管理の方法を明確にする。

（3）物理的セキュリティ

情報システムの設置場所について、不正な立ち入り、損傷及び妨害から情報資産を保護するため、情報機器設置区域を設置する等の物理的な対策を明確にする。

（4）人的セキュリティ

情報セキュリティに関する権限や責任を定め、全ての情報利用者にポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を明確にする。

（5）技術的セキュリティ

財団の情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の必要な対策を明確にする。

（6）運用

ポリシーの実効性を確保するため、セキュリティ情報の収集や対応方法、ポリシーの遵守状況の確認方法を明確にする。また、緊急事態が発生した際の迅速な対応を可能とするため、緊急時対応体制を明確にする。

（7）評価・見直し

ポリシー及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等を踏まえ、定期的に対策基準の評価・見直しを実施することとし、このために必要な措置を明確にする。

2．定義

このポリシーの用語の定義について、次のとおり定める。

（1）情報とは、情報システム内部に記録された情報（アクセス記録等を含む 。）、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関する書面情報をいう。

（2）情報システムとは、情報処理及び通信に係るシステムをいう。ハードウェア及びソフトウェア、ネットワーク並びに記録媒体で構成される。

（3）情報資産とは、前二号に定める情報及び情報システムをいう。

（4）機密性とは、アクセスを許可された者だけが、対象の情報にアクセスできる状態を確保することをいう。

（5）完全性とは、情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

（6）可用性とは、情報へのアクセスを許可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。

（7）脅威とは、情報資産に影響を与え、損失を発生させる直接の要因をいう。不正アクセスによる情報の改ざんや破壊、ウィルス感染、過失による情報

の漏洩や破壊などを含む。
（8）情報セキュリティインシデントとは、財団の情報セキュリティを侵そうとする事柄の発生事象をいう。
（9）機器等とは、情報機器又はソフトウェア若しくは情報機器とソフトウェアの総称をいう。
(10) 記録媒体とは、情報機器から取り外しすることが可能な記録装置 （磁気テープ、磁気ディスク、光ディスク、カセットテープ、ＭＯ、フロッピーディスク、ＵＳＢメモリ等）をいう。
(11) 財団職員等とは、役員、規程集第5編人事によって規定される全ての職員、及び派遣労働者をいう。
(12) ユーザーとは、財団で管理する情報資産を取り扱うSPring-8及びSACLAの共用ビームラインを利用契約等により利用する者をいう。
(13) 外来者等とは、外部委託業者等で、契約等により財団の情報資産を取り扱うことを許可された者をいう。
(14) 情報利用者とは（2）に規定する情報システムを利用する財団職員等、ユーザー及び外来者等をいう。

３．対象範囲

ポリシーの対象範囲は、財団が管理する情報資産（賃借、保管を含む。）とし、人的範囲は財団職員等、ユーザー及び外来者等とする。また、業務遂行のために情報システムを利用する場合は、その情報システムが財団の管理対象であるかどうかに関わらずこの規程の対象とする。

