SNIA
Advancing storage & information technology

ストレージネットワーキング・
インダストリ・アソシエーション

ストレージセキュリティ：データ保護

テクニカル・ホワイトペーパー

2018 年 3 月

要約：*ISO/IEC 27040:2015 (Information technology – Security techniques – Storage security) 標準には、ストレージシステムとエコシステムを保護するための管理および手法に関する詳細な技術的ガイダンスが示されている。このホワイトペーパーでは、データ保護の概要とこの標準内の関連するガイダンスについて説明する。*

使用にあたって

SNIA では、本書の使用を個人に対しては個人的利用に限定して許可し、法人およびその他の事業主体に対しては社内利用（社内での複製、配布、および掲示を含む）に限定して許可する。ただし、次の要件が満たされていることを前提とする。

1. テキスト、図、チャート、表、または定義を複製する場合は、変更を加えずに全体を複製すること

2. 本書からの資料（または本書の一部）を複製した印刷文書または電子文書は、その資料に対する SNIA の著作権を表示し、SNIA から再利用の許可を得ていることを明示すること

上記で明示的に規定されている場合を除き、本書の商業的利用、本書の一部または全部の販売、または本書の第三者への配布を行ってはならない。明示的に付与されていないすべての権利は、明示的に SNIA に留保されている。
上記以外の目的での本書の使用の許可は、tcmd@snia.org に電子メールを送付して要請する。要請する個人および／または法人の識別情報と、要請する使用の目的、性質、および範囲の簡単な説明を含めること。

この SNIA 文書内のすべてのコード、スクリプト、データ・テーブル、およびサンプル・コードは、次のライセンスに基づいて利用できる。

3 条項 BSD ソフトウェア・ライセンス

Copyright © 2018、ストレージネットワーキング・インダストリ・アソシエーション

ソース形式かバイナリ形式か、変更するかしないかを問わず、以下の条件を満たす場合に限り、再頒布および使用が許可される。

* ソース・コードを再頒布する場合、上記の著作権表示、本条件一覧、および下記免責条項を含めること。

* バイナリ形式で再頒布する場合、頒布物に付属のドキュメントなどの資料に、上記の著作権表示、本条件一覧、および下記免責条項を含めること。

* 書面による特別な事前の許可なしに、本ソフトウェアから派生した製品の宣伝または販売促進に、ストレージネットワーキング・インダストリ・アソシエーション（SNIA）の名前またはコントリビューターの名前を使用してはならない。

本ソフトウェアは、著作権者およびコントリビューターによって「現状のまま」提供されており、明示黙示を問わず、商品性および特定の目的に対する適合性に関する暗黙の保証も含め、またそれに限定されない、いかなる保証も行われない。著作権者もコントリビューターも、事由のいかんを問わず、損害発生の原因いかんを問わず、かつ責任の根拠が契約であるか厳格責任であるか（過失その他の）不法行為であるかを問わず、仮にそのような損害が発生する可能性を知らされていたとしても、本ソフトウェアの使用によって発生した（代替品または代用サービスの調達、使用の喪失、データの喪失、利益の喪失、業務の中断も含め、またそれらに限定されない）直接損害、間接損害、偶発的な損害、特別損害、懲罰的損害、または結果損害について、一切責任を負わない。

免責事項

この文書に含まれる情報は、事前の通知なく変更される場合がある。SNIA はこの仕様書に関していかなる種類の保証も行わない。これには商品性および特定の目的に対する適合性の暗黙的保証が含まれるが、これらに限定されない。SNIA は、本書に含まれる誤りあるいはこの仕様書の交付、履行、または使用に関連した偶発的または結果的損害に対して責任を負わない。

改訂に関する提案は、http://www.snia.org/feedback/まで。

Revision History

Revision	Date	Sections	Originator:	Comments
V0.1	*9/13/2015*	All	Eric Hibbard	Initial Draft
V0.2	*12/14/2015*	All	Eric Hibbard	Incorporation of ISO/IEC 27040 summary
V0.3	*7/17/2017*	All	Eric Hibbard	Alignment with DPCO whitepaper and initial draft of SNIA elements
V0.4	*10/10/2017*	4	Eric Hibbard	Data classification, data authenticity, due care, and retention/disposition
V0.5	*12/18/2017*	4	Eric Hibbard	Retention separated and expanded
V0.6	*1/9/2018*	4	Eric Hibbard	Retention and preservation; archives
V0.7	*1/29/2018*	All	Eric Hibbard	Review draft
V1.0	*2/20/2018*	All	Eric Hibbard	Final Approval Draft (for ballot)
V1.1	*3/6/2018*	All	Eric Hibbard	TC Approval Draft
V1.1	*3/8/2018*	All	Arnold Jones	Approved by SNIA Technical Council

Suggestion for changes or modifications to this document should be submitted at http://www.snia.org/feedback/.

Foreword

This is one of a series of whitepapers prepared by the SNIA Security Technical Working Group to provide an introduction and overview of important topics in ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security*. While not intended to replace this standard, they provide additional explanations and guidance beyond that found in the actual standard.

目次

要旨

データ保護は、業界の要件（ストレージ、セキュリティ、プライバシーなど）によって意味が異なる場合があるストレージセキュリティの必須要素である。このことは ISO/IEC 27040（Storage security）標準に記載されている。この標準では、データ保護が直接取り上げられていないが、関連するセキュリティ規制が規定されている。データ保護の認識を高めるために、このホワイトペーパーでは、ISO/IEC 27040 内の関連するデータ保護ガイダンスの概要を示し、それを踏まえて、データ分類、保有と保管、データ認証性、データ廃棄などのテーマについて説明する。この補足資料の一部として、既存のストレージセキュリティ標準を補完するガイダンスと考慮事項を示す。

1 はじめに

ストレージセキュリティは、ストレージシステムとインフラストラクチャだけでなく、それらに保存されたデータも保護するための物理的、技術的、および管理的規制の適用に関係する。ISO/IEC 27040:2015（*Information technology – Security techniques – Storage security*）標準（以下、ISO/IEC 27040 と表記）は、データ保護に特化されたものを含め、様々なストレージセキュリティ規制を規定している。

「データ保護」という用語は、分野によって意味合いが異なる場合がある。この曖昧さが深刻な誤解を生み、データ軽視につながることで、データ侵害（流出を伴う場合と伴わない場合）、金融債務、規制当局による調査などの厳しい事態を招くことがある。

このホワイトペーパーでは、データ保護の複数の側面を調査して、ISO/IEC 27040 内のデータ保護ガイダンスを要約し、SNIA の追加的推奨事項を示す。

2 データ保護の側面

このセクションでは、ストレージ、情報保証／セキュリティ、プライバシーといった 3 つの異なるデータ保護の視点を調査する。データ保護の各側面について簡単に説明して相違点や類似点を確認する。

2.1 ストレージ

2017 SNIA 辞書は、次のようにデータ保護を定義している。

> *［データ管理］データが破壊されておらず、許可された目的のためにのみアクセスでき、適合する規則を順守[1]しているという保証[2]。*

[1] SNIA 辞書では「コンプライアンス」が次のように定義されている。「1.［一般］標準規格、仕様、または明確に定義された要件に従っている状態。2.［法律］法的要件に従っている状態。」

[2] SNIA 辞書では「保証」が次のように定義されている。「［データ・セキュリティ］IT 製品またはシステムのセキュリティに関する目的および目標が持続的に達成されていることを証明するプロセス。」

SNIA のデータ保護の分類[3]は、次のようにデータ保護を説明することにより、この定義を明確化している。

> *データ保護は、データが破壊されておらず、許可された目的のためにのみアクセスでき、適合する規則を順守しているという保証を意味する。保護されたデータは、意図された目的にしか使用できないようにする必要がある。有用性を実現するためには、データ完全性、用途一貫性、バージョン管理、受け入れ可能な性能を提供するための手順の実行を必要とすることがある。*
>
> *このデータ保護の定義は、データが利用可能であると想定される期間のうちで、アプリケーションからそのデータをアクセスできる時間の総和として定義されるデータ可用性の概念の範囲を超えている。受け入れ難い性能は、アプリケーションや関連データへのアクセスが事実上不可能なレベルにまで生産性を低下させる可能性がある。データ・セキュリティとコンプライアンスの問題が密接に関係していることにも注意されたい。これは、データ保護の最終目標が、ビジネスの価値とアジリティを高めながら、リスク、コスト、およびダウンタイムを削減することだからである。*

