平成１１年(ワ)第１１８４１号　差止請求権不存在確認等請求事件
口頭弁論終結日　平成１２年１１月２８日

判　　決

原　　告　　アール・エス・エー・セキュリティ株式会社
代表者代表取締役　　【Ａ】
訴訟代理人弁護士　　花　岡　　巌
同　　木　崎　　孝
補佐人弁理士　　山　本　秀　策
同　　大　塩　竹　志
被告（引受承継人）　　株式会社ローレルインテリジェントシステムズ
代表者代表取締役　　【Ｂ】
脱退被告　　【Ｃ】
両名訴訟代理人弁護士　　松　村　信　夫
同　　和　田　宏　徳
松村信夫復代理人弁護士　　塩　田　千恵子
補佐人弁理士　　葛　西　泰　二

主　　文

１　被告は、原告に対し、登録第２８３５４３３号又は登録第２８８４３３８号の特許権に基づいて、原告が別紙物件目録記載のワンタイムパスワード製品の輸入、販売をしたことについて、損害賠償請求権又は不当利得返還請求権を有しないことを確認する。

２　訴訟費用は被告の負担とする。

事実及び理由

第１　請求

主文同旨

第２　事案の概要

１　原告の請求と被告の主張の概要

(1) 原告は、別紙物件目録記載のワンタイムパスワード製品（①ないし⑨の個別の製品を指す。以下、「原告製品①」等といい、併せて「原告製品」という。）を輸入、販売しているところ、それらの行為は被告が有する後記の特許権を侵害しないから、被告は原告に対し、同特許権に基づく損害賠償請求権又は不当利得返還請求権を有しないとして、その確認を請求した。

(2) これに対し被告は、原告製品の輸入、販売は、被告が有する後記特許権（後記本件特許権１の請求項１及び３、後記特許権２の請求項１及び２）を間接侵害すると主張した。

２　基礎となる事実（いずれも争いがないか弁論の全趣旨により認められる。なお、以下、書証の掲記は「甲１」などと略称し、枝番号のすべてを含む場合はその記載を省略する。）

(1) **被告の特許権**

被告は、次の特許権を有している。

ア　本件特許権１

（ア）　発明の名称
　　アクセス制御方法および認証システムおよび装置

（イ）　出願日
　　昭和５９年１０月１１日（特願平８－５６９６６号）
　　特願昭５９－２１３６８８号の分割

（ウ）　登録日
　　平成１０年１０月９日

（エ）　特許番号
　　第２８３５４３３号

（オ）　特許請求の範囲

本件特許権１の特許出願の願書に添付した明細書（以下「本件明細書１」という。）の特許請求の範囲の記載は、本判決添付の特許公報（以下「本件公報１」という。）の該当欄記載のとおりである（以下、同特許請求の範囲欄中、３項記載の特許発明を「本件発明１」と、１項記載の特許発明を「本件発明２」という。）。

イ　本件特許権２

（ア）　発明の名称

アクセス制御システム

（イ）　出願日

昭和５９年１０月１１日（特願平９－２６４８５０号）

特願平８－５６９６６号（本件特許権１に係る出願）の分割

（ウ）　登録日

平成１１年２月１２日

（エ）　特許番号

第２８８４３３８号

（オ）　特許請求の範囲

本件特許権２の特許出願の願書に添付した明細書（以下「本件明細書２」という。）の特許請求の範囲の記載は、本判決添付の特許公報（以下「本件公報２」という。）の該当欄記載のとおりである（以下、同特許請求の範囲欄中、１項記載の特許発明を「本件発明３」と、２項記載の特許発明を「本件発明４」という。また、本件発明１ないし４を併せて「本件発明」という。）。

⑵　**本件発明の構成要件の分説**

本件発明の構成要件は、次のとおり分説するのが相当である。

ア　本件発明１（本件特許権１の特許請求の範囲３項）

①　アクセスを希望する被認証側と認証側とで共通に変化する共通変化データを利用して前記被認証側が動的に変化する認証用データを生成してデータ通信により前記認証側に伝送し、認証側が前記共通変化データを利用して前記伝送されてきた認証用データの適否を判定して認証を行なうアクセス制御用の認証システムであって、

②　クロック機能を有するクロック手段と、

③　前記被認証側において、前記クロック手段が計時する時間に応じて変化する時間変数データを前記共通変化データとして用いて前記認証用データを生成するデータ生成手段と、

④　該データ生成手段により生成された認証用データであってデータ通信により前記認証側に伝送されてきた認証用データを受信するデータ受信手段と、

⑤　時間に応じて変化する時間変数データを前記共通変化データとして用いて前記データ受信手段で受信した認証用データの適否を判定して認証を行なう適否判定手段と、

⑥　前記クロック手段の狂いに伴い前記時間変数データに誤差が生じた場合にそれを自動的に修復させて経時的に誤差が累積されることを防止可能とするための誤差自動修復手段とを含む

⑦　ことを特徴とする、認証システム。

イ　本件発明２（本件特許権１の特許請求の範囲１項）

①　アクセス希望者側と認証側とで共通に変化する共通変化データを利用して前記アクセス希望者側が動的に変化する認証用データを生成してデータ通信により前記認証側に伝送し、認証側が前記共通変化データを利用して前記伝送されてきた認証用データの適否を判定して認証を行ないアクセス制御を行なうアクセス制御方法であって、

②　前記アクセス希望者側において、クロック機能を有する装置が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記認証用データを生成するデータ生成ステップと、

③　該データ生成ステップにより生成された認証用データであってデータ通信により伝送されてきた認証用データを前記認証側が受信する受信ステップと、

④　前記認証側において、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記受信ステップで受信した認証用データの適否を判定して認証を行なう適否判定ステップと、

⑤　該適否判定ステップにより適正である旨の判定がなされた場合に前記アクセス希望者のアクセスを許容できる旨の判定を出力するアクセス許容ステップとを含み、

⑥　前記クロック機能を有する装置の狂いに伴い前記時間変数データに誤差が生じた場合にそれを自動的に修復させて経時的に誤差が累積されることを防止可能とするための誤差自動修復処理を行なう

⑦　ことを特徴とする、アクセス制御方法。

ウ　本件発明３（本件特許権２の特許請求の範囲１項）

①　アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、

②　前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、

③　該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、

④　演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、

⑤　前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、

⑥　前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、

⑦　前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、

⑧　前記アクセス制御システムは、前記可変型パスワードデータ生成手段のクロックが狂って前記時間変数データに誤差が生じた場合にその誤差を自動的に修復させて経時的に誤差が累積されることを防止可能とするための誤差自動修復手段をさらに含み、

⑨　前記アクセス希望者は、前記認証手段により適正である旨の認証結果が得られたことを条件として前記アクセス対象へのアクセスが許容される

⑩　ことを特徴とする、アクセス制御システム。

エ　本件発明４（本件特許権２の特許請求の範囲２項）

①　アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、

②　前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、

③　該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、

④　演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、

⑤　前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、

⑥　前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、

⑦　前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして利用して前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、

⑧　前記時間同期式認証手段は、

ア　前記転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証を行なわない所定誤差許容認証手段と、

イ　前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定を行なうための誤差許容時間内不正アクセス禁止手段とを含む

⑨　ことを特徴とする、アクセス制御システム。

⑶ **原告の行為**

ア　原告は、原告製品を輸入、販売している。

イ　対象各物件・方法と各発明の関係

（ア）　原告製品（⑨を除く）は、それらを使用するシステム（以下「ＲＳＡシステム」という。）の生産及び実施にのみ使用する物である。

（イ）　ＲＳＡシステムは、

ａ　本件発明１の構成要件②④⑦を充足する。

ｂ　本件発明３の構成要件①③⑤⑨⑩を充足する。

ｃ　本件発明４の構成要件①③⑤⑨を充足する。

（ウ）　ＲＳＡシステムの使用方法は、本件発明２の構成要件③⑤⑦を充足する。

（エ）　原告製品⑨の内容は、別紙「Ｋｅｏｎ説明書」記載のとおりである。

３　争点

⑴ ＲＳＡシステムとその使用方法の内容

⑵ ＲＳＡシステムが、

ア　本件発明１の

（ア）　構成要件①③⑤を充足するか。

（イ）　構成要件⑥を充足するか。

イ　本件発明３の

（ア）　構成要件②を充足するか。

（イ）　構成要件④⑥⑦を充足するか。

（ウ）　構成要件⑧を充足するか。

ウ　本件発明４の

（ア）　構成要件②を充足するか。

（イ）　構成要件④⑥⑦を充足するか。

（ウ）　構成要件⑧アを充足するか。

（エ）　構成要件⑧イを充足するか。

⑶ ＲＳＡシステムの使用方法が、本件発明２の

ア　構成要件①②④を充足するか。

イ　構成要件⑥を充足するか。

⑷ 原告製品⑨は、本件発明に係る物の生産又は方法の実施にのみ使用する物か。

第３　争点に関する当事者の主張

１　争点⑴（ＲＳＡシステムとその使用方法の内容）について

【被告の主張】

ＲＳＡシステムとその使用方法の内容は、別紙「ＲＳＡシステム説明書」記載のとおりである。

【原告の主張】

「ＲＳＡシステム説明書」については、下線部及び第１０図を削除すべきであるが、その余はＲＳＡシステムの説明として認める。

２　争点⑵ア（ア）（ＲＳＡシステムが本件発明１の構成要件①③⑤を充足するか）について

【原告の主張】

⑴ 「共通変化データ」について

ア　本件発明１の構成要件③⑤でいうアクセス希望者側（被認証側）及び認証側の「時間変数データ」は、「アクセス希望者側と認証側とで共通に変化する共通変化データ」（構成要件①）として利用されるものであるから、当然に一致した数値でなければならず、本件明細書１の発明の効果の欄の説明によれば、「時間という全国共通の客観的なパラメータに従って変化する時間変数データ」であり、標準時刻に合致する時刻のように一致して変化する数値であると解される（本件明細書１の発明の詳細な説明によれば、図７及び図８のS1、S2、S5のとおり、時刻標準電波に基づく現在時刻が認証用データ（Ａ）生成用の「共通変化データ」であり、S10によって認証側で生成する認証用データ（Ｂ）の生成に用いる「時間変数データ」が右の現在時刻と同じであるときにのみ、Ａ＝Ｂとなり、アクセスが許容される。また、本件特許権１の審査過程で提出された要約書にも、時刻標準電波によって認証側と被認証側の時刻を一致させることが解決手段として記載されてい

