報道発表

平成19年12月12日
内閣官房情報セキュリティセンター（NISC）

第15回情報セキュリティ政策会議の開催について

－政府機関の情報セキュリティ対策の実施状況等－

本日12月12日、「情報セキュリティ政策会議」（議長：内閣官房長官）の第15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、政府統一基準改定のパブコメ案と次期基本計画策定に必要な調査検討を行う基本計画検討委員会の設置。

1．政府機関の情報セキュリティ対策の実施状況に関する重点検査及び評価結果について

○　政府職員が外部等とメールを送受信するためのサーバであるメールサーバを対象とした重点検査（※1）を実施。

○　政府機関に設置・運用されているメールサーバは合計約1，900台も存在。

○　全19府省庁のうち、実施すべき対策が全て実施されている（実施率100％）府省庁は、10府省庁。

○　平成20年度中には全府省庁が実施率100％予定。

○　今後とも、政府機関において着実かつ計画的な情報セキュリティ対策が図られるよう必要な評価や調査を実施予定。

（別紙1参照）

※1　重点検査とは、「政府機関の情報セキュリティ対策のための統一基準」において必須の対策とされている基本遵守事項の中でも特に重要な事項に着目し、その実施状況を重点的に検査するもの

2．次期情報セキュリティ基本計画（仮称）の検討について（政策会議決定）

○　我が国における情報セキュリティ問題を俯瞰した中長期の戦略である「第1次情報セキュリティ基本計画」（平成18年2月2日決定）は、平成20年度が最終年度。

○　官民における各種の取組み、技術革新の動向、制度改正などを含めた社会環境の変化を踏まえ、次期基本計画の策定に必要な調査検討を行う「基本計画検討委員会」を政策会議の下に設置することを決定。

○　第一次基本計画は体制整備を中心とした我が国の情報セキュリティ政策の取組み開始に重点を置いたが、平成21年度からの次期計画の策定においては、高度情報通信ネットワーク社会を迎えた我が国に適した「情報セキュリティ政策」を幅広く検討予定。

○　同委員会は、1月より検討を開始し、議論の状況を政策会議に報告。

○　政策会議及び検討委員会での検討スケジュール

平成20年　1月　第1回委員会
2～3月　産業界、消費者、府省庁等の関係者からのヒアリング
4月　「第1次提言（仮称）」
12月　「第2次基本計画（仮称）」(案) パブコメ
平成21年　1月　パブコメ締切
2月　「第2次基本計画（仮称）」決定

○　検討項目（例））

情報セキュリティ政策の意義・目的・範囲、状況変化・現状認識、対象分野の設定、推進体制、国際動向その他

（別紙2参照）

３．政府機関の情報セキュリティ向上のための施策について

（1）「政府機関の情報セキュリティ対策のための統一基準」の第3版への改訂（※2）について

○　パブリックコメント案の主な内容は次のとおり。

①　ＤＮＳ（※3）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の追加

②　政府関連への成りすまし対策として、政府機関で使用するドメイン名に関する対策の追加

○　本案について広く意見を募集した上で、来年2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。

（別紙3参照）

※2　「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。

※3　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。

⑵　セキュリティ・バイ・デザイン［SBD］について
（「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」）

ア　取組みの趣旨

電子政府として構築が進みつつある各種業務システムに対して適切に情報セキュリティ要件を取り入れることは必要不可欠（「セキュア・ジャパン2007」の重点施策）。今回の会合では、NISC素案を提示し議論。

イ　現状と課題

・　行政情報システムの最適化が進められているものの、情報セキュリティの観点からは、具体的取組みが明らかにされていないのではないか。

・　政府機関統一基準の目標達成までの「過程」及び「具体的な進め方」が不明確。

ウ　今後の予定

これまでの議論を基に、引き続き各府省庁と調整しつつ、来年2月に予定されている次回会合においてパブリックコメント案を事務局から提案予定。

（別紙4参照）

4．その他

⑴　「平成19年度情報セキュリティの日」表彰等について

○　本年度も前年度に引き続き、情報セキュリティの日（毎年2月2日）の前後に、情報セキュリティの日功労者表彰を実施予定。

○　「情報セキュリティ啓発推進委員会」（※4）を立ち上げ、関係各省庁の協力を得つつ、本年度の表彰者を選考。

○　情報セキュリティの日にあわせて関係省庁や民間企業の強力を得て各種関連行事の開催を予定。現在、昨年度の実績（312件）を超えるべく、12月20日まで関連行事を鋭意募集中。

