ゼロトラストネットワークを実現するための政府職員のアカウントやアセットの管理（ディスカッションペーパー）

2021 年 8 月

待鳥博志[1]、菅原保仁[1]、田丸健三郎[2]

要旨

ネットワークに対する攻撃の高度化や多様化が進む現在、セキュリティ境界に依存しないセキュリティアーキテクチャの構築が必須である。そのために、ネットワーク全体で「ゼロトラストネットワーク」という考え方を取り入れ、多層的な防御により未知の攻撃も含めて対処できる仕組みにしていくことが望まれる。

ゼロトラストネットワークでは、存在するすべての“利用者や機器などの状態”を個別に確認しながら、信頼できるものを判断して動作するため、ネットワーク全体として多層的な防御の仕組みが実現できる。この仕組みの前提として、“利用者や機器などの情報を信用できるものにすること”が必要であり、その機能を実現するのが、政府職員のアカウントやアセットを管理するマスターディレクトリである。

本ディスカッションペーパーでは、新しいガバメントネットワークの構築における「政府職員のアカウントやアセットの管理」を主な論点とし、ゼロトラストネットワークを実現するための仕組みやその運用についての検討を示す。

本ディスカッションペーパーは、政府 CIO 補佐官等の有識者による検討内容を取りまとめたもので、論点整理、意見・市場動向の情報収集を通じて、オープンで活発な議論を喚起し、結果として議論の練度の向上を目的としています。そのため、ディスカッションペーパーの内容や意見は、掲載時期の検討内容であり、執筆者個人に属しており、内閣官房　情報通信技術（IT）総合戦略室、政府の公式見解を示すものではありません。

[1] 内閣官房政府 CIO 補佐官
[2] 内閣官房情報通信技術（IT）総合戦略室 プロジェクトマネージャー

改定履歴

改定年月日	改定箇所	改定内容
2021 年 8 月 31 日		初版

目次

1　はじめに

1.1　背景と目的

「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画」（令和 2 年 7 月 17 日閣議決定）の推進において、省庁内の会議や省庁間の会議をリモートで実施可能な環境の整備と、行政全体のネットワークと情報システムの見直しによる全体最適化が進められている。

この取り組みにおける、行政全体のネットワーク（以下、新しいガバメントネットワークと記載）の整備においては、ネットワークを統合して全体最適化を進めるとともに、近年本格化しているクラウドサービスの利用にあわせた、安全にクラウド環境に接続して利用する仕組み、そして、高度化や多様化が進む様々な脅威への対応も重要である。

1.2　“ディレクトリ”の定義

本ディスカッションペーパー（以下、本書と記載）では、説明において、２種類の“ディレクトリ”という言葉を使用する。

【マスターディレクトリ】

マスターディレクトリは、ゼロトラストネットワークを実現するための、政府職員のアカウントやアセットを格納したディレクトリデータの集合体である。

システムを使用するためのアカウント情報や、役割を与えるためのグループ情報、設定を適用するためのコンピューターの情報など、一般的にアカウント管理と呼ばれるものに加えて、ゼロトラストネットワーク実現のために管理すべき、施設や設備の情報なども含まれる。

本書に示すディレクトリに含まれる情報の例：

- 個人アカウント（政府職員・外部利用者）
- 組織・グループ
- 端末やその他の機器（複合機やネットワーク機器、サーバなど）
- システム・ソフトウェア・アプリケーション
- 会議室・セキュリティゲートなどの設備
- 場所やネットワーク機器、アドレス　等

【認証ディレクトリ】

認証ディレクトリは、マスターディレクトリに格納されたデータの一部を使用して、ユー

ザーにシステムサービスを提供する際に使用する認証や認可の機能を提供するものである。

1.3　マイナンバー等との関係

システムを利用する際に利用する個人のアカウントを考えた場合、個人を識別する ID（マイナンバーなど）との関係を検討することもあるが、本書の検討は「ゼロトラストネットワークを実現するための政府職員の認証・認可について」が主な論点であるため、そのデータに関する定義については対象外とする。

1.4　適用対象

本書はディスカッションペーパーであるため、固有のシステムや環境に制限が発生するものではない。しかし、新しいガバメントネットワーク全体としてのセキュリティの考慮から、本書に記載の内容についての必要性の理解が重要である。そこで、新しいガバメントネットワークに接続し、政府職員のアカウントを使用した認証、認可を使用するシステムすべてにおいて、本書に記載の内容を参考にしていただきたい。

2　政府職員の認証・認可を取り巻く環境の変化と求められる対処

2.1　多様化するサイバー攻撃への対処（環境の変化）

近年、様々なサイバー攻撃が報道等で話題となっており、その攻撃手法も多様化が進んでいる。国内では、金融機関や研究機関を対象とした攻撃だけでなく、行政機関、会員サービスなどを対象とした情報漏洩につながる攻撃、そして、防衛関連情報を対象とした攻撃などが判明している。国外においては、米国の人事管理局への不正アクセスや大規模な個人情報の漏洩につながる攻撃なども発生している。今後、新しいガバメントネットワークの実現においては、定常的に攻撃が行われている状況が続くことを想定し、また、その攻撃はさらに高度に多様化することを認識しておかなければならない。

また、情報システムの利用においては、インターネットを経由したスマートフォンの利用が増え、キャッシュレスサービスの導入も進んでいる。利用環境の変化にあわせて攻撃手法も変化するため、新しいガバメントネットワークの実現においては、環境の変化に追従した対処も必要である。

2.2　急速に進むクラウド技術への対処（環境の変化）

近年、クラウド技術が進み、情報システムの利用の利便性が大幅に向上している。一方で、クラウド利用にあたりセキュリティが心配という声も聞こえてくる。実際のところ、多くの企業や組織が利用するクラウド環境は十分なセキュリティ対策や監視対応などがされていることがほとんどであるため、考慮すべきは、そのクラウド環境を利用する側の「十分な理解と仕組みづくり」、そして、「セキュリティを考慮した運用におけるポリシー定義」と考えられる。

