長岡技術科学大学におけるサイバーセキュリティ対策等基本計画
（計画期間：令和 4 年 10 月～令和 7 年 3 月）

1.全体方針

長岡技術科学大学（以下「本学」という。）において行われる教育研究活動、大学運営業務を安定的に展開・継続するためには、教職員及び学生がサイバーセキュリティに関する正しい知識を有し、情報に対する適切な取扱いができることが必須である。

本方針では、本学におけるサイバーセキュリティ対策に関し、本学の情報セキュリティポリシー及び第 4 期中期目標・中期計画を踏まえて令和 4 年度から 3 か年の基本的な計画を示し、本計画終了後もサイバーセキュリティ対策が継続的に行われるように定めるものである。

2.個別方針

(1)リスク管理体制の構築

(1)-a.ポリシーや対策推進計画、管理規定の策定

情報セキュリティ水準を適切に維持し、リスクを総合的に低減させるため、ポリシーをはじめとする管理文書を整備すること。

- 情報セキュリティポリシーの改正を必要に応じて行う。必要に応じ、最新の IT 事情を取り入れる。
- サイバーセキュリティを維持するための具体的な実施手順書を作成する。

(1)-b.リスク管理体制の構築

サイバーセキュリティ対策を行うための管理体制を構築する。

- 情報セキュリティポリシーの改正に伴い、必要に応じ、サイバーセキュリティ対策を行うための体制として、CSIRT を構築または維持する。
- 外部からの専門人材の登用や担当部署の設置を検討する。

(1)-c.リスク対策にかかる予算、資源

サイバーセキュリティ対策実施にかかる予算及び人材確保を継続的に措置する。

- 情報セキュリティ専門部会及び情報統合管理会議において、サイバーセキュリティ対策に必要な予算や体制を検討し、経営協議会にて審議の上、役員会にて承認・措置する。
- サイバーセキュリティや情報システム部門の人材を確保するため、育成やキャリアパスの構築を検討する。

⑵リスクの特定

⑵-a.大きなリスクの対象となりうる情報の確認

学内で保有する情報について洗い出し、機密性の確認・整理を行う。また、法人文書ファイル管理簿にもその情報を付記する。

- 以下に該当する情報について各組織内で特定し、機密性の確認・整理を行う。
  - 個人情報
  - 先端技術情報
  - 法令の定めにより管理すべき情報

⑵-b.大きなリスクの特定

リスク対象となる情報について、漏洩・棄損した場合にどのような事態に陥るのか、情報の格付け区分毎にリスク特定を行う。

- 厳秘情報、秘情報、学内情報を漏洩・棄損した場合のリスクを特定する。
- 完全性、可用性についても情報の格付け区分を検討すると共に、いずれも区分が最も高いものについてリスクを特定する。

⑵-c.情報機器の洗い出し

保有・稼働している情報機器やサービスについて、管理対象を特定するために状況を把握する。

- 学外公開サーバについて、緊急時に停止可能なものと業務継続のため無停止が求められるものを把握する。
- 学内 LAN 登録ホストについて、定期的な棚卸を行う。
- 学内 LAN 登録ホストについて、通信要件を把握して不必要な接続を遮断する等適切なアクセス制御と権限管理を行う。
- 研究室等において管理責任者（指導教員、技術職員等）に無許可でサーバ等が設置されないように必要な措置等を講ずる。

⑶リスク対策

⑶-a.守るべき情報の保護

リスク評価に応じて、適切なサイバーセキュリティ対策を講じること。

- 秘情報以上の情報資産を扱う可能性のある業務システムでは、多要素認証の導入や定期的なログの確認等、不正アクセス対策を強化する。多要素認証を導入できない場合は、強度の高いパスワードの設定や、定期的なパスワード変更の実施、学外の他のシステムとのパスワードの使い回しの禁止等、対策を強化する。
- ユーザのアカウント情報は定期的に棚卸を行うと共に、退職者のアカウントは速やかに削除または停止する。

