情報セキュリティのプロセスと導入

渡邊研究室　B4 080430093　松尾辰也

本の紹介

- 著作：独立行政法人　情報処　理推進機構セキュリティセンター
- 情報セキュリティ対策での組織体系
- 企業・学校・政府機関・団体等の情報セキュリティ担当者、責任者、部門長、経営者などを対象としている。

はじめに

- 近年の情報技術(IT)の普及により、ITの重要度と浸透度が高まる一方で、情報セキュリティ上の脅威は、サーバやコンピュータ、ネットワーク機器だけでなく、情報家電や携帯電話などの組込みソフトウェアまで普及しつつあります。
  そのため、今までよりも情報セキュリティの重要性を認識する必要性が高まっている。

- 今回は企業や団体での情報セキュリティの対策をするために、そのプロセスや導入までを説明します。

企業の実態と問題点

・実態調査、問題点

プロセス

・PDCAサイクル

・情報セキュリティマネジメントシステム(ISMS)

・リスクマネジメントシステム

導入

・セキュリティ製品とサービス

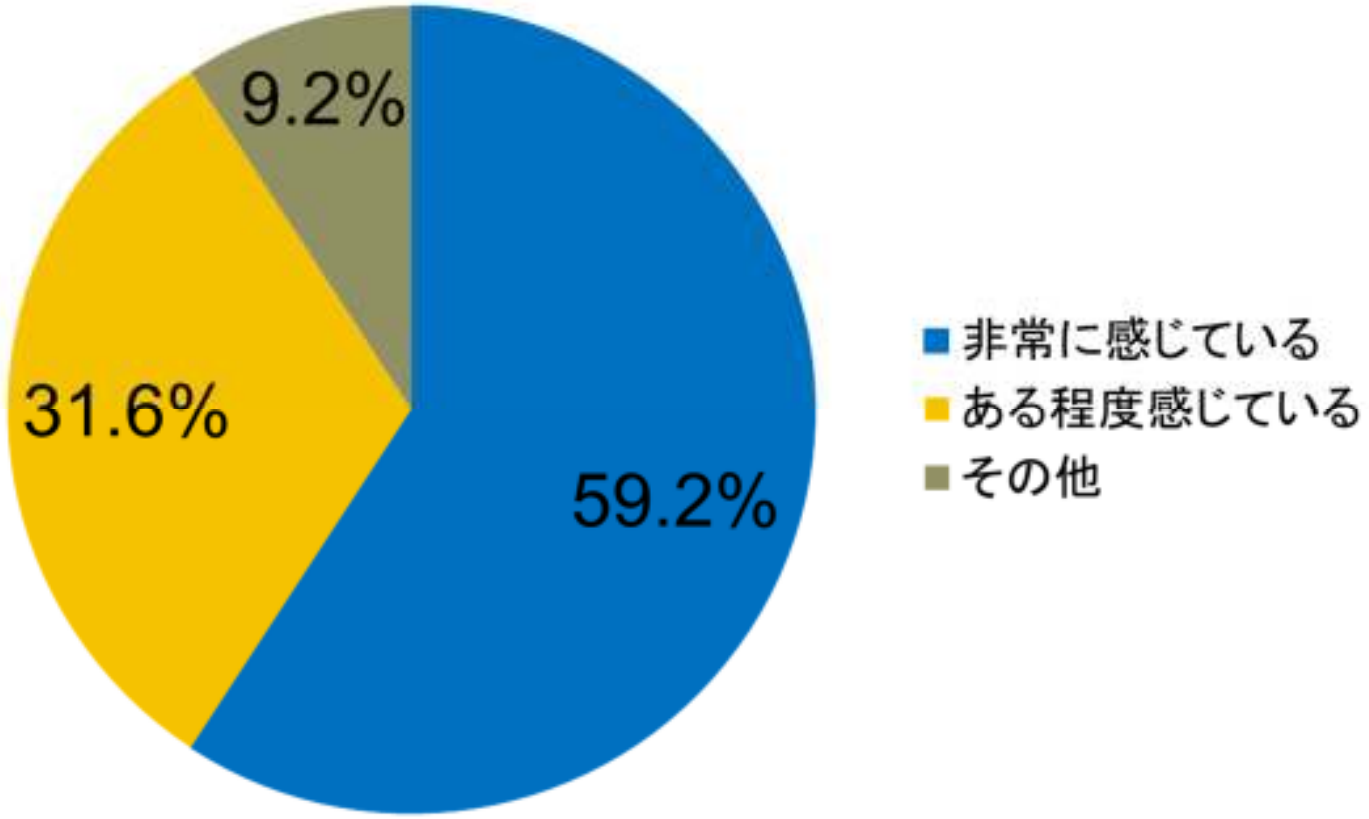
・周知やルールの徹底、管理

まとめ

企業の実態と問題点

企業に対しての実態調査（平成19年度）

Q.情報セキュリティの必要性を感じていますか？



問題点

情報セキュリティの必要性を感じている企業の中で・・・

・どこまで対策を行えればよいかわからない　→　39.3%

・費用対効果が見えない　→　37.0%

・対策を構築するノウハウが不足している　→　36.7%

・コストがかかりすぎる　→　36.2%

といった問題点を挙げる企業が多い。

ガイドライン

- 「情報セキュリティポリシーに関するガイドライン」（2000年7月策定）
  −各府省庁の情報セキュリティ対策。
  −技術的対策だけでなく管理面の対策も重要である。
  −経営層が主導し、組織全体で取り組む。→**情報セキュリティポリシーの策定**

- 「政府機関の情報セキュリティ対策のための統一基準」
  （2005年9月策定）
  −各府省庁の情報セキュリティ対策の強化。

両方とも、民間企業でも十分に活用できる。しかし、このような対策基準や手順が整備されていても、使う側がそれなりのノウハウや知識を身に付けていないと有効活用できない。