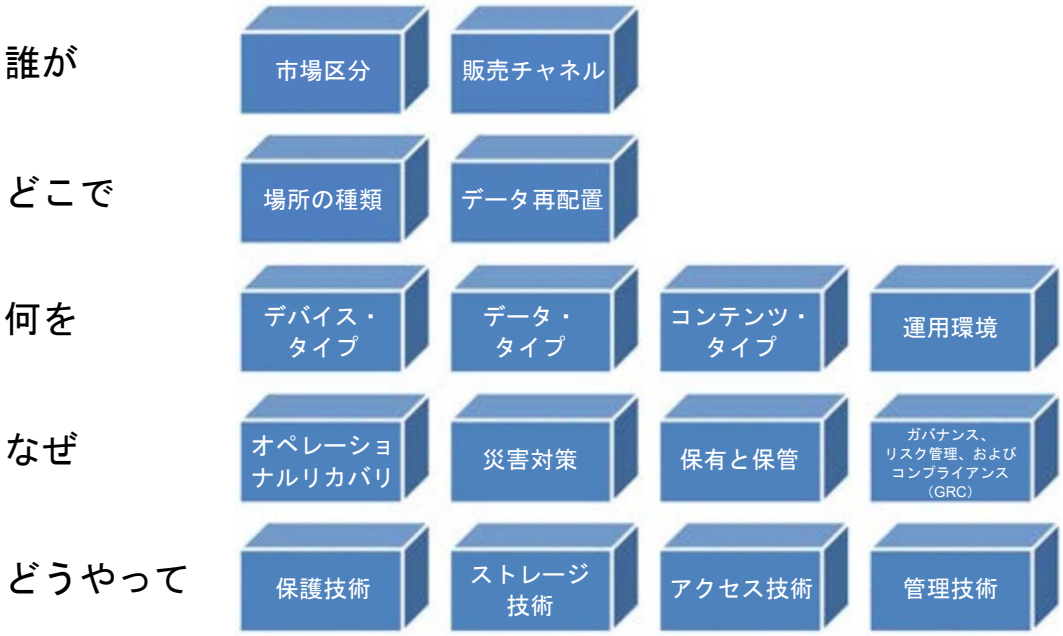

図 1.　データ保護の分類

図 1 は、データ保護の分類の高次元での概要を示している。それぞれの箱がデータ保護ソリューションをのぞくための個別のレンズを表している。各レンズは、他のすべてのレンズから独立している。これらのレンズの多くが相関関係にあり、分類によってそうした関係の調査が容易になる。

図 1 の横列は、誰が、どこで、何を、なぜ、どうやってという特定の質問を示している。各レンズは単純明快な概念を表しており、高次元のカテゴリとそのサブカテゴリの両方で不必要な専門用語の使用が避けられている。

---

[3] SNIA データ保護および容量最適化委員会ホワイトペーパー「A Data Protection Taxonomy（データ保護の分類）」2010 年 6 月

ホワイトペーパー「SNIA Data Protection Best Practices（SNIA データ保護ベスト・プラクティス）[4]」は、SNIA のデータ保護および容量最適化（DPCO）委員会によって定義されたデータ保護に関するベスト・プラクティスに関する SNIA の立場を文書化することにより、分類をさらに詳しく解説している。これらのデータ保護に関するベスト・プラクティスは、次の推進要因別に整理されている。

1. データ破損／データ喪失
2. アクセス可能性／可用性
3. コンプライアンス

DPCO は、各推進要因に関連付けられたデータ保護技術を規定し、適切な既存の標準（該当する場合）を参照し、最終的に各データ保護技術のためのベスト・プラクティスを推奨している。前述したように、このような推進要因のうち、コンプライアンス推進要因がこのホワイトペーパーの内容に最も密接に関係している。

2.2 プライバシー

International Association of Privacy Professionals（IAPP）用語集[5]は、次の関連定義を与えた。

> **プライバシー**：***状況に応じた個人情報の適切な使用。*** 何が適切かは、状況、法律、個人の想定だけでなく、情報の収集、使用、開示を制御する個人の権利によっても異なる。
>
> **データ保護**：***個人情報の管理。*** 米国では、「プライバシー」は、ポリシー、法律、および規制で使用される用語である。しかし、欧州と他の国々では、「データ保護」という用語は、プライバシー関連の法律や規制を意味することが多い。

最新の Web 版の IAPP 用語集でこの両方の用語が削除されているのは注目に値する。

2.3 情報保証／セキュリティ

データ保護のストレージの観点とは対照的に、情報セキュリティ[6]はデータの機密性、完全性、および可用性に焦点を当てる傾向がある。例えば、ISO/IEC 2382:2015（*Information technology -- Vocabulary*）は、データ保護を次のように定義している。

---

4 ホワイトペーパー「SNIA Data Protection Best Practices（SNIA データ保護ベスト・プラクティス）」、SNIA データ保護および容量最適化（DPCO）委員会、2017 年 10 月

5 International Association of Privacy Professionals (IAPP)。IAPP Information Privacy Certification Glossary of Common Privacy Terminology。2011 年。「CIPP Glossary of Terms」として掲載されている Web PDF ファイル（https://iapp.org/media/pdf/certification/CIPP_Glossary_0211updated.pdf）。

6 **情報セキュリティ**：機密性、完全性、および可用性を提供するための、情報および情報システムへの無許可のアクセス、使用、開示、中断、変更、または破壊からの保護。（出典：SP 800-37、SP 800-53、SP 800-53A、SP 800-18、SP 800-60、CNSSI-4009、FIPS 200、FIPS 199、合衆国法典第 44 編第 3542 条）

無許可の意図的または偶発的開示、変更、または破壊からデータを保護する適切な管理的、技術的、または物理的手段の実装

この定義は、基本的に、1993 年（ISO/IEC 2382-1:1993）以降変更されていない。

情報保証[7]は、情報依存性要素を追加することによって情報セキュリティ要素を拡張したものである（図 2 を参照）。

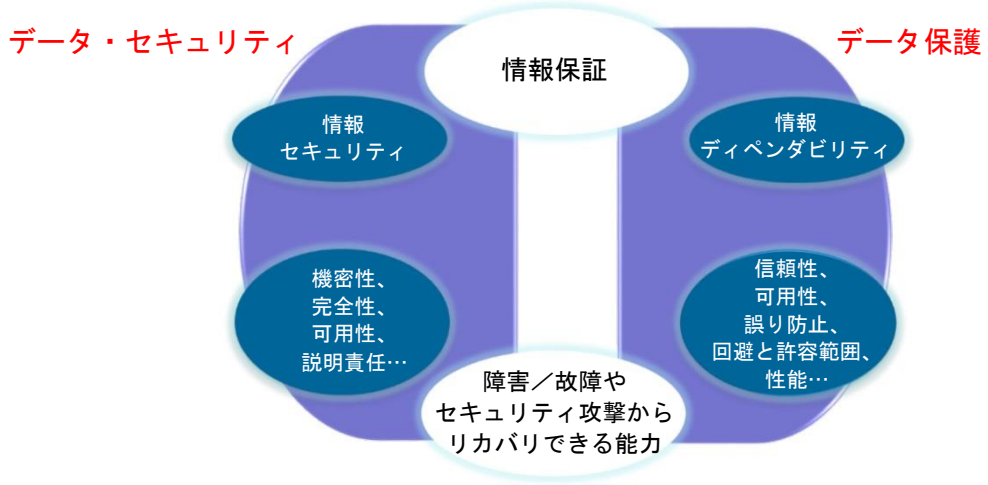

図 2.　情報保証：セキュリティとディペンダビリティの相互作用[8]

