資料５

サイバーセキュリティ基本法の一部改正に伴う関係規則等の改正について

資料５－１　サイバーセキュリティ基本法の一部改正に伴う関係規則等の改正について

資料５－２　サイバーセキュリティ基本法の一部改正に伴う関係規則等の改正（新旧対照表）

資料５－３　サイバーセキュリティ基本法の一部改正に伴う関係規則等の改正後の規則等

サイバーセキュリティ基本法の一部改正に伴う関係規則等の改正について

資料5－1

サイバーセキュリティ基本法の一部改正に伴う関係規則等（別紙のとおり）の改正について所要の手続（サイバーセキュリティ戦略本部長の了解等）を経て、平成31年（2019年）4月1日に行ったので、報告するもの。

（参考）対象となった関係規則の例

サイバーセキュリティ戦略本部重大事象施策評価規則新旧対照案（※条番号の繰り下がり関係部分のみ抜粋）

改正	旧
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。（以下、略）	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25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。（以下、略）

重要インフラ専門調査会の設置について（※引用する施行令の名称が変更された部分のみ抜粋）

改正	旧
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2条の規定に基づき、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、重要インフラ専門調査会（以下「専門調査会」という。）を置く。	1. **サイバーセキュリティ戦略本部令**（平成26年政令第400号）第2条の規定に基づき、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、重要インフラ専門調査会（以下「専門調査会」という。）を置く。

(参考)サイバーセキュリティ基本法の一部改正に伴う関係規則等の改正について

（平成31年（2019年）１月24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が決定した規則等のうち、改正対象の法令を引用する規則等については、改正法の施行等に伴い、当該規則等が引用する法の条項の変更などの技術的な改正が必要。
- ✓ 改正法等が施行された日（平成31年４月１日）において、サイバーセキュリティ戦略本部が決定した規則等の技術的な改正を、サイバーセキュリティ戦略本部として行うものとする。
- ✓ なお、本改正については、サイバーセキュリティ戦略本部長の了解を得て行うものとし、その内容を事後に、サイバーセキュリティ戦略本部に報告するものとする。

(参考)サイバーセキュリティ基本法の一部を改正する法律（平成30年法律第91号。以下「改正法」という。）（※本件関係部分）

- ✓ 「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。）に第17条（サイバーセキュリティ協議会）を新設。改正法の施行後、現行の法第17条が第18条になる等の法第17条以降の条番号が繰り下がる。
- ✓ サイバーセキュリティ戦略本部の所掌事務として「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に関すること」を追加し、当該事務の一部を政令で定める法人に委託することができる（改正後の法第26条第１項第４号、第31条第１項第２号）としており、関係政令の整備（平成31年３月8日閣議決定、平成31年４月1日施行）が行われた。

改正対象の関係規則等の一覧

サイバーセキュリティ基本法及び関係政令を引用する規則等（※サイバーセキュリティ戦略本部長の了解を得た）

＜平成31年(2019年)1月24日サイバーセキュリティ戦略本部決定の対象一覧＞

[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[引用する条項：基本法第25条第1項第3号]
- サイバーセキュリティ戦略本部資料提供等規則[引用する条項：基本法第31条及び法第32条]
- サイバーセキュリティ戦略本部の後援等名義の使用について[引用する条項：基本法第22条]
- 政府機関等の情報セキュリティ対策のための統一規範[引用する条項：基本法第25条第1項第2号]
- 政府機関等の情報セキュリティ対策の運用等に関する指針[引用する条項：基本法第25条第1項第2号]
- 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[引用する条項：基本法第25条第1項第2号]
- 重要インフラ専門調査会の設置について[引用する条項：サイバーセキュリティ戦略本部令第2条]
- 研究開発戦略専門調査会の設置について[引用する条項：サイバーセキュリティ戦略本部令第2条]
- 普及啓発・人材育成専門調査会の設置について[引用する条項：サイバーセキュリティ戦略本部令第2条]

サイバーセキュリティ基本法及び関係政令を引用する決定等（※必要な決裁手続を行った）

[サイバーセキュリティ戦略本部長決定]

- サイバーセキュリティ対策推進会議等について[引用する条項：サイバーセキュリティ戦略本部令(平成26年政令第400号)第4条]

[内閣総理大臣決定]

- サイバーセキュリティ戦略本部の本部員の指定について[引用する条項：基本法第29条第2項第6号]

○サイバーセキュリティ戦略本部重大事象施策評価規則　新旧対照表

一部改定案	現　行
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 一部改定 平成 31 年４月１日 一部改定	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 平成 28 年 10 月 12 日 一部改定
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。	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 25 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）	（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。	第１条　法第 25 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　行政機関等が運用する情報システムにおける障害を伴う事象であって、当該行政機関等が実施する事務の遂行に著しい支障を及ぼし、又は及ぼすおそれがあるもの	一　行政機関等が運用する情報システムにおける障害を伴う事象であって、当該行政機関等が実施する事務の遂行に著しい支障を及ぼし、又は及ぼすおそれがあるもの
二　情報の漏えいを伴う事象であって、国民生活又は社会経済に重大な影響を与え、又は与えるおそれがあるもの	二　情報の漏えいを伴う事象であって、国民生活又は社会経済に重大な影響を与え、又は与えるおそれがあるもの
三　前各号に掲げるもののほか、我が国のサイバーセキュリティに対する国内外の信用を著しく失墜させ、又は失墜させるおそれがある事象	三　前各号に掲げるもののほか、我が国のサイバーセキュリティに対する国内外の信用を著しく失墜させ、又は失墜させるおそれがある事象
（関係行政機関との連携等）	（関係行政機関との連携等）

第２条　サイバーセキュリティ戦略本部(以下「本部」という。）による特定重大事象に対する施策の評価（以下単に「施策の評価」という。）に当たっては、特定重大事象が発生した行政機関等（以下「当該行政機関等」という。）その他の関係行政機関との緊密な連携を図るとともに、秘密の保持に十分留意するものとする。	第２条　サイバーセキュリティ戦略本部（以下「本部」という。）による特定重大事象に対する施策の評価（以下単に「施策の評価」という。）に当たっては、特定重大事象が発生した行政機関等（以下「当該行政機関等」という。）その他の関係行政機関との緊密な連携を図るとともに、秘密の保持に十分留意するものとする。
（施策の評価の手順等）	（施策の評価の手順等）
第３条　施策の評価は、次に掲げる段階を踏まえて行うものとする。 一　事象発生の把握 二　被害の特定及び原因究明（以下「原因究明等」という。） 三　被害の復旧及び再発防止に向けた施策（以下「復旧・再発防止策」という。）の把握 四　復旧・再発防止策の評価	第３条　施策の評価は、次に掲げる段階を踏まえて行うものとする。 一　事象発生の把握 二　被害の特定及び原因究明（以下「原因究明等」という。） 三　被害の復旧及び再発防止に向けた施策（以下「復旧・再発防止策」という。）の把握 四　復旧・再発防止策の評価
２　施策の評価は、法第 32 条の規定により当該行政機関等(当該行政機関等が独立行政法人又は法第 13 条に規定する指定法人（以下「独立行政法人等」という。）の場合は、当該独立行政法人等を所管する行政機関)の長から提供される報告資料を基に行うものとする。	２　施策の評価は、法第 31 条の規定により当該行政機関等（当該行政機関等が独立行政法人又は法第 13 条に規定する指定法人（以下「独立行政法人等」という。）の場合は、当該独立行政法人等を所管する行政機関）の長から提供される報告資料を基に行うものとする。
（特定重大事象に係る通知）	（特定重大事象に係る通知）
第４条　サイバーセキュリティ戦略本部長（以下「本部長」という。）は、特定重大事象に該当する事象の発生を確認したときは、その旨を当該行政機関等の長（当該特定重大事象が独立行政法人等で発生したものであるときは、当該独立行政法人等を所管する行政機関の長及び当該独立行政法人等の長とする。第８条を除き、以下同じ。）に通知するものとする。	第４条　サイバーセキュリティ戦略本部長（以下「本部長」という。）は、特定重大事象に該当する事象の発生を確認したときは、その旨を当該行政機関等の長（当該特定重大事象が独立行政法人等で発生したものであるときは、当該独立行政法人等を所管する行政機関の長及び当該独立行政法人等の長とする。第８条を除き、以下同じ。）に通知するものとする。
（原因究明等）	（原因究明等）
第５条　特定重大事象に係る原因究明等は、当該行政機関等による調査により行われ	第５条　特定重大事象に係る原因究明等は、当該行政機関等による調査により行われ

