Vol.2019-IOT-44 No.14
2019/3/7

九州大学における要機密情報の保護方法に関する一考察

嶋吉 隆夫[1,a)]　久志 昇[2]　笠原 義晃[1]　藤村 直美[1]

概要：九州大学では組織的に取り扱う情報に対して機密性の格付けを指定することが規定されたが，電子化された情報を取り扱う際に職員が実施すべき具体的な手順は明示されていなかった．そこで，機密性を要する情報を電子的に保存，授受する際に保護する方法について検討を行い，職員が従うべき規則を制定した．本稿では検討の内容と取り決めた規則について報告する．保護方法は，九州大学において実現可能かつ実務的に運用可能であることを前提に，機密性保持を確保する中で業務効率について最大限に配慮し，技術的手段だけで漏洩を防止するのではなく，一部のリスクは受容し，ルールとして予防することも含めて検討した．検討の結果，電子化された機密性を要する情報を保存，授受する方法，および，その際に用いる暗号化の方法やパスワードの扱いなどについて，規則を定めた．さらに本稿では，検討の中で明らかとなった今後解決が期待される技術的な課題についても報告する．

A Study on Confidential Information Protection in Kyushu University

1. はじめに

九州大学では 2016 年度に，「九州大学が保有する情報の格付け及び取扱制限に関する規程」[1] が制定され，職員等が組織的に取り扱う情報に格付けを指定することが規定された．併せて情報の取扱い手順に関する要項が定められたが，機密性を要する情報（要機密情報）を電子的に保存，送信する際の方法については，最高情報セキュリティ責任者 (CISO) が別に指定することとなっており，要項では規定されていなかった．一方，2018 年度から上記要項を事務組織に対して適用する計画となっており，職員が実施可能な機密性を確保するための具体的な方法について取り決める必要があった．そこで，CISO の諮問組織として 2017 年 6 月より「要機密情報の保護方法検討ワーキンググループ」（以下，WG）を立ち上げ，学内規則案を作成することとなった．本 WG では，要機密情報を電子的に保存，送信する方法について，九州大学において 2018 年度当初から実現可能，実行可能，運用可能であることを前提として具体的方法を検討した．本 WG が作成した案に基づいて，2017 年 12 月に九州大学 CISO 裁定「要機密情報の保存、送信等における保護方法について」が定められた．

本稿では，WG で規則案を作成する際に検討した内容，および，検討の中で明らかとなった今後解決が期待される課題について報告する．第 2 章では検討の前提である九州大学における情報の格付けについて説明する．第 3 章では本 WG で検討した要機密情報の保護に関する規則の設計について述べ，第 4 章では規則で採用した具体的な保護方法について記す．最後に第 5 章で，解決が期待される技術的課題について述べる．

2. 情報の格付け

九州大学では，組織的に取り扱う情報について機密性 (C: Confidentiality)，完全性 (I: Integrity)，可用性 (A: Availability) の格付けを指定するものと規定されている [1]．ここで，機密性は 3 段階，完全性，可用性は 2 段階に区分される．

機密性 3 情報の分類の基準は，以下の通りに定められている．

秘密文書に相当する機密性を要する情報

ここで秘密文書とは，文書処理に関する規程 [2] において，以下の通りに極秘と秘に区分されて定められているものをいう．

極秘　秘密の保護が高度に必要であって，当該秘密の漏えいが国及び本学の安全又は利益に対し，

[1] 九州大学情報基盤研究開発センター
Research Institute for Information Technology, Kyushu University
[2] 九州大学情報統括本部
Information Infrastructure Initiative, Kyushu University
[a)] simayosi@cc.kyushu-u.ac.jp

重大な損害を与えるおそれのある事項が記載されているもの

秘　極秘に次ぐ程度の秘密の保護が必要であって，関係者以外に知らせてはならない事項が記載されている文書

機密性 2 情報の分類の基準は，以下の通りに定められている．

独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号）第 5 条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって，「機密性 3 情報」以外の情報

機密性 1 情報は，機密性 2 または 3 以外の情報である．また，機密性 3 情報及び機密性 2 情報を要機密情報という．

機密性 3 情報は，非常に限定された情報に対してだけ指定することが想定される．一方，機密性 2 情報は，学外に開示しない情報全般であり，個人情報などの重要情報から，漏えいによる影響が限定的な情報まで，広範な情報が該当する．なお，個人情報の管理については別に規程 [3] が定められている．

