

「個人情報保護法」施行で求められる オフィススペースのセキュリティ対策 忘れてはいけない5つの「大原則」

コクヨオフィスシステム株式会社

今年4月、個人情報保護法(個人情報の保護に関する法律)が施行された。本人の意図しない個人情報の不正な流用や、個人情報を扱う企業によるずさんなデータ管理を防ぐ目的で生まれたこの法律の対象は「5000件以上の個人情報を取り扱う事業者」とされており、ほとんどの事業法人は含まれると考えておいていいだろう。なぜなら、個人情報には顧客名簿やさまざまなデータベースだけでなく、従業員が受けとった名刺まで含まれるからだ。それだけに、当然、オフィスにおいてもさまざまな対策が必要になってくる。ところが、「個人情報保護」という概念そのものが新しいこともあって、具体的にどんな対策から始めたらいいのか、なかなかわかりにくいのが現状だ。今回のオフィス改善工夫事例では、企業のセキュリティ対策のコンサルティングから支援まで手掛けるコクヨオフィスシステムの浅賀直樹氏に、個人情報保護法に関する基本的な考え方から対策の実例までを伺った。

個人情報保護法の施行に伴い、企業は個人データの漏洩や滅失を防止するための安全管理措置が義務づけられる。
個人情報には顧客データだけでなく、名刺や画像・映像データなども含まれるので、オフィス全体でセキュリティ対策が必要。
一点豪華主義のセキュリティシステムで情報は守れない。全体のバランスを考えた対策が不可欠。
どんな情報を、どんな対象から守るのか整理し、その分類ごとに最適なセキュリティ対策を考えなければならない。
オフィスの物理セキュリティの基本は、レベルごとのゾーニングによるレイアウト。そしてゾーンの境界にゲートを設ける。
ゲートとしては、有人受付、ICカードや生体認証システムなどがあり、必要なレベルに合わせて設置する。
キャビネットやファイルボックス、鍵などの単位でも利用許可を設定できるツールがある。

個人情報保護法とは？

目的と適用対象事業者

コンピュータと通信技術の発達により、個人に関するデータの流用性が飛躍的に高まる一方で、その取り扱い規定が明文化されていないという問題が指摘されていたことから、昨年5月に成立。2005年4月1日に施行されたのが個人情報保護法だ。条文の半数以上が「個人情報取扱事業者の義務等」にあてられていることでもわかるように、法制化の第一の目的は、顧客や一般消費者などの個人データを大量に保有する企業に対し、「取り扱う個人データの漏えい、滅失又は毀損防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」(第20条)と行動規定を命じることにある。

なお、法律を補足する政令第507号では、「事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6月以内のいずれの日においても5000を超えない者とする」と除外規定を設けているが、現実には営業活動を行っているほとんどの企業が適用対象になると考えていい。

事業者求められること

条文中にある「個人データの安全管理のために必要かつ適切な措置」とは、具体的には次のような内容の原則が示されている。

1. 個人情報を利用するときは目的を本人に明示しなければならない。
2. 個人情報は本人の了解を得て適正に取得しなければならない。
3. 個人情報は常に正確に保たなければならない。
4. 個人情報の流出や盗難、紛失を防止しなければならない。
5. 個人情報は本人の同意なしに第三者に提供できない。
6. 個人情報は本人の申し出により開示・訂正・停止しなければならない。
7. 個人情報に関する苦情には適正に対応しなければならない。

これらのうち「オフィス」に深く関わってくるのが4だ。セキュリティ対策が不十分で個人のデータが流出や紛失した場合、刑事訴訟の対象となり、法人と行為者が6カ月以下の懲役または30万円以下の罰金刑に処せられるだけでなく、民事訴訟により名誉毀損やプライバシー侵害による損害賠償責任を負う可能性もある。それだけに、オフィスにおける情報管理の仕組みやルールを徹底させなければならない。

ちなみに「個人情報」には顧客名簿はもちろん、名刺、防犯カメラで撮影された映像、電話の音声録音などかなり広範囲のものが含まれる。

なお、個人情報保護に関するJIS(JIS Q 15001:1999個人情報保護に関するコンプライアンス・プログラムの要求事項)に適合し、個人情報の取り扱いを適切に行うための体制を整備していると認定された事業者には財団法人日本情報処理開発協会からプライバシーマーク(Pマーク)が付与される。2005年4月20日現在、認定事業者数は1333社となっている。

