情報セキュリティ緊急時対応手順書

令和５年４月

長岡技術科学大学　情報統合管理会議

目　次

■ **変更履歴**

令和５年４月１日	制定

序　本書の目的と構成

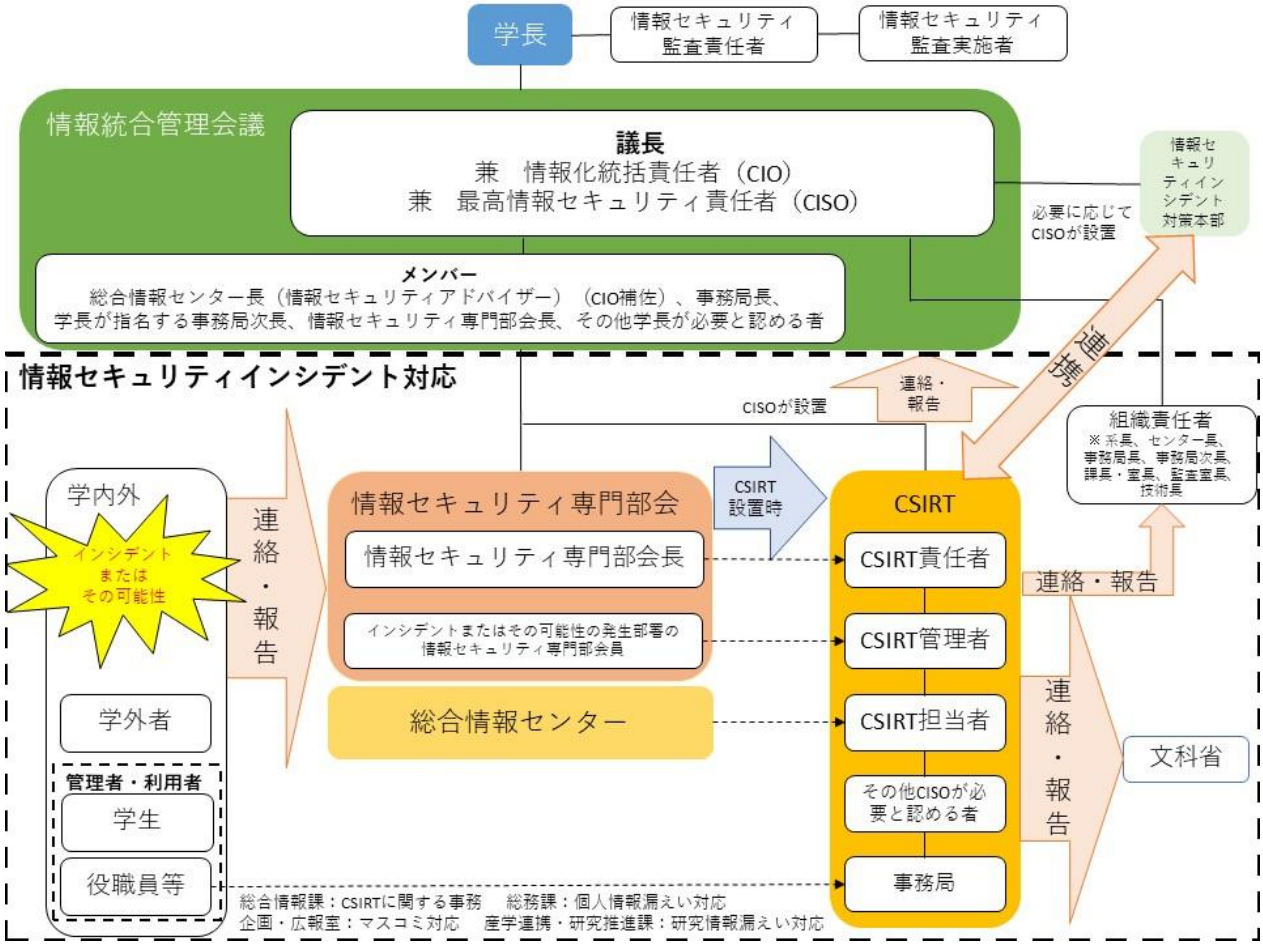
本手順書は、本学が管理する情報システムが正常に動作しない場合、又は情報資産に対する脅威が発生した場合（以下「情報セキュリティにおける緊急時又は緊急時」という。）に、被害の未然防止、又は被害の拡大防止及び早期復旧を図るために必要な手順について定めることを目的とする。

<< 共通編 >>

1　CSIRT の設置

情報セキュリティポリシーの及ぶ範囲に関わる情報セキュリティインシデント（以下「インシデント」という。）に、迅速かつ適切に対応するため、インシデント対応への即応力、専門的知見、情報統合管理会議において迅速かつ的確な意思決定を行うために必要な情報の収集力等を具備した緊急即応チームとして、CSIRT（本学において発生した情報セキュリティインシデントに対応するため、本学に設置された体制をいう。Computer Security Incident Response Team の略。以下「CSIRT」という。）を設置する。

学内情報セキュリティ体制における CSIRT の位置付を以下に示す。



2　体制と責務

CSIRT の体制及び責務は次のとおりとする。

体制	情報セキュリティポリシー上の役割名
CSIRT 責任者	情報セキュリティ専門部会長
CSIRT 管理者	（インシデント発生部署の）情報セキュリティ専門部会員

CSIRT 担当者	総合情報センター及び CSIRT 管理者が指名する者
その他 CISO が必要と認める者	本学システムの開発・保守・運用委託先、データセンター、IPA、JPCERT/CC 等、必要に応じて協力・情報提供を要請
事務局	総合情報課、大学戦略課企画・広報室、総務課、産学連携・研究推進課

（1）CSIRT 責任者

・CSIRT 責任者は、インシデント対応の責任者として、インシデント対応の作業を監督し評価する責任を負う。

・ほかの組織などとの調整役となり、危機を打開し、チームに必要な要員・リソース・技能を確保する。

（2）CSIRT 管理者

・CSIRT 管理者は、チームのリーダーとして、CSIRT 担当者の作業を調整し、CSIRT 担当者からの情報を収集し、インシデントに関する最新情報を必要な関係者に提供する。

・インシデント調査・分析全体に係るプロジェクトマネジメント等を行う。

（3）CSIRT 担当者

・CSIRT 担当者は、インシデント発生時の、インシデント分析及び対処法の検討、関係部署との調整を行う等、インシデントに対応する CSIRT を、実務的な観点から中核として活動する。

（4）その他 CISO が必要と認める者

・外部委託先として、システムベンダー（開発事業者、運用・保守事業者等）、ISP、ASP、クラウド事業者等契約関係のある事業者から CSIRT 責任者が支援を要請する者。

・外部委託先は、検査・分析、証拠の取得・保全・確保・記録、インシデントの封じ込めと根絶、復旧措置、再発防止策の検討等に係る一部作業を行う。

・外部専門家として、セキュリティベンダー、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）セキュリティセンター、JPCERT コーディネーションセンター（JPCERT/CC）、警察等から CSIRT 責任者が支援を要請する者。

・外部専門家は、検査・分析、証拠の取得・保全・確保・記録、インシデントの封じ込めと根絶、復旧措置、再発防止策の検討等に係る作業を行う。

（5） 事務局

インシデント対応における事務局の関係部署は以下のとおり。

・総合情報課は、関係各課の協力を経て、CSIRT に関する事務を処理する。

・大学戦略課企画・広報室は、マスコミ対応等を行う。

・総務課は、個人情報漏えい対応を行う。

・産学連携・研究推進課は、研究情報漏えい対応を行う。

3　CSIRT の連絡網

インシデント発生時の速やかに関係者と連絡、情報交換を行うとともに、迅速な対応をとるため、あらかじめ以下に示す連絡先（担当者名、メールアドレス、電話番号、携帯番号、FAX

