学校法人昌平黌情報セキュリティポリシー

Ⅰ　情報セキュリティポリシーの基本方針

（１）基本方針

学校法人昌平黌に所属する東日本国際大学、いわき短期大学および法人本部（以下「本学」という）における学術研究・教育活動を高めるために情報基盤の整備を図るとともに、教育・研究部門、事務部門の情報資産のセキュリティを確保する。（注：ここでいう情報資産とはICTにより保存された情報機器上の情報データをいう）

（２）目　的

①　本学内や学外の情報セキュリティに対しての侵害を阻止する。

②　学内外の情報セキュリティを損ねる加害行為が発生した場合には、最小限に止められるように抑止する。

③　学内の情報資産に関して重要度による分類を行い、それに見合った管理を行う。

④　本学構成員の情報セキュリティに関する情報の取得を支援する。

（３）対象範囲

①　本ポリシーの対象範囲は、本学の情報資産に加えて、本学以外のコンピュータで本学のネットワークに一時的に接続されたコンピュータを含む。

②　本ポリシーの対象者は、本学教職員、非常勤教職員、委託業者、学生、研究員、来学者（以下「利用者」という）とする。

Ⅱ　組織・体制

（１）最高情報セキュリティ責任者は東日本国際大学学長とし、全学の情報セキュリティに関する総括的な意思決定を行う。対外的対応を必要とする事象が生じた場合には、下記システム管理責任者と協議のうえ、対応にあたる。

（２）システム管理責任者はいわき短期大学学長、東日本国際大学学部長、留学生別科長、法人事務局長とし、最高情報セキュリティ責任者を補佐する。

（３）システム責任者・システム担当者

各部局のシステム責任者は、それぞれの部局の長とする。システム責任者はシステム担当者を任命する（システム責任者本人でも良い）。システム担当者は、システム責任者と連携し各部局内の情報システムの維持・管理を行い、電算室との連携をは

かる。なお、研究室においては各教員がシステム責任者とシステム担当者を兼任する。

（４）電算室（室長・室員）

全学情報システムの管理を行い、対外的対応を必要とする事象が生じた場合には被害状況を把握し情報セキュリティ対応班（下記）に報告する。

（５）情報セキュリティ対応班

上記（１）（２）（４）から構成される情報セキュリティ対応班を置く。

情報セキュリティ対応班の役割については、以下に定める。

（別記１「組織の構成図」）

Ⅲ　情報セキュリティ対応班の役割

（１）不正アクセス等への対応

①　情報セキュリティ対応班は、外部または内部からの不正アクセスを検出した場合、関連する通信の遮断または該当する情報機器の切り離し、状況把握および回復を実施する。必要に応じて対外的な対応を行う。

②　不正アクセスが継続する場合、当該情報機器またはそれを接続するネットワークについて、定常的な利用の停止など抑止措置をとることができる。

③　学内からの不正アクセスによって学外に被害を及ぼし、その事実関係の説明を被害者、第三者から求められた場合、このほか情報セキュリティ上、対学的な対応が必要となった場合の手順は別記２「学外への対応手順」とする。

④　大学構成員がセキュリティポリシーに違反し、学内外に甚大な被害を与えた場合、理事会・教授会等へ状況を報告することができる。

（２）セキュリティポリシーの策定・更新

全学の情報セキュリティに関し基本的なセキュリティポリシーを策定し、必要に応じて更新を行う。

（３）情報セキュリティの啓蒙

情報セキュリティに関する啓発および教育について、システム責任者およびシステム担当者に対する教育を行なうとともに一般の利用者にも幅広く教育を行なう。

（４）情報セキュリティ上の重要事項の審議

上記（１）（２）（３）の他、情報セキュリティ上の重要事項を審議する。

Ⅳ　情報セキュリティ対策と手順

（１）情報の分類と管理

①　学内のそれぞれの部局において、情報の公開・非公開の分類を定めること。
（注：ここでいう非公開情報とは、万一学外に流出した場合、学内外に対し甚大な被害をもたらすことが考えられる情報をいう。）

②　非公開情報を許可された者以外がコンピュータや記憶媒体に保管してはならない。また、一時的であっても、教職員が日常的に使用するコンピュータに非公開情報を不特定の者が読み取り可能な状態で複製してはならない。