※4　「情報セキュリティ啓発推進委員会」メンバー（敬称略、50音順）

岡村　久道　　弁護士/国立情報学研究所客員教授
桑子　博行　　社団法人テレコムサービス協会サービス倫理委員会委員長
辻井　重男　　情報セキュリティ大学院大学学長
土居　範久　　中央大学教授/日本学術会議副会長
滑川　恵理子　株式会社サンケイリビング新聞社編集企画部長

（別紙5参照）

(2)　静的相互依存性解析（※5）の総括について

○　「情報通信分野（通信）」（他の6分野と）や「電力分野」（他の10分野と）だけでなく、「水道分野」も他の8分野と相互依存性があることが判明。

○　その他の分野間については、関係性が明確にならなかったケースもあり、今後の相互依存性解析の中で引き続き検討予定。

（別紙6参照）

※5　重要インフラの IT 障害が、分野横断的に相互に与える影響（相互依存）を定性的に分類、定量的に評価するもので、静的解析はある時点における相互依存性を分析するもの。 IT を介した相互依存関係の時系列変化の様子を分析する動的解析は今後実施予定。

【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（NISC）のホームページにおいて公表。
（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku15）

※　「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）

今回の重点検査の概要

1. 検査対象機関・システム等 ： 全19府省庁（本省及び地方支分部局）の情報システム

内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、警察庁、金融庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省

2. 検査期間 ： 平成19年9月（調査票配布）から同年11月（平成19年9月末時点の実施状況を検査）

3. 検査方法 ： NISCが配布した調査票に基づき、各府省庁が電子メールサーバについて内部調査を行い回答。両者間で回答内容の確認作業等を行い、NISCから11月中旬に評価結果を各府省庁に通知。各府省庁は改善のための方針等を検討。

府省庁外との電子メールの送受信に係わるサーバ装置について、不正プログラム対策、サーバ管理、不正アクセス対策、情報保護対策の4つのカテゴリーに関して検査（対象台数約1900台）。

電子メールサーバに関する重点検査項目	
不正プログラム対策	・OSのセキュリティパッチ適用状況（アップデートの状況） ・電子メールサービス提供ソフトウェアのセキュリティパッチ適用状況（アップデートの状況） ・電子メールコンテンツに対する不正プログラム対策の状況
サーバ管理	・電子メールサーバの管理者に対する認証等の実施状況 ・電子メールサーバの障害等の発生時における復旧対策の状況 ・時刻同期機能の動作
不正アクセス対策	・不正中継対策の状況
情報保護対策	・電子メールの受信に係わる利用者に対する認証等の実施状況

4. 評価方法 ：

各カテゴリーの平均実施率（項目毎に算出した対策実施率（※）の総平均値）の平均値を総合評価の実施率とした。

政府機関統一基準で求める情報セキュリティ対策がすべて実施されていれば、総合評価の実施率は100%、すなわち“A評価”となる。

$$（※）\ 対策実施率 = \frac{実際に情報セキュリティ対策を実施している対象数（メールサーバ台数）}{情報セキュリティ対策を実施すべき対象数（メールサーバ台数）} \times 100\ （\%）$$

別紙1－1

電子メールサーバに関する情報セキュリティ対策の総合評価

重点検査の項目

電子メールサーバに関する重点検査項目	
不正プログラム対策	・OSのセキュリティパッチ適用状況（アップデートの状況） ・電子メールサービス提供ソフトウェアのセキュリティパッチ適用状況（アップデートの状況） ・電子メールコンテンツに対する不正プログラム対策の状況
サーバ管理	・電子メールサーバの管理者に対する認証等の実施状況 ・電子メールサーバの障害等の発生時における復旧対策の状況 ・時刻同期機能の動作
不正アクセス対策	・不正中継対策の状況
情報保護対策	・電子メールの受信に係わる利用者に対する認証等の実施状況