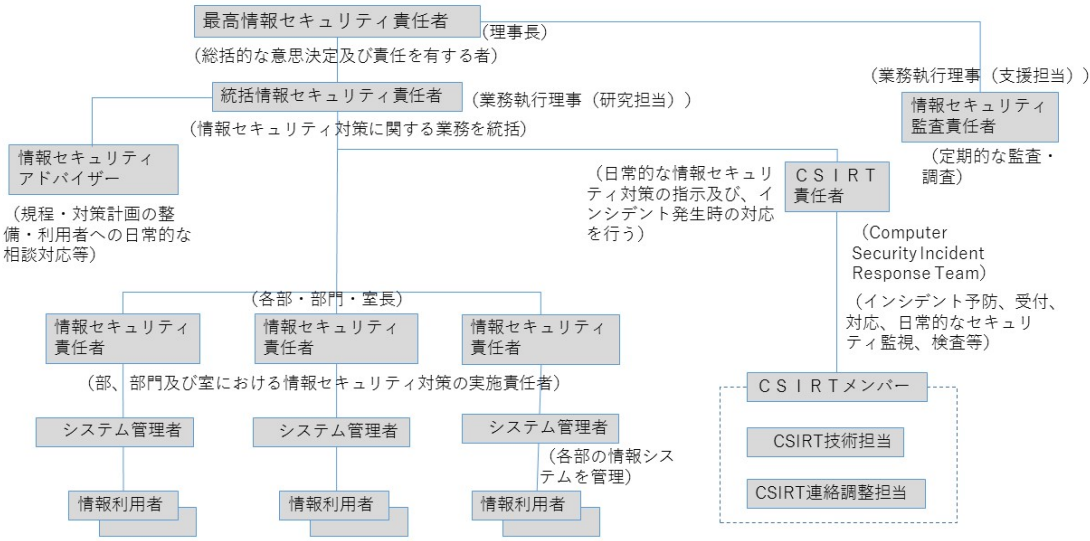
４．ガイドラインの作成

財団のポリシーの下に、情報セキュリティガイドラインを作成する。

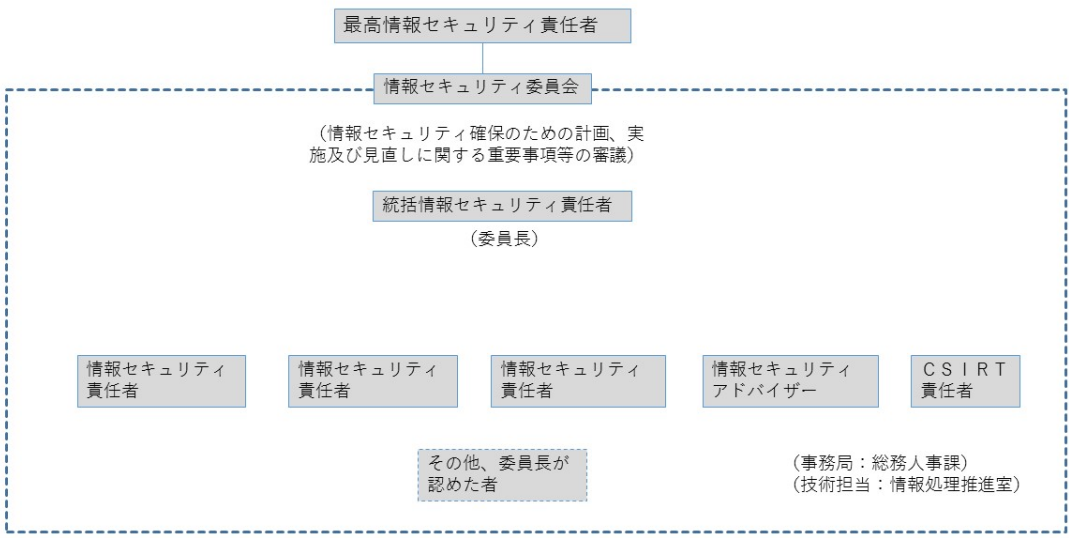
Ⅱ情報セキュリティ対策基準

１．組織・体制

ＪＡＳＲＩ情報セキュリティ体制



情報セキュリティ委員会



１．　１　最高情報セキュリティ責任者
（１）情報セキュリティに関する総括的な意思決定及び責任を有する者として、財団に最高情報セキュリティ責任者を置く。
（２）最高情報セキュリティ責任者は、理事長がこれにあたる。

１．　２　統括情報セキュリティ責任者
（１）財団に統括情報セキュリティ責任者を置く。
（２）統括情報セキュリティ責任者は、業務執行理事（研究担当）とする。
（３）統括情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐し、財団における情報セキュリティ対策の実施に関する業務を統括し、情報利用者に対する指揮にあたる。
（４）統括情報セキュリティ責任者は、情報セキュリティインシデント発生時の緊急時連絡体制を整備する。

１．３　情報セキュリティ責任者
（１）財団の部、部門及び室毎に情報セキュリティ責任者を置く。
（２）情報セキュリティ責任者は、各部・部門・室長がこれにあたる。
（３）情報セキュリティ責任者は、部、部門及び室における情報セキュリティ対策の実施に関して業務を統括し、実施責任を有する。
（４）情報セキュリティ責任者は、部、部門及び室の情報資産を守るために必要と判断したときは、当該情報システムの緊急停止、ネットワークからの遮断等の緊急措置をとることができる。

１．４　情報セキュリティ監査責任者
（１）情報セキュリティに関する法令、規程等が遵守されていることを検証するため、 財団に情報セキュリティ監査責任者を置く。
（２）情報セキュリティ監査責任者は、業務執行理事（支援担当）とする。
（３）情報セキュリティ監査費任者は、最高情報セキュリティ責任者の指示に基づき、情報セキュリティ監査に関する業務を統括する。

