ID カードの券面セキュリティ・ハンドブック

Handbook for Security Features on ID Cards

平成 31 年 2 月

独立行政法人 国立印刷局 作成

目次

ページ

まえがき

本書は，安全・安心な本人確認を脅かす ID カードの偽変造，なりすまし等の不正行為対策のためのハンドブックとして独立行政法人国立印刷局による原案作成の後，次世代 IC カードシステム研究会（会長：大山 永昭 氏）による査読（平成 26 年 12 月～平成 27 年 3 月），その他外部関係者による再査読（平成 30 年 9 月～平成 31 年 1 月）を経て作成された。本書の作成に当たり，既存の関連文書である“公的分野における連携 IC カード技術仕様（改定）”（ 平成 14 年 3 月 26 日に制定後，平成 16 年 3 月 12 日に仕様の見直し及び追加したもの）の中でカード券面の物理仕様の参照情報として規定される“連携 IC カード券面の偽造防止技術ハンドブック”（平成 14 年 7 月）の記載内容を十分に考慮した上で，大幅な増補を行い，包含するものとした。

本書の一部が，特許権，出願公開後の特許出願又は実用新案権に抵触する可能性があることに注意を喚起する。独立行政法人国立印刷局は，このような特許権，出願公開後の特許出願及び実用新案権に関わる確認について，責任はもたない。

ID カードの券面セキュリティ・ハンドブック

Handbook for Security Features on ID cards

序文

“連携 IC カード券面の偽造防止技術ハンドブック” （平成 14 年 7 月）の初版発行から十余年の経過とともに，カード券面のセキュリティに対する脅威，カードへ実装可能な対策技術等が大きく変化した。こうした状況を受け，多様化・巧妙化するカード利用時の不正へのリスク対応の見直しを行い，券面セキュリティの更なる向上等を目的とし，本書を作成した。

1　適用範囲

本書は，行政手続，民間取引等における安全・安心な本人確認を実現するための ID カード券面のセキュリティ設計及び ID カードの製造・発行・利用等の各プロセスにおいて実施すべき対策事項のための包括的指針である。主にカードの要求仕様作成者が仕様の作成時に，カード券面等のセキュリティを確保するための要求事項を策定することに役立てることを目的としている。

本書は，カード券面のセキュリティ仕様の設計を始めとし，カードのライフサイクル全般おけるセキュリティについて記載したものである。カード内の IC 等に記録された電子情報におけるセキュリティは，適用除外とする。

また，券面セキュリティを実現する上で，特定分野の偽変造対策技術及び個別の製品・サービスを推奨するものではない。

2　用語及び定義

主な用語，分類及び定義は，次による。

2.1　カード関連

2.1.1　ID カード カードを使用するに当たって，取引処理のために必要な入力データを記録することが可能な，カードの保有者及び発行者を識別するカード。

注記 1　識別カード - 物理的特性 JIS X 6301（ISO/IEC 7810） による。

注記 2　エンボス付きカード，写真付きカード，磁気カード，IC カード等が採用されている。また，OCR-B 書体と写真とを組み合わせた機械可読式パスポートカードが規格化されている。

2.1.2　IC カード　1 個以上の IC を内蔵する **JIS X 6301** に規定された ID-1 サイズのカード。例えば，外部端子付き IC カード，非接触 IC カード，ISO 型 IC メモリカード，表示付き IC カード及びこれらを組み合わせたカードがある。

注記　外部端子付き IC カードの物理的特性 JIS X 6320-1（ISO/IEC 7816-1）による。

2.1.3　未発行カード　個人情報の記録又は試験作業に使用されていないが，使用目的のために要求されたすべての構成要素を備えたカード。このカードは温度衝撃なしで，温度 5℃～30℃，湿度 10%～90%の清浄な環境で，48 時間以上日光に当てないように保管する。

注記　**識別カード - 物理的特性 JIS X 6301**（**ISO/IEC 7810**）では，“未使用カード”の語として定義されるが，本書では，カード製造業者その他一般読者の理解を考慮し，“未発行カード”とした。

2.1.4　カード券面　カード記載情報が印字，印刷又は付与されるカード基材における，おもて面又は裏面。

2.1.5　カード記載情報　カード券面に印字，印刷又は任意の方法によって付与される，カード名称，カード発行者名，顔写真，保有者氏名，カード番号，有効期限等のカードの識別のための情報。

2.1.6　カード番号　カードの特定が可能な番号。

注記　**ICAO, Doc 9303 Part 1: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs** における“Document number”の語句に対応する。

2.1.7　管理番号　カードの製造時に記録の保持及びセキュリティ確保のためにカード等に割り当てられる番号。

注記　**ICAO, Doc 9303 Part 1: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs** による。

2.2　カードのライフサイクル

2.2.1　ライフサイクル　システム，製品，サービス，プロジェクト又は人が作った他の実体の構想から停止までの漸進的な変化。本書では，プロセス全般における，セキュリティ向上のための，考慮をすることが望ましい事項について記載する。

注記 1　**システムライフサイクルプロセス JIS X 0170**（**ISO/IEC 15288**）による。

注記 2　本書におけるカードのライフサイクルは，製造・発行・利用・停止の 4 つのプロセスから構成されるものとする（**2.2.2~2.2.5** 参照）。

2.2.2　製造プロセス　未発行カードの仕様設計，原材料の調達，製造，検査，試験，保管，輸送，納入等の未発行カードの作製全般に関するプロセス。

注記　記載情報の一つとして分類されるカード名称は，多くの場合，本プロセスにおいて付与される。

2.2.3　発行プロセス　未発行カードに対し，申請情報に基づき，保有者氏名，識別番号等の記載情報を付与し，機能や品質の確認をした上でカード発行の申請者に交付するプロセス。

注記　発行の形態は，“集中発行方式”と“分散発行方式”がある。集中発行方式とは，地理的に局所に設置された記載情報データベースと大量発行が可能な比較的大型の発行機によってカードを発行する方式であり，リスクの一極管理によるセキュリティ向上，効率的な在庫管理等の特長を有する。分散発行方式とは，広域に多数設置された発行機によってカードを発行する方式であり，発行の柔軟性や天災

時等における発行継続性を確保することができる。どちらの発行方式をとるかは，カードの機能要件やセキュリティ仕様，発行に関する作業適性，コスト等を考慮し決定される。

2.2.4　利用プロセス　サービス窓口におけるカード保有者の本人認証，証明のためのコピー物の作成等，カードを介した任意のサービスの取得又は供給を開始し，適切な条件下で利用するためのプロセス。

2.2.5　停止プロセス　有効期限の到来による返却，新たなカードの再発行，発行者又は保有者の返納要求等によるカードの停止と廃棄に関連したプロセス。

2.3　本書におけるセキュリティの概念

2.3.1　一般

本書における，“偽造”，“模造”等のカード券面に対するセキュリティ脅威及び不正行為の用語は，技術的見地において整理されたものであり，必ずしも，刑法における法益侵害に対して評価された結果の用例と同一とは限らない点に注意を喚起する。

2.3.2 券面セキュリティ（security features on cards）　カード券面の偽造，変造，改ざん等の不正・脅威に対し安全であること，又は不正・脅威のための対策技術。

注記　偽造，変造，改ざん等の不正行為の総称として，一般的には，“偽造”又は“偽変造”の語句が用いられる場合がある。本書では，カードセキュリティに対する不正行為の総称として“偽変造”の語句を用いる。

例　通貨偽造の罪，偽造事件，偽造品，偽変造対策技術，偽変造旅券（出入国管理及び難民認定法より）

2.3.3　真正性（authenticity）　本物であること又は本物であることを確実にする特性。

2.3.4　完全性（integrity）　カード券面の記載情報に対する不正な書換え及びカード券面の構成材料の一部の取り外し・差し換えへの耐性を有するとともに，それら不正行為の痕跡を確認できる特性。

2.3.5　偽造（counterfeit, emulation）　真正品を発行する権限のない者が，真正品と同等又は類似の材料を用い，かつ，内部構造を模し，真正品と類似の外観，特性を有する偽物を作ること。

