国立大学法人室蘭工業大学情報システム運用及び管理規程

平成21年３月24日
室工大規程第３号

目次

第１章　総則

（目的）

第１条　この規程は、国立大学法人室蘭工業大学（以下「本学」という。）における情報システムの運用及び管理に関する事項を定めることにより、本学の有する情報資産を適正に保護、活用し、並びに情報システムの信頼性、安全性及び効率性の向上に資することを目的とする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）　基本規程　国立大学法人室蘭工業大学情報システム運用基本規程をいう。

（２）　情報資産　情報システム、情報ネットワークに接続された情報ネットワーク機器並びに電子計算機及びそこで取り扱われる情報をいう。

（３）　情報ネットワーク機器　情報ネットワークの接続のために設置され、電子計算機により情報ネットワーク上を送受信される情報の制御を行うための装置（ファイアウォール、ルータ、ハブ、情報コンセント又は無線ネットワークアクセスポイントを含む。）をいう。

（４）　電子計算機　コンピュータ全般のことを指し、オペレーティングシステム、接続される周辺機器を含むサーバ装置及び端末をいう。

（５）　管理者権限　利用者やシステムを管理するために特別に与えられる権限をいう。

（６）　安全区域　電子計算機及び情報ネットワーク機器（以下「電子計算機等」という。）を設置した事務室、研究室、教室又はサーバルーム等の内部であって、利用者等以外の者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。

（７）　利用者等　基本規程において定める利用者のほか、本学の情報システムを介して情報資産を取扱う者をいう。

（８）　主体認証　識別符号（ユーザＩＤ等）を提示した利用者等又は電子計算機等が、情報システムにアクセスする正当な権限を有するか否かを検証することをいう。ユーザＩＤとともに正しい方法で主体認証情報（パスワード等）が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した利用者等又は電子計算機等を正当な権限を有するものとして認識する。ただし、「認証」という用語は、公的又は第三者が証明するという意味を持つが、この規程における「主体認証」については、公的又は第三者による証明に限るものではない。

（９） 権限管理　主体認証に係る情報（識別コード及び主体認証情報を含む。）の付与及びアクセス制御における許可情報の付与を管理することをいう。
(10) 識別符号（ユーザＩＤ等）　主体認証を行うために、利用者等又は電子計算機等が提示する符号のうち、情報システムが利用者等又は電子計算機等を特定して認識する符号をいう。
(11) 主体認証情報（パスワード等）　主体認証を行うために、利用者等又は電子計算機等が提示する情報のうち、情報システムが利用者等又は電子計算機等を正当な権限を有するものとして認識する情報をいう。
(12) アカウント　主体認証を行う必要があると認めた情報システムにおいて、利用者等又は電子計算機等に付与された正当な権限をいう。また、狭義には、利用者等又は電子計算機等に付与されたユーザＩＤ及びパスワードの組み合わせ、又はそれらのいずれかを指して「アカウント」という。
(13) 証跡管理　情報ネットワーク機器で動作の記録を採取し、その記録を管理することをいう。
(14) 要機密情報　本学の情報システムで取扱う情報のうち、秘密文書に相当する機密性を要する情報、又はその漏えいにより利用者の権利が侵害され、又は本学の業務の遂行に支障を及ぼすおそれがある情報
(15) 要保全情報　本学の情報システムで取扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され、又は本学の業務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
(16) 要安定情報　本学の情報システムで取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され、又は本学の業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
(17) 要保護情報　要機密情報、要保全情報及び要安定情報をいう。
(18) その他の用語の定義は、基本規程の定めるところによる。

（適用範囲）

第３条　この規程は、情報資産及び情報システムを運用及び管理する者に適用する。

（禁止事項）

第４条　情報セキュリティ責任者及び情報技術担当者は、次に掲げる行為を行ってはならない。
（１） 情報資産の目的外利用
（２） 守秘義務に違反する情報の開示
（３） 全学実施責任者の許可なく情報ネットワーク上の通信を監視し、又は情報ネットワーク機器及び電子計算機の利用記録を採取する行為
（４） 全学実施責任者の要請に基づかずにセキュリティ上の脆弱性を検知する行為
（５） その他法令に基づく処罰の対象となり、又は損害賠償等の民事責任を発生させる情報の発信
（６） 管理者権限を濫用する行為
（７） 上記の行為を助長する行為

