資料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整備（案）

資料２－１　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整備について（案）概要

資料２－２　サイバーセキュリティ戦略本部重大事象施策評価規則（一部改定案）　新旧対照表

資料２－３　サイバーセキュリティ戦略本部重大事象施策評価規則（一部改定案）

資料２－４　サイバーセキュリティ戦略本部資料提供等規則（一部改定案）　新旧対照表

資料２－５　サイバーセキュリティ戦略本部資料提供等規則（一部改定案）

資料２－６　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（一部改定案）　新旧対照表

資料２－７　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（一部改定案）

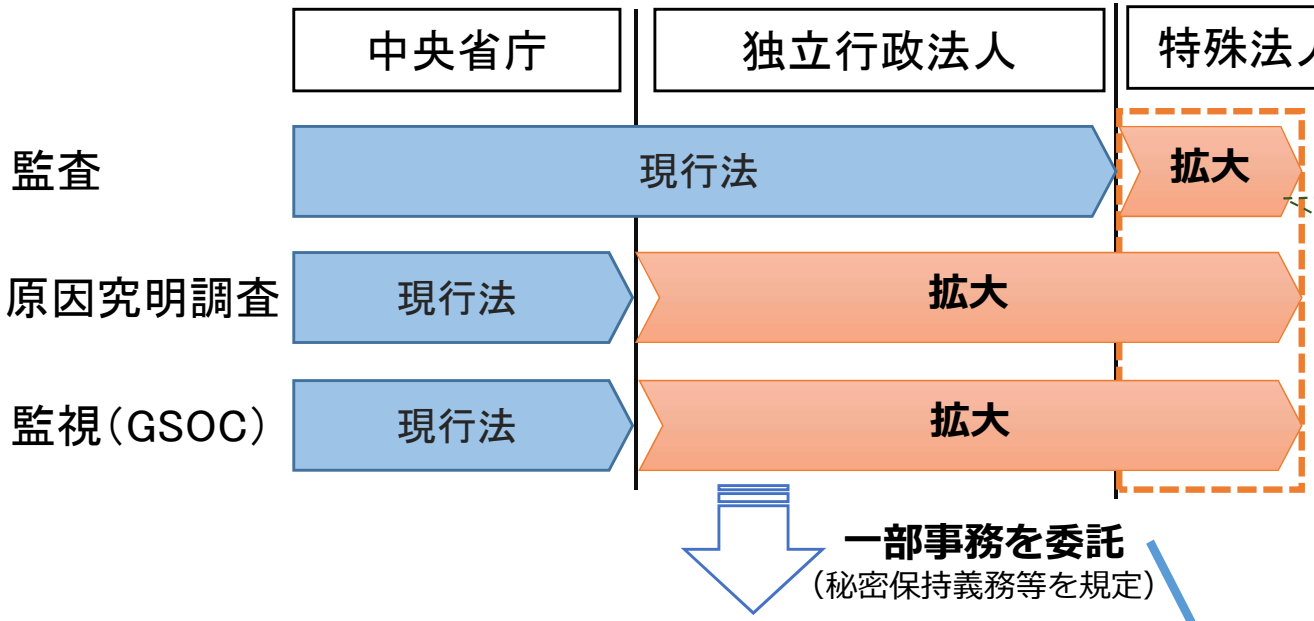
資料２－１

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整備について（案）概要

2016年10月12日

サイバーセキュリティ基本法の改正法の施行（2016年4月15日成立、4月22日公布、10月21日施行予定）

■ 国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大
■ サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）に委託



監視、監査、原因究明調査等の対象となる法人の指定（本部決定）

✓ 日本年金機構等の公的年金関係法人（※）及び地方公共団体情報システム機構（J-LIS）を指定。（9法人）

※ 日本年金機構、国家公務員共済組合連合会（KKR）、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、日本私立学校振興・共済事業団、公立学校共済組合

