名城大学教育研究情報ネットワークシステム（メイネット）

セキュリティポリシー

名城大学は、「穏健中正で実行力に富み、国家、社会の信頼に値する人材を育成すること」を立学の精神としている。この立学の精神に則って、教育・研究活動を行っているが、情報社会の進展に伴い、大学における教育・研究活動並びにこれらを支援する事務・運営業務においては、情報通信技術への依存が高まっている。また、情報資産は、大学の重要な資産でもある。このため、名城大学情報センターは名城大学教育研究情報ネットワークシステム（メイネット）を設置し、教育・研究活動に供しているところであるが、名城大学教育研究情報ネットワークシステムの円滑な利用を促進し、本学の教育・研究の充実を図るとともに、名城大学教育研究情報ネットワークシステムを通じて本学の情報資産が被害を受けないよう対策をとり、また、名城大学教育研究情報ネットワークシステムの利用者の行為によって本学が加害者となりうる状況が発生することを防止する必要がある。そこで、名城大学情報センターは、この名城大学教育研究情報ネットワークシステムセキュリティポリシーを策定する。

情報技術は日々進展しており、革新的な変化も多い。そのため、セキュリティポリシーは多くの事項について事前に詳細で硬直化した制限を設けるのではなく、各利用者が自己の責任のもとに情報利用技術の最新の成果を利用して柔軟な行動をとることを奨励し、自由な活動の結果として問題が発生した場合に、不合理で無限定な責任追及が行われないような活動環境を整備するものでなければならない。したがって、このセキュリティポリシーは、必要に応じて随時見直し、直面する問題の解決に柔軟に対応できるよう運用されなければならない。

第 1 章 総則

目的

第 1 条

このセキュリティポリシーは、次の目的のために、名城大学情報センターが管理する名城大学教育研究情報ネットワークシステム（以下、メイネットという。）を利用し情報を扱うにあたって、遵守するべき最低限の事項を定めるものである。

(1) 不正アクセス、改竄、破壊、漏洩等からメイネットの情報資産を守り、メイネットの情報セキュリティを確保すること。

(2) 名城大学の内外を問わず情報セキュリティを侵害する行為を防止し、名城大学の社会的信頼を守ること。

(3) 情報資産の分類、および、分類に応じた管理に資すること。

(4) 情報セキュリティに関する情報の取得を支援すること。

定義

第 2 条

このセキュリティポリシーで使用する用語の定義は、次のとおりとする。

(1) メイネット 「教育研究情報ネットワークシステム（メイネット）利用内規」第 2 条に定めるものをいう。

(2) 情報処理教室等 「情報センター附属情報処理教室等の利用内規」第 1 条に定めるものをいう。

(3) 情報資産 情報および情報を管理する仕組み（情報システムならびにシステム開発、運用および保守のための資料等）の総称をいう。

(4) 情報システム ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成され、その処理を行うものをいう。

(5) 情報 情報システムで扱うデータをいう。

(6) 情報セキュリティ 情報資産の機密性（権限を有する者だけがその情報を利用することを確実にすること）、完全性（情報および処理方法が正確および完全である状態を完全防護すること）および可用性（許可された利用者のみが必要なときにアクセスできることを確実にすること）を維持することならびに定められた範囲での利用可能な状態を維持することをいう。

適用範囲

第 3 条

このセキュリティポリシーは、メイネットおよびメイネットに接続する名城大学内（天白キャンパス、八事キャンパス、ナゴヤドーム前キャンパス、農学部附属農場、日進総合グラウンドをいう。）のネットワークを対象とし、情報処理教室等に設置された情報機器、名城大学内に設置された情報コンセントまたは無線 LAN を通じてメイネットへ接続された情報機器、インターネットを経由してメイネットへ接続された情報機器（以下、対象機器等という。）に適用されるものとする。

(2)このセキュリティポリシーは、教員、事務職員、学生、委託業者その他対象機器等を管理し、または、使用するすべての者に適用されるものとする。一時的な管理または使用である場合にも適用される。

第 2 章 組織および体制

セキュリティ責任者

第 4 条

メイネットのセキュリティ責任者は、情報センター長とする。

(2)セキュリティ責任者は、メイネットの情報セキュリティに関する総括的な意思決定を行い、名城大学の内外に対して責任を負う。

(3)セキュリティ責任者は、すべての対象機器等の利用者および名城大学内の部局に対し、啓発、研修、教育を通じて、セキュリティポリシーの遵守を励行させる。

(4)セキュリティポリシーの解釈については、セキュリティ責任者がすべての権利を保有し、その解釈をもって最終決定とする。セキュリティ責任者は、情報センター運営委員会の議を経て、以前の解釈を変更することができる。

情報センター運営委員会

第 5 条

情報センター運営委員会は、セキュリティポリシーの策定および改訂、セキュリティポリシーの遵守の励行、学内の調整、学外との折衝その他メイネットの情報セキュリティに関し重要な事項について、審議しまたは決定する。

