サプライヤー管理義務(SCO)

情報とサイバーセキュリティ(ICS)

2023 年 9 月付け第 13.0 版

管理エリア/対象	管理内容	本件が重要である理由
1.許可される使用	サプライヤーは、情報やその他の関連資産が適切に保護、使用、処理されるようにする必要があります。 情報やその他の関連資産を処理する際の許容される使用と手順に関する規則は、識別され、文書化され、実施されるものとします。 組織の情報やその他の関連資産を使用またはアクセスする責任を負う、請負業者、下請業者、復処理者を含むサプライヤーの従業員は、組織の情報やその他の関連資産を保護および処理するための情報セキュリティ要件を認識しておく必要があります。情報処理施設の使用についても、責任を負う必要があります。組織は、情報やその他の関連資産の許容される使用についてトピック固有の方針を確立し、情報やその他の関連資産を使用または処理するすべての人にそれを伝える必要があります。 サプライヤーは、許容される使用要件に確実に適合するための適切な手順を講じるものとします。 以下の内容を考慮する場合があります。 • 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。 • バークレイズ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	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。

	• 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。	
2.境界とネットワークセキュリティ	サプライヤーは、サプライヤーおよび/またはその下請業者/復処理者が運用し、Barclaysへのサービスをサポートするすべてのシステムおよびアプリケーションが、インバウンドおよびアウトバウンドのネットワーク上の脅威から保護されていることを確認する必要があります。ネットワーク内の情報セキュリティを確保し、接続されたサービスを不正アクセスから確実に保護するための制御を実装する必要があります。サプライヤーはセキュリティ上の警告や侵害を特定し、保護し、検出し、対応するものとします。 ネットワークセキュリティ管理は、ネットワーク内の情報およびそれをサポートする情報処理施設の保護を確保するものであり、以下の領域（ただし、これらに限定されない）を含むものとします。 • 組織のネットワーク境界のすべてについて最新の目録を維持し（ネットワークアーキテクチャ/ダイアグラムを介して）、当該目録を少なくとも年に1回見直す必要がある。 • 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、接続が確立される前に検証および承認を受ける。 • サプライヤーネットワークを、多層防御の原則（ネットワークのセグメント化、ファイアウォールなど）を適用することで保護する必要がある。 • サプライヤーは、すべてのインバウンド/アウトバウンドトラフィックの悪意のあるトラフィックを検出および阻止し、業界のベストプラクティスに従ってシグネチャデータベースを更新し、かつソリューションプロバイダーからの更新を適時に適用することができる、ネットワーク侵入防止技術を備える必要がある。 • サプライヤーは、仮想プライベートクラウド（VPC）とサードパーティのオンプレミスネットワーク間のプライベート接続が暗号化され、トラフィックがパブリックインターネットにさらされないようにする必要がある。 • 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。 • デバイス管理ポート/インターフェースをユーザーLAN/トラフィックから論理的に分離し、適切な認証制御を行う。 • 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。	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。

	• SIEM を用いるなどの疑わしい活動の検出と警告（動作とセキュリティ侵害のトリガーのインジケータを使用）を含むロギングと監視を確実に行う。 • 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、ファイアウォールルール（外部ファイアウォールと内部ファイアウォール）を確認し、少なくとも年に 1 回見直す必要がある。 • サプライヤーは、適切なネットワークアクセス制御を通じた内部ネットワークへのアクセスの監視を確認する必要がある。 • 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、および強力な暗号化プロトコルの下に置く。 • サプライヤーは、Barclays へのサービスのためのものとは（論理的に）別のネットワークを持っている必要がある。 サプライヤーは、バークレイズにサービスを提供するために使用するサーバーおよびアプリケーション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、運営管理の範囲を超えるもの）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、復処理者を含む）は、ネットワークセキュリティ管理に関する業界のベストプラクティスの認証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 • バークレイズの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/ラストワンマイル終端ルーターは、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。 　○ SIEM を用いるなどの疑わしい活動の検出と警告（動作とセキュリティ侵害のトリガーのインジケータを使用）を含むロギングと監視を確実に行う。	

	サードパーティプロバイダーは、サービスを提供するシステムおよびアプリケーションのうちバークレイズがハイリスクと考えるもの、ならびにバークレイズがサプライヤーにハイリスクと伝えたものについて、ネットワークを分割しなければならないことを確認するものとします。業務アプリケーションとそのコア基盤となるインフラストラクチャコンポーネント（共有・一般的重要インフラストラクチャを除く）を、以下の原則を満たすために、承認されたバークレイズのセキュリテ技術（ファイアウォールまたはその他の同等の技術）を利用して独自のネットワークセグメントに分割するものです。 i. リスクのエクスポージャーを制限し、ネットワーク全体の横方向の移動を抑制して、ネットワークのブロードキャストに関わるリスクを軽減するには、セグメント化による方法を採用する必要があります。リスクを合理的にできるだけ制限するには、アプリケーションを独立したセグメントに展開する必要があります。例：即時送金ゾーン。 業務アプリケーションに関連するすべてのインフラストラクチャとデータは、独立したセキュアなアプリケーションゾーンに展開し（可能な場合）、CSO が承認した実施技術（ネットワークファイアウォール、承認されたセグメンテーションソリューションなど）を使用してバークレイズの内部ネットワークから分離する必要があります。 注 - 一部のシナリオでは、アプリケーションやデータベースなどのコンポーネントを複数のゾーンに分割しなければならない場合があります（例：共有プラットフォームを利用する場合など）。各アプリケーションは、CSO、セキュリティコンサルタントとともに定義し、合意した最も適切な方法を用いて、個別に評価する必要があります。 ii. サービスは物理的または論理的に分離されている必要があります。基盤となるネットワークファブリック（ケーブル配線/スイッチなど）は、他のアプリケーションやサービスと共有できます。つまり、セグメントは論理的に定義できますが、バークレイズのネットワークにある他の部分から物理的に分離してセグメント化を実行する必要はありません。 iii. アプリケーションゾーンは、サービスの運用に必要なトラフィックフロー、ならびに承認された管理、監視およびセキュリティツールに基づいて、他のゾーン（CIPE を用いた内部ネットワークを含む）との間のトラフィックフローを制限する必要があります。設定では、許可された通信経路に特定のポート、プロトコルおよび IP アドレスを規定し、その他の通信はすべてデフォルトで制限す	

