情報セキュリティ報告書専門委員会報告書

～政府機関の能動的な情報セキュリティ対策のために～

2009 年 9 月 11 日

情報セキュリティ政策会議

情報セキュリティ報告書専門委員会

目　次

はじめに

情報セキュリティ政策会議は、これまでの政府機関の情報セキュリティ対策への取り組みについて、実施状況などを数次にわたり精査し、その結果を公表し、政府機関の取り組みを促してきた。その結果、政府機関の情報セキュリティ対策の底上げについてはおおむね達成しつつあると言えよう。

政策会議は、これらの成果をふまえ、本年２月に第二次情報セキュリティ基本計画を策定した。同計画において政府機関は２０１２年までに情報セキュリティガバナンスの確立に向けた組織・体制の強化を図ることとしている。この取り組みが効果を上げるには、各政府機関において、最高情報セキュリティ責任者（CISO）を中心に広範で平明かつ客観的な現状分析を主体的に行うことが必要となる。その結果を情報セキュリティ報告書としてCISOが広く国民に示していくことによって、自律的な情報セキュリティ対策が運用されると考える。

情報セキュリティ報告書とは、情報セキュリティガバナンス確立の一環として、組織の情報セキュリティの取組み、中でも社会的関心の高いものについて、情報開示することにより、当該組織の取組みが利害関係者や広く国民から適正に評価されることを目指すものである。

そもそも、情報セキュリティへの取り組みには、さまざまな対策を包括した体系的な取り組みが求められるがその実態は組織外からはとてもわかりにくいこと(複雑性)、ひとたび事件や事故が起きるとその影響が広範囲に及ぶ深刻な事態につながりかねないこと(重大性)、さらには、事件や事故につながるような引き金になる事象を引き起こした人とその結果影響を受ける人との間に大きな隔たりがあること(遠隔性)、などに大きな特徴がある。このような特徴もまた、情報セキュリティ報告書が求められる理由となっている。

セキュリティ立国の思想に基づいて、我が国政府が目指す電子政府を実現するには、そこで確立すべき情報セキュリティの取り組みは、日本国の特性を生かしたやり方で世界の模範となるようなものでならなければならないと同時に、このような政府の取り組みが主権者たる国民にとって理解できる形で示されその成果が確認できるような報告の枠組みもまた求められることになる。

当専門委員会は、各府省において自主的に作成される報告書の水準を政府として担保するため、政策会議により設置された。これまで四回の委員会において情報セキュリティ報告書（正確には「政府機関の情報セキュリティに係る年次報告書」という。）作成のためのガイドラインの策定、ならびに情報セキュリティ報告書の定量的評価等の手法等に係る事項について調査検討を行ってきた。

本報告書は、次の 2 部構成になっている。

第1部　情報セキュリティ報告書作成のためのガイドライン

第2部　政府機関における評価等の考え方

第 1 部は上述の情報セキュリティ報告書作成のための府省庁向けのガイドラインであり、第 2 部は､各府省庁の情報セキュリティ報告書並びにその作成のための基礎資料などから、政府全体の評価を行う手法を示している。

また、自律的な取り組みを各政府機関に求めるばかりでなく、本専門委員会報告書における情報セキュリティ報告書作成方法及び評価手法等自体も PDCA サイクルの中で常に磨かれ、改善されていく必要があり、その点についても第 2 部の中で言及している。

本専門委員会報告書が政府の情報セキュリティ対策を進化させる指針として活用され、複雑性、重大性、そして遠隔性に象徴される難しさを克服し、電子政府に向けた取り組みが健全に発展することを念願するとともに、政府の取り組みが民間産業界の取り組みのモデルとしても機能することを期待したい。

これらを通じて、我が国全体の情報セキュリティ対策の向上に寄与することを願ってやまない。

2009 年 9 月 11 日

情報セキュリティ報告書専門委員会委員長

大木榮二郎

Ⅰ　本書の構成

本書の本文は、以下の構成となっている。

１　第１部　情報セキュリティ報告書作成のためのガイドライン

各府省庁の情報セキュリティ報告書の記載内容のバランスを確保することなどを目的として、情報セキュリティ報告書に記載すべき事項、記載に当たっての留意事項等について指針を示している。

２　第２部　政府機関における評価等の考え方

各府省庁の情報セキュリティ対策の一層の充実・向上を図ることなどを目的として、各府省庁の情報セキュリティ対策の実施状況に係る定量的評価の手法等について記載している。

上記の関係を図１に示す。

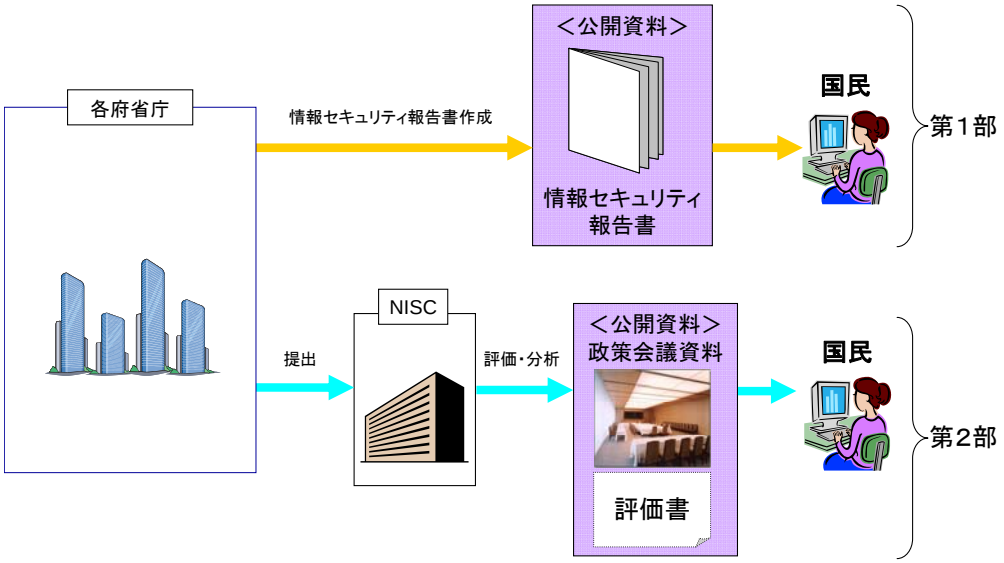


図１　本書の構成

Ⅱ　情報セキュリティ報告書の作成から評価結果の公表までの全体プロセス

各府省庁は、「第１部　情報セキュリティ報告書作成のためのガイドライン」に基づき、当該年度の情報セキュリティ報告書（案）を作成し、翌年度４月の最高情報セキュリティアドバイザー連絡会議（仮称）に報告し、助言等を受け見直した後、情報セキュリティ委員会において情報セキュリティ報告書を決定し、最高情報セキュリティ責任者が、情報セキュリティ対策推進会議等に報告の上、５月末までに公表する。