まず、「十分な理解と仕組みづくり」としては、クラウド技術の活用を前向きに捉え、より安全にかつ効果的にクラウドを活用していくための対処に取り組まなければならない。ネットワークの実装においては、クラウド環境を含めた範囲で、どのようなネットワークで接続され、どのようなデータが管理され、どのようなセキュリティ対策が施されて新しいガバメントネットワークと接続されるのか、という点を全体アーキテクチャーとして整理すしなければならない。

つぎに、「セキュリティを考慮した運用におけるポリシー定義」の部分であるが、これは、クラウドを利用するシステムの運用者側の観点である。システム利用者のアカウントやパスワードなどの情報が不備なく管理され運用できていること、そして、システムにアクセスする機器やソフトウェアなどが常に管理され、システムを構成する全てのパーツのどこにもリスクが存在しない状態であること、これらふたつのことを保証する仕組みを構築することが安全にクラウド技術を利用するために必要である。

2.3　ゼロトラストネットワークを実現するために（求められる対処）

先述のとおり、クラウド技術の活用、個人のスマートフォンの利用増加など、情報システムの利便性が向上することに併せて、攻撃手法の高度化や多様化が進んでいる。この状況において、これまで一般的に使用されてきたファイアウォールを使用したネットワーク分離の手法（外部と内部を分ける守り方）だけでは、情報資産を適切に守る事が困難になってきており、ネットワーク全体としてゼロトラストネットワークの考え方を適用し、多層的に防御する仕組みが求められる。

ゼロトラストネットワークは、人、端末、機器、ソフトウェアなどが、それぞれの信頼度を相互に判断しながら全体として機能するネットワークの仕組みであり、利用者の情報や証明情報、デバイスの状態や証明情報、ソフトウェアの状態、アクセス場所や時間など、様々な情報からお互いの信頼度を推定しアクセスを許可するため、万が一、多様な攻撃によりリスクがある対象が存在していたとしても脅威が広がらず適切に排除することができる。

政府職員の認証・認可を考えた場合、ゼロトラストネットワークの実現には、アカウントやコンピューター、その他関係する情報の管理と保証が重要となるが、これらの情報をディレクトリ上で管理運用するためには、業務フローを含めて整理する必要がある。業務フローにおいて、利用者、申請者、承認者を明確にし、管理された統一的なフローにより運用することで、ディレクトリ上で信頼できるデータを扱うことができる。

2.4　分散管理から一元的な管理へ（求められる対処）

現在の政府職員の認証・認可の仕組みは、府省庁においてそれぞれの手法により管理されている。そのため、アカウント管理の方法や運用は統一されておらず、マスターディレクトリや認証ディレクトリは分散された状態である。

これからの新しいガバメントネットワークでは、システムの共通利用や府省庁での連携、クラウド活用といった利便性を確保しつつ、拡大する脅威に対応できるセキュリティを考慮した仕組みが必要である。そのためには、政府職員のアカウントやアセットの管理の仕組みを統一化し、ネットワーク上に存在するアカウントやアセットの情報の信頼性を保証しながら、柔軟にシステムの共通利用や連携ができる環境が必要である。

3　政府職員の認証・認可に必要な構成要素

3.1　政府職員の認証・認可に必要な構成要素

新しいガバメントネットワークにおける政府職員のアカウントやアセットの管理では、大規模かつ複雑な職員と組織に関する情報を、人事異動に併せて制御する必要がある。その際、ゼロトラストネットワークを正常に運用するために、常にネットワーク上に存在するアカウントやアセットの情報の整合性が取れていて、信頼できる状態であることが担保されている必要がある。

政府職員のアカウントやアセットの管理の仕組みに必要な構成要素は、次の通りである。

① 信頼されたマスターデータを管理するマスターディレクトリ
② クラウドとオンプレミスに対応する認証ディレクトリ
③ 常にデータの整合性を保証する同期機能
④ 利用者の利便性を高めるセルフサービス

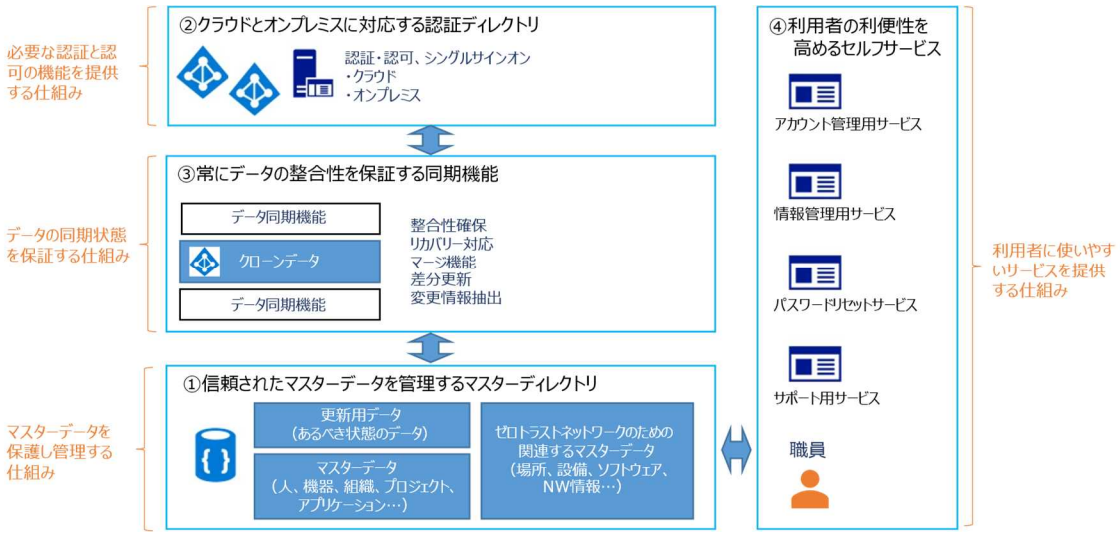

図 1：政府職員の認証・認可に必要な構成要素

3.2　信頼されたマスターデータを管理するマスターディレクトリ

政府職員のアカウントやアセットの管理で使用するデータには、職員の情報や組織の情報、機器（PC やスマートフォン）の情報、アクセス権を与えるためのプロジェクトやグループの情報、そして、アプリケーションの情報などがある。これらの情報は、信頼できる状態で登録管理されている必要があるため、その登録管理の過程にデータを保証するプロセ