注記　多くの場合，真正品の仕様の解明又は特性の推定を経て作られる。

2.3.6　模造（simulation）真正品を発行する権限のない者が，真正品と類似の外観を有する偽物を作ること。

注記　真正品の仕様の解明又は特性の推定を経ていないため，必ずしも，内部の構造・特性まで似せられたものではない。

例　通貨及証券模造取締法，模造品

2.3.7　変造（alteration, transplant）　真正品を発行する権限のない者が，真正品の一部又は構成部品を，他の真正品又は偽物の一部と差し換え，偽物を作ること。

注記　真正品の一部又は構成部品の例として，記載情報が印刷されたカード層，ホログラムや光学的変化材料等のセキュリティ要素，表面保護フィルム等がある。

2.3.8　改ざん（tampering）　真正品を発行する権限のない者が，真正品のカード記載情報，印刷図柄等を書換え，偽物を作ること。

注記　不正な書換えの例として，空白領域への加筆，真正な記載情報の消去，消去によって獲得した領域への上書き等がある。

2.3.9　複写（copy, duplicate）　真正品を発行する権限のない者が，真正品を元にデジタルカラーコピー機等の任意の複製装置を用いて類似の外観を有する偽物を作り出すこと。

2.3.10　真偽判別（authentication）　定められた手順によって，真正品におけるセキュリティ要素の仕様と比較し，本物か偽物かを判定すること。

2.3.11　なりすまし（imposter）　ある人が他の人を装うこと。

注記　**ICAO, Doc 9303 Part 1: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs** による。

2.3.12　開示型偽変造対策技術（overt security features）　偽変造対策技術の実装及びその真偽判別方法に関する知識が，カード保有者等の全ての関係者に開示されたもの。

2.3.13　非開示型偽変造対策技術（covert security features）　偽変造対策技術の実装及びその真偽判別方法に関する知識が，鑑定者等の一部の関係者に制限され開示されたもの。

3　保護すべき資産，セキュリティ要件及び評価の指針

3.1　一般

利用プロセスにおいて想定される偽造，変造，改ざん等の脅威から保護すべき資産を特定し，対策技術に求められるセキュリティ要件及びセキュリティ設計の指針を示す。

なお，ID カードのセキュリティはライフサイクル全般で保持されなければならない。利用面で注意すべき事項（**4.2.4**）及びその他製造・発行・停止プロセスにおいて配慮すべき不正行為（**4.3** 参照）を参考に，カードの製造・発行・利用等のライフサイクル全般の対策の整理が必要である。

3.2　保護すべき資産

3.2.1　カード基材及び券面の真正性

製造及び発行のプロセスを経て完成した記載情報を含むカードは，偽物の作製が困難であり，本物であることが確認できなければならない。

なお，正規の運用として想定されるコピー機等による券面の複写物では，原本性（唯一性）が明瞭に喪失し，複写物であることが明瞭に分かることが望ましい。

注記　カード基材及び券面の原本性（唯一性）は，券面に付与された記載情報と表面保護フィルム，コート剤，背景印刷，その他のセキュリティ要素との密着性や連続性によって担保される。

3.2.2　記載情報の完全性

カード券面に付与された記載情報及びセキュリティ要素は，適切な変造・改ざん対策技術の実装によって，正当なカード発行者が付与した状態を一貫して保持しなければならない。このため，記載情報及びセキュリティ要素の付与には，物理的かつ化学的に十分な耐

久性が求められる。また，不正な消去・修正・上書き等がなされた場合を想定し，不正実行者へのけん制又は不正の痕跡の検知が可能な対策を講ずる必要がある。

なお，カード券面の記載情報と同等の情報を何らかの形で記録し，その完全性を確認できる手段を有することが望ましい。

3.3 セキュリティ要件及び評価の指針

3.3.1 偽変造対策技術に求められる要件

カード基材及び券面の真正性，並びにカード記載情報の完全性を保持するための個別の対策技術に求められる要件を整理する。

a) 対策技術に用いられる原材料の組成あるいは処方は機密扱いであり，その特性を模倣可能な代替材料の入手が困難であること。

b) 対策技術の付与・製造に用いられる装置は機密扱いであり，対策技術の特性を模倣可能な代替装置の入手が困難であること。

c) 対策技術の付与・製造の方法は，機密扱いであり，対策技術の特性を模倣可能な代替方法を見いだすことが困難であること。

d) 対策技術の原理・仕組み及び詳細仕様の解明（リバース・エンジニアリング）が困難であること。

e) 対策技術の付与・製造時の品質の差は，偽物と見誤ることがないよう，可能な限り小さいこと。

f) 使用・経年に伴うカードの外観・性質の変化（製造時のカード個体差を含む。），並びに観察環境及び真偽判別をする人（特にカード保有者）の技量の変動によらず，真偽判別等の検証が実行できること。

3.3.2 偽変造対策技術の実装の指針

3.3.2.1 一般

個別の偽変造対策技術の特性・性能，カード発行者によるカードの運用，保有者の使い勝手等の要件を十分に考慮した上で，適切なセキュリティ設計に基づき，複数の偽変造対策技術の実装が求められる。このとき，対策技術の組合せによっては，技術同士の干渉による性能低下やぜい弱箇所が発生する可能性が懸念される。

次に，各種の偽変造対策技術の実装時の留意点を指針として示す。

3.3.2.2 複数の偽変造対策技術による多重的な防御

単一の対策技術では，カード券面の十分なセキュリティを担保することは困難である。また，不正行為の手段として用いられることが多い複製機器等は日進月歩で高性能化することから，カードの新規発行からの経年による耐偽変造性能の低下のリスクを考慮する必要がある。

この問題への対処として，複数の対策技術を実装し，脅威に対する券面セキュリティを段階的に保護する仕組みが必要である。これによって，単一の対策技術に依拠した場合の急激なセキュリティ危たい化を回避することが可能である。

具体的には，**6.2** で示す真偽判別方法による技術分類（第 1～第 3 認証技術）において，

特定の分類の技術に偏ることなく全ての分類からそれぞれ複数の技術を選定し，多重的な防御の仕組みを実現することが望ましい。

3.3.2.3　偽変造対策技術の多面的な実装

多面的な実装とは，カードに実装された複数の対策技術において，実装される部位，使用される材料及び付与方式がそれぞれ異なることをいう。実装される部位は，特定のカード構成材料に集中化することなく分散することが望ましい。また，インキと印刷版面による印刷的手法に限定されず，エンボス，レーザ加工，圧着（ラミネート，箔押し等）等の様々な付与又は加工方式による対策技術の実装が推奨される。

3.3.2.4　偽変造対策技術の相補的な実装

偽変造の様々な脅威に対し，単一の技術で全ての脅威の対策をとることは不可能である。実装の候補となる対策技術の用途及びセキュリティの特性・性能を十分に把握した上で，各技術の短所を互いに補い合うような技術の選定及び実装を図り，カード全体におけるセキュリティの一貫性を担保する必要がある。

3.3.3　カードの券面セキュリティの評価

完成したカード（試作品及びセキュリティ設計案を含む。）は，偽変造の様々な脅威に対して導出されたセキュリティ要求事項の充足度合の評価を行わなければならない。これらの評価は，セキュリティ評価や分析鑑定に関する十分な技能と知見を有した複数の熟練者によって実施されるべきである。実施すべき内容は，特定の偽変造を想定した模擬的な複製実験，又は偽変造品の作製に要する工数，装置，材料，知識等の偽造資源の見積りに基づく偽変造の採算性に関する検証である。

4　想定される不正行為

4.1　一般

カードのライフサイクルにおいて，想定される主な不正行為を示す。具体的な事例は，不正行為をじゃっ起するため示さない。

なお，記載の順序は，不正の発生頻度及び典型性を考慮したものではない。

4.2　利用プロセスにおける不正行為

カードの真正性及び券面の完全性を脅かす多様な脅威を示す。また，カード券面のセキュリティ仕様と直接的な関連はないが，運用面で想定されるカードを介した詐欺的な不正行為に関し，注意すべき事項を示す。

