理事長・学長決定

第 17 章：情報技術とセキュリティー

17.1　基本方針

本基本方針は、OIST における情報技術資源（以下「IT リソース」という。）が、本学のミッションを果たすため、また法令遵守、契約の義務と職務にしたがい、効果的、効率的、慎重かつ責任ある方法により提供、使用される体制を確立するための事項を定めます。全てのユーザーは、これらの基本方針・ルール・手続き及びこれを違反することによる影響について、熟知しておくことが期待されます。

本学の情報資産は本学の全ての情報を包括するものとします。本学は、情報資産を所有し、管理します。情報資産を適切に取り扱うことは OIST 及び OIST コミュニティーの保護にとって不可欠であり、全てのユーザーは、情報資産を適切に取り扱う責任を有します。

本学は IT リソースのセキュリティを保護するために合理的なセキュリティ対策を講じますが、それによって本学が絶対的なセキュリティ及びプライバシーを保証するものではありません。本学は、電子メールを含むあらゆる IT リソースの使用状況を制限なく監視する権利を有します。本学は、その IT リソースのセキュリティと整合性を確保するために必要なあらゆる措置をとる責任を有します。

日常のシステム管理業務やインシデントの報告により、規程や日本の法令に対する違反が認められた場合、本学は、必要又は指示された調査と情報資産を保護する処置を実施するとともに、調査に関する情報を提供します。
本学は、アーカイブ及びレポート用のために情報資産を保持する義務を有します。加えて、学長又は統括弁護士の指示と最高情報責任者（CIO）又は最高情報セキュリティ責任者（CISO）の同意のもと、訴訟やその他の法的目的のために情報資産を一定期間保管することがあります。

本学の IT リソースは、本学のミッションと関係のない個人的又は私的な目的のために使用されてはなりません。ただし、付随的な個人的使用は、それによって職員の本学に対する業務責任及びその他義務が阻害されず、また本学に直接的な追加費用の負担を生じさせない限りにおいて認められるものとします。ユーザーは個人的なコミュニケーションの内容に責任があります。本学は本学のポリシーや日本の法令

に準拠していない IT リソースの不正使用について一切の責務と法的責任を負いません。すべてのコミュニケーションは、OIST 電子メール及びオンラインコミュニケーション実施規範に準拠する必要があります。

17.2 留意すべき事項

17.2.1 適用範囲

本章のポリシー、ルール、手続きは、全てのユーザーに適用されます。とりわけ、全てのユーザーは、「ユーザーの権限と責任」及び「OIST IT リソース利用規約」が定める要件に準拠することが求められます。

本学の情報資産へのアクセスや、その保管、送信については、その全てが本規程の対象となります。個人のデバイス、大学が全体又は一部を所有するデバイス、外部組織などが管理するデバイスもその対象となります。

17.2.2 情報資産のオーナーシップ

本学は、全ての情報資産を所有し管理します。本学は、情報資産管理責任者と情報資産管理担当者に対して、情報資産の管理と保護、ポリシーと法令を遵守する責任を課します。

研究ユニットにおいては、教員が情報資産管理責任者となり、情報資産管理担当者の役割をユニットメンバー割り当てます。教員は、追加のセキュリティ又は情報資産の保護を必要とする既存の契約を考慮し、未発表の研究データの適切な管理とセキュリティスキームを確保しなければなりません。全ての研究データの 1 次コピーは、常に OIST 管理リポジトリに保存する必要があることに留意してください。

事務部門においては、副学長が情報資産管理責任者として任命され、ディビジョンのメンバーに情報資産管理担当者の役割を委任することができます。

法人文書及び個人情報は、情報資産のサブセットですが、その取り扱いには公文書の管理に関する法律、独立行政法人等の保有する個人情報の保護に関する法律等の追加の法的及びポリシー要件があります。これらの要件と別個の管理及び管理責任の詳細は、PRP 第 12 章に記載されています。

本学の知的財産権、本学の契約書、その他の契約上の要求事項は、PRP 第 4 章及び PRP 第 14 章に記載されています。

17.2.3 情報技術管理の原則

本学の IT リソースは、可能な限り IT 運用に関する世界標準のベスト・プラクティスに沿って提供されます。そのために ITSM フレームワークを用いて IT サービス

を体系的に定義しています。

ITSM フレームワークにはサービス品質保証（以下「SLA」という。）の概念があり、IT ディビジョンと本学における IT サービスに対する範囲、適時性と品質に対する要件を明確化します。

この SLA は、IT 戦略委員会を通じて、CIO が必要と認める利害関係者での審議の上、承認されなければなりません。

17.2.4 情報セキュリティの原則

情報セキュリティは情報資産を不正なアクセスやそれによる損害から保護し、全ての適用される法令、規制及びコンプライアンス要件を遵守することを目的とします。

17.2.5 さらなる規程と手順

本学の研究ユニット、ディビジョンやセクションは各部署の管理下にある IT リソースや設備の利用における追加的な規程を課すことがありますが、それらの追加的な規程は、この全学的な方針と整合していなければなりません。また詳細な事項、ガイドラインや高度な制限が定められることがあっても、それらは制限を緩和するものであってはなりません。

17.2.6 コミュニケーションと広報

本学における電子メール、ウェブサイト、ソーシャルメディアには、副学長（広報担当）によって策定された標準及び規則が適用され、それらを遵守しなければなりません。

17.2.7 学生

学生は、本章の記載事項を熟知するとともに、研究科ハンドブックを参照してください。

17.2.8 常識に則した行動

ここに詳細に記載されている IT リソースの利用に関わるポリシーと手続きに記述されていること以外にも、全てのユーザーは健全に状況を判断し、方針又は手続きがはっきりしない場合は IT ディビジョンや関連当事者の判断を仰ぐことが求められます。

17.2.9 コンプライアンス

本学は情報セキュリティの違反及び IT リソースの悪用を深刻な問題として捉えます。違反をすると解雇を含む懲戒処分の対象となることや法的措置を講ずることがあります。

17.3 ルール

17.3.1 認証とアクセス

IT リソースへのアクセス及びその利用は、適切に申請、承認、登録、監査されなければならなりません。非公開の情報格付けの情報資産又は IT リソースにアクセスを許可された個人や主体をユーザーと定義します。

ユーザーは、ログイン情報、パスワード、その他のアクセス資格情報を常に安全に管理し、アカウント情報を保護する責任を有します。
アカウント情報やパスワードは本人のみが知り得て利用することができ、他者と共有することは禁止されています。

IT リソースを使用するにあたり、ユーザーは該当する全ての本学のポリシー、原則、手順と関連法規を遵守しなければなりません。またユーザーは OIST IT リソース利用規約を熟読したうえで、署名又はデジタル署名によりこれを理解したことを承認しなければなりません。

17.3.1.1 アカウントの作成

アカウントは以下のプロセスで作成されます。

- ユーザーが利用者の分類ごとの入校手続きを通じて OIST ID 管理システムに登録されること。
- OIST IT リソース利用規約を理解したうえで署名（又はデジタル署名）すること。
- 規定以上のアクセス権限が必要な場合、上長による事前の承認があること。
- 個別に管理されている OIST 情報資産にアクセスする場合は、情報資産管理責任者又は情報資産管理担当者の承認があること。

17.3.1.2 アカウントの延長

アカウントの延長は利用者の分類ごとの手続きを通じて、正当な理由をもって申請されなければなりません。アカウントの延長プロセスは上長と、必要に応じてそのほかの承認者による承認を必須とします。

