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：
ストレージ管理に関する概要

バージョン 1.0

2016 年 8 月 2 日

要約：*ISO/IEC 27040（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、ストレージセキュリティに関係する重要なセキュリティ概念の概要を示し、ストレージ管理に該当する標準内のセキュリティガイダンスを概説する。また、組織の特定のニーズを満たすストレージ管理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

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	*4/24/2016*	全体	Richard Austin	初稿
V0.2	*7/19/2016*	全体	Richard Austin	レビューコメントを追加
V1.0	*8/2/2016*	全体	Richard Austin	最終編集コメントを追加

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, 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

この SNIA ホワイトペーパーは、ストレージプロフェッショナルのために情報セキュリティの概要を示し、そのストレージ管理の保護における応用を導入事例として提示する。本書の目的は、ストレージプロフェッショナルが業界のベストプラクティスで補完された ISO-IEC 27040 内のガイダンスを有効に活用して、担当するストレージ資産の適切なセキュリティを保証できるようにすることである。

1 「セキュリティ」とは何か

「セキュリティ」は最近よく耳にする単語であるが、ほとんどの人がその量が多いほど良いと思い込んでいる。まるで、最寄りのコンサルタント会社に行って「セキュリティを 3 トンください」と注文できるかのように。問題は、セキュリティが実際には物ではなく、状態に過ぎないということである。この「安全な」状態は、組織が直面しているすべてのリスクがある時点でリスク許容度以下に管理されている場合に成立すると言える。

最後の文には「リスク」、「管理」、「リスク許容度」などの聞き慣れない単語が多く含まれているが、実は「セキュリティ」と呼ばれるものに関する誤解のほとんどがこれらの用語の理解不足に基づいている。

1.1 セキュリティは実はリスクの管理に関係している

リスクに対する考え方は人それぞれである。朝の通勤の途中で自動車事故に遭うかもしれない、今日は雨が降るかもしれない、株式市場が思わぬ方向に動くかもしれない、競合他社がすごい新製品を発表するかもしれない。これらの状況には共通しているものがある。

- 特定の潜在的損失がある[1]（自動車事故で死亡または負傷するかもしれない。傘を持っていなければ濡れるかもしれない. . . ）。
- 損失を軽減可能な方法がある（傘を持って行く、自動車保険に入って慎重に運転する、株式ポートフォリオを分散する. . . ）。
- 損失の可能性を大まかに予測できる（今日は 40%の確率で雨が降る）。

この 3 つの要素は、リスクは損失の可能性と損失の大きさ、そしてリスク対策によるその抑制によって決定されるという一種の式にまとめることができる[2] 。

リスク = f（損失、可能性） − 抑制策

抑制策を講じるほどリスク[3] は減少するが、どこまで行えば十分だと言えるのだろうか。組織によってリスクに対する許容度が異なる。非常に厳格な場合もあれば、非常に寛容な場合

[1] ここで取り上げるリスクには利点がないことから、正式には「純粋リスク」と呼ばれている。例えば、ポーカーの持ち札に 10 ドル賭けたとすると、その 10 ドルを失う場合もあれば、何回か勝つ場合もあるため、損をする場合と得をする場合の両方を考慮しなければならない。情報セキュリティリスクは損失を被る一方のため、そのような損失を回避する方法を中心に説明する。

[2] リスクを「排除」すると言っているわけではないことに注意してほしい。リスクの排除は、どうでもいいケースを除けば普通は不可能である（家から出ない、絶対に車を運転しない、絶対に車に乗らないなど）。傘を持っていれば暴風雨の中でも濡れずに済むとしても、突風で傘が飛ばされたり、破壊される可能性がある。

もある。例えば、動きの速い新興企業では、許容度がかなり高い。残存リスクが組織の許容範囲に入った段階（または予算をオーバーした段階）でリスクの抑制は終了する。

1.2　敵対的リスク

リスクについて考えると、すぐに、様々な種類のリスクがあることに気付く。情報セキュリティにおけるリスク管理を混乱させていたものは、無機的リスクと敵対的リスクの区別である。

域内で発生した竜巻がメインのデータセンタを破壊するように意図的にコースを変えることはない。これが無機的リスクの例である。竜巻は自然の営みであり、特定の誰かを標的にすることはない（ただし、マーフィー氏が頻繁に警告しているように、そのように思える場合もある）。無機的リスクは、比較的よく理解されており、リスク管理プロセスが成熟している（死亡給付金を支払っても利益が出る保険業界など）。

一方で、多国籍犯罪集団に属しているジェーンハッカーが、あなたの組織に非常に興味を持っているかもしれないし、彼女の標的までの踏み石としてあなた個人に興味を持っているかもしれない。これは、標的型のリスクであり、全く別の問題である。この場合、リスク方程式の係数の決定はかなり困難であり、「情報を保存すれば、狙われるかもしれない」と言っているのとほとんど変わらない当然のような定性的見積もりで終わってしまうことが多い。

残念ながら、ほとんどの情報セキュリティリスクは敵対的人間から発生する。

1.3　リスク管理とコンプライアンスの関係

情報セキュリティ業界は、今日、コンプライアンスに関する話し合いに多くの時間を費やしている。コンプライアンスとは、（できれば）知識が豊富で信頼できる団体が必要だと決定したことを検証可能な形で実行することである。例えば、ペイメントカード情報を処理する場合は、PCI-DSS 要件に従う必要がある。米国で個人の健康情報を保存または処理する場合は、HIPAA に従う必要がある。例を挙げればきりがない。

ただし、「セキュリティ」と「コンプライアンス」は別のものである。コンプライアンスは、基本的に、何らかのチェックリストに掲載された該当する項目のすべてに従っていることを意味するが、セキュリティは、環境内の重要なリスクのすべてが許容

脅威

特定の脅威の目録は非常に長くなる可能性があるが、多くの場合、脅威の影響は次のいずれかの侵害を招く。

- 機密性 - 情報が許可されたエンティティしか利用できないこと
- 完全性 - 情報が意図的か偶発的かに関係なく無許可の変更から保護されること
- 可用性 - 情報を必要に応じて許可されたユーザが利用できること