	る必要があります。レンジを含むルールは回避すべきであり、例外的な場合に限り、最小限の接続要件のみが有効になるように承認する必要があります。 iv. コンテナは強力な論理制御によって確実に分離し、コンテナ間の横方向の移動を阻止して分離を実施する必要があります。1 つのコンテナが侵害されても、同じホスト/クラスター上で実行されている他のコンテナが侵害されないようにする必要があります。 v. すべてのセグメント化の実装において、ポリシーの遵守を検証し報告する能力を備えた（またはこれらが組み込まれた）ポリシーの集中管理機能を提供し（ファイアウォールのコンプライアンス文書を参照）、監査が可能な変更ログを提供する必要があります。 vi. ステートフルインスペクション/管理は、可能/実行可能であれば運用する必要があります。 vii. セグメント化機能は、「フェールセーフ」機構を備えて運用する必要があります（例：機能に不具合が発生した場合でも、引き続き承認されたルールセットでトラフィックをブロック/許可できる必要がある）。 viii. アプリケーションゾーン上の本番システムと非本番システム間のトラフィックは、例外的にのみ許可され、ログに記録される必要があります。 **Barclays へのサービス提供に使用されるクラウドサービス利用者（サプライヤー）向けガイダンス** Barclays へのサービスを保護するため、クラウドサービス利用者（CSC）は、適切なネットワークセキュリティ管理の実行を確認する必要があります。 • クラウドサービス利用者（CSC）は、クラウドサービスの共有環境内でテナントを分離するためにネットワークを分離する要件を定義し、クラウドサービスプロバイダーがこれらの要件を満たしていることを確認する必要があります。 • クラウドサービス利用者がネットワークスサービスを利用する際のアクセス管理ポリシーでは、使用される各クラウドサービスへのユーザーアクセス要件を指定する必要があります。 *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 以外のネットワークを指します。*	
3.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る必要があります。	この原則が実行されない場合、バークレイズとサプライ

	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が、可用性を確保するための DDoS/DoS 攻撃に対する十分な保護体制を具備していることを確認する必要があります。 サプライヤーが**サービスを提供するシステムおよびアプリケーション**を運用してバークレイズのデータを保持している場合、または復旧力分類が 0 もしくは 1 のサービスの基盤となっている場合は、可用性を確保するための DoS に対する十分な保護体制を具備していることを確認する必要があります。	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。
4.在宅勤務（リモートアクセス）	サプライヤーは、従業員がリモートで勤務する際に情報のセキュリティを確保する必要があります。セキュリティ対策を実施して、リモート勤務の際に組織の敷地外でアクセス・処理される情報を保護する必要があります。サプライヤーは在宅勤務に関する指示をスタッフメンバーに提供する必要があります。 **Barclays のネットワークへのリモートアクセス** Barclays の Citrix アプリケーションを介した Barclays のネットワークへのリモートアクセスは、デフォルトでは設定されていません。未承認の場所/外出先/自宅からバークレイズのネットワークにアクセスまたはリモートアクセスを行うには、バークレイズ（最高セキュリティオフィスの ECAM チーム（externalcyberassurance@barclayscorp.com））から事前に承認および許可を受ける必要があります。 サプライヤーは、リモートアクセスのための以下の管理体制を確実に確立する必要があります。 • バークレイズのネットワークにアクセスするには、RSA トークン（ソフト）とサポートされているバージョンの Citrix Workspace アプリが必要です。詳細情報については、バークレイズが提供します。 • サプライヤーは、業務上の正当性を根拠に遠隔/ハイブリッドで業務を行うことを認められた従業員（下請業者/復処理者を含む）について、各従業員の最新かつ正確な記録を維持する必要があります。 • **サプライヤーは、四半期ごとにリモートアクセスを行うすべての従業員の整合を確認し、その結果を Barclays（最高セキュリティオフィスの ECAM チーム（externalcyberassurance@barclayscorp.com））に通知する必要があります。** • バークレイズは、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、**退場日/最終出勤日（LDIO）の 24 時間以内**に認証情報を無効化します。	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。

