

暗号資産関連業務の委託先管理における プラクティスについての研究報告資料

作成日：2026 年 10 月 20 日

版数：第 1 版

一般社団法人 日本暗号資産ビジネス協会

改訂履歴

版数	日付	改訂内容	作成
1.0	2026/10/20	初版発行	JCBA セキュリティ・システム ム部会-

目次

[第 1 章 本資料の目的・適用範囲](#)

[第 2 章 背景・基本的な考え方](#)

[第 3 章 実務上の利用方法](#)

[第 4 章 別紙プラクティス集の見方・使い方](#)

[第 5 章 別紙の作成方針・参照元の実扱い](#)

第1章 本資料の目的・適用範囲

1. 本資料の位置づけ

本資料は、付属の Excel「別紙-委託先管理におけるプラクティス集」（以下「本表」）が、何のために・どのような背景と発想で作られたのかを説明する概要資料です。本表の各シートの構成・列の定義・区分の判定手順・記入方法といった実務詳細は、第4章に記載しています。

2. 本取組の目的

暗号資産交換業、電子決済手段等取引業及び資金移動業並びに暗号資産等関連デリバティブ取引業の自主規制団体一般社団法人である日本暗号資産等取引業協会（JVCEA）が発出している「再発防止点検リストの考え方」等の文書は、いずれも暗号資産交換業者（委託元）向けに書かれています。**本表は、これらの要求を委託先（システム提供者）として何をどう担うか——委託元が要求を満たせる機能・仕様・証跡の提供、委託先自身の運用分の態勢整備、委託元への支援——に翻訳し、監査実務の標準語彙で一覧化したものです。**これにより、委託元の評価負担の軽減、委託先の自己点検と説明可能性の向上、そして当局・監査人・委託元・委託先が同じ言葉で議論できる共通基盤の形成を目指しています。

第2章 背景・基本的な考え方

1. 背景と問題意識

暗号資産業界では、ウォレット等の重要システムの一部を外部の専門事業者へ委託する構造が定着しています。近年、これらの委託先を攻撃対象とする資産流出事案が複数発生し、委託先管理の重要性が高まりました。制度面でも、2026年7月に成立・公布された改正金商法により第三章の六「暗号資産管理関係業務提供者制度」が新設され、重要システムの委託先が直接の規制対象となる枠組みが設けられました（施行は公布から1年以内の政令で定める日）。また金融庁「TPCRM（Third-Party Cybersecurity Risk

Management：サードパーティ・サイバーセキュリティリスク管理）強化に関する調査」の公表により、委託元・委託先双方に管理態勢の強化が要請されています。

一方で、次の4点が業界の課題として残っていると考えています。

- 委託先（サードパーティ）が主導して実施すべきセキュリティ対応の標準形が、十分に議論・検証されていないこと。
- システム導入時に委託先が交換業者へ提示すべき資料・証跡が要件定義されていないこと。
- SOC 2等の第三者認証で説明できる対応と、認証では確認されない暗号資産固有の実務的な対応とが峻別されていないこと。
- 委託先各社が把握している重要システム利用上のリスクや留意点が、委託元に十分共有されていないこと。

2. 設計の考え方

そこで本表では、**委託先が「何を実施すべきか」だけではなく、「なぜ必要なのか」「どのような証跡で説明するのか」「どのような委託形態で求められるのか」を体系的に整理すること**を重視しました。これにより、委託先の自己点検および説明可能性の向上、委託元による評価の効率化、ならびに第三者機関によるレビューの効率化を目指しています。その具体的な設計方針として、以下の3つの考え方で構成しています。

共通言語：当局・監査法人・委託元のリスク管理部門が追加学習なく読めるよう、全347項目を想定されるリスクの例→確認観点の詳細→確認資料例の三つ組に、想定される管理上の位置づけ（指揮的・予防的・発見的・是正的）と想定される確認観点の分類（整備・運用）の2軸を付した評価標準語彙で記述しています。独自のフレームワークや学術的な分類は採用せずに、公知のガイドライン等を参照・整理しています。参照しているガイドライン、フレームワーク等の詳細は第5章を参照ください。

