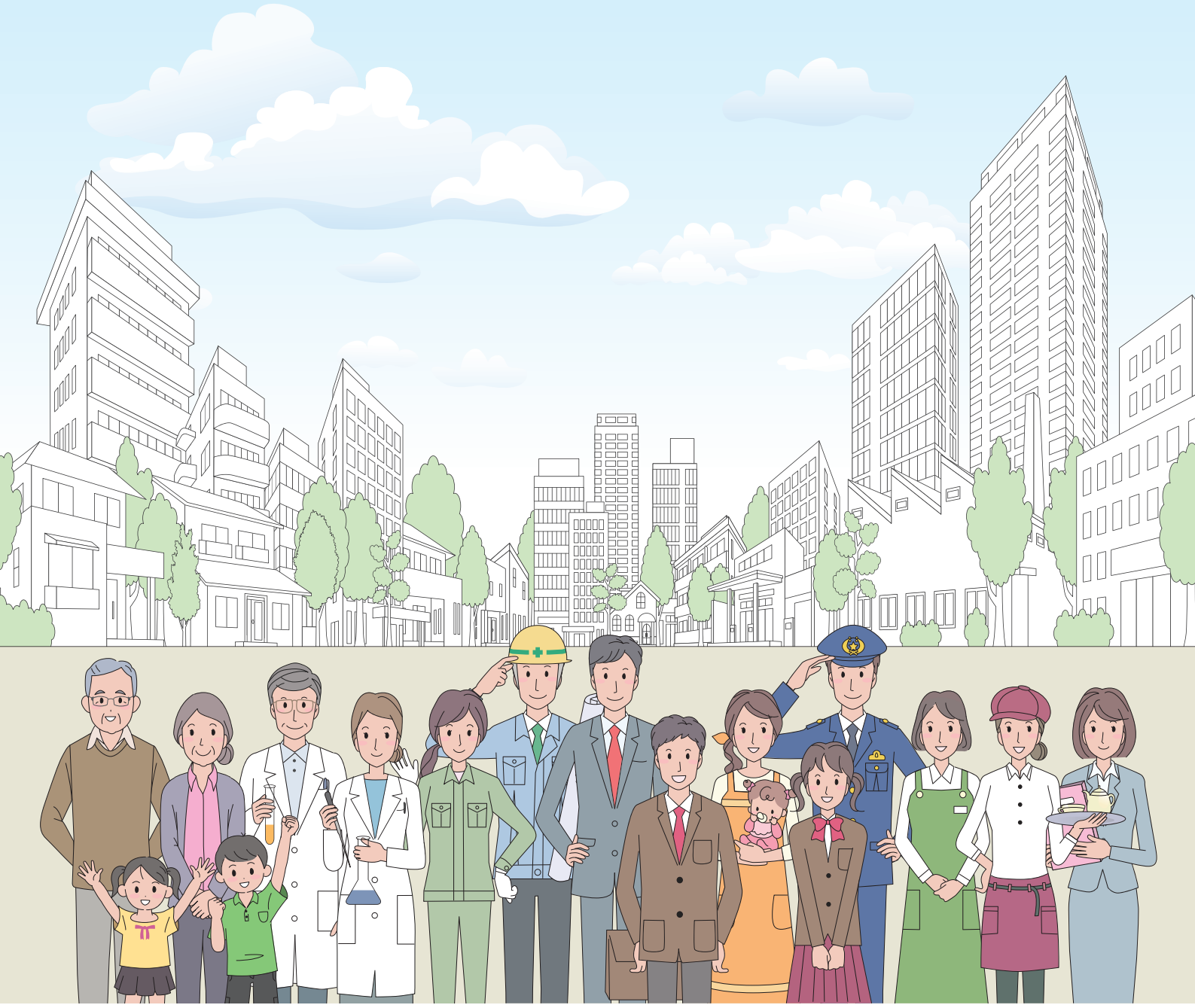
暗証番号やカード、生体認証による出入りの制限と管理

出入口のセキュリティガイド



公益社団法人 日本防犯設備協会

はじめに

刑法犯の認知件数は平成14年をピークに減少しています。これは、官民一体となった総合的な犯罪対策の推進や防犯機器の普及などによるものが考えられます。一方で、人身安全に関わる犯罪、特殊詐欺、サイバー犯罪など、新たな治安上の課題が顕在化しています。また事業所などでは、個人情報を含む機密情報の持ち出しや情報漏えいなどの犯罪も問題となっています。少子高齢化が進行し、コミュニケーションやビジネスにおける情報通信技術の活用が不可欠となる中で、今後深刻な問題となることが予想されます。

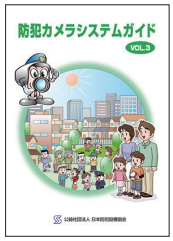
このような犯罪の多様化に的確に対処するためには、従来の対策を不断に見直すことに加えて、社会情勢の変化に迅速かつ柔軟に対応し、それを補完するための専門知識の提供や適切な防犯設備の導入が大変重要なものとなります。

本ガイドは、公益社団法人日本防犯設備協会が、敷地や住宅、オフィスビルなどの建物や部屋への出入りを制限及び管理するシステムについて、一般の方にわかりやすく示したものです。出入管理システムの導入にあたり、本ガイドを参考にしていただければ幸いです。

目　次

■本ガイドの位置づけ

本ガイドは出入口の通行制限及びそれに関わる運用・管理のための入門書としての役割を目的とします。
より幅広く防犯を考えるためには、各種センサーや防犯カメラ、防犯照明などとの併用をおすすめします。
それらの詳細は当協会のガイドがありますので、そちらを参考にしてください。



防犯カメラシステムガイド

防犯照明ガイド

駐車場セキュリティガイド

ホームセキュリティガイド

■侵入犯罪のデータ

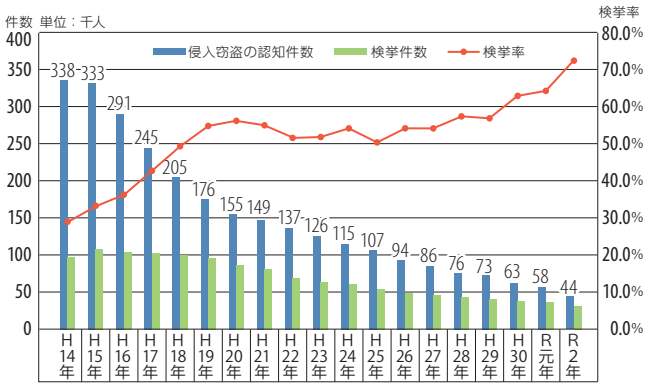
侵入窃盗の認知件数は、ピーク時の平成14年（33万8,294件）以降減少傾向にあり、同年から令和2年にかけて、29万4,201件（87.0％）減少しました。それに伴い検挙件数及び検挙人員も年々減少していますが、検挙率は増加の傾向にあります。

侵入窃盗の発生場所別認知件数は、一戸建住宅が37.0％と最も多く、共同住宅を含めた住宅は約5割です。次いで一般事務所が11.7％ですが、店舗・事務所等は約3割を占めています。

侵入窃盗は、国民にとって最も身近に発生し、被害にあうリスクの高い危険な犯罪です。犯罪から自分自身はもとより、家族や身近な人たちの安全や財産を守るためには、高い防犯意識と正しい知識を身に着け、必要な対策をとることが重要です。

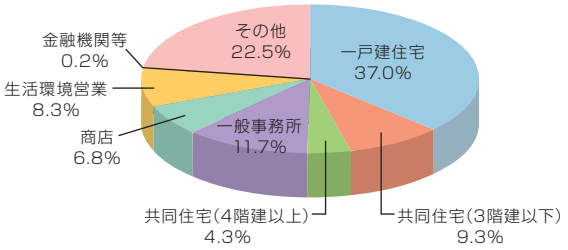
国民の不安を払拭し、安全で安心な社会を作るためには、適切な防犯設備・部品の設置や防犯カメラ、出入管理システム等を有効活用するといったハード面の対策はもとより、地域住民の連携・協力による防犯パトロール等のソフト面の対策も併せて推進していくことが不可欠です。

侵入窃盗の認知・検挙状況の推移



出典：警察庁

侵入窃盗の発生場所別認知件数 総数44,093件（令和2年）



出典：警察庁 住まいる防犯110番

■法令・指針の紹介

法令

平成 15年　5月 28日	「特殊開錠用具の所持の禁止等に関する法律」が成立する。
平成 15年　5月 30日	「個人情報の保護に関する法律」が施行される。
平成 17年　11月　1日	不正競争防止法が改正（営業秘密の保護強化）され、施行される。
平成 25年　5月 31日	不正アクセス禁止法（改正）が施行される。不正なパスワードの取得などが禁止される。
平成 27年　1月　9日	サイバーセキュリティ基本法が施行される。日本のサイバーセキュリティに関する施策に関して、基本理念を定める。
平成 29年　5月 30日	個人情報保護法が改正される。小規模取扱事業者にも適用範囲が拡大。情報漏洩に対する罰則を新設される。

