EBU

OPERATING EUROVISION AND EURORADIO

R 143

邦訳：日本放送協会（NHK）
免責事項（Disclaimer）
本文書は原本にできるだけ忠実に翻訳するよう努めていますが、正確性を保証するものではありません。邦訳者は、本文書に記載されている情報により生じる損失または損害に対して、責任を負うものではありません。
原本は、EBU ウェブサイト(https://tech.ebu.ch/publications/r143)を参照ください。

メディアベンターのシステム、ソフトウェア、サービスに対する サイバーセキュリティ勧告

勧告書

バージョン 2.2

ジュネーブ

2021 年 4 月

このページは両面印刷を考慮し意図的に挿入しているページです。

メディアベンダーのシステム、ソフトウェア、サービスに対するサイバーセキュリティの勧告

EBU 委員会	初版	改訂	再発行
TC(技術委員会)	2016.3	2020.11 / 2021.4[1]	

キーワード： セキュリティ、サービス、インフラ、放送、IP、ソフトウェア、アプリケーション、サイバー、セキュリティコントロールアサーション（セキュリティ管理の適切な条件書）、ベンダー、脆弱性、認証、パスワード、暗号化、証明書、PKI、キー、ログ、インシデント

Recommendation（勧告）

EBU は、以下の点を考慮しています。

1. メディア事業者は、そのシステム、ソフトウェア、サービスを提供するために、ますますサードパーティを利用している。
2. プロダクションのワークフローとインフラは、一般的な IT 技術に急速に移行している。
3. サイバー脅威（マルウェアやランサムウェアなど）の実行が容易になり、継続的に進化している。
4. ネットワークに接続されたメディア機器のセキュリティは、ネットワークに接続しないクローズドな放送メディアの時代から引き継がれた低い閾値のままとなっている傾向がある。

メディア事業者に以下を推奨します。

1. システム、ソフトウェア、およびサービスを計画・設計する際に、「R 143 Security Controls Assertation」[2]および関連するガイダンスに記載されている安全保障措置を適用する。
2. 2. システム、ソフトウェア、およびサービスの潜在的なベンダーに対し、入札や技術要求に応じる際に、R 143 Security Controls Assertation（A 欄および B 欄に記入）および関連ガイダンスに準拠する能力があることを表明するよう求める。
3. 3. 潜在的なリスクを十分に認識した上で，この勧告に基づいて，ベンダシステムの最小許容レベルを定義する。

[R 143 は、付属書 A、B、C および「Security Controls Assertation（セキュリティ管理条件書）」から成っています]

---

[1] 本バージョン(2.2)は、誤記修正版です（IM-02、SM、AA-07 の XLS シートと附属書 A、B の間のテキストの整合性を改善)。

[2] 「Security Controls Assertation」は、本勧告の付属文書です。これは Excel のスプレッドシートで、本勧告の Web ページからダウンロードできます。

スプレッドシート完成ガイドライン

定義

製品： 組織が顧客に提供する製品、サービス、システムまたはソフトウェア。
組織/ベンダー： 製品、サービス、システムまたはソフトウェアを提供する潜在的なベンダー（下請業者を含む）。
顧客： 組織から製品を使用（購入）するユーザー

付属書 A および付属書 B のセクションは、セキュリティ・コントロール・アサーションのスプレッドシートに記入しなければならない要素に対応しています。スプレッドシートに正しく記入するために、これらの付属書をよくお読みください。

付属書 C は、参照の便宜を図るため、セキュリティ・コントロール・アサートのスプレッドシートを複製したものです。セキュリティ・コントロール・アサーションの記入は，EBU 技術ウェブサイトのこの勧告の発行ページからダウンロードできるエクセル・スプレッドシートに記入する必要があります。

付録 A：Vendor ISMS（Information Security Management System）

IS. Vendor ISMS：ベンダーの *ISMS*

IS-01 サイバーセキュリティポリシー

- ✓ **認知されたセキュリティ基準やフレームワークに沿い、文書化され、上級管理者によって承認されたサイバーセキュリティポリシー（または一連のポリシー）が存在すること。**
- ✓ 情報セキュリティポリシーは、組織のセキュリティプログラムの基礎となるものである。情報セキュリティポリシーは、以下の点を考慮して、組織が情報資産を保護する方法を定めたものでなければならない。

  機密性： 不正なアクセスから情報を保護すること。

  完全性： 情報が完全かつ正確であり、不正な方法で改ざん、変更、または破損されていないことを保証すること。

  可用性： 必要なときに適切な人が情報を利用できること。

- ✓ このポリシーは、組織のセキュリティプログラムに対する実行性を示すために、上級管理職によって承認され、署名されること。
- ✓ 認められているサイバーセキュリティのフレームワークや規格は数多くある（以下を含むが、これに限定しない）。ISO27001、米国国立標準技術研究所（NIST）、クラウドセキュリティアライアンス（CSA）、欧州連合サイバーセキュリティ機関（ENISA）、コンテンツ配信・セキュリティ協会（CDSA）、映画協会（MPA）。
- ✓ 組織が認証を受けている場合は、R 143 Security Controls Assertation を満たしている証拠の一部として、認証の証拠を提出する必要がある。
- ✓ **サイバーセキュリティポリシーが最新の状態に保たれており、関係者全員に効果的に伝えられている。**
- ✓ ポリシーは定期的に見直し、組織にとって適切、かつ効果的であることを確認する必要がある。
- ✓ ポリシーは、それを見る必要のあるすべての人に定期的に周知される。これは、対象となる利用者にとって適切、かつわかりやすい方法で行われるべきであり、また、アクセスが容易であるべき。