リスクベースの形態別要求：委託先のリスクは一律ではありません。暗号資産の移転工程（鍵ライフサイクル・指図受付・トランザクション組成・署名・検証送信・モニタリング）のどこまでを委託先の環境・運用に置くかで、委託先が保有する攻撃可能面（アタックサーフェス）が構造的に決まります。本表では、暗号資産を扱う事業において重要なシステムと位置づけられる「鍵管理及びトランザクション署名管理」に関連する委託契約を主に扱います。委託契約における役務範囲の違いをもとに、サービス提供形態を「保持型」～「その他」の5つに区分し、全項目に形態別の参照統制目安を付与しています。これにより、サービス内容や関与の様態に応じた確認観点を整理することができ、委託先に対する確認事項の過不足を

抑制することができます。確認観点の各項目とその説明および各項目の参照目安の詳細は第 4 章に詳述しています。

自己点検と証跡管理の一体化：本表は一覧に留まらず、委託先が自社の形態を選択すると参照目安である確認観点が自動表示されるセルフアセスメントシート、および提示する確認資料を管理する台帳を含みます。委託元は「どの要求に対し・何を根拠に・どの証跡で」説明されているかを、標準化された形で確認できます。想定する委託形態の詳細は第 4 章「サービス提供形態の考え方」に詳述しています。

第3章 実務上の利用方法

1. 本表が想定する利用者

本表は、暗号資産交換業者等の委託元、ウォレット事業者等の委託先、そして監査法人・当局・自主規制団体等の第三者機関が、共通の基準と言葉で委託先管理およびセキュリティ統制を評価できるよう設計しています。

本表は、これまで暗号資産交換業者等の委託元と、監査法人・当局・自主規制団体等の第三者機関の間で共通言語として共有されてきた FISC 等の基準やガイドラインを、委託先目線で翻案することで、国内外で培われてきた金融水準の委託先管理及びセキュリティ統制に委託先もキャッチアップできるよう、自己点検ならびにコミュニケーション円滑化が図れるように設計しています。

従来、委託元ごとに評価観点や質問内容が異なり、委託先は個別対応の負担を負う一方、委託元も評価品質のばらつきや比較可能性の不足という課題を抱えていました。また、第三者評価においても、暗号資産特有の管理態勢をどのような観点で確認すべきかについて、統一的な整理が十分ではありませんでした。

本表は、これらの関係者が共通の枠組みを利用することで、評価の効率化および説明可能性の向上を図ることを目的としています。

2. 委託先における活用

委託先は、本表を自己点検・統制整備・顧客説明のための共通フレームワークとして利用できます。本表では、自社のサービス提供形態を整理した上で、本表に示された要求事項への対応状況を確認することで、自社が備えるべき管理態勢の現状把握およびギャップ分析を行うことができます。これにより、暗号資産関連業務を提供する事業者をはじめとする、サードパーティらが自主的に IT サプライチェーン全体の強靱化・セキュリティ向上に取り組むことができます。

また、本表は委託元から求められるセキュリティ質問票や監査対応に対する説明資料としても利用できます。標準化された要求事項と監査証跡の整理に基づき、自社の統制状況を説明できるため、委託元ごとの個別要求への対応負荷の軽減が期待されます。さらに、自己点検結果と関連証跡を継続的に管理すること

で、管理態勢の改善状況や証跡整備状況を一元的に把握できるようになり、内部統制の継続的な高度化にも活用できます。

活用例：

- ・ 自己点検（セルフアセスメント）
- ・ セキュリティ統制の整備計画策定
- ・ SOC 報告書や第三者認証の補完資料作成
- ・ 委託元への質問票回答
- ・ 営業提案時の管理態勢説明
- ・ 証跡管理台帳の整備

3. 委託元における活用

委託元は、本表を委託先選定時のデューデリジェンス、契約後の定期評価、セキュリティレビュー等に利用することができます。本表では、委託先が担う業務範囲に応じて必要となりうる統制項目の例が列挙されているため、委託元は委託先に対して 業界内における実践例に基づいて対応項目を精緻化することができます。また、各統制に対して想定される監査証跡が整理されているため、「どのような証拠を確認すればよいか」を効率的に把握できます。

これにより、委託先ごとに異なる評価表を作成する必要性が低下し、評価負担の軽減が期待されます。また、複数の委託先を同一基準で比較できることで、委託先選定や継続利用の判断の透明性・客観性が向上します。さらに、評価結果を継続的なモニタリング活動に活用することで、委託先管理の高度化および効率化に資することが期待されます。

