

中小企業経営者、施設管理者、個人宅ユーザー向け

よくある防犯カメラトラブルQ&A

防犯カメラ設置後のトラブルとその対策！



近年、オフィスや商業施設、個人宅においても防犯カメラの導入が一般的になりつつあります。
犯罪抑止やトラブル発生時の証拠として有効であり、安心・安全な環境づくりには欠かせない存在です。

しかしその一方で、
「設置したのに映像が映らない」
「録画データが残っていなかった」
「リモートで映像を確認できない」
など、防犯カメラ設置後に起こる“想定外のトラブル”に直面するケースも少なくありません。

こうした問題は、設置方法や設定、運用管理の不備が原因となっていることが多く、
事前に知識を持っていれば十分に防げるものも多数あります。

本ホワイトペーパーの目的

本資料では、防犯カメラを導入した後によくあるトラブルについて、Q & A 形式でわかりやすく解説し、
具体的な対策・予防策を紹介していきます。
「これから設置を検討している方」はもちろん、「すでに導入済みだが運用に不安を感じている方」も、
本ホワイトペーパーを通じてトラブルを未然に防ぐヒントを得られるはずです。

設置後に起こりやすいトラブル 物理編



Q1 カメラがうまく録画されていない！

主な原因

- 設置位置が不適切で、映したいエリアが死角である
- 夜間撮影で赤外線が反射拡散して映像が白飛びしている
- レンズの角度や焦点距離の調整不足

対策

- 設置前に「映したい範囲」や「動線」を正確に把握し、設置場所を選定する
- 屋内なら「出入口」、屋外なら「人の出入りが多い動線」を中心にカバー
- 夜間撮影用にはIR(赤外線)対応カメラを選定し、設置時に反射物(壁・ガラス)との距離を調整する

ポイント

- 特に多いのが「設置したが実際には録画範囲外だった」という事例です。
- 録画映像を確認しながら微調整することが重要です。



Q2 カメラ映像がノイズまたは映像が途切れる

主な原因

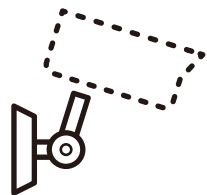
- 電源供給の不安定さ(AC アダプタや延長コードの劣化)
- 屋外使用時の防水対策不足や結露による機器内部のトラブル
- 映像信号ケーブルや同軸ケーブルの劣化・干渉
- ワイヤレスカメラの場合、無線干渉や電波障害の可能性も

対策

- 屋外使用時は防水・防塵対応(IP66 以上)のカメラを使用し、ケーブル接続部に防水テープや専用ケースを利用
- 長期使用の機器は、定期的なケーブルチェックと交換を推奨
- ワイヤレスの場合は、ルーターとの距離や電波状況の最適化を実施
- 電源供給は、UPS(無停電電源装置)の活用も効果的

ポイント

ノイズや接触不良は「録画された映像が使いものにならない」という最悪の結果を招きます。定期点検と保守体制の確保がカギです。



Q3 カメラ本体の盗難・破壊にあってしまった

主な原因

- 手が届きやすい高さへの設置
- 壁面固定が甘く、簡単に取り外しできる状態だった
- 明らかに防犯カメラとわかるため、狙われやすいケースも

対策

- カメラは地上から 2.5m 以上の高さに設置(脚立なしでは届かない位置)
- 屋外カメラはいたずら・破壊防止用のカバー(プロテクター)を使用
- 目立ちすぎない「ドーム型カメラ」や「偽装型カメラ」の併用も有効
- 本体に加えてレコーダーを離れた場所に設置・鍵付き収納にすることで映像消失リスクを分散

ポイント

カメラは「見せることで抑止効果」も期待できますが、狙われるリスクも同時に高まるため、設置の工夫が必要です。

トラブル 物理編 のポイントまとめ

- ① 設置前には「死角」や「光の反射」など撮影環境の確認を怠らない
- ② ケーブルや電源の品質・配置にも注意
- ③ 破壊・盗難リスクを減らすための高さ・設置強度・収納場所の工夫が重要

設置後に起こりやすいトラブル ネットワーク&システム編



Q4 スマホや PC から映像が見られない！

主な原因

- ネットワーク設定ミス（ルーター・Wi-Fi 未接続など）
- カメラや録画機器の IP アドレス重複
- ポート開放やファイアウォール設定の不備
- 専用アプリの不具合／バージョン非対応

