遺言制度研究会	参考資料４

遺言書の真正性の担保等に有用なデジタル技術及び民間事業者における遺言書作成支援等のサービスについて

第１　本資料の位置付け

本資料は、デジタル技術を活用した新たな遺言の方式について検討するに際し、真正性の担保、すなわち、当該遺言が遺言者本人の意思に基づいて作成されたことが事後に確認可能であること（偽造の防止）や、遺言完成後の遺言の改変を防止し、又は改変があった場合にこれを検知すること（変造の防止）等に有用な技術に関して、現段階で把握した情報を提供するものである。

併せて、民間事業者における遺言書作成支援及びそれに関連するサービスについても、現段階で把握した情報を提供するものである。

第２　デジタル技術について

１　遺言者本人の意思に基づいて作成されたことの担保に関する技術

遺言者本人は、遺言の効力が生じるときには既に死亡しており、遺言の内容について改めて本人に意思を確認することは不可能であることから、遺言者の真意を確保し、遺言書の偽造・変造等を防止するため、民法は、遺言について厳格な方式を定めている。

この点、自筆証書遺言においては、遺言書の全文、日付及び氏名の自書が要件とされているところ、その趣旨は、筆跡によって本人が書いたものであることを判定でき、それ自体で遺言が遺言者の真意に出たものであることを保障することができることにある。また、自筆証書遺言における押印要件の趣旨は、遺言の全文等の自書とあいまって遺言者の同一性及び真意を確保するとともに、重要な文書については作成者が署名した上その名下に押印することによって文書の作成を完結させるという我が国の慣行ないし法意識に照らして文書の完成を担保することにある。すなわち、自筆証書遺言においては、主として「筆跡」という人それぞれ固有の特徴を有し、容易に他人の模倣を許さないものに依拠しつつ、「押印」という遺言者本人のものであることを諸般の事情から推認でき、かつ、その有無を形式的かつ客観的に判断できるものにも依拠することで、遺言書の偽造・変造等の防止が図られていると考えられる。

そこで、デジタル技術を活用した新たな遺言の方式においても、人それぞれ固有の特徴を有し、容易に他人の模倣を許さないものに依拠した技術や、

遺言者本人のものであることを諸般の事情から推認でき、かつ、その有無を形式的かつ客観的に判断できる技術を用いることによって、遺言書の偽造・変造等の防止を図ることが考えられる。このような、遺言者本人の意思に基づいて作成されたことを事後に確認することを可能とする技術として、①電子署名（注１）、②録音・録画（注２）、③生体認証（顔貌認証、指紋認証、音声認証等）（注３）、④デジタルタッチペンによる入力（遺言者の筆跡を残す方法）が考えられる。

なお、これらの技術の活用については、択一的なものではなく、必要に応じて複数の技術を併用することも考えられる。

（注１）電子署名は、筆跡や生体とは異なり、それ自体が個人に固有の特徴を有するものではないが、一定の厳格な本人確認手続を経て発行され、発行後の管理を本人のみが行うことなどの諸般の事情により、遺言者本人のものであることを推認でき、かつ、その有無を形式的かつ客観的に判断できるものと評価し得る。

（注２）録音・録画は、撮影された本人の顔貌や身体が、人それぞれ固有の特徴を有するものであり、容易に他人の模倣を許さないものといえる。なお、撮影された人物が遺言者本人であるか否かの判断は、これを視聴する者が、他の資料と比較対照して判断することとなる（本資料においては、デジタル技術を用いて同一性を判断する顔貌認証は「生体認証」の一つとして整理する。）。

（注３）生体認証においては、本人の身体の特徴自体が、人それぞれ固有の特徴を有するものであり、容易に他人の模倣を許さないものといえる。もっとも、生体認証は、生体的な特徴の異同を識別するものであるため、原則として、遺言者の生体的な特徴が、遺言者自身のものとしてあらかじめ登録・保管されていることが前提となる。なお、顔貌認証及び音声認証については、対照すべき顔貌や音声があらかじめ登録・保管されていなかったとしても、遺言者自身のものであることが確実な対照資料（顔貌が撮影された写真や音声の録音された動画等）があれば、その精度は対照資料に係る情報の鮮明さ等によると考えられるものの、デジタル技術を用いて異同を識別し得る。

