監修　ISO 22388 対訳版検討会

第 2 章

ISO 22388 物理的文書のセキュリティガイドライン
附属書活用の手引き

一般財団法人日本規格協会
2026年4月15日

1　まえがき

本手引きの目的は，ISO 22388 の附属書に収録された文書不正のリスクアセスメントや券面設計のためのツール群について，その理解を深め，現場での活用・運用の導入を支援することである。

規格における附属書とは，規格本体に追加的な参考情報を提供するものである。長大な表・サンプルフォーム・リストなど，本体に組み込むと利用者の集中を妨げる特殊な情報を分離し，提示することが主な目的である［1]。ここでは，各附属書において特に重要と考えられる箇所を整理・抜粋し，実務に即した事例を交えて解説する。

ISO 22388 の附属書は，A〜E の五つから構成される。ここには，SD の仕様作成に不可欠なリスクアセスメントやセキュリティ技術の評価方法が具体的事例と共に記載されている。特に，リスクとセキュリティの評価方法については，定式化（又は数値化）され，評価ツールとして利用可能な形態となっている。仕様作成者は，このツール群を用い，リスクベースによる券面設計やセキュリティ対策の妥当性や十分性をレビューすることができる。

本手引きでは，最初に（箇条 2)，ISO 22388 の附属書全体の構造と相互関係を俯瞰する。次に（箇条 3)，各附属書における概念的・抽象的な記述から，SD の仕様作成において最低限必要とされるプロセスを抜き出し，要点を説明する。最後に（箇条 4)，附属書 B の表 B.2 で取り上げられる“出生証明書”を例に，リスクアセスメントの実施の手順を説明する。

2　附属書の全体構成

ISO 22388 の附属書 A〜E は，SD のリスクアセスメントから対策技術の選定，分類，評価など券面の仕様作成を体系的に支援する構造となっている。各附属書の関係性を図 1 に示す。図中の模式化された各附属書内には，実務上の重要事項を付番のうえ記載した。

附属書 A は，券面設計の起点となる SD のリスクアセスメントについての説明である。ここでは，文書不正の脅威とリスクの分析に基づき，SD のリスクレベルに応じた“文書クラス（3 段階）”が決定される。この文書クラスの概念に基づき，最低限実装すべきセキュリティ技術の基準が設定される。また，附属書 A で明示的な解説がなされていない“文書固有のリスク要因”（図 1※印）について，重要事項としてここで説明する。

附属書 B は，附属書 A によるリスク評価結果に基づくセキュリティ対策のプロセスに対応する。本附属書は，券面の対策レベルを半定量的に計量可能（数値的に評価可能）なレーティングシステム，及びレーティングの事例を提供する。仕様作成者は，レーティングシステムを用い，選定された複数のセキュリティ技術による対策の妥当性を評価する。

附属書 C は，附属書 B で参照されるセキュリティ技術のリスト，個別のセキュリティ技術のレーティングのための基準などを提供する。ここで，セキュリティ技術のリストには，7 分野から約 70 個の技術がセキュリティレート（4 タイプの攻撃に対する耐性：例（9, 4, 3, 5））と共に掲載される。また，仕様作成者は，必要に応じ，各技術の追加的なセキュリティのレーティングが可能である。附属書 C には，このレーティングの方法と評価項目が例示されている。

