入退室監理システム提案

2016年3月22日
株式会社アイデンティックサービス

Copyright©2016 Identicservice Co.Ltd all rights reserved

セキュリティレベル毎の対策要点と施策例

セキュリティレベル	レベルの性格	企業における区域例	主要対策要点と施策例
レベル１	外周部に当たり公共スペースから対象区域への境界部。不審者・不審物の進入及び犯罪防止を目的とする	ビル、工場の外周区域、公道との境、フェンス、壁の内側	侵入抑制と監視。人的警備、フェンス、障壁、センサ（衝撃・赤外線）、監視カメラ。プライバシー侵害対策が要注意
レベル２	対象敷地内で且つ一般来訪者が使用するという意味での公共性を有する区域。不審者・不審物の侵入、犯罪に加え防火・防災要件を有する区域	ビル敷地内屋外、工場フェンスの内側、エントランス、ロビー等	機械警備による時間外入館制限、人的警備、監視カメラ、センサ（人感、窓、火災、煙等）。キーボックス
レベル３	対象区域内の居住者・正規来訪者が使用する施設を含む区域	エレベータ、廊下、給湯室、トイレ、制限の無い応接室、ミーティングルーム、テナントエントランス等	機械警備による時間外入館制限、人的警備、監視カメラ、センサ（同上）、禁煙センサ、盗撮・盗聴対策等。監視カメラのプライバシー侵害要注意
レベル４	対象区域において許可された者のみに制限された区域	制限区域のエレベータ、廊下、事務室、会議室等、配送センター	入退室管理、人的管理、セキュリティゲート、監視カメラ、センサ類、持ち込み・持ち出し検査等
レベル５	対象区域における最重要セキュリティゾーン。企業・組織の利益に直接関係する最重要対象が存在する区域。必要に応じてレベル６区域の設置。	サーバルーム、その他個人情報保護区域（宅配便伝票保管区域等）、役員室、毒劇等危険物保管場所、研究所、多額な金品保管場所、金庫	入退室管理、特に金融データ保管室の二人認証、共連れ防止（ゲート、ＡＰＢ）、映像監視、インターロック、持ち出し制限、人的警備

Copyright©2016 Identicservice Co.Ltd all rights reserved

レベル毎のセキュリティ対策要点と対策　レベル1-3

特徴

✓可用性とプライバシーを重視した対策

公共スペースと隣接する地域ですので、多くの利用者がストレス無く使用することを考慮する必要があります。又　、昨今欧米では監視カメラの撮影規制を行う等プラバシー侵害に対する考慮が必要になってきています。

✓時間帯でのセキュリティ性強弱

公共スペースとの最大の区別は時間帯による可用性です。ウィークデイのデイタイムは公共性を考慮にする必要がありますが、休日・土日・夜間の進入制限および張り紙、人的警戒により不要な侵入者の侵入・施設利用を制限する必要があります。又、昨今はトイレ等の盗聴・盗撮対策も視野に入れる必要があります。

✓気象条件、景観を考慮

区域の外部に当たる同ゾーンは、外的な気温・気象による影響もさることながら、区域の顔である為の景観との調和性を考慮に入れる必要があります。反対に、抑止を目的として掲示・ダミーカメラ等セキュリティ対策をアピールする場合もありますので、区域の目的を考慮の上対策を講じる必要があります。

