星槎道都大学 情報セキュリティポリシー

改訂履歴

日 付	改訂内容
2020年2月7日	星槎道都大学情報セキュリティポリシーを制定
2020年7月22日	情報セキュリティ事務局・委員会構成員の変更
2021年5月24日	文書全体の体裁を一部変更 情報セキュリティ事務局・委員会構成員名簿を別紙化
2025年2月20日	文書全体の体裁を一部変更 5.利用者 (10)学外での利用 追記

1. 総則

⑴ 本文書の目的

本文書は、星槎グループの情報セキュリティポリシーを基本として、星槎道都大学情報セキュリティポリシー（以下「本ポリシー」という）を本学の実情に即して編集・策定したものである。

情報のデジタル化が進む中、星槎グループにおける情報セキュリティの確保は、社会的な要請が極めて高いため、情報漏洩等の事故が発生すると、星槎グループとしての信用の失墜、金銭的な補償負担、事後対応に忙殺されることに加え、星槎そのものの存在自体を危うくしかねません。

本ポリシーは、星槎グループにおける情報セキュリティを確保することを基本としつつ、星槎道都大学としての情報セキュリティポリシーを独自に策定し、安全かつ円滑に情報を取り扱える環境を整備することを目的とする。

⑵ 星槎道都大学における情報セキュリティポリシーの位置づけ

本ポリシーは、複数の学校法人等で構成された星槎グループにおける情報セキュリティポリシーに準拠しつつ、現状に即した現実的・暫定的なポリシーのあり方を経過措置としてここに提案するものである。

星槎道都大学として独自の情報セキュリティポリシーを策定あるいは改訂した内容は速やかに星槎グループ情報セキュリティ事務局に連絡するものとする。なお、星槎道都大学にはネットワークに関する下記７つの規程が既に存在するため、今後は本ポリシーとの整合性について、星槎道都大学情報セキュリティ委員会において検討していく必要がある。

- D5-2 星槎道都大学 総合情報ネットワーク管理・運用規定
- D5-3 星槎道都大学 総合情報ネットワーク（MIND）利用基準
- D5-4 星槎道都大学 総合情報ネットワーク（MIND）運用基準
- D5-5 星槎道都大学 電子メール利用要領
- D5-6 星槎道都大学 MIND 審査委員会要領
- D5-7 星槎道都大学 ホームページ管理・運用規程
- D5-8 星槎道都大学 ホームページへのリンク登録に関する要領

⑶ 星槎道都大学における情報セキュリティポリシーの概要

本ポリシーは以下の内容を含む。

- 機密情報の漏洩防止（機密性の確保）
- 情報の改ざん防止（完全性の確保）
- 情報の利用が必要な時に遅滞なく利用可能（可用性の確保）
- 情報セキュリティ確保のための体制
- 情報資産の格付け
- 情報インフラのあり方
- 教職員等の行動指針

⑷ 法令等の遵守

本ポリシーでは、法令等に示される内容は必ずしも明記していないが、法令等を遵守することを前提としている。また、通常業務で行われるような報告・相談・連絡・提案等については、本ポリシーに明示的な記載がなくとも社会人として自然に行われるべき行動である。更には、本ポリシーにおける記載の有無や字句表現だけに頼ることなく、情報の取り扱いがどうあるべきかを理解し考える力を本ポリシーに該当する領域にて発揮するよう努めるべきである。

2. 体制

⑴ 組織

星槎道都大学に、情報セキュリティ委員会（経過措置として、星槎道都大学 図書紀要及び情報委員会がこの情報セキュリティ委員会を兼ねることとする）を設置する。情報セキュリティ委員会は、自らの組織における情報セキュリティの確保を目的とする。また、自らの組織におけるインシデント対応も行うものとする。

情報セキュリティ委員会は、星槎グループ情報セキュリティ事務局からの指導、調査などに協力し、星槎グループとしての情報セキュリティ確保に努めるものとする。また、必要に応じて情報セキュリティ委員会は星槎グループ情報セキュリティ事務局に対し情報セキュリティに関し相談や提言をすることができる。