17.3.1.3 アカウントの有効期限、無効化、削除

上記のアカウントの延長をしない限り、アカウントは大学でのユーザーの任期の満了時に自動的に無効になります。
システム管理者は、無効なアカウントを発見したときや、CIO、CISO 又は統括弁護士による指示を受けた際は、速やかにそのアカウントを無効化し、その作業内容を CISO に報告します。

17.3.1.4 アクセス権限

ユーザーの職務や責任の変更に伴い、上長は IT ディビジョンや関連する情報資産管理責任者に必要なアクセス権限に更新するよう依頼する責任を有します。情報資産管理責任者は、アクセス権を適切に更新する責任を有します。

17.3.1.5 特権アカウント/システム管理者

管理者権限を有する特権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しなければなりません。なお、特権アカウントのシステムへのアクセスは常時記録され、セキュリティ監視の対象となります。

17.3.1.6 共用アカウント

ユーザーによる共用アカウントの利用は原則禁止です。例外的に CIO 又は CISO の同意を得たうえで、システム管理者の裁量で共用アカウントを利用することができます。

17.3.1.7 無許可のアクセス

システム管理者を含む全てのユーザーは、無許可のアクセス行為が疑われる事例を発見した場合には、速やかに CISO に報告しなければなりません。

17.3.2 個人のデバイスの利用（BYOD）

本学において、本学の業務を遂行するにあたり個人的なリソースを使用する必要性はありません。

事務部門においては、IT ディビジョンが許可した場合に限り OIST の業務遂行に個人の IT 資産の利用が認められます。

研究ユニットにおいては、教員は BYOD デバイスの利用を許可することができ、それによりユーザーは個人の資源を利用すること選択することができますが、ユーザーはそれを強制されることはありません。本学は BYOD デバイスの故障にいかなる責務と法的責任を負いません。教員とその IT 資源の所有者は、個人の機器を利用したことに起因するあらゆる結果責任を有するものとします。

個人の機器を OIST ネットワークに接続する場合や、個人の機器に大学の情報を保存又は送受信する場合は、本章を遵守し、また OIST の全ての要件に準拠する必要があります。

BYOD デバイスにおいては、格納できる OIST 情報資産はさまざまなものがあります。ユーザーは、OIST 情報資産及びそれにアクセスするデバイス並びにそのアクセス方法が、OIST 情報資産の格付け及びデバイスの適格性の基準に準拠していることに留意する必要があります。

17.3.3 OIST ネットワークへの接続

OIST ネットワークは必要不可欠な研究リソースであり、その可用性とセキュリティを維持することは大学の運営において不可欠であり、また、全てのユーザーの責任です。

OIST ネットワークに接続する全ての IT 資産は、OIST ネットワークに接続する際に認証され、ネットワークに接続するシステム上のユーザーが一意に識別されなければなりません。ユーザーは、許可された OIST IT 資産を自らの業務遂行のためにのみ OIST ネットワークに接続して使用することができます。

他のユーザー又は第三者に、自身のネットワーク認証を使わせることは固く禁止されています。

ネットワーク認証が研究や OIST における業務の障壁となる場合、ユーザーは例外的な取扱を求めるため IT ディビジョンに連絡しなければなりません。ネットワーク認証を回避又は無効化する任意のデバイスに接続すること、又は他のデバイスをそのようなことができるようにすることは、固く禁止されています。

OIST ネットワークのセキュリティと安定性を確保するために、IT ディビジョンの許可を得ずに、スイッチ、ルータ、ハブなどのネットワーク機器をネットワークに接続することは固く禁止されています。IT ディビジョンに事前の許可を得ずに、OIST 施設内にて OIST が提供していない無線 LAN を使用することは禁止されています。無許可のデバイスが OIST ネットワークに接続されていたり、OIST 敷地内で無許可の無線 LAN の電波が発せられていることが検知された場合、予告なしに切断されることがあります。

17.3.4 調達、外部委託、IT 資産

OIST IT 資産の購入は目的に合ったものでなければなりません。また、それらは適切に調達、監査、再利用、処分がなされなければなりません。IT 資産の購入には、本学の調達に関する基本方針・ルール・手続きに加えて、本章が適用されます。

調達経路や予算にかかわらず、本学が調達した、寄付された、又は受領した IT 資産は、納品された時点で、OIST IT スタッフによって物理的に検査されなければなりません。この検査には、資産の効率的な追跡と監査を可能にするために行われる消せない資産マーキング（ただし CIO によって承認されたものを除く）、OIST 構成管理データベース（CMDB）への登録が含まれます。

IT 資産が、例えば顕微鏡に付属する制御 PC といった大規模な研究装置又は器具に不可欠な部分となっているものについては、資産マーキングや OIST 構成管理デー

タベースへの登録が免除されることがあります。そのような場合には、当該資産の保有者は OIST IT と協議することになります。

OIST IT の設備（サーバールーム、ネットワークスペースなど）に収容する予定の IT 資産は、その購入前に、OIST IT と協議する必要があります。［Link：17.3.30］

17.3.4.1 事務部門における IT 資産の調達

コアファシリティ及び事務部門は、OIST IT を通じて IT 資産を調達又はアップグレード（1 万円以上のソフトウェアの調達を含む）する必要があります。

これは、IT 資産を標準化し効率的に購入するためです。事務部門の IT 資産の購入又はアップグレードのリクエスト手順は、17.5.1 で詳述します。

事務部門における全ての IT 資産は OIST IT の管理下にあり、購入の経緯や購入のために使用された予算にかかわらず、本章の対象となります。

17.3.4.2 研究ユニットにおける IT 資産の調達

研究ユニットにおいては、IT 資産を購入する前に、OIST IT に相談することを強く推奨します。研究ユニットが相談せずに購入した場合、OIST IT が当該 IT 資産に対してサポートできる範囲が限定される可能性があります。また、その場合、OIST ネットワークへの接続は保証されません。それぞれのデバイスごとのサポートレベルは、SLA に詳述されています。研究ユニットにおける IT 資産の調達プロセスは、17.5.3 に記載されています。

大規模な研究装置の一部として調達されるもの又は研究装置に付属する IT 資産は、信頼性と性能を考慮して選定する必要があります。

これらの資産の信頼性は、重要な研究機器の生産性に大きな影響を与えます。これらの購入にかかる選定に関するガイドラインは、研究ユニットにおける IT 資産の調達プロセスに記載されています。

17.3.4.3 コーポレートカードによる IT 資産の調達

コーポレートカード（P-Card）での IT 資産の購入は制限されています。26.3.7 を参照してください。オンラインベンダーからの IT 資産の購入は、OIST IT を通じてのみ行うことができます。

17.3.4.4 IT 資産のトラッキング

本学が全て又は部分的に所有している IT 資産には、OIST 資産管理エージェントをインストールする必要があります。このエージェントは、IT 資産の動的監査を可能にし、年次の資産実査にかかる経費や作業工数を大幅に削減します。これは

事務部門の全ての IT 資産に義務化されており、研究ユニット内の IT 資産については強く推奨されています。

17.3.4.5 IT 資産の移管

あらゆる IT 機器の使用者又は所有者の移管は、ユーザーの変更、セクションの変更又は研究ユニットの変更を含み、OIST IT を通じて行われる必要があります。これにより、資産の登録情報と CMDB の内容が最新の状態に保たれ、また、セキュリティや個人情報保護の違反を防ぐため、移管前にデバイス上のデータは安全に消去されます。ユーザー又はセクションとユニットとの間で IT 資産を移管するプロセスについては、17.5.5 を参照してください。

