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
テクニカル・ホワイトペーパー

ストレージ・セキュリティ：暗号化と鍵管理

2015 年 8 月 26 日

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。本ホワイトペーパーでは、データ機密性に関する推奨ガイドラインについて説明する。これには、転送中データ暗号化、蓄積データ暗号化、および鍵管理が含まれる。この推奨事項の実用的意義については、エンドユーザとストレージ・ベンダーの双方の観点から説明する。*

使用にあたって

SNIA 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。

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。

改訂履歴

版	日付	セクション	作成者	備考
V0.1	*2014 年 8 月 25 日*	全体	Walt Hubis	初稿
V0.2	*2014 年 3 月 6 日*	全体	Walt Hubis	レビュー草稿
V0.3	*2015 年 5 月 5 日*	全体	Walt Hubis	第 1 次投票草稿
V0.5	*2015 年 7 月 10 日*	全体	Walt Hubis	第 2 次投票草稿
V0.7	*2015 年 8 月 15 日*	全体	Eric Hibbard	投票後草稿
V0.8	*2015 年 8 月 18 日*	全体	Eric Hibbard	第 3 次投票草稿
V0.9	*2015 年 8 月 26 日*	全体	Eric Hibbard	最終稿

本書の変更または修正に関する提案は、http://www.snia.org/feedback/まで。

序文

本書は、SNIA セキュリティ技術分科会が ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security* 内の重要なトピックの紹介と概要を提供するために作成した一連のホワイトペーパーの 1 つである。これらのホワイトペーパーは、当標準に代わるものではなく、実際の標準に対する補足的な説明およびガイダンスを提供するものである。

要旨

ストレージ・エコシステムでは、データ・ストレージ・システムに転送されるデータ（転送中データ：data in motion）と格納されるデータ（蓄積データ：data at rest）を保護するために暗号化や鍵管理などの暗号メカニズムの利用が進んでいる。これらの技術を有効活用するためには、組織が、特に、機密データや高価値データが関係する場合に、その利点、課題、影響および制限を理解しておく必要がある。このストレージ・セキュリティ・ホワイトペーパーでは、ISO/IEC 27040 標準内のガイダンスを利用して、ストレージ・システムとエコシステムに適用可能な暗号化と鍵管理に関する有益な情報を提供する。

1　はじめに

ストレージ・エコシステムに暗号化を適用する場合、それをどこにどのように統合するかによって実に様々な保護を提供できる。例えば、ネットワーク・アタッチド・ストレージ（NAS）ファイル・システム内のファイルまたは共有の暗号化は、ドライブ・レベルの暗号化では不可能なユーザ個別の保護を提供できる。そのため、暗号化を検討すべき理由（つまり、対処すべき脅威）を理解しておくことが重要である。

ISO/IEC 27040:2015 *Information technology - Security techniques - Storage security* 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（概要については付録 A を参照）。この標準の対象範囲は極めて広いが、保護を強化するための特定のテーマに関する具体的なガイダンスが不足している。この点は、暗号化や鍵管理の一部についても当てはまる。

ストレージ・セキュリティの様々な要素に対処するために SNIA から提供されているシリーズの 1 つであるこのホワイトペーパーの目的は、ISO/IEC 27040 標準内のガイダンスをベースにして暗号化と鍵管理に特化した内容に再構築することである。加えて、特定のセキュリティ機能および能力についての業界の洞察を盛り込む。このホワイトペーパーでは、暗号化と鍵管理に関する背景情報を示し、セキュリティ上の選択肢について簡単に説明し、関連する ISO/IEC 27040 のガイダンスを紹介し、ストレージの保護に役立つ追加情報を提供する。

1.1　機密性と秘密性

機密性は、許可された関係者はオンデマンドで情報を入手できるが無許可の関係者は入手できないという属性である。秘密性は、機密性の同義語としてよく用いられる用語である。暗号メカニズムは、データ・ストレージ用のアプリケーションとプロトコルに機密性とその他のセキュリティ・サービスを提供する最も強力な手段の 1 つである[1]。

機密性は、多くの場合、無許可の関係者が情報を理解できないようにするための暗号化を使用して実現される。許可された関係者は復号化によって情報を理解できるようになる。暗号化で機密性を確保するためには、無許可の関係者が暗号化に関連付けられた秘密鍵（私有鍵）

[1] 暗号の入門書として、H. X. Mel と Doris Baker による『Cryptography Decrypted』（Addison-Wesley:2000 ISBN 978-0201616477）がある。

[2]を特定できず、鍵を特定せずに直接平文を抽出することもできないように暗号アルゴリズムと動作モードを設計する必要がある。

1.2 暗号化の概要

暗号化（または*暗号変換*）システムの主な目的は、保存または送信されるデータの機密性を確保することである。暗号化アルゴリズムは、平文を暗号文に変換し、復号鍵を知らなければ平文の内容に関するいかなる情報の解読も計算時間の面からみて実行不可能にすることによってこれを実現する。ただし、大抵の場合、暗号文の長さは対応する平文の長さと同じか、わずかに長いだけなので、暗号化によって平文の長さを隠すことはできない。

暗号化はそれ自体でデータの完全性や発生元を必ずしも保護できないことに注意すべきである。多くの場合、鍵の知識がなくても、復元された平文に予測可能な影響を与えるように暗号文を変更することができる。データの完全性と発生元を保証するためには、追加のテクニックを使用する必要があることが多い。

暗号アルゴリズムには、ハッシュ・アルゴリズム、対称鍵アルゴリズム、および非対称鍵アルゴリズムという 3 つの基本的なクラスがある。これらクラスは、アルゴリズムと組み合わせて使用される暗号鍵の数によって定義される。

1.3 鍵管理の概要

ハッシングを除いて、暗号の使用は暗号鍵の管理に依存する。対称と非対称の両方を含むすべての暗号化では、情報をやり取りする関係者全員が必要な鍵にアクセスできなければならない。そのため、鍵の生成、配布、および継続的管理を含む鍵管理が必要になる。鍵管理の全体的なフレームワークが ISO/IEC 11770-1 と NIST SP 800-57 Part 1 に記載されている。

NIST SP 800-57 Part 1 (R3)に記載されているように、鍵は金庫を開けるための番号の組み合わせに似ている。金庫を開けるための番号の組み合わせが敵対者に知られたら、最強の金庫であってもその内容物に対して何の保護も提供できない。同様に、貧弱な鍵管理が強力なアルゴリズムを簡単に無にする可能性がある。最終的に、暗号で保護された情報のセキュリティは、鍵の強度、鍵に関連付けられたメカニズムとプロトコルの有効性、および鍵に施された保護に直接依存する。すべての鍵を改変から保護し、秘密鍵と私有鍵を無許可の開示から保護する必要がある。鍵管理は、鍵の安全な生成、保管、配布、および破壊の基盤となるものである。

1.4 暗号強度

暗号強度は、攻撃者が不明な暗号鍵に対して総当たり攻撃を仕掛けるために投資しなければならない仕事量の尺度である。例えば、112 ビットの強度は、攻撃者が正しい鍵にヒットするまでに平均で 2^{112-1} 個の鍵を試さなければならないことを意味する。しかし、暗号強度は全

[2] 秘密鍵は対称暗号化で使用されるのに対して、私有鍵は非対称暗号化で使用される。

体の一部を示しているに過ぎない。この尺度を現実の問題に直結させるためには、総当たり攻撃を攻撃者が実行可能な唯一の攻撃にする必要がある。暗号アルゴリズムの処理に弱点がある場合は、分析攻撃の方がはるかに効果的である。また、アルゴリズムの実装に弱点がある場合（鍵が鍵空間全体からランダムに選択されていない場合など）は、攻撃者の仕事は容易になる。さらに、攻撃者がソーシャル・エンジニアリングを実行できたり、鍵マテリアルにアクセスすることができたりする場合は、総当たり攻撃を仕掛ける必要がない。十分に確認されたアルゴリズムとそのアルゴリズムの十分に検査された実装を選択することによって、攻撃者の仕事を容易にする弱点を回避できる。強力な鍵管理を導入すれば、ソーシャル・エンジニアリングを実行したり、それ以外の方法で鍵マテリアルにアクセスしたりすることが格段に難しくなる。このような実践を通して、攻撃者の選択肢を総当たり攻撃のみに狭めることができる。