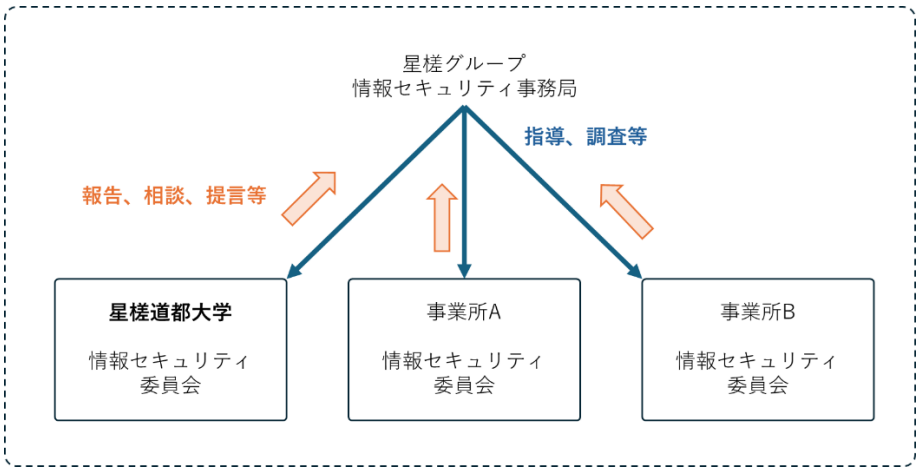

図1 情報セキュリティ体制

⑵ 星槎グループ情報セキュリティ事務局の体制

情報セキュリティ委員会に、本学情報セキュリティ統括者（以下、本学統括者）、ならびに本学情報セキュリティ責任者（以下、本学責任者）と本学情報セキュリティ担当者（以下、本学担当者）を置く。

本学統括者は、星槎道都大学における情報セキュリティ体制を統括し、本学の情報セキュリティ確保のため必要な措置を講ずるものとする。また、本学責任者との連絡を密にし、情報セキュリティの確保が円滑に行われるようにしなければならない。本学統括者は、原則として星槎道都大学長または学長補佐をあてるものとする。

本学責任者は、星槎道都大学における情報セキュリティ確保のため実務を行うものとする。本学統括者と連絡を密にし、協力して情報セキュリティ確保の維持、発展に寄与するものとする。また、本学統括者をおかない場合、本学責任者は本学統括者の役割を果たすものとする。

本学担当者は、本学責任者の指示に基づき、必要な実務を行うものとする。また、必要に応じて本学責任者に報告や提案を行い、積極的に情報セキュリティ確保に務めるものとする。

本学責任者は、本学情報セキュリティ委員会の体制について、グループ事務局に報告しなければならない。また、本学責任者は、本学統括者の承認のもと、グループ事務局に対し報告・連絡・提言等を行い、また指導等を受けるものとする。

⑶ 教育と訓練

グループ統括者と本学統括者は、互いに協力し、グループ全体の情報セキュリティ教育体制および訓練体制を構築しなければならない。また、定期的にグループ全体または星槎道都大学の各部局と協力して、教育と訓練を実施しなければならない。更に、重大なインシデントの発生が予見される場合は、当該インシデントに対応するため、速やかにグループ事務局及び星槎道都大学の各部局に対し、通知しなければならない。

本学統括者は、独自に星槎道都大学における特色のある情報セキュリティ教育および訓練を実施できるものとする。

⑷ インシデント（非常時）対応

本学責任者は、緊急性を要するインシデント発生時は、自らの判断で応急措置を講じることができるものとする。ただし、応急措置後、速やかに本学統括者に報告し承認を得なければならない。情報セキュリティインシデントとは「重要な情報を守ることができなかった結果の事象」と捉え、次のような事象を想定する。

① 重要な情報を決められた以外の人が利用した（重要な情報が漏洩した）
② 重要な情報の完全さ正確さを保護できなかった（重要な情報が改ざんされた）
③ 重要な情報が必要な時使えなかった（重要な情報が利用できなかった）

