Computer Security Symposium 2020
26 - 29 October 2020

ワークフロー型の電子署名によるトラスト管理手法の提案

小栗 秀暢[1] 小嶋 陸大[1] 中村 洋介[1] 角田 忠信[1]
矢崎 孝一[1] 山本 大[1] 伊藤 孝一[1] 二村 和明[1]

概要：インターネット上でのデータ流通が活発化する一方で，文書データの改ざんやなりすましによる詐欺被害が増加している．それに対抗するため，公開鍵暗号を活用してデータの真正性を保証する電子署名技術が広く用いられている．電子署名は，作成したファイルが改ざんされていないことを電子的に保証することで「データ的なトラスト」を保証するが，実際のビジネスの現場では，データ以外の要素である，人・組織・企業などの「社会的なトラスト」を組み合わせて用いられている．近年では，複数の電子署名を組み合わせるワークフロー型の署名によって，社会的なトラストを保持する技術が提案されているが，ワークフロー型の署名でも，社会で利用されている多様なトラストを表現することはできない．加えて，個別の署名が持つ詳細なトラスト情報を喪失する場合もある．本稿では，電子署名の検証用の鍵を保持するトラストサービスの役割に着目して，複数トラスト要件の達成情報をベクトル化し，鍵管理 DB を拡張して保存することで，データに関する多様なトラスト計測を可能とする管理手法を提案する．その上で，ワークフロー型署名のグラフ構造を利用し，トラスト値を要件に合わせてトップダウン型，又はボトムアップ型に変更することで，現実的な利用に即した多様なトラストの検証効率を高める手法を検討した．これらの技術によって，トラストサービスを仲介としてデータ的なトラストだけでなく，多様なトラスト情報の交換・流通を可能とする．

キーワード：電子署名，トラストサービス，ワークフロー型署名

Proposal of Trust Value Management Method using Workflow e-signature

Hidenobu Oguri[1] Rikuhiro Kojima[1] Yousuke Nakamura[1] Tadanobu Tsunoda[1]
Kouichi Yasaki[1] Dai Yamamoto[1] Kouichi Ito[1] Kazuaki Nimura[1]

Abstract: While business data distribution on the internet has become active, fraud damage due to falsification and spoofing of data is increasing. To solve this problem, e-signature technology that applies public key cryptography to guarantee the authenticity of electronic data is widely used. The e-signature provides "Data Trust" by cryptographically guaranteeing that the created file has not been modified. However, in business scenes, "Social Trust" of people, organizations, companies, etc., is used in combination. Therefore, in recent years, there has been proposed a technique for maintaining Social Trust by using a workflow e-signature in which a plurality of e-signatures is combined. Even with workflow e-signatures, it is not possible to express the various trusts used in society, and in some cases, the information related to the detailed trust of each signatures may be lost. In this paper, we focus on the role of “Trust Service” that manages the key for verifying the e-signature, vectorize the achievement information of multiple trust requirements, and expand and store the key management database to measure various type of trusts. Furthermore, we proposed the method that can manage various trusts using the graph relationship of workflow e-signatures and modifying the trust value as top-down type and bottom-up type. These technologies enable not only Data Trust but also exchange and distribution of various trust information via trust services.

Keywords: e-signature, trust service, Workflow e-signature

1. はじめに

現代社会では，インターネット上での電子データ流通が活発化する一方で，電子データの改ざんやなりすましによる詐欺被害が増加している．それに対抗するため，公開鍵暗号を活用して電子データの真正性を保証する電子署名技術が広く用いられている．

電子署名は暗号技術によって「ファイルの真正性」を保証するというトラストを提供する．その基本的な方式は，正当性を保証したいファイルの本体，またはそのハッシュ値を秘密鍵で暗号化し，その際に生成された公開鍵を電子証明書とするのが一般的である．

しかし，電子署名の技術は，それ単体でトラストを保証できるものではなく，実際には署名を発行する前後の技術，即ち個人認証技術や認証局，暗号アルゴリズムなど，多様な技術と組み合わせて初めて機能する．それら技術の組み合わせには無数の選択肢があるため，欧州 eIDAS 規則[1,2]や，米国 SP800-63 [3] 等の安全性基準に沿った電子署名を提供するサービス，所謂トラストサービスを利用するのが一般的である．

しかし，トラストサービス単位で見た場合でも，実際に作成される電子署名は，多様な形態で運営されている．そのため，トラストサービス同士の電子署名に対する技術レベルやトラストへの考え方・ポリシー等を交換することが難しく，インターオペラビリティやサービスとしての利用性が問題となっている．

1 富士通研究所
FUJITSU LABORATORIES LTD.