- 法人内に存在する秘情報以上の情報資産を扱うサーバ、特に Active Directory 等の認証機能を有しているサーバを特定し、アカウントの棚卸、ログ取得、パッチ適用等の基本的な対策を実施する。
- 先端技術情報など重要情報を扱う部門の Active Directory 等認証機能を有するサーバ等については、標的型攻撃を踏まえた多層防御及び堅牢化を行う。
- 学内支給端末において盗難、紛失、不正プログラムの感染等により情報が窃取されることを防止するための技術的な措置や、学内支給以外の端末において不正プログラムの感染等により情報窃取されることを防止するための利用時の措置に関する手順等を整備する。
- USB メモリ等の外部電磁的記録媒体を用いて秘情報を取り扱う場合の手順等を定める。
- 教室、研究室、事務室、会議室、サーバ室等の情報を取り扱う区域において、区域の明示、施錠、入退室管理等の対策を講じ、当該区域で取り扱う情報や情報システム等のセキュリティを確保するとともに、重要な書類や外部記録媒体、ノートパソコン等の備品、その他毒物、劇物等の化学物質等を含む適正な管理が必要な物品等について、管理を徹底し、紛失・盗難の対策を講じる。
- 在宅勤務環境等の学外での端末利用についても、リスク評価に応じて、適切なサイバーセキュリティ対策を講じる。
- クラウド上でのシステム構築、データの保存・管理が増加していることを前提とし、学内情報システムに加え、外部のサービスプロバイダーを利用する（クラウド上で運用する）システムやデータについてもデータ保護について検討を行う。

(3)-b.情報機器の脆弱性対応

保有している情報機器の脆弱性について定期的に情報収集を行い、リスクに応じて脆弱性対応を適宜行うこと。

- 情報セキュリティ関連情報の周知徹底を図る。
- 構成管理ソフトウェアの導入による脆弱性情報の収集自動化、適応自動化を検討する。

(3)-c.災害等のリスク対策

災害復旧計画（DR）及び事業継続計画（BCP）について、情報セキュリティインシデントにかかる事案についても想定を含めること。

- 本学の実情を踏まえ、サイバー攻撃やその他大規模システム障害等が発生した場合に必要な対策等を検討する。
- 【再掲】学外公開サーバについて、緊急時に停止可能な情報機器と業務継続のため無停止が求められるものを把握する。

(3)-d.構成員へのセキュリティ意識の徹底

- 【再掲】情報セキュリティ関連情報の周知徹底を図る。
- 新入生や新採用教職員を対象にガイダンスや研修を実施する。
- 教職員を対象に訓練を実施する。また、訓練の結果に基づき、講習会を実施する。

(4)サプライチェーンリスクへの対応

外部委託や共同研究等の実施状況などを把握した上で、保有する情報のリスク度に応じた取り扱いが委託先や共同研究等参加機関でなされているか確認すること。
また、特にリスク評価が高い情報を取り扱う情報システムについて、サプライチェーンリスクに留意すること。

- 情報システムの見直しを検討する。
- 事務局における業務システムの導入・更新等に係る調達を情報統合管理会議で必ず確認する運用を引き続き維持する。
- 外部委託先において必要なセキュリティ対策が確実に実施されるよう、外部委託先に求めるセキュリティ要件を学内で統一的に整備し、調達仕様書等へ記載するとともに、外部委託先における対策の履行状況を確認する。
- 情報システム・機器・役務・サービス（外部ホスティングサービスやクラウド等を利用している場合を含む）等の調達に当たっては、サプライチェーンリスクを軽減するための要求要件を調達仕様書に記載する。
- 共同研究等、外部機関が保有する情報を管理する場合は、産業競争力強化法（平成二十五年法律第九十八号）第二条第十九項第一号の規定に基づき定められた「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏洩を防止するために必要な措置に関する基準」も参考に対応を行う。

(5)インシデント対応体制の構築

サイバー攻撃による被害を受けた場合、別紙 1-2「情報セキュリティ緊急対応図」に基づき、被害原因の特定および解析を速やかに実施できるよう体制を構築する。

- 速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築する。
- 外部のセキュリティベンダ等、関係機関との連携による調査が行える体制を構築する。
- インシデント発生時の文部科学省への報告手順も含めて連絡体制を整えるとともに、演習を検討する。
- インシデント発生後、再発防止策の検討にあたっては、必要に応じて外部の専門家の知見も活用する。
- 緊急連絡網（システム運用、セキュリティベンダ等の連絡先）、学外を含む情報開示の通知先一覧を整備し、対応に従事するメンバーに共有しておく。
- 初動対応時にはどのような業務影響が出るか検討し、緊急時に関係部署が速やかに協力できるよう予め取り決めをしておく。

