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：
ファイバチャネルセキュリティ

バージョン 1.01

2016 年 9 月 6 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。このホワイトペーパーでは、ストレージエリアネットワーク（SAN）に適用される標準に記載されたファイバチャネル（FC）セキュリティガイダンスの概要を示す。また、組織の特定のニーズを満たす FC セキュリティプログラムを開発する場合の追加の SNIA ガイダンスも提供する。*

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。

3 条項 BSD ソフトウェアライセンス

Copyright (c) 2016、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。

改訂履歴

版	日付	セクション	作成者	備考
VO.1	*4/2/2015*	全体	Eric Hibbard	初稿
V1.0	*5/20/2016*	全体	Eric Hibbard	最終 1.0 版
V1.01	*9/6/2016*		Eric Hibbard	細部の修正

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

ファイバチャネルは、データセンタで使用され、特別なセキュリティ保護を備えておらず、必要ともしないネットワーキングの特殊な形態と見なされることが多い。このような見方は正確ではないが、ファイバチャネルインフラストラクチャを適切に保護するための詳しい内容が公開されていないのも事実である。この SNIA 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ファイバチャネルに関する有益な情報を提供する。

1 はじめに

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の保護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）。この標準の適用範囲は極めて広いが、特定の重要なトピックに関する詳細が欠落している。

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利用してファイバチャネル（FC）セキュリティに特化した内容を補足することである。このホワイトペーパーでは、ファイバチャネルに関する背景情報を示し、FC セキュリティ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、FC ベースのストレージの保護に役立つ追加情報を提供する。

2 ストレージ技術の概要

このセクションでは、セキュリティの説明とガイダンスの前段階として、主要なストレージ技術について簡単に説明する。

2.1 ストレージエリアネットワーク（SAN）

ストレージエリアネットワーク（SAN）は、ブロックレベルのネットワークアクセスをストレージに提供するために特化した高速ネットワークである。一般的に、SAN は、様々な技術、トポロジー、およびプロトコルを使用して相互接続されたホスト、スイッチ、ストレージエレメント、およびストレージデバイスで構成される。また、複数のサイトに及ぶ場合もある。

SAN の主な用途を以下に示す。

- アプリケーションの可用性の向上（複数のデータパスなど）
- アプリケーションの性能の向上（ストレージ機能のオフロードやネットワークの分離など）
- ストレージの利用と有効性の改善（ストレージリソースの統合や階層ストレージの実現など）
- データの保護とセキュリティの向上

加えて、SAN は、組織の事業継続マネジメント（BCM）[1]活動において重要な役割を果たす。

SAN は、ストレージデバイスがホストに直接接続されているかのように見せることができる。ホストへのストレージの見え方のこのような単純化は、様々な種類の仮想化を利用して実現される。

SAN の多くはファイバチャネル（FC）技術[2]をベースにしており、オープンシステムやメインフレーム専用のバリエーションに対してファイバチャネルプロトコル（FCP）を利用する。加えて、Fibre Channel over Ethernet（FCoE）を利用することにより、既存の高速イーサネットインフラストラクチャ上での FC トラフィックの移動や 1 本のケーブル上でのストレージプロトコルと IP プロトコルの共存を可能にする。他にも、中小規模の組織で FC の安価な代用品として広く使用されている Internet Small Computing System Interface（iSCSI）や高性能なコンピューティング環境で広く使用されている InfiniBand などの技術が利用できる。さらに、異なる SAN 技術間でデータを移動するためにゲートウェイを使用できる。

2.2 ファイバチャネル（FC）

SNIA の辞書には、ファイバチャネルは次のように記載されている。

> *オープンシステムストレージへのアクセス（FCP）、メインフレームストレージへのアクセス（FICON）、ネットワーキング（TCP/IP）などの複数のプロトコルをサポートできるシリアル I/O 相互接続*

ファイバチャネルは、様々な速度で動作する様々な銅線リンクと光リンクを使用したポイントツーポイント、アービトレイテッドループ、およびスイッチトポロジーをサポートする。

ANSI INCITS 470-2011 (FC-FS-3) には、ファイバチャネルプロトコル（FCP）が 5 つのレイヤまたはレベルで構成されたネットワークアーキテクチャとして記載されている。次の表で、レベルのそれぞれについて簡単に説明する。

[1] 「事業継続マネジメント（BCM）」は、ISO/IEC 27002:2013 において、災害復旧（DR）や一般的な事業継続性（BC）の問題などのトピックを扱う場合に使用されている。昔は、DR と BC がセキュリティコミュニティによって別々に対処されていたが、最近の傾向では、BCM の要素として取り扱われている。

[2] ファイバチャネルスイッチ型ファブリック（FC-SW）トポロジーをベースにした SAN は、FC ファブリックと呼ばれることがある。

FC-4	プロトコルマッピングレイヤ（SCSI、IP、FICON などのアプリケーションプロトコルが FC-2 に配信するためのプロトコルデータユニットにカプセル化される）
FC-3	共通サービスレイヤ
FC-2	ネットワークレイヤ（ファイバチャネルの核であり、メインプロトコルを定義する）
FC-1	データリンクレイヤ（信号の回線符号化を実装する）
FC-0	物理レイヤ（ケーブル配線やコネクタなど）

FC-2 レイヤは、情報転送に必要な FC フレーム形式、トランスポートサービス、および制御機能を定義する。ファイバチャネル汎用サービスは、ANSI INCITS 463-2010 (FC-GS-6) で規定された FC-4 レベルで共通トランスポート（CT）を共有する。CT は、ファイバチャネル構造の利用を促進する一連のサービスパラメータを使用してサービス（ディレクトリサービスなど）へのアクセスを提供する。

ファイバチャネルポートは、FC リンク（チャネルとも呼ばれる）経由で通信するノードとのやり取りに使用されるハードウェア経路である。FC は、様々な種類のポートを定義するが、このホワイトペーパーに関連するものは次のとおりである（図 1 を参照）。

