サイバー対処能力強化法整備法の一部施行に伴う
関係規則等の改廃について

・「サイバーセキュリティ戦略本部の運営について」の一部改正について

・「サイバーセキュリティ戦略本部重大事象施策評価規則」の一部改正について

・「サイバーセキュリティ対策を強化するための監査に係る基本方針」の一部改定について

・「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」の一部改正について

・「重要インフラのサイバーセキュリティに係る行動計画」の一部改定について

・「政府機関等のサイバーセキュリティ対策のための統一規範」の改定について

・「政府機関等のサイバーセキュリティ対策のための統一基準」の改定について

・「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の一部改定について

・「サイバーセキュリティ戦略本部長の指定する職について」の一部改正について

・「サイバーセキュリティ戦略本部の後援等名義の使用に関し必要な事項について」の一部改正について

・「サイバーセキュリティ対策推進会議等について」の一部改正について

・「サイバーセキュリティ基本法第 17 条第１項の規定に基づくサイバーセキュリティ協議会を組織する国務大臣の委嘱について」の一部改正について

・「重要インフラ専門調査会の設置について」等の廃止について

「サイバーセキュリティ戦略本部の運営について」の一部改正について

（令和７年６月27日
サイバーセキュリティ戦略本部決定）

サイバーセキュリティ戦略本部の運営について（平成27年２月10日サイバーセキュリティ戦略本部決定）の一部を次表のとおり改正する。

（下線部分は改正部分）

改　正　後	改　正　前
サイバーセキュリティ戦略本部の運営について 平成27年２月10日 サイバーセキュリティ戦略本部決定 <u>令和　年　月　日改正</u> サイバーセキュリティ戦略本部（以下「本部」という。）の運営について以下のとおり決定する。 １．本部会合への出席要請について 本部は、必要に応じ、関係者の出席を求めることができるものとする。 ２．議事の公開について 本部会合は非公開とし、議事概要は、原則として、本部会合終了後公開する。ただし、サイバーセキュリティ戦略本部長（以下「本部長」という。）が必要と認めるときは、議事概要の一部又は全部を公開しないものとすることができる。 ３．配布資料の公開について 本部会合で配布された資料は、原則として、本部会合終了後速やかに公開する。ただし、本部長が必要と認めるとき、または資料の提出者の同意が得ら	サイバーセキュリティ戦略本部の運営について 平成27年２月10日 サイバーセキュリティ戦略本部決定 サイバーセキュリティ戦略本部（以下「本部」という。）の運営について以下のとおり決定する。 １．本部会合への出席要請について 本部は、必要に応じ、関係者の出席を求めることができるものとする。 ２．議事の公開について 本部会合は非公開とし、議事概要は、原則として、本部会合終了後公開する。ただし、サイバーセキュリティ戦略本部長（以下「本部長」という。）が必要と認めるときは、議事概要の一部又は全部を公開しないものとすることができる。 ３．配布資料の公開について 本部会合で配布された資料は、原則として、本部会合終了後速やかに公開する。ただし、本部長が必要と認めるとき、または資料の提出者の同意が得ら

れない場合には、非公開とすることができる。 ４．内閣サイバー官は、１の事務について本部を、２及び３の事務について本部長を補佐する。 （略）	れない場合には、非公開とすることができる。 ４．内閣サイバーセキュリティセンター長は、１の事務について本部を、２及び３の事務について本部長を補佐する。 （略）

附　則

この決定は、令和７年７月１日から施行する。

「サイバーセキュリティ戦略本部重大事象施策評価規則」の一部改正について

（令和７年６月27日
サイバーセキュリティ戦略本部決定）

サイバーセキュリティ戦略本部重大事象施策評価規則（平成27年２月10日サイバーセキュリティ戦略本部決定）の一部を次表のとおり改正する。

（下線部分は改正部分）

改　正　後	改　正　前
サイバーセキュリティ戦略本部重大事象施策評価規則 平成27年２月10日 サイバーセキュリティ戦略本部決定 平成28年10月12日一部改正 平成31年４月１日一部改正 令和　年　月　日一部改正 サイバーセキュリティ基本法（平成26年法律第104号。以下「法」という。）第26条第１項第４号に規定する事務（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。）に関することに限る。）を適切に遂行するため、当該事務について、次のとおり定める。 （対象とする事象） 第１条　法第26条第１項第４号に規定する「国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する重大な事象」（以下「特定重大事象」という。）とは、国の行政機関、独立行政法人又は法第13条に規定する指定法人（以下「行政機関等」	サイバーセキュリティ戦略本部重大事象施策評価規則 平成27年２月10日 サイバーセキュリティ戦略本部決定 平成28年10月12日一部改正 平成31年４月１日一部改正 サイバーセキュリティ基本法（平成26年法律第104号。以下「法」という。）第26条第１項第３号に規定する事務を適切に遂行するため、当該事務について、次のとおり定める。 （対象とする事象） 第１条　法第26条第１項第３号に規定する「国の行政機関、独立行政法人又は指定法人で発生したサイバーセキュリティに関する重大な事象」（以下「特定重大事象」という。）とは、国の行政機関、独立行政法人又は法第13条に規定する指定法人（以下「行政機関

という。）で発生したサイバーセキュリティに関する事象のうち、次に掲げるものとする。 一～三　（略） （関係事務の処理等） 第９条　施策の評価に関する事務（特定重大事象に係る原因究明等の結果の審議及び復旧・再発防止策の評価を除く。）は、内閣官房国家サイバー統括室に行わせるものとする。ただし、法第32条の規定に基づく事務については、別に定めるところによる。 ２　緊急を要する場合における特定重大事象に係る原因究明等の結果及び復旧・再発防止策の評価は、前項の規定にかかわらず、内閣官房国家サイバー統括室が行うものとする。 ３　施策の評価に基づき法第28条第３項の規定による勧告を行う場合において、次に掲げる事務は、内閣官房国家サイバー統括室に行わせるものとする。	等」という。）で発生したサイバーセキュリティに関する事象のうち、次に掲げるものとする。 一～三　（略） （関係事務の処理等） 第９条　施策の評価に関する事務（特定重大事象に係る原因究明等の結果の審議及び復旧・再発防止策の評価を除く。）は、内閣サイバーセキュリティセンターに行わせるものとする。ただし、法第32条の規定に基づく事務については、別に定めるところによる。 ２　緊急を要する場合における特定重大事象に係る原因究明等の結果及び復旧・再発防止策の評価は、前項の規定にかかわらず、内閣サイバーセキュリティセンターが行うものとする。 ３　施策の評価に基づき法第28条第３項の規定による勧告を行う場合において、次に掲げる事務は、内閣サイバーセキュリティセンターに行わせるものとする。