・府省庁の調査に基づく結果
・平成19年9月末時点

総合評価	電子メールサーバ	（参考）端　末	（参考）ウェブサーバ
	平成19年9月末	平成19年3月末	平成19年3月末
内閣官房	B	B	B
内閣法制局	B	B	B
人事院	A	A	B
内閣府	B	B	B
宮内庁	B	A	A
公正取引委員会	B	A	A
警察庁	A	A	A
金融庁	A	B	A
総務省	B	B	B
法務省	B	B	B
外務省	B	A	B
財務省	A	B	B
文部科学省	A	A	A
厚生労働省	A	B	B
農林水産省	A	A	A
経済産業省	A	A	A
国土交通省	B	B	B
環境省	A	B	A
防衛省	A	B	A

評価	実施率	評価	実施率	評価	実施率	評価	実施率
A	x＝100%	B	80%≦x＜100%	C	60%≦x ＜80%	D	x＜ 60%

別紙１－２

電子メールサーバの評価結果を受けての対応完了予定

府省庁名	総合評価	平成19年度	平成20年度
内閣官房	B	→	
内閣法制局	B	→	
人事院	A	実施済み	
内閣府	B	→	
宮内庁	B	→	→
公正取引委員会	B	→	
警察庁	A	実施済み	
金融庁	A	実施済み	
総務省	B	→	→
法務省	B	→	→
外務省	B	→	→
財務省	A	実施済み	
文部科学省	A	実施済み	
厚生労働省	A	実施済み	
農林水産省	A	実施済み	
経済産業省	A	実施済み	
国土交通省	B	→	→
環境省	A	実施済み	
防衛省	A	実施済み	

※ 平成19年度中に対応完了予定 →
※ 平成20年度中に対応完了予定 →

別紙1－3

「基本計画検討委員会」の設置について

1．検討のための専門委員会の設置

（1） 3か年の中長期戦略「第1次情報セキュリティ基本計画」は平成20年度（2008年度）が最終年度。

（2） 残された課題
政府機関における情報セキュリティ事故、重要インフラにおけるIT障害の発生などは後を絶たず、企業等における情報セキュリティの具体的な対策や体制作り、人材の確保といった面でも解決すべき課題が多く残されている。

（3） 専門委員会設置
第1次基本計画が最終年度を迎えるにあたり、官民における各種取組み、技術革新や制度改正等を含めた社会環境の変化などを踏まえ、平成21年度（2009年度）からの情報セキュリティ政策の在り方・方向性について検討を行うため、情報セキュリティ政策会議の下に、「基本計画検討委員会」を設置。

2．専門委員会の構成と検討の進め方

（1） 下記のような各分野の者から構成する予定。

（法律分野専門家、技術分野専門家、サプライヤー（SIer、ISP、ベンダー）、ユーザ企業（重要インフラ、大企業、中小企業）、監査関係者（公認会計士）、国家安全保障論専門家、人材育成・資格制度関係者、電子政府・電子自治体専門家、消費者、NPO・NGO、メディア等）

（2） 情報セキュリティ政策会議の有識者構成員は、専門委員会に出席して、意見を述べることができるものとする。
また、専門委員会の検討状況については、適宜、政策会議・有識者会議等に報告するものとする。

別紙2－1

「次期情報セキュリティ基本計画（仮称）」に向けた検討スケジュール（案）

平成19年12月12日　第15回情報セキュリティ政策会議（委員会設置決定）

平成20年1月　　第1回委員会～以後、数回開催

2～3月　　産業界、消費者、府省等の関係者からのヒアリング

ワークショップ開催等の意見インプット機会の設定

4月　　「第一次提言」（仮称）（政策会議）

6、7月頃　検討再開～以後、数回開催

12月頃　　「第2次基本計画（仮称）」（案）（政策会議）、パブコメ

平成21年1月　　パブコメ締切

2月　　「第2次基本計画（仮称）」決定（政策会議）

別紙2－2

次期基本計画に係る検討項目（例）について

1.「情報セキュリティ政策」の意義・目的・範囲

- 本格的な高度情報通信ネットワーク社会を迎えた我が国に適した「情報セキュリティ政策」の構成要素と方向性の検討
- 社会に見られる様々な事象（システムダウン、物理的事故・災害、人的要因、犯罪行為、安全保障上のリスクなど）の検討
- 事前予防、問題発生時の対応体制、事後復旧の在り方など、「情報セキュリティ政策」の射程距離（めざすもの）をどのように設定するか。

