CENTRAL SECURITY PATROLS CO.,LTD.

平成26年度11月度・技術セミナー

『オフィスビルの入退室セキュリティ向上のために』

-ｽﾑｰｽﾞで確実「交通系ICｶｰﾄﾞ」を使ったｾｷｭﾘﾃｨｼｽﾃﾑ-

セントラル警備保障株式会社
関西圏営業部　山田　勝弘

大阪府下の犯罪発生状況

大阪府下の犯罪発生状況①

◆大阪は全国で犯罪率がもっとも高い

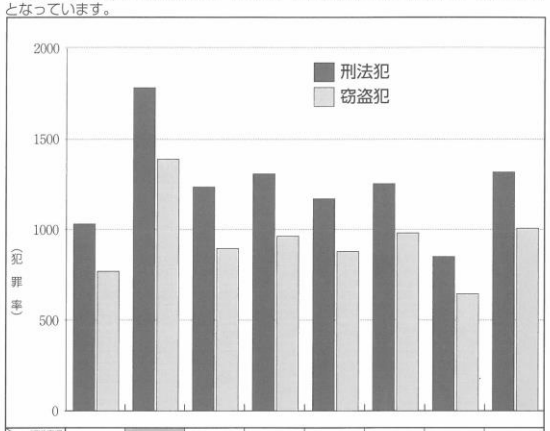
刑法犯の発生件数の、全国の約１割を占めている

人口１０万人当りの発生件数(犯罪率)は全国でもっとも多い

全国での刑法犯のうち、８割弱が窃盗犯が占めているが、
大阪の窃盗犯は、全国平均犯罪率の約1.8倍

主要都道府県刑法犯発生状況（平成25年中）

刑法犯発生件数は、全国の約１割を占めています。
人口１０万人当たりの発生件数（犯罪率）は、大阪が全国で最も多く、次いで福岡となっています。



区分＼都道府県	全国	大阪	東京	愛知	埼玉	千葉	神奈川	福岡
刑法犯発生件数	1,320,678	157,951	162,557	96,839	84,154	77,904	76,962	66,794
犯罪率	1,031	1,782	1,235	1,307	1,170	1,253	851	1,317
凶悪犯	6,766	1,010	854	471	436	376	472	337
犯罪率	5	11	6	6	6	6	5	7
粗暴犯	66,610	6,687	8,603	3,564	4,438	3,395	5,376	2,767
犯罪率	52	75	65	48	62	55	59	55
窃盗犯	986,272	123,075	117,969	71,473	63,270	60,993	58,443	51,081
犯罪率	770	1,388	896	964	879	981	646	1,007
知能犯	43,186	4,678	7,668	2,035	1,829	1,985	2,950	1,519
犯罪率	34	53	58	27	25	32	33	30
風俗犯	12,064	1,746	1,381	628	747	424	712	877
犯罪率	9	20	10	8	10	7	8	17
その他	205,780	20,755	26,082	18,668	13,434	10,731	9,009	10,213
犯罪率	161	234	198	252	187	173	100	201
人　口	128,057,352	8,865,245	13,159,388	7,410,719	7,194,556	6,216,289	9,048,331	5,071,968