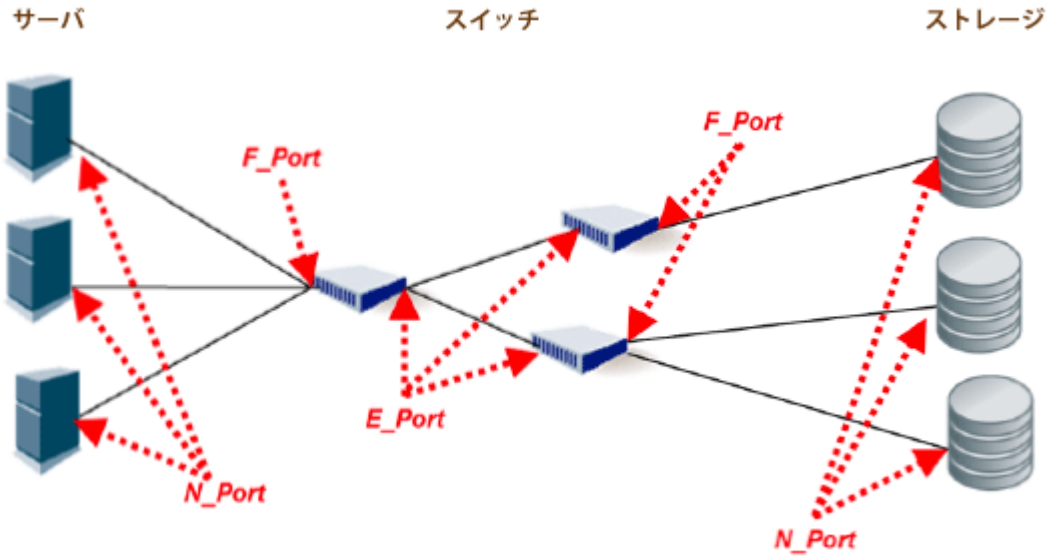


図 1 ― FC ポートの種類

— **N_Port**：ノードを FC スイッチに接続するために使用されるネットワークまたはノードポート。ホスト内のイニシエーターHBA（ホストバスアダプタ）にすることも、ストレージアレイ上のターゲットポートにすることもできる。

— **F_Port**：FC ファブリックをノード（N_Port）に接続するために使用されるスイッチポート。

— **E_Port**：FC スイッチ同士を接続（カスケード）するために使用されるエクステンダポート。2 つの E_Port 間の接続がスイッチ間リンク（ISL）を形成する。

— **NP_Port**：複数の物理 N_Port のプロキシとして機能するスイッチポート。スイッチが NPV モード（後述）で動作している場合は、スイッチをコアネットワークスイッチに接続するインタフェースが NP_Port として設定される。

2.3 FC 仮想化

FC SAN 内部では、2 つの相補的仮想化技術が使用されており、このセクションではそれらについて説明する。これらは NPIV（N_Port ID 仮想化）と NPV（N_Port 仮想化）と呼ばれている。

2.3.1 N_Port_ID 仮想化（NPIV）

非仮想化環境では N_Port と N_Port_ID が一対一で関連付けられるのに対して、NPIV は単一の物理 N_Port に複数のワールドワイドポートネーム（WWPN）を割り当てることを可能にするため、N_Port に複数の N_Port_ID が関連付けられる。NPIV に対応した物理 N_Port は、通常の FLOGI プロセスの後に、追加のコマンドを発行して複数の WWPN を取得して登録し、複数の N_Port_ID（WWPN ごとに 1 つずつ）を受信することができる。

ファイバチャネルスイッチも NPIV をサポートする必要がある。これは、リンクの相手側の F_Port がホストから送られてくる複数の WWPN と複数の N_Port_ID を「検出」するため、この動作の処理方法を理解している必要があるからである。

該当するすべての WWPN を登録したら、それらの WWPN のそれぞれを SAN ゾーニングや LUN の提示に使用できる。物理 WWPN と仮想 WWPN は区別されない。どちらも全く同じように動作し、全く同じように使用できる。

NPIV を実装すれば、サーバ上に膨大な数の仮想マシンが稼働している場合でも、1 台の仮想マシンしかアクセスできないゾーンを FC SAN 内に設置できる。加えて、仮想 WWN は仮想マシンに従うため、ホスト間で移行する仮想マシンには、ターゲットホストが LUN に確実にアクセスできることを保証するための特別な変更は必要ない。これは、仮想マシンにそのアクセス能力があることによって、ホストが LUN へのアクセス能力を継承することを意味する。

NPIV によって作成された N_Port_ID のそれぞれがホスト、ネットワークファブリック、およびストレージ内のリソースを消費するため、大量の仮想ホストでスケーリング問題を解決する場合は注意が必要なことに留意すべきである。

製造元から提供される機能によっては、NPIV を 3.3 節で説明する他のファイバチャネルセキュリティメカニズムと組み合わせて使用できる。

2.3.2 N_Port 仮想化（NPV）

NPIV は主としてホストベースのソリューションであるのに対して、NPV は主としてスイッチベースの技術である。NPV は、大規模な SAN 展開におけるスイッチの管理とオーバーヘッドを減らすように設計されている。

非仮想化環境では、239 個のドメイン ID[3]という制限（したがって、239 台のスイッチという SAN の制限）を上回る大量のエッジスイッチ（大規模なブレードサーバと組み込みスイッチの組み合わせによる構成など）が SAN に必要な場合がある[4]。NPV は、コアスイッチからはファイバチャネルホストに見え、接続先のデバイスからは通常のファイバチャネルスイッチに見える複数のエッジスイッチ[5]間でコアスイッチのドメイン ID を共有することにより、ドメイン ID の制限を緩和する。コアスイッチは、F_Port 機能（ログインやポートセキュリティなど）とすべてのファイバチャネルスイッチング機能を提供する。

NPV の機能の鍵は、F_Port に接続し、NPV 対応スイッチ（通常はエッジスイッチ）上の他の N_Port のプロキシとして機能する新種のファイバチャネルポートである NP_Port の導入である。NP_Port は、相手側の F_Port には NPIV 対応ホストのように「見える」。NPV 対応スイッチは、接続先の N_Port の代わりに、NPIV[6]経由で追加の WWPN を登録（および追加の N_Port_ID を受信）する。物理 N_Port にはこの動作は見えないため、そのサポートを必要としない。すべては NPV に対応したスイッチによって処理される。

また、NPV は、ネットワーク管理者が FCoE ホストを FCoE 非対応 SAN に接続できるようにし、サードパーティの相互運用性の問題を単純化する。これは、NPV に対応したファイバチャネルモジュールがドメイン処理に参加したり、ローカルスイッチングを実行したりしないためである。これにより、相互運用性モードに必要な制限なしでマルチベンダートポロジーを実装できる。