4.2.1　カード券面の偽造

a) カラーコピー機等の複製装置によって複製されたもの。

b) DTP（Desk Top Publishing）等の手段によって作成・出力されたもの。

c) 不正入手した真正材料又は類似の材料を利用したもの。

4.2.2　カード券面の変造

a) 券面の記載情報の一部又は券面全体を除去し（剥離など），他のカードの該当部位又は券面全体と差し換えたもの。

b) 偽の情報が付与されたシールを真正なカード表面に貼付したもの。シール化された顔写真やロゴマーク等が想定される。

4.2.3 カード券面の改ざん

a) 空白領域に偽の情報を加筆したもの。

b) 券面の記載情報の一部又は全面を消去し，偽の記載情報を上書きしたもの。

4.2.4 カードの利用面で注意すべき事項

a) **なりすまし** 偽物のカードを用い，架空又は実在する人物を装う場合と本物のカードを用い，他の人物を装う場合がある。

b) **偽装カード** 不正実行者が，カードの発行目的及び仕様を熟知しない民間サービス提供者[1)]に対し，架空の真正ではないカードを提示し，運用を欺くことが想定される。

注[1)] 民間サービス提供者とは，特定の取引時に本人確認を伴う金融機関，携帯端末販売店，古物商，レンタル店等である。

c) **カードのすり換え** 民間サービス提供者の要求に対して差し出された真正なカードが，偽物とすり換えられ，カード保有者に返却されることが想定される。

4.3 その他製造・発行・停止プロセスにおける不正行為

a) 製造工程，製品の輸送，カード発行・保管施設等，サプライ・チェーンの全てにおける未発行カードの窃盗。

b) セキュリティ原材料，中間製造品，廃棄物等の数量偽装。

c) 水増し製造，横流し，廃材再利用等の内部不正。

d) カード申請のデータ入力，保存データベース，ネットワーク等を含む発行管理システム全体における不正アクセスや不正オペレーション。

e) 本人確認書類の偽造や改ざんによる，なりすましの申請。

f) 停止されたカードの全体又はセキュリティ要素の再利用。

5 ユーザ定義及び真偽判別方法の分類

5.1 一般

偽変造対策をより確実に，かつ，効率的に実行するためには，想定されるユーザの定義・区分，及び各ユーザに適した真偽判別方法の分類を明らかにする必要がある。本書では，カードの真偽判別等を実行するユーザを，一般利用者（**5.2**），特定利用者(**5.3**)及び鑑定者（**5.4**）の 3 つに区分する。また，各ユーザの有する資源，特徴及び要件を考慮した上で，対応する真偽判別方法の分類を示す。

5.2 一般利用者

本区分は，カード保有者及び民間サービス利用者である。一般利用者に適切な不正対策は，第 1 認証技術（**6.2.1**）である。

一般利用者は，真偽判別に適した光源や照度の環境，判別のための十分な時間，知識及び器具を有さないことが想定される。そのため，直観的又は瞬時に真偽判別が可能な第 1 認証技術の利用が適切である。

なお，一般利用者には，視覚及び色覚に障害のある人々が含まれる。触覚応答が可能なものやハイコントラストに色彩・明暗設計されたセキュリティ要素を利用し，可能な限り，検証手段の代替性を確保することが望ましい。

5.3 特定利用者（職員，検査官等）

本区分は，規定のサービスを供給する職員，窓口業務者，検査官等である。特定利用者に対応する対策技術は，第 1～第 3 認証技術（**6.2.1~6.2.3**）の全てである。

特定利用者は，利用者から提示されたカード又は利用者へ交付するカードの真正性及び完全性（本人確認を含む。）の検証の責務を負う。そのため，検証のための十分な時間，特定の知識 **2)** 及び必要な器具・装置を有している。特定利用者は，これらの資源に基づき，第 1 認証技術に加え，第 2，第 3 認証技術による検証の多重化によって真偽判別の確実性を高めることができる。

注 2) 特定の知識とは，非開示型偽変造対策技術（**2.3.13**）の特性・性能に関する情報である。

5.4 鑑定者（券面セキュリティ設計者，公的調査分析機関等）

本区分は，券面印刷におけるセキュリティ仕様の設計者，異同判定の高度な専門知識を有する公的調査分析機関の職員等である。真偽等の判定に関し，一般利用者及び特定利用者では，検証が困難な疑義対象の最終的な判定を担う。

なお，本区分に対応する対策技術や判定要素は機密扱いである。

6 偽変造対策技術の分類

6.1 一般

カードの偽造対策技術，及び変造・改ざん対策技術には，様々なものがある。適切な技術の分類によって，カード全体のセキュリティ設計の精度向上及び効率化を図ることができる。

偽造対策技術は，その真偽判別方法の観点からの分類が一般的である **3)**。本書もこれに従い，第 1～第 3 認証技術の 3 つの分類（**6.2.1~6.2.3**）を定義した。

変造・改ざん対策技術は，カード本体及び券面記載情報の一貫性を保持するための技術である。記載情報・セキュリティ要素を保護する技術（**6.3.1**）と不正実行者へのけん制及び痕跡検知（**6.3.2**）とに大別される。

注 3) Rudolf L. van Renesse, Optical Document Security, 2nd ed., Artech House Publishers, 1997, pp. 60-61 (ISBN 0-89006-982-4)において，”First line inspection”, “Second line inspection“及び“Third line inspection“の語句が使用される。

6.2 カード基材及び券面の偽造対策技術

6.2.1 第 1 認証技術

真偽判別の検証者の感覚（一般に視覚及び触覚）によって真偽判別が実行可能な技術のことである。例として，観察角度の変化によって印刷模様，色彩等が変化するもの，カード基材の特殊エンボス加工，レーザ加工等による独特な凹凸形状によって真正性の確認を

行う技術がある。

6.2.2　第 2 認証技術

倍率 10 倍程度以上のルーペ，特殊フィルタ，紫外線ランプ等の簡易な器具を用いて真偽判別を行う技術のことである。例として，ルーペによって確認が可能なマイクロ文字等の微小な印刷図柄，特殊な光学フィルタ越しに発現する潜像模様，紫外線ランプによって発光効果の確認が可能なインキがある。

6.2.3　第 3 認証技術

カードの構成材料が有する物理的な特徴量を機械的に検出し，真偽判別を行う技術である。例として，電磁気，光学的特性等を利用した技術がある。

なお，**注 3)**の参考文献では，本書における第 3 認証技術と第 2 認証技術とを併合し第 2 認証技術と分類した上で，“鑑定要素”を第 3 認証技術と分類しており，本書における分類とは若干異なる点に注意を喚起する。

6.3　カード券面の変造・改ざん対策技術

6.3.1　券面の記載情報及びセキュリティ要素の保護技術

物理的な研磨・切取り，化学薬品を用いた溶解除去等の不正行為から，券面の記載情報及びセキュリティ要素を物理的又は化学的に保護する仕組みである。記載情報の付与表面における頑強な保護層の積層，耐溶剤性の優れた材料等の使用がある。

6.3.2　不正のけん制及び痕跡検知のための技術

化学薬品を用いた不正な消去に対し，印刷インキ・基材に色の変化及び“にじみ”が発生し，不正実行者へのけん制と不正の痕跡検知を可能とする技術である。また，セキュリティ要素の取り外しへのけん制として，微弱な力で容易に破壊され，再利用を不能とする特殊なぜい弱性加工の技術，加圧や引っ張りの力を検知して発色する材料の実装等がある。

なお，けん制及び痕跡検知を可能とする対策技術は，経年劣化，一部の日常薬品，急激な温湿度変化，直射日光等の外界からの負荷によって，想定外の変化が生じてしまうことがある。カードの耐用保証期間における前記事例の発生のリスクについて配慮すべきである。

