情報セキュリティ規則

JAB S611:2021

第 4 版：2021 年 4 月 15 日
第 1 版：2011 年 1 月 1 日

公益財団法人 日本適合性認定協会

目次

第 1 章　総則

(目的)

第 1 条　この規則は、公益財団法人日本適合性認定協会（以下「本協会」という。）の情報セキュリティの確保を図るために必要な事項を定め、本協会が保有する情報に対する協会内外からの侵害の阻止、脅威を与える行為の抑止、情報の適切な管理、責任体制の明確化等によって、本協会の信頼を確固たるものにし、かつ、それを維持することを目的とする。

(定義)

第 2 条　この規則において、次の各号に掲げる用語の定義は、各号に定めるところのものとする。

(1)情報セキュリティとは、機密性(許可された者だけが情報にアクセスできる状態を確保することをいう。）、完全性（情報が破壊、改ざん又は消去されていない状態を確保することをいう。）及び可用性（許可された者が必要時に中断されることなく、情報にアクセスできる状態を確保することをいう。）を維持することをいう。

(2)情報という場合、紙媒体、電子媒体、業務上接する文字、図形、形状、画像、映像、言葉、音、匂い、感触、表情、雰囲気など、業務上での利用、取扱対象となるあらゆる形態のものを含む。

(3)情報資産とは、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子記録媒体に記録された情報及び情報システムを介して作成された書面に記載された情報並びに情報システム（情報システム開発、運用及び保守のための資料、知的蓄積等を含む。）そのものをいう。

(4)情報機器とは、コンピュータ（情報処理装置）及びコンピュータと接続して使用される情報記憶機器、媒体、接続手段、通信機器、電源機器及びそれらを収納、保護する設備、環境をいう。

(5)情報システムとは、情報を適切に保存、管理及び伝達させるための情報処理及び情報ネットワークに関するシステムで、本協会が保有又は管理しているシステム及び本協会との契約又は協定等に基づき提供されるすべてのものをいう。

(6)情報ネットワークとは、情報通信機器間を相互接続し、相互に情報を伝達しうるための情報通信網で、本協会が保有又は管理している情報通信網及び本協会との契約又は協定等に基づき提供されるすべてのものをいう。

(適用範囲)

第 3 条　この規則は、本協会の職務従事者(理事、監事、職員等、認定審査員等、業務受託者、派遣労働者及び臨時職員、並びに認定委員会委員等、本協会業務に携わり、機密情報に接する又は接する可能性のある者)に適用する。

(情報セキュリティ関連文書)

第４条　情報セキュリティ関連文書は、次の各号に定めるところによる。
(1)情報セキュリティ規則とは、本協会の情報セキュリティ管理上の方針を定めた文書であり、この規則のことを指す。
(2)情報セキュリティマニュアルとは、この規則に則り、本協会の情報セキュリティ管理、運用上の細部にわたる取扱いを定めた文書である。

第２章　協会の管理体制

(管理体制)
第５条　本協会の情報セキュリティを推進するため、情報セキュリティ総括責任者、情報セキュリティ実施責任者を置く。

(情報セキュリティ総括責任者)
第６条　本協会に、本協会における情報セキュリティに関する最高責任者として業務を総括させるため、情報セキュリティ総括責任者(以下「総括責任者」という。）を置き、事務局長をもってこれに充てる。
２　総括責任者に事故があるときは、総括責任者があらかじめ指名する者が、その職務を代行する。

(情報セキュリティ実施責任者)
第７条　本協会に、本協会における情報システムを適切に管理させるため、情報セキュリティ実施責任者(以下「実施責任者」という。）を置く。
２　実施責任者の職務は、次の各号に定めるところによる。
(1)総括責任者からの指示の実行
(2)各部門職制への情報セキュリティに関する指示
(3)総括責任者への実施状況等の報告
(4)本協会の情報システムのセキュリティ維持上の問題への対応
(5)本協会の情報セキュリティに関する自己評価及びマネジメントレビュー

