Infowarに見るわが国の危機の本質

1999.10.21

参議院議員
畑　恵

情報化

利便性が高く効果が大

危険性が高い

「情報の共有化」と「セキュリティ対策」は表裏一体

But 政治家・官僚とも認識しているのは一握り

秘匿をかけてまで情報を共有しようという意志がない

Ex.)・インターネット以上の活用をされていない霞ヶ関WAN
・共通の秘匿手段を持たなかった海上自衛隊と海上保安庁
・危機管理情報の一元的な収集やデータ・ベース化
→未だ実現せず。情報収集衛星を機に進展するか？

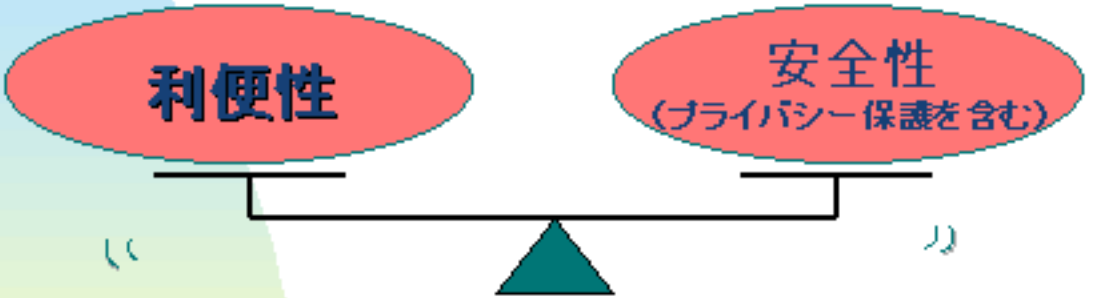
情報共有化の有用性

情報セキュリティの必要性

共に認識が大きく欠如

国家としてのInfowar対策

利便性と安全性のバランスが第一



両者を客観的かつ適切に「評価」するシステム構築が早急に必要
0(ゼロ)or100の水掛け論からの脱却が急務

Infowar対策上の日本の課題

＜危機管理全般における原則＞

■適切な判断　＝

内容の適切さ　×　スピード

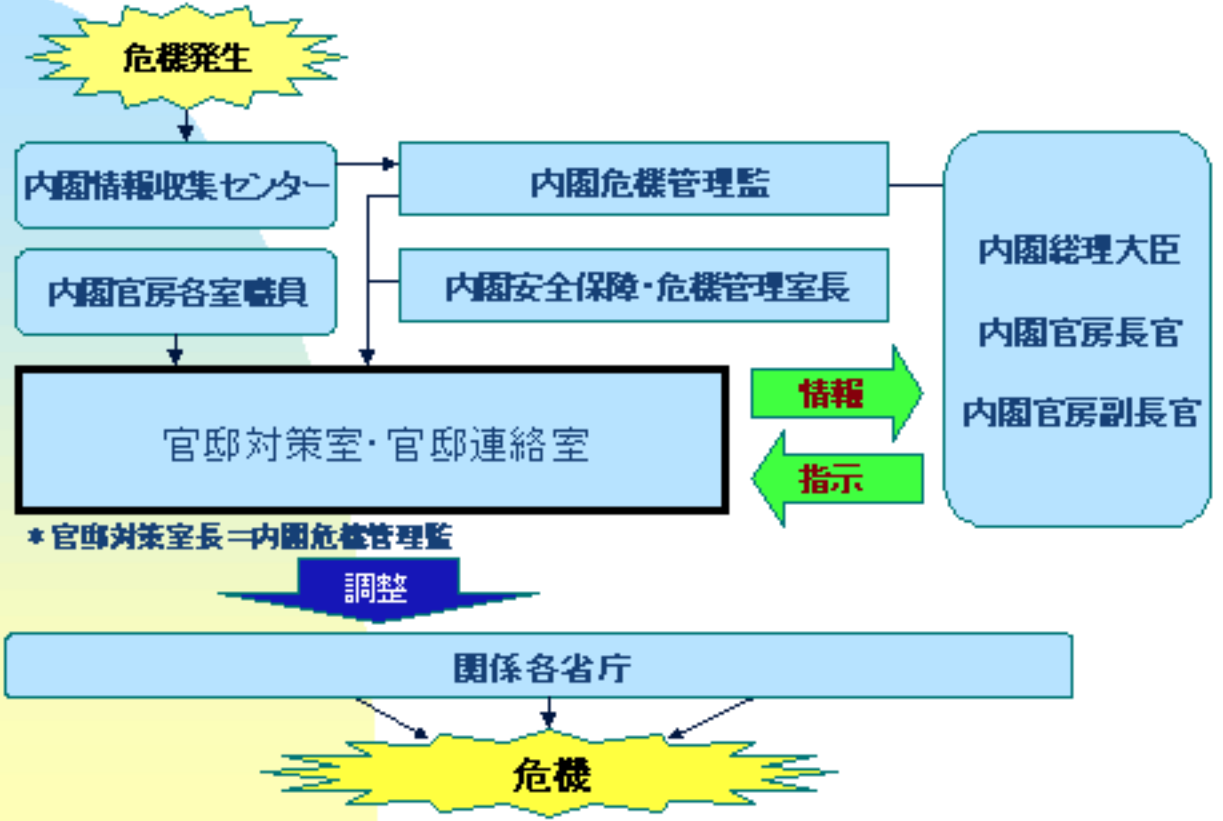
➡ 特にInfowarにおいては「スピード」が命

■情報管理体制が最重要課題

情報収集・分析・伝達における**「一元化」**

- データ・ベース化
- マニュアルの作成
- シミュレーションの徹底

危機への初動対応の流れ



スピーディーな決断

情報の一元化

旧来の日本型社会システムにおいて
両要素の実現は極めて困難

＜日本型システム＞

① リーダーシップより合議制
　　－ 戦略より調整の内閣(総理)
② 戦略機関と執行機関が未分化
③ 縦割り・ヒエラルキー型組織
