報道発表

平成 20 年 2 月 4 日
内閣官房情報セキュリティセンター（NISC）

第 16 回情報セキュリティ政策会議の開催について

－「情報セキュリティの日」功労者表彰の実施等－

本日 2 月 4 日、「情報セキュリティ政策会議」（議長：内閣官房長官）の第 16 回会合が開催され、その概要は次のとおり。

このうち、今回決定されたものは、政府統一基準改定（第 3 版）と政府機関において使用されている暗号アルゴリズムに係る移行指針のパブコメ案。

1.「情報セキュリティの日」に関する取組み

情報セキュリティの重要性について広く国民への普及・啓発を図る観点から、毎年 2 月 2 日（「第1次情報セキュリティ基本計画」を決定した日）を「情報セキュリティの日」と定め（平成 18 年 10 月 25 日第 8 回情報セキュリティ政策会議決定）、本年度は次の事項を実施。

（1）「情報セキュリティの日」功労者表彰（報告及び表彰実施）

内閣官房情報セキュリティセンターに情報セキュリティ啓発推進委員会を設置し、「情報セキュリティの日」を推進する関係省庁（警察庁、総務省、文部科学省、経済産業省）からの推薦と内閣官房が把握している官民における取組みを踏まえ、候補者の上申案を作成。

この上申案による候補者の中から議長が表彰者を決定。本日の情報セキュリティ政策会議終了後、表彰式典を実施。

【本年度の受賞者】

- 安田 浩 氏（東京電機大学教授、東京大学名誉教授）
- 佐々木 良一 氏（東京電機大学教授）
- 神奈川県藤沢市（地方公共団体）
- 国立情報学研究所及び電子情報通信学会
- 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）

（表彰される方の功績及び功労については別紙 1 参照）

(2) 「情報セキュリティの日」関連行事(報告)

「情報セキュリティの日」を中心に広く官民の協力を得て実施。国民各層における情報セキュリティの意識向上を期待。

○ 総件数　593 件(前年比 90%増)
(平成 20 年 1 月 31 日迄に把握した件数、今後も追加する予定)

○ 開催時期　平成 20 年 1 月 26 日(土)から 3 月 2 日(日)までの間

○ 開催地域　全国 47 都道府県

○ 開催形態　セミナー、講演会、特設ホームページ等

2. 政府機関における情報セキュリティ対策について

(1) 「政府機関の情報セキュリティ対策のための統一基準(第 3 版)」(政策会議決定)

○ 前回会合(平成 19 年 12 月 12 日)において決定されたパブリックコメント案について、パブリックコメントを募集(平成 19 年 12 月 12 日～平成 20 年 1 月 10 日)。

○ 計 6 件のコメントが寄せられたものの、既にパブリックコメント案に記載済み等の理由により、文章の修正に至らず、原案どおり決定。

○ 今後も定期的に見直しを実施する予定(※ 1)。

(別紙 2 参照)

(参考) 今回の改訂の概要は次のとおり。

○ ドメインネームシステム(DNS)(※2)に関する対策(新規)
DNS への攻撃によるウェブ、電子メール等の政府機関サービスの妨害等への対策を追加。

○ 監視機能(遵守事項追加)
情報セキュリティ侵害の予防、対処、抑止を目的とした監視に係る対策を追加。

○ 政府機関サイトへの成りすまし対策(新規)
成りすましサイト対策として、政府機関で使用するドメイン名に関して規定。

※1 「政府機関の情報セキュリティ対策のための統一基準」については、政府機関の情報セキュリティ水準を適切に維持していく観点から、技術や環境の変化を踏まえ、毎年その見直しを行うこととされている。

※2 DNS とは、「Domain Name System」の略であり、ホストと IP アドレスの対応付けを行うシステムのこと。

(2) 政府機関における安全な暗号利用の促進(パブコメ案決定)