ることを基本としつつ、必要に応じ、本部による技術的調査その他の補充調査（民間事業者に委託して行うものを含む。）を行うものとする。	ることを基本としつつ、必要に応じ、本部による技術的調査その他の補充調査（民間事業者に委託して行うものを含む。）を行うものとする。
2　本部長は、前項の規定による補充調査を行おうとするときは、その旨を当該行政機関等の長に通知するとともに、必要に応じ、関係物件の提出その他の協力を求めるものとする。	2　本部長は、前項の規定による補充調査を行おうとするときは、その旨を当該行政機関等の長に通知するとともに、必要に応じ、関係物件の提出その他の協力を求めるものとする。
3　本部長は、原因究明等の結果を取りまとめ、本部会合の審議に付した上で、当該行政機関等の長に通知するものとする。	3　本部長は、原因究明等の結果を取りまとめ、本部会合の審議に付した上で、当該行政機関等の長に通知するものとする。
4　本部長は、原因究明等の結果に基づき、法第28条第３項の規定による勧告、当該行政機関等における復旧・再発防止策の立案の促進その他所要の措置を講じるものとする。	4　本部長は、原因究明等の結果に基づき、法第27条第３項の規定による勧告、当該行政機関等における復旧・再発防止策の立案の促進その他所要の措置を講じるものとする。
5　本部長は、原因究明等の事務の一部を法第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その他サイバーセキュリティに関する対策について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人に委託した場合においては、別に定めるところにより、同法人に第１項に定める補充調査を行わせるものとする。	5　本部長は、原因究明等の事務の一部を法第30条第１項の規定に基づき、独立行政法人情報処理推進機構その他サイバーセキュリティに関する対策について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人に委託した場合においては、別に定めるところにより、同法人に第１項に定める補充調査を行わせるものとする。
（指導及び助言）	（指導及び助言）
第６条　本部長は、当該行政機関等の長に対し、特定重大事象に係る原因究明等及び復旧・再発防止策に関し必要な指導及び助言を行うものとする。	第６条　本部長は、当該行政機関等の長に対し、特定重大事象に係る原因究明等及び復旧・再発防止策に関し必要な指導及び助言を行うものとする。
（復旧・再発防止策の評価に係る措置）	（復旧・再発防止策の評価に係る措置）
第７条　本部長は、当該行政機関等が立案した復旧・再発防止策に対する評価が終了したときは、その結果を当該行政機関等の長に通知するとともに、必要に応じ、その他所要の措置を講じるものとする。	第７条　本部長は、当該行政機関等が立案した復旧・再発防止策に対する評価が終了したときは、その結果を当該行政機関等の長に通知するとともに、必要に応じ、その他所要の措置を講じるものとする。

（法第 32 条第２項の運用） 第８条　本部長は、次に掲げる場合には、当該行政機関等（当該行政機関等が独立行政法人等の場合は、当該独立行政法人等を所管する行政機関）の長に対し、法第 32 条第２項の規定により必要な協力を求めるものとする。 一　施策の評価に必要な資料又は情報が正当な理由なく当該行政機関等の長から提供されないとき。 二　第５条第２項の規定により協力を求めた場合において、正当な理由なく協力が得られないとき。 三　本部会合の場において当該行政機関等の関係職員から説明を受けることが施策の評価を行う上で特に必要であると認めるとき。 （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。 一　法第28条第３項の規定による勧告（前項の規定の適用がある場合に限る。） 二　法第 28 条第４項の規定による報告の求め	（法第 31 条第２項の運用） 第８条　本部長は、次に掲げる場合には、当該行政機関等（当該行政機関等が独立行政法人等の場合は、当該独立行政法人等を所管する行政機関）の長に対し、法第 31 条第２項の規定により必要な協力を求めるものとする。 一　施策の評価に必要な資料又は情報が正当な理由なく当該行政機関等の長から提供されないとき。 二　第５条第２項の規定により協力を求めた場合において、正当な理由なく協力が得られないとき。 三　本部会合の場において当該行政機関等の関係職員から説明を受けることが施策の評価を行う上で特に必要であると認めるとき。 （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 31 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 27 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。 一　法第27条第３項の規定による勧告（前項の規定の適用がある場合に限る。） 二　法第 27 条第４項の規定による報告の求め

〇サイバーセキュリティ戦略本部資料提供等規則　新旧対照表

一部改定案	現　行
サイバーセキュリティ戦略本部資料提供等規則 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 一部改定 平成 31 年４月１日 一部改定	サイバーセキュリティ戦略本部資料提供等規則 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 一部改定
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 32 条及び第 33 条の規定に基づき、並びに当該規定による事務を適切に遂行するため、当該事務等について、次のとおり定める。	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 31 条及び第 32 条の規定に基づき、並びに当該規定による事務を適切に遂行するため、当該事務等について、次のとおり定める。
（提供しなければならない資料等） 第１条　法第 32 条第１項の規定に基づき関係行政機関の長がサイバーセキュリティ戦略本部（以下「本部」という。）に対して提供しなければならない資料又は情報は、次に掲げる事項に関するものとする。	（提供しなければならない資料等） 第１条　法第 31 条第１項の規定に基づき関係行政機関の長がサイバーセキュリティ戦略本部（以下「本部」という。）に対して提供しなければならない資料又は情報は、次に掲げる事項に関するものとする。
一～三 （略）	一～三 （略）
２　前項各号に掲げる事項の詳細その他法第 32 条第１項の規定の実施に必要な細目的事項については、内閣サイバーセキュリティセンターが関係行政機関に通知するものとする。	２　前項各号に掲げる事項の詳細その他法第 31 条第１項の規定の実施に必要な細目的事項については、内閣サイバーセキュリティセンターが関係行政機関に通知するものとする。
（特殊法人等の指定） 第２条　法第 33 条第１項の本部が指定する特殊法人及び認可法人は、別表のとおりとする。	（特殊法人等の指定） 第２条　法第 32 条第１項の本部が指定する特殊法人及び認可法人は、別表のとおりとする。
（関係事務の処理等） 第３条　法第 32 条及び第 33 条の規定による事務は、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。	（関係事務の処理等） 第３条　法第 31 条及び第 32 条の規定による事務は、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。

2　法第 32 条又は第 33 条の規定により提供された資料、情報等に基づき法第 28 条第３項の規定による勧告を行う場合において、当該勧告及び同条第４項の規定による報告の求めに関する事務は、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。	2　法第 31 条又は第 32 条の規定により提供された資料、情報等に基づき法第 27 条第３項の規定による勧告を行う場合において、当該勧告及び同条第４項の規定による報告の求めに関する事務は、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。

