平成27年度
デジタル映像コンテンツの
セキュリティ対策に関する調査
報告書

第 1.0 版

2016 年 2 月 19 日

NRI セキュアテクノロジーズ

1. 本調査の目的および本報告書の利用方法

デジタル映像コンテンツには、コピーが容易であり、かつ、コピーしても劣化しないという性質がある。そのため、デジタル映像コンテンツが不正にコピーされ、インターネットに公開されると、オリジナルコンテンツと同等の品質の不正コンテンツが流通する恐れがある。DRM による不正コピー対策等の導入に伴い、不正コンテンツの流通を抑止できるようになっているが、動画共有サイトの普及等の環境的な要因もあり、不正コンテンツの流通による著作権侵害等の被害は依然として大きな問題となっている。

本調査は、デジタル映像コンテンツの製作・利用・保存において必要となるセキュリティ管理策について整理したものである。セキュリティ管理策の整理にあたっては、情報セキュリティ管理の国際標準である ISO/IEC 27001 をベースとし、一般的な情報資産を対象とした情報セキュリティ管理策とデジタル映像コンテンツを対象とした情報セキュリティ管理策とに分けて記載している。

デジタル映像コンテンツを対象とした情報セキュリティ管理策については、アメリカ映画協会(MPAA：Motion Picture Association of America, Inc.)[1]が公開しているコンテンツセキュリティベストプラクティス[2] を参考にしている[3]。

本報告書に記載されているセキュリティ管理策は、デジタル映像コンテンツを扱う組織において実施することが望ましい標準的な管理策であり、そのままでは組織の固有の事情や状況に合わない場合があると思われる。したがって、それぞれの組織の事情や状況に合わせて必要な管理策を必要に応じて適宜修正する等して導入・実施するという使い方をしていただくことを想定している

2. デジタル映像コンテンツに求められる情報セキュリティ対策

一般に情報セキュリティにおいて考慮すべき要素には、機密性、可用性、完全性がある。デジタル映像コンテンツのセキュリティ対策においては、通常の情報資産に対するセキュリティ対策に加えて、デジタル映像コンテンツに特有のセキュリティ対策を検討する必要がある。

デジタル映像コンテンツに特有の観点として、コンテンツを扱う組織の内部における機密性、可用性、完全性の確保と、一般の利用者にコンテンツを提供する際の機密性、可用性、完全性の確保というニつの観点でセキュリティ対策を考える必要がある。

また、デジタル映像コンテンツに対して、適切なレベルの(必要にして十分な)情報セキュリティ対策を実施するためには、デジタル映像コンテンツをその重要性や価値に基づいて分類する必要がある。分類の観点としては、有料で提供するコンテンツか無料で提供するコンテンツか、一般に公開するまで厳重な管理が求められるかどうか、残存するオリジナルデータの数が少ないかどうか、いつでも利用できなければならないかどうか、文化的な価値が高いかどうか等が考えられる。このような観点に基づいてコンテンツを分類し、機密性、可用性、完全性のそれぞれについてどのようなセキュリティ対策が必要となるかを明確化する。一方、そのような観点で分類することが難しい場合もあるため、そのような場合には、機密性、可用性、完全性のそれぞれについて、最も高いレベルの情報セキュリティ対策が求められるコンテンツとして分類するというのが、リスク管理の観点からは妥当と考えられる。

以下では、デジタル映像コンテンツの機密性、可用性、完全性を確保するためのセキュリティ対策の概要について述べる。詳細なセキュリティ対策については、次節以降で述べることとする。

◆　機密性の観点

機密性の観点においては、コンテンツの不正コピーを防止すること、正規のアクセス権あるいは正規のライセンスを有する利用者のみがコンテンツを閲覧できるようにすること、有料コンテンツに対して適切に課金を行うこと等が求められる。

◆　可用性の観点

可用性の観点においては、組織の内部および一般の利用者に提供する場合のいずれの場合においても、デジタル映像コンテンツが毀損・喪失した場合でもバックアップを使用してすぐに利用できるようにしておくことが求められる。そのための対策として、バックアップデータを保管するメディアを複数作成する、バックアップデータを保存する媒体を DVD と磁気テープ等 2 つ以上の異なる形態で用意する、バックアップメディアを地理的に離れた場所に保管する等の対策が考えられる。

---

[1] Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Universal City Studios LLC, Twentieth Century Fox Film Corporation, Walt Disney Studios Motion Pictures, Warner Bros. Entertainment Inc. をメンバーとする業界団体

[2] http://www.mpaa.org/content-security-program/

[3] MPAA コンテンツセキュリティベストプラクティスを参照する理由
大手映画配給会社が扱う映画は、全世界で同時公開することから、撮影から編集、パッケージ作成、配給までの全ての工程において、厳重なセキュリティ管理が求められる。そのような要求を満たすために策定されたコンテンツセキュリティガイドラインは、本調査の目的であるデジタル映像コンテンツのセキュリティ確保においても参考になると考えられる。また、本コンテンツセキュリティガイドラインが、実際に企業においてコンテンツのセキュリティ管理のために導入されていることや、MPAA が、米国のデジタル放送におけるコピー制御に関する法規制の議論に関して、議会の公聴会において証言を行っており、信頼のおける団体であると考えられることも本ガイドラインを参考文書とした理由である。

◆　完全性の観点

完全性の観点では、デジタル映像コンテンツの改変・改ざんとコンテンツを記録している物理媒体(磁気テープ、ハードディスク、半導体メモリ等)の劣化(磁気、電荷、結晶状態等の経時的な変化)によるコンテンツの品質劣化[4]という観点からの検討が必要である。

コンテンツの改変・改ざんの観点では、コンテンツが誤って改変される、あるいは、不正に改ざんされることを防止することおよび、そのような改変あるいは改ざんがあった場合に、誤った改変あるいは改ざんされていないファイルを迅速に利用することができるようにすることが求められる。

コンテンツの不正改ざんの防止については、コンテンツファイルへのアクセス制御の実施、改ざんを検知する仕組みの導入等の対策が想定される。編集中のコンテンツの完全性の確保については、編集プロセスの区切りごとにコンテンツのバックアップを作成するとともに、バックアップの作成時には、コンテンツのハッシュを作成し、コンテンツのバックアップとともに保管する等の対策が考えられる。

コンテンツの品質劣化への対応については、コンテンツを記録している物理媒体の劣化による映像や音声の品質低下を検知し、迅速に正常なコンテンツに差し替えることが求められる。

上記に示した対策は、機密性、可用性、完全性を確保するために事前に実施しておくべき対策であるが、事後対策として、万が一デジタル映像コンテンツの機密性、可用性、完全性が侵害されるインシデントが発生した場合のインシデント対応についても対策を講じておく必要がある。具体的には、インシデント対応手順[5]の策定やインシデント対応チームの設置、インシデント対応担当者の任命等である[6]。

以下では、デジタル映像コンテンツの機密性、可用性、完全性を確保するためのセキュリティ対策について、コンテンツを扱う組織の内部における対策、コンテンツの作成等の作業を外部の組織に委託する場合の対策、一般の利用者にコンテンツを提供する場合の対策とに分けて記述する。それぞれに共通する対策については、項目ごとに記載している。

なお、デジタル映像コンテンツを記録する物理媒体の信頼性や耐久性、物理媒体に記録する技術の変化やそれに伴って物理媒体からデータを読みだすための装置が入手不能となる等の問題への対応については、本報告書のスコープ外であるため、他の文書を参照していただきたい[7]。

2.1 デジタル映像コンテンツの機密性を確保するためのセキュリティ対策

デジタル映像コンテンツの機密性を確保するための対策を考える際の観点としては、以下がある。

- コンテンツの利用料：無料か有料か
- 利用者に関する制限：誰でも利用可能か、利用者を制限するか
- 利用場所に関する制限：どこでも利用可能とするか、利用場所を制限するか
- 利用端末に関する制限：どの端末でも利用可能とするか、利用可能な端末を制限するか
- 利用期間に関する制限：無期限に利用可能とするか、利用可能な期間を限定するか

上記の観点がどのように組み合わされるかによって、また、組織の内部におけるコンテンツの機密性確保なのか、一般の利用者に提供する際のコンテンツの機密性確保なのかによって、機密性を確保するために必要なセキュリティ対策は変わってくる。

2.1.1　組織の内部におけるデジタル映像コンテンツの機密性確保

この場合に求められるのは、デジタル映像コンテンツが、組織の外部に誤って流出したり、不正アクセス等により流出したりしないようにするための対策、および、流出した場合に機密性を確保するための対策である。

コンテンツの誤流出や不正流出を防止するための対策としては、一般の情報資産に対する対策と同様に、コンテンツファイルへのアクセス管理の徹底(ユーザごと、あるいは、プロジェクトごとにアクセス制限を行う等)、電子メールによる外部へのファ

---

[4] ここでは、記録媒体にデータを記録する際に利用される物理的な原理・現象(磁気、電荷、結晶状態等)に関わる経時的な変化により、記録されている情報・データの劣化が生じる場合を想定している。たとえば、以下のような現象により、記録されているデジタル映像コンテンツの品質が劣化する場合が想定される。

- 磁気テープや磁気ディスクの磁性体の劣化
- 半導体メモリ(フラッシュメモリ)の電荷の減少
- 結晶状態の変化によりデータを記録する物理媒体における結晶状態の変化

[5] 具体的には、検知、情報収集・状況の把握、関係者への連絡、インシデントかどうかの判断、インシデント対応プロセスを発動するかどうかの判断、インシデント対応プロセスの発動、担当者の招集、被害状況の把握、対応策の実施、封じ込め、復旧、原因究明、是正措置の実施、対応記録の作成という手順になる。

[6] インシデント対応に関する資料として、JPCERT/CC (https://www.jpcert.or.jp/ir/)、IPA (https://www.ipa.go.jp/security/awareness/johorouei/)等がある。

[7] 記録媒体の物理的な劣化に伴うコンテンツの品質の低下については、2.3 において述べる。

イル送信の禁止、外部へのファイル送信時の業務管理責任者による承認プロセスの導入、外部へファイルを送信する際のファイルの暗号化やVPN 等の暗号化された通信路の使用、デジタルコンテンツ管理システムの導入等がある。