対策

- カメラと録画機器の IP アドレス固定化を行う（DHCP ではなく静的設定）
- ルーター設定で必要なポートの開放（例：HTTP/HTTPS, RTSP など）を実施
- スマホアプリは最新バージョンに更新し、メーカーの推奨アプリを利用
- セキュリティソフト・ファイアウォールの一時的無効化で接続確認を行い、必要な例外設定を追加

ポイント

遠隔監視が「ある日突然できなくなる」のは、IP 変更やアップデートに伴う設定のズレが原因。
設定のバックアップ保存や、再設定手順をマニュアル化しておくで安心です。



Q5 クラウド保存されていない／一部の録画が欠損している

主な原因

- クラウドストレージの容量超過・課金切れ
- ネットワークが不安定でアップロード失敗
- 録画設定（動体検知／スケジュール録画）の誤設定
- カメラ側の時間設定がずれており、記録タイミングにズレ発生

対策

- 利用中のクラウドサービスのプランと保存期間の見直し
- 録画データを定期的にダウンロード／ローカル保存してバックアップ
- スケジュール録画や動体検知設定を分単位で調整
- カメラ・録画装置の時刻同期（NTP 設定）を実施し、時刻ズレを防止

ポイント

クラウドに保存されていると安心してチェックを怠るケースが多く見られます。
通知機能（録画失敗・容量警告）を ON にすることで、早期発見・対処が可能です。



Q6 急にすべてのカメラが 映らなくなった／録画されていない

主な原因

- ルーターや PoE スイッチの電源断／ハングアップ
- ネットワーク全体の障害
- 録画機 (NVR/DVR) のフリーズやストレージ故障

対策

- ルーター・ハブ・録画機の定期的な再起動スケジュールの導入
- UPS(無停電電源装置)を導入し、電源喪失対策を講じる
- 録画装置のログ機能を使って故障・異常の事前検知を行う
- ネットワーク構成図や IP 管理表を作成し、障害時の復旧スピードを高める

ポイント

「全カメラが落ちる」ケースでは、ネットワーク全体の見直しや、ルーター・録画装置のグレードアップが必要になることもあります。

トラブル ネットワーク・システム編 のポイントまとめ

- ① リモート接続やクラウド保存は便利な一方、設定・通信の安定性が命
- ② IP アドレス、ポート開放、時刻同期などの基本設定を見直す
- ③ クラウド任せにせず、ローカルとの併用・バックアップ体制を構築することが安全運用のカギ

設置後に起こりやすいトラブル 運用・管理編



Q7 録画データが上書きされて消えていた…

主な原因

- 保存設定が「上書きあり」になっていた
- ハードディスクの容量不足
- 録画モードが「常時録画」で、データ消費が早かった
- バックアップを取っていなかった

対策

- 録画設定を「上書きあり」から「上書き前に警告」へ変更(機種による)
- 録画期間・画質・フレームレートの最適化で容量を節約
- 重要な映像は手動で USB やクラウドにバックアップ
- 大容量の HDD(4TB ~ 8TB 以上)や RAID 構成で冗長性を確保

ポイント

「いざ必要になった時に映像が残っていない」というトラブルは非常に多いです。定期的な保存チェックとマニュアルの整備が不可欠です。



Q8 関係者から「監視されている」と苦情が来た

主な原因

- カメラの設置場所が私的空間(休憩室・トイレ周辺)に近い
- 導入時に従業員・居住者への説明が不十分だった
- 録画範囲がプライバシーを侵害する恐れがある(例：隣家の敷地)

対策

- プライバシーゾーン設定(映像内でモザイク処理など)を活用
- 設置前に関係者へ説明・同意書の取得を行い、目的・範囲・保存期間を明示
- 監視の意図が業務目的であることを明確化(掲示物、ポリシー策定)
- 苦情が入った場合は速やかに設置角度・録画範囲の見直し

ポイント

プライバシー侵害の問題は法的なトラブルに発展する可能性も。事前に合意形成と文書化を徹底することが、長期的な信頼につながります。



Q9 誰がいつ 設定を変更したかわからない

主な原因

- 複数人が機器にアクセスできる状態
- パスワードが共有されていた
- ログ機能を利用していない

対策

- 管理者アカウントと操作権限を複数レベルに分ける（管理者／一般ユーザー）
- パスワードの定期変更と個別管理を実施
- 操作ログ（アクセス・設定変更）を保存・定期確認
- システムに触れられる人を最小限に制限

ポイント

管理の曖昧さはトラブルの温床です。

「誰が、いつ、何をしたか」が記録に残る環境を整えておくことが重要です。

トラブル 運用・管理編 のポイントまとめ

- ① 防犯カメラの運用ミスや設定不備は「いざという時」に致命傷になる
- ② 映像保存や操作ログなどの「見えない部分」も定期的に確認・管理
- ③ プライバシー配慮は信頼構築と法的リスク回避の両面で重要

