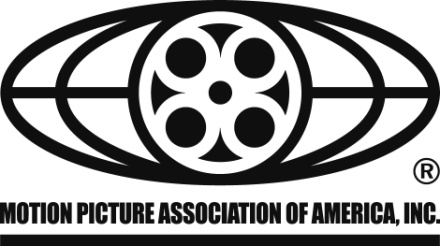
****

**MPAA コンテンツセキュリティ プログラム**

**コンテンツセキュリティ ベストプラクティス**

**共通ガイドライン**

[**http://www.mpaa.org/content-security-program/**](http://www.mpaa.org/content-security-program/)

バージョン3.0

2015年4月2日

文書履歴

|  |  |  |  |
| --- | --- | --- | --- |
| **バージョン** | **日付** | **説明** | **作者** |
| 1.0 | 2009年12月31日 | 初回社外リリース | Deloitte & Touche LLP  MPAA  MPAAメンバー企業 |
| 2.0 | 2011年5月15日 | 更新と改定  共通ガイドラインと補足書類の検討 | PwC LLP  MPAA  MPAAメンバー企業 |
| 2.1 | 2013年1月1日 | 更新と改定 | PwC LLP  MPAA  MPAAメンバー企業 |
| 3.0 | 2015年4月2日 | 更新と改定 | MPAA  MPAAメンバー企業 |

目次

[文書履歴 i](#_Toc428364957)

[I. ベストプラクティス概要 2](#_Toc428364958)

[II. 施設の概要 3](#_Toc428364959)

[III. リスク管理 4](#_Toc428364960)

[IV. ベストプラクティスの書式 6](#_Toc428364961)

[V. MPAAベストプラクティス共通ガイドライン 7](#_Toc428364962)

[付録A — 用語集 74](#_Toc428364963)

[付録B — MPAA作品名とディストリビューションチャネルの定義 78](#_Toc428364964)

[付録 C — 施設のマッピング 80](#_Toc428364965)

[付録D — 参照ポイントへのコントロールのマッピング 92](#_Toc428364966)

[付録e — よくある質問（FAQ） 97](#_Toc428364967)

[付録f — 推奨ポリシーと手順 98](#_Toc428364968)

[付録g — その他のリソースと参考資料 99](#_Toc428364969)

[付録h — MPAAへの不正行為報告 100](#_Toc428364970)

1. ベストプラクティス概要

**はじめに**

Motion Picture Association of America, Inc.（アメリカ映画協会、以下「MPAA」）は、30年以上にわたり、以下のメンバー企業（「メンバー」）のために、コンテンツセキュリティ査定を代行してきました。Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; Twentieth Century Fox Film Corporation; Walt Disney Studios Motion Pictures and Warner Bros. Entertainment Inc.

この調査は2007年に、標準化された調査モデル、プロセス、レポートテンプレートを使用して開始され、現在までに32ヶ国で500を超える施設を調査してきました。

MPAAは世界の視聴者のために、エンターテイメントコンテンツを製作する権利の保護に専心努力しています。現在では、クリエイティブアートからソフトウェア業界まで、世界でアイデアのパワーを用いて生計を立てる人々の数が増え続けています。これは知的財産権の保護と、その保護策が健全な世界的情報経済を守る鍵であるという認識が、拡大していることを示します。

MPAAコンテンツ セキュリティプログラムの目的は、制作、ポストプロダクション、マーケティング、ディストリビューションの各過程でメンバーのコンテンツを保護するプロセスを強化することです。これは、次の施策を実施することによって達成されます。

* メンバーのコンテンツを保護する標準的コントロールを設定する施設サービスを用いた、正規のベストプラクティスを規定する。
* 正規のベストプラクティスに基づき、サードパーティであるパートナーのコンテンツセキュリティを査定・評価する。
* メンバーのコンテンツを保護する重要性を再確認する。
* メンバーとそのビジネスパートナーとの間のコンテンツセキュリティに関して、個々のディスカッションを奨励する標準的な査定手段を提供する。

**目的と適用可能性**

本書の目的は、メンバーが既存および将来に起用・契約するサードパーティベンダーに、期待される一般的なコンテンツセキュリティと、業界における現在のベストプラクティスを理解していただくことです。各メンバーがどのようなベンダーを使用するかは、そのメンバーの単独任意で決定されます。

コンテンツセキュリティのベストプラクティスは、施設が提出するサービス、取り扱うコンテンツ、また施設のリリースの幅を考慮してデザインされています。

本書で言及されているベストプラクティスは、地域、州、地方、連邦、国家の法規法律に準拠します。

本書で言及されているベストプラクティス、業界標準、ISOは、定期的に変更されます。

**ベストプラクティス準拠は完全に任意です。認定プログラムではありません。**

**例外プロセス**

ベストプラクティスの準拠が可能に思われない状況では、ベンダーはベストプラクティスに準拠不能な理由を文書化し、ベストプラクティスの代用となる施策を実施してください。また例外措置を講じる場合は、メンバーに直接報告してください。

**ご質問やご意見**

ベストプラクティスに関するご質問やご意見は、contentsecurity@mpaa.orgまでEメールで送信してください。

1. 施設の概要

次の表は、各施設タイプに関連している代表的なサービス、コンテンツ、リリースの幅をまとめたものです。

| **No.** | **施設タイプ** | **代表的な施設のサービス** | | **コンテンツのタイプ** | **リリースの幅** |
| --- | --- | --- | --- | --- | --- |
| **1** | **オーディオ、ダビング、字幕スーパー** | * オリジナル言語と外国語のダビング * 字幕スーパー * SFX * スコアリング * ADR/フォーリー | | * 低解像度 * 透かし入り/Spoiled * フル/パーシャルフィーチャーコンテンツ * オーディオマスター | * 劇場リリース前 * ホームビデオリリース前 |
| **2** | **宅配業・運送業** | * 宅配業 * 配達業 * 運送業 | | * 多種 | * 劇場リリース前 * ホームビデオリリース前 * カタログ |
| **3** | **クリエイティブ広告** | * 仕上げなし * 予告編 * TVスポット * ティーザー * グラフィックス * ウェブ広告 | | * 透かし入り/Spoiled フル/パーシャルフィーチャーコンテンツ * 静止画 * クリップ | * 劇場リリース前 * ホームビデオリリース前 * カタログ |
| **4** | **デジタル**  **シネマ** | * デジタルシネマ マスタリング * 複製 * キー管理 | | * 高解像度 – フル/パーシャルコンテンツ * デジタルシネマ ディストリビューション マスター * デジタルシネマ パッケージ | * 劇場リリース前 |
| **5** | **デジタル**  **サービス** | * デジタル・インターミディエイト * スキャン * フィルム記録 * フィルム復元 | | * クリーンな高解像度 – フル/パーシャルコンテンツ（フォルムタイプ） | * 劇場リリース前 * カタログ |
| **6** | **ディストリビューション** | * ディストリビューション * フルフィルメント * 倉庫/フィルム保管所 * DVD/テープのリサイクル | | * 高解像度 * クリーンな画像 | * 劇場リリース前 * ホームビデオリリース前 * カタログ |
| **7** | **DVD**  **製作** | * 圧縮 * 許可取得 * 暗号化 * 地域への適合 * スペシャルフィーチャー * DiscQCの確認 | | * クリーン – フルフィーチャー | * ホームビデオリリース前 |
| **8** | | **DVD**  **製作** | * 圧縮 * 許可取得 * 暗号化 * 地域への適合 * スペシャルフィーチャー * Disc QCの確認 | * クリーン – フルフィーチャー | | * ホームビデオ * リリース前 |
| **9** | | **機内エンターテイメント（IFE）および**  **ホスピタリティサービス** | * IFEラボ * IFEインテグレーション * ホテル * 航空会社 * クルーズ船舶/フェリー * 図書館 * 病院 * 刑務所 | * 高解像度 – フル/パーシャルコンテンツ * Spoiled – フル/パーシャルコンテンツ | | * 劇場リリース前 * ホームビデオリリース前 * カタログ |
| **10** | | **ポストプロダクションサービス** | * テレシネ * 複製 * 編集 * 仕上げ * QC | * 高解像度 – フル/パーシャルコンテンツ | | * 劇場リリース前 * ホームビデオリリース前 * カタログ |
| **11** | | **複製** | * プリマスタリング * マスタリング * 複製 * ディスク製作の確認 | * 高解像度 * クリーンな画像 | | * ホームビデオリリース前 |
| **12** | | **ビジュアル**  **エフェクト**  **(VFX)** | * デジタル ポストプロダクション * コンピュータ生成画像 * アニメーション | * 高解像度 – パーシャル * フレーム、ショット、シーケンス、静止画 * 台本 * 絵コンテ | | * 劇場リリース前 * 劇場リリース前（2D～3D） |
| **13** | | **アプリケーション** | * アプリケーション開発 | * 多種 | | * 多種 |
| **14** | | **クラウド** | * ホスティング * データセンター | * 多種 | | * 多種 |

1. リスク管理

**リスク査定**

リスクはリスク査定を通して特定し、適切なコントロールを実装して許容レベルまで低減しなければなりません。またビジネス目標も達成しなければなりません。

国際標準化機構（ISO）27000は、リスクを「イベントの可能性とその発生した結果の組み合わせ」と定義しています。例えば、あるコンテンツが施設のネットワークから盗まれて公開される可能性はどのくらいでしょうか。またこの盗難によって会社と顧客に発生するビジネスの結果とはどのようなものでしょうか（例: 契約違反および／または、そのリリース枠に該当する利益の喪失）。

ISO 27001標準では情報セキュリティ管理システム（ISMS）の設置方法を示すことにより、堅牢な管理システムの重要性も強調しています。

**資産の分類**

施設で資産を分類する一つの方法としては、次に示す4ステッププロセスが挙げられます。

効果性の  
モニターと評価

最低限の一連の  
セキュリティ  
コントロールを判断する

コントロールを実装する

資産を特定、  
分類する

ベンダーはメンバー（顧客）と話し合い、どの顧客の資産に高レベルのセキュリティが必要かを特定する責任を担っています。下表はコンテンツ分類の例を示しています。

| **分類** | **説明** | **例** |
| --- | --- | --- |
| **セキュリティの高いコンテンツ** | 盗難にあったり、漏えいしたりした場合、財務上の損失、ブランドの評判へのダメージ、または重大な罰則につながりかねないと思われる資産 | * 世界初の劇場リリース前の超大作盗難 * 世界初回リリース前のホームビデオコンテンツの盗難 * マスターやスクリーナーの盗難 |

通常各施設タイプに関連しているリスクに関する追加情報も、ベストプラクティスの補足規定に含まれています。

**セキュリティコントロール**

ITガバナンス協会は、コントロールを「ビジネスの目標が達成され、望ましくないイベントが防止または検知・是正されることを妥当な範囲で保証するようデザインされたポリシー、手順、プラクティス、会社構造」と定義しています。通常セキュリティコントロールは、資産の分類、会社にとっての資産の価値、資産が漏えいや盗難にあうリスクに基づいて選択されます。

特定されたリスクを緩和するために、会社には各リスクに見合ったコントロールを実装することが推奨されています。また、現在の脅威環境に基づいて、これらの方策のデザインと効果性を定期的に評価しなければなりません。



**管理システム**



**会社と管理**



**物理的セキュリティ**



**輸送**



**施設**



**デジタルセキュリティ**



**インフラストラクチャ**



**IV. 書類の整理**



**MS-1 エグゼクティブによるセキュリティの認識／監督 ページ 7**

**ベストプラクティスは、顧客のコンテンツを保護する施設の能力の枠組みとなるMPAAコンテンツセキュリティモデルに基づいて整理されます。これらは管理システム、物理的セキュリティ、デジタルセキュリティという3つの分野に分かれています。MPAAコンテンツセキュリティモデルの構成要素は、関連性のあるISO標準（27001～27002）、セキュリティ標準（すなわちNIST、CSA、ISACA、およびSANS）、業界のベストプラクティスから取り入れたものです。**

**MS-2 リスク管理   
ページ 7**

**MS-3 セキュリティ  
構成 ページ 8**

**MS-4 ポリシーと  
手順 ページ 9**

**MS-5 インシデント  
対応 ページ 12**

**MS-6 ビジネス継続性と災害復旧 ページ 14**

**MS-7 変更管理と設定管理 ページ 15**

**MS-8 ワークフロー ページ 15**

**MS-9 任務の分割   
ページ 16**

**MS-10 経歴確認   
ページ 17**

**MS-11 守秘契約   
ページ 17**

**MS-12 サードパーティの利用と審査   
ページ 18**

**PS-1 出入り口  
 ページ 20**

**PS-2 ビジターの  
出入り ページ 21**

**PS-3 身分証明書   
ページ 22**

**PS-4 周辺の  
セキュリティ ページ 22**

**PS-5 アラーム   
ページ 23**

**PS-5 承認 ページ 25**

**PS-8 鍵 ページ 26**

**PS-9 カメラ ページ 28**

**PS-7 電子アクセス  
コントロール   
ページ 25**

**PS-10 ロギングと  
モニタリング   
ページ 29**

**PS-11 検査   
ページ 30**

**資産管理**

**PS-12 在庫トラッキング ページ 33**

**PS-13 在庫確認   
ページ 34**

**PS-14 ブランクメディア／未処理ストックトラッキング ページ 35**

**PS-15 顧客の資産   
ページ 35**

**PS-16 処分   
ページ 36**

**PS-17 出荷   
ページ 38**

**PS-18 入荷   
ページ 39**

**PS-19 ラベル貼り   
ページ 40**

**PS-20 梱包   
ページ 40**

**PS-21 輸送車両   
ページ 41**

**DS-1 ファイヤウォール／WAN／周辺のセキュリティ ページ 42**

**DS-2 インターネット   
ページ 46**

**DS-3 LAN ／内部  
ネットワーク ページ 48**

**DS-4 ワイヤレス   
ページ 51**

**DS-5 I/O デバイスセキュリティ ページ 53**

**DS-6 システムセキュリティ ページ 53**

**DS-7 顧客管理   
ページ 56**

**DS-7.7-8.4 認証   
ページ 58-60**

**DS-9 ロギングとモニタリング ページ 61**

**コンテンツ管理**

**DS-10 モバイルセキュリティ ページ 63**

**コンテンツ転送**

**DS-11 セキュリティ  
テクニック ページ 65**

**DS-12 コンテンツ  
トラッキング ページ 67**

**DS-13 転送システム ページ 68**

**DS-14 転送デバイス  
方法 ページ 68**

**DS-15 クライアント  
ポータル ページ 70**

1. ベストプラクティスの書式

ベストプラクティスは、MPAAコンテンツセキュリティモデルに記載されている各セキュリティトピックに対応するように、次の書式で規定されています。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 管理システム | 物理的セキュリティ | | | デジタルセキュリティ | | |
| 会社と管理 | 施設 | 資産管理 | 輸送 | インフラストラクチャ | コンテンツ管理 | コンテンツ転送 |

各ページの上にある表は、MPAAコンテンツセキュリティモデル全体の中で対象となっているセキュリティ分野をハイライトしたものです。

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| PS-9.0 | キー | **マスターキー**の配布は権限を持つ関係者（例: オーナー、施設管理者）のみに限ります。 | * **マスターキー**を借りることができる**従業員**のリストを維持します。 * **マスターキー**へのアクセスが不要となった**従業員**を削除して、リストを定期的に更新します。 |
| PS-9.1 | **マスターキー**貸与をトラッキングおよびモニターするチェックイン・チェックアウトプロセスを導入します。 | * 次の情報をトラッキングするために、記録を維持します。 * **マスターキー**を貸与されている**従業員** * チェックアウト・チェックインの時刻 * チェックアウトの理由 |

P

**用語集**

用語集に収録されている言葉は**太字**で書かれてあり、付録Aに記載されています。

**実施ガイダンス**

ベストプラクティスの実施に役立つヒント、実施ステップやその他の例などが記載されています。

**ベストプラクティス**

ベストプラクティスは、それぞれのセキュリティトピックごとに規定されています。

**セキュリティトピック**

それぞれの能力分野は、一つ以上の「セキュリティトピック」に分類され、それぞれのセキュリティトピックは、一つ以上のベストプラクティスが対応しています。

**No.**

それぞれのベストプラクティスには、XX-Y.Zという形式の参照番号が付いています。XXは一般的な分野、Yはセキュリティトピック、Zは該当するコントロールを表します。