指針

平成 13年　3月 23日	警察庁・国土交通省が「共同住宅の防犯上の留意事項」及び「防犯に配慮した共同住宅の設計指針」を共同策定する。
平成 14年　11月 25日	「防犯性能の高い建物部品の開発・普及に関する官民合同会議」が設置される。
平成 17年　6月 28日	「安全・安心なまちづくり全国展開プラン」が犯罪対策閣僚会議・都市再生本部合同会議で決定される。
平成 18年　4月 20日	防犯性能の高いマンションを普及させるために、「防犯優良マンション認定制度」がスタートする。 （(財)ベターリビング、(財)全国防犯協会連合会、(社)日本防犯設備協会）
平成 18年　10月 23日	「防犯性能の高い建物部品の開発・普及に関する官民合同会議」にて、電気錠システムの追加が承認される。
平成 25年　12月 10日	「世界一安全な日本」創造戦略が閣議決定される。
平成　31年　4月　1日	「防犯優良マンション認定事業支援要綱」、「防犯優良マンション標準認定規定」及び「防犯優良マンション標準認定基準」の一部が改正される。（(公財)全国防犯協会連合会、(公社)日本防犯設備協会）

防犯性能の高い建物部品

警察庁、経済産業省、国土交通省及び建物部品関連の民間団体から構成される「防犯性能の高い建物部品の開発・普及に関する官民合同会議」では、平成16年4月から、侵入までに5分以上の時間を要するなど一定の防犯性能があると評価した建物部品（CP部品）を掲載した「防犯性能の高い建物部品目録」をウェブサイトで公表するなどして、CP部品の普及に努めています。

この目録には令和3年3月末現在で17種類3,434品目が掲載されており、右のような統一マークが使用されています。

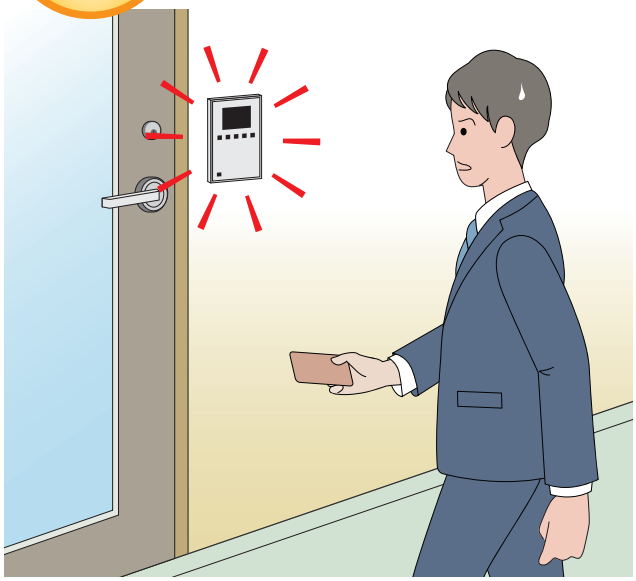
出入管理の基本的な考え方

■出入管理システム導入のメリット

出入管理システムは家やビルなどの建造物や指定地域への出入りを制限及び管理するためのシステムです。認証端末を使って運用・管理することにより、不正な侵入を防ぐことができます。また、一般的に重要施設と言われる空港や発電所、電算室、研究所に始まり、オフィスビルや商業施設だけでなく、最近は住宅など我々の身近なところへの導入が進んできています。認証方法も暗証番号を使った方法から、非接触カードや生体認証など種類が増えてきています。また、ID情報のみで電気錠を解錠して入室する管理方法から、時間帯や使用する人の通行履歴・運用状態まで集中管理するシステムへ変化してきています。侵入犯罪の防止だけでなく、機密情報のある部屋へ出入可能な人を制限したり、通行の履歴を出退勤データに利用することもできます。

威嚇効果 出入管理システムを見てドロボーが諦める

出入制限 部外者の侵入を阻止する



履歴管理 犯罪が発生した場合、いつ誰が出入口を通過したかを確認する

監　視 不正な侵入がないか、離れた場所で監視する

■セキュリティエリア別管理

侵入者や部外者から身を守るためには、まず敷地外周のフェンスや建物の壁といった障壁が重要となります。
次に、建物に入る権限を持った人だけが、その出入口を通行できるようにする必要があります。

セキュリティエリア（基本警戒線）という考え方

敷地内をいくつかのエリアに分割してセキュリティの重要度を分けます。
このエリアごとに守るべき大事な防犯対象物を取り囲むように
設けた各部分及び部分間の境界のことを
基本警戒線と呼びます。

第一警戒線（G1）

- 敷地の外周部【塀、門など】
- 構内部【駐車場】

第二警戒線（G2）

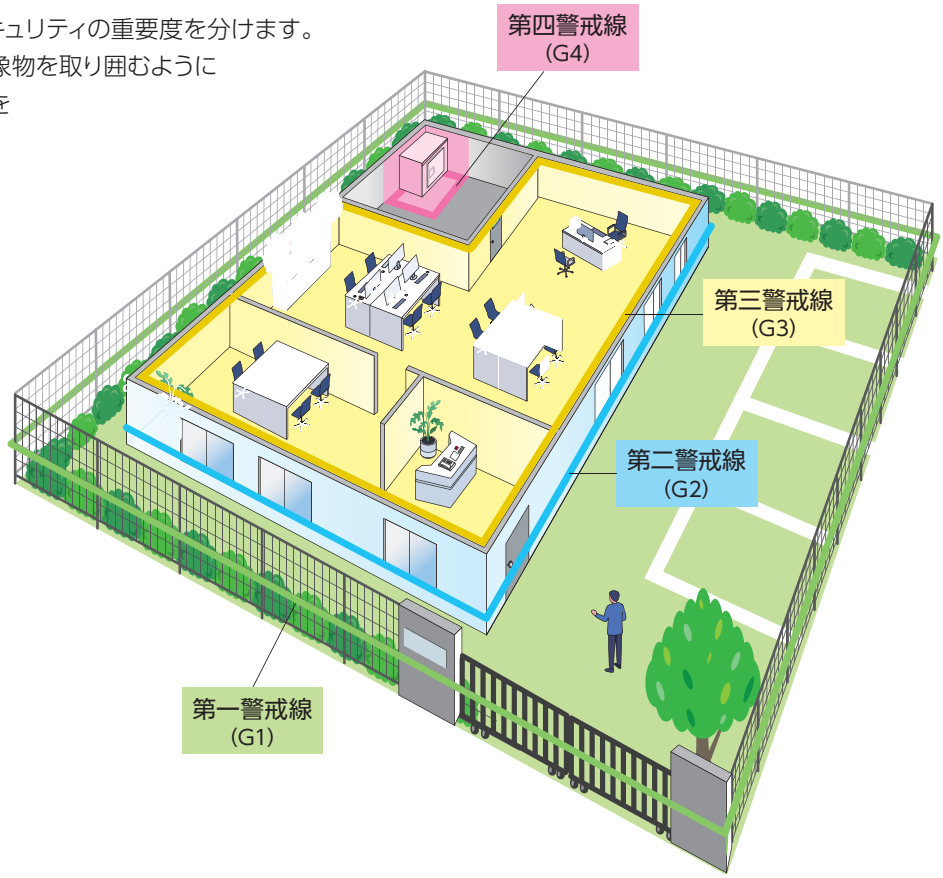
- 建物の外周部
  【玄関、窓、勝手口、屋根、外壁など】

第三警戒線（G3）

- 建造物の内部
  【屋内、施錠する室の壁面・
  開口部・出入口・室内など】

第四警戒線（G4）

- 重要対象物
  【金庫、宝石箱など】



用語解説

【生体認証】
人が持つ行動的または身体的な特徴を用いて、個人を特定する技術です。バイオメトリクスとも呼びます。
指紋、静脈、顔、虹彩認証などがあります。

【出入管理システム】
出入管理システムとは、常時またはあらかじめ設定した時間帯に、家屋、ビルなどの建造物または指定地域への出入りを制限及び、管理することを目的とする装置のことです。
詳細は、P6を参照ください。

【出入口】
建物や敷地に出入りするための開口部です。開き扉（スイングドア）、自動ドア（スライドドア）、ゲートなどがあります。
詳細は、P5を参照ください。

【電気錠】
電気的な施解錠制御が可能な錠前です。

【認証端末】
出入りする権限の有無を認証するための機器です。
あらかじめ登録したデータと入力されたデータを照合します。
認証方式は暗証番号、非接触カード、生体認証など様々なものがあります。