る。）。
　　このように、本件発明１は、認証側と被認証側の時間（時間変数データ）が一致することにより認証が可能となるシステムである。
　イ　これに対して、ＲＳＡシステムは、被認証側と認証側とで標準時刻の如き全国共通の客観的なパラメータを共通に用いることは全く不要とするものであり、各々独立に動作している被認証側と認証側のクロックで計時される時刻、すなわち被認証側と認証側とで個別に変化する時刻（個別変化データ）を利用して認証を行うものであり、「被認証側と認証側とで共通に変化する共通変化データ」を利用していない。
　　すなわち、ＲＳＡシステムの「現在時刻」には、①「被認証側のクロックが計時する現在時刻」と②「認証側のクロックが計時する現在時刻」の二つがあるが、①と②は相互に何の関連もなく刻まれた各クロック固有の時刻であり、異なるものであって「共通変化データ」ではない。
　　ＲＳＡシステムでは、被認証側と認証側の時間変数データは、必ずしも一致するものではない。これが一致しているか否かにかかわらず認証可能とするのがＲＳＡシステムであり、その手段が「窓」による認証なのである。
　(2) 構成要件⑤の「時間変数データ」について
　　被告は、ＲＳＡシステムにおける「オフセット更新後時間変数データ」が構成要件⑤の認証側の「時間変数データ」に該当すると主張する。
　ア　しかし、まず、「オフセット更新後時間変数データ」なるものは、ＲＳＡシステムの認証の過程では全く存在しないものであり、認証用データの適否を判定するために使用されることはない。むしろ、「オフセット補正後時間変数データ」というのが正確である。
　イ　また、本件発明１における認証側の時間変数データは、認証側の「時間」に応じて変化するものである。そして、認証側の「時間」とは標準時刻を意味する。ところが、ＲＳＡシステムにおけるオフセット値は、認証側のクロックと被認証側のクロックの時刻のズレであり、認証側のデータベースに各利用者（被認証側）ごとに記憶されているものである。このようなオフセット値を認証側のクロックが計時する時刻の対応期間に加減したもの（オフセット補正後時間変数データ）は、「時間に応じて」変化するものではなく、本件発明１の構成要件⑤の「適否判定手段」が用いる「時間変数データ」に該当しないことは明らかである。
　　この点について被告は、「時間に応じて変化する時間変数データ」は、時間に応じて変化するデータのすべてを意味し、日本標準時刻でなくてもよいし、被認証側とは共通でなくバラバラに変化する時間データを用いてもよいと主張するようである。しかし、標準時刻以外の時間データを用いる構成は、本件明細書１では全く記載されておらず、当業者が容易に実施できるような記載になっていないことは明らかなので、本件発明１が他の構成を含むとすれば、特許は無効事由を包含することになる。
　ウ　さらに、本件発明１の共通に変化する「時間変数データ」は、被認証側のログイン行為には直接関係しない「全国共通に変化する」客観性のあるパラメータによって変化するものとされている（本件明細書１【０００８】参照）。ところが、ＲＳＡシステムにおけるオフセット値は、被認証側のログイン行為によって初めて認証側に認識され、各利用者ごとに異なるものである。認証側の現在時刻にこのようなオフセット値を加減したものは、被認証側のログイン行為には直接関係しない客観性のあるパラメータによって変化するものであるなどとは到底いえず、本件発明１の「適否判定手段」（認証側）が用いる「時間変数データ」に該当しないことは明らかである。
　【被告の主張】
　(1) 「共通変化データ」について
　ア　本件発明１における「共通変化データ」とは、認証側と被認証側とで認証に必要となる共通因子として利用される変化データのことである。すなわち、動的に変化する可変型パスワードデータを用いて認証する場合には、被認証側から伝送されてくるパスワードデータが毎回変化しているために、次にどのようなパスワードデータが伝送されてくるかを認証側が割り出すことができなければならない。そこで、認証側と被認証側とで何らかの共通因子が必要となる。この共通因子として利用される変化データのことを本件発明１では「共通変化データ」といっているのである。すなわち、本件発明１における「時間に応じて変化する時間変数データを前記共通変化データとして用い」るという考え方（構成要件③）は、従来技術の

ログイン同期方式との対比において、ログイン回数という、やり取りした当事者間でのみ成立するクローズドな共通変化データを共通因子として利用するのではなく、時間という、全国共通に通用するオープンな共通変化データを共通因子として利用するということである。

この点について、原告は、本件発明１における「共通変化データ」とは、認証側と被認証側とで常に一致しているデータである必要があると主張する。しかし、本件発明１では、被認証側の認証用データも、認証側の適否判定用データも、共に共通変化データを利用して生成されるものとされているが、ここで、仮に「共通変化データ」が、認証側と被認証側とで常に一致しているデータであるとするならば、認証側の時間変数データと被認証側の時間変数データとの間に、「クロック手段の狂いに伴う時間変数データの誤差」（構成要件⑥）は生じないという不合理が生じる。したがって、原告の上記主張のように解釈する余地はない。

イ　ＲＳＡシステムは、被認証側と認証側の別個独立のクロックで計時される現在時刻を時間変数データとして利用して認証を行っている。なお、ＲＳＡシステムの教材（乙７）においても、「トークンとＡＣＥ／Ｓｅｒｖｅｒ間では以下の二つの情報が一致している必要」があるとし、そのうちの一つとして「現在時刻」が挙げられており、本来的には、被認証側と認証側とで計時される現在時刻は、それぞれ一致することが指向されている。

そうすると、現在時刻というのは、認証側と被認証側とで共に共通の因子として利用できる変化データであるから、ＲＳＡシステムが「共通変化データ」を利用していることは明らかである。

⑵ 構成要件⑤の「時間変数データ」について

ア　ＲＳＡシステムにおいては、「オフセット更新後時間変数データ」が、構成要件⑤の「時間変数データ」に当たる。

ここにいう「オフセット更新後時間変数データ」は、認証が終了した時点でその認証に使用したオフセットを更に修正した場合の認証側の時間変数データを示すものである（別紙「ＲＳＡシステム説明書」の第７図に示されている「オフセット」に対する「新オフセット」、第６図に示されている「オフセット更新」（Ｓ６１４）の動作に対応する。）。そして、この新オフセットに基づいている「オフセット更新後時間変数データ」を、次回の認証時には原告のいう「オフセット補正後時間変数データ」として用いるものである（したがって、次回の認証時には、両者間に実質的に差がない。）。かかる「オフセット更新後時間変数データ」は、ＲＳＡシステムにおいて、「窓」の中心としてのトークンコードを発生させるために使用されている。

イ　原告は、本件発明１における「時間変数データ」とは、「時間に応じて」変化するものであるが、被告物件のオフセット値は「時間に応じて」変化するものではないので、オフセット更新後時間変数データも「時間に応じて」変化するものではなく、「時間変数データ」に当たらないという主張を行っている。

しかし、まず、構成要件⑤の「時間」を標準時刻を意味すると解する理由が明らかでないし、また、そのように解すると、「前記クロック手段の狂いに伴い前記時間変数データに誤差が生じた場合」（構成要件⑥）という構成要件が出てこなくなり不合理である。したがって、そのような解釈は採り得ない。

また、確かにオフセット値そのものは、「時間に応じて」変化するものではないといえる。しかし、認証側の時刻は、「時間に応じて」変化するものであるから、認証側の時刻にオフセット値という修正値を加減した、オフセット更新後時間変数データが、「時間に応じて」変化するものであることは明らかといえる。すなわち、別紙「ＲＳＡシステム説明書」第７図の記載にもあるように、オフセット更新後時間変数データとは、１時３０分という時間を表現するのに、「１時３３分－３分」という表現方法を使用しているだけなのである。

ウ　次に、原告は、オフセット更新後時間変数データは、利用者ごとに異なるもので、ログイン行為には直接関係しない「全国共通に変化する」客観性のあるパラメータによって変化するものではないので、「時間変数データ」に当たらないと主張する。

しかし、本件明細書１のかかる記載部分が、「共通変化データ」に関して、ログイン回数同期方式との対比から記載されていることからも明らかなように、「ログイン行為には直接関係しない」とは、ログイン回数同期方式のようにデータの値の増減がログイン行為には直接関係しないということであり、また、「全国共通に変化する客観性のあるパラメータ」というのは、ログイン回数同期方式の

ように当事者間で独自に変化するクローズドなパラメータではないということである。そうすると、オフセット更新後時間変数データも、認証側の時刻という、ログイン行為には直接関係しない「全国共通に変化する」客観性のあるパラメータである「共通変化データ」を利用したものであるから、本件発明１の構成要件⑤の「時間変数データ」に当たる。

エ　さらに原告は、日本標準時刻以外の時間変数データを用いる構成は、本件明細書１に全く記載されておらず、当業者が容易に実施できるような構成になっていないので、本件発明１がこのような構成を含むとすれば、特許は無効事由を包含するという。

しかし、これは、特許法３６条における実施可能要件の規定を歪曲した暴論といわざるを得ない。実施可能要件は、特許請求の範囲の記載から把握される発明を具体的に当業者が実施できるように開示されていないと、開示の代償として特許を付与する特許制度の根幹が揺らぐことを防止するためのものである。すなわち、そのクレームの技術的範囲に含まれる発明を具現化する実施例のうち、少なくとも一つが当業者が容易に実施できる程度に開示されていれば、実施可能要件に基づく無効事由が問題となるものではない。また、実施例から抽出される下位概念の技術的思想をもとにして、先行例を含まない上位概念の発明を規定する発明を立案することは通常行われている。原告の論法によれば、このような場合、明細書に記載されていない下位概念の実施例はすべて発明の範囲から除外されることになり、結局その発明の技術的範囲はその明細書に開示された実施例の範囲のみになってしまうことになる。

