裁判所　御中

クラウドサインによる
電子契約の締結等に関する説明書

弁護士ドットコム株式会社（以下「**当社**」という。）は、当社サービスである電子契約プラットフォーム「クラウドサイン」（以下「**本サービス**」という。）による電子契約の締結の仕組み等や、なぜ本サービスを利用することによって契約成立の事実とその後に契約書データが改ざんされていないことを確認することができるのかなどについて、以下のとおり説明する。

なお、本書面による情報は、末尾記載の注意事項・免責条項を条件に、当社から提供するものである。

弁護士ドットコム株式会社 クラウドサイン事業本部

初版　　2019 年　1月　8日
第 6 .2 版　　2024 年　2月19日

目次

第１　本サービスの特徴

本サービスには、①契約当事者による一連の契約締結作業が全てネットワーク上で完結するため、容易かつ迅速に契約を締結できるという特徴に加えて、②契約書データに対して契約当事者の指示を受けた当社がその締結フローの各段階において当社の署名鍵による電子署名を付与することにより、契約成立の事実とその後に契約書データが改ざんされていないことを確認することができるという特徴がある。

本書面では、以下の「第２」において上記①の特徴を説明し、「第４」において上記②の特徴を説明する。また、「第３」においては上記②の特徴の理解の前提となる「電子署名及び署名検証の基本概念」を説明し、また、「第５」ではいわゆる電子署名法との関係等について説明することとする。

第２ 本サービスによる電子契約の締結の仕組み等

１ 本サービスによる電子契約締結のフローの概要

本サービスによる契約締結のフローは、概略、以下のとおりである。

なお、以下では、設例として、契約当事者（となろうとする者）を「Ａ」及び「Ｂ」とし、Ａが既に本サービスにアカウント登録した利用者であり、Ｂが本サービスにアカウント登録していない利用者である場面を想定する。[1]

① 本サービスの利用に先立って、ＡとＢは、それぞれ、必要に応じ相手方当事者の本人確認（身元確認・当人認証）を行った上で、双方が契約締結に用いる電子メールアドレスを確認し、また、適宜の方法によって、これから契約しようとする契約の内容について合意する。

② Ａは、合意された契約内容を記載した契約書（合意書、覚書、発注書など、そのタイトルを問わない。）のＰＤＦファイル（以下「**契約書ＰＤＦファイル**」という。）を作成する。

③ Ａは、本サービスのウェブサイトにアクセスし、本サービスにログインして、所定の操作をすることにより、契約書ＰＤＦファイルを本サービスのために当社が使用するサーバーコンピューター（以下「**当社サーバー**」という。）にアップロードする（図表６参照）。なおＡは、管理画面のセキュリティ設定から、スマートフォンアプリを用いた２要素認証設定を行い、セキュリティを強化することができる。（図表７参照）。

④ その上で、Ａは、本サービスのウェブサイト上で、契約の相手方であるＢの氏名や電子メールアドレス等を本サービスの指示に従って記入する。この段階で、Ａはアクセスコードを設定することもできる（任意）。[2]（図表８参照）

⑤ 次に、Ａは、本サービスのウェブサイト上で、画面に表示されている契約書ＰＤ

---

[1] 当然ながら、Ａ及びＢの双方が本サービスにアカウント登録した利用者である場合にも、本サービスの利用は可能である。なお、Ａが本サービスにアカウントを登録する方法は、別紙１記載のとおりである。

[2] 「アクセスコード」は、送信者が設定した任意の英数字の組み合わせであり、このアクセスコードを入力することにより受信者が契約書ＰＤＦファイルを開くことができるようになる機能である。送信者から受信者へのアクセスコードの通知は、別途の任意の方法（口頭伝達や電話による伝達、電子メール等による伝達など）によって行うことになる。

Ｆファイル上に「フリーテキスト」「チェックボックス」「押印欄」などの入力項目（以下「**入力項目**」という。）を設定することができる（任意）。入力項目を設定した場合、当該入力項目に入力する対象者を選択する必要があり、本設例では、「Ａ」か「Ｂ」を選択することになる。入力する対象者が「Ａ」である場合（入力項目を設定したＡ自身である場合）、Ａはこの段階で必要な事項を入力する。（図表９参照）

⑥ そして、Ａは、「書類の内容に同意の上、送信しますか？」という表示のあるダイアログボックスの中の「キャンセル」「送信」のボタンのうち、「送信」をクリックする。（図表１０参照）

⑦ Ａによる上記の処理により、本サービスからＢの電子メールアドレスに宛てて、「Ａ様から「タイトル」の確認依頼が届いています」と題する電子メールが送付される。[3]（図表１１参照）

⑧ Ｂは、上記電子メール中に表示される「書類を確認する」ボタンをクリックする（ＨＴＭＬメールの場合。テキストメールとして表示される場合には、上記電子メール中に表示されるＵＲＬにウェブブラウザ上でアクセスするか、ＵＲＬがハイパーリンク表示となっている場合には当該記載部分をクリックする。）ことにより、本サービスのウェブサイトにアクセスすることができる。なお、Ｂは、本サービスにアカウント登録していなくても、上記の操作により本サービスを利用することができるが、本サービスのウェブサイトにアクセスした段階で、本サービスの利用規約に同意することを求められる。Ｂが本サービスのウェブサイト上で、「利用規約に同意して書類を開く」ボタンをクリックすると、「書類内容の確認」というウェブページが開かれて、契約書ＰＤＦファイルが表示される（なお、Ａが「アクセスコード」を設定している場合には、アクセスコードを入力した上で、「利用規約に同意して書類を開く」ボタンをクリックする必要がある。）（図表１２参照）。またＢは、Ａから求められた場合など２要素認証設定を必要とする場合には、Ａ と同様の手続きにより本サービスのアカウント登録を行った上で、管理画面のセキュリティ設定から、スマートフォンアプリを用いた２要素認証設定を行い、セキュリティを強化することができる。

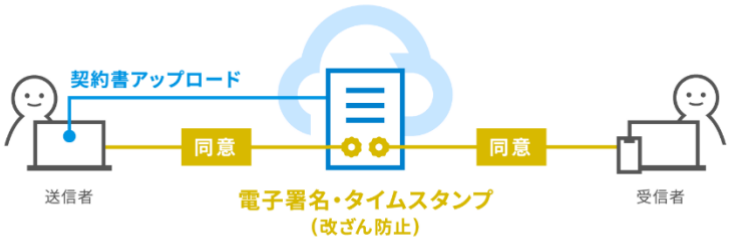
---

[3] この「タイトル」部分には、Ａが③の段階で契約書ＰＤＦファイルを当社サーバーにアップロードした際に指定したタイトルが表示される。⑫の「タイトル」部分や後記３の「タイトル」部分も同様である。

⑨ Ｂは、本サービスのウェブサイト上で、契約書ＰＤＦファイルの内容を確認し、（Ａが契約書ＰＤＦファイル上に「フリーテキスト」「チェックボックス」「押印欄」などの入力項目を設定しており、入力する対象者が「Ｂ」である場合には）適宜それらの入力項目に応じた入力を行う。（図表１３及び図表１４参照）

⑩ Ｂは、本サービスのウェブサイト上で、契約書ＰＤＦファイルの内容に問題がないと判断した場合には「書類の内容に同意」ボタンをクリックする。すると、「書類の内容に同意して確認を完了してよろしいですか？」という表示のあるダイアログボックスが開かれるので、その中の「キャンセル」「同意して確認完了」のボタンのうち、「同意して確認完了」をクリックする。（図表１５及び１６参照）

⑪ 以上の作業を経て、Ａ及びＢによって契約は締結され、同時に、当社からＡの電子メールアドレスとＢの電子メールアドレスの双方に対して、「「タイトル」の合意締結が完了しました」と題する電子メールが送付される。当該電子メールには、送信者の設定によって（後述する）当社の署名鍵による電子署名が付与された契約書ＰＤＦファイルの添付ができる[4]。また、同時に、当社サーバーにも、当該電子署名が付与された契約書ＰＤＦファイルが保管される。[5]



２　当社の署名鍵による電子署名の付与

当社は、以上の契約締結フローの各段階において、以下のとおり、契約当事者の

---

[4] 締結完了メールへのＰＤＦファイル添付設定機能を利用して、締結完了メールに対して締結済み書類ＰＤＦを添付することができる。添付しない設定の場合は、クラウドサインにログインすればダウンロードが可能である。クラウドサインのアカウント登録方法は別紙１「本サービスにアカウントを登録する方法」を参照のこと。

[5] なお、当該契約書ＰＤＦファイルの１頁目の左下端には、当社が付した「書類ＩＤ」が表示される（図表１７参照）。この「書類ＩＤ」は、契約書ＰＤＦファイルが当社サーバーにアップロードされた段階で、当社が当該契約書ＰＤＦファイルに対して付与したユニークなＩＤであり、一定のアルゴリズムによってランダムに構成される文字列である。

指示を受けたことに基づく当社の署名鍵による電子署名を付与する（契約当事者による本サービスの利用は上記の指示を意味し、当社は本サービスのシステムにより自動的・機械的に電子署名を付与することになる。）。

なお、入力項目の有無や数、契約当事者の数によって当社の署名鍵による電子署名の回数は異なることになるので、以下の記載は、前記１の設例において、入力項目が２つ（入力対象者をＡとする項目とＢとする項目がそれぞれ１つずつ）である場合を前提とする。

⑴　Ａが「送信」操作をした段階（上記⑥の段階）

ア　契約書ＰＤＦファイルに対して「書類ＩＤ」の情報が付与され、当該契約書ＰＤＦファイルの１頁左下端に「書類ＩＤ」が表示されたことに対する記録として、当社は、Ａが「送信」操作をした段階（上記⑥の段階）で、契約書ＰＤＦファイル（「書類ＩＤ」の情報を含むもの）に対して当社の署名鍵による電子署名（以下「**電子署名①**」という。）を付与する。

イ　また、契約書ＰＤＦファイルに対して、Ａが入力項目を入力したことに対する記録として、当社は、上記アに続けて、電子署名①を含む契約書ＰＤＦファイル（Ａの入力項目の情報を含むもの）に対して当社の署名鍵による電子署名（以下「**電子署名②**」という。）を付与する。

ウ　そして、Ａが「書類の内容に同意の上、送信しますか？」という表示のあるダイアログボックスの中の「送信」をクリックして契約書ＰＤＦファイルの内容に同意したことに対する記録として、当社は、上記イに続けて、電子署名②を含む契約書ＰＤＦファイルに対して当社の署名鍵による電子署名（以下「**電子署名③**」という。）を付与する。

⑵　Ｂが「同意して確認終了」操作をした段階（上記⑪の段階）

ア　契約書ＰＤＦファイルに対して、Ｂが入力項目を入力したことに対する記録として、当社は、Ｂが「同意して確認終了」操作をした段階（上記⑪の段階）で、電子署名③を含む契約書ＰＤＦファイル（Ｂの入力項目の情報を含むもの）に対して当社の署名鍵による電子署名（以下「**電子署名④**」という。）を付与する。

イ　そして、Ｂが「書類の内容に同意して確認を完了してよろしいですか。」という表示のあるダイアログボックスの中の「同意して確認完了」をクリックして契約

書ＰＤＦファイルの内容に同意したことに対する記録として、当社は、上記アに続けて、電子署名④を含む契約書ＰＤＦファイルに対して当社の署名鍵による電子署名（以下「**電子署名⑤**」という。）を付与する。

3 認定タイムスタンプの取得

本サービスでは、当社は、上記の電子署名⑤を認定タイムスタンプ[6]を埋め込んだ電子署名として行い、また、契約書ＰＤＦファイルに署名検証に必要な情報（失効情報など）を付加した上で、これに対して認定タイムスタンプ（文書タイムスタンプ）を取得する。[7]

このように認定タイムスタンプ(文書タイムスタンプ)を取得して契約書ＰＤＦファイルに付加することにより、契約書ＰＤＦファイルが「いつ存在していた情報か」及び「改ざんされていない真正な情報か」を確認することができる。

4 当社による合意締結証明書の発行

また、当社は、ＡとＢが「タイトル」と題する契約書ＰＤＦファイルのとおり契約を締結したことに関し、ＡとＢの同意日時を証明する書面である「合意締結証明書」を発行し、本サービスにアカウント登録した利用者であるＡは本サービスのウェブサイトから当該「合意締結証明書」をダウンロードすることができる。

「合意締結証明書」に記載されたＡ及びＢのそれぞれの同意日時は、ＡやＢの使用するパソコン(やスマートフォン)の時刻情報ではなく、当社サーバーの時刻情報等に基づいて表示される正確なものである。

---

[6]「認定タイムスタンプ」とは、認定タイムスタンプ局によって付与されたタイムスタンプをいう。ここで、「認定タイムスタンプ局」とは、時刻認証業務の認定に関する規程に基づき総務大臣が認定したタイムスタ ンプ局（時刻認証業務認定事業者）をいう。また、「タイムスタンプ」とは、これを付与する対象と なる電磁的記録のハッシュ値（メッセージダイジェストともいう。第３・３(2)イ参照)に時刻情報を 追加したデータをいう。当社は、アマノ株式会社(https://www.amano.co.jp/)の提供する「アマノタイムスタンプサービス 3161」を利用している。ここで付与されるタイムスタンプ を含む電子署名は、PAdES-T と呼ばれるものである。PAdES は、長期署名（第３・５参照）の標準 規格の１つであり、PDF ファイルに長期署名を組み込んだ規格である（PDF ファイルだけで長期署 名の検証が可能であるという特徴がある。）。

[7] このタイムスタンプを含む電子署名は、アマノタイムスタンプサービス 3161 によるものであり、PAdES-A と呼ばれるものである（アーカイブタイムスタンプやドキュメントタイムスタンプなどともいわれる。当社は「文書タイムスタンプ」と呼んでいる。）。

5 本サービスにおける当人認証の方法

なお、上記１の契約締結フローにおいて、「Ａ」として作業する人物がＡ本人であること、及び、「Ｂ」として作業する人物がＢ本人であることの当人認証は、電子メールアドレス認証を基本として行われる。