内閣官房情報セキュリティセンター（National Information Security Center。以下「NISC」という。）は、「第２部　政府機関における評価等の考え方」に基づき、各府省庁から入手した評価等に必要な資料（報告対象年度の３月末までに入手）及び情報セキュリティ報告書の内容を分析し、各府省庁及び政府機関全体の情報セキュリティ対策の実施状況に係る評価等を行う。なお、評価項目等については、報告対象年度の６月末までに各府省庁に通知する。

評価結果については、翌年度 6 月に予定される情報セキュリティ政策会議に報告し、公表する。

なお、情報セキュリティ報告書作成のためのガイドライン、政府機関における評価等の考え方及びそれらに係る全体プロセスについては、政府機関全体における情報セキュリティ対策の浸透・定着、技術や環境の変化等を踏まえ、必要に応じて、NISC において見直すものとする。

以上の関係を図２、図３に示す。

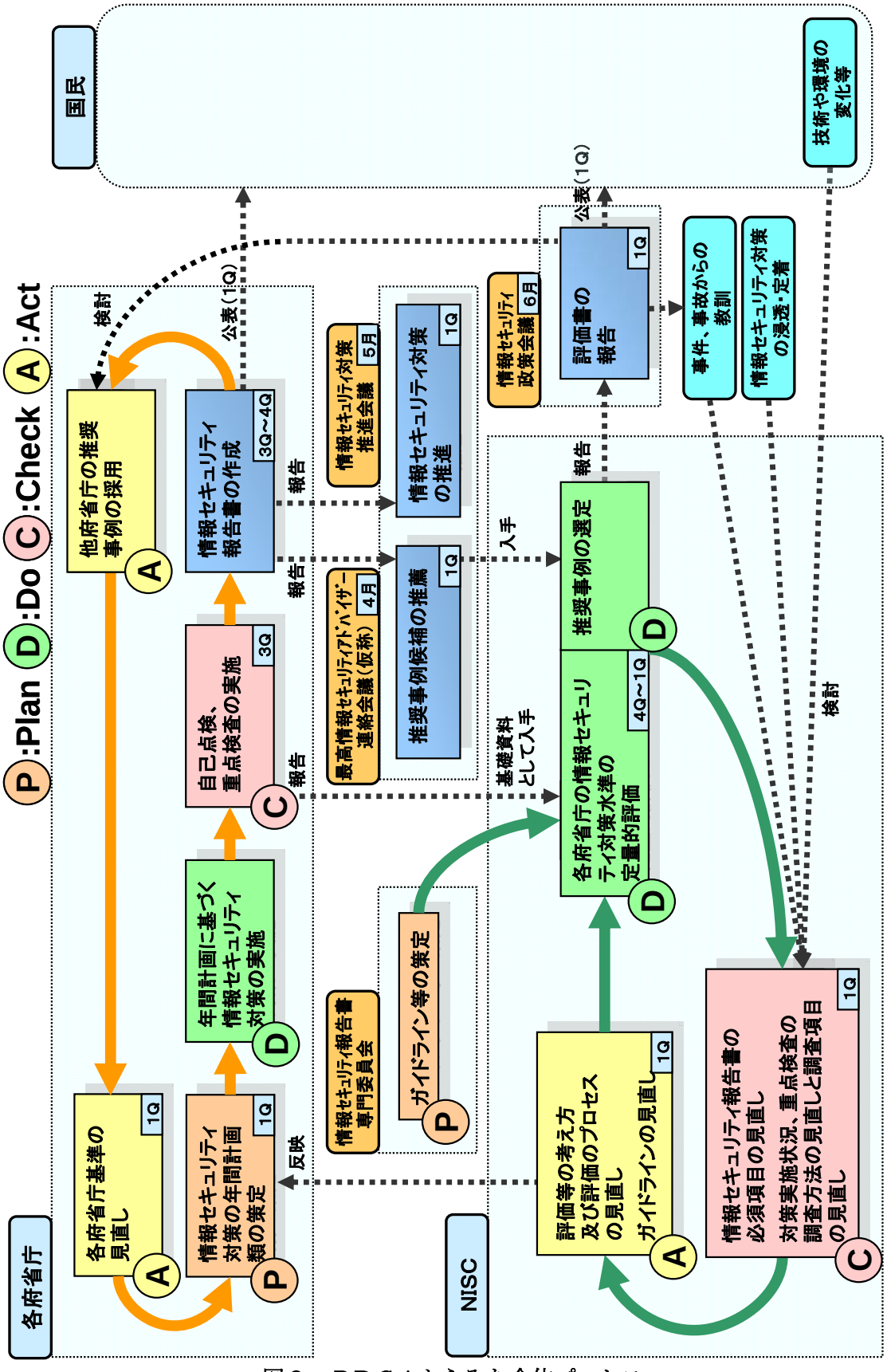


図２　ＰＤＣＡからみた全体プロセス

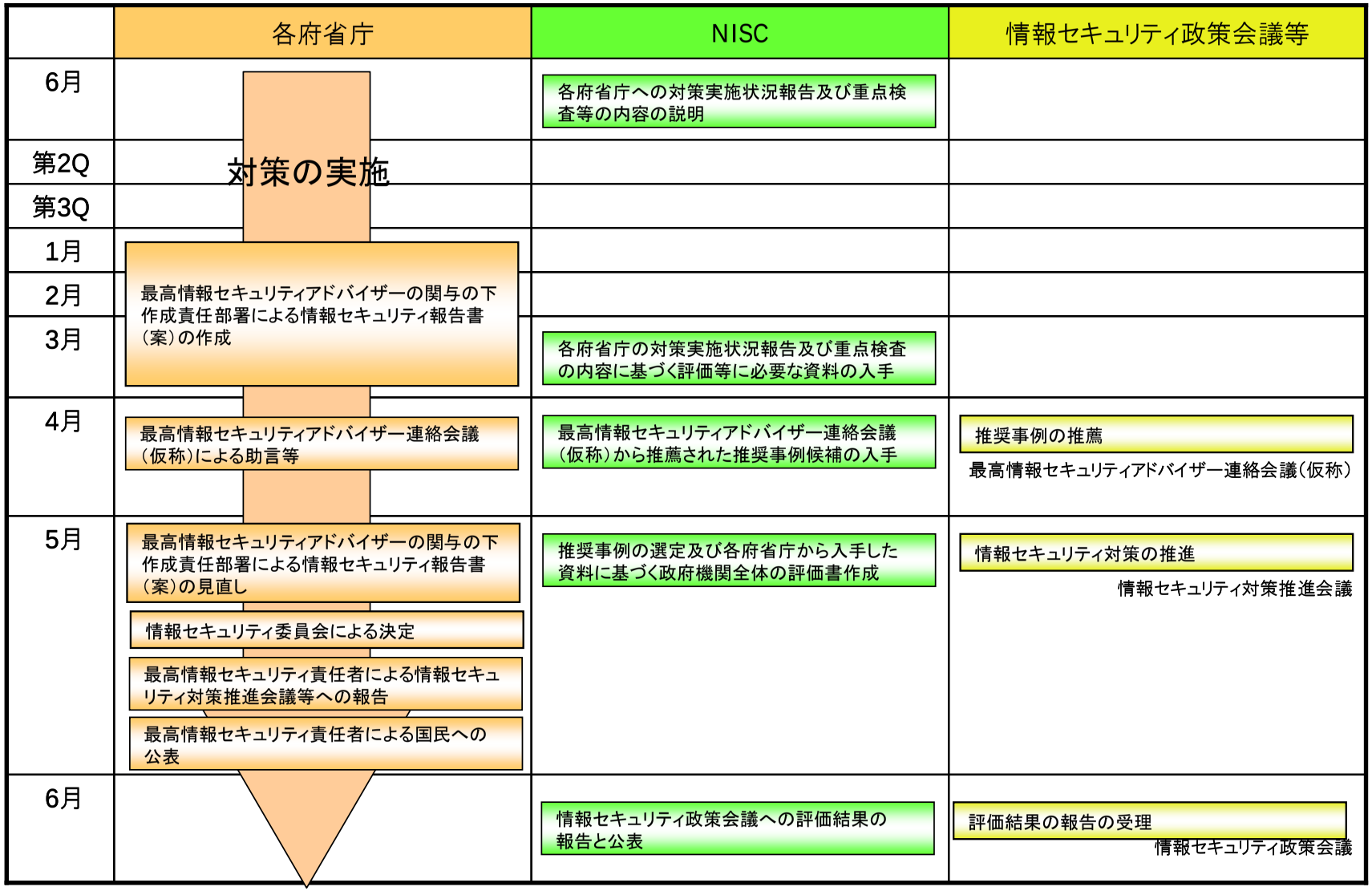


図３　全体プロセスのタイムスケジュール

第１部　情報セキュリティ報告書作成のためのガイドライン

Ⅰ　目的

政府機関においては、第１次情報セキュリティ基本計画の下、すべての政府機関において、政府機関の情報セキュリティ対策のための統一基準（以下、「政府機関統一基準」という。）が求める水準の対策を実施していること等を目指して、各府省庁の PDCA サイクル及び情報セキュリティ政策会議による評価・勧告を中心とした政府機関全体の PDCA サイクルという 2 階層の PDCA サイクルを構築し、情報セキュリティ対策を促進するため様々な取組を推進してきた。第 2 次情報セキュリティ基本計画においては、この取組を定着、浸透させ、すべての府省庁が能動的に情報セキュリティ対策に取り組む体制の確立を目指し、各府省庁が情報セキュリティ報告書を作成し、公表することとしている。

情報セキュリティ報告書の作成及び公表は、各府省庁における情報セキュリティ対策の取組状況等について明らかにし、国民への説明責任を果たすことにより、行政事務全般について国民からの信頼を向上させることを目的とする。また、情報セキュリティ報告書を作成する過程において、各府省庁が改めて自らの情報セキュリティ対策について見直しを行い、更なる向上が図られる効果を期待する。

第１部においては、各府省庁の情報セキュリティ報告書の記載内容のバランスを確保する観点から、各府省庁が情報セキュリティ報告書を作成するためのガイドラインとして、情報セキュリティ報告書の作成から公表までの手順、情報セキュリティ報告書への記載事項の具体的項目等を示している。

なお、本ガイドラインに示す、情報セキュリティ報告書の作成から公表までの手順及び記載事項の具体的項目については、政府機関全体における情報セキュリティ対策の浸透・定着、技術や環境の変化等を踏まえ、必要に応じて、NISC において見直すものとする。

Ⅱ　情報セキュリティ報告書の作成から公表までの手順

各府省庁の情報セキュリティ報告書作成責任部署は、最高情報セキュリティアドバイザーの積極的な関与の下、情報セキュリティ報告書（案）を作成する。

作成した情報セキュリティ報告書（案）は、最高情報セキュリティアドバイザー連絡会議（仮称）において比較・評価等を行い、同会議からの助言等を踏まえ、内容の見直しを行う。