第２章　情報システムのライフサイクル

第１節　設置時

（セキュリティホール対策）

第５条　情報セキュリティ責任者は、電子計算機及び情報ネットワーク機器の構築又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホールの対策を実施する。

（不正プログラム対策）

第６条　全学実施責任者は、不正プログラム感染の回避を目的とした利用者等に対する留意事項を含む日常的実施事項を定める。

２　情報セキュリティ責任者は、不正プログラムから電子計算機を保護するため、アンチウイルスソフトウェアを導入する等の対策を講ずる。ただし、当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。

３　情報セキュリティ責任者は、想定される不正プログラムの感染経路のすべてにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施する。

（サービス不能攻撃対策）

第７条　情報セキュリティ責任者は、要安定情報を取扱う情報システムについては、サービス提供に

必要な電子計算機及び情報ネットワーク機器が装備している機能をサービス不能攻撃対策に活用する。

（安全区域）

第８条　情報セキュリティ責任者は、情報システムによるリスク（物理的損壊又は情報の漏えい若しくは改ざん等のリスクを含む。）を検討し、安全区域に施設及び環境面からの対策を実施する。

２　情報セキュリティ責任者は、安全区域に不審者を立ち入らせない措置を講ずる。

３　情報セキュリティ責任者は、要保護情報を取扱う情報システムについては、電子計算機を安全区域に設置する。ただし、モバイルＰＣについて全学実施責任者の承認を得た場合は、この限りでない。

４　情報セキュリティ責任者は、情報ネットワーク機器を安全区域に設置する。

（主体認証と権限管理）

第９条　情報セキュリティ責任者は、利用者等が電子計算機にログインする場合には主体認証を行うように電子計算機を構成する。

２　情報セキュリティ責任者は、ログオンした利用者等のユーザＩＤに対して、権限管理を行う。

（サーバ装置の対策）

第10条　情報セキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報を暗号化する。

２　情報セキュリティ責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定める。

３　情報セキュリティ責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止する。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能については可能な限り無効化する。

（通信回線の対策）

第11条　情報セキュリティ責任者は、通信回線構築によるリスク（物理的損壊又は情報の漏えい若しくは改ざん等のリスクを含む。）を検討し、通信回線を構築する。

２　情報セキュリティ責任者は、要安定情報を取扱う情報システムについては、通信回線及び情報ネットワーク機器に求められる通信性能を発揮できる能力を､将来の見通しを含め検討し､確保する。

３　情報セキュリティ責任者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化する。

４　情報セキュリティ責任者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、選択する。

５　情報セキュリティ責任者は、遠隔地から情報ネットワーク機器に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保する。

６　情報セキュリティ責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決める。

７　情報セキュリティ責任者は、情報ネットワーク機器上で証跡管理を行う必要性を検討し、必要と認めた場合には実施する。

（学外通信回線との接続）

第12条　全学実施責任者は、最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）の承認を得た上で、学内通信回線を学外通信回線と接続するものとする。利用者等による学内通信回線と学外通信回線との接続は禁止する。

２　全学実施責任者は、学内通信回線を学外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している学内通信回線又は学外通信回線から独立した通信回線として学内通信回線を構築する。