IS-02 効果的なサイバーセキュリティ組織

- ✓ **すべてのサイバーセキュリティの役割と責任が割り当てられ、関係者に周知されていること。**
- ✓ サイバーセキュリティの役割と責任は、サイバーセキュリティポリシーに沿って割り当てられること。
- ✓ **最高情報セキュリティ責任者（CISO）または組織内のサイバーセキュリティの総責任者が任命されていること。**
- ✓ CISO または任命された人物は、組織内で十分な上級職に就き、その役割を効果的に遂行できるだけの関連する経験を持つこと。
- ✓ **すべての従業員（契約社員を含む）に対して、それぞれの役割に関連したサイバーセキュリティ意識向上のためのトレーニングと教育を行うこと。**
- ✓ トレーニングには、最低限、情報保護とセキュリティ、パスワードとユーザーアカウントのセキュリティ、法律と規制

（GDPR など）が含まれること。

IS-03 監査計画

- ✓ **組織は、セキュリティ管理フレームワークの適合性と効果的な運用の定期的なレビューを確認するための監査手順を設けること。**
- ✓ サイバーセキュリティに対する組織のアプローチがその有効性と適合性について継続的に評価されていること、および改善または変更が特定された領域に対処していることを確認するために、定期的なレビューを実行すること。

OS. Operational Security：運用上のセキュリティ

OS-01 技術的なセキュリティ分析

- ✓ **製品やサービスの侵入テストや脆弱性テストなど、技術的なセキュリティ分析を定期的に行う。**
- ✓ 脆弱性スキャンは、システムやアプリケーションの脆弱性を特定する自動テストである。侵入テストは、脆弱性スキャンよりも踏み込んだ形で、弱点を特定するだけでなく、その弱点を利用した攻撃が可能かまで含めて行う。
- ✓ 顧客情報のセキュリティを維持するためには、システムのコンポーネント、プロセス、ソフトウェアを頻繁にテストする必要がある。これは、インフラストラクチャやインターネットに面したサービスに大幅な変更が加えられた場合には特に重要である。
- ✓ **このような侵入テストや脆弱性テストの結果は、顧客に提供すること。**
- ✓ 特定された脆弱性や弱点が修正され、残存するリスクが軽減されたことを顧客に保証しなければならない。

OS-02 脆弱性管理

- ✓ **脆弱性管理プロセスが存在し、特定された脆弱性とそれを修正するパッチを履歴管理すること。**
- ✓ 脆弱性管理プロセスは、脆弱性テストがどのくらいの頻度で実施されているか、また、特定された脆弱性を修正するためのパッチがどのように管理、実施されているかを顧客に示すものでなければならない。
- ✓ このプロセスでは、製品スタック内の潜在的な脆弱性が確実に特定され（例：Oracle DB を実行している場合、Oracle のセキュリティ情報を購読する必要がある）、これに沿って顧客のセキュリティ問題にパッチを当てるためのリリース手段が存在する必要がある。
- ✓ 脆弱性の報告については、「IM：Incident Management」（インシデント管理）の項で説明している。

OS-03 製品のライフサイクル

- ✓ **製品のライフサイクルが明確に定義されており、そのライフサイクル期間中はパッチやアップデートが提供されていること。**
- ✓ 製品又はサービスのライフサイクルは、顧客がポイントとなる日付を認識できるように明確に決められること。製品やサービスの導入から廃止までのライフサイクル期間中は、セキュリティを維持できるように、パッチやアップデートを提供すること。
- ✓ 攻撃者による被害を最小限に抑えるため、重要なパッチ適用は可能な限り早く実施すること。クリティカルでないパッ

チ適用は、リリース後 1 ヶ月以内、遅くとも 90 日以内には実施すること。

✓ また、ベンダーは、システムを構成するソフトウェアコンポーネント（OS、DBMS、アプリケーションサーバーなど）のいずれかがサポートされなくなった場合、そのアップグレードをサポートする必要がある。

OS-04 製品/ソフトウェアの提供

✓ **製品、ソフトウェア、またはサービスの提供には、セキュアなプロセスが用意されていること。**

✓ ベンダーは、製品、ソフトウェア、またはサービスの提供プロセスにおいて、物理的およびデジタル的なセキュリティ管理を行う必要がある。これらのセキュリティ管理には以下のようなものが含まれる。

- 暗号化された USB キー
- 安全なプロトコルによる配送
- 暗号化されたソフトウェアパッケージ
- ハッシュ値のチェック

OS-05 カスタマーメンテナンス

✓ **顧客へのリモートサポートおよびメンテナンスを提供するための安全な方法が用意されていること。**

✓ 製品またはサービスのカスタマーサポートは、以下を含む（ただしこれに限定されない）安全な方法で提供されること。

- 多要素認証（MFA）を使用した仮想プライベートネットワーク（VPN）。
- リモートサポートに使用するアカウントは、トラブルシューティングの期間中のみ有効にすること。
- すべてのトラブルシューティング活動は、記録され、レビューされる必要がある。

OS-06 本番環境と非本番環境の分離

✓ **本番環境と非本番環境は分離されていること。**

✓ 運用環境への不正なアクセスや変更のリスクを低減するために、開発、試験及び本番設備を分離する必要がある。

SD. Secure Development：セキュアな開発

SD-01 開発ライフサイクル

✓ **製品開発のライフサイクル全体を通して、セキュリティが設計され、実装されていること。**

✓ ソフトウェアまたはシステムの開発のためのセキュアなプロセスを概説したポリシーまたは同等の文書が整備されている必要がある。

✓ 開発ライフサイクルには、少なくとも以下が含まれなければならない。

- リスクアセスメント／脅威モデルのプロセス
- 安全な設計／アーキテクチャのレビュー
- 文書化された安全なコーディングガイドラインおよび業界の優れた実践方法（OWASP など）が適用され、常に最新の状態に保たれていること

- 必須のテストステージ／セキュリティゲート
- ソースコードおよび／またはコンパイルされたバージョンのコードを分析して、セキュリティ上の欠陥を発見するためのセキュアなコード分析。
- 最終版に開発プロセスで生じたテストコードが残らないようにするためのコードクリーニング