附　則

この決定は、令和７年７月１日から施行する。

「サイバーセキュリティ対策を強化するための監査に係る基本方針」の
一部改定について

（令和７年６月27日
サイバーセキュリティ戦略本部決定）

サイバーセキュリティ対策を強化するための監査に係る基本方針（平成27年５月25日サイバーセキュリティ戦略本部決定）の一部を次表のとおり改定する。

（下線部分は改定部分）

改　定　後	改　定　前
サイバーセキュリティ対策を強化するための監査に係る基本方針 平成27年５月25日 サイバーセキュリティ戦略本部決定 平成28年10月12日一部改定 平成31年４月１日一部改定 令和７年５月29日一部改定 令和　年　月　日一部改定 ５　監査の進め方 (1)～(4)　（略） (5) 監査事務の処理 以上の監査事務については、内閣官房国家サイバー統括室に実施させる。独立行政法人及び指定法人における監査事務の一部については、法第31条第１項第１号の規定に基づき独立行政法人情報処理推進機構に委託し、同機構に実施させる。	サイバーセキュリティ対策を強化するための監査に係る基本方針 平成27年５月25日 サイバーセキュリティ戦略本部決定 平成28年10月12日一部改定 平成31年４月１日一部改定 令和７年５月29日一部改定 ５　監査の進め方 (1)～(4)　（略） (5) 監査事務の処理 以上の監査事務については、内閣サイバーセキュリティセンターに実施させる。独立行政法人及び指定法人における監査事務の一部については、法第31条第１項第１号の規定に基づき独立行政法人情報処理推進機構に委託し、同機構に実施させる。

附　則

この決定は、令和７年７月１日から施行する。

「政府情報システムにおけるクラウドサービスの
セキュリティ評価制度の基本的枠組みについて」の一部改正について

（令和７年６月27日
サイバーセキュリティ戦略本部決定）

政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて（令和２年１月30日サイバーセキュリティ戦略本部決定）の一部を次表のとおり改正する。

（下線部分は改正部分）

改　正　後	改　正　前
政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて 令和２年１月30日 サイバーセキュリティ戦略本部決定 令和３年９月27日一部改正 令和　年　月　日一部改正 ３　本制度の所管と運用体制 本制度の所管は内閣官房国家サイバー統括室・デジタル庁・総務省・経済産業省とする。また本制度の最高意思決定機関として、有識者と所管省庁を構成員とした制度運営委員会を設置し、事務局を内閣官房国家サイバー統括室に置く。 （略）	政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて 令和２年１月30日 サイバーセキュリティ戦略本部決定 令和３年９月27日一部改正 ３　本制度の所管と運用体制 本制度の所管は内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）・デジタル庁・総務省・経済産業省とする。また本制度の最高意思決定機関として、有識者と所管省庁を構成員とした制度運営委員会を設置し、事務局をNISCに置く。 （略）

附　則

この決定は、令和７年７月１日から施行する。

「重要インフラのサイバーセキュリティに係る行動計画」の
一部改定について

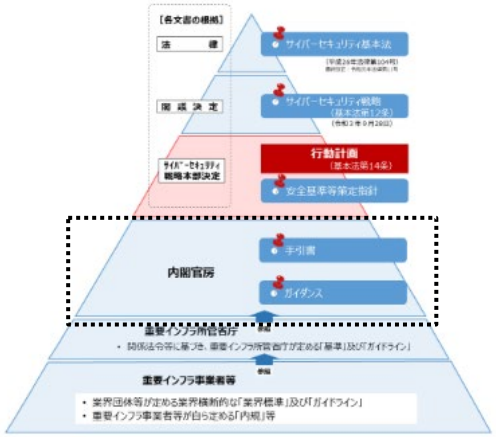
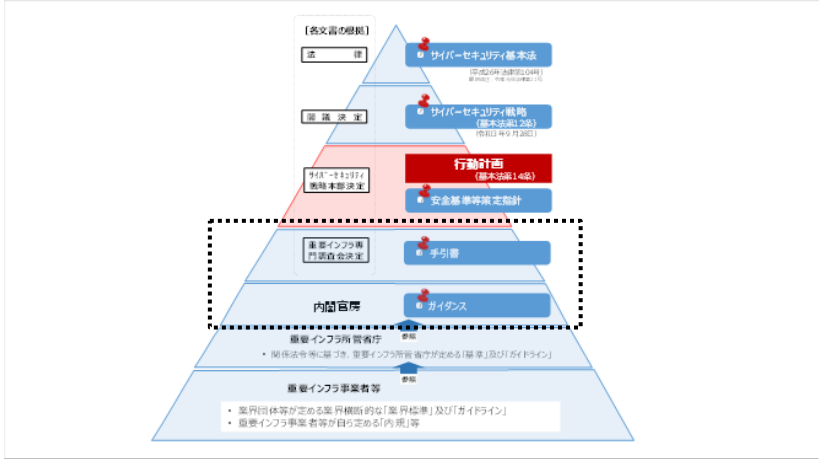
令和７年６月27日
サイバーセキュリティ戦略本部決定

重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）の一部を次表のとおり改定する。

（下線部分は改定部分）

改　定　後	改　定　前
重要インフラのサイバーセキュリティに係る行動計画 ２０２２年　６　月　１７日 サイバーセキュリティ戦略本部 ２０２４年　３　月　８　日 サイバーセキュリティ戦略本部改定 ２０２５年　　月　　日 サイバーセキュリティ戦略本部改定	重要インフラのサイバーセキュリティに係る行動計画 ２０２２年　６　月　１７日 サイバーセキュリティ戦略本部 ２０２４年　３　月　８　日 サイバーセキュリティ戦略本部改定
この行動計画は、サイバーセキュリティ基本法（平成26年法律第104号）第12条の規定に基づき策定するサイバーセキュリティ戦略を踏まえ、同法第14条（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）及び第26条第１項第６号（サイバーセキュリティ戦略本部の所掌事務）の規定に基づき策定するものである。	この行動計画は、サイバーセキュリティ基本法（平成26年法律第104号）第12条の規定に基づき策定するサイバーセキュリティ戦略を踏まえ、同法第14条（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）及び第26条第１項第５号（サイバーセキュリティ戦略本部の所掌事務）の規定に基づき策定するものである。

