

調査研究報告書 「クラウドサービスを利用したシステム調査」

2025年04月

公益社団法人 日本防犯設備協会

映像セキュリティ委員会

□ agenda

1. クラウドカメラシステム概要
2. システム構成
3. 導入メリット、デメリット
4. 導入コストイメージ
5. 活用シーン
6. サイバー攻撃への注意事項

【1】クラウドカメラシステム概要

クラウドカメラシステムとは

一般的なカメラシステムはデジタルレコーダー(HDD/SDD/SDカード)などの記録媒体を使用して映像の録画を行います。

クラウドカメラシステムは、インターネット上に存在するクラウドサーバーを介して映像を録画したり閲覧する事が出来るカメラシステムのことです。

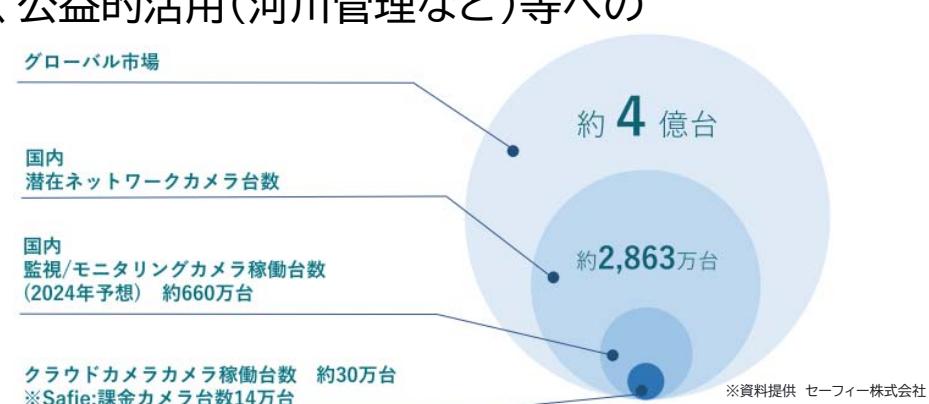


市場動向

カメラシステムのクラウド化は、10パーセントも満たない状態ですが、増加傾向にあります。

国内では約2,800万台の成長余地があり、初期費用がこれまでより抑えられることなどから、今までカメラシステムが導入されていなかった小規模店舗や飲食店、歯科医院や診療所、仮設物件、不動産/マンション、理美容室、小規模オフィス、公益的活用(河川管理など)等への普及拡大が見込まれます。

2021年のパブリッククラウドサービス市場は、1兆5,879億円(前年比28.5%増)となっており、また2030年の有償サービス市場として720億円(2019年比42.4倍)と大幅な拡大が予想されております。



【2】システム構成

システム構成

クラウドカメラシステムには、主に2種類のシステム構成が存在します。

①カメラダイレクト接続タイプ

カメラをインターネット回線に直接接続し、クラウドサーバーで録画

【使用機器/環境】カメラ、カメラ電源(PoEハブ)

インターネット回線、クラウドサーバー



②エッジストレージを介した接続タイプ

※エッジストレージ(カメラなどネットワーク端末側にデータを保存する分散型ストレージ)