3. 設計

3.1 方針

WG では電子化された要機密情報の漏洩への対策について検討した．ただし，検討では情報の完全性と可用性についても考慮した．また，操作ミスや紛失といった過失による漏洩，不正使用や不正開示といった故意による漏洩，サイバー攻撃による漏洩を考慮して検討を行った．

情報セキュリティにおいて，セキュリティと使用性 (usability) はトレードオフの関係にあり，セキュリティと使用性のバランスが重要であってセキュリティを厳しくしすぎることは良いことではないと考えられている [4]．使用性の低下は業務効率を落とすだけでなく，制限の回避やルール違反の常態化などのリスクを増大させる．そこで，必要なレベルの機密性保持を確保する中で使用性に最大限配慮する方針で検討を行った．

あらゆる事態に情報漏洩を防ぐ対策を行うことは，非常に厳しいセキュリティを要求することであり，使用性を著しく低下させる．そこで，高い権限を持つ者による故意の漏洩や，事前想定が困難である高度な標的型サイバー攻撃による漏洩など，一部のリスクについては本 WG の検討では受容し，本 WG 外の対策に委ねることとした．

また，セキュリティ確保を技術的に担保して漏洩対策を行うことは，実現性および経済性の面で困難がある．そこで，技術的手段だけでなくルールとして予防することを含めて漏洩対策を検討した．

3.2 情報の保存

3.2.1 保存された情報の保護方法

組織的に取り扱う電子化された要機密情報は基本的に計算機の記憶媒体に保存される．そこで，計算機に保存される要機密情報の保護方法について考える．

電子的に保存された情報の保護について，アクセス制限と暗号化は区別して考えなければならない．アクセス制限は情報へのアクセスに権限を要求することで保護する方法であり，暗号化は電子データだけから意味のある情報を抽出することを防止する方法である．アクセス制限だけでは，システムを介さない直接アクセスや，アクセス制限のない場所への電子データのコピーといった，制限回避や制限解除などの行為よる情報漏洩は防止できない．一方，暗号化だけでは，暗号化データ自体へのアクセスは防止できず，攻撃者に暗号解読の機会を与える．それゆえ，機密性に応じて適切にアクセス制御と暗号化を組み合わせる必要がある．

機密性 3 情報は特に厳重に漏洩対策を施さねばならず，アクセス制限と暗号化の両方で保護する必要がある．さらに，不正アクセスなどのリスクに備えるために，記録媒体上では必ず暗号化された状態で記録されなければならず，平文の状態で記録媒体上に記憶されることは禁止しなければならない．機密性 2 情報については，情報を取り扱う権限を持たない者によるアクセスを防ぐために，アクセス制限による保護は必須とする．暗号化については，軽微な情報に対して必須とすれば利便性が損なわれることから，情報の重要度に応じて必要であれば暗号化を行うこととする．

3.2.2 アクセス制限

情報の保護に用いるアクセス制限は，ファイルシステムやアプリケーションソフトウェアなどによる電子的なものだけには限定しない．適切に鍵管理された部屋に入室しなければ電子化情報にアクセスできないといった物理的な方法も許容する．

3.2.3 暗号化

容易に解読可能な暗号方式を用いた暗号化は，事実上暗号化していないのに等しく，許容できない．十分な強度を持つ暗号方式の利用に限定する必要がある．

電子ファイルを暗号化する手段についても考慮が必要である．ファイルの暗号化および復号の処理形式は大きく 2 種類に分類できる．その分類と本稿での呼称を以下に示す．

- アーカイバ形式
  パスワード付き ZIP ファイルのような，情報が平文で格納されたファイルを収蔵する暗号化されたファイルを作成し，平文の情報を読み書きするために暗号化ファイルを復号して元のファイルを取り出す形式
- ビルトイン形式
  暗号化された PDF (Portable Document Format) ファイルのように，情報が暗号化されて格納されたファイ

ルを読み出し，保存する際にアプリケーションソフトウェア内部で復号および暗号化処理を行う形式

ビルトイン形式の暗号化は，閲覧や編集の際に平文の情報が記録媒体上に保存されないという点で，アーカイバ形式よりも優れている．

機密性 3 情報については，前記の通り，平文の状態で記録媒体上に記録されることは禁止する必要があることから，アーカイバ形式の使用は禁止する．機密性 2 情報についても，アーカイバ形式よりもビルトイン形式を利用することが望ましいが，利便性を考慮してアーカイバ形式も許容することとする．

