安全宣言はいらない
説明責任をください

あぶないと市長のきみが
いったから８月２日は
不参加記念日

あきら

「やっぱり危ない 住基ネット」集会
2006年8月2日（水）
於：かながわ県民センター
西邑 亨

このスライドの
「セキュリティー」
ということばは、みんな
「プライバシー」
におきかえることができます

例外：「プライバシー基準」ということばは使いません。
プライバシーの基準は自分の内部にあるもので、誰かが決めてくれるものじゃないからです

「具体的危険」は危険ではない（？）

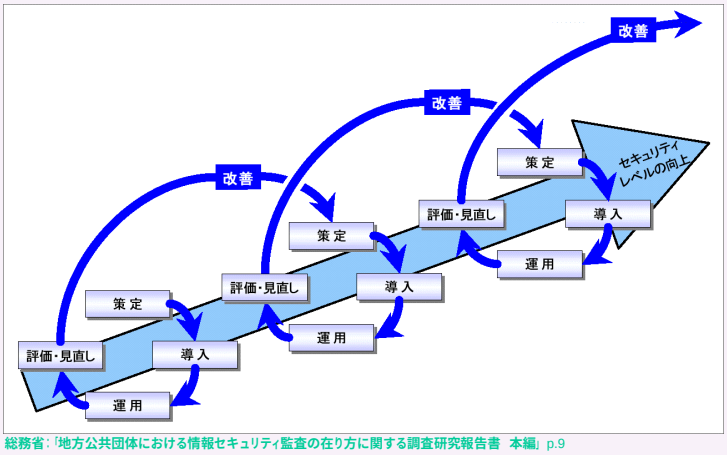
- 各地の住基ネット差止訴訟の中で、「具体的危険」の事例がたくさん立証されてきました
- でも、それらのほとんどは、判決によって「具体的危険ではない」と認定されました
  - ただちに改善された
  - 多重化された他の対策によってカバーできている
  - 他の自治体の危険は、抽象的危険に過ぎない
  - 「抽象的危険」は、システムの差止や損害賠償の要件ではない（訴状では「システムを止めろ」とは言ってないのだけど……）
- 「認知された危険」は排除することができるが、「認知されていない危険」があることに、日本の法制度は対応していない（近代国家がかかえている困難な問題のひとつ）

日本政府のセキュリティ対策基本方針 ―「走りながら考える」

- 行政システムのセキュリティ対策は、当初「ほぼゼロ」だった
- とりあえず適当な（すぐに実現できるはずの）「セキュリティ基準」（制度）を作った
- 後は時間をかけて少しずつ「セキュリティ強度を高めていけばいい」ということにした