1. MPAAベストプラクティス共通ガイドライン

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| MS-1.0 | エグゼクティブによるセキュリティの認識/監督 | ビジネス責任者や経営陣が承認した情報セキュリティを対象とするコントロールフレームワークを実施するための情報セキュリティ管理システムを設置します。 | * たとえば、ISO27001のISMS フレームワーク、NIST、CoBITなど。 |
| MS-1.1 | 情報セキュリティ管理ポリシーおよびプロセスを、少なくとも年に一度レビューします。 |  |
| MS-1.2 | 企業が担うコンテンツ保護の責任について、少なくとも年に一度、経営陣や責任者を教育し、認識を深めるよう指導します。 |  |
| MS-1.3 | 情報セキュリティ管理ポリシーを制定しレビューするために、情報セキュリティ管理グループを結成します。 |  |
| MS-2.0 | リスク管理 | 施設に関連したコンテンツの盗難・漏えいリスクを特定・優先順位付けするために、コンテンツのワークフローと重要資産に焦点をあてた正規のセキュリティリスク査定プロセスを作成します。 | * セキュリティの**リスク査定**の範囲を明確に定義し、**必要に応じて修正します**。 * リスク発生の可能性、会社の目標やコンテンツ保護へのインパクト、優先順位付けをするための資産の分類を使用する体系的なアプローチを導入します。 * 文書化された**ワークフロー**に関するベストプラクティスについては、MS-6.0を参照してください。 |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| MS-2.1 | リスク管理 | 最低限でもMPAAベストプラクティス共通ガイドラインおよび該当する補足ガイドラインに基づき、主要なワークフローの変化に対応して、社内の**リスク査定**を年に一度行い、特定されたリスクへの対応策を実施します。 | * 少なくとも四半期に一度、経営陣および主要関係者と会議を開き、コンテンツの盗難・漏えいのリスクを特定・文書化します。 * DS-1.8 および DS-1.9に基づき、四半期に一度、外部と内部ネットワークの脆弱性スキャンおよび外部侵入テストを行います。 * コンテンツの損失が起きる可能性があると思われる主要なリスクを特定します。 * 特定されたリスクを緩和または軽減するために、コントロールを実装および文書化します。 * 少なくとも四半期に一度、対策と実装されたコントロールの効果性をモニターおよび査定します。 * セキュリティイニシアティブ、アップグレード、保守に関する作業を文書化し、予算を作成します。 |
| MS-3.0 | セキュリティ構成 | コンテンツおよび資産へのアクセスが可能なセキュリティの主要ポイントを特定し、これらを保護するための役割と責任を正式に規定します。 | * 組織図と役職リストを作成し、コンテンツセキュリティに関連する役割と責任の割り当てをスムーズに実行します。 * 職務に関連する範囲で、警備員に対してポリシーや手順に関するオンラインまたは対面式のトレーニングを実施します。 |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| MS-4.0 | ポリシーと手順 | 資産とコンテンツのセキュリティに関するポリシーと手順を規定します。ポリシーは少なくとも次のトピックをカバーしていなければなりません。   * 容認できる使用（例: ソーシャルネットワーク、インターネット、電話、パーソナルデバイス、モバイルデバイス） * 資産とコンテンツの分類および取扱いポリシー * ビジネス継続性（バックアップ、保持、復旧） * 変更管理と設定管理ポリシー * 守秘義務ポリシー * デジタル記録デバイス（例: スマートフォン、デジタルカメラ、カムコーダー） * 例外ポリシー（例: ポリシーからの逸脱を文書化するプロセス） * インシデント対応ポリシー * モバイルデバイスポリシー * ネットワーク、インターネット、ワイヤレス ポリシー * パスワードコントロール（例: パスワードの最低文字数、スクリーンセーバー） * セキュリティポリシー * ビジターポリシー * 懲戒/制裁ポリシー * コンテンツに関する不正行為または誤使用を報告するための、社内の匿名通報手法（例：電話ホットラインまたはEメールアドレス） | * ポリシーと手順を開発する際は、施設/事業に固有のワークフローを検討してください。 * すべてのポリシーと手順は、印刷・公表する前に経営陣の認可が必要です。 * 新入従業員のオリエンテーション研修で、懲戒措置について説明します。 * 検討すべきポリシーと手順の一覧については、付録Fを参照してください。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| MS-4.1 | ポリシーと手順 | 少なくとも年に一度、セキュリティポリシーと手順を見直し、更新します。 | * 年に一度の経営陣によるセキュリティポリシーおよび手順のレビューでは、次の要素を検討してください。 * 最近のセキュリティトレンド * 従業員からのフィードバック * 新型の脅威と脆弱性 * 規制当局（例: FTC）からの推奨事項 * 過去に発生したセキュリティインシデント |
| MS-4.2 | すべての現行ポリシー、手順および／または顧客の要件に関して、すべての**従業員**（例: 社員、一時雇用者、研修生）および**サードパーティの従業員** （例: 契約社員、フリーランサー、派遣会社）に通達し、合意の署名を義務付けます。 | * **従業員**および**サードパーティの従業員**を新規雇用する際、すべての全般的ポリシーと手順を網羅した会社のハンドブックを配布します。 * セキュリティポリシーと手順および顧客の要件における更新事項を、**従業員**および**サードパーティの従業員**に通知します。 * 経営陣は、すべての**従業員**および**サードパーティの従業員**からの、現行ポリシー、手順、および顧客の要件に関する合意の署名を保持しなければなりません。 |
| MS-4.3 | ポリシーと手順 | セキュリティポリシーと手順に関する認識向上プログラムを開発し、定期的に更新すると共に、**従業員**および**サードパーティの従業員**を新規雇用する際、そして以後は年に一度、少なくとも次の分野を対象に、これらのセキュリティポリシーと手順に関する研修を行います。   * ITセキュリティのポリシーと手順 * 一般的なコンテンツ/資産に関するセキュリティと取扱い、および顧客固有の要件 * セキュリティインシデントの報告と上部報告 * 懲戒措置ポリシー * 暗号化されたコンテンツを取り扱うすべての人を対象とする、暗号化とキー管理 * 資産処分と破壊プロセス | * 経営陣/スタッフのミーティング中に、セキュリティの認識に関するメッセージを伝えます * 年一度のセキュリティ研修を完了した**従業員**を追跡するための手順を導入します（例：データベース保管庫、出席者の記録、完了証明書） * **従業員**と**サードパーティの従業員**を新規雇用する際に、よくあるインシデント、それに付随するリスク、探知されたインシデントの報告義務に関する、オンラインまたは対面の研修を行います * セキュリティに関する認識を促すため、ポスター、Eメール、定期ニュースレターなど、セキュリティの認識向上のための資料を配布します * 不正行為の問題発生を緩和するため、職務および重要性の高いコンテンツとの接触状況に基づき（例：IT要員、プロダクション）、対象者に合わせたメッセージと研修を開発します * 研修セッションを録画し、参照用に利用できるようにすることを検討します |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| MS-5.0 | インシデント対応 | セキュリティ問題が検知・報告された際に講じる対応策を規定する正規のインシデント対応プランを作成します。 | * **インシデント対応**プランには、次の各セクションを含めることを検討します。 * インシデントの定義 * セキュリティチームへの通知 * 経営陣への通知 * インパクトと優先事項の分析 * インパクトの抑制 * 撲滅と回復 * 顧客のスタジオ連絡先を含む、主要な連絡先情報 * 影響があるビジネスパートナーと顧客への通知 * 警察への通知 * インシデントの詳細報告 * コンピュータセキュリティ インシデントの取扱いについて規定しているNIST SP800-61第二版を参照してください。 |
| MS-5.1 | セキュリティインシデントの検知、分析、是正を担当するインシデント対応チームを編成します。 | * あらゆるタイプのセキュリティインシデントに対応するために、複数の部課から担当者を集めます。これらの部課の例を下記に挙げます。 * 経営陣 * 物理的セキュリティ * 情報セキュリティ * ネットワークチーム * 人事部 * 法務部 * **インシデント対応**チームのメンバーが、インシデントへの対応における自らの役割と責任を理解できるように、トレーニングを実施します。 |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| MS-5.2 | インシデント対応 | セキュリティの**インシデント対応**チームに、検知されたインシデントを報告するためのセキュリティインシデントの報告プロセスを設定します。 | * 不正や疑わしい活動の報告に使用できる匿名ホットラインやウェブサイトの設置を考慮してください。 * インシデント対応チームの全員に通知されるよう、グループEメールアドレスの導入を検討します。 * 疑わしい活動を匿名で通報するMPAA通報ホットラインを活用することを検討してもよいでしょう。付録Hの24時間通報ホットラインの連絡先情報を参照してください。 |
| MS-5.3 | 漏えい、盗難、またはその他の形で被害に遭ったコンテンツ（例: 紛失した顧客の資産）の所有者である顧客にインシデント発生について速やかに連絡し、経営陣と顧客を交えて事後対策会議を開きます。 | * セキュリティ侵害の通知フォームの使用も含め、セキュリティ侵害通知プロセスを実装します。 * 法務部と相談し、影響を受けた顧客にコンテンツ喪失を報告する際の適切なアクションを決定します。 * 発生したインシデントから学んだことを検討し、インシデント対応プランとプロセスの改善策を特定します。 * 根本原因を分析し、インシデントの発生を許したセキュリティの脆弱性を特定します。 * 類似インシデントの再発を防止するために、是正コントロールを特定・実装します。 * 是正アクションプランを含め、事後会議の結果を顧客に報告します。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| MS-6.0 | ビジネス継続性と災害復旧 | ビジネスの継続性を確実にするために取るべき措置を説明した、正式なプランを制定します。 | * **ビジネス継続性**プランには、次のセクションを組み入れることを検討してください。 * 停電や通信の切断、システムの故障、自然災害を含む、重要な資産およびコンテンツへの脅威 * 重要なWANおよびLAN /内部ネットワーク用デバイスの設定を含む、詳細な情報システム、コンテンツとメタデータ、バックアップ手順と情報システムの文書化 * バックアップの暗号化（最低限でもAES-128ビットの暗号化） * CCTVシステム、アラーム、および重要なシステムを安全にシャットダウンするソフトウェアを含む重要な情報システムを、少なくとも15分間サポートするためのバックアップ用電源供給 * バックアップの置き場所として、施設外の場所を使うことを検討 * セキュリティチームへの通知 * 経営陣への通知 * インパクトと優先事項の分析 * インパクトの抑制 * 手作業で急場をしのぐ手段や復旧されたシステムの詳細な設定を含む、復旧の優先順位および詳細な復旧手順 * 主要な連絡先情報 * 影響があるビジネスパートナーと顧客への通知 * 少なくとも年に一度の、ビジネス継続性および災害復旧プロセスのテスト実施 |
| MS-6.1 | 継続性に関するインシデントの探知、分析、是正を担当するビジネス継続性チームを編成します。 | * 役割と責任の規定を含めます * ビジネス継続性チームのメンバーが自分たちの役割と責任を理解するよう、研修を行います |
| MS-7.0 | 変更管理と設定管理 | 新しいデータ、アプリケーション、ネットワーク、システム構成要素が、事前に会社幹部の承認を得ていることを確実にするためのポリシーと手順を規定します。 | * デバイスのインストール、設定および使用、ならびにサービスと機能について説明した文書を含め、必要に応じて更新します * 既知の問題に対処するためのポリシーと手順を文書化します * バグとセキュリティの脆弱性を報告するためのポリシーと手順を含めます * 許可されていないハードウェアまたはソフトウェアのインストールを制限およびモニターします * データ、アプリケーション、ネットワークのインフラ、およびシステムの変更に関連するリスクを管理します * すべての変更要請、テスト結果、および経営陣の承認を記録し保持します |
| MS-8.0 | ワークフロー | コンテンツと承認チェックポイントをトラッキングする**ワークフロー**を文書化します。物理的コンテンツとデジタルコンテンツについては、次のプロセスを含めます。   * 配送（受領/返送） * 配給 * 移動 * 保管 * 除去/破壊 | * スイムレーン図を使用して**ワークフロー**を文書化します。 * 適宜、資産の処理・取扱い情報を含めます。 * 各接点がコンテンツに与えるリスクを評価します。 * 承認チェックポイントに関するコントロールを実装します。 * 関連するアプリケーションのコントロールを特定します。 |
| MS-8.1 | 変更があった場合には**ワークフロー**を更新し、少なくとも年に一度、変更を明らかにするために**ワークフロー**プロセスを見直します。 | * 脆弱なエリアを特定するために、各プロセスでコンテンツの**ワークフロー**と実装されているコントロールを確認します。 |
| MS-9.0 | 任務の分割 | コンテンツ**ワークフロー**の中で、任務を分割します。分割が実際的でない部分は、補足コントロールを実装・文書化します。 | * 次に挙げるような役職ベースの仕事が重複しないように、役割と責任を文書化します。 * **保管庫**とサーバー/マシンルームの担当者 * 入出荷の担当者 * 施設内の**保管庫**からコンテンツ/制作エリアへの資産の移動（例: ランナー） * **デジタル資産**フォルダーへのアクセス（例: データラングラーがプロデューサーのためのアクセスを設定） * 制作担当者からコンテンツを転送する担当者 * 手動コントロール（例: コンテンツ作業開始前のプロデューサーからの承認）、または自動コントロール（**ワークフロー**の各段階における自動承認）を使用して任務を分割します。 * 分割ができない場合は、次のような補足コントロールを実装します。 * 従業員やサードパーティの従業員の活動をモニターする * 監査ログを維持およびレビューする * 物理的分割を実施する * 経営陣による監督を実施する |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| MS-10.0 | 経歴確認 | すべての**従業員**や**サードパーティの従業員**の経歴を確認します。 | * 経歴確認は、該当法、規制、組合の定款、文化的考慮項目に基づいて行います。 * ビジネス要件に比例した経歴審査を用い、アクセスされるコンテンツの重要度、コンテンツの盗難や漏えいリスクの可能性に照らして、**従業員**や**サードパーティの従業員**を審査します。 * 必要に応じて、身元確認、学歴、職歴や資格なども確認します。 * 経歴審査が法律で禁じられている場合には、例外扱いであることを記述し、身元・経歴照会を行います。 |
| MS-11.0 | 守秘契約 | 雇用時および雇用後は年に一度、全**従業員**に守秘契約書（例: 非開示契約）への署名を求めます。これには、コンテンツの取扱いと保護に関する要件も盛り込みます。 | * 雇用、契約、合意書の終了後における守秘義務関連の非開示ガイダンスを盛り込みます。 * 必要に応じて、守秘義務/NDAの重要性を法律用語を使用せずに説明します。 * **従業員**がビジネスに関連する重要性の高いコンテンツを扱うために使用する機器関連の情報が、すべて確実に会社に転送され、機器から安全な形で削除されるようにします。 * 経営陣は、全**従業員**の署名済みの守秘契約書を保持しなければなりません。 |
| MS-11.1 | 全**従業員**に対し、雇用または契約の終了時点で所持しているコンテンツと顧客の情報を、すべて返却するよう義務付けます。 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| MS-12.0 | サードパーティの利用と審査 | サービスの契約時に、コンテンツを取扱う**サードパーティの全従業員**（例：フリーランサー）に対し、守秘契約書（例: 非開示契約）への署名を義務付けます。 | * 雇用、契約、合意書の期間中または終了後における守秘義務関連の非開示ガイダンスを盛り込みます。 * 必要に応じて、守秘義務/NDAの重要性を法律用語を使用せずに説明します。 * **サードパーティの従業員**がビジネスに関連する重要性の高いコンテンツを扱うために使用する機器関連の情報が、すべて確実に会社に転送され、機器から安全な形で削除されるようにします。 * 経営陣は、**サードパーティの全従業員**の署名済みの守秘契約書を保持しなければなりません。 * コンテンツの取扱いと保護に関する要件を含めます。 |
| MS-12.1 | **サードパーティの全従業員**に対し、契約の終了時点で所持しているコンテンツと顧客の情報を、すべて返却するよう義務付けます。 |  |
| MS-12.2 | サードパーティの契約にセキュリティ要件を含めます。 | * **サードパーティの従業員**に、サードパーティ契約と顧客の要件に指定されているセキュリティ要件に準拠することを義務付けます。 * 重要度の高いコンテンツに関連する活動の監査条項に権利の規定を盛り込みます。 * セキュリティ要件への準拠に照らしたモニターのプロセスを実装します。 |
| MS-12.3 | 関係が終了した時点で**コンテンツ**の返還を要求するためのプロセスを導入します。 | * サードパーティの機器にあるすべての**コンテンツ**が確実に会社に転送され、機器から安全な形で削除されるようにします。 |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| MS-12.4 | サードパーティの利用と審査 | 必要に応じ、**サードパーティの従業員**に身元保証と保険加入を義務付けます（例: 宅配業）。 | * **サードパーティの従業員**に、保険証の提示と、保険会社の記録と保険番号の維持を義務付けます。 * サードパーティの保険会社に、一定レベルの補償内容を義務付けます。 * 連絡先情報が変わった場合を含め、年に一度の情報の更新を義務付けます。 |
| MS-12.5 | サードパーティによるコンテンツ/制作エリアへのアクセスを制限します。ただし職務の遂行に必要な場合は例外とします。 | * **サードパーティの従業員**がコンテンツの保管エリアに電子媒体を使用してアクセスすることを認可してはなりません。 * **サードパーティの従業員**（例: 清掃員）による制限エリア（例: **保管庫**）へのアクセスが必要な場合は、担当者が同伴します。 |
| MS-12.6 | **下請け業者**がコンテンツを取扱う、または作業を他の会社に下請けさせる場合は、その旨を顧客に通達します。 | * 書面による顧客の合意署名/承認を義務付けます。 * 下請け業者に、標準的な**デューデリジェンス**のアクティビティの実行を義務付けます。 * 他の会社に下請けされる作業は、その旨をMPAAメンバーのスタジオに報告し、MPAAベンダーアンケートを記入の上、デューデリジェンスを行うためにメンバーのスタジオに提出しなければなりません。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| PS-1.0 | 出入り口 | 出荷ドックのドアと窓を含む施設のすべての出入り口を、常に安全な状態に保ちます。 | * 受付とそれ以外のエリアとの間がアクセスコントロール付きのドアで仕切られている場合、営業時間内は出入り口を施錠する必要はありません。 |
| PS-1.1 | 施設内でコンテンツを取り扱うエリアと別のエリア（例: 管理事務所、待合室、出荷ドック、運送会社の受取り・引渡しエリア、複製・マスタリング）とを隔離することにより、コンテンツエリアへのアクセスをコントロールします。 | * コンテンツにアクセスする必要がある人だけに、コンテンツ/制作エリアへの出入りを許可します。 * 映写室へのアクセスを制限します。 * **メディア**プレーヤー（例: Blu-ray、DVD）がある部屋へのアクセスを制限します。 * 任務の分割モデルを施行し、同一人物が複製およびマスタリングの両方の部屋へ入室することを制限します。 |
| PS-1.2 | 施設内にある、複数の事業が使用する場所へのアクセスをコントロールします。それには次の方法が含まれますが、それらに限定されません。   * 作業エリアを分割する * 事業ユニットごとに分割できる、アクセスをコントロールした出入り口を設ける * 施設内のすべての出入りを記録・モニターする * 契約前に、施設内のすべてのテナントを顧客に報告しなければならない |  |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| PS-2.0 | ビジターの出入り | 次の項目を記載した、ビジターの詳細な記録を残します。   * 氏名 * 社名 * 来社時間/退去時間 * 社内担当者 * ビジターの署名 * ビジターバッジに記載された名前 | * 各ビジターには写真付き身分証明書（例: 運転免許証または政府発行の身分証明書）を提示してもらい、本人であることを確認します。 * 過去に来社したビジターの氏名を見せないような工夫も考慮してください。 |
| PS-2.1 | 各ビジターには、**IDバッジ**またはスティッカーを発行し、退社するまで見える位置に装着することを義務付けます。また退社の際には返却してもらいます。 | * ビジターバッジは**従業員**のバッジ（例: 色分けされたプラスチック製のバッジ）と簡単に区別できるよう工夫します。 * 紙製のバッジやスティッカーは、毎日色を変えることも考慮してください。 * 期限切れになると変色するバッジの使用も考慮してください。 * 発行したバッジは出入りの際に記録にとります。 * ビジターバッジには連番を付け、トラッキングが可能なようにしておきます。 * バッジは毎日終業時に数がそろっていることを確認します。 |
| PS-2.2 | ビジターには、コンテンツ/制作エリアへのキーカードによるアクセスを許可してはなりません。 |  |
| PS-2.3 | ビジターは施設にいる間、もしくはコンテンツ/制作エリアにいる間は、権限を持つ従業員が同伴する必要があります。 |  |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| PS-3.0 | 身分証明書 | **従業員**と長期雇用の**サードパーティの従業員**（例: 清掃業者）には、写真付きの**身分証明（ID）バッジ**を、常に目に見える位置に携行するよう義務付けます。 | * 経歴確認が完了した**従業員**と長期雇用の**サードパーティの従業員**全員に、**写真付きID**を支給します。 * 雇用や契約の終了時に、**写真付きID**を速やかに返却するプロセスを導入・実行します。 * **写真付きID**には、場所、会社名、ロゴその他の個別情報を省くことを考慮します。 * 可能な場合は、アクセスキーカードとしても使用できる**写真付きID**の採用も考慮してください。 * **写真付きID**の紛失、盗難が発生した場合は、ただちにその旨を報告するよう従業員に義務付けます。 * 一日24時間体制で**写真付きID**の紛失・盗難届けを受け付ける電話番号やウェブサイトを設置してください。 * IDを見えるように身に付けていない人を見かけたら、立ち止まらせて身元確認をするよう従業員を訓練・奨励します。 |
| PS-4.0 | 周辺のセキュリティ | 会社の**リスク査定**で施設が特定されたリスクにさらされている可能性がある場合に、これに対処する周辺セキュリティコントロールを実装します。 | * このセキュリティコントロールは、施設の地理的位置や間取りによって異なりますが、次のような施策を講じてください。 * 8フィート（2.4メートル）以上の高い壁、フェンス、ゲートで終業後のアクセスを制限 * 喫煙指定場所やバルコニーなどの屋外共有エリアの安全を確保するために囲いを設置 * 屋外共有エリア（例: 喫煙指定場所）や駐車場を監視するカメラの取り付け * 標的となることを避けるために、会社を示す看板を過剰に使用することを控える * （必要に応じて）周辺に鳴り響くアラームを設置 |
| PS-4.1 | 周辺の入り口および非常口以外の出入り口には、常時警備員を配置します。 |  |
| PS-4.2 | 周辺のセキュリティ | 毎日の警備パトロールは無作為化したスケジュールで行い、パトロールの結果をログに記録します。 | * 警備員に、建物の内外をパトロールするよう義務付けます。 * 密封箇所が密封状態であることの確認を含めて、非常口も点検します。 * パトロール順路（例: チェックポイント）をトラッキングし、施錠を確認するために、警備員パトロールシステムの使用を考慮してください。 |
| PS-4.3 | 周辺の門は、常に施錠するようにします。 | * 施設への車両の進入を管理するために、電子制御によるゲートアームを設置し、警備員を配置します。 * 書類の記入が完了した従業員とサードパーティの従業員に駐車許可証を配布します。 * ビジターの車両にはIDの提示を義務付け、すべてのビジターが構内に進入する前に事前承認を受けていることを確認します。 |
| PS-5.0 | アラーム | すべての出入り口（非常口を含む）、窓、荷積みドック、火災時の出口、制限エリア（例: **保管庫**、サーバー/マシンルーム）に一斉に響き渡る中央アラームシステムを設置します。 | * 施設に許可なしに侵入した人間がいる場合、警備員に通報するアラームをすべての出入り口に設置します。 * 施設が監督下にない場合にアラームが稼働するようにします。 |
| PS-5.1 | 制限エリア（例: **保管庫**、サーバー/マシンルーム）の効果的な位置に動作検知器を設置し、警備員や他の担当者（例：プロジェクトマネージャー、プロデューサー、編集責任者、インシデント対応チーム）に通報されるように設定します。 | * セキュリティの安全をより一層高めるために、終業後アラームシステムがストレージと**保管庫**（例: 動作検知器を使用）もカバーするように設定します。 |
| PS-5.2 | 制限エリア（例: 保管庫、サーバー、マシンルーム）に開戸アラームを設置し、規定（例: 60秒）以上の長い間、重要な出入り口のドアが開いたままになっている場合に通報するようにします。 | * 規定よりも長い間開いている場合、アラームがトリガーされ、警備員に通知されるようにアクセスコントロール付きドアを設定します。 |
| PS-5.3 | アラーム | セキュリティの責任者、または他の担当者（例：プロジェクトマネージャー、プロデューサー、編集責任者、インシデント対応チーム）に上部通報されるようにアラームを設定します。 | * 通知直後に警備員から応答がない場合、上部へ通報する手順を導入・実行します。 * セキュリティ侵害の発生を自動的に警察に通報するシステムも検討してください。 * 週末や終業後の通知手順も実施します。 |
| PS-5.4 | 固有の緊急時オン・オフ操作コードを全員に割り当てます。これは必要な関係者にはアラームシステムへのアクセスを許可し、その他の者にはアクセスを制限するものです。 | * 固有のアラームコードを使用して、アラームのオン・オフを操作したセキュリティの責任者は誰であったかを確認できます。 * 共有や紛失を防ぐために、割り当てられたアラームの緊急時オン・オフ操作コードを経営陣が認可した間隔で更新します。 |
| PS-5.5 | アラームのオン・オフ操作にアクセス可能なユーザーのリストは、四半期に一度、または担当者が変わった時に見直します。 | * 離職者や異動したユーザーをリストから削除します。 * リストから削除されたユーザーに割り当てられていたアラームコードを無効化します。 |
| PS-5.6 | アラームシステムを四半期に一度テストします。 | * 物理的セキュリティの侵害をシミュレーションし、次の項目を確認します。 * アラームシステムが侵害を検知する * 警備員が通報を受ける * 手順通り、警備員が適時に応答する |
| PS-5.7 | 停電時に、防火扉が開かないよう、また他の扉が閉まらないようにするための火災時の安全対策を導入し、不正アクセスを防止します。 |  |
| PS-6.0 | 承認 | 施設のアクセスを管理し、**アクセス権**の変更を記録するプロセスを作成・実施します。 | * 1人の役職者を施設アクセス承認の責任者として任命します。 * 責任者に従業員（例: 施設管理）のステータスの変化について報告します。 * **従業員**や**サードパーティの従業員**による施設アクセスを上司が依頼する物理的アクセスや電子アクセスのフォームを作成します。 * アクセス依頼に関する調査や承認の責任者を任命します。 |
| PS-6.1 | 制作システムへのアクセスを権限を持つ人間だけに制限します。 |  |
| PS-6.2 | 四半期に一度、および**従業員**および／または**サードパーティの従業員**の役職や雇用ステータスが変更になった場合、制限エリア（例: **保管庫**、サーバー/マシンルーム）へのアクセスを見直します。 | * 従業員とサードパーティの従業員のステータスを確認します。 * 雇用や契約が終了したユーザーのアクセス権を削除します。 * 各ユーザーの役職に対してアクセス権が適切であるかどうかを再確認します。 |
| PS-7.0 | 電子アクセスコントロール | 施設全体で電子アクセスシステムを設置し、すべての出入り口とコンテンツの保存、転送、処理エリアをカバーします。 | * 施設内の特定のエリアへのアクセスは、職務と責任に応じて割り当てます。 * 従業員およびサードパーティの従業員の役職の変更や離職に伴い、電子アクセスを更新します。 * 従業員に割り当てられた電子アクセスデバイスの番号をマッピングしたログを維持します。 * ロギングとモニタリングPS-10.0を参照してください。 * 共通エリア（例: 共用エレベーター）に電子アクセスが不要であった時間をレビューします。 |
