FUJITSU

Fujitsu
Computing as a Service Data e-TRUST

機能説明書

DATA-E-TRUST
2024年4月

まえがき

本書の目的

本書は、Fujitsu Computing as a Service Data e-TRUST(以下Data e-TRUST)の機能を説明しています。
Data e-TRUSTに関わるすべての方は、はじめに本書をお読みください。

本書の読者

本書は、本サービスに関わるすべての方を対象に書かれています。
1章に本サービスの概要、2～6章に主な機能と本サービスを利用する上で理解する必要がある情報を記載しています。
特に2～6章については、本サービスを利用したアプリケーションおよびサービスを企画または開発される方を対象としています。2～6章を読むにあたっては、以下の知識が必要です。

- インターネットに関する基本的な知識
- Web APIに関する基本的な知識
- データベース(以下DB)に関する基本的な知識

また、本書に記載のない各機能・APIの詳細については、APIリファレンスマニュアルおよびAPIリファレンスマニュアル:別冊をご確認ください。

本書の画像が粗く、読みづらい場合は、PDFリーダーの設定のうち、画像レンダリングに関係する設定を見直してください。

マニュアル体系

目的・用途にあわせて、以下の関連マニュアルもお読みください。

マニュアル名称	目的・用途
機能説明書(本書)	本サービスの概要と主な機能、本サービスを利用する上で理解する必要がある情報を記載した資料です。
APIリファレンスマニュアル	Web APIを利用する際の詳細リファレンスを記載した資料です。 HTML形式で記述されています。
APIリファレンスマニュアル:別冊	APIリファレンスマニュアルを補完する資料です。 APIリファレンスと併せてご確認ください。
メッセージ集	Web APIを利用する際のメッセージ内容および対処方法を記載した資料です。
注意事項・制限事項	Data e-TRUSTを利用する上での注意事項、および制限事項を記載した資料です。
リリース情報	Data e-TRUSTのリリース情報について記載した資料です。

本書の構成

本書は、以下の構成になっています。

章／付録	内容
第1章 Data e-TRUSTの概要	Data e-TRUSTの概要を説明します。
第2章 Data e-TRUSTの構成要素	Data e-TRUSTを利用したシステムを構築する上で必要となる知識について説明します。 Data e-TRUSTを利用したシステムを設計開発する際にご確認ください。
第3章 Data e-TRUSTを利用するための前提知識	Data e-TRUSTを利用する上で必要となる知識を説明します。 Data e-TRUSTを利用したアプリケーション開発をする際にご確認ください。

章／付録	内容
第4章 Data e-TRUSTのデータ流通	Data e-TRUSTの分散データ連携機能や同意管理機能を利用したデータの管理について説明します。データ流通を利用する際にご確認ください。
第5章 Data e-TRUSTの証跡・監査機能	Data e-TRUSTの証跡・監査機能について説明します。 証跡・監査機能を利用する場合にご確認ください
第6章 Data e-TRUSTのトラストシール機能	Data e-TRUSTのトラストシール機能について説明します。 トラストシール機能を利用する場合にご確認ください。
付録A 証跡・監査機能のJSONフォーマット	証跡・監査機能を利用する上で必要となるJSONフォーマットについて説明します。
付録B サービスの提供タイプ一覧	Data e-TRUSTが提供するサービスを一覧で記載します。

オープンソースソフトウェアまたは第三者が提供するソフトウェアの利用条件

本サービスで利用しているオープンソースソフトウェアまたは第三者が提供するソフトウェアに関する利用条件等については、ライセンス情報を参照してください。

高度な安全性が要求される用途への使用について

本製品は、一般事務用、パーソナル用、家庭用、通常の産業等の一般的用途を想定して開発・設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう開発・設計・製造されたものではありません。

お客様は本製品を必要な安全性を確保する措置を施すことなくハイセイフティ用途に使用しないでください。また、お客様がハイセイフティ用途に本製品を使用したことにより発生する、お客様または第三者からのいかなる請求または損害賠償に対しても富士通株式会社およびその関連会社は一切責任を負いかねます。

輸出管理規制

本ドキュメントを輸出または第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、必要な手続をおとりください。

変更履歴

版数	日付	変更箇所	概要
第3版 (v1.1対応)	2024/4/19	まえがき	「登録商標について」を追加。
		1.3	図版を削除
		第2章	新規作成。 Data e-TRUSTの全体構成イメージと、IdPについての考え方を記載。
		第3章	エージェントとロールついて、全面的に記述を見直し。 v1.1で追加となった個人エージェントの考え方を追加。
		4.3.4	「参照：クライアント通知について」を更新。 v1.1で追加されたクライアント通知取得APIについて記載。
		付録B	サービスの提供タイプをv1.1に対応
第2版 （v1.0.2対応）	2023/7/10	まえがき	「高度な安全性が要求される用途への使用について」を追加。
		3.3.6	説明文のAPI名記載誤りを修正
初版	2023/3/24		初版公開

登録商標について

Microsoft、Windows、Azure、Azure Active Directory B2Cは、米国 Microsoft Corporation またはその関連会社の、米国およびその他の国における登録商標または商標です。

Amazon Web Services、Amazon Cognitoは、米国Amazon.com, Inc.またはその関連会社の米国およびその他の国における登録商標または商標です。

そのほか、本書に記載されている会社名および製品名は、それぞれ各社の商標または登録商標です。

なお、本書に記載されている会社名、システム名、製品名等には必ずしも商標表示 (TM・(R)) を付記しておりません。

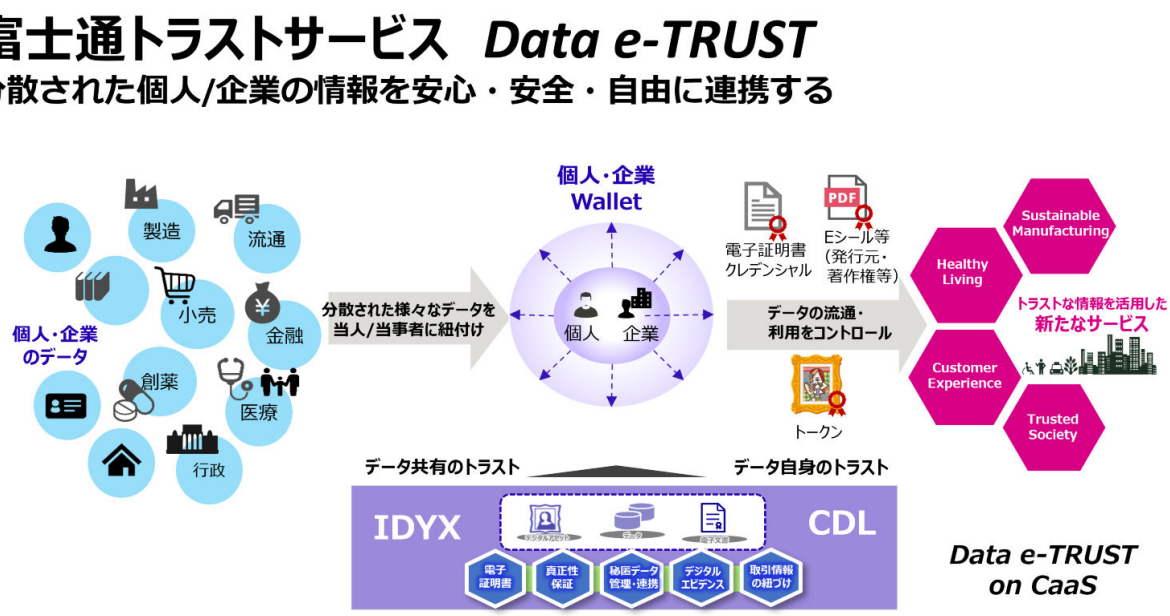
著作権表示

目　次

第1章 Data e-TRUSTの概要

1.1 Data e-TRUSTとは

富士通トラストサービスData e-TRUSTでは、異なるサービス間、個人・企業間での安心安全なデータ流通と活用を実現するためのAPI群を提供します。
Data e-TRUSTを利用することで、当社独自のIDentitY eXchange(IDYX)技術、Chain Data Lineage(CDL)技術により、流通するデータの発行元や所有権、真正性の証明と併せて、データ取引の証跡を改ざん不可能な形で管理できます。
電子文書やデジタルコンテンツなどのデータに関わる、あらゆるオンライン取引に信頼性「トラスト」を付与することで、お客様の業務課題や社会課題などの解決を支援し、サステナブルな社会の実現に貢献します。

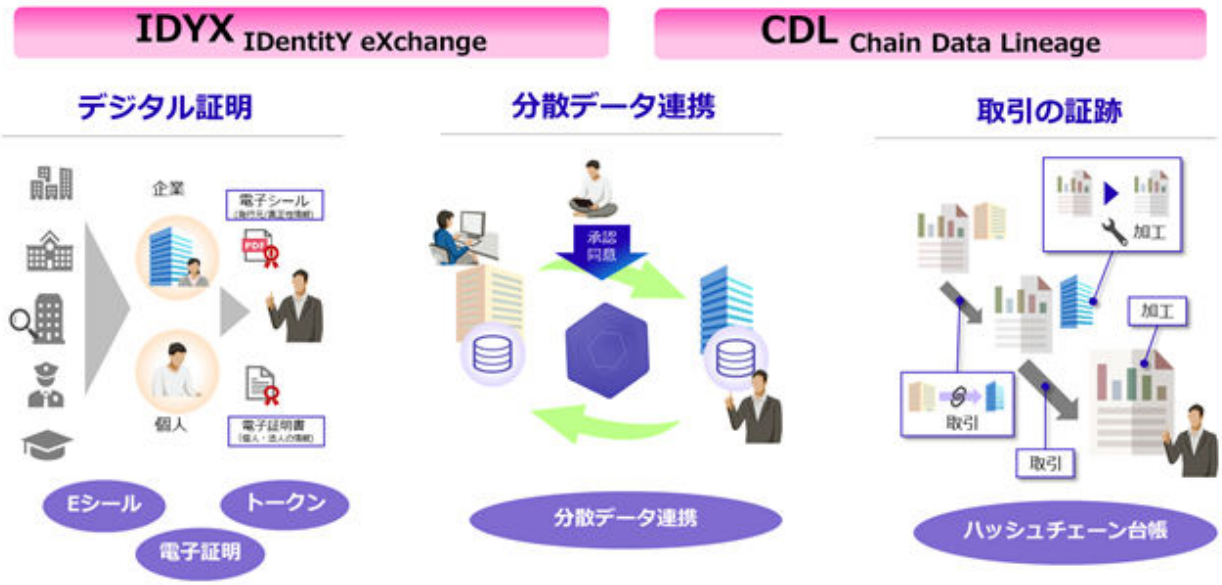


【IDYX技術とは】

IDentitY eXchange(IDYX) 技術とは、活用するデータが正しい情報であり、かつ改ざんされていないことを保証することのできる当社技術です。
IDYXにより、デジタル情報に対する様々な電子証明書の発行と活用を可能にし、デジタル取引でやり取りされる情報の真正性を担保します。

【CDL技術とは】

Chain Data Lineage(CDL)技術とは、ハッシュチェーン台帳技術により個人や企業間の取引や活動履歴を一元管理可能な当社技術です。
CDLにより改ざん不能な形で取引履歴を保管すると共に、取引中に個人/企業間で発生した一連の活動を紐づけて管理できます。



1.2 Data e-TRUSTの特長

Data e-TRUSTには、デジタル取引における個人や企業に関わるあらゆる情報の認証と、安心安全で自由なデータ流通の両立を実現するための3つの特長があります。

- セキュアーな分散型データの連携
- データの真正性を担保
- 改ざん不可能なエビデンス管理

【セキュアーな分散データの連携】

個人/組織によるデータ提供の同意やきめ細やかなアクセス制御により、データ提供時のデータオーナーシップや情報開示管理機能を提供し、ヒト、組織、企業にまたがるデータ連携を可能にします。

【データの真正性を担保】

ヒト、組織、企業を認証するための様々なデジタル証明書を提供し、いろいろなサービスの認証シーンで活用できます。

【改ざん不可能なエビデンス管理】

ヒト、組織、企業でやり取りされる取引や活動の証跡を紐づけて管理し、バリューチェーンやカスタマージャーニーの高度な可視化を支援します。

1.3 Data e-TRUSTのコア機能

Data e-TRUSTには3つのコア機能があります。3つのコア機能により、エコシステムの場、業務プロセス改革、新ビジネスの創出を後押しすることで、金融、製造、流通、医療など、様々な業態の課題解決や業種を超えたDXを強力に推進します。

3つのコア機能

- トラストなデータ流通と活用の場(Trusted Data Hub)
- デジタル証明(Digital Proof)
- デジタル証跡(Digital Footprint)

【トラストなデータ流通と活用の場(Trusted Data Hub)】

個人や企業ごとに秘匿化された分散データベース間で、連携したいデータ項目をきめ細かく制御し、ユーザー本人による同意を取得した上でデータを送信します。
これにより、個人や企業をまたがるセキュアーでオンデマンドなデータ連携を実現します。
Data e-TRUSTはデータの流通先やプライバシーをきめ細かく制御することで、データオーナーシップや情報開示のガバナンスを強化します。それにより、個人や企業が自らの多様なデータを自己管理のもとで、安全に複数の企業・サービスへ提供できます。

【デジタル証明(Digital Proof)】

活用するデータが正しい情報であり、かつ改ざんされていないことを保証するIDYX技術により、デジタル情報に対する様々な電子証明書の発行と活用を可能にし、デジタル取引でやり取りされる情報の真正性を担保します。
IDYX技術により、個人のスキルや経歴企業の実績などのチェックによる認証プロセスの強化や法人認証、顧客情報の相互連携による契約手続などのワンストップ化、デジタルドキュメントやコンテンツの著作権や所有権の管理といった、デジタル上での情報の真正性を担保したい様々な認証のシーンに対応します。

【デジタル証跡(Digital Footprint)】

ブロックチェーンを拡張し、個人や企業をまたがった一連の取引履歴を柔軟かつスケーラブルに一元管理可能にするCDL技術により、デジタル取引や活動の証跡を個人や企業のやり取りと紐づけ、改ざん不能な形で管理します。
CDL技術により、様々な取引履歴を、各事業活動の健全性や社会貢献のエビデンスとして活用可能になります。
例えば、CO2排出量に関わるカーボンフットプリントや消費者行動データの連携など、サプライチェーンやバリューチェーンを高度に可視化し管理できます。

1.4 Data e-TRUSTで提供する機能とは

Data e-TRUSTは5つの機能を提供することで、安心安全なデータ流通と活用を実現します。
各機能の詳細は、APIリファレンスマニュアルおよびAPIリファレンスマニュアル:別冊を参照ください。

【Data e-TRUSTで利用できる機能】

- 分散データ連携機能

  エージェント間で登録されたデータを送信・同期できます。
  分散データ連携機能を利用する際の主な流れを4章に記載しています。

- 同意管理機能

  エージェント間でのデータ送信・同期時に、データオーナーによる同意処理ができます。
  同意管理機能を利用する際の主な流れを4章に記載しています。

- 証跡・監査機能

  エージェント間でのデータ取引を記録し検証できます。
  証跡・監査機能を利用する際の主な流れを5章に記載しています。

- トラストシール機能

  データ発行者やデータ本体が改ざんされていないことを検証します。
  トラストシール機能を利用する際の主な流れを6章に記載しています。

- 管理機能

  Data e-TRUSTの各機能を利用する上で必要となる機能を提供します。
  認証・認可機能については概要を2章に記載しています。
  その他の機能については、APIリファレンスマニュアルおよびAPIリファレンスマニュアル:別冊を参照ください。

第2章 Data e-TRUSTの構成要素

Data e-TRUSTを利用したシステムを構築するにあたり、お客様の開発するサービスアプリを含めた全体の構成イメージと、認証・認可について説明します。

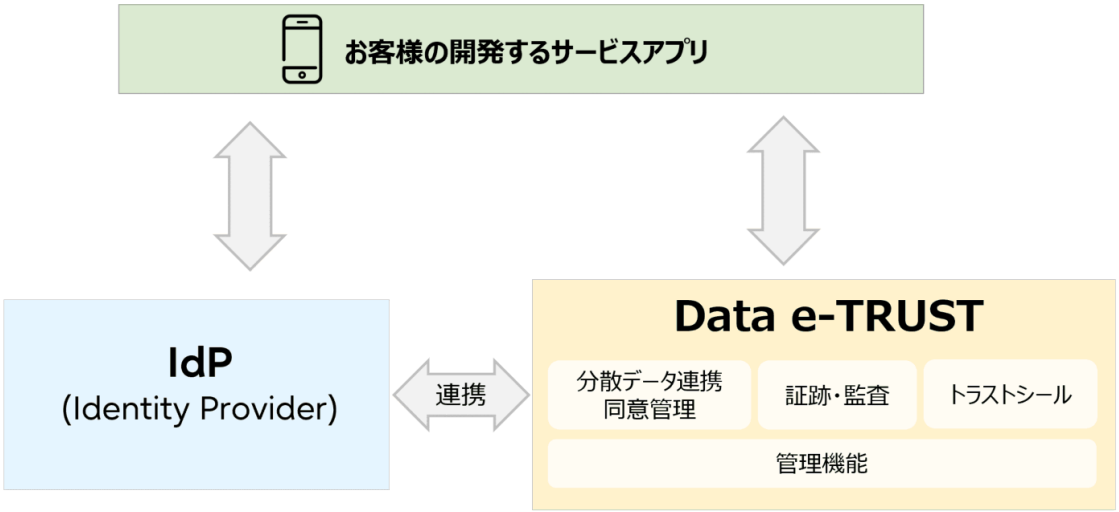
2.1 Data e-TRUSTの構成イメージ

Data e-TRUSTは、トラストサービスをMicrosoft Azure(以下、Azure)環境上で提供します。

お客様の開発するサービスアプリからData e-TRUST APIを実行する際には、Identity Provider(以下、IdP)を利用した認証・認可を行います。