プロセス

PDCAサイクル

- Plan(計画) – Do(実行) – Check(点検) – Act(処置)の略のこと

- 情報セキュリティマネジメントシステム(ISMS)によるPDCAサイクルの場合

①Plan　:情報セキュリティポリシーの策定、情報セキュリティマネジメントシステム(ISMS)の確立を行う。

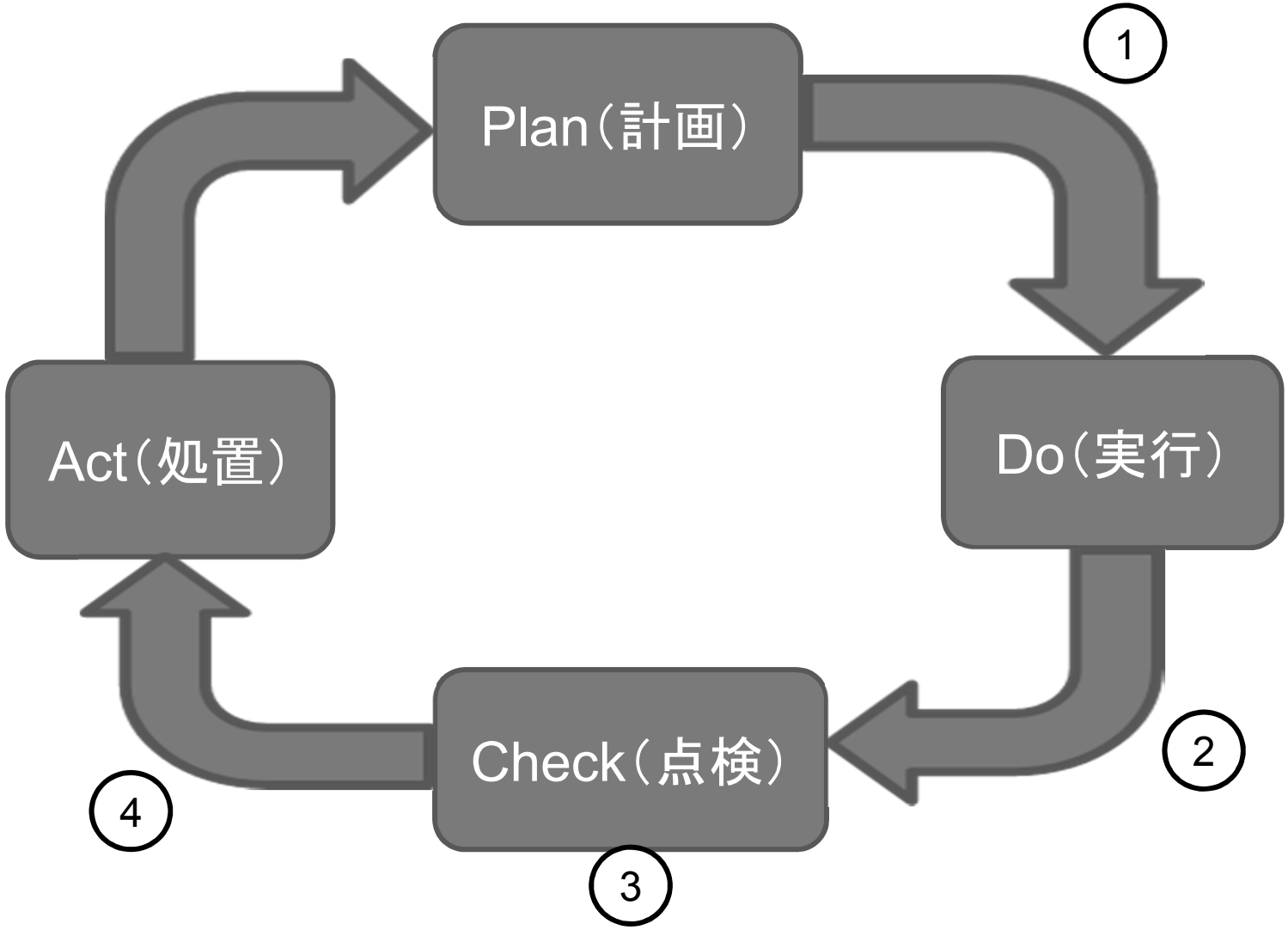
②Do　:Planで作成した対策を導入し運用する。

③Check:ISMSの監査およびレビュー

④Act　:ISMSの維持および改善

螺旋を描くように1周ごとにサイクルを向上させる。

ISMSによるPDCAサイクル



情報セキュリティマネジメントシステム（ISMS）

　情報セキュリティ確保、維持するための、技術的、物理的、人的、組織的それぞれの対策を含んだ、経営層を頂点とした組織的な取り組みのことを言う。

　現実的な対処を行えるよう、情報セキュリティを体系的かつ系統立てて揃えたものである。

例

　組織の情報資産を洗い出し、各情報資産に対するリスクを分析してリスクを軽減させ、組織のセキュリティを高める。

リスク

- リスク：一般的には予期せぬことが起きる可能性
  - 投機的リスク：投資、起業　　→損失 or 利益
  - 純粋リスク　：災害、災難、詐欺　→損失

- リスクマネジメントシステム：

リスクを管理するための活動

リスクマネジメントシステムにおける PDCAサイクル

①Plan　:リスク分析とリスク評価を行い、リスク対応策を選択し、
　　リスクマネジメントプログラム（実行計画）を策定。
②Do　　:リスクマネジメントプログラムに沿って対策を実施。
③Check:リスクマネジメントの効果を測定し、システムを評価。
④Act　:リスクマネジメントシステムに関する是正・改善。

　こうしてみてみると、リスクマネジメントプログラムは情報セキュリティ対策でいうとISMSのことなので、ISMSは情報セキュリティを対象としたリスクマネジメントシステムであるということが分かる。

