［特集］

DXとあわせた検討を 証憑の真正性を担保する内部統制の構築

小寺雅也　EY 新日本有限責任監査法人 公認会計士

◆ *Summary* ◆

昨今の急激な社会情勢の変化は，企業をあらゆる領域で DX に向かわせ，それに伴い業務プロセスも変革されてきた。その一方で，PDF を利用した改ざん，なりすましの不正事例も増加傾向にある。これらは，環境変化に合わせた十分なリスクが検討されていないことを原因としていることが多い。

そこで，昨今のデジタル化の背景を考察したうえで，DX で変革された業務プロセスにおいて，信頼性のある報告の基礎となる証憑の真正性を担保する内部統制を構築するための留意点について検討する。

《はじめに》

昨今の急激な社会情勢の変化は，企業をあらゆる領域で DX に向かわせた。売上に直結する製品やアプリに限らず，製造部門や営業部門の仕組み，管理部門の証憑のあり方や報告の方法など，あらゆるところでデジタル化が進められた結果，業務プロセスは変革し，競争はますます激化している。

われわれ会計士は，日々管理部門に集約される情報と根拠証憑をもとに作成される報告の信頼性に対して保証を与える業務を行っている。DX により組織の業務プロセスが変革することは，報告の信頼性に重要な影響を与えるため，その変化を正しく理解し，場合によっては，信頼性を担保するための内部統制に対して指導的機能を発揮しなければならない。

そのようななか，昨今増加しつつある不正として，PDF を利用した証憑の改ざんやなりすましがある。具体的には，紙で受領した証憑を社内で PDF に変換する際に改ざんが行われ，改ざんされた PDF を利用して業務プロセスが進められていたケースや，なりすまし先から直接 PDF を受領し業務プロセスが進められていたケースなどである。

その多くは，DX により業務プロセスは変革されたものの，改ざんやなりすましに対するリスクを十分に想定していなかったために，必要な統制を整備，運用していないことが原因と考えられる。

今般の内部統制基準の改訂においては，不正に対するリスクへの対応が強調されるとともに，リスクの変化に応じてリスクを再評価し，リスクへの対応を適時に見直すことの重要性が追加されている。

そこで，本稿では，まずは昨今のデジタル化への社会の変化と背景を考察したうえで，DX を目的として変革される業務プロセスに

おいて，信頼性のある報告の基礎となる証憑の真正性を担保する内部統制を構築するための留意点について検討する。

Ⅰ　DXとそれを取り巻く社会の動き

DXとはDigital Transformationの略称であり，経済産業省が策定したデジタルガバナンス・コード2.0ではDXを「企業がビジネス環境の激しい変化に対応し，データとデジタル技術を活用して，顧客や社会のニーズを基に，製品やサービス，ビジネスモデルを変革するとともに，業務そのものや，組織，プロセス，企業文化・風土を変革し，競争上の優位性を確立すること」と定義しており，本稿はこの定義に従う。

DXに至るには，Digitization（以下「デジタイゼーション」という。）の段階とそれに続くDigitalization（以下「デジタライゼーション」という。）の段階を経る必要がある。証憑の真正性に置き換えた場合，紙とハンコの世界から，信頼できるデジタルデータに移行するのがデジタイゼーションであり，信頼できる大量のデジタルデータを利用して様々なアプリケーションを利用する段階がデジタライゼーションである。その結果，組織のプロセス等は変革されて競争上の優位性が生み出される。

昨今は，ディープフェイクが懸念されるなど，信頼性のあるデジタルデータへの注目はますます高まっている。信頼できるデジタル社会の基盤は，適切なデジタイゼーションから始まる。

1　デジタイゼーションの類型

証憑に係るデジタイゼーションには大きく3つの方法があると考えられる。

① 紙を受領し，場合によっては紙をPDFに変換し，最終的には紙またはPDFに記載されている情報をテキストデータに変換してシステムで保存，管理する方法
② PDFを受領し，PDFに記載された情報をOCR等を通じてテキストデータに変換してシステムに保存，管理する方法
③ 構造化されたテキストデータをシステム上で直接やり取りし，当該データをシステムに保存，管理する方法

