

# 「情報セキュリティ総合戦略」の概要

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

IT が社会基盤化し、新次元のリスクに直面する中、単にリスクを低減するとの「守り」の視点のみならず、「安全・安心」面での我が国の強みを活かしながら経済全体の競争力強化と総合的な安全保障向上に役立てるとの視点も加味した「情報セキュリティ総合戦略」を打ち出す。そして、我が国の特性を十分に反映した「情報セキュリティ総合戦略」を、官民が協調しながら着実に実現していく。

## 第1章 戦略の考え方

### 1.1. 現状認識～社会の「神経系」を担うIT

情報技術（IT）の急速な普及は、単なるPC、インターネット、携帯電話などの急速な普及や電子商取引の拡大という次元を超え、経済社会基盤化、ライフライン化というべき状況に。

第一に、金融、エネルギー、交通、医療など諸々の経済社会活動の根幹を支える制御・管理部分に、IT 関連機器やソフトウェアが目に見えない形で組み込まれ、各種社会システムの「神経系」として重要な機能を分担。

第二に、企業の経済活動においても、電子タグや業際的なデータベースの構築などによって、企業という枠組みを超えた、重要な情報を伝達・共有する企業活動全体の「神経系」として急速に相互融合化。資源配分の全体最適化を促進。

### 1.2. 社会全体が直面する新次元のリスク

IT の社会基盤化により、情報セキュリティの側面において、新しい次元のリスクが出現。歴史的に見れば、第三次産業革命（IT をはじめとする先端技術）浸透の中で、時代は大きく変革。

#### （1）リスクの拡大

第一に、リスクの拡大。情報システムの不具合や内外からの悪意ある攻撃が、原因を引き起こした当事者やトラブルに見舞われた被害者だけの問題ではなく、一国の経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない問題へと拡大。

## (2) リスクの変質

第二に、リスクの変質。ITのブラックボックス化、IT利用の多様化、技術革新・ビジネスモデルの変化、責任所在の不明確化等に伴い、リスクの特性が変質。

## (3) 新次元へのリスクへの対応と安全保障の観点から見た問題意識

個々の対策だけでなく、国全体としてリスクを最小化する一方、「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提で、生じた被害を最小化、局限化し、回復力のある、「しなやかな『事故前提社会システム』」を構築するといった観点から対策を検討。

現時点で、我が国においては、経済活動全体を停滞させたり、国民の生命財産を危機に陥れるほどの重大なシステム事故・事件は未発生。しかしながら、新次元のリスクは、愉快犯から組織犯罪・テロリストまで、同様の手法で攻撃を仕掛ける可能性を持つこと、現在はインターネットとの接続やそもそものIT化を慎重に行っている政府・重要インフラの基幹システムも、国際競争力・利便性を確保するためにはIT化は不可避であることから、我が国の政府や重要インフラは常にサイバーテロ等の可能性を認識し、安全保障の観点から最善の対策を選択する必要あり。

「情報セキュリティ」の問題は、単に「安全な経済活動」を阻害するという次元にとどまらず、我が国の安全保障確保の観点から、国家的なレベルで検討すべき問題。

## 1.3. 総合的な情報セキュリティ戦略の必要性

### (1) 対症療法的対応の限界

これまで、我が国においては、企業・個人の個別対策においても、また政府の施策遂行においても、個々の主体がそれぞれの視点から行う対症療法的な情報セキュリティ対策に終始。

大きな時代変化やリスクの本質的な変化を踏まえ対策を抜本的に見直し、我が国の特性を十分加味した「情報セキュリティ総合戦略」を国全体として打ち出し、官民が協調しながら着実に実現していくことが必要。