出入口の種類と管理

出入口には扉の種類・設置場所に応じた最適な防犯設備を設置することが重要です。
出入管理を行う場合は、扉によって電気錠の設置が必要となります。

■出入口の種類

門　扉

建物と外部との境界に設ける扉です。開き扉型と引き扉型があります。
屋外にあるため、錠前には防水性を考慮する必要があります。

自動ドア

扉の前に立ったり、ボタンを押すと自動で左右にスライドする扉です。
認証端末を設けて開扉することもできます。

ゲート

許可された人を認証し、フラップやパネルを開きます。不正通行を検知して阻止・発報することも可能です。

開き扉

ドアノブやハンドルにより開閉する扉です。構造によって大きく2種類に分かれます。

○フラッシュ扉：扉表面が平らな扉
○かまち扉：かまち（囲み枠）によって構成された扉

■電気錠・電気ストライク・電磁錠について

電気錠には使用する条件（目的）によって、設置する電気錠が異なります。

・電気錠：電気錠制御盤からの通電によって、内部の機構を動作させて施錠・解錠する錠前です。
・電気ストライク：扉側には一般の錠前を設置し、枠側のストライクと呼ばれる受座を通電によって施錠・解錠します。
・電磁錠：電気錠制御盤からの通電によって、内蔵した電磁石がストライクプレートを吸着して施錠します。

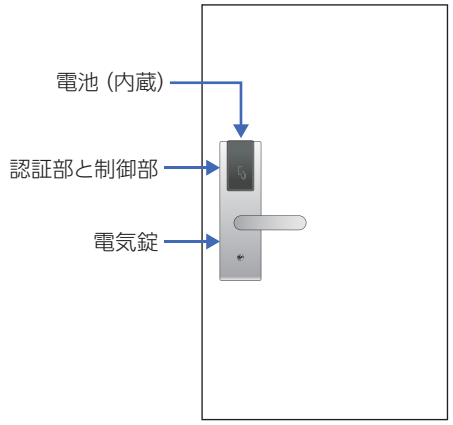
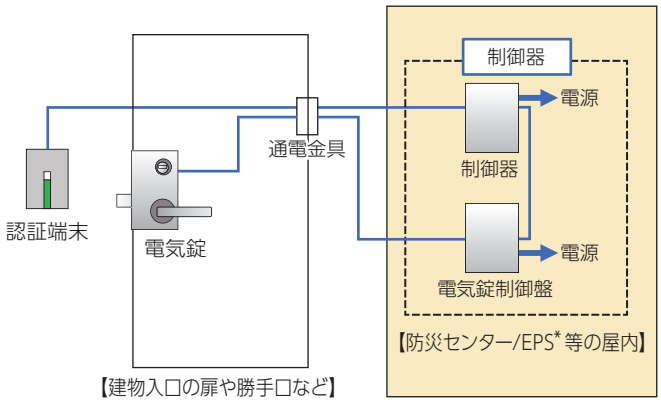
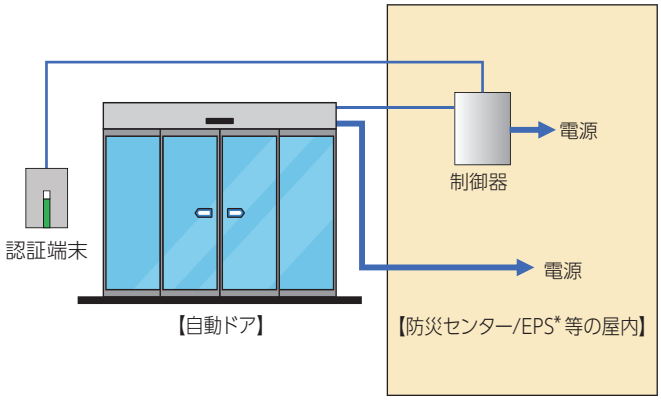
種類・名称		概要	使用条件（目的）			
			防犯性が高い部屋 例）資料室 金庫室	通行の多い場所 例）エントランス 通用口	災害時に通行する場所 例）非常口	通行が多く自動施錠が必要な場所 例）オフィス出入口
電気錠	通電時解錠型	通電中は解錠します（停電時は施錠） ※防災より防犯を優先する場所に使用します。	○	△	△	○
	通電時施錠型	通電中は施錠します（停電時は解錠） ※防犯より防災を優先する場所に使用します。	－	△	○	○
	瞬時通電施解錠型	通電するたび施錠・解錠します（停電時は状態保持） ※エネルギー消費が少ないため、施錠や解錠の状態を長時間維持する場所で効果的です。	○	○	△	△
	モーター式本締錠	通電するたび施錠・解錠します（停電時は状態保持） ※主にノブやハンドルが付けられない扉に使用します。	○	○	△	△
電気ストライク	通電時解錠型	通電中は解錠します（停電時は施錠）	－	○	△	○
	通電時施錠型	通電中は施錠します（停電時は解錠）	－	△	○	○
電磁錠	通電時施錠型	通電中は施錠します（停電時は解錠）	－	△	○	○

凡例　○：適している　△：使用できる（都度検討する）　－：適さない

出入管理システムの基本構成について

出入管理システムを導入するためには、制御するための機器の設置が必要です。
機器は主に『電気錠』(または自動ドア)、『制御器』、『認証端末』の3つに分かれます。
制御器は、認証端末の制御器と、電気錠制御盤が別々になっている場合もあります。

一般的な出入管理システムの機器構成例を紹介します。

分類	扉	概要	システム構成図
一体型	開き扉	電気錠と認証端末、制御器が一体になったシステムです。 一体型の多くが電池で動作するため、配線工事が不要のものが一般的で、機能は比較的シンプルです。 しかし一つの扉単位でシステムが完結するシンプルな構成であるため、火災報知器などと連携できない機器も多く、非常口などの使用は推奨できません。	 【事務所内の扉など】
分離型	開き扉	最も一般的な構成です。 制御器1台で複数の扉を管理することができます。 一般的に火災報知器などと連携できる機器が多く、有事の際に一斉解錠することが可能です。 ネットワークを介することで遠隔操作・通行者を管理することもできます。 認証端末は、一般的に、 ●カードリーダー ●テンキー などを使用します。 詳細は、P7を参照ください。	 【建物入口の扉や勝手口など】
分離型	自動ドア	共用エントランスなどに多い構成です。 上記と同様に、一般的には火災報知器などと連携できる機器が多く、有事の際に複数の自動ドアを一斉解錠することが可能です。 ネットワークを介することで遠隔操作・通行者を管理することもできます。 認証端末は、一般的に、 ●カードリーダー ●テンキー などを使用します。 詳細は、P7を参照ください。	

*EPS（electric pipe shaft 電気配線シャフト）

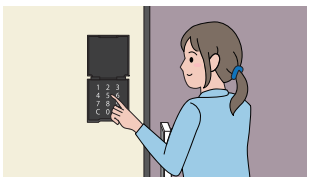
認証端末と認証方法

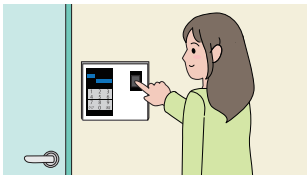
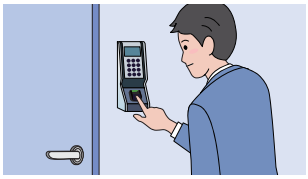
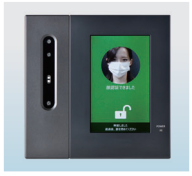
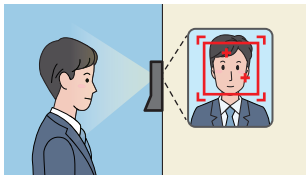
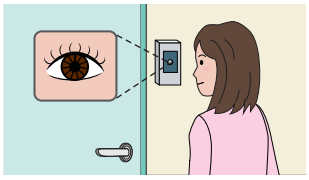
■認証とは

認証とは、本人しか持ち得ないものや情報を利用して本人であることを証明することです。
本人であることを認証する手段を大別すると以下の通りです。

- ●本人しか知らない情報による認証・・・・・・・・・・・・・・・暗証番号、パスワード等
- ●本人しか持っていない所有物による認証・・・・・・・・・・・非接触カード、タグ等
- ●本人しか持っていない身体的な特徴による認証（生体認証）・・・・指紋、静脈、顔、虹彩等

