

大項目	中項目	小項目	マイナポータル	gBizID	LINE ID	Value Direct	dアカウント	
登録	ID管理	ID数	2033万 (令和2年4月1日時点のマイナンバーカード発行数)	13万	月間アクティブユーザ数8300万※ (※LINE利用ユーザの92％はスマホアプリを利用、またLINEアカウントは複数アカウント持つことができる)	非公開	7000万以上 (回線契約をしてなくてもアカウント作成可能)	
		情報更新	利用不能時のリカバリー方法	複数回連続でパスワードを間違えるとアカウントがロックされ、市区町村窓口に向いてアカウントのロック解除が必要になる。	利用不能時のリカバリー方法：パスワード忘れまたはアカウントロックがされた場合は、アカウントに登録しているメールアドレスに送信されるメールから、パスワードの初期化を行う。	アカウントロック時には、登録している電話番号を使ってSMS認証、FacebookとLINEアカウントを紐づけている場合はFacebookアカウントで復旧可能。	専用窓口でキャッシュカードの情報と電話取引用暗証番号を伝え、再設定を行う。	パスワード忘れて携帯回線未契約時には、IDに登録されているメールに仮パスワードが発行され、そのパスワードを使ってログインを実施、パスワードの再設定を行う。
			紛失時	マイナンバーカード紛失時は、警察署で遺失物届の手続きを行い、市区町村窓口に向いて再発行を行う。	-	-	-	-
			失効・退会	本人の死亡や国外への転出に伴い、住民票から削除された場合は、マイナンバーカードが失効する。	マイページ上より退会可能。	LINEアプリのアカウント削除を実行することで退会が可能。	窓口または郵送にて、必要書類を提示して退会手続きが可能。	回線契約している場合：dアカウントの削除を行っても、電話番号と紐づいて情報が残るため、再度作成することで削除前に戻すことができる。 回線未契約時：一度削除すると、削除前に戻ることができない。
			ID登録・身元確認	公的証明書を用了身元確認なし	-	・gBizID エントリー：誰にでも作成できるアカウントで、審査なしで即日アカウント作成可能。（メールアドレスと、法人の場合は法人番号の確認は行う。）	・ID登録：アカウント作成のために、電話番号登録と確認が必須。（2020年4月までは、facebookアカウントを利用してのアカウント作成を可能としていた。） ・年齢確認：青少年保護の観点から一部LINEの機能を利用できるようにするために、通信キャリアの契約情報を使って年齢確認を実施している。	-
	公的証明書を用了身元確認あり	マイナンバーカードを受け取る際に、官公署発行の写真付き本人確認書類（住民基本台帳カードや運転免許証など）または、市区町村長が適当と認めるもの2点を使って、対面での身元確認を実施。		・gBizID プライム：利用者が法人代表者又は個人事業主本人であることを確認したアカウント。アカウント作成には審査が必要となる。 ・gBizID メンバー：組織の従業員用のアカウント。gBizID プライムによって作成される。	・身元確認（LINE Payのみ）：LINE Payで送金等の機能を使う際には、身元確認(eKYC)が必要。	登録の申請を行うと、インターネットバンキングサービス用のアカウントと銀行口座の作成が行われる。 ・インターネット：運転免許証と健康保険証の2点の画像を使って身元確認を実施。 ・郵送：下記の2種類の1~5の書類から2種類を使って身元確認を実施。 1：運転免許証コピー 2：マイナンバーカードコピー、住基カードコピー、住民票の写し 3：印鑑登録証明書原本 4：公共料金領収書・請求書原本 ・店舗：対面で運転免許書等の本人が確認できる書類を使って、身元確認を実施。	いずれかの方法でdアカウントを作成し、回線契約との紐づけ、または身分証明書のアップロードを行った場合。 ・Web ・スマートフォンアプリ ・店頭	
認証	認証方法	ID/パスワードによる認証	-	・gBizID エントリー：ID/パスワードでの認証	【LINEログイン(外部サイトとの認証連携)】 ・ブラウザ：ID/パスワードによる認証 【LINEアプリへのログイン】 ・デスクトップアプリ：ID/パスワードによる認証	-	・パスワード認証	
		多要素認証	・ICカードリーダーでのログイン： ICカードリーダーにマイナンバーカードをセットし、利用者証明用電子証明書パスワードを入力。 ・2次元バーコードでのログイン： マイナポータルAP（スマートフォンアプリ）でバーコードを読み取り、スマートフォンでマイナンバーカードを読み取り、利用者証明用電子証明書パスワードを入力。 ・スマートフォンでのログイン： スマートフォンでマイナンバーカードを読み取り、利用者証明用電子証明書パスワードを入力。	・gBizID プライム：ID/パスワードに加え、スマートフォンアプリまたはSMSワンタイムパスワード ・gBizID メンバー：ID/パスワードに加え、スマートフォンアプリまたはSMSワンタイムパスワード	【LINEアプリへのログイン】 デスクトップアプリ：初回のみ ID/パスワード+LINEをインストールしているスマートフォン上でPINコード入力	・ログイン時：ID/パスワードに加えて、登録している端末以外からのログインなどリスクが高いと判定された場合は、合言葉による追加の確認。	・パスワード+PIN（メール） ・パスワード+PIN（SMS）	
