Verkada

ソリューションの概要

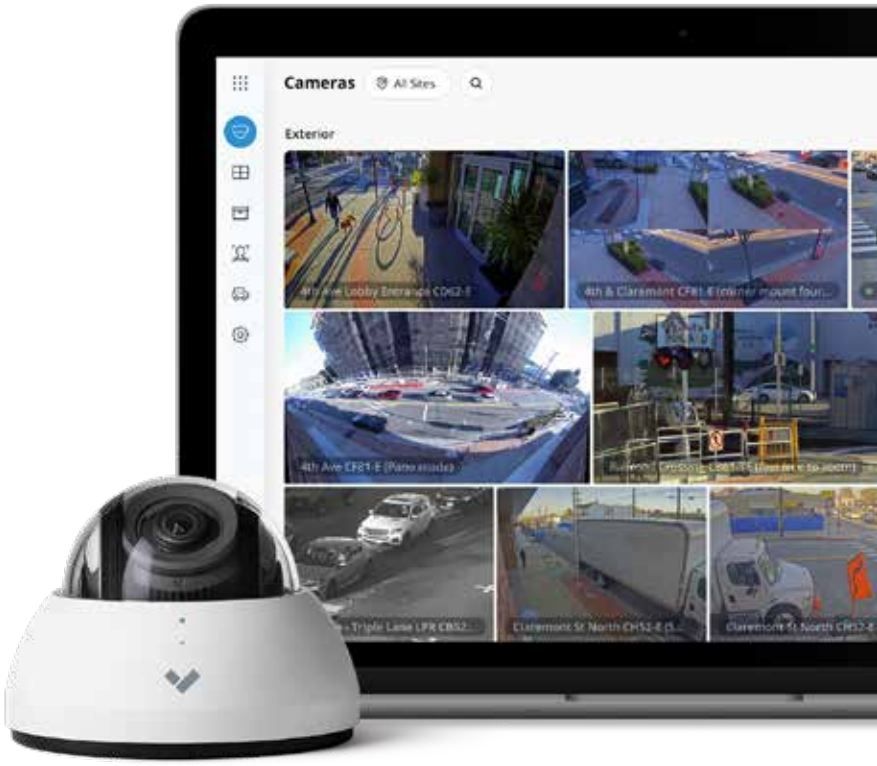
VerkadaのPCI準拠について

VerkadaのPCI準拠について

NVR／DVR不要でローカルとクラウドのストレージに90日以上データを保存

詳細なユーザー監査ログと最新のデータ暗号化標準

早めのアラートで問題を未然に防止



ライブデモを申し込む

verkada.com/demo

概要

Payment Card Industry Data Security Standard（PCI DSS）は、主要なクレジットカード会社がクレジットカード取引を処理する組織に対して義務付けるセキュリティ基準を定めています。この基準はPayment Card Industry Security Standards Councilによって管理され、カード所有者データの保護を強化し、不正行為を低減するために確立されました。

PCIガイドラインへの準拠審査は毎年実施され、組織に応じて次の3つの方法のいずれかで検証されます。

1. 外部のQSA（Qualified Security Assessor: 認定セキュリティ評価機関）によるもの
2. 情報の取り扱い規模の大きな事業者についての特有の認証情報を持つISA（Internal Security Assessor: 内部監査人）によるもの
3. 自己問診票（SAQ）によるもの: 通常、カード情報取り扱い件数の比較的少ない事業所向け

PCI要件9について

PCI DSSバージョン3.0の一部として更新された要件9では、カード会員データへの物理アクセスを制限するために組織が取るべき手順の概要が説明されています。この要件には、販売時点情報管理（POS）システムなどのカード会員データ環境内の物理エリアへのアクセスを制限および監視するために組織が講じるべきガイドラインが含まれています。

PCI DSSでは、この要件（またはその両方）を満たすために、入場アクセスコントロールの装置またはビデオセキュリティカメラを導入することを推奨しています。さらに、次のことが求められます。

- ビデオカメラまたはアクセスコントロールの装置（またはその両方）が、機密エリアへの出入り口を監視するために設置されていることを確認すること。
- ビデオカメラ（またはアクセスコントロール）が改ざんまたは無効化から守られていることを確認すること。
- 収集されたデータを確認し、他のエントリと相関付けること。
- 映像データ（またはアクセスログデータ）を少なくとも3か月間保存されていることを確認すること。

