標準的格付け基準の策定と情報格付けスタートガイドの作成について

戸田 庸介 [1)], 片桐 統 [1)], 斎藤 紀恵 [1)], 石橋 由子 [1)]

1）京都大学 企画・情報部

i-s-office@iimc.kyoto-u.ac.jp

Created the standard information rating and information rating starting guide

Yosuke Toda [1)], Osamu Katagiri [1)], Norie Saito [1)], Yoshiko Ishibashi [1)]

1) Planning and Information Management Department, Kyoto University.

概要

情報格付けは、組織における情報セキュリティ対策基準に沿った対策を適正に実施するための基礎となる重要な事項であり、京都大学では 2008 年度に情報格付け基準を整備した。毎年実施している情報セキュリティ監査において 2009 年度から情報格付けの運用状況の確認を行っているが、情報格付け基準は浸透せず、情報格付けが適切に行われていない実態があることが明らかであった。情報格付けの運用改善に向けての取り組みとして、2013 年度から 2018 年度にかけて学生情報の成績データ、人事情報の勤務記録データといった情報種別ごとに情報格付けの具体的な標準の策定と、2019 年度に情報格付けを今すぐはじめて日々の業務で習慣づけることを目的として、機密性だけに説明を絞った情報格付けスタートガイドを作成した。

1 はじめに

情報セキュリティの定義は、OECD(経済協力開発機構)が、1992 年に発表した情報セキュリティに関するガイドラインの中で「情報セキュリティの目的は、情報システムに依存する者を、可用性、機密性、完全性の欠如に起因する危害から保護することである。」と定義しており、その後の情報セキュリティマネジメントの国際標準でも、この考え方は踏襲されている[1]。機密性、完全性、可用性は情報セキュリティの 3 要素と呼ばれ、重要な概念となっている。

情報セキュリティとは情報資産を安全に守ることであり、守るべき情報資産を明確化するために情報格付けを行う必要がある。情報格付けは情報セキュリティの 3 要素それぞれの観点があり、政府機関統一基準では、機密性については表 1 に示すように 3 段階となっている。機密性は秘密文書に相当するという最も機密性が高い機密性 3 情報が定義されているが、完全性と可用性については相応する定義はなく 2 段階となっている。完全性の分類基準は改ざん、誤びゅう又は破損により権利侵害、業務遂行に支障のおそれがあるかとなっている。可用性の分類基準は減失、紛失又は当該情報が利用不可能であることにより権利侵害、業務遂行に支障のおそれがあるかとなっている。

表 1 機密性の格付け基準

格付け	分類基準
機密性 3 情報	情報公開法にもとづく秘密文書に相当する機密性を要する情報
機密性 2 情報	秘密文書に相当する機密性は要しないが、その漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
機密性 1 情報	機密性 2 情報又は機密性 3 情報以外の情報

組織の情報セキュリティに関する方針を示した文書は、図 1 に示すようにポリシー、スタンダード、プロシージャーという 3 階層が一般的である。情報化技術の発達により、組織における情報資産は増加の一途をたどり、それらを扱う構成員の IT 知識や IT スキルは様々となっているため、すべての構成員に情報セキュリティ文書の理解を広げることは容易ではない。構成員数が 3 万名を超える大きな組織である京都大学（以下、「本学」という）でも同様の課題を抱えている。

本稿では、情報セキュリティにおいて重要な情報格付けについて、本学において構成員への理解を広げるためにスタンダードとプロシージャーにあたる文書の整備について工夫してきた取り組みについて述べる。まずは、スタンダードについて2013 年から 5 年以上に渡って、「京都大学情報格付け基準（以下、「格付け基準」という。）」に情報種別ごとに具体的な標準を明示した別表を加える取り組みについて述べる。次に、プロシージャーについて 2019 年度に IT が苦手な構成員でも理解して運用できるように機密性だけに説明を限定した情報格付けスタートガイドを作成した取り組みについて述べる。

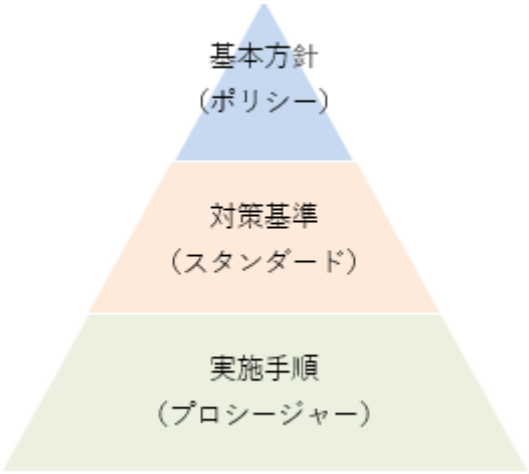

図 1　情報セキュリティポリシーの文書構成

2　標準的格付け基準の策定

2.1 本学における格付け基準の制定

本学の情報セキュリティポリシーの文書構成は、2008 年度に国立情報学研究所が策定した「高等教育機関の情報セキュリティ対策のためのサンプル規程集」[2]を参考として大幅に改正された。格付け基準も合わせて制定された。

