- 国の機関と契約し、その機関の労働力の一部として働く民間企業の従業員（一般にコントラクターと呼ばれる）。
- 国家政府と契約している民間企業の従業員で、主に連邦政府機関の従業員とは別に企業拠点で働きながら、政府プロジェクトに従事する者（一般にコントラクターとも呼ばれる。）
- 連邦機関に物品またはサービスを供給する民間企業の従業員で、そのために連邦施設への立ち入りが必要となる場合がある。従業員に対する信頼のレベルは、その職責によって異なる。信頼度が高いほど、USG は個人の経歴を理解するために多大な努力を払い（バックグラウンド調査）、より高い基準を設定する。

米国のシステムでは、これらの信頼レベルは階層化されており、その間に重複があるが、以下のように構成される（図 4-2-c）。
クレデンシャル、適性、および適格性。

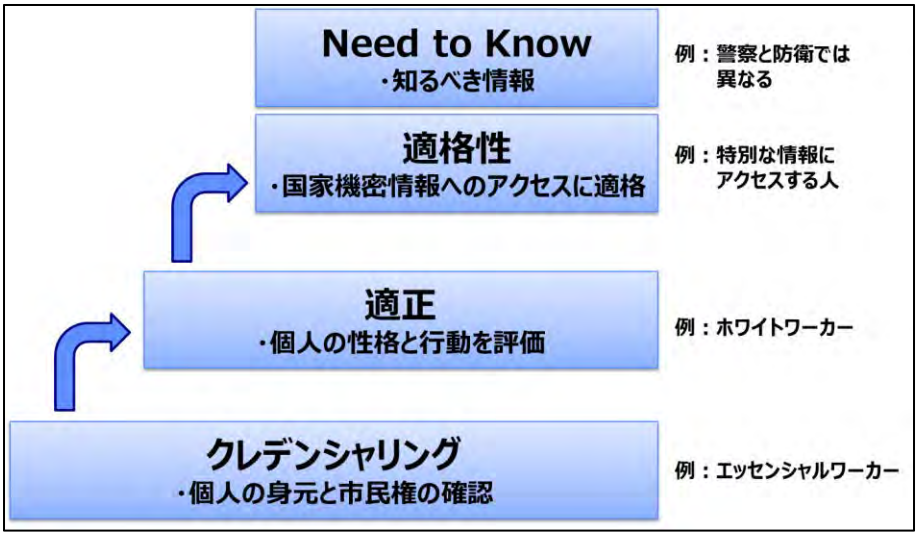

図 4-2-c 信頼レベルの階層化

- クレデンシャルは、信頼の基礎となるレベルで、通常、個人の身元と市民権の確認が含まれる。クレデンシャルは、連邦施設への労働者のアクセス（業者、清掃員、造園作業員など）を許可するための独立したプロセスとして実施される場合もあるが、適性と適格性を決定するための連続した各レベルの審査の最初のステップとしても実施される。

- 適性は、個人の性格と行動を評価し、連邦政府の労働力の一員となるのにふさわしいかどうかを確認するものである。適性とは、政府で働く、または政府と共に働く個人に寄せられる公的信頼のレベルを指す。公的信頼には、2 つの明確なレベルがある。基本的な公的信頼はすべての連邦職員に適用され、高い公的信頼は、指導的地位にある者、および機関の指導、財務管理、買収、または安全/セキュリティ機能など特定の職務を伴う責任を負う地位に適用される。

- 適格性は、特に国家安全保障の機密情報へのアクセスを必要とする職種に関連するものである。米国政府の区分システムには、いくつかの区分レベルがあり、各区分レベルに固有の意思決定のための手順と基準が使用されている。これらの基準は、ある機関の決定を、情報を共有し、または同じ人物と仕事をする他の機関が信頼できるようにするために、すべての連邦機関で統一的に採用されることになっている。

なお、クレデンシャル、適正、適格性をパスした後に、さらに、政府機関ごとに必要となる情報が異なるために、Need to Know の原則によって必要な信頼レベルが付与される。

6. 人事考課のライフサイクル

このような背景のもと、典型的な事例をもとに、審査のライフサイクル（図 4-2-d）に沿って、そのプロセスや各主体の役割について説明する。

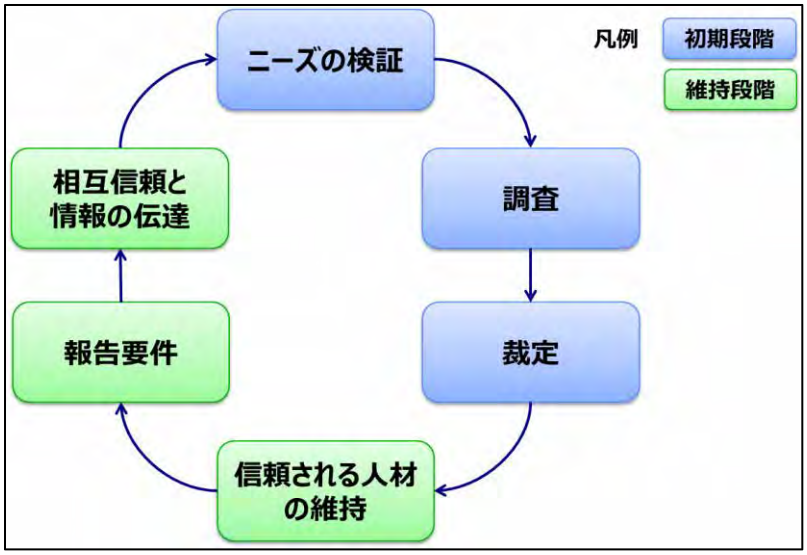

図 4-2-d 人事考課のライフサイクル

- ニーズの検証

個人の雇用形態が確立されると、政府関係者は、その人物が信頼される立場にいる必要性を検証し、最終的な判断につながる調査プロセスを開始しなければならない。この政府関係者は、ある機関の雇用権限者あるいは、契約社員やベンダーが機関のプロジェクトで働く必要があると判断した契約担当者あるいは、ある個人が政府施設に立ち入る必要があると判断した政府関係者かもしれない。いずれにせよ、調査プロセスは常に、政府関係者がその人物の必要性を確認し、どの程度の信頼が必要かを判断し、どのような種類の調査が必要かを決定することから始まる。

- 調査

機関は、特定の信頼レベルの従業員の必要性を検証した後、調査サービス提供者に調査を依頼する。依頼された調査は、監督機関が定めた基準に従って、雇用形態と信頼レベルに対応するものである。調査プロセスは、個人の人格、行動、信頼性について判断できるように、個人の履歴の基本的な要素を確認することを目的としている。

調査プロセスは、調査対象となる個人（調査対象者と呼ぶ）から情報を収集することから始まる。調査対象者の個人履歴情報の収集は、求める信頼の度合いに応じて、標準的なフォーマット（図 4-2-e）を使用する必要がある。

このような書式は、政府が管理する一元的なオンライン・アプリケーションを通じて記入できるようにする必要がある。このプラットフォームは、一連の質問を行い、対象者の回答に応じて、必要に応じてフォローアップの質問をしたり、次の話題に移ったりして、対象者からすべての関連情報を収集できるようにすべきである。

被験者から直接情報を収集することには、2 つの目的がある。1) 対象者は通常、自分の経歴について最も正確な情報を持っている、2) 対象者は、この情報を提供する際に、真実かつ完全であることを法的に証明する。対象者が書式に虚偽又は誤解を招く情報を記入したことが判明した場合、裁決者はこの事実を考慮し、信用レベルを付与するか否かを決定することができる。書式には、対象者及び第三者の情報源から情報を収集するために、日本の法律の下で必要 なあらゆるリリース又は同意が含まれるべきである。

調査によってカバーすることが不可欠な個人履歴の要素は、出生、市民権、忠誠心、教育、雇用、軍務、婚姻状況/履歴、家族、個人的および職業上の照会、住居、財政責任、犯罪歴、心理的および感情的健康、違法薬物の使用、アルコール使用、情報技術の使用、政府に敵対するグループとの提携、外国人との接触、ビジネスまたはその他の関連（資格および国家安全保障上の機密職の場合）である。

調査の範囲は、対象者の年齢、求める信頼の度合い、過去に政府による調査を受けたことがあるかどうかによって異なるが、何年分の履歴をカバーするかは、対象者の年齢によって異なる。一般的に、最初の調査は対象者の 18 歳の誕生日までさかのぼり、年齢が高い場合や過去に調査を受けたことがある場合は、過去 7 年、10 年、15 年などさまざまな期間をカバーすることになる。

調査における情報収集の手段としては、対象者の申請書の入手、訓練を受けた調査員による対象者へのインタビュー、自動化された手段または訓練を受けた調査員による公的記録（出生、教育、雇用、居住、犯罪行為など）の入手、個人および職業上の推薦人、隣人、同僚、家主、その他事件に関連する人へのインタビュー（すべて訓練を受けた調査員により行われる）などがある。

すべての取材が完了したら、報告書または調査書を依頼元に提供し、依頼元が対象者について信頼性の判断を下せるようにする。調査報告書は、電子的にアーカイブされ、将来の問い合わせの際に他のオフィスが発見できるようにする必要がある。

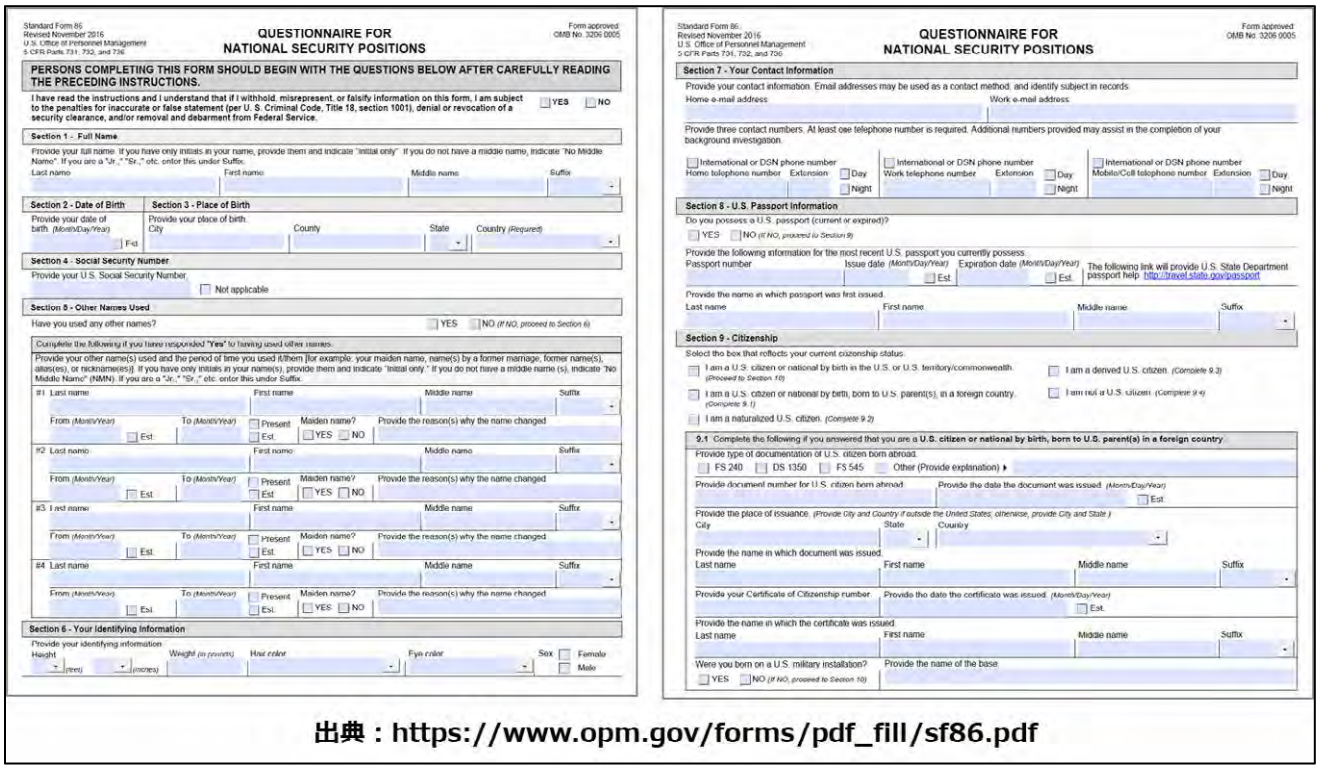

図 4-2-e Standard Form 86 の抜粋（質問票 100 ページ以上にのぼる）

- 裁定

裁定は、機関がその対象について信頼判断を下すステップである。大まかに言えば、これらの基準は、性格、行動、および意思決定のパターンに関する同様の問題を対象としているはずであるが、注目に値するいくつかの違いがある。前述のとおり、適性および資格認定基準は、国家安全保障裁定ガイドラインとして知られる、機密情報へのアクセス資格の基準には存在しない柔軟性を、省庁の長に認めている。また、外国の影響力や外国人の好みに関する事項は、適格性基準にのみ含まれ、適性および資格認定には含まれない。

裁定ガイドラインのトピックは以下の通りである。

- 国家への忠誠
- 海外影響力
- 外国人優先順位（該当する場合）
- 性行動
- 個人的な行動
- 財務上の考慮事項

- アルコール摂取量
- 薬物への関与と薬物乱用
- 心理的条件
- 犯罪行為について
- 保護された情報の取り扱い
- 外部活動
- 情報技術の活用

裁定プロセスでは、訓練を受けた裁定者が、調査で収集されたすべての情報を評価し、対象がその信頼レベルの調査基準を満たしていることを確認し、その結果を分析して、集合的に対象者の積極的な性格、行動、信頼性を確認するかどうかを決定する。もし調査が、上記の裁定ガイドラインに関して対象者に否定的な情報を含む場合、裁定者はその情報を分析し、最終決定（承認または不承認のいずれか）を下すのに十分な情報があるかどうか、発生した問題を解決するためにさらなる情報が必要であるかどうかを判断する。さらなる情報が必要な場合、さらなる調査のために案件を差し戻すか、対象者と直接問題を解決するために対象者の面接を実施することがある。裁定ガイドラインには、この分析を支援するガイドラインのトピックごとに考慮すべき特定の要因が含まれている。対象者が承認された場合、検証された必要性に応じて、雇用、クレデンシャル付与、またはアクセス権付与を行うことができる。対象者が不承認となった場合、信頼される地位への雇用形態を進めない可能性がある。機密情報へのアクセス資格が否定された場合、USG の方針により、対象者はこの決定を行った機関の長に上訴することができる。この決定は、後のセクションで説明するように、政府全体のデータベースにも記録される。

