○旭川医科大学情報セキュリティ対策実施要項

平成24年4月10日
学　長　裁　定

(趣旨)

第1　この要項は，旭川医科大学情報セキュリティポリシー(平成15年3月20日学長裁定)に定める情報セキュリティ対策基準に基づき，情報セキュリティ対策実施に関する取り扱いを定めるものとする。

(定義)

第2　この要項において，「全構成員」とは，役員，職員，学部学生及び大学院生等をいう。

2　この要項において，「一般利用者」とは，不特定多数が利用可能な共同利用情報機器を利用する者及び一時的に学内の情報システムを利用する者や外部委託業者等及び継続してアカウントを利用する者をいう。

3　この要項において，「部局」とは，情報セキュリティ管理規程(以下「セキュリティ規程」という。)第2条に定めるものをいう。

4　この要項において，「クライアント機器」とは，主として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。

5　この要項において，「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をいう。

6　この要項において，「ディスクブート」とは，ディスクによりクライアント機器を起動することをいう。

7　この要項において，「インテリジェントスイッチ」とは，ネットワーク管理機能を持つLANスイッチをいう。

8　この要項において，「ルータ」とは，ネットワーク上を流れるデータを他のネットワークに中継する機器をいう。

9　この要項において，「管理ポート」とは，各種の通信関連装置等において，LANを経由して遠隔から設定管理するための機構をいう。

10　この要項において，「コンソールポート」とは，各種の通信関連装置などにおいて，PC等を接続し通信管理装置を設定管理するための端子をいう。

(非公開情報)

第3　許可された者以外が非公開情報を閲覧及び保管してはならない。また，許可された者であっても，非公開情報を不特定の者が可読な状態とする行為や複製を行ってはならない。

2　非公開情報を扱うネットワークは，公開情報ネットワークと論理的に異なるネットワークで構成するものとする。

3　非公開情報ネットワークから公開情報ネットワークへアクセスする必要がある場合は，逆方向(公開から非公開へのアクセスをいう。)のアクセスを防止する措置を講じなければならない。

4　盗難等を防止するため，利用を許可された場所から外部に非公開情報を持ち出してはならない。

5　インターネット等の公衆回線を介して不特定の者が傍受可能な方式で非公開情報にアクセスすることは原則禁止する。

6　外注などのため，非公開情報を限定された第三者に開示する必要がある場合は，開示の都度，守秘義務契約を結ばなければならない。

(公開情報)

第4　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，情報の改ざんや偽情報の流布に対し，第8に掲げる防止策を講じなければならない。

(発信情報(プッシュ型メール等))

第5　大学側から不特定多数の者に発信する情報は，第7に掲げる防止策を講じるだけでなく，正規の発信者であることを証明しなければならない。

(情報の公開化)

第6　非公開情報を公開化する場合には，個人情報の漏えい，プライバシーや著作権の侵害に十分注意し，公開できる情報だけを抽出するなどの加工を行わなければならない。

(情報の限定公開)

第7　限定公開を要する情報の登録及び閲覧は，許可された者が許可された操作だけを行えるように，認証及びアクセス制御機能を設けなければならない。また，異常な登録や閲覧が行われていないか，定期的に状況を確認しなければならない。

(情報改ざん及び偽情報流布の防止)

第8　非公開情報，限定公開情報及び公開情報の原本は，CD―ROM／CD―R等の書き換え不能な記録媒体に保存するなどにより原本性を保証しなければならない。また，改ざんを受けた場合の速やかな回復機構の備えや，公開情報(Webでの掲示情報やメールマガジンによる情報発信を含む。)の複製・加筆による偽情報の作成及び流布を防止するため，原本性の維持に努めなければならない。

(情報機器及び記憶媒体の処分)

第9　公開又は非公開を問わず，情報機器及び記憶媒体を破棄する場合は，その処分方法に注意しなければならない。特に，ハードディスク及びフロッピーディスク等の記憶媒体の廃棄は，通常の消去操作や数回の上書き消去では情報を復元できる点に十分配慮し，情報の復元を不可能とする措置を施さなければならない。また，情報機器の記憶媒体を保守契約により交換する場合又はレンタル機器の撤去を行う場合は，撤去後の記憶媒体の処理法についても十分配慮しなければならない。