- インシデントに関する被害状況、個人や他法人への影響等について役員に報告する。

(6)セキュリティ運用の実施

世情を踏まえた脅威動向など、日次の脅威動向や脆弱性情報の収集を行う。

- 【再掲】情報セキュリティ関連情報の周知徹底を図る。
- 情報セキュリティ体制について他機関と継続的に情報交換を行う。
- サイバー攻撃の痕跡にかかる技術情報、いわゆる IoC 情報について収集し、本学に対するサイバー攻撃への防御への活用に生かすこと。
- IoC 情報については継続的かつ迅速な更新が重要であるが、手動での更新は非常に煩雑であるため、ファイアウォールやウイルス対策ソフト等により危険なサイトや IP アドレス等へのアクセスをフィルタリング（ウェブフィルタや IP レピュテーションなど）を行う仕組みを活用する。

(7)監査等での運用チェック

年に一度、本計画の進捗を確認し、フォローアップする。また、情報セキュリティ監査を定期的（毎年度）に実施し、脆弱性対応の確認、業務オペレーションの確認を行う。

- 業務システムまたは学外公開用サーバに対する外部監査を実施する。
- 情報セキュリティ監査の指摘事項に対する改善策を対策基本計画に反映し、継続的にフォローアップを行う。
- 監査の実施内容として、情報システムの脆弱性診断だけでなく、情報セキュリティポリシーや実施手順書等の遵守状況を確認するために行うマネジメント監査についても実施する。

3.工程表

別紙 1-3 のとおり。

以上

長岡技術科学大学　情報セキュリティ緊急対応図

標的型攻撃メール、情報漏えい、コンピュータウィルス、不正侵入、不正使用、踏み台、なりすまし、データ改ざん、データ破壊等の情報セキュリティに関して緊急事態が発生した場合は、こちらのフローに沿って関係部署へ速やかに連絡してください。

情報セキュリティインシデント発生

速やかに所属部署の担当者へ連絡する。なお、担当者不在の場合および担当者への連絡完了後は、 総合情報センター に連絡すること。

被災者　又は　発見者

①発生通知・状況確認

紛失・盗難等の場合は、必ず 総務課 にも連絡すること。

【通知元】
・学内外等
・情報・システム研究機構国立情報学研究所NII-SOCS
E-mail：soc-support@nii.ac.jp
・情報処理振興機構（IPA）
ウィルス：virus@ipa.go.jp 不正アクセス：crack@ipa.go.jp
・文部科学省国立大学法人支援課法規係
TEL：03-5253-4111（内3760, 3497）　E-mail：hojinka@mext.go.jp