(平常時の対応)
第８条　平常時における本協会の情報セキュリティに関する事項は、実施責任者が執行する。
２　次の各号に定める事項は事務局会議による審議を経て、確認、決定する。
(1)情報セキュリティに関連する規則等の策定・改廃
(2)情報システムの運用及び利用に関する方針
(3)緊急時における行動計画
(4)インシデント(意図的又は偶発的に生じる情報セキュリティを侵害する事件又は事故）の原因究明と再発防止策
(5)その他、必要とする事項

(緊急時の対応)

第 9 条　本協会に情報セキュリティに関する危機事象が発生又は発生の恐れがあり、かつ、対策を講じる必要があると総括責任者が判断した場合、又は実施責任者が判断しこれを総括責任者が承認した場合、総括責任者は自身を緊急時対策実行責任者に任じてリスク管理手順(S204)の適用の下に対策に取り組む。

2　前項の規定にかかわらず、総括責任者が不在の場合は実施責任者が、実施責任者も不在の場合はリスク管理手順の規定に従って就任可能な者が緊急時対策実行責任者の任に就く。

第 3 章　職務従事者の責務

(職務従事者の責務)

第 10 条　職務従事者は、情報セキュリティ関連文書に定める規則、ルールを遵守しなければならない。それら関連文書に定めなき事項については実施責任者に相談の上、上位となる方針に照らして判断、行動しなければならない。

2　本協会は、職務従事者に対して、情報セキュリティに係る認識と責務の自覚を確実なものとするため、誓約書を提出させるものとする。

3　本協会は、本協会が取り扱う情報に対して必要に応じて機密度を設定し、取扱いを制限するとともに、職務従事者はその指定に従って適切に取り扱わなければならない。

第 4 章　教育研修

(教育研修)

第 11 条　実施責任者は、本協会の情報を利用する職務従事者に対し、情報の取扱いについての理解を深め、情報セキュリティに関する意識の高揚を図るための啓発その他必要な教育研修を行う。

2　実施責任者は、情報システムの管理又は運用に関する業務に従事する職務従事者に対し、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。

3　各部門職制は、当該組織等の職務従事者に対し、情報セキュリティの確保のために、実施責任者の実施する教育研修への参加の機会を付与する等の必要な措置を講じる。

第 5 章　業務の委託

(情報システム運用の外部委託管理)

第 12 条　職務従事者は、本協会がその業務又は必要とする便宜・サービスの全部又は一部を第三者に委託又は外注する場合には、この規則及び契約取扱い手順（S511）に則って当該第三者による情報セキュリティの確保が徹底されるよう必要な措置

を講じる。

2　情報システムの管理又は運用に関する業務に従事する職務従事者は、本協会情報システムの開発、運用業務の全部又は一部を第三者に委託する場合には、その旨、当該第三者とのコンタクトに先立って実施責任者にこれを報告しなければならない。

第 6 章　安全確保上の問題への対応

(事案に係る報告、対処、記録等)

第 13 条　情報の漏えい、滅失、毀損等安全確保の上で問題となる事象を生ぜしめた、又はその発生を知った職務従事者は、速やかに所属する部門職制に報告しなければならない。なお、部門職制不在の場合、又は当該職務従事者が部門職制である場合は実施責任者に、更に実施責任者不在の場合は総括責任者に直接報告するものとする。

2　前項の報告を受けた部門職制は、直ちに実施責任者に報告するとともに、当該情報が他の部門の管理するものであるときは、直ちに、当該部門の部門職制に報告しなければならない。なお、前項の報告を受けた部門職制が特に重大と認める事案については、実施責任者へと同時に総括責任者に報告するものとする。