上述の事故内容や要因によって対応も変わる。

【情報セキュリティインシデント対応の実施フェーズ】

① 検知：事故現場や本学担当者等に通知され、事故の発生を検知する。
② 初期対応：問題の切り分け（情報システムの故障・攻撃、ウイルスの検知、不正アクセス等）や被害拡大の防止、犯罪行為時の証拠保全（偶発的な過失・事故であれば必要なし）などの是非を本学責任者に報告・相談し、その結果を本学統括者等に通報する。
③ 回復：状況・原因の把握が可能であり、保守委託ベンダに状況を連絡し、保守契約内容に該当すると考えられる場合は、対応を依頼する。本学の管理品による障害と判断された場合は、障害の原因がソフトウェアの問題かハードウェアの問題かを迅速に調査・点検し、本学統括者の指示を受け、本学責任者の判断のもとで、本学担当者が事故を復旧し、元の状況に戻すための対応を行う。その結果を本学統括者に報告するとともに、学内関係部局にも通知する。
④ 事後対応：事故の原因・経緯等から、今後同じようなことが起きないような対策について、検討・実施するため、本学統括者と相談の上、本学情報セキュリティ委員会を開催し、事故の原因、経過や再発防止策等について報告する。結果を星槎グループ情報セキュリティ事務局に報告する。

(ア) なお、意図的な犯行による攻撃が疑われるときは、本学統括者からの指示を受け、証拠保全を行うが、本学で証拠保全が対応できない場合は、本学責任者が保守契約ベンダに依頼し、ベンダからの調査結果を確認後、本学統括者に報告する。本学統括者は調査報告を受け、法的措置を講ずるか判断する。その内容によっては、意図的な攻撃と判断される証拠が残っているかなどを精査し、場合によっては弁護士と相談する。法的措置を講ずると決定した場合、警察に証拠とともに届け出る。

(イ) 情報システムの復旧に時間が掛かりそうな場合、次にとるべき対策を検討する。事業継続に関わる重大な問題であれば、本学統括者及び責任者から理事長・事務局長にその旨報告し、情報システム復旧のための対策を検討し、その結果を速やかに情報公開する。（外部の利用者にも現状を報告する）

⑸ 情報セキュリティポリシーの見直し

本ポリシーは、少なくとも年1回は内容の検討を行うものとする。実情にそぐわない点は見直しを行い、本ポリシーの目的が達成できる内容に更新しなければならない。

新たなインシデントの発生が予見される場合は、速やかに本ポリシーの見直しを実施しなければならない。また、予見できなかったインシデントが発生した場合も、事後速やかに本ポリシーの見直しを実施しなければならない。

⑹ 違反への対応

本学統括者は、当該本学における情報セキュリティポリシーへの違反に対し、MIND審査委員会を開催しなければならない。

⑺ 例外措置

本ポリシーを遵守することにより業務の遂行に多大な支障を生ずる場合、情報セキュリティ委員会の審議を経て本学統括者の許可を得ることで本ポリシーを遵守しなくてもよいものとする。

3.情報資産

⑴ 情報の棚卸し

本学は、所有する情報の一覧を作成する。

このとき、例えば「成績管理表」「〇〇指導履歴書」「財務管理」などの代表形とし、情報の種類がわかるようにする。「2016年成績管理簿」「2016年度 1年生成績管理一覧表」のように具体的な細目を一つ一つ列挙する必要はない。

⑵ 情報の格付け

第2ステップでは、部局ごとに第1ステップで一覧にした各情報を機密性・完全性・可用性の観点から格付けする。格付けにあたっては、表1〜3の定義を採用するものとする。

機密性3、機密性2、完全性2、可用性2に相当する情報は、その格付け区分および後述の取り扱いとともに、わかりやすく一覧表などに取りまとめ、教職員等に周知するものとするが、当面は当該部局で把握し、周知の必要性については今後の検討課題とする。