これに加えて、いわゆる電子署名法（第５参照）による推定効を求めるなど、より当事者において慎重を期す場合には、本サービスにアカウント登録した利用者においては、スマートフォンアプリ（Google Authenticator）で発行されたワンタイム・パスワードを用いた２要素認証を利用することができる。[8] また、本サービスにアカウント登録していない利用者の場合であっても、パスワード認証（前記１④のアクセスコードによる認証）を利用することで、当人認証を慎重に行うことができる。

第３ 電子署名及び署名検証の基本概念

１ 総論

上記第２・２のとおり、当社は、契約書データ（契約書ＰＤＦファイル）に対して、その締結作業の各段階において契約当事者の指示を受けたことに基づく当社の署名鍵による電子署名を付与するところ、これにより、後記第４のとおり、契約成立の事実とその後に契約書データが改ざんされていないことを確認することができる。

以上を理解するためには、電子署名の仕組みと電子署名の検証（電子署名が署名者本人により付与され、改ざんされていないことを確認すること）の基本概念を知る必要がある。以下では、その概要を説明する。

２ 電子署名とは何か

電子署名とは、電磁的記録（電子文書）に付与される、電子的なデータであり、紙

[8] ２要素認証を利用した場合、署名パネル（後記第４・３参照）及び合意締結証明書にその旨の記載がなされる。そのため、事後的に、本サービスの利用に際して２要素認証を利用した事実を、署名パネル及び合意締結証明書の記載から確認することができる。また、本サービスには、２要素認証を実装した ID プロバイダとの連携機能があり、そのような ID プロバイダのサービスを利用することによって２要素認証を行うこともできる（この場合、署名パネルには ID プロバイダ認証を経たことが、そして合意締結証明書には利用した ID プロバイダを特定するための情報が、それぞれ記載されることになる）。

文書における印影やサイン（署名）に相当する役割をはたすものである。[9]

3 電子署名の仕組み

電子署名を実現する仕組みとしては､公開鍵暗号方式の応用によるデジタル署名が有力である｡現在実用に供されている電子署名は､ほとんどがこのデジタル署名である。

⑴ 公開鍵暗号方式

ア 公開鍵暗号方式の意義等

そもそも、暗号とは、情報を伝達する際に、送信者と受信者の間で取り決めた一定の手順（これを「**鍵**」という。）によって元の情報（これを「**平文**」という。）を変換し、第三者には解読できないようにする手法をいう。

この暗号の手法には、古くから使われている共通鍵暗号方式と、１９７０年代半ばから用いられるようになった公開鍵暗号方式がある。

暗号化に用いる鍵と復号化に用いる鍵が同一である(これを「**共通鍵**」という。)暗号方式を、共通鍵暗号方式という。例えば、最も古い暗号の一つである単純換字暗号の「シーザー暗号」は、「平文の文字を３字ずらす」という手順（鍵）が用いられており、平文が「Ｒｕｂｉｃｏｎ」であったとすると、暗号化された文は「Ｕｘｅｌｆｒｑ」となる。送信者はこの暗号化された文を受信者に伝達し、受信者は同じ鍵（共通鍵）を逆の手順で使うことにより平文のメッセージを入手することになる。

これに対して、暗号化に用いる鍵（以下「**暗号化鍵**」という。）と復号化に用いる鍵（以下「**復号化鍵**」という。）に別個の鍵を用いることで、暗号化鍵を公開できるようにした暗号方式を、公開鍵暗号方式という。公開鍵暗号方式では、暗号化鍵は何らかの方法によって公開され、一方で、復号化鍵は秘密のままに保持することになる。そして、暗号化鍵で暗号化した情報は、対応する復号化鍵でのみ復号化できることが数学的に証明されている。そのため、受信者が予め暗号化鍵を何らかの方法により公開しておいて、送信者はこの暗号化鍵を用いて平文

---

[9] なお、第５・１⑵で説明するとおり、電子署名法における「電子署名」は、「電磁的記録（中略）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、次の要件のいずれにも該当するものをいう。（後略）」と定義されており、電磁的記録（電子文書）に付与される「電子的なデータ」ではなく、一定の要件を満たす電子的なデータを「付与する行為（＝措置）」を「電子署名」と定義している点に注意が必要である。

を暗号化して受信者に伝達し、受信者は自らの復号化鍵を用いて復号化して平文のメッセージを入手することができる。

公開鍵暗号方式には様々な方式があるが、例えばＲＳＡ暗号は、桁数が大きい合成数の素因数分解の困難性を安全性の根拠としている。十分に大きな素数ｐとｑがある場合に、それらの積（ｐ×ｑ）を計算することは容易である（この答をｎとする）。これに対して、２つの大きな素数の積であるような自然数ｎを素因数分解してｐとｑを導き出すことはとても困難である。例えば、ｐ＝３３７３、ｑ＝６２０３として、ｐ×ｑ（ｎ）＝２０９２２７１９を計算することは容易であるが、２０９２２７１９を素因数分解して３３７３と６２０３を導き出すことは困難である（実際には、もっと大きな素数の組み合わせが用いられることになる。十分に大きな桁数の素数を用いれば、現存するどのようなコンピューターを用いたとしても、素因数分解を行うことは現実的には不可能とされる。）。そして、暗号化鍵としてｎを用い、復号化鍵としてｐとｑを用いるような仕組みをうまく構築することにより、暗号化鍵（ｎ）が分かっていれば暗号化はできるが復号化はできないことになり（復号化には、復号化鍵であるｐとｑを知る必要がある。）、復号化鍵を持っている受信者のみが暗号文を復号化して平文のメッセージを入手することができることになる。

イ 共通鍵暗号方式と公開鍵暗号方式の比較

共通鍵暗号方式には、（公開鍵暗号方式と比較して）暗号化・復号化の処理を高速に行うことができるという長所があるが、送信者がどのように受信者に対して鍵を伝達するかという困難な問題があり（「鍵配送問題」ともいわれる。鍵が漏洩した場合には、当該鍵を入手した者であれば誰でも復号化できてしまうことになる。）、また、多数の当事者間でそれぞれの情報伝達を暗号化したい場合には多数の鍵が必要となるという問題があった。

共通鍵暗号方式のこのような問題を解決する目的で考え出された方式が、上記の公開鍵暗号方式である。

公開鍵暗号方式の場合、受信者の暗号化鍵は予め公開されているため、鍵配送問題は生じないことになるし、また、暗号化鍵で暗号化された暗号文はその暗号化鍵では復号化できない（復号化鍵でないと復号化できない）ことから、鍵の数は１セット（暗号化鍵と復号化鍵の１つの組み合わせ）で足りるため、鍵の数が多数になるという問題も解決されることになる。もっとも、公開鍵暗号方式の場合、暗号化・復号化の処理に時間を要し、経済的には優れない方式といえる。

共通鍵暗号方式と公開鍵暗号方式には、以上のようなメリット・デメリットがあるため、目的等によって使い分けがなされ、また、併用されることもある。

公開鍵暗号方式を実際に利用する場合には、平文を暗号化する際には共通鍵暗号方式により共通鍵を用いて暗号化し、その暗号化に用いた共通鍵の配送にのみ公開鍵暗号方式を使うことも多い。

⑵ デジタル署名

ア デジタル署名の意義等

電子署名のうち、公開鍵暗号方式を応用したものを、デジタル署名という（「デジタル署名」は、署名と同じように本人確認の機能を有することからその名称において「署名」という用語が使われているが、実際にはあくまで「電子的なデータ」である。）。

イ デジタル署名の付与と検証の手順

デジタル署名の付与とその検証は、通常、以下のような手順をとる。

① 送信者は、送信したい電磁的記録（メッセージ）をハッシュ関数[10]により圧縮して「ハッシュ値」という一定の長さのデータ（これを「**メッセージダイジェスト**」ともいう。）を作成する。これは、元のメッセージをそのまま暗号化するとデータ量が膨大になるため、圧縮するものである。ハッシュ関数によって作成されたハッシュ値は、元のメッセージに固有の値であり、同じメッセージからは同じハッシュ値が作られる（元のメッセージを少しでも改変すると、異なるハッシュ値が作られることになる。異なる元のメッセージから同一のハッシュ値が作られる確率は無視しうる程度に十分に低いものである。）。そして、ハッシュ値からは元のメッセージを復元することができないことは、ハッシュ関数の理論から数学的に証明されている。

② 送信者は、作成したメッセージダイジェストを、送信者の暗号化鍵で暗号化する（この送信者の暗号化鍵で暗号化されたメッセージダイジェストを、以下「**暗号化メッセージダイジェスト**」という。この暗号化メッセージダイジェストこそが「デジタル署名」である。）。そして、送信者は、元のメッセージと暗号

[10] ハッシュ関数（要約関数）とは、あるデータが与えられた場合に、そのデータを代表する数値を得る操作、または、そのような数値を得るための関数のことをいう。ハッシュ関数から得られた数値のことを要約値やハッシュ値などという。

化メッセージダイジェスト（デジタル署名）を受信者に送信する。[11]

③ 受信者は、暗号化メッセージダイジェストを、公開されている送信者の復号化鍵で復号化する（以下「**復号済みメッセージダイジェスト**」という。）。また、受信者は、送信者から送付されてきた元のメッセージについて、送信者が用いたものと同じハッシュ関数を用いて、メッセージダイジェストを作成する（以下「**受信者作成メッセージダイジェスト**」という。）。受信者が、上記の復号済みメッセージダイジェストと受信者作成メッセージダイジェストを比較して、両者が一致した場合には、Ⓐ暗号化メッセージダイジェストが送信者の暗号化鍵によって暗号化されたものであることと、Ⓑ送信者が暗号化メッセージダイジェストを作成した時点以降において元のメッセージが変更・改ざんされていないことを確認することができる。上記Ⓐは、送信者の復号化鍵で復号化できたということは、送信者の暗号化鍵で暗号化されたことを意味することから、そのように言える。また、上記Ⓑは、もし暗号化メッセージダイジェストを作成した後に、元のメッセージが変更・改ざんされていた場合には、受信者作成メッセージダイジェストが（ハッシュ関数の性質上）復号済みメッセージダイジェストとは異なるハッシュ値となるために、そのように言える。

④ なお、以上の手順は、送信者のみが送信者の暗号化鍵を使用できるという事実と、送信者の復号化鍵とされている鍵が、真に送信者の復号化鍵であるという事実を前提としている。これらの事実を受信者が確認できるように、送信者は、認証局から電子証明書の発行を受けて（その発行手続において、認証局は送信者の暗号化鍵を送信者が保有している事実を確認する。また、電子証明書には、送信者の復号化鍵のデータが含まれる。）、その電子証明書を受信者に（元のメッセージや暗号化メッセージダイジェスト（デジタル署名）と同時に）送付する。

ウ デジタル署名の機能

以上の手順からも読み取れるように、デジタル署名には、以下のような機能が認められる。

① 署名者特定機能（デジタル署名が添付された元のメッセージを作成し、送付し

[11] 実際には、元のメッセージも暗号化して送信することも多いと思われるが、それはデジタル署名とは別の問題である。

た主体（送信者）が、確かに送信者自身であることを確認することができる機能）

なお、この機能は、認証局において、暗号化鍵の保有者の本人確認を確実に行っている限りにおいて認められるものである。

② 改ざん防止機能(デジタル署名が添付された元のメッセージが変更ないし改ざんされているか否かを確認することができる機能)

受信者において､受信者作成メッセージダイジェストと復号済みメッセージダイジェストを比較することにより､元のメッセージに変更ないし改ざんが加えられているか否かを確認することができる。

4 電子証明書の有効期間

なお、電子証明書には有効期間が設けられており（通常は、１年間から３年間程度である）、認定認証事業者の場合でも、法律上、電子証明書の有効期間は５年を超えないものであることが求められている（電子署名及び認証業務に関する法律６条１項３号、電子署名及び認証業務に関する法律施行規則６条４号）。[12]

また、電子証明書は、有効期間内であっても、利用者からの請求等により失効することがある（電子署名及び認証業務に関する法律施行規則６条１０号）。

電子証明書の有効期間内にデジタル署名（電子署名）が行われた場合に、当該電子署名は有効であることになり、当該事実は認定タイムスタンプなどにより立証することになる。[13]

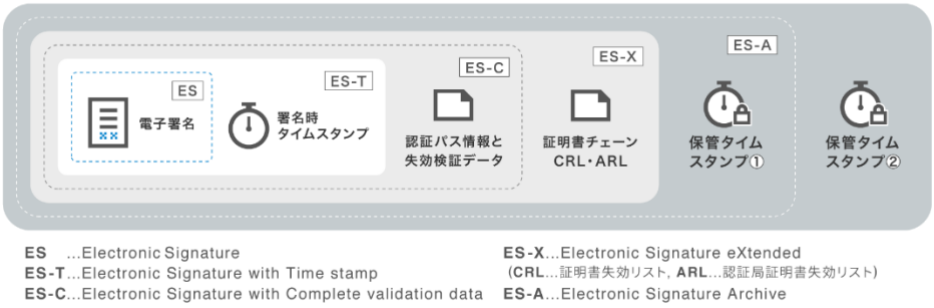
5 長期署名

電子証明書の有効期間内に、電子署名とタイムスタンプ付きの電子文書に対して検証に必要な情報（失効情報など）を付加したものに対して、更に新たなタイムスタンプ（保管タイムスタンプ）を施すことにより、当初の電子証明書の有効期間後に署名検証を可能にする技術が長期署名である。

---

[12] 電子証明書の有効期間は、後記第４の「３　本サービスにおける電子署名の検証方法」に記載のあるとおり、「署名パネル」欄を確認することにより、知ることができる。

[13] ただし、電子証明書の有効期間が経過してしまうと、署名検証ができなくなってしまうため、以下の「長期署名」が必要となる。



ES ...Electronic Signature
ES-T...Electronic Signature with Time stamp
ES-C...Electronic Signature with Complete validation data
ES-X...Electronic Signature eXtended
(**CRL**...証明書失効リスト, **ARL**...認証局証明書失効リスト)
ES-A...Electronic Signature Archive

本サービスは、ＩＳＯ３２０００に定められた標準規格である「ＰＡｄＥＳ（ＰＤＦ Ａｄｖａｎｃｅｄ Ｅｌｅｃｔｒｏｎｉｃ Ｓｉｇｎａｔｕｒｅｓ）」に準拠した長期署名フォーマットを採用しており、当初の電子署名の検証可能期間は認定タイムスタンプの有効期間である１０年間となり、さらに繰り返し認定タイムスタンプを付与することにより検証可能期間を延長することが可能となっている。