- 信頼される人材の維持

政府機関は、裁定が下された後も、信頼される従業員の行動の変化と考えられるリスクレベルを確実に認識するために、様々なプロセスやツールを使用する必要がある。米国の古い慣行では、5 年から 10 年の間隔で定期的に再調査することが義務付けられていたが、この方法の有効性に関する最近の評価により、継続的評価として知られる、よりダイナミックで効果的なアプローチが生み出された（図 4-2-f）。米国セキュリティクリアランス専門家は、この戦略の採用を推奨している。

このプロセスでは、関連する電子データソースが継続的に参照されるため、機関は、5 年または 10 年のサイクルよりも早く、セキュリティ関連情報を知るために対象者をより継続的に調査することができる。機関は、この継続的な報告から発生する問題を解決し、その個人が機密情報にアクセスする資格を持ち続けるかどうかを判断することが求められている。

注：米国政府の政策は、再調査の要件を継続的審査モデルに置き換える方向に進んでいるが、この取り組みはまだ発展途上にある。米政府機関は現在、継続的な審査要件をカバーするプログラムを試験的に実施しており、監督当局は最近、政府全体にわたるセキュリティ、適性、および資格認定プログラムをよりよく統合するために計画された改革を各機関に知らせるため、政策の一般声明を発表した。初期の結果は有望であっ

た。

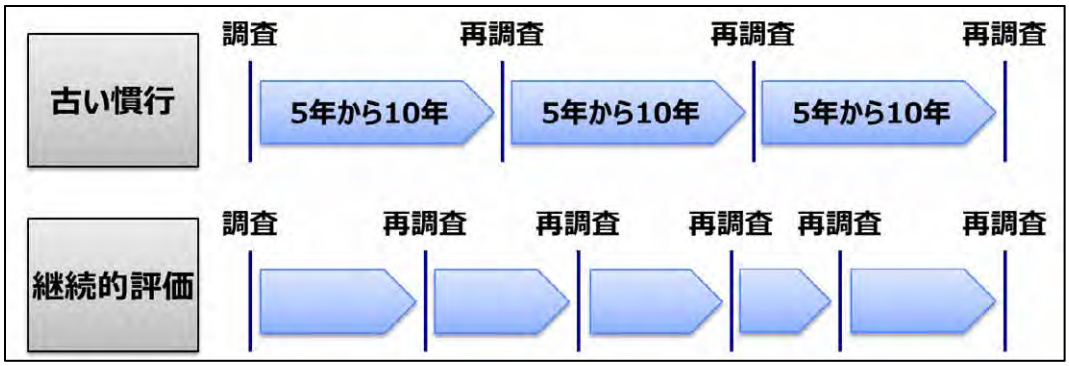

図 4-2-f 再調査の比較イメージ

- 報告要件

機密情報へのアクセス資格を維持するために、職員は特定のセキュリティ関連情報を、その許可を与えたセキュリティ担当者に報告することが義務付けられている。こうした職員からの報告は、図 4-2-g に示すように、継続的評価を有効なものとするために役立つ。

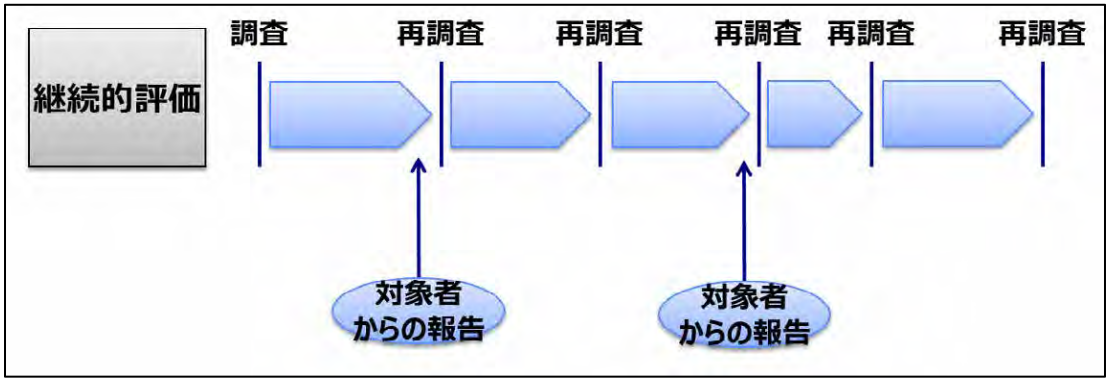

図 4-2-g 報告要件が役立つイメージ

- 相互信頼と信頼の伝達

他の労働力と同様、政府の職員や請負業者は、時間の経過とともに職を変える。政府は、人材を審査する際にかなりのリソースを費やすため、ある機関（または政府プログラムに携わる請負業者）で行われた信頼の決定を、その個人が別の機関で信頼される立場になったときに認識することは、政府の利益となるのである（図 4-2-h）。このプロセスは、信頼の移転と呼ばれ、次のようないくつかの形態がある。ある機関の政府職員が別の機関の職員になる、ある政府プログラムに従事している契約者が別の政府プログラムに従事するために再配置される、契約者が自分の会社を辞めて政府職員になる、政府職員が政府プログラムのための仕事をする会社に勤めるために政府を離れるなどである。

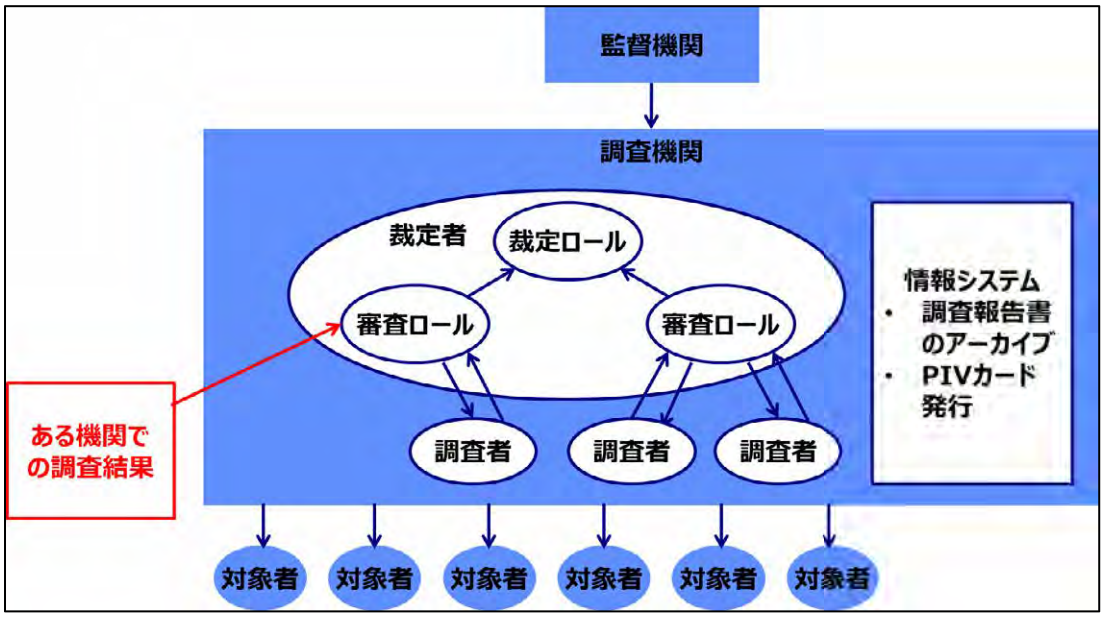

図 4-2-h 信頼の移転のイメージ

7. 人事考課の予算上の留意点

以下は、人事考課プログラムを開発する際に考慮すべき重要な予算と資金調達の項目である。これらの項目は、米国の制度における既知または推定コストに基づく。

- 調査

これは、機密または極秘情報へのアクセスのための資格に関する裁決を通知するために関連情報を収集する審査プロセスの部分である。国防総省防諜安全保障局は、米国政府で最大の統合調査機関である。米国政府の職員、請負業者、その他の関連会社に対する調査の約 95%を実施している。DCSA は、その調査機能を運転資金によって運営しており、以下の費用は、顧客機関への請求価格 に基づいている。この価格設定には、調査要員およびインフラ（施設、IT、機器、車両など）の全費用が含まれる。

調査 1 件あたりの 2024 年のコスト予測。

- ハイティア（トップシークレットまたはパブリックトラスト） - 5,190 ドル
- ミドルティア（秘密または適性） - 715 ドル
- ローティア（クレデンシャル） -180 ドル

- 開始と裁定

これは調査のフロントエンドとバックエンドである。開始は、機関が調査の対象となる候補者を特定し、行動を開始するプロセスである。裁定は、調査結果に基づいて、機関が適格性または適性を最終的に判断す

るプロセスである。米国の制度では、この 2 つの活動は、各雇用機関によって個別に実施され、資金が提供される。さらに、クリアランスの判定によっては拒否されることもあり、また既存のクリアランスの中には理由があって取り消されることもあるので、各機関は不服申し立てプロセスを計画し、予算を立てる必要がある。これらの費用は、依頼する機関の規模によって異なるが、現在の経験に基づく推定では、上記の調査費用に 10〜20%上乗せされると思われる。調査と裁定の両方を中央の組織に組み込むことで、ある程度の節約になる可能性がある。

米国の国家安全保障環境では、職員の審査にかかる費用は政府のみが負担する。産業界は、人事調査のための調達と支払いを行うことは許可されていない。これは主に、1) 産業界が調査プロバイダーに追加要件をいっぱいにさせ、政府のリソースで処理できる量を超えてしまうことが懸念される、2) 誰かのクリアランスを開始するかどうかは、本質的に政府の決定である、3) クリアランスにかかる費用は政府が吸収し、通常契約には含まれない、などの理由による。

8. 結論

本節は、日本における人事評価制度の構築、整備、実行のための有効な根拠と枠組みを提供するものである。信頼の裏切りによるリスクは現実のものであり、国家、経済、社会の各分野にわたって対処されるべきものである。このプログラムのための権限を与える法律の制定は、この努力の成功のための重要な触媒となるであろう。

第３節 データ区分フレームワーク

本節では、日本の国益を守るために特定の情報を機密として保持するための、データ区分のフレームワークについて述べる。

1. エグゼクティブサマリー

敵対者は、国家の防衛や経済的な優位性を高めるために開発された機密情報や技術を発見、収集、利用する機会を常にうかがっている。すべてのものを同じレベルで保護する必要があるわけでも、保護できるわけでもないことを理解した上で、機密情報を明確に特定し、その潜在的な損失のリスクと影響を理解し、そのデータに対して優先順位をつけた保護スキームを開発することが重要である。このようなプログラムは、今日の日本のインフラでは広く開発されておらず、受け入れられていない。プロトコルがないため、政府や業界の関係者は、意図的・偶発的な暴露や侵害から情報を保護する方法について十分な指針を得られないままとなっている。

日本にとって、国家、経済、社会の優先事項を保護するためには、これらの優先事項の成功に不可欠な情

報と技術を保護する必要がある。このような努力の基礎となるのは、重要な情報および技術の要素を特定し、リスク値を割り当てること、つまり本質的にはセキュリティ区分システムであり、これにより保護システムに情報を与え、定義することが義務付けられることであろう。このようなプログラムは、国家資産の保護に向けた国家的な取り組みとして展開されれば、その効果は大きく高まるだろう。同時に、企業も自社の専有情報や技術を特定し、保護するための同様のプログラムを企業規模で開発することを検討する必要がある。

日本の国益を守るためには、特定の情報を機密として保持し、権限を与えられた関係者の間で安全に共有することが必要である。この区分の枠組みは、日本の国民、利益、制度、国家安全保障、および同盟諸国との交流を保護することのみを目的として設定される。

2．フレームワーク概要

この推奨されるフレームワークは、日本政府および関連省庁の管理下にある国家安全保障およびその他のクラスの情報を区分し、保護し、機密指定を解除するための統一的なシステムを説明するものである。最初のステップは、このプログラムのための権限を定義することである。この権限は首相官邸にあり、監督責任は内閣レベルの省庁にあることが推奨される。この提言には 2 つの例がある。米国（US）の情報区分システムは、国家安全保障法（1947 年）にそのルーツがある。これは政府全体で統合された最初の区分の枠組みであり、第二次世界大戦中の情報保護と共有に関する教訓と課題に対応して策定されたものである。その権限は行政府にあり、省庁レベルで実行され、国立公文書記録管理局の一部門である情報セキュリティ監視局（ISOO）が監督している。同様に、イギリス（UK）のシステムは、1911 年に制定された Official Secrets Act（公的秘密法）に端を発し、最近では 1989 年に更新されている。英国のプログラムは陛下の政府の下にあり、実行は内閣府によって行われる。

このフレームワークの多くは米国の区分システムに基づいているが、効率化のために 3 段階（最高機密、機密、極秘）から 2 段階（最高機密、極秘）に引き下げられている。この削減案は、米国や他の国々が 3 段階の国家安全保障区分システムを管理した経験に基づいている。米国では、機密と秘密の資料保護については、審査プロセス、物理的セキュリティ、サイバーセキュリティの要件が実質的に同じである。英国の制度では、国家安全保障の正式なレベルはトップシークレットとシークレットの 2 つだけで、このことを認識している。オーストラリアもこの方向で動いている。プログラムの実行において、国家安全保障情報を 2 つのレベルに圧縮することで、複雑さを軽減し、セキュリティプログラムのすべての側面で効率とコスト削減の両方を実現することができる。

同時に、米国と英国はそれぞれ、国家安全保障情報の閾値を満たさない機密情報を認識し、保護するためのプロトコルを備えている。米国では、それは CUI（Controlled Unclassified Information）と呼ばれるものである。英国では、政府公式情報（Official Government Information）となっている。このアプローチでは、広く共有しない行政情報や個人情報を特定し、カタログ化し、保護要件を定めている。