3.3 情報の授受

3.3.1 電子化された情報の授受方法

組織的に取り扱う要機密情報は，関係者間で共有や受け渡しが行われることが多い．ファイルサーバなどの同じ記憶装置上の実体を共有できる場合は，情報の授受について特段の考慮は必要ない．しかし，組織間や学内外で情報を授受する場合は，同じ実体を共有できないことがほとんどであり，電子データの複製を伴う情報の授受が必要である．そこで，そのような場合に，電子化された要機密情報を安全に授受する方法について考える．

3.3.2 可搬型の記憶装置

情報を授受するときに，USB ストレージやディスクメディアなどの可搬型の記憶装置や媒体に情報を記録し，それを物理的に受け渡す方法がある．しかし，可搬型の記憶装置，媒体は紛失や盗難などの物理的なインシデントのリスクがあり，その利用は推奨できない．利用する場合には十分に保護策を講じる必要がある．

物理的なインシデントが発生した際に情報が漏洩するリスクを削減するために，格納される電子データは必ず暗号化されていなければならない．これは格納する個々のファイルを暗号化することだけでも実現できるが，運用上で暗号化を確実にする目的，および，ファイル名などのメタデータへのアクセスも防止する目的から，媒体全体を暗号化する機能を備えた記録装置の使用に限定し，要機密情報の格納に先だって暗号化機能を有効化しておくべきこととする．

記録装置に保存された情報は一般的に，受け取った側で計算機の内部記録装置に複製して使用される．複製先からの漏洩に備える目的で，要機密情報は暗号化した電子データを可搬型の記憶装置に格納することとする．

記憶装置を物理的に授受する手段としては，物理的な漏洩への対策として，直接受け渡すか，配送の状態及び配達されたことを確認できる機能をもった配送方法により送付し，提供先が受け取ったことを確認することとする．

3.3.3 ネットワークを介した送受信

組織間や学内外で情報を受け渡すとき，計算機ネットワークを介して電子データを送受信する方法が広く用いられる．計算機ネットワーク上で要機密情報を送受信するとき，通信の盗聴に備えて，送信元から送信先に到るまでエンド・ツー・エンドで情報が暗号化されている必要がある．TLS (Transport Layer Security) 等による暗号化通信を用いるか，通信が暗号化されない場合は情報を暗号化した電子データを送信しなければならない．

3.3.4 電子メールによる送信

計算機ネットワークを用いて情報を送信する手段として，現時点で最も一般的なものの一つが電子メールである．しかし電子メールは，TLS を用いた SMTPS や IMAPS などを使用したとしても，メールサーバにおいて電子メールメッセージがスプールやメールボックスに暗号化されずに保存される．それゆえ，要機密情報を暗号化せずにメールメッセージに含めることは認められない．また，電子メールには送信先の指定を誤るなどのリスクがある．これらのことから，電子メールを用いた要機密情報の送信は推奨できない．

他大学にて電子メールへの添付ファイルを全面禁止している例があることや，技術的にメールサーバやファイアウォールにおいて添付ファイル付きメールの受信を拒否することが可能であることから，添付ファイルによる要機密情報の送信を禁止すべきではないかとの議論もあった．しかし，使用性の観点から，暗号化されたファイルを添付する場合に限りメールでの送信を許容する．なお，送信先を間違えるリスクがあることから，意図する送信先が組織内であるか学外であるかといった区別によらず同一の規則を課す必要がある．さらに，誤送信の対策として，送信先にメールの受領を確認することを義務付ける．ただし，機密性 3 情報については，誤送信や転送などによる情報漏洩のリスクを重視して，電子メールでの送信を禁止する．

3.3.5 オンラインシステムを用いた授受

計算機ネットワークを介して情報を送受信する方法として，オンラインストレージなどのオンラインシステムを用いる方法がある．しかし，任意のオンラインシステムで情報セキュリティが保証されるわけではないことから，利用を許可するオンラインシステムは，第三者のアクセスを制限でき，通信経路が暗号化されているもので，機密性の保証が確認できるものを明示的に指定する必要がある．

九州大学では以前から，ノースグリッド社のオンラインストレージシステム Proself[*1] を用いたサービスを全学に提供している [5]．Proself はアクセス制限や通信の暗号化の条件を満たす．また，ファイルのダウンロード回数も制限でき，ファイルダウンロードのログも記録されるのに加えて，ファイルがダウンロードされるとファイルをアップロードした利用者へと電子メールで通知する機能を有する．

[*1] https://www.proself.jp

表 1 要機密情報を含む情報の授受方法
Table 1 Methods for Sensitive File Transmission

区分	Proself	メール添付	可搬型記憶装置
機密性 3 情報	◎	×	△
機密性 2 情報	◎	△	△

さらに，学内にオンプレミスのシステムとして構築されており保存データの機密性も保証される．そこで，要機密情報の送受信に用いるオンラインシステムとして Proself を指定する．