7　偽変造対策技術の具体例

7.1　一般

箇条 **6** に示した偽造対策技術及び変造・改ざん対策技術の各分類について，特徴・機能によって細分類した上で，それらの技術の代表例を示す。

7.2　偽造対策技術の具体的説明

a)　第 1 認証技術の細別，特徴・機能及び代表例を**表 1** に示す。

表 1－第 1 認証技術の細別

細別	特 徴 ・ 機能	代表例
意匠的要素	・特殊な印刷技術を用いて作製され，複製・複写を困難にする図柄パターン等であり，視覚的に容易に真偽判別が可能なもの。 ・カードの名称，保有者情報，原本性（唯一性）等を容易・確実に認識できるもの。	レインボー印刷，特殊画線（複写対策画線等），2 色の地紋・彩紋パターン，ロゴマーク，特殊フォント
光学的要素	・プロセス印刷では再現困難な色によって，視覚的に容易に真偽判別が可能なもの。 ・観察角度に応じた色や画像の変化によって，視覚的に容易に真偽判別が可能なもの。	特色インキ，ホログラム，光学的変化材料，潜像模様
形状的要素	・券面に凹凸等を形成する技術によって，触覚的，視覚的に容易に真偽判別が可能なもの。	エンボス加工，レーザ加工，凹凸付与，穿孔

b)　第 2 認証技術の細別，特徴・機能及び代表例を**表 2** に示す。

表 2－第 2 認証技術の細別

細別	特 徴 ・ 機能	代表例
意匠的要素	・ルーペ等の拡大器具を用いることによって，真偽判別が可能なもの。 ・モアレ等を発生する特殊フィルタを用いることによって，真偽判別が可能なもの。 ・レンチキュラレンズ等をかざすことで，特定の微小画像を拡大し，視認可能な図形として出現させることによって，真偽判別が可能なもの。	特殊画線（耐複写性を有した微細模様等），マイクロ文字，特殊形状スクリーン，補助器具を用いることによって出現する潜像模様
光学的要素	・特殊な光学特性を示す材料を基材・ラミネートフィルム・インキ等に混入し，特殊フィルタ，紫外線ランプ，赤外線可視化装置等の補助器具を用いることによって，真偽判別が可能なもの。	発光基材・発光ラミネートフィルム・発光インキ，サーモクロミックインキ，フォトクロミックインキ，赤外線を利用した潜像模様

c) 第 3 認証技術の細別，特徴・機能及び代表例を**表 3** に示す。

表 3－第 3 認証技術の細別

細別	特 徴 ・ 機能	代表例
電磁気・光学的要素	・電磁気又は光学特性を示す材料を基材・ラミネート・インキ等に混入し，検出機器を用いて，真偽判別が可能なもの。 ・コード化した特定の情報又は通信特性を有するタグ，又は印刷パターンを付与し，電磁気・光学検出機器を用いて，真偽判別や認証が可能なもの。	発光材料，磁性材料，電磁気・光学的認識要素，OCR，磁気バーコード，電子透かし

7.3 変造・改ざん対策技術の具体的説明

変造・改ざん対策技術の細別，特徴・機能及び代表例を**表 4** に示す。

表 4－変造・改ざん対策技術の細別

細別	特 徴 ・ 機 能	代表例
情報及びセキュリティ要素の保護	・物理的な研磨及び切り取り又は化学薬品を用いた溶解除去等から，記載情報及びセキュリティ要素を物理的又は化学的に保護するもの。	カード記載情報をカードと一体構造的にする技術，顔写真付与領域と重複した彩紋状の背景パターン，保護材料の塗布，保護フィルムのラミネート
変造・改ざんの検知の仕組み	・カード券面に対し，物理的又は化学的な不正な加工がなされた場合，不正実行者に対するけん制及び加工の痕跡が検出できるもの。	不正な加工による図柄の消失，変色，材料の変形・破壊，脆弱性の加工（ミシン目，スリット等）

8　偽変造対策技術のリスト及び選定基準

8.1　一般

カード券面のセキュリティを十分に担保するためには，箇条 **7** に示した対策となる技術から複数の技術を選定し，効果的に組み合わせた上で実装することが望ましい。

本書では，**ICAO, Doc 9303 Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs** に規定された 2 段階の選定基準である“Basic Features”と“Additional Features”に基づき，対策技術のリスト[4)]を示す。“Basic Features”と“Additional Features”の語句は，それぞれ，本書における“基本技術”と“追加技術”に相当する。ここで，“基本技術”は“基本的な対策として，選択的に一つ以上の実装が推奨される技術”，“追加技術”は“任意の追加的な対策として，選択的に実装が望ましい技術”と解釈される。

なお，偽変造対策技術の選定とカード全体のセキュリティ設計の詳細仕様の策定に当たっては，“**3.3.2　偽変造対策技術の実装の指針**”も参照することが望ましい。

注 4)　リストに示される候補技術は，我が国のカード製造者における供給実績を考慮し，一部の候補技術の取捨選択がなされた。

8.2　カード基材及び未発行カードに採用することが望ましい技術

8.2.1　カード基材のための技術

8.2.1.1　基本技術

カード基材の製造又は選定において，基本的な対策として，券面への蛍光材料[5)]の付与を考慮し，その特性や性能を阻害しない UV 不活性等の基材を使用することが推奨される。

注 5)　例として，蛍光ラミネートフィルム，蛍光インキがある。

8.2.1.2　追加技術

a)　カード基材又は保護ラミネートフィルム中の可視又は不可視のセキュリティ要素の実装

b)　カード表面層の触覚技術

触覚技術の実装は，機械読取技術及び記載情報の可読性を阻害しないこと。

8.2.2　券面印刷等に関する技術

8.2.2.1　基本技術

a)　2 色の地紋・彩紋パターン

b)　レインボー印刷

c)　特殊画線（複写対策画線等）

耐複写性については，模様細部の精確な複製を困難にする技術及び複写物であることを明確にする意図の技術がある。カードの運用方法を考慮した上で適切なものを選定することが望ましい。

d)　マイクロ文字

8.2.2.2　追加技術

a)　ロゴマーク

b)　特殊フォント

c)　意図的な誤字又は誤スペル（マイクロ文字による隠し文字を含む。）

d)　特殊形状スクリーン

e)　立体的レリーフパターン

f)　ホログラム

g)　光学的変化材料

h)　潜像模様（補助器具等の使用によって視認可能なものを含む。）

i)　光学的認識要素（OCR，バーコード，電子透かし等）

8.2.3　インキに関する技術

8.2.3.1　基本技術

カード券面の印刷で用いられるインキにおいて，基本的な対策として，無色又は有色の発光インキの実装が推奨される。

8.2.3.2　追加技術

a)　光学的変化インキ

b)　メタメリックインキ

c)　赤外線透過インキ

d)　赤外線吸収インキ

e)　燐光インキ

f)　タグインキ，特殊マーカ

g)　サーモクロミックインキ

h)　フォトクロミックインキ

8.3　カード記載情報のための技術

8.3.1　記載情報の付与方法に関する技術

8.3.1.1　基本技術

記載情報の付与装置は，民生用装置では利用できない一つ以上の偽変造対策技術又はその発行プロセスの唯一性を確認できるような特殊材料を利用できることが望ましい。また，カード発行装置の選定には，発行枚数，カードの構成，カードの全製造工程における発行プロセスのタイミング等の複数の要因を考慮する必要がある。どのような装置が選定された場合においても，保護フィルムのラミネート，記載情報と基材の一体化技術のような記載情報の変造・改ざん対策を講じることが望ましい。

a)　電子写真印刷

b)　熱転写印刷

c)　インクジェット印刷

d)　写真転写方式

e)　レーザ加工

8.3.2　カード記載情報における変造・改ざん対策技術

8.3.2.1　基本技術

a) 顔写真及びカード記載情報をカード基材と一体構造的[6)]に形成する技術

b) 顔写真付与領域と重複した彩紋模様又はその他の偽造対策パターンの印刷

c) 顔写真の頑強な付与技術

注[6)] 一体構造的とは，インキ，基材，セキュリティ要素等の各構成材料が頑強に密着，連続する様をいう。

8.3.2.2　追加技術

a) 改ざん検知機能を有したラミネート保護又は保護材料の塗布

b) 顔写真上に付与されたホログラム等光学的変化技術（顔写真の判別性を阻害しない）

c) カードとひも付けされたステガノグラフィ技術

d) カード保有者の 2 次的な顔写真（印刷的手法又はその他任意の加工技術による）

e) IC の拡張的なデータ保存領域への券面情報の保存

f) 生体特徴の機械認証技術

g) エンボス加工

h) 凹凸付与

i) レーザ加工

j) 穿孔（カード基材における一定の強度低下が想定される点について，仕様作成者は配慮すべきである。）

8.3.3　耐複写性のための技術

8.3.3.1　基本技術

耐複写性の基本的な対策として，複写対策画線の実装が推奨される。

8.3.3.2　追加技術

a) 特色インキ（プロセスカラー・インキでは再現困難な色相のもの）

b) ホログラム等の光学的変化を有する保護フィルムのラミネート層

c) 特殊インキ（**8.2.3** 記載の技術を参照すること）

9　その他不正対策実施事項のリスト及び選定基準

9.1　一般

カードのライフサイクル全般におけるセキュリティを確保するためには，カード券面のセキュリティ仕様と直接的な関連はないが，製造，発行，利用等の各プロセスにおいて適切な実施事項を策定し施行することが望ましい。