また、経済安全保障と産業情報の保護についても懸念がある。この文書で推奨するプロセスは、産業環境における国家安全保障情報の保護要件を対象としている。企業独自の情報や機密性の高い企業戦略情報は多岐にわたるため、この推奨プロセスは企業環境には容易に適応できない。我々は、企業が組織内でこのフレームワークを検討し、さらに、重要な情報を保護するために利用可能な物理的およびサイバー的なツールや標準を活用することを推奨する。

本節は、マルチレベルの国家安全保障区分システムを構築するためのガイドを提供するものであるが、複雑な情報管理システムへの移行は、多大な労力を要することがある。移行を簡素化するために、日本では段階的な導入アプローチを検討することが推奨される。中央当局は、政府情報を国家安全保障上の機密（および機密と指定）と公的機密（および公式または内部と指定）に分けることによって、システムを開始する必要がある。国家機密のカテゴリーには、国家安全保障に不可欠とみなされるもの、および紛失すると国家安全保障計画に明らかな損害を与えるものすべてを含めるべきである。このプロセスを成功裏に開始し、経験を積んだ後、各省庁は、広範な秘密カテゴリーを、より個別な最高機密と秘密区分の決定へと絞り込むべきである。最終的に、これは 3 段階の情報保護の枠組みをもたらすことになる。最終的には、トップシークレット、シークレット、オフィシャルという 3 段階の情報保護の枠組みになる。

3．フレームワーク目次と注釈

これは、フレームワークのドラフトを構成する各セクションの概要を説明し、各セクションの目的を説明するためのものである。

パート 1：日本版データ区分体系（案）

セクション 1.1　基準
本セクションでは、情報が機密扱いされる前に満たさなければならない条件について述べる。これには、情報が不正に開示されることによって損害が生じる場合は機密扱いされるという前提が含まれる。

セクション 1.2　レベル
本セクションでは、保護が必要な国家安全保障情報に対して、3 段階の区分を定義する。

セクション 1.3　権限
本セクションでは、どの職員が情報を区分する権限を持つか、また、どのような条件でその権限を他者に委譲できるかを定めている。また、そのような職員は、これらの責任について定期的な訓練を受ける必要があることを定めている。

セクション 1.4　カテゴリー

本セクションでは、機密扱いされる可能性のある国家安全保障情報のカテゴリーをリストアップしている。これは米国の制度が使用している区分のリストを適応したものである。日本政府は、国土安全保障省の経験と既存の慣行に基づき、国土安全保障省と協議の上、そのリストを作成・精緻化することが望ましいと思われる。

セクション 1.5　期間

本セクションでは、情報の機密解除の権限と、機密解除が行われる条件について説明する。

セクション 1.6　識別と表示

本セクションでは、機密情報を文書（紙媒体、電子媒体を問わず）内にマーキングする方法について説明する。これは米国のシステムを参考にしたものであるが、第 1.2 項で説明した 2 段階システム案に準拠する。

セクション 1.7　手引き

本セクションでは、何を区分するかという決定をどのように記録し、情報をいつ、どのレベルで区分すべきかというガイダンスとして、従業員に提供するかについて説明する。

セクション 1.8　ガイダンスの適用

本セクションでは、作業レベル担当者が、彼ら自身はもともと情報を区分する権限がないにもかかわらず、どのように機密資料を作成し、取り扱うかについて説明する。

セクション 1.9　機密情報の共有と保護

本セクションでは、機密資料を可能な限り低いレベルで作成するための明確なガイダンスを提供し、「write to release」の概念を紹介する。

パート 2：セーフガード

セクション 2.1　アクセスに関する一般的な制限

本セクションでは、経歴調査や職務に関連した知る必要性など、個人が機密情報へのアクセスを許可されるための要件について述べる。また、そのような人が従わなければならない安全な取り扱いと保管の手順についても説明する。

セクション 2.2　普及のためのコントロール

本セクションでは、情報を安全に共有する必要性と、正式なセキュリティクリアランスを持たない人物と機密情報を共有することが日本政府の利益になる場合の特別な状況について説明する。

パート 3：実施と見直し

セクション 3.1　一般的な責任

本セクションでは、日本の区分システムの実施を担当する職員の責任について説明する。

セクション 3.2　説明責任と懲戒処分

本セクションでは、本プログラムで確立された機密情報手続きに違反した場合に、どのような結果がもたらされるかについて説明する。

パート４：コスト

本パートでは、費用について簡単に説明する。

パート５：まとめ

本パートでは、結論となる考えを述べる。

4．パート１：日本版データ区分のフレームワーク（案）

セクション 1.1　基準

(a)情報は、以下の条件をすべて満たす場合にのみ、最高機密または機密レベル（セクション 1.2(a)を参照）に区分することができる。

(1)権限を与えられた区分担当者が情報を区分する。

(2)その情報が日本政府によって所有され、日本政府のために作成され、または日本政府の管理下にある場合。

(3)このフレームワークの 1.4 節に記載されている情報のカテゴリーの一つ以上に該当すること。

(4)権限のある区分担当者が、情報の不正な開示が国家安全保障に損害を与えることが合理的に予想されると判断し、かつ、権限のある区分担当者がその損害を特定または説明できる場合。

(b)情報を区分する必要性について重大な疑念がある場合、その情報は区分されないものとする。

セクション 1.2　レベル

(a)情報は、以下の 2 つのレベルのいずれかに区分されることがある。

(1)「最高機密」は、不正に開示されることにより日本の国益または国の安全が著しく損なわれることが合理的に予想される情報で、権限を与えられた区分担当者が特定または説明できるものに適用されるものとする。

(2)「秘密」は、不正に開示されることにより日本の国益または国の安全が損なわれることが合理的に予想される情報で、権限を有する区分担当者が特定または説明できるものに適用される。

(b)法令に別段の定めがある場合を除き、日本の機密情報を識別するために、他の用語を用いてはならない。

(c)適切なレベルの区分に重大な疑義がある場合は、より高いレベルで区分されるものとする。

セクション 1.3　権限

(a)情報を区分する権限は、以下に限定して行使することができる。

(1)内閣レベルの国家安全保障局（NSS）構想の事務局長に就任した。

(2)外務省、国防省、国家安全保障局長の各長官、および。

(3)本項(c)に従ってこの権限を委任された日本政府の職員。

(4)基準 1、2 又は 3 に該当する職員は、日本国民でなければならず、上記 2 又は 3 により委任又は指定された職員は、区分権者としての役割を果たす組織の事項に関し、明白な資格及び経験を有する者でなければならない。

(b)情報を区分する権限のある職員は、あらゆるレベルの区分を行う権限を有する。

(c)区分の権限を委譲する。

(1)区分権限の委譲は、この枠組みを運用するために必要な最小限のものに限定されなければならない。権限を与えられた区分担当者は、委任された下位の職員が、この権限を行使する実証的かつ継続的な必要性を有することを確認する責任がある。

(2)区分の権限の委任は、それぞれ文書で行わなければならず、本規定に定める場合を除き、その権限を再委任してはならない。各委任は、氏名又は職名により職員を特定しなければならない。

(d)すべての区分担当者は、適切な区分と機密解除に関する研修を受けなければならない。

セクション 1.4　カテゴリー

(a)情報は、その不正な開示が、本命令の 1.2 項に従って、日本の国益又は国の安全保障に識別可能又は記述可能な損害をもたらすことが合理的に予想される場合でなければ、区分の対象となるものとみなしてはならない。

(b)この枠組みは、日本の国家安全保障を保護するために情報を区分することと、その他の省業務の遂行に関連する、国家安全保障以外の利益のために区分することを区別する。国家安全保障情報の保護、取り扱い、共有、機密解除にのみ適用される具体的な慣行は、この枠組み全体を通じて規定される。このため、国家安全保障に関連する情報の特定のカテゴリーは、以下の 1 つ以上を含むものとして定義される。

(1)日本当局が検討している審議事項。

(2)軍事計画、兵器システム、または作戦。

(3)国の安全保障に関わる外国政府の情報。

(4)情報活動、情報源や情報方法、暗号学。

(5)日本国の外交関係または対外活動（秘密情報源を含む）。

(6)国家安全保障に関連する法執行情報。

(7)国家安全保障に関連する科学、技術、または経済的な事項。

(8)国家安全保障に関連するシステム、施設、インフラ、プロジェクト、計画、または保護サービスの脆弱性または能力。

(c)国家安全保障業務に関する区分の定義については、各省庁の権限に委ねられる。各省庁の長は、このような指定に関する最終的な権限を持つ。

セクション 1.5　期間

(a)情報を機密解除する権限は、その情報が国家安全保障上の理由で機密化されているか、あるいは、セクション 1.4 で詳述されているように、省庁が行う国家安全保障以外の業務で機密化されているかによって決まる。国家安全保障上の機密情報の場合。

(1)NSS のみが、セクション 1.4(b)に記載されているように、国家安全保障上の理由から区分されていた記録、文書、その他の資料の機密を解除することができる。

(2)情報は、1.1 項の区分の基準を満たさなくなったとき、あるいは NSS の判断により、公共の利益が情報保護の必要性を上回ったときに、機密解除可能であるとみなされる。

(3)情報は、本セクションに従って機密解除が命じられるまで、機密のままでなければならない。

(4)機密情報は、NSS が決定した場合のみ公開される。

(5)閣僚は、NSS に国家安全保障情報の機密解除を要請することができる。要請は NSS のスタッフを通じて行われ、NSS のスタッフは、NSS に問題を提示し決定する際に、すべての省庁の公平性を考慮することを保証する。

(b)省庁が行う国家安全保障以外の業務案件の場合。

(1)セクション 1.4 に記載されているように、国家安全保障以外の理由で区分された記録、文書、その他の資料の機密解除は、省庁の長のみが行うことができる。

(2)情報は、セクション 1.1 の区分の基準を満たさなくなったとき、又は省令で定めるところにより、公共の利益が情報の保護の必要性を上回ったときに、機密解除可能であるとみなされるものとする。

(3)情報は、本セクションに従って機密解除を命じられるまで、機密扱いのままであること。

(4)機密扱いの情報は、省庁の長が決定した場合のみ公開される。

セクション 1.6　識別とマーキング

(a)資料が最初に区分された時点で、NSS が発行する指示に従い、以下の事項を一目でわかるように表示しなければならない。

(1)本パートのセクション 1.2 に定義された 3 つの区分レベルのうちの 1 つを指す。

(2)権限のある区分担当者の名前と職位、または個人識別情報による身元。

(3)特に明記されていない場合は、原産省および原産地。

(4)セクション 1.4(b)項の該当する区分項目、または本省固有の主題領域のいずれかを引用した、簡潔な区分理由。国家安全保障上の理由が引用される場合、文書の表示において、セクション 1.4(b)のサブパラグラフを明示するものとする。

(5)適用可能な普及コントロール（セクション 2.2 に記載）。

(b)各区分された文書に関して、その文書を作成した省は、マーキングまたはその他の手段により、どの部分が区分され、どの部分が非区分であるかを示すものとする。

セクション 1.7　手引き

(a)区分ガイドとは、区分を必要とする個々の情報要素を特定する、当初の区分決定の記録である。組織

内で標準化され、使用されることにより、情報の適切かつ均一な区分が可能になる。
(b) NSS は、権限のある区分担当者に区分ガイドの適切な作成方法を指導するためのマニュアルを発行するものとする。
(c)権限ある区分担当者は、自らが権限を有する情報のための区分ガイド（又はガイド）を作成しなければならない。　これらのガイドは、NSS が発行したマニュアル及び上級省職員が定めた関連する省内手続きに従わなければならず、少なくとも年 1 回は最新の状態に保たなければならない。NSS は、すべての区分ガイドのための中央保管庫を維持しなければならない。

セクション 1.8　ガイダンスの適用
(a)機密情報の保有者は、機密情報を含む文書の作成、編集、複製、要約、またはその他の作業を行う際に、区分ガイドのすべての指示を参照し、これに従わなければならない。このような保有者は、NSS が提供するガイダンスに従って区分記号を適用しなければならない。
(b)区分記号を適用する者は、以下を行わなければならない。
(1)各区分の派生的な行動において、氏名と職位、または個人識別情報によって、すぐにわかるように識別されること。
(2)権限のある区分担当者の決定を遵守し、尊重すること。
(3)新たに作成された文書には、原文にある適切な区分記号を適用する。
(c)機密情報の保有者は全員、その適切な運用に関する訓練を受けなければならない。

セクション 1.9　機密情報の共有と保護
(a)機密文書または資料は、最も広範な普及と利用を保証するために、可能な限り低い区分レベルで作成されるものとする。より高い保護が必要な機密情報は、アクセスを適切に管理するための配布コントロールを使用する、より高いレベルで区分された文書または添付資料で提供されるものとする。
(b)より広範な情報共有が必要な場合、職員は必要に応じて機密情報を排除し、より低い機密、あるいは非機密の文書を作成し、利用者に有用な情報をできるだけ低いレベルで提供する「ライティング・トゥ・リリース」を行う。

5．パート２：セーフガード

セクション 2.1　アクセスに関する一般的な制限
(a)ある者は、次の条件を満たせば、機密情報にアクセスすることができる。
(1)人事課による調査及び人事課からの勧告を受け、アクセス資格の有利な決定が省庁によってなされた場合。
(2)その人が承認された秘密保持契約に署名していること。
(3)そのような決定に責任を負う省庁の上級職員によって決定された、その情報を知る必要がある人。
(b)本セクション(a)の機密情報へのアクセス基準を満たした者は、機密情報の適切な保護に関する訓練を受けなければならない。