等）を明確にしておくものとする。

（1）自 CSIRT

（2）CSIRT に関係する事務局関係各課

（3）外部委託先

（4）外部専門家

IPA セキュリティセンター

JPCERT/CC

（5）関係省庁

文部科学省、個人情報保護委員会、国立情報学研究所（NII）、新潟県警察

4　CSIRT 並びに情報セキュリティ専門部会の役割

CSIRT の役割は（1）、並びに情報セキュリティ専門部会の役割は（2）のとおりとする。

（1）インシデント発生時の対応

a）インシデントレスポンス

初動対応（対応方針の検討、証拠の取得・保全・確保・記録、インシデントの封じ込め・根絶）の実施、復旧措置（暫定対応）の実施及び再発防止策（恒久対策）の検討を行う。

b）報告・公表

被害状況や影響範囲等に応じ、内外の関係者（情報統合管理会議、最高情報セキュリティ責任者（CISO）、インシデントが発生した部署の組織責任者、文部科学省、個人情報保護委員会、NII、新潟県警察等）への報告及び対外的な対応（報道発表、関係者への連絡）を行う。

c）事後対応

インシデントの収束宣言を行い、報告書をまとめる。

（2）平常時の事前準備・予防等

a）インシデント発生時の対応に必要な事前準備・予防

b）インシデントの発生を想定した訓練・演習の定期的な実施

c）インシデントレスポンス手順等の定期的な評価・見直し（自己点検）

d）その他情報セキュリティ専門部会長が定めるもの。

5　対象インシデント

CSIRT が対応するインシデントは、以下のとおりとする。

a）ネットワーク系インシデント

b）物理的インシデント

c）盗難・紛失インシデント

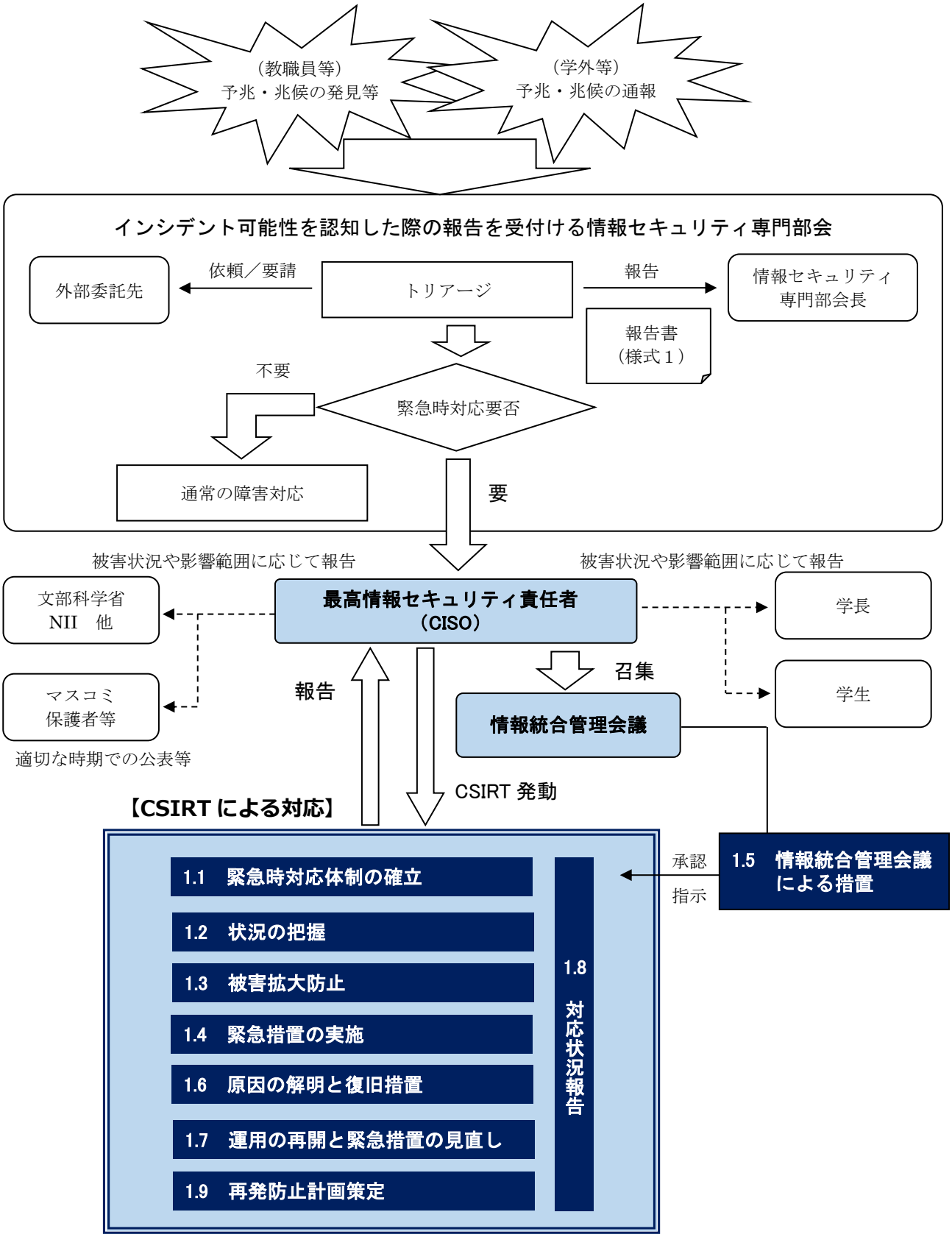
d）外部（（クラウド）サービスインシデント）

各インシデントの詳細は、国立大学法人長岡技術科学大学情報セキュリティ管理運用の取扱い第 6 章運用第 4 節情報セキュリティインシデントへの対応 6 -33 に記載のとおりとする。

≪インシデント別対応手順≫

1　ネットワーク系インシデント

ネットワーク系インシデント発生時の対応手順を以下に示す。



図中の各手順（1.1～1.9）について次頁以降に示す。

1.1 緊急時対応体制の確立

ａ）CSIRT 責任者は CSIRT を招集し、緊急事態宣言をし、全学横断的な協力体制が得られるようにする。

ｂ）インシデントの種類に応じて、対応できる関係者に特定したインシデントの内容を伝え、対応を依頼する。外部委託先に対応依頼をする場合は、必ず対応方法の確認をとる。

ｃ）CSIRT 責任者は、CSIRT 管理者及び CSIRT 担当者に対し以下の対応を指示する。

1.2 状況の把握

（1）詳細情報の把握

ａ）CSIRT 管理者は、不正アクセス等の詳細情報を把握するために次の対応を取る。

・不正アクセス等に係る情報を集約する。

・関係部署と連携して事象の調査・分析を実施するとともにインシデントによる影響範囲を特定する。

（2）連絡・指示

ａ）データ保護等に支障が生じ、又は生じるおそれがあるときは、不正アクセス等の状況、支障の程度等を、CSIRT 責任者、CISO 及びインシデントが発生した部署の組織責任者に報告する。

ｂ）CSIRT 責任者は、必要に応じて学生、役職員等への対応等について指示を行う。

ｃ）CSIRT 責任者は、文部科学省、NII その他関係機関相互に連絡調整を行い、被害状況を把握するための措置等の対応を依頼する。

ｄ）CSIRT 責任者は、被害により影響を受ける者からの問合せ等が想定される場合は、その連絡受付窓口を設置し、公表する。

1.3 被害拡大防止

CSIRT 責任者は、直ちに CSIRT 管理者に対し、データ保護等について必要な指示を行い、当該指示を受けた CSIRT 管理者は、次のとおり被害拡大措置を実施する。

ａ）緊急措置の実施にあたっては、学内関係各部署と連絡調整を図り、被害拡大を防止するための措置等、必要な協力を要請する。

ｂ）必要に応じて、システムの停止（機能の一部停止、機器の一部切り離し、学内 LAN からの切り離しを含む。）を行う。

ｃ）必要に応じて、関係者からの報告の徴収、関係者への調査、保有情報の廃棄等必要な措置を講じる。

1.4 緊急措置の実施

ａ）CSIRT 責任者は、学内関係各部署と連絡調整を図るとともに、緊急措置を実施するよう指示する。

ｂ）CSIRT 管理者は、直ちに原因の解明を行い、その対策の実施について、CSIRT 責任者、CISO 及びインシデントが発生した部署の組織責任者に報告する。

c）CISO は、個人情報、研究情報への脅威が生じる可能性が高いと判断したとき、その他必要があると認めるときは、速やかに学長に報告を行うとともに、その対策について協議するため、情報統合管理会議を招集する。

d）CISO は、CSIRT 責任者に、情報統合管理会議において不正アクセス等の状況、原因、対応策等を報告させるものとする。

1.5 情報統合管理会議による措置

a）CISO は、情報統合管理会議を招集する。

b）CSIRT 責任者は、情報統合管理会議において、インシデントの状況、原因、支障の程度等を報告するとともに、緊急措置等についてその承認を得るものとする。

c）情報統合管理会議は、以下の項目について協議し、協議結果は学長に報告するとともに、承認を得る。

【情報統合管理会議における協議事項】

決定する項目	内　容
システムの停止	・システムの完全停止、機能の一部停止 ・機器の一部切り離し ・学内 LAN からの切り離し
関係機関への連絡	・文部科学省、個人情報保護委員会 ・NII、新潟県警察等
技術的支援依頼	・JPCERT/CC ・保守委託会社等
詳細な被害状況・復旧作業の把握	・システムの具体的な被害状況 ・個人情報への侵害度合い、範囲 復旧に要する作業、期間等
緊急時体制の確立	・役割分担、指揮命令系統の確認
学生への対応	・来訪者への対応・ホームページ等での告知 ・問合せ対応・苦情処理
広報対応	・情報資料提供 ・記者発表等
代替措置の実施	・業務ごとにシステムが停止した場合の措置を検討し、当該措置を実施する。
緊急措置の見直し判断	・追加措置 ・復旧作業等緊急時対応の進捗状況 ・恒久対策の立案等
運用再開の決定	・障害復旧状況及び個人情報の整合性等の報告を受け、運用再開の決定を行う。

