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２－８　独立行政法人等における標的型攻撃対策について　※１

資料２－９　高度サイバー攻撃対処のためのリスク評価等のガイドライン（一部改定案）新旧対照表

資料２－10　高度サイバー攻撃対処のためのリスク評価等のガイドライン（一部改定案）

資料２－11　情報セキュリティ緊急支援チームの支援対象機関等について

資料２－12　情報セキュリティ緊急支援チームの運営等について（一部改定案）新旧対照表

資料２－13　情報セキュリティ緊急支援チームの運営等について（一部改定案）

※１は非公表

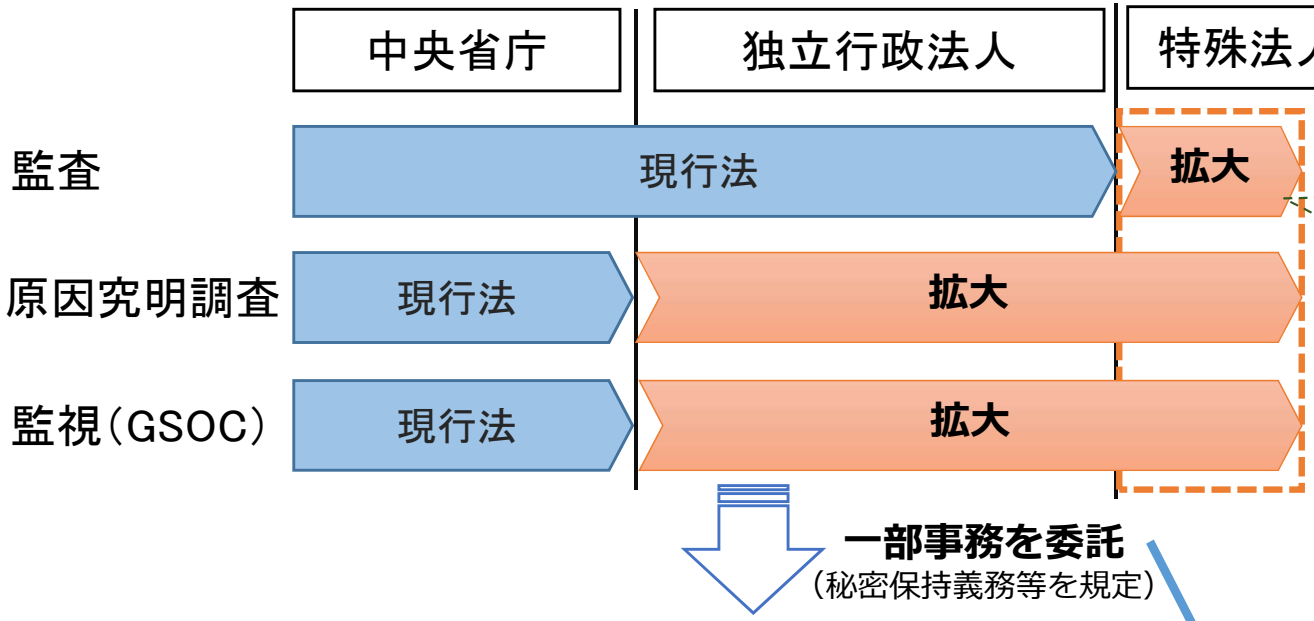
資料２－１

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。

資料２－９

高度サイバー攻撃対処のためのリスク評価等のガイドライン　新旧対照表

（下線部分は改定部分）

改定案	現　行
高度サイバー攻撃対処のための リスク評価等のガイドライン 平成 28 年　月　日 サイバーセキュリティ対策推進会議	高度サイバー攻撃対処のための リスク評価等のガイドライン 平成 26 年６月 25 日 情報セキュリティ対策推進会議
第１部　総則	第１部　総則
１　本ガイドラインの目的	１　本ガイドラインの目的
今日において、政府機関等（府省庁及び独立行政法人等（独立行政法人及びサイバーセキュリティ基本法第十三条に定める指定法人をいう。以下同じ。）をいう。以下同じ。）の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、政府機関等の運営上、極めて重要である。	今日において、各府省庁の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、各府省庁の運営上、極めて重要である。
情報セキュリティ上の脅威は、内部者による規律違反から外部者による攻撃まで多岐にわたって存在し、これらの様々な脅威に対処するため、政府機関等においては、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基づき、従来から情報セキュリティ水準の斉一的な引き上げを図っているところである。	情報セキュリティ上の脅威は、内部者による規律違反から外部者による攻撃まで多岐にわたって存在し、これらの様々な脅威に対処するため、政府機関においては、「政府機関の情報セキュリティ対策のための統一基準群」に基づき、従来から情報セキュリティ水準の斉一的な引き上げを図っているところである。
一方で、政府機関等においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃（以下「高度サイバー攻撃」という。）が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。	一方で、政府機関においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃（以下「高度サイバー攻撃」という。）が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

（略） このため、本ガイドラインでは、政府機関等において、高度サイバー攻撃の標的とされる蓋然性が高い業務・情報に重点を置いたメリハリのある資源の投入を計画的に進め、それらの業務・情報に係る多重的な防御の仕組みを実現する際に採るべき手法として、以下に焦点を当てた取組（以下「本取組」という。）について示す。 ① 情報セキュリティガバナンスの確立 最高情報セキュリティ責任者（以下「CISO」という。）の指揮の下で、重点的・計画的な情報セキュリティ対策を実施するための方針を決定する。 ② （略） ③ （略）	（略） このため、本ガイドラインでは、各府省庁において、高度サイバー攻撃の標的とされる蓋然性が高い業務・情報に重点を置いたメリハリのある資源の投入を計画的に進め、それらの業務・情報に係る多重的な防御の仕組みを実現する際に採るべき手法として、以下に焦点を当てた取組（以下「本取組」という。）について示す。 ① 情報セキュリティガバナンスの確立 CISO の指揮の下で、重点的・計画的な情報セキュリティ対策を実施するための方針を決定する。 ② （略） ③ （略）
２ 本ガイドラインの位置付け 本ガイドラインは、サイバーセキュリティ戦略（平成 27 年９月４日閣議決定）に基づき、政府機関等における情報及び情報システムに係る情報セキュリティ水準の一層の向上及びサイバー攻撃への対処体制の充実・強化に資するために策定するものである。 本ガイドラインでは、前述の目的を実現するための基本的な考え方及び取組のプロセスを示し、想定される具体的な脅威及び対策その他の迅速かつ柔軟に対応すべき事項については、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。）が策定する本ガイドラインの付属書（以下「付属書」という。）に記載する。 （略）	**２ 本ガイドラインの位置付け** 本ガイドラインは、サイバーセキュリティ戦略（平成 25 年６月 10 日情報セキュリティ政策会議決定）に基づき、各府省庁における情報及び情報システムに係る情報セキュリティ水準の一層の向上及びサイバー攻撃への対処体制の充実・強化に資するために策定するものである。 本ガイドラインでは、前述の目的を実現するための基本的な考え方及び取組のプロセスを示し、想定される具体的な脅威及び対策その他の迅速かつ柔軟に対応すべき事項については、内閣官房情報セキュリティセンター（以下「NISC」という。）が策定する本ガイドラインの付属書（以下「付属書」という。）に記載する。 （略）