SD-02 トレーニング

- ✓ **開発スタッフは、最新のセキュアなコーディングの原則とグッドプラクティスについてトレーニングを受けていること。**
- ✓ 開発スタッフは、最新のセキュアなコーディングの原則とベストプラクティスを維持するために、定期的なトレーニングと継続的な開発を受けること。

SD-03 ソースコード

- ✓ **プログラムのソースコードへのアクセスは制限されており、厳密に管理されていること。**
- ✓ プログラムのソースコードは、許可されていない機能の導入や意図しない変更を防ぐため、また知的財産権に関わる場合は機密性を保持するために、保護し、アクセスを厳密に制御する必要がある。

IM. Incident Management：インシデント管理

IM-01 インシデント対応

- ✓ **文書化されたインシデント対応および危機管理のプロセス／手順があり、それが定期的に見直され、最新の状態に保たれていること。**
- ✓ 情報セキュリティインシデントへの迅速かつ効果的で秩序ある対応を確保するために、セキュリティインシデント対応の責任体制と手順を確立しなければならない。これには、さまざまな攻撃シナリオに対する明確な対処方法や、明確なエスカレーションルートの構築を含む。
- ✓ また、このプロセスには、インシデント発生後のレビューが含まれており、こうすることにより同一または類似のセキュリティインシデントの再発を防止するための適切な措置を講じることができる。

IM-02 連絡先

- ✓ **セキュリティインシデントに迅速かつ効果的に対処するために、明確に決められた連絡先(社内、社外、顧客)が存在すること。**
- ✓ 連絡先のリストは、連絡が取れない場合のリスクを考慮する必要がある (例えば、各エスカレーションポイントに複数の担当者と連絡方法を用意する)。
- ✓ 組織は、ゼロデイ攻撃などの重要または重大な情報セキュリティインシデントに対応するために、24 時間 365 日対応可能な連絡先を用意しておくこと。
- ✓ **セキュリティインシデントが発生したときに顧客に通知するための文書化されたプロセスが用意されていること。**
- ✓ 組織は、顧客に影響を与える可能性のあるセキュリティインシデントが組織に発生した場合、インシデントの簡単な説明とその重要度のレベルを記載した通知を顧客の連絡先にタイムリーに送信することを保証する文書化されたプ

ロセスを用意する必要がある。

IM-03 フォレンジック対応（証跡保全対応）

- ✓ **セキュリティインシデントに関連する証拠の保存を管理するための、文書化されたポリシーまたはプロセスが実施されている。**
- ✓ 懲戒処分または法的手続きが必要な場合に備えて、証拠を保全するための文書が整備されていること。これには、そのような証拠の収集、保管、提示が含まれる。

IM-04 脆弱性の公開

- ✓ **脆弱性が責任を持って報告されるよう、脆弱性開示ポリシーまたはプロセスがあること。**
- ✓ 脆弱性開示ポリシー／プロセスがあることで、インシデント発生のリスクを低減することができる。こうすることで、脆弱性が一般に公開される前に、ベンダーが脆弱性パッチを提供するための合理的な時間が確保できる。
- ✓ ベンダーは EBU R 160 を遵守することが望ましい。

PS. Physical security：物理的セキュリティ

PS-01 物理アクセス制御

- ✓ **オフィスビル、データセンター、通信サーバーが設置されている部屋などのエリアへの人員、機器、メディアの出入りを制限するために、物理的な入出管理が行われていること。**
- ✓ 組織は、顧客情報の紛失、損傷、盗難、侵害を防ぐために、あらゆる機器および施設のセキュリティを確保しなければならない。これには以下が含まれる。
    - 組織のデータセンターへの入り口のアクセス制御（例：警備員、バッジリーダー、電子ロック、証拠能力のある監視カメラ）と、必要に応じて記録、レビュー、保持されたログ。
    - 物理的なアクセスは、業務上の必要性があり、かつ業務遂行に必要な最小限のアクセスに限定する。
    - 無許可の人が施設に入る可能性のある配送・搬入エリアおよびその他のアクセス先の管理。
    - 非常口は、適切な地域、国、および国際的な基準に沿って、警報、監視、およびテストが行われること。
    - 電源および火災安全装置が定期的に保守点検され、健康および安全に関する規制に準拠していること。
    - 侵入者検知システムは、地域、国、国際的な適切な基準に沿って設置、監視、テストされること。

PS-02 サービス停止

- ✓ **セキュリティ対策は、電力会社等のインフラのサービス停止（停電やネットワークの中断など）に機器が影響を受けないよう、適切に設置されること。**
- ✓ セキュリティ対策は、顧客情報を保護するために設置されるべきであり、以下のものが含まれる（ただし、これらに限定されない）。
    - バックアップ電源の設置

- 二重化/多重化ルーティング
- ロードバランシングと冗長性
- 帯域幅容量の監視と警告
- 定期的なテスト

PS-03 環境上の脅威

✓ **環境上の脅威や危険、および意図的な攻撃からのリスクを軽減するために物理的な保護を行うこと。**

✓ 環境上の脅威は考慮され、リスク評価されなければならない。これには、洪水、火災、地震、内乱、その他の形態の自然または人為的災害などの脅威が含まれる。適切な防護策を講じるためには、専門家の助言が必要な場合もある。

CS. Cloud Security：クラウドセキュリティ

CS-01 クラウド型サービス導入手順

✓ **ベンダーは、EBU 勧告 R 146 に規定されているクラウド導入手順に沿って、顧客が必要とするすべての情報を提供することが可能であること。**

✓ 勧告 R 146 は、メディア企業によるクラウド型サービスの受け入れのための手順を規定している。ベンダーは、サービスの機能性、プロセス、システムおよびデータ、データの分類、地域または欧州の法律に則った使用制限、サービスを運用するための技術的および組織的な要件等、メディア企業が手続きを行うために必要なすべての情報を協力して提供するものとする。