一部のベンダーのスイッチ実装は、NPV for Fibre Channel over Ethernet（FCoE-NPV）もサポートすることにより、ファイバチャネル NPV 上に構築される。FCoE-NPV は、ファイバチャネル NPV モードと同様のメリットを純粋な FCoE 実装にもたらす。スイッチは、FIP スヌーピング[7]を使用しながら、FCoE トラフィックを識別し、分離を維持してセキュリティを提供する。FCoE NPV は、VNP 用の新しいポートの種類（仮想 NPV ポート）も構築する。

製造元から提供される機能によっては、NPV を 3.3 節で説明する他のファイバチャネルセキュリティメカニズムと組み合わせて使用できる。

---

[3] ファブリック内の特定のスイッチを識別する番号。
[4] すべてのベンダーが 239 個の最大ドメイン ID をサポートしているわけではない。
[5] エンドユーザデバイスに直接接続されたスイッチは「エッジ」または「アクセス」スイッチと呼ばれる。一般的に、ネットワークのバックボーンは、スイッチングが終了してルーティングが開始される場所であり、コアスイッチがスイッチングエンジンとルーティングエンジンの両方（および場合によってファイアウォール）として機能している。
[6] NPV の正しい動作を可能にする重要な要素は、コア／アップストリームファイバチャネルスイッチ上の N-Port ID 仮想化（NPIV）に対するニーズである。
[7] FIP スヌーピングは、マルチホップ FCoE 環境で使用され、FIP スヌーピングに対応したデータセンターブリッジ（DCB）デバイスが FIP フレームを監視してそれらのフレーム内の情報に基づいてポリシーを適用するために使用可能なフレーム検査手法である。

3 FC および SAN セキュリティの背景

このセクションでは、特に SAN とファイバチャネルに多く見られる脅威の形態とセキュリティ対策について説明する。

3.1 脅威

ISO/IEC 27040:2015 ではストレージのセキュリティリスクと脅威について高いレベルで解説されているが、このホワイトペーパーにはファイバチャネルに関連したより具体的な情報を含めている。ファイバチャネルの実装と展開で発生する可能性のある重大な脅威[8]を以下に列挙する。

- *ストレージの窃盗*：ストレージメディアやストレージデバイスの窃盗は、データへのアクセスを得るためだけでなく、データの正当な使用を拒否するために行われる可能性もある。
- *ストレージトラフィックのスニッフィング*：専用ストレージネットワークまたは共有ネットワーク上のストレージトラフィックは、データ、メタデータ、およびストレージプロトコル信号処理を暴露するパッシブネットワークタップやトラフィックモニタリングを介して傍受される可能性がある。傍受されたトラフィックに認証の詳細が含まれていた場合は、攻撃者がその情報をリプレイ[9]（再送信）して攻撃をエスカレートさせる可能性がある。
- *ネットワークの中断*：基礎となるネットワーク技術に関係なく、ユーザとストレージシステム間のネットワークに対して引き起こされるソフトウェア的中断や輻輳は、ストレージ機能の低下または無効化をもたらす可能性がある。
- *WWN のなりすまし*：攻撃者が、ストレージシステムへのアクセス権を取得して、データまたはメタデータのアクセス／変更／拒否を行う。
- *ストレージの見せかけ*：攻撃者が、不正なストレージデバイスを挿入して、ホストから提供されるデータまたはメタデータのアクセス／変更／拒否を行う。
- *データの破損*：不正なホストがストレージへのアクセス権を取得した場合に、データの偶発的または意図的な破損が生じる可能性がある。
- *不正なスイッチ*：攻撃者が、不正なスイッチを挿入して、ファブリック（コンフィギュレーション、ポリシー、セキュリティパラメータなど）に対する偵察を実行したり、その他の攻撃を容易にしたりする。
- *サービス拒否（DoS）*：攻撃者は、ストレージネットワークをエラーメッセージで溢れさせたり、ネットワーク内部の特定のシステムに負荷を掛けたりする様々な方法でデータへのアクセスを中断、阻止、または低速化することができる。

[8] リスクは特定の環境内の状況に左右されるため議論できない。リスクとは、組織に不利益をもたらす出来事が起きる可能性とその影響を意味する。脅威は一般的な方法で分類できるが、脅威が具現化する可能性とその影響を環境に基づいて評価する必要がある。

[9] リプレイ攻撃は、正当なデータ伝送が不当にまたは不正に再度行われるネットワーク攻撃の一形態である。

3.2 SAN セキュリティ

SAN に関連するセキュリティ管理は次のカテゴリに分類される。

— **アクセス制御**：SAN 上でのアクセス制御は、ゾーニング、論理ユニット（LUN）マスキング、およびポートバインディングメカニズムの応用を通して実装される。また、SAN 上でのアクセス制御は、より馴染みのあるユーザ ID やグループ ID の類ではなく、マシン ID に基づく。

  — **ポートバインディング**：SAN では識別にワールドワイドネーム（WWN）が使用される。ポートバインディングは、物理ポート経由の接続を許可する WWN を指定する SAN のセキュリティメカニズムである。この関連付けは、攻撃者によるスヌーピングやスプーフィングの試みを抑制できるため、可能な限り使用すべきである。

  — **ゾーニング**：SAN ファブリックは、複数のゾーンに分割することによって、特定のホストやストレージデバイスから SAN の一部を隠すことができる。ソフトゾーニングは、ホストがネームサーバ経由で検出されないストレージデバイスには接続しないという前提の下に、SAN ファブリックネームサーバの問い合わせに対する応答を制限することをベースにしている。一部の新型のスイッチは、SAN スイッチ上の物理ポート番号を使用してトラフィック転送を制限する WWN に基づく「ハード」（スイッチ ASIC）ゾーニングを可能にする。これは、正しいホスト動作に依存しないうえ、特に、ホスト ID のスプーフィングに強いため、よりセキュアなゾーニング手法と言える。

  — **LUN マスキング**：ストレージデバイスは、論理ユニット番号（LUN[10]）で識別される論理ユニットに分割できる。LUN マスキングは、一部のホストから LUN を隠すことを意味する。

— **認証**：SAN では、各スイッチが SAN 内の通信相手となる他のスイッチの ID を確認し合うことにより、不正なスイッチが SAN に参加しないようにすることが重要である。同様に、SAN 内のノード（ストレージデバイスやホストなど）は、認証を導入してデータに対する不正アクセスから保護する必要がある。