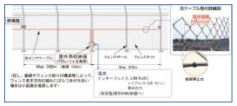
対策

映像監視

◆不審者・不審物監視
◆クレーマー対策
◆事故監視（車両、来訪者）
◆防水・暗視対策
✓公道等公共スペースの監視
録画にはプライバシー配慮必要

フェンスセンサ・赤外線センサ

◆敷地内へ不審者・不審物侵入検知
◆不審者侵入抑止
◆外周監視カメラとの連携



機械警備・人的警備

◆館内への不審者侵入抑止・検知
◆巡回、検問、持ち物検査
◆緊急時の駆けつけ
◆防災システムとの連携

ゲート（車両・人）

◆不振車両進入制限
◆車両出入り確認
◆入館権限チェック
◆共連れ防止
◆在館（滞留）時間チェック

キーボックス

◆鍵管理
◆警備セット・解除

喫煙検知器

◆禁煙地区での喫煙防止

入館管理

◆不審者の館内侵入防止
◆災害時の在監者把握
◆空調との連動による省エネ
◆入退室管理との連動

エレベータ不停止

◆不審者・不審物の真勇防止
◆不要な立ち入り防止

Copyright©2016 Identicservice Co.Ltd all rights reserved

レベル毎のセキュリティ対策要点と対策　レベル4

特徴

✓昼夜を問わぬ進入制限（入退室管理）

この区域はもはや公共性を考慮する必要はありません。企業・組織の内部の専有区域であり、その中にある人的・物的無形資産に対する外部からの脅威を排除するのが第一の目的になります。但し、日常の業務に支障を来さない可用性の考慮と進入制限が要点です。

✓入室（入館）権限の管理

企業・組織の正規構成要員の他に、外注・派遣等期間的な要員及び不定期来訪者・ビル管理保守要員・警備会社職員等利益に合致した入室（入館者）の進入を許可し、それ以外の侵入を制限する必要があります。この観点から、認証権限認証手段、解錠手段等実態に合わせた組合せとその管理を検討する必要があります。

✓入室（入館）状況の記録・保管と利用

この区域への出入の記録は必要に応じて、顧客・監査要員・警察等の所轄官庁への提出を求められる場合があります。又、正確な入室管理を行う為にも、その記録（入退室ログ、監視映像）は確実に、必要とされる期間保管し、必要な場合に利用できる手段を講じる必要があります。

対策

自動施錠

◆不審者・不審物の入室制限
◆入退室管理の徹底
✓時間帯での施錠・解錠


入退室管理

◆区域内への不審者・不審物の侵入制限
◆権限による入室の制限
◆時間帯による進入制限
◆照明・エアコンとの連動

映像監視

◆うろつき防止
◆共連れ防止
◆不正作業防止・監視
◆作業状況確認
◆コミュニケーション

ロッカー

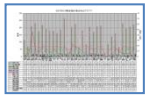
◆ＰＣ、ＵＳＧ、携帯
カメラの持ち込み防止


持ち物検査

◆不正持ち込み防止
◆不正持ちだし防止

履歴・在室・行動分析

◆入退室履歴
◆在室管理
◆行動分析管理
◆入館記録者のみ
入退室許可




エアコン・照明コントロール

◆入館・退館時の照明点灯
◆在室者数に応じてのエアコン管理

出退勤管理

◆出退勤管理
◆入館・退館履歴
◆在館時間管理

Copyright©2016 Identicservice Co.Ltd all rights reserved

レベル毎のセキュリティ対策要点と対策　レベル5

特徴

✓企業・組織の死命を決する重要な人・物・金・情報の保管場所

経営陣居室、製品開発室、個人情報管理室、金庫室、サーバルーム等その企業の重要区域のセキュリティにおいてはもはや可用性を考慮する必要はありません。厳格な侵入制限とその記録が要求されます。又、広義のセキュリティ対策として無停電、サージ電圧対策等も視野に入れる必要があります。

✓厳格な入退室管理

機械的な入退室管理における不完全性が正規入室者との同伴（意図すると意図せざるとにかかわらず）者の入室といわれます。いわゆる共連れです。共連れはその直接的な危険性もさることながら、共連れが横行することによりセキュリティ意識が薄れる“ブロークンウィンドウ”問題が深刻です。出・入管理、アンチパスバック、インターロックが対策です。

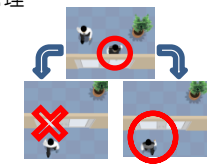
✓合わせ技によるセキュリティ強化

認証技術同様に、セキュリティ施策は複合化することにより強化が可能で且つ可用性の維持も図ることができます。映像と入退室の統合、在室カウンター入退室の統合等の複合ソリューションが効果的です。