17.3.4.6 OIST 敷地外での IT 資産の利用

出張や自宅での作業などの目的により、IT 資産を OIST の敷地外に持ち出す場合は、事前に IT ディビジョンから許可を得る必要があります。ラップトップ及びモバイルデバイスの場合、この許可はデバイスの配付時にユーザーが署名した利用承諾書に組み込まれています。

17.3.4.7 IT 資産の廃棄

全ての OIST IT 資産は、購入の経緯やその予算元、OIST がその一部又は全部を所有しているかにかかわらず、IT ディビジョンを通じて廃棄されなければなりません。

17.3.4.8 IT 資産の盗難、紛失又は破損

ユーザーは IT 資産の盗難、紛失又は破損について IT ヘルプデスクに速やかに報告しなければなりません。［Link：26.3.3］

17.3.5 エンタープライズアプリケーション

エンタープライズアプリケーションは、大学の業務を運営する上で重要なアドミニストレーションシステムであると定義されます。これらシステムの機能と品質は、大学の業務の生産性に大きな影響を与える可能性があります。このようなシステムの設計と実装は、IT ディビジョンに相談しながら、17.5.7 で詳細を記載する必要なプロセスを経て、相当な注意を払って行われなければなりません。

17.3.6 IT サービスの外部委託

OIST 情報資産を保持、送受信するサービス又はシステムを提供する外部の者と契約を締結する場合は、さらに以下に示す要因を考慮する必要があります。

これらは、第 28 章で詳細を定める調達のプロセス及びエンタープライズアプリケーションによる評価プロセスでの優先事項です。

- サービスプロバイダとの間のサービスレベル契約（SLA）
- 秘密保持契約及び OIST 情報資産の目的以外の利用を防止する条項
- サービスプロバイダの情報セキュリティ管理に関する成熟度
- OIST 情報資産に関し、下請け業者を含む第三者による意図しない変更からそれを保護するためのサービスプロバイダの内部統制及びそのインフラストラクチャ
- サービスプロバイダの契約上の要件及びセキュリティ要件の遵守に対する監査権
- 情報セキュリティパフォーマンスに関する監視と、OIST への定期的な報告

17.3.7 外部委託と情報セキュリティ

システム又はサービスの運用・保守を外部委託する場合、システム所有者は、OIST の情報セキュリティ要件に従って監督するとともに、CISO にあらゆる瑕疵を報告する責任を有します。

システムの情報セキュリティ事故又は誤用があった場合、システム所有者又は CISO は、外部委託したサービスを中断することがあります。システム所有者は CISO にサービス停止のための手順及び承認の権限を提供します。

システム所有者は、契約の期間中に外部委託先に引き渡される全ての情報資産が、契約終了時又は終了前の適切な時点で正当に回収又は破棄するよう徹底しなければなりません。

個人情報の取り扱いを含むシステム又はサービスの運用・保守を外部委託する場合は、OIST 個人情報保護ガイドラインに規定される事項を遵守しなければなりません。

17.3.8 ソフトウェアとライセンス

IT ディビジョンは、OIST ユーザーに幅広いリサーチ及び業務ソフトウェアを提供しています。ユーザーはこれらのソフトウェアを使用することを推奨されますが、著作権法及びライセンス規約を常に遵守しなければなりません。

IT ディビジョンが保有するソフトウェアは、一般的に大学がその全てを所有している IT 資産にのみインストールすることが許可されることに留意し、ユーザーは IT ディビジョンにソフトウェアをインストールできる IT 資産であるか事前に確認せずに、IT 資産にソフトウェアをインストールしてはなりません。利用可能なソフトウェア及びライセンス制限の詳細は、ソフトウェアカタログに記載されています。

事務部門は、ソフトウェアカタログ以外のソフトウェアを使用することは許可さ

れていません。追加のソフトウェアが必要な場合は、ソフトウェアカタログへの追加を求めるため IT ディビジョンに連絡しなければなりません。
研究部門は、ソフトウェアカタログ以外のソフトウェアの使用を許可されていますが、セキュリティを考慮する必要があります。ソフトウェアカタログ以外のソフトウェアを使用する場合、ユーザーは以下の管理を徹底する必要があります：

- 公式のウェブサイトなど、信用のある場所からソフトウェアをダウンロードすること
- セキュリティパッチを適用すること

17.3.8.1 ライセンス契約又は商用ソフトウェア

IT ディビジョンは、事務部門の全ての商用ソフトウェア又はライセンス契約と、多くの研究用ソフトウェアを管理しています。

研究ユニットは、追加のソフトウェアを購入する前に IT ディビジョンに連絡することを強く推奨されています。ソフトウェアカタログに掲載されていないソフトウェア製品を継続的に利用する必要がある場合、IT ディビジョンは大学に有利なライセンス契約を調査します。

17.3.8.2 オープンソースソフトウェアとフリーウェア

研究ユニットは、オープンソースソフトウェアとフリーウェアの使用が認められていますが、IT ディビジョンにも相談してください。ソフトウェアを継続的に利用したい場合、IT ディビジョンはソフトウェアをパッケージ化し、アップデートを管理し、セキュリティの警告と問題を監視します。

17.3.9 情報資産の格付け

情報資産管理責任者は、情報の価値、機密性、完全性、可用性に基づいて以下の 4 つのいずれかの区分に情報資産を格付けするものとします。異なる格付けの情報資産がグループ化されている場合、その中の最も高い格付けに分類されます。

情報資産の取り扱い方法については17.8.9 情報の格付けとデバイスで詳述します。

17.3.9.1 公開

「公開（Public）」と格付けされた情報資産とは、公の記録である性質のもの、あるいは一般的に公開しても差し支えないと考えられるもの又は OIST の事業、評判、人事に好意的又は中立的であるもののいずれかを指します。

17.3.9.2 学内

「学内（Internal）」と格付けされる情報資産とは、開示することが適切でなく、OIST の事業、評判又は人事に多少の悪影響をもたらす可能性があるものをいいます。これらの資産は、OIST ユーザーが知る必要がある場合にのみアクセスできる

ように管理する必要があります。未発表の研究データ又は論文は、一般的にこの分類に該当するとみなされます。

第三者には、正当な理由がある場合に限り「学内」区分の情報資産へのアクセスが許可されます。

この区分はOISTの情報資産におけるデフォルト（初期設定）とみなされなければなりません。

17.3.9.3 機密

「機密（Confidential）」と格付けされた情報資産とは、それが開示されることによりOISTの事業、評判又は人事に重大な悪影響を及ぼすものを指します。
この区分には、個人番号、クレジットカード、パスポート情報などの個人情報や、その他、法律又は政府規制のもとで保護される情報資産が含まれます。
これらの情報資産は、情報資産管理責任者によって許可された必要最低限のグループだけにアクセスが限定される必要があります。情報資産へのアクセスは定期的に監査されます。

17.3.9.4 クリティカル

「クリティカル（Critical）」と格付けされた情報資産とは、それが開示されることによりOISTの事業、評判又は人事に深刻な悪影響をもたらすものを指します。
「クリティカル」の情報資産へのアクセスは、許可されたユーザーからなる必要最低限に厳選されたグループにのみ限定されます。厳格なシステムアクセスとデータアクセスコントロールを適用し、アクセスは定期的に監査されます。
「クリティカル」の格付けはプロボスト又は事務局長のいずれかの承認を得た場合のみ割り当てることができます。