情報セキュリティポリシーの文書構成としては、ポリシーにあたる「京都大学の情報セキュリティ対策に関する規程」の第 10 条に情報資産の格付け及び管理が定められ、スタンダードにあたる「京都大学情報セキュリティ対策基準」の第 4 章の第 61 条から第 70 条に情報の格付けと取扱いが定められている。そして、同じスタンダードの位置づけとして格付け基準が定められている。

2.2 標準的格付け基準に至る経緯

格付け基準が浸透していないという課題認識から、毎年実施している情報セキュリティ監査において情報格付けに関するアンケート監査に盛り込んでいる。アンケート監査の結果、格付け基準が浸透しない理由に以下の意見が挙げられた。

- 情報格付けそのものがよくわからない
- どうやって格付けを決めたら良いかわからない
- 抽象的なルールはあっても、実際に具体的な情報への格付けができない

これらの意見から、実際の情報資産に対して教職員がどのように情報格付けしてよいかがわからない状態であることが判明した。

この状態を改善するため、教職員は標準を参照するだけで情報格付けが行えることを目標として、学生情報の成績データ、人事情報の勤務記録データのような情報種別ごとに具体的な情報格付けの標準を作成する方針とした。本学で扱うことが想定される情報種別を網羅するには、時間を要することから 2015 年度から 3 ヵ年で標準的格付け基準を整備していく計画とした。

2.3 標準的格付け基準作成の概要

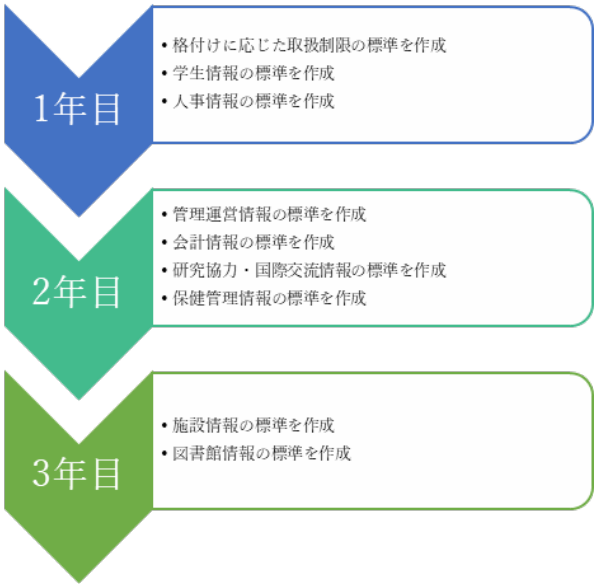

図 2　標準的格付け基準策定の 3 ヵ年の流れ

3 ヵ年の作成作業を図 2 に示す。まず格付けに応じた取扱制限の標準を作成した。格付けに応じた取扱制限の標準とは、機密性の暗号化に関する取扱制限を例に挙げると、機密性 3 情報は「必須」、機密性 2 情報は「通信時必須、保存時推奨」、機密性 1 情報は「指定なし」を標準としている。この

ように機密性３情報から機密性１情報までの格付けごとに情報をどうのように取り扱うべきかを具体的に示した標準である。それぞれの詳細については次節以降で述べる。

人事情報および2年目以降の情報の格付け標準の作成については、「京都大学における法人文書の管理に関する規程（以下、「文書管理規程」という。）」の別表 「法人文書分類基準表」に従って、管理運営、人事、会計、施設、研究協力・国際交流、保健管理、図書館に分類し、当該情報を所掌する事務本部の部署において格付け標準の原案を作成した。「法人文書分類基準表」を表２に抜粋する。

表２ 法人文書分類基準表（抜粋）

所掌	文書の類型	保存期間
管理運営	法人登記に関するもの	永久
管理運営	訴訟に関するもの	30 年
人事	人事記録・附属書類	永久
会計	国立大学法人に定める財務諸表等	永久
保健管理	学生の健康診断票	5 年