エッジストレージにて映像を録画し、クラウドサーバー経由で録画映像を閲覧

【使用機器/環境】カメラ、カメラ電源(PoEハブ)、エッジストレージ

インターネット回線、クラウドサーバー



【3】導入効果メリット・デメリット比較

導入メリット

録画をクラウドサーバーで行う事により録画映像の管理などが簡単になる一方、システム運用をインターネット回線に委ねるためシステムの安定性や情報漏洩に懸念がある。

但し、対抗策としてエッジストレージを利用する方法などもあり、どのような目的で使用するかに併せて適切なシステムを選定する必要がある。

項目	大項目	内容	補足、対策等
メリット	録画データ保管用のハードディスクがカメラ設置場所には不要	<ul style="list-style-type: none">・ハードディスクの設置スペースが不要・壊れやすいハードディスクの管理やメンテナンスの手間が不要・震災や大規模災害が発生した場合も、カメラとネットワークが稼動している限り、クラウド上に蓄積される録画映像を確認可能・クラウドサーバーの冗長化により録画映像を担保する事が可能	
	複数の監視場所を一括で管理できる	<ul style="list-style-type: none">・遠隔地から各店舗の様子を一覧で確認することができるため、多店舗展開する企業の監視業務を効率化できる。・管理コストの省人化実現	例)本社の社員やエリアマネージャーなどが訪問して直接指導を行う場合訪問日時が平日の昼間であっても、週末の夜などの多忙な時間帯の様子をクラウド監視カメラで確認しておけば、忙しい時間帯の状況も理解したうえでアドバイスができる。
	スマホ等へのアラート通知	<ul style="list-style-type: none">・動体検知機能や通知機能を搭載した製品を利用することで、侵入者を検知したらスマホにアラートを入れるように設定できるため、迅速な対応ができるで犯罪の被害を最小限に抑えられる。	
	スピーカーと連動した警告	<ul style="list-style-type: none">・店舗にあるスピーカーやマイクと連動させれば、侵入者に遠隔で警告を発することも可能。	
	各種ソフト連携が可能 解析AI機能の活用	<ul style="list-style-type: none">AI検知時など教師データ量が豊富、常にアニメーション更新ができるシステムの拡張性	

【3】導入効果メリット・デメリット比較

導入デメリット

項目	大項目	内容	補足、対策等
デメリット	インターネット回線を利用するため通信環境に影響される。	<ul style="list-style-type: none">・災害などでインターネット接続に障害があると「映像が録画できない」「監視カメラの内容を確認できない」などのリスクがある。・「通信状況が安定していない」「速度が遅い」などの問題があれば、録画が中断する懸念がある。	自動で別回線やSDカードでの保存に切り替え可能な機能を搭載した製品もあり、エッジストレージを介した接続タイプの場合、インターネット回線不具合の場合でも録画映像を担保する事が可能
	クラウドサーバーの利用に月額費用がかかる	<ul style="list-style-type: none">・支店や工場が多い場合にカメラを設置する箇所が多くなると費用がかかる。・カメラの台数だけでなく、撮影した際のデータ量や映像の保存期間などで費用が変わる。	
	情報漏洩に注意しなければならない	盗み見や改ざんなどのリスクがある。	<ul style="list-style-type: none">①録画データや通信の暗号化②カメラへのアクセス遮断③VPN内での送受信
	サイバー攻撃、情報漏洩の危険性	通信データの暗号化やアカウントなどの管理が必要	