2. 状況変化と現状認識

- この間、社会はどう変化したか（ネットビジネス、個人の利用状況、技術革新の動向等）
- 制度改正の状況、関連制度（個人情報保護、情報公開、知的財産権、会社・企業法制、取引法制、重要インフラに係る法制、労働法制等）との整合性確保

3. 対象分野の設定

- 対策4分野（政府、重要インフラ、一般企業、個人）と横断的事項（技術、人材、国際、犯罪対策・権利保護）の妥当性の検討（政策の継続性と見直しの必要性）
- 第1次基本計画の欠落部分（例えば地域、中小企業、安全保障の視点、重要インフラの範囲等）の検討

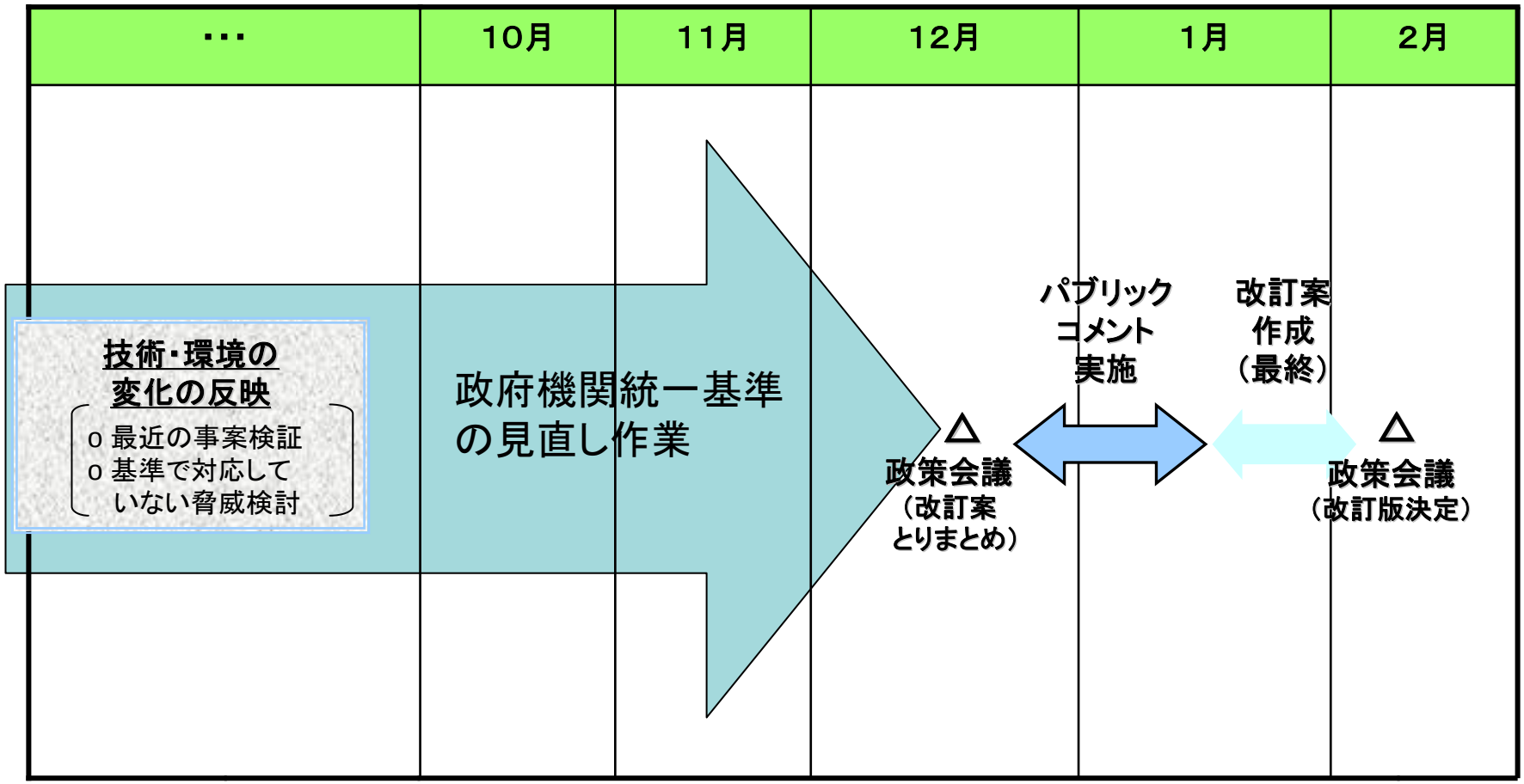
4. 推進体制・その他

- 政策推進体制の検討：政策会議、NISC、各府省の役割・機能その他の推進体制の在り方、関係会議・本部等との連携の在り方
- 国際動向・諸外国の政策との整合性、各国の参考事例等の採否　　等

別紙2－3

政府機関統一基準の改訂スケジュールについて

政府機関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定期的に見直しを行うこととされており、技術・環境の変化等を踏まえ、下記のスケジュールで見直し・改訂を実施



別紙３－１

政府機関統一基準　第3版　改訂案の概要

1. 技術・環境の変化の反映

1-1　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

1-2　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