1.6 原因の解明と復旧措置

（1）原因の再確認

a）CSIRT 管理者は、必要に応じて、学内関係各部署と協力し、収集したアクセスログ等により原因を再確認する。

b）インシデントによる影響範囲については、時系列（過去、現在、将来）での影響、情報提供者に対する影響、利用者に対する影響、業務処理に対する影響等を考慮し、影響による被害を修復する対応策を検討する。

（2）復旧作業の実施

a）CSIRT 管理者は、インシデントの原因を取り除き、業務が継続できるように対応策を実施する。

b）必要に応じて外部委託先に依頼する。

1.7 運用の再開と緊急事態解除

（1）運用再開

a）CSIRT 管理者は、情報の整合性を確認し、修復した後、CISO、CSIRT 責任者及びインシデントが発生した部署の組織責任者の承認を経て、運用を再開する。
ただし、CSIRT においてシステム停止等の決定を受け、その後運用を再開する時は、情報統合管理会議に対し、障害復旧状況及び情報の整合性確認結果等の報告を行い、運用再開の決定を受けなければならない。

b）運用再開に当たっては、必要に応じて、アクセス権限の設定変更、端末操作者の識別コードの再発行、学生向けサービスの停止解除等を実施する。

（2）緊急事態解除宣言

a）CSIRT 管理者は、影響を受けた部署、利用者等関係者へ正常稼動の連絡をする。

b）CSIRT 責任者は、インシデント対応完了を確認し、緊急事態解除宣言を行う。

（3）報告

c）CSIRT 責任者は、インシデントによる関係者への対応状況等について情報統合管理会議に報告する。

1.8 対応状況報告

インシデント対応状況について速やかに関係者と連絡、情報交換を行うとともに、迅速な対応をとるため、対応中も適時、以下に従い連絡、報告を行うものとする。

a）CSIRT 管理者は、状況や事態が推移する都度、報告書（情報セキュリティ緊急時対応計画　報告様式１）を作成し、CSIRT 責任者を通して、関係者へ報告する。

b）インシデント対応の最終結果は、CSIRT 責任者を通じて、学長、CISO 及びインシデントが発生した部署の組織責任者に報告する。

c）インシデント対応の詳細報告とは別に、復旧状況連絡を関係部署に徹底する。

d）報告は、インシデントの内容、対応の期間等を考慮して行う。

e）報告は、少なくとも、以下の段階で実施するようにする。

- 被害拡大防止策実施時
- 緊急措置実施時
- 復旧措置実施時

なお、緊急時対応で実施した事項等については、可能な限り詳細に記録し、総合情報課にて保管する。

1.9　再発防止計画策定

CISO は、インシデントの解消後、再び同様の原因でインシデントが発生しないように、必要に応じて、再発防止のための対策を検討及び計画し、実施することを関係者に指示する。

再発防止計画の策定・実施は、次の手順に沿って推進する。

なお、（2）～（5）について、CISO が情報セキュリティインシデント対策本部を設置した場合は、CSIRT と情報セキュリティインシデント対策本部が連携して対応すること。

