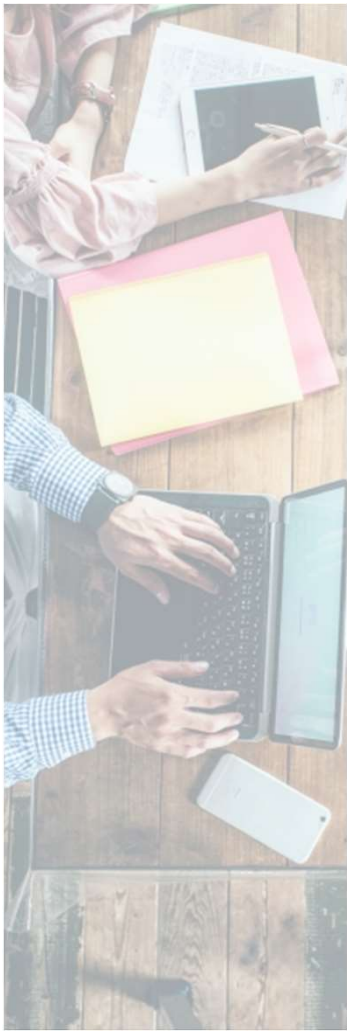
3分でわかる
あなたのオフィス
セキュリティ
対策

入退室管理システム&
監視カメラシステム
導入企業数　4,000社以上！
(2019年現在)

SECURE

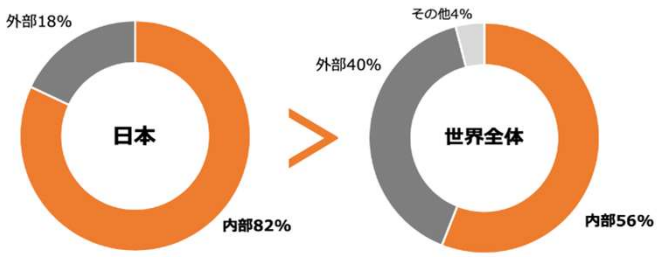
目　次



1．はじめに

オフィスセキュリティのうち、インターネットやパソコンのインターネットセキュリティや、施錠時の侵入に対するセキュリティ対策は進んでいるものの、営業時間中の「ひと」を対象した物理セキュリティ対策は遅れているのが実情です。その為に情報漏洩、部外者侵入によるリスク管理が問われるようになっています。