1-3　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

2. 実務に即した見直し等

2-1　遵守事項の明確化

2-2　用語の整理

参考：　政府機関統一基準解説書の記述の明確化

○　国民等がPCにダウンロードするソフトウェアの安全性確保について解説を充実

別紙3－2

セキュリティ・バイ・デザイン（SBD）について（案）

1. 現状と課題

①「最適化指針（CIO連絡会議）」に基づいて行政情報システムの最適化が進められているものの、情報セキュリティの観点からは、具体的取組みが明らかにされていないのではないか？
②政府機関統一基準によって、各府省庁が遵守すべき事項を明確化している一方、統一基準第4部、第5部において、どのような取組みを行うことが目標達成となるのか、目標達成までの「過程」及び「過程の進め方」が明らかではないのではないか？

2. 今次の取組み（案）

ア）「最適化指針」の補完など、行政情報システムの情報セキュリティの取組みを進めるべく、 また、
イ）政府機関統一基準の目標の実現に必要な取組みを容易化することで、行政情報システム全体にセキュリティの観点から必要な要素を確実に盛込むとともに、過剰・不要なセキュリティ投資を防止するべく、

①「情報セキュリティの観点から見た望ましい行政情報システムのあり方」について示す
②新しく構築される個々の行政情報システムについて、（利便性や効率性とのバランスを維持しつつ）情報セキュリティの観点を着実かつ容易に盛込めるような取組みを進める［構築の各段階における点検リストの作成］
③企画から運用・保守まで行政情報システムの情報セキュリティを担保するための方策を示しこれの実現を目指す