また一方で，ビジネスの現場では，電子署名を用いたトラストだけでは対応できない性質のトラストの利用も増加している．特にグローバルに展開するビジネスでは，電子データの真正性だけでなく取引企業の収益状況や組織構造，個人の肩書と事業上の権限範囲など，他の多様なトラスト情報を組み合わせ，事業取引のリスクと対照し，ビジネスを推進する行為が一般的である．

同じトラストの名を冠しながら，電子署名によるファイル真正性のトラストと，企業や組織構造から得られるトラストとでは，その性質が大きく異なる．しかし．これら一連のトラストは，ビジネス上の取引を安全・円滑にするという役割は同じである．このような性質の異なるトラスト情報を，ビジネス上の判断に活用できるように一律に管理する仕組みが求められている．

そこで本稿では，多様なトラスト種類をベクトル化して管理する手法を提案し，複数の電子データにまたがった文書のトラストを管理する方式を提案する．また，電子署名の構造に応じて，複数のトラストの値を実際のビジネスで用いられるトラスト利用状況に近づけるよう修正する方式について検討する．

本稿の構成は以下のとおり．２章で背景と従来技術の説明，３章でユースケースの提示，４章でトラストの管理手法の提案，５章でトラスト値の修正方法を検討し，６章で全体をまとめる．

2. 背景・従来技術

2.1 電子署名の安全性基準の多様性

まず，電子署名技術のトラストを確保するための技術として，大きく２つの要素がある．まず認証技術により人・モノ・サービス等の真正性を確保すること，もう一つは公開鍵暗号技術を用いてデータの真正性を確保することである．この両方が満たされることで，ある正当な個人が正当な電子データを生成したことを証明する，データの真正性としてのトラストを提供することができる．

半面，これらの技術は多様に存在し，国や企業，業種業態によって採用する安全性基準やフォーマットが異なることから，統一された安全性基準が存在しない．

例えば日本の電子署名法[4]では第 3 条で「本人による電子署名」であることを署名の真正性を推定する要件としている．その際に同法の施行規則[5] 第 6 条にて署名鍵を本人に安全かつ確実に渡すことを定めているが，署名者の鍵管理状態や，署名鍵の利用時の技術的要件の詳細を定めているものではない．

行政書類の中でも政府認証基盤（GPKI）など，電子認証・電子署名等を用いて申請が可能なものも複数存在するが，それぞれ安全性基準が定められており，事業者は自社の方式がそれに対応できるかを検討するコストが必要となる．

一方，欧州におけるトラストサービスの統一基準を定めた法的規則 eIDAS [1,2]では，安全性に関する基準が多く制定されている．例えば電子署名についても，高度電子署名や適格電子署名などの技術的な基準が定められており，適格電子署名は手書きの署名と同等の法的有効性を持つことを，EU 各国が相互に認定している．また，欧州独自の方式である e シールは，ある電子データがその企業の保持するシステムから生成されたことを示す特殊な電子署名である．e シールの中でも適格基準を満たした Advanced e シールや Qualified e シール等が区分されており，現実的にその制度のない他の国や地域では，それらの安全性基準をどのように用いるかは定まっていない．

また，米国では NIST が作成した電子認証に関するガイドライン SP800-63[3]において，電子署名のような繰り返し利用されるサービスにおいて，個人の認証方式がハックされ，なりすましや悪用が発生するリスクをまとめ，技術要件として AAL (Authenticator Assurance Level）等の安全基準をまとめている．３段階にまとめられている AAL は，攻撃者が政府機関のシステムにアクセスした場合を想定し，各機関による被害想定に基づいて場合分けした技術セットである．大まかに分類すると，AAL1 は単要素での認証，AAL2 は 2 要素以上での認証，AAL3 は 2 要素認証の内 1 つはハードウェア認証を利用することを求めている．

2.2 トラストサービスの多様性

個人認証や電子署名の要件が国ごとに異なるのに加え，現状のトラストサービスは，立会人型と当事者型，リモート署名による鍵管理型など，複数の方式によってサービス展開されており，それぞれの技術の問題点などが明確に整理されていない．

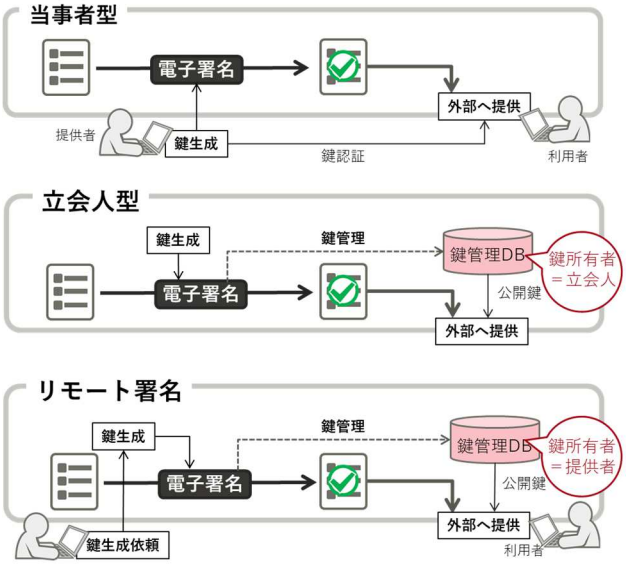


図１　トラストサービスの方式の違い

トラストサービスの方式の違いを図１に示す．当事者型とは，電子署名を付与するユーザ（提供者）自身が電子署

名の鍵を生成・管理して電子データに署名を付与する方式である．多くの電子署名の方式はこれを想定しているが，一般ユーザが多数の鍵を管理し，また検証者の求めに応じて対応する鍵を提供することが困難なため，利用性の向上が課題となっている．