この 3 つのカテゴリーは、C-I-A トライアドと呼ばれている。例を挙げれば、データ漏洩は機密性の侵害であり、小切手の金額を 30 ドルから 3,000 ドルに変更することは完全性の侵害であり、サービス妨害攻撃は可用性の侵害である。

[3] これが残存リスクと呼ばれるものである。つまり、対策が講じられた後に残るリスクである。

可能なレベルまで抑制されていることを意味する。

2　リスクについての ISO の見解

ISO は、リスク全般、特に、情報セキュリティリスクの検討に多くの時間を費やしてきた。この幅広いアプローチのために、リスクについての ISO の見解は、複数の標準の様々な文脈に登場する。情報セキュリティの文脈での概要を以下に示す。

図 1 は、リスク（「目的に対する不確実性の影響」、ISO/IEC 27000）につながる重要な用語を示したものである。リスクは脅威（「システム、個人、または組織に害を及ぼす可能性のある望ましくないインシデントの潜在的原因」、ISO/IEC 27032）から始まる。竜巻や特権ログオンクレデンシャルの侵害が脅威の例である。ここでは特に敵対的リスクに注目するため、別の重要な用語（図 1 には示されていない）として脅威エージェント（「資産に害を及ぼす可能性があるエンティティ」、ISO/IEC TR 2004）を取り上げる。ジェーンハッカーは脅威エージェントの例である[4] 。

脅威は、脆弱性（「脅威によって攻撃可能な資産または制御[5] の弱点」、ISO/IEC 27032）を利用（攻撃）する。脆弱性の例には、ソフトウェアの欠陥が常に存在していることでパッチチームが常に多忙になっている状態や、「I Love You!」という件名の知らない人からの電子メール内のリンクをクリックする不注意な従業員がいることが挙げられる[6]。

脆弱性の攻撃に成功すると、我々の関心を引く結果を引き起こすイベント（「情報セキュリティポリシーの侵害の可能性や制御の不具合を示すシステムやネットワークの状態の特定された出現またはセキュリティに関係している可能性のある未知の状況」、ISO/IEC 27000）が発生する（ここでも、例えば、敵対者が望んでいる結果が「I Love You!」電子メール内の悪意のあるリンクをブロックするマルウェア対策製品などの制御によって阻止されることがあるため、確実に発生するとは限らない）。脅威エージェントと脆弱性について考えるうえで有益なもう一つの概念が脅威ベクトルである（ISO では、これを攻撃ベクトル（「攻撃者がコンピューターまたはネットワークサーバへのアクセス権を取得して悪意のある結果を招くことが可能な経路または手段」、ISO/IEC 27032）と呼んでいる）。脅威ベクトルは脅威エージェントと脆弱性を結ぶ線である。「I Love You」の例では、電子メールが脅威ベクトルになる。

影響が大きいものであれば、セキュリティインシデント（「事業運営の混乱や情報セキュリティの侵害を招く可能性が高い単一のまたは一連の望ましくない情報セキュリティイベント」、ISO/IEC 27000）を引き起こす可能性がある。インシデントは、敵対者がこちらの防御を突破するという目的を達成した可能性があることを意味する。

[4] 脅威エージェントについての知識は、彼らの動機や能力の評価に役立つため重要である。素人「ハッカー」が、オンラインフォーラムで自慢げに披露された手口を実行しようとするかもしれず、この場合、既知の一般的な攻撃しか行われない。どこかの国の工作員が、価値の高い知的財産を入手する攻撃を実行するかもしれず、この場合、高度な技術や機能が利用されることがある。

[5] 制御は、上で抑制策と呼んでいたものである。

[6] これは、すべての脆弱性が技術由来（ソフトウェアのバグやファイアウォールの設定ミスなど）というわけではなく、人間の行動のような非技術的な脆弱性も含まれるということを伝える重要な注意喚起である。

