JCIF03－01

JCSS 校正証明書の
電磁的発行に係るガイドライン

（第 1 版）

2024 年 9 月 30 日

独立行政法人製品評価技術基盤機構

認定センター

発行所　独立行政法人製品評価技術基盤機構　認定センター
住所　〒151-0066 東京都渋谷区西原2丁目49－10
TEL　03－3481－8242
FAX　03－3481－1937
E-mail jcss@nite.go.jp
Home page　https://www.nite.go.jp/iajapan/jcss/index.html

目　次

JCSS 校正証明書の電磁的発行に係るガイドライン

1．はじめに

本指針は、JCSS登録事業者（以下、事業者）が校正証明書を電磁的発行する際の具体的な手順の例、及び発行・交付の管理等に係る情報をまとめたものである。

JCSS校正証明書の電磁的発行については、特定の法令要求事項は適用されず、ISO/IEC 17025及び「JCSS登録及び認定の一般要求事項（JCRP21）」（以下、一般要求事項）の該当する要求事項への適合が求められる。発行形態及び管理手順は、事業者が置かれている状況（顧客（校正の依頼者）の電磁的発行に対するニーズ、顧客との関係、顧客による改ざんの可能性、等）を考慮し、リスクに基づいて確立、運用することになる。

本指針を管理する担当課は認定センター計量認定課である。

2．用語の定義

本指針では次の用語を定義し、使用する。

(1) 電磁的記録[1]

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。

(2) 電磁的発行

電磁的記録による発行。

なお本指針では、電磁的発行されたJCSS校正証明書を「JCSS電子校正証明書」と称する。

本指針における電磁的発行の形態の例は附属書1を参照。

(3) 電子署名[2]

電磁的記録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。

① 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。

② 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。

本指針では、①（当該措置を行った者の作成に係るものであること）を“真正性”、②（改変が行われていないかどうか）を“非改ざん性”と称する。

備考1: 上記のうち、①の「当該措置を行った者」については一般的に、特定の個人に対する証明として「電子署名」、法人や法人内部の組織に対する証明として「電子シール（eシール）」、と証明の対象（者）や用途を区別した呼称や形態でサービスが提供されている[3]。これらは技術的な本質は大きく異ならず、主として証明の対象が異なる観点での区別であることから、本指針ではこれらを区別せずに電子署名と記載する。

(4) 電子証明書[4]

電磁的記録の利用者（JCSS電子校正証明書の発行者）が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明するために作成する電磁的記録。

備考2: 電子証明書は、「電子署名を検証する際のデータの復号化に必要な電子的な検証鍵（公開鍵）」の持ち主を証明する。実際には、認証局の信頼性を示す上で複数の電子証明書の連鎖（積み重ね）で構成されていることが多い。

(5) タイムスタンプ[5]

データがある時刻に確実に存在していたことを証明する電子的な時刻証明書の役割を果たす技術。証明された時刻以降に改変が行われた場合には上記（3）の電子署名と同様に検出が可能となる。

備考3: 上記(3)の電子署名と併用し、電子署名が行われた日時の証明として利用する場合も多い。

3. JCSS 校正証明書の電磁的発行の利点

JCSS校正証明書を電磁的発行する利点として、以下の例が挙げられる。

① 資源、コストが削減できる（ペーパーレス化の達成、紙媒体発行版の郵送に係るコストの削減）。

② 発行に係る内部手続き（押印、郵送等）が簡略化できる。

③ 発行証明書の内部管理が効率的に行える。（事業者、顧客の双方にとっての利点）

④ 紙媒体発行版に特有の破損、紛失、汚損のリスクがなくなる。

⑤ 郵送が不要になるため、顧客へ迅速に校正証明書を交付することができる。

事業者は、これら利点と種々リスク（コスト、運用の困難さ、顧客のニーズ等）とを考慮し、適用の是非を検討することになる。

4. JCSS 校正証明書の電磁的発行に係る要求事項等

一般要求事項には、JCSS校正証明書の電磁的発行に関して、以下の要求事項及び参考情報（備考）が記載されている。

5.2.2.5 校正証明書の扱い

1 件の校正対象又は校正結果に対して、紙媒体の校正証明書を複数部発行する場合及び紙発行と電磁的方法による発行を併せ行う場合においては、個々の校正証明書に固有の識別を与えなければならない（ただし、熱量標準安息香酸及び各種標準液を除く。）。校正証明書の複写については、この一般要求事項の9. 項に定める規定に従うものとする。

5.2.2.9 電磁的方法による校正証明書の発行

電磁的方法により校正証明書を発行する場合、発行及び交付に係る手順をもち適用すること。その手順には、記載事項の改ざんを防止するための措置及び機密情報の管理を含めること[備考 1～3)]。

備考 1: 電磁的方法により発行される校正証明書の交付の方法として、以下の種類が挙げられる。

- 校正事業者のシステムから、顧客にメール添付等により交付する方法
- 校正事業者のシステムにおいて、顧客が校正証明書の閲覧を可能とし、PC にダウンロード等により保存する方法
- CD 等の電磁的記録媒体に保存し、顧客に交付する方法