| PS-7.1 | 電子アクセスコントロール | 電子アクセスシステムの管理を適切な責任者に制限します。 | * 電子システム管理は指定された担当者にのみ制限します。たとえ制作コンテンツにアクセスできる関係者であっても電子アクセスタスクは任せてはなりません。 * 電子アクセスを管理する独立チームを編成します。 |
| PS-7.2 | 在庫のカードおよび**電子アクセスデバイス**（例：キーカード、キーフォブ）を施錠したキャビネットに保管し、割り当てられる前は**電子アクセスデバイス**が無効になっていることを確認します。割り当て前の電子アクセスデバイス（例：キーカード、キーフォブ）を施錠したキャビネットに保管し、割り当てられる前はこれらが無効になっていることを確認します。 | * 施錠したキャビネットへのアクセスは、**キーカード**/**電子アクセスデバイス**システム管理チームにのみに制限します。 * キャビネットから電子アクセスデバイスを取り出すときは、担当者の署名を義務付けます。 |
| PS-7.3 | 新規の**電子アクセスデバイス**（例：キーカード、キーフォブ）を発行する前に、紛失した**電子**アクセスデバイス**を、システムで無効化します**。 | * 施設への不正アクセスを防ぐために、**従業員**および**サードパーティの従業員**に、**電子アクセスデバイス**を紛失した場合は速やかに報告するよう教育します。 * 代わりの**電子アクセスデバイス**を発行する前に、身分証明の提示を義務付けます。 |
| PS-7.4 | サードパーティ用の**電子アクセスデバイス** は、承認されている期間に基づき、有効期限（例: 90日間）付きで発行します。 | * サード**パーティ用の電子アクセスデバイス**は、必ず **従業員**用の電子アクセスデバイスと簡単に区別できるようにします。 * **電子アクセスデバイス**の有効期限は、簡単に確認できるようにします。 * サード**パーティ**の電子アクセスデバイスは、知る必要がある場合にのみ割り当てます。 |
| PS-8.0 | キー | 制限エリアへの**マスターキー（複数の場合もある）**の配布は、権限を持つ関係者（例: オーナー、施設管理者）のみに制限します。 | * **マスターキー**を借りることができる**従業員**のリストを維持します。 * **マスターキー**へのアクセスが不要となった**従業員**を削除して、リストを定期的に更新します。 |
| PS-8.1 | 制限エリアへの**マスターキー（複数の場合もある）**の配布をトラッキングおよびモニターする、チェックイン・チェックアウトプロセスを導入します。 | * 次の情報をトラッキングするために、記録を維持します。 * **マスターキーを貸与されている従業員** * チェックアウト・チェックインの時刻 * チェックアウトの理由 * **マスターキー**を約束の日時までに返却することを義務付け、定刻までに返却されていないマスターキーは調査して所在を確認します。 |
| PS-8.2 | 屋外への出入り口には、特殊技術を持つ鍵職人でなければ複製できない鍵を使用します。 | * 高セキュリティの鍵（シリンダー型）は次の要素に強いため、このタイプを使用してください。 * 鍵を使わない開錠手法 * 鍵のインプレッション * 鍵の複製 * ドリル開錠 * その他の違法開錠手段 |
| PS-8.3 | 四半期に一度、**マスターキー**および施設出入り口を含む制限エリアの鍵の在庫数を数えます。 | * 足りない鍵（紛失/盗難）を特定、調査、対応します。 * ログを見て、見つからない鍵を最後に借り出した人物を特定します。 * **マスターキー**が紛失したり、制限エリアの鍵がそろっていない場合、錠を交換します。 |
| PS-8.4 | 離職した従業員/サードパーティ、またはアクセスが不要になった者から、すべての鍵を回収します。 |  |
| PS-8.5 | キー | マスターキーまたはサブのマスターキーが紛失もしくは足りない場合、電子アクセスコントロールを実施するか、もしくは全施設の鍵を再発行します。 |  |
| PS-9.0 | カメラ | 施設のすべての出入り口と制限エリア（例：サーバー/マシンルーム）を録画する**CCTV**システムを設置します。 | * カメラのケーブルと配線は見えないように完全に隠し、通常の方法では手の届かない位置に設置します。 * 施設は、建物が設置したCCTVだけで十分だと考えるべきではありません。 * 施設のすべての出入り口にカメラを設置します。 * カメラが、必ずストレージと**保管庫**をカバーするように設置します。 |
| PS-9.1 | 監視対象範囲、機能、画像の品質、照明の状況、監視記録のフレームレートが適切であることを確認するため、少なくとも一日に一度、カメラの位置と記録をチェックします。 | * すべての出入り口とその他の重要エリアで、撮影の障害となる物体がないように、カメラの位置を再確認します。 * 暗い環境でも撮影できるカメラ（例: 低照明カメラ、赤外線カメラ、動作感知光）を使用します。 * 画像の品質を見て、照明が十分であるか、顔が見分けられるかを確認します。 * 写っている人物の活動が適切に記録できるように、フレームレートを確認します。 * 画像にコンテンツが写らないようにカメラの位置に注意します。 * 顔の特徴を明らかにできるよう、十分な解像度で記録します。 * 一秒間に最低7フレームのレートで記録します。 |
| PS-9.2 | **CCTVコンソール**と**CCTV**機器（例: DVR）への物理的アクセスとロジカルアクセスを、システムの管理・監視の責任者だけに制限します。 | * **CCTV**機器をアクセスコントロールされた安全な場所（例: コンピュータルーム、施錠してあるクローゼット、ケージ）に設置します。 * 定期的にアクセスレビューを行い、適切な関係者だけが監視機器へのアクセス権を持つことを確認します。 * IPベースの**CCTV**システム用ウェブコンソールが承認されている関係者だけに制限され、強力なアカウント管理コントロール（例: 複雑なパスワード、個々のユーザーログイン、ロギング、モニタリング）が施行されていることを確認します。 |
| PS-9.3 | カメラ | カメラの監視記録には必ず正確な日付とタイムスタンプが記録されるようにすると共に、**CCTV**監視記録と電子アクセスログを少なくとも90日間、または法律で認められている最大日数、安全な場所に保管します。 | * テープやディスクに記録されたカメラ映像を収録した物理**メディア**に日時を刻印します。 * デジタルカメラ映像を収録する機器に正確なタイムスタンプが保持されていることを確認します。 * 少なくとも週に一度、日付とタイムスタンプが正確であることを確認します。 * ログをアクセスコントロール付きのテレコムクローゼットまたはコンピュータルームに保管することを検討してください。 * 一日分のログに必要な平均的スペースを特定し、ログサイズが少なくとも90日間または法律で認められている日数分の記録を維持するのに十分であることを確認します。 * CCTVの監視記録は、制作品が最初にリリースされる日まで保持することを検討します。 |
| PS-9.4 | 一人の従業員またはグループを指名し、営業時間に監視ビデオをモニターし、検知したセキュリティインシデントを即座に調査するようにします。 | * セキュリティインシデントを取り扱うために、インシデント対応プロセスを導入します。 * 受付またはITオフィスに監視用モニターを追加することを検討します。 |
| PS-10.0 | ロギングとモニタリング | 疑わしい現象をチェックするため、制限エリアへの電子アクセスのログを取り、少なくとも週に一度レビューします。 | * 疑わしいと見なされる現象を特定し、そのリストを文書化します。 * 疑わしい電子アクセス活動が検知された際に適切なセキュリティ担当者にリアルタイムアラートが送信される、自動報告プロセスの実施を検討してください。 * ログは、少なくとも一年間保存します。 * 次に挙げる現象を記録にとり、レビューします。 * 繰り返し失敗しているアクセスの試み * 一日の中で不自然な時間帯のアクセス * 複数のゾーンにおいて連続的に起こるドアアクセス |
| PS-10.1 | ロギングとモニタリング | 次のエリアへの電子アクセスを記録に取り、少なくとも一日に一回レビューします。   * マスター/スタンパーの保管庫 * プリマスタリング * サーバー/マシンルーム * スクラップルーム * セキュリティ保護されたケージ | * 通常と異なる事象を特定・文書化します。 * 疑わしい電子アクセス活動が検知された際に適切なセキュリティ担当者にリアルタイムアラートが送信される、自動報告プロセスの実施を検討してください。 |
| PS-10.2 | 検知された疑わしい電子アクセス活動を調査します。 | * 通常と異なる電子アクセス活動の検知の際に通報するべき連絡先情報を特定し、関係者に通知します。 * 第一連絡先がイベント通知に適時に反応しない場合に、上部に連絡する手順を設定・実行します。 |
| PS-10.3 | すべての電子アクセスの確認済みインシデントを継続的にログに記録・維持し、実行したフォローアップ活動の記録文書もそれに含めます。 | * **インシデント対応**報告フォームを使用して、確認済みの**キーカード/電子アクセスデバイス**のインシデントを文書化します。 * 最近発生したすべての**キーカード/電子アクセスデバイス**のインシデントを定期的にレビューし、根本原因を分析して脆弱性と適切な是正策を特定します。 |
| PS-11.0 | 身体検査 | 現地の法律で認められる範囲で、警備員が顧客のコンテンツがないかどうかチェックするため、人、かばん、荷物、および個人の所持品を無作為に検査できるポリシーを制定します。 | * **従業員**と**サードパーティの従業員**全員の所持品検査に関するポリシーを発行します。 * ポリシーに準拠して、定期的に**従業員**と**サードパーティの従業員**の所持品検査を行います。 |
| PS-11.1 | 身体検査 | 従業員やビジターを含め、施設から出る人全員を対象として次のような身体検査を行います。   * コートや上着、帽子、ベルトを取り外す * ポケットの中身は全部出す * 警備員が見守る中で、本人が身体の各部を平手で軽くたたく * バッグ、かばん、袋は中身をすべて調べる * ラップトップのCD/DVDトレイを検査する * 3インチ（7.6センチ）以内で使用するハンドヘルド式の金属探知機で各個人をスキャン | * 警備員に、正式の承認なしでは外からの持ち込みが制限されているアイテム（例: カメラ）や、外への持ち出しが禁止されている映画資材を探すよう指示します。 * 従業員とサードパーティの従業員全員の所持品検査に関するポリシーを発行します。 * 検査を待つ行列ができたり、待ち時間が長くなったりしないよう、警備員のシフトを工夫します。 |
| PS-11.2 | デジタル記録デバイス（例: **USB**、サムドライブ、デジタルカメラ、携帯電話）を所持しての施設への出入りは禁止されています。これらのデバイスは退去する際も検査の対象となります。 | * 検知されたデジタル記録デバイスは没収し、セキュリティ保護されたロッカーに保管します。 * コンテンツ窃盗の試みはすべて文書化します。 * コンテンツ窃盗を試みた個人への懲戒措置を講じます。 * デジタル記録機能の付いたモバイルデバイスを禁止するポリシーを策定・施行します。 * 不正操作の証拠を示すスティッカーを使用している場合、デジタル記録機能の付いた携帯電話を許可します。 |
| PS-11.3 | 制作エリアへ食べ物を持ち込むときは、透明なビニール袋と容器の使用を徹底します。 | * 制作エリアの外に食事エリアを確保することを考慮してください。 |
| PS-11.4 | オーバーサイズの衣類（例: バギーパンツ、オーバーサイズのフード付きトレーナー）を禁止する服装規定ポリシーを実施します。 |  |
| PS-11.5 | 施設内外への持ち出し・持ち込みが承認されているデバイスを確認できるように、番号付きの不正操作の証拠を示すスティッカー/ホログラムを使用します。 |  |
| PS-11.6 | 身体検査 | 退出時の身体検査手順をテストするプロセスを導入します。 | * 定期的に身体検査の監査を行い、警備員が身体検査を怠りなく実行していることを確認します。 * 退出時の身体検査プロセスを改善する方法を特定します。 * 身体検査プロセスの監査と改善策をすべて文書化します。 |
| PS-11.7 | 施設の駐車場から退去する車両を無作為検査します。 |  |
| PS-11.8 | 重要度が非常に高いコンテンツを処理する複製ラインを隔離し、隔離エリアから出る人の身体検査を行います。 |  |
| PS-11.9 | 追加のコントロールを導入して、警備員の活動をモニターします。 | * 警備員の退出時の身体検査をレビューします。 * プラント/制作エリアの監視を、出入り口監視と分離します（例: 身体検査）。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| PS-12.0 | 在庫トラッキング | コンテンツの資産管理システムを実装して、物理的資産（例：顧客から受領、施設で制作）の詳細なトラッキングを行います。 | * 特定の関係者がコンテンツを借り出すことができることを確認するには、リリースフォームまたはワークオーダーが必要です。 * 各個人から身分証明書を提示してもらい、本人であることを確認します。 * すべての資産にはタグ（例: バーコード、固有のID）が必要です。 * 借り出し・返却された資産はすべて記録にとります。 * 借り出しの際は返却予定期間を記録にとります。 * 営業日の終業時、または承認された期間の終わりまでに返却されていない資産がある場合、それを通報するための自動アラームの使用を検討します。 * 返却期日を超過した場合、記録を確認し、借り出した人に連絡をとってフォローアップを行います。 * 各資産の所在場所をログに記録します。 * 各借り出し・返却の日時を記録します。 |
| PS-12.1 | 顧客の資産および作成された媒体（例: テープ、ハードドライブ）には、受領時にバーコードを付けるか固有のトラッキング用識別子を割り当て、非使用時には保管庫に保管します。 | * 資産トラッキングのためにデュアルバーコード（資産と容器・ケースの両方）を使用します。 * 資産は、バーコードを付けた後、直接**保管庫**に返送します。また、必要がなくなった資産もただちに**保管庫**に返送します。 |
| PS-12.2 | 少なくとも一年間、資産移動トランザクションログを維持します。 | * すべての資産の動きを物理的ログまたはデジタルログに記録します。これらのログには次の情報を含みいれます。 * 借り出し・返却された資産のバーコードまたは固有のID * 借り出し・返却の日時 * 資産を借り出した人の氏名と固有のID * 借り出しの理由 * 資産の場所 |
| PS-12.3 | 在庫トラッキング | 少なくとも週に一度コンテンツの**資産管理**システムからのログをレビューし、異常がないか調査します。 | * 返却予定日までに返却されていない資産を特定します。 * 返却されていない資産を最後に借り出した人に連絡をとって、フォローアップを行います。 * **資産管理**ポリシーに準拠しない個人に対して懲戒措置を施します。 * 資産が長期にわたって借り出されている場合は、自動リマインダーを送信するシステムを検討してください。 |
| PS-12.4 | 該当する場合、物理的資産と資産トラッキングシステムにおいて、スタジオ映画タイトルには別名を使用します。 | * 適宜、物理的資産のスタジオ名を消去することを検討してください。 |
| PS-12.5 | 日別レポートを作成・レビューして、**保管庫**から借り出されて返却されていない重要度のきわめて高い資産を特定します。 | * 手作業または**資産管理**システムで日別レポートを実行します。 * すべての例外を調査します。 |
| PS-12.6 | 荷物が適時に配送されない場合、遅延や返却された資産を確認し、記録します。 | * 資産をアクセスコントロール付きのエリアに保管する手順を設定します。 * 保管の日付と理由を含め、資産を現場で保管していることを記録した文書を維持します。 |
| PS-13.0 | 在庫確認 | 四半期に一度、顧客の資産の在庫を確認し、**資産管理**記録と照合し、不一致はただちに顧客に連絡します。 |  |
| PS-13.1 | **保管庫**のスタッフと在庫確認を行う個人の間で任務を分割します。 | * **保管庫**以外のスタッフに個数結果の無作為チェックを行ってもらいます。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| PS-14.0 | ブランクメディア/未処理ストックトラッキング | ブランクメディア/未処理メディアは、受け取った際に、ユニットごとにタグ（例: バーコード、固有のIDを割り当てる）を付けます。 | * 制作のために必要な場合以外は、ブランクまたは未処理の**メディア**ストックをセキュリティ保護された制作エリアに入れてはなりません。 |
| PS-14.1 | 未加工資材（例: ポリカーボネート）の使用を月に一度トラッキングするプロセスを設定します。 | * 現在ある未加工資材をワークオーダーと照合し、在庫の差を特定します。 * 超過すると**インシデント対応**プロセスが作動するような、不一致件数の上限を設定します。 * 月に一度のトラッキングプロセスの一環として、未加工資材を物理的に数える作業も考慮してください。 |
| PS-14.2 | ブランク**メディア**/未処理ストックをセキュリティ保護された場所に保管します。 | * 不正アクセスを防止するために、アクセスコントロール（例: 施錠されたキャビネット、金庫）を義務付けます。 * 作品制作責任者のブランク**メディア**/未処理ストックへのアクセスを制限します。 * ブランク**メディア**/未処理ストックを借り出すには、正式なワークオーダーリクエストを提示することを義務付けます。 |
| PS-15.0 | 顧客の資産 | 終了した顧客の資産へのアクセスを、資産のトラッキングおよび管理の責任者のみに制限します。 | * 顧客の資産のアクセスを**保管庫**のスタッフのみに制限します。次に、保管庫のスタッフは有効なワークオーダーリクエストを提示した個人にアクセスを許可することができます。 * **保管庫**のスタッフが制作データを処理するために取り扱う必要がないように、任務を分割します。 |
| PS-15.1 | 顧客の資産は、セキュリティ保護された制限エリア（例: **保管庫**、金庫、または他のセキュリティ保護された保管場所）に保存します。 | * 非常に重要度の高い作品は、**保管庫**の中に金庫か高セキュリティのケージを設置して保存します。 * 金庫は部屋の構造にボルトで締めて、壁または床に固定させます。 |
| PS-15.2 | 終業後の重要エリア（例: 金庫、セキュリティ保護されているケージ）を開錠する場合は、異なるアクセスカードを持つ2名の**従業員**の立ち会いを義務付けます。 |  |
| PS-15.3 | 顧客の資産 | 未配送の荷物を施設に一晩おいておく場合、施錠した防火金庫を使用します。 | * 金庫は不動の表面（例: 床、壁）にボルトで固定します。 |
| PS-15.4 | 未配送のスクリーナーを保管するために専用のセキュリティ保護されたエリア（例: セキュリティ保護されているケージ、部屋）を用意します。このエリアは、施錠およびアクセスコントロールされ、監視カメラおよび／または警備員によってモニターされなければなりません。 | * 職務上必要な関係者のみに入室を制限します。 * スクリーナーの保管エリアには隙間がなく、施錠されていて、始終モニターされていることを確認します。 * 定期的に、監視ビデオをレビューするプロセスを実施します。 |
| PS-16.0 | 処分 | 却下されたり、損傷を受けたり、もしくは時代遅れとなった顧客の資産を含むストックは、処分の前に削除、消磁、シュレッド、または物理的に破壊しなければなりません。 | * 在庫の確認と照合を行い、拒否されたり、損傷を受けたり、時代遅れとなったストックを安全な形でリサイクルしたり、破壊したりします。 * 媒体は、スクラップ容器に入れる前に修復不能になるよう破壊します。 * デジタルシュレッディングとワイピング標準については、米国国防省の5220.22-Mを参照することを検討してください（付録Gを参照）。 |
| PS-16.1 | リサイクルや破壊する部品はセキュリティ保護された場所や容器内に保存し、資産の処分前にコピーや再使用されるのを防ぎます。 | * リサイクルや破壊する前に、拒否されたり、損傷を受けたり、時代遅れとなったストックを保存する期間（例: 30日間）を制限するポリシーを設定・実施します。 * リサイクルや破壊する前に、重要度の高い資産をセキュリティ保護されたエリア（例: **保管庫**、金庫）で保管します。 * 処分するストックを入れる容器には必ず施錠してください。 |
| PS-16.2 | 資産処分のログは少なくとも12ヶ月間維持します。 | * 資産処分のログは**資産管理**プロセスに統合します。 * 処分ログに処分資産の最終記録を含めます。 |
| PS-16.3 | 処分 | 破壊は施設内で行わなければなりません。施設での破壊は、二人の従業員の監視と署名による承認が必要です。サードパーティの会社を使って破壊を行う場合は、二人の従業員の監視と署名による承認が必要で、かつ破壊証明書を保持しなければなりません。 | * 破壊証明書には次の情報を盛り込むよう義務付けることを考慮してください。 * 破壊期日 * 破壊・処分された資産の説明 * 破壊の手段 * 資産破壊の実行者 |
| PS-16.4 | 廃棄するディスクを複製器から直接スクラップ容器に移動する自動手段を使用します（機械オペレータの処理なし）。 | * 自動処分が利用できない場合、任務の分割を実行します（チェックディスクの作成者とディスクを破壊する担当者が別々の人であること）。 * ディスクを処分した日時を記録・署名したログを維持します。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| PS-17.0 | 出荷 | 顧客の資産を施設から出荷することを許可するために、有効なワークオーダー/出荷オーダーを作成するよう施設に義務付けます。 | * ワークオーダー/出荷オーダーには次の情報を含めます。 * ワークオーダー/出荷オーダー番号 * コンテンツの受取人の氏名と会社名 * 受取り日時 * 施設の説明 * 資産が通常以外の手段で施設外へ運送されたことを文書化するフォームを作成します。 |
| PS-17.1 | 顧客の資産出荷の詳細をトラッキング・ログ記録します。それには、少なくとも下記の項目を含めます。   * 出荷時刻 * 出荷人の氏名と署名 * 受取人の氏名 * 宛先 * 運送会社が割り当てたトラッキングナンバー * 該当するワークオーダーの記述 | * 受取人の署名を要する * 少なくとも一年間、出荷ログを保持します。 |
| PS-17.2 | 受取人を待つ顧客資産を安全な状態に保ちます。 | * 担当者がいない場合、入出荷エリアのドアと窓をすべて施錠します。 * 資産は、ベンダー/運送会社に受け渡すまで施錠した場所で保管します。 |
| PS-17.3 | 施設から出荷する資産は、有効なワークオーダー/出荷オーダーと照らし合わせて確認します。 | * 運送会社と配達担当者に有効なIDを依頼し、該当するワークオーダーに対して受取人を認証します。 * 出荷個数が送り状と一致していることを確認します。 * 荷物の差や傷をただちに報告します。 |
| PS-17.4 | 出荷 | 運送会社や宅配業者が施設のコンテンツ/制作エリアに入ることを禁じます。 | * コンテンツ/制作エリアへのアクセスが必要な場合は、施設の担当者が同伴します。 |
| PS-17.5 | ドラックドライバー用に別のログ記録をとり、保持します。 | * すべてのドラックドライバーをログに記録し、次の情報も記載します。 * 氏名 * トラクターやトレーラーのナンバープレート番号 * 所属会社 * 受取り日時 * 取り扱ったコンテンツ |
| PS-17.6 | 出荷前には、現場でのパッケージングやトレーラーの密封作業を観察・モニターします。 | * トレーラーに荷積みし、密封される間、セキュリティ担当者が始終現場に立ち会います。 |
| PS-17.7 | 施設間の荷物の運送時間、ルート、配達時間を記録、モニター、レビューします。 | * 共通の出荷場所の間で基準となる配達時間を設定し、実際の時間をモニターして差を特定します。 * 大きな差が出たときは、調査し、上部に報告します。 * 休憩場所を承認・指定します。 * 予想外の遅延をモニターし通報するために、リアルタイムのGPSトラッキングシステムの導入を検討します。 |
| PS-17.8 | 顧客のスタジオが認可した目的以外のためにフィルム資材を転送することを禁じます。 |  |
| PS-17.9 | 映画館での公開前に上映する作品は、部分に分けて出荷します（例: 奇数リール、偶数リール）。 |  |
| PS-18.0 | 入荷 | 受取り時に配送された顧客の資産を検査し、送り状（例: 梱包明細書、マニフェストログ）と照らし合わせます。 | * 差異（例: 不足、損傷した**メディア**）を特定し、ログ記録をとります。 * 差異を経営陣、顧客、出荷人に報告します。 |
| PS-18.1 | 入荷 | 配達の受取り時に指定された責任者が記入する受取りログを維持します。 | * これには次の情報を記録します。 * 運送会社/宅配業者の名前と署名 * 受取り人の氏名と署名 * 受取り日時 * 受け取った資産の詳細 |
| PS-18.2 | 次のアクションを速やかに行います。   * 受け取った資産にタグを付ける（例: バーコード、固有のIDを割り当てる） * 資産を**資産管理**システムに入力する * 資産を制限エリア（例: **保管庫**、金庫）に移動する | * すぐにタグ付けや保管庫にいれることができない資産は**ステージングエリア**（例: セキュリティ保護されたケージ）に保存する |
| PS-18.3 | 夜間配達の品を受け取るために、セキュリティ保護された手段を導入します。 | * 配達される品が必要のある人のみが受け取ることができるように、慎重に手配します。 |
| PS-19.0 | ラベル貼り | 顧客から別途指示がある場合を除き、荷物の表面にAKA（「別名」）を含めた作品の情報を表記することは禁止します。 |  |
| PS-20.0 | パッケージング | すべての顧客の資産は容器に入れ、閉じて封印した状態で送付します。また資産の価値に応じ、もしくは顧客の指示があった場合は、施錠付き容器に入れます。 |  |
| PS-20.1 | 少なくとも次のコントロールのうち、一つを実装します。   * 途中で開封されたことが分かるテープ * 途中で開封されたことが分かる梱包 * 開封されたことが分かる封印（例：ホログラムの形態） * セキュリティ保護された入れ物（例: コンビネーションロック付きのペリカンケース） | * 途中で開封された商品の取扱い方に関するプランを制定し伝達します * 途中開封がなされたすべての事象は、インシデント対応チームに報告します（MS-5.0） |
| PS-20.2 | パッケージング | すべての出荷物はコンパクトに梱包します。そして、最終出荷前に包装が十分であることを確認します。 | * バルク出荷をする場合、スピンドルごとに個々の資産（例: スキッド、パレット）をコンパクトに梱包します。 |
| PS-21.0 | 輸送車両 | 自動車やトラックは常に施錠し、荷物は外から見えない場所に置きます。 | * 人がいない時に荷物を置いたままにしてはなりません。 |
| PS-21.1 | 運送車両（例: トレーラー）には次のセキュリティ機能を含めます。   * ドライバーキャビンからの分離 * 貨物室のドアを施錠・密封できること * 重要度の高い荷物の運送にはGPS | * 重要度の高いコンテンツや高価値資産の配達には、GPSのトラッキングシステム付きの車両を使用します |
| PS-21.2 | 重要度の高い作品の運送には、貨物室のドアに番号付きのシールを貼付します。 | * 警備員に、シールを貼り、記録、モニターするよう義務付けます。 * 重要度の高い荷物の場合、追加のセキュリティ手法（例: 施錠/セキュリティ保護された貨物室、施錠したペリカンケース）の導入を検討します。 |
| PS-21.3 | 高リスクエリアへ重要度の高いコンテンツを配送する場合、追加の警備員の護衛を義務付けます。 | * ハイジャック、奇襲、その他の方法による強奪から重要度の高いコンテンツを保護する能力を持つ警備員を雇用します。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| DS-1.0 | ファイヤウォール /WAN /周辺のセキュリティ | 外部ネットワーク/WANは、内部ネットワークへの不正アクセスを防ぐアクセスコントロールリスト、およびアップロードとダウンロードのトラフィックへの対応機能を伴う検査用ファイヤウォールを使って、内部ネットワークと分離させます。 | * 内部ネットワークに、**DMZ**に存在する明白なホスト以外のすべてのトラフィックを拒否するアクセスコントロールリストを用いて**WAN**の**ファイヤウォール**を構成します。 * 内部のコンテンツ/制作ネットワークへの直接のアクセスを禁止する形で、**WAN**ネットワークを構成します。 * 外部との接点をもつすべてのデバイスへ向けた、またはそこからの接続回数を正確に示し説明する、詳細なWAN記録を含めます。 * ファイヤウォールの規則は、すべてのトラフィックおよび設定の変更についてのログを作成するよう設定されなければなりません。またログは、少なくとも月に一度検査する必要があります。 * ファイヤウォールは、抗ウィルスと侵入検出の更新を定期的に行うサービスを使い、更新は少なくとも週に一度実施する必要があります。 * 次のようなファイヤウォールの設定を導入することを検討してください。 * なりすまし対策フィルター * ルーティング不可能なIPアドレスをブロックする * 外部ポートで内部アドレスをブロックする * UDPおよびICMPエコーの要請をブロックする * 使用されていないポートおよびサービスをブロックする * 許可されていないDNSゾーンへの転送をブロックする * 外向けトラフィックが内部アドレスからのものに限定されるよう、出口フィルターを設ける |