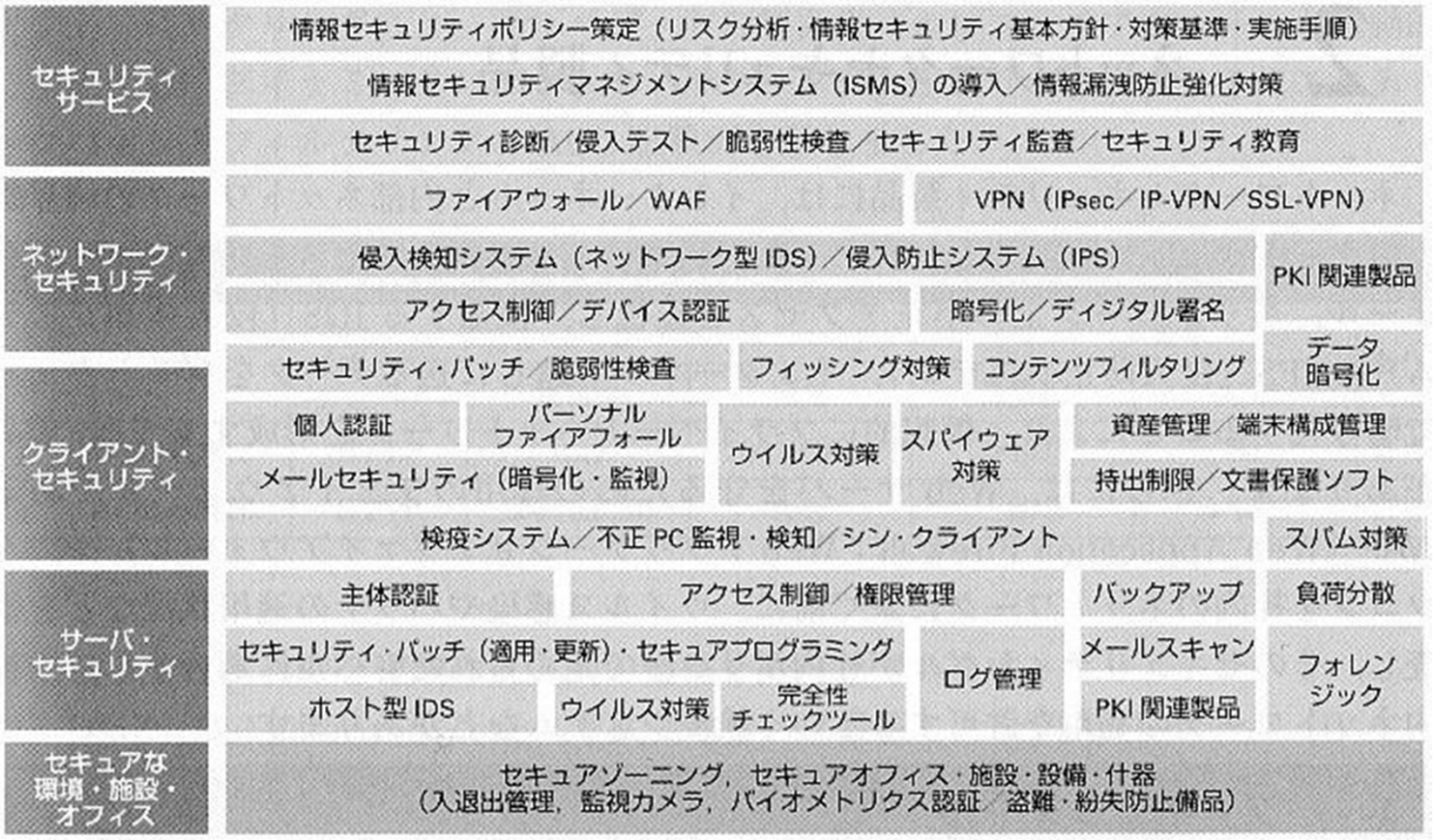
導入と運用

導入にあたって

　情報セキュリティーポリシーがあることを前提として、ルールや手順が多すぎると運用負荷が高くなり、運用自体が難しくなることがある。