3.3.6 使用する情報の授受方法

表 1 に要機密情報を含むファイルを送受信する方法をまとめる．要機密情報は原則的に Proself を用いて送受信することとする．使用性を考慮して，電子メールへの添付による送信や可搬型の記憶装置による授受も，上述の制約を課した上で許容する．

3.4 パスワード

個人認証や共通鍵暗号方式の鍵生成などの手段として広くパスワードが用いられる．個人認証に用いるパスワードは他者に開示しないことが原則である．また，一個人として情報の暗号化に用いるパスワードは他者に開示する必要はない．しかし，組織的に取り扱う情報の場合，時間軸も含めて考えれば，他者と情報を共有することが基本であり，要機密情報の保護にパスワードを用いる場合は，そのパスワードは複数人で共有することを前提に考えなければならない．要機密情報の保護に用いるパスワードは，それが漏洩した場合には要機密情報の漏洩に繋がることから，パスワードが保護する情報の機密性と同様の保護策を講じる必要がある．なお，パスワードの共有には漏洩のリスクがあることから，要機密情報の暗号化や授受においてパスワードの共有を必要としない方法を優先する．

オンラインシステムで用いるパスワードと，ファイルの暗号化などのようにオフライン状態で利用できるパスワードは，区別して考える必要がある．オンラインシステムではパスワード試行の回数や間隔を制限できるが，オフライン状態で利用できるパスワードは，高頻度や並列化した大量の試行が可能であり，辞書攻撃や総当たり攻撃などのパスワードクラック手法に対して十分な強固さを持つ必要がある．パスワードの強度はパスワードクラックへの耐性に直結することから，パスワード強度を確保するためにパスワードポリシーの指定が必要である．

4. 具体的保護方法

4.1 Information Rights Management

不正アクセスから機密情報を保護する技術として Information Rights Management (IRM) （e-DRM: Enterprise Digital Rights Management とも呼ばれる）がある．IRM は一般的に，認証された利用者に対して認可されたアクセス権限（閲覧，変更，複製など）の操作だけを許可する方法として用いられ，不認可アクセスを防止するために電子データは暗号化されて，復号にはオンライン認証が必要である．IRM は，ファイルやディレクトリへのアクセス権限とは異なり，暗号化と個人認証によりコンテンツに対する権限を管理するので，たとえ IRM を適用したファイルにアクセスできたとしてもコンテンツにはアクセスできない．それゆえ，電子データが外部に流出したとしても情報漏洩を防止できる．また，パスワードによる暗号化とは異なり，複数の利用者間で情報を共有する際にもパスワードを共有する必要がなく，また，オンライン認証を用いるのでパスワード試行攻撃への耐性が高いという利点がある．

IRM 技術を使った Microsoft のサービスとして，オンプレミスの Active Directory (AD) を認証に用いる AD Rights Management Services (RMS)，および，Microsoft のクラウドサービス Office 365 で用いられる Azure AD を認証に用いる Azure RMS がある．Microsoft Office には標準で RMS 機能が統合されており，Office 文書に対して，閲覧，内容コピー，印刷，変更の権限を AD アカウント別に制限できる．Azure RMS では，アクセス制限の対象者として Office 365 アカウントを指定する．九州大学では Office 365 を全学認証基盤と連携してサービス提供 [6] しており，Azure RMS が利用可能である．また，学外者についても，Office 365 アカウントを所持しているか，または，無償で誰でも取得できる個人用 Azure RMS アカウントを所持していれば，そのアカウントを指定してアクセス権限の設定が可能である．

Microsoft Office アプリケーションにおける Azure RMS によるアクセス制限では，Azure AD 管理者が用意するテンプレートが利用できる．しかし，テンプレートとして部課のような組織単位のものを用意すると，対象数が多くなりすぎることから，運用上の問題がある．そこで，本学のすべての構成員（教職員，学生），すべての教職員などのテンプレートを提供し，学外への情報漏洩を防止することとした．ただし，特定の者だけが閲覧して良い重要な機密性 2 情報および機密性 3 情報は，個別にアカウントを指定して権限を制限すべきとした．

