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
セキュリティ点検ガイド

2024.06

目次

1. はじめに

本ドキュメントはデジタルサイネージシステムの設置・運用におけるセキュリティリスクを認識し、安全なサービス提供を行うための一助となることを目的とします。

本ドキュメントで扱う範囲は、一般的に言われるセキュリティ保護ソフトの導入や Web サイト閲覧時の注意やメール受信時の注意事項などは各社のセキュリティ対策に任せるとし、デジタルサイネージシステムとその運用に関しての注意点について記載します。

現在のデジタルサイネージは様々な場所で誰もが目にする大きなメディアの一つとなり社会的重要性が高まっています。デジタルサイネージの社会的重要性が高まるなかで、一度事故が発生した場合のリスクも大きくなり、セキュリティ対策の重要性が上がっています。

セキュリティ対策と言うとちょっと難しそうだと考えてしまうかもしれませんが、デジタルサイネージシステムを運用するには必要なことですので、本ドキュメント **4 セキュリティ点検ガイドの確認ポイント**をチェックして、自社のデジタルサイネージシステムでは問題無いか確認ください。

本ドキュメントではデジタルサイネージサービスを提供する際に、セキュリティ面で注意すべきことを明確にすることで、設置時及び運用時でのセキュリティ対策の点検契機となることを期待しています。

2. デジタルサイネージシステムのセキュリティ概要

デジタルサイネージシステムは、情報表示や広告配信に使用されるデジタル表示装置を利用したシステムであり、セキュリティの重要性が高まっています。この章では、デジタルサイネージシステムのセキュリティ概要について検討します。

2.1 デジタルサイネージシステムの基本構成

デジタルサイネージシステムは、表示装置、表示コントローラ、コンテンツ管理システム (CMS) などから構成されます。セキュリティ点検では、これらの各要素がセキュリティ上の脆弱性を持たないかどうかを確認する必要があります。
下記の図に示す通り、デジタルサイネージシステムと外部との接触点がセキュリティ確保のためには重要になります。

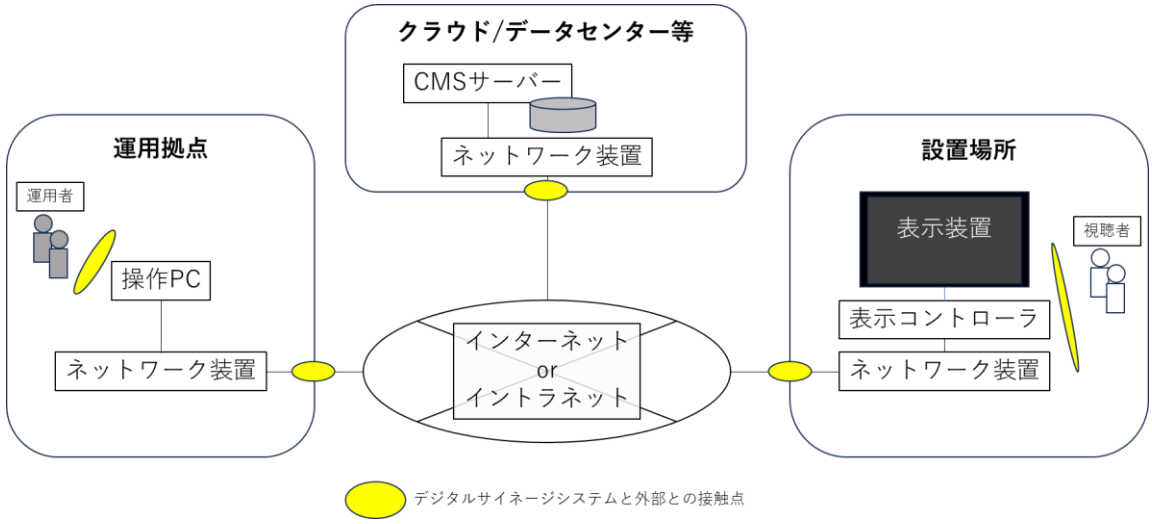

図 *1* デジタルサイネージシステムの構成イメージ

2.2 セキュリティリスクと脅威の概要

デジタルサイネージシステムは、ハッカーによる不正なコンテンツの挿入・表示、ネットワーク攻撃、不正アクセスなどのセキュリティリスクにさらされます。また、物理的なアクセス制御が不十分な場合、デバイスへの不正なアクセスや損傷のリスクもあります。且つ、運用面での管理が不十分であると大きな事故につながる可能性があります。