	• 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、バークレイズの情報システムに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（externalcyberassurance@barclayscorp.com））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（ノート PC/デスクトップ PC に限定）による、サプライヤーが管理する環境（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、下請業者/復処理者など）内に存在/格納されているバークレイズの環境および/またはバークレイズのデータへのアクセスを許可してはなりません。** 注：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。 **サプライヤーの環境/ネットワークへのリモートアクセス** サプライヤーの環境/ネットワーク内に存在/保存/処理されたバークレイズのデータを含む、サービス提供のためのサプライヤー管理環境へのリモートアクセス。 サプライヤーは、サプライヤー企業ネットワークのリモートアクセスのための以下の管理体制を確実に確立する必要があります。 • サプライヤーのネットワークへのリモートログインアクセスは、転送中のデータを強力に暗号化し、多要素認証を使用する必要があります。 • サプライヤーは、リモートアクセスに仮想デスクトップを使用できます。 • サプライヤーは、リモート/ハイブリッドで勤務する個人の記録を保持する必要があります。 • **サプライヤーは、サプライヤーのスケジュールどおりに、すべてのリモートユーザーの整合を確認する必要があります。** • サプライヤーは、アクセスが不要になった（従業員の雇用終了、プロジェクトの再配置など）認証情報を、**退場日/最終出勤日（LDIO）の 24 時間以内**に無効化します。	

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

個人所有のデバイス/BYOD（ノートPC/デスクトップPCに限定）による、サプライヤーが管理する環境（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/格納されているバークレイズのデータへのアクセスを許可してはなりません。

従業員には、すべきこととしてはならないことを含む、在宅勤務に関するサプライヤーからの規則を提供する必要があります。

通常の業務において、銀行専用スペースまたはサプライヤーの施設からサービスを提供することが契約上義務付けられている場合や、規制要件が適用される場合は、（在宅を含む）リモート勤務は禁止されています。ただし、バークレイズと合意した災害復旧/危機/パンデミックの対応の場合、また、契約上の合意の一部としてリモート勤務を余儀なくされるセキュリティ要件では、サードパーティの事業継続計画において規定が認められています。
</td>
<td></td>
</tr>
<tr>
<td>5.セキュリティログの管理</td>
<td>
サプライヤーは、十分に確立された、監査に対応できるログ管理フレームワークを有している必要があります。このフレームワークには、主要な IT システム（アプリケーション、ネットワーク機器、セキュリティデバイスおよび重要なイベントを記録するために設定されたサーバーなど）を含める必要があります。イベントの記録、証拠の生成、ログ情報の完全性の確保には、ログを改ざんができないようにし、不正アクセスの防止措置が取られ、情報セキュリティインシデントにつながる可能性のある情報セキュリティイベントを特定し、調査のサポートができるようにする必要があります。サプライヤーは、ログが一元管理され、改ざんおよび/または削除のリスクから適切に保護され、最低 12 ヵ月間、または規制要件のいずれか長い方の期間までサプライヤーによって保持されることを確実に実施する必要があります。
<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>
セキュリティログの管理フレームワークは、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。

</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>

	• 攻撃の監視、検出、把握、および/または攻撃からの復旧のため、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。 o 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 o 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 o 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） • 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）。 • 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。 • ログ分析では、情報セキュリティイベントの分析と解釈をカバーし、セキュリティ侵害の兆候を示す可能性がある、異常な活動や異常な動作を特定するのに役立てる。 • 記録される主要イベントには、バークレイズへのサービスの機密性、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が含まれていること。 • フレームワークが上記の要件を継続的に満たしていることを定期的にテストします。	

	Barclays へのサービス提供に使用されるクラウドサービス利用者（サプライヤー）向けガイダンス Barclays へのサービスを保護するため、クラウドサービス利用者（CSC）は、適切なセキュリティーログ管理制御の実装を確認する必要があります。 • クラウドサービス利用者は、イベントログの要件を定義して文書化し、クラウドサービスがこれらの要件を満たしていることを確認するものとします。 • 権限のある業務がクラウドサービス利用者に委任された場合は、それらの業務の運用と実績を記録するものとします。クラウドサービス利用者は、クラウドサービスプロバイダーが提供するロギング機能が適切かどうか、またはクラウドサービス利用者が追加のロギング機能を実装する必要があるかどうかを判断するものとします。 • クラウドサービス利用者は、クラウドサービスプロバイダーのシステムで使用されるクロック同期に関する情報提供を求めるものとします。 • クラウドサービス利用者は、クラウドサービスごとに利用が可能なサービス監視機能に関する情報提供をクラウドサービスプロバイダーに求めるものとします。	
6.マルウェア対策	サプライヤーは、業界のベストプラクティスに従い、マルウェアが実行されるのを IT 環境全体で防ぐための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。 マルウェア対策には以下が含まれるものとしますが、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がスキャンエンジンを更新していることを確認する。 • 定期的にシグネチャデータベースを更新する。 • 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、Barclays へのサービスに使用するモバイルデバイスをマルウェアや攻撃から保護するために、適切な管理を実施する。	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。