ディペンダビリティ（総合信頼性）[9]は、主に、以下の手段を通して、故障時にも指定されたサービスを提供するシステムの能力をいかに定量的に表現するかに主眼が置かれている。

- 信頼性（システムが指定された期間を通してサービスを提供する確率）
- 可用性（システムが指定された期間内に意図された目的のために使用可能な時間の割合）
- 安全性（システムが重大な損害をもたらすような故障を起こさない可能性）
- 実行可能性（故障時のシステムの性能レベルを定量的に測定）

ディペンダビリティのコミュニティとセキュリティのコミュニティが別々のものとして存在しているにもかかわらず、両者の相互作用が望ましいと認識されていることは注目に値する。この 2 つの領域のよく引き合いに出される明確な違いは、ディペンダビリティが主に悪意のないシステム内の障害やエラー（主に耐障害性設計が原因）に焦点を置いているのに対して、セキュリティは主にその目的に反する悪意のある試みに対

7　**情報保証**：可用性、完全性、認証性、機密性、および否認防止を保証することによって情報と情報システムを保護および防御する手段。このような手段には、保護、検出、および対処機能を組み込むことによる情報システムの復元の提供が含まれる。（出典：SP 800-59、CNSSI-4009）

8　図は、『*Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, New York, ISBN: 978-0-12-373566-9』の「Information assurance: Interaction between security and dependability」の図に基づく。

9　（SNIA 日本支部による脚注）**総合信頼性**：Dependability の日本語訳として、JIS Z 8115:2019 に準拠する形で併記した。

する保護に焦点を置いている点である。実際には、この把握されている違いは正確ではない。なぜなら、2 つのコミュニティにはかなりの重複部分と相乗効果が見られるが、それらが必ずしも認識されていないからである。

3 ISO/IEC 27040 データ保護ガイダンス

ISO/IEC 27040 では、データ保護の概念が明示的に取り上げられていない。とは言うものの、SNIA が公開している ISO/IEC 27040 目録[10]を参照することによって、この標準のデータ保護に関するガイダンスに対する何らかの洞察が得られる[11]。

ISO/IEC 27040 データ保護規制は、データの信頼性、可用性、および回復力の保証に使用されるバックアップ／リカバリ・システム、継続的データ保護（CDP）、およびレプリケーション技術に関連する。この標準では、すべてのデータ保護ソリューションをデータ回復力メカニズムとして見なすべきだということも強調されている。この焦点は、プライバシーや情報保証の観点よりもデータ保護の保管の観点により密接に関係している。

このセクションの後半では、データ保護に関連付けられた ISO/IEC 27040 ガイダンスの概要と、その他の関連領域（災害対策や事業継続など）の規制について説明する。

3.1 バックアップの安全化

ISO/IEC 27002:2013 の「運用セキュリティ」では、バックアップの目的は、「データの喪失に対して保護すること」としている。また、規定された規制は「情報、ソフトウェア、およびシステム・イメージのバックアップコピーを合意されたバックアップポリシーに従って定期的に作成してテストする必要がある」となっている。さらに、ISO/IEC 27002 は、次のような実装ガイダンスを与えている。

- 情報、ソフトウェア、およびシステムのバックアップに関する組織の要件を定義したバックアップポリシーを制定する必要がある。このポリシーでは、保有と保護の要件を定義する必要がある。
- 適切なバックアップ設備を設置して、災害や媒体故障後に不可欠な情報とソフトウェアのすべてをリカバリできることを保証する必要がある。
- バックアップ計画では、バックアップコピーの記録と回復手順の文書化、バックアップの範囲（完全か差分かなど）と頻度、リモートの場所にあるストレージ、物理的保護と環境的保護の必要性、バックアップ媒体の定期テスト、およびバックアップの暗号化（機密性が重要な場合）を考慮する必要がある。
- 運用手順では、バックアップポリシーに従って、バックアップの実行をモニターし、スケジュールされたバックアップの不具合を解決して、バックアップの完全性を保証する必要がある。
- 個別のシステムやサービスのバックアップ体制は、定期的にテストして、事業継続計画の要件が満たされていることを保証する必要がある。重要なシステムやサービスの場合は、バックアッ

[10] ISO/IEC 27040 標準の発行に先立って、目録用のメタデータが除外され、発行された標準から目録が消去されている。

[11] ISO/IEC 27040 に関する SNIA 発行目録については、http://www.snia.org/securitytwg を参照のこと。

プ体制が災害発生時に完全なシステムを復旧するために必要なすべてのシステム情報、アプリケーション、およびデータをカバーしている必要がある。

- 不可欠なビジネス情報の保有期間は、アーカイブ・コピーを恒久的に保有する必要があるという要件を踏まえて決定する必要がある。

ISO/IEC 27040 は、以下の内容を参照するだけでなく、さらに詳しく解説することにより、上記推奨事項を活用している。

- バックアップ・システムとストレージ媒体は、無許可のアクセスに対して適切に保護される必要がある（媒体の暗号化やオペレーターの認証と承認など）。
- バックアップするデータ、特に、ビジネス／基幹業務データは、関連するデータ復元戦略に合わせてバックアップ・アプローチを調整する必要がある。
- ストレージ媒体は、必ず信頼された個人（ベンダーを含む）が取り扱う必要がある。この文脈での「信頼された」は身元調査に合格した個人や保証付きの個人を意味する。
- バックアップが実施されたことを示す監査証跡が必要なだけでなく、復元要件が満たされていることの「証拠」も必要である。

3.2 レプリケーションの保護

ISO/IEC 27002:2013 ではレプリケーションが明示的に取り上げられていないが、「情報セキュリティ継続性」(「冗長性」の下)の項で、「情報処理設備の可用性を保証すること」という目的と、「情報処理設備は可用性要件を満たすのに十分な冗長性を備えて実装される必要がある」という規制が示されている。この特定の実装ガイダンスの焦点は、実装されたフェイルオーバ・メカニズムの可用性とテストに関するビジネス要件の理解に置かれている。

データ可用性に関連する ISO/IEC 27040 のガイダンスには、以下の推奨事項が示されている。

- レプリケートするデータ、特に、事業/ミッションクリティカルデータの場合は、レプリケーション・アプローチは、そのデータに関連する信頼性、耐障害性、または性能の要件に合わせて調整される必要がある。
- レプリケーション・アプローチは、無許可のアクセスに対する適切な保護(移動中データの暗号化など)を提供する必要がある。

ISO/IEC 27040 の他のセクションでは、以下のガイダンスも与えられている。

- 圧縮と重複排除がリモート・レプリケーションに悪影響を及ぼさないように、注意する必要がある。
- プライマリ・ストレージ上で暗号化される機密データまたはビジネス/基幹業務データのレプリケーションは、レプリケート先のストレージ上でも暗号化する必要がある。
- 暗号化されたデータ(暗号文)のレプリケーションでは、特に、DR/BC ソリューション(リモート/地域外レプリケーション)の場合に、データ暗号鍵の追加の管理が必要なことがある。

3.3 継続的データ保護 (CDP) の確保

レプリケーションと同様に、ISO/IEC 27002:2013 は CDP を明示的に取り上げていない。しかし、ISO/IEC 27040 は、以下を取り上げている。

- CDP アプローチ(連続的、ほぼ連続的、定期的など)は、特に、事業/ミッションクリティカルデータと組み合わせて使用する場合に、関連する復元戦略に合わせて調整する必要がある。
- 高ネットワーク帯域幅シナリオ(マルチメディア・ファイルなど)では、日常業務に対する CDP の影響を軽減するために、ネットワーク・トラフィックに優先順位を付けるための帯域幅調整テクニックを採用するべきである。
- CDP アプローチでは、無許可のアクセスに対する適切な保護(移動中データや蓄積データの暗号化など)を提供する必要がある。

3.4 データ保護に関連した規制

ISO/IEC 27040 は、データ保護(ストレージの観点)に関連したその他の技術に関するガイダンスを包含している。これらは、事業継続管理ソリューションとデータ保有(アーカイブ)およびクラウド技術を含む。

