# 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
# 第3回会合 議事要旨

1 日時　平成 17 年 12 月 13 日（火）　17:00～18:00

2 場所　総理官邸大会議室

3 出席者（敬称略）

| | |
|---|---|
| 安倍 晋三 | 内閣官房長官 |
| 松田 岩夫 | 情報通信技術（IT）担当大臣 |
| 沓掛 哲男 | 国家公安委員会委員長 |
| （欠）額賀 福志郎 | 防衛庁長官 |
| | （※髙木 毅 防衛庁長官政務官代理出席） |
| （欠）竹中 平蔵 | 総務大臣 |
| | （※古屋 範子 総務大臣政務官代理出席） |
| （欠）二階 俊博 | 経済産業大臣 |
| | （※西野 あきら 経済産業副大臣代理出席） |
| 与謝野 馨 | 内閣府特命担当大臣（金融担当） |
| 猪口 邦子 | 内閣府特命担当大臣（少子化・男女共同参画担当） |
| （欠）川崎 二郎 | 厚生労働大臣 |
| | （※赤松 正雄 厚生労働副大臣代理出席） |
| （欠）北側 一雄 | 国土交通大臣 |
| | （※石田 真敏 国土交通大臣政務官代理出席） |
| 江畑 謙介 | 拓殖大学客員教授／軍事評論家 |
| 小野寺 正 | KDDI 株式会社代表取締役社長 |
| 金杉 明信 | 日本電気株式会社代表取締役執行役員社長 |
| 野原 佐和子 | 株式会社イプシ・マーケティング研究所代表取締役社長 |
| 前田 雅英 | 首都大学東京教授 |
| 村井 純 | 慶應義塾大学教授 |

（上記のほか以下が出席）

| | |
|---|---|
| 二橋 正弘 | 内閣官房副長官（事務） |
| 野田 健 | 内閣危機管理監 |
| 伏屋 和彦 | 内閣官房副長官補 |
| 柳澤 協二 | 内閣官房副長官補 |
| 山口 英 | 内閣官房情報セキュリティ補佐官 |

4　議事概要

(1)　「第１次情報セキュリティ基本計画」について
(2)　政府機関の情報セキュリティ対策について
(3)　重要インフラの情報セキュリティ対策について

事務局より、資料に基づき、一括して説明を行った。

(4)　出席者意見開陳

上記(1)～(3)について、出席者から以下のような意見が述べられた。

○ 「安全保障」という言葉の捉え方が各々異なっており、用語に対する認識概念の統一が必要。

○ 第1次情報セキュリティ基本計画にあるように、この分野で世界をリードするというのであれば、セキュリティ対策を完備したＮＩＳＣのようなそれにふさわしい態勢が必要。

○ 外部･内部からの脅威に対する対策のみならず、システムの多重化あるいはダイバシティといった対策の実施についても充分な配慮が必要。

○ 情報共有、セキュリティ基準の取組みも必要であるが、一旦起こった後の復旧のための優先措置なども視野に入れた対策の検討が必要。

○ 重要インフラ事業者の「安全基準等」については、内閣官房におけるフォローアップとして、指針への準拠性確認、各インフラが策定した「安全基準等」の間のレベル合わせなどに関わる助言を行うことが必要。

○ 政府機関をはじめとした諸機関の情報セキュリティを充実させるためには、各機関の情報セキュリティに関する情報開示が不十分。

○ 次世代のネットワークの構築においては、我が国独自の研究開発と調達をリンクさせることが必要。

○ 厳しい国家予算の状況下ではあるが、情報セキュリティ政策推進のための継続的かつ弾力的な予算措置が必要。

○ 海外へのアピールの観点からも、第1次情報セキュリティ基本計画のキャッチフレーズを考えるべき。

○ 各政府機関の対策の推進においては、各府省庁における対策の評価結果を分かりやすい形で公表することが重要。

○ 個人の情報リテラシーをあげることも重要であるが、より重要なことは個人が負担感なく利用できるような環境を整備すること。

○ 重要インフラ対策を行うにあたって、情報セキュリティセンターに情報が集まってきた際に、その機微な情報を如何に安全に管理していくかが重要。

○ IT社会の大事さは分かるが、IT社会によって心が壊れていくような問題も将来的には視野に入れることが必要。

○ 今回の基本計画は、教科書として使うぐらい充実した内容。政府の情報セキュリティ対策の検査のメカニズムが重要。評価結果を共有することが価値を生んでいくことであり重要。

○ 国際連携・協調の具体的な体制作りに取り掛かれるものと期待。

○ 世界に冠たる最高の組織を作るためには、最高の人材が集まらないといけないが、どのように集めるか、どこに人材がいて、どのようにキャッチアップするかが非常に難しい問題。人材登用、人材交換など具体的な取り組みが必要。

