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

情報およびサイバーリスク低に分類されたサプライヤー用

2019 年 4 月付け第 9.0 版

管理対象	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、方針、標準	サプライヤーは、技術環境と情報とサイバーセキュリティ管理の状態についての理解を確かなものとし、優れた業界標準（NIST、SANS、ISO27001 など）および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徹底する情報/サイバーリスクのガバナンスプロセスを設けるものとします。 サプライヤーは、情報/サイバーセキュリティに関連する、定期的なリスク評価を実施し、特定されたリスクを軽減するために必要な管理を履行し、手順を講じるものとします。 サプライヤーは上級経営陣が承認した方針、およびサプライヤーの情報/サイバーリスクを管理する標準を維持管理するものとします。 サプライヤーは、情報/サイバーセキュリティの役割と責任を定義するものとします。	この管理が実施されない場合、Barclays またはサプライヤーは、情報/サイバーセキュリティに関する適切な監視を持てず、またそれを実証できない場合があります。 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。
2. インシデント管理プロセス	Barclays 情報、および/または Barclays により使用されるサービスに関連するインシデントについての適時な処理と定期的な報告を行うためのインシデント対応プロセスを確立および管理するものとします。インシデント対応手順の一環として以下を定義するものとします： • Barclays の資産および/または Barclays に提供されるサービスに影響を及ぼす、またはこれらを標的としたセキュリティインシデントおよびデータ違反が発生した場合には、できるだけ早急に Barclays に連絡し、改善措置に関する最新状況を提供するものとします。 • 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（アクション、責任者、実施日）によって対処され、Barclays に情報を提供するよう徹底するものとします。	インシデント管理および対応プロセスは、インシデントを速やかに解決し、エスカレートすることを防止するためのものです。

3. 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 のデータ処理に使用されるエンドポイントには、攻撃に対して強固な防御策を設けるものとします。 これには、不必要なソフトウェア/サービス/ポートを無効化することにより攻撃対象領域を限定すること、すべてのデプロイ版が公開サポート期間内であることを確認すること、マルウェア保護およびホストのファイアウォール機能を設け、適切に設定すること、エクスプロイトの試みを阻止するための管理を設けることなどが含まれます。	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。
4. クラウドコンピューティング	あらゆるクラウドコンピューティング（パブリック/プライベート/コミュニティ/ハイブリッド）サービスの使用 Barclays への提供サービスの一環として使用される SaaS/PaaS/IaaS には十分な保護を施すものとします。Barclays の情報とサービスを保護するための管理は、データ漏洩とサイバー違反を防止するため、リスクプロフィールおよび情報資産の重要度にふさわしいものである必要があります。	この原則が履行されない場合、不適切に保護された Barclays の情報資産が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、名声の毀損を招く場合があります。
5. マルウェア保護	ウィルスや他の形式のマルウェアなどの悪意あるソフトウェアから適切に保護するために、マルウェア対策管理とツールを整備しなければなりません。	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。
6. 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 システムは、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横への広がり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、Barclays に提供するサービスに基づいて、以下の保護メカニズムを検討するものとします： **外部接続：** ネットワークへのすべての外部接続は文書記録し、ファイヤーウォールを経由させ、接続が確立される前に検証し承認することで、データセキュリティ違反を防止しなければなりません。 **無線アクセス：** ネットワークへのすべての無線アクセスは、セキュリティ違反を防止するため、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。	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。

	侵入検知/防止： 侵入検知、防止システムおよびツールをネットワークの適切な位置に配置し、持続的標的型攻撃（APT）を含む、サイバーセキュリティ違反を検知するために、アウトプットを監視しなければなりません。 **分散サービス妨害（DDoS）：** 多層防御アプローチを、ネットワークと主要システムに実装し、サイバー攻撃によるサービス中断を常時、防止しなければなりません。 *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。*	
7. アプリケーションの保護	サプライヤーソフトウェア/アプリケーション開発においては、サービス中断やセキュリティ脆弱性、サイバーセキュリティ違反を防止するため、すべての主要なセキュリティ活動がソフトウェア開発プロセスに組み込まれるよう徹底しなければなりません。 サプライヤーは、緊急時にブレークグラス方式などの適切な管理によってアクセスが保護されない限り、システム開発者が実環境にアクセスできないことを保証することを含む、システム開発の任務の分離を保証するものとします。これらの環境におけるこのような活動では、ログが作成され、単独で審査できるものとします。 サプライヤーはソースコードが安全に実行、保存、Barclays 宛てに送信されることを徹底するものとします。	アプリケーション開発を保護する管理は、デプロイにおいてアプリケーションがセキュアであることを確認する上で役立ちます。
8. 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、サプライヤーが Barclays に提供するサービスに関連するITインフラおよびアプリケーションを対象とした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、有資格のセキュリティプロバイダーを採用するものとします。 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。 サプライヤーは特定された脆弱性を記録、トリアージ、対応するための一貫した仕組みを運用するものとします。	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。

9. 資産およびセキュリティ保護技術	攻撃の実施、実行、エクスプロイトおよび漏洩を防ぐため、一貫した管理基本が維持された現在および将来のサイバー脅威に対処するための適切な技術を適用するものとします。 サプライヤーのシステムの一部を構成するホストシステムおよびネットワークデバイスは、優れた業界標準（NIST、SANS、ISO27001 など）に従って機能するよう設定されるものとします。 それを保管または処理する資産またはシステムは、物理的な改ざん、損失、損害、または押収、および不適切な設定または変更から守られる必要があります。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、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。 システムは不必要な違反を防ぐため安全に設定される必要があります。不適切または悪意ある活動を検知するため、システムの監視、監査、ログ記録体制を設ける必要があります。	この管理が実施されない場合、Barclays へのサービス提供のためにサプライヤーが使用する Barclays の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。
10. 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。