1.5 ストレージ管理

ISO/IEC 27040 では、ストレージ管理（ストレージ・システムの運用、管理、保守、プロビジョニング、およびサニタイズに関連した操作、方式、手順、ツールなど）を安全に行うことの重要性が強調されており、ストレージ管理インタフェースを保護し、システムとユーザの説明責任と追跡可能性を維持し、ストレージ管理に使用される基礎システムを十分に保護するために、認証と認可についての統制が必要であるとも述べられている。このホワイトペーパーでは取り上げないが、ストレージ管理の不備がデータの侵害や損失につながる可能性があることには留意すべきである。ストレージ管理通信プロトコル用の転送中データ暗号化は、このような脅威に対する保護において重要な役割を担っている。

2 データ・ストレージ暗号化

ストレージ・エコシステムに関連した暗号化の議論には、必然的に、転送中データ暗号化と蓄積データ暗号化の違いが含まれる。この概念を定義することは難しいが、理解しておくことは重要である。以下にその要約を示す。

- *蓄積データ暗号化* ― メディアに保存されたデータを保護する暗号化。データが逆方向に同じポイント（または同等のもの）を通過したときに復号化されるデータの暗号化が含まれる。暗号化ポイントは、ストレージ・デバイス内（テープ・ドライブ暗号化）またはデータが作成／使用されるエンティティ内（エンドツーエンド暗号化）に存在する場合、あるいはまたデータ・パス上の任意のポイントの場合がある。
- *転送中データ暗号化* ― 2 つの通信エンティティ（ホスト・バス・アダプターまたは HBA とスイッチなど）間の物理リンク上を転送されているデータを保護する暗号化。2 つのエンティティが何らかの形で通信暗号化をネゴシエートして実装している場合とデータが転送前に暗号化される場合がある。

上記の説明から分かるように、蓄積データ暗号化メカニズムは、実際のデータがダウンストリームのすべての通信リンクを通過する際の機密性を保護できる可能性を持っているが、この保護は暗号化がデータ・パス内のどこで適用されるかによって異なる。通信ベースの暗号化（IPsec、TLS、SSH など）は、データをやり取りする関係者が平文データにアクセスできるよ

うにするが、暗号文が転送中に変更されていないことを保証する完全性チェックを含めることもできる。

2.1 転送中データに関する推奨事項

高価値データや機密データ[3]は、TCP/IP、Fibre Channel over IP (FCIP)、Fibre Channel over Ethernet (FCoE)、iSCSI などのプロトコルを使用し、ワイド・エリア・ネットワークを介してシステム間で頻繁に交換される。また、データは、ファイバー・チャネル、シリアル SCSI（SAS）、およびその他のストレージ・エリア・ネットワーク（SAN）プロトコルを使用して、ホスト・コンピューター・システムから SAN 経由でストレージ・デバイスに転送される場合もある。いずれの場合も、特定のネットワーク・プロトコルで使用できる個別のセキュリティ・プロトコルが存在することがあり、その場合、データをよりセキュアに転送することができる。また、送信中のデータを保護することが可能なトランスポート・レベルのセキュリティ・メカニズムが存在することもある。特定の保護メカニズムと暗号化ポイントを選択することは、データの保護だけでなく、適用可能なコンプライアンス要件の順守においても重要な要素である。

一般的に、転送中データの暗号化は、転送中のデータを一時的に保護するだけである。ファイル・システム、アプリケーション、ホスト・バス・アダプター（HBA）などで使用される特定の暗号化方式は、中間のスイッチング・デバイスやルーティング・デバイスに関係なく、エンドツーエンドの保護を提供する。このような方式を採用している場合は、転送中データの暗号化によって追加のデータ保護が得られることはほとんどない。また、暗号化データにはデータ量削減技術（圧縮や重複排除など）がほとんど役に立たないことにも注意したい。さらに、データ保護に関するベスト・プラクティスでは、転送中データには短寿命鍵が、蓄積データには長寿命鍵が推奨されている[4]。したがって、暗号化ポイントと復号化ポイントを選択する前にシステム全体の要件を考慮する必要がある。

ISO/IEC 27040 では、転送中データに対して TLS、IPsec、FC-SP-2 などのデータ保護プロトコルを使用するように具体的に推奨されている。ファイバー・チャネル・ネットワークの保護に関する問題は、このシリーズのホワイトペーパー「SNIA Storage Security: Fibre Channel Security（SNIA ストレージ・セキュリティ：ファイバー・チャネル・セキュリティ）」に記載されている。

2.1.1 IP SAN

IP ネットワークを使用してストレージ・プロトコルを提供するための 2 つの方式が ISO/IEC 27040: Internet SCSI (iSCSI) and Fibre Channel over TCP/IP (FCIP) に記載されている。

---

[3] *ISO/IEC 27040 Annex B* では、低いデータ機密性と高いデータ機密性が区別されている。この両方に対して保護制御が必要である。これは、機密性の低いデータでも企業、政府、または個人に悪影響を及ぼす可能性があるためである。B.1.2 Data sensitivity classes を参照のこと。

[4] 短寿命鍵や短命セッション鍵は、データがネットワークを通過中に復号化される可能性を減らすことができる。蓄積データ用の長寿命鍵は、データを別の鍵で暗号化し直す回数を削減できる。SNIA ホワイトペーパー「Encryption of Data at Rest - a Step by Step Checklist（蓄積データの暗号化 ― 段階的チェックリスト）」を参照のこと。

iSCSI と FCIP はどちらもネットワーク上のイニシエーターとターゲットの間のトラフィックを制御できるというメリットがある。この制御は、送信元と宛先の IP アドレスとプロトコルをフィルタリングすることで実現でき、これはターゲットと中継スイッチのどちらかで行うことができる。そして、攻撃ベクトルの数も削減しながらターゲットが扱う必要のあるトラフィックの量が削減される。

IP SAN では、一般的に、ネットワーク上のリソースを特定するために様々な情報サービスが利用される。例として、インターネット・ストレージ・ネーム・サーバ（iSNS）、サービス・ロケーション・プロトコル（SLP）、ドメイン・ネーム・サーバ（DNS）などが挙げられる。ISO/IEC 27040 では、これらのサービスを適切なセキュリティ管理と一緒に使用してデータ・ストレージ・リソースに関する攻撃や情報収集を防止することが推奨されている。RFC 3723 では、適合した実装のための特定のセキュリティ要件が推奨されている。RFC 2608 *Service Location Protocol, Version 2* では SLP のセキュリティに関する一般的なガイダンスが提供されているが、RFC 3723 では IPsec を使って SLPv2 を保護することが推奨されている。同様に、IETF RFC 4171 *Internet Storage Name Service (iSNS)*では iSNS のセキュリティに関する一般的なガイダンスが提供されているが、RFC 3723 では iSNS と IPsec の組み合わせを使用した間接的攻撃の回避を含むより具体的な推奨事項が提供されている。ネットワーク情報サービスを管理する方法も保護する必要がある。

実用的観点からすると、様々なデバイスにリソースの制約があり、高度なセキュリティ・ソリューションのスケーラビリティの確保が困難なことや現実的ですらないことがある。このことは、特に、実装の範囲が大規模なサーバから小規模な組み込みシステムにまで及ぶ iSCSI ネットワークに当てはまる。ファイバー・チャネル・システムはデータセンター内で使用されることが多いため、一般的にリソースの制約が比較的少ない。したがって、セキュアな IP SAN を実装するには、ネットワークのあらゆる部分の慎重な評価が不可欠である。

