サイバーセキュリティ基本法の成立とその影響

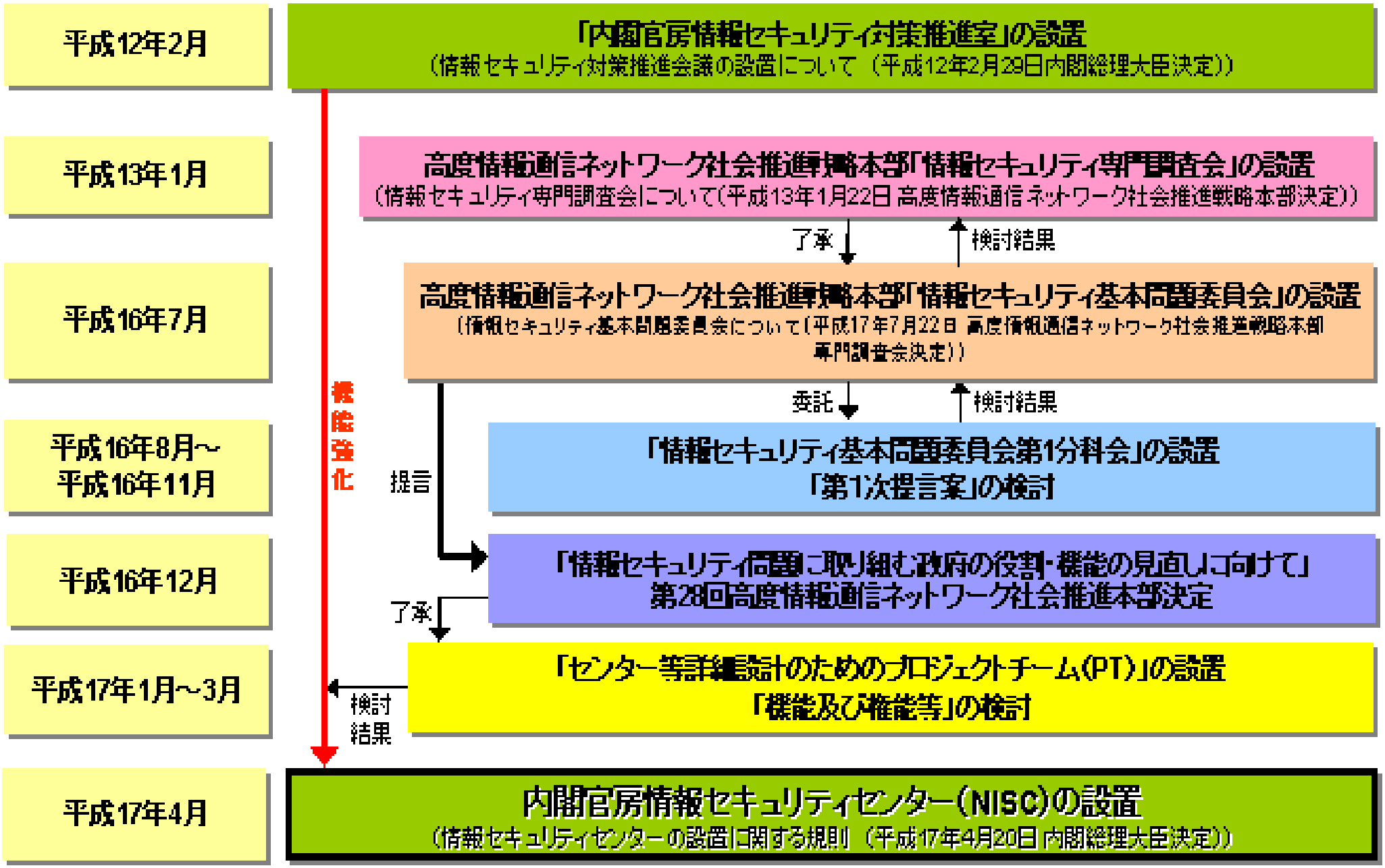
2015年1月20日

野村総合研究所
主席研究員　関　啓一郎

資料中の解釈・意見にわたる部分はあくまで個人のものである。

基本法成立以前の政策推進体制

情報セキュリティ政策推進体制の推移（基本法成立前）



内閣サイバーセキュリティセンター資料を一部変更

基本法成立以前の情報セキュリティ政策の推移

各省における試行錯誤

サイバー攻撃への対応を中心とした対策実施時期

IT障害への対応も含めた総合的な対策基盤づくりの推進

サイバー攻撃事態発生を念頭、新たな環境変化対応、能動的情報セキュリティ対策
「事故前提社会」への対応力強化など成熟した情報セキュリティ先進国へ向けた取組み

対策推進の枠組み

約1箇月で組織を立ち上げ

基本戦略

【基本戦略】

国民を守る情報セキュリティ戦略
（2010.5.11 情報セキュリティ政策会議決定）

サイバーセキュリティ戦略
2013年6月10日に策定）

基本戦略

第１次情報セキュリティ基本計画
（2006.2.2 情報セキュリティ政策会議決定）

第２次情報セキュリティ基本計画
（2009.2.3 情報セキュリティ政策会議決定）

【年度計画：セキュア・ジャパン】
※ 基本戦略に基づき策定する年度計画

SJ2006 SJ2007 SJ2008 SJ2009 情報セキュリティ2010 2011 2012 2013 2014

政府機関対策

情報セキュリティポリシーに関するガイドライン
（2000.7 情報セキュリティ対策推進会議決定）

政府機関の情報セキュリティ対策のための統一基準（第1～4版）
（2005.12.13 情報セキュリティ政策会議決定）

政府機関の情報セキュリティ対策のための統一基準群
（2011.4.21情報セキュリティ政策会議決定）
（2012.4.26,2012.4.18　同会議等改定）

政府

重要インフラ対策

重要インフラのサイバーテロ対策に係る特別行動計画
（2000.12 情報セキュリティ対策推進会議決定）

重要インフラの情報セキュリティ対策に係る行動計画
（2005.12.13 情報セキュリティ政策会議決定）

同第２次行動計画
（2009.2.3 情報セキュリティ政策会議決定）
（2012.4.26　同会議改定）

同第３次行動計画
（2014.5.19
情報セキュリティ政策会議決定）

組織体制

内閣官房情報セキュリティ対策推進室（2000.2設置）

① 内閣官房情報セキュリティセンター（2005.4 設置）
② 情報セキュリティ政策会議（2005.5 設置）
③ GSOC（2008.4 運用開始）

内閣サイバーセキュリティセンター資料を一部変更

「情報セキュリティ政策会議」時代の枠組み

内閣官房を中心に関係省庁も含め横断的な体制を整備

内閣サイバーセキュリティセンター資料を一部変更

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

本部長　内閣総理大臣
副本部長　情報通信技術（ＩＴ）政策担当大臣
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
内閣情報通信政策監（政府CIO）
有識者（９人）

（事務局）

内閣官房IT総合戦略室

室長（内閣情報通信政策監＝政府CIO）

情報セキュリティ政策会議　（2005年５月30日　IT戦略本部長決定により設置）

議長　内閣官房長官
議長代理　情報通信技術（ＩＴ）政策担当大臣
構成員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
有識者（６人）

閣僚が参画

- **重要インフラ専門委員会**（2005.9.15設置）
- **技術戦略専門委員会**（2005.7.14設置）
- **普及啓発・人材育成専門委員会**（2011.7.8設置）
- **情報セキュリティ対策推進会議**（2005.7.14設置）

（事務局）

内閣官房情報セキュリティセンター（NISC）

センター長（官房副長官補（安危））
副センター長（内閣審議官）２名
内閣参事官６名
情報セキュリティ補佐官３名

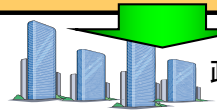
情報セキュリティ緊急支援チーム（CYMAT）

協力

協力５省庁
- 警察庁（サイバー犯罪の取締り）
- 総務省（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

その他の関係省庁
重要インフラ所管省庁
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス）
国土交通省（鉄道、航空、物流）
その他
文部科学省（セキュリティ教育）　等