3.4.1 事業継続管理

ISO/IEC 27002:2013 では、「情報セキュリティ継続を組織の事業継続管理システムに組み込むべきである」という 1 つの主要目標と共に、「事業継続管理の情報セキュリティの側面」が、ある 1 つの項全体を使って述べられている。この目的に関連付けられた規制は、以下を含む。

- 組織は、危機や災害などの困難な状況における情報セキュリティと情報セキュリティ管理の継続のための要件を特定する必要がある。
- 組織は、困難な状況における情報セキュリティの継続の必要なレベルを保証するためのプロセス、手順、および規制を設定、文書化、実装、および維持する必要がある。
- 組織は、確立し、実装した情報セキュリティ継続規制を定期的に検証し、それらが困難な状況でも有効で効果的なことを保証する必要がある。

また、ISO 22301[12]と ISO 22313[13]は、それぞれ、組織が事業継続ニーズを特定するための要件とガイダンスを与えている。さらに、ISO/IEC 27031[14]は、組織が、より大規模な事業継続を支持し、ICT 回復力とリカバリに関する要件を特定するためのガイダンスが示しているのに対して、新しい ISO/IEC 27036[15]多部構成標準は、サプライヤからの IT サービスの調達に関する様々なレベルのガイダンスを与えている。ISO/IEC 24762:2008[16]が取り下げられていることにも注意されたい。これは、既に関連文書ではなく、ISO/IEC 27036 に置き換えられているからである。

一般的に、ストレージは、典型的には、組織の ICT Readiness for Business Continuity（IRBC）プログラムまたは非公式の DR/BC 活動の重要な要素であるという認識に基づいて、ISO/IEC 27040 は以下の DR/BC に関連付けられたガイダンスを含んでいる。

- ストレージ・エコシステムが DR/BC の計画立案と実装に組み入れられていることを保証する。
- 限定的な中断イベント（システムの故障、敵対者の攻撃、オペレーターのエラー）に備える。
- ストレージ・エコシステムに関連付けられたスタッフ配置と設備に特有の要件を特定して文書化する。
- 継続的計画立案と想定の定期的テストを実施する（これは DR/BC の成功に不可欠である）。DR/BC テストの結果は DR/BC 計画の継続的保守にフィードバックされる必要がある。

---

12 『ISO 22301、*Societal security -- Business continuity management systems --- Requirements*』は、『ISO/TC 223、*Societal security*』によって策定されたものである。ISO 22301 は、事業継続マネジメントの枠組みを定義した主要標準である。

13 『ISO 22313、*Societal security -- Business continuity management systems -- Guidance*』も ISO/TC 223 によって策定されたものである。ISO 22313 は、ISO 22301 の実装を支援する補助標準である。

14 『ISO/IEC 27031:2011、*Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity*』

15 『ISO/IEC 27036、*Information technology -- Security techniques -- Information security for supplier relationships*』は現在 4 部構成の標準である。

16 『ISO/IEC 24762:2008、*Information technology -- Security techniques -- Guidelines for information and communication technology disaster recovery services*』

3.4.2 データ保持（アーカイブ）

ISO/IEC 27040 は、1) 短期～中期（10 年未満）と 2) 長期の 2 つの異なる観点からデータ保有を取り上げている。短期～中期の保有促進要因は、法律、規制、または法令の要件（セキュリティ規定も含む）に基づくことが多い。これらの要件を満たせなかった場合は、組織に対して重大な責任が問われることがある。

長期アーカイブ・ストレージシステムは、通常、非アーカイブ・ストレージシステムには存在しない完全性、認証、およびプライバシーの脅威をもたらす。また、データの保存期間が長いほど、攻撃者がセキュリティ・システムへの侵入を試みる時間が増えることになる。アーカイブ・ストレージでは、攻撃者は何十年という時間を攻撃に費やすことができる（スロー攻撃）。このような問題を解決するために、ISO/IEC 27040 は、以下を推奨している。

- アーカイブ・ストレージは、1 回だけ書き込んでたまに読み取る[17]アクセス・パターンを前提としているため、読み取りを待つのではなく、システム内のデータの完全性を定期的かつ積極的にチェックする必要がある。
- アーカイブ・データをより新しいストレージ技術に移行する場合は、新しい場所でデータをより適切に保護するための高度なセキュリティ対策を提供可能なセキュリティ機能を導入する。
- 長期アーカイブ内のデータは、データ管理者より長く保持される可能性があるため、安全なアーカイブ・ストレージシステムで新しいユーザを認証し、既存のユーザに付属するリソースとの関係を構築できる必要がある。
- 秘密保持メカニズム（暗号化や秘密分散など）は、データを書き込んだユーザが不在でも機能する必要がある（例えば、データを読み取る権限が付与された新しいユーザにはデータを復号できる能力も付与する必要がある）。
- セキュリティ・ログは、スロー攻撃の検出を支援できるように、また、データ保護の調整に関する決定を下すために使用可能な攻撃履歴を保持できるように、十分完全で長期保存される（10 年単位で）必要がある。
- システムは、あらゆる侵害に即座に対処するか、是正措置をインテリジェントにスケジュールするために侵害の履歴を保持する必要がある。
- データ削減技術（圧縮や重複排除など）は、データ完全性の侵害を回避する方法で（データ削減技術との関連性がないコピーに含まれるなど）使用する必要がある。

短期～中期の保有期間中のデジタル情報の確実な保有を保証するには、保有されている情報の価値、すべての要因からの損失のリスク、および保有期間中の受け入れ可能な損失量に見合うデータ保護、災害対策、およびデジタル保管およびキュレーションの慣行を使用する必要がある。ストレージの観点から、このような短期～中期のデータ保有シナリオは、通常、1 世代以上の技術に及び、関連するメタデータの収集と保有を必要とする。短期～中期の保有に関する留意点を以下に示す。

---

[17] アーカイブに記録されたデータの大部分は一度もアクセスされないという事実を強調するために、この標準では、この用語が使用されている。

- 複数のデータの物理または論理レプリカを作成して保存する必要がある[18]。レプリカはできるだけ独立した状態で整理（地理的位置、管理／経営上、プラットフォーム／オペレーティング・システムなど）し、その数はデータの価値とリスクの許容範囲に基づいて選択する必要がある。
- 定義したスケジュールに基づいて監査を実施し、明らかな障害や潜在的な障害がないか、またそれが引き起こした被害について、テスト（完全性チェックなど）する必要がある。破損したデータは、被害が拡大する前に他のレプリカ内の正常なデータを使用して修復する。
- アクセス制御方式を、保存している情報向けの法律や規制の要件に合わせる。
- 説明責任対策と追跡可能性対策が適切で機能していることを保証する。すべてのデータ・アクセスが、監査ログエントリを必要とする場合がある。
- 特に証拠になりそうなデータについて、データの信憑性、出所、および生産物流管理を実証するメカニズムを実装する。
- 暗号化が使用されている場合は、鍵と鍵材料をアーカイブ／エスクローする。推奨されている暗号期間内にまたは基礎となる暗号アルゴリズムを交換する必要がある時には、鍵を変更し暗号化し直す。

3.4.3 クラウド・コンピューティング

専用と標準ベースの両方のクラウド・コンピューティング・ストレージ製品が使用されており、一般的に、コピー機能（システム上のストレージの一部または全部のミラー化など）、バックアップおよびリカバリ機能、長期保有機能（アーカイブなど）、およびマルチシステム同期機能（ユーザに複数の（場合によっては多様な）種類のデバイス上でのデータを同期させることを許可するなど）が提供されている。ISO/IEC 27040は、次のクラウドストレージに関するガイダンスを示している。