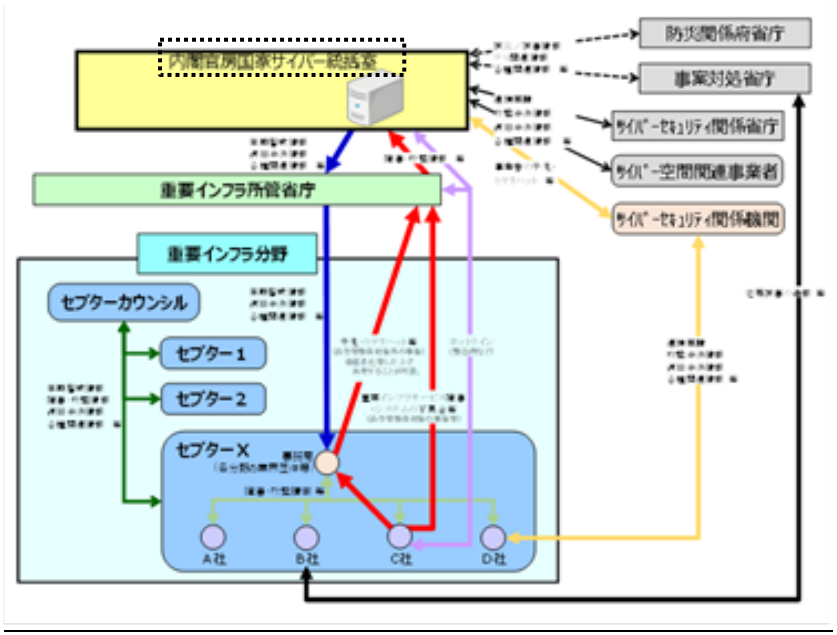
Ⅰ. 総論 3. サイバーセキュリティ基本法との整合性について 3.1 サイバーセキュリティ基本法における行動計画の位置付け 行動計画は、サイバーセキュリティ基本法(平成26年法律第104号)第12条の規定に基づき策定されるサイバーセキュリティ戦略を踏まえ、同法第14条(重要社会基盤事業者等におけるサイバーセキュリティの確保の促進)及び第26条第１項第６号(サイバーセキュリティ戦略本部の所掌事務)の規定に基づき策定される。 3.2・3.3　(略)	Ⅰ. 総論 3. サイバーセキュリティ基本法との整合性について 3.1 サイバーセキュリティ基本法における行動計画の位置付け 行動計画は、サイバーセキュリティ基本法(平成26年法律第104号)第12条の規定に基づき策定されるサイバーセキュリティ戦略を踏まえ、同法第14条(重要社会基盤事業者等におけるサイバーセキュリティの確保の促進)及び第26条第１項第５号(サイバーセキュリティ戦略本部の所掌事務)の規定に基づき策定される。 3.2・3.3　(略)
Ⅳ. 計画期間内の取組 1. 障害対応体制の強化 (略) 1.1　組織統治の一部としての障害対応体制 (略) (1) 組織統治に必要な観点 組織統治の一部として障害対応体制を強化するためには、「サイバーセキュリティ関係法令Q&Aハンドブック Ver2.0(令和５年９月 内閣官房内閣サイバーセキュリティセンター)」における４つの観点が必要となる。 (略) (2)　(略) 1.2～1.4　(略)	Ⅳ. 計画期間内の取組 1.障害対応体制の強化 (略) 1.1　組織統治の一部としての障害対応体制 (略) (1) 組織統治に必要な観点 組織統治の一部として障害対応体制を強化するためには、「サイバーセキュリティ関係法令Q&Aハンドブック Ver1.0(令和2年3月2日 内閣官房内閣サイバーセキュリティセンター)」における４つの観点が必要となる。 (略) (2)　(略) 1.2～1.4　(略)

2. 安全基準等の整備及び浸透  図 2 重要インフラ防護に関する安全基準等に係る体系	2. 安全基準等の整備及び浸透  図 2 重要インフラ防護に関する安全基準等に係る体系