附属書 D は，技術の認証方法と SD の利用者視点による技術分類の説明である。附属書 B における技術選定の補完的資料と位置付けられる。

附属書 E は，技術名称などを整理した用語集である。セキュリティ対策全体の理解と一貫性を支えるベースとなる。

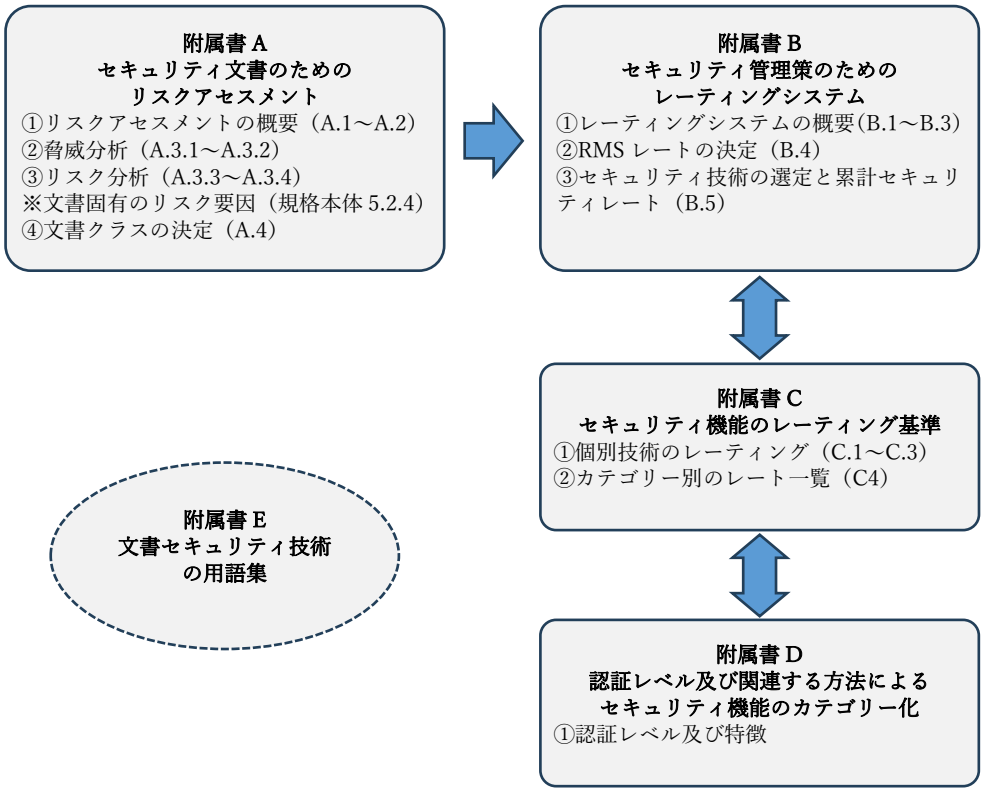

図 1　各付属書の関係性

3　各附属書の要点解説

3.1 附属書 A　セキュリティ文書のためのリスクアセスメント

3.1.1　①リスクアセスメントの概要（A.1～A.2）

リスクアセスメントは，組織のリスクフレームワーク及び文書に対する攻撃手段を踏まえ，関連する脅威を特定し，文書クラスを決定し，リスクを許容レベルまで低減するための対策を講じる一連のプロセスである。具体的には，文書不正リスクの評価として，SD の価値・重大性，脆弱性，脅威の発生源，リスクの発生可能性と潜在性，経済的・法的・人的・サービス提供への影響，情報の信頼性と確実性などを総合的に評価する。これらのプロセスは，A.2.1 に記載される ISO 31000 のプロセスモデルを参考に，自社のリスクマネジメント方針と業務特性に応じ，特定プロセスの簡素化や補強等のカスタマイズが可能である［2]。

A.2.2～A.2.4 記載のリスク（文書固有のリスク要因を含む）の特定・評価・分析は，主として文書発行者との協議によって実施される。これは，文書不正の実態把握，リスク対応（回避，転嫁，軽減，受容）にかかる意思決定などを含むからである。

3.1.2　②脅威分析（A.3.1～A.3.2）

脅威分析の各論に入る前に，附属書 A の A.3 の名称でもある“半定量的リスクアセスメント”について説明する。半定量的リスクアセスメントとは，定性的評価をレートやランクで数値化することで比較を容易にするものである。文献［3]では，確率モデルや統計解析までは行うことなく，分析の迅速化や汎用性の高い点が利点とされている。つまり，ざっくりとした数値で分析結果を見える化し，意思決定が補強可能な，定量と定性の中間的なアプローチであるといえる。ただし，数値で表現されているがあくまで疑似

的なものであり，過信は避けるべきとされる。

脅威分析は，SD に対する不正行為の発生可能性とその要因を体系的に把握するためのプロセスである。本プロセスの実施に当たり，A.3.1 に列記される考慮すべき要因について補足説明をする。

・脅威アクターの意図及び能力：意図（intentions）とは，不正行為を行う意思，動機，目的意識の強さである。能力とは，文書不正を実行する技術力，資源（人・物・金）の有無，組織力などを意味する。ここで特記すべきは，意図と能力の両立によって脅威が最大化する，ということである。参考として各脅威アクターの意図と能力に関する分析例を表 1 に示す。

・対応前の文書の脆弱性：セキュリティ対策が未実施，不十分な状態（対応前の意），又は定期的仕様変更の未実施において，どの程度攻撃されやすいか，又は攻撃耐性を有しているかという性質である。ただし，一般的には脆弱性だけではリスクにはならないとされる。よって，ここに併記される脅威アクターの意図及び能力，攻撃の機会など，複数の要因（A3.1）を考慮した多元的な評価が必要である。

・攻撃の機会：機会とは，SD へのアクセシビリティを判断するための重要な要因である。脅威アクターが SD にアクセスできる状況（どこで，どのように），管理・保管体制などの環境的要因をはじめ，SD の流通量，使用頻度などが考慮される。

・攻撃が成功した場合の影響，及びそのような攻撃が発生する可能性：影響には，信用失墜，金銭的損失，及び法的・社会的影響を含む。

表 1　各脅威アクターの意図と能力（例）

脅威アクター	意図	能力	備考
問題意識に基づく活動家組織	中～高（社会的・倫理的主張，抗議目的）	中（限定的な技術力，組織力はあるが資源は限定的）	特定の文書（ID，許可証など）を標的にした抗議活動である。攻撃は一時的だが，注目を集めるため派手な行動の可能性あり。
政治的動機に基づくグループ又は国家	高（SD の信用失墜による政治的影響，外交的圧力，なりすまし）	高（高度な技術，資源，組織的支援）	国家間の対立や情報戦の一環として SD を標的化。長期的・持続的な攻撃が想定される。
犯罪組織	高（金銭的利益，偽造・流通目的，資金洗浄や闇市場での取引拡大も視野）	中～高（偽造技術，資金，人員，流通網）	偽造は最も現実的かつ継続的な脅威である。収益性が高い限り，攻撃が続く。偽造品の作製・流通・行使が分業化され，複数の脅威アクターが連携する構造に留意すべき。また，製造済みで未流通の偽造品ストックも脅威の一部と捉えるべきである。
利益を求める日和見主義者／個人	中（短期的利益，模倣，小規模な転売）	低～中（市販機材，基本的知識）	偽物の精巧度は低いが，行使場面によっては騙されることがある。また，流通量や SNS 等を介した拡散力が特徴である。
内部関係者	中～高（個人的利益，報復，共犯）	中（アクセス権，情報知識，操作可能性）	情報漏洩や真正性の消失に直接的に影響・関与する。検知の遅れや暗躍の可能性が高い。