〇サイバーセキュリティ戦略本部の後援等名義の使用について　新旧対照表

一部改定案	現　行
サイバーセキュリティ戦略本部の後援等名義の使用について 平成 27 年２月 10 日 サイバーセキュリティ戦略本部決定 平成 31 年４月１日 一部改定 サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 23 条の趣旨を踏まえ、国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及等の施策の推進を図るため、サイバーセキュリティ戦略本部は、求めに応じてサイバーセキュリティ戦略本部の後援等名義の使用を承認することとする。 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は、サイバーセキュリティ戦略本部長が定める。 なお、従前、情報セキュリティ政策会議が情報セキュリティ政策会議の後援等名義の使用を承認した行事等については、サイバーセキュリティ戦略本部の後援等名義の使用を承認するものとする。	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基本法（平成 26 年法律第 104 号）第 22 条の趣旨を踏まえ、国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及等の施策の推進を図るため、サイバーセキュリティ戦略本部は、求めに応じてサイバーセキュリティ戦略本部の後援等名義の使用を承認することとする。 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は、サイバーセキュリティ戦略本部長が定める。 なお、従前、情報セキュリティ政策会議が情報セキュリティ政策会議の後援等名義の使用を承認した行事等については、サイバーセキュリティ戦略本部の後援等名義の使用を承認するものとする。

〇政府機関等の情報セキュリティ対策のための統一規範　新旧対照表

一部改定案	現　行
政府機関等の情報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 サイバーセキュリティ戦略本部決定	政府機関等の情報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 サイバーセキュリティ戦略本部決定
第一章　目的及び適用対象（第一条―第二条） 第二章　政府機関等の情報セキュリティ対策のための基本方針（第三条―第四条） 第三章　政府機関等の情報セキュリティ対策のための基本対策（第五条―第二十三条） 附則	第一章　目的及び適用対象（第一条―第二条） 第二章　政府機関等の情報セキュリティ対策のための基本方針（第三条―第四条） 第三章　政府機関等の情報セキュリティ対策のための基本対策（第五条―第二十三条） 附則
第一章　目的及び適用対象 （目的） 第一条　本規範は、サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）第二十六条第一項第二号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準として、機関等がとるべき対策の統一的な枠組みを定め、機関等に自らの責任において対策を図らしめることにより、もって機関等全体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。	第一章　目的及び適用対象 （目的） 第一条　本規範は、サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）第二十五条第一項第二号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準として、機関等がとるべき対策の統一的な枠組みを定め、機関等に自らの責任において対策を図らしめることにより、もって機関等全体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。
（適用対象） 第二条　本規範の適用対象とする組織は、次の各号に掲げるとおりとする。 一　国の行政機関　法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定	（適用対象） 第二条　本規範の適用対象とする組織は、次の各号に掲げるとおりとする。 一　国の行政機関　法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定

する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関 二　独立行政法人　独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人 三　指定法人　法第十三条に規定する指定法人 2　本規範の適用対象とする者は、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。 3　本規範の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報及び情報システムの設計又は運用管理に関する情報とする。 第二章・第三章 （略） 附則 （略）	する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関 二　独立行政法人　独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人 三　指定法人　法第十三条に規定する指定法人 2　本規範の適用対象とする者は、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。 3　本規範の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報及び情報システムの設計又は運用管理に関する情報とする。 第二章・第三章 （略） 附則 （略）

○政府機関等の情報セキュリティ対策の運用等に関する指針　新旧対照表

一部改定案	現　行
政府機関等の情報セキュリティ対策の運用等に関する指針 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 サイバーセキュリティ戦略本部決定	政府機関等の情報セキュリティ対策の運用等に関する指針 平成 28 年８月 31 日 平成 30 年７月 25 日改定 サイバーセキュリティ戦略本部決定
１　本指針の目的 本指針は、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２号に定める国の行政機関、独立行政法人（独立行政法人通則法（平成 11 年法律第 103 号）第２条第１項に規定する法人をいう。以下同じ。）及び指定法人（法第 13 条に規定する指定法人をいう。以下同じ。）（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準の運用に関して、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。）における政府機関等の情報セキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定。以下「統一規範」という。）及び政府機関等の情報セキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定。以下「統一基準」という。）の案の策定、政府機関等の対策基準策定のためのガイドライン（NISC 決定。以下「対策基準策定ガイドライン」という。）の策定、独立行政法人及び指定法人における情報セキュリティ対策の運用並びに複数の機関等で共通的に使用する情報システム（一つの機関等でハードウェアからアプリケーションまで管理・運用している情報システムを除く。以下「基盤となる情報システム」という。）に関する情報セキュリティ対策の運用のために必要な事項を定めるものである。	１　本指針の目的 本指針は、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 25 条第１項第２号に定める国の行政機関、独立行政法人（独立行政法人通則法（平成 11 年法律第 103 号）第２条第１項に規定する法人をいう。以下同じ。）及び指定法人（法第 13 条に規定する指定法人をいう。以下同じ。）（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準の運用に関して、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。）における政府機関等の情報セキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定。以下「統一規範」という。）及び政府機関等の情報セキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定。以下「統一基準」という。）の案の策定、政府機関等の対策基準策定のためのガイドライン（NISC 決定。以下「対策基準策定ガイドライン」という。）の策定、独立行政法人及び指定法人における情報セキュリティ対策の運用並びに複数の機関等で共通的に使用する情報システム（一つの機関等でハードウェアからアプリケーションまで管理・運用している情報システムを除く。以下「基盤となる情報システム」という。）に関する情報セキュリティ対策の運用のために必要な事項を定めるものである。

２～４ （略）	２～４ （略）
附則 （略）	附則 （略）

○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　新旧対照表

一部改定案	現　行
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	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
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２号の規定に基づきサイバーセキュリティ戦略本部（以下「戦略本部」という。）がつかさどる事務のうち、監査について、その実施のための基本方針を以下のとおり定める。	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 25 条第１項第２号の規定に基づきサイバーセキュリティ戦略本部（以下「戦略本部」という。）がつかさどる事務のうち、監査について、その実施のための基本方針を以下のとおり定める。
１　監査の目的 本監査は、戦略本部が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、国の行政機関、独立行政法人及び指定法人のサイバーセキュリティ対策に関する現状を適切に把握した上で、これらの組織において対策強化のための自律的かつ継続的な改善機構であるＰＤＣＡサイクルの構築、及び必要なサイバーセキュリティ対策の実施を支援するとともに、当該ＰＤＣＡサイクルが継続的かつ有効に機能するよう助言することによって、これらの組織におけるサイバーセキュリティ対策の効果的な強化を図ることを目的とする。	１　監査の目的 本監査は、戦略本部が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、国の行政機関、独立行政法人及び指定法人のサイバーセキュリティ対策に関する現状を適切に把握した上で、これらの組織において対策強化のための自律的かつ継続的な改善機構であるＰＤＣＡサイクルの構築、及び必要なサイバーセキュリティ対策の実施を支援するとともに、当該ＰＤＣＡサイクルが継続的かつ有効に機能するよう助言することによって、これらの組織におけるサイバーセキュリティ対策の効果的な強化を図ることを目的とする。
２～４ （略）	２～４ （略）
５　監査の進め方 (1) 監査方針の策定 本基本方針を踏まえ、年度ごとの監査の基	５　監査の進め方 (1) 監査方針の策定 本基本方針を踏まえ、年度ごとの監査の基