○ 現在、電子政府システムでは、電子署名等のために SHA-1 (※ 3)及び RSA1024 (※ 4)と呼ばれる暗号方式を広く使用。

○　しかし、電子計算機の性能の向上等によりそれらの暗号の安全性が相対的に低下。

○　情報システムの相互運用性確保や政府全体の情報セキュリティ向上のため、政府統一的な移行指針の策定が不可欠であり、同指針のパブコメ案を決定。

○　本案について広く意見を募集した上で、4 月に予定されている次回の政策会議において決定する予定（意見募集期間 2 月 4 日～ 3 月 7 日）。

○　パブコメ案の概要は次のとおり。

①　技術的な対応

・ 新たな暗号方式として、SHA-256（※ 5）及び RSA2048（※ 6）を採用。

・ 移行完了前に安全性低下の影響が発生する場合に備え、緊急避難的な対応も想定。

②　制度的な対応

・ 各府省庁において、システムの移行時期を踏まえ、必要な対応の取りまとめ、移行手順書の整備を実施。

③　スケジュール

・ 2008 年度中に新たな暗号方式へ切り替える時期を検討。

・ 2010 年度から 2013 年度までの間に、各府省庁における情報システムの対応を完了。

・ 総務省及び経済産業省は暗号の安全性に係る状況を監視し、内閣官房は必要な情報を速やかに各府省庁に提供。

（別紙 3 参照）

（参考）　米国では期限を決めて対応する方法を採用し、 2010 年末以降、政府機関において、SHA-1 の新規使用を停止する方針。

※3　ハッシュ関数 SHA の一つで、与えられたデータから 160 ビットの固定長の値を生成する。

※4　公開鍵暗号方式の一つで、暗号アルゴリズムを RSA 、鍵の長さを 1024 ビットとしたもの。

※5　ハッシュ関数 SHA の一つで、与えられたデータから 256 ビットの固定長の値を生成する。

※6　公開鍵暗号方式の一つで、暗号アルゴリズムを RSA 、鍵の長さを 2048 ビットとしたもの。

3．セキュリティ･バイ･デザイン[SBD]の今後の予定

「情報セキュリティの観点から見た行政情報システムの望ましいあり方」と「行政情報システムの企画･設計段階からのセキュリティ確保に向けた取組み」の進捗状況として次の事項を報告。

○　各府省庁において取り組まれている既存の枠組みに留意しつつ、段階的に進める。

○　平成 19 年度は「企画から運用・保守までの各段階における点検リスト」の一部として、「政府機関統一基準のうち情報システムに関する遵守事項についての実施手引書」を作成。

（別紙 4 参照）

4．国際協調・貢献に向けた取組みの進捗状況

「我が国の情報セキュリティ分野における国際協調・貢献に向けた取組み」（平成 19 年 10 月 3 日政策会議決定）の進捗状況として次の事項を報告。

○　アジア地域のビジネス環境向上に向けた協調・貢献の推進（セキュア・アジアビジネス環境構想）

・ 経済関係が深化する日・ ASEAN 間において安心・安全に事業活動を行えるような環境の整備、地域的な IT 障害への共同対応の枠組み作りを目指す。

・ 2007 年 8 月に開催された日・ ASEAN 情報通信大臣会合、経済産業大臣会合の場において日・ ASEAN 間の情報セキュリティ政策会合の設立を提案。

・ 2008 年度中の我が国での第 1 回アジア情報セキュリティ政策会議（仮称）の開催に向けた検討を引き続き継続。

○　サイバー攻撃等、 IT に起因する脅威への対応のための取組みの推進（リスクのない ICT 構想）

・ サイバー攻撃等、 IT に起因する脅威に関して、先進国のハイレベルで問題意識を共有し、適切に対処すべく議論を積極的に喚起、参加・貢献を行う。

・ 世界共通の社会インフラである IT の信頼性・堅牢性の維持・確保に向けた多国間の国際会合の議論を加速化。

○　様々な国際フォーラム等における提案や議論への積極的な参加

・ 多国間フォーラムの開催場所として貢献するなど、多国間のフォーラムを主導すべく努力

・ 必要な情報を適時適切に入手できるよう、既存のグローバルな取組みについても、より積極的に参加・関与

（別紙５－１、５－２、５－３参照）

５．重要インフラにおける情報セキュリティ対策について

（1）「重要インフラ連絡協議会(CEPTOAR-Council)」（仮称）（※ 7 ）創設に向けた検討状況（報告）

○ 「重要インフラ連絡協議会(CEPTOAR-Council)」（仮称）の創設についての基本的な考え方（案）を本年 3 月を目処に取りまとめる予定。

○ CEPTOAR-Council 創設準備会設置要綱（素案）を検討中。2008 年 6 月を目処に創設準備会を設置し、2008 年度内の創設を目指す。

（別紙 6 参照）

※7 「重要インフラの情報セキュリティ対策に係る行動計画」（平成 17 年 12 月 13 日情報セキュリティ政策会議決定）において、各 CEPTOAR 間での横断的な情報共有の場として創設することとされている協議会。

