平成２６年１１月２１日判決言渡　同日原本交付　裁判所書記官

平成２６年（ワ）第１４０８６号　損害賠償請求事件

口頭弁論終結日　平成２６年９月２６日

判　　決

横浜市都筑区＜以下略＞

原　　告　　クオード株式会社

東京都千代田区＜以下略＞

被　　告　　株式会社エヌ・ティ・ティ・データ経営研究所

同訴訟代理人弁護士　　升　永　英　俊

同補佐人弁理士　　佐　藤　　睦

主　　文

１　原告の請求を棄却する。

２　訴訟費用は原告の負担とする。

事　実　及　び　理　由

第１　請求

１　被告は，原告に対し，１５０万円及びこれに対する平成２６年６月２５日から支払済みまで年５分の割合による金員を支払え。

２　仮執行宣言

第２　事案の概要

１　前提となる事実（証拠を掲げていない事実は当事者間に争いがない。以下，証拠番号の枝番を省略することがある。）

(1) 原告の有する特許権

ア　原告は，次の特許権を有している（以下「本件特許権」といい，本件特許権に係る特許を「本件特許」という。）。

発明の名称　　内容証明を行う通信システムおよび内容証明サイト装置

特許番号　　第３７９６５２８号

出　願　日　　平成１１年１２月２８日

登　録　日　　平成１８年４月２８日

イ　本件特許の特許請求の範囲，明細書及び図面の内容は，別紙特許公報記載のとおりである（以下，上記明細書及び図面を「本件明細書等」という。）。

ウ　本件特許の特許請求の範囲

本件特許の特許請求の範囲における請求項の数は１４であるが，そのうち請求項８の記載は，別紙特許公報の特許請求の範囲【請求項８】記載のとおりである（以下，同請求項記載の発明を「本件発明」という。）。

(2) 構成要件の分説

本件発明を構成要件に分説すると次のとおりである。

１　発信者の装置から暗号化された状態で送信された伝達情報が，ネットワークを介して受信者の装置に受信されて復号化されたことを証明する内容証明サイト装置であって，

２　前記発信者装置から，該発信者装置が送信した伝達情報の内容の同一性を確認できるデータに該発信者が電子署名した発信者署名データを受け取る第１の受信手段と，

３　前記受信者装置から，該受信者装置が受け取って復号化した伝達情報の内容の同一性を確認できるデータに該受信者が電子署名した受信者署名データを受け取る第２の受信手段と，

４　前記発信者装置から受け取った前記発信者署名データと前記受信者装置から受け取った前記受信者署名データとを内容証明を行うために保管する保管手段と，

５　前記内容証明の一環として，前記発信者署名データのうち，前記発信者装置が送信した伝達情報の内容の同一性を確認できるデータと，前記受信者署名データのうち，前記受信者装置が受け取って復号化した伝達情報の内容の同一性を確認できるデータとを照合する手段と，を備え，

6　前記発信者装置が送信した伝達情報の内容の同一性を確認できるデータが，該発信者装置が送信した伝達情報のダイジェスト又は該伝達情報を暗号化した暗号情報のダイジェストに限られ，

7　前記受信者装置が受け取って復号化した伝達情報の内容の同一性を確認できるデータが，該受信者装置が受け取って復号化した伝達情報のダイジェスト又は該伝達情報を暗号化した暗号情報のダイジェストに限られている，

ことを特徴とする内容証明サイト装置。

(3) 被告の原本性証明装置及び被告の行為

被告は，顧客に対し，「ＣＥＣＴＲＵＳＴ」と称する電子契約サービス（以下「ＣＥＣサービス」という。）を行うに当たり，原本性証明装置（以下「ＣＥＣサーバ」という。）を使用して，内容証明の一環として原本性証明を行っている。〔甲２，弁論の全趣旨〕

(4) ＣＥＣサーバは本件発明の構成要件１ないし４を充足する。

２　本件は，本件特許権を有する原告が，被告に対し，被告が顧客と契約して実施している内容証明の一環としての原本性証明に係る装置であるＣＥＣサーバは，本件発明の技術的範囲に属し本件特許権を侵害すると主張して，民法７０９条に基づき，不法行為による損害賠償請求（一部請求）として１５０万円及びこれに対する平成２６年６月２５日（訴状送達の日の翌日）から支払済みまで民法所定の年５分の割合による遅延損害金の支払を求めた事案である。

３　本件の争点

(1) ＣＥＣサーバは，本件発明の技術的範囲に属するか

ア　構成要件５の充足性

イ　構成要件６及び７の充足性

(2) 損害発生の有無及びその額

第３　争点に関する当事者の主張

1　争点(1)ア（構成要件５の充足性）について

〔原告の主張〕

ＣＥＣサーバは，契約者（甲）の署名データのうち，同契約者が送信した電子契約文書の内容の同一性を確認できる照合値εと，契約者（乙）の署名データのうち，同契約者が受け取って復号化した電子契約文書の内容の同一性を確認できる照合値ζを照合している。