|  |  |  |  |
| --- | --- | --- | --- |
| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| DS-1.1 | ファイヤウォール /WAN /周辺のセキュリティ | ファイヤウォールのアクセスコントロールリスト（**ACL**）をレビューするプロセスを作成し、6ヶ月に一度、構成の設定がビジネスに適切で、かつ必要であることを確認します。 | * ファイヤウォールやルーターから**ACL**をエクスポートします。 * **ACL**をレビューして、ネットワークアクセスが適切であることを確認します。 * レビュー、およびファイヤウォールに関するあらゆる規則の変更には、経営陣からの署名による承認を義務付けます。 * それに応じて**ACL**を更新します。 |
| DS-1.2 | WANとファイヤウォールへのアクセスは、デフォルトですべてのプロトコルを拒否し、特定の許可されているセキュリティ保護されているプロトコルのみを有効にします。 | * **Telnet**や**FTP**などの暗号化されていない通信プロトコルをすべて制限します。 * 暗号化されていないプロトコルを、暗号化されているプロトコルに置き換えます。 |
| DS-1.3 | **DMZ**内に外部アクセスサーバー（例: ウェブサーバー）を設置します。 | * **DMZ**内のサーバーをアイソレートし、サーバー（例: ウェブサーバーなど）ごとに1タイプのサービスのみを提供するようにします。 * **ACL**を実行し、**DMZ**からの内部ネットワークへのアクセスを制限します。 |
| DS-1.4 | ネットワークインフラデバイス（例: ファイヤウォール、ルーター、スイッチなど）SAN/NAS（ストレージエリアのネットワークおよびネットワークに付属するストレージ） 、サーバーをパッチするプロセスを導入します。 | * ネットワークインフラデバイス、SAN/NAS、サーバーを対象とするにパッチを特定、評価、テストするプロセスを定期的に（例：毎月一度）実行します。 * ネットワークインフラデバイス、SAN/NAS、サーバーを、重大なセキュリティの脆弱性の問題に対応するレベルに更新します。 * 重要なパッチは48時間以内に対応します。 * 中央で一括管理するパッチ管理システムの設置を検討します。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| DS-1.5 | ファイヤウォール /WAN /周辺のセキュリティ | セキュリティ設定標準に基づいて、ネットワークインフラデバイス、SAN/NAS、サーバーをハードニングします。SNMP（簡易ネットワーク管理プロトコル）は、使用されていない場合、もしくはSNMPv3かそれ以上のみが使われている場合は無効化し、強力なパスワードのSNMPコミュニティ・ストリングを選択します。 | * 次のハードニングのオプションを検討します。 * ゲストアカウントと共有を無効化する * 抗ウィルス/抗マルウェアをインストールする * ソフトウェアファイヤウォールを有効化する * 不要なソフトウェアを削除する * 不要なサービスをアンインストール/無効化する * すべてのユーザーが制限対象ユーザーとして使用することを義務付ける * 権限を与えられた管理システムのみがSNMPを使って接続できるよう、デバイスへのアクセスを制限する**ACL**を使用する * 次に挙げる、ネットワークインフラデバイスをハードニングする際のセキュリティハードニング標準を参照してください。 * NIST * SANS * NSA |
| DS-1.6 | いかなる外部インターフェースからも、ファイヤウォールのリモート管理を許可してはなりません。 | * リモート管理機能を使う場合は、その代わりに二つの要素を含む認証と、 128ビット以上の高度暗号化基準（AES）によるVPN接続を使います * 管理以外のリモートアクセスについては、各個人に次の2つの提供を義務付けます。 * 個人が知っている情報（例: ユーザー名、パスワード） * 個人が持っている固有の物理的アイテム（例: トークン、**キーカード、**スマートフォン、証明書） * 各人ごとに異なる固有の身体的特徴/バイオメトリクス（例: 指紋、網膜） |
| DS-1.7 | ファイヤウォール /WAN /周辺のセキュリティ | ネットワークインフラ/SAN/NASデバイスおよびサーバーのバックアップは、内部ネットワークのセキュリティ保護されている集中サーバーに安全に保存します。 | * ネットワークインフラデバイスを設定し、構成ファイルのバックアップを、セキュリティ保護された方法で（例：暗号化）内部ネットワークのロケーションに保存します。 * 保管場所および暗号化されたバックアップへは、必ず認可管理者のみがアクセスできるようにします。 * Trivial File Transfer Protocol（TFTP）がバックアップ用に使用された場合、容赦ない攻撃や不正なアクセスを緩和する制限が設けられていることを確認します。 |
| DS-1.8 | 少なくとも四半期に一度、すべての外部IPレンジとホストの脆弱性スキャンを行い、問題を是正します。 | * コンテンツへの不正アクセスを可能にする重大な問題は、即座に是正します。 * スキャン/テストに使用されるツールは、バーチャル技術が使われている場合には、必ずそれに対応するようにします。 * サードパーティを使ってこれを実施することを検討します。 |
| DS-1.9 | 少なくとも一年に一度、すべての外部IPレンジとホストの侵入テストを行い、問題を是正します。 | * コンテンツへの不正アクセスを可能にする重大な問題は、即座に是正します。 * スキャン/テストに使用されるツールは、バーチャル技術が使われている場合には、必ずそれに対応するようにします。 * サードパーティを使ってこれを実施することを検討します。 |
| DS-1.10 | ポイントからポイントへの接続は、専用のプライベート接続と暗号化を使い安全に保護します。 | * 暗号化には、128ビット以上の高度暗号化基準（AES）を使います。 |
| DS-1.11 | すべてのシステムが共通の時間レファレンスを有するよう、同期化された時間サービスプロトコル（例：ネットワーク時間プロトコル）を導入します。 | * システムが、必ず正確かつ一貫性のある時間を有するようにします。 * 時間データは、必ず保護されるようにします。 * 時間設定は、必ず業界で認められた時間ソースから得たものとします。 |
| DS-1.12 | ファイヤウォール /WAN /周辺のセキュリティ | WANネットワークインフラデバイスとサービスについて、ベースラインとなるセキュリティ要件を制定、文書化、導入します。 | * 脆弱性の原因となりかねないシステム上の欠陥は、制作で使われる前に必ず修正するようにします。 * セキュリティベースラインに対するインフラの準拠状況を報告するため、継続的にモニターすることを検討します。 |
| DS-2.0 | インターネット | Eメールを含め、インターネットに直接アクセスするところから送られたデジタルコンテンツを処理または保管する制作ネットワークとすべてのシステムを禁止します。仕事上、デジタルコンテンツを処理または保管する制作ネットワークもしくはシステムからインターネットへのアクセスが必要な場合は、リモートホストされたアプリケーション/デスクトップセッション経由で、承認された方法のみで行うことが許可されます。 | * インターネットゲートウェイシステム（例: Citrix、Terminal Services、VNCなど）を使用して例外を処理します。その際、次に挙げるコントロールが適用されます。 * システムが厳正にコントロールされており、ウェブブラウジングがサーバーの唯一の機能です。 * 制限されているサイトへのアクセスは禁止されています。これには、ウェブベースのEメールサイト、P2P、デジタルロッカー、その他の既知の悪意のあるサイトが含まれます。 * システムから、またはシステムへコンテンツを転送することを禁じます。 * 最新ウィルスの定義を用いて、システムを定期的にパッチ・更新します。 * システムのアクティビティを定期的にレビューします。 * 制作ネットワークは、ローカルドライブのマッピング、USB大量ストレージ、プリンターのマッピング、コピー＆ペースト機能、インターネットのゲートウェイシステムへのダウンロード/アップロードからブロックします。 * **ファイヤウォール**の**規則**を実践し、デフォルトではすべてのアウトバウンドのトラフィックを拒否し、抗ウィルス定義サーバー、バッチサーバー、ライセンスサーバー（ローカルでのライセンスが利用できない場合のみ）などの指定された内部ネットワークへのアウトバウンド転送を要求する特定のシステムとポートのみを明白に許可します。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| DS-2.1 | インターネット | **制作以外のネットワーク**から、以下のアイテムをブロックするEメールフィルタリングソフトウェアまたはアプライアンスを導入します。   * フィッシングの可能性を持つEメール * 禁じられている添付ファイル（例: ビジュアルベーシックのスクリプト、実行可能ファイルなど） * ファイルサイズは10MBに制限 * マルウェアまたはウィルスの源であることが知られているドメイン | * Eメールの添付ファイルとEメールの本文メッセージの中で、制限されているコンテンツタイプを特定します。 * Eメールのフィルタリングソリューションを実装し、制限されているコンテンツタイプに基づいて設定します。 |
| DS-2.2 | P2Pファイルのトレーディング、ウィルス、ハッキング、その他の悪意のあるサイトとして知られるウェブサイトへのアクセスを制限するウェブフィルタリングソフトウェアまたはアプライアンスを実行します。 | * 悪意のあるサイトを検知し、アクセスを妨げるために、ウェブフィルタリング/プロキシサーバーソフトウェアを実行します。 |
| DS-3.0 | LAN /内部ネットワーク | **コンテンツ/制作ネットワーク**を**制作以外のネットワーク**（例: オフィスネットワーク、**DMZ**インターネットなど）から隔離します。これには、物理的ネットワークと論理ネットワークのセグメンテーションを使用します。 | * アクセスを要求する特定のホストからの**コンテンツ/制作ネットワーク**へのアクセス（例: 抗ウィルスサーバー、パッチ管理サーバー、コンテンツデリバリーサーバーなど）を明白に許可するアクセスコントロールリストを定義します。 * **アクセスコントロールリスト**に、アクセスを許可する明白に定義されたポートとサービスを含めます。 * 定義されたセキュリティゾーンに基づいて、ネットワークをセグメント化または隔離します。 * **ファイヤウォールの規則**を実践し、デフォルトではすべてのアウトバウンドのトラフィックを拒否し、抗ウィルス定義サーバー、バッチサーバー、ライセンスサーバー（ローカルでのライセンスサーバーが利用できない場合のみ）などの指定された内部ネットワークへのアウトバウンド送信を要求する特定のシステムとポートのみを明白に許可します。 * **ファイヤウォールの規則**を 実践し デフォルトではすべてのインバウンドのトラフィックを拒否し、指定されたコンテンツデリバリー用サーバーからのインバウンド送信を要求する特定のシステムとポートのみを明白に許可します。 * 制作環境でのインターネットへのアクセスに関するガイダンスは、DS-2.0を参照してください。 * **スイッチ**上のMACアドレスによって、**静的IPアドレス**を割り当てます。 * **コンテンツ/制作ネットワーク**上で**DHCP**を無効にします。 * どの制作コンピュータシステムも、一度に複数のネットワークと接続することを禁止します。 * コンテンツが制作以外のネットワークで使用される、もしくはそこに保存されることを禁止します。 |
| DS-3.1 | コンテンツ/制作システムへのアクセスを権限を持つ関係者のみに制限します。 | * ネットワークケーブルが代替/承認されていないデバイスに決して接続できないようにするため、物理的イーサネットケーブルロックを使用することを検討します。 |
| DS-3.2 | LAN /内部ネットワーク | **コンテンツ/制作ネットワーク**へのリモートアクセスを、職務上の責任を果たすためにアクセスが必要な承認された関係者のみに制限します。 | * コンテンツ/制作ネットワークへのリモートアクセスを禁止します。 * **コンテンツ/制作ネットワーク**へのリモートアクセスが許可されている**従業員**のリストを維持します。 * 経営陣が、**コンテンツ/制作ネットワーク**上に存在するシステムへのモニターアクセスで、リモートのアクティビティをレビューするためのプロセスを開発します。 * 個々のアカウントを使用するために、リモートアクセスシステムを設定します。 * アクセスコントロールリストを使用してリモートアクセスを1つの手法のみに制限します。 * 緊急リモートアクセスが必要な場合には、次のことを実行します。 * できれば証明書に基づく2つの要素を含む認証を使う * FTP、 SSH、 IRC、 IMを含むファイル転送プロトコルをブロックする * **VPN**設定では、スプリットトンネルを許可しない * 制作ネットワークへ接続するためには、Launchpad/bastion（踏み台）のホストモデルを仲介として活用する |
| DS-3.3 | スイッチ/レイヤー3のデバイスを使いネットワークトラフィックを管理し、**コンテンツ/制作ネットワーク**上の使用していない**スイッチ**ポートをすべて無効化し、不正デバイスによるパケット盗聴を防止します。 | * デバイス管理者には、次を含む強力な認証を使うことを義務付けます。 * 暗号化されたプロトコルを使う * パスワードは巧みな寄せ集めにする * 実行コマンドのパスワードを別にする * デバイスコンソールを接続し、設定ファイルを更新して、非使用の**スイッチ**ポートを無効化します。 * スイッチ/レイヤー3デバイスへのロギングを有効化します。 |
| DS-3.4 | **コンテンツ/制作ネットワーク**上のハブやリピーターなどの非スイッチ型デバイスの使用を制限します。 | * すべてのハブ/リピートを**スイッチ**またはLayer 3のデバイスと取り替えます。 |
| DS-3.5 | LAN /内部ネットワーク | **コンテンツ/制作ネットワーク**内のコンピュータシステムへのデュアルホームネットワーク（物理的なネットワークブリッジング）を禁じます。 | * ネットワークレイヤー（例: **ルーター**、**ファイヤウォール**、**スイッチ**など）での論理的ネットワークブリッジングを、一つのコンピュータシステムにおける**複数NIC**を使用する代わりに行います。 |
| DS-3.6 | **コンテンツ/制作ネットワーク**上で、ネットワークベースの侵入検知または防止システム（**IDS/IPS**）を実装します。 | * ネットワークベースの侵入検知または防止システムを設定し、疑わしいネットワークのアクティビティをアラートまたは防止します。 * **IDS/IPS**のために、抗ウィルス/抗マルウェアの定期サービスを購入します。 * 少なくとも毎週一度、 **IDS/IPS**上で攻撃シグネチャ/ポリシーと抗ウィルス/抗マルウェアを更新します。 * **IDS/IPS**でのすべてのアクティビティと設定変更を記録します。 * すべてのワークステーションに、ホストベースの侵入検知システムソフトウェアを実装します。 |
| DS-3.7 | SNMP（簡易ネットワーク管理プロトコル）は、使用されていない場合、もしくはSNMPv3かそれ以上のみが使われている場合は無効化し、強力なパスワードのSNMPコミュニティ・ストリングを選択します。 | * 権限を与えられた管理システムのみがSNMPを使って接続できるよう、デバイスへのアクセスを制限する**ACL**を使用する |
| DS-3.8 | システムは、**LAN /内部ネットワーク**に設置する前にハードニングします。 | * DS-1.5で提案事項を参照してください |
| DS-3.9 | 少なくとも年に一度、内部ネットワークの脆弱性スキャンを実施し、問題があれば是正します。 | * スキャンに使用されるツールは、バーチャル技術が使われている場合には、必ずそれに対応するようにします。 * 以下が含まれます。 * 制作ネットワーク * 制作以外のネットワーク * 接続された機械/デバイス * 接続されていない機械/デバイス |
| DS-3.10 | LAN /内部ネットワーク | LANのSAN/NAS、デバイスおよびサーバーとワークステーションのバックアップは、内部ネットワークのセキュリティ保護されている集中サーバーに安全な状態で保存します。 | * LANデバイスを設定し、構成ファイルのバックアップを内部ネットワークに安全な方法（例：暗号化）で保存します。 * 保管場所および暗号化されたバックアップへは、必ず認可管理者のみがアクセスできるようにします。 |
| DS-4.0 | ワイヤレス/WLAN | **コンテンツ/制作ネットワーク**上で、ワイヤレスネットワークおよびワイヤレスデバイスの使用を禁じます。 | * ワイヤレスゲストネットワークをインターネットのみにアクセスし、**コンテンツ/制作ネットワーク**にはアクセスしないよう制限します。 * コンテンツ/制作ネットワークでコンテンツを処理または保存するワークステーション/ラップトップ上のワイヤレスアクセス機能は、削除または無効化します。 |
| DS-4.1 | ワイヤレス/WLAN | **制作以外**のワイヤレスネットワーク（例: 管理事務所、ゲスト）を、次のセキュリティコントロールを用いて構成します。   * WEP / WPAを無効化する * **AES**128**暗号化（WPA2）、**またはそれ以上のみを有効化する * 「ゲスト」ネットワークを会社の他のネットワークから隔離する * 管理者用ログオン証明書のデフォルトを変更する * デフォルトのネットワーク名を変更する（**SSID**） | * 次のようなセキュリティコントロールを考慮してください。 * 会社固有ではない**SSID**名を使う * オプションが利用可能な場合は、IEEE 802.1XまたはIEEE 802.11iを有効化する * オプションが利用可能な場合は、RADIUS認証を使用する * **MACアドレスフィルタリング**を有効化する * 制作ワークステーションとデバイスのワイヤレスMACアドレスをブラックリストに載せる * ワイヤレスアクセスポイント/コントロールを設定し、必要なレンジ内でのみブロードキャストします。 * ワイヤレスネットワーキングのための802.1Xフレームワークを実装します。これには次のアイテムが含まれます。 * RADIUS（Remote Access Dial In User Service）による認証、承認、確認 * LDAP（Lightweight Directory Access Protocol）サーバーによるユーザーアカウントの管理 * パブリックキーインフラによるクライアントおよびサーバー証明書の生成と管理 * 事前共有キーの使用が必要な場合、次のコントロールを実装します。 * CCMP（**AES-128**）**暗号化**かそれ以上を用いてWPA2を設定 * 複雑なパスフレーズを設定（推奨される複雑なパスフレーズについてはDS-8.1を参照してください） * パスフレーズを少なくとも90日ごと、および主要な**従業員**が離職した際に変更 |
| DS-4.2 | ワイヤレス/WLAN | 不正ワイヤレスアクセスポイントを発見するためのスキャンプロセスを実施し、確認された問題是正します。 | * 保護されていないワイヤレスアクセスポイントを発見するために、少なくとも四半期に一度、施設をローミング・スキャンするプロセスを実施します。 * 集中型ワイヤレスアクセスソリューション（ワイヤレスコントローラ）を設定し、可能な限り、不正ワイヤレスアクセスポイントを検知し次第、管理者にアラートします。 |
| DS-5.0 | I/Oデバイスセキュリティ | コンテンツの入出力（I/O）として使用するために、特定のシステムを指定します。 | * **ACL**を実行し、**コンテンツ/制作ネットワーク**と特定のソース/ディスティネーション**IPアドレス**用のI/Oとして使用されるシステムの間でトラフィックを許可します。 |
| DS-5.1 | 入出力（I/O） 、大量ストレージ、 外付けストレージ、モバイルストレージデバイス（ 例：**USB**、 **ファイヤウォール**、 サンダーボルト、 SATA、**SCSI**など） および 光学媒体バーナー（例：DVD、Blu-Ray、CDなど）を、コンテンツを取扱い・保存するすべてのシステム上でブロックします。ただし、コンテンツI/Oのために使用されるシステムは例外とします。 | * **I/O デバイス**をブロックするために次の方策を考慮してください。 * 登録設定を変更し、MS Windowsベースのシステムでは**I/Oデバイス**へのライトアクセスを制限します。 * 大量ストレージファイルを削除して、Macベースのシステムのプロダクションステーション上でのライトアクセスを制限します。 * Microsoft Active DirectoryまたはApple Open Directoryを使用するシステム用のグループポリシーを使用して、**I/Oデバイス**を無効化します。 * 出力デバイスのブロックが不可能な場合、I/Oポートモニタリングソフトウェアを使用してポート使用状況を検知します。 |
| DS-6.0 | システムセキュリティ | 抗ウィルスと抗マルウェアのソフトウェアを、すべてのワークステーション、サーバー、およびSAN/NASシステムに接続するあらゆるデバイスの上にインストールします。 | * 集中管理コンソールを持つエンタープライズ抗ウィルスソリューションをインストールします。 * エンドポイント保護のインストールを検討します。 |
| DS-6.1 | すべての抗ウィルスと抗マルウェアの定義を、毎日一度またはそれ以上の頻度で更新します。 | * 集中型抗ウィルスと抗マルウェア管理コンソールを設定し、少なくとも毎日一度は定義更新をダウンロードまたはプッシュします。 |
| DS-6.2 | ウィルスとマルウェアが**コンテンツ/制作ネットワーク**に侵入する前に、すべてのコンテンツをスキャンします。 | * **コンテンツ/制作ネットワーク**にコネクトしていないシステム上でスキャンを実行します。 |
| DS-6.3 | システムセキュリティ | 以下のようにスキャンを行います。   * すべてのワークステーションで、全システムを対象とするウィルスおよびマルウェアのスキャンを定期的に有効化します * サーバーとSAN/NASに接続するシステムについて、全システムを対象とするウィルスとマルウェアのスキャンを有効化します | * 抗ウィルスと抗マルウェアソフトウェアを設定し、抗ウィルスと抗マルウェア戦略に基づいて全システムのスキャンを行います * 抗ウィルスと抗マルウェアソフトウェアを設定し、アイドル期間に実行します |
| DS-6.4 | セキュリティの脆弱性を是正するパッチ/アップデートを用いて、システム（例: ファイル転送システム、オペレーティングシステム、データベース、アプリケーション、ネットワークデバイス）を定期的に更新するプロセスを実施します。 | * 可能な場合、集中型パッチ管理ツール（例: WSUS、Shavlik、Altiris）を実装して、すべてのシステムに対してパッチを自動的に配備します。 * ベンダーとその他のサードパーティによるパッチを検討します。 * パッチは配備の前にテストします。 * システムにパッチを使用しないビジネス上の合理的な理由がある場合は、例外プロセスと補足コントロールを実装します。 |
| DS-6.5 | ユーザーが自分のワークステーションの管理者となることを禁止します。ただし、ソフトウェアで必要な場合（例：ProTools、ClipsterおよびBlu-Print、Scenarist、Toshibaなどのオーサリングソフトウェア）を除きます。ソフトウェア提供者からの文書には、管理権が必要である旨を明確に記載しなければなりません。 | * ワークステーションのログインに使用されるユーザーアカウントには、システムの管理者としての権利がないことを確認します。 |