それに対して立会人型とは，契約に関する第三者（例えば弁護士やサービス事業者）がデータの内容を確認し，第三者が鍵を生成･管理して電子署名を発行する方式である．この方式は技術的な手間の多い鍵の生成・管理と鍵検証を専門サービス事業者が仲介することから利用性に優れるが，署名者が本人でないため，あくまでもトラストサービス側が不正をしないという前提条件を持った上での信頼によって成り立っている．また，トラストサービスにログイン等を行う必要があるため，パスワードのハッキング等によって偽の書類を発行される等の可能性も指摘されている．

そこで近年では，リモート署名による鍵管理が提案されている．これは，鍵生成の一部の機能をクラウド型のサービスを用いて代行することで，安全性と利便性を高める仕組みである．これによって提供者自身が鍵を保持することとなり．安全性が増している，しかし，この場合においても，署名鍵を保存するクラウドストレージの運営会社は鍵を盗み取ることが可能であり，完全に安全性を保証することは困難である．

2.3 電子署名で用いる暗号技術

電子署名の方式の多様さに加え，電子署名で用いる暗号技術についても多様な方式が提案されている．電子署名では多くの場合に公開鍵暗号方式として RSA, ハッシュ関数として SHA-256 等を用いているが，明確な定めは無い．日本では電子署名法のガイドラインにおいて RSA，DSA，ECDSA の 3 方式を指定しているが，これ以外の署名方式を用いた場合でも電子署名を発行することは可能である．その場合，利用者にはその暗号的強度まで伝達されないことから，暗号の脆弱性を利用したなりすましや悪用をされる可能性がある．

その一方で，これらの暗号方式を更に改良し，多様な安全性を満たす，新しい電子署名の提案もされている．

例えば Lim らは，電子署名の中にワークフローの正当性を交えて署名することで，電子データの真正性だけでなく，その認証に関わった組織内での認証手順の安全性を検証する電子署名[6]を提案している．また，Kumar らは 1 つのドキュメントに対して，定義したワークフローに沿って電子署名を順番に付与することで電子署名の組織としての真正性を確保する方式[7]を提案している．これら新たな暗号技術は暗号としての強度やユースケースによって発生する脆弱性などが十分に検討，評価されていない．

他にもワークフローではないが，複数人での署名の方式の一つとして，徳永らは１つの電子データに含まれる複数のレイヤー構造で定義された内容について，それぞれのレイヤーデータの真正性と，その順番について検証が可能な方式を提案している[8].

これら新しい方式を用いた電子署名技術により，今まで電子データの真正性しか保証できなかった状態から，それ以外の要素，例えば組織や組み合わせといった社会的な要素を保証することが可能となった．今後，様々なトラスト要素を表現できる電子署名技術が増加すると考えられる．

しかし，これら新しい暗号方式を利用する場合にも，その暗号の強度や利用方法，及び個人認証を行った形態などと組み合わせて採用を検討する必要があり，トラストサービス全体の構成を含めた安全性を実現する必要がある．

このような，電子署名の技術の多様性が進む一方で，ビジネスの現場で用いられるトラストの種類は，技術以上に多様に存在している．ビジネスにおけるトラストの種類とは，国家・業種・業態以上に細分化されており，極端に言えば利用する企業や担当者ごとに重視するトラストが異なる．このような技術や社会の状況に応じて多様に存在するトラスト基準を一律に管理する手法が求められている．

そこで本稿では，利用する企業ごとにトラストの基準が異なる状態を前提として，多様なトラスト形態をトラストサービスが管理するための手法を提案する．その上で，ワークフローを検証することが出来る電子署名において，定義されたトラストの値を実際のビジネスの状況に応じて修正する仕組みについて検討する．

3. 準備・ユースケース

3.1 用語定義

まず前提として，電子署名技術を拡張して，電子データだけでなく，複数人による承認作業，所謂ワークフローの真正性を表現することが出来る電子署名技術が存在するものとする．本稿では特定の技術を指定せず，総称して**ワークフロー型署名**とする．

また，業務で利用するトラストを大きく二種類と定義する．まず，電子署名や個人認証技術によって得られる，データの真正性を保証するトラストを**「データ的トラスト」**，それ以外に，ビジネスリスク等を検証するための，組織や人に関する周辺情報によって得られるトラストを**「社会的トラスト」**と呼び，区別する．

実際のビジネスでは，トラストサービスで真正性を保証された,データ的トラストのある電子データを取得した後，その中身を社会的トラストと対照して，ビジネスリスクを判定するのが一般的である．

3.2 ユースケース

そこで，本稿でのユースケースを以下のように定義する．ある電子データを作成するＸ社には，ユーザ A，B，C の３人が存在し，それぞれが異なる署名技術を用いている．特