TRY改善/ファシリティマネジャー特集のバックナンバーは<http://websanko.com>をご覧ください。

「TRY改善」

05年 11号	「特別予算」を相らずに移転できるフルパッケージオフィスレイトサービス(CWファシリティソリューション)
04年 7月号	見えてきた、オフィス生産性評価指標(日本オフィス学会)
04年 4月号	健康増進法の基準を満たしたオープン型喫煙コーナー(エーザイ)
FM特集	
03年 11月号	史上最大級122,000人が移動したオフィス再編成(みずほ銀行)
03年 9月号	理想的な本社オフィスの創造でFMの有効性を全社的に伝達(日本生命)
03年 7月号	事前に戦略を立て行動できるファシリティマネジャー(ソニー)
03年 5月号	「認定ファシリティマネジャー」はオフィスが共通語(東京海上あんしん生命保険)
03年 3月号	会社の枠を越えて広い人脈を得られた(エーザイ)
02年 11月号	オランダ、イギリスの先進的なオフィスづくり(富士ゼロックスゼネラルビジネス)
02年 9月号	経営戦略の中でFMを推進する。それが日本企業の課題(松岡総合研究所)
02年 7月号	コミュニケーションの促進がモチベーション向上に(リンクアンドモチベーション)
02年 5月号	郵政事業庁がすすめる先進的なマネジメント手法(総務省郵政事業庁)
02年 3月号	欧米から学ぶ、文化の響りのするファシリティマネジャーに(グローバルFM集団)
02年 1月号	FM業務支援サービスをオフィス移転プロジェクトに活用(三幸エステート)

01年 11月号	組織統合によるオフィスの新スタイル(アイ・ティ・フロンティア)
01年 9月号	FMの先進企業に見るオフィス戦略(日本アイ・ピー・エム)
01年 7月号	自分流のワークスタイルを実現する新しいオフィス(ソニー)
01年 5月号	在席率40%以下のフリーアドレス型オフィス(日本ビュレット・パッカー)
01年 3月号	オフィスデザインが社員のモチベーションを変える(日本ビュレット・パッカー)
01年 1月号	先進的なFM手法は「日本の発想」から(エクソンモービル)
00年 11月号	これからのオフィスについて広く意見交換する集まり(WFM)
00年 9月号	全社員完全フリーアドレスで創造とコミュニケーションが向上(JRパス関東)
00年 7月号	先進的なFM戦略が企業の経営体質強化に(ソニー)
00年 5月号	社内課金制度でコスト意識を徹底(オムロン)
00年 3月号	オフィスの効率化にはFM手法が最適(富士化学工業)
00年 1月号	日本企業にあったFM(富士通)
99年 11月号	ファシリティマネジャーが経営のスピードアップを促す(富士ゼロックス)
99年 9月号	財務評価手法で移転メリットを分析(中津元次氏)
99年 7月号	オフィスは考え抜いた作品である(日本オラクル)
99年 5月号	会社の経営全体を把握するファシリティマネジャー(東京海上)



ココヨオフィスシステム株式会社
CRM本部 CRM戦略企画部
CRM戦略企画グループ
リーダー
浅賀 直樹氏

セキュリティ対策は一点豪華主義ではなく 全体のバランスを考えながら進めるべき

個人情報保護法が成立した昨年の春以降、「完全なセキュリティ対策のできるオフィスにしたい」「入退室管理にICカードシステムを導入すればPマークは取得できるのか?」といった問い合わせが急増してきました。確かにこの法律の第四章「個人情報取扱事業者の義務等」の中では、安全管理措置として「個人情報取扱事業者は、その取り扱う個人情報の漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じなければならない」と企業側の対策を義務づけており、従来以上にセキュリティ意識を高める必要があるでしょう。しかし、残念ながら、法律では具体的な対策方法まで明示していませんから、たとえばオフィスのセキュリティにテーマを絞った場合、どこから手をつけていいのかわかりにくく、なかなかわかりにくいと思います。