３　用語定義 本ガイドラインにおける用語の定義は、以下に定めるところによる。 ・「業務領域」：府省庁組織令上の所掌事務、その集合若しくはその一部又は独立行政法人等の個別法等で定める業務、その集合若しくはその一部をいう。 ・「機微業務領域」：所掌事務又は業務に以下の情報の収集、作成等が含まれる業務領域をいう。 （略） ・「情報保全担当部署」：自組織における情報保全の推進を担当する課室をいう。 ・「情報セキュリティ担当部署」：自組織における情報セキュリティ対策の推進を担当する課室をいう。 （略） ・「資源配分部署」：自組織における人的資源又は資金の配分・管理を行う課室をいう。 （略）	３　用語定義 本ガイドラインにおける用語の定義は、以下に定めるところによる。 ・「業務領域」：各府省庁組織令上の所掌事務又はその集合若しくはその一部をいう。 ・「機微業務領域」：所掌事務に以下の情報の収集、作成等が含まれる業務領域をいう。 （略） ・「情報保全担当部署」：各府省庁における情報保全の推進を担当する課室をいう。 ・「情報セキュリティ担当部署」：各府省庁における情報セキュリティ対策の推進を担当する課室をいう。 （略） ・「資源配分部署」：各府省庁における人的資源又は資金の配分・管理を行う課室をいう。 （略）
４　適用範囲 (1)　府省庁 本ガイドラインは、法律の規定に基づき内閣に置かれる機関及び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）第四十九条第一項及び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並びにこれらに置かれる機関に対して適用する。 (2)　独立行政法人等 本ガイドラインは、独立行政法人及びサイバーセキュリティ基本法第	４　適用範囲 本ガイドラインは、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若しくはこれらに置かれる機関に対して適用する。

十三条に定める指定法人に対して適用する。	
第２部　実施事項	**第２部　実施事項**
１　本取組の流れ	**１　本取組の流れ**
(1)～(3)　（略）	**(1)～(3)**　（略）
(4)　CISO による方針決定等	**(4)　CISO による方針決定等**
ア　（略）	**ア**　（略）
イ　CISO による方針決定 政府機関等における情報セキュリティガバナンスを確立し、CISO の指揮の下で高度サイバー攻撃の脅威に対抗していくため、リスク評価結果を判断材料として、対策導入計画の承認等の CISO による方針決定を行う。	**イ　CISO による方針決定** 各府省庁における情報セキュリティガバナンスを確立し、CISO の指揮の下で高度サイバー攻撃の脅威に対抗していくため、リスク評価結果を判断材料として、対策導入計画の承認等の CISO による方針決定を行う。
(5)　NISC への報告 政府機関等全体としての本取組の実施状況等を取りまとめ、サイバーセキュリティ対策推進会議等への報告を行うため、CISO が方針決定した対策導入計画等について、府省庁の計画等は直接、独立行政法人等の計画等は所管府省庁を通じて、それぞれ NISC に報告を行う。	**(5)　NISC への報告** 政府全体としての本取組の実施状況等を取りまとめ、情報セキュリティ対策推進会議等への報告を行うため、CISO が方針決定した対策導入計画等について、各府省庁から NISC に報告を行う。
２　本取組の実施プロセス	**２　本取組の実施プロセス**
(1)　リスク評価等の実施に向けた準備	**(1)　リスク評価等の実施に向けた準備**
ア　（略）	**ア**　（略）
イ　リスク評価の対象とする業務領域の選定 情報保全担当部署は、自組織の業務領域から、本取組におけるリスク評価の対象とする「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を、(ｱ)の要領に従い、自組織において最適な方法により選定する。また、リスク評価の対象とする業務領域の選定に当たっては、(ｲ)の事項に留意する。	**イ　リスク評価の対象とする業務領域の選定** 情報保全担当部署は、自府省庁の業務領域から、本取組におけるリスク評価の対象とする「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を、(ｱ)の要領に従い、自府省庁において最適な方法により選定する。また、リスク評価の対象とする業務領域の選定に当たっては、(ｲ)の事項に留意する。
(ｱ)　選定要領	**(ｱ)　選定要領**

① 自組織内の局部課等の事務分掌等に照らした外形的な判断により「機微業務領域」に該当する業務領域を選定する。また、「機微業務領域」には該当しないものの、情報が窃取、破壊等されることにより、行政運営等に壊滅的又は深刻な影響を及ぼすと考えられるなど、その特性等に照らして高度サイバー攻撃の標的となる蓋然性が高いと考えられる業務領域がある場合は、当該業務領域も併せて選定する。	① 自府省庁内の局部課等の事務分掌等に照らした外形的な判断により「機微業務領域」に該当する業務領域を選定する。また、「機微業務領域」には該当しないものの、情報が窃取、破壊等されることにより、行政運営等に壊滅的又は深刻な影響を及ぼすと考えられるなど、その特性等に照らして高度サイバー攻撃の標的となる蓋然性が高いと考えられる業務領域がある場合は、当該業務領域も併せて選定する。
② ①に該当する業務領域がない場合は、自組織において定常的に取り扱う機密性の高い情報の有無について検討し、該当がある場合は当該情報を取り扱う業務領域を選定する。	② ①に該当する業務領域がない場合は、自府省庁において定常的に取り扱う機密性の高い情報の有無について検討し、該当がある場合は当該情報を取り扱う業務領域を選定する。
③ ①又は②の業務領域を自組織における「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」として、リスク評価の対象とする。	③ ①又は②の業務領域を自府省庁における「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」として、リスク評価の対象とする。
(ｲ) （略）	(ｲ) （略）
(2) リスク評価の実施	**(2) リスク評価の実施**
ア （略）	**ア** （略）
イ 対象システムの特定・現状点検	**イ 対象システムの特定・現状点検**
(ｱ) 対象システムの特定	**(ｱ) 対象システムの特定**
① （略）	① （略）
② オープン系ネットワーク上に存在する情報システム（①に該当するものを除く。）であって、機微業務等実施部署が「保護対象とする業務領域」の業務を遂行する上で使用する外部ネットワークから切り離された情報システムとの間で、何らかの手段により「保護対象とする業務領域」に係る電子デー	② オープン系ネットワーク上に存在する情報システム（①に該当するものを除く。）であって、機微業務等実施部署が「保護対象とする業務領域」の業務を遂行する上で使用する外部ネットワークから物理的に切り離された情報システムとの間で、何らかの手段により「保護対象とする業務領域」に係る電