①発生通知・状況確認　①発生通知・状況確認　①発生通知・状況確認

【情報セキュリティ専門部会　（CSIRT部門）】

部会長
湯川 高志（内9366）
yukawa@vos

機械
梅本 和希（内9375）
umemoto@mech

横田 和哉（内9718）
yokokazu@vos

技術職員　機械
吉田 昌弘（内9742）
yoshida@mech

環境社会基盤
熊倉 俊郎（内9672）
kumakura@vos

電気電子情報
原川 良介（内9546）
harakawa@vos

技術職員　電気
山浦 賢太郎（内9546）
yamaura@konomi

物質生物
本間 剛（内9312）
honma@mst

技術職員　物質生物
高柳 充寛（内9434）
taka@konomi

情報・経営システム
吉田 富美男（内9352）
fyoshida@vos

量子原子力
菊池 崇志（内9506）
tkikuchi@vos

システム安全
三好 孝典（内9574）
miyoshi@mech

基盤共通教育
原 信一郎（内9652）
sinara@vos

総合情報センター
ネットワークインフラ部門
白清 学（内9873）
hakusei@vos

②状況連絡、調整

事務局
総合情報課事務情報システム係
（内9219, 9266）joho-kiban@jcom

各系等の情報セキュリティ専門部会員と総合情報センター・総合情報課との間で
②状況連絡　を行うと共に、
③応急処置の指示　を行う

⑧報告　②状況連絡、調整　④状況連絡

大学戦略課
企画・広報室
（内9016, 9207）

総務課総務係
（緊急時：内9999）
（内9201, 9203）

取材対応

報道機関

⑧対応・調整（文科省報告時）

文科省サイバーセキュリティ緊急対応支援チーム（M-CYMAT）

⑥連絡・支援要請、対応支援（必要に応じて）

総合情報センター　総合情報課

④状況連絡、⑥対応指示
⑦対応完了報告

④状況連絡、
⑥対応指示（M-CYMATへの連絡・支援要請の判断を含む）
⑦対応完了報告
⑤対策方法決定

情報セキュリティ専門部会
⑨再発防止の対策協議・指導

⑥対応指示
⑦対応完了報告

情報統合管理会議　CISO
総合情報センター長
学長、担当役員

【対応状況・完了等報告先】
・国立情報学研究所NII-SOCS（上記通知・情報提供元に同じ）
・文科省国立大学法人支援課支援第一係
TEL：03-5253-4111（内3757）　E-mail：hojinka@mext.go.jp
・文科省サイバーセキュリティ・情報化推進室情報統括係・サイバーセキュリティ係
TEL：03-5253-4111（内2248, 3060, 3040, 2251）
E-mail：security-incident@mext.go.jp
（※個人情報漏えいが関係する場合）文科省大臣官房総務課文書情報管理室
TEL：03-5253-4111（内3244）　E-mail：bunjou@mext.go.jp

長岡技術科学大学　情報セキュリティ緊急対応の手引

インシデント発生

被災者又は発見者

通報①

通報②

緊急事態発生時は、右側の連絡体制に沿って連絡等をお願いします。
ただし、下記のような事象を含む場合、情報漏えい等に発展する情報セキュリティインシデントとなるおそれがあります。

・パソコン、周辺機器等の紛失、盗難
・パソコン等へのウィルス感染、脆弱性攻撃等

上記のような事象を含む場合は、初めに各教員の系等を確認の上、該当する各系等の下記担当者まで連絡し、応急処置等の指示を仰いでください。(2022年4月現在)

機械	梅本 和希(内線9735、umemoto@mech.nagaokaut.ac.jp) 横田 和哉(内線9718、yokokazu@mech.nagaokaut.ac.jp) 吉田 昌弘(内線9742、yoshida@mech.nagaokaut.ac.jp)
電気電子情報	原川 良介(内線9546、harakawa@vos.nagaokaut.ac.jp) 山浦 賢太郎(内線9546、yamaura@konomi.nagaokaut.ac.jp)
情報・経営システム	吉田 富美男(内線9352、fyoshida@vos.nagaokaut.ac.jp)
物質生物	本間 剛(内線9312、honma@mst.nagaokaut.ac.jp) 高柳 充寛(内線9434、taka@konomi.nagaokaut.ac.jp)
環社	熊倉 俊郎(内線9672、kumakura@vos.nagaokaut.ac.jp)
量子原子力	菊池 崇志(内線9506、tkikuchi@vos.nagaokaut.ac.jp)
シス安	三好 孝典(内線9574、miyoshi@mech.nagaokaut.ac.jp)
基盤共通教育	原 信一郎(内線9652、sinara@vos.nagaokaut.ac.jp)
事務局	本澤 英伸(内線9219、joho-kiban@jcom.nagaokaut.ac.jp) 種岡 諒介(内線9266、joho-kiban@jcom.nagaokaut.ac.jp)

通報①の際に担当者が不在の場合、または通報①の完了後に下記担当まで御連絡ください。(2022年4月現在)

・紛失、盗難の場合:	総務課(内線9999)
・ウィルス感染等の場合:	総合情報センターネットワークインフラ部門(内線9873)

(※本学「安全のための手引(令和4年度版)」より抜粋)

緊急事態発生時の連絡体制

事故事件

被災者又は発見者

通報

事項	連絡先	電話番号
火災 交通事故	消防署 警察署	119 110 携帯電話からの発信も、 119 110
電気 ガス ｴﾚﾍﾞｰﾀｰ 等の故障	エネルギーセンター	0258−47−9290
ケガ、急病	体育・保健センター 救急車(消防署)	0258−47−9824 0258−36−0119

※ 内線電話から外線電話する場合は、0発信することを忘れずに！

通報

総務課(緊急時通報専用電話)
0258−47−9999
※転送完了まで保留音が流れる。
平日(8:30~17:15) : 総務課受信
時間外、休日、祝日 : 警備員受信