（上流ネットワークとの関係）

第13条　全学実施責任者は、本学情報ネットワークを構築し運用するに当たっては、本学情報ネットワークと接続される上流ネットワークとの整合性に留意する。

第２節　運用時

（セキュリティホール対策）
第14条　情報セキュリティ責任者は、管理対象となる電子計算機及び情報ネットワーク機器上で利用しているソフトウェアに関連する公開されたセキュリティホールに関連する情報を適宜入手する。
２　情報セキュリティ責任者は、入手したセキュリティホールに関連する情報から、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、次に掲げる事項について対策を講ずる。
（１）　対策の必要性
（２）　対策方法
（３）　対策方法が存在しない場合の一時的な回避方法
（４）　対策方法又は回避方法が情報システムに与える影響
（５）　対策の実施予定
（６）　対策テストの必要性
（７）　対策テストの方法
（８）　対策テストの実施予定
３　情報セキュリティ責任者は、信頼できる方法で対策用ファイルを入手する。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行う。
（不正プログラム対策）
第15条　情報セキュリティ責任者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、利用者等にその対処の実施に関する指示を行う。
（脆弱性検査）
第16条　情報セキュリティ責任者は、全学実施責任者の指示のもと行われる脆弱性検査を受け、セキュリティの維持に努める。
２　情報セキュリティ責任者が正当な理由なく脆弱性検査を受けない、または脆弱性検査の結果に基づいて適切な対処を行わない場合、全学実施責任者は当該情報セキュリティ責任者が管理する情報機器をネットワークから遮断することができるものとする。
（接続の管理）
第17条　全学実施責任者は、情報ネットワークに関する接続の申請を受けた場合は、管理運営部局に対して接続の諾否を通知し必要な指示を行う。
２　管理運営部局は、全学実施責任者からの指示に基づき、情報セキュリティ責任者に対して接続の諾否を通知し、接続が許諾された場合は、情報ネットワークで使用するドメイン名やＩＰアドレス等のネットワーク情報について通知する。
（ネットワーク情報の管理）
第18条　情報セキュリティ責任者は、情報ネットワークで使用するドメイン名やＩＰアドレス等のネットワーク情報について、管理運営部局から割り当てを受け、利用者等からの利用形態に応じて適切に分配し管理する。
（サーバ装置の対策）
第19条　情報セキュリティ責任者は、定期的にサーバ装置の構成の変更を確認する。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対応する。
２　情報セキュリティ責任者は、要安定情報を取扱うサーバ装置に保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理する。
３　情報セキュリティ責任者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録する。
４　情報セキュリティ責任者は、サーバ装置上で証跡管理を行う必要性を検討し、必要と認めた場合には実施する。
５　情報セキュリティ責任者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期する。
（通信回線の対策）
第20条　情報セキュリティ責任者は、通信回線を利用する電子計算機のホストＩＤ、電子計算機の利用者等と当該利用者等のユーザＩＤの対応及び通信回線の利用部局を含む事項の管理を行う。
２　情報セキュリティ責任者は、定期的に通信回線の構成、情報ネットワーク機器の設定、アクセス

制御の設定又はユーザＩＤを含む事項の変更を確認する。また、当該変更によって生ずる通信回線のセキュリティへの影響を特定し、対応する。
3　情報セキュリティ責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更する。
4　情報セキュリティ責任者は、全学実施責任者の許可を受けていない電子計算機及び情報ネットワーク機器を通信回線に接続させないものとする。
5　情報セキュリティ責任者は、要安定情報を取扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測又は検知する。
6　情報セキュリティ責任者は、情報システムにおいて基準となる時刻に、情報ネットワーク機器の時刻を同期する。

（学外通信回線との接続）

第21条　全学実施責任者は、学内通信回線と学外通信回線の接続において情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している学内通信回線又は学外通信回線から独立した通信回線に構成を変更する。
2　全学実施責任者は、通信回線の変更に際し、及び定期的に、アクセス制御の設定の見直しを行う。
3　全学実施責任者は、定期的に、学外通信回線から通信することが可能な学内通信回線及び情報ネットワーク機器のセキュリティホールを検査する。
4　全学実施責任者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視する。

第３節　運用終了時

（電子計算機の対策）

第22条　情報セキュリティ責任者は、電子計算機の運用を終了する場合に、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊等の方法を用いて、すべての情報を復元が困難な状態にする。

