****

**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**

 **アプリケーションとクラウド／分散環境のセキュリティ 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1.0

2015年3月17日

文書履歴

|  |  |  |  |
| --- | --- | --- | --- |
| **バージョン** | **日付** | **説明** | **作者** |
| 1.0 | 2015年3月17日 | 初回社外リリース | MPAAMPAAメンバー企業 |

**目次**

文書履歴 i

1. ベストプラクティス概要 2
2. プロバイダー概要 3
3. リスク管理 4
4. 書類の整理 5
5. ベストプラクティスの書式 6
6. ベストプラクティスのアプリケーションセキュリティ ガイドライン 7
7. ベストプラクティスのクラウドセキュリティ ガイドライン 25

付録A — 用語集 34

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 44

付録C — よくある質問 46

付録C — MPAAへの不正行為報告 47

**I. 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、サイトセキュリティ調査を代行してきました。Walt Disney Studios Motion Pictures; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLC; 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、世界中で自分の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、知的財産権の保護における危険性が増大すると共に、その保護策が世界における健全な情報経済を守る鍵であるとの認識が定着しつつあることを示します。

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ための標準的コントロールを設定する施設サービスを用いた、一連のベストプラクティスを規定する。
* 規定された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において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ための、標準的査定手段を提供する。

**目的と適用性**

本書の目的は、メンバーが現在および将来に起用、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ウインドウを考慮して設定されています。

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、国家の法律または規制に準拠します。

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は、**アプリケーション**と、**クラウド /分散環境の**セキュリティ ガイドラインに分かれています。**ベンダーは、まず最初にベストプラクティス共通ガイドラインに基づいて評価されなければなりません。両方のガイドラインが適用される場合は、より厳しい方が優先されます。**

**ベストプラクティスへの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への準拠が可能と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できない理由を文書化し、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。

**II. プロバイダー概要**

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、リリースウインドウをまとめたものです。

| **No.**  | **プロバイダーのタイプ** | **一般的なプロバイダー サービス** | **機能のタイプ** | **リリースウインドウ** |
| --- | --- | --- | --- | --- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1** | **アプリケーション** | * アプリケーション開発
* ウェブアプリケーション
* エンタープライズ・リソース・プラニング（ERP）
* 情報担当者用ソフトウェア
* SaaS （サービス型ソフトウェア）
 | * アプリケーション開発環境
* 多種
* 多種
* 多種
* 多種
 | * 多種
* 多種
* 多種
* 多種
* 多種
 |
| **2** | **クラウド** | * IaaS （サービス型インフラ）
* PaaS （サービス型プラットフォーム）
* SaaS （サービス型ソフトウェア）
* プライベート クラウド
* パブリック クラウド
* ハイブリッド クラウド
 | * データ ストレージ、コンピューティング リソース
* アプリケーション開発環境
* ビジネスアプリケーション
* 多種
* 多種
* 多種
 | * 多種
* 多種
* 多種
* 多種
* 多種
* 多種
 |

**コントロールの適用性**

本文書にあるガイドライン（アプリケーションセキュリティとクラウドセキュリティ両方のガイドライン）は、すべてのアプリケーションおよびクラウドベンダーに適用されます。

**III. 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すると共に、ビジネス目標を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、それが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、そのリリースウインドウに該当する利益の喪失）。さらに、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。

資産を特定、分類する

効果性をモニター、評価する

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

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、コンテンツ分類法の例を示すものです。

|  |  |  |
| --- | --- | --- |
| 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における超大作の盗難
* 世界初回リリース前における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
 |

**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、組織構造」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ます。また、これらの方策のデザインと有効性は、現在の脅威環境に基づいて定期的に評価しなければなりません。本書で概説されているベストプラクティスは、Open Web Application Security Project（**OWASP**）、Cloud Security Alliance（**CSA**）、**PCI Data Security Standard**、**NIST 800-53**、**SANS Critical Security Controls**、および**ISO 27002**のガイダンスに基づくものです。



**CS-3.11**

**ページ 33**

**CS-3.6、CS-3.7、CS-3.8、CS-3.9、CS-3.10**

**ページ 32**

**CS-3.0、CS-3.1、CS-3.2、CS-3.3、CS-3.4、CS-3.5**

**ページ 31**

**データ**

**セキュリティ**

**CS-2.5、CS-2.6**

**ページ 30**

**CS-2.0、CS-2.1、CS-2.2、CS-2.3、CS-2.4**

**ページ 29**

**業務**

**CS-1.16、CS-1.17**

**ページ 28**

**CS-1.13、CS-1.14、CS-1.15**

**ページ 27**

**CS-1.6、CS-1.7、CS-1.8、CS-1.9、CS-1.10、CS-1.11、CS-1.12**

**ページ 26**

**CS-1.0、CS-1.1、CS-1.2、CS-1.3、CS-1.4、CS-1.5 ページ 25**

**会社と管理**

**クラウド セキュリティ**

**安全なコーディングと脆弱性管理**

**AS-3.0**

**ページ 16-17**

**AS-3.1、AS-3.2、AS-3.3**

**ページ 17**

**AS-3.4**

**ページ 18-19**

**AS-3.5、AS-3.6**

**ページ 19**

**AS-3.7**

**ページ 20**

**AS-3.8**

**ページ 21-22**

**AS-3.9、AS-3.10、AS-3.11、AS-3.12**

**ページ 22**

**AS-3.13、AS-3.14**

**ページ 23**

**AS-3.15**

**ページ 24**

**AS-2.9、AS-2.10**

**ページ 15**

**AS-2.6、AS-2-7、AS-2.8 ページ 14**

**AS-2.5**

**ページ 13-14**

**AS-2.2、AS-2.3、AS-2.4 ページ 12**

**AS-2.1**

**ページ 11**

**AS-2.0**

**ページ 10-11**

**認証とアクセス**

**AS-1.1、AS-1.2、AS-1.3、AS-1.4**

**ページ 9**

**AS-1.0**

**ページ 7-8**

**開発**

**ライフサイクル**

**アプリケーション セキュリティ**

**IV. 書類の整理**

**ベストプラクティスは、プロバイダーにおける顧客コンテンツの保護能力査定の枠組みとなる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。本文書においては、モデルはアプリケーションセキュリティとクラウドセキュリティの二つの分野にわたるセキュリティ関連トピックから構成されます。MPAAコンテンツセキュリティ モデルの内容は、関連するISO標準（27001-27002）、各種セキュリティ標準（the Open Web Application Security Project [OWASP]、Cloud Security Alliance [CSA]、PCI Data Security Standard、NIST 800-53、SANS Critical Security Controlsなど）、および業界のベストプラクティスから引用されたものです。**

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。

**V. ベストプラクティスの書式**

|  |  |
| --- | --- |
| アプリケーション セキュリティ | クラウド セキュリティ |
| 開発ライフサイクル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。 | 認証とアクセス | 安全なコーディングと脆弱性管理  | 会社と管理 | 業務 | データセキュリティ |

**V. ベストプラクティスの書式**

| 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 |
| --- | --- | --- | --- |
| AS-2.7 | 認証とアクセス | CAPTCHA**または**reCAPTCHA**などの人的確認ツールと**ウェブアプリケーションを併用します | * ボットを防止するために、**CAPTCHA**または**reCAPTCHA**を使用します
 |

**用語集**

用語集に収録されているすべての言葉は**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追加的な検討事項、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。