2.1.1.1 インターネット SCSI（iSCSI）

IETF RFC 3720 *Internet Small Computer Systems Interface (iSCSI)*には、TCP/IP 上で動作する SCSI トランスポート・プロトコルの説明が記載されている。このプロトコルは、SCSI RDMA Protocol (SRP)またはiSCSI Extensions for RDMA (iSER)を使用してリモート・ダイレクト・メモリ・アクセス（RDMA）を提供するように拡張されている。ISO/IEC 27040 には、これらの RDMA プロトコルに関するセキュリティ問題は記載されていない。IETF RFC 3720 に記載されたすべての iSCSI セキュリティ要件が適用される。

iSCSI プロトコルは、CHAP 認証の使用を通してある程度のアクセス保護を提供する（IETF RFC 1334 *PPP Challenge Handshake Authentication Protocol (CHAP)*を参照）。双方向 CHAP（イニシエーターがターゲットを認証し、ターゲットがイニシエーターを認証する）はランダム・チャレンジと一緒に使用する必要がある。

IP SAN へのアクセスを制御するには、SCSI インタフェースを汎用の IP ネットワークに接続しないようにする必要がある。パフォーマンスとセキュリティの両面において、物理的に分離された iSCSI IP ネットワークは最適な制御を実現する。これが不可能な場合は、仮想エリア・ネットワーク（VLAN）を使用して IP SAN を他のネットワーク・トラフィックから分離する必要が

ある。

2.1.1.2 Fibre Channel over TCP/IP (FCIP)

IETF RFC 3821 *Fibre Channel Over TCP/IP (FCIP)*には、IP ベースのネットワークを介したファイバー・チャネル・ストレージ・エリア・ネットワークの相互接続で単一のファイバー・チャネル・ファブリックにストレージ・エリア・ネットワークを統合できる純粋なカプセル化プロトコルが記載されている。IETF RFC 3821 と ISO/IEC 27040 は、IPsec を使用した機密性と認証に依存している。

2.1.1.3 IP セキュリティ・プロトコル（IPsec）

ISO/IEC 27040 と IETF RFC 3723 *Securing Block Storage Protocols over IP* では、IPsec を使用して通信チャネルを保護し、iSCSI と FCIP の両方の機密データまたは高価値データを保護する必要がある。ISO/IEC 27040 では、IPsec バージョン 3 とインターネット鍵交換（IKE）バージョン 2 の併用が推奨されている。IPsec バージョン 3 は一連の IETF ドキュメントに記載されている。

- RFC 4301 *Security Architecture for the Internet Protocol*
- RFC 4302 *IP Authentication Header*
- RFC 4303 *IP Encapsulating Security Payload (ESP)*
- RFC 4306 *Internet Key Exchange (IKEv2) Protocol*

加えて、IETF RFC 3723 *Securing Block Storage Protocols over IP* では、iSCSI プロトコルおよび Fibre Channel over TCP/IP (FCIP)プロトコルと一緒に使用される IPsec スイート上の次の要件が規定されている。

- 機密性：IETF RFC 2451 *The ESP CBC-Mode Cipher Algorithms* に記載されているように CBC モードの 3DES を使用した ESP をサポートする必要があるが、IETF RFC 3686 *Using Advanced Encryption Standard (AES) Counter Mode* に記載されているようにカウンター・モードの AES をサポートする必要がある。新しい実装では AES 暗号化を使用することが強く推奨されている（NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices* を参照）。
- 認証と完全性：IETF RFC 2404 *The Use of HMAC-SHA-1-96 within ESP and AH* に記載されている HMAC-SHA1 をサポートする必要がある。RFC 3566 *The AES-XCBC-MAC-96 Algorithm and Its Use with IPsec* に記載されている XCBC 拡張を使用した CBC MAC モードの AES をサポートする必要がある。新しい実装では AES 暗号化を使用することが強く推奨されている。CBC モードの DES は使用しないこと。
- IPsec モード：IETF RFC 2406 *IP Encapsulating Security Payload (ESP)*に基づくトンネル・モードの ESP をサポートする必要がある。トランスポート・モードの ESP を使用した IPsec をサポートしてもよい。

2.1.2 ファイバー・チャネル（FC）SAN

IP SAN と同様に、FC SAN は、ファイバー・チャネル・エンティティを認証するためのプロトコルを含む多様なセキュリティ機能の活用、セッション鍵のセットアップ、フレーム単位の完全性と機密性を保証するためのパラメーターのネゴシエーション、およびファイバー・チャネル・ファブリック全体でのポリシーの定義と配布を可能にする。これらのメカニズムの多くは理解しにくく、正しく設定することは容易ではない。この状況を踏まえて、SNIA では、FC セキュリティをさらに掘り下げた別のホワイトペーパー「SNIA Storage Security: Fibre Channel Security（SNIA ストレージ・セキュリティ：ファイバー・チャネル・セキュリティ）」を作成した。

2.2 蓄積データ暗号化

2.2.1 SNIA による暗号化の位置付け

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）は、データ、特に一次データの暗号化に関するセキュリティにおいて、暗号化を最終手段として位置付けている。つまり、SNIA では、*機密データ*がそれに対する責任を認識または所有している組織の直接的な管理を離れた時点で、適切な暗号化を使用するように強く推奨している。この文脈では、機密データは、機密性の保護に関する法律または規制要件が課されたデータだけでなく、組織の*注意義務*の一部として保護が必要なデータ（企業秘密や知的財産など）も意味する。

SNIA では、管理組織の管理を離れたデータを*外在データ*と呼んでいる。この外在データが機密データでもある場合の推奨事項を以下に示す。

- 組織の管理を離れる可能性のあるリムーバブル・メディア（バックアップ用テープなど）に保存されるデータには、蓄積データ保護が必要である[5]。
- サードパーティのデータセンターに保存されるデータには、このような「信頼できない」データセンター内での転送中データ保護と蓄積データ保護の両方が必要である。
- 「信頼できる」（組織によって管理されている）データセンター間で転送されるデータは、保護する必要がある。

2.2.2 暗号化ポイント

一般的に、蓄積データ暗号化は、データ・フロー・パス内の単一の暗号化／復号化メカニズムの配置に依存し、これは暗号化ポイントと呼ばれる。暗号化ポイントの配置は、ストレージ・エコシステム内のどの位置に平文データをルーティングして暗号文に変換するかを決定し、また逆に暗号文を使用可能な平文データに変換するために通過しなければならないストレージ・エコシステム内のポイントを示すものであるため、非常に重要である。また、暗号化ポイントは、ストレージ・エコシステム内でデータが平文形式で存在する場所とデータが暗号文で存在する場所も決定する。