一般的にセキュリティレベルをより高くするために、上記認証方法を組み合わせる場合があります。

認証種類	認証端末と認証方法	特　　徴
本人しか知らない情報による認証	**テンキー認証** 登録した番号（例：0から9までの数字を組み合わせた暗証番号）を押すことによって認証します。 番号が一致した場合に施解錠や警備の開始などを行います。 	•暗証番号を覚えておけば非接触カードやタグが不要 •鍵や非接触カードの紛失、盗難、複製による不正な解錠を防止 •個人の入退室の履歴を記録できない •定期的に暗証番号の変更が必要 •暗証番号ののぞき見により他人に知られると、不正侵入される恐れがある 
本人しか持っていない所有物による認証	**非接触カード／タグ認証** カード内部にICチップとアンテナを埋め込んだ非接触カード／タグを使って認証します。非接触カードをリーダーにかざすようにして認証します。反応する範囲は数cm程度です。電磁誘導を利用して通信を行うため、非接触カードには電池が必要ありません。また、接触する金属部分がなく、保守性に優れています。 	•認証媒体として、非接触カード／タグが必要 •個人の入退室の履歴を記録することが可能 •非接触カードの場合は、券面印刷が必要な証書（社員証、学生証など）との兼用も可能 
	スマートフォンによる認証 スマートフォンやタブレットなどに標準搭載されているBLE通信機能やNFCタグを使って認証を可能にします。※ユーザーが普段から使っているスマートフォンに専用アプリケーションをインストールすることで認証端末として利用することができます。 ※BLE：Bluetooth Low Energy NFC：Near Field Communication	•認証媒体として、スマートフォンやタブレットが必要 •機能的に社員証や学生証等の兼用も可能

認証種類	認証端末と認証方法	特　　徴
本人しか持っていない身体的な特徴による認証【生体認証】	**指紋認証（指の指紋）** 読取装置に指を置き、読み取った指紋があらかじめ登録した指紋パターンに一致するか否かで本人を認証します。指紋は人によって異なり、年月を経ても変化しないという特徴があります。指先を読み取るだけでよいので機器の小型化が可能です。 	•暗証番号忘れ、非接触カードの紛失・盗難リスクがない •指紋は年月を経ても変化しない •指紋が薄いなどの理由で読み取れない場合がある 
	静脈認証（指/手のひら/手の甲） 赤外線などを使って手の静脈を撮影し、あらかじめ登録した静脈パターンに一致するか否かで本人を認証します。静脈パターンは人により異なり、大きさ以外は成長や老化などによらず生涯変わらないという特徴があります。  	•静脈パターンは大きさ以外は、成長・老化によらず生涯変わらない •静脈は体内の器官であり、偽造は非常に困難 •手袋装着では認証不可 
	顔認証（輪郭/目/鼻/口の配置） 撮影した顔の画像から特徴点（輪郭、目、鼻、口の配置など）を抽出し、あらかじめ登録した特徴データに一致するか否かで本人を認証します。人の顔は髪形や表情、成長、老化、整形、怪我によって変化するため、これらの影響を極力受けないように補正を行います。   	•カメラの前に立つだけで、心理的な抵抗感が少ない •ハンズフリーでの認証が可能で、衛生面での心配がない •サングラスをかけたり目を閉じたり、毛髪で目が隠れたりして顔の特徴が撮影できないと認証できない場合がある 
	虹彩認証（虹彩の模様） 眼球の黒目部分には瞳孔の外側に「虹彩（アイリス）」と呼ばれる環状の部分があり眼球の形成時に細かい皺ができます。これは年を取っても変化することがなく、この皺のパターンを指紋のような本人固有の情報と捉え、認証に利用するのが虹彩認証です。	•目の虹彩（放射状の模様）の特徴点照合であり、年を取っても変化することがなく、偽造も困難 •カメラの前に立つだけで、心理的な抵抗感が少ない •ハンズフリーでの認証が可能で、衛生面での心配がない •目の細い人は認証しにくい場合がある 

出入管理システム導入までの流れ

■出入管理システム導入までの流れ

① 導入 / 運用方針の策定 → ② 具体的な導入計画 機器選定 → ③ 工事 / 運用開始準備 → ④ 運用開始 評価・是正

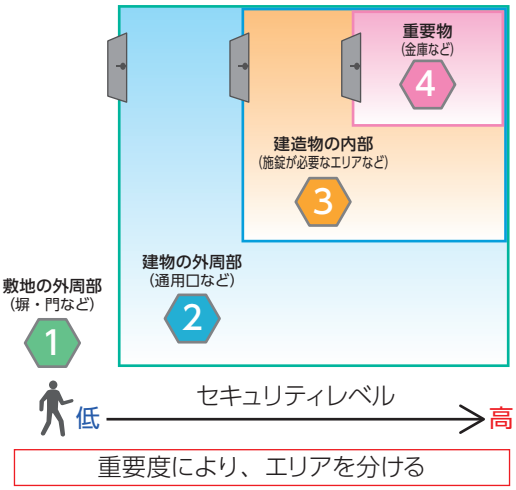
運用方針や導入規模によって選定する機器や使用する機能が変わってくるため、事前に以下のような防犯対策の検討を行う必要があります。

① 導入 / 運用方針の策定

施設の部屋ごとに守りたいものと、それに対する考え得る脅威を洗い出します。

部屋の種類（例）	守りたいもの（例）	脅威（例）	重要度
共用部 エントランス	物品	●部外者による 暴力/破壊行為・盗難	低
事務室	物品・機器 内部書類	●部外者による 暴力/破壊行為・盗難 ●内部犯罪による 会社情報の漏洩	中
サーバールーム	物品・機器 重要データ	●内部犯罪による 会社情報の漏洩 ●物理的破壊行為による システム停止・サーバーダウン	高

・部屋とセキュリティレベルの定義



② 具体的な導入計画と機器選定

出入管理機器の選定においては、セキュリティレベルの高さや利便性、火災や停電時の対応など、様々な観点から検討します。

部屋の重要度（エリア）	セキュリティレベル	利便性	認証方法	火災・停電時の対応	選定機器（例）
低	低	高	暗証番号や 非接触カード	避難のため開放	電気錠 テンキー／カードリーダー 警戒センサー／防犯カメラ　等
中	中	中	暗証番号や 非接触カード	避難のため開放	電気錠 テンキー／カードリーダー 警戒センサー／防犯カメラ ゲート　等
高	高	低	非接触カードや 生体認証	重要物保護の ため施錠	電気錠 カードリーダー／生体認証端末 警戒センサー／防犯カメラ ゲート　等

③ 工事 / 運用開始準備

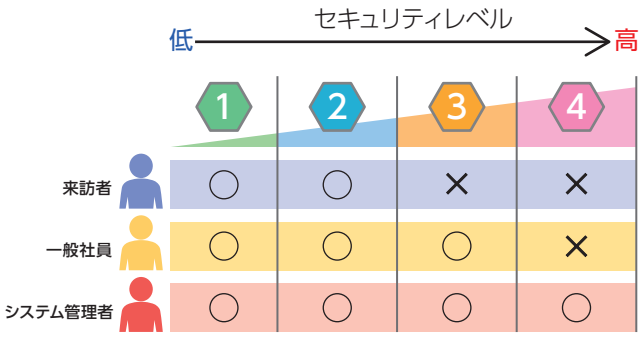
●導入工事内容と工事区分の確認

導入機器が決まったら、機器の設置工事に入ります。
工事の内容及び区分については販売会社へお問い合わせ、及び施工会社と打ち合わせの上、ご準備ください。

●運用ルールと通行権限設定

出入管理の運用が開始します。
工事準備と並行して運用開始に向けた運用ルールや認証方法、通行（出入）権限を決めます。

●セキュリティレベルに応じた運用方針の定義（通行権限）



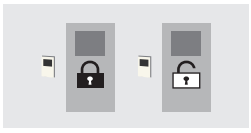
部屋の重要度	施解錠のルール	認証方法	通行可能者	セキュリティ機能
低	夜間・休日のみ施錠 平日日中は解錠	夜間休日：非接触カード＋暗証番号 平日日中：認証なし	全社員 受付後の来訪者	なし
中	常時施錠	常時：非接触カード	全社員	アンチパスバック機能
高	常時施錠	常時：非接触カード＋生体認証	関係者のみ	アンチパスバック機能 2人認証機能

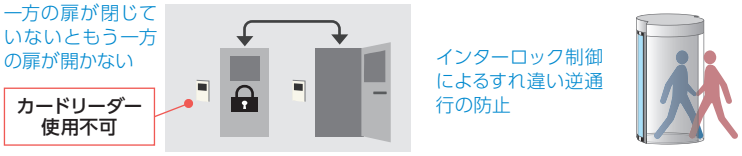
④ 運用開始と評価・是正

運用が始まると、日々の登録／削除作業や定期的な履歴の確認作業などが必要となります。また、常に機器が正常に動く状態とするための定期メンテナンスに加え、運用やルールの見直しも定期的に行う必要があります。

作業項目	発生頻度	内　　容
利用者登録/削除	都　度	人事異動や入社／退社に伴い都度作業
トラブル対応	都　度	緊急対応やルール違反者への警告
メンテナンス	定期的	機器の正常稼働確認
運用・ルールの是正	定期的	組織変更やレイアウト変更に伴う部屋の重要度の変更 人事異動等に伴う通行権限の見直し 法改正や犯罪傾向の変化による見直し