①の方法は，従来の紙の業務プロセスであり，PDF化し税務上の保存要件を満たす場合，電子帳簿保存法（以下「電帳法」という。）のスキャナ保存制度（電帳法4③）に該当する。

②の方法は，電帳法では電子取引（電帳法2五）に該当し，たとえば，PDFが添付された電子メールの受領などが該当する。

③の方法も，電帳法では電子取引（電帳法2五）に該当し，たとえば，EDIシステムを利用したやり取りが該当する。

わが国は，あらゆる要素がデジタル化したSociety5.0の社会を目指している。その社会でのデジタルデータのやり取りは，③の方法，すなわち，構造化されたテキストデータで取引の開始から終了まで行われるようになるこ

Profile

こでら・まさや◇EY新日本有限責任監査法人　アシュアランスイノベーション本部・第4事業部　公認会計士。Eコマース，AIソリューション，ライフサイエンスを中心に，上場会社の会計監査，IPO支援，デジタル内部統制構築支援，大学および大学発ベンチャーに対する利益相反マネジメント支援等の業務に従事。主な著書（共著）は『実践　不正リスク対応ハンドブック―内部統制の強化，不正会計の予防，発見・事後対応』（中央経済社）。

とを想定していると思われるが，その段階には現状至っていない。

足元は，③の方法は一部で行われているが，大勢はいまだ①の方法，または，徐々に②の方法に移行してきている段階といえる。前述した現在増加しつつあるPDFを利用した不正の具体的な手法の多くが，紙で受領した証憑を社内でPDFに変換する際に改ざんを行い，改ざんされたPDFで業務プロセスを進めていたケース（①の段階）や，なりすまし先から直接PDFを受領し業務プロセスを進めていたケース（②の段階）であることからも明らかである。

一方で，③の方法は，特定の業界の特定の取引先との間でEDIシステムを利用して従来から行われてはいるが，適用されている範囲は狭い。昨今は，同一のベンダーシステムを利用している者同士では，業種の壁を越えて取引が広まりつつある。さらに，異なるベンダー同士でも，Peppolという共通基盤を通じて，消費税法上の要件を満たしたデジタルインボイスのやり取りが2023年10月以降から可能になり，おそらくこの領域は今後ますます広がりをみせるだろう。

2　DFFT

あらゆる要素がデジタル化されるSociety5.0の社会は，DFFTという基本的概念によって支えられる。

DFFTとは，Data Free Flow with Trust（信頼性のある自由なデータ流通）の略称である。2019年1月のダボス会議において，わが国が提唱した概念であり，現在デジタル庁を中心に推進されている。

DFFTの考え方は，情報の発行者が電子署名など何かしらの信頼性を確保したデータを受領者に発信し，受領者は当該データの真正性を確認できる仕組みがあることを前提に，国際的に信頼できるデジタルデータの自由な流通を目指すものである。

発行者が誰だかわからないまたは改ざんされているかどうかわからないデジタルデータを仮に受領したとして，その後受領者側でいかになりすまし，改ざんを防止する内部統制を敷いたとしても，本質的にはデジタルデータの真正性は担保できないという考え方があると理解できる。

3　電子帳簿保存法

将来のデジタル社会を見据えてDFFTという概念がある一方で，現在わが国の電子証憑の実務慣行を形成している電帳法では，今後増加するであろうPDFの真正性については以下のように整理されている。