（情報ネットワーク機器の対策）

第23条　情報セキュリティ責任者は、情報ネットワーク機器の利用を終了する場合には、情報ネットワーク機器の内蔵記録媒体のすべての情報を復元が困難な状態にする。

第４節　ＰＤＣＡサイクル

（サーバ装置の計画及び設計）

第24条　情報セキュリティ責任者は、サーバ装置について、導入時、運用時並びに運用終了時までのライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、全学実施責任者に求めるものとする。
2　情報セキュリティ責任者は、サーバ装置のセキュリティ要件を決定する。
3　情報セキュリティ責任者は、サーバ装置のセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策並びにサーバ装置の構成要素についての対策について定める。
4　情報セキュリティ責任者は、構築したサーバ装置を運用段階へ導入するに当たって、情報セキュリティの観点から、導入のための手順及び環境を定める。

（サーバ装置の構築、運用及び監視）

第25条　情報セキュリティ責任者は、サーバ装置の構築、運用及び監視に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行う。

（サーバ装置の情報セキュリティ対策の見直し）

第26条　情報セキュリティ責任者は、サーバ装置の情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずる。

第３章　主体認証

（主体認証機能の導入）

第27条　情報セキュリティ責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討する。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断する。
2　情報セキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、識別及

び主体認証を行う機能を設ける。
3　情報セキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、パスワードを秘密にする必要がある場合には、当該パスワードが明らかにならないように次のとおり管理する。
（1）　パスワードを保存する場合には、その内容の暗号化を行うこと。
（2）　パスワードを通信する場合には、その内容の暗号化を行うこと。
（3）　保存又は通信を行う際に暗号化を行うことができない場合には、利用者等に自らのパスワードを設定、変更、提供（入力）させる際に、暗号化が行われない旨を通知すること。
4　情報セキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、利用者等にパスワードの定期的な変更を求める場合には、利用者等に対して定期的な変更を促す機能のほか、次に掲げるいずれかの機能を設ける。
（1）　利用者等が定期的に変更しているか否かを確認する機能
（2）　利用者等が定期的に変更しなければ、情報システムの利用を継続させない機能
5　情報セキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、パスワード又はＩＣカードを他者に使用され又は使用される危険性を認識した場合に、直ちに当該パスワード若しくはＩＣカードによる主体認証を停止する機能又はこれに対応するユーザＩＤによる情報システムの利用を停止する機能を設ける。
6　情報セキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識による主体認証方式を用いる場合には、次に掲げる機能を設ける。
（1）　利用者等が、自らのパスワードを設定する機能
（2）　利用者等が設定したパスワードを、他者が容易に知ることができないように保持する機能
7　情報セキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、知識、所有、生体情報以外の主体認証方式を用いる場合には、次の各号の要件について検証した上で、当該主体認証方式に適用することが可能な要件をすべて満たさなければならない。また、用いる方式に応じて、次の各号を含む要件を定めるものとする。
（1）　正当な主体以外の主体を誤って認証しないこと。
（2）　正当な主体が本人の責任ではない理由によって認証を妨げられないこと。
（3）　正当な主体が容易に他者にパスワードを付与及び貸与ができないこと。
（4）　パスワードが容易に複製できないこと。
（5）　ログオンを個々に無効化できる手段があること。
（6）　主体認証について業務遂行に十分な可用性があること。
（7）　新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられること。
（8）　主体に付与したパスワードを使用することが不可能になった際に、正当な主体に対してパスワードを安全に再発行できること。
8　情報セキュリティ責任者は、生体情報による主体認証方式を用いる場合には、当該生体情報を本人から事前に同意を得た目的以外の目的で使用してはならない。また、当該生体情報について、本人のプライバシーを侵害しないように留意しなければならない。
9　全学実施責任者は、セキュリティ侵害又はその可能性が認められる場合、パスワードの変更を求め又はアカウントを失効させることができる。