（2） 2007 年度分野横断的演習の実施（報告）

○ 目的

IT 障害発生時の重要インフラのサービスの維持・早期復旧に向けた現状の情報共有の仕組みの検証

○ 検証課題

・ サイバー攻撃が発生した場合の当該重要インフラ事業者における関係者を含めた対応方法
・ サイバー攻撃が発生した場合の当該重要インフラ事業者、 CEPTOAR 、所管省庁、NISC 間の情報連絡及び情報提供の方法
・ NISC 、所管省庁から他分野のサイバー攻撃の情報提供を受けた場合の、各重要インフラ事業者における重要システムでの影響の検証方法
・ 事象収束後の CEPTOAR を経由した情報共有の方法

○ 演習の概要

重要インフラ事業者のサイトが、ボットネットによる DDoS （ Distributed Denial of Service ）攻撃を受け、数時間程度、ホームページの閲覧不能や重要システムの影響が発生したという想定で、官民における連絡・連携、情報共有の仕組みを検証

○ 実施日 2008 年 2 月 6 日（水）

○ 政府機関、重要インフラ分野事業者、 CEPTOAR 、分野横断的演習検討会有識者等が参加予定。

（別紙 7 － 1 、 7 － 2 参照）

（参考）
前回演習時（2007年2月7日実施）からの改善点は以下のとおり。
・ 新たに7分野11CEPTOARが参加
・ NISCや所管省庁もプレイヤーとして演習に直接参加
・ 実態により近い演習方式を採用
・ 事象として新たにDDoS攻撃を想定

6．その他

（1） 基本計画検討委員会（報告）

○ 前回政策会議で設置を決定したみだしの委員会の第1回会合を1月16日に開催し、須藤修委員を委員長として選出。

○ 第2回会合を2月14日、第3回会合を2月21日、第4回会合を3月19日、第5回会合を3月下旬から4月上旬に開催予定。

○ 本年4月を目処に「第一次提言（仮称）」を取りまとめる予定。

（別紙8－1、8－2参照）

（2） 2007年度重要インフラにおける「安全基準等の見直し状況等の把握及び検証」（最終報告）

○ 平成19年6月に行われた指針の改定を踏まえ、重要インフラ全10分野において安全基準等の見直しを実施し、5つの安全基準等において改定を実施。

○ 指針改定箇所について、重要インフラ全10分野において対応していることを確認。

（別紙9－1、9－2参照）

【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）
山口補佐官、関参事官、中田参事官補佐
電話　03-3581-3768（センター代表）

※ 本日の会議資料は、内閣官房情報セキュリティセンターのホームページにおいて公表。
（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku16）

※ 「情報セキュリティ政策会議」は、平成17年5月30日のIT戦略本部決定によって設置。
（http://www.nisc.go.jp/press/pdf/050530seisaku-press.pdf）