タ（機密性の高い情報そのもののほか、当該情報を推測し得る周辺情報を含む。）をやり取りするもの	子データ（機密性の高い情報そのもののほか、当該情報を推測し得る周辺情報を含む。）をやり取りするもの
(ｲ)　（略）	(ｲ)　（略）
(3)・(4)　（略）	(3)・(4)　（略）
(5)　NISC への報告	(5)　NISC への報告
ア　府省庁 府省庁の情報セキュリティ担当部署は、CISO が方針決定した対策導入計画等について、第３部の３に掲げるものを NISC に報告する。	情報セキュリティ担当部署は、CISO が方針決定した対策導入計画等について、第３部の３に掲げるものを NISC に報告する。
イ　独立行政法人等 独立行政法人等の情報セキュリティ担当部署は、CISO が方針決定した対策導入計画等について所管府省庁に報告する。 府省庁は、所管する独立行政法人等の報告を取りまとめ、第３部の３に掲げるものを NISC に報告する。	（新設）
ウ　公表 NISC は、政府機関等からの報告に基づき、本取組が適切に実施されているか確認を行い、政府機関等全体としての進捗状況等についてサイバーセキュリティ対策推進会議等に報告した上で、政府機関等を代表して公表する。	NISC は、各府省庁からの報告に基づき、本取組が適切に実施されているか確認を行い、政府機関全体としての進捗状況等について情報セキュリティ対策推進会議等に報告した上で、政府機関を代表して公表する。
第３部　リスク評価ダッシュボード等	第３部　リスク評価ダッシュボード等
１　リスク評価ダッシュボードの位置付け	１　リスク評価ダッシュボードの位置付け
（略） NISC は、政府機関等からの報告内容から、政府機関等全体としての対策実施状況や対策導入計画の進捗状況を評価するとともに、対策実施に係る技術的な課題や運用上の課題を把握・分析し、本取組の改善を図る。	（略） NISC は、各府省庁からの報告内容から、政府機関全体としての対策実施状況や対策導入計画の進捗状況を評価するとともに、対策実施に係る技術的な課題や運用上の課題を把握・分析し、本取組の改善を図る。
２　（略）	２　（略）

３　NISC への報告	３　NISC への報告
（略）	（略）
なお、NISC への報告時期については、NISC からの事務連絡文書等を通じて別途連絡する。また、サイバーセキュリティ対策推進会議に加え、府省庁相互の緊密な連携を確保し、カウンターインテリジェンスの強化に向けた施策の総合的かつ効果的な推進を図る場であるカウンターインテリジェンス推進会議においても報告を行うため、当該内容については、内閣情報調査室と共有する。	なお、NISC への報告時期については、NISC からの事務連絡文書等を通じて別途連絡する。また、情報セキュリティ対策推進会議に加え、各府省庁相互の緊密な連携を確保し、カウンターインテリジェンスの強化に向けた施策の総合的かつ効果的な推進を図る場であるカウンターインテリジェンス推進会議においても報告を行うため、当該内容については、内閣情報調査室と共有する。
第４部　本取組の運用管理	**第４部　本取組の運用管理**
１　（略）	１　（略）
２　本ガイドライン等の改定	２　本ガイドライン等の改定
(1)　本ガイドラインの改定	(1)　本ガイドラインの改定
本取組の実施プロセス等に係る見直しの必要が生じた場合には、NISC において内閣情報調査室と連携して検討を行った上で、サイバーセキュリティ対策推進会議において本ガイドラインの改定について決定を行う。	本取組の実施プロセス等に係る見直しの必要が生じた場合には、NISC において内閣情報調査室と連携して検討を行った上で、情報セキュリティ対策推進会議において本ガイドラインの改定について決定を行う。
(2)　付属書の改定	(2)　付属書の改定
対策セットを含む付属書の記載事項に係る見直しの必要が生じた場合には、府省庁の意見を踏まえた上で NISC において改定を行う。	対策セットを含む付属書の記載事項に係る見直しの必要が生じた場合には、各府省庁の意見を踏まえた上で NISC において改定を行う。
（略）	（略）
３　NISC への報告	３　NISC への報告
(1)　対策セットに係る評価検討体制等の構築	(1)　対策セットに係る評価検討体制等の構築
新たな攻撃方法の出現や既存の攻撃方法の変化に対応するため、NISC において、政府機関等との情報共有を行い、これらの攻撃を監視・把握するとともに、高度サイバー攻撃対処に係る評価・検討等に関する以下の	新たな攻撃方法の出現や既存の攻撃方法の変化に対応するため、NISC において、府省庁等との情報共有を行い、これらの攻撃を監視・把握するとともに、高度サイバー攻撃対処に係る評価・検討等に関する以下の役

役割を担うための体制（以下「評価検討委員会」という。）を構築する。また、評価検討委員会は、高度サイバー攻撃に関する学識者委員を中心に構成する。 ① 政府機関等が喫緊の課題として対処すべき新たな高度サイバー攻撃手法及び新たな対策に関する情報収集 ②・③ （略） **(2) 対策セットの見直し** 政府機関等が喫緊の課題として対処すべき新たな高度サイバー攻撃手法が把握された場合その他対策セットに係る見直しが必要であると判断された場合には、対策セットの見直しについて検討を行う。 対策セットには、高度サイバー攻撃のシナリオに対応する情報システムの設計、監視強化等に係る対策のうち、評価検討委員会において評価を行い、技術的・運用上の見地から有効であることが確認された新たな対策について、府省庁と協議の上、取り入れる。	割を担うための体制（以下「評価検討委員会」という。）を構築する。また、評価検討委員会は、高度サイバー攻撃に関する学識者委員を中心に構成する。 ① 政府機関が喫緊の課題として対処すべき新たな高度サイバー攻撃手法及び新たな対策に関する情報収集 ②・③ （略） **(2) 対策セットの見直し** 政府機関が喫緊の課題として対処すべき新たな高度サイバー攻撃手法が把握された場合その他対策セットに係る見直しが必要であると判断された場合には、対策セットの見直しについて検討を行う。 対策セットには、高度サイバー攻撃のシナリオに対応する情報システムの設計、監視強化等に係る対策のうち、評価検討委員会において評価を行い、技術的・運用上の見地から有効であることが確認された新たな対策について、各府省庁と協議の上、取り入れる。

資料２－10

高度サイバー攻撃対処のための
リスク評価等のガイドライン（案）

平成 28 年　月　日

サイバーセキュリティ対策推進会議

目次

第１部　総則

１　本ガイドラインの目的

今日において、政府機関等（府省庁及び独立行政法人等（独立行政法人及びサイバーセキュリティ基本法第十三条に定める指定法人をいう。以下同じ。）をいう。以下同じ。）の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、政府機関等の運営上、極めて重要である。

情報セキュリティ上の脅威は、内部者による規律違反から外部者による攻撃まで多岐にわたって存在し、これらの様々な脅威に対処するため、政府機関等においては、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基づき、従来から情報セキュリティ水準の斉一的な引き上げを図っているところである。

一方で、政府機関等においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃（以下「高度サイバー攻撃」という。）が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