ＣＥＣサーバにおける原本性証明は本件発明の「内容証明」に，契約者（甲）の署名データは「発信者署名データ」に，契約者（甲）は「発信者装置」に，契約者（甲）の署名データのうち同契約者が送信した電子契約文書の内容の同一性を確認できるデータが「発信者装置が送信した伝達情報の内容の同一性を確認できるデータ」に，契約者（乙）の署名データは「受信者署名データ」に，契約者（乙）は「受信者装置」に，契約者（乙）の署名データのうち電子契約文書の内容の同一性が確認できるデータは「受信者装置が受け取って復号化した伝達情報の内容の同一性を確認できるデータ」にそれぞれ該当する。

これに対して被告は，ＣＥＣサーバは発注者の電子署名した文書と受注者の電子署名した文書が同一であるか否かを照合するサービスを一切提供していないから，構成要件５の「照合する手段」を備えていないと主張する。しかし，原本性を検証する契約書データＤから算出してある照合値をδとすると，ＣＥＣサーバにおいては，発信者署名データのうち，発信者Ａが送信した契約書Ｄの内容の同一性を確認できる照合値εをもって，上記δと照合し，受信者署名データのうち，受信者Ｂが受け取って復号化した契約書Ｄの内容の同一性を確認できる照合値ζをもって，上記δと照合しているから，構成要件５の「照合する手段」を充足する。

したがって，ＣＥＣサーバは，構成要件５を充足する。

〔被告の主張〕

ＣＥＣサーバにおける原本性証明の処理態様は，別紙「図１　ＣＥＣＴＲＵＳ

Ｔ処理ステップ抜粋」（以下「本件処理ステップ」という。）のとおりである。

ＣＥＣサービスでは，受注者が電子署名をして発注者に送信した文書について，発注者が「完了の確認」の文字をクリックして当該契約締結案件を完了すると，当該文書にタイムスタンプを登録し，案件完了時以降１０年間当該文書を保管し，発注者又は受注者の求めに応じて，「案件完了時以降，保管中の当該文書が非改ざんであること」の「原本性検証」をするというサービスを提供するだけである。

ＣＥＣサーバは発注者の電子署名した文書と受注者の電子署名した文書が同一であるか否かを照合するサービスを一切提供していないから，構成要件５の「照合する手段」を備えていない。

したがって，ＣＥＣサーバは，構成要件５を充足しない。

２　争点(1)イ（構成要件６及び７の充足性）について

〔原告の主張〕

(1) 構成要件６について

ＣＥＣサーバでは，契約者（甲）の署名データのうち，契約者（甲）が送信した電子契約文書の内容の同一性を確認できるデータεは，契約者（甲）が送信した電子契約文書のダイジェスト（ハッシュ）に限られている。

契約者（甲）は本件発明の「発信者装置」に，契約者（甲）の署名データのうち，契約者（甲）が送信した電子契約文書の内容の同一性を確認できるデータは「発信者装置が送信した伝達情報の内容の同一性を確認できるデータ」に，契約者（甲）の署名データのうち電子契約文書の照合値は「発信者装置が送信した伝達情報のダイジェスト」にそれぞれ該当する。

したがって，ＣＥＣサーバは，構成要件６を充足する。

(2) 構成要件７について

ＣＥＣサーバでは，契約者（乙）の署名データのうち，契約者（乙）が受け取って復号化した電子契約文書の内容の同一性を確認できるデータζは，契約者（乙）が受け取って復号化した電子契約文書のダイジェスト（ハッシュ）に

限られている。

契約者（乙）は本件発明の「受信者装置」に，契約者（乙）の署名データのうち契約者（乙）が受け取って復号化した電子契約文書の内容の同一性を確認できるデータは「受信者装置が受け取って復号化した伝達情報の内容の同一性を確認できるデータ」に，契約者（乙）の署名データのうち電子契約文書の照合値は「受信者装置が受け取って復号化した伝達情報のダイジェスト」にそれぞれ該当する。

したがって，ＣＥＣサーバは，構成要件７を充足する。

〔被告の主張〕

原告は，本件特許の審査経過において提出された平成１７年１２月１６日付け手続補正書（方式）（乙１。以下「本件手続補正書」という。）において，「伝達情報」が，「発信者装置」又は「受信者装置」から「内容証明サイト装置」に送られることを明確に除外している。そうすると，構成要件６及び７の「伝達情報」は，「発信者装置」又は「受信者装置」から「内容証明サイト装置」に送られるものではないと解するのが相当である。

