リスク評価に基づくデジタルリポジトリ監査法

公開試験と意見募集用草案

Digital Repository Audit Method Based on Risk Assesment

Draft for Public Testing & Comment

DRAMBORA

作成：デジタル・キュレーション・センター（DCC）、デジタル・プリザベーション・ヨーロッパ（DPE）

第1.0版（草案）

公開日：2007年2月28日

日本語版公開日：2010年9月1日

DCC

digital preservation europe

オリジナル版についての目録記載事項

タイトル	Digital Repository Audit Method Based on Risk Assessment
作成者	Digital Curation Centre （DCC）
作成者	DigitalPreservationEurope （DPE）
件名	Information Technology; Science; Technology– Philosophy; Computer Science; DigitalPreservation; Digital Records; Science and the Humanities
備考	DCC/DPE *Digital Repository Audit Method Based on Risk Assessment* （DRAMBORA） provides a methodological framework, guidelines and audit tools to support the identification, assessment and managing of risks in a digital repository.
発行者	Digital Curation Centre （DCC） and DigitalPreservationEurope （DPE）
執筆参加者	Andrew McHugh
執筆参加者	Raivo Ruusalepp
執筆参加者	Seamus Ross
執筆参加者	Hans Hofman
作成日	28.02.2007 （creation）
種類	Text
形式	Adobe Portable Document Format v. 1.3
言語	English
著作権	© Digital Curation Centre Partners and DigitalPreservationEurope Partners

作成に関与した人々

<著者>
アンドリュー・マクヒュー、ライボ・ルーサレップ、シェーマス・ロス、ハンス・ホフマン

<オリジナル版刊行>
デジタル・キュレーション・センター（以下、DCC）、デジタル・プリザベーション・ヨーロッパ（以下、DPE）

<日本語版刊行>
国立国会図書館関西館電子図書館課

オリジナル言語：英語（2007年）

文書の版管理

版	作成日	更新履歴 （必要に応じ更新理由）	注釈者又は著者のイニシャル
1.0	2007年2月28日	初版刊行	AM、RR、SR、HH

著者略歴

著者のイニシャル	著者名	機関名
AM	アンドリュー・マクヒュー	DCC及びグラスゴー大学HATII
RR	ライボ・ルーサレップ	オランダ国立公文書館、DPE、エストニアン・ビジネスアーカイブ
SR	シェーマス・ロス	DCC、DPE、グラスゴー大学HATII
HH	ハンス・ホフマン	オランダ国立公文書館、DPE

1 要約

本文書は、DCC／DPE作成「リスク評価に基づくデジタルリポジトリ監査法」（以下DRAMBORA）の初版である。DRAMBORAツールキットの公式試験の各フェーズが終了し、それに対するパブリックコメントが寄せられた後、2007年から2008年の間に改訂版が発行される予定である。本ツールキットは動的なプロセスで作成されており、これはそうしたプロセスの第2段階に相当する。本ツールキットは、デジタルリポジトリの監査と認証についての基準、手段及び方法を考案するために進められている国際的な活動の中から生まれた最新の成果である。開発期間を通して目指されてきたことは、既存の活動を基礎とし、それらを拡張して補完するということであった。特に要求されたのは、単一のリポジトリ評価プロセスを確立するためのツールキットを開発するということであった。国際協力と協働の重要さ、意見の相違に起因する潜在的な危険性は、DCCとDPEがこの分野での作業を進める過程で、ごく初期の段階から認識されていた。

既に行われている同様の取組みのうち、最も注目に値するのは、信頼できるデジタルリポジトリの監査及び認証基準を開発するため、RLG／NARAタスクフォースとnestor（Network of Expertise in Long-Term Storage and Long-Term availability of Digital Resources in Germany）ワーキンググループの内部で行われた取組みであろう。さらに、研究図書館センター（CRL）の主導で重要な作業が実施されている。そうした取組みの成果は、本ツールキットの開発過程を通して、さらにはそれに先立ち、DCCの指導の下で実施されたパイロット監査において、最重要事項として検討されてきた。DCC／DPEワーキンググループは、保存リポジトリに関する基本的で客観的な基準を表す一連の原則について合意するため、他のグループの代表者たちと連携しており、そうした原則とそれらの基礎となる概念は、本ツールキットの中で非常に重要な位置を占めている。DRAMBORAに基づく自己監査は、チェックリストのどちらか又は両方を併用すれば実施しやすくなると思われ、逆もまた然りである。DRAMBORAというリスクに基づく手法は、リポジトリとチェックリストが要求する事項との照合作業に役立つ。監査人は、組織の事業背景とその暗黙のリスクを明確に認識して初めて、チェックリストの要求事項を効果的に利用することができるのである。本ツールキットは、そうしたリストを個別の状況に当てはめ、より効果的に適用することを可能にしてくれる。この他にも、広範な国際的情報基準等、さまざまな新しい情報源からアイデアや概念を取り入れ、適合化を図るための努力も行ってきた。それらの多くは、私たちがこれまでに各国で確立してきた全体像のさらなる拡大を目指すリスク管理業界を基盤としている。

2 目次

はしがき

「デジタルリポジトリ」という言葉は、さまざまな意味で使用される。あらゆるデジタル資料のコレクションについて、この言葉を用いる人もいる。多くの人々は、特定のプロトコルでメタデータを共有するデジタルコレクション（ePrintsのコレクションについて言う場合が多い）を指して、この言葉を使っている。非常に長期間にわたって理解可能な方法で保存されることになっているデジタル資料コレクションだけを指してこの言葉を使用する人もなくはない。開放型アーカイブ情報システム（OAIS）基準が当てはまるのは、この最後の例にほかならない。

OAISとは"an archive, consisting of people and systems, that has accepted responsibility to preserve information and make it available to a Designated Community ... [meeting] responsibilities defined in [the OAIS standard]"と定義されている[1]。このような信頼された（又は信頼できる）デジタルリポジトリの属性と、それらの監査に使用しうる基準を明らかにするための取組みが、ここ数年間にわたって継続されてきた。「信頼できる」という語は、ここでは専門的な意味で使用されているので、注意が必要である。

しかし、今日あるデジタルリポジトリの多くや、学術データの管理を支援するために利用されるデータベースやコレクションの大半について言えば、長期保存が明確に公的使命とされたり、それに必要な長期的な予算が組まれたりはしておらず、当面のアクセスと再利用の支援が義務づけられているに過ぎない。長期保存は、目的の1つであったり、少なくとも期待や希望であったりはしても、（現在のところ）責任とはされていないのが実情である。上述した属性や基準の多くは、このような大多数のリポジトリに対して配慮していないが、部分的には有用であるかもしれない。

本ツールキットは、長期保存を目指しているか否かに関わらず、すべてのリポジトリを対象とすることによって、既存のリポジトリ監査及び認証作業を補完することを目的としている。長期保存が全面的に義務づけられているデジタルリポジトリのような特定のケースでは、必要に応じてその他のツールやプロセスで本ツールキットを補強してもよいだろう。

クリス・ラスブリッジ
デジタル・キュレーション・センター所長
2007年2月28日

[1] ISO 14721:2003　宇宙データ・情報転送システムーオープンアーカイブ情報システムー参照モデル、shttp://public.ccsds.org/publications/archive/650x0b1.pdf（1.1　目的と範囲1-1）

3 序文

ここでは、デジタル・キュレーション・センター（DCC）とデジタル・プリザベーション・ヨーロッパ（DPE）が開発したデジタルリポジトリ監査ツールキットを紹介する。本ツールキットは、リポジトリの性能を評価し、弱点を特定し、長所を認識するための手段をリポジトリ管理者に提供することによって、内部監査を支援することを目的としている。デジタルリポジトリはまだ揺籃期にあり、このモデルは、状況の急速な展開に対応できるように設計されている。本ツールキットの開発は、DCCが各国立図書館、学術的データの所蔵機関、文化遺産データアーカイブ等、さまざまな組織で集中的にリポジトリパイロット監査を実施した後に行われている。DCCとDPEの提携による本ツールキットの開発が可能になったのは、これら協力機関がDCCによるパイロット監査を快く受け入れたことに負うところが大きい（付録1の謝辞参照）。パイロット監査は非常に有益で、組織のコンプライアンスやエビデンス（訳注：以下「根拠」という。）について、またリポジトリが信頼されるということ、信頼できるものであるということが、実際には何を意味するのかという問題について、示唆を与えてくれた。これらの試験監査を行うことによって、公式な評価手段を模索するに至った要因を理解する上での重要な洞察を得ることができた。

本ツールキットでは、信頼性が高く理解可能なデジタルオブジェクトがリスクに基づく監査手法の中心に据えられている。デジタル・キュレーションは、「制御可能な不確実性と制御不能な不確実性を管理可能なリスクの枠組みへと変容させるプロセス」と特徴づけられ、リポジトリのアクティビティ、資産、規制をめぐる状況に基づいて分類されている。そのため、本ツールキットでは、信頼性が高く、文脈、構文上及び意味論上理解可能なデジタル情報を受け取り、管理し、アクセスを提供する性能を妨害しうるリスクを回避し、抑制するために、リポジトリがあらゆる努力を払っているかどうかが明らかにされる。この監査ツールは、リポジトリの職員が各自のアクティビティの各段階で遭遇するリスクを識別して分類し、その発生確率の評価を行い、リスクが発生した場合の潜在的な影響を認識して、それらにどの程度対応できているかを検討するよう推奨している。こうした枠組みの中では実証が非常に重要である。リポジトリは、リスクを識別してそれらを適切に管理するだけでなく、内部だけであっても、そうしたことを行う性能を証明するよう期待される。

本ツールキットの主な利用者は、現在の活動の妥当性を確認し、性能強化のために最も効果的な資源の配置場所を体系的に知りたいと考えているリポジトリ管理者だろう。リポジトリの資金提供者、コンテンツ提供者、利用者は、リポジトリがデジタル資料のキュレーションプロセスに付随するリスクを効果的かつ効率的に管理していることを実証することを、ますます求めるようになるだろう。DRAMBORAツールキットは、そうした期待に応えるメカニズムを提供する。

本ツールキットは、厳密なベンチマーク法をも一意図、主にプロセスを実施する組織の具体的で主観的な目標に基づいた自己評価を実施するよう促している。監査人は、一連のインタラクティブなステージの全過程を通して、組織の目標と組織が準拠する法的枠組、そしてその結果、実施しなければならないアクティビティの包括的なイメージを創り出すよう求められている。こうした監査の出発点から、監査人は関係するリスクの一覧を作成するよう求

められ、識別されたリスクごとに、リスクの所有者（オーナー）、発現可能性と潜在的な影響のスコア、さらには、想定されている又は実施された回避、緩和及び処理手段等、多数のリスク属性を明らかにすることが求められる。このようにして作成されたリスク登録簿は非常に有用なツールであり、各組織は、その業務上の最優先課題を識別し、それらの解決のために効果的に資源を配分すると共に、目標全体に対するアクティビティの達成度を確認できるようになる。このプロセスを通して、各組織は、その後に行われる評価の要件を満たせるよう準備することができる。タスク自体は、外部主導の監査を行う前に必要となる準備作業とほぼ同じで、内部で実施した監査の結果が、外部監査人に対する重要な根拠となることがある。

リスクの解明・識別プロセスを容易にするため、リポジトリ機能の各クラス間に下位区分が導入されている。第1グループには、主にリポジトリのワークフローを重視した機能、すなわち真正で使用可能なオブジェクトの受入、保管、文書記録、提供という主要機能に関連する機能が含まれる。これらは、この監査ツールキットを利用するすべてのリポジトリ、アーカイブもしくはインフラにとっての基本機能である。さらに、組織の管理、人事、財務、技術インフラ、セキュリティに関連する副次的な機能クラスも定義されている。

組織が直面するリスクは、既に発生している事例に関連していることもあれば、発生していない事例に関連していることもある。これは、脅威という面から分類することができるが、この場合、リスク（及びそれに付随する悪影響）は発生と機会に分類され、後者の場合には、リスクは未発生と関連づけられる。本ツールキットでは、そうした状況はリスクの実行と記述される。内在的なリスクは、その位置づけによって特徴づけられ、計画、アーカイブ、コレクション又はアイテムの各段階で提起や管理が行われ、さらに細かい下位区分も適用される。外在的なリスクとは、御可能なパラメータを超えて発生するリスクを意味し、ある程度は緩和することができるが、制御可能な範囲が狭いため、一般的に不確実性の程度が高い状況にある。リスクがリポジトリにとって内在的か外在的かという位置づけを認識することによって、リスクの回避、緩和又は対応のための戦略にはっきりと現れているか否かに関わらず、リスク管理のためのメカニズムがわかる場合がある。

本文書は、次の7つの主要要素で構成されている。

- 第I部では、リポジトリの概念、リスクに基づく監査法の基本となる考え方、本ツールキットの開発の参考となった先行研究について紹介する。
- 第II部では、監査プロセスを提示し、監査の6段階について説明する。
- 第III部では、ツールキットのさらなる改善に関する展望や、その開発過程におけるコミュニティの関与への期待について説明する。
- 付録1には謝辞が記載されているが、多様な環境において各種デジタルリポジトリがどのように機能するかということや、それらの順調な運用に関わるプロセスをツールキット制作チームに理解する過程でコミュニティの関与は非常に大きな役割を果たしたため、このセクションも本文書の主要要素の1つである。
- 付録2には、自己監査の実施プロセスを支援する一連のテンプレートを収録した。
- 付録3は、リスクに関する思考を促進するメカニズムを監査人に提供することを目的としている。ツールキットの開発者の中には、リスク登録簿テーブルを例示すると、リスク

評価を行う際に、リポジトリがツールキットに含まれている例に容易にならってしまい、自己監査プロセスに不可欠な自己評価のレベルが低下すると考える人もいたため、当初、リスク登録簿テーブルは含まれないことになっていた。その場合、リポジトリは、各自が直面したリスクを表面化できず、組織を取り巻く特定の状況の中で特殊リスクやリスク固有の特性について考察しなくなるおそれがあった。熟考の末、リスク事例を含めると同時にオンラインツールを提供して、ツールキットの利用者がツールキットのリスク登録簿にリスク事例を追加したり、ツールキットに含まれているリスク登録簿の修正を提案したりできるようにした。リポジトリ運営に携わる人々と働いた経験から、着実かつ有益なリスク登録簿を開発するためには、コミュニティ全体で取り組むのが一番良いという結論に達したからである。

◆ 付録4では、監査報告書の有効な構成方法を例示する。

DRAMBORAツールキット本体は、第II部、付録2、付録4から構成される。

本文書の公開と平行して、DRAMBORAを利用した監査の実施組織を支援するオンラインツールを2007年3月30日に公開する予定である。

3.1 ツールキットの開発に関する提携

本ツールキットは、情報システム合同委員会（JISC）とコアeサイエンスの資金提供を受けた英国のDCCと、欧州委員会の共同出資イニシアティブであるDPEの提携によって開発された。2つの機関は、ツールキットの試験と改善、オンラインツール（http://www.repositoryaudit.euで入手可能）の管理、英国、欧州、さらにはその他の地域で最大限に普及させるため、今後も協力関係を維持していくことにしている。

3.1.1 デジタル・キュレーション・センター（DCC）とは

DCC[2]はJISCから資金提供を受けており、デジタル・キュレーションに関する専門知識と、デジタル情報の長期的な利用及び再利用が可能な蓄積、管理、保存に関するベストプラクティスの研究に焦点を合わせている[3]。このプロジェクトは、エジンバラ大学、グラスゴー大学人文学高等技術・情報研究所（HATII）、バース大学内の英国図書館・情報ネットワーキングオフィス（UKOLN）、研究評議会中央研究所評議会（CCLRC）の提携の下で運営されている。DCCは、全関係分野からの積極的な参加とフィードバックに大きく依存しているが、DCC自体はデータリポジトリではない。データキュレーションや長期保存に関するより広範な問題を扱う活発な研究プログラムから得た洞察に基づき、アウトリーチサービスや実用的

[2] http://www.dcc.ac.uk

[3] C. Rusbridge、P. Burnhill、S. Ross、P. Buneman、D. Giaretta、L. Lyon、M. Atkinson、 2005、'The Digital Curation Centre: A Vision for Digital Curation', In *Proceedings IEEE's Mass Storage and Systems Technology Committee Conference on From Local to Global: Data Interoperability and Technologies*
http://eprints.erpanet.org/archive/00000082/01/DCC_Vision.pdf

なサービスに関するプログラムを開発して提供し、デジタル・キュレーション問題に直面する人々を支援してきた。また、関連機関と重複するサービスではなく、その活動を補完又は貢献できるように努めている。

3.1.2 デジタル・プリザベーション・ヨーロッパ（DPE）とは

デジタル・プリザベーション・ヨーロッパ（DPE）[4]は、欧州委員会が共同出資した3年間（2006～2009年）にわたるプロジェクト（IST-2006-034762）で、欧州8か国から9つの機関が参加している。DPEは、欧州研究領域で既存の国家イニシアティブ間の連携や相乗効果を促進しており、現在の活動の中でデジタル資料の効果的な保存を保証するための調整、協力、整合性を改善する必要性に取り組んでいる。DPEのプロジェクトパートナーは、次のような活動で主導的な役割を果たしている。

- デジタル保存の認知度を高める。
- 欧州全域でデジタル保存に関するアクティビティの価値を高めるため、連携しいる欧州連合加盟国の能力を高める。
- 過剰な活動や重複を避けるため、部門横断的な協力を行う。
- デジタル保存プロセスに関する監査可能で認証された基準を確実に選択及び導入する。
- 研修パッケージを通して技能開発を促す。
- 関連する研究の調整や情報交換を行えるようにする。
- 研究課題のロードマップを作成し、促進する。
- 市民にも専門家にも、各自の生活や仕事の中でデジタル保存が果たす中心的な役割が認識されるよう、支援する。

DPEの成功は、デジタル資料の長期的な管理に必要なプロセス、アクティビティの相乗効果、システム及び技術に関する共通の知識基盤の確立に役立つだろう。リポジトリ間の連携を支援するメカニズムと、各自が実現可能な最高水準の活動を行っていることを確認できるようにする監査の開発は、いずれもDPEが携わっている中心分野である。DPEは、第5次枠組みプログラム[5]の下で欧州委員会の支援を受けている重要な保存イニシアティブであるERPANETの成功を基礎としている。

4 第I部 監査法の背景

4.1 デジタルリポジトリの作業環境

情報環境のさまざまな分野で「リポジトリ」と呼ばれるコンテンツコレクションの範囲が広がりつつある。言葉の使用範囲が広がるにつれ、意義の多様化も進んでいる。JISCの委託

[4] http://www.digitalpreservationeurope.eu

[5] http://www.erpanet.org

より行われた最近の調査では、次の特性によって、デジタルリポジトリをその他のデジタルコレクションと区別すべきだという提案が示された[6]。

- コンテンツが、作成者、所有者または第三者等によってリポジトリに提供される。
- リポジトリは、コンテンツとメタデータを管理できるような構造になっている。
- リポジトリは、受入、入手、検索、アクセス制御等、最小限の基本サービスを提供する。
- リポジトリは、持続可能で信頼でき、十分なサポートや管理が行われていなければならない。

研究図書館グループ（RLG）によって最初に提案され、しばしば引用されるデジタルリポジトリの一般的な定義では、デジタルリポジトリは次のように定義される[7]。

「デジタル資源の長期的な管理と、コンテンツ提供者及びリポジトリが合意したコミュニティへのそれら資源の提供とに責任を負う組織。」

オープンアーカイブ情報システム（OAIS）参照モデルでは、アーカイブは、特定のコミュニティによるアクセスと利用が想定された情報の保存を目的として運営される組織と定義されている。「信頼できるデジタル・リポジトリの認証のための基準：監査チェックリスト（TRAC Criteria for Measuring Trustworthiness of Digital Repositories and Archives: Audit Checklist）」（2007年2月刊）におけるデジタルリポジトリの概念は、OAISによるアーカイブの定義（「長期的なデジタル資源の保存に責任を負う組織」）に基づいている。

DCCが実施した試験評価では、貴重なデジタルコレクションを持つすべてのリポジトリが一様であるわけではなく、同じ目的又は類似のサービスを提供するために設置されたわけでもないという理解を裏付ける根拠が集まった。リポジトリは、電子図書館、研究、学習、eサイエンス、出版、データの商業利用、記録管理、保存等、さまざまな実践分野の重要な交差点となっている。そうした分野ではリポジトリの設置に対するモチベーションが異なっており、リポジトリが提供しうる主要サービスが、次のいくつかの機能領域にまたがる場合もある。

- 資源へのアクセスの拡充
- 新しい出版及びピアレビュー方法
- 情報の共同管理（記録及びコンテンツ管理システム）
- データの共有（研究データ、学習用素材等の再利用）
- デジタル資源の保存（長期的）

そのため、このデジタルリポジトリ自己監査ツールキットは、あらゆる規模のさまざまな目的を持ったデジタルリポジトリで広く利用できるように工夫されている。2007年1月、研究図書館センター（CRL）[8]は、リポジトリの監査、認証、認定を支援するメカニズムや基準の開発プロジェクトの関係者による会議を主催した。この会議の成果として、使命、ビジネス

[6] Rachel Heery、Sheila Anderson、*Digital Repositories Review*（2005）、p.2
[7] Cf. http://www.bl.uk/about/strategic/glossary.html
[8] http://www.crl.edu

モデル、財源の如何に関わらず、すべてのデジタル保存リポジトリが遵守すべき一連の共通基準が作成された。それは次のようなものである。

1. 特定のコミュニティのためのデジタルオブジェクトの継続的な保存を責務とする。
2. 責務を履行するための組織としての適合性（財務、人事、構造、プロセス等）を備えている。
3. 必要な契約及び法律上の権利を取得、維持して、責任を果たす。
4. 効果的で効率的な方針の枠組みを持っている。
5. 各リポジトリの責務と能力に応じて明確に規定された基準に基づいてデジタルオブジェクトを収集し、受入れる。
6. 保持しているデジタルオブジェクトの完全性、真正性、有用性を長期にわたって維持／確保する。
7. 保存の過程でデジタルオブジェクトに講じられた措置及び関連する作成、アクセス支援、保存前の使用プロセスについて必要なメタデータを作成し、保存する。
8. 必要な提供要件を満たす。
9. 保存計画及び保存のために行われる措置に関し、戦略的なプログラムを持っている。
10. デジタルオブジェクトの継続的な保存とセキュリティに適した技術インフラを持っている。

上記の10原則の根元にある重要な前提条件は、リポジトリの種類や規模が多様化すると予想されるため、保存要件は各リポジトリが対象とする特定の一つ又は複数のコミュニティのニーズと手段に合わせて決定されなければならないということである。

収集、保存、提供を主業務とする機関が運営するリポジトリとまったく異なる使命を持った大規模な組織の一部として運営されているリポジトリも、はっきりと区別すべきである。こうした分類は、リスク分析及びリスク管理という面で重要になる。独立した組織として運営されているデジタルリポジトリ（主題別データセンター等）は、リポジトリ作業のすべての側面に責任を負い、リスク管理手段の全領域を明らかにしなければならない。大規模な組織の１ユニットとして存在するデジタルリポジトリ（製薬会社のデジタルデータ収集部門等）は、所属機関にその機能の一部を委任したり、リスクの一部を移転したりすることができる。ただし、後者の場合は、実際のリポジトリ作業という面だけでなく、より広範な組織の目的を達成する上でのリポジトリの役割という面からもデジタルリポジトリの使命や目的を明確にし、検討しなければならないだろう。

実際の監査におけるこうした状況の違いをサポートするため、DRAMBORAには、デジタルリポジトリのアクティビティについて、合計8つの大まかな「機能クラス」が定義されている。それらは「作業機能クラス」と「サポート機能クラス」というグループに分けられ、前者にはデジタルリポジトリの主要機能である「収集と受入」「保存と蓄積」「記述とメタデータ管理」「アクセスと提供」が含まれ、後者にはどこの組織にもある「組織と管理」「人事」「財務管理」「技術サポートとセキュリティ」が含まれる。監査人は、リポジトリの重要なアクティビティと資産を明らかにし、それらに関連するリスクを識別する際に、どの業務領域で直接の責任を負うのかという点についてより柔軟に選択できるようになるだろう。リポジトリ事業の主要資産、すなわちリポジトリで保存するデジタル情報は、確実で安全な技術インフラに依存するところが大きいため、最後に挙げた機能クラスは、デジタルリポジ

トリにとって比較的重要性が高い。

序文の項で述べたように、この監査ツールは、リポジトリの職員が各自のアクティビティの各段階で遭遇するリスクの識別と分類を行い、その発生確率と潜在的な影響について評価を実施し、リスクへの対処方法の効果を検討するよう奨励している。根拠が非常に重要とされ、リポジトリは、リスクを識別してそれを適切に管理するだけでなく、たとえ内部に対してだけであっても、各自のリスク管理能力を実証するよう期待される。

4.2 リスクに基づく監査法の導入

リスク管理は、新しい概念ではない。あらゆるレベルでの優れた管理と意思決定に不可欠な要素である。すべての組織が、気づいているか否かに関わらず、リスクを継続的に管理しており、より厳格かつ体系的に行う場合もあれば、緩やかに行う場合もある。環境保護や公衆衛生及び安全、事業の継続、情報システムのセキュリティ等の分野では、より厳格なリスク管理が非常に目に見える形で行われている。

リスク管理は、長い時間をかけて明確な専門分野へと発展してきた。リスク管理戦略を採用することによって、組織はその規模や官民の別に関わらず、損失を防止して業績、製品及びサービスの質、安全性を改善することを学んできた。リスク管理システムは、既存の経営情報ツールやシステムを補完するツールとして登場し、主要事業機能、資産管理及びプロジェクトに関してあらかじめ設定された目標や戦略の達成という面で、組織を支援することができる[9]。

「オーストラリア／ニュージーランドリスク管理基準」（AS/NZS 4360:2004、p.V）では、リスク管理が、次のように説明されている。

> *損失を最小化しつつ利益を実現する機会の適切なバランスを達成するための管理。*[中略]*連続的に実施されれば、意思決定の継続的に改善でき、継続的な業績の改善を促進するステップで構成された反復的なプロセスである。*
>
> *リスク管理業務には、適切なインフラとカルチャーの確立、状況を確認する論理的で体系的な方法の適用、組織が損失の最小化と利益の最大化を実現できるような方法でのアクティビティ、機能又はプロセスに関連するリスクの識別、分析、評価、処理、モニタリング、伝達等が含まれる。*[中略]*組織がリスクを効果的かつ効率的に管理していれば、組織の目標を達成しやすくなり、それに伴う総コストも抑えることができる。*

リスクの概念は、脅威、危害、損失、及びその他の否定的な影響という面から語られることが多い。組織を取り巻く一般的な状況の下では、不確実性の結果にさらされること、あるいは計画又は予想からの逸脱の可能性としてリスクを捉えた方が有益である。

[9] Victoria Lemieux、*Managing Risks for Records and Information*（2005）、p.2

優れたリスク管理によって、ステークホルダーたちは、組織のコーポレートガバナンスや説明責任、実現能力への信頼を深めることができる。組織の目的が何であれ、その目標を実現する過程は不確実性に包まれている。不確実性は、成功への脅威になると同時により大きな成功への機会を提供してくれる。リスクとは、行為や事象から生じる結果のこのような不確実性を指し、不確実性は、機会でも脅威でもありうるのである。リスクの評価は、何かが発生する尤度と、実際に発生した場合に生じる影響との組み合わせという点から実施されなければならない。リスク管理には、リスクの識別と評価、そしてそれらへの対応が含まれる[10]。

リスク管理は、通常、独立したいくつかの段階で構成されたサイクルとして表される。各段階は、階層的に並べることができる[11]。

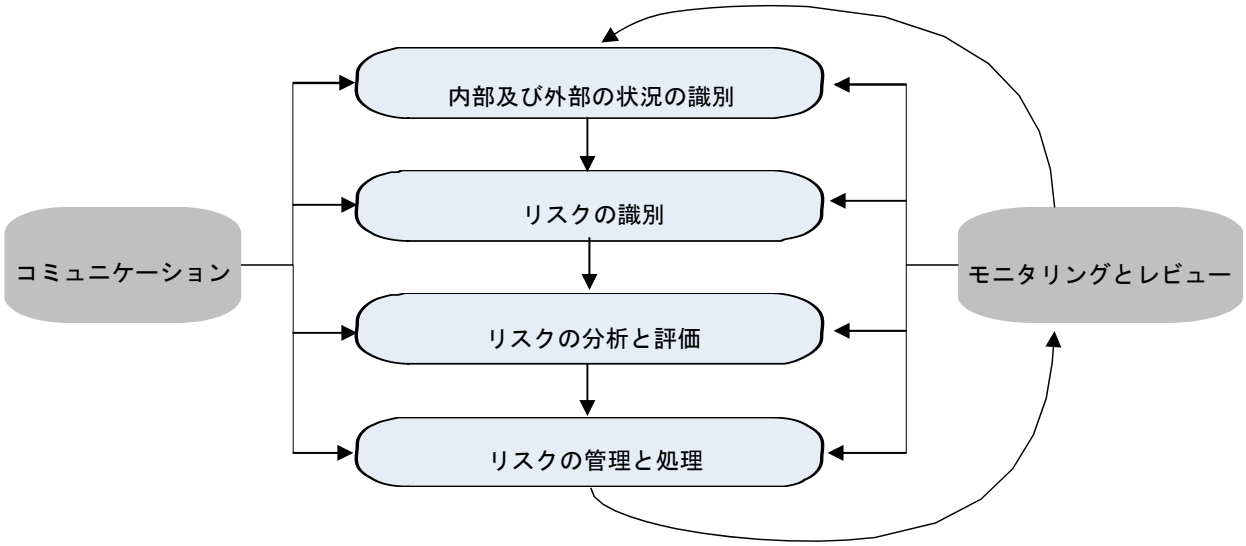


図1：リスク管理段階の階層的序列の例

あるいは、リスク管理アクティビティを円で表し、各段階で関与するステークホルダーが異なることを示すこともできる。

[10]英国財務省、*Orange Book. Management of Risk – Principles and Concepts*（2004）、p. 7
[11]又はAS/NZS 4360:2004、p.9等を参照。

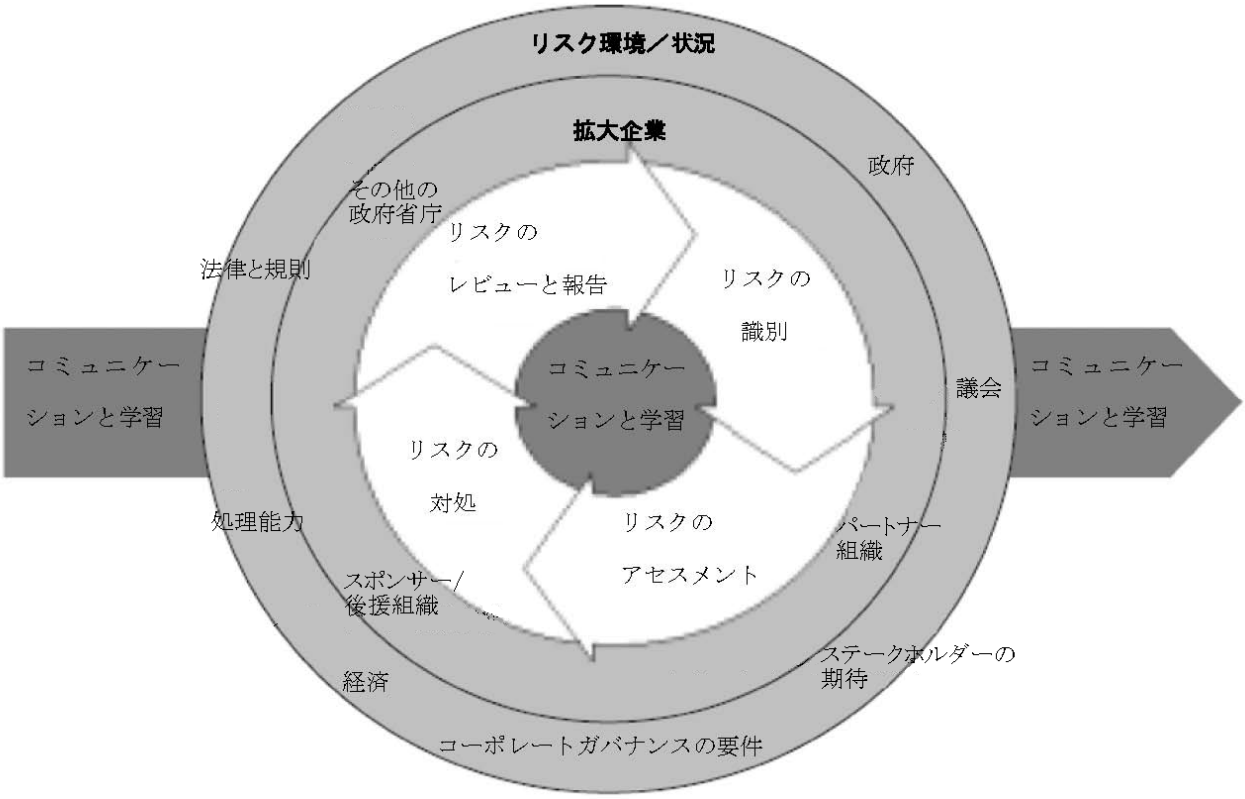


図2：リスク管理モデル（出典：Orange Book. *Management of Risk--Principles and Concepts* © Crown copyright 2004）

リスク管理の実行段階には、次のようなものがある。

- リスクを管理しなければならない状況の識別
- リスクの識別
- リスクの評価
- リスクへの対処及び管理方法の明示

リスク管理とは、先を見越して行動するということである。リスクとは、悪い結果が起こる可能性にさらされることを意味する。リスク管理とは、勝算を高める、つまり良い結果が得られる確率を上げて悪い結果が生じる確率を下げるために慎重な措置を講じることを意味する。リスク管理に利用できる資源には限りがあるため、リスク評価に基づいて優先順位が決定されたリスクに対し、最適な対応をすることが目標となる。リスクは避けることができず、各組織が許容可能なレベルで正当化しうる方法で、リスクを管理するための措置を講じる必要がある。許容可能かつ正当と判断されるリスクの程度は、「リスク選好度」と呼ばれる。

今日では、デジタル保存は、真正なデジタルオブジェクトの有用性の維持をめぐる不確実性を定量可能なリスクに置き換えることを目的としたリスク管理方法と定義されることが多い。デジタルリポジトリは、真正なデジタル情報へのアクセス提供性能を阻害するリスクを緩和するため、あらゆる手段を尽くすということを目的としている。リポジトリ業務の成功は、リポジトリが利用者に提供する情報の「質」によって測られる。

4.3 本取組みを促進する周囲の情況状況

4.3.1 リスクとデジタル保存

リスク問題は、デジタル・キュレーション及びデジタル保存という文脈の中でさまざまな観点から検討されてきた。たとえば、特定のファイル形式に関連するリスクを分析するため、種々の研究が行われているが、リスクは、デジタルファイルや記憶媒体の有用性の維持に関連する技術的な課題に基づき、デジタルリポジトリの作業に固有のものとして認識されてきた。最近の成果として、数人の著者がデジタル保存に付随する固有の不確実性について説明している（Ross[2006]、Ross and McHugh[2006]等）。したがって、リポジトリのタスクは、状況の不確実性を識別して評価を行い、測定可能なリスクに換え、それらに効果的に対処し、緩和することができる手段を明示して実施することにある。リスクが技術だけでなく、組織、人事、システムに関連しており、デジタルリポジトリが運営されている環境に起因する外部要因に関連しているということは、容易に見て取れる。他の組織と同様に、デジタルリポジトリも、一般的な管理業務とデジタル・キュレーションやデジタル保存等を内容とする主要業務の両面において、リスク分析及びリスク管理のための手法から利益を得ることができる。

2003年、ERPANETプロジェクトは、「リスク・コミュニケーション・ツール（Risk Communication Tool）」[12]を発表し、「デジタル保存は、経済的にも技術的にもまだ成熟しておらず、十分な経験や根拠の欠如が問題となっている」と主張した。そのため、このツールは、デジタルリポジトリが次の各項を実施できるよう、助言を与えることを目的としていた。

- 各組織の中で、どのようなデジタル資源がリスクにさらされているかを明らかにする。
- そうしたデジタル資源がどのようなリスクにさらされているかを明らかにする。
- デジタル資源への脅威によって組織がさらされているリスクを明らかにする（世評、業務停止等）。
- リスクの分類と優先順位付けを行い、それらの管理に役立てる。
- リスクの各分野に関する組織内のコミュニケーションを促進する。
- リスク管理戦略の開発を促す。

リスク分析法はウェブサイトの保存という場面でも利用されており、コーネル大学図書館は、ウェブ資源の変化を長期にわたってモニタリングし、評価するため、リスク管理モデルを採用している。コーネル大学図書館バーチャルリモートコントロール（VRC）ツール[13]は、ウェブ資源の長期存続の可否を決める重要な指標の存在又は欠如に基づき、損失の確率を予測するために開発された。VRCツールはリスク管理の原則や記録管理の基本原則に則っており、ウェブ資源を選定、モニタリング及びキュレーションする際に組織が実施すべき一連の作業段階が設定されている。

[12] http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf
[13] http://irisresearch.library.cornell.edu/VRC/methods.html

4.3.2 既存のリポジトリ監査法

今日までに行われてきた主な監査・認証の取組みのうち、よく知られたものにRLGや米国国立公文書館・記録管理局（NARA）[14]及びnestor[15]の活動がある。これらは、DRAMBORA開発の下地となる基礎調査を実施する際の出発点になった。これらの取組みでは、成功を収め、また信頼を得たリポジトリを特徴づける主要基準を明文化したチェックリストの作成に重点を置いている。最近TRACと改名されたRLG／NARAデジタルリポジトリ及び認証タスクフォースの研究は、重要なデジタルリポジトリ評価手法の開発につながった。この研究は、デジタルアーカイブの監査と認証のためのプロセスと方法を開発するため、CRLの指導の下で行われたデジタルアーカイブ認証に関するプロジェクトにアンドリュー・W・メロン財団が支援を行うきっかけにもなった。DCCは、当初、CRLと連携して監査活動手法の開発を行っていた。