⑴　電子署名

ア　電子署名とは、電磁的記録に記録することができる情報について行われる措置であって、当該情報が当該措置を行った者の作成に係るものであることを示すためのものであり、かつ、当該情報について改変が行われていないかどうかを確認することができるものをいう（電子署名及び認証業務に関する法律第２条第１項、（研究会資料１及び研究会資料２参照）。

現在の実務においては、公開鍵暗号方式と呼ばれる技術方式が用いら

れている。公開鍵暗号方式とは、暗号化と復号とで異なる２つの鍵（秘密鍵と公開鍵）を使用する方式であり、このうち秘密鍵はその所有者が秘密に管理しなければならない鍵であり、また、公開鍵は公開可能で、他の人に利用してもらう鍵である。電子署名の対象となる電子文書のハッシュ値（注１）を秘密鍵を用いて暗号化した結果が、電子文書に対する電子署名となる。一対の秘密鍵及び公開鍵は、それに対応する電子証明書とともに発行されており、電子署名の付された電子文書を受領した者は、電子証明書を発行した認証局に対し、署名時に当該電子証明書がその有効期間内であったか否かなどの電子証明書の有効性確認を行った上で、電子文書自体のハッシュ値と、公開鍵を用いて復号された電子文書のハッシュ値を比較することにより、電子文書が改ざんされていないことなどを確認することができる（参考資料１－３参照）

イ　住民基本台帳に記録されている者であれば、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律に基づいて、マイナンバーカードに記録される自己の署名用電子証明書の発行を申請することができるため（同法第３条第１項）、マイナンバーカードの普及状況等に鑑みると、電子署名は、本人確認の技術として利用しやすいと思われる。また、電子署名及び認証業務に関する法律に基づく認定認証事業者である民間事業者が発行する電子証明書を使用することも考えられる。

もっとも、電子署名は、一定の厳格な本人確認手続を経て発行され、発行後の管理を本人のみが行うことによって、遺言者本人のものであると推認でき、かつ、その有無を形式的かつ客観的に判断できるものと評価し得るものであるところ、家族等の第三者が電子証明書の記録されたマイナンバーカードを管理したり、同カードを用いて電子署名の措置を講ずる際に必要となるパスワードを管理したりしている場合も想定され得る。

また、電子証明書の有効期間は、おおよそ５年を超えないものとされていることから（注２）、遺言の効力が生じた際には有効期間を経過してしまっており、電子証明書の有効性を検証することができない可能性がある。

（注１）ハッシュ値とは、元データからハッシュ関数と呼ばれる計算手順により求められた固定の桁数の値のことであり、ハッシュ値から元データの内容を復元することはできない。電子文書のほか、動画及び音声等のデータであっても、ハッシュ値を求めることができる。

ハッシュ関数とは、ハッシュ値を計算する手順において使われる関数の

ことである。同一のハッシュ値を持つ異なる内容のデータ作成を防止するため、ハッシュ関数の改善が進められているところ、過去には、ＭＤ５、ＳＨＡ－１と呼ばれるハッシュ関数が使用されてきたが、いずれも現在では安全性に不安が残るものとなっており、現在では、ＳＨＡ－２やＳＨＡ―３が主に使用されている。なお、近年普及が進んでいる量子計算機は、ＳＨＡ－２の安全性に影響を及ぼす可能性があると指摘されている。

（注２）電子証明書の有効期間は、おおよそ５年を超えないものと定められている（電子署名及び認証業務に関する法律第６条第１項第３号及び同法施行規則第６条第４号、並びに電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律第５条及び同法施行規則第１３条）。有効期間が満了したときは、電子証明書は、失効する。

なお、技術的には、電子署名の付与直後にタイムスタンプ（電子データがある日時に存在していたこと及びその日時以降に当該電子データが改変されていないことを証明できる機能を有する時刻証明情報のこと。）を付与するとともに検証に必要な情報を署名データ内に格納し、それら全体に対してタイムスタンプを（数回）付与することにより、長期にわたって有効性検証を可能とする長期署名の仕組みがあるが、長期署名の利用が一般化しているとはいえない。

また、デジタル庁「次期個人番号カードタスクフォース　中間とりまとめ」によると、電子証明書の有効期間を、マイナンバーカード本体の有効期間に合わせて１０年に延長することが検討されている。

⑵　録音・録画

ア　ビデオカメラ、スマートフォンの内蔵カメラ、パーソナルコンピュータの内蔵カメラ等により、遺言作成状況等における遺言者の顔貌等を録音・録画する方法である。

具体的には、①遺言作成開始から遺言作成終了までを録音・録画すること、②遺言者が当該遺言につき自らが作成したものである旨述べる様子を録音・録画すること、又は③遺言者が当該遺言内容を読み上げる様子を録音・録画することなどが考えられ、それら録音・録画された動画データを遺言に係る電子文書に添付して保存することが考えられる。