高度サイバー攻撃のうち、昨今、特に大きな脅威となっている標的型攻撃の主目的は、情報システムの端末を不正プログラムに感染させること等ではなく、外部からの情報システム内部への侵入による情報の窃取・破壊等であり、そのために組織力を動員した攻撃が行われることから、内部統制的な手法だけでは十分な防御を行うことは困難であり、情報システムにおける適切な対策の実施及び運用・監視の強化を伴う計画的で持続可能な情報セキュリティ投資が必要となる。

このため、本ガイドラインでは、政府機関等において、高度サイバー攻撃の標的とされる蓋然性が高い業務・情報に重点を置いたメリハリのある資源の投入を計画的に進め、それらの業務・情報に係る多重的な防御の仕組みを実現する際に採るべき手法として、以下に焦点を当てた取組（以下「本取組」という。）について示す。

①　情報セキュリティガバナンスの確立

最高情報セキュリティ責任者（以下「CISO」という。）の指揮の下で、重点的・計画的な情報セキュリティ対策を実施するための方針を決定する。

②　高度サイバー攻撃対処のためのリスク評価の実施

高度サイバー攻撃の標的とされる蓋然性が高い業務領域を選定し、当該業務領域に係るリスク評価に基づく情報セキュリティ対策を重点的に実施する。

③　高度サイバー攻撃対処のための対策の計画的な実施

高度サイバー攻撃の脅威に対抗するための対策の着実な実施に向けて、複数年にわたる計画を策定する。

２　本ガイドラインの位置付け

本ガイドラインは、サイバーセキュリティ戦略（平成 27 年９月４日閣議決定）に基づき、政府機関等における情報及び情報システムに係る情報セキュリティ水準の一層の向上及びサイバー攻撃への対処体制の充実・強化に資するために策定するものである。

本ガイドラインでは、前述の目的を実現するための基本的な考え方及び取組のプロセスを示し、想定される具体的な脅威及び対策その他の迅速かつ柔軟に対応すべき事項については、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。）が策定する本ガイドラインの付属書（以下「付属書」という。）に記載する。

なお、本ガイドライン等の改定を含む本取組の運用管理については、第４部に示す。

３　用語定義

本ガイドラインにおける用語の定義は、以下に定めるところによる。

- 「業務領域」：府省庁組織令上の所掌事務、その集合若しくはその一部又は独立行政法人等の個別法等で定める業務、その集合若しくはその一部をいう。
- 「機微業務領域」：所掌事務又は業務に以下の情報の収集、作成等が含まれる業務領域をいう。
  - 窃取、破壊等されることにより、国の安全が害されるおそれがある情報
  - 窃取、破壊等されることにより、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがある情報
  - 窃取、破壊等されることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがある情報
- 「情報保全担当部署」：自組織における情報保全の推進を担当する課室をいう。
- 「情報セキュリティ担当部署」：自組織における情報セキュリティ対策の推進を担当する課室をいう。
- 「機微業務等実施部署」：本取組におけるリスク評価の対象として選定された業務領域に係る業務を主管する課室をいう。

- 「対象システム」: 本取組の対象として特定された情報システムをいう。
- 「対象システム管理責任部署」: 対象システムの整備又は運用管理を担当する課室をいう。
- 「資源配分部署」: 自組織における人的資源又は資金の配分・管理を行う課室をいう。
- 「対策セット」: 高度サイバー攻撃のシナリオ並びにそれに対応した統制目標及び当該目標を達成するための情報システムの設計、監視強化等に係る対策の集合として、付属書に掲げられたものをいう。

4　適用範囲

(1)　府省庁

本ガイドラインは、法律の規定に基づき内閣に置かれる機関及び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）第四十九条第一項及び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並びにこれらに置かれる機関に対して適用する。

(2)　独立行政法人等

本ガイドラインは、独立行政法人及びサイバーセキュリティ基本法第十三条に定める指定法人に対して適用する。

第２部　実施事項

１　本取組の流れ

(1)　リスク評価等の実施に向けた準備

ア　リスク評価等の実施に向けたコミュニケーション

本取組は、情報セキュリティ対策についてメリハリのある資源配分を行うため、対象システムを特定し、当該情報システムについて重点的かつ計画的に対策を実施することを最終的な目的として、その過程において「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を選定し、リスク評価等を実施するものである。

リスク評価等の実施に当たっては、中心的な役割を担う情報保全担当部署と情報セキュリティ担当部署との間で本取組の目的等に関する認識を共有しておく必要があるため、事前に十分なコミュニケーションを図る。

イ　リスク評価の対象とする業務領域の選定

本取組では、高度サイバー攻撃の脅威に対抗することを目的としていることから、その標的とされる蓋然性が高いと考えられる業務領域を選定し、当該業務領域をリスク評価の対象とする。

(2)　リスク評価の実施

ア　保護対象とする業務領域の特定

選定した「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」に対する高度サイバー攻撃事案が発生した場合における組織・業務への影響度等について検討を行い、想定される影響度等に応じて、当該業務領域から本取組における「保護対象とする業務領域」を特定する。

イ　対象システムの特定・現状点検等

特定した「保護対象とする業務領域」において使用されている情報システムを本取組における情報セキュリティ対策の重点化の対象（対象システム）として特定し、対策セットの対策の実施状況を始めとした対象システムの現状点検を行い、対策実施状況及び残存リスクについて評価する。

(3)　リスク評価結果を踏まえた対策導入計画（案）の作成等

ア　対象システムごとの対策導入計画（案）の作成

リスク評価結果、システム更改時期等を踏まえ、対策セットの対策導入を始めとした対象システムごとの対策強化について、検討を行う。また、予算措置や設計変更を伴う対策の実施には一定程度の時間が必要となるため、検討結果から、優先順位や資源配分も勘案し、対策の着実

な導入に向けた計画（以下「対策導入計画」という。）の案を作成する。

イ　対策導入計画（案）の調整

対象システムの情報セキュリティ対策の水準について、関係者間で認識の相違が生じると、情報セキュリティ上の問題が生じる可能性があるほか、対策の導入により対象システムの利便性が低下することも想定されることから、関係者間で共通認識を持ち、協力して計画的に対策を推進するため、対策導入計画（案）の内容を共有するとともに、必要に応じて調整を行う。また、複数の対象システムが特定され、複数の対策導入計画(案)が作成されている場合においては、必要に応じて、それらの間での調整も行う。

(4)　CISOによる方針決定等

ア　リスク評価ダッシュボードの作成

CISOによる方針決定において、CISOがリスク評価結果を基に対策導入計画の妥当性等を円滑に判断できるよう、それらについて的確かつ簡潔に取りまとめた資料（以下「リスク評価ダッシュボード」という。）を作成する。

イ　CISOによる方針決定

政府機関等における情報セキュリティガバナンスを確立し、CISOの指揮の下で高度サイバー攻撃の脅威に対抗していくため、リスク評価結果を判断材料として、対策導入計画の承認等のCISOによる方針決定を行う。

(5)　NISCへの報告

政府機関等全体としての本取組の実施状況等を取りまとめ、サイバーセキュリティ対策推進会議等への報告を行うため、CISOが方針決定した対策導入計画等について、府省庁の計画等は直接、独立行政法人等の計画等は所管府省庁を通じて、それぞれNISCに報告を行う。