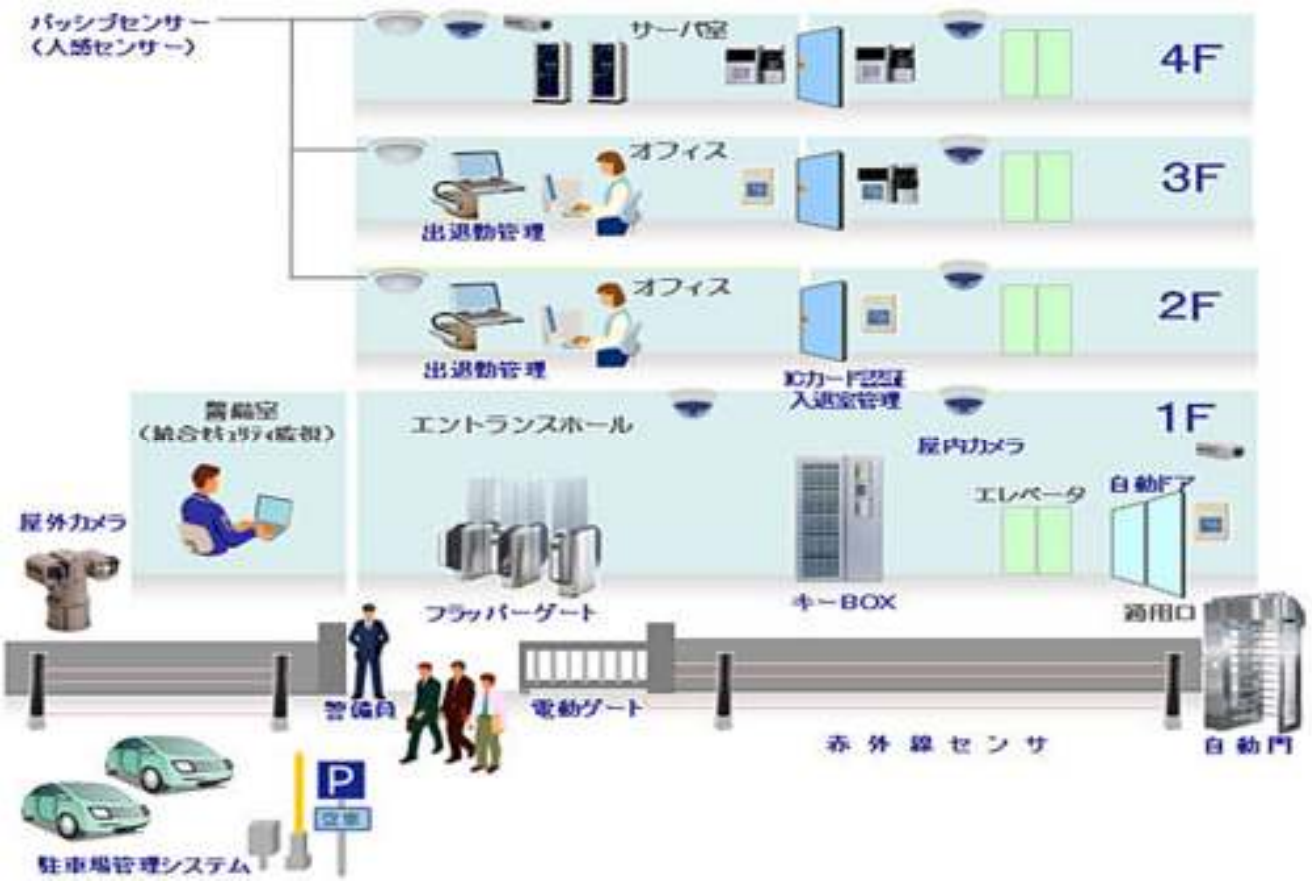
→セキュリティ製品やサービスを導入することにより、コストと運用負荷とのバランスを取ることが出来る。