設置後トラブル 法的リスクとコンプライアンス編



Q10 カメラの設置が違法になることはある？

主なリスク

- 撮影対象に不特定多数の通行人や隣接住居などが含まれる
- マンション・ビルなどで住民・入居者の同意なく設置した
- 休憩所やトイレ付近などのプライベート空間を監視対象にした

対策

- 撮影範囲は必要最小限にとどめる（目的に合った配置に）
- 建物内では、管理組合や入居者の合意・告知を必ず行う
- 「防犯カメラ作動中」「録画中」の表示を明示する
- 自治体によっては条例でガイドラインがあるため、地域ごとの確認を必須

ポイント

「防犯目的なら何を撮っても OK」は誤解。
個人情報保護法や民法上の“プライバシー権”を常に意識することが重要です。



Q11 録画映像が証拠として使えなかった…なぜ？

主な原因

- 映像の画質が悪くて人物が特定できない
- 時刻設定がずれていて、信用性が損なわれた
- 映像が編集・改ざんされた疑いが生じた
- データ保存形式や再生ソフトが不適切で提出できなかった

対策

- 撮影解像度は 720p 以上、できれば 1080p（フル HD）以上を推奨
- 録画機・カメラの時刻を定期的に NTP サーバと同期
- 映像データは暗号化・改ざん防止の設定を有効にする（メーカー機能）
- 法的提出が想定される場合、メーカー指定の再生ソフトも保管しておく

ポイント

裁判や警察への提出時は、「映像の信頼性」が問われます。
画質、時刻、連続性、改ざん防止の 4 点が鍵です。



Q12 個人が撮影した映像でも問題ないの？

関連法規

- 個人情報保護法により、特定個人を識別可能な映像は「個人情報」に該当
- ただし、防犯目的での設置は一定の範囲で「正当な利用」とされるケースが多い
- インターネット上への無断アップロードは違法となる可能性大

対策

- 映像データの保管には適切な管理体制（パスワード・アクセス制限）を敷く
- SNS や動画サイトへのアップロードは事前に弁護士等と相談を推奨
- 会社・団体に利用する場合は「個人情報取扱規程」への明記が望ましい

ポイント

撮影自体が違法なのではなく、「どう使うか」に問題が生じやすいのが現実。利用目的と方法が正当であることを常に確認しましょう。

トラブル 法的リスクとコンプライアンス編 のポイントまとめ

- ① 防犯カメラの設置には、プライバシーと法令順守の視点が欠かせない
- ② 録画映像を証拠として活用するためには、信頼性の確保が必要
- ③ 地域条例・個人情報保護法などの確認と社内ルール整備が、トラブル回避につながる

トラブルを防ぐためのベストプラクティス

～「備えあれば憂いなし」実践的な防犯カメラ運用術～

計画段階・導入前のチェックリスト

目的の明確化

- ☐ 防犯、監視、証拠記録など用途を整理

撮影範囲の確認

- ☐ 必要なエリアに死角がないか下見を実施

プライバシー配慮

- ☐ 住宅・休憩所などへの撮影が含まれないか

合意形成

- ☐ 関係者・住民・従業員などに説明・同意取得

法令確認

- ☐ 個人情報保護法・条例の確認・相談

防犯カメラ運用の要点チェックリスト

設置前の計画と確認

- ☐ 目的を明確にし、撮影範囲・法令に配慮した設置を行いましょう。
- ☐ 利用する目的やエリアによっては、関係者への説明と同意を必ず取ることが大切です。

運用中の定期的なチェック

- ☐ 録画データの保存状況やカメラの状態、設定の見直しを定期的に行いましょう。
- ☐ 映像データのバックアップや操作ログの管理も重要です。

法的リスクとコンプラの遵守

- ☐ 個人情報保護法やプライバシー権に注意し、侵害を防止する配慮を常に行ってください。
- ☐ 録画映像を証拠として使用する場合は、改ざん防止措置と正確な日時設定が必要です。

防犯カメラの導入でお悩みの場合、
機器選定・現地調査～施工・購入後のサポートまで
アルコムが一貫して対応致します。
まずはご相談ください。

防犯カメラ・
監視カメラ専門店

株式会社アルコム

ARUCOM

製品・サービスに関する
お問い合わせはこちら



0120-7970-83

受付時間ー平日 9:15～17:00

防犯カメラ アルコム