17.3.10 情報資産の保護

OIST 情報資産の基本的な保護を確実にするために、ユーザーは利用する情報に明示された格付に従い、当該情報資産を適切に取り扱わなければなりません。
情報資産にアクセスするために使用するデバイスのセキュリティレベルとそのアクセス方法は、その情報資産の機密性や保護の必要度に沿ったものであり、OISTの情報資産の格付けやデバイス適格性の基準に従ったものでなければなりません。

OIST情報資産は事業を遂行するためにのみに使用され、使用者はOIST情報資産を職務以外の目的で使用してはなりません。情報資産へのアクセスは、ユーザーが職務を遂行するために必要であってその職務の必要性に沿った「必要最低限」で付与される必要があります。

個人情報の保護で詳述されている規定によってさらに制限されています。個人情

報を取り扱う全てのユーザーは、これらのルールを熟知しておくとともに、その変更について常に状況を把握しておく必要があります。

17.3.11　情報セキュリティ

情報セキュリティポリシーの遵守は、OIST 情報資産のセキュリティの維持に不可欠であり、全てのユーザーの責任です。大学とその情報資産を保護する上で、ユーザーは情報を作成、処理又は保存する際に、本章を遵守しなければなりません。CISO が大学の利益を守るのをサポートするにあたり、システム管理者はここに記載されている全ての規則を遵守するとともに、CISO からの指示に迅速に従わなければなりません。

17.3.12　情報セキュリティインシデントの対応

情報セキュリティインシデントは、OIST 情報資産の機密性、完全性又は有用性を侵害する（又は侵害する可能性のある）、あるいは OIST の規則や日本の法律に反する単一又は一連の望ましくない事象として定義されます。

情報セキュリティインシデント対応は、データフォレンジクスと異なり、通知又は事象によって発動されるものであって、情報セキュリティインシデント調査の結果のみが IT における調査担当者から関係者に開示されます。データが開示されることはありません。CISO は、セキュリティインシデントを調査し、OIST とそのリソースを保護するために必要な処置を講じ、インシデントの調査に関連する情報を提供する責任があります。この点に関して、その他の関係者は、CISO が示す指示に従うものとします。
情報セキュリティインシデントに気づいた全てのユーザー等は、速やかに CIO 及び CISO にメール（cio@oist.jp ciso@oist.jp）又は電話（OIST ディレクトリ https://directory.oist.jp/を参照すること）で連絡するものとします。

詳細については、情報セキュリティインシデント対応手順を参照してください。

17.3.13　データフォレンジクス

データフォレンジクスは、インシデントに関わるデータを識別、抽出、証拠性を明らかにする手段です。これは、IT 資産、電子メール、SharePoint 又はその他の電子データとして保持されているデータが対象となります。

データフォレンジクスは、通常はデータの所有者と協議して同意を得たうえで実行されます。データ所有者が同意しない場合又は法的要件若しくはその他の要件によってデータ所有者の同意を求めることができない場合は、以下に示される承認手順を必要とします。

包括的原則として、データフォレンジクスにおいては、PRP1.3.2　互いに尊重しあ

う職場の実現に向けた基本方針に従うものとします。

データフォレンジクスを実行しようとするインシデントの多くは、関連するデータと IT 資産も含め、本質的に慎重に扱うべきものや機密性の高いものです。データフォレンジクス手順は、このプロセス全体を通して、データフォレンジクス活動が調査される情報の客観性、完全性及び真正性を満たす方法で実行されることを保証するものです。この手続きでは、適切な承認が行われ、関係者の特権が分離され、データへのアクセスはインシデントに関連するもののみに限定されることを要件とします。

リクエスト

データフォレンジクス調査リクエストフォーム（以下本項において「リクエストフォーム」という。）は、データの分析を指示された者（調査担当者）、警察、裁判所又はこれらに準ずる機関が関与する場合は捜査機関に証拠データを提出する責任を負うものが作成しなければなりません。リクエストフォームには、以下の事項を記載してください：

- フォレンジクスを実行する事由
- 調査対象のデータ
- データへのアクセスが必要な期間
- データ所有者に通知し、承認を求めるかどうか（通常の承認手続き）
- そうでない場合は、データ所有者に通知できない又は同意を得られない理由

承認手続

1. データ所有者の承認：
   データ所有者は常に最初にデータアクセスへの承認をするように求められるべきです。データ所有者が同意しない場合又はデータ所有者に尋ねることができない場合は、以下の 2 つの承認手順のいずれかが適用されます。
2. 簡易承認がとられる場合について：
   a. コンプライアンス調査委員会、公的研究費調査委員会、又は本調査委員会（PRP 第 23 章）又はその他の委員会（PRP 第 39 章）による内部要請。
   b. 警察、裁判所又はこれらに準ずる機関による外部からの要請又は命令。

リクエストフォームは下記により承認される必要があります：
- 副学長、ディーン、事務局長又はプロボスト
- 統括弁護士
- データ所有者又は学長

上記にかかわらず、調査担当者は承認者を兼ねることはできません。

3. その他の場合の承認

その他の場合については、リクエストフォームは以下の承認委員会、統括弁護士及び学長の承認を得なければなりません。

承認委員会は下記により構成されます：

a. 教授会議長又はその代理人
b. 人事担当副学長又はその代理人
c. 大学運営に携わる副学長のうち 1 名とし、関連事項及び利害対立の可能性を考慮し、2 名の常任委員が合意の上で選出します。選出は招集後 24 時間以内とします。

上記のいずれかが調査担当者である場合、その委員は、プロボスト若しくはファカルティ長又はその代理人が承認した他のエグゼクティブにより対応するものとします。

承認委員会は、リクエストへの拒否権、承認権又はリクエストを変更して承認する権限を有します。

検証

CIO 又は委任された代理人は、リクエストを受け付け、適切な承認が行われていることを確認します。その後、関連するデータを抽出するために IT ディビジョン又は情報セキュリティセクションの担当者を任命します。

IT ディビジョン又は情報セキュリティセクションは、必要と判断された場合には、フォレンジクコンサルタントを雇うことができます。

抽出

IT ディビジョン、情報セキュリティセクション又はフォレンジクコンサルタントの調査担当者は、暗号化された専用のテンポラリーPC に要求されたデータを抽出し、CIO 又は委任された代理人にそれを預けます。

アクセス

CIO 又は委任された代理人は、テンポラリーPC と関連するアクセス資格情報を調査担当者に預けます。調査担当者は、データ検索を、例えばメッセージの対象者又は受信者など、リクエストに関連する資料のみに制限します。個人的なコミュニケーションやプライバシー、第三者の権利は、できる限り尊重されます。

削除

アクセス期間が終了すると、CIO はテンポラリーPC が返却され、抽出された全てのデータが確実に消去されるよう徹底します。

報告

CIO は、データフォレンジクス活動の結果と抽出されたデータの削除日を最終報告書にまとめ、学長に提出します。

CIO は毎年、BOG、エグゼクティブ委員会、教授会にて、3 つの承認手続それぞれにおける申請件数と承認件数を報告します。

ファイリング
リクエストフォームは最終報告とともに情報セキュリティセクションで文書管理されます。

IT セキュリティインシデント対応はここでは扱いませんが、代わりに本章の17.3.12 情報セキュリティインシデントの対応で扱います。

17.3.14 IT 資産の除去

IT 資産の除去とは、インシデントに対応するため IT 資産を一時的に除去し留保しておくことです。ラップトップ、デスクトップ、モバイルドライブ又はその他のあらゆる IT 資産が除去及び留保の対象になります。IT 資産は業務遂行において重要な場合があるため、その除去は日常的に行われるものではなく、下記のとおり適切にリクエストされ、承認されなければなりません。