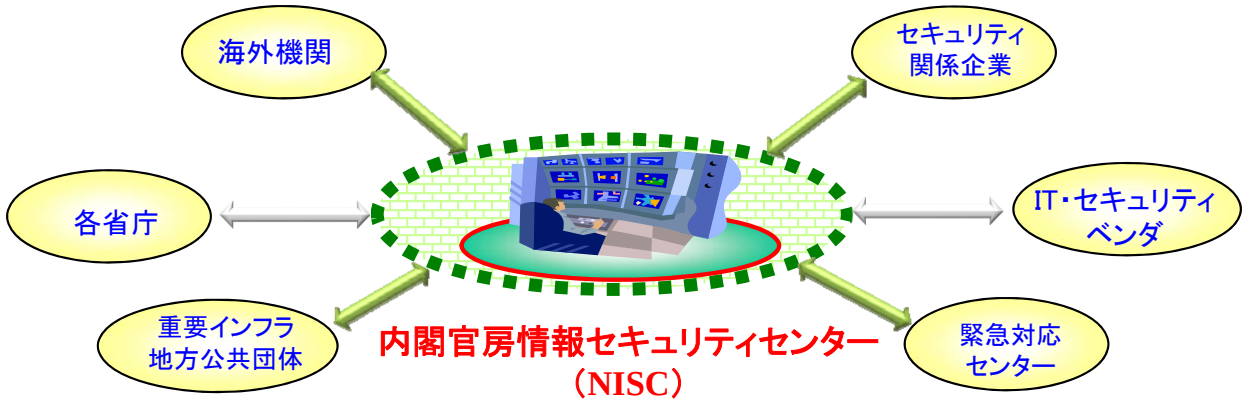

重要インフラ事業者　等


政府機関（各府省庁）


企業


個人

情報セキュリティ政策のフレームワーク



- ◆ NISCを結節点とした官民連携の強化、我が国全体としての対処能力の最大化
- ◆ 統一的・横断的な情報セキュリティ対策の推進による底上げ
- ◆ PDCAサイクルによる持続的改善
- ◆ 国際連携の強化によるイニシアティブの発揮

政府機関・地方公共団体

「政府機関統一基準」等により情報セキュリティを確保

【主な施策】

① サイバー攻撃等への対処

②情報セキュリティ体制の整備
（最高情報セキュリティ責任者（CISO）の設置など）

③政府機関統一基準の策定
（各省庁が守るべき最低限の対策水準を規定）

④政府機関におけるPDCA

⑤政府横断的な情報収集・分析システム（GSOC）の運用

重要インフラ

「重要インフラ行動計画」に基づく官民連携による重要インフラ防護

【主な施策】

① 安全基準等の整備・浸透

② 情報共有体制の強化

③重要インフラ防護対策の向上
（共通脅威分析、演習等）

※重要インフラ（13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
- 化学
- 石油
- クレジットカード

企業・個人

普及啓発の推進

【主な施策】

①情報セキュリティ普及・啓発プログラムの推進

②「情報セキュリティ月間」の実施

③情報セキュリティガバナンス確立の支援

横断的取組

- 情報セキュリティ研究開発戦略の推進
- 情報セキュリティ人材育成プログラムの推進
- 国際連携・協調の推進
- 情報セキュリティ関係の制度整備等

内閣サイバーセキュリティセンター資料を一部変更

基本法の検討経緯

NISCの機能強化に向けた検討状況（2014年１月23日）

～検討事項等～

サイバー脅威の高度化・深刻化	NISCの機能強化の方向性	機能強化に向けた検討事項
サイバー脅威の甚大化 ●標的型メール攻撃など機微情報や技術情報への攻撃の急増 ●重要インフラへの攻撃の増加	NISCの知見が各府省等に活用される仕組みの構築 東京オリンピック・パラリンピックにも備え先行的に政府の体制強化	●GSOCの機能の強化 ●重大なインシデントに関する原因究明など事後調査機能の強化 ●専門的人材の配備・育成（分析研究員の配置等）
サイバー脅威の拡散 ●スマートフォンの普及等に伴うリスクの拡散 ●自動車、制御系システム等へのリスクの高まり	各府省等のセキュリティ水準の向上に向けたNISCの積極的貢献 関係省庁のセキュリティ政策間の組織・分野横断的な実効性の確保	●各府省等の情報システムに関するセキュリティ監査機能の強化 ●ITセキュリティ投資に関する評価機能の強化（政府CIOと連携） ●関係省庁のセキュリティ政策間の総合調整機能の強化（政府CIOと連携）
サイバー脅威のグローバル化 ●国境を越えたサイバー攻撃等の急増 ●国家機関の関与が疑われる攻撃の顕在化	脅威情報等の集約・共有化の促進 国際連携取組方針に基づく米、EU、ASEAN等との連携強化	●政府機関・重要インフラのインシデント情報の集約機能の強化 ●官民にまたがる複数の国際的窓口機能の在り方の整理 ●政府間連携のための人員拡充

＜出典：第38回情報セキュリティ政策会議資料（2014年1月23日）＞

NISCの機能強化に関する政府方針

サイバーセキュリティ戦略（2013年6月情報セキュリティ政策会議決定）

NISCについては、世界を率先する強靭で活力あるサイバー空間を構築するための我が国の司令塔として、機能強化を行う。具体的には、GSOCの抜本的な強化を図るとともに、サイバー攻撃に関するインシデントに関する情報等の集約、サイバーセキュリティに関する国内外の動向等の実態及び政府の関連施策の現状に関する分析・周知、政府機関及び独立行政法人等の関連専門機関等に分散している各種機能の有機的な連携による動的な対応等を強化する。その際、国際的なインシデント対応における我が国の窓口となるCSIRT機能の在り方についても併せて検討する。

以上を踏まえ、NISCについては、専門職員の採用や育成等の人事管理による人材の確保や権限等の必要な組織体制を整備することにより、2015年度を目途として「サイバーセキュリティセンター」（仮称）に改組するものとする。

国家安全保障戦略（2013年12月国家安全保障会議決定・閣議決定）

サイバーセキュリティを脅かす不正行為からサイバー空間を守り、その自由かつ安全な利用を確保する。また、国家の関与が疑われるものを含むサイバー攻撃から我が国の重要な社会システムを防護する。このため、国全体として、組織・分野横断的な取組を総合的に推進し、サイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を図る。

そこで、平素から、リスクアセスメントに基づくシステムの設計・構築・運用、事案の発生の把握、被害の拡大防止、原因の分析究明、類似事案の発生防止等の分野において、官民の連携を強化する。また、セキュリティ人材層の強化、制御システムの防護、サプライチェーンリスク問題への対応についても総合的に検討を行い、必要な措置を講ずる。

さらに、国全体としてサイバー防護・対応能力を一層強化するため、関係機関の連携強化と役割分担の明確化を図るとともに、サイバー事象の監査・調査、感知・分析、国際調整等の機能の向上及びこれらの任務を担う組織の強化を含む各種施策を推進する。

かかる施策の推進に当たっては、幅広い分野における国際連携の強化が不可欠である。このため、技術・運用両面における国際協力の強化のための施策を講ずる。また、関係国との情報共有の拡大を図るほか、サイバー防衛協力を推進する。

内閣サイバーセキュリティセンター資料を一部変更

わが国のサイバーセキュリティ体制の強化に向けて

（2014年４月10日、自民党サイバーセキュリティ対策関係合同会議）

1　体制強化の必要性
～ 急速に高まるサイバー脅威への対処 ～

●安倍政権の成長戦略を確固たるものとするためには、ITの利活用等とともに、急速に高まるサイバー脅威に対処するため、**サイバーセキュリティを含む情報セキュリティの強化**について、**国自らがリーダーシップを強く発揮できる体制**への抜本的強化が必要。

2　体制強化に向けた基本的考え方
～ 国の主導的な役割の明確化 ～

●「インターネット前提社会」では、**民間の主導的役割等を定めるIT基本法は堅持**しつつ、**官民の緊密な連携**を前提に、**国家の安全保障、国民１人１人の認識醸成、東京オリンピック等への対策**のため、国の主導的役割の明確化が必要。

3 「サイバーセキュリティ基本法」（仮称）の制定 ～ 基本理念等の確立、司令塔の強化 ～

●**基本理念**として次を規定。

① **情報の自由な流通の確保**等を基本として、サイバー脅威に対し、**官民連携により能動的・積極的に対応。**

② **国民１人１人が情報セキュリティの認識を深化**し、被害から円滑・迅速に復旧等できる**強靭な体制を構築。**

③ **将来に渡りITの恵沢を享受**するため、その持続的な開発・利用による**創造的・活力ある経済社会を構築。**

④ **グローバルに密接な相互依存**の中、協調、規範策定、信頼醸成や能力構築支援等における**先導的な役割。**

●**国・重要インフラ事業者等の責務、関係者間の連携強化、必要な措置・行政組織の整備、基本的施策**等を規定。

●**司令塔となる「情報セキュリティ政策会議」の機能・権限**として次を規定。

①**サイバーセキュリティ戦略**の策定、②各府省等の対策に関する**統一基準の策定・監査**、
③**経費見積もり方針**等の策定、④重大インシデントの**原因究明調査**、⑤関係行政機関への**議長による勧告**　等