イ　デジタル機器の普及により、スマートフォンやパーソナルコンピュータ等を用いることで比較的鮮明な動画撮影が容易に可能であり、本人確認の技術として利用しやすいと考えられる。

しかし、遺言作成の開始から終了までに一定の期間を要すること（一つの遺言を継続的に複数の機会に作成すること）も想定できるところ、

①については、仮に遺言作成に長期間を要した場合、複数の動画データが存在することとなるため、データ量が膨大となる可能性がある上、遺言作成の開始から終了までの一部始終が録音・録画されているかについて事後的に検証することが困難となる可能性も否定できない。

加えて、仮に遺言の入力状況を撮影するとした場合、録音・録画によっても、撮影範囲外から第三者が入力作業を行っている可能性を完全に排斥することは困難であると考えられ（注１）、そうすると、①の場合であっても、パーソナルコンピュータ等に入力された文章が本人の作成によるものではない可能性を完全に排斥することは困難である。

また、①から③までの各場合において、ディープフェイク技術（注２）により偽動画が作成される可能性があり、現在の技術水準では、動画がディープフェイク技術により作成された偽動画であるか否かを、デジタル技術を用いて完全に誤りなく判断することは困難であるとされる。

（注１）例えば、遺言者がノート型パーソナルコンピュータを用いて遺言を作成する場合において、本人以外の者が、録音・録画の画面外から当該パーソナルコンピュータに接続された外付けキーボードによって入力し、遺言者になりすまして遺言を作成した場合には、複数のキーボードのいずれから入力作業が行われたかを特定することは技術的に困難であり、作成された遺言の入力作業につき本人以外の者が行ったか否かを判断することは困難である。

（注２）ディープフェイク技術とは、本来、機械学習アルゴリズムの一つである深層学習（ディープラーニング）を使用して、２つ以上の画像や動画の一部を結合させ元とは異なる動画を作成する技術である。「ディープフェイク」とは、一般的には、フェイク動画、偽動画を指すことが多く、現実の映像や音声、画像の一部を加工して偽の情報を組み込み、あたかも本物のように見せかけて相手をだます方法として認識されつつある。

現在の技術水準では、ディープフェイク技術を用いた偽動画の作成は高コストであり、容易に作成できるとはいい難いが、今後の技術の進歩により、容易にディープフェイク技術を用いた偽動画を作成することができるようになる可能性がある。

なお、ディープフェイク技術を用いた偽動画に対処するための技術も日々進歩しており、今後、ディープフェイク技術を用いた偽動画であるか否かを判断する技術が開発される可能性もある。

⑶　生体認証

生体認証の具体例としては、顔貌認証、指紋認証、音声認証、虹彩認証

及び静脈認証等が考えられ、具体的な活用例としては、遺言に係る電子文書に、これらの生体認証の対象となる遺言者の特徴に係るデータを添付することが考えられる。

生体認証は、いずれも特定の生体的特徴の異同識別を行うものであることから、遺言作成時における遺言者の生体的特徴の登録・保管のみならず、その前提として、遺言作成時に登録・保管された生体的特徴と対照するために必要となる生体的特徴が、遺言者のものとして、事前に登録・保管等されている必要がある。

仮に遺言者以外の者が、自らの生体的特徴を遺言者の生体的特徴であると偽って登録・保管した場合には、遺言者以外の者が遺言者になりすまして遺言を作成することが可能となってしまうため、生体的特徴の事前登録・保管方法については、当該生体的特徴が遺言者本人のものであることを担保することのできる方法である必要がある（注）。

（注）生体認証のうち、顔貌認証については、自動車運転免許証の顔写真、マイナンバーカードの顔写真又はパスポートの顔写真など、厳格な本人確認を経た上で発行される公的な本人確認書類が存在することから、これを利用する制度を構築することが考えられる。

ア　顔貌認証

顔貌認証は、カメラに写された顔貌（写真、動画を含む。）と、対照資料である写真等に撮影された顔貌の目、鼻、口などの特徴点の位置や顔領域の位置及び大きさなどをもとに照合を行い、その同一性を判断する技術である。

