デジタルサイネージコンソーシアム

デジタルサイネージサービス選定時のセキュリティ面での注意点

－デジタルサイネージセキュリティ点検ガイド　別冊－

2025.05

１．本書の位置づけ

デジタルサイネージは情報発信の手段として様々な場所に設置され、その社会的な役割の重要性が増してきています。本書は、デジタルサイネージサービスを選定する際に考慮すべきセキュリティ要件の確認項目をまとめたものです。情報漏洩や不正アクセスを防ぐために、以下を参照の上、情報セキュリティ部門と連携して要件の確認とサービスの選定にお役立てください。

２．組織要件

デジタルサイネージサービスを選ぶ際には、サービス提供事業者の ISO27001 認証の有無を確認することが重要です。ISO27001 は、情報セキュリティ管理システム（ISMS）の国際規格であり、その事業者が業界標準の情報セキュリティ管理を実施していることを示します。この認証を持つ事業者を選ぶことにより、サービスの信頼性が向上し、リスクを低減できます。具体的には以下の項目を確認します。

・情報セキュリティ方針

組織全体の情報セキュリティに関する基本方針が文書として明示され、従業員全体に共有される方法が確立されていること。

・人の管理

従業員に対する定期的な情報セキュリティ教育が行われているか、また役割に応じた作業エリアへのアクセス管理が適切に行われていること。

・システムへのアクセス管理

デジタルサイネージシステムへのアクセスには、役割に応じた権限管理を行い管理していること。

・インシデント管理と SLA 確認

万が一の事態に備える体制の確認として、インシデント発生時の対応策やサービスレベルアグリーメント（SLA）が明確にされていること。

３．サーバー要件

◎使用する OS とミドルウェアのサポート状況

選定するデジタルサイネージ用の OS やミドルウェアが、定期的なアップデートとサポートを受けているか、脆弱性を抱えるリスクとなるサポートが終了したソフトウェアを利用していないこと。

◎定期的な脆弱性診断

サービスが利用しているシステムに対して定期的に脆弱性診断を実施し、診断結果に基づき対処していること。

◎Web アプリへの IP アドレス制限の可否

外部からのアクセス制御が実施可能であること。特に重要な情報を扱う場合は、IP アドレス制限機能があること。

◎ログ管理

セキュリティインシデント発生時の影響範囲の見極めのために十分なログの記録と管理が行われていること。最低でもシステムへのアクセスログと操作ログなどが操作元の IP アドレスやアカウント ID と紐づいて記録されていること。

４．STB 要件

◎OS やミドルウェア・ブラウザの情報公開

透明性が高いことにより、脆弱性のリスクを事前に把握できるため、使用されるアプリケーションに加え、OS やミドルウェアの情報を事業者が適宜公開していること。

◎通信仕様の透明性

通信に関する仕様やセキュリティプロトコルが明示され、データが安全に送信される仕組みが整備されていること。セキュア通信要件として対応する暗号アルゴリズムのバージョンが明示され、セキュリティリスクの低いアルゴリズムをサポートし、セキュリティリスクの高いアルゴリズムをサポートから外されていること。（例：TLS のバージョンなど）

◎脆弱性検査の合格

STB が脆弱性検査に合格しているか、その検査結果が開示されていること。

◎最小限のオープンポートの維持

外部からの攻撃を最小限に抑えるため、常に最小限のオープンポートを維持し、不必要なサービスを停止していること。

◎必要なセキュリティ機能

正常動作監視、表示確認機能、リモートプログラム更新機能があること。特に、リモートプログラム更新機能により、脆弱性が判明した際に迅速な対応ができること。

これらの要点を考慮し、慎重にデジタルサイネージサービスの選定を進めることで、セキュリティリスクを低減し、より安全なデジタルサイネージサービスを選定することが可能になります。