セキュリティ機能

分　　類	戸建住宅	共同住宅	オフィス	工場	保育園・幼稚園
状態監視機能 認証端末や扉の状態をパソコン画面に表示した平面図上のシンボルや一覧表で確認することができます。  警備員	ー	△	○	○	○
警報機能 扉の状態異常（開超過／異常開／故障）、システム状態異常（通信異常、機器故障）、非接触カード認証NG（不正カード）などの発生時はパソコンに警報を出力することができます。	ー	△	○	○	○
履歴管理機能 誰がいつ、どこで、どのような操作を行ったなどの入退室記録を残します。また、施解錠、扉の開閉、異常の有無も記録可能です。  システム管理者	ー	○	○	○	○
遠隔解錠機能 パソコンから指定した扉を一時解錠したり、連続解錠することができます。 	△	○	○	○	○
警戒（警備）セット/解除機能 認証端末の操作やパソコンからの操作で警戒(警備)を開始/解除することができる機能です。出入管理システムと警備機器を連動して働かせることもできます。  警備員	ー	○	○	○	○
通行権限設定機能 個人ごとに入室可能なエリアの通行権限を付与することができます。また、通行可能時間帯を設定することもできます。	ー	○	○	○	○
期限管理機能 個別に通行権限の有効期限を設定することができます。通行権限の削除漏れを防止することもできます。	△	○	○	○	○
映像連携機能 防犯カメラシステムとの連携により、履歴一覧から履歴発生前後の現場の映像を確認することが可能です。また、ライブ映像表示も可能です。	△	○	○	○	○
火災時出力連動機能 火災信号（接点信号）の状態を監視し、火災発生時に事前に設定された扉を強制解錠して速やかに避難経路を確保できます。	ー	○	○	○	△
設備間連携機能 空調設備や照明設備、エレベーターなどと連携することができます。警戒セット時に設備を自動停止して切り忘れを防止したり、該当階をエレベーターの不停止階に設定することができます。 また運用時間をスケジュールに設定して運用することもできます。	ー	△	○	○	ー

分　　類	戸建住宅	共同住宅	オフィス	工場	保育園・幼稚園
アンチパスバック機能 共連れやすれ違いによる不正入退室を抑制する機能です。認証操作なしで入室(退室)すると次に退室(入室)ができなくなります。 	―	―	○	○	―
共連れ防止機能 ゲートを用いた方法とアラームによる方法があります。 ＜ゲートによる共連れ防止＞ 不正侵入が行われるとゲートをロックし、共連れ通行を防止します。 ＜アラームによる共連れ抑止＞ 共連れ検出センサーにより、不正入室者を検出するとアラームを出し共連れ通行を抑止します。 	―	―	△	○	―
2人認証機能 2人が続けて認証して初めて入退室できる機能です。入退室操作を1人で行わないことで、内部犯罪などの抑止効果が期待できます。 	―	―	△	○	△
インターロック機能 通行部の入室側と退室側に別々の扉を設置し、一方の扉が開いている間は、他方の扉は開けることができないようカードリーダーの使用可・不可を扉の開閉に合わせて制御する機能です。不正入退室を防ぎます。 	―	―	△	○	―
出退勤管理機能 認証端末の入退室履歴を使用して、出退勤の時間を記録します。	―	―	○	○	△
在室者管理機能 各部屋の在室人数、在室者の一覧を表示する機能です。 部屋の滞在時間を設定することで、一定時間経過後に警報通知することもできます。	―	―	○	○	△

凡例　○：必要　△：必要に応じて使用　―：不要

システム事例（戸建住宅）

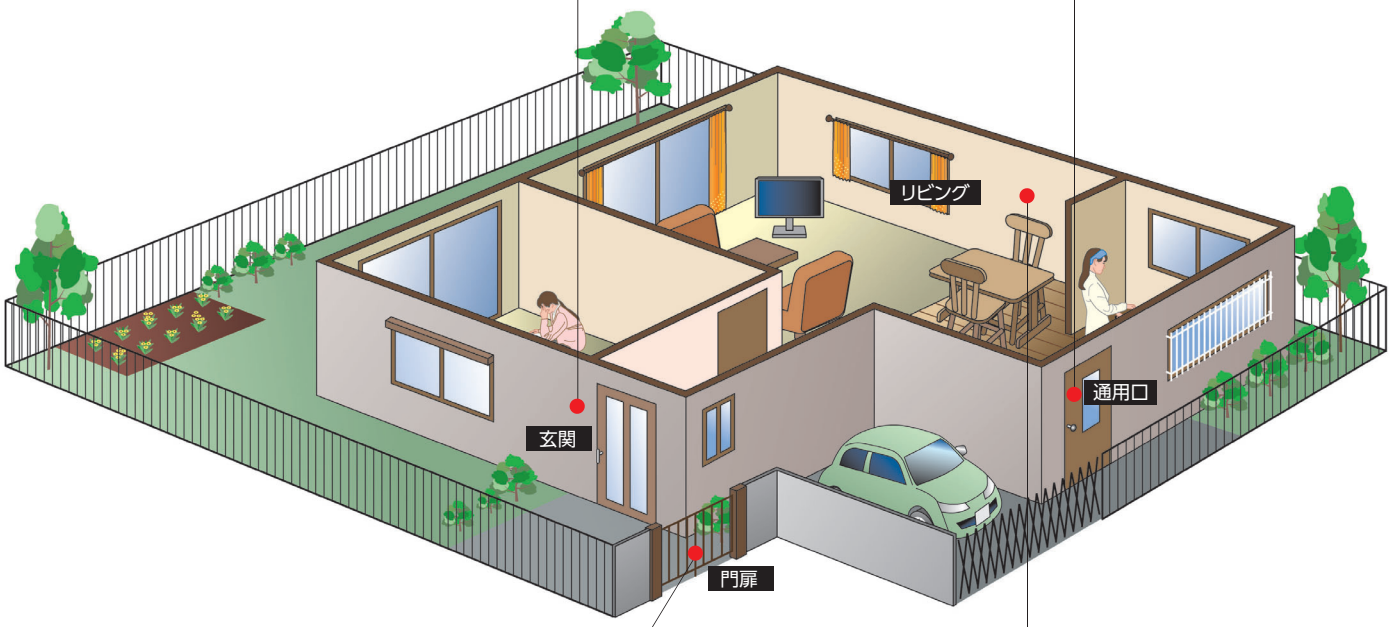
門扉にテンキーと電気錠（電磁錠）を設置し、通行制限することで敷地内への不用な侵入を防ぎます。
また、室内の制御盤により電磁錠の遠隔操作・監視が可能です。
建物の玄関及び通用口は非接触カードで出入りできるので利便性が向上します。
カード紛失時には、紛失したカードの情報を抹消するだけで良く、鍵紛失時のようにシリンダー交換などの工事は不要です。

非接触リーダー／電気錠

カードをリーダー部に近づけるだけで電気錠が施解錠します。カード紛失時の登録抹消も容易です。

非接触リーダー／電気錠（電動サムターン）

カードをリーダー部に近づけるだけで電気錠が施解錠します。カード紛失時の登録抹消も容易です。



テンキー（操作部）

暗証番号を入力することで電磁錠が解錠します。

電磁錠

扉をオートロック化し、第3者の不要な出入りを制限します。インターホンやテンキーなどと連携して開け閉めすることも可能です。

テンキー（制御部）

暗証番号の設定などを行います。

電気錠制御盤

室内から電磁錠の施解錠をすることができます。

システム事例（共同住宅）

共用エントランスに非接触リーダーによるオートロックシステムを導入することで、
利便性、保守性がよくなると同時に不法侵入を防止できます。
また、エレベーターも非接触リーダーで運用することで、建物内の防犯性をより向上させることができます。

