**報道発表**

平成 17 年 11 月 17 日
内閣官房情報セキュリティセンター(NISC)

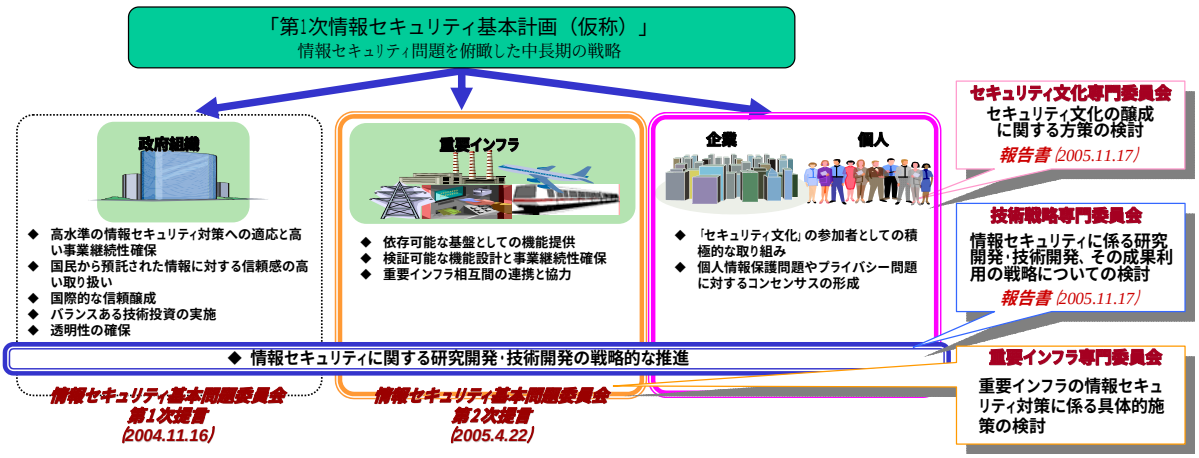
高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議

# セキュリティ文化専門委員会及び技術戦略専門委員会の報告書の正式決定・公表について

1．セキュリティ文化専門委員会（委員長；安田 浩 東京大学国際・産学共同研究センター教授）及び技術戦略専門委員会（委員長；佐々木 良一 東京電機大学教授）は、情報セキュリティ政策会議における「第１次情報セキュリティ基本計画（仮称）」（情報セキュリティ問題全体を俯瞰した我が国としての中長期的な基本戦略）策定の検討に当たり、審議の充実に資するために当該会議に設置されたものであり、専門家・実務家を集め本年夏から検討を開始しました（それぞれの専門委員会の委員名簿については別添参考資料１をご参照ください。）。

（※）設置及び検討の経緯については、http://www.nisc.go.jp/conference/seisaku/index.html を参照。

2．セキュリティ文化専門委員会においては、企業・個人の情報セキュリティ対策を強化するための「セキュリティ文化」の醸成に関する方策を、技術戦略専門委員会においては、情報セキュリティ関連の研究開発・技術開発に関する戦略方策について、それぞれ検討を行いました。本日、それぞれの委員会について、検討の結果を報告書として取りまとめましたので、公表いたします。




「第１次情報セキュリティ基本計画（仮称）」に向けた枠組み

３．セキュリティ文化専門委員会報告書においては、昨今、企業からの個人情報や営業秘密等の情報漏洩のトラブルや、個人がサイバー犯罪に巻き込まれる事例が多発している中、こうした問題を解決するための企業・個人の情報セキュリティ対策の在り方が示されています。報告書に示された主な具体的な方策は以下のとおりです（報告書の全体像については、別添参考資料２をご参照下さい。）。

【企業の情報セキュリティ対策強化のための方策】
○政府調達の入札条件に情報セキュリティ対策レベルの評価を導入すること等により、企業の情報セキュリティ対策が市場評価に繋がる環境を整備
○「情報セキュリティ報告書」の作成推進等、企業における情報セキュリティ関連制度の活用推進
○企業における情報セキュリティをめぐるリスクに対する定量的評価手法の研究推進　等

【個人の情報セキュリティ対策強化のための方策】
○初等中等教育からの情報セキュリティ教育の推進
○世代横断的な情報セキュリティ教育の推進
○ランドマーク的イベントの実施（「情報セキュリティの日」の創設等）
○日常からの世論喚起の仕組みの構築（「情報セキュリティ天気予報（仮称）」の実施検討）
○個人が情報セキュリティ機能を負担感なく利用できるための環境整備　等