対策

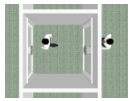
アンチパスバック

◆厳格な入退室管理
◆共連れ防止



インターロック

◆共連れ防止
◆不正侵入禁止



在室カウンター

◆共連れ防止

持ち出し・持ち込み管理

◆ＰＣ、ＵＳＧ、携帯
カメラの持ち込み防止

複合認証

◆厳格な入退室管理
◆生体認証の正確さとカードの便利さ

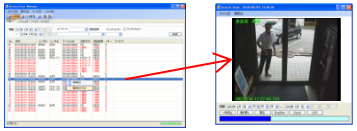
非接触IC
カード

アラーム

◆不正入室・不正行動への警告

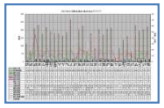
映像・入退室統合管理

◆入退室履歴による映像検索



履歴・在室・行動分析

◆入退室履歴
◆在室管理
◆行動分析管理
◆入館履歴者のみ
入室許可



Copyright©2016 Identicservice Co.Ltd all rights reserved

レベル毎のセキュリティ対策要点と対策　レベル6

特徴

✓社会の安全を資する究極のセキュリティ

一企業・組織だけではなく社会の経済基盤、生活基盤に甚大な影響を与える可能性がある人・物・金・情報を保管管理するこの区域ではもはや通常のセキュリティ対策にとどまらず、完全を目指した対策が必要になります。