— **暗号化**：SAN 上で暗号化を使用してデータの機密性を保証する主な場合は 2 つあり、1) 転送中データと 2) 蓄積データである。機密性と価値の高いデータ[11]は、SAN 内を転送中はもちろん、ストレージデバイス上に蓄積中も暗号を使って保護する必要がある。

[10] よく業界の混乱の元になるのが論理ユニット（論理ブロックアドレスの連続配列）を「LUN」と呼ぶ慣例である。一般的に、LUN に言及した場合は、基礎となる論理ユニット、つまり、ストレージそのものを指すのであって、ホストに提示するために任意に割り当てられた番号ではない。

[11] 「機密性と価値の高い」は、組織がデータを機密扱いにしているか、何が実際にどこに保存されているかを認識していることを前提とする。そうでない場合は、その場所に保存されている可能性のある最も機密性の高いデータに合わせて適切なレベルの保護を行う必要がある。

3.3 ファイバチャネルセキュリティの概要

ファイバチャネルのファブリックは、離れた場所に設置された複数のサイトにわたって展開することができるが、その場合は、一貫したコンフィギュレーションと適切なアクセス制御を保証するために使用可能なセキュリティサービスが不可欠である。

ANSI INCITS 496-2012, Information Technology - Fibre Channel - Security Protocols - 2 (FC-SP-2) は、ファイバチャネルのエンティティを認証したり、セッション暗号鍵をセットアップしたり、パラメータをネゴシエートしてフレーム間の完全性と機密性を保証したり、ポリシーを定義してファイバチャネルファブリック全体に配布したりするためのプロトコルを規定している。FC-SP-2 には、FC 標準には珍しくコンプライアンス要素が含まれていることも注目に値する。

FC-SP-2 で規定されたセキュリティアーキテクチャは次の要素で構成される。

a) *認証インフラストラクチャ* ― 秘密ベース、証明書ベース、パスワードベース、事前共有鍵ベースなどの様々な認証インフラストラクチャ向けのアーキテクチャを定義する。

b) *認証* ― 通信するエンティティ同士で ID を確認できるようにするための認証プロトコルを定義する。2 つのエンティティは、認証が必要かどうかとどの認証プロトコルを使用するかをネゴシエートする。認証は、次のプロトコルのいずれかを使用して、スイッチ間、ノード／スイッチ間、およびノード間で定義される（図 2 を参照）。

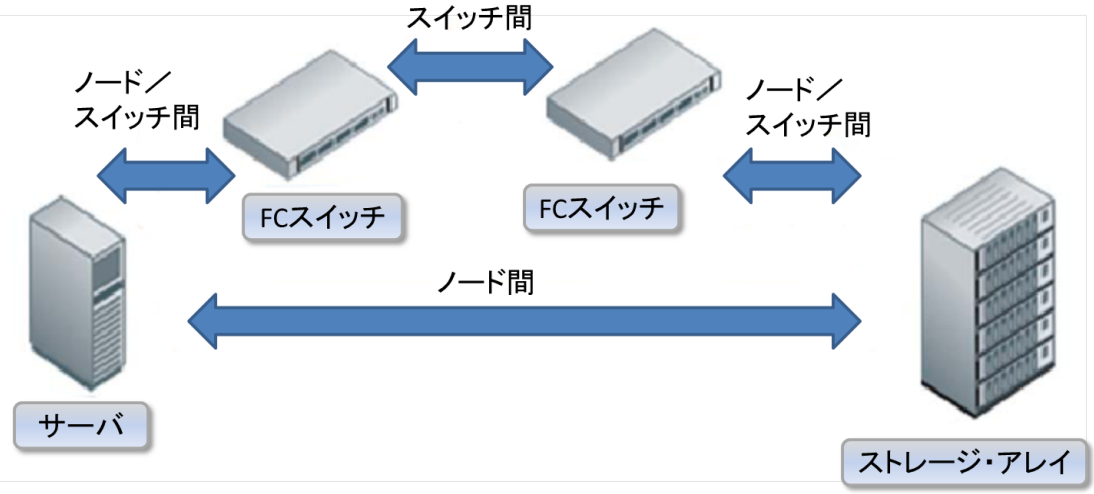


図 2 ― FC 認証

- Diffie-Hellman Challenge Handshake Authentication Protocol（DH-CHAP）（必須、3.3.1 を参照）
- Fibre Channel Certificate Authentication Protocol（FCAP）
- Fibre Channel Password Authentication Protocol（FCPAP）
- Fibre Channel Extensible Authentication Protocol（FCEAP）
- The Security Association Management Protocol（IKEv2-AUTH）

セキュリティアソシエーション ― ファイバチャネルに適したインターネット鍵交換プロトコルバージョン 2（IKEv2）[12]プロトコルのサブセット（つまり、セキュリティアソシエーション管理プロトコル）がエンティティ間のセキュリティアソシエーションを確立するために規定されている（3.3.4 を参照）。

暗号の完全性と機密性 ― フレーム間の暗号の完全性と機密性、リプレイ保護、およびトラフィック起源認証（トラフィックが指定されたエンドポイントから送られてくることの確認）が ESP_Header を使用して実現される（3.3.2 を参照）。CT_Authentication（3.3.3 を参照）を利用して、暗号の完全性と機密性、リプレイ保護、およびトラフィック起源認証を共通トランスポート情報ユニットに提供できる。ESP_Header 処理と CT_Authentication 処理は独立して動作する。

許可（アクセス制御） ― ファブリックポリシーは、次の 2 種類があり、基本的な許可制御を提供する。

- ファブリック全体のデータを含み、ファブリックのすべてのスイッチに配布されるポリシー
- スイッチ単位のデータを含み、個別のスイッチに送信されるポリシー

ファブリックポリシーは、ファブリックを構成可能なスイッチとファブリックに接続可能なノードを制御するために使用できる。さらに、ポリシーは、ファブリック環境内のトポロジー制限（他のスイッチに接続可能なスイッチやスイッチに接続可能なノードなど）を指定するためにも使用できる。

ファブリックポリシーは、ファブリックに対する管理アクセス、認証選択肢を管理する能力、およびファブリックエンティティ（ノードやスイッチなど）用のオプションのセキュリティ属性を指定できる能力を制御するためのメカニズムも提供する。ファブリックに対する管理アクセスは、共通トランスポートまたは IP アクセスに対して制御できる。

FC-SP-2 標準の 4.5 節から引用した図 2 は、認証プロトコルとセキュリティアソシエーションの関係を示している。規定された認証プロトコルは、オプションの共有鍵設定を使用した相互認証を実行できる。認証トランザクションの最終段階で計算される共有鍵は、セキュリティアソシエーションの確立に使用できる。