活用例：

- ・ 新規委託先選定時のデューデリジェンス
- ・ 年次委託先評価
- ・ 再委託先を含む委託先管理
- ・ 重要システムのリスクアセスメント
- ・ 当局検査・内部監査対応時の説明資料

4. 第三者機関における活用

監査法人、自主規制団体、当局等の第三者機関は、本表を委託先の統制状況を確認する際の参考例として利用することができます。

本表は、暗号資産管理業務に固有のリスクを起点として、確認すべき項目および確認資料を体系的に整理しているため、これを参考として評価者が委託先管理のリスクと統制、確認資料の関係性を一定の観点から効率的に把握することが可能となります。また、監査やレビューにおいて、SOC 報告書等で確認可能な事項と、暗号資産特有の管理態勢として追加的に確認すべき事項を整理する際の補助資料として利用することも想定しています。これにより、委託先の管理態勢評価における説明可能性および比較可能性の向上が期待されます。

活用例：

- 外部監査における統制評価
- SOC 保証業務の補助資料
- 当局検査やモニタリング活動
- 自主規制団体による実態把握
- 委託元・委託先間の評価結果のレビュー

第4章 別紙-委託先管理におけるプラクティス集の見方・使い方

1. 本章の概要

本表は、暗号資産関連業務における委託先管理について、業界における実務上の知見並びに FISC、NIST および JVCEA 等の基準・ガイドライン・関連法令を参考として、委託先管理上の確認観点をプラクティス集として整理したものです。

本表は、法令上の義務や画一的な評価項目を定めるものではなく、委託元、委託先および第三者機関が、委託先管理に係る実務上の確認観点を共通的に理解し、必要に応じて自社の態勢整備や説明に活用するための参考資料として位置付けられます。

本資料は、特定の法令、規制、基準またはガイドラインへの適合性を保証するものではなく、利用者の業務内容、サービス提供形態、リスクおよび関連する法令等を踏まえ、各確認観点の適用可否および具体的な対応方法を個別に検討することが望ましいです。

本章では、本表のうち中核となる「①委託先管理のプラクティス一覧」シートを中心に、管理領域、確認観点の構成および個別項目の参照方法について説明します。

2. ①委託先管理のプラクティス一覧の概要

「①委託先管理のプラクティス一覧」シートは、本表の中核となるシートであり、暗号資産関連業務における委託先管理上のプラクティス集を一覧形式で整理しています。

各項目は、確認テーマを表す「確認観点」と、具体的な確認内容を表す「確認観点の詳細」を中心として構成されています。また、確認観点を考慮しない場合に生じ得る「想定されるリスクの例」および取組状況を確認・説明する際に参考となる「確認資料例」を併せて記載しています。

さらに、各項目には、実施主体および対象の例並びに、委託先のサービス提供形態に応じた参照目安を付しています。利用者は、これらの情報を組み合わせて確認することで、各項目の目的、背景、想定されるリスクおよび確認時に参考となる資料を把握することができます。「①委託先管理のプラクティス一覧」シートの各項目の詳細は以下に記載しています。

表 1. ①委託先管理におけるプラクティス集の各項目とその説明

No.	項目名	説明
1	大カテゴリ	A～J の管理領域を示す。
2	確認観点番号	同一の確認テーマに属する項目を識別する番号を示す。
3	確認観点	確認テーマの名称を示す。
4	確認観点的概要	当該確認観点的目的、背景および全体的な考え方を示す。
5	項目番号	個別の確認項目を識別する主キーを示す。
6	確認観点的詳細	委託先管理上、具体的に確認することが考えられる内容を示す。
7	想定されるリスクの例	当該確認観点が考慮されない場合に想定されるリスクを示す。
8	確認資料例	当該項目の取組状況を確認または説明する際に参考となる資料の例を示す。
9	実施主体の例	当該項目に係る取組の実施主体となることが考えられる部門、役職または関係者の例を示す。
10	対象の例	当該項目に係る取組の対象となることが考えられる人、組織、システム、情報等の例を示す。
11-15	委託先のサービス提供形態	委託先のサービス提供形態を「保持型」「介在型」「供給型」「参照型」「その他」を大別し、それぞれの提供形態における当該項目の参照目安を「○」または「NA」で示す ※各提供形態の詳細・分類は次節で詳述する。
16	想定される管理上の位置づけ	当該確認観点について、実務上整理されることがある管理上の位置付けの例を示す。*1