(c)日本政府の役人または職員は、政府の管理下から機密情報を取り除くこと、または政府の管理下から取り除くために情報の機密解除を指示することはできない。
(d)機密情報は、適切な許可なく日本政府の公式施設から持ち出すことはできない。
(e)NSS 外で機密情報を発信する権限を有する者は、NSS 内で提供されるのと同等の方法で、情報の保護を確保するものとする。
(f)NSS は、機密情報を収集、作成、通信、計算、配布、処理、保管するネットワークや電気通信システムを含む自動情報システムに対して、統一された手順を確立しなければならない。
(1)不正なアクセスを防止する。
(2)情報の完全性を確保すること、および
(3)以下を実務上可能な限り使用する。
(A)認可された利用を促進する形式と方法で、情報の利用可能性とアクセスを最大化する共通の情報技術標準、プロトコール、インターフェース
(B)本パートのセクション 2.1(a)に記載されている基準を満たす人が情報に最大限アクセスできるように、標準化された電子フォーマット。
(g)NSS は、機密情報が適切な保護を提供し、無権限者によるアクセスを防止する条件下で使用、処理、保管、複製、伝送、破棄されることを保証するために、物理的及び技術的なセキュリティ管理を確立しなければならない。
(h)機密情報の権限保持者である要員は、外国政府の情報を、その情報を提供した政府または政府の国際組織が要求する保護と少なくとも同等の程度を提供する基準に基づいて保護しなければならない。
(i)NSS に由来する機密情報は、本枠組みのセクション 2 に基づくアクセスと保護に関する基準を満たす限り、他省庁に広めることが可能である。

セクション 2.2　普及のためのコントロール
(a)機密文書を作成する場合、その文書を受け取ることができる者または受け取ることができない者に関する制限は、承認された配布管理マークを使用することにより、文書上に明確に示されるものとする。例としては、以下のようなものがある。
NODIS=省外への配布禁止
NOFORN=日本人以外の職員への配布禁止
ORCON=発信者管理、受信者は発信元の省庁に相談することなく文書を再配布してはならない、など。
(b)NSS は、承認された配信制御マーキングのマニュアルを発行し、当該マーキングが標準化され、政府全体で統一的に使用されることを確保するものとする。
(c)上級省職員は、本命令のセクション 2.1(a)に規定された基準を満たす個人が、機密情報に最大限アクセスできるようにするための手続きを確立するものとする。
(d)緊急事態において、人命に対する差し迫った脅威に対応するため、または国土防衛のために必要な場合、事務局長またはその指名する者は、機密情報（本枠組みのセクション 2.1（i）に従ってマークされた情報を含む）を、通常アクセス権を持たない個人または個人に開示する権限を付与することができる。本規定に基づき開示された情報は、当該開示またはその後の受領者による使用の結果、機密解除されたと

はみなされないものとする。このような開示は、機密情報の発信者に速やかに報告されるものとする。

6．パート３：実施と見直し

セクション 3.1　一般的な責任

機密情報を発信または取り扱う省庁の長は、以下を行う。

(a)このフレームワークで確立されたプログラムを成功裏に実施するために、上級管理職が個人的なコミットメントを示し、コミットすること。

(b)日本の安全保障上の区分プログラムを効果的に実施するために必要な資源を投入する。

(c)省内の記録システムが、機密情報の適切な共有と保護を最適化するように設計され維持されるようにすること、及び

(d)セキュリティ区分プログラムを指揮・管理する省政府高官を指名し、その責任には以下が含まれるものとする。

(1)NSS が発行するポリシーマニュアルに定められた基準にすべての要素が合致していることを確認するため、省内の区分プログラムを監督すること。

(2)省職員向けの実施規則を発行すること。そのような規則は、NSS と協議の上、作成されるものとする。

(3)省庁のセキュリティ区分ガイドの制作を統括する。

(4)セキュリティ教育・訓練プログラムの確立と維持。

(5)継続的な自己点検プログラムを確立し、維持すること。このプログラムには、同省の区分行動の代表的なサンプルの定期的な点検を含む。

(6)NSS と協働して、区分システムの適切な運用を確保する。

(7)機密情報への不要かつ／または不正なアクセスを防止するための手順を確立すること。

(A)管理上のセキュリティクリアランス手続きを開始する前に、機密情報へのアクセスの必要性を確立することを要求すること。

(B)機密情報へのアクセスを許可された人数が、省内のミッションの必要性を満たすようにすること。

(8)敵対的または潜在的な地域で使用される機密情報を保護するための特別な緊急時対応計画を策定すること。

(9)政府職員を評価するために使用される年次業績評価システムが、以下の職員に対する機密情報の適切な取り扱いに関する評価を含むことを確保すること。

(A)権限を持った区分担当者

(B)セキュリティ管理者またはセキュリティ専門家

(C)その他、機密情報にアクセスできるすべての人員。

(10)省内で区分の責任を与えられた職員が、その職員が区分の責任を持つことになる事項に関して、明白な資格と経験を有していることを確実にすること。

セクション 3.2 説明責任と懲戒処分説明責任と懲戒処分

(a)日本政府の機密情報へのアクセスを許可された者は、故意または過失により適切な懲戒処分の対象となる。

(1)この命令または前任の命令の下で適切に区分された情報を、権限のない者に開示すること。

(2)本枠組みまたは実施指令に違反して情報を区分または区分を継続すること。

(3)本フレームワークの要件に反して、特別なアクセスプログラムを作成または継続すること。

(b)制裁には、譴責、無給の停職、解任、区分権限の終了、機密情報へのアクセスの喪失または拒否、または適用される日本の法律および方針に従ったその他の制裁が含まれる場合がある。

(c)大臣または上級省職員は、少なくとも、本命令の区分基準の適用において無謀な無視または誤りのパターンを示す個人の区分権限を速やかに削除しなければならない。

7．パート４：コスト

この活動には、NSS の少人数のスタッフと、国の区分システムを確立し維持するための各省庁の追加職員が必要である。より正確な数字は、どの省庁が区分の権限を持つか、またどの情報を区分するかという決定によって決まる。より大きなコストは、職員の審査活動と情報システムの安全性報告書にかかるものである。

8．パート５：まとめ

この国家安全保障区分システムの提案は、当然ながら非常に複雑であるが、いったん情報が適切に識別・区分されれば、そのマークは、情報の相対的重要性と機密性、および不正な放出や開示から情報を保護する責任について、情報利用者に最初に通知する役割を果たすことになる。区分システムの開発と維持における厳密さは、省庁間および産業界全体における情報サービスの開発者と提供者に情報を提供する上で重要である。

第４節 技術開発フレームワーク

1．エグゼクティブサマリー

敵対者は、常に人間関係を構築し、機密情報や技術を発見、収集、利用する機会を狙っている。日本政府が包括的な審査プロセスを通じて政府全体の信頼できる人材を確立するのに伴い、政府はその審査をサポートするための技術システムを開発する必要がある。物理的およびデジタル的な識別、認証、アクセスの承認を提供する標準化されたクレデンシャルが最重要である。さらに、政府全体の日本式区分システムの確立に伴い、政府は、個人のクリアランス審査を支援し、適切な区分レベルの機密情報を相応の保護付きで作成、処理、保管するための技術システムを開発する必要がある。

日本の国益を保護するためには、ID 認証およびポリシー・ベースの認可決定を提供することによって、機密情報および施設の基礎的な保護を促進するために、政府全体のクレデンシャルが必要である。この区分の枠組みは、日本の国民、利益、制度、国家安全保障、および同盟国との交流を保護することのみを目的として確立されている。

2．フレームワークの概要

推奨される枠組みは、人員の吟味、区分のための統一システム、および ID、認証、認可のための政府全体のクレデンシャル・システムの確立を支援する技術的な開発について述べている。最初のステップは、プログラムの権限を定義し、包括的な標準と方針を確立することである。人事審査および区分システムのための技術開発は、これらのプログラムの標準、方針、および実行の確立と入れ子になっていなければならない。

日本政府のための ID、認証、および承認システムを含む国家クレデンシャル・システムの確立は、 関連する技術開発と密接に関連している。日本がこの国家プログラムを確立するとき、この権限を首相官邸に発し、監督責任を閣僚レベ ルの省庁に持たせることが推奨される。米国（US）のクレデンシャル標準は、個人識別検証（PIV）クレデンシャルと呼ばれ、2004 年の国土安全保障 大統領指令 12 号（HSPD-12）によって連邦政府内または連邦政府と働く個人向けに確立され、政府 全体の ID、認証および承認システムを提供している。

本書の標準および政策の枠組みの多くは、米国のクレデンシャル・システムに基づいている。これは、米国立標準技術研究所（NIST）が発行した連邦情報処理標準出版物 201-2（FIPS 201-2）の技術的強度と国際的採用により、ID 証明、登録、発行および相互運用性を含む、PIV クレデンシャルのアーキテクチャと技術標準が確立されているためである。さらに、米国で使用される PIV クレデンシャルは、1）物理的識別と認証、および 2）非区分政府ネットワークおよびサービスでのハードウェアに裏付けられたデジタル識別と認証の両方を達成する。スタイルおよび具体的な実装に若干の違いがあるが、同じ FIPS 201-2 標準が多数の国際的パートナーによって採用され、NATO 軍人のジュネーブ条約準拠クレデンシャルにも使用されている。

また、経済的安全性および産業情報の保護に対する懸念も存在する。この文書で推奨するプロセスは、産業環境における国家安全保障情報のクレデンシャル要件を対象としている。企業は、組織内でこの枠組みを検討し、さらに重要な情報および重要な施設を保護するために利用可能な物理的およびデジタルクレデンシャルの枠組みのツールおよび標準を利用することを推奨する。

この文書は、マルチレベルの国家安全保障クレデンシャル・システムを構築するためのガイドを提供するものであるが、その実施には多大な努力が必要である。移行を単純化するために、日本は段階的なアプローチを考慮することが推奨される。中央当局は、最も機密性の高い情報および施設から始めて、クレデンシャル化、物理的および論理的アクセス制御の両方の展開を順次行うことによって、システムを開始すべきである。最終的には、物理的および論理的アクセスの両方に強力な識別、認証、および承認メカニ ズムを与える包括的なクレデンシャル・システムに帰結することになる。

3. クレデンシャルの原則

これは、クレデンシャル用語の概要とそれらに関連する定義を提供し、曖昧さをなくし、フレームワーク全体の一貫性を確立するためである。

(1) アイデンティティ

この報告の目的では、ID は個人が一意に認識できる物理的および行動的特性の集合である。ID の証明とも呼ばれる ID の検証、および信頼とリスクの判断に使用される明示（ポリシー、プロセス、技術）は、検証および信頼された後にその ID の真正性を認証するために使用されるメカニズム とは異なり、別個のものである。

(2) 認証

認証は、真正性の信頼を確立するプロセスである。この場合、人の ID およびその物理的またはデジタルクレデンシャルの検証においてである。クレデンシャル（PIV または運転免許証など）は、「信用または権限に対する自分の権利を証明する証拠、および ID（およびオプションで追加属性）をその個人に権威的に結びつける個人に関連するデータ要素」である。

認証は、3 つの要因の組み合わせに依存する。1) 個人が認知しているもの（パスワードなど） 2) 個人が所有しているもの（バッジ、電話番号、電子メールアカウント、暗号鍵など） 3) 個人の生体的な証し（指紋などの生体データなど）である。 認証プロトコルは、より安全でユーザーフレンドリーな標準に進化し続けている。

物理的認証は、最も一般的には ID バッジで実装される。バッジの中には、視覚的認証のみを提供するものもあるが、磁気ストリップ、無線周波数識別（RFID）パッシブ認証、バーコード、集積回路チップに格納された暗号キーなど、追加の認証メカニズムを持つものが多い。

最も一般的なデジタル認証は、「あなたが知っている何か」としてパスワードを使用することに変わりはない。ユーザー名と組み合わせた場合、ほとんどのシステムやウェブサイトでは、これがデフォルトになっている。

多要素認証は、しばしば MFA または 2 要素認証の 2FA と呼ばれ、2 つ以上の要素を使用して、セキュリティと真正性の信頼性を向上させるものである。公開鍵基盤（PKI）暗号を使用する MFA は、クレデンシャルの真正性を数学的に検証するメカニズムを提供し、セキュリティが重要なアプリケーションでよく使用される。

X.509 公開鍵暗号化標準は、認証用の暗号クレデンシャルを生成するために一般に使用される。X.509 証明書は、認証局によって署名されるか、または自己署名されるデジタル署名を使用して、ID を公開かぎと暗号的に結合する。証明書が信頼できる認証局によって署名されるか、または他の手段によって検証されると、証明書および対応する公開鍵は、他の当事者との安全な通信を確立したり、対応する秘密鍵によってデジタル署名された文書を検証するために使用することができる。X.509 のライフサイクルには、4 つの重要なステップがある。

·登録 - 認証局がユーザーのために証明書を発行する前に、ユーザーが直接または（認証局から委任された）登録機関を通じて、認証局（CA）に自己を明らかにするプロセス。

·初期化 - クライアントが、インフラストラクチャ内の他の場所に保管されている鍵との適切な関係を持つ鍵材料をインストールするプロセス。例えば、クライアントは、証明書パスの検証に使用するため、信頼できる認証機関の公開鍵及び その他の保証情報とともに安全に初期化される必要がある。クライアントは通常、自身の鍵ペアで初期化される必要がある。

·認証 - CA がユーザーの公開鍵に対する証明書を発行し、その証明書をユーザーのクライアントシステムに返却し、その証明書をリポジトリに掲載するプロセス。

·失効 - 証明書が失効または無効にされ、証明書とシリアルナンバーが一般に公開されている証明書失効リスト（CRL）に追加されるプロセスである。証明書は発行されたとき、その有効期間中ずっと使用されることが期待されている。しかし、様々な事情により、証明書が早期に無効となることがある。

Fast Identity Online 2 (FIDO2) は、FIDO アライアンスの最新仕様の包括的な用語で、モバイルとデスクトップ環境の両方でオンラインサービスを容易に認証するために、一般的なデバイスを活用するように設計されている。FIDO プロトコルは、X.509 などの標準的な公開鍵暗号を使用し、より強力な認証を提供する。オンラインサービスに登録する際、ユーザーのクライアントデバイスは新しいキーペアを作成する。秘密鍵を保持し、公開鍵をオンラインサービスに登録する。認証は、クライアントデバイスがチャレンジに署名することで、秘密鍵を所有していることをサービスに証明することで行われる。クライアントの秘密鍵は、ユーザーによってデバイスのローカルロックが解除された後でのみ使用できる。ローカルロック解除は、指のスワイプ、PIN の入力、マイクへの発話、セカンドファクターデバイスの挿入、ボタンの押下など、ユーザーフレンドリーで安全な操作で実現される。