情報処理安全確保支援士制度の開始に伴う規定の整備（情報処理の促進に関する法律の一部改正に伴う政省令の整備）

✓ IPAへの委託は「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」「サイバーセキュリティ戦略本部重大事象施策評価規則」を踏まえて実施

その他法改正に伴い整備する規則等（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基準群（※前回戦略本部で改定済）
✓ 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
✓ サイバーセキュリティ戦略本部重大事象施策評価規則
✓ サイバーセキュリティ戦略本部資料提供等規則

基本法第13条の規定に基づき戦略本部が指定する法人（指定法人）について

■ 特殊法人・認可法人は、その行う業務や保有する情報も様々であることから、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動に及ぼす影響を勘案して、サイバーセキュリティ戦略本部が指定。

①から④の要件に該当するかを検討

①国の業務との一体性	②保有情報の機微性、業務の国民生活・経済活動へ与える影響	③法人の自主的な対策のみに委ねることの適切性	④NISCの知見・能力の活用可能性
		※ 自主的な対策に委ねた場合に必要な対策が講じられず、重大かつ深刻な事象を発生させた、又は発生させるおそれがあること	※ （NISCが行ってきた）インターネット接続口にセンサーを設置した監視による実効性あるセキュリティ対策が図られること）

以下の法人を指定

■ 公的年金関係
- 日本年金機構
- 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
- 国家公務員共済組合連合会
- 日本私立学校振興・共済事業団
- 公立学校共済組合

■ マイナンバー関係
- 地方公共団体情報システム機構

その他法改正に伴い整備する規則等について

※ []内は基本法の関連規定(改正後)

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

✓ サイバーセキュリティ戦略本部が実施する監査について、その目的、基本的な方向性、実施内容の概要等を定めるもの。

[一部改定の概要]

- 監査の対象を、国の行政機関及び独立行政法人に加えて、指定法人(特殊法人及び認可法人のうち改正後の基本法第13条の規定に基づき戦略本部が指定したもの。以下同じ。)に拡大。[第25条第1項第2号]
- 独立行政法人及び指定法人への監査事務の一部をIPAに実施させることを規定。[第30条第1項]

サイバーセキュリティ戦略本部重大事象施策評価規則

✓ サイバーセキュリティ戦略本部が行う原因究明調査の対象となる特定重大事象について、その定義及び手続等を定めるもの。

[一部改定の概要]

- 原因究明調査の対象を、国の行政機関に加えて、独立行政法人及び指定法人に拡大。[第25条第1項第3号]
- 改正後の基本法第30条の規定を踏まえ、独立行政法人及び指定法人への原因究明調査の事務の一部をIPAへの委託があった場合の手続を規定。[第30条第1項]

サイバーセキュリティ戦略本部資料提供等規則

✓ 各府省庁から戦略本部への資料提供及び戦略本部との情報共有の対象となる特殊法人等を定めるもの。

[一部改定の概要]

- 資料提供の対象となる事項を、各府省庁における特定重大事象に関するものに加えて、その所管する独立行政法人及び指定法人における特定重大事象に関するものに拡大。[第25条第1項第2号・第3号]
- あわせて、1月の戦略本部決定等を踏まえ、各省庁が所管する重要インフラ事業者等におけるインシデントに関するものを追加。
- 情報共有の対象となる特殊法人等について、各法人の根拠法の改正等を踏まえた整備を実施。

※ 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については、前回戦略本部(2016.8.31)で改定済。

（参考１）サイバーセキュリティ基本法の概要（平成28年改正後）

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、強靱な体制の構築

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（第24条）**

■**所掌事務等（第25条）**

⇒サイバーセキュリティ戦略案の作成、国の行政機関、独立行政法人・指定法人に対する監査・原因究明調査等の実施

■**組織等（第26条～第29条）**

⇒内閣官房長官を本部長として、副本部長（国務大臣）、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、総理が指定する国務大臣、有識者本部員で構成