第４　本サービスにおける契約の成立の真正及び不改ざんの確認

１　なぜ契約の成立の真正をいえるのか

本サービスにおいては、契約書データ（契約書 PDF ファイル）に対して、当社がその締結作業の各段階において契約当事者の指示を受けたことに基づく当社の署名鍵による電子署名を付与することにより、契約成立の事実（契約の成立の真正）を確認することができる。

すなわち、前記第２・２で説明したとおり、Ａが「送信」操作をした段階、そしてＢが「同意して確認終了」操作をした段階の各段階において、当社が個々の情報付与や入力、同意に対する記録として、契約書ＰＤＦファイルに当社の署名鍵による電子署名を付与していることから、契約当事者（Ａ又はＢ）は、当該電子署名付与の理由となった行為（入力や同意）を行った事実について、（電子メールアドレス認証等の本人確認がなされる限りにおいて）「自らはそのような契約締結の意思表示をしていない」として契約締結を否認することができないのである（個々の電子署名を検証すること（後記３参照）によって、当該行為（入力や同意）をした人物の使用する電子メールアドレスと当該行為の行われた日時を確認することができるためである。）。

２　なぜ契約書ＰＤＦファイルが改ざんされていないといえるのか

また、本サービスにおいては、契約書データ（契約書 PDF ファイル）に対して、当社がその締結作業の各段階において契約当事者の指示を受けたことに基づく当社の署名鍵による電子署名を付与することにより、契約成立の後に契約書データが改ざんされていないことを確認することができる。

これは、上記１のとおり契約締結フローの各段階で当社が契約書ＰＤＦファイルに当社の署名鍵による電子署名を付与することから、仮に契約書ＰＤＦファイルを事後的に改ざんすると、電子署名（暗号化メッセージダイジェスト）と契約書ＰＤＦファイルから作成された受信者作成メッセージダイジェストが相違することになり、当該改ざんの事実が判明してしまうためである。

なお、紙の契約書の場合には、契約書本文の改ざんを事後的に行うことも（そのような技術を有する者であれば）技術的に可能であるのに対し、本サービスの場合には、電子署名の改ざん防止機能ゆえに、契約書ＰＤＦファイルの改ざんを事後的に行うことは技術的に不可能であるため（改ざんを行うと、電子署名の検証作業によって、改ざんの事実が明らかになってしまうためである。）、紙の契約書と比較しても改ざん

防止の観点において本サービスに優位性があるといえる。

3 本サービスにおける電子署名の検証方法

本サービスにおいて、契約締結フローの各段階において当社が契約書ＰＤＦファイルに対して当社の署名鍵による電子署名を付与した事実とその電子署名の内容等の確認は、例えば Adobe Systems 社製の無償でダウンロードできるＰＤＦ閲覧ソフトウエアである「Acrobat Reader」によって当該契約書ＰＤＦファイルを閲覧して、「署名パネル」欄を確認することにより、行うことができる。[14]（図表１８参照）

[14] 署名パネルには、「バージョン１：Bengo4.com,Inc.によって署名済み」などの表示がなされる。当社が電子署名を行った回数に応じて、バージョンの数は複数となる。そして、署名パネルにおいて各バージョンの電子署名の詳細を表示させると、署名の有効性、文書が当該署名の適用後変更されていないこと、署名者の ID が有効であること、署名時刻が署名者のコンピューターの計算に基づいていること、電子署名が付された理由などが表示される。

第５ 補足説明（電子署名法との関係ほか）

１ 電子署名法とは何か

⑴ 電子署名法の内容

電子署名及び認証業務に関する法律（平成１２年法律第１０２号。以下「**電子署名法**」ともいう。）は、平成１３年４月１日に施行された。

電子署名法により、本人による一定の要件を満たす電子署名が行われた電磁的記録は、真正に成立したもの（本人の意思に基づき作成されたもの）と推定される。

また、電子署名法の施行により、認証業務（電子署名が本人のものであること等を証明する業務）のうち一定の基準（本人確認方法等）を満たすものは国の認定を受けることができる制度が導入された。

⑵ 電子署名法による電子署名の定義

電子署名法２条１項は、同法にいう「電子署名」を以下のように定義している。

> この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）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、次の要件のいずれにも該当するものをいう。
>
> 一　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ること。
>
> 二　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であること。

同項１号の要件ゆえに、電子署名法にいう「電子署名」に当たるというためには、当該情報（電磁的記録の情報）が当該措置（電子署名を付与する措置）を行った者の作成に係るものであることを示すという「目的」が必要であるということになる。したがって、改ざん防止機能を働かせることを目的として、他人が作成した電磁的記録の情報に電子署名を付する措置を行ったとしても、それは電子署名法２条１項の要件を満たすものではなく、同法にいう「電子署名」には該当しないことになる。

また、電子署名法３条は、電磁的記録の真正な成立の推定について、以下のように規定している。

> 電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

このように、電子署名法は、同法にいう電子署名のうち、「本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）」と言えるもの（換言すれば、署名者特定機能があるもの。すなわち、当該電子署名から、その電子署名を行った者が誰であるかを特定できるもの。）に限って、電磁的記録の真正な成立の推定という法律上の効果を与えている。

電子署名法３条の電子署名に該当するものの一例として、既述したデジタル署名が挙げられる。もっとも、電子署名法３条は（技術的中立性を確保する観点から）具体的な方式を指定しておらず、同条の定める要件に該当するものであれば、同条の電子署名に該当することになり、同条の法律上の効果が与えられることになる。

また、電子署名法３条は、電子署名が認証機関に登録されているものであることも要求していない。電子署名法２条１項及び３条の求める目的及び機能があると認められる場合には、本人による電子署名があれば、同法３条の法律上の効果が与えられることになる。

以上のとおり、電子署名には、①広義の電子署名、②（広義の電子署名のうち）電子署名法２条１項の定める「電子署名」に該当する電子署名（以下「**２条電子署名**」ともいう。）、③（２条電子署名のうち）電子署名法３条の要件を満たす署名者特定機能があり電磁的記録の真正な成立の推定が及ぶ電子署名（以下「**３条電子署名**」ともいう。）があることになる。

⑶ 電子署名法３条の推定規定の効果（二段の推定との関係）

前記のとおり、電子署名法３条により、３条電子署名が付された電磁的記録は真正に成立したものと推定される（以下「**電子署名法３条の推定効**」ともいう。）。

この電子署名法３条の推定効は、いわゆる二段の推定[15]における二段目の推定（民事訴訟法２２８条４項による推定）と同様の効果を有することになる。

ここで、電子署名法３条による推定が行われるためには、３条電子署名を当該電磁的記録の作成者本人が行ったことが立証されなければならない点に注意が必要である。この点は、民事訴訟法２２８条４項による推定がなされるために本人またはその代理人の意思に基づく押印がなされたことが立証されなければならないことと同様であるが、私文書については二段の推定における一段目の推定（判例に基づく事実上の推定）が及ぶことにより私文書の作成名義人の印影が当該名義人の印章によって顕出されたものであることを印鑑登録証明書などによって立証できればよいことに対して、電磁的記録の場合にはこの一段目の推定と同様の事実上の推定が認められるか否かについて現時点では判例などが存在しない点に留意する必要がある。

また、二段の推定自体、必ずしも絶対的なものではなく、その各段階の推定が反証によって覆される可能性があるなどという点に留意する必要がある。

2 本サービスで契約当事者それぞれの署名鍵を用いた電子署名を行わない理由は何か

本サービスでは、契約当事者の間で締結された契約（契約書ＰＤＦファイル）に対して、契約当事者それぞれの署名鍵（暗号化鍵）を用いた電子署名ではなく、契約当

[15] 私文書の作成名義人の印影が当該名義人の印章によって顕出されたものであるときは、反証のない限り、当該印影は本人の意思に基づいて顕出されたものと事実上推定され（最判昭和３９年５月１２日民集１８巻４号５９７頁）、その推定がなされる結果、当該私文書は民事訴訟法２２８条４項により真正に成立したものと推定されることを、実務上「二段の推定」ということがある。

事者の指示を受けたことに基づき当社が当社の署名鍵による電子署名を付与する点に特徴がある。

これは、契約当事者がそれぞれ契約書ＰＤＦファイルにそれぞれの署名鍵（暗号化鍵）を用いた電子署名を付与するためには 電子証明書を取得する必要があるところ、認証局に対して電子証明書の発行を求めるためには費用も時間も要することから、契約当事者の双方が電子証明書を取得するコスト等に課題があるため、代わりに当社が当社の署名鍵による電子署名をする必要性があり、また、当社が当社の署名鍵による電子署名をすることによっても電子署名の改ざん防止機能等により契約当事者の間で契約が締結された事実及びその内容を確認することができるという許容性があるためである。

3 本サービスによる電子契約に電子署名法３条の推定効は及ぶか

本サービスによる電子契約に電子署名法３条の推定効が及ぶためには、契約書データ（契約書 PDF ファイル）に対して当社が当社の署名鍵による電子署名を付与することにつき、当該電子署名が２条電子署名に該当し、その上で、３条電子署名にも該当する必要があることになる。

⑴ ２条電子署名該当性

本サービスの場合、当社が契約書データ（契約書 PDF ファイル）に対して当社の署名鍵による電子署名を付与するところ、この電子署名が２条電子署名に該当するか、すなわち「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ること」と言えるかが問題となる。

総務省、法務省及び経済産業省が令和２年７月 17 日付けで公表した「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A」（以下「**２条 Q&A**」という。）では、「電子署名法第２条第１項第１号の「当該措置を行った者」に該当するためには、必ずしも物理的に当該措置を自ら行うことが必要となるわけではなく、例えば、物理的にはＡが当該措置を行った場合であっても、Ｂの意思のみに基づき、Ａの意思が介在することなく当該措置が行われたものと認められる場合であれば、「当該措置を行った者」はＢであると評価することができるものと考えられる。」「このため、利用者が作成した電子文書について、サービス提供事業者自身の署名鍵により暗号化を行うこと等によって当該文書の成立の真正性及びその後の非改変性を担保しようとするサービスであっても、技術的・機

能的に見て、サービス提供事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保されていると認められる場合であれば、「当該措置を行った者」はサービス提供事業者ではなく、その利用者であると評価し得るものと考えられる。」「そして、上記サービスにおいて、例えば、サービス提供事業者に対して電子文書の送信を行った利用者やその日時等の情報を付随情報として確認することができるものになっているなど、当該電子文書に付された当該情報を含めての全体を１つの措置と捉え直すことよって、電子文書について行われた当該措置が利用者の意思に基づいていることが明らかになる場合には, これらを全体として１つの措置と捉え直すことにより、「当該措置を行った者（＝当該利用者）の作成に係るものであることを示すためのものであること」という要件（電子署名法第２条第１項第１号）を満たすことになるものと考えられる。」との見解が示されている。

この２条Ｑ＆Ａの示す見解からすれば、本サービスのように、契約当事者の指示に基づき、当社の意思が介在することなく当社が当社の署名鍵による電子署名を契約書 PDF ファイルに付与するサービスであって、当該契約書 PDF ファイルの署名パネルを確認することによりサービス提供事業者（当社）に対して電子文書の送信を行った利用者やその日時等の情報を付随情報として確認することができるものとなっている電子契約サービスについては、当社の行う当社の署名鍵による電子署名が電子署名法２条１項の定める電子署名（２条電子署名）に該当するものと解される。

この点については、当社が産業競争力強化法に基づく「グレーゾーン解消制度」を利用して確認した結果として、所管官庁としての経済産業省、総務省、法務省、財務省から、令和３年２月５日付け回答によって、本サービスを利用した当社の署名鍵による電子署名は電子署名法２条１項の定める電子署名（２条電子署名）に該当する旨の見解が示されているところである。

⑵ ３条電子署名該当性

本サービスの場合、当社が契約書データ（契約書 PDF ファイル）に対して契約当事者の指示に基づき当社の署名鍵による電子署名を付与するところ、この電子署名が３条電子署名に該当するか、すなわち「これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるもの」と言えるかが問題となる。

総務省、法務省及び経済産業省が令和２年９月４日付けで公表した「利用者の指

示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A（電子署名法第３条関係）」（以下「**３条 Q&A**」という。）では、「この電子署名法第３条の規定が適用されるためには、次の要件が満たされる必要がある。①電子文書に電子署名法第３条に規定する電子署名が付されていること。②上記電子署名が本人（電子文書の作成名義人）の意思に基づき行われたものであること。」「その上で、上記サービス（注：利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービス。以下同じ。）が電子署名法第３条に規定する電子署名に該当するには、更に、当該サービスが本人でなければ行うことができないものでなければならないこととされている。そして、この要件を満たすためには、（中略）同条に規定する電子署名の要件が加重されている趣旨に照らし、当該サービスが十分な水準の固有性を満たしていること（固有性の要件）が必要であると考えられる。」「より具体的には、上記サービスが十分な水準の固有性を満たしていると認められるためには、①利用者とサービス提供事業者の間で行われるプロセス及び②①における利用者の行為を受けてサービス提供事業者内部で行われるプロセスのいずれにおいても十分な水準の固有性が満たされている必要があると考えられる。」「①及び②のプロセスにおいて十分な水準の固有性を満たしているかについては、システムやサービス全体のセキュリティを評価して判断されることになると考えられるが、例えば、①のプロセスについては、利用者が２要素による認証を受けなければ措置を行うことができない仕組みが備わっているような場合には、十分な水準の固有性が満たされていると認められ得ると考えられる。２要素による認証の例としては、利用者が、あらかじめ登録されたメールアドレス及びログインパスワードの入力に加え、スマートフォンへのＳＭＳ送信や手元にあるトークンの利用等当該メールアドレスの利用以外の手段により取得したワンタイム･パスワードの入力を行うことにより認証するものなどが挙げられる。」「②のプロセスについては、サービス提供事業者が当該事業者自身の署名鍵により暗号化等を行う措置について、暗号の強度や利用者毎の個別性を担保する仕組み（例えばシステム処理が当該利用者に紐付いて適切に行われること）等に照らし、電子文書が利用者の作成に係るものであることを示すための措置として十分な水準の固有性が満たされていると評価できるものである場合には、固有性の要件を満たすものと考えられる。」「以上の次第で、あるサービスが電子署名法第３条に規定する電子署名に該当するか否かは、個別の事案における具体的な事情を踏まえた裁判所の判断に委ねられるべき事柄ではあるものの、一般論として、上記サービスは、①及び②のプロセスのいずれについても十分な水準の固有性が満たされていると認められる場合には、電子署名法第３条の電子署名に該当するものと認められること

