報道発表

平成19年10月3日
内閣官房情報セキュリティセンター（NISC）

第14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10月3日、「情報セキュリティ政策会議」（議長：内閣官房長官）の第14回会合が開催され、その概要は次のとおり。

1．「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」（政策会議決定）

近年、国民生活、社会経済活動が、ボーダーレスに世界と繋がっているIT基盤への依存を強めている状況を踏まえ策定。

具体的には、

- 経済関係の深化が進むアジア地域での企業活動や投資を支援するため、我が国が主体となって情報セキュリティ水準の高いビジネス環境（セキュア・アジアビジネス環境構想）の構築支援を推進
- G8等の国際会議のハイレベルでサイバー攻撃等ITに起因する脅威への対応をより一層促進することを目指すこと（リスクのないICT構想）

等について、政策会議で決定。

本決定は、各地域又は情報セキュリティ政策領域に応じて、我が国が国際協調・貢献をどのように進めていくのかの政府横断的な基本方針となるもの。

（別紙1参照）

2．電子政府の安全性確保に向けた取組み（JRE問題等への対応）

（1） JRE問題への対応

NISCでは、7月に緊急調査を行ったJRE（※1）の脆弱性の問題について、8月に全府省庁（19機関）にヒアリングを実施し、その結果を踏まえた対応策について検討した。

※1 JREとは、「Java Runtime Environment」の略であり、Java（特定のOSに依存しないプログラミング言語）アプリケーションを利用するために必要なユーザ側にインストールされるソフトウェアのセットのこと。

ア　当面の対応として

システムを運用している府省庁は、脆弱性が判明した時点で利用者に注意喚起を行う。また、速やかにシステム改修について検討を行い、改修までの間は利用者に危険が及ばないよう適切な対処を実施。

イ　今後の対応として

情報システムの企画・設計段階から必要なセキュリティの検討を行うことが適当。このため、NISCでは「セキュリティ・バイ・デザイン」の一部としてこの問題を検討。

(2) 重点検査の実施

端末・ウェブサーバの重点検査に続き、政府職員が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を9月より実施中。12月の政策会議において報告予定。

(3) 政府機関統一基準の改定

DNS(※2)を利用したDoS攻撃(サービス不能攻撃)等が生じている状況を踏まえ、DNSサーバの設置と運用管理に関する政府機関統一基準の改定案を12月の政策会議に諮る予定。

(別紙2参照)

※2　DNSとは、「Domain Name System」の略であり、ホスト名(例：nisc.go.jp)とIPアドレス(例：202.221.60.XXX)の対応付けを行うシステムのこと。

3．平成20年度情報セキュリティ関連予算概算要求状況

各府省庁における平成20年度予算の概算要求のうち、情報セキュリティに関係しているものは次のとおり。

(1) 平成20年度概算要求額は338億円、平成19年度の当初予算(300億円)と比較して38億円、13%増。

(2) 施策の内訳　(平成19年度当初予算→平成20年度概算要求)

- 電子政府の安全性　190億円→229億円(39億円増、21%増)
- 電子自治体の安全性　0．8億円→2．8億円(2億円増、250%増)
- 重要インフラ(※3)関係　4．6億円→5．1億円(0．5億円増、11%増)
- 企業関係　15億円→16億円(1億円増、8%増)
- 個人関係　15億円→27億円(12億円増、80%増)

(別紙3参照)

※3　重要インフラとは、「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」の10分野を指す。

4．情報セキュリティの日（2月2日）に係る表彰式の開催

本年度も前年度に引き続き、2月2日の情報セキュリティの日の前後に、情報セキュリティの日功労者表彰を実施する。

情報セキュリティの日にあわせて各種行事を積極的に開催予定。

（別紙4参照）

5．その他

（1） 年度計画「セキュア・ジャパン2007」の進捗状況（上半期）

今年度中に実施することとなっている全159施策について

- 「既に実施済み」　27施策（17%）
- 「実施中であり、年度内に完了予定」　111施策（70%）
- 「実施はまだであるが、年度内に完了予定」　18施策（11%）
- 「年度内に実施できるか不明」　3施策（2%）

（別紙5参照）

（2） 情報セキュリティ政策・2007年度の評価等に向けた「作業方針」の策定

情報セキュリティ政策のPDCAサイクルにおけるCHECK段階の作業方針を定めたもの。分野別の評価指標、補完調査の項目及び関係府省庁を記載するとともに分析課題・方法、スケジュール等を内容としている。