脅威分析の実務では，脅威マトリックス（A.3.2）が使用される。このマトリックスの特徴は，乗算モデル（掛け合わせ）で表現されるリスクマトリックスとは異なり，加算モデル（附属書 A の表 A.1, A.2）が採用される点である。加算モデルの利点は，公差 1 の均等な差分で構成されるため，結果の解釈が直観的で一貫性を保ちやすいことである。また，一般的に，意図・能力・機会などの要因間には高い相関が

あり，各要因の評価は互いに影響し合うため，単独での評価は困難である。しかし，加算モデルの枠組みを用いることで，個別の要因を明確に評価しつつも，全体の傾向や脅威の水準を統合的に捉えることが可能となる。

3.1.3 ③リスク分析（A.3.3〜A.3.4）

一般的に，リスク分析では，事象の“起こりやすさ”と“影響”の 2 軸で評価する。起こりやすさの評価は，前項の脅威分析の結果に基づく。この加算評価によって，意図と能力が共に高い場合は，“起こりやすく”，共に低い場合は，“起こりにくい”とされる。起こりやすさの一般的な指標として，附属書 A の表 A.3 が参考になる。

リスクの評価モデルは，表 A.4 に示される“起こりやすさ”と“影響”の掛け合わせのマトリックスによる。各要因の乗算によって，リスクの重大性（1〜25）が算出される。この乗算モデルの性質として，どちらか一方の要因に高レートを含む場合，リスクレートは増大し，強調されることになる。逆に，どちらかに低レートを含む場合のリスクレートは，抑制された値になる。

このように，加算モデルと比較すると，より明確でメリハリのある判断が可能となる。一方，評価スケールが大きすぎる場合（例：10 段階×10 段階），リスクレートが極端化し，比較や優先順位の判断が困難となるため注意が必要である。

3.1.4 ※文書固有のリスク要因（規格本体 5.2.4）

これは，規格本体に明記される重要事項である。脅威分析が攻撃する側の意図と能力に着目するのに対し，文書固有のリスク要因は，攻撃対象となる文書そのものの特性に着目する。具体的には，SD の使用頻度・範囲，有効期間，第三者利用の有無，制度的背景など，文書固有の属性が不正リスクを誘引する可能性を評価するものである。

文書固有の要因を考慮するためには，リスク分析の基本である“起こりやすさ”と“影響”による 2 軸評価に加え，固有のリスク要因を組み込んだ多軸評価モデル [4, 5, 6]の導入が推奨される。これによって，SD を汎用のリスク分析の枠組みに一律に当てはめるのではなく，SD の使用状況や個別事情に則したリスクアセスメントが可能となる。

一般的な多軸評価の方法としては，計数化された固有のリスク要因（以下，固有リスク計数）をリスク（起こりやさと影響の掛け合わせ）に乗算するものである。ここでの注意すべき点は，固有リスク係数をどのように配置し，乗算するかである。つまり，起こりやすさと影響の両方に掛け合わせるのか（係数が 2 乗される），又は一方のみに反映させるのか，というアセスメントモデルの設計上の選択がある。本手引きでは，例示という趣旨から，各要因の固有リスク計数の平均値を代表値とし，3.1.3 で算出されたリスクレートに掛け合わせている。

3.1.5 ④文書クラスの決定（A.4）

文書クラスは，各攻撃モードのリスクレートを算出し，決定される（附属書 A の表 A.5〜表 A.7）。決定に当たっては，いわゆる“最大リスクの原則”を適用する必要がある。これは，最も深刻な攻撃シナリオに備える券面設計を促すものであり，不正リスクの過小評価を防ぐ効果もある。高リスク文書のリスクレートの計算例（表 A.5）における最大値は，“偽造 = 20”である。この値は，表 A.8 において赤色で示されたレベル（12〜25）であり，高リスク文書であると判定される。ここで，固有リスク係数の考慮（乗算）によって，リスクレートが増減し，文書クラスに変更が生じることがある。また，レートが 25 以上となることもあるが，その場合は，高リスク文書となる。

3.2　附属書 B　セキュリティ管理策のためのレーティングシステム

3.2.1　①レーティングシステムの概要（B.1～B.3）

附属書 B では，SD に実装されるセキュリティ技術の性能を半定量的に評価するためのレーティングシステムについての説明がなされる。この半定量的評価の尺度は，“とても低い：1～2”から“とても高い：9～10”までの 5 段階である。各レートは，主観的な表現と数値との対応関係によって，技術の相対的な耐性を示すものであり，実務における意思決定の透明性と一貫性を支援する。また，新規の技術や新種の脅威に対する耐性については，後述する附属書 C の表 C.1 を参考に，関係者間の合意に基づくレーティングの加減が推奨される。