CS-02 顧客データの分離

✓ **顧客データがマルチテナント環境で保存または処理されている場合、顧客データの適切な分離が行われていること。**

✓ 顧客データが複数のテナントが存在するクラウドプラットフォームでホストされている場合、各顧客のデータが機密に保たれ、他の顧客に開示されないように、また、ある顧客に影響を与えるインシデントが他の顧客やその情報に悪影響を及ぼさないように、顧客間での分離すること。

CS-03 顧客のプラットフォーム/インフラストラクチャの分離

✓ **顧客のプラットフォームとインフラの間には適切な分離が存在し、必要に応じて更新や変更を個別に適用できるようになっていること。**

✓ CS-02 項と同様に、ある顧客に更新や変更を個別に適用する必要がある場合、他の顧客に悪影響を及ぼさないよう、顧客間の分離がされること。

BC. Business Continuity：事業継続

BC-01 事業継続計画

- ✓ **事業継続計画または災害復旧計画が策定されており、定期的に訓練と見直しが行われていること。**
- ✓ 組織は、不測の事態が発生した場合に顧客情報のセキュリティを維持することを含む、事業継続計画または災害復旧計画を策定しなければならない。
- ✓ 最低限、この計画は以下のとおりである。
  - 事業プロセスの中断または障害が発生した場合に、合意した期間内にどのように事業を復旧させるかを規定する（顧客と合意）。
  - 情報セキュリティがどのように維持されるかを説明する。
  - 実行に際し、適切なお客様の担当者に通知し、関わってもらうための取り決めを含むこと。
  - 定期的にテストされること。
  - 定期的に見直し、必要に応じて更新すること。
- ✓ 顧客にサービスを提供するための可用性の要件を満たすために、十分な冗長性を確保すること。

SC. Supply Chain Management：サプライチェーン管理

SC-01 サプライチェーンにおけるセキュリティ管理の評価

- ✓ **ベンダーは、サプライヤー（自社製品を構成する部品の提供者）に対しても、同じレベルのセキュリティ管理評価手順を適用する。**
- ✓ 販売者は、自らの潜在的な供給者及び製品に組み込まれる主要なサブシステム、ソフトウェア及びサービスの供給者に対して、本勧告に規定されているのと同じレベルの詳細なセキュリティの担保及び指針に準拠することができることを示すこと。ベンダーは、その結果を顧客に伝えることができるようにすること。

このページは両面印刷を考慮し意図的に挿入しているページです。

付録 B：製品のセキュリティ要件

DO. Documentation：ドキュメント

DO-01 パスワードの変更

- ✓ **特にインターネットに接続されたシステムでは、デフォルトのパスワードを変更するよう明確に指示されていること。**
- ✓ デフォルトのパスワードはよく知られた脆弱性となる。製品と一緒に発行されるドキュメントには、デフォルトのパスワードを変更するよう明確に指示すること。

DO-02 セキュリティ機能

- ✓ **製品のドキュメントには、セキュリティ機能の詳細な説明が含まれていること。**
- ✓ 提供される文書には、製品で提供されるすべてのセキュリティ機能の詳細が含まれている必要がある。これは最低でも本勧告の附属書 B のすべての要件をカバーする必要がある。

DO-03 ネットワーク

- ✓ **製品のドキュメントには、インターフェース、アクセスポイント、ネットワーク通信および機能に関する詳細な説明が含まれていること。**
- ✓ 詳細には、ベンダーは以下を提供する必要がある。
  - どのレイヤ 3 機能が使用されているか
  - アプリケーション／システムが使用している IP ポート
  - どの IP ポートが開放されているか（使用されていないが、アプリケーションへの攻撃に使用される可能性がある）
  - どの IP ポートがアプリケーションの標準的な設定の一部として無効になっているか

DO-04 統合

- ✓ **製品のドキュメントには、セキュリティフレームワークに製品を統合する方法（異なるネットワークゾーン、統一認証サービス、ワークフロー、インターフェース、必要な TCP/UDP ポートのみを開くなど）に関する情報が含まれていること。**
- ✓ 様々なセキュリティシナリオに製品を統合する方法の詳細を含む明確な文書を提供する必要がある。

DO-05 堅牢化（ハードニング）

- ✓ **製品には、デフォルト状態を含め、堅牢化またはベストプラクティスの構成に関する推奨事項が含まれている。必要最低限のサービスのみ有効であること。**
- ✓ システムのハードニングについては、CIS Benchmarks や SANS Institute などの業界のベストプラクティスが利用可能な場合は、それに従うものとする。

✓ 最低限必要なサービスのみを稼働させること。

DO-06 パッチ管理プロセス

✓ **製品のドキュメントには、パッチおよびリリース管理プロセス（特にセキュリティアップデートに関する）の説明が含まれていること。**

✓ 製品のパッチマネジメント及びリリースマネジメントの文書は、OS-O3 製品ライフサイクルの項に沿って作成されること。

AA. Authentication & Authorization：認証と認可

AA-01 Central authentication：統一認証

✓ **製品は、業界で最も使用されている統一認証サービスに対応していること。**

✓ 製品は統一認証サービスに対応する必要がある。業界で最も使用されているものを以下に列挙する。

- Active Directory：Kerberos ベースの認証
- LDAP over SSL：LDAPS
- アイデンティティプロバイダー
  - ✧ SAML IdP：Simple Authentication Mark-up Language
  - ✧ OpenID IdP：OAuth プロトコル上のアイデンティティ層
- RADIUS
- TACACS+

AA-02 セッションタイムアウト

✓ **製品は、セッションのタイムアウトに対応していること。**

✓ セッションのタイムアウトは、セキュリティと利便性のバランスを考慮して設定する必要がある。攻撃者の機会を制限する必要があるが、ユーザーはセッションが頻繁にタイムアウトすることなく製品内の操作を快適に行うことができるようにすること。

AA-03 ロールベースのアクセス制御（RBAC）

✓ **製品は RBAC に対応していること。**

✓ 役割ベースのアクセスは、組織内のユーザーの役割に基づいてアクセスを制限すること。

AA-04 パーソナライズされたアカウント

✓ **製品は、個々のユーザーの認証に対応していること。**

✓ すべてのユーザーは、固有の個人アカウントを使用してシステムにログインすること。これにより、アカウントを使用する各人の個人的な活動が識別および監査され、個人の証跡が維持される。