備考 2:「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項に規定される“電子

署名”の使用は、発行者の明確な特定、及び記載事項の改ざん等を防止するために有効である。電子署名やタイムスタンプを付す外部サービス提供者を利用する場合は、その外部提供者の機密情報管理が適切であることを確実にする必要がある。(ISO/IEC 17025 7.11.4)

備考 3: 発行及び交付に係る手順には以下が含まれるが、これらに限定されない。

- “電磁的方法による発行”について、契約段階で顧客の合意を得ること
- 紙発行版と“電磁的方法による発行”版の識別管理方法
- 電磁的方法により発行される校正証明書の誤送付を防止するための手順

9.3.3 紙発行校正証明書の複写物及び電磁的方法により発行される校正証明書の印刷物の扱い

（略）また、電磁的方法により発行した校正証明書について、その印刷物は正式な校正証明書ではない旨を校正証明書に記載する、印刷物に「COPY」、「写し」等が明瞭に表示されるような工夫をしておく、等の配慮が必要である。

事業者が JCSS 校正証明書を電磁的発行する場合には、上記要求事項への適合が求められる。特に 5.2.2.9 及び同備考 3 にある、事業者がもつべき手順について、5.で解説する。

JCSS 校正証明書の電磁的発行を行う場合、発行手順にもよるが、一般的には ISO/IEC 17025 の下記の条項へ適合する必要がある。

- 4.2.1　機密保持（下記 5(9)に関連）
- 6.2.5　JCSS 電子校正証明書の発行に係る権限付与（下記 5(10)に関連）
- 6.4　JCSS 電子校正証明書の発行に用いる、証明結果に影響する設備（ソフトウェア等）の管理
- 6.6　JCSS 電子校正証明書の発行に係る外部提供サービスの利用
- 7.1　JCSS 電子校正証明書の発行に関する顧客との合意（下記 5(2)-(6)に関連）
- 7.5 及び 7.11　技術的記録及び情報マネジメント
- 7.8　JCSS 電子校正証明書の記載事項及び発行に係る諸手順（特に 7.8.8 報告書の修正の手順）

5. JCSS 電子校正証明書の発行及び交付の管理

事業者が JCSS 校正証明書の電磁的発行を行うためにもつべき手順について、次に解説する。

なお、この内容の一部は、計量法に基づく計量証明事業における「計量証明書」の電磁的発行に係るガイドライン文書[6]を参考にしている。

(1) 顧客による改ざんのリスク

考慮の程度は、顧客による校正証明結果の利用目的に依存する。顧客に改ざんされた校正結果が市場に深刻な影響を及ぼし、その責任が発行主体である事業者に負わされるリスクを考慮して、必要であれば真正性及び非改ざん性を確実に立証できる方法を採用するべきである。電磁的発行方法の事例、及び事例毎の真正性・非改ざん性については、附属書 1 及び 2 を参照。

(2) 電磁的発行に係る顧客の合意

顧客が紙媒体発行と電磁的発行とのどちらを希望するのかは、顧客の JCSS 校正証明書の利用方法に依存する。発行形態に関する顧客のニーズを充足するためには、電磁的発行について事前に顧客の合意を得ておく必要がある。契約の段階で、紙媒体発行又は電磁的発行（若しくはその両方）に係る了承を得ておくことが一般的である。

(3) 交付の管理（誤送信をしないための手順、機密管理上のリスクを減らす手順）

JCSS 電子校正証明書には顧客情報等機密管理すべき情報が含まれており、メール添付等による交付における誤送信は機密情報漏えいにつながる。リスク低減の方策として、次の例が挙げられる。

- ➢ 顧客に事前に確認メールを送信し、当該送信に対して返信されたメールアドレス宛てに添付して送信する
- ➢ 添付ファイルの開封のための情報（パスワード、電子証明書等）を添付ファイルとは別に顧客に送付する

また、顧客は唯一名が想定されており、同一の JCSS 電子校正証明書を複数のメールアドレス宛てに添付し送信することは、機密管理の観点からも適切ではない。

(4) 電磁的発行における複数発行（正本／副本）の考え方

JCSS 校正証明書の電磁的発行においては、紙媒体発行におけるような正本の複写における（正本／副本）管理、及び同一校正対象に係る複数部を発行し交付するという概念は適用しない。事業者は顧客に対して一つの電磁的記録（JCSS 電子校正証明書）を交付するのみであり、当該電磁的記録の顧客による（顧客組織内部及び外部への）複写、転送、共有について事業者は責任を負うことはなく、顧客の責になる。電磁的記録の複写物が不適当に出回ることで誤用、改ざん等のリスクが高まることを含め、その旨を顧客に通知しておくことが望ましい。

(5) 紙媒体発行と電磁的発行を併用する場合

顧客のニーズ等に基づき紙媒体発行と電磁的発行とを併用する場合、それらを明確に識別管理するための手順をもたなければならない（一般要求事項 5.2.2.9 備考 3）。事業者が発行管理するための管理台帳等で、各発行証明書が紙媒体発行なのか電磁的発行なのかを明確に識別しておく必要がある。