3.2.2　②RMS レートの決定（B.4）

5.5 の逐条解説でも述べたとおり，RMS レートとは，攻撃対象となる SD が備えるべき“推奨される最低限のセキュリティ”である。ここで留意すべきは，附属書に記載される RMS レートは，一意の値ではなく，例えば，“35～55”というように 20 の幅を有するということである。これは，異なる仕様作成者や SD の運用環境における多様性と柔軟性の確保のためである。したがって，運用上の RMS レートは，仕様作成者と文書発行者等の関係者との間での綿密な協議を経て設定されるべきである。例えば，脅威とリスクのレートを目安に，未然防止を目的とするのか，発生してしまった不正事案への緊急的な対処なのか，又は再発防止を重視するのかといった，対策の目的や優先度に応じた調整が求められる。

また，RMS レートの値は，附属書の既定値のように各攻撃モードで必ずしも一定になるとは限らない。どの攻撃モードに対する耐性を重視するかは，SD の使用目的，脅威のプロファイル，運用環境などを考慮した上で決定されるべきである。

3.2.3　③セキュリティ技術の選定と累計セキュリティレート（B.5）

ここでは，各文書クラスの典型として出生証明書，職業資格証明証及び低額のイベントチケットを取り上げ，それぞれのセキュリティ技術の構成例が示される。実務的には，附属書 C のカテゴリー別の技術リストから複数の技術を選定し，各攻撃モードの累計セキュリティレートの RMS レートへの適合性を評価する。ここで，累計セキュリティレートは，SD の性能プロファイル（攻撃モードごとの耐性）を構成するものであり，対策シナリオ又は設計方針との整合性をレビューするため指標とすることができる。

3.3　附属書 C　セキュリティ機能のレーティング基準

3.3.1　①個別技術のレーティング（C.1～C.3）

附属書 C の前半は，個別技術のレーティング基準，及びこれらの基準を用いたレーティングの手順が説明される。

個別技術のレーティング基準の例は，表 C.1 中の“キー”（凡例）として，“a～o”の 15 個のレーティングの基準が掲載される。これらは，原材料の限定性，リバースエンジニアリング耐性，設計の複雑性など抽象的又は概念的な特性に基づく。

表 C.2 は，各技術カテゴリーにおける典型技術のレーティングの事例を示したものである。仕様作成者は，個別技術のセキュリティレーティングのツールとして表 C.2 を活用することができる。また，レーティングプロセスの概要が図 C.1 に示される。これらを踏まえ，実務的観点から“白黒すき入れ”のセキュリティレーティングの手順及び評価結果を表 2 に整理する。他の個別技術のレーティングにおける参考とされたい。

表２　白黒すき入れのレーティング手順

プロセス（図 C.1 から引用）	手順	結果
1　評価基準の決定	攻撃モードごとに, a～o の中から適切なレーティング基準を選定する。必要に応じて独自の基準や項目を設定する。	偽造：a, b, c, h 模造：d, g 変造・改ざん：e, f 不正入手：l, m, n, o
2　“該当無し”から“とても高い”までの定性評価	各基準について，Very low から Very high までの 5 段階の評価スケール（尺度）に基づき，定性評価をする。	偽造：a=5, b=5, c=5, h=5 模造：d=3, g=2 変造・改ざん：e=2, f=2 不正入手：l=2, m=2, n=2, o=2
3　競合技術との比較/当該カテゴリーにおける相対的位置のレビュー	多階調すき入れ，及び白黒すき入れを交えた相対的な性能比較。相対的位置の例として，性能の序列がある。	例：多階調すき入れとの比較ではやや劣るが，疑似透かしに対しては顕著な優位性を有する。
4　セキュリティ技術のレート（0, 1, 2, ...8, 9, 10）	各攻撃モードにおいて，5 段階の複数の評価結果を統合，再評価し，次に，単一の 10 段階のセキュリティレートへと変換する。評価結果の統合方法としては，最も基本的なものとして単純平均法がある。その他，レーティング基準に重み付けをする重み付き平均法などがある。	偽造：4, 5, 5, 5 を統合し，セキュリティレートは 9 模造：3, 2 を統合し，セキュリティレートは 4 変造：2, 2 を統合し，セキュリティレートは 3 不正入手：2, 2, 2, 2 を統合し，セキュリティレートは 4 なお，10 段階への変換後の値には，類似技術のレートとの比較のうえ，レート増減の微調整がなされる。

3.3.2　②セキュリティレートの表（C.4）

附属書 C の後半には, 8 個のカテゴリーからなるセキュリティ技術(表 C.3～表 C.8, 表 C.10, 表 C.11）と DOVIDs のサブ機能（表 C.9）のセキュリティレートが記載される。仕様作成者は，これらのセキュリティレートを参照し，SD に実装する技術を選択する。

どのカテゴリーにも分類されない新技術については，既存の評価基準（a～o）を基本とし，必要に応じて独自の評価項目を設定のうえ，表 C.2 の形式に準じ，セキュリティレーティングを実施する。これにより，既存技術との整合性を保ちつつ，技術の特性に応じた柔軟な評価が可能となる。

なお，評価の恣意性を排除するため，仕様作成者（又は新技術の提供者）は，レーティングの根拠を文書化し，発行者との合意の一部とすることが望ましい。また，必要に応じ，知識を有したセキュリティ専門家による第三者的なレビューが推奨される。