電気錠

オートロックにより不法侵入を防止します。

非接触リーダー

タグをリーダー部に近づけるだけでオートロックが解錠します。

非接触リーダー/電気錠

タグを外側グリップのボタン部にかざして施解錠します。

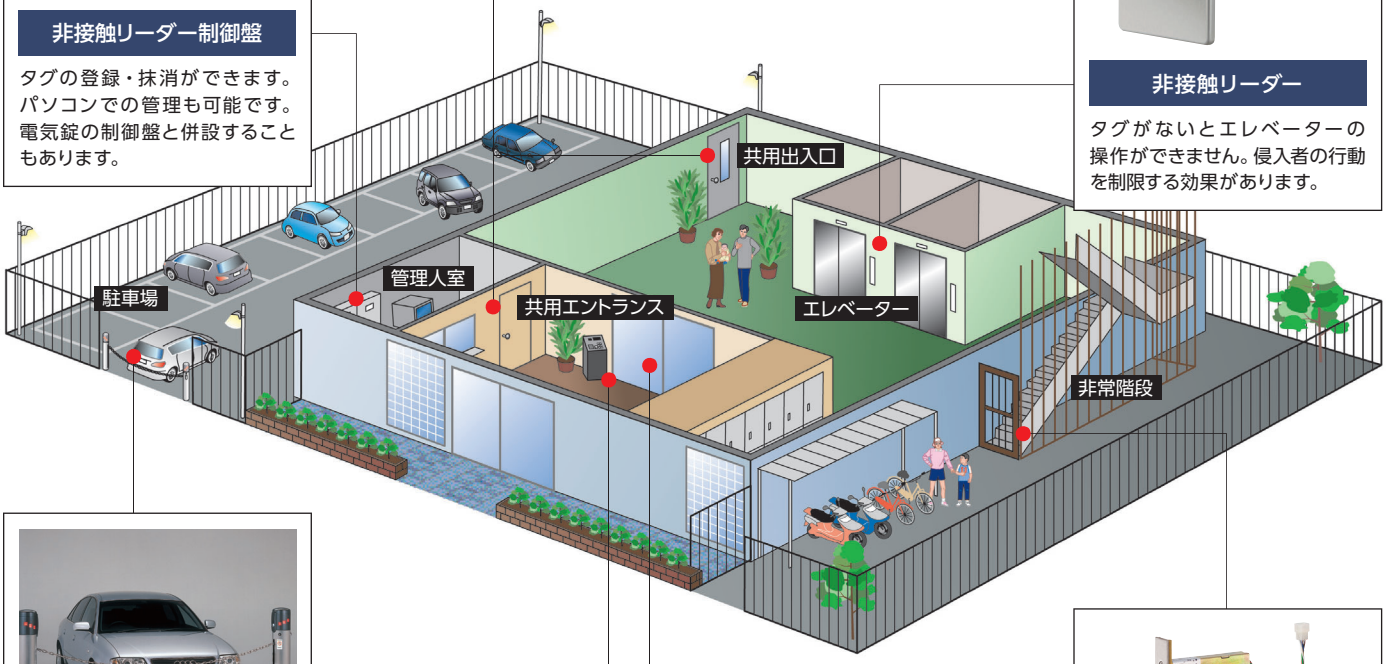
非接触リーダー制御盤

タグの登録・抹消ができます。
パソコンでの管理も可能です。
電気錠の制御盤と併設することもあります。

各住戸の玄関

非接触リーダー

タグがないとエレベーターの操作ができません。侵入者の行動を制限する効果があります。



電動チェーンゲート

不法駐車や不法侵入を防止します。

自動ドア

オートロックにより不法侵入を防止します。

非接触リーダー

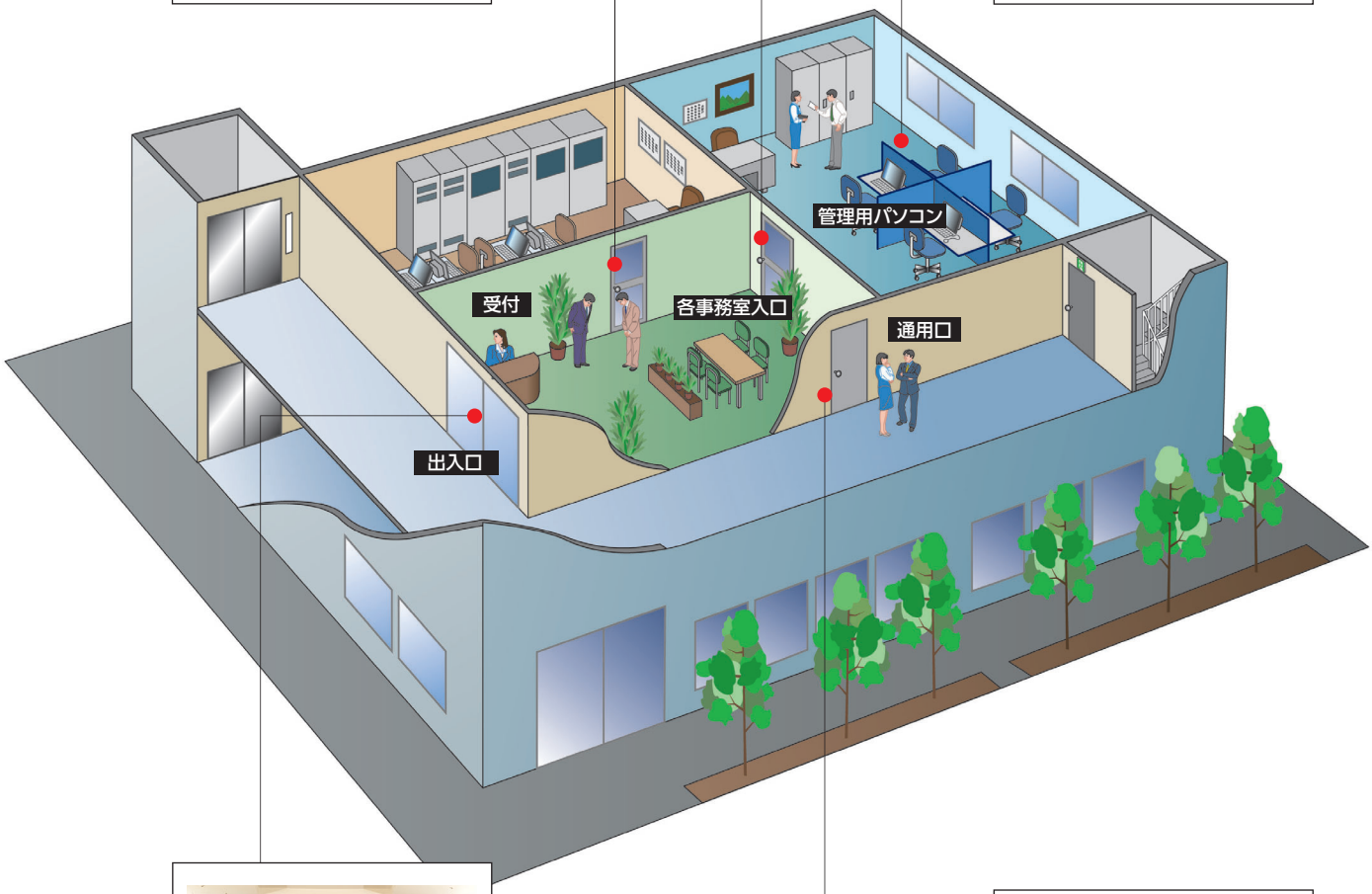
タグをリーダー部に近づけるだけでオートロックが解錠します。

電気錠

常時施錠していますが、非常時には解錠状態になります。管理人室で扉の状態を管理することもできます。

システム事例（オフィス 中・小規模）

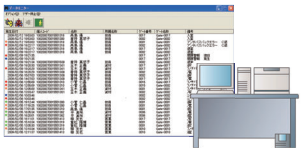
賃貸オフィスビルなど、1フロア（またはその一部）の比較的少ない出入口を管理する事例です。
各出入口には非接触リーダーが併設されており、入室権限のあるカードを持った人だけが入室できます。
管理用パソコンでカードの登録、抹消、各種設定、履歴の確認ができます。



電気錠/非接触リーダー

入室権限のあるカードを持った人だけが入室できます。

履歴画面



制御器/管理用パソコン

管理用パソコンでカードの登録、抹消、各種設定、履歴の確認ができます。

自動ドア

営業時間内は自由に通行できます。タイマー制御で通行できる時間帯を設定できます。

電気錠/非接触リーダー

入室権限のあるカードを持った人だけが入室できます。

システム事例（オフィス 大規模）

自社ビルやテナントビルなど、多くの出入口を管理する事例です。
受付の場所にはゲートを設置し、事務エリア及び事務室には、入室権限のあるカードを持った人だけが入室できます。
特に重要な部屋では生体認証を行い、入室権限のある本人しか入室できません。防災センターでは、各種設定、履歴の確認以外に扉の状態確認も可能です。外部の人間だけでなく、内部の人間に対する管理も行うことで、より防犯性が向上します。