そして，ＣＥＣサービスでは，伝達情報である契約書がＣＥＣサーバに送信されるから，ＣＥＣサーバは構成要件６及び７をいずれも充足しない。

３　争点(2)（損害発生の有無及びその額）について

〔原告の主張〕

被告がＣＥＣサービスによって過去３年間に得た利益は，２億１０００万円を下回ることはないのであり，少なくともその額が被告の侵害行為によって原告が失った得べかりし利益というべきである。

そこで，原告は，一部請求として，被告に対し，１５０万円及び訴状送達の日の翌日である平成２６年６月２５日から支払済みまで民法所定の年５分の割合による遅延損害金の支払を求める。

〔被告の主張〕

否認ないし争う。

第４　当裁判所の判断

１　本件発明の意義

本件明細書等の【発明の詳細な説明】の段落【０００１】ないし【０００６】，【００２１】及び図１ないし図５によれば，本件発明は，インターネット等のネットワークを用いて送受信する伝達情報の内容証明を行う通信システムと内容証明サイト装置に関するものであり，従来，インターネット等のネットワークでは，通信を行っている者の本人確認をパスワードや公開鍵暗号などにより行う電子認証（デジタル認証）や，送る伝達情報に公開鍵暗号などにより署名を入れる電子署名（デジタル署名）などがよく知られていたが，ネットワーク上における伝達情報の内容証明，すなわち，ある発信者から送られたある伝達情報がある受信者に渡されたことを第三者が内容証明を行うという技術はなかったため，本件特許は，かかるネットワーク上における伝達情報の内容証明を行うことを目的とし，特に，本件発明は，特許請求の範囲請求項８記載の構成を採用することにより，保管手段に保管されている発信者署名データと受信者署名データとに基づいて，発信者と受信者の本人確認及び発信者が送った伝達情報と受信者が受け取って復号化した伝達情報の同一性確認を行うことができ，それにより伝達情報に関する内容証明を第三者の立場で行うことができるようにした発明であると認められる。

２　争点(1)ア（構成要件５の充足性）について

(1) 本件発明における「照合する手段」の意義

ア　本件明細書等には，次の記載がある。

・「以下，図２に示すシーケンス図と，図３～図５に示すフローチャートを参照してこの実施例システムの動作概要を説明する。この図２のシーケンス図では，左側から順に発信側端末Ａ，内容証明サーバＣ，認証サーバＮ，受信側端末Ｂが配置され，それらの間でネットワークを介して受け渡され

るデータの種類が図中に書き込まれている。これらのデータ中，〔α〕βの表記は，データαが鍵βで暗号化されていることを表す。また，〔α，ε〕βの表記は，データαとデータεがそれぞれ鍵βで暗号化されていることを表し，〔α〕βと〔ε〕βとが各々独立してあることと等価であるものとする。さらに，（γ）xという表記は，サイトＸでデータγをダイジェスト化（後述する）した値であることを表している。」（段落【００２１】）

・「また，図３～図５は発信側端末Ａ，受信側端末Ｂ，内容証明サーバＣにおいて各々実行される処理手順をフローチャートの形で示したものである。これらの図では，発信者たる発信側端末Ａが伝達情報Ｄを受信者たる受信側端末Ｂに内容証明サイト１の内容証明サーバＣ経由で送り，内容証明サイト１ではその伝達情報Ｄを受け渡すにあたりその内容証明を行うものとする。」（段落【００２２】）

・「まず，発信側端末Ａが内容証明サーバＣに内容証明付の通信を行うことを要求する。この際，発信側端末Ａは，以下の処理を行う（ステップＡ１）。すなわち，送りたい伝達情報Ｄを用意するとともに，この伝達情報Ｄを暗号化するための共通鍵暗号方式の共通鍵（秘密鍵とも称する）Ｒを生成する。この共通鍵Ｒとしては例えば乱数などが利用できる。この共通鍵Ｒを用いて伝達情報Ｄを暗号化して暗号文〔Ｄ〕Ｒを作成する。この共通鍵Ｒの生成は，発信側端末Ａがこの内容証明通信を行う毎に新たなものに変更して生成しており，それにより通信機密性の高いセキュリティを確保している。」（段落【００２４】）

・「さらに，この暗号文〔Ｄ〕Ｒと伝達情報Ｄとをそれぞれハッシュ関数などで変換演算を行って圧縮してダイジェスト値（〔Ｄ〕Ｒ）ａとダイジェスト値（Ｄ）ａ を得る。」（段落【００２６】）