この方針に基づく評価結果は、年度計画「セキュア・ジャパン2008（仮称）」や平成21年度からの「第2次情報セキュリティ基本計画（仮称）」の策定に活用する。

（別紙6参照）

【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（NISC）のホームページにおいて公表。

（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku14）

※　「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）

国際協調・貢献に向けた取組みの経緯

○ 情報セキュリティ政策会議等における検討

・情報セキュリティ政策会議等の場で、有識者構成員等から、「我が国の情報セキュリティの取組みの国際展開が必要」との度重なるご意見。

・「第１次情報セキュリティ基本計画」をもとに、「セキュア・ジャパン2007」において、国際戦略の基本方針を2007年度に策定することを明記。

○ 経済財政諮問会議等における検討

・平成19年4月20日、官房長官から、「ITによる生産性改革を支えるセキュリティ基盤の重要性-国内対策の推進と国際的な政策展開-」を発表。

・「成長力加速プログラム」（平成19年4月25日）において、情報セキュリティ分野の国際戦略を7月までに策定することを決定。

・「経済財政改革の基本方針2007」（平成19年6月19日、いわゆる骨太の方針）において、「情報セキュリティの向上に向け、（中略）各国との連携・協力等を推進する。」ことを明記。

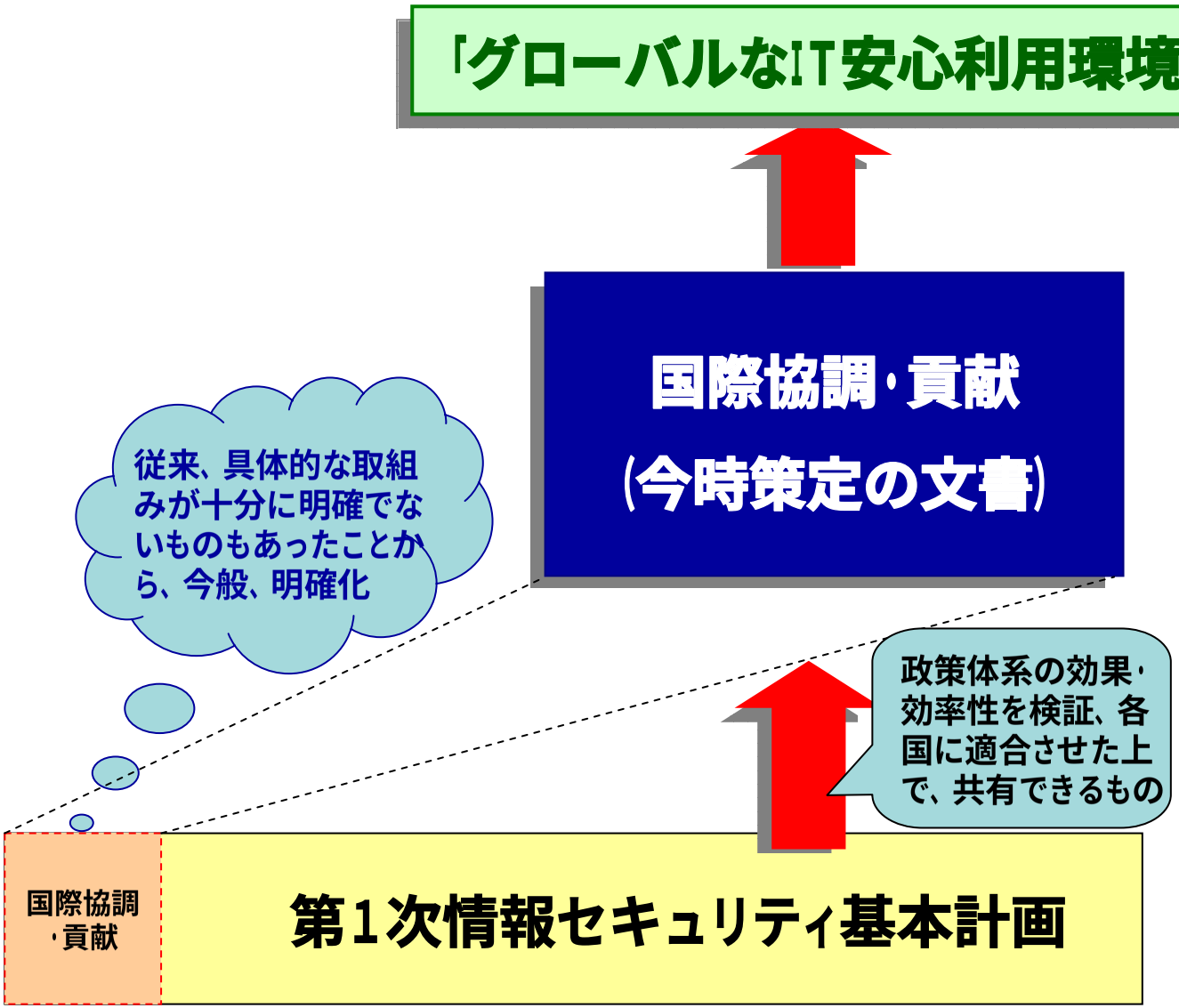
○ 国際協調・貢献に向けた取組みの策定

・以上の状況を踏まえ、平成19年8月3日の政策会議において、これまでの作業や調整等を踏まえ、中間報告を提出。

・政策会議での議論を踏まえ、速やかに具体的施策を盛り込んだ上で、各省庁の協力を得て、国際協調・貢献に向けた取組みを決定。

別紙1－1

「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」の位置付けと基本的な考え方



IT基盤は、24時間・365日、世界とつながっている(IT基盤のボーダーレス性)ため、「グローバルなIT安心利用環境」が重要

①IT利用に係る世界のトップランナーとして、「グローバルなIT安心利用環境」の構築に大きな貢献を行うべき

②「グローバルなIT安心利用環境」の実現が、ひいては我が国の国民生活・社会経済活動の安心を確保することにつながる

別紙1－2

「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～