３　争点⑵ア（イ）（ＲＳＡシステムが本件発明１の構成要件⑥を充足するか）について

【原告の主張】

⑴　本件発明１では、認証側と被認証側とが一致した時刻値を用いないと認証できないシステムであることから、被認証側が用いる時刻データが常に正しいことを確保する必要がある。そのために設けられたのが「誤差自動修復手段」である。

すなわち、まず、構成要件⑥の「前記クロック手段の狂いに伴い」とは、被認証側（アクセス希望者側）のクロック手段の狂いに伴い、という意味である。そして、構成要件⑥の「それを自動的に修復させて」とは、被認証側のクロック手段に生じた狂いを自動的に修復させることを意味する。アクセス希望者は多数いるため、認証側のクロック手段を修復させてしまうと、システムが維持できないのである。実際、実施例も、アクセス希望者側のクロック手段が狂った場合に、このアクセス希望者側の狂いを修正することしか記載されていない。

他方、本件発明１における認証側の時間変数データは、認証側の「時間」に応じて変化するものである。そして、認証側の「時間」（構成要件⑤）とは標準時刻を意味することは争点１で主張したとおりである。

したがって、構成要件⑥において修復の対象となる「誤差」は、被告が主張するような、被認証側と認証側の時間変数データの誤差一般ではなく、被認証側のクロック機能の狂いに伴って生じた、標準時刻との誤差に限られることは明らかである。本件明細書１においても、その旨の記載しかない。

⑵　一方、ＲＳＡシステムでは、被認証側にも認証側にも別個独立のクロック手段があり、どちらの時計も狂う可能性が当然あり、時間変数データに誤差が生じるが、そもそもどちらの狂いによって誤差が生じているのかは判別できないし、被認証側のクロック手段を修復したりはしない。ＲＳＡシステムでは、被認証側のクロックと認証側のクロックの時間のズレを、アクセスごとに認証側の装置に記憶させ（オフセット更新処理）、次のアクセスの際には、前回アクセス時にオフセット更新処理された時間のズレが存在することを前提に、その後更に累積された時間の差が一定範囲に収まっている場合には認証を可とした上で、更に累積した時間の差を認証側の装置に追加して記憶させるのであり（オフセット更新処理）、時間の誤差は累積していく一方であり、これを修正することはない。

また、本件発明１は、前記のとおり時間（時間変数データ）が一致することにより認証が可能となるシステムであるが、ＲＳＡシステムはそうではない。すなわち、ＲＳＡシステムにおける認証機能は、利用者が正しいトークン（すなわち正しいシード）と正しいＰＩＮを持っていることを確認することであり、それが正しく確認できさえすれば、本来は、認証側と被認証側の時刻のズレは全く問題ではない。

したがって、ＲＳＡシステムは、構成要件⑥を充足しない。

【被告の主張】
(1) 構成要件⑥における「誤差」とは、認証用データの適否判定、すなわち、アクセス希望者側と被認証側双方での同期が狂ってしまう不都合を防止するために観念されるものであるから、「誤差」とは、アクセス希望者側で認証用データの生成に使用された時間変数データと、認証側で適否判定用データの生成に使用された時間変数データとの差のことをいうことは明らかである。
したがって、ＲＳＡシステムにおける「オフセット更新後誤差」（前回アクセス時のオフセット更新処理後に、被認証側と認証側との間に累積された時間の差）は、構成要件⑥における「誤差」に該当する。また、ＲＳＡシステムにおいては、認証前に、アクセスしてきたユーザーのオフセット値を検索して認証側の現在時刻に対しオフセット値を加算しており、認証前にオフセット加減算をして修復を行っている。
したがって、ＲＳＡシステムは、構成要件⑥を充足する。
(2)ア 原告は、本件発明１においては、認証に用いるデータが被認証側と認証側で一致していなければならないため、誤差自動修復手段があると主張する。
しかし、誤差に対処する方法としては、「所定誤差許容認証手段」等が考えられる。しかし、それでも「所定誤差」の範囲内でしか、認証を行うことができない。そのため、誤差がどんどん大きくなり、「所定誤差許容認証手段」等をもってしても、認証ができない事態に陥らないように、誤差自動修復手段により、誤差を修正するということである。そのため、構成要件上も、「誤差が『生じる』ことを防止可能とするための誤差自動修復手段」とされないで、「経時的に誤差が『累積される』ことを防止可能とするための誤差自動修復手段」とされているのである。
イ また、原告は、「誤差自動修復手段」における「誤差」とは、「クロック手段に生じた狂い」であると考えているようである。
しかし、まず、本件発明１において、「誤差」の修復は、誤差が生じた場合、アクセス希望者側の認証用データと、認証側の適否判定用データに齟齬が生じ、認証に支障をきたすため、これを防止するために行われるものであるから、本件発明１における「誤差」とは、前記のように、アクセス希望者側で認証用データの生成に使用された時間変数データと、認証側で適否判定用データの生成に使用された時間変数データとの差のことをいうことは明らかである。
また、「クロック手段の狂いに伴い」生じたというのは、単に誤差が生じる一原因を述べたものであり、そのことと「誤差」が認証側と被認証側の時間変数データの差であるということとが矛盾するものではなく、両者は両立するものである。
さらに、仮に原告主張のように解したとしても、ＲＳＡシステムにおいて、アクセス希望者側のクロック手段の狂いに伴い、アクセス希望者側の時間変数データと、認証側の時間変数データに誤差が生じるのであるから、ＲＳＡシステムは、本件発明１の構成要件を充足することになる。

４　争点(2)イ(ア)（ＲＳＡシステムが本件発明３の構成要件②を充足するか）について

【原告の主張】
(1) 平成１２年９月８日付け原告第三準備書面までの主張
ＲＳＡシステムが本件発明３の構成要件②を充足することは争わなかった。
(2) 平成１２年１０月１６日付け原告第四準備書面による主張
ＲＳＡシステムは、アクセス対象が複数という構成で譲渡、使用等がされる場合もあるが、アクセス対象が単数という構成で譲渡、使用等がされる場合もあるから、後者の場合には、本件発明③の構成要件②の「複数のアクセス対象」を充足しない。
【被告の主張】
原告の主張(2)は、自白の撤回に当たり、許されない。

５　争点(2)イ(イ)（ＲＳＡシステムが本件発明３の構成要件④⑥⑦を充足するか）について

本争点に関する当事者の主張は、争点(2)ア(ア)についてのものと同様である。

６　争点(2)イ(ウ)（ＲＳＡシステムが本件発明３の構成要件⑧を充足するか）について

本争点に関する当事者の主張は、争点(2)ア(イ)についてのものと同様である。

７　争点(2)ウ(ア)（ＲＳＡシステムが本件発明４の構成要件②を充足するか）について

本争点に関する当事者の主張は、争点(2)イ(ア)についてのものと同様である。

８　争点(2)ウ(イ)（ＲＳＡシステムが本件発明４の構成要件④⑥⑦を充足するか）について

本争点に関する当事者の主張は、争点(2)ア(ア)についてのものと同様である。

９　争点(2)ウ(ウ)（ＲＳＡシステムが本件発明４の構成要件⑧アを充足するか）について

【原告の主張】

(1) 構成要件⑧アには単に「誤差」とあるが、本件発明４は、認証側と被認証側の時間変数データの一致を基本とする認証用変化データの時間同期式認証手段である以上、許容されるズレにも一定の限界があるはずであるが、特許請求の範囲記載の文言からはそれを窺い知ることはできない。そこで、本件明細書２における発明の詳細な説明の記載を見ると、シークレット関数ｆ（ｗ，ｘ，ｙ，ｚ）のｗ、ｘ、ｙは一致し、ｚ値にズレがあり、それがＫ秒以内である場合について説明しており（本件公報２の【0041】【0042】参照）、具体的には、「被認証側での識別信号算出に要する時間やデータ通信所要時間等を考慮した遅延時間であり、３秒等の短い時間の範囲内」という記載しかないのであるから、「誤差」というのも、「被認証側での識別信号算出に要する時間やデータ通信所要時間等を考慮した遅延時間であり、３秒等の短い時間の範囲内」のものと解さざるを得ない。すなわち、本件発明４の誤差許容認証手段とは、誤差の大きさがＫ秒以内の場合に認証を与えるということである。

したがって、認証側と被認証側のズレの大きさを問題にしないＲＳＡシステムは、本件発明４の構成要件⑧アの「所定誤差許容認証手段」を有しない。

(2) また、構成要件⑧アの「誤差許容時間」は「予め定められた」ものとされているが、ＲＳＡシステムの時刻誤差自動許容範囲は、「予め定められた」ものではなく、ズレの大きさを問題にしないのであり、この点からも、ＲＳＡシステムは構成要件⑧アの「所定誤差許容認証手段」を有しない。

すなわち、ＲＳＡシステムでは、時刻誤差自動許容範囲は、初期値は±１期間（セル）であるが、認証間隔に応じて徐々に広がっていくものであり（別紙「ＲＳＡシステム説明書」第二の四の１(1)(2)、２(1)(2)、３(1)(2)参照）、「予め定められた」誤差許容範囲というものはない。

【被告の主張】

原告は、本件発明４の「所定誤差許容認証手段」における「誤差」について、本件公報２に実施例の説明として記載された、「被認証側での識別信号算出に要する時間やデータ通信所要時間等を考慮した遅延時間であり、３秒等の短い時間の範囲内」のものであると考えているようである。

しかし、この「所定誤差許容認証手段」の機能は、可変型パスワードデータを生成する時間変数データに何らかの誤差がある場合に、その誤差が予め定められた許容時間の範囲に入る場合にはアクセス禁止の認証を行わないとするものである。すなわち、「許容時間」の範囲内では多少「誤差」があってもアクセスを許容しようというものであり、「誤差」と「許容時間」との関係が問題であって、「誤差」の値の大小を問題にしているものではない。構成要件⑧アには、「前記転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても」と記載されており、「所定誤差許容認証手段」において、「時間変数データのズレ」を「誤差」としていることは明らかである。