特にデジタルサイネージはその主目的のために不特定多数の人の目に触れる場所に設置されていますので、一度不正なコンテンツが挿入・表示された場合や緊急速報、対価がともなう広告配信などのコンテンツが適切に表示されない場合の影響は大きなものとなります。

2.3 セキュリティ対策について

デジタルサイネージシステムのセキュリティ対策は、情報の機密性、完全性、可用性を保護し、システム全体の信頼性を確保するために重要です。

セキュリティ対策は一般的に以下のようなステップでサイクルを回すことで行います。

1. 評価: 現在のセキュリティ状況を評価し、リスクを特定します。セキュリティの脆弱性や侵入経路を分析します。

2. 計画: 評価の結果をもとに、セキュリティ対策の計画を立てます。どのような対策を実施するか、どのようなリソースや予算が必要かを検討します。

3. 実装: 計画を実行に移し、セキュリティ対策を実装します。これには、セキュリティシステムやソフトウェアの導入、セキュリティポリシーの策定などが含まれます。

4. 監視: 実施したセキュリティ対策の効果を監視し、定期的にセキュリティの状況をチェックします。不審な活動や異常が検出された場合、迅速に対処します。

5. 更新: セキュリティ対策を常に最新の状態に保つために、新たな脅威や技術の変化に対応するための更新を行います。これにはシステムのパッチ適用、セキュリティポリシーの改訂などが含まれます。

このようなサイクルを継続的に繰り返すことで、デジタルサイネージシステムのセキュリティを維持し、向上させることができます。

しかし、このようなセキュリティ活動には当然コストが必要となります。

デジタルサイネージサービスを運用する上では、ネットワークの対策・サーバーの対策・ソフトウェアによる対策などの**システム的な対策**と**運用面の対策**、主に設置場所などに施す**物理的対策**などの対策を費用対効果のバランスを考えて行うことが重要となります。社内ネットワークのセキュリティ要件を単純に当てはめるなどの対策はコストに跳ね返ることになります。より重要な情報を取り扱う社内ネットワークとデジタルサイネージサービス用のネットワークを別にした上で対策を検討するなども費用面では有効です。

なお、本ドキュメントの記載内容はデジタルサイネージシステムにおける最低限の点検内容となります。各機器の脆弱性情報やハッキング技術は日々変化していますし、システム構成によっても注意点は異なるため、詳細（各機器のファームウェアのバージョンアップや管理など）については各ベンダーへご確認・ご相談ください。

【参考】
リスクに対する一般的な対応は、以下のようなものとなります。
①リスクの評価→②リスクの回避→③リスクの軽減→④リスクの受容→⑤リスクの転嫁

① リスクの評価: リスクを正確に評価することが重要です。リスクの大きさや影響を把握し、その後の対応を計画するための基礎となります。

② リスクの回避: リスク発生を回避するために、可能な限りその原因を排除したり、リスクが発生する可能性を減らすような対策を取ることが重要です。

③ リスクの軽減: リスクを完全に回避することが難しい場合は、リスクの軽減策を考えることが重要です。たとえば、リスクが発生した場合の影響を最小限に抑えるための対策を行うことが含まれます。