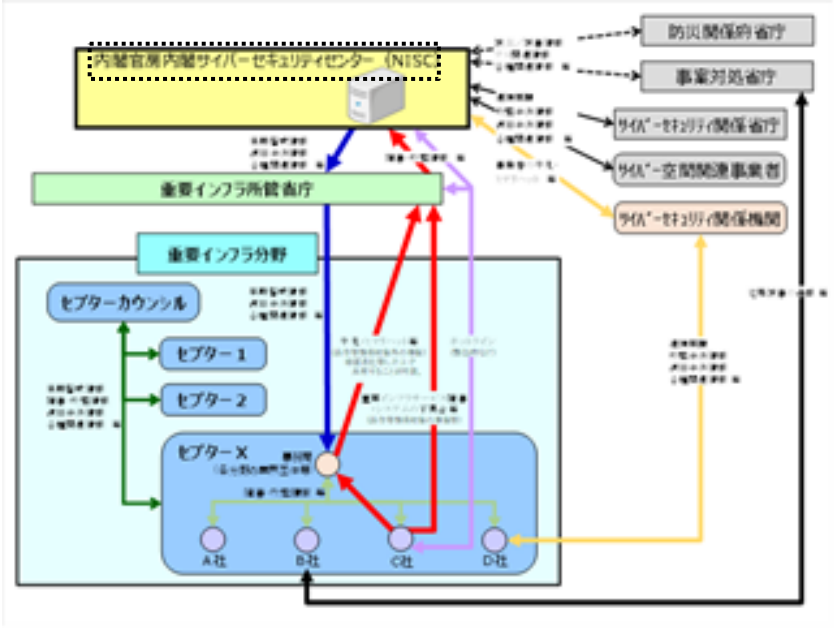
2.1　安全基準等策定指針の継続的改善 （略） (1) 組織統治に関する基準の整備 　組織統治の一部としてサイバーセキュリティを取り入れる方策に係る記載を強化すべく、「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0(令和５年９月 内閣官房内閣サイバーセキュリティセンター)」で規定している①内部統制システムとサイバーセキュリティとの関係、②サイバーセキュリティと取締役等の責任、③サイバーセキュリティ体制の適切性を担保するための監査等、④サイバーセキュリティと情報開示、を活用するなどして、安全基準等策定指針の記載を充実させる。 2.2～2.4　（略）	2.1　安全基準等策定指針の継続的改善 （略） (1) 組織統治に関する基準の整備 　組織統治の一部としてサイバーセキュリティを取り入れる方策に係る記載を強化すべく、「サイバーセキュリティ関係法令 Q&A ハンドブック ver1.0」（令和２年３月２日)で規定している①内部統制システムとサイバーセキュリティとの関係、②サイバーセキュリティと取締役等の責任、③サイバーセキュリティ体制の適切性を担保するための監査等、④サイバーセキュリティと情報開示、を活用するなどして、安全基準等策定指針の記載を充実させる。 2.2～2.4　（略）
3.　情報共有体制の強化 3.1　本行動計画期間における情報共有体制 （略） 　なお、サイバーセキュリティ戦略本部長がサイバーセキュリティ基本法第28条第3項の規定に基づき、同法第32条(資料提供等)又は第33条(資料の提出その他の協力)の規定に基づき重要インフラ所管省庁の長又は重要インフラ事業者等の長若しくは代表者からサイバーセキュリティ戦略本部に提供された重要インフラ事業者等のサイバーセキュリティに関する資料、情報等に基づき、重要インフラ所管省庁の長に勧告できる等の仕組みを、その事務を行う内閣官房(国家サイバー統括室)は適切に運用する。 （略）	3.　情報共有体制の強化 3.1　本行動計画期間における情報共有体制 （略） 　なお、サイバーセキュリティ戦略本部長がサイバーセキュリティ基本法第28条第3項の規定に基づき、同法第32条(資料提供等)又は第33条(資料の提出その他の協力)の規定に基づき重要インフラ所管省庁の長又は重要インフラ事業者等の長若しくは代表者からサイバーセキュリティ戦略本部に提供された重要インフラ事業者等のサイバーセキュリティに関する資料、情報等に基づき、重要インフラ所管省庁の長に勧告できる等の仕組みを、その事務を行う内閣官房(内閣サイバーセキュリティセンター)は適切に運用する。 （略）

3.2～3.4　（略）	3.2～3.4　（略）
Ⅵ. 評価・検証 1. 本行動計画の評価 1.1 評価運営 （略） なお、本行動計画の評価は、サイバーセキュリティ戦略本部が実施するものとする。 （略）	Ⅵ. 評価・検証 1. 本行動計画の評価 1.1 評価運営 （略） なお、本行動計画の評価は、サイバーセキュリティ戦略本部が実施し、そのために必要な調査・検討は重要インフラ所管省庁の協力を得て重要インフラ専門調査会で行うものとする。 （略）
1.2　（略） 2. 本行動計画の検証 2.1 検証運営 （略） なお、本行動計画の検証は、サイバーセキュリティ戦略本部の主管の下、重要インフラ事業者等及び重要インフラ所管省庁の協力を得て各年度に内閣官房が行い、サイバーセキュリティ戦略本部に付議するものとする。 （略） 2.2・2.3　（略）	1.2　（略） 2. 本行動計画の検証 2.1 検証運営 （略） なお、本行動計画の検証は、サイバーセキュリティ戦略本部の主管の下、重要インフラ事業者等及び重要インフラ所管省庁の協力を得て各年度に内閣官房が行い、重要インフラ専門調査会での審議を経て、サイバーセキュリティ戦略本部に付議するものとする。 （略） 2.2・2.3　（略）
Ⅶ. 本行動計画の見直し 本行動計画の見直しは、本行動計画の評価を踏まえ、サイバーセキュリティ戦略本部において実施する。 （略）	Ⅶ. 本行動計画の見直し 本行動計画の見直しは、本行動計画の評価を踏まえ、サイバーセキュリティ戦略本部において実施し、そのために必要な調査・検討は、重要インフラ所管省庁の協力を得て重要インフラ専門調査会で行う。 （略）