4.2 暗号化の方法

ファイルや記憶装置の暗号化は，オフラインでの暗号解読が可能であり，GPU やクラウド計算資源を用いるなどすれば並列に暗号解読できる．ファイルや記憶装置を暗号化するときに用いるパスワードは，総当たり攻撃への耐性を高めるために，オンラインアカウントのパスワードなどよりも，十分に複雑である必要がある．そこで，12 文字以上，かつ，英大文字，英小文字，数字，半角記号の 4 種類を全てを少なくとも 1 文字以上含めるパスワードを設定す

ることとした．

弱い暗号方式を用いた暗号化は総当たり攻撃でも短時間で解読でき，十分に強固な暗号化を行う必要がある．また，以前に普及していた暗号方式の一つである RC4 は複数の脆弱性が知られており [7]，その使用は危険である．Office 2003 以前のファイル形式では暗号化に RC4 を用いており脆弱であるので，使用を禁止する．Office 2007 以降の Office Open XML 形式の暗号化 [8] では，既定の暗号方式は 128 ビット AES (Advanced Encryption Standard) であり鍵ストレッチングも行われることから，現時点では十分に強固だと考えられる．PDF のパスワードを用いる暗号化 [9] において，Acrobat 6.0 で用いられる PDF 1.6 以前の形式では暗号方式に RC4 を用いており脆弱であるから，使用を禁止する．Acrobat 7.0 以降が対応する PDF 1.7 では，暗号方式に 128 ビット AES が用いられ鍵ストレッチングも行われることから，現時点では十分に強固だと考えられる．

標準的なパスワード付き ZIP ファイルで用いられる ZipCrypto と一般的に呼ばれる暗号方式は非常に脆弱であり [10]，10 桁以下のパスワードでは短時間で解読が可能である．なお，暗号方式に AES を用いる ZIP ファイルの暗号化に対応したソフトウェアも存在するが，Microsoft Windows の OS 搭載機能では解凍できない．また，標準的なパスワード付き ZIP ファイルの暗号化の対象はファイル内容だけであり，ファイル名は暗号化されない．これらのことから，標準的なパスワード付き ZIP による暗号化は脆弱であり決して推奨できない．しかしながら，標準的なパスワード付き ZIP ファイルと同程度かそれ以上に多くの環境で復号できるファイル暗号化の手段は現時点では存在せず，その利用を全面的に禁止することは，使用性の観点から不都合がある．そこで，暗号方式の強度が弱いことからパスワードの強度に十分に注意する必要があることを明記した上で，パスワード付き ZIP ファイルの利用を許容することとした．ただし，可能な限りビルトイン形式の暗号化を利用することとしている．

4.3 Proself による送受信の方法

4.3.1 Proself の送受信機能

Proself にはファイルを送受信する手段として，Web 公開，共有フォルダ，受信フォルダの機能がある．Web 公開は，Proself に保存したファイルまたはフォルダについて，Proself のアカウントを用いないウェブアクセスによるダウンロードを可能にする機能である．共有フォルダは，Proself 上のフォルダについて，別のアカウントからのアクセスを可能にする機能である．受取フォルダは，Proself 上のフォルダに対する，Proself のアカウントを用いないウェブアクセスによるファイルのアップロードを可能にする機能である．

4.3.2 共有フォルダ

共有フォルダ機能を用いれば，Proself 上のアカウントを限定してファイルを受け渡しでき，また，各自のアカウントでアクセスすることからパスワードを共有する必要がない．このことから，ファイルを送信する相手が学内者だけの場合は，最優先の方法として共有フォルダ機能を利用することを推奨する．

共有フォルダの共有先には複数のアカウントを指定できる．学内グループでのファイル共有などの場面で有効だと考えられるが，グループ構成員が変更になった際などに共有設定を見直すことを規則に指定する．また，情報を共有する必要のないアカウントとも共有されているフォルダを流用してファイルを受け渡すことは規則により禁止する．

4.3.3 受取フォルダ

受取フォルダ機能では，アップロードされたファイルに，受取フォルダを設定したアカウント以外では，そのファイルをアップロードした利用者も含めて一切アクセスできない．また，ファイルのアップロード画面において，受取フォルダにアップロードされているファイルの一覧を非表示に設定可能である．それゆえ，授受される要機密情報の漏洩に対する耐性は高い．このことから，学内の者がファイルを受け取る場合は，受取フォルダ機能の利用を推奨する．ただし，複数の相手にファイルを共有したい場面では効果的な方法ではない．