・「この暗号化された伝達情報のダイジェスト値（〔Ｄ〕Ｒ）ａと伝達情報

のダイジェスト値（D）a とを発信側端末Aの秘密鍵（プライベート鍵）ＳKa で暗号化した暗号文〔（〔D〕R）a，（D）a〕ＳKa を作成する。この暗号文〔（〔D〕R）a，（D）a〕ＳKa は，それを受け取った側にて，発信側端末Aの公開鍵（パブリック鍵）ＰKa を用いて暗号解読できることで,その発信者が発信側端末Aであると本人確認でき,また,ダイジェスト値（〔D〕R）a とダイジェスト値（D）a は発信側端末Aが送った伝達情報Dの内容を一意的に特定して内容の完全性(変更されていないこと）を確認できるデータであるので，本発明における発信者の本人確認と伝達情報の内容特定とを行う電子署名データとして用いることができる。」（段落【００２８】）

・「そして，発信側端末Aは送信データとして以下のものを揃えて，インターネット４を介して内容証明サイト１の内容証明サーバCに送る(図３のステップＡ２）。

マル１アドレスＡＡ:発信元としての発信側端末Aのネットワーク上のアドレス

マル２アドレスＢＢ:受信先としての受信側端末Bのネットワーク上のアドレス

マル３暗号文〔〔（〔D〕R）a，（D）a〕ＳKa〕ＰKc ：

暗号化された伝達情報のダイジェスト値（〔D〕R）a と伝達情報のダイジェスト値（D）a とを発信側端末Aが秘密鍵ＳKa で電子署名した暗号文〔（〔D〕R）a，（D）a〕ＳKa を，内容証明サーバCの公開鍵ＰKc で暗号化した暗号文

マル４暗号文〔D〕R：伝達情報Dを共通鍵Rで暗号化した暗号文

マル５暗号文〔〔R，（R）a〕ＳKa〕ＰKc ：共通鍵Rとそのダイジェスト値（R）a を発信側端末Aが秘密鍵ＳKa で電子署名した暗号文〔R，（R）a〕ＳKa を，内容証明サーバCの公開鍵ＰKc で暗号化し

た暗号文」（段落【００３１】）

・「そして，内容証明サーバＣは，自己の秘密鍵ＳＫc を用いて暗号文〔〔（〔D〕R）a，（D）a〕ＳKa〕ＰKc と暗号文〔〔R，（R）a〕ＳKa〕ＰKc を暗号解読して，伝達情報に関するダイジェスト値の暗号文〔（〔D〕R）a，（D）a〕ＳKa と共通鍵に関する暗号文〔〔R，（R）a〕ＳKa を得る。この暗号解読をできるのは内容証明サーバＣだけであるので，通信の高い秘匿性が確保できる。」（段落【００３３】）

・「受信先の受信側端末Ｂは，内容証明サーバＣからデータを受信すると，そのうちの発信元アドレスＣＣに基づいて，内容証明サーバＣからの通信であることを認識する。」（段落【００３９】）

・「さらに，内容証明サーバＣから受信した伝達情報の暗号文〔D〕Ｒを発信側端末Ａ側と同じハッシュ関数を用いてダイジェスト化してダイジェスト値（〔D〕R）b を作成する（図４のステップＢ１）。」（段落【００４２】）

・「受信側端末Ｂは，内容証明サーバＣから受け取った発信日時Ｔa と自局算出のダイジェスト値（〔D〕R）b とに自局の秘密鍵ＳKb で電子署名して暗号文〔（〔D〕R）b，Ｔa〕ＳKb を作成し，この暗号文〔（〔D〕R）b，Ｔa〕ＳKb を受取証とする。この受取証〔（〔D〕R）b，Ｔa〕ＳKb は，これを受け取った側で受信側端末Ｂの公開鍵ＰKb を用いて暗号解読できることで，発信元が受信側端末Ｂであることを確認でき，また受信側端末Ｂが受け取った伝達情報の暗号文〔D〕Ｒの内容を一意的に特定して内容の完全性（変更されていないこと）を確認できるデータであるので，本発明における受信者の本人確認と伝達情報の内容特定とを行う電子署名データとして用いることができる。」（段落【００４４】）

・「受信側端末Ｂは，この受取証〔（〔D〕R）b，Ｔa〕ＳKb を内容証明サーバＣの公開鍵ＰKc で暗号化した暗号文〔〔（〔D〕R）b，Ｔa〕

ＳＫb〕ＰＫc を作成して，内容証明サーバＣに送る（ステップＢ３）。」（段落【００４５】）

・「この受取証〔（〔D〕Ｒ）ｂ，Ｔａ〕ＳＫb を受け取った内容証明サーバＣは，受信側端末Ｂの公開鍵ＰＫb を用いて暗号解読して，受信側端末Ｂで算出したダイジェスト値（〔D〕Ｒ）ｂを得る。この暗号解読により，この受取証〔（〔D〕Ｒ）ｂ，Ｔａ〕ＳＫb が受信側端末Ｂから発信されたものであることを本人確認できる。」（段落【００４６】）