スを組み込み、信頼されたマスターデータとしなければならない。

また、上記データに加えて、新しいガバメントネットワークにおけるゼロトラストネットワークを実現するためには、ネットワーク上に存在する設備やソフトウェア、場所（会議室など）、ネットワークのアドレスなどの情報なども、適正に管理された状態で保持しておく必要がある。

【ゼロトラストネットワークのトラストアンカー】

ゼロトラストネットワークは、すべてのネットワーク上に存在する情報が信頼できる状態であるかどうかを確かめながら動作する。その際、マスターディレクトリは、「信頼できる情報＝人やデバイスなどを証明する要素」を新しいガバメントネットワーク全体に対して提供する役割を持つ。そのため、マスターディレクトリは、信頼されたマスターデータとその証明する要素を併せて保管し、信頼の源（トラストアンカー）となる。

【マスターデータの保証】

マスターディレクトリ上のマスターデータを信頼できるデータとして保証するためには、そのデータを登録、変更、管理する業務において、すべてのデータの操作が”保証に値する操作”である必要がある。そのため、データの操作が必要な業務については、業務フローの検討整理が重要である。（政府職員のアカウントやアセット管理に関する業務フローについては後述する。）

【信頼されたマスターデータを管理するマスターディレクトリに求められること】

- すべての情報の識別子が一意であること
- すべての情報の関連性が管理されていること
- すべての情報が追跡管理できること
- すべての格納されたデータが分析可能であること

3.3　クラウドとオンプレミスに対応する認証ディレクトリ

新しいガバメントネットワークでは、コミュニケーション基盤や様々な業務アプリケーションが稼働する。それぞれのサービスは利用者を認証しアクセス権を認可することでサービスを提供する。これらすべてのサービスの認証と認可を、OpenID Connect など標準的な認証プロトコルを実装した単一の認証ディレクトリで実現することができれば、シンプルであり、管理しやすい仕組みにすることができる。この場合、今後構築予定のアプリケーションやシステムは、共通利用する認証ディレクトリが提供する認証・認可の機能をそのまま利用することができ、実装において個別の認証・認可、そして認証・認可に関する管理系の機能の実装は必要ない。

しかし、実際には、クラウドの認証基盤とオンプレミスの認証ディレクトリを完全にひとつとし、かつ、すべての業務アプリケーションの認証・認可をひとつの認証ディレクトリで実装することは、特に多くのアプリケーションを保持していたり、システム移行が順次行われていたりする場合などには、容易ではない。

そこで、将来的にはひとつの仕組みに統合するという目標を立てたうえで、システム移行の過渡期のセキュリティも考慮し、複数の認証・認可に関わる仕組みを統一的に制御しながら最終的な形態に段階的に移行することも考慮すべきである。

本書は、政府職員のアカウントやアセットの管理についてのディスカッションペーパーであるため、管理に関する手法に焦点をあてることとし、認証ディレクトリの選択や実装については言及しないこととする。

また、将来、新しいガバメントネットワークの拡大に伴い、既存の認証・認可に関する仕組みとの連携についても検討する可能性があるが、同期機能の拡張で対応が可能であるため、個別の対応については言及しないこととする。

3.4　常にデータの整合性を保証する同期機能

認証ディレクトリはその仕組み上、様々な種類のデータが書き込まれる。それは、複数の種類、複数のデータが書き込まれることに加えて、その中のひとつのデータだけを見た場合でも、複数のソース（元となる情報）からデータが書き込まれ更新される場合がある。

例えば、アカウントに関するデータを考えてみると、アカウント名や名前は対象の人の情報を管理するシステムから書き込まれ、パスワードは使用する人（利用者）から直接書き込まれる。また、メールアドレスはメールシステムと連携して更新されたり、アカウントの属性情報はアプリケーションに使用されるためアプリケーションと連携して更新されたりする。もちろん、データの更新のルールやポリシーの定義で、極力ひとつのソースから更新されるように制御することは可能であるが、それでも、認証ディレクトリの性質上、複数のソースからデータを更新されると仮定すべきであり、同期機能を実装する場合、常に認証ディレクトリ上のデータが意図するデータに自動的に戻す仕組みを実装しておかなければならない。

また、それ以外にも認証ディレクトリのデータが意図しない状態になる可能性が考えられる。例えば、認証ディレクトリに障害が発生してリストアされたケース、管理者が手動で間違えたデータを上書きしたケース、使用しているアプリケーションの設定中にデータが変更されてしまうケース、認証ディレクトリが攻撃されてデータが改竄されるケースなどである。このような状況においても、常に認証ディレクトリ上のデータを意図するデータに自動的に戻す仕組みを実装しておかなければならない。

【常にデータの整合性を保証する同期機能】

常にデータの整合性を保証する同期機能は、同期先の認証ディレクトリのデータを常に確認し、意図しない状態のデータがあれば見つけ出し、あるべき姿に更新し、その更新結果まで保証する仕組みである。これは、意図する更新が認証ディレクトリに正しく反映されていなかったケースや、本来は更新対象ではないデータが認証ディレクトリ側で更新されていたケースなどが考えられ、それらすべての状態を見つけ出して処理するものである。

一般的には、同期機能が、更新元のデータと更新先のデータを取得し、更新すべきデータを比較し、更新すべきデータを差分更新、そして、更新されたかどうか最終的にチェックする、という仕組みが採用されることが多い。これは、古くから使われるデータ同期の方法であるが、認証ディレクトリのデータ更新に適している方法のひとつである。