機密性 3 情報を受け取る際には，1 回ごとに受取フォルダを作成すること，公開期限とアップロード回数制限を指定すること，アップロードファイル非表示を設定することを義務付ける．なお，受取フォルダを設定する際にアップロード画面へのアクセスに対してパスワードを設定できるが，意図しないアップロードを防ぐ効果はあるものの機密性の向上には寄与しないことから，公開パスワードの設定は任意とする．ただし，受取フォルダへアクセスする URL が漏洩した場合には，マルウェアが混入したファイルがアップロードされるリスクも考えられるので注意を要する．

4.3.4 Web 公開

Web 公開機能では，ウェブアクセスに対するパスワード（公開パスワード）を設定できる．ただし，ファイルの送信相手に対して，ウェブアクセスに用いる URL（公開 URL）に加えて，公開パスワードを何らかの手段で伝える必要がある．公開 URL はランダムに生成されることから，公開パスワードを設定しなくともある程度のセキュリティは認められる．しかし，公開 URL は第三者への伝達や通信盗聴などで漏洩するリスクがあることに注意が必要である．

Proself には公開パスワードとは独立して，メール認証という機能がある．メール認証機能では，ダウンロード時にまずメールアドレスの入力が求められ，入力したメールアドレスへと送付される 1 時間有効のワンタイムパスワードにより認証を行う．また，入力されたメールアドレスは

Web 公開を設定した利用者に通知されることから，誰がダウンロードしたかを把握できるという利点もある．ただし，ダウンロードを行う利用者のメールが盗聴されている場合にはファイルの不正ダウンロードを完全に防ぐことはできない．メール認証機能では，公開先メールアドレスを指定できる．指定しなかった場合は任意のメールアドレスでワンタイムパスワードを取得できるが，指定した場合は指定外のメールアドレスを入力してもワンタイムパスワードを取得できない．メール認証機能を用いる場合は基本的に公開先メールアドレスを指定すべきであるが，漏洩の影響が軽微な情報を多数の相手に送信する場合などの使用性に考慮して，公開先メールアドレスを制限しない方法も許容することとする．公開パスワードとメール認証は，両方を同時に指定でき，その場合は公開パスワードとワンタイムパスワードの両方が必要である．

これらのことから，機密性 3 情報を Web 公開する場合は，公開パスワードを付けることを義務づける．また，メール認証を用いることでダウンロードした者のメールアドレスが把握できることから，メール認証の利用も推奨する．さらに，機密性 3 情報は一対一で送信することを前提とし，不正なダウンロードを防ぐ目的で，公開制限を翌日まで，ダウンロード回数制限を 1 回に設定することを義務づける．機密性 2 情報については，公開するファイルが暗号化されている場合は，公開パスワードを設定しなくとも良いものとする．そうでない場合は，公開パスワードかメール認証のいずれか一方を必ず利用する規則とする．また，機密性 2 情報は多数に送信する場面も多いことから，公開制限やダウンロード回数制限の設定値は指定しないが，事情に応じて適切に設定することとする．

4.4 パスワード共有の方法

IRM 技術が利用できる場合は，ファイルの共有や授受においてパスワードを共有する必要はない．しかし現時点では，Office 文書ファイル以外の暗号化や，学外者とのファイル受け渡しなどで IRM 技術が利用できない場面があり，ファイル暗号化に用いるパスワードや Proself の Web 公開の公開パスワードなどを共有または伝達する必要が生じる．そこで，パスワードを共有，伝達する方法について考える．

現時点では，パスワードは口頭で伝えるのが最良の方法だと考えられる．要機密情報の授受に先だって事前にパスワードを取り決めておくといった方法が考えられる．必要に応じてパスワードを連絡する場合は電話などによる口頭での伝達が望ましい．しかし，業務において対話ではなく非同期にパスワードを伝えなければならない場面などが現実に存在することから，電子的にパスワードを伝達できる必要がある．

日本では，パスワードを用いて暗号化されたファイルを添付したメールや，アクセスにパスワードを必要とする URL を記載したメールを送信した後に，そのパスワードを別のメールに記載して送信する方法が広く用いられているが，これは非常に危険である．添付ファイル付きメールや URL が記載されたメールだけが第三者に渡るという場面は想定しづらく，メールが盗聴されている場合や不正アクセスされた場合には両方のメールを攻撃者が入手できると想定されることから，上述の方法は機密性保護の面でパスワードを設定していない場合とセキュリティが同等である．さらに，機密性が確保されないということ以上に，上述の方法でセキュリティが確保されると誤解されていることが危険である．そこで，いかなる場合においても電子メールで平文のパスワードを送信することを禁止する．これには，共通鍵暗号方式による暗号化に用いたパスワード，および，Proself の公開パスワードが含まれる．