現在、標準的な金融機関でも採用されている認証技術であり、本人確認の技術として利用しやすく、本人確認の精度も高い上、対照すべき顔写真があれば、顔写真と異なる表情の場合だけでなく、メガネやマスクを着用していた場合であっても、同一性を判断することが可能である。また、自動車運転免許証等の顔写真と対照することが可能である。

他方で、本人以外の者が遺言者の写真を入手し、同写真をカメラに写された顔貌であるかのように装って遺言に係る電子文書に添付した場合には、遺言者になりすまして遺言を作成することが可能となり得る。また、遺言作成時に顔貌を撮影していたとしても、遺言作成時の年齢と対照すべき顔写真撮影時の年齢が大きく離れていたり、体重の増減等により顔貌が変化していたりする場合には、仮に真実は同一人であったとしても、同一人であると認証されない可能性が高くなる。

イ　指紋認証

光センサー等で指紋の凹凸を検知した上、検知した指紋の特定範囲における特徴点及び特徴点間を横切る隆線（指紋の凸部分）の数等につき、あらかじめ登録・保管された指紋の特定範囲における特徴点及び特徴点間を横切る隆線の数等と合致しているか否かによって、両指紋の同一性を判断する技術である。

スマートフォンにおける本人確認技術として採用されるなど生体認証技術として比較的広く認知されており、本人確認の精度は高い。

他方、指紋の凹凸も再現可能な精密な３Ｄプリンタ等を使用して指紋を複製した場合には、複製された指紋が認証されるおそれがある。

ウ　音声認証

音声認証とは、人間の発声器官が、声帯振動を喉・口・鼻で調音しており、各器官の形状や動きが個人性を形成していることに着目し、声の特徴を捉え、本人を特定する技術である。対照資料である特定のフレーズの音声と同一のフレーズを発声して同一性の判断を行う方法と、異なるフレーズを発声して同一性の判断を行う方法がある。

スマートフォンやタブレットなどの一般的に普及している集音マイク等を用いることによって利用可能であり、比較的導入しやすい本人確認技術である。

もっとも、音声認証の精度は、集音マイクの精度によって異なるほか、録音環境（周囲の雑音及び集音マイクとの距離など）、本人の状況（風邪をひいているか否か、マスク着用の有無など）に左右されるため、対照すべき音声のみならず、認証時の音声についても、適切な設備が整った場所で発声・録音しなければ、高精度の認証は期待できない。また、ＡＩを用いた音声操作など、人の声を復元する技術は近年目覚ましい進化を遂げており、音声認証だけでは、将来にわたって偽造・変造を防ぐことは難しいとされる。

エ　虹彩認証及び静脈認証

虹彩認証とは、虹彩（黒目の内側にある瞳孔の周りのドーナツ状の部分）につき、微小空間に分割した上で虹彩の輝度を数値化し、隣接する微小空間との数値変化を符号化することで特徴量を生成し、あらかじめ登録・保管された虹彩の特徴量と比較照合して同一性を判断する認証方法である。

静脈認証とは、赤外線などを照射することにより、静脈の形状をパタ

ーン化して読み取り、あらかじめ登録・保管していたデータと照合して同一性を判断する認証方法である。

いずれも、他の認証技術と併用することで、認証の精度を高めることが可能となるが、虹彩情報や静脈情報を事前に登録・保管するためには、一般には普及していない専用の機器を用いて各情報を取得する必要があり、専用の機器が設置されている場所に出向く必要がある。なお、静脈認証については、銀行のＡＴＭの一部で対応しているものの、現時点では普及率は低く、継続するにはコストの観点から難しいのではないかとの議論もある。

⑷　デジタルタッチペンによる入力（遺言者の筆跡を残す方法）

デジタルタッチペン等を用いて文章の入力作業を行う方法である。

遺言者の筆跡を残すことが可能であるが、筆跡の同一性の判断において対照すべき筆跡は、紙媒体に自書された文字ではなく、同じくデジタルタッチペン等を用いて入力された文字となるところ、現時点において、社会に広く普及された入力方法とはいい難いことなどから、筆跡の同一性の判断は困難である可能性がある。

２　遺言完成後に変造されていないことを担保する技術

⑴　電子署名

前記１⑴のとおり、電子文書を受領した者は、電子証明書を発行した認証局に対し、署名時に当該電子証明書がその有効期間内であったか否かなどの電子証明書の有効性確認を行った上で、電子文書自体のハッシュ値と、公開鍵を用いて復号された電子文書のハッシュ値を比較することにより、電子文書が改ざんされていないことなどを確認することができる（参考資料１－３参照）