【メディアへの情報提供】
○情報セキュリティに関する一般情報を的確にメディアに提供する仕組みの構築　等

【犯罪の取締り強化】
○法執行機関のサイバー犯罪捜査の技能水準の向上や体制の強化　　等

４．技術戦略専門委員会報告書においては、情報セキュリティに関する技術開発についての総合的な戦略の在り方が示されています。具体的には、いわゆるDDoS 攻撃（Distributed Denial of Service 攻撃；複数のホストから特定の攻撃目標に対して、同時に大量のパケットを送り付ける攻撃）の深刻化や、内部の者の行為による企業等からの情報漏洩の多発などを踏まえると、1)急速に拡大するIT の利活用に、情報セキュリティ技術の開発が対応できていない、2)既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスが欠けているといった問題点があることを指摘し、主に以下のような具体的方策を提示しています（報告書の全体像について、別添参考資料３をご参照下さい。）。

【情報セキュリティに関する技術開発の新しい推進構造】
○技術開発成果の利用までを含めた循環モデルの構築（政府調達ガイドラインの策定、政府が活用することを前提とした新たな技術開発の主導）
○情報セキュリティ技術開発全般について、1)事前評価、2)中間評価、3)事後評価の各段階における投資効果の評価を実施　等

【情報セキュリティ技術開発の重点化】
○以下のような領域に対し、技術開発投資を重点化。
・脆弱性をなくす高信頼ソフトウェア開発環境構築のための研究
・次世代ネットワーク基盤に関する研究
・高信頼性組織デザインについての研究
・デジタルフォレンジックに係る研究　等

【「グランドチャレンジ型」技術開発の実施】
○情報セキュリティ分野において、長期的な視野で抜本的な技術革新等の実現を目指すため、「グランドチャレンジ型」の技術開発を実施

５．情報セキュリティ政策会議においては、今後、両報告書を踏まえ、本年内を目処に情報セキュリティ問題を俯瞰した中長期の基本戦略としての「第１次情報セキュリティ基本計画（仮称）」を策定するための検討を行っていく予定です。

**【本件に関する問合せ先】**
内閣官房情報セキュリティセンター（NISC）
佐藤(隆)、中田、山崎
電話　03-3581-3768（直通）

**参考資料1**

セキュリティ文化専門委員会委員名簿

【委員長】

| | |
|---|---|
| 安田　浩 | 東京大学国際・産学共同研究センター教授 |

【委員】

| | |
|---|---|
| 稲垣　隆一 | 弁護士 |
| 岡村　久道 | 弁護士 |
| 志波　幹雄 | (株)電通アカウント・プランニング計画局エグゼクティブ・プロジェクト・マネージャ |
| 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<br>（(株)ディアイティ代表取締役社長） |
| 関口　和一 | 日本経済新聞編集委員兼論説委員 |
| 田邊　則彦 | 慶應義塾湘南藤沢中・高等部教諭 |
| 経沢　香保子 | トレンダーズ(株)代表取締役 |
| 土居　範久 | 中央大学教授 |
| 苗村　憲司 | 情報セキュリティ大学院大学教授 |
| 廣川　聡美 | 横須賀市企画調整部情報政策担当部長 |
| 藤原　静雄 | 筑波大学大学院教授 |
| 村上　輝康 | (株)野村総合研究所理事長<br>（(社)日本経済団体連合会・IT ガバナンスに関する WG 座長） |
| 吉川　誠司 | WEB110 代表 |
| 若槻　絵美 | 弁護士 |

（五十音順、敬称略）

技術戦略専門委員会委員名簿

【委員長】

| | |
|---|---|
| 佐々木　良一 | 東京電機大学教授 |

【委員】

| | |
|---|---|
| 河田　惠昭 | 京都大学防災研究所所長 |
| 志方　俊之 | 帝京大学教授 |
| 篠田　陽一 | 北陸先端科学技術大学院大学教授 |
| 須藤　修 | 東京大学大学院教授 |
| 田尾　陽一 | セコム株式会社顧問 |
| 中西　晶 | 明治大学助教授 |
| 西尾　章治郎 | 大阪大学大学院教授（文部科学省科学官） |
| 宮川　晋 | NTT コミュニケーションズ株式会社先端 IP アーキテクチャセンタ・経営企画部（兼務）担当部長 |
| 米澤　明憲 | 東京大学大学院教授 |