○ 企業の信頼性が、情報セキュリティのメトリックで変わってくる時代。明確なメトリックの中で、日本の企業価値、日本の市場価値がきちんと捉えられるということに、情報セキュリティの体制が寄与する環境作りが重要。

○ IT戦略本部では、今月8日にIT新改革戦略の案を策定し、現在パブリックコメントを募っているところ。この新改革戦略においても、情報セキュリティをもっとも重要な一つと位置づけている。

○ 金融分野においても、セキュリティは大変重要だと認識。昨今の非意図的な問題については、市場の信頼を損ねかねない事故と認識。再発防止にしっかりと取り組みたい。本日決定される行動計画等を踏まえ、安全対策等の検証など、金融分野における情報セキュリティ対策の一層の取り組みに努めたい。

○ サイバー犯罪を未然に防止するとともに、サイバー犯罪を行った者を確実に検挙することにより、ＩＴを安心して利用可能な環境を構築するなど、より一層の取組みが求められているものと認識。

○ サイバーテロの脅威が現実のものとなっていることを踏まえ、装備資機材の高度化や情報収集体制の強化等、事案の発生を見据えた各種のサイバーテロ対策を推進し、政府全体の対処能力の強化に貢献していきたい。

○ 情報共有にあたっては、その情報が漏洩するなどによって、安全保障・危機管理上の脅威となることのないよう、情報の管理に万全を期すことが不可欠。

○ 内閣府としては、この第１次情報セキュリティ基本計画の内容を国民生活審議会での議論に反映させつつ、個人情報保護制度の見直しに向けた検討を進めて参りたい。

○ 医療情報システムの安全管理に関するガイドラインの策定等を含めて、医療機関のセキュリティ意識の啓発につとめてきたところ。今回決定される行動計画に基づき、当該ガイドラインも含めて既存の指針の見直しの検討、情報共有や分析機能の整備等に取り組みたい。

○ 日々増大している問題に対して、ただちに実行に移す姿勢が大事であり、内閣官房が先頭にたってリーダーシップを政府が率先して発揮すべき。ＩＴ商品の調達という問題やアウトソーシング先の水準の確認等を確実に実施することが大事。

○ ＩＴに起因する新たな脅威に対応すべく、情報セキュリティを確保する専門部隊の充実や人材育成などを行っているところ。

○ 防衛庁としては、指揮命令の確実・迅速な伝達と情報セキュリティの確保の両立が必要と考えている。また、安全保障上の問題から、情報セキュリティに関する評価、確認について、自ら評価、確認を行う必要があり、政府機関統一基準の適用にあたっては、これら防衛庁・自衛隊の特性を踏まえて対応していきたい。

○ 重要インフラの情報セキュリティについては、テロ関連情報など各種情報の提供や関係機関との連携等の期待に応え、積極的な役割を果たしていきたい。

○ 政府機関統一基準の運用により、政府全体のセキュリティ水準を向上させるためには、技術や環境変化を踏まえた基準の見直しや、各省庁の実態に併せ、内閣官房情報セキュリティセンターにおいて適切なフォローを行うことが重要。

○ 重要インフラの情報セキュリティ対策について、国民生活・社会経済活動の基盤である重要インフラについて、想定する脅威の範囲を拡大した行動計画については、重要インフラの安定運用のために極めて重要。

○ 情報システム障害に起因する行政サービスの低下防止、鉄道、航空等所管分野の安全かつ安定的な事業運営体制の確保のために、政府全体の指針に基づき対策を推進してきたところ。本日決定される諸計画を踏まえ、今後も必要かつ十分な対策を講じたい。

○ 「政府の情報セキュリティ対策の評価の結果を公表すべきである」との御指摘については、安全保障上の問題などがない限り、可能な限り結果を公表し、透明性の高い運営を行えるよう、内閣官房として責任を持って検討を行っていきたい。

○ 東証におけるシステム障害の発生など、証券市場をはじめとした重要インフラにおける情報セキュリティ対策の必要性がとみに高まっていることはかねてから認識。「重要インフラの行動計画」に基づき、今後、内閣官房情報セキュリティセンターを中心に関係省庁及び関係業界が緊密に連携し、着手可能なものから早急に対策を強化していく所存。

(5) 政策会議決定等

「第1次情報セキュリティ基本計画」および「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針」についてパブリックコメントに付すこととし、「政府機関の情報セキュリティ対策のための統一基準」および「重要インフラの情報セキュリティ対策に係る行動計画」について政策会議決定とした。パブリックコメントは、約一か月の間受け付け、意見に基づき必要な修正を施した上で、次回の政策会議において最終決定することとした。

－以 上－