17	想定される 確認観点の分類	当該確認観点について、一般的に整理されることが想定される確認観点の分類例を示す。*1 なお、ここでの「整備」は基準や仕組みを定めることを、「運用」は実施・記録・見直しを行うことを指す。この際、運用の前提として整備が含まれるケースがありえる。
----	------------------	--

*1：各項目は確認観点を理解するための参考情報であり、特定の実施方法、評価方法または監査手続を規定するものではありません。

3. 大カテゴリの構成

「④委託先管理のプラクティス一覧」シートでは、委託先管理に関する確認観点を大カテゴリとして、整理しています。

大カテゴリは A～J の 10 分類で構成され、一般的な情報セキュリティ管理領域に加え、暗号資産関連業務に特徴的な「鍵管理・署名運用」を独立した分類として設けています。

表 2. 大カテゴリの分類と主な確認観点

分類	管理領域	主な確認観点
A	ガバナンス・組織体制	経営関与、3 線体制、CISO、委員会、説明責任
B	リスク管理	リスク特定・評価、残存リスク管理、脅威・脆弱性情報収集、BIA
C	人的セキュリティ	採用・異動・退職時管理、教育・訓練、内部不正、アクセス権管理
D	鍵管理・署名運用	鍵生成・保管、署名運用、コールド／ホット分離、出庫時検証、鍵片の分散管理
E	システムセキュリティ	認証・認可、暗号化、ネットワーク制御、脆弱性管理、ログ監視、供給データの正確性・継続性

F	物理セキュリティ	データセンター、サーバ室、入退室、媒体、端末管理
G	運用・変更管理	運用マニュアル、変更管理、環境分離、バックアップ、構成管理
H	インシデント対応・BCP	検知・報告、訓練、BCP、委託元への通知、流出時対応
I	再委託先管理	再委託先の選定・評価、契約、モニタリング、集中リスク
J	関連法令・契約・監査	関連する法令・規則等の動向把握、契約条件、内部監査、外部監査、報告・記録管理、委託元監査への対応

D「鍵管理・署名運用」の項目のうち「～する機能を提供する」と記載したものは、委託先が当該工程を自ら運用する形態（鍵・鍵片を保持する保持型等）では、委託先自身が当該統制を実施し、その実施記録を委託元に提示することを含みます。

利用者は、まず委託先の業務範囲およびサービス提供形態を踏まえ、参照対象となる管理領域を確認します。その上で、該当する大カテゴリ配下の「確認観点の詳細」「想定されるリスクの例」「確認資料例」および「サービス提供形態別の参照目安」を確認します。

4. サービス提供形態の考え方

委託先による暗号資産関連業務への関与の様態に応じてサービス提供形態を区分し、各サービスに求められる確認観点の参照目安の詳細を記載しています。各サービス提供形態の分類は、委託元の業務への関与方法を整理し分類することが可能であり、以下の観点を考慮してサービス提供形態を検討する必要があります。

- ・ 秘密鍵等を保持するか
- ・ 委託元の承認を経ずに稼働中システムへ影響を与えられるか
- ・ 成果物等を委託元が確認・承認したうえで利用するか
- ・ 委託元の判断材料となるデータを提供するか

上記を考慮したうえでの委託先の委託形態の判断手順の例を以下に示します。



図1 委託形態の判断手順の図（例）

また、「①委託先管理のプラクティス一覧」シートでは、各項目について、委託先のサービス提供形態に応じた参照目安を「○」または「NA」で記載しています。参照目安の「○」または「NA」については以下の認識のもと作成しています。

表 3. 各項目の参照目安の詳細

記号	説明
○	当該サービス提供形態において、参照することが望ましい、または参照することが望ましいが、優先度が相対的に低いと考えられる項目。
NA	当該サービス提供形態において、対象外と考えられる項目。

「表 3. 各項目の参照目安の詳細」に記載の通り、「○」または「NA」は、法令上の対応義務や一律の適用可否を示すものではありません。また、「NA」が付された項目について、その実施または参照を妨げるものではありません。利用者は、自社の業務内容、委託範囲、リスク特性およびサービスの重要性等を踏まえ、必要に応じて「NA」が付された項目についても参照することが推奨されます。