Data e-TRUSTの構成イメージを次に示します。

図2.1 Data e-TRUSTの構成イメージ



参考

IdPとは、ユーザの認証情報を保存・管理するサービスのことです。
Azure Active Directory B2C(以下、Azure AD B2C)、Amazon Cognito、Keycloakなど様々なサービスがあります。

利用可能なIdPについて

Data e-TRUSTは標準機能として、Azure AD B2CをData e-TRUSTと同一のAzure環境上に保有しています。このIdPのことを以後、内部IdPと表現します。

お客様の用意したIdPをData e-TRUSTと連携させることができます。この時お客様が用意するIdPのことを以後、外部IdPと表現します。

利用可能な外部IdP

- Azure AD B2C
- Amazon Cognito
- Keycloak

内部IdPおよび外部IdPを利用した場合の構成例を次に示します。

図2.2 内部IdPを利用する場合の構成例

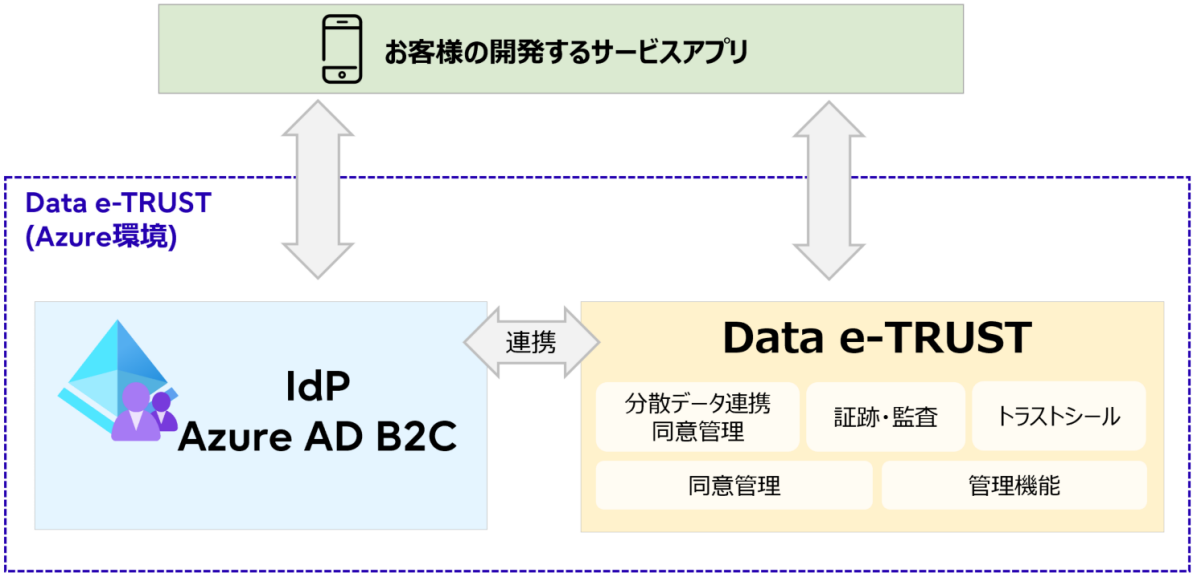
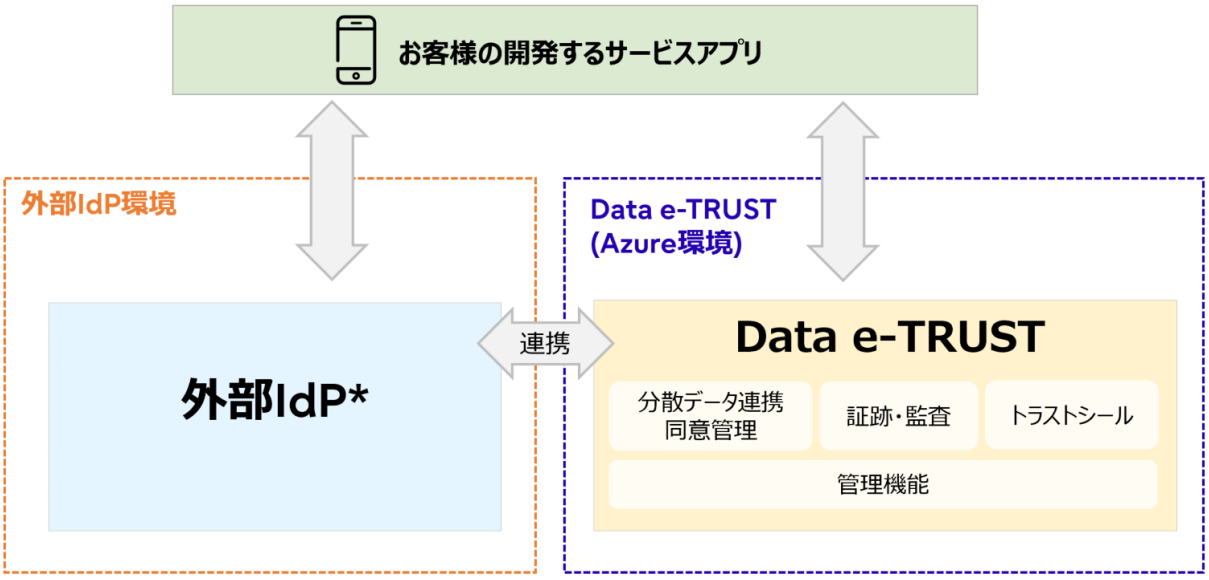


図2.3 外部IdPを利用する場合の構成例



*Azure AD B2C、 Amazon Cognito、 Keycloakを利用可能。

2.2 Data e-TRUSTの認証・認可について

Data e-TRUSTにおける認証・認可についての考え方と、IdP連携のパターンについて説明します。

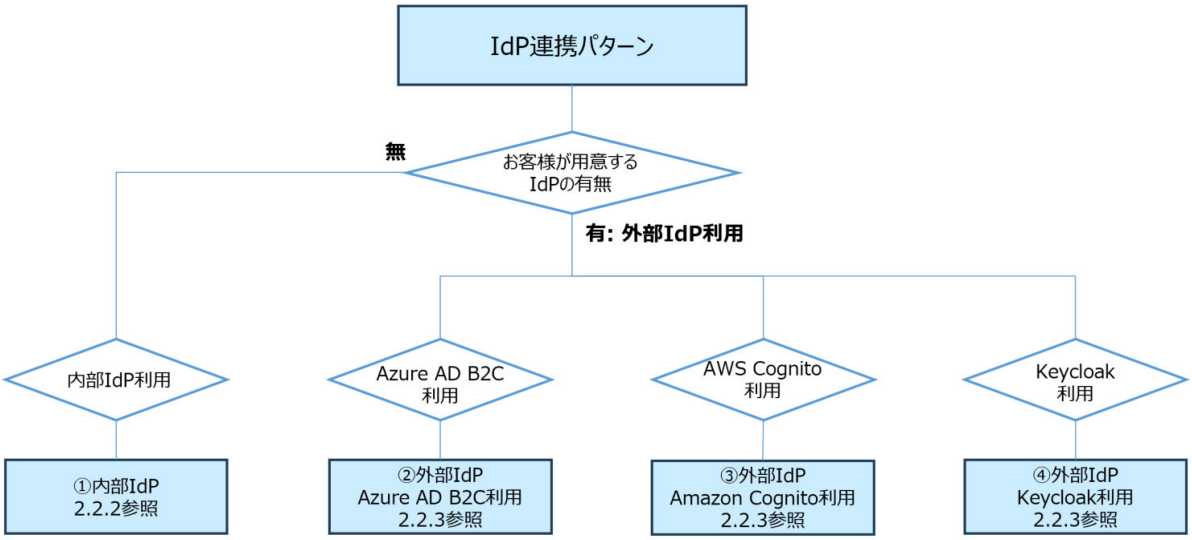
各手順の詳細については、環境構築後に提供する以下の資料を参照ください。

- Data e-TRUST 設定完了通知書
- ユーザーマニュアル01_Data e-TRUST 各種設定変更申請手順
- ユーザーマニュアル02_Data e-TRUST ユーザー登録手順
- ユーザーマニュアル03_Data e-TRUST API利用手順

2.2.1 Data e-TRUSTにおけるIdP連携のパターン

Data e-TRUSTでは、IdP連携、および3章で紹介するData e-TRUSTの持つロール設定によって認証・認可を行います。

IdP連携として、以下の図に示す4パターンを提供します。
各パターンで認証・認可をする際に必要な手続の概要を、2.2.2～2.2.3に記載します。



2.2.2 内部IdPを利用する場合

内部IdP利用時の認証・認可の流れ

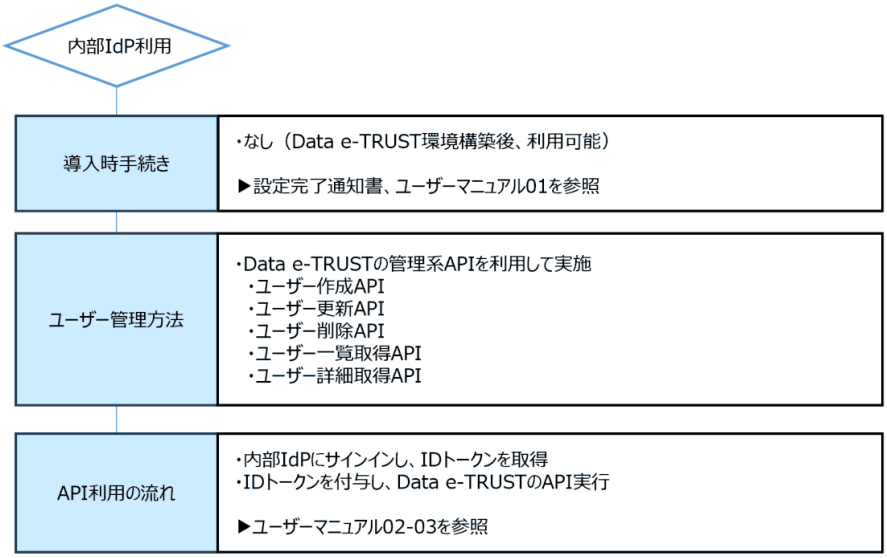
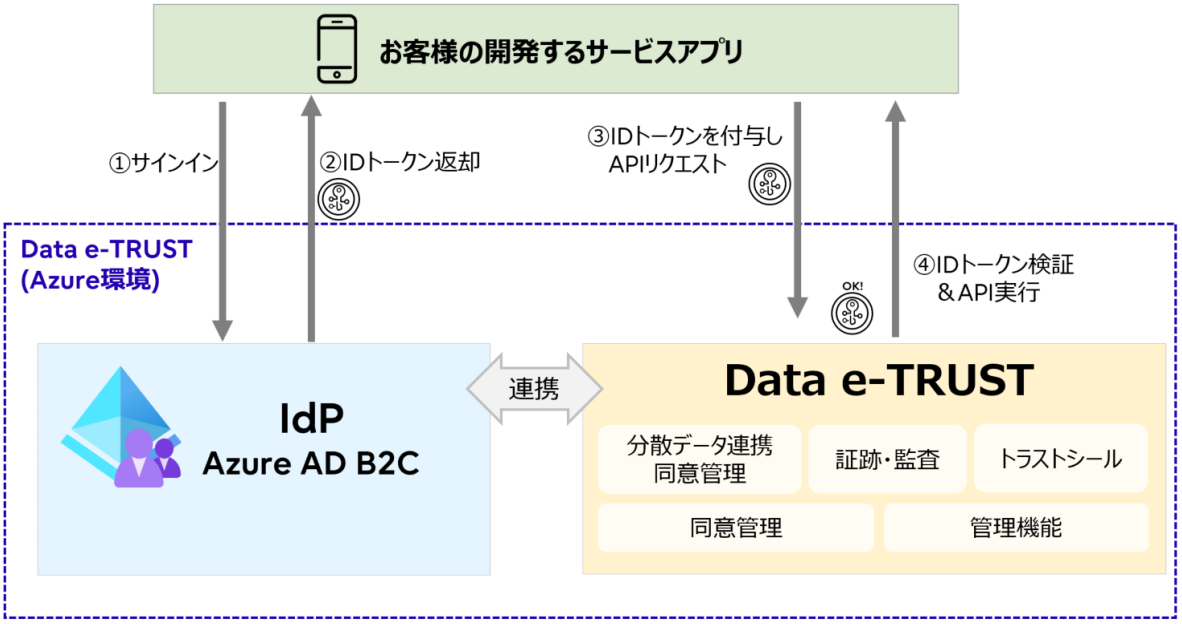


図2.4 API実行の流れ

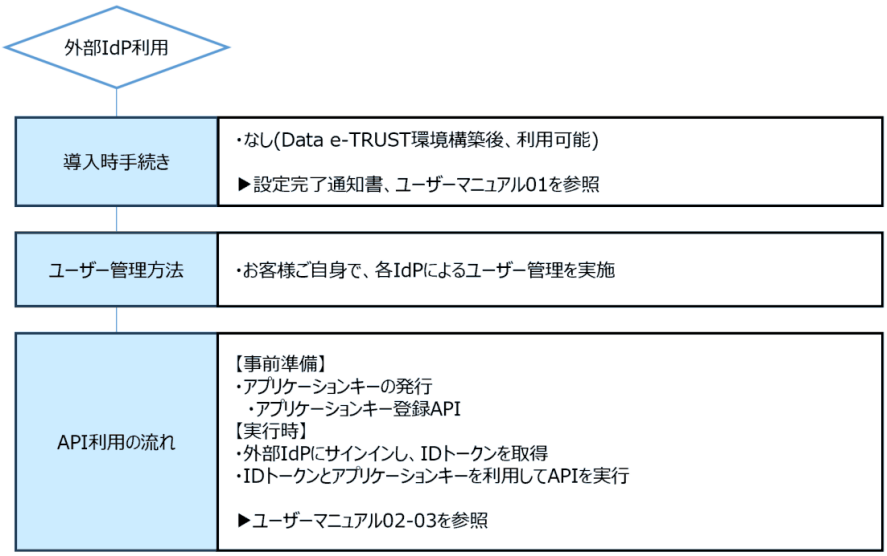


内部IdPを利用する場合、API実行時にIDトークンを利用します。
内部IdPにサインインすることで取得したIDトークンを、APIリクエスト時に付与することで、APIを実行してください。

詳しい手順については、「ユーザーマニュアル03_Data e-TRUSTAPI利用手順」の「3.API実行手順」を参照してください。

2.2.3 外部IdPを利用する場合

外部IdP利用時の認証・認可の流れ



外部IdPを利用する場合、API実行時にIDトークンとアプリケーションキーを利用します。
アプリケーションキーの利用にあたり、以下の作業を実施してください。

- 事前準備
- API実行方法

詳細は「ユーザーマニュアル03_Data e-TRUSTAPI利用手順」の「6.アプリケーションキーによるAPI実行」を参照してください。

参考

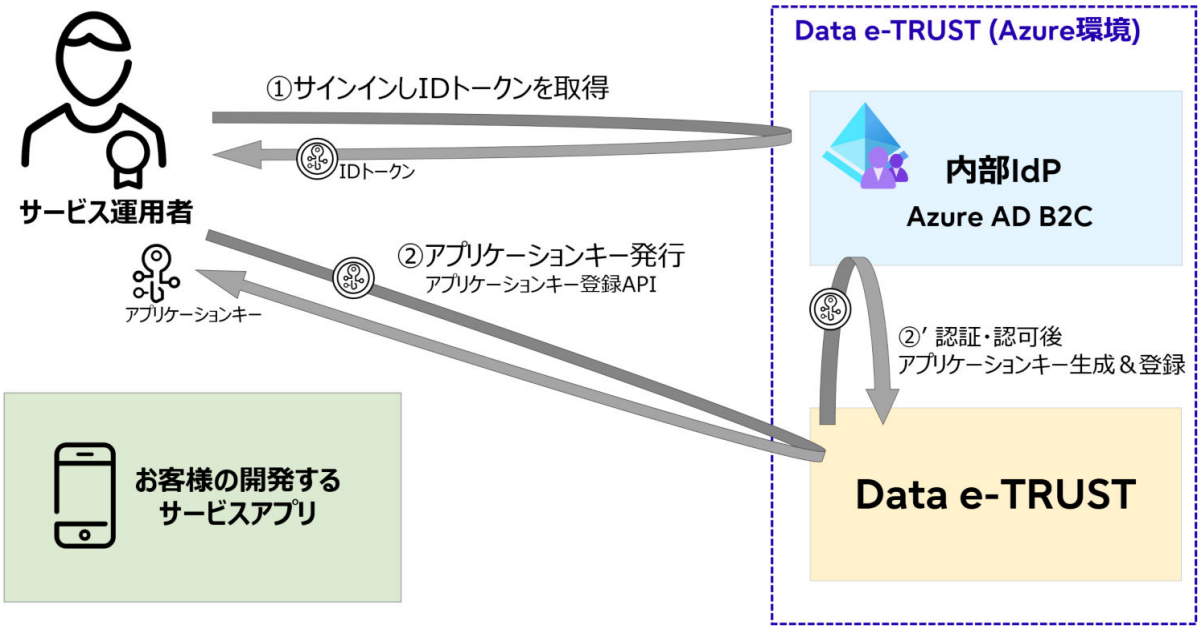
外部IdPとしてAzure AD B2Cを利用する場合に限り、導入時にフェデレーション設定を実施することで、アプリケーションキーを利用しないAPI実行が可能となります。