一般要求事項では、同一の校正対象品目に対して、紙媒体及び電磁的方法の双方による JCSS 校正証明書の発行を許容している（一般要求事項 5.2.2.5）。紙媒体発行と電磁的発行とを明確に識別する方法として、

- ➢ 校正証明書識別番号に、それが明確に把握できる情報を含める
- ➢ 校正証明書に識別可能な情報を記述する（一般要求事項の附属書に電磁的発行による校正証明書記載例がある。）

といった手順が挙げられる。

(6)既発行 JCSS 電子校正証明書の修正再発行について

JCSS 電子校正証明書の再発行の必要が生じた場合、紙媒体発行のように事業者が顧客から JCSS 電子校正証明書を回収することは現実的にはできない。その状況においても顧客が修正再発行前の版（旧版）の電磁的記録を誤用するリスクを排除するため、顧客に旧版の

電磁的記録の削除を依頼するべきである。その場合、顧客から的確に削除した旨の連絡を受け、当該連絡を保持しておくことも重要である。

(7) 電子署名の有効期限

JCSS 電子校正証明書に電子署名を行った場合、電子証明書や、その電子署名に組み込まれた上位の電子証明書にはそれぞれの有効期限が定められている[備考 4]。電子署名の有効性は電子証明書の有効期間内に限られること、及び有効期限以降の真正性の確認手段[備考 5]について、顧客に説明を行う必要がある。詳細については下記(9)を参照。

備考 4: 「電子署名及び認証業務に関する法律施行規則」第 6 条第 4 項には“電子証明書の有効期間は、五年を超えないものであること。”とされている。実際に認証局が電子署名用に発行する電子証明書の有効期間は 2 年程度、タイムスタンプ用は 10 年程度であることが多い。複数の電子証明書が組み込まれている場合には、いずれかの電子証明書の有効期間を満了した時点で当該証明書に付随する電子署名の有効性の情報を確認できなくなる場合がある(「電子署名及び認証業務に関する法律施行規則」第 6 条延長の 11 を参照)。

備考 5: 電子証明書の有効期間をする措置として、“長期署名”(例えば PDF ファイルにおける PAdES フォーマットによる署名[7])によるタイムスタンプの再付与がある。また、有効期限超過後の危殆化した電子署名の真正性を確認する手段として、発行校正事業者が署名に用いた電子証明書のダイジェスト情報を発行校正事業者等から入手し、ユーザ自らの責任の下で確認するなどの手段が存在する。

(8) 顧客への注意喚起

事業者がリスクに基づいて確立、運用する発行・交付の手順であっても、顧客又は結果の使用者が校正証明結果を非意図的又は意図的に不正使用する可能性を完全に排除することはできない。そのリスクを想定して、必要に応じ顧客に次のような注意喚起をしておくことが望ましい。

- ➢ 電磁的発行された JCSS 電子校正証明書を紙媒体に印刷したものは、紙媒体発行 JCSS 校正証明書をハードコピーしたものと同等であり、正式な JCSS 校正証明書ではないこと(一般要求事項 9.3.3)
- ➢ 顧客又は JCSS 電子校正証明書を入手した者が、交付された電磁的記録を一部でも修正した場合や自ら電子署名等を行った場合は、その原本性を失い、有効な JCSS 電子校正証明書ではなくなること
- ➢ JCSS 電子校正証明書に関する不正行為(改ざん、偽造)について、刑法において紙媒体の私文書偽造、変造及び行使に相当する罪は、電子交付の場合は第 161 条の 2(私電磁的記録不正作出及び供用)が該当すること

(9) 顧客及びエンドユーザ(結果の利用者)への情報提供

JCSS 電子校正証明書の真正性の確認のために、顧客又はエンドユーザへ電子証明書やハッシュ等の情報を提供することが望ましい。情報を提供する場合には、情報セキュリティのリスクや ISO/IEC 17025 の機密保持に係る要求事項等に留意する必要がある。

備考 6: 認証局が事業者組織の要員に対し、そのマネジメントシステムにおける役割や権限をも勘案して電子証明書を発行しているケースは稀である。仮に情報通信技術の観点で適切な電子署名等が行われていたとしても、JCSS 電子校正証明書が事業者のマネジメントシステムの下で規定された

正規の権限者により正規の手続きで発行されたものであるか否かの検証はできない。マネジメントシステムの下で事業者が提供する JCSS 電子校正証明書の発行に使用している電子証明書や電子証明書に組み込まれた情報（電子証明書の識別番号、発行者、サブジェクト、ダイジェスト等）、個々の校正証明書のハッシュ情報等は、顧客が JCSS 電子校正証明書の真正性を確認するための助けとなる。