現時点では，RMS によるアクセス制限を設定した Office ファイルにパスワードを記録して授受する方法が，現実的かつ安全な方法だと考えられる．しかし，パスワードの共有相手が RMS を利用できない場合も想定される．本来であればパスワードを平文でファイルに記録することは許容できないが，実現可能な適当な代替方法が存在しないことから，パスワードを保存したテキストファイル等を Proself で受け渡す方法を暫定的に認めることとする．ただし，Proself の公開パスワードをさらに Web 公開で送信することはセキュリティ上意味を成さないことから，明示的に禁止する．

業務上では要機密情報を含んだ多くのファイルを共有することが想定される．そのような場合に，全てのファイルに手動で別個のパスワードを設定して管理することは非現実的であるので，複数のファイルに共通のパスワードを設定することを許容せざるを得ない．ただし，共通のパスワードを知っている者は，同じパスワードが設定された全ての要機密情報を取得できうることに留意しなければならない．パスワードを計算機上に保存するときは必ず暗号化する必要がある．なお，RMS で個別指定の適切なアクセス制限をかけた Office ファイルに保存すれば，特定の複数人でパスワードを共有することも可能である．

5. 解決が期待される技術的課題

5.1 パスワードの管理・伝達

現時点では，パスワードを安全かつ効率的に管理および伝達する電子的手段として推奨できる選択肢が見当たらない．前述の通り，業務上では要機密情報を含んだ多くのファイルを共有する必要がある．組織単位などで共通のパスワードを用いるといった運用方法も考えられるが，組織構成員が変更になった際などには，以前の構成員による情報アクセスを回避するために，共通のパスワードの変更が必要になる．しかし，共通のパスワードを設定した全てのファイルに対してパスワードを変更することは現実的では

ない．

パスワードを伝達する手段として携帯電話のショートメッセージサービス (SMS) を利用する方法も考えられるが，個人の携帯電話を利用する必要があり私費負担が発生する，SMS を利用できない構成員も存在するといった問題があることから，推奨方法としては採用できない．クラウドサービスとして提供されるコミュニケーションツールやコラボレーションツールを利用する方法も考えられるが，安全性や適切な利用方法の検討，全学への配備，学外者の利用などの課題がある．

パスワードを管理するソフトウェアやオンラインサービスは多数存在しており，パスワードの共有機能を有するものもある．しかし，有償，無償によらず商用のオンラインサービスについては，機密性や可用性を確実に検証することが困難である．また，オンプレミスで利用できるシステムやソフトウェアは一般的に，全学的導入に必要なライセンス費用が高額であり，経済的な課題がある．パスワードを管理および共有できる，オンプレミスシステムに導入可能なオープンソースのソフトウェアや，信用できる公的な機関が運営するオンラインサービスなどの出現が期待される．

5.2 メールの暗号化

電子メールの本文と添付ファイルを含めたメッセージ全体を暗号化する方法には，標準化された方式として S/MIME があり，主要なメールクライアントソフトウェアで利用できる．しかし，S/MIME の実利用にはいくつか課題がある．

S/MIME を使って暗号化した電子メールを送信するためには，メール送信先の受信者が個人の電子証明書を取得している必要がある．学術機関に所属する者であれば国立情報学研究所による UPKI 電子証明書発行サービス[*2]を利用して個人の電子証明書を取得できるので，九州大学の構成員は全員が個人の電子証明書を取得することが可能である．しかし，実際に構成員が電子証明書を入手するためには，高い機密性を要する秘密鍵を含む証明書を構成員に安全に配布する必要があり，その方法が課題である．また，一般的には取得に費用を要することから個人の電子証明書を持たない者が大多数である．それゆえ，学外者と送受信する電子メールで利用することには，個人証明書の普及という課題がある．

S/MIME を用いて電子メールを暗号化するには，電子メールの送信者が送信先メールアドレスの証明書の公開鍵を知っている必要がある．メールクライアントソフトウェアでは一般的に受け取った公開鍵は以降の利用のために保存され登録されるが，そのためには S/MIME で署名された電子メールを一度受信しておく必要がある．また，ウェブメールで S/MIME を使うためには秘密鍵の扱いについて実用上の課題がある．さらに，電子証明書には有効期限があるが，過去のメールは失効した証明書を用いて暗号化されていることから，証明書の履歴を管理する必要がある．このように，S/MIME の実運用には，環境整備の面で解決が期待される様々な技術的課題がある．