電帳法施行規則（以下「電帳法規則」という。）4条では，電子取引を行った場合の証憑の保存要件として，発行者側のタイムスタンプが規定（電帳法規則4①一）されており，一見すると，なりすまし，改ざんを意識した建付けのようにも読める。しかし，実務上は，この方法がとられている事例は少なく，ほとんどのケースでは受領後速やかにタイムスタンプ（電帳法規則4①二），訂正削除の記録が残るシステムによる授受（電帳法規則4①三），訂正削除の防止に関する事務処理規程の整備運用（電帳法規則4①四）による対応がほとんどである。理由は，電子証憑の保存義務は受領者側にあるにもかかわらず，発行者側のタイムスタンプだけは電子証憑を発行する側のコスト負担となってしまうため，経

済合理性の観点から選択されにくいからである。

したがって，現行の電帳法からは，PDFによる電子取引で発行者側によるなりすまし，改ざんを防止する措置が自主的にとられるほどの社会的機運は高まっておらず，受領者側の企業が現状の実務慣行を理解したうえで，なりすまし，改ざんに対応した内部統制を構築することが，社内で信頼性のあるデジタルデータとして受領，管理するために必要となる。

なお，スキャナ保存制度やEDI取引の場合，細かい保存要件はあるものの，自社スキャナ保存システムまたはEDIシステムを介した取引情報が電子証憑となるため，システムの機能によりその真正性を担保することができる。

Ⅱ　内部統制構築上の留意点

内部統制を検討するにあたっては，内部統制の有効性の判断規準となる６つの基本的要素（統制環境，リスクの評価と対応，統制活動，情報と伝達，モニタリング，ITへの対応）を切り口に検討することにはなるが，実務上はリスクの評価，統制活動，ITへの対応に特に着目したい。

１　リスクの評価

リスクの評価が適切に行われない場合，その後の内部統制の運用をいかに厳しくしたとしても所期の目的を達することはできない。そこで，証憑の性質，情報の転換点，取引の性質の３つの観点から，DXによりどのようなリスクが新たに発生するのかを検討する。

⑴　証憑の性質

情報源である証憑が，紙か，PDFか，EDI等を通じて構造化されたテキストデータであるかにより管理上の検討事項は異なる。

図表１は，証憑の種類の相違による管理上の長所と短所を挙げてみた。

業務プロセスにPDFを積極的に導入することは，意思決定を迅速にするという意味では重要であり，かつ，画面を通じてとはいえ従来の紙のような一覧性といった直感を残したデジタル化ができ，一見，紙の業務プロセスから大きく逸脱せずにデジタル化への移行が可能なようにも思える。しかし，実際は，紙の業務プロセスで想定するリスクとは相当異なるため，内部統制構築にあたっては慎重に判断する必要がある。

前述のPDFによる不正の中には，上記のような，改ざんやなりすましに対するリスクを十分に想定しなかったことで，必要な統制が設定されなかったことに起因している事例がある。

また，紙とハンコの世界では，原本は１つのため，会計伝票の原本と紙の証憑の原本は常に１対１で対応し，同じ場所にとじられて保管される。そのため，原本の証憑を用いないで会計処理されるリスクは構造的に難しいという点が一般的に言われている建付けである。

一方で，PDFを証憑とする場合は，原本もコピーも違いがないため，必ずしも電子伝票と同じ場所に保管する必要性がなく分散管理されやすくなる。そこで，新たに電子伝票とPDF証憑が１対１で対応することを確認できる管理手法が必要な点に留意すべきである。

