学校法人Ｃ２Ｃ Ｇｌｏｂａｌ Ｅｄｕｃａｔｉｏｎ Ｊａｐａｎ
情報セキュリティポリシー

2021 年 4 月 1 日改定

Ⅰ．情報セキュリティの基本方針

学校法人Ｃ２Ｃ Ｇｌｏｂａｌ Ｅｄｕｃａｔｉｏｎ Ｊａｐａｎ（以下、本学）における教育、研究活動は、情報ネットワークを介した情報の収集、格納及び伝達といった手段に強く依存し、その利便性とともに情報の公開性が求められる。一方、情報の漏洩や破壊、改ざん、もしくは不正アクセス等により情報資産が侵害されれば、教育、研究活動が停滞し、さらに本学に対する社会からの信頼喪失につながる危険性がある。従って、教職員、学生、および本学に関わるすべての関係者が弛まぬ努力をもって、本学の情報資産の機密性、完全性、可用性に配慮し、保護しなければならない。また本学が提供する情報資産に関連するサービスを利用する者は、本ポリシーを遵守する責任があり、意図の有無を問わず、学内外の情報資産に対する権限のないアクセスや改竄、複写、破壊、漏洩等をしてはならない。

（1）本学の情報システムを利用する全ての者は、ポリシーを遵守する義務と責任を有し、本学内外の情報資産に対し権限のないアクセス、改ざん、破壊、漏洩等の不正行為をしてはならない。

（2）本学は、個人のプライバシーに関する情報等の機密性を確保すると共に、情報資産のセキュリティを高めなければならない。

（3）本学は、情報セキュリティの保持と強化及び教育指導・啓発活動等のポリシーの実施に関するすべての責任を負う。

＜参考＞
* 機密性とは、情報に関して、認められた者だけがアクセスできる状態を確保することをいう。
* 完全性とは、情報が破壊、改ざんまたは消去されていない状態を確保することをいう。
* 可用性とは、アクセスを認められた者が、必要時に中断することなく、情報にアクセスできる状態を確保することをいう。

Ⅱ．情報セキュリティの対策基準

1. 組織・体制

本学は、情報セキュリティを組織的に管理運用するため、その役割と責任を次のとおり定める。

(1) 最高情報セキュリティ責任者

本学に最高情報セキュリティ責任者（Chief Information Security Officer。以下「CISO」という。）を置く。CISO は、適切な情報セキュリティ対策を図るための権限及び責任を有する。

(2) 法人本部

本ポリシー及び情報セキュリティマネジメントに関する重要事項を決定する。

(3) 情報基盤センター

本ポリシー及び情報セキュリティマネジメントに関する重要事項を策定し、法人本部に諮問する。遵守状況の確認、評価及び見直しを行うとともに、情報セキュリティインシデントや障害時の対応状況を確認し、必要に応じて対策等に係る助言・指導・勧告を行う。また C2C Global Education Japan CSIRT（Computer Security Incident Response Team）を設置し、インシデント関連情報、脆弱性情報等を常に収集、分析し、対応方針や手順の策定などの活動を行う。

本ポリシー及び情報セキュリティマネジメント遂行に際し、ICT に関連する最新情報及び関連法令に係る情報収集を定期的に行うものとする。

(4) 本学構成員

本学構成員とは、本学に在籍するすべての教職員、学生、生徒等を示す。

本学の構成員は、本ポリシーを遵守するとともに、情報セキュリティインシデントを発見したときは、速やかに情報基盤センターに報告しなければならない。

２．情報セキュリティポリシーの対象範囲並びに対象者

（1）ポリシーの対象範囲は、本学の情報ネットワークに接続された情報システム（本学以外の情報システムで本学の情報ネットワークに一時的に接続された情報システムを含む）とする。

（2）ポリシーの対象者は、本学の教職員、学生、生徒等、及び委託業者や来学者など、本学の情報システムを利用するすべての者とする。

３．情報セキュリティ侵害の阻止及び侵害行為の抑止

本学は、次の情報セキュリティ侵害の阻止及び侵害行為の抑止に努める。

（1）情報システムの設置場所は、安全性を保ち、不正な立ち入りを阻止する対策とともに、盗難、災害、バックアップ、情報ネットワークやサーバの保全等の対策に十分に配慮する。

（2）本学内外からの不正なアクセスによる情報資産の改ざん、破壊等の行為を阻止するため、不正アクセスの防止並びに検出のための適切な手段を講じなければならない。また、不正アクセスが検出された場合は、速やかに関連する通信の遮断又は該当する情報機器の切り離しを行う。

（3）全構成員に対して、ポリシーを周知徹底させると共に、情報セキュリティを確保するための教育や啓発活動を実施する。

４．情報資産の分類

情報資産の取り扱いは、それが果たすべき役割と影響を十分に認識し、常にその機密性、完全性、可用性に配慮して適切に分類し、管理しなければならない。従って、以下の点に留意し実施する。

（1）公開情報とすべき情報は、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等に対し、防止策を講じなければならない。

（2）非公開情報に不正にアクセスしてはならない。非公開情報の盗難、漏洩、改ざん、複製等を防止するため、非公開情報を扱う情報ネットワークには防止策を講じなければならない。また、非公開情報の利用は、情報の利用を許可された者が、許可された情報の操作だけを行えるよう、認証、アクセス制御等の措置を講じなければならない。さらに、非公開情報を記録した媒体は、適切に管理しなければならない。

５．情報資産の管理

サーバに保存された情報はサーバの管理者が管理し、パソコン、記録媒体等に保存された情報は管理者と利用者が管理する。また、情報機器及び記録媒体の廃棄にあたっては、その処分方法に注意すること。特に、非公開情報とすべき情報を削除するときは、記録媒体の初期化、物理的な処置等を行い情報が復元できないよう処分する。

６．実施手順

ポリシーの実施に係る手順は、別に定めるものとする。

７．評価・見直し

ポリシーは、情報通信技術の発展並びに制定したポリシーの実効性等に鑑みて、定期的に見直しを行い、セキュリティレベルの高い、遵守可能なポリシーとして保持する。

８．その他必要事項

このポリシーに関し、必要な事項は別に作成・管理するものとする。