4　組織体制の強化に向けて ～ NISCの法制化等 ～

●**平成27年度からの本格稼働**を目指すべく、**政府において**、政府機関の横断監視機能（**GSOC**）**等を担うNISC（内閣官房情報セキュリティセンター）の法制化**等の組織体制を強化すべき。

自由民主党資料を一部変更

基本法案における民主党の修正

民主党大野元裕議員の説明によると、サイバーセキュリティ基本法案の民主党提案による修正は次のとおり。
（2014年06月10日　BLOGOS　民主党大野元裕議員の記事より抜粋）

① 附則部分にサイバー空間の安全保障について、緊急事態に相当する場合に防御するための能力を強化するための幅広い観点から検討することを付け加えた

② 国民の人権への配慮項目を追加した。

③ サイバーセキュリティ戦略策定の際には、国会への報告を義務付けた。

④ 国民のサイバーセキュリティに関する義務項目を削除し、国民のサイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努める項に訂正した。

⑤ サイバーセキュリティに関する事象の内、我が国の安全に重大な影響を及ぼすそれがあるものへの対応を特出しし、関係機関における体制強化を加えた。

サイバーセキュリティの確保に関する件（衆議院内閣委員会決議）（1）

政府は、サイバーセキュリティ基本法の施行に当たっては、次の諸点について法的措置も含めて検討を加え、その遺憾なきを期すべきである。

一　具体的な施策

1　サイバーセキュリティ戦略本部は、国家安全保障会議、高度情報通信ネットワーク社会推進戦略本部、内閣危機管理監等と緊密な連携を図ることとするほか、サイバーセキュリティに関する幅広い分野の有識者の意見を十分に取り入れ、施策に反映させるよう努めること。

2　サイバー攻撃関連情報の集約、予防策の構築並びにサイバー攻撃に対応するための演習及び訓練の企画及びその実施については、内閣官房情報セキュリティセンターを中心として総合的に実施すること。

3　内閣情報通信政策監と連携して、サイバーセキュリティに関する施策の評価を定期的に実施すること。

4　政府の各機関、重要社会基盤事業者及びサイバー関連事業者その他の事業者等における情報通信関連機器等の安全性に関する基準等については、未知の攻撃手法や想定外の攻撃対象への攻撃にも柔軟に対応できるよう、防護対象の重要性の段階に応じたものとするなど、総合的かつ有機的な視点から策定すること。

5　大規模サイバー攻撃への対応要領を作成し、関係者の協力の下に行われる定期的な演習及び訓練を通じて実効性のある対応策の構築に努めること。

6　サイバーセキュリティ確保のため、サイバーセキュリティに関する技術の向上のための研究開発予算の充実等の取組を積極的に推進すること。

7　中小企業者その他の民間事業者におけるサイバーセキュリティの確保のための自発的な取組を積極的に促進すること。

8　国民一人一人が自発的にサイバーセキュリティの確保に努めることができるよう、必要な情報の提供及び助言その他の施策を積極的に推進すること。

9　地方公共団体が自主的な施策の策定及びその実施を推進できるよう、積極的な支援を行うこと。

10　内閣官房情報セキュリティセンターについては、サイバーセキュリティ対策を着実に実施するために必要かつ十分な人員、予算を継続的に確保し、サイバーセキュリティ戦略を積極的に実施すること。

11　サイバーセキュリティ戦略本部の事務のうち、監査、原因究明のための調査、府省横断的な計画及び関係行政機関の経費の見積り方針等の作成等について、迅速かつ効果的に行う体制を整備すること。

出典：衆議院内閣委員会決議（2014年6月11日）下線は筆者

サイバーセキュリティの確保に関する件（衆議院内閣委員会決議）（2）

二　人材の育成及び登用

１　サイバーセキュリティに関する高度かつ専門的な知識を有する人材の育成に早急に取り組むとともに、人材を関係行政機関及び民間企業等から幅広く登用するよう努め、官民の連携体制を整備すること。

２　国の行政機関等でサイバーセキュリティに係る事務に従事する者の関係府省庁及び民間企業等との積極的な人事交流を推進するとともに、過去の人事慣行にとらわれない人事評価の在り方を検討すること。

三　連携体制の整備

１　サイバー攻撃のもたらす被害の重大性に鑑み、国家安全保障会議等との連携の下、安全保障上の観点から迅速かつ実効性のある措置を講ずることを検討した上で、必要な措置を講ずること。その際には、平素から危機管理、安全保障までを連続的に対応できる体制を整備すること。

２　サイバーセキュリティに関する国際的な連携を推進するため、サイバーセキュリティに関する諸外国の政策や国内外における情勢等の分析、国際的な会議への対応等に関する十分な人員体制を確保し、迅速な情報共有と協力体制の構築を実現すること。

四　サイバー攻撃を組織的に行う集団等の動向を分析し、捜査機関等との情報の適切な共有を図ること。

五　二〇二〇年オリンピック・パラリンピック東京大会におけるサイバーセキュリティに関する事象に対処するための国内外の関係機関との連絡調整等を行う組織の在り方について、将来の推進体制を見据えて検討した上で、必要な措置を講ずること。

六　国民の基本的人権について十分に配慮しつつ、サイバーセキュリティの確保を図るため、インターネットその他の高度情報通信ネットワーク上の通信における実効ある帯域制御の在り方について検討すること。

七　立法機関及び司法機関におけるサイバーセキュリティの確保について、それらの機関からの要請に応じ、必要な協力を行うよう努めること。

右決議する。

出典：衆議院内閣委員会決議（2014年6月11日）
下線は筆者

サイバーセキュリティ基本法案に対する附帯決議（参議院内閣委員会決議）

政府は、本法の施行に当たり、次の諸点について適切な措置を講ずべきである。

一　サイバー攻撃関連情報の集約、予防策の構築並びにサイバー攻撃に対応するための演習及び訓練の企画及びその実施については、内閣官房情報セキュリティセンターを中心として総合的に実施すること。

二　サイバーセキュリティ戦略本部と内閣情報通信政策監との連携の下、サイバーセキュリティに関する施策の評価を定期的に実施すること。

三　政府の各機関、重要社会基盤事業者及びサイバー関連事業者その他の事業者等における情報通信関連機器等の安全性に関する基準等については、未知の攻撃手法や想定外の攻撃対象への攻撃にも柔軟に対応できるよう、防護対象の重要性の段階に応じたものとするなど、高度情報通信ネットワークの特性を踏まえた総合的な視点から策定すること。

四　サイバーセキュリティに関する高度かつ専門的な知識を有する人材の育成に早急に取り組むとともに、人材を関係行政機関及び民間企業等から幅広く登用するよう努め、官民の連携体制を整備すること。

五　サイバーセキュリティに関する国際的な連携を推進するため、サイバーセキュリティに関する諸外国の政策や国内外における情勢等の分析、国際的な会議への対応等に関する十分な人員体制を確保し、迅速な情報共有と協力体制の構築を実現すること。

六　サイバー攻撃を組織的に行う集団等の動向を分析し、捜査機関等との情報の適切な共有を図ること。

七　国民の基本的人権について十分に配慮しつつ、サイバーセキュリティの確保を図るため、インターネットその他の高度情報通信ネットワーク上の通信における実効ある帯域制御の在り方について検討すること。

八　立法機関及び司法機関におけるサイバーセキュリティの確保について、それらの機関からの要請に応じ、必要な協力を行うよう努めること。

右決議する。

出典：参議院内閣委員会決議（2014年10月23日）
下線は筆者

基本法の概要と戦略本部の枠組み

なぜ内閣提出法案（閣法）でなかったのか？

議院内閣制の下で、閣議を経て行政府から国会に提出される内閣提出法案が多いが、サイバーセキュリティ基本法は、自由民主党、民主党・無所属クラブ、日本維新の会、公明党、みんなの党及び生活の党の共同提案により、衆議院内閣委員会提出の法律案とされた。（2014年６月11日）

（考えられる理由等）

- サイバーセキュリティに関する基本的施策を強い政治的なリーダーシップのもとで推進するための基本的枠組みを立法府が明確化すること
- サイバーセキュリティはすべての府省に関係するため事務的な調整に時間がかかるが、喫緊の課題であるために議員・政党の主導で迅速な成立を図る。
- 内閣提出法案では、法律に「サイバーセキュリティ」などのカタカナ用語を入れるなど、内閣法制局審査を通せなかった部分が多い。
- 内容面では、内閣の不作為・反対などの緊張関係があったわけではない。与党内、与野党間だけでなく、政府・与党間、府省間も十分な調整が図られている。