### (2) 「高信頼性社会」構築による競争力強化と総合的な安全保障の向上

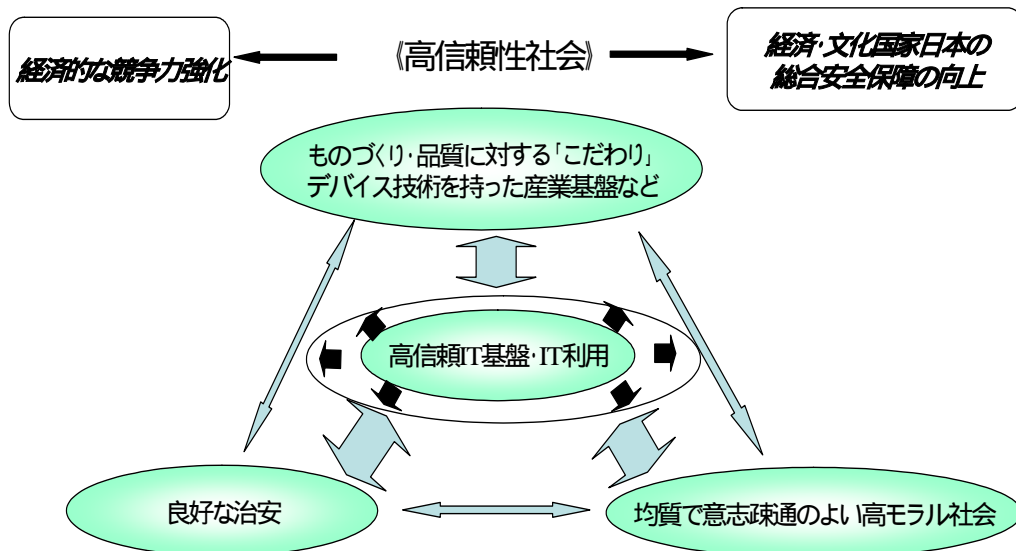
軍事力などのハード・パワーでなく、経済力や文化的な魅力によって国際関係上望ましい結果を導き出していくこと(ソフト・パワー)を目指す我が国にとって、情報セキュリティの確立を基軸に世界最高水準の「高信頼性社会」を構築することは、最重要の国家戦略たるに値するもの。

第一に、情報セキュリティの確立を通じた「高信頼性社会」の実現は、我が国の経済的な競争力強化をもたらす。すなわち、物質的豊か

さを競う「工業経済」から、知恵とノウハウの活用の巧みさを問う「情報経済」への移行の中で、その便益を最大限に引き出すための基盤を提供し、リスクプレミアムの構造的低下を通じて海外からの投資を誘引。また、急速に進展する高齢化と人口減少に直面する中においても、種々な面でのコストダウンと効率化の追求を図ることが可能。雇用の増大にも直結。

第二に、情報セキュリティの確立を通じた「高信頼性社会」の実現は、サイバーテロの防止を図るだけでなく、エネルギーの安定供給の確保や、食糧安全保障の確保にも直結し、総合安全保障の向上にも寄与。

第三に、「高信頼性」は我が国の強みを生かせる分野。ハード・ソフト両面での供給者・消費者双方の「品質」に対するこだわりや、電子デバイス分野などの技術基盤などの潜在的可能性を活かし、世界最高水準の「高信頼性社会」の確立が可能。



**「高信頼性社会」の構成要素**

## 第2章 情報セキュリティを強化するための3つの戦略

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」を「基本目標」として位置付け。その要となる「情報セキュリティ対策」について、従来の個別対症療法的対応からの脱却を図るとともに、国全体としての資源の重点的・戦略的投入強化に向けた3つの戦略を提示。

### 2.1. 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）

事前に事故を予防することや、起きた事故に対症療法的に対応することばかりでなく、「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提で、被害を最小化、局限化し、回復力の高い仕組み、すなわち、「しなやかな『事故前提社会システム』」を構築。

こうした観点を踏まえ、事前予防策及び事故対応策の両面に亘る施策を確立・強化。

### 2.2. 戦略2：「高信頼性」を強みとするための公的対応の強化

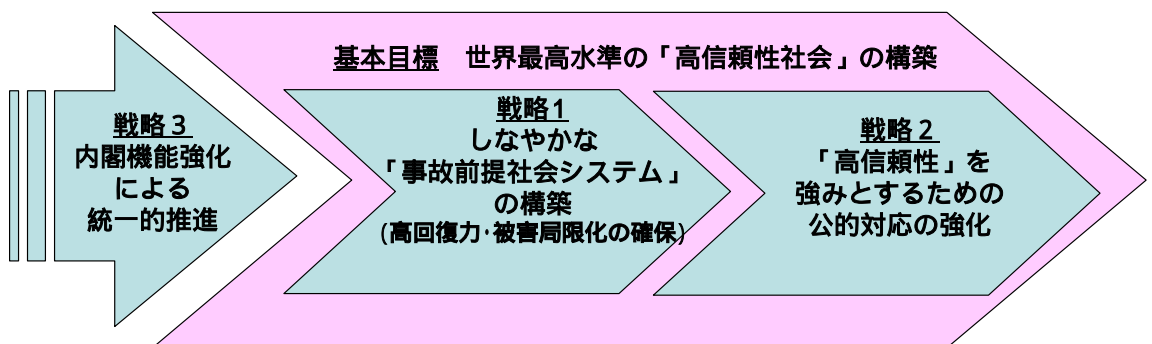
「安全・安心」面における日本本来の「強み」を活かしながら、「高信頼性」を我が国の比較優位にまで高めていくために、国家的視点に立脚した公的対応を強化。

このため、「戦略1」の各般の施策を着実に実行。加えて、市場における情報セキュリティ対策全体の基盤を支え、我が国の強みを活かすことのできる「高信頼性」確保につながるような技術的・制度的基盤、例えば、一極集中・依存リスクを回避した情報通信基盤の形成、サイバー犯罪のための法的基盤作りなどに、政府自らが積極的に取り組む。