表1　機密性に関する格付け

区分	分類の基準
機密性3	秘密文書に相当する情報。また、本来知り得る者以外に漏洩した場合、人権侵害、危険の発生、多大な金銭的損害が発生するなど大きな支障を及ぼす恐れのある情報。
機密性2	秘密文書には相当しないものの、本来知り得る者以外に漏洩することで、業務の遂行に支障（※）を及ぼす恐れのある情報。※軽微なものは除く。
機密性1	公表済みの情報。公表しても差し支えの無い情報。機密性3にも機密性2にも該当しない情報。

表2　完全性に関する格付け

区分	分類の基準
完全性2	改ざん・誤謬・破損などにより、権利の侵害・危険の発生・金銭的損害が発生するなど業務の適切な遂行に影響（※）を及ぼす恐れのある情報。※軽微なものは除く。
完全性1	完全性2ではない情報。

表3　可用性に関する格付け

区分	分類の基準
可用性2	紛失・滅失・アクセス不能などにより、権利の侵害・危険の発生・金銭的損害が発生するなど業務の安定的な遂行に影響（※）を及ぼす恐れのある情報。※軽微なものは除く。
可用性1	可用性２ではない情報。

⑶ 情報の取り扱い

本学責任者は、機密性3、機密性2、完全性2、可用性2に相当する情報について、その取り扱い方法等を検討し、なるべく早い時期に本学情報セキュリティ委員会に提案することとするが、当面は当該部局が判断し、取り扱うこととする。情報のサイクル例及び機密性に関する取り扱い制限の例として、表４～７の内容を含むものとする。

表4 情報のサイクル例

情報の各局面
入手・作成・利用・保存・運搬・提供・送信・公表・バックアップ・廃棄

表5　機密性に関する取り扱い制限の例

指定方法	指定方法
複製禁止・複製要許可	閲覧禁止・閲覧要許可
配布禁止・配布要許可	対象者の制限（○○限り）
暗号化必須・平文要許可	期日の制限（○日限り）
印刷禁止・印刷要許可	期限の制限（○月○日まで）
転送禁止・転送要許可	作業時の取り次ぎ禁止
再利用禁止・再利用要許可	人数指定（複数人で作業）
送信禁止・送信要許可	数量制限（不要な複製禁止）
場所の指定（施錠できる○○に保存）	方法の指定（○○に保存、PC禁止）

表6　完全性に関する取り扱い制限の例

指定方法	指定方法
書き換え禁止・書き換え要許可	期日の指定（○日まで保存）
削除禁止・削除要許可	場所の指定（○○において保存）
保存期間終了後要廃棄	方法の指定（○○ディスクに保存）

表7　可用性に関する取り扱い制限の例

指定方法	指定方法
所要時間の指定（１日以内復旧）	場所の指定（○○において保存）
作業者指定（○○会社に連絡）	方法の指定（○○ディスクに保存）

4.情報インフラ

⑴ 管理区域

情報インフラを設置するにあたり、管理区域を表８のように定義する。

表8 管理区域（各部局の該当する部屋・施錠可能な書庫等の確認）

クラス	立ち入り	構造	取り扱い
クラス３	予め許可された者が、業務上必要な場合にのみ立ち入り可。	窓が無く、天井・壁・床下からの侵入を防ぐ構造で、ドアを施錠できること。	監視カメラや入退室管理システムを導入するなど入退室管理を厳格に行う。
クラス２	予め許可された者が、業務上必要な場合のみ立ち入り可。	ドアを施錠でき、簡単には侵入できないか、侵入を検知できる構造であること。	監視カメラや施錠管理を行う。
クラス１	教職員等のみが立ち入りができるものとする。他の者が立ち入る場合は教職員等と共に立ち入ること。	必要に応じ施錠あるいは盗難防止構造をとる。	必要に応じ施錠管理あるいは盗難防止措置をとる。
クラス０	教職員等および他の者が立ち入ることができる。	規定せず。	規定せず。