[12] IKEv2 は、IETF RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2) で規定されている。

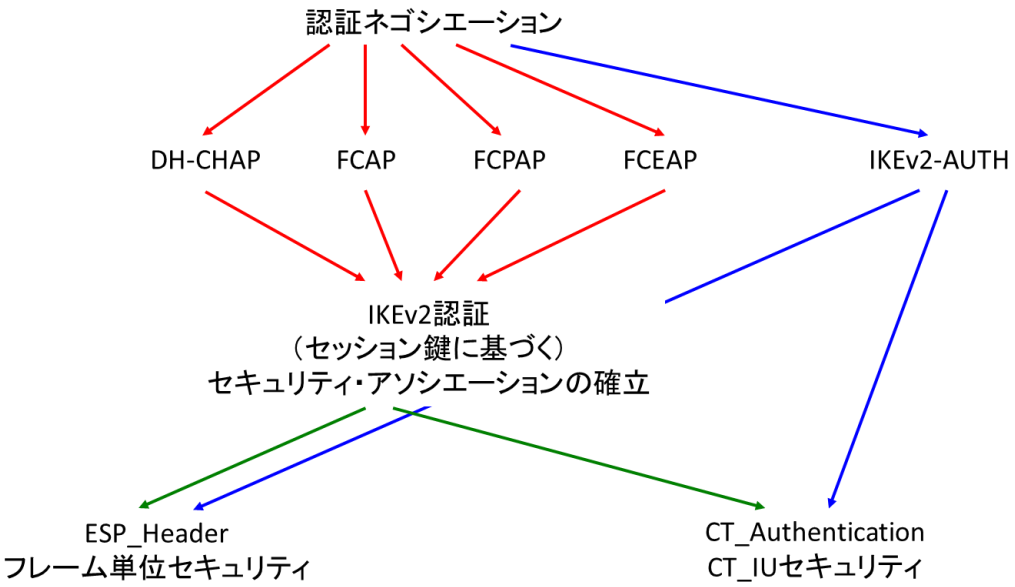


図 2 ― FC-SP-2 認証プロトコルとセキュリティアソシエーションの関係

3.3.1 DH-CHAP 認証

DH-CHAP は、CHAP アルゴリズムとオプションの Diffie-Hellmann アルゴリズムを使用する秘密ベースの認証および鍵管理プロトコルである。DH-CHAP は、認証イニシエーターと認証レスポンダー間の一方向または双方向認証を提供する。このプロトコルの Diffie-Hellmann 部分が使用されない場合は、DH-CHAP がその処理を CHAP プロトコルの処理まで縮小する。これは、NULL DH アルゴリズムを使用した DH-CHAP と呼ばれている。すべての FC-SP 準拠実装で NULL DH アルゴリズムを使用した DH-CHAP をサポートする必要がある。FC-SP-2 準拠を主張するには、実装で 2048 ビット DH アルゴリズムを含む AUTH-A コンプライアンス要素（FC-SP-2 の付録 A で規定されている）をサポートする必要がある。

認証アルゴリズムの特定に加えて、FC-SP-2 は、認証がスイッチ間、デバイス／スイッチ間、およびデバイス間エンティティに対して定義される（図 2 を参照）ことと、プロトコルで相互認証をサポートできることを規定している。つまり、該当する場合は、対応するまたは準拠する製品で次のそれぞれを実装する必要もある。

— スイッチ間 ― この種のエンティティ間の認証を含む製品は、スイッチを認証できるだけでなく、スイッチから認証されることができる必要もある。

— デバイス／スイッチ間 ― この種のエンティティ間の認証を含む製品は、デバイスの観点では、スイッチを認証できるだけでなく、スイッチから認証されることもできる必要があり、スイッチの観点では、デバイスを認証できるだけでなく、デバイスから認証されることができる必要もある。

— デバイス間 ― この種のエンティティ間の認証を含む製品は、デバイスを認証できるだけでなく、デバイスから認証されることができる必要もある。加えて、各デバイスがこの認証を実行する前に該当するデバイス／スイッチ間認証を完了する必要がある。

FC-SP-2 に準拠した製品は、エンティティがいつでも他のエンティティから再認証されるように再認証も実装する必要がある。

3.3.2 ESP_Header

ESP_Header は、起源認証、完全性保証、アンチリプレイ保護、および機密性を提供する FC-2 ファイバチャネルフレーム用のセキュリティプロトコルである。

ANSI INCITS 470-2011, *Information Technology - Fibre Channel - Framing and Signaling* - 3 (FC-FS-3) は、ファイバチャネルフレーム内部で使用可能なオプションヘッダを規定している。これらのオプションヘッダである ESP_Header と ESP_Trailer は、フレームペイロードの暗号化をサポートするために使用されるメカニズムであり、重要なセキュリティの役割を担っている。

RFC 4303 で規定されたセキュリティペイロードのカプセル化（ESP）は、IP パケットの機密性、データ起源認証、およびアンチリプレイ保護を提供する汎用メカニズムである。FC-SP-2 は、ファイバチャネルでの ESP の使用方法を規定している。

FC-FS-3 には、「エンドツーエンドの ESP_Header 処理はトランスポートモードで FC フレームに適用する必要があり（RFC 4303[13]を参照）、リンク間の ESP_Header 処理はトンネルモード[14]で FC フレームに適用する必要がある（RFC 4303 を参照）。認証オプションを使用する必要があり、機密性は 2 つの通信する FC_Port でネゴシエートできる（FC-SP-2 を参照）」と記載されている。

注意 ― リンク間の ESP_Header 処理の意図する用途は、すべての Nx_Port[15]で ESP を使用することなく、ファブリック内またはファブリック間のリンクを保護することである。

3.3.3 CT_Authentication

ファイバチャネルは、ファイバチャネルトラフィックの異なる部分にセキュリティサービスを提供する 2 つのセキュリティプロトコル（ANSI INCITS 463-2010, Information Technology - Fibre Channel - Generic Services - 6 (FC-GS-6) で規定された ESP_Header（3.3.2 を参照）と CT_Authentication）を定義する。CT_Authentication プロトコルは、制御情報を伝送するための共通トランスポート情報ユニットの起源認証、完全性保証、アンチリプレイ保護、およびオプションで機密性保護を提供する。