本的な考え方、前述の監査テーマを含む年度監査方針を、サイバーセキュリティ戦略を実施するために戦略本部が決定する年次計画の一部として策定する。	本的な考え方、前述の監査テーマを含む年度監査方針を、サイバーセキュリティ戦略を実施するために戦略本部が決定する年次計画の一部として策定する。
(2) 監査の実施	(2) 監査の実施
(1)の年度ごとに策定する監査方針に基づいて、監査を実施する。監査の実施に当たっては、必要に応じて外部の専門家の協力を得る。	(1)の年度ごとに策定する監査方針に基づいて、監査を実施する。監査の実施に当たっては、必要に応じて外部の専門家の協力を得る。
また、過年度の監査実施結果のうち重要な事項については、その改善状況を継続的にフォローアップする。	また、過年度の監査実施結果のうち重要な事項については、その改善状況を継続的にフォローアップする。
(3) 個別の監査実施結果の通知	(3) 個別の監査実施結果の通知
個別の監査実施結果については、改善のために必要な助言等を含めて、各機関の最高情報セキュリティ責任者（ＣＩＳＯ）へ通知する。	個別の監査実施結果については、改善のために必要な助言等を含めて、各機関の最高情報セキュリティ責任者（ＣＩＳＯ）へ通知する。
なお、重要な事項については、改善策の提案を含めて通知する。また、独立行政法人及び指定法人における監査実施結果については、所管府省庁を通じて通知する。	なお、重要な事項については、改善策の提案を含めて通知する。また、独立行政法人及び指定法人における監査実施結果については、所管府省庁を通じて通知する。
通知を受けた各機関は、速やかに必要な改善を実施又は改善計画を策定し、改善結果又は改善計画を戦略本部に報告するものとする。なお、独立行政法人及び指定法人は所管府省庁を通じて報告を行うものとする。	通知を受けた各機関は、速やかに必要な改善を実施又は改善計画を策定し、改善結果又は改善計画を戦略本部に報告するものとする。なお、独立行政法人及び指定法人は所管府省庁を通じて報告を行うものとする。
(4) 監査実施結果の取りまとめ・報告	(4) 監査実施結果の取りまとめ・報告
サイバーセキュリティの特性を踏まえ、攻撃者を利することにならないよう配慮した形で、当該年度に実施した監査の結果を取りまとめる。戦略本部は、当該結果について、報告を受ける。	サイバーセキュリティの特性を踏まえ、攻撃者を利することにならないよう配慮した形で、当該年度に実施した監査の結果を取りまとめる。戦略本部は、当該結果について、報告を受ける。
(5) 監査事務の処理	(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	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30条第１項の規定に

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。	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。

○重要インフラ専門調査会の設置について　新旧対照表

一部改定案	現　行
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 平成 31 年４月１日 一部改定	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
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２条の規定に基づき、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、重要インフラ専門調査会（以下「専門調査会」という。）を置く。	１．サイバーセキュリティ戦略本部令（平成 26 年政令第 400 号）第２条の規定に基づき、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、重要インフラ専門調査会（以下「専門調査会」という。）を置く。
２～９ （略）	２～９ （略）

〇研究開発戦略専門調査会の設置について　新旧対照表

一部改定案	現　行
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 平成 31 年４月１日 一部改定 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２条の規定に基づき、サイバーセキュリティに係る研究開発及び技術開発並びにそれらの成果利用の戦略に係る事項について、調査検討を行うため、研究開発戦略専門調査会（以下「専門調査会」という。）を置く。 ２～９ （略）	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 １．サイバーセキュリティ戦略本部令（平成 26 年政令第 400 号）第２条の規定に基づき、サイバーセキュリティに係る研究開発及び技術開発並びにそれらの成果利用の戦略に係る事項について、調査検討を行うため、研究開発戦略専門調査会（以下「専門調査会」という。）を置く。 ２～９ （略）

〇普及啓発・人材育成専門調査会の設置について　新旧対照表

一部改定案	現　行
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 平成 31 年４月１日 一部改定 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２条の規定に基づき、サイバーセキュリティに関する普及啓発及び人材育成に係る事項について、調査検討を行うため、普及啓発・人材育成専門調査会（以下「専門調査会」という。）を置く。 ２～９ （略）	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 １．サイバーセキュリティ戦略本部令（平成 26 年政令第 400 号）第２条の規定に基づき、サイバーセキュリティに関する普及啓発及び人材育成に係る事項について、調査検討を行うため、普及啓発・人材育成専門調査会（以下「専門調査会」という。）を置く。 ２～９ （略）

「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新旧対照表

○ 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）　（下線部分は改正部分）

改　正　案	現　行
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　（略）	１　サイバーセキュリティ戦略本部令（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　（略）

「サイバーセキュリティ戦略本部の本部員の指定について」の一部改正について新旧対照表

〇サイバーセキュリティ戦略本部の本部員の指定について　（下線部分は改正部分）

一部改定案	現　行
サイバーセキュリティ戦略本部の本部員の指定について （平成 27 年 7 月 22 日 内閣総理大臣決定） 平成 27 年 10 月 23 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）第 30 条第２項第６号のサイバーセキュリティ戦略本部員として、情報通信技術（IT）政策担当大臣及び東京オリンピック競技大会・東京パラリンピック競技大会担当大臣を指定する。	サイバーセキュリティ戦略本部の本部員の指定について （平成 27 年 7 月 22 日 内閣総理大臣決定） 平成 27 年 10 月 23 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）第 29 条第２項第６号のサイバーセキュリティ戦略本部員として、情報通信技術（IT）政策担当大臣及び東京オリンピック競技大会・東京パラリンピック競技大会担当大臣を指定する。

サイバーセキュリティ戦略本部重大事象施策評価規則

（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
一部改定
平成31年４月１日
一部改定

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　行政機関等が運用する情報システムにおける障害を伴う事象であって、当該行政機関等が実施する事務の遂行に著しい支障を及ぼし、又は及ぼすおそれがあるもの

二　情報の漏えいを伴う事象であって、国民生活又は社会経済に重大な影響を与え、又は与えるおそれがあるもの

三　前各号に掲げるもののほか、我が国のサイバーセキュリティに対する国内外の信用を著しく失墜させ、又は失墜させるおそれがある事象

（関係行政機関との連携等）

第２条　サイバーセキュリティ戦略本部（以下「本部」という。）による特定重大事象に対する施策の評価（以下単に「施策の評価」という。）に当たっては、特定重大事象が発生した行政機関等（以下「当該行政機関等」という。）その他の関係行政機関との緊密な連携を図るとともに、秘密の保持に十分留意するものとする。

（施策の評価の手順等）

第３条　施策の評価は、次に掲げる段階を踏まえて行うものとする。

一　事象発生の把握

二　被害の特定及び原因究明（以下「原因究明等」という。）

三　被害の復旧及び再発防止に向けた施策（以下「復旧・再発防止策」という。）の把握

四　復旧・再発防止策の評価

２　施策の評価は、法第32条の規定により当該行政機関等（当該行政機関等が独立行政法人又は法第13条に規定する指定法人（以下「独立行政法人等」という。）の場合は、当該独立行政法人等を所管する行政機関）の長から提供される報告資料を基に行うものとする。

（特定重大事象に係る通知）

第４条　サイバーセキュリティ戦略本部長（以下「本部長」という。）は、特定重大事象に該当する事象の発生を確認したときは、その旨を当該行政機関等の長（当該特定重大事象が独立行政法人等で発生したものであるときは、当該独立行政法人等を所管する行政機関の長及び当該独立行政法人等の長とする。第８条を除き、以下同じ。）に通知するものとする。

