兵庫県における
リスクマネジメント手法について

2006年 7月7日・14日

兵庫県企画管理部
教育･情報局自治情報課
津川誠司

Hyogo Prefectural Government

県庁WANのリスク分析

－内部統制手法－

兵庫県の情報インフラ

兵庫情報ハイウェイ

兵庫県の情報基盤
28アクセスポイント

兵庫県庁WAN

兵庫県行政の情報基盤
情報ハイウェイ上に構築
323の県機関を接続

Hyogo Prefectural Government

リスク分析の手法

※ISMS2.0を基本とした

１　リスク値の算出

資産価値　×　脅威　×　脆弱性

２　許容値の設定

３　詳細リスク分析　　※改善点

４　リスクマネジメント

情報資産の分類

・個人情報や行政情報等は、通常、データ化され、使用される。
・そのため、情報資産を情報機器でグループ化して評価した。
・グループ化により、短時間で網羅的なリスク分析とが実施可能。

情報資産	台数	システム	評価値	被害の影響
中枢サーバ	42	Ｗｅｂ,SMTP,DNSサーバ	４	深刻
管理サーバ	22	ログイン，ＤＨＣＰ等の管理用サーバ	３	重大
業務サーバ	108	各課で導入した業務用サーバ、プロクシ	２	部分的
職員端末	13000	職員の使用する端末	１	個人的

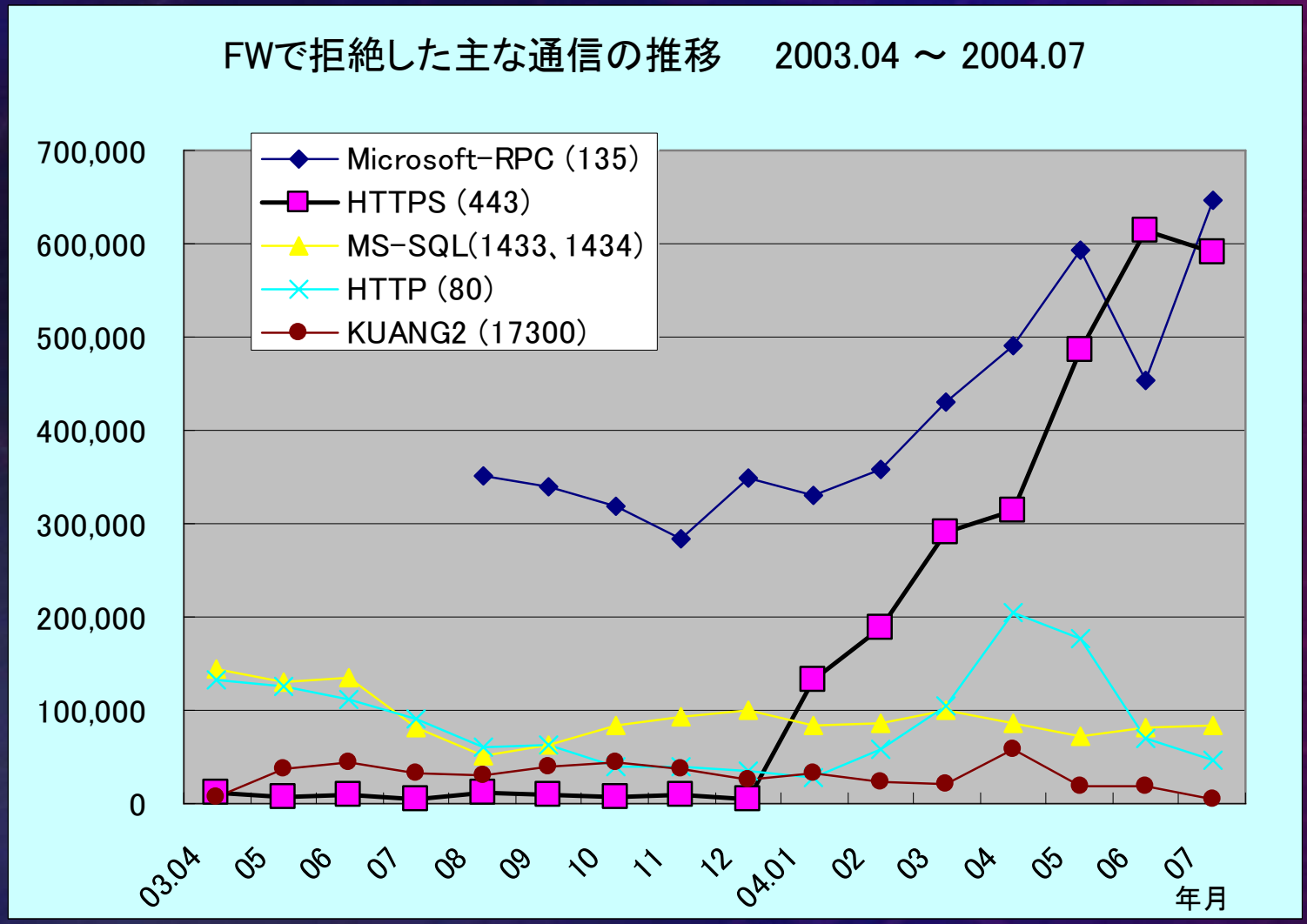
脅威の分析

脅威の種類、調査方法

分類	説　明	調査方法
物理的脅威	水害、火災、侵入、破壊、故障、停電、災害等	現地調査 システム調査票
技術的脅威	（種類） １　不正アクセス ２　ウィルス ３　破壊行為、DOS攻撃	侵入テスト
人的脅威	誤操作、持出し、不正行為、パスワードの不適切管理等	職員アンケート 契約内容のチェック