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

別紙1－3

政府機関対策に関する２００７年度下半期の主な取組みについて

NISC

1　重点検査の実施

○　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を9月上旬より実施。
○　１２月の政策会議において報告予定。

2　政府機関統一基準の改定

○　ＤＮＳ(Domain Name System)はメールやウェブを含めたインターネットの基盤をなすものであるが、昨今ＤＮＳを使用したサービス不能攻撃（ＤｏＳ）等が生じている状況を踏まえ、毎年の見直しの一環として、ＤＮＳサーバに関する事項の追加等について検討しているところ。
○　１２月の政策会議において改定案を諮る予定。

3　ＪＲＥ問題への対応

○　政府機関の電子申請システム等広く国民に向けて公開している情報システムの一部において、これらを利用するに際して、利用者である国民の方々がパソコンなどにインストールすることが必要なＪＲＥ（Java Runtime Environment）に脆弱性が存在していることを受け、緊急調査を実施し、１２府省庁の２０のシステムに更新が必要であることが判明（７月２０日報道発表）。
○　８月に全府省庁（１９府省庁）に対してヒアリングを実施し、その結果を踏まえ、今後の対応策等について検討（別紙）。

別紙２－１

別紙

ＪＲＥ問題への対応について

1　これまでの経緯（詳細は参考を参照）

○　政府機関の電子申請システム等広く国民に向けて公開している情報システムの一部において、これらを利用するに際して、利用者である国民の方々がパソコンなどにインストールすることが必要なＪＲＥ（Java Runtime Environment）に脆弱性が存在していることを受け、ＮＩＳＣにおいて緊急調査を実施し、７月６日時点で１２府省庁の２０のシステムに更新が必要であることが判明（７月２０日報道発表）。

○　８月に全府省庁（１９府省庁）に対してヒアリングを実施。

2　現状と課題

①　ＪＲＥ問題に対応し、迅速な改修が行われたシステムがあったが、たまたま改修が計画されていたものであり、通常は、**改修のための予算措置等が必要となっており、迅速な対応が困難**。
予期せぬ課題に対する政府機関の構造的問題。

②　そもそもＪＲＥなど利用者が導入しているソフトウェアの脆弱性への対応については、迅速な対応が可能なように設計・開発等を行ったシステム構築が望ましい。
しかし、現時点では、**設計・開発時のセキュリティ面からのガイドラインが十分整っていないのが現状**。