※資料　総務省統計局　平成22年国勢調査人口集計結果（平成23年10月26日付）

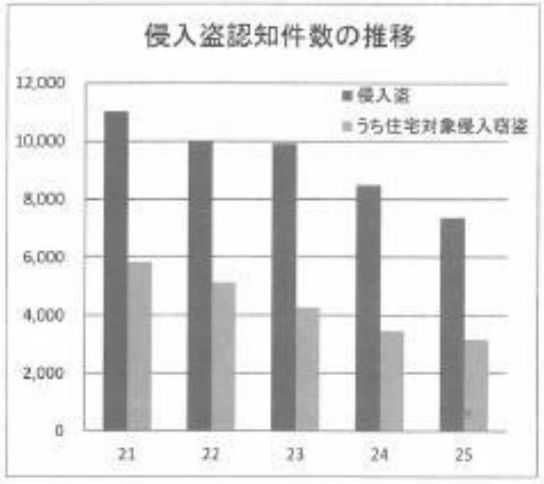
安全なまちづくり
ー地域安全活動資料ー　＜平成26年＞より

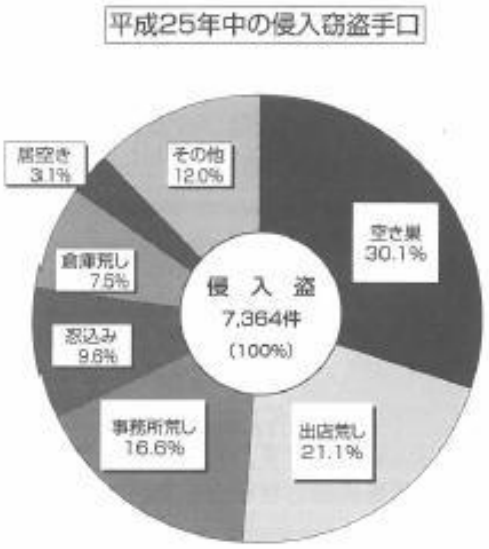
大阪府下の犯罪発生状況②

◆侵入盗

窃盗犯は『侵入盗』と『非侵入盗』に分かれる

大阪の侵入犯の手口別発生状況は、『空き巣』が全体の３割を占め、
ついで、『出店荒し』と『事務所荒し』の順になっている

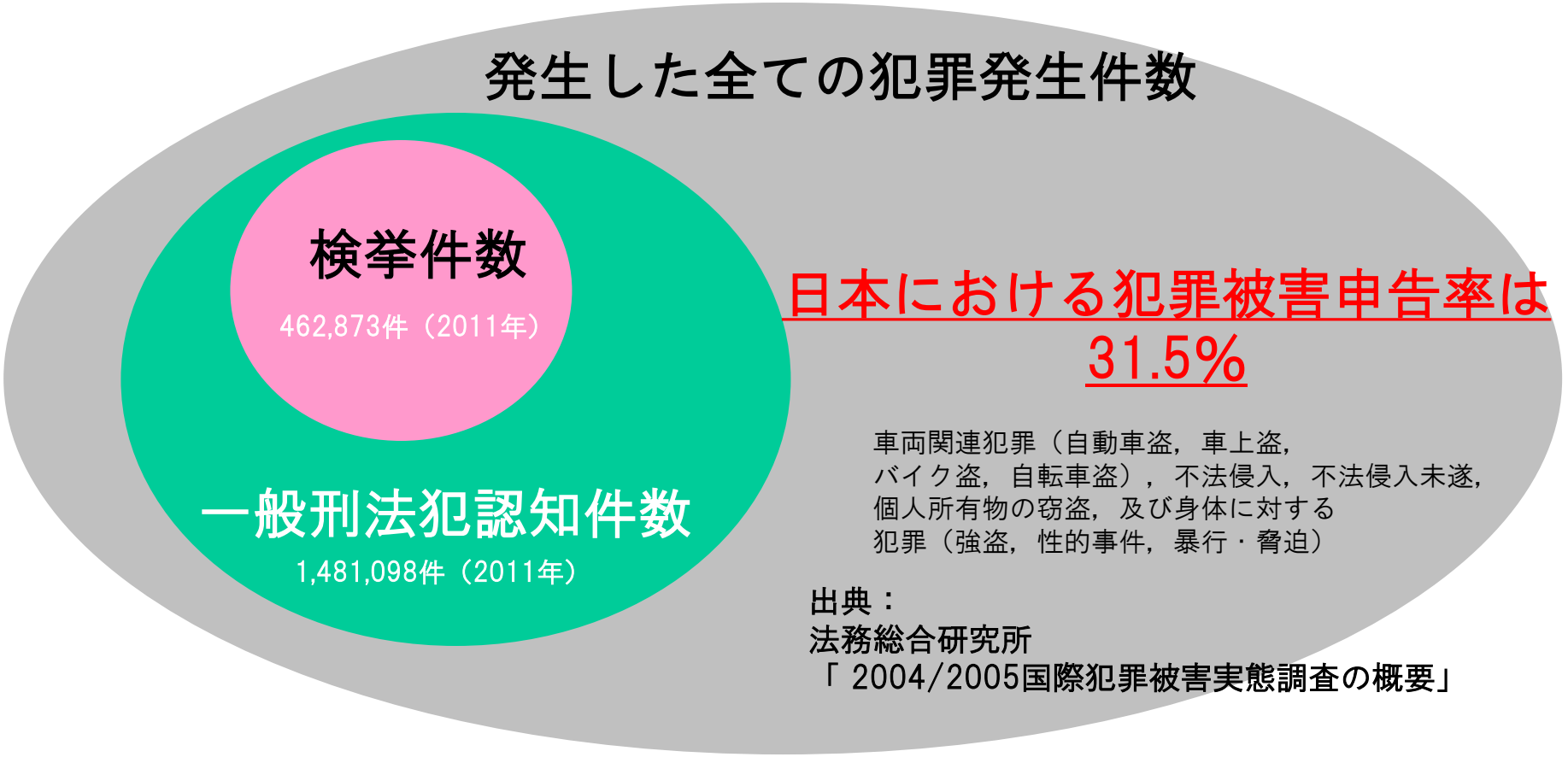




安全なまちづくり
ー地域安全活動資料ー　＜平成26年＞より

暗数の存在

◆発生した犯罪の全てが警察に届けられ認知されている訳ではありません



日本における犯罪被害申告率は
31.5%

車両関連犯罪（自動車盗，車上盗，
バイク盗，自転車盗），不法侵入，不法侵入未遂，
個人所有物の窃盗，及び身体に対する
犯罪（強盗，性的事件，暴行・脅迫）

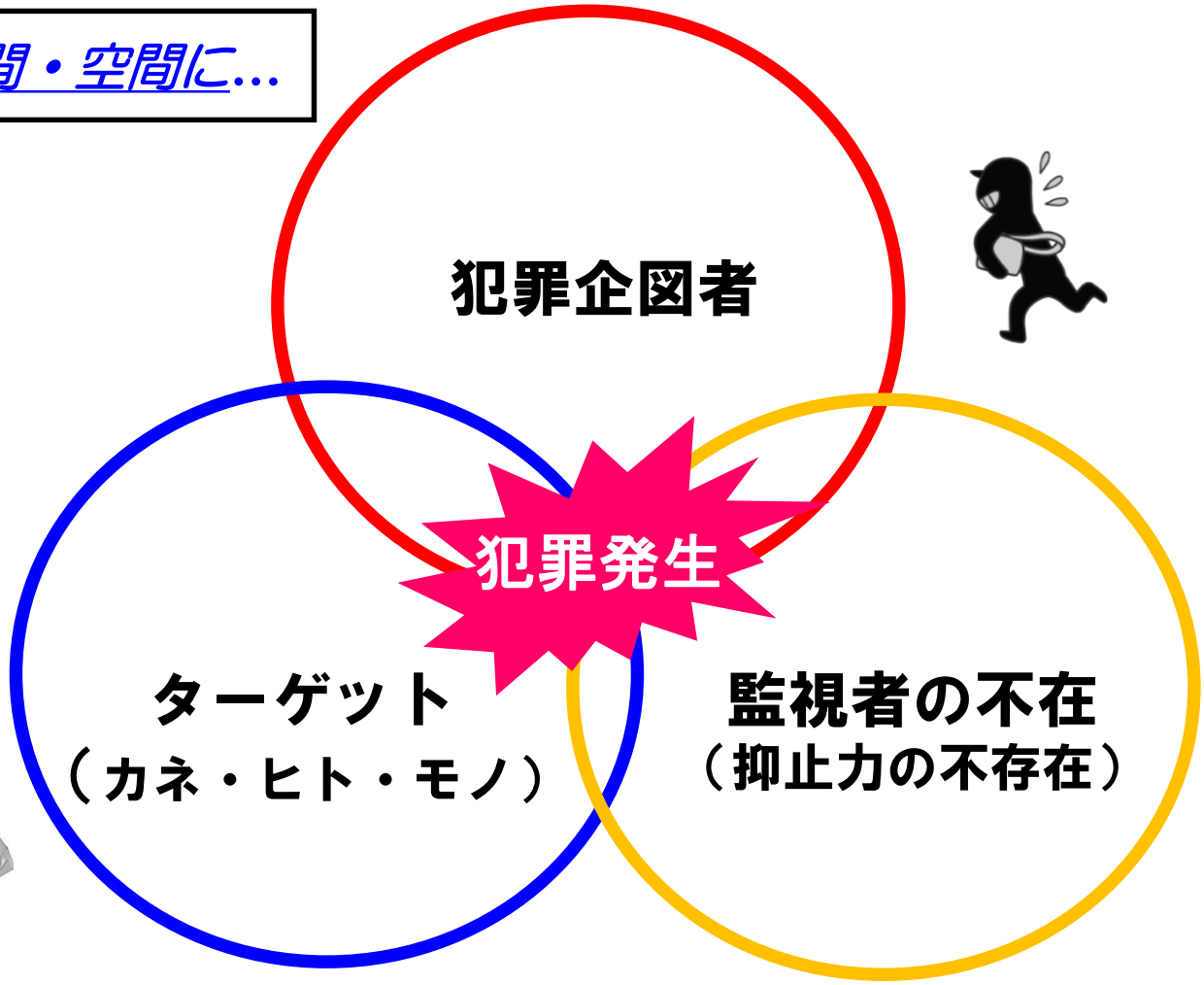
出典：
法務総合研究所
「2004/2005国際犯罪被害実態調査の概要」

オフィスビルのリスクと
セキュリティの必要性

犯罪に対抗するために①

◆ルーティンアクティビティセオリー

同じ時間・空間に…



犯罪に対抗するために②

◆ＣＰＴＥＤ理論(Crime Prevention Through Environmental Design)

犯罪が発生する物的な環境や状況に着目した犯罪予防の防犯環境設計手法

ＣＰＴＥＤ理論のイメージ

【対象物の強化】
- 鍵、ガラス、扉の強化
- 金庫を防盗性の高いものを使用

【監視性の確保】
- 植栽の手入れ
- 防犯カメラの設置
- 通行人の目を利用する
- 常駐警備員配置

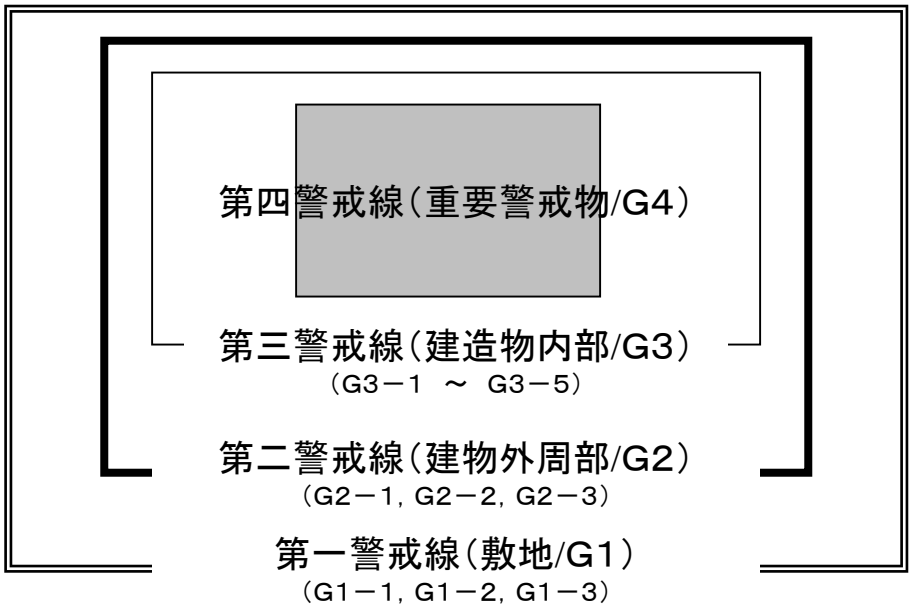
【接近の制御】
- エントランスを二重アクセスとする
- 侵入対策に有効なフェンスや生垣設置