デジタルコンテンツ管理システムは、デジタル映像コンテンツがどの端末に保存されているのか、どの端末・物理メディアにコピーされたのか等、全てのデジタル映像コンテンツの所在およびデジタル映像コンテンツに対して行われた操作を記録し、デジタル映像コンテンツが不正に、あるいは、意図しない状況でコピーや利用がされないようにするためのシステムである。また、デジタルコンテンツに対して実行された操作についてのログ(操作実行時間、操作実行者、操作対象ファイル名、操作の内容：移動、コピー、削除、変更等)の作成・チェックを行うことにより、コンテンツに対する不正な操作やコンテンツの外部への転送等が行われていないかどうかを確認するという機能を有するシステムである。

デジタル映像コンテンツの編集プロセスにおけるセキュリティ対策としては、以下が挙げられる。

- デジタル映像コンテンツ編集用の情報システムを特定の端末に制限する。
- デジタル映像コンテンツ編集用の情報システム以外の端末にデジタル映像コンテンツを保存しない。
- デジタル映像コンテンツを物理メディアに記録するための端末を特定の端末に制限する。

組織内部でのデジタル映像コンテンツのやりとりの際に使用するUSB メモリ等の可搬記憶媒体のマルウェア感染・紛失等の対策としては、コンテンツを記録する際に暗号化を行う、セキュリティ機能つきのUSB メモリを使用する、素性が明らかでないシステムに接続しない、PC の外部記憶媒体接続時の自動実行機能を無効化する等がある。

上記以外の組織の内部におけるデジタル映像コンテンツの機密性確保のための対策としては､以下のような対策が考えられる。

- 全てのデジタル映像コンテンツの所在や利用状況を管理・監視・記録し、不正利用・改ざん等の有無を監視する。具体的には、デジタルコンテンツ管理システムを導入する等。
- 秘密分散技術を使用して、デジタル映像コンテンツを複数のパーツに分けて異なるシステムに保存することにより、コンテンツの一部が漏えいするあるいは、不正に取得される等した場合でも、コンテンツ全体の漏えい・不正取得を防止する
- 組織内・組織間で通信路を経由してデジタル映像コンテンツをやりとりする際に、VPN 等の暗号化された通信路を使用する

万が一デジタル映像コンテンツが組織外に流出した場合に、コンテンツの不正利用を防止するための対策としては、以下がある。

- コンテンツの不正な複製の防止：DRM によるコピー防止／コピー回数制限
- 物理メディアに記録されたコンテンツへのアクセス制限：コンテンツを暗号化して記録する、ハードディスク全体を暗号化する、セキュリティ機能つきの可搬記憶媒体を利用する等
- デジタル映像コンテンツへのアクセス制御：DRM 等により権限を有するユーザのみがデジタル映像コンテンツにアクセスできるようにする

2.1.2 外部の組織との間でデジタル映像コンテンツのやり取りが行われる場合の機密性確保

デジタル映像コンテンツの制作には、映像製作会社、編集会社、個人で事業を営む者等さまざまな主体が関係する。デジタル映像コンテンツの機密性の確保においては、これらの主体間でデジタル映像コンテンツがやり取りされることを想定した対策の実施が必要となる。

基本的な対策は、組織の内部におけるデジタル映像コンテンツの機密性確保に必要な対策と同様であるが、外部の組織に業務を委託する、あるいは、外部の組織と業務を分担する場合に、委託元の組織や業務全体の責任を負う組織には、機密性を確保するために委託先の組織や業務を分担する組織を適切に管理することが求められる。

したがって、.外部の組織との間でデジタル映像コンテンツのやり取りが行われる場合には、3 章の A.15 外部委託先のセキュリティ管理に記載されている管理策を実施するとともに、2.1.1　組織の内部におけるデジタル映像コンテンツの機密性確保に記載されている対策を必要に応じて実施することとする。

2.1.3 一般の利用者にデジタル映像コンテンツを提供する際のコンテンツの機密性確保

誰でも無料で閲覧・視聴が可能なコンテンツであっても、コンテンツの動画配信サイトへの不正なアップロードの防止や、不正にDVD 等に複製して販売・配布する等の行為の防止が必要となる。そのためには、ストリーミングによる配信に限定する(コンテンツのダウンロードは許可しない)、DRM によりコンテンツのライセンス管理を実施する、コンテンツの不正な複製を抑止するといった対策が必要となる。

その他、必要に応じて、コンテンツを利用可能な場所の制限、コンテンツを利用可能な期間の制限、コンテンツの漏えい・不正入手の防止等の対策を実施する。

組織外部からの不正アクセスによるデジタル映像コンテンツの不正ダウンロード・漏えい等の防止のための管理策としては、

一般の情報資産に対する対策と同様にファイアウォール等の境界セキュリティ対策の導入、ウェブサイトの定期的な(6 か月に 1 回程度)脆弱性チェックおよび修正プログラムの適用、ウェブサイトのペネトレーションテスト[8]の定期的な実施(6 か月に 1 回程度)と発見された脆弱性の是正等が挙げられる。

内部からの不正アクセス等への対策としては、デジタル映像コンテンツを保存する情報システムと業務用ネットワークとを物理的あるいは論理的に分離することや、デジタル映像コンテンツを扱う情報システムのインターネット接続の禁止等が挙げられる。

以上を整理すると、一般の利用者にデジタル映像コンテンツを提供する際に必要となる機密性確保のための対策として、以下のような対策が挙げられる。

- コンテンツの複製抑止 ：DRM によるコピー防止／コピー回数制限
- 物理メディアに記録されたコンテンツへのアクセス制限： コンテンツの暗号化によりライセンス保有者のみ閲覧可能とする
- 再生機器の制限：配信先の端末の認証(ID・パスワード等による)や、DRM[9] による再生可能機器の制限
- 利用者の制限：ID・パスワード等による利用者認証や DRM を利用した閲覧制御により、ライセンス保有者のみ閲覧可能とする
- 利用場所の制限： 特定の場所に設置された端末でのみ利用可能とする
- 利用可能期間の制限：DRM による利用可能期間の制限
- 有料コンテンツの場合、課金メカニズムの実装： 否認防止を可能とする課金メカニズム
- 配信先の端末においてコンテンツのダウンロードを抑止するためにストリーミングによる配信に限定する
- 動画配信サイトへのアップロードの防止 ：DRM によるコンテンツのライセンス管理
- コンテンツの漏えい・不正取得の防止： 秘密分散技術を使用して、コンテンツを複数のパーツに分けて異なるシステムに保存することにより、コンテンツの一部が漏えいするあるいは、不正に取得される等した場合でも、コンテンツ全体の漏えい・不正取得を防止する

2.2 デジタル映像コンテンツの可用性を確保するためのセキュリティ対策

可用性の要件は、デジタルコンテンツを利用する権限・ライセンスを持つ者が、必要な時にいつでもデジタルコンテンツを利用することができることである。そのためには、デジタルコンテンツが、適切なアクセス制御がされた上で、サーバに保存されていることが必要である。

デジタルコンテンツ自体の可用性を確保するための対策に加えて、コンテンツを提供する情報システムの可用性が適切に確保されている必要がある。

また、デジタル映像コンテンツの可用性を考える場合、コンテンツの重要度についても考慮する必要がある。コンテンツの重要度とは、たとえば、オリジナルのアナログフィルムの残存数が少なく、また、フィルム自体が劣化しているような場合、当該フィルムからデジタルデータへの変換を行う回数が制限される場合が考えられる。このように、デジタルデータへの変換を行うことができる回数が制限される場合、そのコンテンツの重要度を高いと考え、他のコンテンツよりも厚く、完全性を確保するための対策を実施する必要がある。

たとえば、バックアップデータを保存する媒体を DVD と磁気テープの 2 つの異なる形態で用意する、デジタル化されたデータの複製を複数作成しておき、互いに地理的に離れた場所に保管することにより、いずれかのデジタルデータが毀損・喪失した場合でも、他の複製されたデータにより、可用性が確保できるようにしておく等の対策が考えられる[10]。

2.2.1 組織の内部におけるデジタル映像コンテンツの可用性確保

組織の内部におけるデジタル映像コンテンツの可用性の観点としては、編集中のコンテンツの可用性と既存のコンテンツの可用性がある。

編集中のコンテンツの可用性については、コンテンツの受け渡し時のセキュリティ対策、通信路を経由して転送する際のセキュリティ対策、編集プロセスにおけるセキュリティ対策が考えられる。

既存のコンテンツの可用性については、コンテンツ保存用のサーバの設置やコンテンツのバックアップの取得と安全な保管等が考えられる。

以上を整理すると、組織の内部におけるコンテンツの可用性確保のための対策として、以下のような対策が挙げられる。

- 組織内･組織間で物理メディアを介してデジタル映像コンテンツをやりとりする際に、たとえば、バックアップ用の USB メモリを用意し、一つを紛失してもすぐにバックアップできるようにしておく。

---

[8] システムやネットワークに、攻撃に利用される可能性がある脆弱性が残っていないかどうかをチェックするために、疑似的な攻撃を行うことにより実施されるテスト

[9] Digital Rights Management： デジタル著作権管理　デジタルコンテンツの著作権などの権利が侵害されることを防止するために、コンテンツの利用や複製を制限するための仕組み

[10] 最近増加している攻撃手法として、コンピュータに保存されているデータを不正に暗号化し、データの復号と引き換えに金銭を要求するというものがあることから、データのバックアップを取得することの重要性は増している。

- デジタル映像コンテンツを記録した物理媒体を組織外に送付する場合に、信頼できる輸送業者を利用する。
- 編集プロセスの区切りごとにデジタル映像コンテンツのバックアップを作成する。
- デジタル映像コンテンツのバックアップを複数の物理メディアに保存し、地理的に離れた場所に保管する。
- デジタル映像コンテンツを保存するための専用サーバを組織内に設置する。
- デジタル映像コンテンツ保存用サーバを二重化する。

2.2.2 外部の組織との間でデジタル映像コンテンツのやり取りが行われる場合の可用性確保

デジタル映像コンテンツの制作には、映像製作会社、編集会社、個人で事業を営む者等さまざまな主体が関係する。デジタル映像コンテンツの可用性の確保においては、これらの主体間でデジタル映像コンテンツがやり取りされることを想定した対策の実施が必要となる。

基本的な対策は、組織の内部におけるデジタル映像コンテンツの可用性確保に必要な対策と同様であるが、外部の組織に業務を委託する、あるいは、外部の組織と業務を分担する場合に、委託元の組織や業務全体の責任を負う組織には、可用性を確保するために委託先の組織や業務を分担する組織を適切に管理することが求められる。