セキュリティ製品とサービス



セキュリティ製品の例

・トータルセキュリティシステム（日立セキュリティサービス）



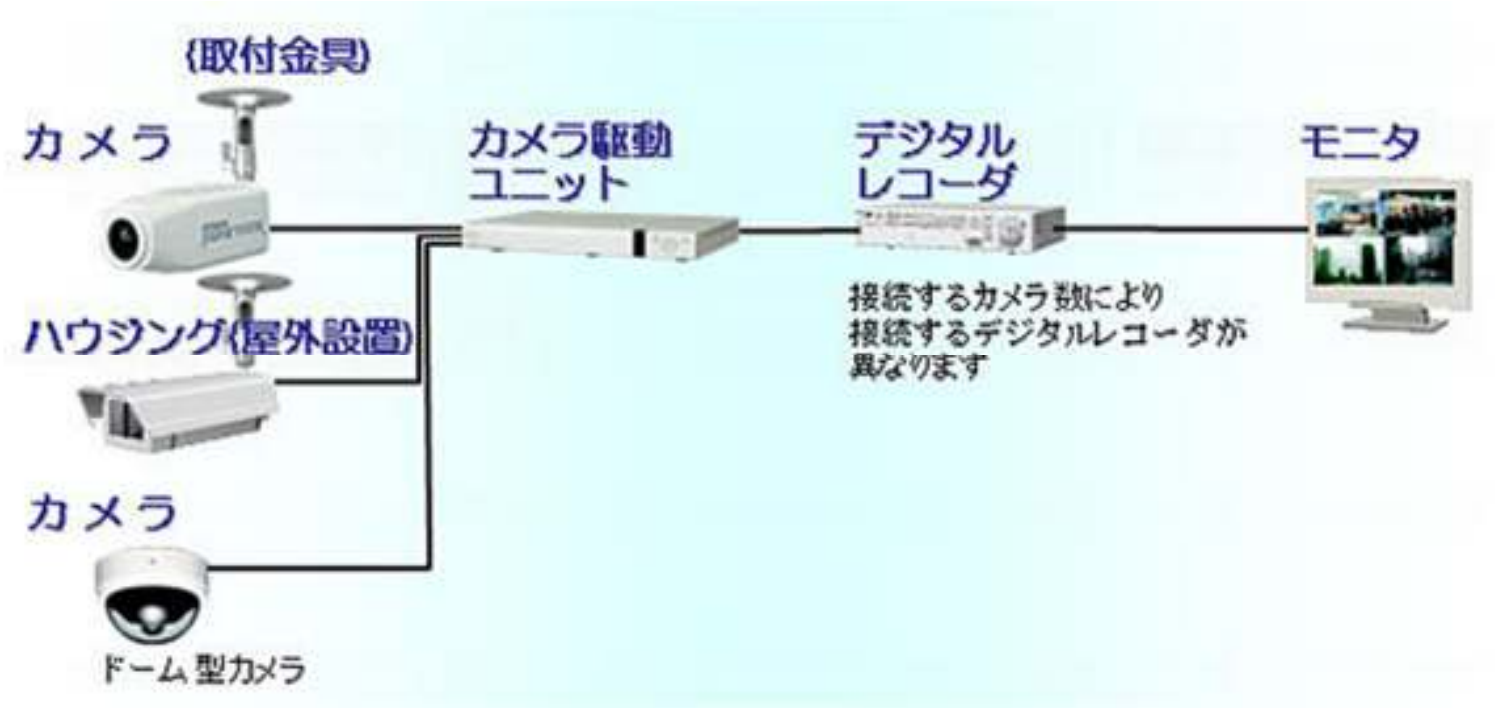
入室管理システム

- ICカードを利用した非接触読取式の入退室管理システム。
- 指静脈認証装置を組合わせることで、より高度なセキュリティを提供できる。

ICカード認証

指静脈認証＋ICカード＋テンキー

防犯カメラシステム



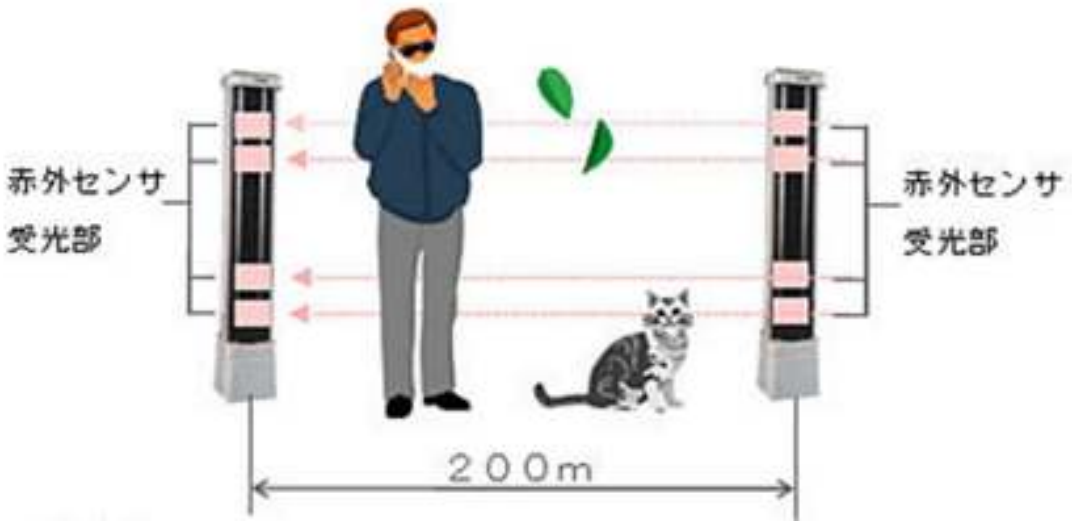
基本構成

- 遠隔操作システム
- カメラ旋回台コントロールシステム

センサシステム

- **パッシブセンサ（人感センサ）**
  人の動きなどを赤外線センサを用いて検知する。
- **境界線侵入者検知**
  ４段ビーム同時遮断方式により小動物と人間の区別が可能。

パッシブセンサ



境界線侵入者検知

鍵管理システム

- 指静脈認証により本人認証を行い、鍵の貸出、返却が行える。
- LANと接続することでき、遠隔管理が可能。

周知やルールの徹底

　前項のような製品やサービスを導入し、運用する際には、全従業員に対して周知させることが必要である。そのため、以下のような事項を行う必要がある。

- **告知**
  　対策基準を策定し、承認を受けたら、運用開始を全組織に伝えます。その際に、告知文を作成する。
- **情報セキュリティ教育**
  　組織として情報教育の責任者や担当者を定め、全従業員に漏れなく受講させる体制を整えます。そこで、情報セキュリティポリシーの周知に加え「何のために情報セキュリティ対策が必要か」ということについても教育します。