3　対応方針

①　当面の対応

脆弱性が判明した時点で、システム運用府省庁は、**利用者に注意喚起**を行う。
また、速やかに**システム改修について検討**を行い、改修までの間は、システム運用府省庁の責任において、利用者に危険が及ばないよう代替措置等による適切な対処を実施。

②　今後の対応

新規開発する情報システムについて、利用者に導入させるソフトウェアの更新に容易に対応できる等、情報システムの**企画・設計段階から必要なセキュリティの検討を行うことが適当。**
ＮＩＳＣでは**セキュリティ・バイ・デザイン（ＳＢＤ）の一部としてこの問題を検討していく。**

別紙２－２

別紙3

平成20年度情報セキュリティ関連予算
概算要求について

平 成 １ ９ 年 １ ０ 月 ３ 日
内閣官房情報セキュリティセンター

平成２０年度予算概算要求のうち、情報セキュリティ関連のものは次のとおり。

１　要求額

○ 平成２０年度予算概算要求額　　３３，７５０百万円

○ 予算額推移（平成２０年度は概算要求額）

	平成１６年度	平成１７年度	平成１８年度	平成１９年度	平成２０年度
当初予算	２６７億円	２８８億円	３１９億円	３００億円	３３８億円
補正予算	―	―	―	―	―
合　　計	２６７億円	２８８億円	３１９億円	３００億円	３３８億円

（注）通常のシステム管理一般の中でセキュリティ対策を行っているなど、情報セキュリティ関連予算のみを取り出すことが困難なものは除く。

２　施策の内訳

各施策を第１次情報セキュリティ基本計画に掲げる対策実施領域別に分類した結果は以下のとおり。

分類	平成１８年度	平成１９年度	平成２０年度	前年比
１-１政府機関（政府機関統一基準遵守に係るシステム構築関係）	２０，７１５	１８，１１３	１９，１５６	111%
１-２政府機関（政府機関統一基準遵守に係る体制整備関係）			５５７	
１-３政府機関（政府機関統一基準遵守に係るその他）			３８６	
２　政府機関（１以外）		８４８	２，７６７	326%
３　地方公共団体		７６	２７６	363%
４　重要インフラ	１，７２５	４６０	５０５	110%
５　企業	３，５５３	１，４８２	１，６３９	111%
６　個人	４１	１，５２１	２，６５４	174%
７　横断的な基盤の形成	５，８８４	７，５０２	５，８０９	77%