4.3.3 DCCのパイロット監査プログラム

2006年4月から2007年1月にかけて、DCCは、保存用リポジトリに最適な監査法を見極め、RLG-NARA及びnestorの作成した監査チェックリストの適用可能性と安定性を評価するために、一連のパイロットリポジトリ監査を実施した。その主な目的は、リポジトリがチェックリストの基準に十分に適合していることを実証できる根拠について理解することにあった。

合計5件のリポジトリがこの活動に賛同し、参加した。その際、重要な要件とされたのは、この活動から導き出される原則と結論とが非常に代表的なものであると担保できるだけの多様性を、対象機関が示しているということであった。監査を受けたリポジトリには学術データの所蔵機関、国立図書館、文化遺産アーカイブが含まれており、多様性は間違いなく実現されていた。しかも、これは非常に国際的な活動、3つの大陸から5つの組織が参加していた。規模の多様性も達成されており、参加リポジトリの運営予算は数千ポンドから800～900万ポンドまでさまざまであった。

最初に監査対象となった機関は研究評議会中央研究所評議会（CCLRC）の英国大気データセンター（BADC）である。BADCは、自然環境研究会議（NERC）の資金提供を受けた研究の成果として、大量かつ複雑なものを多く含むデータのキュレーションに責任を負っており、多数の気象学者に信頼されている。続いて、オックスフォード大学に設置されたビーズレーアーカイブ（Beazley Archive）の監査が行われた。1970年代後半に創設されたこの陶器及び宝石用原石のデジタルイメージ並びに関連データのデータベース・コレクションは、学者を中心とする大規模なユーザー基盤にサービスを提供しているが、そのコンテンツの質は高く、ロンドンを拠点とする大手オークション会社にもよく利用されている。次に監査の対象となったのは、英国国立データセット・デジタルアーカイブ（NDAD）である。英国国立公文書館と契約を結んでおり、英国の行政官庁が作成したデータセットの保存と提供に責任を負っている。その後、ニュージーランド国立図書館が提唱した国家デジタル遺産アーカイブ（The National Digital Heritage Archive）の公式監査が実施され、ニュージーランドのデジ

[14] http://www.rlg.org/en/page.php?Page_ID=20769
[15] http://nestor.cms.hu-berlin.de/tiki/tiki-index.php?page=wg-repositories

タル記憶を収蔵するリポジトリを創設する野心的なプロジェクトが完了するまでの暫定システムとの比較等が行われた。最後に、フロリダ州立大学の各図書館で作成されたデジタル資料の長期保存アーカイブサービスの提供を目指すフロリダ図書館自動化センター（The Florida Center for Library Automation）のフロリダ・デジタル・ライブラリ（The Florida Digital Library）で監査メカニズムが適用されたが、その頃までには、この監査メカニズムはかなり確立されていた。

監査結果は、一連の監査報告書（Ross and McHugh、近刊a）に既にまとめられているか、あるいは公開までにはまとめられる。結論の詳細は、Ross and McHugh（2006）とRoss and McHugh（近刊b）[16]にまとめられている。

DCCによる監査で使用された既存のツールには、実際の適用性という面で問題があることがわかった。現時点では、それらのツールには、組織のコンプライアンスの程度や効果を測定するための測定基準が存在しない。そのため、規模、事業範囲、又は使命の点で異質なリポジトリの比較及び評価を行うための信頼できる方法を考案するのは、依然として困難な状況である。デジタルリポジトリ監査の方法論や基準に関する国際的な合意が達成されることこそが、最も重要な成果として期待されている。DCC／DPEの研究は、リポジトリ評価のための直接的な代替（したがって競合）手段を提示することではなく、TRACとnestorのいずれの活動とも連携して利用できる補完的な手法を提供することを目指している。

こうした手法は、特定の基準に基づく最良事例基準又はベンチマークの包括的なリストを示そうとするものではない。本ツールキットは、デジタル保存分野の内外で実施されたリスク管理に関する研究を基礎とし、当該組織の中核となる特性やアクティビティに基づいて分類された一連のタスクを通して、監査人に指針を与えてくれる。さらに本ツールキットは、リポジトリの管理者と職員が各組織の業務の継続性という点で最も重要な意味を持つリスクを識別し、リスクを予測、回避、緩和、処理できるような対処法を明らかにするとともに、内部でしか必要とされない場合でも、こうした評価の結論が検証可能であることを確認するため、適切な根拠書類を保管するよう奨励している。用途の広いツールで、リスクへの積極的なアプローチと受動的なアプローチのどちらにも対応しており、リポジトリ内でのデジタル保存やキュレーション戦略の開発又は効果の確認という面では、非常に重要な出発点となる。

4.4 リスクに基づく自己監査法の原則

自己監査の成功は、プロセスを実施する組織がどれだけ真剣に関与するかという点に大き

[16] Seamus Ross,Andrew McHugh, *The Digital Curation Centre Repository Pilot Audits: Results and Lessons* （近刊a）.
Seamus Ross、Andrew McHugh,*Preservation Pressure Points: Evaluating Diverse Evidence for Risk Management*,（近刊b）.
Seamus Ross, Andrew McHugh, *The Role of Evidence in Establishing Trust in Repositories.*
D - Lib Magazine, July/August, vol. 12, nos 7/8 (Also published in *Archivi e Computer*, August 2006),
http://www.dlib.org/dlib/july06/ross/07ross.html

く依存する。目的やアクティビティ及びそれらに伴うリスクの識別プロセスを容易にするツールキットの潜在的なタスクを設計するため、あらゆる努力が払われてきた。本ツールキットは、内部監査プロセスを促進する仕組みとして有用であると思われる。監査プロセスで提出された回答に基づき、勧告が提示される。リポジトリの一次的な価値は、監査プロセスの実施自体から、さらには主要成果物となるリスク登録簿や関連報告書の作成から発生する。

上述のように、このツールにおける成功と失敗は、単一の客観的に定義されるベンチマークとは対応していない。代わりに各リポジトリが、それぞれの業績予測に基づいて成功の尺度を決定しなければならない。このツールの目的は、監査人がアクティビティやその他の作業で発生したリスクに注目しつつ、そして最終的にはすでに監査プロセスを実施したその他の類似組織からもたらされた回答に注目しつつ、一連の包括的な対応をとるようにするということにある。ただし、本ツールキットは規範的なものではなく、単に特定の自己監査組織に関連しうる問題を提示してくれるに過ぎない。各組織の状況を明示し、それをアクティビティや内部分析の過程で識別されたリスクに当てはめ、外部の情報源に照会してこれらの作業を補完することによって、この監査ツールキットは、もしこういったことをしなければ見落としていたかもしれない問題を捉えるメカニズムとなる。本ツールキットは、監査人が一連の包括的な対応策を策定し、有意義な組織の全体像を描いていく上で役立つだろう。自己監査プロセスを実施する組織が増えるにつれ、特定の種類の組織が直面した具体的なリスクに関する理解を深めていくことができる。自己監査を行ったリポジトリは、その公的使命、資金、規模、コレクションの種類、地理的位置に基づいて分類され、ツールのインタラクティブな要素の改善が進むにつれ、こうした情報を利用して、類似又は比較可能な組織の評価プロセスにおける焦点をより明確に絞り込めるようになるだろう。リポジトリはこの文書を使ってオフラインで監査を行うことができるが、http://www.repositoryaudit.euで入手可能なツールキットを使ってオンラインで実施することが望ましい。オンラインで提供されるツールは、監査報告書の作成を支援するだけでなく、デジタル・キュレーションに付随するリスクへの理解を深めることを目的とした国際的な活動に利用者が貢献できるようにする機能も備えている。オンラインツールの利用者は、匿名での報告書やリスクテーブルの作成と、DCC／DPEリポジトリリスクデータベースへの追加を選択することによって、監査ツールの改善を支援することができる。

ツールキットの直接的な価値は、自己監査を行う組織の内部にもたらされる。自己監査プロセスを簡単に見直してみると、この監査ツールキットには、当然のことながら、リポジトリがプロフィール及びリスクテーブルに不完全な又は誤った回答をしたり、リポジトリが直面している個々のリスクが適切に管理されている、又はリスク回避又は処理戦略が確立され、適切に実施されているというような誤った結論を下すのを止める機能はないということがわかる。「リポジトリがリスクに基づく自己監査ツールキットを現実的かつ合理的に適用している」か否かということ自体がリスクの1つであり、その他のあらゆるリスクと同様に、識別され、管理されなければならない。最近（2006年4月～2007年1月）のDCCによる監査では、ほとんどのリポジトリにとって、監査メカニズムを求める主な理由は、各リポジトリが成功を収めている分野と、改善の余地があり改善しなければならない分野について、組織内部の考え方を確立するためであるということが明らかになった。これらの目的を達成するため、この手法においては、誠実で完全な回答をするという組織の決意が前提とされている。した

がって自己改善の意欲があるリポジトリと、単に潜在的な外部パートナーや顧客に見せる保証が欲しいだけのリポジトリは区別される。ただしツールの対外的な価値が否定されるわけではまったくなく、自己監査プロセスは、外部監査人を迎え入れる前にリポジトリが実施しなければならない作業を反映するように計画されている。組織の自己認識を示す文書、すなわち「根拠」の提示を求めるツールキットの要求に応えることによって、その後の外部機関による監査プロセスは大幅に簡素化されるだろう。同様に、DCCによるパイロット監査プログラムでは、リポジトリの長所と短所への理解を構築する過程で、組織のリスク登録簿が持つ価値についての信念が確認された。

自己監査プロセスのもう1つの落とし穴は、単に組織が直面したすべてのリスクを集めてリストを作成し、リポジトリに関連するリスクが少ない方が成功の度合いが大きいと考える可能性があるということである。後者の仮説は誤っており、後述のように、本ツールキットはリスクを管理する手段であって、リスクを数える手段ではない。直面しているリスクの数が少ない組織の方が本質的に能力が高いということを示唆するものではない。重要なのは、組織がどれだけリスクを識別、回避、処理する能力を持っているかということである。同様に、あるリスクが客観的に他のリスクより深刻だということはない。個々のリスクの発生しうる可能性とその潜在的な影響は必ず変化するものであり、最も大きな成功を収めるリポジトリは、件数に関わらず、直面したすべてのリスクの発生しうる可能性と潜在的な影響を減少させる能力を示したリポジトリだということになる。

自己監査を適切に実施することができた場合、各組織は、次のような成果を期待できる。

- 各リポジトリの使命、目標、目的や、それらに固有のアクティビティと資産に対する包括的で文書化された自己認識が確立されている。
- リスクの種類とリスク間の関係に基づいて分類され、各リスクの所有権（オーナーシップ）、発生確率、潜在的影響という面から詳しく記述された詳細な関連リスク登録簿が作成されている。
- 組織の成功と欠点に対する内部理解が生まれ、最大の緊急課題に対処するため、効果的に資源の配分や再配分を行えるようになる。
- 今後、TRAC、nestor又は新しいCCSDSデジタルリポジトリ監査基準のいずれの基準に基づく外部監査であっても、そのための準備が整っている。

4.5 監査結果の測定

自己監査プロセスでの成功を完全に定量化するのは依然として困難だが、関連する影響及び確率指数を使ってリスクを定義することによって個々のリスクの深刻度を表すことができ、その結果、特定の組織環境の総合的な危険性を表すことができる。

上述のように、文書化されたリスクの数が少ないからといって、組織の能力が高いとは限らない。直面しているリスクの数とリポジトリの能力とはほとんど関係がなく、むしろ直面

している個々のリスクの確率と影響だけを考慮しなければならないのである。そうした数値は自然発生確率と影響を考慮した後、組織が実施している回避及び処理メカニズムを考慮して決定される。たとえば、主要職員を失うリスクは、何も対策をしなければ非常に尤度が高く、壊滅的な影響を与える可能性があると考えることができよう。しかし、リポジトリは、職員の給与や雇用条件を他の類似組織より優遇することで回避措置を講じることができ、またリスクが現実化した時に残りの職員の内部での配置換えで対応できるように十分な（実際には複数職種に関する）訓練を施しておいたり、離職する職員の役割のあらゆる側面を詳しく文書化しておいたりといった処理メカニズムを導入することもできる。

5 第II部 DCC／DPE監査ツールキット

5.1 自己監査ツールキットの概要

自己監査ツールキットの目的は、監査人による次の作業を支援することにある。

- リポジトリの各機能の公的使命と適用範囲の定義
- リポジトリのアクティビティと資産の識別
- 公的使命、アクティビティ、資産に関連するリスクと脆弱性の識別
- リスクの評価と算定
- リスク管理手段の定義
- 自己監査に関する報告

自己監査ツールキットは、2006年に実施されたDCCパイロット監査の経験に基づき、外部監査人がリポジトリの活動を検証・分析する際に利用するのと同様の手順に従って、自己監査における監査人を支援できるように設計されている。監査人ができるだけ簡単に自己監査プロセスを実施できるよう、自己監査ツールキットの第2版は、インタラクティブなウェブベースのツールになる予定である。このツールには、半自動化されたワークフローメカニズムや記入済みのフィールドからの選択、例や提案、比較等の形式の教材が用意されている。本文書で説明しいるツールキットは、インタラクティブなオンラインツールの基礎となっている。

5.2 自己監査プロセスの要件

監査プロセスは、監査を実施する個人の誠実さ、有能さ、能力に大きく依存する。監査プロセスから最大限の利益を得るため、各組織は、監査人や監査チームを慎重に選ぶ必要がある。個人又はチームが組織内で適切に配置されていることを確認するだけでなく、彼らに適切な根拠資料が提供されるようにすることも不可欠である。

5.2.1 監査人の特性

監査人協会（The Institute of Auditors）は、監査人の役割を次のように定義している。

「内部監査とは、価値を付加し、組織の業務を改善するよう計画された独立的、客観的な保証及びコンサルティング活動である。内部監査は、組織がリスク管理、統制、ガバナンスプロセスの効果を評価し、改善するため、体系的で規律正しい手法を導入して、その目的を達成できるよう支援する。内部監査では、情報の信頼性と完全性、政策や規制の遵守、資産の保護、経済的で効率的な資源の利用、所定の業務目標及び目的がレビューされ

る。」[17]

自己監査プロセスの実施に関しては個人が主たる責任を負うとするのが普通だが、上述のように、組織全体がプロセスに投資し、参加するということが肝要である。組織内の重要人物の監査プロセスへの参加が、監査の成功に貢献する。主たる監査人は、組織内からあらゆる適切な協力が得られるように働きかけ、それを獲得し、適切な評価が行われるようにする責任を負う。内部でのプロセスの信頼性を高め、結果が正しく完全であると見なされるようにするため、各組織は、監査人が適切な訓練を受け、適切な個人的技能を備えていることを確認すべきである。

5.2.2 個人的特質

ISO 19011「品質及び／又は環境マネジメントシステム監査のための指針」は、監査人が身につけ、体現すべき理想的な特性がわかりやすく示されている。

- 高度な倫理基準
- 寛容性
- 交渉力
- 卓越した観察力
- 明敏さ
- 融通性
- 粘り強さ
- 決断力
- 自信

5.2.3 組織内での位置づけ

理想的な監査人は、組織の中心にあって、リポジトリの業務のできるだけ多くの側面に影響力又は責任を持つような人物である。特定の業務上の目的やアクティビティに関する深い理解よりも、知識の広さを優先すべきである。監査人は、適度に上級の役割を担い、組織内で同僚たちの関わりを促進できる程度の信頼度があり、広範な内部文書にアクセスできることが望ましい。監査の期間中、監査人には、全面的なシステムアクセス権が与えられるべきである。

5.2.4 根拠の要件

監査ツールには、根拠として示されるべきさまざまな文書類が記述されている。これは、組織は各自のリスクを効果的に管理する能力を持つことを実証できなければならないという信念を反映している。リスク回避又は処理手段は、公式の文書を根拠としているか、そこに記録されている場合でなければ、真剣に考慮されない。しばしば利用されうるソースとして

[17] The Institute of Internal Auditors, *Code of Ethics*

は、組織の公的使命や任務を明記した文書、寄託契約書の雛形、職務説明書、組織図、職員の履歴書、事業計画及び年次会計報告書、方針書及び手続きマニュアル、ワークフロー文書、技術アーキテクチャー計画、保守報告書、公開されているその他の監査の結果等がある[18]。そのうち、リスク管理手段のために最も有用なのは、方針や手続きに関する文書であろう。まもなく公開予定のTRAC認証チェックリスト（2007年2月刊行）には、すべてのリポジトリにとって最低限必要な方針書のリストが付録として添付されている。監査人は、監査プロセスを開始する前にこれらの各文書（又は同等の文書）をまとめておくことが望ましい。リストには、次の項目が含まれる。

- 緊急避難措置、継承計画又はエスクロー（第三者寄託）計画（状況に応じ、これらのうちのいずれか）
- コミュニティの定義とサービスレベルに関連する方針
- 法的許可に関連する方針
- フィードバックの取得と利用に関連する方針と手続き
- 財務手続き
- 権利侵害に関連する方針／手続き
- 受入に関連する方針／手続き
- 保存戦略
- 保管／マイグレーション戦略
- アクセス行為の記録に関する方針
- アクセスに関する方針
- 媒体変換プロセス
- 変更管理プロセス
- 重要変更試験プロセス
- セキュリティ更新プロセス
- ハードウェアへの必要な変更のモニタリングプロセス
- ソフトウェアへの必要な変更のモニタリングプロセス
- 防災計画

DCCによる監査の結果、各組織が実施しているリスク管理の方法の文書化は、この種の文書によって行われていることが実証された。しかし、このリストはとても網羅的とは言えず、方針のその他の側面に関連するリスクにも、ほとんどとはいかなくても多くの組織が直面することだろう。たとえば研修や専門的能力の開発等の人事関連問題は、別途記述したり文書化されている可能性がある。一例をあげると、技術の停滞に関連するリスクは潜在的に深刻で、したがって監査人たちは、このリストの範囲を超えて考え、まずリスクを検討した後、それらを回避又は処理するための手段を記述した関連方針を検討するよう奨励される。このプロセスの間、監査人たちは、リスク登録簿を作成し、リポジトリの量的及び質的な成功を記述し、実証するための報告メカニズムを添付して、既存の文書を補完する。

文書化は非常に重要だが、追求すべき唯一の根拠というわけではない。DCCによる監査の

[18] S. Ross and A. McHugh, 2006, ‘The Role of Evidence in Establishing Trust in Repositories’, *D - Lib Magazine*, July/August, vol. 12, nos 7/8（*Archivi e Computer*, 2006にも掲載), http://www.dlib.org/dlib/july06/ross/07ross.html

結果、実験、証言及び観察に基づく根拠も確認されている。個人が1人で自己監査プロセスを実施すると仮定した場合、その人自身がリポジトリのアクティビティのあらゆる側面について包括的な知識を持っているとは考えにくい。こうした点を考慮すると、監査プロセスは、さまざまな職員が意見を出し、総合的なリスク登録簿に含めるべきリスクを指摘できるような開放的なプロセスであることが肝要である。リポジトリ全体の管理者、ハードウェア及びソフトウェア管理者、受入、アーカイブ、保存、文書化、アクセスといった主要機能の責任者等の意見を聞くべきである。組織の長から雑用係や清掃員に至るまで、だれもがリポジトリ管理プロセスに関して洞察を与えることができる。そうした付加的な貢献は過度に冗長である必要はないが、プロセスの結果がリポジトリ全体を表す場合には、考慮しなければならない。

5.2.5 所要作業量の推定

自己監査プロセス全体の所要時間は、24～40時間（1日6時間で4日又は7日）程度の想定である。個々のタスクは予想所要作業量に基づいて配分されるが、リポジトリの業務の規模と範囲や評価における精査の程度によって変化する場合があり、大きく変化することもありうる。この4日間という推定日数には、監査人がリスク識別及び評価プロセスで参照する必要が生じると思われる文書を収集するための準備時間が含まれていない。この作業量は、パイロット監査での経験に基づく。本ツールキットはさまざまな個人や組織によって使用されるため、監査が上記の予想所要時間内に終了したかどうか、もし終了しなかったとすれば、期間内に終了できなかった要因はどこにあったのかを知らせてほしい。

5.3 定義及び用語集

本文書において、重要な用語には次の定義が適用される。

アクティビティ（Activity）
機能面で、それを完遂するために組織が実施する主要タスク。

資産（Asset）
組織にとって価値のあるすべてのもの（ISO/IEC 13335-1:2004による）。

デジタルリポジトリ（Digital Repository）
真正で理解可能なデジタル資源の長期保存に責任を負う組織又はその一部。デジタルリポジトリは、次の10項目の基準を満たしていることが期待される。

1. 特定のコミュニティのためのデジタルオブジェクトの継続的な保守を責務とする。
2. 責務を履行するための組織としての適合性（財務、人事、構造、プロセス等）を備えている。
3. 必要な契約及び法律上の権利を取得、維持して、責任を果たす。
4. 効果的で効率的な方針の枠組みを持っている。
5. 各リポジトリの責務と能力に応じて明確に規定された基準に基づいてデジタルオブジェクトを収集し、受入れる。
6. 保持しているデジタルオブジェクトの完全性、真正性、有用性を長期にわたって維持／確保する。
7. 保存の過程でデジタルオブジェクトに講じられた措置及び関連する作成、アクセス支援、保存前の使用プロセスについて必要なメタデータを作成し、維持する。
8. 必要な提供要件を満たす。
9. 保存計画及び保存のために行われる活動に関し、戦略的なプログラムを持っている。
10. デジタルオブジェクトの継続的な保存とセキュリティに適した技術インフラを持っている。

自己監査ツールキットは、特定の種類のデジタル資源や、特定の種類の組織構造を持つリポジトリを想定していない。リスクに基づく自己評価は、アーカイブ、電子図書館、データアーカイブ、e-サイエンスコレクションの別に関わらず、リポジトリの公的使命の範囲内で実施されることになる。

機能クラス（Functinal class）
相関性のあるデジタルリポジトリアクティビティの個々のグループ。アクティビティ間の結びつきの強さは、緩やかな拘束から強力な結合までさまざまである。この自己監査ツールキットの機能クラスは、収集と受入、保存と蓄積、記述とメタデータ管理、アクセスと提供といったデジタルリポジトリの主要機能や、組織と管理、スタッフ配置、財務管理、技術サポート、セキュリティ等、どこの組織にもある一般的な機能を区別するため、「作業」と「サポート」というカテゴリーに分けられている。

機能クラスは、主に監査プロセスとその過程で作成されるリスク登録簿を構造化し、監査プロセスで監査人に指針を与えるために設定されている。これらの機能クラスは、リポジトリの体系的な機能分析に基づいているわけではなく、業務分類体系に代わるものではない。リポジトリが最新の業務又は記録分類体系を持っている場合には、自己監査ツールキットでデフォルトとして提供されている8つの機能クラスに代えてこの分類を利用すれば、監査結果の解釈に役立つだろう。

尤度（Likelihood）
確率又は頻度を指す一般的な用語（AS/NZS 4360:2004）。

公的使命（Mandate）
組織又はその親組織が特定の目標を達成するために公表した法的根拠、又は公式的に明示された意図。

所有者（Owner）
資産の生産、開発、保存、使用及びセキュリティ管理に関し、管理責任を承認した個人又は実体（ISO 27001:2005）。

リスク（Risk）
リスクとは、将来の事象や結果を取り巻く不確実性のことをいい、組織の目的達成に影響を与える可能性がある事象の尤度と影響を表す[19]。

リスク評価（Risk assessment）
尤度と影響のスコアを総合して、リスクの規模を予測する体系的なプロセス。

リスクの回避（Risk avoidance）
リスクが存在する状況に関与しない、又はそうした状況から撤退するという意思決定（ISO/IEC指針73:2002）。

リスクコミュニケーション（Risk communication）
意思決定者とその他のステークホルダーの間で行われるリスク情報の交換又は共有（ISO/IEC指針73:2002）。

リスクの識別 （Risk identification）
リスク識別プロセス。その後の詳細な分析の基礎として、事業の目的、アクティビティと資産、それらの脅威と脆弱性を検討する。

リスク管理（Risk management）
リスクに関して組織を指揮管理するための協調的なアクティビティ（ISO/IEC指針73:2002）。

[19] Treasury Board of Canada, *Integrated Risk Management Framework* (2001).

ステークホルダー （Stakeholders）

意思決定、アクティビティもしくはリスクに影響を与えうる、それらから影響を受けうる、又は影響を受けうることを認識している人々と組織（AS/NZS 4360:2004）。

脅威 （Threat）

組織、その資産又はシステムに危害をもたらす可能性がある出来事の潜在的な原因。

脆弱性（Vulnerability）

1つもしくは複数の脅威の悪影響を受けうる資産又はアクティビティの弱点。

5.4 リスク評価の原則

リスクの評価を行う際には、その確率と影響を定量化しなければならない。確率とは、リスクが発生する尤度を意味する。自己監査ツールキットは、次の尺度に基づいてリスクの確率を検討する。

リスクの発現可能性のスコア	説明
1	可能性が極めて低い。**100年**に1回以下の発現頻度
2	可能性が非常に低い。**10年**に1回の発現頻度
3	可能性が低い。**5年**に1回の発現頻度
4	可能性が中程度である。**1年**に1回の発現頻度
5	可能性が高い。**1か月**に1回の発現頻度
6	可能性が非常に高い。**1か月に複数回**の発現頻度

リスクの潜在的な影響は、次の尺度に基づいて分類される。

リスクの影響のスコア	説明
0	影響なし。デジタルオブジェクトの真正性及び見読性の**損失はない**[20]。
1	軽微な影響にとどまる。デジタルオブジェクトの真正性及び見読性の**損失は単独であり、完全に復元可能である。**
2	表面的な影響にとどまる。デジタルオブジェクトの真正性及び見読性の**損失は広範囲に及ぶが、完全に復元可能である。**
3	中程度の影響がある。デジタルオブジェクトの真正性及び見読性の**損失は全般に及ぶが、完全に復元可能である。**
4	影響が大きい。デジタルオブジェクトの真正性及び見読性が**復元不可能な状態になるなど、単独の損失を招く。**
5	相当に影響が大きい。デジタルオブジェクトの真正性及び見読性が**復元不可能な状態になる又はサードパーティによってのみ復元可能な状態になるなど損失が広範囲に及ぶ。**
6	壊滅的な影響。デジタルオブジェクトの真正性及び見読性の**損失が全体に及び、復元不可能な事態を招く。**

自己監査ツールキットに使用されているリスクについての全記述項目は次のとおりだが、監査人はいかなる場合もこれに制限されず、リスク登録簿に記載されているリスクの特性を

[20] ここでは、見読性（understandability）という言葉が技術、文脈、統語論、意味論的見読性を含む最も広義な意味で使用されているので注意すること。

表す際には、これ以外の属性も使用することができる。

リスクのラベル	リスクの記述
リスク識別子	リスクを一意に識別し、リスクの関連性を表す表現の中でリスクを参照しやすくするため、リポジトリが提供するテキスト文字列。
リスク名称	リスクを記述する短いテキスト文字列。
リスク記述	リスクをより詳細に記述した長いテキスト文字列。
リスク発現例	リスクが現実化される、又はその可能性がある状況の例。
リスク識別日	リスクが初めて識別された日。
リスクの性質	・物理的環境。 ・人事、経営及び管理の手法。 ・業務及びサービス提供。 ・ハードウェア、ソフトウェア、あるいは通信機器・設備。
所有者	リスク所有者の氏名。通常、対応するアクティビティの所有者と同じ。
上位所有者	所定のリスク所有者が管理を放棄した場合に、そのリスクに対して最終的な責任を負う個人の氏名。
ステークホルダー	リスクが現実化することによって脅かされる出資案件もしくは資産を所有している、又は対象となるリスクの管理に責任を負っている当事者。
リスクの関係	対象となるリスクと関連している個々のリスクを記述したもの。
リスクの発現可能性	対象となるリスクが現実化される尤度として認識された数値を表す。
リスクの潜在的影響	デジタルオブジェクトの見読性と真正性の喪失という面で認識されたリスクが現実化した際の影響の大きさを表す。
リスクの深刻度	発現可能性と潜在的影響のスコアを乗じて算定される数値。
リスク管理戦略	リスクを管理（回避及び／又は処理）するために掲げられる方針と手続きを記述したもの。
リスク管理アクティビティ	明示されている方針と手続きに基づく実際のアクティビティ。
リスク管理アクティビティの所有者	リスク管理アクティビティの遂行に責任を負う個人。
リスク管理アクティビティの目標	目標となるリスク深刻度の評点とリスクの再評価日。

5.5 リスク分析に基づく自己監査法

上述のように、本ツールキットの基本的な思想は、支援することであって規制することではない。監査人には広範な指針が与えられるが、監査結果が価値を持つためには、監査人自身の積極的な関与と取組みが不可欠である。リスク管理は、リポジトリの目標と目的を背景として実施されるため、そうした背景を定義し理解するということが最優先事項となる。これは、組織の目的という点から実施することができ、その結果、評価実施時の基準となるパラメータが決定される。オーストラリアとニュージーランドの「リスク管理基準」には、内部の状況の重要性が次のように明記されている。

- 「多くの組織にとって重要なリスクとなるのは、戦略、事業又はプロジェクトの目的を達成できないことや、達成されなかったとステークホルダーたちに認識されることである。
- 組織の方針と目標及び関心は、組織のリスクについての方針の策定に役立つ。さらに、
- プロジェクト又はアクティビティの特定の目的と基準は、組織全体の目的という点から考慮されなければならない」（AS/NZS 4360:2004、p.14）。

実際には、自己監査プロセスは多数のタスクで構成されており、それぞれ独立した価値を持っているが、総合すると組織のリスクの全体像を描き出すことができる。簡単に言えば、監査人は、指針に導かれて、最初に目的を、次に具体的なアクティビティや資産及び人々を、最終的にはそれらに関連するリスクの識別を行うのである。

5.5.1 目的の識別

監査プロセスは、自己監査組織が各自の公的使命を特定することから始まる。これを出発点として、基本的な目的とアクティビティの階層化が行われる。そして、その後に続く作業の実施を促進するために必要な粒度によっては、さらに細分化することもできる。一般に、粒度が高くなればなるほどアクティビティとリスクの識別と調整はより直接的なものになっていくと考えられているが、必ずしも厳密にそうなるわけではない。DRAMBORAには、参加組織が適切な「レベル」で各自の目的を識別する作業を支援するため、一連の目的が例示されている。

5.5.2 アクティビティと資産の識別

アクティビティは、主に組織の目的に基づいており、これには、リポジトリの大まかな目標の実際の実現方法が含まれている。資産とは、満足な結果を得るための人材や技術的ソリューションをはじめとする関連資源を意味する。

5.5.3 アクティビティと資産に対するリスクの関連付け

監査人は、最初の2つのタスクの結果を組織文書にまとめた後、識別されたアクティビティと資産のそれぞれに関連する具体的なリスクを文書化しなければならない。これに関しても、リスクが適切な粒度で特性付けられるようにするため、例が示されている。単一のリスクが複数のアクティビティと関連づけられたり、複数のリスクが単一のアクティビティと関連づけられたりすることが多いが、いずれもまったく問題はない。どちらもその後のリスクの分類とそれらの評価に役立てられる。リスクの分類は、リスクが発生した状況、その潜在的な影響、又はそれらを管理しうる手段との関連から定義することができる。同様に、この段階でリスクの関連性についても考えることができる。リスクの関連性は、次のいずれか1つ以上の特性を持つ。

リスクの関連性	リスクの関連性の定義
爆発的	n件のリスクが同時に現実化した時の影響が、単独で発生した各リスクの合計値を上回る場合。
連鎖的	単一のリスクが現実化されると、他のリスクの尤度が大きくなる場合。
相補的	あるリスクについての回避又は処理メカニズムが、他のリスクの管理にも役立つ場合。
ドミノ的	あるリスクに関連する回避又は処理が、他のリスクについての回避又は処理の有効性を減少させる場合。
原子的	リスクが単独で存在しており、他のリスクに一切関係していない場合。

実際には、他とまったく関連していないリスクというのは考えにくく、任意のリスクの処理又は回避のために資源の配分量を増やせば、ほぼいずれのケースにおいても、他のリスクに配分できる資源は減少するという状況が発生する。少なくともこの点に関しては、各リスクは他のリスクとは逆相関の関係にあるが、リスク処理戦略はその他のリスクの管理に有益で、その関係は補完的である。

5.5.4 リスクの評価、回避及び処理

監査人は、関連するリスクのリストを作成した後、各リスクに関し、各自の組織に固有のさまざまなリスク属性を明らかにする。必須記述項目には、リスクの発現可能性、影響、所有者及び回避もしくは処理を可能にするために行われている又は提案されているメカニズムに関する情報が含まれる。リスクの特性を記述するプロセスは根拠書類の入手可能性に依存するが、ほとんどの場合、そのような根拠書類は方針書の形で存在する。

5.5.5 自己監査の結果

自己監査プロセスから得られる主な成果物は組織のリスク登録簿で、それ自体が非常に有

用な管理ツールであり、その後の正規監査の基礎とすることができる。さらに、特にツールキットの相互作用性が広く実現されるにつれ、監査人は、各自が識別したリスク分類に基づいてさまざまな報告書を提示したり、改善が必要な分野を正確に表現しうるさまざまな方法で結果を視覚化したり、改善を実現するために組織として行う活動の優先順位を決定したりすることができるようになるだろう。

5.5.6 リスク登録簿

リスク登録簿には、識別されたすべてのリスクと、それらの分析及び評価結果が列記される。これには、各リスクの現状に関する情報が含まれる。こうした詳細情報を利用して、最も重要な組織目標を実現するためのアクティビティの一部として、リスク管理の成功例を追跡し、モニタリングすることができる。この種の文書は「リスクログ」と呼ばれることもあるが、意味は同じである。

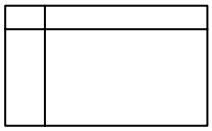
適切に維持されたリスク登録簿は、リポジトリの管理者、出資者（現実の及び潜在的な）、コンテンツ提供者に対してリスクに関する情報を伝える有用な媒体となる。

5.5.7 リスクに基づく自己監査プロセス

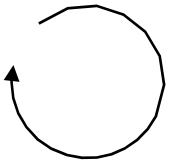
次ページの図は、自己監査プロセスの段階を表したものである。本文書中の図では、次の凡例が利用されている。

自己監査ツールキットに独立した画面が存在するプロセスを表す。

監査人が監査書類の必要事項に記入する際に役立つ代表的な文書や情報が記載されたガイダンスフィールドを表す。

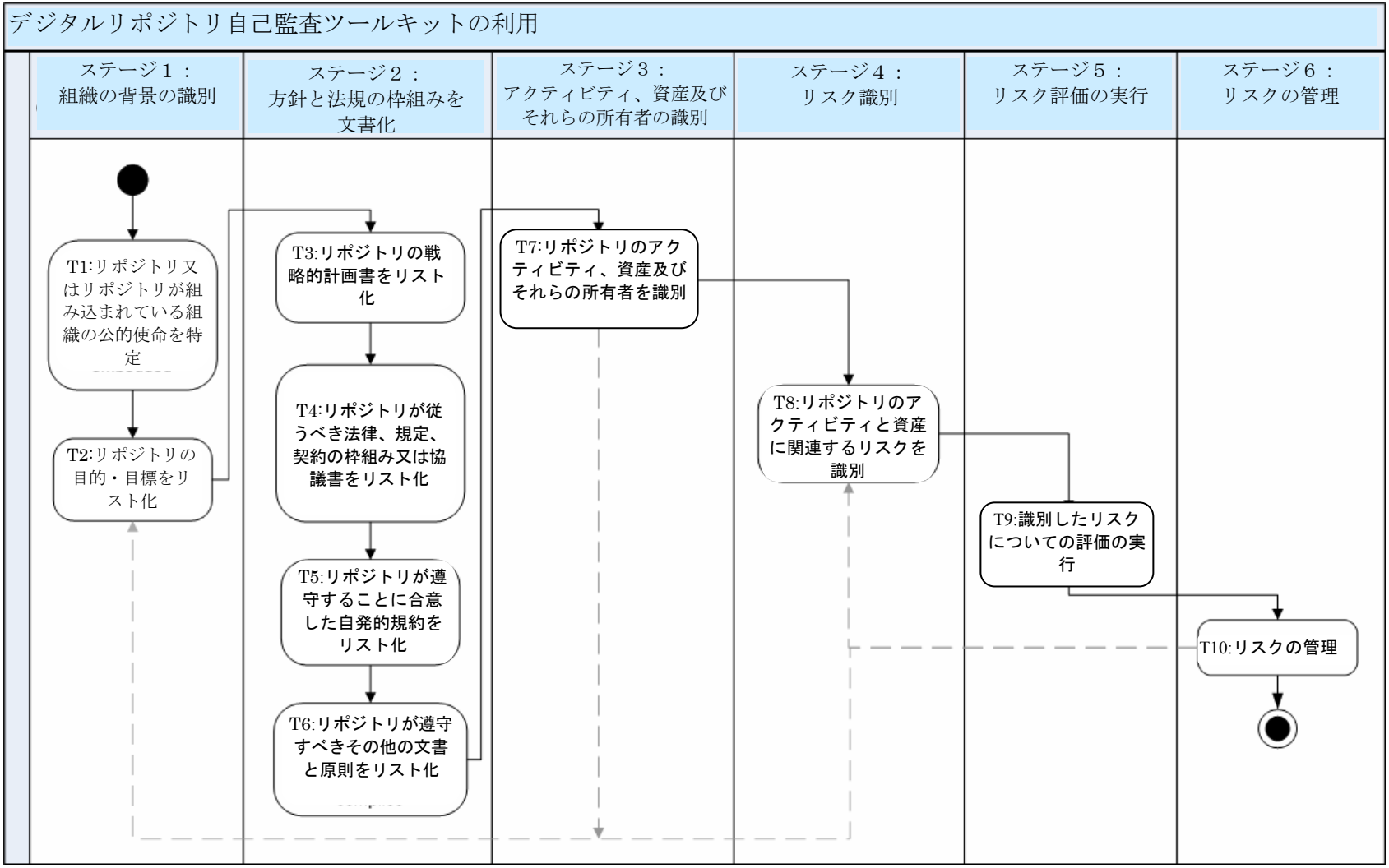


質問表の形式で記入された情報を分類する複数のカテゴリーのリストを表す。



プロセス中のループを表す。ループ状の矢印が付いているボックス内に記載されている各カテゴリーについて、質問を繰り返さなければならない。

リスク管理アクティビティの連続サイクルとなりうるルートを表す。


デジタルリポジトリ自己監査ツールキットの利用
ステージ１：
組織の背景の識別
ステージ２：
方針と法規の枠組みを
文書化
ステージ３：
アクティビティ、資産及び
それらの所有者の識別
ステージ４：
リスク識別
ステージ５：
リスク評価の実行
ステージ６：
リスクの管理
T1:リポジトリ又はリポジトリが組み込まれている組織の公的使命を特定
T2:リポジトリの目的・目標をリスト化
T3:リポジトリの戦略的計画書をリスト化
T4:リポジトリが従うべき法律、規定、契約の枠組み又は協議書をリスト化
T5:リポジトリが遵守することに合意した自発的規約をリスト化
T6:リポジトリが遵守すべきその他の文書と原則をリスト化
T7:リポジトリのアクティビティ、資産及びそれらの所有者を識別
T8:リポジトリのアクティビティと資産に関連するリスクを識別
T9:識別したリスクについての評価の実行
T10:リスクの管理