3.4　附属書 D　認証レベル及び関連する方法によるセキュリティ機能のカテゴリー化

3.4.1　①認証レベル及び特徴（D.2）

附属書 D は，セキュリティ機能・技術の分類方法の一つである認証方法（認証レベル）についての説明である。附属書 C における分類が技術の物理的構成，実装形態，機能などによるものに対し，附属書 D では，技術の検知手段，利用者の属性，及び検証に必要なツールの有無といった運用上の視点からの技術分類がなされる。仕様作成者は，この分類に基づき，文書の運用環境に応じて適切な認証レベルを選定し，それに対応する技術を附属書 C から選択することができる。

5.5 の逐条解説で述べたとおり，券面設計における多重性の構築の一つとして，異なる認証レベルに対応する複数技術の組み合わせがある。仕様作成者は，附属書 D に示された認証方法の特徴を参照し，認証システムという観点での設計が推奨される。

4　各種レーティングの手順

4.1　脅威のレーティング

附属書 B に例示される出生証明書を用い，脅威レーティングの手順を説明する。欧米諸国において，出生証明書とは，旅券や運転免許証などの身分証明書を取得する際に提出が求められる本人確認の信用起点となる文書のことである。一方，日本では，これに相当する文書として戸籍謄本と住民票が挙げられ，その脅威の種類やリスクの影響度において出生証明書と共通点があると考えられる。

規格本体の 5.2 及び附属書 A の A.3.2 に準拠した脅威レーティングの方法を示す。脅威レートは，半定量的に表現された脅威アクターの“意図”と“能力”の加算によって算出される。実施に当たっては，規格本体の 5.2.3 記載の 5 タイプの脅威アクター，及び“意図（動機及び目的）”の 4 類型を参考にすることができる。脅威レートの算出手順を次に示す。

①脅威アクターの定義

評価対象となる 5 タイプの脅威アクターの特徴を把握する。

②脅威アクターの特性のプロファイリング

規格記載の各脅威アクターの意図を参考に，アクターの動機・目的・不正行為を成功させる技術力・装置・知識などについて分析・評価する（本手引きの表 1)。

③脅威アクターの半定量的評価

4 攻撃モードに対する全ての脅威アクターの“意図”及び“能力”を 5 段階で評価する。

④脅威レートの集計

附属書 A の A.3.1 記載の式 “$a_n = a_1 + (n - 1)d,\ d = 1$” を用い，各脅威レートを算出する。例えば，意図が 3，能力が 4 のときの脅威レートの計算式は，“3＋4－1＝6”となる（表 3)。脅威レートは，1～9 の 9 段階で表現される。

本レートは，次プロセスのリスクレーティングにおいて，“起こりやすさ”の評価に用いられる。

表 3　脅威レーティングの例

意図	**能力**				
	無視できる–1	低い–2	中位–3	**高い–4**	とても高い–5
とても高い–5	5	6	7	8	9
高い –4	4	5	6	7	8
中位 –3	3	4	5	**6**	7
低い –2	2	3	4	5	6
無視できる–1	1	2	3	4	5

例として，出生証明書の脅威レートの集計結果を表 4 に示す。

表 4　脅威レートの集計結果（例）

攻撃モード	脅威アクター	意図	能力	脅威レート
偽造	活動家組織	高い － 4	高い － 4	7
	テロリスト又は敵対的国家	とても高い － 5	とても高い － 5	9
	犯罪組織	高い － 4	中程度 － 3	6
	日和見主義者/個人	低い － 2	低い － 2	3
	内部関係者	低い － 2	中程度 － 3	4
模造	活動家組織	低い － 2	高い － 4	5
	テロリスト又は敵対的国家	低い － 2	とても高い － 5	6
	犯罪組織	高い － 4	中程度 － 3	6
	日和見主義者/個人	高い － 4	低い － 2	5
	内部関係者	低い － 2	中程度 － 3	4
変造/改ざん	活動家組織	無視できる － 1	中程度 － 3	3
	テロリスト又は敵対的国家	無視できる － 1	中程度 － 3	3
	犯罪組織	中程度 － 3	中程度 － 3	5
	日和見主義者/個人	高い － 4	低い － 2	5
	内部関係者	低い － 2	中程度 － 3	4
不正入手	活動家組織	中程度 － 3	高い － 4	6
	テロリスト又は敵対的国家	高い － 4	とても高い － 5	8
	犯罪組織	中程度 － 3	中程度 － 3	5
	日和見主義者/個人	無視できる － 1	無視できる - 1	1
	内部関係者	低い － 2	低い － 2	3

4.2　リスクのレーティング

引き続き，出生証明書を例として，規格本体の 5.2 及び附属書 A の A.3.4 に準拠したリスクレーティングの手順について説明する。リスクレートは，半定量的に表現された文書不正の“起こりやすさ”と“影響”の掛け合わせによって算出される。本レーティングは，4 攻撃モードと 5 脅威アクターの全ての組み合わせで実施される。レート算出の手順を次に示す。