■**事務の委託（第30条）**

⇒独立行政法人・指定法人に対する監査・原因究明調査の事務の一部をIPAその他政令で定める法人に委託（秘密保持義務を規定）

■**資料提供等（第31条～第36条）**

第Ⅴ章．罰則

■**罰則（第37条）**

⇒戦略本部からの事務の委託を受けた者が秘密保持義務に反した場合。1年以下の懲役又は50万円以下の罰金

（参考２）参照条文等

○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）（抄）

（国の行政機関等におけるサイバーセキュリティの確保）

第十三条　国は、国の行政機関、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独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第一項第九号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関、独立行政法人及び指定法人（特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。第三十二条第一項において同じ。）のうち、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するものをいう。以下同じ。）におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、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、独立行政法人又は指定法人の情報システムに対する不正な活動の監視及び分析、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演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。

（所掌事務等）

第二十五条　本部は、次に掲げる事務をつかさどる。

一　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。

二　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。

三　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。

四　前三号に掲げるもののほか、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。

２～４　略

（事務の委託）

第三十条　本部は、第二十五条第一項第二号に掲げる事務（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対策の基準に基づく監査に係るものに限る。）又は同項第三号に掲げる事務（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の原因究明のための調査に係るものに限る。）の一部を、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することができる。

２　前項の規定により事務の委託を受けた法人の役員若しくは職員又はこれらの職にあった者は、正当な理由がなく、当該委託に係る事務に関して知り得た秘密を漏らし、又は盗用してはならない。

３　第一項の規定により事務の委託を受けた法人の役員又は職員であって当該委託に係る事務に従事するものは、刑法（明治四十年法律第四十五号）その他の罰則の適用については、法令により公務に従事する職員とみなす。

○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）（抄）

（資料提供等）

第三十一条　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　前項に定めるもののほか、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。

（資料の提出その他の協力）

第三十二条　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、地方公共団体及び独立行政法人の長、国立大学法人（国立大学法人法（平成十五年法律第百十二号）第二条第一項に規定する国立大学法人をいう。）の学長、大学共同利用機関法人（同条第三項に規定する大学共同利用機関法人をいう。）の機構長、日本司法支援センター（総合法律支援法（平成十六年法律第七十四号）第十三条に規定する日本司法支援センターをいう。）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並びに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に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な資料の提出、意見の開陳、説明その他の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、同項の協力を依頼することができる。

○我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針（2016年1月25日サイバーセキュリティ戦略本部決定）（抄）

（4）重要インフラ事業者等に関する取組支援の強化

その際、基本法により設けられた仕組みを、適切に運用することとする。具体的には、本部長は、本部が行う関係行政機関における重要インフラ事業者等に関する施策に対する評価に基づき、又は本部が関係行政機関の長を通じて入手した重要インフラ事業者等に係る資料又は情報等に基づき、必要があると認めるときは、関係行政機関の長への勧告を行う。当該勧告は、あくまで各業法等に基づく重要インフラ事業者等に対する所管大臣等の監督等の権限を適切に行使させることを目的に運用されるものであり、その範囲において、本部及びNISCは関係行政機関と連携しつつ、重要インフラ事業者等における迅速かつ自主的な取組を促進していくこととする。

資料２－２

○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　月　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
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。	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 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。	第１条　法第25条第１項第３号に規定する「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」（以下「特定重大事象」という。）とは、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　国の行政機関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、行政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	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。	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（以下「当該行政機関」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。	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	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。）	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	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	四　復旧・再発防止策の評価
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。	２　施策の評価は、法第30条の規定により当該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の長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	第５条　特定重大事象に係る原因究明等は、当該行政機関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

事業者に委託して行うものを含む。）を行うものとする。	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、第一項の規定による補充調査を行ったときは、その結果を当該行政機関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 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 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）	（結果の通知等）
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、施策の評価が終了したときは、その結果を当該行政機関の長に通知するとともに、必要に応じ、法第27条第３項の規定による勧告を行うものとする。
（法第 31 条第２項の運用）	（法第30条第２項の運用）
第８条　本部長は、次に掲げる場合には、当	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。	該行政機関の長に対し、法第30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。	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。	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。	三　本部会合の場において当該行政機関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）	（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。	第９条　施策の評価に関する事務（特定重大事象に係る復旧・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30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。	２　緊急を要する場合における特定重大事象に係る復旧・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。	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。）	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	二　法第27条第４項の規定による報告の求め