5. 確認観点の記載例

以下では、「①委託先管理のプラクティス一覧」に記載されている項目のうち、A-1-①を例に、各記載項目の参照方法を示します。

利用者は、個別項目を確認する際に、「確認観点の詳細」のみを単独で参照するのではなく、「想定されるリスクの例」「確認資料例」および「サービス提供形態別の参照目安」を併せて確認することが望ましいです。

表 4. 確認観点の参照方法の例

No	項目	A-1-①の記載例	参照方法
1	大カテゴリ	A. ガバナンス・組織体制	当該項目が属する管理領域を示す。
2	確認観点番号	A-1	同一の確認テーマに属する項目群を識別する番号を示す。
3	確認観点	セキュリティガバナンス（経営関与・3線体制）	当該項目が扱う確認テーマを示す。
4	確認観点的概要	委託先として、経営層がサイバーセキュリティに関与し、1線（事業部門）／2線（リスク管理部門）／3線（内部監査部門）の体制を整備していること	当該確認観点で確認すべき概要を示す。
5	項目番号	A-1-①	関連シート間で共通して参照する個別項目の主キーとなる。
6	確認観点的詳細	経営層がサイバーセキュリティを経営課題として位置づけ、定期的なレビューを行う体制を整備する	委託先管理上、具体的に確認することが考えられる内容を示す。
7	想定されるリスクの例	経営層のサイバーセキュリティへの関心不足によるガバナンス機能不全	当該確認観点が考慮されない場合に想定されるリスクを示す。

8	確認資料例	経営会議議事録（サイバー議題）／経営層レビュー実施記録	取組状況を確認または説明する際に参考となる資料の例を示す。
9	実施主体の例	経営層・取締役会	当該取組の実施主体となることが考えられる役職または会議体の例を示す。
10	対象の例	規程・プロセス	当該取組の対象となることが考えられる事項の例を示す。
11-15	（委託先のサービス提供形態）	○	当該サービス提供形態において、参照することが望ましい、または参照することが望ましいが、優先度が相対的に低いと考えられる項目。
16	想定される管理上の位置づけ	指揮的	当該確認観点について、実務上整理されることがある管理上の位置付けの例を示す。 *1
17	想定される確認観点の分類	整備	当該確認観点について、一般的にどのような観点で整理されることがあるかの例を示す。 *1

*1：各項目は確認観点を理解するための参考情報であり、特定の実施方法、評価方法または監査手続を規定するものではありません。

上記の例では、「確認観点の詳細」に記載された内容が具体的な確認対象となります。

「想定されるリスクの例」を確認することで、当該確認観点がどのようなリスクへの対応を意図しているかを把握することができます。また、「確認資料例」を参照することで、委託先が取組状況を説明する際

に、どのような資料を利用できるかを特定することができます。「①委託先管理のプラクティス一覧」の利用例を以下に記載します。

大カテゴリ	確認観点番号	確認観点	確認観点の概要	項目番号	確認観点の詳細	想定されるリスクの例	確認資料例
A. ガバナンス・組織体制							
A. ガバナンス・組織体制	A-1	セキュリティガバナンス（経営関与・3線体制）	委託先として、経営層がサイバーセキュリティに関与し、1線（事業部門）／2線（リスク管理部門）／3線（内部監査部門）の体制を整備していること	A-1-①	経営層がサイバーセキュリティを経営課題として位置づけ、定期的なレビューを行う体制を整備する	経営層のサイバーセキュリティへの関心不足によるガバナンス機能不全	経営会議議事録（サイバー議題）／経営層レビュー実施記録

ポイント①
「想定されるリスク」にて「確認観点の概要」「確認観点の詳細」がどのようなリスクへの対応を意図しているかを確認できる。

ポイント②
「確認資料例」を参照することで、「確認観点の詳細」に対する取組状況を説明するための参考資料を特定することができる。

図2 「①対応項目一覧」の利用例

第5章 別紙の作成方針・参照元の取扱い

1. 別紙資料の全体概要の説明

本表を構成する各シートについて説明します。

第4章で説明した「①委託先管理のプラクティス一覧」を本体としつつ、「②セルフアセスメントシート」「③社内証跡管理台帳」を組み合わせることで、プラクティスの背景確認、自己点検、証跡管理および外部説明を一体的に実施することができます。