２　本取組の実施プロセス

(1)　リスク評価等の実施に向けた準備

ア　リスク評価等の実施に向けたコミュニケーション

情報セキュリティ担当部署は、情報保全担当部署に対して、現在の情報セキュリティ上の脅威、発生事案例等、高度サイバー攻撃事案発生時の影響を検討するための情報を提供する。また、リスク評価の実施を始めとした本取組の目的、実施プロセス等を説明し、それらについて認識を共有するとともに、本取組における両者の役割を明確化する。

イ　リスク評価の対象とする業務領域の選定

情報保全担当部署は、自組織の業務領域から、本取組におけるリスク評価の対象とする「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を、(ｱ)の要領に従い、自組織において最適な方法により選定する。また、リスク評価の対象とする業務領域の選定に当たっては、(ｲ)の事項に留意する。

(ｱ)　選定要領

①　自組織内の局部課等の事務分掌等に照らした外形的な判断により「機微業務領域」に該当する業務領域を選定する。また、「機微業務領域」には該当しないものの、情報が窃取、破壊等されることにより、行政運営等に壊滅的又は深刻な影響を及ぼすと考えられるなど、その特性等に照らして高度サイバー攻撃の標的となる蓋然性が高いと考えられる業務領域がある場合は、当該業務領域も併せて選定する。

②　①に該当する業務領域がない場合は、自組織において定常的に取り扱う機密性の高い情報の有無について検討し、該当がある場合は当該情報を取り扱う業務領域を選定する。

③　①又は②の業務領域を自組織における「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」として、リスク評価の対象とする。

(ｲ)　選定に当たっての留意事項

・　「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」は、CISO がその重要性を容易に認識できる粒度で選定すること。

・　選定要領の②によって選定する場合は、個別の情報の機密性ではなく、適当な粒度の集合（カテゴリ）としての機密性に焦点を当てた検討を行うこと。

・　「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を選定するための作業に極力負荷をかけず、継続的に実施できる方法で選定すること。

(2) リスク評価の実施

ア　保護対象とする業務領域の特定

情報保全担当部署は、選定した「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」の機微業務等実施部署に対して、当該業務領域に係るリスク評価を依頼する。

機微業務等実施部署は、「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」に対する高度サイバー攻撃事案が発生した場合における組織・業務への影響度等について検討を行い、その結果をリスク評価等に係る作業シート（以下「リスク評価ワークシート」という。）に記入する。

情報保全担当部署は、機微業務等実施部署における検討結果に応じて、選定した「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」の全部又は一部を本取組における「保護対象とする業務領域」として特定する。

なお、本プロセスの過程で、情報保全担当部署が選定したもの以外の業務領域を「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」として扱う必要性が認められた場合は、情報保全担当部署その他の関係部署において必要な調整を行う。

イ　対象システムの特定・現状点検等

(ｱ)　対象システムの特定

情報保全担当部署又は情報セキュリティ担当部署は、以下に該当する情報システムを対象システムとして特定する。

なお、対象システムに該当がない「保護対象とする業務領域」については、以降の実施プロセスの対象外とする。

①　インターネットに直接又は間接的に接続されているネットワーク（以下「オープン系ネットワーク」という。）上に存在する情報システムのうち、機微業務等実施部署が「保護対象とする業務領域」の業務を遂行する上で使用するもの

②　オープン系ネットワーク上に存在する情報システム（①に該当するものを除く。）であって、機微業務等実施部署が「保護対象とする業務領域」の業務を遂行する上で使用する外部ネットワークから切り離された情報システムとの間で、何らかの手段により「保護対象とする業務領域」に係る電子データ（機密性の高い情報そのもののほか、当該情報を推測し得る周辺情報を含む。）をやり取りするもの

(ｲ)　対象システムの現状点検等

情報セキュリティ担当部署は、特定した対象システムの対象システム管理責任部署に対して、当該情報システムに係るリスク評価等

を依頼する。

対象システム管理責任部署は、当該システムの構成要素を確認し、対策セットの中で対策が求められている構成要素ごとに対策セットの対策を実施しているかなど、対策実施状況を点検する。また、現在の対策実施状況における残存リスクを把握し、これらのリスク評価結果をリスク評価ワークシートに記入する。

なお、対象システムが他の情報システム上に構築されているなど、対象システム管理責任部署のみで点検等を実施できない場合は、情報セキュリティ担当部署とともに、当該他の情報システムの整備又は運用管理を担当する課室と調整を行い、必要に応じて、当該情報システム及びその整備又は運用管理を担当する課室を、それぞれ対象システム及び対象システム管理責任部署に加えた上で以降の実施プロセスの対象とする。

(3) リスク評価結果を踏まえた対策導入計画（案）の作成等

ア 対象システムごとの対策導入計画（案）の作成

対象システム管理責任部署は、リスク評価結果、対策の優先順位、予算措置の要否、システム更改時期等を踏まえ、対象システムに導入すべき対策及びその導入時期について検討を行い、付属書において設定されている統制目標を達成するための対策導入計画の案を作成し、リスク評価ワークシートに記入する。

なお、初年度に対策導入計画を策定済みの対象システムについては、次年度以降に当該計画の進捗状況等を踏まえた見直しを行う。

イ 対策導入計画（案）の調整

対象システム管理責任部署は、対象システムに係るリスク評価結果及び対策導入計画（案）、対策導入に伴うユーザ側への影響等がある場合は、その内容等について、当該システムのユーザ側である機微業務等実施部署に説明を行う。

機微業務等実施部署は、対策導入計画（案）について、業務遂行上求める情報セキュリティ水準、ユーザ側への影響等の観点から確認し、必要に応じて、対象システム管理責任部署と対策導入計画（案）の修正等に係る調整を実施する。

情報セキュリティ担当部署は、複数の対策導入計画（案）の間での調整の要否を確認し、必要に応じて、対象システム管理責任部署を始めとした関係部署との調整を実施した上で、CISO に承認を求めるための対策導入計画の案として確定させる。また、本プロセスにおいて資源配分関連の調整が必要であれば、資源配分部署とも調整を実施する。

(4) CISOによる方針決定等

ア　リスク評価ダッシュボードの作成

情報セキュリティ担当部署は、リスク評価ワークシートに基づき、リスク評価結果、対策導入計画（案）等の内容を取りまとめ、リスク評価ダッシュボードを作成する。

イ　CISOによる方針決定

情報セキュリティ担当部署は、作成したリスク評価ダッシュボードを用いて、CISOにリスク評価結果について報告するとともに、対策導入計画の承認を求める。

CISOは、残存リスク等を把握した上で、承認を求められた対策導入計画の実行方針を承認・決定し、又は再検討・修正を関係部署（資源配分担当部署を含む。）に指示する。

(5) NISCへの報告

ア　府省庁

府省庁の情報セキュリティ担当部署は、CISOが方針決定した対策導入計画等について、第３部の３に掲げるものをNISCに報告する。

イ　独立行政法人等

独立行政法人等の情報セキュリティ担当部署は、CISOが方針決定した対策導入計画等について所管府省庁に報告する。

府省庁は、所管する独立行政法人等の報告を取りまとめ、第３部の３に掲げるものをNISCに報告する。

ウ　公表

NISCは、政府機関等からの報告に基づき、本取組が適切に実施されているか確認を行い、政府機関等全体としての進捗状況等についてサイバーセキュリティ対策推進会議等に報告した上で、政府機関等を代表して公表する。