本書では，**ICAO, Doc 9303 Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs** に規定された 2 段階の選定基準である“Basic Measures”と“Additional Measures”に基づき，実施事項のリストを示す。“Basic Measures”と“Additional Measures”の語句は，それぞれ，本書における“基本対策”と“追加対策”に相当する。ここで，“基本対策”は“基本的な対策として，選択的に一つ以上の実施が推奨される事項”，

“追加対策”は“任意の追加的な対策として，選択的に実施が望ましい事項”と解釈される。

9.2 未発行カード及びカード構成材料の窃盗，並びにその他不正の対策

9.2.1 基本対策

a) カードの配達・配送，製造，保管庫及び発行装置へのアクセス制御機能を有した建屋の物理的対策

b) 全ての原材料の計数と使途管理（使用，不使用，不具合，仕損）を含む完全な監査及びその監査記録

c) カードの製造から発送までにおける，全ての未発行カード及びセキュリティ上の考慮を必要とする材料は，完全な監査の下で管理番号を付与し，管理すること。

d) 未発行カードの紛失及び盗難の情報は速やかに関係者間で共有すること。

e) カードの製造・発行システムにおける，内部不正防止のための管理体制

9.2.2 追加対策

a) 未発行カード及び主要構成材料の護衛付きの配達・配送

b) カードの製造及び発行の集中化

c) テレビカメラによる全ての製造エリアの監視及び記録

d) ステガノグラフィ等のデジタルセキュリティ技術の採用によるカード発行のトレーサビリティの確保が可能なコンピュータシステムの導入

e) 停止カードの管理

9.3 カードの発行及び発行手続における内部セキュリティの確保

9.3.1 基本対策

a) 発行申請用データ及び申請書の取扱・保存は，発行までの全ての工程において，情報の完全性が保証されること。また，保存された情報の不正な書換えを防止するための対策をとること。

b) カードの交付に先立つ機械読取機能の検査，及び本人とカードの原本性（唯一性）に関する相互参照（開発製造元と発行者間，又は発行者とカード申請者間）

c) 一個人の裁量だけでは発行不可能な形態であること。

d) 発行プロセスにおける全アクティビティの監査証跡を保存すること。申請書及び申請者データの扱い時，又はデータベースの処理実行時には，これらの操作を実行する者の署名又は作業権限に関連する本人確認を行うこと。

e) 監査証跡の完全性は，アクセス権管理，暗号化等の適切な手段[7)]によって保護されること。

注[7)] 情報セキュリティ対策のための統一基準，運用に関する指針等は，内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）によって策定された次の文献を参照することが望ましい。
http://www.nisc.go.jp/active/general/kijun30.html（**「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」**について）

また，情報セキュリティ・システムを構築する上で採用すべき暗号アルゴリズム，仕様書等の詳細については，CRYPTREC（Cryptography Research and Evaluation Committees）による次の文献の参照が望ましい。

http://www.cryptrec.go.jp/method.html（**CRYPTREC 暗号の仕様書**）

9.3.2 追加対策

a) カード発行の意思決定は，所掌官庁の担当官及び身元確認を行うためのデータベースを配備してなされること。

b) カード発行の申請時及び交付時の両方において，厳格な申請者の本人確認を行うこと。

c) 発行申請及びカードの取扱い過程において，職員の共謀による不正行為の阻止・監視ができるような職員の任命と配置をすること。

d) 発行工程の集中化

e) 生体認証ログインツールを利用したカードの発行装置への厳格なアクセス管理

9.4 カードの真偽判別及び利用プロセスにおけるセキュリティ

9.4.1 基本対策

a) 規定の本人写真は，正規のカード保有者の様相を確実に表していること。

b) カードの真偽判別を行う窓口業務者の教育及び訓練（カードの利用及び経年に伴う見かけ上の真正性の低下に影響されないこと。）

c) 紛失，盗難，不具合又はその他セキュリティの低下が懸念されるカードの検索及び照合機能を備えたデータベース

d) 開示型対策技術と非開示型対策技術の区分に関する機密性の確保

9.4.2 追加対策

a) 生体認証によるカードと保有者の関係性（ひも付け）の強化

b) 関連団体間における疑義者又は疑義カード（ブラックリスト）のデータベース

c) カード申請者の申請履歴等に関する完全な監査証跡

d) カード発行の申請書・写真及び身元確認書類への照会履歴を含む調査の記録

附属書 A
(参考)
偽変造対策技術の詳細説明

A.1　偽造対策技術

A.1.1　感覚による真偽判別 - 意匠的要素

A.1.1.1　レインボー印刷

一本のローラに，異なる色のインキを隣り合うように供給し，ローラを回転方向とは直交方向にしゅう動させることによって，異なるインキ同士を一定の領域で混色し，あたかも虹のように色が連続的に変化した印刷方式。

A.1.1.2　特殊画線（複写対策画線等）

汎用の複製機器では細部の複写再現が困難な印刷画線のこと。網点表現される複製機器では滑らかな線画表現が失われるほか，機器の入出力周波数との干渉によって特定の図柄が現れる等，目視で真偽判別が可能な画線構成がある。

A.1.1.3　2 色の地紋・彩紋パターン

異なる 2 色の彩紋要素を刷り合わせて構成されたパターンのこと。コンピュータ生成された彩紋データを用いる場合，カード上に付与された彩紋印刷物にピクセル構造が検知されてはならない。

A.1.1.4　ロゴマーク

カード発行者又は各アプリケーションを識別可能な固有のマーク等のこと。カード券面へのロゴマークの付与によって，カードの適用範囲が明示され不正利用，誤利用等を防ぐことができる。

A.1.1.5　特殊フォント

明朝体，ゴシック体等の一般的な印刷用書体とは異なる特徴と様式を備えた字形のこと。

A.1.2　感覚による真偽判別 - 光学的要素

A.1.2.1　特色インキ

シアン（藍色），マゼンタ（紅色），イエロー（黄色）及びブラック（墨色）によるプロセスカラー・インキで再現困難な色を表現するために，特別に調合・調色されたインキのこと。中間色，金属光沢，蛍光色等のインキがある。

A.1.2.2　ホログラム

主として回折，その他散乱，反射等の光学現象によって，光の強さと方向を制御することで，画像の色彩や形状の変化，又は奥行き・飛び出し・動き等の視覚的効果を有した箔，フィルム等の光学素子。微細な表面レリーフ構造や感光材料の屈折率分布差を用いて記録・量産される。

注記　ここでの“ホログラム”の語は，券面セキュリティ用途としての便宜上の呼称である。**JIS Z 8120 光学用語**におけるホログラムの定義は，“物体からできる光波と，それと干渉性がある光波との干渉パターンを写真感光材料などに記録したもの”