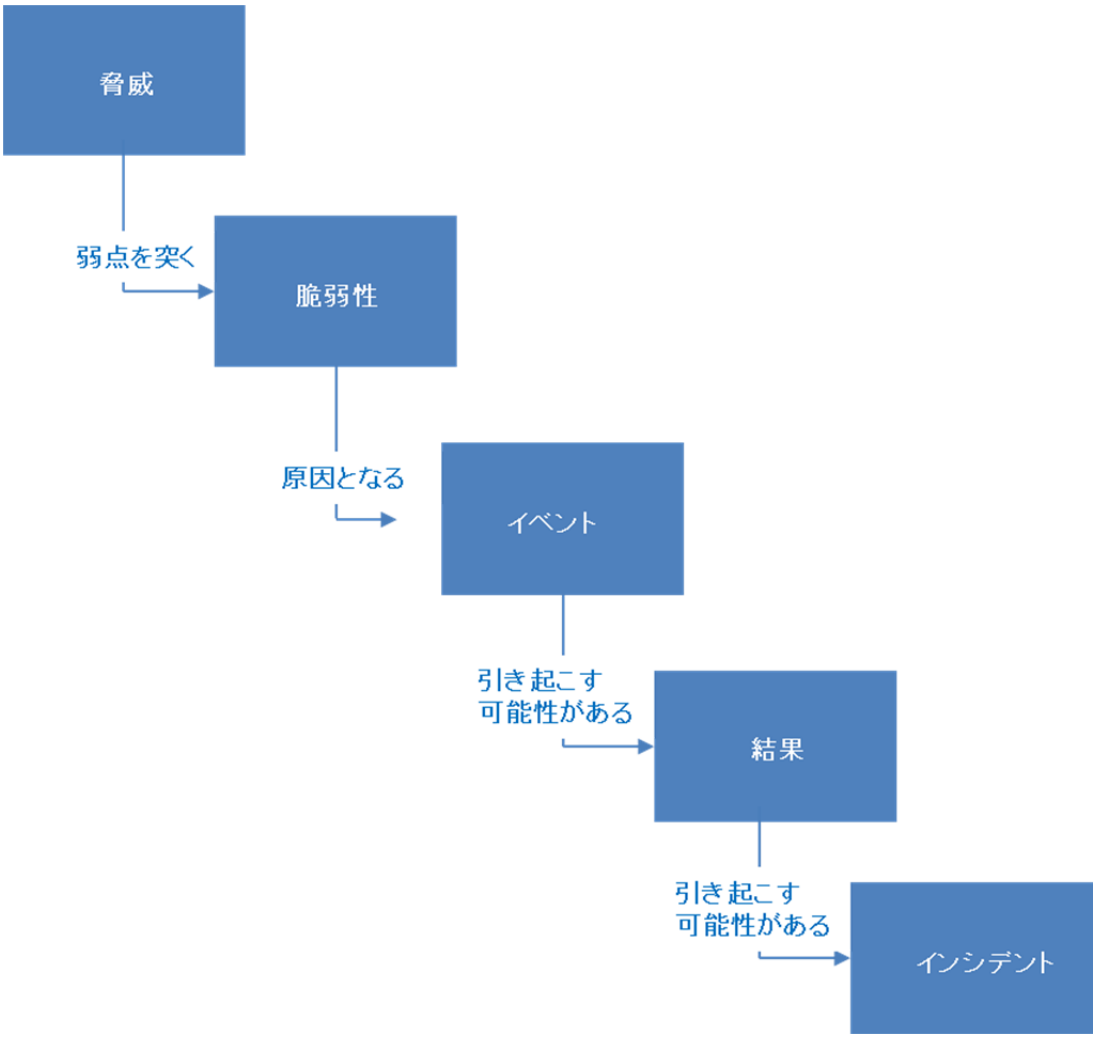


図 1　ISO リスクモデル

これらの用語は馴染みのない暗号のように聞こえるかもしれないが、損失の可能性と大きさを見積もるアプローチを具体化するものである。可能性は脅威と脆弱性（および脅威が脆弱性を侵害する容易さ）に依存し、結果は損失を示す。

2.1　リスク管理

リスク管理は、基本的に、組織が環境内のリスクを特定してできるだけ抑制することの保証に関係する[7] 。理想的な環境では、リスクを高い順に並べたリストを作成するリスクアセスメントが実施され、制御（抑制策）を適用することによってそのようなリスクを管理することになる。例えば、会社の Web サーバに入ってくるトラフィックの種類を制限するためにファイアウォールを購入してインストールしたり、ドメインに入ってくるすべての電子メールからマルウェアなどをスキャン可能な電子メールゲートウェイを購入したりする。これらの抑制策はその調達と運用にお金がかかるうえ、予算や適任者の確保などには必ず限界があるため、組織のリスクを最も大幅に抑制できるところで対策を講じることが重要である。

[7] 一般的な ISO リスク管理の用語集とプロセスは曖昧すぎるため、ここでは省略する。

理想的には、リスク管理が完全であれば、すべての既知のリスクを組織のリスク許容度以下に抑制できる。ただし、まだ一部のリスク項目が残っている状態で予算や使用可能な人材が底を突いて抑制できなくなるケースも多い。これは残念なことではあるが、リスクの評価と管理を試みた結果、残存リスクとそれが組織に及ぼす影響が分かっているため、状況は大きく改善されている。

3　ストレージ脅威モデル[8]

ISO/IEC 27040 では、ストレージとそれをサポートするインフラストラクチャに関する一般的な脅威のクラスが規定されている。

- 不正使用　-　許可なくストレージ容量そのものを使用すること。敵対者は、ストレージを、自分の組織または他の組織から盗み出したデータを最終目的地に配信する前に、保管するための倉庫として使用することがある。
- 不正アクセス　-　情報、管理ネットワーク、管理アプリケーションなどへの許可のない（または権限を超えた）アクセス。例えば、敵対者は、一連の管理者のクレデンシャルを侵害して、それらを使って管理アプリケーションにアクセスし、機密情報が格納されたストレージにアクセス権を付与することがある。
- 規制違反による負債　-　データの損失（つまり、データ漏洩）に対する厳しい姿勢は強まっており、規制機関が情報の保護に失敗した組織に対して厳しい罰金やその他のペナルティを課すことがある。
- サービス拒否（DoS）攻撃と分散サービス拒否（DDoS）攻撃
- メディアの窃盗または不慮の紛失
- マルウェア攻撃または導入
- 使用終了後の不適切な処置またはサニタイズ

これらの脅威がもたらす結果には、データ漏洩、データ破損または破壊、アクセス／可用性の一時的または恒久的消失、および法定要件、規制要件、または法的要件の不履行が含まれる。

これらの結果のそれぞれが、組織に損失をもたらす可能性があり、その額はインシデントの範囲と影響に応じて異なる。

[8] 特定の組織におけるリスクは、その特性や環境に応じて異なるため、一般論として議論することができない。一方、脅威は、はるかに一般的な形で議論することができる。このホワイトペーパーの読者は、脅威、関連する脆弱性、および可能性のある結果の影響を評価してリスクのレベルを判定する必要がある。

4　ストレージ管理のセキュリティが重要な理由

鋭敏な読者は既にお気付きだろうが、脅威のクラス全体に関係する共通の脅威が存在する。つまり、ストレージ管理はそれらのほとんどに関係する。ストレージインフラストラクチャは、多数の相互接続されたデバイスからなる複雑な構造をしており、任意のホストと任意のストレージを接続可能な大量の曲がりくねった SCSI ケーブルの山だというイメージがある。このケーブルの山には、その継続的運転を設定して保証するための十分な管理が必要である。「ストレージ管理」を話題にする場合、我々は 5 つの一般的な活動のクラス（ISO/IEC 27040、6.4.1 節）について言及する。