	• 電子メールゲートウェイは、添付ファイルや URL など、受信、送信、社内のすべての電子メール通信をスキャンして、悪意のあるコンテンツや有害なコンテンツの兆候を特定する。 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。	
8.エンドポイントセキュリティ	サプライヤーは、統合的エンドポイント管理手法を導入し、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および/または処理に使用されるエンドポイントに、あらゆる悪意ある攻撃に対する強固な防御策が設けられていることを確認する必要があります。 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ア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。 • ハードディスクの完全暗号化。 • 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。 • サプライヤーの従業員が、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、アンチウイルスなどの基本設定を変更することは許可されない。 • Barclays の情報/データを外部メディアへコピーするための USB 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にで更新を実施する。 • 印刷スプーラーサービスを無効にする。 • バークレイズのデータ侵害からデータを保護するためのデータ防止ツール。 • サプライヤーは、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 google ドライブ、Dropbox、iCloud など（ただし、これらに限定されない）の情報を保存できるサイトに Barclays のデータが流出することを防ぐ必要がある。 • インスタントメッセンジャー/ソフトウェアを使用した Barclays のデータの共有/転送を無効にする。 • 悪意のあるソフトウェアを含む不正なソフトウェアの存在および/または使用を検出、阻止、修正する。 • ロック画面のタイムアウト、TCP IP 接続の企業ネットワークのみへの制限、疑わしい動作を検出する Advanced EPS セキュリティエージェント。	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。

	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ー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、承認された画像またはテンプレートを使用して構成を行うものとします。 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、バークレイズのリレーションシップマネージャー/バークレイズの IT サポートチーム/ECAM チームに連絡する必要があります。 Mobile devices used for Barclays Services - • サプライヤーは、ライフサイクル全体を通じて、分類された Barclays の情報にアクセスし、および/または、当該情報を含むモバイルデバイスを安全に管理し運用するために、統合的エンドポイント管理（UEM）または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。 • サプライヤーは、デバイスに紛失、盗難、セキュリティー侵害が生じた場合に情報を保護することができるよう、必ずリモートロックやリモート消去の機能が搭載されたモバイルデバイスを所持および使用する必要があります。 • モバイルデバイスのデータに保存する、および/または、データ上で処理される Barclays のデータを暗号化します。 • サプライヤーは、モバイルデバイスがルート化されておらず、高強度の認証ポリシーが有効になっていることを確認する必要があります。	
9.データ漏えい防止	サプライヤーは、Barclays のデータを漏えい/流出から保護するために、マネジメントが承認した効果的なフレームワークを使用しなければならず、これにはデータ漏えい経路が含まれますが、これに限定されません。- • 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	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

	○ 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。 • 接続可能媒体（シリアル、USB など）でワイヤレス（Bluetooth、Wi-Fi など）を介したポータブルメディアへの情報の不正な転送。 • 第三者（下請業者、復処理者）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。 データ漏洩防止策は、バークレイズのデータ/情報を処理、保存、または送信するシステム、ネットワーク、その他の装置に適用する必要があります。	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、バークレイズの機密情報が、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。
10.データセキュリティ	サプライヤーは、暗号化、整合性保護、およびデータ損失防止の手法を組み合わせて、Barclays が保有する、および/または処理するデータを確実に保護する必要があります。Barclays のデータへのアクセスは、権限を持つ従業員のみが行えるものとし、コンタミネーション、アグリゲーション攻撃、推論攻撃、クラウドコンピューティング環境からの脅威を含むがこれに限定されないストレージ脅威から保護される必要があります。 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る。 2. ポリシー、プロセスおよび手順を確立し、業務プロセスならびに技術的な対策をサポートする。サービスを提供する地理的な場所（物理的および仮想的）に存在するデータのデータフローを文書化し、維持する。この文書には、データフローのアプリケーションおよびシステム構成要素に関する詳細説明を含める必要があります。 3. アプリケーションおよびシステム構成要素において、地理的な場所（物理的および仮想的な場所を含む）に存在する Barclays のデータのデータフローダイヤグラムを維持する。 4. サプライヤーが保存、処理、または送信したすべての Barclays の機微/機密情報について、目録を保持する。	

	5. すべての Barclays のデータが、マネジメントが承認した情報分類および保護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. 保存データの保護 a. Barclays の情報資産の露出を防ぐために、保存データを強力に暗号化する。 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. 使用中のデータの保護 a. 機密情報の悪用を防ぐため、アクセス管理機能によって機密情報処理の制御を徹底する。 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. 転送中のデータの保護 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. 転送中のデータの強力な暗号化は、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。 10. 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） 11. 本番環境・非本番環境に保存されているすべてのデータは、暗号化で保護する必要があります（コントロール 16「暗号化」を参照）。	
11.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 が使用するアプリケーション、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、サプライヤーは、セキュリティーをソフトウェア開発のライフサイクルに統合するためのセキュアなソフトウェア開発フレームワークを確立するものとします。サプライヤーは、Barclays にソフトウェアを提供する前に当該ソフトウェアの脆弱性をテストし、必要な修正を行う必要があります。 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。

	• 脆弱性やサービスの中断を防ぐために、マネジメントの承認を得て、業界のベストプラクティスに沿ったセキュアコーディング標準を確立し導入する。 • 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。 • 開発システムやテストシステムに同等の制御が備わっていない限り、機密情報を開発やテストのシステム環境にコピーしないこと。 • 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（個人情報を含む）が非本番環境で使用されていないことを確認する。 • 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。 • パブリックコードのリポジトリの使用を禁止する。 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実現可能でない場合は、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。	