内容の見直し後、情報セキュリティ委員会において情報セキュリティ報告書を決定し、最高情報セキュリティ責任者が、情報セキュリティ対策推進会議等に報告した後、公表する。

Ⅲ　情報セキュリティ報告書の構成のひな形

情報セキュリティ報告書の記載事項の具体的項目を以下、構成のひな形として列挙する。各パートは、基本的に、「項目名」、「目的」、「記載内容（必須項目・任意項目）」及び「留意事項」で構成される。

必須項目は、各府省庁が情報セキュリティ報告書を作成するに当たり、その内容を記載することが必須の事項である。

任意項目は、各府省庁が情報セキュリティ報告書を作成するに当たり、その内容を記載することが任意の事項である。

なお、情報セキュリティ報告書の作成に当たっては、以下の共通的な留意事項を参考とすること。

- 情報セキュリティ報告書の作成に当たり、項目名又は記載順番の変更を行うことや、複数の項目をまとめて記載することは差し支えない。
- 必須項目及び任意項目にかかわらず、各府省庁において実施した独自の情報セキュリティ対策については、積極的に記載することが望ましい。
- 国民に向けて公表することにかんがみ、国民が分かりやすい記述及び構成とするように努めること。
- セキュリティ脆弱性についての類推が可能となるような内容（例えばIPアドレス）や特定の製品名等については、情報セキュリティの維持・確保の観点から、記載しないよう注意すること。
- 第三者組織を利用した監査等を実施した場合は、その結果を情報セキュリティ報告書の作成に積極的に活用することが望ましい。

1　最高情報セキュリティ責任者によるメッセージ及び当該年度の総括

1．1　最高情報セキュリティ責任者からのメッセージ

（目的）

各府省庁の情報セキュリティ対策の最高責任者である最高情報セキュリティ責任者から、当該府省庁における情報セキュリティ対策の取組、考え方等について、国民に対してメッセージを発信することにより、情報セキュリティ対策に関する当該府省庁の姿勢を明らかにすることを目的とする。

（記載内容）

【必須項目】

⑴最高情報セキュリティ責任者からのメッセージ

当該府省庁における情報セキュリティ対策の取組、考え方等について、最高情報セキュリティ責任者から国民へのメッセージを記載する。

⑵最高情報セキュリティ責任者名等

最高情報セキュリティ責任者の役職及び氏名を記載する。

⑶メッセージ発出年月

メッセージ発出年月を記載する。

（留意事項）

情報セキュリティ報告書は、国民に対する説明責任を果たす観点から作成することにかんがみ、一般論のみではなく、時勢を踏まえた記述を加えることが望ましい。また、最高情報セキュリティ責任者が自らメッセージを発信していることを強調するために責任者の写真を掲載すること等も考えられる。

１．２　当該年度の総括

（目的）

各府省庁における当該年度の情報セキュリティ対策を総括することを目的とする。

（記載内容）

【必須項目】

⑴当該年度の評価

当該年度の情報セキュリティ対策について、最高情報セキュリティ責任者による自己評価を記載する。

⑵翌年度の目標

翌年度重点的に取り組むべき目標を記載する。

（留意事項）

情報セキュリティ報告書に記載する以下の事項を踏まえ、最高情報セキュリティ責任者自らが評価した結果についての総括を記載すること。なお、本文と重複した内容が多くならないように、内容を引用する場合は簡潔に記載すること。