そして、ＲＳＡシステムにおいて、前回のアクセスによるオフセット更新処理後に時間変数データのズレが例えば１分以内である場合は（ＳｅｃｕｒＩＤスタンダードタイプトークン及びＳｅｃｕｒＩＤキーフォブタイプトークンの場合）、そのままアクセスを許容するものであることに争いはない。

そうすると、ＲＳＡシステムは、「所定誤差許容認証手段」を備えているといえる。

１０　争点(2)ウ(エ)（ＲＳＡシステムが本件発明４の構成要件⑧イを充足するか）について

【原告の主張】
構成要件⑧イの「誤差許容時間内不正アクセス禁止手段」は、構成要件⑧アの「所定誤差許容認証手段」と一体となってセキュリティを向上させるものであるから、その「誤差許容時間」の解釈は、構成要件⑧アについて述べたのと同様であり、「被認証側での識別信号算出に要する時間やデータ通信所要時間等を考慮した遅延時間であり、３秒等の短い時間」と解さざるを得ない。
したがって、ＲＳＡシステムは、構成要件⑧イを充足しない。
【被告の主張】
構成要件⑧アにおけるのと同様に、構成要件⑧イの「誤差許容時間内不正アクセス禁止手段」における「誤差」とは、「時間変数データのズレ」である。
そして、ＲＳＡシステムにおいては、原告の提出した技術説明書に「ワンタイムパスワードという言葉の通り、一度使用されたパスワードは、パスワードが有効である同じセル内でも再利用できません（認証が拒絶される）」と記載されている（甲17）。ここでセルとは、同一のパスワードが有効な時間であり、誤差許容時間のことである。
したがって、ＲＳＡシステムは構成要件⑧イを充足する。

１１　争点(3)ア（ＲＳＡシステムの使用方法が本件発明２の構成要件①②④を充足するか）について

本争点に関する当事者の主張は、争点(2)ア(ア)についてのものと同様である。

１２　争点(3)イ（ＲＳＡシステムの使用方法が本件発明２の構成要件⑥を充足するか）について

本争点に関する当事者の主張は、争点(2)ア(イ)についてのものと同様である。

１３　争点(4)（原告製品⑨は、本件発明に係る物の生産又は方法の実施にのみ使用する物か）について

【原告の主張】
(1) 原告製品⑨は、ＲＳＡシステムの生産及び実施にのみ使用する物であることは否認する。原告製品⑨の内容は、別紙「Ｋｅｏｎ説明書」記載のとおりであり、本件発明とは無関係である。
(2) 前記のとおり、ＲＳＡシステムが本件発明の技術的範囲に属しない以上、原告製品⑨の輸入、販売等は、本件発明の間接侵害とはならない。
【被告の主張】
(1) 原告製品⑨は、ＲＳＡシステムの生産及び実施にのみ使用する物である。
(2) 前記のとおり、ＲＳＡシステムが本件発明の技術的範囲に属する以上、原告製品⑨の輸入、販売等は、本件発明の間接侵害になる。

第４　争点に対する当裁判所の判断

１　争点(2)ア(ア)(イ)（ＲＳＡシステムが、が本件発明１の構成要件①③⑤及び⑥を充足するか）について

(1) 本件発明１における「共通変化データ」、「時間変数データ」、「誤差」、「誤差自動修復手段」の意義について
ア　本件発明１の特許請求の範囲の記載について
(ア)　本件発明１の特許請求の範囲の記載は、前記のとおりであるが、そこでは、「共通変化データ」、「時間変数データ」、「誤差」、「誤差自動修復手段」は、次のようなものとして記載されている。
ａ　「共通変化データ」は、「アクセスを希望する被認証側と認証側とで共通に変化する」ものである（構成要件①）。
ｂ　被認証側では、「動的に変化する認証用データを生成してデータ通信により前記認証側に伝送」するが（構成要件①）、この認証用データは、「クロック手段が計時する時間に応じて変化する時間変数データを前記共通変化データとして用いて」生成するものであり（構成要件③）、このクロック手段は、「クロック機能を有する」ものである（構成要件②）。
ｃ　認証側では、「時間に応じて変化する時間変数データを前記共通変化データとして用いて」、「認証用データの適否を判定して認証を行なう」ものである（構成要件①⑤）。
ｄ　「誤差自動修復手段」は、「前記クロック手段の狂いに伴い前記時間変数データに誤差が生じた場合に」、「それを自動的に修復させて経時的に誤差が累積されることを防止可能とする」ものである（構成要件⑥）。

（イ）　上記ｂ及びｃを比較すると、被認証側も認証側も、同じく「時間変数データ」を「共通変化データ」として用いているが、被認証側が用いる「時間変数データ」は、「前記クロック手段が計時する時間に応じて変化する」ものとされているのに対し、認証側が用いる「時間変数データ」は、単に、「時間に応じて変化する」ものとされており、明らかに文言上の相違があること、また、上記(d)では、「誤差自動修復手段」が修復対象とする「誤差」は、「前記クロック手段の狂いに伴い前記時間変数データに…生じた」ものであるとされていることが指摘できる。

イ　次に、本件明細書１の他の部分の記載を参酌して検討する。

（ア）　本件公報１（甲12）によれば、本件明細書１の発明の詳細な説明には、次の記載があると認められる。

ａ　まず、従来技術として、「被認証側が認証用データ（パスワード）を生成して認証側に伝送してアクセス制御等に際しての認証を受ける場合に、毎回同じ内容の認証用データ（パスワード）を生成して伝送したのでは、その伝送途中で第三者に認証用データ（パスワード）が盗聴されて不正なアクセスが行なわれる恐れがあるために、前回の認証時と今回の認証時とで異なった内容の認証用データ（パスワード）を生成して認証側に伝送するように構成」するとの観点から、「被認証側と認証側とで共通に変化する共通変化データを双方の共通因子として利用し、その共通変化データに基づいて動的に変化する認証用データを生成してそれに基づいて認証を行」うこととし、そのために、「被認証側と認証側とで共通に変化する共通変化データが、認証のためのログインが行なわれるたびに被認証側と認証側とで共に「１」ずつ加算更新される数値データ（ログイン回数）を用いて認証用データを生成するというログイン回数同期方式」が用いられていた。（本件公報１【０００２】～【０００７】）

ｂ　しかし、この従来技術には、次の問題点があった（本件公報１【０００７】）。

(a)　「被認証側とある特定の限られた認証側とでのみ前記共通変化データが両者の共通因子として利用できるにとどまる。その結果、たとえば認証側が複数存在し、ある１つの被認証側がたとえば認証側Ａにログインして認証を行なってもらった後、次に認証側Ｂにログインして認証を行なってもらおうとした場合には、既に認証側Ａとの間での認証によって共通変化データが「１」加算更新されているために、その後認証側Ｂでの認証に際しては、被認証側と認証側Ｂとの間で前記共通変化データが食い違った状態となっており、被認証側が適正なものであるにもかかわらず適正でない旨の認証が行なわれてしまうという欠点が生ずる。」（以下「問題点１」という。）

(b)　「被認証側と認証側との相互の交信に基づいてログイン回数を更新するために、交信エラーによる誤った更新が生じやすいという不都合も生ずる。」（以下「問題点２」という。）

(c)　「被認証側と認証側とで一旦ログイン回数の同期が狂った場合には、認証側にしてみれば、不適正なアクセス希望者（被認証側）が認証用データ（パスワード）を盗聴してそれを用いて不正にアクセスしてきたのか、または、適正なアクセス希望者（被認証側）がアクセスしてきたにも拘らず交信エラー等の何らかの原因でログイン回数の同期が狂ってしまったのかの判定がつきにくくなり、被認証側と認証側とで一旦狂ったログイン回数の同期を修復させるのが困難になることが予想される。」（以下「問題点３」という。）

(d)　「これらの問題点は、「従来のログイン回数同期方式による認証システムの場合には、被認証側のログインという行為に起因して被認証側と認証側との間で交信が行なわれてその結果ログイン回数が双方の間で更新されるという当事者間でのやりとりに基づいた更新を行なっているために、前述した種々の欠点が生ずる。」

ｃ　本件発明の目的は、「被認証側と認証側とで共通に変化する共通変化データを被認証側のログイン行為には直接関係しない客観性のあるパラメータによって変化するものにし、ログイン回数同期方式の持つ不都合を防止することである。」（本件公報１【０００８】）

ｄ　そして、本件発明１の作用としては、「被認証側においてデータ生成手段の働きにより、クロック機能を有するクロック手段が計時する時間に応じて変化する時間変数データを前記共通変化データとして用いて前記認証用データが生成される。データ受信手段の働きにより、前記データ生成手段により生成された認

証用データであってデータ通信により前記認証側に伝送されてきた認証用データが受信される。適否判定手段の働きにより、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記データ受信手段で受信した認証用データの適否を判定して認証が行なわれる。誤差自動修復手段の働きにより、前記クロック手段の狂いに伴い前記時間変数データに誤差が生じた場合にそれが自動的に修復されて経時的に誤差が累積されることが防止可能となる。」（本件公報１【００１０】）

ｅ　そして、実施例では、まず、被認証側の認証用データ生成は、「ＪＪＹによる時刻標準電波等のコード／データ放送を受信し、その受信信号に基づいて時刻を表示する腕時計により設備利用者所有の装置３３を構成してある。そして、腕時計３３内に記憶されているシークレットルールとしてのシークレット関数（それぞれの腕時計によって相違する）に、その腕時計３３が表示している現在の時刻を入力信号として代入し、答えを算出し、その答えと使用した入力信号のうち秒に相当する部分を識別信号としてアウトプットする」（本件公報１【００３７】）とされ、「前記腕時計３３は、コード／データ放送による信号に基づいて逐一表示時刻との誤差が修正されるように構成されている」とされており（同【００４３】）、より具体的には、「ステップＳ（以下単にＳという）１により、コード／データ放送による時刻標準電波を受信したか否か判別され、受信するまで待機する。そして受信した場合にはＳ２に進み、その時刻標準電波に基づき分周器を修正し、修正後の時刻を表示する動作が行なわれ」、その後、「シークレット関数ｆ（ｗ，ｘ，ｙ，ｚ）のそれぞれのｗ，ｘ，ｙ，ｚに現在の時刻からなる入力信号を代入し、答えＡを算出する処理がなされる。次にＳ６に進み、その算出した答えＡとｚに代入された数値ＮＺとを識別信号としてアウトプットする処理がなされる」とされている（同【００４４】）。