	サプライヤーは、バークレイズのサービスで使用されるすべてのインターネット向けSaaS（サービスとしてのソフトウェア）ベースのアプリケーションソリューションに、従来の認証制御（ユーザー名/パスワード）に加えて、補足的なアクセス制御（認証制御）が備わっていることを確認する必要があります。 サプライヤーには以下の機能が必要ですが、これらに限定されるものではありません。 • 多要素認証（トークン、SMS など） • SSO（シングルサインオン） • IP アドレスベースのアクセス制御 サプライヤーの従業員、下請業者/復処理者/バークレイズの従業員/バークレイズのクライアントやお客様のために、補足的なアクセス制御を用意する必要があります。	
12.ローカルアクセスマネジメント（LAM）	情報資産（ソフトウェア、ハードウェア、データなど）へのアクセスは、最小限の権限の原則に従って、知る必要がある場合にのみ許可します。IT システム/情報資産の所有者は、システム/情報資産へのアクセス権を持つすべてのアカウントのリストを提供するとともに、アクセスプロファイルと職務分掌（SoD）ルールを含む、論理アクセスセキュリティモデルを定義する責任があります。 サプライヤーがホストするウェブアプリケーションはバークレイズ LAM オンボーディングの対象であり、これらについてはバークレイズ LAM 管理を実装する必要があります。 • **知る必要**ベースとは、従業員が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を意味します。例えば、従業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**の原則とは、従業員が自らの許可されている職務を遂行するために必要な最小限水準のアクセスのみを持つことを意味します。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。 • **職務分掌（SoD）**は、タスクを一個人では完了できないような方法で構成するアプローチであり、主に不正行為のリスクを軽減することを目的としています。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。 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。

	アクセス管理プロセスは、以下を要件とする、バークレイズグループの情報・サイバーセキュリティポリシーならびに ID およびアクセス管理（IAM）基準のとおり、業界のベストプラクティスに従って定義、文書化、施行されなければなりません。 • **バークレイズ LAM オンボーディング**：サプライヤーは、アクセス管理プロセスがバークレイズの集中 IAM ツールセットを活用して、LAM 管理が円滑に行われていることを確認する必要があります。IT システムを IAM ツールセットにオンボーディングするプロセスの一環として、IT システムアクセスコントロールリスト（ACL）を IAM チームに提出する必要があります。下流の LAM 管理を最も効果的に動作させるための最適なフィード頻度は毎日の自動フィードですが、最低限の要件としては、月次ベースで供給する必要があります。 • **参加者管理**：プロビジョニングの前に、すべてのアクセスが適切であり承認されている必要があります。 • **異動者管理**：すべてのアクセス権を異動日の前に確認し、保持、取り消し、有効化する必要のあるアクセス権を確認する必要があります。取り消しが確認されたアクセスは、異動日の前に削除する必要があります。 • **退職者管理**：バークレイズの情報リソースへのアクセスやバークレイズへのサービス提供に使用するすべてのアクセス権は、サプライヤーとの契約終了日に削除する必要があります。 • **アカウント所有権**：一意のアカウントは、そのアカウントを使用して行う活動に責任を負う 1 名の従業員に関連付けられている必要があります。アカウントの詳細とパスワードは、他の従業員と共有してはなりません。 • **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）必要があります。 • **アクセスの再認証**：アクセスが適切であることを確認にするために、すべてのアクセスを 12 ヵ月ごと（非特権アクセス）または 6 ヵ月ごと（特権アクセス）に確認する必要があります。 • **身元の検証（ID&V）**：アクセス管理プロセスに、検証を識別するための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。 • **認証**：論理アクセスが許可される前に、すべてのアカウントを認証する必要があります。アプリケーションおよび認証メカニズムでは、パスワードまたは PIN を表示してはなりません。適切なパスワードの長さと複雑さ、パスワードの履歴、パスワード変更の頻度、多要素認証、および安全な資格情報管理を整備する必要があります。	

	• **非個人資格情報**：非個人資格情報（パスワードや秘密情報など）は、適切な資格情報管理ツール（CyberArk など）にオンボーディングする必要があります。この方法が不可能な場合は、誰も使用できないように認証情報を安全に保護する必要があります。アカウントの使用を必要とする人がいる場合、アクセスは時間制限のある一時的なものとし、認証情報はその後にリセットする必要があります。 • **資格情報の管理**：個人アカウントのパスワードは、少なくとも 90 日ごとに変更する必要があります。特権アカウントとインタラクティブアカウントのパスワードは、誰もパスワードを知ることがないように、90 日ごとまたは誰かが使用するたびに変更する必要があります。また、パスワードが 50 文字以上の場合は、誰もパスワードを知ることがないように、365 日ごとまたは誰かが使用するたびに変更する必要があります。インタラクティブアカウントのパスワードは、過去の 12 個のパスワードとは異なるものにする必要があります。 • **時間制限のあるアクセス**：バークレイズのスタッフまたはバークレイズの非正規職員が使用する本番および災害復旧インフラへの個人特権アクセスは、適切な承認を得たうえ、時間制限を設けている必要があります。 • **特権的活動の監視**：特権的活動の監視を実施する必要があります。 Barclays へのサービス提供に使用されるクラウドサービス利用者（サプライヤー）向けガイダンス Barclays へのサービスを保護するため、クラウドサービス利用者（CSC）は、適切な論理アクセス管理の制御の実装を確認する必要があります。 • クラウドサービス利用者は、クラウドサービス利用者のクラウドサービス管理者について、特定されたリスクに応じたクラウドサービスの管理機能を認証するために十分な認証技術（多要素認証など）を使用するものとします。 • クラウドサービス利用者は、クラウドサービス内の情報へのアクセスを、そのアクセス制御ポリシーに従って制限できること、およびそのような制限が実現されていることを確認するものとします。これには、クラウドサービス、クラウドサービス機能、およびサービスの実施中に維持されるクラウドサービス利用者データへのアクセスの制限が含まれます。 • ユーティリティプログラムの使用が許可されている場合、クラウドサービス利用者は、クラウドコンピューティング環境で使用されるユーティリティプログラムを特定し、それらがクラウドサービスの管理を妨げないようにする必要があります。	