**VI. ベストプラクティスのアプリケーションセキュリティ 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 |
| --- | --- | --- | --- |
| AS-1.0 | 開発ライフサイクル |  **システム/ソフトウェア開発ライフサイクル**（**SDLC**）全体にセキュリティを組み込みます。 | * 業界標準手法の使用を検討します：
	+ **ウォーターフォール**
	+ **高速アプリケーション開発**（**RAD**）
	+ **アジャイル**
* ソフトウェアのライフサイクルを規定し、ソフトウェア システムの開発、購入、設定のモデルを提供するプロセスを対象とする、**ISO/IEC 12207**の実装ガイダンスを指します
* **任務の分割**を行います:
	+ 要件/設計、構築、テスト、リリース、メンテナンスの各段階にわたり、すべてのプロセスとデータを文書化します。それには以下が含まれます：
* プログラム変更要請
* ユーザーを対象とする受容テストと承認
* 経営幹部の承認
	+ 開発およびテスト環境と制作環境を分離させます。アクセス コントロールを使って分離を実行します。
	+ 制作データが開発およびテスト環境で使用されていないことを確認します。
* 設計を始める前に、以下を含むシステム/ソフトウェアのリスク分析を行います。
	+ 予想される脆弱性と脅威を含む脅威モデル
	+ アプリケーション **セキュリティ**の専門家によるレビュー
	+ セキュリティとプライバシーの要件
	+ テスト範囲
* 安全なコーディング標準を使用します
 |
| AS-1.0続き | 開発ライフサイクル |  | * 変更コントロール**を実施します:**
	+ プロダクションに移行されたすべての変更を記録します
	+ プロダクションへの変更移行のためのアクセスを制限します
	+ 変更が行われた場合、もしくは、少なくとも四半期に一度テストを繰り返します
	+ 変更が及ぼす影響に基づき、バックアウトの手順を準備しておきます
* テスト実施：
	+ **SDLC**全体を対象にセキュリティのテストを行い、脆弱性、脅威、プライバシー関連の問題に対応します
	+ 自動テストと共に、手動によるテストを実施します
	+ 静的コード分析、動的コード分析を含む、自動セキュリティテストを実施します
	+ アウトソースされたソフトウェア開発活動を対象に、ソースコードにおけるセキュリティ上の欠陥を検知するためのコントロールを実装します
	+ あらゆる問題を是正します
* アプリケーション**コードの**詳細を、不正使用または開示されないように保護します：
	+ アカウンタビリティを確実にするため、特権をもつユーザーに対し個別の管理者アカウントを割り当てます
	+ すべてのユーザーのアクセス状況を、四半期に一度レビューします
	+ アプリケーションが**有効化される、もしくは顧客にリリースされる前に、**開発、テストおよび/またはカスタム**アプリケーション**のアカウント、ユーザーID、およびパスワードを削除します
	+ アプリケーション**／プログラム**／ソースコードへの不正アクセスを防止します。コードは権限のある者のみに制限します
	+ テナント**アプリケーション**、プログラム、またはオブジェクト ソースコードへの不正アクセスを防止し、アクセスが権限がある者にのみ制限されていることを確実にします
 |
| AS-1.1 | 開発ライフサイクル | 全アプリケーションとインフラを対象としてセキュリティのテストを実施します。 | * テスト範囲は、以下を確実に含むようにします：
	+ アプリケーションサーバー
	+ データベースサーバー
	+ サーバーのオペレーティング システム
	+ 仮想サーバーのコンポーネント
	+ ウェブサーバー（フロントエンドとバックエンド）
	+ エンタープライズ アーキテクチャのコンポーネント（例：サービス志向型アーキテクチャ）
* 変更が行われた場合、もしくは、少なくとも四半期に一度テストを繰り返します
 |
| AS-1.2 | システムに大量のランダムデータを入力して意図的にクラッシュさせることにより、ソフトウェア、オペレーティングシステム、またはネットワークにあるセキュリティの抜け穴を発見するために、**ファズテスト**および**欠陥の是正**を行います（**バッファオーバーフロー**、**クロスサイトスクリプティング**、**サービス妨害攻撃**、**フォーマットバグ**、**SQL インジェクション**など）。 | * 予想外の入力をテストします
* アプリケーションの反応を評価します
* 変更が行われた場合、もしくは、少なくとも四半期に一度テストを繰り返します
 |
| AS-1.3 | 大規模なブラックボックス テスト**、**ベータテスト**、おおよびその他の実証済みのデバッグ手法と併せて、**バグトラック**および欠陥の是正**を行います。 | * 機能上のエラーとセキュリティ上の脆弱性の両方について、バグレポートを入手します
* 欠陥を是正します
 |
| AS-1.4 | アプリケーションへの追加および変更に関するトレーニングとユーザーガイドを提供します。 |  |