仮に、電子署名後に電子文書が変更された場合には、当該電子文書のハッシュ値も変更されるため、これらのハッシュ値の比較により、電子文書の改ざんの有無を把握することができる。

⑵　ブロックチェーン

ア　ブロックチェーンとは、特定のデータを「ブロック」と呼ばれる形式にまとめ、それを時系列に沿って保存する技術をいう。

「ブロック」には、直前のブロックのハッシュ値（注１）が書き込まれているため、仮に特定のブロックに保存されたデータが改ざんされた場合には、後のブロックに保存されたハッシュ値と整合しないこととな

るため、容易に改ざんの事実が発見可能となる。また、データを管理するコンピュータノード（注２）が複数分散して構成され、同じデータを全てのノードで管理しているため、仮にひとつのノードのデータを改ざんしようとしても、残りのノードのデータと一致しなければ改ざんは成立せず、ノードの多数決でデータの信頼性を担保している。

ブロックチェーンを活用する具体例としては、公的機関又は民間事業者において遺言に係る電子文書等を管理するネットワークを構築し、同ネットワーク上にアップロードされた遺言に係る電子文書等につきブロックチェーンを用いて保存することなどが考えられる。なお、同ネットワーク上にアップロードされた遺言に係る電子文書については、スマートフォン等向けのアプリケーションソフトを利用して作成する場合や、インターネットのウェブサイト上で作成する場合、パーソナルコンピュータ等を使用して作成する場合などが想定される。

イ　ブロックチェーンは、暗号資産を運用するための技術として普及しており、現在の技術水準では、データの改ざんがほぼ不可能といわれていることから、遺言完成後の遺言の改変を防止し、又は改変があった場合にこれを検知すること（変造の防止）に有用な技術であるといえる。

なお、遺言が遺言者本人の意思に基づいて作成されたことを事後に確認することを可能とするためには、他の技術を併用することが考えられる。

また、複数のノードで管理するため、保存データの容量が膨大である場合（長時間の動画や大容量の画像ファイル等）、ノードの数だけデータを複製する必要があるため、管理コストが高くなる可能性がある。その対策として、ブロックチェーンを利用しつつデータのハッシュ値のみを保存することも考え得るが、その場合には、保存すべきデータの原本は、ブロックチェーンとは別に保存されることが必要となる。

なお、複数のノードを利用せず、単一のノードのみでブロックチェーン技術を利用することも可能ではあるが、その場合には、ノードの多数決によってデータの信頼性を担保する機能は意味を有しない。

（注１）ハッシュ値及びハッシュ関数については、前記１⑴（注１）参照。

（注２）コンピュータノードとは、コンピュータネットワークに接続されている１つ１つの機器のこと。コンピュータネットワークに接続されたパーソナルコンピュータも、「ノード」に該当する。

３　その他の関連する技術

⑴　元データと複製データを区別することのできる技術

ア　デジタルデータは複製コピーが可能であり、元データと複製コピーされたデータは同一の電磁的記録となる。すなわち、両データはハッシュ値も同一であり、基本的には区別できない。

この点について、元データと複製データを区別することのできる技術として、ＮＦＴという技術が考えられる。

ＮＦＴ（Non-Fungible Token、非代替性トークン）とは、ブロックチェーンを基盤にして作成された代替不可能なデジタルデータのことであり、デジタルデータに、「ＮＦＴ」といういわゆる保証書のようなデータを付けることで、当該デジタルデータを唯一無二の非代替的なデジタルデータとすることができる。そして、複製コピーされたデータにはＮＦＴが付かないため、ＮＦＴの有無によって元データと複製コピーとを区別することが可能となる。ＮＦＴは、現在、デジタルアート等有形・無形の様々なものに用いられるようになっており、今後市場が拡大していくと予想されている。

イ　コピーが可能な電磁的記録については、同一の電磁的記録が複数存在し得るため、そのうちの一つの電磁的記録を削除したことをもって遺言の撤回と認めることは困難になり得るところ、ＮＦＴを活用した場合には、電磁的記録の唯一性を確保することができる。しかし、ＮＦＴは、ブロックチェーンを前提とする技術であるため、ブロックチェーンと同様に、当該遺言が遺言者本人の意思に基づいて作成されたことが事後に確認可能となる機能は有していないため、当該遺言が遺言者本人の意思に基づいて作成されたことを事後に確認することを可能とする他の技術と併用することが必要となる。