したがって、.外部の組織との間でデジタル映像コンテンツのやり取りが行われる場合には、3 章の A.15 外部委託先のセキュリティ管理に記載されている管理策を実施するとともに、2.2.1　組織の内部におけるデジタル映像コンテンツの可用性確保に記載されている対策を必要に応じて実施することとする。

2.2.3 一般の利用者にデジタル映像コンテンツを提供する際のコンテンツの可用性確保

一般の利用者に対して、デジタル映像コンテンツ提供サービスを継続して提供する上で求められる情報セキュリティ対策として、以下が挙げられる。これらの対策を全て実施しなければならないということではなく、求められるサービスレベルに応じて、必要な対策を選択し実施する。

- 一定のサービスレベル(映像コンテンツの品質)の確保

  デジタル映像コンテンツの品質を確保するための対策として、データパケットの遅延時間を一定以下に抑える等が挙げられる。具体的には以下のような対策である。

  - ✓ サーバの過負荷防止：トラフィックコントロール装置の導入、負荷分散装置の導入(DoS 攻撃対応)
  - ✓ ウェブサイトの性能の維持管理
    - 必要に応じて、ハードウェア、ソフトウェアのアップグレードを行う
  - ✓ ネットワーク回線の帯域幅の拡張

- デジタル映像コンテンツを提供するウェブサイトの可用性確保

  - ✓ ウェブサイトの定期的な(6 か月に 1 回程度)脆弱性チェック・適時の修正プログラムの適用
    - 脆弱性情報の収集、ベンダが発行する修正プログラムの取得および適用
    - Web サーバに使用されているハードウェア、ソフトウェアのバージョンを最新に保つこと
    - Web サーバに使用されているハードウェア、ソフトウェアのインベントリ管理
  - ✓ ウェブサイトの定期的な(6 か月に 1 回程度)ペネトレーションテストの実施
  - ✓ バックアップサイトの設置：バックアップサイトの形態は、求められるサービスレベルにより決定する。
  - ✓ ウェブサイト掲載データ(コンテンツファイル等)のバックアップ取得・安全な保管
  - ✓ ウェブサイトの設定データのバックアップ取得・安全な保管
  - ✓ バックアップデータの遠隔地保管
  - ✓ バックアップデータがリストアできることの確認

デジタル映像コンテンツ提供サービスに求められるサービスレベルとしては、たとえば、ストリーミングによるスポーツの生中継のような、途中で配信が中断してはならないようなクリティカルなコンテンツは、現時点ではないという前提を置くこととする。従って、求められるサービスレベルとしては、途中でコンテンツの配信が中断した場合には、最初から、あるいは、中断したところから再開されることとし、そのために必要な対策を実施することでよい。

2.3 デジタル映像コンテンツの完全性を確保するためのセキュリティ対策

デジタル映像コンテンツの完全性を確保する上で求められるのは、コンテンツの誤った改変や不正な改ざんの防止、コンテンツを記録している物理媒体の劣化によるコンテンツの品質劣化の防止およびデジタル映像コンテンツ提供サービスを提供するウ

ェブサイトに掲載されているデジタル映像コンテンツコンテンツの改ざんを防止することである。
コンテンツの品質劣化については、コンテンツを記録している物理媒体(磁気テープ、ハードディスク、半導体メモリ等)の劣化によるコンテンツの品質劣化への対策が必要である。
また、電子透かしを使用して、不正に複製されたデジタルコンテンツを検知することも完全性確保のための対策として検討する必要がある。
デジタル映像コンテンツの完全性を確保するための情報セキュリティ対策として、以下が挙げられる。

2.3.1 組織の内部におけるデジタル映像コンテンツの完全性確保

デジタル映像コンテンツの改変・改ざんの観点では、コンテンツが誤って改変される、あるいは、不正に改ざんされることを防止することおよび,そのような改変あるいは改ざんがあった場合に、改変あるいは改ざんされていないファイルを迅速に利用することができるようにすることが求められる。デジタル映像コンテンツの品質劣化については、コンテンツを記録している媒体の劣化による映像や音声の品質低下を検知し、迅速に正常なコンテンツに差し替えることが求められる。
編集中のデジタル映像コンテンツの完全性の確保については、編集等の作業プロセスの各段階においてデータの改ざんや劣化がないことを確認するために、コンテンツをハッシュ化したデータを保存しておき、次の段階の作業実施時に、対象のコンテンツファイルのハッシュ値と保存されているコンテンツファイルのハッシュ値を比較し、同一であれば、改ざんや劣化がないと判断する。もしデジタル映像コンテンツの改ざんや劣化があった場合には、改ざんや劣化がないことが確認されたデジタル映像コンテンツで置き換える。
ハードディスクから DVD にデジタル映像コンテンツをコピーする等、異なるメディアにコンテンツをコピーする(メディア変換)場合、オリジナルコンテンツのハッシュ値を保管しておき、メディア変換後のコンテンツのハッシュ値をオリジナルコンテンツのハッシュ値と比較することにより、変換後のコンテンツの改ざんや劣化がないことを確認できるようにすることも必要である。
また、デジタル映像コンテンツを物理メディアに記録する際には、物理メディアに記録されているコンテンツが改変・改ざんされていないことが保証されていることが求められる。そのための対策として、コンテンツを記録する物理メディアに Write Once 型の記録媒体(CD-R、DVD-R 等)を使用することが挙げられる。
コンテンツを記録している物理媒体の劣化に起因するコンテンツの品質劣化への対策を含む包括的な完全性確保のための対策として、改ざん検知、完全性チェックツールの導入も考えられる。
組織の内部におけるデジタル映像コンテンツの可用性確保に必要な対策は以下の通りである。

- コンテンツのハッシュ値を保存しておき、編集作業中に元に戻す必要がある場合やコンテンツを他のメディアにコピーした際にハッシュ値の比較により、改ざんや劣化がないことのチェックができるようにする
- コンテンツの暗号化や電子透かしの挿入、改ざん検知ツール、完全性チェックツールの導入
- 物理メディアへの記録の制限 :Write Once 型の記録媒体(CD-R、DVD-R 等)の使用等
- コンテンツを記録している物理媒体の劣化による映像や音声の品質低下を検知し、迅速に正常なコンテンツに差し替えるための手順を策定し、適切に運用する

2.3.2 外部の組織との間でデジタル映像コンテンツのやり取りが行われる場合の完全性確保

デジタル映像コンテンツの制作には、映像製作会社、編集会社、個人で事業を営む者等さまざまな主体が関係する。デジタル映像コンテンツの完全性の確保においては、これらの主体間でデジタル映像コンテンツがやり取りされることを想定した対策の実施が必要となる。
基本的な対策は、組織の内部におけるデジタル映像コンテンツの完全性確保に必要な対策と同様であるが、外部の組織に業務を委託する、あるいは、外部の組織と業務を分担する場合に、委託元の組織や業務全体の責任を負う組織には、完全性を確保するために委託先の組織や業務を分担する組織を適切に管理することが求められる。
したがって、.外部の組織との間でデジタル映像コンテンツのやり取りが行われる場合には、3 章の A.15 外部委託先のセキュリティ管理に記載されている管理策を実施するとともに、2.3.1 組織の内部におけるデジタル映像コンテンツの完全性確保に記載されている対策を必要に応じて実施することとする。
編集途中でのコンテンツの品質低下を未然に防止するためには、コンテンツを記録している物理媒体の劣化による映像や音声の品質低下を検知し、迅速に正常なコンテンツに差し替えるための仕組みや手順・ツールを導入することも重要である。

2.3.3 一般の利用者にデジタル映像コンテンツを提供する際のコンテンツの完全性確保

一般の利用者にデジタル映像コンテンツを提供する際のデジタル映像コンテンツの完全性確保に必要な対策は以下の通りである。
2.3.1 組織の内部におけるデジタル映像コンテンツの完全性確保に記載されている対策と同様に、コンテンツをハッシュ化し

たデータを保存しておき定期的にデジタル映像コンテンツ提供ウェブサイトに掲載されているコンテンツファイルのハッシュ値と保存されているコンテンツファイルのハッシュ値を比較し、同一であれば、改ざんや劣化がないと判断する。もしデジタル映像コンテンツの改ざんや劣化があった場合には、改ざんや劣化がないことが確認されたデジタル映像コンテンツで置き換える。

コンテンツを記録している物理媒体の劣化に起因するコンテンツの品質劣化への対策を含む包括的な完全性確保のための対策として、改ざん検知、完全性チェックツールの導入も考えられる。

また、以下の対策も必要に応じて実施する。

- デジタル映像コンテンツの暗号化や電子透かしの挿入、改ざん検知ツール、完全性チェックツールの導入
- デジタル映像コンテンツ提供ウェブサイトへの不正アクセスの防止：Web アプリケーションファイアウォールの導入
- デジタル映像コンテンツ提供ウェブサイトの改ざん検知ツール、完全性チェックツールの導入
- コンテンツを記録している物理媒体の劣化による映像や音声の品質低下を検知し、迅速に正常なコンテンツに差し替えるための手順を策定し、適切に運用する

電子透かしについては、デジタル映像コンテンツの不正利用を牽制・検出するための対策として使用することができる[11]。

3. ISO/IEC 27001 に基づく情報セキュリティ管理策

一般的な情報資産を対象とした情報セキュリティ管理策とデジタル映像コンテンツを対象とした情報セキュリティ管理策を、ISO/IEC 27001 に基づいて記載する。多くの情報セキュリティ管理策は、一般的な情報資産と情報セキュリティ管理策とデジタル映像コンテンツにおいて共通であるが、デジタル映像コンテンツに特有の情報セキュリティ管理策については、枠で囲うことにより、一般的な情報資産を対象とした情報セキュリティ管理策との記載上の区分を行っている。

なお、管理策に付与されている番号は、ISO/IEC 27001 の管理策との対応をとり易くするために、ISO/IEC 27001 の管理策の番号に合わせているため、開始番号が 5 となっている。

A.5.1.1　情報セキュリティのための方針

情報セキュリティ方針および各種対策を定義し、管理者の承認をもって発行し、職員及び関連する外部関係者に伝えること。

当センターが保有する情報資産を、情報セキュリティ上のリスクから保護するため、情報セキュリティポリシーに基づく情報セキュリティ対策を策定し、職員及び関連する外部関係者に周知徹底すること。