〔図表１〕証憑の種類の相違による管理上の長所・短所

	管理上の長所	管理上の短所
紙	・改ざんや複製には技術を要するため比較的困難 ・押印等を組み合わせることでなりすましも比較的困難 ・原本性を維持したまま納品情報，支払情報等を付記できる ・会計伝票との1対1対応での管理がしやすい ・災害，盗難等物理的な紛失リスクは低い	・原本は１つ（１カ所にしか保管できない） ・実物があり保管コストが大きい ・バックアップをとりにくい ・回付に時間がかかり意思決定が遅くなる ・効率的な情報管理のためには紙の内容をテキストデータに変換しなければならない ・紛失した場合に元に戻らない可能性が高い
PDF	・必要な場所に瞬時に送付でき意思決定が早い ・複製が可能なため同時に複数で情報共有が可能 ・分散して保管できる ・実物がないので保管コストが小さい	・改ざん，なりすましが容易（ただし，改ざん防止措置は可能） ・原本性を維持したまま情報を付加できないため，別途文書管理システムが必要な場合がある ・効率的な情報管理のためには PDF の内容をテキストデータに変換しなければならない ・複製が可能なため会計伝票との1対1対応に工夫が必要 ・紛失リスクが高いためバックアップ等対策が必要 ・電子メールを利用している場合，類似ドメインを利用したなりすましのリスクを想定する必要がある
EDI 等	・PDF 同様意思決定が早い ・適切に設計された場合，誤謬や不正が起こりにくい環境を創出できる ・カスタマイズ可能な場合，改ざん，複製，なりすましの防止を始めとした様々な機能（管理情報の付加，会計システムとの自動連携等）を構築できる	・設定するまでに時間とコストがかかる ・利用できる場面が制限されるなど汎用性が低い ・設計を誤ると，適時の修正が困難など，想定を上回る誤謬が発生する可能性がある

⑵ 情報の転換点

情報の転換点とは，たとえば，紙の情報をシステムに直接入力するなどの場面を指し，このようなタイミングでは一般的に誤謬が起きやすいため内部統制上注意が必要である。紙の情報をシステムに入力する，PDF の内容を OCR を介してシステムに入力する，EDI システムと会計システムを API 連携するなど，あらゆる場面で情報の転換点は存在する。

前述の PDF の改ざんによる不正では，紙の情報を改ざんして PDF 化しており，紙を PDF 化するという情報の転換点を利用した不正である。また，受領した PDF を加工して経理部に提出した事例もある。

情報の転換点に対する統制には，情報の転換点ごとに確認する方法や，最終的に管理される情報と原始情報の整合性を確認する方法などがいろいろ考えられる。

その際には，原始情報が正しいかどうか，なりすまし防止の観点も内部統制上必要となる。

前述の PDF のなりすましによる不正では，営業担当者が取引先に類似した偽ドメインを作成し，そこから送付されてきた PDF 証憑を正として経理部門に提出した事例である。

これに対して，あえて情報の転換点を企業内に置かない方法も考えられる。

紙の証憑や PDF を自社で受け取らず，アウトソーシング業者に受領を委託し，当該業

者が文書管理システムにPDF化して格納し，改ざんできない格納されたPDFをスタート地点として，委託者である企業は業務プロセスとして利用する。なお，アウトソーシング業者が提供するサービス内容を評価する内部統制は別途必要になる。

⑶ 取引の性質

取引の性質によっては，その証憑にしか記載されない取引情報が重要な場合もある。また，その証憑以外からも同じ取引情報を入手でき，その証憑自体にそこまで重要性がない場合もあるため，それぞれの取引の性質に合わせた内部統制の構築が望まれる。

①証憑からしか入手できない取引情報

その証憑でしか取引日を確認できないような場合，容易に改ざん可能なPDFを添付した電子メールのやり取りのみで業務プロセス上問題がないか十分な検討が必要である。

そのような場合，EDI等のシステムを業務プロセスとして導入することを検討する可能性がある。また，クラウドサービスのような電子契約システムを利用して電子検収書を作成し取引先から電子サインを受領する方法もある。

システムを通じて取引先情報がマスター登録され，マスター登録された取引先からしか入手できない検収情報が，テキストデータまたはPDFとして自動的にシステム内に保存される場合，なりすまし，改ざんに対して一定の防止効果を発揮できると考えられる。

②証憑以外から入手できる取引情報

取引情報をPDFで受領した場合，前述のとおり，発信元が信頼性を保証するケースはまれであり，なりすまし，改ざんが比較的行いやすい環境であることを前提にすると，PDF以外から入手できる情報との整合性を確認できる仕組みを構築することが，内部統制上有効といえる。