<table>
<tr>
<td>13.脆弱性管理</td>
<td>
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、開発したアプリケーション/コード、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て適時に検出、修正するためのプロセス/全社的措置、および技術的対策をサポートする効果的な脆弱性管理プログラムを、確立された方針と手順を通じて実施し、実装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必要があります。

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。

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。
サービスプロバイダーは、最新の脆弱性シグネチャを使用して、脆弱性調査をルーティンベースで（業界の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。
脆弱性が悪用されるリスクを軽減するために、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（業界のベストプラクティス/またはパッチ管理プログラムに従って適時に実施される是正措置）。
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。
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。

Barclays に代わってインフラストラクチャ/アプリケーションをホスティングすることに関連するサプライヤーのサービスについては、以下に従うものとします（事前に連絡を受けたハイリスクの第三者を含む）。

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、またはバークレイズ（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。

<table>
<tr><th>優先順位</th><th>評価</th><th>閉鎖日数（最大）</th></tr>
</table>
</td>
<td>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。</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>P1</td><td>重大</td><td>15（最大 30 日）</td></tr>
<tr><td>P2</td><td>高い</td><td>60</td></tr>
<tr><td>P3</td><td>中程度</td><td>180</td></tr>
<tr><td>P4</td><td>低い</td><td>SLA なし</td></tr>
</table>
サプライヤーが提供する Barclays のホスティングインフラストラクチャ/アプリケーションに重大な影響を与える可能性のある、すべてのセキュリティー問題や脆弱性について、サプライヤーがリスクの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（最高セキュリティーオフィスの ECAM チーム（externalcyberassurance@barclayscorp.com））と書面で合意する必要があります。

Barclays へのサービス提供に使用されるクラウドサービス利用者（サプライヤー）向けガイダンス

Barclays へのサービスを保護するため、クラウドサービス利用者（CSC）は、適切な脆弱性管理制御の実装を確認する必要があります。

• クラウドサービス利用者は、提供されるクラウドサービスに影響を与える可能性のある技術的脆弱性の管理に関する情報を、クラウドサービスプロバイダーに要求する必要があります。クラウドサービス利用者は、技術的な脆弱性を特定して管理する責任を負うとともに、それらを管理するプロセスを明確に定義する必要があります。
</td>
<td></td>
</tr>
<tr>
<td>14.パッチ管理</td>
<td>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パッチを導入するため、確立された方針および手順、業務プロセス/全社的措置、ならびに技術的措置に支えられたパッチ管理プログラムを備えているものとします。

サプライヤーは、サーバー、ネットワークデバイス、アプリケーションおよびエンドポイントデバイスが最新のセキュリティーパッチによって最新の状態に保たれていることを確認するものとします。また、業界のベストプラクティスに従って、次のことを確認します。</td>
<td>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。</td>
</tr>
</table>

	• 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評価およびテストし、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。 • 将来の監査、調査、トラブルシューティング、分析に必要な条件に対応するため、すべての主要な IT 変更は、実施前にログを取得し、テストし、承認済みの堅牢な変更管理プロセスに基づく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。	
15.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、バークレイズ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 インフラストラクチャを対象とする IT セキュリティ評価/ペネトレーションテストを実施するため、独立した適格なセキュリティサービスプロバイダーと契約するものとします。 これは、サイバー攻撃による Barclays のデータのセキュリティー侵害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 1 回実施する必要があります。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。 Barclays に代わって**インフラストラクチャ/アプリケーションをホスティング**することに関連するサプライヤーのサービスについては、以下に従うものとします（事前に連絡を受けた**ハイリスクの第三者**を含む）。 • バークレイズの主要活動の中断を防ぐため、サプライヤーはバークレイズ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、ECAM の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、バークレイズ（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ー評価報告書を年に 1 度、Barclays（最高セキュリティーオフィスの ECAM チーム（externalcyberassurance@barclayscorp.com））に提供する必要があります。** • 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。	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。

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

サプライヤーは、以下の表に従って、またはバークレイズ（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。

<table>
<tr><th>優先順位</th><th>評価</th><th>閉鎖日数（最大）</th></tr>
<tr><td>P1</td><td>重大</td><td>15（最大 30 日）</td></tr>
<tr><td>P2</td><td>高い</td><td>60</td></tr>
<tr><td>P3</td><td>中程度</td><td>180</td></tr>
<tr><td>P4</td><td>低い</td><td>SLA なし</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>16.暗号</td>
<td>
サプライヤーは、事業および情報セキュリティ要件に従ってバークレイズのデータ/情報の機密性、真正性、完全性を守るために、暗号化技術に関連する法律、法定、規制、契約の各要件を考慮して、暗号化技術を適切かつ効果的に使用する必要があります。