- 当該年度の重点事項
- 省庁対策基準に関する自己点検結果
- 情報システムごとの状況
- 教育・啓発
- 調達・外部委託
- その他取り組んだ事項
- 情報セキュリティに関する障害・事故等の報告

２　報告の基本情報

（目的）

情報セキュリティ報告書が対象とする期間、組織等について明記することにより、説明範囲を明らかにすることを目的とする。

（記載内容）

【必須項目】

⑴府省庁の概要

所掌事務、導入している主な情報システムなどについて、府省庁の業務の

全体像が分かるように、概要を簡潔に記載すること。

⑵対象とする期間

情報セキュリティ報告書の対象とする期間は原則として年度（4 月 1 日～3 月 31 日）とし、前年度との間で間隙が無いようにすること。ただし、関連する事項があればその前後の期間の事項を含めることも可能とする。

⑶対象とする組織

情報セキュリティ報告書の対象とする組織について簡潔に記載する。地方支分部局等も含めた全組織とすることが望ましいが、対象としない組織がある場合は、明確に記載する。なお、所管する独立行政法人等については、報告の対象外とする。

⑷対象とする情報

情報セキュリティ報告書の対象とする情報を記載する。ただし、政府機関統一基準で対象とする情報（情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。）は必須とするが、その他の情報については、必要に応じて記載すること。

⑸責任部署

情報セキュリティ報告書の責任部署名又は連絡先となる部署を明記する。担当となる係名まで記載することが望ましい。

【任意項目】

⑹府省庁の行政事務従事者数又は定員数

情報セキュリティ報告書の対象となる行政事務従事者数又は定員数を記載する。対象外となる者がいる場合は、その理由、人数等を記載する。

⑺ 情報システム予算額

府省庁の情報システム予算総額を記載する。

（留意事項）

図表などを用いて分かりやすく表現する工夫をすること。

3　情報セキュリティ対策の枠組み

（目的）

各府省庁の情報セキュリティ対策の体制等､情報セキュリティ対策に係る府省庁全体の枠組みが整備されていることを明らかにすることを目的とする。

（記載内容）

【必須項目】

⑴情報セキュリティ対策に関する文書体系

府省庁にて定めている情報セキュリティ対策に関する文書（基本方針、省庁対策基準、規程類等）の概要及びそれらの文書の対応関係を記載する。府

省庁の情報セキュリティ対策の枠組みの中で各文書がどのような位置付けにあるかを明記する。

⑵情報セキュリティ対策の推進体制

府省庁における情報セキュリティ対策の推進体制を記載する。府省庁の情報セキュリティ対策の枠組みの中で各責任者及び推進部署がどのような位置付けにあるかを明記する。

なお、情報セキュリティ対策に係る組織体制や推進部署の体制については、以下の事項を参考に、記載する。

・ 情報セキュリティ対策に係る組織体制

最高情報セキュリティ責任者、情報セキュリティ委員会、情報セキュリティ監査責任者、情報セキュリティ責任者、情報システムセキュリティ責任者、情報システムセキュリティ管理者、課室情報セキュリティ責任者、最高情報セキュリティアドバイザーなど、省庁対策基準に定める情報セキュリティ対策に係る組織体制について、その整備状況、意志決定の枠組み、役割、活動状況等を記載する。

地方支分部局等が設置されている府省庁においては、地方支分部局等における情報セキュリティ対策に係る組織体制も記載する。

また、府省庁内横断的な連絡会議等の情報セキュリティ対策に係る会議体の体制、役割（例えば、幹部への報告とその後の対応、環境変化に対する対応といった役割等）、活動状況等を記載する。

・ 情報セキュリティ対策に係る推進部署の体制

IT 部門及び情報セキュリティ対策に係る総合調整を行う具体的な推進部署名と体制、役割、活動状況等を記載する。また、推進部署の担当者の数、業務平均経験年数等を記載する。

⑶監査等

監査等について、以下の事項を参考に、実施している内容を記載する。

・ 情報セキュリティ監査計画の策定、監査報告の実施

当該年度の情報セキュリティ監査計画の概要について記載する。監査計画は、過去に実施した監査結果で明らかになった課題及び問題点を踏まえたものとなっていることが望ましい。

また、当該年度の監査報告の実施状況等（最高情報セキュリティ責任者への説明、報告等）を記載する。

・ 監査報告書に基づく対応の実施

監査報告書の内容を踏まえ、改善のための以下 a～e のような取組状況等を記載する。

a. 指摘事項に対する、最高情報セキュリティ責任者による対応実施の指示

b. 同種の課題及び問題点の有無について、最高情報セキュリティ責任者による確認の指示

c. 改善を指示された事項について、情報セキュリティ責任者による対応計画（達成可能な対応目標の設定を含む。）の作成と報告

d. 情報セキュリティに関する文書について、情報セキュリティ責任者による妥当性評価及び必要に応じた見直しの指示

e. 上記 a～d の見直し指示等に基づき、どのように対応したか

・ 第三者組織による監査・検査等

a. 監査について、客観性及び専門性をより向上するために第三者組織を利用した場合は、内部監査との関係を含めて記載する。

b. 情報システム脆弱性検査

情報システムに対する脆弱性検査を実施した場合は、第三者組織の利用の有無、検査対象、結果等を記載する。

【任意項目】

⑷情報セキュリティ対策の予算額

情報セキュリティ対策の予算として執行した総額、情報システム予算額に占める割合等を記載する。

⑸政府機関統一基準と省庁対策基準の差異

省庁対策基準において、政府機関統一基準に特に加えて基準としている事項等、差異として特徴的なものがある場合は、記載する。

⑹業務・システム最適化における取組の管理

各府省庁の PMO（プログラム・マネジメント・オフィス）において、業務・システム最適化の中で、情報システムの安全性・信頼性を確保するための取組を、どのように管理しているか（例えば、業務・システム最適化の企画、設計・開発段階における情報セキュリティ対策要領の作成、情報セキュリティ要件定義の作成等の管理）を記載する。

⑺情報資産台帳の整備と活用

各府省庁の PMO において、情報資産台帳を整備し、どのように活用しているかを記載する。

⑻ 情報セキュリティ対策に関する文書の見直し状況

情報セキュリティ対策に関する文書の見直しの検討状況、改訂の実施状況等を記載する。

⑼業務継続計画の策定

保有する情報システムにおける、災害・障害発生時に備えた業務継続計画の策定状況を記載する。

（留意事項）

頻繁な変更が想定される事項ではないが、変更があった場合には、その点を明

確に記載する。図表などを用いて分かりやすく表現する工夫をすること。

4　当該年度の重点事項

（目的）

府省庁において年度当初に当該年度の情報セキュリティ対策の重点的な取組として定めた事項の目標、実績及び評価を明らかにすることを目的とする。

（記載内容）

【必須項目】

⑴重点事項の目標、実績及び評価

前年度の情報セキュリティ報告書で課題とした事項に加えて、当該年度当初に新たに重点的な取組と定めた事項について、測定方法と成否判断基準を含めて目標、実績及び評価を記載する。