私にご相談を受けた場合、最初に以下のことから説明するようにしています。

オフィスセキュリティの原則 1 セキュリティ対策はオフィス全体で考えなければいけません。

これは、あたりまえのようで、案外、忘れがちな原則です。

わかりやすいように、よく使われる「水の入った樽」の例えで解説しましょう。

樽は全体が一定の高さの板で囲まれていなければ水を貯めることはできません。一部だけ高くしても、他に低い部分があればそこから水が漏れてしまい、まったく意味をなさないので。



この場合、水とは個人データだけでなく、業務上のノウハウなどを含めた、漏洩してはならないすべての情報になります。

実際、ちくちく漏れのようなセキュリティ対策を行っている企業は少ないのです。

たとえば、個人情報保護法の施行に合わせて最新のファイアウォールを構築し、ネットワーク経由で情報が流出するのを防いでいながら、派遣社員を含む従業員が自由にノートパソコンを社外に持ち出しているため、そっちの危険性のほうが高いケースなどがそれにあたります。

また、「とにかく壁を高くすればいいんだろ」と、どんどん樽を上に乗せていってしまう企業もあります。たしかに情報漏洩のリスクは減りますが、そこに入る水(データ)の量以上に大きな樽(過剰なセキュリティ)を導入すると、今度は業務上の利便性が損なわれ、経営上のマイナスが生じます。もし、オフィス内のすべてのドアを個人認証でしか開かないようにしたら、いかに不便かわかりますよね。

したがって、セキュリティ対策を強化するにあたって、もう一つ、次の原則も考えてください。

オフィスセキュリティの原則 2 「何」を「誰」から守るかを整理し、 セキュリティの目的を明確にしましょう。

守るものが「何か」をはっきりさせなければ、オフィスをどう構築すればいいかわかりません。そして「誰から」を決めることで、どんなシステムを導入すればいいか、そこから具体的なプランニングを考えるのです。

セキュリティの目的を整理して 4つの「系」で対策を進めよう

ココヨオフィスシステムでは、この「セキュリティの目的」を、もう一度、原点から見直していただくために、次のようなチャートを用意しました。(図1)

セキュリティの対象となる「何」は、大きくアナログ(紙の書類など)とデジタル(コンピュータ上のデータなど)に分けられます。そして「誰」とは、昔は社外からの侵入者だけを考慮してはよかったです。最近では従業員が外にデータを持ち出す事件もあり、社内にも目を向けなければなりません。

このように、縦軸と横軸で4つに分類された「系」ごとに具体的な対策を考えます。

オフィスセキュリティの原則 3 セキュリティの目的によって対策は異なります。

- 空間ガード系
書類などを社外から守るには、入退室管理システムなどによって物理的に侵入を防ぎます。
- 空間管理系
オフィス内部をセキュリティレベルごとのゾーンに分け、「誰が」「いつ」入室したのか、チェック・管理を徹底します。キャビネットごとにセキュリティレベルを設定することもできます。
- ID管理系
データへのアクセスを制限するには、システム上のセキュリティ対策を

- ネットワークガード系
ネットワークへの社外からの侵入に対しては、ファイアウォールなどで対策を行います。

私たちは、この4つの系すべての対策をサポートしていますが、今回は、特にオフィスのセキュリティというテーマなので、1と2にあてはまる物理的な空間構築の方法について詳しく説明していきます。

そこにあるデータと利用できる人を整理し セキュリティレベルごとのゾーニングを

個人情報や業務ノウハウなどのデータの漏洩を防ぐ物理的セキュリティは、オフィス内のゾーニングレイアウトが基本になります。しかし、それを行うには、事前にレベルの設定が必要です。どのゾーンにどんなデータがあり、利用者は誰なのか、それを明確にすることから、レイアウトを考えていく必要があります。

オフィスセキュリティの原則 4 オフィススペースをセキュリティのレベルによっていくつかに分けます。 そしてゾーンごとに入室できる利用者を設定し、レベルの境界に何らかのゲートを設けます。

簡単な例として、レベルを3つに分けた場合を考えてみましょう。レベル1はロビーで、ここにはあらゆる人が入ってきます。(図2)次に「受付」というゲートを通るとオフィススペースに入れます。通常、ここからは社員のみ利用可能であり、取引先などのお客様は、レベル1のミーティング、応接コーナーで対応します。そしてレベル3になると、社員であっても許可された人しか入れません。当然、ここには物理的な境界ゲートを設け、入退室管理を厳しく行う必要があります。