| 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 |
| --- | --- | --- | --- |
| AS-2.0 | 認証とアクセス | 安全な**認証を導入します。s** | * ユーザー名／ユーザーID:
	+ 重複するユーザー名／ユーザーIDの使用を禁止します
	+ ユーザー名／ユーザーIDの共有、および同じユーザー名／ユーザーIDの同時使用を禁止します
	+ ユーザー名／ユーザーIDで大文字と小文字を区別するようにします
* 以下のようなパスワード コントロールを行います：
	+ 最小文字数を少なくとも8文字に設定します
	+ パスワードの最大文字数の使用を検討します
	+ 少なくとも次の5つの規則の3つを使用した、強力なパスワード設定を実施します
* 少なくとも1つの大文字（A-Z）
* 少なくとも1つの小文字（a-z）
* 少なくとも1つの数字（0-9）
* 少なくとも1つの特殊文字（句読点またはスペース）
* 同じ文字を2つ以上続けて使用しない
* 少なくとも10のパスワード履歴を保持し、再使用を禁止する
* 有効期限は最大90日
* 5〜10回パスワード入力に失敗したらユーザーアカウントをロックします。管理者が手動でロック解除するまで、アカウントをロックしておきます。
* 無活動状態が30分間続いたら、ユーザーを自動的にログオフします。使用しているかどうかに関わらず、ログイン状態が4時間続いたら、ユーザーをログオフするか、もしくは強制的に新規セッションを始めさせることを検討します。
* パスワードを安全な方法で保存します（テキスト形式にしない、パスワードの送信は**TLS**上でのみ行うなど）
* 重要度の高い機能に関しては、再**認証**を義務付けます
* **SSL** クライアント**認証**の使用を検討します
 |
| AS-2.0続き | 認証とアクセス |  | * ディレクトリーサービスを使用して**認証**を行います
* 複数要素**または**2要素**認証を使用します**:
	+ 自分が知っている何か（アカウントの詳細またはパスワード）
	+ 自分が持っている何か（トークンまたはスマートフォン）
	+ 自分に関する何か（バイオメトリクス）
* ユーザーおよびユーザーのアクセス許可を自動的に開始、把握、記録、管理するために、身元証明およびアクセス管理（**IAM**）システムの導入を検討し、以下のことを確実にします:
	+ 特権はポリシーの解釈に基づいて与えられる
	+ すべての個人とサービスは、適切に認証、承認、監査される
 |
| AS-2.1 | ユーザーのデバイスを登録します。 | * アプリケーションのユーザーが使用するデバイスを、以下のような方法で登録します（以下の方法に限定されない）：
	+ デバイスIDまたはハードウェアID
	+ **IMEI**（International Mobile Equipment Identity）番号または**MEID**（Mobile Equipment Identifier）番号
	+ **MAC**（Media Access Control）**アドレス**
* 認証プロセスの間に、ユーザーが使用しているデバイスを登録デバイスのリストに照らしてチェックします
* ユーザーが安全に新しいデバイスを登録できるようにするため、複数要素の**認証**を使用します（一回のみの使用が可能な帯域外のパスワード、スマートフォンのPINなど）
* 実際的である場合は、ユーザーアカウントを一つまたは二つのユーザーデバイスに固定することを検討する
* ユーザー一人当たりのデバイスの数を限定することを検討します（デバイスは、ユーザー一人あたり最大5つまでなど）
* ユーザーが複数のデバイスで同時にセッションを開始しないようにします
 |
| AS-2.2 | 認証とアクセス | パスワードの回復を安全に行います。 | * 以下のステップを検討します：
	+ ユーザーが作成した質問、よくある質問、または身元確認データに関する質問（プライバシーへの配慮をすること）を収集します
	+ 質問に対する答えについて、最低の長さを設定します
	+ セキュリティに関する質問と答えを確認します
	+ 質問と答えのためのストレージシステムを設計します
	+ ユーザーに、定期的に質問と答えをレビューおよび更新させることを検討します
	+ スマートフォンに送信されるピンなど、サイドチャネルを使うことなどを行って、質問の変更要請を認証します
	+ ユーザーのアカウントを即座に探し出し、サイドチャネルでトークンを送信します
	+ ユーザーが既存のセッションでパスワードを変更できるようにします
	+ ソーシャルエンジニアリング**を阻止する**パスワード回復のプロセスをテストします
	+ セキュリティの質問リストに、LinkedInやFacebookのようなインターネットのウェブサイトを通してアクセス可能な、学校、生年月日、旧姓、その他の記録に関する質問が含まれていないことを確認します。
 |
| AS-2.3 | 最低レベルの特権を基準とする原則に従います。 | * アプリケーションは、特権のあるアカウントではなくユーザーアカウントを使用し、存在する最も低いレベルの許可に基づいて実行します
* アプリケーションを、システムまたは管理者レベルの許可に基づいて実行することを禁止します
 |
| AS-2.4 | 容赦ない攻撃を阻止するためのコントロールを実装します。 | * 間違ったパスワードによるアクセスの試みが設定された回数を超えた場合、そのユーザーアカウントをロックアウトします。5～10回を限度とすることを検討します。
* 管理者が手動でロック解除するまで、ユーザーアカウントをロックしておくことを検討します
 |
| AS-2.5 | 認証とアクセス   | キー／暗号化ストレージを保護するプロセスを導入、文書化し、継続的な安全管理を確実にします。 | * 維持する必要がある重要なデータのみを保存します
* データを保存する際は、プライバシーに関する問題を検討します
* テナントが生成した**暗号化**キーをサポートするか、もしくは、テナントが公開鍵証明にアクセスせずに、識別子にデータを暗号化することを許可します（IDベース**暗号**など）
* 強力な暗号化アルゴリズムのみを使用します（**AES**、RSA公開鍵暗号、SHA-256かそれ以上など）
* 弱いアルゴリズムを使用しないこと（MD5かSHA1など）
* 暗号化の観点から、ランダムに生成された数字（ファイル名またはGUIDなどで使用）が強いことを確認します
* 広範に受け入れられている暗号化アルゴリズムのみを使用します（NIST FIPS 140-2を参照）
* パスワード自体ではなく、ハッシュ化し、ソルトを使用したパスワードの値を保存します。
* 暗号化のストレージ保護は、最初のコントロールに失敗した場合でも安全であることを確実にします（暗号化データを常に静止状態にしておくなど）
* 秘密鍵（シークレットキー）が、不正アクセスから確実に保護されるようにします
* キーのライフサイクルを明確にします：
	+ ライフサイクル全体を通したキーの取扱い手順を文書化します
	+ キーのセキュリティ侵害対応の手順を文書化します
	+ 手動でキーを配布するのではなく、中央集中化された自動**キー管理**アプローチを導入します
	+ キーは**保管庫**で保護します
	+ キーは暗号化に使うデータから離れた場所に保管します
	+ キーはアプリケーションサーバー、ウェブサーバー、データベースサーバーなどの上に保管しないようにします
 |
| AS-2.5続き | 認証とアクセス |  | * + テナントごと、場合によってはプロジェクトごとに固有の**暗号化**キーを作成することを奨励します
	+ キーは定期的に、少なくとも1～3年に一度は変えます
	+ 少なくとも1～3年に一度はデータのキーを変えます
	+ **キーの作成**、管理および使用の任務を分割します
	+ キーの管理者に、関連する任務と責任に関するフォームに署名することを義務づけます
	+ キーの配布には、安全な方法のみを使用します（**TLS**など）
	+ 複数のキーが必要な場合は、別個のキーを使用します（例：第一のキーと関連するような第二のキーを選択しない）
	+ 未承認の代替キーを阻止します
 |
| AS-2.6 | ユーザーが設定した期間が過ぎた後は、すべての外部からのコンテンツへのリンクが期限切れとなる、自動終了設定を有効化します。 | * 24時間でリンクが期限切れとなるデフォルトの設定を有効化します
 |
| AS-2.7 | CAPTCHA**または**reCAPTCHA**などの人的確認ツールと**ウェブアプリケーションを併用します。 | * ボットを防止するために、**CAPTCHA**または**reCAPTCHA**を使用します
 |
| AS-2.8 | クライアントが、特定ユーザーによる資産のダウンロードまたはストリーミングの可能回数を限定できるようにします。 |  |
| AS-2.9 | 認証とアクセス | すべてのコンテンツと重要な資産のアップロードとダウンロードを確認します。 | * コンテンツがアップロード、ダウンロード、または閲覧された場合は、毎回、コンテンツの所有者、プロジェクトの所有者、またはプロジェクトマネージャーに即座に電子メールを送ります
* 以下の詳細情報を含むこと：
	+ すべての活動の正確なタイムスタンプ
	+ アクセス規則に基づくダウンロード／ストリーミングの試み（成功と失敗の両方）
	+ フォレンジック情報（**IP**または**MACアドレス**、**位置**情報など）
	+ 資産ごと、ユーザーごとのダウンロード／ストリーミング回数
 |
| AS-2.10 | デバイスのパスワードおよび、リモートワイプとデバイスの位置確認ソフトウェアを有効化するためのリマインダーとして、ユーザーのモバイルアプリケーションに送信する簡単なメッセージを含めます。 | * ユーザーに**Find My iPhone**、**Android Device Manager**などの位置確認およびリモートワイプのツールをインストールするよう喚起します
* **モバイルデバイス管理**システムをインストール、設定、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 |
| --- | --- | --- | --- |
| AS-3.0 | 安全なコーディングとシステム | 制作開始前、および、その後少なくとも四半期に一度、**侵入テスト**／**ウェブアプリケーションテスト**を実施します。再テストにより脆弱性が是正されたことを確認します。 | * サイバーセキュリティの業界標準ツールを使用します
* **OWASP**トップテンをテストします:
	+ A1 インジェクション（SQL、OS、LDAPを含む）
	+ A2 XSS
	+ A3 弱い**認証**および**セッション管理**
	+ A4 安全でない直接的なオブジェクトの参照
	+ A5 クロスサイトリクエストフォージェリ
	+ A6 セキュリティの不適切な設定
	+ A7 不十分な暗号化ストレージ
	+ A8 **URL**アクセス制限の失敗
	+ A9 トランスポート層の不十分な保護
	+ A10 有効性が確認されていないリダイレクトおよび転送
	+ 以下で更新情報を参照のこと: https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project
* バッファオーバーフロー**のテスト**
* 不適切な**エラー対応**のテスト
* **URL**アクセス制限失敗のテスト
* ディレクトリトラバーサル**のテスト**
* 変更が行われた場合、もしくは、少なくとも四半期に一度、社内および独立業者によるテストを繰り返します
* 四半期に一度、および変更が行われた際に、独立業者によるテストを実施します
* 自動テストと手動テストを組み合わせて、以下などをテストします（以下に限定されない）：
	+ インタラクティブなインラインのプロキシ
	+ **ヒープ**および**スタック・オーバーフロー**の検出
	+ **認証**の不安定さ
	+ ユーザー一覧表
	+ **入力検証**
	+ 日付の脱構築または改ざん
 |