IT 資産は、学長、統括弁護士、プロボスト、事務局長、研究担当ディーン又は教員担当学監のいずれかのリクエストにより、CIO の同意を得て、除去、留保されます。
CIO は、その資産の所有者にデバイスの除去を通知し、IT ディビジョンのメンバーに IT 資産を除去し安全な IT 施設内にそれを保持するよう委任します。
IT 資産の除去は、法的要件又はその他の要件によって事前の通知ができないときは、資産所有者に通知する前に行われる場合があります。

IT 資産に保持されているデータへのアクセスは、除去され留保されたものの中にあるものも含め、17.3.13 データフォレンジクス手順の対象となります。

IT セキュリティインシデントへの対応はここでは扱いませんが、代わりに情報セキュリティインシデント対応で扱います。

17.3.15 ラベル

情報資産は、フォーマットに関係なく、それぞれの情報資産の表紙、フッター、ヘッダー又は透かしに情報の格付けを明確に記さなければなりません。これは印刷されたもの、手書きのもの、電子文書やその記録、電子メールの内容や件名等を含み、またそれに限ったものではありません。

ラベルがない文書は「学内」として格付けされます。

17.3.16　複製

ユーザー及び文書管理担当者は、メディアの形式にかかわらず、必要最小限の機密情報のコピー数を保持するものとします。ユーザー及び文書管理担当者は、必要に応じそれらの配布について記録しなければなりません。ユーザーは、全ての印刷物又はストレージメディアを、施錠された引出し又はファイリングキャビネットなどの物理的に安全な保管場所に保管しなければなりません。ユーザーは、不要になった情報資産の複製コピーを安全に廃棄しなければなりません。
情報を複製する場合には、元となる情報の機密性に係る格付を継承するものとします。ユーザーは、情報を作成又は複製するときは、その情報のセキュリティについての完全性及び有用性を評価しなければなりません。

17.3.17　電子メール

ユーザーは、電子メールで交換する情報を、情報の格付けに応じて適切に保護する責任を有します。「機密」又はそれ以上の格付けの情報を電子メールで交換する場合は、強力なデータ暗号化を適用する必要があります。
支払に関する情報（クレジットカード番号、銀行口座の詳細など）、個人番号（マイナンバー）、パスポート情報、その他の個人情報を電子メールにより送受信することは、データを最初に暗号化しない限り、固く禁止します。
電子メールの使用に伴うリスクの管理の詳細については、情報セキュリティサイトを参照してください。
全ての事務職員及び研究支援職員は、OIST に提供されている電子メールシステムのみを使用するものとします。OIST の電子メールを外部の電子メールプロバイダに転送することや、外部のプロバイダから OIST の電子メールサーバへアクセスすることは許可されていません。

17.3.18　送受信における情報漏洩や情報操作の防止

ユーザーは、「機密」又はより高い格付けのデータを外部当事者に送信する際は、セキュリティコントロールを施さなければなりません。

- このようなデータは、送信前に暗号化すること
- 暗号化されたデータとパスワードは、理想的には異なる方法により別々に送信すること
- 複数のセキュリティ管理を適用すること

17.3.19　リムーバブルメディアの使用

USB ドライブ、モバイルハードディスク、SD カードやその他の携帯可能なストレージ機器等のリムーバブルメディア機器については、次の制限が適用されます。

- 事務部門は、リムーバブルメディアの使用を原則禁止とし、IT ディビジョンが提供するデータリポジトリを使用する必要があります。例外的な使用については、IT ディビジョンに連絡し、CISO 又は CIO の許可を得てください。
- リサーチユニットにおいては、「機密」や「クリティカル」な情報を保存するためのリムーバブルメディアの使用は、教員の裁量に委ねられています。

リムーバブルメディアに伴うリスクの管理の詳細は情報セキュリティサイトを参照してください。（情報セキュリティサイト）

17.3.20　リモートアクセス

外部のネットワークから OIST の IT リソースにアクセスするには、事前に IT ディビジョンの許可を得て、必ず承認された OIST IT リモートアクセスサービス（VPN、SSH など）を介してリソースにアクセスしなければなりません。
部外者に OIST の IT リソースにアクセスさせる目的で、OIST 管理外のリモートアクセスソフトウェアやサービス（チームビューアなど）を用いることは禁止します。例外的な取扱は、ネットワークセキュリティーが充実している状況下であれば、CIO 又は CISO がそれを許可することがあります。例外的な取扱が必要な場合は、ユーザーは IT ディビジョンに連絡しなければなりません。

17.3.21　情報の廃棄

ユーザーは、「学内」又はそれ以上の格付けがされた情報が不要になったときは、速やかに回復不能な方法でそれを安全に消去しなければなりません。ユーザーは、機密文書の全てのハードコピーを、回復不能な方法で物理的に破棄しなければなりません。ユーザーは必要に応じて IT ディビジョンに廃棄処理を申請するものとします。

17.3.22　IT 資産の物理セキュリティ

ユーザーは、IT 資産の盗難を防止する責任を有します。ユーザーは IT 資産の盗難及び IT 資産への不正なアクセスを防止するために、以下のような対策を講ずることとします。

- 誰でもアクセス可能な場所においては、又は「機密」若しくはそれ以上の格付けがされた情報にアクセスする場合は、モバイル端末を除く IT 資産をセキュリティワイヤを用いて固定する。
- 使用しないときは、IT 資産は施錠できる袖机やキャビネット等に確実に収納しなければならない。
- 5 分間以上操作が無いと自動的にスクリーンロックするよう設定する。

17.3.23　悪意のあるソフトウェア対策

ユーザーは、自身が管理している IT 資産を次の通り管理する責任があります。

- 最新のソフトウェアパッチとアップデートが適用されていること。
- アンチウィルス又はその他のアンチマルウエア機能がインストールされ、最新のバージョンに更新されていること。
- 悪意のあるソフトウェアとファイルを検知するためのリアルタイムスキャン機能が有効になっていること。
- 潜在的な悪意のあるファイルが検知されたときに検疫する機能が有効になっていること。
- 悪意のあるソフトウェアを検出するために全てのファイルを検査するフルスキャンが定期的に実施されること。
- 外部から受信した全てのデータとソフトウェアが開かれる前又は取り込む前にスキャンされること。

ユーザーは、IT ディビジョンからの最新のセキュリティ更新プログラムを適用して、悪意のあるソフトウェアの感染を防止するよう努めなければなりません。

17.3.24 IT サービスに対する脅威対策

OIST は、IT リソースにアクセスして利用しようとする外部の攻撃者から絶えず攻撃を受けています。IT ディビジョン及びシステム管理者は、OIST とそのユーザーを保護するために、次の要件を満たす必要があります。