資料２－３

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　月　日
一部改定（案）

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）

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

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）

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）

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

資料２－４

○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　月　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
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。	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 30 条及び第 31 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 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。	（提供しなければならない資料等） 第１条　法第 30 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	一　当該行政機関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 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 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 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 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。	二　前号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 30 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 31 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 30 条及び第 31 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 30 条又は第 31 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。
別表	別表
沖縄振興開発金融公庫	沖縄振興開発金融公庫
沖縄科学技術大学院大学学園	学校法人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	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	原子力損害賠償支援機構
銀行等保有株式取得機構	銀行等保有株式取得機構
預金保険機構	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	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	日本放送協会
日本電信電話株式会社	日本電信電話株式会社
東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	西日本電信電話株式会社
日本郵政株式会社	日本郵政株式会社
日本郵便株式会社	日本郵便株式会社
日本たばこ産業株式会社	日本たばこ産業株式会社
株式会社日本政策金融公庫	株式会社日本政策金融公庫
株式会社日本政策投資銀行	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	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	株式会社国際協力銀行
日本銀行	日本銀行
国家公務員共済組合連合会	
公立学校共済組合	公立学校共済組合
日本私立学校振興・共済事業団	日本私立学校振興・共済事業団
放送大学学園	放送大学学園
日本年金機構	日本年金機構
日本赤十字社	日本赤十字社
健康保険組合連合会	健康保険組合連合会
全国健康保険協会	全国健康保険協会
国民年金基金連合会	国民年金基金連合会
日本中央競馬会	日本中央競馬会
農水産業協同組合貯金保険機構	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	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	日本アルコール産業株式会社
株式会社産業革新機構	株式会社産業革新機構
株式会社海外需要開拓支援機構	海外需要開拓支援機構
北海道旅客鉄道株式会社	北海道旅客鉄道株式会社
四国旅客鉄道株式会社	四国旅客鉄道株式会社
	九州旅客鉄道株式会社
日本貨物鉄道株式会社	日本貨物鉄道株式会社
東京地下鉄株式会社	東京地下鉄株式会社
成田国際空港株式会社	成田国際空港株式会社
東日本高速道路株式会社	東日本高速道路株式会社
中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	西日本高速道路株式会社
首都高速道路株式会社	首都高速道路株式会社
阪神高速道路株式会社	阪神高速道路株式会社
本州四国連絡高速道路株式会社	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	新関西国際空港株式会社
	中部国際空港株式会社
中間貯蔵・環境安全事業株式会社	日本環境安全事業株式会社

資料２－５

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　月　日
一部改定（案）

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　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。

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

資料２－６

○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　９　月　２５　日 サイバーセキュリティ戦略本部決定 平　成　２８　年　　月　　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　９　月　２５　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。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。	サイバーセキュリティ基本法（平成 26 年法律第 104 号）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、国の行政機関及び独立行政法人（以下「行政機関等」という。）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、行政機関等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、行政機関等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	２　監査の対象 国の行政機関、すなわち、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

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。	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監査の対象とする。 なお、独立行政法人については、当面、特に必要があると認める場合に監査の対象とする。
３　監査の基本的な方向性 （略）	３　監査の基本的な方向性 （略）
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 （略）	４　監査の実施内容 (1) マネジメント監査 「政府機関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 （略）
５　監査の進め方 (1)・(2) （略）	５　監査の進め方 (1)・(2) （略）

(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。	(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。 　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報告するものとする。
(4) 監査実施結果の取りまとめ・報告 （略）	(4) 監査実施結果の取りまとめ・報告 （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 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に委託し、同機構に実施させる。	(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。

資料２－７

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　月　日
一部改定（案）

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。

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に委託し、同機構に実施させる。