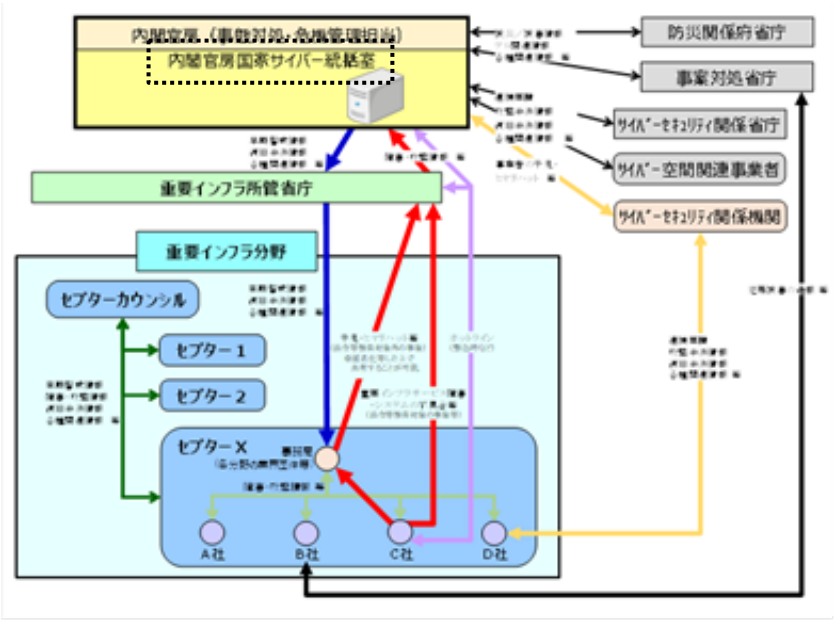
別紙４－１　情報共有体制（通常時）



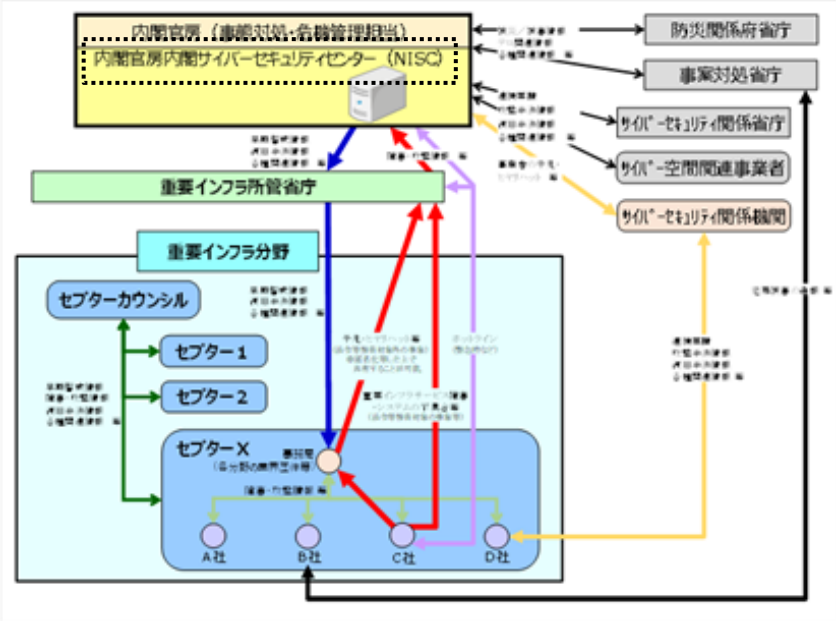
別紙４－１　情報共有体制（通常時）



別紙４－２　情報共有体制（大規模重要インフラサービス障害対応時）



別紙４－２　情報共有体制（大規模重要インフラサービス障害対応時）



別紙４－３　情報共有体制における各関係主体の役割

関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における各関係主体の役割
○ 内閣官房 （事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、国家サイバー統括室と相互に情報の共有を行う。	通常時の役割に加え、国家サイバー統括室と一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、国家サイバー統括室と相互に情報の共有を行う。
○ 内閣官房 （国家サイバー統括室）	重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処	内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所

別紙４－３　情報共有体制における各関係主体の役割

関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における各関係主体の役割
○ 内閣官房 （事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、ＮＩＳＣと相互に情報の共有を行う。	通常時の役割に加え、ＮＩＳＣと一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、ＮＩＳＣと相互に情報の共有を行う。
○ 内閣官房 （ＮＩＳＣ）	重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処	内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所

	省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。	管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。		省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。	管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。
○ 重要インフラ所管省庁	所管する重要インフラ事業者等から受領したシステムの不具合等に関する情報を国家サイバー統括室及び必要に応じ該当するセプターに連絡する。国家サイバー統括室から受領したシステム	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応時の体制に協力する。		○ 重要インフラ所管省庁	所管する重要インフラ事業者等から受領したシステムの不具合等に関する情報をＮＩＳＣ及び必要に応じ該当するセプターに連絡する。ＮＩＳＣから受領したシステムの不具合等に関する情報	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応時の体制に協力する。

	の不具合等に関する情報を該当するセプターに提供する。			を該当するセプターに提供する。	

附　則

この決定は、令和７年７月１日から施行する。

「政府機関等のサイバーセキュリティ対策のための統一規範」の
改定について

（令和７年６月27日
サイバーセキュリティ戦略本部決定）

政府機関等のサイバーセキュリティ対策のための統一規範（令和５年７月４日サイバーセキュリティ戦略本部決定）を次表のとおり改定する。

（下線部分は改定部分）

改　定　後	改　定　前
政府機関等のサイバーセキュリティ対策のための統一規範 平成28年８月31日 平成30年７月25日改定 平成31年４月１日改定 令和３年７月７日改定 令和５年７月４日改定 令和　年　月　日改定 サイバーセキュリティ戦略本部決定	政府機関等のサイバーセキュリティ対策のための統一規範 平成28年８月31日 平成30年７月25日改定 平成31年４月１日改定 令和３年７月７日改定 令和５年７月４日改定 サイバーセキュリティ戦略本部決定
（策定） 第二十四条　本規範は、内閣官房国家サイバー統括室が原案を策定し、サイバーセキュリティ戦略本部において決定する。	（策定） 第二十四条　本規範は、内閣官房内閣サイバーセキュリティセンターが原案を策定し、サイバーセキュリティ対策推進会議（平成27年２月10日サイバーセキュリティ戦略本部長決定）を経てサイバーセキュリティ戦略本部において決定する。
（略）	（略）

附　則

この決定は、令和７年７月１日から施行する。

「政府機関等のサイバーセキュリティ対策のための統一基準」の
改定について

（令和７年６月27日
サイバーセキュリティ戦略本部決定）

政府機関等のサイバーセキュリティ対策のための統一基準（令和５年７月４日サイバーセキュリティ戦略本部決定）を次表のとおり改定する。

（下線部分は改定部分）

改　定　後	改　定　前
政府機関等のサイバーセキュリティ対策のための統一基準（令和７年度版）	政府機関等のサイバーセキュリティ対策のための統一基準（令和５年度版）
令和　　年　　月　　日 サイバーセキュリティ戦略本部	令和５年７月４日 サイバーセキュリティ戦略本部
第１部　総則 1.1　本統一基準の目的・適用範囲 (1)・(2)　（略） (3)　本統一基準の改定 情報セキュリティ水準を適切に維持していくためには、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。 このため、情報技術の進歩に応じて、本統一基準を定期的に点検し、必要に応じ規定内容の追加・修正等の改定を行う。本統一基準の原案は、内閣官房国家サイバー統括室が策定し、サイバーセキュリティ戦略本部において決定する。 なお、内閣官房国家サイバー統括室は、新たな脅威の発生や機関等における運用	第１部　総則 1.1　本統一基準の目的・適用範囲 (1)・(2)　（略） (3)　本統一基準の改定 情報セキュリティ水準を適切に維持していくためには、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。 このため、情報技術の進歩に応じて、本統一基準を定期的に点検し、必要に応じ規定内容の追加・修正等の改定を行う。本統一基準の原案は、内閣官房内閣サイバーセキュリティセンターが策定し、サイバーセキュリティ対策推進会議（平成27年２月10日サイバーセキュリティ戦略本部長決定）を経てサイバーセキュリティ戦略本部において決定する。 なお、内閣官房内閣サイバーセキュリティセンターは、新たな脅威の発生や機