17.3.24.1 ソフトウェアに関する脆弱性対策

システム管理者は、ソフトウェアを使用する前に、公表されている脆弱性に対するパッチ又は回避策を確実に適用しなければなりません。
システムの本番稼働後は、システム管理者は引き続きシステムのアップデートやパッチを評価し、システムやそのユーザーに与える潜在的な影響を考慮しながらそれを適時に適用しなければなりません。
OIST の情報資産を危険にさらす可能性がある脆弱性が検出された場合、システム管理者は直ちに CIO 及び CISO に連絡し、OIST 情報資産を保護するための適切な措置を取る必要があります。

17.3.24.2 不正プログラム対策

システム管理者は、サーバ又は他のデバイスに、マルウェア対策ソフトウェアや同等の機能を持ったソフトウェアをインストールする必要があります。システム管理者は、マルウェア対策ソフトウェアの状態を監視し、必要な措置を取る必要があります。システム管理者は、マルウェア対策ソフトウェアとその定義ファイルを最新の状態に維持します。システム管理者のみが、マルウェア対策ソフトウェアの構成を変更できる権限を持ち、そのような権限は他のユーザーには付与されません。システム管理者は、マルウェア対策ソフトウェアによるシステムの定期的なスキャンを設定します。

17.3.25　不正侵入対策

システム管理者は、サーバやシステムへの侵入を防ぐために、以下の処置を講じなければなりません。

- 不要なサービスを削除又は無効にする。
- 未知又は許可されていないプログラムやコードの実行を防止する。
- システム又はソフトウェアの動作に必要な通信チャネルのみを許可するように、ファイアウォールを構築、アップデートする。

システム管理者は、リムーバブルメディア（そのようなデバイスの使用が許可されている場合）による侵入を防止するために、以下の処置を講じなければなりません。

- 不要な USB ポート、サーバ又はデバイスへの物理接続を全て無効にする。
- 接続時にアンチマルウェアソフトウェアを使用してリムーバブルメディアをスキャンする。

17.3.26　訓練

17.3.26.1　ユーザーの訓練

上長は、ユーザーが業務を開始する前に情報セキュリティに関して適切に訓練されていることを確認する責任があり、ユーザーが自ら訓練を遂行するように指導します。

17.3.26.2　システム管理者の訓練

システム管理者は、OIST システムの管理者権限が付与される前に、システムセキュリティのあらゆる側面について十分な訓練を受けていなければなりません。

17.3.27　公開 Web

17.3.27.1　インターネットドメイン名の管理

IT ディビジョンは、コミュニケーション・広報ディビジョンに代わって oist.jp ドメインを管理しています。

研究ユニットのウェブサイトは、unit.oist.jp ドメイン又は他のサブドメイン配下にあり、OIST IT の管理下にあります。このルールは、大学全体の Web と研究ユニット又はプロジェクトの Web を明確に区別するためのものです。

17.3.27.2　目的ごとのインターネットドメイン名

OIST ドメインの外部にある URL を必要とする研究プロジェクトは、IT ディビジョンに外部ドメイン名の登録と、サイトを格納する仮想マシンを作成するようリ

クエストすることとします。このリクエストは、CIO と教員担当学監の承認を必要とします。
これらのドメインは、通常、.org 又は.net（非営利）に限定され、他のドメインが必要な場合は CIO との協議と承認が必要となります。全てのユニットは OIST ユニット（グループ）のサイトを最新の状態に保つ必要がありますが、このスペース以外の場所におけるユニット自体を宣伝するためのウェブサイトの作成は推奨されません。

17.3.28　運用管理

17.3.28.1　事業継続計画

情報資産管理責任者及び OIST IT は、OIST 情報資産及びリソースの可用性を保証する事業継続計画を策定するものとします。
事業継続計画は、その有効性を検証し、スタッフの訓練が適切に遂行されることを確実にするために、少なくとも年 1 回は試験されなければなりません。

17.3.28.2　バックアップ

情報資産管理責任者及び IT ディビジョンは、情報資産が資産の価値に見合った頻度と冗長性をもってバックアップされることを徹底します。情報資産管理責任者は、情報資産の保存期間を指定し、それを管理します。

「クリティカル」と格付けされる情報資産や、急速に増加する情報資産については、年に一度以上の頻度で、復元テストを実施することを推奨します。

情報資産管理責任者は、IT ディビジョンに対し、保存期間を超過した又は必要でなくなった情報資産のバックアップデータを、削除、取り消し又は物理的に破棄するよう要請します。

17.3.28.3　変更管理

変更管理は、IT リソースに対するあらゆる変更が文書化され、レビュー、承認されることを保証するプロセスです。この変更管理プロセスは、プロジェクト等の計画された大規模な変更と、ソフトウェアパッチや予定外のサーバーメンテナンスなどの必要に迫られた小規模な変更の両方を網羅しています。変更管理プロセスと手順は、文書化され、全ての OIST IT リソースに対して適切に実施されなければなりません。監督責任と手順は、機器、ソフトウェア又は手順の全ての変更を適切に管理するために定義されます。これらの手順は、SLA で定義されます。

17.3.29　OIST IT 設備へのアクセス

サーバールームやネットワーク・コミュニケーションスペースを含む IT 設備へのアクセスは制限されています。これらの施設へのアクセスは全て認証の対象となり、アクセスは CIO 又は CISO の承認を受けなければなりません。

現地視察の目的でアクセスは、CIO オフィスを通じて調整する必要があります。

17.3.30　OIST IT 設備におけるハードウェアのホスティング

ハードウェア（サーバ及びストレージを含む）を購入する又は OIST IT 施設内にそれを保管することを希望する全ての者は、事前に IT ディビジョンに相談しなければなりません。事前の相談がない場合、ハードウェアが収納できない場合があります。IT ディビジョンは、OIST 施設に設置することが適切でないものや、安全でないと判断されるハードウェアの設置を拒否する権利を有します。ハードウェアは OIST サーバのハードウェア要件に準拠していなければなりません。サーバーハードウェアの基本要件は 17.5.6 に記述されています。

17.3.31　ログの記録と監視

IT ディビジョンは、リソースへの侵入や誤使用を検出するために、IT リソースからのログ情報を自動的に収集して分析します。IT ディビジョンは、この目的のために IT リソースによって生成された全てのログ情報にアクセスする権利を有します。法的要件及び契約上の義務を遵守するために、IT ディビジョンは、ユーザー活動、セキュリティ事象及びその他の関連情報を含む監査ログを記録します。得られた情報は「機密（Confidential）」に格付けされ、その情報へのアクセスは IT ディビジョンの適切なメンバーのみに限定されます。

17.3.32　追加の規程と手順

本学内の教員や副学長が、OIST 情報資産の利用について、追加的な規則や手順を課すことがあります。そのような追加的な規則や手順は、この章と整合性がなければなりません。また、その追加的な規則や手順によって、追加的な詳細事項やより高度な制限が定められることはあっても、制限が緩和されることはありません。

学生は、この章に加え、第 5 章「研究科ハンドブック」を参照してください。

17.4　権利と責任

17.4.1　　本学について

本学は情報資源を所有し、管理します。本学は IT リソースのセキュリティを保護するために合理的なセキュリティ対策を講じますが、それによって本学が絶対的なセキュリティ及びプライバシーを保証するものではありません。本学は、電子メールを含むあらゆる IT リソースの使用を制限なく監視する権利を有します。本学は、その IT リソースのセキュリティと整合性を確保するために必要なあらゆる措置をとる責任を有します。日常のシステム管理業務やインシデントの報告により、規程や日本の法令に対する違反が認められた場合、本学は、必要な又は指示された調査と情報資産を保護する処置を実施するとともに、調査に関する情報を