別紙1

情報セキュリティの日功労者表彰受賞者一覧

受賞者･団体	功績又は功労（概要）
安田　浩（63歳） （東京電機大学教授、東京大学名誉教授）	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」委員長として、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」醸成に関する方策についてのとりまとめに尽力。 また、マルチメディアコンテンツにおける知的財産権保護技術、インターネットセキュリティの分野での本人認証手法等の研究において、顕著な功績・功労があったほか、インターネットカフェ等における匿名性の問題やインターネット上における違法情報への対策の検討など、サイバー犯罪対策に多大な貢献があった。
佐々木　良一（60歳） （東京電機大学教授）	情報セキュリティ政策会議「技術戦略専門委員会」委員長として、我が国の情報セキュリティに係る研究開発・技術戦略と、その成果の利用方法に関する戦略のとりまとめ（「技術戦略専門委員会報告書」、「同2006」）に尽力。 また、日本セキュリティ・マネジメント学会及び情報ネットワーク法学会等の役職を務め議論を主導しているほか、ASP・SaaSの情報セキュリティ対策及びIPネットワークの脆弱性対策など、我が国の安心・安全なネットワーク環境の構築に向けた活動において顕著な功績・功労があった。
神奈川県藤沢市 （地方公共団体）	「藤沢市情報セキュリティポリシー」等に基づく内部・外部監査を実施し、国際規格の情報セキュリティマネジメントシステム（ISMS）の認証を先行的に取得するとともに、シンクライアントや生体認証の導入、IT-BCP策定に取り組むなど、先進的な取組みは他の地方公共団体等の模範となる顕著な功績があった。 また、全職員を対象とした研修や訓練により、そのセキュリティ意識の改革を図るとともに、市民に対するボランティアやNPOと協働したセキュリティ相談窓口の設置、地域における広報啓発行事の開催に取り組み、他の地方公共団体等の模範となる顕著な功績があった。
国立情報学研究所（国立大学法人等における情報セキュリティポリシー策定作業部会）及び電子情報通信学会（ネットワーク運用ガイドライン検討ワーキンググループ）	情報セキュリティ対策において、高等教育機関を取り巻く社会情勢の変化を踏まえるとともに、各機関で情報セキュリティ対策を検討する上で、具体的な参考事例として役立つよう、高等教育機関に適した標準的かつ活用可能な情報セキュリティ規定群（高等教育機関の情報セキュリティ対策のためのサンプル規定集）を両団体が共同で策定し、セキュリティ水準の維持、向上に貢献した。
特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）	ネットワークセキュリティ製品を提供しているベンダー、システムインテグレータ、インターネットプロバイダーなどの情報セキュリティに携わるベンダーが結集した特定非営利活動法人（NPO）として、各事業者が抱える問題解決のための事例等の調査、各種セミナーの開催、不正アクセス対策ガイドラインの作成など、情報セキュリティ対策の向上に顕著な功績があった。 また、情報セキュリティ教育事業者連絡会の事務局を担当するほか、全国各地のNPO等とのネットワークも構築し、情報セキュリティに関する事業者や一般利用者の対策の推進、意識の向上に多大な貢献をした。

※　年齢は平成20年2月4日（表彰日）現在

「政府機関の情報セキュリティ対策のための統一基準（第3版）」の決定について

経　　緯

第15回情報セキュリティ政策会議（H19.12.12）

○ 政府機関の情報セキュリティ対策のための統一基準（第3版）（案）について審議を実施、
パブリックコメントに付すことを決定。

- ■ 実　施　期　間　：　平成19年12月12日（水）　～　平成20年1月10日（木）
- ■ パブリックコメント総数　：　6件【内訳　企業・団体・大学　：　6件、　個人　：　0件】
- ■ 施策実施にあたっての配慮・要望として、無線ＬＡＮの利用やIPv6技術の導入等について意見の提出あり。

パブリックコメントの結果

パブリックコメント案において既に記載済み等の理由により、文章の修正に至らず、原案どおり。

第3版改訂内容の概要

1 **ドメインネームシステム（DNS）に関する対策（新規）**
　DNSへの攻撃によるウェブ、電子メール等の政府機関サービスの妨害等への対策を追加

2 **監視機能（遵守事項追加）**
　情報セキュリティ侵害の予防、対処、抑止を目的とした監視に係る対策を追加

3 **政府機関サイトへの成りすまし対策（新規）**
　成りすましサイト対策として、政府機関で使用するドメイン名に関して規定

別紙2

暗号の安全性低下への対応

1　現状と課題

①電子政府システムでは、電子署名等のために暗号が使用されており、SHA-1及びRSA1024と呼ばれる暗号方式を広く使用。
②しかし、このSHA-1及びRSA1024は、安全性の低下が指摘されており、より安全な暗号方式への移行が必要。
③より安全な暗号方式への移行にあたっては、情報システムの相互運用性確保や政府全体の情報セキュリティの向上のため、政府統一的な移行指針を策定することが必要。

2　暗号の移行指針（案）の概要

①技術的な対応

【政府認証基盤とそれに依存する各府省庁の情報システム】

- ○ 相互運用性確保のため、新旧暗号方式の双方に対応し、適切な時期に暗号方式を切り替える運用を可能に。
- ○ 新たな暗号方式として、SHA-256及びRSA2048を採用。
- ○ 移行完了前に安全性低下の影響が発生する場合に備え、緊急避難的な対応も想定。

【上記以外の情報システム】

- ○ 現実的な脅威となる攻撃手法が示された時点で、速やかに別の暗号方式に変更する等の対応措置を可能とする。
- ○ 新たな暗号方式は、より安全なものを各府省庁において判断し決定する。