✓人に対する対策以外に外部からの影響への対策

内部に侵入する不審者への対策にとどまらず、電磁波、停電、破壊、地域災害など外部からの影響への対策も広義のセキュリティ対策として講じる必要があります。

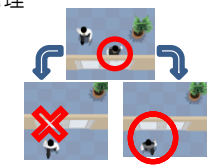
✓最重要区域で要求される二人認証

入退室管理、権限管理の最後の盲点がシステム管理者による不正です。これに対する対策はもはや人が人を監視する二人認証が必要になります

対策

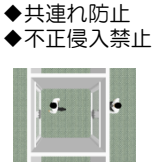
アンチパスバック

◆厳格な入退室管理
◆共連れ防止



インターロック

◆共連れ防止
◆不正侵入禁止



在室カウンター

◆共連れ防止

持ち出し・持ち込み管理

◆ＰＣ、ＵＳＧ、携帯
カメラの持ち込み防止

二人認証

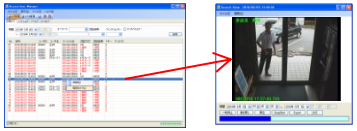
◆管理者とオペレータ二人認証時のみ
入室許可

アラーム

◆不正入室・不正行動への警告

映像・入退室統合管理

◆入退室履歴による映像検索



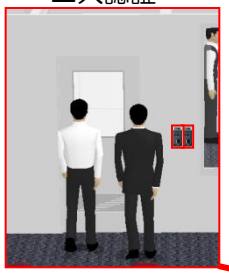
耐震・防磁サーバラック

◆地震対策
◆電磁波対策

Copyright©2016 Identicservice Co.Ltd all rights reserved

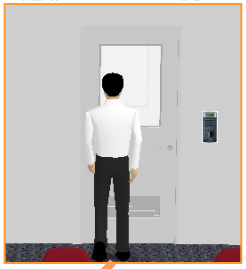
セキュリティ区分に応じた総合入退室施策例

顧客情報サーバ室
二人認証

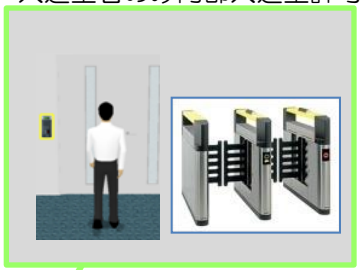


サーバ前室
インターロック

サーバ室
指紋＆カード認証

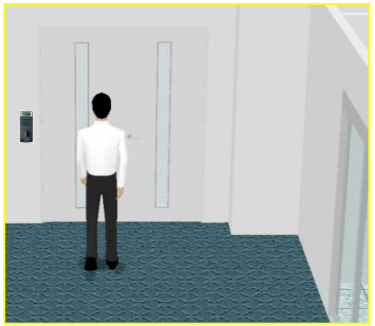


トレース機能
入館・入退室者のみ内部入退室許可

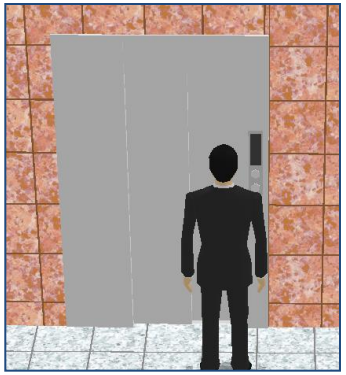


メインエントランス
時間外は入退室管理最終退館後は機械警備

執務スペース入り口
カード認証（もしくは生体認証）



エレベータ不停止



Copyright©2016 Identicservice Co.Ltd all rights reserved

入退室認証技術のチェックポイント

実用性・信頼性
ビジネスシーンで使用される製品に求められる最も重要なチェックポイントです。認証技術の場合は、それが科学的に十分な検証がなされているか、実運用の実績があるかそしてその技術を有して世に出している企業に信頼性があるか等が評価基準になります。

機密性
認証技術は事前に登録された情報と認証時にユーザが使用する媒体の情報とを技術的に比較を行い一致又は相当以上の近似性を確認する技術です。ですから、登録情報に非可逆性、転用制限がセキュリティ上重要です。機密性はそのようなリスクに対する対策が問われるチェックポイントです。

認証性・本人確認性
上記の通り、本人認証には本人を認証する本人認証性と他人を受け入れない排他性が問われます。生体認証技術においては本人排斥率（ＦＲＲ）、他人受容率（ＦＡＲ）という指標で判断されます。カード認証の場合には基本的には一意性（ユニーク性）がその指標として問われます。

容易さ
これは大きく分けて、　登録の容易さと使用の容易さを指します。登録の容易さには、登録時のユーザ・管理者の手間がかからないということに加えて、一度登録したものを複数のリーダで使用できること及び、登録時のユーザの心因的な負担が少ないことがあげられます。使用の容易さはまさにシンプルに、スピーディに使用できることがポイントです。

社会的責任の重さ
認証技術は入退室のみに使用される物ではありません。最近では指静脈・掌静脈の銀行カード認証への使用。Felicaの電子マネーへの使用など非常に重要な場面での認証にも使用されます。それ故、そのようなセンシティブ情報の保管には最重要のセキュリティが求められる場合があり、コスト高・リスク高につながる可能性があります。

拡張製
拡張製に関しては、多くのリーダへの展開性という物理的な面（登録性に関連します）と、ＰＣセキュリティ等入退室以外に利用できる論理的な面がチェックポイントになります。

経済性
やはり御導入の検討に欠かせないファクタがこの経済性です。経済性の観点では、機器の初期導入コスト、認証メディアのコスト、保守性（堅牢性）に裏打ちされたメンテナンスコスト、そして拡張要求に容易に応えるカスタマイズ性等がチェックポイントになります。

Copyright©2016 Identicservice Co.Ltd all rights reserved

入退室認証技術の比較

		生体認証（Biometrics ）						トークン（Token）	
認証方法		指紋	静脈（指）	静脈（掌）	静脈（手の甲）	顔	虹彩	非接触カード	非接触タグ
技術的な側面	実用性・信頼性（利点問題点）	◎ 歴史・実績	◎ 実績	◎ 実績	△	◎ 実績	◎ 実績	◎ 技術	◎ 技術
	機密性	◎	◎	◎	◎	◎	◎	◎	◎
	他人非受入（問題点）	◎	◎	◎	○	◎	◎	× 盗難・貸与	× 盗難・貸与
	本人非拒否（問題点）	○ 乾燥・湿潤	○ 低血圧	○ 位置ずれ	○ 体毛	○ 照明	○ コンタクト	◎	◎
運用上・経済的な側面	登録の容易さ	◎	◎	△ 位置ずれ	○	◎	○	◎	◎
	使用の容易さ	◎	◎	△ 位置ずれ	◎	◎	△ 恐怖心	◎	◎
	社会的責任の重さ	軽い	重い 銀行カード	重い 銀行カード	軽い	軽い	軽い	重い 銀行カード	軽い
	拡張製	◎ 情報S	◎ 情報S	◎ 情報S	×	◎	×	◎ 情報S	△
	経済性（万円/ゲート）	◎ (40~70)	△ (80~120)	× (100~150)	○ (50~70)	○ (50~70)	△ (80~120)	◎ (40~70)	△ (80~120)
特記事項			銀行ＡＴＭでの使用故超センシティブ情報	銀行ＡＴＭでの使用故超センシティブ情報				Felicaは金融カードとして取り扱い	

