

政府機関における情報セキュリティ対策の評価指標について (各論整理)

情報セキュリティ政策会議
政府機関評価指標専門委員会

1. 評価指標の考え方とその活用の枠組み

政府機関における情報セキュリティ対策は、各府省庁が政府機関統一基準を踏まえた府省庁基準に基づくPDCAサイクルを持続的に進め、また政府全体としても各府省庁の対策実施状況の評価や政府機関統一基準の適時・適切な見直しも含めた情報セキュリティ対策のPDCAサイクルが推進されることが基本となっている。そのため、この各府省庁と政府全体の2つのPDCAサイクルが確実にかつ自律的に回っているかを確認するとともにそれらの改善に活用が可能な評価指標を設定する。

● 各府省庁のPDCAサイクルにおける活用

- ・ 各府省庁における対策実施状況を総合的に評価するための指標。各府省庁における改善に活用

● 政府全体のPDCAサイクルにおける活用

- ・ 情報セキュリティ政策会議において各府省庁の対策実施状況を総合的に評価するための指標(結果に基づき改善を勧告等)
- ・ 必要に応じ、政府機関共通施策(情報セキュリティ年度計画、政府機関統一基準等)に反映

2. 府省庁における情報セキュリティ対策と評価指標

府省庁における情報セキュリティ対策の評価には、

- i) 情報セキュリティマネジメントの評価(マネジメント指標): 定性的指標、定量的指標
- ii) 情報セキュリティ対策実施状況の評価(対策実施指標): 定量的指標
- iii) 情報セキュリティ対策の効果の評価

の3つの評価が考えられる。そのうち、効果の評価については、各府省庁で客観的かつ効率的に評価する指標を設定することは困難であるため、間接的にマネジメント及び対策実施状況の一部を代替指標として活用する。

3. 情報セキュリティマネジメントの評価

(1) 評価の視点

府省庁における情報セキュリティマネジメントが PDCA サイクルの各段階で確実に効果的に行われているかを以下の視点で評価する。これらの視点については、マネジメントが対象とする段階を踏まえて、「計画」、「周知」、「実施」及び「評価と改善」の大分類と、その中での要素や場面に応じた小分類を設けている。その際、職員の情報セキュリティ意識及び認識に関する視点については、その重要性にかんがみ、「計画」から切り出して、「周知」としている。また、PDCA サイクル推進の前提となる情報セキュリティガバナンスの視点は、主として「計画」に含めている。

| 大分類 | 小分類 | 視点 |
|---------|---|--|
| 計画 | 資源 | <input type="checkbox"/> 情報セキュリティ対策管理部門に適切な人的資源が割り当てられているか |
| | 組織 | <input type="checkbox"/> 基準で定める責任者等が指名されているだけでなく、実態において組織として機能し得るものであるか |
| | 規程 | <input type="checkbox"/> 情報システムに適用する規程は、それぞれの情報システムの特性や取り扱う情報等を考慮して策定されているか <input type="checkbox"/> 現場への適合性を適時に評価し、必要に応じて見直しをしているか |
| 周知 | 啓発 | <input type="checkbox"/> 規程が定められているだけでなく、職員一人一人まで理解しているものであるか |
| | | <input type="checkbox"/> 規程がその利用者にとって容易に参照・利用できるようになっているか |
| | | <input type="checkbox"/> 組織内外のひやり事案を事例として活用しているか |
| 教育 | <input type="checkbox"/> 情報セキュリティ教育を適切に実施し、また試験等により職員の理解度を確認しているか | |
| 実施 | 業務改善 | <input type="checkbox"/> 先端的技術の活用(対策のシステム化等)等により、情報セキュリティ対策が業務プロセスにシームレスに組み込まれているか |
| | 障害等への対応 | <input type="checkbox"/> 府省庁外からの脅威情報を周知しているか |
| | | <input type="checkbox"/> 障害等(インシデント及び故障を含む。)への対応が適切に行われるか |
| | | <input type="checkbox"/> 障害等の事後策を実施しているか |
| | 例外措置 | <input type="checkbox"/> 基準への例外事項をあまねく把握し、例外措置を適用できているか |
| 調達・外部委託 | <input type="checkbox"/> 調達及び外部委託における情報セキュリティ確保のために十分な対策が採られているか | |
| 評価と改善 | 評価と改善 | <input type="checkbox"/> 自己点検が有効に行われ、必要な改善が図られているか |
| | | <input type="checkbox"/> 情報セキュリティ監査が有効に行われ、必要な改善が図られているか |

