

## 「情報セキュリティ総合戦略」の策定について

2003年10月10日  
経済産業省

### 1. 「情報セキュリティ総合戦略」の位置付け

産業構造審議会情報セキュリティ部会(部会長;寺島実郎(財)日本総合研究所理事長/三井物産戦略研究所所長)<sup>(注)</sup>において「情報セキュリティ総合戦略 - 世界最高水準の『高信頼性社会』実現による経済・文化国家日本の競争力強化と総合的な安全保障向上」が策定され、本日、中川経済産業大臣に答申がなされました。

本戦略は、関係省庁(内閣官房、内閣府、警察庁、防衛庁、総務省)の参加も得て、我が国で初めて策定された総合的な情報セキュリティに関する戦略です。

「情報セキュリティ総合戦略」の本文及び概要は、以下のURLからダウンロードできます。

<http://www.meti.go.jp/policy/netsecurity/strategy.htm>

### 2. 背景

情報技術(IT)は、単にPCやインターネット、携帯電話などの急速な普及という次元を超え、今や経済、社会の「神経系」を担う基盤となっています。

その一方、送電網(米国)や水道システム(豪州)への侵入\*、コンピュータウイルス(ブラスターワーム等)の蔓延\*、金融・運輸でのシステムダウンによる混乱\*といった事故・事件が実際に発生するなど、ITの問題が社会に損害を及ぼす危険性が飛躍的に大きくなっています。( \*参考1,2参照)

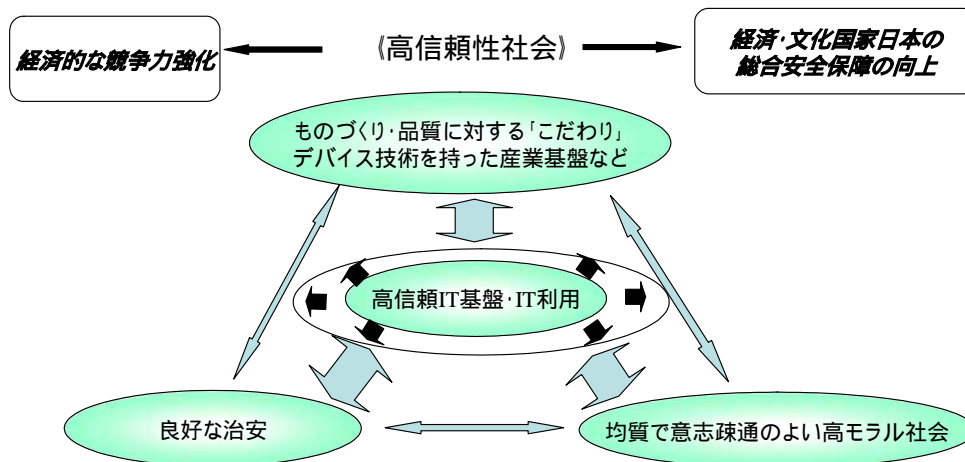
その中で、我が国においては、国や自治体の取り組みは遅れている上、企業や個人の多くは対症療法的対応しか行っていないという状況だと言え、官民が協調しながら、総合的な戦略の下で対策を講じていくことが必要です。

### 3. 「戦略」の概要

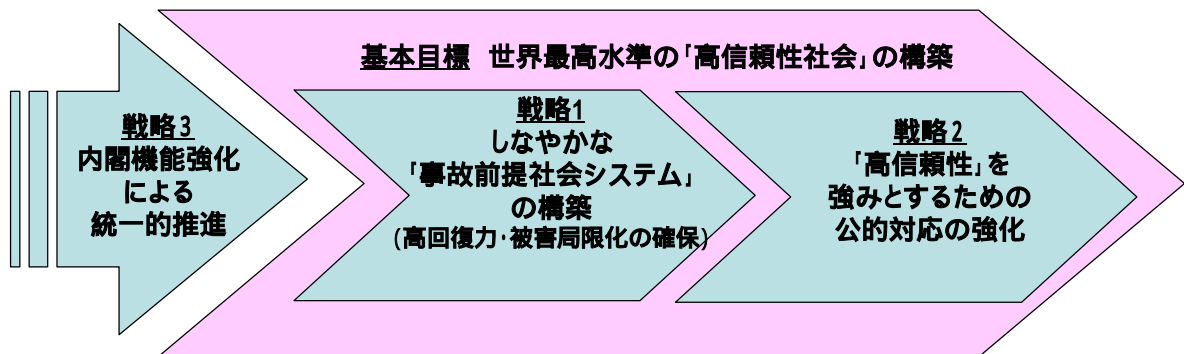
「戦略」の基本目標を、経済・文化国家日本の強みを活かした「世界最高水準の「高信頼性社会」の構築」と位置付け、その要となる「情報セキュリティ対策」について、3つの戦略と42の施策項目（別紙参照）を提言しています。