詳細は「ユーザーマニュアル01_各種設定変更申請手順」の「5.外部認証連携設定申請」を参照してください。

【事前準備】

アプリケーションキーを以下の手順で取得してください。

図2.5 事前準備



(1)サインインしIDトークンを取得

アプリケーションキーの発行には、Data e-TRUSTのアプリケーションキー登録APIを実行する必要があります。
アプリケーションキー登録APIの実行には内部IdPによる認証が必要なため、内部IdPにサインインしてIDトークンを取得してください。

環境構築時に提供する「Data e-TRUST 設定完了通知書」記載の初期ユーザー情報に記載のユーザーなどで、内部IdPへサインイン可能です。

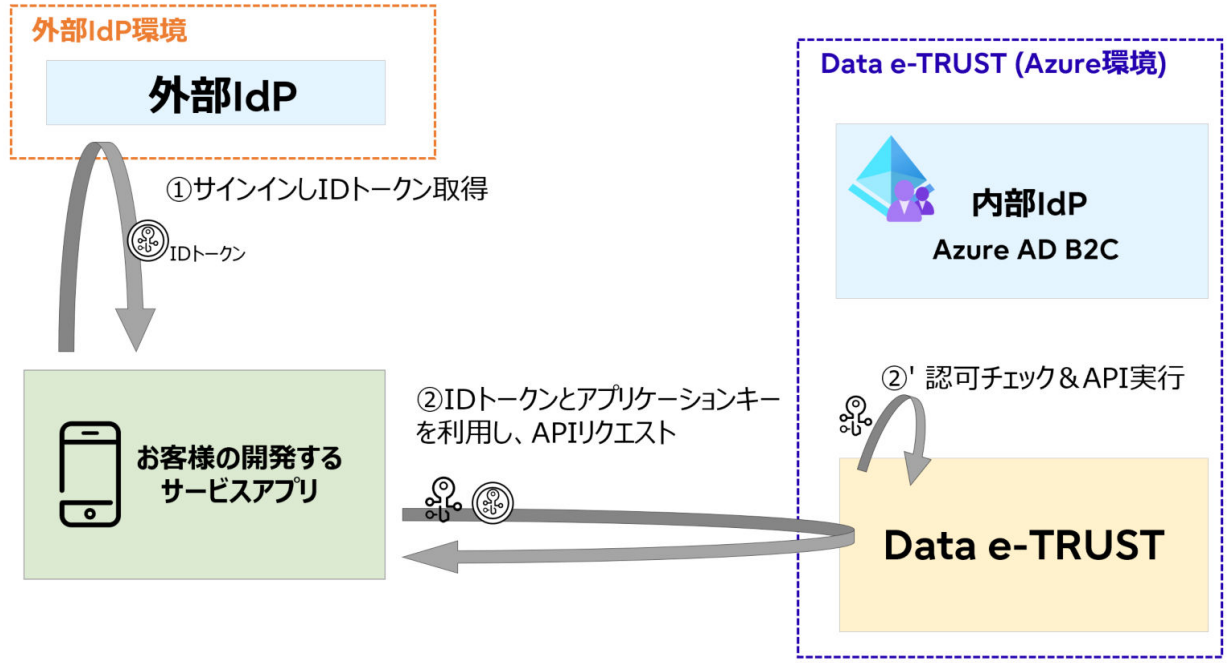
(2)アプリケーションキー発行

(1)で取得したIDトークンを利用し、アプリケーションキー登録APIを実行してください。

【API実行方法】

API実行の流れは以下の通りです。

図2.6 API実行方法



(1)外部IdPにサインインしIDトークン取得

お客様の開発するサービスアプリから、外部IdPにサインインし、IDトークンを取得してください。

(2)IDトークンとアプリケーションキーを付与しAPIリクエスト

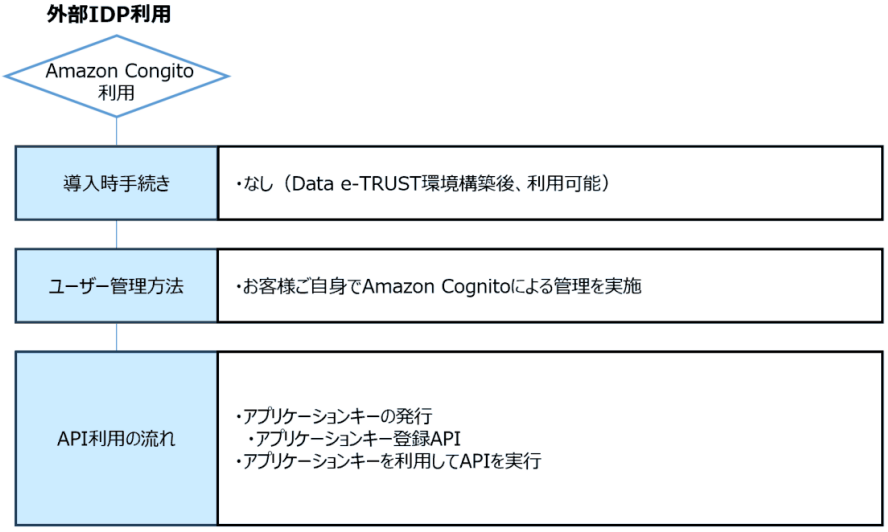
(1)で取得したIDトークンと事前準備で取得したアプリケーションキーを付与し、対象のAPIを実行してください。

注意

発行したアプリケーションキーは、暗号化やHSM領域への格納を行うなど、セキュアに管理してください。

2.2.4 外部IDPとしてAmazon Cognitoを利用する場合

外部IDPとしてAmazon Cognito利用時の認証・認可の流れ



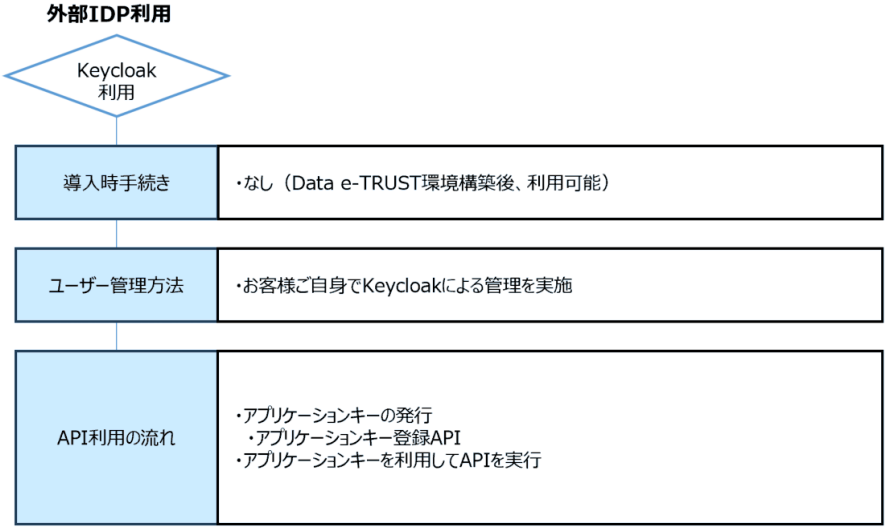
外部IDPとしてAmazon Cognitoを利用する場合、アプリケーションキーを利用してAPI実行時の認証・認可を行います。

アプリケーションキーを利用した場合のAPI利用の流れは2.2.6 アプリケーションキーを利用したAPI実行の流れ を参照してください。

フェデレーションによるAmazon Cognitoとの連携を希望される場合は、Data e-TRUSTシステム運用者にお問い合わせください。

2.2.5 外部IDPとしてKeycloakを利用する場合

外部IDPとしてKeycloak利用時の認証・認可の流れ



外部IDPとしてKeycloakを利用する場合、アプリケーションキーを利用してAPI実行時の認証・認可を行います。

アプリケーションキーを利用した場合のAPI利用の流れは2.2.6 アプリケーションキーを利用したAPI実行の流れ を参照してください。

2.2.6 アプリケーションキーを利用したAPI実行の流れ

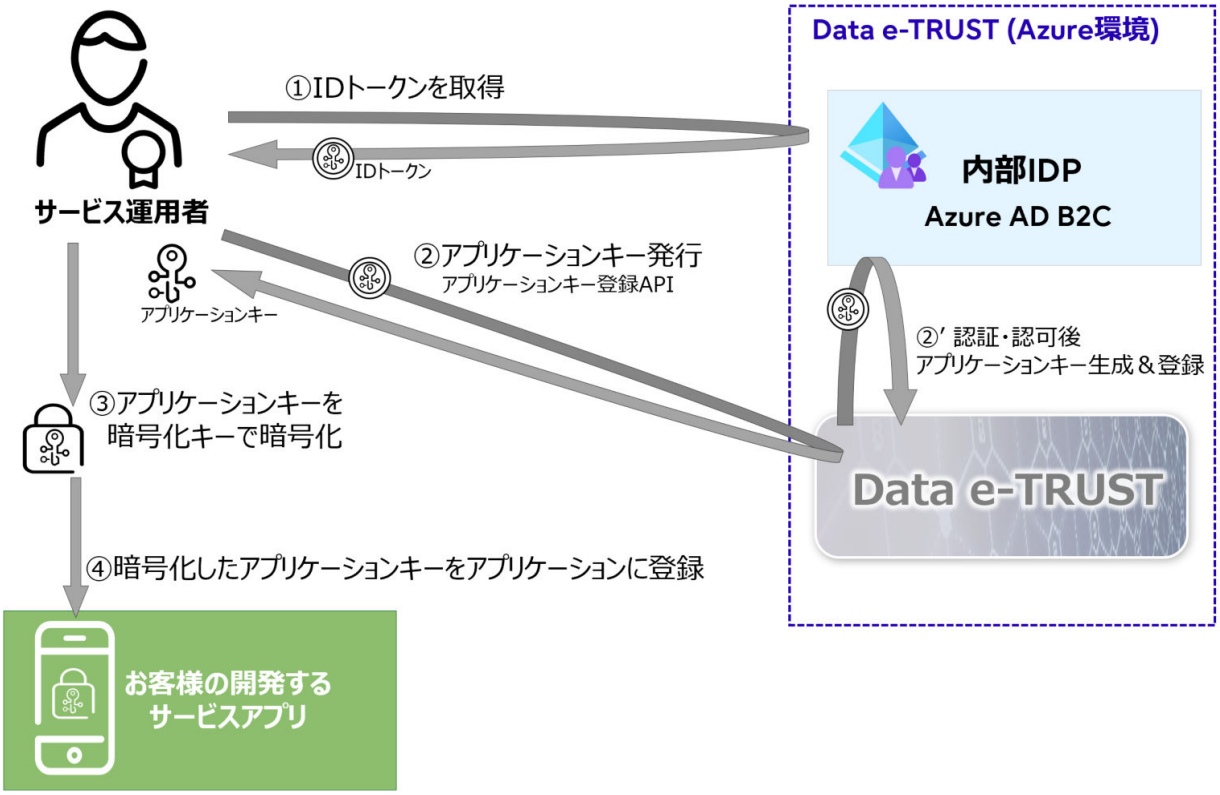
認証・認可にアプリケーションキーを利用する場合のAPI実行の流れを説明します。

詳細は、Data e-TRUST環境の払い出し時に提供するユーザーマニュアルを参照してください。

【アプリケーションキー利用時の事前準備】

アプリケーションキーによる認証・認可方式を利用する場合、事前に以下の作業を実施し、アプリケーションキーを準備する必要があります。

図2.7 アプリケーションキー利用時の事前準備



IDトークンを取得

アプリケーションキーの発行に「アプリケーションキー登録API」を実行するために必要となるIDトークンを取得してください。
環境構築時に払い出される初期登録用のサービス運用者ロールユーザー（★TODO名称確認★）を利用して、内部IDPに対してサインインを行うことでIDトークンを取得できます。

アプリケーションキー発行

取得したIDトークンを利用して、アプリケーションキー登録APIを実行してください。
Data e-TRUST内部では、IDトークンを利用した認証・認可ののち、アプリケーションキーを生成及び登録します。

アプリケーションキーを暗号化キーで暗号化

取得したアプリケーションキーを、暗号化キーにより暗号化してください。
アプリケーションキーの暗号化処理はお客様で担保ください。

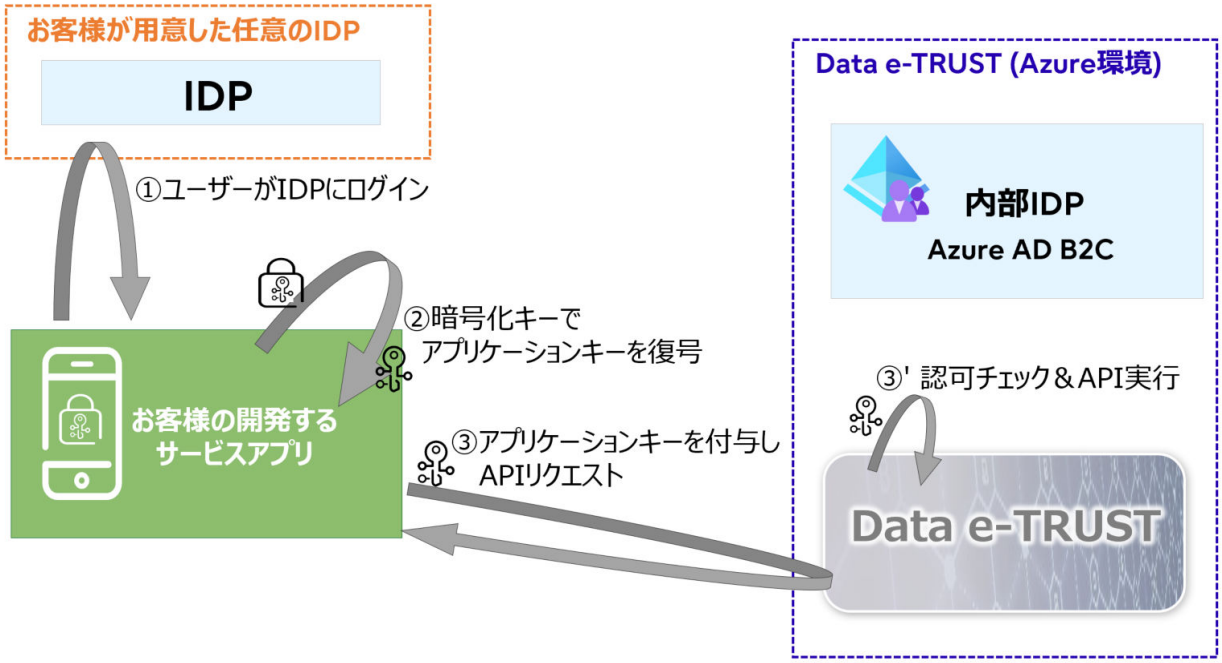
暗号化したアプリケーションキーをアプリケーションに登録

暗号化したアプリケーションキーを、アプリケーション内部（HSM領域など）にセキュアに登録してください。

【アプリケーションキーを利用したAPI実行の流れ】

アプリケーションキーによる認証・認可方式を利用時のユーザーによるAPI実行の流れは以下の通りです。

図2.8 アプリケーションキー利用時のAPI実行方法



ユーザーがIDPにログイン

お客様の開発するサービスアプリから、IDPを利用してログイン処理を実施してください。

暗号化キーでアプリケーションキーを復号

ログイン成功後、暗号化キーを用いてアプリケーションキーを復号してください。
アプリケーションキーの復号処理はお客様側で担保ください。

アプリケーションキーを付与しAPIリクエスト

復号したアプリケーションキーを付与し、APIリクエストを実行してください。
Data e-TRUST内部では、アプリケーションキーにより認可チェックののち、APIを実行します。