報告

執行部

指導教員・上司(所属長)へ連絡

事故等の種類に応じて

各課へ連絡・調査を要請する。

区分	担当課	連絡先
地震、台風、大雪	総務課 施設課	0258−47−9201、9203 0258−47−9233、9234
火災、器物損壊	施設課	0258−47−9233、9234
不審者、盗難	総務課	0258−47−9201、9203
授業中、実験時の事故等	学務課	0258−47−9246、9248
課外活動中の事故、交通事故 学生の不祥事	学生支援課	0258−47−9253
学生の食中毒、急病	学生支援課	0258−47−9253
感染症	総務課(教職員) 学生支援課(学生)	0258−47−9926、9206 0258−47−9253
海外渡航中の事故等	総務課(教職員) 学務課(学生)	0258−47−9201、9203 0258−47−9243
学外からの問い合わせ(報道機関等)	企画・広報室	0258−47−9016、9207

サイバーセキュリティ対策等基本計画工程表

（計画期間：令和4年10月～令和7年3月）

長岡技術科学大学
2022年9月

長岡技術科学大学サイバーセキュリティ対策等基本計画
2022年9月　別紙1-3

長岡技術科学大学　サイバーセキュリティ対策等基本計画				
年度		令和4年度	令和5年度	令和6年度
個別方針	取組事項	工程		
(1)-a.ポリシーや対策推進計画、管理規定の策定	情報セキュリティポリシーの改正	改正の実施	点検の実施	必要に応じた見直し
	サイバーセキュリティの具体的な実施手順書の作成	作成の実施	点検の実施	必要に応じた見直し
(1)-b.リスク管理体制の構築	サイバーセキュリティ対策を行うための体制としてCSIRTを構築または維持	構築の実施	点検の実施	必要に応じた見直し
	外部からの専門人材の登用や担当部署の設置の検討	方針の検討	実施方法の検討	実施
(1)-c.リスク対策にかかる予算、資源	サイバーセキュリティ対策に必要な予算や体制の検討	方針の検討	実施方法の検討	実施
	サイバーセキュリティや情報システム部門の人材確保のための育成やキャリアパスの構築	方針の検討	実施方法の検討	実施
(2)-a.大きなリスクの対象となりうる情報の確認	情報の特定及び機密性の確認・整理	方針の検討	実施方法の検討	実施
(2)-b.大きなリスクの特定	厳秘情報、秘情報、学内情報を漏洩・棄損した場合のリスク特定	格付け区分の見直し	実施方法の検討	実施
	完全性、可用性の格付け区分の検討及び最高区分のリスク特定	格付け区分の検討	実施方法の検討	実施

長岡技術科学大学
Nagaoka University of Technology

長岡技術科学大学サイバーセキュリティ対策等基本計画
2022年9月　別紙1-3

長岡技術科学大学　サイバーセキュリティ対策等基本計画				
年度		令和4年度	令和5年度	令和6年度
個別方針	取組事項	工程		
(2)-c.情報機器の洗い出し	学外公開サーバの緊急時停止可能機器及び要無停止機器の把握	実施方法の検討	実施	必要に応じた見直し
	学内LAN登録ホストの定期的な棚卸の実施	継続実施		
	学内LAN登録ホストの適切なアクセス制御と権限管理の実施	継続実施		
	研究室等における管理責任者に無許可でサーバ等を設置されないための措置の検討	継続実施		
(3)-a.守るべき情報の保護	秘情報以上の情報資産を扱う業務システムの不正アクセス対策強化	継続実施		
	ユーザーアカウント情報の定期的な棚卸及び退職者の削除、停止	継続実施		
	認証機能サーバの特定、アカウント棚卸、ログ取得、パッチ適用等実施	継続実施		
	認証機能サーバに対する標的型攻撃を踏まえた多層防御及び堅牢化	継続実施		
	学内支給端末の情報窃取防止の技術的措置及び利用手順の整備	整備の実施	点検の実施	必要に応じた見直し
	外部電磁的記録媒体の秘情報取扱手順の制定	制定の実施	点検の実施	必要に応じた見直し
	情報を取り扱う区域の明示及び対策、物品紛失盗難対策の検討	方針の検討	実施方法の検討	実施
	学外端末利用におけるサイバーセキュリティ対策の検討	方針の検討	実施方法の検討	実施
	学内情報システム及びクラウド運用システムのデータ保護の検討	方針の検討	実施方法の検討	実施