5.6 監査のステージ

自己監査は6つのステージを通して行われる。

- ステージ1：組織の背景の識別
- ステージ2：方針と法規の枠組みを文書化
- ステージ3：アクティビティ、資産及びそれらの所有者の識別
- ステージ4：リスクの識別
- ステージ5：リスク評価の実行
- ステージ6：リスクの管理

5.7 ステージ1：組織の背景の識別

ステージ1では、組織の背景を確立することに焦点を当てる。

5.7.1 ステージ1の目的

ステージ1の目的は、リポジトリの役割を識別し、目的・目標を示すことである。監査の範囲は、概ねリポジトリ自体の範囲や公的使命によって定められる。

ステージ1において、監査人は公的使命を文書化し、リポジトリの目的・目標を導き出す。監査ステージ1の最終目的は、リポジトリの業務範囲を明確化し、組織の枠組みに対する内部意識を確認すると同時に、適切な裏付け文書の存在を確認することである。リポジトリがより大きな組織又は組織体（LOCKSS[21]や連合リポジトリなど）に所属する場合、その組織内のリポジトリの位置づけ及び背景は、ステージ1の一部として示される。

5.7.2 ステージ1の関連タスク

ステージ1において、監査人はリポジトリの目標全体を概観し、リスク分析及びその後の評価の対象となる特性を決定しなければならない。ステージ1のタスクは2つの部分から成る。まず、監査人はリポジトリの公的使命を識別しなければならない。それらは組織のミッション・ステートメント又は規定文書に記述されているだろう。次に、監査人はリポジトリに関して、公的使命の範囲内における各組

[21] http://www.lockss.org/lockss/Home

織の目的・目標を識別しなければならない。

5.7.3 ステージ1で期待される成果

ステージ1を終了すると、監査人は次の成果を得る。

- ◆ 公的使命、及びリポジトリの目的・目標の包括的リスト
- ◆ リポジトリ、及び組織の目的・目標の理解
- ◆ リスク分析に基づく監査の範囲を決める確固たる根拠

これらの成果は、監査人がリポジトリのアクティビティと資産を識別、解釈し、それらの関連リスクについて効果的な決定を下す際に役立つ。また、リスクについて、リポジトリについての幅広い背景を考慮した上で、あるいは組織についての幅広い視野の中で考えることができ、組織とその環境に対する確固たる理解に基づいてあらゆる解決方法を提案することができる。

5.7.4 監査プロセス全体におけるステージ1の位置づけ

ステージ1とステージ2の監査は同時に完了することが望ましい。なぜなら、ステージ2において、監査人は既存の関係文書を参考にしながら、ステージ1の答えを実証していかなければならないからである。また、監査人は、リポジトリの運営に係る業務上・法規上の枠組みに関する追加の文書も洗い出さければならない。

ステージ１で監査人が得た情報は、組織のアクティビティ、資産及び関連リスクを識別するこの後の各ステージの中で参考にされる。

5.7.5 ステージ1を完了させるために必要な資源

完了までの予想時間：3時間

ステージ1のタスクを効果的に完了するよう努力することが、監査結果全体によい影響を与えることになるが、回答の精度や粒度によっても、この後の自己監査のステージにおけるリスク識別や評価の質が大きく左右される。本プロセスの初期のステージにより力を入れることにより、後のステージが効率的にできるようになるだろう。

ステージ1を始める前に、まず準備期間が必要である。監査を始める前に、自己監査プロセスのステージ1を完了するのに必要な文書を収集し、ついでリポジトリのスタッフと共に組織の目的、アクティビティ及び最終的にはリスクの範囲について決定しなければならない。

必要であれば、監査人は後のステージでの作業中にステージ1でまとめたリストに戻り、情報を追加することもある。

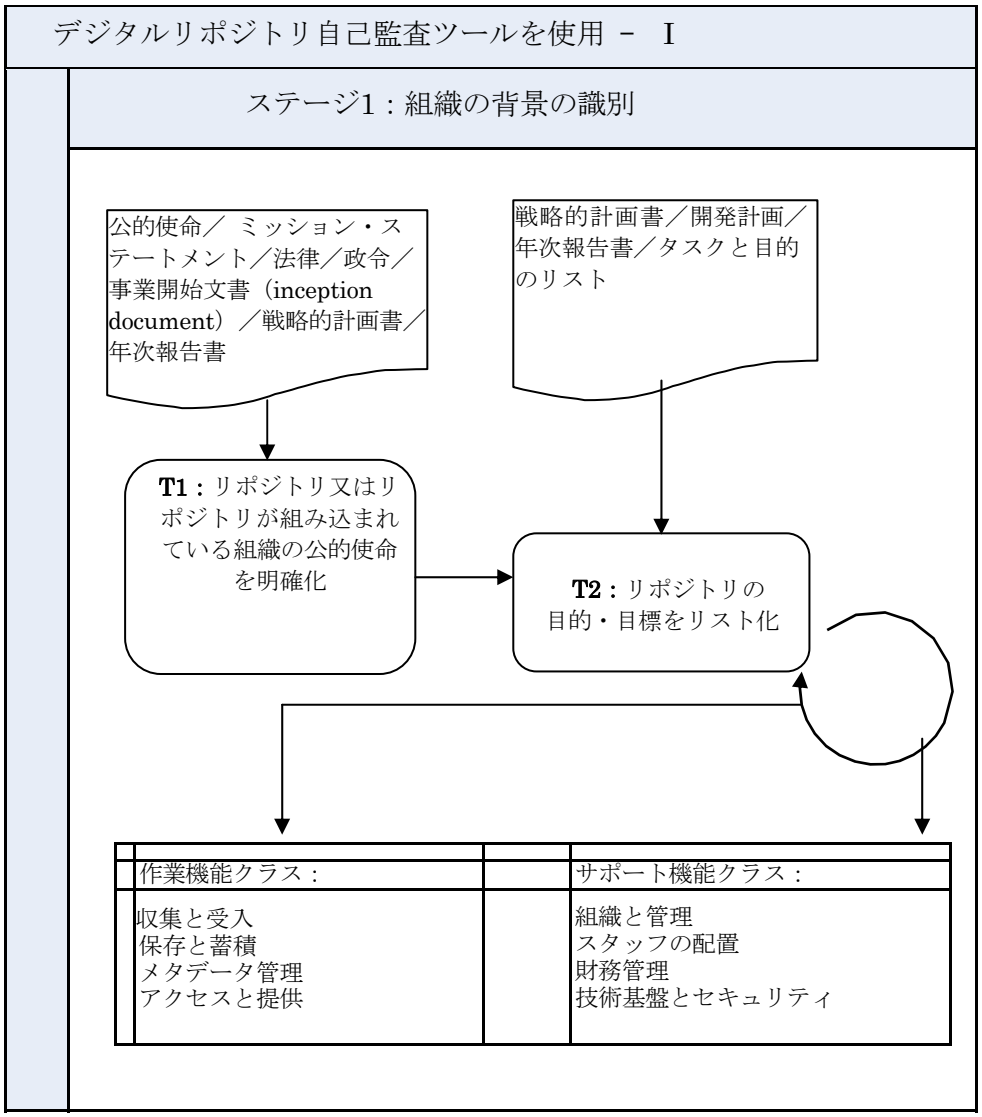
ステージ1を始める前に、監査人は次のことをしなければならない。

- 必要な文書の予備リストを作成する。
- リポジトリ内又はリポジトリに関連するさまざまな人々に情報提供を求め、リポジトリの基本情報及びミッションをより深く理解する。対象者には上級管理職者、法定代理人、外部ステークホルダー、出資者などが含まれるが、これに限るものではない。

ステージ1を完了するために、監査人は次のことを確実に行わなければならない。

- 内部文書（戦略的計画書、企業業務計画、年次報告書、目標リスト、契約書など）へのアクセス
- 各組織が設定した目的・目標について詳しく知る人々へのアクセス

5.7.6 ステージ1を示す略図



5.7.7 ステージ1を完了するための指示

監査プロセスの最初の2つのステージで、以下が識別される。

- リポジトリ、アクティビティ及びステークホルダー・コミュニティの範囲
- リポジトリが利害を考慮するべき内外のステークホルダー
- リポジトリのミッションを達成するために確立された目的・目標
- リポジトリの作業に影響を与える法的枠組み
- リポジトリが満たすようコミュニティに望まれている事業、社会、倫理上の基準
- 利用可能な知識基盤－リポジトリに存在する最先端の考え方や実践

ステージ1で行うタスクは、集中して分析を行うことを支援し、調査結果の文書化のための枠組みを提供する。また、ステージ1のタスクを完了すると、リポジトリの具体的な情報が作成され、監査の後のステージでそれらを活用することができる。

このセクションのタスクを遂行するにあたり、監査人は書式T1、T2（本文書の第III部を参照）を利用すべきである。手作業でこれらの書式に記入する場合、様式T2については、リポジトリにおける作業を体系的に記載する8つの機能クラスそれぞれにつき一つの書式が必要になるため、複写が必要になる。

5.7.7.1 T1：リポジトリ又はリポジトリが組み込まれている組織の公的使命

監査人は所定の記入欄に組織の公的使命について記載しなければならない。

組織の公的使命とは、組織又はその親組織が、ある目的・目標を達成するために正式に表明した意志又は組織の法的根拠のことをいう。いかなる組織も目的があって設立される。リポジトリの典型的な公的使命には、ある種の資料の収集、保存、アクセスの実現化などがある。

組織の公的使命は、組織の正式な根拠及び組織の設立理由や継続的存在理由を伝えるため、表明されなければならない。あるビジネスアクティビティに関連するミッション・ステートメントとして解釈されなければならないこともある。どのような形式をとるかどうかは、公的使命の解釈、ある時点におけるニーズ及び資源の利用可能性によって左右される[22]。ミッション・ステートメントとは、組織が長期的に達成しようとしていることを簡潔に記述したもの、つまり存在理由である。

通常、組織の公的使命及びミッション・ステートメントは、組織のホームページ、年次報告書、設立趣意書、あるいは法律、もしくは憲法にさえ記載されうる。後者の例としては、定款（アーカイブ法など）、法律、政令、協約などがある。

[22] Hans Hofman, Babak Hamidzadeh, Ken Hawkins, Bill Underwood, *Business-driven recordkeeping model. Version 5.0* (February 2007) (InterPARES-2で公開予定)

タスクの回答例の抜粋：

T1：	**リポジトリ又はリポジトリが組み込まれている組織の公的使命**
例：	[リポジトリ名]の役割は、研究者が[データの種類]の場所を突き止め、アクセスし、解釈できるように支援すること、及び公的支援研究プロジェクトが生産する[データの種類]の完全性を長期にわたり確保することである。

5.7.7.2 T2：リポジトリの目的・目標をリスト化

このタスクにおいて、監査人は8つの機能クラスそれぞれに関連する組織の目的・目標を記述する。機能クラスには、4つの作業機能クラス（収集と受入、保存と蓄積、メタデータ管理、アクセスと提供）及び4つのサポート機能クラス（組織と管理、スタッフ配置、財務管理、技術インフラとセキュリティ）がある。記入が終了したら、8つの機能クラスそれぞれについて、別紙T2を利用して記入すべきである。

組織の日常の作業を計画・管理するため、通常は短期と中期の目標を立てる。これらの目標は、戦略的計画書、開発計画、年次報告書、タスク・目的のリストなど、さまざまなものに明示されていることが多いが、組織が所属するコミュニティの識別可能な期待値として存在していることもある。目標リストがすぐに入手できない場合は、組織の公的使命、ミッション及び設立文書から作ってもよい。

各目的・目標は、もっとも密接に関連する機能クラスに分類されなければならない。一つの目的が二つ以上の機能クラスに関連していることもある。目的やアクティビティによっては既存の機能クラスに適合しないことも予想されるが、そのような場合、監査人はここに提供されている8つのカテゴリーに、さらにカテゴリーを追加してもよい。

タスクの回答例の抜粋：

T2：	**リポジトリの目的・目標をリスト化**
例：	作業機能：収集と受入
	コンテンツ提供者がファイルを提供したときに、動的にファイルの有効性を確認するファイル受入システム
	コンテンツ提供者にデータセットの利用統計を提供
	受入れ可能な提出フォーマットを規定
	[コンテンツ提供者]の[データの種類]をコンテンツ提供後12か月以内に収集、配布
	作業機能：保存と蓄積

	アーカイブしたコンテンツに対するすべての変更を文書化
	作業機能：メタデータ管理
	[リポジトリ名]内のデータを効率的に処理できるようにする。
	メタデータとアーカイブされたコンテンツ間の参照整合性を維持する。
	作業機能：アクセスと提供
	ユーザーコミュニティが全ての合意済みデータセットに常にすぐアクセスできるようにする。
	ユーザーに、資源の許す範囲内の付加価値サービスを提供する。
	新しいユーザー登録・アクセス管理システムを設定する。
	コンテンツ提供者にデータセットの利用統計を提供する。
	ユーザーにデータセットに関する情報及び一般情報を提供する。
	サポート機能：組織と管理
	ユーザーコミュニティが全てのあらかじめ合意されたデータセットに常にただちにアクセスできるようにする。[リポジトリ名]内のデータの取り扱いをできる限り効率的にする。ユーザーに、資源の許す範囲で付加価値サービスを提供する。
	学会への定期的出席や適切な広報資料の提示を通して、[リポジトリ名]やそのデータ収集を促進する。
	サポート機能：スタッフの配置
	スタッフの役割、責任、関係を明確化する。
	サポート機能：財務管理
	2007年以後[プロジェクト名]からの資金調達が終わった後も、財政面での実現可能性を維持する。
	サポート機能：技術的インフラとセキュリティ
	e-サイエンスのアクティビティを支える業務の開発など、[リポジトリ名]のインフラの開発・拡張を継続的に行う。
	最大80TBまでのデータ蓄積を支えるコンピュータシステム、及びユーザーのデータ加工の制限
	2007-2009年の戦略的IT計画を2007年1月3日までに立案

5.7.8 必要な情報が利用不可能な場合

5.7.8.1 T1：リポジトリ／組織の公的使命

監査人はリポジトリ又は組織の公的使命を既存の文書中に見つけることができない場合、少なくとも本監査の目的のために、そうした文書を作成しなければならない。この文書は、当然ながら後に調整する必要があるかもしれないが、この

ステージで作っておく必要がある。役員会（又は同様の委員会）はその公的使命を承認する必要があり、また必要に応じてその決定又は調整に貢献しなければならない。

リポジトリの公的使命を定義するため、監査人は組織の設立文書を調査し、組織の根拠及び目的を説明したステートメントを得る必要がある。

5.7.8.2 T2：組織の目的・目標をリスト化

監査人は、目的・目標をリスト化するプロセスで入手可能な文書を揃え終えた場合、次のような資料をさらに考慮に入れることで、組織の目的・目標の明確化作業を再開することができるだろう。

- 年次報告書
- 戦略的計画書（ビジネス計画、企業計画、部門開発計画など）
- 手続きマニュアル、作業マニュアル
- 文書記録システム及び分類体系
- 組織図
- 特定のステークホルダーの利益を目的とした出版物

このような文書は一般的に組織のイントラネットを通じてアクセス可能であったり、共有のファイルストレージで利用可能である。

この目的は、このステージが終わるまでにリポジトリの目的・目標に関するある程度完全なリストを作ることである。適切であれば、主な目的のリストについて上級管理職者及び／又はスタッフの合意を得るべきである。しかしながら、監査人は評価のプロセス全体を通して、いつでもこのリストに戻り、自由に回答を追加することができる。

このステージで質問に答えるための方法論的背景として、監査人はさらに次のものを参照にするとよいだろう。

- 『記録管理システムの設計と実行マニュアル（Design and Impelementation of Recordkeeping Systems （DIRKS） Manual）』（オーストラリア国立公文書館[23]発行）のステップA
- HB 436:2004『リスク管理ガイドライン：AS/NZS 4360:2004の手引き（Risk Management Guidelines. Companion to AS/NZS 4360:2004）』のセクション4

[23] http://www.naa.gov.au/recordkeeoing/dirks/dirksman/step_A.html

5.7.9 考察

一連の目的を識別した後、監査人はそれらの目的と、リポジトリの構成方法、資金調達方法、促進方法、及びスタッフの配置方法とを比較するだろう。これにより、さらなるリスクの重要原因になりうる現在の構成や施設の潜在的な可能性と有効性、資源とスタッフ配置の妥当性を分析することができる。

5.7.10 意見募集

DCC/DPE監査・認証ワーキンググループは監査人の方々からのコメント、懸念事項、あるいは意見をお待ちしております。feedback@repositoryaudit.euまでお寄せください。

5.7.11 チェックリスト

次のステージに進む前に、監査人は次のことを完了していること。

- ◆ リポジトリの公的使命を記述する。
- ◆ 8つの機能クラスそれぞれについて、短期及び中期の目的・目標リストを作成する。（機能クラスは必要に応じて集約されていてもよい。）
- ◆ 目的・目標を詳細に記述した文書がどこにあるのか、十分に理解している。

5.8 ステージ2：文書方針と規定の枠組み

このステージは、自己監査6ステージのうちの2番目のステージである。

5.8.1 ステージ2の目的

ステージ2において、監査人は、リポジトリが次のことを行うことができる根拠を提供又は参照できる。

- 関連する法規上の枠組みに準拠して、適切に運営されている。
- 効果的・効率的な政策上の枠組みをもっている。
- 社会、倫理、法制、行政上の枠組みを認識している。
- リポジトリが従うべき法律、契約、規定上の必要条件を認識している。

これらの方針類は必ずしも外在的なものとは限らない。時には、規定の枠組みが、リポジトリの基盤となる制度から影響を受けることもある。

リポジトリの法規上の枠組みは、内部又は外部に由来する法規や規定を総合して、大まかに定義される。関連する外在の責務や影響を及ぼすものには、法令、法令文書、国際的又はビジネス上の規定、事実上の又は確立された行動基準などがある。内部で発生する責務には、契約、方針書、戦略的計画、ビジネス上の規範などがあるだろう。

5.8.2 ステージ2の関連タスク

ステージ2において、監査人は次のことを行わなければならない。

- 何を求めるべきかを決定する。
- 机上調査の実践として、文書を収集する。
- リポジトリの作業を規制する文書のリストを編集する。
- ステージ1でリスト化した目的・目標の根拠書類の妥当性を分析する。

5.8.3 ステージ2で期待される成果

ステージ2が完了することにより、監査人は次のことを達成する。

- リポジトリの業務に対する規制的背景を構成する内外部の文書の包括的リストを作成する。

- ◆ 規制の枠組みを定めるさまざまな文書を分析する。
- ◆ リポジトリが稼働する条件（資金提供者、コンテンツ提供者、ユーザーとの契約上の合意内容など）をより深く理解する。
- ◆ リポジトリの業務に関わる実際の及び潜在的なステークホルダーについて、より包括的に理解する。

ステージ2で作成するソースドキュメント及び参考文書のリストは、自己監査の以降のステージにおいて、リポジトリのアクティビティやそれに関連するリスクについて効果的な決定を下す際に、参考文書として役に立つ。また、リポジトリ内のリスクを定義したり、提案されたソリューションが組織やその環境の確固たる理解に基づいていることを保証するのに役立つ。

5.8.4 監査プロセス全体におけるステージ2の位置づけ

繰り返しになるが、ステージ2で識別されリスト化された文書は、この後の自己監査のステージで参考資料として利用される。

ステージ1でリスト化した目的・目標、及びステージ3で識別するアクティビティ、資産、技術は、目的と規制上の必要条件との乖離、又は規制上の必要条件と定められたアクティビティとの乖離から生じるリスクを識別するための枠組みを形成する。

5.8.5 ステージ2を完了させるために必要な資源

完了までの予想時間：3時間

自己監査のステージ2は、必ずとは限らないが、多大な時間を要することがある。ステージ2の完了に必要な時間は、監査人が持つリポジトリの法的背景に関する一般知識、契約協定についての知識やアクセス、及びリポジトリに適用されるかもしれない基準に関する知識に依存する。ステージ2の結果は、それだけでもリポジトリの貴重な資源になるかもしれない。すべての法令、規定、契約上の義務、及び戦略的方針文書のリストは、十分詳細に、また適切な参考資料をつけて提出されなければならない。現在の監査ではそれほど詳細な参考資料を明白に必要としていないが、それらが用意できれば、役に立つと思われる。

主に、関連する規定の必要条件リストを作成するために文書や資源を探し出したり分析する時間が必要になると思われる。

リストをまとめあげた後も、組織の枠組みに対応する貴重な資源として役に立ったり、将来の監査のために必要になるため、組織は常にリストの最新状態を維持しておかなければならない。

ステージ2を始める前に、監査人は次のことを行わなければならない。

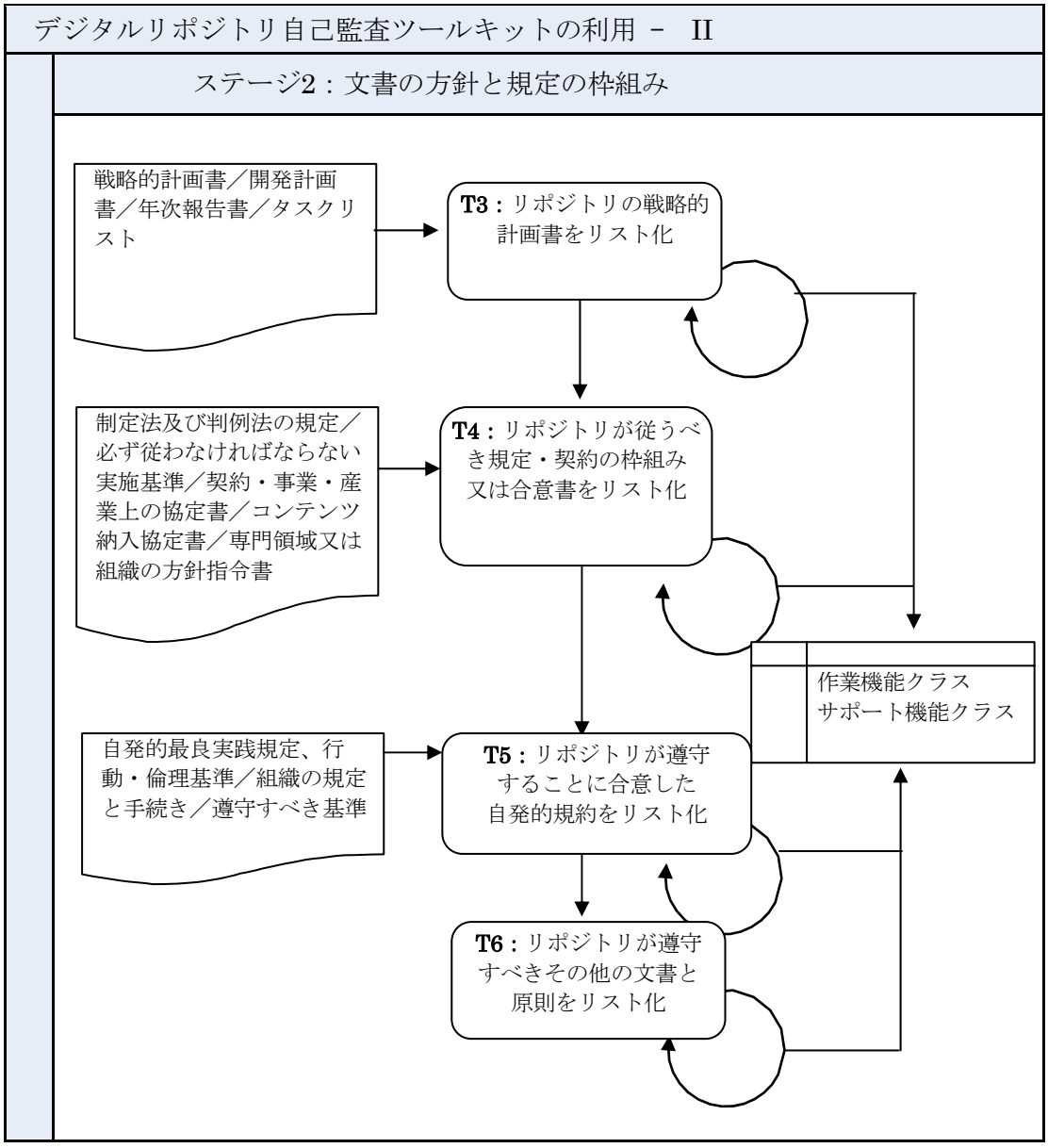
- ◆ 自分が認識している関連文書の予備リストを作る。

◆ リポジトリの法規上、契約上の義務の概要がわかる法律家及び／又は上級管理職者にアクセスする。

ステージ2を完了するために、監査人は次のことを確実に実行しなければならない。

◆ 戦略的計画書、企業・ビジネス計画書、年次報告書、目標リスト、契約書などの内部文書へのアクセス
◆ 法律、基準、行動基準などの外部文書へのアクセス
◆ 可能であれば、リポジトリの法規上・契約上の必要条件、及び基準の遵守について深い知識のある人材へのアクセス

5.8.6 ステージ2を示す略図



5.8.7 ステージ2を完了するための指示

参照する文書の出所をリスト化する作業は容易である。監査人は文書のタイトルを書き出し、必要であれば、版情報や発行日、及びどこでその文書を取得できるかの情報も記述する。複数のカテゴリで同じ文書を繰り返し使用しなければならない場合、監査人は文書に参照簡略記号をつけ、その記号を使って複数の事象

から参照させるとよい。

規定の必要条件の包括的リストの作成は、非常に時間のかかる作業である。多くの場合、監査人がリポジトリのアクティビティとリスクを効果的に記述するために必要な情報は、ソースドキュメントの中に一部しか明らかになっていないかもしれないが、なぜ、どのように、あることがリポジトリで行われているのかについて趣旨が書いてある文書はすべて、このステージでリスト化しなければならない。

5.8.7.1 T3：リポジトリの戦略的計画書をリスト化

戦略的計画書はさまざまなタイトルで存在しうる。監査人は手続き上又は運用上のマニュアルを探し、イントラネット又は共有のネットワークストレージ設備を参照し、戦略的計画書について上級管理者に問い合わせることが望ましい。

まずは、リポジトリの現在の戦略的焦点に注目し、それを確立した戦略的計画書及び実行ステートメントを識別するとよい。また、リポジトリのクライアント、顧客、及び対象読者にとっては、彼らのコミュニティに適合するように調整された方針や手続きについて検討することも有益である。

方針は、なぜリポジトリがあるアクティビティを実行するのか、大まかに言って、どのようにアクティビティが実行されるのかを説明する。すべての組織には、組織の経営陣に承認された方針、あるいは産業界やビジネス界全体に適用される方針がきちんとある。方針はある機能、ある機能の一部、複数の機能のある面、あるいは組織の機能全体などに関係している場合がある。方針書には、組織が行うアクティビティについての情報があるはずである。

手続きは多くの場合、ある特定のレベルにおける機能の実行方法について詳述されたマニュアルに記載されている。マニュアルは多くの場合、ある一つの機能に対応しており、一つ又は数個のアクティビティに関する手続きについて書かれている。ある個別の手続きは一般的に、アクティビティのある特定の面と関連している。手続きを定めたマニュアルはあるアクティビティについて、その要素を把握するのに役立つ。ある組織に固有の機能又はプログラムに関連する方針及び手続きは、内部で入手可能だろう。

方針や手続きによっては、グローバルレベルで、あるいはグローバルに関連して存在していることがあるので、監査人にとって、自分たちのような組織がもっとも幅広いレベルで活動するための方法を理解しておくことは不可欠である。

タスクの回答例の抜粋：

T3：	**リポジトリの戦略的計画書をリスト化**
例：	作業機能：収集と受入
	リポジトリ X：コア・アクティビティ （2005） http://www.xxx.org/policies/activities.pdf
	作業機能：保存と蓄積
	リポジトリ X：コア・アクティビティ （2005） http://www.xxx.org/policies/activities.pdf
	作業機能：メタデータ管理
	リポジトリ X：コア・アクティビティ （2005） http://www.xxx.org/policies/activities.pdf
	リポジトリ X データ・ポリシー （2003） K:\ Core_Documents\ DataPolicy.rtf
	作業機能：アクセスと提供
	リポジトリ X：コア・アクティビティ （2005） http://www.xxx.org/policies/activities.pdf
	サポート機能：組織と管理
	リポジトリ X：コア・アクティビティ （2005） http://www.xxx.org/policies/activities.pdf
	リポジトリ X リスクの記録簿 （2006） Intranet/Risk/Risk_Register.html
	サポート機能：スタッフ配置
	サポート機能：財務管理
	リポジトリ X リスクの記録簿 （2006） Intranet/Risk/Risk_Register.html
	サポート機能：技術的インフラとセキュリティ
	リポジトリ X リスクの記録簿 （2006） Intranet/Risk/Risk_Register.html

5.8.7.2 T4：リポジトリが遵守すべき法律、規定、契約の枠組み又は合意文書をリスト化

リポジトリが機能する法的環境要件は、組織によって大きく異なる場合が多い。このセクションでは、監査対象組織の外部にあるものの、組織の運営方法に影響を及ぼす文書も含めなければならない。

関連の法規文書や組織の契約義務の検討に入る前に、関連法規（未制定の法規も含む）の識別と分析を始める方が簡単かもしれない。規定の枠組みを構成する要素の階層構造は、次のようなものになると思われる。

- 制定法、判例法、その他の規則
- 必ず従わなければならない実施基準
- 部門又は専門領域の固有の規定
- 契約上の義務及びサービスレベルの協議書

監査人は分析範囲の確定を助ける簡単な質問に答え、影響を及ぼす法的行為の展望について適応の度合いを示すことができる。

- リポジトリはどのようなタイプの組織のものか。たとえば、私的機関、公的機関、部門、国家機関、非国家機関、企業、あるいは大学など。
- リポジトリは何を行っているのか、リポジトリはどんな部門に所属しているのか。たとえば、リポジトリが従事するビジネス又は産業部門は一般的にどのような内容を扱っているのか。（科学研究、製薬、教育など）リポジトリが提供する主な生産物、サービス、製品は何か。
- どんな法律がリポジトリの役割や作業に影響を与えるか。
- 組織が管理するのはどのような法規か。
- リポジトリはビジネス活動の一部を外部に委託したことがあるか。
- リポジトリのビジネス分野の一部が明らかな訴訟に巻き込まれたことはあるか。

法律はその他のさまざまな目的のために作られており、リポジトリの作業にほとんど影響を及ぼさない場合もあることを留意しておくとよい。

組織が法律に基づいて設立されている場合、組織の機能及び権限は関連する現行法規の中で概略が述べられているだろう。重要な用語について定義し、組織の目的を明確に示してあるだろう。また改正について詳しく説明し、組織のアイデンティティ又はビジネス活動が法律の変更によって影響を受けるかどうかが明示してあるだろう。

組織が法律に基づいて設立されていない場合、監査人は次のようなさまざまなソースを見て、組織の始まりや発展について、情報を得なければならない。

- 経営の取り決めに関する命令
- 憲章
- マスコミへの報道文
- 大臣声明

設置の根拠法に加え、その他の法律や、他の組織が管理する法律に定められた独自の義務の履行についても、組織には直接の責任があるかもしれない。監査対象の組織が準拠する法律は、通常、年次報告の中に見つけられる。

タスクの回答例の抜粋：

T4：	**リポジトリが遵守すべき法律、規定、契約の枠組み、又は協議書をリスト化**
例：	作業機能：収集と受入

	データ保護に関する法律
	知的財産の保護
	電子商取引と民事・刑事法の枠組み
	コンテンツ提供者Zとのコンテンツ提供合意文書
	作業機能：保存と蓄積
	ISO 9001 品質管理の原則
	作業機能：メタデータ管理
	作業機能：アクセスと提供
	データ保護に関する法律
	情報公開法
	プライバシー立法、個人情報の窃盗
	知的財産の保護
	電子商取引と民事・刑事法の枠組み
	消費者保護法と遠隔取引についてのEC指令
	データ利用についてのライセンスアグリーメント
	サポート機能：組織と管理
	ISO 9001 品質管理の原則
	電子商取引と、民事・刑事法の枠組み
	電子署名についてのEC指令
	欧州評議会、サイバー犯罪条約
	サポート機能：スタッフ配置
	サポート機能：財務管理
	サポート機能：技術的インフラとセキュリティ
	ISO 27001 情報セキュリティ管理システム

5.8.7.3 T5：リポジトリが遵守することに合意した自発的規約をリスト化

このセクションでは、リポジトリがリポジトリの運営方法を管理、統制するために策定、実効化した文書をリスト化しなければならない。この中には自発的最良実施規定、行動・倫理規定、組織の規定と手続きマニュアル、その他リポジトリが遵守するすべての基準が含まれるだろう。

このセクションにおいて、監査人は次のような質問を自分自身に問いかけなければならない。

- リポジトリが課している基準又は採用している基準はあるか。その中には、最良実施規定、技術又は産業上の基準など、必須及び任意の基準（あるいはその一部）が含まれているか。
- リポジトリ又はリポジトリの事業の一部が、最近、内部又は外部の監査対象となったことがあるか。それらの監査はどのような基準に基づいて行われたか。
- リポジトリが、法律、基準、規定を遵守するために、正式な遵守プログラム、戦略及び／又は手続きを適切に保持しているか。
- リポジトリが正式なリスク管理プログラムを既に適切に保持しているか。

タスクの回答例の抜粋：

T5：	**リポジトリが遵守することに合意した自発的規約をリスト化**
例：	作業機能：収集と受入
	リポジトリ X オペレーションマニュアル （2006） Intranet/Operations/OpManual.html 望ましい受入ファイルフォーマット （2006）
	作業機能：保存と蓄積
	リポジトリ X 災害計画 （2004） 非常事態計画 （2005）
	作業機能：メタデータ管理
	データ文書化の推奨基準 （2003） ISO 15489 記録管理
	作業機能：アクセスと提供
	サポート機能：組織と管理
	サポート機能：スタッフ配置
	サポート機能：財務管理
	サポート機能：技術的インフラとセキュリティ

5.8.7.4 T6：リポジトリが遵守すべきその他の文書と原則をリスト化

上述のリポジトリの運営方法に関する文書リストにすべてが網羅されていない場合、監査人はさらに次の文書に関する参考文書を提出しなければならない。

タスクの回答例の抜粋：

T6：	**リポジトリが遵守すべきその他の文書と原則をリスト化**
例：	作業機能：収集と受入
	作業機能：保存と蓄積
	作業機能：メタデータ管理
	作業機能：アクセスと提供
	サポート機能：組織と管理
	サポート機能：スタッフ配置
	サポート機能：財務管理
	サポート機能：技術的インフラとセキュリティ
	デスクにいないときはコンピュータの画面を消すこと、という内部文書に記録された共通理解

5.8.8 必要な情報が入手不可能な場合

監査のこのステージで必要なほとんどの情報は、リポジトリ内で又は公に入手可能なものであり、また入手可能でなければならない。万一、関係文書へのアクセスが困難な場合は、監査人は上級管理職者に連絡し、監査作業を完了するためにはその文書へのアクセスが重要であることを説明しなければならない。

このステージでリスト化すべき文書の中には、契約例や前回の監査結果など、機密文書や運営上慎重に扱うべき文書が含まれていることがある。そのような文書は、たとえばタイトルを匿名にしたり、物理的な場所の情報を明らかにしないなど、適切な扱いをしなければならない。

監査人がこのステージで提供する情報は全ステージを通して参照される。しかし、入手できないソースドキュメントがある場合やリストが不完全な場合、監査人は一部のリスク、特に、リポジトリの規定上の必要条件やその他の責務を果たすための組織のアクティビティが不十分なことによるリスクを識別できないかもしれない。

5.8.9 他のリポジトリから提供されるもの

リポジトリは明確に定義された法規上の枠組みの中で運営される。以下に、英国内のリポジトリがその運営において基づくであろう法規上の枠組みの一部を、完全なものではないが、例示する。ここに掲げる例は、主に英国を背景とするものであるが、監査人は自分自身の管轄地域における法規について、同等のものを推測することができる。

英国の議会制定法

- 情報自由法（2000）
- データ保護法（1998）
- 電子通信法（2003）
- 人権法（1998）
- 全国最低賃金法（1998）
- 労働時間規制（1998）
- 雇用法（2002）
- 障害者差別禁止法（1995）
- 法定納本図書館法（2003）
- 会社法（1985）
- 著作権、意匠及び特許権法（1988）