表 5. 委託先セキュリティ対応項目の構成

シート	主な役割	主な利用者
①委託先管理におけるプラクティス一覧	委託先管理上の確認観点を整理した本体。確認観点の詳細、想定されるリスク、確認資料例およびサービス提供形態別の参照目安等を確認する。	委託元、委託先、第三者機関
②セルフアセスメントシート	委託先が自社の確認状況、確認結果、今後の対応事項および対応予定・ロードマップ等を整理する。	委託先、委託元
③確認資料管理台帳	セルフレビュー等において使用する証跡を一元的に管理する。	委託先
④参照資料一覧	本一覧は、本表の作成にあたり参考とした主な資料を掲げるものであり、特定の用途は想定していない。	-

2. ②セルフアセスメントシート

「②セルフアセスメントシート」は、委託先が自社の取組状況を自己点検し、委託元または第三者に対して説明するためのシートです。

利用者は、サービス提供形態を選択し、表示された参照目安を踏まえて、各項目の確認状況、実施頻度、実施方法、確認結果、今後の対応事項、対応予定・ロードマップおよび確認資料等を整理します。

記入項目	説明
サービス提供形態別の参照目安	選択したサービス提供形態に応じて、各項目の参照目安を「○」または「NA」で表示する。
確認状況	未着手、整備済、運用中、検証済等の区分により、取組の状況を整理する。
実施頻度	都度、日次、週次、月次、四半期、年次、イベント発生時等、取組の実施頻度を記載する。
実施方法	閲覧、観察、質問、再実施等、自己点検時に用いた確認方法を記載する。
確認結果	有効、一部不備、不備、対象外等の確認結果を記載する。
今後の対応事項	確認の結果、追加対応または改善が必要と考えられる事項を記載する。
対応予定	今後の対応事項について、対応方針、期限および担当部門等を記載する。
確認資料	取組状況を説明する上で主要となる確認資料を記載する。
確認資料開示手法	確認資料の開示可否や提示方法を記載する。

サービス提供形態別の参照目安が「NA」である場合でも、利用者の業務内容またはリスク特性によっては、当該項目を自己点検の対象とすることが考えられます。

3. ③確認資料管理台帳

「③確認資料管理台帳」は、「②セルフアセスメントシート」に記載した確認資料を登録・管理するための台帳です。

委託先は、確認資料名、証跡類型、関連する対応項目、所管部署、取得・実施サイクル、状態、開示区分および整備期日等を整理することで、委託元からの照会や第三者による確認に備えることができます。

主な利用方法は、以下のとおりです。

- ・ 自己点検に利用した確認資料を一覧化し、証跡の所在および管理責任を明確にする。
- ・ 確認資料ごとに「開示可」「抜粋開示」「非開示」等の開示区分を設定し、外部説明時の取扱いを明確にする。
- ・ 確認資料の取得・更新サイクルおよび整備期日を管理し、確認時点で有効な確認資料を提示できる状態を維持する。
- ・ 同一の確認資料が複数の確認観点に関連する場合に、関係する項目を横断的に管理する。

なお、「確認資料例」は、各項目について参考となる資料を例示したものであり、必ずしも記載された資料をすべて作成または提示することを求めるものではありません。

4. ④参照資料一覧

本表の確認観点は、特定の団体が独自に定めた枠組みではなく、既存の基準・ガイドラインおよび公開されている研究・調査の内容を、暗号資産関連業務の委託先管理という文脈に置き直して整理したものです。

「④参照資料一覧」は、その出所を利用者が確認できるようにすることを目的としています。

利用にあたっては、以下の点に留意してください。

- ・ 本一覧は、参考とした主な資料を掲げるものであり、関連する資料を網羅したものではありません。
- ・ 本一覧は、個々の確認観点と個々の資料との対応関係を示すものではありません。各確認観点は複数の資料の内容を踏まえて整理しており、特定の資料の記載をそのまま引き写したものではありません。

- 本一覧に資料を掲げていることは、本表が当該資料に準拠していることを示すものではなく、また利用者に当該資料への準拠を求めるものでもありません。
- 記載している版および所在は、本資料の作成時点のものです。最新の内容は、各発行元において確認してください。
- 会員向けに発出されている資料および作成・検討の過程にある資料については、所在の記載に代えてその旨を付しています。

5. 各シートの関連性

本表では、「①委託先管理のプラクティス一覧」を起点として、各確認項目の詳細を確認することができます。

委託先は、「②セルフアセスメントシート」に自社の確認状況および確認結果を記入し、取組状況の説明に使用する証跡を「③確認資料管理台帳」で管理できます。