　　－ 各省庁別の予算・法税制整備
④ 前例主義・横並び主義 － 責任の所在が曖昧
⑤ 密室主義 － 評価より情実
⑥ 変化を忌避

Infowar対策上、最大の障害は
日本の旧来型社会システム

Infowarへの具体的対応策

1. 総理直属の“タスクフォース”の創設
2. 予算・人員の拡充
3. 警察庁と防衛庁の緊密な連携
4. 情報機関(内閣情報調査室)の強化・拡充
5. 民間との協力体制の強化
6. 日本独自の暗号技術・認証システムの開発
7. 情報セキュリティに関する法整備
8. コンピュータ危機に対応可能な専門家の育成
9. 被害にあった際のバックアップ体制の整備

1. 総理直属の“タスクフォース”の創設

（日本版PCCIP）

情報ネットワークを中心とした国家安全保障政策を専門的に企画・立案・実施する危機管理機関

－総理大臣直属とし、内閣官房or内閣府に設置

－メンバーとしては、有能な元ハッカー、企業の情報部門責任者、防衛機関、情報通信の関係者など幅広く起用

－急速な変化のスピードに対応できるよう、メンバーはフレキシブルに入れ替える。

Cf.）・サイバーテロ対策研究会
・重要インフラ対策委員会

<注> PCCIP（重要インフラ保護に関する米国大統領諮問委員会）
＝Presidnt's Commission on Critical Infrastructure Protection

2. 予算・人員の拡充

日本の現状

－不正アクセス対策関連予算　約30億円

・サイバー・ポリス(警察庁)の設置
・大規模プラント等へのコンピュータ・セキュリティ評価事業(通産省)

米国の動き

－クリントン大統領「サイバー部隊構想」を発表(1999．1．22)