③　情報の原本は、ＣＤ－ＲＯＭ／ＣＤ－Ｒ等の書き換え不能な媒体に保存するなど、原本性を保証しなければならない。

④　非公開情報を学外に持ち出してはならない。

（２）物理的セキュリティ

①　クライアント機器

クライアント機器とは、おもにパーソナルな利用で用いられ、他の情報機器へアクセスすることで処理を進めていくものをいう。

イ．本学内にクライアント機器を設置する場合は、学外へ持ち出されることのないよう管理部局により何らかの対策を施すこと。

ロ．新たにクライアント機器を増設する場合には、所定のガイドライン（別記３「学内ネットワーク接続の手続き」）に沿っていないものは接続してはならない。

ハ．クライアント機器利用者は、常に最新のセキュリティパターンを取得し、機器のアップデートを図る。

ニ．クライアント機器には、原則として個人所有の機器を用いてはならない。職務上止むを得ず接続する場合は、以下のことを守らなければならない。

１）機器には最新の（ウィルス駆除ソフト）が使用できる契約が結ばれていること。

２）学内の情報の保存と学外へ持ち出しを禁止

３）業務を含め不必要に学外のネットワークに接続しない。

ホ．クライアント機器の廃棄は所有部局・研究室が責任をもって行う。以下の廃棄手順を守らなければならない。

１）備品管理管轄部局へ申請書（廃棄）を提出する。

２）すべての情報を復元が困難な状態にするため、以下のいずれかの方法を実施すること。

ａ．データ消去のソフトウェアを利用する。

ｂ．専門業者のデータ消去サービスを利用する。

ｃ．ハードディスクや記憶媒体を物理的に破壊する。

② サーバ

サーバとは、複数のクライアント機器からアクセスされ、共同で利用される情報機器（物理サーバ）およびその上で稼働する個別のサービス提供ソフトウェア（仮想サーバ）をいう。

イ．サーバ（物理・仮想）ごとにシステム担当者を定めること。
ロ．サーバへアクセスできるクライアントは必要最小限とすること。
ハ．ネットワーク保守管理のため、サーバに不必要なサービスは立ち上げない。
二．セキュリティ対策を施すこと。
ホ．サーバ上のデータはサーバ（物理・仮想）ごとにシステム担当者が定期的にバックアップを行うこと。
ヘ．サーバ機器が管理区域から持ち出されないよう対策を施すこと。
ト．サーバ機器の廃棄は専門業者による「廃棄処理証明書」をとること。

③外部記憶媒体

外部記憶媒体とは、クライアント機器あるいはサーバに補助的に接続して使用し、携帯が可能な外付けハードディスク、USB メモリ、記録型 DVD 等をいう。

イ．外部記憶媒体を使用する際は、最新のウィルス駆除ソフトが入っているクライアント機器で使用するなど、ウィルスに感染しないよう十分配慮すること。
ロ．外部記憶媒体に非公開情報を記録する際は、その外部記憶媒体を暗号化する等の手段を講じ、第三者がその外部記憶媒体を手に入れることがあったとしても中に入っているデータを閲覧できないようにすること。それが困難な事情がある場合は、紛失、盗難等のないよう物理的な管理に十分配慮すること。
ハ．外部記憶媒体の廃棄および他者への提供（再利用）の際は、情報漏えいのないよう復元が困難な状態にすること。

（３）人的セキュリティ

① アクセス制限

イ．システム責任者はシステム担当者と連携して、情報の内容に応じて情報にアクセス可能な利用者を定めなければならない。ＩＤ・パスワードなどにより利用制限をすること。
ロ．利用者は、アクセス権のない情報システムや情報に入り込もうとしてはならない。意図的でなく入り込んだときは、速やかにアクセスを切断すること。

② 利用管理

すべての教職員および学生は、セキュリティポリシーを遵守しなければならない。また、情報セキュリティを維持する義務を有する。

イ．システム責任者・システム担当者からセキュリティ維持管理のために協力を依頼された場合には従わなければならない。

ロ．自己のパスワードは秘密としなければならない。

ハ．他の利用者のアカウントを使用してはならない。

ニ．他の利用者のパスワードを聞きだしてはならない。

ホ．システム責任者・システム担当者がパスワードの変更を求めた場合、利用者はそれに従わなければならない。

ヘ．システム管理権限を有するものや利用者になりすました第三者からのパスワードの聞き取りには応じてはならない。

ト．学生は本セキュリティポリシーを遵守すると同時に、別に定められた利用規程に基づき利用しなければならない。

（別記４：「学生利用のセキュリティポリシー」）

（４）事故・障害の報告および対応

① 利用者は情報セキュリティに関する事故、情報システムへの不正アクセス、情報の改ざん、システム上の障害および誤動作、ウィルス感染の疑いを発見した場合には、システム責任者・システム担当者および電算室に直ちに報告しなければならない。