（原因究明等）

第５条　特定重大事象に係る原因究明等は、当該行政機関等による調査により行われることを基本としつつ、必要に応じ、本部による技術的調査その他の補充調査（民間事業者に委託して行うものを含む。）を行うものとする。

２　本部長は、前項の規定による補充調査を行おうとするときは、その旨を当該行政機関等の長に通知するとともに、必要に応じ、関係物件の提出その他の協力を求めるものとする。

３　本部長は、原因究明等の結果を取りまとめ、本部会合の審議に付した上で、当該行政機関等の長に通知するものとする。

４　本部長は、原因究明等の結果に基づき、法第28条第３項の規定による勧告、当該行政機関等における復旧・再発防止策の立案の促進その他所要の措置を講じるものとする。

５　本部長は、原因究明等の事務の一部を法第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その他サイバーセキュリティに関する対策について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人に委託した場合においては、別に定めるところにより、同法人に第１項に定める補充調査を行わせるものとする。

（指導及び助言）

第６条　本部長は、当該行政機関等の長に対し、特定重大事象に係る原因究明等及び復旧・再発防止策に関し必要な指導及び助言を行うものとする。

（復旧・再発防止策の評価に係る措置）

第７条　本部長は、当該行政機関等が立案した復旧・再発防止策に対する評価が終了したときは、その結果を当該行政機関等の長に通知するとともに、必要に応じ、その他所要の措置を講じるものとする。

（法第32条第２項の運用）

第８条　本部長は、次に掲げる場合には、当該行政機関等（当該行政機関等が独立行政法人等の場合は、当該独立行政法人等を所管する行政機関）の長に対し、法第32条第２項の規定により必要な協力を求めるものとする。

一　施策の評価に必要な資料又は情報が正当な理由なく当該行政機関等の長から提供されないとき。

二　第５条第２項の規定により協力を求めた場合において、正当な理由なく協力が得られないとき。

三　本部会合の場において当該行政機関等の関係職員から説明を受けることが施策の評価を行う上で特に必要であると認めるとき。

（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。

一　法第28条第３項の規定による勧告（前項の規定の適用がある場合に限る。）

二　法第28条第４項の規定による報告の求め

サイバーセキュリティ戦略本部資料提供等規則

（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
一部改定
平成３１年４月１日
一部改定

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32条及び第33条の規定に基づき、並びに当該規定による事務を適切に遂行するため、当該事務等について、次のとおり定める。

（提供しなければならない資料等）

第１条　法第32条第１項の規定に基づき関係行政機関の長がサイバーセキュリティ戦略本部（以下「本部」という。）に対して提供しなければならない資料又は情報は、次に掲げる事項に関するものとする。

一　当該行政機関又は当該行政機関が所管する独立行政法人若しくは法第13条に規定する指定法人において発生したサイバーセキュリティに関する事象に関する事項のうち、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）第１条に規定する特定重大事象に該当する事象に関する重要なものその他我が国のサイバーセキュリティの向上に資するもの

二　当該行政機関が所管する法第12条第2項第3号に規定する重要社会基盤事業者等において発生したサイバーセキュリティに関する事象に関する事項のうち、重要社会基盤事業者等のサービスの安定的かつ適切な提供に著しい支障を及ぼし、又は及ぼすおそれがある事象に関する重要なものその他我が国のサイバーセキュリティの向上に資するもの

三　二に掲げるもののほか、サイバーセキュリティに関する事項であって、本部の所掌事務の遂行に資すると当該行政機関の長が認めるもの

２　前項各号に掲げる事項の詳細その他法第32条第１項の規定の実施に必要な細目的事項については、内閣サイバーセキュリティセンターが関係行政機関に通知するものとする。

（特殊法人等の指定）

第２条　法第33条第１項の本部が指定する特殊法人及び認可法人は、別表のとおりとする。

（関係事務の処理等）

第３条　法第32条及び第33条の規定による事務は、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。

２　法第32条又は第33条の規定により提供された資料、情報等に基づき法第28条第３項の規定による勧告を行う場合において、当該勧告及び同条第４項の規定による報告の求めに関する事務は、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。

別表

沖縄振興開発金融公庫
沖縄科学技術大学院大学学園
株式会社地域経済活性化支援機構
原子力損害賠償・廃炉等支援機構
銀行等保有株式取得機構
預金保険機構
株式会社東日本大震災事業者再生支援機構
地方公共団体情報システム機構
地方公務員共済組合連合会
地方職員共済組合
都職員共済組合
全国市町村職員共済組合連合会
日本放送協会
日本電信電話株式会社
東日本電信電話株式会社
西日本電信電話株式会社
日本郵政株式会社
日本郵便株式会社
日本たばこ産業株式会社
株式会社日本政策金融公庫
株式会社日本政策投資銀行
輸出入・港湾関連情報処理センター株式会社
株式会社国際協力銀行
日本銀行
国家公務員共済組合連合会
公立学校共済組合
日本私立学校振興・共済事業団
放送大学学園
日本年金機構
日本赤十字社
健康保険組合連合会
全国健康保険協会
国民年金基金連合会
日本中央競馬会
農水産業協同組合貯金保険機構
株式会社商工組合中央金庫

日本アルコール産業株式会社
株式会社産業革新機構
株式会社海外需要開拓支援機構
北海道旅客鉄道株式会社
四国旅客鉄道株式会社
日本貨物鉄道株式会社
東京地下鉄株式会社
成田国際空港株式会社
東日本高速道路株式会社
中日本高速道路株式会社
西日本高速道路株式会社
首都高速道路株式会社
阪神高速道路株式会社
本州四国連絡高速道路株式会社
新関西国際空港株式会社
中間貯蔵・環境安全事業株式会社

サイバーセキュリティ戦略本部の後援等名義の使用について

（平成２７年２月１０日
サイバーセキュリティ戦略本部決定）
平成３１年４月１日
一部改訂

サイバーセキュリティ基本法（平成26年法律第104号）第23条の趣旨を踏まえ、国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及等の施策の推進を図るため、サイバーセキュリティ戦略本部は、求めに応じてサイバーセキュリティ戦略本部の後援等名義の使用を承認することとする。

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は、サイバーセキュリティ戦略本部長が定める。

なお、従前、情報セキュリティ政策会議が情報セキュリティ政策会議の後援等名義の使用を承認した行事等については、サイバーセキュリティ戦略本部の後援等名義の使用を承認するものとする。

政府機関等の情報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
サイバーセキュリティ戦略本部決定

第一章　目的及び適用対象

（目的）

第一条　本規範は、サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）第二十六条第一項第二号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準として、機関等がとるべき対策の統一的な枠組みを定め、機関等に自らの責任において対策を図らしめることにより、もって機関等全体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。

（適用対象）

第二条　本規範の適用対象とする組織は、次の各号に掲げるとおりとする。

一　国の行政機関　法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関

二　独立行政法人　独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人

三　指定法人　法第十三条に規定する指定法人

２　本規範の適用対象とする者は、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱

う者（以下「職員等」という。）とする。
３　本規範の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報及び情報システムの設計又は運用管理に関する情報とする。

第二章　政府機関等の情報セキュリティ対策のための基本方針

（リスク評価と対策）
第三条　機関等は、自組織の目的等を踏まえ、第十条に定める自己点検の結果、第十一条に定める監査の結果、法に基づきサイバーセキュリティ戦略本部が実施する監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講じなければならない。
２　機関等は、前項の評価に変化が生じた場合には、情報セキュリティ対策を見直さなければならない。