１．５　情報セキュリティアドバイザー
（１）情報セキュリティについて専門的な知識及び経験を有する者として、財団に情報セキュリティアドバイザーを置く。
（２）情報セキュリティアドバイザーは、統括情報セキュリティ責任者が指名する。
（３）情報セキュリティアドバイザーは、以下の業務を行うものとする。
　１）情報セキュリティ関係規程等の整備に係る助言
　２）教育実施計画の策定に係る助言
　３）情報システムに係る技術的事項に係る助言
　４）情報セキュリティ委員会への参加
　５）財団職員等に対する日常的な相談対応

6）情報セキュリティインシデントへの対処の支援
7）前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

1．6　CSIRT責任者
（1）財団において発生した情報セキュリティインシデントに対処するため、財団にComputer Security Incident Response Team（以下「CSIRT」という。）責任者を置く。
（2）CSIRT責任者は、統括情報セキュリティ責任者が指名する。

1．7　CSIRT
（1）情報セキュリティインシデントに対処するための専門的な知識または適性を有する者から構成するCSIRTを置く。CSIRT構成員はCSIRT技術担当及びCSIRT連絡調整担当で構成され、CSIRT責任者が推薦し、委員会で選任する。
（2）CSIRTは、情報セキュリティインシデントに対処するため、以下の業務を行うものとする。
1）情報セキュリティ監視
2）情報セキュリティインシデントの未然防止策の実施
3）本人又は発見者からの情報セキュリティインシデント報告の受付
4）情報セキュリティインシデントの統括情報セキュリティ責任者への報告
5）被害の拡大防止を図るための応急措置の指示又は勧告、及びこれらに係る体外的な連絡
6）セキュリティ検査（脆弱性診断と改善対策の実施）

1．8　情報セキュリティ委員会
（1）財団に情報セキュリティ委員会（以下 「委員会」という。） を置く。
（2）委員会は、統括情報セキュリティ責任者、情報セキュリティアドバイザー、情報セキュリティ責任者及びCSIRT責任者で構成される。
（3）委員会の委員長は、統括情報セキュリティ責任者とする。
（4）委員長は、第２号の他、必要と認めたものを参加させることができる。
（5）委員会は 、次の各号に掲げる事項について審議する 。また、必要に応じて最高情報セキュリティ責任者に意見具申することができる。
1）情報セキュリティ確保のための計画、実施及び見直しに関する重要事項
2）その他財団の情報セキュリティに関する事項
（6）委員会の事務局は、研究支援部総務人事課が行う。また、技術担当業務を情報処理推進室が行う。

1．9　情報システム管理者
（1）情報セキュリティ責任者は、所管する情報システムの管理業務において、必要に応じて情報システム管理者を置くことが出来る。
（2）情報システム管理者は、情報セキュリティ責任者の指示により、当該情

報システムが健全に運用できるよう、情報セキュリティ対策を実施する。

２．情報の分類と管理

２．１　情報の管理責任

（１）管理責任

財団の情報は、当該情報を作成した各部署等が管理責任を有する。ただし、別の規定がある場合はそれに従う。

（２）情報利用者の責任

財団の情報を利用する情報利用者は、情報の分類に従い利用及び管理する責任を有する。

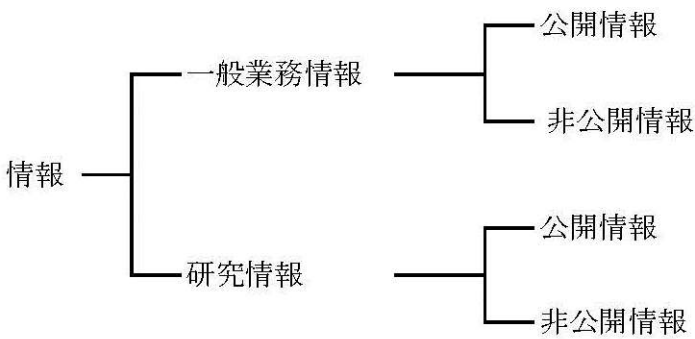
（３）重要性の効力

財団の情報が複製又は伝送された場合には、当該複製も分類に基づき管理しなければならない。

２．２　情報の分類と管理

（１）情報の分類

財団の情報は、財団運営に係る一般業務情報と研究に係る研究情報に大別できる。さらに、それぞれの情報はセキュリティの観点から情報セキュリティ責任者が、公開情報と非公開情報に分類する。