(3) オーソライズ

認証とは、NIST SP 800-162 に概説されているように、認証されたユーザーに対して以下のような特定の要求を許可または拒否するために使用される一連のポリシーおよび属性である。1) 情報および関連情報処理サービスの取得と使用、2) 特定の物理的施設（建物や軍事基地など）への立ち入りなど。

アクセス制御の判断は、1) 採用時など一度だけ、2) 定期的に、3) 個別に行うことができる。1) 個人の採用時など一度だけ、2) 機密情報へのアクセスのための「適格性」判断など定期的に、3) 建物へのバッジやウェブサイトへのログインなどリクエストごとに判断されるような個別的な場合である。アクセス制御の実装は、ポリシーや標準的な慣行に基づき、その決定を行うために必要なリクエストと認証に固有のものである。この報告では、アクセス制御の実装を詳しく説明しない。アクセス制御の実装は多数あり、微妙に異なる。物理的なアクセスに対する認証が標準化されていても、米国の省庁は、個々の施設や部屋に対して個別にアクセス制御の決定を行うことが多い。

4．パート１：人事考課を支援する技術開発

政府全体の人事審査を確立するためには、必要な情報の収集、資格証明書、適性、および資格判定をサポートする技術システムを開発する必要がある。技術システムは、人事考課をサポートするためにいくつかの機能を実行しなければならない。

(a)国の方針で、候補者が自分自身について提供することが要求されている、または認められているすべての情報を収集する。

(1)テキスト入力、画像、文書のスキャン、転写など、さまざまな種類の情報を必要とすることを考慮する必要がある。

(2)候補者一人ひとりの個人情報は、安全に保護・保管されなければならない。

(3)必要な情報を集めて入力するのは面倒なので、入力システムは、候補者が意図的に完成したパッケージを提出するまで、すべての情報を下書きとして保存しておく必要がある。

(4)情報の入力は、個人のアイデンティティと安全な認証メカニズムに結びつけられるべきである。

(b)必要な身分証明情報を取得する。

(1)パスポートや運転免許証などの身分証明書との相関性について、国家政策を満足させるに足る情報を保存する。

(2)指紋、網膜スキャン、顔画像、DNA、声紋など、国の政策で必要とされる生体情報を取得する。

(c)素行調査の結果を記録する。

(1)要求される様々な種類の情報と報告を考慮しなければならない。

(2)ほとんどの調査は、インタビュー、物理的な場所の訪問、デジタル記録へのアクセスを伴うため、システムはモバイルと定置のユースケースとインターフェースを考慮する必要がある。

(3)調査員は多くの候補者の機密情報にアクセスすることになるため、強力な認証と承認が重要になる。

(d)候補者情報を提供するデジタルシステムとのインターフェース。

(1)可能な限り、国の政策で必要とされるデジタル記録の収集は自動化されるべきである。

(2)金融信用調査、成績表、警察記録、軍歴、納税記録、係争中の訴訟などは、自動プログラミングインタフェース（API）を通じて容易にアクセスできるようにする必要がある。

(3)情報がデジタル化されていない、あるいはプログラム的にアクセスできない場合、国の政策として、これらの投資を義務付ける、あるいはインセンティブを与えることを検討する必要がある。

(e)審査員に候補者のすべての情報を確認する手段を提供すること。

(1)候補者の提供、背景調査、個人の記録情報を一貫したユーザーインタフェースで提供し、裁定者による検討をサポートする。

(2)情報が不足している場合、フォローアップのための重要な質問事項の把握や調査タスクを促進する必要がある。

(f)判定結果の記録

(1)裁決の決定と補足情報を把握する。

(2)自動的または人事担当者による候補者通知のトリガー。

(g)申請者および従業員の裁定状況を確認するための一元的なメカニズムを提供する。
(1)権限のある関係者が一元的にアクセスできる、すべての裁決の記録を提供する。
(2)国の方針に従い、裁決に関連する情報を必要なだけ、あるいは最小限に保存する。

5．パート 2：データ区分フレームワークを支える技術開発

セクション 2.1 クリアランス検討のための技術システム

区分フレームワークの実装には、上記の人事審査システムの強化、またはクリアランスの検討のための別のデジタルシステムが必要となる。技術システムは、人事審査に必要な要件に加え、いくつかの機能を果たす必要がある。

(a)国の方針で、候補者が自分自身について提供することが要求されている、または認められているすべての情報を収集する。
(1)人事考課に必要な情報以外に、クリアランスの検討に必要な追加情報を考慮する必要がある。
(2)候補者は、審査とクリアランス検討の両方に同時に情報を提供するか、クリアランス検討システムにデータを取り込み、候補者に正確さを確認する必要がある。

(b)素行調査の結果を記録する。
(1)人事考課に必要な情報以外に、クリアランスの検討のために必要な追加情報および報告を考慮しなければならない。
(2)国の政策に従ったクリアランスの検討は、テーマの範囲と時間軸の両方において、より広範な調査を必要とすると思われる。国の方針で認められている場合、複数の調査員が同時にクライアントを調査することができるため、システムは複数の入力を考慮する必要がある。
(3)システムは、研究者が文脈上隔離されて作業すべきか、同じ候補者を研究している他の研究者の調査結果を見ることができるようにすべきかを検討する必要がある。

(c)審査員に候補者のすべての情報を確認する手段を提供すること。
(1)すべての審査とクリアランスの検討情報を裁定者に提供すること。
(2)検討するために要求された区分レベルを特定する。

(d)判定結果の記録
(1)許可された区分レベルや補足情報など、判定に関する情報を取得する。
(2)自動的または人事担当者による候補者通知のトリガー。
(3)潜在的な利益相反など、特別な配慮が必要な場合は、裁決の一部として把握する。

(e)個人が機密施設、ネットワーク、情報にアクセスする際に、そのクリアランス状況を確認するための一元化されたメカニズムを提供すること。
(1)審査とクリアランスの両方を含むすべての判定記録を提供し、権限のある関係者が一元的にアクセスできるようにする。
(2)適切な権限を持つ政府内のセキュリティ担当者が、個人の現在のクリアランスレベルを検証できるようにする。

(f)従業員からの定期的な更新情報を取得するための手段を提供する。

(1)テキスト入力、画像、文書のスキャン、転写など、さまざまな種類の情報を必要とすることを考慮する必要がある。

(2)候補者一人ひとりの個人情報は、安全に保護・保管されなければならない。

(3)情報の入力は、ID および認証のために個人の政府全体のクレデンシャルに関連付けられるべきである。

(4)個人は更新された新しい情報を提供し、以前に提供した情報の正確性を再度確認する必要があるため、人事審査とクリアランスの検討のために個人が以前に提供した情報を考慮する必要がある。

(g)定期的な再調査を把握するための手段を提供する。

(1)国の政策により再調査が必要とされる範囲とテーマを説明する。

(2)要求される様々な種類の情報と報告を考慮しなければならない。

(3)再調査のためのインタビューでは、本人およびその同僚は機密情報を議論する必要があるため、システムは機密情報を保存する手段、または他のシステムに保存されている情報への参照を提供する手段を備えていなければならない。

(h)個人によるセキュリティ関連情報の継続的な自己申告の仕組みを提供する。

(1)国の政策で要求されるように、個人は海外旅行、海外との接触、または軽蔑的な出来事を自己報告できるようにする必要がある。

セクション 2.2 機密情報システム

現代における機密情報の生産と保管は、一つ以上の機密ネットワークの開発も必要となる。日本の機密情報を作成、処理、保管するために作成された情報システムは、以下の基準を満たさなければならない。

(a)機密情報を処理または保存するシステム（データセンタを含む）は、不正アクセスや不注意による開示から機密情報を物理的に保護する能力が評価された施設または部屋である安全作業区域（SWA）内に収容され、使用される。商業機密用ソリューション（CSfC）モバイルアクセス能力パッケージ（MACP）アーキテクチャおよび要件を満たすデバイスは、ミッション要件を考慮したリスクバランスの決定に基づき、ユースケースと個人が書面で許可された場合、SWA 外で機密情報にアクセスするために使用することができる。

(b)非区分された長距離輸送手段を用いて区分された情報を保護するために、商用国家安全保障アルゴリズム・スイートのハードウェアまたは強力なソフトウェア暗号分離を使用する。

(c)機密情報を保護するために、コンピューティングデバイスとローカルエリアネットワークの物理的な分離を使用する。機密とトップシークレットなどの機密レベル間では、デジタルポリシー決定ポイントによって実施される強力な権限制御を使用して、機密情報を保護し、全体的なコストを削減することができる。

(d)機密ネットワーク、特に 802.11 Wi-Fi または 802.15 Li-Fi のための無線ネットワークの使用は、CSfC MACP デバイスのための非区分および信頼されないトランスポートとして無線ネットワークを使用して許可されるべきである。CSfC デバイスは、機密インフラとこれらの特別に構成されたデバイスの間で層状の暗号化を使用し、無線ネットワーク内の悪用から機密情報を保護する。

(e)適切な日本の標準および参照アーキテクチャに従って開発され、ポリシー決定ポイントを介したポリ

シーの実施として属性ベースのアクセス制御の決定を使用して認可を容易にする。
(f)国の政策要件に基づき、セキュリティ評価、認定、リスクマネジメントを受ける。

6. パート 3 : 日本版クレデンシャルフレームワークの草案

セクション 3.1 政府機関共通のクレデンシャル基準

このセクションは、以下を含む日本の PIV クレデンシャル標準を確立する。
(a)PIV は、連邦機関の職員、連邦機関で働く民間企業の職員、政府プロジェクトに従事する民間企業の職員、政府に商品やサービスを供給し連邦施設へのアクセスを必要とする可能性がある民間企業の職員など、信頼される労働力に対して発行される予定である。
(b) PIV クレデンシャルには、識別および認証のために物理的カードに印刷された 6 つの必須項目がある、具体的には以下の項目である。
(1)写真 - 頭頂部から肩までの正面からのポーズで、解像度 300 ドット/インチ（dpi）以上で撮影すること。
(2)氏名 - 大文字で印字されたフルネーム、苗字、名前の順で記載される。
(3)Employee Affiliation - "Employee", "Contractor", "Active Duty", "Foreign National", "Civilian "など、省庁によって定義された個人の所属先。白が政府職員、緑が請負業者、青が外国人を示し、対応する色のバーと対応するブロック文字（色覚異常者用）が追加される。
(4)個人が所属する機関、部署、または組織。
(5)カードの有効期限 - YYYYMMDD 形式で 1 回、MMMYYYY 形式で右上に大きく太字で 2 回印字されている。
(6)汎用一意カード・シリアル番号-背面に印刷された、PIV クレデンシャルの汎用一意シリアル番号。
(c)PIV クレデンシャルには、物理的識別および認証に使用される 7 つの必須データ・フィールドがある。
(1)カード能力コンテナ - カードの製造およびモデルに関する情報、および様々なアプリケーション間の相互運用性を可能にし、カードが進化する際の後方互換性を提供するために使用される関連データモデルを指定する。
(2)カード保持者固有識別子-技術的実装ガイダンスに従って発行される固有のクレデンシャル 番号。接触型（例 : 集積回路チップ）および非接触型（例 : RFID）インターフェース間で共有されるスマー ト・カード有効物理アクセス制御システムに従って発行された固有のクレデンシャル番号。
(3) PIV 認証用 X.509 証明書 - カードおよびカード所有者を認証するために使用される、FIPS 201-2 に定義される X.509 証明書およびその関連秘密鍵。
(4)カード認証用 X.509 証明書 - 物理的なカードを認証し、アクセスコントロールアプリケーションをサポートするために使用される非対称の X.509 証明書とその関連する秘密鍵。
(5)カード保持者の指紋 - 指紋データオブジェクトは、FIPS 201-2 および NIST Special Publication (SP) 800-76 に従って、オフカード照合をサポートするために、カード保持者の一次および二次指紋を指定する。

(6)カード保持者顔画像-警備員による視覚的認証のため、およびオペレーターが立ち会う PIV 発行、再発行、検証データ・リセット・プロセスにおいて、NIST SP 800-76 に規定される顔画像データオブジェクト。

(7)セキュリティ・オブジェクト - チップに格納されたすべてのファイルのハッシュ値、およびこれらのハッ シュのデジタル署名を、機械可読旅行書類パート 2 の第 IV 章付録 3（出典は ICAO）に従って実装し、中央発行者のデジタル署名によってカードの真正性を確認し、クレデンシャル置換を防止するもの。

(d) PIV クレデンシャルには、具体的には、デジタル認証のための 2 つのデータ・フィールドがある。

(1)デジタル署名用 X.509 証明書 - FIPS 201 に定義される、デジタル署名を目的とした X.509 証明書とそれに関連する秘密鍵。電子署名用秘密鍵およびそれに対応する証明書は、集積回路チップのコンタクトインタフェースを介してのみ利用可能である。暗号機能は、電子署名鍵の操作の直前に毎回 PIN を提出し検証しなければならないような「PIN Always」アクセスルールで保護される。

(2)鍵管理のための X.509 証明書 - FIPS 201 で定義された、機密保持を目的とした X.509 証明書とそれに関連する秘密鍵。鍵管理の秘密鍵およびそれに対応する証明書は、集積回路チップのコンタクトインタフェースを介してのみ利用可能である。暗号機能は「PIN」アクセスルールで保護され、一旦 PIN が提出され検証されると、その後の鍵管理操作はそのセッション中に再度 PIN を要求することなく実行できるようになる。

(e)電子署名および鍵管理の証明書は、NIST SP 800-63A に従って証明および登録される必要がある。

(f)中央発行機関は、デジタル認証のための派生 PIV クレデンシャルをプロビジョニングしライフサイクルする能力を提供する。 派生クレデンシャルは、ID 証明プロセスを重複させないように、以前に発行されたクレデン シャルに関連する認証子の所有および制御の証明に基づいて生成される。派生クレデンシャルは、具体的には次の 2 つの方法でサポートされる。

(1)カード・リーダのない政府が管理するスマートフォン、タブレット、ラップトップのセキュリティ・モジュールまたは要素（Trusted Platform Module 2.0、Apple Secure Element、Google Titan Chip など）内の仮想派生クレデンシャル。