FC フレームレベルで機能する ESP_Header とは異なり、CT_Authentication は、共通トランスポート（CT）レベルで機能し、ファイバチャネル構造を利用しやすくする一連のサービスパラメータを使用してサービス（ディレクトリサービスなど）へのアクセスを提供する。

---

[13] IETF RFC 4303, IP Encapsulating Security Payload (ESP) に最新版の ESP の記述がある。この ESP は、機密性、データ起源認証、コネクションレス型完全性、アンチリプレイサービス（部分列完全性の形態）、および制限付きトラフィックフロー機密性を提供するために使用される。

[14] 「トンネルモード」では、オリジナルのパケット／フレームのヘッダを暗号化することによって内部ルーティング情報が保護されるのに対して、「トランスポートモード」では、ペイロードが暗号化を使用して保護されるだけである。

[15] Nx_Port という用語は、N_Port（ノードポート）と NL_Port（ノードループポート）のどちらかを指すために使用される。

3.3.4 ファイバチャネルセキュリティアソシエーション

前述のように、特定のトラフィックのクラスを保護するために 2 つのメカニズムを使用できる。ファイバチャネルフレームを保護する ESP_Header と共通トランスポート情報ユニットを保護する CT_Authentication である。2 つのファイバチャネルエンティティ（ホスト、ストレージ、またはスイッチ）間の ESP_Header プロトコルと CT_Authentication プロトコルのセキュリティアソシエーションは、ファイバチャネルセキュリティアソシエーション管理プロトコル（FC-SP-2 で規定されている）によってネゴシエートされる。このプロトコルは、鍵交換プロトコルバージョン 2（IKEv2）の修正されたサブセットであり、中核的処理は同じだが、ファイバチャネル AUTH プロトコルを使用して IKEv2 メッセージを伝送する。IETF RFC 4595, Use of IKEv2 in the Fibre Channel Security Association Management Protocol に、IKEv2 のファイバチャネル使用に関する追加情報が記載されている。

注意 － ファイバチャネルセキュリティアソシエーションには、1 つのプロトコル（ESP_Header と CT_Authentication のどちらか）しか適用できない。

3.3.5 FC-SP ゾーニング

既存のゾーニング定義および実装との下位互換性を維持するために、FC-SP-2 には、ANSI INCITS 461-2010, Information Technology - Fibre Channel - Switch Fabric - 5（FC-SW-5）と ANSI INCITS 463-2010, Information Technology - Fibre Channel - Generic Services - 6（FC-GS-6）で規定された拡張ゾーニングモデルのバリアントが FC-SP ゾーニングとして記載されている。これは、拡張ゾーニングモデルの一般的な概念に従っているが、ゾーニング管理や適用を他のポリシー管理や適用から完全に切り離している。

ファブリックポリシーとゾーニングポリシーは、次の 3 種類のスイッチの定義を使用したファブリック内のポリシー情報の非対称分布を可能にする。

a) ホストスイッチ：すべてのポリシーオブジェクトとすべてのノード間（ゾーニング）情報を保持するスイッチ

b) 自律スイッチ：個別のスイッチ単位ポリシーオブジェクト、すべてのファブリック全体ポリシーオブジェクト、およびすべてのノード間（ゾーニング）情報を保持するスイッチ

c) クライアントスイッチ：スイッチ単位ポリシーオブジェクト、すべてのファブリック全体ポリシーオブジェクト、および必要に応じてホストスイッチから抽出したノード間（ゾーニング）情報の処理に関するサブセットを保持するスイッチ

4　ISO/IEC 27040 内の FC ガイダンスの要約

ISO/IEC 27040 を使用して関連するファイバチャネル制御を特定する場合は、その資料が少なくとも 1) ストレージネットワーキングと 2) ブロックベースのストレージの 2 カ所に配置されていることを覚えておくことが重要である。

4.1　FC SAN セキュリティ

SAN の一部としてのファイバチャネルの使用に関連付けられた ISO/IEC 27040 ガイダンスは、FCP ノード（ホストやストレージなど）の管理、スイッチベースの制御の実装、および FC SANS の相互接続の管理に焦点が当てられている。このガイダンスの要約を以下に示す。

— アクセス制御リスト（ACL）、バインディングリスト、FC-SP-2 ファブリックポリシーなどのテクニックを使用してスイッチ上のホストアクセスを制限することで FCP ノードアクセスを制御する。仮想化ホストの場合は、NPIV（N_Port_ID 仮想化）に対応した HBA を使用して、個別の N_Port_ID を仮想ホストに割り当てる。

— ACL、バインディングリスト、FC-SP-2 ファブリックポリシーなどのテクニックを使用してスイッチ相互接続を制限することでスイッチベースの制御を実施する。加えて、FC SAN ファブリックではゾーニングを使用する必要があり、ハードゾーニングの方が望ましい。デフォルトのゾーンとゾーンセット（最小特権状態が前提）は慎重に使用すること。基本ゾーニングがターゲット環境のセキュリティ対策として不十分な場合は、ベンダーがサポートしているのであれば、FC-SP ゾーニングなどのより強力なテクニックを使用すること。また、スイッチ上の未使用ポートは無効にすることも大切である。

— 必要なスイッチ、エクステンダ、ルータ、およびゲートウェイを、要件を満たすように設定することで複数の FC SAN を安全に相互接続する。残念なことに、ISO/IEC 27040 には「要件を満たす」とはどういうことかについて、詳しい説明が記載されていない。

全体として、ISO/IEC 27040 には FC SAN の保護に関するガイダンスが不足している。

4.2　FC デバイスセキュリティ

ファイバチャネルデバイスに関連付けられた ISO/IEC 27040 ガイダンスは、FC SAN 内に実装可能なものを超えている。このガイダンスの要約を以下に示す。

— LUN マスキング、WWN フィルタリング、およびその他のアクセス制御メカニズムを使用してストレージへのアクセスを制限する。

— 可能であれば集中型認証サービス（RADIUS[16]）を利用しながら、すべてのホストとスイッチによる FC-SP-2 AUTH-A を使用した相互認証などの FCP セキュリティ対策を利用する。機密情報が保護された領域（物理的に管理されたデータセンタの領域など）を

[16] IETF RFC 2865 Remote Authentication Dial In User Service (RADIUS)

離れる場合は、リンク暗号化（GCM 暗号化[17]を使用した ESP_Header など）を使用する。

— 機密性の高い／規制対象のまたは価値の高いデータの場合は、ストレージデバイスまたはメディアに蓄積データ暗号化と適切な鍵管理対策を実装する。このトピックに関する追加情報については、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）」を参照のこと。