（２）情報の管理

１）公開情報

・　公開情報は任意の場所からアクセス可能な性質を持つため、改ざん等の防止策を講じることは勿論、個人情報の漏洩、プライバシーの侵害や知的所有権及び著作権の侵害に十分注意しなければならない。

２）非公開一般業務情報

・　非公開の一般業務情報を扱うネットワークは、研究開発用の一般ネットワークと論理的に異なる必要がある。

・　許可されたもの以外が、コンピュータ及び記録媒体等の非公開一般業務情報を取り扱ってはならない。

３）非公開研究情報

・　非公開の研究情報は、個々の研究者あるいは研究グループの管理下

で、適切なアクセス制限を行うなどして改ざんや漏えい等に十分注意しなければならない。

4）アクセス制限

・　情報について、それぞれの分類と情報利用者の範囲を考慮し、適切なアクセス権限を設定しなければならない。

5）情報の原本性

・　情報の原本は、適切なアクセス権限の設定等により、情報の原本性を保証しなければならない。

・　公開情報は改ざんのへの対策を講じなければならないが、常に進化する不正アクセス技術の脅威に対し、改ざんを受けた場合の速やかな回復機構を備え、情報の原本性の維持に務めなければならない。

6）非公開情報の取り扱い

・　情報利用者は、情報セキュリティ責任者の許可がある場合を除き、非公開情報の持ち出し及び送付をしてはならない。

・　非公開情報を所外で扱う場合には情報セキュリティ対策のなされた環境で行い、情報漏洩に注意しなければならない。

7）記録媒体の管理

・　取り外しが可能な記録媒体は、適切な管理を行わなければならない。

・　非公開情報を記録した記録媒体を、部署内から外部に持ち出す場合には、情報セキュリティ責任者の許可を得なければならない。

・　非公開情報を記録した記録媒体は、適切な場所に保管しなければならない。

8）情報機器及び記録媒体の処分

・　情報機器及び記録媒体が不要となった場合は、その処分方法に十分注意しなければならない。一般的な記録媒体は、通常の消去操作では管理情報のみが消去されるだけでデータ自体は消去されず情報の復元が可能である点に十分配慮し、復元できないような対策を行った上で廃棄しなければならない。