(2)派生証明書を含む秘密鍵および X.509 証明書をネイティブにサポートする FIDO2 準拠のハードウェアトークン。これらのトークンが、他の FIDO2 鍵、Open Authentication (OATH) の時間ベースのワンタイムパスワード、他のプライベート 鍵および対応する X.509 証明書（または派生証明書）、および OpenPGP プライベート鍵などの追加クレデンシャルを同時にかつ安全に保持できる場合は許容される。

セクション 3.2 機密アクセスに関する資格認定

このセクションは、以下を含む機密アクセスのための機密アクセス PIV（CAPIV）クレデンシャル標準を確立する。

(a) CAPIV クレデンシャルは、日本の機密情報や施設にアクセスできる個人に発行されるもので、PIV とは別物だが技術的には相関している。

(b) CAPIV は、個人が許可されている範囲において、区分レベルを超えて機密リソースにアクセスするた

めに使用される。
(c)個人の PIV からの身元証明は、CAPIV の生成時に検証され使用される。
(g) CAPIV は、本人確認と認証のために、物理的なカードに 4 つの必須項目が印刷される。
(1)氏名 - 大文字で印字されたフルネーム、苗字、名前の順で記載される。
(2)個人が所属する機関、部署、または組織。
(3)カードの有効期限 - YYYYMMDD 形式で 1 回、MMMYYYY 形式で右上に大きく太字で 2 回印字される。
(4)汎用一意カード・シリアル番号-背面に印刷された、PIV クレデンシャルの汎用一意シリアル番号。
(5)なお、個人の許可されたアクセスレベルは、カードに印刷されてはならない。
(h) CAPIV クレデンシャルには、物理的な識別と認証に使用される 6 つの必須データ・フィールドがある。
(1)カード能力コンテナ - カードの製造およびモデルに関する情報、および様々なアプリケーション間の相互運用性を可能にし、カードが進化する際の後方互換性を提供するために使用される関連データモデルを指定する。
(2)カード保持者固有識別子-技術的実装ガイダンスに従って発行される固有のクレデンシャル 番号。接触型（例：集積回路チップ）および非接触型（例：RFID）インターフェース間で共有されるスマー ト・カード有効物理アクセス制御システムに従って発行された固有のクレデンシャル番号。
(3) PIV 認証用 X.509 証明書 - カードおよびカード所有者を認証するために使用される、FIPS 201-2 に定義される X.509 証明書およびその関連秘密鍵。
(4)カード認証用 X.509 証明書 - 物理的なカードを認証し、アクセス・コントロール・アプリケーションをサポートするために使用される非対称の X.509 証明書とその関連する秘密鍵。
(5) PIV ユニバーサル・ユニーク・カード・シリアル番号-CAPIV は、PIV および PIV アイデンティティ・プルーフィングに直接関連付けられ、それに応じて PIV シリアル番号を格納する。
(6)セキュリティ・オブジェクト - チップに格納されたすべてのファイルのハッシュ値、およびこれらのハッ シュのデジタル署名を、機械可読旅行書類パート 2 の第 IV 章付録 3（出典は ICAO）に従って実装し、中央発行者のデジタル署名によってカードの真正性を確認し、クレデンシャル置換を防止するもの。
(i) CAPIV クレデンシャルには、個人が持つ区分アクセスのレベルごとに、デジタル認証のための 2 つのデータ・フィールドがある、具体的には。
(1)デジタル署名用 X.509 証明書 - FIPS 201 に定義される、デジタル署名を目的とした X.509 証明書とそれに関連する秘密鍵。電子署名用秘密鍵およびそれに対応する証明書は、集積回路チップのコンタクト・インターフェイスを介してのみ利用可能である。暗号機能は、電子署名鍵の操作の直前に毎回 PIN を提出し検証しなければならないような「PIN Always」アクセスルールで保護される。
(2)鍵管理のための X.509 証明書 - FIPS 201 で定義された、機密保持を目的とした X.509 証明書とそれに関連する秘密鍵。鍵管理用秘密鍵およびそれに対応する証明書は、集積回路チップのコンタクト・インターフェースを介してのみ利用可能である。暗号機能は「PIN」アクセスルールで保護され、一旦 PIN が提出され検証されると、その後の鍵管理操作はそのセッション中に再度 PIN を要求することなく実行できるようになる。

(j)中央発行局は、各区分レベルの機密情報を保有するすべてのシステムでアクセス可能なネットワークパスのある認証局および証明書失効リストを提供する。

(k)中央発行局は、機密施設または空間へのアクセスを許可するすべての物理的アクセス制御システムからアクセス可能なネットワークパスのある認証局および証明書取り消しリストを提供する。

(l)中央発行機関は、デジタル認証のための派生 CAPIV クレデンシャルをプロビジョニングしライフサイクルする能力を提供する。派生クレデンシャルは、ID 証明プロセスを重複させないように、以前に発行されたクレデンシャルに関連する認証子の所有および制御の証明に基づいて生成される。派生的クレデンシャルは、具体的には次の 2 つの方法でサポートされる。

(1)カード・リーダのない政府が管理するスマートフォン、タブレット、ラップトップのセキュリティ・モジュールまたは要素（Trusted Platform Module 2.0、Apple Secure Element、Google Titan Chip など）内の仮想派生クレデンシャル。

(2)派生証明書を含む秘密鍵および X.509 証明書をネイティブにサポートする FIDO2 準拠のハー ドウェアトークン。これらのトークンが、他の FIDO2 鍵、Open Authentication (OATH) の時間ベースのワンタイムパスワード、他のプライベート 鍵および対応する X.509 証明書（または派生証明書）、および OpenPGP プライベート鍵などの追加クレデンシャルを同時にかつ安全に保持できる場合は許容される。

セクション 3.3 機密情報システム、機微・機密情報システム

このセクションは、相互運用性、情報共有、再利用、ポータビリティ、サイバーセキュリティを促進するために、日本政府全体で使用する技術標準を開発するための枠組みを確立するものである。標準は、以下の基準に基づいて検討される。

(a)実用性この規格の主な特徴や機能は要求事項を満たしている。

(b)相互運用性。アプリケーションやサービスを接続し、アクセスし、共有するための要件を満たす規格。

(c)技術的な成熟度。規格が確立され、安定しており、市場での支持も確立している。

(d)実装可能であること。規格が連邦政府または民間企業内のアプリケーションで使用されている。

(e)セキュリティ規格は、環境に対して許容できないサイバーセキュリティのリスクを導入しない。

(f)適用性規格が適切であり、潜在的なリスク、コスト、スケジュール、性能、セキュリティへの影響を含むプログラムのニーズに合致していること。

(g)知的財産権規格は一般に公開されており、関連する知的財産の所有者が、その知的財産を非差別的、ロイヤリティフリー、または妥当なロイヤリティベースですべての利害関係者に提供することに同意したことを要求する条項を含んでいる。

(h)一般に公開されていること。規格は一般に公開され、無制限に使用できる。

セクション 3.4 機密情報システムのリスク管理

このセクションは、審査、クリアランスの検討、資格認定をサポートするシステムを含め、機密情報または極秘情報を作成、処理、保管するすべてのシステムのためのリスク管理の枠組みを確立する。

(a)リスクマネジメントの考え方

(1)情報技術リスクマネジメントの主要な目標は、システムが含む情報の保護と、そのシステムが主要な機能を効果的に実行する能力のバランスをとることでなければならない。
(2)リスクマネジメントは、セキュリティへの配慮と設計がシステム開発にしっかりと織り込まれている場合に最も効果的である。
(3)リスクは完全に排除することはできないので、リスクマネジメントプロセスにより、意思決定者はシステム要件と運用上の必要性に照らし合わせて、保護手段の運用コストと経済コストのバランスをとることができなければならない。例えば、非常に高いレベルのセキュリティは、リスクを非常に低いレベルまで下げるかもしれないが、非常に高価であり、許容できないほど重要なオペレーションを阻害する可能性がある。
(4)情報システムに要求されるセキュリティのレベルは、システム内に含まれる情報の機密性を考慮し、情報共有と協力を可能にするシステムの能力と必要性を評価することによって決定されるものとする。
(5)省庁の技術システム間の相互運用性と効率的な連携は、重要な機能を追加するが、リスクも発生させる。個々の要素のセキュリティ評価と認可の決定を企業全体で信頼し、相互に受け入れるための健全な基盤を提供するために、各省は共通の基準を適用し、共通のプロセスに従ってシステムのリスクを管理するものとする。

(b)セキュリティ評価

(1)セキュリティ評価とは、情報技術システムまたは情報技術の特定の項目における管理、運用、技術的なセキュリティ管理について、認可の決定を支援するために必要な包括的な評価である。
(2)セキュリティ評価は、情報システムまたは情報技術項目の運用を許可するかどうかについて、信頼できるリスクベースの決定を行うために必要な、本質的な情報技術システムのセキュリティ分析を提供するものでなければならない。
(3)セキュリティ評価は、認可担当者または委任された認可担当者が認可の決定の基礎とする要因、同等性、および懸念事項のうち情報技術システムセキュリティの部分として機能し、それによってリスクを適切に受容するものとする。

(c)セキュリティ認可

(1)認可決定は、省庁に代わって、特定の環境下で特定のセキュリティレベルの情報技術システムの運用に関連する定義されたリスクレベルを明示的に受け入れる公式の管理決定である。
(2)情報システムを認可することにより、総務省は特定の環境において特定のセキュリティレベルで運用することを承認し、システムの運用に関連するリスクのレベル、および運用、資産、または個人に対する関連する影響を確立する。
(3)情報技術システムの運用に関連する許容可能なリスクのレベルを決定する際、省庁は、上記のリスク管理の概念および本書で付与された権限に従って後に発行される可能性のある基準に従って認可を決定するものとする。
(4)省庁による認可の決定は、システム内の情報の機密性に見合ったリスクが、可能な限り軽減されることを保証するものとする。各省庁は、システムの認可が、運用上の要件を満たすのに十分な協力及び情報共有を可能にすることを確保しなければならない。
(5)各大臣は、省を代表して認可の決定を行う 1 名以上の認可担当者を指名するものとする。大臣は、

大臣に代わって行われる全ての認可及び関連するリスク管理の決定について最終的な責任を保持するものとする。

(d)互恵関係

(1)省庁の認可担当者は、適切なセキュリティ認可の決定文書を他の省庁に提供するものとする。

(2)各省庁の権限ある職員は、情報技術システムまたはその他の情報技術の項目に関する適切なセキュリティ評価文書を他の省庁が利用できるようにしなければならない。

(3)省庁の認可担当者は、他の省庁によるシステムまたは情報技術の他の項目のセキュリティ・アセスメントを、システムまたは情報技術の項目の追加のバリデーションまたは検証テストを要求または要請することなく、受け入れるものとする。

セクション 3.5 民間企業や国際的なパートナーとの連携

(a)連盟は標準化され、民間企業や国際的なパートナーとの機密情報共有が必要な場合に使用されるものとする。

(1)フェデレーションは、接続またはネットワーク化された一連のシステム間で、検証者から依拠当事者への ID および認証情報の伝達を可能にするプロセスである。

(2)依拠当事者とは、通常、トランザクションを処理したり、情報またはシステムへのアクセスを 許可するために、加入者の認証子およびクレデンシャル、または請求者の ID に関する検証者の主張に依拠するエンティティのことである。

(3)フェデレーションアシュアランスとは、フェデレーションが使用するプロトコルが、認証情報や属性情報を依存者に伝達する際の信頼性のことである。

(b)機密情報の共有は、日本政府がフェデレーションを決定し、関係者間の作業関係及び技術的なフェデレーションを確立するためにフェデレーション・オーソリティとして設計したエンティティを通じてフェデレーションされるものとする。フェデレーション・オーソリティは、政府のネットワークやシステムとフェデレーションされる当事者に対し、 NIST SP 800-63C に概説されている少なくともフェデレーション保証レベル 2 のセキュリティおよび完全性基準への準拠を確認するため、 標準化されたレベルの審査を実施する。

(c)機密情報共有は、日本政府によって設計された、フェデレーションを決定し、当事者間の技術的なフェデレーションを確立するための機関である機密フェデレーション機関を通じてフェデレーションされるものとする。機密フェデレーション機関は、フェデレーションされる当事者に対して、NIST SP 800-63C に概説されるフェデレーション保証レベル 3 のセキュリティ及び完全性基準への準拠を確認するために、標準化されたレベルの審査を実施する。

7．パート 4：実施と見直し

セクション 4.1 一般的な責任

法令で指定され、認可されることになる。

(a)集中化された政府全体のクレデンシャル・システムの確立と継続的な運用を監督する実体。

(1)この組織は、この制度に関わるすべての省庁や組織のパフォーマンスと進捗を監視し、進捗状況を立法府に報告する。これらの業務の監視を設立後も継続することは、長期的な成功のために不可欠である。

(b)すべての政府全体の PIV および CAPIV クレデンシャルを発行し取り消す、中央クレデンシャル発行機関 として機能する実体。このエンティティは、以下を行うものとする。

(1)資格情報を認証し、取り消された資格情報をチェックするための分散型高可用性システムを確立する。

(2)十分なアクセス権を持つユーザーが、提供されたクレデンシャルで常に ID を確認できるように、ID をグローバルに検証可能で標準クレデンシャルに結び付けたシステムを構築する。

(3)不変、非エクスポート、ハードウェアベースの証明書と FIDO2 標準に基づく中央ルート認証局から X.509 デジタルクレデンシャルを発行する。

(4)任意の中間認証局の作成を管理し、中間認証局の X.509 証明書に署名を行う。

(5)デジタル認証のための派生的な CAPIV クレデンシャルの提供およびライフサイクル

(6)個人が複数の役割を持つ場合でも、単一のアイデンティティしか持たないようにし、認証された同一人物が、ある時点における現在の機能またはその他の要因に基づいて属性ベースの認可を受けた結果、異なるアクセスを持つことができるようにする。

(c)政府全体のクレデンシャル・システムのポリシー、基準、および手順を監督および維持する主体。このエンティティは、以下を行う。

(1)物理的およびデジタルなクレデンシャル標準と、それらのクレデンシャルを使用する物理的およびデジタルな認証標準を確立する。

(2)情報への物理的または論理的アクセス、および建物や施設へのアクセスの承認に関する方針と基準を確立する。

(d)機密情報および機密情報を処理または保存するネットワークおよび通信機器への物理的または論理的アクセスに関する認可方針および基準を設定し、維持する主体。

(e)公的な機密情報を処理または保管するシステムのリスク評価と管理のための方針と基準を確立し、維持する事業者。

(1)また、政府のネットワークやシステム間のフェデレーション、民間企業や海外パートナーとのフェデレーションのためのポリシーや基準を確立し、維持すること。

(f)民間企業や国際的なパートナーとの機密情報共有が必要な場合に、政府の機密ネットワークやシステムを連携させるためのフェデレーション・オーソリティとして機能する団体。