他方、認証側の適否判定は、「シークレットルールが登録されているコンピュータ１３または１４」が行い（本件公報１【００４５】）、識別信号を受信して、一定の条件を満たしていると判断された場合には、「予め登録されているシークレット関数ｆ（ｗ，ｘ，ｙ，ｚ）のｗ，ｘ，ｙに現在の時刻からなる入力信号を代入し、ｚに前記ＮＺを代入して答えＢを算出する処理がなされる。そしてＳ１１に進み、そのＢと前記受信したＡとが等しいか否かの判断がなされ、等しくなければＳ１２に進み、アクセスを許容できない旨の判断がなされ、等しい場合にはＳ１３に進み、設備へのアクセスを許容できるとの判断をアウトプットする処理がなされてＳ７に戻る」とされている（同【００４７】）。

また、別の実施形態としては、①「前記シークレット関数への入力信号として、現在の時刻を用いる代わりに、コード／データ放送に基づいて経時的に増加または減少する全国共通または全世界共通の数字を用いる」、②「設備利用者所有の装置３３は腕時計に限らず、電子卓上計算機等の個人端末であれば何でもよい」とされている（同【００４８】【００４９】）。

ｆ　そして、「本発明の構成要件と前記実施の形態との対応関係を説明する」（本件公報１【００６８】）として、次の記載がある（同【００７０】）。

(a)　「腕時計３３により、クロック機能を有する装置（クロック手段）が構成されている。」

(b)　「図７のＳ５の現在の時刻からなる入力信号と図８のＳ１０の現在の時刻からなる入力信号とにより、被認証側（アクセス希望者側）と認証側とで共通に変化する共通変化データであって時間に応じて変化する時間変数データが構成されている。図７のＳ１とＳ２とＳ５とにより、前記アクセス希望者側において、クロック機能を有する装置が計時する時間に応じて変化する時間変数データを前記共通変化データとして用いて前記認証用データを生成するデータ生成ステップが構成されている。」

(c)　「図７のＳ１とＳ２とＳ５とにより、前記被認証側において、前記クロック手段が計時する時間に応じて変化する時間変数データを前記共通変化データとして用いて前記認証用データを生成するデータ生成手段が兼用構成されている。」

(d)　「図８のＳ７により、受信ステップ（データ受信手段）が構成されている。」

(e)　「図８のＳ９とＳ１０とＳ１１とにより、前記認証側において、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記受信ステップで受信した認証用データの適否を判定して認証を行なう適否判定ステップ

が構成されている。」

(f)　「図８のＳ９とＳ１０とＳ１１とにより、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記データ受信手段で受信した認証用データの適否を判定して認証を行なう適否判定手段が構成されている。」

(g)　「図７のＳ１とＳ２とにより、前記クロック機能を有する装置の狂いに伴い前記時間変数データに誤差が生じた場合にそれを自動的に修復させて経時的に誤差が累積されることを防止可能とするための誤差自動修復処理が構成されている。」

ｇ　そして、本件発明１の効果としては、次の記載がある（本件公報１【００７１】）。

(a)　「被認証側と認証側との双方で同期を保ちながら認証用データを変化させるにおいて、時間という全国共通の客観的なパラメータに従って変化する時間変数データを双方の共通因子として利用して認証用データの更新の同期をとっているために、前述したログイン回数同期方式のような共通変化データが双方の間で食い違ってしまい同期が狂ってしまう不都合を極力防止し得る。」（以下「効果１」という。）

(b)　「しかも、クロック手段の狂いに起因した時間変数データの誤差が自動的に修復されるために、時間変数データの誤差が徐々に蓄積されて双方での認証用データの更新の同期が狂ってしまう不都合も極力防止し得る。」（以下「効果２」という。）

（イ）　これらの記載に基づいて検討する。

ａ　前記の従来技術の問題点及び目的の記載によれば、本件発明１は、まず、従来のログイン回数同期方式の問題点１ないし３の不都合を、「共通変化データを被認証側のログイン行為には直接関係しない客観性のあるパラメータによって変化するものに」することによって解決するものであると認められる。

これをまず問題点２について見ると、従来のログイン回数同期方式では、被認証側と認証側とのやりとりに基づいて認証用データの更新の同期をとっているために、交信エラーによる誤った更新が生じやすいという不都合があったのを、「被認証側のログイン行為には直接関係しない」「時間という全国共通の客観的なパラメータに従って変化する時間変数データを双方の共通因子として利用して認証用データの更新の同期をとっている」ものとしたことによって、「ログイン回数同期方式のような共通変化データが双方の間で食い違ってしまい同期が狂ってしまう不都合を極力防止し得る」（前記効果１）ようにしたものであると認められる。

また、問題点３について見ると、従来のログイン回数同期方式では、被認証側と認証側とで一旦ログイン回数の同期が狂った場合には、認証側において、不正なアクセスか同期の狂いによるアクセスかの判定がつきにくくなり、同期を修復させるのが困難になるという問題点が指摘されているが、これは、ログイン回数同期方式では、被認証側と認証側とのやりとりに基づいて認証用データの更新の同期をとっているために、被認証側のデータと認証側のデータの同期が狂った場合に、本来は何が正しいかを判定する基準がないため、同期が狂っているか否かの判定ができなくなるからであると考えられる。これに対して本件発明１は、「被認証側のログイン行為には直接関係しない」「時間という全国共通の客観的なパラメータに従って変化する時間変数データを双方の共通因子として利用して認証用データの更新の同期をとっている」（前記効果１）ものとしたことによって、「時間という全国共通の客観的なパラメータ」を判定基準として、同期が狂っているか否かを判定することができるようにし、それによって、被認証側と認証側とで一旦狂った同期を容易に修復できるようにしたものであると考えられる。

さらに、ログイン回数同期方式の前記問題点１の解決原理については、本件明細書１に特段明示されていないが、ログイン回数のような、被認証側と特定の認証側との間でのみ通用するパラメータではなく、「被認証側のログイン行為には直接関係しない」「時間という全国共通の客観的なパラメータに従って変化する時間変数データを双方の共通因子として利用して認証用データの更新の同期をとっている」（前記効果１）ものとしたことによって、複数の認証側間でのパラメータも共通のものとなり、被認証側と複数の認証側との間で更新の同期を図ることができるようになったものであると解される（なお、ログイン回数を共通変化データとする場合のこのような問題点は、認証側が複数の場合以外に、被認証側が複数の場合にも同様に生起する問題点であることは容易に理解できるところであるが、

この点も、本件発明１では、同様の原理によって解決されることになると考えられる。）。

このように、本件発明１では、まず、「時間という全国共通の客観的なパラメータに従って変化する時間変数データを双方の共通因子として利用」することによって、従来のログイン同期回数方式の問題点を解決したものであると認められる。

そして、それを前提として、「クロック手段の狂いに起因した時間変数データの誤差が自動的に修復されるために、時間変数データの誤差が徐々に蓄積されて双方での認証用データの更新の同期が狂ってしまう不都合も極力防止し得る」（前記効果２）ようにしたものであると認められる。

ｂ　ところで、前記のとおり、本件発明１の構成要件における「時間変数データ」については、被認証側が用いるものは「クロック手段が計時する時間に応じて変化する」とされているのに対し、認証側が用いるものは、単に、「時間に応じて変化する」とされており、両者の間には相違があるが、このような相違の技術的意義については、本件明細書１では直接明示されていない。

そこで、前記実施例の記載を検討すると、実施例では、被認証側の腕時計３３は、クロック機能を有しているが、時刻標準電波等のコード／データ放送による信号に基づいて、逐一、標準時刻と表示時刻との誤差が修正されるようにされており、この修正された表示時刻から時間変数データを生成し、それを認証用データとしているものと認められる。

他方、認証側のコンピュータ１３又は１４も、予め登録されているシークレット関数に現在時刻からなる入力信号を代入して、認証を行うこととされているが、認証側のコンピュータ１３又は１４の計時する現在時刻については、被認証側の腕時計３３のように、標準時刻との誤差を修正する旨の記載は全くないから、そのような修正は行われないものと解される。そしてこの場合、認証側のコンピュータ１３又は１４の現在時刻も、被認証側の腕時計３３と同じく、標準時刻との間で誤差を生じるとしたならば、単に被認証側の腕時計３３の表示時刻と標準時刻の誤差を修正するだけでは、両者の計時時刻は一致したものとはならず、適正な認証が行われないこととなってしまうから、実施例における認証側のコンピュータ１３又は１４が計時する現在時刻は、常に標準時刻に一致していることが前提とされているものと解さざるを得ない（なお、本件明細書１の【００４５】に記載されている許容値Ｋ秒の設定は、「腕時計３３内で識別信号を算出するまでに要する時間やシークレットルール登録コンピュータ１３または１４までのデータ通信所要時聞等を考慮した遅延時間であり、たとえば３秒等の短い時間である」とされているから、これは、腕時計３３とコンピュータ１３又は１４の計時する現在時刻が一致していて初めてその機能を発揮するものでもある。）。

そうすると、実施例においては、認証側の現在時刻は標準時刻そのものであるのに対し、被認証側の現在時刻は標準時刻との間で誤差が生じ得るものであり、被認証側の腕時計３３に生じる誤差を標準時刻に逐一修正することによって、被認証側の時間変数データと認証側の時間変数データを一致させて、適正な認証が行われるようにしている例が記載されているといえ、これ以外の実施例は記載されていないと認められる。

ｃ　このような実施例の記載を、前記構成要件上の「時間変数データ」の相違と照らし合わせると、被認証側と認証側で用いる「時間変数データ」には、前者が「前記クロック手段が計時する時間に応じて変化する」ものであるのに対して、後者が「時間に応じて変化する」ものとされている趣旨は、被認証側の「時間」は、「クロック手段」（構成要件②）が計時するもので、標準時刻との間で誤差が生じる性質を有するものであるのに対し、認証側の「時間」は標準時刻そのものであり、両者の「時間変数データ」には、このような性質上の差異があることを意味するものと解するのが相当である。