②制度的な対応

- ○ 各府省庁において次を実施
  ・システムの移行時期を踏まえ、必要な対応の取りまとめ
  ・移行手順書の整備

③スケジュール

- ○ 内閣官房、総務省、法務省、経済産業省等
  新たな暗号方式へ切り替える時期等を2008年度中に検討。
- ○ 内閣官房、総務省等
  相互接続の技術要件、緊急避難対応等について2008年度中に検討。
- ○ 各府省庁
  2010年から2013年までの間に、各情報システムの対応を完了。
- ○ 内閣官房、総務省、経済産業省
  安全性の状況を監視し、必要な情報を速やかに各府省庁に提供。

別紙3

セキュリティ・バイ・デザイン［ＳＢＤ］の検討状況について

1　これまでの経緯

前回政策会議（12月）にＮＩＳＣ素案を提示して議論
【主な課題】
○　政府機関統一基準については、ゴール（基準）のみの提示に留まり、ゴールへ至る方法（過程や具体的な進め方）が不明。

主な指摘
○各府省庁の主体的な取組みを促すような進め方にすべき。
○官のみでなく官民連携の下でのＳＢＤ確立が望ましい。

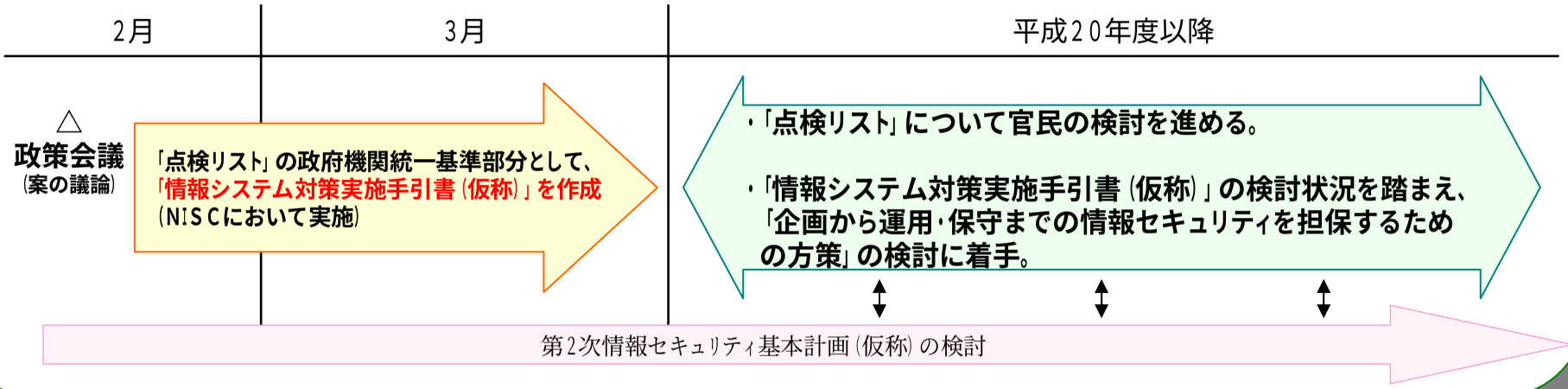
2　検討状況と今後のスケジュール

①進め方について

各府省庁において取り組まれている既存の枠組みに留意しつつ、段階的に進める。
平成19年度は「企画から運用・保守までの各段階における点検リスト」（以下、「点検リスト」という。）の一部として、「政府機関統一基準のうち情報システムに関する遵守事項についての実施手引書」（以下、「情報システム対策実施手引書」という。）を作成する。

【平成19年度】「点検リスト」の一部として、統一基準の遵守事項（システム要件に関するもの）について、システムの企画から運用・保守までの各段階における実施について参考となる情報を記載した「情報システム対策実施手引書（仮称）」をＮＩＳＣにおいて作成。
【平成20年度以降】「点検リスト」について各府省庁や民間等との検討を進める。これらの検討状況を踏まえ、「企画から運用・保守までの情報セキュリティを担保するための方策」の検討に着手する。

②検討スケジュール（イメージ）



別紙４

「情報セキュリティ分野における国際協調・貢献に向けた取組み」
～取組みの5つの方向性と進捗状況～

NISC

○経済関係の深化が進むアジア地域のビジネス環境向上に向けた協調・貢献の推進（セキュア・アジアビジネス環境（Secure Asian Business Environment）構想）