なお、上記に掲げた全ての情報まで提供する必要はなく、顧客のニーズや、電子署名に利用する電子証明書の階層構造などに応じた情報提供で十分である。

備考 7: 電子証明書やハッシュ情報等の情報、電子証明書をダウンロードできるようにしたサイトの例には、法務省の商業登記に基づく電子証明書制度の登記官証明書の例[8]や、総務省から認定を受けているタイムスタンプ事業者の電子証明書の例[5]がある。また、民間の認証局の中にも中間証明書をダウンロードできるように提供している例もある。

(10) パスワードや秘密鍵の管理

JCSS 電子校正証明書にパスワードや電子署名を行う場合には、使用するパスワードや秘密鍵の管理が重要である。これらが流出した場合、事業者のマネジメントシステムの下で規定された正規の権限者以外の者による校正証明書の改変、偽造等が可能となることを踏まえ、的確に管理する必要がある。

(11) 参考データを埋め込む（データファイルを添付する）際の留意事項

JCSS 電子校正証明書の電磁的記録の形式において、PDF形式の場合は、参考情報として校正証明書と関連するデータ（CSV ファイル、XML ファイル、バイナリ形式のファイル等）を埋め込む（添付する）方法がある。その方法を採用する場合は、埋め込まれるデータが参考情報である（校正証明対象外である）旨の識別が必要である。埋め込むファイルのデータ形式の仕様から、埋め込む電磁的記録内にその識別を付すことが困難な場合には、顧客に対して埋め込み利用方法と共に、埋め込まれたファイルが参考情報である旨を別途に説明を行う必要がある。

備考 8: PDF ファイルに別の添付ファイルを添付する場合、その内容の正確さを確保すると共に、利用者が利用する際に添付ファイル自体が改ざんされていないことを検証できることが望ましい。一般的には個々の添付ファイルのハッシュ情報の提供（附属書1(5)）などの手段で実現できる。

附属書1 JCSS 校正証明書の電磁的発行方法に適用できる技術要素の例

JCSS 電子校正証明書は、汎用性の高い PDF 形式による作成が主であることが想定される。以下に、情報の真正性及び非改ざん性（一般要求事項 5.2.2.9 記載事項の改ざんを防止するための措置）の確保に着目した PDF 形式 JCSS 電子校正証明書作成の例を挙げる。ここに挙げる事例以外の方法を含め、求められる真正性、非改ざん性に応じ、事業者ごとにリスクに基づいて計量法 144 条及び計量法施行規則第 94 条の規定を満足する形での作成方法を選択する必要がある。

JCSS 校正証明書の電磁的発行方法に適用できる技術要素の例を次に挙げる。個々の技術要素について、相対的なリスクとその度合いとについても簡単に解説する。実際に事業者が JCSS 電子校正証明書の発行の手順を確立する上では、次の技術要素を単独で適用するよりも、リスクの対処のために他の方法と組み合わせた複合的な対応を検討するケースが多いと想定できる。そこで、まず、この附属書１では単純なケースの例を挙げ、より現実的な複合的シナリオの例を附属書２で取り上げる。

⑴ 第三者認証局が発行する電子証明書を伴う電子署名及びタイムスタンプの付与

高い真正性及び非改ざん性が確保された電子署名及びタイムスタンプのサービスが提供されており、活用されている。それらサービスは、電子証明書が権威ある第三者認証局により発行される、国際時刻標準機関にトレーサブルなタイムスタンプを使用する、情報マネジメント規格（ISO 27001）に準拠した運用を行う、等により、高い真正性及び非改ざん性を確保している。

これらサービスの詳細は、JNLA の電子試験証明書発行に係る手引き[9]に記載されているので参考にされたい。これらは有料のサービスなので、コストとメリットとから導入を検討する必要がある。

⑵ 第三者認証局が発行する電子証明書を伴う電子署名のみの実施

真正性及び非改ざん性が確保されるが、電子署名を行った日時については事業者が電子署名を行ったコンピュータの時刻を使用している点で、タイムスタンプを併用した⑴と比較して客観的な証明としては弱いものとなる。

⑶ 第三者認証局が発行する電子証明書を伴うタイムスタンプのみの付与

タイムスタンプを単体で使用した場合には、タイムスタンプの付与以後に改ざんが行われたことが検出できる点で非改ざん性は確保される。同じ時刻認証事業者を用いて他者もタイムスタンプの付与を行っていることから、タイムスタンプは書類作成者の証明とはならず、真正性の証明については別途検討する必要がある。

⑷自ら電子証明書を発行する簡易的電子署名

コンピュータコマンドにより自らの操作で秘密鍵、公開鍵と電子証明書を生成して、電子署名を行うことも技術的には可能である。また、一部の PDF 表示ソフトウェアの機能として、電子署名用の電子証明書を自作する機能が提供されている。

これらのような簡易的電子署名を行った PDF 形式の電磁的記録には署名者名が付され、

真正性の証拠となる。また、電磁的記録に変更を施した場合、電子署名の検証機能を有するソフトウェアを用いた場合には、改ざんがあった旨が電磁的記録を開く際にメッセージ表示されることから、非改ざん性も立証できることになる。