特に、デジタル映像コンテンツを保護するための情報セキュリティ管理策について、一般の情報資産に求められる管理策に加えて必要な管理策を策定すること。たとえば、デジタル映像コンテンツに対するアクセスや操作に関するログの取得、デジタル映像コンテンツを物理メディアに保存する場合に必要な管理策や、デジタル映像コンテンツを記録した媒体を処分する場合の管理策等である。

A.5.1.2　情報セキュリティのための方針のレビュー

情報セキュリティのための方針は、あらかじめ定められた間隔又は重大な変化が生じた場合に、それが適切・妥当で且つ有効であることを継続するためにレビューすること。

A.6 情報セキュリティのための組織

A.6.1.1　情報セキュリティの役割及び責任

情報セキュリティ対策の立案、維持管理、管理策の導入・運用を行うために、以下の担当者を設置する。

- 情報セキュリティ管理責任者

各部署における情報セキュリティ管理策の導入・運用計画を策定する。また、情報セキュリティ担当者に対して、情報セキュリティ管理策の導入・運用に関する指示を行う。

計画の進捗状況を確認し、計画の達成に必要な施策の実施や計画の見直しを行う。

既に実施している情報セキュリティ管理策が適切に導入・運用されているかどうかについて定期的に(半年または 1 年に 1

[11] たとえば、デジタルシネマ(DCI)に準拠した映画館におけるスクリーンの不正な撮影によるコンテンツの盗用の牽制・抑止

回)および組織の業務や組織体制、業務プロセス、情報システムに変更が生じた場合に)レビューを行う。

- 情報資産管理責任者

組織が保有する全ての情報資産の特定および、情報資産一覧表の作成および維持管理を行う。
情報資産の数が多い場合には、複数の情報資産管理責任者を任命する。

- 情報セキュリティ担当者

情報セキュリティ管理責任者の指示に基づいて、情報セキュリティ管理策の導入・運用の実務を行う。
情報セキュリティ管理責任者に対して、情報セキュリティ管理策の導入・運用状況の報告を行う。

A.6.1.2　職務の分離

組織の情報資産に対する、意図しない変更や不正利用のリスクを低減するために、依頼・承認・権限付与等の各職務を分離することで、
情報資産を恣意的に使用しないようにすること。
例：ユーザが自らのアクセス権の付与を行わない(アクセス権の付与をユーザとは異なる人が行うようにする)。

想定されるリスク：ユーザが恣意的に情報資産へのアクセス権を割り当てることにより、情報資産の不正利用等が発生する。

A.6.1.3　関係当局との連絡

監督省庁との適切な連絡体制(連絡先リストの維持・更新、連絡担当者の任命、組織内での連絡網の整備等)を維持することで、情報セキュリティインシデント発生時等に速やかに連絡が取れるよう整備しておくこと。

想定されるリスク：インシデントに関する報告が遅れることにより、対応に遅れが生じ、被害が拡大する可能性がある。

A.6.2.1　モバイル機器の方針

モバイル機器を使用することによって生じる情報セキュリティリスクを管理するための対策を講じること。
対策の例：
1) モバイル機器の組織外への持ち出しは、許可された職員のみ可能とすること。
2) モバイル機器の組織外への持ち出しに関する申請手続きを整備し、適切に運用すること。
3) 個人所有のモバイル機器の業務利用（BYOD）は禁止する。
4) デジタル映像コンテンツを扱う情報システムが設置されているエリアへの個人所有端末(スマートフォン、携帯 PC、デジタルカメラ等)の持ち込みを禁止する。
5) デジタル映像コンテンツをモバイル機器に保存することを禁止する。
6) 業務上やむを得ず、デジタル映像コンテンツをモバイル機器に保存する場合には、暗号化(AES 128bit 以上)を必須とする。
7) デジタル映像コンテンツを保存するモバイル機器の盗難・紛失等に備えて、リモートからのコンテンツの削除を可能とすること。

想定されるリスク：モバイル機器からの情報漏えい、個人所有端末を使用したデジタル映像コンテンツの窃盗

A.7 人的資源のセキュリティ

A.7.1.2　雇用条件

職員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない。

デジタル映像コンテンツに関わる全ての職員および外部委託先従業員から、秘密保持契約あるいは守秘義務契約に関する誓約書を受領すること。

A.7.2.1　組織の長の責任

組織の長は、組織の確立された方針及び手順に従った情報セキュリティの適用を全ての職員及び外部委託先従業員に要求しなければならない。

A.7.2.2　情報セキュリティの教育及び訓練

採用時・異動時・職種変更時あるいは、その他定期的に(半年または 1 年に 1 回)、全職員および外部関係者に対し、情報セキュリティを含む職務に関連する組織の方針及び手順についての教育・訓練を提供すること。

想定されるリスク：情報セキュリティに関する知識や理解の不足によるマルウェア感染や情報漏えい等の情報セキュリティインシデントの発生

A7.2.3　懲戒手続

情報セキュリティ違反(本ポリシーに記載されている事項に違反した行動)を犯した職員に対する懲戒手続を備えること。

想定されるリスク：情報セキュリティに対する意識が低い職員や情報セキュリティポリシーを遵守しない職員による情報セキュリティインシデントの発生

A.7.3.1　雇用の終了又は変更に関する責任

雇用・業務契約の終了又は変更に際して、守秘義務契約等を対象者となる職員又は外部関係者と締結し、遵守するよう要求すること。

想定されるリスク：職員又は外部関係者による機密情報やデジタル映像コンテンツの不正持ち出し等のリスクの増加

A.8 資産の管理

A.8.1.1　情報資産一覧表

組織が保有する全ての情報資産およびデジタル映像コンテンツを特定し、情報資産一覧表を作成の上維持管理すること。
情報資産およびデジタル映像コンテンツには、ユニークな識別番号を付与し、管理すること。

情報資産一覧表の更新は、新規情報システム・機器の導入、既存の情報システムの変更・更新、新規アプリケーションの導入、新規デジタル映像コンテンツの作成・保存、新規の可搬記憶媒体の導入、情報システム・デジタル映像コンテンツ・可搬記憶媒体の廃棄等を契機として実施すること。

想定されるリスク：組織が把握していない情報資産およびデジタル映像コンテンツの不正持ち出しや不正に持ち出されたことに気付かない

A.8.1.2　情報資産の管理責任

情報資産一覧表で維持・管理される情報資産およびデジタル映像コンテンツに対して、その管理責任者を定めること。管理責任者には、A6.1.1 に記載の情報資産管理責任者を任命することとするが、他の者を任命してもよい。

想定されるリスク：情報資産一覧表の維持・管理に責任を持つ担当者がいない結果、組織が把握していない情報資産やデジタル映像コンテンツが増加し、それらの不正持ち出しや紛失等のリスクが増加する。

A.8.1.3　情報資産の利用範囲

組織が保有する全ての情報資産について、それらの利用者・利用部門を特定し、情報資産の保存期間・保存方法とともに情報

資産一覧表に明記すること。

想定されるリスク：組織が把握していない情報資産やデジタル映像コンテンツが発生し、それらの不正持ち出しや紛失等のリスクが増加する

A.8.1.4　情報資産の返却

職員及び関連する外部関係者は、雇用または契約が終了した時点で、センターが貸与した情報資産を全て返却すること。
また、異動により職務上不要となった時点でも、同様に返却すること。
情報資産の例：PC、モバイル機器、可搬記憶媒体等

想定されるリスク：職員又は外部関係者による情報資産の不正持ち出し

A.8.2.1　情報資産の分類

情報資産やデジタル映像コンテンツの価値や漏えいした場合の影響等を考慮し、情報資産の分類を行うこと。

想定されるリスク：情報資産の重要度に応じた適切な情報セキュリティ管理策が実施されないことによる、影響や被害の大きい情報セキュリティインシデントの発生

A.8.2.3　情報資産の取扱い

資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施しなければならない。

デジタル映像コンテンツ編集用の情報システムを特定のシステムに制限する。
デジタル映像コンテンツ編集用の情報システム以外のシステムにデジタル映像コンテンツを保存しない。
デジタル映像コンテンツを物理メディアに記録するためのシステムを特定のシステムに制限する。
デジタル映像コンテンツを扱う情報システムへの組織外からのリモートアクセスを禁止する。
デジタル映像コンテンツの完全性の確保については、たとえば、編集等の作業プロセスの各段階においてデータの改ざんや劣化がないことを確認するために、コンテンツをハッシュ化したデータを保存しておき、次の段階の作業実施時に、対象のコンテンツファイルのハッシュ値と保存されているコンテンツファイルのハッシュ値を比較し、同一であれば、改ざんや劣化がないと判断する。
また、ハードディスクから DVD にデジタル映像コンテンツファイルをコピーする等、異なるメディアにコンテンツをコピーする(メディア変換)場合、オリジナルコンテンツのハッシュ値を保管しておき、メディア変換後のコンテンツのハッシュ値をオリジナルコンテンツのハッシュ値と比較することにより、変換後のコンテンツの改ざんや劣化がないことを確認できるようにする。

想定されるリスク：情報資産やデジタル映像コンテンツの価値や漏えいした場合の影響に応じたセキュリティ対策が実施されていない場合、不正アクセス等により、情報資産やデジタル映像コンテンツの漏えい・不正利用が発生する。

A.8.3.1　取り外し可能な媒体(可搬記憶媒体)の管理

可搬記憶媒体の管理手順を策定し、文書化し、実施すること。
可搬記憶媒体の利用は、許可された職員のみに限定すること。ただし、業務上必要な場合は、別途判断することとする。

デジタル映像コンテンツの可搬記憶媒体への保存は、バックアップを作成する場合を除き、原則として禁止する。
業務上やむを得ず、デジタル映像コンテンツを可搬記憶媒体へ保存する場合は、暗号化を必須とする。
デジタル映像コンテンツが記録された可搬記憶媒体を組織の外部に持ち出す場合の承認手続きを規定すること。
デジタル映像コンテンツが記録された可搬記憶媒体を組織の外部に持ち出す場合、持ち出しを行う者、持ち出し日、返却予定日、返却日、持ち出し対象のコンテンツの名称、媒体の形式、持ち出しの理由、持ち出し先等を記録した可搬記憶媒体持ち出し記録を作成し保存すること。