第３部　リスク評価ダッシュボード等

１　リスク評価ダッシュボードの位置付け

リスク評価ダッシュボードは、CISO にリスク評価結果等について報告するとともに、対策導入計画の承認を求める際に用いるため、対策導入計画に照らした進捗状況等を可視化した資料である。

CISO は、リスク評価ダッシュボードにより残存リスク等を把握し、対策導入計画の進捗状況及び次年度以降の計画内容について評価した上で、当該計画の承認の可否について判断する。

NISC は、政府機関等からの報告内容から、政府機関等全体としての対策実施状況や対策導入計画の進捗状況を評価するとともに、対策実施に係る技術的な課題や運用上の課題を把握・分析し、本取組の改善を図る。

２　リスク評価ダッシュボードの記載項目

リスク評価ダッシュボードへの記載項目は、保護対象とする業務領域、対象システム、リスク評価結果及び対策導入計画（案）の概要とする。また、リスク評価ダッシュボードに係る細部的事項については、本ガイドライン付属書に記載する。

３　NISC への報告

NISC への報告資料は、リスク評価ワークシート及びリスク評価ダッシュボード（CISO による方針決定の際に変更が生じた場合は、変更後のもの）とする。

なお、NISC への報告時期については、NISC からの事務連絡文書等を通じて別途連絡する。また、サイバーセキュリティ対策推進会議に加え、府省庁相互の緊密な連携を確保し、カウンターインテリジェンスの強化に向けた施策の総合的かつ効果的な推進を図る場であるカウンターインテリジェンス推進会議においても報告を行うため、当該内容については、内閣情報調査室と共有する。

第４部　本取組の運用管理

１　目的

高度サイバー攻撃は、時間の経過とともに新たな攻撃方法が出現したり、既存の攻撃方法に変化が生じたりすることが想定されることから、高度サイバー攻撃に対する効果的な防御を中長期的に実現していくためには、本取組の運用管理を適切に実施していく必要がある。中でも付属書に掲げる対策セットについては、技術動向や攻撃手法の進歩・変化に応じた継続的な見直しを行うことが特に重要であることから、そのための体制構築その他の必要な事項について、以下に示す。

２　本ガイドライン等の改定

(1)　本ガイドラインの改定

本取組の実施プロセス等に係る見直しの必要が生じた場合には、NISCにおいて内閣情報調査室と連携して検討を行った上で、サイバーセキュリティ対策推進会議において本ガイドラインの改定について決定を行う。

(2)　付属書の改定

対策セットを含む付属書の記載事項に係る見直しの必要が生じた場合には、府省庁の意見を踏まえた上でNISCにおいて改定を行う。

なお、付属書の改定のうち、対策セットの運用管理に係る事項については、３にその詳細を示す。

３　対策セットの運用管理

(1)　対策セットに係る評価検討体制等の構築

新たな攻撃方法の出現や既存の攻撃方法の変化に対応するため、NISCにおいて、政府機関等との情報共有を行い、これらの攻撃を監視・把握するとともに、高度サイバー攻撃対処に係る評価・検討等に関する以下の役割を担うための体制（以下「評価検討委員会」という。）を構築する。また、評価検討委員会は、高度サイバー攻撃に関する学識者委員を中心に構成する。

①　政府機関等が喫緊の課題として対処すべき新たな高度サイバー攻撃手法及び新たな対策に関する情報収集
②　新たな対策の有効性に係る技術的・運用上の見地からの評価
③　既存の対策の見直しに係る検討

(2) 対策セットの見直し

政府機関等が喫緊の課題として対処すべき新たな高度サイバー攻撃手法が把握された場合その他対策セットに係る見直しが必要であると判断された場合には、対策セットの見直しについて検討を行う。

対策セットには、高度サイバー攻撃のシナリオに対応する情報システムの設計、監視強化等に係る対策のうち、評価検討委員会において評価を行い、技術的・運用上の見地から有効であることが確認された新たな対策について、府省庁と協議の上、取り入れる。

資料２－11

情報セキュリティ緊急支援チームの支援対象機関等について

１　概要

サイバー攻撃等により政府機関等の情報システム障害が発生した場合等に、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、情報セキュリティ緊急支援チーム（以下「CYMAT」という。）がNISCに設置されており、その運営等はCISO等連絡会議申合せ事項として決定されている。

CYMATの活動において支援の対象とする機関等（支援対象機関等）には独立行政法人が含まれ、政府機関は、所管する独立行政法人において支援対象事象となりうる事象が発生した場合は、当該独立行政法人の要請を踏まえ、CYMATに事象対策の支援を要請することができるとされている。

今般のサイバーセキュリティ基本法の改正を踏まえ、独立行政法人と同様に、サイバーセキュリティ基本法に定める指定法人において支援対象事象となり得る事象が発生した場合にも、当該法人の要請を踏まえ、所管府省庁がCYMATに事象対策の支援を要請できるよう、申合せを改正したい。

２　申合せ事項の改定（案）

別紙のとおり。

資料２-12

情報セキュリティ緊急支援チームの運営等について　新旧対照表

（下線部分は改定部分）

改定案	現　行
情報セキュリティ緊急支援チームの 運営等について 平成24年6月20日 サイバーセキュリティ対策推進会議 申合せ事項 改正　平成26年9月26日 平成28年8月9日 平成28年10月　日	情報セキュリティ緊急支援チームの 運営等について 平成24年6月20日 サイバーセキュリティ対策推進会議 申合せ事項 改正　平成26年9月26日 平成28年8月9日
１　（略）	１　（略）
２　支援対象機関等	２．支援対象機関等
CYMAT の活動において支援の対象とする機関等（以下「支援対象機関等」という。）は、次に掲げるものとする。	CYMAT の活動において支援の対象とする機関等（以下「支援対象機関等」という。）は、次に掲げるものとする。
ア　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 11 年法律第 89 号）第 49 条第１項若しくは第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項に規定する機関又はこれらに置かれる機関（以下「政府機関」という。）	ア　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 11 年法律第 89 号）第 49 条第 1 項若しくは第 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 項に規定する機関若しくはこれらに置かれる機関（以下「政府機関」という。）
イ　（略）	イ　（略）
ウ　独立行政法人又はサイバーセキュリティ基本法（平成 26 年法律第 104 号）第 13 条に規定する指定法人（以下「独立行政法人等」という。）	ウ　独立行政法人
エ　政府機関、オブザーバー参加機関又は独立行政法人等へクラウドサービスを提供している事業者、政府機関、オブザーバー参加機関又は独立行政法人等へ意図せずにサイバー攻撃を行っている電子計	エ　支援対象機関等へクラウドサービスを提供している事業者、非意図的に支援対象機関等へサイバー攻撃を行っている電子計算機を管理している事業者など、１０．（１）又は（２）に基づき要請さ