となるものと考えられる。したがって、同条に規定する電子署名が本人すなわち電子文書の作成名義人の意思に基づき行われたと認められる場合には、電子署名法第３条の規定により、当該電子文書は真正に成立したものと推定されることとなると考えられる。」「「これを行うために必要な符号及び物件を適正に管理すること」の具体的な内容については、個別のサービス内容により異なり得るが、例えば、サービス提供事業者の署名鍵及び利用者のパスワード（符号）並びにサーバー及び利用者の手元にある２要素認証用のスマートフォン又はトークン（物件）等を適正に管理することが該当し得ると考えられる。」との見解が示されている。

この３条Ｑ＆Ａの示す見解からすれば、スマートフォンアプリ（Google Authenticator）で発行されたワンタイム・パスワードを用いた２要素認証などを利用しかつデジタル署名を用いて利用者毎の固有性を担保した電子署名を契約書PDFファイルに付与する本サービスの利用については、３条Ｑ＆Ａにいう①及び②のプロセスで求められる十分な水準の固有性が満たされていると認められる。

なお、３条Ｑ＆Ａにいう①及び②のプロセスに関しさらに詳述すれば、a.利用者のブラウザと当社サーバー間及び b.当社サーバーと業務委託先であるサイバートラスト株式会社が運用管理する署名サーバー（以下「署名サーバー」という。）間で、それぞれ大要以下の通信を行ない、当社サーバー及び署名サーバー上のプログラムによる自動処理を実行する。

a.　本サービスの利用者（送信者）は、契約書ＰＤＦファイルの内容を確認した後、ブラウザ上の「書類の内容に同意の上、送信しますか？」という表示のあるダイアログボックスの中の「キャンセル」「送信」のボタンのうち、「送信」をクリックすることにより、当社に対して個別に署名指示を行う。この際、当社は、利用者（送信者）のID・パスワード（さらにオプションとして送信者が保有するスマートフォンアプリを用いた所有物認証の組み合わせ）により当人認証を行う。本サービスの利用者（受信者）についても、契約書ＰＤＦファイルの内容を確認した後、「書類の内容に同意して確認を完了してよろしいですか？」という表示のあるダイアログボックスの中の「キャンセル」「同意して確認完了」のボタンのうち、「同意して確認完了」をクリックすることにより、当社に対して個別に署名指示を行う。当社は、受信者が送信者に対して指定した電子メールアドレスに宛てて、本サービスのウェブサイトにアクセスするための電子メール（個々の契約書ＰＤＦファイルに対応する一意的なURLを含むもの）を送付すること（さらにオプションとして送信者が定めるアクセスコード、受信者が所有するスマートフォンアプリを用いた所有物認証の組み合わせ）により当人認証を行う。こうして当人認証を経た利用者（送信者及び受信者）から発信される

署名指示は、ブラウザと当社サーバー間の通信が SSL（Secure Sockets Layer）/TLS（Transport Layer Security）を利用して暗号化されていることから、経路途中での署名指示の改ざんやなりすましはできず、利用者毎の固有性が担保される。

b.　上記プロセスにより、利用者（送信者及び受信者）が、契約書ＰＤＦファイルに同意する際に、ブラウザから当社に対して個別に署名指示を行うと、当社は、当社サーバー上のプログラムにより自動的に当該利用者のシステム利用権限について確認を行い、利用権限があることを確認する。その後、当社サーバー上のプログラムにより自動的に電子署名を付与する際に必要となるデータ（利用者情報から、電子署名後の契約書PDFファイルに係る署名パネルに表示すべき情報を抽出して作成したもの）が作成され、当該データが署名サーバーに自動的に送信され、署名サーバーにおいて当社が預託した署名鍵（秘密鍵）により契約書ＰＤＦファイルに対して電子署名が付与される。なお、当社サーバーと署名サーバー間の接続においては、電子証明書を用いた認証が行われ、双方のサーバー間の通信も SSL/TLS を利用して暗号化されていることから、経路途中での署名指示の改ざんやなりすましはできず、ここにおいても利用者毎の固有性が担保される。

加えて、当社の署名鍵（秘密鍵）により暗号化を行う措置についてみると、暗号の強度を担保する署名アルゴリズムとして、当社は、ハッシュ関数 SHA256、鍵長 2048 ビットの RSA 方式を用いている。これは電子署名法施行規則第二条が定める「一　ほぼ同じ大きさの二つの素数の積である二千四十八ビット以上の整数の素因数分解」の有する困難性に基づく電子署名の安全性を持つデジタル署名である。

以上から、3 条 Q&A にいう①及び②のプロセスで十分な水準の固有性が満たされていると認められるから、「これを行うために必要な符号及び物件を適正に管理すること」の要件を満たすことによって、当社の行う当社の署名鍵による電子署名が電子署名法３条の定める電子署名（３条電子署名）に該当するものと解される。

そして、この場合、電子文書に電子署名法第３条に規定する電子署名が付されていると言えるところ、これに加えて、本サービスによる電子契約の締結の仕組み等（前記第２参照）からして、当社は契約当事者の指示を受けて上記電子署名を付与しているものであるから、上記電子署名が契約当事者本人（電子文書の作成名義人）の意思に基づき行われたものであることも認められるため、電子署名法３条の推定効が認められると言えることになる。

⑶　電子署名法 3 条の推定効が及ばない場合の証拠価値

なお、電子署名法３条の推定効が及ばない場合であっても、本サービスによる電子契約の証拠価値は十分に認められる。これは、契約当事者ではない第三者的立場にある当社がいわば「立会人」のようにして、契約当事者の指示を受けたことに基づく当社の署名鍵による電子署名をすることにより、当該契約自体に利害関係のない（それゆえに虚偽を述べる利益のない）立会人の契約締結現場の目撃証言がある場合と同様に、当該電子署名の付与された契約書ＰＤＦファイルが契約の成立を裏付ける十分な証拠となりうることから、そのように言えるものである。[16]

⑷ 判例・裁判例の動向

現時点では、本サービスを利用した電子契約を含め、電子署名の付された電子契約について、電子署名法３条の推定効が及ぶか否かについて明示的に争われた判例・裁判例は見当たらない。

なお、本サービスを利用したものではないと思われるが、電子署名の付された電子契約につき、契約の一方当事者名下の電子署名が本人の意思に基づくものであるか否かが争われた事案において、契約締結後の当該一方当事者の行動を踏まえて、契約の有効な成立が認められた裁判例が存在しており（東京地判令和元年７月10日・D1-Law判例ID29057497）、既に裁判上の証拠として電子署名の付された電子契約が用いられている事例が存在することが分かる。

[16] なお、当社は、電子署名の改ざん防止機能ゆえに、（万が一）当該契約に利害関係があると仮定しても、事実と異なる説明をすることもできないことになる。上記の「立会人の契約締結現場の目撃証言」の例に沿っていえば、当該立会人が契約締結現場における一連の経緯をビデオカメラで録画しているようなものである。

第６ 参考資料

・ 高野真人・藤原宏高編著『電子署名と認証制度―e-business のための実務運用上の指針と問題点―』（第一法規出版、２００１）

・ タイムビジネス協議会調査研究ワーキンググループ「電子署名検証ガイドライン V1.0.0」
（https://www.dekyo.or.jp/tbf/data/seika/densiguideline.pdf）

・ 総務省「電子署名・認証・タイムスタンプその役割と活用」
（https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/pdf/090611_1.pdf）

・ 独立行政法人情報処理推進機構のウェブサイトのうち「2.3 セキュアハッシュ関数」
（https://www.ipa.go.jp/security/pki/023.html）及び「2.4 デジタル署名」
（https://www.ipa.go.jp/security/pki/024.html）

・ 司法研修所編『民事訴訟における事実認定』（一般社団法人法曹会、２００７）

・ 総務省、法務省及び経済産業省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A」
（http://www.moj.go.jp/content/001323974.pdf）

・ 総務省、法務省及び経済産業省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A（電子署名法第３条関係）」
（http://www.moj.go.jp/content/001327658.pdf）

以 上

【注意事項・免責条項】

- 本書面の記載内容のうち電子署名に係る説明部分は、当該電子署名の有効期間内においてのみ妥当するものであることに留意されたい。電子署名の有効期間は、本書面第４・３記載の電子署名の検証方法によって確認することができる。
- 当社は、本書面の作成にあたり、正確な情報を記載するよう十分に注意を払っている。しかし、当社は、本書面に記載された情報、資料等の正確性及び信頼性について、明示的、黙示的にかかわらず、いかなる保証もしないものとする。
- 本書面上に記載された情報に依拠した結果により損失が発生した場合でも、当社は一切の責任を負わないものとする。
- 本書面の記載内容は予告なく変更されることがある。

以 上

別紙 1

本サービスにアカウントを登録する方法

本サービスにアカウントを登録する方法は、以下のとおりである。

① 本サービスにアカウント登録することを希望する利用者は、まず、本サービスのウェブサイトのトップページ（https://www.cloudsign.jp/）にアクセスする（図表 1 参照）。

② 利用者は、当該ウェブページに表示された「新規登録（無料）」ボタンをクリックする。すると、利用者は、当該ウェブページ上の「メールアドレス」と「パスワード」の入力欄にそれぞれを入力するよう求められるので、自分が利用しているメールアドレスと任意のパスワードを入力し（ただし、パスワードには、安全性の観点から、一定の条件がある）、再度「新規登録（無料）」ボタンをクリックする（図表 2 参照）。

③ 本サービスのシステムから、利用者が先ほど入力したメールアドレス宛に本登録用電子メールが届くので、利用者は、当該電子メールに記載されている「登録を完了する」ボタンをクリックする（図表 3 参照）。

④ すると、ウェブブラウザ上に本サービスの「アカウント登録確認」と題するウェブページが開かれて、「アカウント登録を完了させる前に、利用規約をご確認ください。」[17]、「パスワードを入力すると登録は完了です。」、「アカウント登録を完了させることにより、利用規約に同意したものとみなされます。」という表示が現れるので、利用者は、利用規約を確認した上で、当該ウェブページの「パスワード」の入力欄に（②で入力した）パスワードを入力し、その下に配置されている「登録」ボタンをクリックする（図表 4 参照）。

⑤ ウェブブラウザ上に「ユーザー登録が完了しました。」という表示とともに、「氏名」と「会社名」の入力欄が表示されるので、それらを入力し（ただし、会社名の入力は任意である）、その下に配置されている「保存」ボタンをクリックする（図表 5 参照）。