第４章　アクセス制御

（アクセス制御機能の導入）
第28条　情報セキュリティ責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討する。この場合、要保護情報を取扱う情報システムについては、アクセス制御を行う必要があると判断する。
2　情報セキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設ける。
（利用者等による適正なアクセス制御）
第29条　情報セキュリティ責任者は、それぞれの情報システムに応じたアクセス制御の措置を講ずるよう利用者等に指示する。

２　利用者等は、情報システムに装備された機能を用いて、必要なアクセス制御の設定を行う。

（無権限のアクセス対策）

第30条　情報セキュリティ責任者は、無権限のアクセス行為を発見した場合は、速やかに全学実施責任者に報告する。

２　全学実施責任者は、前項の報告を受けた場合は、新たな防止対策等必要な措置を講ずる。

第５章　アカウント管理

（アカウント管理機能の導入）

第31条　情報セキュリティ責任者は、すべての情報システムについて、アカウント管理を行う必要性の有無を検討する。この場合、要保護情報を取扱う情報システムについては、アカウント管理を行う必要があると判断する。

２　情報セキュリティ責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理を行う機能を設ける。

（アカウント管理手続の整備）

第32条　情報セキュリティ責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理について、次に掲げる事項を含む手続を明確にしなければならない。

（１）　主体からの申請に基づいてアカウント管理を行う場合には、その申請者が正当な主体であることを確認するための手続

（２）　パスワードの初期配布方法及び変更管理手続

（３）　アクセス制御情報の設定方法及び変更管理手続

２　情報セキュリティ責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理を行う者（以下「アカウント管理者」という。）を定める。

（共用アカウント）

第33条　情報セキュリティ責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、共用アカウントの利用許可については、情報システムごとにその必要性を判断するものとする。

２　アカウント管理者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウントを発行する際に、それが共用アカウントか、共用ではないアカウントかの区別を利用者等に通知する。ただし、共用アカウントは、情報セキュリティ責任者が、その利用を認めた情報システムでのみ付与することができる。

（アカウントの発行）

第34条　アカウント管理者は、利用者等からのアカウント発行申請を受理したときは、申請者が第49条第２項第３号による処分期間中である場合を除き、遅滞なくアカウントを発行しなければならない。

２　アカウント管理者は、アカウント管理を行う必要があると認めた情報システムにおいて、情報システムを利用する許可を得た主体に対してのみ、アカウントを発行する。

３　アカウント管理者は、アカウント管理を行う必要があると認めた情報システムにおいて、管理者権限を持つアカウントを、業務又は業務上の責務に即した場合に限定して付与する。

４　アカウント管理者は、アカウント管理を行う必要があると認めた情報システムにおいて、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス制御に係る設定をする。

（アカウント発行の報告）

第35条　アカウント管理者は、アカウントを発行したときは、速やかにその旨を情報セキュリティ責任者に報告する。

２　全学実施責任者は、必要により情報セキュリティ責任者にアカウント発行の報告を求めることができる。

（アカウントの有効性検証）

第36条　アカウント管理者は、発行済みのアカウントについて、次に掲げる項目を１か月毎に確認しなければならない。

（１）　利用資格を失ったもの

（２）　情報セキュリティ責任者が指定する削除保留期限を過ぎたもの

（３）　パスワード手順に違反したパスワードが設定されているもの

（４）　６か月以上使用されていないもの

２　アカウント管理者は、人事異動等、アカウントを追加又は削除する時に、不適切なアクセス制御設定の有無を点検しなければならない。

（アカウントの削除）

第37条　アカウント管理者は、前条第１項第１号及び第２号に該当するアカウントを発見したとき、又は第49条第２項第３号による削除命令を受けたときは、速やかにそのアカウントを削除し、その旨を情報セキュリティ責任者に報告しなければならない。

２　アカウント管理者は、アカウント管理を行う必要があると認めた情報システムにおいて、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等のアカウントを削除し、その旨を情報セキュリティ責任者に報告しなければならない。

３　アカウント管理者は、アカウント管理を行う必要があると認めた情報システムにおいて、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等に交付した主体認証が記録された媒体（ＩＣカード等）を返還させ、その旨を情報セキュリティ責任者に報告しなければならない。