管理者

第 6 条

それぞれの情報資産ごとに管理者を設けるものとする。

(2)「情報センター附属情報処理教室外でのメイネットの利用に関するガイドライン」の定めるところにより情報処理教室外でのメイネットの利用を許可された情報機器については、その所有者を管理者とする。その管理にあたっては、このセキュリティポリシーに定めるほか、「情報センター附属情報処理教室外でのメイネットの利用に関するガイドライン」に従わなければならない。

(3)研究室等に設置された情報コンセントを通じてメイネットに接続される情報機器またはその情報機器によって構成されるネットワークについては、各研究室等において管理者（専任の教員または職員に限る。）を定め、毎年、管理者および情報機器・ネットワークに関する所定の事項をセキュリティ責任者に届け出なければならない。

第 3 章 情報資産の分類および管理

情報の分類

第 7 条

情報の内容および性質に応じて、広く学外に公開するもの、学内に限定して公開するもの、特定の利用者にのみ公開するもの、非公開とするものに分類し、その分類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。

(2)利用者は、権限のない情報に対してアクセスを行ったり利用したりしてはならない。

情報資産の管理

第 8 条

情報資産は適切に管理されなければならず、情報資産の管理者は情報の改竄、偽情報の流布、情報の漏洩の防止対策を講じなければならない。

(2)特定の利用者に限定して公開する場合には、情報の登録および閲覧は、許可された者が許可された操作だけを行えるように、認証およびアクセス制御機能を設けなければならない。さらに、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。

(3)非公開情報を扱うネットワークは、可能な限り、一般のネットワークと論理的に異なるものとしなければならず、また、暗号化や盗聴防止策を講じなければならない。

(4)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、守秘義務契約を締結しなければならない。

(5)情報の漏洩の防止等の観点から、ファイル交換ソフトの利用については、十分な注意を払わなければならない。非公開情報もしくは限定公開情報が保存された情報機器、または、非公開情報もしくは限定公開情報が保存されたネットワークに接続する情報機器には、ファイル交換ソフトをインストールしないようにするものとする。

情報機器および記憶媒体の処分

第 9 条

非公開・限定公開・公開の別を問わず、情報機器および記憶媒体を破棄する場合には、その処分方法に注意しなければならない。

情報の公開化

第 10 条

非公開情報を公開化する場合には、個人情報の漏洩、プライバシーまたは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、統計処理などの加工を行う等の措置を講じなければならない。

(2)個人情報の取り扱いにあたっては、「学校法人名城大学における個人情報保護のためのガイドライン」その他関連の規程に準拠するものとする。

情報機器のメイネット接続の許可

第 11 条

メイネットに情報機器を接続しようとする場合には、「教育研究情報ネットワークシステム（メイネット）利用内規」および「情報センター附属情報処理教室外でのメイネットの利用に関するガイドライン」の定めるところによ

り、あらかじめ、セキュリティ責任者に届け出て、その許可を得なければならない。届出事項に変更があった場合には、すみやかに、セキュリティ責任者に届け出なければならない。

(2)インターネットを経由してメイネットを利用しようとする場合には「教育研究情報ネットワークシステム（メイネット）利用内規」および「情報センター附属情報処理教室外でのメイネットの利用に関するガイドライン」の定めるところにより、利用を認められたものでなければならない。

情報の自己管理

第 12 条

利用者は、メイネットを使用して受信しまたは送信する情報については、メイネット用設備の故障による消失を防止するための措置（バックアップ等）をとるものとする。また利用者は、やむを得ない事由によりメイネット用設備が故障した場合、利用者の情報が消失することがあることをあらかじめ了承するものとする。

(2)メイネットに接続された情報機器およびその情報機器内にある情報については、その情報機器の管理者および利用者が自己の責任で管理しなければならない。

(3)利用者は、メイネットのサーバーのディスク容量に余裕がなくなるおそれがあるときは、そのディスクに蓄積されている利用者の情報を消去することがあることをあらかじめ了承するものとする。

第 4 章　物理的セキュリティ

第 13 条

情報機器の設置場所については、安全性を保ち、不正な立ち入りを阻止する対策を講じなければならない。

(2)情報資産の管理者は、情報機器について盗難防止対策を講じなければならない。

(3)移動して使用する情報機器については、紛失することのないよう対策を講じなければならない。また、紛失しても第三者がその情報機器内の情報を読み取ることができない措置を講じなければならない。

(4)情報資産の管理者は、情報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。

第 5 章　人的セキュリティ

セキュリティポリシーの遵守等

第 14 条

第 3 条第 2 項に定めるものは、このセキュリティポリシーを遵守しなければならない。学生も情報セキュリティを維持する義務を負う。

(2)対象機器等の利用者は、このセキュリティポリシーおよび関連の規程を遵守して、対象機器等を使用しなければならない。セキュリティ責任者が情報セキュリティの維持または情報システムの管理のために協力を依頼したときは、それに従わなければならない。

(3)対象機器等の利用者は、情報セキュリティに関する事故、情報システムの不審な動作、公開情報の改竄、システム上の障害および誤動作を発見した場合には、セキュリティ責任者に直ちに報告するものとする。