(クライアント機器の認証)

第10　非公開情報を参照可能なクライアント機器を設置する場合(据付及び一時的設置の場合を含む。)，使用者がクライアント機器を使用する前に物理的認証又は電子的認証，あるいは両方を経なければならない。

2　電子的認証を用いる場合，ディスクブートによる電子的認証すり抜けに対する対

策を講じなければならない。

(据付型クライアント機器の盗難対策)

第11　セキュリティ規程第6条に定める部局情報セキュリティ管理者(以下「部局セキュリティ管理者」という。)は，据付型クライアント機器が盗難等により学外に持ち出されないよう何らかの対策を講じなければならない。

(ネットワークへの接続)

第12　部局セキュリティ管理者は，ネットワークケーブルを使用する場合には，過失によるネットワークケーブルの切断を防ぐための措置を講じなければならない。

2　セキュリティ規程第4条に定める部門情報セキュリティ責任者(以下「部門セキュリティ責任者」という。)は，有線，無線どちらの場合においても，ネットワークの盗聴に対する対策を講じなければならない。

3　部局セキュリティ管理者は，クライアント機器接続用のネットワークケーブルに違うコンピュータが接続されないよう，物理アドレスとIPアドレスの定期的な監視に努めなければならない。

(貸出型クライアント機器の備品管理)

第13　部局セキュリティ管理者は，当該部局の構成員がクライアント機器を学外へ持ち出す場合においては，貸し出しの事実について管理しなければならない。

2　部局セキュリティ管理者は，当該部局の構成員が個人で所有する機器を学内に持ち込みクライアント機器として使用する場合及びこれを学外へ持ち出す場合においては，この事実について管理しなければならない。

3　全構成員及び一般利用者は，クライアント機器経由による秘密又は非公開情報の漏えいが発生しないよう留意しなければならない。

4　全構成員以外の者がクライアント機器を学外に持ち出すことは，原則として禁止する。

(管理区域の設置)

第14　サーバ及びクライアント機器は，設定された管理区域に設置されなければならない。

2　管理区域内はサーバの動作保証範囲内の温度及び湿度を24時間保たなければならない。

3　管理区域内の物理的隔離の度合いは守るべきサーバの重要性に応じて段階的に設定しなければならない。

4　重要なサーバ(重要なサーバとは，停止したときに大学内の業務遂行に重大な支障を来すサーバを指す。以下同じ。)に対しては物理的に区切られており，第三者の認証と入退室の記録が残される区域を設定するものとする。ただし，重要度の軽微なサーバについては，鍵などによる認証による入退室管理形態であっても可とする。

5　管理区域の物理的な場所は，当該サーバのシステム管理者以外には非公開とする。

6　部局セキュリティ管理者は，当該部局内のサーバを把握しなければならない。

(電源)

第15　部局セキュリティ管理者は，電源を供給する際には，電圧の流動や突発的な停電，過電流に対応する装置を経由するよう努めなければならない。

(データのバックアップ)

第16　サーバに記録されるデータは，定期的にバックアップを行わなければならない。

2　バックアップスケジュールは，サーバの重要度に応じて決定するものとする。

3　データをバックアップしたメディアは，温度及び湿度が適切な場所に保管するものとする。

4　重要なデータのバックアップは，複数本作成し物理的に離れた場所に保管するものとする。

5　データをバックアップしたメディアは，認証による入退室管理が行われている管理区域内に保管するものとする。

(サーバの多重化)

第17　ダウンタイムを短くすることを求められるサーバについては，多重化を検討するものとする。なお，多重化した場合には，順番に運用機を切り替えるか，一定時間ごとのチェック等によりスタンバイ機が故障してないことを確認しなければならない。

(サーバ盗難への対策)

第18　部局セキュリティ責任者は，サーバが管理区域から持ち出されないよう何らかの対策を講じなければならない。

(災害への対策)

第19　重要なサーバは，耐震を考慮した据付を行うものとする。

2　管理区域には，火災の一次消火手段が提供されていなければならない。

(コンソールポートの隔離)

第20　ルータ，インテリジェントスイッチは，コンソールポート，管理ポートが許可された特定の情報システム管理者以外は使用できないように電子的認証等を用いるものとする。