④ リスクの受容: ある程度のリスクを受け入れることも一つの対応策です。ただし、この場合はリスクの管理と監視を怠らないようにすることが大切です。

⑤ **リスクの転嫁:** リスクを他者に転嫁することも一つの対応策です。たとえば、保険を利用して特定のリスクを転嫁することができます。

これらの対応策はリスクの種類や大きさに応じて適切な組み合わせを考えることが重要です。

3. デジタルサイネージシステムのセキュリティリスク

3.1 不適切なコンテンツの表示によるリスク

デジタルサイネージシステムは一般の人に向けて情報や広告を表示することを目的とするため、多くの表示装置は人々の目に触れる場所に設置されていますので、これらの表示装置に設置者の想定外のコンテンツが表示されるとその影響は大きなものとなります。

デジタルサイネージシステムにおいて発生し得る不適切、または意図しない情報やコンテンツの表示と、その結果発生するリスクには、下記のようなものがあります。

発生し得る事象		その結果発生するリスク
不適切なコンテンツの表示	公序良俗に反する情報やコンテンツが表示される	・ 訴訟されるリスク ・ SNS などにより拡散され社会的信用が失墜するリスク ・ 契約された広告が表示されないことなどによる経済的損害リスク ・ 犯罪行為や不正行為へ加担してしまうリスク ・ 誤った情報の拡散や集団パニックの誘発などの社会問題に発展してしまうリスク
	個人のプライバシーや第三者の権利を侵害する情報やコンテンツが表示される	
	違法な広告、違法な商品や犯罪に関わる情報やコンテンツが表示される	
	反社会的な情報やコンテンツが表示される	
	特定の政治活動や、思想、信条などにおいて、中立的立場を欠くとみなされる情報やコンテンツが表示される	
意図しない表示	期日前や期日を過ぎた情報やコンテンツが表示される	
	OS の画面が表示される	
	表示した QR コードから詐欺サイトなどへ誘導される	
	表示がされない（ブラックアウト）	

不適切、または意図しない情報やコンテンツが表示されてしまった場合には、訴訟や信用失墜、経済的損失などの直接的なリスクだけでなく、間接的に犯罪行為や不正行為へ加担してしまったり、社会問題を誘発してしまうなどの大きなリスクも内在しています。適切なセキュリティ対策を行い、運用を行うことで安全なサービス提供を行うことが大切です。

3.2 機器の乗っ取りによるリスク

デジタルサイネージシステムがインターネットやローカルネットワークに接続されている場合、ハッカーや悪意のある者がネットワークを介してシステムにアクセスし、不正なコンテンツを表示するだけでなく、様々なリスクが発生する可能性があります。

リスクの種別	リスクの内容
機密性に対するリスク	表示コントローラに直接アクセスされ、内部のデータ（コンテンツや計測データなど）の改ざんや盗難、流出されるリスク
	ID やパスワードが漏洩し、コンテンツ管理システム（CMS)や表示コントローラ、操作 PC などが乗っ取られたりアクセスががができなくなるリスク
完全性に対するリスク	コンテンツ管理システム（CMS)や表示コントローラ、操作 PC が、他システム攻撃のために踏み台として利用され、攻撃対象からの訴訟や損害請求されるリスク
	コンテンツ管理システム（CMS)や表示コントローラ、操作 PC に侵入されて、情報の改ざんや漏洩につながるリスク
	表示コントローラの USB の抜き取りや差し替え、表示コントローラ自体のすり替え等により、情報の改ざんや漏洩につながるリスク
	表示コントローラのカメラやマイクなどの関連機器の乗っ取りにより、盗撮や盗み見、盗聴などに利用されるリスク
可用性に対するリスク	コンテンツ管理システム（CMS)やメディアプレイヤーの停止や破壊により、デジタルサイネージが利用できなくなるリスク

デジタルサイネージは、不正アクセスやパスワードリスト攻撃、DDoS 攻撃、脆弱性を狙った攻撃、標的型攻撃やマルウェアなどのサイバー攻撃により、様々なセキュリティインシデントが発生するリスクがあり、サイバーセキュリティに対する十分な配慮や備えが必要になります。

サイバーセキュリティの対策には、一般的に、体制の構築やセキュリティソフトの導入、必要なソフトウェアのアップデート、アクセス権限やログの管理、侵入の検知・防御の仕組みの導入、規程やルールの整備などを包括した取り組みを行い、技術や状況の日々の変化に合わせて点検を行い、必要な見直しを心がけるようにしましょう。