PCI DSSは、物理セキュリティに特有の要件にとどまらず、組織が施設のネットワークとデータのセキュリティを確保するために講じなければならない一連の対策の概要を示しています。

Verkadaのビデオ監視テクノロジーは、現代の企業の高い稼働時間と厳しいデータセキュリティ要件を満たすように特別に設計されています。

Verkadaのハイブリッドクラウドアーキテクチャ

NVRやDVRは不要
産業グレードのオンボードストレージで、最大365日の連続映像を保存1

拡張が容易
帯域幅を圧迫せず、設置箇所の上限数なしで数千台のカメラをサポート

一元化された管理
最新のプラットフォームにより、場所やデバイスを問わず安全なアクセスが可能

Verkadaソリューション

Verkadaは、PCI物理セキュリティ要件を満たすプロセスを簡素化するテクノロジーソリューションを提供します。これまでのCCTVシステムとは異なり、VerkadaはNVR、DVR、オンプレミスサーバーなどの従来型の機器を使用しません。その結果、最新のデータセキュリティ基準と革新的なソフトウェア機能を標準搭載したシステム設計が生まれました。

製品のハイライト

- NVR／DVRやサーバーは不要
- 映像を90日以上保存できるカメラのオンボードストレージ
- クラウドバックアップ（オプション）
- モーションの検出と検索
- 改ざんの検出とアラート
- 詳細なユーザー監査ログ
- HTTPS／SSLデータ暗号化（転送中）
- RSA + AESデータ暗号化（保存時）
- ファームウェアの自動更新

PCI要件9:
物理セキュリティのガイドライン

PCI要件	Verkada対応	備考
9.1.1 カード会員データ環境内のシステムを備えたすべてのコンピュータ室、データセンター、その他の物理エリアで、カメラまたはアクセスコントロールのいずれか、あるいはその両方を使用すること	✓	NVR／DVRの制約を受けないVerkadaシステムは、完全なモジュール式で、拡張が可能です。例えば、データ室をカバーするために1台のカメラを設置し、様々な場所にある数千台のカメラを集中管理できます。
9.1.1.b カメラが改ざんまたは無効化から守られていることを確認すること	✓	Verkadaカメラは、物理モーションセンサーとコンピュータビジョン技術を使用して、改ざんを自動的に検出し、報告します。
9.2 人員と訪問者を区別するための手順を開発すること	✓	Verkadaを使用すると、モーション付きビデオを検索し、異常または予期しない活動が検出できます。インシデントが発生した場合、ユーザーは検出されたインシデントだけでなく、発生の時間と場所を通知するアラートを受け取り事前に対策を講じることができます。
9.3 現場の人員に対する物理アクセスを管理すること	✓	録画されたビデオを簡単に検索して、進入ポイントを通過した人物を具体的に特定します。Verkadaユーザーセッションログを確認して、どの従業員がシステムにアクセスしたかを特定します。

その他のPCI要件

PCI要件	Verkada対応	備考
2.1 ベンダ提供のデフォルトパスワードを使用しないこと	✓	Verkadaシステムには、ベンダが提供するデフォルトのパスワードはありません。SAML／OAuthおよび2要素認証が標準オプションとして利用できます。
10.1 監査証跡を実装すること	✓	Verkadaは、すべてのユーザーアクセスとセッションを自動的に記録します。
10.4 時刻同期技術を使用して、すべての重要なシステムクロックと時間を同期すること	✓	Verkadaシステムは、業界標準のネットワークタイムプロトコル（NTP）を使用して、常に正しい日付と時刻を保持します。
10.5 監査ログへの不正な変更を防止すること	✓	Verkada監査ログは、変更・改ざんできません。
10.5.3 監査ログをバックアップすること	✓	すべてのVerkada監査ログは、地理的に冗長なデータセンターにバックアップされます。
10.6 ログとセキュリティイベントを確認して不審な動きを特定すること	✓	Verkadaを使用すると、管理権限者は、任意のデバイス上の安全な接続を介して、ライブビデオと録画ビデオ、およびユーザーセッションデータを定期的に確認できます。
10.7 監査ログを1年間保管すること	✓	Verkada監査ログは地理的に冗長なデータセンターに安全に保存され、12か月間データを 保存できるように設定できます。