・セキュリティ文化の醸成やセキュリティ水準の向上等を通じ、安心・安全に事業活動を行えるような環境の整備

・人材育成や啓発、セキュリティ対策のベストモデルの普及等の協調・貢献を行うとともに、域内各国による自発的な啓発活動を促進

○情報セキュリティに係る新しい諸権利に係る検討及び議論への貢献

・自由なIT利用との関係や、IT利用に起因する脅威によって被害を受けた者の救済等の観点から、グローバルな議論に貢献

○サイバー攻撃等、ITに起因する脅威への対応のための取組みの推進（リスクのないICT（ICT Risk - Free）構想）

・サイバー攻撃等、ITに起因する脅威に関して、ハイレベル等で問題意識を共有し、適切に対処すべく議論に積極的に参加・貢献

・国境を越えたサイバー犯罪対策について、多国間における議論を引き続き促進

○情報セキュリティに係るグローバルなルールや標準の形成への貢献

・我が国の情報セキュリティに関する取組みの優れた点を把握し、ベストプラクティスと言えるような取組みルール等を明確化

・国際的なフォーラム等での議論に積極的に参加し、貢献

○様々な国際フォーラム等における提案や議論への積極的な参加

・必要な情報を適時適切に入手できるよう、既存のグローバルな取組みについても、より積極的に参加・関与

・国際協力・貢献の一環として、多国間のフォーラムの開催場所として貢献するなど、多国間のフォーラムを主導すべく努力

我が国としての取組み

○経済関係の深化が進むアジア地域のビジネス環境向上に向けた協調・貢献の推進
（セキュア・アジアビジネス環境 (Secure Asian Business Environment) 構想）

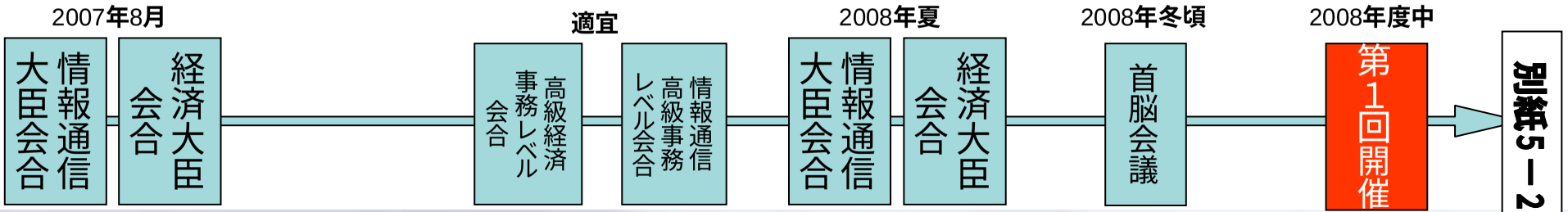
- ２００７年８月に開催された、日・ASEAN情報通信大臣会合（田村総務副大臣出席）、経済大臣会合（甘利経済産業大臣出席）において、「アジア情報セキュリティ政策会合（仮称）」の創設に向けた提案が行われた。
- 我が国は、２００８年度内の当該会合の招致のため、必要な予算確保等を含めた取組を推進中。

２００８年度中に以下を軸とした第１回会合を日本において開催予定。

①高級事務レベルにおける日・ASEAN間の政策対話

②国際的な研究機関等を活用した政策研究、普及啓発

③成果を活用した日ASEANの協力強化



我が国としての取組み

NISC

○サイバー攻撃等、ITに起因する脅威への対応のための取組みの推進
（リスクのないICT（ICT Risk - Free）構想）

- 2007年8月に米国（DHS）との間で日米サイバーセキュリティ会合を開催。日米で協力してAPEC、G8等の国際会合の場でITに起因する脅威への対応のための取組みの推進を行う必要があるとの認識を共有。
- OECD等の国際会合の場で、ICTインフラの信頼性、堅牢性の向上のための国際協力の必要性を求める議論が開始。
- 2007年10月に開催されたARF (ASEAN Regional Forum)のセミナーにおいて、サイバー空間の安全を確保するためのWGの立ち上げを合意。

*アジア太平洋地域における政治、安全保障分野を対象とする全域的な対話のフォーラム。

① **ICTが社会、経済活動に不可欠なインフラとなりつつあることを受け、主要な先進国のハイレベルで問題意識を共有する。**

② **サイバー攻撃等、ICTに起因するリスク、脅威については、既存の取組（CERT組織の取組等）を加速する。**

CEPTOAR-Council（セプターカウンシル）創設に向けた検討の場の開催状況

開催状況

◆1月までに、8回の会合を開催。3月に最終会合を開催予定。

メンバー

◆CEPTOAR（セプター）代表者（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービスの各分野）
◆CEPTOAR整備を進めている業界団体代表者（水道、物流の各分野）