にCが利用している技術は，社内でも不適格となる不正な証明書を用いた電子署名，即ちデータ的なトラストが無い状態である．

その３名が共同して，ある経費請求書を作成する．Aが全体の請求書を作成し，その明細としてBとCが書類を提出した．その際にCが提出した書類は企業名の記載が無い，品目欄が抽象的であるなど，即ち社会的なトラストが無い書類であった．これらの書類に対して，それぞれの担当者が電子署名を付与し，最後にそのワークフローを証明するためのワークフロー型署名を付与して提出する．

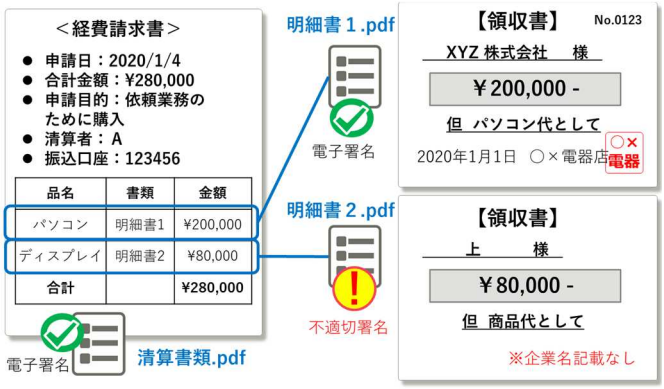
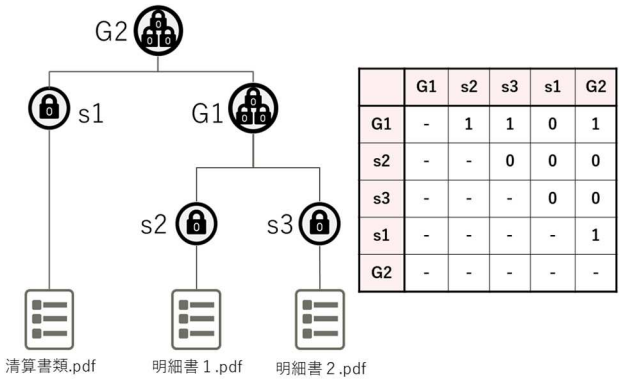


図２　使用する書類の関係性



	G1	s2	s3	s1	G2
G1	-	1	1	0	1
s2	-	-	0	0	0
s3	-	-	-	0	0
s1	-	-	-	-	1
G2	-	-	-	-	-

図３　使用する書類の関係性グラフによる管理例

ワークフロー型署名では，複数の書類の関係性をグラフ構造で表示することが可能となる．例えば図２で示した書類群は図３のようなグラフ構造や分散共分散行列を示して検証を行う仕組みを内包しているものとする．

明細書１，２に付与された電子署名 s_2，s_3 の組み合わせを証明するワークフロー型署名 G_1 を付与した後，G_1 と経費請求書に付与された電子署名 s_1 を統合した G_2 によって，書類同士の関係性を定義する．これによって，s_1，s_2，s_3 を生成した個人の組織上の定義情報を知っている場合，このワークフロー型署名が正常な業務の中で生成されたことが検証可能となる．

3.3　トラストサービスとの関係性

今回のユースケースでは，このワークフロー型署名を生成するためのトラストサービスを図４のように定義する．X社に所属するA,B,Cは，アプリケーションを利用して電子データ(f_1,f_2,f_3)のハッシュ値をトラストサービス T に送付し，電子署名(s_1,s_2,s_3) 及び，その構造を示すためのワークフロー型署名(G_1,G_2)を生成する，（※図中では s と G を総称して s_n としている）．トラストサービスはそれらに対応する Pkey 群を PkeyDB に格納する．最終的に生成された G_2 を最終的なワークフロー署名 S とし，データ f_1,f_2,f_3 に付与してY社に送付する．Y 社は，T に対して電子データ(f_1,f_2,f_3)のハッシュ値とワークフロー署名 S を送付することで，その署名の結果を得る．この流れによってY社では，電子データの真正性（データ的トラスト）と，その電子データの文面の真正性（社会的トラスト）を検証し，ビジネスリスクと対照することで業務を進める．

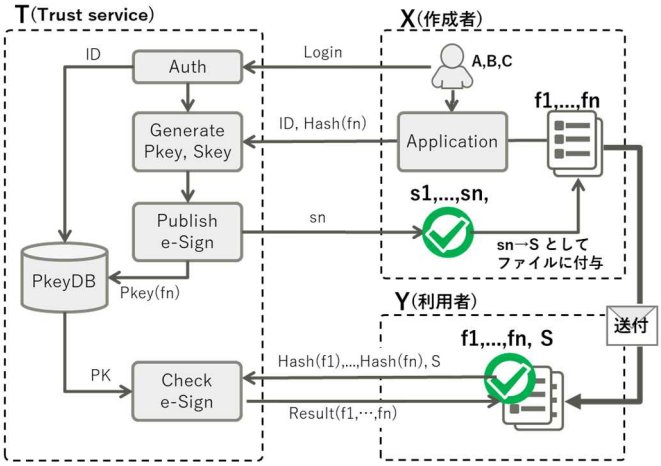


図４　プレイヤーの関係図

この状況の課題は２点ある．まず，本ユースケースでは，ユーザCが作成した書類は，データ的にも社会的にも不完全なものである．しかし，電子署名の強度要件は，その証明書内に保持されないことから，Y社はCの作成した書類の真正性が保証されていない（データ的トラストが無い）ことを検証できない．