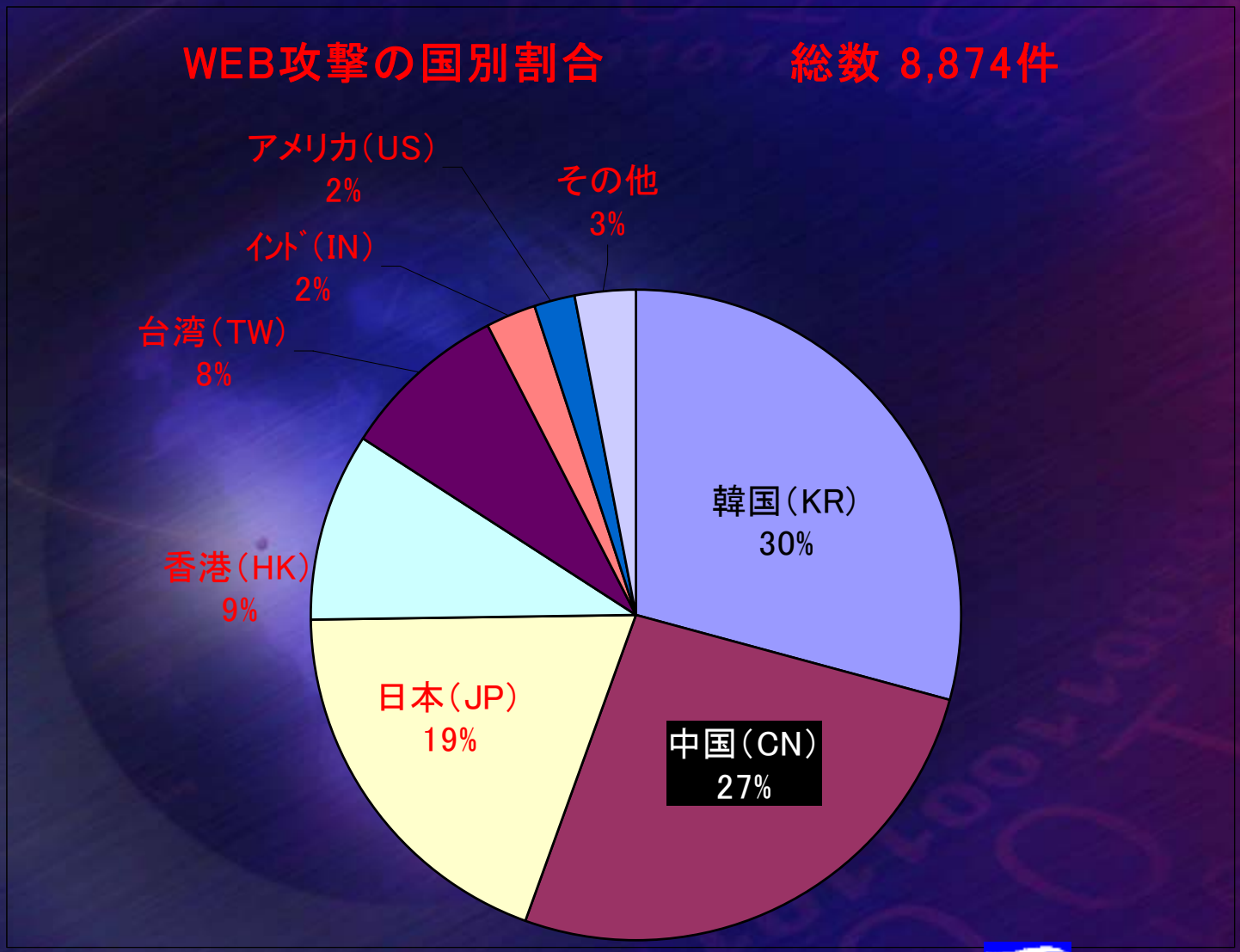
インターネットからの攻撃の分析

ワームとWEB攻撃が多い



WEBへの攻撃

アジアからの攻撃が多い



県庁WANの情報資産と脅威

323拠点（161庁舎　162校）

接続機器数は約15,000台

※　資産3，4間の攻撃の可能性で評価

脆弱性の分析

侵入テストの実施

- セキュリティスキャナ、UGツールの使用
  全機器（15000台）への侵入テスト
- 天才的なハッカーによる侵入は非現実的
- UG（アンダーグラウンド）サイトで仕入れた
  セキュリティホール情報をもとにアタックする。
- UGサイトの例

Packet Storm : http://packetstormsecurity.nl/
RootShell : http://www.rootshell.com

侵入テストの手法

手法	コマンド、ツール等
① ポートスキャン	nmap
② セキュリティスキャナ	Internet Security Scanner Nessus Shadow Security Scanner
③　ＵＮＩＸ系サーバ	fingerコマンド rusersコマンド smtpコマンド　　expn ユーザID popコマンド
④　Windows系サーバ	Null Session　　ntis422 共有フォルダの脆弱性　　Legion Ver.2.1
⑤　パスワードの検出	brute force attack Joe Account ID=Password popサーバを使う方法 John the Ripper
⑥　exploitプログラム	バグを利用し、管理者権限（root）を手に入れるツール。