⑵　保存されたデータにつき、厳格な閲覧制限等を設ける技術

ア　保存されたデータにつき、厳格な閲覧制限・印刷制限等を設ける技術として、ＶＤＲという技術が考えられる。

ＶＤＲ（ヴァーチャル・データルーム）とは、セキュリティが確保されたウェブサイト上に電子文書やデータをアップロードし、パスワードを使って閲覧者がアクセスする方法であり、平成１２年頃から、Ｍ＆Ａのデューデリジェンスなど機密性と確実性が求められる文書の共有の際に活用されている。

また、単にアクセス権限の設定のみならず、閲覧制限、ダウンロード制限及び印刷制限などの設定が可能である上、閲覧履歴等を細かく把握することが可能であり、厳格な管理が可能となる。また、ＶＤＲへのログイン時に、前記生体認証を併用することは、技術的には可能である。

ＶＤＲを活用する具体例としては、公的機関又は民間事業者が、ＶＤＲを利用して遺言に係る電子文書を保存すべきウェブサイトを設けることが考えられ、その場合には、ログイン時に前記生体認証を用いることや、前記ブロックチェーンを併用することが考えられる。

イ　ＶＤＲ自体は、当該遺言が遺言者本人の意思に基づいて作成されたことが事後に確認可能となる機能や、遺言完成後の遺言の改変を防止し、又は改変があった場合にこれを検知する機能は有していないことから、前記各技術と併用する必要がある。

第３　民間事業者における遺言書作成支援等のサービスについて

一部の民間事業者は、インターネットやスマートフォン向けのアプリケーションソフトを利用し、遺言書作成支援及びそれに関連するサービスを提供していることから、以下では、その概要を紹介する（注）。

（注）本項は、デジタル技術を活用した新たな遺言の方式を検討するに当たって参考となる情報として、民間事業者により提供されている遺言書作成支援及びそれに関連するサービスの内容について情報提供するものである。なお、民間事業者が提供する遺言書作成支援及びそれに関連するサービスについては、別途弁護士法第７２条（非弁護士の法律事務の取扱い等の禁止）等の法令の規定との関係が問題となり得る。

１　インターネットを利用した遺言書作成支援サービスの提供の例

Ａ事業者は、遺言をしようとする者がインターネット上のウェブサイトにアクセスし、画面上に表示された指示に従って、その家族関係及び遺産関係（自らが所有する不動産、預貯金及び現金等の遺産の有無や相続分の指定等）等を入力することで、遺言書案を自動作成することができるサービスを提供している。

同サービスでは、作成された遺言書案については、入力時に使用した各端末に保存され、Ａ事業者も遺言書案の内容や入力内容を把握することができないとのことである。

２　アプリケーションソフトを利用した遺言書作成支援及びそれに関連するサービスの提供の例

Ｂ事業者は、遺言をしようとする者がアプリケーションソフトをダウンロードして起動し、画面上に表示された指示に従って、その基本情報（氏名、性別、住所等）、家族関係及び遺産関係（自らが所有する不動産、預貯金及び現金等の遺産の有無や相続分の指定等）等を入力（注１）することにより、

遺言書案を自動作成することができるサービスを提供している。

また、上記に加え、同サービスでは、遺言書案作成者に対する通知の有無、方法及び頻度を設定することができ（注２）、仮に遺言書案作成者が当該通知に対して３回以上反応しなかった場合には、遺言書案作成者が事前に指定していた連絡先に、遺言書案データが転送されることとなる（なお、同サービスを利用して作成される遺言書案は、民法上の方式に従ったものではないから、それとは別に、民法上の方式を遵守した遺言書の作成が必要である。）。

上記アプリケーションソフトの本人確認は、メールアドレスとパスワードによって行われ、同アプリケーションソフトを利用して作成した遺言書案データは、ブロックチェーンを用いて保存されており（注３）、仮に遺言書案作成者が、自己のスマートフォンから同アプリケーションソフトを削除したとしても、遺言書案作成者に対する通知や遺言書案データの転送は妨げられないとのことである。

（注１）入力方法としては、スマートフォン等の画面をタップする方法のほか、音声入力も可能とのことである。

（注２）メール、ＬＩＮＥ又はその双方での通知を設定することができ、その頻度については、どの程度の期間に１回の通知を希望するかを設定することができる。

（注３）保存された遺言書案データについては、Ｂ事業者でも閲覧することが不可能である。

以　上