#### 世界最高水準の「高信頼性社会」の構築

- ・ 情報セキュリティ問題を、経済・文化国家日本の重要な国家戦略に組み込む。
- ・ 我が国の強みである「品質・技術へのこだわり」、「良好な治安」、「均質で意思疎通のよい高モラル社会」などと情報セキュリティ対策を相互補強的に融合した社会システム（高信頼性社会）を形成。
- ・ 経済的な競争力強化の基盤となり、総合的安全保障の向上にも寄与。



#### 基本目標と3つの戦略



## **【戦略1】 しなやかな「事故前提社会システム」の構築**

### **(高回復力・被害局限化の確保)**

- ・ 「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提に立ち、事故・事件の回避(予防)、被害の最小化・局限化、回復力の確保の最適化を図った対応を徹底化する。
- ・ 官民が連携して、総合的な視点からそれぞれの対応を強化。

#### **施策例**

##### 脆弱性に対処するためのルールと体制の整備

政府とIT事業者が中心となって、情報システムの脆弱性情報を集積するためのルールを構築。また、脆弱性やコンピュータウイルス、ワームの危険性について検証・解析する体制を整備。

##### コンピュータウイルス等の警戒情報を提供する機能の整備

コンピュータウイルスやワームの発生について予測し、天気予報的に注意を促す機能の整備を検討。国内の脆弱性分析機能やトラフィック監視機能を連携させて、効率的に情報を共有。

##### 政府・重要インフラ共同でのサイバーテロ演習の実施

高度なサイバーテロシナリオを想定した実践的な演習や、システム事故を想定した訓練を、政府と重要インフラが共同で実施。

(参考)米国では1996年以降、重要インフラのサイバーテロ演習を繰り返し実施し、知見を蓄積。

##### 国・自治体・重要インフラの事故情報共有体制の構築

内閣官房と各所管省庁が「重要インフラ情報セキュリティ委員会」を組織して、問題意識を共有。また、重要インフラの情報システム事故の原因分析と再発防止策検討のため、官民の専門家による「情報システム事故調査委員会」の設置を検討。

##### リスクに対する定量的評価手法の開発

政府が、情報セキュリティを巡るリスクに対する定量的評価手法を開発・公開し、企業の情報セキュリティ投資を促進。また、リスクの定量的評価に用いるため、公的機関が情報セキュリティの事故データを継続的に収集。

## **【戦略2】「高信頼性」を強みとするための公的対応の強化**

- ・【戦略1】の充実強化に加え、個々の主体では取り組めないような公的な問題について、国家的な視点に立って政府自らが積極的に取り組む。
- ・個々の取り組みにおける国際的な調和に十分に配慮しながら、国際的な協調を積極的に推進。

### **施策例**

#### 一極集中・依存リスクを回避したIT基盤の形成

OS や GPS のような、一極集中・依存リスクが生じる恐れのある基盤について、企業や国民が選択肢を持てるよう、国として何らかの代替案の確保を検討。

#### セキュアプログラミング手法の確立と実用化

ソフトウェアの脆弱性(弱点)をできる限り少なくするセキュアプログラミング手法を確立し、国や自治体のシステム開発への適用を検討。

#### ソフトウェア製造技術、デバイス技術などにおける国内基盤技術の確立

産学連携の下でソフトウェア工学の実践を強化する拠点を創設。また、情報セキュリティを基軸に構築され、我が国の強みを活かす基盤技術(デバイス、暗号応用等)に立脚した産業基盤を強化。

## **【戦略3】内閣機能強化による統一的推進**

- ・個々の政策機関における情報セキュリティ対策体制の強化を図るとともに、内閣官房の体制を大幅に拡大し、一元的な推進体制を構築。

### **施策例**

#### 内閣官房情報セキュリティ対策推進室の機能の大幅拡大

内閣官房情報セキュリティ対策推進室の体制、人員及び機能を強化。

(機能強化の例)

- ・国・自治体・重要インフラなどの情報を総合的に収集する体制構築
  - ・各省庁に対するセキュリティ監査や侵入テスト等の検査の実施
  - ・国・自治体の機密保持を支える技術開発等の企画立案
- 等

## **「戦略」の評価体制**

- ・専門家からなる非常勤の「情報セキュリティ政策顧問会議」を設置し、戦略の実施状況の評価と改善案を検討。

(注) 「産業構造審議会情報セキュリティ部会」は、本年5月設置(委員名簿につき、(参考3参照)。また、同時に、情報セキュリティ部会に対して、専門的・実務的観点を付与した具体的な総合戦略案を提示する目的で、商務情報政策局長の諮問機関として、「情報セキュリティ総合戦略策定研究会」(委員長:土居範久中央大学理工学部教授/慶應義塾大学名誉教授)(委員名簿につき(参考4)参照)を設置。