の状況を定期的に点検した結果を踏まえ、次の点に留意の上、原案の策定を行う。	関等における運用の状況を定期的に点検した結果を踏まえ、次の点に留意の上、原案の策定を行う。
(4)　(略)	(4)　(略)
(5)　機関等の対策基準	(5)　機関等の対策基準
本統一基準では、機関等が行うべき対策について、目的別に部、節及び款の３階層にて対策項目を分類し、各款に対して目的及び趣旨並びに遵守事項を示している。	本統一基準では、機関等が行うべき対策について、目的別に部、節及び款の３階層にて対策項目を分類し、各款に対して目的及び趣旨並びに遵守事項を示している。
内閣官房国家サイバー統括室が別途策定する政府機関等の対策基準策定のためのガイドラインには、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）が例示されるとともに、対策基準の策定及び実施に際しての考え方等が解説されている。基本対策事項は遵守事項に対応するものであるため、機関等は基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより、対応する遵守事項を満たす必要がある。	内閣官房内閣サイバーセキュリティセンターが別途策定する政府機関等の対策基準策定のためのガイドラインには、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）が例示されるとともに、対策基準の策定及び実施に際しての考え方等が解説されている。基本対策事項は遵守事項に対応するものであるため、機関等は基本対策事項に例示される対策又はこれと同等以上の対策を講じることにより、対応する遵守事項を満たす必要がある。
（略）	（略）
1.2　(略)	1.2　(略)
1.3　用語定義	1.3　用語定義
（略）	（略）
●　「CYMAT」とは、サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房国家サイバー統括室に設置される体制をいう。Cyber Incident Mobile Assistance Team（情報セキュリティ緊急支援	●　「CYMAT」とは、サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team（情報セキュ

チーム）の略。 （略） ●　「GSOC」とは、24時間365日、政府横断的な情報収集、攻撃等の分析・解析、政府機関への助言、政府関係機関の相互連携促進及び情報共有等の業務を行うため、内閣官房国家サイバー統括室に設置される体制をいう。Government Security Operation Coordination Team（政府機関情報セキュリティ横断監視・即応調整チーム）の略。なお、GSOCには、政府機関を対象とした「第一GSOC」と独立行政法人及び指定法人を対象とした「第二GSOC」がある。 （略）	リティ緊急支援チーム）の略。 （略） ●　「GSOC」とは、24時間365日、政府横断的な情報収集、攻撃等の分析・解析、政府機関への助言、政府関係機関の相互連携促進及び情報共有等の業務を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Government Security Operation Coordination Team（政府機関情報セキュリティ横断監視・即応調整チーム）の略。なお、GSOCには、政府機関を対象とした「第一GSOC」と独立行政法人及び指定法人を対象とした「第二GSOC」がある。 （略）
第２部　情報セキュリティ対策の基本的枠組み 2.1　（略） 2.2　運用 2.2.1～2.2.3　（略） 2.2.4　情報セキュリティインシデントへの対処 （略） (1)・(2)　（略） (3)　情報セキュリティインシデントに係る情報共有 (a)　国の行政機関におけるCSIRTは、当該機関の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房国家サイバー統括室に連絡すること。また、独立行政法人及び指定法人におけるCSIRTは、当該法人の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速	第２部　情報セキュリティ対策の基本的枠組み 2.1　（略） 2.2　運用 2.2.1～2.2.3　（略） 2.2.4　情報セキュリティインシデントへの対処 （略） (1)・(2)　（略） (3)　情報セキュリティインシデントに係る情報共有 (a)　国の行政機関におけるCSIRTは、当該機関の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房内閣サイバーセキュリティセンターに連絡すること。また、独立行政法人及び指定法人におけるCSIRTは、当該法人の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事

やかに、当該法人を所管する国の行政機関に連絡すること。この連絡を受けた国の行政機関におけるCSIRTは、当該事象について速やかに、内閣官房国家サイバー統括室に連絡すること。 2.3～2.5　（略）	象について速やかに、当該法人を所管する国の行政機関に連絡すること。この連絡を受けた国の行政機関におけるCSIRTは、当該事象について速やかに、内閣官房内閣サイバーセキュリティセンターに連絡すること。 2.3～2.5　（略）

附　則

この決定は、令和７年７月１日から施行する。

「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の
一部改定について

（令和７年６月27日
サイバーセキュリティ戦略本部決定）

重要インフラのサイバーセキュリティに係る安全基準等策定指針（2023年７月４日サイバーセキュリティ戦略本部決定）の一部を次表のとおり改定する。

（下線部分は改定部分）

改　定　後	改　定　前
重要インフラのサイバーセキュリティに係る安全基準等策定指針 ２０２３年　７　月　４　日 サイバーセキュリティ戦略本部 ２０２５年　　月　　日 一　　部　　改　　定	重要インフラのサイバーセキュリティに係る安全基準等策定指針 ２０２３年　７　月　４　日 サイバーセキュリティ戦略本部
３．　組織統治におけるサイバーセキュリティ 脚注4　経済産業省「サイバーセキュリティ経営ガイドライン」、内閣官房国家サイバー統括室（以下「統括室」という。）「サイバーセキュリティ関係法令　Q&A　ハンドブック」が参考になる。	３．　組織統治におけるサイバーセキュリティ 脚注4　経済産業省「サイバーセキュリティ経営ガイドライン」、内閣サイバーセキュリティセンター（以下「NISC」という。）「サイバーセキュリティ関係法令　Q&A　ハンドブック」が参考になる。
3.4　責任及び権限の割当て 脚注8　（略） また、サイバーセキュリティに関する内部統制システムの構築において、「必要な内部組織及び権限」等について取締役会で決定されるべき事項としている。（NISC「サイバーセキュリティ関係法令Q&A　ハンドブックVer2.0」〔令和５年９月〕）	3.4　責任及び権限の割当て 脚注8　（略） また、サイバーセキュリティに関する内部統制システムの構築において、「必要な内部組織及び権限」等について取締役会で決定されるべき事項としている。（NISC「サイバーセキュリティ関係法令Q&A　ハンドブック」〔2020年3　月2　日〕）