[5] データセンター間を移動するテープ上に保存されたデータは蓄積データと見なされることに注意されたい。

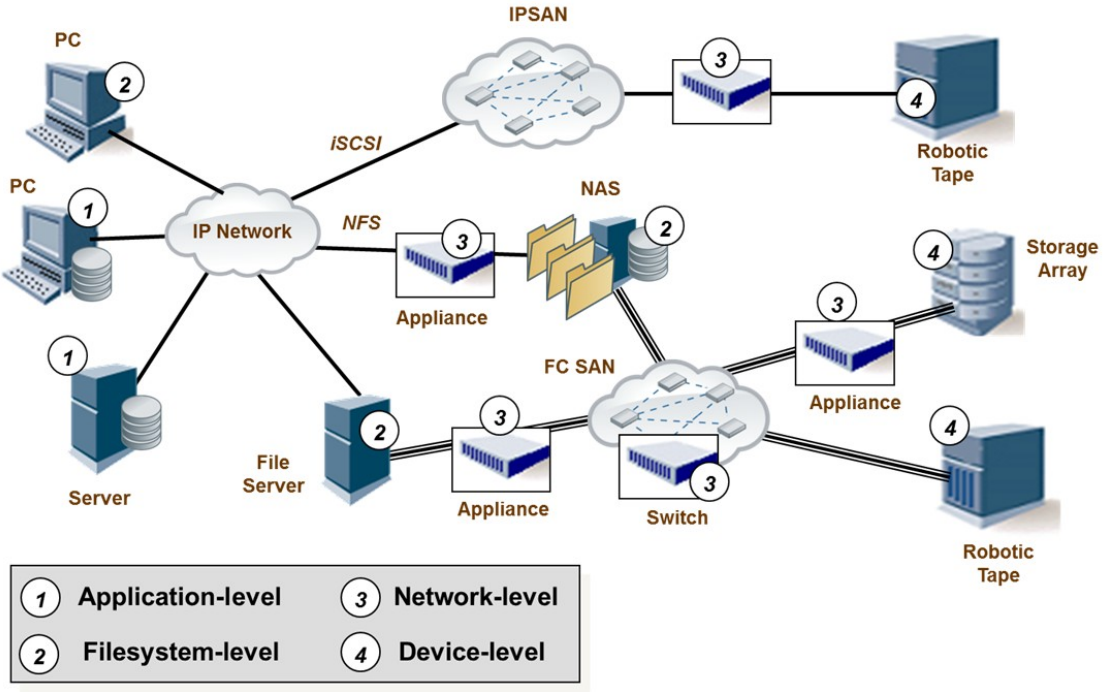


図 1：ストレージ・エコシステム内の暗号ポイントの選択肢

暗号の使用についてのセキュリティ専門家の一般的考えによれば、暗号化はできるだけデータの発生元（生成するアプリケーション）の近くで適用すべきである。そうすることによって、保護（転送中データと蓄積データの保護）が最大化され、データの特性や属性を考慮した保護が可能になる。残念ながら、この一般的なガイダンスは環境内のその他の要因のせいで実際的でない場合がある（生成するアプリケーションが暗号化機能を提供していない場合など）。

アーキテクチャー上は、複数の暗号化ポイントの候補があり得る。このような状況では、選択プロセスの一環として次の要素と影響を考慮する必要がある。

- *使いやすさ* ― インタフェース、プロセス、および／またはストレージ・メカニズムが変更され、ユーザがそれを受け入れがたい場合がある。
- *可用性* ― システム／ソリューションの全体的な可用性が制限、低減、または排除される度合い。
- *インフラストラクチャー* ― ネットワーキング、システム、およびストレージ・インフラストラクチャーを変更（LUN の移動など）しなければならない度合い。
- *パフォーマンス／スループット* ― 既存のものと比べた場合の悪影響（小＝10%、中＝20%、大＝35%、最大＝50%以上）。
- *拡張性* ― 既存のシステムの全体的な拡張性が制限、低減、または排除される度合い。

- *転送中機密性* ― ユーザ・システム／アプリケーションからストレージ・デバイス／メディアまでの機密性保護の特性。
- *事業継続性／災害対策* ― 全体的な事業継続性／災害対策が制限、低減、または排除される度合い。
- *暗号化の証明* ― 暗号化証明の様々な側面の特性（機能性、既存のインフラストラクチャーへの統合、証拠）。
- *環境* ― 環境的側面の特性（電力、冷却、スペース）。

これらの要素のそれぞれを暗号化ポイントの 4 つのカテゴリ（表 1 を参照）に関して比較対照すると、明確に優位なものは存在しない。つまり、受け入れ可能なソリューションを決定するためには、組織に固有の要件（コンプライアンスなどに関する）、データ機密性、および既存のインフラストラクチャーを慎重に検討する必要がある。

影響	アプリケーション	ファイル・システム	ネットワーク	デバイス
使いやすさ	小	小～中	なし	なし
可用性	～大	～大	小～中（冗長性）	小～中
インフラストラクチャー	～大	～大	小～中	小
パフォーマンス／スループット	～最大	～大	小	小～中
拡張性	～大	～大	～中	最小
転送中機密性	最大	小～中（NAS）、最大（ホスト）	小～中	なし
事業継続性／災害復旧	～超複雑	～複雑	～超複雑	～超複雑
暗号化の証明	～複雑	比較的容易	小～中	～複雑
環境	小～中	小～中	～大	小

表 1：暗号化に影響する要素

そうは言っても、ネットワーク・レベルの暗号化（重要性は低い）とデバイス・レベルの暗号化をセーフティ・ネットとして期待している組織もある。主な目的は、機密データと組み合わせて使用されるストレージ・メディア（テープやディスク）の暗号化を保証することである。このよう

にして保護されたメディアでは、取り扱いミス（紛失、未完成、無許可の関係者への転送など）やベンダーやサプライヤーへの返却時に、組織はセキュリティ・インシデントに関連したコストや信頼失墜を免れることができる。

2.2.3 蓄積データに関する推奨事項

ISO/IEC 27040 では、データはその発生元のできるだけ近くで暗号化されることが最良であると認めているが、ストレージ・ポイントの近くで使用される暗号化がメディアの管理が失われた状況（ストレージ・メディアの再利用や廃棄など）に対処するための有効なメカニズムを提供することも認めている。このような場合は、自己暗号化ドライブ（SED）、コントローラ・ベースの暗号化、テープ暗号化などの技術が特に有効である。ただし、これらの技術では、以下の提供を慎重に検討した計画が必要である。

- 暗号化のポイントとタイプの選択
- 暗号化の識別、場所、および検証（監査）
- 鍵管理

適切な暗号化アルゴリズムを採用してデータ機密性を保証する必要がある。これには、ドライブ用の XTS-AES やテープ用のガロア／カウンター・モード（GCM）などの AES ブロック連鎖暗号化方式が含まれる。いずれにしても、鍵管理は蓄積データの保護の非常に重要な部分であり、本書のセクション 3 でさらに詳しく説明する。

すべての暗号化のタイプに対して、以下の管理が推奨されている。

- ストレージ・ベースの暗号化を暗号化の基本形態にすべきではない。データの機密性と完全性の保証は蓄積データ暗号化に留まらない。
- 暗号化ポイントは必要なデータ量削減処理に依存する。
- 暗号化の導入時にデータ保有要件に対処する必要がある。
- 暗号化の強度は 112 ビット以上（推奨は 128 ビット以上）にする必要がある。
- 暗号モジュールは広く認められた基準に基づいて検証する必要がある。
- 複数の暗号化手順を使用できる。例えば、アプリケーション層で暗号化してから自己暗号化ドライブに保存する場合など。
- 暗号化操作は、適切な監査ログ・エントリー（有効化、鍵再作成、検証など）を生成する必要がある。

高価値データの暗号化は、蓄積データ暗号化と転送中データ暗号化を含むエンドツーエンドなものにする必要がある。詳細については、ISO/IEC 27040, Section 7.5 *Data confidentiality and integrity* を参照のこと。

3 鍵管理

3.1 適切な鍵管理の重要性

蓄積データについても転送中データについても、暗号化データの適切な鍵管理が、そのデータの機密性と可用性に不可欠である。転送中データの鍵管理は重要であり、この状況で使用される鍵の多くは、短寿命で、自動鍵交換方式（IKEv2 など）を通して生成される。また、大抵の場合、単一の鍵で保護されるデータ量は少ない。一方、蓄積データの保護用の鍵は細心の注意を要する。これは、暗号化データの寿命が長く、単一の鍵で保護されるデータ量が転送中データに比べてはるかに多いためである。ISO/IEC 27040 に加えて、NIST Special Publication 800-57, *Recommendation for Key Management – Parts 1-3* には、鍵管理に関する詳細情報と推奨事項が数多く記載されている。

鍵と鍵マテリアルのライフサイクルは、どの鍵管理方式においても重要な考慮事項である。鍵管理の考慮事項には、鍵の生成、鍵のセキュアな配布、鍵の有効化と無効化が含まれる。加えて、鍵のアーカイブ方法、有効期限が切れた後の破壊方法、鍵の漏洩への対処方法を管理する手順を導入する必要がある。単純な鍵のライフサイクル・システムを図 2 に示す。