①各攻撃モードにおける各脅威アクターによる文書不正の“起こりやすさ”の評価（5 段階）

起こりやすさの評価は，本手引き 4.1 記載の脅威の 9 段階評価（1～9）の結果に基づき，5 段階で行われる（図 2）。

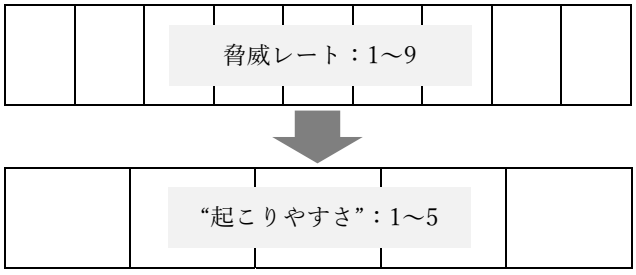

図 2　脅威レートのスケール変換

②各攻撃モードにおける各脅威アクターによる“影響”の評価（5 段階）

影響は，文書不正が成功した場合に生じる被害の大きさや負の結果の評価指標である。出生証明書の場合，不正な国籍や市民権の取得，社会保障制度の不正利用，金融取引上のなりすましなど，個人

の法的身分や社会的信用に重大な影響を及ぼす事象が含まれる。影響は，5 段階で入力される。

③リスクレートの集計

攻撃の重大性を示す指標として起こりやすさと影響を掛け合わせ，リスクレートを算出する。出生証明書を例としたリスクレートの集計結果を表 5 に示す。表 5 には各攻撃モードのリスクレートの最大値が抽出されている。この最大レートは，リスクの俯瞰や文書クラスの決定に用いられる。

表 5　出生表明書のリスクレートの集計結果（例）

攻撃モード	脅威アクター	起こりやすさ	影響	リスクレート	最大レート
偽造	活動家組織	とても起こりやすい–4	壊滅的 – 5	20	20
	テロリスト又は敵対的国家	とても起こりやすい–4	壊滅的 – 5	20	
	犯罪組織	起こりやすい – 3	中程度 – 3	9	
	日和見主義者/個人	起こりにくい – 2	軽微 – 2	4	
	内部関係者	起こりにくい – 2	大きい – 4	8	
模造	活動家組織	起こりやすい – 3	壊滅的 – 5	15	15
	テロリスト又は敵対的国家	起こりやすい – 3	壊滅的 – 5	15	
	犯罪組織	起こりやすい – 3	中程度 – 3	9	
	日和見主義者/個人	起こりやすい – 3	軽微 – 2	6	
	内部関係者	起こりにくい – 2	中程度 – 3	6	
変造・改ざん	活動家組織	無視できる – 1	軽微 – 2	2	12
	テロリスト又は敵対的国家	無視できる – 1	軽微 – 2	2	
	犯罪組織	起こりやすい – 3	大きい – 4	12	
	日和見主義者/個人	起こりやすい – 3	中程度 – 3	9	
	内部関係者	起こりにくい – 2	中程度 – 3	6	
不正入手	活動家組織	起こりやすい – 3	大きい – 4	12	16
	テロリスト又は敵対的国家	とても起こりやすい–4	大きい – 4	16	
	犯罪組織	起こりやすい – 3	中程度 – 3	9	
	日和見主義者/個人	無視できる – 1	軽微 – 2	2	
	内部関係者	起こりにくい – 2	軽微 – 2	4	

4.3　文書固有のリスク要因

ここでは，出生証明書を例にとり，固有リスク要因の定義から評価項目の導出，レーティング，リスク係数への変換，そして最終的な集計方法までの一連の手順を示す。ただし，“文書固有”の表現が示すとおり，リスク要因は，対象文書の特性や運用形態に強く依存するため千差万別である。したがって，本手順の汎用化には慎重になるべきである。特に，個別の評価項目，加重の設定，リスク係数の乗算方法など関係者間の事前の合意が望ましい。

①リスク要因の決定

規格本体 5.2.4 記載の固有のリスク要因をもとに，評価対象となる文書のリスク要因を定義する。

②評価項目の導出

リスク要因の評価検討が可能な具体的な評価項目の導出，及び尺度（目盛り）を定義する。これらの導出と定義に当たっては，個別文書ごとにその特性や運用形態を十分に精査し，考慮することが求められる。評価項目と尺度の例を表 6 に示す。

表 6　評価の項目と尺度の例

評価項目	評価尺度				
使用頻度	1 数年に一度	2 年に数回	3 月に数度	4 週に 1 回程度	5 毎日
通用力（公開範囲）	1 ほとんど無い	2 低い	3 普通	4 高い	5 とても高い
所在・保管状態	1 厳重保管	2 所定場所保管	3 持出有り保管	4 不定期携行	5 常時携行

③固有のリスク要因のレーティング

それぞれの評価項目について 5 段階の半定量的評価を実施する。

④固有リスク係数の集計（表 7）

各評価項目の平均レートを係数（0.8～1.2）に変換し，各要因における固有リスク係数とする。次に，各リスク係数の平均値を固有リスク係数の代表値とする。（リスク係数の変換式は，リスク係数 ＝ 0.1×平均レート＋0.7）