＊上記の認証技術は技術面、運用・経済的な側面で実用レベルにある物のみ選択しております。

Copyright©2016 Identicservice Co.Ltd all rights reserved

企業向け入退室監理の要点

Copyright©2016 Identicservice Co.Ltd all rights reserved

入（退）室管理とは・・・・・・

入退室管理の目的	施策
不正侵入防止	自動施錠型ロックによる施錠 外部からの不正、不必要な侵入を防ぐ為、内部からの不正退出を防ぐ為に扉は自動的に施錠　（例）電気錠、ホテル錠、電気錠付き自動ドア、エレベータ不停止，警備員による侵入制止　等
正当な利用者の確認と通過許可	正当な利用者の認証 正当な利用者を確実に且つ円滑に通過させる為に正当であることの証明と確認（認証）が必要、認証時の解錠通過許可が行えること （例）カード、生体認証、警備員によるID確認
入室（退室）履歴の記録	入室（退室）者、時間、場所の記録 正当な入室（退室）者の入室場所、時間を記録し、閲覧検索が可能な形で保管し、その証跡記録の利用が許された者が必要な時に容易に利用できること。（例）ISMS、プライバシーマーク監査対応
組織的なセキュリティ施策の基礎	究極のセキュリティは構成要員の“目”と“声” “こんにちは”、“何かごようですか”、“どちらへ”・・不正、犯罪の抑止に最も有効なのは周りの“目”であり“声”です。安全意識の高い組織をつくることが入退室管理の究極目標

入退室管理は利用者の不便の代償として組織・構成要員の安全と安心を提供します。
そして、組織の安全を真剣に考える構成要員によるWin-Win関係を構築します。

Copyright©2016 Identicservice Co.Ltd all rights reserved

組織のセキュリティ管理：　出・入りの管理

出・入り管理の目的	その理由
共連れの防止	<u>共連れは不正のゆりかご</u> 正当な入室者の後を付いて入室する共連れ入室は、“私は入室権限があるからいいだろう“ではすまされません。“万里の長城も蟻の一穴から”の如く、組織のモラルが低下することが最大の脅威です。
在室者の管理	<u>業務上、緊急時の対応上在室者数管理が求められる場合</u> セキュリティ目的以外にも、労働安全管理上、生産性向上の目的等で労働区域への立ち理解数・滞在時間の記録とその利用は有用です。又、災害発生時に在室者を把握して避難指示に利用する等のニーズも増えています。
監査への対応	<u>セキュリティ認定監査が要求</u> ISMS、プライバシーマーク等のセキュリティ認定の中で特に個人情報等を集中的に扱う区域への入室・滞在時間等の詳細な記録を求められる場合が多く、又、監査による“出・入り”の管理を求められます。

外部からの侵入を物理的に守る入室管理から、組織を・情報を・信頼を守る
入退室管理（出・入り）への要求が増えてきています。

Copyright©2016 Identicservice Co.Ltd all rights reserved

参考情報　アンチパスバック

アンチパスバック機能とは・・・・・

入退室管理を厳格に行うために入室記録があった通過者のみ退室を可能にし、退室記録があった通過者のみ再入室を可能にする機能

又、アンチパスバックには

① グローバルアンチパスバック
セキュリティ区画の内・外を定義して外から内への入室と内から外への退室を必ず一対にして管理する方法
（欠点）　複数のセキュリティ区画が存在する場合、セキュリティ上の穴ができてしまう。