グループ責任者およびセキュリティ責任者は、管理区域を指定し必要な設備を備えるようにしなければならない。

⑵ ネットワーク設備

ネットワーク設備は、ネットワーク担当部署またはネットワーク専任の機関の者が設置するものとし、それ以外の者が設置する場合は、必ずネットワーク責任者または担当者の許可を得ること。

ネットワーク設備として表9のような物を対象とし、適切な管理区域に備え付けること。本学責任者は、ネットワーク図の作成状況や管理状態を確認できるものとし、情報セキュリティの確保に必要な指導を行うものとする。

表9 ネットワーク設備例と設置場所

カテゴリ	設備例	設置場所
インターネットアクセス	光ファイバ等の回線、ONU等の終端装置、ルータ	管理区域クラス2またはクラス3
基幹LAN	ネットワークスイッチ、ファイアウォール、UTM	管理区域クラス2またはクラス3
末端（各部屋）内LAN	ネットワークスイッチ（HUB）、Wi-Fiアクセスポイント	管理区域クラス1またはクラス0

(3) サーバ

サーバは、原則として本学統括者の承認を得た上で、サーバ設置部署がサーバの構築あるいは設置できるものとし、それ以外の者が構築したり設置したりする際には、ネットワークへの影響を点検した上で、設置に関する申請手続きを経た上で、情報セキュリティ委員会の承認を得る必要がある。

本学責任者は、サーバの設置部署と協力し、情報セキュリティ確保の観点からサーバの仕様を決定し、設置する部局ごとに必要な規程類を整備しなければならない。

サーバとして表10のような物を対象とし、適切な管理区域に設置すること。データセンターについては、約款やカタログ等で管理区域クラス2またはクラス3相当であることを確認しなければならない。

表10 サーバ例と設置場所（DNSサーバは(6)で規定する）

カテゴリ	設備例	設置場所
基盤サーバ	DHCP、RADIUS、LDAP	データセンター、あるいは管理区域クラス2またはクラス3
アプリサーバ	Web、メール、ファイル、グループウェア、データ処理	データセンター、あるいは管理区域クラス2またはクラス3

⑷ 特定用途機器

特定用途機器にはネット会議システム、ネットワーク接続型の複合機・プリンタ・コピー機・スキャナ・FAX・表示装置・ネットワークカメラ・ネットワーク音響装置などがある。購入部署は、本学責任者に相談し、特定用途機器の使用目的に合わせて、適切な管理区域を指定し、設置しなければならない。

特定用途機器をネットワークに接続する場合は、購入部署はネットワーク管理担当部署の接続許可を購入手続きの前に得なければならない。すでに設置済みの私物で持ちこみ利用申請済みの情報機器で個人情報の取り扱う際は、クラウド上にデータを保存し、ローカルディスクに保存することは禁止する。ただし、授業や入試広報活動等でプレゼンテーション等の限定的な利用の際は個人情報及び著作権等の取り扱いに十分注意した上での利用は認めることとする。機器の購入部署は、特定用途機器の担当者を決め、特定用途機器の管理を十分に行える体制をとらなくてはならない。

本学責任者は、必要に応じて特定用途機器の状態を調査・確認などを行うことができるものとする。また、情報セキュリティに関する懸念や事故がある場合、当該機器のネットワーク接続や使用を禁止できるものとする。

⑸ インターネット上のサービス

インターネット上に存在するサービス（例：Zoom・生成AIサービスなど）の利用にあたって事前に許可を得る必要はないが、利用するサービスの特性を十分に理解した上で個人情報や機密情報の取扱いに十分注意し利用しなければならない。

また、本学責任者は、利用禁止サービスに関して事前に通知しなければならない。

⑹ アカウントの管理

メール・グループウェア・ファイル共有等の利用にあたり、利用者にアカウントを発行する。アカウントの管理（発行・変更・削除一覧）は、それぞれのシステムごとに管理担当者を置き、管理担当者が実施する。管理職はアカウント管理の実態を十分把握しなくてはならない。

メーリングリスト(ML)の管理もアカウントの管理に準ずるものとする。

グループ責任者及び本学責任者は、アカウントの管理状況を確認・指導できるものとし、アカウント管理担当者ならびにその管理職は、調査に協力し指示に従わなければならない。