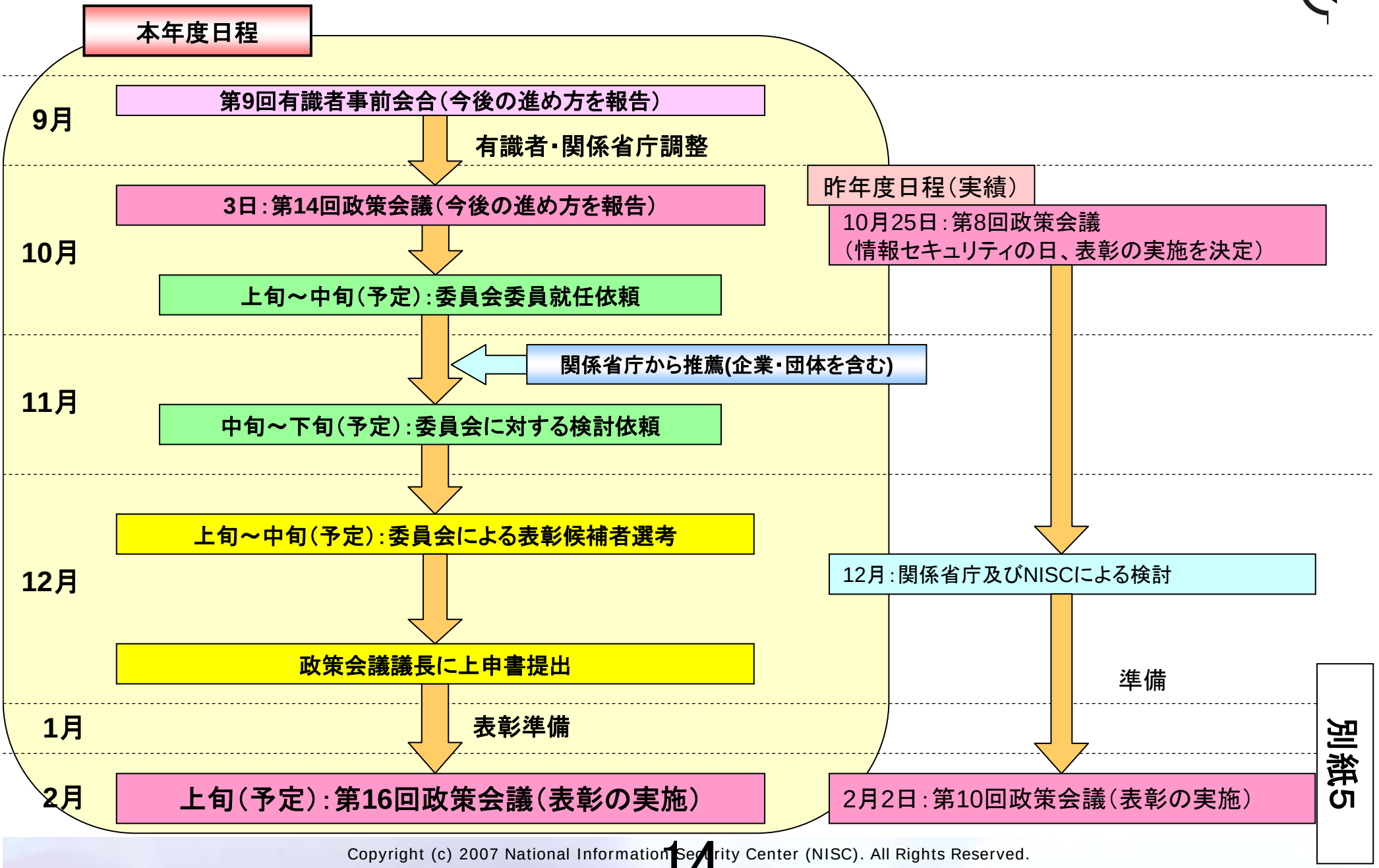
3. セキュア・ジャパン2007での記述（2008年度の重点施策部分）

・電子政府の情報セキュリティを企画・設計段階から確保する（Security by design）ための方策の強化
【内閣官房、総務省及び関係府省庁】

電子政府として構築が進みつつある各種業務・システムに適切に情報セキュリティ要件が取り入れられることは必要不可欠であり、情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策を強化する。