| DS-6.6 | コンテンツを扱う携帯用のコンピューティングデバイス（例: ラップトップ、タブレット、タワー）を置いたまま席を外す場合、ケーブルロックを使用します。 | * ケーブルロックを固定物体（例: テーブル）にしっかりとつなぎます。 |
| DS-6.7 | システムセキュリティ | 顧客のプロジェクトに関連するコンテンツまたは重要な情報を含むラップトップと携帯用のコンピューティング ストレージデバイスについては、追加的なセキュリティコントロールを導入します。すべてのラップトップを暗号化します。ハードウフェアで暗号化された携帯用のコンピューティング ストレージデバイスを使います。コンテンツを扱うすべてのラップトップ/モバイルデバイスにリモートキル ソフトウェアをインストールし、ハードデバイスとその他のストレージデバイスのリモートワイピングを可能にします。 | * セキュリティ保護されていない場所で使わねばならない場合は、ラップトップにプライバシースクリーンを付けます * ラップトップを公共のワイヤレスの場所に接続してはなりません * 使用していない時には、ラップトップの電源を切ります。「スリープ」や「冬眠」モードにしてはなりません。 |
| DS-6.8 | ソフトウェアをインストールする権限は、IT管理者に限定します。 | * 不正ソフトウェア（例: 違法ソフトウェア、悪意のあるソフトウェア）を含む未承認ソフトウェアのインストールと使用を禁じます。 * 少なくとも四半期に一度、インストールしたアプリケーションの目録を作るため、すべてのシステムをスキャンします。 |
| DS-6.9 | システムを社内で設定する場合（例: ラップトップ、ワークステーション、サーバー、SAN/NAS）は、セキュリティベースラインと標準を実装して、システムを構成します。 | * すべてのシステムに適用するためのセキュリティ保護された標準を作成します。 |
| DS-6.10 | 不要なサービスやアプリケーションをコンテンツ転送サーバーからアンインストールします。 | * すべてのコンテンツ転送サーバーにあるインストールされたサービス（例：services. MSc）のリストをレビューし、必要のないものはアンインストール、または無効化します。 * すべてのコンテンツ転送サーバーにインストールされているアプリケーションのリストをレビューし、不要なものをアンインストールます。 * スタートアップアプリケーションのリストをレビューし、すべての重要ではないアプリケーションが実行されていないことを確認します。 |
| DS-6.11 | システムおよびシステムの構成要素の目録を維持します。 | * 少なくとも月に一度の頻度で目録を更新します。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| DS-6.12 | システムセキュリティ | 年に一度、またはインフラに重要な変更があった場合にネットワークのトポロジーを文書化し、図を更新します。 | * WAN、DMZ、LAN、WLAN（ワイヤレス）、VLAN、ファイヤウォール、サーバー/ネットワークのトポロジーを含みます。 |
| DS-7.0 | 顧客管理 | コンテンツを扱うすべての**情報システム**とアプリケーションに関連して、管理者、ユーザー、サービスアカウント用のアカウント管理プロセスを作成・実行します。 | * 次の項目に対応するアカウント管理のポリシーと手順を文書化します。 * 新規ユーザーリクエスト * ユーザーアクセスの変更 * ユーザーアカウントの無効化と有効化 * ユーザーの終了 * アカウント期限 * 休職 * 複数のユーザーがユーザーアカウントを共有することを禁止します。 * サービスアカウントの使用を、それを必要とするアプリケーションのみに制限します。 * 少なくとも、次に挙げるインフラシステムとデバイスへのロギングを有効化します。 * インフラのコンポーネント（例: **ファイヤウォール**、認証サーバー、ネットワークオペレーティングシステム、**VPN**を含むリモートアクセスメカニズム） * プロダクションオペレーティングシステム * コンテンツ管理のコンポーネント（例: ストレージデバイス、コンテンツサーバー、コンテンツストレージツール、コンテンツ転送ツール） * インターネットアクセス可能なシステム * 中央保管場所にログを管理するサーバー（例: syslog/ログ管理サーバー、Security Information and Event Management (**SIEM**)ツール）を設置します。 |
| DS-7.1 | 顧客管理 | アカウント管理活動のトレース可能な証拠（例: 承認のEメール、変更リクエストフォーム）を維持します。 | * 可能な限り、すべてのアカウント管理活動に関連して、マネージャーによる承認および関連するアクションの証拠を維持します。 |
| DS-7.2 | 必ず必要な関係者にのみ権限を与えるという原則に基づき、知る必要性を持つ人だけに固有の証明書を割り当てます。 | * 少なくとも次に挙げる**情報システム**に関して、知る必要性を持つ人だけに固有の証明書を発行します。 * プロダクションシステム * コンテンツ管理ツール * コンテンツ**転送ツール** * ネットワークインフラデバイス * ロギング&モニタリングシステム * クライアントウェブポータル * アカウント管理システム（例: Active Directory、Open Directory、LDAP） * どうしても必要な場合にのみ与えられるべき**VPN**リモート許可 |
| DS-7.3 | デフォルトの管理者アカウント、およびその他のデフォルトのアカウントの名前を変更し、これらのアカウントの使用は証明書が必要な特殊な状況（例: オペレーティングシステムの更新、パッチのインストール、ソフトウェアの更新）のみに制限します。 | * すべてのデフォルトアカウントを特定するために、すべてのハードウェアとソフトウェアのマニュアルを参照します。 * すべてのデフォルトアカウントのパスワードを変更します。 * 可能な限り、各アカウントのユーザー名も変更します。 * 非使用時には、管理者のアカウントを無効化します。 |
| DS-7.4 | 情報システムへのアクセスを割り当てる責任者が自らそれらのシステムのエンドユーザーとはならないように、職務を分割します（自分自身にアクセスを割り当てる権限は誰にも与えてはなりません）。 | * 可能な場合、情報システムへのアクセスを許可する独立チームのサービスを利用します。 * 分割ができない場合は、次のような補足コントロールを実装します。 * 従業員とサードパーティの従業員の活動をモニターする * 監査ログを維持およびレビューする * 物理的分割を実施する * 経営陣による監督を実施する |
| DS-7.5 | 顧客管理 | 管理者とサービスアカウントの活動をモニター・監査します。 | * ロギングをサポートするシステムとアプリケーションを対象としてモニタリングコントロールを有効化します。 * 管理者の活動をログ記録し、少なくとも次の情報を記録するようにシステムとアプリケーションを設定します。 * ユーザー名 * タイムスタンプ * アクション * 追加情報（アクションのパラメータ） * サービスアカウントをモニターし、意図された目的（例: データベースクエリー、アプリケーション間の通信）にのみ使用されていることを確認します。 * 毎月管理者とサービスアカウントをレビューするプロセスを実施し、通常と異なる疑わしい動きを特定して、不正使用の可能性を調査します。 |
| DS-7.6 | すべてのコンテンツを取扱う**情報システム**でユーザーアクセスをレビューするプロセスを実施し、四半期に一度アクセスが不要になったユーザーアカウントを削除します。 | * **従業員**や**サードパーティの従業員**の異動や離職によってアクセスが不要となった場合、ユーザーから**情報システム**への**アクセス権**を削除します。 * 90日以上使用されていないアカウントは削除または無効化します。 |
| DS-7.7 | プロジェクトベースでコンテンツへのユーザーアクセスを制限します。 | * プロジェクトが完了してアクセスが不要になったユーザーから、**情報システム**への**アクセス権**を削除します。 |
| DS-7.8 | 顧客管理 | 技術的に可能な限り、コンテンツを扱うシステム上のローカルアカウントは無効化または削除します。 | * 集中型アカウント管理サーバー（例: LDAP、Active Directory）を設置し、**情報システム**へのユーザーアクセスを認証します。 * ネットワークインフラデバイスとしては、アカウント管理用のAuthentication, Authorization, and Accounting（AAA）を設置します。 * ゲストアカウントを無効化します。 * ローカルアカウントを使う必要がある場合、可能な限り、各デフォルトのアカウントについてユーザー名とパスワードを変更し、ローカルアカウントを使ってネットワーク経由でシステムにログインする機能を無効化します。 |
| DS-8.0 | 認証 | **情報システム**にアクセスするために、**固有のユーザー名**とパスワードの使用を徹底させます。 | * すべての**情報システム**を対象として、**固有のユーザー名**とパスワードの使用を実施するプロセスを作成します。 * 少なくとも**固有のユーザー名**とパスワードを使用した認証を要求するように**情報システム**を設定します。 |
| DS-8.1 | **情報システム**へのアクセスを取得するために、強力なパスワード使用のポリシーを徹底させます。 | * 次の条件をそろえたパスワードポリシーを作成します。 * 最低文字数が8文字 * 大文字、小文字、数字、記号の中から少なくとも3種類を使用 * パスワードの最長保持期間は90日 * パスワードの最短保持期間は1日 * 無効なログオンの試みの最大回数は3～5回 * 無効なログインを試みた後にロックされたユーザーアカウントは、手動でロック解除されなければなりません。一定時間が経過した後に、自動的にロック解除してはなりません。 * 過去10個のパスワードの履歴 |
| DS-8.2 | 認証 | ネットワークへのリモートアクセス（例: **VPN**）には、2つの要素を使った認証（例: ユーザー名/パスワードおよびハードトークン）を実施します。 | * 各個人に、リモートアクセスのために次の2つの提供を義務付けます。 * 個人が知っている情報（例: ユーザー名、パスワード） * 個人が持っている固有の物理的アイテム（例: トークン、**キーカード、**スマートフォン、証明書） * 各人ごとに異なる固有の身体的特徴/バイオメトリクス（例: 指紋、網膜） * 遠隔管理機能を使う場合は、二つの要素を含む認証と、128ビット以上の高度暗号化基準（AES）によるVPN接続を使います |
| DS-8.3 | パスワード保護のスクリーンセーバーまたはスクリーンロックソフトウェアを、サーバーとワークステーションに実装します。 | * サーバーとワークステーションを手動またはポリシー（Active Directoryグループポリシーなど）を介して設定し、10分間活動のない状態を続けてから、パスワード保護のスクリーンセーバーをアクティベートします。 |
| DS-8.4 | WANおよびLAN /内部ネットワークへのアクセスにおいて階層化された認証戦略を実現するために、追加的な認証メカニズムを導入することを検討します。 | * 次のうちの1つ以上の認証メカニズムの追加を検討します。 * 複数要素の認証 * 身分証明とアクセス管理システム * シングルサインオンのシステム * IDフェデレーション基準 |
| DS-9.0 | ロギングとモニタリング | リアルタイムロギング・レポーティングシステムを実装し、セキュリティイベントを記録・報告し、少なくとも次の情報を集めます。   * いつ（タイムスタンプ） * どこ（ソース） * 誰（ユーザー名） * 何（コンテンツ） | * 少なくとも、次に挙げるインフラシステムとデバイスへのロギングを有効化します。 * インフラのコンポーネント（例: **ファイヤウォール**、認証サーバー、ネットワークオペレーティングシステム、リモートアクセスメカニズム（例：**VPN**システム） * プロダクションオペレーティングシステム * コンテンツ管理のコンポーネント（例: ストレージデバイス、コンテンツサーバー、コンテンツストレージツール、コンテンツ転送ツール） * インターネットアクセス可能なシステム * アプリケーション |
| DS-9.1 | 中央保管場所にログを管理するサーバー（例: syslog/ログ管理サーバー、Security Information and Event Management (**SIEM**)ツール）を設置します。 |  |
| DS-9.2 | インシデントにアクティブレスポンスで対応するために、セキュリティイベントが検知され次第、自動通知を送付するロギングシステムを考慮してください。 | * 調査が必要なイベントを定義し、自動通知メカニズムが担当者に通知を送付することを可能にします。その際、次に挙げる事項を考慮します。 * 成功と失敗を含む、**コンテンツ/制作ネットワーク**へのアクセスの試み * コンテンツの転送で、ファイルサイズと一日の中の時間が通常と異なる * 未認可のファイルアクセスの試みを繰り返している * 特権的エスカレーションでの試み * 中央保管場所にログを集積するサーバー（例: syslog/ログ管理サーバー、Security Information and Event Management (**SIEM**) ツール）を設置します。 |
| DS-9.3 | ロギング・レポーティングシステムによって報告された通常と異なる活動を調査します。 | * 検知されたセキュリティイベントの取り扱うために、**インシデント対応**手順を導入します。 |
| DS-9.4 | ロギングとモニタリング | 次の機能を果たす、すべてのシステムにロギングメカニズムを実装します。   * キーの生成 * **キー管理** * ベンダー証明書管理 | * すべての生成されたキーと追加された証明書がトレース可能で、ユーザーが判別できることを確実にします。 |
| DS-9.4 | すべてのログを週に一度レビューし、すべての重要度が高いものについては毎日一回レビューします。 | * 重大なセキュリティインシデントを示す可能性がある通常と異なる活動を調査します。 * 現在アラートの対象となっていない通常と異なるイベントを追加的に特定し、これらのイベントでアラートが送付されるようにロギング・レポーティングシステムを設定します。 * 異なるシステムからのログを照合して、通常と異なる活動のパターンを特定します。 * ログのレビュー結果に基づき、必要に応じて**SIEM**の設定を更新します。 |
| DS-9.5 | 社内・社外のコンテンツの動きをロギングできるようにし、そこには少なくとも次の情報を含めます。   * ユーザー名 * タイムスタンプ * ファイル名 * 送信元**IPアドレス** * 送信先**IPアドレス** * イベント（例: ダウンロード、表示） |  |
| DS-9.6 | ロギングとモニタリング | ログは、少なくとも一年間保存します。 | * 弁護士に相談して、ログの保持に関して規制があるかどうかを確認します。 * 集中サーバーにコンテンツのログを保存します。これは特別なユーザーのみがアクセスでき、アクセスコントロール付きの部屋に安全に保管されます。 |
| DS-9.7 | ログへのアクセスは適切な関係者のみに制限します。 | * アクセスコントロールリストを維持し、ログモニタリングとレビューの責任者のみにログを閲覧できる許可を与えます。 * 各個人が自分自身の活動をモニターする責任者とならないよう、職務を分割します。 * ログファイルに適切な**アクセス権**を適用することにより、ログを不正な削除や変更から保護します。 |
| DS-10.0 | モバイルセキュリティ | コンテンツにアクセスする、またはそれを保存するモバイルデバイスについて、BYOD（自前のデバイス使用）ポリシーを策定します。 | * 次のような、モバイルデバイスの抗ウィルス/抗マルウェア保護の実施を検討します。 * 定義の更新 * 毎日一回のスキャン実施 |
| DS-10.1 | コンテンツにアクセスする、またはそれを保存するモバイルデバイスについて、承認されたアプリケーション、アプリケーションストア、およびアプリケーションプラグイン/拡張子のリストを作成します。 | * 承認されていないアプリケーション、または事前承認されたアプリケーションストア以外から入手した承認されたアプリケーションのインストールは禁止されます。 * モバイルデバイスの管理システムを検討します。 |
| DS-10.2 | コンテンツにアクセスする、またはそれを保存するすべてのモバイルデバイスの目録を維持します。 | * それには、オペレーティングシステム、パッチレベル、インストールされたアプリケーションを含めます。 |
| DS-10.3 | デバイス全体、もしくはデバイスの中でコンテンツを扱うまたは保存するエリアのいずれかを対象に、暗号化を義務付けます。 | * モバイルデバイスの管理システムを検討します。 |
| DS-10.4 | セキュリティコントロールの迂回を防ぎます。 | * 「牢破り」、ルーティングなどの使用を防ぎます。 |
| DS-10.5 | モバイルセキュリティ | モバイルデバイスの紛失/盗難/セキュリティ侵害、その他による必要性が生じた場合のために、リモートワイプを実施するシステムを導入します。 | * デバイスのリモートワイプが実施された場合、会社関係以外のデータが失われる可能性がある旨を従業員に改めて知らせます。 |
| DS-10.6 | 10分間使用されない状態が続くとデバイスが自動ロックされる機能を導入します。 |  |
| DS-10.7 | すべてのモバイルデバイスのオペレーティングシステムのパッチ、およびアプリケーションの更新を管理します。 | * セキュリティ関連のパッチ/更新は、デバイスのメーカー、通信事業者、または開発者が一般向けにリリースした時点で、入手可能な最新のものを使用します。 |
| DS-10.8 | パスワードに関するポリシーを徹底させます。 | * DS-8.1を参照してください。 |
| DS-10.9 | モバイルデバイスのバックアップと復旧を実施するためのシステムを導入します。 | * バックアップを暗号化し、セキュリティ保護された場所に保存します。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| DS-11.0 | セキュリティテクニック | セキュリティテクニック（例: spoiling、目に見えない/見える**透かし**）が使用可能で、指示された場合には実行することを徹底させます。 |  |
| DS-11.1 | **AES**128ビット以上の**暗号化**を使用して、ハードドライブ上のコンテンツ、またはハードドライブ全体を暗号化します。ここでは、次のうちいずれかのテクニックを使用します。   * ファイルベースの**暗号化**: （例: コンテンツそのものの暗号化） * ドライブベースの**暗号化**: （例: ハードドライブの暗号化） | * 外付けのハードドライブの場合、事前に暗号化されているドライブの購入を考慮してください（例: Rocstor Rocsafe、LaCie Rugged Safe）。 * 次を含む、ハードウフェア上のすべてのコンテンツを暗号化します。 * SAN / NAS * サーバー * ワークステーション * デスクトップ * ラップトップ * モバイルデバイス * 外付けストレージデバイス * 次に挙げるテクニックのうち1つ以上を実装します。 * DMG、暗号化ZIP ファイルなどのファイルベースの**暗号化** * ソフトウェアを使用する、ドライブベースの**暗号化** |
| DS-11.2 | 通常の帯域外の通信プロトコルを使用した暗号化キーやパスワードを送信します（コンテンツと同じストレージ**メディア**上にはない）。 | * コンテンツ転送に使用されるものとは異なるメソッドで暗号化キーやパスワードを送信します。 * キーネームやパスワードがプロジェクトやコンテンツと関連していないことを確認します。 |
| DS-11.3 | セキュリティテクニック | キー管理のポリシーと手順を導入し文書化します。   * 所在場所に関係なく（例：サーバー、データベース、ワークステーション、ラップトップ、モバイルデバイス、送信中のデータ、Eメール）、重要性の高いコンテンツまたはデータは、保護のために暗号化プロトコルを使用 * 信頼されているデバイスの承認と取り消し * コンテンツキーの生成、更新、取り消し * コンテンツキーの内外への配布 * 暗号化キーは、特定可能なオーナーに連携 * キーの管理と使用を分離させるため、任務を分割 * キー保管の手順 * キーバックアップの手順 | * 各顧客ごと、および重要な資産に固有の暗号化キーを作成することを検討します * 未承認の暗号化キーの代替手法を禁じます * 暗号化キーの管理者に対し、暗号化キーの管理者としての責任を理解し、それを承認する旨を正式に表明することを義務付けます |
| DS-11.4 | **AES**128ビット以上の**暗号化**を使用した、バーチャルサーバーインスタンス全体を含む、静止中または稼働中の暗号化されたコンテンツ。 | * [http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1\_Dec2005.pdf](mailto:http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf) |
| DS-11.5 | セキュリティテクニック | データ/コンテンツの暗号化に使用される秘密のプライベートキー（パブリックキーではない）は、常に次の中の1つ以上の形態で保管します。   * 少なくともデータ暗号化キーと同等の強さをもち、かつデータ暗号化キーと別の場所に保管されている、キー暗号化キーで暗号化されている * セキュリティ保護された暗号化デバイスの中にある（例：Host Security Module (HSM) または Pin Transaction Security (PTS) 接触点デバイス） * セキュリティ業界で認可された方法に基づく、少なくとも2つの完全な長さをもつキー構成要素またはキーシェアを備えている |  |
| DS-11.6 | **信頼されているデバイスのリスト（TDL）**にのっているデバイスが、権利所有者の承認に準拠していることを確認します。 | * コンテンツの再生が可能であると信頼されているデバイスのリストを提供するよう、顧客に要求します。 * **TDL**のデバイスについては、キー配布メッセージ（KDM）のみを作成します。 |
| DS-11.7 | コンテンツキーの有効性を確認し、有効期限が顧客の指示と適合していることを保証します。 | * コンテンツキーの有効期限を提供するよう、顧客に要求します。 * コンテンツの表示が可能な期間を限定するキーの有効期限最終日を指定します。 |
| DS-12.0 | コンテンツトラッキング | デジタルコンテンツの詳細なトラッキングを実現するため、デジタルコンテンツ管理システムを導入します。 | * 借り出し・返却されたデジタルコンテンツは、すべてログに記録します。 * すべてのコンテンツのデジタル所在場所をログに記録します。 * 借り出しの際は返却予定期間をログに記録します。 * 各借り出し・返却の日時をログに記録します。 |
| DS-12.1 | コンテンツトラッキング | デジタルコンテンツの出し入れのトランザクションログは、一年間保持します。 | * 以下が含まれます。 * 借り出し・返却の日時 * 資産を借り出した人の氏名と固有のID * 借り出しの理由 * コンテンツの所在場所 |
| DS-12.2 | デジタルコンテンツ管理システムからのログを定期的にレビューし、異常な状況を調査します。 |  |
| DS-12.3 | 該当する場合、デジタル資産のトラッキングシステムでは顧客のAKA（「別名」）を使用します。 | * 顧客AKAを知る者は、顧客資産の処理の関係者だけに制限します。 |

