

○情報セキュリティ監査実施要領の制定について

平成17年3月31日例規（情）第60号

この度、別記のとおり情報セキュリティ監査実施要領を制定し、平成17年4月1日から実施することとしたので、了知されたい。

別記

情報セキュリティ監査実施要領

第1 趣旨

この要領は、情報セキュリティに関する規程（平成30年訓令第2号）第21条第2項の規定に基づき、情報セキュリティに関する監査（以下「情報セキュリティ監査」という。）の実施に関し必要な事項を定めるものとする。

第2 実施体制

1 情報セキュリティ管理者の任務

情報セキュリティ管理者は、情報セキュリティ監査の実施について総括管理するものとする。

2 情報セキュリティ副管理者の任務

情報セキュリティ副管理者は、情報セキュリティ管理者の命を受け、情報セキュリティ監査の実施に関する事務を行うものとする。

3 情報セキュリティ監査実施担当者の指定

情報セキュリティ副管理者は、情報セキュリティ監査を実施するときは、高度情報推進課員のうちから情報セキュリティ監査実施担当者を指定して、その事務を処理させるものとする。

第3 監査の種別

情報セキュリティ監査の種別は、次のとおりとする。

- (1) 通常監査（計画的に、所属ごとに実施期日を定めて実施するものをいう。）
- (2) 随時監査（情報セキュリティ副管理者が必要と認めるときに実施するものをいう。）
- (3) 特別監査（情報セキュリティを侵害する事案が発生したとき、又は発生するおそれがあるとき情報セキュリティ管理者が認めるときに実施するものをいう。）

第4 監査する事項及び内容

情報セキュリティ監査において監査する事項及び内容は、別表のとおりとする。

第5 通常監査の実施

1 実施計画

- (1) 情報セキュリティ副管理者は、毎年度4月末日までに、次に掲げる事項を定める通常監査実施計画（以下「実施計画」という。）を策定し、情報セキュリティ管理者の承認を受けなければならない。

ア 所属ごとの実施時期

イ 監査の重点とする事項

ウ 対象とする期間

- (2) 情報セキュリティ副管理者は、前記(1)の承認を受けたときは、実施計画を各所属長に速やかに通知するものとする。

- (3) 通常監査は、実施計画に基づき実施するものとする。ただし、情報セキュリティ副管理者は、特に必要があると認める場合は、情報セキュリティ管理者の承認を受けた上で、実施計画を変更することができる。

なお、情報セキュリティ副管理者は、当該承認を受けたときは、その内容を速やかに関係する所属長に通知するものとする。

2 実施の通知

情報セキュリティ副管理者は、通常監査を実施するときは、対象とする所属の長に、実施日時その他必要な事項をその実施の日の1週間前までに通知するものとする。

第6 随時監査の実施

情報セキュリティ副管理者は、随時監査を実施する必要があると認める場合は、対象とする所属の長に次に掲げる事項を事前に通知した上、実施するものとする。

- (1) 実施日時

(2) 監査する事項

第7 特別監査の実施

情報セキュリティ管理者は、特別監査を実施する必要があると認める場合は、情報セキュリティ副管理者に、対象とする所属の長に次に掲げる事項を事前に通知した上、実施させるものとする。

(1) 実施日時

(2) 監査する事項

第8 実施の方法

情報セキュリティ監査は、書類監査及び実地監査の方法により行うものとする。

第9 結果の報告

情報セキュリティ副管理者は、情報セキュリティ監査を実施したときは、その結果を総合的に評価した上、通常監査については1月ごとに、随時監査及び特別監査についてはその都度、書面により情報セキュリティ管理者に報告しなければならない。ただし、情報セキュリティの維持に関する事務（以下「セキュリティ維持事務」という。）について改善を要する事項があると認める場合は、情報セキュリティ監査を実施した後、速やかに報告するものとする。

第10 事務の改善

1 改善の通知

情報セキュリティ管理者は、前記第9により情報セキュリティ監査の実施に係る報告を受けた場合において、当該報告に係るセキュリティ維持事務について改善を要すると認める事項があるときは、当該情報セキュリティ監査を受けた所属の長に必要な措置を講ずるように通知するものとする。

2 改善の結果の報告

前記1による通知を受けた所属長は、速やかに当該通知に係る措置を講じ、その結果を情報セキュリティ管理者（高度情報推進課）に報告しなければならない。

前 文（抄）（令和4年3月30日例規（情）第31号）

令和4年4月1日から実施することとしたので、了知されたい。

別表

監査する事項	監査する内容
情報セキュリティ責任者等の任務の遂行に関する事項	1 情報セキュリティの維持を図るための方策を定めた達の制定状況 2 情報セキュリティの維持についての点検状況及び是正状況 3 その他
端末装置等の設置場所の管理に関する事項	1 部外者が立ち入る場合の職員による立会いに関する措置状況 2 その他
職員の責務の遂行に関する事項	1 パスワードの管理状況 2 アクセス権の使用状況 3 端末装置、電磁的記録媒体等の使用状況及び管理状況 4 コンピュータウイルス等不正プログラムの感染の防止に関する措置状況 5 その他
情報システム等における情報セキュリティ対策に関する事項	1 電子計算機、端末装置及びネットワーク機器（情報を伝送するための機器）についての許可のない者による操作の防止に関する措置状況 2 災害発生時等における障害対策及び代替措置状況 3 障害発生時の対応手順についての制定状況 4 情報システム機械室についての環境対策並びに入室及び退室の管理状況 5 システムドキュメント（情報システム等に関する設計、仕様等を説明するために作成された文書をいう。）の整備状況

	及び管理状況 6 外部委託に当たって定めた措置の実施状況 7 情報システム等を構成する機器の設置の実態 8 その他
アクセスの管理に関する事項	1 アクセス権の付与の対象となる者の範囲の指定状況等 2 アクセス権の付与状況 3 アクセス権を付与した者の管理状況 4 アクセスについての記録状況及び分析状況 5 アクセスに係る認証情報の設定状況 6 その他
電磁的記録媒体等の管理に関する事項	1 配分及び使用についての管理状況 2 保管、使用及び廃棄の実態 3 持ち出しについての管理状況 4 その他
事案発生時の対応に関する事項	1 情報セキュリティを侵害する事案が発生した場合の措置状況及び報告状況 2 その他
教養に関する事項	1 情報セキュリティに関する教養の状況 2 情報セキュリティを侵害する事案が発生した場合の措置に関する教養の状況 3 その他