AA-05 デフォルトのパスワード

- ✓ **製品は、組み込みアカウントのデフォルトのパスワードを変更することができること。**
- ✓ デフォルトのパスワードは変更できるようにしなければならない。工場出荷時やデフォルトのパスワードはよく知られており、公に文書化されていることが多いため、特にインターネットに公開されている機器では、不正アクセスの原因となる可能性がある。
- ✓ **製品は、すべての製品および顧客に対して同じパスワードを持つ包括的な隠しアカウントを持っていないこと。**
- ✓ 製品には、ベンダーが保守作業を行うために使用する「隠しアカウント」が組み込まれていることが多い（つまり、これらのアカウントは高い権限を持っているということである）
- ✓ このような「隠しアカウント」が存在する場合、少なくとも顧客ごとに異なるパスワードを設定しなければならない。

AA-06 パスワードポリシー

- ✓ **製品は、強力なパスワードポリシーの実装に対応していること。**
- ✓ 強力なパスワードを実装するために、パスワードポリシーには最低でも以下の内容を含める必要がある。
    - パスワードの長さが最低 8 文字であること（管理者アカウントの場合はそれ以上）。
    - 大文字/小文字の区別
    - 数字
    - 特殊文字および拡張特殊文字

AA-07 認証

- ✓ **製品は、多要素認証（MFA）メカニズムに対応していること。**
- ✓ 強力な認証メカニズムは、従来の認証スキームに追加のセキュリティレイヤーを提供する。強固な認証方法は、以下の認証要素を複数実装することに依存している（多要素認証 - MFA）。
    1. 記憶
    2. 所有物
    3. 生体
- ✓ 例えば、信頼できるデバイス上の認証アプリ、物理的なセキュリティトークン、定期的に更新される、または有効期限の短いワンタイムパスワード/コードなどを使用する。
- ✓ **製品は、インターネットから接続するインターフェースにおいて、強化された認証方式に対応している。**
- ✓ 製品は、インターネットに接続するインターフェースにおいて、強化された認証方式（Security Assertion Mark-up Language V2（SAML2）を使用した第二認証要素（2FA））に対応する必要がある。この方法は SSO と組み合わせることができ、ユーザーはアクセスするアプリケーションごとに認証するのではなく、一度だけ認証すればよい。

AA-08 認証、許可、およびアカウンティング（AAA）のロギング

- ✓ **製品は、認証イベント、認可イベント、およびユーザーの活動を記録するログを生成すること。**
- ✓ 製品は、以下の詳細を記録するセキュリティ・イベント・ログを生成すること。
    - 認証：システムへのログインの詳細と、それが成功したか失敗したかを示す。

- 認可：特定のシステム機能（特に機密性の高い管理機能）へのユーザーのアクセス試行の詳細と、それらが許可されたか拒否されたか。
- アカウンティング：ユーザーがシステム上で行った活動や行動の詳細。

✓ 生成されたログの管理方法に関する推奨事項については、BA-01 を参照する。

EN. Encryption：暗号化

EN-01 パスワードの保存と転送

✓ **パスワードは、製品内に保存したり、平文テキストや可逆的な方式で転送したりしてはいけない。**

✓ また、画面上でのパスワードのマスキング（パスワードを入力する際に、実際のパスワードではなくアスタリスクの列を表示すること）を実装しなければならない。これにより、ユーザーパスワードの入力を他のユーザーから見えないようにする。

EN-02 保存データ

✓ **製品は、業界のベストプラクティス勧告と最新の標準に沿った最先端の暗号化技術に対応していること。**

✓ 保存データは、少なくとも AES256 以上の最新の暗号化技術を用いて暗号化されていること。

✓ また、以下の暗号化動作モードを考慮すること。

- GCM（Galois/Counter Mode）：ガロア/カウンターモード
- CTR（Counter Mode）：カウンターモード
- CBC（Cipher Block Chaining Mode）：暗号ブロック連鎖モード

✓ また、以下の点にも留意する必要がある。

- 同じ暗号化アルゴリズムであれば、一般的に暗号化キーが長いほど防御力が高い。
- 長い複雑なフレーズは、短いパスフレーズよりも強力である。

EN-03 転送中のデータ

✓ **製品は、暗号化されたネットワークプロトコルに対応していること。**

✓ ネットワークを介して通信を行う際には、権限のないユーザーによるネットワークトラフィックの盗聴を防ぐために、通信を暗号化する必要がある。

- 以下のプロトコルを使用する。
  - HTTPS
  - SFTP
  - FTPS
  - SCP
  - SSHv2
  - SNMPv3
- 以下プロトコルは避けること。
  - HTTP

- FTP
- TELNET
- SNMPv1-SNMPv2
- SSHv1
- VNC

EN-04 証明書と公開鍵基盤（PKI）のサポート

- ✓ **製品は、証明書および公開鍵基盤（PKI）に対応していること**
- ✓ PKI と証明書は、人、機器、サービスを認証し、情報の転送を安全に行うために必要である

EN-05 マスターキーの管理

- ✓ **マスターキーは安全に管理されること。**
- ✓ すべての暗号化ベースのシステムには、構成内のすべての秘密鍵とパスワードを暗号化して保護するデフォルトのマスターキーがある。以下のことが推奨される。
  - デフォルトのマスターキーを使用せず、新しいマスターキーを設定する。
  - マスターキーを定期的に変更する（期間は、保護するデータの重要性／機密性などの要因によって異なる）
  - マスターキーを安全な場所に保管する。
- ✓ マスターキーの設定方法やリセット方法についての情報は、ベンダーからの提供が必要な場合がある。