想定されるリスク：可搬記憶媒体の不正使用や紛失等による情報資産やデジタル映像コンテンツの漏えい

A.8.3.2　媒体の処分

情報資産が不要になった場合は、紙媒体は再生不可能なように速やかに裁断または溶解し、電子媒体についてはデータが復旧できないよう、物理的に破壊すること。

デジタル映像コンテンツが記録された媒体(DVD、ハードディスク、USB メモリ等)については、上記の事項に特に留意の上処分すること。
デジタル映像コンテンツが記録された媒体の処分に関する承認プロセスを規定し実施すること。
デジタル映像コンテンツが記録された媒体の処分について、処分対象の媒体の名称や媒体の形態、処分日時、作業実施者等を記録したログを作成し、保存すること。
デジタル映像コンテンツが記録された媒体の処分について、作業を外部の事業者に委託することを禁止する。
やむを得ず外部の事業者に委託する場合は、委託先で業務に携わる全ての従業員から署名入りの秘密保持契約書あるいは守秘義務契約書を受領すること。
委託先から、媒体が確実に廃棄されたことを証明する廃棄証明書を受領すること。

想定されるリスク：デジタル映像コンテンツが記録された媒体が正しく処分されていなかったために、情報資産やデジタル映像コンテンツが不正に使用される

A.8.3.3　物理的媒体の輸送

情報資産を記録した媒体は、輸送の途中の不正アクセス・不正使用・破損・盗難から保護すること。

デジタル映像コンテンツを記録した媒体を組織外の場所へ輸送する場合、媒体に記録するコンテンツの暗号化(AES 128 bit 以上)を必須とする。
輸送する際には、媒体を鍵付きの運搬ケースに格納すること。可能であれば、GPS 装置による媒体の追跡ができること。
媒体の輸送を外部の業者に委託する場合、信頼できる輸送業者を利用すること。その際に、輸送業者との間で秘密保持契約あるいは守秘義務契約を締結すること。
また、輸送業者との契約には、輸送途中での媒体の紛失等があった場合の輸送業者の責任や損害賠償に関する規程を記載すること。
輸送対象の全ての媒体について、発送するコンテンツの名称、発送作業実施者、発送先名称、発送数、発送日時等を記録したログを作成すること。
媒体の輸送を外部の業者に委託する場合、輸送業者から配送先が媒体を受領したことを証明する受領書を受領すること。

想定されるリスク：情報資産やデジタル映像コンテンツを記録した媒体の紛失や権限を持たないユーザによる不正利用

A.9 アクセス制御

A.9.1.1　アクセス制御方針

情報資産へのアクセス権については、業務上必要な職員のみに割当てること。
情報資産へのアクセス権の割当てに関する手続きを規定し、業務管理責任者による承認を得たのちに割当てること。

想定されるリスク：業務上必要のない職員や不正ユーザによる情報資産やデジタル映像コンテンツへの不正アクセスや不正利用

A.9.2.1　利用者登録及び登録削除

情報システムおよび報資産の利用者の登録抹消のプロセスを実装し、適切に運用すること。

デジタル映像コンテンツを扱う情報システムについては、特に厳格な運用を行うこと。たとえば、ユーザアカウントの管理をプロジェクトごとに実施し、プロジェクト終了時に全てのユーザアカウントを削除する等。

想定されるリスク：業務上必要がないユーザのアカウントが削除されずに残っていることにより、当該ユーザあるいは当該アカウントを不正利用した者が、情報資産やデジタル映像コンテンツに不正にアクセスする、あるいは不正利用する

A.9.2.3　特権的なアクセス権の管理

特権的なアクセス権（admin 権限等の権限）の割当て及び利用については、制限の上管理すること。
特権的なアクセス権を割当てる場合は、実際の利用者が識別できるようにすること(共用 ID の禁止等）。

デジタル映像コンテンツを扱う情報システムについては、特に厳格な運用を行うこと。
デジタル映像コンテンツの編集等の作業を行う者に特権的なアクセス権を割り当てないこと。
業務上やむを得ず特権的なアクセス権により作業を行う必要がある場合は、業務管理責任者の承認を得た上で情報システム管理者に依頼する等の手続きに従うこと。
デジタル映像コンテンツを扱う情報システムについては、特権的なアクセス権によるシステムの操作履歴やファイルへのアクセス履歴をログとして記録し、定期的に(1 日に 1 回程度)ログのレビューを行い、不正な操作やアクセスがないか確認すること。

想定されるリスク：特権的なアクセス権を不正に使用されることにより、システム上であらゆる操作が可能となり、情報資産やデジタル映像コンテンツが不正に使用されるだけでなく、組織内の他のシステムや情報資産への不正アクセス等が可能となる。

A.9.2.5　アクセス権の見直し

アクセス権は、人事異動があった場合や雇用又は契約が終了した際および定期的に(6 か月に 1 回程度)見直しを行うこと。
アクセス権の変更や不要なアクセス権の削除に関する手続きを規定し、適切に運用すること。

想定されるリスク：アクセス権をもたない者による情報資産への不正アクセス。

A.9.3.1　パスワードの利用

パスワードの利用ルールに従うことを利用者に要求すること。

1) パスワードは、PC 等に明示したり、紙に書いて他の人に見える場所に貼付したり、メールに記載したりして他人に知られることのないよう、各個人が厳重に管理すること。

2) パスワードは以下の条件を満たすこと。

・8 文字以上の長さに設定すること
・推測されやすい、あるいは解読されやすい文字列をパスワードに設定しないこと
・大文字・小文字、数字、記号を組み合わせること。

3) パスワードの変更条件

・少なくとも半年に 1 回変更すること
・他人に知られた可能性がある場合、変更すること
・ログインの際のパスワード入力の手間を省くための、アプリケーション等へのパスワード保存は禁止する
・過去に使用したパスワードを再利用しないこと

想定されるリスク：他人のパスワードを不正に入手した利用者が他人になりすましてシステムや情報資産に不正にアクセスする

A.10 暗号

A10.1.1　暗号による管理策の利用方針

情報を保護するための暗号による管理策の利用に関する方針を策定し、実施しなければならない。

重要な情報資産は暗号化すること。

デジタル映像コンテンツの暗号化には、十分な強度を有する暗号化アルゴリズム(AES 等)および十分な長さの暗号鍵(128bit 以上等)を使用すること。

想定されるリスク：暗号化されていない情報資産やデジタル映像コンテンツが漏えいし、不正に利用される。

強度が十分ではない暗号化アルゴリズムあるいは、長さが十分ではない暗号鍵を使用して暗号化された情報資産やデジタル映像コンテンツが不正に復号され利用される。

A10.1.2　鍵管理

暗号鍵の利用、保護及び有効期間に関する方針を策定し、暗号鍵のライフサイクル全般にわたって管理すること。

想定されるリスク：暗号鍵が漏えいし、暗号化された情報資産やデジタル映像コンテンツが不正に復号され利用される

A.11 物理的及び環境的セキュリティ

A11.2.6　組織外にある装置及び資産のセキュリティ

組織外で使用する情報機器に対しては、組織外での利用に伴うリスクを考慮に入れて、セキュリティ対策を適用すること。

1) 業務に使用する全てのモバイル PC、スマートフォンおよびタブレット端末は、モバイル機器管理ソリューションを通じて集中管理すること。
2) 組織外で使用する全てのモバイル PC、スマートフォンおよびタブレット端末にデジタル映像コンテンツを保存することを禁止する

想定されるリスク：モバイル PC 等の紛失やマルウェア感染に起因する情報資産やデジタル映像コンテンツの漏えい

A.12 運用のセキュリティ

A.12.1.1　操作手順書

情報システムの操作手順書を文書化し、業務でシステムを使用する者が利用できるようにすること。

想定されるリスク：間違った操作手順で情報システムを操作することにより、情報システムの誤動作や意図しない情報開示等のインシデントが発生する。また、業務上使用する必要がない利用者による不正使用リスクの増加。

A.12. 1.2　変更管理

情報セキュリティに影響を与える、組織、業務プロセス、情報システムの変更を管理すること。具体的には、人事異動、業務プロセスの変更、情報システムの基盤やアプリケーションの変更等が発生した場合に、情報資産へのアクセス権やセキュリティ上の手続きの承認者、脆弱性管理方法の変更等が確実に行われるよう管理すること。

想定されるリスク：組織、業務プロセス、情報システムの変更に合わせてセキュリティ管理策の変更・修正が行われないことにより、それまで防止できていたセキュリティインシデントが防止できなくなる。

A.12.1.3　容量・能力の管理

要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要となる容量・能力を予測すること。

想定されるリスク：システムの資源が不足することにより、サービスレベルの低下やシステムの停止等が発生する。

A.12.1.4　開発・テスト環境と、本番環境の分離

開発・テスト環境と、本番環境は分離すること。

想定されるリスク：本番環境で開発・テストを行うことにより、本番環境の情報システムが影響を受け、組織の業務の停止、顧

客に提供しているサービスの品質低下や停止が発生する

A.12.2.1　マルウェアに対する管理策

マルウェア対策の重要性を利用者に自覚させるとともに、検出、予防、回復のための管理を実施すること。

デジタル映像コンテンツを扱う情報システムについては、特に厳格なマルウェア対策を実施すること。
たとえば、デジタル映像コンテンツを扱う全ての情報システムについて、マルウェアスキャンの実施状況をチェックし、最新のマルウェア定義ファイルによるマルウェアスキャンが実施されていない場合には、即時にマルウェアスキャンを実施する等。

1) 情報資産およびデジタル映像コンテンツをマルウェアから保護するため、全ての PC およびサーバ、デジタル映像コンテンツを扱う全ての情報システムへのマルウェア対策ソフト(マルウェアスキャン)の導入、マルウェア情報の定期的更新、マルウェア検知状況監視等のマルウェア対策を講じる。

2) リアルタイムスキャンを有効化し、最新のマルウェア定義ファイルにより、最低でも週に 1 回フルスキャンを実施すること。

3) マルウェアに感染していることを発見した場合は、直ちに感染した PC あるいはデジタル映像コンテンツを扱う情報システムをネットワークから切り離すとともに情報セキュリティ管理責任者に連絡し、その指示に従い対応しなければならない。

4) 身に覚えのないメールや送信者不明の電子メール、不審な送信元からの電子メールおよび、そのメールに添付されているファイルを開いてはならない。そのようなメールを受信した場合は、速やかに削除すること。

5) 組織の外部からデータを持ち込む場合は、組織内のシステムに取り込む前にマルウェア対策ソフトによるスキャンを行い、マルウェアに感染していないことを確認しなければならない。