**(本件に関する問い合わせ先)**

**経済産業省 商務情報政策局 情報セキュリティ政策室**

URL <http://www.meti.go.jp/policy/netsecurity/index.html>

電話 03-3501-0397(直通)

ファクシミリ 03-3501-6639

電子メール [it-security@meti.go.jp](mailto:it-security@meti.go.jp)

担当:山崎、川口、赤松

## (別紙) 具体的施策の全体構成

	国・自治体のセキュリティ向上	重要インフラのセキュリティ向上	企業・個人のセキュリティ向上
事前 予防策	<p>情報管理体制の見直しとそれに伴った技術開発及びシステム構築 システム調達時におけるIT製品や暗号などに係る安全性基準等の利用 情報セキュリティ監査の実施やISMS認証取得の促進</p>	<p>情報セキュリティ監査の実施 サイバーテロを想定した情報セキュリティ技術の開発</p>	<p>(1)官民連携した脆弱性対応体制の整備 脆弱性に対処するためのルールと体制の整備 コンピュータウイルス等の警戒情報を提供する機能の整備</p>
			<p>(2)人材育成 情報セキュリティに関わる多面的な実務家・専門家の育成手法の検討 プロフェッショナル向け資格認定制度のあり方の検討 セキュリティインシデント対応機関におけるセキュリティ技術者研修の実施 情報セキュリティ分野の研究・教育人材の育成</p> <p>(3)セキュリティリテラシーの向上 政府による積極的な普及啓発活動の実施 義務教育段階からのセキュリティリテラシー教育の実践 経営者・従業員を対象としたセキュリティ研修の強化 個人が負担感なく安全なIT製品・サービスを利用できる環境整備</p>
事故 対応策	<p>国や自治体における情報共有・活用体制の見直し・設置 サービス継続・復旧計画の策定ガイドラインの整備</p>	<p>情報システム事故に関する省庁間の情報共有・活用と調査委員会の設置 サイバーテロ演習・訓練の実施 重要インフラにおける情報共有体制の設置 サービス継続・復旧計画の策定ガイドラインの整備</p>	<p>(1)技術とセキュリティマネジメントの両輪からなる既存の予防対策の強化 (1-1)技術評価及び技術開発の促進 ITセキュリティ評価・認証制度の普及促進 暗号の安全性評価の強化 安全性向上に向けた技術・製品・サービスの開発 暗号・認証技術を用いた安全な情報流通体制の確立 (1-2)セキュリティマネジメントの促進 情報セキュリティ監査の実施やISMS認証取得の促進 情報セキュリティ格付けのあり方の検討 (1-3)情報セキュリティ関連の国内基準・標準の全体的な整合性の検討</p>
			<p>IT事業者間における情報共有・活用・協力体制の設置 サービス継続・復旧計画の策定ガイドラインの整備 リスクに対する定量的評価手法の開発 保険機能をはじめとする被害軽減手段のあり方の検討 情報セキュリティ関連の法制度上の問題点に係る検討</p>
全体を支える基盤	<p>(1)国の主権に関わるリスクへの対応 情報収集・解析機能の整備 一極集中・依存を回避した情報通信基盤の形成 RMAへの取り組み強化</p>	<p>(2)犯罪対策やプライバシー対策と国際協調 犯罪対策の推進 プライバシー情報保護のあり方に関する検討 国際協調の推進</p>	<p>(3)基礎技術基盤の確立 ソフトウェア製造技術の高度化 セキュアプログラミング手法の確立と実用化 デバイス等基盤技術に関する産業基盤の強化</p>