3　前項の報告を受けた総括責任者又は実施責任者が、特に重大な案件であり、緊急の対応を要すると認めた場合は、第 9 条(緊急時の対応)の規定に従う。

4　実施責任者は、発生した事案による被害の拡大防止及び復旧等のために、関係する部門職制に対応を指示するほか必要な措置を講じなければならない。

5　事案の発生に主として関係した職制等の管理責任者は、実施責任者の指示に基づき、速やかに事案にかかる事実関係及び被害状況等を調査し、実施責任者及びコンプライアンス責任者に報告しなければならない。なお、主として関係した職制等が判然としない場合は、実施責任者が報告を行う部門職制を指名する。
実施責任者、コンプライアンス責任者が調査内容及び対処状況に不足があると認めた場合は、関係する部門職制は、追加調査、追加対応等必要な措置をとり、改めて連絡書による報告を行うものとする。

6　関係する部門職制は、実施責任者の指示に従い、事案の発生した原因を分析し、再発防止のために必要な措置を講じる。

7　一連の対処プロセスの報告、記録は、内部監査、不適合管理、改善及びマネジメントレビュー実施手順 (QP901)に則り行う。

(公表等)

第 14 条　実施責任者は、発生した事案について即近の事務局会議に速報するとともに、調査内容、対処状況、再発防止等一連の関係情報をそれぞれとりまとまり次第、事務局会議に報告する。

2　総括責任者は、事案の内容、影響、普遍性等に応じて、事実関係及び再発防止策を事務局内又は職務従事者関係先に公表する。

また、事案の原因が職務従事者の重大な過失又は背任行為にある場合は、当該職務従事者への対応等の必要な措置を講じるものとする。

第７章　自己評価及びマネジメントレビュー

(自己評価)

第 15 条　実施責任者は、本協会の情報の媒体、処理経路、保管方法等について、定期に又は随時に自己評価を行い、必要があると認めるときは、その結果を、統括責任者に報告するものとする。

(マネジメントレビュー)

第 16 条　総括責任者は、情報セキュリティの維持、管理状況について、マネジメントレビュー実施手順に則ってレビューを行い、その結果を報告書に取りまとめるものとする。

(評価及び見直し)

第 17 条　総括責任者は、情報の適切な管理のための措置について、自己評価及びマネジメントレビューの結果等を踏まえ、実効性確保等の観点から評価し、必要があると認めるときは、その見直し等の措置を講ずるものとする。

第８章　雑則

(雑則)

第 18 条　この規則の運用にあたって生じた疑義、情報セキュリティの対策に関してこの規則に定めのない事項については、総括責任者の指揮の下に実施責任者が取扱いを定める。

(引用文書、関係様式)

第 19 条

文書番号	文書名
QP901	内部監査、不適合管理、改善及びマネジメントレビュー実施手順
S204	リスク管理手順
S511	契約取扱い規則
S691	情報セキュリティマニュアル

様式番号	様式名
SF01	誓約書

様式番号 JAB NF18 REV.0

改　定　履　歴（公開文書用）

版番号	改　定　内　容　概　略	発行日	文書責任者	承認者
1	新規発行	2011.01.01	総務部長	事務局長
2	第3条(適用範囲)の修正、S691情報セキュリティマニュアルの整合をとった	2012.02.15	総務部長	事務局長
3	第2条(定義)の記述整理 第3条(適用範囲)からの評議員の除外 第7条(情報セキュリティ実施責任者)から情報システムの技術的側面の職務を除外 第9条(平常時の対応)の事務局会議の執行機能を削除 第10条(緊急時の対応)の緊急時対策発動契機を整理 第14条(事案の報告等)、第15条(公表等)の記述を具体化 第20条(引用文書、関係様式)の新設	2015.04.07	総務部長	事務局長
4	第19条(引用文書、関係様式)の最新化 文書全体における職制表記の最新化	2021.04.15	情報セキュリティ実施責任者	事務局長

公益財団法人日本適合性認定協会
〒108-0014 東京都港区芝 4 丁目 2-3
NMF 芝ビル 2F
Tel.03-6823-5700 Fax.03-5439-9586