英国の規則等

- 雇用均等規則（2003）
- 職場安全衛生管理規則（1999）
- 消費者規制（2000）
- 一般に認められた会計原則（UK GAAP）
- プライバシー及び電気通信（EC指令）規制（2003）

ヨーロッパの指令、規則、決議

- 指令 2001/29/EC （ヨーロッパ著作権指令）
- 年度予算及び連結予算に関する第4次及び第7次会社法指令

標準等

- ISO 9000：2000 品質管理システムシリーズ
- ISO 27001：2005 情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-要件

5.8.10 意見募集

DCC/DPE監査・認証ワーキンググループは監査人の方々からのコメント、懸念事項、あるいは意見をお待ちしております。feedback@repositoryaudit.euまでお寄せください。

5.8.11 チェックリスト

次のステージに進む前に、監査人は次のことを行わなければならない。

- リポジトリの記録管理システムをチェックし、リポジトリの全戦略計画書が確実に識別されていることを確認する。
- 本ステージで識別・調査された文書の分析に基づき、ステージ1の目的・目標のリストを修正する必要があるかどうかを確認する。
- 本ステージでリスト化したソースドキュメントをこの後のステージで参照する必要が生じたときに、それらの文書の場所を特定しアクセスすることができるかどうかを確認する。

以上でこのステージは完了する。監査人は次の監査ステージに進み、リポジトリが目的・目標を達成するために利用する重要なアクティビティ、資産、システム、及びそれらの所有者を識別する。

5.9 ステージ3：アクティビティ、資産及びそれらの所有者の識別

本ステージは、自己監査6ステージのうちの3番目のステージである。

5.9.1 ステージ3の目的

ステージ3の目的は、リポジトリのアクティビティと作業プロセス、重要な資産と技術、及び関係スタッフについて調査し、リポジトリの作業内容と作業方法についての概念モデルを作成することである。

本ステージにおいて監査人は、リポジトリの幅広いミッション及び目的を、各リポジトリが目的を達成するために行う、より詳細なアクティビティ又は作業プロセスに分割しなければならない。各アクティビティは通常複数のスタッフにより実行され、一人がアクティビティの責任者として配置される（この自己監査ツールキットでは「所有者」と呼ぶ）。各アクティビティはリポジトリの一つ以上の重要資産と関連している。さらに、各アクティビティは、スタッフが信頼する複数の技術システムやソリューションに支えられている。技術、ソフトウェア、及びさまざまなサポートシステムが、この自己監査の資産カテゴリーの中に含まれる。たとえば、ウェブサーバーは、一つ以上の重要なリポジトリサービス（ユーザー・サービス部門によるユーザーへのデジタルコンテンツの供給など）を提供するために利用される。

自己監査プロセスの次のステージ４では、このステージでリスト化されたアクティビティ、資産、及びそれらの所有者と関連するリスクを識別する。リスクは、アクティビティや作業プロセスと関連しているだけでなく、現在危険にさらされているかもしれない重要な資産と技術や、リポジトリの機能の継続性に不可欠な重要な資産と技術にも関連している。

5.9.2 ステージ3の関連タスク

本タスクにおいて監査人は、リポジトリが所定の目的・目標を達成する助けとなるようなアクティビティ、資産、及びそれらの所有者の構造化リストを作成する。組織の公的使命、目的、目標はこのステージでリストを編集する際の参考資料として利用される。また、さまざまな内部計画書、外部の規定に関する文書も本プロセスにおいて常に参考にされる。

リストは、様式T7（自己監査ツールキットの付録1を参照）の表に基づいて編集される。

5.9.3 ステージ3で期待される成果

リポジトリのアクティビティ、資産、及びそれらの所有者のリストは、リポジトリがさらされるリスクを識別する基礎となる。このステージで作成するリストの包括性が、次のステージで作成する潜在的リスクのリストを完全にするためのきわめて重要な役割を果たす。

このステージの主要なアウトプットは、リポジトリの重要なアクティビティ又は作業プロセス、それらのアクティビティと関連する資産及びアクティビティと資産の責任者についてリスト化した表である。

5.9.4 監査プロセス全体におけるステージ3の位置づけ

アクティビティのリスト編集は、リポジトリの公的使命、目的、目標の範囲及び法規上の必要条件という背景を考慮して行わなければならない。この監査のこれまでのステージで得た情報を道標及び参考資料として利用して、このステージを実施する。

このステージで作成する重要なアクティビティと資産のリストは、後に行うリスクの識別や評価の基礎となる。

リポジトリの重要なアクティビティ、資産、技術的ソリューション及び関係するスタッフのリストは、リポジトリの業務管理、あるいは資産の目録として、この監査プロセスとは独立して役に立つことだろう。

5.9.5 ステージ3を完了させるために必要な資源

完了までの予想時間：2～4 時間

組織のアクティビティの分析は、非常に骨の折れるプロセスである。自己監査のこのセクションは、リポジトリが現在さらされており、対処が必要なリスクの包括的リストを完成させるために必要不可欠な段階である。

主に時間を費やさなければならないのは、リポジトリのアクティビティを識別すること及びアクティビティ、資産、スタッフを互いに有機的に関連するものして検討することである。既存の最新のビジネス分類体系及び資産と技術の一覧表が入手できない場合は、これらをこのステージの作業の一部として作成しなければならない。

監査人は後の監査プロセス中に、このステージで作成したリストに戻り、項目を追加したりリストを改良することができる。

ステージ3を始める前に、監査人は次のことを行わなければならない。

- 組織及び組織が運営されている背景について一般的理解を深める。
- ビジネス・アクティビティの分析を行うに当たって管理者の支援を得る。
- リポジトリのスタッフ及びそれぞれの責任範囲に関する一覧を入手する。
- 組織が自らのアクティビティや業務プロセスについて過去に分析し文書化しているかどうかを確認する。

もし他の目的のためにリポジトリがすでに分析されているのであれば、一から作業を始めるのではなく、以前の作業結果を利用できることがある。アクティビティの分析を伴うプロジェクトには次のようなものがある。

- ビジネスプロセスの再設計
- イメージ化及びワークフローのオートメーション
- アクティビティに基づく単価計算（ABC）又は管理

- ビジネスの分類化
- 品質の認定
- システムの導入

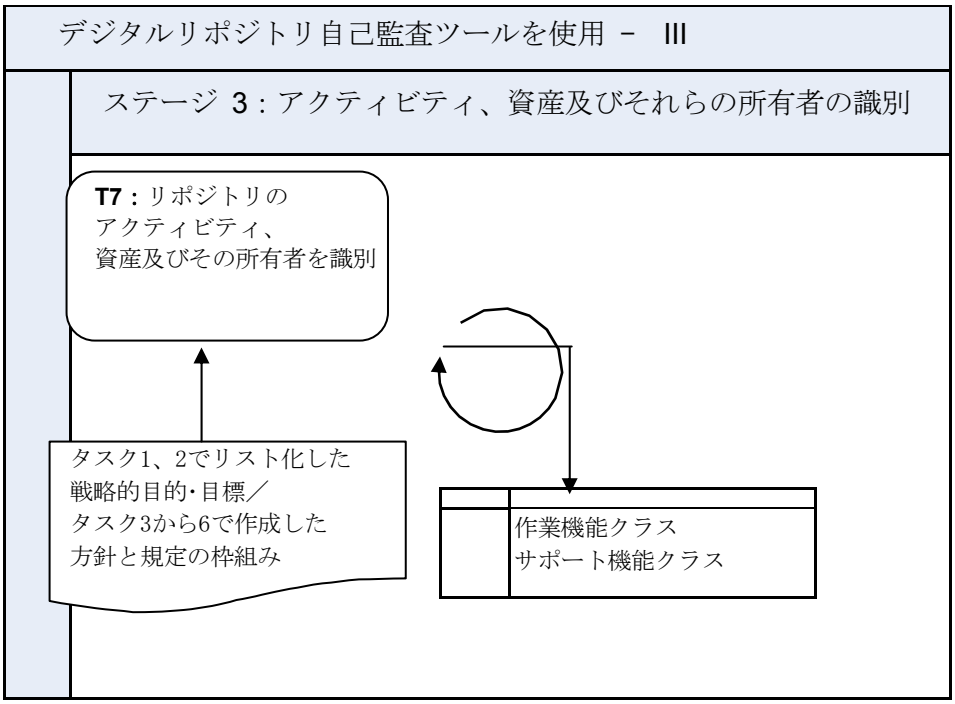
もしこのようなプロジェクトで生じた分析結果を利用できるのであれば、監査人はどのように、なぜ、いつ、これらのプロジェクトを取り上げたのかを検討し、プロジェクトの結果をこの監査のために適用できるかどうかを決定しなければならない。

資産と技術のリスト、登録簿、あるいは一覧表が、ビジネスの分析、法規遵守の調査と監査、危機管理計画の実施などを行っている間に、さまざまな目的で編集されている可能性がある。ほとんどの組織は、ITのハードウェア、ソフトウェア及びそれらのライセンスに関する一覧表を持っている。その他の有形資産（リポジトリの設備など）の一覧表も、組織の財務や資産に関するセクションから入手できるかもしれない。

ステージ3を完了するために、監査人は次のようなアクセス権を得ていなければならない。

- 内部文書（作業マニュアル、手続きガイド、タスクや目的のリスト、組織図、資産・技術・システムのリストなど）へのアクセス
- アクティビティ、資産、技術、システム及びそれらの所有者についてよく知る管理者及びIT担当者へのアクセス

5.9.6 ステージ3を示す略図



5.9.7 ステージ3を完了するための指示

組織の機能とアクティビティを識別するもっとも一般的な2つの方法は、階層分析とプロセス分析である。

階層分析では、組織の業務を一連のパートとサブパートに論理的に分割する。このプロセスは「機能分析」とも呼ばれる。このプロセスでは、まず組織のビジネスの全体像を把握し、次に詳細なパート、つまり大きなものから順に、機能、アクティビティ、トランザクションに分割する。機能とは、組織のアクティビティの高レベル集合体であり、組織の公的使命と直接結びついたものである。機能という文脈の中で、機能を達成するために組織が実施する主なタスクのことをアクティビティと呼ぶ。トランザクションとは、アクティビティの最小単位（レベル）のことをいう。

階層分析を実施するため、監査人は次のことを考慮しなければならない。

- 組織の憲章又はミッション
- 組織を特色づけているもの
- 組織が管理している機能
- 組織が実施している業務
- 組織が責任を負っているアクション
- 組織の中でアクションがどのように実施されているか。
- アクティビティが特定のエリア又はプログラム内に限定されているかどうか、あるいは組織全体で共有されているかどうか。
- 組織がどのように内部で業務を行っているか。また、外部のクライアントやパートナーとはど

のように業務を行っているか。

リポジトリに業務又は記録の分類体系があるのなら、監査人はそれをアクティビティをリスト化するための基礎として利用できるかもしれない。もし業務の分類体系がまだ作成されていないのであれば、監査人は自己監査の付加価値成果として作成を検討してもよいかもしれない。

記録分類のための分析方法の詳細については、オーストラリアの国立公文書館「DIRKSマニュアル」[24] セクションB、又はコレクションズ・カナダ[25] が提供する「ビジネスアクティビティ構造分類システム（BASCS）ガイダンス」を参照のこと。これらの資料はどちらもこのステージの指示書として利用された。

階層分析は、組織が行っていることに関する概要を明らかにしてくれる点で有益である。一方、プロセス分析では、組織がどのように業務を行うか、また、アクティビティを実施するためにどのような資産、システム、人々が関与するかについて詳細に検討する。プロセス分析（時にはシークエンシャル分析（sequential analysis）と呼ばれることもある）では、組織のタスクが機能上及び構造上の境界を越える方法について分析する。これを行うため、まず上から下への階層分析を行い、その後、どのようにアクティビティが行われるかを詳細に調査する。

資産（asset）とは組織、組織のビジネスアクティビティ及びアクティビティの継続性にとって価値又は有用性があるものである。したがって、正しいアクティビティやビジネスの継続性を確実にするためには、資産が保護される必要がある。資産の適正な管理及び説明責任は必要不可欠であり、それらはすべての管理者の重要な責任である。資産には次のように多くの種類がある。

- 情報：データベースとデータファイル、契約と協定、システム文書、研究情報、ユーザーマニュアル、研修資料、業務手続き又は事務手続き、ビジネス継続計画、故障時の代替処理、監査証跡、アーカイブされた情報
- ソフトウェア資産：アプリケーションソフトウェア、システムソフトウェア、開発ツールとユーティリティ
- 物理的資産：コンピュータ設備、通信機器、リムーバブルメディア、その他の機器
- サービス：コンピュータサービス、通信サービス、一般ユーティリティ（暖房、照明、電力、空調など）
- プロセス：ビジネスプロセス、アプリケーション固有のアクティビティ
- 人、資格、知識、スキル、経験
- 無形物（組織の評判、イメージなど）

資産の一覧があれば、資産を効果的に保護することができる。また、資産の一覧は他の業務目的、たとえば健康と安全、保険、あるいは財務（資産管理）などの目的でも必要になるかもしれない。

「所有者」という言葉は、資産の生産、開発、保存、利用及びセキュリティの管理責任を受託している個人又は実体を表す。

[24] http://www.naa.gov.au/recordkeeping/dirks/dirksman/step_B.html
[25] http://www.collectionscanada.ca/information-management/002/007002-2089-e.html

5.9.7.1 T7：リポジトリのアクティビティ、資産及びそれらの所有者の識別

自己監査のこれまでのステージで識別された公的使命、目的、目標に基づき、監査人はリポジトリのアクティビティをリスト化しなければならない。目的、目標及びそれらを統制する文書が、作業機能クラス及びサポート機能クラスに従って提示される。監査人はこのステージでできるだけ多くのアクティビティをリスト化すると共に、アクティビティの所有者、アクティビティと連結する重要な資産及びそれらを裏付ける技術的ソリューションを識別しなければならない。

タスクの回答例の抜粋

T7：	**リポジトリのアクティビティ、資産及びそれらの所有者を識別**		
機能クラス：	**収集と受入**	**資産**	**所有者**
アクティビティ：	コンテンツ提供者と納入協定書を作成	提供協定書の本文	法務担当部署
	コンテンツ提供者と提出について合意		収集担当部署
	コンテンツ提供者と共に提出に関する協定書に署名	提出に関する協定書の本文	法務担当部署
	さまざまな通信チャンネルを通して提出物を送信	FTPサーバ、DVD、提出管理ソフトウェア・ソリューション	収集担当部署
	送信されたデータのウィルスチェック	ウィルス管理ソフトウェア、プロセスエリアのセキュリティ	IT担当部署
	…	…	…

5.9.8 必要な情報が利用不可能な場合

監査人はリポジトリのアクティビティ及び資産の情報を完全、無削除な状態で入手可能でなければならない。もしそれが困難であると判明した場合は、上級管理者に連絡し、必要な情報にアクセスするための権限を取得しなければならない。このステージで作成するアクティビティと資産のリストについては、その中に含まれているかもしれない機密情報を保護するため、利用制限についての協定を結ぶことができる。リポジトリが行っていることに関する情報にアクセスできない場合は、リポジトリ自体の重要なリスクになる恐れがある。

完全なリストができるかどうかは、アクティビティと資産の識別プロセスがどの程度詳細に行われるかに左右される。このステージにおいて監査人は、後のステージで抽出されリスト化されるアクティビティや資産の潜在的リスクについて、ある程度考慮することが望ましい。リスクにさらされているとみなされるものに意識的であることが、このステージで行う作業の粒度を決定する助けとなる。

5.9.9 他のリポジトリから提供されるもの

次に示すアクティビティ及び関連資産の一般的なリストは、TRACチェックリスト及びnestorに提示された基準の分析及びISO 27001:2005 「情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム – 必要条件」から導いたものである。監査人は次のアクティビティの例から一部を選択し、自らの回答内容に取り入れるとよいかもしれない。あるいは、適時、同意義の自らの回答として言い換えるとよいかもしれない。

機能クラス	関連アクティビティと資産	所有者
S1. 組織管理（S）：	S1A1. ミッション・ステートメントと組織の目的を定義	マネジメント担当部署
	関連資産：ミッション・ステートメント	
	S1A2. リポジトリの存続期間を超える保存のためのアクティビティの継続計画	マネジメント担当部署
	関連資産：継承、不測の事態、又は第三者寄託に関する取り決め	
	S1A3. 識別されたコミュニティの定義に関する文書化と再検討	マネジメント担当部署
	関連資産：識別されたコミュニティの定義	
	S1A4. 識別されたコミュニティの見読性に関する必要条件を満足するための方針の定義、文書化、及び再検討	マネジメント担当部署
	関連資産：組織の評判	
	S1A5. 識別されたコミュニティからフィードバックを得るための仕組みの確立と利用	マネジメント担当部署
	関連資産：Eメール、その他のフィードバックの仕組み、信頼性	
	S1A6. 情報を保護するために必要なデジタルコンテンツの重要な特徴の定義	マネジメント担当部署
	関連資産：	
	S1A7. ビジネス・アクティビティの各面を統制するための方針と手続きの定義、文書化及び再検討	マネジメント担当部署
	関連資産：方針と手続きの文書	
	S1A8. 著者、コンテンツ提供者、ユーザーとの法的協議書に関する交渉及び履行	マネジメント担当部署
	関連資産：契約書	
	S1A9. 法的又は規定上の必要条件に関する責任の履行	法務担当部署
	関連資産：	
	S1A10.組織の評価制度（内外の監査やリスク分	マネジメント

	析を含む）を利用する	担当部署
	関連資産：認定証、リスク登録簿、組織の評判	
S2. スタッフ配置（S）：	S2A1.適正な人材を必要数配置する	人事担当部署
	関連資産：スタッフ	
	S2A2.役割、責務とそれらの関連を定義する	人事担当部署
	関連資産：スタッフ、組織概要文書	
	S2A3.実施中のスタッフの研修に必要な事項を識別し、満足するメカニズムの定義と導入	人事担当部署
	関連資産：研修実施のためのリソース、スタッフ	
	S2A4.人事評価方法（内外の監査やリスク分析を含む）の利用	マネジメント担当部署
	関連資産：認定証、リスク登録簿、組織の評判	
S3.財務管理（S）：	S3A1.短期・長期のビジネスプランを定義、導入、レビューする	マネジメント担当部署
	関連資産：事業計画書、売上高（利益）	
	S3A2.財務上の赤字をモニターし、対処する	マネジメント担当部署／予算担当部署
	関連資産：売上高（利益）、財務計画	
	S3A3.法律上の管轄地域における財務関連法への準拠	法務担当部署
	関連資産：	
	S3A4.財務評価方法（内外の監査やリスク分析を含む）の活用	マネジメント担当部署
	関連資産：財務監査結果、リスクの登録簿、組織の評判	
S4. 技術的インフラとセキュリティ（S）：	S4A0. 戦略的IT計画を定義	技術担当部署
	関連資産：IT計画書	
	S4A0.1. 情報アーキテクチャーを定義	技術担当部署
	関連資産：システムのハードウェア、ソフトウェア、通信インフラ	
	S4A1. ハードウェア、ソフトウェアのインフラの現在の適合性、適性を確実にするための監視	技術担当部署
	関連資産：ソフトウェア、ハードウェア	
	S4A2. ハードウェア及び媒体のリフレッシュ方策の実施	技術担当部署
	関連資産：	
	S4A3. システムの維持、セキュリティパッチの	技術担当部署

	インストール、及びソフトウェアの更新を適時実施	
	関連資産：ソフトウェア更新の仕組み	
	S4A4. 最重要システム変更の試験結果、必要な場合は変更を取り消し	技術担当部署
	関連資産：ソフトウェア、ハードウェアの試験環境	
	S4A5. ITインフラと物理的インフラにおけるセキュリティ方策の実施	
	関連資産：セキュリティのインフラ（セキュリティ・ドア、セキュリティ・スタッフ、通行カード、エンコード・ソフトウェア、パスワード、セキュリティ試験ツールなど）	技術担当部署／物理的セキュリティ担当部署
	S4A6. 冗長コピーデータの保存と蓄積、オフサイトでのバックアップ	
	関連資産：バックアップの仕組み、バックアップのテープ	技術担当部署
	S4A7. 災害復旧についての検討と試験、及びビジネス継続計画	
	関連資産：継続性、災害計画又は撤退戦略	マネジメント担当部署
	S4A8. 技術とセキュリティの評価方法（内外の監査やリスク分析を含む）の活用	
	関連資産：認定証、リスクの登録簿、組織の評判	マネジメント担当部署
C1. 収集と受入（C）：	C1A1. 受入可能な提出フォーマットの定義	
	関連資産：提出パッケージの定義	受入担当部署
	C1A2. 受け入れたコンテンツの監視、記録、及び可能であれば完全性の実証	
	関連資産：チェックサム、チェックサムの比較アルゴリズム	受入担当部署
	C1A3. 受け入れたコンテンツの完全性と正確性を実証	
	関連資産：デジタルオブジェクト	受入担当部署
	C1A4. 受け入れたコンテンツの物理的・技術的管理を確立	
	関連資産：デジタルオブジェクト	受入担当部署
	C1A5. 著者及びコンテンツ提供者に、保存責任の引受又は拒否を報告する仕組みの確立	
	関連資産：Eメール、その他の報告の仕組み	受入担当部署
	C1A6. 提出されたコンテンツからアーカイブ形式への変換を実施	受入担当部署

	関連資産：変換ツール、デジタルオブジェクト	
	C1A7. アーカイブ形式に変換しない提出物の廃棄	受入担当部署
	関連資産：廃棄ツール	
	C1A8. 機能評価（内外の監査やリスク分析を含む）の方法の活用	マネジメント担当部署／受入担当部署
	関連資産：認定証、リスクの登録簿、組織の評判	
C2. 保存と蓄積（C）：	C2A1. アーカイブコンテンツに唯一不変的な識別子を割り当て	保存担当部署
	関連資産：識別子スキーム、デジタルオブジェクト	
	C2A2. アーカイブコンテンツに対するすべての変更を文書化	保存担当部署
	関連資産：変更管理ツール、デジタルオブジェクト	
	C2A3. アーカイブコンテンツをオブジェクトごと及びコレクションごとの単位で監視及び完全性の実証	保存担当部署
	関連資産：チェックサム、チェックサムの比較ツール、デジタルオブジェクト	
	C2A4. 物理的な保存用ストレージとマイグレーションに関する戦略の実施と再検討	保存担当部署
	関連資産：マイグレーションツール、媒体、デジタルオブジェクト	
	C2A5. 保存計画の定義、再検討、及び実施	保存担当部署
	関連資産：保存戦略、保存ツール	
	C2A6. 機能評価（内外の監査やリスク分析を含む）の方法の活用	マネジメント担当部署／保存担当部署
	関連資産：認定証、リスクの登録簿、組織の評判	
C3. メタデータ管理（C）：	C3A1. アーカイブコンテンツの保存メタデータを収集	文書化担当部署
	関連資産：保存メタデータの記録	
	C3A2. アーカイブオブジェクトの見読性確保のために必要な意味的・技術的コンテキストの確立、文書化及び監視	文書化担当部署
	関連資産：表示情報記録、表示情報の登録	
	C3A3. 検索を容易にするための適切な記述メタ	文書化担当部署

	データの取得又は作成	
	関連資産：記述メタデータの記録	
	C3A4. メタデータとアーカイブコンテンツ間の参照整合性を維持	文書化担当部署
	関連資産：デジタルオブジェクト、メタデータ記録、関連を維持するためのソフトウェア	
	C3A5. 機能評価（内外の監査やリスク分析を含む）の方策の活用	マネジメント担当部署／文書化担当部署
	関連資産：認定証、リスクの登録簿、組織の評判	
C4. アクセスと提供（C）：	C4A1. コンテンツの検索、選択、アクセスを行うための仕組みを提供	提供担当部署
	関連資産：提供システム（ウェブサーバ、アプリケーション）	
	C4A2. 合意済みアクセス権と制限を反映するための認証と認可のサブシステムを実施	提供担当部署
	関連資産：認証と認可のシステム、契約	
	C4A3. アーカイブコンテンツを提供形式に（ユーザー及びユーザーコミュニティの要望に合わせて）変換	提供担当部署
	関連資産：変換の仕組み	
	C4A4. 提出されたとおりの完全で真正なオブジェクト（提出された原資料に対応させることのできるオブジェクト）を提供	提供担当部署
	関連資産：デジタルオブジェクト、比較の仕組み	
	C4A5. 機能評価（内外の監査やリスク分析を含む）の方策の活用	マネジメント担当部署／提供担当部署
	関連資産：認定証、リスクの登録簿、組織の評判	

*注 （C）＝作業機能クラス、（S）＝サポート機能クラス

5.9.10 考察

組織の構造及び割り当てられた資源の適性の分析も行うことが望ましい。リポジトリの目的、アクティビティ、及び資産の比較によって、潜在的リスクが明らかになる。

5.9.11 意見募集

DCC/DPE監査・認証ワーキンググループは、監査人の方々からのコメント、懸念事項、あるいは意見をお待ちしております。feedback@repositoryaudit.euまでお寄せください。

5.9.12 チェックリスト

次のステージに進む前に、監査人は次のことを確実に終えていなければならない。

- ◆ リポジトリのアクティビティ、資産及びそれらの所有者を識別する。
- ◆ 必要に応じて、これまでのステージで作成された目的・目標、及び規定に関する文書のリストを更新する。
- ◆ 上級管理職者と共に調査結果を承認する。

5.10 ステージ4：リスク識別

このステージは、自己監査の6ステージのうちの4番目のステージである。

5.10.1 ステージ4の目的

ステージ4の目的は、組織のアクティビティと資産から、リポジトリが直面する関連リスクをすべて洗い出すことである。一部のリスクは、公的使命と目的、法規上の枠組み及びリポジトリの作業（アクティビティ、資産、スタッフ配置、技術的ソリューション）のモデルを調査することにより把握できるかもしれない。このステージの主な成果は、組織の「懸念の範囲」を明確にし、リスク管理が必要になる領域を詳述することである。リスクの影響及び尤度の評価は、自己監査プロセスの次のステージで行う。

5.10.2 ステージ4の関連タスク

ステージ3で識別したアクティビティと資産は、必然的に、このツールキットの中でリスクと見なされる脆弱性と関連することになる。このタスクにおいて監査人は、組織の目的、及びそれらの達成に必要となるアクティビティと資産に基づき、リスクを構造化した一覧を作成する。リスクを識別する方法に、唯一普遍的なものはない。もっとも効果的なアプローチは、ブレーンストーミング法により潜在的リスクをすべて洗い出してリスト化し、その後、必要に応じて、詳細化、グルーピング、及び分割を行う方法である。いったん最初のリストを作成した後、監査人は外部ソースや、類似の組織が行った評価から、リスク例をさらに知ることになるだろう。自己監査人はこれらのリスクを使って残りのすき間を埋め、リスクを網羅するリストを確実に文書化することができる。

添付の様式を使い、監査人は関連リスクの記述、リスクに関する所有者の任命（特に指定がなければ、資産又はアクティビティの識別された所有者を任命する）、及びリスクに関するステークホルダーの特定を行うことができる。また、監査人は、各入力に関連するリスクを詳細化することにより、リスク間の関係を文書化することもできる。

リスクを洗い出すとき、監査人は、アクティビティと資産に関する次のようなリスクを考慮することが望ましい。

- 資産又はアクティビティが、関連する組織の目的・目標を達成することができないリスク、又は達成に十分貢献できないリスク
- 内部の脅威がアクティビティの達成を1つ以上妨げるリスク
- 外部の脅威がアクティビティの達成を1つ以上妨げるリスク
- 脅威により、リポジトリの資産に対して、許可されていない開示、修正、不正行為、破壊、利用不可能な状態又は損失が起こるリスク

リスクは、その原因について長々と思案するのではなく、その影響について考えなければならない。原因については、後に文書化するリスクの明示の中で取り組む。

5.10.3 ステージ4で期待される成果

ステージ4は、自己監査プロセスの中のリスクに焦点を当てた3つのステージのうちの、最初のステージである。ある意味では、このステージがもっとも重要なステージである。なぜなら、このステージにおいて監査人は、リポジトリの各面で直面するすべてのリスクを洗い出すからである。このステージの成果が十分でないと、後の作業が不完全なものになる。

監査プロセスの次のステージに進む前に、次のことを達成していなければならない。

- 後のプロセスを確実に遂行するため、機能クラス、組織の目的及び識別されたアクティビティと資産に従って分類されたリスクの包括的リストを作成
- 識別されたリスク間の関係についての第一段階の検討
- 各リスクに対し、必須項目として所有者と種別分類、及び任意項目として他のリスクとの関係を記した属性のサブセットを作成（後者は、今後の自己監査のステージにおいて引き続き分析されることになる。）

ステージ4で洗い出すリスクのリストは、後の自己監査のステージでさらに練り上げられる。特に、各リスクはそれぞれのより詳細な記述により、変わることがある。このステージの成果は初期段階のリスク登録簿ではあるが、適切なリスク評価が行われるまで、この最初の形式の資源にほとんど価値はない。

5.10.4 監査プロセス全体におけるステージ4の位置づけ

ステージ4では、監査プロセスのこれまでのステージで作成した組織についての記述に基づき、自己監査の対象リポジトリに関するリスクの包括的な目録を作成する。

ステージ4で識別されるリスクは、評価及びより詳細な記述の対象となると共に、各リスク間の関係がさらに詳しく検討され、文書化される。

5.10.5 ステージ4を完了させるために必要な資源

完了までの予想時間：4 時間

自己監査のステージ4は、非常に時間のかかる作業になると思われる。監査人はステージ5に進む前に、このステージの作業結果の包括性に確信を持っていなければならない。このステージに戻り、リスクに対して修正や追加を行う必要性が出てくることは十分にありうるが、これはきわめて好ましいことである（実際、そうする方がよい）。リスクの洗い出しが容易かどうかは、監査人がアクティビティと資産をどれだけ詳細に定義したかによって、大きく左右される。リスクは、大まかに述べた少しの例から洗い出すよりも、より精密に定義した多くのアクティビティから洗い出す方がより効率的である。このプロセスを容易に行うためには、アクティビティと資産を洗い出すレベルが、ステージ3で提供した例のレベル相応であることが望ましい。

監査人は、必要であれば、後にこのステージに戻り、情報の追加や修正を行うことができる。

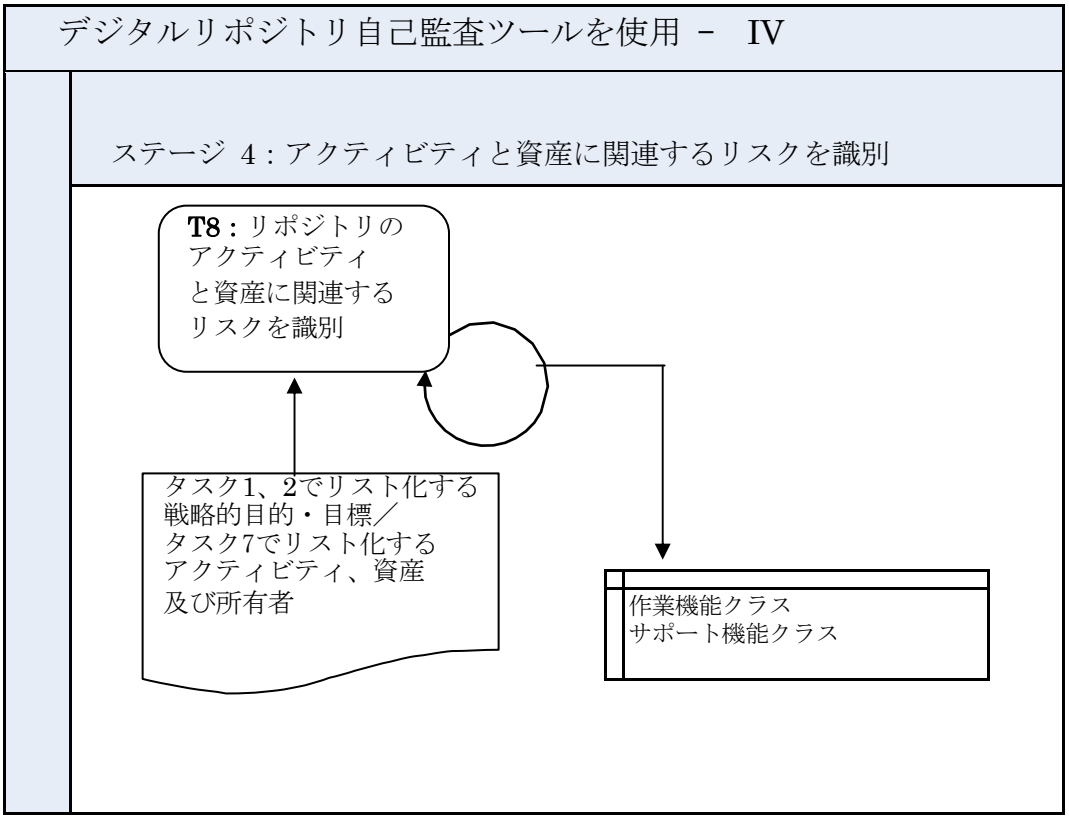
ステージ4を始める前に、監査人は次のことを行わなければならない。

- リポジトリの適切な担当者と関係を築き、識別したアクティビティと資産の完全性及び正確性について承認してもらう。
- リポジトリの適切な担当者に、特定のリスクと、アクティビティと資産との関係に応じて分類した関連リスクについて、意見を求める。
- 組織内ですでに行われたリスク評価の結果、又はすでに着想されている継続的計画を参照する。

ステージ4を完了するために、監査人は次のようなアクセス権を得ていなければならない。

- 内部の政策文書へのアクセス
- 外部の文書やソースへのアクセス（法規、標準、実施規準など）
- リポジトリの特定の領域に関連するリスクについてよく知るリポジトリの職員へのアクセス

5.10.6 ステージ4を示す略図



5.10.7 ステージ4を完了するための指示

組織の資産とアクティビティからリスクを導き出すタスクは単純であるが、リスクを包括的に洗い出すためには、多大な努力が必要かもしれない。

5.10.7.1 T8：リポジトリのアクティビティと資産に関連するリスクを識別

リスクの洗い出しのプロセスは、機能クラスによって構造化される。つまり各機能クラスにおいて、内在する組織の目的、及びその目的の達成に必要な関連する資産やアクティビティが、リスクやリスクのグループと関連づけられる。自己監査人はこれまでの3つのステージで出した回答を参照にして、組織のリスクの全体像を構造化し、完全なものにしなければならない。

リスクは一般的にアクティビティと関連しているだけでなく、アクティビティ自身、アクティビティの目的／実現可能なこと、及びアクティビティの構成方法の中に含まれていることもある。さらに、リスクはスタッフの不足、未熟なスタッフ、知識不足又は関連する知識基盤へのアクセス不可、及び適切なツールの不足と関連していることもある。

タスクの回答例の抜粋

T8：	リポジトリのアクティビティと資産に関連するリスクを識別	
機能クラス：	収集と受入	所有者
アクティビティとリスク：	コンテンツ提供者と納入協定書を作成	法務担当部署
	コンテンツ提供者と提出について合意	収集担当部署
	コンテンツ提供者と共に提出協定書に署名	法務担当部署
	さまざまな通信チャンネルを通して提出物を送信	収集担当部署
	送信されたデータのウィルスチェック	IT担当部署
	...	...