2014（平成26）年６月11日の衆議院内閣委員会で次のような質疑があった。（下線は筆者）

【高木美智代議員（公明党）】

本法案を閣法ではなくて議員立法とした趣旨につきまして、その立法意思、また主なポイント等を含めまして、国民の皆様によくおわかりになりますように、説明をお願いしたいと思います。

【遠山敬議員（公明党）】

（前略）サイバーセキュリティに関する基本理念あるいは基本的施策、それらを強い政治的なリーダーシップのもとで推進するための基本的枠組みを立法府が明確化することによって、政府のみならず、民間も含めて、関係者が一丸となって、スピード感を持って対策に取り組むことが必要であるというふうに思っております。

そのためにも、今回、サイバーセキュリティに関する施策を総合的かつ効果的に推進するための法律を議員立法として制定することは大変な意義があると思っておりますし、また喫緊の課題でありまして、（以下略）

新法とされた理由：ＩＴ基本法との思想的差異

IT基本法は民間主導原則を掲げるのに対し、サイバーセキュリティでは、国主導で安全・安心を確保していくべきことが志向された。
このため、IT基本法の改正ではなく、新法としてのサイバーセキュリティ基本法が制定されることとなった。
また、サイバーセキュリティ基本法は、IT基本法を補完するものと位置付けられている。

【IT基本法】 抜粋
（国及び地方公共団体と民間との役割分担）
第七条　高度情報通信ネットワーク社会の形成に当たっては、民間が主導的役割を担うことを原則とし、国及び地方公共団体は、公正な競争の促進、規制の見直し等高度情報通信ネットワーク社会の形成を阻害する要因の解消その他の民間の活力が十分に発揮されるための環境整備等を中心とした施策を行うものとする。

【サイバーセキュリティ基本法】 抜粋
（国の責務）
第四条　国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する。

（下線は筆者）

サイバーセキュリティと国主導の考え方

2014（平成26）年６月11日の衆議院内閣委員会で次のような質疑があった。（下線は筆者）

【関芳弘議員（自民党）】

サイバーセキュリティは、世界最先端のIT国家実現といった成長戦略の礎でありますとともに、また、オリンピック・パラリンピック大会の成功や国家安全保障にもかかわりまして、今後の日本にとって極めて重要なテーマであります。

これにつきまして、民間に任せるのではなくて、ぜひ私は国に主導的役割を担ってもらいたいと思いますが、いかがでしょうか。

【平井卓也議員（自民党）】

IT社会の形成については、基本法として、高度情報ネットワーク社会形成基本法、IT基本法ですね、これは2001年に施行されて、私、国会議員として初めてこの議論に参加をした思い出深い法律ですけれども、この法律では、ブロードバンドの整備等は民間が主導的な役割を担うということが基本理念になっています。（中略）

サイバーセキュリティに関しては、国家の安全保障、危機管理にも関する分野であり、国と民間の役割を明確化した上で、国が主導的立場を果たしながら、官民の緊密な連携により取り組みを着実に進めていかなければならないと考えています。

そこで、今回の基本法案は、IT基本法を補完する、要するに、時代に対応し切れなくなったIT基本法を補完するものとして、各省庁、地方公共団体、重要インフラ事業者等、多様な主体が連携し、野球でいいますと、内野と外野が緊密に連携して、できるだけポテンヒットを打たれないようにする、そのために国がリーダーシップを発揮するための体制を整備しようということであります。

サイバーセキュリティ基本法の概要

内閣サイバーセキュリティセンター資料

第Ⅰ章．総則

■目的（第1条）

■定義（第2条）

⇒ 「サイバーセキュリティ」について定義

■基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民1人1人の認識を深め、自発的な対応の促進等、強靭な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■法制上の措置等（第10条）

■行政組織の整備等（第11条）

第Ⅱ章．サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）

■民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■多様な主体の連携等（第16条）

■犯罪の取締り及び被害の拡大の防止（第17条）

■我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）

■産業の振興及び国際競争力の強化（第19条）

■研究開発の推進等（第20条）

■人材の確保等（第21条）

第Ⅲ章．基本的施策（つづき）

■教育及び学習の振興、普及啓発等（第22条）

■国際協力の推進等（第23条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置等（第24条～第35条）

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■施行期日（第1条）

⇒ 公布の日から施行（ただし、第Ⅱ章及び第Ⅳ章は公布日から起算して1年を超えない範囲で政令で定める日）する旨を規定

■本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等（第2条）

⇒ 情報セキュリティセンター（NISC）の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

■検討（第３条）

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■IT基本法の一部改正（第４条）

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

サイバーセキュリティ基本法の目的（第１条）

1. 環境変化

前提として、「インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化」を掲げている。

2. 環境変化に伴う現状認識

変化に伴う現状として、「情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況」を掲げている。

ここで、「情報の自由な流通」はキーワードである。サイバーセキュリティ確保のために、情報の流通を犠牲にしては本末転倒であることを注意喚起したものと考えられる。

3. 我が国のサイバーセキュリティに関する施策の総合的かつ効果的推進

(1) 基本理念を定める
(2) 国及び地方公共団体の責務等
(3) サイバーセキュリティ戦略の策定
(4) その他サイバーセキュリティに関する施策の基本となる事項
(5) サイバーセキュリティ戦略本部を設置すること等

により、高度情報通信ネットワーク社会形成基本法（平成十二年法律第百四十四号）と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進する。

4. 狭義の目的

(1) 経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現
(2) 国際社会の平和及び安全の確保並びに我が国の安全保障に寄与

サイバーセキュリティの定義（第２条）

わが国で初めて法制上「サイバーセキュリティ」の定義が定められた。この文言が広く国民、企業、政府、自治体等の中で浸透することによって意識が高まることが期待される。

基本法2条によると、「サイバーセキュリティ」とは、次の①及び②の措置が講じられ、その状態が適切に維持管理されていることとされている。

① 電磁的方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置

② 情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置

（①②には、情報通信ネットワーク等※を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む）

※　情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体

この定義では、ネットワークと機器の安全確保をベースとして、その上で生成・流通・消費される電磁的情報の保護が含まれることになる。

従来の「情報セキュリティ」に比べて、「サイバーセキュリティ」では①からも②からも紙に書かれたものや知識・知恵の類が抜けているのが大きな相違点である。

サイバーセキュリティの定義といわゆるＣＩＡ

一般にOECD等では、「情報セキュリティ」について、CIA、すなわち、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を維持することと定義されているが、本法では採用されなかった。このCIAを法律の条文化することは立法技術的に難しかったのだと考えられる。

基本法成立後の情報セキュリティ政策会議（2014年11月25日）で、同法成立を踏まえて決定された「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」の中では、