（1）真因追求

・インシデント発生の真の原因を突き止める。

・インシデント発生の直接原因､そのまた原因等できるだけ深く追求し､真因を究明する。

（2）再発防止策検討

・把握した真の原因を取り除くための対応策を検討する。

・仕組み（設備、システム、制度）面での対応策、運用（要員、教育）面での対応策等を検討する。

（3）再発防止計画策定

・再発防止が計画的に実施できるようにする。

・計画では、必要資源等を明確にする。

・可能なら、実施スケジュール等を明確にする。

（4）再発防止計画承認

・再発防止計画の実施には、資源（予算、要員、設備等）が関わるため、学長及び情報統合管理会議の承認を得るようにする。

（5）再発防止計画実施

・再発防止計画に従って作業を実施する。

・作業が長期にわたる場合は、確実に進捗管理を行う。

（6）効果確認・報告

・再発防止計画が終了した時点で、問題がないことを確認する。

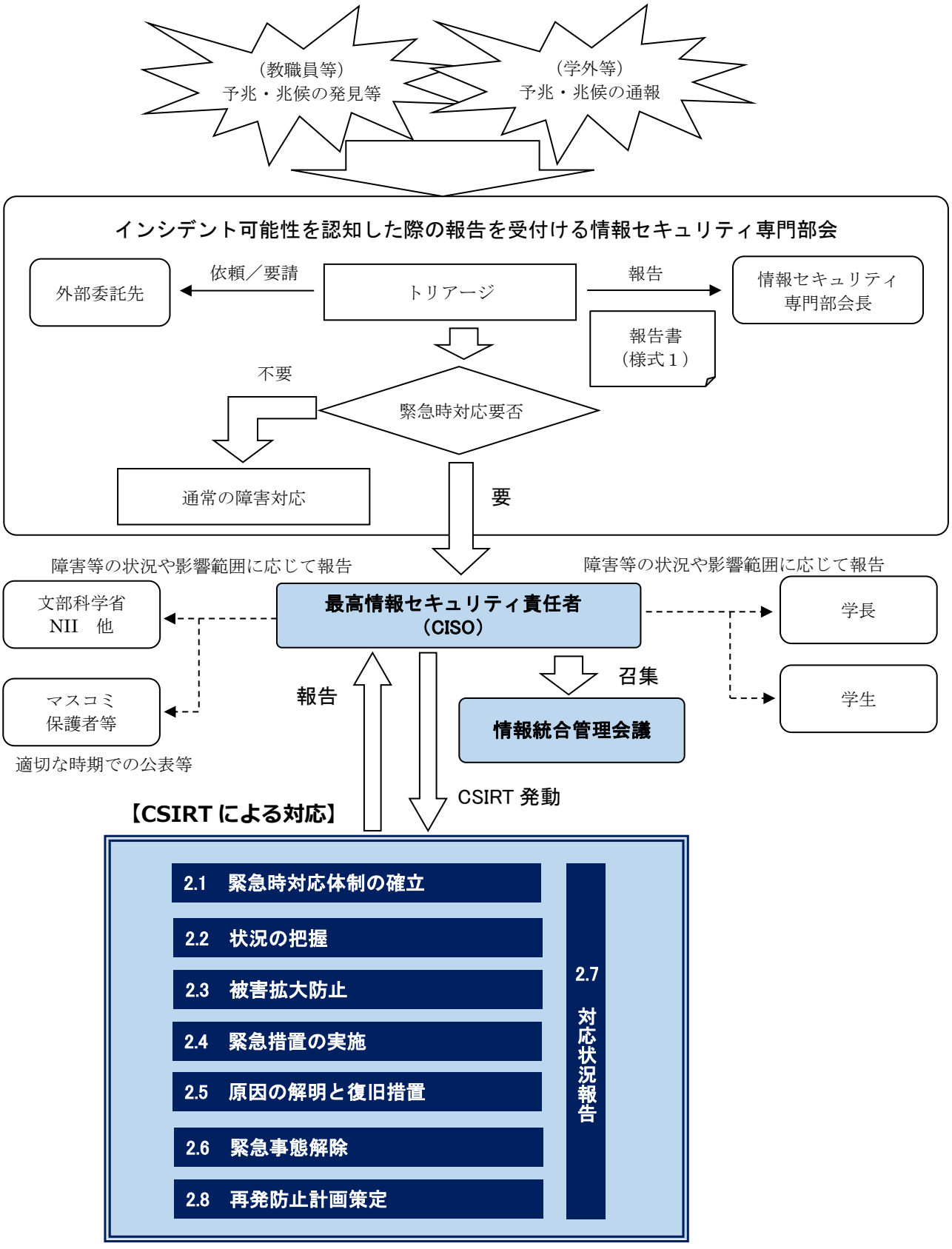
・再発防止計画の実施結果の効果を関係者に報告する。

（7）変更事項の徹底

・再発防止計画の実施によって、業務の運用方法等が変更になった場合は、その関係者に変更事項を周知徹底する。

2　物理的インシデント

物理的インシデント発生時の対応手順を以下に示す。



図中の各手順（2.1～2.8）について以下に示す。

2.1 緊急時対応体制の確立

a）CSIRT 責任者は CSIRT を招集し、緊急事態宣言をし、全学横断的な協力体制が得られるようにする。

b）インシデントの種類に応じて、対応できる関係者に特定したインシデントの内容を伝え、対応を依頼する。外部委託先に対応依頼をする場合は、必ず対応方法の確認をとる。

c）CSIRT 責任者は、CSIRT 管理者及び CSIRT 担当者に対し、以下の対応を指示する。

2.2 状況の把握

（1）障害の特定

a）CSIRT 管理者は、何時、何処で、何が発生したかを下表を参考に特定し、発生した障害の種類を明確化する。

b）CSIRT 管理者は、障害が発生した原因を確認し、障害による影響範囲を特定できるようにする。

【情報機器障害の種類】

障害の種類	事　象	チェック事項
ハードウェアの障害	・故障、停電等	・電源スイッチ・コンセントの確認 ・警告ランプの確認 ・形状異常の確認等 ・サーバの設定ポリシー確認
ネットワークの障害	・学外通信回線の切断 ・学内 LAN の切断 ・交換機の故障 ・ルータ、ハブなどの通信機器の故障等	・電源スイッチ・コンセントの確認 ・警告ランプの確認 ・コマンドによる通信確認 ・目視チェック等 ・ルータ等の設定内容確認

（2）障害の連絡

a）CSIRT 管理者は、障害の発生により影響を受けると思われる関係者へ連絡をする。
障害状況、復旧見込み等を可能な限り連絡し、必要に応じて、障害復旧への協力を依頼する。

b）CSIRT 責任者は、国、新潟県、新潟県県警察等関係機関へ連絡が必要と判断した場合は速やかに連絡する。
被害による影響を受ける者からの問合せ等が想定される場合は、その連絡受付窓口を設置し、公表する。

2.3 被害拡大防止

（1）原因確認、影響範囲の特定

・被害状況の確認結果及び過去の類似事例等をもとに直接の原因を把握する。

・被害の拡大のおそれがある場合は、その影響範囲を把握する。

（2）被害拡大防止策の検討、実施

・CSIRT 管理者は、被害を拡大させないために、物理的措置（通信回線切断、情報セキュリティ稼動停止等）人的措置（対応要員の確保等）を検討し、実施する。

2.4 緊急措置の実施

a）CSIRT 責任者は、学内関係各部署と連絡調整を図るとともに、緊急措置を実施するよう指示する。

b）CSIRT 管理者は、障害により停止する業務の中で、運用を止めると大きな支障がある業務を特定する。

c）CSIRT 管理者は、・運用を止めると支障のある業務については、業務の代替手段を実施する。

d）CSIRT 管理者は、・短時間で可能な場合は、情報システムの修正、機器故障の修復等を実施する。

2.5 原因の解明と復旧措置

（1）原因の再確認

a）CSIRT 管理者は、障害発生の直接原因を再確認する。

b）障害による影響範囲については、時系列（過去、現在、将来）での影響、情報提供者に対する影響、利用者に対する影響、業務処理に対する影響等を考慮し、影響による被害を修復する策を検討する。

（2）復旧作業の実施

a）CSIRT 管理者は、障害の原因を取り除き、障害発生前の状態で、業務が継続できるように対応策を実施する。

b）必要に応じて外部委託先に依頼する。

c）正常稼動後に、対応措置に問題がないかを確認する。

2.6 緊急事態解除

（1）運用再開

a）CSIRT 管理者は、正常稼動に戻ったことを確認し、CISO、CSIRT 責任者及びインシデントが発生した部署の組織責任者に報告する。

（2）緊急事態解除宣言

a）CSIRT 管理者は、影響を受けた部署、利用者等関係者へ正常稼動の連絡をする。

b）CSIRT 責任者は、正常稼動を確認し、緊急事態解除宣言を行う。

（3）報告

a）CSIRT 責任者は、インシデントによる関係者への対応状況等について情報統合管理会議に報告する。

2.7 対応状況報告

インシデント対応状況について速やかに関係者と連絡、情報交換を行うとともに、迅速な対応をとるため、対応中も適時、以下に従い連絡、報告を行うものとする。

ａ）CSIRT 管理者は、状況や事態が推移する都度、報告書（情報セキュリティ緊急時対応計画　報告様式１）を作成し、CSIRT 責任者を通して、関係者へ報告する。

ｂ）インシデント対応の最終結果は、CSIRT 責任者を通して、学長、CISO 及びインシデントが発生した部署の組織責任者に報告する。

ｃ）インシデント対応の詳細報告とは別に、復旧状況連絡を関係部署に徹底する。

ｄ）報告は、インシデントの内容、対応の期間等を考慮して行う。

ｅ）報告は、少なくとも、以下の段階で実施するようにする。

・被害拡大防止策実施時
・緊急措置実施時
・復旧措置実施時

なお、緊急時対応で実施した事項等については、可能な限り詳細に記録し、総合情報課にて保管する。

2.8　再発防止計画策定

CISO は、インシデントの解消後、再び同様の原因で障害が発生しないように、必要に応じて、再発防止のための対策を検討及び計画し、実施することを関係者に指示する。

再発防止計画の策定・実施は、次の手順に沿って推進する。

なお、（２）～（５）について、CISO が情報セキュリティインシデント対策本部を設置した場合は、CSIRT と情報セキュリティインシデント対策本部が連携して対応すること。

（１）真因追求

・障害発生の真の原因を突き止める。
・障害の直接原因、そのまた原因等できるだけ深く追求し、真因を究明する。

（２）再発防止策検討

・把握した真の原因を取り除くための対応策を検討する。
・仕組み（設備、システム、制度）面での対応策、運用（要員、教育）面での対応策等を検討する。

（３）再発防止計画策定

・再発防止が計画的に実施できるようにする。
・計画では、必要資源等を明確にする。
・可能なら、実施スケジュール等を明確にする。

（４）再発防止計画承認

・再発防止計画の実施には、資源（予算、要員、設備等）が関わるため、学長及び情報統合管理会議の承認を得るようにする。

（５）再発防止計画実施

・再発防止計画に従って作業を実施する。
・作業が長期にわたる場合は、確実に進捗管理を行う。

（６）効果確認・報告

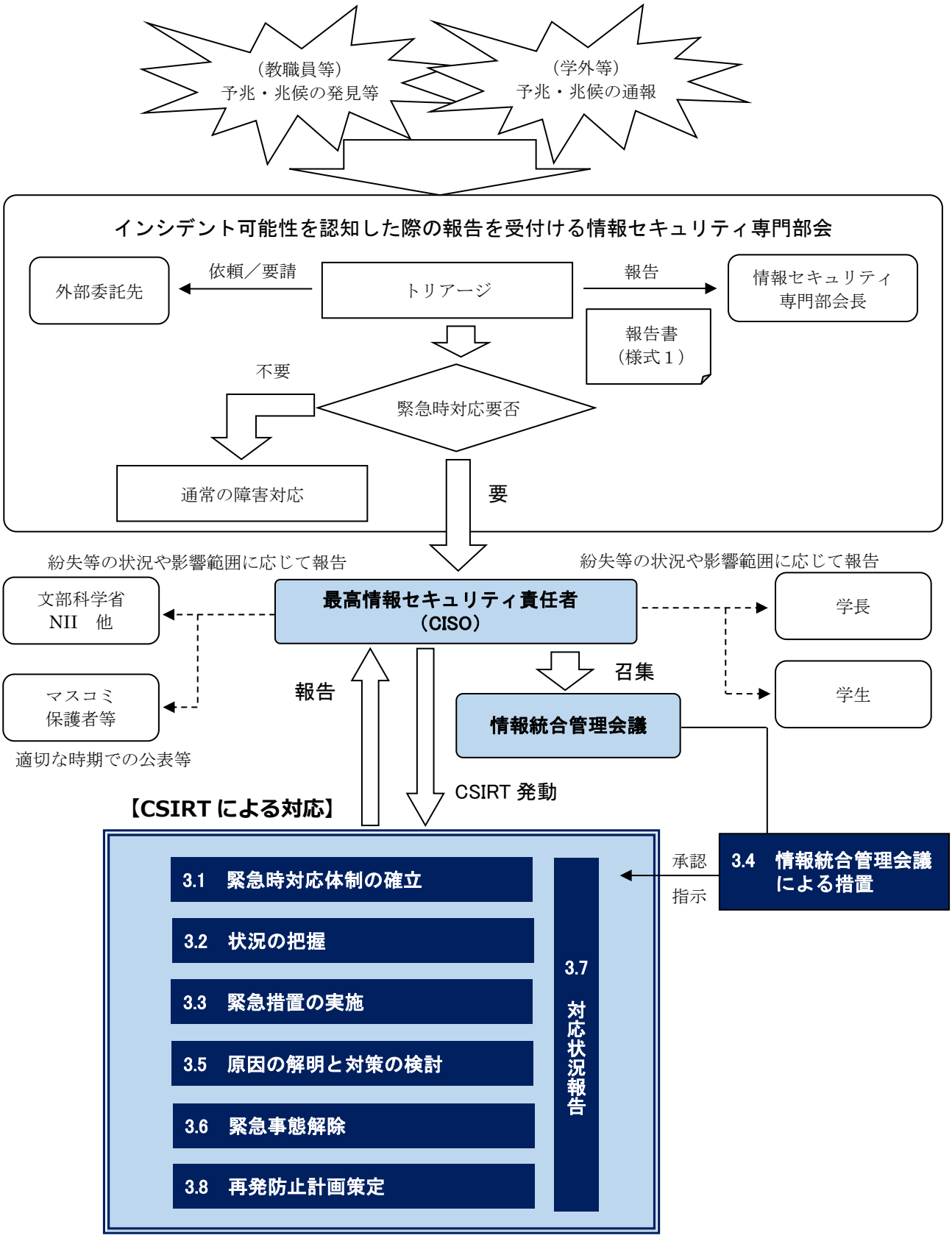
・再発防止計画が終了した時点で、問題がないことを確認する。
・再発防止計画の実施結果の効果を関係者に報告する。