- ここには、「必要な水準」という概念がない

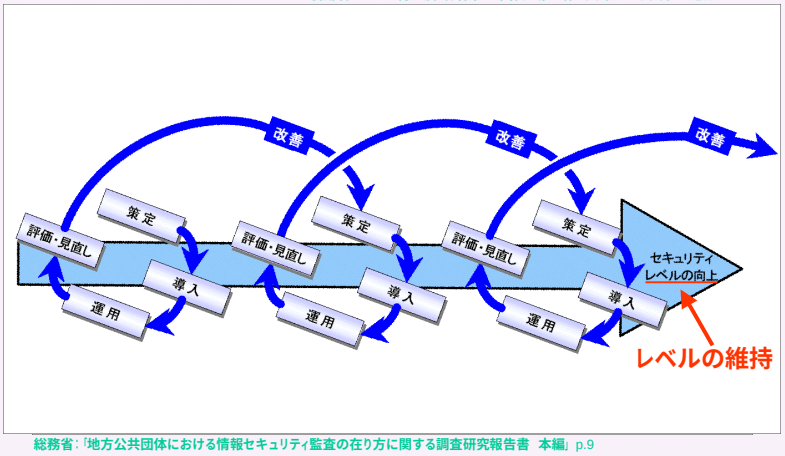
PDCAサイクル



総務省:「地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書　本編」p.9

PDCAサイクル

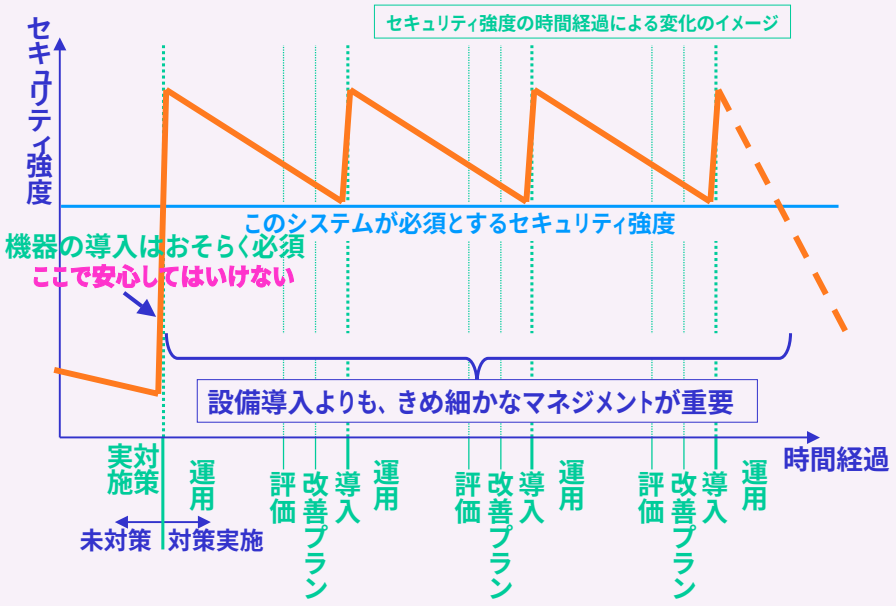
イラストは、引用者によって約20度時計回りに回転し赤い線と矢印および文字が追加されている



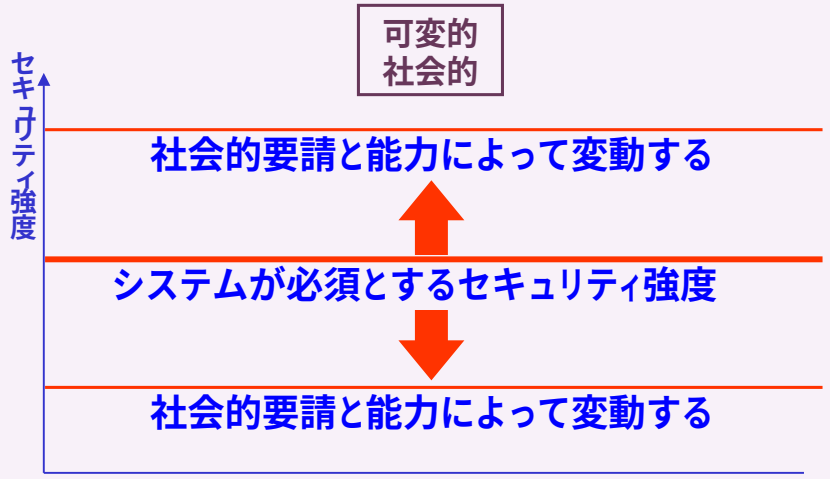
総務省:「地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書　本編」p.9

このイラストでは「レベルの向上」となっているが
システムを取り巻くさまざまな環境は変化し、また対策はほころびをかぶるので
実際には「**レベルの維持**」となる (**矢印は水平**)

PDCAサイクル



必須のセキュリティ強度ってどうなってるの？



必須のセキュリティ強度ってどうなってるの？

可変的
社会的

セキュリティ強度

- システムベンダーが提案する強度？
- 技術者が必要だろうと考えている強度？
- 横浜市の「不参加」市民が求めている強度？
- 国の制度･基準が想定している強度？
- お金のない自治体の実際の強度？