【4】導入コスト比較

導入 優位性・コストイメージ

想定規模: 小規模(屋内) カメラ8台 5年間利用した場合

■優位性

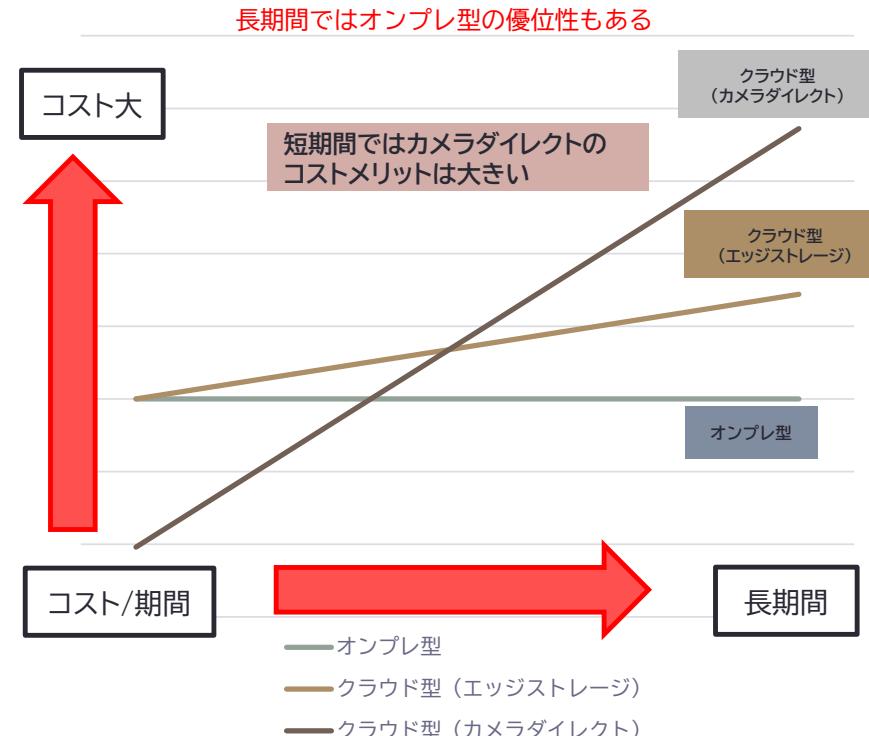
コストイメージ	オンプレ型 (オンプレミス 使用者管理型)	クラウド型 (エッジストレージ)	クラウド型 (カメラダイレクト)
カメラ/レコーダー (イニシャル)	△ (カメラ・レコーダー必要)	△ (カメラ・エッジストレー必要)	◎ (カメラのみ)
ネットワーク回線 (ランニング)	不要	○～△ (台数によって変動)	△ (高速な回線必要)
クラウドサービス利 用料 (ランニング)	不要	○ (台数によって変動)	△～○ (台数によって変動)
工事・保守	既設依存	既設依存	既設依存
特徴	メリット	イニシャルコストのみで 導入できる	遠隔管理が可能 ネットワーク回線は比較的 選びやすい
	デメリット	イニシャルコスト負担大 遠隔管理は出来ない	イニシャルコストと ランニングコストがかかる ランニングコストがかかる 高速安定したネットワーク 回線が必要
ユースケース	中期～長期間の利用 小規模～大規模システム	中期間の利用 中規模～大規模システム	短期、中期間の利用 小規模システム

※上記は一例です、システムの規模や要件(録画期間や画質、閲覧アカウントの数など)によりコストは変動します

インターネット回線経由でクラウドサーバーに映像データを伝送するため、必要な帯域を確保し録画欠損の軽減を考慮する。
また防犯カメラ映像は個人情報にあたるデータが含まれる可能性が高いため、セキュリティの高い伝送方式で暗号化など適切な処理を行っているサービス事業者を選択する必要がある。
利用に際してはサイバーアクセスなどに注意し、複数のサービスでIDやパスワードを流用しないなど、アカウントの管理を適切に行い、データ漏洩を防止する必要があるなど利用者側も配慮すべき点がある。

参考: 総務省 国民のためのサイバーセキュリティサイト
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_staff_13.html
参考 総務省・国立研究開発法人情報通信研究機構・ISPが連携し、IoT機器のセキュリティ対策向上を推進するプロジェクトサイト
<https://notice.go.jp/>