注)情報セキュリティ予算を評価の視点に含めることも将来的には考えられるが、セキュリティ要件により一律には想定しにくいこと、情報システム予算の中で区別して捕捉されない場合が少なくないことから、当面は、可能な精度の範囲で情報収集を行うに留めることとする。

(2) マネジメント指標

これらの評価の視点ごとに、【別紙】のとおり、一群のマネジメント指標を定める。

この際、評価指標に関しては、各府省庁独自の取組みを示すものも、評価の視点に沿った効果を上げていることがヒアリング等で確認できれば追加して評価対象に含めることとする。

(3) 情報セキュリティマネジメントの総合的な評価 — マネジメント力 —

各府省庁について、「計画」、「周知」、「実施」及び「評価と改善」の大分類とそれぞれの小分類について、情報セキュリティマネジメントの度合い「マネジメント力」を下表により評価する。また、内閣官房情報セキュリティセンターは、項目別評価結果のレビュー、総合評価結果の導出及び各府省庁へのフィードバックを行う。

| マネジメント力 | 評価指針 |
|--|---|
| <p>★★★(Ⅲ) 適切に行われているだけでなく、特に効果的な手法・プラクティスの採用や、府省庁業務についての統合的視点からの施策等も導入している。</p> | <ul style="list-style-type: none"> ● マネジメント指標に採用した政府機関統一基準の基本遵守事項(必須)を実施している ● 各指標の評価結果が適正である ● さらに、情報セキュリティ対策をより確実にいき、又は高い効果を得ることのできる以下のような施策も導入している(★★の事項に加えて) <ul style="list-style-type: none"> ・ 効果的な手法・プラクティスの採用 ・ 関連する業務・制度等(教育、PMO、文書管理、個人情報保護等)との統合・連携 |
| <p>★★(Ⅱ) 適切に行われているだけでなく、対策を確実に行うための施策等も導入している。</p> | <ul style="list-style-type: none"> ● マネジメント指標に採用した政府機関統一基準の基本遵守事項(必須)を実施している。 ● 各指標の評価結果が適正である。 ● さらに、情報セキュリティ対策をより確実に行うための以下のような施策も幾つか導入している。 <ul style="list-style-type: none"> ・ 対策実施や評価における自動化、IT 活用 ・ 政府機関統一基準／省庁基準以上のきめ細かなマネジメント |
| <p>★(Ⅰ) おおむね適切に行われている。</p> | <ul style="list-style-type: none"> ● マネジメント指標に採用した政府機関統一基準の基本遵守事項(必須)は実施している。 ● 各指標の評価結果がおおむね適正である。 |
| <p>—(不足) 不十分であり、政府機関統一基準で期待するセキュリティ水準が確保されていない懸念がある。</p> | <ul style="list-style-type: none"> ● マネジメント指標に採用した政府機関統一基準の基本遵守事項(必須)で、実施していないものがある。 ● このため、政府機関統一基準／省庁基準の適用により達成されるべきセキュリティ水準が確保されていないことが懸念される。 |

4. 情報セキュリティ対策実施状況の総合的な評価

政府機関統一基準の基本遵守事項 346 項目の中でも重要な項目に着目し、重点検査を実施し、対策の実施率の定量的な評価を行う。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。

| 評価 | 実施率 |
|----|-----------------------|
| A | $X = 100\%$ |
| B | $80\% \leq X < 100\%$ |
| C | $60\% \leq X < 80\%$ |
| D | $X < 60\%$ |