想定されるリスク：デジタル映像コンテンツを扱う情報システムのマルウェア感染による情報資産やデジタル映像コンテンツの漏えいや改ざん、情報システムの停止

A.12.3.1　情報のバックアップ

業務継続性を確保するために、情報資産のデータバックアップの実施に関する方針を策定し、それに基づいてデータバックアップを実施すること。

デジタル映像コンテンツを扱う情報システムについては、提供しているサービスに求められる品質やコンテンツの重要度に応じて、適切にデータバックアップを実施すること。たとえば、バックアップデータを保管するメディアを複数作成する、バックアップデータを保存する媒体を DVD と磁気テープの 2 つの異なる形態で用意する、バックアップメディアを地理的に離れた場所に保管する等である。
編集中のコンテンツについては、編集プロセスの区切りごとにコンテンツのバックアップを作成する。バックアップの作成時には、コンテンツの完全性を確保するために、コンテンツのハッシュを作成し、コンテンツのバックアップとともに保管する等の対策を実施する。

想定されるリスク：地震等の災害や、情報システムの障害やマルウェア感染等により、情報資産やデジタル映像コンテンツが毀損・喪失した場合に、情報資産やデジタル映像コンテンツの復旧ができない等

A.12.4.1　イベントログ取得

全ての PC およびデジタル映像コンテンツを扱う情報システムの利用状況、サーバに保管されているファイルへのアクセス、インターネット接続、過失及び情報セキュリティ事象に関するログ・記録を取得・保持し、適用される法律に基づいて監視の上、セキュリティインシデントを早期に検知するために、定期的に(数日～週に 1 回程度)レビューすること。
監査対象のログ・記録は以下の通りとする。

1) 組織内サーバ等へのアクセスログ（組織内から組織内へのアクセス）
2) ホームページや業務用サーバ等へのアクセスログ（組織外インターネットから組織内へのアクセス）
3) インターネットアクセスログ（組織内から組織外インターネットへのアクセス）

4) デジタル映像コンテンツへのアクセスログ
5) デジタル映像コンテンツに対する操作ログ

デジタル映像コンテンツを扱う情報システムについては、コンテンツに対して実行された操作についてのログを収集するとともに、可能であればリアルタイムでログの監視を行い、不正な操作や外部への転送等が行われていないかどうかを確認すること。
ログに記録する情報・監視対象とする情報は以下の通りである。

1) 操作実行時間
2) 操作実行者
3) 操作対象ファイル名
4) 操作の内容：移動、コピー、削除、変更等
5) ファイルの移動・コピーが行われた場合、移動・コピー元のシステムの IP アドレスと移動・コピー先のシステムの IP アドレス

想定されるリスク：情報資産やデジタル映像コンテンツへの不正アクセスや外部への漏えいがあった場合に、その原因を特定することができないため、是正措置を実施することができず、再度同じインシデントが発生する可能性がある

A.12.4.2　ログ情報の保護

ログ機能及びログ情報は、不正アクセス等から保護すること。

デジタル映像コンテンツを扱う情報システムについては、ログ情報のバックアップを取得し、最低 1 年間保存すること。

想定されるリスク：何らかの理由によりログ情報が消去された場合、インシデントの解析を行うことができず、是正措置を実施することができない。

A.12.4.3　システム管理者及び運用担当者の作業ログ

システム管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的に(毎日～数日に１回程度)レビューすること。

想定されるリスク：作業ログが記録されていない、あるいは、保護されていない場合、システム管理者あるいは運用担当者が不正行為を行ったことが疑われる場合に、作業ログを解析することにより原因の究明を行うことができない可能性がある。

A.12.4.4　システム時刻の同期

全ての情報システムのシステム時刻は、基となる単一の時刻に同期させる。

想定されるリスク：各情報システムのログに記録されている時刻が共通の基準時刻に基づいていないために、ログに記録されているイベントを正しい時系列で並べることができず、インシデントの正確な解析ができない。

A.12.5.1　運用システムに関わるソフトウェアの導入

運用中のシステムにおけるソフトウェアのインストールを管理するための手順を策定し、文書化し、実施すること。

想定されるリスク：ソフトウェアのインストール中に情報システムに障害が発生し、業務やサービスが停止する可能性がある。

A.12.6.1　技術的な脆弱性の管理

情報システムの技術的な脆弱性に関する情報は、適時に獲得し、必要に応じて修正プログラムを適用すること。

デジタル映像コンテンツを扱う情報システムについては、修正プログラムを適用することにより、情報システムやコンテンツを扱うアプリケーション等に障害が発生しないことを確認の上適用すること。

想定されるリスク：脆弱性が残ったままの状態で情報システムを運用することにより、マルウェア感染や不正アクセスの可能性が高くなり、情報漏えい等のインシデントが発生する恐れがある。

A.12.6.2　ソフトウェアのインストールの制限

利用者によるソフトウェアのインストールを管理する規則を確立し、実施すること。
ライセンスされたソフトウェア、組織が許可したソフトウェア、および組織から自動的に配布されたソフトウェア以外のソフトウェアのインストールは禁止すること。

想定されるリスク:正式なライセンスを有さないソフトウェアや許可されていないソフトウェアをインストールすることにより、知的財産の侵害や当該ソフトウェアに起因するマルウェア感染等が発生する。

A.12.7.1　情報システムの監査

情報システムの監査については、情報システムおよび業務プロセスの中断を最小限に抑えるように計画し、合意すること。

想定されるリスク：無計画な情報システム監査により、業務や情報システムの正常な運用に支障が出る、あるいは、業務や情報システムが可用性に関する規定を超過して停止する可能性がある

A.13 通信のセキュリティ

A.13.1.1　ネットワーク管理策

無線 LAN の業務利用を原則として禁止する。
組織外からインターネットを経由して、組織内の情報システムにアクセスすることを原則として禁止する。

想定されるリスク：無線 LAN やインターネットを経由した組織内の情報システムへの不正アクセス

A.13.1.3　ネットワークの領域分割

情報システムは、業務や利用者の役割等に応じて、ネットワーク上で分離すること。

デジタル映像コンテンツを扱う情報システムについては、他の業務システムと論理的あるいは物理的にネットワークを分離すること。
デジタル映像コンテンツを転送する情報システムについては、デジタル映像コンテンツを扱う情報システムおよび、他の業務システムと論理的あるいは物理的にネットワークを分離すること。

想定されるリスク：業務上の権限を持たない者による情報システムやデジタル映像コンテンツへの不正アクセス。

A.13.2.1　情報転送の方針及び手順

転送した情報を保護するために、正式な転送方針、手順及び管理を備えること。
FTP 等のセキュアでない転送方法やクラウドストレージ、クラウドファイル転送サービスの利用は原則禁止とする。
クラウドファイル転送サービスを利用する場合、サービス提供事業者およびサービスの基盤となる情報システムにおいて十分なセキュリティ対策が実施されていることを確認するために、サービス提供事業者から情報セキュリティ監査報告書等の情報セキュリティに関する証明書を取得し、情報セキュリティ対策が実施されていることを確認の上、利用すること。

デジタル映像コンテンツを転送するシステムについては、転送専用のシステムとし、コンテンツの編集や保存等を行わないこと。
デジタル映像コンテンツを転送するシステムについて、DVD ドライブや USB インタフェースを無効化すること。また、メディア書き込み装置の接続を禁止すること。
コンテンツを組織の外部に転送する場合、コンテンツの暗号化(AES 128 bit 以上)を必須とする。
コンテンツの転送が完了したら、速やかにコンテンツ転送システムからコンテンツを削除すること。

想定されるリスク：転送対象の情報(デジタル映像コンテンツを含む)への不正アクセスや転送途中での情報漏えいの発生、編集中のデジタル映像コンテンツの誤送信

A.13.2.3　電子的メッセージ通信

電子的なメッセージを発信する場合、情報を適切に保護すること。

機密情報や個人情報を電子的メッセージにより送信する場合、暗号化しなければならない。
暗号化に使用したパスワードは、セキュリティが確保された方法(別の電子的メッセージまたは口頭等)にて電子的メッセージの受信者へ知らせなければならない。
クラウドメールの業務利用を原則禁止する。業務上やむを得ない場合は、セキュリティの担保されたビジネス向けサービス(メールアカウントを組織の管理下に置くことができるようなサービス)を使用すること。

デジタル映像コンテンツを電子的メッセージにより送信する場合、コンテンツの暗号化(AES 128 bit 以上)を必須とする。
デジタル映像コンテンツを電子的メッセージにより送信する必要がある場合、業務管理責任者による電子的メッセージ送信の承認プロセスを導入すること。
デジタル映像コンテンツを電子的メッセージにより送信する必要がある場合、セキュア電子メールアプライアンスを使用し、電子的メッセージの送信に関するリスクを抑えること。
また、電子メールの送信ログ(送信者、送信先、送信日時、送信ファイル名)の記録・保存・レビューを行うこと。

想定されるリスク：送信途中での機密情報や個人情報、デジタル映像コンテンツの漏えい

A.13.2.4　秘密保持契約又は守秘義務契約

情報資産保護のために組織のニーズを反映した秘密保持契約又は守秘義務契約の要件を特定し、レビューし、必要に応じて文書化すること。

デジタル映像コンテンツに関する秘密保持契約又は守秘義務契約の要件については、特に厳格な運用を行うこと。たとえば、デジタル映像コンテンツに関わる全ての職員および外部委託先従業員を対象とする秘密保持契約あるいは守秘義務契約に関する誓約書に、デジタル映像コンテンツに特有の秘密保持・守秘義務要件とそれらに違反した場合の罰則規定を記載する等。

想定されるリスク：職員や外部委託先従業員による情報資産やデジタル映像コンテンツへの不正アクセスが発生した場合における、損害賠償請求時の法的根拠の欠落

A.14 システムの取得、開発及び保守

A.14.1.1　情報セキュリティ要求事項の分析及び仕様化

新しい情報システムの仕様や、既存の情報システムの改善要求事項には、情報セキュリティに関する要求事項を含める。

想定されるリスク：新規に開発する情報システムにおいて情報セキュリティ対策が実施されない、あるいは、既存の情報システムに対して情報セキュリティに関する改善がされない結果、脆弱性のある情報システムが運用されることになり、情報セキュリティインシデントが発生する恐れがある。