1. 運用 - ストレージ（およびその上に構築されたサービス）の正常な稼働状態の維持
2. 管理 - ストレージインフラストラクチャ内のリソースとその割り当て方の追跡
3. メンテナンス - 効率的な運用を保証する修理、アップグレード、および日々の一般的なチューニングと調整の実施
4. プロビジョニング - サービスを提供するためのシステムの準備
5. サニタイズ - ストレージをサービスから除外または再目的化する場合にその過去の内容を読み取れないようにすることの保証

管理は、インバンドにすることも、アウトオブバンドにすることも、そのハイブリッドにすることもできる。インバンド管理では、データの転送に使用されているものと同じネットワークが使用されるが、アウトオブバンド管理では、別の管理ネットワーク（TCP/IP が一般的）が使用される。ハイブリッドソリューションでは、一部の機能にインバンドが使用され、残りの機能にアウトオブバンドが使用される。例えば、認証サーバとの通信にアウトオブバンドネットワークが使用される場合に、実際の管理トラフィックをインバンドとすることができる。

アウトオブバンド管理ネットワークは、TCP/IP ネットワークを使用して実装されることが多いため、特に懸案事項になる。敵対者は、何よりも TCP/IP ネットワークを経由した攻撃に精通しているからである。

ストレージ管理が侵害されたら、かなり深刻な事態を招くことになる。敵対者が強力な一連のストレージ管理者クレデンシャルを侵害可能な場合は、SAN 環境の大部分を管理下に置いて、ゾーニング設定の変更、ストレージの割り当て／割り当て解除、ディスクアレイ全体のファクトリリセットなどを実行し、ストレージ資産の機密性、完全性、および可用性に大きな影響を及ぼすことができる。

5　ストレージ管理の保護

ストレージ管理は、ストレージインフラストラクチャ（ローカルとリモートのどちらかで提供されている）の管理担当者、ベンダーのサポート要員（通常はリモート）、および監査者からアクセスできる必要があるため、極めて強力であると同時に、かなり無防備でもある。TCP/IP ネットワーク経由のアウトオブバンド管理が一般的であることも手伝って、敵対者にとって格好の標的になる。

ISO/IEC 27040 には、ストレージ管理の保護に関する実用的なガイダンスが記載されている。

5.1 認証と認可

認証に関して、ISO/IEC 27040 では、次のベストプラクティスが推奨されている。

- すべてのユーザが一意の識別子を持つべき - これは自明のことのように思えるが、管理タスクを実行するときに複数のエンティティが使用する「Administrator」などの一般的なユーザ識別子が使われることがある。問題は、特定の人物の行動を追跡できなくなることである。これにより、パスワードを変更すると当該ユーザだけでなく他のユーザも影響を受けることになるなど、クレデンシャルの侵害に対する対応が複雑になる。

- 適切な認証テクニックを使用する - この決定は良好な実践とクレデンシャルの侵害に伴うリスクの両方に基づく（例えば、広範な管理者機能に伴うクレデンシャルは限定された機能セットに伴うクレデンシャルよりもはるかに大きなリスクを伴う）。推奨事項を以下に示す。

「認証と認可」とは何か

認証と認可は、誰に何を許すかを決める場合に関係する表裏一体の要素である。認証は何らかの形で主張された ID 情報を証明することである。銀行の Web サイトにログインするときは、ユーザ名、電子メールアドレス、携帯電話の番号、またはその他の自分が誰かを示す情報で自分自身を識別する。その後で、実際に自分が何者であるかの証拠を提出する必要がある。この証拠は 4 つの一般的な形態を取ることができる。

1. 知識 - パスワードやその他の秘密情報
2. 所有物 - ハードウェアトークン
3. 身体的特徴 - 通常は、指紋、網膜スキャン、ジェスチャーなどの生体的特徴
4. 居場所 - ある場所へのアクセスを取得する場合に適用されるセキュリティ制御に依存する（SWIFT 電信送金端末や弾道ミサイルの発射基地など）。

これらの保証は単独で使用される場合（単一要素）と組み合わせて使用される場合（多要素）がある。2 要素認証の例は、PIN（知識）が必要なハードウェアトークン（所有物）である。

認可は、認証された ID で何ができるかに関係する。ほとんどの人がラップトップを標準ユーザとして起動し、管理タスクを実行するために自分の権限を昇格させなければならない（sudo やユーザアカウント制御経由で）ことに慣れている。認可は、最小権限のセキュリティ原則（エンティティはタスクの実行に必要な権限の最小セットのみを所有すべき）を実装する手段である。これは、クレデンシャルのセットを侵害した敵対者がもたらす可能性のある損害を制限する点で重要である。

認可は、管理者は何でもできるがユーザはほとんど何もできないという単純な方式から特定の機能を個別のユーザに割り当てる方式やロールの設計まで、様々な形態を採ることができる。単純なオールオアナッシングの認可は実装が容易だが、管理クレデンシャルの侵害によって壊滅的な事態を招く可能性があるため、非常に大きなリスクを伴う。ユーザに個別の機能を割り当てる（ベンダーか許可している場合）方式では、ユーザの機能をこと細かく制御できるが、すぐに管理が手に負えなくなる可能性が高い。ロール（同様に、ベンダーが実装している場合）はまずまずの妥協案となる。例えば、ゾーニングを管理可能なゾーン管理者ロールを定義してから、ユーザの Jane. Smith をそのロールに割り当てたとする。その後、Jane が退社または異動した場合は、そのロールを削除するだけで済むため簡単である。この RBAC（ロールベースアクセス制御）は、魅力的だが、ロール定義の設計（最小権限の原則の実装と職務の分離）には計画と規律が必要である。

- 強力なパスワードを使用し、長さ、複雑さ（特殊文字の使用など）、および使用期間に関する要件を適用する。
- チャレンジレスポンスプロトコル（リプレイ攻撃の可能性を減らす）や多要素認証などを使用して認証プロセスを強化する。