※　平成２０年度は概算要求額

※　単位は全て百万円

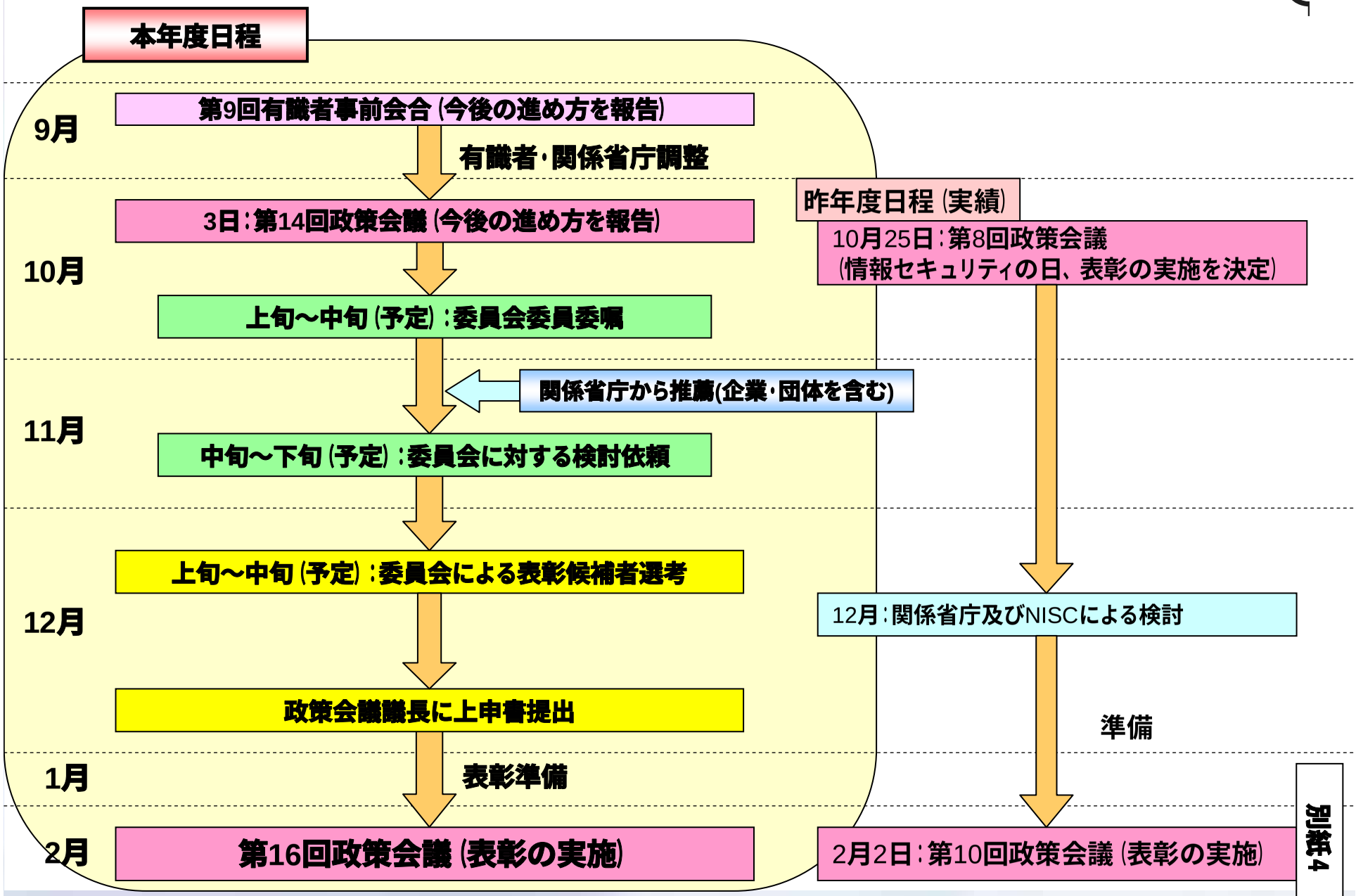
３　府省庁別予算額

各府省庁別の予算額は以下のとおり。

府省庁名	平成１８年度予算額（単位：千円）	平成１９年度予算額（単位：千円）	平成２０年度概算要求額（単位：千円）
内閣官房	３５３，４１６	８６７，６０６	１，４２３，１８９
内閣法制局	６，８３２	７，７４３	７，７４３
人事院	２１，１０５	２８，９４４	２６，５６２
内閣府	１６６，７０２	１５６，０８３	１５５，４６１
宮内庁	４０，７９９	２４，９２３	２４，９２３
公正取引委員会	３０，６１９	３６，５４９	３４，７００
警察庁	１，２４４，３３３	１，３３４，８８４	１，４７３，６３６
防衛省	１２，７９６，４４６	１０，９０９，４５１	１０，２９２，４９３
金融庁	１５２，５８０	１３９，２４５	１３５，５７７
総務省	７，２４３，３２５	５，９４１，０７０	７，７１０，０５２
法務省	１４８，７７６	５３９，３７５	７０６，４４４
外務省	２，７０２，６９４	２，９５９，２８６	３，４９０，２２９
財務省	９１７，６４０	７３６，０９３	１，２８７，３１８
文部科学省	６８２，６２６	６５４，８８０	９７７，０６３
厚生労働省	５５３，７１９	６５，４２６	８７，７８７
農林水産省	２７３，５６１	５１６，８４６	２２５，１４４
経済産業省	３，８６２，４０３	４，４４１，７５８	５，１１２，９３３
国土交通省	５９７，１４２	４６６，４７３	４８３，０３１
環境省	１２３，５９８	１７４，２６２	９５，８２７

合計	３１，９１８，３１６	３０，０００，８９７	３３，７５０，１１２

平成19年度情報セキュリティの日功労者表彰の進め方



「セキュア・ジャパン2007」の進捗状況（上半期）について

NISC

「セキュア・ジャパン2007」の進捗状況（上半期）の概要

①	「既に実施済み」	・・・ 27施策（17%）
②	「既に具体的な検討や実施に向けた準備を進めており、年度内（又は予定内）に実施できる予定」	・・・111施策（70%）
③	「今後具体的な検討や実施に向けた作業を開始する予定だが、年度内（同上）に実施できる見込み」	・・・ 18施策（11%）
④	「現時点では、年度内（同上）に実施できるどうか不明」	・・・ 3施策（2%）