【領域性の確保】
- 敷地内外の清掃活動
- 立入り禁止などの告知
- 近隣とのコミュニケーション醸成

犯罪に対抗するために③

◆ゾーンディフェンス理論

施設を第一警戒線（敷地）、第二警戒線（建物外周部）、第三警戒線（建造物内部）、第四警戒線（重要物警戒）の四段階に警戒線を設定し、
それぞれに対して個別の評価と対策を行うことが有効であるとした理論。



注意
防犯＝侵入されにくい ⇔ 災害＝避難しやすい

特に大規模火災や地震など避難の緊急性が高い場合において、避難上の手立てが必要！
高度なセキュリティを構築する一方、
防災面を考慮した設計が必要！

オフィスビルのリスク

◆オフィスビルのリスク
◆リスク管理の要求増加

◆知る、見る、調べる、そして連絡するがキーポイント

放火・破壊

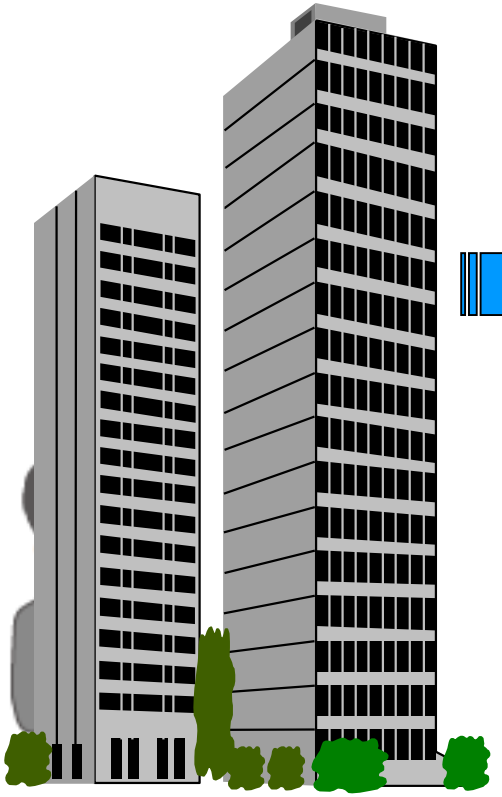
事故・災害

ビル施設を取り巻くリスク

侵入・窃盗

内部問題

悪戯行為



知る
施設への侵入者発見

見る
施設内外の状況監視

対策のキーポイント

調べる
施設への入場者管理

連絡する
施設の連絡通報管理

オフィスビルのセキュリティシステムの必要性

◆防犯・防火・防災対策

侵入盗の防止

防火・防災

企業の内部管理強化

◆コスト削減

人的管理からシステムによる管理へ

入室制限・在室管理～残業抑制

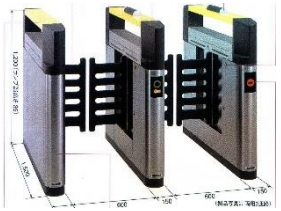
照明等の設備との連動

ビルの価値の向上

他ビルとの差別化

◆利便性向上

２４時間出入可能（気兼ねなく･･･結構ポイント）

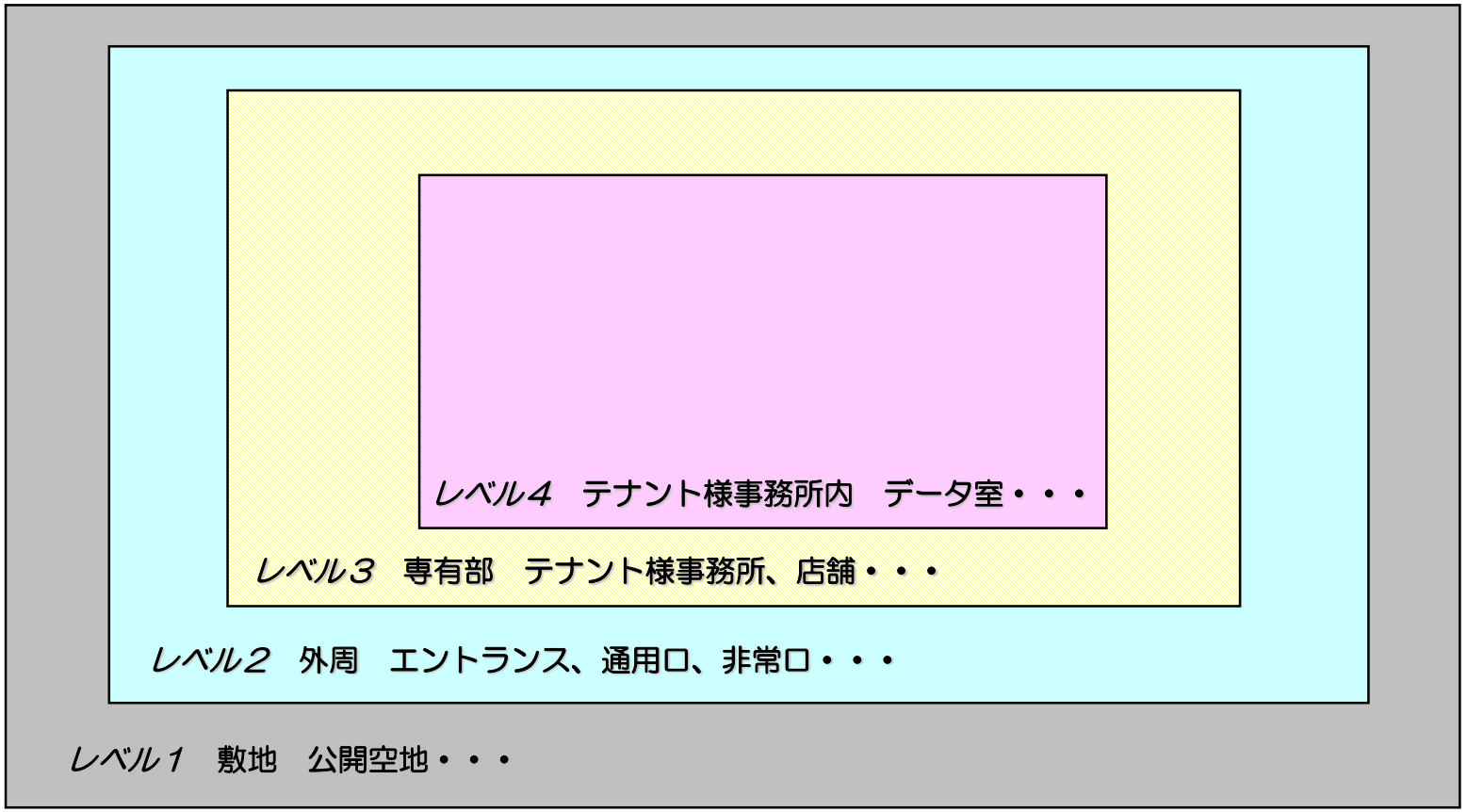


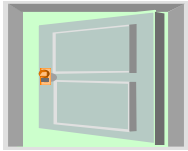
オフィスビルのセキュリティシステム

オフィスビルのセキュリティシステムの構築

◆オフィスビルのゾーンディフェンス

ビル全体を構造、用途、導線に適したレベル（ゾーン）に分割しそれぞれのレベルと運用に適したセキュリティを設置することにより、安全性と利便性のバランスの取れたセキュリティが実現できます。