・「さらに，発信側端末Ａ側から取得した発信側端末Ａ側算出のダイジェスト値（〔D〕Ｒ）a と，受信側端末Ｂ側で算出したダイジェスト値（〔D〕Ｒ）b とを照合する（ステップＣ７）。両者が一致している場合には，発信側端末Ａから送信された伝達情報の暗号文〔D〕Ｒはその内容が改ざん，破損などされずに完全な形のままで受信側端末Ｂに受信されたという伝達情報の完全性を確認することができる。また，発信日時Ｔa についても，受信側端末Ｂ側の電子署名を得ることができる。」（段落【００４７】）

・「この後，内容証明サーバＣは，受信側端末Ｂからの受取証〔（〔D〕Ｒ）b，Ｔa〕ＳＫb の受取日時Ｔb を確定する。そして，この受取日時Ｔb と，伝達情報の暗号文〔D〕Ｒを暗号解読するための共通鍵Ｒと，その共通鍵のダイジェスト値（Ｒ）a とに自己の秘密鍵ＳＫc で電子署名した暗号文〔〔Ｒ，（Ｒ）a，Ｔb〕ＳＫc を作成し，さらにこの暗号文を受信側端末Ｂ側の公開鍵ＰＫb で暗号化した暗号文〔〔〔Ｒ，（Ｒ）a，Ｔb〕ＳＫc〕ＰＫb を作成して受信側端末Ｂに送る。」（段落【００４８】）

・「受信側端末Ｂは，この受け取った暗号文〔〔〔Ｒ，（Ｒ）ａ，Ｔb〕ＳＫc〕ＰＫb を，自己の秘密鍵ＳＫb と内容証明サーバＣの公開鍵ＰＫc を用いて暗号解読して，共通鍵Ｒとそのダイジェスト値（Ｒ）ａ，さらに受取日時Ｔb を取得する。そして，この共通鍵Ｒを用いて，先に内容証明サーバＣから受け取った伝達情報の暗号文〔D〕Ｒを暗号解読して伝達情

報Ｄを得る。そして，この伝達情報Ｄを，ハッシュ関数を用いてダイジェスト化して伝達情報のダイジェスト値（Ｄ）ｂ を作成する（図４のステップＢ４）。」（段落【００４９】）

・「この伝達情報のダイジェスト値（Ｄ）ｂ と受取日時Ｔｂ に自己の秘密鍵ＳＫｂ で電子署名した暗号文〔（Ｄ）ｂ，Ｔｂ〕ＳＫｂ を作成し，これを暗号解読済証（受取証）とする。この暗号解読済証〔（Ｄ）ｂ，Ｔｂ〕ＳＫｂ を更に内容証明サーバＣの公開鍵ＰＫｃ で暗号化することで，通信の秘匿化を図った上で内容証明サーバＣに送る（図５のステップＢ５）。」（段落【００５０】）

・「内容証明サーバＣは，受信した暗号文を自己の秘密鍵ＳＫｃ で暗号解読して暗号文〔（Ｄ）ｂ，Ｔｂ〕ＳＫｂ を得て，この暗号文〔（Ｄ）ｂ，Ｔｂ〕ＳＫｂ を受信側端末Ｂの電子署名入の暗号解読済証（受取証）とする。さらに，この暗号解読済証〔（Ｄ）ｂ，Ｔｂ〕ＳＫｂ を受信側端末Ｂの公開鍵ＰＫｂ で暗号解読してダイジェスト値（Ｄ）ｂ と受取日時Ｔｂ を得る。この受信側端末Ｂ側作成のダイジェスト値（Ｄ）ｂ と発信側端末Ａ側から受信した発信側端末Ａ側作成のダイジェスト値（Ｄ）ａ とを照合し，内容が一致していれば，発信側端末Ａ側から送信された伝達情報の暗号文〔Ｄ〕Ｒは間違いなく受信側端末Ｂ側に受け取られて，そして伝達情報Ｄとして正しく暗号解読されたことが確認できる（図５のステップＣ９）。」（段落【００５１】）

イ　以上の記載によれば，本件発明は，内容証明の一環として，前記発信者署名データ（実施例の〔（〔Ｄ〕Ｒ）ａ，（Ｄ）ａ〕ＳＫａ）から作成される，前記発信者装置が送信した伝達情報の内容の同一性を確認できるデータ（実施例の（Ｄ）a，（〔Ｄ〕Ｒ）a）と，前記受信者署名データ（実施例の〔（〔Ｄ〕Ｒ）ｂ，Ｔａ〕ＳＫｂ）から作成される，前記受信者装置が受け取って復号化した伝達情報の内容の同一性を確認できるデータ（実施例の（Ｄ）b，（〔Ｄ〕

