システム監査学会　研究プロジェクト調査研究報告書

電子文書の監査証拠としての要件等の研究

(Study of requirements for electronic documents as audit evidence)

「監査の適合性チェックとコンサルティング機能の実効性・有効性の達成」研究プロジェクト

2022年6月10日

報告者：稲留　和紀
メンバー：赤尾　嘉治
木村　裕一
尾崎　孝章

目次

1. 検討に当たって
2. 電子文書の特徴
3. 電子文書の背景情報
4. 証拠としての電子文書
5. 電子文書の類型
6. 電子文書の信頼性
7. 各種要求における電子文書
8. 拒否への対応
9. 監査人の対応
10. その他
11. 参考資料
12. おわりに

1. 検討に当たって

■電子文書を監査証拠とする際に具備すべき要件

- 証拠としての電子文書に要求するレベル
- 電子文書の信頼性を確保するための手段
- 情報システムや文書管理システムが満たすべき要件
- 資料の提示拒否への対応や監査人の対応

■ 本研究における基本的な文書

- 参考資料[1] 公益社団法人日本文書情報マネジメント協会「電子文書信頼性向上プロジェクト中間報告」
- 参考資料[2] 公益社団法人日本文書情報マネジメント協会「電子文書信頼性向上ガイドライン」

2. 電子文書の特徴

■紙
「捺印、印影の印鑑証明」＝「正式な文書」

■電子文書固有の特徴

①永続的に保持・保存可能性
②大容量のデータの保存可能性
③全く同じデータのコピーの可能性
④改ざん検知の不可能性

電子文書が作成された<u>背景情報</u>をあわせて示すことが重要

3. 電子文書の背景情報

■電子文書の作成背景

5W1H：いつ(When) どこで(Where) だれが(Who)
何を(What) なぜ(Why) どのように(How)

	管理手段や方法
いつ(When) どこで(Where) だれが(Who)	電子署名とタイムスタンプ
なぜ(Why)	電子文書の作成目的や運用ルール・ 運用規定や利用規約などの整備と保存
どのように(How)	「署名システム」の仕様や操作説明書 操作ログなどの提示

4. 証拠としての電子文書

■内部監査の証拠文書としての電子文書

① 監査証拠は監査基準に関連し、かつ、検証できる、記録、事実の記述又はその他の情報

② どのような背景で作成または取得された文書であるかが保存期間を通して確認できること

③ 真正性、成立時期、完全性が保存期間を通して証明可能なこと

5. 電子文書の類型

■電子文書の類型を整理

図表１　電子文書の類型

類型	特質	例
A	法令により規定され、必要とされる文書・記録	・公的申請書、届け出 ・外部との議事録 ・設計図書
B-1	外部と取り交わす電子文書（意思表示あり）	・契約書、注文書、請書、借用書 ・領収書、検収書 ・誓約書、預金通帳、預かり証
B-2	外部と取り交わす電子文書（通知）	・見積書、請求書、納品書
C-1	内部の電子文書（意思表示あり）	・社内会議議事録、稟議書、決裁記録 ・システムログ、
C-2	内部の電子文書	・企画書、計画書、研究ノート ・訪問報告書 ・ノート、メモ

6. 電子文書の信頼性

■電子文書の類型と信頼性確保の要求レベル

電子文書の類型	信頼性確保の要求レベル
外部から受領する文書 (類型：A, B-1, B-2)	作成者の真正性が重要
外部へ提出する文書 (類型：A, B-1, B-2)	基本的には受領側の要求に従う （申請などの場合は真正性が重要となるなど、受領側のポリシーに沿った内容とすることが重要）
内部の文書 (類型:C-1, C-2)	責任追及などの場合は信頼性が重要

6. 電子文書の信頼性

■文書情報管理システムの信頼性確保要件

① 電子文書の作成から廃棄までの社内規定策定

② 文書の背景情報の管理・保存

③ 文書管理運用やアクセスログ等の記録

④ 文書の成立時期を記録

⑤ セキュリティ状況管理・対策

⑥ 上記の①～⑤の検証を第三者により実施

⑦ 目的の文書を直ちに取り出せる機能・性能
（再生方法の共有）

6. 電子文書の信頼性

■情報システムの機能・特性や技術進歩に応じた課題への対応

① 文書作成ソフトの特性・差異などによる影響
（WORD OASYS 一太郎 Pages等）

② PDF文書に加筆修正、上書き等できるアプリ

③ スキャナー、カメラ、記憶媒体などの性能・品質

④ システム障害発生での監査の中断や監査証拠の提示が困難な場合

⑤ クラウド、リモートでのリスク分析とバックアップ等証拠の保全

6. 電子文書の信頼性

■作成・取得背景を特定する要素

リスクの大きいもの	＝	厳格レベル
多くの文書に共通に必要となるもの	＝	推奨レベル
やむを得ないもの	＝	簡易レベル

この３つのレベルに分けて整理

6. 電子文書の信頼性

図表２　作成・取得背景を特定する要素

カテゴリ	作成・取得背景を特定する要素	簡易	推奨	厳格
文書	作成日時	○	○	○
	作成者、関係者	○	○	○
	様式		○	○
	文書と取引/活動の関係			◎
	関係する文書、ファイルとの関係			◎
業務プロセス	文書、要員、取引先、業務/取引/活動の関係	○	○	○
	取引相手	○	○	○
	アクセス規制	○	○	○
	業務分類	○	○	○
	文書の分類	○	○	○
	取引日時	○	○	○
業務規程等	文書の作成と管理に関する業務規程/システム統制規程	△	○	○
	メタデータの作成と管理に関する業務規程/システム統制規程	△	○	○
	文書管理運用に関する業務規程/システム統制規程	△	○	○
	アクセスと権限に関する業務規程/システム統制規程	△	○	○
規制等	生成に関する法令・規制要件		▲	◎
	保存、セキュリティ、破棄に関する法令・規制要件		▲	◎
	文書、文書管理プロセスと法令・規制情報の関係		▲	◎
部門、要員	作成担当者	○	○	○
	承認者	○	○	○
	アクセス権限を与えられた関係者	○	○	○