（７）変更事項の徹底

・再発防止計画の実施によって、業務の運用方法等が変更になった場合は、その関係者に変更事項を周知徹底する。

3　盗難・紛失インシデント

盗難・紛失インシデント発生時の対応手順を以下に示す。



図中の各手順（3.1～3.8）について以下に示す。

3.1 緊急時対応体制の確立

a）CSIRT 責任者は CSIRT を招集し、緊急事態宣言をし、全学横断的な協力体制が得られるようにする。

b）インシデントの種類に応じて、対応できる関係者に特定したインシデントの内容を伝え、対応を依頼する。外部委託先に対応依頼をする場合は、必ず対応方法の確認をとる。

c）CSIRT 責任者は、CSIRT 管理者及び CSIRT 担当者に対し以下の対応を指示する。

3.2 状況の把握

（1）詳細情報の把握

a）CSIRT 管理者は、盗難・紛失の詳細情報を把握するために次の対応を取る。

・盗難・紛失した情報資産の種類、データ量などの情報を集約する。

・盗難・紛失時の状況・経緯等について当該役職員等にヒアリングする。

・関係部署と連携し盗難・紛失による影響範囲を特定する。

（2）連絡・指示

a）CSIRT 責任者は、必要に応じて学生への対応等について指示を行う。

b）CSIRT 責任者は、国、新潟県、新潟県警察等関係機関へ連絡が必要と判断した場合は速やかに連絡する。

c）CSIRT 責任者は、被害により影響を受ける者からの問合せ等が想定される場合は、その連絡受付窓口を設置し、公表する。

3.3 緊急措置の実施

CSIRT 責任者は、次のとおり緊急措置を実施するよう指示する。

a）緊急措置の実施においては、学内関係各部署と連絡調整を図り、必要な協力を要請する。

b）盗難・紛失の経緯等について関係者からの報告聴取、調査等必要な措置を講じる。

3.4 情報統合管理会議による措置

a）CISO は、情報統合管理会議を招集する。

b）CSIRT 責任者は、情報統合管理会議において、盗難・紛失の状況、原因、支障の程度等を報告するとともに、CISO の指示による緊急の措置等についてその承認を得るものとする。

c）情報統合管理会議は、以下の項目について協議し、協議結果は学長に報告するとともに、承認を得る。

【情報統合管理会議における協議事項】

決定する項目	内　容
関係機関への連絡	・文部科学省、個人情報保護委員会 ・NII、新潟県警察等
詳細な被害状況	・盗難・紛失した個人情報への侵害の度合い

決定する項目	内　容
緊急時体制の確立	・役割分担、指揮命令系統の確認
個人への対応	・来訪者への対応・ホームページ等での告知 ・問合せ対応・苦情処理 ・個人への謝罪方法
広報対応	・情報資料提供 ・記者発表等
緊急措置の見直し判断	・追加措置 ・調査等緊急時対応の進捗状況 ・恒久対策の立案等

3.5　原因の解明と対策の検討

ａ）CSIRT 管理者は、盗難・紛失の直接原因を解明し適切な対策を検討するよう盗難・紛失を引き起こした当該部署に指示する。

ｂ）盗難・紛失を引き起こした部署以外への対策展開も考慮する。

3.6　緊急事態解除

（1）緊急事態解除宣言

ａ）CSIRT 責任者は、インシデント対応完了を確認し、緊急事態解除宣言を行う。

（2）報告

ｂ）CSIRT 責任者は、盗難・紛失による関係者への対応状況等について情報統合管理会議に報告する。

3.7　対応状況報告

CSIRT 管理者は、インシデント対応状況について速やかに関係者と連絡、情報交換を行うとともに、迅速な対応をとるため、対応中も適時、以下に従い連絡、報告を行うものとする。

ａ）CSIRT 管理者は、状況や事態が推移する都度、報告書（情報セキュリティ緊急時対応計画　報告様式１）を作成し、CSIRT 責任者を通して、関係者へ報告する。

ｂ）インシデント対応の最終結果は、CSIRT 責任者を通して、学長、CISO 及びインシデントが発生した部署の組織責任者に報告する。

ｃ）インシデント対応の詳細報告とは別に、復旧状況連絡を関係部署に徹底する。

ｄ）報告は、インシデントの内容、対応の期間等を考慮して行う。

ｅ）報告は、少なくとも、以下の段階で実施するようにする。

・被害拡大防止策実施時

・緊急措置実施時

・復旧措置実施時

なお、緊急時対応で実施した事項等については、可能な限り詳細に記録し、事務局にて保管する。

3.8　再発防止計画策定

CISO は、インシデントの解消後、再び同様の原因で盗難・紛失が発生しないように、必要に応じて、再発防止のための対策を検討及び計画し、実施することを関係者に指示する。

再発防止計画の策定・実施は、次の手順に沿って推進する。

なお、（２）～（５）について、CISO が情報セキュリティインシデント対策本部を設置した場合は、CSIRT と情報セキュリティインシデント対策本部が連携して対応すること。