原則として、アカウントは利用者個人に対して発行するものとする。もし、共同利用するアカウントを発行する場合でも、その必要性を十分吟味し、インシデント発生時の責任の所在が不明とならないよう措置しなくてはならない。

アカウントは、業務上の必要性のある場合のみ発行するものとする。異動や退職などで不在となった利用者のアカウントは速やかに無効化あるいは消去しなくてはならない。

5.利用者

⑴ パソコン

利用者は業務で使うパソコンについて、下記事項を遵守しなければならない。

①OSは、最新の種類とバージョンを利用する。
②インストールならびに利用してよいソフトウェアを指定する。また必要に応じ、利用してはいけないソフトウェアを列挙する。指定外ソフトウェアを利用している場合は、そのソフトウェア名と利用目的を本学担当者に報告する。
③OSとアプリケーションソフトウェアの更新は適宜行うようにすること。特にOSは自動更新できるように設定すること。
④「Windows Update」の更新を義務づける。本学担当者は、定期的に利用状況を調査し、台数確認・利用場所・氏名・バージョン情報・更新状況の確認をして本学責任者に報告する。
⑤パソコンを起動し利用するにあたり、パスワードの入力が必要となるよう設定しなければならない。
⑥パソコンを起動し、利用可能な状態のまま離席する等、パソコンを放置してはならない。離席等の場合は、操作ができない状態とし作業再開にはパスワード入力が必要となるよう設定しなければならない。
⑦パソコンのパスワードを他者に見える状態にしてはならない。
⑧パソコン内の情報は、同一部署などの関係者が共有できるよう措置すること。（管理職がパソコンのパスワードを管理する・ファイルは共有フォルダに保存する等）
⑨パソコンを廃棄する際は、内蔵ストレージ内を完全に消去すること。
⑩前任者から後任者にパソコンを引き継ぐ場合は、パソコンをクリーンインストールし安定的に動作させるように措置すること。
⑪機密性2、機密性3、完全性2および可用性2の情報は、パソコン内に保存しないこと。

⑵ タブレットおよびスマートフォン

利用者は業務で使うタブレット及びスマートフォンについて、(1)パソコンと同等の内容を遵守しなければならない。

⑶ 私物デバイスの利用

利用者は業務で使う私物のデバイス（パソコン・タブレット・スマートフォンなど）について、下記の事項を遵守しなければならない。

①現状は、私物デバイスの利用を認める。ただし、利用は許可制とし、業務資料等をPC本体には保存せず、クラウド上に保存し、②以降の条件を満たす必要がある。
②私物利用が業務上、真に必要であること。
③私物デバイスは、前項「(1)パソコン」の要件を満たすこと。このとき必要な費用は利用者が負担すること。
④私物デバイスは許可された本人だけが利用するものとし、家族等が利用できないよう措置されていなければならない。
⑤業務上の必要性に応じ、利用者は、業務に関係するメールやファイル類を管理職あるいは同僚が閲覧できるようにすること。
⑥管理職は、業務に関係するメールやファイルの編集や削除ができるものとし、利用者はこれに協力しなくてはならない。
⑦業務上あるいは情報セキュリティ上の必要性に応じ、管理職・グループ責任者ならびに本学責任者は、許可したデバイスの利用を終了させることができる。

⑷ デバイスの持ち出し

本学責任者は、利用者がデバイス（パソコン・タブレット・スマートフォンなど）を本学から持ち出すことに関し、下記のような持ち出しに関する基準を設定して、遵守するように指導しなければならない。持ち出しを行う部局では、以下の内容を含め情報漏洩等を防ぐ上で必要な措置を講ずるものとする。

①持ち出しは事前の許可制とする。
②持ち出しは業務上の必要性があること。
③機密性2および機密性3の情報を持ち出し機器に保存しないこと。（情報資産の取り扱いの規程に準じる）
④持ち出しの際は目的地を明らかとし、申告地以外への立ち寄りは禁止とする。
⑤持ち出したデバイスは、常に身近に置き盗難防止措置を講ずること。