表 7　固有リスク係数の集計結果（例）

リスク要因	評価項目	評価結果	平均レート	固有リスク係数	代表値
使用頻度	NA	2	2.0	0.9	1.1
利用可能性	通用する範囲（公開範囲）	4	3.8	1.1	
	所在・保管状態	2			
	普及度・発行量	5			
	無効化・失効後の確実性	4			
	ブラックマーケット	4			
有効期間	NA	5	5.0	1.2	
信頼性	発行機関	4	4.5	1.2	
	社会的認知度	5			
	制度化の有無	5			
	再発行の厳密性	4			
第三者利用	使用要件（コピー不可）	3	4.3	1.1	
	真偽判別方法の徹底	5			
	照会・検証の可能性	4			
	不正・脆弱性事例の共有	5			

⑤固有リスク計数の反映

本手引き 4.2 で得られたリスクレートに固有リスク係数の代表値を乗算する。

（例：リスクレート（最大値）×固有リスク計数の代表値 ＝ 20×1.1 ＝ 22）

なお，係数の範囲（0.8～1.2）は，標準化されたものではなく実務上の設計判断による。セキュリティ重視の運用の場合など，最終リスク係数の上限を 1.4 程度まで高めることによってリスク感度の高い評価が可能となる。

4.4　文書クラスの決定

表 5 記載の最大リスクレート，又は表 7 記載の固有リスク計数の代表値によって補正された最大リスクレートを用いて出生証明書の文書クラスを判定する。

①最大リスクレート（又は補正された）による文書クラスの判定

クラス判定のリスクレートの閾値は，表 8 による。4.3 の⑤に基づき，出生証明書の最大リスクレートは，22（固有リスク計数による補正有り）となり，文書クラスは，“高リスク文書”となる。

なお，固有リスク計数の反映によるリスクレート 11 の発生（表 8 において 11 は欠番），及びレー

トの端数処理には注意が必要である。

表 8　クラス判定の閾値

リスクレート	文書クラス
12～25	高リスク文書
5～10	中リスク文書
1～4	低リスク文書

4.5　セキュリティレーティング

出生証明書を想定し，評価の基準となる RMS レートの設定とセキュリティ技術の選択について説明する。ここでは，各攻撃モードにおける対策性能の妥当性，RMS レートの適合性などがレビューされる。

①RMS レートの設定

附属書 B 記載の RMS レートの一覧を示す（表 9)。出生証明書は，高リスク文書に該当するため，表 9 記載の 35～55 の範囲を下回ることなく各攻撃モードの RMS レートを定める。ここでは，試験的な RMS レートとして（50, 40, 35, 45）を用いた（後述)。

表 9　各クラスの RMS レート

タイプ	偽造	模造	変造・改ざん	不正入手
高リスク文書	35～55	35～55	35～55	35～55
中リスク文書	20～40	20～40	20～40	20～40
低リスク文書	10～15	10～15	10～15	10～15

②セキュリティ技術の選択と累計

対策シナリオに基づき，複数カテゴリーから技術を選択する（表 10)。附属書 C の表 C.3～C.11 記載のセキュリティレートを参照し，各攻撃モードでレートを累計する。本例の累計セキュリティレートは，（86, 51, 48, 67）である。

表 10　出生証明書の技術選択の例

カテゴリー	選択技術	偽造	模造	変造・改ざん	不正入手
基材技術	白黒すき入れ	9	4	3	4
	薬剤反応	5	2	5	3
	UV 機能	5	2	2	2
セキュリティ印刷	地紋模様	7	4	2	6
	マイクロ印刷・ナノ印刷	7	6	0	8
	複写対策画線・モアレパターン	7	2	5	2
	光学的変化又は潜像	8	5	0	8
セキュリティインキ	赤外又は紫外蛍光インキ	5	3	5	3
パーソナライゼーション技術及び技法	機械読取技術	2	2	7	1
	冗長性データ	0	0	5	0
	周波数変調イメージ	7	6	4	8
タガント	希土類	8	0	0	8
DOVIDs	透明 DOVIDs	6	5	4	5
DOVIDs のサブ効果	回折型ウォーターマーク	1	1	0	0
デジタルセキュリティ技術	物理層デジタル検証保護	9	9	6	9
累積セキュリティレート		86	51	48	67
RMS レート（試験値）		50	40	35	45

③RMS レートへの適合性の確認

各攻撃モードの累計セキュリティレートの全てが RMS レート（50, 40, 35, 45）（表 10 の最下段）を上回っていることを確認する。参考として，レートの可視化の例を図 3 に示す。

なお，RMS レートは一つの目安である。既に顕在化した特定リスクへの対応など，不正の特性や文書の使用実態を踏まえたうえで，追加的，補完的な対策技術の検討が必要である。

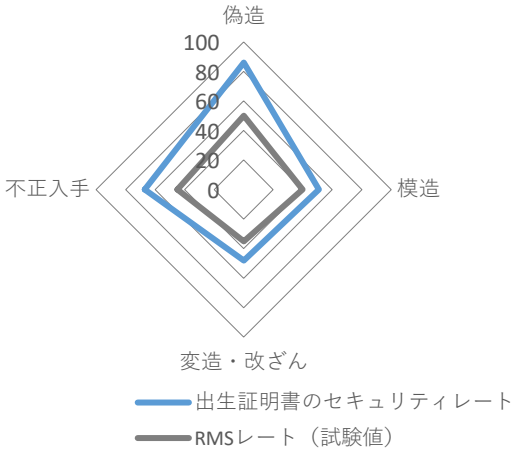

図 3　セキュリティレートの可視化

5　DOVIDs の補足説明

DOVIDs とは，Diffractive Optically Variable Image Devices の略語であり，光学的変化素子（OVDs：Optical Variable Devices）の一種である。OVDs は，見る角度によって色や絵柄が変化する特性を有し，視覚的に分かりやすく，コピー機などでは再現できないため，広く利用されている。OVDs は，干渉，回折，屈折を利用した素子に大別され，クレジットカードや日本の紙幣に使用されるホログラムは，回折を利用した素子であり，DOVIDs に分類される。各技術の一例を図 4 に示す。これは，文献 [7]に掲載された図を参考に，規格利用者の使い勝手を考慮し，検討会で作成したものである。