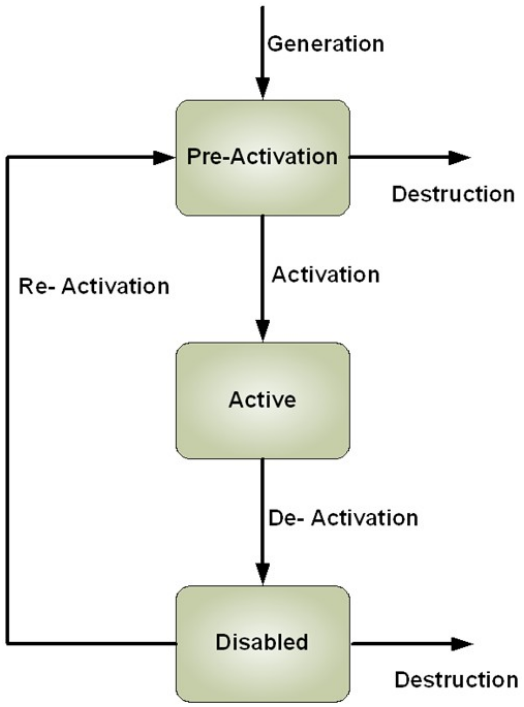


図 2: 単純な鍵のライフサイクル

鍵のライフサイクル管理の問題の様々な側面には非常に複雑な点があり、それはこのホワイトペーパーの範囲を超えている。NIST Document SP 800-57 Part 1-Rev.3 *Recommendations for Key Management: Part 1: General (Revision 3)* に

鍵のライフサイクルに関する推奨事項が記載されている。また、OASIS *Key Management Interoperability Protocol (KMIP) Specification Version 1.2* に、業界標準の鍵のライフサイクル・モデルが示されている。

3.2 KMIP に関する考慮事項

鍵管理は、正しい実装がより困難な暗号化要素の 1 つである。ストレージ・クライアントによる KMIP の使用は、問題の多い様々な要素（ランダム鍵の生成など）の多くを「外部委託」する有効な方法である。KMIP を使用する場合やその使用を検討する場合は、以下を考慮することが重要である。

- *鍵マテリアルの可用性* ― ストレージ・システムがそのデータ暗号化鍵や鍵ラップ鍵を外部の鍵管理サーバに依存している場合は、これらの鍵が使用可能になるまでストレージ・システム上のデータにアクセスできない、つまり、暗号文に対する操作（複製やバックアップなど）を実行できないことを意味する。したがって、複数の鍵管理サーバに対する冗長アクセスを組み込むことが重要である。加えて、ストレージ・システムは、適切な鍵が入手可能になるまで、ユーザまたはホストによるデータへのアクセスの試みをブロックする必要がある。
- *セキュアなトランスポート* ― 暗号化鍵は機密情報と見なされるため、常に、特に転送中は、保護する必要がある。KMIP 仕様では、この保護が要求されているが、その詳細は KMIP プロファイルに委ねられている。このプロファイルで、基*本認証群*と *TLS 1.2 認証スイート*における TLS の使用が指定されている。KMIP サーバは TLS 1.0 のサポートが必須であるが、TLS 1.1 と TLS 1.2 のサポートは任意である。KMIP クライアントには、このような要件が適用されない。基本認証スイートには TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートが必須であり、TLS 1.2 認証スイートには TLS_RSA_WITH_AES_128_CBC_SHA256 暗号スイートと TLS_RSA_WITH_AES_256_CBC_SHA256 暗号スイートが必須である[6]。

  注意：*SNIA TLS Specification for Storage Security*（ISO/IEC 20648）では、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートと TLS_RSA_WITH_AES_128_CBC_SHA256 暗号スイートが必須である。
- *監査セキュリティ* ― ストレージ・システムが KMIP サーバとのやり取りに依存している場合は、KMIP トランザクションのロギングが問題の根本原因の特定に不可欠である。そのため、すべての KMIP クライアント／サーバ間の動作を、問題を診断するのに十分な詳細さでログに記録する必要がある。鍵は、絶対にログ内で公開してはいけない。加えて、多くの組織が暗号化の証明と災害対策／事業継続性の証拠として機能するレコードを保持する必要がある。一部の KMIP 処理がこれらの活動で特定の役割を果

[6] TLS に必須の暗号スイートは TLS のバージョンによって異なり、KMIP に必須のものとは異なる場合がある。TLS バージョン 1.0（IETF RFC 2246 を参照）では TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA が、TLS バージョン 1.1（IETF RFC 4346 を参照）では TLS_RSA_WITH_3DES_EDE_CBC_SHA が、TLS バージョン 1.2（IETF RFC 5246 を参照）では TLS_RSA_WITH_AES_128_CBC_SHA が必須である。

たす。これは、監査ログ内で適切なイベント・エントリーを収集する必要があることを意味する。

- *KMIP サーバの互換性* ― KMIP ベースの鍵管理を使用する重要な動機は、KMIP クライアントが様々なベンダー（Cryptsoft、HP、IBM、Quintessence Labs、Thales e-Security、Townsend Security、Gemalto、Vormetric など）の鍵管理サーバを使用できることである。KMIP クライアント実装は、KMIP 仕様の解釈を間違えることによって事故的に互換性（場合によっては仕様適合性）を損なうことがないように慎重に設計する必要がある。分かりやすい例として、KMIP データ型の「テキスト文字列」は最大長が関連付けられていない（また、null 終端が許されない）ため、「テキスト文字列」が KMIP サーバによって特定される「一意の識別子」や「証明書発行者識別名」に使用される場合は、KMIP クライアントは短い文字列と長い（256 文字を超える）文字列の両方を処理できるようにしておく必要がある。
- *KMIP 適合の検証* ― 組織が複数のベンダーの鍵管理サーバを導入したり、ベンダーを変更したりするのは珍しいことではない。このような KMIP クライアントと KMIP サーバ間の相互運用性は重要であり、組織の環境に導入する際の必須条件として、この相互運用性を立証する必要があることもある。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）のストレージ・セキュリティ業界フォーラム（SSIF）は、製品に KMIP を実装したベンダーが、コロラド州コロラドスプリングスの SNIA テクノロジー・センターにあるテスト・ツールやその他の製品を使って自社製品のプロトコル順守をテストできるようにする KMIP Conformance Test Program を開設した。このプログラムは、特定の KMIP 実装が KMIP 標準に準拠していることの、信頼できる第三者からの独立検証を提供する。この検証は、評価済みの製品が他の同様にテストされた KMIP 製品と相互運用可能であるという信用を顧客に提供できる。テスト料金は、製品のタイプ（クライアントかサーバか）、製品に対して検証するプロファイルの数、およびその会社が SSIF のメンバーかどうかによって異なる。

3.3 鍵管理に関する推奨事項

鍵管理は、鍵の安全な生成、配布、および破壊の基盤となるものである。それに応じて、ISO/IEC 27040 には鍵の使用と管理に関する重要なガイダンスが記載されている。

- 鍵空間全体からランダムに選択された鍵を使用する。
- 脆弱な鍵の使用を避け、脆弱な鍵が使用されないようにチェックする（特に、ユーザが選択する場合）。一般的に、ユーザが選択した鍵を直接データ暗号化鍵として使用すべきではない。また、鍵は攻撃者が簡単に推測できないようにする必要がある。推奨ガイドラインについては、NIST SP-800-132 *Recommendation for Password-Based Key Derivation Part 1: Storage Applications* を参照のこと。
- 鍵の使用期間を NIST の推奨最大暗号有効期間である 2 年に制限する。特定の環境では、この期間を大幅に短くするべきかもしれない。
- 1 つの鍵で保護する最大データ量を制限する。

- 鍵の生成、変更、および配布に対して厳密なアクセス制御を実施する。KMIP を使用したほとんどの鍵管理システムが必要な制御を実装している。
- 一元管理された相互運用可能な鍵管理インフラストラクチャーを使用する。
- 鍵管理は完全に自動化する必要がある。
- OASIS KMIP 準拠のサーバとクライアントを使用して鍵を管理する必要がある。