セキュリティの種類①

◆大きく分けて、人的警備と機械による警備がある

常駐警備(人的警備)のメリットとデメリット

状況に応じた判断・対応が可能
人が常駐することによる犯行抑止効果
温かみのある対応
大量の情報処理時や集中力の低下によるミスが懸念
コストが高い(また、毎月継続)

機械による警備(セキュリティシステム)のメリットとデメリット

機械は確実に判断、休まない
コストが低い(初期に投資すれば　更に毎月安く)
柔軟な判断・対応は出来ない

人的警備＋セキュリティシステムが、一番いい！
防災センターの無い様なビルでは、セキュリティシステム＋機械警備を推薦

セキュリティの種類②

◆機械による警備(セキュリティシステム)

防犯カメラシステム

視認性補完、記録、犯行抑止、監視(防災センター等)

入退管理システム

不必要な人を入れない
入退室の資格と必要性をシステムで判断
機械警備と連動可能

機械警備(警備業法による)

各種センサーを設置
警備会社の基地局で遠隔監視、パトロール員が対応
※最近では画像の監視も

オフィスビルの入退管理システムの種類①

◆エリア別

共用部

シャッター制御
通用口・電気錠制御　　スケジュール・認証
エレベーター制御

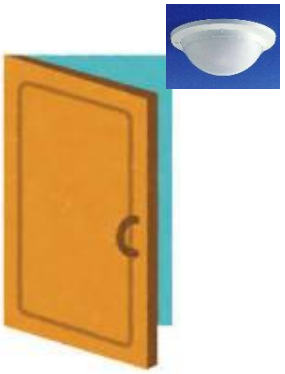
ゲート(自動改札のイメージ、資格と必要性の判断が確実、人員削減)

共用部　防犯センサー（注意あり）

専有部

専有部　防犯センサー

出入口電気錠制御



◆認証別

生体認証　指紋、静脈、虹彩、顔面･･･(大人数の登録は？しょっちゅう出入)

カード　　生体に比較しセキュリティレベルは落ちるが、管理面で有利

注）機器姿図はご参考

オフィスビルの入退管理システムの種類②

◆認証場所別

通用口外側　(入館用)

通用口内側　操作集合盤(専有部警戒・入室用)

鍵ボックスなし

専有部扉の電気錠連動　　専有部扉は鍵で開閉

鍵ボックスあり

専有部扉の鍵をボックスで保管　キーケースで保管

専有部扉　　操作機(専有部警戒・入室用)