そして、このような理解からすれば、構成要件⑤の「時間に応じて変化する時間変数データ」とは、「標準時刻に応じて変化する時間変数データ」という意味であると解される。

もっとも、このように被認証側の時間変数データと認証側の時間変数データとは性質が異なるものであるとすると、両者は常に一致する保証はないことになる。それにもかかわらず、両者を「共通変化データ」として用いるということの意味を検討すると、①前記効果１でも、時間変数データを共通変化データとして利用することによって、「共通変化データが双方の間で食い違ってしまい同期が

狂ってしまう不都合を極力防止し得る」と記載されているにとどまることや、②被認証側と認証側とで常に一致する保証がないとされているログイン回数でさえも、本件明細書１では「共通変化データ」として記載されていることからすると、「共通変化データ」とは、本来は被認証側と認証側とで共通に変化して一致するはずのデータという程度の意味であると解するのが相当である。

そして、以上のように解することは、先に検討したような、「時間という全国共通の客観的なパラメータに従って変化する時間変数データを双方の共通因子として利用」することによって、従来のログイン回数同期方式の問題点１ないし３を解決する原理とも符合する。すなわち、認証側の時間を標準時刻とし、被認証側の時間をクロック手段が計時する時間とした場合、両者は通常は一致するようにセットされるものであり、本来は一致すべきものであるから、両者を共通変化データとして利用する場合には、「同期が狂ってしまう不都合を極力防止し得る」（問題点２関係）。また、認証側と被認証側の同期が狂った場合でも、標準時刻という客観的なパラメータがあるために、これを基準に同期が狂ったか否かを判定することが可能となる（問題点３関係）。さらに、被認証側又は認証側が複数存する場合でも、いずれも標準時刻を基準として統一的に同期を行うことができる（問題点１関係）。前記効果１において、「時間という全国共通の客観的なパラメータに従って変化する時間変数データを双方の共通因子として利用して認証用データの更新の同期をとっている」とあるのは、このように、標準時刻を基準として同期を行うことを意味するものと解するのが相当である。

そしてまた、前記のように従来のログイン回数同期方式の問題点１が、「時間という全国共通の客観的なパラメータに従って変化する時間変数データを双方の共通因子として利用」したことによって解決されていると考えられることからすると、被認証側及び認証側の「時間変数データ」及び「共通変化データ」は、いずれも、「クロック手段が計時する時間」（被認証側）又は「時間」（認証側）のみに応じて変化するものであることを要し、特定の被認証側と特定の認証側との間でのみ通用（共有）するデータを用いて生成されたものは含まれないと解するのが相当である。

ｄ　次に、「誤差自動修復手段」について検討すると、特許請求の範囲の記載上、「誤差」とは、「前記クロック手段の狂いに伴い前記時間変数データに…生じた」ものであるとされているが、先に検討したところからすれば、本件発明１では、ここにいう「クロック手段」は被認証側に設けられているものであり、他方、認証側の時間は標準時刻に一致しているから、「クロック手段の狂い」とは、被認証側の時間が標準時刻との間で生じた狂いのことを意味すると解される。したがって、ここにいう「誤差」とは、被認証側のクロック手段が標準時刻との間で狂いを生じたことに伴い、被認証側の時間変数データに生じた狂いを意味すると解するのが相当である。そして、「修復」とは、このように被認証側のクロック手段に生じた狂いを、標準時刻を基準に同期できるように修正することを意味すると解するのが相当である。そしてこのことは、前記のような従来技術の問題点３の解決原理とも符合する。

ウ　被告の主張について

（ア）　被告は、構成要件⑤の「時間」を標準時刻を意味すると解する理由が明らかでないし、また、そのように解すると、「前記クロック手段の狂いに伴い前記時間変数データに誤差が生じた場合」（構成要件⑥）という構成要件が出てこなくなり不合理であると主張する。

しかし、構成要件⑤の「時間」は、明らかに、構成要件③の「クロック手段が計時する時間」とは区別して記載されており、しかもその区別は、実施例の記載を参酌し、かつ時間変数データを共通変化データとして利用することによってログイン回数同期方式の問題点が解決される原理を踏まえると、構成要件⑤の「時間」は、標準時刻を意味するものと解するのが合理的であることは、先に述べたとおりである。

そして、このように解しても、構成要件⑤の「時間」は、構成要件③の「クロック手段が計時する時間」とは異なる性質を有するものであり、常に両者が一致する保証はないから、「前記クロック手段の狂いに伴い前記時間変数データに誤差が生じた場合」（構成要件⑥）という構成要件は十分に意味がある。

したがって、被告の上記主張は採用できない。

（イ）　被告は、本件発明の目的及び効果の記載中、「ログイン行為には直接関係しない」「全国共通に変化する客観的なパラメータに従って変化する時間変

数データを双方の共通因子として利用」との意味は、「共通変化データ」に関して、ログイン回数同期方式のように、データの値の増減がログイン行為には直接関係せず、当事者間で独自に変化するクローズドなパラメータを利用するものではないという意味であるにすぎないと主張する。

しかし、前記のとおり、「時間変数データを双方の共通因子として利用」することによって、ログイン回数同期方式の３つの問題点を解決することができるのは、標準時刻を基準とする同期を行うからである。そしてまた、時間に関して、「全国共通に変化する客観的なパラメータ」というのは、標準時刻以外に存しない（標準時刻との間で誤差を生じ得るようなクロック手段が刻む時間は、全国共通に変化するものとはいえない。）。

したがって、本件発明１は、標準時刻に従って変化する時間変数データを、双方で共通に変化するはずの因子として利用するものであると解されるから、被告の主張は採用できない。

（ウ） 被告は、本件発明１において、「誤差」の修復は、誤差が生じた場合、アクセス希望者側の認証用データと、認証側の適否判定用データに齟齬が生じ、認証に支障をきたすため、これを防止するために行われるものであるから、構成要件⑥における「誤差」とは、アクセス希望者側で認証用データの生成に使用された時間変数データと、認証側で適否判定用データの生成に使用された時間変数データとの差のことをいうと解すべきであると主張する。

確かに、本件発明１における「誤差修復」の目的からすれば、構成要件⑥における「誤差」は、アクセス希望者側で認証用データの生成に使用された時間変数データと、認証側で適否判定用データの生成に使用された時間変数データとの差でなければならないとはいえる。

しかし、先に述べたとおり、本件発明１では、認証側の「時間」は標準時刻そのものであるのに対し、被認証側の「時間」は「クロック手段が計時する」ものであるから、「クロック手段の狂いに伴い…生じた」誤差は、被認証側の「時間」について標準時刻との間で生じた狂いを意味するものと解され、単に被認証側と認証側の「時間」の差一般を意味するものとは解されない。

したがって、被告の主張は採用できない。

（エ） 被告は、上記のように解するのは、特許発明の技術的範囲を実施例に限定して解釈するものであって不当であると主張する。

特許発明の技術的範囲が明細書に記載された実施例に限定されるものでないことは、一般論としてはそのとおりである。

しかし、本件では、先に見たように、①特許請求の範囲に記載された文言、②従来技術の問題点を解決する原理、③それらが具体化されたものとしての実施例の記載を総合的に検討した結果として、特許請求の範囲の文言を合理的に解すると、前記のような解釈に至るのであって、単に特許発明の技術的範囲を実施例に限定して解釈するものではない。

⑵ ＲＳＡシステムについて

ア ＲＳＡシステムとその使用方法の内容につき当事者間に争いのない別紙「ＲＳＡシステム説明書」（下線部分及び第１０図を除く。）によれば、ＲＳＡシステムは、同別紙第一の一の⑴ないし⑻記載の製品名の製品から構成され、そのうち、被認証側で使用するのが製品⑶ないし⑻（原告製品③ないし⑧）であり、認証側で使用するのが製品⑴⑵（原告製品①②）である。

被認証側装置には、トークンコード方式、パスコード方式及びソフトウェアトークン方式の３タイプがある。トークンコード方式では、製品⑶又は⑷が使用され、パスコード方式では製品⑸が使用され、ソフトウェアトークン方式では製品⑹ないし⑻が使用される（３つとも使用される場合と製品⑹のみが使用される場合とがある。）。

イ このうち、まず、被認証側に製品⑶⑷（原告製品③⑤）が使用される場合（トークンコード方式）について検討する。

（ア） 別紙「ＲＳＡシステム説明書」によれば、製品⑶⑷が使用されるシステムの内容は、次のとおりである。

ａ 認証側の製品⑴⑵は認証側で使用されるものであり、コンピュータにインストールして使用される。他方、被認証側の製品⑶⑷には、クロック手段が内蔵されており、このクロック手段は、製品に組み込まれる時点で協定世界時間に合わせられるが、それ以後は時刻の調節は不可能である。