- すべてのリモートアクセスに対して強力な認証テクニックを使用する。
- 集中型認証ソリューション（RADIUS やその他のシングルサインオン技術など）を使用する - デバイスの数が増えるほど、ユーザクレデンシャルの管理が複雑になる可能性がある。何百台ものデバイス上のローカルユーザデータベースの管理と比較して、集中型認証ソリューションはすべての変更を一か所で一度に行うことができる。
- 機密データや高価値データを管理する場合は多要素認証を使用する - このようなデータは、敵対者がそのアクセス権を取得した場合に大きなリスクを伴うが、最も強力な認証プロセスを使用することでこのようなリスクの実現可能性が抑制される。

認可に関して、ISO/IEC 27040 では、最小権限を実装するロールの利用が推奨されている。最小権限は、特定の作業を実行するのに必要な最小限に機能を抑えようとすることを思い出して欲しい。ここでの考え方は、クレデンシャルの侵害やその他の悪用がもたらす可能性のある損害を細分化することである。少なくとも、次のロールが推奨されている。

- セキュリティ管理者 - このロールは、関連する権限を持つアカウントを作成して管理し、監査記録の構成と内容を制御し、IT インフラストラクチャとの信頼関係（どの RADIUS サーバがユーザを認証できるかなど）を築き、証明書やキーストアだけでなくその他の暗号インフラストラクチャ（鍵管理[9] など）も管理する能力を持っている。
- ストレージ管理者 - セキュリティ管理者ロール用として予約された能力を除いて、ストレージインフラストラクチャのすべての側面に対する閲覧権限と変更権限を持っている。これは、非セキュリティロールと見なされることが多いことに注意すること。
- セキュリティ監査者 - このロールは、資格（つまり、ユーザが持っている能力）の監査、セキュリティ関連設定項目の確認、および監査ログを可能にするセキュリティ関連情報への閲覧（読み取り専用）アクセス権を持っている。このロールは何も変更できないことに注意すること。
- ストレージ監査者 - セキュリティ監査者と同様に、このロールは、ストレージのパラメータ、設定、および正しい動作の確認（ヘルス／障害ログの閲覧など）を可能にする閲覧アクセス権を持っている。このロールは、設定を閲覧することはできるが、変更することはできない。

SNIA では、各ユーザに関連づけるこれらのロールを 1 つに限定することを推奨している。これにより、職務の分離の原則の実装が容易になる。例えば、新しい認証サーバの追加など、セキュリティにとって重要な操作を実行するには、セキュリティ管理者ロールとストレージ管理者ロールの両方の協力が必要になる。

[9] 標準では特に明記されていないが、環境によっては、暗号インフラストラクチャの管理が別の暗号責任者ロールに分離される場合がある。

5.2 管理インタフェースの保護

ほとんどの SAN デバイスは、物理管理インタフェースを公開することで、その動作の設定、制御、および監視を可能にしている。シリアルポートなのか、モデム（リモートサポートアクセスに使用される場合がある）なのか、ネットワーク（インバンドとアウトオブバンドのどちらか）なのかに関係なく、この管理インタフェースの保護が不十分な場合は、データの破壊、破損、またはアクセス拒否を伴う不正使用につながる可能性がある。

物理管理インタフェースを保護するために、ISO/IEC 27040 では次のように推奨されている。

- 管理インタフェースへの物理アクセスを制限する - 侵入者が簡単に SAN スイッチなどに近づいて、そのシリアルポートにプラグを差し込めるようにすべきではない。
- 使用していないときは、シリアル管理ポートは無効にして切り離しておく。
- 管理トラフィックに使用されている LAN インタフェースを他の LAN トラフィックから分離する - この目的は、より大規模なネットワークからの管理 LAN へのアクセスを制限することである。物理的な分離が望ましいが、必要に応じて、仮想的な分離（VLAN）も使用できる。

物理インタフェースだけでなく、デバイスがソフトウェア（またはファームウェア）と API（アプリケーションプログラミングインタフェース）を提供して、コマンドラインツール、SNMP、および GUI アプリケーション経由での動作の管理と監視ができることもある。ISO/IEC 27040 では、これらのインタフェースの保護に関する次のベストプラクティスが推奨されている。

- ファイアウォールまたは TCP ラッパーを使用して管理ネットワークへのアクセスを制限する。
- エンティティ認証を使用してストレージシステムと管理システム間の信頼関係を構築する - 以前の認証の議論ではユーザの分かりやすさに焦点を当てたが、ストレージシステムでは、それを制御しようとしている管理ステーションが信頼できることを保証できることが重要である。
- IDS と IPS を利用して異常な動作を特定してブロックする。
- 補助インフラストラクチャ（DNS、SLS、NTP など）が攻撃に使用されないように適切に保護する。
- 「認証と認可」で述べたように、特権ユーザ制御を効果的に使用する。
- オペレーティングシステムとアプリケーションが最新であり、十分強化されていることを確認する - 残念ながら、最近は、ソフトウェアの脆弱性が目立っている。既知の脆弱性ができるだけ迅速に修正され、潜在的な攻撃のベクトルが閉じられることを保証することが重要である。「強化」としては、可能性のある攻撃のベクトル（業界では、「攻撃対象領域」と呼ばれている）を最小限に抑えるために、未使用のサービスの無効化や安全性の低いプロトコルの禁止などを行う。

ストレージシステムのリモート管理はかなり一般化している（例えば、ストレージ管理者は中央に配置され、ストレージそのものは分散化される）。悪意のある使用を最小限に抑えながら、リモート管理を有効にするためには、次の追加のセキュリティ制御が必要である。

- リモートアクセス用の安全なチャネルを使用する - これには VPN、TLS[10] 、または SSH が含まれる。これらのプロトコルは、リモート管理トラフィックを使用した傍受、偽装、および改ざんのリスクを抑制できる。
- 多要素認証などの強力な認証を要求する。
- 最小権限の原則に従ってリモートアクセスを必要最小限の機能に制限する。