4. セキュリティ点検ガイド

本章では、セキュリティ点検の基本的な手法、ポイントをわかりやすく解説いたします。安心して運用できる方法を学び、セキュリティのリスクを最小限に抑えましょう。

4.1 デジタルサイネージシステムの運用にあたって

4.1.1 アカウントの管理

アカウント管理は、システムへのアクセスに必要なアカウントを適切に管理するプロセスです。

以下のような運用をしていないでしょうか。

確認ポイント

- みんなで同じアカウントを使っている
- 退職者のアカウントがそのままになっている
- 管理者や担当者以外に不要なアカウントを発行している

アカウントを管理する上で、アカウントのライフサイクルを意識しましょう。アカウントのライフサイクルとは、アカウントの登録から削除までの一連のプロセスを指し、このサイクルを適切に管理することが重要です。アカウントのライフサイクルには以下のステップが含まれます。

ライフサイクルのステップ	内容
登録	メンバーが新しく参加した際に、新メンバー用のアカウントを登録します。 新しいアカウントには、新メンバーの役割に応じた権限を付与します。
変更	メンバーの異動や担務変更などに応じて、アカウントを変更します。 メンバー情報を変更したり、メンバーの役割に変更があった場合には、変更後の役割に応じた権限に変更します。
休止、有効化	メンバーの休職/復職などに応じて、一時的に使用できない状態（休止）や再び使える状態（有効化）にします。 また、不正ログインを防ぐ目的で、複数回ログインを失敗した場合にも、システムによりアカウントが休止（システムによっては"ロック"）される場合があります。
削除	メンバーの異動や退職などにより、該当のアカウントが不要になった場合に、アカウントを削除します。

また、正確なアカウント管理をした上で、運用マニュアルを整備して、定期的に担当者の教育を行うことも重要となります。

4.1.2 パスワードの管理

パスワードは、操作者が”本人”であることを証明するために必要な”秘密”の文字列です。

以下のような管理をしていないでしょうか。

確認ポイント

- 覚えやすいからといってパスワードを簡単な文字列にしている
- 同じパスワードを使いまわしている
- パスワードを付箋に書いて見やすいところに貼っている
- ブラウザやアプリケーションソフトにログイン情報を保存させている

名前や生年月日、ID と同じものなど、類推されやすい単語を使ったパスワードは危険です。また、「123456」、「password」、「qwerty」のような簡単なパスワード、規則性のあるパスワードも危険です。悪意のある攻撃者はこれらのパスワードを優先して試し、侵入を試みます。

以下のような長く、複雑なパスワードが安全です。

- 12 文字以上
- 英大文字/小文字、数字、記号の組み合わせ

複数のサービスで同じパスワードを使用することも危険です。一つのサービスのパスワードが漏洩した場合、他のサービスにも不正アクセスされるリスクがあります。

サービスごとに異なるパスワードを設定することをおすすめします。

パスワードは「**長く**」「**複雑に**」「**使いまわさない**」ようにしましょう。

また、せっかく安全なパスワードを作っても、付箋に書いてデスクに貼っていたら意味がありません。パスワードは、ほかの人に知られないように管理しましょう。

パスワードの管理方法には、例えば以下があります。

- パスワード管理アプリを利用する
- 表計算ソフトなどに記載して、ファイルを暗号化する
- 紙などに書いて、書いた紙を施錠保管する

4.1.3 操作 PC の管理

デジタルサイネージを操作する PC はシステムへの入り口です。その入り口となる操作 PC のセキュリティ対策も重要です。

操作 PC で、以下のような使い方をしていないでしょうか。

確認ポイント

- 自動ログインで利用している
- ブラウザを開いたら ID/パスワードが記憶されている
- 担当者が離席する際に画面を開きっぱなしにしている

「セキュリティ」は「利便性」とトレードオフの関係にあると言われています。

「セキュリティ」を高めると「利便性」が下がる（使いにくくなる）、「利便性」を高める（使いやすくする）と「セキュリティ」が下がることが多いため、このように言われますが、あまりに高いセキュリティ対策は、業務効率を下げるだけでなく、メンバーがセキュリティ対策を守らなくなり、結果としてセキュリティレベルが下がってしまうことになりかねません。