⑵障害・事故等の再発防止状況

前年度の情報セキュリティ報告書で報告し､対策を実施している情報セキュリティに関する障害・事故等の再発防止策の取組状況を記載する。

【任意項目】

⑶年度途中に発生した重点事項

当該年度当初には重点事項としなかったが、途中で重点的に取り組むこととした事項について、理由等も含めて目標、実績及び評価を記載する。

（留意事項）

後述の「５　情報セキュリティ対策の実施状況」の記載内容と重複しないことが望ましい。

5　情報セキュリティ対策の実施状況

5．1　省庁対策基準に関する自己点検結果

（目的）

すべての行政事務従事者が省庁対策基準に準拠した運用を行っているか否かを自ら点検した結果を、府省庁において集計及び分析し報告することにより、省庁対策基準に対する準拠の全体像を明らかにすることを目的とする。

（記載内容）

【必須項目】

⑴課題と対策

前回調査時に判明した課題とその改善対策を記載する。

⑵自己点検結果の状況

(a) 府省庁全体の把握率

各府省庁が報告対象とした者のうち、対策実施状況が把握できた者の割合を主体者別に記載する。

(b) 府省庁全体の実施率

把握した者のうち、責務が生じた者に占める対策を実施した者の割合を主体者別に記載する。

(c) 府省庁全体の到達率

把握した者のうち、責務が生じた一定の割合（100%、95%、90%）以上の者が対策を実施した遵守事項の割合を主体者別に記載する。

(3)総評

自己点検結果について分析を行い、課題の改善状況、次年度に向けた課題、全体としての傾向等を記載する。

【任意項目】

(4)特筆すべき事項

自己点検結果について特徴的な事項がある場合は記載する。

(5)特定テーマの実施率及び到達率

自府省庁として特に重要と考えている事項など特定テーマに絞って実施率、到達率、分析結果等を記載する。

(6)自己点検の計画策定、結果に基づく改善指示等の状況

当該年度の自己点検計画の概要を記載する。また、自己点検結果に基づく改善指示等の状況を記載する。

（留意事項）

原則として、【必須項目】の範囲は、省庁対策基準の全基本遵守事項とする。

自己点検において府省庁全体の把握率の母数は、回収時の全行政事務従事者とする。ただし、休職等により把握できない者を除く。

自己点検結果は、府省庁において監査を実施した後の結果を記載することにより回答の信頼性を担保する。

５．２　情報システムごとの状況

（目的）

情報セキュリティ対策が不十分な場合、情報の漏えい、改ざん、破壊等の要因となり、府省庁の業務や利用する国民・職員に特に重大な影響を及ぼす情報システムについて、対策の実施状況を明らかにすることを目的とする。

（記載内容）

【必須項目】

(1)課題と対策

前回調査時に判明した当該システムにおける情報セキュリティ対策の課題とその改善対策を記載する。

(2)情報システムの対策状況

(a) 端末

全端末を対象に、省庁対策基準の端末に関する基本遵守事項を実施した台数の割合を記載する。

(b) 公開用ウェブサーバ

全公開用ウェブサーバを対象に、省庁対策基準の公開用ウェブサーバに関する基本遵守事項を実施した台数の割合を記載する。

(c) メールサーバ

全メールサーバを対象に、省庁対策基準のメールサーバに関する基本遵守事項を実施した台数の割合を記載する。

(3)総評

情報システムの対策状況に関して分析を行い、課題の改善状況、次年度に向けた課題、全体としての傾向等を記載する。

【任意項目】

(4)特筆すべき事項

情報システムの対策状況に関して特徴的な事項がある場合は記載する。

(5)特定システムの対策状況

障害・事故等が発生した場合に国民に重大な影響を及ぼすシステム（例えば、最適化対象システムのうち、国民の関心の高い情報システム、個人情報を処理する情報システム等）について、システムごとの対策状況を記載する。

（留意事項）

特に対策状況に不備が認められない場合でも問題ない旨を記載する。

前年度、全基本遵守事項に準拠（100%）となり、システムの更新又は運用の変更等が発生せず、当該年度もその結果に変更がない場合は、記載を簡略化できる。

５．３　教育・啓発

（目的）

すべての行政事務従事者が、情報セキュリティに関する文書への理解を深め、情報セキュリティ対策を適切に実施できるようにするために取り組んでいる教育・啓発の状況を明らかにすることを目的とする。

（記載内容）

【必須項目】

(1)教育

教育について、以下の事項を参考に、実施している内容を記載する。

・　教育計画の策定、教育の企画等

教育計画の概要、行政事務従事者及び情報セキュリティ対策の役割を担っている者はそれぞれの役割に応じた教育の企画や府省庁教育メニューへの組み込み等の状況について記載する。

・　対象者の役割に応じた教育教材の整備

各対象者への教育教材の整備状況、情報システムの更新、セキュリティ事故の状況等を反映した教材の更新状況等を記載する。

・　教育受講状況の管理

教育の受講状況を管理する仕組みや対象者ごとの受講者の割合を記載する。

また、理解度の確認、人事異動に伴う教育の実施状況について記載する。

・　情報セキュリティ対策担当者の知識向上等

情報セキュリティ対策推進部署において、効果的に業務を遂行するために、担当者の情報セキュリティ対策に係る知識向上について、どのような対策を講じているかを記載する。

【任意項目】

⑵実施手順等の平易化や参照の容易化

実施手順等について、遵守事項を漏れなく含めるだけでなく、理解しやすいものとするため工夫している点について記載する。

また、日常的な参照を容易とするために工夫している点（例：府省庁内ウェブサイト等の分かりやすい場所に置いて日常的に参照可能としている等）を記載する。

⑶ひやり事案を含む障害等の事例の活用

組織内外のひやり事案を含む障害等の事例について、教育等への活用状況を記載する。（事例収集、モデル化、訓練・教育への活用）

（留意事項）

定量的に測定可能ではない項目であっても、自由に記載して構わない。

５．４　調達・外部委託

（目的）

外部委託先から情報漏えい事案等が発生した場合、府省庁の業務に対する国民の信頼が損なわれることから、調達・外部委託に係る情報セキュリティ対策の取組み内容等を明らかにすることを目的とする。

（記載内容）

【必須項目】

⑴外部委託先の管理

外部委託先の管理について、以下の事項を参考に、実施している内容を記載する。

・　調達仕様への記載事項の標準化

調達仕様に記載する情報セキュリティ対策関連事項について標準を定め、

手順書やひな形に含めて示していれば、その状況等を記載する。

・　契約書への記載事項の標準化

契約に記載する情報セキュリティ対策関連事項について標準を定め、手順書やひな形に含めて示していれば、その状況等を記載する。

・　カスタマイズを想定した調達のひな形の策定

契約の手順書やひな形は、留意点を記述する等により、案件ごとにカスタマイズして運用できるようにされていれば、その状況等を記載する。

・　外部委託先の情報セキュリティ対策の履行状況等の確認

委託先における情報セキュリティ対策の履行状況を確認するための方法、情報セキュリティ対策の履行が不十分である場合の対処方法の整備状況、実際に確認している内容等を記載する。