長岡技術科学大学
Nagaoka University of Technology

長岡技術科学大学サイバーセキュリティ対策等基本計画
2022年9月　別紙1-3

長岡技術科学大学　サイバーセキュリティ対策等基本計画				
年度		令和4年度	令和5年度	令和6年度
個別方針	取組事項	工程		
(3)-b.情報機器の脆弱性対応	情報セキュリティ関連情報の周知徹底	継続実施		
	構成管理ソフトウェアの導入による脆弱性情報の収集自動化、適応自動化の検討	方針の検討	実施方法の検討	実施
(3)-c.災害等のリスク対策	本学の実情を踏まえたサイバー攻撃やその他大規模システム障害等発生時に必要な対策の検討	方針の検討	実施方法の検討	実施
	【再掲】学外公開サーバの緊急時停止可能機器及び要無停止機器の把握	方針の検討	実施方法の検討	実施
(3)-d.構成員へのセキュリティ意識の徹底	【再掲】情報セキュリティ関連情報の周知徹底	継続実施		
	新入生や新採用教職員を対象としたガイダンスや研修の実施	継続実施		
	教職員を対象とした訓練の実施及び訓練の結果に基づく講習会の実施	訓練内容の検討	訓練の実施、講習会の検討	講習会の実施

長岡技術科学大学
Nagaoka University of Technology

長岡技術科学大学サイバーセキュリティ対策等基本計画
2022年9月　別紙1-3

長岡技術科学大学　サイバーセキュリティ対策等基本計画				
年度		令和4年度	令和5年度	令和6年度
個別方針	取組事項	工程		
(4)サプライチェーンリスクへの対応	情報システムの見直しの検討	継続実施		
	事務局における業務システムの導入・更新等に係る調達の確認	継続実施		
	外部委託先に求めるセキュリティ要件の統一的整備、調達仕様書等への記載及び外部委託先における対策の履行状況確認	方針の検討	実施方法の検討	実施
	情報システム等の調達におけるサプライチェーンリスク軽減のための要求要件の調達仕様書への記載	方針の検討	実施方法の検討	実施
	共同研究等、外部機関が保有する情報管理の関連法令に基づく対応の実施	方針の検討	実施方法の検討	実施
(5)インシデント対応体制の構築	証拠保全体制の構築	構築の実施	点検の実施	必要に応じた見直し
	関係機関との連携による調査体制の構築	構築の実施	点検の実施	必要に応じた見直し
	インシデント発生時の文科省への報告手順・連絡体制の整備及び演習の検討	手順・体制の整備の実施	手順・体制の点検の実施	手順・体制の必要に応じた見直し、及び演習の検討
	再発防止策の検討における外部専門家の知見活用の検討	継続実施		
	緊急連絡網、情報開示の通知先一覧の整備、及び関係者への共有	整備の実施	点検の実施	必要に応じた見直し
	初動対応時の業務影響検討及び緊急時対応検討	業務影響及び緊急時対応の検討	業務影響及び緊急時対応の点検	必要に応じた見直し
	インシデント被害状況、個人や他法人への影響等の役員への報告	継続実施		

長岡技術科学大学サイバーセキュリティ対策等基本計画
2022年9月　別紙1-3

長岡技術科学大学　サイバーセキュリティ対策等基本計画				
年度		令和4年度	令和5年度	令和6年度
個別方針	取組事項	工程		
(6)セキュリティ運用の実施	【再掲】情報セキュリティ関連情報の周知徹底	継続実施		
	情報セキュリティ体制について他機関との継続的な情報交換の実施	継続実施		
	IoC情報の収集及び本学に対する攻撃への防御への活用	方針の検討	実施方法の検討	実施
	ファイアウォールやウイルス対策ソフト等によるアクセスフィルタリングの活用	継続実施		
(7)監査等での運用チェック	業務システムまたは学外公開用サーバに対する外部監査の実施	継続実施		
	情報セキュリティ監査の指摘事項に対する改善策の本計画への反映及び継続的なフォローアップの実施	継続実施		
	監査の実施内容として情報セキュリティポリシーや実施手順書等の遵守状況を確認するマネジメント監査の実施	ポリシーの改正の実施	監査の検討	監査の実施