(g)民間企業や国際的なパートナーとの機密情報共有が必要な場合に、政府の機密ネットワークやシステムを連携させるための機密連携機関として機能するエンティティ。

(h)相互運用性、情報共有、再利用、ポータビリティ、サイバーセキュリティを促進するために、日本政府全体で使用する標準および標準プロファイルの特定、開発、処方を担当する組織である。

(i)デジタルポリシーに基づく認可を可能にする情報技術を開発・運用し、日本政府のシステムおよびネットワーク間で安全なフェデレーションを推進し、民間企業や国際的なパートナーとのフェデレーションが必要な場合には技術的な専門知識を提供する事業体である。

セクション 4.2 説明責任と懲戒処分

(a)日本版 PIV または CAPIV を付与された者は、故意または過失により、適切な懲戒処分を受けるものとする。

(1)物理的なクレデンシャルまたはデジタル証明書を無許可の個人に提供する。

(2)不正な目的でクレデンシャルを使用または乱用すること。

(b)懲戒処分には、譴責、無給の停職、解任、解雇、機密情報へのアクセスの喪失または拒否、あるいは適用される日本の法律および政策に従ったその他の懲戒処分が含まれる場合がある。

(c)大臣又は上級省職員は、少なくとも、本命令の区分基準の適用において無謀な無視又は誤りのパターンを示す個人については、速やかに CAPIV を削除するものとする。

8. パート 5：コスト

この活動には、中央発行機関および関連スタッフの設置、または中央発行機関として指定された既存の機関または省庁のスタッフの増強が必要である。さらに、国家安全保障事務局（NSS）または他の監督機関は、基準の策定と実施の調整のために小規模なスタッフを必要とする場合がある。必要な物理的、デジタル的認可システムおよび機密ネットワークの確立には、これらのシステムを確立、維持、および保護するために、各省に追加的な職員が必要となる。

人材の審査とクリアランスの検討を支援するシステムの導入には、初期のソフトウェア開発費用と、その後の継続的なメンテナンス、ホスティング、セキュリティの費用がかかる。

物理アクセス制御システムのコストは、具体的な導入方法によって大きく異なる。クレデンシャル認証と認可のアクセス制御を施設のエントランスにのみ配置することは、建物全体に多層に配置するよりもコスト効率が良いが、安全性は低くなる。同様に、デジタル認証の導入は、認証ポリシーの複雑さによって異なる。

機密ネットワークには、初期費用と、各区分レベルにおけるユーザーごとの関連費用がかかる。ギャップ・ネットワークの導入にはいくつかの方法があるが、いずれも機密ネットワークの構築には避けられない初期費用がかかる。ベストプラクティスは、SWA に設置された「ゼロクライアント」端末にクライアントセッションを提供する大規模な仮想化環境である。このモデルは、ハードウェア暗号でネットワーク化された 2 つの高可用性データセンターのために約 1500 万ドルの初期費用と、すべてのハードウェア、メンテナンス、IT サポートのライフサイクルコストをカバーするためにユーザーあたり年間 1500 ドルがかかる。SWA を 1 つ追加するごとに、さらに 100 万ドルの初期費用と年間 50 万ドルの費用がかかる。米国と英国では、Commercial Solutions for Classified capability package を利用したセキュアモビリティが一般的になってきており、現在のワークフローへの影響を最小限に抑えるために適切であると思われる。これは、ユーザーに安全なラップトップを提供し、SWA 内で、非 SWA、自宅、または旅行中の信頼できる Wi-Fi 接続で暗号トンネルを介して動作するようになる。このモデルのスタートアップ費用は、ソフトウェア暗号でネットワーク化された高可用性データセンター2 か所に 15,000,000 ドル、そしてすべてのハードウェアのライフサイクルコスト、メンテナンス、IT サポートとして 1 ユーザーあたり年間 3,500 ドルとなる。SWA を追加す

る場合の追加費用は発生しない。また、ほとんどが「ゼロクライアント」端末で、一部にセキュアモビリティラップトップを使用するハイブリッドモデルの導入も可能である。初期費用は 2,500 万ドル近くになり、その後は個別のアプローチと同じユーザーごとの価格設定になる。日本以外の国では、セキュリティ担当者は、電子機器、特にすべての機密 IT からの発散を制御するための追加コストを考慮する必要がある。

9．パート 6：結論

この国家安全保障クレデンシャル・システムの提案は、コンセプトとしては単純だが、適切に実施するためには膨大な努力と資源が必要となる。職員の審査と区分の実施と並んで、これは日本政府にとって重要な取り組みであり、幅広い支持と参加を得るためには、期待、スケジュール、およびリソースについて優れたコミュニケーションが必要である。これらのシステムを導入するために時間と資源を投入することは、日本の国家安全保障情報のセキュリティを大幅に向上させるだけでなく、重要情報、知的財産、技術の保護の基盤を提供することによって、日本経済にも利益をもたらすことになる。時間と資源を投入することで、意図した効果を発揮する安全で信頼性の高いシステムを実現するためには、これらのシステムの開発と実装における厳密さが重要になる。

10.パート 7：参考文献

[1] Computer Security Division, Information Technology Laboratory, "FIPS PUB 201-2:Personal Identity Verification (PIV) of Federal Employees and Contractors," National Institute of Standards and Technology, NIST FIPS 201-2, Aug. 2013. doi: 10.6028/NIST.FIPS.201-2.

[2] D.Cooper et al. , "RFC5280:Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." https://datatracker.ietf.org/doc/html/rfc5280 (accessed Nov 29, 2021).

[3] "FIDO 2.0:Overview." https://fidoalliance.org/specs/fido-v2.0-rd-20170927/fido-overview-v2.0-rd-20170927.html (accessed Nov 30, 2021).

[4] "FIDO2。Moving the World Beyond Passwords using WebAuthn & CTAP," FIDO Alliance. https://fidoalliance.org/fido2/ (accessed Nov. 29, 2021)。

[5] V.C. Hu ら、「NIST SP 800-162:Guide to Attribute Based Access Control (ABAC) Definition and Considerations," National Institute of Standards and Technology, NIST SP 800-162, Jan.2014. doi: 10.6028/NIST.SP.800-162.

[6] G. W. Bush, "Homeland Security Presidential Directive 12," Department of Homeland Security, Aug. 27, 2004. https://www.dhs.gov/homeland-security-presidential-directive-12 (accessed Nov 28, 2021)。

[7] Rigas, Michael J., "Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials," p.15, Dec. 2020.

[8] D. Deasy and J. N. Stewart, "Modernizing the Common Access Card - Streamlining Identity and Improving Operational Interoperability." Dec. 07, 2018. Accessed: Nov. 28, 2021. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Cyber/modernizing_the_cac.pdf

[9] P.A. Grassi, M. E. Garcia, and J. L. Fenton, "NIST SP 800-63r3:Digital identity guidelines," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63-3, Jun.2017. doi: 10.6028/NIST.SP.800-63-3.

[10] D.A. Cooper, H. Ferraiolo, K. L. Mehta, S. Francomacaro, R. Chandramouli, and J. Mohler, "NIST SP 800-73r4: Interfaces for Personal Identity Verification," National Institute of Standards and Technology, NIST SP 800-73-4, May 2015.doi: 10.6028/NIST.SP.800-73-4.NIST SP 800-73r4.

[11] P.Grother, W. Salamon, and R. Chandramouli, "NIST SP 800-76r2: Biometric Specifications for Personal Identity Verification," National Institute of Standards and Technology, NIST Special Publication (SP) 800-76-2, Jul. 2013. doi: 10.6028/NIST.SP.800-76-2.

[12] W.Polk, D. Dodson, W. Burr, H. Ferraiolo, and D. Cooper, "NIST SP 800-78r4: Cryptographic Algorithms and Key Sizes for Personal Identity Verification," National Institute of Standards and Technology, NIST Special Publication (SP) 800-78-4, May 2015.doi: 10.6028/NIST.SP.800-78-4.NIST SP 800-78r4, 2015.5.1.

[13] H. Ferraiolo, R. Chandramouli, N. Ghadiali, J. Mohler, and S. Shorter, "NIST SP 800-79r2: Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)," National Institute of Standards and Technology, NIST Special Publication (SP) 800-79-2, Jul. 2015. doi: 10.6028/NIST.SP.800-79-2.

[14] H. Ferraiolo et al., "NIST SP 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials," National Institute of Standards and Technology, NIST Special Publication (SP) 800-157, Dec. 2014. doi: 10.6028/NIST.SP.800-157.

[15] "Personal Identity Verification Guide Introduction." https://playbooks.idmanagement.gov/piv/ (accessed Nov. 30, 2021).

[16] General Services Administration, "FIPS 201 Approved Products List - PIV Cards." https://www.idmanagement.gov (accessed Nov 28, 2021.)。

[17] Physical Access Interagency Interoperability Working Group, "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems," Dec. 20, 2005. https://www.idmanagement.gov/docs/pacs-tig-scepacs.pdf (accessed Nov. 30, 2021).

[18] International Civil Aviation Organization, "ICAO 9303: Machine Readable Travel Documents, Part 3, Volume 2." Third Edition 2008. Accessed: Dec. 02, 2021. [Online]. Available: https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf

[19] P. Grassi et al., "NIST SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing," National Institute of Standards and Technology, NIST Special Publication (SP) 800-63A, Mar. 2020. doi: 10.6028/NIST.SP.800-63a.

[20] P. Grassi et al., "NIST SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology, NIST Special Publication (SP) 800-63B, Mar. 2020. doi: 10.6028/NIST.SP.800-63b.

[21] P. Grassi et al., "NIST SP 800-63C: Digital Identity Guidelines: Federation and Assertions," National Institute of Standards and Technology, NIST SP 800-63C, Mar. 2020. doi: 10.6028/NIST.SP.800-63c.

[22] R. T. Vought, "M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management," p. 13, May 2019.

[23] N.Keller, "Cybersecurity Framework," NIST, Nov. 12, 2013. https://www.nist.gov/cyberframework (accessed Dec. 15, 2021).

[24] N.Grayson, "Privacy Framework," NIST, Jan. 08, 2020. https://www.nist.gov/privacy-framework/privacy-framework (accessed Dec 15, 2021)。

[25] "rfc1422." https://datatracker.ietf.org/doc/html/rfc1422 (accessed Dec 15, 2021).

[26] "TPM 2.0 Library," Trusted Computing Group. https://trustedcomputinggroup.org/resource/tpm-library-specification/ (accessed Dec. 02, 2021)。

[27] "Secure Enclave," Apple Support. https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web

(accessed Dec. 02, 2021)。

[28] "Why Yubico," Yubico. https://www.yubico.com/why-yubico/ (accessed Dec. 02, 2021).

[29] "U2F and FIDO2 Keys," TOKEN2 MFA Products and Services. https://www.token2.com/shop/category/u2f-and-fido2-keys/1 (accessed Dec 02, 2021)。

[30] "A single sign-on and digital identity solution for government - Government Digital Service." https://gds.blog.gov.uk/2021/07/13/a-single-sign-on-and-digital-identity-solution-for-government/ (accessed Nov. 29, 2021).

第５節 日本向けセキュリティクリアランスの提言

1. エグゼクティブサマリー

日本政府は最近発表した 3 つの文書で、日本の国家安全保障と防衛に関する詳細な戦略を示した。この戦略は、日本の国家、経済、社会の優先事項を重要かつ関連性のある問題として特定し、競合国からの脅威の高まりを認識し、効果的な防衛を開発し、同盟国との関係を改善・拡大する必要性を強調している。この戦略の実行を開始するにあたり、重要な基盤となるのは、防衛や製造の分野において、日本の優位性をもたらす機密情報、プログラム、活動を保護するためのセキュリティシステムの開発である。　本報告で述べたように、機密性の高いデータや製品を効果的に特定し、保護するためのプログラムには、3 つの重要で基礎的な分野があることが判明した。その 3 つの領域とは、1) 人事考課、2) データ区分フレームワーク、3) 技術開発フレームワークである。セキュリティプログラムの重要性から、これら 3 つの活動の開発は並行して行われ、国家安全保障と防衛戦略の実行の中で早期の成果物として開始されるべきである。

人事考課（パーソナル・ベッティング）

政府と契約の従業員に対する信頼と信用の確立と維持は、セキュリティプログラムの最も基本的かつ長年の要件である。このように信頼された従業員は、重要な機密情報の知識を持ち、それらにアクセスすることができる。機密プログラムの侵害のほとんどは、職員または関連会社による故意または無意識の行動が原因で、防衛、国家安全保障、または製造の要素に戦略的、戦術的、または競争上の優位性を与える機密情報または能力が露呈している。信頼と信用を確立し、維持することができなければ、広範な戦略を成功裏に実行することができなくなる。

データ区分フレームワーク

日本が国家、経済、社会の優先事項を保護するためには、これらの優先事項の成功に不可欠な情報と技術を保護する必要がある。このような努力の基礎となる要素は、これらの重要な情報および技術の要素を特定

し、リスク値を割り当てること、つまり本質的にはセキュリティ区分システムであり、これは保護システムに情報を与え、定義するものである。このようなプロトコルの確立は、何かが秘密であるかどうかという大まかなレベルから始まり、特定されたリスクに基づいて保護戦略を強化するためにより微妙なニュアンスへと拡大する必要がある。

技術開発フレームワーク

日本政府が政府全体の信頼される労働力を確立するのに伴い、その審査と、物理的およびデジタルな識別、認証、およびアクセスの承認を提供する標準化されたクレデンシャルをサポートする技術システムを開発する必要が付随している。さらに、データ区分システムの確立に伴い、政府は個人のクリアランス審査をサポートし、適切な区分レベルの機密情報を相応の保護とともに生成、処理、保管するための技術システムを開発する必要がある。