Ｒ）b）とを「照合」することによって，発信側端末Ａ側から送信された伝達情報の暗号文〔Ｄ〕Ｒが間違いなく受信側端末Ｂ側に受け取られて，伝達情報Ｄとして正しく暗号解読されたことを確認するものであると認められる。

⑵　ＣＥＣサーバにおける原本性証明の処理態様

ア　証拠（乙２，４，５，１２）及び弁論の全趣旨によれば，次の事実が認められる。

㋐「写真報告書１」と題する書面（乙２，５）及びＣＥＣサービスの「原本性検証」の表示画面（乙４）には，ＣＥＣサービスの処理手順につき，大要，次の内容が記載されている。

ａ　発注者（送信者）が電子署名付き契約書（パターン４－１署名済）を作成する。

ｂ　発注者がＣＥＣサーバにログインし，発注者の電子署名付き契約書（パターン４－１署名済）を送信する。

ｃ　受注者（受信者）はサーバにログインし発注者の電子署名付き契約書（パターン４－１署名済）を受注者端末に表示し，この発注者の電子署名付き契約書（パターン４－１署名済）に基づき修正したと思われる受注者のみの電子署名付き契約書（パターン４－２署名済）を作成するが，このとき受注者のみの電子署名付き契約書（パターン４－２署名済）には受注者の電子署名が２つ埋め込まれているものの，発注者の電子署名は埋め込まれていない。

ｄ　受注者がサーバに受注者のみの電子署名付き契約書（パターン４－２署名済）を送信する。

ｅ　発注者がサーバにログインし受注者のみの電子署名付き契約書（パターン４－２署名済）を発注者端末に表示すると，「案件内容に問題がない場合は，完了処理を行ってください」と表示され，内容を確認し「完

了の確認」ボタンを押すと，契約処理を完了し，ＣＥＣサーバは受注者のみの電子署名付き契約書を保管する。

ｆ　発注者は契約が完了した案件を検索し，電子署名付き契約書（パターン４－２署名済）を発注者端末に表示することができる。

ｇ　発注者が発注者端末に「原本性検証」画面を表示すると，同画面には，検証日，案件番号，ファイル名，タイムスタンプ検証結果（「案件完了時以降，改ざんされていません。」との記載）が表示される（乙４）。

(ｲ) 電子契約内容証明装置説明書（乙１２）の模式図には，ＣＥＣサービスにおいては，契約者（甲）及び契約者（乙）が電子署名された電子契約書（伝達情報）そのものをＣＥＣサーバに送付し，同サーバが当該電子契約書（伝達情報）を保管すること，「ＳｅｃｕｒｅＳｅａｌ（Ｒ）センタ」がタイムスタンプを発行し，同タイムスタンプをもって原本性確認がされることが記載されている。

(ｳ) ＣＥＣサーバにおいて，文書が発信者Ａ又は受信者Ｂから送られたものであるか，当該文書が誰かに改ざんされていないかを検証するために電子署名の検証（以下「署名検証」という。）が行われるが，署名検証の具体的態様は，本件処理ステップが示すように，ＣＥＣサーバが，発信者Ａから送信された文書Ｄ及び〔（Ｄ）ａ〕ＳＫａのうち，文書Ｄからダイジェスト（Ｄ）ｃを作成し，〔（Ｄ）ａ〕ＳＫａを復号化して（Ｄ）ａを得て，（Ｄ）ｃと（Ｄ）ａを照合することによって行われ，また，受信者Ｂから送信された文書Ｄ’及び〔（Ｄ’）ｂ〕ＳＫｂのうち，文書Ｄ’からダイジェスト（Ｄ’）ｃを作成し，〔（Ｄ’）ｂ〕ＳＫｂを復号化して（Ｄ’）ｂを得て，（Ｄ’）ｃと（Ｄ’）ｂを照合することによって行われる。

イ　上記アの認定事実によれば，ＣＥＣサービスにおいては，発信者が，契約書等の文書データ（伝達情報）に電子署名して受信者に送信し，受信者が，同伝達情報に電子署名して発信者に送信した後，発信者が，同伝達情報に問

題がないか確認して完了処理を行うこと，同完了処理が行われたときは，同伝達情報がＣＥＣサーバに送信されて保管され，「ＳｅｃｕｒｅＳｅａｌ（Ｒ）センタ」がタイムスタンプを発行し，同タイムスタンプがＣＥＣサーバに存置されること，ＣＥＣサーバにおいては，同タイムスタンプの情報を検証した結果として，同タイムスタンプの情報に変更がないことで同伝達情報の改ざんがないことを証明するものであること，以上の事実が認められる。