OASIS Key Management Interoperability Protocol は、広く業界に受け入れられている一般的なプロトコルを提供する。OASIS Key Management Interoperability Protocol Specification では、鍵管理システムによって保存および維持されたオブジェクト（暗号化鍵が一般的）に対する管理操作を実行するためにクライアントとサーバ間の通信に使用されるプロトコルが規定されている。SNIA のストレージ・セキュリティ業界フォーラム（SSIF）では、Key Management Interoperability Protocol (KMIP) Conformance Test Program を提供している。詳細については、http://www.snia.org/forums/SSIF/kmip を参照のこと。

4 その他の鍵管理と暗号化に関する問題

ISO/IEC 27040 では、特に大規模なシステムや仮想化されたシステムにおけるセキュアなストレージ・システムのエンドユーザ向けの手順とインフラストラクチャーが推奨されている。

- 暗号と鍵管理に関する政府規制を理解し、それに従う。
- 鍵エスクロー要件を理解し、それに従う。
- 鍵漏洩リカバリー計画を策定する。
- 鍵バックアップ計画を実行に移す。
- 同じデータにアクセスするデバイスや同じデータを処理するデバイスに鍵を安全に配布する。

4.1 暗号的消去

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）」、ISO 27040:2015、および NIST Special Publication 800-88R2 に記載されているように、データ・サニタイズ手法として暗号消去が使用されている場合は、関係するデータ暗号化鍵／鍵ラップ鍵のすべてのコピーの有効で検証可能な破壊を保証する必要がある。健全な鍵管理プロセスでは、関連する鍵のすべてのコピー（使用中のコピーとアーカイブされたコピーの両方）を確実に特定し、それらを検証可能かつ監査可能な方法で破壊できる。

不注意による暗号鍵の紛失はデータの暗号消去を実行した場合と同じ結果になることに注意する必要がある。

4.2 データ量削減技術との併用

重複排除や圧縮を含むデータ量削減の様々な形態をデータ暗号化と組み合わせて使用する場合は順序付けが必要なため、蓄積データ暗号化がシステム・トポロジーに影響を与える。一般的に、データは、暗号化を実行する前に圧縮して、復号化を実行した後に展開する必要がある。

4.3 輸出入の管理

様々な国同士の暗号化技術の輸入と輸出の両方に関する政府規制を理解し、それに従うことが重要である。このような規制の多くでは、強力な暗号化方式の輸入が禁止されている。同様に、平文データと暗号文データの両方を見ることができる強力な暗号化技術は、通常は輸出制限の対象となる汎用の暗号化デバイスと見なされる。これらの問題は、政府間で結ばれた貿易協定の差異によって複雑化しており、大抵の場合、データ暗号化装置と鍵管理装置の両方に適用される。

加えて、政府要件と企業要件のどちらかで鍵エスクローが要求される場合がある。これは、暗号化されたデータを復号化するために必要な鍵をエスクロー内に保管して、特定の状況下で、許可された第三者がその鍵にアクセスできるようにする取り決めである。鍵エスクローは転送中データと蓄積データの両方に対して要求される場合があることに注意すること。

例えば、暗号化技術および装置の輸出に関連した米国規制に関する大量の実用的情報が米商務省産業安全保障局の Web サイト（https://www.bis.doc.gov/index.php/policy-guidance/encryption）で公開されている。

4.4 リカバリー計画

暗号化されたデータのリカバリーには、暗号化されたデータとその復号化に必要な鍵の両方が必要である。その結果、鍵は冗長性を確保するために配布する必要があるが、鍵の漏洩や破損を回避するセキュアな方法で交換する必要がある。意図しない鍵の改変によってもデータへのアクセスが失われるため、鍵管理システムは鍵に対して冗長性と災害対策メカニズムの両方を提供する必要がある。リカバリー計画は鍵が漏洩した場合にも使用できる必要がある。

4.5 コンプライアンス

監査の対象となるストレージ・システムと鍵管理システムのコンプライアンスの側面には、説明責任、追跡可能性、検出と監視、サニタイズ、プライバシー、および法的要件が含まれる。これらの多くのプロセスがコンピューティング・インフラストラクチャー全体に対して実施されるが、監査ロギングをストレージ層にまで広げることが重要である。これは、データの暗号化、復号化、または破壊や鍵の作成、削除、または使用などのイベントに関するセキュアな監査ログの維持を意味する。このような変更の発生元と特定の個人を識別できる十分な情報を収集する必要がある。

5　サマリー

暗号化の使用を通して保護されるデータの管理は、データ・システム・インフラストラクチャーのすべての部分に関係する複雑な取り組みである。データを適切に保護するためのデータ・パスの必要性は、転送中データと蓄積データで大きく異なる。鍵を安全に保護するための鍵管理システムの必要性にその複雑さが反映されている。

すべてのデータを保護する必要はない。ほとんどの場合、転送するデータのごく一部を暗号化で保護する必要があるだけである。データを慎重に評価してデータの機密性面での優先順位とデータの流れを確認することで、暗号化システムの簡素化を実現し、コストのかかる強引なアプローチを回避することができる。

ISO/IEC 27040 は、これらの領域とセキュアなストレージに関連したその他の領域に関する明確なガイダンスを提供している。ユニークな点は、各国のセキュリティおよびストレージ・セキュリティ・コミュニティのベスト・プラクティスをまとめて国際的なガイダンスを提供していることである。

6 謝辞

6.1 執筆者について

Walt Hubis は Hubis Technical Associates のオーナーである。ストレージ・インタフェースとストレージ・セキュリティの標準化組織に関連した専門知識を有し、プロトコルとソフトウェア・インタフェースのほか、革新的で破壊的なコンピューター・ストレージ技術がこれらの標準に与える影響に精通している。Walt には、ストレージ・システム・エンジニアリングの開発職と管理職の両方において 25 年以上の経験があり、RAID やその他のストレージ関連技術の重要な特許をいくつか執筆している。現在は SNIA SSSI Initiative の副議長を務め、Trusted Computing Group Key Management Services Subgroup の議長、IEEE SISWG P1619.3 Key Management subcommittee の議長、および IEEE Security in Storage work group (SISWG)の書記を歴任してきた。電気工学の理学士号を取得している。

Eric Hibbard は、Hitachi Data Systems の CTO Security and Privacy を務め、製品セキュリティ戦略を担当し、製品とサービスにおけるセキュリティ対策とプライバシー対策の統合を統括している。Hibbard 氏は、政府機関（DoD、DoE、および NASA）、教育機関（カリフォルニア大学）、および産業界で 30 年以上のエンタープライズ・クラスの ICT の経験を持つセキュリティおよび IS 監査の上級専門家である。様々な技術に積極的に関与しており、複数の標準開発組織（ISO/IEC、ITU-T、INCITS）と業界団体（SNIA、TCG、DMTF、ODCA、IIC、ISACA、ISSA）で Hitachi と HDS の代表を務めている。現在は、INCITS/CS1 Cyber Security の国際代表、IEEE Information Assurance Standards Committee の議長、Cloud Security Alliance International Standardization Council の共同議長、ABA Electronic Discover & Digital Evidence (EDDE) Committee の共同議長、ABA IoT Committee の共同議長、ABA Cloud Computing Committee の副議長、SNIA セキュリティ TWG の議長、および IEEE Security in Storage WG (SISWG)の副議長を務めている。加えて、ISO/IEC 27050 (Electronic discovery)と ISO/IEC 20648 (TLS for Storage Systems)のドラフト標準だけでなく、最近公開された ISO/IEC 27040:2015 (Storage security)と Rec. ITU-T Y.3500 | ISO/IEC 17788:2014 (Cloud computing - Overview and vocabulary)の編集者でもある。Hibbard 氏は、ISSAP、ISSMP、および ISSEP を中心とした(ISC) 2 CISSP 認定、CCSP 認定、および ISACA CISA 認定を取得している。学歴面では、コンピューター科学の理学士号とデータ通信の能力認定書を取得している。

6.2 査閲者と貢献者

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。

Richard Austin, CISSP	HP
Dr. Alan Yoder	Huawei Technologies Co. Ltd.
Mark Carlson	Toshiba America Information Systems, Inc.
Gary Sutphin	個人
Roger Cummings	Antesignanus Inc.