⑸ デバイスの持ち込み

本学責任者は、同業者・共同研究者および事業者等がデバイス（パソコン・タブレット・スマートフォンなど）を本学内に持ち込む場合は、以下のことについて十分注意した上で利用するように指導を行うものとする。

①本学のネットワークを利用する場合は、事前の使用許可を必要とする。
②本学にとっての業務上の必要性があること。
③必要に応じ、グループ責任者ならびに本学責任者は、持ち込みデバイスにおけるウイルス対策状況等を確認できるものとし、不備があれば本学内での利用を禁止できる。
④持ち込みデバイスの管理は持ち込み者が行い、いかなる理由であっても持ち込みデバイスの損傷やファイル消失等の不具合に、本学は責任を負わない。

⑹ 外部記憶装置

本学責任者は、外部記憶装置の利用に関して、以下の事項について十分注意した上で利用するように指導を行うものとする。

①業務上必要となる場合、外部記憶装置を利用できるものとする。
②私物の利用については、本学責任者の了承を得た上で認めることとする。
③利用して良い外部記憶装置を指定すること（不必要に種類を増やさないこと）。
④全数、個体管理できる体制を整え、紛失対策を講じること。
⑤常時利用しない場合は、常に中身を完全消去した状態で保管すること。
⑥保管場所はクラス２またはクラス３の管理区域を指定すること。
⑦持ち出しや持ち込みは、デバイスのそれらと同等の基準を設けること。
⑧持ち込み物を本学のパソコン等に接続することは原則禁止とする。ただし、業務上の必要性がある場合は、予めウイルススキャンを行い、無害であることを確認すること。
⑨廃棄の際は、中身を完全に消去すること。

⑺ アカウントの利用

利用者は、メールやグループウェア等で業務用のアカウントの発行を受けた時は、利用に先立ち初期パスワードを変更しなければならない。

利用者は、アカウント情報を他の者に知らせてはならない。

利用者は、アカウントを利用するにあたり原則として、不特定の者が利用するパソコン等の端末にてアカウントを使用してはならない。授業等で止むを得ず利用する際は、ユーザー設定の管理を利用する教職員が行い、パスワードの設定・変更などの確認を定期的に実施する。

利用者は、アカウントを利用するにあたり、安全が確認できないネットワーク（設置者が不明なWi-Fi等）を利用してはならない。

利用者は、アカウントを利用するにあたり、使用するパソコン等が、「(1) パソコン」あるいは「(2) タブレットおよびスマートフォン」に準じた状態のものを使用しなくてはならない。

管理職および本学責任者は、アカウントの利用状態を確認し必要な指導をすることができるものとし、利用者は調査や指導に従わなくてはならない。

管理職は、利用者によるアカウントの利用内容（ファイル共有であれば、閲覧等ができるファイルの名称やその中身）を確認することができるものとする。このとき、利用者は管理職に協力しなくてはならない。

原則として、私的なアカウントを業務に使用してはならない。

⑻ パスワードの管理

何人も、利用者からアカウント用パスワードを聞き出すなどして、パスワードを知ろうとしてはならない。

利用者は、アカウント用パスワードとして十分強度の高いものを採用しなければならない。

利用者は、パスワードの強度を高めるため、パスワードの文字列を決める際には、以下の対応を取らねばならない。

①文字列の長さは、最低8文字以上とすること。
②アルファベット大文字・小文字・数字を混ぜること。
③可能な限り、記号を含めること。
④英単語やその組み合わせは利用しないこと（辞書攻撃対応のため）。
⑤自分の誕生日・家族・趣味・思想・業務内容等、自分の属性に密接に関連しかつ他人が予想する可能性の高い情報をパスワードとして用いないこと。

⑼ メールの利用

利用者は、業務用のメールアカウントの発行を受けたときは、そのメールアカウントを「(7) アカウントの利用」並びに「(8) パスワードの管理」に準じて取り扱わねばならない。メールアカウントは、業務のみに利用するものとする。