「セキュリティ」と「利便性」はバランスが大切です。各社で業務内容や使用サービス/ツールに即したセキュリティ規定が策定されていると思いますので、操作 PC のセキュリティ対策は各社のセキュリティ規定に従って行ってください。

セキュリティ規定が策定されていない場合には、内閣サイバーセキュリティセンター（NISC）が、「インターネットの安全・安心ハンドブック Ver 5.00＜中小組織向け抜粋版＞（令和 5 年 3 月 1 日）」を公開していますので、こちらを参考にしてください。

インターネットの安全・安心ハンドブック
https://security-portal.nisc.go.jp/guidance/handbook.html

また、一度対策しておしまい！ではなく、セキュリティ規定が守られているか年に 1 回は点検するようにしましょう。

4.2 デジタルサイネージシステムの設置にあたって

4.2. 1 物理的保護

デジタルサイネージシステムは多数の人に見ていただくという設置目的の半面、多数の人との接触にさらされているため、物理的なアクセスを制限することが重要です。

デジタルサイネージシステムの機器が、以下のようになっていないでしょうか。

確認ポイント

- 表示コントローラー（STB など）が、施錠されていない
- ディスプレイの HDMI ポートや USB ポートがむき出しになっている

以下は、基本的なデジタルサイネージシステムの構成と、注意箇所（物理的なリスクがある箇所）です。

＜基本的なデジタルサイネージシステムの構成＞

＜ネットワーク型＞

＜スタンドアロン型＞

物理的なリスクには、機器の盗難や、イタズラにより不適切なコンテンツが表示されるといったものがあります。リスクの具体的な内容と、その対策には以下のようなものがあります。

■機器に関するリスク

リスクの具体的な内容	対策
➢ ディスプレイ本体が盗まれる。 ➢ 表示コントローラが盗まれる。 ➢ ディスプレイが表示されない。 ・ ディスプレイ本体、表示コントローラの電源が切られる(切れる)。 ・ ディスプレイ本体、表示コントローラが壊される(壊れる)。 ・ ディスプレイ本体、表示コントローラが故障する。	➢ 不正操作の防止 ・ ディスプレイ、表示コントローラを筐体の中に入れて、電源ボタン等を押されないようにする。 ➢ 破損・破壊・盗難の防止 ・ ディスプレイ、表示コントローラを筐体の中に入れる。 ・ ディスプレイ、表示コントローラにセキュリティロックを施す。

■表示するコンテンツに関するリスク

リスクの具体的な内容	対策
➢ 意図しないコンテンツが表示される。 ・ ディスプレイに別の機器(USB メモリなど)を接続される。 ・ コンテンツが差し替えられる。 ・ コンテンツが改ざんされる。 ・ コンテンツデータが削除される。 ➢ コンテンツが盗まれる。 ・ コンテンツがコピーされる。 ・ コンテンツが転送される。	➢ 外部との境界線を保護し不正アクセスから守る ・ 利用しているインターフェース(特にHDMI,LAN,USB)について、ロックを取り付けてケーブル等が外れないようにする。 ・ 利用しないインターフェース(特にHDMI,LAN,USB)について、ポートを塞ぐなどの対応を行う。 ※ 対処方法は CMS、STB により異なりますので、CMS、STB のマニュアルを参照するか、提供ベンダーにご確認ください。