（留意事項）

外部委託の適用範囲は、省庁対策基準で示される範囲であるが、例えば次に掲げる営業品目に該当するものに適用する。

・　ソフトウェア開発（プログラム作成、システム開発等）
・　情報処理（統計、集計、データエントリー、媒体変換等）
・　賃貸借
・　調査・研究（調査、研究、検査等）

５．５　その他取り組んだ事項

（目的）

上記以外に府省庁が取り組んだ対策及び運用について､その実施状況を明らかにすることを目的とする。

（記載内容）

【任意項目】

⑴実施

業務の改善や例外措置について、以下の事項を参考に、実施している内容を記載する。

・　IT 活用等による情報セキュリティ対策実施の自動化、強制化

情報セキュリティ対策を確実に実施するために、IT 活用等により対策実施の自動化や強制をしている場合、その取組の概要を記載する。

例：外部記録媒体に格納する情報の暗号化の強制

・　IT 活用等による情報セキュリティ対策実施状況の点検・調査の自動化

情報セキュリティ対策実施状況の点検・調査を効率的に行うために、IT 活用等による自動化をしている場合、その取組の概要を記載する。

例：自己点検自動集計ツール

・　例外措置件数、例外措置許可案件のリスク低減、適用期間等の検討

例外措置申請件数及び許可件数並びに許可案件のうちリスクを低減させるための代替手段等の提案が申請に含まれている割合を記載する。

また、採用した例外措置について、継続することの妥当性を適時に判断しているか、例外措置を終了するための検討や準備を行っているか（予算措置、基準への反映の要求等）等を記載する。

（留意事項）

定量的に測定可能ではない項目であっても、自由に記載して構わない。IT 活用等による情報セキュリティ対策実施状況の点検・調査の自動化により、より幅広い点検等の実施ができる。

6　情報セキュリティに関する障害・事故等報告

（目的）

府省庁において、情報セキュリティに関する障害・事故等をどのように把握しているのかを明らかにするとともに、府省庁で発生し、公表した障害・事故等の概要、それに対する対応、再発防止策等を記載することにより、国民への説明責任を果たすことを目的とする。

【必須項目】

⑴情報セキュリティに関する障害・事故等の把握

府省庁において、情報セキュリティに関する障害・事故等が発生した場合に、どのように最高情報セキュリティ責任者が把握しているのかを記載する。

⑵公表した障害・事故等の概要、それに対する対応等

⒜情報セキュリティに関する障害・事故等の発生日時

府省庁として把握した日時だけではなく、実際に発生した日時を記載する。

⒝概要

当該事象により行政事務に対して、どのような影響を与えたかを含めて、事象の概要について記載する。

⒞原因

当該事象の発生原因について記載する。

⒟府省庁の対応

暫定措置及び恒久措置について記載する。

⒠原因が省庁対策基準違反によるものか否か

当該事象発生の原因が省庁対策基準違反によるものか、否かを記載する。

⒡再発防止策

当該事象の再発防止策及び情報セキュリティ報告書作成時点までの改善状況を記載する。

【任意項目】

⑶対応コスト

当該事象の発生に伴いかかった対策経費等を記載する。

⑷障害対応に係る対応手順の整備や障害・事故等が発生した際の対応訓練等

障害・事故等が発生した際の対応手順（ウイルス感染時の対応手順、情報システムの停止時の代替業務手順等）について、発生時に容易に参照できるようになっているかなど整備状況を記載する。

また、障害・事故等が発生した際の対応を想定し、訓練を実施している場合、対象システム、訓練内容、訓練にて判明した課題と改善策等を記載する。

⑸一般職員向けの注意喚起

一般職員向けの注意喚起（ウイルスについての警告、ソフトウェアの更新指示等）の実施状況（府省庁内ウェブサイトへの掲載、電子メールでの通知、文書での通達等により適時に広く周知しているか等）を記載する。

（留意事項）

⑵(a)～(f)については、原則として情報セキュリティに関する障害・事故等ごとに記載すること。ただし、同様の障害・事故等が複数ある場合は、まとめて記述しても差し支えない。

情報セキュリティに関する障害・事故等について、報道発表したものは記載しなければならないが、公表には至らない事案も含めた傾向分析等を記載することが望ましい。

原因の分析においては、省庁対策基準に反していれば違反再発防止策を記載し、それ以外の場合は、省庁対策基準の改訂の必要性について記載する。なお、事故公表直後は、事故の内容と暫定的対応措置の公表を優先する必要があるが、情報セキュリティ報告書においては、恒久的対応措置や再発防止策についても記載することが重要である。

7　情報セキュリティ対策に関する次年度の計画

（目的）

本年度の情報セキュリティ対策の総括を次年度に連続して反映させることを目的として、情報セキュリティ対策に関する次年度の計画を記載するものである。なお、本項では、政府機関統一基準において策定を求めている情報セキュリティ対策に関する計画類、情報セキュリティ報告書の中で記載した課題や目標を再掲することなどにより、次年度に実施すべき情報セキュリティ対策を概観できるようにすることを目的としており、新たな内容の計画の策定を求める趣旨ではない。

（記載内容）

【必須項目】

⑴次年度の計画

情報セキュリティ対策に関する次年度の計画を記載する。

【任意項目】

(2) 政府機関統一基準において策定を求めている情報セキュリティ対策に関する計画類、情報セキュリティ報告書の中で記載した課題や目標以外に新たな計画類を作成した場合は、その内容を記載する。

（留意事項）

情報セキュリティ報告書の中で記載した課題や目標などの引用で差し支えない。

8　結び

（目的）

最高情報セキュリティ責任者の情報セキュリティ対策に対する考え方等を踏まえ、最高情報セキュリティアドバイザーとして、特に注力した情報セキュリティ対策の事項について、国民に対してメッセージを発信することにより、課題認識を明確にすることを目的とする。

（記載内容）

【必須項目】

(1)最高情報セキュリティアドバイザーからのメッセージ

最高情報セキュリティアドバイザーとして、特に注力した事項、課題等を記載する。

（留意事項）

最高情報セキュリティアドバイザー連絡会議（仮称）で検討された事項のうち、府省庁内に周知をしたことや、特に注力した事項を記載することも考えられる。

なお、本文と重複した内容が多くならないように、内容を引用する場合は簡潔に記載すること。

第２部　政府機関における評価等の考え方

Ⅰ　目的

政府機関においては、第１次情報セキュリティ基本計画の下、すべての政府機関において、政府機関統一基準が求める水準の対策を実施していること等を目指して、各府省庁の PDCA サイクル及び情報セキュリティ政策会議による評価・勧告を中心とした政府機関全体の PDCA サイクルという２階層の PDCA サイクルを構築し、情報セキュリティ対策を促進するため様々な取組を推進してきた。第 2 次情報セキュリティ基本計画においては、この取組を定着、浸透させ、すべての府省庁が能動的に情報セキュリティ対策に取組む体制の確立を目指し、各府省庁が情報セキュリティ報告書を作成し、公表することとしている。また、各府省庁の情報セキュリティ対策の実施状況に係る定量的評価等を行い、その結果を情報セキュリティ政策会議に報告することとしている。