7　追加情報

セキュリティ TWG を含む SNIA のセキュリティ活動に関する追加情報については、
http://www.snia.org/security 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。

付録 A ISO/IEC 27040 の概要

国際標準化機構（ISO）は、国際電気標準会議（IEC）と共同で、合同技術委員会 1（JTC 1）の小委員会 27（SC 27）の下でストレージ・セキュリティに関する標準を完成させつつある。このことは、SC27 の作業プログラム（付録 B を参照）の重要な要素に ISO/IEC 27001（組織の ISMS 認定に使用される基準）などの ISO/IEC 27000 シリーズとしても知られる情報セキュリティ管理システム（ISMS）に関する国際標準が含まれるため、注目に値する。

新しい SC27 ストレージ・セキュリティ標準の正式名称は、ISO/IEC 27040:2014, *Information technology — Security techniques — Storage security* である。ISO/IEC 27040 の目的は、ストレージ・システムやエコシステムだけでなく、これらのシステム内のデータの保護に関するセキュリティ・ガイダンスを提供することであり、ISO/IEC 27001 で指定された一般的な概念を支持している。また、ISO/IEC 27040 は、組織内のデータ・ストレージと情報セキュリティのリスク管理に関わる管理職と一般従業員、および、必要に応じて、このような活動を支援している外部関係者に関係する。

この標準には、次の重要な定義を含む関連用語も記載されている。

- ***ストレージ・セキュリティ*** ― ストレージ・システムおよびインフラストラクチャーに加えて、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、および管理的制御の適用。

  *初心者向けの注意 1 :*ストレージ・セキュリティは、無許可の開示、変更、または破壊からデータ（およびそのストレージ・インフラストラクチャー）を保護し、その可用性を許可されたユーザに保証することに焦点が当てられる。

  *初心者向けの注意 2 :*このような管理は、本来、予防的、発見的、是正的、抑止的、復元的、または補償的なものである。

- ***データ侵害*** ― 送信、保存、またはそれ以外の処理が行われる保護されたデータの事故的または違法な破壊、損失、改変、無許可の開示、またはアクセスにつながるセキュリティの侵害。

データ侵害は主要な関心領域（一般的なタイプはこの標準で扱われている）であるため、この定義は標準全体を通して極めて重要な役割を担っている。これまで、ストレージ業界は無許可の開示／アクセスのみを懸念してきたが、新しい EU の一般データ保護ルールに沿ったこの業界の新しい定義では破壊、損失、および改変が追加されている。これは、ストレージに関与した個人がデータの損失や破損を引き起こす操作（マイクロコードの更新の失敗など）が原因でデータ侵害に関与したことになる可能性が出てきたことを意味する。

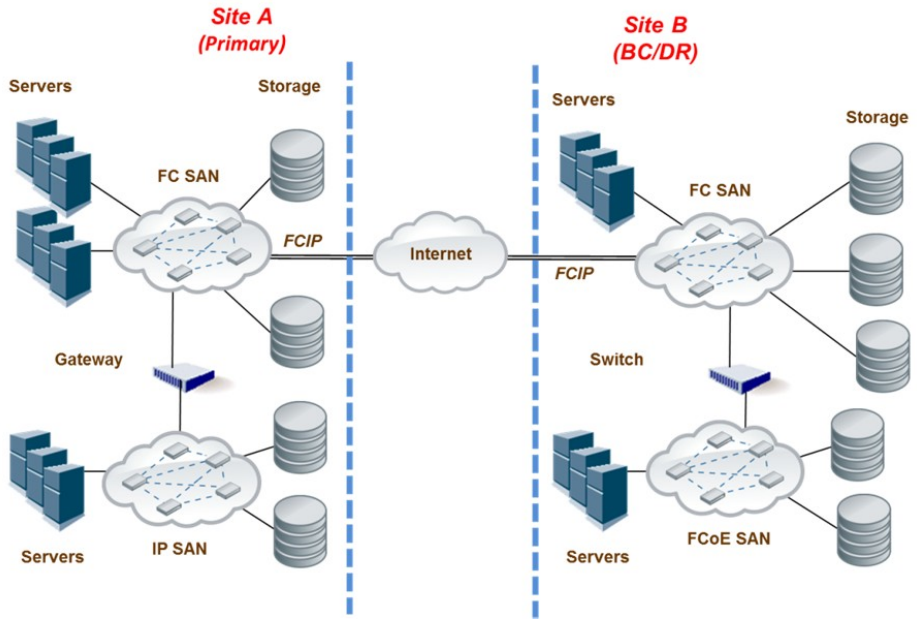
ISO/IEC 27040 は、1) 補助管理と 2) ストレージ・セキュリティの設計と実装という 2 つの角度からストレージ・セキュリティ・ガイダンスにアプローチしている。この両方が、セキュリティの知識が不足しているストレージ・プロフェッショナルやストレージ経験の少ないセキュリティ／監査プロフェッショナルが資料を活用できるように詳しく扱われている。

ストレージ・セキュリティ ー 補助管理

ISO/IEC 27040 の補助管理の条項では、ストレージ・セキュリティ・アーキテクチャーを補助する管理（対策）、それらの関連する技術的管理、およびその他のストレージ以外に適用可能な管理（技術的と非技術的）を特定している。以下の項目が扱われている。

- 直接接続ストレージ（DAS）
- ストレージ・ネットワーキング（様々な種類の SAN と NAS）
- ストレージ管理
- ブロック・ベースのストレージ（ファイバー・チャネルと IP）
- ファイル・ベースのストレージ（NFS、SMB／CIFS、pNFS）
- オブジェクト・ベースのストレージ（クラウド、OSD、CAS）
- ストレージ・セキュリティ・サービス（サニタイズ、データ機密性、およびデータ量削減）

他と比べて特に推奨されているストレージ技術はない。代わりに、特定のストレージ技術が選択または導入された場合にセキュリティの観点から必要とされるものや期待されるものを明確にする形でガイダンスが提供されている。この標準では、図に示すような複雑なシナリオも考慮されている。



（出典：SNIA セキュリティ TWG で作成された ISO/IEC 27040:2014 の図 2）

ストレージ・セキュリティ ー 設計と実装

ストレージ・ソリューションの設計と実装では、中核的なセキュリティ原則に従う必要がある。ISO/IEC 27040 は、ストレージ・セキュリティの観点からこれらの設計原則を扱い、補助管理を活用してストレージ・セキュリティの脅威と脆弱性に対処する。設計ミスは深刻な問題

（データ侵害など）につながる可能性があるということを、基本的な前提としている。
この条項内の資料では以下の内容がカバーされている。

- ストレージ・セキュリティの設計原則（多重防御、セキュリティ・ドメイン、復元力のある設計、およびセキュアな初期化）
- データの信頼性、可用性、および回復力（バックアップと複製だけでなく、災害対策と事業継続性も含む）
- データ保有（長期保有と中／短期保有）
- データの機密性と完全性
- 仮想化（ストレージの仮想化と仮想化されたシステム用のストレージ）
- 設計と実装に関する考慮事項（暗号化と鍵管理の問題、ストレージとポリシーの調整、コンプライアンス、セキュアなマルチテナント、セキュアな自律データ移動）

セキュアなマルチテナントとセキュアな自律データ移動（ILM セキュリティと同様）は、高度な課題であり、様々な用途（クラウド・コンピューティングなど）に使用できる。