BA. Base configuration：基本構成

BA-01 ログ管理

- ✓ **製品は、セキュリティイベントやエラーのログを生成すること。**
- ✓ 製品では、最低限、以下の種類のログを生成する必要がある。
  - セキュリティイベント：AA-08 に基づいて AAA データを記録する。
  - エラー：システムは、何か問題が発生したときにエラー・ログを生成する。
- ✓ **製品は、ログをリアルタイムで集中管理プラットフォームに安全に配信する機能を備えている。**
- ✓ 製品は、組織が使用する共通の時間源との定期的な時刻同期（NTP を使用するなど）に対応すること。ネットワーク上のシステムが同じタイムソースを使用していない場合、問題の調査は困難となる。
- ✓ 製品は、集中管理されたロギングシステムがデータを確実に受信したことを保証するメカニズムを介したロギングに対応すること（例：UDP よりも TCP を優先）。
- ✓ 製品は、製品と集中ログ管理プラットフォーム間のログデータの転送における暗号化に対応すること。

BA-02 ポータブルメディア制御

- ✓ **製品は、ポータブルメディアのインターフェースやアクセス権の無効化や制御に対応していること。**
- ✓ ポータブルメディア（USB デバイスなど）は、偶発的または意図的なマルウェアの侵入経路として頻繁に使用され

る。製品は、この種のデバイスのインターフェースとアクセス権を無効化または制御に対応すること。ベンダーは以下のことを明示的に述べること。

- どのようなインターフェースが利用できるか。
- インターフェースのデフォルトのアクセス権、およびデフォルトの動作状態（例：インターフェースがデフォルトで有効、またはデフォルトで無効）。
- 必要に応じて、これらのインターフェースを有効にするために必要な方法。

BA-03 不必要なプロトコルの無効化と OS の堅牢化（ハードニング）

- ✓ **不要なプロトコルは無効化すること。**
- ✓ OS のハードニングのベストプラクティスに従い、製品で使用されていないプロトコル/機能は、デフォルトで無効にする必要がある。

BA-04 ウイルス/マルウェアからの効果的な保護

- ✓ **製品は、ウイルス/マルウェア、サーバー側およびクライアント側の攻撃に対する効果的な保護に対応していること。**
- ✓ 製品は、ウイルス/マルウェア、サーバー側およびクライアント側の悪用に対する効果的な保護に対応すること。ベンダーは、インストールおよび使用に関して、以下の詳細情報を提供する必要がある。
  - システム上でテストされたアンチウィルスソリューションのリスト。
  - インストール/アップデート/ロールバックの方法。

BA-05 モニタリングサポート

- ✓ **製品は、リアルタイムの監視プロセスに対応するデータへのアクセスを提供すること。**
- ✓ 製品は、リアルタイムの監査証跡とログ監視プロセスに対応すること。製品の管理者は、システム活動の監査証跡、システム/アプリケーションのエラー、およびセキュリティ関連イベントを含むイベントログにアクセスできること。
- ✓ 製品は、適切なメカニズム（SNMP 経由など）により、システムのステータス／健全性データおよびパフォーマンス・メトリクスを利用可能にし、サードパーティの監視プラットフォームを使用して監視できるよう対応すること。

BA-06 バックアップ／復元のサポート

- ✓ **製品はバックアップと復元に対応していること。**
- ✓ 製品は、少なくとも以下を含むバックアップと復元に対応すること。
  - ユーザーデータ
  - ファームウェア
  - システムデータ
  - 設定

BA-07 ソフトウェア/ OS 分離

- ✓ **製品は、OS とソフトウェアの分離に対応しており、OS と実行環境へのパッチ適用が可能であること。**
- ✓ OS とソフトウェアの分離に対応し、OS と実行環境のパッチ適用を可能にすること。ベンダーは、オペレーティングシ

ステムのパッチが検証され、インストールが可能になったときに、その旨をお知らせすること。

NE. Network configuration：ネットワーク構成

NE-01 ネットワークセグメンテーション

- ✓ **製品は、ネットワークの細分化（MPLS、マルチ VLAN、ルーティング）に対応していること。**
- ✓ 製品は、ネットワークの細分化（MPLS、マルチ VLAN、ルーティング）に対応していること。また、一般的なネットワーク管理・監視ツールで行われているように、管理用ネットワークインターフェースとデータ用ネットワークインターフェースを分離する機能を備えていること。

NE-02 障害自動通知(コールホーム)利用におけるインターネット接続のセキュリティ

- ✓ デバイスがデフォルトの障害自動通知のための接続を必要とする場合、適切な手段でセキュリティを確保する必要がある。特に
- ✓ **製品は、インターネットへの常時かつ直接の接続を必要とせずに動作すること。**
- ✓ **製品は、インターネット接続時のコンテンツ検査に対応していること。**
- ✓ このような検査は、認証機構を含むフォワードプロキシおよびリバースプロキシによって実現できる。
- ✓ **本製品は、ジャンプホスト(踏み台)に対応すること。**
- ✓ 製品は、非武装地帯（DMZ）内の保守用アクセスポイントに対応しており、ベンダーや管理者がアプライアンス本体ではなく、まず DMZ に接続できるようになっている。
- ✓ **製品は、トラフィックの監視（インバウンド／アウトバウンド）を提供すること。**
- ✓ トラフィックを監視またはフィルタリングすることは、不正な活動に関連する異常な動作を検出するのに役立つ。

AP. Application security アプリケーションのセキュリティ

アプリケーション・セキュリティのコントロールについての詳細は、OWASP のウェブサイト
https://cheatsheetseries.owasp.org/ を参照してください。