② 報告を受けたシステム担当者および電算室は、連携して後日の調査に備え発生時の状況に関する記録を作成、一定期間保存し、重大な事故については情報セキュリティ対応班に報告するとともに、迅速に対応しなければならない。

③ 報告および対応についての手順は別記５―１、５―２とする。

（５）ネットワーク管理

学内のネットワーク管理者として、全学ネットワークについては電算室が、各部局内ネットワークについては各部局のシステム責任者と連携しつつシステム担当者がこれにあたる。ネットワーク管理者は、以下のことを実施し適切にネットワークを管理しなくてはならない。

① 利用資格者以外に情報端末のアカウントを発行してはならない。また、利用資格を失った者のアカウントを適切に処理しなければならない。

② 定期的なデータのバックアップを行うと同時に、一定期間のログの保存を行う。

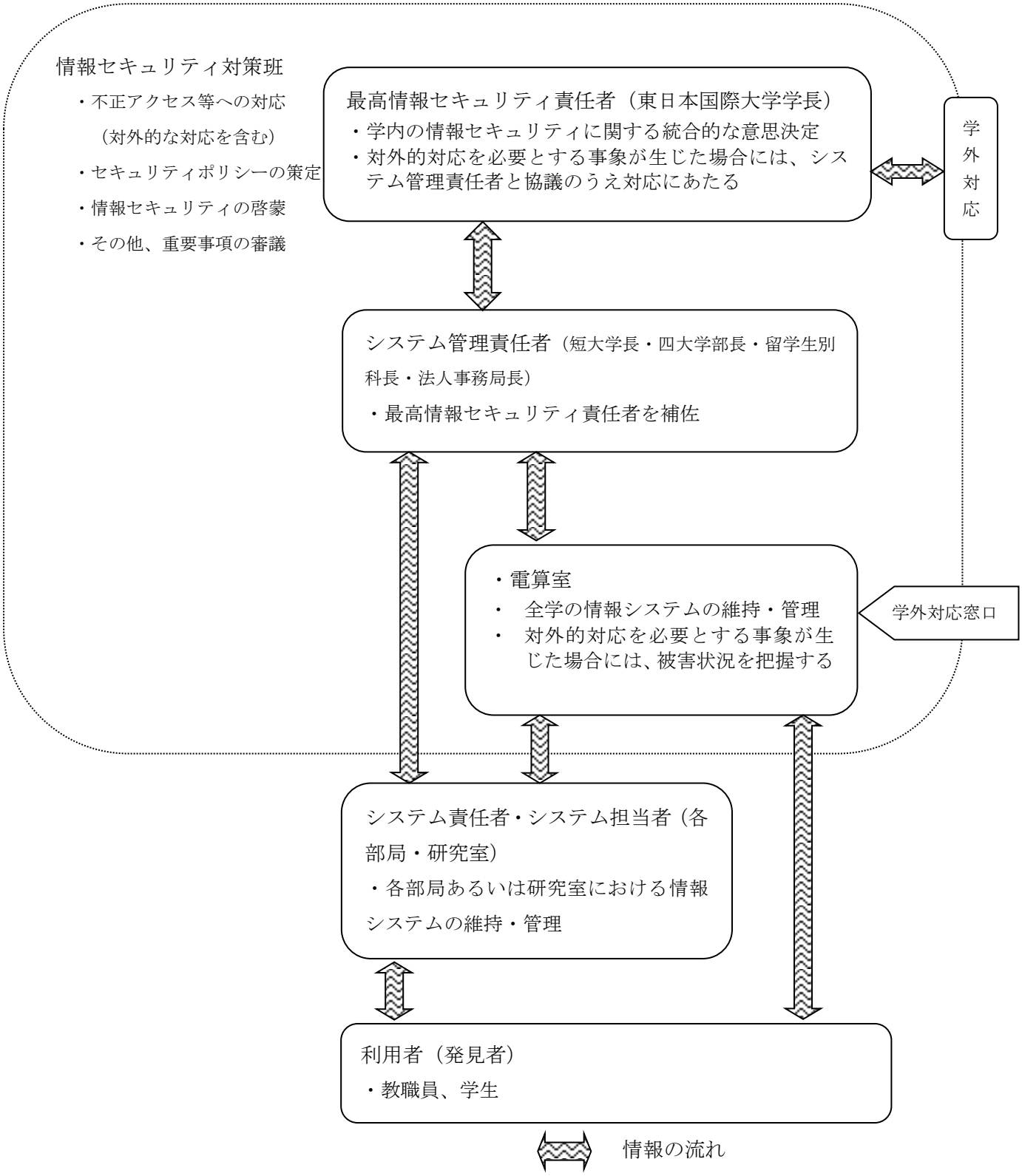
③ ネットワークを監視し、障害の発生あるいはその疑いのある場合は状況を早急に把握し、上司に報告、対策を講じる。