４　情報セキュリティ責任者は、第１項から前項までの報告を受けたときは、速やかにその旨を利用者等に通知する。ただし、電話、郵便等の伝達手段によっても通知ができない場合はこの限りでない。

５　全学実施責任者は、必要により情報セキュリティ責任者にアカウント削除の報告を求めることができる。

（アカウントの停止）

第38条　アカウント管理者は､第36条第１項第３号及び第４号に該当するアカウントを発見したとき、第49条第２項第３号による停止命令を受けたとき、又はパスワードが他者に使用され若しくはその危険が発生したことの報告を受けたときは、速やかにそのアカウントを停止し、その旨を情報セキュリティ責任者に報告しなければならない。

２　情報セキュリティ責任者は、前項の措置の報告を受けたときは、速やかにその旨を利用者等に通知する。ただし、電話、郵便等の伝達手段によっても通知ができない場合はこの限りでない。

３　全学実施責任者は、必要により情報セキュリティ責任者にアカウントの停止の報告を求めることができる。

（アカウントの復帰）

第39条　アカウントの停止を受けた利用者等がアカウント停止からの復帰を希望するときは、その旨を情報セキュリティ責任者に申し出るものとする。

２　情報セキュリティ責任者は、前項の申し出を受けたときは、アカウント管理者に当該アカウントの安全性の確認及びアカウントの復帰を指示する。

３　アカウント管理者は、前項の指示に従い当該アカウントの安全性を確認した後、速やかにアカウントを復帰させる。

（管理者権限を持つアカウントの利用）

第40条　管理者権限を持つアカウントを付与された者は、管理者としての業務遂行時に限定して、当該アカウントを利用する。

第６章　証跡管理

（証跡管理機能の導入）

第41条　情報セキュリティ責任者は、すべての情報システムについて、証跡管理を行う必要性の有無を検討する。

２　情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設ける。

３　情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、事象を証跡として記録するに当たり、事象ごとに必要な情報項目を記録するように情報システムの設定を行う。

４　情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方針を整備し、必要に応じ、これらの場合に対応するための機能を情報システムに設ける。

５　情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得

した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行い、外部記録媒体等その他の装置・媒体に記録した証跡についてはこれを適正に管理する。

（証跡の取得と保存）

第42条　情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、情報システムに設けた機能を利用して、証跡を記録する。

２　情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間を定め、当該保存期間が満了する日まで証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去する。

３　情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合は、定められた対処を行う。

（証跡管理に関する利用者等への周知）

第43条　全学実施責任者又は情報セキュリティ責任者は、証跡を取得する必要があると認めた情報システムにおいては、利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明する。

（通信の監視）

第44条　利用者等は、ネットワークを通じて行われる通信を傍受してはならない。ただし、全学実施責任者は、セキュリティ確保のため、あらかじめ指定した者に、ネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

２　全学実施責任者は、監視の範囲をあらかじめ具体的に定めておかなければならない。ただし、不正アクセス行為又はこれに類する重大なセキュリティ侵害に対処するために特に必要と認められる場合、全学実施責任者は、セキュリティ侵害の緊急性、内容及び程度に応じて、対処のために不可欠と認められる情報について、監視を行うよう命ずることができる。

３　監視を行う者は、監視によって知った通信の内容又は個人情報を、他の者に伝達してはならない。ただし、前項ただし書きに定める情報については、全学実施責任者及び情報基盤委員会に伝達することができる。

４　全学実施責任者は、監視を行う者に対して、監視記録の作成を命ずるとともに、当該監視記録の保存期間をあらかじめ指示するものとする。監視を行う者は、指示された期間を経過した監視記録を直ちに破棄しなければならない。ただし、監視記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。

５　監視を行う者及び監視記録の伝達を受けた者は、ネットワーク運用及び管理のために、これを閲覧し、かつ、保存することができる。ただし、監視記録を不必要に閲覧してはならない。