リスク識別子：	R1	
リスク名称：	契約義務の不履行に対する法定責任	
関連アクティビティ：	コンテンツ提供者と納入協定書を作成 コンテンツ提供者と共に提出協定書の署名	
リスクの性質：	物理的環境	
	人事、経営及び管理の手続き	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者：	法務担当者	
ステークホルダー：	コンテンツ提供者または作成者	
関連リスク：	R5、R6	
リスク識別子：	R2	
リスク名称：	構造的非有効性または受け取ったパッケージが適切な形式でないこと	
関連アクティビティ：	コンテンツ提供者と提出について合意	
リスクの性質：	物理的環境	
	人事、経営及び管理の手続き	
	業務及びサービス提供	X

	ハードウェア、ソフトウェアまたは通信機器・設備
所有者：	受入、保存
ステークホルダー：	コンテンツ提供者または作成者
関連リスク：	R3、R4

5.10.8 必要な情報が利用不可能な場合

内部の方針や外部の規定に関する文書及び関連する組織のリスクについて説明できるスタッフが欠如しているまたは利用できない場合は、それ自体をリポジトリの継続的な運用可能性についての深刻な潜在的リスクと見なすべきである。したがって、こ監査プロセスのその後のステージにおける評価、退避及び対処の仕組みについて考えるまえに、まずはこれらを文書化しておく必要がある。

5.10.9 他のリポジトリから提供されるもの

以下に示すリスクの一般的なリストは、TRACとnestorのチェックリスト、及びISO 27001基準に規定されるアクティビティを分析して、作成したものである。監査人は、次の回答にあるリスク例を選択して取り込むほか、適切な場合は、言い換えを行うことができる。。

ただし、ここに示したリスクは機能クラスに従って分類してあるが、中には2つ以上のグループに関係しているものもあるかもしれない。この可能性を軽視してはならない。

No.	*リスク名*
組織管理	
R01	マネジメントの失敗
R02	信頼または評判の喪失
R03	アクティビティの見落とし及び不適当な資源配分
R04	事業目的の未達成
R05	リポジトリの公的使命の喪失
R06	コミュニティの要求の大幅な変更
R07	コミュニティの要求の錯誤または誤解
R08	リポジトリの業務の強制的な停止
R09	コミュニティからのフィードバックの不受理
R10	コミュニティからのフィードバックに対する不対応
R11	デジタル情報の必要不可欠な特徴の保存の失敗
R12	事業方針及び手法の不周知
R13	非効率な事業方針及び手法
R14	一貫性を欠くまたは矛盾する事業方針及び手法
R15	知的財産権の侵害に対する法的責任
R16	契約上の義務違反に対する法的責任
R17	法律要件違反に対する法的責任

R18	規制違反に対する責任
R19	リポジトリの成功の度合いに対する評価能力不足
R20	リポジトリの成功の度合いに関する誤った認識
スタッフ配置	
R21	主要なスタッフの喪失
R22	スタッフのスキルの低下
R23	スタッフのスキルの陳腐化
R24	スタッフの効率または適性を評価するための能力の不足
財務管理	
R25	リポジトリの責務を果たすための財源の不足
R26	資金配分の失敗
R27	財務関連法規を遵守しない事に対する責任
R28	資金不足または収入の制限
R29	予算の削減
技術的インフラとセキュリティ	
R30	ハードウェアの不具合または非互換性
R31	ソフトウェアの不具合または非互換性
R32	ハードウェアやソフトウェアが、リポジトリにおいて新たに出現してくる目標の達成をサポート出来ない。
R33	ハードウェアまたはソフトウェアの陳腐化
R34	メディアの劣化または陳腐化
R35	セキュリティの脆弱性の悪用
R36	未確認のセキュリティ侵害、脆弱性または情報の劣化
R37	ハードウェアのストレージスペースに対する物理的な侵入
R38	ソフトウェアへのローカル侵入又はリモート侵入
R39	当該地域における破壊的な環境現象
R40	偶発的なシステムの混乱
R41	故意によるシステムへの破壊行為
R42	リポジトリのサイトが壊れる、または使用不可能になる
R43	基幹的公益サービスが利用できない（電気、ガス、ネットワークサービス、水など）
R44	第三者によるその他サービスの停止
R45	第三者サービス業者とのサービス契約における条件の変更
R46	主要な文書の破壊
R47	技術的インフラ及びセキュリティの有効性を評価するための能力の不足
収集と受入	
R48	受け取った情報パッケージが構造的に無効または不正な形式をとっている。
R49	提出された情報パッケージに不備がある
R50	受入中に、情報の変更やメンテナンスが、外部の意思により行われる
R51	受け取った情報パッケージを追跡できないアーカイブ情報
保存と蓄積	
R52	情報の機密性の喪失
R53	情報やサービスが提供出来なくなる
R54	情報の真正性の喪失
R55	情報の完全性の喪失
R56	未確認の情報変更
R57	責務否認を防止する能力の喪失
R58	情報の信頼性の喪失
R59	情報来歴の喪失
R60	バックアップの喪失または不適合
R61	冗長コピーの不一致
R62	何がアーカイブオブジェクトの範囲に入るのか不明確
R63	受入プロセスの有効性を確認する事ができない

R64	情報参照整合性のための識別子に障害が起きる
R65	保存計画を実施に移せない
R66	保存対策の実施が情報の喪失をもたらす
R67	保存プロセスの有効性の確認が出来ない
R68	受入時、アーカイブ時、提供時の情報パッケージが追跡できない
メタデータ管理	
R69	情報参照整合性のためのメタデータに障害が起きる
R70	変更履歴の記録が不完全あるいは不正確
R71	情報オブジェクトの検索不能
R72	見読性の定義が曖昧
R73	情報の意味的または技術的見読性における欠陥
アクセスと提供	
R74	情報提供サービスが利用不能
R75	認証サブシステムの障害
R76	権限付与サブシステムの障害
R77	情報提供メカニズムの有効性を確認する能力の不足
R78	パフォーマンス水準やサービス水準の低下

5.10.10 意見募集

DCC/DPE監査・認証ワーキンググループは監査人の方々からのコメント、懸念事項、あるいは意見をお待ちしております。feedback@repositoryaudit.euまでお寄せください。

5.10.11 チェックリスト

次のステージに進む前に、監査人は次のことを終えているかどうかチェックすること。

- ◆ 各機能クラスに対応するリスク及び組織のアクティビティと資産に関連するリスクをすべて洗い出し、文書化している。

5.11 ステージ5：リスク評価の実行

これは自己監査6ステージ中5番目のステージである。

5.11.1 ステージ5の目的

このステージの目的は、ステージ4で導き出されたリスクとリスクの関係を特徴付けし、各リスクの深刻度についての評価を実行することである。各リスクは、いくつかの特性が付与されなければならない。中でも最も重要な特性は、各リスクが実際に起こる可能性（尤度）及び潜在的影響を表す値である。この値は、累積的には、リポジトリの事業活動についての全般的な危険性に関する定量化された指標となる。

5.11.2 ステージ5の関連タスク

リスク評価の基本的な構成要素は、各特定のリスクに関連する可能性及び潜在的影響である。これらの値を単純に掛け合わせた積は、そのリスクの深刻度として表すことができる。これらの値は、組織が業務を行う状況、組織が管理するインフラ、方針及び仕組み、ならびに他の関連リスクとの関係による影響を受ける可能性がある。

監査人は、ステージ4で識別した各リスクについて包括的なリスク評価を実行しなければならない。これは主として連続的なプロセスであり、既に認識されている各リスクに対応した個々のリスク記入フォーム（このリポートの第Ⅲ部のフォームT9を参照のこと）を完成させる。各リスクに関して、監査人は次のことを提示しなければならない。

リスク特性	リスク特性の定義
リスクの発現	このリスクが実際に発現する恐れのある状況の例。リスクの発現は主として、特定の脅威（起こるかもしれないことあるいは起こらないかもしれないこと）及び脆弱性（ある特定の状況下においてリスクにさらされる組織の特性）という観点で提示する。
リスクの可能性のスコア	このスコアは、下欄で詳述される値に対応しており、この特定のリスクが発現する尤度として考えられている程度を表す。
リスクの影響のスコア	このスコアもやはり、下欄で詳述される値に対応しており、このリスクが発現した場合の影響として認識されている程度を表す。影響の大きさは、アーカイブされたデジタルオブジェクトの真正性と見読性が失われることに関連して決まる。これらが失われることは、このツールキットの監査対象となりうるリポジトリの失敗の表出と見なされるからである。
リスクの深刻度	可能性と潜在的影響のスコアを乗じて算出される値。
リスクの関係	監査人はこの欄に当該リスクと関係のある各リスクを記述するべきである。
リスクの上位所有者	定められたリスク所有者がリスクを管理できない場合に、そのリスクに対する最終的な責任を負う者。

監査人による各関連リスクについてのリスク評価が完了したら、そのリスク評価の結果と外部ソース

からの事例及び類似リポジトリが実施した評価の事例とを照らし合わせることとする。監査人は、リスク評価が完全かつ正確であることを確かめるためにこれらの事例を参照することができる。

5.11.3 ステージ5で期待される成果

ステージ5は、自己監査プロセスのうち、リスクに焦点を当てた3ステージ中2番目のステージである。リスクの包括的なリスト化が完了したと仮定すると、このことによって監査人は自分の組織が直面するリスクのうち最も優先度の高いリスクはどれなのか、及び最も深刻な脅威はどこにあるのかということがよりわかるようになる。

次の監査プロセスであるステージ6に移る前に成し遂げるべき成果を次に示す。

- ステージ5までにリスト化された各リスクは、発現する可能性と潜在的影響に従って、他のリスクとの関係という観点から特徴付けすべきである。
- 完了したと確認された、機能クラス、組織の目的ならびにアクティビティ及び資産による分類が既にあるが、監査人はまた他の特徴、とりわけリスクの関係に従ってリスクを分類してもよい。
- 各リスクに対して、その予想される尤度と潜在的影響のスコアを基に定量化した深刻度のスコアが算定されるものとする。

5.11.4 監査プロセス全体におけるステージ5の位置づけ

ステージ5は、ステージ4で識別したリスクのリストに基づいており、監査人は自分の組織が直面する各リスクの評価を行うものである。

リスクが評価された後、続くステージ6では、監査人は、現在実施されている又は実施が予定されているリスク管理の仕組みを記入することになる。このことによって、リスク回避（リスクが発現する可能性を制限する）及びリスク対処（潜在的影響を制限する）のための方法が取り入れられることになる。ステージ5では、既に実施しているリスク管理の手法についてある程度考慮することを前提とする。リスクの尤度あるいは影響についての評価はいずれも、既に実施されている管理インフラと切り離して考えることはできないからである。また、いずれの特性に対しても中立的な値は想定し難い。これらの特性はそれを取り巻く状況に依存するからである。たいていの組織では雨による損傷を防ぐために確実に屋根を取り付けているという事実を考慮しないのであれば、リポジトリの文書が破壊される「自然発生的」尤度は非常に高い。しかし、ステージ6では、すべての管理手段についてさらに明確に言及する。そして監査人は、その時点でリスクの発現可能性及び影響についての評価を修正する機会が得られるものとする。

5.11.5 ステージ5を完了させるために必要な資源
完了までの予想時間：4時間

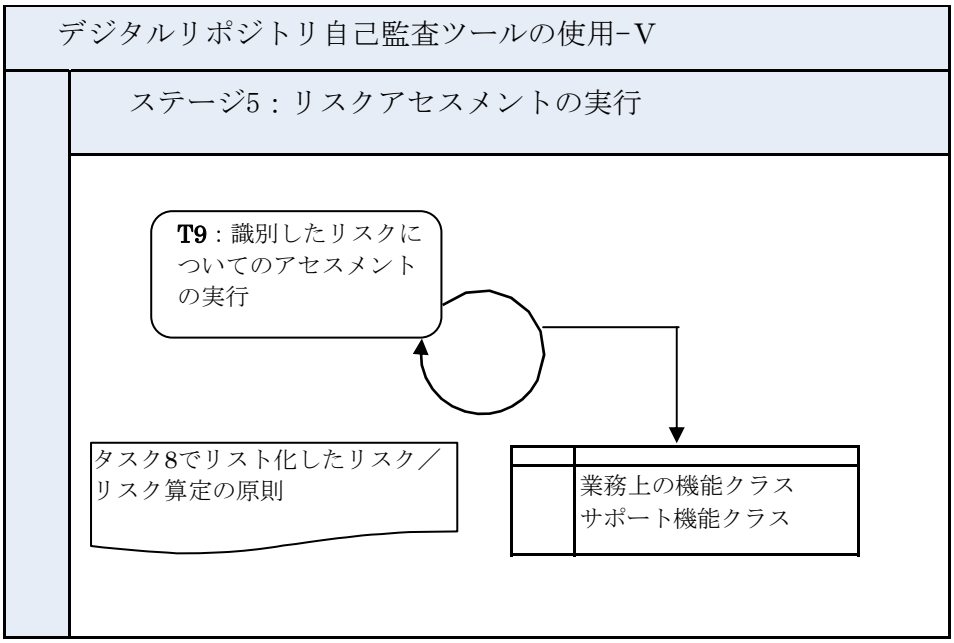
ステージ5を開始する前に、監査人は次のことをすべきである。

- 適切なリポジトリの担当スタッフと協働し、識別したリスクが完全かつ正確であることを保証すること。

ステージ5を完了させるために、監査人は次のことを行う必要がある。

- リスク回避及びリスク対処手段についての方針を記載した内部文書へのアクセス
- リスクの発現可能性あるいは潜在的影響の値の根拠あるいはその正当性を示すための内部又は外部で作成された文書へのアクセス
- 法律、規範、行動基準などの外部の文書及び資源へのアクセス
- そのリポジトリの特定の特徴に関連するリスクについての知識を持っている他のリポジトリ要員へのアクセス

5.11.6 ステージ5を表す略図



5.11.7 ステージを完了するための指示

5.11.7.1 T9 識別したリスクについての評価の実施

自己監査人は、各リスクについて以下の各項目を追記し、リスク表の記入項目を完成すべきである。

- リスク発現例
- リスクの発現可能性
- リスク発現の潜在的影響
- 当該リスクと他のリスクとの特定の関係
- 当該リスクに対して最終的な責任を負うリスクの最終的所有者
- 発現可能性の値と潜在的影響の値を乗じて算出するリスクの深刻度、すなわち深刻さを定量化した値

各リスクの発現例を提示することにより、監査人が各リスクの発現可能性及び潜在的影響に対する理解を深めることが期待される。加えて、リスクが発現する状況についての理解を深めることによって、効果的なリスク回避及びリスク対処の手段を考えるこの後のプロセスが容易になることが期待できる。

監査人は特定のリスクの発現を招く脅威及び脆弱性の種類をリスト化しなければならない。これには複数の実例を記入してよい。リスクが存在しうる様々な状況をすべて考慮したと確信するまで監査人はこの作業を続けるべきである。

発現可能性とは、特定のリスクが発現する尤度を表す。これは特定の期間内における発現件数という観点で表される。個々の可能性を示す6つの値（スコア）のうちどれか1つを選択することができる。最小の可能性値（「最も起こりにくい」ことを示す）は可能性が極めて低いことを表しており、これは100年に1回又はそれより低い頻度で発現する可能性のあるリスクに対する値として適切である。可能性の最も高いリスクは、1か月に1回以上の頻度で発現する可能性があるものとする。監査人は、可能性を適切に示す数値で表した指標を提示するとともに、その数値の選択が正当であることを証明しなければならない。これは、組織自体がそれまでに内部で蓄積した経験あるいは着手した評価、あるいは外部で着手された作業の参照であってもよい。正当であることの証明にあたっては、可能な限り、その値を選択した根拠となる根拠書類に言及すべきである。既述のとおり、いかなるリスク尤度あるいは影響の評価も、既存の管理インフラと切り離して考えることはできない。従って、可能性は既存のリスク回避手段に準拠すべきである。これについては、評価プロセスのステージ6でさらに詳細に取り組むことになる。
自己監査ツールキットは、次の基準に従ってリスクの発現可能性を考慮する。

リスクの発現可能性のスコア	説明
1	可能性が極めて低い。100年に1回以下の発現頻度
2	可能性が非常に低い。10年に1度の発現頻度
3	可能性が低い。5年に1回の発現頻度
4	可能性は中程度である。1年に1回の発現頻度
5	可能性が高い。1か月に1回の発現頻度
6	可能性が非常に高い。1か月に複数回の発現頻度

リスクの影響は、直接的なコストあるいは財政面での損失という観点でのみ評価されることが多いが、デジタル情報を保存している組織について評価を実施するときには、財政面での直接的影響の評価が最も重要なものだと言うことはできないだろう。デジタルリポジトリにおいては、財政的な損失は、情報の損失や情報への不当なアクセスによって、あるいは保存管理が適切にされていないことによって発生する。リポジトリが真正性及び見読性のあるデジタルオブジェクトへのアクセスを提供できることが、リスクの影響を決定する最も重要な要因として考慮されるべきである。従って、監査人は、次の領域におけるリスクの影響を第一に考慮すべきである。

- リポジトリスタッフあるいは公共の福祉に対する影響
- 施設、技術あるいは情報資産についての損害あるいは損失の影響
- 法令違反の影響
- リポジトリの評判における損害
- リポジトリの財政運営における損害
- リポジトリの成果あるいはサービスの質の低下
- 環境に対する損害

これらのリスク領域を考慮に入れた上で、デジタルオブジェクトの真正性及び見読性の損失という観点による潜在的影響を導き出すことは監査人の責任である。本評価ツールの視点からすれば、真正性及

び見読性を損なうことは、リポジトリがその機能を果たすことができないということを表す。この場合もまた、現実にはリスクの影響をまったく独立したものとして考えることはできないため、リポジトリが利用できる既存のリスク対処の手段をすべて考慮に入れて、値を選択すべきである。これについては評価プロセスのステージ6でさらに詳細に取り組まれるべきものである。

リスクの潜在的影響は次の基準に従って分類される。

リスクの影響スコア	説明
1	影響なし。デジタルオブジェクトの真正性及び見読性の損失はない。
2	軽微な影響にとどまる。デジタルオブジェクトの真正性及び見読性の損失は単独であり、完全に復元可能である。
3	表面的な影響にとどまる。デジタルオブジェクトの真正性及び見読性の損失は広範囲に及ぶが、完全に復元可能である。
4	中程度の影響がある。デジタルオブジェクトの真正性及び見読性の損失は全般に及ぶが、完全に復元可能である。
5	影響が大きい。デジタルオブジェクトの真正性及び見読性が復元不可能な状態になるなど、単独の損失を招く。
6	相当に影響が大きい。デジタルオブジェクトの真正性及び見読性が復元不可能な状態になる又はサードパーティによってのみ復元可能な状態になるなど損失が広範囲に及ぶ。
7	壊滅的な影響。デジタルオブジェクトの真正性及び見読性の損失が全体に及び、復元不可能な事態を招く。

この場合もまた、監査人は、適切な影響度に対応した指標を提示するとともに、その値の選択が正当であることを証明すべきである。可能性の場合と同様に、これは内部向けに提示されたものであっても外部的に提示されたものであってもよい。そして、できればその値を選択した根拠となる書類に言及すべきである。

リスク間の関係は次の特徴のうち1つないし2つ以上で表すことができる。

リスクの関係	リスクの関係の定義
爆発的	n件のリスクが同時に現実化した時の影響が、単独で発生した各リスクの合計値を上回る場合。
連鎖的	あるリスクが現実化されると、他のリスクの尤度が大きくなる場合。
相補的	あるリスクについての回避または処理メカニズムが、他のリスクの管理にも役立つ場合。
ドミノ的	あるリスクに関連する回避または処理が、他のリスクについての回避または処理の有効性を減少させる場合。
原子的	リスクが単独で存在しており、他のリスクに一切関係していない場合。

実際には、原子的リスクのような状況が起こることはまれであり、あるリスクを処理あるいは回避するためにより多くの資源を割り振ると、ほとんどの場合、他に割り振る資源が少なくなるということを意味する。少なくともこの意味において、あるリスクを処理するための戦略が他のリスクの管理に役立ち、関係が相補的である場合を除いては、すべてのリスクがすべての他のリスクと負の関係を持つこと

になる。関係の例は、一方向あるいは双方向の場合がある。また階層性をもつ場合もある。リスクのつながりの強さは様々である場合もある。また2つ以上のリスクとの関係を持つこともあり得る。

各リスクの関係欄に、監査人は（短いリスク識別子を使って）関係するリスクを記録し、可能性、影響あるいは管理のしやすさのヴァリエーションの観点からその関係の性質及びその因果関係を記述すべきである。

リスクの上位所有者を順に記入する。リスクの上位所有者とは、特定のリスクについて責任を持つ人々及びそのリスク管理における最終的な責任者となる人物である。ほとんどすべての場合、これは第一段階のアクティビティ及びリスク所有者と同じであるが、説明責任の所在がこの最初の人物以外にある場合には、本欄がその連鎖を記述するのに適している。

最後の欄にはリスクの深刻度を記述する。これは選択したリスクの発現可能性の値及び影響の値を単純に掛け合わせた積である。リスクの関係が曖昧かもしれない場合には、リスクの深刻度がどの程度変動する可能性があるのかを記述すべきである。

T9	特定のリスクについての評価の実施	
リスク識別子		
リスク名称		
リスクの説明		
リスク発現例		
リスク識別日		
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	運用及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者		
上位所有者		
ステークホルダー		
リスクの関係		
リスクの発現可能性		
リスクの潜在的影響		
リスクの深刻度		

5.11.8 必要な情報が利用不可能な場合

多くの組織において、リスクの発現可能性あるいは潜在的影響を明確に示すための情報の入手は難しい。従って、監査人は、関連するさまざまなソースから、回答を導き出さなければならない。発現可能性に関しては、最初に考慮の対象とすべきなのは、組織の過去の経験であろう。過去に頻繁に実際に起こったことのあるリスクは、そのリスクを取り巻く状況及び直接影響を与える状況が変わらない限り、発現可能性が高いと考えなければならない。例えば、最近（昨年の業務において）、組織内でハードウェアの故障が少なくとも月に1度起きたとすると、そのシステムが交換されていない限り、あるいはその問題の原因が適切に調査され、それが対処されていない限り、その組織における当該リスクの発現可能性を決定する際に非常に重要な要因となる。発現する間隔が様々であるリスクに関しては、組織は直近に導入されたリスク回避の手段が試行されてからの平均発現間隔を決定すべきである。この概算算

定値は、過去の平均的な発現可能性からリスク回避のための仕組みによる相殺効果をマイナスした値となる。

潜在的影響も多くの場合、同様の方法で導き出すことができる。過去に発現したリスクに関して、組織は、その時記録された影響を単純に割り出すことができる。他の状況の変動が一定であると仮定すれば、組織はそのリスクが今後発現した場合の潜在的影響を同程度であると推定することができる。リスク対処のための仕組みが、最後にそのリスクが発現した後に導入された場合には、そのことを考慮に入れるべきである。過去に何度も発現したリスクに関しては、組織は直近に導入されたリスク対処のための仕組みが試行されてからの平均発現影響を決定すべきである。この概算算定値は、過去の平均的な影響の大きさからリスク対処のための仕組みによる相殺効果をマイナスした値となる。

多くの場合（とりわけ最も壊滅的な深刻度のリスクの場合）、組織はそのリスクの発現を経験したことがほとんどないか、或いはまったくないかである。監査人が自分の組織以外の他の組織における経験やコミュニティで行われたテストベッド作業の調査を必要とするのはこのような場合である。多くのリスクに関して、相当量の研究が行われている。例えば、メディアの故障はよく研究されているテーマであり、組織はこのリスクの発現可能性を評価するための根拠にできる多数の文献を見つけ出せるだろう。また、文献が比較的少ない場合もある。監査人は実行したリスク評価が確かであるということを可能な限り根拠に基づいて保証すべきである。これを行うためには、様々なコミュニティとの協議が必要になる可能性がある。例えば、危険な竜巻が多発する地域にあるリポジトリの監査人は、その回答の根拠として地元の気象に関する情報を参照すべきである。他の類似組織における経験は、監査を受ける特定の組織と関連がある評価を探し出すのに役立つ。このツールキットが発展し、またその使用が増えるに従って、類似組織における経験が匿名で利用できるようになる。それは、多くの組織において、直面した問題や降りかかった惨事に関する情報は外部に知らせないようにするのが一般的であるからである。このことは、特定のリスクが及ぼした影響に対する組織としての責任については特に当てはまる。

5.11.9 他のリポジトリから提供されるもの

特定のリスクとその重大さはリポジトリによって様々であろう。手がかりとして、一般的なリスクのリストを添付する（別表2）。これは公開されている文書のレビューや試験的な監査を行い、識別されたものである。この自己監査ツールキットの今後の版において、このリスト及び関連する記入フォームをさらに向上させ続けることが企図されている。このツールキットのユーザーからのリスクに関するフィードバックは、リストへの追加を勧めるものであれ、ここにリスト化されているリスクについての説明を洗練させるのに役立つものであれ、大歓迎である。現在のところ、ユーザーからのフィードバックを促進する目的でリストは順不同にしてある。現在のところ、公表されている文書で記載のあったリスクに対してはリスク特性全般が提示されているものの、リストは、リスクの名称、依存状態、機能クラス及びカテゴリーのみが完成している。

前セクションで識別した他のリスクはその下に添付されている。リスクごとにリスク例を記述したテーブルとなっている。代表的な項目はリスク発現例、可能性及び潜在的影響などである。これらのリスク特性はリポジトリの回答に組み込まれる可能性がある。あるいは組織が受けている自己監査に対して主観的な回答を導き出すのに使用される場合がある。

別表3を参照してリスクの記述例をご覧いただきたい。

5.11.10 意見募集

DCC/DPE監査・認証ワーキンググループは監査人の方々からのコメント、懸念事項、あるいは意見をお待ちしております。feedback@repositoryaudit.euまでお寄せください。

5.11.11 チェックリスト

ステージ6に進む前に、監査人は次のことを確認すべきである。

- 既にリスト化された各リスクが可能性及び潜在的影響に従って特徴付けされていること。
- 各リスクに対して、それが発現する可能性のある状況の詳細な例が付与されていること。
- 各リスクに対して、他のリスクとの関係が、リスクの発現可能性、影響及び管理のしやすさに対する潜在的な影響とともに記録されていること。
- 最終的所有者が特定されていること。
- 各リスクに対して、定量化した深刻度のスコアがその尤度及び潜在的影響のスコアに基づいて算定されており、またリスクの関係に基づいて深刻度が変動する可能性についても記録されていること。

5.12 ステージ 6：リスクの管理

これは自己監査6ステージ中最後のステージである。

5.12.1 ステージ6の目的

この作業に関わる基本的な規範は、リスクは適切に管理しなければならないということである。リスクについての評価が完了すれば、どのようにしてそのリスクにアプローチするのかを決定するビジネス上の決断をしなければならない。この決断をする際には、リスクの潜在的影響、その発現頻度、その所有者及びそのステークホルダーを考慮すべきである。リスクの軽減方法及びタスクを、あらかじめ定められた目的の達成期限とともに決定すべきである。

リスクは、その防止及び検知の制御、その回避方法ならびにその受入れの組み合わせによって、あるいはそれを他の組織へ移転することによって管理できる。識別したリスクによる悪影響に組織が対処できるいくつかの方法がある。オーストラリア及びニュージーランド規格AS/NZS 4360：2004リスクマネジメントは次の選択肢をリスト化している。

- リスクを発現させるアクティビティを開始あるいは継続しない（これが可能な場合）という決断をすることによってリスクを避ける。個人あるいは組織がいたずらに危険を避けようとすると、リスクを適切に回避できなくなる。不適切なリスク回避によって、他のリスクの重大さが増す可能性がある。あるいは利益を得る機会の損失を招くかもしれない。
- リスクの尤度を変え、マイナスの結果が起こる尤度を減らす。
- 因果関係を変え、損失の程度を減らす。これには、在庫の削減あるいは防止装置の設置のような事前措置及び継続計画のような事後措置が含まれる。
- リスクを分担させる。リスクの一部に対して責任や負担を、できれば双方の合意によって、他のグループに負わせるあるいは分担させる。この仕組みには、責任及び負担を分散させるための契約、保険手配及び提携や共同事業のような組織的な体制などを利用する。概して、他の組織とリスクの一部を分担するには、保険料のような財政的なコストあるいは利益が付随する。リスクの全部あるいは一部を分担することにより、リスクを移転する組織は、リスクを移転された組織がそのリスクを効果的に管理できない可能性があるという新たなリスクを持つことになる。
- リスクを維持する。リスクを変化させた後、あるいはリスクを分担した後も維持すべきリスクが存続する。リスクは、識別できなかった、適切に分担できなかった、あるいは何か別の理由で対処できなかったなどの場合にも残ることがある。

この監査ツールキットは、特定のリスク管理方法を定めたり、あるいは義務づけることはしない。最終的には、監査対象の組織がどのような手法を採用したのかにかかわらず、このプロセスの主要な成果であるリスクの登録によって、選択された方法をサポートし、促進することができるだろう。組織は、組織が業務を行う状況において最適の成果が挙げられ、また利用可能な資源を反映した手法（2つ以上の場合もある）の選択を促される。この自己監査プロセスを完了した組織は、リスクの体系的なテーブルを手に入れることになるだろう。このテーブルは、特定の組織の具体的な状況を考慮して、価値のある追加情報に対応するために拡大される可能性がある。

リスク管理の意思決定プロセスに影響を及ぼすかもしれない他の要因は次のとおりである。

- 組織のリスクを積極的に受入れようとする取組み。リスク許容度あるいはリスク選好とも呼ばれる。
- 適切な管理の考案しやすさ
- 利用できる資源
- 現在のビジネスあるいは技術の優先度
- 組織の方針及び経営方針

監査ステージ6の目的は、識別し評価を実行したリスクを効果的かつ効率的に管理するためのツールを監査人に提供することである。リスク管理についてのさらなる提案が次のセクション「改善方法：リスク管理についての勧告」で示す。

5.12.2 ステージ6の関連タスク

ステージ6では、監査人は次のことを行うことが求められる。

- リスク管理方法の選択
- リスク軽減措置の記述
- リスク軽減アクティビティに対する責任の割り当て
- リスク軽減アクティビティの目標期日及び／又は成果目標の設定

リスク管理ツール及び方法は、自己監査プロセスのステージ6に含まれるものに限定されない。監査人は自分たちがリスク管理作業を行った成果をリポジトリの上層部経営者と共有し、他のリスク管理のノウハウを活用するよう求められる。

さらなる情報及び手引きが次より入手可能である。

- AS/NZS 4360：2004リスクマネジメント
- 英国政府商務局．成功のためのツールキット　リスク管理
- 英国政府財務局．オレンジブック　リスク管理－方針と概念（2004）

5.12.3 ステージ6で期待される成果

ステージ6の完了から得られる主な成果は、リスクの登録である。登録されたリスクの記述にはリスク管理の特徴が含まれている。リスクの登録によってリスク管理作業を停止すべきではない。見直しやモニタリングの継続は、確実にリスク管理計画の妥当性を維持するために不可欠である。リスクの尤度と因果関係に影響する要因は変化する可能性があり、リスク軽減措置の適切性及びコストに影響する要因もまた変化する可能性がある。また、リポジトリのビジネス状況、規制状況あるいは社会的状況も時間の経過と共に変化する。従って、中には消滅したり、その重要度が下がったりするリスクがあるかもしれない。その一方で、新たな他のリスクが出現する可能性もある。そのため、リスク管理サイクルを定期的に繰り返し、目標期日が到来した時には成果目標を見直すことが必要である。

リスク軽減計画が実際に進捗すれば、効率的な業務基準が得られることになる。またその進捗結果は組織の業績管理・測定・報告システムに組み込まれるべきである。モニタリング及び見直しもまた、起こった事象、対処計画及びその成果を見直すことによってリスク管理プロセスから学んだことと関係する。

リスクコミュニケーションは効果的なリスク管理の一部であり、確実に組織全体でリスクに対して関与するためのものである。リスクコミュニケーションについてのさらなる情報は、リスク管理標準規格ならびにERPANETリスクコミュニケーションツール[26]にある。

また、リスク分析の成果によって、リポジトリの保存についての方針及び方法がもたらされる可能性があり、また内部的な公的使命についての新たな定義がもたらされるかもしれない。

5.12.4 監査プロセス全体におけるステージ6の位置づけ

リスク管理は、この自己監査の最後のステージであり、最終的な成果となる。これまでの5ステージでは、リスクの対処及び管理プロセスに最終的に役立つ包括的な情報群を作成してきた。

監査の成果物は、監査ツールの対話型ウェブバージョン（利用可能になった時）で印刷される監査報告である。監査報告はリスク管理作業が完了した後に印刷される。

リポジトリのリスク登録はステージ6で完了するが、定期的な見直し及び更新を継続的に行うことが期待される。リスクについての軽減アクティビティが施され、リポジトリの業務状況は時間の経過とともに変化するからである。

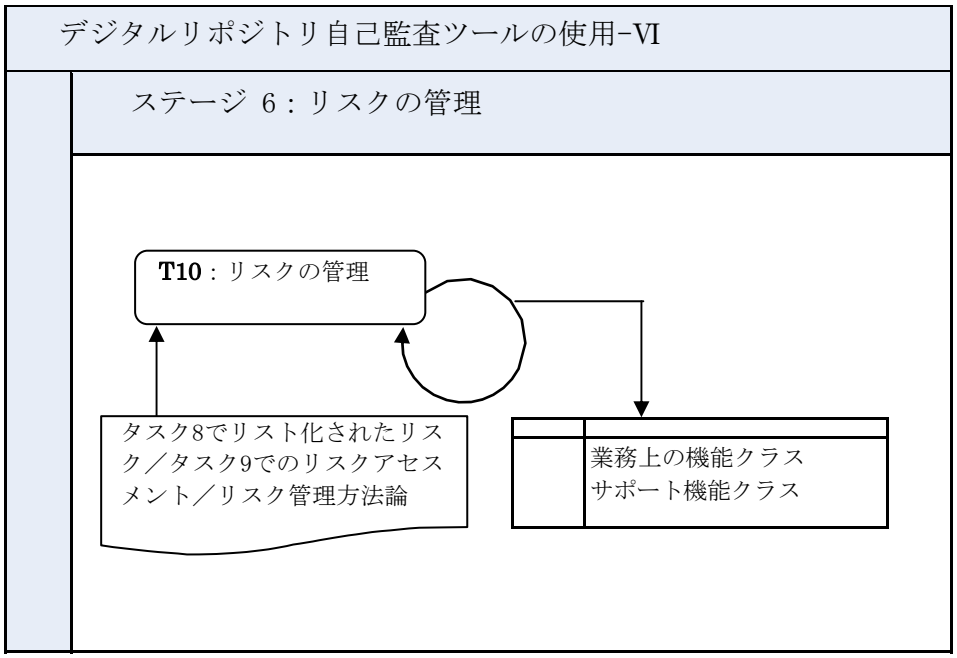
5.12.5 ステージ6を完了させるために必要な資源

完了までの予想時間：4時間

ステージ4で識別されたリスクの数によってリスク軽減措置を検討しなければならない時間回数が決まるが、リスクのタイプ、深刻度及び対処の難易度によって、ステージ6で費やさなければならない時間は大きく左右される。最終的に、ステージ6を完了するのに必要な時間は、リポジトリとその上層部経営者がどの程度深刻にリスク管理作業を実行する用意があるのかによって決まる。識別されたリスクに対処する方法を考慮し、計画し、決定するのに費やされた時間はリポジトリに対しプラスにのみ働き、そのビジネスアクティビティを長期的に保護することになる。

[26] ERPANET Risk Communication Tool （2003），
http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf

5.12.6 ステージ6を示す略図



5.12.7 ステージ6を完了させるための指示

5.12.7.1 T10：リスク管理

次テーブルで、監査人は望ましいリスク管理措置、リスク管理アクティビティに対して責任を持つスタッフ名及び各リスク管理措置の目標を記録すべきである。
本タスクを完了するために推奨されるステップは次のとおりである。

- ◆ リスクに対する適切な対応を識別し、リスク管理のタイプを選択する。
- ◆ 各リスクに対する一連の現実的な対応を識別し、リスク管理アクティビティという観点からそれを記述する。
- ◆ リスク管理アクティビティの所有者を識別し、その所有者が成し遂げるべき目標を定める。
- ◆ リスク管理アクティビティ及び対応自体が他の分野のアクティビティに対して新たな脅威をもたらしていないかを調べ、それらの関係を識別する。必要であれば、ステージ4及び5に戻り、適宜記録されたリスクの関係を修正する。
- ◆ リスクを優先順位ごとに分類する。
- ◆ リスク登録を更新し、管理者が適切な情報を確実に受け取れるようにする。
- ◆ 計画及びリスク所有者の割り当てについての承認を得る。
- ◆ 計画に対する資源の割り当て及び／またはリスク管理アクティビティに対する責任の配分についての経営者の承認を得る。

T10：	リスクの管理

リスク識別子		
リスク名称		
リスクの説明		
リスク発現例		
リスク識別日		
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者		
上位所有者		
ステークホルダー		
リスクの関係		
リスクの発現可能性		
リスクの深刻度		
リスク管理アクティビティ		
リスク管理アクティビティの所有者		
リスク管理アクティビティの目標		

5.12.8 必要な情報が利用不可能な場合

リスク管理の文化及び原則が組織にまだ存在していない場合、監査人には組織のリスクへの対応方法を定義する機会があるだろう。監査人は、組織及び情報セキュリティリスク管理に関する既存の規範やハンドブックを考慮し、ステージ4及び5で作成したリスク登録をもとにして、リポジトリのためのリスク管理方法を考案することが推奨される。

5.12.9 他のリポジトリから提供されるもの

次の「改善の仕方：リスク管理勧告」セクションを参照のこと。

5.12.10 意見募集

DCC/DPE監査・認証ワーキンググループは監査人の方々からのコメント、懸念事項、あるいは意見をお待ちしております。feedback@repositoryaudit.euまでお寄せください。

5.13 監査結果の解釈方法

リスク評価をベースとした自己監査によって、8つの機能クラスの各々について各種の要素からなるリスクスコアが付与されている。この数値は機能クラスのリスクスコアを比較するのに役立ち、またこれによって脅威に対して最も脆弱なリポジトリの作業領域を識別することができる。

自己監査ツールキットのオンラインバージョン（http：//www.repositoryaudit.eu）は、監査スコアと、自己監査を行った他の類似リポジトリによって得られた平均リスクスコアを比較するための手段を提供することになる。リスクスコアの比較は各機能クラス内で提供される。

オンラインバージョンにおける自己監査の終了時になされる監査報告はリスク管理ツールとして、またリポジトリを管理する上でのリスク情報として利用することができる。監査報告の仮の構成はこの文書の別表4にある。

5.13.1 改善の仕方：リスク管理勧告

リスク管理は、脆弱性及び脅威の識別あるいは評価を完了したからといって、あるいはリスクに対する対処計画を作成したからといって終了すべきではない継続的な作業である。この監査によるリスク登録は、リスク管理のモニタリング、リスクの軽減・回避・対処措置の改正及び選択した措置の成果の評価を行うために利用することのできる効率的なツールである。リポジトリのリスク登録は、例に含まれる情報のみの記録に限らない。リスクを分析する上で、監査人がリスク登録にさらに詳細な情報を加えることもできる。拡大バージョンのリスク登録に含まれる属性の構成例は次のとおりである。

拡大バージョンのリスク属性タグの例
リスク名称
リスクタイプ及び／またはグループ
リスクの所有者
識別日
最終更新日
リスクの説明
リスク発現（リスクが発現しうる状況）
発現した場合のコスト（経費など）
リスクの発現可能性
リスクの影響
近似例
回避方法
対処方法
目標日
実行所有者／管理者
完了日
計画及び関連リスクの相互参照
リスク状況及びリスク対処状況
最終評価日

リスクの優先度が変わる重大な変更の報告、制御の有効性の保証、及びリスクがまだ存在しているか、

新たなリスクが生まれていないか、リスクの尤度及び影響が変化していないかについての見直しを行うためのプロセスを導入すべきである。

リスク管理のモニタリングには少なくとも次のステップが含まれるべきである。

- リスク管理方法の有効性についての保証を得る。そのリスク管理方法によって目的とする成果がもたらされているか？
- リスクが、定められたリスク許容レベル内におさまっているかを確認する。
- リスクに対する再評価を実行し、しかるべくリスク登録を修正する。
- リスク管理アクティビティを再評価し、必要に応じて変更を加える。
- 管理者のさらなる注意が必要な変更及び改善領域を識別する。
- リスク管理の有効性についての報告書を作成し、管理者に提出する。