- IPsec やトランスポート層セキュリティ（TLS）などのトランスポート・セキュリティが、すべてのトランザクションに対して使用されるべきである。
- 機密データがサードパーティ・クラウド環境に保存されている場合は、無許可の関係者（クラウド・サービス・プロバイダの担当者、他のテナント、敵対者など）によるアクセスを阻止するために、蓄積データの暗号化と適切な鍵管理のプロセスが使用されるべきである。
- ユーザ登録はセキュリティを確保して処理し、データへのアクセスを保護するために、強力なパスワード認証が使用されるべきである。
- データへのアクセスが許可されたユーザに適切なアクセス特権を付与しながら、他のテナントからの無許可アクセスをガードするアクセス制御が使用されるべきである。
- クラウド・コンピューティング・ストレージから機密データをクリアする場合は、サニタイズ機能が使用されるべきである。

[18] コピー数には全く関係なく、むしろ、デジタル・アーカイブ・プロセスの品質や特徴に関係する。

ISO/IEC 27040 は、SNIA クラウドデータ管理インターフェイス(CDMI)[19]の実装と使用に関する追加の特定のガイダンスを与えている。

4 SNIA データ保護ガイダンス

4.1 データの機密性

ISO/IEC 27000 は、機密性を、「情報が無許可の個人、事業体、またはプロセスに公開または開示されない特性」と定義している。ISO/IEC 27040 は、「ストレージ・インフラストラクチャ内では、データの機密性は、通常何らかの暗号化方式を使用して保たれる。このような方式は、ほとんどの場合、ストレージ・インフラストラクチャ内で転送中(伝送中または移動中とも言う)のデータ、あるいは、デバイス内またはストレージ媒体上に保存(または蓄積)された状態のデータの保護に関連する」ということを指摘している。ホワイトペーパー「SNIA Storage Security: Encryption and Key Management(SNIA ストレージセキュリティ: 暗号化と鍵管理)」は、これらの概念の多くを取り上げ、ストレージに関するガイダンスを示している。

暗号メカニズムは機密性を提供する最も強力な方法の 1 つだが、データの機密性を保証するための追加のメカニズムが必要な場合もある。

- 認証プロセス
- 認可とアクセス制御
- データ分類とポリシー
- 管理の証明と監査ログ

データ保護の観点では、データの機密性の保持が個人データの保護の保証における最も重要な側面の 1 つである。

4.2 データ分類

ホワイトペーパー「SNIA Data Protection Best Practices(SNIA データ保護ベスト・プラクティス)」の機密性の説明では、実稼働と非実稼働の側面と機密と非機密の側面(表を参照)を比較した単純なデータ分類体系(図 3)が提案されている。実稼働システムは、セキュリティ要件や管理が厳しくない開発システムとは異なるセキュリティ領域として扱われることが多い。この状況は、この 2 つの環境の分離を奨励しているガイダンスが記載された ISO/IEC 27040 で認識されている。

重要性／優先順位	実稼働	非実稼働
機密	高	中
非機密	中	低

[19] SNIA テクニカル・ポジション:クラウドデータ管理インターフェイス(CDMI)v1.1.1、SNIA、2015 年 3 月、ISO/IEC 17826:2016 (SNIA) とも呼ばれる。情報技術 -- クラウドデータ管理インターフェイス(CDMI)

図 3.　DPCO 単純なデータ分類体系

この単純な体系を使用すれば、優先順位の基本セットまたは特定のデータの相対的重要性を設定できる。しかし、これは多くの組織には適さないかもしれない。「機密」はPIIが関係する規制要件（GDPRなど）に対応するためにサブカテゴリが必要な場合があり、ヘルスケアには PII の特別なバージョン（HIPAA/HiTECH など）がある場合があり、国家のセキュリティは別の次元のカテゴリを強制する。また、ISO/IEC 27040 は、データ分類のテーマを明示的に取り上げらていないが、データの機密性または重要度に焦点を当てることが、環境に必要なストレージセキュリティ制御（サニタイズ、アクセス制御、認証、暗号化、鍵管理など）を特定するための分析を組織が開始することを支援できることが提案されているのは注目に値する。

一般的な推奨事項として、SNIA では、できるだけ少ない数の機密性カテゴリを使用するように奨励している。しかし、これは組織的リスクの明確な理解に基づくべきである。

4.3 慎重評価／注意義務

多くの場合、個人データまたは PII（プライバシー）のデータ保護に関連する規制は、使用されなければならない特定のセキュリティ規制に関する詳細を含まない。代わりに、組織は、運用の状況に応じてリスクを抑制するための義務を満たすような、適切な技術的及び組織的対策を講じることを求められる。別の表現をすれば、組織は、規制違反を避けるための十分な注意と精査を実施しなければならない。

「セーフ・ハーバー」は存在しない以上、正しいことをやるしかない。その場合でも、データ漏洩は起きる可能性がある。

これらの概念の理解を深めるために、以下を考慮すること。

- ***デュー・ディリジェンス*** ― 関係する状況下で、合理的で慎重な人物から期待され、かつそのような人物によって通常発揮される慎重さ、責任、努力 の評価基準。［BusinessDictionary.com］法的要件を満たすことまたは義務を果たすことを追求している人物から合理的に期待され、かつ通常は発揮される、努力。［ブラック法律辞典（第 10 版、2014 年）］
- ***過失*** ― 関係する状況下で、合理的または慎重な人物が行うであろう他者への配慮を行うことを怠ること、またはそのような合理的な人物が行わないであろう行動を取ること。［law.com］
- ***配慮*** ― 職務または法的義務として当事者に要求される、考え得る危険、ミス、落とし穴、およびリスクの回避に向けられた積極的な気遣いまたは怠慢の欠如のレベル。*注意義務*と*配慮の義務*も参照のこと。［BusinessDictionary.com］*過失法*では、特定の状況で個人（または事業体）に要求される行為。［ブラック法律辞典（第 10 版、2014 年）］
- ***妥当な配慮*** ― 怠慢への責任の試金石としての、配慮の度合い。それは、同じ事業や企画に関わっている慎重で有能な人物が、同じような環境で行うと考えられるものである。一般的に、妥当な配慮は、人がニーズを満たすために有しているあらゆる知性や心遣いを適用することである。この用語は、常に相対的であり、特定の環境に依存する。あるケース（例えば、大人が関係する）では妥当な配慮とされるものが、別のケース（例えば、幼児が関係する）では重大な怠慢とされる場合がある。［ブラック法律辞典（第 10 版、2014 年）］
- ***配慮義務*** ― 自分自身の財産に関して、または問題となっている状況と似た状況において普通の合理的な人物が通常発揮するであろう*配慮*の度合い。*配慮義務*の概念は、*怠慢*に対する法的責任の試金石として使用される。［BusinessDictionary.com］
- ***配慮の標準*** ― *配慮義務*が課せられた個人に要求される慎重さや警戒の度合い。［メリアム・ウェブスター法律辞典。メリアム・ウェブスター。1996 年］過失法では、合理的な人物が行うであろう配慮の度合い。［ブラック法律辞典（第 10 版、2014 年）］

リスクにさらされていることを理解する基本的なステップを踏み損ねた場合や、特定されているリスクに対処しない場合は、注意義務やデュー ディリジェンスが欠如していることを示すことになる。これらは、深刻な悪い結果をもたらすことがある。必須の侵害通知[20]がなされなかった、または誤って処理された場合、特にデータ侵害が配慮義務やデュー ディリジェンスの欠如に起因している場合は、この状況は、さらに複雑になる可能性がある。

ストレージシステムやエコシステムは、このような概念が頻繁に適用される ICT インフラストラクチャの不可欠な部分であるが、この状況は、責任と説明義務を負っているストレージ・マネージャや管理者に理解されないかもしれない。こうした個人は、以下の点を認識することが重要である:

- 無許可の、偶発的な、または意図的な破損、変更、または破壊からデータを守るために、ストレージインフラストラクチャには、多くの場合保護が必要である。
- データ侵害に伴うリスクは組織によっては重大なものとなりうる。そこで、慎重さの姿勢として、それらの侵害を防ぐための SNIA ベスト・プラクティスや ISO/IEC 27040 内のガイダンスなどの合理的手段を使用することを指示する。
- 組織が法的義務を満たすためには、適切なデータ保管および廃棄活動（4.6 を参照）が必要である。
- ポリシーは、適切なデータハンドリングを促進するための重要な管理制御である。