注意

事前準備およびAPI実行時のアプリケーションキーの暗号化処理、複合処理などアプリケーションキーの管理については、お客様側で責任を持って実施ください。

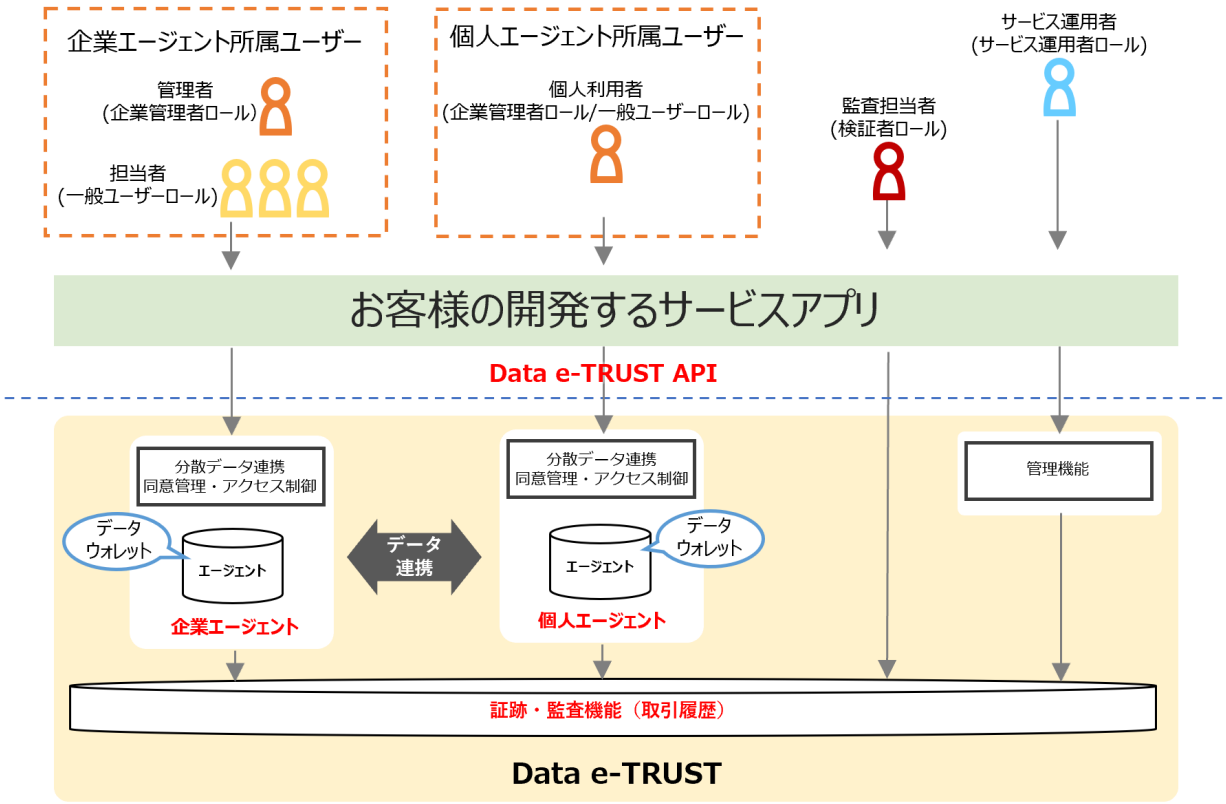
第3章 Data e-TRUSTを利用するための前提知識

Data e-TRUSTを利用してアプリケーションを開発するために、本サービスでの用語や概念を説明します。

【説明する用語・概念】

- Data e-TRUSTにおけるエージェント
- Data e-TRUSTにおけるユーザーとロール

図3.1 Data e-TRUSTにおけるエージェントとロール、各機能のイメージ図



3.1 Data e-TRUSTでのエージェントとは

Data e-TRUSTにおけるエージェントとは、データウォレットを管理する単位のことです。

エージェントはAPI操作を介して、データ操作とデータ送受信(連携)を実行します。
エージェント間でのデータ送受信は以下の組み合わせで実行可能です。

- 企業対企業
- 企業対個人
- 個人対個人

データへのアクセス権限は、エージェント単位で制御され、自身の所属するエージェントが保有するデータにのみアクセスできます。
他のエージェントが保有するデータにアクセスする場合は、APIを介して当該エージェントの管理者の許可の下、データ送受信(連携)を行うことでアクセスできます。

エージェントには、企業エージェントと個人エージェントの2種類があります。いずれも保有する機能は同じですが、ウォレットの利用方法により使い分けます。

- 企業エージェント
  - 企業・組織に所属するユーザーがアクセス可能なウォレットを管理します。

- 1つのエージェントを、企業・組織に所属する複数のユーザーが利用します。
- エージェントを管理する企業管理者ロールを持つユーザーと、一般ユーザーロールをもつユーザーが存在します。ロールについては3.2を参照ください。
- 企業エージェントの作成数の上限は、契約プランにより異なります。

・ 個人エージェント

- ユーザー本人のみがアクセス可能なウォレットを管理します。
- 個人ユーザーはエージェントの管理者を兼ねるため、企業管理者ロールを保有します。ロールについては、3.2を参照ください。
- 個人エージェントの作成数の上限は、契約プランごとのユーザー数の上限に依存します。

図3.2 企業間のデータ管理とデータ連携のイメージ

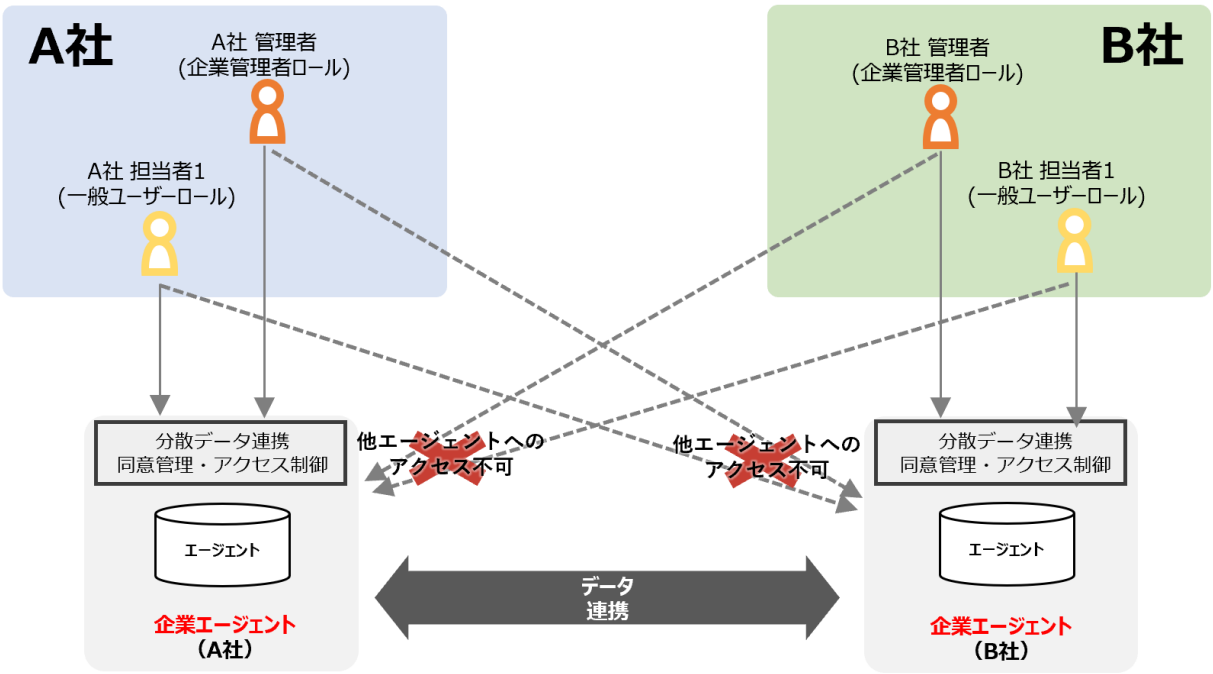
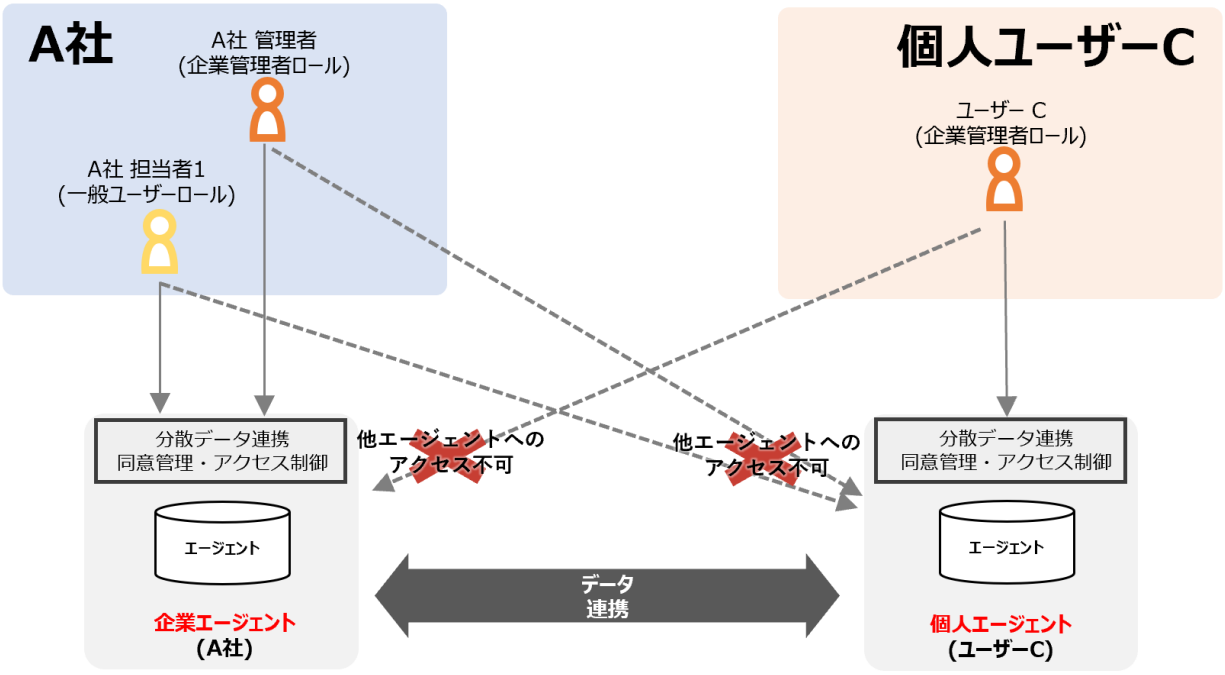


図3.3 企業と個人間のデータ管理とデータ連携のイメージ



3.2 Data e-TRUSTでのロールとは

Data e-TRUSTでのロールとは、利用するユーザーの役割に応じて付与される権限です。
付与されたロールにより、実行可能なAPIやAPI実行時に指定可能なオプション、レスポンス内容が異なります。

1ユーザーに、複数のロールを付与できます。

ロールにはAPI実行時にシステム全体でのユーザーの振る舞いを規定するユーザーロールと、各エージェント内での振る舞いを規定するエージェントロールの2種類があり、ユーザーロールとエージェントロールの組み合わせによって、API実行に必要なロールを決定します。

ユーザーロールとエージェントロールを組み合わせて決定するロールには、「分散データ連携機能、証跡・監査機能用ロール」4種類と、「トラストシール機能用ロール」3種類の合計7種類があります。

散データ連携機能、証跡・監査機能用のロールと、トラストシール機能用のロールはそれぞれ独立しています。

各ロールの指定方法は3.2.2を参照してください。

分散データ連携機能、証跡・監査機能用ロール

- サービス運用者ロール
  - Data e-TRUSTを利用したサービスを運用する管理者が付与されるロール
- 企業管理者ロール
  - 各企業エージェントに所属する一般ユーザーが付与されるロール
- 一般ユーザーロール
  - 各企業エージェントに所属する一般ユーザーが付与されるロール
- 検証者ロール
  - 証跡・監査機能を利用し監査作業をするユーザーが付与されるロール

トラストシール機能用ロール

- トラストシール管理ロール
  - ー 所属するエージェントの証明書とトラストシールの取得・検証の閲覧操作のみが可能なロール
- エージェント用トラストシール利用ロール
  - ー エージェント単位での証明書やトラストシールを利用・作成可能なロール
- ユーザー用トラストシール利用ロール
  - ー エージェントに属するユーザー単位での証明書やトラストシールを利用・作成可能なロール

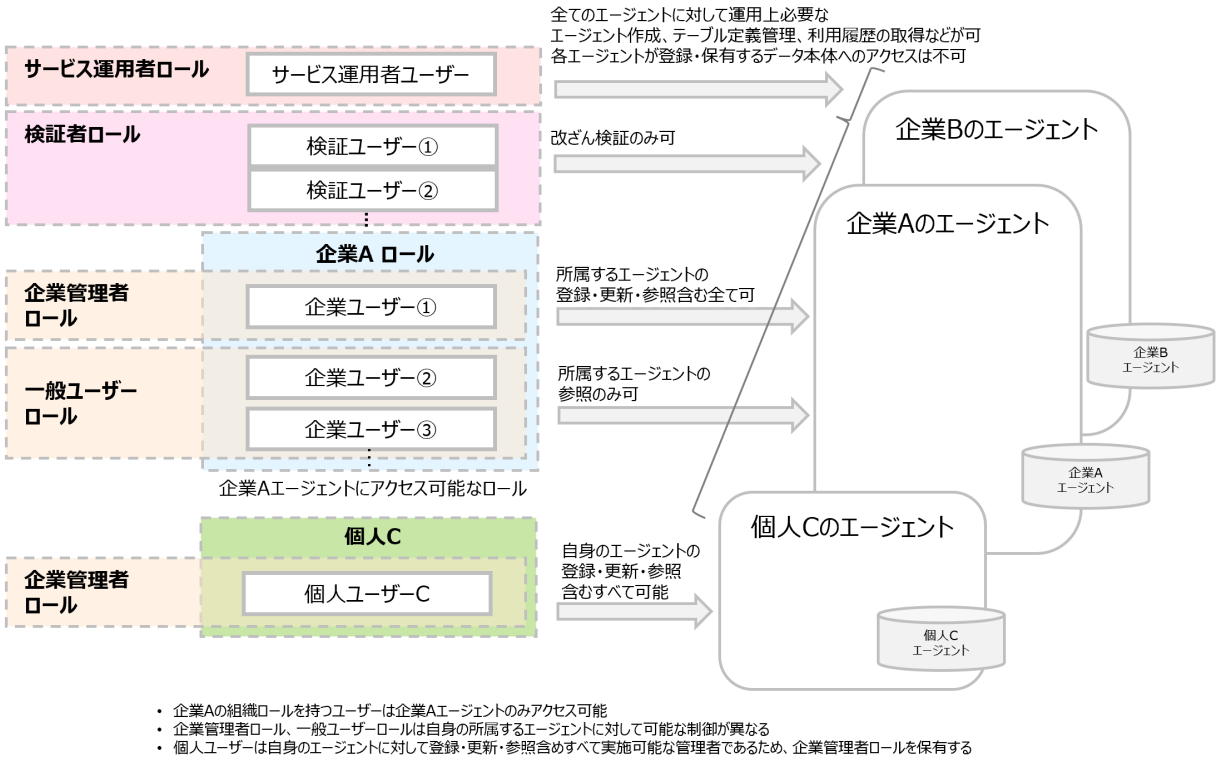
分散データ連携機能、証跡・監査機能用のロールの考え方については3.2.1を、トラストシール機能用のロールの考え方については6.1を参照してください。

3.2.1 分散データ連携機能、証跡・監査機能用ロールの考え方

分散データ連携機能、証跡・監査機能用のロールについての考え方を説明します。

各ロールで実行可能な機能およびアクセス可能なエージェントの範囲を次に示します。

図3.4 データ連携機能、証跡・監査機能用各ロールのアクセス権限



- 企業Aの組織ロールを持つユーザーは企業Aエージェントのみアクセス可能
- 企業管理者ロール、一般ユーザーロールは自身の所属するエージェントに対して可能な制御が異なる
- 個人ユーザーは自身のエージェントに対して登録・更新・参照含めすべて実施可能な管理者であるため、企業管理者ロールを保有する

【サービス運用者ロール】

Data e-TRUSTを利用したサービスを運用する管理者が付与されるロールです。

サービス運用に必要となるエージェント作成やテーブル定義の管理、利用履歴の取得などができます。
各エージェントが登録・保有するデータ本体にはアクセスできません。

【企業管理者ロール】

Data e-TRUSTを利用したサービスを利用する企業・組織の管理者が付与されるロールです。

自身が管理するエージェントが登録・保有するデータにアクセスできます。

【一般ユーザーロール】

各企業エージェントに所属する一般ユーザーが付与されるロールです。

自身が所属するエージェントが保有するデータに参照アクセスのみができます。

【検証者ロール】

証跡・監査機能を利用し監査作業をするユーザーが付与されるロールです。

証跡・監査機能を利用した改ざん検証のみができます。

各ロールが実行可能なAPIの詳細については、APIリファレンス及びAPIリファレンス別冊を参照してください。

3.2.2 API実行時のロール指定方法

API実行に必要なロールは、ユーザーロールとエージェントロールを組み合わせることで決定します。

APIをリクエストする際に、操作対象のエージェントをリクエストヘッダーで指定し、操作対象ロールをリクエストに付与するIDトークンで指定します。

ユーザーは複数のエージェントに所属可能であり、各エージェントに対してロールを保持できます。
そのため、所属するエージェントごとに保持するロールを指定します。

各ロールの設定方法(組み合わせ)