▲･･･努力義務、◎･･･強化、△･･･文書化までは求めない、○･･･必要、空白･･･不要

6. 電子文書の信頼性

■信用性確保の手段

(1) 真正性：本人が本人の意思で作成したこと	
①電子署名	公開鍵による検証
②電子サイン	筆跡
③ワンクリック	事前の認証
(2) 成立時期の正しさ	
①タイムスタンプ	TSA（時刻認証局）
(3) 完全性	
①改ざん防御	WORM媒体に記録 耐タンパ装置に保管 ソフトウェア統制により変更・削除を制限
②改ざん検知	電子署名 タイムスタンプ ダイジェスト値の管理

6. 電子文書の信頼性

■レベルにおける管理対策の例

厳格レベル	⇒	電子署名 タイムスタンプ アクセス制御
推奨レベル	⇒	電子署名 タイムスタンプ
簡易レベル	⇒	PDF文書化

6. 電子文書の信頼性

■有効性を証明するための資料

1. 電子証明書が本人に対して発行されていたことを示すもの
2. 認証局の証明書発行に関する規程
3. 認証局が受領した発行申請書や本人確認書類、受領書
4. 秘密鍵は本人だけが使用でき、その署名操作が確認できるもの
5. システム概要書、仕様書、必要に応じ署名時の操作ログなど
6. 長期署名の検証結果
7. 署名検証レポートやその解説書など

7. 各種要求における電子文書

■裁判手続きにおける電子文書

① コンピュータで処理の対象となりえるデータ

② 電磁的方法で記録され、コンピュータやスマートフォンで処理されるデータ　＝「電磁的記録」

①②かつ、持続的に存在するファイル等のデータを「電子文書」と定義

7. 各種要求における電子文書

■認証審査における電子文書

① 前述の裁判手続きにおける電子文書の証拠の要件を満たしていること

② 認証基準における電子文書の証拠の要件を満たしていること

7. 各種要求における電子文書

■内部監査手続きにおける電子文書

・「図表1 電子文書の類型」(スライド７)
・「図表2 作成・取得背景を特定する要素」(スライド12)

を参考に電子文書の持つ信頼性、有効性やリスクに応じた
「厳格、推奨、簡易」レベルの対策を講じて、
証拠管理をしていること

（ただし、法的規制を受ける立場にある組織、認証審査を受けている
組織は前述の認証審査における電子文書の証拠の要件を
満たしていることも必要となる）

8. 拒否への対応

■監査証拠となる情報提出・提示の拒否

拒否には監査人はその状況をありのままに報告する

拒否の例）

①個人情報だから提示・提出できない
②守秘義務があるので出さない
③顧客情報のため個別具体的な内容は提示しない
④社内でも取扱者限定である

※被監査部署の故意でおこなわれた場合は別の問題

①証拠隠滅のため、データ消去
②証拠隠滅のため、データ改ざん
③証拠隠滅のため、媒体を廃棄

9. 監査人の対応

■第一者、第二者、第三者監査による違い

A) 第一者監査の場合
資料へのアクセス権、取扱いは社内規定による

B) 第二者監査の場合
製品購入、サービス提供の顧客との契約事項による

C) 第三者監査の場合
監査依頼者と監査人の契約事項による
第三者監査の場合には、事前に十分な協議が必要
第三者では契約事項遵守を見極めての契約が必要
「見極める」方法と手段を明確にすることは難しい

10. その他

- ✓ 犯罪捜査のような場合で強制的に証拠を押さえることと、監査とは同一の議論はできない
- ✓ 拒否の理由と監査人の立場・契約内容により、いろいろなパターンが発生し、対応が変わる
- ✓ 具体的に検討していないが、画像データ、音声記録データなどの証拠についても検討を要する
- ✓ ここで検討した情報をもとに最終的には各企業が電子文書の情報としての資産価値を評価して、その電子文書の持つ脆弱性をどのように克服して、監査を成立させるのかに帰すると考えられる

11. 参考資料

[1] 公益社団法人日本文書情報マネジメント協会
「電子文書信頼性向上プロジェクト中間報告」
[2] 公益社団法人日本文書情報マネジメント協会
「電子文書信頼性向上ガイドライン」
[3] システム監査学会　研究プロジェクト
「オンラインによる監査手法に関する調査研究」
[4] 日本工業規格
「JIS Q 19011マネジメントシステム監査のための指針」
[5] 日本工業規格
「JIS Q 27001情報セキュリティマネジメントシステム－要求事項」
[6] 経済産業省
「システム管理基準」「システム監査基準」
[7] 石島 隆
「リモート監査に利用する電子的監査証拠とその証拠力」

12. おわりに

- デジタル化の進展に伴い、利便性向上とは裏腹にインシデントの増加が懸念される
- 企業にとって業務遂行上の根拠となる電子文書の真正性、完全性、成立時期などの証明が責務となる
- 法的規制への対応、電子化のコスト増、個人情報の保護など、課題が山積している
- この避けて通れない課題に対して、微力ながら本稿が参考になれば幸いである

ご清聴ありがとうございました。