## 【参考1】 情報システムのダウンの事例(報道資料等より抜粋)

	コンピュータウイルス、ワーム	不正アクセス	人為的ミス
国・自治体	<ul style="list-style-type: none"> <li>・英国防省(MoD)のLAN上の機器がウイルスに感染し、3日間LANをシャットダウンした(2003/04)</li> <li>・世田谷区、大阪府、山口県、郵政公社等で庁内PCがBlasterに感染(2003/08)</li> </ul>	<ul style="list-style-type: none"> <li>・イラク戦争反対者により、米国陸軍・海軍、英国内務省の公的サイトに大量の攻撃メールが送られ、外部からのアクセス要求を受け付けられなくなった(2003/03)</li> </ul>	<ul style="list-style-type: none"> <li>・新居浜市で、操作ミスにより本庁等のオンラインサービスが停止、住民票、税証明書等の発行や窓口照会業務が中断(2003/05)</li> </ul>
重要インフラ	<ul style="list-style-type: none"> <li>・米鉄道の信号システムがウイルスに感染、ワシントン周辺3路線で列車が停止したりダイヤが乱れるなどした(2003/08)</li> <li>・SQL slammerワームが猛威を振るい、韓国では一時インターネットに障害が発生(2003/01)</li> </ul>	<ul style="list-style-type: none"> <li>・世界のルートDNSサーバ13箇所に対するDDoS攻撃が行われ、うち9箇所が一時影響を受けた(2002/10)</li> <li>・米カリフォルニア州の電力会社の送電網システムに外部者が不正侵入(2001/06)</li> <li>・豪クイーンズランド州で、市の水道施設の制御システムに侵入した犯人が、未処理の汚水100万リットルを河川および沿岸部に流し込んだ(2000/03)</li> </ul>	<ul style="list-style-type: none"> <li>・大手銀行の合併に伴うシステム統合において、口座振替の未処理など大規模なシステム障害が発生、復旧に約1ヶ月を要した(2002/04)</li> <li>・インターネットバンキングのサービスがデータベースサーバの障害により全面的にダウン(2003/05)</li> <li>・飛行計画情報処理システムがプログラムミスによりダウンし、200便近くが遅れるなど、航空ダイヤが全国的に混乱(2003/03)</li> <li>・証券取引所の売買システムや株価情報システムがダウン(2003/07)</li> </ul>
企業・個人	<ul style="list-style-type: none"> <li>・”I Love You”ウイルスが世界中のネットワークに蔓延し、電子メールサーバを溢れさせた(2000/05)</li> </ul>	<ul style="list-style-type: none"> <li>・米国有力サイトへのDDoS攻撃により、複数の商用サイトが30分から3時間程度の業務停止に追い込まれた(2000/02)</li> </ul>	<ul style="list-style-type: none"> <li>・顧客登録システムの設定ミスが原因で、携帯電話の新規加入や機種変更などの処理が不能に(2002/03)</li> </ul>

## 【参考2】 機密情報の漏えい、不正操作等の事例(報道資料等より抜粋)

	不正アクセス、不正操作等	人為的ミス
国・自治体	<ul style="list-style-type: none"> <li>・科学技術庁、総務庁、運輸省のホームページが相次いで改ざんされる(2000/01)</li> <li>・宇治市のシステム作成に携わった会社のアルバイトが住民基本台帳データ約21万件を盗み出し、売却(2000/05)</li> <li>・NASDAQのシステムが不正アクセスされ、企業の機密情報が盗み出された(2001/12)</li> </ul>	<ul style="list-style-type: none"> <li>・ポータルサービスセンターのサイトでクレジットカード番号が漏洩しうる欠陥が発覚(2002/10)</li> <li>・防衛庁のシステムの開発資料の一部が流出(2002/08)</li> <li>・四日市市の職員が、個人情報を含む文書が残ったままのパソコンをごみ集積場に廃棄(2003/05)</li> </ul>
重要インフラ	<ul style="list-style-type: none"> <li>・和歌山県の病院で約1700人分の患者のカルテが入った光ディスクが盗まれ、死亡した幼児のカルテを含む個人情報がホームページで掲示された(1999)</li> <li>・豪州の病院で、職員が病院のシステムに入り、患者の投薬データを改ざん、患者が死亡(1995)</li> <li>・長野県赤十字血液センターの献血登録者台帳から個人情報が外部に流出(2003/07)</li> </ul>	<ul style="list-style-type: none"> <li>・高知県の病院で入院患者のカルテ100人分が紛失、誤って廃棄されたものと見られる(2003/08)</li> <li>・生命保険会社で住所、氏名、生年月日、保険掛金額などの顧客情報74人分が流出(2003/07)</li> </ul>
企業・個人	<ul style="list-style-type: none"> <li>・米カード決済処理会社のコンピュータが不正侵入され、クレジットカード番号約800万枚分が盗難(2003/02)</li> <li>・人材派遣会社の登録者約9万人分の個人データを外注会社の社員が持ち出し、ホームページ上で販売(1998/01)</li> <li>・コンビニエンスストアの会員カードの顧客データ約56万件が社外に流出(2003/05)</li> <li>・インターネットカフェにキーロガーソフトを仕掛け、他人のインターネットバンクのパスワードを入手し、1600万円を不正に振り替える事件が発生(2003/03)</li> <li>・国分寺市の市議が、以前交際していた女性のわいせつ画像や実名、生年月日、中傷情報等と掲示板に書き込み、名誉毀損容疑で逮捕される(2000/04)</li> </ul>	<ul style="list-style-type: none"> <li>・エステ会社が顧客等約5万人の個人情報が掲載されたホームページを閲覧可能な状態にしていた(2002/05)</li> <li>・パソコンショップが運営するISPで、会員299人分の住所、氏名、電話番号クレジットカード番号などがインターネット上経由で閲覧可能な状態にあった(2001/06)</li> </ul>