▶企業が受けた経済的被害の原因は８割が内部要因

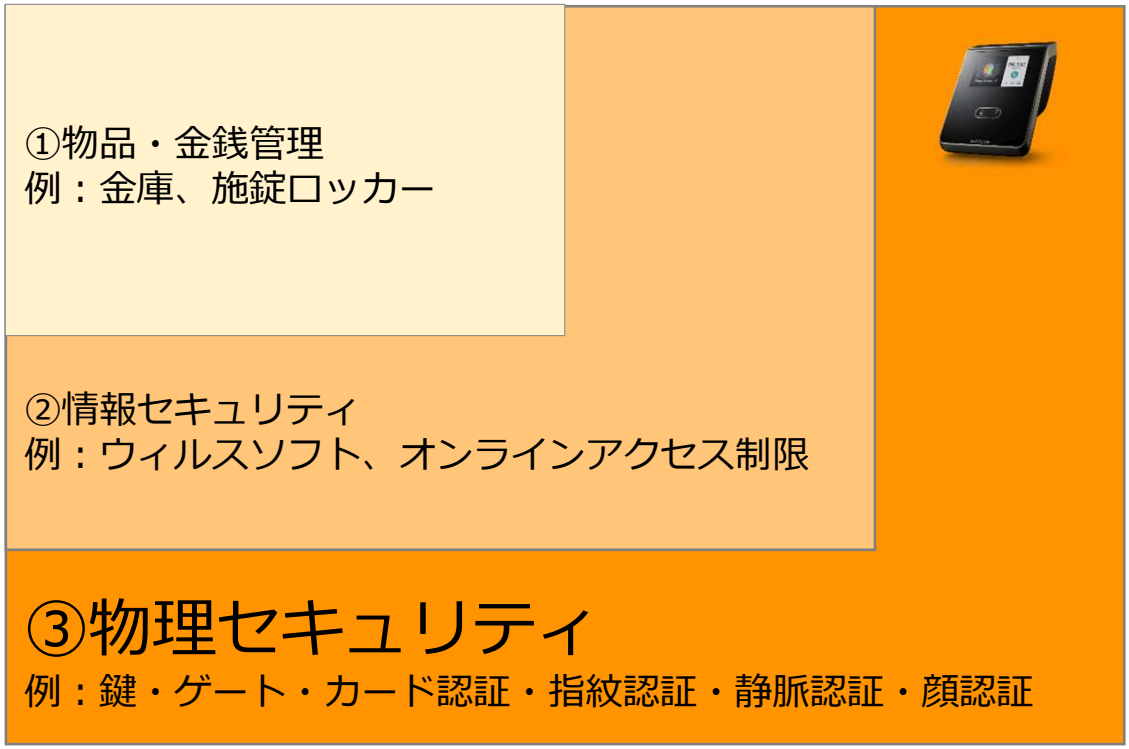


従業員数300名以上の企業からのアンケートによると
10社に1社の割合で、内部不正の経験があると回答さ
れています。この比率は増加傾向にあり、不正の内容によっては、事業の継続を困難にするケースがあります。

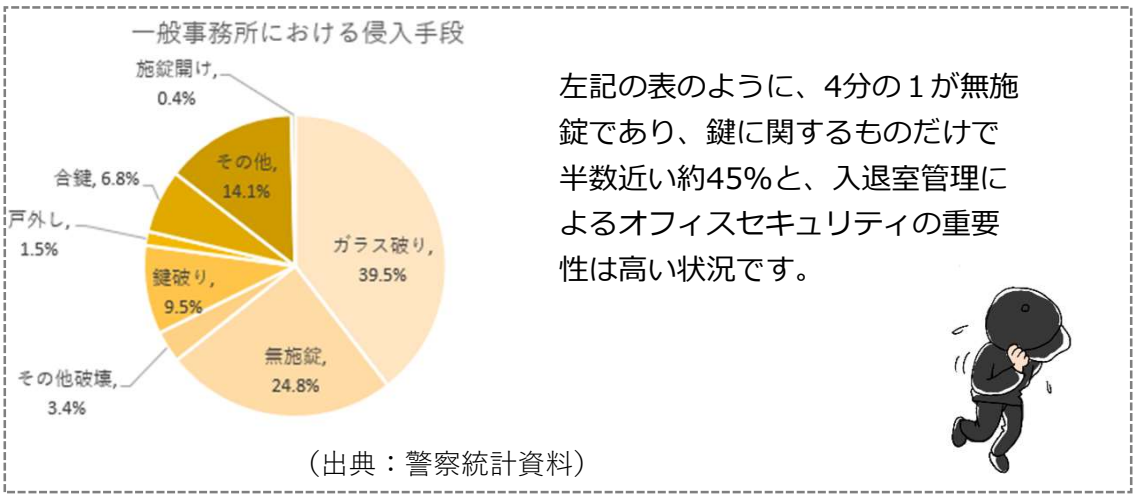
※出所：PWC『経済犯罪実態調査 』

2．オフィスセキュリティとは？

オフィスには幾つかのセキュリティ領域があります。



- 上記①、②は企業規模に関わらず浸透してきました。
  ただ③については、金融機関や大手企業では導入されていますが、昨今は犯罪の多様化により、規模に関係なく、人の出入りに関しても物理的セキュリティ対策のレベルが課題となっています。