であり，本説明とは異なる点に注意を喚起する。

A.1.2.3　光学的変化材料

光源や観察角度を変化させることによって，印刷された画線の色，光沢等が変化する特性を有する材料のこと。例として，金，銀等の金属光沢色，パール光沢色等がある。

A.1.2.4　潜像模様

特殊な画線構成，インキ等によって潜在化された図柄が，観察角度を変えることによって，出現，又は画像が変化する模様のこと。

A.1.2.5　印刷図柄と位置同期された多階調のすき入れ

カード基材が紙の場合，カードに付与する印刷図柄と位置が同期した多階調のすき入れを施すことは，偽造困難性を更に高める効果がある。

A.1.2.6　サーモクロミックインキ

温度の変化に応じて色が変化する機能を有するインキのこと。このインキを用いて印刷した模様は，体温や任意の熱源によって色変化を呈し，目視での確認が可能となる。

A.1.3　感覚による真偽判別 - 形状的要素

A.1.3.1　レーザ加工

レーザ照射により発生する熱によってカード基材の一部を焼灼除去，膨張/収縮による変形又は変色し，文字，画像等を記録するもの。カード基材とレーザ種類の組合せによっては，カードの基材内部に記録することができる。

A.1.3.2　エンボス加工

型押し等によって，カード基材に凹凸部を形成する技術のこと。視覚や触覚で確認が可能であり，券面の記載情報やロゴマーク等がエンボス加工される。

A.1.3.3　微細凹凸加工

型押し等によって，カード基材表面に対し微細な凹凸模様を形成し，特殊な知覚効果を付与すること。

A.1.3.4　穿孔

物理的，化学的手法によって，微細な穴，凹形状を基材上に施すこと。

A.1.4　補助器具による真偽判別 - 意匠的要素

A.1.4.1　微細画線，特殊画線，マイクロ文字

ルーペで拡大することによって確認される印刷図柄のこと。例として，微小な文字（字高 150um 程度）を線状に配置したマイクロ文字がある。また，特殊な光学フィルタを使用することによって，特徴的なモアレ及び色変化が発現する画線構成，配色等がある。

A.1.4.2　特殊形状スクリーン

一般的なプロセス印刷物の網点とは異なり，三角・星形等の特殊な形状で構成された網点を用いて表現する技法である。マイクロ文字と同様に，ルーペを使用すれば，特殊な形状を確認できる。

A.1.4.3　潜像模様（補助器具によって顕像化される）

補助器具を用いずに観察した場合には図形等の潜像模様を視認できないが，レンチキュ

ラレンズ等の補助器具をかざすことで，カード券面に印刷された特定の画像が拡大され，潜像が模様として顕像化される。

A.1.5　補助器具による真偽判別 - 光学的要素

A.1.5.1　発光基材，発光ラミネートフィルム，発光インキ

電磁波，磁界，応力等を与えることによって，入射エネルギーとは異なるエネルギーを持つ光を発する基材，ラミネートフィルム，インキである。一般的には，紫外線の照射によって発する可視光を“蛍光”と称し，これを目視確認することによって真偽判別を行うものがある。セキュリティを更に高める目的で，蛍光の発光スペクトルにおいて複数のピークを持つもの，赤外線を照射し可視光を発するもの，可視光を照射し赤外光を発するもの，照射後も発光が持続する残光特性等が利用される。

A.1.5.2　フォトクロミックインキ

紫外線を照射することによって，色変化する機能を有するインキである。このインキを用いて印刷した模様は，紫外線ランプによって色変化を呈し，目視での確認が可能となる。なお，一定時間経過後に元の状態に戻る可逆的色変化を示す。

A.1.5.3　赤外線を用いることによって視認可能な潜像模様

一般の可視光線での観察下では潜像模様を視認できないが，赤外線可視化装置等の補助器具を用いることによって，潜像模様の視認が可能なもの。赤外線に対する透過・吸収特性を利用して実現する潜像技術。

A.1.6　機械処理による真偽判別 - 電磁気・光学的要素

A.1.6.1　発光材料

紫外線・赤外線等の照射によって，発光する材料のこと。例えば，発光材料を配合したインキによる印刷パターンを光学センサで読み取り，その信号を用いて，機械による真偽判別が可能である。

A.1.6.2　磁性材料

磁気特性を有する材料のこと。磁性材料が配合されたインキを用いた印刷パターンを磁気センサで入力し，機械による真偽判別が可能である。記載情報文字の認識が可能な MICR（磁性インキ文字読取方式）や磁気バーコード等に利用される。また，あらかじめ磁気テープ・磁気コートを券面に施し，記載情報等を発行時に記録することも可能である。

A.1.6.3　電磁気・光学的認識要素

電磁的又は光学的に読取可能な，文字，記号，パターン等の模様のこと。この模様をセンサで読み取り，その信号を用いて，機械による真偽判別が可能である。一般的には，OCR，磁気バーコード等がある。

A.1.6.4　電子透かし

カード券面の印刷画像の中に視認困難な形で秘匿情報を埋め込み，専用の検出ソフトを使用することによって埋め込まれた情報の取り出しが可能となる。

A.2　変造・改ざん対策技術

A.2.1　情報の保護

A.2.1.1　保護材料の塗布

ID カード券面の記載情報を改ざん行為から保護するため，記載情報を付与した後にその表面にコーティングを施す技術のこと。

A.2.1.2　保護フィルムのラミネート

ID カード券面の記載情報を改ざん行為から保護するため，記載情報を付与した後にその表面にラミネートを施す技術のこと。ラミネートの接着性が十分強固で容易に剥離されないことが必要である。

なお，ラミネートフィルムにホログラム等の機能を施すことによって，耐改ざん性を高めることが可能となる。

A.2.2　改ざんの検知

A.2.2.1　不正加工による図柄の消失，変色，材料の変形

カード券面のカード記載情報の全て，又は一部に対して行われた不正な書換え行為の痕跡を目視によって検証できるような特殊な加工のこと。化学的な対策方法として，書換えに用いられた薬剤等に反応し，カード記載情報が消失又は変色等を呈するものがある。物理的な対策方法として，フィルムの剥離や差し換え等の改変行為に対しぜい弱破壊が発生し，意図したとおりの改変を困難とするものがある。

附属書 B
（参考）
謝辞

B.1　査読委員会の招集及び査読の模様

独立行政法人国立印刷局は，次世代 IC カードシステム研究会（NICSS: the Next generation Ic Card System Study group，会長 : 大山　永昭　氏）に査読委員会の召集をお願い致しました。

主旨説明会を含む合計 6 回の委員会を開催し（平成 26 年 12 月～平成 27 年 3 月），ゆうに 20 を越える参考資料の議論を行いました。活発な意見交換を通し，大変有益な専門知識と深い洞察に富む助言を頂戴することができました。

この場を借りて，再度，お礼を申し上げさせていただきます。

B.2 券面セキュリティ関係者の招請による検討及び再査読の模様

独立行政法人国立印刷局は，外部カード関係企業等に属する合計 12 名のエキスパートをお招きし，本書の再査読を行いました（平成 30 年 9 月～平成 31 年 1 月）。

合計 3 回の対面審議のほか，100 か所以上のコメント処理を e メール等で行いました。

検討会の構成表を次に示すとともに，この場を借りて，お礼を申し上げさせていただきます。

券面セキュリティ・ハンドブック検討会の構成表（五十音順）

	氏名	所属等
（主査）	村松　正男	共同印刷株式会社
（幹事）	中澤　明	有識者
（委員）	鎌田　康昌	凸版印刷株式会社
	木村　重之	富士フイルムイメージングシステムズ株式会社
	幸城　雅之	日本データカード株式会社
	齋藤　八郎	有識者
	榊　純一	パナソニックシステムソリューションズジャパン株式会社
	野村　真義	凸版印刷株式会社
	宮野　哲紀	大日本印刷株式会社
	本松　健	株式会社 NTT データ
	山内　豪	大日本印刷株式会社
	鷲塚　純一	東芝インフラシステムズ株式会社
（事務局）	山越　学	独立行政法人国立印刷局
	齋藤　和春	独立行政法人国立印刷局
	角　憲祐	独立行政法人国立印刷局
	内田　享佑	独立行政法人国立印刷局