(3) 「照合する手段」の充足性

上記(2)によれば，ＣＥＣサービスは，あくまで，完了処理が行われて伝達情報がＣＥＣサーバに保管された後に，保管時に発行されて存置されているタイムスタンプの情報を検証することによって，同完了処理後の伝達情報の改ざんがないことを証明するものであり，発信者署名データ，受信者署名データを用いたデータを照合することにより伝達情報の改ざんがないことを証明するものではない。

したがって，ＣＥＣサーバは，構成要件５の「前記発信者署名データのうち，前記発信者装置が送信した伝達情報の内容の同一性を確認できるデータと，前記受信者署名データのうち，前記受信者装置が受け取って復号化した伝達情報の内容の同一性を確認できるデータとを照合する手段」を有していると認めることはできない。

よって，ＣＥＣサーバは，構成要件５を充足しない。

(4) 原告の主張について

この点に関して原告は，原本性を検証する契約書データＤから算出してある照合値をδとすると，ＣＥＣサーバにおいては，発信者署名データのうち，発信者Ａが送信した契約書Ｄの内容の同一性を確認できる照合値εをもって，上記δと照合し，受信者署名データのうち，受信者Ｂが受け取って復号化した契約書Ｄの内容の同一性を確認できる照合値ζをもって，上記δと照合しているから，構成要件５の「照合する手段」を充足すると主張する。

しかし，前記(2)ア(ｳ)のとおり，本件処理ステップでは，受信者Ｂが署名した文書であることの検証として，「Ｄ＋〔（Ｄ）ａ〕ＳＫａ」というデータである「Ｄ’」のダイジェストを照合するが，発信者Ａが署名した文書であることの検証としては，「Ｄ」というデータのダイジェストを照合するのであり，「Ｄ’」と「Ｄ」が異なるものであることは明らかである。そうすると，前者の照合と後者の照合によって，（Ｄ’）ｂ＝（Ｄ’）ｃであること，及び（Ｄ）ａ＝（Ｄ）ｃが検証できるとしても，それだけでは，発信者Ａと受信者Ｂが同一の契約書Ｄに署名しているかどうかを確認，照合することはできない。

したがって，発信者署名データのうち，発信者Ａが送信した契約書Ｄの内容の同一性を確認できる照合値εは，原本性を検証する契約書データＤから生成される照合値δと照合されるが，受信者署名データのうち，受信者Ｂが受け取って復号化した契約書Ｄの内容の同一性を確認できる照合値ζは，「Ｄ＋〔（Ｄ）ａ〕ＳＫａ」である「Ｄ’」から生成される照合値とは照合されるものの，契約書データＤから生成される上記照合値δとは照合されないから，ＣＥＣサーバにおいて，照合値εをもって照合値ζと照合して発信者Ａと受信者Ｂが同一の契約書Ｄに署名しているかどうかを確認していると認めることはできない。

また，本件全証拠を精査しても，ＣＥＣサーバが，タイムスタンプを取得するためにどこから取得したダイジェストを使用するかを説明するものは見当たらず，ＣＥＣサーバの動作については，前記(2)のとおりであって，ＣＥＣサーバが，発信者及び受信者の双方の伝達情報を突き合わせるような形式で原本性を証明することを具体的に裏付けるに足りる証拠はない。

以上によれば，原告の上記主張は採用することができない。

３　争点(1)イ（構成要件６及び７の充足性）について

(1) 本件特許の出願経過

証拠（乙１）及び弁論の全趣旨によれば，原告は，本件特許の拒絶査定不服

審判請求書の理由補充書である本件手続補正書において，下記のとおり記載し，その結果，平成１８年３月７日付けで特許査定がされ，平成１８年４月２８日付けで本件特許権が設定登録された（甲１）ことが認められる。

記

・「原査定の拒絶理由は，本願・・・発明が，引用文献１（「暗号を用いた内容証明・配達証明サービス」，電子情報通信学会論文誌，１９８７年２月２５日，Vol.J70-D No.2，p.423-432）と特開平１０－１８７８３６号公報とに基づいて当業者が容易に想到し得たものであるから，特許法第２９条第２項の規定により特許を受けることができない，というものである。」

・「３－１）本願発明が，発信者装置Ａ及び受信者装置Ｂから内容証明サイト装置Ｃにそれぞれ送るデータを，伝達情報の内容の同一性を確認できるデータに関して，伝達情報等のダイジェストだけとしているのに対して，引用文献１及び特開平１０－１８７８３６号公報は，伝達情報等に相当するものをも送っている。・・・引用文献１及び特開平１０－１８７８３６号公報においては，内容証明サイト装置に相当する調停者（取引証明装置１）に送信する通信量（情報量）は，ダイジェストに比べて格段に多くならざるを得ず，内容証明サイト装置（調停者，取引証明装置１）への通信量の点で，引用文献１及び特開平１０－１８７８３６号公報は，本願発明に比べて劣らざるを得ない。」

