃棄または削除される際には、Barclays のデータが確実に復元不可能となるよう、その関連リスクに適切な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、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 データを安全に消去し完全に除去するため、事業プロセスと技術的手段を含む方針と手順を構築するものとします。	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。
9.境界とネットワークセキュリティ	サプライヤーは、Barclays へのサポートサービスを提供するサプライヤーまたはその下請業者が運営するすべての IT システムがサプライヤー（および関連する下請業者）のネットワーク内の脅威の水平展開から保護されるよう徹底するものとします。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検出、予防、修正するものとします。 ネットワーク整合性メカニズムは、以下の条件を満たす必要があります。 • 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、または何らかの事案によって変更を余儀なくされる要件がある場合に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。 • インターネットへの、またはインターネットからのすべてのネットワークトラフィックが、不正な接続をフィ	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。

	ルタリングするよう設定された、認証済みのアプリケーション層のプロキシを通過する。 • 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 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。*	
10.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。	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。
11.リモートアクセス	Barclays の Citrix アプリケーションを介した Barclays ネットワークへのリモートアクセス、および/またはサプライヤーが管理する環境内に存在/格納されている Barclays のデータは、デフォルトでは提供されません。また、未認証の場所/外出先/自宅から接続されることはありません。リモートアクセスはすべて、Barclays（最高セキュリティ・オフィス:ECAM チーム）によって承認・認証される必要があります。 サプライヤーは、リモートアクセスのために以下の項目が確立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	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。

<table>
<tr>
<td></td>
<td>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。
• 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、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。
• 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設定されていることを確認する必要があります（パッチレベル、マルウェア対策の状態など）。
• 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（サプライヤーのスタッフ、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）内に存在/格納されている BarclaysBarclays のデータへのアクセスを許可してはなりません。

注意: Barclays のネットワークおよび Barclays のデータへのリモートアクセスは、Barclays が特別に承認・認証した場合を除き、許可されません。</td>
<td></td>
</tr>
<tr>
<td>12.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、セキュリティ機器、サーバーなどの主要な IT システムが主要イベントを記録するよう設定されていることを確認する、監査およびログ管理のための確立された、根拠のあるフレームワークを確実に備えている必要があります。また、ログは集中化し、適切にセキュリティ管理し、少なくとも 12 か月間サプライヤーにより保持されるものとします。
<table>
<tr><th>分類</th><th>影響の少ないシステム/</th><th>影響が中程度のシステム/</th><th>影響の大きいシステム/サービス</th></tr>
</table>
</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>

	サービス	サービス	
ログの保管	3ヶ月	6ヶ月	12ヶ月

セキュリティログの管理プロセスは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:
    - 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。
- イベント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、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。	
13.マルウェア対策	サプライヤーは、組織が所有または管理するユーザーのエンドポイントデバイス（提供されたワークステーション、ラップトップ、およびモバイルデバイスなど）や IT 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でのマルウェアの実行を阻止するための方針と手順を確立し、サポートする業務プロセスと技術的な対策を実行するものとします。 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。 • マルウェア対策ソフトウェアを集中管理し、組織の各ワークステーションとサーバーを継続的に監視し、防御する。 • 組織のマルウェア対策ソフトウェアにより、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。 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。
14.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、業界標準（NIST、SANS、CIS など）に従って安全に構成されていることを確認するものとします。 構成標準プロセスは、以下の条件を満たすものとします。 • 認可されたすべてのネットワーク機器とオペレーティングシステムのセキュリティ構成標準のための方	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。 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

	針、手順、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限制御の概念や、不正なソフトウェアを使用しないことなど）に従って機能するよう構成されている。 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。	保護を確実にする上で役立ちます。
15.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 のデータアクセス/処理に使用されるエンドポイントには、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。 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。- • 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、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 データの共有/転送は、インスタントメッセンジャー/ソフトウェアを使用して無効にするものとします。	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。

	• 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。 Barclays のサービスで使用されているモバイルデバイス 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たり、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）。 4. すべてのクラウドベースのサービスは、サプライヤーが提供するモバイルデバイス上でデフォルトで許可されないようにする必要があります。	

16.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）
	• 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（下請業者）との安全でない情報交換。
		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

	• 情報の不適切な印刷または複写。	危険にさらされる可能性があり、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。
17.データ保護	サプライヤーは、Barclays のデータが、暗号化、完全な保護、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保護されていることを確認するものとします。Barclays のデータへのアクセスを制限するために、適切に配慮することが重要です。 データ保護管理は、以下の条件を満たす必要があります。 1. 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と技術的施策を実施する。 2. サプライヤーが保存、処理、または送信したすべての機密情報（Barclays のデータ）の目録を保持する。 3. 機密情報（Barclays のデータ）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。 4. 組織内のすべてのデータがデータ分類基準に基づいて識別表示されていることを確認する。 5. データ利用方針 - データへのアクセス 6. 保存データの保護 a. 不正アクセスによる機密情報の悪用を防ぐため、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 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・レイヤー・セキュリティ (TLS) • 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。	
18.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のセキュリティは、以下の条件を満たす必要があります。 • 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、業界の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。	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。