上記で「③」とされている施策について：

他の施策による検討の結果・結論等が出るまでは検討できないために未着手という施策もあるが、いずれの施策も実施に向けたスケジュールは立っており、全て年度内（予定内）に実施できる見込み。

上記で「④」とされている施策について：

法律整備、条約の締結等に係る施策であり、国会審議の状況や諸外国との関係等で、明確な予定を示すことが困難。

結論

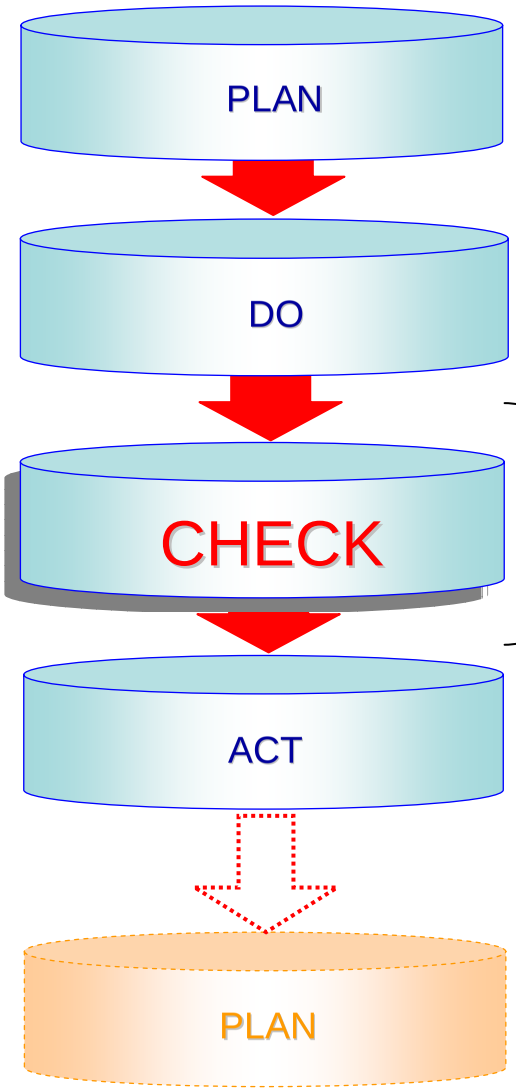
政府として実施すべき施策については、ほぼ全て年度内（又は予定内）に実施できる目途が立っており、「セキュア・ジャパン2007」は概ね順調に進捗。

別紙5

情報セキュリティ政策・評価等に向けた「作業方針」について

NISC

（情報セキュリティ政策のPDCAサイクル）



作業方針
＝PDCAサイクルの下でのCHECK段階に向けた方針

○情報セキュリティ政策の評価の枠組み文書※（平成１９年２月２日情報セキュリティ政策会議決定・了解）に基づき、毎年の評価、補完調査、分析等の実施に向けて策定するもの

※「「セキュア・ジャパン」の実現に向けた取組みの評価及び合理性を持った持続的改善の推進について（決定）」及び「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方（了解）」