Ⅴ　情報セキュリティポリシーの更新

本情報セキュリティポリシーの情報社会への適合性を検討し、必要に応じて更新する。

Ⅵ　この情報セキュリティポリシーは　平成１６　年　４　月　１　日から実施する。
この情報セキュリティポリシーは　平成２１　年　４　月　１　日から実施する。
この情報セキュリティポリシーは　平成２６年　１０　月　１　日から実施する。

（別記）１　　**組織の構成図**


情報セキュリティ対策班
・不正アクセス等への対応
（対外的な対応を含む）
・セキュリティポリシーの策定
・情報セキュリティの啓蒙
・その他、重要事項の審議
最高情報セキュリティ責任者（東日本国際大学学長）
・学内の情報セキュリティに関する統合的な意思決定
・対外的対応を必要とする事象が生じた場合には、システム管理責任者と協議のうえ対応にあたる
学外対応
システム管理責任者（短大学長・四大学部長・留学生別科長・法人事務局長）
・最高情報セキュリティ責任者を補佐
・電算室
・　全学の情報システムの維持・管理
・　対外的対応を必要とする事象が生じた場合には、被害状況を把握する
学外対応窓口
システム責任者・システム担当者（各部局・研究室）
・各部局あるいは研究室における情報システムの維持・管理
利用者（発見者）
・教職員、学生
情報の流れ