| AS-3.0続き | 安全なコーディングとシステム |  | * 自動テストと共に、手動によるテストを実施します
* ウェブのフロントエンド、バックエンド、および関連するすべての接続箇所のテストを実施します 発見された正当な問題点は、調査後、即座に是正します：
	+ 重要: 即座の是正が必要
	+ 高: 即座の是正が必要
	+ 中程度: アプリケーションの次回の定期リリースで是正が必要
	+ 低: 相互で合意できるスケジュールで、是正に対応するための予定が必要
 |
| AS-3.1 | 少なくとも四半期に一度、脆弱性テストを実施します。 | * サイバーセキュリティの業界標準ツールを使用します
* 変更が行われた場合、もしくは、少なくとも四半期に一度テストを繰り返します
* 独立業者によるテストを実施します
* 発見された問題点は、調査後、即座に是正します
* ウェブのフロントエンドとバックエンドのサーバー、および関連するすべての接続箇所のテストを実施します
 |
| AS-3.2 | クッキー**を使用する必要がある場合は、安全な方法で**利用します | * クッキー**は**ハッシュ**するのではなく、暗号化します**
* **HttpOnly**設定を使用します
* クッキー**は**個別アプリケーションに限定します
* クッキー**は**個別セッションに限定します
 |
| AS-3.3 | ユーザーの入力を確認し、**安全なエラー対応方法を導入します。** | * すべての入力を確認します
* すべての入力をサニタイズします
* ユーザーの不適切な入力に対しては、安全保持エラーのメッセージで対応します。すなわち、悪意あるユーザーが使うことでシステム攻撃を容易にする可能性のある情報を渡さないようにとのメッセージを送ります
 |
| AS-3.4 | 安全なコーディングとシステム | 安全なロギング手順を導入します。 | * 少なくとも次のイベントを記録します：
	+ **入力検証**の失敗
	+ アウトプット検証の失敗
	+ **認証の**成功と失敗
	+ **承認**（アクセスコントロール）の失敗
	+ **セッション管理**の失敗（クッキーセッションの特定値の変更など）
	+ アプリケーションエラー
	+ システムエラーとイベント
	+ アプリケーションとシステムの起動、終了、中断、ロギング初期化
	+ 高リスク職務の使用（管理者および開発者など）
	+ 法的およびその他のオプトイン
	+ すべてのコンテンツとクライアントフォルダー／ファイルイベント
	+ あらゆる種類のキーの取扱い
	+ システムレベルのオブジェクトの作成と削除
	+ **ジオロケーション**ブロッキング
* 次の属性を記録する：
	+ いつ（日付と時間など）
	+ どこで（アプリケーション識別子、アプリケーションアドレス、**地理的位置**、エントリーポイント、コードの位置など）
	+ 誰が（ソースアドレスまたはユーザー識別子など）
	+ 何を（イベントのタイプ、重大性、イベントフラッグ、および説明、成功・失敗の結果表示など）
 |
| AS-3.4続き | 安全なコーディングとシステム |  | * 監査ログを改ざんされないよう保護します：
	+ 静止状態：
* 改ざん検出機能を組み込みます
* 出来るだけ早くログを読み出し専用媒体に保管またはコピーします
* ログへのすべてのアクセスを記録、モニターします
* ログの特権を頻繁にレビューします
	+ 送信中：
* 安全な送信プロトコルを使用します
* イベントデータの情報源の確認を検討します
* 送信中のデータが本当に暗号化されていることを確認します
* ログは、少なくとも2年間保存します
 |
| AS-3.5 | 多種多様なログを集積して分析するために、**SIEM** （Security Information Event Management System） を導入します。 | * 以下を含む**SIEM**を実装します:
	+ サーバー、システム、アプリケーション、インフラデバイスからのデータ／イベントログを集積する、一元化されたイベントログポジトリ
	+ 複数の単独セキュリティイベントを、一つの関連したセキュリティ インシデントに自動的に関連付ける機能
	+ 緊急を要する問題を、ダッシュボードおよび／または電子メールでセキュリティチームに通報するアラート
	+ 既存のログデータがアラートなしで決して変更できないようにするための（ただし、追加された新しいデータに対してはアラートを発生させない）、ログを対象とするファイルの完全性モニタリングまたは変更検出ソフトウェア
	+ 二つの異なる場所から同じアカウントに同時にログインしたことを知らせるアラート
 |
| AS-3.6 | 静止状態にあるすべてのコンテンツとクライアントデータを暗号化します。 | * **AES**-256 以上を使用する
* モバイルアプリケーション上のすべてのコンテンツを暗号化します
 |
| AS-3.7 | 安全なコーディングとシステム  | 送信中のすべてのコンテンツとクライアントデータを暗号化します。 | * 以下を検討します：
	+ **トランスポート層セキュリティ（TLS）を使用すること:**
* すべてのログインページと認証されたページに**TLS**を使用すること
* 重要なコンテンツを送信する場合は**TLS**を使用すること
* 安全なコンテンツに**TLS**が使われなかったページを入れないこと
* 強力なプロトコルのみをサポートすること：**TLS**1.0、**TLS**1.1および**TLS** 1.2
* 相互認証には、**TLS**-PSKおよび**TLS**-SRP**をサポートすること**
* **HTTP ストリクト トランスポート セキュリティ**を使用すること
* 安全な再交渉のみをサポートすること
	+ 証明書を導入します：
* アプリケーションのユーザーベースに対し、適切な証明権限を使用します
* 証明書では、完全に資格要件を満たす名前を使用します
* 要請されたドメイン名をサポートする証明書を使用します
* 万能型証明書を使用しないこと
* 証明書の中で**RFC 1918**（プライベート）アドレスを使用しないこと
* 常に、必要とされるすべての証明書を与えます
* 強力なキーを使用し、それを保護します
	+ 重要なデータをキャッシングしないようにします
	+ 圧縮機能を無効化します
	+ 重要なデータは**URL**から外します
 |
| AS-3.8 | 安全なコーディングとシステム | 安全な**セッション管理のためのコントロールを実装します。** | * セッションを安全に管理します：
	+ ユーザー名／ID、トークン、またはプログラミング言語やウェブアプリケーションに使用された技術など、不必要な詳細情報を明らかにしない安全なセッション名を使用します
	+ 容赦ない攻撃を阻止するため、十分な長さのセッションIDを使用します
	+ 予測不可能な、ランダムなセッションIDを使用します
	+ 可能な場合は、常に厳しい**セッション管理**を行います
	+ プロセスする前に、無効なセッションIDを確認し排除します
	+ 特権レベルに変更があった後は、セッションIDを新しいものに変えます
	+ セッションID交換機能を限定します（**クッキー**または**URL**パラメーターなど）
	+ すべてのセッションに、アイドル・タイムアウトを導入します
	+ すべてのセッションに、期限切れタイムアウトを義務付けます
	+ 手動によるセッション期限切れを含めます（ログアウトボタンなど） ウェブブラウザ ウインドウ上のイベント終了機能で、強制的にセッションをログアウトさせます
	+ 可能な場合は、常にウェブコンテンツのキャッシングを避けます
	+ 他の理由でキャッシングが必要でも、セッションIDを決してキャッシュしないこと
	+ ユーザーが同じコンピュータまたはデバイスを他と共有している場合、最初のログインのタイムアウトを使用します
	+ 同じユーザー名／ユーザーIDを使った、複数の同時セッションを許可しないこと
	+ ブラウザのクロスタブ セッションを無効化します
 |
| AS-3.8続き | 安全なコーディングとシステム |  | * クッキーが使用される場合、クッキーを安全に管理します
	+ クッキー**には、「安全な」属性を使用します**
	+ クッキー**には、「**HttpOnly**」の属性を使用します**
	+ クッキー**には、「ドメイン」の属性を使用します**
	+ クッキー**には、「パス」の属性を使用します**
	+ クッキー**には、非永続型の属性を使用します（「期限切れ」、「マックスエイジ」など）**
	+ 同じアプリケーションの中では、異なるパスまたはドメイン範囲に対して同じクッキー名を使うことを避けます
 |
| AS-3.9 | **SQL インジェクションを防止するためのコントロールを導入します** | * すでに用意されているステートメントを使用します
* 保管されている手順を使用します
* ユーザーからのすべての入力を避けます
* 環境内のすべてのデータベース アカウントに割り当てられた特権所有者の数を最小にします
* ホワイトリスト**を使用して**入力を確認します
 |
| AS-3.10 | 有効性が確認されていない**URL**リダイレクトおよび転送を防止するためのコントロールを導入します。 | * リダイレクトおよび転送の使用を避けます
* リダイレクトを使用しなければならない場合は、ユーザーが**URL**を入力することを禁止します
* ユーザーの入力が避けられない場合は、提供されたURLが正当なものであることを確認します
* URL**の入力を許可せざるを得ない場合は、ホワイトリスト**を使用して入力をサニタイズします
 |
| AS-3.11 | 可能な場合、匿名ネットワーク（**Tor**、**Freenet**、**Netshade**など）からの接続を阻止するためのコントロールを導入します | * 可能な場合、ユーザーの**IPアドレス**が匿名化されていたら、アプリケーションのどの部分への接続も一切拒否します
 |
| AS-3.12 | **IPアドレス**の漏えいを阻止するコントロールを導入します。 | * ユーザーの**IPアドレス**が、第三者アプリケーション（ソーシャルメディアなど）に漏えいすることを阻止します
 |
| AS-3.13 | 安全なコーディングとシステム | XSS（**クロスサイトスクリプティング**）を阻止するコントロールを導入します。 | * 許可されている場所以外では、決して信頼できないデータを挿入しないようにします
* 信頼できないデータをHTML要素から成るコンテンツに挿入する前に、「HTMLエスケープ」とします
* 信頼できないデータをHTML共通の属性に挿入する前に、「属性エスケープ」とします
* 信頼できないデータをJavaScriptデータ値に挿入する前に、「JavaScriptエスケープ」とします
* 信頼できないデータをHTML型のプロパティ値に挿入する前に、「CSSエスケープ」とし厳しい検証を行います
* **信頼できないデータをHTMLURL**パラメータ値に挿入する前に、「**URL**エスケープ」とします
* ライブラリを使用してHTMLマークアップをサニタイズします
* DOM-ベースのXSSを阻止します
* 可能な場合（JavaScriptを使用していない時など）は、**HTTPOnly**クッキーフラッグを使用します
 |
| AS-3.14 | 送信者が、コンテンツにセッションベースのフォレンジック（目に見えない）**透かし**を入れるオプションを与えます。 | * **ストリーミングされているコンテンツに透かし**を入れる
* **ダウンロードされているコンテンツに透かし**を入れる
* フォレンジック用の**透かし**が、スクリーンキャプチャおよび様々な質のカムコーダーで有効であることを確認します
* フォレンジック用の**透かし**が首尾よく読み出され、受領者が各々を特定できることを確認します
* フォレンジック用の**透かし**の強度を、定期的にテストします
 |
| AS-3.15 | 安全なコーディングとシステム | 正式な、文書化されたコンテンツ／資産ライフサイクルを導入します。 | * コンテンツ／資産には以下を含めます：
	+ 製作
	+ 編集されたバージョン
	+ 返品
	+ 保存
	+ 認定された廃棄／破壊
	+ 各段階の保管期間
 |