「第２部　政府機関における評価等の考え方」においては、各府省庁の情報セキュリティ対策の一層の充実・向上を図ることなどを目的として、NISC が行う各府省庁の情報セキュリティ報告書に係る評価等の手法について記載している。

NISC は、同手法に基づき、各府省庁の情報セキュリティ報告書及び各府省庁から入手した情報セキュリティ報告書作成のための基礎資料から、政府機関全体の評価書を作成し、情報セキュリティ政策会議に報告・公表する。

Ⅱ　位置付け

NISC は、「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方について」(2007 年２月２日情報セキュリティ政策会議了解)に基づき、各府省庁と政府機関全体の 2 つの PDCA サイクルが確実かつ自律的に回っていることを確認するために、政府機関全体としての総合的な評価の運用に取り組んできた。

第１次情報セキュリティ基本計画の３ヶ年において、これまでの取組が徐々に浸透してきた段階であることから、これまでの取組を踏まえつつ本委員会で検討された手法に基づき、政府機関全体としての評価を行う。

なお、本評価等の考え方及び評価のプロセスは、政府機関全体における情報セキュリティ対策の浸透・定着、技術や環境の変化等を踏まえ、必要に応じて、NISC において見直すものとする。

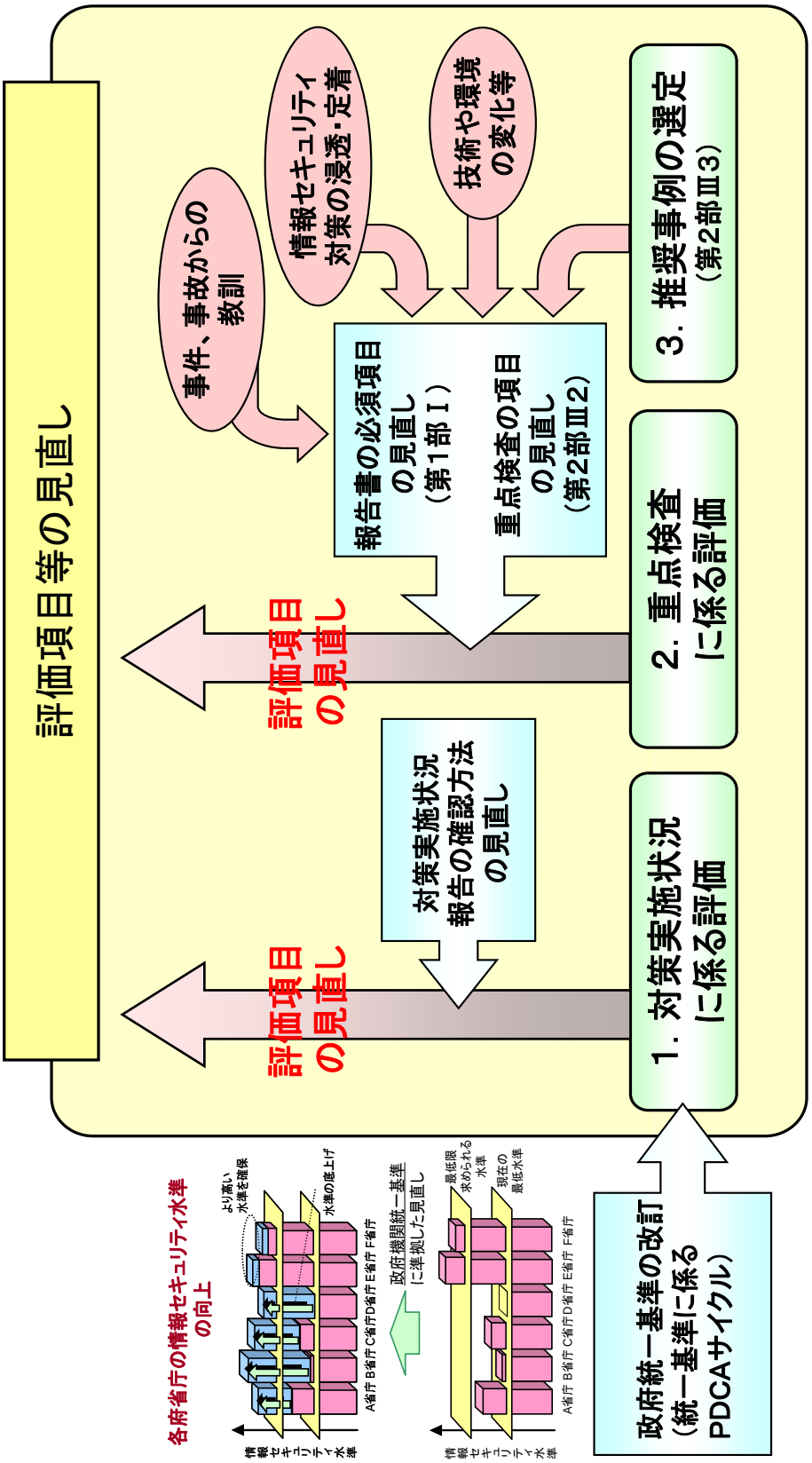


図４　評価項目等の見直し

Ⅲ　評価等の手法に関する内容

NISC は、以下の１～３の各手法に基づく評価を行うとともに、各評価結果をもとに各府省庁及び政府機関全体の総合評価結果を示す。

１　対策実施状況に係る評価

⑴目的

政府機関全体の情報セキュリティ対策実施状況を継続的に把握・評価することにより、政府機関統一基準に基づく情報セキュリティ対策水準の維持・向上を図ることを目的とする。

⑵評価手法等

NISC は、「第１部　情報セキュリティ報告書作成のためのガイドライン　Ⅲ５．１　省庁対策基準に関する自己点検結果」について、各府省庁が情報セキュリティ報告書を作成する際に収集した基礎資料を入手し、評価を行う。

具体的に、NISC は、政府機関統一基準に準拠する省庁対策基準に基づく自己点検、監査等により把握した対策実施状況報告を各府省庁から入手し、百分率（%）で示された把握率、実施率及び到達率を集計し、政府機関全体の平均値を責任者等、システム、職員の３つの実施主体ごとに区分し算出する。把握率及び実施率については、各府省庁ごとに ABCD 評価を行う。また、経年度比較を行うなど改善の進捗が確認できるような形で評価を行う。