⇨ サイバーテロ対策に14億6，000万ドルを計上
＜約1，800億円＞

3. 警察庁と防衛庁の緊密な連携体制

■Infowarへの取り組み状況

警察庁
- ハイテク犯罪対策室を各都道府県警察に設置
- 主要な都道府県警察にサイバーテロ対策ユニットを設置
- ナショナルセンター（技術対策課）を設置

防衛庁
- 特段無し
  （外部と接続していないので侵入の可能性はないと主張）

cf.）米国国防総省 ： １年間で約25万回の不正アクセス攻撃
（うち65％の約16万回が不正アクセスに成功した可能性有り）
＜H10　警察白書より＞

■サイバースペースはボーダレス

あらゆる攻撃に**国境が無い** ⇨ 警察庁と防衛庁の所管の区別は不可

情報交換をはじめ、両庁の緊密な連携が国家安全保障に必須

4. 情報機関（内閣情報調査室）の強化・拡充

内閣情報調査室

:内閣の重要政策に関する情報の収集・分析・調査を担当

cf.）米国：FBI, CIA ／ 英国：MI5, MI6

- 人員（調査官） － 約174名（うち併任・非常勤88名）
- 予算 － 年間約34億円（H11年度）
  （うち、情報収集衛星関係費約13億7400万円）

➡ 拡充

- 調査（捜査）権限の拡大
  ➡ 特に、各省庁への「アクセス権」の付与
- 防衛庁・警察庁・外務省等との人事交流を含めた連携の強化

5. 民間との協力体制の強化

- 政府の安全保障に関する通信網のほとんどは民間に依存

  ＜例＞米国政府でもクリティカルな通信の90％は民間通信網を使用
  （BY：PCCIPレポート）

- 社会基盤システムの管理者のほとんどは民間

  ⇨ 民間の情報危機管理 ＝ 国家の情報危機管理

- 情報機関を持たない特殊事情

  ⇨ 民間からの情報提供がない限り、セキュリティに関する状況は把握できない。

⇨ **サイバーテロに関する民間との意見交換，助言，指導，広報啓発，捜査協力への環境づくりなど**

Infowarへの具体的対応策

1. 総理直属の“タスクフォース”の創設
2. 予算・人員の拡充
3. 警察庁と防衛庁の緊密な連携
4. 情報機関(内閣情報調査室)の強化・拡充
5. 民間との協力体制の強化
6. 日本独自の暗号技術・認証システムの開発
7. 情報セキュリティに関する法整備
8. コンピュータ危機に対応可能な専門家の育成
9. 被害にあった際のバックアップ体制の整備

7. 情報セキュリティに関する法整備

現在、「不正アクセス防止法」が成立(99.8)したのみ

「個人情報保護法」の早期制定

- 現在の三党合意スケジュールでは、3年後

速やかに「情報」自体に価値があることを
法的に規定すべき

★過度の「規制」は望ましくないが、
一定の「規律(ルール)」の徹底は肝心

Infowarへの具体的対応策

1. 総理直属の“タスクフォース”の創設
2. 予算・人員の拡充
3. 警察庁と防衛庁の緊密な連携
4. 情報機関(内閣情報調査室)の強化・拡充
5. 民間との協力体制の強化
6. 日本独自の暗号技術・認証システムの開発
7. 情報セキュリティに関する法整備
8. コンピュータ危機に対応可能な専門家の育成
9. 被害にあった際のバックアップ体制の整備

Infowarへの具体的対応策

1. 総理直属の“タスクフォース”の創設
2. 予算・人員の拡充
3. 警察庁と防衛庁の緊密な連携
4. 情報機関(内閣情報調査室)の強化・拡充
5. 民間との協力体制の強化
6. 日本独自の暗号技術・認証システムの開発
7. 情報セキュリティに関する法整備
8. コンピュータ危機に対応可能な専門家の育成
9. 被害にあった際のバックアップ体制の整備

その他の検討課題

電子商取引に関する国際協定

国際金融に関わる国際協定

電子商取引に関する国際協定

- 互換性＆安全性を備えた認証システムの構築
- 税制をはじめ商法・商慣習の標準化
- 米国はもちろん、「EU」や「アセアン諸国」など
  ともきめ細かく連携を

国際金融に関わる国際協定

- 加熱するヘッジ・ファンドの危険性
  デリバティブなど

最後に

今後、最も重要となるのは「教育」

⋮

様々なことがボーダレスになる時代

➡ 自らの「個」を実現するためには、他者の「個」やその総和としての社会の安定を尊重する義務があることを徹底させることが必須