もう一つは検証作業の順番の課題である．電子データをヒエラルキー構造の上部から確認していくとき，ユーザCの書類の検証は最後になる．今までの書類を全て検証した後に，会社名が記載されていない（社会的トラストの不足）ことを発見したことで，今までの書類検証が信頼に足るものではないことが判明し，却下する．その上で，再度，誰の責任の元でトラストを与えたのか等を調べ，ユーザ A,C に調査を依頼するなど，業務の手戻りが発生する．

次章では本ユースケースを用いて，トラストサービスを介して多様なトラストを管理する手法について提案する．

4. トラスト管理方式の提案

前章までの議論のとおり，ビジネスで利用するトラストはデータ的・社会的共に多様に存在しており，業種・業態や個人の考え方などでも変化するため，明確に定義することが困難である．しかし，そのような個別のトラスト定義や判断基準を多く集めることで，使用されている全てのトラストをベクトルとして表現することが可能となる．

4.1 トラストベクトルの生成

表 1 にその例を示す．例えば，データ的トラストにおいて，ある会社は AAL1（SP800-63 における認証強度，単要素認証）では，トラストが担保できない＝リスクが高いためビジネスしてはいけない，とするポリシーがあったとする．その場合，トラスト種類 t_1 を設定し，AAL1 のデータに対してはポリシー違反ということで 0 を設定し，それ以外を 1 に設定する，

同様に社会的なトラストを記述することもできる，例えば，トラストサービス内に保持する企業 DB に含まれている企業からの書類しか対応しない，という会社の方針がある場合を考える．その企業 DB に含まれる，という条件を t_2 として，含まれていない場合を 0，それ以外を 1 にすることでトラスト値を表現する．

No.	属性値			値1	値2	値3	...
t1	データ的トラスト	認証方式 SP800-63	しきい値	0	1	1	...
			基準	AAL1	AAL2	AAL3	...
t2	社会的トラスト	企業DBに含まれるか	しきい値	0	1	-	...
			基準	登録なし	登録あり	-	...
t3	社会的トラスト	署名者	しきい値	0	1	1	...
			基準	立会人型	クラウド型	自署	...
...		...	...	...	...	...	...

表 1　トラストのベクトル化を行うための基準例

トラストサービスに登録する各社が，自由なトラストの判断基準をトラストサービスに申請し，判定可能なトラスト基準を登録することで，その企業が重視するトラスト基準のリストが作成される．

これにより，ある電子署名と電子データに付与されているデータ的・社会的トラストをトラストベクトル $T = (t_1,t_2,\ldots,t_n)$, $t_n = (0,1]$として表現することが可能となる．ベクトルの大きさはトラストの要件をどこまで満たしているのかであるため，$1/n * \Sigma(t_n)$ とすることで数値としても比較できる．

4.2 トラストベクトルとワークフロー型署名の連携

このトラストベクトル T を，複数の電子署名を利用するワークフロー型署名に適用することで，それぞれの電子署名が持つトラストレベルを記録できる．トラストサービスには，電子署名ごとに保持するべき鍵のデータベースが存在するため，そのデータベースを拡張してトラストベクトルを保存し，各署名の有効性を検証する際に同時にトラストを検証する仕組みを構築する．

表 2 にその例を示す．電子署名 s_3 に紐づくデータは，企業名が記載されておらず（$t_2=0$），かつ，トラストサービスのログイン時に異なる手法で作成した（$t_1=0$）と判定されるため，その値が記載されている．これにより，本電子署名の署名鍵を読みだす際に，データ的・社会的トラストに関わらず，どの項目のトラストが満たされた上で，電子署名が付与されたのかを追加情報として利用することができる．また，これらは一つのワークフロー署名下で同一のトラスト項目を利用しているため，各署名鍵の T の総合値を利用することで，相対的にトラストの量が少ない電子署名とその紐づけられた電子データを特定できる．

				トラスト記録のための拡張領域			
署名 ID	電子データ	認証鍵	作成日	t1	t2	t3	T
				データ的	社会的	社会的	総合
				認証方式	企業 DB	署名者	Σ(tn) /n
G1		ABC1	2020/1/1	1	1	1	1
s2	明細書1.pdf	DEF2	2020/1/2	1	1	1	1
s3	明細書2.pdf	GHI3	2020/1/3	0	0	1	0.33
s1	清算書類.pdf	JKL4	2020/1/4	1	1	1	1
G2		MNO5	2020/1/5	1	1	1	1