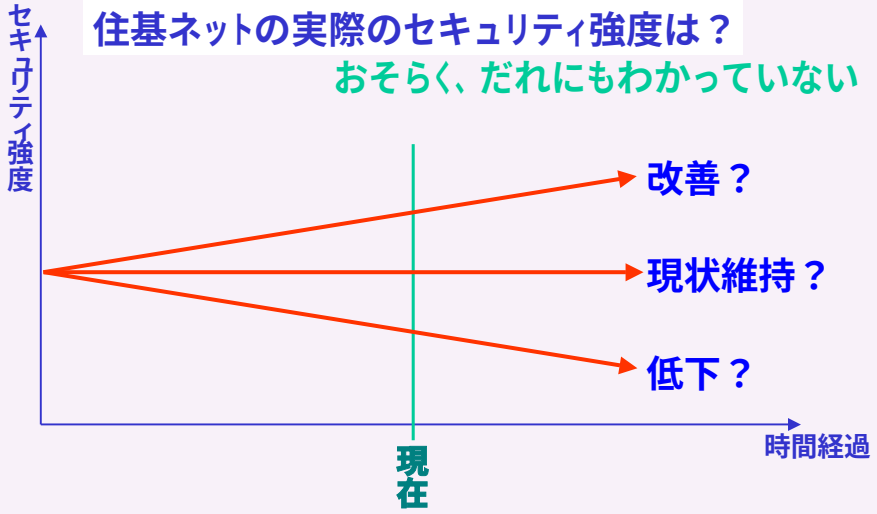
これらの違いを相互に理解し、調整し、現実的なセキュリティ強度として合意形成する社会的機能が存在しない

あぶないと
きみはいった

それで、セキュリティ強度は改善されたのか？

住基ネットの実際のセキュリティ強度は？

おそらく、だれにもわかっていない



- 正確に評価（測定）されていない
- 評価の基準がよくわかってない

セキュリティ強度の評価基準

＜定性的強度を表すことば：安全／危険＞

- 安全
  - 総合的に見て安全
  - 具体的危険がない
  - 危険の可能性（抽象的危険）
  - 具体的危険がある
- 危険

境界はない

- 「どのような制度にも抽象的危険はある」（名古屋判決）
- どのようなシステムにも抽象的危険は常にある

セキュリティ強度の評価基準

＜実用的な定量的セキュリティ強度の単位＞

- 「システム侵入」や「情報窃取」に必要な**「時間」**
  ただし
  - セキュリティ強度はシステムの部分ごとに異なる
    - 全国センター・各都道府県センター・各自治体・各政府機関など
  - 全体の強度は、もっとも弱い部分の強度で評価する

- 通常この「時間」は
  - 時間・日・月の単位で測定される（侵入実験など）
  - 「安全な暗号」は、「年」を単位として考えられている

この評価基準は、「セキュリティは、かならず破ることができる」ことを基礎としている

セキュリティ強度の評価基準

＜セキュリティ強度の社会的・制度的基準＞

「情報セキュリティ・マネジメント」では、社会的な「制度」の制定とその実施状況によって、5段階に分けている

1. 情報セキュリティポリシーが策定されている
2. ポリシーの実施手順が決められている
3. 決められた手順が実施されている
4. 手順の実施をきちんとモニターしている
5. 環境が変化してもタイムリーに対応できる仕組みがある

総務省住基ネット調査委員会第10回議事録p.33 松尾委員の発言を参照して、西邑が整理
http://www.soumu.go.jp/c-gyousei/daityo/juki_system.html

社会的要請と能力によって、「ポリシー」の内容が決まる。
そこでは「時間」単位の定量的な評価ができる「対策」が策定されている

安全宣言は
いらない

「横浜方式」が約束したこと

- 市民の個人情報の安全に関する、首長の「説明責任」を履行するために「横浜方式」を採用する
- 「横浜方式」は、一定の安全が確認できたときに「全員参加」することを前提とする
- 「安全の確認」は市長の判断で行う

「安全の確認」について、中田市長は「説明責任」の履行を約束している。

「説明責任」の履行とは、少なくとも判断の具体的根拠を、明示的・論理的に示し、理性的な批判を受け入れること

説明責任を
ください

このスライドの
「セキュリティー」
ということばは、みんな
「プライバシー」
におきかえることができます

例外：「プライバシー基準」ということばは使いません。プライバシーの基準は自分の内部にあるもので、誰かが決めてくれるものじゃないからです

Cyber Human Rights Workshop Office 情報人権ワークショップ事務局

illustration：masanao nakajima（http://bw-house.com/）