侵入テスト用ツールの開発

例　Notesのパスワードクラッカーの作成

Undergroundの情報をもとに、notesのuser.idのパスワード・クラックツール（辞書使用可能）
すべてのuser.idに対し、Joeユーザ（IDとPasswordが同じユーザ）との脆弱なパスワード（hyogo, 111等）をチェック

Notescrackの使用法 1　　引数

```
>C:¥lotus¥notes¥notescrack
Notes User.id Crack  v1.0.0 by <S.Kuroda>                    >
-----------------------------------------------------------------
 notescrack [options]
            -u*     <idpathfile> IDファイルを記述したファイル名
            -p*     <dicfile> 辞書ファイル名
            -o      <logfile>
            -r      リバースの辞書解析
            -h      ヘルプ
```

Notescrackによるパスワード解析の実行

```
C:¥lotus¥notes > notescrack -u c:¥__note16¥usr¥usr.txt -p c:¥__note16¥usr¥dic1.txt
解析しています　...
スペースキーで統計出力、qで終了します
ID: c:¥__note16¥usr¥m041500¥user.id
Password: m041500
--------------------
ID: c:¥__note16¥usr¥s311400¥user.id
Password: s311400
--------------------
合計件数　4134 in 5.55 seconds
所要時間(秒)　　= 745.27
```

QNDの活用

➡ リモートコントロールの実施

323拠点　兵庫県の地域特性で現地解決は困難

➡ ソフトウェア資産の管理

・ソフトのインストールは許可制
・インベントリを利用して状況調査
（違法コピーしたソフト、Winny等の導入阻止）

➡ バージョンアップ、パッチ適用

・小容量のパッチ
県庁WAN上でQNDエージェントを配布
・大容量のパッチ（ WindowsのSP等）
CD-RでQNDエージェントを配布

QNDの選定理由

※H13に採用

➡ 操作性

・リモート機能が使いやすいこと
・他のアプリケーションと衝突しないこと

➡ 安全性

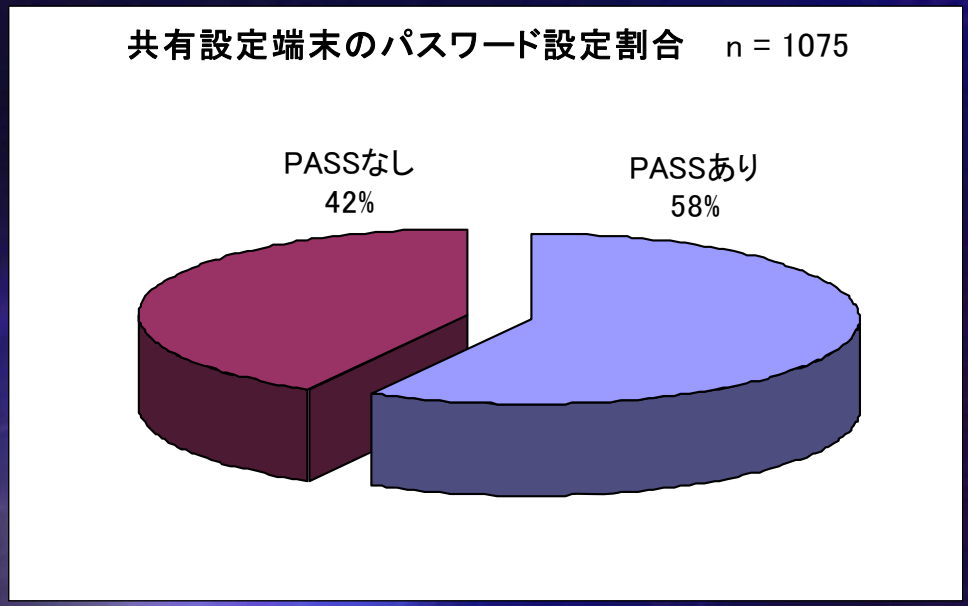
・一般ユーザが簡単に入手できないこと
（侵入手口を探り出す危険性がある）
・Well-Known Portは使用しないこと

➡ 費用対効果

過度なライセンス管理機能は不要

職員端末（資産4）におけるリスク事例

共有フォルダの脆弱性



共有フォルダを調査するツールにより調査した。
　共有設定を行っている端末1075台を検出し、調査した。
　　→　脆弱な共有フォルダを持つ端末が42% 16年度(60%)
　毎年監査・改善措置を実施しているのにもかかわらず、翌年には多く発見されている。
　　→　共有フォルダの禁止、ファイルサーバの導入等を検討する。

※　脆弱なユーザアカウント（Nullパスワード、Joeアカウント）はシステム上不可

許容値の設定

		中枢ｻｰﾊﾞ	管理ｻｰﾊﾞ	業務ｻｰﾊﾞ	職員端末
脅威	不正アクセス	4	3	3	2
	ウイルス	4	4	4	3
	DOS攻撃	3	2	2	1
脆弱性		各情報資産、各脅威　すべて許容値は　2			