	• システムがセキュア開発のベストプラクティス（OWASP など）に沿って開発される。 • 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、主要な業界標準（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。	
19.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。	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。 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ければ、Barclays の秘密情報が、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、法制上

	アクセス管理プロセスは、業界の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。 • 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。 • 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。 • 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 • 停止/無効化するものとします。 • 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 の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、アクセス試行が最高で 5 回連続で失敗した場合、無効にすることが必要で	の制裁、名声の毀損、または、ビジネスの遺失/損壊を招く場合があります。

	す。	
20.脆弱性管理	サプライヤーは、組織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適時に検出するための方針と手順を確立し、それを支えるプロセスと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、以下の条件を満たす必要があります。 • 組織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タイムリーに検出するために、方針と手順を確立し、それを支えるプロセスと技術的手段を実施して、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。 • 役割と責任の定義。 • 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。 • 脆弱性調査を日常的に実施し、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。 • 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。	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、Barclays およびサプライヤーに対しサイバー攻撃を行う場合があります。
21.パッチ管理	サプライヤーは、管理されたユーザーのエンドポイントデバイス（発行されたワークステーション、ラップトップ、モバイルデバイスなど）と IT 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にセキュリティパッチを展開するために、方針と手順を確立し、それを支えるビジネスプロセスと技術的な対策を実行するものとしま	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

	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。 • サプライヤーは、パッチが本番環境と DR 環境に反映されていることを確認するものとします。	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。
22.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	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、業界の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。	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、法律上および規制上の制裁、または、名声の毀損を招く場合があります。
23.暗号	• 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	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の発生を招く可能性がありま

	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ことを確認するものとします。 o 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の要件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。 o 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。 o 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。 o 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。 o HSM の保護に必要でない限り、暗号化処理の期間後、ホストメモリで消去される。 • 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。 o HSM が義務化されている規制サービスのキー。 o 公的な認証局が Barclays を代表する証明書。 o 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 o 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	す。

	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。 • 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。 o IT サポートチーム o 関連の資産 o 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。 o 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。 o 強力なアルゴリズムとキー長さにより、高度な処理能力を持つハッカーによって機密データが失われたり、危殆化したりするリスクを最小限に抑えることができます。 o デプロイされた暗号の強度は運用やパフォーマンスに影響を及ぼす可能性があるため、リスクに見合ったものである必要があります。	
24.クラウドコンピューティング	サプライヤーは、クラウド技術のすべての使用が適切なセキュリティ管理下に置かれていることを確認し適切なセキュリティ管理が実施されていることを確認するため、それを支える事業プロセスと技術的な対策を実施していることを証明するために ISO/IEC27017 または 27001、SOC1 または 2 の認証を取得するものとします。 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 Barclays のデータは、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。 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。 • ID・アクセス管理/アクセス制御 • ネットワーク接続性 • データ保護 (転送/休止/保存) • セキュリティロギングと監視 • 暗号化とキー管理 • アプリケーションとインターフェースのセキュリティ • インフラストラクチャと仮想化のセキュリティ • サービスの分離	この管理が実施されない場合、保護が不適切な Barclays のデータは危害を受ける可能性があり、法律上および規制上の制裁、または、Barclays に対する風評被害を招くおそれがあります。
25.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	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の発生を招く可能性があります。

	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。	
25.1 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。	
25.2 BDS - 物理的アクセス管理	• 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。 • 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: ○ 常時見ることができる写真付き ID バッジ ○ 近接カードリーダーを配置 ○ 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。	
25.3 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。
25.4 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。 セクション 11「リモートアクセスのセキュリティ」を参照してください。
25.5 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。
25.6 BDS - ネットワークセキュリティ	• 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。 　　○ 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。 セクション 9「境界とネットワークセキュリティ」を参照してください。
25.7 BDS – 無線ネットワーク	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。
25.8 BDS - エンドポイント	BDS 内のコンピューター用に、安全なデスクトップビルドを、「業界ベストプラクティス」に設定しなければなりません

セキュリティ	BDS エンドポイント機器のセキュリティビルドには以下が必要です。 • ディスクの暗号化、 • 他のアクティブなデバイスからの起動を無効にする • 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 データの共有/転送は、インスタントメッセンジャー/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 セクション 15「エンドポイントセキュリティ管理」を参照してください。	

25.9 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。	

25.10 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	これが合意されない場合、サプライヤーはこ

	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。 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。	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。