異なるリスクに対してどのリスク管理方法を採用すべきかについての決断を下すことは、リスク管理において重要である。分野によっては、適切な行動を適宜とることによって、リスクを回避することやリスクの発現を防ぐことが容易である。また分野によっては、リスクをある程度のレベルまで受け入れたり許容したりしなければならず、効果的なリスク影響軽減アクティビティが計画されなければならない。また、最も脆弱なアクティビティあるいは資産は、より効率的なリスク回避手段を持つ他の組織に、サービス契約の締結などの方法で移転することもある。

リスク評価を実行した、あるいはこの自己監査を行ったデジタルリポジトリでは、作業領域の中には特定のリスク管理方法が適しているものがあるということを実証している。以下に例を挙げる。

5.13.1.1 リスク回避及び対処方法

リスク例：知的所有権の侵害に対する公的使命

回避方法：

- 保存対象資料を評価し、知的所有権によって制限されているかもしれない資料を識別する。
- 知的所有権によって制限されたコンテンツに関するアクティビティが適法かどうかを裁定するために法律専門家の意見を求める。

リスクが発現した場合：

- 知的所有権に関する異議申し立てがあった場合に取るべき方針及び手法を確立する。

リスク例：スタッフのスキルの陳腐化

回避方法：

- スタッフのスキルの訓練方法及びスタッフが限られた頻度でしか使うことのないスキルをテスト環境で使えるようにするための手段を確立する。
- スキルレベル及び訓練の必要性を定期的に見極めるために、スタッフの業務遂行能力の見直しを行う。

リスクが発現した場合：

- スキルの陳腐化を食い止めるために、訓練設備を提供する。

リスク例：組織の目的達成に不十分な財政

回避方法：
- サービスの有料化で自立性を高める。
- 予算レベルの保証を求める。

リスクが発現した場合：
- 組織の目的が達成できるように追加の資金を募る。
- 資金の流れの柔軟性が不十分であれば目的を変更する。
- 可能であれば不足額を補填するために残余資金を取っておく。

リスク例：情報の機密性の喪失

回避方法：
- リポジトリに対する機密性要件のすべてを十分考慮して方針及び手法を確実に考案する。
- ソフトウェアやハードウェアシステム及び保存方法が方針の要件を確実に満たすことができるようにする。

リスクが発現した場合：
- 機密資料を利用できなくするための方針を実行し、評判の低下を緩和するための対処方法を行使する。

5.13.1.2 リスク移転方法

リスク例：リポジトリ業務の強制的な停止

移転方法：
- 継承のための手筈を整える。
- 危機管理計画あるいはエスクロー契約（条件付譲渡契約）を確立する。
- 撤退戦略を確立する。

リスク例：ハードウェアのストレージ領域への物理的侵入

移転方法：
- 確実な物理的セキュリティサービスを提供するために、サービスレベル契約を第3者のセキュリティ会社と結ぶ。

リスク例：ハードウェアの故障あるいは非互換性

移転方法：
- ハードウェアシステムの故障に対して保険をかける。

5.13.1.3 リスク許容方法

リスク例：保存方法による情報の喪失

許容方法：

◆ 保存アクティビティによる許容可能な喪失条件を定義する方針を策定する。

リスク例：バックアップの喪失あるいは不適合

許容方法：

◆ バックアップストレージを余分に実装する。

リスク例：情報及び／あるいはサービス提供の休止

許容方法：

◆ 最低限のサービスレベルの提供を約束するための方針を明確にする。これには故障時間あるいは情報が利用できない時間の許容範囲を盛り込む。

特定のリスクについてのリスク管理方法を選択する時、あるいはリスク管理措置の効率性を評価する時には、多数の異なる方法を考慮することが可能である。

5.13.1.4 業務レベル

業務レベルにおけるリスク管理は、第一にサービスの継続性に関わっている。リポジトリには、いくつかのサービスに関係するリスク管理を行っているパートナーやサービスプロバイダがいるかもしれない。しかし、リスクを完全に移転することはできないということを、リポジトリは認識しなければならない。リポジトリは、リポジトリ自体のリスクを確実に管理しなければならない。リスク及びその管理についての共通理解や合意があるべきである。

5.13.1.5 プロジェクトレベル

プロジェクトレベルにおけるリスク管理は、望ましくない結果を最小限に抑えておくことが中心である。このレベルにおけるリスク管理についての決定は、事業上極めて重要である。プロバイダ及び／またはパートナーが関与する場合には、リスク及びリスクの管理方法についての共通見解を持たなければならない。

5.13.1.6 戦略的なレベル

戦略的なレベルにおけるリスク管理は、戦略的な方向性を定め、コストとリスクに対する潜在的可能性のバランスを取ることに関わっている。高レベルの戦略的リスクの査定は、計画の変更を考慮する際事業上重要な要件である。例えば、組織は新しい科学技術を伴う事業サービスを提供する革新的な方法を考えるかもしれない。比較的実績のない科学技術及び／または民間部門のパートナーとの提携に関連するリスクについて、業績が向上する可能性を開発するための選択肢に対する評価が実行されるだろう。

6 第Ⅲ部、結論及び次のステップ

6.1結論

我々は常にリスクを識別し、軽減し、それに対処する事業に携わっている。従って、言うまでもなく、適切にリスクに対応する能力は事業を成功させるためには不可欠である。リスク管理の原則は、すべての事業上の決定に内在しており、目的を反映し、それに影響を及ぼしている。そして、事業活動及び資産において事実上実現されている。リスク管理の原則は、デジタル情報を取り扱う場合には、さらに深いレベルの重要性を帯びている。それはデジタルの領域を特徴付けている固有の不確実性である。リポジトリは、活動を行う上で多数の技術的、組織的及び方法論的な課題に直面する。それらの課題が対処可能あるいは回避可能であると考えれば、リスクはより都合良く適切に対処することができ、その後克服することができる。

DRAMBORAプロセスの完了によって、いくつかの有益な成果が生み出され、参加組織にとって遡及的な反映及び事前計画の両方が促進されることになる。第一に、組織は基本的な目的ならびに関連アクティビティ及び資産についての自己認識を文書化することができる。その業務上の状況を明確にすることにより、組織は評価パラメータを決定し、資源が確実に成功するために最適に投入され、配置されていることを実証する体制を整えている。第二に、組織は直面するリスクについての理解をその尤度及び潜在的影響という観点から文書化することができる。組織の目標及び取組みを計画することにより、その後の組織の開発及び資源の配分が促進されるだろう。そして、直面しているリスクの最新の深刻度に関する定量化できる知見を得ることができる。最後に、組織はリスク管理について選択した手段を明らかにし、リスクの回避・対処・移転・許容のための適切な方法及びそれを実行するための仕組みを決定するだろう。定期的に行うべきこのプロセスによって、定量化できる目標を設定し、それを達成する機会が得られ、組織のアクティビティのあらゆる側面における進行中の開発を促進するだろう。

DRAMBORAによる自己評価は非常に有効なプロセスであるのと同時に、このサービスが広く利用されるようになると、外部監査、認可、証明に対する準備として価値ある役割を果たすと期待される。6ステージの自己監査は、組織が全面監査を受ける際に着手する予定である準備作業と密接に関連がある。そして、文書化された情報はすべて非常に有効である。

6.2 期待される次のステップ

これは繰り返し提供するDCC/DPEリスク評価に基づくデジタルリポジトリ監査法ツールキットの第1回目である。2007年中に、我々は翌年のリポジトリ監査を通じてテストを行いながら、このツールキットを向上させるつもりである。正式なテスト期間は各リリースの後である。我々は組織に改良のためのフィードバック及び提案を提供してくれる評価パートナーになってもらいたいと考えている。
フィードバックの仕組みは、今後リリース予定であるオンラインバージョンのツールに組み込まれる予定である。また、Eメールアドレス（feedback@repositoryaudit.eu）がこのツールについてのすべてのフィードバック、批評及び考えを送ってもらうために用意されている。

初期のテスト段階では、このツールキットを評価するために、DCCからの参加者がJISCデジタルリポジトリプログラムと連携することを目指している。DPEは、第1版を評価するために、ヨーロッパのパートナーと協働する。また、このツールキットを公式監査シリーズの基礎として、現在ある国際的に定義された監査基準とともに使用する。DCC及びDPEは、2007年4月1日から2007年12月1日の間にさらに17～20件の監査が完了すると予想しており、2008年2月28日にこのツールキットの次をリリースす

るという目標を立てている。

7 付録

7.1 付録1：謝辞

著者一同は、デジタル・キュレーション・センター（DDC）所長Chris Rusbridgeに対し、この試みへの励まし、貢献、そして継続的支援への謝意を表明したい。DDC副所長でありCASPAR主任調査員であるDavid Giaretta、及び元研究図書館グループ所属、現OCLC所属のRobin Dale のおかげで、DCCサービスチームがTRACの作業に参加できるようになったことに感謝している。

このプロセス全体を通して、研究図書館センター（シカゴ）所長Bernard F Reillyが与えてくれた戦略ガイダンスに深く感謝する。

通常はCharles Sturt大学の図書館情報管理学教授であり、2007年前半にグラスゴー大学客員研究員及び客員教授の任にあったRoss Harveyは、貴重な批評を行い、有益な問いを投げかけ、素晴らしい指導を行った。

このツールキットの開発において、Stefan Strathmann及びその他のnestorチーム、特にバイエルン州立図書館のDr. Astrid Schogerからの情報、支援、フィードバックに厚く感謝している。

特に、グラスゴー大学HATII内DCC及びLOCKSS技術サポート担当のAdam Rusbridgeには、試験監査に参加してくれたことに感謝する。また、Lorna Cullenには、公開前に専門家の目でこの文書を確認してくれたことに謝意を伝えたい。

何よりも重要なのは、時間と労力を注いでくれた文書館、図書館、eサイエンス、データの保存に関わるコミュニティの多くのメンバーの好意により、このツールキットの初版を出すことができたということである。異なる環境下でリポジトリがどのように稼働するかということや、うまく作動させるためのプロセスについて見識を与えてくれた以下の団体及び個人に感謝申し上げたい。

英国大気データセンター (BADC)
Tim Folkes, Atlas Data Store Project
Wendy Garland, Environmental Data Scientist
Rob Harper, Storage Coordinator
Andrew Harwood, BADC Infrastructure Manager
Charles Kilburn, Environmental Data Scientist
Bryan Lawrence, Head of the BADC
Sam Pepler, Curation Manager

ビーズリー・アーカイブ
Professor Donna Kurtz, Director
Thomas Mannack, Pottery Database Administrator
Greg Parker, Technical Director
Claudia Wagner, Gem Database Administrator

ロンドン大学コンピュータセンター内国立データセットデジタルアーカイブ
Kevin Ashley, Head of Digital Archives
Joanne Anthony, Archivist

Kate Bradford, Archivist
Mina Creathorn, Content Specialist
Sally Hughes, Team Leader, Content Specialists
Jim Jamieson, Team Leader, Archivists
Jenny Leigh, Archivist
Jo Marsh, Content Specialist
Ed Pinsent, Archivist

ニュージーランド国立図書館
Mat Black, Integration Architect
Steve Knight, NDHA Programme Architect
Pauline LaRooy, Collections Development
Ingrid Mason, (Former) Resource Analyst
Ann O'Rorke, Business Change Manager
Leigh Rosin, Digital Archivist
Lockie Stewart, Enterprise Architect
Ann Thompson, Collections Development

フロリダ・デジタル・アーカイブ
James F Corey, FCLA Director
Priscilla Caplan, Assistant Director, Digital Library Services
Jennifer Childree, IT Entry
Carol Chou, IT Senior
Randy Fischer, IT Expert
Franco Lazzarino, IT Expert
Manny Rodriquez, IT Expert
Chris Cuevas, IT Expert
Daryl Marsee, Coordinator, Computer Applications
Martin Johnson, Coordinator, Computer Applications

7.2 付録2：自己監査ツールキットのテンプレート

T1：リポジトリ又はリポジトリが組み込まれている組織の公的使命

T2：リポジトリの目的・目標をリスト化

T3：リポジトリの戦略的計画書をリスト化

T4：リポジトリが遵守すべき法律、規定、契約の枠組みまたは合意文書をリスト化

T5：リポジトリが遵守することに合意した自発的規約をリスト化

T6：リポジトリが遵守すべきその他の文書と原則をリスト化

T7：リポジトリのアクティビティ、資産及びそれらの所有者を識別

T8：リポジトリのアクティビティと資産に関連するリスクを識別

T9：識別したリスクについての評価の実施

T10：リスク管理

リポジトリ		監査人		日付	
ステージ	**ステージ1：組織の背景の識別**	フォーム	**T1**	ページ	

T1: リポジトリまたはリポジトリが組み込まれている組織の公的使命

リポジトリ		監査人		日付	
ステージ	**ステージ1：組織の背景の識別**	フォーム	**T2**	ページ	

T2: リポジトリの目的・目標をリスト化
作業機能: 収集と受入
作業機能: 保存と蓄積
作業機能: メタデータ管理
作業機能: アクセスと提供
サポート機能: 組織と管理
サポート機能: スタッフ配置
サポート機能: 財務管理
サポート機能: 技術的インフラとセキュリティ

リポジトリ		監査人		日付	
ステージ	**ステージ1：組織の背景の識別**	フォーム	**T2**	ページ	

目的・目標リスト化のための独自のカテゴリーまたはクラスを定義

T2: リポジトリの目的・目標をリスト化

リポジトリ		監査人		日付	
ステージ	**ステージ 2: 文書の方針と既定の枠組み**	フォーム	**T3**	ページ	

T3: リポジトリの戦略的計画書をリスト化	
作業機能: 収集と受入	参照
作業機能: 保存と蓄積	参照
作業機能: メタデータ管理	参照
作業機能: アクセスと提供	参照
サポート機能: 組織と管理	参照
サポート機能: スタッフ配置	参照
サポート機能: 財務管理	参照
サポート機能: 技術的インフラとセキュリティ	参照

リポジトリ		監査人		日付	
ステージ	ステージ 2: 文書の方針と既定の枠組み	フォーム	T3	ページ	

戦略計画文書リスト化のための独自のカテゴリーまたはクラスを定義

T3: リポジトリの戦略的計画書をリスト化	
	参照
	参照
	参照
	参照

リポジトリ		監査人		日付	
ステージ	**ステージ 2: 文書の方針と既定の枠組み**	フォーム	**T4**	ページ	

T4: リポジトリが遵守すべき法律、規定、契約の枠組みまたは合意文書をリスト化
作業機能：収集と受入
作業機能：保存と蓄積
作業機能：メタデータ管理
作業機能：アクセスと提供
サポート機能：組織と管理
サポート機能：スタッフ配置
サポート機能：財務管理
サポート機能：技術的インフラとセキュリティ

リポジトリ		監査人		日付	
ステージ	**ステージ 2: 文書の方針と既定の枠組み**	フォーム	**T4**	ページ	

リポジトリが遵守すべき法律、規定、契約の枠組みまたは合意文書をリスト化するための独自のカテゴリーまたはクラスを定義

T4: リポジトリが遵守すべき法律、規定、契約の枠組みまたは合意文書をリスト化

リポジトリ		監査人		日付	
ステージ	**ステージ 2: 文書の方針と既定の枠組み**	フォーム	**T5**	ページ	

T5: リポジトリが遵守することに合意した自発的規約をリスト化	
作業機能: 収集と受入	参照
作業機能: 保存と蓄積	参照
作業機能: メタデータ管理	参照
作業機能: アクセスと提供	参照
サポート機能: 組織と管理	参照
サポート機能: スタッフ配置	参照
サポート機能: 財務管理	参照
サポート機能: 技術的インフラとセキュリティ	参照
独自のカテゴリーを定義	

リポジトリ		監査人		日付	
ステージ	**ステージ 2: 文書の方針と既定の枠組み**	フォーム	**T5**	ページ	

リポジトリが遵守することに合意した自発的規約をリスト化するための独自のカテゴリーまたはクラスを定義

T5: リポジトリが遵守することに合意した自発的規約をリスト化	
	参照
	参照
	参照
	参照

リポジトリ		監査人		日付	
ステージ	**ステージ 2: 文書の方針と既定の枠組み**	フォーム	**T6**	ページ	

T6: リポジトリが遵守すべきその他の文書と原則をリスト化
作業機能: 収集と受入
作業機能: 保存と蓄積
作業機能: メタデータ管理
作業機能: アクセスと提供
サポート機能: 組織と管理
サポート機能: スタッフ配置
サポート機能: 財務管理
サポート機能: 技術的インフラとセキュリティ

リポジトリ		監査人		日付	
ステージ	**ステージ 2: 文書の方針と既定の枠組み**	フォーム	**T6**	ページ	

リポジトリが遵守すべきその他の文書と原則をリスト化するための独自のカテゴリーまたはクラスを定義

T6: リポジトリが遵守すべきその他の文書と原則をリスト化

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
	作業機能: 収集と受入	所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
	作業機能: 保存と蓄積	所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
作業機能: メタデータ管理		所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
作業機能: アクセスと提供		所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
サポート機能: 組織と管理		所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
	サポート機能: スタッフ配置	所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
	サポート機能: 財務管理	所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
サポート機能: 技術的インフラとセキュリティ		所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
作業機能: 収集と受入		所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 3: アクティビティ、資産及びそれらの所有者の識別	フォーム	T7	ページ	

アクティビティ、資産及びそれらの所有者を識別するための独自のカテゴリーまたはクラスを定義

T7: リポジトリのアクティビティ、資産及びそれらの所有者を識別		
		所有者
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		
アクティビティ		
資産		

リポジトリ		監査人		日付	
ステージ	ステージ 4: リスク識別	フォーム	T8	ページ	

T8: リポジトリのアクティビティと資産に関連するリスクを識別		
リスク識別子		
リスク名称		
リスクの説明		
リスク発現例		
リスクを識別した日付		
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者		
上位所有者		
ステークホルダー		
リスクの関係		

リポジトリ		監査人		日付	
ステージ	ステージ **5:** リスク評価の実行	フォーム	**T9**	ページ	

T9: 識別したリスクについての評価の実施		
リスク識別子		
リスク名称		
リスクの説明		
リスク発現例		
リスクを識別した日付		
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者		
上位所有者		
ステークホルダー		
リスクの関係		
リスクの発現可能性		
リスクの潜在的影響		
リスクの深刻度	… x … = …	

リポジトリ		監査人		日付	
ステージ	ステージ 6: リスクの管理	フォーム	T10	ページ	

T10: リスク管理		
リスク識別子		
リスク名称		
リスクの説明		
リスク発現例		
リスクを識別した日付		
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者		
上位所有者		
ステークホルダー		
リスクの関係		
リスクの発現可能性		
リスクの潜在的影響		
リスクの深刻度	… x … = …	
リスク管理戦略		
リスク管理アクティビティ		
リスク管理アクティビティの所有者		
リスク管理アクティビティの目標		

7.3 付録3：デジタルリポジトリのリスク例(記述付き)

次の各テーブルには監査人がそのリスク登録に組み入れたいと希望するかもしれないリスク例が含まれている。しかし、下記のテーブルに含まれる項目は包括的ではない。極めて特定のリポジトリに特有の項目は省略されている。含まれているとすれば余分な情報になりうるからだ。監査人は、リスク登録に含まれなければならない項目を完全にリスト化したものとしては、上述の「5.4. リスク評価の原則」セクションのテーブルを参照すべきである。

7.3.1 組織マネジメント

リスク識別子	R01	
リスク名称	マネジメントの失敗	
リスクの説明	組織のマネジメントについての1つ以上の側面がうまくいっておらず、期待されるまたは求められる事業成果を発揮できない。	
このリスクは該当するか？	・組織は中央管理の制御下にあるか？	
リスク発現例	・リポジトリの経営者が1つ以上の事業活動を完了するための十分な資源を配分できない。 ・リポジトリの経営者が採用した保存戦略によって情報の喪失を招く。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者	
軽減方法	回避方法: ・包括的な経営方針及び手法を考え、定期的な見直しをするための仕組みを確立する。 ・ベンチマークを定め、経営方針及び手法の有効性を見極める。 リスクが発現した場合： ・リスクの影響から回復するための継続または修復の仕組みを確立する。	
リスクの関係	←→R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R02	
リスク名称	信頼または評判の喪失	
リスクの説明	1つ以上のステークホルダー・コミュニティが、リポジトリの事業上の目的を達成する能力について疑問を抱いている。	
このリスクは該当するか？	・組織が事業資産としての評判に依存しているか？ ・組織が事業資産としての信頼性に依存しているか？ ・組織が事業の有効性と組織が受ける評判及び信頼性のレベルとの間の相関関係を認識しているか？	
リスク発現例	・デジタルオブジェクトが回復不能なまでに失われたことにより、リポジトリの力量についてコミュニティが懸念を抱く。 ・予算縮減を公表したことにより、リポジトリが効果的に業務を行うための資源が不足するのではないかという懸念が引き起こされる。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・リポジトリの業務の有効性を公に証明するための入手可能で妥当な証明書をすべて求める。 ・方針及び手法の適合性及びその対象範囲を明らかにするために、組織の透明性を向上させる。 ・組織の目的を達成するために卓越性を目指す。 ・ユーザーコミュニティが期待していると思われることを反映するためのアウトリーチの方法を確立する。	
リスクの関係	←→R01[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R03	
リスク名称	活動の見落とし及び不適当な資源配分	
リスクの説明	マネジメントを誤ったことにより、不可欠な事業活動が完了できない。	
このリスクは該当するか？	・リポジトリは予算整備及び資源配分に対する責任を負っているか？	
リスク発現例	・リポジトリの予算編成にセキュリティ保守システムへの予算配分が含まれていない。 ・1人が1オブジェクトを受け入れるのに平均30分要するにもかかわらず、常勤換算0.5人（0.5FTE）が1日100オブジェクトの受入れに対する全責任を負っている。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・リポジトリの基本的な目的から活動、方針及び手法を導き出す。 ・識別した活動に対応した資源配分をする。 ・資源配分を見直し、調整する仕組みを確立する。 リスクが発現した場合： ・最初に見落とした活動に対する後からの資源配分に役立つよう予備資金を取っておく。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R04	
リスク名称	事業目的の未達成	
リスクの説明	１つ以上の重要な事業の成果が達成されないまたは達成が不十分である。	
このリスクは該当するか？	リポジトリは、そのステークホルダーグループに対して１つ以上の規定の目的を達成するための約束をしているか？	
リスク発現例	・オブジェクトxをその要求から５分以内に提供する必要があるが、平均15分かかっている。 ・リポジトリが受け入れた資料の重要な特性を適切に保存できない。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・対応する重要な目的に厳密に照らし合わせて、活動、方針及び手法を明確にする。 ・事業の優先順位を基に資源を確保し配分する。 ・目的を確実に達成するために、方針及び手法の定期的な見直しを行い、必要であれば調整するための仕組みを確立する。 リスクが発現した場合： ・障害を招いた欠陥を見つけ出し、適宜方針を更新するための適切な内部調査を行う。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R05	
リスク名称	リポジトリの公的使命の喪失	
リスクの説明	リポジトリが存在するための基盤が撤回または大幅に変更され、事業活動と相容れなくなる。	
このリスクは該当するか？	・リポジトリの公的使命の見直し作業が現在行われているか？ ・主要なリポジトリサービス契約が更新または再交渉の対象であるか？	
リスク発現例	・リポジトリの責任範囲が法的改正によって変更される。 ・リポジトリの義務が契約再交渉で変更される。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・リポジトリの業務の有効性を公に証明するための入手可能で妥当な証明書をすべて求める。 ・方針及び手法の適合性並びにその対象範囲を明らかにするために、組織の透明性を向上させる。 ・組織の目的を達成するために卓越性を目指す。 リスクが発現した場合： ・継承のための手続きを整える。 ・危機管理計画またはエスクロー契約を確立する。 ・撤退戦略を確立する。	
リスクの関係	→R08[連鎖的] →R01[連鎖的] →R02[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R06	
リスク名称	コミュニティの要求の大幅な変更	
リスクの説明	コミュニティの期待または要求が大幅に変更され、もはや事業活動と一致しない。	
このリスクは該当するか？	・過去にユーザーの要求が変更されたことがあるか？ ・リポジトリまたは外部の他の類似リポジトリは、コンテンツを利用または寄託するコミュニティ内における変更または変革を経験したことがあるか？	
リスク発現例	・ユーザーコミュニティが、従来主流であった旧来のデータフォーマットをサポートしない新しいソフトウェアシステムを採用する。 ・コミュニティが次第に、従来よく知られており、広く用いられていた学術的マークアップ言語の意味論になじみがなくなってきている。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ユーザーコミュニティの要求、期待及び知識ベースをモニタリングする。 ・各ユーザーコミュニティ独自の見読性の組織的な定義を文書化し、見直す。 リスクが発現した場合： ・新しく現れてくるコミュニティの要求に対応するため、業務目的に対する柔軟なアプローチを維持する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R11[連鎖的] →R67[連鎖的] →R74[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R07	
リスク名称	コミュニティの要求の錯誤または誤解	
リスクの説明	リポジトリが、そのステークホルダー・コミュニティの期待を見極めることができないために、事業活動を適切に適応させることができない。	
このリスクは該当するか？	・リポジトリはコミュニティの知識ベース、要求または期待をモニタリングするための仕組みを確立しているか？ ・提供しているサービスレベルの妥当性についてコミュニティメンバーに意見を聞いているか？	
リスク発現例	・リポジトリのユーザーコミュニティにとって、データが利用可能であるためには、.abcというファイル形式にエンコードされて提供される必要があるということに当該リポジトリが気付かない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ユーザーコミュニティの要求、期待及び知識ベースのモニタリングを促進するための適切な技術的メカニズムを確立する。 リスクが発現した場合： ・確実に見読性の定義が適切であり続けるためにコミュニティとの対話を継続する。 ・要求の解釈を誤った場合に対応できるよう業務目的の柔軟性を保つ。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R11[連鎖的] →R67[連鎖的] →R74[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R08	
リスク名称	リポジトリの業務の強制的な停止	
リスクの説明	リポジトリがその事業活動の強制的な停止に追い込まれる。	
このリスクは該当するか？	・リポジトリの設立に責任を負う仕組みの中で、更新措置を取らなければならない時期までの存続期間が指定され、限定されているか？ ・財政的な損失または制約が生じた期間の埋め合わせをする仕組みがあるか？ ・事業活動の重要な側面は法的な異議申し立ての影響を受けやすいか？ ・リポジトリのユーザーコミュニティの規模が時間の経過とともに小さくなっていくということを示す根拠はあるか？	
リスク発現例	・リポジトリの責任が法律の改正によって消滅する。 ・リポジトリが主要なクライアントや資金供給者との保存契約を更新できない。 ・リポジトリが倒産する、またはもはや財政的に維持できなくなる。 ・リポジトリが競争市場における地位を失う。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・リポジトリの業務の有効性を公に証明するための入手可能で妥当な証明書をすべて求める。 ・方針及び手法の適合性並びにその対象範囲を明らかにするために、組織の透明性を向上させる。 ・組織の目的を達成するために卓越性を目指す。 リスクが発現した場合： ・継承のための手続きを整える。 ・危機管理計画またはエスクロー契約を確立する。 ・撤退戦略を確立する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R09	
リスク名称	コミュニティからのフィードバックの不受理	
リスクの説明	リポジトリが、そのサービスレベルについてのコミュニティからの反応を受け取ることができない。またはフィードバックを受け取る仕組みを提供することができない。	
このリスクは該当するか？	・リポジトリには、コミュニティメンバーからのフィードバックを募るための仕組みがあるか？ ・スタッフの就業時間の一部がコミュニティからのフィードバックを募集し受け取るために配分されているか？ ・フィードバックを受け取る仕組みは、正確に機能することを保障するために定期的に検証されているか？	
リスク発現例	・リポジトリが選択したフォーマットでエンコードされたデータを、そのユーザーコミュニティが主として採用しているソフトウェアで次第に利用できなくなってきているということをリポジトリが認識できない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・Eメール、ウェブ上のフォーム、電話によるヘルプデスク、連絡先（の掲載）など、コミュニティがフィードバックを提供できるように適切な仕組みを維持する。 ・スタッフの就業時間をコミュニティに対する取組みに配分し、フィードバックを積極的に募る。 リスクが発現した場合： ・コミュニケーション不足に陥った理由を特定し、しかるべく方針及び手法を改正する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R10[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R10	
リスク名称	コミュニティからのフィードバックに対する不対応	
リスクの説明	フィードバックを受け取ったにも関わらず、リポジトリの事業活動に何の変更もない。	
このリスクは該当するか？	・スタッフの就業時間の一部が、コミュニティからのフィードバックへの対応または業務目的の変更への反映に配分されているか？ ・コミュニティからのフィードバックにリポジトリが適切かつ適時に対応できるような方針及び手法があるか？ ・コミュニティからのフィードバックに対応するために業務目的を適応させられるか？	
リスク発現例	・リポジトリが選択したフォーマットでエンコードされたデータを、そのユーザーコミュニティが主として採用しているソフトウェアで次第に利用できなくなってきているということにリポジトリが対応することができない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・コミュニティからのフィードバックを認識しそれに対応するための方針を確立する。 リスクが発現した場合： ・コミュニティと足並みが揃っていないということを認識し、受け取ったフィードバックに対して遡及的に対応する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R11[連鎖的] →R67[連鎖的] →R74[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R11	
リスク名称	デジタル情報の必要不可欠な特徴の保存の失敗	
リスクの説明	リポジトリの保存活動が、そのユーザーコミュニティにとって最も重要なデジタル情報の特徴を維持するのに不十分である。	
このリスクは該当するか？	・リポジトリ内のオブジェクトの各クラスに対して、重要な特徴が定義され、文書化されているか？ ・コミュニティメンバーは、重要な特徴を定義するプロセスを通して終始相談を受けているか？ ・保存方針及び手法は定義した特徴を維持するのに十分か？	
リスク発現例	・ユーザーコミュニティがその後の研究において手書きの原本を参照することに関心があるのにもかかわらず、リポジトリはデジタル化した原本をテキスト化したテキストファイル（.txt）を保存する。 ・リポジトリは手書き原稿の画像を保存しようとしたが、選択した解像度ではユーザーコミュニティが要求したレベルで詳細を表示するには不十分である。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・コミュニティの期待及び要求に基づいてデジタルオブジェクトの維持すべき重要な特徴を文書化する。 リスクが発現した場合： ・組織として不十分であった点を認識し、方針及び重要な特性の定義をしかるべく改正する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R04[連鎖的] →R67[連鎖的] →R74[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R12	
リスク名称	事業方針及び手法の不周知	
リスクの説明	リポジトリの事業活動の実施理由と方法の原則が文書化されておらず、また知られていない。または特定の個人にしか知られていない。	
このリスクは該当するか？	・方針及び手法は包括的に文書化されているか？ ・文書は組織全体で広範にアクセスでき読むことができるか？ ・方針及び手法に関する文書の場所を記録し、周知しているか？	
リスク発現例	・組織面に関する方針及び手法を担当者しか知らない。 ・方針をMicrosoft Wordファイルで文書化しているが、ワークステーションのハードディスクの非共有区画で保存している。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・包括的な方針及び手法を考え、文書化する。 ・リポジトリのスタッフに文書を回覧し、複数箇所で複数部数コピーを作成する。 ・文書の保管場所の詳細を回覧する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R04[連鎖的] →R19[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R13	
リスク名称	非効率な事業方針及び手法	
リスクの説明	事業に採用されている原理や実務的アプローチでは最適な効率性を発揮できない。	
このリスクは該当するか？	・類似組織と比べて測定可能な業績面について遜色がないか？ ・リポジトリの現行作業の効率性はそのピーク時に比べてどの程度なのか？	
リスク発現例	・リポジトリでは提供の依頼を受けてから1時間後にオブジェクトが提供可能だが、類似のコンテンツを提供している同等の組織はわずか30分でそれが可能である。 ・改正した方針が改正前よりも明らかに非効率である。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・組織の目標に照らし合わせてその効率性及び妥当性を見極めるために、方針及び手法を定期的に見直す。 ・外部（公認監査機関またはユーザーコミュニティなど）による方針及び手法の妥当性確認を求める。 リスクが発現した場合： ・非効率な方針を特定し、しかるべく改正する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R14	
リスク名称	一貫性を欠くまたは矛盾する事業方針及び手法	
リスクの説明	特定の事業目的に採用されている原理や実務的アプローチが他の事業活動の完了を成功させる際の障害となっている。	
このリスクは該当するか？	・リポジトリの業務全体を考慮して事業方針及び手法を考案しているか？ ・方針や手法の矛盾を解消するための仕組みが整っているか？	
リスク発現例	・リポジトリでは、各オブジェクトの受入れ時にスタッフが品質確認を行うように定めており、その平均所要時間は10分であるが、別の方針書では受入れ作業を10分以内に完了するよう定めている。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・組織の目標に照らし合わせてその一貫性を見極めるために、方針及び手法を定期的に見直す。 ・外部（公認監査機関またはユーザーコミュニティなど）による方針及び手法の妥当性確認を求める。 リスクが発現した場合： ・一貫性を欠く方針を特定し、しかるべく改正する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R15	
リスク名称	知的財産権の侵害に対する法的責任	
リスクの説明	リポジトリはその事業活動の直接的な結果として生じた著作権の侵害、特許権の侵害、または他の知的財産権の侵害に対する法的な責任を持つ。	
このリスクは該当するか？	・リポジトリは特定の知的財産権に関連するコンテンツを扱っているか？ ・リポジトリは知的財産権によって制限されたコンテンツに関連する活動が適法かどうかを裁定する時、法律専門家の意見を求めるか? ・リポジトリ業務の分野または管轄区域において、訴訟になる頻度が高いという根拠があるか？	
リスク発現例	・保存活動の一環として、リポジトリのソフトウェアアプリケーションのリバースエンジニアリングを行う際、そのエンドユーザーライセンス契約の条件に違反する。 ・機関リポジトリが電子雑誌のコンテンツを提供する際、著作権違反を犯す。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	法律専門家	
上位所有者	法律専門家	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・保存された資料を点検し、知的財産権上の制限が付されているかもしれない資料を抽出する。 ・知的財産権上の制限があるコンテンツに関する活動が適法かどうかを裁定するために法律専門家の意見を求める。 リスクが発現した場合： ・知的財産権に関する異議申し立てがあった場合に取るべき方針及び手続きを確立する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R04[連鎖的] →R14[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R16	
リスク名称	契約上の義務違反に対する法的責任	
リスクの説明	リポジトリは、ステークホルダー契約に詳述されているように、義務の不履行または許容範囲を超える行為のいずれに対しても法的な責任を持つ。	
このリスクは該当するか？	・リポジトリは契約関係を持っているか？ ・リポジトリがその活動の適法性を自身が関与する有効な契約に照らして判断する際に、法律専門家の意見を求めるか？ ・リポジトリ業務の分野または管轄区域において、訴訟になる頻度が高いという根拠があるか？	
リスク発現例	・当該の寄託契約には限られたコミュニティのみがアクセスできると記されているにも関わらず、リポジトリでは保存対象コンテンツを公共のインターネット上で無制限に提供している。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	法律専門家	
上位所有者	法律専門家	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・契約を点検し、実行した方針が契約条件に確実に合致するようにする。 ・知的財産権によって制限されたコンテンツに関する活動が適法かどうかを裁定するために法律専門家の意見を求める。 リスクが発現した場合： ・契約に関する異議申し立てがあった場合に取るべき方針及び手法を確立する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R04[連鎖的] →R14[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R17	
リスク名称	法律要件違反に対する法的責任	
リスクの説明	リポジトリは、法令に詳述されているように、義務の不履行または許容範囲を超える行為のいずれに対しても法的な責任を持つ。	
このリスクは該当するか？	・リポジトリは法に基づいて設置されているか？ ・法律または法令のいずれかがリポジトリの活動に関して制限または義務を課しているか？ ・リポジトリは関連制定法に関する活動の適法性を裁定する際に法律専門家の意見を求めるか？ ・リポジトリ業務の分野または管轄区域において、訴訟になる頻度が高いという根拠があるか？	
リスク発現例	自治体で制定された法定納本に関する法律に違反するため、寄託資料をリポジトリで受け入れることができない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	法律専門家	
上位所有者	法律専門家	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・制定法固有の要件及び禁止事項に、方針及び手法が確実に対応できるよう制定法をモニタリングする。 ・制定法に関する活動が適法かどうかを裁定するために法律専門家の意見を求める。 リスクが発現した場合： ・法的な異議申し立てがあった場合に取るべき方針及び手続きを確立する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R04[連鎖的] →R14[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R18	
リスク名称	規制違反に対する責任	
リスクの説明	リポジトリは、産業規制、事業上の規制または国際的な規制に従い、活動を行えないことに対する責任を負う。	
このリスクは該当するか？	・リポジトリの活動に関して制限または義務を課す規制があるか？ ・リポジトリは関連規制に関する活動の適法性を裁定する際に法律専門家の意見を求めるか？ ・リポジトリ業務の分野または管轄区域において、訴訟になる頻度が高いという根拠があるか？	
リスク発現例	スタッフの健康及び安全に関する適切な管轄下の規制にリポジトリが準拠できていない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	法律専門家	
上位所有者	法律専門家	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・規制の枠組みをモニタリングし、方針及び手法によってその要件及び禁止事項に確実に対応できるようにする。 ・規制の枠組みに関する活動が適法かどうかを裁定するために法律専門家の意見を求める。 リスクが発現した場合： ・知的財産権（訳注：原文の直訳）に関する異議申し立てがあった場合に取るべき方針及び手法を確立する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R04[連鎖的] →R14[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R19	
リスク名称	リポジトリの成功の度合いに対する評価能力不足	
リスクの説明	リポジトリの事業目的達成度を効果的に見極めることができない。	
このリスクは該当するか？	・リポジトリにアーカイブされた情報の完全性、真正性、出典及び見読性を検証し記録するための方針及び手法を維持しているか？ ・リポジトリがリポジトリプロセスの実行を評価し記録するための方針及び手法、並びに成果が完全で正しいことを確認するための方針及び手法を維持しているか？ ・リポジトリが、ユーザーコミュニティの全般的な満足度を見極めるために、ユーザーコミュニティと関わっているか？ ・リポジトリ業務の有効性を見極めるための仕組みが定期的に活用されているか？	
リスク発現例	・リポジトリにアーカイブされた資料の完全性及び真正性が維持されていることを証明する方法がない。 ・リポジトリが、提供された情報を正確に受け入れ、対応する完全で正しいアーカイブパッケージに変換したことを証明できない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・リスク管理など内部的な評価手段を確立する。 ・性能を示すため外部の関連証明を求める。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R20	
リスク名称	リポジトリの成功の度合いに関する誤った認識	
リスクの説明	リポジトリの成功についての評価に不備があり、現実と一致しない業績レベルを示している。	
このリスクは該当するか？	・リポジトリの有効性を見極めるための取組みが複数あることによって、矛盾した結果がもたらされていないか？ ・リポジトリ評価の仕組みは、包括的で信頼性が高いか？	
リスク発現例	・ユーザーコミュニティ内の小規模グループのみから募った不完全なエンドユーザー調査の結果を基にして、リポジトリの取組みが成功であると安心している。しかし実際には、現在の仕組みではアーカイブされた情報の見読性、完全性及び真正性を維持するには不十分である。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・リスク管理など内部的な評価手段を確立する。 ・性能を示す外部の関連証明を求める。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R19[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