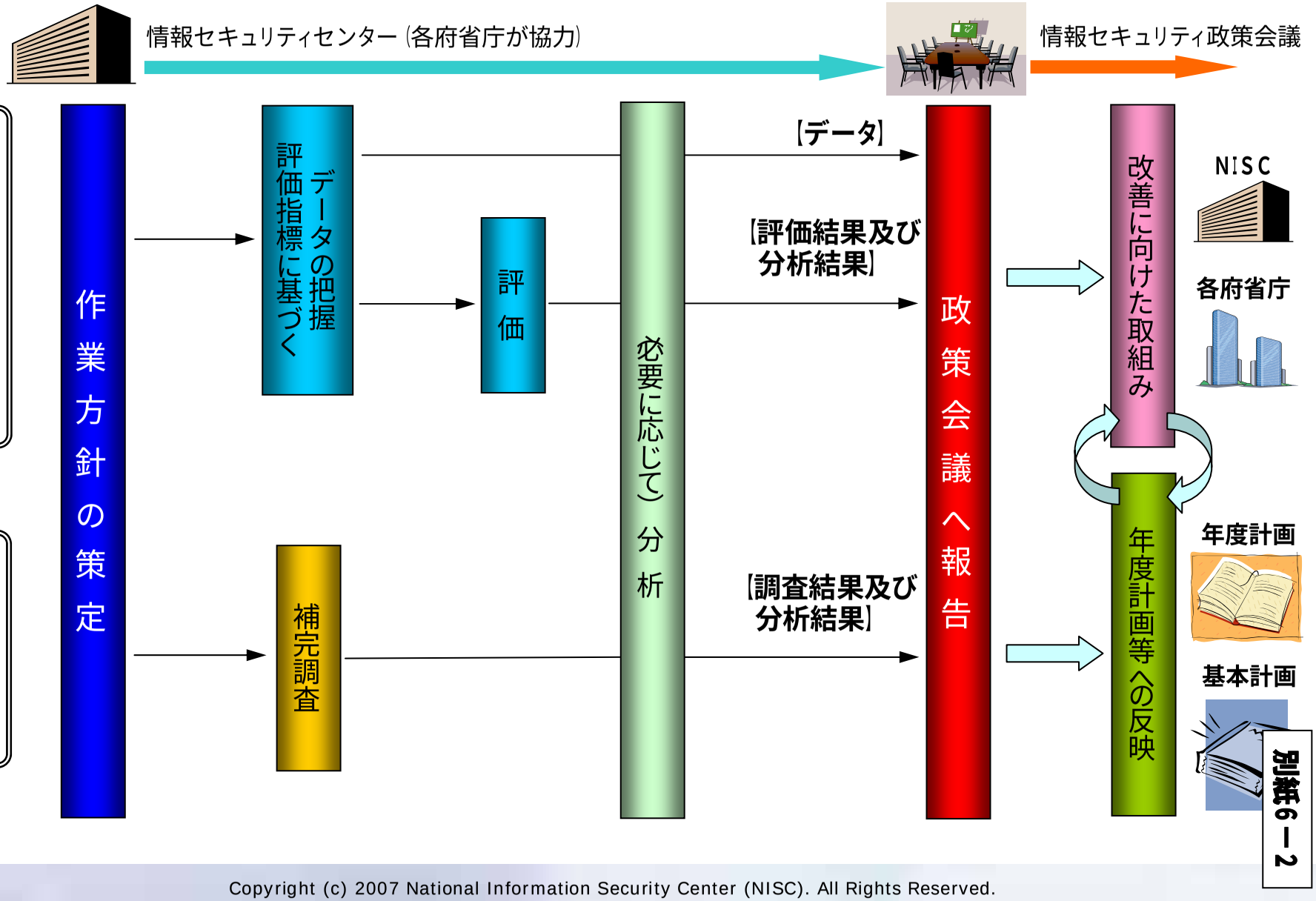
○「作業方針」には、
（1）評価指標の項目及び関係府省庁、
（2）補完調査の項目及び関係府省庁、
（3）分析課題及び分析方法
（4）評価等の実施に係るスケジュール、その他、評価等を実施する上で必要となる事項
を盛り込む

