資料２－２

サイバーセキュリティ対策を強化するための監査（マネジメント監査）に係る実施要領

平　成　　２８　年　〇　月　〇　日
サイバーセキュリティ対策推進会議申合せ（案）

第１章　総　則

（目的）

第１条　この要領は、サイバーセキュリティ戦略本部（以下「戦略本部」という。）が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 日戦略本部決定。以下「基本方針」という。）に基づき実施する監査のうち、国の行政機関に対し実施するマネジメント監査について、必要な事項を定める。

（監査の実施主体）

第２条　本監査事務は、基本方針５（５）に基づき、内閣サイバーセキュリティセンター（以下「NISC」という。）が実施する。

２　NISC は、必要かつ適切と判断される場合には、外部の専門家による協力を得ることができる。

（監査の権限）

第３条　NISC は、本監査の実施に当たって、監査対象の国の行政機関（以下「監査対象組織」という。）に対し、資料の提出、事実などの説明、あらかじめ合意した監査期間内における施設の立入り及びその他 NISC が必要とする事項の開示を求めることができる。

２　監査対象組織は、前項の求めに対して、協力しなければならない。

（監査の実施主体の責務）

第４条　NISC は次の責務を負う。

一　独立性及び中立性を保つこと

二　公正かつ客観的な監査判断を行うこと

三　取り扱う情報の秘密の保持を厳守すること

四　監査及び情報セキュリティに関する専門知識を有し、正当な注意をもって監査を実施すること

（文書の管理）

第５条　NISC は、監査において収集した資料は、漏えい、紛失等が発生しないよう、適切に管理しなければならない。

第２章　監査計画

第６条　NISC は、原則として、戦略本部が決定した当該年度における年度監査方針に基づき、監査対象組織の状況を踏まえて、監査計画を立案する。

第３章　監査の実施

（監査の実施通知）

第７条　NISC は、監査計画に基づく監査の実施に当たり、監査対象組織と協議の上、あらかじめ、監査実施の時期、範囲、項目、従事者等を記載した監査実施通知書を監査対象組織に通知する。

２　NISC は、サイバーセキュリティに影響しうるリスクを新たに発見し、当初の監査計画における監査では不十分であると認められた場合等、追加的な監査を実施する必要が生じた場合においては、監査対象組織と協議の上、監査実施通知書を策定又は変更する。

（事実の確認）

第８条　NISC は、監査の結果、発見した事項について、監査対象組織と事実誤認等がないことの確認を行う。

第４章　監査報告

（個別監査結果の通知）

第９条　NISC は、監査対象組織における監査の概要、発見した重要な事項と改善のために必要な助言、その他特記すべき事項等を記載し、監査対象組織の最高情報セキュリティ責任者に通知する。

（最高情報セキュリティ責任者の執るべき措置）

第 10 条　個別監査結果の通知を受けた最高情報セキュリティ責任者は、その内容を踏まえ、速やかに必要な措置等を検討し、改善計画を策定し、NISC に提出するとともに、既に改善したものについては改善結果を報告する。

２　NISC は、前項に規定する改善計画の提出があった場合は、必要に応じ助言等行う。

（フォローアップ）

第 11 条　NISC は、各監査対象組織における改善計画に対する改善の実施状況について、適宜確認を実施し、各監査対象組織の求めに応じて助言を行う。

（戦略本部への報告）

第12条　NISCは、当該年度の監査の結果、監査結果に基づき各監査対象組織が実施した改善の状況、各監査対象組織における優れた取組（グッドプラクティス）、その他特記すべき事項等を取りまとめ、戦略本部に報告する。上記の報告内容は、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とならないよう、個別組織名を明らかにしないその他の配慮を行う。

以　　上