（出典：警察統計資料）

左記の表のように、4分の１が無施錠であり、鍵に関するものだけで半数近い約45%と、入退室管理によるオフィスセキュリティの重要性は高い状況です。

3．リスクのお話

～もしオフィスセキュリティがなかったら～

その１．簡単に部外者が行き来出来てしまう。

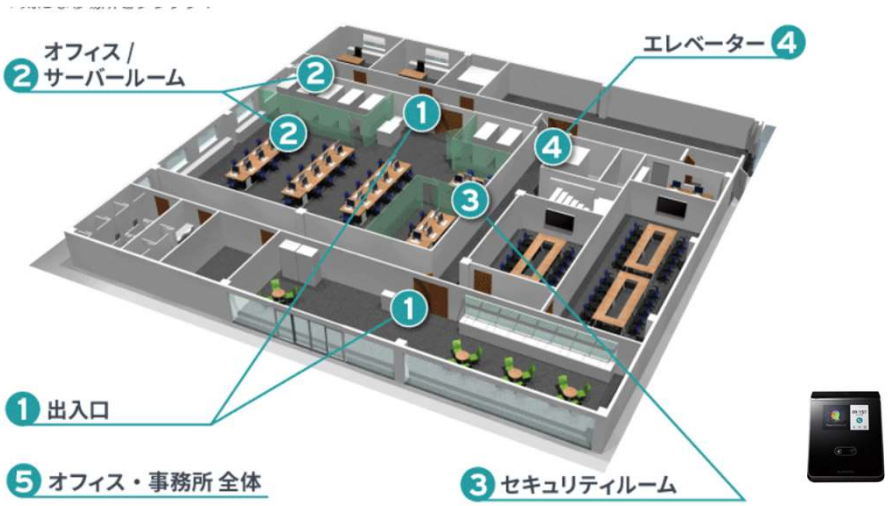
→部外者が入れてしまうことで入室者に余計な気が取られる。
→窃盗目的で侵入されてPCや物品、資料等が盗まれる。
→会社や社員に対する恨み等から事件が発生する。

その２．個人情報の持ち出された時に証拠保全が出来ない。

→いつ、誰がとうい情報が無い為に後追いが出来ない。
→カメラ等記録されるものが無いと心理的ブレーキがかからない。
→個人情報保護やPマーク維持、保持に支障をきたす恐れがある。