表3.1 分散データ連携機能、証跡監査機能用ロールの指定方法

ロール種別	APIリクエスト時のパラメーター指定		備考
	ユーザーロール (user_role)	エージェントロール (agent_role*)	
サービス運用者ロール	operator	-	
企業管理者ロール	user	administrator	user_roleとagent_roleのパラメーターの組み合わせで指定。個人ユーザーは個人エージェントの管理者であるため、企業管理者ロールを保有する。
一般ユーザーロール	user	user	user_roleとagent_roleのパラメーターの組み合わせで指定。
検証者ロール	verifier	-	

*正確にはagent1_role, agent2_role,…agent10_roleの10種類が指定可能。詳細はAPIリファレンスを参照してください。

表3.2 トラストシール機能用ロールの指定方法

ロール種別	APIリクエスト時のパラメーター指定		備考
	user_role	agent_role*	
トラストシール管理ロール	user	tseal_administrator	user_roleとagent_roleのパラメーターの組み合わせで指定。
エージェント用トラストシール利用ロール	user	tseal_agent	user_roleとagent_roleのパラメーターの組み合わせで指定。
ユーザー用トラストシール利用ロール	user	tseal_user	user_roleとagent_roleのパラメーターの組み合わせで指定。

* 正確にはagent1_role, agent2_role,…agent10_roleの10種類が指定可能。詳細はAPIリファレンスを参照してください。

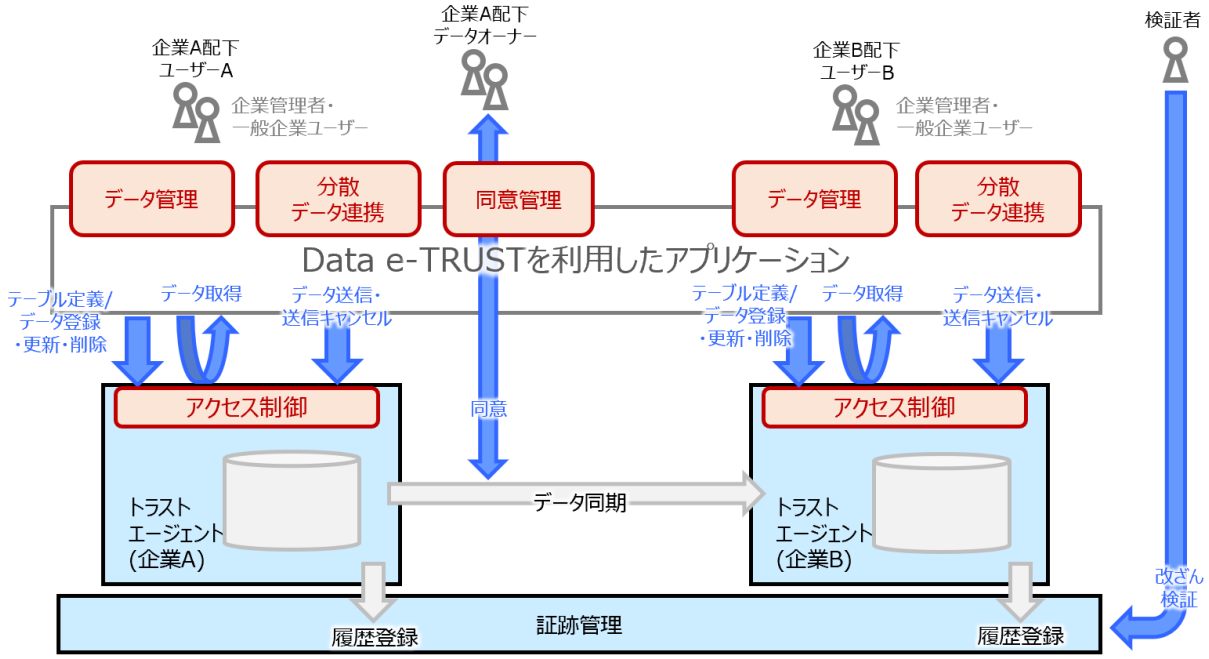
第4章 Data e-TRUSTのデータ流通について

Data e-TRUSTの分散データ連携機能では、企業や組織が持つそれぞれのエージェント間で、データの共有・連携が可能です。
また、分散データ連携機能と同意管理機能を組み合わせることで、データオーナーの同意に基づいたデータ流通が実現できます。

4.1 データ流通を利用するための前提知識

Data e-TRUSTのデータ流通を利用する上で必要となる、各APIの関係について示します。

データ流通は、分散データ連携機能の各APIと、同意管理機能のAPIによって実現します。
データ流通に関連する機能と、主なAPIの関係は図のとおりです。
各APIの詳細については、APIリファレンスマニュアルおよびAPIリファレンスマニュアル:別冊を参照ください。



4.2 Data e-TRUSTでのデータ流通の流れ

Data e-TRUSTの分散データ連携機能を利用してデータ流通をするための基本的な流れを説明します。
ここでは、他の組織に対してデータ送信をする際の基本的な利用方法について、「データ流通をするための準備手順」、「データ流通開始手順」、および、「データ流通停止手順」に分けて記載しています。

	項番	操作	説明
データ流通をするための準備手順	1	エージェントの作成・登録	企業・組織ごとに発行されるエージェントIDに紐づけ、各エージェント専用のDBを作成します。 3.3.1で説明します。
	2	テーブル定義の登録	作成したエージェント上のDBにテーブルを登録します。 3.3.2で説明します。
データ流通開始手順	3	データ登録	定義済のテーブルにデータを登録します。 3.3.3で説明します

	項番	操作	説明
	4	エージェント間でのデータ送信	エージェント間でデータを送信・同期します。 3.3.4で説明します。
	5	データ取得	DBに登録したデータ、自エージェントに送信されたデータを取得します。 3.3.5で説明します。
データ流通停止手順	6	データ同期の停止	他エージェントに送信・同期中のデータの同期を停止します。 3.3.6で説明します。
	7	データ削除	DBに登録したデータを削除します。 3.3.7で説明します。

4.3 Data e-TRUSTでの基本的なデータ流通操作

4.3.1 Data e-TRUSTでのエージェントの作成・登録方法とは

Data e-TRUSTを利用するために、管理機能のエージェント作成APIで、エージェントを作成・登録します。

エージェント作成API

エージェント作成は、Data e-TRUSTを利用するための最初の操作です。
指定したエージェントIDに紐づけ、エージェントとエージェント専用のデータベースを作成します。
これにより、エージェントごとにデータを管理できます。
エージェント作成APIは、サービス運用者ロールおよび企業管理者ロールのみ実行できます。
また、データベースは1エージェントにつき1つ作成されます。

4.3.2 Data e-TRUSTでのテーブル定義の登録とは

Data e-TRUSTで扱うデータ登録の準備のために、分散データ連携機能のテーブル定義APIで、エージェントのデータベースに対しテーブル定義をします。

テーブル定義

各エージェント専用のデータベースでデータを扱うための準備として、テーブル定義をします。

ポイント

データオーナー型について

テーブルに指定可能なカラムの型に、文字列型などの一般的なデータ型に加え、Data e-TRUST独自のデータオーナー型を定義できます。
これにより、レコードを所有しているデータオーナーを指定できます。
データオーナー型のカラムをもつレコードは、他エージェントにデータ送信・同期をする際に、データオーナーによるデータ送信・同期への同意(許諾)を必要にできます。
詳細は、データ送信API、同意APIを参照してください。

テーブル定義には、以下3つのAPIエンドポイントがあります。

テーブル定義(新規作成)API

指定したテーブル構成(カラム)で新規のテーブルを作成します。
新しいテーブルを作成するときに利用してください。

テーブル定義(更新)API

指定したテーブルに対して、カラムの追加と削除、インデックスの追加と削除、参照関係の追加と削除を実施します。
作成済みのテーブル定義を更新する際に利用してください。

テーブル定義(削除API)

指定したテーブルを削除します。

注意

テーブルを削除すると、テーブルに格納されているデータも削除されます。

4.3.3 Data e-TRUSTで扱うデータの登録方法とは

エージェントのデータベースに対して、Data e-TRUSTで扱うデータを登録します。

データ登録

定義したテーブルにデータを登録します。
登録するデータは、テーブル定義で設定済みのカラム構成で登録します。

データ登録に利用するAPIは2種類あります。JSON形式でデータ登録をする個別データ登録・更新APIと、ファイルに登録したデータを登録可能な一括データ登録・更新APIです。

個別データ登録・更新API

JSON形式で指定したデータをテーブルに登録します。

一括データ登録・更新API

CSV形式、または、CSVファイルを圧縮したZIP形式のファイルにより、データを一括で登録・更新します。
データの初期登録時など、大量のデータを一度に登録する際に利用ください。

4.3.4 Data e-TRUSTで扱うデータの送信方法とは

Data e-TRUSTに登録されている自エージェントのデータを、他のエージェントに送信(同期)できます。
データ送信処理のパターンにより、分散データ連携機能の3つのAPIと、同意管理機能の1つのAPIを組み合わせることで、データ送信を実現します。

データ送信操作に関連するAPI

データ送信API

指定したエージェントに対して連携したいデータを送信・同期します。

データ送信依頼API

他のエージェントに対して指定したデータの送信を依頼します。

データ送信依頼応答API

データ送信依頼APIによって依頼されたデータの送信可否を、依頼元エージェントに回答します。

同意回答API

「同意依頼通知」のクライアント通知を受け、データオーナーがデータの送信可否を通知元エージェントに回答します。

参照

クライアント通知について

クライアント通知の取得方法にはPush型の「クライアント通知機能」を利用する方法と、Pull型の「クライアント通知取得API」を利用する方法の2種類があります。

いずれの方法も、取得可能な情報は同じです。クライアント通知で取得可能な内容についてはAPIリファレンス:別冊を参照してください。

クライアント通知機能

事前に指定した通知先サーバーに、各種処理の結果をPush型で通知します。利用するためには事前に通知先を設定する必要があります。

詳細はAPIリファレンスマニュアル、APIリファレンスマニュアル:別冊、環境構築時に提供するユーザーマニュアル_01を参照してください。

クライアント通知取得API

API実行により、通知済みのクライアント通知内容をPull型で取得することができます。
本APIはクライアント通知設定の有無によらず、クライアント通知内容を取得できます。
詳細はAPIリファレンスマニュアル、APIリファレンスマニュアル:別冊を参照してください。

エージェント間でのデータ送信パターン

エージェント間でのデータ送信処理には、大きく分けて以下の3つのパターンがあります。

- 同意取得が不要なデータの送信
- 同意取得が必要なデータの送信
- 他エージェントからの依頼をもとにデータを送信

以下に、企業Aから企業Bにデータを送信した場合のエージェント間でのデータ送信パターンを示します。

登場人物

- 送信元企業:企業A
  - ユーザーa:企業A配下の企業管理者ユーザー
  - ユーザーc:企業A配下の一般ユーザーであり、送信対象データのデータオーナー
- 送信先企業:企業B
  - ユーザーb:企業B配下の企業管理者ユーザー

注意

クライアント通知の通知先について

クライアント通知はクライアント通知設定先のペイロードURLに通知されます。
そのため、クライアント通知を利用する場合は、アプリケーション側で通知を受けとり各ユーザー宛に通知処理をしてください。

以降の説明では便宜上「○○のクライアント通知により、ユーザー●●に△△を通知」と記載していますが、Data e-TRUSTの機能では直接ユーザー宛に通知はしません。ユーザーへの通知はアプリケーション側で実施してください。

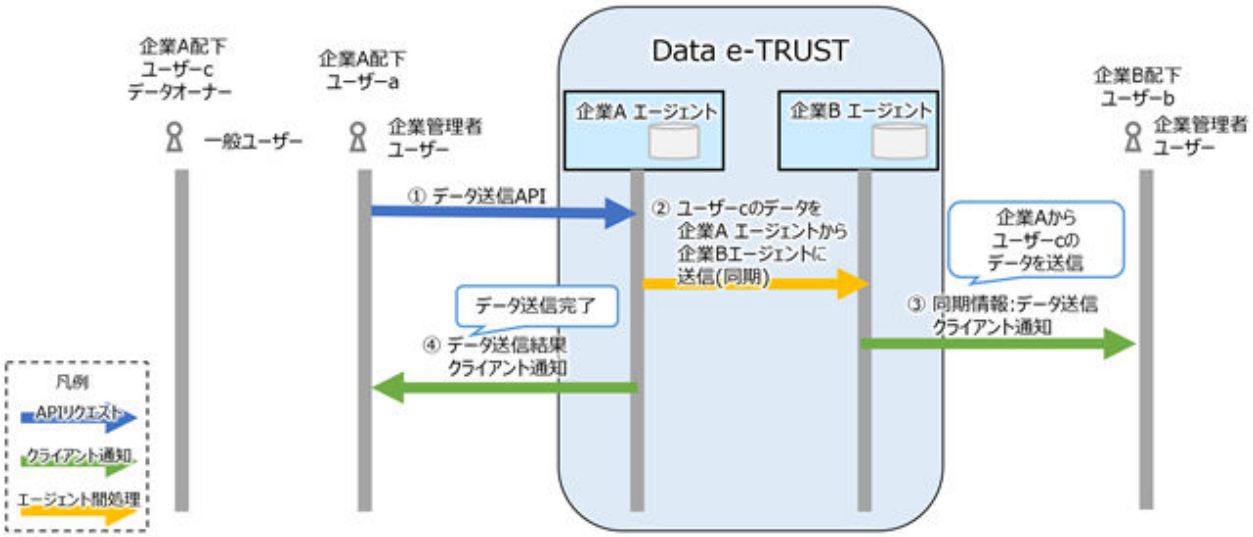
クライアント通知についてはAPIリファレンスマニュアルのクライアント通知設定APIの項、およびAPIリファレンスマニュアル:別冊の6章3節を参照してください。

同意取得が不要なデータの送信

別エージェントへのデータ送信時に、データオーナーのユーザーcによる同意が不要な場合、データ送信APIを利用します。
本処理の流れは以下のとおりです。

1. 企業A配下のユーザーaがデータ送信APIを実行。
2. 企業Aエージェントが企業Bエージェントに送信対象データを送信。

   企業B配下のユーザーbは、ユーザーaが送信したデータを利用可能となる。
3. 「同期情報:データ送信」のクライアント通知により、送信先のユーザーbにデータ送信処理の結果を通知。
4. 「同期情報:データ送信結果」のクライアント通知により、送信元のユーザーaにデータ送信処理の結果を通知。



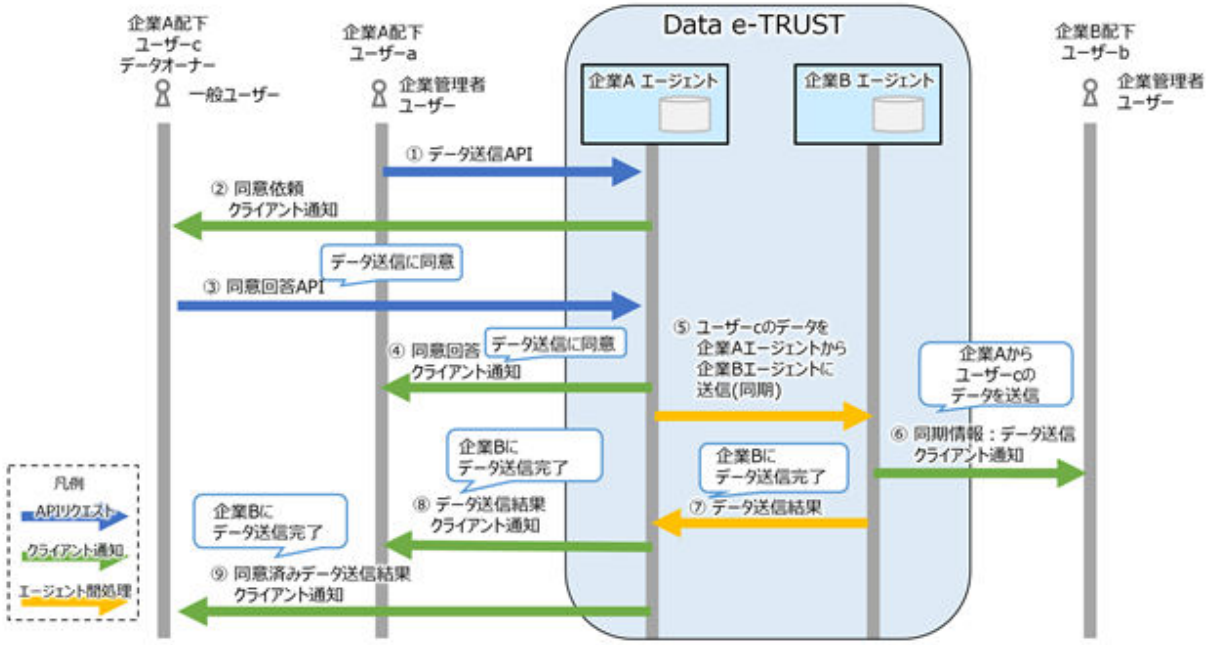
同意取得が必要なデータの送信

別エージェントへのデータ送信時に、データオーナーのユーザーcによる同意が必要な場合、データ送信APIと同意回答APIの2つのAPIを利用します。

本処理の流れは以下のとおりです。

1. 企業A配下のユーザーaがデータ送信APIを実行。
2. 「同意依頼」のクライアント通知により、企業A配下のデータオーナーのユーザーcにデータ送信の同意依頼を通知。
3. ユーザーcが同意回答APIを実行し、送信に同意する旨を企業Aエージェントに送信。
4. 「同意回答」のクライアント通知により、ユーザーaにユーザーcがデータ送信に同意したことを通知。
5. 同意回答に従い、企業Aエージェントから企業Bエージェントにデータを送信。