６　不必要となった監視記録については、直ちに破棄しなければならない。また、監視記録の内容を、法令に基づく場合等を除き、他の者に伝達してはならない。

（利用記録）

第45条　複数の者が利用する情報システムの情報セキュリティ責任者は、当該機器に係る利用記録（以下「利用記録」という。）をあらかじめ定めた目的の範囲でのみ採取することができる。ただし、当該目的との関連で必要性の認められない利用記録を採取することはできない。

２　前項に規定する目的は、法令の遵守、情報セキュリティの確保、課金その他当該情報システムの利用に必要なものに限られるものとし、個人情報の取得を目的とすることはできない。

３　当該情報システムの情報セキュリティ責任者は、第１項に規定する目的のために、利用記録を閲覧することができる。ただし、他人の個人情報及び通信内容を不必要に閲覧してはならない。

４　当該情報システムの情報セキュリティ責任者は、第２項に規定する目的のために、利用記録を他の者に伝達することができる。

５　第１項の規定により情報システムの利用を記録しようとする者は、第２項の目的、これによって採取しようとする利用記録の範囲及び前項により利用記録を伝達する者を、あらかじめ全学実施責任者に申告し、かつ、当該機器の利用者等に開示しなければならない。全学実施責任者は、申告の内容を不適切と認めるときは、これを修正させるものとする。

６　当該システムの情報セキュリティ責任者又は利用記録の伝達を受けた者は、第１項に規定する目的のために、これを保有することができる。不要となった利用記録は、直ちに破棄しなければなら

ない。ただし、当該システムの情報セキュリティ責任者は、利用記録から個人情報に係る部分を削除して、ネットワーク運用及び管理のための資料とすることができる。

（個人情報の取得と管理）

第46条　情報セキュリティ責任者は、電子的に個人情報の提供を求める場合、提供を求める情報の範囲、利用の目的、その情報が伝達される範囲を、あらかじめ相手方に示さなければならない。

２　前項の個人情報は、当人の請求により開示、訂正又は削除をしなければならない。また、そのための手続を示さなければならない。

（利用者等が保有する情報の保護）

第47条　利用者等が保有する情報は、ネットワーク運用に不可欠な範囲又はインシデント対応に不可欠な範囲において、閲覧、複製又は提供することができる。

第７章　暗号と電子署名

（暗号化機能及び電子署名の付与機能の導入）

第48条　情報セキュリティ責任者は、要機密情報（書面を除く。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討する。

２　情報セキュリティ責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設ける。

３　情報セキュリティ責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討する。

４　情報セキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムには、電子署名の付与を行う機能を設ける。

第８章　違反と例外措置

（違反への対応）

第49条　全学実施責任者は、情報セキュリティに係る違反を受けた場合及び自らが違反を知った場合には、速やかに調査を行い、事実を確認する。事実の確認に当たっては、可能な限り当該行為を行った者の意見を聴取する。

２　全学実施責任者は、調査によって違反行為が判明したときには、速やかにＣＩＳＯに報告する。

３　ＣＩＳＯは、違反行為の報告を受けたときには、次に掲げる措置を講ずることができる。

（１）　当該行為者に対する当該行為の中止命令

（２）　情報セキュリティ責任者に対する当該行為に係る情報発信の遮断命令

（３）　情報セキュリティ責任者に対する当該行為者のアカウント停止命令又は削除命令

（４）　その他法令に基づく措置

（例外措置）

第50条　情報基盤委員会は、情報セキュリティに係る例外措置の適用についての審査手続を整備する。

２　ＣＩＳＯは、利用者等からの例外措置の適用に係る申請を、定められた審査手続に従って審査し、許可の可否を決定する。また、決定の際に、次に掲げる項目を含む例外措置の適用審査記録を整備しなければならない。