表 2　署名鍵保存 DB を拡張した例

4.3 トラストベクトルと企業 DB の連携

トラストベクトルは電子署名の安全基準管理だけではなく，それを利用する企業に関するトラストのポリシー管理にも利用可能である．

企業がトラストサービスに登録する際に技術要件や重視する情報などを登録することで，付与された電子署名のトラストベクトルとの乖離による不正検知や，類似しているトラストベクトルを持つ企業同士のマッチングなどの応用が考えられる．

図 5 は複数のトラストサービスに属している複数の企業群のトラスト要件を収集して集合化し，属性のデータベースに変換する例である，これによって，企業同士のトラスト要件の類似性を求めることが可能である．

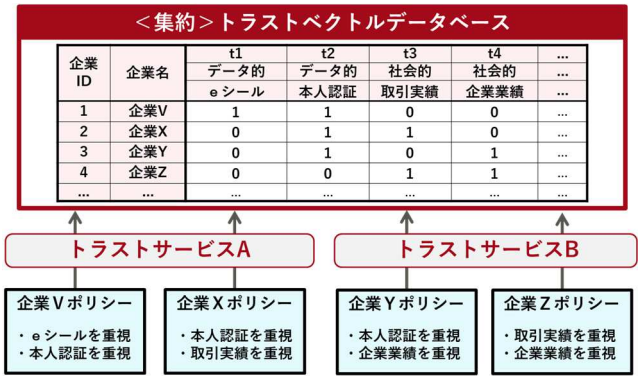


図 5　複数企業によるトラストベクトル DB 作成の例

このようにトラストサービスをプラットフォームとして展開する場合，複数の企業が持つトラストポリシー要件の集合を作成し，要件を抽象化した大きなトラストベクトルを設計することによって，より詳細なトラスト管理が可能となる．

企業 DB のトラストベクトルと電子署名のトラストベクトルを組み合わせることで，今まで利用されてこなかった多様なトラスト値を一律の基準で扱うことが可能となり，ビジネス上で電子データを検証するユーザの手戻りや誤認が少なくなると期待できる．

しかし，実際のビジネス慣習を考えた場合，トラストベクトルの値をそのまま表示するだけではトラストの考え方として合致しない点が多く出てくる．

本稿ではその中から，複数の人間によって，異なるトラストを与えられた場合に発生する課題について検討を行った．次章では，実際のトラストの利用シーンに基づいた課題を検討し，本管理手法を活用して解決する手法について述べる．

5. トラスト値修正方式の検討

5.1 トラスト検証の順番と手戻りの発生

まず，実際のビジネスシーンとして複数の電子データと電子署名を組み合わせて提供された場合の検証の順番について検討する．

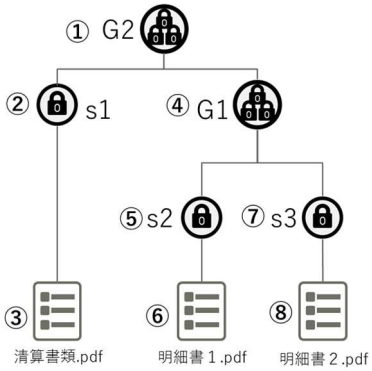


図 6　一般的なトラスト検証の順番の例

図 6 はユースケースに即した検証順番の例である．通常の検証は，より上位の書類から行うため，まず①全体の電子署名 G_2 と②清算書類の電子署名 s_1 のデータ的トラスト＝暗号上の不備がないかを確認する．その後に③清算書類の社会的トラスト＝書類上の不備を検証する．

そこまでの内容に不備がない場合に検証を先に進め，④添付されている明細書の全体の電子署名 G_1 のデータ的トラスト，⑤個別の明細書の電子署名．⑥その内容，の順番に検証していく．今回のユースケースの中で最も問題が多い明細書２のデータの検証は⑦，⑧と，ほぼ最後の順番で行われる．

このように，検証するドキュメントが増加する場合，より詳細を示すドキュメントほど，調査順番が後ろになる傾向があるが，直感的には詳細なデータであるほど，細かい記載上の問題などが増加し，チェックするべき項目が増えると考えられる．

このような，検証するべき順番と，トラストの不一致が発生したとき，検証者は内容の読み込みやデータ同士の対照を行い，問い合わせや修正依頼を行うなど，所謂「手戻り」となって業務効率が下がる．

このような手戻りを減少させるためには，あらかじめ上位の電子署名を検証する際に，下位のデータ的トラストと社会的トラストの両方の値が反映されていることが有効である．G_2 の電子署名を見ただけで社会的トラストが足りない，などの要件が判明することで，検証者はそのトラストが足りない部分の検証を優先して進めることができ，手戻りが減少する．

5.2 トップダウン型のトラスト修正

実際のビジネスシーンとしてありうるパターンとして，対外的なトラスト（ここでは過去の実績や会社の規模などを指す）が少ない子会社の作成物を集約し，トラストの大きな親会社が全体のチェックを行った上で，提出物全体の真正性を保証して，書類群を提出するケースがある．

このような状況は，複数のトラストサービスを併用する場合でも発生する．例えば，立会人型で電子署名を付与した電子データを複数集めた後に，ワークフロー型署名によって，当事者型の署名に付け替えるケースが考えられる．