3.5　利用者の利便性を高めるセルフサービス

セルフサービスについては、サービスポータルの実装として、５章に記載する。「５章 政府職員のアカウントやアセットの管理のためのサービスポータル」を参照。

4　マスターディレクトリの構成

4.1　マスターディレクトリが管理すべき項目

政府職員のアカウントやアセットの管理では、アカウント情報だけでなく、グループやアセットなどを含めて、すべての管理すべき対象に一意の識別子を使用して管理する必要がある。また、それらの情報は、それぞれのつながりを正しく反映し、情報と情報を紐付けた管理にすることで、データの整合性を確保することができる。これらの情報を扱うマスターディレクトリは次のような項目を管理することになる。

マスターディレクトリの管理対象の例：

- アカウント情報
  - 政府職員のアカウント
  - 外部利用者のアカウント
- グルーピング情報
  - 組織情報
  - グループ情報（システム利用における申請ベースの集合）
- アセットや設備
  - コンピューター
  - スマートフォン
  - 複合機等の機器情報
  - 入館ゲートなどのセキュリティ情報
  - 会議室等のエリア情報
  - ソフトウェア等のライセンス情報
  - メールや Web 会議などのサービス情報
- 特殊権限
  - アカウント情報の管理者の情報
  - 組織等の管理者の情報

4.2　マスターディレクトリのデータ構造

マスターディレクトリのデータを効率的に管理するための構成例のひとつとして、グラフスキーマで管理する方法を示す。この方法では、データを、スキーマ、ノード、エッジの 3 つの要素に定義して管理することで、データとその関係を明確にし、整合性を担保している。

[スキーマ]

人、組織、資産、場所などの管理

[ノード]
　オントロジーそれぞれの性質としてどのようなものがあるかを管理
[エッジ]
　オントロジーに従って他のノードとの関係（リンクまたはマップ）を管理

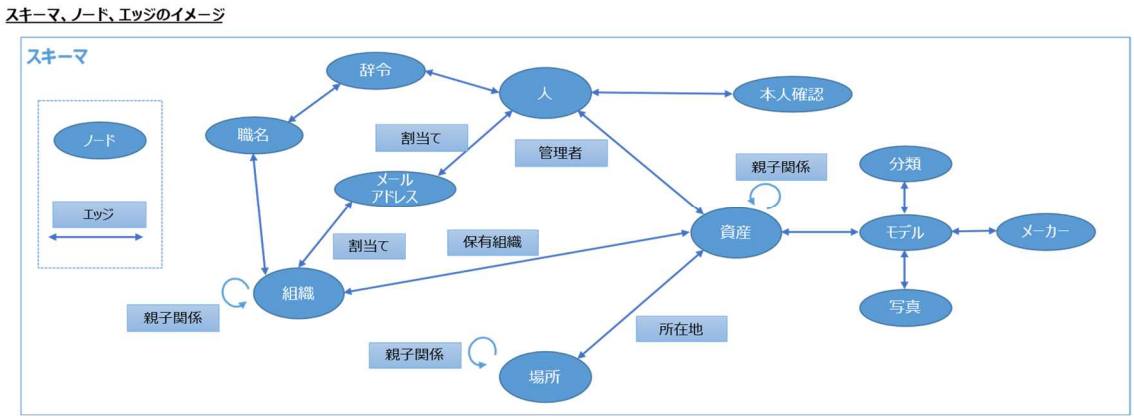

図２：管理するデータの構成例

4.3　BI/レポーティング機能の実装

長期の運用においては、定期的なシステムの変更があったり、データのルールの変更があったりすることもあるため、いつでもそのデータの整合性や状態を簡単にチェックできる仕組みが必要である。また、セキュリティインシデントが発生した場合や、予定していない管理者の変更があった場合などは、様々な情報をキーとしてデータを抽出しアドホックにデータの分析ができる仕組みが必要となる。

そこで、政府職員のアカウントやアセットの管理の仕組みにおいて、データ抽出と分析の機能として、BI（ビジネスインテリジェンス）の機能を活用するべきである。BI の機能により登録されているデータを自由分析したり、必要な定型レポートを作成したりすることができるため、長期の運用におけるデータに起因する問題を解決することができる。

5　政府職員のアカウントやアセットの管理のためのサービスポータル

5.1　サービスポータル

政府職員のアカウントやアセットの管理は、ゼロトラストネットワークを実現するために最も信頼できる仕組みでありながら、利用者に対しては最大限の利便性を提供する仕組みでなければならない。そこで、業務フローと一体化したデータ操作を行う UI と、利用者が自分自身で操作可能なサービス利用のための UI を実装し、信頼性と利便性を両立させる必要がある。

これらの UI は、業務を効率化するためにユーザー自身が操作するセルフサービスを多く取り入れることが重要である。ユーザー自身が多く関与することで、申請などに関わる処理時間を短くすることができるため、結果として利便性を高めることができ、また、対象のシステム規模が大きくなった場合でも効率的である。

なお、セルフサービス UI は、個人が自分自身で実施する操作もあるが、大規模な組織においては、組織の代表者による操作も存在する。システム管理者が行う操作以外の操作をセルフサービスとして位置付け、実装するほとんどの操作をシステム管理者の操作ではなく組織や個人に任せることで、全体としてのシステム利用をスムーズなものとすることが目的である。

5.2　サービスポータルが実現すべき機能

サービスポータルが実現すべき機能として想定されるものは下記の通りである。これは、新しいガバメントネットワークの構成にあわせ、管理面、セキュリティ、利便性などを考慮した議論において執筆時点で検討した内容である。

表 1：サービスポータルが実現すべき機能

分類	機能
アカウント（職員・外部利用者）管理	アカウントの登録管理
	アカウントの情報更新（属性変更・使用の中断）
	アカウントの組織間の異動や併任
	アカウントの削除/廃止
グルーピング情報の管理	組織情報の登録管理
	組織に紐づかないグループの登録管理
アセット・設備管理	業務端末の登録管理
	共用設備の登録管理
	調達外端末に関する登録管理
	個別ソフトウェア利用に関する管理