管理

- **従業員の管理**
  雇用契約、就業規則、懲戒規程の整備。雇用の終了または異動による、資産の返却や本人のアカウントの削除。
- **外部委託先の管理**
  外部委託に関する基準類の整備。委託先の監督。
- **ソフトウェア開発の委託**
  要求仕様にセキュリティに関する要求を含める。セキュリティホールを作られないように、情報セキュリティの観点からコーディング規程（プログラミングなどで使用を控える構文、使用禁止等を定めた規程）などを整備。

まとめ

- **情報セキュリティマネジメントシステム**(ISMS)を確立するために、Plan(計画)で情報セキュリティポリシーを策定してISMSを確定させ、Do(実行)で計画した対策を導入し運用する。そして、Check(点検)でISMSの監査、レビューを行い、Act(処置)でISMSの維持および改善を行う。一連の流れを**PDCAサイクル**と呼び、このサイクルを回し続けることにより、情報セキュリティ対策の向上を図る。

- セキュリティ製品やサービスは多種多様であり、コストや運用負荷とのバランスを考えて導入する。

- 運用するにあたっては、周知やルールを徹底し、従業員や外部委託先などの管理を怠らないようにする。

参考

- 情報セキュリティポリシーに関するガイドライン
  http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html
- Wikipedia
  http://ja.wikipedia.org/wiki
- 日立セキュリティサービス
  http://www.hitachi-ss.co.jp/

補足

情報セキュリティポリシー

企業などの組織における情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的にとりまとめたもの。

構成

1.情報セキュリティ基本方針

組織における、情報セキュリティ対策に対する根本的な考え方を表すものであり、組織が、どのような情報資産を、どのような脅威から、なぜ保護しなければならないのかを明らかにし、組織の情報セキュリティに対する取組み姿勢を示すもの。

2.情報セキュリティ対策基準

基本方針で定められた情報セキュリティを確保するために遵守すべき行為や判断などの基準。つまり基本方針を実現するために何をしなければいけないかを示すもの。

PDCAサイクルの他の例

Plan

東大合格という目標を立てる。
行くべき予備校を決める。
勉強方法を決める（毎日10時間勉強とか）

Do

実際に勉強してみる
模試などを受けて結果を見てみる

Check

模試などの結果をみてみる
本当に東大に行く学力があるかみてみる
苦手な科目はないか確認してみる

Act

勉強方法を再確認する
苦手科目を補う勉強方法を考える

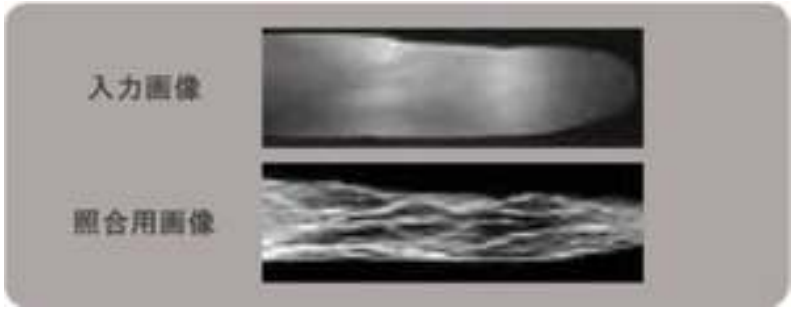
Plan

東大が身の丈に合っているか再確認
場合によっては志望校を変える
場合によっては予備校を変える
場合によっては勉強法を変える（20時間勉強とか）

生体認証

- **指紋**：犯罪捜査にも用いられ、手軽だが信頼性の高い認証方式である。また、生体認証としては古参の部類に入るため欺瞞の方法も数多く編み出されている。

- **指静脈**：日立が開発した認証方法で、近赤外線LEDによる透過光撮影方式により皮膚の表面（しわ、手相、指紋）が写りにくく、高コントラストな画像静脈パターンを抽出できるので、偽造が極めて困難です。



コーディング

コーディング：ソフトウェアの設計図にあたるソースコードを作成すること。「プログラミング」とほぼ同義