これら 3 つのセキュリティ要素はまだ始まったばかりであることを認識した上で、どのように進めていくかの推奨事項を提供する。この 3 つの活動はすべて早期に、かつ並行して開発を始めるべきであるが、それぞれの中に優先順位をつけることができるステップがある。開発は、協力的で同期化されたプログラムであることを保証するために、単一の組織によって監督されるべきである。

2．人事考課に関する提言

ポリシーと審査機関

適切な法律が立法され、実行可能な資金源が特定されたら、最初のステップは、審査プログラムの実施を開発・監督する政府機関の設立である。この組織は、当初から独自の信頼性を確立することが重要であるため、人事審査プログラムの確立と成長を構築・実行するために割り当てられる人材は、防衛省（MOD）など既存のプログラムのいずれかを通じて審査されることをお勧めする。このコアグループは、その後、より強固な国家プログラムを構築し始めることができる。このプログラムが完全に運用された場合の規模は、何千人もの政府職員、請負業者、関連会社をカバーすることになり、この全範囲を直ちにサポートすることができないであろう。我々は、基礎を築き、適用範囲を拡大するために、段階的なアプローチを推奨する。

参加省庁及び段階的初期アプローチ

最初のステップは、最も大量の機密データを持つ機関及び省庁を特定することであろう。次に、これらの機関内で、この機密データに日常的にアクセスする役職と人員（従業員、請負業者、および関連会社）を特定する。特定できたら、これらの個人について初期調査プロトコルの実施を開始し、機密データへのアクセスに対する適格性を肯定的に判断する。これにより、これらの機関や省庁の中に信頼できる人材のコアグループを確立することができる。

プログラムの拡大

第一段階が順調に進んだら、この最初のグループの省庁は、最終的に機密データにアクセスできるすべて

の職員を対象とした「人事審査プロトコル」の拡大を開始すべきである。同時に、残りの省庁も上記のベッティング・プログラム確立計画に従い始めるべきである。最終的な目標は、機密データにアクセスできるすべての政府職員が徹底的かつ一貫して審査されるようになることである。

トラストの維持

人事考課を通じた最初の信頼確立の推進は、次の要素である継続的審査（Continuous Vetting）の基礎となるもので、各人員について行われた最初の信頼判断が長期にわたって有効であることを保証するプロセスである。この活動の重要な要素は、信頼された人物の行動や活動に関する疑問や懸念に対応し、適切な情報を収集し、懸念を解決または軽減するために適切な手順を踏むことができる機関を省庁内に設置することである。

完全に実施されれば、日本政府は、国民全体に強固で永続的な信頼を確立するための、信頼性が高く再現可能なプロセスを手に入れることができる。その結果、政府内および同盟国との信頼関係を改善できる。

3．データ区分フレームワークに関する提言

基礎的な政策と権限

人事考課と同様、最初に必要なステップは、適切な権限の法的割り当てと実行可能な資金調達の特定である。安全保障区分の枠組みを確立する作業には、政府全体の枠組みの開発を推進し、その後、その枠組みにおける政策の実施と遵守を監督する責任を負う中央組織を指定すること、どの省庁が機密および区分された情報を開発、利用、共有、保護するかを決定し、政策開発プロセスにおけるこれらの省庁の代表的な参加を確認し、次に政府全体の枠組みのための政策を開発すること、が含まれる。

政府全体の中央当局

法制化の最初の検討課題は、政府全体のセキュリティ区分の枠組みを調整し、最終的に実現するための中央当局として、ある組織を選ぶことである。この組織は、国家安全保障、経済安全保障、市民・社会保障の各省庁など、政府のすべての関係部門からの参加を促し、バランスをとることができる首相官邸に置くことを提案する。また、政府内に設置することで、予算面でも政府のパフォーマンス面でも、人事審査とサイバーセキュリティの取り組みを統合することができるようになる。

参加省庁

次に、中央当局は、セキュリティシステムの影響を受ける／参加する省庁を指定する必要がある。各省庁は、首相と中央当局に責任を持つ省庁の高官を指定して、政府のパートナーと協力し、各省庁の高官を動員して実施計画を立てなければならない。そのような高官は、人事審査やサイバーセキュリティの問題に取り組むパートナーと連携し、すべての取り組みが全体的な戦略に対応するようにする必要がある。

政策展開の取り組み

中央官庁と参加省庁が特定されれば、中央官庁はフレームワークを構成する政策プロセスを主導し、日本のニーズを満たすフレームワークの基本要素について意思決定を開始することができる。本報告で述べたデータ区分フレームワークは、フレームワークの多くの構成要素に関するガイドであり、日本の政策開発プロセスに応じて使用または修正することができる。

実施

枠組みができあがると、各省庁による新政策の実施に取り組み、中央当局の焦点は各省庁の実施努力の推進と監督に移る。このような取り組みは、政府全体の取り組みに関する各省のパフォーマンスをレビューする既存のメカニズムに統合されるべきであり、目標が達成され、より広範な安全保障戦略が成功するよう、各省の実施のペースを推進することも含まれるべきである。

4. 技術開発フレームワークに関する提言

適切な権限が立法され、実行可能な資金源が特定されたら、最初のステップは、審査プログラムをサポート し、標準化されたクレデンシャルを発行し、クリアランス検討をサポートし、機密情報を保護する技術を開発 し、その実施を監督する政府機関を設立することである。

人事考課システムと標準化されたクレデンシャルの開発

物理的およびデジタルな識別、認証、アクセスの認可を提供する審査プログラムをサポートする技術の開発と実行を監督するために特定されたエンティティは、迅速に推進する必要がある。このエンティティは、当初から独自の信頼性を確立することが重要であるため、人事考課プログラムへの技術サポートを構築および実行し、標準化されたクレデンシャルを開発するために割り当てられる人員は、MOD などの既存のプログラムの 1 つを通じて審査されることを推奨する。このコアグループは、その後、より強固な国家プログラムの構築を開始することができる。人事考課プログラムをサポートする技術システムは、大規模な審査プロセスを開始する前段階として開発されるべきであり、そのようなシステム開発への早期投資は重要である。このプログラムが完全に運用された場合の規模は、数千人の政府職員、請負業者、および関連会社に信任状を発行することになり、この全範囲を直ちにサポートすることはできないと認識している。最初は基盤を構築し、適用範囲を拡大するための段階的なアプローチを推奨する。

物理的および論理的アクセス制御

クレデンシャルが確立され発行されると、物理的および論理的アクセス制御システムは政府の施設およびシステム全体に展開される必要がある。所定の施設で働く職員は、標準化されたクレデンシャルを与えられると、アクセスのためにそれを使用し始めるべきである（同じ施設内の他の人がまだクレデンシャルを持っていない場合でも）。所定の施設の労働力が完全にクレデンシャル化されたら、施設アクセスにそのクレデンシャルを使用するよう全員に要求することを強制するものとする。

クリアランス審査システムの開発

人事考課を支援する組織の設立後直接、またはそれと並行して、個人のクリアランス審査を支援し、適切な区分レベルの機密情報を相応の保護とともに作成、処理、保管するための技術システムの開発及びその実施を監督する組織は、主要システムの開発に投資するべきである。クリアランス検討システムの開発は、質問事項や情報の重複が多いため、人事調査システムと慎重に調整する必要がある。この開発の一環として、事業体は、ID、認証、およびアクセスの許可のための機密クレデンシャル・システムを開発し、実施すべきである。

機密ネットワークの実装

その後直ちに、責任ある事業体は、機密として識別される情報、およびその情報の生産、処理、保管に関連するリスクに基づき、優先順位をつけて機密ネットワークおよびシステムの開発に投資する必要がある。これらのシステムで働く個人は、前述のクリアランス検討プロセスで評価され、有利なクリアランス判定を受けている必要がある。リソースの制約に基づき、責任主体はこれらのシステムの開発に優先順位をつけるための自治権と、必要な投資を実行するための予算を有するべきである。これらのシステムの開発と実装における厳密さは、時間と資源の投資によって、意図した影響を与える安全で信頼できるシステムを生み出すために、非常に重要である。

5. 実現に向けたロードマップ

セキュリティクリアランス、データ区分フレームワーク、技術開発フレームワークを実現するための、推奨される一連の実施手順を表 4-5-a に示す。

表 4-5-a 実現に向けたロードマップ

節との対応	基本的な方針と権限	承認され配分される資金	中央省庁が策定するフレームワーク	各省庁が連携してプログラムを開発・実行
人事考課のフレームワーク	法案は、身元調査プログラムの開発と実施を監督する政府機関を設立する	機密情報およびセキュリティクリアランス保持者のために、中央当局および省庁に認可され割り当てられた資金	人事評価プログラムの構築と成長を担う人材は、防衛省(MOD)などの既存のプログラムのいずれかを通じて審査されることを推奨する	人事考課の対象を拡大し、最終的には関係省庁の全職員を対象とする
	事業体は、各省庁と協力して、調査、裁定、継続的な審査に関する基準を設定する。		機密データを持つ機関や省庁を特定する	継続的審査（Continuous Vetting）を計画・確立する
			日常的な業務を行う役職や担当者を特定するは、この機密データにアクセスすることができる	
			選ばれた人物を調査し、	

節との対応	基本的な方針と権限	承認され配分される資金	中央省庁が策定するフレームワーク	各省庁が連携してプログラムを開発・実行
			裁定する	
データ区分フレームワーク	情報区分プログラムの策定と実行を監督する政府機関を設立する法案[首相府が推奨]	機密情報およびセキュリティクリアランス保持者のために、中央当局および省庁に認可され割り当てられた資金	どの省庁が機密情報を開発、利用、共有、保護するか指定する	中央当局は、フレームワークを構成するような政策プロセスの主導を開始し、日本のニーズに合ったフレームワークの本質的な要素について意思決定を行う
			政策立案プロセスに参加するよう指定された省庁の上級職員	
技術開発フレームワーク	法案は、審査プログラムを支援し、標準化されたクレデンシャルを発行し、クリアランスの検討を支援し、機密情報を保護するための技術を開発し、その実施を監督する政府機関を設置する	中央省庁が機密情報やセキュリティクリアランス保持者を持つために認可され、割り当てられた資金	技術開発プログラムを開発し、実行を監督する主体を早急に特定する必要がある	クレデンシャルが確立され、発行されるようになったら、物理的およびデジタルアクセス制御システムを政府施設およびシステム全体に展開する必要がある
	政府全体のクレデンシャル基準および技術的なルート証明書（クレデンシャル）権限を確立する事業体		人事審査プログラムの技術サポートを構築・実行し、標準化された資格を開発するために割り当てられた人材は、MODなどの既存のプログラムのいずれかを通じて審査される	所定の施設で働く要員に標準化されたクレデンシャルが提供されたら、アクセスのためにそれを使い始めるべきである（同じ施設内の他の人がまだクレデンシャルを持っていない場合でも）。所定の施設の労働力が完全にクレデンシャル化されたら、施設アクセスにそのクレデンシャルを使用するよう全員に要求することを強制する
			人事審査プログラムを支える技術システムは、審査プロセスを大規模に開始する前段階として開発されるべきである	責任主体は、機密と認定された情報及びその情報の作成、処理、保管に関連するリスクに基づき優先順位をつけて、各省庁の機密ネットワーク及びシステムの開発に投資すべきである
			クリアランスの検討を支援する技術的なシステムは、質問や情報の重複が多いため、人事	機密プログラムおよびシステムに従事する個人は、前述のクリアランス検討プロセスによ

節との対応	基本的な方針と権限	承認され配分される資金	中央省庁が策定するフレームワーク	各省庁が連携してプログラムを開発・実行
			審査システムと慎重に調整する必要がある	って評価され、有利なクリアランス判定を受けている必要がある
			責任ある事業者は、ID、認証、およびアクセスの承認のための区分されたクレデンシャルのシステムを開発し、実装する必要がある	責任主体は、これらのシステムの開発に優先順位をつけるための自律性と、必要な投資を実行するための予算を持つべきである。時間と資源を投資することで、意図した効果を発揮する安全で信頼できるシステムを作り上げるためには、機密システムの開発と実装における厳密さが重要である

第５章 量子関係

最近、量子コンピュータ、量子センサー、量子暗号等々情報科学の分野で量子技術を利用した新たな情報通信システムの実用化に向けた革新的な展開が大きな話題になっている。また、昨年（2022 年）のノーベル物理学賞の受賞は、量子力学の分野で「量子もつれ」と、それを利用した「量子テレポーテーション」の研究者が受賞した。これらの技術は、量子コンピュータや量子通信の実現には欠かせない技術であり、今後の量子技術を利用したシステムの基盤になる。この量子技術は、世の中の一般的な現代科学技術（ニュートン力学やマックスウェルの電磁気学に基づく現在の一般的な科学技術。量子に対して古典技術と呼ばれている）が進化すると、理論の上で成り立っていた量子論が実験により確認、検証することができるようになり、より具体的に実社会への応用が検討できるようになってきた。これは、進化した古典技術を利用しシステムを具現化できるようになってきたからである。

本章では、量子コンピュータ関連および量子コンピュータの解読計算に耐性のある暗号における昨今の公開情報を基に、情報セキュリティおよび安全保障の観点から俯瞰的な視点で、捉え、その対策を考察していく。なお、この章で記述する量子コンピュータとは、特に説明の記載がない限り、超電導量子ビット型の量子コンピュータのことである。

第１節 各国の量子技術の動向とその取り組み

近年、各国の量子技術への研究開発投資は、非常に大きくなってきている。表 5-1 に各国の量子技術に対する政策と研究開発投資予算を纏めて示す。各国ともに、量子技術を先行して有することは、現代の社会活動におけるイニシアティブを確保する上で大きな影響を与えるため積極的に投資を行っている。特に、中国は、先行する米国や他国からの巻き返しのため巨額な研究開発投資を行ってきている。その額は、1 兆円をこえる投資額であり、中国東部にある安徽省・合肥市に大規模な研究拠点を整備している。

日本においても近年ようやく欧州並みの予算額がついてきているが、現在のシステムへの適用や実社会への実装例は、非常に少なく、実用化の面での更なる加速が必要である。そのためには、一般社会への実用化（実装）開発と、純粋な科学技術の発展のための研究との両輪での研究開発投資が必要と考えられる。