専有部扉の電気錠制御　　専有部は鍵で開閉

鍵は紛失した場合　シリンダー交換　全社員の鍵の交換も

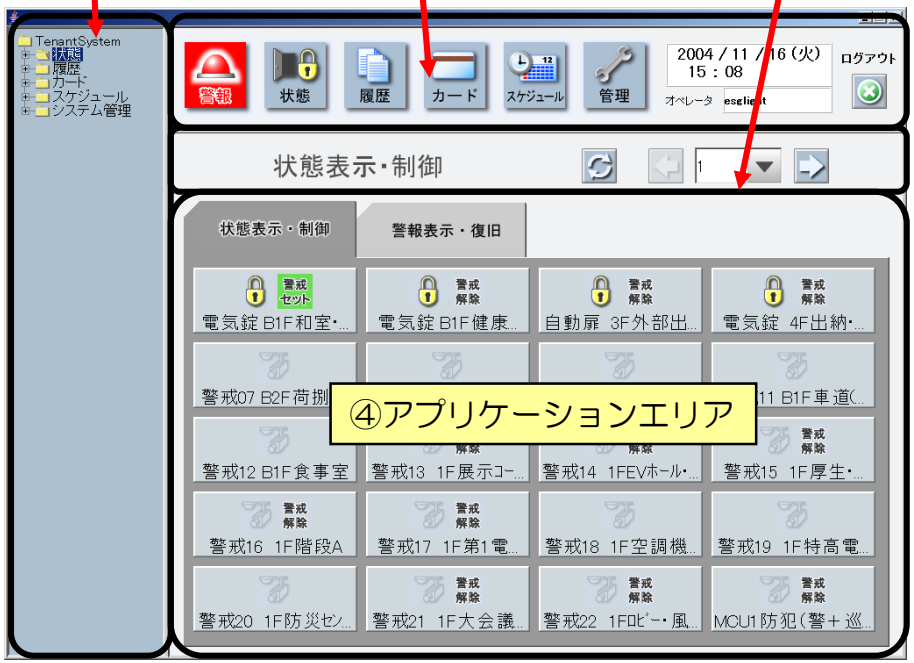
内部管理強化には入退室管理・電気錠制御が必要

やっぱり　入退室管理！　カード　＋　電気錠制御

オフィスビルの入退管理システムの例①

◆入退室管理システム【画面構成と操作メニュー】

ユーザ認証後に各操作を行う画面は、下図のレイアウト構成となります。

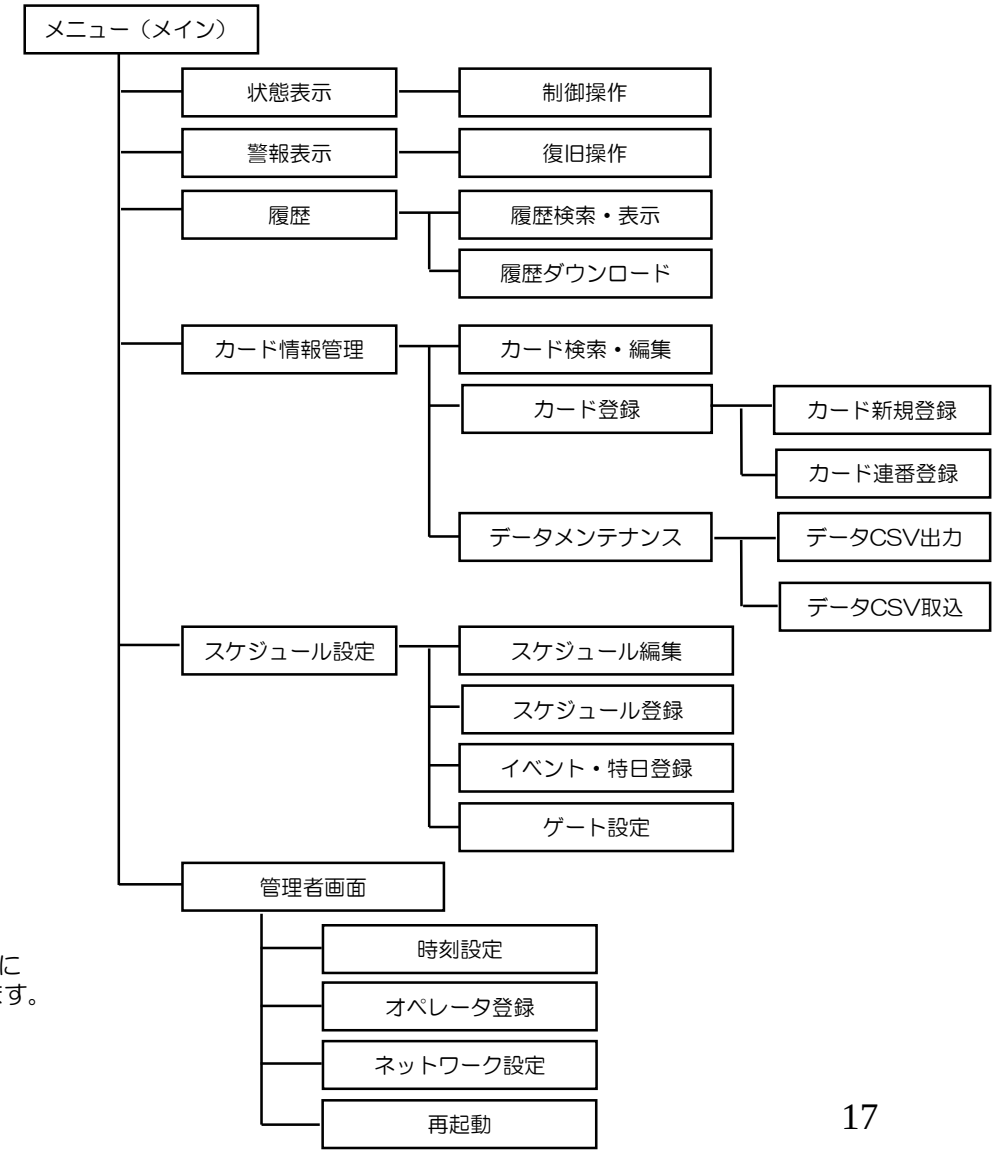


①メニュー構成
　使用可能な項目がツリー状に表示されます。項目を選択すると該当する画面へ遷移します。

②メニュー選択
　メニューの選択及びログアウト操作を行います。この部分は定期的（5秒おき）にコントローラへアクセスを行うことで異常・警報発生時に警報発報表示を行います。

③ページ操作
　ページの遷移及び状態更新を行います。

④アプリケーションエリア
　各操作を行う画面を表示します。メニュー画面によって選択された画面がこのエリアに表示されます。



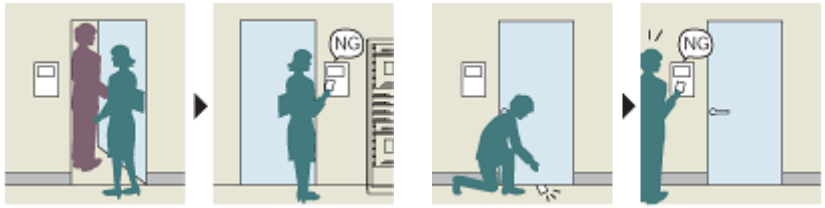
オフィスビルの入退管理システムの例②

◆入退室管理システム【各種機能】

アンチパスバック機能

●アンチパスバック

許可された人に紛れて入退室すると、次に入室や退室ができません。



カードをもっていても、カード操作なしで入室（退室）すると　次に退室（入室）できません　入室したカードを室内から受け取って再入室しようとしても　入室できません

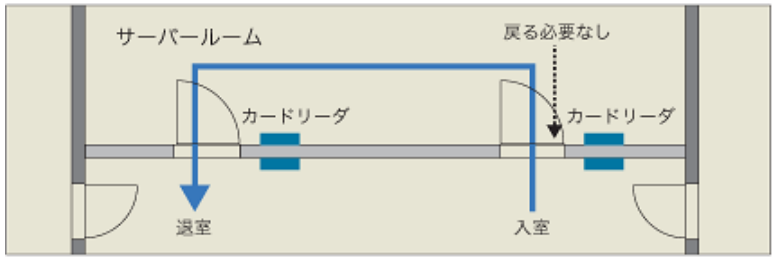
カード操作なしの入退室を防ぐ機能。
「入室」⇔「退室」の手順をふまないと不正使用と判断します。

グローバルアンチパスバック機能

●グローバルアンチパスバック

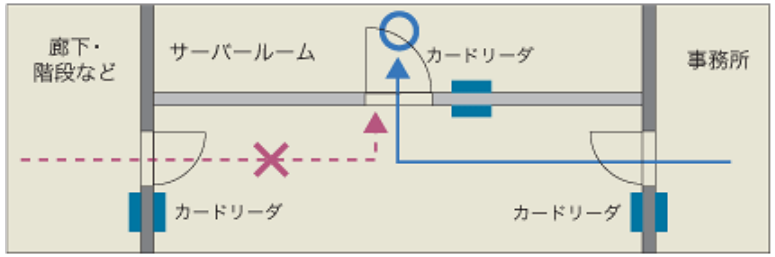
入室したゲートに関わらず、アンチパスバックを機能させることができます。

アンチパスバックを複数のゲートで運用。
入室ゲートと退室ゲートが異なってもチェック機能がはたらきます。



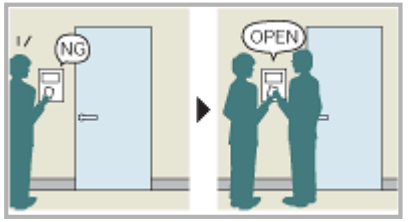
ルートチェック機能

特定のゲートを通過しないと、次のゲートが通過できないようにする機能です。
アクセスルートを限定することで、非常階段などからのアクセスを防ぎます。



ツーパーソンルール（２名照合機能）

たとえ登録者でも、１人では入退室できない機能です。
2名照合で初めて解錠できるため心理的なけん制による犯罪抑止が期待できます。
2名以上の在室がある場合は、1人でも入退室できます。