3．物理的セキュリティ

3．1　サーバ機器等

（1）サーバ機器の定義

サーバ機器とは、複数のクライアント機器等（3．2参照）からアクセスされ、財団内外にサービスを提供する情報システムである。

（2）情報機器設置区域の設定

1）サーバ機器は設定された情報機器設置区域に設置しなければならない。

2）情報機器設置区域内はサーバ機器の重要度に応じて、動作保証内温度、湿度を２４時間保たなければならない。

3）情報機器設置区域は、制御機能、鍵、警報装置等によって許可されていない者の立ち入りを防止できなければならない。

（3）装置の取り付け等

サーバ機器の取り付けを行う場合は、火災、水、埃、振動等の影響を可能な限り排除した場所に設置し、固定等の必要な措置を施さなければなら

ない。

（4）電源

1）サーバ等の機器の電源については、可能な限り当該機器を適切に停止するまでの間に重要度に応じて十分な電力を供給できる容量の予備電源を備えなければならない。

2）落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

（5）配線

サーバ等の機器の配線は、損傷等を受けることがないように可能な限り必要な措置を施さなければならない。

（6）多重化

ダウンタイムを短くすることを求められる重要なサーバ機器については、多重化を検討しなければならない。

3．2　クライアント機器等

（1）クライアント機器の定義

クライアント機器とは、主として個人的な利用で用いられ、サーバ機器へアクセスすることで処理を進めていく情報システムである。

（2）外部に設置する機器

1）財団外で使用する財団資産のクライアント機器については、外部持ち出しについて情報セキュリティ責任者の許可を得なければならない（4．2参照）。

2）財団外で使用する財団資産のクライアント機器については、財団外での使用方法を定め、適切に管理しなければならない。

（3）外部から持ち込まれる機器

情報利用者が外部より持ち込んだクライアント機器を使用する場合は、財団のポリシーを遵守し、許可した者にのみネットワークを利用させなければならない。

（4）クライアント機器の利用

クライアント機器を利用して財団の情報システムにアクセスする場合には、許可されたサービス以外にアクセスしてはならない（4．1参照）。

3．3　ネットワーク機器等

（1）ネットワーク機器の定義

ネットワーク機器とは、ルーターやスイッチ、ファイアウォール装置などネットワークシステムを構成する機器である。

（2）設置場所の秘匿

バックボーンを構成するネットワーク機器をはじめ、重要と思われるネットワーク機器については、その設置場所を限られた情報システム管理者以外に公表してはならない。

（3）コンソールポートの隔離

ルーター、インテリジェントスイッチ等は、コンソールポート、管理ポートを許可された情報システム管理者以外は使用できないように施錠などによって物理的に隔離された区域に設置しなければならない。

（4）ネットワークケーブル

1）バックボーンを構成するケーブルは、故意又は過失によるケーブル切断を防ぐためのシールド等の措置を施さなければならない。

2）ネットワークの接続口（スイッチのポート等）は、管理者以外が配線を変更、追加できないように必要な措置を講じなければならない。

（5）多重化

機器障害によるネットワーク断が重大な影響を及ぼすようなネットワーク機器については、多重化による信頼性の向上を検討しなければならない。

4．人的セキュリティ

4．1　役割・責任

（1）最高情報セキュリティ責任者

1）最高情報セキュリティ責任者は、全ての情報セキュリティに関する総括的な権限と責任を有する。

2）最高情報セキュリティ責任者は、統括情報セキュリティ責任者を通じて、全ての部署にポリシーの遵守を励行させる。

（2）統括情報セキュリティ責任者

1）統括情報セキュリティ責任者は、財団内の情報セキュリティに関する権限と責任を有する。

2）統括情報セキュリティ責任者は、ポリシーの遵守を励行するために、関係部署と協議の上、財団内の情報セキュリティの保持と強化について検討し物理的ならびに人的体制等を調整する。

（3）情報セキュリティ責任者

情報セキュリティ責任者は、部署内の情報セキュリティについての調整と実務を行う。

（4）情報利用者

1）全ての情報利用者は、当該ポリシーを遵守しなければならない。

2）情報利用者は、情報システム（財団内外の情報システムを含む）を利用する場合には、許可されたアクセス以外は行ってはならない。

3）すべての情報利用者は財団内外を問わずファイアウォール等の制限を意図的に回避する行為をしてはならない。

4）情報利用者は、使用する端末や記録媒体について、第三者に使用されること又は許可なく情報を閲覧されることがないように、適切な措置を施さなければならない。

5）情報利用者は、個人的に利用している電子メールアドレス宛に業務に係わる重要な情報を転送してはならない。ただし、情報セキュリティ責任者が許可した場合はその限りではない。

6）情報セキュリティ対策について不明な点、遵守することが困難な点等については、情報セキュリティ責任者に相談し、指示等を仰がなければならない。

7）情報利用者は、知り得た情報を異動後および退職後においても外部に漏らしてはならない。

４．２　研究開発・利用支援業務上の必要性の配慮

（１）情報セキュリティ対策について研究開発・利用支援業務上の利便性を著しく損なう点、遵守することが現実的に困難な点については、委員会に対し、ポリシー及びガイドラインの改善を求めることができる。

（２）情報利用者は、情報セキュリティ責任者の許可を得ずに非公開情報や非公開情報が保存されたノートパソコン等を財団外に持ち出してはならない。情報セキュリティ責任者は、研究開発・利用支援業務上の必要性に配慮して、情報利用者に対して適当な期間を設け持ち出し許可を与えることができる。情報セキュリティ責任者が持ち出す場合には統括情報セキュリティ責任者の許可を必要とする。

（３）財団外のコンピュータ等を財団のネットワークに接続する場合、情報セキュリティ責任者の許可を得た上で、情報利用者に別に定める申請書を提出させるとともに、本ポリシー、情報セキュリティガイドライン等に従って使用すること。