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。
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。
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。または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	2 つ以上の異なる認証技術を使用した認証。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。
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。
共有アカウント	アクセスするシステムの性質上、許可されたアクセス権を持つが、個人アカウントのオプションは付与されない、複数の社員、コンサルタント、請負業者または派遣社員に付与されるアカウント。
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、別の選択肢を選択する前に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	セキュリティーインシデントとは、明示的または暗示的なセキュリティポリシーに違反する事象と定義されます。 • （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	• 資産には情報所有者を割り当てることが必須。	• 資産には情報所有者を割り当てることが必須。	• 資産には情報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。 • 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	• 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	• 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。	せん。	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	• 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	• 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。

	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。	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、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。 • 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。	• 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。

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、お客様識別データ（以下 CID という）の取り扱いの役割と責任を定義し、伝達するものとします。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 の役割と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、文書化された管理およびプロセス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。 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有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

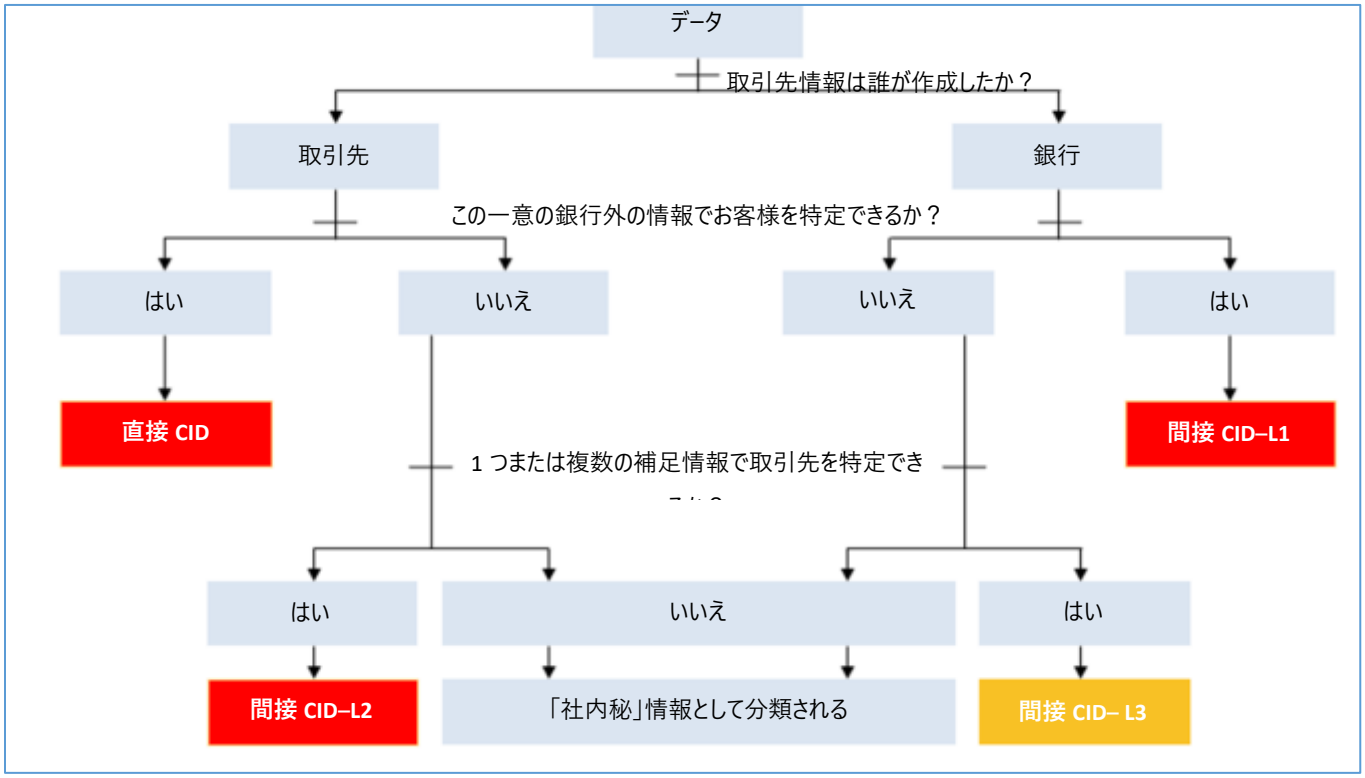
   (DCID) = 銀行秘密違反

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



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 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。	• 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。

	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。	• 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。 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	• 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。 • 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

	「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。	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 **ラベリング**	「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	• 資産には情報所有者を割り当てることが必須。	• 資産には情報所有者を割り当てることが必須。	• 資産には情報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）。 • 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。	• 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。
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	• 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	• 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。

	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。	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。	• 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。	• 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。	• 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。 • 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。