詳細リスク分析

① 情報資産別・脅威別のリスク値の算出

リスク値 ＝ 脅威値 × 脆弱値

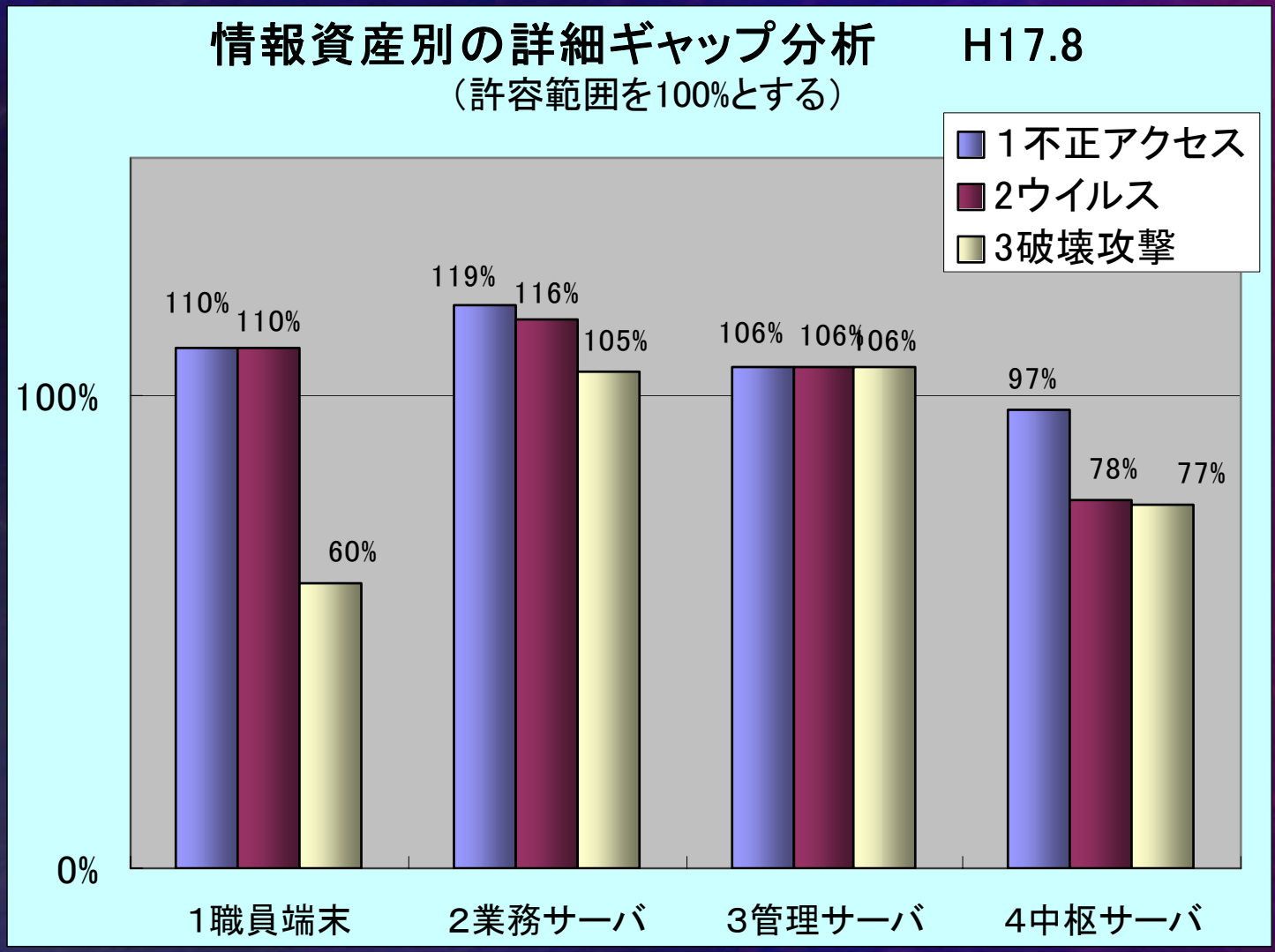
② 情報資産別・脅威別の許容値計の算出

許容値計 ＝ 脅威許容値 × 脆弱性許容値

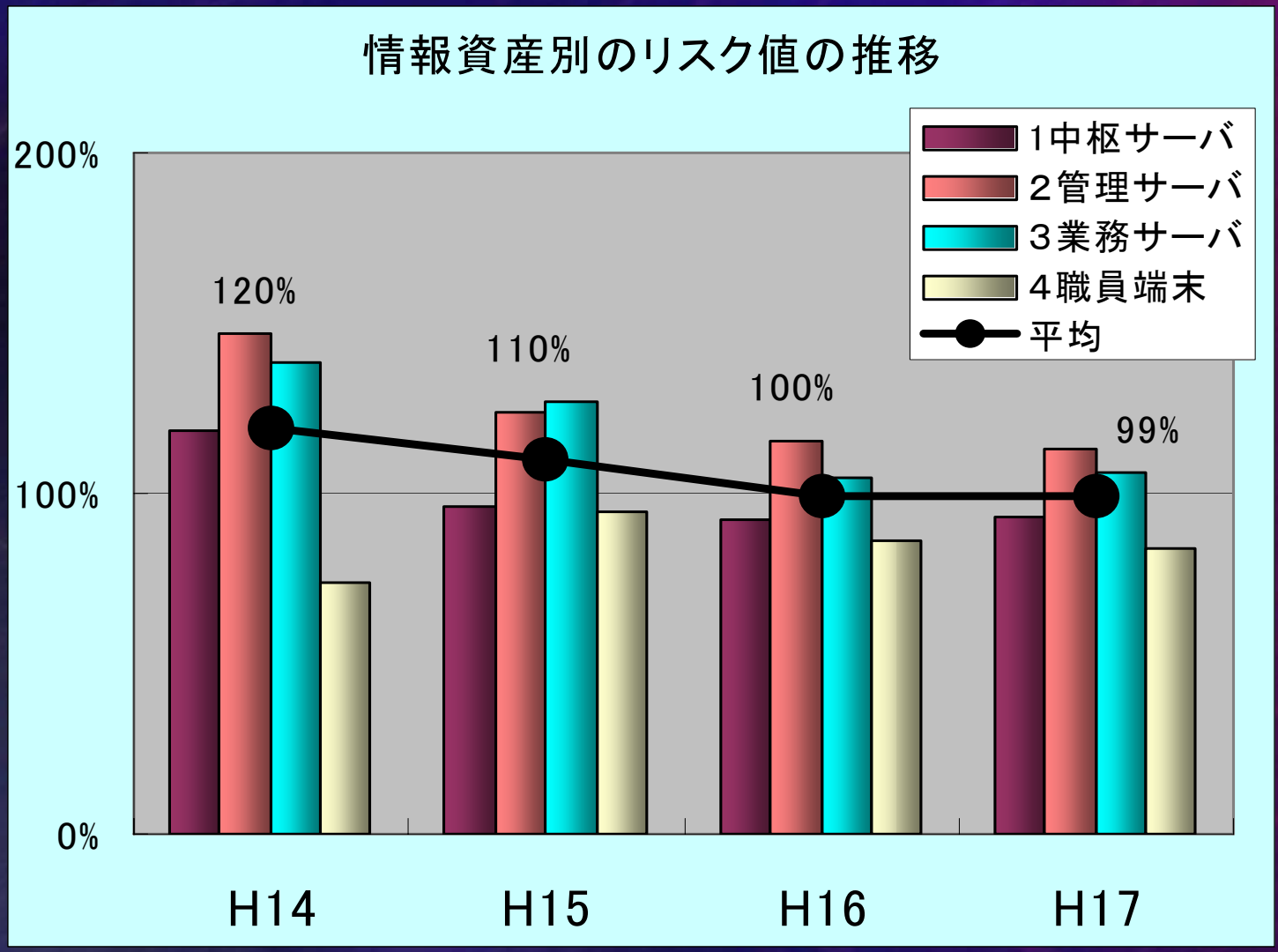
③ 情報資産別・脅威別のギャップ値の算出

ギャップ値（%）＝　リスク値　÷　許容値計