そもそも企業の取引は，開始から完了に至るまでに様々な証憑を介して段階的に意思決定されており，申請者が添付した証憑の内容を，管理部門が別ルートから入手した情報と照らし合わせて当該取引の実在性を裏づけて承認するケースは多いと考えられる。

また，PDFによる取引証憑の受領行為を取引担当者のみとせず，同時に管理部門も受領する設定にして，取引の透明性を高める方法も不正や誤謬の防止に役立つ。

2 統制活動

日常の業務プロセスの過程でどこまでの職責を各担当者に課すかは論点となる。業務プロセスの途中で紙の証憑からPDFに変換されている場合，常にPDFと紙とを突合する職責を日常の決裁業務に携わる担当者に課すとしたら，PDFで業務を効率化したにもかかわらず，内部統制により，むしろ業務の効率性を著しく下げる可能性がある。一方で，不正の事例のようにリスクを顧みず，送られてきたPDFになりすまし，改ざんはないと何の根拠もなく通してよいものかは内部統制の設計上慎重に検討しなければならない。

この点で，内部監査部門によるモニタリングとしてPDF証憑の真正性の確認を強化することは，管理部門の負荷を軽減し，業務の迅速な意思決定を維持しつつ，内部統制の有効性を確保できる可能性があると考えられる。

3　IT への対応

DX と IT への対応は密接に結びつく。スキャナ保存制度，PDF，EDI，Peppol 等を利用するには，それらで利用されるシステムが統制目標を達成できる機能を有しているか確認する必要がある。

システムの評価は，IT 基盤に対して行う IT 全般統制の評価と，IT 基盤の上で稼働するアプリケーションシステムに対して行う IT 業務処理統制の評価の２段階で行われる。

IT 基盤に対する IT 全般統制の評価対象は，主にアクセス権管理，プログラム変更管理，システム運用管理（バックアップ等）の３つである。

アクセス権管理とはシステム上の職務分掌，職務権限の管理である。システムは同じプログラムが変更されない限りずっと同じ処理をし続けるため，プログラムが勝手に変更されない仕組みになっていることを確認するのがプログラム変更管理である。そして，システム運用管理として，不測の事態に対してバックアップ等で復旧できる体制が確保されていることも確認しなければならない。

IT 基盤の上で稼働する IT 業務処理統制の評価とは，認識したリスクに対して，システムとして具体的に有効に機能しているか確認することである。IT 全般統制とは異なり，企業が想定する個別具体的なリスクに対して，システムの仕様が当該リスクを合理的に低減するデザインとなっているか，そして，そのデザインどおりに実際に機能しているかを確認する。たとえば，改ざん防止機能のあるシステムの場合，そもそも編集できない機能になっているか，編集できたとしても編集内容と編集履歴が残る機能になっているか等を個別に確認することである。

システムベンダー等の委託先が，上記の改ざん，なりすまし防止等のシステム機能を内部統制として提供している場合，単に機能があるという事実だけをもって内部統制の有効性を推察することはできない。リスクを評価し，そのリスクに応じた対応手続を行う必要がある。

《おわりに》

現在のデジタイゼーションは道半ばである。しかし，今後，信頼できるデータ基盤をどの企業も当たり前のように構築できるようになった際には，デジタライゼーションが企業の優位性の源泉になる。

現在，EY 新日本有限責任監査法人は Assurance4.0 を掲げ，わが国の Society5.0 を見据えた次代の監査，そしてデジタル社会に期待される保証サービスへの挑戦を行っている。

DX の次の段階であるデジタライゼーションにおける挑戦の１つとして，われわれ EY は，大量データを利用した分析手法であるプロセスマイニングを活用した次世代の内部統制評価方法を検討している。本誌であわせて寄稿しているので（加藤・原稿58頁），ぜひご一読願いたい。