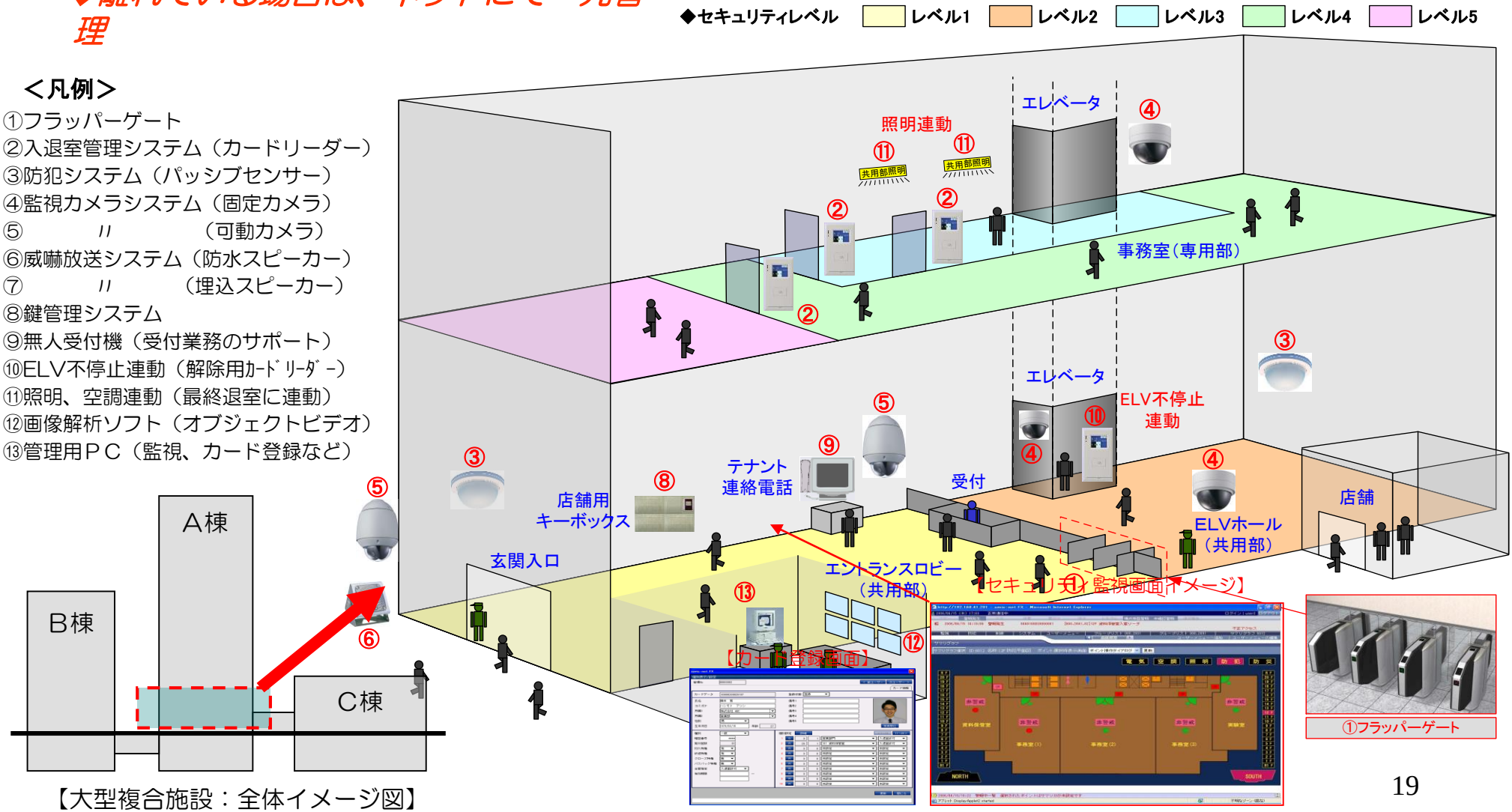
１人では解錠不可　2名照合で解錠

オフィスビルの入退管理システムの例③

◆入退室管理システム【他システムとの連動】

- ◆複数棟の一元管理が可能
- ◆離れている場合は、ネットにて一元管理

【A棟1～2階　拡大イメージ図】



【大型複合施設：全体イメージ図】

カードの基礎知識

セキュリティとカード社会

現代はカード社会とも呼ばれ、カードは非常に身近な存在になっています。

セキュリティ市場もカード認証による個人識別が主流であり、このカードを
中心とした様々な設備連携による利便性の向上が求められています。

カードの種類

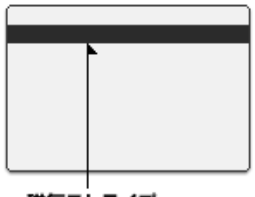
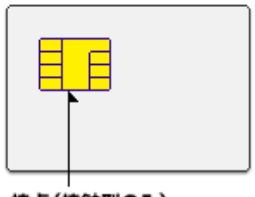
◆カード市場の傾向

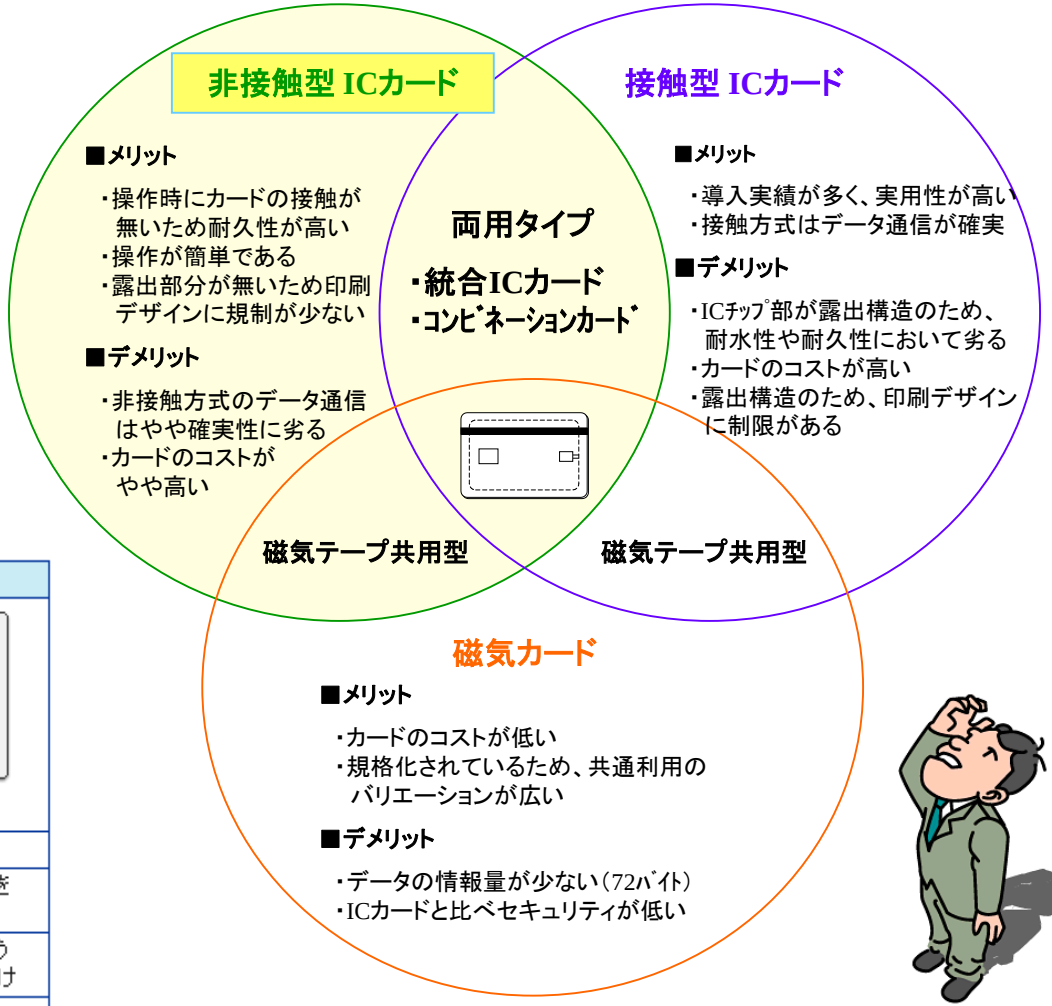
従来、市場では磁気カードが幅広く普及していましたが、近年は操作性と安全性から
非接触ＩＣカードが多く導入されています。

◆非接触ＩＣカードの種類

TypeA（マイフェア）・・欧州で広く流通
TypeB　・・・・・・・・国民基本台帳など
FeliCa（フェリカ）・・・電子マネー（Edy）が有名

◆磁気カードとＩＣカードの比較

項　目	磁気カード	ICカード
外　観		
メモリー容量（文字数）	～72文字程度	～16000文字程度
カード内での情報処理	不可能（情報を記憶するのみ）	CPU（中央演算処理装置）を内蔵していれば可能
情報の読み取り／書き込み方法	磁気ストライプに磁気ヘッドを接触させて行う。	接触型：表面の接点から行う 非接触型：R/Wに近づけるだけ
認　証	磁気カードリーダと中央センタ間（オンライン認証）	リーダライタとICカード間（ローカル照合）
不正アクセス・改竄	比較的容易	困　難
カードの複製	比較的容易	困　難
セキュリティ機能	比較的弱い	強　い



一般的に非接触ＩＣカードの認証距離は10cm以下である。
これ以外に、近傍型：認証距離が約70cm、遠隔型：認証距離が数ｍのタイプがあり、ＵＨＦ帯の周波数を使ったＲＦＩＤと呼ばれている。
※ＲＦＩＤとは「電波による個別識別」の技術を意味する。
　広義では、非接触ＩＣカードも含まれる。