４．　リスクマネジメントの活用と危機管理 4.1　組織状況の理解 脚注13　例えば、重要インフラの事業法、個人情報の保護に関する法律（平成 15年法律第57号）、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第43号）等。NISC「サイバーセキュリティ関係法令　Q&Aハンドブック Ver2.0」を参照。 （略） 4.8　平時の運用 4.8.1　セキュリティ対策の導入、運用プロセスの確立・実行 4.8.2　情報共有 統括室「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス 」（令和５年３月８日サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会）も踏まえ、組織内外と情報共有を実施する。 （略） 4.10　演習・訓練 脚注23　例えば、統括室が主催する「全分野一斉演習」。	４．　リスクマネジメントの活用と危機管理 4.1　組織状況の理解 脚注13　例えば、重要インフラの事業法、個人情報の保護に関する法律（平成 15年法律第57号）、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第43号）等。 NISC「サイバーセキュリティ関係法令Q&Aハンドブック」を参照。 （略） 4.8　平時の運用 4.8.1　セキュリティ対策の導入、運用プロセスの確立・実行 4.8.2　情報共有 NISC「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス 」（令和５年３月８日サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会）も踏まえ、組織内外と情報共有を実施する。 （略） 4.10　演習・訓練 脚注23　例えば、NISCが主催する「分野横断的演習」。

附　則

この決定は、令和７年７月１日から施行する。

「サイバーセキュリティ戦略本部長の指定する職について」の一部改正について

令和７年６月27日
サイバーセキュリティ戦略本部長決定案

サイバーセキュリティ戦略本部長の指定する職について（平成27年２月10日サイバーセキュリティ戦略本部長決定）の一部を次のように改正する。

次の表により、改正前欄に掲げる規定の破線で囲んだ部分をこれに対応する改正後欄に掲げる規定の破線で囲んだ部分のように改める。

改　正　後	改　正　前
「サイバーセキュリティ対策推進会議等について」（平成27年２月10日サイバーセキュリティ戦略本部長決定）第２項の規定に基づき、サイバーセキュリティ対策推進会議の構成員及びオブザーバーについて、以下の職を指定する。 構　成　員　内閣総務官 内閣官房副長官補（内政） 内閣官房副長官補（事態対処・危機管理） 内閣広報官 内閣情報官 内閣サイバー官 内閣法制局総務主幹 人事院事務総局総括審議官 内閣府大臣官房長	「サイバーセキュリティ対策推進会議等について」（平成27年２月10日サイバーセキュリティ戦略本部長決定）第２項の規定に基づき、サイバーセキュリティ対策推進会議の構成員及びオブザーバーについて、以下の職を指定する。 構　成　員　内閣総務官 内閣官房副長官補（内政） 内閣官房副長官補（事態対処・危機管理） 内閣広報官 内閣情報官 内閣法制局総務主幹 人事院事務総局総括審議官 内閣府大臣官房長

宮内庁長官官房審議官	宮内庁長官官房審議官
公正取引委員会事務総局官房総括審議官	公正取引委員会事務総局官房総括審議官
警察庁長官官房長	警察庁長官官房長
警察庁サイバー警察局長	警察庁サイバー警察局長
個人情報保護委員会事務局長	個人情報保護委員会事務局長
カジノ管理委員会事務局次長	カジノ管理委員会事務局次長
金融庁総合政策局総括審議官	金融庁総合政策局総括審議官
消費者庁次長	消費者庁次長
こども家庭庁長官官房長	こども家庭庁長官官房長
デジタル庁統括官（戦略・組織担当）	デジタル庁統括官（戦略・組織担当）
復興庁統括官	復興庁統括官
総務省大臣官房長	総務省大臣官房長
総務省サイバーセキュリティ統括官	総務省サイバーセキュリティ統括官
法務省大臣官房長	法務省大臣官房長
外務省大臣官房長	外務省大臣官房長
財務省大臣官房長	財務省大臣官房長
文部科学省大臣官房長	文部科学省大臣官房長
厚生労働省厚生労働審議官	厚生労働省厚生労働審議官
農林水産省大臣官房長	農林水産省大臣官房長
経済産業省大臣官房長	経済産業省大臣官房長
経済産業省商務情報政策局長	経済産業省商務情報政策局長
国土交通省大臣官房政策立案総括審議官	国土交通省大臣官房政策立案総括審議官
環境省大臣官房長	環境省大臣官房長
防衛省整備計画局長	防衛省整備計画局長

オブザーバー　衆議院事務局庶務部情報管理監 参議院事務局庶務部長 国立国会図書館電子情報部長 会計検査院事務総局次長 最高裁判所事務総局情報政策課長 日本銀行理事	オブザーバー　衆議院事務局庶務部情報管理監 参議院事務局庶務部長 国立国会図書館電子情報部長 会計検査院事務総局次長 最高裁判所事務総局情報政策課長 日本銀行理事

附　則

この決定は、令和７年７月１日から施行する。

「サイバーセキュリティ戦略本部の後援等名義の使用に関し必要な事項について」の一部改正について

（令和７年６月27日
サイバーセキュリティ戦略本部長決定案）

サイバーセキュリティ戦略本部の後援等名義の使用に関し必要な事項について（平成27年２月10日サイバーセキュリティ戦略本部長決定）の一部を次のように改正する。

次の表により、改正前欄に掲げる規定の下線を付した部分をこれに対応する改正後欄に掲げる規定の下線を付した部分のように改める。

改　正　後	改　正　前
二　後援等名義の使用の承認に関する事項については、内閣サイバー官が処理する。	二　後援等名義の使用の承認に関する事項については、内閣サイバーセキュリティセンター長（以下「センター長」という。）が処理する。
三　後援等名義の使用の承認は、行事等の主催者、制作者、発行者等（以下「主催者等」という。）が、別記様式による申請書に関係書類を添えて、当該行事等の１か月前（印刷物等に後援等名義を掲載する場合には、その制作の１か月前）までに、内閣サイバー官に対して行った申請につき、四に定める基準に適合するものに対して行うものとする。	三　後援等名義の使用の承認は、行事等の主催者、制作者、発行者等（以下「主催者等」という。）が、別記様式による申請書に関係書類を添えて、当該行事等の１か月前（印刷物等に後援等名義を掲載する場合には、その制作の１か月前）までに、センター長に対して行った申請につき、四に定める基準に適合するものに対して行うものとする。
五　後援等名義の使用の承認後においても、内閣サイバー官は、行事等について主催者等又は関係者が本決定の趣旨に反する行為を行わないよう常に注意するとともに、主催者等又	五　後援等名義の使用の承認後においても、センター長は、行事等について主催者等又は関係者が本決定の趣旨に反する行為を行わないよう常に注意するとともに、主催者等又は関