   企業B配下のユーザーbは、ユーザーaが送信したデータを利用可能となる。
6. 「同期情報:データ送信」のクライアント通知により、送信先のユーザーbにデータ送信処理の結果を通知。
7. エージェント間処理で、企業Bエージェントから企業Aエージェントにデータ送信の完了を通知。
8. 「データ送信結果」のクライアント通知により、送信元のユーザーaにデータ送信処理の結果を通知。
9. 「同意済みデータ送信結果」のクライアント通知により、データオーナーのユーザーcにデータ送信処理の結果を通知。



他エージェントからの依頼をもとにデータを送信

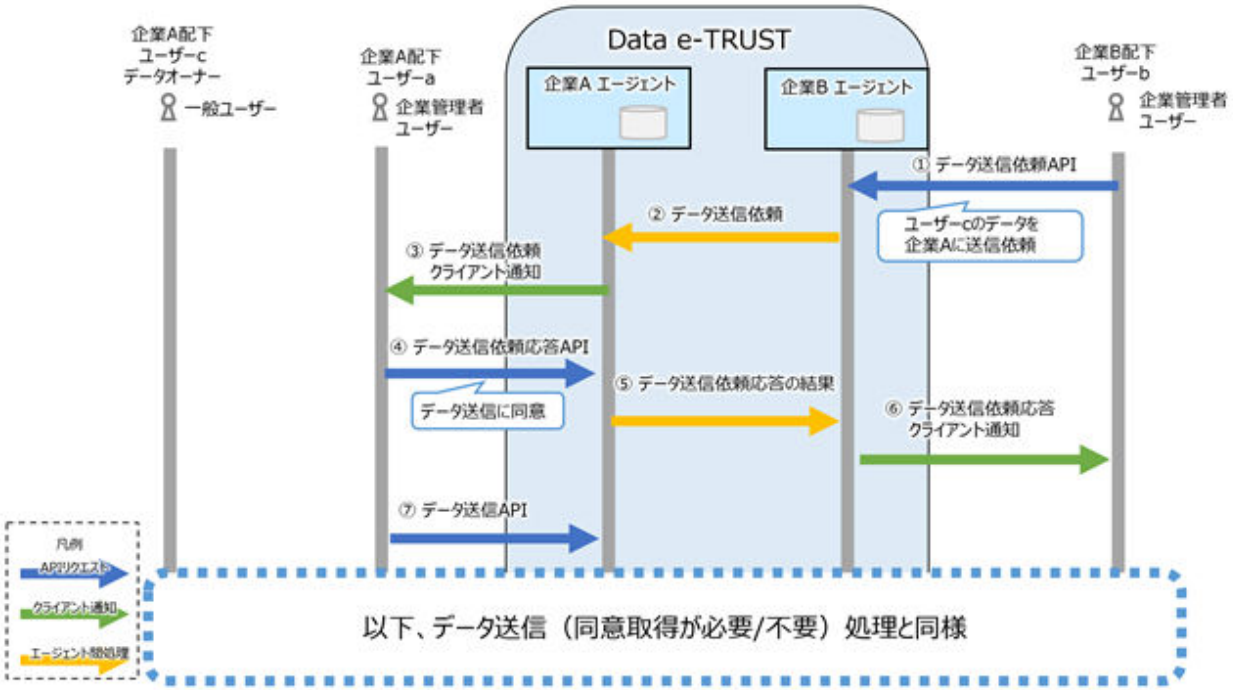
他エージェントの企業B配下の、ユーザーbの依頼でデータを送信する場合は、データ送信依頼API、データ送信依頼応答API、データ送信APIの3つのAPIを利用します。
本処理の流れは以下のとおりです。

1. 企業B配下のユーザーbがデータ送信依頼APIを実行。
2. エージェント間処理で、企業Bエージェントから企業Aエージェントにデータ送信依頼を通知。
3. 「データ送信依頼」のクライアント通知により、企業A配下のユーザーa宛にデータ送信依頼を通知。
4. ユーザーaがデータ送信依頼応答APIを実行し、データ送信に同意する旨を企業Aエージェントに通知。

   データ送信依頼応答APIを実行し、データ送信に対する同意を回答するだけでは、企業Bにデータは送信されない。
5. エージェント間処理で、企業Aエージェントから企業Bエージェントにデータ送信依頼応答の結果を通知。
6. 「データ送信依頼応答」のクライアント通知により、ユーザーbに対しデータ送信の同意を得たことを通知。

7. ユーザーaがデータ送信APIを実行

これ以後、企業Bエージェントにデータを送信するため、「同意取得が不要なデータの送信」または「同意取得が必要なデータの送信」どちらかの処理を実行する必要がある。



4.3.5 Data e-TRUSTで扱うデータの取得方法とは

データ取得APIにより、自エージェントに登録されているデータを取得できます。

データ取得API

自エージェントまたはアクセス権限のあるエージェント内のテーブルに対して、指定した条件で検索しデータを取得できます。

自エージェントに登録したデータや、自エージェントに送信・同期されたデータを取得する場合に、利用してください。

4.3.6 Data e-TRUSTで扱うデータ同期の停止方法とは

データ送信キャンセルAPIにより、他のエージェントに送信・同期されたデータの同期を停止できます。

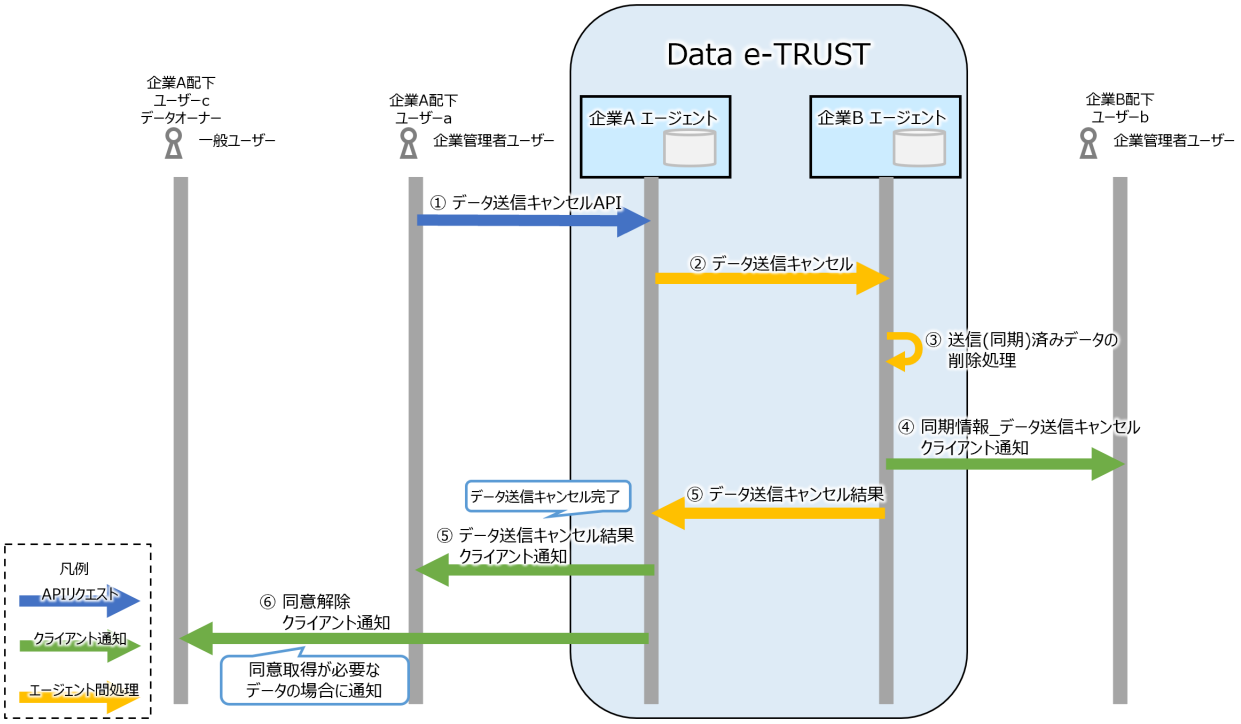
データ送信キャンセルAPI

指定したデータの同期が停止され、データ送信先エージェント上のデータが削除されます。

データ同期の停止

データの送信元の企業A配下のユーザーaがデータ送信キャンセルAPIを実行することで、データ送信先エージェントの企業B上のデータが削除されます。

データ送信・同期の停止結果は、クライアント通知によって、データ送信元の企業Aエージェント、データ送信先の企業Bエージェント、データオーナーのユーザーcに通知されます。



4.3.7 Data e-TRUSTで扱うデータの削除方法とは

Data e-TRUSTに登録されているデータを削除する場合は、データ削除APIを利用します。

データ削除API

データ削除APIでは、自エージェントに登録した任意のレコードを指定した条件で削除できます。

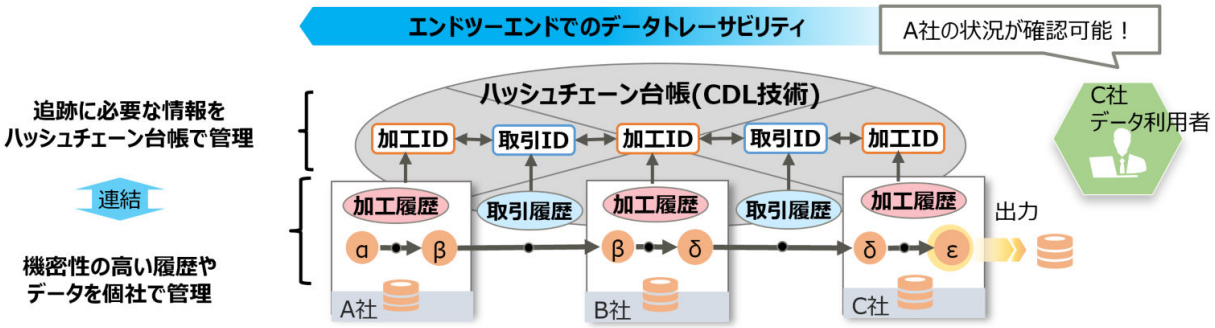
削除対象のデータが、データ送信APIにより他エージェントに対して送信・同期済みの場合は、送信・同期先のエージェントに登録されているデータもすべて削除します。

不要なデータをレコード単位で削除する場合に利用してください。

第5章 Data e-TRUSTの証跡・監査機能

Data e-TRUSTの証跡・監査機能では、データの取引・流通の過程で発生する一連の履歴を、改ざん不可能、相互検証可能、公開・非公開制御可能な形式で管理します。

本章では、証跡・監査機能を利用する上で必要となる知識と、基本的な利用の流れを理解します。



5.1 証跡・監査機能を利用するための前提知識

Data e-TRUSTの証跡・監査機能を利用する上で知る必要のある用語とデータモデル、データ構造について理解します。

5.1.1 証跡・監査機能で必要となる用語

CDLによる証跡・監査機能を利用する上で、必要となる用語を理解します。

履歴/履歴情報

証跡・監査機能が管理する、個々の発生事象、事項、処理、出来事を表す情報のことです。
履歴の例を以下に示します。

- 企業・組織間での「送った」「受け取った」などの個々の事象を表す取引情報・来歴情報
- モノのサプライチェーンやトレーサビリティーでの個々の発生事象、処理情報
- データ利活用における、データに対する加工や送受信の情報

リネージュ(Lineage)

履歴を連結し、一繋がりにした履歴群のことです。

「いつ何が起きたか」を示す個々の履歴を、前後に連結することで表現されるデータ群です。

グローバルデータ

履歴を構成する情報のうち、全組織に対して無条件に公開・共有する情報のことです。

ローカルデータ

履歴を構成する情報のうち、全組織に対して無条件では公開せずに、アクセス制御をした上で特定の組織・ユーザーに対してのみ公開する情報のことです。

5.1.2 証跡・監査機能のデータモデルとリネージュ構造とは

証跡・監査機能では実世界の様々なサプライチェーンやトレーサビリティーを写像・記録するため、専用のデータモデルを持ちます。

データモデルは、CDLが管理するデータの最小単位「履歴情報」と、「履歴情報」を前後に連結する「リネージュ」で構成されます。

リネージュは、履歴データを[ヘッダー]部の「次履歴ID群」と「前履歴ID群」を前後に連結したもので構成されます。

リネージュのデータ構造により、CDLからデータを取り出したあとも、データが改ざんされていないことを検証できます。

リネージュの履歴に分岐がある場合、リネージュの末端の履歴は複数存在しますが、その末端の履歴それぞれにデジタル署名が付与されます。

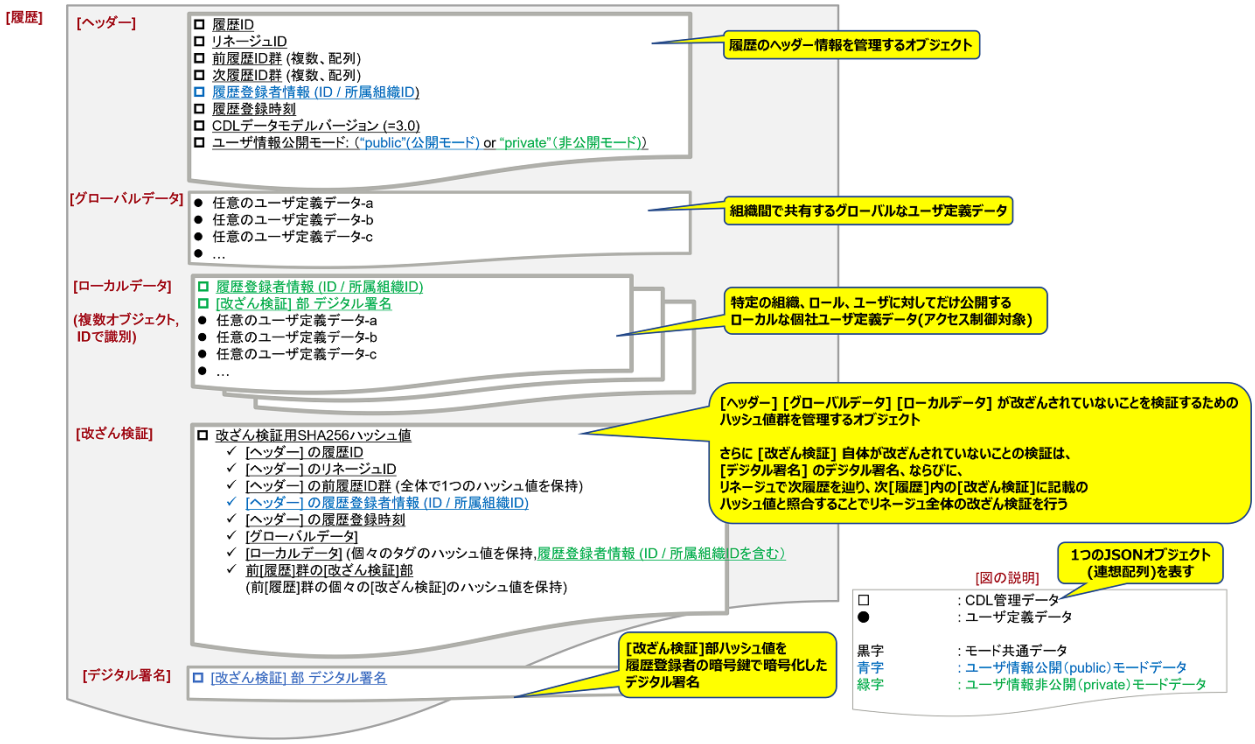
証跡・監査機能の改ざん検証APIを実行すると、各項目のハッシュ値が算出・照合されるため、データ改ざん検証をできます