**VII. ベストプラクティスのクラウドセキュリティガイドライン**

| **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** |
| --- | --- | --- | --- |
| CS-1.0 | 会社と管理  | MPAAコンテンツ ベストプラクティス共通ガイドラインの遵守を義務付けます。アプリケーション セキュリティ、および**クラウド／分散環境**ガイドラインの中により厳しいコントロールがある場合は、より厳しいポリシーの方を優先させます。 | * 適用可能なガイドライン：
	+ MS-1からMS-12
	+ PS-1からPS-21
	+ DS-1からDS-15
 |
| CS-1.1 | 少なくとも年に一度、第三者によるセキュリティ監査を実施します（**SSAE 16 タイプ2**、**SOC 1**、**ISO 27000/27001**、MPAAなど）。 | * 監査は、標準「情報セキュリティ管理システム」のフレームワークに基づいて測定されなければなりません
 |
| CS-1.2 | 情報セキュリティ管理を対象とするセキュリティ業界のフレームワーク（ISO-27001、ISO-22307、CoBITなど）と一致する、セキュリティおよびプライバシーに関するポリシーを文書化し、導入します。 |  |
| CS-1.3 | インフラのすべてのコンポーネント（**ハイパーバイザー**、オペレーティングシステム**ルーター**、DNS サーバーなど）について、情報セキュリティのベースラインを文書化し、導入します。 | * セキュリティ ベースラインは、セキュリティ業界の標準に基づいてベンチマークされなければなりません
* 四半期に一度テストします
 |
| CS-1.4 | 会社の現行情報セキュリティ手順に沿った、従業員向けのセキュリティ手順を文書化し、導入します。 |  |
| CS-1.5 | すべての従業員、請負業者、第三者に対し、雇用プロセスの中で機密保持／守秘義務契約への署名を求めます。 |  |
| CS-1.6 | 会社と管理 | 第三者に機能またはサービスを委託する場合は、セキュリティを対象とする**デューデリジェンス**の実施のための手順を文書化し、導入します。 | * 文書レビュー（ 独立監査、ログ、コンプライアンス、**侵入テスト**の結果、および是正プランなど）
* セキュリティ コントロールの確認
* すべてのソフトウェア プロバイダーが、システム／ソフトウェア開発ライフサイクル（**SDLC**）のセキュリティに関する業界標準に従っていることを確認します
 |
| CS-1.7 | 事業にとって重要なタスクの**任務の分割**を文書化し、導入します。 | * **任務の分割**が不可能な場合は、それを補うコントロールを文書化します。必ず以下を含めます：
	+ **キー管理**
	+ アプリケーション**の変更コントロール**
	+ セキュリティ設定の変更管理
 |
| CS-1.8 | クライアントに、自分たちのコンテンツとデータがある場所に関する情報を提供します | * データ転送の方法に関する情報を提供します
* コンテンツとデータの所在場所／司法管轄区に関する情報を提供します
 |
| CS-1.9 | 政府または第三者からの、クライアントのデータ提出要請に対応するために、文書化された手順を作成します。 |  |
| CS-1.10 | データやその他のものが入っている容器のラベリング、取扱い、および安全確保のポリシーと手順を確立します。 | * 構造化されたデータラベリング標準に従います（**ISO 15489**、Oasis XML Catalog Specification、**CSA**データタイプ ガイドラインなど）
 |
| CS-1.11 | 保存およびバックアップされたコンテンツ／データを含む、コンテンツ／データを安全に削除するための手順を確立します。 | * 取扱いに注意を要するコンテンツ／データのスクラブに関する法的、規制上のすべての要件を遵守します
 |
| CS-1.12 | クライアントのコンテンツ／データが物理的に別の場所に移動される可能性があるシナリオを確立、文書化し、導入します。 | * たとえば、オフサイトにおけるバックアップ、ビジネス継続性のための障害迂回、複製など
* 移動はすべて、実施前に書面により開示します
 |
| CS-1.13 | 会社と管理 | 追加的な**キー管理**の機能、コントロール、ポリシーおよび手順を確立、文書化し、導入します。 | * 社外／公共ネットワークを通した顧客のコンテンツ／データの移動について、強力な**暗号化**（AS-3.6およびAS-3.7を参照）を実施します
* インフラのコンポーネントが公共ネットワークを通して相互にコミュニケーションをとる必要がある場合は、常に強力な**暗号化**を使います。プラットフォームと関連データは、少なくとも**AES**-256以上を使用して暗号化します
* **キーの作成**、管理および使用の任務を分割します
* 顧客のプロジェクトにおいて、従業員がキーの管理を許可されるかどうかを決めます。
* 顧客が、自身の**暗号化**キーを作成、コントロールすることを許可するかどうかを決める
* テナントごと、場合によってはプロジェクトごとに固有の**暗号化**キーを作成することを許可します
* **暗号化**キーのライフサイクルの各段階における所有者を記録します
* **暗号化**キーの管理に使用されるシステムを記録します
* テナントが作成した**暗号中化**キーに関するポリシーを文書化します
* ネットワーク内およびネットワーク間で転送している間、**ハイパーバイザ**インスタンス中、および静止中のデータを暗号化している間、データと仮想マシンのイメージを保護するために**暗号化**を使用します
* キーはクラウドに保存しないこと
 |
| CS-1.14 | すべてのポリシーと手順に関して従業員の研修を行います | * セキュリティとデータの完全性に関する法的責任について、管理者およびデータ担当者が必ず適切な教育を受けているようにします
 |
| CS-1.15 | セキュリティ／プライバシーに関するポリシーに重大な変更があった場合、それを顧客に通知するためのプロセスを確立します |  |
| CS-1.16 | 会社と管理 | 容認できるサービスレベル維持を確実にするため、求められるシステムのパフォーマンスを計画、準備、測定します。 | * 以下を検討します：
	+ サービスの可用性
	+ サービスの質
	+ 適合能力の計画
* 継続的なパフォーマンスのモニタリングを行います
 |
| CS-1.17 | システムまたはコンテンツへの不正アクセスが発生した場合に、**インシデント対応**および顧客への即時通知を行うための、追加的要件を作成し、維持します。 | * セキュリティ関連のインシデントが発生した場合の規則、および、顧客の責任事項と会社の責任事項を具体的に公表します
* 法執行機関の連絡窓口を明らかにしておきます
* 顧客の固有要件を、セキュリティ対応プランに組み込みます
* **SIEM**が個別の顧客データについて、必ず粒度の高い分析およびアラートができるようにします
* **インシデント対応**プランが、預かり責任者の連続性管理プロセスとコントロールに準拠していることを確認します
* **インシデント対応**プランの機能の中に、法的に許容されるフォレンジック データの収集および分析の活用を必ず含めるようにします
* 他の顧客データを凍結せず特定顧客データだけを対象として訴訟ホールド（特定期間からのデータを凍結する）を支援できる機能を備えます
* 法的召喚状に対応するためのデータを作成する場合、テナントデータを強制的に分離し、その正当性を保証する機能を備えます
* セキュリティ関連のインシデント データがある場合、顧客とどれを共有するかに関するポリシーを規定します
* 顧客にインシデントを知らせるための通知基準、およびプロセスを規定します
 |