４．３　教育・研修

（１）統括情報セキュリティ責任者は、教育訓練等の実施により、役員を含めすべての情報利用者に対しポリシーについて啓発しなければならない。

（２）情報セキュリティ責任者は、財団職員等に職務の内容に応じた講習会等の情報セキュリティ教育を受講させる等、啓発向上を支援しなければならない。

（３）情報利用者は、ポリシー及びガイドラインを理解し、情報セキュリティ上の問題が生じないように務めなければならない。

４．４　法令遵守

情報利用者は、職務の遂行において使用する情報資産について、次の法令を遵守し、これに従わなければならない。

・不正アクセス行為の禁止等に関する法律
・著作権法
・個人情報の保護に関する法律等

４．５　外来者等の受入

情報セキュリティ責任者は、外来者に情報及び情報システムを利用させる場合には、情報セキュリティの確保のために必要な措置を講じたうえで利用させなければならない。

５．技術的セキュリティ

５．１　ＩＰアドレスの管理

財団で取得したIPアドレスを、財団の目的以外に使用することは禁止する。

５．２　パスワードの管理

自己のパスワードは秘密としセキュリティの確保を十分担保するものに

しなければならない。

5．3　コンピュータ及びネットワークの管理

（1）アクセス記録の取得・管理

1）情報システム管理者は、アクセス記録及びセキュリティ関連事案に関する記録を取得し、一定の期間保存しなければならない。

2）アクセス記録が窃取、改ざん、消去されないように必要な措置を施さなければならない。

3）情報システム管理者は、定期的にアクセス記録を分析、監視しなければならない。

（2）システム管理簿等の管理

1）情報システム管理者は、行ったシステム変更等の処理について、記録を作成し、適切に管理を行わなければならない。

2）情報システム管理者は、情報利用者から報告のあった情報、情報システムの障害に対する処理又は通信システムの問題等は、障害記録として体系的に記録し、常に活用できるよう保存しなければならない。

（3）情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図、情報システム仕様書については、記録媒体、紙媒体にかかわらず、業務上必要とする者のみが閲覧できる場所に保管しなければならない。また、情報システムに記録する場合には業務上必要とする者のみがアクセスできるようにしなければならない。

5．4　アクセス制御等

（1）利用者登録

情報システム管理者は、情報利用者の登録情報の管理、ファイルアクセス権の付与等について厳重に管理しなければならない。

（2）管理者権限

情報システムの管理者権限は、情報システム管理者にのみ与え、厳重に管理しなければならない。また、管理者権限を使用する場合には、必要最小限の時間とするなど、慎重に行わなければならない。

（3）サーバのアクセス制御

1）財団内外にサービスを提供するサーバは、ファイアウォールあるいはファイアウォールと同等の機能で防御し、アクセス制限、サービスの制限、プロトコル制限等を行わなければならない。

2）サーバへのアクセス許可は、必要最低限にしなければならない。

5．5　サーバの監査

（1）CSIRTは、財団内外にサービスを提供するサーバのセキュリティについて、定期的に監査しなければならない。

（2）財団内外にサービスを提供するサーバは、CSIRTの実施するサーバ監査を受験し、サービス開始の許可を得なければならない。

（3）情報システム管理者は、CSIRTの監査でセキュリティ問題が発見された

場合は速やかに問題解消の措置を行わなければならない。

５．６　コンピュータウィルス等セキュリティ対策

（１）情報セキュリティ責任者は、財団の情報資産について、十分なセキュリティ対策を施さなければならない。

（２）財団で使用するクライアント機器、サーバ等は、ウィルス対策ソフトを必ずインストールし、ウィルスパターンファイル等を常に最新の状態を維持し続けなければならない。

（３）情報セキュリティ責任者は、ウィルス情報について情報収集し情報利用者に対する注意喚起を行わなければならない。

６．運用

６．１　セキュリティ情報の収集及び対応

（１）情報セキュリティ責任者は、セキュリティに関する情報を収集し、情報資産を守らなければならない。

（２）情報システム管理者は、セキュリティに関する通知や情報に従い、システムやアプリケーションのパッチアップ作業を行いセキュリティ問題の解消に努めなければならない。

６．２　ポリシーの遵守状況の確認

（１）統括情報セキュリティ責任者及び情報セキュリティ責任者は、ポリシーが遵守されているかどうかについて、また、問題が発生していないかについて、積極的に確認を行わなければならない。

（２）情報利用者は、ポリシーの違反が発生した場合は、直ちに部署内の情報セキュリティ責任者に報告しなければならない。情報セキュリティ責任者は、それがただちに情報セキュリティ上重大な影響を及ぼす可能性があると判断される場合には、緊急時連絡体制に従ってCSIRTに連絡を行わなければならない。