電気錠/非接触リーダー

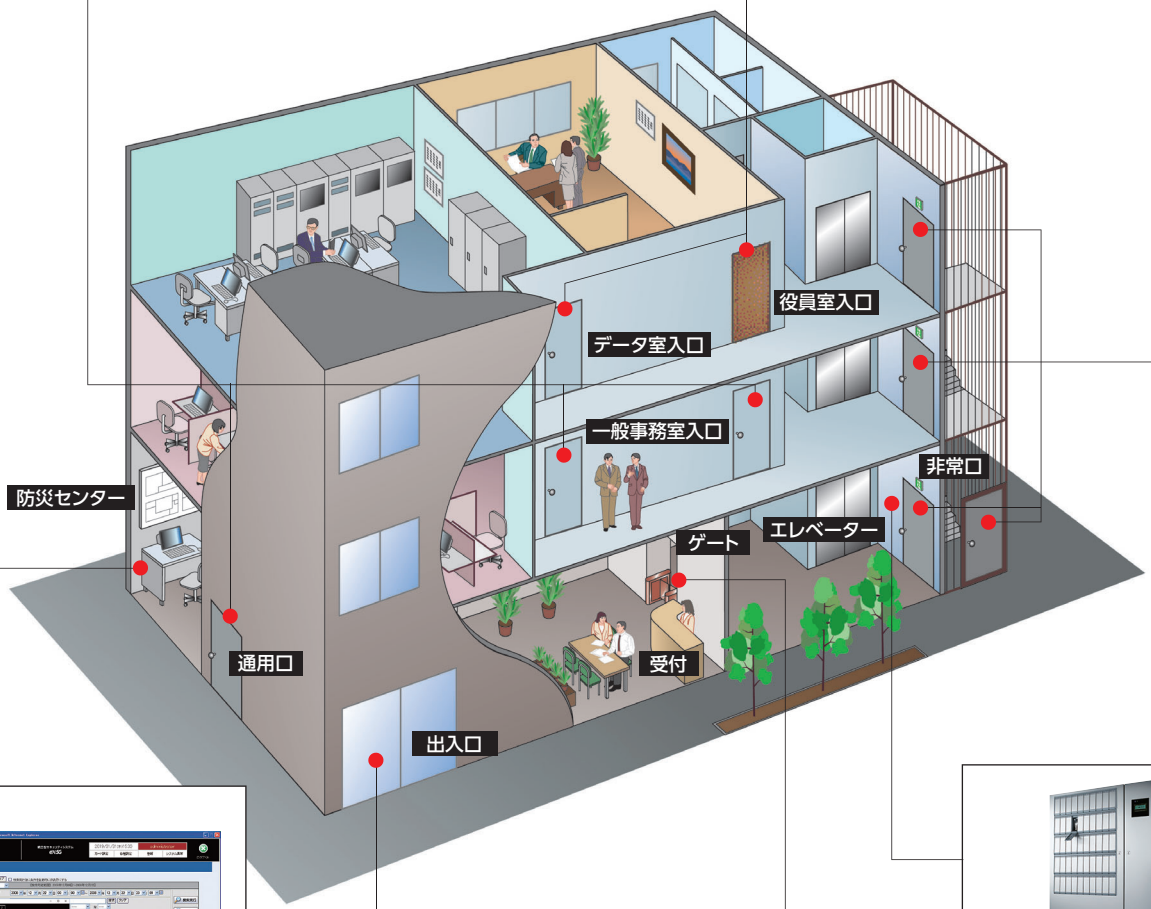
入室権限のあるカードを持った人だけが入室できます。

電気錠/生体認証リーダー

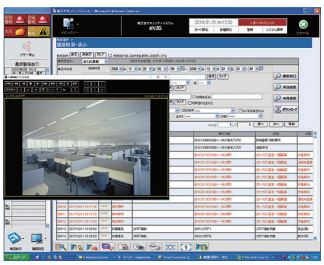
特に重要な部屋には生体認証により入室を制限します。入室権限のある本人しか入室できません。

電気錠

常時施錠していますが、非常時には解錠状態になります。防災センターで扉の状態を監視します。



履歴画面



制御器/管理用パソコン

建物内の扉の状態を監視します。
また、管理用パソコンでカードの登録、抹消、各種設定、履歴の確認ができます。

自動ドア

タイマー制御で通行できる時間帯を設定できます。

ゲート/非接触リーダー

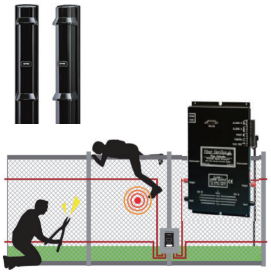
事務エリアに入るためには、入室権限のあるカードをリーダーにかざして、ゲートを通過します。

キーボックス

テナントや店舗への鍵の貸し借りを無人で行い、貸し借りに関わる管理業務を省力化します。利用者履歴の検索をしたり、鍵の貸し借り状態に応じて居室の警戒セット／解除機能が連携します。

システム事例（工場）

工場敷地全体の監視と出入口を管理する事例です。
敷地外周・重要エリアには防犯カメラ、センサーを設置し、侵入を監視、敷地への出入管理は守衛所前にゲートを設置し、共連れを防止、車両の敷地への出入り、各棟及び各棟内の出入りは、権限のあるカードを持った人だけが入場・入室可能とします。
特に重要な部屋（サーバールームなど）では生体認証を行い、権限のある本人しか入室できません。管理室では、各種設定、履歴の確認以外に扉の状態確認も可能です。外部の人間だけでなく、内部の人間に対する管理も行うことで、より防犯性が向上します。