別紙4

平成19年度情報セキュリティの日功労者表彰の進め方



静的相互依存性解析の総括の目的と考え方

静的相互依存性解析の総括の目的

- 2006年度の調査における静的相互依存性解析の結果等に対する認識の共通化
- 上記に基づく動的相互依存性解析へのインプットの整理

静的相互依存性解析の総括の進め方

- 「相互依存性」を明確化するための視点の整理
- 「分野の特性」、「分野間の関係性」の整理に基づく分野間の相互依存性の明確化

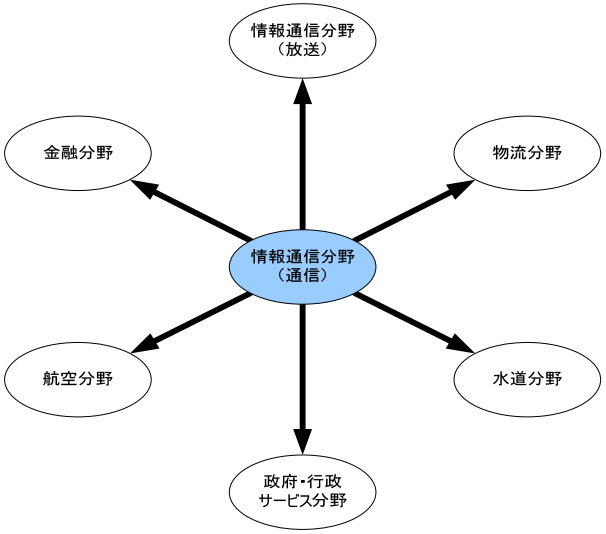
別紙6－1

静的相互依存性解析の検討結果

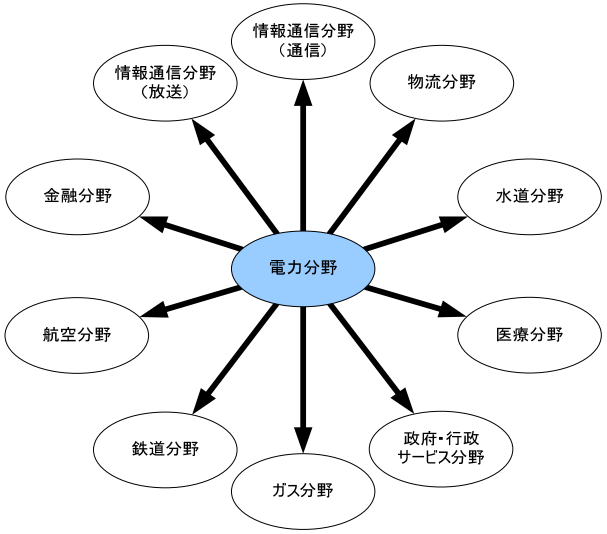
◆本総括では整理した視点に基づき、相互依存性を次のように捉える
- ある重要インフラ分野にIT障害が生じた場合に、他の重要インフラ分野に影響が波及する場合。
- ある重要インフラ分野にサービスの停止や機能の低下等が生じた場合に、他の重要インフラ分野の重要システムに影響が波及する場合。

◆相互依存性解析の結果、下図に示すように、「情報通信分野（通信）は他の6分野と」、「電力分野は他の10分野と」、「水道分野は他の8分野と」相互依存性があることが明確になった。　注：情報通信分野については、「通信」と「放送」の2分野にわけて検討した。

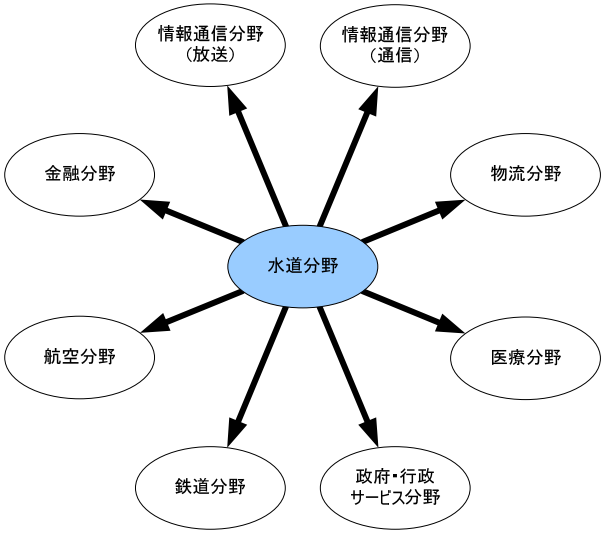
◆上記以外の分野間においても、相互依存性の可能性はあるものの、その関係性と波及が必ずしも明確にならなかったケースもあり、それらについては今後の相互依存性解析の中で検討を深めていく。



通信分野と他分野との相互依存性



電力分野と他分野との相互依存性



水道分野と他分野との相互依存性

※上記相互依存性関係において、一般的には各分野におけるサービスに影響しないよう、適切な対策がとられている。

※上記における各分野に係る記載は、各分野の主要な事業者へのヒアリングに基づくものであることに留意が必要である。

凡例　A分野 → B分野

A分野のサービスの停止や機能の低下等により、B分野の重要システムが機能不全（定常運用ではない状態）に陥る

別紙6－2