AP-01 入力検証

- ✓ **製品は、アプリケーション内に適切な入力検証を実装していること。**

AP-02 XSS と SQL バリデーション

- ✓ **製品は、Web フロントエンドのクロスサイトスクリプティングと SQL インジェクションに対する制御を実装していること。**

AP-O3 非管理者権限での実行

- ✓ **すべてのプログラムとユーザーシステムは、ジョブを完了するために必要な最小限の権限を使用して動作すること。**

AP-04 アカウント一覧情報の不正取得

- ✓ **製品は、アカウント一覧情報の不正取得から保護するためのメカニズムを実装すること。**

AP-05 セッション管理

- ✓ **製品は、セッションハイジャック攻撃からユーザーセッションを保護する仕組みを実装していること。**

AP-06 フェイルセキュア（フェイルセーフ）

- ✓ **アプリケーションは誤操作・誤作動時にその影響を受けないようにフェイルセキュアに設計されており，すべての誤作動・誤操作はこれを許可しない場合と同じ実行経路をたどること。**

CM. Change management 変更管理

CM-01 変更管理

- ✓ **製品やサービスのセキュリティに影響を与える変更は、文書化された正式なプロセスによって管理され、承認されること。**
- ✓ 製品またはサービスのセキュリティに影響を与える変更は、正式なプロセスを通じて制御、文書化、および認可されなければならない。このような変更は、顧客に提供する製品やサービス、または顧客情報のセキュリティに悪影響を及ぼさないことを確認するために、レビューとテストを行わなければならない。

付属書C：セキュリティ管理条件書（情報のみ - スプレッドシートを使用してください）

ベンダーのセキュリティ要件			A	B	C
			この条件を満たしているか？	A欄の回答の根拠(詳細)	レビュアーコメント
IS. Vendor ISMS- このセクションでは、情報セキュリティに対する組織のアプローチについて説明します。					
IS-01	サイバーセキュリティポリシー	認知されたセキュリティ基準やフレームワークに沿い、文書化され、上級管理者によって承認されたサイバーセキュリティポリシー（または一連のポリシー）が存在する。			
		サイバーセキュリティポリシーが最新の状態に保たれており、関係者全員に効果的に伝えられている。			
IS-02	効果的なサイバー・セキュリティ組織	すべてのサイバーセキュリティの役割と責任が割り当てられ、関係者に周知されている。			
		最高情報セキュリティ責任者（CISO）または組織内のサイバーセキュリティの総責任者が任命されている。			
		すべての従業員（契約社員を含む）に対して、それぞれの役割に関連したサイバーセキュリティ意識向上のためのトレーニングと教育を行う。			
IS-03	監査計画	組織は、セキュリティ管理フレームワークの適合性と効果的な運用の定期的なレビューを確認するための監査手順を設ける。			
OS. Operational Security：運用上のセキュリティ					
OS-01	技術的なセキュリティ分析	製品やサービスの侵入テストや脆弱性テストなど、技術的なセキュリティ分析を定期的に行う。			
		侵入テストや脆弱性テストの結果は、顧客に提供される。			
OS-02	脆弱性管理	脆弱性管理プロセスが存在し、特定された脆弱性とそれを修正するパッチを履歴管理している。			
OS-03	製品のライフサイクル	製品のライフサイクルが明確に定義されており、そのライフサイクルを通じてパッチやアップデートが提供されている。			
OS-04	製品/ソフトウェアの提供	製品、ソフトウェア、サービスを提供する際に、セキュアなプロセスがある。			

OS-05	カスタマーメンテナンス	顧客へのリモートサポートやメンテナンスを提供するためのセキュアな方法が用意されている。			
OS-06	本番環境と非本番環境の分離	本番環境と非本番環境は分離されている。			
SD. Secure Development：セキュアな開発					
SD-01	開発ライフサイクル	製品開発のライフサイクル全体を通して、セキュリティが設計され、実装されている。			
SD-02	トレーニング	開発スタッフは、最新のセキュアなコーディングの原則とグッドプラクティスについてトレーニングを受けている。			
SD-03	ソースコード	プログラムのソースコードへのアクセスは制限されており、厳密に管理されている。			
IM. Incident Management：インシデント管理					
IM-01	インシデント対応	文書化されたインシデント対応および危機管理のプロセス／手順があり、それが定期的に見直され、最新の状態に保たれている。			
IM-02	連絡先	セキュリティインシデントに迅速かつ効果的に対処するために、明確に決められた連絡先(社内、社外、顧客)が存在する。			
		セキュリティインシデントが発生した場合、顧客に通知するための文書化されたプロセスが整備されている。			
IM-03	フォレンジック対応（証跡保全対応）	セキュリティインシデントに関連する証拠の保存を管理するための、文書化されたポリシーまたはプロセスが実施されている。			
IM-04	脆弱性の公開	脆弱性が責任を持って報告されるよう、脆弱性開示ポリシーまたはプロセスがある。			
PS. Physical Security：物理的なセキュリティ					
PS-01	物理アクセス制御	オフィスビル、データセンター、通信サーバーが設置されている部屋などのエリアへの人員、機器、メディアの出入りを制限するために、物理的な入出管理が行われている。			
PS-02	サービスの停止	セキュリティ対策は、電力会社等のインフラのサービス停止（停電やネットワークの中断など）に機器が影響を受けないよう、適切に設置されている。			
PS-03	環境上の脅威	環境上の脅威や危険、および意図的な攻撃からのリスクを軽減するために物理的な保護を行う。			

CS. Cloud Security：クラウドセキュリティ					
CS-01	クラウド型サービス導入手順	ベンダーは、EBU 勧告R 146に規定されているクラウド導入手順に沿って、顧客が必要とするすべての情報を提供することが可能である。			
CS-02	顧客データの分離	顧客データがマルチテナント環境で保存または処理されている場合、顧客データの適切な分離が行われている。			
CS-03	顧客のプラットフォーム/インフラの分離	顧客のプラットフォームとインフラの間には適切な分離が存在し、必要に応じてアップデートや変更を独立して適用することができる。			
BC. Business Continuity：事業継続					
BC-01	BCP(事業継続計画)	事業継続計画または災害復旧計画が策定されており、定期的に訓練と見直しが行われている。			
SC. Supplier Management:サプライヤーマネジメント					
SC-01	サプライチェーンにおけるセキュリティ管理の評価	ベンダーは、サプライヤー（自社製品を構成する部品の提供者）に対しても、同じレベルのセキュリティ管理評価手順を適用する。			