5.1.3 CDLのリネージュを構成する履歴情報のデータ構造

CDLのリネージュを構成する個々の履歴情報は以下の5つのパートから構成されます。

- ヘッダー部
- グローバルデータ部
- ローカルデータ部
- 改ざん検証部

・ デジタル署名部



[ヘッダー]部

[ヘッダー]部は履歴インデックスとリネージュ情報の2つで構成されます。

履歴インデックス

履歴インデックスは以下の4つで構成されます。

・ 履歴ID

・ 登録者ID

・ 登録者組織ID

・ 登録時刻

リネージュ情報

履歴の前後関係を管理します。
リネージュ情報は以下の2つで構成されます。

・ 前履歴ID群

・ 後履歴ID群

[グローバルデータ] 部

履歴情報のうち、他組織に対して公開する共有部の情報を表します。

[ローカルデータ] 部

許可した組織に対してだけ公開し、他組織にはアクセス制御をする情報を表します。
複数のデータを登録できます。個々のデータはID(ローカルデータID)で識別します。

[改ざん検証] 部

CDLからリネージュとして履歴データ群を取り出した後も、履歴データが改ざんされていないことを検証するために利用する情報です。
[ヘッダー]部、[グローバルデータ]部、[ローカルデータ]部のSHA256ハッシュ値を格納します。

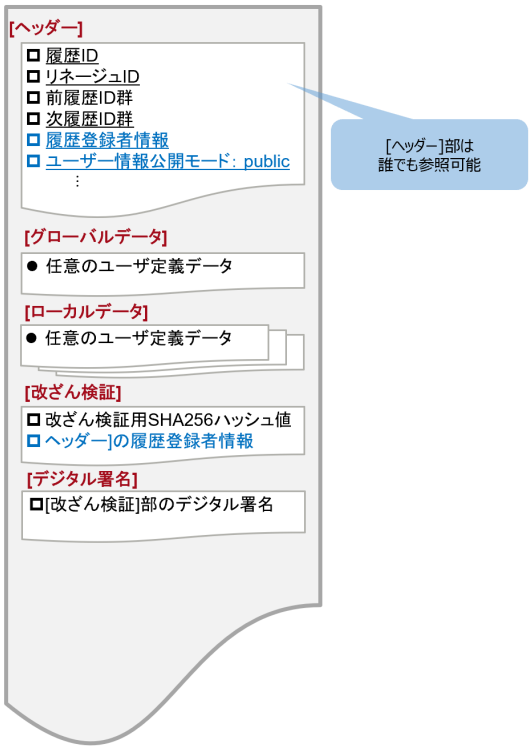
[デジタル署名] 部

[改ざん検証] 部が(履歴登録者以外から)改ざんされていないことを検証可能とするために、[改ざん検証] 部のSHA256ハッシュ値を履歴登録者の秘密鍵で暗号化したデジタル署名を格納します。

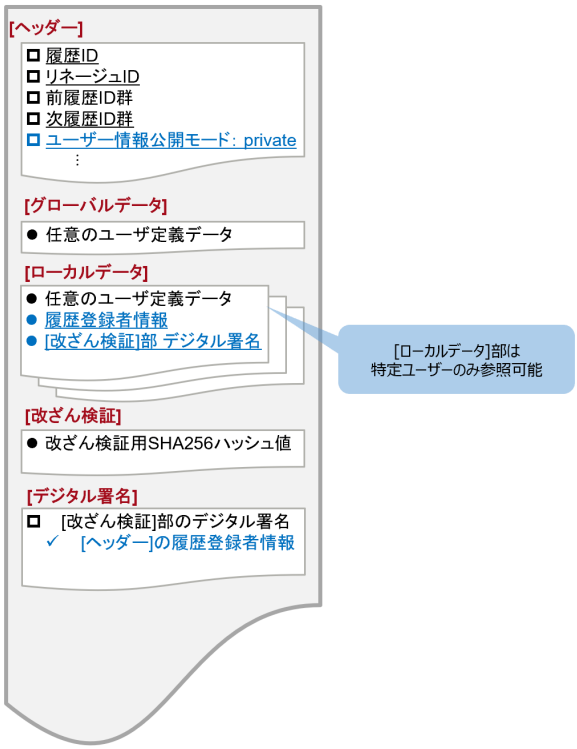
5.1.4 「ユーザー情報公開モード」と「ユーザー情報非公開モード」とは

証跡・監査機能には「ユーザー情報公開モード」と「ユーザー情報非公開モード」の2種類のモードがあります。
このモードは証跡の「履歴登録API」におけるパラメタ「cdl:DataModelMode」で指定します。

ユーザー情報公開モードの履歴情報



ユーザー情報非公開モードの履歴情報



ユーザー情報公開モード

情報のオープン性、透明性を重視し、組織(エージェント)間で基本情報を共有する運用の場合に選択します。

ユーザー情報(登録者ID、登録者組織ID) と履歴登録者のデジタル署名は[ヘッダー]部に格納され、全組織に公開されます。

ユーザー情報非公開モード

直接取引する組織(エージェント)間以外はユーザー情報を機密情報とし、組織同士のデータ取引情報を見せない運用の場合に選択します。
ユーザー情報非公開モードでも、履歴登録後に参照ポリシー設定をすることで、直接取引を行わない組織に対してユーザー情報を公開できます。

以下に、A社からE社まで順にデータが送信された場合の例を示します。

この時C社が直接取引するのは、データ送信元のB社と、データ送信先のD社のみです。

ユーザー情報公開モードの場合、C社はA社からE社まで関係するすべての取引相手を履歴情報から確認できます。

ユーザー情報非公開モードの場合、C社は直接取引をするB社とD社は確認できますが、A社とE社の情報を確認することはできません。

ユーザー情報公開モードの場合：C社が直接取引していない相手も、履歴情報から確認できる

ユーザー情報非公開モードの場合：C社がデータを直接取引していない相手は不明

5.1.5 証跡・監査機能のデータモデルのJSONフォーマット

証跡・監査機能で履歴データを扱うときに、履歴データ用のJSONフォーマットを利用します。JSONフォーマットは2種類あります。

- 履歴データのJSONフォーマット
- 履歴登録用JSONフォーマット

各JSONフォーマットの詳細については、付録を参照ください。

5.2 証跡・監査機能の各操作の概要

Data e-TRUSTの証跡・監査機能で利用可能な各操作の概要は以下の通りです。

操作	説明
履歴登録	指定した履歴情報を登録し、リネージュとして管理します。
リネージュ取得	「履歴登録」によって登録したリネージュを取得できます。
履歴検索	「履歴登録」によって登録した履歴情報を、指定した条件で検索できます。
ローカルデータ削除	「履歴登録」によって登録した履歴情報のうち、指定した履歴情報のローカルデータ部に含まれる情報を削除できます。
参照ポリシー設定	履歴情報ごとに、ローカルデータ部を参照するために必要な権限を管理できます。
改ざん検証	指定したリネージュ全体、または個別の履歴情報に対して、改ざんの検知と登録者の検証ができます。

リネージュ取得、履歴検索、ローカルデータ削除、参照ポリシー設定、改ざん検証をするためには、各操作の対象となるリネージュがあらかじめ履歴登録によって登録されている必要があります。

5.3 証跡・監査機能の利用方法

5.3.1 証跡・監査機能の履歴登録とは

Data e-TRUSTで証跡・監査機能を利用するために履歴登録APIで、履歴情報を登録し、リネージュとして管理します。

履歴登録API

指定した履歴情報をリネージュとして登録し、管理します。

5.3.2 証跡・監査機能のリネージュ取得とは

リネージュ取得APIとは、履歴登録APIによって登録されたリネージュを、取得するためのAPIです。

リネージュ取得API

指定した履歴IDが所属しているリネージュを取得します。

5.3.3 証跡・監査機能の履歴検索とは

履歴登録APIで登録した履歴情報を検索するためのAPIです。

検索対象により、5つのAPIエンドポイントがあります。

履歴検索(検索対象:ヘッダー部)API

履歴のヘッダー部を対象に、検索方法を指定して履歴検索ができます。

履歴検索(検索対象:グローバルデータ部)API

履歴のグローバルデータ部を対象に、検索方法を指定して履歴検索ができます。

履歴検索(検索対象:ローカルデータ部、組織横断検索)API

履歴のローカルデータ部を対象に、検索方法を指定して、エージェント(組織)を横断した履歴検索ができます。

履歴検索(検索対象:ローカルデータ部、対象組織内検索)API

履歴のローカルデータ部を対象に、検索方法を指定して、指定したエージェント(組織)内に限定した履歴検索ができます。

履歴検索(検索対象:改ざん検証部)API

履歴の改ざん検証部を対象に、検索方法を指定して履歴検索ができます。

5.3.4 証跡・監査機能のローカルデータ削除とは

ローカルデータ削除APIとは、履歴登録APIで登録された履歴情報のうち、指定した履歴情報のローカルデータ部に含まれる情報を削除するためのAPIです。

ローカルデータ削除API

指定された履歴IDまたはローカルデータIDの履歴情報に含まれる、ローカルデータを削除します。

このとき、履歴登録時に改ざん検証部に追加されたローカルデータのハッシュ値は削除しません。

5.3.5 証跡・監査機能の参照ポリシー設定とは

参照ポリシー設定APIは、履歴情報ごとに、ローカルデータ部を参照するために必要な権限を設定するAPIです。

参照ポリシー設定APIには3つのエンドポイントがあります。

参照ポリシー設定(設定)API

指定したローカルデータIDに対して、組織(エージェント)名、ロール、ユーザーのどれかを指定して参照ポリシーを設定できます。

複数指定した場合はエラーとなります。

また、ユーザー情報非公開モード時に、ローカルデータ部に格納された履歴登録者情報に対して参照ポリシー設定を利用することで、直接データの取引がない組織(エージェント)であっても履歴登録者情報を公開できます。

参照ポリシー設定(削除)API

指定したローカルデータIDに対して、組織(エージェント)名、ロール、ユーザーのどれかを指定して参照ポリシーを削除できます。

参照ポリシー設定(一覧取得)API

指定したローカルデータIDに設定されている、参照ポリシーの一覧を取得します。

5.3.6 証跡・監査機能の改ざん検証とは

改ざん検証APIを利用することで、証跡監査機能により登録されたリネージュの改ざん検知や登録者の検証ができます。

改ざん検証API

指定したリネージュ全体または個別の履歴情報に対して、改ざん検証部を利用することで、改ざんの検知と登録者の検証ができます。

第6章 Data e-TRUSTでのトラストシール機能

Data e- TRUSTのトラストシール機能では、データの発行者やデータ自体の改ざんがされていないことを証明できる、トラストシールを利用します。

トラストシールは、証明機関が作成した証明書と証明対象のデータを元に作成します。

このトラストシールとセットでデータを取引することで、データ本体の真正性だけでなく、データを発行した組織・ユーザーが正しく存在することを担保できます。

6.1 Data e-TRUSTでのトラストシール機能を利用するための前提知識

Data e-TRUSTのトラストシール機能を利用する際に、以下の役割が登場します。

トラストシール機能利用時の役割

Data e-TRUSTでトラスト機能を利用する際の役割には、issuer、holder、creator、verifierの4つがあります。

issuer

issuerは証明書の作成者です。
ユーザー(個人)またはエージェント(組織)として、holderの真正性を証明するための証明書を作成します。

holder

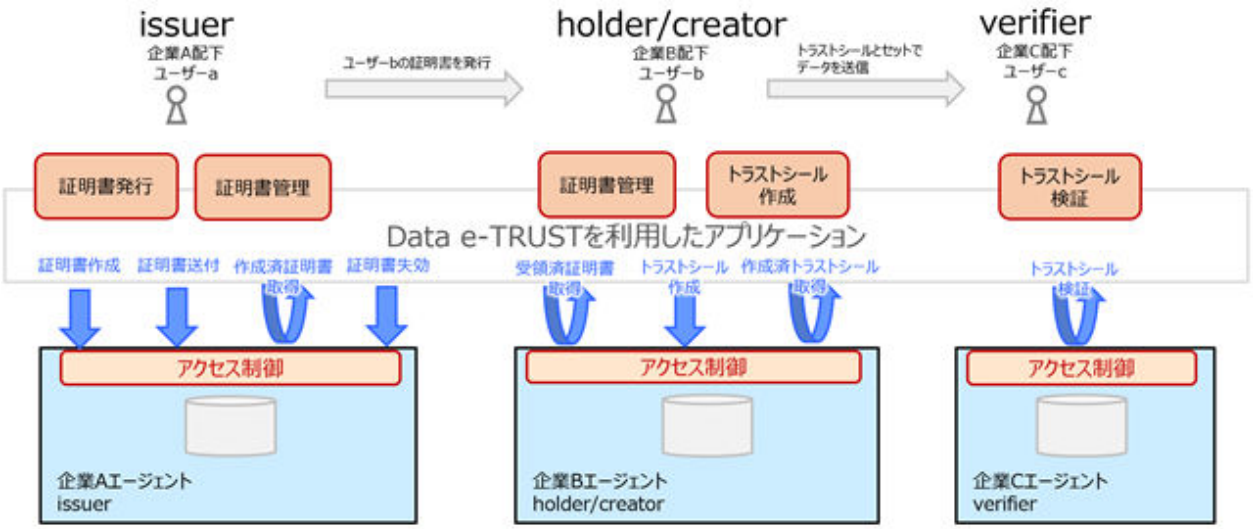
holderはissuerによって作成された証明書の受信者です。
ユーザー(個人)またはエージェント(組織)として、証明書を受け取ります。証明書は、holder自身をcreatorとしてトラストシールを作成する際に利用します。

creator

creatorはトラストシールの作成者です。
ユーザー(個人)またはエージェント(組織)として、証明書を利用してトラストシールを作成します。作成したトラストシールは、データとセットで送付されます。

verifier

verifierはトラストシールの検証者です。
ユーザー(個人)またはエージェント(組織)として、トラストシールの検証対象のデータに対し、トラストシールを作成したcreatorが正しいか、またデータ本体が改ざんされていないかを検証します。



トラストシール機能用ロールと、トラストシール利用時の役割、実行可能な操作の関係は以下の通りです。

役割	操作		トラストシール 管理ロール	ユーザー用 トラストシール 利用ロール	エージェント用 トラストシール 利用ロール
issuer	証明書発行	個人として発行 ・例：個人的に「この人はこれができる」ことを保証する場合などを想定	×	○	×
		組織として発行 ・例：学校が発行する成績証明書など	×	×	○
holder	証明書の参照	holderが個人の証明書	○	○ ただし本人の 証明書のみ	×
		holderが組織の証明書	○	○	○
creator	証明書を利用したトラストシールシールの作成	holderが個人の証明書	×	○ ただし本人の 証明書のみ	×
		holderが組織の証明書	×	×	○
verifier	トラストシール検証	個人をverifierとしたシール	○	○ ただし本人の トラストシールのみ	×
		組織をverifierとしたシール	○	×	○

6.2 Data e-TRUSTでのトラストシール機能利用の流れ

Data e-TRUSTでのトラストシール機能では、トラストシールを利用するための手順があります。

トラストシール機能を利用するときの、主な流れは次のようになります。
各操作の詳細や、その他の機能に関してはAPIリファレンスおよびAPIリファレンス:別冊を参照してください。

表6.1 証明書に関わる操作の流れ

手順	操作	説明
1	証明書の作成	issuerが証明対象のholderに対して、個人や組織を証明するための証明書を作成します。
2	証明書の参照権限を付与	作成した証明書の参照権限をholderに付与します。
3	証明書の管理	作成した証明書を管理します。

表6.2 トラストシールに関わる操作の流れ

手順	操作	説明
1	トラストシール作成	creatorが、作成済の証明書を利用してトラストシールを作成します。
2	トラストシールとセットでデータを送信	トラストシールとセットでデータをverifierに送信します。 ※トラストシールの機能外の操作です
3	トラストシールとセットでデータを受信	トラストシールとセットでデータを受信します。 ※トラストシールの機能外の操作です
4	トラストシールの検証	verifierは受信したデータとトラストシールを利用して、データの送信元および内容の真正性を検証します。
5	トラストシールの管理	作成したトラストシールを管理します。