リモートアクセスの特殊なケースは、ベンダーがメンテナンスやサポート機能のためにストレージシステムへのリモートアクセスを必要とする場合である。このようなリモートサポートセッションでは外部ネットワークや電話システムが使用されることが多いため、リモート管理に関するガイダンスに従って、リモートサポートセッションを可能にするための特別な認可を設け、実行されたアクセスやアクションの特定の監査ロギングを有効にする必要がある。電話システムが使用される場合は、モデムコールバックプロトコルを実装して、ベンダーセッションが必要な場合に個別に認可する必要がある。

5.3 セキュリティ監査、アカウンティング、およびモニタリング

ストレージシステムは、様々な種類のログレコードを生成して、ストレージインフラストラクチャ内のイベントの詳細なタイムラインを提供することができる。これらのイベントの一部は、セキュリティの観点から重要性が高く、コンプライアンスモニタリング、インシデント対応やフォレンジック調査の一部として使用される。ISO/IEC 27002（12.4 節）は一般的なイベントロギングに関するガイダンスを提供しているが、ISO/IEC 27040 はストレージシステムに特化した次のガイダンスを提供している。

5.3.1 組織ロギングにストレージシステムを含める

これは自明のことかもしれないが、多くの場合、組織が監査ロギングの実装を検討しているときにストレージインフラストラクチャはほとんど無視されている。ストレージインフラストラクチャは組織の運営に不可欠なため、組織のロギングプロセスの対象として参加させることが重要である。

- ストレージシステムが組織のロギングポリシーに従うことを義務付ける。
- すべての重要なストレージ管理イベントを収集する必要がある - 調べるべきイベントの数が多いため、重要なイベントの特定が困難になる可能性があり、特定のイベントが実際に何を意味するかについてのベンダーのマニュアル中の記述がかなり曖昧なことがある。関連性の高いイベントを特定する一般的な方法は、アクション（管理ログオンやゾーニング変更の実施など）が実行されたときに生成されたすべてのイベントを収集して、それらを審査して収集候補を特定することである。ベンダーによっては、特定の製品によって生成されるすべてのイベントを列挙した「メッセージマニュアル」を発行している場合があり、このマニュアルが第一歩として役立つことがある。
- ログデータが保存されている - 残念ながら、敵対者もログレコードの存在を知っていて、その生成を阻止しようとしたり、それをアーカイブストレージから消去しようとしたりする可能性がある。

[10] ストレージシステムで TLS を使用する場合の推奨事項が、SNIA のテクニカルポジションとしても入手可能な ISO/IEC 20648 に記載されている。

- ログデータが組織のログデータ保持ポリシーに従ってアーカイブされ、保持されている。
- デバイス時刻が信頼できる外部ソースに同期されている - 多くの場合、インシデント対応は複数のソースからのイベントの分析を必要とするため、潜在的なソースのすべてで時刻が一貫していない場合は、ログ分析が悪夢になる可能性がある。

5.3.2 信頼できるリモートソースへの外部（または集中型）イベントロギングの導入

デフォルトで、多くのデバイスがイベントログをローカルに保持するが、それらを集中管理点に転送すれば、保護が強化されるだけでなく、複数のソースからのイベントの関連づけや分析が容易になる。次の実践が推奨されている。

- 集中型（つまり、単一のセキュリティドメイン内のイベントが共通のポイントに転送される）監査ロギングを実装して複数のソースからイベントを単一のリポジトリに収集する。
- 環境全体で共通の正確な時刻ソースを設置して使用することで、複数のソースからのイベントを正確なタイムラインに揃えて関連づけと分析が行えることを保証する。
- ヘルスモニタリングや問題解決以外では、デバイス内ログの使用を避ける。これは、このようなログは存続期間が短く（オンボードストレージは厳しく制限されることが多い）、敵対者によって容易に消去または変更される可能性が高いためである。
- 複数のログサーバを使用してイベントを収集することで冗長性を確保する。
- syslog などの標準的なロギングプロトコルの、信頼できる配信と安全な転送（TLS 経由など）を提供するバージョンを優先的に使用する。
- イベントをバッファに蓄えて収集点にバッチ送信するのではなく、すぐに転送するようにデバイスを設定する。
- 分析の際は複数のイベントソースを関連づけてインシデントの検出を促進する（例えば、認証サーバで複数の無効なログオンの試みが記録された後に管理クレデンシャルを使用したストレージデバイスへの正常なログオンが行われた場合は、クレデンシャルのブルートフォース攻撃が成功したことを意味する）。
- ストレージイベントロギングがセキュリティ情報イベント管理（SIEM）システムに統合されていることを確認する（そのような製品が使用されている場合）。

5.3.3 完全なイベントロギングの保証

ストレージインフラストラクチャ（およびその補助技術）で発生したイベントの監査ログは、コンプライアンスの評価やセキュリティインシデントの検出および調査のサポートにとって宝の山である。ただし、所有していないデータは使用できないため、監査ログが容量の制限内でできるだけ完全であることを保証することが不可欠である（例えば、監査ログには記録容量が必要であり、記録するイベントが増えて、それを保持する期間が延びれば、記録容量全体も増やす必要がある）。有効で有益な監査ログを提供するために、ISO/IEC 27040 には次の推奨事項が記載されている。