	会議室情報の登録管理
	機器等の一時的な貸し出し管理の機能
	メール環境、Web 会議・ポータルサイトの登録管理
特殊権限の管理	特権アカウントの登録管理
アカウントモニタリング	使用されていないアカウントを抽出して一覧にする機能
	登録データを様々な形式で集計出力できる BI の機能
パスワード管理	セルフパスワードリセット
サポート	問い合わせ（Q&A）
	FAQ

5.3　サービスポータルの運用に必要なロール（権限）の定義

政府職員のアカウントやアセットの管理を実現するにあたり、その運用において必要なユーザーのロール定義例を示す。

ゼロトラストネットワークの実現においては、アカウントを含むすべてのネットワーク上に存在する情報が信頼できるものでなければならない。そのため、申請者と承認者を分離することが必要である。大規模な組織においては、申請者や承認者を各組織に配置する必要があり、各申請者や承認者を登録管理するロール（権限）も必要となる。

表 2：アカウントやアセットの管理に必要なロールの定義

ユーザーロール	概要	タスク
一般職員	システム利用者・申請者	自身の属性情報の変更 認証設定の変更
外部利用者	職員ではなくセキュリティ上、管理が必要な人	—
利用機関取りまとめ管理承認者	「組織取りまとめ管理承認者」、「組織取りまとめ管理作業者」のアカウント作成、権限付与及び組織構造変更申請の承認ができる。	承認作業（アカウント作成、権限付与、組織構造編集、本人確認）
利用機関取りまとめ管理作業者	「組織取りまとめ管理承認者」、「組織取りまとめ管理作業者」のアカウント作成、権限付与申請、及び組織構造の編集ができる。	申請作業（アカウント作成、権限付与、組織構造編集）
組織取りまとめ管理承認者	管理している組織（部・課・室など）内のアカウント作成、権限付与及び組織構造変更申請の承認ができる。	承認作業（アカウント作成、権限付与、組織構造編集、本人確認）
組織取りまとめ管理作業者	管理している組織（部・課・室など）内のアカウント作成、権限付与及び組織構造の編集ができる。	申請作業（アカウント作成、権限付与、組織構造編集）
ヘルプデスク（サポート担当者）	サポート担当者として SR の受付/管理、エスカレーション、各種作業対応ができる	問い合わせ管理
設備・アセットマスター管理者	「設備・アセットの管理承認者/作業者」のアカウント作成、権限付与申請の承認ができる	承認作業（アカウント作成、権限付与）
設備・アセット管理承認者	「設備・アセットの管理承認者/作業者」権限付与申請及び設備・アセット登録、利用者申請の承認ができる。	承認作業（設備・アセットの登録） 申請作業（設備・アセット管理者の登録）
設備・アセット管理作業者	設備・アセットの登録申請、利用者申請及び、設備情報の編集ができる。	申請作業（設備・アセットの登録）

データ管理者	スキーマの管理者	スキーマ情報の追加・変更
システム管理者	システム管理者	システム情報の変更・管理

5.4　アカウント管理における代表的な機能のシステムフロー

本項では、サービスポータルが実現すべき機能のうち、アカウント管理において代表的な機能のシステムフローを示す。本項に記載のフロー図は、政府職員のアカウント管理を想定している。

5.4.1　アカウントの登録管理

アカウントの初期作成時は初期パスワードを設定し、かつ、無効化した状態で作成する。異動日（利用開始日）以降に、本人確認書類を提出してもらい本人確認をしたのち、対象アカウントを有効化する操作を行い、初期パスワード情報と併せて使用者に通知し利用を開始する。本人確認をすることで、アカウントの使用者を証明することができる。