管理職は、利用者のメールのやり取りにてインシデントが起きた際、閲覧を求めることができるものとする。利用者は管理職の求めに応じて調査に協力する。

グループ責任者ならびに本学責任者は、情報セキュリティ確保の必要性がある場合、利用者のメールのやり取りを確認することができるものとする。

利用者は、複数の相手にメールを送信する場合、原則としてBcc欄にメールアドレスを記載するものとし、Cc欄やTo欄に記載しないものとする。ただし、星槎グループ教職員等や本学教職員等だけに送信する場合や、通常の取引相手のようにお互いのメールアドレスを知り得たとしても差し支えの無い場合については、この限りではない。

利用者は、情報漏洩の起点としてメールが原因となることが多いことを認識しなければならない。

利用者は、メールで機密性2または機密性3の情報を送信してはならないものとする。

利用者は、受信したメールに表示される送信相手は、詐称されている可能性があることを常に意識し、送信相手は偽者である可能性を排除してはならない。

利用者は、受信したメールの内容が本物であるとは限らないことを意識し、曖昧な表現や通常と異なる点に敏感に対応しなければならない。

利用者は、受信したメール内のリンクを安易にクリックしてはならない。学内関係者からのメールであっても危険なWebサイトへの誘導の可能性を排除せず、メール内容に不審な点がないかよく考察しなければならない。

利用者は、受信したメール内の添付ファイルを安易に開いてはいけない。ウイルスが添付されている可能性を排除せず、メール内容に不審な点がないかよく考察しなければならない。利用者は、受信したメールに不審な点があった場合は、本学担当者に速やかに所定のルートで連絡し、指示に従わなければならない。

グループ責任者ならびに本学責任者は、受信したメールの取り扱いについて連絡体制などを整備し、不審なメールへの対応策を講じなくてはならない。

利用者は、メールの送信相手に不審感を抱かせないように対応しなければならない。例えば、私的なメールアドレスではなく業務用のメールアドレスを用いる・メール本文に曖昧な表現を用いない・むやみにリンクや添付ファイルを添えない・本人であることの傍証となるような表現（過去の経緯 等）を本文に盛り込む、など必要な措置を行うものとする。これを習慣化することで、受信メールにおける微妙な変化にも機敏に対応できる可能性が高まる。

⑽学外での利用

出張先や自宅等にて業務を行う際は、以下の項目を遵守しなければならない。

① 学外で業務データを取り扱う場合は、事前に所属長からの業務指示を得ること。個人の判断にて業務データを取り扱うことは禁止する。
② 業務データを取り扱う前に、デバイス全体のウイルススキャンを実行すること。また、学外での利用後に学内のネットワークに接続する場合も、接続前にデバイス全体のウイルススキャンを実行すること。特に各事務室のネットワークに接続する際は、より詳細な検査を実行すること。
③ デバイスのOSバージョンを常に最新の状態に更新した上で利用すること。
④ インターネット接続時は、信頼できるネットワークに接続して利用すること。不特定多数の利用者が接続できる公共施設や商業施設のフリーWi-Fi等は、絶対に利用しないこと。
⑤ 基本的に業務データは全てクラウド上に保存し、デバイス上に保存しないこと。やむを得ずデータをダウンロードする場合は、利用後にデバイス上から必ず削除すること。
⑥ デバイスのログインパスワードをより強固な文字列に設定すること。推測されやすいパスワードを避け、可能な限り多要素認証等を用いて、盗難や紛失等に備えた対策を心掛ける。
⑦ デバイスは常に肌身離さず所持し、携帯したまま不用意な場所へ立ち寄らないこと。
⑧ 個人情報を取り扱う業務など機密性の高い業務は、学外で行わないこと。学外での取り扱いを許可する業務は事前に所属長と協議し、トラブル時の情報漏洩リスクを最小限に抑えること。
⑨ 大学に関する業務データ全般について、情報漏洩の可能性がある場合は、すぐに所属長へ報告を行い、指示を仰ぐこと。

以 上