- 関心のあるイベントのセットを決定したら、そのイベントのすべての発生を（インバンドかアウトオブバンドかに関係なく）記録する必要がある。
- *最小*セットのイベントは、常に記録する必要がある。
  - 失敗したログオンの試みと成功したログオンの試み - 短期間の一連の失敗したログオンの試みはブルートフォース攻撃の試みを示している可能性があり、成功したログオンはインフラストラクチャ内でのアクションとそれを実行したエンティティとの対応付けに役立つ。
  - 機密データと高価値データに対する失敗したファイルおよびオブジェクトアクセスの試み - 失敗したアクセスの試みは、インフラストラクチャ内での敵対者による予備調査の実施を示している可能性がある。
  - アカウントとグループプロファイルの追加、変更、および削除 - 侵入の成功後に敵対者がよく使う戦術が権限の昇格である（例えば、不正入手したクレデンシャルを管理者グループに追加する）。敵対者は、侵害したクレデンシャルが発見され、無効にされた場合にアクセスを維持するために新しいクレデンシャルを作成することもできる。
  - ログ設定、ネットワークフィルタリングルール、ゾーニング設定などのシステムセキュリティ設定に対する変更 - これは、敵対者がインフラストラクチャ内のアクセス権を昇格させるもう一つの方法である。
  - セキュリティサーバの用途（syslog、NTP、DNS など）の変更 - 例えば、ネットワーク名を関連するネットワークアドレスにマップするために DNS がよく使用されるが、敵対者が組織のサーバ名を自分たちの管理下のサーバのアドレスにマップし直す可能性がある。
  - システムのシャットダウンと再起動 - 予期せぬシャットダウン／再起動は、再設定などの敵対者のアクションを示している可能性がある。
  - 特権操作
  - 機密ユーティリティの使用
  - 重要なシステムファイルへのアクセス
  - 物理ホスト間での仮想サーバの移動
- 各ログエントリには少なくとも以下を含める必要がある。
  - 日付と時刻の両方を含むタイムスタンプ
  - 重大度レベル - これは、典型的な「設計者の選択」であるため、フィルタリングや分析の観点から重要な場合とそうでない場合がある。例えば、重要なセキュリティイベントに「informational」のコードが付されている可能性がある。
  - ログエントリのソース - つまり、ログレコードを生成したエンティティ。これは、名前の形式にも、ネットワークアドレスの形式にもできる。
  - イベント識別子と、言語ローカライズ可能なテキスト識別子（つまり、イベント ID は定数でも、テキスト識別子はローカル言語に変更できる）。
  - イベントの説明 - テキストの説明の解釈は、広く受け入れられている標準がないうえ、テキストはベンダーで任意に選択されるため、イベントの分析の最も難しい部分である。
- フィルターを慎重に選択する - 前述したように、「重大度」などのフィールドがイベントの重要度の指標として信頼できない可能性がある。組織のロギングおよび保持ポリシーを、関連するイベントがどれで、それらをどのくらい保持するかの最終決定手段にすべきである。

5.3.4　適切なログの保持と保護の実装

監査ログは、コンプライアンスの実証やインシデント調査の支援に使用される場合があるため、適切に保持して保護する必要がある。ISO/IEC 27040 には、次の考慮事項が記載されている。

- 証拠的価値を有する監査ログデータは正しく処理する必要がある - 一般的な法律制度は、保管の継続性、検証可能な完全性、認証性などの法的手続きで使用されるデータに対する要件を課している。
- 特定の保持要件（規制順守など）を伴う監査データは、組織のデータ保持プロセスを使用して保存する必要がある。
- ログの完全性を維持し、それを無許可の変更や破壊（意図的か偶発的かに関係なく）から守るための適切な保護を実装する。
- 監査ログに機密データ（認証情報や暗号鍵など）が含まれている場合は、そのデータの機密性を保証する必要がある。
- 独自の監査ロギング要件（コード署名など）がある場合は、専用の特別に強化されたシステムを使用する必要がある。
- ログリレーやログフィルタリングを使用して特殊なストレージ要件（WORM など）の影響を最小限に抑える。

5.4　システムの強化

強化は、システムの攻撃対象領域を最小化して敵対者が攻撃する機会を制限するプロセスである。システム強化のベストプラクティスには以下が含まれる。

- 不要な／未使用のソフトウェアとサービスを削除／無効化する - 残念ながら、オペレーティングシステムには、すべての環境に必要なわけではないソフトウェアとサービス（その多くがユーザビリティの名目で）が含まれる傾向がある。このような不要なアイテムを無効化または削除すれば、それらの中で見つかった脆弱性によってシステムが危険に晒されることがなくなる。
- 不要なアカウントを削除する。
- デフォルトアカウントを変更（名前の変更、無効化、デフォルトパスワードの変更など）する。
- 必要なネットワークポートだけを有効にする - ポートを閉じるかブロックすれば、そのポートを利用した攻撃ができなくなる。
- 信頼できるソースからのパッチを速やかにインストールする - 基礎となる脆弱性を特定してそれらに対するセキュリティ上の弱点を突く手段を開発するためにベンダーのセキュリティ情報をリバースエンジニアリングすることに、かなりの労力が注ぎ込まれている。パッチをできるだけ速やかにインストールすることが重要である。ただし、「セキュリティパッチ」と思われたものをベクターとした攻撃が何回もあったため、パッチが信頼できるソースから取得されたものであることを保証することも同じように重要である。
- 信頼できるソースからファームウェアを更新する - ファームウェアは、ソフトウェアの一形態に過ぎず、通常は表に出ないものであるため、悪意のあるストレージデバイスファームウェアを使用した攻撃が確認（または認識）されたことはないが、やはり更新は慎重に行う方が良い。

- 最新のマルウェア保護をインストールして維持する - マルウェアは常にある脅威であり、それに対する保護が重要な要件となる。この分野における敵対者の革新は迅速で持続的なため、マルウェア保護を継続的に更新することが不可欠である。

6 追加の SNIA ガイダンス

その他のセキュリティ関連トピックに関するガイダンスは次の SNIA 出版物[11] で確認できる。

SNIA ストレージセキュリティ：サニタイズ - このホワイトペーパーでは、有用性を失った（または保持が不要になった）データを回復不可能なものにすることを不注意な開示に伴うリスクに見合った方法で保証するという重要なトピックが取り上げられている。

SNIA ストレージセキュリティ：暗号化と鍵管理 - 暗号化はデータの機密性の保証において重要な役割を果たすが、正しく実装されていない場合は、保護の幻想をもたらすだけであり、この状態は全く保護されていない状態よりも危険である。このホワイトペーパーでは、暗号化と関連する鍵管理プロセスの正しい実装に関する有益なガイダンスが示されている。

