JQA 情報システム及び関連設備の運用基準

制定：２００９年　４月　１日
２版：２００９年　８月　１日
３版：２０１１年　４月　１日

一般財団法人　日本品質保証機構

JQA 情報システム及び関連設備の運用基準

次の事項について社内規程を整備するとともに、当該社内規程に従って事業所の管理及び情報システムの運用を実施すること。

1 事業所の組織体制

a) 事業所の組織体制を整備すること。特に情報システム及び関連設備の運用、データの管理等、安全対策に係る業務については、管理責任者及び担当者の責任体制を定めること。

b) 防災組織を設け、責任体制を定めること。

c) 防犯組織を設け、責任体制を定めること。

d) 監査組織を設けること。

2 情報システム安全対策に係る規程等の制定

2.1 入退管理

a) 入館・入室資格の付与

1) 役員及び職員には、写真入身分証明書を発行すること。

2) 他社の勤務者には、写真入勤務証を発行すること。

b) 入退館管理

事業所の出入口では、以下の入退館管理を行うこと。

1) 役員及び職員には、写真入身分証明書等により入館の資格を確認し、館内にあっては識別章を常時着用させること。

2) 他社の勤務者には、写真入勤務証等により入館の資格を確認し、館内にあっては識別章を常時着用させること。

3) 訪問者には、身元及び用件を確認の上入館を許可し、館内にあっては、識別章を常時着用させること。

4) 出入口の鍵は、定めた場所に保管し、管理は特定者が行うこと。

5) 解錠及び施錠の時間及び氏名を記録すること。

6) 不審者に対しては、持込み物品及び持出し物品の確認を行うこと。

7) 機械により入退管理を行う場合は、特定者が機械の操作及び保守の管理を行うこと。

c) 入退室管理

1) コンピュータ室、サーバ室、事務室、データ等保管室、電源室及び空気調和機械室への入室者を特定すること。

2) コンピュータ室、サーバ室、事務室及びデータ等保管室への入室者の資格確認は、次により行うこと。

2.1) 役員及び職員は、写真入身分証明書等により確認すること。

2.2) 他社の勤務者は、写真入勤務証等により確認すること。

3) コンピュータ室、サーバ室、事務室及びデータ等保管室への入退室者の氏名及び入退室時間を記録すること。

4) 出入口の鍵は、定めた場所に保管し、管理は特定者が行うこと。

5) 解錠及び施錠の時間及び氏名を記録すること。

6) 機械により入退管理を行う場合は、特定者が機械の操作及び保守の管理を行うこと。

7) コンピュータ室、サーバ室への搬出入物品は内容を確認すること。

2.2 **情報システムの運用管理**

a) 情報システムの操作方法、障害発生時の対処方法について定めたマニュアルを常備すること。

b) 情報システムへのアクセスの資格、権限を定めておくこと。

c) 情報システムの操作は特定者が行うこと。ただし、無人運転の場合は、非常時の処置を定めておくこと。

d) 情報システムの運転記録を作成し、運転状況を把握すること。

e) 情報システムの点検の結果及び修理の内容について把握すること。

f) パスワード、識別コード等の管理を適切に行うこと。

g) コンピュータ室、サーバ室への可燃物の持込みは必要最小限にすること。

h) 危険物及び燃焼器具は、コンピュータ室、サーバ室へ持ち込まないこと。ただし、保守又は工事のためのものは、この限りでない。

i) 情報システムを設置した室は禁煙とすること。

2.3 **データ等の保管管理**

a) データ等の取扱い及び受渡しは定めた方法によって行うこと。

b) データ等は常に定めた場所に保管すること。

c) データ等保管室へはデータ等及びこれらの管理に必要なもの以外の持込を禁止すること。

d) 保管管理は、特定者によって行い、定期的に保管状況を点検すること。

e) 管理記録を整備し、データ等の作成、追加、更新、廃棄等について十分把握すること。

f) 重要なデータ等を定め、次の措置を講ずること。

1) 使用（複写を含む）及び廃棄は、管理責任者の許可を得ること。

2) 保管場所は、データ等保管室の施錠可能なデータ等保管設備内とし、その鍵は、特定者が管理すること。

3) 分散保管等の必要な損壊防止措置を講ずること。

g) データ等保管室は禁煙とすること。

2.4 **電源設備、空気調和設備、防災設備及び防犯設備の管理**

a) 関連設備の取扱い方法、障害発生時の対処方法について定めたマニュアルを常備すること。

b) 関連設備の取扱いは、特定者に行わせること。

c) 関連設備の操作部には、定常状態を明示すること。

d) 関連設備の定期点検を実施すること。

2.5 **監視**

a) 火災、漏水等の異常警報については、常時監視を行うこと。

b) 事業所内を定期的に巡回し、異常状態の早期発見を行うとともに、関連設備の稼働状況を監視すること。

c) 亜鉛の導電性ヒゲ状結晶(Whisker：ウィスカ)の発生状況を監視すること。

d) 立地環境の変化に伴う災害および障害の発生の可能性を調査し、防止対策を講ずること。

2.6 **外部委託**

a) 情報システム及び関連設備の安全対策に関する項目を盛り込んだ契約等を締結すること。

b) 委託先における安全対策の実施状況を把握すること。

3 **情報システム安全対策に係る教育及び訓練**

a) 安全対策に係る規程の教育を実施すること。

b) 防災、防犯の訓練を実施すること。

4 **情報システム安全対策に係る監査**

a) 情報システム及び関連設備の安全対策に係る監査を実施すること。