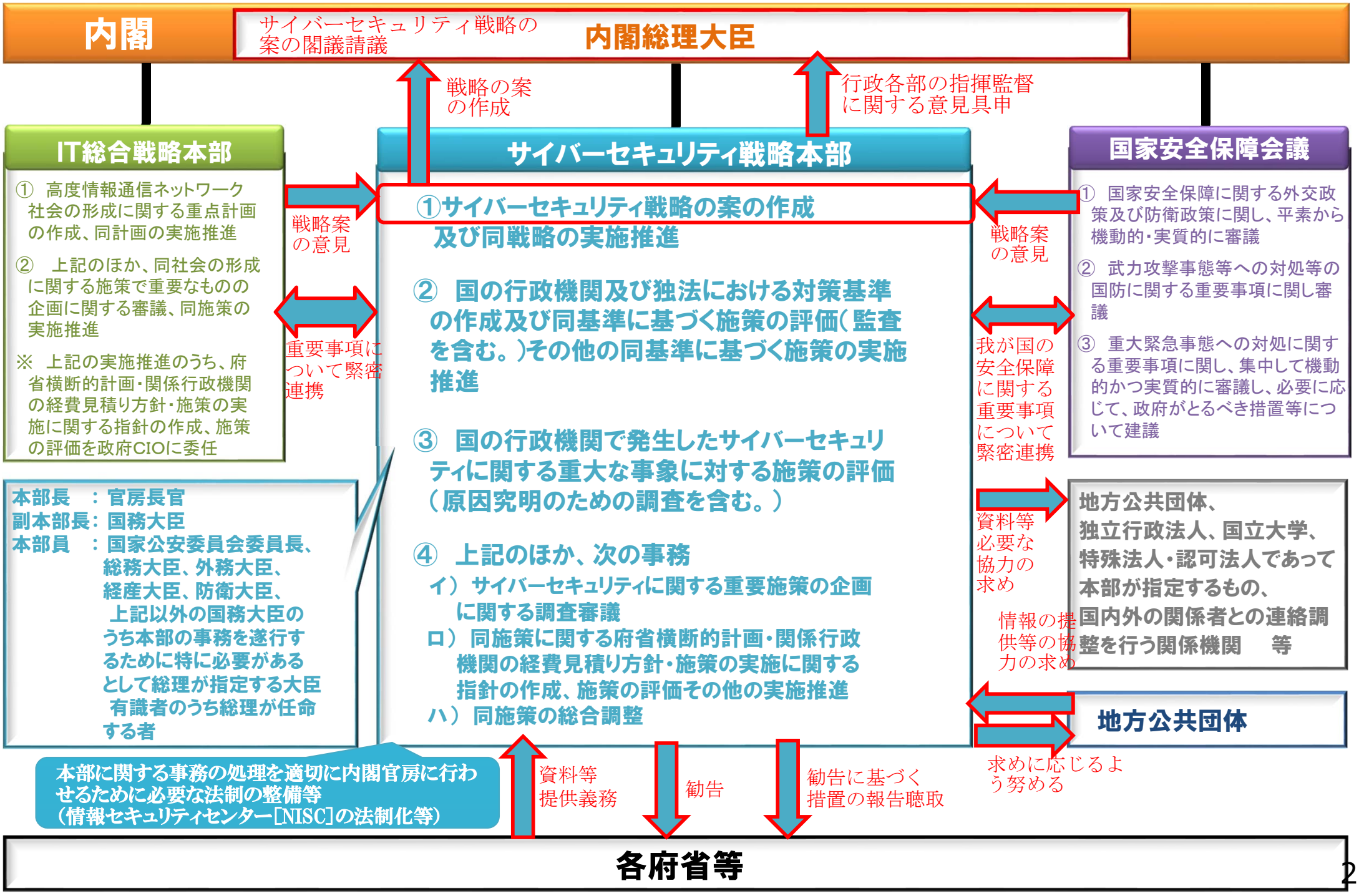
「サイバー空間を構成する情報システムや情報通信ネットワーク等において処理される情報及び実空間における重要インフラ等であって当該情報システムや情報通信ネットワーク等と一体化・融合しているものに関する機密性・完全性・可用性等が確保された状態である『サイバーセキュリティ』」

という説明をしている。これは、いわゆるCIA概念を用いて基本法の定義を言い替えたものであろう。

（注）
C：　権限がない者に情報内容が漏れないようにすること、情報漏洩は機密性の侵害に当たる。
I：　情報内容が正しく完全であることで、改ざんは完全性の侵害に当たる。
A：　利用したい時に利用できることで、システムダウンの発生は可用性の侵害に当たる。

サイバーセキュリティ戦略本部の機能・権限（イメージ）

内閣サイバーセキュリティセンター資料



サイバーセキュリティ戦略本部の構成と従来の政策会議との相違点

サイバーセキュリティ戦略本部の構成

1. 内閣官房に本部を置き（24条）、**本部長、副本部長及び本部員**をもって組織（26条）する。
2. **本部長には内閣官房長官**を充て（27条１項）、副本部長には国務大臣をもって充てる（28条）。副本部長には情報通信技術（IT）政策担当大臣が充てられている。
3. 本部員は、閣僚としては、特に関係が深い行政機関の長として、**国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣**のほか、総理大臣が指定する国務大臣が充てられ、民間からは、サイバーセキュリティに関し優れた識見を有する者のうち、内閣総理大臣が任命する者が充てられることとされている（29条）

従来の「情報セキュリティ政策会議」との相違点

1. 情報セキュリティ政策会議は、**IT基本法に基づくIT総合戦略本部の下に設けられた**会議体という位置づけであり、IT総合戦略本部の運営に関して必要な事項として設置されたもの
2. 同政策会議には府省等に対する明示的な法的権限は付与されておらず、**議長である官房長官の権威及び内閣官房の一般的な企画・立案・総合調整権限により政策が遂行される**というもの
3. サイバーセキュリティ戦略本部はIT総合戦略本部とは別に**基本法に基づいて設置された機関であり、法的権限も付与**されている点が大きな相違

（参考）　内閣法（抜粋）

第一条　内閣は、国民主権の理念にのつとり、日本国憲法第七十三条その他日本国憲法に定める職権を行う。

２　内閣は、行政権の行使について、全国民を代表する議員からなる国会に対し連帯して責任を負う。

第三条　各大臣は、別に法律の定めるところにより、主任の大臣として、行政事務を分担管理する。２（略）

第四条　内閣がその職権を行うのは、閣議によるものとする。

２　閣議は、内閣総理大臣がこれを主宰する。この場合において、内閣総理大臣は、内閣の重要政策に関する基本的な方針その他の案件を発議することができる。３（略）

第五条　内閣総理大臣は、内閣を代表して内閣提出の法律案、予算その他の議案を国会に提出し、一般国務及び外交関係について国会に報告する。

第六条　内閣総理大臣は、閣議にかけて決定した方針に基いて、行政各部を指揮監督する。

第七条　主任の大臣の間における権限についての疑義は、内閣総理大臣が、閣議にかけて、これを裁定する。

第八条　内閣総理大臣は、行政各部の処分又は命令を中止せしめ、内閣の処置を待つことができる。

第十二条　内閣に、内閣官房を置く。

２　内閣官房は、次に掲げる事務をつかさどる。

一　閣議事項の整理その他内閣の庶務

二　内閣の重要政策に関する基本的な方針に関する企画及び立案並びに総合調整に関する事務

三　閣議に係る重要事項に関する企画及び立案並びに総合調整に関する事務

四　行政各部の施策の統一を図るために必要となる企画及び立案並びに総合調整に関する事務

五　前三号に掲げるもののほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務

六　内閣の重要政策に関する情報の収集調査に関する事務

七～十四（略）

３、４（略）

サイバーセキュリティ本部の所掌事務（25条１項）

1. サイバーセキュリティ戦略の案の作成及び実施の推進に関すること
2. 国の行政機関及び独立行政法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること
3. 国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）に関すること
4. そのほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

- 本部の事務局である「内閣サイバーセキュリティセンター」は、内閣官房の一般的な企画・立案・総合調整事務だけでなく、本部が有するこれらの事務を遂行することとなる。
- 戦略や基準の策定事務だけでなく、基準に基づく施策の（監査を含む）評価や、重大な事象に対する（原因究明のための調査を含む）施策の評価が所掌事務として規定された。特に**府省に対する監査や原因究明の権限**を得たことは政府全体のサイバーセキュリティ対策を行う上での大きな前進と言えよう。

サイバーセキュリティ戦略本部長の権限（27条）

1. 内閣官房長官の充て職とされた本部長は、本部の事務を総括し、所部の職員を指揮監督（同条2項）する権限を持つ。
2. 本部長は、本部が行う各種の評価や提供された資料・情報に基づき、必要があると認めるときは、関係行政機関の長に対して勧告する（同条3項）ことができる。
3. さらに、勧告に基づいてとった措置について報告を求める（同条4項）ことができる。この勧告と報告徴収によるフォローアップにより、関係行政機関に対して、サイバーセキュリティに係る統制力が以前に比べて大いに高められたと考えられる。
4. 加えて、本部長は、勧告した事項に関し特に必要が認められるときは、内閣総理大臣に対して内閣法6条の規定による措置が取られるよう意見を具申する（同条5項）ことができる。総理大臣による指揮監督により、勧告の遵守を担保しようとするものである。

内閣法（抜粋）

第六条　内閣総理大臣は、閣議にかけて決定した方針に基いて、行政各部を指揮監督する。

戦略本部への資料提供義務及び資料提出その他の協力（1）

関係行政機関の長の義務（30条）

1. 関係行政機関の長は、本部の定めるところにより、本部に対し、サイバーセキュリティに関する資料又は情報であって、本部の所掌事務の遂行に資するものを、適時に提供しなければならない。
2. このほかにも、関係行政機関の長は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する資料又は情報の提供及び説明その他必要な協力を行わなければならない。

IT基本法、知的財産基本法、宇宙基本法等の他の同種の法律が、その所掌事務を遂行するため必要があると認めるときは、資料の提出、意見の表明、説明その他「必要な協力を求めることができる」という書き振りであるのに対し、「～なければならない」という義務を強調しており、より大きな権限を本部に与えているものと考えられる。

※　強い権限を持つ例として、「国家安全保障会議設置法」がある。

（資料提供等）

第六条　内閣官房長官及び関係行政機関の長は、会議の定めるところにより、会議に対し、国家安全保障に関する資料又は情報であつて、会議の審議に資するものを、適時に提供するものとする。