○「作業方針」は、毎年概ね9月頃に内閣官房情報セキュリティセンターが策定し、各府省庁の協力を得て、翌年3月頃まで評価、補完調査、分析等の作業を行う。

作業の結果については、評価文書としてとりまとめるとともに、以降の政策の企画・立案（翌年度セキュア・ジャパンや次期基本計画の策定）等にも適宜活用する。

別紙６－１

評価指標に基づく評価等の基本的な枠組み



情報セキュリティ政策全体に関する2007年度の評価等の考え方

評価等の視点

・2007年度の重点である「官民における情報セキュリティ対策の底上げ」の達成度を測る視点

・情報セキュリティに係る2007年度の様々な動向を測る視点

・2008年度の重点である「情報セキュリティ基盤の強化に向けた集中的な取組み」の具体化等に向けた助けとする視点

評価対象

・様々な主体による情報セキュリティ政策（セキュア・ジャパン2007に基づく施策全般）の取組みの進捗、及びその結果見られた情報セキュリティに係る動向の変化

関係府省庁

・内閣官房及び全府省庁

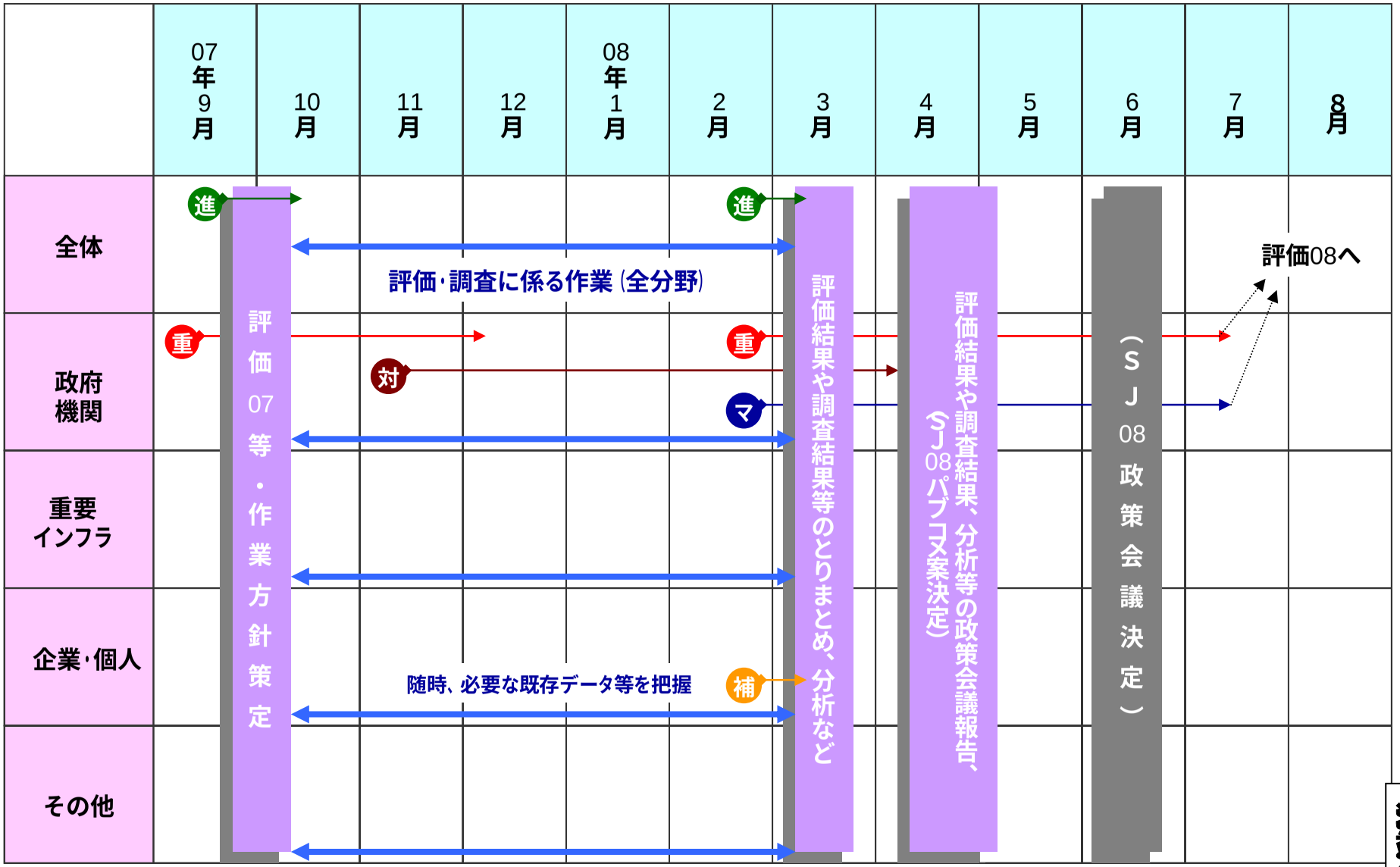
評価方法

・セキュア・ジャパン2007に基づく取組みの進捗状況調査を行う（2007年9月及び2008年2月頃の2回）。

・その上で、2006年度の評価等に準じ、検討枠組み（図1）を活用して、2007年度の情報セキュリティ政策の取組みの進捗やその結果見られた社会情勢の変化などを分析。これに基づいて、政策全体に関する定性的な評価を行う。

別紙6－3

全体のスケジュール



別紙6－4