ISO/IEC 27040 の付加価値要素

ISO/IEC 27040 の適用可能性と使いやすさを向上させるための重要な取り組みが行われ、以下が組み込まれた。

- ***メディア・サニタイズ*** ― この標準には、様々なタイプのストレージ・メディアをサニタイズする方法に関する詳細情報（NIST SP 800-88r1 と同様）が記載された付録が添付されている。このテクニックには、暗号消去（鍵廃棄）を通した上書きアプローチの使用が含まれる。これは、このトピックの詳細情報を提供する唯一の国際標準であり、多くのベンダーに使用されている DoD 5220.22-M 文書の 1995 年版のように参照できるように構成されている。
- ***ストレージ・セキュリティ管理の選択*** ― 一般の組織では、ISO/IEC 27040 に記載されている 330 を超える管理に対応できないのではないかと判断された。対応がまったく行われなくなってしまう事態を避けるために、セキュリティ基準（機密性、完全性、可用性など）やデータ機密性（低または高）に基づいてストレージ・セキュリティ管理の選択と実装の優先順位付けを支援する付録が作成された。この付録は、ストレージ・システムやエコシステムの監査者がチェックリストとして使用することもできる。
- ***重要なセキュリティ／ストレージの概念*** ― 読者層（セキュリティ、ストレージ、および監査）が多様であるため、特定の概念の共通理解を確保するために特定の「チュートリアル」資料が必要なことが分かってきた。そのため、認証、許可、およびアクセス制御、自己暗号化ドライブ（SED）、サニタイズ、ロギング、N_Port_ID Virtualization（NPIV）、ファイバー・チャネル・セキュリティ、OASIS KMIP などのトピックの概要が付録に記載されている。ファイバー・チャネル資料は、FC-SP-2 やその他の FC セキュリティ・メカニズムの説明が記載された数少ない資料の 1 つであり、特に重要である。

- ***参考文献*** ― 通常、標準の参考文献に大きな価値はない。しかし、ISO/IEC 27040 では、これが、関連するストレージ・セキュリティ情報の参照リストになっているため、事情が異なる。見方によっては、ストレージ・セキュリティに関する中核的原資料と見なすことができる。

サマリー

データ侵害が後を絶たないため、組織は、自分たちのシステムとデータを保護するための新たな方法を模索し続けている。ストレージ・セキュリティは見落とされることが多く、最後の砦としてどうにか使用されている程度である。ISO/IEC 27040 には、この導入を支援する詳細情報が記載されている。

ISO/IEC 27040 は「ガイダンス」標準である（つまり、すべてが「すべき」として指定されている）。このガイダンスの一部または全部を実装*しなければならない*と指定するか、ベンダー向けの資料（例えば、RFP）の場合は、ベンダーが ISO/IEC 27040 ガイダンス（一部または全部）を実装するために必要な能力や機能を*提供しなければならない*と指定することによって、比較的簡単にこのガイダンスを要件に変えることができる。

付録 B ISO/IEC JTC 1/SC27 の概要

国際標準化機構（ISO）は自発的な国際標準の世界最大の開発機関であり、164 の国の標準化団体と 3,368 の技術団体からのメンバーで構成された独立系の非政府組織である[7]。1947 年の設立以来、ISO は、技術、ビジネス、および製造のほとんどすべての側面（例えば、食の安全からコンピューター、農業、医療まで）をカバーする 19,500 を超える国際標準を発行してきた。

1906 年に設立された国際電気標準会議（IEC）は、「電気工学」と総称される電気技術、電子技術、および関連技術のすべてに関する国際標準を策定して発行している世界を主導する組織である[8]。「産業界、商業界、政府機関、試験・研究施設、教育機関、および消費者グループからの 10,000 人を超える専門家が IEC 標準化作業に参加している。」

ISO と IEC は、世界規模で国際標準を開発している 3 つのグローバル姉妹組織のうちの 2 つである（3 つ目は国際電気通信連合（ITU））。必要に応じて、これらの SDO の一部または全部が協力して、国際標準同士が緊密に整合し、相互に補完し合っていることを確認している。「合同委員会［JTC1 など］は、関連分野で働いているすべての専門家の関連知識が国際標準に反映されることを確実にしている。」すべての ISO／IEC 国際標準は、完全な合意に基づいており、ISO／IEC の作業に参加しているすべての国の主要な利害関係者のニーズを反映している。「国の大小に関係なく、すべてのメンバー国に、何を［ISO または］IEC の国際標準にするかに対する投票権と発言権が与えられている。」

小委員会 27（SC27）

JTC1 内部の SC27 は、情報および情報通信技術（ICT）の保護に関する標準の策定を担当している。これには、次のようなセキュリティとプライバシーの両面に関係する汎用の方式、テクニック、およびガイドラインが含まれる。

- セキュリティ要件収集方法
- 情報および ICT セキュリティの管理。特に、情報セキュリティ管理システム（ISMS）、セキュリティ・プロセス、セキュリティ管理、セキュリティ・サービス
- 暗号メカニズムとその他のセキュリティ・メカニズム。情報の説明責任、可用性、完全性、および機密性を保護するためのメカニズムを含むがこれらに限定されない。
- セキュリティ管理支援文書。用語集、ガイドライン、およびセキュリティ・コンポーネントの登録手順を含む。
- ID 管理、生体認証、およびプライバシーのセキュリティ面
- 情報セキュリティ分野の適合性評価、適格性認定、および監査に関する要件
- セキュリティ評価基準および方法論[9]

1990 年 4 月に初の全体会議を開催して以来、SC27 は、120 を超える標準を発行し、

[7] 国際標準化機構（ISO）については、http://www.iso.org/iso/home/about.htm（最終訪問日：2014 年 9 月 15 日）
[8] 国際電気標準会議（IEC）については、http://www.iec.ch/about/?ref=menu（最終訪問日：2014 年 9 月 15 日）
[9] 国際標準化機構／国際電気標準会議［ISO／IEC］、*SC 27 Business Plan October 2013—September 2014*, at 1.2, ISO/IEC JTC 1/SC 27 N12830（2013 年 9 月 30 日）

現在は、75 を超えるプロジェクトが活動中である。これらのプロジェクトと発行された標準に関連した継続的保守を管理するために、SC27 は次の作業部会（WG）に分かれている[10]。

- WG1：情報セキュリティ管理システム（ISMS）
- WG2：暗号メカニズムとセキュリティ・メカニズム
- WG3：セキュリティの評価、テスト、および仕様化
- WG4：セキュリティ管理とセキュリティ・サービス
- WG5：ID 管理技術とプライバシー技術
- SWG-M：管理項目の特別作業部会
- SWG-T：横断的項目の特別作業部会

[10] *ISO/IEC JTC 1/SC 27 IT Security techniques*、国際標準化機構、http://www.iso.org/iso/iso_technical_committee?commid=45306（最終訪問日：2014 年 5 月 15 日）

Bibliography

[01] ISO/IEC 27040:2015, Information technology – Security techniques – Storage security

[02] ISO/IEC 11770-1:2010, Information technology -- Security techniques -- Key management -- Part 1: Framework

[03] NIST Special Publication (SP) 800-57 Part 1-3, Recommendation for Key Management

[04] NIST Special Publication (SP) 800-88 (R2), Guidelines for Media Sanitization

[05] NIST Special Publication (SP) 800-111, Guide to Storage Encryption Technologies for End User Devices

[06] NIST Special Publication (SP) 800-132, Recommendation for Password-Based Key Derivation Part 1: Storage Applications

[07] Storage Networking Industry Association (SNIA), Storage Security: Fibre Channel Security, Draft

[08] Storage Networking Industry Association (SNIA), Storage Security: Sanitization

[09] IETF RFC 1334, PPP Challenge Handshake Authentication Protocol (CHAP)

[10] IETF RFC 2246, The TLS Protocol Version 1.0

[11] IETF RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH

[12] IETF RFC 2406, IP Encapsulating Security Payload (ESP)

[13] IETF RFC 2451, The ESP CBC-Mode Cipher Algorithms

[14] IETF RFC 3686, Using Advanced Encryption Standard (AES) Counter Mode

[15] IETF RFC 3720, Internet Small Computer Systems Interface (iSCSI)

[16] IETF RFC 3721, Fibre Channel Over TCP/IP (FCIP)

[17] IETF RFC 3723, Securing Block Storage Protocols over IP

[18] IETF RFC 4171, Internet Storage Name Service (iSNS)

[19] IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1

[20] IETF RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2

[21] OASIS Key Management Interoperability Protocol Specification Version 1.2