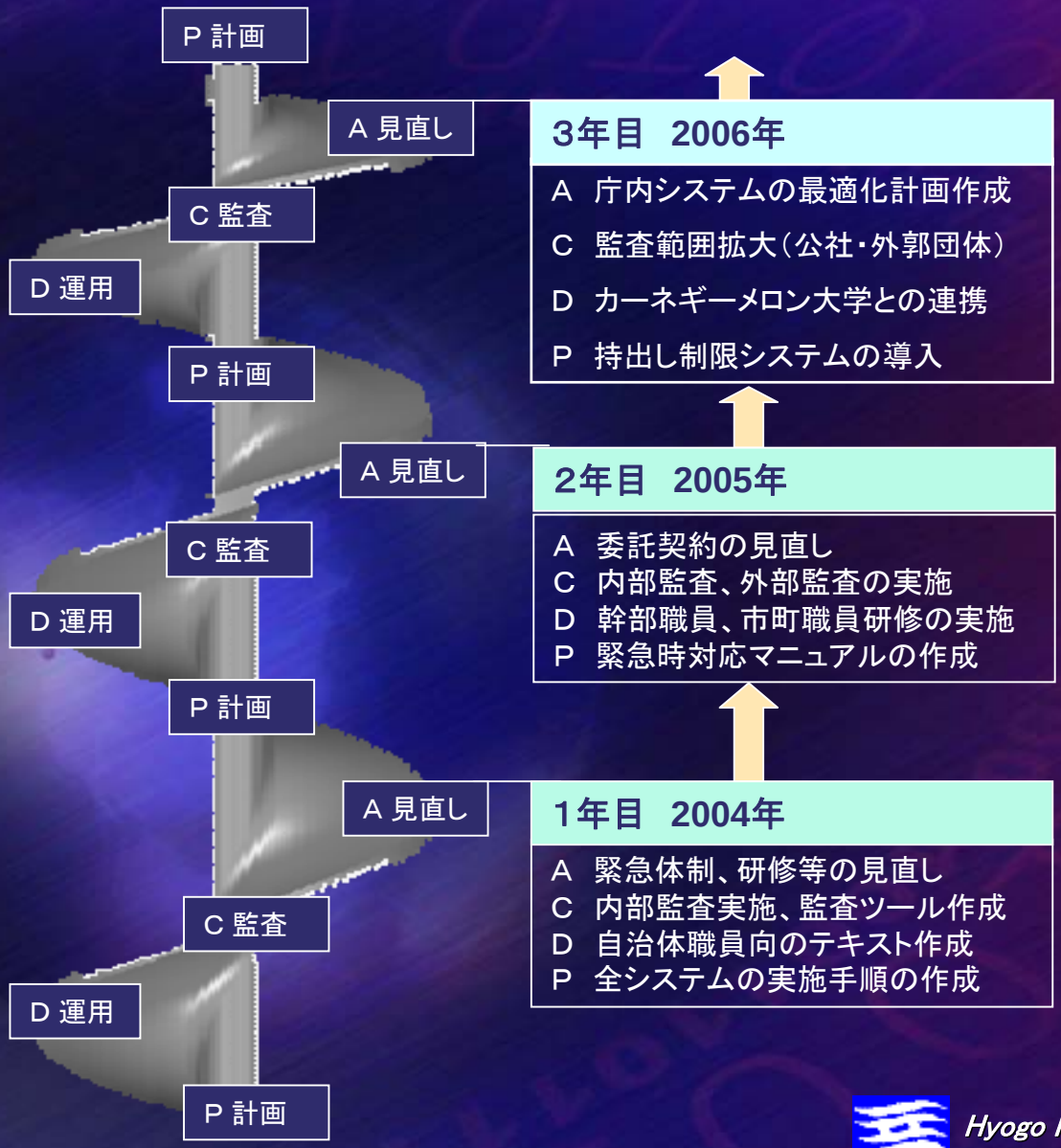
詳細ギャップ分析


情報資産別の詳細ギャップ分析　H17.8
（許容範囲を100%とする）
1不正アクセス
2ウイルス
3破壊攻撃
100%
0%
110%
110%
60%
119%
116%
105%
106%
106%
106%
97%
78%
77%
1職員端末
2業務サーバ
3管理サーバ
4中枢サーバ