このような，最後に電子署名を付与したユーザの社会的トラストによって，ヒエラルキー下位に存在する電子署名の社会的トラストを上書きするケースが多く存在するため，それを表現する手段が必要である．

そこで，ワークフロー型署名によって，より上位のヒエラルキーによって定義された社会的トラスト値を，下位の社会的トラストに適用する，所謂トップダウン型のトラスト値変換を行うことで，実際のビジネスで利用されるトラストの利用方法に近づけ，電子データの検証業務を低減する方式を提案する．

図 7 は図 2 のユースケースに即したトラスト値修正の例である．修正対象の t_2 は企業 DB に含まれているかどうかという社会的なトラストである．上位に存在する G_1 を生成した署名者が t_2 を検証しているため，下位にある s_3 の t_2 の値を書き換え，トラスト要件を満たすものに変更する．上位の署名者が内容に対して保証する電子署名を付与することで，下位の電子署名の社会的トラスト不足をカバーする形となる．

本手法は，データ作成者と検証者が，事前に特定の社会的なトラストの処理方針について合意しておくことで，よりビジネスにおける検証効率を高めることができる．

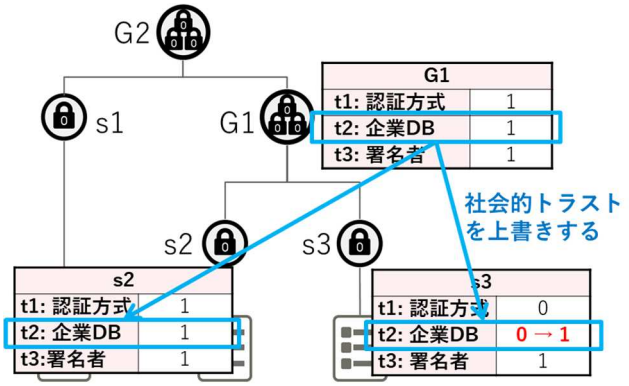


図 7　トップダウン型のトラスト修正の例

5.3　ボトムアップ型のトラスト修正

社会的なトラストの多くが，最後に電子署名を付与したユーザのトラストで評価されるのに対して，データ的なトラストは下位のユーザのトラストが上位に影響する場合がある．

特にパスワードやアカウントをハッキングした上で電子署名を付与する行為や，不正な認証局を利用して不正な電子データを作成するなどの行為は，データ的なトラストの根本に関わる重要な要件である．そのため，仮に上位のユーザが低いセキュリティ体制を認めたとしても，その技術的な安全性まで保証し，理解しているとは限らない．

このようなデータ的トラストをビジネス現場に適用する場合，セキュリティ上の発生リスクは全体の中の最も脆弱な部分, 即ち最小値から想定するべきである. その場合，ヒエラルキーの下部まで含めた全てから，データ的なトラストの最小値を検索し，そこからボトムアップ型で他の電子署名に対してトラスト値を修正する手法を提案する．

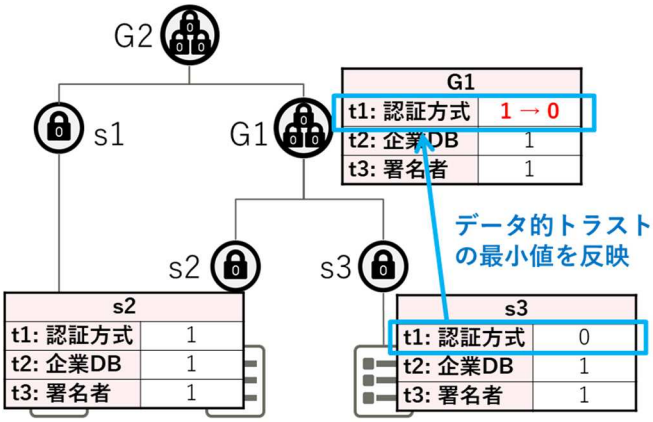


図 8　ボトムアップ型のトラスト修正の例

図 8 は図 2 のユースケースに即したトラスト修正の例である．修正対象の t_1 はユーザの認証に関する要件であるため，データ的なトラストである．グラフ構造の中で最も下位にある s_3 における t_1 の値が低いため，ワークフロー署名の検証を行うユーザのデータ的トラストが高い場合でも，なりすましなどの危険性があると考え，上位のデータのトラスト値を変更している．

5.4　トラスト値の分散に応じた重みづけ

本稿で記載している図 2 のユースケースでは，書類数が全体で 3 つと少ないが，実際のワークフロー型署名のユースケースを考えると，多量の電子署名を付与したドキュメントについて，全ての鍵検証を行うのが非効率であるために，集約する場合もある．

しかし，大量の電子署名と電子データが，全て同じ基準で作成されたものとは限らない．特に，データ的な安全性については，会社全体が同じシステムを利用しており，全員が一律で低い基準の電子署名を付与している場合と，会社として高い基準を採用している中で，あるユーザ 1 名だけが低い基準で電子署名を付与している場合とでは，その意味合いが大きく異なる．