## 「情報セキュリティ部会」委員名簿

### 【部会長】

寺島 実郎 財団法人日本総合研究所理事長 / 株式会社三井物産戦略研究所所長

### 【委員】

青木 千栄子 株式会社ディーワンダーランド代表取締役社長 兼 CEO  
池上 徹彦 会津大学学長 / 独立行政法人産業技術総合研究所理事  
今井 秀樹 東京大学教授  
岡部 直明 株式会社日本経済新聞社取締役論説主幹  
金杉 明信 日本電気株式会社代表取締役社長  
坂村 健 東京大学教授  
重村 勝弘 日立製作所ディフェンスシステム事業部顧問  
島田 精一 日本ユニシス株式会社代表取締役社長  
杉浦 康之 三菱商事株式会社国際戦略研究所所長  
土居 範久 中央大学理工学部教授 / 慶應義塾大学名誉教授  
中村 直司 株式会社NTT データ代表取締役副社長  
山口 英 奈良先端科学技術大学院大学情報科学研究科教授

### 【オブザーバ】

吉原 順二 内閣官房情報セキュリティ対策推進室副室長 / 内閣参事官  
久保田 誠之 内閣府総合科学技術会議 / 参事官  
宮城 直樹 警察庁生活安全局生活安全企画課セキュリティシステム対策室長 / 警視長  
河村 延樹 防衛庁長官官房情報通信課長  
牧 慎太郎 総務省自治行政局自治政策課情報政策企画官  
武井 俊幸 総務省情報通信政策局情報流通振興課長

## 「情報セキュリティ総合戦略策定研究会」委員名簿

【委員長】 土居 範久	中央大学理工学部教授
【委員長代理】 山口 英	奈良先端技術大学院大学情報科学研究科教授
【委員】 岩村 奉武	社団法人日本経済団体連合会情報通信委員会情報化部会委員 (石川島播磨重工株式会社 理事・情報システム部長)
歌代 和正	株式会社インターネットイニシアティブ取締役技術本部 システム技術部部长
大木 栄二郎	NPO ネットワークリスクマネジメント協会幹事 (IBM ビジネスコンサルティングサービス株式会社 チーフ・セキュリティ・オフィサー)
大野 浩之	内閣官房情報セキュリティ対策推進室 NIRT 総括・指導担当 (独立行政法人通信総合研究所 非常時通信グループリーダー)
岡村 久道	弁護士・近畿大学講師
勝山 光太郎	社団法人電子情報技術産業協会セキュリティ政策専門委員会委員長 (三菱電機情報技術総合研究所情報セキュリティ技術部部长)
楠 正憲	マイクロソフト アジア リミテッド法務・政策企画統括本部政策企画本部 技術戦略部長
小山 覚	NTT コミュニケーションズ株式会社 IP インテグレーション事業部担当部長
佐々木 良一	東京電機大学工学部情報メディア学科教授
下村 正洋	NPO 日本ネットワークセキュリティ協会事務局長 (株式会社ディアイティ代表取締役社長)
田尾 陽一	セコムトラストネット株式会社代表取締役会長
高木 浩光	独立行政法人産業技術総合研究所グリッド研究センター セキュアプログラミングチーム長
手塚 悟	日本PKIフォーラム相互運用技術検討部会部会長 (株式会社日立製作所システム開発研究所第7部長)
中尾 康二	株式会社KDDI 技術開発本部情報セキュリティ室長
長嶋 潔	東京海上火災保険株式会社情報産業部eリスクプロジェクトリーダー
西尾 秀一	情報サービス産業協会セキュリティ委員会委員 (NTTデータ・セキュリティ株式会社技術本部コンサルティング部長)
廣川 聡美	横須賀市企画調整部情報政策担当部長
保科 剛	日本ユニシス株式会社アドバンステクノロジー本部長
松浦 幹太	東京大学生産技術研究所・大学院情報学環助教授
松本 勉	横浜国立大学大学院環境情報研究院教授
丸山 満彦	公認会計士 監査法人トーマツ エンタープライズリスクサービス部 シニアマネジャー
三輪 信雄	株式会社ラック代表取締役社長

【オブザーバ】  
 情報処理振興事業協会セキュリティセンター  
 製品評価技術基盤機構  
 日本情報処理開発協会  
 JPCERT コーディネーションセンター