2.4 取扱制限の標準の作成

格付け基準の取扱制限の種類という項で、機密性、完全性、可用性ごとの取扱制限の種類と指定方法について定義している。例えば、機密性の複製という取扱制限の指定方法としては、複製禁止、複製要許可と定義している。これらの取扱制限の種類のそれぞれについて、どのように取り扱うべきかを検討し、機密性、完全性、可用性を格付け基準の別表として標準を示した。機密性についての格付けに応じた取扱制限の標準を表３に抜粋する。

格付け基準の機密性についての取扱制限で、参照者の制限については「○○限り」という指定方法が定義されていた。このような定義では、「担当者限り」と「関係者限り」など、格付けを行う者によって指定が様々であった。これを統一するため、「担当者限り」は、「情報を直接扱う者」と定め、「関係者限り」は「担当者を含めた関係する委員会の委員等」とするなど、機密性の取扱制限において指定しやすいように定義を作成し、格付け基準の別表として標準を示した。

表３ 機密性についての格付けに応じた取扱制限の標準（抜粋）

取扱制限	機密性 3 情報	機密性 2 情報	機密性 1 情報
複製	要許可	指定なし	指定なし
暗号化	必須	通信時必須、保存時推奨	指定なし
印刷	要許可	指定なし	指定なし
参照者制限	担当者限り	関係者限り	指定なし

2.5 学生情報の格付け標準の作成

本学は部局自治の文化が根付いており、学生に関する情報についても部局が保有し、管理している。このため、学生に関する情報も部局独自のものが多数あり、学生情報の格付けを行うに当たっては、部局に調査を行う必要があった。

全部局に対し、どのような情報があるのか、またどのような格付けと取扱制限を設けているかの調査を実施した。調査結果から本学が保有する学生情報の一覧および格付けと取扱制限の標準を作成し、格付け基準の別表として標準を示した。

2.6 法人文書分類基準表からの格付け標準の作成

学生情報以外の情報については、事務本部により所掌されており、法人文書分類基準表により約550 種類の文書に分類されている。

したがって、法人文書分類基準表の分類ごとに、京都大学本部事務分掌規程から担当部署を割り当て、担当部署に対して当該分類の情報の格付けと取扱制限の標準の原案作成を依頼した。これらを取りまとめ、格付け基準の別表として標準を示した。表２で示した文書について格付け基準の別表から抜粋して表４に示す。

表４　標準的な格付け基準（抜粋）

分類	情報名	格付け 機密性 完全性 可用性	取扱制限
管理運営	法人登記に関するもの	2	
		2	書換禁止
		2	
管理運営	訴訟に関するもの	3	
		2	書換禁止
		2	
人事	人事記録・附属書類	2	
		2	書換禁止
		2	
会計	国立大学法人に定める財務諸表等	2	
		2	書換禁止
		2	
保健管理	学生の健康診断票	3	複製禁止、転送・転記要許可
		2	
		2	

3 スタートガイドの作成

3.1 実施手順についての課題

前章では、スタンダードのレベルで、格付け基準に別表を加えて具体的な標準を示すという取り組みについて述べた。別表を参考にすることで、情報格付けを行うことが容易になったが、利用者が実際に運用を行うには実施手順書の整備が課題となっていた。

2018 年度の国立大学法人等情報化発表会における『九州大学における「情報格付け及び取扱い手順の手引き」の作成事例について』[3]という発表を参考に、本学でも実施手順書の作成に取り組んだ。

3.2 スタートガイドの基本方針

冒頭でも述べたように、本学における構成員の IT 知識や IT スキルは様々である。IT の専門家ではない一般的な構成員にとっては、新しい専門用語を覚え、その言葉の意味を正確に理解し、使い分けができるようになるには相当な労力が必要となる。IT が苦手な構成員にも受け入れられるよう、出来る限り簡潔に説明することが最も重要なことであると考えた。

機密性、完全性、可用性は重要な概念ではあるが、情報改ざんに関係が深い完全性、サービス不能攻撃に関係が深い可用性は、IT に馴染みがないとイメージし難く理解が難しいと考えた。一方で、機密性は情報へのアクセス許可という情報セキュリティとして一般的にイメージするものである。また、情報セキュリティ上も機密性についての取扱制限が最も重要な要素である。以上のことから 3 要素の中から機密性に対象を絞ったスタートガイドを作成することで、より多くの構成員に理解しやすい実施手順となると考えた。

3.3 スタートガイドの作成

図表やアイコンを使用して視覚的にわかりやすくなるよう PowerPoint で作成した。サンプルとして抜粋したページを図 3 に示す。すぐに実践できるように情報格付けから、格付けの明示までの手順を具体例で説明した。全体は 20 ページで、タイトル、目次を除くと 15 ページという簡潔な内容にまとめた。