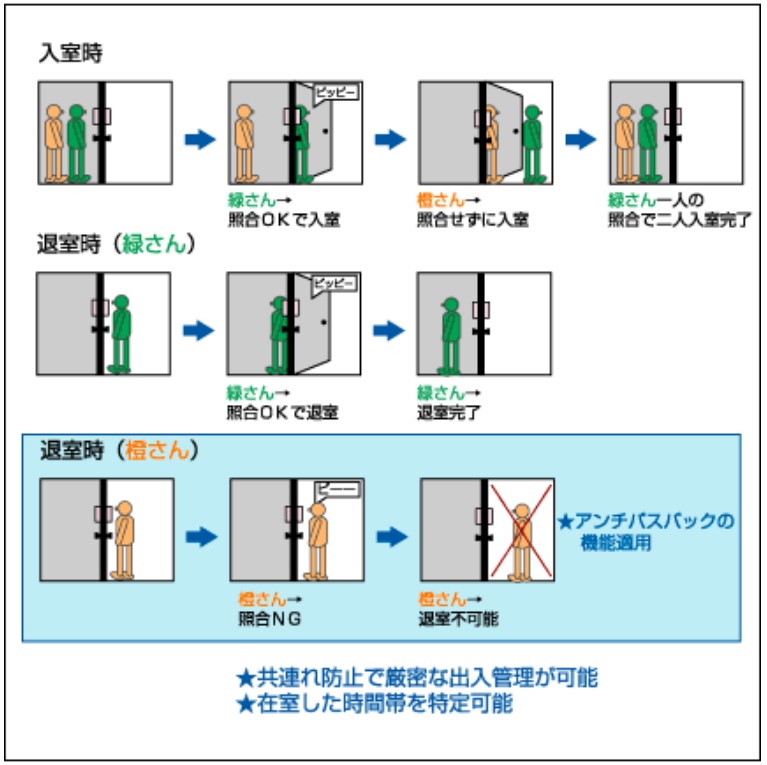
② ゾーンアンチパスバック
各区画をそれぞれ別個のセキュリティゾーンとして捉え、それぞれの内・外を定義することにより、各ゾーンへの入室・退室が一対であることを要求するより厳格な方式。

があります。

アンチパスバック機能により入室する制限としては

A　アンチパスバックエラーが発生したユーザは入室・退室が不可
この場合、意図的なエラーのみならず認証後入室（退室）を行わなかったことによる誤りもエラーとなります。

B　その為、最近ではアンチパスバックエラーとして履歴保存し通知若しくは映像記録するが、再入室制限は解除する（一定時間後）を要求する傾向があります。



Copyright©2016 Identicservice Co.Ltd all rights reserved

参考情報　インターロック

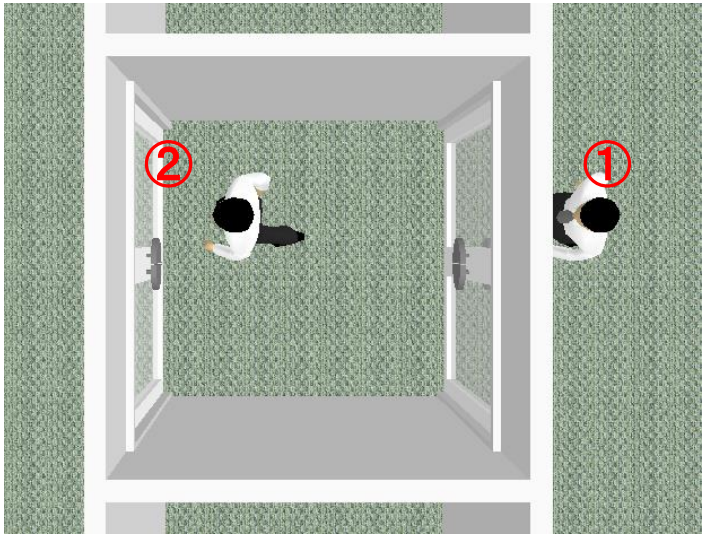
インターロック機能とは・・・・・

セキュリティ区域の入室箇所に前室を設置して区域外から前室への入室時（右図①）に前室からの区域内入室（右図②）をするユーザがいないか確認の上入室を許可する方法です。