情報資産別のリスク値の推移

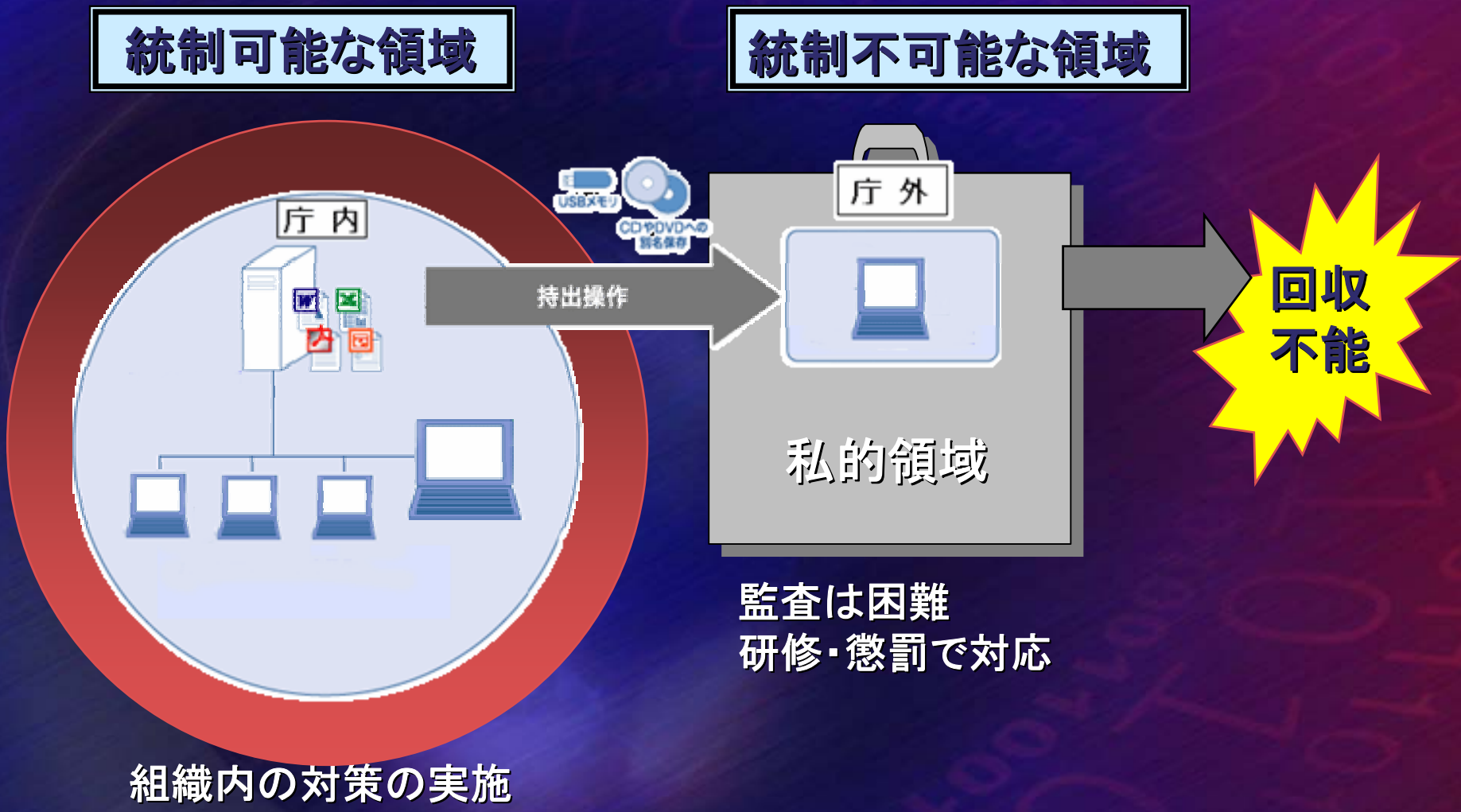


マネジメントサイクルの確立



脅威の変容と内部統制の改善

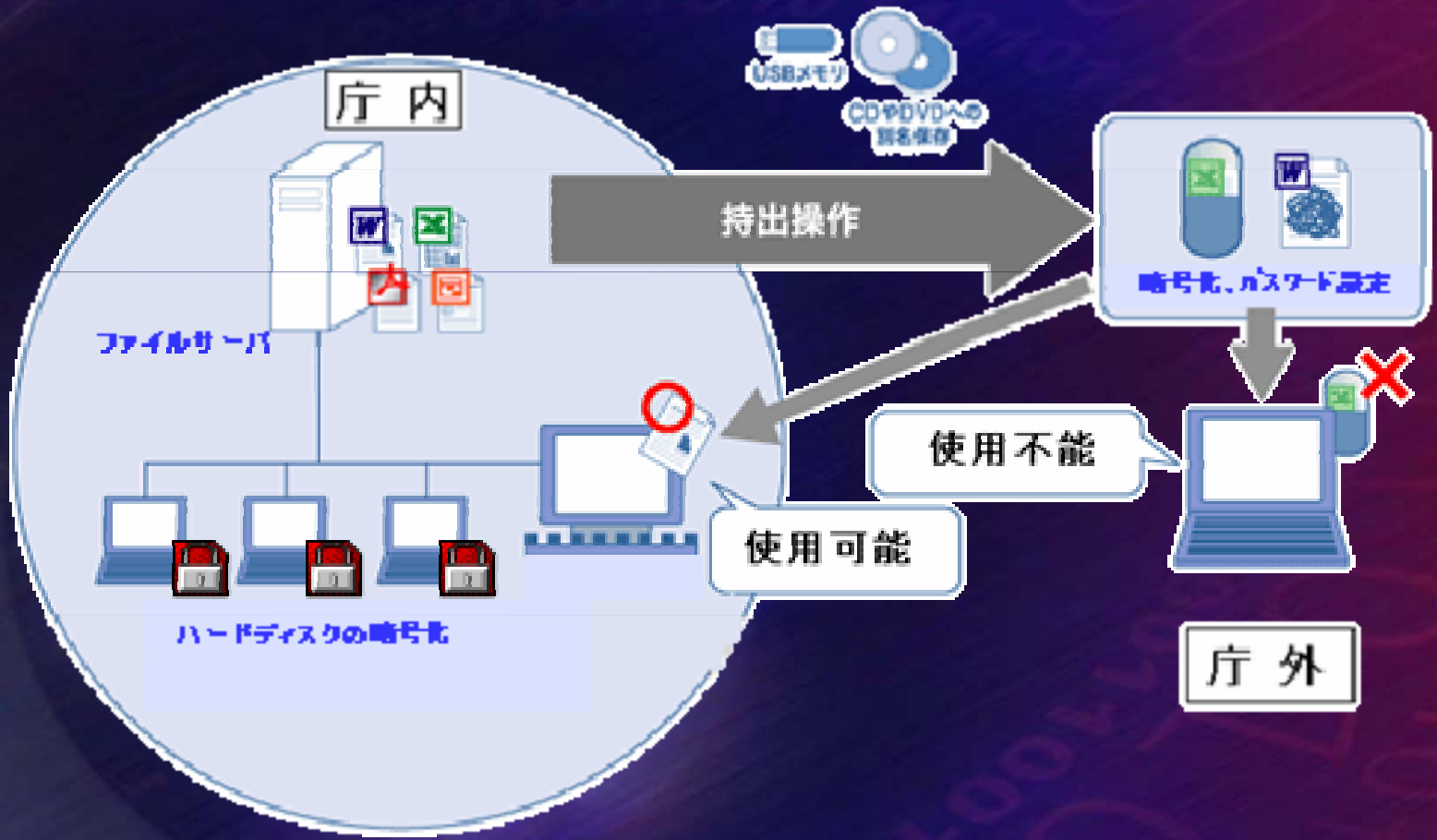
脅威の変容　→ 持出しによる漏えいの増加



組織内の対策の実施

監査は困難
研修・懲罰で対応

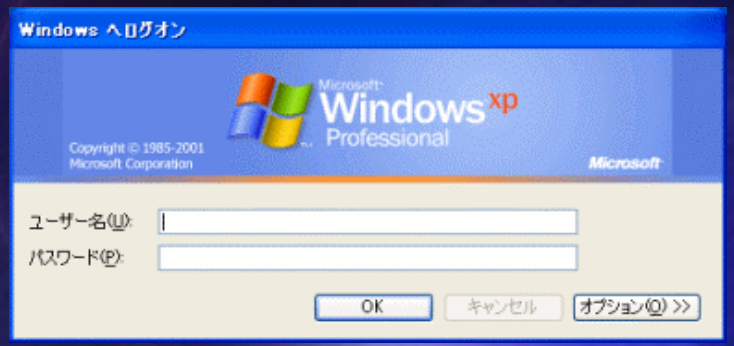
技術的対策　案1
情報漏えい対策ソフトの導入を検討



技術的対策　案2
ICカードによる職員認証の導入を検討

現在のWindowsログオン

ユーザID（職員番号）とパスワードの入力のみ

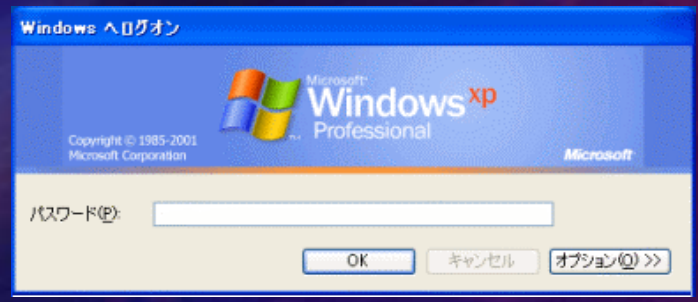


ICカードを使ったWindowsログオン

①カードをパソコンにかざす

（イメージ図）