暗号化技術を使用する場合は、以下の内容を考慮する必要があります。

情報保護の一般原則を含む、組織が定義した暗号化に関するトピック固有の方針。暗号化技術の使用に関するトピック固有の方針は、利益を最大化し、暗号化技術を使用するリスクを最小限に抑え、不適切または誤った使用を回避するために必要です。
必要なレベルの保護と情報の分類を特定し、必要な暗号化アルゴリズムのタイプ、強度、品質を設定します。
暗号化技術を使用して、ストレージ媒体に保存されている情報を保護し、ネットワーク経由でそのようなデバイスまたはストレージ媒体に送信すること。
暗号鍵の生成と保護、鍵の紛失、侵害、損傷が発生した場合の暗号化された情報の復旧に対処する方法を含む、鍵管理へのアプローチ。
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

</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>

	します。サービス期間が終了した後、または必須のキーローテーションプログラムを設定した後、サプライヤーはキーを回収する必要があります。 • 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。 • 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。 • 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。 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。 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。 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。	

	○ 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。	
17.クラウドコンピューティング	サプライヤー（クラウドサービス利用者（CSC））は、Barclays へ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目標を達成し、Barclays へのサービスを保護するためにセキュリティー管理が実施され、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ー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、クラウド内の個人情報を含む Barclays の情報資産/データに関連するデータセキュリティー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ーの CSP は、クラウドコンピューティング環境のセキュリティーについて責任を負います。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	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。

	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。 • 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） • セキュアなデータ削除/データ消去 • 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 バークレイズ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、個人情報を含むバークレイズの情報資産/データは、バークレイズ（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。サプライヤーは、Barclays に対し、Barclays のデータが保存または保持されるデータゾーン、およびフェイルオーバーデータゾーンの場所を提供するものとします。	

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、**バークレイズ**に管理される LAN、WAN、デスクトップが**バークレイズ**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、バークレイズによって管理されます。

ティア 2（ビジネスクラス） - IT インフラストラクチャ全体が**サプライヤー**によって管理され、**バークレイズ**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 インフラストラクチャ全体が**サプライヤー**によって管理され、**バークレイズ**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。

18.1 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。
18.2 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御し、物理的なアクセス管理の仕組みによって監視し、許可された従業員のみが（役割限定）アクセスを許可され、（BDS 所有者により）承認されていることを確認する必要があります。 • 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、異動者や所在不明の従業員のアクセス権は、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： 許可された従業員の場合： 　　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して監視 • 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下請業者、復処理者を含む、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必要があります。
18.3 BDS - ビデオによる監視	• 不正アクセスおよび/または悪質な活動を効果的に記録または警告を発し、調査するために、BDS エリアのビデオ監視を実施します。 • 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。 • 運用と品質のためのカメラのテスト。また、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。
18.4 BDS - バークレイズのネットワークおよびバークレイズ	• 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、バークレイズの認証トークン（RSA 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。

認証トークンへのアクセス	• バークレイズは、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、そのサプライヤーの**退場日/最終出勤日/LDIO 受付日**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 - 4 を参照。在宅勤務（リモートアクセス）
18.5 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。 通常の業務において、銀行専用スペースまたはサプライヤーの施設からサービスを提供することが契約上義務付けられている場合や、規制要件が適用される場合は、（在宅を含む）リモート勤務は禁止されています。ただし、バークレイズと合意した災害復旧/危機/パンデミックの対応の場合、また、契約上の合意の一部としてリモート勤務を余儀なくされるセキュリティ要件では、サードパーティの事業継続計画において規定が認められています。
18.6 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ー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および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 • バークレイズの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 - 2 を参照。境界とネットワークセキュリティ
18.7 BDS - ワイヤレスネットワーク	Barclays へのサービスに用いる BDS ネットワークのワイヤレスネットワークを無効にします。

18.8 BDS - エンドポイントセキュリティ	デスクトップのセキュアビルド（ノート PC を含む）は、BDS ネットワーク内のコンピューター向けの業界のベストプラクティスに従って構成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。 • ハードディスクの完全暗号化。 • 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。 • サプライヤーの従業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 の情報/データを外部メディアへコピーするための USB を無効にする • 最新のマルウェア対策シグネチャとセキュリティパッチで更新を実施する。 • プリンタスプーラーサービスを無効にする。 • バークレイズの情報資産/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。 • 悪意のあるソフトウェアを含む不正なソフトウェアの存在および/または使用を検出、阻止、修正する • ロック画面のタイムアウト、TCP IP 接続の企業ネットワークのみへの制限、疑わしい動作を検出する Advanced EPS セキュリティエージェント。 コントロール - 8 を参照。エンドポイントセキュリティ

18.9 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。

18.10 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、バークレイズによる少なくとも 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バークレイズに対する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/復処理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、バークレイズがセキュリティ審査を実施することを許可しなければなりません。サプライヤーは、Barclays に年に 1 回の視察、および/またはセキュリティーインシデント後の即時の視察を許可しなければなりません。

視察中に Barclays により管理の非遵守が特定された場合、Barclays によるリスク評価が行われなければなりません。Barclays は改善期間を定める必要があります。サプライヤーは、その後、期間内に必要な改善を完了しなければなりません。