しかしながら簡易的電子署名は、電子証明書（発行者の身分を証明する情報）を署名者自身が発行するいわゆる“自己署名”であり、第三者証明ではないこと、また、署名者になりすました偽造も可能であることから、(1)に掲げる電子署名と比較すると真正性は確保されているとは言い難い。真正性の確保には他の補足的手段（例えば、自身が作成し行使している電子署名である旨を示す 5.(9)に掲げる情報の提供、等）が必要である。

(5) ハッシュの利用

事業者が JCSS 電子校正証明書を作成した際に、ファイルのハッシュを計算し記録しておくことで、それ以降に改ざんが行われたか否かを確認できる。JCSS 電子校正証明書の利用者が手元にあるファイルのハッシュを計算し、校正事業者が計算したハッシュと一致した場合には改ざんが無いと判定できる。このために、校正事業者は JCSS 電子校正証明書の利用者に校正証明書のハッシュと、そのハッシュを計算した際のハッシュアルゴリズムの情報を提供する手順が必要となる。

これら方法の詳細については、一般的なハッシュの解説等を参照のこと。

備考 9: ハッシュは非可逆変換であることから、ハッシュのみを無関係の第三者が入手したとしても元の情報をハッシュから復元することは不可能である。

備考 10: SHA256 等の一般的なアルゴリズムのハッシュの計算については、Windows 等の OS の標準機能としてコマンドが組み込まれている。また、ハッシュはファイル転送の際の検証に使われてきた歴史から、一般的に使われている高機能のファイル圧縮ソフト（ZIP ファイル等の生成ツール）には、ハッシュの計算機能を備えるものもある。

附属書２ JCSS 電子校正証明書作成のシナリオの例

附属書１において、真正性及び非改ざん性に着目した電磁的発行の技術要素について紹介した。本附属書では、事業者がリスクに応じた発行方法を検討、採用する際の参考のために、いくつかの JCSS 電子校正証明書作成のシナリオ、及び各シナリオの“真正性”、“非改ざん性”及び“作成日時の証明”に係る検討例並びに残るリスクの対処の例を示す。

＜シナリオ1＞

事業者 A は、JCSS 電子校正証明書の発行に際し、紙媒体発行の校正証明書と同じ様式で校正証明書を専用の背景すかし入りの用紙に印刷した上で、専用印を用いて押印したものを、スキャナで取り込んで PDF 形式の JCSS 電子校正証明書とすることにした。改ざんを防止するために、PDF ファイルにはパスワードによる保護を行う。

真正性の検討

紙媒体発行の JCSS 校正証明書と同様の専用の様式の使用や押印を行っている点で、PDF ファイルの表示面としてはある程度の真正性の確保はできている。ただ、紙媒体発行の JCSS 校正証明書をスキャンし電子化したファイルは誰でも作成可能であることについてのリスクを検討する必要がある。また、PDF ファイルを顧客やエンドユーザを含む校正証明書のユーザが紙に印刷した場合についてのリスクも検討する必要がある。

非改ざん性の検討

紙媒体発行の JCSS 校正証明書と同様の様式の使用や押印を行っている点で、PDF ファイルの表示面としてはある程度の非改ざん性の確保もできている。ただし、紙媒体発行の JCSS 校正証明書をスキャンし電子化したファイルは誰でも作成可能であることについてのリスクを検討する必要がある。また、パスワードによる保護も行っているが、パスワードが流失した場合や推測された場合等にはファイルの改変が可能となる。

作成日時の証明の検討

紙媒体発行の JCSS 校正証明書をスキャンして PDF 形式の電磁的記録とした場合では、作成日時の証明となる情報は当該電磁的記録には残らない。

残るリスクへの対処の例

- 表示面に電磁的記録が原本である旨を書き込むなど、紙媒体発行と区別した表示をする等の対策を検討すべき。
- 紙媒体のスキャンであることから記載されている情報の書換えはデジタルデータと比べて困難であるものの、パスワードを設定する際に複雑なパスワードを生成するツールの活用、同じパスワードを使い回さないなど、リスクを低減する手段は検討しうる。
- 作成日時の証明のためにタイムスタンプの付与を検討できる。タイムスタンプを付与した場合には、タイムスタンプ付与後の改ざんも検出できることから非改ざん性も向上する。
- JCSS 電子校正証明書を発行する際に、PDF ファイルのハッシュを計算し、記録として保存することで、発行時の原本の内容の特定ができる。ユーザ等から照会があった際には、発行者の手元のハッシュの情報と、ユーザの手元のファイルのハッシュと対比することで非改ざん性が証明できると共に、発行者の手元に情報をもっていることから真正性の傍証となりうる。

＜シナリオ２＞

事業者 B は、JCSS 電子校正証明書の発行に際し、スプレッドシートソフトの出力形式として PDF 形式を指定して PDF 形式の JCSS 電子校正証明書とすることにした。改ざんを防止するために、JCSS 標章／認定シンボル及び印影（計量法施行規則第 94 条三号でいう“押印又は署名”に相当）と、電磁的発行した旨の記述も PDF の表示面に表示される形とする。PDF 形式の電磁的記録にはパスワードによる保護を行う。