なお、レベル設定をするとき、ただ利用者を分類するだけでなく、利用でき

図1 セキュリティ対策への基本理念

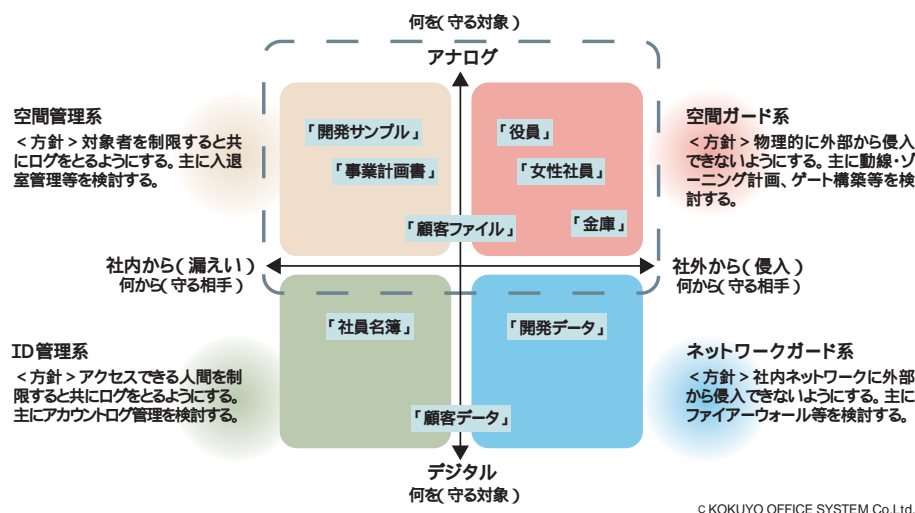


図2 セキュリティレベルの設定

(設定例)	エリア名称	対象スペース	利用者				
			セールス等	パートナー業者	派遣社員	一般社員	システム管理者等
レベル1	誰でも出入りできるエリア	受付・ロビーなど	利用可 平日: 夜間: x 休日: x	利用可 平日: 夜間: x 休日: x	利用可 平日: 夜間: x 休日: x	利用可 平日: 夜間: x 休日: x	利用可 平日: 夜間: x 休日: x
ゲート A	社員のみが通過できるゲート (外部からの不審者の侵入防止)						
レベル2	社員のみ出入りできるエリア	一般オフィススペースなど	利用不可	利用不可	利用可 平日: 夜間: x 休日: x	利用可 平日: 夜間: x 休日: x	利用可 平日: 夜間: x 休日: x
ゲート B	許可された社員のみが通過できるゲート (不特定多数の社員が利用することでの漏えい事故防止)						
レベル3	許可された社員のみ出入りできるエリア	サーバー室・金庫室など	利用不可	利用不可	利用不可	利用不可	利用可 平日: 夜間: x 休日: x