把握率、実施率及び到達率の定義は、以下のとおりである。

・把握率

各府省庁が報告対象とした者のうち、対策実施状況が把握できた者の割合

・実施率

把握した者のうち、責務が生じた者に占める対策を実施した者の割合

・到達率

把握した者のうち、責務が生じた一定の割合（100%、95%、90%）以上の者が対策を実施した遵守事項の割合

遵守事項については、政府機関全体の傾向を分析し、重要な課題又は継続的な課題を抽出する。なお、改善した前年度の課題があれば、記載する。

ABCD 評価の見方例は図５のとおりである。

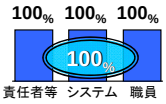
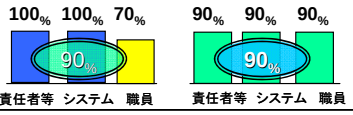
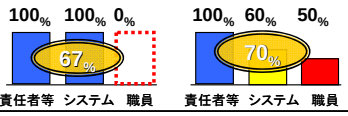
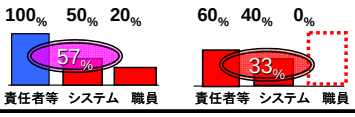
評価	実施率/(把握率)	対策状況	個別対策項目についての 評価パターン例
A	100%	適切に実施すべき対策について、**すべての項目で**統一基準に準拠した**対策が実施**されている。	
B	80%≦x＜100%	適切に実施すべき対策について、**概ねすべての項目で**統一基準に準拠した**対策が実施**されているが、**一部の項目で不十分なもの**が含まれている。	
C	60%≦x＜80%	適切に実施すべき対策について、**不備の項目が一部に見られる**など、対策が遅れている。	
D	60%未満	適切に実施すべき対策について、**不備の項目が相当数、見られるなど**、対策が著しく遅れている。	

図５　対策実施状況のＡＢＣＤ評価

評価方法は、例えば実施率については、対策実施状況報告の３つの実施主体者の平均実施率（項目ごとに算出した実施率の総平均値）の平均値を総合評価の実施率としている。したがって、政府機関統一基準で求める情報セキュリティ対策がすべて実施されていれば、総合評価の実施率は 100%、すなわち“A 評価”となる。

(3)評価書の内容等

NISC は、政府機関全体の対策実施状況報告に係る評価の目的、対象範囲等を記載するとともに、実施主体ごとの把握率、実施率、到達率の評価結果、課題、改善点等を評価書に記載する。

なお、参考として、各府省庁の対策実施状況報告の集計結果を添付する。

２　重点検査結果の評価

(1)目的

政府機関統一基準の基本遵守事項の中でも重要な項目及び「３　情報セキュリティ対策に係る推奨事例の選定」のプロセスで過去に選定された推奨事例の中で特に政府機関全体に浸透・定着を図るべきものについて、重点検査を行い、具体的な情報セキュリティ対策状況を把握・評価することにより、改善促進を図ることを目的とする。

(2)評価手法等

NISC は、「第１部　情報セキュリティ報告書作成のためのガイドライン」において情報セキュリティ報告書への記載を必須とした項目の中から、「①第１部 Ⅲ５．２情報システムごとの状況」及び「②過去に選定された推奨事例の中で特

に政府機関全体に浸透・定着を図るべきもの」について、各府省庁から基礎資料を入手し、以下の①及び②の評価手法等に基づき、評価を行う。

①「第１部Ⅲ５．２情報システムごとの状況」に係る評価手法等

NISC は、重点検査項目に関する各府省庁の検査結果を入手し、各府省庁の実施率について、ABCD 評価を行う。その際には、経年度比較を行うなど改善の進捗が可能な限り見られるような形で評価を行う。

ABCD 評価の見方例は図６のとおりである。

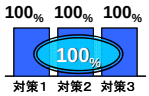
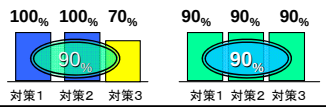
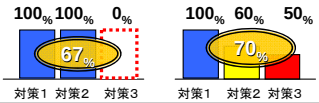
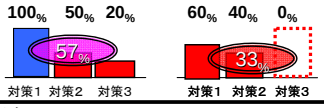
評価	実施率	対策状況	個別対策項目についての評価パターン例
A	100%	適切に実施すべき対策について、**すべての項目で**統一基準に準拠した**対策が実施**されている。	
B	80%≦x<100%	適切に実施すべき対策について、**概ねすべての項目で**統一基準に準拠した**対策が実施**されているが、**一部の項目で不十分なもの**が含まれている。	
C	60%≦x<80%	適切に実施すべき対策について、**不備の項目が一部に見られる**など、対策が遅れている。	
D	60%未満	適切に実施すべき対策について、**不備の項目が相当数、見られるなど**、対策が著しく遅れている。	

図６　重点検査項目のＡＢＣＤ評価

評価方法は、重点検査項目の各カテゴリーの平均実施率（項目毎に算出した実施率の総平均値）の平均値を総合評価の実施率としている。したがって、政府機関統一基準で求める情報セキュリティ対策がすべて実施されていれば、総合評価の実施率は 100%、すなわち“A 評価”となる。

なお、実施率は、「実際に情報セキュリティ対策を実施している対象数」を「情報セキュリティ対策を実施すべき対象数」で割った式で求められる。

②　過去に選定された推奨事例の中で特に政府機関全体に浸透・定着を図るべきものに係る評価手法等

検査項目に応じて、適宜、NISC において定量的又は定性的評価手法を検討する。

(3)評価書の内容等

NISC は、政府機関全体の重点検査の評価結果に基づき、対象機関や対象システム及びその数、所見等の概要を記載するとともに、重点項目に関する情報セキュリティ対策の総合評価、評価結果を受けた各府省庁の対応方針を記載する。なお、(2)②に関しては、適宜、NISC において検討する。

3　情報セキュリティ対策に係る推奨事例の選定

⑴目的

各府省庁が独自に取り組んだ情報セキュリティ対策から、推奨事例を選定することにより、当該府省庁の独自性や創意工夫を評価し、モチベーションを高めるとともに、府省庁間における取組事例の共有を通じ、政府機関全体としての情報セキュリティマネジメント水準の向上を図ることを目的とする。

なお、情報セキュリティマネジメント水準の向上を図るために、選定された推奨事例は、政府機関全体への浸透状況を踏まえ、「第１部Ⅲ情報セキュリティ報告書の構成のひな形」の必須項目とするとともに、「第２部Ⅲ２重点検査結果の評価」の検査項目とすることにより、マネジメント水準の評価に活用する。

⑵評価手法等

最高情報セキュリティアドバイザー連絡会議（仮称）は、各府省庁の情報セキュリティ報告書に記載されている事項を相互に評価し、推奨事例候補となる取組事例を NISC に推薦する。NISC は、推薦された事例から、以下の選定基準に基づき、推奨事例を選定する。

（推奨事例選定の基準）

府省庁の模範となる工夫が見られる、参考にすべき優れた取組事例であること。

⑶評価書の内容等

NISC は、選定した推奨事例の内容、選定理由等を評価書に記載する。