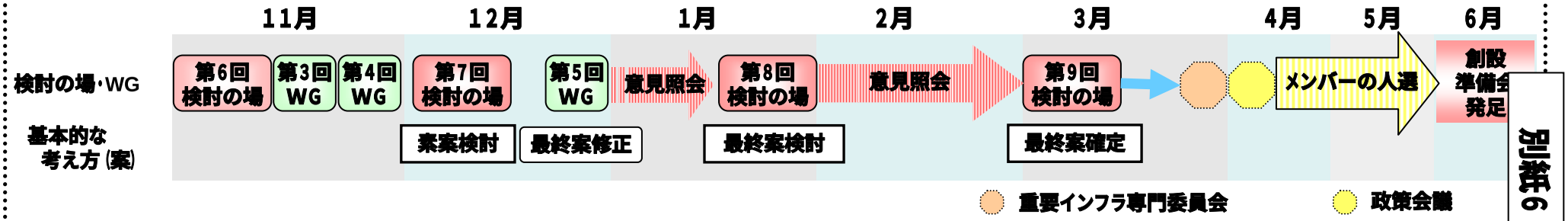
オブザーバ

◆重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）
◆CEPTOAR代表者の選出した者（CEPTOAR代表者の随行者等）

主な検討内容

◆「重要インフラ連絡協議会（ＣＥＰＴＯＡＲ－Ｃｏｕｎｃｉｌ）」（仮称）の創設についての基本的な考え方（案）
◆CEPTOAR-Council創設準備会設置要綱（素案）
◆「「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）創設に向けた検討の場」における2007年度活動のまとめ（素案）

＜基本的な考え方（案）のとりまとめに向けた想定スケジュール＞



別紙6

1. 2007年度分野横断的演習の概要

1. 日時　2008年2月6日(水)

2. 場所　(株)三菱総合研究所　2階セミナー室　他

3. 参加者

(政府)

岩城内閣官房副長官(予定)、内閣官房情報セキュリティセンター、重要インフラ所管省庁

(重要インフラ分野)

情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

(CEPTOAR)

7分野11CEPTOAR

(関係機関)

(分野横断的演習検討会有識者)

大林 慶應義塾大学教授(座長)ほか、検討会有識者

別紙7－1

2. シナリオの概要

目的

IT障害発生時の重要インフラのサービスの維持･早期復旧に向けた現状の情報共有の仕組みの検証

(具体的な目的)

大規模なサイバー攻撃時に、被害を最小化する。具体的には、重要インフラ事業者のサイバー攻撃に対する準備機能と、重要インフラ事業者･所管省庁･NISCにおける情報提供機能及び情報連絡機能の検証を目的とする

検証課題

・サイバー攻撃が発生した場合の当該重要インフラ事業者における関係者を含めた対応方法

・サイバー攻撃が発生した場合の当該重要インフラ事業者、CEPTOAR、所管省庁、NISC間の情報連絡及び情報提供の方法

・NISC、所管省庁から他分野のサイバー攻撃の情報提供を受けた場合の、各重要インフラ事業者における重要システムでの影響の検証方法

・事象収束後のCEPTOARを経由した情報共有の方法

事象概要

重要インフラ事業者のサイトが、ボットネットによるDDoS (Distributed Denial of Service) 攻撃を受け、数時間程度、ホームページの閲覧不能や重要システムの影響が発生したという想定で、官民における連絡･連携、情報共有の仕組みを検証

