「処分通知等のデジタル化に係る基本的な考え方」Q&A

全般

問1.　要機密情報に該当しない処分通知等において、発行元を証明したい場合や完全性を担保したい場合、処分通知等のデジタル化の最も簡易な方法はどのようなものがあるか。また、このときの留意事項は何か。

通知を受ける者からの問い合わせに対応できるよう、デジタル化された処分通知等に責任者・担当者の氏名や文書番号等を記載した上で、電子メールに添付して通知を受ける者に送信することが考えられる。

問2.　行政機関及び独立行政法人等から地方公共団体への処分通知等をデジタル化する場合、どのような手段で送信すればよいか。

本基本的な考え方で示した、個人や法人等に送信する方法と同様の方法が適用できる。なお、参考資料である「処分通知等のデジタル化に係る短期的手法例の検討フロー」においても具体的な検討手順及び手段を示しているため参照されたい。

問3.　書面の処分通知等で公印を押印している場合、デジタル化する際に電子署名の要否はどう判断すればよいか。また、公印に代えて電子署名を行う場合、行政機関等内部の行政文書取扱規則では、どのように規定することが考えられるか。

書面の処分通知等に公印を押印していた場合であっても、その処分通知等のデジタル化を行う際に機械的に電子署名に置き換えるのではなく、公印の根拠（法令上の規定の有無）や必要性（完全性の担保等）を踏まえた上で、法令上必要な場合や第三者による検証が想定される場合等、真に必要な場合に限って電子署名を利用することが考えられる。

また、公印に代えて電子署名を行う場合の行政文書取扱規則での記載として、次のように規定することが考えられるため、参照されたい。

（行政文書の施行）

第〇条 行政文書を施行する場合における公印（電子署名を含む。）又は契印の使用は、法令に定めのある場合その他の真に必要な場合に限るものとする。

２　前項の規定による公印を使用する場合には、原議を添えて、公印を管理する者から、浄書した施行文書に公印を受ける。

オンラインストレージ

問4.　オンラインストレージの導入を検討する場合、どのようなことに留意すればよいか。

「政府機関等の対策基準策定のためのガイドライン（令和３年度版）」（令和３年７月７日内閣官房内閣サイバーセキュリティセンター）（以下「統一基準ガイドライン」という。）において、「要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること」[1]とされており、その例として「機関等独自で運用するなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する」[2]ことが示されている。

また、クラウドサービスのウェブメールサービス又はオンラインストレージ環境を利用することも考えられるが、統一基準ガイドラインにおいて、「クラウドサービスのセキュリティ要件策定に当たっては、ISMAP 管理基準[3]の管理策基準が求める対策と同等以上の水準[4]を求めること」と示されている[5]。加えて、「要機密情報を取り扱わない場合においても、考慮すべきリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、利用の可否を判断する」[6]旨も示されている。

問5.　オンラインストレージ等又は PDF にパスワードをかける場合、どのようにして通知を受ける者（個人や法人等）にパスワードを通知すればよいか。

統一基準ガイドラインにおいて、パスワードの通知方法は「パスワードを暗号化された情報と同じ経路で送信したり、第三者が容易に知り得る方法[7]で送信したりしてしまうと、第三者によって情報が復号されるおそれが高くなることから、例えば、事前の面会時に共有しておいたり、事前に共有できない場合は暗号化された情報とは別の方法

---

[1] 統一基準ガイドラインの＜3.1.1(6)(b)関連＞3.1.1(6)-3 を参照。

[2] 統一基準ガイドラインの＜3.1.1(6)(b)関連＞3.1.1(6)-3 の e)を参照。

[3] 「ISMAP 管理基準」（令和２年６月３日 ISMAP 運営委員会）

[4] 統一基準ガイドライン＜4.2.1(2)(c)関連＞4.2.1(2)-1 の（解説）を参照。

「クラウドサービスのセキュリティ要件策定に当たっては、ISMAP 管理基準の管理策基準における統制目標（３桁の番号で表現される項目）及び末尾に B が付された詳細管理策（４桁の番号で表現される項目）を原則として全て満たす対策を含める必要があることに注意する。また、各機関等において定められた対策基準から求められる内容もすべて反映されるようにする必要がある。」

[5] 統一基準ガイドラインの＜4.2.1(2)(c)関連＞ 4.2.1(2)-1 を参照。

[6] 統一基準ガイドライン 4.2.2(1)(a)(ア)の解説を参照。

[7] オンライン上の掲示板や公式ウェブサイトに掲示する等が考えられる。

で送信するなどしてパスワードの秘匿性を確保することが必要である。」[8]旨が示されている。例えば、オンラインストレージを利用する場合は、デジタル化された処分通知等のダウンロード用の URL を電子メール（オンラインストレージサービスから送信される場合を含む)で通知し、パスワードは電話番号を利用した SMS(Short Message Service)で通知することが考えられる。

マイナポータル

問6.　地方公共団体がマイナポータル「お知らせ機能」での通知を行いたい場合は、具体的にどのような手続を行えばよいか。

マイナポータルにおいて自治体中間サーバーの「お知らせ機能」を用いてお知らせを送信する場合、情報連携用の機関別符号を利用することから、お知らせをすることができる事務は個人番号利用事務に限られる。

当該機能の活用に当たっては、マイナポータルの位置づけや機能等を踏まえるようマイナポータルの担当部局と密に連携されたい。

電子署名

問7.　公印省略している処分通知等において、電子署名は必要であるか。

公印省略している文書であれば、電子署名も不要であると考えられる。

問8.　デジタル化された処分通知等に電子署名を付す場合、電子証明書に記載すべき項目はどのような内容か。

政府認証基盤（GPKI）の官職証明書又は地方公共団体組織認証基盤（LGPKI）の職責証明書の基本領域を参考にする[9]ことが考えられる。

問9.　民間認証局が発行する職責を含む電子証明書に係る電子署名は、電子署名法上の電子署名に当たるか。

民間認証局が発行する職責を含む電子証明書に係る電子署名は、以下の要件を満たす限り、電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）第２条第１項

---

[8] 基本対策事項＜3.1.1(6)(a)関連＞3.1.1(6)-2 の a の（解説）を参照。

[9] 「政府認証基盤相互運用性仕様書」(URL：https://www.gpki.go.jp/session/index.html) 及び「LGPKI プロファイル設計書」(URL：https://www.lgpki.go.jp/doc/index.html) を参照。

[10]の電子署名に当たるといえる。

同法に基づく「電子署名」の２つの要件は、本人性（当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。同項第１号）と非改ざん性（当該情報について改変が行われていないかどうかを確認することができるものであること。同項第２号）である。職責を含む証明書に係る電子署名では、ある官職にある自然人が電子署名を行う限りにおいて、同項の「電子署名」に該当すると考えられるものであるが、当該自然人がその官職にあるという属性（職責）は電子署名法上の電子署名の要件ではない。

[10] 第二条　この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。