被認証側と認証側のクロックは別個独立のものであり、双方のクロ

ックが計時する時刻に誤差が生じることは避けられない。
ｂ　被認証側の製品(3)(4)には、トークンコード・アルゴリズム及びクロック等が内蔵されており、クロックが計時する時刻データ等から、トークンコード・アルゴリズムに従って、一定時間ごとに変化する認証用データ（トークンコード）が生成され、これが、被認証側の利用者のコンピュータから、製品(2)が組み込まれたコンピュータを経由して製品(1)が組み込まれたコンピュータへ送信される。
ｃ　認証用データ（トークンコード）を受信すると、認証側の製品(1)は、その利用者名に対応するオフセット値（後記ｄ参照）等の情報を、製品(1)が組み込まれたコンピュータのデータベースから読み出す。そして、製品(1)が組み込まれたコンピュータのクロックが計時する時刻を協定世界時間に変換して、前記オフセット値を加え、そのオフセット加算した時刻データ等から、トークンコード・アルゴリズムに従って、比較用トークンコードを生成する。ただし、比較用トークンコードは、製品(1)が組み込まれたコンピュータのクロックが計時する時刻を協定世界時間に変換して前記オフセット値を加えた時刻データを中心とするその前後±１期間の時刻データ（３つの時刻データ）によって３種類生成される。
３種類の比較用トークンコードのいずれかと被認証側のコンピュータから送信されてきた認証用データ（トークンコード）が一致した場合には、ＹＥＳの判断がなされて、他の条件も判定した上で、認証する旨の判定をして、被認証側にアクセスを許容する旨の返答を行う。
ｄ　利用者から初めて認証要求があった際、製品(1)は、製品(1)が組み込まれたコンピュータのクロックが計時する時刻を協定世界時間に変換した時刻データを中心とするその前後±７２０期間の時刻データに基づき、１４４１個の比較用トークンコードを生成させ、当該利用者から送られてきた認証用データと比較して、期間のズレを認識し、認証後直ちに、当該被認証側（利用者）の情報として、認証側の製品(1)が組み込まれたコンピュータのデータベースに記憶させる（オフセット処理）。
当該利用者が２回目の認証を受けようとする場合、製品(1)は、前記によってデータベースに記憶されたオフセット値を読み出して、認証側のクロックが計時する現在時刻に前記オフセット値を加え、そのオフセット加算したものを時刻データとして用いて、比較用トークンコードを生成する。
２回目の認証が行われた場合、前回認証時に認証側コンピュータのデータベースに記憶されたオフセット値に、前回認証時から今回認証時までに新たに生じた期間のズレを加算して、これを認証側のコンピュータのデータベースに記憶させる。
３回目以降の認証後のオフセット更新も同様である。
（イ）　これによれば、被認証側に製品(3)(4)（原告製品③⑤）が使用される場合のＲＳＡシステムとして、次の点を指摘できる。
ａ　製品(3)(4)に内蔵されたクロック手段も、製品(1)が組み込まれた認証側のコンピュータのクロックも、本来は協定世界時間に一致するものとしてセットされると思われるが、稼働後も協定世界時間に一致することが保証されているわけではない（特に、被認証側のクロック手段は、製品に組み込まれた後は協定世界時間とのずれを修正するよう調節することができない。）。
ｂ　したがって、被認証側のトークン・コードと認証側の比較用トークン・コードとの差は、被認証側のクロック手段の狂いだけでなく、認証側のクロック手段の狂いによっても生じるものである。
なお、乙７（ＲＳＡシステムの構築のための教材）の13頁では、被告指摘のとおり、トークンとＡＣＥ／Ｓｅｒｖｅｒ間では、トークンに内部的に組み込まれた時計とＡＣＥ／Ｓｅｒｖｅｒがインストールされた端末のシステム時刻が一致している必要があるとも記載されている。しかし同号証の14頁では、「トークンの時刻とＡＣＥ／Ｓｅｒｖｅｒの時刻は必ずしも一致するとは限りません」と明記されている上、甲17からしても、ＲＳＡシステムでは、両者が一致しないことを前提に、比較用トークンコードを複数作成・照合する処理が設けられていると認められる。したがって、乙７の前記記載は、単にトークンとＡＣＥ／Ｓｅｒｖｅｒ間の現在時刻が一致するようにしておくことが望ましい旨を記載したにとどまるものと解される。
ｃ　被認証側の時刻と認証側の時刻にズレがある場合は、専ら認証側において、オフセット処理等によって対応がなされている。
ｄ　認証側の比較用トークン・コードを作成するために用いられるオフ

セット値は、被認証側ごとにそれぞれ異なるものである。

（ウ）　以上に基づいて、被認証側に製品(3)(4)（原告製品③⑤）が使用される場合のＲＳＡシステムの構成要件①③⑤⑥の充足性を検討すると、まず、総体的にいえば、前記のとおり、本件発明１は、標準時刻という客観的な基準に基づいて被認証側と認証側の同期を図るシステムであるのに対し、ＲＳＡシステムでは、標準時刻を特に基準とすることなく、特定の被認証側と認証側との計時時間に着目して、両者間でその時間差を相対的に調整することによって同期を図るシステムであるという相違があるということができる。これを、各構成要件について具体的にいえば、次のとおりである。

ａ　認証側たる製品(1)がインストールされるコンピュータは、当然にクロック手段を備えているが、コンピュータのクロック手段は標準時刻との間で誤差が生じ得るものであり、それを自動的に修正する機能が特に製品(1)に備わっているわけでもないから、認証側が計時する時間は必ず標準時刻とは一致するわけではない。

したがって、被認証側に製品(3)(4)（原告製品③⑤）が使用される場合のＲＳＡシステムは、本件発明１の構成要件⑤にいう「時間」、すなわち標準時刻を用いない点で、構成要件⑤と異なる。

ｂ　被告が被認証側に製品(3)(4)（原告製品③⑤）が使用される場合のＲＳＡシステムにおいて認証側の時間変数データに当たると主張する「オフセット更新後時間変数データ」は、オフセット更新がなされた次のアクセス時に生成される、３種類の比較用トークンコードの中心値と実質的に同一であると解されるが、この比較用トークンコードの中心値は、認証側のクロックが計時する時刻にオフセット値を加算した時間データから生成されるものである。そうすると、被認証側に製品(3)(4)（原告製品③⑤）が使用される場合のＲＳＡシステムにおいては、時間とオフセット値という２種類のデータを組み合わせたものを認証側の共通変化データとして利用しているといえる。

しかし、これら２種類のデータのうち、オフセット値は、認証側と特定の被認証側との間でのみ通用するデータである点で、本件明細書１で従来技術として挙げられているログイン回数と同じ性質を有する。そして、そうであるために、オフセット値をも共通変化データの一部として利用する場合には、複数の被認証側との間での共通変化データとして利用することができないというログイン回数同期方式の問題点を帯有しており、被認証側に製品(3)(4)（原告製品③⑤）が使用される場合のＲＳＡシステムにおいてこれらの問題点が解決されているのは、被認証側（利用者）ごとに異なるデータ（オフセット値）を使い分けて、個々の被認証側との間での相対的な同期を行うようにすることによってであると認められる。

また、何らかの事情でオフセット値が狂った場合には、認証側にとって、不正なアクセスと同期が狂ったことによるアクセスとの判別がつきにくく、一旦狂った同期を修復させるのが困難になるというように、ログイン回数同期方式で指摘された問題点も帯有している（ＲＳＡシステムでは、ネクストトークンコードモードという処理を施すことによって解決されているものと認められる。）。

他方、本件発明１は、これらの問題を、標準時刻という統一的・客観的な基準を共通変化データとして採用することによって解決したものであることは前記のとおりであるから、構成要件⑤の「時間に応じて変化する時間変数データ」は、標準時刻のみに基づいて生成されると解すべきことは前記のとおりである。

したがって、ＲＳＡシステムは、本件発明１の構成要件⑤の「時間に応じて変化する時間変数データ」を充足しない。

ｃ　被告が構成要件⑥の「誤差」に当たると主張する「オフセット更新後誤差」は、前回アクセス時のオフセット更新後に、被認証側と認証側との間に累積された時間の差を意味するものであるが、この差は、被認証側と認証側の間での相対的な差であるにとどまり、本件発明１の「誤差」のように、被認証側のクロック手段の狂いによって生じた、被認証側の時刻と標準時刻との差ではない。

また、本件発明１における「誤差」の「修復」は、被認証側においてのみ行われるものと解されるところ、被告がＲＳＡシステムにおいて「修復」に当たると主張するオフセット処理は、専ら認証側において行われている。

したがって、被認証側に製品(3)(4)（原告製品③⑤）が使用される場合のＲＳＡシステムは、構成要件⑥の「誤差自動修復手段」を具備しない。

ｄ　なお、ＲＳＡシステムの内容については、争点(1)のとおり争いがあ

るが、ＲＳＡシステムが少なくとも上記(ア)記載の内容であることについては争いがなく、上記判断は、争いのある部分の認定いかんによっては左右されない。
　　ウ　次に、被認証側に製品(5)(原告製品④）が使用される場合（パスコード方式）は、別紙「ＲＳＡシステム説明書」によれば、製品(5)には、製品(3)(4)の内容に加えてパスコード・アルゴリズムが内蔵されており、利用者が認証要求時にＰＩＮ(Personal Identification Number、各利用者に割り当てられた固有の識別番号）をトークンに入力すると、ＰＩＮとトークンコードからパスコード・アルゴリズムによって認証用データ（パスコード）が生成される点が、製品(3)(4)を使用する場合と異なっているが、その他は概ね同一である。
　　また、被認証側に製品(6)ないし(8)（原告製品⑥ないし⑧）が使用される場合（ソフトウェアトークン方式）は、別紙「ＲＳＡシステム説明書」によれば、被認証側のクロック手段として、製品(6)がインストールされたコンピュータのものを利用するため、時刻の調整をすることが可能であるという点は異なるが、その他は上記パスコード方式の場合と概ね同一である。
　　そうすると、先にイ(ウ)で述べたところと同様に、被認証側に製品(5)ないし(8)（原告製品④、⑥ないし⑧）を使用したＲＳＡシステムについても、本件発明１の構成要件⑤及び⑥を充足しない。
　(3) まとめ
　　以上によれば、原告製品（⑨を除く）は、本件発明１の構成要件⑤⑥を充足しない。
２　争点(2)イ(イ)(ウ)（ＲＳＡシステムが本件発明３の構成要件④⑥⑦及び⑧を充足するか）について
　(1) 本件発明３における「共通変化データ」、「時間変数データ」、「誤差」、「誤差自動修復手段」の意義について
　　ア　本件発明３の特許請求の範囲の記載について
　　(ア)　本件発明３の特許請求の範囲の記載の記載は、前記のとおりであるが、そこでは、「共通変化データ」、「時間変数データ」、「誤差」、「誤差自動修復手段」は、次のようなものとして記載されている。
　　ａ　「共通変化データ」は、「前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な」ものである（構成要件④）。
　　ｂ　被認証側（アクセス希望者側）では、「アクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成」し（構成要件④）、この「可変型パスワードデータが前記認証手段に転送され」るが（構成要件⑤）、この可変型パスワードデータは、「クロック機能を有」する「可変型パスワードデータ生成手段」が、「該クロック機能が計時する時間に応じて変化する時間変数データ」を用いて生成するものである（構成要件⑥）
　　ｃ　認証側では、「時間に応じて変化する時間変数データ」を用いて、「転送されてきた可変型パスワードデータの適否を判定して認証を行なう」ものである（構成要件⑦）。
　　ｄ　「誤差自動修復手段」は、「前記可変型パスワードデータ生成手段のクロックが狂って」「前記時間変数データに誤差が生じた場合にその誤差を自動的に修復させて経時的に誤差が累積されることを防止可能とする」ものである（構成要件⑧）。
　　(イ)　これらの特許請求の範囲の記載に対しては、先に本件発明１について述べたのと同様の指摘をすることができる。
　　イ　また、本件明細書２の他の部分には、次の記載がある（甲14）。
　　(ア)　実施例では、本件発明１について指摘した本件明細書１の記載と同一の記載がある（【００３４】【００４０】【００４１】【００４２】【００４４】【００４５】【００４６】）。
　　(イ)　そして、「本発明の構成要件と前記実施の形態との対応関係を説明する」（本件公報２【００６５）】として、次の記載がある。
　　ａ　「前記設備利用者所有の装置３３により、アクセス希望者固有の秘密の変換用データを記憶している、前記アクセス希望者所有のパーソナル演算装置が構成されている。そして、前述したように、図７のＳ５，図８のＳ１０に示された現在の時刻あるいは図９のＳ２４に示されたＩ，Ｓ１８に示されたＪにより、前記パーソナル演算装置と後述するアクセス許否判定手段との両者に共通に使用される変数データであって、前回のアクセス時と今回のアクセス時とで変化可能な変数