算機を管理している事業者その他の政府機関、オブザーバー参加機関又は独立行政法人等の情報システムに関係するもののうち、10(1)又は(2)に基づき要請された事象に直接関係するものであって、CYMAT による支援を行う必要があるものと当該要請を行った機関等が認めたもの（以下「直接関係者」という。）	れた事象に直接関係するものであって、CYMAT による支援を行う必要があるものと当該要請を行った機関等が認めたもの（以下「直接関係者」という。）
３～９　（略）	３～９　（略）
10　支援要請	１０．支援要請
(1)　（略）	（１）　（略）
(2)　政府機関は、所管する独立行政法人等において支援対象事象となりうる事象が発生した場合は、当該独立行政法人等の要請を踏まえ、CYMAT に事象対策の支援を要請することができる。	（２）政府機関は、所管する独立行政法人において支援対象事象となりうる事象が発生した場合は、当該独立行政法人の要請を踏まえ、CYMAT に事象対策の支援を要請することができる。
(3)～(4)　（略）	（３）～（４）　（略）
11　出動	１１．出動
(1)（略）	（１）　（略）
(2)　統括責任者は、支援要請を受ける前であっても、政府機関において支援対象事象が発生していると認めた場合には、CYMAT の出動について、当該政府機関の組織内 CSIRT の合意を得た上で、CYMAT に対し、出動を命ずることができる。	（２）統括責任者は、支援要請を受ける前であっても、政府機関において支援対象事象が発生していると認めた場合には、CYMAT の出動について、当該政府機関の組織内 CSIRT（組織内 CSIRT が設置されていない場合は、該当システムに関連する部署とする。）の合意を得た上で、CYMAT に対し、出動を命ずることができる。
(3)　統括責任者は、支援要請を受ける前であっても、オブザーバー参加機関において支援対象事象が発生していると認めた場合には、CYMAT の出動の必要性について、当該オブザーバー参加機関に対し打診をすることができる。統括責任者は、当該オブザーバー機関の要請を受けた上で、	（新規）

CYMAT に対し、出動を命ずることができる。	
(4)　統括責任者は、支援要請を受ける前であっても、独立行政法人等において支援対象事象が発生していると認めた場合には、CYMAT の出動について、所管府省庁における当該事象に対応する部署の合意を得た上で、CYMAT に対し、出動を命ずることができる。その際、所管府省庁は、当該独立行政法人等の合意を得ることとする。	（新規）
12～18　（略）	１２～１８　（略）
附則 本申合せに基づく運用は、平成 28 年 10 月　日から実施する。	附則 本申合せに基づく運用は、平成 28 年 8 月 9 日から実施する。

資料２－13

情報セキュリティ緊急支援チームの運営等について

平成２４年６月２０日
サイバーセキュリティ対策推進会議
申合せ事項

改正　平成 26 年 9 月 26 日
平成 28 年 8 月 9 日
平成 28 年 10 月　日

1　目的

サイバー攻撃等により政府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（以下「NISC」という。）に設置される情報セキュリティ緊急支援チーム（Cyber　Incident Mobile　Assistance Team、以下「CYMAT」という。）の運営等について、以下の事項を申し合わせる。

2　支援対象機関等

CYMAT の活動において支援の対象とする機関等（以下「支援対象機関等」という。）は、次に掲げるものとする。

ア　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 11 年法律第 89 号）第 49 条第１項若しくは第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項に規定する機関又はこれらに置かれる機関（以下「政府機関」という。）

イ　サイバーセキュリティ対策推進会議オブザーバー参加機関（以下「オブザーバー参加機関」という。）

ウ　独立行政法人又はサイバーセキュリティ基本法（平成 26 年法律第 104 号）第 13 条に規定する指定法人（以下「独立行政法人等」という。）

エ　政府機関、オブザーバー参加機関又は独立行政法人等へクラウドサービスを提供している事業者、政府機関、オブザーバー参加機関又は独立行政法人等へ意図せずにサイバー攻撃を行っている電子計算機を管理している事業者その他の政府機関、オブザーバー参加機関又は独立行政法人等の情報システムに関係するもののうち、10(1)又は(2)に基づき要請された事象に直接関係するものであって、CYMAT による支援を行う必要があるものと当該要請を行った機関等が認めたもの（以下「直接関係者」という。）

3　支援対象事象

CYMAT の活動において支援の対象とする事象は、サイバー攻撃等により支援対象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（以下「支援対象事象」という。）とする。

4　統括

(1)　政府 CISO である NISC センター長（以下「統括責任者」という。）は、CYMAT の運用に関する事務を統括する。

(2)　NISC 副センター長（以下「統括副責任者」という。）は、必要に応じ、統括責任者を補佐する。また、統括責任者と連絡がとれず、かつ、急を要する場合は、統括副責任者が統括責任者の職務を行う。

5　構成

(1)　CYMAT は、管理責任者、現場責任者、要員をもって構成する。

(2)　管理責任者は、命を受けて、CYMAT の運用に関する事務を掌理する。

(3)　現場責任者は、命を受けて、CYMAT の運用に関する事務を整理する。

(4)　要員は、命を受けて、CYMAT の活動にあたる。

(5)　管理責任者、現場責任者及び要員には、常時勤務に服することを要する国家公務員を充てる。

6　構成員の指名

(1)　管理責任者は、NISC に常駐する参事官のうちから、統括責任者が指名する。

(2)　現場責任者は、NISC に常駐する者のうちから、２名程度を統括責任者が指名する。

(3)　要員は、政府機関から要員候補者として推薦のあった者及び NISC に常駐する者のうちから、統括責任者が指名する。政府機関から推薦を受けて統括責任者が指名する要員は、内閣事務官（内閣官房内閣サイバーセキュリティセンター）に併任又は兼官とした上で、NISC の非常駐職員とし、本務に大きな支障が生じない範囲で CYMAT の活動にあたる。なお、管理責任者は、緊急の場合、NISC に常駐する者を CYMAT の活動に参画させることができる。

7　研修員

(1)　政府機関及びオブザーバー参加機関は、事象対策（事象の正確な把握、被害拡大防止、復旧、原因調査及び再発防止をいう。以下同じ。）に関する能力の向上又は要員候補者の育成等のため、CYMAT の活動として実施される研修又は訓練に参加させる者（政府機関又はオブザーバー参加機関において、常時勤務に服することを要する者に限る。）を、研修員として NISC に登録することができる。なお、政府機関が研修員を登録することができる期間は、当分の間とする。

(2)　政府機関及びオブザーバー参加機関は、CYMAT に対し、当該機関が登録した研修員の研修又は訓練への参加を申し出ることができる。この場合、研修及び訓練に必要な経費の負担は、研修員を登録した当該機関に求める。