以 上

[17] この一文の「利用規約」の文字部分のみ色が変わっており、その文字部分をクリックすると、利用規約の内容が表示される。

別紙 2

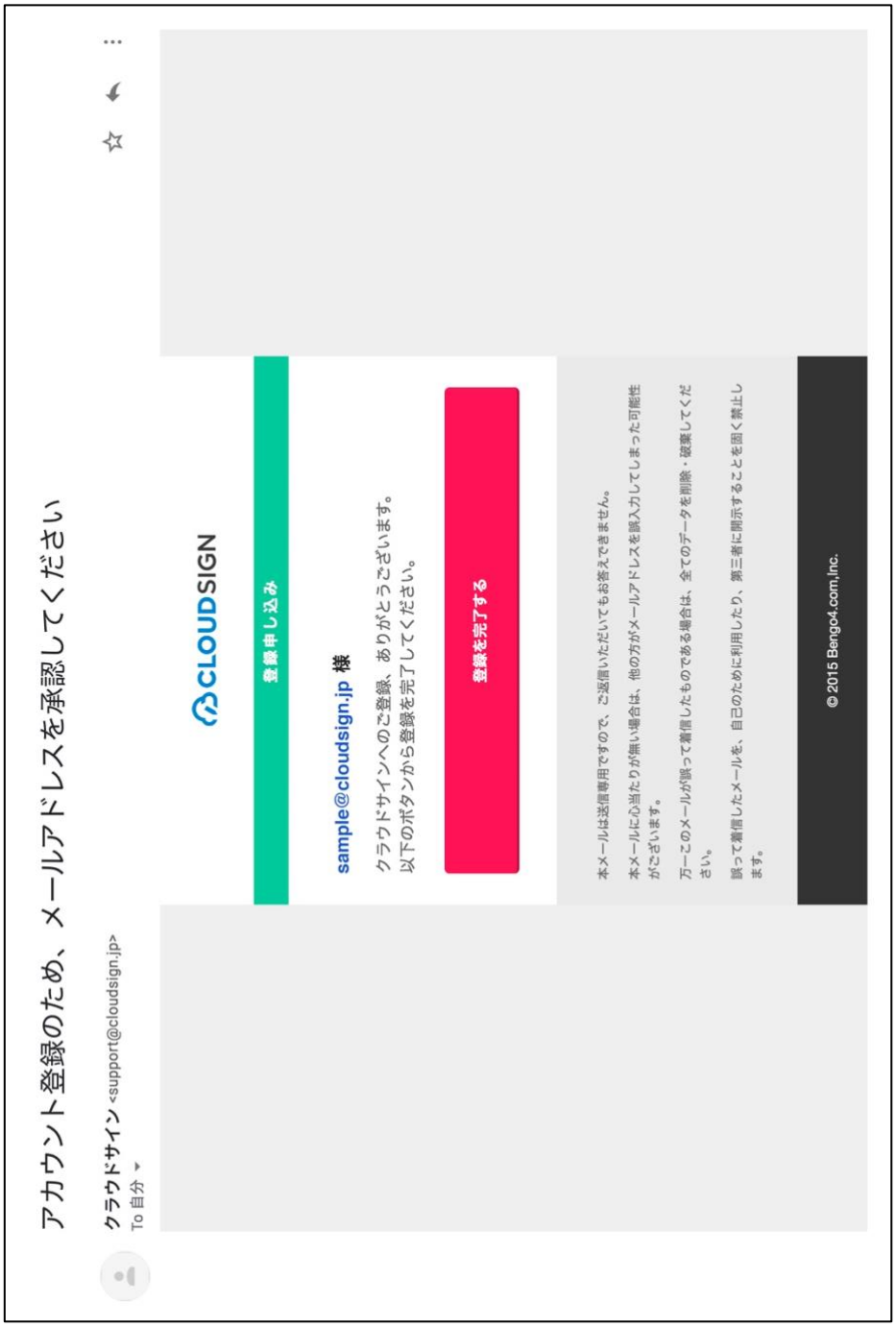
図表集

図表 1 ：別紙 1 の①

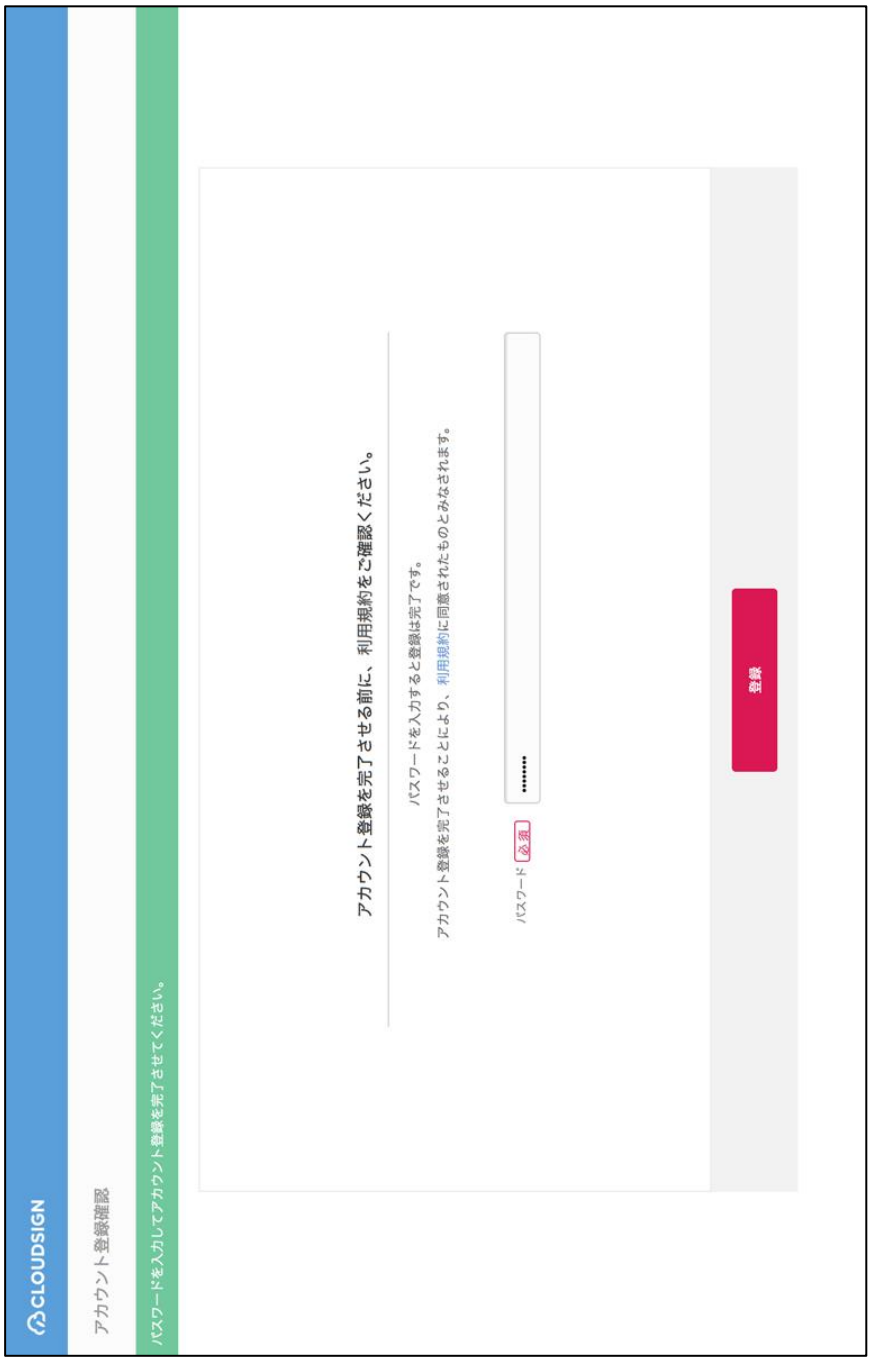
図表２：別紙１の②


CLOUDSIGN
製品紹介
活用方法
ログイン
新規登録
資料ダウンロード
いますぐクラウドサインを始めよう！
30秒で登録完了。無料で試してみましょう。
sample@cloudsign.jp
パスワードの安全度：高い
推測されにくいパスワードを設定してください。安全なパスワードの要件
パスワードの条件
・英小文字・英大文字・数字・記号(スペース以外)を2種以上含む
✓ 8文字以上32文字以下
✓ メールアドレスの一部を含まない
✓ 安全度が「高い」
クラウドサインについて詳しく知りたい方はこちら
資料ダウンロード

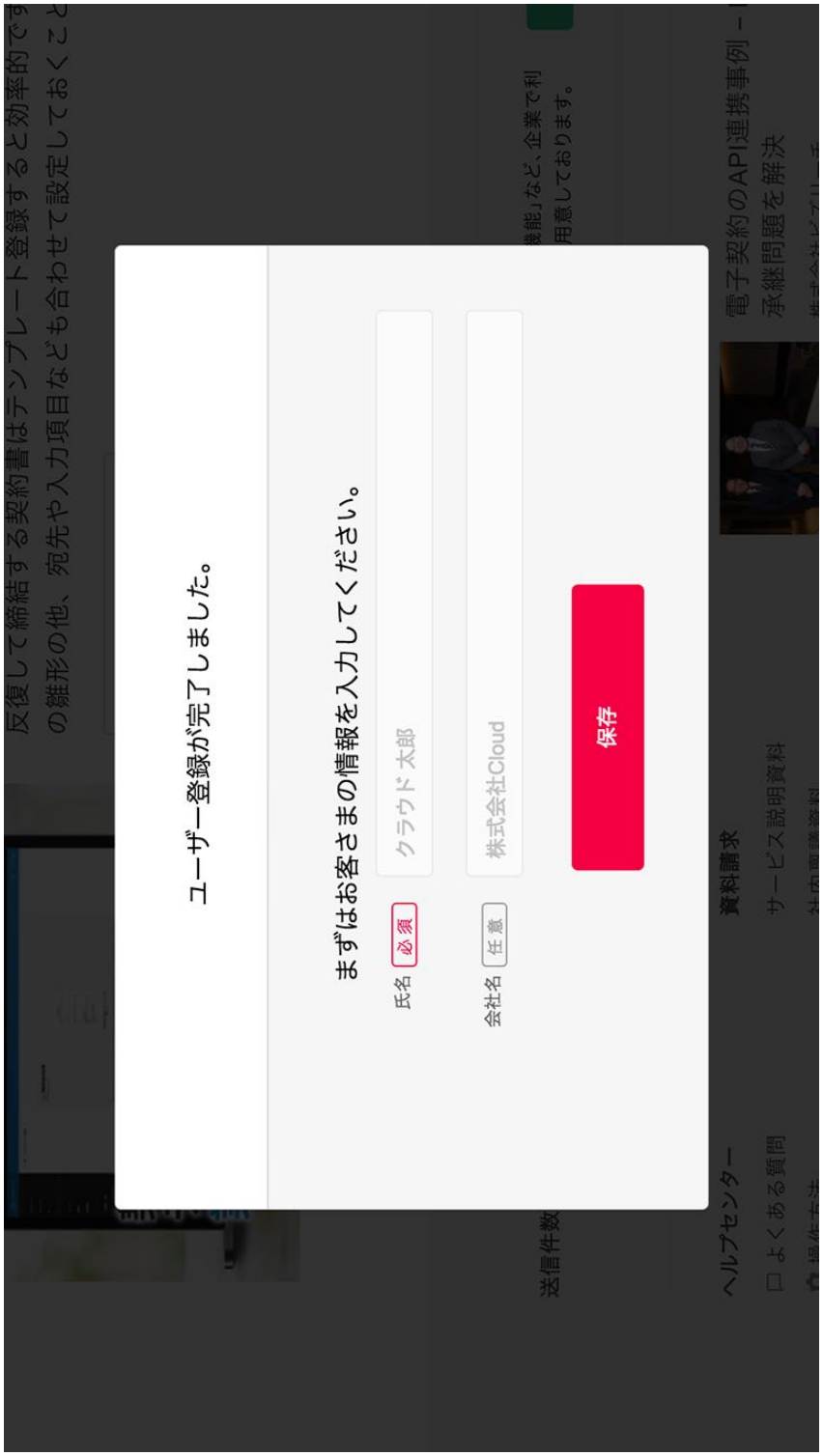
図表３：別紙１の③


アカウント登録のため、メールアドレスを承認してください
クラウドサイン <support@cloudsign.jp>
To 自分
CLOUDSIGN
登録申し込み
sample@cloudsign.jp 様
クラウドサインへのご登録、ありがとうございます。
以下のボタンから登録を完了してください。
登録を完了する
本メールは送信専用ですので、ご返信いただいてもお答えできません。
本メールに心当たりが無い場合は、他の方がメールアドレスを誤入力してしまった可能性がございます。
万一このメールが誤って着信したものである場合は、全てのデータを削除・破棄してください。
誤って着信したメールを、自己のために利用したり、第三者に開示することを固く禁止します。
© 2015 Bengo4.com,Inc.

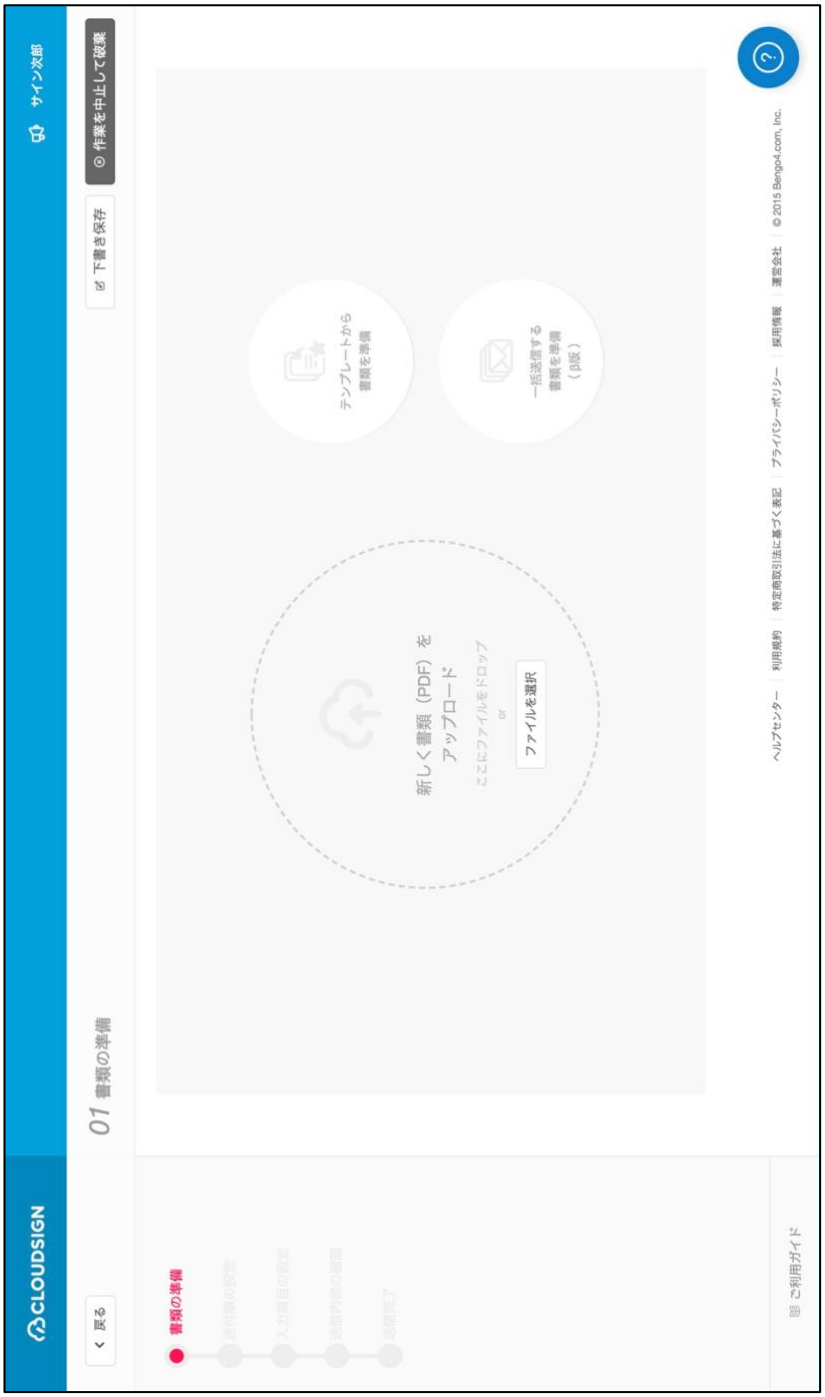
図表４：別紙１の④


CLOUDSIGN
アカウント登録確認
パスワードを入力してアカウント登録を完了させてください。
アカウント登録を完了させる前に、利用規約をご確認ください。
パスワードを入力すると登録は完了です。
アカウント登録を完了させることにより、利用規約に同意されたものとみなされます。
パスワード 必須
登録