なお、強化遵守事項については、府省庁における省庁基準への取り込み状況を調査し、その結果を政府機関統一基準の見直し等に活用する。

5. 政府機関全体としての総合的な評価の運用

情報セキュリティ政策会議において、「情報セキュリティマネジメントの総合評価」(マネジメント力)と「情報セキュリティ対策実施状況の総合評価」(実施率(スナップショット))について実施し、改善に向け、府省庁へ指示を行う他、参考にすべき優れたプラクティス等については、府省庁に還元するなど、各府省庁での持続的な取り組みを促進する。

その際、評価の結果については、必要なものについて、情報セキュリティ基本計画・年度計画、政府機関統一基準への反映等を行うとともに、優れたプラクティス等を参考に水準向上に向けた府省庁毎の取り組みへ還元する等、政府機関全体としての改善を行う。また、評価指標についても、運用段階で把握された問題点等を踏まえ、逐次見直し、改善を行う。

なお、地方支分部局等については、一般に地理的分散、管理体制等について課題が存在することから、府省庁毎の評価において課題の所在を明確化するとともに、府省庁間での評価に際しては共通の条件に基づく比較を可能とする評価方法を採用する。

| 大分類 | 小分類 | 視点 | 評価指標 | | | | |
|----------------------------------|---|--|--|---|---|--|---------------------------------------|
| | | | 定量的な指標 | | 定性的な指標 | | |
| | | | | 見方 | | 見方 | |
| 計画 | 資源 | 情報セキュリティ対策管理部門に適切な人的資源が割り当てられているか | ①情報セキュリティ担当者数 ÷ 職員数 ②情報セキュリティ担当者の情報セキュリティ業務平均経験年数 | 適正値は組織規模等に依存実績を見て今後判断 適正値は実績を見て今後判断 | ①情報セキュリティ対策管理部門の担当者の情報セキュリティ知識向上のための対策を講じているか | 情報セキュリティ対策管理部門の担当者の知識水準に係る一指標 | |
| | | 組織 | 基準で定める責任者等が指名されているだけでなく、実態において組織として機能し得るものであるか | | | ①府省庁全体の業務について、その把握や総合調整を行う権限を有する部署があるか | 特に、規模の大きい府省庁において、府省庁内全体での施策の遂行力に係る一指標 |
| | | | | | ②各府省庁のPMO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り組みを管理しているか(例えば業務・システム最適化の企画段階での情報セキュリティ対策要領の作成、情報システムの構築の要求仕様策定段階での情報セキュリティ要件定義の作成等の管理) | 今後の情報システム投資における情報セキュリティへの考慮を測る一指標 | |
| | | | | | ③各府省庁のPMOにおいて、情報資産台帳を整備しているか | 情報セキュリティ対策実施の前提の整備状況についての一指標 | |
| | | | | | ④最高情報セキュリティアドバイザーを置いているか(最高情報セキュリティ責任者に助言を行う専門家の有無) [関連: 政府機関統一基準2.1.1(1)(c)] | 最高情報セキュリティ責任者のマネジメントに係る一指標 | |
| | ①情報セキュリティ委員会の年度内開催回数 | | | 一般には2回以上の開催が想定される(省庁基準の策定・改定、教育実績の把握等情報セキュリティ委員会の業務を遂行していること目安) | ⑤省議等、府省庁幹部職員が出席する会議で当該府省庁の情報セキュリティ状況について報告を行っているか ⑥情報セキュリティ責任者、情報システムに係る責任者等を集めた府省庁内横断的な連絡会議等を行っているか | 情報セキュリティに関する府省庁幹部職員の理解と支援を示す一指標 情報セキュリティ対策の実効性に関する一指標 | |
| | | | | | ⑦地方支分部局等を持つ場合に、情報セキュリティに係る責任者及び担当者をそれぞれの支分部局ごとに置いているか | 地方支分部局等の課題への対応力に関する一指標 | |
| | 規程 | 情報システムに適用する規程は、それぞれの情報システムの特性や取り扱う情報等を考慮して策定されているか | | | ①情報システムに係る手順書等の策定にあたり、当該情報システムの情報システムセキュリティ責任者が関わり、内容を確認しているか [政府機関統一基準5.2.1(1)(a), 5.3.1(1)(a)] | 必須 | |
| | | 現場への適合性を適時に評価し、必要に応じて見直しをしているか | | | ②各規程の見直しを行う必要性の有無を適時検討し、必要があると認められた場合にその見直しをしているか [政府機関統一基準2.4.1(1)(a)] | 必須 | |
| | 周知 | 啓発 | 規程が定められているだけでなく、職員一人一人まで理解しているものであるか | | | ①一般職員向けの手順書等は、その策定にあたり、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に努めたか | 対策の実効性を確保する上で重要な事項 |
| 規程がその利用者にとって容易に参照・利用できるようになっているか | | | | | ①一般職員向けの手順書等は、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か | 対策の実効性を確保する上で重要な事項 | |
| 組織内外のひやり事案を事例として活用しているか | | | | | ①組織内外のひやり事案を含む障害等の事例を活用しているか ・事例収集 ・モデル化 ・訓練・教育への活用 | 情報セキュリティ水準の確保・向上を図る上で効果的な施策 | |