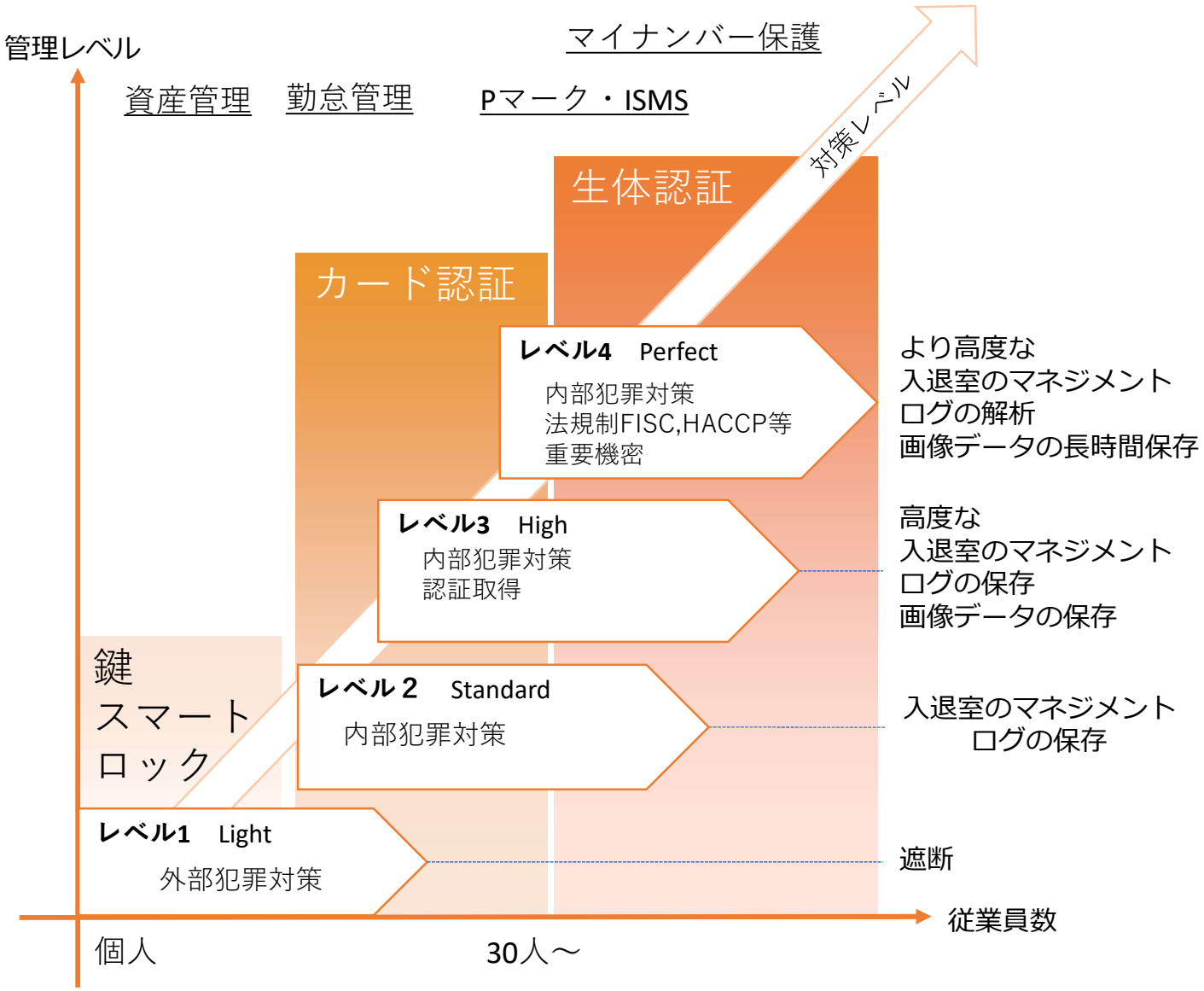
その３．アクセスレベルのコントロールが大変

→ビル共有部分、社員と入室許可された人が共有できるエリア、社員のみ、限られた社員のみが入れるエリアなどを分けて、導線まで考えると何らかセキュリティシステムが無いと管理が複雑になります。



4．アクセスレベルからみるセキュリティの選び方

ではどんな段階でどのような認証機器が必要になるかを
下の図にまとめてみました。



5.スマートロックでも大丈夫なのか？

万一外れても大丈夫な場所での使用にとどめる。

既存のサムターン鍵の上に取り付ける為、万一、外れてドアが開かない場合や電池式で電池切れの場合に、生命的な被害が出ない場所につけましょう。

メリット	デメリット
取付工事が不要な場合が多く、簡単につけられる。	取付が簡単ゆえに外れやすい。 （粘着テープ次第） 電池式の為、電池が切れると開かなくなる。
初期費用が低く抑えられる。	耐久性は元々がそれ程人の出入りが少ない扉につける想定の為、それ程高くない。 オフィスでは扉の出入りが多く、電池が消耗しやすい。 その為、電池式だと交換頻度が高くなり、交換費用がかさむことがある。ローコストが売りのスマートロックが寧ろ高くつく。

6.生体認証のメリット・デメリット

最近導入が進む顔認証や指紋認証などの生体認証は何がよくて何がデメリットかを簡単にまとめてみました。

	メリット	デメリット
全般	ICカードやテンキーによる認証方式と比べた場合、生体認証は成りすましが困難なため、セキュリティ性を高めることができます。本人の生態的な特徴によってIDの認証を行うためICカードなど物理的なID情報を携帯する必要がないため運用面、管理面での負担が軽減されます。	テンキーやカードの認証リーダーに比べてコストが高いこと、また、生体的特徴によって認証を行うため、認証精度に個人差が出る場合があります。

	メリット	デメリット
指紋認証	カードやPINコード入力を使わずに、数千人規模の運用にも対応できる。屋外での使用にも対応する。	生体認証の中では比較的個人差の影響を受けやすい。手荒れや乾燥などの要因から季節的な精度変動が起こることもある。
静脈認証	指紋認証と比べて個人差や季節による精度の差が少ない。	認証に時間がかかるため、通行量の多い場所には不適。100人を超える運用では、IDカードやPINコード入力との併用が必要となる場合がある。屋外の使用には収納ケースが必要。
顔認証	リーダーに触れずにハンズフリーでの認証が可能。認証速度も非常に速く、個人差や季節的な精度の差もほとんどない。	屋外で使用することができない。1000人を超える運用では、IDカードやPINコード入力との併用が必要。