非接触ＩＣカードの種類

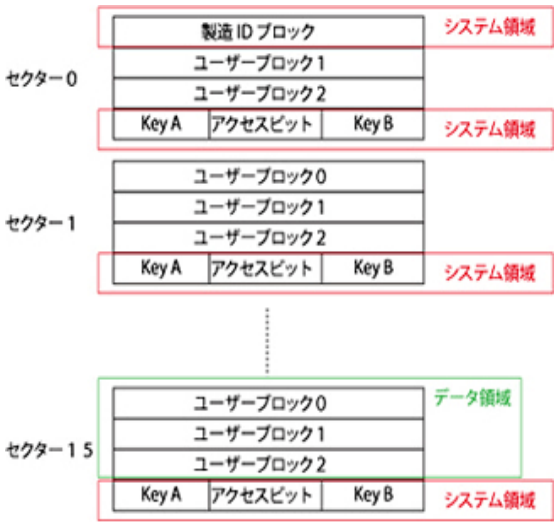
◆非接触ＩＣカードは大きく分けて
FeliCa（フェリカ）
TypeA（マイフェア）
TypeB（eLWISE）
の３種類があります。

◆交通系ICカードは
FeliCa（フェリカ）がベースです。

参考　◆FeliCa（フェリカ）

エリアとはフォルダに相当するもので、エリアの下にさらに階層的にエリアを作成することも可能。サービスは、データへのアクセス種類や権限を定義する。エリアやサービスに設定する「アクセスキー」は権限の無い者のアクセスを防ぐ。

参考　◆TypeＡ（マイフェア）



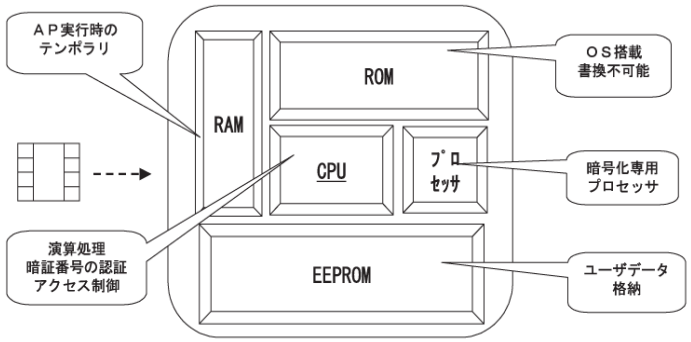
■セクター
・セクターは全部で16個（0～15）ある。
・1セクターは4つのブロックから成り立つ。
・3つのユーザーブロックと1つのシステムブロック（セクタートレイラー）で構成。

■アクセスビット
・ユーザーブロックとセクタートレイラーに対するアクセス条件を定義する。
・アクセスパターンは各8種類ある。
・ユーザーブロックへはアクセス方法と使用するkeyを定義している。

■ユーザーブロック
・ユーザーのデータを格納するブロック。
・1ブロック＝16バイト

参考　◆TypeＢ（eLWISE）

・CPU が暗号化，認証，アクセス制御を可能にしている.
・ROM にはOS，権限情報などを格納するが書換え不可。
・書換え可能なユーザのデータはEEPROMに格納している.
・通常のＩＣカードと比べ、10倍以上の情報管理が可能。
・非接触型と接触型の両方のインターフェースを搭載。



交通系ICカードを使った
入退室管理システム

交通系ＩＣカードのエリア図

2013年3月23日より、主要10種類の相互利用サービスが開始されました。
企業の支店・営業所が共通して利用できるカードとしてご提案しております。

【交通系ICカードの相互利用図】

相互利用可能

京阪神エリア

PiTaPa 【対応済み】

ICOCA 【対応済み】

岡山･広島･香川エリア

北海道エリア

【対応済み】 Kitaca

首都圏エリア

Suica 【対応済み】

【対応済み】 PASMO

仙台･新潟エリア

九州エリア

【対応済み】 SUGOCA

【対応済み】 nimoca

【対応済み】 はやかけん

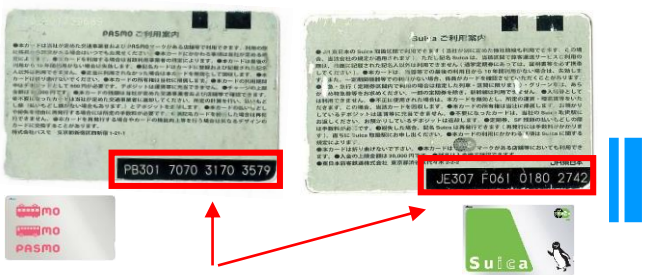
【対応済み】 Manaca

【対応済み】 TOICA

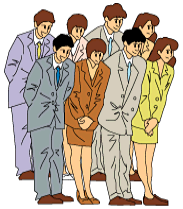
東海エリア

カード登録がスムーズ

◆店舗など従業員の入れ替わりが多い施設（運用）に最適



（カード裏の17桁を登録申請します）



こんな大勢！
わからんやん

カード発行の手配や
離職時の回収など
管理の手間･･･

カード番号を
教えて下さい

ビル側に申請

登録も楽勝！

個人所有のカードが
登録可能です。
（手配・回収が不要）

カード運用がスムーズ①

◆カードが少なくてすみます

＜独自ｾｷｭﾘﾃｨのカードを所有するテナント様＞

社員証はビルに登録でけへんの？

【○階】

- 社員証
- ビルカード

財布がパンパンやん！
どのカードやったかなぁ

＜新しくセキュリティを導入するテナント様＞

ビル共用部の通行には別のビルカードが必要やなあ

【△階】

- 独自カード
- ビルカード

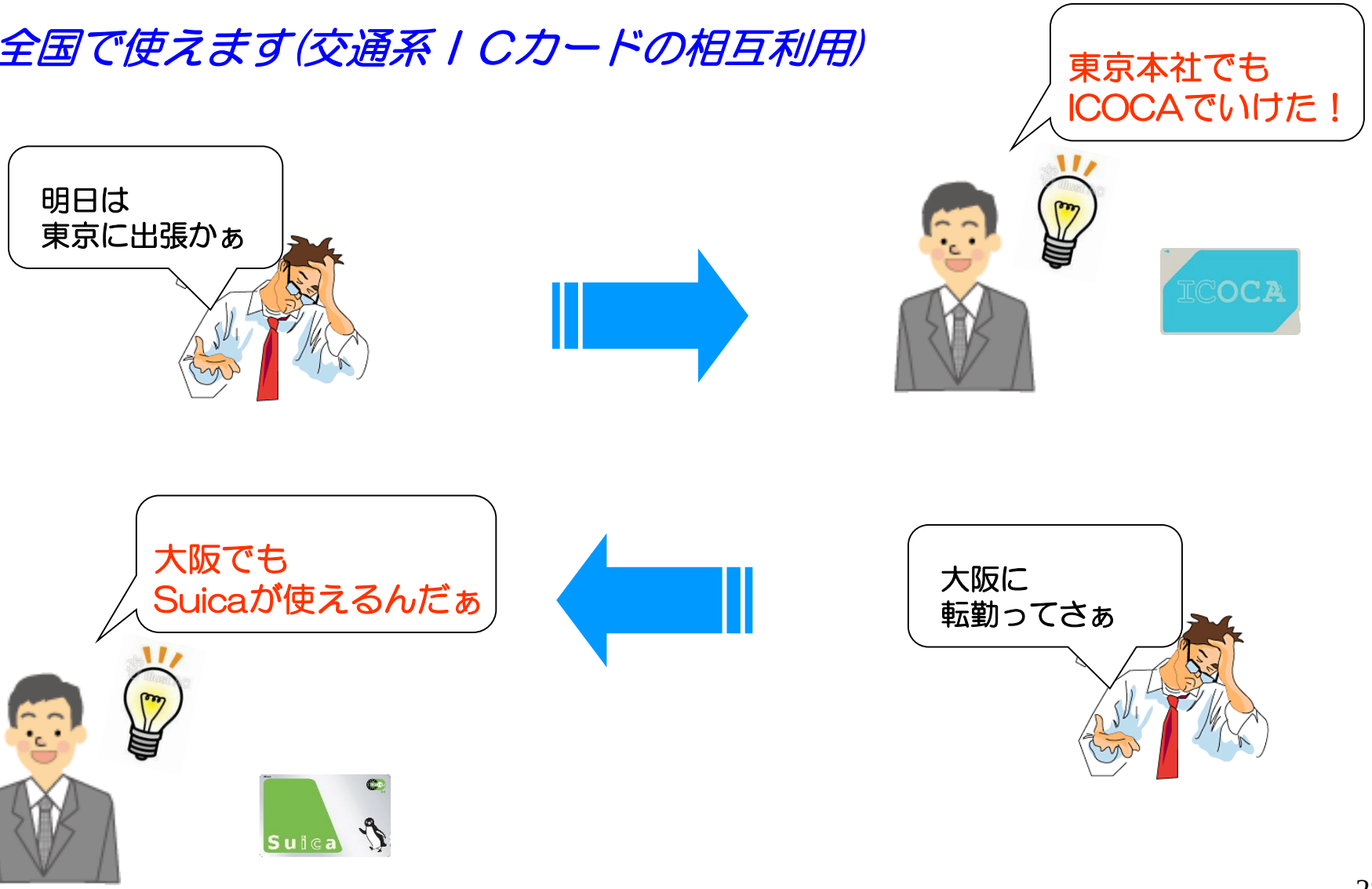
多くのお客様は、
カード枚数が
できる限り少なく
運用できる方法を
希望されています。

