

アクセスコントロールにおいてWiegandではなくOSDPを選択する理由

5月 2025

概要

Wiegandは、アクセスコントロールアプリケーションにおいては現在も一般的なインターフェースですが、セキュリティ上の欠陥があるため、急速に時代遅れになりつつあります。セキュリティを優先する組織は、OSDPに移行し、さまざまな攻撃からの保護を強化すべきです。OSDPでは暗号化され、監視された通信が可能になるため、安全な環境実現に最適です。アクセスコントロールシステムをOSDPにアップグレードすれば、現在のセキュリティが向上するだけでなく、進化する脅威から組織を守ることができます。

目次

1	はじめに	4
2	物理セキュリティソリューションにおけるアクセスコントロール	4
3	リーダーとコントローラー間の通信プロトコル	4
3.1	レガシー規格:Wiegand	5
3.2	安全な代替案: OSDP	5
3.2.1	OSDP認証済み	5
4	WiegandリーダーとOSDPリーダーの比較	5
4.1	Wiegandリーダー	5
4.2	OSDPリーダー	6
4.3	操作性	7
4.4	セキュリティ	7
5	提案・推奨事項	8
6	WiegandからOSDPへの移行	8
6.1	オプション1: WiegandリーダーをOSDPリーダーに置き換える	9
6.2	オプション2: Wiegand-to-OSDPコンバーターを使う	9

1 はじめに

アクセスコントロールシステムの最重要ポイントは、それらが使用する通信プロトコルです。

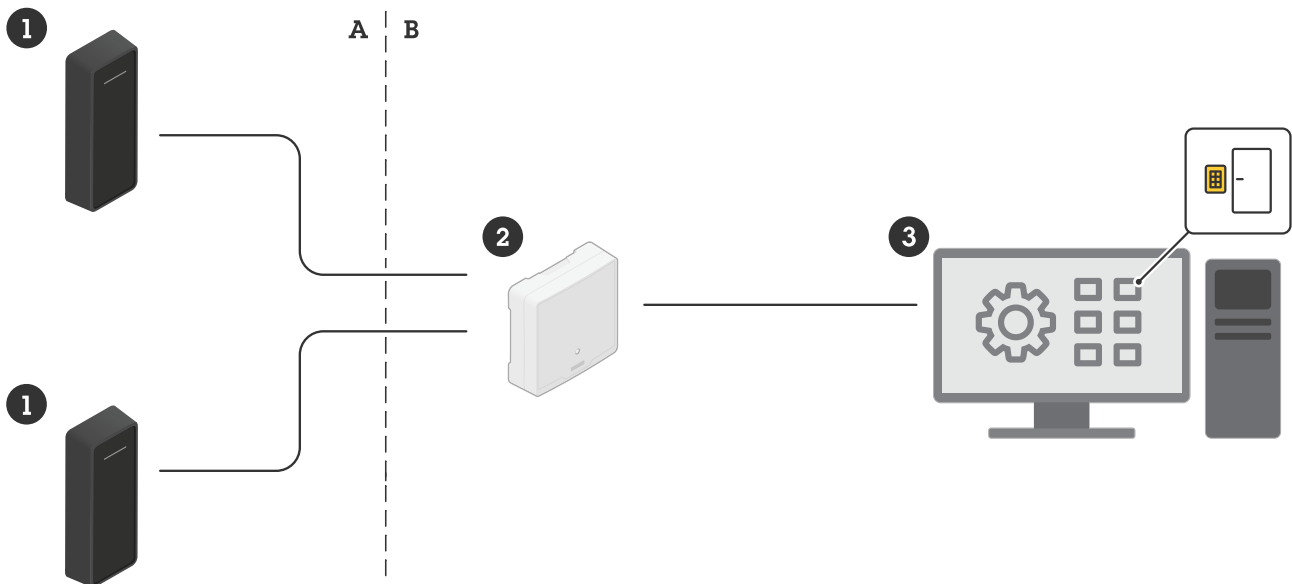
このホワイトペーパーでは、アクセスコントロールシステムでリーダーとドアコントローラーの間で使用される2つの主な通信プロトコルを検討しています。この2つのメリットとデメリットをセキュリティの見地から紹介し、より安全なオプションへの移行を開始する方法についてご説明します。