### 2.3. 戦略3：内閣機能強化による統一的推進

「戦略1」及び「戦略2」を実現するためには、全体的なポートフォリオ管理を的確に行うことができる一元的な体制が必要。

このため、内閣官房の体制を大幅に拡大し、内閣官房による積極的な対策推進や重複業務調整等一元的な推進体制を構築。



情報セキュリティ強化のための基本目標と3つの戦略

## 第3章 戦略の具体策

### 3.1. 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）の実現（1）～事前予防策の強化

#### （1） 国・自治体・重要インフラにおける事前予防策

##### （国・自治体）

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

##### （重要インフラ）

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

#### （2） 企業・個人における新たな事前予防策

##### （脆弱性対策）

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に関する警戒情報を提供する機能の整備

##### （高度人材の育成）

実務家・専門家の育成手法の検討

専門家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

##### （セキュリティリテラシーの向上）

政府による普及啓蒙

義務教育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

#### （3） 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事前予防 策の強化

##### （技術評価及び技術開発）

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

##### （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と 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

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

### **3.2. 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）の実現（2）～事故対応策の抜本的強化**

#### **（1）国・自治体、重要インフラにおける事故対応策**

##### **（国・自治体）**

国や自治体における情報共有・活用体制の見直し  
サービス継続・復旧計画ガイドラインの整備

##### **（重要インフラ）**

情報システム事故に関する省庁間の情報共有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・活用体制の設置  
サービス継続・復旧計画ガイドラインの整備

#### **（2）企業・個人における事故対応策**

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在り方の検討  
情報セキュリティ関連の法制度上の問題点に係る検討

### **3.3. 戦略2：「高信頼性」を強みにするための公的対応の強化**

「戦略1」の着実な推進  
一極集中・依存リスクを回避した情報通信基盤の形成（基本ソフト、GPSなど）  
サイバー犯罪のための官民協力、新技術に対応した個人情報保護の在り方検討  
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

## **第4章 戦略の実現のための体制と進捗管理**

### **4.1. 戦略3：内閣機能強化による統一的推進**

#### **（1）内閣機能の強化**

内閣の体制や人員を強化し、以下の機能を担う組織として変革を推進。  
・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  
・国・自治体の機密保持等を支える技術開発等の企画立案  
・各省庁に対するセキュリティ監査や侵入テスト等、国としての対外窓口 等

## **(2) 統一的な推進体制の整備**

国と民間企業との協調体制が重要な施策については、役割分担と連携方法を明確化し、我が国において統一的な施策展開を実現すべく、内閣官房の主催で各省庁の情報セキュリティ関連政策担当官による「情報セキュリティ政策委員会」を発足。