付属書C：セキュリティ管理条件書（情報のみ - スプレッドシートを使用してください）

製品のセキュリティ要件			A	B	C
			この条件を満たしているか？	A欄の回答の根拠(詳細)	レビュアーコメント
DO. Documentation：ドキュメント					
DO-01	パスワード変更	特にインターネットに接続されたシステムでは、デフォルトのパスワードを変更するよう明確に指示されている。			
DO-02	セキュリティ機能	製品のドキュメントには、セキュリティ機能の詳細が含まれている。			
DO-03	ネットワーク	製品のドキュメントには、インターフェース、アクセスポイント、ネットワーク通信および機能に関する詳細な説明が含まれている。			
DO-04	統合	製品のドキュメントには、セキュリティフレームワークに製品を統合する方法（異なるネットワークゾーン、統一認証サービス、ワークフロー、インターフェース、必要なTCP/UDPポートのみを開くなど）に関する情報が含まれている。			
DO-05	堅牢化（ハードニング）	製品には、デフォルトの状態を含め、堅牢化やベストプラクティスの構成に関する推奨事項が含まれている。必要最低限のサービスのみ有効である。			
DO-06	パッチ管理プロセス	製品のドキュメントには、パッチおよびリリース管理プロセス（特にセキュリティアップデートに関する）の説明が含まれている。			
AA. Authentication & Authorisation：認証と認可					
AA-01	統一認証	製品は、業界で最も使用されている統一認証サービスに対応している。			
AA-02	セッションタイムアウト	製品は、セッションのタイムアウトに対応している。			
AA-03	ロールベースのアクセス制御（RBAC）	製品がRBACに対応している。			
AA-04	パーソナライズされたアカウント	製品は、個々のユーザーの認証に対応している。			
AA-05	デフォルトのパスワード	製品は、組み込みアカウントのデフォルトパスワードを変更することができる。			
		製品は、すべての製品および顧客に対して同じパスワードを持つ包括的な隠しアカウント（メンテナンスアカウントなど）がない。			

AA-06	パスワードポリシー	強力なパスワードポリシーの実装に対応している。			
AA-07	認証	製品は、MFA（Multi-Factor Authentication）など、インターネット接続のインターフェースにおける強化された認証メカニズムに対応している。			
		製品は、インターネットから接続するインターフェースにおいて、強化された認証方式に対応している。			
AA-08	認証、認可、アカウンティング（AAA）の記録	製品は、認証イベント、認可イベント、ユーザーの活動を記録するログを生成する。			
EN. Encryption：暗号化					
EN-01	パスワードの保存と転送	製品は、すべてのパスワードを安全な方法で保存・転送し、平文を使用しない。製品に保存されるすべてのパスワードは、非可逆的な暗号化/ハッシュ化を使用する必要がある。			
EN-02	保存データ	製品は、業界のベストプラクティス勧告や最新の規格に沿った最先端の暗号化技術に対応している。			
EN-03	転送中のデータ	暗号化されたネットワークプロトコルに対応している。			
EN-04	証明書と公開鍵基盤（PKI）のサポート	製品は、証明書とPKIの使用をサポートしている。			
EN-05	マスターキーの管理	マスターキーは安全に管理されている。			
BA. Base configuration：基本構成					
BA-01	ログ管理	製品は、セキュリティイベントやエラーログを生成する。			
		製品は、ログを集中管理するプラットフォームにリアルタイムで安全に配信する機能を備えている。			
BA-02	ポータブルメディアの制御	製品は、ポータブルメディアのインターフェースやアクセス権の無効化や制御に対応している。			
BA-03	不必要なプロトコルの無効化とOSの堅牢化（ハードニング）	不要なプロトコルは無効にしている。			

BA-04	ウイルス/マルウェアからの効果的な保護	製品は、ウイルス/マルウェア、サーバー側およびクライアント側の攻撃に対する効果的な保護に対応している。			
BA-05	モニタリングサポート	製品は、リアルタイムのモニタリングプロセスをサポートするデータへのアクセスを提供する。			
BA-06	バックアップ／復元のサポート	製品は、バックアップと復元に対応している。			
BA-07	ソフトウェア/ OSの分離	製品は、OSとソフトウェアの分離をサポートし、OSと実行環境のパッチ適用を可能にする。			
NE. Network configuration：ネットワーク構成					
NE-01	ネットワーク・セグメンテーション	ネットワークの細分化（MPLS、マルチVLAN、ルーティング）に対応している			
NE-02	障害自動通知（コールホーム）利用におけるインターネット接続のセキュリティ	インターネットへの常時接続を必要としない。			
		インターネットに接続した状態で、コンテンツ検査に対応している。			
		ジャンプホスト（踏み台）に対応している。			
		トラフィックの監視（インバウンド/アウトバウンド）ができる。			
AP. Application security：アプリケーションセキュリティ					
AP-01	入力検証	製品は、アプリケーション内で適切な入力検証を実装している。			
AP-02	XSSとSQLバリデーション	製品は、Webフロントエンドのクロスサイトスクリプティングや SQLインジェクションに対する制御を実装している。			
AP-03	非管理者権限での実行	すべてのプログラムとユーザーシステムは、ジョブを完了するために必要な最小限の権限で動作する。			
AP-04	アカウント一覧情報の不正取得	製品は、アカウント一覧情報の不正取得から保護するメカニズムを実装している。			
AP-05	セッション管理	製品は、セッションハイジャック攻撃からユーザーセッションを保護する仕組みを実装している。			
AP-06	フェイルセキュア（フェイルセーフ）	アプリケーションは誤操作・誤作動時にその影響を受けないようにフェイルセキュアに設計されており，すべての誤作動・誤操作はこれを許可しない場合と同じ実行経路をたどる。			

CM. Change Management：変更管理					
CM-01	変更管理	製品やサービスのセキュリティに影響を与える変更は、文書化された正式なプロセスを通じて管理され、承認される。			