ID カードの券面セキュリティ・ハンドブック

解説

この解説は，本書に定義又は記載した事柄を補足的に説明するものである。

この解説は，独立行政法人国立印刷局が編集・発行するものであり，これに関する問合せ先は，独立行政法人国立印刷局である。

1　作成の趣旨

各種の行政手続や特定の商取引において，本人確認の位置付けは重要である。しかし，ID カードの偽変造や“なりすまし”によって，安全・安心な本人確認が脅かされている。

現在，広く普及する IC 内蔵型の ID カードは，暗号や電子署名等の情報セキュリティ技術によって，券面不正の検出が可能となっている。これらの技術は，IC リーダ等の機器を用いた確認が前提とされるが，ID カードの発行主体ではない，いわゆる“第三者”には十分に普及していない。そのため，第三者による ID カードの“2 次利用”（目的外利用）では，目視による券面の確認が主流となっている。また，我が国特有のリスクとして，地震・津波・洪水等の頻発する自然災害がある。このような非常時は，IC リーダ等の電源喪失や認証インフラが機能しない場合が想定され，その代替手段の確保が必要とされている。

第三者による 2 次利用時や非常時における実効性の確保の手段となるものが，券面セキュリティ（偽変造対策技術）である。多くの偽変造対策技術は，銀行券や IC 旅券と同様に，見る・触る等の人の感覚又は簡易な道具によって，カード券面の真偽判別が可能となる。適切なリスク分析に基づく券面セキュリティの設計によって，耐偽変造性の確保やカード内 IC による情報セキュリティ技術の補完が可能になることが期待される。

本書は，“公的分野における連携 IC カード技術仕様”（ 平成 16 年 3 月，仕様の見直し・追加）の中で参照情報として規定される “連携 IC カード券面の偽造防止技術ハンドブック”（平成 14 年 7 月）に置き換わるものである。本書の作成にあたっては，旧ハンドブックの記載内容を十分に考慮した上で，大幅な増補を行い，それを包含するものとした。

旧ハンドブックの発行から十余年の経過とともに，カード券面のセキュリティ脅威，実装可能な対策技術，カードに求められる機能等が大きく変化した。また，諸外国では，国民 ID カード等のための偽変造対策技術の標準化議論が活発化し，その策定と施行が推進されている。こうした状況を考慮し，本書では，カード券面のセキュリティ向上のために，基本的な対策として券面に実装することが推奨される技術，任意の追加的な対策として実装が望ましい技術，実装の指針等を記載した。

また，本書に示された指針だけでは，時代とともに刻々と変化する不正の手口やセキュリティ脅威への完全な対処は困難である。使用者，中立者等の他分野の利害関係者を交え

た継続的な議論やカード券面のセキュリティ対策仕様の定期的な見直しが望まれる。

なお，ID カードの仕様作成時の本書への準拠は， ID カード発行者における調達要件の参照情報として位置付けることができるものの，ID カード製造者又は販売者にとって，必ずしも受注又は契約を決定する際の絶対的な根拠となるものではない。

2 “連携 IC カード券面の偽造防止技術ハンドブック”からの主な変更点

本改訂版の主旨は，カード券面セキュリティ向上のための具体的な方策を示すことである。そこで，偽変造対策に関する用語の定義及び脅威分析の精緻化，ライフサイクル，ユーザ定義等の新たな箇条を設定した上で，偽変造対策技術の選定及び実装の留意点を導出した。

次に，主な変更点について記載する。

a) 箇条 2 用語及び定義

2.3 本書におけるセキュリティの概念の新たな細分箇条による，大幅な見直し及び増補を行った。また，可能な限り，引用文献を明記した。

b) 箇条 3 保護すべき資産，セキュリティ要件及び評価の指針

保護すべき資産（**3.2**）に大幅な増補を行った。“**3.3 セキュリティ要件及び評価の指針**”の新たな細分箇条を設け，対策技術に求められる要件，対策技術の実装の指針等についての詳細説明を記載した。

c) 箇条 4 想定される不正行為

利用プロセスにおける不正行為（**4.2**），その他製造・発行・停止プロセスにおける不正行為（**4.3**）等，大幅な増補となった。

d) 箇条 5 ユーザ定義及び真偽判別方法の分類

新たな箇条として設置した。ユーザを一般利用者（**5.2**），特定利用者（**5.3**）及び鑑定者（**5.4**）に分類し，各ユーザの資源，特徴及び要件を定義した上で，各ユーザに適切な偽変造対策技術の分類を示した。

e) 箇条 8 偽変造対策技術のリスト及び選定基準

券面セキュリティ向上の具体的な方策として，新たな箇条を設置した。本書で引用した **ICAO Doc 9303 Part 2** に規定される **Security Standards**（セキュリティ標準）に基づき，推奨される対策技術のリスト及び選定基準（**8.2** 及び **8.3**）を記載した。

f) 箇条 9 その他不正対策実施事項のリスト及び選定基準

ライフサイクル全般において，ID カードのセキュリティ確保の具体的な実施事項（**9.2~9.4**）を示す新たな箇条として設置した。推奨される実施事項のリストは，**ICAO Doc 9303 Part 2** に依拠した。

3 ICAO Doc 9303 Part 2 との差異

ICAO Doc 9303 Part 2, Appendix に規定される“**Security Standards for Machine Readable Official Travel Documents（機械読み取り式渡航文書のためのセキュリティ標準）**”は，カー

ド形態をとるセキュリティ文書の世界で唯一の先行標準である。そのため，欧州，米国を始めとするいくつかの諸外国では，国民 ID カード，当該国家職員カード等の券面のセキュリティ標準としての準拠がなされている。本書においても，推奨される基本的な対策及び任意の追加的な対策の候補リストは，原則として **ICAO Doc 9303 Part 2** に基づいた。しかし，前記標準は，冊子形態である旅券における査証カード（冊子形態の一部としてとじられたカード又はラベル），又は地域協定等で合意されたカード形態をとる準旅券を想定したものである。したがって，前記標準には，国際的な相互運用を前提としたいくつかのセキュリティに関する規定，又は渡航文書ならではの規定がなされている。本書の適用範囲である汎用の ID カードを考慮した場合の解釈の不整合について十分な考慮をし，適宜，修正又は割愛をした。

4　査読中に問題になった事項

本書の査読で問題となった主な事項及び議論結果は，次のとおりである。

a) 想定される不正行為の記述について

不正行為のじゃっ起及び波及につながるため，具体的及び詳細な偽造，変造・改ざん等の描写は控えることで一致した。

b) 一部の用語定義・説明のあいまいさ

1) 不正行為・セキュリティ脅威の整理

偽造，変造等の用語に関し，我が国においては，刑法における法益侵害に対して評価された結果の用例と，侵害の手段が必ずしも一致しないため，不正行為やセキュリティ脅威の類型の認識に差異があった。例えば，刑法における文書偽造の罪は“社会的信用”を保護法益としており，“他人の名義を偽って（冒用して）文書を作成すること”（大判明 43・12・20，最判昭 51・5・6）とされる。この場合，侵害の具体的手段については問わず，文書の“本質的部分”に変更を加えた場合を“偽造”とし，それ以外の場合を“変造”としており，この両方を合わせた用語として“偽変造”という用語が利用される。

一方，本書における用語の整理では，“記載情報，印刷図柄等を書換え，偽物を作ること”を“改ざん”とし，“真正品の一部又は構成部品を，他の真正品又は偽物の一部と差し換え，偽物を作ること”を“変造”としている。このように，刑法における用例は，技術的観点に基づく本書における整理とは明らかに異なったものとなっており，注意が必要である。

2) “模造”について

“偽造”の類義語として用いられることが多い“模造”の概念整理に工数を要した。**ASTM F1448 – 93a** [1] その他外国文献等において，“emulation 又は counterfeit（偽造）”と“ simulation（模造）”は，別の語とする定義がなされている。そのため，本書においても，“模造”の語を新たに定義するという結論に至った。

以下を，参考として付記する。我が国の通貨偽造罪等の法的解釈 [2] においても“偽

造”と“模造”の事実認定は慎重に扱われている。通例として，一般人に真正なものと誤認させる程度の精巧な偽物は“偽造”，その程度に達しないが，真正品と紛らわしい程度の稚拙な偽物は“模造”とするようである。また，真正品として行使を目的に作製された偽物は“偽造”，そうでないものは“模造”とされるなど，行使の目的が併せて考慮されるようである。