なお，附属書 E や図 4 に記載された技術は全ての技術を網羅しているわけではない。新しい技術が開発され続けているため，最新技術の確認を推奨する。

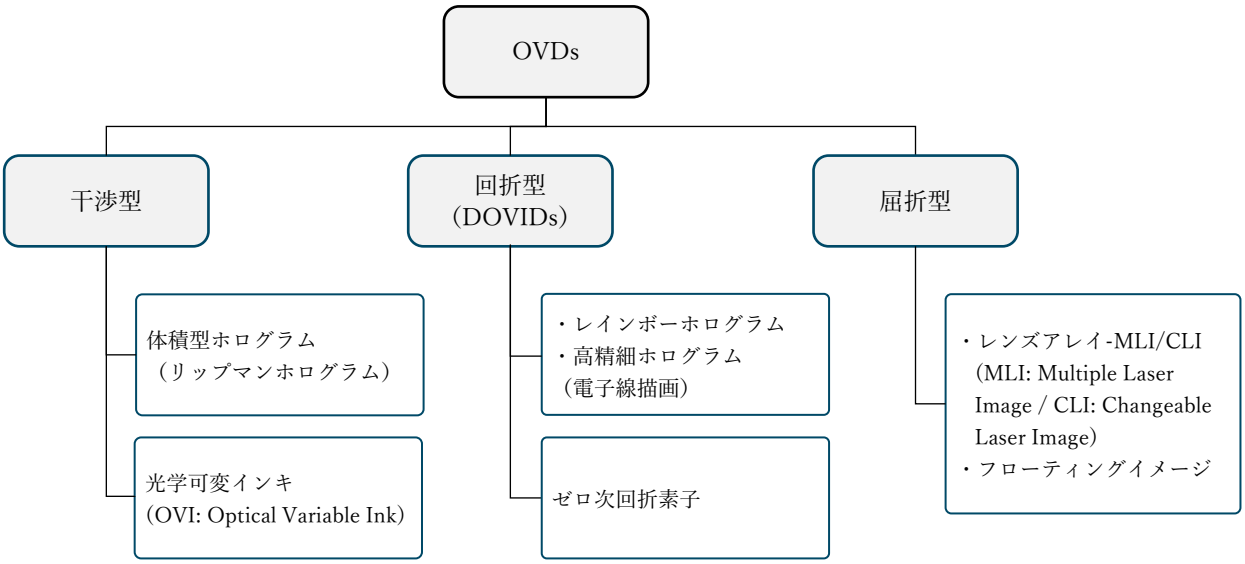

図 4　OVDs の分類

参考文献

[1] ISO/IEC, ISO/IEC Directives, Part 2 Principles and rules for the structure and drafting of ISO and IEC documents, ISO/IEC, 2021.

[2] International Organization for Standardization, “Risk Management ISO 31000 (PUB100426.pdf),” 2018.

[3] IEC, IEC 31010:2019 Risk management — Risk assessment techniques, IEC, 2019.

[4] CIA フォーラム No.a3 ＥＲＭ研究会（第９期）, “リスク評価手法の内部監査での 25 の活用事例,” 一般社団法人 日本内部監査協会, 2016.

[5] 日本機械工業連合会, “メーカのための機械工業界リスクアセスメントガイドライン,” 日本機械工業連合会, 2010.

[6] ISO/IEC, “ISO/IEC 27005:2022 – Information security risk management,” ISO/IEC, 2022.

[7] R. L. v. Renesse, Optical Document Security, Third Edition, Artech House, 2005.

ISO 22388 対訳版検討会メンバー構成表（五十音順）

	氏名	所属
（座長）	小　尾　高　史	国立大学法人東京科学大学
（幹事）	榊　原　幹　彦	株式会社セキュリシス総合研究所
（委員）	赤　尾　佳　則	科学警察研究所
	鎌　田　康　昌	TOPPAN エッジ株式会社
	鈴　木　宏　昌	特種東海製紙株式会社
	関　根　　聡	特種東海製紙株式会社
	花　田　朋　広	東洋インキ株式会社
	村　松　正　男	次世代 IC カード研究会
	山　内　　豪	大日本印刷株式会社
	家根田　正　美	一般社団法人日本資金決済業協会
（オブザーバ）	坂　本　敦　志	三井住友カード株式会社
	渡　邉　恵　美	株式会社ジェーシービー
（事務局）	岩　﨑　　健	独立行政法人国立印刷局
	川　口　泰　正	独立行政法人国立印刷局
	杉　山　博　之	独立行政法人国立印刷局
	長　澤　慎之介	独立行政法人国立印刷局
	山　越　　学	独立行政法人国立印刷局