| **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** |
| --- | --- | --- | --- |
| CS-2.0 | 業務 | データセンターの電気、ガス、水道などの公共サービスおよび環境状態を確保します。 | * モニター
* 維持
* 少なくとも年に一度テストします
 |
| CS-2.1 | データセンターの周辺、および物理的なセキュリティコントロールを確実にします。 | * 損害に対する物理的保護策を導入します（自然要因、自然災害、意図的攻撃など）
* 予想される自然または人的災害への対策を導入します
* 大きな環境リスクのインパクトをもたらす可能性／発生率が高い（洪水、竜巻、地震、台風、地政学的な不安定性など）場所にあるデータセンターを使用しないようにします
 |
| CS-2.2 | ビジネス継続性プランのための追加的要件を作成、文書化、維持します。 | * 電気、ガス、水道などの公共サービスの供給停止に備えた保護策を導入します
* 少なくとも四半期に一度、バックアップ、復旧、冗長性の仕組みをテストします
* 個別顧客のコンテンツとデータが修復されることを確実にするための、バックアップおよび復旧のオプションを導入します
* 全ての顧客資産の完全な目録を維持します
* 全ての重要なサプライヤー／ビジネス関係の完全な目録を維持します
 |
| CS-2.3 | 追加的な変更および設定コントロールを開発、文書化、維持します。 | * システムに認可されていないソフトウェアがインストールされることを制限、モニターするためのコントロールを導入します
* ポリシー／メタタグ（ TXT／TPM、VN-Tagなど）を通して、仮想マシンを特定する機能を導入します
* ポリシータグ／メタデータ／ハードウェアタグ／ハードウェアIDを通して、ハードウェアを特定する機能を導入します
 |
| CS-2.4 | 資産の所有者情報を含む、全ての重要資産の完全な目録を維持します | * 定期的に資産目録の数を数え、照合を行います
 |
| CS-2.5 | 業務 | 全ての重要なサプライヤー関係の目録を維持します |  |
| CS-2.6 | 顧客、パートナー、およびサービスプロバイダーとサービス内容合意書（**SLA**）を作成、維持します。 | * そこには、少なくとも以下を含めます：
	+ ビジネス関係および提供サービスの範囲
	+ 連絡窓口情報
	+ 顧客の**SLA** パフォーマンス（すなわち、アップタイム標準とサービスレベルのモニタリング）の継続的な可視化および報告:
* 顧客が実行可能なモニタリング
* システムのオーバーサブスクリプションに関するポリシー（ネットワーク、ストレージ、メモリ、I/Oなど）
* ダウンタイムに対する顧客への払い戻し
	+ 情報セキュリティ要件
* 複数テナントの環境における、テナント間でのデータ漏えい、または意図的／偶発的なセキュリティ侵害を阻止するためのポリシー
* 顧客に第三者による脆弱性および侵入評価実践を許可することに関するポリシー
* インシデント対応ポリシー
	+ 機能の復旧、回復に関するポリシーを含む、ビジネス継続性に関するポリシー
	+ 契約の期限切れ、または解約時のコンテンツ／データの取扱い
	+ 顧客に影響を与える、第三者または下請け業者との関係に関する情報
	+ 少なくとも年に一度、**SLA**の更新を行うことに関するポリシー
	+ シングルサインオン（SSO）のサポートに関するポリシー
	+ 以下を検討します：
* セキュリティ違反の報告要件
* 監査および施設現場調査を行う権利
 |

| **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** |
| --- | --- | --- | --- |
| CS-3.0 | データセキュリティ  | セキュリティ関連のインシデントが発生した場合、正当な理由で請求されたすべての関連ログを、分析のためにプラットフォームから簡単にエクスポートできるフォーマットで顧客に提供するためのプロセスを導入します。 | * **AES**-128 ビッド以上の**暗号化**を使用して、監査ログを転送します
 |
| CS-3.1 | 追加的な**認証**要素として、システムの地理的位置を使用する機能を提供することを検討します。 |   |
| CS-3.2 | 要請された場合は、顧客のコンテンツ／データが保管されている物理的位置／地理的場所のコントロール機能を提供します。 | * 顧客が自分のコンテンツ／データを置く地理的場所を決定できるようにします
* 顧客が、自分のデータが出入りして行き来できる地理的場所を特定できるようにします（データへのアクセスではなく保存されている場所に基づく法的管轄区を考慮できるようにするため）
* 顧客のコンテンツ／データが、特定された地理的境界線を決して超えないようにします
 |
| CS-3.3 | 制作以外のデータが、決して制作環境で複製されないための手順を確立します | * 制作以外のデータを制作データから分離させます
 |
| CS-3.4 | 顧客とのサービスの取り決めを終了する場合の公開手順を確立、文書化して実践します。これには、顧客との契約が終了したら、顧客のコンテンツ／データを扱う全てのコンピューティング システムをサニタイズする確約も含まれます。 | * コンテンツ／データの復元を不可能にするような削除ソリューション、または破壊プロセスを導入する（物理的破壊、消磁／暗号化による削除、ライセンスの取り消しなど）
* 機器の再使用に関するポリシーを策定します
 |
| CS-3.5 | 資産タイプ別に分類された、会社施設外で使用される機器を安全に処分するためのポリシーと手順を確立し文書化します。 | * 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**を参照してください
 |
| CS-3.6 | データセキュリティ  | 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（NTPなど）を導入します。 | * 少なくとも、二つの独立した時間ソースの導入を検討します
 |
| CS-3.7 | 信頼できる接続と信頼できない接続の間のトラフィックを制限、モニタリングするためのネットワークおよび仮想環境を設計、設定します。 | * 少なくとも年一度、これらの設定をレビューします
* インフラ全体を文書化します
* すべての文書を定期的に更新します
* ネットワーク内のセキュリティドメイン／ゾーン間で許可されたアクセス／接続を定期的にレビューします
 |
| CS-3.8 | 複数テナント用のアプリケーション、システム、およびコンポーネントを、顧客のコンテンツとデータが適切に分割されるような形で設計、開発、導入します。 | * 以下に対応するための、データ管理ポリシーと手順を含めます：
	+ 不正監査
	+ テナントデータへの不正アクセスを発見するための、ソフトウェア インテグリティ機能
 |
| CS-3.9 | 物理的サーバー、アプリケーションおよびコンテンツデータを仮想サーバーへ、または仮想サーバーからそこへ移動する場合は、安全な暗号化されたコミュニケーション チャネルを使用します。 |  |
| CS-3.10 | 異常な侵入／退出トラフィックパターンに関連するネットワークベースの攻撃（NAC偽装やARPポイスニング攻撃および／またはDDOS攻撃など）を検出しタイムリーに対応するために、技術的な対策を導入し、徹底した防御テクニック（パケットの詳細分析、トラフィック制限、ブラックホールなど）を使用します。 |  |
| CS-3.11 | データセキュリティ | 仮想環境を保護するためのコントロールを確立し、文書化します。 | * 仮想分離を管理できるユーティリティの使用を制限し、モニターします
* 仮想インフラを直接標的にできる攻撃（シミング、ブルーピル、ハイパージャンピングなど）を検出するためのシステムを導入します
* 仮想インフラの攻撃を阻止するための、技術的コントロールを導入します
* 実行状態に関わらず、仮想マシンのイメージに加えられた変更をコントロールします
* すべての**ハイパーバイザ**管理機能または管理コンソールは最低レベルの特権の原理に基づき制限し、追加的な技術的コントロール（複数要素の**認証**など）を通して支援します
* ポリシータグまたはメタデータ（タグはゲストオペレーティング システムがブート処理／インスタンス作成／間違った国でのデータ転送するのを制限するために使用できるなど）を通して、仮想マシンを特定する機能を導入します
 |