A.14.1.2　インターネット上のアプリケーションサービスのセキュリティ考慮

インターネット等のパブリックネットワークを通じて情報をやり取りするサービスに含まれる情報は、不正行為、契約紛争、不正アクセス・改ざんから保護すること。

想定されるリスク：機密書類の転送や課金サービス等において、契約書等の機密書類が紛失する、適切な課金が行われない、詐欺行為が発生する等。

A.14.1.3　アプリケーションサービスのトランザクションの保護

アプリケーションサービスのトランザクションに関する情報に対する保護策を講じること。具体的には、通信路の暗号化、トランザクションにおいてやりとりされるデータの暗号化、セキュアな通信プロトコルの使用等である。

想定されるリスク：サービスの提供に必要なデータの送信が完了しない、データ送信先の誤り、データの不正改ざん、不正開示、不正な複製

A.14.2.1　ソフトウェアやシステムの開発方針

情報セキュリティが考慮された開発ルールを策定し、全てのソフトウェア・システム開発に適用すること。
情報セキュリティ管理策が確実に実装されるようにするとともに、効率的な開発を行うために、情報システムの企画・設計の段階から情報セキュリティを組み込む Security by Design の考え方を導入し、情報セキュリティを確保することとする。
開発を外部に委託する場合も、Security by Design に基づく開発を委託先に徹底させる。

想定されるリスク：適切な情報セキュリティ管理策が実施されていないソフトウェアあるいは、情報システムが利用・運用されることにより、
ソフトウェアあるいは、情報システムの脆弱性を突いた攻撃が行われる可能性がある。

A.14.2.2　システムの変更管理手順

開発のライフサイクルの中で発生するシステム変更は、正式な変更管理手順を用いて管理すること。
変更管理手順を文書化し、定期的に(半年～1 年に 1 回程度)、又はシステムを構成するハードウェア・ソフトウェア等に変化が生じた場合に、見直しを実施すること。

想定されるリスク：システム変更時に情報セキュリティが考慮されないことにより、新たな脆弱性が発生する。

A.14.2.3　オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー

情報システムの運用基盤を変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションについてレビューし、テストすること。

想定されるリスク:情報システムの運用基盤の変更に起因するシステムエラー等により重要なアプリケーションに障害が発生し、組織の業務が停止する。

A.14.2.4　パッケージソフトウェアの変更に対する制限

パッケージソフトウェアの変更は、必要な変更だけに留める。又、全ての変更は、厳重に管理すること。

想定されるリスク：パッケージソフトウェアに組み込まれているセキュリティコントロールが無効化されることにより、想定していいない情報セキュリティ上の問題が発生する。

A.14.2.5　システムの構築・実装方針

安全なシステムの構築・実装方針を確立し、全ての情報システムの実装に対して適用すること。

想定されるリスク：情報セキュリティが考慮されていない情報システムが構築・運用され、外部からの攻撃等により、情報セキュリティインシデントが発生する。

A.14.2.6　セキュリティに配慮した開発環境

全ての開発のライフサイクルをカバーするシステム開発・インテグレーションのために、セキュリティに配慮した開発環境を

確立し、適切に保護すること。

想定されるリスク：開発環境に必要なセキュリティ管理策が実施されていないことにより、プログラムやデータの保護・変更管理等において不具合が発生し、システム開発が遅延する、開発したシステムに不正な改変が加えられる。

A.14.2.7　外部委託による開発

外部委託したシステム開発を監督し、監視すること。

想定されるリスク：外部委託により開発したシステムに脆弱性等の情報セキュリティ上の問題が発生し、その修正に追加のコストを要する。あるいは、システムの脆弱性を修正せずに実運用を開始した結果、情報セキュリティインシデントが発生する。

A.14.2.8　システムのセキュリティ機能テスト

システムのセキュリティ機能についてのテストを開発期間中に実施すること。

システムのテストを行う際のテストデータに、組織が保有・管理するデジタル映像コンテンツを使用しないこと。

想定されるリスク：開発期間中にセキュリティ機能のテストが実施されていない結果、セキュリティ機能が実装されないままシステムの運用が開始され、外部からの攻撃等を防止することができず、情報セキュリティインシデントが発生する。

A.14.2.9　システムの受入れテスト

新しい情報システムおよび既存の情報システムの更新に関する受入れ試験のプログラムおよび関連する基準を確立すること。

想定されるリスク:仕様書において規定したセキュリティ機能が実装されていることをテストにより確認できない可能性があり、脆弱性が残存したままシステムの運用が開始され、情報セキュリティインシデントが発生する。

A.15 外部委託先のセキュリティ管理

A15.1.1　外部委託先管理のための情報セキュリティの方針

外部委託先による情報の不正利用や、情報漏洩、プライバシーの侵害などを防止するため、契約時に不正防止、機密保持などの対策を明確に文書化すること。

デジタル映像コンテンツに関する業務を委託する場合には、委託先における情報セキュリティ管理策の運用・管理体制を検証し、委託元と同等の情報セキュリティ管理策実施していることが確認できた場合に限り、委託を可能とする。 また、委託先の業務担当者全員から署名入りの秘密保持契約書又は守秘義務契約書を受領すること。

想定されるリスク:外部委託先による情報・デジタル映像コンテンツの不正利用や、情報漏洩、プライバシーの侵害などの発生。

A15.1.2　外部委託先との合意に含まれるセキュリティの取り組み

外部委託先に対して、関連する全ての情報セキュリティ要求事項を確立すること。
組織の情報を対象として、アクセス・処理・保存・通信を行う外部委託先、又は組織の情報のために IT インフラを提供する外部委託先と、その要求事項について合意すること。

デジタル映像コンテンツに関する業務を委託する場合には、特に厳格な運用を行うこと。 具体的には、以下の項目について委託先と事前に合意し、徹底するよう委託先に指示すること。 ・　使用機器（カメラ等含む）について ・　データの受け渡し方法（使用可能な媒体、コンテンツの暗号化など） ・　データのバックアップの取得 ・　インシデントが発生した場合の委託元への迅速な報告を含むインシデント対応

- 情報システム・デジタル映像コンテンツへの適切なアクセスコントロールの実施
- 可搬記憶媒体の利用ポリシーの遵守
- 物理記憶媒体の廃棄ポリシーの遵守
- 委託元から貸与した情報資産の返却・廃棄・削除ポリシーの遵守

想定されるリスク：情報セキュリティに関する取り組みに関する外部委託先との合意内容が不十分であったため、適切な情報セキュリティ管理が実施されず、情報セキュリティインシデントが発生する。

A15.1.3　ICT サプライチェーン

外部委託先が再委託を行っている場合は、再委託先に対して、情報セキュリティ上の要求事項を徹底させること。

デジタル映像コンテンツに関する業務について、再委託を原則として禁止すること。
やむを得ず再委託を行う場合には、再委託先の情報セキュリティ管理策の実施状況を報告させ、委託元と同等の情報セキュリティ管理策を実施していることが確認できた場合に限り再委託を行うこと。
また、再委託先の業務担当者全員から署名入りの秘密保持契約書又は守秘義務契約書を受領すること。
具体的には、以下の項目について再委託先と事前に合意し、徹底するよう再委託先に指示すること。

- 使用機器（カメラ等含む）について
- データの受け渡し方法（使用可能な媒体、コンテンツの暗号化など）
- データのバックアップの取得
- インシデントが発生した場合の委託元への迅速な報告を含むインシデント対応
- 情報システム・デジタル映像コンテンツへのアクセスコントロールの実施
- 可搬記憶媒体の利用ポリシーの遵守
- 物理記憶媒体の廃棄ポリシーの遵守
- 委託元から貸与した情報資産の返却・廃棄・削除ポリシーの遵守

想定されるリスク：再委託先における情報セキュリティインシデントの発生。

A15.2.1　外部委託先のサービス提供の監視及びレビュー

外部委託先が提供するサービスの品質や情報セキュリティに対する取り組み状況を定期的に(半年～1 年に 1 回程度)レビューし、監査すること。

デジタル映像コンテンツに関する業務を委託する場合には、特に厳格な運用を行うこと。

想定されるリスク：外部委託先における情報セキュリティインシデントの発生。

A15.2.2　外部委託先のサービス提供の変更に対する管理

外部委託先が提供するサービスに変更がある場合、情報システム及び業務プロセスの重要性やリスクの再評価の結果を考慮して、管理すること。

想定されるリスク：重要な業務あるいは情報システムに関連する外部委託先サービスの変更により、業務の停止につながるリスクが増加する、あるいは、情報システムに関する脆弱性が発生する。

A.16 情報セキュリティインシデントの管理

A.16.1.1　責任及び手順

情報セキュリティインシデントに対する、迅速で、効果的で整然とした対応を確実にするために、職員および、情報セキュリティ管理責任者の責任及び手順を確立すること。

想定されるリスク：情報セキュリティインシデントへの対応が遅れる結果、情報システムや業務の停止時間が長期に渡る、ある

いは、インシデントの原因究明に長期間を要する。

A.16.1.2　情報セキュリティ事象の報告

情報セキュリティ事象は､情報セキュリティ管理責任者および所属部署の業務管理責任者にできるだけ速やかに報告すること。

情報セキュリティ事象は、情報セキュリティに関連するあらゆる出来事。具体的には不審なファイルが添付された電子メールの受信、可搬記憶媒体の紛失等を指す。情報セキュリティ事象が、マルウェア感染や情報漏えい等、現実のセキュリティ事故となった場合に情報セキュリティインシデントとして分類される。従って、情報セキュリティインシデントになるかどうかの判断が行われる前に、全ての情報セキュリティ事象を報告することが求められる。

想定されるリスク：情報セキュリティインシデントにつながるリスクの高い情報セキュリティ事象が放置されることにより、情報セキュリティインシデントが発生する可能性が高くなる、あるいは、情報セキュリティインシデントの発生を未然に防止することができない。

A.16.1.3　情報セキュリティリスクの報告

情報セキュリティ管理責任者は、情報システム又はサービスの中で発見した又は疑いがある情報セキュリティ上のリスクについて、どのようなものでも記録し、報告するよう、職員および契約相手に要求すること。

想定されるリスク：情報セキュリティリスクが放置されることにより、情報セキュリティインシデントが発生する可能性が高くなる、あるいは、情報セキュリティインシデントの発生を未然に防止することができない。

A.16.1.4　情報セキュリティ事象の評価及び決定

情報セキュリティ事象について、事業・業務に対する影響度を評価し、情報セキュリティインシデントに分類するか否かを決定すること。

想定されるリスク：事業・業務に対する影響が大きい情報セキュリティ事象が情報セキュリティインシデントとして分類されないために、情報セキュリティインシデントへの対応が遅れ、事業・業務への影響・被害が大きくなる。