■コスト比較



【5】活用シーン

クラウドカメラシステムの活用シーン

適用先	用途
防犯	①飲食店や小売店舗などを中心に導入されており、万引きや強盗などの外部リスクへの対策 ②従業員による不正・トラブルなど、内部リスク対策
河川監視	①遠隔地から水位の上昇を把握できるので安全水位標を常時監視し、一定の水位に達したら管理者にメールでアラート(通知)する機能
オフィス	①社員の働いている様子を確認 ②会社のルールを社員がしっかりと守っているか確認
店舗 (飲食・小売・チェーン店)	①店舗内の防犯・内引き抑止だけでなく、複数店舗の一括管理が可能 ②業務の流れを改善して、お客さまの満足度を向上金銭の受け渡しミスや、金銭の抜き取りなどトラブル時に映像を確認
工場	①従業員や機械の稼動状況を事務所から確認 ②生産ラインの作業効率化の検討素材に使えたり、機械のトラブルや故障発生時には原因究明に活用
介護施設	①人手を使わずに施設内の見守りを強化 ②トラブル発生時の入居者家族との対応をスムーズに進める
建設現場に	現場の入退車両の管理や資材の盗難防止以外に遠隔地からでも現場の様子を確認、遠隔指示が可能
大型店舗・倉庫	広い店舗・倉庫内に設置することで、店舗の様子や在庫状況などを一括で確認可能
農業	農作物の育成状況確認

【6】サイバー攻撃への対策

サイバー攻撃の注意事項

- ・防犯カメラにおけるクラウドサービスを利用する場合、以下のような注意点がある。
クラウドサービス全般を利用する際の注意点について総務省がガイドラインを公開しており、
共通点も多いため詳細は参考にされたい。

注意点	ポイント
サービス側への攻撃	クラウドサービス業者側の障害、運用の不備や外部からの攻撃などにより、クラウドサービスが利用できなくなったり、保存していたデータ(録画映像など)が利用できなくなる可能性があることは留意して置く必要がある。万が一の場合に備え、本当に必要な録画データはバックアップしておくなどの対策も必要となる。またデータの暗号化やVPNなどセキュリティを担保した接続など、セキュリティ対策を行っているクラウドサービス業者を利用する必要がある。
アカウントの管理	クラウドサービスのIDやパスワードが漏洩することで、誰でもどこからでも記録映像やライブ映像にアクセスできるようになってしまう。 特に防犯カメラなど映像を利用するサービスにおいては、個人情報にあたるデータが含まれる可能性も高いため、 複数のサービスでIDやパスワードは流用しない、などアカウントの管理を適切に行う必要がある。 また覗き見によるパスワードの窃取や標的型攻撃メールなどのソーシャルエンジニアリングと呼ばれる攻撃への対応も必要になる。

参考：国民のためのサイバーセキュリティサイト(総務省)

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_staff_13.html

参考 総務省・国立研究開発法人情報通信研究機構・ISPが連携し、IOT機器のセキュリティ対策向上を推進するプロジェクトサイト

<https://notice.go.jp/>

作成・編集 映像セキュリティ委員会

委員長	中村 民雄	池上通信機株式会社
副委員長	小柳 康之	ホーチキ株式会社
	伊藤 雅彦	キヤノン株式会社
	大藪 覚	i-PRO株式会社
	難波 剛	株式会社JVCケンウッド・公共産業システム
	芳野 雅美	東芝テリー株式会社
	角戸 忠和	株式会社国際電気
	山本 健一	株式会社タムロン
	浪瀬 一文	株式会社タムロン
	鈴木 卓哉	株式会社ジャパン・セキュリティシステム
	木村 泰之	グローリー株式会社
	三田村 圭介	株式会社ケービデバイス
	船曳 将	TOA株式会社
	山崎 卓也	三菱電機株式会社
	宮崎 隆広	株式会社セノン
	古川 佳弘	株式会社セノン

事務局 内藤 義和 公益社団法人日本防犯設備協会

2025年3月現在

クラウドサービスを利用したシステム調査報告書

発行 2025年4月

編集 公益社団法人日本防犯設備協会 映像セキュリティ委員会

本書は、著作権法で保護対象となっている著作物で、下記行為を無断で行うことを禁じています。

- ・本書の内容を複写し、他に転用すること
- ・本書の内容を全部又は一部を転用すること
- ・本書の内容を変更し転用すること

お問い合わせは、下記へお願いします。

公益社団法人日本防犯設備協会
〒105-0013 東京都港区浜松町1-12-4(第2長谷川ビル)
TEL:03-3431-7301 FAX:03-3431-7304