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（NISTなど）、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、または256ビットのキー長さを使用するNIST対称キー**暗号化**標準。 |
| **アジャイル**  | アジャイルソフトウェア開発は、自発的に組成された機能横断型チーム間のコラボレーションを通して、要件とソリューションが次第に形成される一連のソフトウェア開発手法です。そこでは適応的プランニング、進化的開発、早期デリバリー、継続的改善が促進され、迅速かつフレキシブルに変更に対応することが奨励されます。 |
| **Android デバイスマネージャー** | ユーザーが遠隔で自分のAndroid デバイスを追跡、位置確認し、そこにあるデータ削除ができるコンポーネント。 |
| **アプリケーション** | アプリーションソフトウェア（*アプリケーション*）とは、ユーザーが、相互に協調的に作用するユニットとなった機能、タスク、またはアクティビティを実行できるよう設計された一連のコンピュータプログラムです。アプリケーションソフトウェアはそれ自身では実行できず、それを実行するシステムソフトウェアに依存します。 |
| **認証** | 単一のデータまたはエンティティの属性が真実であることを確認する行為。本人確認は、人やモノのアイデンティティを証明するための表明または示唆を行う行為を指すのに対し、認証は実際にそのアイデンティティを確認するプロセスを指します。多くの場合、認証は少なくとも一種の身分証明の信頼性の確認を含みます。 |
| **承認** | 承認とは、情報セキュリティおよびコンピュータ セキュリティ一般に関連するリソースへの**アクセス権**、特にアクセスコントロールへのアクセス権を特定する機能です。より正式には、「承認する」とは、アクセスに関するポリシーを規定することです。 |
| **ベータテスト** | ベータテストはアルファテストの後に行われるもので、外部ユーザーを対象とする受容度テストの一形態と言えます。ベータバージョンと呼ばれるソフトウェアのバージョンは、ベータテスターと言われる、プログラミングチーム以外の限定された対象者にリリースされます。ソフトウェアは、さらなるテストによって製品に間違いやバグがあまりないことを確認するために、いくつかのグループにリリースされます。 |
| **ブラックボックステスト** | ブラックボックステストは、内部構造や機能を詳しく見ずにアプリケーションの機能性を検査するソフトウェアのテスト手法です。この手法は、ユニット、インテグレーション、システムおよび受容など、事実上、ソフトウェアにおけるテストのあらゆるレベルに適用することができます。 |
| **バグトラッキング** | バグトラッキング システムもしくは欠陥トラッキング システムとは、ソフトウェア開発プロジェクトの中で報告されるソフトウェアのバグを追跡するソフトウェアアプリケーションです。 |
| **バッファオーバーフロー** | コンピュータのセキュリティとプラグミングにおけるバッファオバーフロー（もしくは、バッファオバーラン）とは、バッファにデータを書いている途中に、プログラムがバッファの境界を超えて隣接するメモリ上に上書きしてしまうという異常な状況です。これは、メモリの安全性違反の特別ケースです。 |
| **CAPTCHA** | **CAPTCHA**（「**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part」の頭字語）は、ユーザーが人かどうかを判断するためにコンピューティングで使用される、チャレンジ−レスポンス型テストの一つです。 |
| **変更コントロール** | 品質管理システム（QMS）と情報技術（IT）システム内での変更コントロールは、製品またはシステムへの変更が、管理、調整された方法で行われたことを確実にするために使用される正式なプロセスです。 |
| **クラウド／分散環境** | クラウド コンピューティングは、コンピュータリソースのユーティリティおよび消費モデルに基づくものです。クラウドコンピューティングは、クラウド内で実行されるアプリケーション ソフトウェアと、インターネット対応のデバイスを通して実行されるアプリケーション ソフトウェアを含むことができます。クラウドコンピューティングは、以下の3つのタイプのサービスを提供します：1）インフラストラクチャ・アズ・ア・サービス（IaaS）、2）プラットフォーム・アズ・ア・サービス（PaaS）、3）ソフトウェア・アズ・ア・サービス（SaaS）。IAASには、仮想マシン、サーバー、および/またはデータストレージが含まれます。PAASには、データベース、開発環境、およびウェブサーバーが含まれます。SAASには、電子メールや仮想デスクトップなどのアプリケーションが含まれます。クラウドは、パブリック、プライベート、またはハイブリッドに分類することができます。パブリッククラウドは、一般人にサービスを提供します。プライベートクラウドは、一つの企業だけが利用できるものです。ハイブリッドクラウドは、二つ以上の異なるクラウドが一つにされたものです（プライベートとパブリッククラウドなど）。 |
| **クッキー** | **認証**クッキーは、ウェブサーバーが、ユーザーがアカウントにログインしたかどうかを判断するために最も一般的に使われる手法です。このような仕組みがないと、サイトは重要な情報を含むページを送るべきか、もしくは、ユーザーに対し、ログインすることで自分自身を認証することを求めるべきかどうかが分かりません。一般に**認証**クッキーのセキュリティは、それを提供しているウェブサイトのセキュリティ、ユーザーのウェブブラウザ、およびクッキーデータが暗号化されているかどうかによって決まります。 |
| **クロスサイト スクリプティング** | クロスサイト スクリプティング（XSS）とは、通常ウェブアプリケーションの中に見られる、コンピュータセキュリティの脆弱性の一種です。XSSは、攻撃者が他のユーザーが閲覧したウェブページの中に、クライアント側のスクリプトを挿入することを可能にします。 |
| **CSA** | クラウドセキュリティアライアンス（CSA）は、「クラウドコンピューティング内でのセキュリティを保証するためのベストプラクティスを推進し、他のすべての形態におけるコンピューティングを保護するために、クラウドコンピューティングの使用に関する教育を提供する」という使命をもつ非営利団体です。 |
| **欠陥の是正** | ソフトウェアのテスト段階で発見されたあらゆる欠陥を、コードが制作に移行される前に解決します。 |
| **サービス妨害攻撃** | コンピューティングにおけるサービス妨害（DoS）または分散型サービス妨害（DDoS）攻撃とは、意図されたユーザーが機械やネットワークリソースを利用できないようにする試みです。 |
| **デジタル資産** | バイナリーソースの形にフォーマットされた、あらゆる形態のコンテンツおよび/またはメディアで、使用権限も含まれます。 |
| **ディレクトリ トラバーサル** | ディレクトリ トラバーサル（別名パストラバーサル）は、ユーザーが供給した入力ファイル名のセキュリティ検証／サニタイジングが不十分であることが[悪用](http://en.wikipedia.org/wiki/Security_exploit)され、「親ディレクトリへの横断」を示す文字がファイルAPIにすり抜けてしまうときに発生します。この攻撃の目的は、アクセスを可能にすることを意図していない[コンピュータファイル](http://en.wikipedia.org/wiki/Computer_file)へのアクセスを、アプリケーションに命令することです。この攻撃は、コードに含まれるバグの攻略と異なり、セキュリティの欠如（ソフトウェアの意図された動作）を攻略する。ディレクトリ トラバーサルには、the ../ （ドットドットスラッシュ）攻撃、[ディレクトリ](http://en.wikipedia.org/wiki/Directory_%28file_systems%29)クライミング、およびバックトラッキングのような別名があります。この攻撃の形態の中には、[正規化攻撃](http://en.wikipedia.org/wiki/Canonicalization)であるものもあります。 |
| **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。 |
| **暗号化** | 認可のない人には簡単に理解できない暗号文と呼ばれる形式にデータを転換すること。 |
| **エラーの取扱い**  | エラーまたは例外の取扱いとは、コンピューティングの途中で発生した*例外*（特別な処理が必要となる異常または例外的状態）に対応するプロセスで、多くの場合、正常なプログラム実行のフローを変更します。これは、特別なプログラム言語構成、またはコンピュータのハードウェア機構によって実施されます。 |
| **Find My iPhone** | Find My iPhone （[SpringBoard](http://en.wikipedia.org/wiki/SpringBoard)ではFind iPhone、また特定デバイスごとにFind My iPad、Find My iPod、またはFind My Macとも呼ばれる）は、iOSデバイスおよびMacコンピュータの位置を遠隔で追跡できるサービスで、Apple Inc. が提供するものです。 |
| **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。 |
| **フォーマットバグ** | コントロールされていない書式文字列は、セキュリティ上の弱点を突くために使用できるソフトウェアの脆弱性のひとつです。書式文字列を悪用して、プログラムのクラッシュまたは有害なコードを実行することができます。 |
| **フリーネット** | 情報の保存と送信のために分散化されたデータストアを使用する、ピア・ツー・ピアのプラットフォーム。ウェブ上での出版とコミュニケーションのための、無料ソフトウェアのスイートが使われています。 |
| **ファズテスト** | ファズテスト（別名ファジング）は、コンピュータのプログラムに無効、予想外、またはランダムなデータを入力して行うソフトウェアのテスト手法で、多くの場合、自動または半自動で実施されます。 |
| **ジオロケーション** | ジオロケーションは、携帯電話やインターネット接続されたコンピュータ端末などの対象物がある、実際の地理的位置を特定するものです。 |
| **ヒープオーバーフロー** | ヒープオーバーフローとは、ヒープデータ領域で発生する**バッファ・オーバーフロー**の一種です。ヒープオーバーフローは、スタックベースのオーバーフローとは異なる方法で悪用できるものです。ヒープ領域上のメモリは、ランタイムにアプリケーションが動的に割り当てるもので、通常、プログラムデータが含まれています。アプリケーションが、リンクされたリストポインタなど内部構造で上書きするようにさせる特定の方法によりこのデータを破壊することで、セキュリティー上の弱点を突きます。正規化ヒープオーバーフロー手法は、ダイナミックなメモリ割り当てリンケージ（マロック メタデータなど）に上書きするもので、操作の結果引き起こされたポインタ交換を使ってプログラムの機能ポインタを上書きします。 |
| **HTTPOnly** | HttpOnlyクッキー（または**HTTPS**）は、HTTPを通して送信される時にのみ使用可能です。JavaScriptのような、HTTP以外のAPIを通してアクセスすることはできません。この制限は**クロスサイト スクリプティング**（XSS）を通したセッションクッキー窃盗の脅威を緩和しますが、排除するものではありません。HttpOnlyクッキーは、現代のブラウザの大半がサポートしています。 |
| **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。 |
| **HTTPストリクト トランスポート セキュリティ** | HTTPストリクト トランスポート セキュリティ（HSTS）はウェブセキュリティに関するポリシーによる手法で、**HTTPS**ウェブサイトをダウングレート攻撃から保護するうえで必要です。これにより、クッキーをハイジャックから保護することが非常にシンプルになります。これによりウェブサーバーは、ウェブブラウザ（または、その他の準拠したユーザーエージェント）が安全な**HTTPS**接続によってのみ、サイトとのやり取りを行わねばならず、安全でないHTTPプロトコルを通したやり取りは行わない旨を明らかにすることができます。 |
| **ハイパーバイザー** | ハイパーバイザー（別名virtual machine monitor ：VMM）は、仮想マシンを構築し、実行するコンピュータソフトウェア、ファームウェア、またはハードウェアです。 |
| **IAM** | 「アイデンティティ管理」（IdM）と「アイデンティティおよびアクセス管理」（またはIAM）の用語は、アイデンティティ アクセス管理の分野で互換的に使用されますが、アイデンティティ管理自体はITセキュリティの中に含まれるものです。アイデンティティ管理（IdM）は、セキュリティおよび生産性を向上させると共に、コスト、ダウンタイム、重複作業を減らすために、システムおよび企業内、またはシステムおよび企業間における個人の責任者、**認証**、**承認**および特権の管理について説明するものです。 |
| **IMEI** | The International Mobile Station Equipment Identity（IMEI）は、3GPP（すなわちGSM、UMTS、LTE）および[iDEN](http://en.wikipedia.org/wiki/IDEN)携帯電話、サテライト電話の一部を特定するために使われる、通常は固有に設定された番号です。通常は電話のバッテリーがある場所の内側に印刷されていますが、大半の電話では、ダイヤルパッドで**\*#06#**を入力すると画面に表示されるか、もしくは、スマートフォンのオペレーティングシステム上の設定メニューの中で、他のシステム関連情報と一緒に表示されます。 |
| **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。 |
| **入力検証** | 入力検証またはデータ検証は、プログラムがクリーンで正しく、かつ有用なデータに基づいて動作することを確実にするプロセスです。そこでは、しばしば「検証規則」「検証制約」「チェックルーティン」と呼ばれる所定の作業が行われ、システムに入力されるデータの正確性、有意性、およびセキュリティをチェックします。 |
| **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）。 |
| **ISO/IEC 12207** | ISO/IEC 12207 *Systems and software engineering — Software life cycle processes* は、ソフトウェアのライフサイクルプロセスにおける国際標準です。これは、ソフトウェアの開発および維持に必要とされるすべてのタスクを定義する*唯一の標準*となることを目指しています。 |
| **ISO 15489** | 以下の題名をもつ国際標準: 「Information and documentation – Records management」。 |
| **ISO 27000/27001** | ISO/IEC 27000は、以下の題名をもつ国際標準: *Information technology — Security techniques — Information security management systems — Overview and vocabulary****。***ISO 27001:2013 は、以下の題名をもつ情報セキュリティ標準: 「Information technology— Security techniques — Information security management systems — Requirements」。 |
| **ISO 27002** | ISO/IEC 27002は国際標準化機構（ISO）および国際電気標準会議（IEC）が出版した情報セキュリティ標準で、*Information technology – Security techniques – Code of practice for information security management*という題名のものです。 |
| **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。 |
| **ローカルエリア ネットワーク（LAN）** | 小さな物理的エリア（オフィスなど）を範囲とするコンピュータネットワーク。 |
| **MAC アドレス** | メディアアクセス コントロールアドレス（MACアドレス）とは、物理的ネットワークのセグメント上でコミュニケーションを行うために、ネットワークのインターフェースに割り当てられた固有の識別子です。MACアドレスは、イーサネットおよび[WiFi](http://en.wikipedia.org/wiki/WiFi)を含む、ほとんどのIEEE 802 ネットワーク技術で、ネットワークアドレスとして使用されています。必然的にMACアドレスは、OSI参照モデルのメディアアクセス コントロールプロトコルの副層で使用されます。 |