— 蓄積データ暗号化と同様に、メディアに合わせた対策または論理サニタイズ対策を使用して機密性の高い／規制対象のまたは価値の高いデータを保護する。後者は、特に、実際のストレージデバイスとメディアが特定できない場合に、仮想化ストレージに非常に有効な場合がある。このトピックに関する追加情報については、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）」を参照のこと。

5 FC に関する SNIA の見解とガイダンス

ファイバチャネル標準は、汎用的に使用できない幅広い特徴と機能性を規定している。このセクションでは、既知の FC セキュリティの課題と問題点の一部を紹介し、ISO/IEC 27040 に記載されていないガイダンスを提供する。

5.1 FCP リンク暗号化

リンク暗号化は、特定の通信経路に沿ってすべてのデータを暗号化するデータセキュリティプロセスである。通常、リンク暗号化は、2 つの通信ポイント（ルータなど）間のデータリンクレイヤと物理レイヤで実施される。また、リンク暗号化は、送信デバイスと受信デバイス間の通信を保護するエンドツーエンド暗号化とは異なることに注意する必要がある。

ファイバチャネルの環境では、リンク暗号化は FCP の一部（ESP_Header など）または外部メカニズム（FCIP を保護する IPsec など）として利用できる。通常、リンク暗号化は、Fibre Channel over IP（FCIP）をトランスポートとして採用しているサイト間の FCP 接続を保護するためにしか使用されない。ESP_Header 暗号化を実装しているストレージベンダーが少ないため、ファイバチャネル SAN 内部にリンク暗号化を実装するのは不可能ではないが困難である。この状況は、顧客がこの機能を要求し始めることによって変わる可能性がある。

リンクレベルの暗号化が使用できると仮定した場合、その使用がデータセンタ間に導入されたデータリダクション技術（圧縮や重複排除など）に大きな影響を及ぼす可能性があることを覚えておく必要がある。

この執筆時点では、IPsec を使用した FCIP がファイバチャネルに使用可能な唯一のリンク暗号化の形態である。

[17] ファイバチャネルフレームの完全性または機密性は、ANSI INCITS 470-2011, Fibre Channel - Framing and Signaling - 3 (FC-FS-3) で規定された ESP_Header オプションヘッダを使って提供できる。

5.2 蓄積データ暗号化

蓄積データ暗号化は、ファイバチャネルセキュリティの要素ではないが、リンク暗号化と同様に、データリダクション技術に影響を及ぼす可能性があるため、ここで簡単に説明する。

ストレージエコシステム内の暗号化はメディアレベルの保護を提供するため、セーフティネットにはなるが、実際に機密性を保護するためには、データをそのソースまたは用途（ホストやアプリケーションなどによる）の近くで暗号化する必要があることを忘れないようにする必要がある。蓄積データ暗号化の詳細については、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）」を参照のこと。

5.3 FCoE を使用した FC セキュリティの維持

コンバージドネットワークアダプタ（CNA）を内蔵した Fibre Channel over Ethernet（FCoE）デバイスは、FCoE 初期化プロトコル（FIP）プロセスを使用して、FC ネットワークに FCoE ノード（ENode）としてログインする。このログインプロセスによって、ENode 上の仮想 N_Port（VN_Port）と FC スイッチ上の仮想 F_Port（VF_Port）間の専用仮想リンクが確立される。この専用仮想リンクがポイントツーポイント接続をエミュレートする。エミュレートされる接続は仮想リンクと呼ばれており、仮想リンクは中継スイッチを透過的に通過する（つまり、中継スイッチは ENode VN_Port と FC スイッチ VF_Port から見えず、仮想リンクは直接ポイントツーポイントリンクのように見える）。

FCoE はイーサネットネットワーク上で FC フレームを公開するため、必ずしもネイティブな FC ネットワークと同じセキュリティレベルではないことに注意する必要がある。潜在的リスクを抑制するためには、ファイバチャネル（FC）ネットワークへの不正なアクセスとデータ伝送を避けるように設計された、FIP スヌーピングと呼ばれるセキュリティメカニズムを実装して、次のメカニズムのいずれかを介してトラフィックをフィルタリングする必要がある。

- FCoE VLAN 上の VN_Port／VF_Port 間（VN2VF_Port）FIP スヌーピング[18]、システム（中継スイッチなど）は VN_Port／VF_Port 間パケットをスヌープして、VN2VF_Port 仮想リンク上でのみセキュリティを適用する。
- FCoE VLAN 上の VN_Port 間（VN2VN_Port）FIP スヌーピング[19]、システム（中継スイッチなど）は VN_Port 間パケットをスヌープして、VN2VN_Port 仮想リンク上でのみセキュリティを適用する。

注意：FCoE VLAN は、VN2VF_Port FIP スヌーピングと VN2VN_Port FIP スヌーピングのどちらかをサポートできるが、両方はサポートできない。

[18] FC-BB-5 で規定されている。
[19] FC-BB-6 で規定されている。

5.4 追加の考慮事項

このセクション内の資料では、FC セキュリティメカニズムの適切な使用に影響を与える可能性のある課題と問題点について説明する。

5.4.1 FC 認証用の共有秘密の数

エンタープライズクラスのストレージシステムとディレクタクラスの FC スイッチでは、FC-SP-2 AUTH-A を使用して認証する大量（50,000 台以上）のエンティティが存在する場合がある。これらのエンティティ（ホスト／スイッチ、ストレージ／スイッチ、およびホスト／ストレージ）のどの 2 つの間にも相互認証に共有秘密のペアが必要なことを考えると、この膨大な数の共有秘密によって、このような環境を保護するために必要な共有秘密を正しく生成、配布、および実装することが運用上の課題になる可能性がある。オーバーヘッドを最小限に抑え、設定ミスによるダウンタイムを避けるために、様々なデバイスが RADIUS を使用して、管理すべき共有秘密の数を減らすことが望ましい。

5.4.2 FC 共有秘密の構成

FC-SP-2 標準は、ユーザインタフェースの課題を扱っていないが、この状況が共有秘密の曖昧さの原因になっている。この問題は、両方のエンドポイントで同じ共有秘密を使用しなければならないという制限に起因するが、共有秘密をそれぞれに入力する方法が非互換性をもたらす場合がある。例えば、あるデバイスはユーザに 128 ビットの 16 進数を入力するように要求するが、別のデバイスは英数字値を入力するように要求する場合である。後者のケースではさらに、受け入れ可能な文字に違いがある場合もある。このような違いは、異種混在環境の相互運用性を大幅に制限または阻害する可能性がある。また、このような制限は、共有秘密のエントロピーに影響する可能性もある。