そのような，トラスト値の分散にまつわる値を記録する場合には，各トラスト値の出現率をワークフロー型署名単位で計算し，その出現率を正規化エントロピーに変換することで重みづけを行うことで表現が可能となる．p_iをあるトラスト値の出現率，nを電子データ数と考えた場合，以下の式を用いる．

$$\text{正規化エントロピー } S = 1 + \sum_{i=1}^{n} p_i * log(p_i)/log(n)$$

正規化エントロピーでは 1 が最も情報量の多い状態となるため，1 から減じることでトラストベクトルの方式と基準を揃えている．

図 9 は 4 つの電子データの内，1 つのデータのデータ的トラストが低い場合を表現したものである．本来ならばボトムアップによって上位のトラスト値を低くするが，図の例では特異に 1 データだけ値が低いことを表現することが出来ない．

そこで，ボトムアップで値を修正するだけでなく，正規化エントロピー s_4 = -(1/4)*log$_2$(1/4)/log$_2$(4)＝0.25 を重みづけとして利用し，トラスト値 0.33×重みづけ (1 - 0.25)≒0.24 として記録する方法を示している．

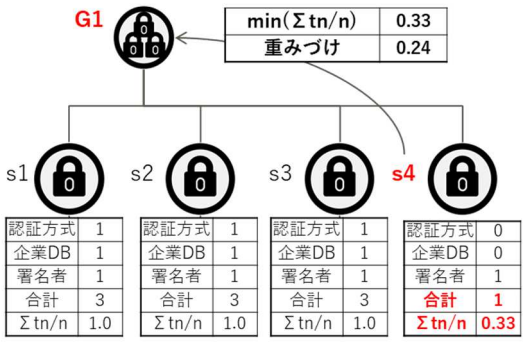


図 9　エントロピーによるトラスト重みづけの例

6. まとめ

本稿では，企業ごとに異なる基準を設定する，多様なトラスト基準について，それぞれの基準ごとにしきい値を定めることでトラスト要件をベクトル化して表現し，署名鍵データベースを利用してトラストの値を管理する手法を提案した．

これにより，現状では利用されていないトラストサービス内のセキュリティ要件に関するデータや，過去の行動履歴に基づく個人スコア等の要素を，同一のトラスト値に変換可能となるため，複数の電子署名付き電子データのトラストが比較可能となる．

また，同様の方式を利用している企業同士のトラストベクトルを揃えることで，企業同士のトラスト基準の比較や，共同事業を行う上でのトラストマッチング等に活用できる．

その上で，本手法でトラストを管理した場合を想定して，ワークフロー型署名を用いた際の複数の電子署名のトラスト値を修正する方式を検討した．

現状のビジネス慣習に沿ったトラスト値の更新を行う例として，トップダウン型のトラスト値の更新，ボトムアップ型のトラスト値の更新，分散を考慮したトラスト値の重みづけなどの手法について述べた．5 章で述べた 3 つのトラスト値の変更パターンは，あくまでも現状で考えられるビジネスユースケースでの問題について述べているが，これ以外にもトラストの修正方法は多く存在する．

今後，複数の企業のトラストポリシーを扱うトラストサービスでは，電子署名の鍵を管理するだけでなく，その企業のトラストポリシーを管理し，他の企業との橋渡しをする役割が求められるようになると考える．

2019 年のダボス会議で日本政府が提唱した，信頼ある自由なデータ流通[8]（Data Free Flow with Trust : DFFT）のような取り組みを通じて，データ流通におけるトラストの重要性が高まりつつある．今後は，電子データを作成した企業の持つトラストポリシーを透明化し，実際の取引リスクの検討に利用するため，本研究のようなトラストの管理方法が必要になると考える．本提案がそのような社会を実現する一助となることを望む．

参考文献

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; eIDAS, (2014).

[2] 手塚 悟, “欧米におけるトラストサービスに関わる調査業務報告書”, 一般社団法人データ流通推進協議会, (2020).

[3] NIST, William E. Burr, Donna F. Dodson, W. Timothy Polk, “NIST Special Publication 800-63-3 Digital Identity Guidelines”, NIST, (2006).

[4] “電子署名及び認証業務に関する法律”, 平成十二年法律第百二号, (2000).

[5] “電子署名及び認証業務に関する法律施行規則”, 平成十三年総務省・法務省・経済産業省令第二号, (2001).

[6] Lim, Hoon Wei, Florian Kerschbaum, and Huaxiong Wang, “Workflow signatures for business process compliance”, IEEE Transactions on Dependable and Secure Computing 9.5, (2012)

[7] Kumar, Divij, and Aditya Kumar Pandey, “Controlling a document electronic-signing (E-signing) workflow based on criteria specified by a document sender.”, U.S. Patent No. 10,628,596, (2020).

[8] 徳永 稔, 本多 義則, “電子データの真正性保証方法及びシステム”, 特許公報 特開 2009-010504, (2009).

[9] 経済産業省 商務情報政策局, “デジタル経済の進展への対応について”, (2019).