図3 レベルに合わせてゾーニング

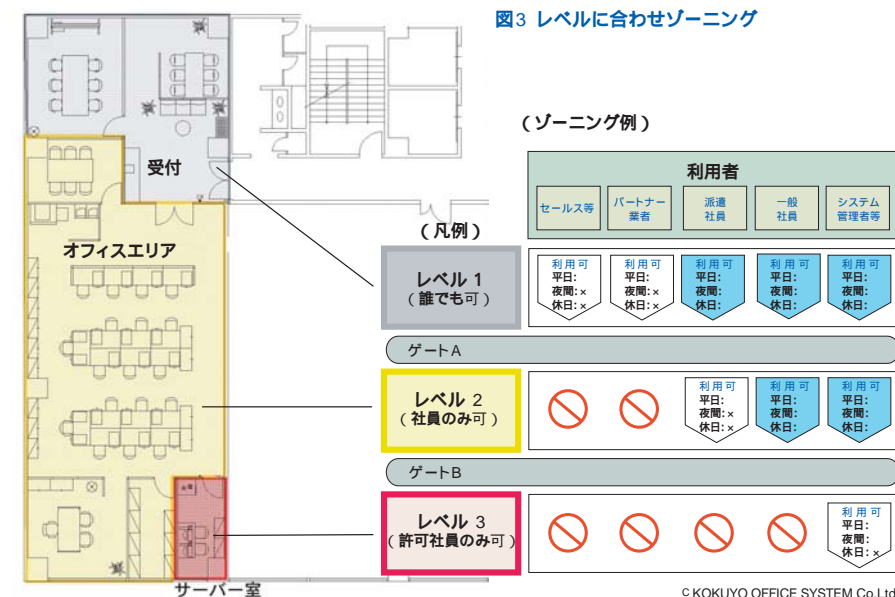


図4 オフィスのレベル設定例

レベル	名称	対象スペース	利用者				
			セールス等	顧客	パートナー 業者	一般 社員	システム 管理者等
レベル 1	パブリックエリア	受付・ロビー スペース等	利用可	利用可	利用可	利用可	利用可
ゲート			有人受付				
レベル 2	共用来客エリア	接客・応接 スペース等	不可	利用可	不可	利用可	利用可
ゲート			ICカード(非接触)式 セキュリティドア 社員同伴で開錠				
レベル 3	共用打合せエリア	商談・社内打合せ スペース等	不可	不可	利用可 要社員同伴	利用可	利用可
ゲート			ICカード(非接触)式 セキュリティドア				
レベル 4	一般執務エリア	一般執務・打合せ スペース等	不可	見学可 要社員同伴	不可	利用可	利用可
ゲート			施錠管理 一部担当者・利用者のみ鍵を保有				
レベル 5	特殊エリア	サーバー室・ 更衣室等	不可	不可	不可	不可	利用可

© KOKUYO OFFICE SYSTEM Co.Ltd.

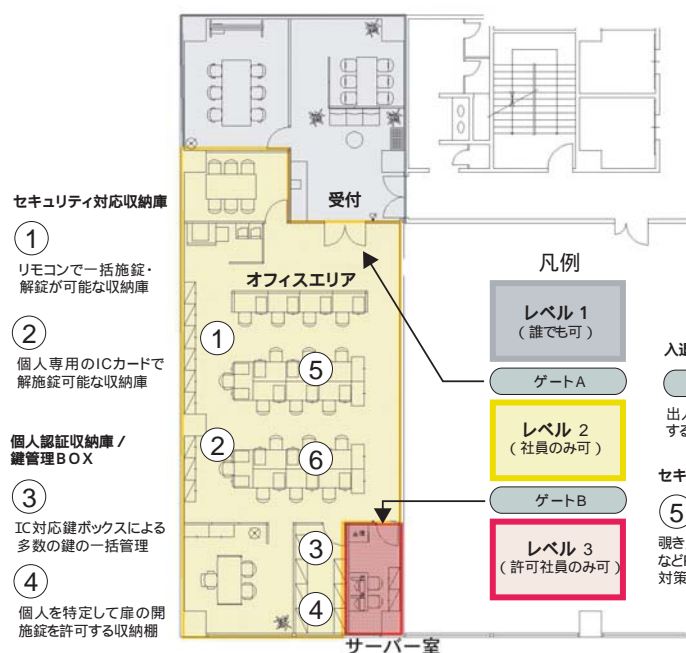
る曜日や時間も整理しておく、より精度の高いセキュリティが実現できます。

レベル設定が済んだら、次に平面図の上でオフィススペースのゾーニングをしていきます。このとき、原則としては入口から遠いところほどレベルを高くしてください。というも、スペースの関係でオフィスの奥にお客様も利用できる会議室を設置してしまうと、たとえ社員が同伴して案内したとしても、そこに行く途中で執務スペースが丸見えになってしまいます。これではせっかくゾーニングする意味がありません。つまり、セキュリティレベルによるゾーニングでは、人の動線も考えておく必要があるのです。

(47P図3)

ここで、霞が関ビルにあるコクヨオフィスシステムの本社の例を紹介します。私たちのオフィスでは、セキュリティのレベルは5段階に設定しました。そして各境界に設けるゲートは「有人受付 ICカード 施錠」として、確

図5 ゾーニング例



実な入退室管理を行っています。(図4)

コクヨオフィスシステムの場合、オフィスの構築事例を見せるショールーム「ライブオフィス」としての役目を果たさなければならぬため、一般執務スペースにも見学者が入ることがあります。その場合は社員が必ず同伴します。社員同伴の上に、来訪者はゲストカードとして全員色つきの首かけストラップを着用してもらっています。そのストラップの色で、視覚的にゲストと認知できるため、重要書類を裏返す、大きな声で会話を控えるなどの対応を全社員が行っています。また、最もレベルの高いサーバ室などは、システム管理者しか利用できないようになっています。