4.4 保持と保管

「保持」と「保管」という用語は同義的に使用されたり、間違って使用されたりすることが多い。それによって、同じ情報がどのように保持されるか、それがどのくらい維持されなければならないか、それがどのように保護され安全に保たれるか、またそれが保護され安全に保たれるか否かということを支配する要件が異なったり、矛盾したりする。

ISO TR 18492:2005 は、電子文書ベースの情報が、日常の業務行為やイベントの「業務記憶」を構成し、事業体が後でそのような行為やイベントを審査、分析、または文書化できるようにすると記述している。このように、電子文書ベースの情報は、事業体が現在と将来の経営意思決定を支援すること、顧客を満足させること、規制順守を実現すること、不利な訴訟から身を守ることを可能にするような、商取引の証拠である。この目標を実現するには、電子文書ベースの情報が保有され、適切に保管される必要がある（例えば認証性を含む証拠要件への対応など）。

保管要件は、法律面（リーガルホールドなど）および／または有用性の面が関係することが多い。有用性保管は、データまたは情報のライフサイクルを通した読み取り、解釈、認証、保護、および損失に対する保護の能力が可能なことを保証するためのプロセスと運用に関係する[21]。有用性保管は、データの変換（旧式のワープロで作成されたファイルの変換や関連するエコシステムの保管など）を含む場合もある。

---

20 漏洩通知は、世界各地の多くのデータ保護規制の必須要素になっている。

21 「保管」の SNIA 定義。

組織は、何を記録し[22]、記録をどのように管理するか[23]を定義した記録管理ポリシーを制定する必要がある。また、組織は、その記録を記録系列に分類する保有スケジュールを立てる必要があり、これには保有期間とメタデータを関連付ける。組織の所有、監督、または管理下のすべての文書化された情報に記録ステータスが必要なわけでないことに注意することが重要である。代わりに、組織の事業運営に関する文書化された情報のうち、維持することが法的に求められているものや法令順守または事業上の価値を備えたもののみを記録すべきである。

任意の時点で、同じ情報が複数の「状態」で存在する可能性がある。この状態とは、物理的な場所や媒体ではなく、情報を維持する目的を意味する。このような様々な状態を認識することは、それらを記述するときに一貫した用語を使用することと同様に、該当する保有と保管に関する要件が特定されることを保証するために不可欠である。

4.4.1 一般データの保持

記録すべき品質を備えた情報は、記録の媒体（紙、デジタル・データ、マイクログラフィックスなど）に関係なく、保有スケジュールに従って通常の業務において保持される必要がある。保有期間は、ポリシーで成文化し、法的要件と法的考慮に基づくと同時に、情報の事業価値と事業ニーズを考慮することによって決定する必要がある。法令順守と事業考慮は、記録が保持される方法（保護される方法を含む）に影響する場合がある。また、通常の業務において、記録がスケジュールで指定された期間だけ保有されたら、その順守と事業価値の有効期限が切れるため、適切に廃棄される必要がある。保有スケジュールにデータ廃棄ポリシーを含めるのは矛盾するように思われるかもしれないが、すべてを持ち続ける組織は自組織をかなりのリスクにさらしている。

米国の少なくとも 1 つの法律事務所が、米国連邦制度と 50 州の法令と開示規制には 56,000 件を超える法的要件と法的考慮が含まれていると指摘している。

記録の保持に関する様々な要件を考えると、組織の記録を適切に保護するストレージ・インフラストラクチャを設計するのは困難である。米国の記録保持要件（表 1 を参照）の一部を抽出すれば、このような要件が「恒久的」保有と 10 年以下の「一時的」保有のどちらかに分類されることが分かる。

---

22 記録の定義の例：「記録は、通常の業務において作成または受信され、組織のポリシー、手順、活動、および決定の証拠となり、技術的、管理的、歴史的、および／または法律的価値を有することから、一時的または恒久的に、保管する価値がある任意の媒体内の文書資料として大まかに定義される。」

23 SNIA クラウドデータ管理インターフェイス（CDMI）仕様では、保有管理には、保有ポリシーの実装、特定の目的（訴訟など）のためのオブジェクトのホールドを可能にするホールドポリシーの定義、およびオブジェクトに保有ポリシーおよび／またはホールドを設定することによってオブジェクトの削除ルールが受ける影響の定義が含まれるとされている。

表 1.　文書の種類と最小保有期間[24]

文書の種類／内容	保有
定款、認可状、附属定款、議事録、およびその他の設立記録	恒久
著作権、商標、特許登録	恒久
証書、抵当、請求書	恒久
減価償却明細書	恒久
綱領、戦略計画	恒久
労災補償書類	最初の終了後 10 年
契約、抵当、手形、およびリース契約（期限が切れたもの）	7 年
株券と債券（キャンセルしたもの）	7 年
人事ファイル、退職した従業員	退職後 7 年
保険証券	失効後 3 年
顧客やベンダーとのやり取り	2 年
補助金（不採用）	1 年

ISO/IEC 27040 では、長期保有と短中期保有の観点からデータ保有（3.4.2 を参照）に言及している。後者は、伝統的なアーカイブ（10 年未満）より短い法律、規制、または法令の要件に左右される。短中期保有の証拠性は、セキュリティに影響する可能性のある注目すべき違いと見なされる。

4.4.2 アーカイブ

ISO 14721 では、「アーカイブ」という用語は様々な保存と保管の機能とシステムを参照するために使用されるようになったことに加えて、伝統的なアーカイブは、元々、公的または私的コミュニティがアクセスするために、政府組織、公共団体、または民間企業によってまたはそれらのために生成された記録を保管する設備または組織として理解されていることが指摘されている。アーカイブは、記録の所有権を取得して、アクセスするコミュニティが理解可能なことを保証し、情報の内容と認証性を保存するように管理することによって、このタスクを完遂している。

ホワイトペーパー「SNIA Data Protection Best Practices（SNIA データ保護ベスト・プラクティス）」では、アーカイブは、公式のデータの作業コピーを表すが、長期保管やコスト削減などの目的のために、よりアクティブな実稼働データとは別に管理されるデータ・オブジェクトのコレクションとして特徴付けられている。また、アーカイブは、特定の規制および／または法的／契約義務を満たす必要があるデータ・セットの保存に使用されることが多く、通常は、アプリケーションの復元よりも監査や分析のために使用される。また、こ

[24] 『*Records Retention and Disposition Guidelines*』Rockefeller Archive Center の Collaborative Electronic Records Project 作成、2008 年 11 月改訂

のホワイトペーパーでは、保有要件の違い（短期、中期、長期など）にかかわらず、アーカイブは、適切な完全性、不変性、認証性、機密性、および出所を保証する必要があることが言及されている。

ISO TR 18492:2005 は、「長期保管」が「電子文書ベースの情報がアクセス可能で真正の証拠として保持される期間」として定義し、さらに次のように言及している。

> *この期間は、組織のニーズと要件に応じて、数年から数百年の範囲で異なることがある。組織によっては、この期間が規制順守、法的要件、および事業ニーズに基づいて決定される場合がある。公的記録を保持するアーカイブ・リポジトリなどのその他の組織では、通常、電子文書ベースの情報を保有することが必要な期間が数百年と見なされる。*