# 參考資料

# 情報セキュリティ総合戦略 (2003年10月10日発表)

～ 世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上 ～

## 要点

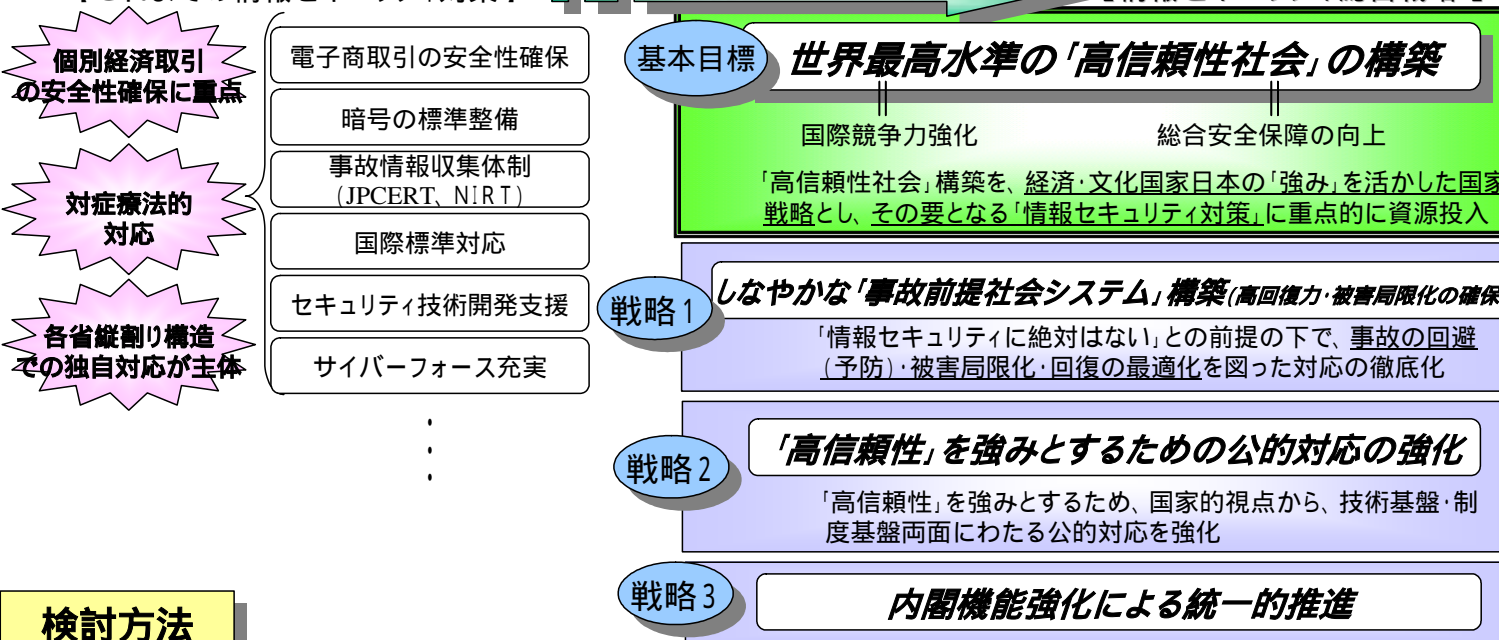
社会全体の「神経系」へ = 新次元のリスクに直面

ITのライフライン化、社会基盤化

(例) 米国: 送電網への不正侵入、豪州: 水道制御システムへの侵入  