②ICカードのパスワード（PINコード）を入力



人的対策（実施中）　カーネギーメロン大学日本校との連携

1900年、鉄鋼王のAndrew Carnegie により、米国ペンシルベニア州ピッツバーグ市に、カーネギー工科大学として設立。その後、金融のメロン財閥により設立されたメロン大学と合併してカーネギーメロン大学となり、技術分野では全米をリードする存在

大学院の全米ランキング（抜粋）

- コンピュータ科学　（1位）
- 情報公共政策管理学（1位）

（出典：U.S NEWS & WORLD REPORT America's Best Graduate Schools 2006 ）

○情報セキュリティ参与の派遣

○兵庫県からの学生派遣

CMU日本校の教育

- 学位：カーネギーメロン大学修士
（情報技術ー情報セキュリティ）
Master of Science in Information Technology – Information Security（MSIT-IS）

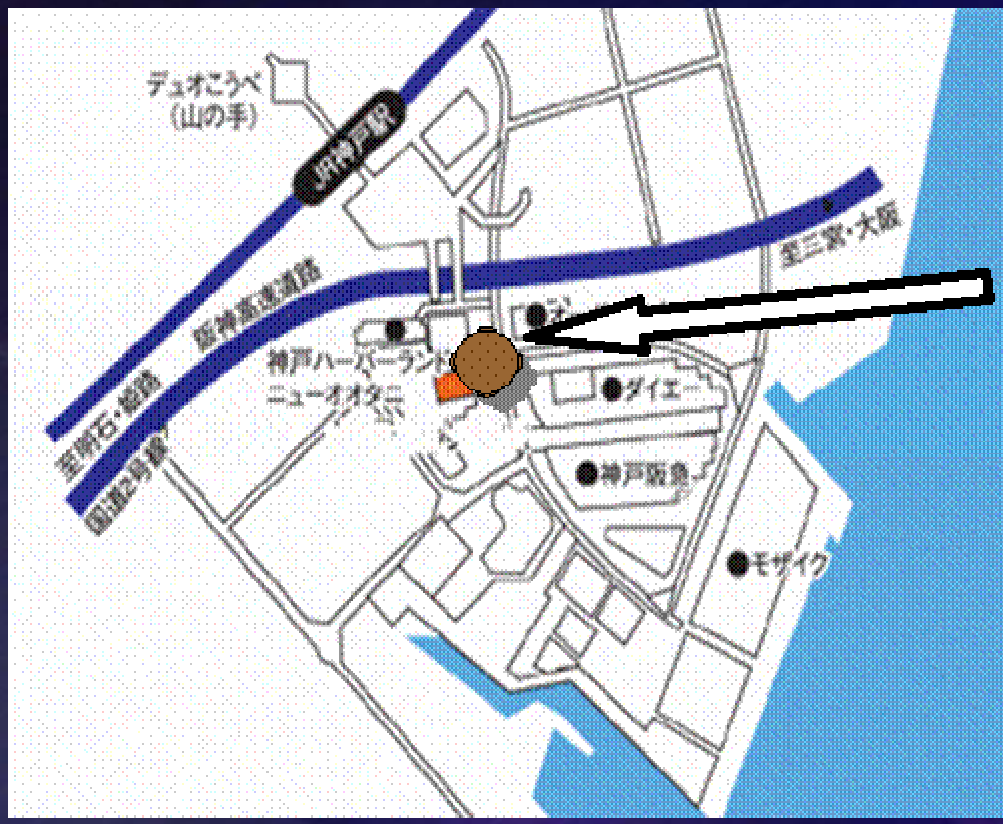
- 履修期間　１年4ケ月（4ケ月×4学期）

- 出願締切　　平成18年7月31日（月）
開講予定　　平成18年8月28日（月）

http://www.cmuj.jp/

CMU日本校の所在地

神戸ハーバーランドセンタービル　17F　（ＪＲ神戸駅前：神戸市中央区東川崎町）



提 言　共同による対策実施の必要性

➡ 組織内での対策の実施

・セキュリティ規程の整備
・職員研修と周知徹底の実施
・持出し防止の技術的対策の徹底
　→私物ＰＣ接続制限、暗号化ソフトの導入
・違反者への罰則の適用

➡ 組織共同の対策の実施

・産官学での共同体制の整備
・Ｐ２Ｐネットワークの監視
　情報が２ｃｈ等で拡散する前に遮断

➡ 国家的対策の実施

・法制度の整備（刑事罰による規制が必要）
・被害者の救済措置の実施