１枚でいけた！

交通系ＩＣカードは多くの人が通勤用で所持しています。ビルのセキュリティカードとして導入すれば、テナント様にカード所持の負担をかけない運用が可能です。

カード運用がスムーズ②

◆全国で使えます(交通系ＩＣカードの相互利用)



セキュリティが確実

◆交通系ＩＣカードの照合方式

通常、交通系カードの所有権は鉄道会社に帰属しているため、入退室管理システムの照合に使用する個人識別データを書き込むことはできません。
そのため、弊社は鉄道会社以外には開示されていないＩＤデータ（ＩＤＩ）を照合できる入退室管理システムを構築しました。
尚、このＩＤデータは外部に開示できないため、システムに登録する方法に工夫が必要でした。

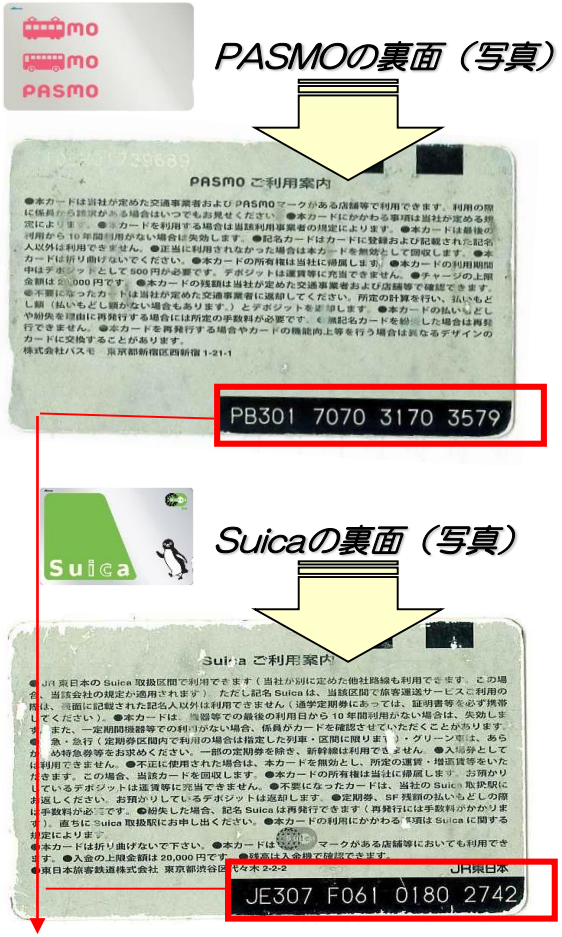
そこで・・・

交通系ＩＣカード
の裏面右下に刻印されている17桁のコード（英字と数字）をシステムに登録することでカードのＩＤデータが認証できる仕組みを構築しました。

これの利点は、誰でも容易に確認できる識別コード（カード番号）で運用ができ、カード内に特別なデータを書き込む必要がないため、既存のカードをそのまま使用する事（照合）ができることです。

※ＩＤデータ（ＩＤＩ）認証方式の理由

- 一般的にidm番号（製造番号）のみを認証に使用する方法もありますが、idm番号は容易に読み取り可能なデータとなっているため、これだけの認証はセキュリティ性が大きく劣ります。
  また、idm番号はカードに刻印されていない内部データのため、登録の際には登録用カードリーダーに都度カードを照合させる方法と、事前にカードリーダーの照合でidm番号を抽出しておく必要があります。
  これらのことから、弊社はセキュリティ性が高く維持できつつ、容易にカード番号を識別できるＩＤデータ（ＩＤＩ）認証方法を構築しました。



この17桁のコードをシステムに登録して運用します

交通系ＩＣカードで無い場合でもスムーズで確実

◆Felicaも使える！

◆しかも確実！

ＩＣカード（Felica）の管理者が発行する
“システムコード（カードを作成する企業ごとに割り振ります）”
と“Idm番号（カードの製造番号です）”の
ダブルチェックにて照合できる方式をとります。

これの利点は、カード内に特別なデータを書き込む必要なく認証（照合）できることです。（カード発行に関する制約を受けずに運用が可能です）
つまり、既存のカードをそのまま使用する事（照合）が可能になります。

※ダブルチェックの理由
- 一般的にidm番号（製造番号）のみを認証に使用する方法もありますが、idm番号は容易に読み取り可能なデータとなっているため、これだけの認証はセキュリティ性が大きく劣ります。
  このため、カード自体を最初に認証するために使用する“システムコード”を同時に認証することにより、高いセキュリティ性を確保します。

※既存のFelicaカードには、システムコードとidm番号は必ずあります。

カードが破損・故障しても安心

◆カードが破損・故障したら？

故障？

駅窓口に
依頼

認証しない･･･
折れ曲がりなど

データ移行した
新しいカードを
発行

交通系ＩＣカードの所有権は
鉄道事業者に帰属します

交通系ＩＣカードが不要になる際は、
駅に返却すると、デポジット代金
（保証金￥500）が戻ります。
デポジットのみSuicaが購入も可能です

つまり･･･

カード代金￥0の運用が可能！

交換しても再登録不要！

コストも安心

◆結構　見落としがちな　セキュリティカードのランニングコスト

導入当初はもちろんのこと、

人事異動の度にセキュリティカードを発行するとなると・・・・

【　例　】
毎年４月　１０テナント様　各１０名異動(１０枚)＝１００枚
カード１枚の単価が1,500円の場合
150,000円となります

安なるやん！

定期券等の交通系ＩＣカードを使った場合は、
その、150,000円の費用が不要になるうえに、

登録も簡単で
登録に係る費用も安心です。

最後に

近年、セキュリティのスタンダードとして活躍するＩＣカードは多様化が進み、様々な設備やサービスとの連携が可能になっています。

交通系ＩＣカードをセキュリティシステムに使うことにより、
お客様に適した、また、喜ばれる『スムーズで確実な』セキュリティシステムの構築が可能になると考えております。

＜　ご静聴ありがとうございました　＞