		その他の認証	-	-	【LINEアプリへのログイン】 ・スマホアプリ：端末認証 ・デスクトップアプリ：QRコード認証	・振込処理時：アプリのワンタイムパスワードまたは乱数表による認証	・FIDO認証 ・回線認証	
		認証連携	ID連携プロトコル	非公開	OpenID Connect（認可コードフロー）	OpenID Connect（認可コードフロー）	-	OpenID Connect（認可コードフロー）
認証連携	連携しているサービス	連携しているサービス	国税電子申告納税システム（e-Tax）、ねんきんネット、MyPost(日本郵便)、e-私書箱（野村総研）、総務省 電波利用 電子申請・届出システムLite	社会保険手続きの電子申請、IT導入補助金2020、農林水産省共通申請サービス等20システム	主にB to Cビジネスを展開している多種多様な業界・サービスと連携している。	-	自社サービス、リーグオンラインストア、gaccoなど	
		認証連携の同意・情報提供の管理等	サービス連携時の同意取得 エンドユーザのマイページから外部サイトに連携した履歴の確認および取り消しの実行	利用規約の同意取得等	サービス連携時の同意取得 マイページより連携しているサービスの解除可能	サービス利用時の同意の取得	自身のデータの提供に関して、どのデータを誰に提供するのが管理できる。 マイページから外部サイトに情報を連携した履歴の確認および取り消しの実行。 パーソナルデータ憲章と、プライバシーポリシーを定め、プライバシーの保護とパーソナルデータを活用する際の利用目的を明示。	
		関連法制度・ガイドライン等	関連法制度	・行政手続における特定の個人を識別するための番号の利用等に関する法律 ・行政手続における特定の個人を識別するための番号の利用等に関する法律施行規則	・情報通信技術を活用した行政の推進等に関する法律 ・各省の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則	犯罪収益移転防止法	犯罪収益移転防止法	携帯電話不正利用防止法 犯罪収益移転防止法
関連法制度・ガイドライン等	関連ガイドライン	NIST SP800-63A	アイデンティティ保証レベルIAL3に相当	・gBizID プライム・メンバー アイデンティティ保証レベルIAL2に相当 ・gBizID エントリー アイデンティティ保証レベルIAL1に相当	・通常のLINEアカウント作成時 アイデンティティ保証レベルIAL1に相当 ・LINE Payで身元確認を実施した場合 アイデンティティ保証レベルIAL2に相当	アイデンティティ保証レベルIAL2に相当	・対面で回線契約をしているアカウント アイデンティティ保証レベルIAL3に相当 ・ネット上で回線契約をしている、または身分証明書のアップロードをして本人確認済みのアカウント アイデンティティ保証レベルIAL2に相当 ・回線契約をしておらず、本人確認もしていないアカウント アイデンティティ保証レベルIAL1に相当	
			NIST SP800-63B	認証保証レベルAAL3に相当	・gBizID プライム・メンバー 認証保証レベルAAL2に相当 ・gBizID エントリー 認証保証レベルAAL1に相当	・LINE PayのFIDO認証：認証保証レベルAAL3に相当 ・デスクトップアプリのLINE初回認証時：認証保証レベルAAL2に相当 ・それ以外：認証保証レベルAAL1に相当	・サービスログイン時 認証保証レベルAAL1 ・重要取引時 認証保証レベルAAL2	・FIDO認証でログイン 認証保証レベルAAL3に相当 ・回線認証、ID/パスワード+スマホアプリ操作 認証保証レベルAAL2に相当 ・ID/パスワード、ID/パスワード+メール 認証保証レベルAAL1に相当
		NIST SP800-63C	非公開	認証連携における保証レベルFAL1	認証連携保証レベルFAL2に相当	-	非公開	
		その他	行政手続におけるオンラインによる本人確認の手法に関するガイドライン	行政手続におけるオンラインによる本人確認の手法に関するガイドライン	-	-	-	
		セキュリティ向上のための施策	ログイン履歴	利用履歴より確認可能	ログイン履歴等を取得	なし	マイページから確認することができる。	利用履歴より確認可能
その他		ログインアラート	ログインするたびに指定したメールアドレスへの通知が可能。	一度もログインしたことがない端末からログインがあった場合、SMSまたはメールで通知する。	デスクトップアプリとブラウザ上でログインした際には、アプリ上で通知される。	なし	普段利用しない環境からログインがあった場合にはログイン通知メールが送付される。	
		ログインセッション	なし	なし	デスクトップアプリとブラウザからのログインセッションの取り消しができる。	なし	なし	
		その他	重要な手続きをする際に、認証の際に使われる利用者証明書電子証明書ではなく、署名用電子証明書を用いて、送信内容が改ざんされないようにする。	-	-	-	パスワードレス認証設定をすることで、フィッシング詐欺やリスト型アカウントハッキング等を防ぐことができる。	