２　前項に定めるもののほか、内閣官房長官及び関係行政機関の長は、議長の求めに応じて、会議に対し、国家安全保障に関する資料又は情報の提供及び説明その他必要な協力を行わなければならない。

本部への資料提供義務及び資料提出その他の協力（2）

関係行政機関の長以外の者に対しては、他の類似立法と同様の規定が盛り込まれている。（31条）

本部は、その所掌事務を遂行するため必要があると認めるときは、次の者に対して、資料の提出、意見の開陳、説明その他必要な協力を求めることができる。（31条１項）。

- 地方公共団体及び独立行政法人の長
- 国立大学法人の学長
- 大学共同利用機関法人の機構長
- 日本司法支援センターの理事長
- 特殊法人及び認可法人であって本部が指定するものの代表者
- サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者

また、本部は、その所掌事務を遂行するため特に必要があると認めるときは、これら以外の者に対しても、必要な協力を依頼することができる（同2項）。

例えば、「知的財産基本法」に次のような規定がある。

（資料の提出その他の協力）

第三十条　本部は、その所掌事務を遂行するため必要があると認めるときは、関係行政機関、地方公共団体、独立行政法人及び地方独立行政法人の長並びに特殊法人の代表者に対して、資料の提出、意見の表明、説明その他必要な協力を求めることができる。

２　本部は、その所掌事務を遂行するために特に必要があると認めるときは、前項に規定する者以外の者に対しても、必要な協力を依頼することができる。

ＩＴ総合戦略本部、国家安全保障会議（ＮＳＣ）との関係（25条）

1. 本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、IT総合戦略本部及び国家安全保障会議の意見を聴かなければならない（25条2項）。
2. 本部は、サイバーセキュリティに関する重要事項について、IT総合戦略本部との緊密な連携を図る（同条3項）とともに、我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国家安全保障会議との緊密な連携を図る（同条4項）。
3. 附則4条により、IT基本法26条（IT総合本部の所掌事務）1項が改正され、サイバーセキュリティ戦略本部の所掌事務（25条1項）のうち、サイバーセキュリティに関する施策で重要なものの実施の推進に関するものが、IT総合戦略本部の所掌事務から明示的に除かれた。

ここで、**サイバーセキュリティと危機管理レベルとの関係**は次のように整理されると思われる。

- 平時でのインシデントレスポンス：サイバーセキュリティ戦略本部・NISCによる対応
- 大規模インシデント：内閣危機管理監、内閣官房副長官補（事態対処・危機管理担当）、事態対処室による対応
- 武力攻撃相当：国家安全保障局

具体的判断に当たっては、危機管理担当の内閣官房副長官補がNISCセンター長、国家安全保障局次長を兼ねているので、同一人物が判断して役割を調整することになるのであろう。

基本法附則２条が求める体制整備

1. 総理大臣決定で内閣官房に置かれている「情報セキュリティセンター」の法制化も含めて、本部に関する事務を内閣官房に行わせるために必要な法制の整備その他の措置を講ずることを政府に義務付けている。（附則２条１項）
2. 必要な法制の整備その他の措置を講ずるに当たって、次の事項について検討を加え、その結果に基づいて必要な措置を講ずる（同条２項）ものとしている。
   (1) 専門的知識を有する者を内閣官房において任期を定めて職員又は研究員として任用すること
   (2) 情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析並びにサイバーセキュリティに関する事象に関する国内外の関係機関との連絡調整に必要な機材及び人的体制の整備等のために必要な法制上及び財政上の措置等

現状では不十分なので、サイバーセキュリティ専門家の任期付き任用、政府の情報システムへの不正活動の監視・分析、内外関係機関との連絡調整に必要な物的・人的体制整備を検討し、必要な措置を講ずることを政府に求めたものである。

政府は、2014（平成26）年12月16日の閣議決定で、内閣官房組織令・行政機関職員定員令等の一部を改正し、内閣官房に内閣サイバーセキュリティセンターを設置、その所掌事務を定めるとともに、内閣の機関の職員の定員を増加（10名）させる等の改正を行ったところである。

基本法における情報の保護と流通（利用）のバランス

基本法は、安全保障・危機管理面に偏っているのではないかという批判がある。サイバーセキュリティには、サイバー攻撃対策だけでなく、経済社会活動の円滑な継続の確保、ICT業務継続という情報の流通・保護を重視すべき面への配慮が足りないのではないかという批判である。
しかし、条文を見ると、基本法では両者のバランスに配慮しているのではないかと考えられる。

1. 法律の目的

基本法1条では、「情報の自由な流通を確保しつつ」、IT基本法と相まって、という表現のほか、「経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現」という文言が挿入されており、「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与」だけではない。

2. サイバーセキュリティの定義

定義を見る限り、情報の安全管理が重視されており、サイバー攻撃などの安全保障・危機管理面だけでなく、ICT業務継続の確保なども含まれている。

3. 基本理念

3条の基本理念でも、1項で「情報の自由な流通の確保」、「表現の自由の享受」、「イノベーションの創出」、「経済社会の活力の向上」等の重要性を謳っている。

3項では、サイバーセキュリティに関する施策の推進は、「インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築するための取組を積極的に推進することを旨」として行われなければならないとしている。

5項でも、サイバーセキュリティに関する施策の推進は、「高度情報通信ネットワーク社会形成基本法の基本理念に配慮して行われなければならない」としている。

6項では、サイバーセキュリティに関する施策の推進に当たっては、「国民の権利を不当に侵害しないように留意しなければならない」としている。

取組の現状と今後の課題

サイバーセキュリティ基本法の施行に伴う関係政令の整備等の概要

１ 内閣官房組織令・行政機関職員定員令等の一部改正

サイバーセキュリティ基本法（平成26年第104号。以下「法」という。）の施行に伴い、内閣官房に内閣サイバーセキュリティセンターを設置し、その所掌事務を定めるとともに、内閣の機関の職員の定員を増加させる等の改正を行う。また、同センターの設置に伴い、必要となる政令を改正する。

２ サイバーセキュリティ戦略本部令

法第35条に基づき、法第29条第１項に規定するサイバーセキュリティ戦略本部員のうち、国務大臣以外の本部員の定数（10名以内、任期２年）を定めるなど戦略本部の内部組織について定める。