A.16.1.5　情報セキュリティインシデントへの対応

情報セキュリティインシデントについて、文書化した手順に従って対応すること。また、情報セキュリティインシデントが発生した場合、サービスの提供先や関係する組織等に対し、被害状況や対応状況に関する最新情報を提供すること。

想定されるリスク：情報セキュリティインシデント対応手順が文書化されていない場合、迅速かつ適切な対応ができない可能性がある。

A.16.1.6　情報セキュリティインシデントからの学習

情報セキュリティインシデントの分析や解決から得られた知識は、インシデントが将来起こる可能性又は、その影響を低減するために用いる。

想定されるリスク：同じ原因による情報セキュリティインシデントが発生する可能性がある。

A.16.1.7　証拠の収集

情報セキュリティインシデントの証拠となり得る情報の特定、収集、取得、保存のための手順を定め、文書化し、適用すること。

想定されるリスク：情報セキュリティインシデントの証拠収集に関する手順が定められていない場合、インシデント発生の原因

を特定することができず、是正措置を実施することができない可能性があるため、同じ原因による情報セキュリティインシデントが発生する可能性がある。

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1.1　情報セキュリティ継続の計画

災害等により、サービスの一部あるいは大部分が停止する状況において、情報セキュリティ及び情報セキュリティマネジメントを継続するための要求事項を決定すること。

想定されるリスク：業務やサービスの一部あるいは大部分が停止する状況において、情報セキュリティ管理策が適切に機能しない場合、情報セキュリティインシデントが発生する可能性がある。

A.17.1.2　情報セキュリティ継続の実施

サービスの一部あるいは大部分が停止する等の困難な状況の下で、情報セキュリティ継続に関する要求レベルを確実にするためのプロセス、手順及び管理策を定め、文書化し、実施し、維持すること。

想定されるリスク：業務やサービスの一部あるいは大部分が停止する状況において、情報セキュリティ管理策に要求されるレベルを達成することができない場合、情報セキュリティインシデントが発生する可能性がある。

A.17.1.3　情報セキュリティ継続の検証、レビュー及び評価

情報セキュリティ継続のために確立及び実施した管理策が妥当且つ有効であることを確実にするために、年に 1 回または重要な変更が発生したとき、これらの管理を検証すること。

想定されるリスク：情報セキュリティ継続のための管理策の有効性が低下していた結果、情報セキュリティインシデントが発生する可能性がある。

A.17.2.1　情報処理施設の可用性

情報システムは、自ら運用するか運用を外部に委託するかに関わらず、可用性の要求事項を満たすのに十分な冗長性をもって導入すること。

デジタル映像コンテンツの配信に使用する情報システムについては、提供するサービスに求められる品質に応じて、適切に可用性に関する要求事項を規定すること。

想定されるリスク：情報システムの一部あるいは全てが停止した場合に、業務やサービスの品質が低下する、あるいは、業務やサービスの提供ができなくなる。

A.18 コンプライアンス

A.18.1.1　適用法令及び契約上の要求事項の特定

情報セキュリティに関する法令(個人情報保護法等)、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを明確に定め、文書化し、最新に保つこと。

想定されるリスク：法令違反により罰則を課される可能性がある。

A.18.1.2　知的財産権

知的財産権及び登録商標が存在するソフトウェア製品を利用する場合、法令、規制及び契約上の要求事項の順守を確実にする

こと。

想定されるリスク：正規のライセンスを有していないソフトウェアを使用した場合、ソフトウェアの権利保有者あるいは開発元等から、損害賠償を求められる可能性がある。

A.18.1.3　記録の保護

アクセスログ等の記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、不正アクセス及び公開から保護すること。

デジタル映像コンテンツに関するログについては、特に厳格な運用を行うこと。

想定されるリスク：政府機関からの要求により、アクセスログ等の記録を提出する必要がある場合に対応することができない、あるいは、訴訟対応において、法令等により保存することが求められるアクセスログ等を証拠として提出できない結果、不利な状況に陥る。

A.18.1.4　プライバシー及び個人を特定できる情報の保護

プライバシー及び個人を特定できる情報は、関連する法令及び規制が適用される場合には、その要求に従って確実に保護すること。

想定されるリスク：国内および海外の法令及び規制を遵守できていない場合、何らかの罰則が適用される可能性がある。

A.18.1.5　暗号化機能に対する規制

暗号化機能は、関連する全ての協定、法令及び規制を順守して用いること。

想定されるリスク：暗号化機能の使用あるいは暗号化機能を有する製品の使用に関する法律を遵守できていない場合、何らかの罰則が適用される可能性がある。

A.18.2.1　情報セキュリティの独立したレビュー

情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に関する組織の取組みは、定期的に(半年～1 年に 1 回程度)、又は重大な変化が生じた場合に、独立したレビューを実施すること。

想定されるリスク：情報セキュリティのための管理目的、管理策、方針、プロセス、手順等が実態と合わなくなっている場合、情報セキュリティインシデントが発生するリスクが増加する。

A.18.2.2　情報セキュリティのための方針及び標準の順守

情報セキュリティ管理責任者は、情報処理及び手順が、適切な情報セキュリティのための方針、標準類、及び他の全ての情報セキュリティ要求事項を順守していることを定期的に(半年～1 年に 1 回程度)レビューすること。

想定されるリスク：情報セキュリティ要求事項を順守できていない場合、情報処理及び手順に脆弱性が存在する可能性があり、情報セキュリティインシデントが発生する可能性がある。

A.18.2.3　技術的順守のレビュー

情報システムに対して適切な情報セキュリティ施策が実施されていることを定期的に(半年～1 年に 1 回程度)または、情報システムに重大な変化が生じた場合に)レビューすること。

デジタル映像コンテンツを扱う情報システムについては、特に厳格な運用を行うこと。

情報セキュリティ施策の例：物理的に安全な場所への配置、脆弱性スキャン、ペネトレーションテスト、等。

想定されるリスク：定期的なレビューが行われない場合、情報セキュリティ施策が実施されていない情報システムが存在する可能性があり、情報セキュリティインシデントが発生する可能性がある。

4. デジタル映像コンテンツの管理・保存・活用に関して考慮するべき法律等

デジタル映像コンテンツの管理・保存・活用に関して考慮するべき法律について、日本、米国、ヨーロッパにおいて施行されている法律をまとめる。

デジタル映像コンテンツに関する業務の実施やサービスの提供に際しては、法令・規制の遵守のみならず、サービス規約、業務契約において規定されている事項や義務等に違反することを避けるために、関係する法律や規則を理解するとともに、どのような対応が必要かを明確化し、適切な対応を行う必要がある。そのためには、業務の実施やサービスの提供および業務契約の締結に際して、各組織の法務部門や弁護士等の専門家の助言を得ることが重要である。

4.1 日本

- 電子署名及び認証業務に関する法律[12]
- 不正競争防止法[13]
- 不正アクセス行為の禁止等に関する法律[14]
- 個人情報の保護に関する法律[15]
- 電気通信事業法[16]
- 著作権法[17]
- 知的財産基本法[18]
- 特許法[19]
- e-文書法(正式名称：民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律)[20]
- 刑法[21]
  - ✓ 第三十五章 信用及び業務に対する罪
    電子計算機損壊等業務妨害
    第二百三十四条の二
  - ✓ 第十七章 文書偽造の罪
    電磁的記録不正作出及び供用
    第百六十一条の二
  - ✓ 第三十七章 詐欺及び恐喝の罪
    電子計算機使用詐欺
    第二百四十六条の二
  - ✓ 第十九章の二 不正指令電磁的記録に関する罪
    不正指令電磁的記録作成等
    第百六十八条の二

    不正指令電磁的記録取得等

[12] http://law.e-gov.go.jp/htmldata/H12/H12HO102.html
[13] http://law.e-gov.go.jp/htmldata/H05/H05HO047.html
[14] http://law.e-gov.go.jp/htmldata/H11/H11HO128.html
[15] http://law.e-gov.go.jp/htmldata/H15/H15HO057.html
[16] http://law.e-gov.go.jp/htmldata/S59/S59HO086.html
[17] http://law.e-gov.go.jp/htmldata/S45/S45HO048.html
[18] https://www.kantei.go.jp/jp/singi/titeki/hourei/021204kihon.html
[19] http://law.e-gov.go.jp/htmldata/S34/S34HO121.html
[20] http://law.e-gov.go.jp/htmldata/H16/H16HO149.html
[21] http://law.e-gov.go.jp/htmldata/M40/M40HO045.html

第百六十八条の三

4.2 米国

- 著作権法 [22]

  著作権侵害行為に対し、刑事罰(5 年以下の自由刑または 25 万ドル以下の罰金又は両方)が科される

- デジタル・ミレニアム著作権法（The Digital Millennium Copyright ACT (DMCA) [23]

  WIPO 著作権条約及び WIPO 実演・レコード条約を締結するために、著作権法を改正した法律。著作権保護技術を解除する技術的手段などを公表することも禁止している。
  一定の要件を備えた著作権侵害に関する主張があった場合、調査や侵害対象となっている著作物の削除義務が生じる。また、著作権侵害容疑者に確認を取る前にコンテンツを削除しても罪に問われない。(ノーティス・アンド・テイクダウン)

4.3 ヨーロッパ

ＥＵ著作権指令に基づき加盟国において、著作権法が制定されている。

4.3.1 イギリス

Copyright, Designs and Patents Act 1988 [24]

複数回に渡る著作権侵害行為に対して、インターネット接続速度の制限等の「技術的措置」(technical measure)が適用される場合がある。

4.3.2 フランス

知的所有権法 [25]

著作権侵害行為に対して 2 度の勧告が行われてもなお著作権侵害行為が行われている場合に、刑事罰(3 年以下の禁錮刑又は 30 万ユーロ以下の罰金刑)が科される。(スリーストライク制)

4.3.3 ドイツ

著作権法 [26]

著作権侵害行為に対し、刑事罰が科される(3 年以下の自由刑又は罰金)。

[22] http://www.cric.or.jp/db/world/america.html
[23] www.copyright.gov/legislation/dmca.pdf
[24] http://www.cric.or.jp/db/world/england.html
[25] http://www.cric.or.jp/db/world/france.html
[26] http://www.cric.or.jp/db/world/germany.html

本報告書は、東京国立近代美術館フィルムセンターによる委託業務として、NRI セキュアテクノロジーズが実施した『デジタル映像コンテンツのセキュリティ対策に関する調査』の成果を取りまとめたものです。