（１）真の原因追求

・盗難・紛失発生の真の原因を突き止める。

・盗難・紛失の直接原因の確認、その原因になった原因、そのまた原因等できるだけ深く追求し、真の原因を究明する。

（２）再発防止策検討

・把握した真の原因を取り除くための対応策を検討する。

・仕組み（設備、システム、制度）面での対応策、運用（要員、教育）面での対応策等を検討する。

（３）再発防止計画策定

・再発防止が計画的に実施できるようにする。

・計画では、必要資源等を明確にする。

・可能なら、実施スケジュール等を明確にする。

（４）再発防止計画承認

・再発防止計画の実施には、資源（予算、要員、設備等）が関わるため、学長及び情報統合管理会議の承認を得るようにする。

（５）再発防止計画実施

・再発防止計画に従って作業を実施する。

・作業が長期にわたる場合は、確実に進捗管理を行う。

（６）効果確認・報告

・再発防止計画が終了した時点で、問題がないことを確認する。

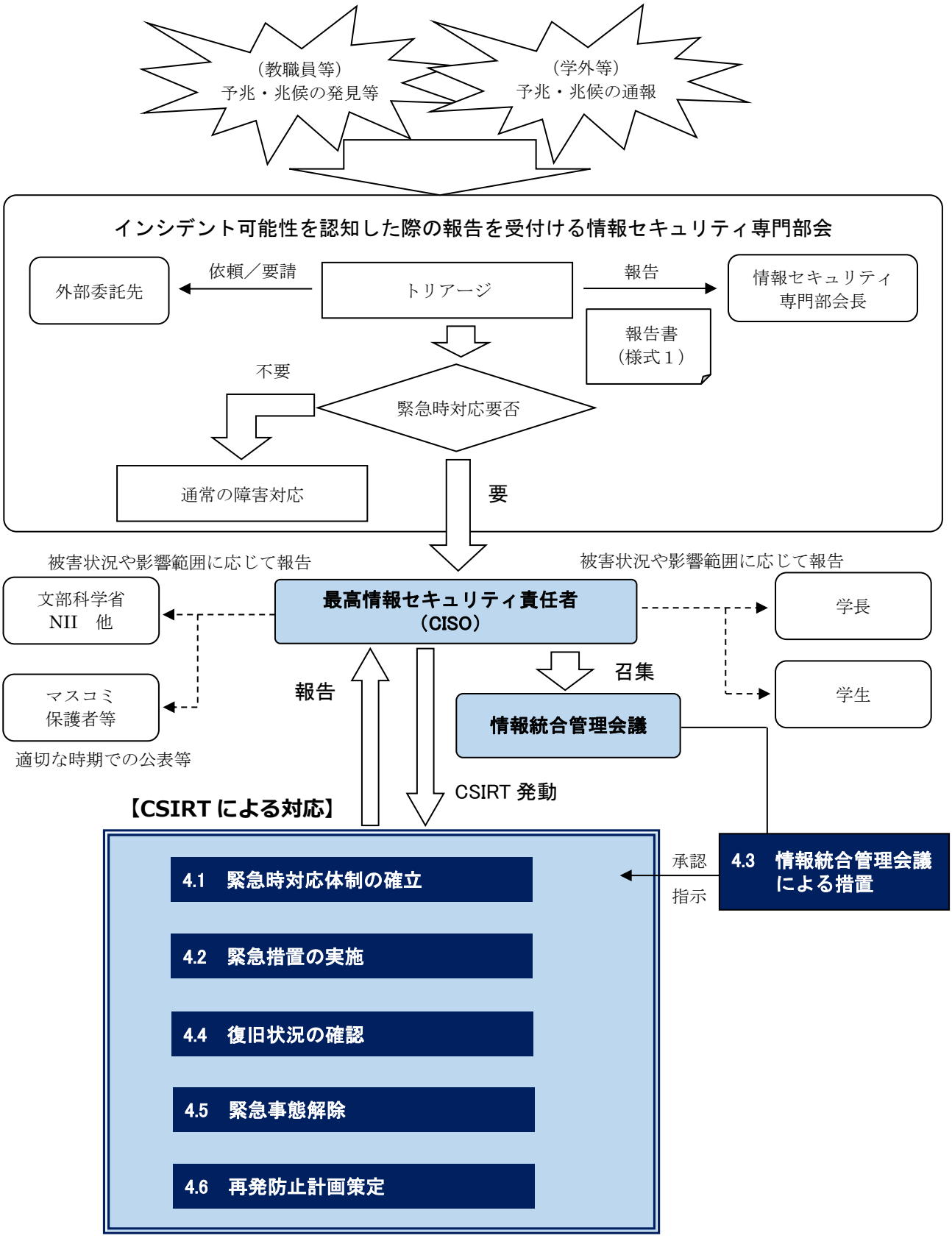
・再発防止計画の実施結果の効果を関係者に報告する。

（７）変更事項の徹底

・再発防止計画の実施によって、業務の運用方法等が変更になった場合は、その関係者に変更事項を周知徹底する。

4　外部（クラウド）サービスインシデント

外部（クラウド）サービスインシデント発生時の対応手順を以下に示す。



図中の各手順（4.1～4.6）について以下に示す。

4.1 緊急時対応体制の確立

ａ）CSIRT 責任者は CSIRT を招集し、緊急事態宣言をし、全学横断的な協力体制が得られるようにする。

ｂ）インシデントの種類に応じて、対応できる関係者に特定したインシデントの内容を伝え、対応を依頼する。

ｃ）CSIRT 責任者は、CSIRT 管理者及び CSIRT 担当者に対し、以下の対応を指示する。

4.2 緊急措置の実施

CSIRT 責任者は、次のとおり緊急措置を実施するよう指示する。

ａ）緊急措置の実施にあたっては、学内関係各部署と連絡調整を図り必要な協力を要請する。

ｂ）クラウド事業者からの報告の徴収、関係者への調査等必要な措置を講じる。

4.3 情報統合管理会議による措置

ａ）CISO は、情報統合管理会議を招集する。

ｂ）CSIRT 責任者は、情報統合管理会議において、インシデントの状況、支障の程度等を報告するとともに、CISO の指示による緊急の措置等についてその承認を得るものとする。

ｃ）情報統合管理会議は、以下の項目について協議し、協議結果は学長に報告するとともに、承認を得る。

【情報統合管理会議における協議事項】

決定する項目	内　容
関係機関への連絡	・文部科学省、個人情報保護委員会 ・NII
詳細な被害状況	・本学システム、情報への具体的な被害状況 ・個人情報への侵害の有無、度合い
緊急時体制の確立	・役割分担、指揮命令系統の確認
個人への対応	・ホームページ等での告知 ・問合せ対応・苦情処理
広報対応	・情報資料提供 ・記者発表等
緊急措置の見直し判断	・追加措置 ・調査等緊急時対応の進捗状況 ・恒久対策の立案等

4.4 復旧状況の確認

CSIRT 責任者は、クラウド事業者に対して、復旧時期を含むインシデント対応状況について随時状況報告するよう要請する。

4.5　緊急事態解除

（1）運用再開

a）CSIRT 管理者は、クラウド事業者からの復旧連絡を受け、システムの復旧状況、情報の整合性を確認する。

（2）緊急事態解除宣言

a）CSIRT 管理者は、インシデント対応の詳細とあわせ、関係部署に復旧状況の連絡を行う。

b）CSIRT 責任者は、インシデント対応完了を確認し、緊急事態解除宣言を行う。

（3）報告

a）CSIRT 責任者は、クラウド事業者における対応状況等について情報統合管理会議に報告する。

b）インシデント対応の最終結果は、CSIRT 責任者を通して、学長、CISO 及びインシデントが発生した部署の組織責任者に報告する。

4.6　再発防止計画策定

CISO は、インシデントの解消後、再び同様の原因でインシデントが発生しないように、クラウド事業者に対し、再発防止策を検討し、速やかに実施することを要請する。

また、学内においても、インシデント再発時でもインシデントレベルが最小となるよう対策を検討する。

なお、CISO が情報セキュリティインシデント対策本部を設置した場合は、CSIRT と情報セキュリティインシデント対策本部が連携して対応すること。

≪ 平常時の準備・予防等 ≫

1　連絡網の整備

・各部署では、インシデント発生時の速やかな連絡、情報交換を行うとともに、緊急時の初動体制を円滑に行うために、事前に緊急時連絡網を整備しておくものとする。
・緊急時連絡網は、「勤務時間内緊急時連絡網」と「勤務時間外（夜間・休日）緊急時連絡網」を作成する。
・緊急連絡網は、担当者名、メールアドレス、電話番号、携帯番号、FAX 等を明確にする。

2　前提となる規程の確認

情報セキュリティポリシー、手順等及び危機管理対策マニュアルを確認し、内容を把握しておく。

3　セキュリティ情報の収集

・情報セキュリティインシデントにはあたらない「ヒヤリハット」に関しても情報収集する。
・標的型攻撃においては、検査・分析で何も発見されない場合でも、依然として組織が危機に晒されているおそれや標的型攻撃の端緒の可能性が考えられる。近い将来、同様の侵入経路や攻撃手口を使って組織を狙う可能性を想定し、検査・分析結果の情報の保持、予兆等の整理、監視の継続などを行い、予防的に防御する。

4　検査・分析に必要な情報の保全

インシデント発生時の迅速な検査・分析に不可欠な以下の情報について状態を確認する。

（1）システム構成図

情報システムを構成するソフトウェア及びソフトウェアが稼働するハードウェアを示す資料が最新版に維持されていることを確認

（2）ネットワーク構成図

情報システムを構成するハードウェア及びネットワーク機器の繋がりを示す資料が最新版に維持されていることを確認

（3）ログ

各サーバ（特に DNS サーバ、プロキシサーバ、ファイアウォール）のアクセスログ、シス

テム稼動ログ、障害時のシステム出力ログ及び障害対応記録の取得・保管等の状況について確認する。

・仕様どおりにログ等が取得されているか
・改ざんや消失等が起こらないよう、ログ等が適切に保全されているか
・システム上の制約等により、ログの一部を外部ストレージやバックアップメディア等に保存している場合は、それらがインシデント発生時等に閲覧可能かどうか確認
・サーバの時刻同期が適切に実施されているか