（別記）２

学外（第三者）への対応手順

学内から学外へ被害を及ぼした場合に、被害者または第三者から事実関係の説明を求められた場合の対応手順については以下のとおりとする。

１．電算室は、学外へもたらした被害の状況を正確に、詳細に把握する。

２．被害の内容から、学内の加害者となった利用者の判明に努めると同時に通信ログの解析等を行う。（場合によっては外部に委託する）

３．電算室は被害状況をセキュリティ対応班に報告する。

４．セキュリティ対応班は加害者となった利用者に事実確認を行う。

５．最高情報セキュリティ責任者は、情報セキュリティ対応班を招集し、システム管理責任者および本学関係者と協議のうえ第三者への対応にあたる。

（別記）３

学内ネットワーク接続の手続き（ガイドライン）

１）接続申請書の提出

電算室書類「ネットワーク接続申請書」提出

現在のIPアドレスの使用状況によってはネットワーク構成の変更をお願いすることがあります。

2）ネットワーク機器設置

ＬＡＮケーブル、HUＢ等の準備（研究室・部局単位で対応）

3）設　定

①学内ネットワーク接続の設定　（部局または電算室にて対応）

②ウィルス駆除ソフトのインストール、最新パターンの確認

③ＯＳアップデート

④ブラウザ・メーラーの設定

※ 所定の数以上のＩＰアドレスを必要とする場合、サブネットとする。

※ サブネットの場合、サーバ機器のセキュリティについても十分に考慮する。

（別記）４

学生利用のセキュリティポリシー

本学学生は以下のことを遵守しなければならない。

学内のクライアント機器を利用する際には

・備え付けの機器、通信機器、ケーブルに破損を加えないこと

・自己のパスワード管理を行い紛失しないこと

・他のパスワードを使用しないこと

・学内外において利用権限のない情報について故意的にアクセスを行わないこと

・ウィルス感染が疑われるサービスを利用しない、またウィルスに感染した可能性がある場合はすみやかに電算室に報告すること

・学外で利用した媒体（USB フラッシュメモリ、ＳＤカードなど）を持ち込み利用する場合はウィルス感染に十分注意すること

・学習に必要とするもの以外はダウンロードを実施しないこと

・個人所有のアプリケーションソフト等をインストールしないこと

・学内外への不正にアクセス、大量パケットを送信等、セキュリティに違反する加害活動を行わないこと。

・電算室より学内に掲示される警告・注意、呼び出しに従うこと

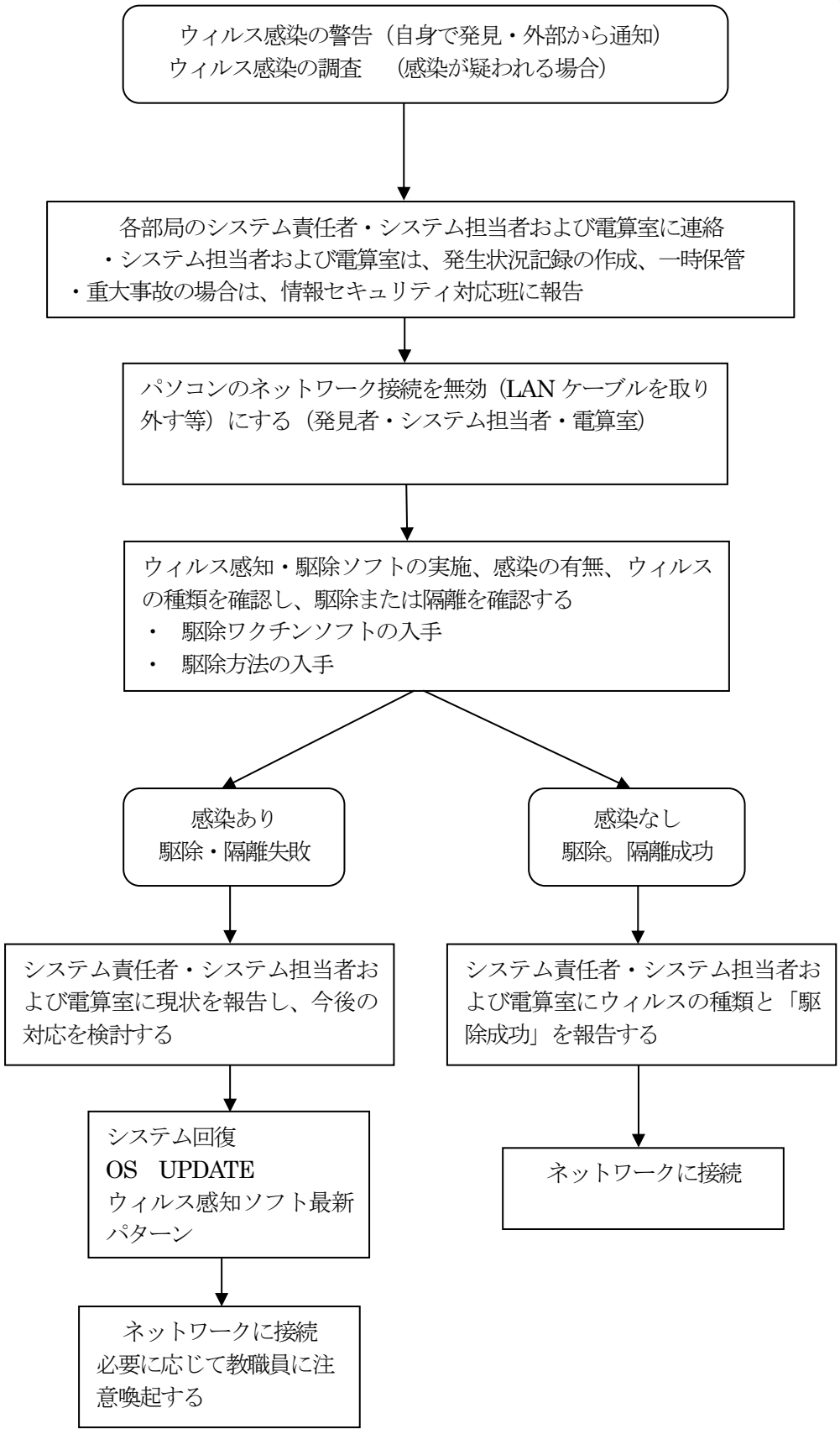
・他の利用者の迷惑にならないよう十分注意すること

・上記のセキュリティポリシーに違反した場合は、利用を停止し、しかるべき処分を受ける場合がある

（別記）５－１

クライアントにおけるウィルス感染発生時の対応

①



（別記）５－２

サーバにおけるクラッキング発生時の対応

②