6.2.1 トラストシール機能での証明書の作成方法とは

トラストシールを作成するために必要となる証明書を、証明書作成APIで作成します。

証明書作成API

issuerが証明書作成APIを実行することで、指定したholder用の証明書を作成します。

証明書作成APIによって作成された証明書は、作成時点ではholderに対する参照権限がないため、別途参照権限を付与する必要があります。

証明書作成書APIはissuerが実行します。

6.2.2 トラストシール機能での証明書の参照権限の付与方法とは

証明書送付APIによって、証明書作成APIで作成した証明書に対して、holderに参照権限を付与できます。

証明書送付API

被証明者のholderには、証明書作成APIで作成した証明書の参照権限がありません。そのため、証明書送付APIによって参照権限を付与します。

証明書送付APIはissuerが実行します。

6.2.3 トラストシール機能での証明書の管理とは

作成した証明書を管理するためのAPIとして、3つのAPIがあります。

証明書失効API

不要になった証明書を失効させます。

作成済証明書取得API

作成済の証明書の一覧を、指定した条件で取得できます。

受領済証明書取得API

証明書送付APIによってissuerから受領した証明書の一覧を、指定した条件で取得できます。

受領済み証明書取得APIはholderが実行します。

6.2.4 トラストシール機能でのトラストシールの作成とは

真正性を証明したいデータとセットで送付するためのトラストシールを、トラストシール作成APIによって作成します。

トラストシール作成API

証明書送付APIによって受領した証明書を利用して、creatorがトラストシールを作成します。

作成したトラストシールは、真正性を証明したいデータとセットでverifierへ送付します。

トラストシール作成APIはcreatorが実行します。

6.2.5 トラストシール機能でのトラストシールの検証とは

トラストシール検証APIによって、トラストシールの検証を実施します。

トラストシール検証API

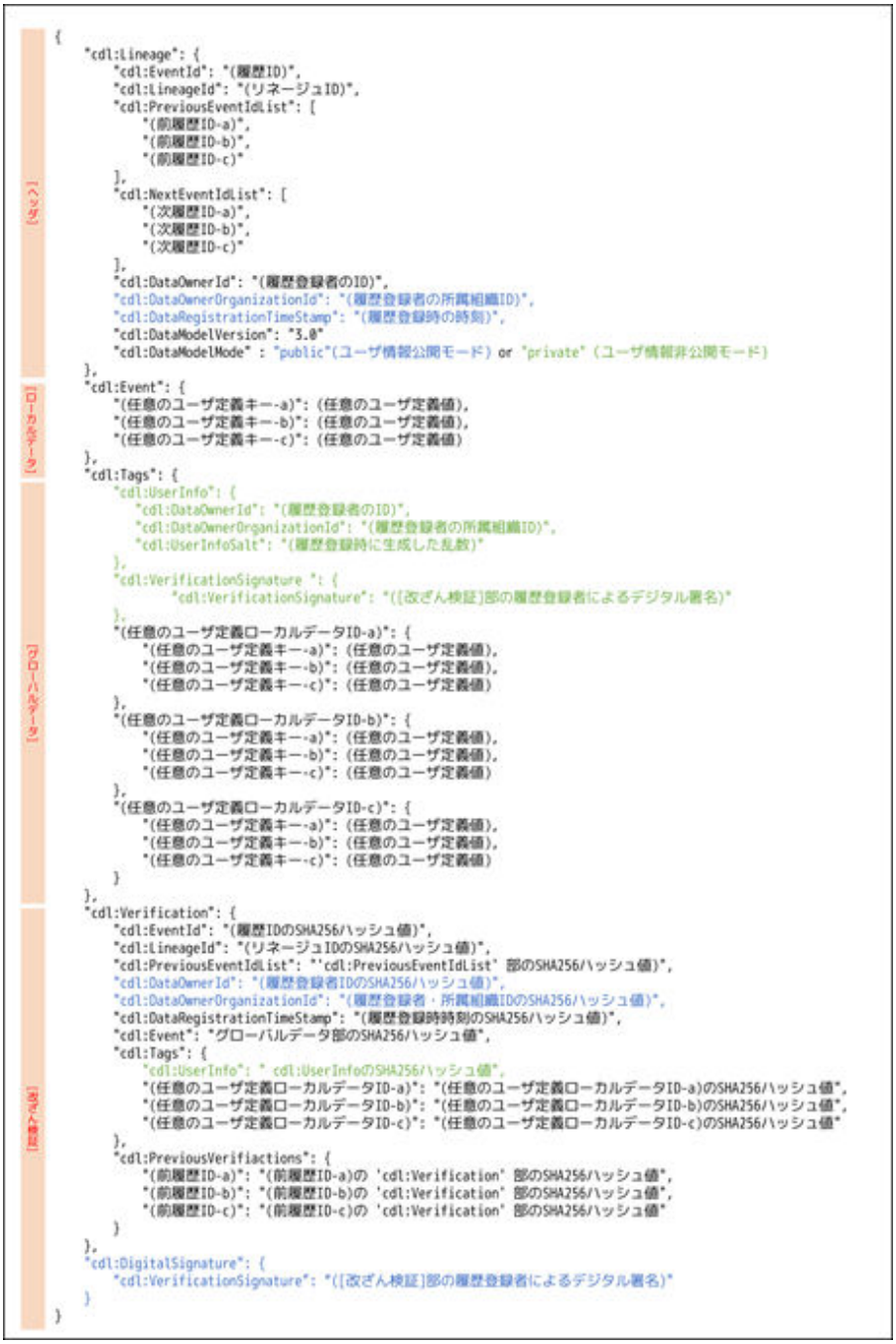
受領したデータとトラストシールを利用して、トラストシール作成に利用された証明書がcreator本人のものか、トラストシール本体が改ざんされていないかを検証します。

トラストシール検証APIはverifierが実行します。

付録A　証跡・監査機能のJSONフォーマット

履歴データのJSONフォーマット

証跡・監査機能を利用してAPIによりリネージュを取得した際に、返却される履歴データのJSONフォーマットです。



履歴データの構成要要素一覧

履歴データ 構成要素	キー名	型	必須	内容・備考
[ヘッダー]部	cdl:Lineage	オブジェクト	○	
履歴ID	cdl:EventId	文字列	○	個々の履歴を識別。履歴間で重複不可

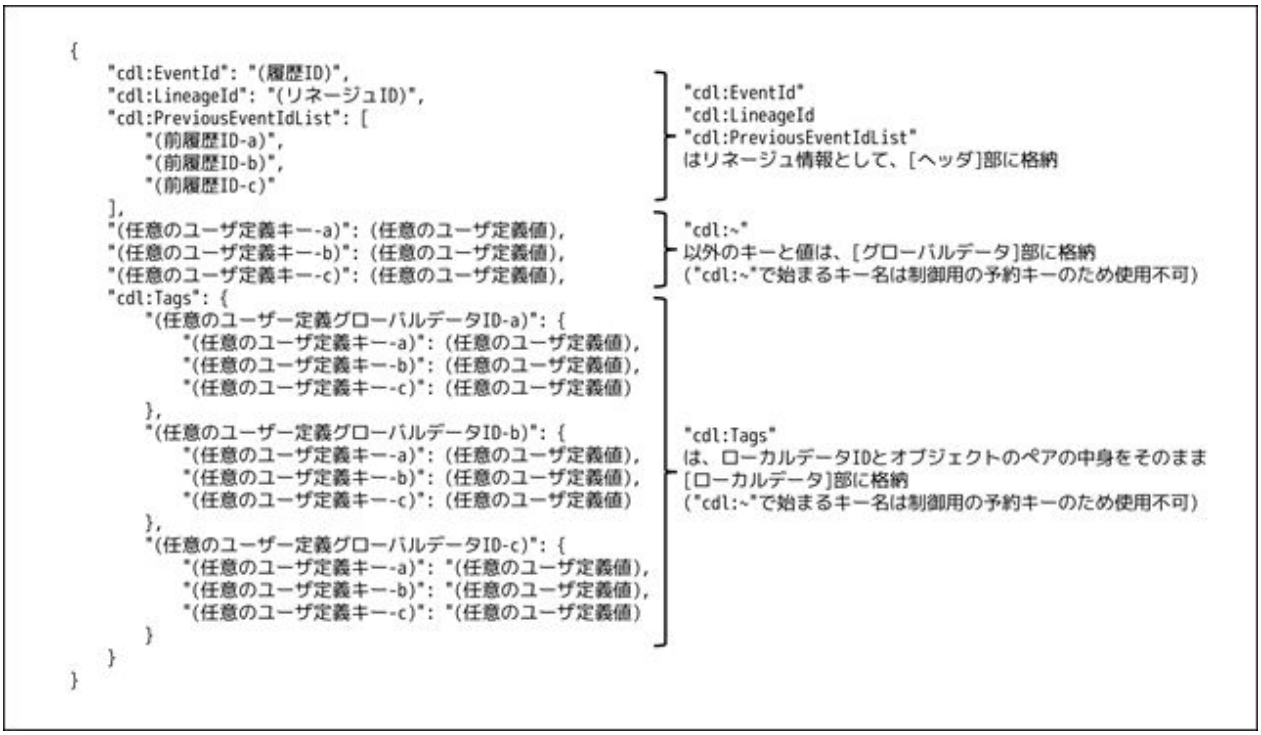
履歴データ 構成要素	キー名	型	必須	内容・備考
				省略時はUUIDを生成
リネージュID	**cdl:LineageId**	文字列	○	個々のリネージュを識別するための一意なID。 [省略時] 前履歴IDが指定されている場合→前履歴のリネージュIDを設定(つまり、前履歴のリネージュを引き継ぐ) 前履歴IDが未指定の場合(=リネージュ先頭時) → 履歴IDと同じID文字列を設定
前履歴ID群	**cdl:PreviousEventIdList**	配列	○	前履歴ID(文字列)のリスト。リネージュ先頭の履歴は空配列となる。また、複数の前履歴IDがある場合はリネージュの合流を表す。 履歴登録時に空配列が指定されている場合は、リネージュIDによるリネージュの自動連結機能により前履歴IDを抽出し設定される。
次履歴ID群	**cdl:NextEventIdList**	配列	○	次履歴ID(文字列)のリスト。リネージュ末端の履歴は空配列となる。また、複数の次履歴IDがある場合はリネージュの分岐を表す。本履歴の次履歴が追加されたときに、次履歴IDを追記
履歴登録者ID	**cdl:DataOwnerId**	文字列	-	履歴登録者のID ユーザー情報公開モードの場合のみ必須
履歴登録者所属組織ID	**cdl:DataOwnerOrganizationId**	文字列	-	履歴登録者の所属組織ID ユーザー情報公開モードの場合のみ必須
履歴登録時刻	**cdl:DataRegistrationTimeStamp**	文字列	○	履歴データ登録時の時刻
CDLデータモデルバージョン	**cdl:DataModelVersion**	文字列	○	3.0 (固定)
CDLデータモード	**cdl:DataModelMode**	文字列	○	public:(ユーザー情報公開モード) または private:(ユーザー情報非公開モード)
[グローバルデータ]部	**cdl:Event**	オブジェクト	-	グローバルデータ部のユーザー定義データがない場合は、キー自体存在しない
(ユーザー定義データ)	**任意のユーザー定義キー (ただし “cdl:” で始まらないこと)**	(任意のユーザー定義値)	-	ユーザーが自由に定義できる任意のkey-valueデータ
[ローカルデータ]部	cdl:Tags	オブジェクト	-	ローカルデータ部のユーザー定義データがない場合は、キー自体存在しない
ユーザー情報	cdl:UserInfo	オブジェクト	-	ユーザー情報 ユーザー情報非公開モードの場合のみ必須
履歴登録者のID	cdl:DataOwnerId	文字列	-	履歴登録者のID ユーザー情報非公開モードの場合のみ必須
履歴登録者の所属組織ID	cdl:DataOwnerOrganizationId	文字列	-	履歴登録者の所属組織ID ユーザー情報非公開モードの場合のみ必須

履歴データ 構成要素	キー名	型	必須	内容・備考
履歴登録時に生成した乱数	cdl:UserInfoSalt	文字列	-	ハッシュ値からのユーザー情報特定防止目的の乱数。 ユーザー情報非公開モードの場合のみ必須
[改ざん検証]部デジタル署名	cdl:VerificationSignature	オブジェクト	-	
[改ざん検証]部の履歴登録者によるデジタル署名	cdl:VerificationSignature	文字列	-	[改ざん検証]部のSHA256ハッシュ値の履歴登録者によるデジタル署名 ユーザー情報非公開モードの場合のみ必須
ローカルデータID群	任意のユーザー定義キーを、ローカルデータIDとして識別 (ただし “cdl:” で始まらないこと)	オブジェクト	-	ユーザーが自由に定義できる、「任意のローカルデータID-オブジェクト」ペア 他履歴のローカルデータIDと重複してもよいが、別のローカルデータとして扱う (履歴ID+ローカルデータIDで一意)
[改ざん検証]部	cdl:Verification	オブジェクト	○	
[改ざん検証]部デジタル署名	cdl:VerificationSignature	文字列	-	[改ざん検証]部のSHA256ハッシュ値の履歴登録者によるデジタル署名
リネージュID改ざん検証	cdl:LineageId	文字列	○	[ヘッダー]部「リネージュID」のSHA256ハッシュ値
前履歴ID群改ざん検証	cdl:PreviousEventIdList	文字列	○	[ヘッダー]部「前履歴ID群」のSHA256ハッシュ値
履歴登録者ID改ざん検証	cdl:DataOwnerId	文字列	○	[ヘッダー]部「履歴登録者ID」のSHA256ハッシュ値
履歴登録者所属組織ID改ざん検証	cdl:DataOwnerOrganizationId	文字列	○	[ヘッダー]部「履歴登録者所属組織ID」のSHA256ハッシュ値
履歴登録時刻改ざん検証	cdl:DataRegistrationTimeStamp	文字列	○	[ヘッダー]部「履歴登録時刻」のSHA256ハッシュ値
[グローバルデータ]部改ざん検証	cdl:Event	文字列	-	[グローバルデータ]部のSHA256ハッシュ値
[ローカルデータ]部改ざん検証	cdl:Tags	オブジェクト	-	キー「[ローカルデータ]部のローカルデータID」 文字列「そのローカルデータのSHA256ハッシュ値」 のペアを保持するオブジェクト
前履歴[改ざん検証]部改ざん検証	cdl:PreviousVerifiactions	オブジェクト	○	キー「前履歴の履歴ID」 文字列「その前履歴の[改ざん検証]部のSHA256ハッシュ値」 のペアを保持するオブジェクト
[デジタル署名]部	cdl:DigitalSignature	オブジェクト	-	ユーザー情報公開モードの場合のみ必須
[改ざん検証]部デジタル署名	cdl:VerificationSignature	文字列	-	[改ざん検証]部のSHA256ハッシュ値の履歴登録者によるデジタル署名
リネージュ終端デジタル署名	cdl:LineageTerminationDigitalSignature	文字列	-	リネージュ末端の履歴にのみ存在。[改ざん検証]部のSHA256ハッシュ値とCDLからリネージュを取り出した時刻をJWS(RFC7515)でデジタル署名した文字列。

履歴登録時のJSONフォーマット

履歴登録時に利用するJSONフォーマットです。

履歴情報のJSONフォーマットでは、同一の内容が複数箇所に記載されているなど煩雑なため、履歴登録のAPIリクエストには簡易化したバージョンのフォーマットを利用します。



履歴登録時のJSONフォーマット構成要素一覧

履歴登録時JSONフォーマット構成要素	キー名	型	内容	指定省略時の動作
履歴ID	cdl:EventId	文字列	個々の履歴を識別する履歴ID。履歴間で重複不可	自動でUUIDを生成・設定する
リネージュID	cdl:LineageId	文字列	個々のリネージュを識別するリネージュID。リネージュ自動連結機能で用いるID	前履歴ID群に前履歴IDが指定されている場合: → 前履歴のリネージュIDを設定(つまり、前履歴のリネージュIDを引き継ぐ) 前履歴ID群に前履歴IDが未指定の場合(=リネージュ先頭時): → 履歴IDと同じ文字列を設定
前履歴ID群	cdl:PreviousEventIdList	配列	当履歴の前履歴を表す、前履歴ID(文字列)のリスト 当履歴がリネージュの先頭の場合は、空配列となる また、複数の前履歴ID指定時は、当履歴でリネージュが合流していることを表す	当キー自体が省略されている場合は、リネージュIDによるリネージュの自動連結機能により、前履歴IDを自動抽出し設定する。

履歴登録時 JSONフォーマット 構成要素	キー名	型	内容	指定省略時の動作
ローカルデータ	任意のユーザー定義キー (ただし“cdl:”で始まらないこと)	任意のユーザー定義値 (任意の型)	ユーザーが自由に定義できる任意のkey-valueデータ 履歴データの[ローカルデータ]部に格納され、全参加組織に共有同期される(アクセス制御不可)	ユーザー定義データがない場合は、履歴データの[グローバルデータ]部を表すキー“cdl:Event”自体が存在しない
ローカルデータ	cdl:Tags (ただし“cdl:”で始まらないこと)	オブジェクト	オブジェクトの中身に、ユーザーが自由に定義できる、「(任意のローカルデータID)-(JSONオブジェクト)」のペアでローカルデータを指定 履歴データの[ローカルデータ]部に格納され、参照時にアクセス制御で保護・隠蔽される ローカルデータIDは他履歴のローカルデータIDと重複してもよいが、別のローカルデータとして扱う(履歴ID+ローカルデータIDで一意)	ローカルデータの指定がない場合は、履歴データの[ローカルデータ]部を表すキー“cdl:Tags”自体が存在しない

付録B　サービスの提供タイプ一覧

Data e-TRUSTのサービス提供タイプは以下のとおりです。

表B.1 品名別諸元

品名		企業ID数の上限	ストレージ容量	ユーザー数
スタンダードモデル	20,000ユーザーモデル	100	256GB	～20,000
	100,000ユーザーモデル		512GB	～100,000
	300,000ユーザーモデル		4TB	～300,000
	1,000,000ユーザーモデル		16TB	～1,000,000
開発実証モデル		100	50GB	～100

企業ID数の上限は、オプションの企業ID追加により最大5000まで拡張可能です。