外周警戒センサー

敷地外周はフェンスセンサーや赤外線センサーにより不審者の侵入を監視します。

電気錠/非接触リーダー

入室権限のある非接触カードを持った人だけが入室できます。

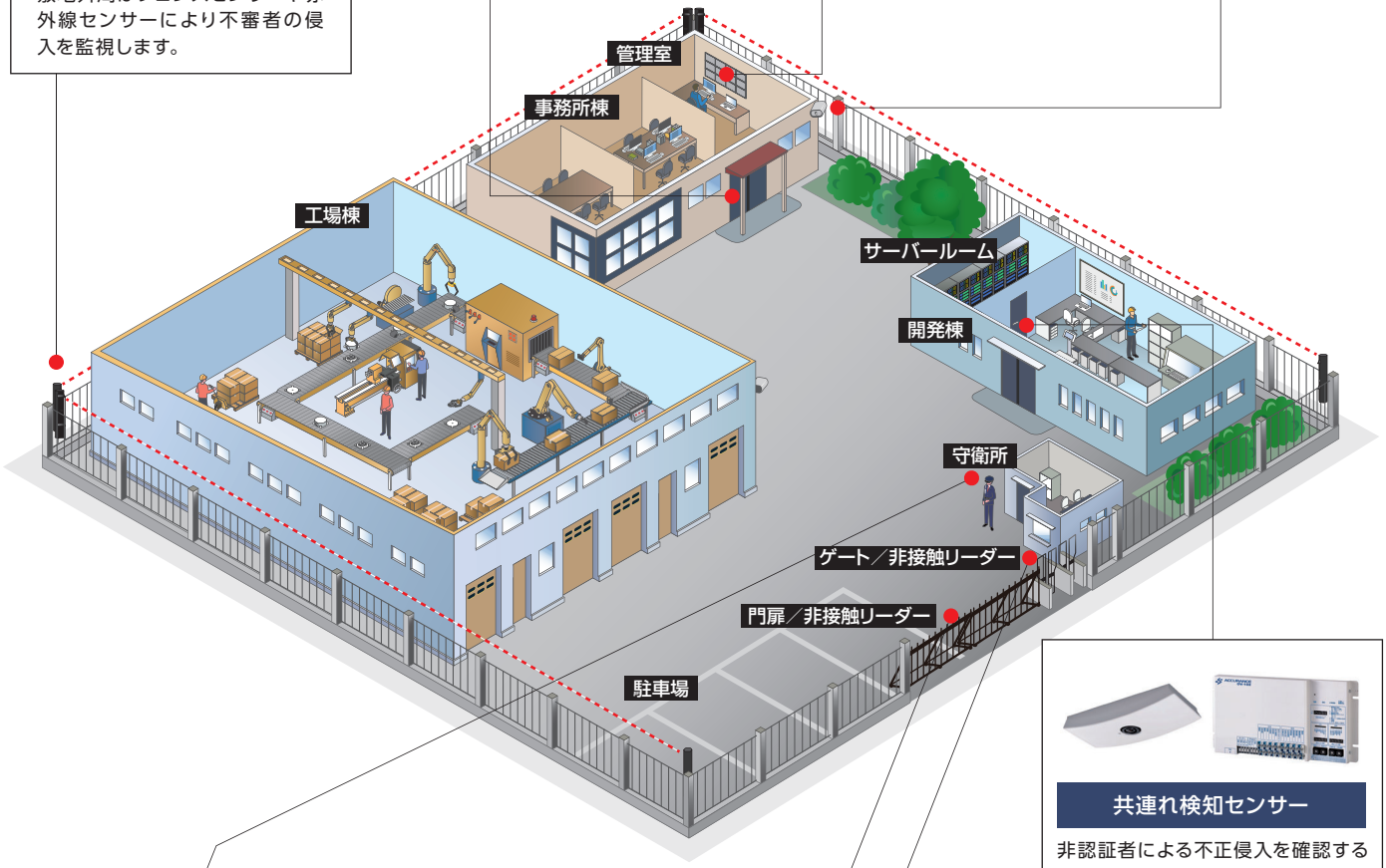
履歴画面

制御器/管理用パソコン

建屋の扉の状態を監視します。また、管理用パソコンでカード、タグの登録、抹消、各種設定、履歴の確認ができます。

防犯カメラ

場所、目的に応じたカメラを設置し、映像を記録します。出入口付近に設置することで、侵入者の立ち入りを抑止します。



共連れ検知センサー

非認証者による不正侵入を確認することで、共連れ通行を抑止します。

出入管理業務

人、物、車両等の出入りをチェックすることによって犯罪・事故等を防止します。

門扉／非接触リーダー

工場への出入りを管理します。カードやタグなどによる認証方法があります。

ゲート／非接触リーダー

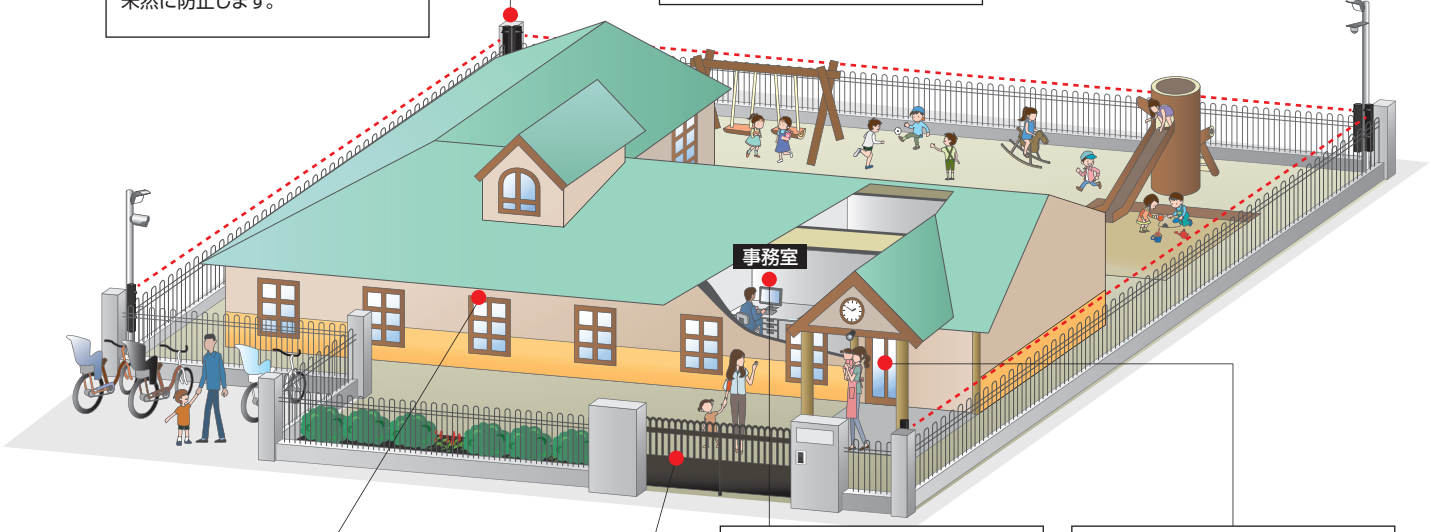
工場敷地への通路は、ゲートによって管理され、共連れを防ぎます。

電気錠/生体認証リーダー

特に重要な部屋には生体認証により入室を制限します。入室権限のある本人しか入室できません。

システム事例（保育園・幼稚園）

保育園・幼稚園の外周や出入口を管理する事例です。
外周には、センサーと防犯カメラを設置、映像を職員室のモニターに映し、事前に訪問者を確認します。
非常通報を利用すれば、警備会社が現地にかけつけます。門扉や玄関は、インターホンで訪問者を確認し、職員室から遠隔で解錠します。園児が知らぬ間に園外に出て行くことも防止できます。非接触リーダーなど照合端末を設置することで、保護者のお迎えに利用することもできます。



屋外警戒センサー

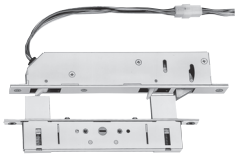
外壁やフェンスといった建物の外周を警戒し、建物に侵入される前に未然に防止します。

録画監視システム

防犯カメラと接続し、リアルタイムでの監視や映像の録画を行います。園内の状況の確認などにも使用できます。

防犯カメラ

園内の状況確認などに使用できます。



採風錠

窓の開放量を一定に制限し、窓から園児が外に出たり、転落したりするのを防止します。制御器からの操作で窓を全開にすることも可能です。

電磁錠

門扉をオートロック化し、第3者の不要な出入りを制限します。インターホンやカードリーダーなどと連携して開け閉めすることも可能です。

非常押ボタン

非常時にボタンを押し込み異常を知らせます。

電気錠

扉をオートロック化し、第3者の不要な出入りを制限します。インターホンやカードリーダーなどと連携して開け閉めすることも可能です。

非常通報装置

各種センサー、警報器を接続し通信回線を使用して異常を監視センターへ通報します。

かけつけサービス

非常通報を受け、現場へ急行かけつけ事案に対応します。

RBSS認定品を用いたシステムの導入にあたっては防犯設備士の活用を！

RBSS（優良防犯機器認定制度）は防犯カメラなどの機器単体を認定する制度であり、防犯システムを導入する際には、RBSSをよく理解した防犯設備の専門家に相談することをおすすめします。
当協会は、平成４年より防犯設備の専門家の育成に取り組んでおり、資格認定試験で一定の知識・技能を備えた者を「防犯設備士」として認定しています。
認定試験は年4回実施しています。詳細は当協会のホームページをご覧ください。

「 防犯設備士 」＝「 防犯のプロフェッショナル 」

当協会は、RBSSによる「優良な機器」と防犯設備士による「優良な設計・施工・維持管理」により、「優良な防犯システム」の普及を促進しています。

防犯設備士の地域活動拠点

公益社団法人日本防犯設備協会（★）は、各地域協会とコミュニケーションを図りながら、防犯活動を展開しています。
また、地域に根ざした更なる防犯活動を目指し、全国にネットワークの輪を広げていきます。
なお、地域活動拠点の最新情報は当協会ホームページをご覧いただくと共に、防犯設備、防犯診断、防犯講演等のご相談は当協会及び各地域協会までお問い合わせください。

2022年１月現在

北海道	❶ 北海道防犯設備士協会	長野県	⓯ 長野県防犯設備協会	岡山県	㉚ 岡山県防犯設備業防犯協力会
青森県	❷ 青森県防犯設備協会	静岡県	⓰ 静岡県防犯設備士生活安全協議会	広島県	㉛ NPO法人 広島県生活安全防犯協会
岩手県	❸ 岩手県防犯設備協会	富山県	⓱ 富山県防犯設備協会	山口県	㉜ 一般社団法人 山口県防犯設備士協会
秋田県	❹ 秋田県防犯設備協会	石川県	⓲ 石川県防犯設備促進協力会	徳島県	㉝ 一般社団法人 徳島県防犯設備協会
宮城県	❺ 宮城県防犯設備士協会	福井県	⓳ NPO法人 福井県防犯設備協会	香川県	㉞ 香川県防犯設備業防犯協力会
山形県	❻ 山形県防犯設備協会	岐阜県	⓴ 岐阜県防犯設備協会	愛媛県	—
新潟県	—	愛知県	㉑ 愛知県セルフガード協会	高知県	㉟ NPO法人 高知県防犯設備協会
福島県	❼ 福島県防犯設備協会	三重県	㉒ NPO法人 三重県防犯設備協会	福岡県	㊱ NPO法人 福岡県防犯設備士協会
栃木県	❽ 栃木県防犯設備協会	滋賀県	㉓ 滋賀県防犯設備士協会	佐賀県	—
茨城県	—	京都府	㉔ 一般社団法人 京都府防犯設備協会	長崎県	㊲ 長崎県防犯設備協会
群馬県	❾ 一般社団法人 群馬県防犯設備協会	奈良県	㉕ NPO法人 奈良県防犯設備士協会	熊本県	㊳ 一般社団法人 熊本県防犯設備協会
埼玉県	❿ 一般社団法人 埼玉県防犯設備協会	和歌山県	㉖ 和歌山県防犯設備協会	大分県	㊴ 大分県防犯設備士協会
千葉県	⓫ 一般社団法人 千葉県防犯設備協会	大阪府	㉗ NPO法人 大阪府防犯設備協会	宮崎県	㊵ NPO法人 宮崎県防犯設備士協会
東京都	⓬ NPO法人 東京都セキュリティ促進協力会	兵庫県	㉘ NPO法人 兵庫県防犯設備協会	鹿児島県	㊶ 鹿児島県防犯設備協会
神奈川県	⓭ NPO法人 神奈川県防犯セキュリティ協会	鳥取県	—	沖縄県	㊷ 沖縄県防犯設備協会
山梨県	⓮ NPO法人 山梨県防犯設備士協会	島根県	㉙ 島根県防犯設備協会		

●各地域協会への連絡先は、当協会のホームページを参照してください。 https://www.ssaj.or.jp/chiiki/index.html

編集協力会社（順不同）　株式会社アート、ＮＥＣプラットフォームズ株式会社、オプテックス株式会社
株式会社クマヒラ、株式会社ゴール、株式会社セノン、パナソニック株式会社
株式会社日立産業制御ソリューションズ、三菱電機株式会社、美和ロック株式会社

編集・発行

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
https://www.ssaj.or.jp/

2022年３月発行