６．３　緊急時の連絡及び体制

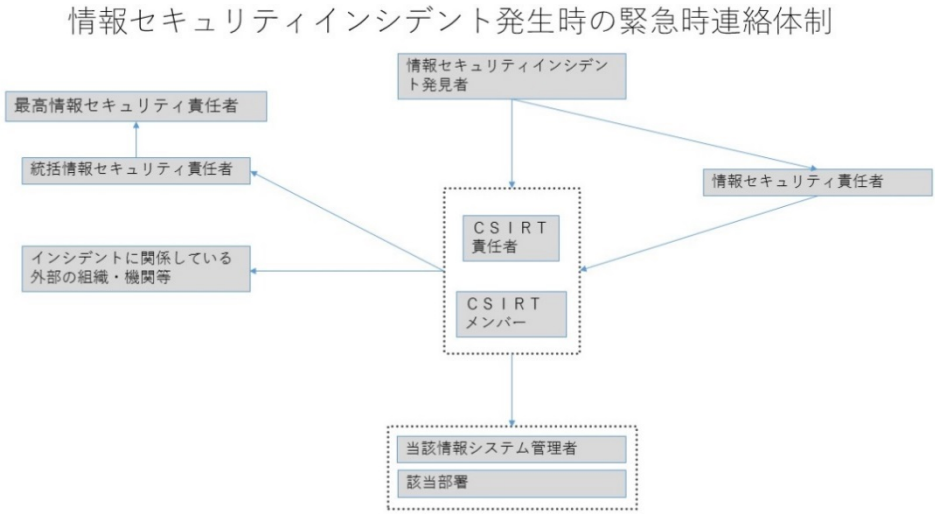
（１）情報利用者は、情報セキュリティに関する事故、システム上の不審な動作、公開情報の改ざん等の事故を発見した場合には、直ちにCSIRT責任者、CSIRTメンバー及び情報セキュリティ責任者に報告しなければならない。

（２）CSIRT責任者は、報告のあった事故について、緊急時連絡体制に従って、直ちに当該情報システム管理者、当該情報セキュリティ責任者及び統括情報セキュリティ責任者に連絡しなければならない。

（３）CSIRTと当該情報システム管理者及び当該情報セキュリティ責任者は相互に連絡を取り、必要な措置を講じなければならない。

（４）統括情報セキュリティ責任者は、報告のあった事故について最高情報セキュリティ責任者に報告しなければならない。

（５）CSIRTは、インシデントの解消を行うため、インシデントに関係している外部の機関に連絡及び相談を行わなければならない。



（６）CSIRTは、これらの事故を分析し、再発防止のための情報を収集し、再発防止について検討し統括情報セキュリティ責任者に報告しなければならない。
（７）統括情報セキュリティ責任者は、再発防止の検討報告を受け、必要に応じて委員会を開催し、予算的な措置等の必要な対策について検討しなければならない。

６．４　外部委託等

（１）情報システムの開発・保守担当する外部委託事業者及び外部委託事業者から下請けとして受託する業者が、財団内の情報システムを使用する場合には財団のポリシーを遵守させなければならない。
（２）情報システムの開発・保守担当する外部委託事業者及び外部委託事業者から下請けとして受託する業者が、委託業務に係わって知り得た財団の情報については守秘させなければならない。
（３）外部委託等の契約時にはポリシーの遵守、守秘義務等については協議し必要な場合には覚書あるいは契約書による明文化等を検討しなければならない。

７．評価及び見直し

７．１　監査

（１）情報セキュリティ監査責任者によるセキュリティ及び情報システムの監査を定期的に行わなければならない。
（２）情報セキュリティ監査責任者は監査の結果を委員会及び最高情報セキュリティ責任者に報告しなければならない。

７．２　ポリシーの更新

（１）情報セキュリティ委員会は、ポリシーの実効性を評価し、必要な部分の見直し、内容、時期について検討しなければならない。

（2）情報セキュリティ委員会は、新たに必要な対策が発生した場合、あるいは監査の結果及び点検の結果を踏まえ、ポリシーの更新について検討しなければならない。
（3）ポリシー更新の内容については、十分なものについては、委員会で検討し最高情報セキュリティ責任者が承認しなければならない。

7．3　例外措置

業務遂行上、情報セキュリティポリシーの例外措置適用が必要となる場合には、最高情報セキュリティ責任者による例外の適用承認を受けなければならない。