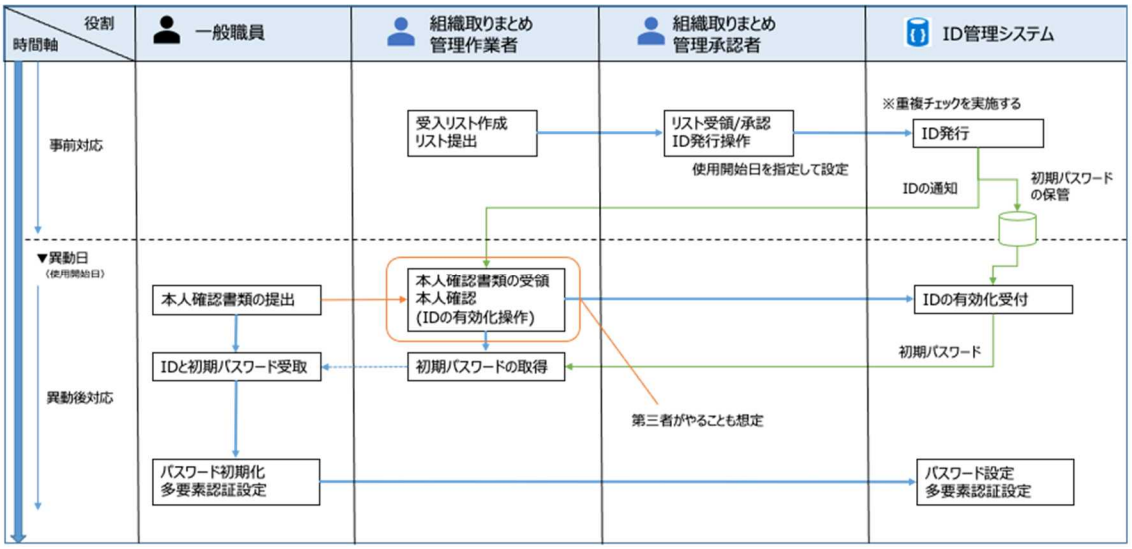

図３：アカウントの登録管理

5.4.2　アカウントの情報更新（属性変更・使用の中断）

属性情報の変更（名前などの変更、権限の変更、状態の変更/使用の中断）は、事前登録しておき、異動日（適用日）に変更を適用する。

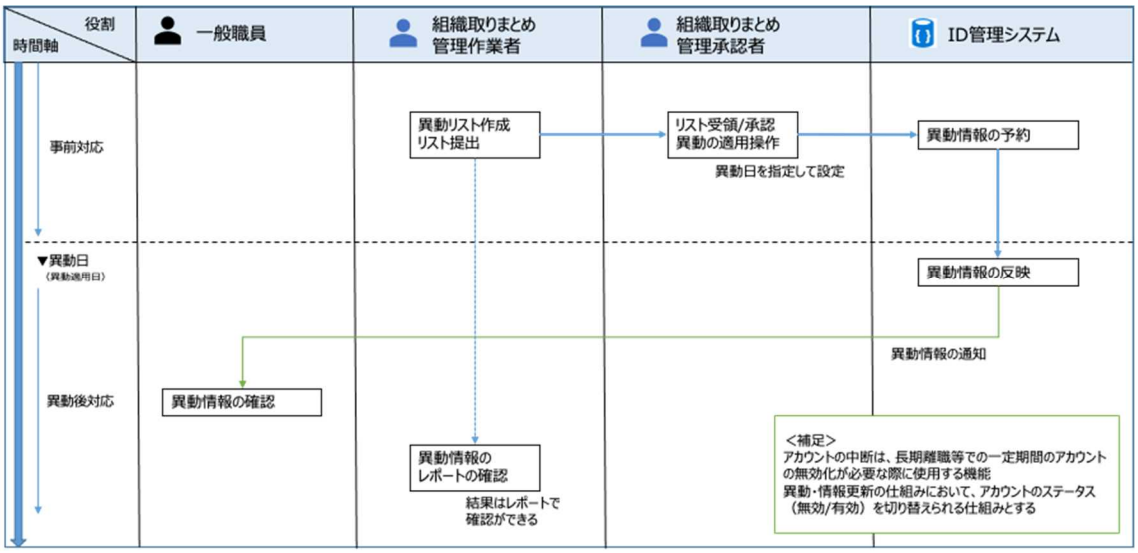

図４：アカウントの情報更新（属性変更・使用の中断）

5.4.3　アカウントの組織間の異動や併任

アカウントの組織間の異動は、一度に２つ以上の組織を異動する多段階の異動や、複数の組織を担当する併任などがある。

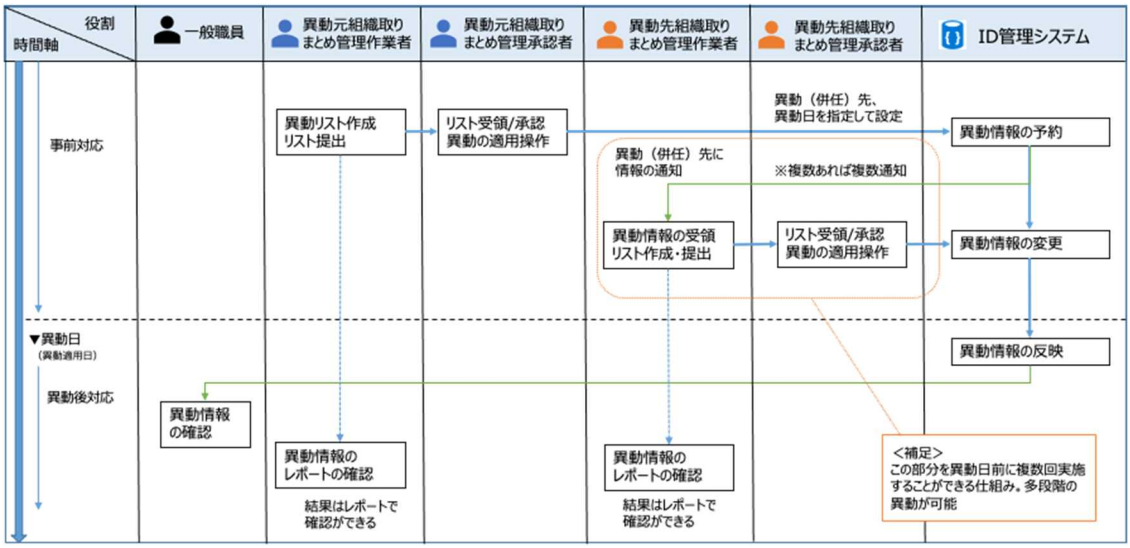

図５：アカウントの組織間の異動や併任

5.4.4　アカウントの削除/廃止

アカウント情報は必ず使用期限を設け、使用されていなかったり、適切に管理されていなかったりするアカウントが残らないようにする。また、アカウントを廃止する際には、使用期限になったら無効化し、一定期間経過後に削除する。