6 サマリー

ファイバチャネルのセキュリティメカニズムは、様々な標準で規定されているため、ベンダーの実装や顧客の使用の障害になっている。加えて、規定されたメカニズムの一部はベンダーの実装が必須でないため、セキュリティ機能の使用可能性が保証されない。最後に、異種混在環境の FC SAN では、使用可能な FC セキュリティ機能に相互運用性の問題がある。

7 謝辞

7.1 執筆者について

Eric Hibbard は、HDS の CTO Security & Privacy を務め、30 年間 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 の共同議長であり、ABA、IEEE、CSA、および INCITS の指導的立場も務めている。これまで、複数の ISO/IEC および IEEE 標準、ISO/IEC 27040（ストレージセキュリティ）、および ISO/IEC 20648（ストレージシステムの TLS 仕様）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。

7.2 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	HPE
Walt Hubis	Hubis Technical Associates
Dr. Alan Yoder	
Gary Sutphin	
Tim Hudson	Cryptsoft
Thomas Rivera	Hitachi Data Systems

8 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。
ISO/IEC 27040 に関連付けられた追加の SNIA 資料については、http://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。

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、SC 27 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）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。

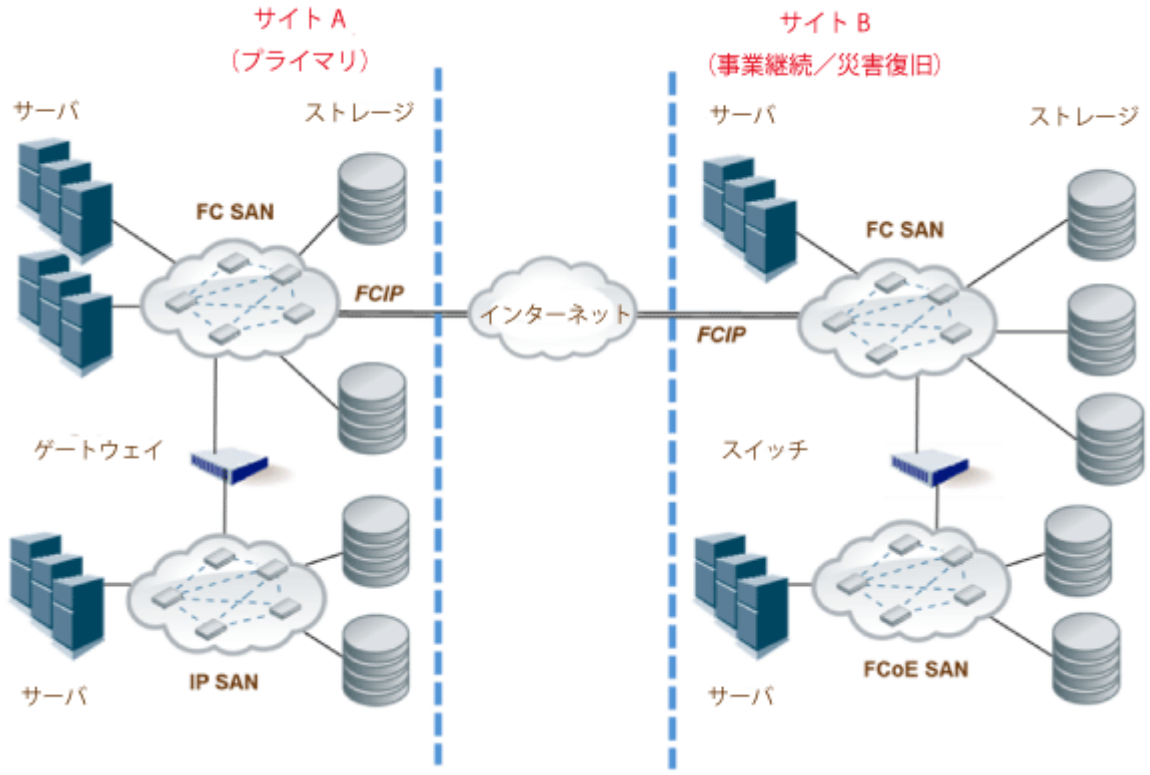
ISO/IEC 27040 は、1) 補助管理と 2) ストレージセキュリティの設計と実装という 2 つの角度からストレージセキュリティガイダンスにアプローチしている。この両方が、セキュリティの知識が不足しているストレージプロフェッショナルやストレージ経験の少ないセキュリティ／監査プロフェッショナルが資料を活用できるように詳しく扱われている。

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、およびデータリダクション）

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 － 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）
- データの機密性と整合性
- 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。対応が全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、整合性、可用性）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 仮想化（NPIV）、ファイバ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[20]。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[21]。「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。」

[20] 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）
[21] 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）

小委員会 27（SC 27）

JTC1 内部の SC 27 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、整合性、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
- セキュリティの評価基準および方法論[22]

1990 年 4 月に初の全体会議を開催して以来、SC 27 は、120 を超える標準を発行し、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、SC 27 は次の作業部会（WG）に分かれている[23]。

- 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

[22] 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）

[23] 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）

参考文献

[01] IETF RFC 2865 *Remote Authentication Dial In User Service (RADIUS)*

[02] IETF RFC 4303 *IP Encapsulating Security Payload (ESP)*

[03] IETF RFC 4595 *Use of IKEv2 in the Fibre Channel Security Association Management Protocol*

[04] IETF RFC 7296 *Internet Key Exchange Protocol Version 2 (IKEv2)*

[05] ANSI INCITS 461–2010, *Fibre Channel — Switch Fabric — 5 (FC-SW-5)*

[06] ANSI INCITS 462–2010, *Information Technology — Fibre Channel - Backbone — 5(FC-BB-5)*

[07] ANSI INCITS 463–2010, *Fibre Channel — Generic Services — 6 (FC-GS-6)*

[08] ANSI INCITS 470–2011, *Fibre Channel — Framing and Signaling-3 (FC-FS-3)*

[09] ANSI INCITS 496–2012, *Information Technology — Fibre Channel — Security Protocols — 2 (FC-SP-2)*

[10] SNIA *Storage Security: Encryption and Key Management*, August 2015