米国でのサイバーテロ演習の結果金融システムに脆弱性 など

【これまでの情報セキュリティ対策】

【情報セキュリティ総合戦略】



## 検討方法

【広い視点からの全体戦略】

「キャッチボールしながら」  
集中的に検討

【現場に立脚した技術論・制度論】

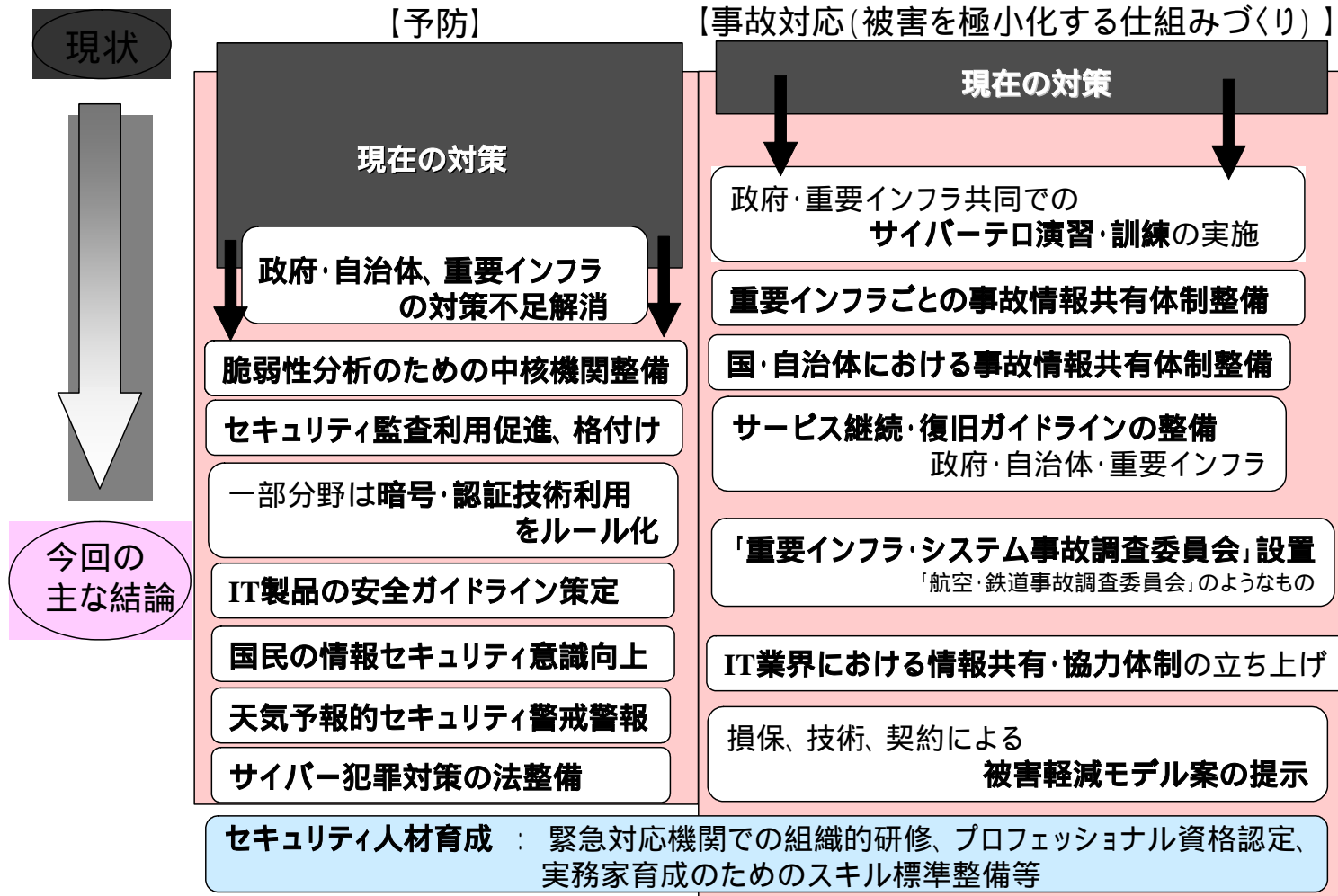
総合安全保障の観点からの情報セキュリティ問題  
戦略的強化に向けた体制のあり方・官民の役割