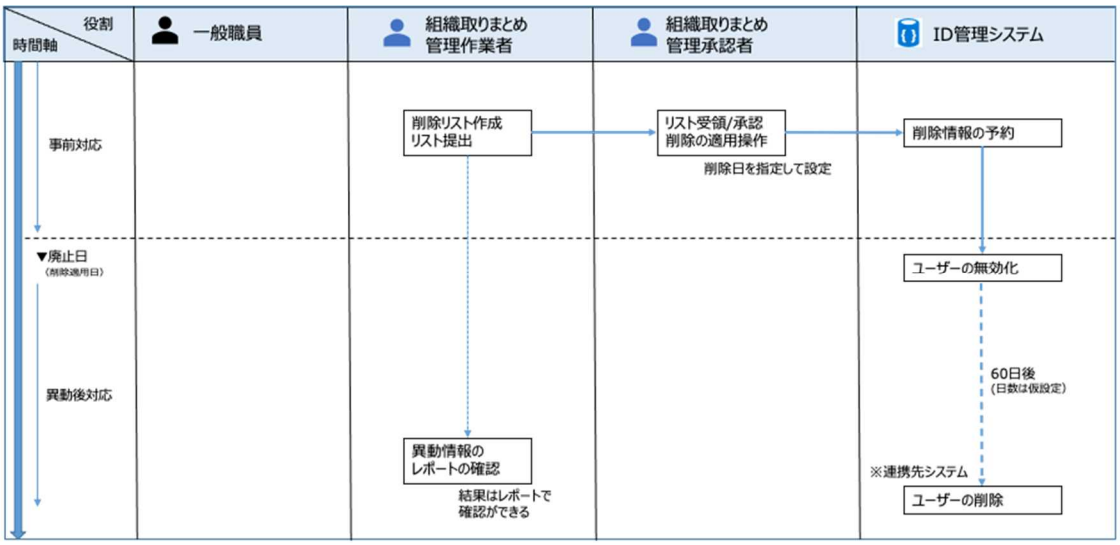

図６：アカウントの削除/廃止

5.4.5　組織情報の登録管理

組織情報の変更が発生した場合、アカウントの操作と同様に、異動日を指定して変更を適用する必要がある。組織はアカウントが所属するグルーピング情報のひとつであるため、アカウントの操作と常に整合性をとりながら動作する仕組みが必要である。

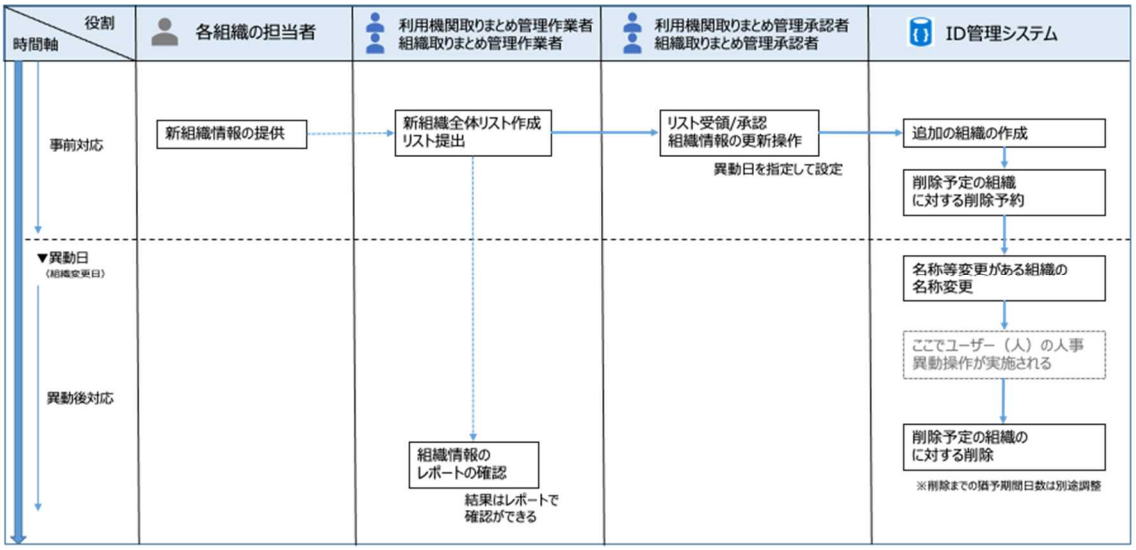

図７：組織情報の登録管理

5.4.6　組織に紐づかないグループの登録管理

アプリケーションの使用などにおいて使用するグループは、必ずしも組織に紐づくものではない場合がある。例えば、あるプロジェクトに参加する人のグループや、ある職種の人

の集まりのグループなどである。このようなグループは、グループの作成から運用までをサービスポータルを通して実施できるようにする。また、手動で作成したグループとなるため、必ず管理者と有効期限を決めて運用することが重要である。