| No. | セキュリティトピック | ベストプラクティス | 実施ガイダンス |
| --- | --- | --- | --- |
| DS-13.0 | 転送システム | **転送**システムは、アクセスコントロールと、静止中または稼働中のコンテンツについて**AES**128ビット以上の暗号化を使用した、顧客が承認したシステムのみを利用し、かつ、コンテンツの転送セッションでは強力な認証を使用します。 | * コンテンツ転送システムへのアクセスは、権限のあるユーザーのみに許可します * また、プロジェクトごとにアクセスを制限することを検討します * 使用前に、コンテンツ転送システムが顧客に承認されていることを確認します |
| DS-13.1 | 暗号化された**転送ツール**が使用されないケースでは、顧客から事前に書面による承認を取り、例外プロセスを実施します。 | * 無作為に作成され、安全な形で認証を得たユーザー名とパスワードを使用します。 * 顧客が承認したツールやアプリケーションのみを使用します。 * 暗号化されていない**転送ツール**を使用する場合は、顧客に署名を要求します。 * すべての例外を文書化し、保存します。 |
| DS-14.0 | 転送デバイス方法 | コンテンツ転送には専用のシステムを実装・使用します。 | * 編集ステーションとコンテンツストレージサーバーが、コンテンツの転送に直接使用されていないことを確認します。 * 転送システム、もしくはコンテンツの保管、転送、処理に使われるあらゆるシステムにおいて、**VPN**/リモートアクセスを無効化します。 |
| DS-14.1 | コンテンツ転送システムは、管理および制作ネットワークと分離させます。 | * ネットワークは、物理的または論理的に分離させます |
| DS-14.2 | 転送デバイス方法 | コンテンツ転送システムは**中立ゾーン**（**DMZ**）に置きます。**コンテンツ/制作ネットワーク**に置いてはなりません。 | * **DMZ**に設置する前に、コンテンツ転送システムはハードニングします（DS-1.5で提案事項を参照してください）。 * コンテンツ**転送ツール**が要求するポートを除き、すべてのポートを制限する**アクセスコントロールリスト（ACL）**を実施します。 * 内部ネットワークと**DMZ**の間のトラフィックを、特定の送信元・送信先**IPアドレス**に制限するように、**ACL**を設定します。 * コンテンツの転送に使用するシステムでは、インターネットへのアクセスを無効化します。ただし、顧客のコンテンツをダウンロードしたり、承認された場所にコンテンツを転送するうえで必要な場合は、その限りではありません。 |
| DS-14.3 | 送受信が完了したら、ただちにコンテンツ転送デバイスからコンテンツを除去します。 | * コンテンツを受領した際は通知を送信するよう顧客に要求します。 * ゴミ箱を含め、転送デバイスとシステムからコンテンツを除去するプロセスを導入します。 * 適宜、プロジェクトの完了後ただちに**転送ツール**への顧客アクセスを削除します。 * セッション終了後に接続が解除されたことを確認します。 |
| DS-14.4 | アウトバウンドのコンテンツ転送の際は、制作コーディネータに自動通知を送付します。 | * ユーザーがコンテンツをネットワークから送信するたびに、制作コーディネータに自動通知（例: Eメール）が送付されるようにコンテンツ転送システムを設定します。 |
| DS-15.0 | クライアントポータル | コンテンツの転送、コンテンツのストリーミング、キーの配布に使用するウェブポータルへのアクセスは、認可ユーザーのみに制限します。 | * コンテンツ転送、コンテンツのストリーミング、キーの配布を行うウェブポータルの周辺で、アクセスコントロールの方策を講じます。またその際は、次に挙げる項目を1つ以上実行します。 * ユーザー証明書の要求 * 認証と確認のためのマシンとユーザーキーの統合 * 適切な任務の分割（例：一人がキーを作成し、別の人がそのキーを使用してコンテンツを暗号化する）を使い、暗号化キーを管理します。 * 特殊ネットワークへのポータルアクセスを、**VLAN**、サブネット、**IP アドレス**の範囲に制限します。 * クライアントポータルからアップロード・ダウンロードする能力を適宜制限します。 |
| DS-15.1 | クライアントポータル | ポータルのユーザーに固有の証明書を割り当て、証明書をクライアントに安全に配信します。 | * ユーザー名やパスワードをコンテンツのリンクに埋め込んではなりません。 * ユーザー証明書とコンテンツリンクは別々のEメールに記載することを考慮してください。 * ユーザー証明書の配布は電話またはSMSで行うことも考慮してください。 * 暗号化のキーを帯域外転送により配布することを考慮してください。 * 次の条件をそろえたパスワードポリシーを作成します。 * 最低文字数が8文字 * 大文字、小文字、数字、記号の中から少なくとも3種類を使用 * パスワードの最長保持期間は90日 * パスワードの最短保持期間は1日 * 無効なログオンの試みの最大回数は3～5回 * 無効なログインを試みたためにロックされたユーザーアカウントは、手動でロック解除されなければなりません。一定時間が経過した後に、自動的にロック解除してはなりません。 * 過去10個のパスワードの履歴 |
| DS-15.2 | ユーザーが自分の**デジタル資産**のみへのアクセスを持っていること（すなわち、顧客Aは顧客Bのコンテンツにアクセス可能であってはなりません）を確実にします。 | * 少なくとも四半期に一度、ファイル/ディレクトリの許可をレビューするプロセスを実施します。 * アクセスは必要な関係者のみに制限されていることを確認します。 |
| DS-15.3 | **DMZ**の専用サーバーにウェブポータルを置き、特定の**IP**とプロトコルとの間のアクセスを制限します。 | * クライアントポータルが要求するポートを除き、すべてのポートを制限する**アクセスコントロールリスト（ACL）**を実施します。 * 内部ネットワークと**DMZ**の間のトラフィックを、特定の送信元・送信先**IPアドレス**に制限するように、**ACL**を設定します。 * **DMZ**に設置する前にハードニングします （DS-1.5で提案事項を参照してください）。 |
| DS-15.4 | クライアントポータル | 顧客から承認を受けた場合を除き、インターネットウェブサーバーでホストされているサードパーティの制作ソフトウェア/システム/サービスの使用は禁止されています。 | * 次のうちの1つ以上の認証メカニズムの追加を検討します。 * 複数要素の認証 * 身分証明とアクセス管理システム * シングルサインオンのシステム * IDフェデレーション基準 * 128ビッド以上の高度暗号基準（AES）に基づく**VPN**接続を使用 |
| DS-15.5 | 社内外のウェブポータルでは、**HTTPS**を使用し、強力な暗号化サイト（例: TLS v1）の使用を徹底します。 |  |
| DS-15.6 | 繰り返し実行されるクッキーや証明書をプレーンテキストで保存するクッキーは使用しないでください。 | * 既存のウェブベースのアプリケーションによるクッキーの使用をレビューし、プレーンテキストで保存するクッキーがないことを確認します。 * プレーンテキストのクッキーに証明書を保存しているアプリケーションがあった場合、次に挙げる措置のうち1つを講じてください。 * アプリケーションを再設定する * アプリケーションをアップデートする * アプリケーション開発者にセキュリティパッチを依頼する |
| DS-15.7 | 社内外のポータル上におけるコンテンツへのアクセスを、可能な限り、事前指定した期限で自動的に失効するように設定します。 |  |
| DS-15.8 | 四半期に一度、ウェブアプリケーションの脆弱性をテストし、確認された問題を是正します。 | * Open Web Application Security Project (OWASP) が発行したガイドラインなどの業界で受け入れられているテストガイドラインを使用して、Cross Site Scripting (XSS)、SQL Injection、Cross Site Request Forgery (CSRF)などの一般的なウェブアプリケーションの脆弱性を特定します。 * テストは、独立したサードパーティが実施しなければなりません。 * 詳細については、付録Gを参照してください。 |
| DS-15.9 | クライアントポータル | 年に一度、ウェブアプリケーションの侵入テストを行い、確認された問題を是正します。 | * Open Web Application Security Project (OWASP) が発行したガイドラインなどの業界で受け入れられているテストガイドラインを使用して、Cross Site Scripting (XSS)、SQL Injection、Cross Site Request Forgery (CSRF)などの一般的なウェブアプリケーションの脆弱性を特定します。 * テストは、独立したサードパーティが実施しなければなりません。 * 詳細については、付録Gを参照してください。 |
| DS-15.10 | テレコムサービスプロバイダとのコネクションの設置の依頼は、認可済みの関係者だけに許可します。 |  |
| DS-15.11 | Eメール（ウェブメールも含む）を使ってコンテンツを送信することを禁止します。 | * Eメールと添付資料の暗号化には、セキュリティ保護されているEメールアプライアンスサーバー（例: Cisco IronPort、Sophos E-Mail Security Appliance、Symantec PGP Universal Gateway Email）の使用を考慮してください。 |
| DS-15.12 | 少なくとも四半期に一度、クライアントウェブポータルへのアクセスをレビューします。 | * プロジェクトが完了したら、クライアントウェブポータルへの**アクセス権**を削除します。 * インアクティブなアカウントを削除します。 * データを転送した時は、常に、適切な関係者にEメールによる自動通知を送信することを検討します。 |