図表５：別紙１の⑤

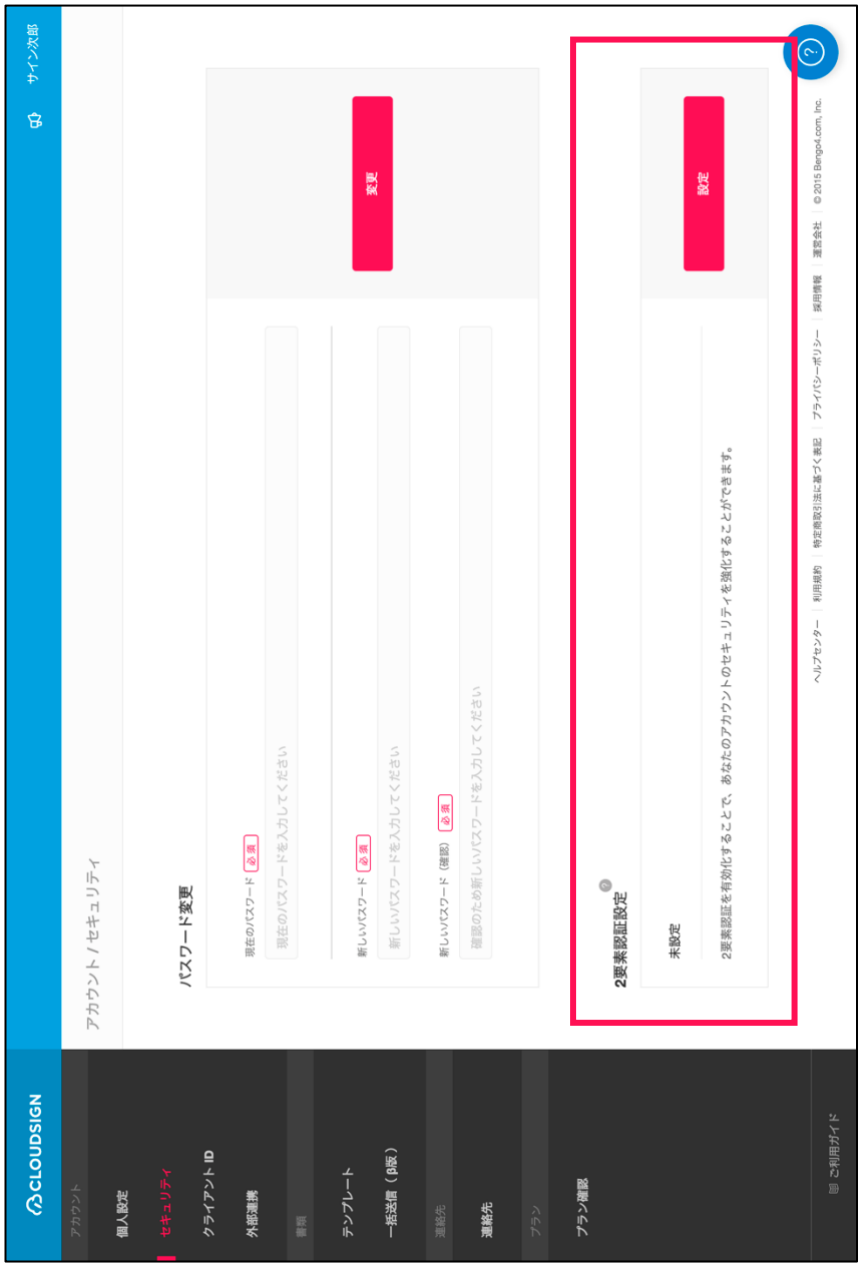

ユーザー登録が完了しました。
まずはお客さまの情報を入力してください。
氏名
必須
クラウド 太郎
会社名
任意
株式会社Cloud
保存
資料請求
サービス説明資料
電子契約のAPI連携事例
承継問題を解決
ヘルプセンター
よくある質問

図表６：本文の第２・１③

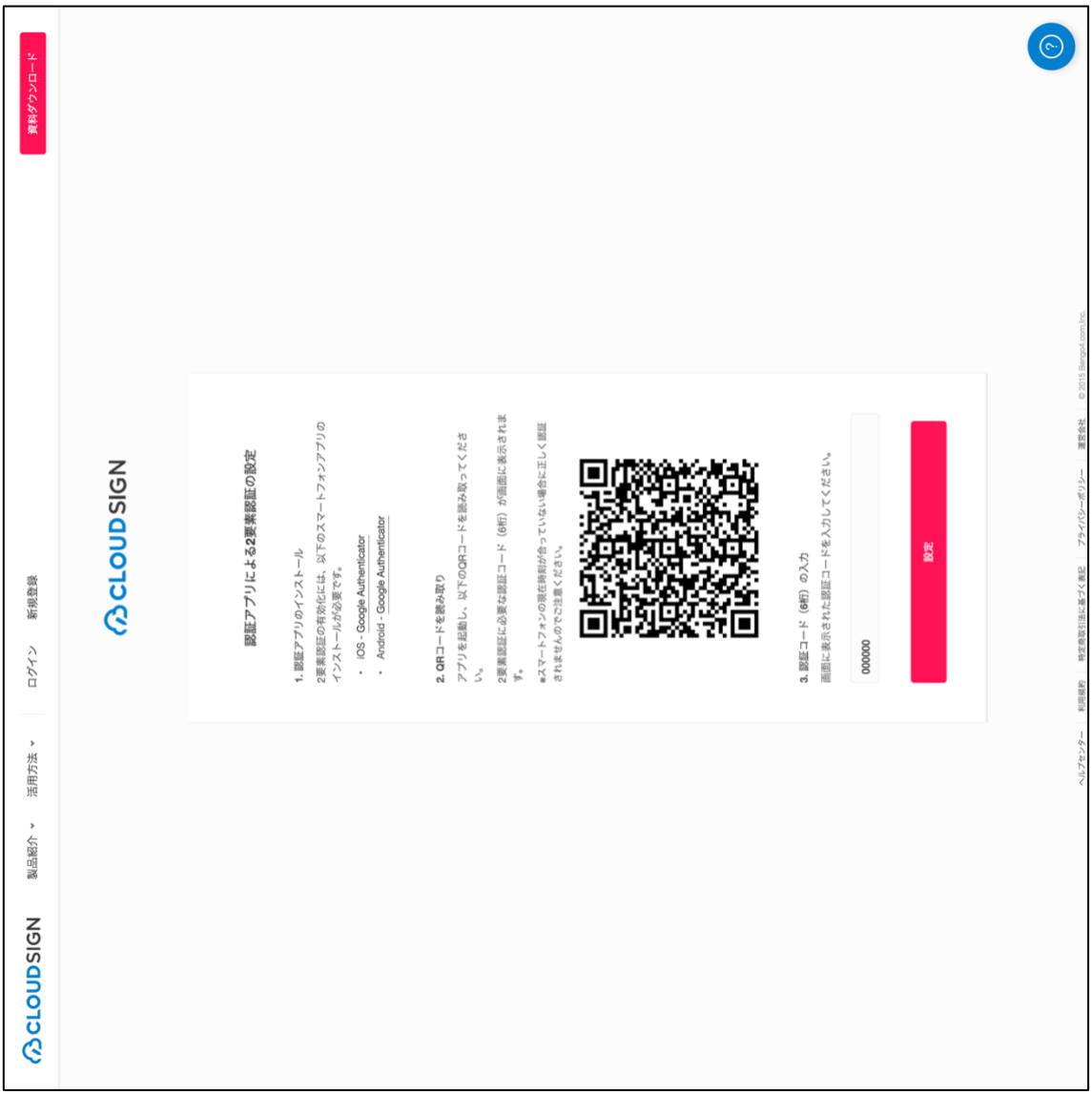

CLOUDSIGN
サイン次郎
戻る
01 書類の準備
下書き保存
作業を中止して破棄
書類の準備
テンプレートから
書類を準備
一括送信する
書類を準備
（β版）
新しく書類（PDF）を
アップロード
ここにファイルをドロップ
or
ファイルを選択
ご利用ガイド
ヘルプセンター
利用規約
特定商取引法に基づく表記
プライバシーポリシー
採用情報
運営会社
© 2015 Bengo4.com, Inc.