別添7－2

「第一次提言」（仮称）策定までの進め方について（案）

NISC

第１回　【１月16日水曜日　13時00分～15時00分】

○　検討項目例の紹介及び今後のスケジュールについて（事務局）
○　ヒアリング事項の検討
○　自由討議

第２回　【２月14日木曜日　15時00分～18時00分】
第３回　【２月21日木曜日　16時00分～19時00分】

○　ヒアリングの実施（各府省庁及び地方公共団体／重要インフラ／産業界／消費者団体／法曹団体）
○　自由討議

第４回　【３月19日水曜日　13時00分～16時00分】

○　論点整理（事務局）
○　自由討議

第５回　【３月下旬～４月上旬】

○　「第一次提言」（仮称）案の検討
○　自由討議

第６回　【４月中旬】

※　予備日程

別紙8－1

基本計画検討委員会　委員名簿

委員長	須藤　修	東京大学大学院情報学環・学際情報学府教授
委員	有賀　貞一	株式会社CSKホールディングス代表取締役
	井川　陽次郎	読売新聞東京本社論説委員
	井上　雅博	ヤフー株式会社代表取締役社長
	筧　捷彦	早稲田大学理工学術院教授
	木内　里美	大成建設株式会社社長室理事情報企画部長
	重木　昭信	株式会社NTTデータ代表取締役副社長執行役員
	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
	神保　謙	慶應義塾大学総合政策学部専任講師
	関　正樹	関彰商事株式会社代表取締役社長
	高橋　伸子	生活経済ジャーナリスト
	富永　新	日本銀行金融機構局考査役兼企画役システム関連考査担当総括
	中尾　康二	テレコム・アイザック推進会議委員（KDDI株式会社情報セキュリティフェロー）
	深谷　聖治	東日本旅客鉄道株式会社総合企画本部システム企画部長
	満塩　尚史	環境省情報化統括責任者（CIO）補佐官 （各府省情報化統括責任者(CIO)補佐官等連絡会議情報セキュリティワーキンググループリーダー）
	宮地　充子	北陸先端科学技術大学院大学情報科学研究科教授
	三輪　信雄	綜合警備保障株式会社参与
	安冨　潔	慶應義塾大学大学院法務研究科（法科大学院）・法学部教授
	和貝　享介	監査法人トーマツ

このほかに情報セキュリティ政策会議有識者構成員（その代理人を含む）も必要に応じ会議に出席し意見を述べることができる。

別紙8－2

「安全基準等の見直し状況等の把握及び検証」の概要

○2006年度、重要インフラ10分野において「安全基準等」の策定・見直しが行われ、内閣官房にて安全基準等の策定状況の把握・評価を実施（2007年4月23日 情報セキュリティ政策会議）。

○定常的なIT障害の発生状況の把握を通じて、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行った結果、「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」を改定（2007年6月14日 情報セキュリティ政策会議決定）

○改定された指針に基づき、各重要インフラ分野においては「安全基準等」の見直しを実施。

○NISCにて「安全基準等」の策定状況の把握及び検証を実施。

セキュア・ジャパン 2006
（2006年6月15日情報セキュリティ政策会議決定）
【具体的施策】

イ）「安全基準等」の策定状況の把握及び評価（内閣官房）

ウ）指針の見直し（内閣官房）

重要インフラにおける安全基準等の整備状況について把握及び評価の実施（報告：2007年4月23日情報セキュリティ政策会議）

・行動計画策定時点において、安全基準等が存在しなかった分野も含め、全ての分野において安全基準等の策定・見直しが完了。
・指針の各項目が規定する必要が無い場合を除き、各安全基準等に盛り込まれており、指針との対応が取れていることを確認。

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の見直し
（改定：2007年6月14日情報セキュリティ政策会議決定）

・定常的なIT障害の発生状況の把握等を通じて、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行う等見直しの結果、該当する10カ所について指針の改定を実施。

セキュア・ジャパン 2007
（2007年6月14日情報セキュリティ政策会議決定）
【具体的施策】

ア）各重要インフラ分野の安全基準等の策定・見直し
a)安全基準等の見直し

b）「安全基準等」の見直し状況等の把握及び検証

イ）各重要インフラ分野における「安全基準等」の浸透状況等に関する調査の実施

ウ）指針の見直し

別紙9－1

19

まとめ

重要インフラ10分野で安全基準等の見直しが実施されており、重要インフラにおける情報セキュリティ対策が着実に前進

①「安全基準等」の見直し状況等
　指針改定を踏まえた安全基準等の見直しを重要インフラ10分野で実施

各分野毎の安全基準等のPDCAサイクルにおいて、各分野毎の独自の観点に加えて、政府の指針の観点を盛り込んだ見直しが進展

②「指針」との対応状況の検証
　指針改定箇所について重要インフラ10分野で対応していることを確認

同一指針に基づく分野横断的な検証によって、各分野毎の安全基準等の特徴等が明らかになり、分野間でのノウハウの共有が進むことが期待

③「相互依存性解析」の成果を踏まえた検証
　情報通信（電気通信）分野及び電力分野への依存については現行の安全基準等に既に記載があるが、水道分野への依存については安全基準等への記載は1分野のみ

水道分野への依存については指針にも記載がないため、指針の見直しの際に記載の要否を検討

別紙9－2