提供します。

この点に関し、CIO 及び CISO は特定の権利と責任を有し、その他の関係者は彼らの指示のもとで業務を遂行します。

17.4.2　ユーザーの権限やその責任について

大学で業務を行うために、ユーザーは IT リソースへのアクセス権限が付与されます。IT リソースを使用するにあたり、ユーザーは本学の該当する基本原則、ルール、手続や関連法規を遵守しなければなりません。ユーザーは沖縄科学技術大学院大学 IT リソース利用規約を熟読し、手書き署名又はデジタル署名して、これらについて理解したことを知らせなければなりません。

17.4.3　教員

教員は、当該の研究の範囲内の情報資産における情報資産管理責任者に従事するとともに、ユニットのメンバー1 名を情報資産管理担当者に指名することができます。研究に関する情報資産の管理については、教員が他の大学や会社との研究に関する合意などといった契約上の要求事項を十分に考慮します。

教員は、自身が監督するユーザーが業務に従事する前に、関連する IT についての基本方針・ルール・手続や適用される法規に関して教育されているかを確認する責任があります。

17.4.4　副学長、シニアマネージャーとマネージャー

副学長は、権限を有する組織内の情報資産を管理するために、情報資産管理担当者を任命する責任があります。

また、副学長、シニアマネージャー、マネージャーは、自身が監督するユーザーが業務に従事する前に、関連する IT についての基本方針・ルール・手続や適用される法令に関して教育されているかを確認する責任があります。

17.4.5　最高情報責任者（CIO）

CIO は、本学の IT について、以下に記述する全体的な責任を有します。

- 本学の IT の戦略計画の立案
- IT システムの開発、設置、保守の監督
- 情報資産へのアクセスと許容される使用に関するルールの確立、普及
- データとシステムを保護するための合理的なセキュリティポリシー及び対策の確立
- システムリソースの使用状況の監視及び管理
- 本学のポリシー違反が疑わしものについて調査、学長への違反の報告

- 最高情報セキュリティ責任者（CISO）の任命

17.4.6　最高情報セキュリティ責任者（CISO）

CISO は、以下を含む、本学のセキュリティを維持する全責任を有します。

- セキュリティプロセスと手順の確立
- 情報セキュリティインシデント対応の実施、CIO への結果報告
- IT セキュリティ監視システムの開発、構築、運用

17.4.7　情報セキュリティ委員会

情報セキュリティ委員会は、OIST の情報資産を保護するため、情報セキュリティプログラムを見直し、情報セキュリティリスクを評価します。また、委員会は、セキュリティインシデント対応において、CISO を支援します。委員会規程は別に定めます。

17.4.8　情報セキュリティ監査責任者

情報セキュリティ監査責任者は、毎年情報セキュリティ監査を計画し、実施するものとし、監査に関する統括を行います。情報セキュリティ監査責任者は、最高内部監査責任者（CIAO）をもって充てます。

17.4.9　情報資産管理責任者

情報資産管理責任者は、関連する全ての法令、規則や規制に基づき、自身が権限を有する組織の情報資産の格付けの決定、情報資産へのアクセス権限の付与及び適切な許可スキームについての説明責任を有します。

情報資産管理責任者は、通常、研究ユニットの長や OIST の情報資産を管理するディビジョンの長が務めます。情報資産管理責任者は、情報資産を管理する情報資産管理担当者を任命することができますが、情報資産管理責任者としての説明責務は引き続き有します。

17.4.10　情報資産管理担当者

情報資産管理担当者は、OIST の情報資産の適切な取扱いを確保する責務を有します。

17.4.11　特権ユーザー/システム管理者

システム管理者を含む特権を付与された全てのユーザーは、システム所有者と情報資産管理責任者の指示のもとで、本ポリシー及び関連ポリシーを IT リソースに適用させる責任を有します。これらのユーザーは、OIST IT リソース利用規約以外にも、システム管理者行動規範を読み、署名する必要があります。

17.4.12　第三者ユーザー

OIST は、全ての協力会社、コンサルタント、ベンダーに対して関連する本学の基本手続・ルール・手続及び関連する法令に同意し、それらを遵守することを求めます。第三者が「公開」の格付けよりも上位の情報資産にアクセス又は第三者とそれらの情報を共有する場合は、その第三者は OIST IT リソース利用規約及び適切に作成された守秘義務契約書に拘束されます。

17.4.13　システム開発者やインテグレーター

システム開発者やインテグレーターは、これらのポリシーをシステム、情報及びその他の情報リソースに適用させる責務を有します。「公開」の格付けよりも上位の情報資産やリソースが第三者によってアクセス又は共有される場合は、その第三者は OIST IT リソース利用規約及び適切に作成された守秘義務契約書に拘束されます。

17.5　手順

IT 手順と情報セキュリティの詳細については、サービスポータルウェブサイトをご参照ください。

17.5.1　IT ディビジョンへのリクエストプロセス

IT ディビジョンへの問い合わせ方法は以下の通りです。

- E メール：mailto:it-help@oist.jp
- Web リクエスト フォーム：https://oist.service-now.com/sp
- 対面：Lab 2 Level B（Mountain side）

17.5.2　事務部門における IT 機器の購入とアップグレード

事務部門における IT 機器の購入とアップグレードは IT ディビジョンを介して行う必要があります。標準的なデバイスのカタログは、サービスポータルウェブサイトのリストにあるとおりです。購入にはセクションマネージャーの承認が必要となり、承認を得た後に IT に連絡する必要があります。例外として、CIO が標準ではないデバイスを承認することがあります。

17.5.3　研究ユニットにおける IT 機器の購入とアップグレード

標準的なハードウェアのカタログはサービスポータルウェブサイトにあります。

これらのデバイスは評価済みであり、OIST 環境下でのサポートが保証されています。カタログに記載されているアイテムを購入したい研究者は、17.5.1 に記載の手順より IT ディビジョンに連絡を取ってリクエストしてください。

カタログに記載されていないアイテムを購入したい研究者は、まず IT ディビジョ

ンに連絡して OIST のシステム環境に適合するか確認することが強く推奨されます。また、IT ディビジョンは日本国内の業者との連携があり、交渉をサポートします。

IT 資産を研究機器の一部に組み込む場合、そのガイドラインや仕様は
https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0012668
に記載されています。

17.5.4 学外での利用申請

https://oist.service-now.com/sp?id=sc_cat_item&sys_id=ea1eea70db8aeb004a187b088c9619f2&sysparm_category=59d4b9b2db65e380d7c7e5951b961906

17.5.5 IT 資産の再割り当て又は廃棄方法

https://oist.service-now.com/sp?id=sc_cat_item_guide&sys_id=87501059db2ce3406885f00ebf961971&sysparm_category=ef2e888edb47df004a187b088c96199a

17.5.6 IT サーバールームへの機器の設置

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013494

17.5.7 エンタープライズアプリケーションに関するリクエスト

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013670

17.5.8 情報セキュリティインシデント対応

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013553
https://groups.oist.jp/ja/it/info-sec-incident-response

17.5.9 メールとオンラインコミュニケーションの行動規範

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013668

17.6 フォーム

17.6.1 OIST IT リソース利用規約

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013570
https://groups.oist.jp/it/it-aup

17.6.2 システム管理者の行動規範

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013709
https://groups.oist.jp/ja/it/info-sec-aua