2 物理セキュリティソリューションにおけるアクセスコントロール

アクセスコントロールシステムは、建物や資産、人々を保護するために不可欠です。このシステムは、許可された人のみが安全なエリアに入れるようにすることで、セキュリティリスクを軽減し、業務効率を向上させます。このようなシステムは、企業のオフィスやデータセンター、医療機関、政府機関など、さまざまな分野で広く使用されています。

一般的なアクセスコントロールシステムは、次の3つの主要コンポーネントで構成されています。

- 1 アクセスコントロールリーダー: ユーザー認証情報を読み取り、認証情報をコントローラーに送信するデバイス。一般的なユーザー認証情報には、キーカード、モバイル認証情報、PIN、生体認証が含まれます。
- 2 ドアコントローラー: 認証情報を処理し、アクセスを許可するか拒否するかを決定する決定ユニット。
- 3 管理ソフトウェア: セキュリティ管理者がアクセス・ポリシーを設定し、アクティビティを監視し、ユーザーを管理するインターフェース。



物理アクセスコントロールでは、リーダー (1) はドアの外側 (非安全エリア、A) に設置され、内側 (安全エリア、B) に設置されたドアコントローラー (2) と通信します。

3 リーダーとコントローラー間の通信プロトコル

アクセスコントロールプロトコルは時とともに進化し、セキュリティ、機能性、統合のしやすさが向上してきました。ここで、主な2つのプロトコルを詳しく見てみましょう。

3.1 レガシー規格:Wiegand

Wiegand は、2 本のデータ線を使用して、認証情報をリーダーからコントローラーに伝送します。Wiegandは何十年も前から存在しており、主にそのシンプルさとレガシーシステムへの対応可能性により、今でも広く使われています。

Wiegandの最大の欠点はセキュリティの低さです。何よりも、暗号化ができません。データは平文で送信されるため、傍受やクローニング攻撃に対して脆弱です。

3.2 安全な代替案: OSDP

Open Supervised Device Protocol (OSDP) は、アクセスコントロールやセキュリティ製品間の相互運用性を向上させるために、Security Industry Association (SIA) によって開発されました。OSDPは、国際電気標準会議によって国際標準として承認され、AES-128暗号化、双方向通信、リアルタイムデバイス監視を導入しています。OSDPはコントローラーがリーダーにコマンドを送り返すことを可能にするため、LED制御やブザー作動、いたずら検知などの機能が可能になります。

OSDPの主な特長は、スマートカードリーダーとコントローラー間で生の認証データの安全な伝送を可能にするセキュアチャンネルモードです。これは、生体認証情報やモバイル認証情報の検証など、高度な認証方法に対して特に有効です。

3.2.1 OSDP認証済み

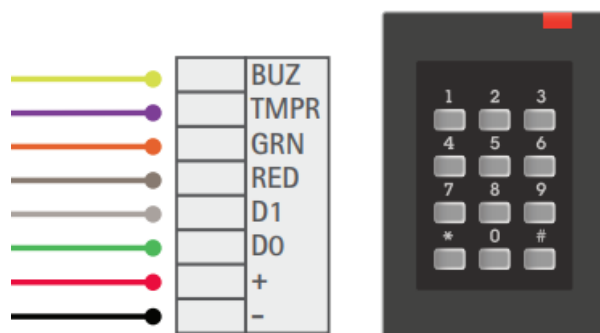
SIA OSDP認証済みプログラムは、デバイスが OSDP 規格および関連する性能プロファイルに適合していることを実証する包括的な試験イニシアティブです。SIAは、試験を受け、規格の基準とリスト内に示されたプロファイルに適合していることが確認された検証済みデバイスのリストを保持しています。リストに含まれるデバイスは、マーケティング資料にOSDP認証マークを使用することができます。

OSDP認証マークは、そのOSDPデバイスがさまざまなタイプのアクセスコントロールのユースケースで意図したとおりに動作するという安心感をインテグレーターや仕様作成者、ユーザーに与えることができます。

4 WiegandリーダーとOSDPリーダーの比較

各リーダーには、使用する通信プロトコルによって異なる長所と短所があります。

4.1 Wiegandリーダー



Wiegandリーダーとその配線（ブザー、いたずら検知、LED用の追加ケーブルを含む）。

メリット:

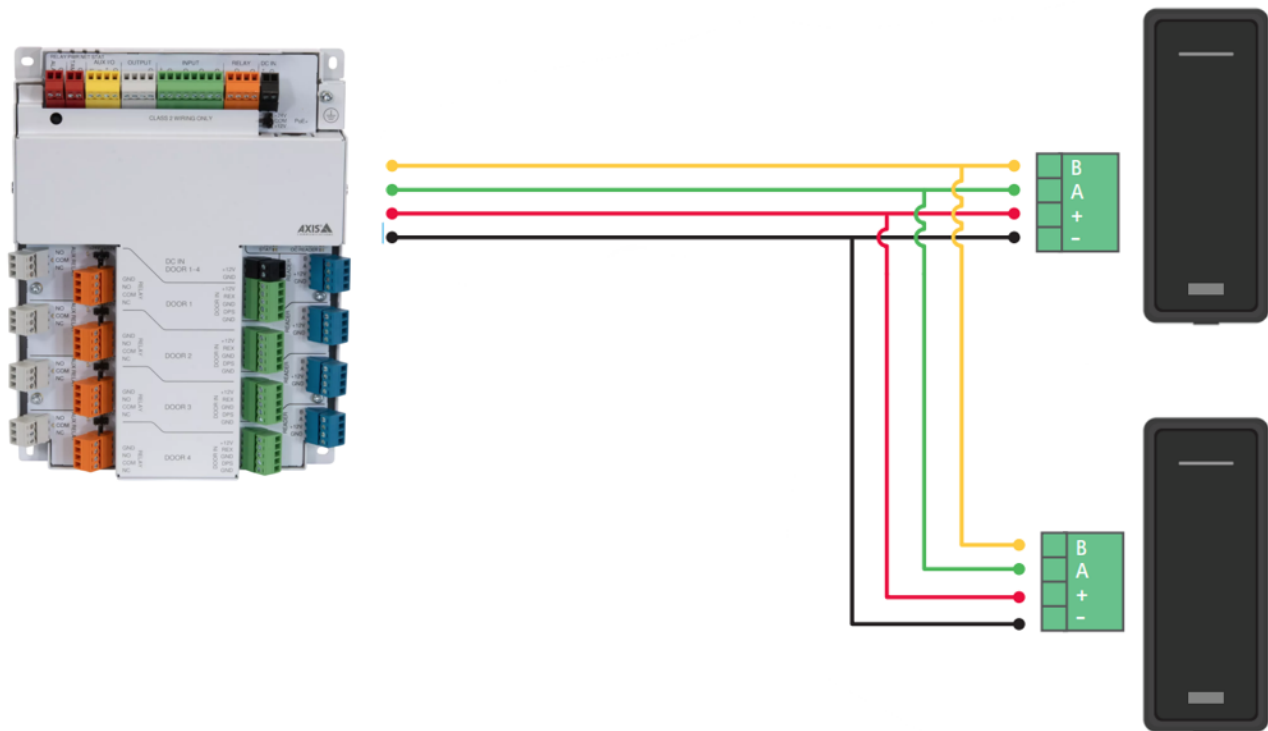
- シンプルで古いシステムとの多くに対応可能。

デメリット:

- 暗号化されない。データは平文で送信されるため、傍受が容易です。

- 通信は一方通行。コントローラーはリーダーにコマンドを送り返すことができません。つまり、リーダーが監視されていないため、リーダーがいたずらされたり交換されたりしても、それを検知する方法がないのです。
- 複雑な配線。Wiegandプロトコルを使用するリーダーは、リーダーブザー、いたずら検知、LED用の追加ケーブルが必要です。
- ケーブルの最大距離は500フィート（約150メートル）です。

4.2 OSDPリーダー



OSDPリーダー（右）とドアコントローラー（左）への配線。LED制御、ブザー作動、リーダー監視などの機能に追加のケーブルは不要です。

OSDPはRS-485配線を使用します。これは、ツイストペアケーブルを使って長距離のデータ伝送を行うシリアル通信規格で、信頼性の高いマルチポイント通信を必要とするシステムでよく使用されています。主な特長に、長距離伝送とマルチドロップ機能があります。

メリット:

- 暗号化通信により、認証情報の傍受を防止できます。
- OSDPにより、コントローラーはリーダーにコマンドを送り返すことができます。この双方向のデータ交換により、監視と遠隔設定が可能になります。配線も容易になります。
- RS-485配線により、最大ケーブル距離がさらに長くなります。
- マルチドロップ機能により、複数のリーダーが1つの接続を共有できるようになります。

