２３．監査標準

0.91 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.91 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.91 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

２３．監査標準

２３．１　趣旨

本標準では、マネジメントシステムの内部監査にかかわる事項を規定する。

２３．２　対象者

本標準は、情報資産を扱うすべての人を対象とする。権限および責務は以下のグループによって区別される。

・情報セキュリティ委員会およびその構成メンバ
・情報セキュリティ委員会から任命された監査組織、およびその監査人
・被監査組織および被監査人

２３．３　対象システム

本標準は監査に関するものであり、情報システムや情報機器を対象としない。

２３．４　遵守事項

２３．４．１　共通事項

（１）　情報セキュリティ委員会は、監査組織を構成し、定期的に監査を実施しなければならない。監査の周期は、１年に１回とする。監査の周期を変更する際には、情報セキュリティ委員会での承認を得なければならない。

（２）　情報セキュリティ委員会は、監査の対象、目的について、監査組織と協議した上で合意しなければならない。情報セキュリティ委員会は、合意した内容が監査の目的に合致しているかについての責任をもつ。

（３）　監査組織は、合意された内容に基づいて監査を実施し、その結果を情報セキュリティ委員会へ報告しなければならない。情報セキュリティ委員会は、監査の結果を受けて、必要に応じて適切な是正措置を行わなければならない。

（４）　監査組織は、被監査組織、対象に対して独立していなければならない。もし独立した監査組織を構成できない場合には、相互監査体制をとることでできる限り独立性を維持しなければならない。監査組織は、客観的に監査を行わなければならない。

（５） 監査組織は、監査の実施にあたり専門の知識や技能を必要とする場合、専門家の協力を得ることができる。監査組織は、監査の目的について専門家に説明し、専門家による作業の結果について最終的な判断を下すことができなければならない。
（６） 監査組織は、監査の過程において知りえた情報を、監査目的以外に公開してはならない。
（７） 被監査組織および被監査人は、監査の円滑な実施のために、スケジュール調整、資料の提示、監査立会い等、監査組織の活動に協力しなければならない。

２３．４．２　監査の計画

（１） 監査組織は、合意された監査内容に基づいて、監査の計画を立てなければならない。監査組織は、監査の目的として以下を含めなければならない。
・内部統制が正しく規定されているか
・規定された内容にしたがって組織が効率的に実行しているか
（２） 監査組織は、監査の計画にあたり以下の内容を検討または実施しなければならない。
・内部統制として実施されている活動内容
・資産およびそれらへのリスクの分析
・セキュリティ方針や標準等の規定の分析
・組織を取り巻く環境の変化
・内部統制を理解するためのヒアリングや観察
（３） 監査組織は、監査項目に以下の内容を含めなければならない。
・セキュリティ方針および標準
・情報セキュリティ委員会の構成および実行
・情報資産を含む財産の管理
・社員、契約社員等の扱い
・物理セキュリティ
・通信および運用
・アクセス制御
・システム開発
・事業継続計画
・法律、規制等への準拠
（４） 監査組織は、計画した監査項目のそれぞれについて、問題点が内在する可能性について検討し、予測される内部統制リスクを判断した上で、実施手

続きや監査のサンプリング密度を決定しなければならない。

（５） 監査組織は、監査の実施手順および項目について、主要な内容を文書化しておかなければならない。

２３．４．３　監査の実施

（１） 監査組織は、各監査人に対して監査の実施を指示する。

（２） 監査人は、あらかじめ決められた手続きに基づいて監査を実施する。監査手続きは以下を含む。

・インタビュー
・行動の観察
・証拠等の検閲
・監査人による作業手順の実施

（３） 監査人は、組織内で提供されているサービスの可用性を考慮しなければならない。

（４） 監査人は、システム監査ツールを使用するとき、システムへの影響に細心の注意を払わなければならない。監査時には、一般へのサービスは停止していることが望ましい。

（５） 監査人は、セキュリティ方針と、実際のマネジメント活動を比較して、有効性についての判断をしなければならない。判断する観点としては以下を含む。

・組織の存在意義とセキュリティ方針との整合性
・セキュリティ方針と標準の整合性
・標準の実行に関して使用している設備費用および運用費用等のコストとそれらの妥当性
・PDCA サイクルの適切な実施

（６） 監査人は、監査結果を裏付けるために、監査によって得られた情報を記録しなければならない。

（７） 監査人は、監査によって得られた情報を元に、内部統制リスクが予測範囲内であるかを評価し、実施手続きの妥当性を判断しなければならない。

（８） 監査組織は、監査人からの報告を受けて、発見された問題の量や質が予測範囲を超えており、実施した手続きが妥当でないと判断した場合には、再度監査計画を立案して実行しなければならない。

２３．４．４　監査結果の報告

（1） 監査組織は、監査結果を元に監査報告書を作成し、情報セキュリティ委員会へ報告しなければならない。監査組織は、対象者の不在、機密情報に関する閲覧の拒絶など、さまざまな理由によって実施できなかった監査項目を監査報告書に含めなければならない。
（2） 監査組織は、監査結果の裏付けとなる十分な根拠を提示できなければならない。
（3） 監査組織は、問題点の指摘事項を報告する場合、問題点の重大性に応じて分類しなければならない。監査組織は、問題点を解決するための改善策について、可能な限り監査報告書に含めることが望ましい。
（4） 監査報告書は、開示範囲を情報セキュリティ委員会のみとする。

２３．４．５　是正措置

（1） 情報セキュリティ委員会は、監査組織からの報告を受けて、是正措置の計画立案をし、実行の判断をしなければならない。
（2） 情報セキュリティ委員会は、実行することになった是正措置について、緊急性、および重要性を考慮して、適切な時期に行う。
（3） 是正措置の指示を受けた被監査組織または被監査人は、速やかに是正措置を行い、実施した是正内容および時期を情報セキュリティ委員会に報告しなければならない。

２３．５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

２３．６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

２３．７　公開事項

本標準は対象者にのみ公開するものとする。

２３．８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

＊＊＊用語集＊＊＊
内部統制リスク
システム監査ツール
PDCA サイクル