付録A — 用語集

この用語集は、頻繁に使用される基本的な用語と短縮形を収録したもので、本書の本文で参照されています。これらの定義は該当するISO標準（27001/27002）、セキュリティ標準（例: NIST）、および業界のベストプラクティスから集めたものです。ベストプラクティスのガイドラインでは、本用語集に収録されている用語はすべて**太字**で書かれています。

| **用語または短縮形** | **説明** |
| --- | --- |
| **アクセスコントロールリスト（ACL）** | リソースへのアクセスが許可されているシステムのリストを特定することにより、システムリソースへのアクセスコントロールを実行するメカニズム。 |
| **アクセス権** | 物体またはシステムを使用・変更する権利 |
| **高度暗号化標準（AES）** | 128ビットブロックと128、192、256ビットのキー長さを使用するNIST対照キー暗号化標準。 |
| **資産管理** | ワークフローの最初から最後（獲得から処分）まで資産をトラッキングするシステム。 |
| **クローズドサーキットテレビジョン（CCTV）** | 一定のモニターセット上にある特定の場所へ信号を転送するために使用されるビデオカメラ。 |
| **CCTVコンソール** | 集中CCTVモニタリング インターフェースシステム。 |
| **従業員** | 社員、一時雇用者、研修生を含め、施設に直接雇用されている個人。 |
| **コンテンツ/制作ネットワーク** | メディアコンテンツを保存、転送、処理するために使用されるコンピュータネットワーク。 |
| **デジタル資産** | コンテンツやメディアの一種で、バイナリーソースの形にフォーマットされたもの。使用権限も含まれます。 |
| **デューデリジェンス** | 経歴が良好であることを確認するために、従業員やサードパーティの従業員の雇用前に行われる調査。 |
| **Dynamic Host Configuration Protocol (DHCP)** | ネットワークのすべてのノードにIPアドレスを自動的に割り当てるために使用されるプロトコル。 |
| **中立ゾーン (DMZ)** | 会社の外部サービスを含み、それを信頼されていない大規模ネットワーク（通常はインターネットを指す）にさらす物理的・ロジカルサブネットワーク。 |
| **暗号化** | 認可のない人には簡単に理解できないciphertextと呼ばれる形式にデータを転換すること。 |
| **フィンガープリンティング** | ソフトウェアがメディアの特徴のコンポーネントを特定、抽出、圧縮するテクニック。圧縮した形で独自のメソッドでメディアを特定します。 |
| **ファイヤウォール** | ローカルのセキュリティポリシーに従って、ネットワーク間のアクセスを制限するゲートウェイ。 |
| **ファイヤウォール ルールセット** | 送信元と送信先の間でパケットをルーティングする方法を決定するためにファイヤウォールが使用する指示表。 |
| **FireWire** | 外部のデバイスからコンピュータへのデータの転送を許可する高速インターフェース。 |
| **File Transfer Protocol (FTP)** | TCP/IPプロトコルは、暗号化なしにネットワークを介したファイル転送を指定します。 |
| **HTTPS** | コンピュータネットワーク上でセキュリティ保護されたコミュニケーションを行うためのコミュニケーションプロトコル。特にインターネット上で広く使われます。 |
| **IDバッジ** | 施設へのアクセスを許可された個人を特定するカード（例: 従業員、ベンダー、ビジター）。 |
| **侵入探知/ 侵入防止（IDS/IPS）** | 侵入探知システム (IDS) は、悪意のあるアクティビティやポリシー違反がないかネットワークまたはシステム上のアクティビティをモニターし、管理ステーション向けの報告書を作成する、デバイスまたはソフトウェアアプリケーションです。侵入防止システム（IPS）も同様の機能をもつと同時に、アクティビティをブロックするよう試みます。 |
| **インシデント対応** | セキュリティインシデントの検知、分析、是正。 |
| **情報システム** | 情報処理のために施設が使用する電子形式またはコンピュータベースのシステム。情報システムには、アプリケーション、ネットワークデバイス、サーバー、ワークステーションなどが含まれます。 |
| **I/Oデバイス** | コンピュータ間、またはコンピュータと別のデバイスの間で通信のために使用されるデバイス（例: USB、FireWireドライブ）。 |
| **IPアドレス** | コンピュータネットワークに参加しているデバイスに割り当てられるID番号（ロジカルアドレス）。 |
| **キー管理** | 暗号化コンテンツへのアクセスに使用される暗号化キーの作成、配布、保管、取り消し。 |
| **キーカード** | 電子アクセスコントロールロックとともに使用されるデジタル署名を補完するプラスチックのカード。 |
| **Local Area Network (LAN)** | 小さな物理的エリア（例: オフィス）を範囲とするコンピュータネットワーク。 |
| **MACアドレスフィルタリング** | コンピュータネットワークへのアクセスを制限するために使用されるセキュリティアクセスコントロールメソッド。 |
| **マスターキー** | 一つの施設ですべてのドア（内外ともに）を開けることができる鍵 セキュリティの高いすべてのエリアにアクセスできる鍵もマスターキーと呼ばれます。 |
| **メディア** | 情報システム内にある磁気テープ、オプティカルディスク、磁気ディスク、LSIメモリーチップ、情報が記録・保存されている印刷物を含むがこれに限定されない、物理的デバイスや記述のある表面。 |
| **ネットワークプロトコル** | コンピューティングエンドポイント間における接続、通信、データ送信をコントロールまたは可能にする取決めや標準。 |
| **ネットワーク インターフェースカード（NIC）** | コンピュータをコンピュータネットワークと接続する、コンピュータハードウフェアの構成要素。 |
| **制作以外のネットワーク** | メディアコンテンツの処理や転送以外に使用されるすべてのコンピュータネットワーク。事務ネットワークや顧客のネットワークも制作以外のネットワークに含むことができます。 |
| **リスク査定** | ビジネスへの脅威を特定するために実行されるリスクの特定と優先順位付け。 |
| **リスク管理** | リスク査定とセキュリティコントロールの実施を介して行うリスクの特定、分析、緩和。 |
| **ルーター** | ソフトウェアとハードウェアで情報の方向付けと転送を行うデバイス。 |
| **セキュリティ情報とイベント管理（SIEM）** | セキュリティ情報管理（SIM）とセキュリティイベント管理（SEM）を組み合わせたソフトウェア製品およびサービスを指す用語。SIEM 技術は、ネットワークハードウェアとアプリケーションが生成したセキュリティアラートを、リアルタイムで分析します。 |
| **任務の分割** | 一人だけで任務を完了する能力を持つ人間は存在しないという安全に関する原則、および一人だけで関連性のない複数の機能の責任を持つことができる人間は存在しないという原則から発生した考え。 |
| **Service Set Identifier (SSID)** | ワイヤレスLAN専用の特定ツール。多くの場合、人間が解読できるストリングなので、通常「ネットワーク名」と呼ばれます。 |
| **Small Computer System Interface (SCSI)** | コンピュータと周辺機器の間を物理的に接続し、データを転送する標準。 |
| **ステージングエリア** | 受取り前にコンテンツが保存されるエリア（例: 配達、配給）。 |
| **静的IP** | コンピュータが始動する際に毎回同じIPアドレスを使用するように設定すること。 |
| **スイッチ** | ネットワーク内の複数のマシンを接続し、トラフィックを特定の目的地へと進ませるコンピュータネットワークデバイス。 |
| **Telnet** | リモートのマシンにアクセスするために、インターネットまたはローカルエリアネットワークで使用されるネットワークプロトコル。 |
| **サードパーティの従業員** | 他社に雇用されているが、当施設でサーバーを提供する個人。サードパーティの従業員には、契約社員、フリーランサー、派遣会社が含まれます。 |
| **トラッキングメカニズム** | 資産の登録、資産の動き（例: 保管庫から編集部への資産の移動）のトラッキング、出荷、資産の破壊を含む、制作プロセスで資産をトラッキングするために使用されるツール、プロセス、手法。 |
| **転送ツール** | ネットワークでデジタル資産の電子形式による転送に使用されるツール。通常、受け入れられている暗号化と認証メカニズムを用います。 |
| **転送プロトコル** | コンピュータネットワークまたはインターネットを介してのファイル転送に関連した手順。 |
| **Trusted Device List (TDL)** | コンテンツを再生することが承認されている特定のデジタルデバイスのリスト。 |
| **固有のユーザー名** | 判別可能なログインID。 |
| **Universal Serial Bus (USB)** | デバイスはホストコンピュータに接続するシリアルバス標準。 |
| **ユーザーアクセス管理** | ユーザー権限の作成と変更、およびシステムやアプリケーションからユーザーアカウントを取り除くプロセス。 |
| **保管庫** | コンテンツを収録した物理的メディアを保存する専用保管エリア。 |
| **Virtual Local Area Network (VLAN)** | LANまたは内部ネットワークの特性を持ちながら、物理的な場所に制限されないコンピュータネットワーク。 |
| **Virtual Private Network (VPN)** | 別の大規模ネットワークへのアクセスを可能にするコンピュータネットワーク。 |
| **Wide Area Network (WAN)** | 広範囲（例: 企業）に広がるコンピュータネットワーク。 |
| **透かし** | デジタル資産に情報を埋め込むプロセス（取り消しができない場合を含む）。 |
| **進行中の作品** | 最終の形とはみなされない作品や製品。 |
| **ワークフロー** | 企業がコンテンツを対象として講じる一連の作業。 |

付録B — MPAA作品名とディストリビューションチャネルの定義

**作品のタイプ**

| **作品のタイプ** | **説明** |
| --- | --- |
| **フィーチャー** | 映画館用の長編映画。ホームビデオやインターネット向けとされることもあります。これには次のタイプがあります。   |  |  | | --- | --- | | **フィーチャータイプ** | **説明** | | フィーチャーフィルム | 長編映画。 | | 短編 | フィーチャーフィルムよりも短い映画。 | | ロングフォーム、ノンフィーチャー | 上記以外のもので、ドキュメンタリーなど。 | |
| **TVエピソード** | TV、ウェブ、モバイルと関連した作品で、シーズンやミニシリーズのエピソードを含みます。他の特殊シーケンスと同様に「パイロット」もエピソード（「ウェビソード」や「モバイソード」）です。 |
| **TVノンエピソード** | TV、ウェブ、モバイルと関連した作品ですが、エピソードを含みません（例: TV用映画、スポーツイベント、ニュース番組）。 |
| **プロモーション/宣伝** | 次の要素を含む仕事。   * + 「プロモーション」– メディアと関連したプロモーション資料。これには、ティーザー、予告編、電子プレスキット、その他の資料が含まれます。プロモーションは宣伝の特殊な形です。 |
| **宣伝** | TVコマーシャル、インフォマーシャル、パブリックサービスアナウンス、プロモーションを含む宣伝の形は「プロモーション」に属しません。これには、TVのCMとして放送されることがあっても、映画の予告編、ティーザーは含まれません。 |
| **ミュージック** | リングトーン、ミュージックビデオ、その他の音楽を含む仕事のタイプ。 |
| **その他** | 次の要素を含む仕事。   |  |  | | --- | --- | | **タイプ** | **説明** | | 抜粋 | 主に他の作品の一部を持ってきて構成した資産。 | | 補足 | 他の仕事を補足するようデザインされた資料。例えば、DVDと関連した番外など。 | | コレクション | 資産の集合体。他のカテゴリーには属しません。例えば、映画のコレクションなど。 | | フランチャイズ | 異なるタイプのコレクションまたは組み合わせ。例えば、複数のTV番組を合わせたり、TV番組と映画を合わせたりしたものをフランチャイズと呼びます。 | |

**ディストリビューションチャネル**

| **ディストリビューションチャネル** | **説明** |
| --- | --- |
| **映画館向け** | 映画館で初回リリースされるフィーチャーフィルム。 |
| **映画館以外** | TV、ホームビデオ、映画館以外の形で公にリリースされるモーションピクチャー。この映画の上演は次の場所で行われます。(i) 航空機、列車、船、その他の公共の場所。(ii) 学校、大学、その他の教育機関、図書館、官公庁、企業や商店、サービス組織、クラブ、教会やその他の宗教団体、博物館や美術館、映画協会（上映場所の周辺でクローズドサーキットによる上映を含む） (iii) 臨時・常設の軍隊の施設、収容施設、刑務所、シニアセンター、オフショア採油装置、木材採取業合宿所、遠隔地の林業または建設業の合宿所（上映場所の周辺でクローズドサーキットによる上映を含む）。 |
| **ホームビデオ** | 卸売レベルでパッケージされ、販売やレンタルセールのためにリリースされるモーションピクチャー。例えばDVD、Blu-Rayなど。 |
| **無料TV** | 無料ブロードキャスト信号で公にリリースされる映画。通常はネットワーク、TV局、ベーシックなケーブルネットワークとの契約で放映されます。 |
| **有料TV** | ビデオオンデマンド、有線、衛星、ペイバイビューなど、少なくともブロードキャストチェーンで一人の参加者が支払うことを要求され、公にリリースされる映画。 |
| **インターネット** | 次に挙げるオンライン ディストリビューションチャネルのひとつでリリースされる映画。   |  |  | | --- | --- | | **タイプ** | **説明** | | Electronic Sell-Through (EST) または Download to Own (DTO) | オンラインで販売される永久に所有できるデジタルコピー。 | | オンラインレンタルまたはビデオオンデマンド (VOD) | オンラインで料金を支払い、一時的に視聴できるレンタル。 | | サブスクリプション ビデオオンデマンド (SVOD) | オンラインのサブスクリプションでレンタルして視聴。 | | オンライン無料ビデオオンデマンド (FVOD) | 通常広告の宣伝費でサポートされる無料オンラインストリーミングによる視聴。 | | その他 | モバイルやインターネットプロトコルTVなどのオンラインメディアとニューメディア。 | |

付録 C — 施設のマッピング

以下にある凡例を確認し、自社が提供するサービスに該当する施設タイプを特定し、リスク査定に基づく適切なコントロールを実施してください。

|  |  |  |  |
| --- | --- | --- | --- |
| **凡例** | | | |
| ADS | オーディオ、ダビング、字幕スーパー | FL | フィルムラボ |
| CA | クリエイティブ広告 | IFE | IFEおよびホスピタリティサービス |
| CDF | 宅配業・運送業 | PP | ポストプロダクション |
| D | ディストリビューション | R | 複製 |
| DC | デジタルシネマ | VFX | ビジュアルエフェクト |
| DS | デジタルサービス | AS | アプリケーション セキュリティ |
| DVD | DVD製作 | CS | クラウド セキュリティ |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| MS-1.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-1.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-2.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-2.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-3.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-4.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| MS-5.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-5.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-6.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-6.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-7.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-8.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-8.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-9.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-10.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-11.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-11.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| MS-12.6 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-1.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-1.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-1.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-2.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-3.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-4.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-4.1 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-4.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-4.3 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-5.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.6 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-5.7 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-6.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-6.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-6.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-7.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-8.5 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-9.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-10.0 | X | X | X | X | X | X | X | X | X | X |  | X | X | X |
| PS-10.1 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-10.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-10.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-11.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-11.1 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.3 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.4 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.5 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.6 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.7 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-11.8 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-11.9 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-12.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-12.1 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.2 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.3 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.4 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.5 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-12.6 |  |  | X | X |  |  |  |  |  |  |  |  |  |  |
| PS-13.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-13.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-14.0 | X | X |  | X | X | X | X | X | X | X | X | X |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-14.1 | X | X | CDF | X | X | X | X | X | X | X | X | X | AS | CS |
| PS-14.2 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-15.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-15.3 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| PS-15.4 |  |  | X |  |  |  |  |  |  |  |  |  |  |  |
| PS-16.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-16.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.3 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.4 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-17.5 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-17.6 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-17.7 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-17.8 |  |  |  |  |  |  |  | X |  |  | X |  |  |  |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| PS-17.9 |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| PS-18.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-18.1 |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
| PS-18.2 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-18.3 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-19.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-20.0 | X | X | X | X | X | X | X | X | X | X | X | X |  |  |
| PS-20.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-20.2 |  |  |  | X |  |  |  |  |  |  | X |  |  |  |
| PS-21.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PS-21.1 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-21.2 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| PS-21.3 |  |  | X | X |  |  |  | X |  |  | X |  |  |  |
| DS-1.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-1.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-1.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-2.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-3.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-4.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-4.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-4.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-5.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-5.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-6.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-7.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-7.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-8.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-9.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-10.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-10.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-11.6 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
| DS-11.7 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
| DS-12.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-12.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-13.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-13.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
|  | ADS | CA | CDF | D | DC | DS | DVD | FL | IFE | PP | R | VFX | AS | CS |
| DS-14.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-14.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.0 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.1 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.2 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.3 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.4 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.5 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.6 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.7 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.8 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.9 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.10 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.11 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |
| DS-15.12 | X | X |  | X | X | X | X | X | X | X | X | X | X | X |