4.3 操作性

表 4.1 WiegandリーダーとOSDPリーダーの操作性の比較。

	Wiegand	OSDP
セキュリティ	暗号化がなく、ハッキングに弱い	AES-128暗号化、いたずら検知
コミュニケーション	一方向（リーダーからコントローラー）	双方向
ケーブルの長さ	最大500フィート（約150メートル）	最大4000フィート（約1200メートル）
マルチドロップ	不可: 1デバイス1バス	可: 1つのバスで複数のデバイスをサポート
いたずら検知	不可: 追加配線が必要	必要
監視	不可: 追加配線が必要	必要
データの完全性	認証情報リプレイ攻撃に弱い	暗号化された安全な伝送
設置の複雑さ	複雑な配線（D0/D1とLED、いたずら、ブザー）	容易（RS-485、AおよびB）
拡張性	配線の制約による制限あり	複数のリーダーを1本のディジーチェーンで接続可能
最適なユースケース	レガシーシステムでセキュリティニーズが低い場合	政府機関や企業などの分野における最新のセキュアな設備

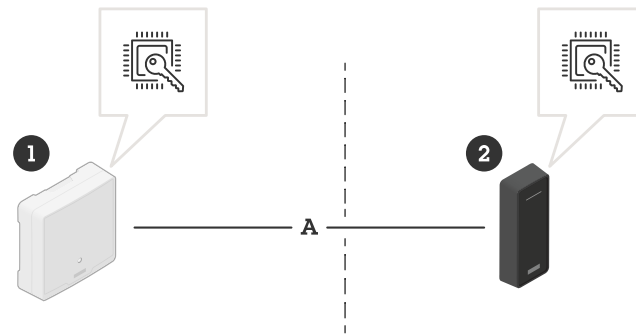
4.4 セキュリティ

アクセスコントロールプロトコルを選択する際には、セキュリティを最優先事項とすべきです。Wiegandは暗号化されていないため、次のようなタイプの攻撃を受けやすくなります。

- 認証情報の傍受。攻撃者はデータ回線を盗聴し、認証情報を取得することができます。
- リプレイ攻撃。認証情報が一度盗まれると、同じ情報を利用して不正アクセスを行うことができます。
- いたずら。システムは、リーダーが取り外されたり交換されたりしても、それを検知できません。

これとは対照的に、OSDPはAES-128（セキュアチャンネル）でデータを暗号化し、デバイスを監視することによって、これらのリスクを軽減できます。これにより、コントローラーはリーダーへのいたずらが行われた場合にそれを検知でき、不正アクセスを防ぐことができます。

暗号化によってデータは安全に保たれますが、暗号化を安全に保つには鍵を保護する必要があります。鍵をしっかりと保護しなければ、システム全体が危険にさらされる恐れがあります。そのため、セキュアチャンネルの鍵は、コントローラーとリーダーの両方にある特別なハードウェアチップに安全に保管する必要があります。このようなセキュアハードウェアエリア（例: セキュアエレメント）は、攻撃者がそのデバイスに物理的にアクセスしても鍵を入手できないように設計されています。



アクセスコントロールにおける安全なキーストアにより、エンドツーエンドセキュリティが実現します。マスターキーと個々のSCBKはそれぞれ、ドアの両側にあるデバイスの安全なキーストアに格納されます。

- 1 ドアの安全側に設置されたドアコントローラー
- 2 ドアの非安全側に設置されたリーダー
- 3 A: OSDPセキュアチャンネル通信

表 4.2 WiegandリーダーとOSDPリーダーのセキュリティ面の比較。

	Wiegand	OSDP
暗号化	なし、平文データ	AES-128暗号化
データ傍受	認証情報の傍受が容易	傍受を防ぐために暗号化
リプレイ攻撃	認証情報のコピー/再生が可能	暗号化によって防止
いたずら検知	不可: リーダーへのいたずらを検知できない	可: コントローラーがリーダーのステータスを監視
監視	不可: コントローラーはリーダーのステータスを確認できない	可: リアルタイム監視
コンプライアンス	安全な環境実現には推奨されない	最新のセキュリティ基準に適合

5 提案・推奨事項

今日のセキュリティシステムでは、Wiegandはもはや、新規設置にあたっての有効な選択肢ではありません。より優れたセキュリティ、信頼性、将来の拡張性を考慮すれば、組織はOSDPリーダーに移行すべきです。

- 現在のアクセスコントロールインフラストラクチャーを評価してください。現在Wiegandを使用している場合は、移行戦略を練り始めましょう。完全なOSDPマイグレーションとWiegand-to-OSDPコンバーターのどちらが最良のオプションかを判断します。
- 新規設置の場合は、暗号化され、いたずらを防止できる通信を確実にするため、可能な限りOSDPリーダーを選択してください。
- セキュリティの専門家と協力して、脅威から守られる安全で最新のアクセスコントロールシステムを導入しましょう。