（情報セキュリティ文書）
第四条　機関等は、自組織の特性を踏まえ、基本方針（機関等における情報セキュリティ対策の基本的な方針をいう。以下同じ。）及び対策基準（機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。以下同じ。）を定めなければならない。基本方針及び対策基準（以下「ポリシー」という。）の呼称は機関等で独自に定めることができる。
２　基本方針は、情報セキュリティを確保するため、情報セキュリティ対策の目的、対象範囲等の情報セキュリティに対する基本的な考え方を定めなければならない。
３　対策基準は、別に定める政府機関等の情報セキュリティ対策のための統一基準（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるように定めなければならない。
４　国の行政機関は、必要に応じて、所管する独立行政法人及び指定法人に対して、自らのポリシーを当該法人がポリシーを定める際に参照するよう求めることとする。
５　独立行政法人及び指定法人は、前項の求めに応じることとする。
６　機関等は、前条第一項の評価結果を踏まえ、ポリシーの評価及び見直しを行わなければならない。

第三章　政府機関等の情報セキュリティ対策のための基本対策

（管理体制）

第五条　機関等は、情報セキュリティ対策を実施するための組織・体制を整備しなければならない。

２　機関等は、最高情報セキュリティ責任者１人を置かなければならない。

３　最高情報セキュリティ責任者は、対策基準等の審議を行う機能を持つ組織として情報セキュリティ委員会を設置し、委員長及び委員を置かなければならない。

４　最高情報セキュリティ責任者は、本規範にて規定した機関等における情報セキュリティ対策に関する事務を統括するとともに、その責任を負う。

５　最高情報セキュリティ責任者は、統一基準に定められた自らの担務を、統一基準に定める責任者に担わせることができる。

（対策推進計画）

第六条　最高情報セキュリティ責任者は、第三条第一項の評価の結果を踏まえた情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めなければならない。

２　機関等は、対策推進計画に基づき情報セキュリティ対策を実施しなければならない。

３　最高情報セキュリティ責任者は、前項の実施状況を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行わなければならない。

（例外措置）

第七条　機関等は、ポリシーに定めた情報セキュリティ対策の実施に当たり、例外措置を適用するために必要な申請・審査・承認のための手順と担当者を定めなければならない。

（教育）

第八条　機関等は、職員等が自覚をもってポリシーに定められた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行わなければならない。

（情報セキュリティインシデントへの対応）

第九条　機関等は、情報セキュリティインシデント（JIS Q 27000:2014 における情報セキュリティインシデントをいう。以下同じ。）に対処するため、適正な体制を構築するとともに、必要な措置を定め、実施しなければならない。

２　情報セキュリティインシデントの可能性を認知した者は、ポリシーに定める報告窓口に報告しなければならない。
３　ポリシーに定める責任者は、情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じなければならない。

（自己点検）
第十条　機関等は、情報セキュリティ対策の自己点検を行わなければならない。

（監査）
第十一条　機関等は、対策基準が本規範及び統一基準に準拠し、かつ実際の運用が対策基準に準拠していることを確認するため、情報セキュリティ監査を行わなければならない。

（情報の格付）
第十二条　機関等は、取り扱う情報に、機密性、完全性及び可用性の観点に区別して、分類した格付を付さなければならない。
２　機関等は、機関等間での情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、いかなる区分に相当するかを明示等しなければならない。

（情報の取扱制限）
第十三条　機関等は、情報の格付に応じた取扱制限を定めなければならない。
２　機関等は、取り扱う情報に、前項で定めた取扱制限を付さなければならない。
３　機関等は、機関等間での情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等しなければならない。

（情報のライフサイクル管理）
第十四条　機関等は、情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要とされる取扱いが損なわれることがないように、必要な措置を定め、実施しなければならない。

（情報を取り扱う区域）
第十五条　機関等は、自組織が管理する又は自組織以外の組織から借用している施設等、自組織の管理下にあり、施設及び環境に係る対策が必要な区域の範囲を定め、その特性に応じて対策を決定し、実施しなければならない。

（外部委託）
第十六条　機関等は、情報処理に係る業務を外部委託する場合には、必要な措置を定

め、実施しなければならない。
２　機関等は、外部委託（約款による外部サービスの利用を除く。）を実施する場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めなければならない。
３　機関等は、要機密情報を約款による外部サービスを利用して取り扱ってはならない。
４　機関等は、機器等の調達に当たり、既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処を含む選定基準を整備しなければならない。

（情報システムに係る文書及び台帳整備）
第十七条　機関等は、所管する情報システムに係る文書及び台帳を整備しなければならない。

（情報システムのライフサイクル全般にわたる情報セキュリティの確保）
第十八条　機関等は、所管する情報システムの企画、調達・構築、運用・保守、更改・廃棄及び見直しの各段階において、情報セキュリティを確保するための措置を定め、実施しなければならない。

（情報システムの運用継続計画）
第十九条　機関等は、所管する情報システムに係る運用継続のための計画（以下「情報システムの運用継続計画」という。）を整備する際には、非常時における情報セキュリティ対策についても、勘案しなければならない。
２　機関等は、情報システムの運用継続計画の訓練等に当たっては、非常時における情報セキュリティに係る対策事項の運用が可能かどうか、確認しなければならない。

（暗号・電子署名）
第二十条　機関等は、自組織における暗号及び電子署名の利用について、必要な措置を定め、実施しなければならない。

（インターネット等を用いた行政サービスの提供）
第二十一条　機関等は、インターネット等を用いて行政サービスを提供する際には、利用者端末の情報セキュリティ水準の低下を招く行為を防止するために、必要な措置を定め、実施しなければならない。

（情報システムの利用）

第二十二条　機関等は、情報システムの利用に際して、情報セキュリティを確保するために職員等が行わなければならない必要な措置を定め、実施させなければならない。

（統一基準への委任）

第二十三条　本規範に定めるもののほか、本規範の実施のため必要な要件は、統一基準で定める。

附則

政府機関の情報セキュリティ対策のための統一規範（平成 23 年４月 21 日情報セキュリティ政策会議決定）は廃止する。

政府機関等の情報セキュリティ対策の運用等に関する指針

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
サイバーセキュリティ戦略本部決定

１　本指針の目的

本指針は、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２号に定める国の行政機関、独立行政法人（独立行政法人通則法（平成 11 年法律第 103 号）第２条第１項に規定する法人をいう。以下同じ。）及び指定法人（法第 13 条に規定する指定法人をいう。以下同じ。）（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準の運用に関して、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。）における政府機関等の情報セキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定。以下「統一規範」という。）及び政府機関等の情報セキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定。以下「統一基準」という。）の案の策定、政府機関等の対策基準策定のためのガイドライン（NISC 決定。以下「対策基準策定ガイドライン」という。）の策定、独立行政法人及び指定法人における情報セキュリティ対策の運用並びに複数の機関等で共通的に使用する情報システム（一つの機関等でハードウェアからアプリケーションまで管理・運用している情報システムを除く。以下「基盤となる情報システム」という。）に関する情報セキュリティ対策の運用のために必要な事項を定めるものである。

２　統一基準群の策定

統一基準群は、統一規範、統一基準、本指針及び対策基準策定ガイドラインの総称をいい、統一規範、統一基準及び本指針の原案は、NISC 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。また、対策基準策定ガイドラインは、国の行政機関と協議の上、NISC において決定する。