17.7 連絡先

本方針の所管:最高情報責任者

17.8 定義

17.8.1 情報技術資源（IT リソース）

大学の情報技術資源（IT リソース）は、全ての情報資産と IT 資産からなります。

17.8.2 情報資産

情報資産とは、研究用、管理用を問わず、またメディア形式も問わないデータ、ファイル、ワークフロー及び本学の情報管理のためのメカニズム等の全ての本学の情報です。この広範な定義には、法人文書、個人情報等、さらなる規則や手続が適用される特別な種類のものも含みます。

17.8.3 情報技術資産（IT 資産）

情報技術資産（IT 資産）とは、本学のデジタル情報にアクセス又はそれらを格納及び送信する全てのコンピュータや通信機器、その他の技術をいいます。またそれは、大学が全てを所有しているか、又は他者が所有しているかを問わず、また電子ネットワーク、システム、クラウドサービス、コンピュータ、デバイス、電話、ソフトウェア等の種類を問いません。

17.8.4 デバイス

デバイスは、情報技術資産の同義語です。

17.8.5 情報技術サービス管理（ITSM）

情報技術サービス管理（ITSM）とは、ビジネスの要件に合わせて IT サービスを提供するための実践的なフレームワークです。

17.8.6 サービス レベル契約（SLA）

サービスレベル契約（SLA）とは、ITSM スタンダードに規定される文書です。この文書は、IT ディビジョンがユーザーに提供するサービスレベルを記載するものであり、サービス品質を測定する基準を定義するものです。
https://groups.oist.jp/it/it-service-level-agreement

17.8.7 情報セキュリティ

情報セキュリティの原則は、OIST 情報セキュリティウェブサイトに記載されています。

17.8.8 情報セキュリティの関連法規

OIST の情報セキュリティの主な関連法規は以下の通りです。

- 不正アクセス行為の禁止等に関する法律
- 独立行政法人等の保有する個人情報の保護に関する法律
- 独立行政法人等の保有する情報の公開に関する法律

- 電子署名及び認証業務に関する法律（電子署名法）
- 著作権法
- 不正競争防止法

17.8.9　情報の格付けとデバイス

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013460

17.8.10　情報システム

情報システムとは、情報を処理又は解釈する人とコンピュータで構成されるシステムです。OIST における情報システムは、OIST 情報資産を処理、送信又は格納するシステムです。これには、開発、購入又は外部委託されたシステムが含まれますが、これに限定されません。

17.8.11　ユーザー

一般に公開されるレベルを超えた IT リソースへのアクセス権が付与された個人又は主体をさします。

17.8.12　情報資産管理責任者

関連する法律及び規制に従って、情報の格付け分類の定義、アクセスの許可及び情報資産への適切なアクセス方式の策定に関する責任者をさします。

17.8.13　情報資産管理担当者

OIST 情報資産の適切な管理を保証する任を課された者をさします。

17.8.14　管理者権限

ユーザーが情報資産又は IT リソースに通常許可されているレベルを超えてアクセスできるようにする特権のことを指します。

17.8.15　特権ユーザー

権限昇格が付与されたユーザーです。

17.8.16　システム管理者

システム又はサービスに対する管理権限を持つ特権ユーザーのサブセットです。

17.8.17　ID 管理システム（IDM）

OIST ID 管理システム（IDM）は、大学又はネットワーク間のアイデンティティ管理を処理します。システムは、OIST の認証及び認可システムを制御し、情報資産への適切なアクセス方式を容易にします。

17.8.18　サーバ

コンピューターネットワークから送信されるリクエストに対応する又はネットワ

ーク、データサービスを提供するシステムです。

17.8.19　ストレージメディア
USB メモリー、外部ハードディスク、DVD-R を含む情報（データ）を記録（収納）するためのデバイス又は有体物を指します。

17.8.20　リムーバブルメディア
システムに簡単に着脱できる記憶媒体。USB フラッシュドライブ又は光学式メディアなどです。

17.8.21　安全な消去
記憶媒体上の全てのデータを回復不能な形で抹消することです。

17.8.22　外部委託
学外の業者から契約によるサービス又はシステムを提供されることです。

17.8.23　主体
情報システムにアクセスする者、プロセス、クライアント端末又はサーバ装置のことをいいます。

17.8.24　主体認証
ある主体が別の主体を保証するプロセスをいいます。

17.8.25　識別
情報システムにアクセスする主体を特定することです。

17.8.26　アクセス制御
情報へのアクセスを許可する者を制限することです。

17.8.27　アクセス権限管理
主体認証にかかるアカウント及びアクセス制御における許可情報を管理することです。

17.8.28　アカウント
OIST IDM に登録された全ての主体のことをいいます。

17.8.29　暗号化
認可された主体だけがそれを読むことができるように情報資産をエンコードするプロセスをいう。

17.8.30　不正プログラム（マルウェア）

マルウェアとは、コンピュータやモバイルの操作を中断させる、機密情報を収集する、プライベートコンピュータシステムにアクセスする、望ましくない広告を表示する目的のために用いられるソフトウェアです。

17.8.31　不正プログラム定義ファイル

不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいいます。

17.8.32　CMDB

OIST 構成管理データベース（CMDB）は、IT 資産に関する情報及びそれらの間の記述的関係を格納するリポジトリです。

17.8.33　ソフトウェアカタログ

https://groups.oist.jp/ja/it/oist-software

17.8.34　災害復旧と事業継続計画

災害復旧（DR）は、自然災害や人為的災害に続く重要な技術インフラストラクチャやシステムの復旧や継続を可能にする一連のポリシー、手順、システム及び組織からなります。

事業継続計画（BCP）は、事業所が短期間の災害を局地的に受けた場合や発生や建物が広範囲で被害を受けた場合のような、さまざまなレベルの災害によって影響を受けた場合に、事業を継続させるための計画です。

17.8.35　情報セキュリティインシデント

情報セキュリティインシデントは、OIST ポリシー又は日本の法律に反し、OIST 情報資産の機密性、完全性若しくは可用性を侵害する（又は侵害する可能性のある）単一若しくは一連の望ましくない事象として定義されます。侵害とはシステム又はその情報のセキュリティが実際に侵された事象をさします。

情報セキュリティインシデントの例。

- 間違った受信者に電子メールで送信される個人データなど操作エラーなどあらゆる原因によるデータの損失
- 処理やデータのストレージシステムの不正使用
- 情報セキュリティと利用規約違反
- 大学によって所有されているか否かに関わらず、大学情報を格納するラップトップ、デスクトップ、PDA 等のデバイスの盗難等による損失
- システム又はデータへの不正アクセスを得るための試み（失敗又は成功のいずれの場合も含む。）
- 望ましくないサービスの停止やアクセス拒否

- ソフトウェアやハードウェアの誤動作

17.8.36　APT 攻撃（APT）

APT 攻撃（Advanced Persistent Threat）は、特定の主体に狙いを定め、多くの場合人間による、隠密的かつ連続的なコンピュータハッキングプロセスを指します。APT プロセスは、長期間にわたる高度な潜伏性を要します。高度なプロセスは、システム内の脆弱性を悪用するマルウェアを用いた精巧な手法を意味します。継続的なプロセスは、外部の制御システムが特定のターゲットのシステムを継続的に監視し、データを抽出することを指します。脅威のプロセスは、APT 攻撃の指揮に関し人的な関与があることを示します。