ICカードと生体認証システムの併用は有効 キャビネットでゾーニングできるツールも

このように、ゾーニングによるレイアウトプランが完成したら、ようやく、セキュリティシステムやツールの導入計画に進みます。

それでは、最近の企業の導入例をもとに、どのようなツールが利用されているのか解説しておきましょう。

オフィスセキュリティの原則 5 ゾーンごとのセキュリティレベルに合わせて最適なシステムやツールでゲートを構築していきます。

まず入退室管理システムとしては、私たちが導入しているICカードによる認証システムが一般的です。磁気カードのように第三者にコピーされる可能性はほとんどありませんし、オフィスの出入口のゲートや、さらにセキュリティレベルの高いゾーンの境界などによって細かく入室許可を設定できる点が大きなメリットといえます。

また非接触式なので認証にかかる時間も短く、通勤退勤時や昼休みのように大人数が移動するときにも、ドアのところで滞留することはありません。

ただ、ICカードは、紛失した場合、取得者

に悪用される可能性がないとはいえません。拾ったり、盗んだりした人が使えば、自由にオフィスに入ることができるからです。

このような心配から、個人データなどが最も集約しているサーバ室の入退室管理に指紋や静脈などのバイオ生体認証システムを採用する企業も増えてきました。つまり、通常のオフィススペースへのゲートはICカード、よりセキュリティレベルの高いゾーンへは生体認証という2段階の物理セキュリティでデータをより安全に守るのです。

生体認証システムは、ここ数年、技術は急激に進歩し、性能的にも價格的にも十分に検討材料になってきました。しかし、個人の認識にかかる時間は1秒もかからないものの、装置の前に立ち止まって手をかざしたり、適正な位置に合わせるのに若干の手間がかかるため、最高のセキュリティレベルが求められるデータセンターなどを除けば、オフィスの出入口を含むすべてのゲートに設置する方法はあまりお勧めできません。

ICカードによる入退室管理は、すでに多くの企業で採用され、従業員にとって導入に抵抗はないでしょうから、まずこのシステムを利用し、さらにより高いレベルのゾーンについてどうするか考えるほうが現実的なのでは

ないでしょうか。

また、何も壁を立てるだけがゾーニングではありません。部屋単位のゾーニングができないオフィスでは、セキュリティ対応収納庫や個人認証収納庫 / 鍵管理ボックスといった新しいツールが商品化されています。

セキュリティ対応収納庫は個人専用のカードで利用者を特定できるキャビネット、中のファイルボックスごとにもセキュリティレベルの設定が可能ですから、非常に細かいゾーニングに対応できます。また個人認証収納庫 / 鍵管理ボックスは、やはり鍵ごとに利用者を決められますので、あらゆるキャビネットに最適なセキュリティ対策を行えます。

また、IC対応セキュリティ収納庫で使うカードは、出入口に設置する認証機器で使用するカードとの共通化が可能であり、社員は複数枚持ち歩く必要がなくなります。

個人情報保護法の施行は、企業にとってセキュリティ意識を高めるうえでいい機会だと思います。それだけに、しっかりしたポリシーを持ち、全体にバランスのとれた対策を進めていけば、決して利便性を損なわないセキュリティオフィスが構築できるのではないのでしょうか。

具体的なセキュリティ対応什器

入退室管理システム

テンキー・ICカード
カードやパスワード入力によって
出入口をシャットアウトする認証機器群



テンキー



磁気カード



ICカード

バイオ認証機器

個人を特定し、
カードの貸し借りなどによる
なりすましを防ぐバイオ認証機器群



指紋照合機



虹彩認証



静脈パターン認証

セキュリティ対応収納庫

IC対応鍵ボックス

ICカードなどで管理できる鍵管理ボックス。個人を特定し、許可された鍵しか抜き差しができない。



IC対応収納庫

ICカードで認証・開錠を行うセキュリティ収納庫。オートロック機能により、鍵のかけ忘れを防止できる。



個人認証収納庫

個人を特定し、許可された社員だけが開錠できるキャビネットシステム。許可されていないファイルボックスを取り出すとエラーメッセージが出てログが残る仕組み。