図表７：本文の第２・１③

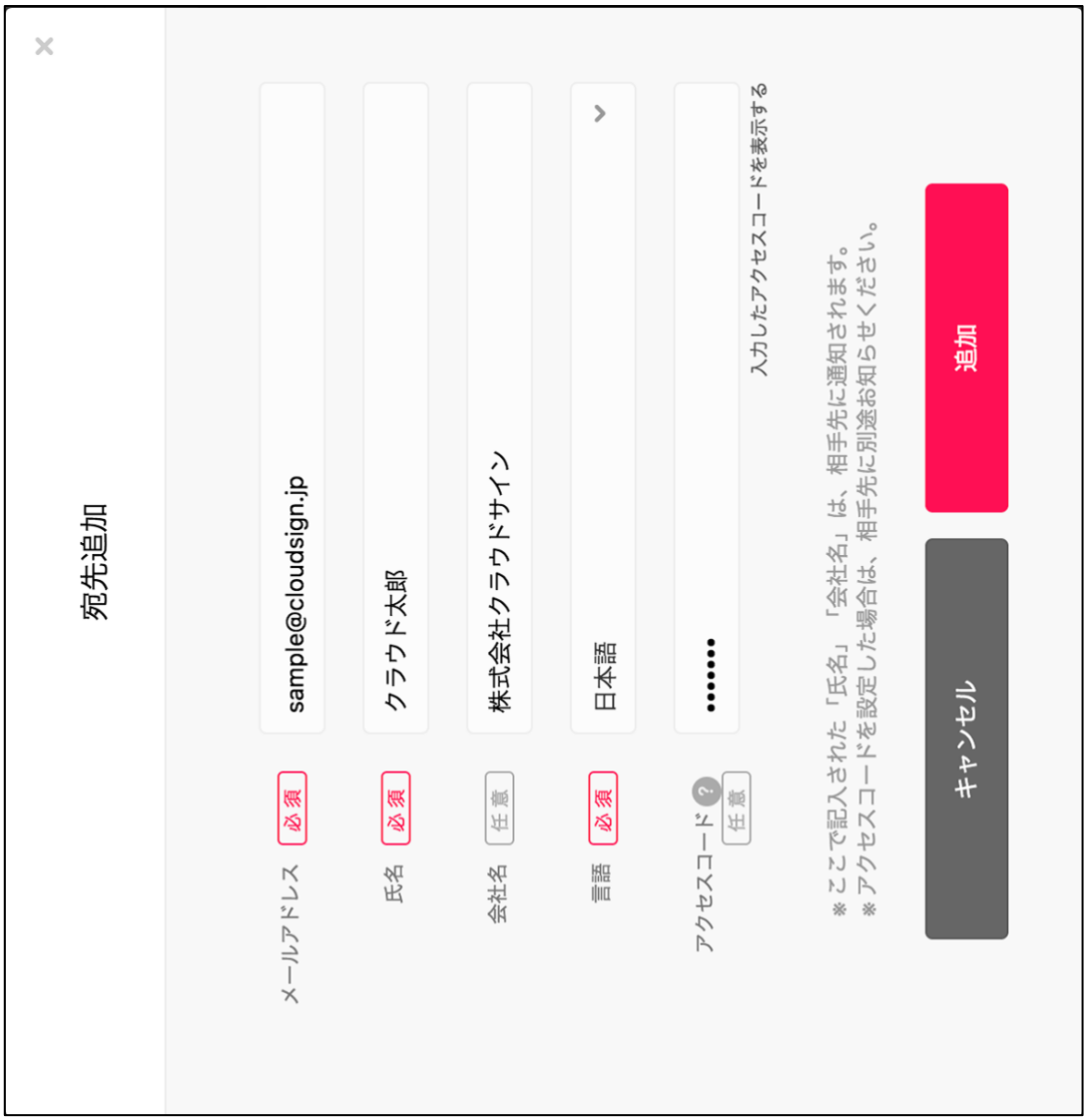
（管理画面のセキュリティ設定）



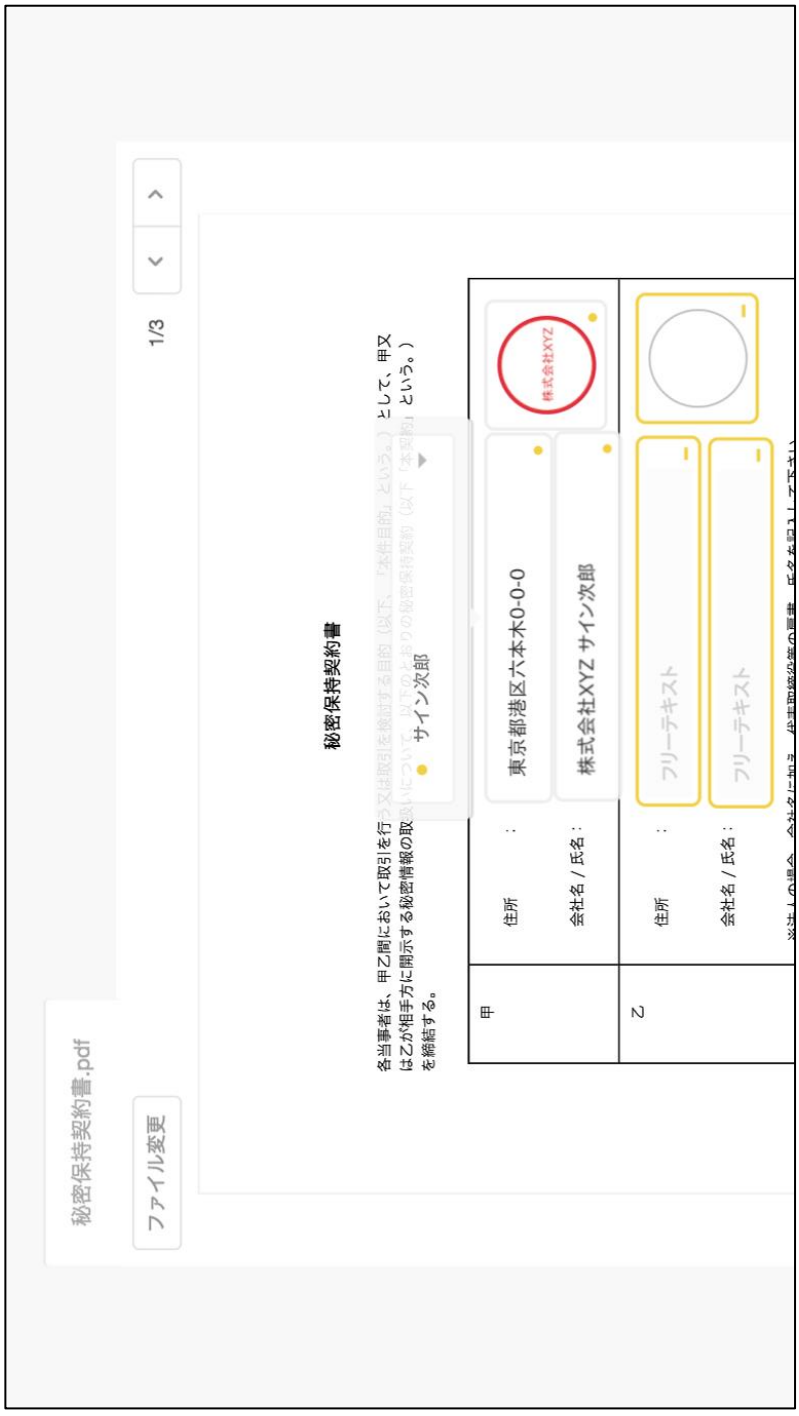
図表７：本文の第２・１③
（スマートフォンアプリを用いた２要素認証設定）



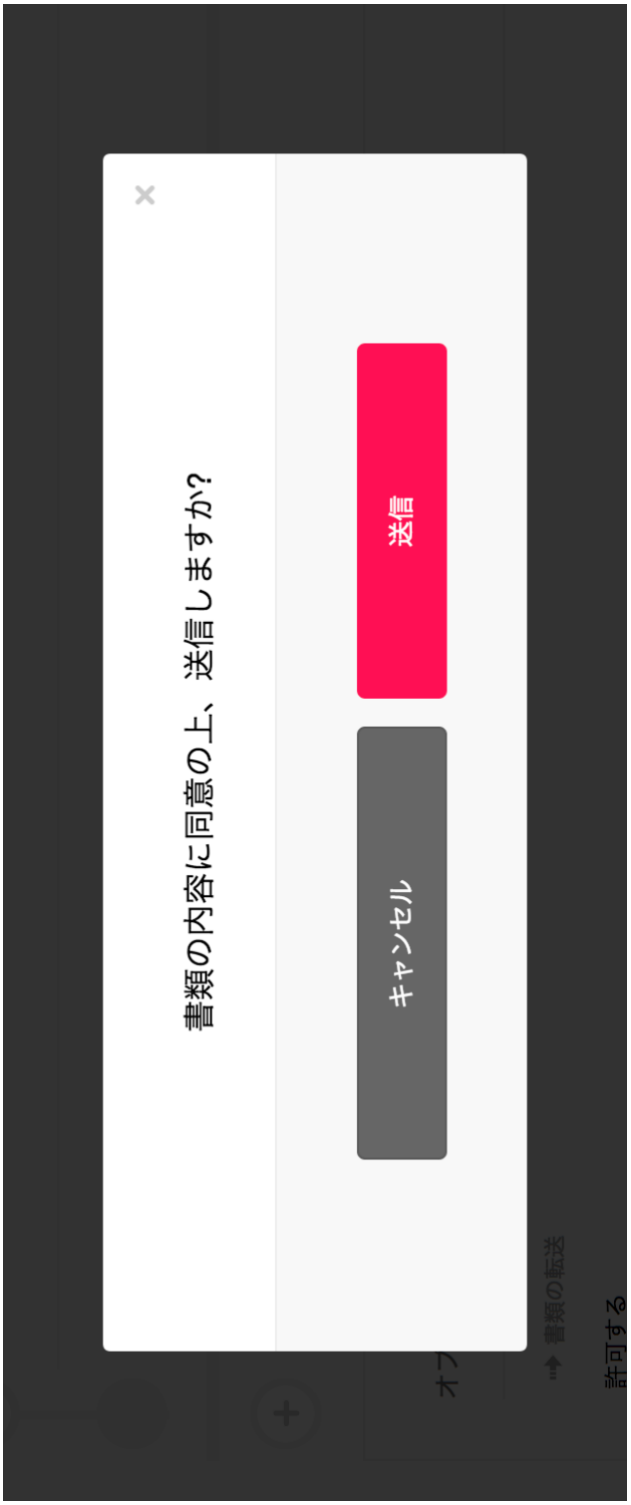
図表８：本文の第２・１④


宛先追加
メールアドレス
必須
sample@cloudsign.jp
氏名
必須
クラウド太郎
会社名
任意
株式会社クラウドサイン
言語
必須
日本語
アクセスコード
任意
入力したアクセスコードを表示する
※ここで記入された「氏名」「会社名」は、相手先に通知されます。
※アクセスコードを設定した場合は、相手先に別途お知らせください。
キャンセル
追加

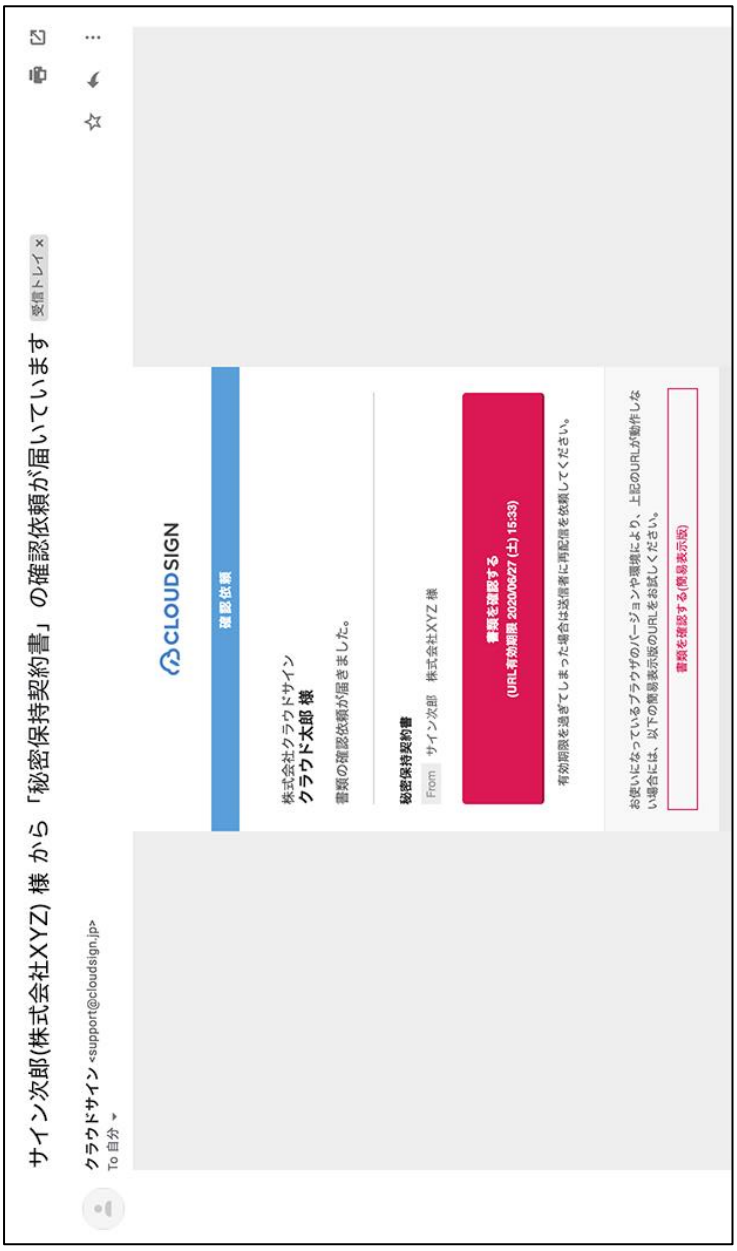
図表９：本文の第２・１⑤


秘密保持契約書.pdf
ファイル変更
1/3
秘密保持契約書
各当事者は、甲乙間において取引を行う又は取引を検討する目的（以下、「本件目的」という。）として、甲又はこが相手方に開示する秘密情報の取扱いについて、以下のとおり秘密保持契約（以下「本契約」という。）を締結する。
サイン次郎
甲
住所：東京都港区六本木0-0-0
会社名 / 氏名：株式会社XYZ サイン次郎
株式会社XYZ
乙
住所：フリーテキスト
会社名 / 氏名：フリーテキスト