真正性の検討

JCSS 標章／認定シンボル及び印影を PDF の表示面に表示させる形で、ある程度の真正性の確保はできている。ただし、事業者のマネジメントシステムの規定の下で正規の権限をもたない者が JCSS 標章／認定シンボル及び印影を無断で行使することについてのリスクを検討する必要がある。

非改ざん性の検討

JCSS 標章／認定シンボル及び印影を PDF の表示面に表示させる形で、ある程度の非改ざん性の確保はできている。ただし、真正性の検討に挙げたものと同様のリスクを検討する必要がある。

また、パスワードによる保護も行っているが、パスワードが流失した場合や推測された場合等にはファイルの改変が可能となる。

作成日時の証明の検討

単純に PDF 化したファイルでは、作成日時の証明となる情報は当該電磁的記録には残らない。

残るリスクへの対処の例

- 権限の無い者が JCSS 標章／認定シンボル及び印影を無断で行使することへの対策が必要かもしれない。事業所内での管理や、表示された印影等を容易に複製されないような対策を検討するか、原本性を証明する他の手段の併用を検討しうる。
- デジタルデータを直接 PDF の表示面に書き込んでいるため、パスワードが判明すれば容易にデータの書換えが可能となり、また、書き換わったことの判別もシナリオ１と比べて一層困難である。パスワードを設定する際に複雑なパスワードを生成するツールの活用、同じパスワードを使い回さない、電子署名、e シールやタイムスタンプ等の署名技術の適用で改ざんを防止するなどリスクを低減する手段は検討しうる。
- 作成日時の証明のためにタイムスタンプの付与を検討できる。タイムスタンプを付与した場合には、タイムスタンプ付与後の改ざんも検出できることから非改ざん性の確保も格段に向上する。
- JCSS 電子校正証明書を発行する際に、PDF ファイルのハッシュを計算し、記録として保存することで、発行時の原本の内容の特定ができる。ユーザ等から照会があった際には、発行者の手元のハッシュの情報と、ユーザの手元のファイルのハッシュと対比することで、非改ざん性が証明できると共に、発行者の手元に情報をもっていることから真正性の傍証となりうる。

＜シナリオ３＞

事業者 C は、JCSS 電子校正証明書の発行に際し、スプレッドシートソフトの出力形式として PDF 形式を指定して PDF 形式の JCSS 電子校正証明書とすることにした。改ざんを防止するために、JCSS 標章／認定シンボル及び印影と、電磁的発行した旨の記述も PDF の表示面に表示される形とする。PDF 形式の電磁的記録にはタイムスタンプを適用する。

真正性の検討

JCSS 標章／認定シンボル及び印影を PDF の表示面に表示させる形で、ある程度の真正性の確保はできている。ただし、権限の無い者が JCSS 標章／認定シンボル及び印影を無断で行使することのリスクを検討する必要がある。また、タイムスタンプについては時刻認証事業者の情報は書き込まれる一方でタイムスタンプの付与操作を行った者の情報は残らないことから、タイムスタンプでは真正性の証明にはならない。

非改ざん性の検討

タイムスタンプの適用により、適用後の改変が検出できることから、非改ざん性の確保の状態は高い。

作成日時の証明の検討

タイムスタンプの適用により、時刻認証事業者による日時の客観的な証明がなされる。

残るリスクへの対処の例

- 権限の無い者が JCSS 標章／認定シンボル及び印影を無断で行使することへの対策が必要かもしれない。事業所内での管理や、表示された印影等を容易に複製されないような対策を検討するか、原本性を証明する他の手段の併用を検討しうる。
- タイムスタンプの適用により改ざんを防止できている一方で、真正性については表示面以外の客観的な証明がないため、ユーザがソフトウェアにより真正性を判定したい等のニーズがあるようであれば、電子署名の導入などの手段は検討しうる。
- JCSS 電子校正証明書を発行する際に、タイムスタンプを付与した後の PDF ファイルのハッシュを計算し、記録として保存することで、発行時の原本の内容の特定ができる。ユーザ等から照会があった際には、発行者の手元のハッシュの情報と、ユーザの手元のファイルのハッシュと対比することで、非改ざん性が証明できると共に発行者の手元に情報をもっていることから、真正性の傍証となりうる。

＜シナリオ４＞

事業者 D は、JCSS 電子校正証明書の発行に際し、スプレッドシートソフトの出力形式として PDF 形式を指定して PDF 形式の JCSS 電子校正証明書とすることにした。改ざんを防止するために、JCSS 標章／認定シンボル及び印影と、電磁的発行した旨の記述も PDF の表示面に表示される形とする。PDF ファイルには自作の秘密鍵を基に、第三者認証局を利用せずに自身が生成した電子証明書を用いて電子署名を適用する。タイムスタンプは付与しない。