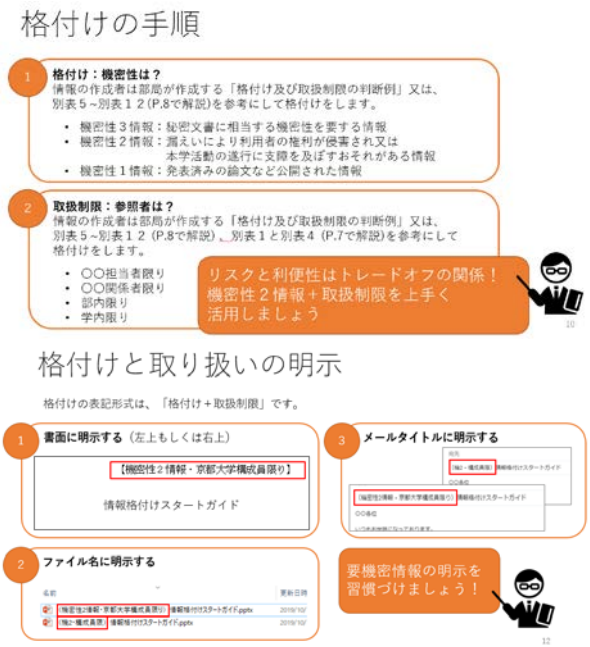

図３　スタートガイドの例

スタートガイドは 3 章構成になっており、各章のタイトルは下記の通りである。

- 第 1 章　情報格付けって何？
- 第 2 章　情報格付けの手順について
- 第 3 章　情報の取り扱い方について

第 1 章では、格付けの対象となる情報、格付けを行う目的、格付け基準の機密性に関する説明、

格付け基準の別表のうち機密性に関するものを掲載して、4 ページにまとめて解説している。

第 2 章では、格付けの手順を図 3 に示すとおり 2 ステップで説明し、あわせて具体例も示している。格付けと取扱いの明示の解説も含めて、3 ページで解説している。

第 3 章では、格付けと取扱いの継承と変更、情報の複製、印刷、再利用、暗号化、送付、配付、保存、廃棄を 6 ページで解説している。

スタートガイドに関する目的と対象を記載した「はじめに」、まとめを記載した「おわりに」がそれぞれ 1 ページとなっている。

スタートガイドの作成にあたって苦労をした点は、苦手な人に配慮して文字数を少なくし、読みやすくするという方針で、アイコンを効果的に利用しつつ、なるべく少ない文字数で説明することであった。2019 年の 5 月末に原案を作成したが、推敲を行って初版が完成したのは 2019 年 11 月となった。この間、プロジェクトに関わるメンバー以外にもたくさんの人から意見をもらうことで、試行錯誤を繰り返し、理解し、活用してもらうために必要最低限の説明を付加するよう心掛けた。

3.4 スタートガイドの公開と周知活動

スタートガイドは 2019 年 12 月 4 日に本学の情報環境機構 Web サイトにて学内公開を開始し、同日、情報セキュリティ実施責任者から部局情報セキュリティ責任者へ情報セキュリティ連絡網を使用して全学へ通知を行った。

2020 年 2 月に開催された全学情報セキュリティ委員会をはじめ、全学情報セキュリティ技術連絡会、新規採用者研修の中で情報格付けの重要性とスタートガイドについて説明している。また、全構成員に毎年受講を義務付けており、昨年は教職員で 94%の受講率である情報セキュリティ e-Learning でもスタートガイドの紹介を行っている。

4 おわりに

本学では 2013 年から 5 年以上に渡って、情報格付けに関するスタンダードとプロシージャーの整備を行ってきた。スタンダードにあたる格付け基準に、情報格付けに応じた取扱制限の具体例を示すため、4 つの別表を追加した。また、大学で取り扱う情報種別に対する具体的な情報格付けについて 8 つの別表を追加した。プロシージャーにあたる情報格付けスタートガイドは優先度が最も高い機密性に絞って説明することで、IT に苦手意識がある構成員でも受け入れやすいものになったと考えている。

情報セキュリティにおいて、規程の整備は大切なことであるが、実際に PDCA サイクルをまわして運用していくことも忘れてはならない。新規採用者研修、情報セキュリティ e-Learning などを通して構成員への教育を行い、情報セキュリティ監査で運用実施状況を確認し、更なる改善に取り組む所存である。

参考文献

[1] 独立行政法人情報処理推進機構、情報セキュリティ教本　改訂版、2009

[2] 国立情報学研究所、高等教育機関の情報セキュリティ対策のためのサンプル規程集（2019 年度版）

[3] 山本保文、九州大学における「情報格付け及び取扱い手順の手引き」の作成事例について、国立大学法人等情報化発表会、2018