（１）　申請内容

ア　申請者の情報

イ　例外措置の適用を申請する情報セキュリティ関係規程の該当箇所

ウ　例外措置の適用を申請する期間

エ　例外措置の適用を申請する措置内容

オ　例外措置の適用を終了した旨の報告方法

カ　例外措置の適用を申請する理由

（２）　審査結果の内容

ア　許可又は不許可の別

イ　許可又は不許可の理由

ウ　例外措置の適用を許可した情報セキュリティ関係規程の適用箇所

エ　例外措置の適用を許可した期間

オ　許可した措置内容

カ　例外措置を終了した旨の報告方法

3　ＣＩＳＯは、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な対応を講ずる。ただし、全学総括責任者が報告を要しないとした場合は、この限りでない。

第９章　インシデント対応

（インシデントの発生に備えた事前準備）

第51条　ＣＩＳＯは、情報セキュリティに関するインシデント（故障を含む。）が発生した場合、被害の拡大を防ぐとともに、インシデントから復旧するための体制を整備しなければならない。

2　全学実施責任者は、インシデントについて利用者等からの報告手順を整備し、当該報告手段をすべての利用者等に周知しなければならない。

3　インシデントへの対応手順はＣＩＳＯが別に定める。

第10章　学外の情報セキュリティ水準の低下を招く行為の禁止

（学外の情報セキュリティ水準の低下を招く行為の防止）

第52条　情報セキュリティ責任者は、学外の情報セキュリティ水準の低下を招かぬよう、以下の内容を確保すること。

（１）　提供するアプリケーション・コンテンツが不正プログラムを含まないようにすること。

（２）　提供するアプリケーションが脆弱性を含まないこと。

（３）　実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

（４）　電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

（５）　提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

（６）　サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

第11章　教育・研修

（情報セキュリティ対策の教育・研修）

第53条　全学実施責任者は、情報セキュリティ対策について、情報セキュリティ責任者、情報技術担当者及び利用者等（以下「教育啓発対象者」という。）に対し、その啓発を行う。

2　全学実施責任者は、情報セキュリティ対策について、教育啓発対象者に対する教育・研修の内容及び体制を整備する。

3　全学実施責任者は、教育啓発対象者の入学時、着任時、異動時に３か月以内に受講できるように、情報セキュリティ対策の教育を企画、立案し、その体制を整備する。

4　全学実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備する。

5　全学実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況について、当該教育啓発対象者の所属する情報セキュリティ責任者に通知する。

6　情報セキュリティ責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告する。教育啓発対象者が当該勧告に従わない場合には、全学実施責任者にその旨を報告する。

7　全学実施責任者は、毎年度一回、ＣＩＳＯ及び情報基盤委員会に対して、教育啓発対象者の情報セキュリティ対策の教育の受講状況について報告する。

8　その他、教育・研修に関する事項については、別に定める。

第12章　評価

（自己点検に関する年度計画の策定）

第54条　全学実施責任者は、年度自己点検計画を策定する。

2　全学実施責任者は、年度自己点検計画に基づき、自己点検票及び自己点検の実施手順を作成する。

（自己点検の実施）

第55条　全学実施責任者は、情報セキュリティ責任者に対して、自己点検の実施を指示する。
２　情報セキュリティ責任者は、全学実施責任者から指示された自己点検票及び自己点検の実施手順を用いて自己点検を実施する。
（自己点検結果の評価・改善）
第56条　情報セキュリティ責任者は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、全学実施責任者にその旨を報告すること。
２　全学実施責任者は、情報セキュリティ責任者による自己点検及び改善が行われていることを確認し、その結果を評価する。
３　全学実施責任者は、必要があると判断した場合には情報セキュリティ責任者に更なる改善を指示する。
（監査）
第57条　情報セキュリティ責任者その他の関係者は、ＣＩＳＯの行う監査の適正かつ円滑な実施に協力する。

第13章　雑則

（雑則）
第58条　この規程に定めるもののほか、情報システムの運用及び管理に関し必要な事項は、別に定める。

附　則

この規程は、平成21年３月24日から施行する。

附　則（平成24年度室工大規程第４号）

この規程は、平成24年７月26日から施行する。

附　則（平成28年度室工大規程第26号）

この規程は、平成29年３月27日から施行する。