(4)セキュリティ責任者は、非常勤教職員および臨時職員（委託業者を含む。）に、あらかじめ、このセキュリティポリシーの内容を理解させ、遵守させるものとする。

(5)情報システムの開発および保守ならびにシステム管理業務を委託業者に発注する場合は、委託業者から下請けとして受託する業者を含めて、セキュリティポリシーの遵守を明記した契約を締結しなければならない。その契約には、責任所在の境界、ならびに、セキュリティポリシーが遵守されなかった場合の規定を定めなければならない。

教育研修等

第 15 条

セキュリティ責任者は、すべての対象機器等の利用者に対し、このセキュリティポリシーの内容その他情報セキュリティについて普及啓発しなければならない。

(2)セキュリティ責任者は、必要に応じて、教育研修を実施する。定められた者は、研修に参加し、情報セキュリティについて理解を深め、情報セキュリティ上の問題が生じないようにしなければならない。

(3)セキュリティ責任者は、情報セキュリティの維持のため、問題のある行為をした利用者に対して、メイネットの適正利用のために必要な指導を行うものとする。

(4)セキュリティ責任者は、各情報資産の管理者に対し、情報セキュリティの維持のため必要な指導を行い、または、適切な措置の勧告を行うことができる。

(5)セキュリティ責任者は、対象機器等の利用者に対し、情報セキュリティに関し重要な情報の提供を行うものとする。

パスワード等の管理

第 16 条

自己のパスワードを秘密とし、また、十分なセキュリティを維持できるよう、自己のパスワードの設定および変更に注意しなければならない。

(2)他人のアカウントを使用すること、または、他人に自己のアカウントを使用させることは、してはならない。いかなる場合も他人のパスワードを聞き出してはならない。

(3)利用資格を有する者以外に情報機器のアカウントを発行してはならない。また、利用資格を失った利用者のアカウントは、直ちに削除されなければならない。

(4)自己の管理する身分証、学生証等の認証等に使用する IC カードの貸し借りをしてはならない。

第 6 章 技術的セキュリティ

第 17 条

名城大学の情報資産を学外または学内からの不正なアクセスなどから適切に保護するため、セキュリティ責任者および情報資産の管理者は、情報資産へのアクセス制御、ネットワークの監視および管理などの必要な対策を講じなければならない。

(2)セキュリティ責任者、情報資産の管理者および対象機器等の利用者は、コンピュータウイルス対策等のセキュリティ対策を講じなければならない。

第 7 章 禁止事項

第 18 条

対象機器等の利用にあたっては、次の行為をしてはならない。

(1) 刑法その他の法令により処罰の対象とされる行為

(2) 民法その他の法令に定める損害賠償等の民事責任を発生させる行為

(3) 対象機器等の機能に障害を与え、または、他の利用者による対象機器等の利用に支障を及ぼす行為

(4) 他人のメール等の閲覧、他人の情報の盗聴または改竄、他の情報機器への攻撃または侵入、コンピュータウイルスの作成または流布等の不正な利用行為

(5) 名城大学における教育・研究に支障を及ぼす行為

(6) その他個人や社会の利益を不当に損なう行為

(2)名城大学の内外を問わず、あらゆる教育・研究機関、企業、組織、団体、個人等の情報資産を侵害してはならない。

(3)前 2 項に定めるほか、法令または条約、名城大学が加入するネットワークの規約、メイネットに関する利用内規、利用心得、ガイドラインを遵守しなければならない。

第 8 章 改訂

第 19 条

情報センター運営委員会は、少なくとも毎年１回、利用者の意見の聴取、運用実態等の把握等の方法により、このセキュリティポリシーの実効性について評価し、必要な見直し等を行って、よりセキュリティレベルの高い、かつ、遵守可能なポリシーに更新するものとする。

(2)セキュリティポリシーは、メイネットが更改されるごとに、見直されるものとする。

(3)このセキュリティポリシーの改訂は、情報センター運営委員会の議決によって行う。

附則

(1)このセキュリティポリシーは、平成 19 年 4 月 1 日から適用する。

(2)セキュリティ責任者は、このセキュリティポリシーと一体をなすものとして、対策基準、実施手順等の細則を定めるものとする。

(3)メイネット以外の名城大学内のネットワークにおいて、情報セキュリティ上の問題が発生し、その結果メイネットの円滑な運営に支障を来す場合または支障を来すおそれがある場合には、セキュリティ責任者は、そのネットワークの管理者に対して適切な措置を講じるよう指導もしくは勧告すること、または、メイネットとの接続を切断すること等メイネットの円滑な運営を維持するために必要な一切の措置を講じることができる。この場合には、重大な影響を受ける可能性がある者に対して、措置の実施後すみやかに通知するように努めるものとし、情報センター運営委員会にすみやかに報告して、その了承を得なければならない。

附則

このセキュリティポリシーは、令和４年１月 31 日に改訂し、令和３年４月１日から適用する。

附則

このセキュリティポリシーは、令和４年９月７日に改訂し、令和４年９月１４日から適用する。