| 教育 | | 情報セキュリティ教育を適切に実施し、また試験等により職員の理解度を確保しているか | ①教育の年度内受講者の割合(幹部(指定職以上)、管理職(課室長)、一般職員) [政府機関統一基準2.2.1(2)] | 不在者等を考慮した水準を設定 例: 95%以上 | ①すべての対象者(一般職員、各責任者・管理者)に対して、教育教材が整備されているか [政府機関統一基準2.2.1(1)] | 必須 | |
| | | | | | ②教育教材は、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て更新されているか | 教育内容の適切性を確保する上で、実質的に必須の事項 | |
| | | | | | ③教育に関する計画が定められているか [政府機関統一基準2.2.1(1)] | 必須 | |
| | | ④教育に関する計画では、情報セキュリティに係る責任者及び管理者の役割に応じた教育を企画しているか [関連: 政府機関統一基準2.2.2(2)] | 教育の実効性を確保する上で、実質的に必須の事項 | | | | |
| | | ⑤教育の年次計画を定める際には、人事部門、情報システム部門等、関係者間と調整をしているか(府省庁教育メニューへの組み込み、情報システム部門の支援等、教育の準備及び実施のための条件整備) | 情報セキュリティに関する教育を府省庁における組織的な活動に位置づけていることに関する、実効性の向上において重要な指標 | | | | |
| | | ⑥行政事務従事者の転入や情報セキュリティに係る責任者及び管理者の指名にあわせて、役割に応じた教育を行っているか | 教育の実効性を確保する上で、実質的に必須の事項 | | | | |
| | | ②eラーニングの活用率 ・eラーニング教材の準備率 ・利用可能職員の割合 | 適正値は実績を見て今後判断するが、府省庁の規模等にも依存 | ⑦教育の受講状況を管理する仕組みはできているか [政府機関統一基準2.2.1(1)(e)] ⑧教育の実施時等に、試験等により職員の理解度を確保しているか | 必須 教育の実効性を確保する上で重要な事項 | | |
| 実施 | 業務改善 | 先端技術の活用(対策のシステム化等)により、情報セキュリティ対策が業務プロセスにシームレスに組み込まれているか | | | ①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か 例: 外部記録媒体に格納する情報の暗号化の強制 | 人の意識に頼ることなく対策実施を徹底する上で有効な事項 | |
| | | 異常・障害等への対応 | 府省庁外からの脅威情報を周知しているか | | | ①一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)を、府省庁内ウェブサイトへの掲載、電子メールでの通知又は文書での通達等により適時に広く周知しているか | 対策を適切に行うために重要な事項 |
| | 障害等(インシデント及び故障を含む)への対応が適切に行われるか | | ①障害等が発生した際の対応訓練の回数(年間)(特定の重要な情報システムについて) [関連: 政府機関統一基準2.2.2(2)] | 一般には、重要な情報システムについて年1回以上実施することが適切であると考えられる | ①障害等が発生した際の対応手順があるか、また、発生時に容易に参照できるようになっているか 例: 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 | 障害等発生時の対応に重要な事項 | |
| | 障害等の事後策を実施しているか | | | | ①障害等が発生した場合に、その原因を調査して再発防止策を策定し、必要な措置を講じているか [政府機関統一基準2.2.2(3)(a), (b)] | 必須 | |
| | 例外措置 | 基準への例外事項をあまねく把握し、例外措置を適用できているか | ①例外措置申請件数、許可件数 | 経年変化を観察 例外措置の内容によりその解消の必要性、解消に要する期間等が異なることに留意 評価方法については実績を見て今後判断 | | | |
| | | | ②例外措置の許可案件のうち、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 | | | | |
| 調達・外部委託 | 調達及び外部委託における情報セキュリティ確保のために十分な対策が採られているか | | | ①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、また、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) | | 例外措置の適切な運用を維持する上で重要な事項 | |
| | | | | ①調達仕様に記載する情報セキュリティ関連事項について標準を定め、手順書や雛形に含めて示しているか [関連: 政府機関統一基準4.3.1(1)(b), (c), 6.1.1(1)(a), (b), (2)(c), 6.1.2(1)(b), (2)(a), (b), (c), 6.1.3(1)(a), (b)] | | 機器等の調達及び外部委託における情報セキュリティ確保の基本的な事項 | |
| | | | | ②契約に記載する情報セキュリティ関連事項について標準を定め、手順書や雛形に含めて示しているか [関連: 政府機関統一基準6.1.2(4)(a)] | | 外部委託における情報セキュリティ確保の基本的な事項 | |
| | | | | ③調達・契約の手順書や雛形は、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なっているか | 適切な調達を行うために重要な事項 | | |