	これらの原則はリスクベースに基づいて適用され、情報の機密性 評価を考慮するものとします。 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。 このことは共有アカウントの使用を除外するわけではありませんが、1 名の個人が各共有口座の責任を負わなくてはならないことに変わりはありません。 アクセス管理プロセスは、業界の最良慣行に従って定義されるものとし、最低でも以下を含むものとします： • アカウントの作成/修正/削除に先立ち実施される堅牢な許可プロセス。 • 定期的なユーザーアクセスレビュープロセス。 • 異動者管理 – 異動日から 5 営業日以内にアクセスを修正/削除する。 • 離職者管理 – 離職日から 24 時間以内に Barclays へのサービス提供に使用されたすべての論理アクセスを削除する。その他すべての二次アクセスは 7 日以内に削除する。 • 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するものとする。 • 対話型アカウントのパスワードは最低でも 90 日ごとに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 日ごとに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、無効となる必要があります。 サプライヤー管理環境内に保存された Barclays の情報資産へのリモートアクセスが許可されている場合、ユーザーの身元、機器の種類、機器のセキュリティ面（パッチレベル、アンチマルウェアの状況、ルート化または非ルート化のモバイル機器など）を考慮したエンドポイントの 2 要素認証および許可を行うものとします。	
11. データ漏えい防止	サプライヤーが Barclays に提供するサービスに関連する情報がネットワークまたは物理的媒体を通じて漏れるデータ漏洩リスクは、評価され、軽減されるものとします。 以下のデータ漏洩チャンネルを考慮するものとします： • 社内ネットワーク/サプライヤーネットワーク外の情報の不正な転送。	適切なデータ漏えい防止管理は情報セキュリティにおける不可欠な要素であり、Barclays 情報の損失を防ぎます。

	• ポータブル電子メディア（ノートブック上の電子情報、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。 • 第三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	
12. 情報のラベリングスキーム	***適宜****、サプライヤーは、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対して、Barclays 情報ラベリングスキームおよび取り扱い要件（付属書 B、表 B1 および B2）を適用するか、または Barclays と合意した代替スキームを適用する必要があります。 * 「***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。
13. 視察の権利	サプライヤーは、Barclays による少なくとも 10 営業日 前の書面による通知により、サプライヤーがその義務へのコンプライアンスを果たしているかの審査をするために、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。 またサプライヤーは、セキュリティインシデント後、Barclays が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、すべての視察に関し、Barclays から合 理的に要求されたすべての 支援を提供するものとします。	これが合意されない場合、サプライヤーはこれらのセキュリティ義務に対するコンプライアンスの完全な保証を与えることができなくなります。

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）。
持続的標的型攻撃（APT）	持続的標的型攻撃（APT）とは、個人またはグループがネットワークへの不正なアクセスを得て、長期間検知されない密かなコンピューターネットワーク攻撃のこと。
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。
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。 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。 通常、高（ビジネスプロセス）レベルでグループ化される。
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。
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。
ユーザー	高レベルの権限を持たず、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 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がある場合には、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 • 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。	• 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。

	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。	
社外秘	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、情報所有者が許可している特定の対象者または外部関係者に制限されている Barclays マネージドサービスプロバイダー（MSP）である場合、情報は社外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。	• 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 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	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。	• 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。

	• 電子資産には、明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。	• 紙印刷された資産が入っている封筒には、表面に明確な情報ラベルを貼るものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。 複数ページの電子文書のコピーには、全ページに明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。 • 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。	• 紙印刷された資産が入っている封筒には、表面に明確な情報ラベルを貼り、開封明示シールを貼るものとします。 それらは配布前に、ラベルのない別の封筒に入れるものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。 複数ページの電子文書のコピーには、全ページに明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。 • 資産は、情報所有者により受信を個別に許可された人員のみに配布するものとします。 • 資産はファックスで送信してはなりません。 • 電子資産を社内ネットワーク外に転送する場合は、承認済みの暗号保護メカニズムを使用して暗号化するものとします。 • 電子資産の流通管理を維持するものとします。
アーカイブ化と処分	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。 • 秘密電子資産が保存されていたメディアは、処分の前または処分中に、適切に機密情報を分離するものとします。

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 回は、サプライヤーは CID の役割と責任に重点を置いた文書をレビューし、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シニア幹部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）。	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。 取り扱い要件の違反（表 C2 に定義される）は、サプライヤーが対応し、直ちに（遅くとも 24 時間以内）対応する銀行秘密法域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（アクション、責任者、実施日）によって対処され、対応する銀行秘密法域と共有され、合意を得ることを確認するものとします。	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 に深刻な風評上の損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到ることがあります
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、規制に新たな変更があった後、または少なくとも年に 1 回は CID 銀行秘密要件の実施トレーニング*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 C の表 C1）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 C の表 C2 に提供されています。 *「**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不十分な 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上の損害が発生する恐れがあります。

** 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 B：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** は一意の識別子（取引先が所有）として定義することができる。これは銀行アプリケーションまたはその他の **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取引先を一意に識別できる。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	名	社内処理 ID
	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	静的一意の識別子
	アカウント明細	住所	国籍	動的識別子
	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		姓	
	役職または PEP タイトル		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	
			大型ポジション/取引価値	

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 C：Barclays 情報ラベリングスキーム

表 C1： 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、刑事訴訟に到ることもあり、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 B）

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。	• 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

	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。	• 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 C2： 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）。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所で作業したり、無人状態で放置してはなりません。 資産は、適切な管理が確立されている場合のみ作業可能です（覗き見防止フィルムなど）。

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