は関係者が当該行為を行っている場合には、主催者等に対しその行為の中止又は是正を求めるものとする。	係者が当該行為を行っている場合には、主催者等に対しその行為の中止又は是正を求めるものとする。
六　主催者等が五による中止又は是正の求めに従わない場合は、内閣サイバー官は、承認を取り消し、速やかに当該主催者等に通知するとともに、必要な措置を講じなければならない。	六　主催者等が五による中止又は是正の求めに従わない場合は、センター長は、承認を取り消し、速やかに当該主催者等に通知するとともに、必要な措置を講じなければならない。
七　内閣サイバー官は、行事等の終了後速やかに、主催者等から行事等の実施内容、収支決算その他必要な事項を記載した結果報告書の提出を求めるものとする。	七　センター長は、行事等の終了後速やかに、主催者等から行事等の実施内容、収支決算その他必要な事項を記載した結果報告書の提出を求めるものとする。
八　本決定の実施に関しその他補足的に必要な事項は、内閣サイバー官が定める。	八　本決定の実施に関しその他補足的に必要な事項は、センター長が定める。

別紙様式 年　月　日 内閣官房内閣サイバー官 ○○ ○○　殿 申請者住所 氏名（※）　　印 ※法人又は団体にあっては、名称及び代表者氏名 ○○○○に対するサイバーセキュリティ戦略本部の後援等名義の使用の承認申請について 下記○○○○に対するサイバーセキュリティ戦略本部の［後援／協賛／賛助／監修 等］名義の使用の承認を受けたいので、関係書類を添えて申請します。 記 1　行事等の名称及び目的 2　行事等の主催者 3　行事等の期間（期日）及び場所 （添付書類）	別紙様式 年　月　日 内閣官房内閣サイバーセキュリティセンター長 ○○ ○○　殿 申請者住所 氏名（※）　　印 ※法人又は団体にあっては、名称及び代表者氏名 ○○○○に対するサイバーセキュリティ戦略本部の後援等名義の使用の承認申請について 下記○○○○に対するサイバーセキュリティ戦略本部の［後援／協賛／賛助／監修 等］名義の使用の承認を受けたいので、関係書類を添えて申請します。 記 1　行事等の名称及び目的 2　行事等の主催者 3　行事等の期間（期日）及び場所 （添付書類）

1　行事等の概要（議事次第、出席者、出品内容、使用施設、入場料、後援等の団体等）を明らかにする書類 2　行事等の収支予算書 3　主催者等が民間団体の場合には、定款又は寄附行為、会則、役員名簿、活動状況等団体の性格及び内容を明らかにする書類 4　その他必要書類	1　行事等の概要（議事次第、出席者、出品内容、使用施設、入場料、後援等の団体等）を明らかにする書類 2　行事等の収支予算書 3　主催者等が民間団体の場合には、定款又は寄附行為、会則、役員名簿、活動状況等団体の性格及び内容を明らかにする書類 4　その他必要書類
備考　表中の［ ］の記載は注記である。	

附　則

この決定は、令和７年７月１日から施行する。

「サイバーセキュリティ対策推進会議等について」の一部改正について

（令和７年６月27日
サイバーセキュリティ戦略本部長決定案）

サイバーセキュリティ対策推進会議等について（平成27年２月10日サイバーセキュリティ戦略本部長決定）の一部を次のように改正する。

次の表により、改正前欄に掲げる規定の下線を付した部分をこれに対応する改正後欄に掲げる規定の下線を付した部分のように改める。

改　正　後	改　正　前
１　サイバーセキュリティ基本法施行令（平成26年政令第400号）第５条の規定に基づき、関係行政機関の最高情報セキュリティ責任者（CISO）等相互の緊密な連携の下、政府機関におけるサイバーセキュリティ対策の推進を図るため、サイバーセキュリティ戦略本部（以下「本部」という。）に、サイバーセキュリティ対策推進会議（以下「推進会議」という。）を置く。 ［２～７　略］	１　サイバーセキュリティ基本法施行令（平成26年政令第400号）第４条の規定に基づき、関係行政機関の最高情報セキュリティ責任者（CISO）等相互の緊密な連携の下、政府機関におけるサイバーセキュリティ対策の推進を図るため、サイバーセキュリティ戦略本部（以下「本部」という。）に、サイバーセキュリティ対策推進会議（以下「推進会議」という。）を置く。 ［２～７　同左］
備考　表中の［ ］の記載は注記である。	

附　則

この決定は、令和７年７月１日から施行する。

「サイバーセキュリティ基本法第17条第１項の規定に基づくサイバーセキュリティ協議会を組織する国務大臣の委嘱について」の一部改正について

令和７年６月27日
サイバーセキュリティ戦略本部長決定案

サイバーセキュリティ基本法第17条第１項の規定に基づくサイバーセキュリティ協議会を組織する国務大臣の委嘱について（平成31年４月１日サイバーセキュリティ戦略本部長決定）の一部を次のように改正する。

次の表により、改正前欄に掲げる規定の破線で囲んだ部分をこれに対応する改正後欄に掲げる規定の破線で囲んだ部分のように改める。

改　正　後	改　正　前
サイバーセキュリティ基本法（平成26年法律第104号）第17条第１項の規定に基づき、サイバーセキュリティ協議会を組織する国務大臣として以下の者を委嘱する。	サイバーセキュリティ基本法（平成26年法律第104号）第17条第１項の規定に基づき、サイバーセキュリティ協議会を組織する国務大臣として以下の者を委嘱する。
内閣官房長官 サイバーセキュリティ戦略本部に関する事務を担当する国務大臣	サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
国家公安委員会委員長 デジタル大臣 総務大臣 外務大臣 経済産業大臣 防衛大臣	国家公安委員会委員長 デジタル大臣 総務大臣 外務大臣 経済産業大臣 防衛大臣

経済安全保障担当大臣	経済安全保障担当大臣

附　則

この決定は、令和７年７月１日から施行する。

「重要インフラ専門調査会の設置について」等の廃止について

（令和７年６月27日
サイバーセキュリティ戦略本部決定）

次の各号に掲げる決定については、廃止する。

一　重要インフラ専門調査会の設置について（平成27年２月10日サイバーセキュリティ戦略本部決定）

二　研究開発戦略専門調査会の設置について（平成27年２月10日サイバーセキュリティ戦略本部決定）

三　普及啓発・人材育成専門調査会の設置について（平成27年２月10日サイバーセキュリティ戦略本部決定）

附　則

この決定は、令和７年６月 30 日から施行する。