ISO TR 18492:2005 では、ストレージ・リポジトリで長期保管戦略を策定するときに考慮すべき 6 つの重要な問題も規定されている。

- *読み取り可能な電子文書ベースの情報* ― 電子文書ベースの情報を構成するビット・ストリームは、それを最初に作成し、現在それを保存し、それにアクセスし、今後それを保存するために使用される予定のコンピュータ・システムまたはデバイス上でアクセス可能になっている必要がある。媒体陳腐化とデータ書式も考慮事項である。
- *判読可能な電子文書ベースの情報* ― 電子文書ベースの情報の判読可能性は、実際にビット・ストリームが何を表しているかに関する情報と、その情報に基づいて適切なアクションを実行する処理ソフトウェアの能力に左右される。
- *識別可能な電子文書ベースの情報* ― 文書ベースの情報は、ユーザと情報システムが名前や ID 番号などの一意の属性に基づいて情報オブジェクトを区別できるような方法で整理、分類、および記述する必要がある。検索および読み出しを容易にすることも考慮事項である。
- *読み出し可能な文書ベースの情報* ― 個別の情報オブジェクト（またはその一部）は読み出して表示することができる。一般に、読み出し可能性は、情報オブジェクト（データ・フィールドやテキスト文字列など）の論理構造を物理的な保存場所にリンクするキーまたはポインタが必要な点でソフトウェア依存である。
- *理解可能な文書ベースの情報* ― 作成や使用の状況（メタデータ）や他の文書との関係など、文書の内容を超えた情報をコンピュータと人間の両方に伝達すること。
- *真正な電子文書ベースの情報* ― 情報が標榜通りのもの（つまり、時が経過しても改ざん、変更、またはそれ以外の方法で破損されていない情報）であることを保証する。a) 転送と保管、b) 保存環境、c) アクセスと保護が中心となる。

アーカイブの潜在的証拠性とデータ認証性、出所、および証拠保全に対応するニーズは、アーカイブで大量のメタデータを保有、保護、および保持する必要があるという点で、注目に値する。これは、ISO 14721 で規定された以下のセキュリティ・サービスが情報とメタデータの両方に適用されることを意味する。

- *識別／認証サービス*は、情報システム・リソースを使用する要求者の ID を確認する。加えて、認証をデータの提供者に適用できる。認証サービスは、セッションの開始時またはセッション中に実行される。
- *アクセス制御サービス*は、情報システム・リソースの無許可使用を阻止する。このサービスは、無許可の方法でのリソースの使用も阻止する。また、このサービスは、リソースへのアクセスの様々な側面（リソースとの通信へのアクセス、情報／データ・リソースの読み取り、書き込み、または削除、処理リソースの実行など）にもリソースへのすべてのアクセスにも適用できる。
- *データ完全性サービス*は、データが無許可の方法で改ざんまたは破壊されていないことを保証する。このサービスは、恒久データ・ストア内のデータと通信メッセージ内のデータに適用される。
- *データ機密性サービス*は、無許可の個人またはコンピュータ・プロセスにデータが公開または開示されていないことを保証する。このサービスは、人間と情報システムとの対話を許可するデバイスに適用される。また、このサービスは、通信リソースの使用パターンの観測が不可能であることを保証する。
- *否認防止サービス*は、情報交換に関わった当事者がそれに関与したことを否認できないことを保証する。このサービスは、2 つの形態のどちらかまたは両方を取る。まず、データの受信者にデータの起源の証拠が提供される。これにより、データまたはその内容を送信したことを送信者が不当に否認する試みから保護される。次に、データの送信者にデータの配信の証拠が提供される。これにより、受信者がデータまたはその内容を受信したことを不当に否認するその後の試みから保護される。

このようなセキュリティ・サービスは、データとメタデータの保存中とアーカイブへ／からの転送中に適用される必要がある。同様に重要なこととして、セキュリティ・サービス／制御が調整／置き換えられるときには、アーカイブされたデータが攻撃および／または開示にさらされること（つまり、リスク）を回避するよう、注意しなければならない。

標準や公表文献の多くで、アーカイブの文脈ではプライバシーが直接取り上げられていない。しかし、世界中のプライバシー（PII の保護）規制の増加に伴って、この点への対応が必要だと SNIA は考えている。

出所と認証性は、ほとんどのアーカイブに不可欠な要素であり、これは、適切なメタデータ処理が必須であることを意味する。SNIA では、証拠保全施策が証拠要件に対応するためにも必要であり、このことが使用されるアーカイブ・ソリューションの特性を複雑にしている可能性がある（例えば、クラウドストレージは必要な詳細を提供できないことがある）ことにも言及している。

多くのアーカイブは、データが変更されていないことの「証明」を行っている（認証性）。しかし、代わりの戦略は、完全性検証アプローチの代わりに、不変性対策（WORM ストレージなど）を採用するということである。

4.5　データ認証性とデータ完全性

「データ認証性」と「データ完全性」という用語は、一緒に使用されることが多く、時には同義として使用されるが、正確な意味は理解されていないことがほとんどである。ISO/IEC 27000 は、「完全性」が「正確さと完全さの特性」と定義しており、さらに、ISO 7498-2 は、「データ完全性」が「データが無許可の方法で改ざんまたは破壊されていない特性」と定義している。また、ISO/IEC 27000 は、「認証性」は「実体が自称通りである特性」と定義している。「データ認証性」に関する定義はほとんど存在しないが、存在している定義は、しばしば「データの真正性」、「データの出所の保証」、また／あるいは「情報源に関する保証」などに沿っている。あるいは他方で、この 2 つの概念の関係については、データ認証性はデータ完全性と認証が結合されたときに実現される、または、データ認証性は完全性を通してデータのある一部に適用される認証であると説明できる。

データ完全性は、レプリケーションやデータ移行などの一部としてデータ完全性を保証するために消費されている多くのリソースを備えたストレージシステムやエコシステムにおける中心課題である。データ完全性もデータ認証性も、デジタル・アーカイブ内では、さらに重要性が高い。例えば、アーカイブ・ソリューションは、複数の技術に基づいて複数の独立したコピーを持つように設計される。そこでは、様々なコピー間の完全性と同様に、それぞれの技術に基づく完全性も維持されなければならない。データ認証性では、アーカイブはデータを認証するためのメカニズムとして位置付けられる。そのため、SNIA は、デジタル・アーカイブのデータ完全性要素とデータ認証性要素を、記録がそれを作成した組織の管理を離れた後に資料の証拠性を維持する責任をデジタル・アーカイブが担うように実装することを推奨している。

4.6　監視、監査、および報告

ISO/IEC 27040 は、一般的なセキュリティ・ガイダンスに沿った、ストレージ向けの監査ログ・ガイダンスを提供している。プライバシーが監査ログに含まれている場合は、考慮すべき問題と複雑さが増える。このような問題のいくつかを詳しく探索するために、組織が遭遇する可能性のある事象の例として欧州連合（EU）の一般データ保護規則（GDPR）が使用される。

GDPR には、ログ戦略に影響を与える可能性のある少なくとも 3 つの異なる側面（ある目的のための保持、ある期間の保持、および非特定化された保持）がある。一般的なログ戦略は、データのすべてのアクセスおよび／またはすべての更新を記録することである。「プライバシー・バイ・デザイン」を念頭に置いてシステムを設計しなかった場合は、個人情報がログに記録されるデータ・ストリームの中に埋もれてしまう可能性がある。GDPR は、EU 市民の個人情報が保持されている場合は、そのデータを非特定化して個人が直接識別されないようにし、データはそれが収集された目的をタグ付けされなければならず、データは存続期間（その存続期間の後は、当該データは抹消（完全削除）される）をタグ付けされなければならず、当該個人の要求によっても末梢可能となっていなければならない。一般的なログ戦略のほとんどがこのようなニーズを踏まえて作成されていないため、EU PII を含む現在のログの方式では、組織は GDPR 違反となり、世界中の年間収益の最大 4%の罰金が課されることになるかもしれない。GDPR は、関係機関に対して情報の保持を許可しているが、それが何かが定義されていないため、どの機関が何へのアクセスを許可されるのか不明確である。また、GDPR は、目的を集約できるかどうか（例えば、「ヘルスケア」は「歯」、

「身体」、「視力」を含むと考えることができそうである）を明記していないため、注意書きは、判例で境界が明確に定義されるまでは、慎重に細かい分類にしておくことを提案している。