通常は①の際に②が施錠されていることを確認して、施錠されていれば①の認証（解錠）を許可することで制限を加えていますが

より厳格に対処する為に、②の区画に人が居ないことを①の許可条件にする方法

さらに厳格に対処する為に、②の区画が1人であるかどうかを確認の上、②の認証を許可する機能を付け加える方法もあります。



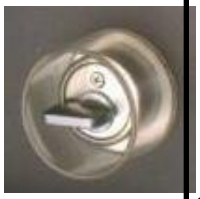
Copyright©2016 Identicservice Co.Ltd all rights reserved

入退室システム設置・運用イメージ

緊急時の入室用シリンダ

緊急時の外側からの入室には電気錠付属の鍵により入室が可能です。鍵はマスタプラン化することにより１つの鍵で複数（若しくは全て）の電気錠解錠が可能です。

緊急時の退室用サムターン。



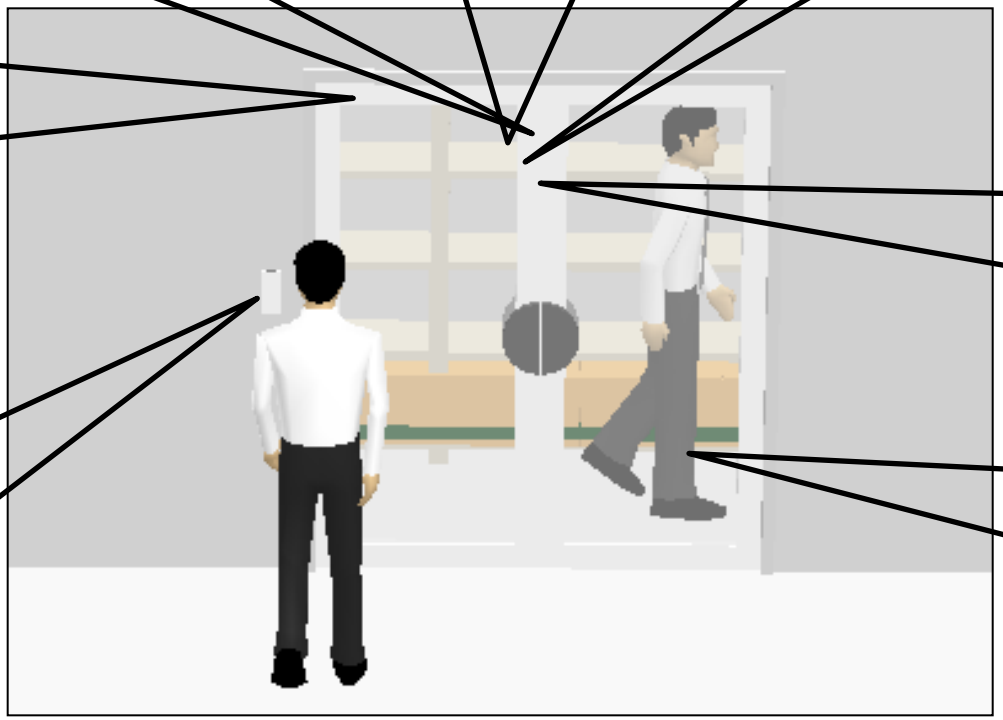
扉の内側（セキュリティ区域側）のシリンダー部にはひねることで解錠できるサムターンを設置します。通常は、プラスチック製のサムターンカバーにより被覆し緊急時に取り外し解錠します。

火災報知器発報時の自動解錠

火災報知器発報時に当該箇所（若しくは全）電気錠を自動的に解錠します。

ドアクローザ

自動施錠を確実にする為に、稼働側の扉はドアクローザにより自動的に閉扉することが必要です。



電気錠設置箇所。

ガラス窓が付いている枠付き扉（かまち扉）の場合は枠部分にモータ錠（AL3M)を設置します。

入退室機器設置箇所

稼働する扉側横壁に入退室機器を設置します。　高さは機器中心が床面から1,200mm程度が最適といわれております。

＊実際の機器の色は黒です。

両開き扉の片側は固定します。

自動施錠を確実にする為に片側の扉は固定します。

Copyright©2016 Identicservice Co.Ltd all rights reserved