なお、NISC は、新たな脅威の発生や機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。

(1)　統一規範及び統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策を包含するものとし、責任体制、実施体制及び対策内容について、機関等が準拠できるよう、実状を踏まえるとともに、国際的な基準等との整合性に配慮の上、策定する。統一基準には、情報セキュリティ対

策の項目ごとに機関等が遵守すべき事項（以下「遵守事項」という。）を規定する。

(2) 対策基準策定ガイドラインは、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。）を例示するとともに、機関等による対策基準の策定及び実施に際しての考え方等を解説することを目的として策定する。基本対策事項は遵守事項に対応するものであるため、機関等は対策基準策定ガイドラインを参照し、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ものである。

3 独立行政法人及び指定法人の情報セキュリティ対策に係る主務大臣等の責務

(1) 導入・計画

独立行政法人を所管する主務大臣は、独立行政法人通則法（平成 11 年法律第 103 号）第 29 条第 1 項の規定により指示した同項の中期目標、第 35 条の 4 第 1 項の規定により指示した同項の中長期目標又は第 35 条の 9 第 1 項の規定により指示した同項の年度目標に、統一基準群に基づいて定めたポリシーに従って情報セキュリティ対策を講ずる旨を盛り込むこととする。指定法人に対しては、個別の根拠法に基づき、当該指定法人を所管する国の行政機関が必要な情報セキュリティ対策についての指導等を実施する。

(2) 評価

独立行政法人を所管する主務大臣は、独立行政法人通則法に基づく業務の実績等に関する評価の際に、情報セキュリティ対策の実施状況に関しても評価を行い、評価結果を公表する。指定法人を所管する国の行政機関は、当該指定法人に対して、個別の根拠法に基づき、情報セキュリティ対策の実施状況に関して評価を行う。

独立行政法人及び指定法人の情報セキュリティ対策に係る評価の結果に関しては、NISC においても確認し、必要に応じてこれら法人を所管する国の行政機関に対して助言等を行う。

4 共通的に使用する情報システムにおける情報セキュリティ対策

基盤となる情報システムについては、これを使用する各機関等の情報システムと連携して運用管理を行うものであることから、各機関等の間での情報セキュリティ対策の遺漏防止を図る必要がある。また、基盤となる情報システムと連携する一部の情報システムにおける情報セキュリティインシデントが他の情報システムに影響を及ぼす可能性等も踏まえ、情報セキュリティマネジメントを適切に実行し、情報システム全体としての情報セキュリティ水準を適切に確保しなければならない。

このため、基盤となる情報システムの整備・運用管理を行う機関等及び基盤となる情報システムと連携する情報システムを管理する機関等（以下「整備・運用管理機関等」という。）は、基盤となる情報システムの運用管理を行う体制を整備する

に当たっては、各機関等の責任と役割分担を明確化するとともに、情報セキュリティ対策を確実かつ迅速に調整・実施できる体制にする必要がある。

また、整備・運用管理機関等は、基盤となる情報システムの情報セキュリティを確保するための方策等について包括的に定めた文書を整備するに当たっては、それぞれのポリシーとの関係について検討し、適切な運用管理が行われるよう、以下の事項等を整理するものとする。

・各機関等の間の責任分界
・平常時及び非常時の協力・連携体制
・非常時の具体的対応策　等

以上の検討・実施に当たっては、各機関等の間での十分な合意形成を図るとともに、情報セキュリティ対策の円滑かつ迅速な実施に支障を来さないように留意する必要がある。

なお、基盤となる情報システムの情報セキュリティ対策を共通的に行うため、基盤となる情報システムを整備し、運用管理を行う機関等は、当該基盤となる情報システムと連携する情報システムを管理する機関等と協議の上、基盤となる情報システムの情報セキュリティについて、各機関等が定めるそれぞれのポリシーの定めにかかわらず、共通的な規程を定めることができるものとする。

附則　政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針（平成 17 年 9 月 15 日情報セキュリティ政策会議決定）は廃止する。

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

（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

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2号の規定に基づきサイバーセキュリティ戦略本部（以下「戦略本部」という。）がつかさどる事務のうち、監査について、その実施のための基本方針を以下のとおり定める。

1　監査の目的

本監査は、戦略本部が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、国の行政機関、独立行政法人及び指定法人のサイバーセキュリティ対策に関する現状を適切に把握した上で、これらの組織において対策強化のための自律的かつ継続的な改善機構であるＰＤＣＡサイクルの構築、及び必要なサイバーセキュリティ対策の実施を支援するとともに、当該ＰＤＣＡサイクルが継続的かつ有効に機能するよう助言することによって、これらの組織におけるサイバーセキュリティ対策の効果的な強化を図ることを目的とする。

2　監査の対象

国の行政機関、独立行政法人及び指定法人（以下「行政機関等」という。）を監査の対象とする。

なお、本基本方針において「国の行政機関」とは、法律の規定に基づき内閣に置かれる機関、内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成11年法律第89号）第49条第1項及び第2項に規定する機関、国家行政組織法（昭和23年法律第120号）第3条第2項に規定する機関並びにこれらに置かれる機関をいう。また、本基本方針において「指定法人」とは、法第13条に規定する指定法人をいう。

3　監査の基本的な方向性

(1) 助言型監査

サイバーセキュリティ対策は、技術や環境の変化に応じて、段階的に実

施内容の向上を図ることが重要であるため、監査をそのためのモニタリング機能として位置づけることが有効である。このことを踏まえて、本監査は、被監査主体である行政機関等がサイバーセキュリティ対策を強化する上で有益な助言を行うことを目的とする「助言型監査」を志向する。

また、行政機関等のサイバーセキュリティ対策を全体的に強化するため、それぞれの行政機関等（以下「各機関」という。）が実施している優れた取組（グッドプラクティス）については、他の各機関におけるサイバーセキュリティ対策の強化に資するよう、それらの取組を適切に共有するとともに、サイバーセキュリティ対策を強化する観点からの監査の必要性、有効性について、各機関がより深い理解を得られるよう、丁寧な説明を行う。

(2) 第三者的視点からの監査

監査の客観性、専門性等を確保することを目的として、各機関で実施している内部監査とは独立した、第三者的視点から監査を実施する。

(3) 各機関の状況を踏まえた監査

各機関のサイバーセキュリティ対策の実施状況、体制の整備状況等を踏まえ、各機関におけるサイバーセキュリティ対策に係る課題等について対話し、相互認識と信頼関係を深めるよう努めるとともに、各機関における監査の実施方法を双方協議の上、決定する。

また、各機関におけるサイバーセキュリティ対策の推進体制の発展段階に応じて、監査の内容も段階的に発展させていくよう配慮する。

(4) サイバーセキュリティに関する情勢を踏まえた監査テーマの選定

我が国を取り巻くサイバーセキュリティに関する情勢を踏まえて、行政機関等のサイバーセキュリティ対策において、より重要性・緊急性・リスクの高いものから監査テーマを適切に選定する。

4　監査の実施内容

(1) マネジメント監査

「政府機関等の情報セキュリティ対策のための統一基準群」等に基づく施策の取組状況について、国際規格において基本的な考え方である組織全体としてのＰＤＣＡサイクルが有効に機能しているかとの観点から、関係者への質問、資料の閲覧、情報システムの点検等により検証し、改善のために必要な助言等を行う。

また、サイバーセキュリティ対策を強化するための体制等の整備状況についても検証し、改善のために必要な助言等を行う。

なお、上記の検証の一環として、各機関がサイバーセキュリティに係るポリシー等において定めたサイバーセキュリティ対策を適切に実施しているか検証する。

(2) ペネトレーションテスト

インターネットに接続されている情報システムについて、疑似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点から、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。