6 WiegandからOSDPへの移行

現在もWiegandリーダーを使用している組織の多くが、システム全体を交換することなくセキュリティを強化したいと考えています。現実的な移行方法は2つあります。どちらのオプションもセ

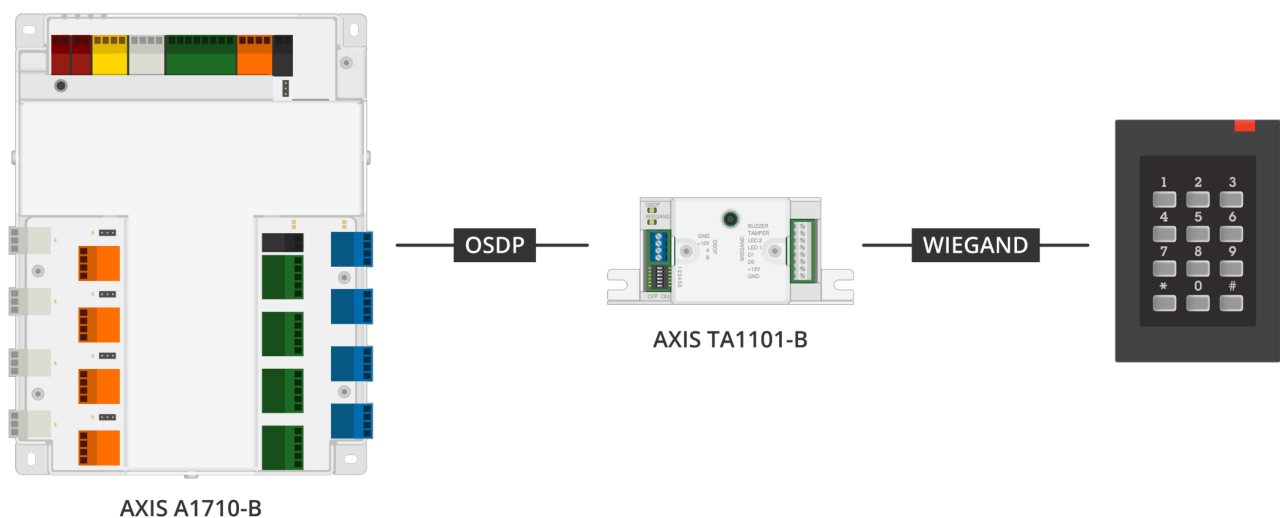
セキュリティを向上させますが、将来も使用できるアクセスコントロールシステムを求める組織にとっては、OSDPを直接導入することが長期的な投資として最適です。

6.1 オプション1: WiegandリーダーをOSDPリーダーに置き換える

長期的には、これが最善の策です。旧式のWiegandリーダーをOSDP準拠モデルに置き換えることで、組織は暗号化、双方向コミュニケーション、リーダー監視というメリットを得ることができます。ただし、そのためにはアクセスコントロールパネルがOSDPをサポートしていることを確認する必要があります。

6.2 オプション2: Wiegand-to-OSDPコンバーターを使う

すべてのリーダーをすぐに交換できない組織にとって、Wiegand-to-OSDPコンバーターは費用対効果の高い代替手段です。このデバイスは、OSDP対応コントローラーに送信する前にWiegandデータを暗号化するため、ハードウェアを完全にオーバーホールしなくても、セキュリティを向上させることができます。



Wiegand-to-OSDPコンバーター（中央）を使えば、セキュリティを向上させることができます。

Axis Communicationsについて

Axisは、セキュリティ、安全性、運用効率、ビジネスインテリジェンスを向上させることで、よりスマートでより安全な世界の実現を目指しています。ネットワークテクノロジー企業として、また業界をけん引するリーダーとして、Axisは映像監視、アクセスコントロール、インターコム、音声ソリューションを提供しています。これらのソリューションは、インテリジェントアプリケーションによって強化され、質の高いトレーニングによってサポートされています。

Axisは50ヶ国以上に5,000人を超える熱意にあふれた従業員を擁し、世界中のテクノロジーパートナーやシステムインテグレーションパートナーと連携することで、カスタマーソリューションをお届けしています。Axisは1984年に創業し、本社はスウェーデン・ルンドにあります。