３ サイバーセキュリティ基本法の一部の施行期日を定める政令

サイバーセキュリティ基本法附則第一項ただし書に規定する施行の日は、平成27年１月９日とする。

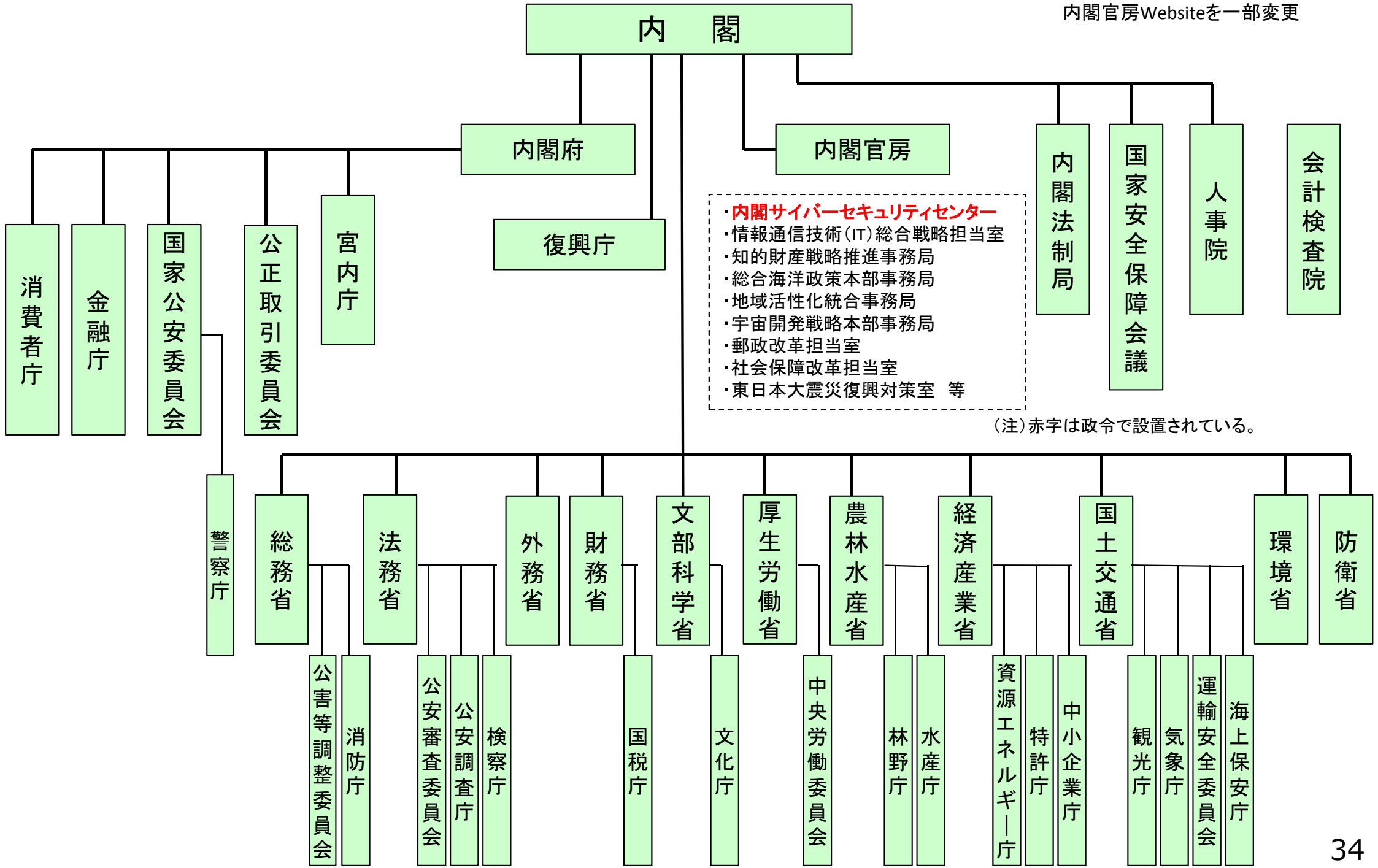
４ サイバーセキュティ戦略本部の副本部長を特定する件について

法第28条第１項に規定するサイバーセキュリティ戦略副本部長に情報通信技術（IT）政策担当大臣を充てることとする（閣議決定）。

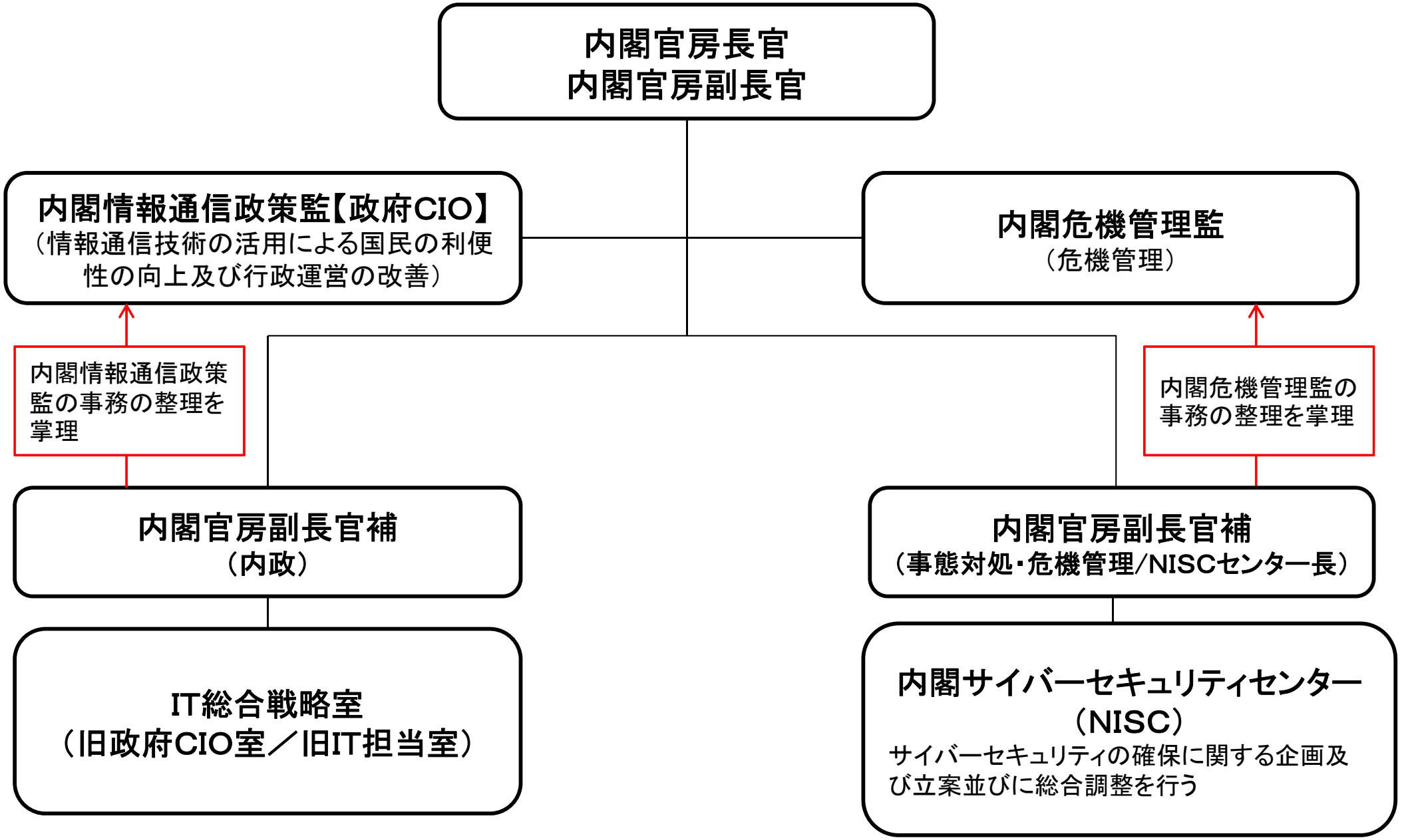
※ 閣議決定日：2014（平成26）年12月16日（火）

内閣サイバーセキュリティセンター資料を一部変更

我が国の行政機構とＮＩＳＣの位置付け



政府ＣＩＯ、ＩＴ総合戦略室、ＮＩＳＣの関係



内閣サイバーセキュリティセンター資料を一部変更

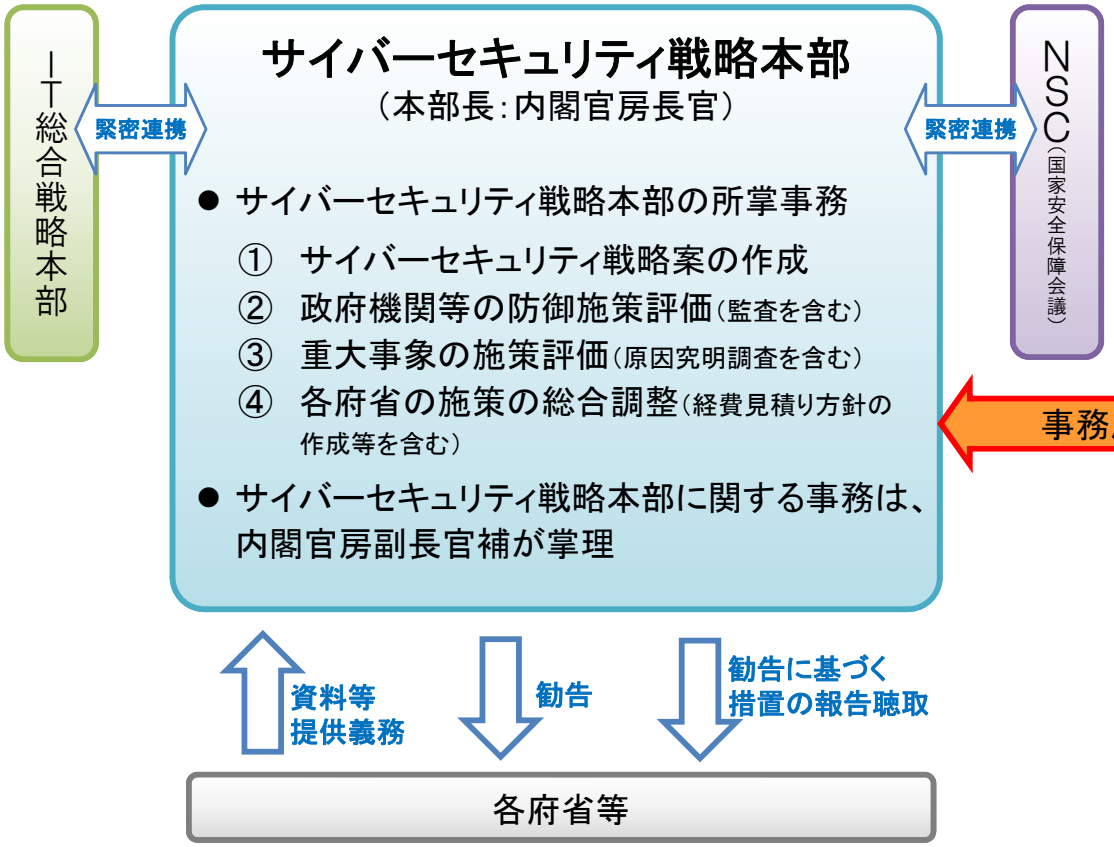
「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」概要