※対象サーバ、ログの種類・内容、保管期間については、実情に合わせ別途定める。

5　インシデント予兆等の検知、発見

役職員等は、平常時において下記に示すようなインシデント予兆等の有無に注視し、検知、発見した場合、直ちに情報セキュリティ専門部会員へ連絡する。

（1）PC 画面

・ウイルス対策ソフトから、ウイルス等が検出・駆除・隔離された旨のメッセージが表示される。
・インターネット環境で特定の URL へ誘導するような画面展開が見られる。
・不審なメッセージが表示される。
・身に覚えのないログオン履歴がある。（前回ログオンした日時が表示される機能を持っている場合等）
・普段見ている WEB のページに表示内容等に違和感がある。
・安全ではないとされる WEB ページを開いてしまった。
・画面からエラーや停止等何らかの異常を示すメッセージが表示されている。
・画面に表示されるべき情報の様子が通常と異なっている。
・通常利用できている画面が利用できない。
・通常利用できない画面が利用できてしまう。
・画面がロックされ、一切の操作ができない。

（2）電子メール

・電子メールが利用できない。又は利用できても何らかの異常を示すメッセージが表示されている。
・不審なメールが再三送られている。（このようなメールは開けない、開けても添付ファイルの開封やリンクのクリック等は行わない。）
・知り合いからのメールであるが、内容が不審なために本人に確認したところ、送付した記憶がない旨の回答があった。
・知り合いからのメールであるが、メールの題名や内容等に違和感がある。
・知り合いからのメールの添付ファイルを開封、あるいはリンク先をクリックしたところ、異常な動きを始めた。

・不審なメールに対して添付ファイルの開封、あるいはリンク先をクリックした。

（3）システム操作

・情報システムにアクセスできない。
・情報システムの動作が非常に遅い。
・端末が正常に作動しない、又は自らの操作通りに画面展開しない。
・通常利用できているサービスが利用できない。
・通常利用できないサービスが利用できてしまう。
・不審なメッセージが表示される。
・身に覚えのないログオン履歴がある。（前回ログオンした日時が表示される機能を持っている場合等）
・自らが操作していない処理が行われている。
・自らが操作していない通信が行われている。
・端末からエラーや停止等何らかの異常を示すメッセージが表示されている。
・端末に表示されるべき情報の様子が通常と異なっている。

（4）システム運用

・情報システムのログの記録ができない。
・情報システムのログの記録に欠落（ログに記録を残す処理が稼働している時間帯であるにもかかわらず、ログの記録がない等）を発見した。
・情報システムのログのバックアップができない。
・データベースのバックアップができない。
・情報システム（プログラムとそれに関わるリソース）のバックアップができない。
・情報システムが使用するディスク領域が不足している。
・情報システムが使用するメモリー領域が不足している。
・情報システムが使用する CPU 使用率が上限値を超えたままで下がらない。
・情報システムの処理スケジュールが遅延している。
・情報システムの処理スケジュールにない処理が稼働している。
・情報システムの処理スケジュールで指定されていない処理が稼働している。
・ネットワーク機器、監視装置、セキュリティ製品等からアラートが発せられた。

（5）その他

・落し物の PC や媒体（USB メモリ、CD/DVD）等を発見し、中を確認したら本学関連の情報が入っていると外部通報者から連絡があった。
・許可されていない外付けディスクの利用や、媒体（USB メモリ、CD/DVD）等への情報のコピー等が行われていることを発見した。
・本学の要機密情報が公開されていることを発見した。
・機密性の高い情報を保存したモバイル端末の所在が不明であるが、紛失したことや盗難されたことが確定的でない。
・平時の情報システムの利用において確認されないはずのエラーメッセージが端末に表示

される。
・重要情報や設備を設置し、担当外の事務従事者の立入を制限する必要がある区域（サーバ室、資料保管室（＝バックアップメディアの保管場所として想定）で通常は施錠されている区域において施錠されていない場合があった。

6　訓練・演習

CSIRT 責任者は、必要に応じインシデントの発生を想定した訓練・演習を定期的に実施する。

（1）訓練・演習計画の策定

・CSIRT 責任者は、CSIRT 管理者及び CSIRT 担当者に対する緊急時対応に関する訓練・演習計画を策定し、情報統合管理会議の承認を得なければならない。
・異動等により新たに CSIRT 管理者、CSIRT 担当者となる者に対しては、緊急時対応に関する研修を実施しなければならない。
・CSIRT 責任者は、役職員等を対象とした、インシデント予兆等発見の演習計画を策定する。

（2）訓練・演習の実施

・訓練・演習実施では、範囲等を定め、効果的に実施できるようにする。

（3）訓練・演習結果の報告

・CSIRT 責任者は、必要に応じて、情報統合管理会議に対して、緊急時対応訓練等の実施状況について報告しなければならない。

報告書（様式１）

情報セキュリティインシデント報告書

（当該部署→情報セキュリティ専門部会員
→
情報セキュリティ専門部会長→ＣＩＳＯ）

第　　報

報告日時　20　　年　　月　　日　　時　　分（24時間表示）

事案名		
報告者	所属	
	役職・氏名	
	電話番号	
事案の概要	□ネットワークインシデント　□物理的インシデント □盗難・紛失インシデント　□外部（クラウド）サービスインシデント	
影響範囲	確認した被害状況・影響範囲（損害規模等） （情報漏えいの場合は、漏洩した情報の概要及び件数）	
発生日時	年　月　日　時　分（西暦、24時間表示）	
発生場所	施設等の名称	
	住所	
情報入手経路	入手日時	年　月　日　時　分（西暦、24時間表示）
	入手方法（誰から、どのように）	
被害状況	直接被害を受ける対象を含めた被害状況	
原　因	インシデントが発生した原因及び原因として想定される行為	
対応状況	情報連絡先（組織名等）	
	緊急対応の状況	
	システム運用状況 □継続　□縮小　□停止　□その他（　　）	
今後の対応	復旧対応、再発防止策等	
その他参考事項	関係情報又は報告書添付資料名等	

■ 記入要領

No.	項目	記入要領
①	事件・事故名	インシデント名：インシデントの内容を簡潔に記入する。 （第２報以降とのつながりが分かる程度）
②	第　報、報告日時	報告回数（版数）を記入する。 年月日欄は、報告書作成日付を記入する。また、報告書に記入する時間は、24 時間表示とする。（以下同じ）
③	報　告　者	インシデントの発見者名又は当該インシデントに関係する部署の責任者名を記入する。所属（部署名）、役職、氏名及び電話番号（内線番号）等を表記する。
④	事案の概要	インシデントの内容をセキュリティインシデント、物理的インシデント、盗難・紛失インシデント、外部（クラウド）サービスインシデントに分けて該当する項目欄の□にレ点を記入する。報告書作成時点で発生事象及び原因等について判明している事項をできるだけ詳細に記入する。
⑤	影響範囲	確認した被害状況・影響範囲（損害規模等）を記載する。 情報漏えいの場合は、漏えいした情報の概要及び件数を記載する。
⑥	発生日時	インシデントが発生した日時又は発生の恐れを察知した日時を記入する。
⑦	発生場所	インシデントの発生場所を記載する。（発生場所が特定できていない場合は、インシデントを発見した場所を記入する。） 当該施設名称、所在地名等を明記する。
⑧	情報入手経路	インシデントの発生の情報をどのようにして入手したかを記入する。 入手日時、入手先、入手方法等をできるだけ詳細に記入する。 入手先は、詳細調査に必要になる場合があるため、支障のない限り具体名を記入する。
⑨	被害状況	インシデントの結果、被害が出ている場合は、直接被害を受ける対象を含めて具体的に記入する。
⑩	原因	インシデントが発生した原因（及び原因として想定される行為）
⑪	（対応状況） 情報連絡先	連絡した組織・施設名称等を記載する。特に連絡先等で、既連絡先を重複連絡にならないように明記する。
⑫	（対応状況） 緊急対応の状況	インシデントレスポンスに基づく初動対応（対応方針の検討、証拠保全、封じ込め、根絶）及び復旧措置に係る対応状況を記載する。
⑬	（対応状況） システム運用状況	システム運用状況を示す該当欄の□にレ点を記入する。その他の場合は、できるだけ具体的に表記する。
⑭	今後の対応	報告時に判明している範囲でその内容を記入する。 少なくとも、復旧の見通し、再発防止策の要否等が分かるようにする。
⑮	その他参考事項	その他参考事項：インシデントに関する参考情報、又は報告書に添付して提出する資料があれば、その資料名等を記入する。