サプライヤーは、視察および視察中に提出された書類に関連して Barclays から合理的に要求されたすべてのサポートを提供する必要があります。文書は記入し、速やかに Barclays に返送する必要があります。また、サプライヤーは保証審査中に要求された証拠とともに、Barclays の評価質問者をサポートする必要があります。

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バークレイズ専属の下請業者、復処理者が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小限水準のアクセス/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。
個人情報	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。
仮想マシン：	ゲストソフトウェアの実行をサポートする完全な環境。 注：仮想マシンは、仮想ハードウェア、仮想ディスク、および仮想マシンに関連付けられたメタデータを完全にカプセル化したものである。仮想マシンでは、ハイパーバイザーと呼ばれるソフトウェアレイヤーを介して、基盤となる物理マシンを多重化できる。

BARCLAYS

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

2023 年 9 月付け第 13.0 版

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必要があります。 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、銀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、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、サプライヤーの新従業員全員（CID へのアクセスを持ち、および/またはそれらを取り扱う）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（約 3 ヵ月）内にトレーニングを完了する必要があります。 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 B：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、バークレイズ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従業員、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 C：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**サードパーティアプリケーション**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	クライアント//見込み顧客名	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	表題	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

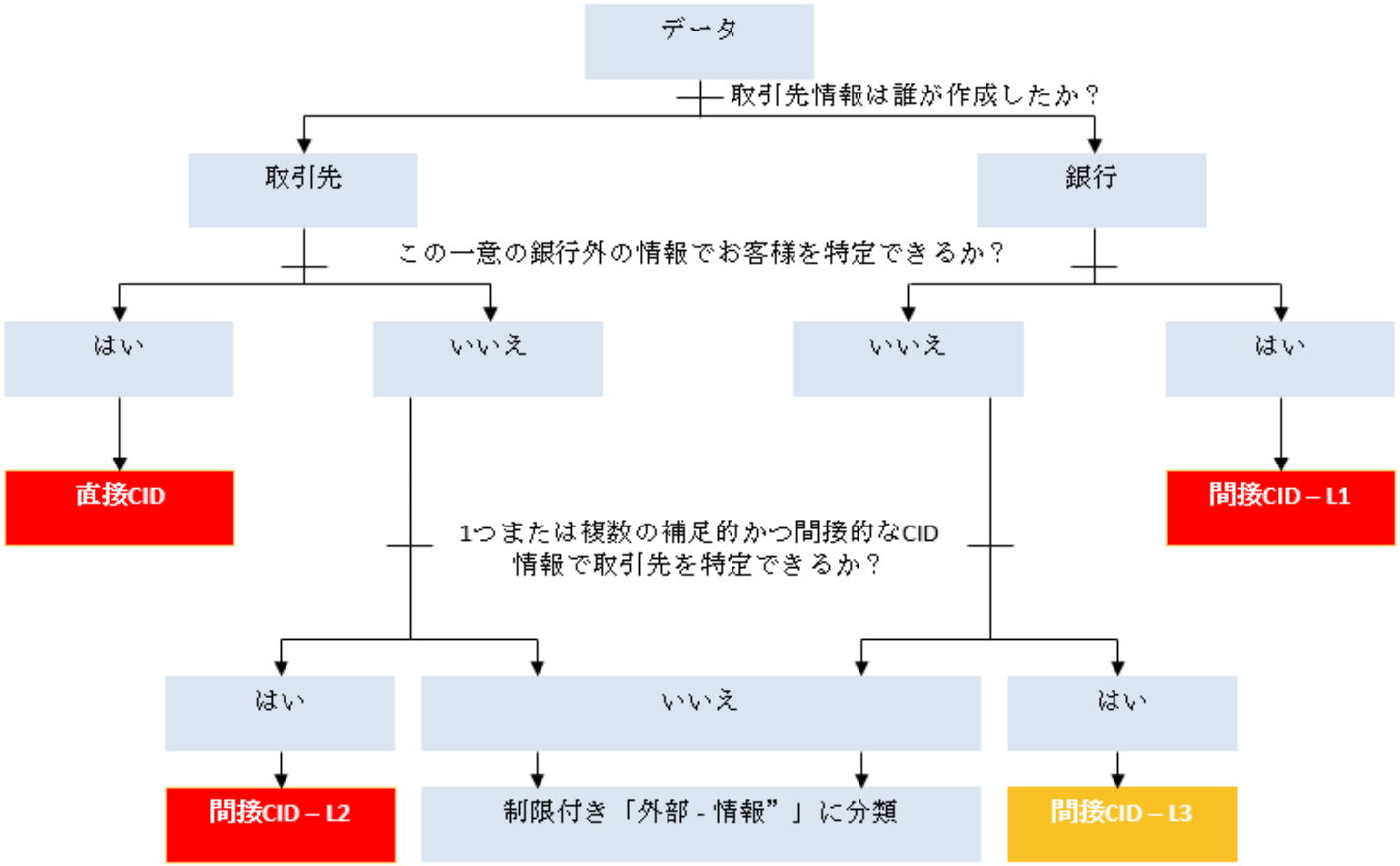
(DCID) = 銀行秘密違反

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 D：Barclays 情報ラベリングスキーム

表 D1：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。 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「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。	• 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（目論見書、募集要項など）。 • 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 D2：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）。 • 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。	• 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。	• 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のみを使用して配布する必要があります。 • 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のみを使用して配布する必要があります。 • 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。	• 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のみを使用して配布する必要があります。 • 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。