真正性の検討

JCSS 標章／認定シンボル及び印影を PDF の表示面に表示させる形で、ある程度の真正性の確保はできている。ただ、権限の無い者が JCSS 標章／認定シンボル及び印影を無断で行使することのリスクを検討する必要がある。また、自作の電子証明書を適用していることから、電子証明書の所有者については客観的な証明はない。

非改ざん性の検討

電子署名の適用により、適用後の改変が検出できることから、非改ざん性の確保の状態は高い。

作成日時の証明の検討

この事例ではタイムスタンプを適用していないことから、電子署名の日時は事業者が電子署名を行ったコンピュータに設定された時刻であり、客観的な証明がない。

残るリスクへの対処の例

- 権限の無い者が JCSS 標章／認定シンボル及び印影を無断で行使することへの対策が必要かもしれない。事業所内での管理や、表示されたロゴ等を容易に複製されないような対策を検討するか、原本性を証明する他の手段の併用を検討しうる。
- 電子署名についても、事業者 D の権限ある者が適切に実施していることを示す手順の確立や、使用している電子証明書（と公開鍵）について事業者 D のウェブサイトに公開することで自己署名の信頼性を確保できるだろう。
- 自作の秘密鍵を失効させることができないため、秘密鍵とそのパスワードが流出した場合には、流出する以前に発行した JCSS 電子校正証明書と同じ電子署名を行った偽造証明書が無関係の第三者によって作成される可能性はある。秘密鍵とそのパスワードの厳重な管理が基本ではあるものの、リスクを勘案して電子署名の客観性をさらに向上したい場合には、第三者認証局によって発行された電子証明書の導入を検討しうる。
- タイムスタンプの適用により電子署名を行った日時の客観的な証明を追加できる。
- JCSS 電子校正証明書を発行する際に、電子署名を行った後の PDF ファイルのハッシュを計算し、記録として保存することで、発行時の原本の内容の特定ができる。ユーザ等から照会があった際には、発行者の手元のハッシュの情報と、ユーザの手元のファイルのハッシュと対比することで、非改ざん性が証明できると共に発行者の手元に情報をもっていることから、真正性の傍証となりうる。

＜シナリオ５＞

事業者 E は、JCSS 電子校正証明書の発行に際し、スプレッドシートソフトの出力形式として PDF 形式を指定して PDF 形式の JCSS 電子校正証明書とすることにした。改ざんを防止するために、JCSS 標章／認定シンボル及び印影と、電磁的発行した旨の記述も PDF の表示面に表示される形とする。PDF ファイルには第三者認証局が発行した電子証明書を用いて電子署名とタイムスタンプをあわせ適用する。

真正性の検討

第三者認証局が発行した電子証明書を用いて電子署名が行われているので、基本的に真正性は確保されていると言える。JCSS 標章／認定シンボル及び印影を PDF の表示面に表示させることにより、ある程度の真正性の確保はできている。ただし、権限の無い者が JCSS 標章／認定シンボル及び印影を無断で行使することのリスクを検討する必要がある。

非改ざん性の検討

電子署名及びタイムスタンプの適用により、適用後の改変が検出できることから、非改ざん性は高い。

作成日時の証明の検討

タイムスタンプを適用しており、時刻認証事業者による客観的な証明がある。

残るリスクへの対処の例

・ 権限の無い者が JCSS 標章／認定シンボル及び印影を無断で行使することへの対策が必要かもしれない。事業所内での管理や、表示されたロゴ等を容易に複製されないような対策を検討するか、原本性を証明する他の手段の併用を検討しうる。
・ 電子署名については、第三者認証局が発行した電子証明書を用いて電子署名が行われているので基本的に問題は無いと言える。
・ JCSS 電子校正証明書を発行する際に、電子署名を行った後の PDF ファイルのハッシュを計算し、記録として保存することで、発行時の原本の内容の特定ができる。ユーザ等から照会があった際には、発行者の手元のハッシュの情報と、ユーザの手元のファイルのハッシュと対比することで、非改ざん性が証明できると共に、発行者の手元に情報を持っていることから真正性の傍証となりうる。

附属書３　第三者認証局が発行する電子証明書に基づく電子署名を適用する場合の配慮事項

附属書2にあるように、信頼できる第三者認証局が発行する電子証明書に基づく電子署名を JCSS 電子校正証明書に適用することは、その情報に係る真正性及び非改ざん性を確保する上で非常に適切である。一方で、細かい点では配慮が必要となる。

次に、第三者認証局が発行する電子証明書を用いた際の電子署名の的確な適用のために配慮すべき事項を挙げる。

① 電子証明書の対象

電子証明書の対象が何であるか（法人の代表者個人、その他の特定の個人、法人又は法人内の組織）を認識する必要がある。電子証明書の対象によっては、必ずしも人事異動や組織変更、マネジメントシステム内での権限の変更と連動しているとは限らないため、電子証明書としての客観的な証明が有効であったとしても、正規の権限の下での署名であることが確実でない場合がある。