なお、インターネットとの境界を突破できた場合を仮定して、内部ネットワークについても、サイバーセキュリティ対策上の問題を検証し、改善のために必要な助言等を行う。

5　監査の進め方

(1) 監査方針の策定

本基本方針を踏まえ、年度ごとの監査の基本的な考え方、前述の監査テーマを含む年度監査方針を、サイバーセキュリティ戦略を実施するために戦略本部が決定する年次計画の一部として策定する。

(2) 監査の実施

(1)の年度ごとに策定する監査方針に基づいて、監査を実施する。監査の実施に当たっては、必要に応じて外部の専門家の協力を得る。

また、過年度の監査実施結果のうち重要な事項については、その改善状況を継続的にフォローアップする。

(3) 個別の監査実施結果の通知

個別の監査実施結果については、改善のために必要な助言等を含めて、各機関の最高情報セキュリティ責任者（ＣＩＳＯ）へ通知する。

なお、重要な事項については、改善策の提案を含めて通知する。また、独立行政法人及び指定法人における監査実施結果については、所管府省庁を通じて通知する。

通知を受けた各機関は、速やかに必要な改善を実施又は改善計画を策定し、改善結果又は改善計画を戦略本部に報告するものとする。なお、独立行政法人及び指定法人は所管府省庁を通じて報告を行うものとする。

(4) 監査実施結果の取りまとめ・報告

サイバーセキュリティの特性を踏まえ、攻撃者を利することにならないよう配慮した形で、当該年度に実施した監査の結果を取りまとめる。戦略本部は、当該結果について、報告を受ける。

(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。

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）
平成３１年４月１日
一部改定

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２条の規定に基づき、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、重要インフラ専門調査会（以下「専門調査会」という。）を置く。

２．専門調査会の委員は、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について優れた見識を有する者のうちから、内閣総理大臣が任命する者（当該委員がサイバーセキュリティ戦略本部員の場合にあっては、サイバーセキュリティ戦略本部長が指名する者）とする。

３．専門調査会の会長は、その委員の互選により決する。

４．専門調査会の会長は、必要があると認めるときは、当該専門調査会の委員以外の者に対し、当該専門調査会の会議に出席して意見を述べることを求めることができる。

５．専門調査会の会長は、必要があると認めるときは、専門調査会の下にワーキンググループを置くことができる。

６．専門調査会の委員の任期は、任命又は指名の日から２年以内とする。ただし、再任又は再指名を妨げない。

７．専門調査会の庶務は、関係省庁の協力を得て、内閣官房において処理する。

８．前各項に掲げるもののほか、専門調査会の運営に関する事項その他必要な事項は会長が定める。

９．「重要インフラ専門委員会」（平成17年９月15日情報セキュリティ政策会議決定）が決定した事項及び検討した事項等については、専門調査会に引き継がれるものとする。

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）
平成３１年４月１日
一部改定

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２条の規定に基づき、サイバーセキュリティに係る研究開発及び技術開発並びにそれらの成果利用の戦略に係る事項について、調査検討を行うため、研究開発戦略専門調査会（以下「専門調査会」という。）を置く。

２．専門調査会の委員は、サイバーセキュリティに係る研究開発及び技術開発並びにそれらの成果利用の戦略に係る事項について優れた見識を有する者のうちから、内閣総理大臣が任命する者（当該委員がサイバーセキュリティ戦略本部員の場合にあっては、サイバーセキュリティ戦略本部長が指名する者）とする。

３．専門調査会の会長は、その委員の互選により決する。

４．専門調査会の会長は、必要があると認めるときは、当該専門調査会の委員以外の者に対し、当該専門調査会の会議に出席して意見を述べることを求めることができる。

５．専門調査会の会長は、必要があると認めるときは、専門調査会の下にワーキンググループを置くことができる。

６．専門調査会の委員の任期は、任命又は指名の日から２年以内とする。ただし、再任又は再指名を妨げない。

７．専門調査会の庶務は、関係省庁の協力を得て、内閣官房において処理する。

８．前各項に掲げるもののほか、専門調査会の運営に関する事項その他必要な事項は会長が定める。

９．「技術戦略専門委員会」（平成17年７月14日情報セキュリティ政策会議決定）が決定した事項及び検討した事項等については、専門調査会に引き継がれるものとする。

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）
平成３１年４月１日
一部改定

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２条の規定に基づき、サイバーセキュリティに関する普及啓発及び人材育成に係る事項について、調査検討を行うため、普及啓発・人材育成専門調査会（以下「専門調査会」という。）を置く。

２．専門調査会の委員は、サイバーセキュリティに関する普及啓発及び人材育成に係る事項について優れた見識を有する者のうちから、内閣総理大臣が任命する者（当該委員がサイバーセキュリティ戦略本部員の場合にあっては、サイバーセキュリティ戦略本部長が指名する者）とする。

３．専門調査会の会長は、その委員の互選により決する。

４．専門調査会の会長は、必要があると認めるときは、当該専門調査会の委員以外の者に対し、当該専門調査会の会議に出席して意見を述べることを求めることができる。

５．専門調査会の会長は、必要があると認めるときは、専門調査会の下にワーキンググループを置くことができる。

６．専門調査会の委員の任期は、任命又は指名の日から２年以内とする。ただし、再任又は再指名を妨げない。

７．専門調査会の庶務は、関係省庁の協力を得て、内閣官房において処理する。

８．前各項に掲げるもののほか、専門調査会の運営に関する事項その他必要な事項は会長が定める。

９．「普及啓発・人材育成専門委員会」（平成23年７月８日情報セキュリティ政策会議決定）が決定した事項及び検討した事項等については、専門調査会に引き継がれるものとする。

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）
改　正　　平　成　２８年　４　月　１　日
改　正　　平　成　２８年　８　月　３１日
改　正　　平　成　３１年　４　月　１　日

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　推進会議は、議長、副議長、構成員及びオブザーバーをもって構成する。議長は内閣官房副長官（事務）、副議長は内閣危機管理監及び内閣情報通信政策監とし、構成員及びオブザーバーは、本部長の指定する職にある関係機関の最高情報セキュリティ責任者（CISO）等とする。

３　推進会議にサイバーセキュリティ対策推進専任審議官等会議（以下「専任審議官等会議」という。）を置く。専任審議官等会議は、関係機関の職員で議長の指定する職にある者によって構成する。

４　専任審議官等会議にサイバーセキュリティ対策推進会議幹事会（以下「幹事会」という。）を置く。幹事会は、関係機関の職員で議長の指定する職にある者によって構成する。

５　推進会議、専任審議官等会議及び幹事会の庶務は、内閣官房において処理する。

６　前各項に掲げるもののほか、推進会議、専任審議官等会議及び幹事会の運営に関する事項その他必要な事項は、議長が定める。

７　情報セキュリティ対策推進会議について（平成17年７月14日情報セキュリティ政策会議決定。以下「同決定」という。）第１項に基づき設置された情報セキュリティ対策推進会議が決定した事項、検討した事項及び議長指示等については、推進会議に、同決定第３項に基づき設置された幹事会が決定した事項及び検

討した事項等については、幹事会に、それぞれ引き継がれるものとする。

サイバーセキュリティ戦略本部の本部員の指定について

（平成 27 年 7 月 22 日
内閣総理大臣決定）
平成 27 年 10 月 23 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）第 30 条第２項第６号のサイバーセキュリティ戦略本部員として、情報通信技術（IT）政策担当大臣及び東京オリンピック競技大会・東京パラリンピック競技大会担当大臣を指定する。