新型コロナ対策に最適

7.テレワーク時代のセキュリティ対策

～顔認証のぞき見ブロッカー～

自宅や外出先でのテレワーク時、のぞき見防止フィルターを貼っていても、背後からは、丸見えである点はお気づきでしたでしょうか？
集中して作業をしていて背後の気配に気づかず、背後からディスプレイを除かれて個人情報や機密情報が洩れては一大事です。

「顔認証」のぞき見ブロッカーは、登録者以外の人物によるのぞき見を顔認証により検知しWindowsをロックします。登録作業者以外のパソコン操作やのぞき見を防止し情報を守ります。
また、作業者が特定のファイルにアクセスした場合、自動で監視モードを開始し、情報を保護します。作業者のパソコン操作のログ保存機能によりテレワークなどに最適です。

横からの覗き見防止フィルターと一緒にご利用頂くとより一層保護対策がとれて安心です。

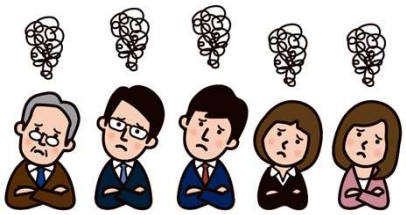
こんな使い方も！「のぞき見許可モード」
顧客にパソコン画面を見せながら説明をする時や社外でのプレゼンテーション時などに一時的な画面ロックオフモードを利用できます。一時的に画面がロックされなくなる代わりに、一定間隔で操作画面キャプチャ、パソコン前のカメラ画像をログとして保存します。

機能一覧

●作業者監視機能：登録されたユーザーが作業しているかを監視
●作業者不在判定：作業者、非登録ユーザーがどちらも検出されていない状態を異常と判断
●非登録者検知：作業者として登録されていないユーザーを検知し異常と判断
●のぞき見防止：登録ユーザと未登録ユーザが検知された場合、のぞき見と判断
●異常発生時のWindows ロック：異常状態が確定された場合、Windows をロックする
●自動開始：特定のフォルダ下のファイルへのアクセス、特定のアプリケーションの起動があった場合、自動的で監視を開始する
●イベントログの保存と閲覧：利用ログ、操作画面キャプチャ、カメラ画像をログとして保存可能

8.運用課題

導入を考えいる人達はどんな課題、どんなことをしたいと考えているのだろう？



- 部屋ごとに入室できる権限を設定したい
- 部外者の立ち入りを制限したい
- 部屋・エリアへの出入り日時を記録したい
- エリア・区画ごとにセキュリティレベルを設定したい
- 監視カメラをつけたい
- 事件・事故の証拠を残したい
- 作業内容、状況を監視したい
- どのような人物が来店（来社）されたのかを記録したい
- 従業員の不正を防止したい
- エレベーターを制御したい
- 不審者のエレベータの使用を制限したい
- ユーザーごとに行けるフロアを制限したい
- Ｐマーク、ＩＳＯ認定を取得したい
- お客様からセキュリティの強化を求められた
- 社員のモラル向上を図りたい
- セキュリティの水準が取引の条件として求められた
- セキュリティルームをつくりたい
- 個人情報の漏えいを避けたい
- マイナンバー情報の漏えいを避けたい
- 業務請負に厳格なセキュリティが条件を提示された
- 生体認証を導入したい
- なりすまし入室を防止したい
- 顔認証・指紋認証で、鍵を開けたい
- ICカードの管理、運用が煩わしい
- 部屋ごとにセキュリティレベルを変えたい
- 監視カメラで顔認証をしたい
- お得意様の来店（来社）を知りたい
- お客様
- 注意
- ピー

運用課題は色々ありますが
セキュアでは10年以上のソリューション実績からお客様の課題に対して最適なご提案をさせていただきます。

気になることがございましたら、お気軽にお問い合わせください。

導入のご相談、お見積りなど専門スタッフが丁寧に対応させて頂きます。

【お問い合わせ先】

・ホームページ

https://secureinc.co.jp/contact/

・お電話でのお問い合わせ

フリーダイヤル　0800-919-9500

（土日祝を除く平日9：30～18：00）