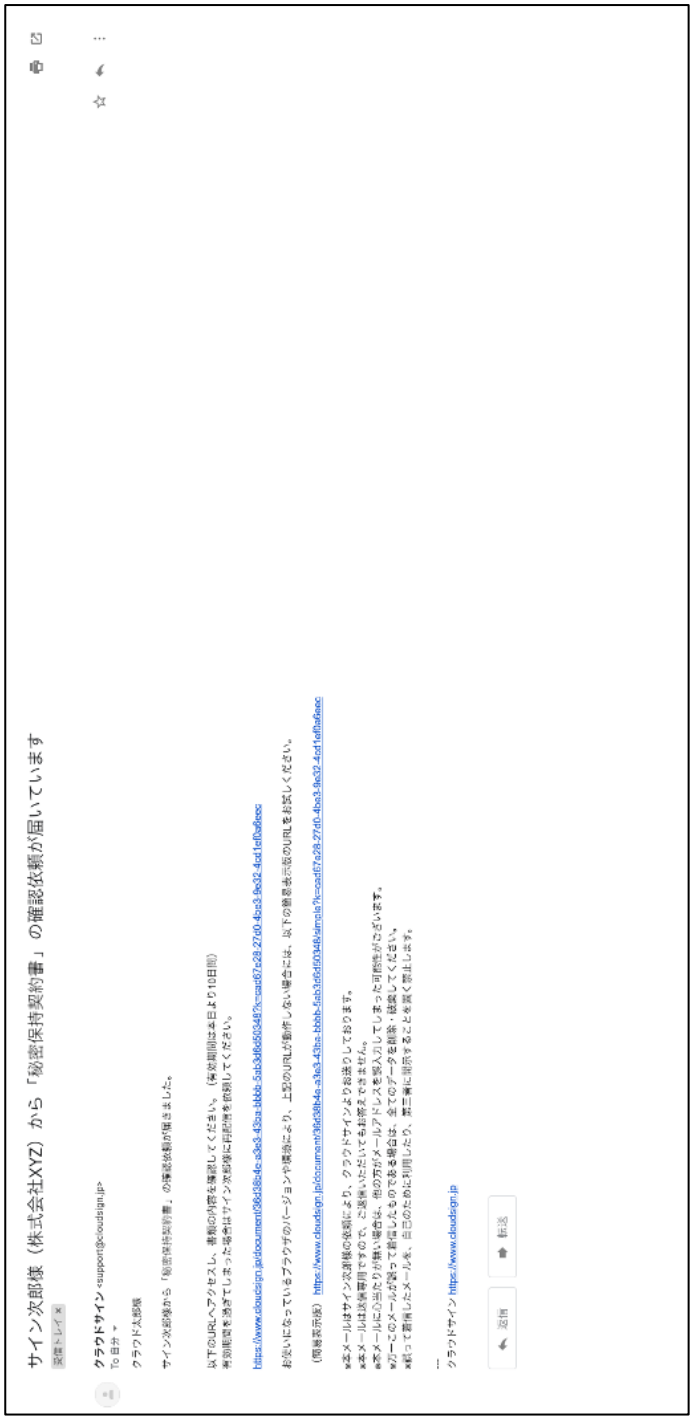
図表１０：本文の第２・１⑥



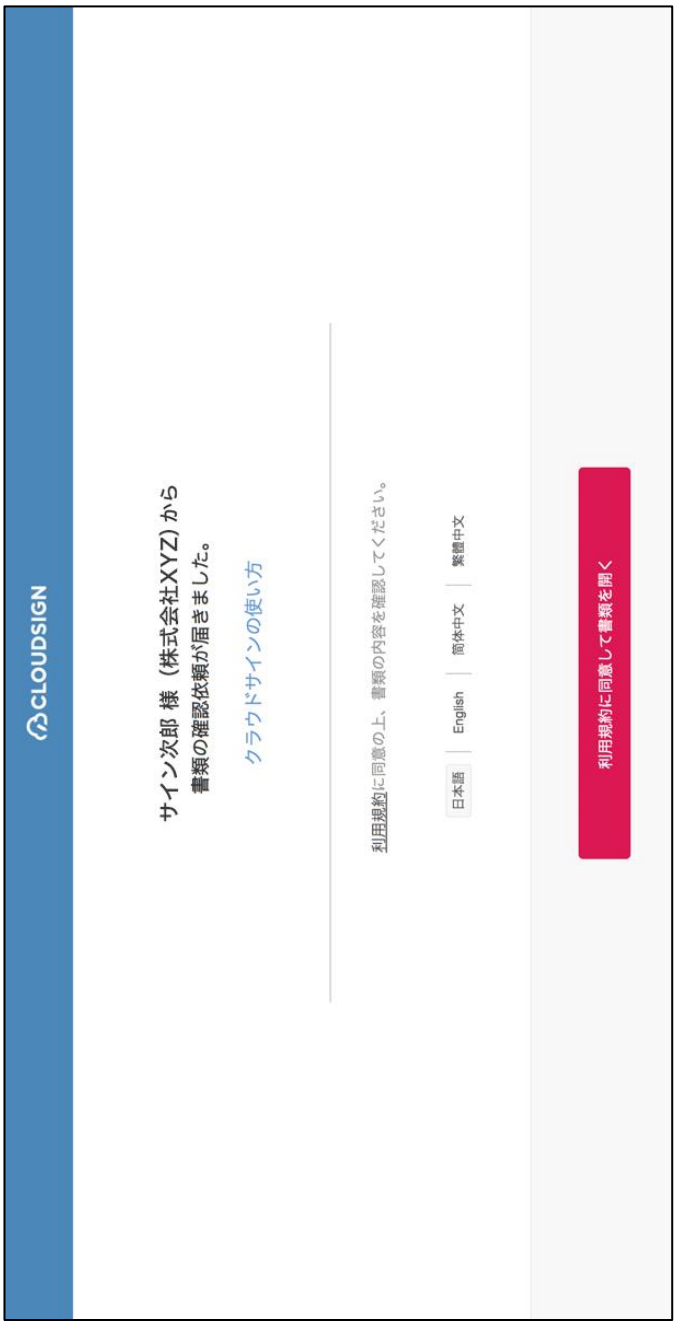
図表１１：本文の第２・１⑦
（HTML メールの場合）



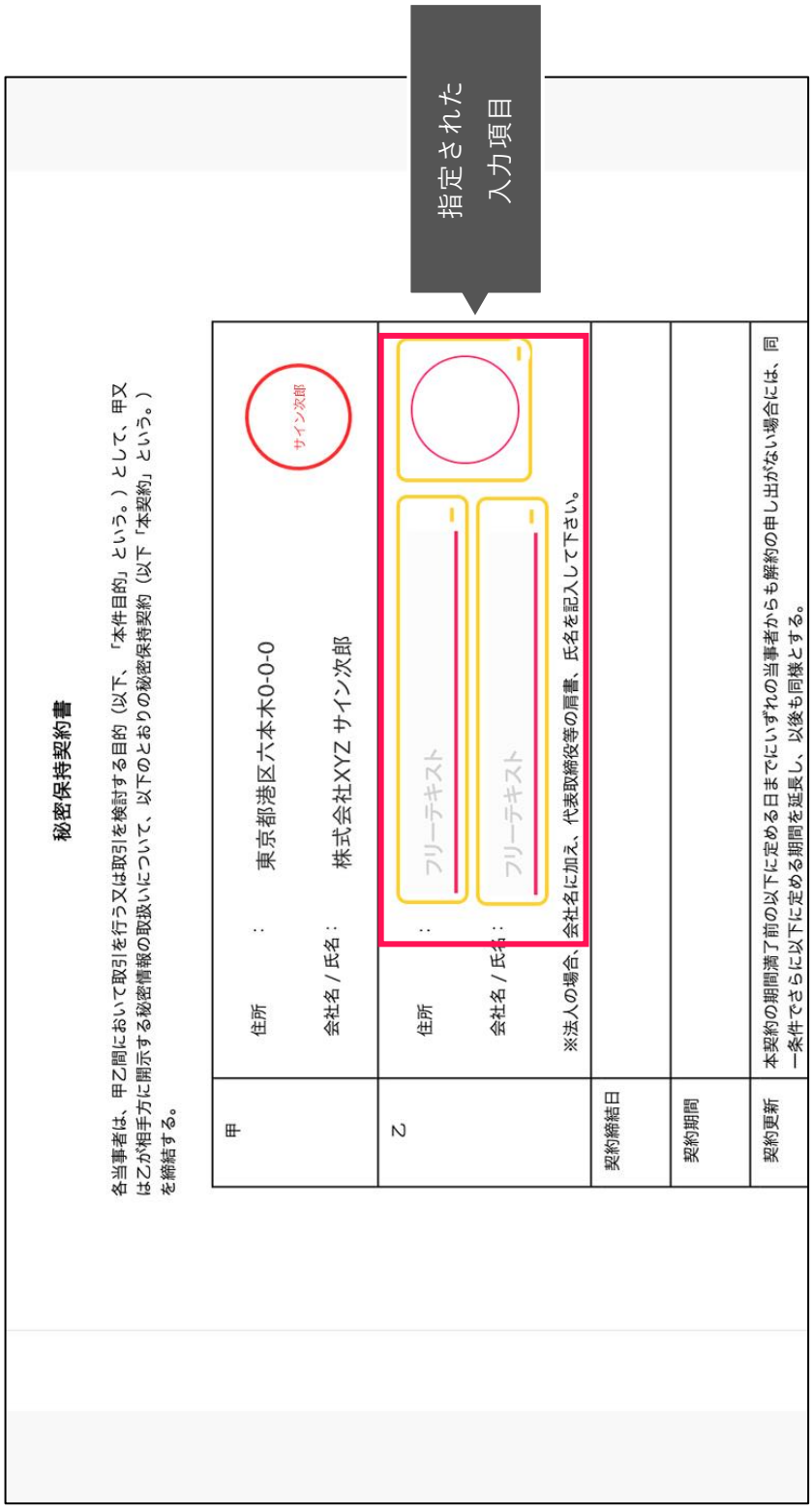
図表１１：本文の第２・１⑦
（テキストメールの場合）



図表１２：本文の第２・１⑧

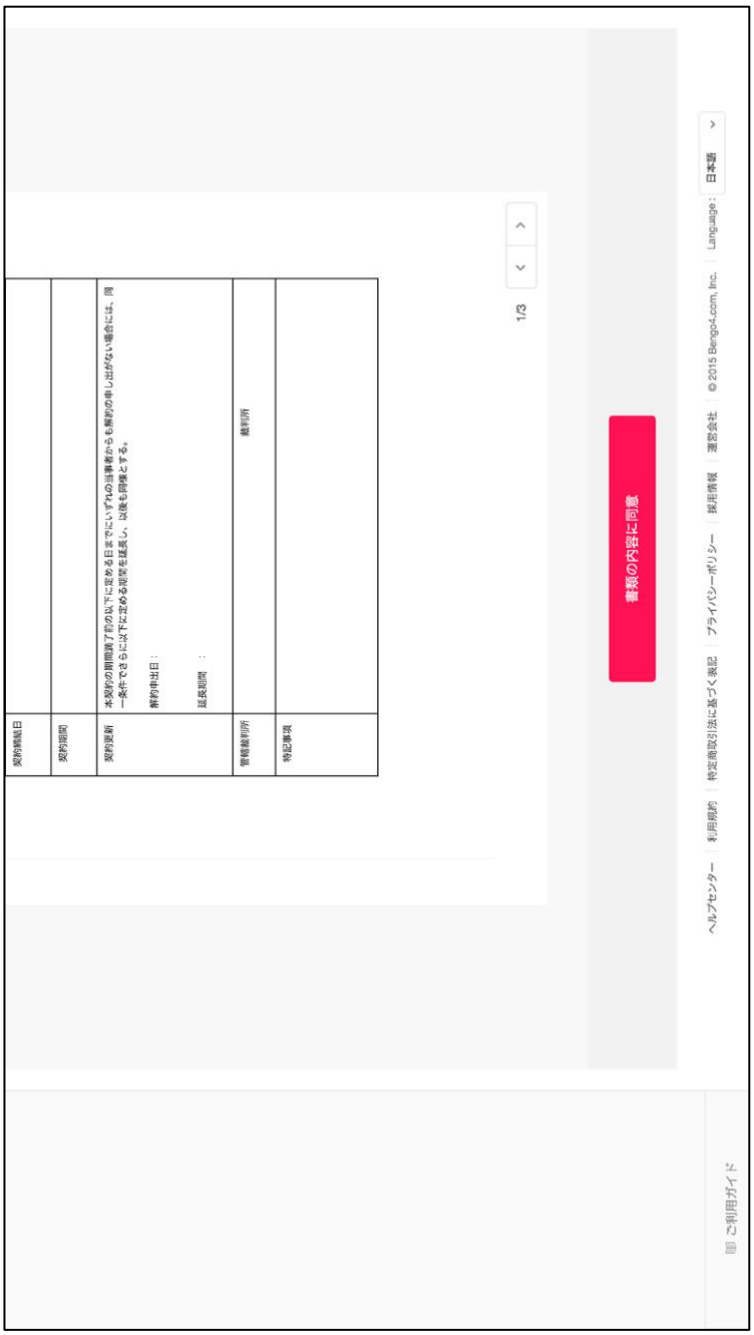


図表１３：本文の第２・１⑨



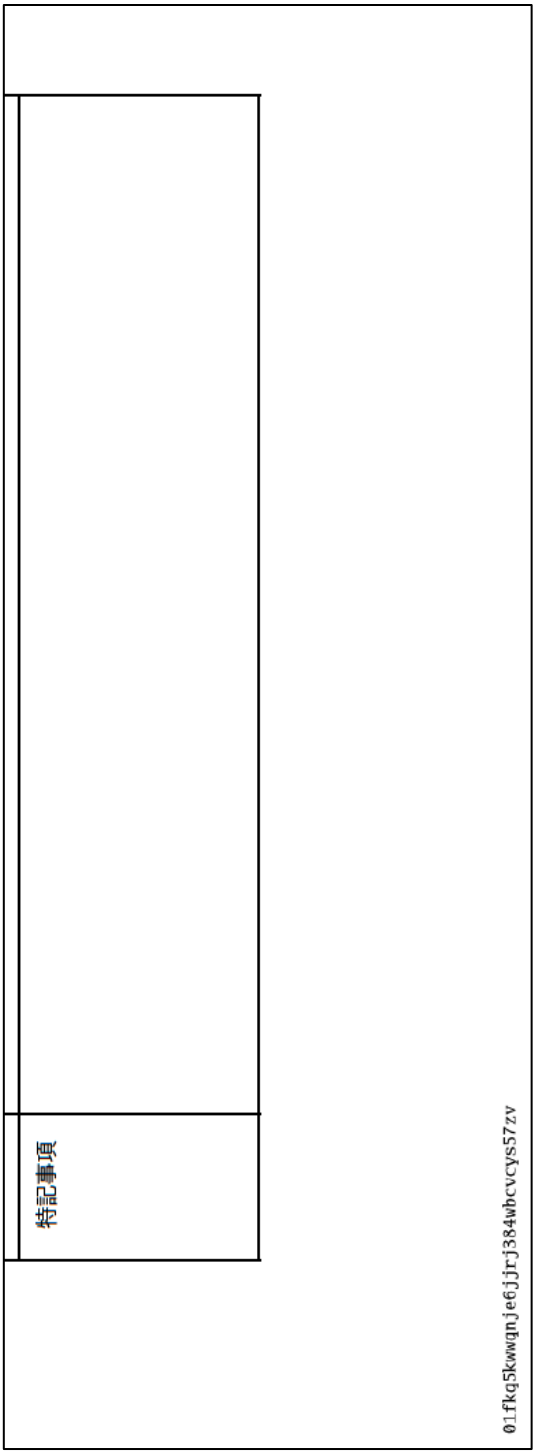
図表１４：本文の第２・１⑨

図表１５：本文の第２・１⑩

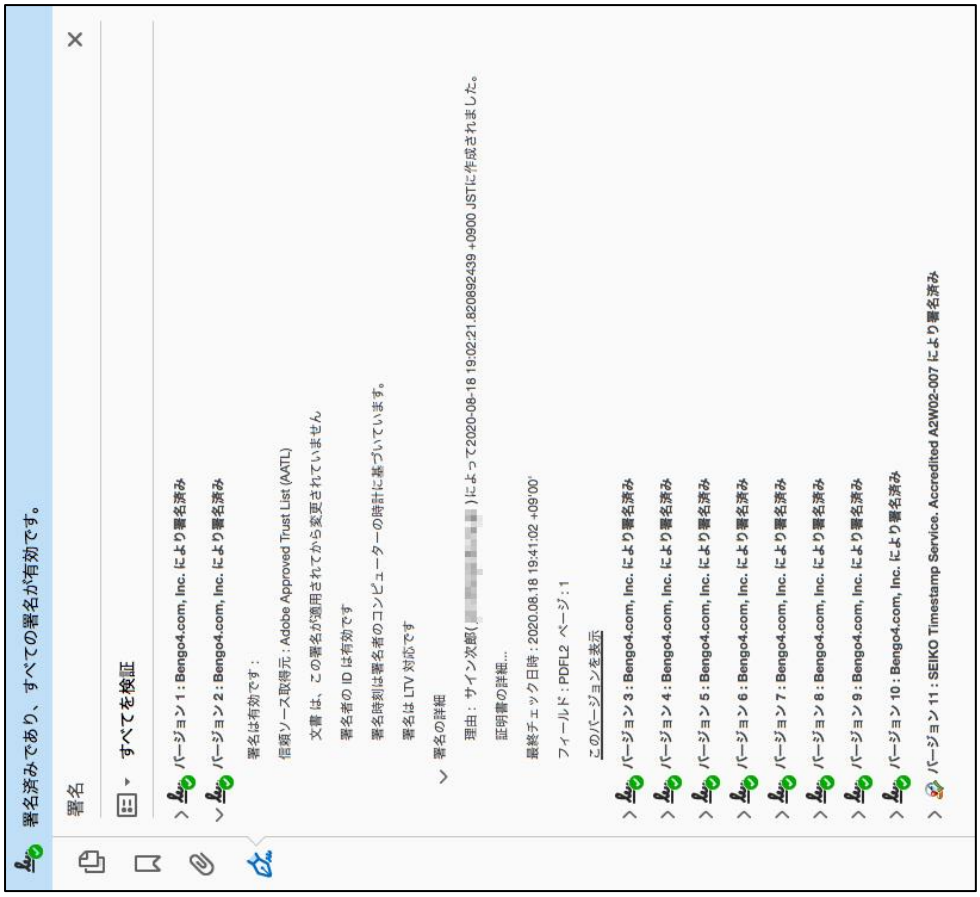


図表１６：本文の第２・１⑩

図表１７：本文の第２・１⑪



図表１８：本文の第４・３


署名済みであり、すべての署名が有効です。
署名
すべてを検証
バージョン 1 : Bengo4.com, Inc. により署名済み
バージョン 2 : Bengo4.com, Inc. により署名済み
署名は有効です：
信頼ソース取得元 : Adobe Approved Trust List (AATL)
文書 は、この署名が適用されてから変更されていません
署名者の ID は有効です
署名時刻は署名者のコンピューターの時計に基づいています。
署名は LTV 対応です
署名の詳細
理由： サイン次郎( )によって2020-08-18 19:02:21.820892439 +0900 JSTに作成されました。
証明書の詳細...
最終チェック日時 : 2020.08.18 19:41:02 +09'00'
フィールド : PDFL2 ページ : 1
このバージョンを表示
バージョン 3 : Bengo4.com, Inc. により署名済み
バージョン 4 : Bengo4.com, Inc. により署名済み
バージョン 5 : Bengo4.com, Inc. により署名済み
バージョン 6 : Bengo4.com, Inc. により署名済み
バージョン 7 : Bengo4.com, Inc. により署名済み
バージョン 8 : Bengo4.com, Inc. により署名済み
バージョン 9 : Bengo4.com, Inc. により署名済み
バージョン 10 : Bengo4.com, Inc. により署名済み
バージョン 11 : SEIKO Timestamp Service. Accredited A2W02-007 により署名済み