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 - ファイバーチャネルセキュリティプロトコル（FC-SP）は、ストレージインフラストラクチャ内の実体認証などの有益な機能を提供する。このホワイトペーパーでは、FC-SP の概要とそれをストレージインフラストラクチャの保護に効果的に使用するための推奨事項が示されている。

SNIA テクニカルポジション、ストレージシステムの TLS 仕様 - TLS（トランスポート層セキュリティ）は、Web アプリケーションとの相互作用の保護に広く使用されており、このホワイトペーパーでは、ストレージシステム内での TLS の適切な使用に関するガイダンスが示されている（推奨暗号群など）。

主にストレージベンダーが対象であるが、このドキュメントでは、ストレージコンシューマによる要件策定に関する有益な指針が示されている。このドキュメントは ISO/IEC 20648 としても標準化されている。

ISO/IEC 27040 に関する SNIA インデックス - 残念ながら、ISO 標準にはインデックスが含まれていないため、特定の情報を検索するのが困難である。このドキュメントは、標準の広範なインデックスを示し、実務での標準の利用を容易にするものである。

7 まとめ

ISO/IEC 27040 の補足として、このホワイトペーパーでは、特定の環境におけるリスク管理プロセスとして情報セキュリティの概要を示した。ストレージシステムの一般的な脅威カテゴリーを確認してから、ストレージ管理の保護に関する ISO/IEC 27040 のガイダンスを確認した。

読者は、自社の環境内の特定のリスクを評価できる体制を整え、そのようなリスクを許容可能なレベルまで引き下げるために ISO/IEC 27040 に記載されたセキュリティガイダンスを適用する必要がある。

[11] http://www.snia.org/securitytwg からダウンロード可能

8 謝辞

8.1 執筆者について

Richard Austin は、35 年以上 IT 業界に携わっており、ソフトウェア開発者からセキュリティアーキテクトまで務めた経験がある。現在は、HPE Cyber Security でセキュリティアーキテクチャーに携わっている。IEEE と ACM の両方のシニアメンバーであり、CISSP 認定を取得している。SNIA のセキュリティ技術分科会に積極的に参加しながら、INCITS/CS1 を通して国際的な標準化活動にも参加している。

8.2 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。

Eric Hibbard, CISSP	Hitachi Data Systems
Walt Hubis	Hubis Technical Associates
Gary Sutphin	
Tim Hudson	Cryptsoft
Thomas Rivera	Hitachi Data Systems

9 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 に関連づけられた追加の 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 SC 27 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。

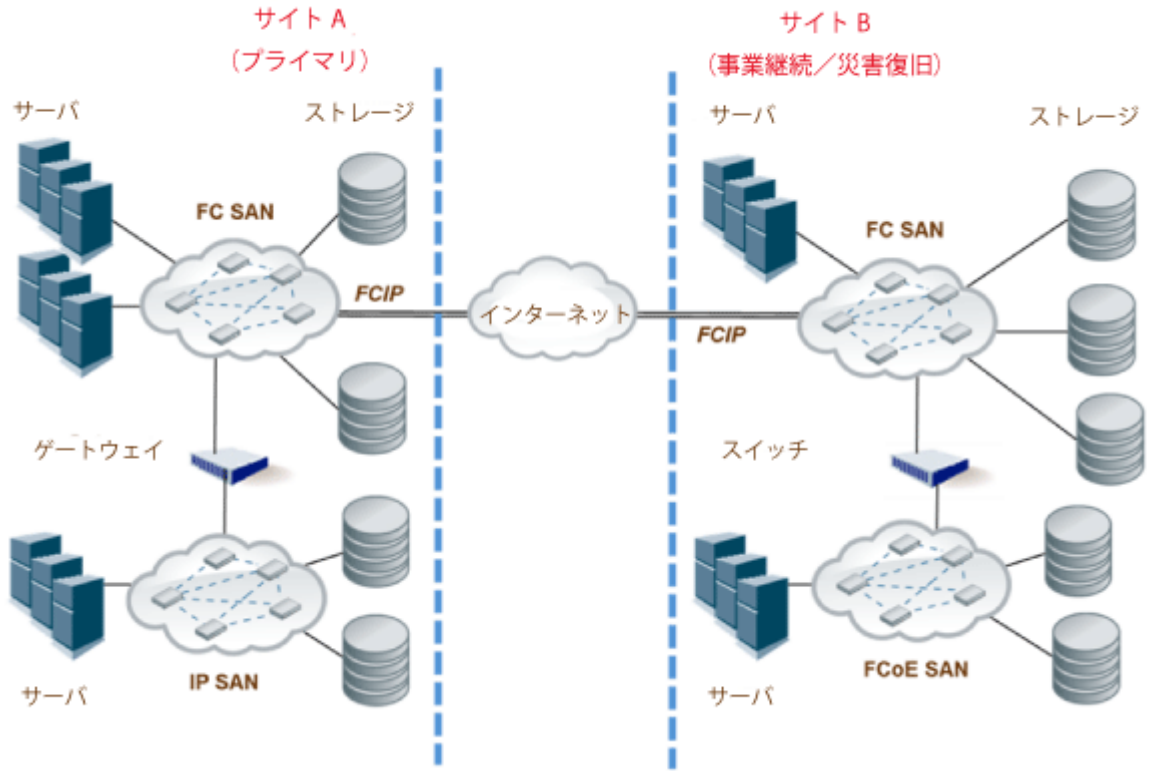
ISO/IEC 27040 は、1) 補助管理と 2) ストレージセキュリティの設計と実装という 2 つの角度からストレージセキュリティガイダンスにアプローチしている。この両方が、セキュリティの知識が不足しているストレージプロフェッショナルやストレージ経験の少ないセキュリティ／監査プロフェッショナルが資料を活用できるように詳しく扱われている。

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、認可、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[12]。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[13]。「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。」

[12] 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）
[13] 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[14]

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[15]。

- 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

[14] 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）

[15] 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）