1　機能強化の必要性

以下の観点から、我が国の「サイバーセキュリティ」強化のための推進体制の機能強化が不可欠

- あらゆる活動のサイバー空間への依存の高まりにより、リスクが深刻化（甚大化・拡散・グローバル化）
- 「世界最高水準のIT利活用社会」の実現が成長戦略の柱の1つ
- 国際的な連携の強化が必要な諸外国においても、積極的な体制強化を実施
- 2020年東京オリンピック・パラリンピックに向けた対策の強化が必要

2　サイバーセキュリティ基本法の制定



3　我が国の推進体制の機能強化に向けた取組

（1）情報セキュリティ政策会議の担ってきた機能は、サイバーセキュリティ戦略本部が担うこととなる。

（2）内閣官房情報セキュリティセンター（NISC）を以下の組織に法制化（内閣官房組織令）する。

内閣サイバーセキュリティセンター（注）

- 内閣サイバーセキュリティセンターの所掌事務
  - ①GSOCに関する事務
  - ②原因究明調査に関する事務
  - ③監査等に関する事務
  - ④サイバーセキュリティに関する企画・立案、総合調整
- センター長には、内閣官房副長官補をもって充てる

（3）今後、戦略本部の事務の稼働状況、オリンピック・パラリンピック東京大会開催に向けた準備、サイバー空間における脅威の増大等の諸情勢を踏まえつつ、法制の追加的な整備等について引き続き検討。

（注）英名称：National center of Incident readiness and Strategy for Cybersecurity

内閣サイバーセキュリティセンター資料を一部変更

内閣サイバーセキュリティセンター（ＮＩＳＣ）の所掌事務

基本法の施行に伴い、内閣官房に内閣サイバーセキュリティセンターを設置し、その所掌事務を定めるとともに、内閣の機関の職員の定員を増加させる等の改正（内閣官房組織令・行政機関職員定員令）を行った。

同センターは2015（平成27）年１月９日に発足した。英文名称は内閣官房情報セキュリティセンター時代の”National Information Security Center”から”National center of Incident readiness and Strategy for Cybersecurity”とされたが、内外に知られている略称の“NISC”はそのまま。

また、内閣官房の事務として位置づけが曖昧であったGSOC関係も正式に位置づけられた。

【内閣サイバーセキュリティセンターの所掌事務】（内閣官房組織令４条の２）

一．情報通信ネットワーク又は電磁的記録媒体※を通じて行われる行政各部の情報システムに対する**不正な活動の監視及び分析**に関すること。

二．行政各部におけるサイバーセキュリティの確保に支障を及ぼし、又は及ぼすおそれがある**重大な事象の原因究明のための調査**に関すること（内閣情報調査室においてつかさどるものを除く。）。

三．行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助に関すること。

四．行政各部におけるサイバーセキュリティの確保に関し必要な監査に関すること。

五．これらのほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務のうちサイバーセキュリティの確保に関するもの（国家安全保障局、内閣広報室及び内閣情報調査室においてつかさどるものを除く。）

※　電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものに係る記録媒体をいう。

制度整備を踏まえた内閣サイバーセキュリティセンター（ＮＩＳＣ）に関する主な検討事項

制度整備を踏まえ、内閣サイバーセキュリティセンター（NISC）に関して、2020年オリンピック・パラリンピック東京大会も見据えつつ、主に以下の項目について必要な措置の検討を行い、可及的速やかに結論を得る。

① GSOC機能の強化

- 新システム（2017年度～）の運用を見据えた体制、機材の整備　等

② 総合的分析機能の強化

- 諸外国の政策、サイバー攻撃の脅威情勢及び攻撃に使用された技術等の総合的な分析
- 高度な専門知識と深い知見を有する専門的人材の確保及び資質の向上

③ 国内外の情報集約機能の強化

インシデント情報の集約機能や助言機能等の強化に向けた、

- 官民連携のスキーム強化・構築
- NISC内の体制・システム整備及び能力向上

④ 国際連携の強化

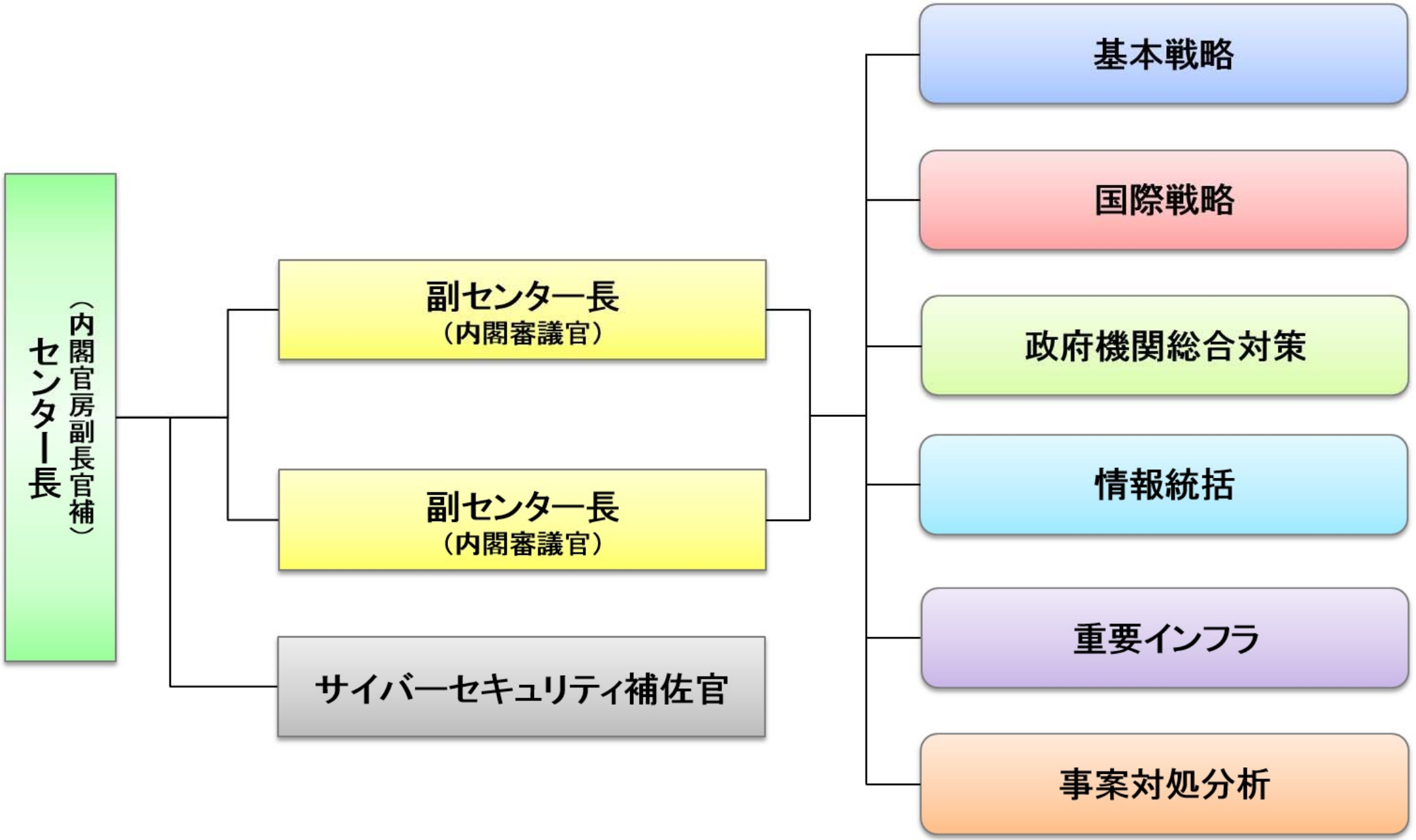
- 緊急対応関連機関とのパートナーシップ構築等による国際的な窓口機能の強化

⑤ 人材の育成及び登用

- 各省庁からの出向等人材を通じ、NISC内の知見・経験を各省庁に還元
- 任期付任用や人事交流の推進等による技能を備えた人材の確保

内閣サイバーセキュリティセンター資料を一部変更

ＮＩＳＣの組織



内閣サイバーセキュリティセンター資料を一部変更

ご静聴ありがとうございました。
何かご質問は？