7.3.2 スタッフ配置

リスク識別子	R21	
リスク名称	主要なスタッフの喪失	
リスクの説明	事業目的の達成に欠かせない役割、責任または能力を持つ個人がリポジトリ業務をやめてしまい、目的の達成が難しくなる。	
このリスクは該当するか？	・リポジトリで重要なスタッフが離職したことがあるか？ ・いずれかのスタッフの地位、専門技術または知識が、その喪失によって組織の事業目的に大きな不利益がもたらされるようなものであるか？	
リスク発現例	・リポジトリシステムのrootパスワードを唯一知っている基幹システム管理者が別の産業で働くために組織を辞める。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	人事	
上位所有者	人事	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・スタッフに有利な待遇を提示する リスクが発現した場合： ・スタッフの喪失による影響を制限するため、組織内の責任の分担及びスキルを持つ人間を複数にすることを促進する。 ・方針及び手法の周知を徹底し、特定の個人のみが知っているということのないようにする。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R12[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R22	
リスク名称	スタッフのスキルの低下	
リスクの説明	スタッフのスキルレベルが時の経過とともに低下する。	
このリスクは該当するか？	・実際にはめったに用いられないスキルを持つことがスタッフに必要とされているか？ ・スキルを更新する機会がスタッフに与えられているか?	
リスク発現例	・リポジトリの技術担当職員は、バックアップからコンテンツを復元するように求められることはほとんどない。そのため、バックアップ復元のための適切なスキルが低下する。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	人事	
上位所有者	人事	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・スタッフのスキルを更新するための手段及びスタッフが限られた頻度でしか用いられないスキルをテスト環境で用いられるようにするための手段を確立する。 ・スキルレベル及び訓練の必要性を定期的に見極めるために、スタッフの業務遂行能力の見直しを行う。 リスクが発現した場合： ・スキルの喪失を食い止めるために、訓練施設を提供する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R23	
リスク名称	スタッフのスキルの陳腐化	
リスクの説明	スタッフのスキルが停滞し、もはや通用しない。	
このリスクは該当するか？	・リポジトリの成長に応じてスタッフが常に新たなスキル及び能力を向上できることを前提としているか？ ・訓練及び専門的な開発の機会がスタッフに与えられているか？ ・スタッフは適切な訓練活動を見つけ、追求することを求められているか？	
リスク発現例	・スタッフが時代遅れの保存手段を用いることしかできず、新しい技法または技術の訓練を受けていない、もしくはそれらの新しい技法または技術を知らない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	人事	
上位所有者	人事	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・スタッフのトレーニング手段及びスタッフが限られた頻度でしか用いられないスキルをテスト環境で用いられるようにするための手段を確立する。 ・スキルレベル及び訓練の必要性を定期的に見極めるために、スタッフの業務遂行能力の見直しを行う。 リスクが発現した場合： ・スキルの陳腐化を食い止めるために、訓練施設を提供する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R24	
リスク名称	スタッフの効率または適性を評価するための能力の不足	
リスクの説明	リポジトリが、スタッフがどの程度事業目的を達成する能力を持っているのかを効果的に見極めることができない。	
このリスクは該当するか？	・スタッフの業務遂行能力の見直しを行う方針及び手法をリポジトリにおいて維持しているか？	
リスク発現例	・リポジトリにスタッフ個人の業務遂行能力レベルの記録または訓練の必要性を効果的に見極める手段がない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営者	
上位所有者	経営者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・リスク管理など内部的な評価手段を確立する。 ・スタッフの技量を証明する外部の関連証明を求める。 ・スタッフの能力開発の見直しを定期的に実施する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R19[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

7.3.3. 財務管理

リスク識別子	R25	
リスク名称	リポジトリの責務を果たすための財源の不足	
リスクの説明	事業に不可欠な諸活動に十分な資金を供給するための財源が不足している。	
このリスクは該当するか？	・ リポジトリにおいて予算管理がなされているか？ ・ リポジトリの目的達成のために、資金投資が必要か？ ・ 現在の事業モデルにおいて、リポジトリは自立的に収益を上げることができるか？	
リスク発現例	・リポジトリの運営が年間において赤字。 ・リポジトリに固有の活動全てを促進するための資金が不足。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	予算管理者	
上位所有者	予算管理者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 有料サービスによって自立性を高める。 ・ 予算水準の安定を追求する。 リスクが発現した場合： ・ 組織の目的達成のために追加資金を懇請する。 ・ 財源に十分な柔軟性が無い場合、目的を見直す。 ・ 不足額を補うための余剰資金を保持する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R*[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R26	
リスク名称	資金配分の失敗	
リスクの説明	リポジトリにおいて、メリットの少ない投資となるような無分別な資金配分がなされ、支出に見合った利益が得られない。	
このリスクは該当するか？	・ 予算管理及び支出はリポジトリの責任範囲にあるのか？	
リスク発現例	・ 限定的ではあるが十分な機能を備えたソフトウェアがもっと安価で入手できるにもかかわらず、経営者が、業務に必要な条件をはるかに上回る機能を備えたソフトウェアに多額の投資をおこなう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	予算管理者	
上位所有者	予算管理者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リポジトリ資金を確実に適切利用するため、方針の策定及び予算承認のためのインフラ構築を行う。 リスクが発現した場合： ・ さらなる配分失敗の尤度を抑えるために、方針の見直しを行う。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R25[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R27	
リスク名称	財務関連法規を遵守しないことに対する責任	
リスクの説明	当該法域における財務的義務を果たさなかったリポジトリは責任を負う。	
このリスクは該当するか？	・ リポジトリは、法規により、財務記録を特定の方法で管理することを義務付けられているか？ ・ リポジトリは、財務及び会計に関する義務を果たすために、適切な専門家に助言を要請しているか？	
リスク発現例	・ 租税に関する必要事項が満たされない。 ・ 強制財務監査を実施しない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	予算管理者	
上位所有者	予算管理者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 方針や手続きが、固有の要件や禁止事項に確実に対応するよう、財務に関する法律や規定をモニターする。 ・ 確実に義務を遂行するため、法律家及び専門家から財務に関する助言を得る。 リスクが発現した場合： ・ 法的問題が発生した場合に対処するための方針や手続きを定める。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R04[連鎖的] →R14[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R28	
リスク名称	資金不足または収入の制限	
リスクの説明	業務において特殊な状況が発生した結果、予算不足または赤字予算が発生する。	
このリスクは該当するか？	・ リポジトリの年間予算配分はどの程度確実か？ ・ リポジトリは、何らかの設備投資を１年１回よりも頻繁に行う必要があるか？ ・ 突然前触れ無しに、即時の投資を必要とする出費義務が生じる可能性があるか？	
リスク発現例	・ 機能しない技術的資産の交換など、予期せぬ強制的出費。 ・ 新しいサーバーシステムに対する4年毎の出費。これにより、その予算年度の投資額が他の予算年度よりもはるかに上回ってしまう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	予算管理者	
上位所有者	予算管理者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 年一度を超える頻度の投資を考慮した上で、予算配分の管理を行う。 ・ リポジトリ資源の交換時期を計算し、定期的に再投資をすることでハードウェアに不具合が起きる前に先手を打つ。 リスクが発現した場合： ・ 余剰の緊急資金を保持する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R25[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R29	
リスク名称	予算の削減	
リスクの説明	リポジトリ運営予算が削減される。	
このリスクは該当するか？	・ リポジトリの資金はどの程度保証されているか？ ・ 予算について、リポジトリが自ら生み出す資金ではなく、外部により管理され割り当てられる資金の割合はどの程度か？	
リスク発現例	景気後退により、政府出資のリポジトリの予算が削減される。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	予算管理者	
上位所有者	予算管理者	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・有料サービスによって、自立性を高める。 ・予算水準の安定を追求する。 リスクが発現した場合： ・組織の目的達成のために追加資金を懇請する。 ・財源に十分な柔軟性が無い場合、目的を見直す。 ・不足額を補える場合、余剰資金を保持する。	
リスクの関係	→R02[連鎖的] →R25[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

7.3.4. 技術的インフラとセキュリティ

リスク識別子	R30	
リスク名称	ハードウェアの不具合または非互換性	
リスクの説明	システムのハードウェアが、現在の事業目標達成の促進を行えなくなる。	
このリスクは該当するか？	・ コミュニティからの要求や外部からの影響が変化していく中で、ハードウェア技術が十分であるかどうかをモニターするための方針や手続きは定められているか？ ・ 第三者ハードウェアサービス会社から提供されるサービス水準保証はどのようなものか？ ・ ハードウェアの現時点での適合性及び操作上の機能性を判断するために、スタッフの就業時間の一部が割り当てられているか？	
リスク発現例	サーバーの電源が高熱で故障し、ハードウェアが使用できなくなる。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リポジトリハードウェアの現時点での適合性の確認、また、新技術の潜在的価値の評価を行うために、スタッフの就業時間の一部を割り当てる。 ・ システムの変更が実施される前に、その影響を査定する。 ・ 先行投資を行い、ハードウェアの不具合が起きる前に対処する。 リスクが発現した場合： ・ ハードウェア供給業者または第三者ハードウェアサービス会社から、サービス品質保証契約（SLA）の正式な保証を得られるよう働きかける。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R32[連鎖的] →R35[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	

リスクの深刻度	12

リスク識別子	R31	
リスク名称	ソフトウェアの不具合または非互換性	
リスクの説明	システムのソフトウェアが、現在の事業目標達成の促進を行えなくなる。	
このリスクは該当するか？	・ コミュニティからの要求や外部からの影響が変化していく中で、ソフトウェア技術が十分であるかどうかを点検するための方針や手続きは定められているか？ ・ 第三者ソフトウェアサービス会社から提供されるサービス水準保証はどのようなものか？ ・ ソフトウェアの現時点での適合性及び操作上の機能性を判断するために、スタッフの就業時間の一部が割り当てられているか？	
リスク発現例	・ ソフトウェアのアップデートにより、他の基幹的ソフトウェアサービスとの依存関係が壊れる。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リポジトリソフトウェアの現時点での適合性の確認、また、新技術の潜在的価値の評価を行うために、スタッフの就業時間の一部を割り当てる。 ・ システムの変更が実施される前に、その影響を査定する。 ・ 先行投資を行い、ソフトウェアが陳腐化する前に対処する。 リスクが発現した場合： ・ ソフトウェア供給業者または第三者ソフトウェアサービス会社から、サービス品質保証契約（SLA）の正式な保証を得られるよう働きかける。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R32[連鎖的] →R35[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R32	
リスク名称	ハードウェアやソフトウェアが、リポジトリにおいて新たに出現してくる目標の達成をサポート出来ない。	
リスクの説明	技術的インフラが、現在の目標達成には十分なのだが、組織が自然と進化することにより出現する新たな要件を満たすことが出来ない。	
このリスクは該当するか？	・ 予想されるリポジトリの成長を促進するために、技術的設備の追加は必要か？ ・ リポジトリの現在のサービス水準は、時間の経過とともに、どの程度まで拡大すると思われるか？	
リスク発現例	・ 予想される目標や要求数の拡大に対処するにあたり、技術的インフラの拡張性が不十分。 ・ ハードウェアと新しいOSとの互換性がない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： 新たに出現する組織目標に関連して、リポジトリ技術の拡張性及び互換性を点検するために、スタッフの就業時間の一部を割り当てる。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R33	
リスク名称	ハードウェアまたはソフトウェアの陳腐化	
リスクの説明	基幹的技術がもはや最新のものではなく、類似の組織の基幹的技術と一致しない。	
このリスクは該当するか？	・ 現在使用されているハードウェアやソフトウェアの供給業者は、サポートの保証期間を提示しているか？ ・ ハードウェアやソフトウェアの技術は、現代の類似組織において広く採用されているものか？ ・ リポジトリが採用している技術の平均故障間隔は？	
リスク発現例	・ 供給業者によるOSのサポートが終了し、セキュリティのアップデートが入手できない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リポジトリ技術の現時点での適合性のモニター、また、新技術の潜在的価値の評価を行うために、スタッフの就業時間の一部を割り当てる。 ・ 先行投資を行い、技術が陳腐化する前に対処する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R34	
リスク名称	メディアの劣化または陳腐化	
リスクの説明	ストレージメディアが劣化し、書き込みや読み取りの能力が制限される。	
このリスクは該当するか？	・ リポジトリは、デジタルコンテンツを、テープ、光ディスク、フラッシュメモリ等のリムーバブルメディアに保存しているか？ ・ 採用しているストレージメディアのフォーマットは、現代の類似組織において広く採用されているものか？ ・ 依存しているメディア技術の平均寿命を、理解し、記録しているか？	
リスク発現例	・ 磁気テープの物理的劣化により、テープに蓄積されたコンテンツにアクセス出来ない。または、コンテンツが破損する。 ・ 現在のテープドライブでは、アーカイブに大量に存在する古いストレージメディアの読み込みが出来ない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ ストレージメディアの予想寿命の確認、また、新技術の潜在的価値の評価を行うために、スタッフの就業時間の一部を割り当てる。 ・ 先行投資を行い、メディアが陳腐化する前に対処する。 リスクが発現した場合： ・ 情報オブジェクトの冗長コピーを保持する。 ・ アーカイブされた資料を、劣化したメディアから取り出すための方針や手続きを定める。	
リスクの関係	→R02[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R35	
リスク名称	セキュリティの脆弱性の悪用	
リスクの説明	リポジトリにおけるセキュリティ対策の欠陥が特定され、不正アクセスのために利用される。	
このリスクは該当するか？	・リポジトリの物理的セキュリティやシステムセキュリティにおいて、顕著な脆弱性があると考えられるか？ ・リポジトリの内部または外部の人間が、資料の入手や破壊を目的としてセキュリティを侵害しようとすることは有り得るか？ ・アーカイブされた資料は、ネットワークにアクセス可能なコンピュータに蓄積されているか？	
リスク発現例	・パッチを当てられていないソフトウェアセキュリティの抜け穴を利用してハッキングされる。 ・侵入者が防犯ドアを無理に開けて、リポジトリに物理的にアクセスする。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェア、または通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・関連基準に従い、物理的セキュリティやソフトウェアセキュリティのための方針及び手続きを定め、それらに対する評価を定期的に実施する。 ・不可欠ではないサービスの実施を制限する。 ・ソフトウェアを最新のセキュリティパッチでアップデートする。 ・過去のセキュリティ侵害の試みの分析、及び、既知の脆弱性の詳細を知るためのセキュリティ情報源のモニターのために、スタッフの就業時間の一部を割り当てる。 ・ユーザーがパスワードを頻繁に変更することを必須にする。 リスクが発現した場合： ・システム侵害の影響を残さないために、システムを再構築する。	
リスクの関係	→R01[連鎖的]　→R02[連鎖的] →R36[連鎖的]　→R37[連鎖的] →R38[連鎖的]　→R42[連鎖的] →R46[連鎖的]　→R52-79[連鎖的]	
リスクの発現可能性	4	

リスクの潜在的影響	3
リスクの深刻度	12

リスク識別子	R36	
リスク名称	未確認のセキュリティ侵害、脆弱性または情報の劣化	
リスクの説明	セキュリティの悪用または脆弱性が発生しているにもかかわらず、リポジトリのスタッフによってモニターされることも、確認されることもない。	
このリスクは該当するか？	・ システムへのアクセスの試みを全て確認するための仕組みは整っているか？ ・ 蓄積されたコンテンツへの変更が、いつ、どのように行われたかを判断するための仕組みは整っているか？ ・ セキュリティ侵害の証拠またはセキュリティ侵害の試みの証拠を探すための、システムログの定期的な分析は行われているか？	
リスク発現例	・ システムがハッキングされ、スタッフに知られることなしに、キーロガーがインストールされる。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ システム侵害の尤度を抑えるための適切な措置を取る。また、関連基準に従い、侵害の試みがどこで行われたかをモニターする。 リスクが発現した場合： ・ システムログの分析によってセキュリティ侵害の詳細情報を得るために、スタッフの就業時間の一部を割り当てる。 ・ システム侵害の影響を残さないために、システムを再構築する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R42[連鎖的] →R46[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R37	
リスク名称	ハードウェアのストレージスペースに対する物理的な侵入	
リスクの説明	リポジトリのテクニカルハードウェアが物理的に設置されている場所に侵入者がアクセスする。	
このリスクは該当するか？	・ リポジトリの物理的セキュリティにおいて、顕著な脆弱性があると考えられるか？ ・ リポジトリの内部または外部の人間が、資料の入手や破壊を目的として、セキュリティを侵害しようとすることは有り得るか？	
リスク発現例	・侵入者が、セキュリティ対策を回避してリポジトリに侵入する	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 関連基準に従い、物理的セキュリティに関する方針及び手続きを定め、試験し、定期的に評価を実施する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R42[連鎖的] →R46[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R38	
リスク名称	ローカルまたはリモートのソフトウェアによる侵入	
リスクの説明	ネットワークのセキュリティ対策を回避して、施設内または遠隔地からの侵入を受ける。	
このリスクは該当するか？	・リポジトリのセキュリティにおいて、顕著な脆弱性があると考えられるか？ ・リポジトリの内部または外部の人間が、資料の入手や破壊を目的として、セキュリティを侵害しようとすることは有り得るか？ ・アーカイブされた資料は、ネットワークにアクセス可能なコンピュータに蓄積されているか？	
リスク発現例	・ ハッカーが、セキュアシェル・トンネリングによって、遠隔地からサーバーソフトウェアのセキュリティ上の弱点を突き、サーバー上で悪質なコードを実行する。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 関連基準に従い、ソフトウェアセキュリティのための方針及び手続きを定め、それらに対する評価を定期的に実施する。 ・ 不可欠ではないサービスの実施を制限する。 ・ ソフトウェアを、最新のセキュリティパッチでアップデートする。 ・ 過去のセキュリティ侵害の試みの分析及び既知の脆弱性の詳細を知るためのセキュリティ情報源の確認のために、スタッフの就業時間の一部を割り当てる。 ・ ユーザーがパスワードを頻繁に変更することを必須にする。 リスクが発現した場合： ・ システム侵害の影響を残さないために、システムを再構築する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R42[連鎖的] →R46[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R39	
リスク名称	当該地域における破壊的な環境現象	
リスクの説明	リポジトリ外部で発生する、局地的な影響を伴う事態によって、リポジトリの事業活動が影響を受ける。	
このリスクは該当するか？	・ リポジトリが、悪天候や異常気象にさらされる可能性は高いか？ ・ リポジトリは、地質学的な危険、または人為起源の危険にさらされているか（地震、火山、採掘に関連した地盤沈下や海岸侵食など）？	
リスク発現例	・非常に近い場所でのハリケーン、竜巻、または台風 ・地震	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 該当する環境問題発生の尤度をモニターする。 ・ ハリケーン被害防止用の窓を取り付けるなど、現地で最も深刻な脅威に対する予防対策を取る。 リスクが発現した場合： ・ 遠隔地に冗長ストレージを設置する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R42[連鎖的] →R46[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R40	
リスク名称	偶発的なシステムの混乱	
リスクの説明	故意によらない介入または悪影響を及ぼすことを意図しない介入によって、事業活動が悪影響を受ける	
このリスクは該当するか？	・ リポジトリのシステムは、合意された方針や手続きに反する操作を実行することをスタッフに許可しているか？ ・ 操作は可逆的か？	
リスク発現例	・ スタッフが誤って、リポジトリに不可欠なソフトウェアサービスを停止してしまう。 ・ 受入時に、不注意によりコンテンツが削除されてしまう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 無効な操作や、方針に反する操作が物理的に起き得る程度を制限するためのシステムを構築する。 ・ システムの使用に関してスタッフが十分な訓練を受けるようにする。また、操作を実行する前にチェックを行うことの重要性について、スタッフへの周知徹底を行う。 リスクが発現した場合： ・ 不慮の行動が取られた理由を確認し、ユーザーが失敗を繰り返すことを許さない、または、繰り返さないように注意を促すための方策を導入する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R41	
リスク名称	故意によるシステムへの破壊行為	
リスクの説明	システムの破壊を意図した手段により、事業活動が悪影響を受ける。	
このリスクは該当するか？	・ 個人が悪意を持って、リポジトリのコンテンツやシステムにダメージを与えようとすることは考えられるか？ ・ システムにおける操作またはシステムをすり抜けて実行された操作の可逆性はどの程度か？ ・ 当該組織を脱退したスタッフは、現場の外まで追跡され、システムへのアクセス手段や権限を剥奪されるか？	
リスク発現例	・電子テロ行為または物理的な（従来的な）テロ行為 ・組織に不満を持つスタッフが、悪意を持ってシステムを破壊する。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 関連基準に従い、物理的セキュリティ及びソフトウェアセキュリティを保持、試験、また見直しする。 ・ ネットワーク上の不審な行動または異常と見受けられる身体的行動をモニターする。 ・ 組織に不満を持っている可能性が高いスタッフや元スタッフを排除し、即座にシステムに関する権限を取り消す。 リスクが発現した場合： ・ システム上の全ての操作の可逆性を可能な限り確保する。 ・ システム状態及びアーカイブ情報の冗長コピーを、地理的に離れた場所で確保する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R42[連鎖的] →R46[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R42	
リスク名称	リポジトリサイトのサイトが壊れる、または使用不可能になる。	
リスクの説明	リポジトリの物理的基盤が壊れる、または、永久または一時的に使用不可能になる。	
このリスクは該当するか？	・ リポジトリの業務活動は、１棟の物理的建物、または、地理的に小さな範囲にある１グループの物理的建物の中で行われているか？ ・ 冗長システム及び冗長ストレージ施設は構築されているか？	
リスク発現例	・火災によるダメージ ・建物中でのアスベストの使用が判明する。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 関連基準に従い、物理的システム及びソフトウェアシステムのセキュリティ方針を保持、試験、見直しする。 リスクが発現した場合： ・ 業務拠点として使用可能な冗長ストレージ施設を構築する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R52-79[連鎖的] →R52-79[爆発的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R43	
リスク名称	基幹的公益サービスが利用できない。	
リスクの説明	外部からサービスを提供している第三者が、一時的にサービスを中断せざるを得ない状況に陥り、それらのサービスが利用できなくなる。	
このリスクは該当するか？	・ リポジトリは、ガス、電気、ネットワークサービス、水など、外部から提供される公益サービスに依存しているか？	
リスク発現例	・リポジトリへの電力供給が一時的に中断される。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営	
上位所有者	経営	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 公益サービス会社と、サービス水準合意書、または、サービス契約書を締結する。 リスクが発現した場合： ・ ガソリン発電機や無停電電源装置（UPS）を設置するなど、可能な範囲すべてにおいて、サービス中断による被害をゼロにするための手段を組織内で構築する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R42[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R44	
リスク名称	第三者によるその他サービスの停止	
リスクの説明	リポジトリが依存する、第三者によるその他サービスが中断される。	
このリスクは該当するか？	・ リポジトリは、何らかの活動について、下請け業者に依頼しているか？ ・ リポジトリは、清掃やケータリングなど、公益サービス以外で第三者による何らかのサービスに依存しているか？	
リスク発現例	・ リポジトリの情報提供システムにサービス提供をしているウェブホスティング会社が廃業する。 ・ リポジトリにサービス提供をしている仕出し業者がストライキ等に入り、スタッフに食事が供給されない。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	経営	
上位所有者	経営	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 公益サービス会社と、サービス水準合意書、またはサービス契約書を締結する。 リスクが発現した場合： ・ 可能な範囲すべてにおいて、サービス中断による被害をゼロにするための手段を組織内で構築する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R42[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R45	
リスク名称	第三者サービス業者とのサービス契約における条件の変更	
リスクの説明	第三者によるサービス提供においての条件が大幅に変更される。	
このリスクは該当するか？	・ 第三者サービスまたは第三者公益サービスに関する契約は更新されることがあるか、また、再交渉がなされることに決まっているか？	
リスク発現例	・ 電気料金が段階的に値上がりする。 ・ リポジトリが依存している技術を、ウェブホスティングサービス会社がサーバーから取り除いてしまう。	
リスクの性質	物理的環境	X
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	経営	
上位所有者	経営	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： 再交渉可能な範囲を最小限にした、永続的なサービス水準合意書を、第三者サービス会社と取り交わす。 リスクが発現した場合： ・ もっと有利な条件を提示することが可能な別のサービス会社を探す方針を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R42[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R46	
リスク名称	主要な文書の破壊	
リスクの説明	リポジトリの文書が部分的または完全に破壊される。	
このリスクは該当するか？	・ リポジトリの文書は、リポジトリの主たる事業所にて保存、蓄積されているか？ ・ 複数の文書コピーが保存、蓄積されているか？	
リスク発現例	・ リポジトリの事務局で発生した火災によって、契約や方針に関する文書が破壊される。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	経営	
上位所有者	経営	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 文書の電子コピー及びハードコピーを、複数の場所で複数蓄積する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R12[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R47	
リスク名称	技術的インフラ及びセキュリティの有効性を評価するための能力の不足	
リスクの説明	保有する技術的インフラ及びセキュリティ対策の使用により、どの程度まで事業目標達成を推進することが可能なのか、効果的に判断する能力がリポジトリに無い。	
このリスクは該当するか？	・ リポジトリにおいて、セキュリティ侵害の試みの確認と記録のための方針及び手続きは定められているか？ ・ リポジトリにおいて、システム上での不正または不適切な交信を確認するための方針及び手続きは定められているか？ ・ リポジトリにおいて、ハードウェア・ソフトウェア技術及びストレージメディアの現時点での適合性や機能性を確保するための方針及び手続きは定められているか？ ・ 技術的設備やセキュリティ対策の有効性を判断するための仕組みが定期的に活用されているか？	
リスク発現例	・ リポジトリにおいて、セキュリティ対策の試験、または技術的インフラの有効性の評価を行うための仕組みが用意されていない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	経営	
上位所有者	経営	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リスクマネジメントを含めた、内部評価の方法を確立する。 ・ 能力を実証するために、関連する認証を外部機関から取得することをめざす。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R19[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

7.3.5. 収集と受入

リスク識別子	R48	
リスク名称	受け取った情報パッケージが構造的に無効または不正な形式をとっている	
リスクの説明	受け取った情報パッケージが、リポジトリの期待するもの、または、リポジトリで保存可能なものと異なる。	
このリスクは該当するか？	・ 提出されるコンテンツについて、準拠すべき構造がリポジトリにおいて定められているか？ ・ リポジトリは、受け入れ可能なフォーマットを規定しているか？	
リスク発現例	・ 提出されたコンテンツが、リポジトリではサポートされていないフォーマットにエンコードされている。 ・ 提出されたXMLエンコード済みのコンテンツが、リポジトリの提供するスキーマに適合しない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	受入	
上位所有者	受入	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 提出される情報パッケージの構造について、定義付けを行う。 ・ 受入可能な情報パッケージフォーマットのリストを作成する。 ・ コンテンツ提供者及び生産者に対し、定義に関する情報提供を行う。 リスクが発現した場合： ・ 情報パッケージが破棄されるのか、返却されるのか、または、受入されるのかを判断するための方針及び手続きを保持する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R49[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R49	
リスク名称	提出された情報パッケージに不備がある	
リスクの説明	保存のために必要な情報が、受け取った情報パッケージに含まれていない。	
このリスクは該当するか？	・ 提出されるコンテンツについて、準拠すべき構造がリポジトリにおいて定められているか？ ・ 提出されるコンテンツについて、メタデータに関する要件がリポジトリにおいて規定されているか？	
リスク発現例	・ 提出される全ての情報パッケージに契約通り付加されるべきメタデータ情報が、提出されたコンテンツに含まれていない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	受入	
上位所有者	受入	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 提出される情報パッケージの構造について、定義付けを行う。 ・ 受入可能な情報パッケージフォーマットのリストを作成する。 ・ コンテンツ提供者及び生産者に対し、定義に関する情報提供を行う。 リスクが発現した場合： ・ 情報パッケージが破棄されるのか、返却されるのか、または、受入されるのかを判断するための方針及び手続きを保持する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R50	
リスク名称	受入中に、情報の変更やメンテナンスが、外部の意思により行われる	
リスクの説明	情報パッケージに対して、受け取り時からアーカイブ可能なオブジェクトの作成までの期間に、リポジトリの認可や実施によるものではない変更が加えられる。	
このリスクは該当するか？	・ リポジトリは、提出されるコンテンツについて、完全な物理的及び知的管理権限を取得しているか？	
リスク発現例	・ 提出される情報パッケージに本来備えられているべき情報が、提供された情報パッケージに含まれておらず、これらの情報がリモート参照の対象となっている。このリモートオブジェクトが、受入中に、外部の主体により変更を加えられることがある。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	受入	
上位所有者	受入	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： 受け取ったオブジェクトについて、独占的かつ完全な、物理的及び知的管理権を必ず取得するようにする。 リスクが発現した場合： ・ 情報パッケージが破棄されるのか、返却されるのか、または、受入されるのかを判断するための方針及び手続きを保持する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R52-79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R51	
リスク名称	受け取った情報パッケージを追跡できないアーカイブ情報	
リスクの説明	アーカイブされたオブジェクトを追跡して、それに対応する、提出された情報パッケージをトレースできない。	
このリスクは該当するか？	・ アーカイブコンテンツと、元々提出された情報パッケージの一致を確認するための方針及び手続きは定められているか？ ・ 受入されたコンテンツは、アーカイブ情報パッケージ（AIP）に変換されるか？	
リスク発現例	・ 完全性が適切に保存されていることを確認するために、アーカイブ情報パッケージの元となった情報パッケージの確認をリポジトリが行うことができない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	受入	
上位所有者	受入	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 受け取り時と受入時に行われるやり取りの詳細が記述された、適切な来歴情報を記録する。 リスクが発現した場合： ・ 情報パッケージが破棄されるのか、返却されるのか、または、保持されるのかを判断するための方針及び手続きを保持する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R55[連鎖的] →R60[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