4.2.2 システム設定による保護

デジタルサイネージシステムのセキュリティ対策として、システム設定による保護も有効です。

以下のような設定のままになっていないでしょうか。

確認ポイント

- ディスプレイの USB 再生機能が有効のままになっている
- ディスプレイの使っていない入力が有効のままになっている

例えば、システム設定で USB 再生機能を停止しておくことで、USB メモリを接続されたとしても、不正コンテンツの再生を防ぐことができます。

■システム設定により予防できるリスク

リスクの具体的な内容	対策
➢ 意図しないコンテンツが表示される。 ・ ディスプレイに別の機器(USB メモリなど)を接続される。 ➢ ディスプレイが表示されない。 ・ ディスプレイ本体、表示コントローラの電源が切られる(切れる)。	➢ 不正操作の防止※ ・ ディスプレイの USB 再生機能を停止する。 ・ 利用しないインターフェース(HDMI,USB)を無効化する。 ・ 本体ボタンをロックする。 ・ 赤外線リモコンでの操作を無効化する。 ※ 製品により設定の可/不可がございます。マニュアルを参照するか、提供ベンダーにご確認ください。

4.3 デジタルサイネージシステム導入にあたって

デジタルサイネージシステムの導入にあたっては、導入時の確認、および、導入後の定期的な確認によりセキュリティを確保することができ、ビジネスの安全性と信頼性を確保することができます。

本章の内容は技術的な内容となりますので、利用・検討されているデジタルサイネージベンダーにお問い合わせください。

4.3.1CMS サーバー

CMS サーバーはデータ管理や表示コントローラを管理するシステムの中核です。

この CMS サーバーが攻撃者の手に落ちると大きな損害が発生しますので厳重なセキュリティ対策が必要となります。

以下の確認を行いましょう。

確認ポイント

- CMS サーバーは脆弱性試験を行い、発見された問題点は解決されている
- 新たな脆弱性や攻撃手法に対して定期的に検査・対応を行っている
- 管理者の CMS サーバーへのアクセスはルール化されて安全に管理されている
- 必要に応じて IP によるアクセス制限が可能である
- 表示コントローラとの通信は暗号化されている
- クラウドサービスの場合、運用中・解約時のデータの取り扱いが明確になっている
- セキュリティ事故発生時のフローや補償について明確になっている
- CMS サーバーの所在地にカントリーリスクがない（日本国内が望ましい）

4.3.2 表示コントローラ

表示コントローラは表示装置に接続され実際に映像や情報を表示する装置です。

この表示コントローラが攻撃者の手に落ちると表示装置に意図しない表示が行われたり、サーバー攻撃の踏み台や他システム攻撃に利用されたりします。

以下の確認を行いましょう。

確認ポイント

- 表示コントローラは脆弱性試験を行い、発見された問題点は解決されている
- 基本的に表示コントローラにオープンされたポートがない
- ベンダーにて OS などソフトウェアの脆弱性情報を確認している
- OS などに新たな脆弱性が見つかった際にリモートでパッチ適用できる

4.3.3 ネットワーク装置

ネットワーク装置はセキュリティ確保の要となります。

最近では VPN ルータの脆弱性なども報告されており、VPN だからいつまでも大丈夫と安易に考えないようにしましょう。

以下の確認を行いましょう。

確認ポイント

- ネットワーク装置の管理用パスワードはデフォルトから十分複雑なものに変更している
- デジタルサイネージシステムで使用しないプロトコルは遮断している
- 利用している機材の品番とファームウェアを管理し、脆弱性情報を監視しており、必要に応じてファームウェアを最新化している