・「３－２）本願発明が，内容証明サイト装置Ｃにおいて，伝達情報の内容の同一性を確認できるデータに関して，・・・伝達情報等のダイジェストだけを保管対象としているのに対して，特開平１０－１８７８３６号公報は，取引証明装置１（公証人，公証装置１１）において，伝達情報等に相当する取り引き文書Ｍも保管対象としている。このため，特開平１０－１８７８３６号公報においては，取引証明装置１（公証人，公証装置１１）は，本願発明に比して，多くの情報量を保管する構成とならざるを得ないと共に，公証人

等による取り引き文書Mへの不正関与の可能性が高まることになり，特開平１０－１８７８３６号公報は，保管量，秘密保持性の点で，本願発明に比べて劣らざるを得ない。また，引用文献１については，・・・調停者が保管しない構成をとっており，この引用文献１が本願発明と基本的に異なることは明らかなことである。」

(2) 以上によれば，原告は，本件特許の拒絶査定不服審判において，拒絶査定の理由（進歩性欠如）における引用文献１及び特開平１０－１８７８３６号公報（以下「引用文献等」という。）との相違点を，本件発明は「伝達情報」等を発信者装置Ａ及び受信者装置Ｂから内容証明サイト装置Ｃに送信せず，「伝達情報」を内容証明サイト装置Ｃが保管しないこととし，そのことにより，本件発明は，引用文献等記載の発明と異なり，通信量（情報量）が多くならず，多くの情報量を保管する構成でもなく，公証人等による伝達情報への不正関与の可能性を高くしないという効果を奏すると陳述したこと，本件発明は，原告のこのような陳述を踏まえた上で，特許査定がされたこと，以上の事実が認められる。

したがって，本件発明の構成要件６及び７の意義は，契約当事者双方が契約書の「原本」を管理し，内容証明サイト装置は原本が改ざんされていないことを伝達情報のダイジェスト又は伝達情報を暗号化した暗号情報のダイジェストのみに基づいて検証することで証明するサービスであると解するのが相当である。しかるに，前記２(2)イで認定したとおり，ＣＥＣサーバでは，伝達情報である原本そのものがセンタに送られてこれを保管する構成を有するものであるから，ＣＥＣサーバは，構成要件６及び７を充足しないというべきである。

(3) この点に関して原告は，ＣＥＣサーバでは，契約者（甲）の署名データのうち，契約者（甲）が送信した電子契約文書の内容の同一性を確認できるデータεは，契約者（甲）が送信した電子契約文書のダイジェスト（ハッシュ）に限られているとして，構成要件６を充足すると主張し，また，ＣＥＣサーバでは，

契約者（乙）の署名データのうち，契約者（乙）が受け取って復号化した電子契約文書の内容の同一性を確認できるデータとは，契約者（乙）が受け取って復号化した電子契約文書のダイジェスト（ハッシュ）に限られているとして，構成要件７を充足すると主張する。

しかし，ＣＥＣサーバにおける署名検証の具体的態様は前記２(2)イで認定したとおりであり，ＣＥＣサーバは署名検証を行うに当たり，発信者及び受信者から文書が送信されて，当該文書からダイジェストを作成して，これを照合に用いていることが認められる。そうすると，ＣＥＣサーバが署名検証を行うには，発信者及び受信者から，それぞれ伝達情報のダイジェストのみならず，伝達情報も受信する必要があり，ＣＥＣサーバが受け取り保管する伝達情報は，原本性を証明してもらうためのデータという位置付けにとどまらず，原本性を証明するためのデータとして扱われると認められるから，伝達情報は「伝達情報の内容の同一性を確認できるデータ」に該当するということができる。したがって，ＣＥＣサーバについては，「伝達情報の内容の同一性を確認できるデータ」が，「伝達情報のダイジェスト又は該伝達情報を暗号化した暗号情報のダイジェストに限られ」るものではないから，原告の上記主張は採用することができない。

４　結論

以上によれば，ＣＥＣサーバは，本件発明の構成要件５，６及び７のいずれについても充足するとは認められないから，その余の点について判断するまでもなく，原告の請求は理由がない。

よって，主文のとおり判決する。

東京地方裁判所民事第４０部

裁判長裁判官

東　海　林　　保

裁判官

実　　本　　滋

裁判官

足　　立　　拓　　人

【別紙】特許公報

＜以下略＞

【別紙】「図１　ＣＥＣＴＲＵＳＴ処理ステップ抜粋」

＜以下略＞