現場が直面している新次元のリスクとは？  
対応策の現状の実態評価・国際比較  
今後の課題 ・ 新しい具体策の提案

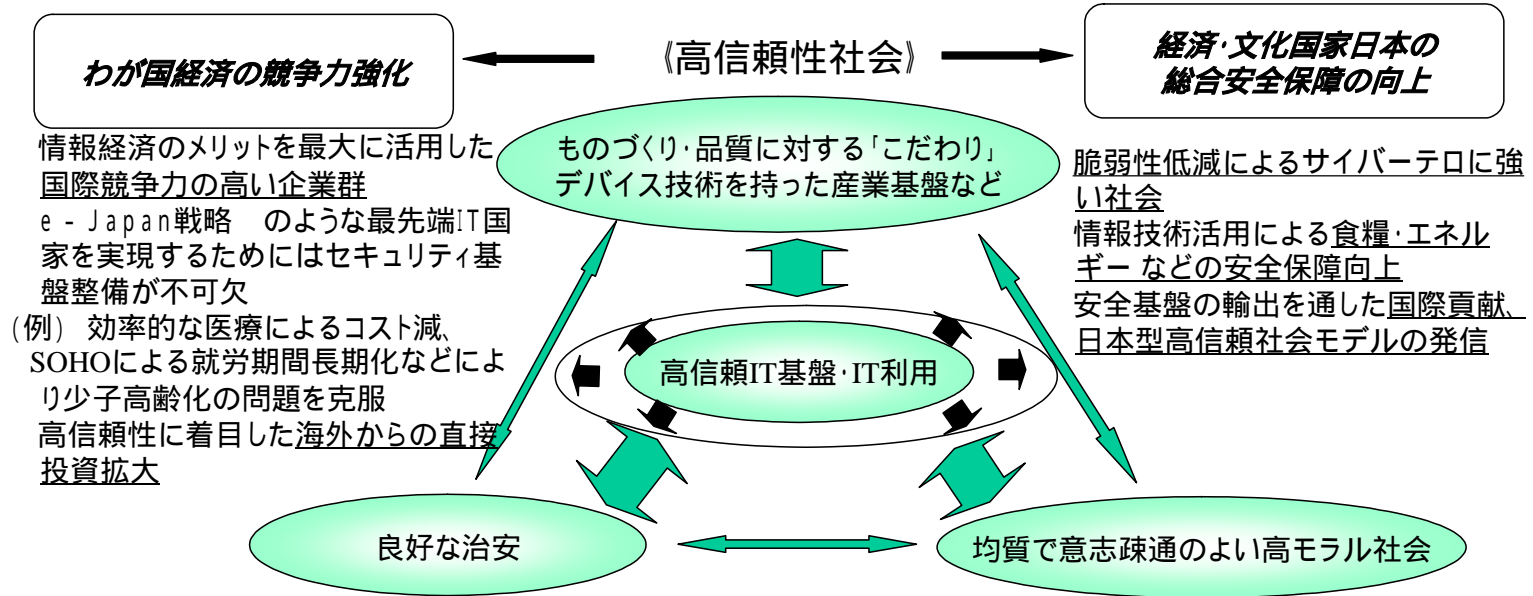
< 経済・安保問題有識者、経営者、研究者 >

< 最前線のセキュリティ技術者、研究者、弁護士、自治体関係者など >

**戦略1: しなやかな「事故前提社会システム」の構築(高回復力・被害局限化の確保)**



## 戦略2: 「高信頼性」を強みとするための公的対応の強化



しなやかな「事故前提社会」の構築(高回復力・被害局限化の確保) = 「戦略1」参照

今回の  
主な結論

国家的視点からの全体を支える基盤の強化

- ・一極集中・依存リスクを考慮した情報通信基盤の形成 (基本ソフト、GPSなど)
- ・サイバー犯罪対策のための官民協力、新技術に対応した個人情報保護のあり方検討

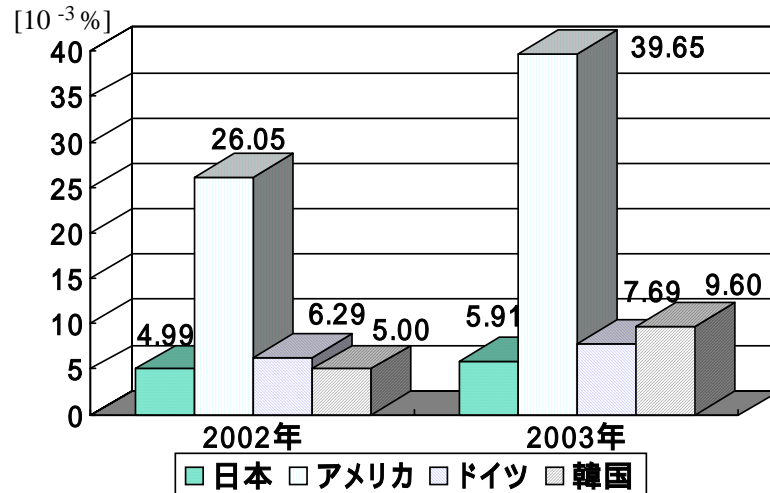
ソフト製造技術高度化、セキュアプログラミング技術普及  
デバイス等基盤技術に関する産業基盤の維持強化

公的対応のあり方の見直し(「政府関与のリバランス」)

- ・「安全保障」「安全な経済活動」の両面に役立つ分野では公的投資を拡大
- ・民主体の分野では「リスクを見せる」ための標準を提供するなど市場機能促進型施策

## 戦略3: 「内閣機能強化による統一的推進」

【政府の情報セキュリティ予算額の対GDP比率】



【各国政府の情報セキュリティ専任部局】

【米国】国土安全保障省(DHS)の創設:現在整備中、国家安全保障局(NSA):人数非公表、国立標準技術研究所(NIST):50名  
 【イギリス】通信電子セキュリティグループ(CESG):300名  
 【ドイツ】連邦情報技術安全局(BSI):390名  
 【韓国】韓国情報保護振興院(KISA):300名  
 【フランス】情報システムセキュリティ中央局(DCSSI):90名

【日本】 内閣官房セキュリティ対策推進室:9名  
 (NIRT:17名、専門調査チーム11名)(非常勤)  
 JPCERT/CC:10名  
 IPAセキュリティセンター:30名

今回の  
主な結論

### 内閣官房セキュリティ室の機能・人員の大幅拡大

- ・公的機関に対するセキュリティ監査・侵入テストの実施
- ・政府、自治体、重要インフラなどの事故情報を総合的に収集する体制の構築
- ・政府機密の保持を支える技術開発の企画・立案 など

### 政府統一的な推進体制構築

- ・各省の役割の明確化、内閣官房による重複業務の調整
- ・政府横断的な“情報セキュリティ政策委員会”における情報共有、統一的実行
- ・専門家からなる“情報セキュリティ政策顧問会議”による「総合戦略」実施状況の評価