（五十音順、敬称略）

参考資料2

# セキュリティ文化専門委員会報告書の全体像

## 現状認識

背景：ITの普及状況、企業・個人の情報セキュリティ対策の必要性、対策推進上の課題

進むべき方向：「何のために情報セキュリティ対策を行うのか」という点についての共通認識を形成することが必要

## 問題の所在

### 企業
- 情報セキュリティ対策と市場評価の非直結
- 情報セキュリティ人材の不足等

### 個人
- 「当たり前のこと」であることが認識できる環境にない
- ITのわかりにくさと個人の「自己責任」の限界

### メディア
- 問題の本質についてわかりやすい情報を、報道に的確かつ幅広く提供する環境が不足

### 基盤形成
- 各主体の責任・役割等の位置づけ
- サイバー犯罪等
- 急速に変化するサイバー空間の情勢への対応

## 解決の方向性と具体的方策

### 企業
- 情報セキュリティ対策が市場評価に繋がる環境の整備
  - 政府調達への各種制度の活用
  - 企業の情報セキュリティリスク明確化に向けた取組み　等
- 情報セキュリティ人材の確保・育成
  - 経営トップ等の理解の普及
  - 情報システム担当者への啓発　等

### 個人
- 「当たり前のこと」であることが認識できる環境の整備
  - 情報セキュリティ教育、広報啓発、情報発信の強化・推進
- 個人が負担感なく情報関連製品等を利用できる環境整備
  - 情報セキュリティ・ユニバーサルデザインを開発・供給する環境の整備　等

### メディア
- メディアへの情報の提供
  - 情報セキュリティに関する一般情報を的確かつ幅広くメディアに提供する仕組みの構築

### 基盤形成
- 法制度等の検討
  - 位置づけ明確化・普及促進のための法制度整備を含めた幅広い検討　等
- 犯罪の取締り及び権利・利益の保護・救済
  - サイバー犯罪の取締り及び権利利益の保護・救済のための基盤整備
  - サイバー空間の安全性・信頼性を向上させる技術の開発・普及

**評価体制の確立**：基盤の形成の度合を測る指標の策定、導入及び評価状況の公表の実施等について検討

参考資料3

# 技術戦略専門委員会報告書の全体像

## 1．情報セキュリティ技術戦略を考える上での基本的な考え方

情報セキュリティの大目標

①そもそもITが安全であること

②利用者がITが安全であると分かること

③万が一事故が起こった場合でも、その被害の局限化や救済等が図られること

### 1．1　これまでの情報セキュリティ技術の開発モデル

### 1．2　これまでの情報セキュリティ技術の社会展開プロセス

### 1．3　社会基盤としてのITにおける情報セキュリティ問題

急速に拡大するIT利活用に、情報セキュリティ技術の開発が対応できていない

①情報セキュリティ技術の高度化

- 多種多様な研究と技術の相互連関性
- 技術のオープン性
- 多様性によるセキュリティ確保
- 投資効率の改善

既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスを欠いている

②組織・人間系管理手法の高度化

- ITと社会との相互影響関係の認知
- 情報セキュリティ技術を実装する組織のデザイン
- 人間的要因（ヒューマンファクター）への配慮

### 1．4　環境整備の必要性

- ●社会システムデザイン研究
- ●継続的なリスクアセスメントの実施
- ●ベストプラクティクスの収集と活用
- ●人材育成
- ●プライバシーの適切な取り扱い
- ●IPv6利活用の推進

## 2．情報セキュリティ技術の研究開発・技術開発を推進するための新しい構造のあり方

### 2．1 投資領域設定の継続的見直し構造の実現

- ●実施状況の把握
- ●資源配分方針の評価・見直し

### 2．2 成果利用までを見据えた研究開発・技術開発の実施体制の構築

- ●循環モデルの構築
- ●継続的評価プロセルの構築
- ●産官学共同プロジェクトの実施

## 3．情報セキュリティ技術開発の重点化と環境整備のあり方

### 3．1 情報セキュリティ技術の高度化及び組織・人間系管理手法の高度化を実現するための具体的な方向性

### 3．2　情報セキュリティ技術を支える環境整備

## 4．「グランドチャレンジ型」研究開発・技術開発の推進

### 4．1　「グランドチャレンジ型」研究開発・技術開発とは

### 4．2　情報セキュリティ領域における「グランドチャレンジ型」研究開発・技術開発の実施