4.7　データの廃棄／サニタイズ

一般的な記録および情報管理（RIM）フレームワーク[25]内では、廃棄は記録のライフサイクルの最終段階である。このようなフレームワークの中では、廃棄は破壊ではなく、アーカイブへの転送を意味する。後者の場合、これは、ほとんどの記録の破壊の実施を先延ばししているにすぎない（政府機関でなければ、無期限に保持されなければならない記録はほとんどない）。記録（データ）が不要になると、データの破壊が、有効なデータ・ガバナンス・プログラムの極めて重要で、時に必須のコンポーネントになる。データ破壊は、判読不可（紙の記録の場合）または回復不可能[26]（デジタル記録の場合）にする方法で情報を削除するプロセスである。

記録は、それに含まれている情報が、運用上の、法的な、政府の、または専門組織のコンプライアンスの理由で必要なくなったことが確認されるまでは最終処分できない。また、運用を統治するすべての電子記録廃棄規制と組織の記録保持ポリシーの順守を保証するのは組織の責任である。

今日の世界では、デジタル記録と電子記録からすべてのデータの形跡が十分削除されているとは言えない。プライバシーやセキュリティに関する懸念が増えているということは、情報への不正なアクセスおよび／または無許可のアクセスのリスクを最小限に抑えるように、電子データの廃棄を慎重かつ体系的に処理しなければならない。法的義務を満たすためには、媒体の適切なサニタイズ[27]とサニタイズ記録の証拠の保全が必要なことがある。

データ保護の文脈では、データ廃棄、特に、データ破壊が組織にとっての主要なリスク要因になっている。保持されなければならないデータの破壊は、サニタイズ・テクニックを使用したデータの適切な破壊の失敗、または除去されなければならないデータの破壊の失敗と同様に、重大な暴露につながる可能性がある。

5　サマリー

ISO/IEC 27040 の発行により、ストレージシステムとエコシステムの保護を支援する幅広いガイダンスをストレージ業界は提供された。この標準は、データ保護を明示的なテーマとして取り上げていないが、このペーパーで注目したような関連する規制を提供している。とは言うものの、データ保持および保管、データ認証性、アーカイブ・セキュリティ、およびデータ廃棄は、この標準によって完全には解決されないデータ保護の要素となっている。SNIA は、このような要素の重要性を認識しており、他の標準からガイダンス

---

25 『ISO 15489-1:2001、*情報および文書化 ― 記録管理 ― 第 1 部：全般*』は、記録管理プログラムを計画して実装するための多くのフレームワークの 1 つである。

26 デジタルの世界では、データを回復不可能にするということは、回復するために所定のレベルの労力が必要になることを意味する。

27 ホワイトペーパー「SNIA Storage Security – Sanitization（SNIA ストレージセキュリティ ― サニタイズ）」で、これらの概念の多くが取り上げられ、ストレージに関するガイダンスが示されている。

を利用したり、独自のガイダンスの一部を公開したりしながら、このホワイトペーパーでそのような要素を扱った。

6 参考文献

ISO 7498-2:1989, *Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture*

ISO 14721:2012, *Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model*

ISO 15489-1:2001, *Information and Documentation – Records Management – Part 1: General*

ISO TR 18492:2005, *Long-term preservation of electronic document-based information*

ISO 22301:2012, *Societal security -- Business continuity management systems --- Requirements*, was developed by developed by ISO/TC 223, *Societal security*

ISO 22313:2012, *Societal security -- Business continuity management systems – Guidance*

ISO/IEC 2382:2015, *Information technology -- Vocabulary*

ISO/IEC 2382-1:1993, *Information technology -- Vocabulary -- Part 1: Fundamental terms*

ISO/IEC 24762:2008, *Information technology -- Security techniques -- Guidelines for information and communication technology disaster recovery services*

ISO/IEC 27000, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*

ISO/IEC 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*

ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security*

ISO/IEC 27031:2011, *Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity*

ISO/IEC 27036 (multiple parts), *Information technology -- Security techniques -- Information security for supplier relationships*

A Data Protection Taxonomy, SNIA Data Protection and Capacity Optimization (DPCO) Committee, June 2010, https://www.snia.org/sites/default/files/A_Data_Protection_Taxonomy_V51.pdf

SNIA Data Protection Best Practices whitepaper, SNIA Data Protection and Capacity Optimization (DPCO) Committee, October 2017,

https://www.snia.org/sites/default/files/DPCO/Data%20Protection%20BP%20White%20Paper%20Final%20v1_0.pdf

SNIA Index for ISO/IEC 27040, SNIA, February 2015, https://www.snia.org/sites/default/files/SNIA-WD_ISO-IEC-27040-Index.pdf

SNIA Storage Security: Encryption and Key Management whitepaper, SNIA, August 2015, https://www.snia.org/sites/default/files/technical_work/SecurityTWG/SNIA-Encryption- KM-TechWhitepaper.R1.pdf

SNIA Storage Security: Sanitization whitepaper, SNIA, August 2015, https://www.snia.org/sites/default/files/technical_work/SecurityTWG/SNIA-Sanitization-TechWhitepaper.R2.pdf

SNIA Technical Position: Cloud Data Management Interface (CDMI) v1.1.1, SNIA, March 2015, https://www.snia.org/sites/default/files/CDMI_Spec_v1.1.1.pdf

SNIA Dictionary, https://www.snia.org/education/dictionary

Records Retention and Disposition Guidelines, Prepared by the Collaborative Electronic Records Project, Rockefeller Archive Center, Revised November 2008

European Union (EU) General Data Protection Regulation (GDPR), L 119/1 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6- ba9a-01aa75ed71a1/language-en

Archival Authenticity in a Digital Age, https://www.clir.org/pubs/reports/pub92/hirtle.html

7 謝辞

7.1 執筆者について

Eric Hibbard は、Hitachi Vantara の CTO Security & Privacy であり、30 年以上 ICT インフラストラクチャに携わってきたデータ／ストレージセキュリティの専門家である。また、SNIA セキュリティ TWG の議長であり、ABA、IEEE、CSA、および INCITS の指導的立場も務めている。これまで、ISO/IEC 27040（ストレージセキュリティ）、ISO/IEC 20648（ストレージシステムの TLS 仕様）、および ISO/IEC 27050（電子証拠開示）を含む複数の ISO/IEC および IEEE 標準を編集してきた。現在は、$(ISC)^2$ CISSP および CCSP 認定だけでなく、ISSAP、ISSMP、および ISSEP を中心とした資格と ISACA CISA 認定を取得している。www.linkedin.com/in/ericahibbard/も参照のこと。

Gary Sutphin は、2007 年からの SNIA セキュリティ TWG のメンバーである。いくつかの SNIA 認定試験の SME、Storage Networking World Conference のボランティア、SNIA Hands-on-Lab プログラムのボランティア兼インストラクター、および旧 SNIA End User Council のアクティブ・メンバーとしても活躍してきた。Sperry Univac で IT に携わって以来、Entrex/Nixdorf Computer、Prime Computervision、Sequent、および IBM での勤務経験がある。最近、セント・ピーターズバーグ・カレッジでシスコ・トレーニング・プログラムを修了し、タンパ・ベイ・エリアに居を構えている。www.linkedin.com/in/garysutphin/も参照のこと。

7.2 査閲者とコントリビューター

セキュリティ TWG は、本ホワイトペーパーに貢献した次の方々に感謝の意を表する。

Thomas Rivera, CISSP, CISA	Co-Chair, SNIA DPCO
Gene Nagle	Co-Chair, SNIA DPCO
Richard Austin	退職
Tim Hudson	Cryptsoft Pty Ltd
Bruce Rich	Cryptsoft Pty Ltd
Glenn Jaquette	IBM
Tim Chevalier	NetApp
Srinivasan Narayanamurthy	NetApp
Mark Carlson	Toshiba Memory America
Mike Wellman	SNIA/Colorado Technical University
Steven Teppler, Esq.	Abbott Law Group, P.A.

8 追加情報

SNIA のセキュリティ活動に関する追加情報については、https://www.snia.org/security を参照のこと。ISO/IEC 27040 に関するその他の SNIA ストレージセキュリティ・ホワイトペーパーについては、https://www.snia.org/securitytwg を参照のこと。

改訂に関する提案は http://www.snia.org/feedback/まで。

ISO/IEC 27040 標準は http://www.iso.org で購入できる。