2　ルータ，インテリジェントスイッチは，施錠などによって物理的に隔離された区域に設置するよう努めるものとする。

(設置場所の秘匿)

第21　部局情報システム(部局セキュリティ責任者が管理する情報システムをいう。以下同じ。)を構成する機器をはじめ，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非公開とする。

(ネットワークへの接続の制限)

第22　非公開情報システムへは，原則として物理的認証または電子的認証，あるいは，両方を経た後でなければ，コンピュータを接続してはならない。

(ネットワークケーブル)

第23　部局情報システムに接続されたネットワークケーブル及び重要と思われるネットワークケーブルについては，故意又は過失によるケーブル切断を防ぐ措置を

施さなければならない。
2　有線，無線どちらの場合においても，ネットワークの盗聴に対する対策を講じなければならない。
(ネットワークの多重化)
第24　機器の障害によるネットワークの切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目指すものとする。
(保守)
第25　機器の保守においては，保守部品をできるだけ確保し，迅速に保守を行える体制を整えなければならない。
2　業者が行う保守においては，パスワードやネットワーク構成などの非公開情報の開示についての守秘義務契約を結ばなければならない。
(ネットワーク設計，機器導入及び設定)
第26　大学での新たなネットワークの設計及び構築にあたっては，教育，研究，医療及び管理事務といった目的の異なるネットワーク上の情報を物理的又は論理的に混在させないようにしなければならない。
2　ネットワークの改変を行う場合は，情報セキュリティ委員会の許可を得なければならない。
(ネットワーク機器)
第27　部局セキュリティ管理者は，ルータ，ソフトウェア，設定可能なハブ等が機器障害や権限のないアクセスによって機器の構成や制御機能が損なわれないように管理しなければならない。また，これらの機能を常に最新のものとするように努めなければならない。
(ネットワークの無許可利用等)
第28　ネットワークに接続する装置は，共同利用端末を除き，不特定多数の手に触れさせてはならない。
2　ネットワークのセキュリティ機能の管理を回避する目的でのバックドア(PPPサーバ，コンピュータに接続する公衆回線，VPN装置及びソフトウェア等をいう。)の設置を原則禁止する。
3　独自のハードウェア回線等を設置する場合には，情報セキュリティ委員会の許可を受けなければならない。また，情報セキュリティ委員会の求めに応じて運用状況を報告しなければならない。
(ネットワークの日常運用)
第29　部局情報セキュリティ担当者は，ファイアウォールや侵入検知システムのログを一定期間保存しなければならない。
2　部局情報セキュリティ担当者は，情報システムへのアクセス記録を取得し一定期間保存しなければならない。また，定期的にそれらのログを分析し，侵入の試みがなされていないかなどをチェックしなければならない。
3　部局情報セキュリティ担当者は，ネットワークに対して不正な接続の監視を行わ

なければならない。

(端末機器等に関する基準)

第30　セキュリティ規程第3条に定める最高情報セキュリティ責任者は，必要に応じ，ネットワークに接続を許される機器の満たすべき最低限のセキュリティ対策基準を示す技術ガイドラインを，セキュリティポリシーに従って策定しなければならない。また，ガイドラインの基準に満たない機器をネットワークに接続してはならない。

2　全構成員及び一般利用者は，ガイドラインにかかわらず，常に最新のセキュリティ情報に注意を払い，端末機器を安全に運用できるように努力しなければならない。

3　全構成員及び一般利用者は，情報セキュリティ運営室または情報セキュリティ委員会の要請があった場合には，ログ等に関する情報を情報セキュリティ運営室または情報セキュリティ委員会に対して開示しなければならない。

(端末機器設置運用基準)

第31　ネットワークに接続する機器は，利用者を何らかの方法で認証(部屋の入退室管理といった物理的な方法でも可とする。)できなければならない。

2　機器を設置しようとする者は，設定作業(セキュリティ対策を含む。)の完了していない装置をネットワークに接続してはならない。

3　機器の管理者は，設置機器の利用者を特定可能でなければならない。

附　則

この要項は，平成24年4月10日から実施し，平成24年4月1日から適用する。

附　則

この要項は，令和 2 年 6 月 11 日から施行し，改正後の旭川医科大学情報セキュリティ対策実施要項は，令和元年 8 月 26 日から適用する。