### **4.2. 望ましい実現時期**

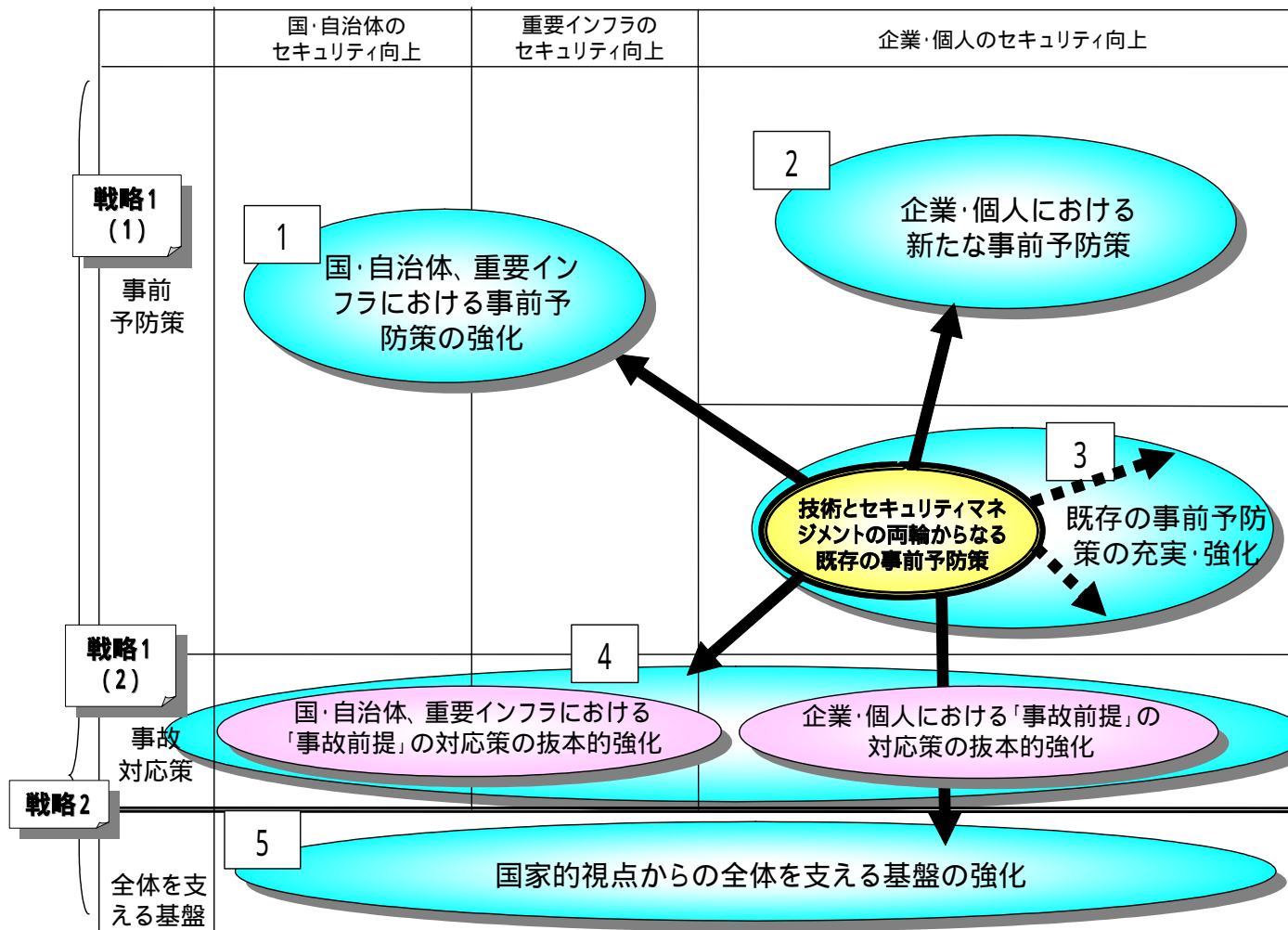
施策毎にマイルストーンを設定。

### **4.3. 戦略の評価体制**

専門家からなる「セキュリティ政策顧問会議」による「戦略」実施状況の評価。

以上

### これまでの施策との関係及び施策の柱立ての概観



### 具体的施策の構成

	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
<b>戦略1 (1)</b> <b>事前            予防策</b>	<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</p> <p>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</p> <p>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</p> <p>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>
<b>戦略1 (2)</b> <b>事故            対応策</b>	<p>国や自治体における情報共有・活用体制の見直し・設置</p> <p>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</p> <p>サイバーテロ演習・訓練の実施</p> <p>重要インフラにおける情報共有体制の設置</p> <p>サービス継続・復旧計画の策定ガイドラインの整備</p>	<p>IT事業者間における情報共有・活用・協力体制の設置</p> <p>サービス継続・復旧計画の策定ガイドラインの整備</p> <p>リスクに対する定量的評価手法の開発</p> <p>保険機能をはじめとする被害軽減手段のあり方の検討</p> <p>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>
<b>戦略2</b> <b>全体を支える基盤</b>	<p>(1) 国の主権に関わるリスクへの対応</p> <p>情報収集・解析機能の整備</p> <p>一極集中・依存を回避した情報通信基盤の形成</p> <p>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</p> <p>犯罪対策の推進</p> <p>プライバシー情報保護のあり方に関する検討</p> <p>国際協調の推進</p>	<p>(3) 基礎技術基盤の確立</p> <p>ソフトウェア製造技術の高度化</p> <p>セキュアプログラミング手法の確立と実用化</p> <p>デバイス等基盤技術に関する産業基盤の強化</p>

## 「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 システム技術部部長
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長)
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	

## 活動記録

### 【情報セキュリティ部会】

2003年6月13日	第1回会合	総合戦略策定の基本的視点について
2003年9月3日	第2回会合	情報セキュリティ総合戦略骨子案について
2003年10月7日	第3回会合	情報セキュリティ総合戦略(案)について

### 【情報セキュリティ総合戦略策定研究会】

2003年5月14日	第1回会合	論点整理について
2003年5月29日	第2回会合	検討に関する基本方針について 情報セキュリティに係るリスクイメージについて
2003年6月12日	第3回会合	「総合戦略」策定の検討手順について 第1回情報セキュリティ部会の資料案について
2003年7月1日	第4回会合	視点の整理について 情報セキュリティの課題の全体像について 重要インフラセキュリティについて
2003年8月8日	第5回会合	「戦略」の視点について 重点課題と実現化施策について
2003年9月8日	第6回会合	情報セキュリティ総合戦略骨子案について
2003年10月2日	第7回会合	情報セキュリティ総合戦略(案)について