5.3 Office 文書ファイル以外の IRM

Office 文書以外の形式のファイルについて，RMS によるアクセス制限を付加するツールを Microsoft が無料で配布している．しかし，このツールは元のファイルを収蔵する RMS 付きファイルを作成するアーカイバ形式のファイル暗号化であり，利用は推奨できない．

Office 文書ファイル以外で業務上特に利用頻度の高い形式は PDF ファイルである．上述した Microsoft の無償配布ツールでは，PDF ファイルに対して RMS によるアクセス制限が付加されたファイルを直接表示することもできる．しかし，一般の PDF リーダーソフトウェアと比べて利便性が限られている．また，Microsoft の RMS を用いたアクセス制限の機能を持つ PDF リーダー製品も存在するが，全学的に導入するにはライセンス費用面で課題がある．なお，有償製品である Adobe Acrobat には，暗号化と閲覧や印刷の制限などの文書の保護を電子証明書を用いて行う機能があり，復号や閲覧などは無償で配布されている Acrobat Reader で可能である．しかし，前述の S/MIME と同様に，制限を許可する対象者が個人証明書を持つ必要があり，文書を保護する者は対象者の証明書を受信者一覧に設定する必要があるという課題がある．

様々なファイル形式に対して IRM 技術を用いたアクセス制限を適用できる製品もいくつか存在している．しかし，調査した範囲内の製品においては，macOS での利用ができないか大幅に機能制限があった．九州大学では多くの macOS 端末が利用されており，macOS の対応が十分ではないシステムを導入することは難しい．また，それらの製品は高額であり，費用面での課題もある．将来的な IRM 技術のオープン化や標準化が期待される．

6. おわりに

本稿では，九州大学において電子化された要機密情報を保護する方法について検討した内容を報告し，また，そこで明らかとなった解決が期待される課題について述べた．本稿で述べた保護方法は 2018 年度から学内規則として運用されている．

現在の規則には今後改定を検討すべき課題も残されている．本学では前述の通り Office 365 を全学で導入しており，Office 365 に含まれるサービスとしてファイルの共有設定が可能なオンラインストレージサービスが利用できる

[*2] https://certs.nii.ac.jp

が，検討段階では安全性などについて十分に検討できていなかったことから，要機密情報の授受に利用可能なオンラインサービスとしては指定しなかった．今後 Office 365 の利用について検討する必要がある．その他のオンラインストレージ，インスタントメッセンジャー，コラボレーションツールなどのクラウドサービスの利用についても今後の検討課題である．ただし，個人向け無償サービスは一般的に機密性などの観点で業務利用には問題があることから，検討の対象外である．また，データベース等の情報システム内に要機密情報を保存する場合についても，不正アクセス対策やシステムへの侵入などを考慮した暗号化などの保護対策を行う必要がある．しかし，既存システムについて改修が必要になり費用と期間を要することから，具体的な暗号化方法などの指針については定めることができておらず，今後の検討課題である．

参考文献

[1] 九州大学：九州大学が保有する情報の格付け及び取扱制限に関する規程，平成 28 年度九大規程第 124 号 (2017).
[2] 九州大学：九州大学文書処理等規程，平成 16 年度九大規程第 30 号 (2004).
[3] 九州大学：九州大学個人情報管理規程，平成 16 年度九大規程第 160 号 (2005).
[4] Whitman, M. E. and Mattord, H. J.: *Principles of information security*, chapter 1. Introduction to Information Security, pp. 1–38, Cengage Learning (2011).
[5] 藤村直美，平山善一：ファイル共有システムの運用と利用状況について，研究報告インターネットと運用技術 (IOT)，Vol. 2011-IOT-12, No. 18, 情報処理学会，pp. 1–6 (2011).
[6] Kasahara, Y., Shimayoshi, T., Obana, M. and Fujimura, N.: Our Experience with Introducing Microsoft Office 365 in Kyushu University, *Proceedings of the 2017 ACM Annual Conference on SIGUCCS*, SIGUCCS '17, New York, NY, USA, ACM, pp. 109–112 (online), DOI: 10.1145/3123458.3123491 (2017).
[7] Popov, A.: Prohibiting RC4 Cipher Suites, RFC 7465, IETF (2015).
[8] Microsoft Corporation: Office Document Cryptography Structure Specification (2018).
[9] ISO/TC 171(ed.): *Document management – Portable document format – Part 1: PDF 1.7*, ISO 32000-1:2008, chapter 7.6 Encryption, International Organization for Standardization (2008).
[10] Biham, E. and Kocher, P. C.: A known plaintext attack on the PKZIP stream cipher, *International Workshop on Fast Software Encryption*, Springer, pp. 144–153 (1994).