8　要員候補者の推薦数等

(1)　各政府機関から NISC へ要員候補者として推薦する者の数は６名を上限とし、原則として１名以上とする。

(2)　当分の間、要員候補者を推薦することが困難な政府機関は、少なくとも１名を研修員として登録する。なお、研修員として登録する者の数と要員候補者として推薦する者の

数の合計は、各政府機関で６名以下とする。ただし、そのうち研修員として登録する者の数は４名以下とする。

(3)　各オブザーバー参加機関が研修員として登録する者の数は、４名以下とする。

9　要員及び研修員の変更

(1)　政府機関は、要員の変更を求める場合においては、可能な限り速やかに、NISC へ新たな要員候補者を推薦する。

(2)　政府機関及びオブザーバー参加機関は、研修員を変更する場合においては、可能な限り速やかに、NISC へ新たな研修員を登録する。

10　支援要請

(1)　支援対象事象となりうる事象が発生した政府機関及びオブザーバー参加機関は、CYMAT に事象対策の支援を要請することができる。

(2)　政府機関は、所管する独立行政法人等において支援対象事象となりうる事象が発生した場合は、当該独立行政法人等の要請を踏まえ、CYMAT に事象対策の支援を要請することができる。

(3)　10 (1)又は(2)に基づく要請を行った政府機関及びオブザーバー参加機関は、直接関係者において支援対象事象となりうる事象が発生した場合は、当該直接関係者の要請を踏まえ、CYMAT に事象対策の支援を要請することができる。

(4)　10(1)から(3)に基づく政府機関及びオブザーバー参加機関の要請は、当該機関の最高情報セキュリティ責任者から統括責任者に対して行うことを原則とする。なお、緊急時には、当該機関の組織内 CSIRT （組織内 CSIRT が設置されていない場合は、該当システムに関連する部署とする。）又は要員から管理責任者又は現場責任者に対して要請することも可能とする。

11　出動

(1)　統括責任者は、10(1)から(3)に基づく要請を受けた事象が、支援対象事象であると認めた場合には、CYMAT に対し、出動を命ずる。

(2)　統括責任者は、支援要請を受ける前であっても、政府機関において支援対象事象が発生していると認めた場合には、CYMAT の出動について、当該政府機関の組織内 CSIRT の合意を得た上で、CYMAT に対し、出動を命ずることができる。

(3)　統括責任者は、支援要請を受ける前であっても、オブザーバー参加機関において支援対象事象が発生していると認めた場合には、CYMAT の出動の必要性について、当該オブザーバー参加機関に対し打診をすることができる。統括責任者は、当該オブザーバー機関の要請を受けた上で、CYMAT に対し、出動を命ずることができる。

(4)　統括責任者は、支援要請を受ける前であっても、独立行政法人等において支援対象事象が発生していると認めた場合には、CYMAT の出動について、所管府省庁において当該事象に対応する部署から合意を得た上で、CYMAT に対し、出動を命ずることができる。その際、所管府省庁は、当該独立行政法人等の合意を得ることとする。

12　活動内容

(1)　出動を命じられた場合、CYMAT は、出動を命じられて支援を行っている支援対象機関等（以下、「事象発生機関等」という。）と情報を共有し、次の活動（以下「支援活動」という。）を行う。

ア　事象の正確な把握（発生事象に関連する情報の収集、分析及び被害拡大の予測等）

イ　被害拡大防止、復旧、原因調査及び再発防止のための技術的な支援及び助言（事象発生機関等以外の支援対象機関等の類似事象に関する、被害拡大防止、復旧、原因調査又は発生防止のため、事象発生機関等以外の支援対象機関等に対する支援及び助言を行うことを含む）

ウ　その他統括責任者の特命に関すること

(2)　CYMAT は、事象発生時に効果的な活動を行うため、平常時において、次の活動を行う。

ア　連絡体制の構築

イ　予兆の認知及び事象発生時における効果的な支援活動の実施に向けて必要な情報セキュリティに関する情報の調査、収集及び分析

ウ　活動に必要な技能を習得するための研修及び訓練

エ　習得した技能を政府機関及びオブザーバー参加機関と共有し、これらの機関における職員の事象対策能力の向上を図るための取組

オ　その他統括責任者の特命に関すること

(3)　管理責任者は、要員の本務に大きな支障が生じない範囲で CYMAT の活動に従事させるよう配慮する。

(4)　管理責任者は、要員がおおよそ 40 名程度になることを想定し、12(1)及び(2)の活動のための準備を行うよう配慮する。

13　被害状況の報告

(1)　CYMAT が出動した場合、事象発生機関等は、随時、CYMAT に被害状況を報告する。

(2)　13 (1)に基づく被害状況の報告（以下「被害状況報告」という。）を、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）及びサイバー攻撃に係る情報収集・集約担当に対する報告・連絡（以下「GSOC への報告等」という。）として NISC が取り扱うことに支援対象機関等が同意する場合、当該支援対象機関等は、被害状況報告に記載した内容について、GSOC への報告等を行うことを省略することができる。

(3)　大規模サイバー攻撃等を始めとする緊急事態（その可能性のある事態を含む。）においては、事象発生機関等は、「緊急事態に対する政府の初動対処体制について」（平成 15 年 11 月 21 日閣議決定）等に基づく報告等も行う。

14　支援活動終了

支援活動の終了については、事象発生機関等における最高情報セキュリティ責任者等の意見を踏まえ、統括責任者が決定する。

15　情報の取扱い

CYMAT がその活動により得た支援対象機関等の情報システム障害等に関する情報は、

支援対象機関等が行う機密性格付けに従い、「政府機関の情報セキュリティ対策のための統一基準」で定める機密性２情報及び機密性３情報に相当するものについては、当該支援対象機関等における事象の正確な把握、被害拡大防止、復旧、原因調査及び再発防止のための技術的な支援及び助言に限って活用する。ただし、情報を提供した支援対象機関等と事前に協議し、同意を得た場合には、次の目的に活用することができる。

ア　情報を提供した支援対象機関等以外の支援対象機関等における事象の正確な把握、被害拡大防止、復旧、原因調査及び再発防止のための技術的な支援及び助言

イ　12(2)アからエに定める活動

ウ　その他統括責任者が必要と認めた目的

16　サイバーセキュリティ対策推進会議への報告

CYMAT の活動状況については、定期的に、統括責任者からサイバーセキュリティ対策推進会議に報告し、その要旨を公表する。

17　支援対象機関等の協力等

(1)　支援対象機関等は、その任務に大きな支障のない範囲で、可能な限り CYMAT の活動に協力する。

(2)　CYMAT の支援を受けている支援対象機関等における要員及び研修員は、その任務に大きな支障のない範囲で、可能な限り CYMAT へ情報を提供するよう努める。

(3)　支援対象機関等は、CYMAT が行う技術的な支援及び助言に基づく措置を行う場合には、各支援対象機関等が必要と判断した範囲で実施する。

18　その他

CYMAT の設置及び運営等に関する規程は、統括責任者が定める。

附則

本申合せに基づく運用は、平成 28 年 10 月　日から実施する。