7.3.6. 保存と蓄積

リスク識別子	R52	
リスク名称	情報の機密性の喪失	
リスクの説明	秘密保持契約によって保護された情報が、それらの契約に違反して一般に公開される。	
このリスクは該当するか？	・リポジトリは、情報の秘密保持を義務付けられているか？	
リスク発現例	・ リポジトリの認可サブシステムに障害がおき、商業的機密情報が、寄託に関連する合意事項に基づいた正規にアクセス権限を与えられる対象よりも、相当に広い範囲の一般に公開されてしまう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リポジトリが負う全ての秘密保持義務を十分に考慮した上で、方針や手続きの案を出すようにする。 ・ ソフトウェアシステム、ハードウェアシステム及び保存戦略が、方針に定められた要件を確実に満たせるものであるようにする。 リスクが発現した場合： ・ 機密資料の公開を止めるための方針及び評判の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R53	
リスク名称	情報やサービスが提供出来なくなる	
リスクの説明	リポジトリが、総合的なサービスの提供及びアクセス可能であるべき全ての保有情報へのアクセスの提供を行えない。	
このリスクは該当するか？	・リポジトリは、規定されたサービス水準を保つことを誓約しているか？ ・情報の利用可能性について、リポジトリは保証を行っているか？	
リスク発現例	・ アクセスの提供が契約書に明記されているにもかかわらず、リポジトリのサーバーに障害が起き、保有情報の一部へのアクセスが不可能となる。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ サービス水準に関してリポジトリが誓約している事項を十分に考慮した上で、方針や手続きの案を出すようにする。 ・ ソフトウェアシステム、ハードウェアシステム及び保存戦略が、サービス水準を確実に満たせるものであるようにする。 リスクが発現した場合： ・ 評判や信頼の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R54	
リスク名称	情報の真正性の喪失	
リスクの説明	・ リポジトリによって表明されるものと、実際に提供される情報オブジェクトが一致していることを証明する能力がリポジトリに無い。	
このリスクは該当するか？	・ 情報の真正性を保存することをリポジトリは誓約しているか？	
リスク発現例	・ 政府省庁の支出を記述した保存記録の真正性を、リポジトリが証明出来ない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 真正性に関する要件を十分に考慮した上で、方針や手続きの案を出すようにする。 ・ アーカイブ資料が、最初に提出され受け取った資料に相当する正真正銘の資料であることを証明するため、来歴情報の適切な記録を確実に行うための方針や手続きの保持及び見直しを行う。 ・ ソフトウェアシステム、ハードウェアシステム及び保存戦略が、真正性を確実に保持できるものであるようにする。 リスクが発現した場合： ・ 評判や信頼の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R55	
リスク名称	情報の完全性の喪失	
リスクの説明	受け取り時点から情報の完全性が維持されていること、また、蓄積されている情報が元々受け取った情報と正確に一致していることを証明する能力がリポジトリに無い。	
このリスクは該当するか？	・リポジトリは、情報の完全性を保存することを誓約しているか？	
リスク発現例	・ 政府支出の記録文書に、予期されていない無権限での変更が加えられ、その記録文書が元々提出されたコンテンツに相当するものではなくなってしまう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 完全性に関する要件を十分に考慮した上で、方針や手続きの案を出すようにする。 ・ 提出・受け取り後にアーカイブ情報の完全性が喪失していないことを証明するため、チェックサムの適切な記録及び比較を確実に行うための方針や手続きの保持及び見直しを行う。 ・ ソフトウェアシステム、ハードウェアシステム及び保存戦略が、完全性を確実に保持できるものであるようにする。 リスクが発現した場合： ・評判や信頼の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R56	
リスク名称	未確認の情報変更	
リスクの説明	アーカイブ情報に対する変更がどこで行われたか、追跡やモニターする能力がリポジトリに無い。	
このリスクは該当するか？	・ 保存情報を対象とした交信または変更がどこで行われたかを確認するための手段をリポジトリは保有しているか？	
リスク発現例	・ アーカイブ情報への変更がどこで行われたのかを検出するための、適切なチェックサム情報の記録や保持をリポジトリが怠る。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ アーカイブ情報のチェックサム値を定期的に記録、計算、比較するための方針及び手続きを導入する。 リスクが発現した場合： ・ アーカイブ情報のチェックサム値を定期的に記録、計算、比較するための方針及び手続きを導入する。 ・ 評判や信頼の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R57	
リスク名称	責務否認を防止する能力の喪失	
リスクの説明	当事者のいずれかが後で責務の否認を行うことを確実に防止する能力がリポジトリに無い。	
このリスクは該当するか？	・ 契約当事者が何らかの義務を負う契約を、リポジトリは取り交わしているか？	
リスク発現例	・ 請負業者が、交わした情報及び暗黙の義務に同意した事実を後になって否定したときに、その会議の詳細の記録を採っていない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 契約上の責務について、両当事者が知り、理解し、記録し、合意したことを確実にするための、方針及び手続きを保持また見直しする。 リスクが発現した場合： ・ 手続き上の適切な対応を（契約履行の強制に向けて法的助言を求めるなど）明確化するための方針を導入する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R16[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R58	
リスク名称	情報の信頼性の喪失	
リスクの説明	保有する情報の信頼性を証明する能力がリポジトリに無い。	
このリスクは該当するか？	・リポジトリは、情報の信頼性を保存することを誓約しているか？	
リスク発現例	・ 気象データセンターにあるアーカイブ情報について、科学的研究の根拠として利用するに足りる信頼性が無いとみなされる。 ・ アーカイブ情報が、信頼性が無いという理由により、法廷において証拠として認められない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 信頼性に関する要件を十分に考慮した上で、方針や手続きの案を出すようにする。 ・ 提出・受け取り後にアーカイブ情報の完全性が喪失していないことを証明するため、チェックサムの適切な記録及び比較を確実に行うための方針や手続きの保持及び見直しを行う。 ・ アーカイブ資料が、最初に提出され受け取った資料に相当する正真正銘の資料であることを証明するため、来歴情報の適切な記録を確実に行うための方針や手続きの保持及び見直しを行う。 ・ ソフトウェアシステム、ハードウェアシステム及び保存戦略が、信頼性を確実に保持できるものであるようにする。 リスクが発現した場合： ・ 評判や信頼の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R59	
リスク名称	情報来歴の喪失	
リスクの説明	保有する情報の来歴及びそれらの受入や、それらが関与した各操作についてのトレーサビリティを証明する能力がリポジトリに無い。	
このリスクは該当するか？	・ アーカイブ情報パッケージ（AIP）の出所やライフサイクル、また、その情報パッケージに対して行われた全てのやり取りや操作を記録するための機構は、リポジトリにおいて整っているか？	
リスク発現例	・ 受け取ったMicrosoft Wordファイルをプレーンテキストのマスターファイルに変換するために行われた保存プロセスの記録を、リポジトリが怠る。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 来歴に関する要件を十分に考慮した上で、方針や手続きの案を出すようにする。 ・ アーカイブ情報パッケージの出所やライフサイクル及びその情報パッケージに対して行われた全てのやり取りや交信を記録するための、方針や手続きの保持及び見直しを行う。 ・ ソフトウェアシステム、ハードウェアシステム及び保存戦略が、来歴情報の保持や記録を確実に行えるものであるようにする。 リスクが発現した場合： ・ 評判や信頼の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R51[連鎖的] →R69[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R60	
リスク名称	バックアップの喪失または不適合	
リスクの説明	バックアップ機構から、コンテンツやシステム状態の情報を、リポジトリが読み出せない。	
このリスクは該当するか？	・ 一次的なデジタル資料の喪失や利用不可能への対応として、リポジトリはシステムやコンテンツのバックアップに依存しているか？ ・ バックアップシステムは、十分に確立し、広く使用されている技術を基に作られているか？ ・ 一次的なリポジトリサイトの破壊や損傷の際、バックアップ資料の安全性も脅威にさらされるか？	
リスク発現例	・ 一次的なアーカイブ資料が喪失した際、バックアップテープが修復不可能な状態まで破損しているため、リポジトリがコンテンツを復元できない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	技術	
上位所有者	技術	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ バックアップのコピーを複数保持する。 ・ バックアップコンテンツを遠隔地で蓄積しておく。 ・ システム及びデータがバックアップから復元可能か判断するために、定期的に「火災訓練」テストを行う。 リスクが発現した場合： ・ デジタル考古学やデジタル科学捜査などの技術を利用して、できるだけ多くのコンテンツを回復する。 ・ 評判の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R52-69[爆発的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R61	
リスク名称	冗長コピーの不一致	
リスクの説明	リポジトリがアーカイブ情報のコピーを複数保持しているが、それらが一致しない。	
このリスクは該当するか？	・ リポジトリは、アーカイブコンテンツの冗長コピーを複数保持しているか？ ・ リポジトリは、複数のコピーの不一致をチェックするための機構を採用しているか？ ・ そのような不一致の発見に対応するための方針及び手続きは定められているか？	
リスク発現例	・ リポジトリがアーカイブ情報の冗長コピーを３つ保持しているが、チェックサムの比較をランダムに行ったところ、１つのコピーが他のコピーと異なっていることが明らかになる。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 冗長情報パッケージに対応するチェックサム情報を定期的に記録及び比較する。 ・ データの破損やデータに対する不正行為の尤度を制限するための技術及びセキュリティを保持する。 リスクが発現した場合： ・ 上記のような不一致の発見に対処するための方針及び手続きを案出する（例えば、多数派となるチェックサム値は正確とみなされ、少数派となるチェックサム値は破棄及び交換されるという、多数決システムを使用する）。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R12[爆発的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R62	
リスク名称	何がアーカイブオブジェクトの範囲に入るのか不明確	
リスクの説明	アーカイブオブジェクトのどの部分が進行中の保存作業の対象となるのか判断する能力がリポジトリに無い。	
このリスクは該当するか？	・ アーカイブ情報パッケージ（AIP）のフォーマットの領域や範囲を、リポジトリは定義しているか。 ・ アーカイブ情報パッケージ（AIP）の完全性及び正確性を認証するための方針及び手続きは存在するか？	
リスク発現例	・ 保有するアーカイブ情報パッケージ（AIP）のフォーマットの適切な定義付けを、リポジトリが怠る。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ アーカイブ情報パッケージ（AIP）の定義を案出する。 リスクが発現した場合： ・ アーカイブオブジェクトに関する曖昧さに対処するための方針を案出する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R12[爆発的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R63	
リスク名称	受入プロセス有効性を確認することが出来ない	
リスクの説明	デジタル情報の受入プロセスを通じて完全性及び真正性が保たれていることを確認する能力がリポジトリに無い。	
このリスクは該当するか？	・ リポジトリは、チェックサム値の記録と比較のための方針や手続きを保持しているか？ ・ リポジトリの諸プロセスの実行を記録及び評価し、それらのプロセスによるアウトプットの完全性及び正確性をチェックするための方針や手続きを、リポジトリは保持しているか？ ・ 受入手続きの有効性を判断するための機構が定期的に用いられているか？	
リスク発現例	・ 受入手続きを経て完成したアーカイブ情報パッケージ（AIP）が完全で正確なものであることをリポジトリが証明できない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リスクマネジメントを含めた、内部評価の方法を確立する。 ・ 受入プロセスの有効性を証明するために、関連する認証を外部機関から取得することをめざす。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R19[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R64	
リスク名称	情報参照整合性のための識別子に障害が起きる。	
リスクの説明	情報に識別子が当てられているが、識別子に対応するアーカイブ情報パッケージ（AIP）を、リポジトリが特定できない。	
このリスクは該当するか？	・ リポジトリは情報パッケージに対し、現存する永続的な識別子を適用しているか？ ・ 識別子と関連情報との違いを識別することは可能か？	
リスク発現例	・ デジタルオブジェクトの元の環境から引き継いだファイルパスを、リポジトリにおいてアーカイブオブジェクトの識別子として使用し続け、その結果、異なるロケーションからの２つの異なるオブジェクトが、“C:¥Documents and Settings¥John Smith¥Document.pdf”といった同一の識別子を使用することになる。 ・ 受入時点のタイムスタンプによって、受入時に作られる識別子が構成されるのだが、２つの受入システムが同時に稼働した結果、同一の識別子が適用されてしまう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 識別子と、それに対応する情報パッケージを関連付ける方法を説明するための方針及び手続きの明確化、文書化、見直しを行う。また、これに関する情報を組織内で広く伝達する。 ・ 識別子の唯一性を確保するために、識別子の作成に関して説明するための方針及び手続き、または、第三者が提供する識別子技術（Handle, DOI, PURL等）の採用を義務付けるための方針及び手続きの明確化、見直しを行う。 リスクが発現した場合： ・ 識別子と情報との関連性の破壊に対処するための方針を明確化する。 ・ 評判の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R12[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R65	
リスク名称	保存計画を実施に移せない	
リスクの説明	立案した保存計画を、リポジトリが実行できない。	
このリスクは該当するか？	・ リポジトリで行われる保存計画の立案は、後の実施を視野に入れて行われているか？ ・ 保存計画の立案において、組織目標のみならず、リポジトリが利用できる技術的・財的・人的資源の範囲も反映されているか？	
リスク発現例	・ リポジトリで計画されるエミュレーション方策の実施には、リポジトリのスタッフが持っていない技術的専門知識が必要となる。また、その作業を第三者開発業者に依頼するための資金が不足している。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 保存計画の立案に際し、組織目標のみならず、リポジトリが利用できる技術的・財的・人的資源の範囲も反映することを目指す。 ・ 当初の計画を推進するための追加資金調達を目指す。 リスクが発現した場合： ・ 保存計画を、組織独自に実施可能なものとすることを目指して改善するための方針を実施する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R67[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R66	
リスク名称	保存対策の実施が情報の喪失をもたらす	
リスクの説明	アーカイブオブジェクトに対して保存計画が実施された結果、そのオブジェクトの重要な特性が１つまたは複数、喪失または損傷する。	
このリスクは該当するか？	・ 保存活動の結果として起こり得る喪失の許容範囲を、リポジトリは定義しているか？	
リスク発現例	・ リポジトリが提案する移行方策を実施した結果、ユーザーコミュニティでは不可欠な特性だと考えられている、アーカイブ文書の「見た目や雰囲気」が失われてしまう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 保存戦略を実施する前にテストベッド環境で評価する。 ・ 予期しない結果または不適切な結果が起きた場合に、手続きを可逆にしておく。 リスクが発現した場合： ・ リポジトリにおける情報喪失の許容レベルを説明する方針を定義する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R52-R69[連鎖的] →R61[爆発的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R67	
リスク名称	保存プロセスの有効性の確認が出来ない	
リスクの説明	事業目標の観点から、保存活動がどの程度成功しているかを効果的に判断する能力がリポジトリに無い。	
このリスクは該当するか？	・ リポジトリにおいて、情報の見読性、真正性、また完全性が保存されていることを確認するための方針及び手続きは保持されているか？	
リスク発現例	・ リポジトリの設立から長い年月が経過し、保有情報も長年保存されている場合に、しかるべきユーザーコミュニティにとっての見読性も含め、保有情報の保存状態が長年に渡り継続していることを証明する手段が、リポジトリにおいて不足している。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	保存	
上位所有者	保存	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リスクマネジメントを含めた、内部評価の方法を確立する。 ・ 能力を証明するために、関連する認証を外部機関から取得することをめざす。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R19[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R68	
リスク名称	受入時、アーカイブ時、提供時の情報パッケージが追跡できない	
リスクの説明	情報パッケージを、リポジトリの情報サイクルの初期段階までさかのぼり、対応する１つ、または１組の情報パッケージに辿り着くことが出来ない。	
このリスクは該当するか？	・ 情報パッケージの出所やライフサイクル及びそれら情報パッケージに対して行われた全てのトランザクションややりとりを記録するための機構は、リポジトリにおいて整っているか？	
リスク発現例	・ 情報パッケージの出所やライフサイクル及びそれら情報パッケージに対して行われたすべてのやり取りや交信を記述した適切な文書を保持することを、リポジトリが怠る。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	経営	
上位所有者	経営	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 受け取り、受入、保存、また提供のプロセスにおいて行われた操作の詳細が記述された適切な来歴情報を記録する。 リスクが発現した場合： ・ 情報パッケージが破棄されるのか、返却されるのか、あるいは、受入されるのかを判断するための方針及び手続きを保持する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

7.3.7 メタデータ管理

リスク識別子	R69	
リスク名称	情報参照整合性のためのメタデータに障害が起きる	
リスクの説明	情報パッケージと、それに対応するメタデータとの関連性が壊れ、行き来ができない。	
このリスクは該当するか？	・ リポジトリは、アーカイブ情報に関連付けられたメタデータ記録を保持しているか？ ・ メタデータ記録が、対応するアーカイブ情報から切り離されてしまう可能性はあるか？ ・ 関連性はどのように定義・記述されているか？	
リスク発現例	・ メタデータと、それに対応するオブジェクトとの関係を表す、リポジトリのディレクトリ構造を記述した文書が、完全に喪失し、回復不能。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	文書管理	
上位所有者	文書管理	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ メタデータと、それに対応する情報パッケージを関連付ける方法を説明するための方針及び手続きの明確化、文書化、見直しを行う。また、これに関する情報を組織内で広く伝達する。 ・ リポジトリの活動において利用されるメタデータスキーマを説明するための方針及び手続きの明確化並びに見直しを行う。 リスクが発現した場合： ・ メタデータと情報との関連性が壊れた場合に対処するための方針を明確化する。 ・ 評判の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R52-69[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R70	
リスク名称	変更履歴の記録が不完全あるいは不正確	
リスクの説明	情報パッケージについて、メタデータの記録における操作及び実施された保存戦略や手続きが、記録されていない、または、部分的にしか記録されていない。	
このリスクは該当するか？	・ 情報パッケージの出所やライフサイクル及びその情報パッケージに対して行われた全てのトランザクションややりとりを記録するための機構は、リポジトリにおいて整っているか？	
リスク発現例	・ アーカイブ情報パッケージの出所やライフサイクル及びそれら情報パッケージに対して行われたすべてのやり取りや操作を記述した適切な文書を保持することを、リポジトリが怠る。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	文書管理	
上位所有者	文書管理	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 来歴に関する要件を十分に考慮した上で、方針や手続きの案を出すようにする。 ・ アーカイブ情報パッケージの出所やライフサイクル及びその情報パッケージに対して行われた全てのやり取りや操作を記録するための、方針や手続きの保持及び見直しを行う。 ・ ソフトウェアシステム、ハードウェアシステム及び保存戦略が、来歴情報の保持や記録を確実に行えるものであるようにする。 リスクが発現した場合： ・ 評判や信頼の低下を軽減するための方策を実行する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R60[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R71	
リスク名称	情報オブジェクトの検索不能	
リスクの説明	情報パッケージの検索をサポートするメタデータが不十分。	
このリスクは該当するか？	・ リポジトリは、対象となるユーザーコミュニティの規模の大きさに関わらず、検索用メタデータを利用可能にしているか？ ・ アーカイブコンテンツの検索に関して、ユーザーに提供されるフレキシビリティはどの程度か？ ・ 情報オブジェクトの検索に不可欠なシステムは何か？	
リスク発現例	・ 地球物理学データセンターにおいて、データセットの名前のみで検索をサポートするようにメタデータが記録されているが、対象となるユーザーコミュニティの研究者から、データ取得の物理的な場所や、使用された方法の名前によって検索を行いたいとの要望が出る。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	文書管理	
上位所有者	文書管理	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 指定されたユーザーコミュニティと協議の上で、検索システムや検索可能領域の規模に関する判断を下す。 ・ ユーザーコミュニティに対して、利用可能な情報検索システムに関する全体的な情報を伝達する。 リスクが発現した場合： ・ 把握されている欠陥に基づいて、情報検索の代替手段を導入する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R75[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R72	
リスク名称	見読性の定義が曖昧	
リスクの説明	リポジトリが、ステークホルダーとなるユーザーコミュニティからの期待や要望を考慮した上で見読性という言葉の意味を説明することが出来ない。	
このリスクは該当するか？	・ リポジトリは、ユーザーコミュニティからの期待や要望を考慮した上で見読性の定義付けを行っているか？	
リスク発現例	・ 必ずしも代表的といえないユーザーコミュニティからの要望に基づいて、情報とそれに関連するメタデータの保存が行われる。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	文書管理	
上位所有者	文書管理	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ ユーザーコミュニティの期待、要望、知識基盤を考慮した上で、見読性の概念の定義付け及び定期的見直しを行う。 ・ ユーザーコミュニティに対し、見読性の定義に関する情報を提供し、それに関する意見を求める。 リスクが発現した場合： ・ 事後に見読性の定義の詳細を示す方針を導入する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R73	
リスク名称	情報の意味的または技術的見読性における欠陥	
リスクの説明	情報の見読性を促進するための完全な表現情報を適切に保持することを、リポジトリが怠る。	
このリスクは該当するか？	・ リポジトリでは、ファイルフォーマット情報など、適切な表現情報の記録や参照が行われているか？ ・ 最小限の不可欠な意味的または技術的メタデータを決定する際、見読性に関する要件は参照されているか？	
リスク発現例	・ 社会科学データを保存しているリポジトリにおいて、多くの保有コンテンツのエンコードが行われているSPSSフォーマットに関する情報が記録されているが、これらのファイル全体にわたってフィールド見出しとして使用されている頭字語の意味が記録されていない。	
リスクの性質	物理的環境	
	人事、経営、及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェア、または通信機器・設備	
所有者	文書管理	
上位所有者	文書管理	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 見読性に関するユーザーコミュニティの要請を考慮に入れて、ファイルフォーマット情報など、適切な表現情報の記録・参照を行う。 ・ 保存情報の見読性がどの程度維持されているかについて、ユーザーコミュニティの意見を求める。	
リスクの関係	→R01[連鎖的] →R02[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

7.3.8. アクセス及び提供

リスク識別子	R74	
リスク名称	情報提供サービスが利用不能	
リスクの説明	リポジトリが、情報パッケージへのアクセス提供を行えない	
このリスクは該当するか？	・ 情報提供サービスには、どのようなシステムが必要か？ ・ リポジトリは、様々な代替的情報提供サービスを行っているか？ ・ 情報提供の手段を説明する方針及び手続きは定められているか？	
リスク発現例	・ ネットワークサービスの障害により、資料提供において依存しているウェブサーバーがオフラインとなる。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	提供	
上位所有者	提供	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 利用可能な情報提供サービスを説明する方針を明確化し、その方針をユーザーコミュニティに伝達する。 ・ 情報提供の方針で定められる要件を満たすために、適切なシステムを導入する。 ・ 提案される情報提供サービスに関する要件を満たすために、十分に堅固な技術的インフラを構築する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R75	
リスク名称	認証サブシステムの障害	
リスクの説明	不十分な情報アクセス制限システムにより、不適切なアクセスやアクセス失敗が起きる。	
このリスクは該当するか？	・ リポジトリは、契約または公的使命により、アーカイブ情報へのエンドユーザーのアクセスを制限する手段を構築し、維持する義務を負っているか？ ・ リポジトリの認証管理のオペレーションを維持するには、どのようなシステムが必要か？	
リスク発現例	・ コンテンツへのアクセス権を持っていない個人がアクセス出来るようになる。リポジトリシステムがIPベースの認証に依存しているが、X大学内の全てのユーザーがウェブプロキシを通じてウェブにアクセスしているため、その大学内からの全てのアクセスが１つのIPから来ているとアプリケーションが認識してしまい、学内に住む全てのユーザーがアクセスを得てしまう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	提供	
上位所有者	提供	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 認証に関する要件を説明する方針を、寄託契約に記載される条件及びその他の法律、規制または文脈上の定めに従って明確化する。 ・ 認証に関する方針の要件を満たせるように、適切なシステムを導入する。 ・ 提案される認証サービスで求められる条件を満たせるように、十分に堅固な技術的インフラを構築する。 リスクが発現した場合： ・ 認証の失敗の原因となった欠陥を究明し、修復する。 ・ システムが失敗を自己認識している場合、適切な反応を記述する方針を実施する（例：失敗の場合、全てのアクセスの試みを拒否する）。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R76	
リスク名称	権限付与サブシステムの障害	
リスクの説明	システム特権の適切な割り当てを確保するためのシステムが不十分で、ユーザーへの権限割り当てが不適当に行われる。	
このリスクは該当するか？	・ リポジトリは、契約または公的使命により、エンドユーザーによるアクセスを複数のレベルで定義し、管理する義務を負っているか？ ・ リポジトリの権限付与管理のオペレーションを維持するには、どのようなシステムが必要か？	
リスク発現例	・ ２人の異なるユーザーが同一のユーザーネーム文字列を使用することが許可されているため、データベースでのユーザーネーム検索を元に特権割り当てを行う権限付与システムが上手く機能しない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	提供	
上位所有者	提供	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 権限付与に関する要件を説明する方針を、寄託契約に記載される条件及びその他の法律、規制または文脈上の定めに従って明確化する。 ・ 権限付与に関する方針の要件を満たせるように、適切なシステムを導入する。 ・ 提案される権限付与サービスで求められる条件を満たせるように、十分に堅固な技術的インフラを構築する。 リスクが発現した場合： ・ 権限付与の失敗の原因となった欠陥を究明し、修復する。 ・ システムが失敗を自己認識している場合、適切な反応を記述する方針を実施する（例：失敗の場合、全てのユーザー特権を制限する）。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R79[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R77	
リスク名称	情報提供メカニズムの有効性を確認する能力の不足	
リスクの説明	全体的な事業目標の観点から、情報提供メカニズムがどの程度上手く機能しているのか、効果的に判断する能力がリポジトリに無い。	
このリスクは該当するか？	・ リポジトリにおいて、提供する情報の完全性、真正性、来歴及び見読性の確認と記録のための方針及び手続きは定められているか？ ・ リポジトリにおいて、使用権の決定及び不適切なアクセスの制限のための方針及び手続きは定められているか？ ・ 情報提供オペレーションの有効性を判断するためのシステムが定期的に活用されているか？	
リスク発現例	・ リポジトリがエンドユーザーの意見を求めるアンケートで、選択項目が限定的なため、情報提供の成功度が限定的にしか反映されない。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	X
所有者	提供	
上位所有者	提供	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ リスクマネジメントを含めた、内部評価の方法を確立する。 ・ 能力を証明するために、関連する認証を外部機関から取得することをめざす。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R19[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

リスク識別子	R78	
リスク名称	パフォーマンス水準やサービス水準の低下	
リスクの説明	事業目標に従ってサービス水準の目標を達成する能力が、リポジトリに無い。	
このリスクは該当するか？	・ リポジトリはステークホルダーに対して、最低限のパフォーマンスやサービスの提供を確約しているか？	
リスク発現例	・ リポジトリは、リクエストから５分以内に各オブジェクトを提供することを目指しているが、各オブジェクトの提供にいつも10分かかってしまう。	
リスクの性質	物理的環境	
	人事、経営及び管理の手法	X
	業務及びサービス提供	X
	ハードウェア、ソフトウェアまたは通信機器・設備	
所有者	提供	
上位所有者	提供	
ステークホルダー	経営者、出資者、スタッフ、コンテンツ提供者、ユーザー、生産者	
軽減方法	回避方法： ・ 現実的なサービス水準を定義し、その見直しや調整のための方針及び手続きを導入する。 ・ 資源を、事業の優先順位に基づいて確保・割り当てする。 ・ 目標の実現を確認するための方針及び手続きを定期的に見直し、必要に応じて調整するための機構を構築する。 リスクが発現した場合： ・ 障害の原因となった欠陥を究明するために、適切な内部調査を行い、結果に従って方針を改定する。	
リスクの関係	→R01[連鎖的] →R02[連鎖的] →R04[連鎖的]	
リスクの発現可能性	4	
リスクの潜在的影響	3	
リスクの深刻度	12	

7.4 付録4：監査報告書の予備的構造

前述のとおり、これは繰り返し提供されるツールキットの第1回目という意図である。いずれ第2版のDRAMBORAをオンラインツールとして公開し、それに引き続いて、ユーザーからのコメントや、DCC及びDPEがこのプロセスの一環として実行予定の監査を反映してツールを改善する際に、紙媒体及びオンラインの両方で改版することを予定している。

自己監査のオンラインバージョンの最後に自動的に生成される最終レポートには、監査人によって入力される情報のほとんどが含まれ、リポジトリの上級管理者が識別されたリスクに対して効果的な行動を開始する手助けとなる分析的材料によって強化される。

自動生成されるレポートは、言語、レイアウト及び組織上の詳細の点でさらなるフォーマット化と編集が必要になる。例えばレポートのある部分を含めるか含めないかというようなある程度のカスタマイズやテキスト情報の編集を許容するフォーマットで生成されるが、リスク値は編集のためロックされる。最終成果物はPDFフォーマットで出力される。

自動生成される自己監査レポートのセクションには以下が含まれる。

1) 表題紙

2) リポジトリの概要

3) リポジトリの目的及び公的使命

4) リポジトリの定められた目標及び目的

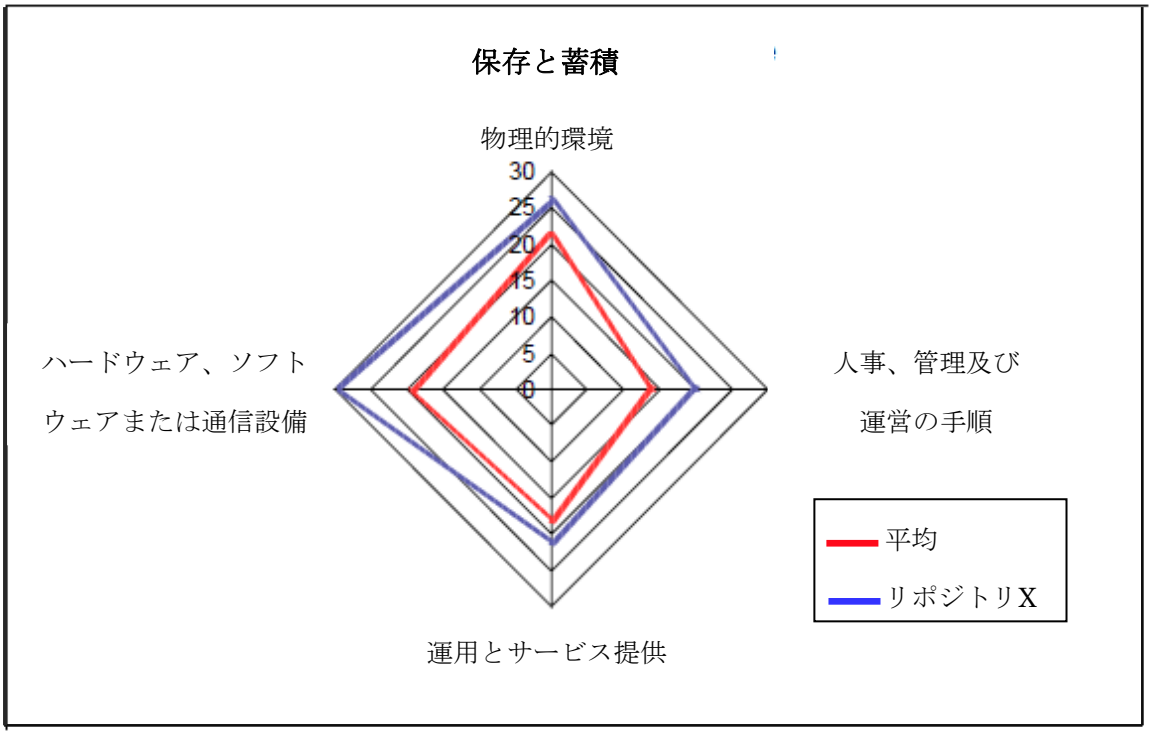
5) リポジトリのアクティビティ
定められた目的を達成するためにリスト化されたアクティビティ。理想的には、機能グループ別ないし監査人が選んだ他のパラメーターに応じてソートされる。

6) リポジトリのリスク登録簿
リスク登録簿は、監査人が選んだパラメーターに応じて順序付けされる。

7) 自己監査を行った類似のリポジトリの平均値とのリスク値の比較
結果は、以下のような表及び図の形式で表示される。

機能クラス	平均値	[リポジトリ名]
作業機能		
収集と受入	12	11
保存と蓄積	18	24
メタデータ管理	8	14

アクセスと提供	15	17
サポート機能		
組織と管理	9	6
スタッフの配置	20	18
財務管理	26	24
技術的インフラとセキュリティ	24	22



8) リスク管理タスク
リスクと、そのリスクを回避、緩和、転嫁または受け入れるための対策のリスト

9) 推奨
継続的なリスク管理行使、リスクの監視及びその合間に、自己監査を繰り返し行うことが推奨される。

7.5 付録5：頭字語と略語

AZ/NZS 4360	Australian and New Zealand standard for Risk Management （オーストラリア及びニュージーランドのリスク管理基準）
BASCS	Business Activity Structure Classification System

	（企業活動構造分類システム）
CASPAR	Cultural, Artistic and Scientific knowledge for Preservation, Access and Retrieval （保存、アクセス及び検索のための文化、芸術及び学術知識）
CCLRC	Council of the Central Laboratory of the Research Councils （研究会議中央研究所会議）
CCSDS	The Consultative Committee for Space Data Systems （宇宙データシステム諮問委員会）
CRL	Centre for Research Libraries （研究図書館センター）
DCC	Digital Curation Centre （デジタルキュレーションセンター）
DIRKS	Design and Implementation of Recordkeeping Systems （記録管理システムの設計と実施）
DPE	DigitalPreservationEurope （デジタルプリザベーションヨーロッパ）
DRAMBORA	Digital Repository Audit Method Based on Risk Assessment （リスク評価に基づくデジタルリポジトリ監査方法）
ERPANET	Electronic Resource Preservation and Access Network （電子資源保存アクセスネットワーク）
HATII	Humanities Advanced Technology and Information Institute （人文科学高等技術情報研究所）
InterPARES	The International Research on Permanent Authentic Records in Electronic Systems （電子システムにおける記録の永続的真正性に関する国際研究）
ISO 19011	*Guidelines for quality and/or environmental management systems auditing* （品質及び/または環境マネジメントシステム監査のための指針）
ISO 27001	Information technology – Security techniques – Information security management systems - Requirements（情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項）
JISC	Joint Information Systems Committee （情報システム合同委員会）
LOCKSS	Lots of Copies Keeps Stuff Safe （「LOCKSSプロジェクト」）
NARA	National Archives and Records Administration (USA) （米国国立公文書館）
nestor	Network of Expertise in long - term STOrage of digital Resources

	（デジタル資源の長期保存における専門知識のネットワーク）
OAIS	Open Archival Information System （オープンアーカイブ情報システム）
OCLC	Online Computer Library Centre （オンラインコンピューターライブラリーセンター）
RLG	Research Libraries Group （研究図書館グループ）
TRAC	Transparent Approach to Costing （経費透明手順）
UKOLN	UK Office for Library Networking （英国図書館ネットワーク局）
VRC	Virtual Remote Control （バーチャルリモートコントロール）

7.6 著者略歴

アンドリュー・マクヒューは2004年からDCCの諮問サービスマネージャーを務めており、世界有数のデジタルキュレーションの実務者のチームを率いて様々な問題に対し最新の専門的知識と見識を与えている。DCCにおける彼の最近の業績の中には、信頼性の高いリポジトリ監査と認証における業務を進めてきたことが挙げられる。マクヒューはまた、グラスゴー大学のコンピューティングサイエンス学部における情報技術の修士課程において、マルチメディアシステムとデザインの講義を担当している。

ライボ・ルーサレップは現在EUのデジタルプリザベーションヨーロッパ（DPE）プロジェクトのデジタルリポジトリ業務の監査及び認証に携わっている。オランダ国立公文書館及びエストニアンビジネスアーカイブに所属。歴史へのコンピューターの応用でロンドン大学から修士号を取得、10年以上デジタルアーカイブ及び電子記録管理の業務を担当している。

シェーマス・ロスはグラスゴー大学人文情報科学及びデジタルキュレーション教授並びに人文科学コンピューティング及び情報管理部長であり、自身が所長として創設されたHATII（人文科学高等技術情報研究所）を運営している。DCC副所長、DELOS最先端デジタル図書館ネットワーク学術委員会及び同デジタル保存クラスターのリーダーの一員、デジタルプリザベーションヨーロッパ（DPE）首席ディレクター。DPEの前身であるERPANETの首席ディレクターを務めた。

ハンス・ホフマンはオランダ国立公文書館のデジタル情報の永続性に関する相談役である。ERPANETの共同ディレクターを務めていた。メタデータ、デジタル保存及びオープンスタンダードに関する政府及び自治体レベルの様々な委員会に出席している。国際的な活動としては、Inter Pares 2研究プロジェクトの共同調査員及びオランダ国立公文書館代表、

2000年以降記録管理に関するISO TC46/SC11[27]のオランダ代表であり、同分科会の記録管理メタデータに関するワーキンググループの座長を務めている。DELOS NOEの保存クラスター、PLANETS、DPE等近年のヨーロッパでのプロジェクトに、オランダ国立公文書館代表として参加している。

7.7 付録6：参考資料（関連標準規格を含む）

7.7.1 デジタルリポジトリの監査と認証

Robin Dale, *Making Certification Real: Developing Methodology for Evaluating Repository Trustworthiness*. *RLG DigiNews*, Issue index: October 15, 2005, http://www.rlg.org/en/page.php?Page_ID=20793#article2

Deutsche Initiative für Netzwerkinformation E.V., Electronic Publishing Working Group, *DINI - Certificate Document and Publication Services. Draft Version*. (2007), http://www.dini.de/documents/DINI_certificate_eng_2006-10-12_draft.pdf

Susanne Dobratz, Astrid Schoger, *Digital Repository Certification: A Report from Germany. RLG DigiNews*, Issue index: October 15, 2005, http://www.rlg.org/en/page.php?Page_ID=20793#article3

ERPANET, *Workshop on Audit and Certification in Digital Preservation* (2004), http://www.erpanet.org/events/2004/antwerpen/index.php

nestor Working Group on Trusted Repositories Certification, *The Catalogue of Criteria for Trusted Digital Repositories . Version 1*. nestor Studies, no. 8 (2006), http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf

RLG/NARA Task Force, *An Audit Checklist for the Certification of Trusted Digital Repositories* (2005), http://www.rlg.org/en/pdfs/rlgnara-repositorieschecklist.pdf

RLG/OCLC Task Force, *Trusted Digital Repositories: Attributes and Responsibilities* (2002), http://www.rlg.org/legacy/longterm/repositories.pdf

Seamus Ross, Andrew McHugh, *Audit and Certification of Digital Repositories: Creating a Mandate for the Digital Curation Centre (DCC) . RLG DigiNews*, Issue index: October 15, 2005, http://www.rlg.org/en/page.php?Page_ID=20793#article1

[27] （訳注）国際標準化機構第46専門委員会（情報とドキュメンテーション）文書・記録管理分科会

Seamus Ross, Andrew McHugh, *The Role of Evidence in Establishing Trust in Repositories. D-Lib Magazine* , July/August, vol. 12, nos 7/8 (Also published in *Archivi e Computer*, August 2006), http://www.dlib.org/dlib/july06/ross/07ross.html

Seamus Ross, Andrew McHugh, *The Digital Curation Centre Repository Pilot Audits: Results and Lessons*, (forthcoming a).

Seamus Ross, Andrew McHugh, *Preservation Pressure Points: Evaluating Diverse Evidence for Risk Management*, (forthcoming b).

World Bank, *Assessment of Organisational Capacity to Manage Records: A Top Level Checklist* (2004), http://web.worldbank.org/WBSITE/EXTERNAL/EXTABOUTUS/EXTARCHIVES/0,,contentMDK:20035550~pagePK:36726~piPK:437378~theSitePK:29506,00.html

7.7.2 デジタルリポジトリ

Rachel Heery, Sheila Anderson, *Digital Repositories Review* (2005), http://www.jisc.ac.uk/uploaded_documents/digital-repositories-review-2005.pdf

Hans Hofman, Babak Hamidzadeh, Ken Hawkins, Bill Underwood, *Business-driven recordkeeping model. Version 5.0* (February 2007) (forthcoming by InterPARES-2)

National Council on Archives, *Your Data At Risk. Why you should be worried about preserving electronic records* (2005), http://www.ncaonline.org.uk/materials/yourdataatrisk.pdf

7.7.3 デジタル保存におけるリスク管理

Cornell University Library Virtual Remote Control (VRC) tool, http://irisresearch.library.cornell.edu/VRC/methods.html

ERPANET *Risk Communication Tool* (2003), http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf

JISC, *Managing Risk: a Model Business Preservation Strategy for Corporate Digital Assets* (2005), http://www.jisc.ac.uk/whatwedo/programmes/programme_preservation/programme_404/project_managingrisk.aspx

Gregory Lawrence, William Kehoe, Oya Rieger, William Walters, Anne Kenney, *Risk*

Management of Digital Information: A File Format Investigation. CLIR Report no. 93 (2000),
http://www.clir.org/pubs/reports/pub93/pub93.pdf

Victoria Lemieux, *Managing Risks for Records and Information*. ARMA International (2004).

Nancy McGovern, Anne Kenney, Richard Entlich, William Kehoe, Ellie Buckley, *Virtual Remote Control. Building a Preservation Risk Management Toolbox for Web Resources. D-Lib Magazine*, vol. 10, no. 4, April 2004,
http://www.dlib.org/dlib/april04/mcgovern/04mcgovern.html

Seamus Ross , *Uncertainty, Risk, Trust, and Digital Persistency*, 2006 NHPRC Electronic Records Research Fellowships' Symposium Lecture, University of North Carolina at Chapel Hill, 6 October 2006 [a pre-print of the lecture is available form the erpaeprints server].

7.7.4 リスクアセスメントと管理に関する文献

Institute of Risk Management, Association of Insurance and Risk Managers, ALARM (The National Forum for Risk Management in the Public Sector), *A Risk Management Standard* (2002),
http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

Institute of Internal Auditors, *Code of Ethics*,
http://www.iia.org.uk/cms/IIA/uploads/2c9103-ea9f7e9fbe--7f73/2002CodeofEthics2.pdf

Treasury Board of Canada, Integrated Risk Management Framework (2001),
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

UK Office of Government Commerce, *Successful Delivery Toolkit. Risk Management* (2005).

UK Treasury, *Orange Book. Management of Risk – Principles and Concepts* (2004),
http://www.hm-treasury.gov.uk/media/FE6/60/FE66035B-BCDC-D4B3-11057A7707D2521F.pdf

7.7.5 オペレーショナル・コンテクスト分析方法論

National Archives of Australia, *The DIRKS Manual: A Strategic Approach to Managing Business Information* (2003),

http://www.naa.gov.au/recordkeeping/dirks/dirksman/dirks.html

Collections Canada, *Business Activity Structure Classification System (BASCS) Guidance*,
http://www.collectionscanada.ca/information-management/002/007002-2089-e.html

7.7.6 標準規格

AS/NZS 4360:2004 *Risk Management,*
HB 436:2004 *Risk Management Guidelines – Companion to AS/NZS 4360:2004.*
Cf. http://www.riskmanagement.com.au/

BS 7799-3:2006 *Information security management systems – Part 3: Guidelines for information security risk management.*

BS 25999-1:2006 *Business continuity management – Part 1: Code of practice.*

ISO/IEC Guide 73:2002 *Risk management – Vocabulary – Guidelines for use in standards*

ISO/IEC 13335-1:2004 *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*

ISO 9001:2000 *Quality management systems – Requirements.*

ISO 14721:2003 *Space data and information transfer systems -- Open archival information system -- Reference model*

ISO 15489:2001 *Information and Documentation – Records Management. Part 1 & 2.*

ISO 17799:2005 *Information technology – Security techniques – Code of practice for information security management.*

ISO 19011:2002 *Guidelines for quality and/or environmental management systems auditing.*

ISO 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements.*

7.7.7 関連プロジェクト

Certification of Digital Archives Project, Center for Research Libraries (CRL) http://www.crl.edu and http://www.crl.edu/content.asp?l1=13&l2=58&l3=142

Digital Curation Centre (DCC), http://www.dcc.ac.uk/

DigitalPreservationEurope (DPE), http://www.digitalpreservationeurope.eu/

Digital Repository Infrastructure Vision for European Research (DRIVER), http://www.driver-repository.eu/

nestor Working Group on Trusted Repositories Certification, http://nestor.cms.hu-berlin.de/tiki/tiki-index.php?page=wg-repositories

RLG, Digital Repository Certification, http://www.rlg.org/en/page.php?Page_ID=580&projGo.x=33&projGo.y=12