② 電子証明書の有効性及び信頼性

電子証明書の有効性の確認は、証明書失効リスト（CRL）の確認又は OCSP（Online Certificate Status Protocol）によって行われるが、どちらもインターネットに接続された環境が必要である。JCSS 電子校正証明書のユーザがオフラインや接続制限が課された閉じたネットワーク環境下で証明書を利用する場合には、これら検証のための機能が働かないことから、そのリスクへの対応（検証用に電子証明書を別途入手するなどの代替手段の準備等）が必要となる。

使用している電子証明書（及び公開鍵）の信頼性は、それらを公開する（例えば、事業者のウェブサイトに公開し、ユーザによるダウンロードを可能とする）ことにより向上させることができる。

③ 電子証明書の有効期限

第三者認証局が発行する電子証明書は複数の証明書の連鎖で成り立っていることが多く、それぞれの証明書の有効期間は比較的短いことから、そのリスクへの対応が必要となる。（5.(7)備考 4 を参照のこと。）

備考 11: 複数の証明書の連鎖で成り立っている場合、手元に発行された電子証明書の有効期間は発行された時点から2年程度あったとしても、第三者認証局が使用する連鎖の上位の電子証明書の有効期限満了の間近で発行された場合には、結果として連鎖全体が一貫して確認できる期間は比較的短くなることも原理的には生じうる。

④ 秘密鍵及びそのパスワードの流出時のリスク

秘密鍵及びそのパスワードが流出した場合には、第三者認証局が発行する電子証明書については認証局が失効させる手段がある。失効後は電子証明書に対応する秘密鍵を用いた電子署名が行使できなくなる点では、認証局が電子証明書を失効扱いと登録した後の被害の拡散は防止できる。しかし、流出する以前に発行した JCSS 電子校正証明書の電子署名に組み込まれた電子証明書も一般的には失効扱いとなるため、過去に発行した証明書のユ

ーザに影響を与えうることを、リスクとして検討すべきである。

以上

参考　電子署名等のサービスがもつ機能とその用途等

一般に提供されている電子署名等のサービスがもつ機能とその用途等を下表に示す。

サービス種類 / 機能	電子署名（認証局が関与するもの）	タイムスタンプ	e シール
「発行者の特定」	○ 個人の特定 第三者機関（認証局）による作成者「個人」としての証明 特定の個人に紐付け 異動があれば新任の証明書を再作成	× タイムスタンプには作成者を証明する機能はない	○ 法人・組織の特定 第三者機関（認証局）による作成者「法人や団体、組織」としての証明 特定の個人に紐付けせず、また個人の意思とも関連しないため、人事異動があっても組織としての証明となる
「改ざん防止」	○ 実施後の改変が検知可能	○ 付与後の改変が検知可能	○ 付与後の改変が検知可能
「作成日時の証明」	× ただしタイムスタンプと併用可能で、タイムスタンプが証明を担う	○ 第三者機関（認証局）による時刻の証明	× ただしタイムスタンプと併用可能で、タイムスタンプが証明を担う
電子証明書の有効期間※1	数年（2 年程度）※2	10 年程度が一般的	2 年程度
電子証明書の有効期間経過後の有効性	法的には有効でなくなる（暗号化のアルゴリズムの危殆化のリスクを考慮して、電子証明書の有効期間が設定されている）		
危殆化の防止方法	最初の署名は PAdES（PDF）等の長期署名により行い、署名に組み込まれた電子証明書の期限が切れる前にタイムスタンプの付与		
有効性確認の方法	認証局に対して「失効確認」の照会を行うことで有効性を確認する※3		

※1:　電子証明書の有効期限は各証明書の提供者が独自に決定している。情報は提供者に確認されたい。

※2:　法律での上限は 5 年。

※3:　電子証明書の検証（失効確認）ができない場合であっても、電子署名後の改変（改ざん）の有無は確認可能。

引用文献等

[1] 民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成16 年法律第 149 号）

[2] 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）

注：法令に基づく電子署名や技術の概要については、デジタル庁のウェブサイト【電子署名】及びそこに掲載される関連情報を参照
（https://www.digital.go.jp/policies/digitalsign/）

[3] 総務省ウェブサイト 【タイムスタンプ・e シール】
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/law-index.html）

[4] 電子署名及び認証業務に関する法律施行規則（平成 13 年総務省・法務省・経済産業省令第 2 号）

[5] 総務省ウェブサイト 【タイムスタンプについて】
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html）

[6] 計量証明事業における計量結果の電子交付の運用基準(ガイドライン)例示＜（一社）日本環境測定分析協会 計量証明書の電子発行に関する WG＞
（https://www.jemca.or.jp/wp-content/uploads/2019/01/e-measurement.pdf）

[7] ISO 32000-2:2020 Document management — Portable document format — Part2: PDF 2.0

[8] 法務省ウェブサイト 【電子認証登記所登記官の電子証明書について】
（https://www.moj.go.jp/ONLINE/CERTIFICATION/REGISTRY/registry12-1.html）

[9] JNLA 試験証明書の電磁的方法による発行について（NITE 公開文書）

※：上記 URL のいずれも、2024/09/17 に確認したもの