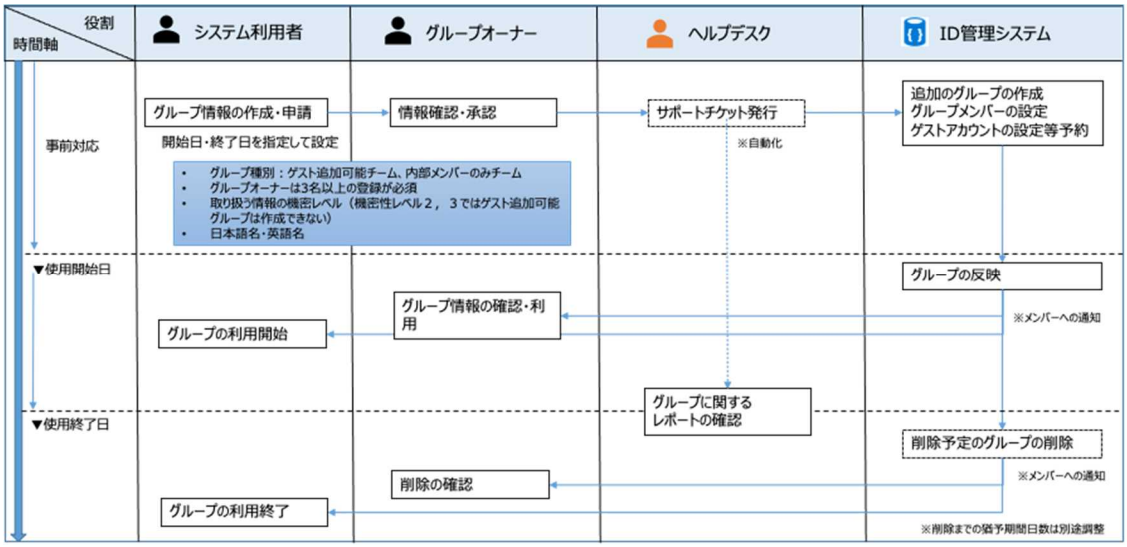

図８：組織に紐づかないグループの登録管理

5.4.7　業務端末の登録管理

業務端末の管理では、実際の端末の準備（手配、キッティング、権限設定）とデータベースでの情報の管理を、ひとつの業務として実施する。

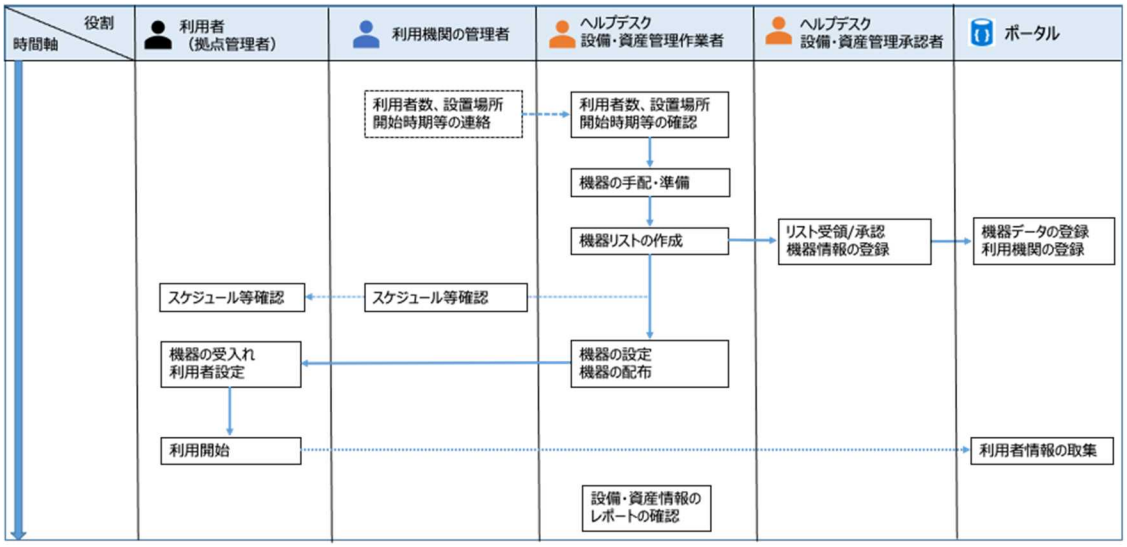

図９：業務端末の登録管理

5.4.8　共用設備の登録管理

共用設備の管理では、業務端末の管理と同様に、設備の準備とデータベースでの情報管理

を、ひとつの業務として実施する。その際、共用設備のデータには、設置場所の情報を入れておき、ネットワーク上で容易に検索と管理ができる仕組みとする。

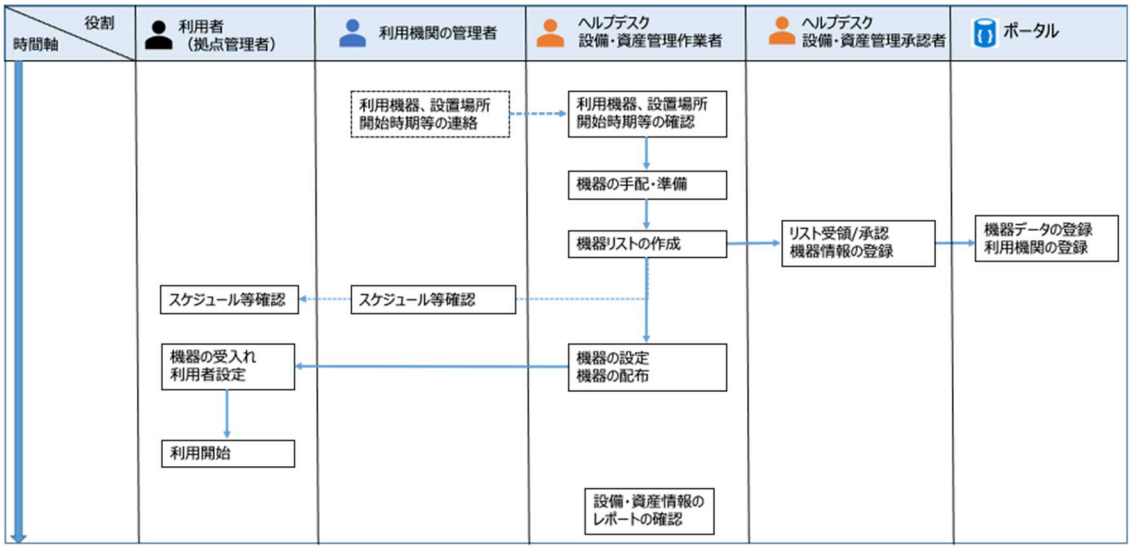

図 10：共用設備の登録管理

6　まとめ

ゼロトラストネットワークの考え方を取り入れた新しいガバメントネットワークにおいては、政府職員のアカウントやアセットの管理が重要である。ゼロトラストネットワークでは、職員個人のアカウントだけでなく、外部利用者のアカウント、組織やプロジェクトのグループ、端末、機器、設備など、ネットワーク上にあるすべての情報に対して、取り扱う際に状態や信頼性を評価しながら動作を進めるため、それらの信頼の元となるマスターディレクトリ、つまり、政府職員のアカウントやアセットの管理の仕組みが重要となる。

また、政府職員のアカウントやアセットに関する情報の管理では、情報の“確からしさ”を運用においても担保する必要がある。例えば、アカウントは職員に紐付けられるが、その職員が本人であることを十分に確認することは重要であり、それは運用で行うこととなる。

信頼できるマスターディレクトリ、信頼できる運用、それがゼロトラストネットワークを実現するために重要な要素であり、本書において特に注目して検討した内容である。今後、政府職員のアカウントやアセットの管理の仕組みを検討するうえでの参考になれば幸いである。

7　参考資料

(1) 政府情報システムにおけるクラウドサービスの利用に係る基本方針
政府 CIO ポータル 標準ガイドライン群
https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

(2) 政府情報システムにおけるゼロトラスト適用に向けた考え方
政府 CIO ポータル ディスカッションペーパー
https://cio.go.jp/dp2020_03

(3) Zero Trust Architecture, NIST SP800-207
https://csrc.nist.gov/publications/detail/sp/800-207/final