付録D — 参照ポイントへのコントロールのマッピング

下表は、ISO 27001/27002およびNIST 800-53標準に対するベストプラクティスの一般的なマッピングを示すものです。これらの標準は、提供されたセキュリティコントロールの実装に関する詳細な情報として参照できます。

| **No.** | **セキュリティトピック** | **ISO 27002 -2013 参考資料** | **NIST 800-53 第4版 参考資料** |
| --- | --- | --- | --- |
| **MS-1.0** | エグゼクティブによるセキュリティの認識/監督 | 6.1.1 | PM-1, PM-2 |
| **MS-1.1** | 6.1.1 | AT-2, AT-3, PM-1, PM-2 |
| **MS-1.2** | 5.1.2, 6.1.1 | PM-1, PM-6, AT-3 |
| **MS-1.3** | 5.1.2, 6.1.1 | PM-1, PM-6, AT-3 |
| **MS-2.0** | リスク管理 | 6.1.1 | CA-1, RA-1 |
| **MS-2.1** | 5.1.2 | RA-2 |
| **MS-3.0** | セキュリティ構成 | 6.1.3 | PM-2 |
| **MS-4.0** | ポリシーと手順 | 5.1.1, 6.1.1 | PL-1 |
| **MS-4.1** | 5.1.2 | PL-1 |
| **MS-4.2** | 8.1.3 | PL-1, PS-7 |
| **MS-4.3** | 8.2.2, 8.1.3 | AT-1, AT-2, AT-3, AT-4 |
| **MS-5.0** | インシデント対応 | 16.1.1 | IR-1, IR-8 |
| **MS-5.1** |  | IR-2 |
| **MS-5.2** | 16.1.2 | IR-6, IR-7 |
| **MS-5.3** | 16.1.2 | IR-4, IR-5 |
| **MS-6.0** | ビジネス継続性と災害復旧 | 17.1.1 | CP |
| **MS-6.1** | 17.1.1 | CP |
| **MS-7.0** | 変更管理と設定管理 | 14.2.2 | CM |
| **MS-8.0** | ワークフロー | 11.1 |  |
| **MS-8.1** | 11.1 |  |
| **MS-9.0** | 任務の分割 | 6.1.2 | AC-5 |
| **MS-10.0** | 経歴確認 | 7.1.1 | PS-3 |
| **MS-11.0** | 守秘契約 | 7.1.2 | PL-4, PS-6, SA-9 |
| **MS-11.1** | 8.1.4 | PS-4, PS-8 |
| **MS-12.0** | サードパーティの利用と審査 | 7.1.2 | PL-4, PS-6, SA-9 |
| **MS-12.1** | 8.1.4 | PS-7, SA-9 |
| **MS-12.2** | 7.2.1 | PS-4 |
| **MS-12.3** | 8.14 |  |
| **MS-12.4** | 7.1.2 | PS-7 |
| **MS-12.5** | 11.1.2 | PL-4, PS-6, SA-9 |
| **MS-12.6** | 7.1.1 |  |
| **PS-1.0** | 出入り口 | 11.1 | PE-3 |
| **PS-1.1** | 11.1 | PE-3, PE-6 |
| **PS-1.2** | 11.1 | PE-1, PE-2, PE-3 |
| **PS-2.0** | ビジターの出入り | 11.1 | PE-8 |
| **PS-2.1** | 11.1 | PE-7, PE-2, PE-3 |
| **PS-2.2** | 11.1 | PE-3 |
| **PS-2.3** | 11.1 | PE-7, PE-2, PE-3 |
| **PS-3.0** | 身分証明書 | 11.1.2 | PE-3 |
| **PS-4.0** | 周辺のセキュリティ | 11.1.1 | PE-3 |
| **PS-4.1** | 11.1.1 | PE-3 |
| **PS-4.2** | 11.1.1 | PE-3 |
| **PS-4.3** | 11.1.1 | PE-3 |
| **PS-5.0** | アラーム | 11.1.1 | PE-3, PE-6 |
| **PS-5.1** |  | PE-6 |
| **PS-5.2** | 11.1.1 | AC-6 |
| **PS-5.3** | 11.1.1 |  |
| **PS-5.4** | 11.1.1 | PE-3, PE-6 |
| **PS-5.5** | 11.1.1 | PE-3 |
| **PS-5.6** | 11.1.1 | PE-6 |
| **PS-5.7** | 11.1.1 | PE-9, PE-10, PE-11, PE-13 |
| **PS-6.0** | 承認 | 11.1 | PE-1, PE-2, PE-3 |
| **PS-6.1** | 11.1 | PE-2, |
| **PS-6.2** | 11.1 | PE-2, PS-4, PS-5 |
| **PS-7.0** | 電子アクセスコントロール | 11.1 | PE-2, PE-3 |
| **PS-7.1** | 11.1 | PE-2, PE-3 |
| **PS-7.2** | 11.1 | PE-2, PE-3 |
| **PS-7.3** | 11.1 | PE-2, PE-3 |
| **PS-7.4** | 11.1 | PE-2, PE-3 |
| **PS-8.0** | キー | 11.1 | PE-2, PE-3 |
| **PS-8.1** | 11.1 | PE-2, PE-3 |
| **PS-8.2** | 11.1 | PE-2, PE-3 |
| **PS-8.3** | 11.1 | CM-8 |
| **PS-8.4** | 9.2.6 | CM-5, CM-8 |
| **PS-8.5** | 9.2.6 | CM-5, CM-8 |
| **PS-9.0** | カメラ |  | PE-6 |
| **PS-9.1** | 11.1 | PE-6 |
| **PS-9.2** | 11.1 | PE-2, PE-3 |
| **PS-9.3** | 11.1 | AU-6, PE-6 |
| **PS-9.4** | 11.1 | PE-6 |
| **PS-10.0** | ロギングとモニタリング | 12.4 | AU-3, AU-6  AU-9, AU-11 |
| **PS-10.1** | 12.4 | AU-6 |
| **PS-10.2** | 12.4 | AU-6 |
| **PS-11.0** | 身体検査 | 11.1 |  |
| **PS-11.1** |  |  |
| **PS-11.2** |  |  |
| **PS-11.3** |  |  |
| **PS-11.4** |  |  |
| **PS-11.5** |  |  |
| **PS-11.6** | 11.1 |  |
| **PS-11.7** |  |  |
| **PS-11.8** |  |  |
| **PS-11.9** |  |  |
| **PS-12.0** | 在庫トラッキング | 8.1 | CM-8 |
| **PS-12.1** | 8.2.2 | MP-3 |
| **PS-12.2** | 8.2.3 | AU-9, AU-11 |
| **PS-12.3** |  | AU-6, CM-8 |
| **PS-12.4** |  |  |
| **PS-12.5** | 8.2.3 | AU-1, AU-3, AU-6 |
| **PS-12.6** | 8.2.3 |  |
| **PS-13.0** | 在庫確認 | 8.1.1 | AU-6, CM-8 |
| **PS-13.1** | 6.1.2 | AC-5 |
| **PS-14.0** | ブランクメディア/未処理ストックトラッキング | 8.2.2 | MP-4 |
| **PS-14.1** | 8.1.1 | MP-4, PE-2, PE-3 |
| **PS-14.2** |  |  |
| **PS-15.0** | 顧客の資産 | 8.2.3 | MP-4, PE-2, PE-3 |
| **PS-15.1** | 8.2.3 | MP-2, MP-4 |
| **PS-15.2** |  |  |  |
| **PS-15.3** |  |  |  |
| **PS-15.4** |  |  |  |
| **PS-16.0** | 処分 | 8.3.2 | MP-6 |
| **PS-16.1** | 8.3.2 | MP-6 |
| **PS-16.2** |  | MP-6 |
| **PS-16.3** |  | MP-6 |
| **PS-16.4** |  |  |
| **PS-17.0** | 出荷 | 8.3.3 | MP-5 |
| **PS-17.1** | 8.3.3 | AU-11, PE-16, MP-5 |
| **PS-17.2** | 8.2.3 | MP-5 |
| **PS-17.3** | 8.3.3 | PE-3, PE-7 |
| **PS-17.4** | 8.3.3 | PE-3, PE-7 |
| **PS-17.5** |  |  |
| **PS-17.6** |  |  |
| **PS-17.7** |  |  |
| **PS-17.8** |  |  |
| **PS-17.9** |  |  |
| **PS-18.0** | 入荷 | 8.2.3 | PE-16 |
| **PS-18.1** |  | MP-5 |
| **PS-18.2** | 8.2.2 | MP-3, MP-4 |
| **PS-18.3** | 8.2.3 | MP-3, MP-5 |
| **PS-19.0** | ラベル貼り | 8.2.2 | MP-3 |
| **PS-20.0** | パッケージング | 8.3.3 | MP-5 |
| **PS-20.1** | 8.3.3 |  |
| **PS-20.2** |  |  |
| **PS-21.0** | 輸送車両 |  | MP-5 |
| **PS-21.1** |  |  |
| **PS-21.2** |  |  |
| **PS-21.3** |  |  |
| **DS-1.0** | 外部ネットワーク/WAN | 13.1 | AC-4, SC-7 |
| **DS-1.1** | 9.1, 13.1, 13.2 | AC-3, AC-4 |
| **DS-1.2** | 10.1, 13.2 | CM-7 |
| **DS-1.3** | 13.2 | AC-20, CA-3, SC-7 |
| **DS-1.4** | 12.6 | CM-6, SI-2 |
| **DS-1.5** |  | CM-6, CM-7 |
| **DS-1.6** | 9.4, 10.1 | AC-6, AC-17 |
| **DS-1.7** | 12.3, 17.1 |  |
| **DS-1.8** | 12.6, 13.1 | RA-5, SC-7 |
| **DS-1.9** | 12.6 | RA-5, SC-7 |
| **DS-1.10** | 10.1, 13.1 | SC-7, SC-12, SC-33 |
| **DS-1.11** | 12.4 | SC-7, SC-12, SC-33 |
| **DS-1.12** | 12.2, 16.1 | SC-7, SC-12, SC-33 |
| **DS-2.0** | インターネット | 12.1, 13.1 | CA-3 |
| **DS-2.1** | 13.2 | PL-4 |
| **DS-2.2** | 13 | AC-6, PL-4 |
| **DS-3.0** | LAN/内部ネットワーク | 9.4, 13.1 | SC-7 |
| **DS-3.1** | 11.2 |  |
| **DS-3.2** | 6.2, 13.1, 9 | AC-3, AC-17 |
| **DS-3.3** | 10.1 | CM-6, CM-7 |
| **DS-3.4** | 13.1 | SC |
| **DS-3.5** | 13.1 | SC |
| **DS-3.6** | 16.1 | SI-4 |
| **DS-3.7** | 9.4 | SC |
| **DS-3.8** | 9.1 | SC |
| **DS-3.9** | 12.6 | SC |
| **DS-3.10** | 12.3, 17.1 | SC |
| **DS-4.0** | ワイヤレス | 9.1, 13.1 | AC-18 |
| **DS-4.1** | 9.1, 13.1 | AC-18 |
| **DS-4.2** | 9.1, 13.1 | SI-4 |
| **DS-5.0** | I/Oデバイスセキュリティ | 10.7.1 | SC-7 |
| **DS-5.1** |  | AC-19, MP-2 |
| **DS-6.0** | システムセキュリティ | 12.2 | SI-3 |
| **DS-6.1** | 12.2 | SI-3 |
| **DS-6.2** | 12.2 | SI-3 |
| **DS-6.3** | 12.2 | SI-3 |
| **DS-6.4** | 12.5, 12.6 | SI-2, RA-5 |
| **DS-6.5** | 9.4 | AC-5, SC-2 |
| **DS-6.6** | 11.2 | PE-3 |
| **DS-6.7** | 6.2, 10.1, 11.1 | MA-4, PE-5 |
| **DS-6.8** | 8.1, 12.5 | CM-11 SI-7 |
| **DS-6.9** | 12.1, 12.5 | CM-10, SI-7 |
| **DS-6.10** | 12.6 | AC-3, AC-6, CM-7 |
| **DS-6.11** | 8.1 | CM-8 |
| **DS-6.12** | 8.1, 14.1, 14.2 |  |
| **DS-7.0** | 顧客管理 | 9 | AC-2 |
| **DS-7.1** | 9.1 | AC-2 |
| **DS-7.2** | 9.2, 9.4 | AC-2, AC-6, IA-4 |
| **DS-7.3** | 8.1, 9.2, 9.4 | AC-2, AC-6, IA-4 |
| **DS-7.4** | 12.4, 18.2 | AC-2, AC-6, IA-4 |
| **DS-7.5** | 12.1, 12.4 | AU-3, AU-6 |
| **DS-7.6** | 9.2, 9.4 | AU-2, AU-12 |
| **DS-7.7** | 9.2, 9.4 | PS-4, PS-5 |
| **DS-7.8** | 9.2, 9.4 | AC-2, PE-2 |
| **DS-8.0** | 認証 | 9.1 | IA-2, IA-4 |
| **DS-8.1** | 9 | AC-7, IA-5 |
| **DS-8.2** | 9.4, 10.1 | AC-17 |
| **DS-8.3** | 9.2, 9.4 | AC-11 |
| **DS-8.4** | 9.4 | AC-1 |
| **DS-9.0** | ロギングとモニタリング | 12.4 | SI-4, AU-2, AU-3 |
| **DS-9.1** | 12.4 | AU-1, AU-6 |
| **DS-9.2** | 12.4 | AU-1, AU-6 |
| **DS-9.3** | 12.4 | AU-1, AU-2, AU-6 |
| **DS-9.4** | 10.1 | AU-2, AU-3 |
| **DS-9.5** | 12.4 | AU-3, AU-8 |
| **DS-9.6** | 10.1.3, 10.10.3 | AU-9, AU-11 |
| **DS-9.7** | 12.4 | AU-6 |
| **DS-10.0** | モバイルセキュリティ | 6.2, 11.2 | SC, AC, IA-2 |
| **DS-10.1** | 6.2, 11.2 | SC, AC |
| **DS-10.2** | 6.2, 11.2 | SC, AC |
| **DS-10.3** | 6.2, 11.2 | SC, AC |
| **DS-10.4** | 6.2, 11.2 | SC, AC |
| **DS-10.5** | 6.2, 11.2 | SC, AC |
| **DS-10.6** | 6.2, 11.2 | SC, AC |
| **DS-10.7** | 6.2, 11.2 | SC, AC |
| **DS-10.8** | 6.2, 11.2 | SC, AC |
| **DS-10.9** | 6.2, 11.2 | SC, AC |
| **DS-11.0** | セキュリティテクニック | 8.2, 10.1 |  |
| **DS-11.1** | 8.2, 10.1 | IA-5, SC-13 |
| **DS-11.2** | 8.2, 10.1 | SC-8, SC-12 |
| **DS-11.3** | 8.2, 10.1 | SC-12 |
| **DS-11.4** |  |  |
| **DS-11.5** |  |  |
| **DS-11.6** | 10.1 |  |
| **DS-11.7** | 10.1 |  |
| **DS-12.0** | コンテンツトラッキング |  |  |
| **DS-12.1** |  |  |  |
| **DS-12.2** |  |  |  |
| **DS-12.3** |  |  |  |
| **DS-13.0** | 転送システム | 10.1, 13.2 | IA-5, SC-13 |
| **DS-13.1** | 10.1, 13.2 |  |
| **DS-14.0** | 転送デバイス方法 | 13.1 |  |
| **DS-14.1** | 13.1 | AC-4, SC-7 |
| **DS-14.2** | 13.1 | AC-4, AC-20, SC-7 |
| **DS-14.3** | 13.2 | MP-6 |
| **DS-14.4** | 12.4, 13.2 |  |
| **DS-15.0** | クライアントポータル | 13.1 | AC-6 |
| **DS-15.1** | 9.2, 9.4 | IA-5 |
| **DS-15.2** | 9.2, 9.4 | AC-2, AC-3, AC-6 |
| **DS-15.3** | 12.6, 13.1 | AC-4, AC-20 |
| **DS-15.4** | 9.2, 9.4, 10.1 |  |
| **DS-15.5** | 10.1 | SC-8, SC-13 |
| **DS-15.6** | 9.4 | AC-4 |
| **DS-15.7** | 9.4 | AC-2 |
| **DS-15.8** | 12.6 | SI-7 |
| **DS-15.9** | 12.6 |  |
| **DS-15.10** |  |  |
| **DS-15.11** | 13.2 | AC-4 |
| **DS-15.12** | 12.1 |  |

付録e — よくある質問（FAQ）

1. **わたしの施設では、提示されたすべてのベストプラクティスを実行しなければならないのですか?**

ベストプラクティス準拠は完全に任意です。これらはセキュリティ手順のプランニング、実施、変更を考慮する場合に、ご考慮いただくために推奨されているガイドラインです。

1. **わたしの施設では、複数のサービス（例: フィルムラボ、ポストプロダクション）を提供しています。どの補足ベストプラクティスを適用したらよいでしょうか?**

常にもっとも厳しい補足ベストプラクティスを適用します。ただし、ワークプロセスが分割されている場合は、そのサービス用の環境に適した補足ベストプラクティスを適用してください。

1. **わたしの施設には、ベストプラクティスの「実施ガイダンス」のセクションにすべての項目を適用することが義務付けられているのですか?**

いいえ。ガイドラインのこのセクションに記載されている情報は、特定のセキュリティコントロールを設定する最良の方法を決定するためのヘルプとして意図されています。MPAAによるコンテンツセキュリティ査定を行う施設の場合、弊社の査定では、ある一時点における施設の仕事状況をガイドラインの該当するベストプラクティスのセクションを比較するだけです。（MPAA コンテンツセキュリティ査定の受け方に関する詳細情報については、 contentsecurity@mpaa.orgまでお問い合わせください。）

1. **現在のシステムでベストプラクティスの実施ができないとしたら、どうしたらよいでしょうか?**

システムのベンダーに連絡をとり、システムでベストプラクティスが実施できるようにするためのソリューションを特定してください。ソリューションには、パッチング、バージョンアップデート、セキュリティの高いシステムへの変更などが考えられます。技術的な限界によってベストプラクティスの実施が妨げられている場合、別のセキュリティ対策を取ることも考えられます。ただし、これらの対策は関連リスクのすべてをカバーできないと言われています。システムの限界によるセキュリティガイドライン実施の例外は、正式に文書化され、顧客の承認を受けなければなりません。

1. **このガイドラインのベストプラクティスを適用しても、MPAAメンバーが設定したセキュリティ要件にも準拠する必要がありますか?**

ベストプラクティスの実施はガイドラインであり、各MPAAメンバーとの契約内容にとって代わることはありません。各メンバーがどのようなベンダーを使用するかは、そのメンバーの単独任意で決定されます。MPAAは、貴社が顧客とのセキュリティに関する話し合いの際、ベストプラクティスをガイドラインとして使われることを推奨します。

付録f — 推奨ポリシーと手順

コンテンツを保護するために、セキュリティポリシーと手順を作成・実施する一般的なエリアを下記に挙げます。

1. **物理的セキュリティのポリシーと手順**

* 出入り口のセキュリティ
* ビジターアクセスプロトコル
* 本人確認と認証
* 緊急時プロトコル
* 施設アクセスコントロール
* 施設モニタリング

1. **在庫と資産管理**

* 在庫トラッキング
* 出荷プロトコル
* 在庫の保管（現場、運送中）

1. **ITセキュリティ**

* インターネット使用ポリシー
* 認証と承認
* パスワードポリシー
* 悪意のあるコード保護/抗ウィルス
* 注：すべてを含む（容認される使用など）

1. **人事ポリシーと手順**

* 職務上の責任にセキュリティを含める
* スタッフの審査
* 守秘性、財産権、知的財産の保護合意
* 雇用条件
* 任務の分割
* 雇用の終了
* 懲戒措置
* セキュリティへの認識とトレーニングプログラム
* 従業員と一時雇用者/フリーランサー 経歴照会および検査
* 従業員と一時雇用者/フリーランサー 非開示契約（NDA）
* 記録保持

1. **サードパーティ**

* サードパーティの契約書
* 非開示契約（NDA）

1. **インシデント対応**

* インシデントの特定と分析
* インシデントの報告と上部報告
* インシデント対応プロセスと手順
* 事後レビュー手順と学んだこと

付録g — その他のリソースと参考資料

国際標準化機構 (ISO) 標準27001. *Information technology - Security techniques - Information security management systems – Requirements.* 2005年10月<http://www.27000.org/iso-27001.htm>

国際標準化機構 (ISO) 標準27002*. Information technology - Security techniques - Code of practice for information security management.* 2007年7月<http://www.27000.org/iso-27002.htm>

国際標準化機構 (ISO) 標準 27005. *Information technology - Security technique- Information security risk management*. 2008年6月<http://www.27000.org/iso-27005.htm>

National Institute of Standards and Technology Special Publication 800-53. *Recommended Security Controls for Federal Information Systems*, 2005年2月 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute of Standards and Technology Special Publication IR 7298. *Glossary of Key Information Security Terms,* 2006年4月

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

SysAdmin, Audit, Networking, and Security (SANS Institute). *Glossary of Terms Used in Security and Intrusion Detection*

<http://www.sans.org/resources/glossary.php#m>

The Open Web Application Security Project (OWASP) – Testing Guide

<http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf>

National Institute of Standards and Technology Special Publication 800-88. *Guidelines for Media Sanitization*, 2006年9月　http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Industrial Security Program - Operating Manual (DoD 5220.22-M), 2006年2月

http://dtic.mil/whs/directives/corres/pdf/522022m.pdf

The Center for Internet Security – Security Benchmarks http://benchmarks.cisecurity.org/

National Security Agency - Security Configuration Guides http://www.nsa.gov/ia/guidance/security\_configuration\_guides/

National Institute of Standards and Technology Special Publication 800-92. *Guide to Computer Security Log Management,* 2006年9月 <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

National Institute of Standards and Technology Special Publication 800-44.. *Guidelines on Securing Public Web Servers,* 2007年9月 <http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>

National Institute of Standards and Technology Special Publication 800-40. *Creating a Patch and Vulnerability Management Program,* 2005年11月 <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

付録h — MPAAへの不正行為報告

**MPAAへのオンライン不正行為報告**

不正行為はMPAAに直接報告することができます。

http://www.mpaa.org/contact-us/

**MPAAおよびMPAの24時間不正行為報告オンライン**

次のリストは各国の24時間不正行為報告オンラインの連絡先情報です。MPAAは地域のコンテンツ保護オフィスと協力しています。

|  |  |
| --- | --- |
| **北米と中南米地域** | |
| カナダ | (800) 363-9166 |
| 米国 | (800) 371-9884 |
| **欧州、中東、アフリカ（EMEA）地域** | |
| ベルギー | +32 2 778 2711 |
| イタリア | (800) 864 120 |
| オランダ | (909) 747 2837 |
| ウクライナ | +38 0 445 013829 |
| 英国 | (800) 555 111 |
| **アジア太平洋（APAC）地域** | |
| オーストラリア | +61 29997 8011 |
| 香港 | +65 6253-1033 |
| マレーシア | +65 6253-1033 |
| ニュージーランド | +65 6253-1033 |
| フィリピン | +65 6253-1033 |
| シンガポール | +65 6253-1033 |
| 台湾 | +65 6253-1033 |

すべてのコンテンツ保護地域と各国のオフィスに関する完全なリストは、 <http://www.mpaa.org/contact-us/>をご覧ください。

**MPAAオンラインリソース**

MPAAに関する詳細はウェブサイト[www.mpaa.org](http://www.mpaa.org)をご覧ください。

展示会の間は、[www.fightfilmtheft.org](http://www.fightfilmtheft.org)で世界のコンテンツ保護のプログラムについて詳細をご覧いただけます。

**以上**