| **MEID**  | 携帯機器識別番号（MEID）とは、物理的なCDMA移動端末機器を特定する全世界で固有の番号です。番号の形式は3GPP2レポートS.R0048で明らかにされていますが、実質的にはIMEIとして見ることができます。ただし、これは十六進の数字で表記されます。 |
| **モバイルデバイス管理** | モバイルデバイス管理（MDM）は、スマートフォン、タブレット型コンピュータ、ラップトップ型およびデスクトップ型コンピュータなどのモバイルデバイスの管理を指す業界用語です。通常MDMは、第三者が提供する、モバイルデバイスの特定ベンダー向けの管理機能を備えた製品を使って実施されます。 |
| **複数要素の認証** | 複数要素の**認証**（MFA）は、複数の異なる**認証**ステップで適切な提示をすることでユーザーが通過できるような、コンピュータへのアクセスコントロール手段です。 |
| **ネットシェイド** | ネットシェイドは、匿名のプロキシおよび**VPN**サーバーへのアクセスを可能にする、Mac OS XとiOS用のアプリケーションです。 |
| **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。 |
| **NIST 800-53** | NIST Special Publication 800-53である「Security and Privacy Controls for Federal **Information Systems** and Organizations」は、国家安全に関連するものを除く、すべての連邦**情報システム**を対象としたセキュリティコントロールのカタログを提供します。これは、米国商務省の非規制機関である米国標準技術局が出版するものです。 |
| **OWASP** | Open **Web Application Security** Project （OWASP）は、ウェブアプリケーションのセキュリティに特化したオンラインコミュニティです。OWASPコミュニティには、世界中の企業、教育機関、個人が参加しています。コミュニティは、無料で入手できる記事、手法、文書、ツール、技術の開発に努めています。 |
| **PCIデータセキュリティ標準**  | **Payment Card Industry Data Security Standard**（PCI DSS）は、Visa、MasterCard、American Express、DiscoverおよびJCBを含む、主要カード機構が発行するブランド名を冠したクレジットカードを取扱う機関を対象とした専有の情報セキュリティ標準です。主要カード機構の一部ではない自社ブランドカードは、PCI DSSの適用対象に含まれません。 |
| **侵入テスト** | 侵入テスト（略称ペンテスト）とは、セキュリティ上の弱点、潜在的に可能なシステムおよびその機能とデータへのアクセスを明らかにする目的で、コンピュータシステムに加える攻撃です。 |
| **高速アプリケーション開発（RAD）** | 高速アプリケーション開発とう用語は、一般にソフトウェア開発における従来型**ウォーターフォール**モデルの代替を指して使われると共に、James Martinの高速開発アプローチの名称として使われることもあります。一般にRADのソフトウェア開発アプローチは、計画段階のタスクにあまり重点を置かず、開発を重視します。これとは対照的に、**ウォーターフォール**モデルでは厳密な仕様と計画に重点がおかれます。 |
| **RFC 1918** | インターネット対応のアーキテクチャにおいて、プライベートネットワークは**IPアドレス**スペースを使用したネットワークで、RFC 1918がInternet Protocol Version 4（IPv4）およびRFC 4193 for Internet Protocol Version 6（IPv6）で制定した一連の標準に準拠します。通常これらのアドレスは、グローバルでルーティング可能なアドレスの使用が義務付けられていない場合、もしくは、それが意図されたネットワークアプリケーションで使用できない場合に、家庭、オフィス、および企業のローカルエリア ネットワーク（**LAN**）のために使用されます。 |
| **reCAPTCHA** | reCAPTCHAは、元々ピッツバーグにあるカーネギーメロン大学の本キャンパスでLuis von Ahn、 Ben Maurer、Colin McMillen、David Abraham、Manuel Blumが開発した、ユーザーダイアログ システムです。reCAPTCHAは、2009年9月にGoogleに買収されました。**CAPTCHA**インターフェース同様、reCAPTCHAはユーザーに対し、画面上で見える歪んだテキストイメージの入力を要請するものです。これは、二つの言葉を表示することで、ボットが制限された領域にアクセスしようとするのを阻止してウェブサイトを保護すると共に、書籍のテキストのデジタル化を支援します。 |
| **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。 |
| **SANS Critical Security Controls** | The Twenty Critical Security Controls for Effective Cyber Defense（通常、Consensus Audit Guidelines または CAGと呼ばれる）は、コンピュータセキュリティを対象とする、ベストプラクティスのガイドラインです。このプロジェクトは、米国の国防産業基盤における機関で起こった大規模なデータ喪失に対応するために、2008年初期に開始されたものです。この出版物は、SANS Instituteのウェブサイトにあります。 |
| **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。 |
| **セッション管理** | コンピュータサイエンス、特にネットワーキングにおいて、セッションとは、コミュニケーションを行う二つ以上のデバイスの間、もしくはコンピュータとユーザーの間で行われる、ほぼ恒久的なインタラクティブな情報交換（ダイアログとも呼ばれる）、会話、もしくは会議のことです。セッションは、一定の時点で設定または開設され、その後、いずれかの時点で解消されます。 |
| **シングルサインオン** | シングルサインオン（SSO）は、複数の関連しつつも相互に独立したソフトウェア システムのアクセスコントロールにおける属性です。ユーザーはこの属性を使って一旦ログインすると、各々のシステムへのログインを求められることなく、すべてのシステムにアクセスできます。通常これは、ライトウェイト ディレクトリ アクセスプロトコル（LDAP）およびサーバー上に保存されているLDAPデータベースを使用して行うことができます。 |
| **SLA** | サービス内容合意書（SLA）は、サービスが正式に定義されているサービス契約の一部です。サービスの範囲、質、責任などサービスの特定側面について、サービスプロバイダーとサービスのユーザーの間で合意されます。どのSLAにも見られるのは、契約納期（サービスまたはパフォーマンスの）です。 |
| **SOC 1 レポート** | [SOC 1](http://www.ssae-16.com/ssae-16/soc-1-report/)レポート（Service Organization Controls Report） は、ユーザー事業体の財務報告対する内部コントロールと関連するサービス組織におけるコントロールレポートです。SOC1 レポートは、おそらく標準SAS70だと考えたであろうものに、[Type I](http://www.ssae-16.com/ssae/ssae-16-type-i-report-background-information/) とType IIを加えたものですが、**SSAE 16**ガイダンスに準拠します。 |
| **ソーシャルエンジニアリング** | 情報セキュリティにおけるソーシャルエンジニアリングとは、心理的操作によって人に一定の行動をさせたり、機密情報を漏えいさせたりすることを指します。これは、情報収集、不正行為、またはシステムへのアクセスを目的とする信用詐欺の一種で、通常、より複雑な不正計画の中にある多くのステップの一つである、従来型のいわゆる「詐欺」とは異なります。 |
| **SQL インジェクション** | SQL インジェクションは、データ主導型アプリケーションを攻撃するために使われるコードインジェクション手法で、ここでは実行の際、悪意あるSQLステートメントがエントリーフィールドの中に挿入されます（データベースのコンテンツを攻撃者ダンプするなど）。SQL インジェクションは、アプリケーションのソフトウェアにセキュリティ上の脆弱性を悪用する必要があります。たとえば、ユーザー入力が誤ってSQLステートメントに組み込まれた文字列リテラル拡張文字として分類されたり、ユーザーが入力の際に強くタイプしなかったため突如実行されてしまったりというような場合です。 |
| **SSAE 16 タイプ 2** | **SSAE 16は、サービス提供組織におけるコントロールの報告を対象とした現行の標準であるSAS70を強化したものです。** |
| **SSL** | 定義は**TLS**を参照のこと。 |
| **スタックオーバーフロー** | スタックオーバーフローは、スタックポインタがスタックバウンドを超えた場合に起こります。コールスタックは限定された量のアドレススペースで構成されることがあり、多くの場合プログラムの最初に決定されます。コールスタックのサイズは、プログラミング言語、マシンのアーキテクチャ、マルチスレッディング、利用可能なメモリ容量などによって決まります。プログラムがコールスタックで利用可能なサイズ以上のスペースを使おうとした場合（つまり、コールスタックのバウンド以上のメモリアクセスを試みた場合で、これは基本的に**バッファオーバーフロー**となる）、スタックがオーバーフローしたと言われ、通常、プログラムがクラッシュします。 |
| **システム／ソフトウェア開発ライフサイクル（SDLC）** | システム開発ライフサイクルは、システムエンジニアとシステム開発者が**情報システム**の計画、設計、構築、テスト、納品のために使用する、明確に定義、区別された数多くの作業段階から構成されています。 |
| **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。 |
| **TLS** | **トランスポート層セキュリティ**（**TLS**）およびその前身である**セキュア ソケット レイヤー**（**SSL**）は、コンピュータネットワーク上でコミュニケーション セキュリティを提供するために設計された暗号化プロトコルです。そこではX.509証明書が使用されているため、コミュニケーションを行っている相手の認証と対称キーの交渉を行うための非対称暗号が使用されます。その後、このセッションキーは関係者間でやり取りされるデータを暗号化するために使用されます。 |
| **TOR** | Torは、匿名でコミュニケーションを行えるようにするための無料ソフトウェアです。この名称は、元のソフトウェアのプロジェクト名である*The Onion Router*の頭字語です。Torは、ネットワークの監視またはトラフィック分析を行っているすべての人の目からユーザーの所在位置と使用を隠蔽する6000以上のリレーから構成され、無料で全世界対応のボランティアのネットワークを通してインターネットのトラフィックを管理します。 |
| **2要素の認証** | 2要素の**認証**（別名2FA）は、2つの異なるコンポーネントを組み合わせることにより、明瞭なユーザー身分証明を実現します。これらのコンポーネントとしては、ユーザーが知っている何か、ユーザーが持っている何か、またはユーザーと切り離せない何かなどが使われます。2要素の**認証**は**複数要素の認証**の一種です。 |
| **URL** | ユニフォーム リソース ロケーター（URL）は、コンピュータネットワーク上にあるリソースの所在位置を特定するリソースの参照、および、それを読み出す仕組みです。多くの人はURLと統一資源識別子（Uniform Resource Identifier：URI）の2つの用語を互換的に使用しますが、URLはURIの中の特定のタイプです。URLは指示されたリソースへのアクセスの手段を意味しますが、それは、すべてのURIに当てはまることではありません。URLが最も一般的に使われるのはウェブサイトのページを参照する（http）場合ですが、ファイルの転送（ftp）、電子メール（mailto）、データベースへのアクセス（JDBC）など、他にも多くのアプリケーションで使用されます。 |
| **米国国防省 5220.22-M****（NISP Operating Manual）** | DoD 5220.22-M（別名NISP Operating Manual）は、機密情報に関し、すべての政府請負業者を対象とする標準手順と要件を制定したものです。NISP（National Industrial Security Program）は、民間業界が機密情報へアクセスするためのニーズを管理する、名目上の管轄機関となっています（米国内）。 |
| **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。 |
| **仮想ローカルエリア ネットワーク（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。 |
| **仮想プライベート ネットワーク（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。 |
| **ウォーターフォール** | ウォーターフォール モデルは、ソフトウェア開発プロセスで使用される、順次的に設計されたプロセスです。ここでは、開発の進展は、着想、開始、分析、設計、構築、テスト、製造/導入およびメンテナンスの各段階を通して着実に上から下へと進む流れとしてとらえられます。 |
| **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）。 |
| **ウェブ アプリケーション セキュリティ**  | ウェブ アプリケーション セキュリティは情報セキュリティから派生したもので、特にウェブサイト、ウェブアプリケーション、およびウェブサービスを対象として扱うものです。 |
| **ホワイトリスト** | ホワイトリストとは、特定の特権、サービス、モビリティ、アクセス、または承認を与えられた事業体のリスト、または登録一覧です。リストにある事業体は、容認、認可および/または承認されます。 |
| **ワイドエリア ネットワーク（WAN）** | 広範囲（例: 企業）に広がるコンピュータネットワーク。 |
| **進行中の作品（WIP）** | 最終の形とはみなされない作品や製品。 |

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 — よくある質問（FAQ）

1. **私のサービスプロバイダーは、提示されたすべてのベストプラクティスを実施しなければならないのですか？**

ベストプラクティスへの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. **私のサービスプロバイダーには、ベストプラクティスの「実施ガイダンス」のセクションにある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支援を意図したものです。プロバイダーがMPAAを使ってコンテンツセキュリティ査定を行う場合、弊社の査定では、当該時点において、プロバイダーの仕事状況と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、そ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、さらにMPAAメンバーが個別に設定したセキュリティ要件に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D — 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 |

コンテンツ保護地域と各国のオフィスに関する詳細は、 [www.mpaa.org/about/around-the-world](file:///C%3A%5CUsers%5Cramirezr.MPAA-DOM%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CTemporary%20Internet%20Files%5CContent.Outlook%5CZRFHOPRK%5Cwww.mpaa.org%5Cabout%5Caround-the-world)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**