| 大分類 | 小分類 | 視点 | 評価指標 | | | |
|-------|-------|---------------------------------|---|--|---|------------------|
| | | | 定量的な指標 | | 定性的な指標 | |
| | | | | 見方 | | 見方 |
| 評価と改善 | 評価と改善 | 自己点検が有効に行われ、必要な改善が図られているか | ①自己点検票回収率(幹部(指定職以上)、管理職(課室長)、一般職員) [政府機関統一基準2.3.1] | 不在者等を考慮した水準を設定 例:85%以上 | ①当該年度の自己点検計画が定められているか [政府機関統一基準2.3.1(1)(a)] | 必須 |
| | | | | | ②自己点検結果に基づき、その評価及び必要な場合に改善指示がなされているか [政府機関統一基準2.3.1(5)] | 必須 |
| | | 情報セキュリティ監査が有効に行われ、必要な改善が図られているか | | | ①当該年度の情報セキュリティ監査計画が定められているか [政府機関統一基準2.3.2(1)(a)] | 必須 |
| | | | | | ②以前実施した監査結果で明らかになった課題及び問題点の改善状況についての監査が当該年度の情報セキュリティ監査計画に盛り込まれているか [政府機関統一基準2.3.2(1)(a)] | 持続的に改善を図る上で重要な事項 |
| | | | | | ③当該年度の監査報告が行われているか [政府機関統一基準2.3.2(5)] | 必須 |
| | | | ④監査報告書の内容を最高情報セキュリティ責任者に(単に提出するだけでなく)説明しているか | 監査報告に関して最高情報セキュリティ責任者が適切な判断及び指示を行うために重要な事項 | | |
| | | | ⑤監査報告書の内容を踏まえ、改善のための以下の措置をとっているか a. 指摘事案に対する対応実施の指示(最高情報セキュリティ責任者) b. 同種の課題及び問題点の有無についての確認の指示(最高情報セキュリティ責任者) c. 改善を指示された事案についての対応計画(達成可能な対応目標の設定を含む。)の作成と報告(情報セキュリティ責任者) d. 情報セキュリティ関係規程の妥当性評価と必要に応じ見直しの指示(情報セキュリティ責任者) [政府機関統一基準2.3.2(6)(a), (b), (c), (d)] | 必須 | | |