注 1) **Standard Guide for Selection of Security Technology for Protection Against Counterfeiting, Alteration, Diversion, Duplication, Simulation, and Substitution (CADDSS) of Products or Document**s

注 2) 佐伯仁志，通貨偽造罪の研究，日本銀行金融研究所，金融研究, 2004. 8, p. 153

3) ホログラムの説明

世界の銀行券や旅券にも広く用いられているホログラムの説明に苦慮した。その背景には，昨今の券面セキュリティ用途としてのホログラムの実態が，学術的（歴史的）な定義から外れるほどに多様化したことがある。現状のホログラムは，干渉縞の記録状態，再生光源の種類，量産方法等の観点から 30 種類以上の分類と様々な呼称があるという **3)**。一方，**JIS Z 8120 光学用語**におけるホログラムの定義は，“物体から出る光波と，それと干渉性がある光波との干渉パターンを写真感光材料などに記録したもの”となっている。これに従うと，券面セキュリティ用途として用いられるホログラムのいくつかはこの定義から外れてしまう。このため，**ICAO Doc9303 Part 1** 等の関連文献では，ホログラムの語は使用せずに，OVD（Optical Variable Device：光学的変化デバイス），DOVID（回折型光学像変化デバイス），OVF（Optical Variable Feature：光学的変化特性）等の用語で整理されている。

以上より，本書における“ホログラム”の語は，当該業界において定着した便宜上の呼称と位置付けた。その上で，発行者の調達時の有益性と分かりやすさを考慮した説明とした。

注 3) 鎌田康昌ら，この 10 年間の印刷の科学と技術の進歩と今後の展望，日本印刷学会，日本印刷学会誌, 55, 5, 2018, p. 214

c) 模造の対策について

偽物の精巧さを考慮しない限りにおいては，類似の外観を有する偽物を“模造”することは可能である。この意味において，模造対策として取り得る券面に実装可能な技術というものは成立し難い。この対策となり得るのは，本物の特徴を熟知した上で模造された偽物をしっかりと判別し，本物として受理しない，という運用が重要である。

また，カード製造者側の実践・努力としては，偽物とは明らかに一線を画す一定の真正性（本物であること又は本物であることを確実にする特性）が維持可能な緻密なセキュリティ設計の提案や高度な製造・品質管理体制の確立が重要であることなどが共有された。

d) 本物らしさの重要性

模造の対策（**c**）と関連し，“本物らしさ”の話題が提起された。例えば，銀行券の場合，有価印刷物ならではの重厚なデザインと凹版印刷[4]，すき入れ等の特殊な製造技術による独特の質感に対し，人々は共通の本物らしさや信頼性を見いだしている。一方，同じく有価印刷物でありながら，本人確認書類の場合は状況が異なる。犯収法[5]で定められる公的機関が発行する写真付き本人確認書類は，87 の独立行政法人が発行する身分証明書（ID カード）を筆頭に，100 種類以上に及ぶが，我が国には ID カードの券面セキュリティに関し，一般に利用可能な標準や規格は存在しない。本書で提唱される券面セキュリティへの準拠やロゴマーク（**A.1.1.4**）等の導入によって，一定水準の券面セキュリティと本物らしさを確保し，第三者による 2 次利用の際の信頼性や非常時の実効性を高めることが望ましいとの見解に至った。

注 4) 印刷版面の凹状の画線部分にインキを詰め，大きな圧力をかけて紙に転写する印刷方式。紙に転移したインキの画線は盛り上がっているため，独特の手触り感を有する。

注 5) “犯罪による収益の移転防止に関する法律”の通称。金融機関等における取引時確認，取引記録等の保存，疑わしい取引の届出の義務など，資金洗浄及びテロ資金供与対策のための規制を定める法律である。

e) 対策技術のリスト，選定基準の根拠等

引用規格（**ICAO Doc9303 Part 2**）における対策技術のリストには，紙基材を前提とした技術及び我が国においては提供実績がないものが散見された。これらは実現可能性という観点から削除することで一致した。

また，対策技術の写真付き説明文の掲載，選定基準の明確な根拠の提示等が成員から要望された。写真掲載については著作権の整理，選定基準の根拠はセキュリティの低下が懸念されるため，懸案事項とし，次期改版に委ねることにした。

f) 新規開発による偽変造対策技術の取扱い

本書の偽変造対策技術のリスト（**8.2** 及び **8.3**）に記載されない新規開発による対策技術の実装は，どの程度セキュリティに貢献し，どのような評価の説明がなされるべきかの問題が提起された。あくまで **ICAO Doc 9303 Part 2** は，最低限実装すべき偽変造対策技術を扱ったものである。そのため，偽造者が使用可能な複製機器の進歩によって高まる偽造の脅威に対し，永続的なセキュリティを担保するものではない。したがって，新規開発技術の採用は，リスク対応における多様性を向上するためにも，むしろ奨励されるべきではないかとの見識が共有された。

あわせて，個別対策技術のセキュリティ及びカード全体のセキュリティ設計の具体的な評価方法の必要性が確認された。

g) 考慮すべき製品の範囲

本書で適用を考慮すべき製品は，ID カードに限定されることなく本人確認書類全般であるべきではないか，との意見が提起された。

各種の行政手続や特定の商取引において，本人確認の際に用いられる本人確認書類の種類は多岐にわたる。写真付きのものとしては運転免許証，旅券，マイナンバーカード等，写真無しのものとしては各種保険証，国民年金手帳等がある。写真無しの場合は，なりすまし対策として，併せて住民票の写し等の提示が求められる。また，当該書類に住居等の記載がない場合には，納税証明書，社会保険料領収書，公共料金領収書等が補完書類として用いられている。

このように，本人確認書類は，その形態（カード・冊子・A4 紙等）や書式仕様を始め，その厳格性や券面セキュリティが一律ではない。そのため，リスクの平準化を図るために複数書類を用いた多様な運用がなされている。以上のことから，検討対象となる製品の範囲は，本人確認書類の形態や書式仕様に依存しない“不定形”（Form Factor Free）であるべきである。また，保護すべき資産を明らかにした上で，想定される不正行為，不正によるダメージの大きさ，発生頻度，コスト等の観点によるリスクベースの検討が望ましいとの考えが示された。

h) 本人確認の重要性の高まり

本人確認の重要性や身分証明書の位置付けが世界的にも高まっている。第 70 回国連総会で採択された SDGs[6)]における達成基準 16-9 では，平和で包摂的な社会の実現に向け，「2030 年までに，すべての人々に出生登録を含む法的な身分証明を提供する。」とある。

また，達成基準 16-4 には，違法な資金及び武器の取引，組織犯罪の激減等が提唱されている。他方，具体的な動きとして，マネーロンダリング対策やテロ資金対策等における国際的な協調指導，協力推進などを行う FATF[7)]を中心に，特定の民間の商取引における本人確認の重要性が提起されている。この対応として，行政では，受入可能な本人確認書類の種類を制限するなど，法制度・運用面での本人確認の厳格化の対応を図ってきた。このような中，券面セキュリティの確保・向上は，技術面からの施策の一つとなり得るものと思われる。

注 6) Sustainable Development Goals の略で，“持続可能な開発目標”と訳される。17 のグローバル目標と 169 の達成基準から構成される。採択文書“我々の世界を変革する： 持続可能な開発のための 2030 アジェンダ”（2015 年）の中で具体的行動指針として示された。

注 7) Financial Action Task Force（金融活動作業部会）の略で，“ファトフ”と呼ばれることが多い。1989 年のアルシュ・サミット経済宣言により設立された政府間機関であり，G7 諸国を含む 35 か国及び 2 つの地域機関（EC・GCC）が加盟するほか，3 か国のオブザーバ国，多くの国連関係機関等が参加している（2018 年現在）。我が国では，警察庁 JAFIC（犯罪収益移転防止対策室）が中心に FATF と連携し，国際的な FIU（金融情報部門）としての業務を担っている。