別表　インシデント発生時の対応手順例

以下に、標的型攻撃メールの受信、ホームページ改ざん、ランサムウェアの感染のそれぞれの場合の対応事例を示す。

実際のインシデントへの対応は、インシデントの規模や複雑性、攻撃の高度さ、学内システムの規模や構成、事業者のスキル等によって変わってくるため、あくまでも参考として利用のこと。

1　標的型攻撃メールの受信

分　類	対応等
インシデント発生	01. XX 省教職員を名乗る添付ファイル付き電子メールが A 課アドレスに届く。 02. A 課職員が開封し添付ファイル（ZIP ファイルに偽装した exe ファイル）をダウンロードし実行したところ、Windows がセキュリティの警告ダイアログを表示。同ダイアログを閉じるボタンで取り消した。
検査・分析	03. 不審に思った A 課職員が情報セキュリティ専門部会員に連絡。XX 省に当該メールの真正性（本当に送ったのか）を確認するよう助言。
初動対応	04. XX 省が送信していないことが確認できたため、A 課から CSIRT へ連絡。 05.すぐに、添付ファイルをダウンロードしたパソコン及びハードディスクをネットワークから切断。 06. CSIRT 担当者で当該パソコン及びハードディスクを回収し、当該メールを A 課から情報セキュリティ専門部会員及び XX 省へ転送。 07. CSIRT 担当者が、ウイルス対策ソフトでスキャンしたところ、添付ファイルからウイルスを検知したため、CSIRT 責任者の判断により A 課に繋がるネットワークを切断。 08. スタンドアロンのパソコンにより添付ファイルのウイルスの検証を実施。より広範囲の調査の必要性を認めたため、CSIRT 責任者の判断により上記以外に拡散の可能性がある A 課と同じセグメントにある所属のネットワークを切断。 09. CISO 及びインシデントが発生した部署の組織責任者へ報告 10. 切断した A 課の全てのパソコンについて、ウイルスから生成される exe ファイルの存在を調査。 11. 調査した A 課の全てのパソコンについて、ウイルスがないことを確認。
復旧措置（暫定対応）	12. CSIRT 責任者の判断により、切断したネットワークを接続。（復旧） 13. インシデント報告書（第 1 報）を文部科学省へメールで送付。 14. 学長、CISO 及びインシデントが発生した部署の組織責任者へ報告。 15. 当該パソコンの操作ログを確認し、添付ファイルをアプリケーションとして実行していないことを確認。 16. 当該パソコン及びハードディスクを最新の定義ファイルでウイルス検索し駆除。 17. 当該パソコン以外に添付ファイルをダウンロードしたパソコンがないことを確認。 18. A 課の全てのパソコンについて、最新の定義ファイルによるウイルス検索ソフトで完全スキャンを実施。

分　類	対応等
再発防止策 （恒久対策） 検討	19. XX 省から解析結果の連絡があり、特定のサイトへ不正な通信を行う可能性があるウイルスであることが判明。 20. URL フィルタリングシステムにおいて、上記 IP アドレスへのアクセスが無いことを確認。 21. インターネットへの最後の出口となるファイアウォールにおいて、上記 IP アドレスへのアクセスが無いことを確認。 22. 役職員等に対し、今回の事案を受けた今後の標的型攻撃メールにおける情報セキュリティ対策の徹底について注意喚起。 23. ウイルス駆除が終了した当該ハードディスクについて、A 課へ返却。 24. A 課職員に対し、改めて今般の詳細な経緯を説明し、標的型攻撃メールにおける情報セキュリティ対策の徹底について注意喚起。 25. CSIRT に対し、インシデント対応体制を再確認するとともに、不審メールへの対応及び迅速な報告について、注意喚起。

2　ホームページ改ざん

分　類	対応等
インシデント発生	01. 本学の公式ホームページまたは情報セキュリティ専門部会員へ、ウェブサイトが改ざんされた旨の連絡（メール）がある。CSIRT 担当者が当該メールを受付
検査・分析	02. 通報してきた機関に電話し事実関係の確認を行う。 03. 保守事業者に改ざんの事実の確認を依頼 04. 保守事業者から改ざんの事実について報告（日時、場所、内容（概要）、原因、被害状況と影響範囲、情報の漏えいの有無等）
初動対応	05. 保守事業者と今後の対応について検討（ウェブサイトを停止すべきか、停止の範囲、期間、緊急度、停止に伴う影響、代替手段、調査、対応作業を他事業者に依頼する必要性等） 06. 上記内容について CSIRT 責任者に報告 07. 保守事業者に証拠保全を依頼し、ウェブサイトの停止を指示 08. 被害に遭ったウェブサイトの公開を停止 09. 学内にウェブサイトを停止した旨周知 10. 関係機関及び国へ報告
復旧措置（暫定対応）	11. 保守事業者にて引き続き次の作業等を実施 ・コンテンツのアップロード作業を FTP で行っている場合、FTP パスワードの変更。（管理用パソコンがウイルス感染し FTP パスワードが漏えいした可能性もあるため、確実にウイルスに感染していない別のパソコンから変更） ・保管しておいたクリーンなファイルとウェブサーバー上のファイルの比較などで、全ての改ざん箇所の洗い出しを行う。 ・FTP のアクセスログの確認を行い、接続元 IP アドレス、FTP コマンドとファイル名、接続日時より被害状況の調査を行う。 ・HTML ファイル、JavaScript ファイル、PHP ファイル、CSS ファイル、Apache などの.htaccess ファイルや mod ファイル、ディレクトリなど、全ての改ざん箇所の修正を行う。 ・管理用パソコンの OS と各種プログラムが最新状態であることを確認する。 ・サーバープログラムの脆弱性を悪用されて改ざんされた場合、脆弱性が修正されたバージョンにアップデートする。 12. 保守事業者から、調査等の結果、IFRAME インジェクション攻撃であったこと、情報漏えいはなかった旨の報告がある。 13. 保守事業者から、今日中に復旧できる旨の報告がある
再発防止策（恒久対策）検討	14. 保守事業者から作業が終了し、復旧の準備が整った旨報告がある 15. CSIRT 責任者に報告 16. ウェブサイト復旧 17. 関係機関にウェブサイトが復旧した旨報告 18. 報道発表 19. 保守事業者に、再発防止策（恒久対策）の検討を指示

3　ランサムウェアの感染

分　類	対応等
インシデント発生	01. 役職員等から、ファイルサーバのファイルが改ざんされ、読取できない旨の報告を受ける。
検査・分析	02. 保守事業者へ連絡。改ざんを確認。
初動対応	03. 感染が疑われる情報機器に対し、ネットワークからの切り離しを実施。 04. 改ざんが疑われる該当ファイルサーバの共有設定を解除。 ・一部の端末⇔該当ファイルサーバへ接続の禁止 ・すべての端末⇔インターネット通信の禁止 ・感染の疑いのある情報機器の運用停止 ・上記措置の実施に影響のある各種システムの利用制限 05. 副学長に対し、状況報告を実施。 06. 感染が疑われる情報機器に対し、ネットワーク切り離し及び NIC の不活性化を実施。 07. 学内ネットワークからインターネットへの通信遮断を保守業者に指示。 08. 国及び関係機関への連絡を実施。 09. 学内ネットワークからインターネットへの通信の遮断を完了。 10. 感染の疑いのある情報機器を使用していた教職員が所属するネットワークセグメントから、学内基幹ネットワーク接続を遮断。 11. ウイルス対策ソフト業者及び保守業者にウイルス検体を提出。 12. 警察に対し、状況報告を実施。 13. メール受信ログを精査した結果、同様のウイルスが添付されたメール（文面も同様）を追加で 3 件発見したため、メールサーバより削除。
復旧措置（暫定対応）	14. インターネット通信（FTP、HTTPS）以外の通信遮断の解除を開始。 15. 外部とのメール通信を再開、議会動画配信サービスを再開。
再発防止策（恒久対策）検討	16. 保守業者からウイルス解析結果報告を受け、今後の対応策を検討。 17. メールサーバに対し、ウイルスメール送信元メールサーバからのメール受信を拒否する設定を実施。 18. 国及び関係機関へインシデント報告書（第 1 報）を提出。 19. 保守業者から対応状況の進捗について報告を受ける。 20. 情報機器内に当該ウイルスが存在しないことを確認。 21. インターネット通信（FTP、HTTP、HTTPS）の通信遮断を解除。 22. 情報機器を、ネットワークに再接続し、運用を再開。当時点をもって該当ファイルサーバを除き、すべて復旧。該当ファイルサーバについては、翌日以降に復旧の見通し。

以上