◎点検シート

点検項目		結果
導入時		☐
CMS サーバー	CMS サーバーは脆弱性試験を行い、発見された問題点は解決されている	☐
	新たな脆弱性や攻撃手法に対して定期的に検査・対応を行っている	☐
	管理者の CMS サーバーへのアクセスはルール化されて安全に管理されている	☐
	必要に応じて IP によるアクセス制限が可能である	☐
	表示コントローラとの通信は暗号化されている	☐
	クラウドサービスの場合、運用中・解約時のデータの取り扱いが明確になっている	☐
	セキュリティ事故発生時のフローや補償について明確になっている	☐
	CMS サーバーの所在地にカントリーリスクがない（日本国内が望ましい）	☐
表示コントローラ	表示コントローラは脆弱性試験を行い、発見された問題点は解決されている	☐
	基本的に表示コントローラにオープンされたポートがない	☐
	ベンダーにて OS などソフトウェアの脆弱性情報を確認している	☐
	OS などに新たな脆弱性が見つかった際にリモートでパッチ適用できる	☐
ネットワーク装置	ネットワーク装置の管理用パスワードはデフォルトから十分複雑なものに変更している	☐
	デジタルサイネージシステムで使用しないプロトコルは遮断している	☐
	利用している機材の品番とファームウェアを管理し、脆弱性情報を監視しており、必要に応じてファームウェアを最新化している	☐
設置時		☐
物理的保護	装置は施錠された場所に設置されている	☐
	ディスプレイの HDMI ポートや USB ポートに第三者がアクセスできない	☐
システム設定による保護	ディスプレイの USB 再生機能は無効になっている	☐
	ディスプレイの使っていない入力は無効になっている	☐
運用時		☐
アカウントの管理	みんなで同じアカウントを使っていない	☐
	退職者のアカウントは削除されている	☐
	管理者や担当者以外に不要なアカウントを発行していない	☐
パスワードの管理	覚えやすいからといってパスワードが簡単な文字列になっていない	☐
	同じパスワードを使いまわしていない	☐
	パスワードを付箋に書いて見やすいところに貼っていない	☐
	ブラウザやアプリケーションソフトにログイン情報を保存させていない	☐
操作 PC の管理	自動ログインで利用していない	☐
	ブラウザを開いたら ID/パスワードが記憶されていない	☐
	担当者が離席する際には画面をロックしている	☐

◎用語集

用語	説明
CMS	Content Management System の略。 コンテンツ（静止画や動画など）を保存、管理するシステム。 デジタルサイネージではコンテンツを配信する機能も有する。
DDoS 攻撃	Distributed Denial of Service attack の略。ディードス攻撃。 複数マシンから意図的に多量のアクセスやデータ送付を行い、攻撃対象のサーバーやネットワークへ膨大な負荷をかけることで、サービスへのアクセス困難や停止を引き起こすサイバー攻撃。
OS	Operating System の略。 パソコンやスマートフォン、STB などで使われており、コンピューター全体の動作を管理するシステムソフトウェア。 代表的なものに、Windows、macOS、Linux、Android、iOS などがある。
STB	Set Top Box の略。 ディスプレイに接続して動画などのコンテンツを表示する機器。 表示コントローラやメディアプレーヤとも呼ばれる。
VPN	Virtual Private Network の略。 インターネット上に仮想的な専用線を作る技術。VPN を利用することにより、セキュリティが高い通信が可能になる。
可用性	情報が必要なときに利用できる状態を保つこと。
完全性	情報の改ざんや破損を防ぎ、情報が正確かつ信頼性のある状態を維持すること。
機密性	情報へのアクセスを制限し、機密情報が不正に閲覧されないようにすること。
ファームウェア	ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェア。OS よりもハードウェア寄りの制御を行う。
プロトコル	コンピューターやネットワークにおける通信規格。 インターネット通信で使用する TCP/IP や、Web で用いられる HTTP、HTTPS などがある。
マルウェア	不正かつ有害な動作を行う意図で作成された、悪意のあるソフトウェアを総称する言葉。ウイルスもマルウェアの一種。

【参考情報】

サイバーセキュリティに関する、より詳しい情報が欲しい場合は下記のサイトをご確認ください。

内閣サイバーセキュリティセンター（NISC）：

https://www.nisc.go.jp/

総務省サイバーセキュリティ統括官：

https://www.soumu.go.jp/main_sosiki/cybersecurity/

警察庁サイバー警察：

https://www.npa.go.jp/bureau/cyber/index.html

独立行政法人情報処理推進機構（IPA）の情報セキュリティ情報：

https://www.ipa.go.jp/security/index.html

一般社団法人 ICT-ISAC：

https://www.ict-isac.jp/

特定非営利活動法人日本ネットワークセキュリティ協会：

https://www.jnsa.org/

NOTiCE：

https://notice.go.jp/