データが構成されている。」（本件公報２【００６５】）

ｂ　「コンピュータ１３または１４により、前記アクセス対象とは別の場所に設置されて該アクセス対象側とデータ通信が可能であり、アクセス制御のための認証を統括して行なって集中管理を行なう認証手段が構成されている。」（同【００６７】）

ｃ　「図７のＳ１，Ｓ２により、前記の可変型パスワードデータ生成手段のクロック機能の狂いに伴い前記時間変数データに誤差が生じた場合にそれを自動的に修復させて経時的に誤差が累積されることを防止するための誤差自動修復手段が構成されている。」（同【００７０】）

（ウ）　そして、本件発明３の効果としては、次の記載がある（本件公報２の１９欄３１行目以下）。

ａ　「時間に応じて変化する時間変数データを共通変化データとして用いて転送されてきた可変型パスワードデータの適否が判定されて認証が行なわれるために、前回のアクセス時と今回のアクセス時とで異なった内容の可変型パスワードデータとなり、セキュリティが向上する。」

ｂ　「可変型パスワードデータ生成手段のクロックが狂って時間変数データに誤差が生じた場合にその誤差が自動的に修復されて経時的に誤差が累積されることが防止可能となるために、時間変数データの誤差に起因したアクセス不能状態等が発生する不都合を極力防止することができる。」

（エ）　そして、コンピュータ１３、１４を始め、認証側については、被認証側の腕時計３３のように、標準時刻との誤差を修正する旨の記載は全くない。

ウ　このように、本件発明３についての特許請求の範囲の記載は、本件発明１とほぼ同じ（構成要件②③により、アクセス対象が複数あり、そのための認証の集中管理を行う手段がある点のみが異なる）であって、実施例及び作用効果もほぼ同じであること、また、本件発明３は、本件明細書１に係る特許出願からの分割出願であって、その内容は、本件明細書１に記載された範囲のものに限られることからすると、本件発明３の構成要件④⑥⑦⑧の「共通変化データ」、「時間変数データ」、「誤差」、「誤差自動修復手段」の意義は、本件発明１の構成要件①③⑤⑥におけるものと同様に解するのが相当である。

⑵　そうすると、本件発明１について述べたのと同様に、ＲＳＡシステムは、本件発明３の構成要件⑦とは「時間」及び「時間に応じて変化する時間変数データ」の点で異なり、また構成要件⑧の「誤差自動修復手段」を具備しないから、構成要件⑦及び⑧を充足しない。

３　争点⑵ウ（イ）（ＲＳＡシステムが本件発明４の構成要件④⑥⑦を充足するか）について

本件発明４の特許請求の範囲の記載は、前記のとおりであるが、その構成要件①ないし⑦の記載は、本件発明３の構成要件①ないし⑦の記載と同一である。そして、同一の明細書中で同一の文言が使用されている以上、特段の記載のない限り、その意味も同様に解するのが相当であるところ、本件明細書２には、本件発明４での意味を特に本件発明３と区別して用いる旨の記載はなく、また同明細書からその趣旨が読み取れるともいえない。

したがって、本件発明４の構成要件⑦は、本件発明３の構成要件⑦と同じ意味に解するのが相当であり、先に述べたのと同様、ＲＳＡシステムは、本件発明４の構成要件⑦とは「時間」及び「時間に応じて変化する時間変数データ」の点で異なり、構成要件⑦を充足しない。

４　争点⑶アイ（ＲＳＡシステムの使用方法が本件発明２の構成要件①②④及び⑥を充足するか）について

本件発明２における「共通変化データ」、「時間変数データ」、「誤差」、「誤差自動修復手段」の意義は、先に本件発明１について述べたところと同様に解されるから、ＲＳＡシステムを使用した方法は、本件発明２の構成要件④とは「時間」及び「時間に応じて変化する時間変数データ」の点で異なり、また、構成要件⑥の「誤差自動修復手段」を具備しないから、構成要件④及び⑥を充足しない。

５　争点⑷（原告製品⑨は、本件発明に係る物の生産又は方法の実施にのみ使用する物か）

原告製品⑨の内容が、別紙「Ｋｅｏｎ説明書」のとおりであることは当事者間に争いがないところ、同説明書によれば、「電子証明書の発行管理・暗号鍵の管理機能などを提供する」ものである。そして、甲18によれば、ＲＳＡシステムと組み合わせて使用することもできるが、組み合わせないで使用することも可能である

と認められる。したがって、原告製品⑨は、本件発明１ないし４の生産又は実施にのみ使用する物とはいえない。

第５　結論

以上によれば、原告の請求は理由があるから、主文のとおり判決する。

大阪地方裁判所第２１民事部

裁判長裁判官　小　松　一　雄

裁判官　高　松　宏　之

裁判官　安　永　武　央

（別紙）　物件目録

（別紙）　ＲＳＡシステム説明書

第一　製品の説明

一　製品名

(1)ＡＣＥ／Ｓｅｒｖｅｒ
(2)ＡＣＥ／Ａｇｅｎｔ
(3)ＳｅｃｕｒＩＤ スタンダードタイプトークン
(4)ＳｅｃｕｒＩＤ キーフォブ（キーホルダ）タイプトークン
(5)ＳｅｃｕｒＩＤ ピンパッドタイプトークン
(6)ＳｅｃｕｒＩＤ ソフトウェアトークン
(7)ＳｅｃｕｒＩＤ スマートカード
(8)ＳｅｃｕｒＩＤ カードリーダー

二　製品の概要

１　製品(1)(2)(6)はソフトウェア・プログラムであり、ＣＤ（コンパクトディスク）やＦＤ（フロッピーディスク）に収容された形で販売される。それ以外の製品(3)(4)(5)(7)(8)はハードウェアである。

製品(1)(2)は認証側で使用されるものであり、コンピュータにインストールして使用される。

製品(3)～(8)は被認証側で使用されるものであるが、これらすべてが認証システムを構成するために必要であるということはない。

ある特定の認証システムの中で選択使用される製品の組み合わせの例は以下のとおりである。

製品(1)及び(2)及び［(3)又は(4)］
製品(1)及び(2)及び(5)
製品(1)及び(2)及び(6)
製品(1)及び(2)及び(6)及び(7)及び(8)

２　製品(3)(4)(5)には、クロック手段が内蔵されている。このクロック手段は、製品に組み込まれる時点でＵＴＣ（Coordinated Universal Time。協定世界時間）に合わせられるが、それ以後は時刻の調節は不可能である。

第二　上記製品を利用したアクセス制御用認証システム（ＲＳＡシステム）の説明

一　認証システムの概要（第１図参照）

１　被認証側装置Ⅰと認証側装置Ⅱからなり、両者は通信可に接続⑤される。

２　被認証側装置Ⅰには、トークンコード方式、パスコード方式、ソフトウェアトークン方式の３つのタイプがある。トークンコード方式では、ＳｅｃｕｒＩＤ スタンダードタイプトークン（製品(3)）又はＳｅｃｕｒＩＤ キーフォブ（キーホルダ）タイプトークン（製品(4)）が使用され、パスコード方式では、ＳｅｃｕｒＩＤ ピンパッドタイプトークン（製品(5)）が使用され、ソフトウェアトークン方式では、ＳｅｃｕｒＩＤ ソフトウェアトークン（製品(6)）とＳｅｃｕｒＩＤ スマート

カード（製品(7)）とＳｅｃｕｒＩＤ カードリーダー（製品(8)）が使用される（３つとも使用される場合と、ＳｅｃｕｒＩＤ ソフトウェアトークンのみが使用される場合とがある）。

いずれの方式の場合も、利用者が、利用者のコンピュータ①で認証側装置Ⅱと通信する。

３　認証側装置Ⅱは、ＡＣＥ／Ｓｅｒｖｅｒ（製品(1)）が組み込まれたコンピュータ⑦とＡＣＥ／Ａｇｅｎｔ（製品(2)）が組み込まれたコンピュータ⑥からなり、両者（⑥⑦）は通信可に接続⑤され、ＡＣＥ／Ａｇｅｎｔが組み込まれたコンピュータ⑥は利用者のコンピュータ①と通信可に接続⑤される。

二　被認証側での認証用データ生成

１　トークンコード方式の場合（第２図参照）

各利用者が所持するＳｅｃｕｒＩＤ スタンダードタイプトークン（製品(3)）又はＳｅｃｕｒＩＤ キーフォブ（キーホルダ）タイプトークン（製品(4)）には、シード（各利用者が所持するトークンに固有の番号）、トークンコード・アルゴリズム（トークンコード生成のための乱数発生プログラム。当該認証システムを利用するすべての利用者が所持するトークンとＡＣＥ／Ｓｅｒｖｅｒに同じプログラムが内蔵されている）及びクロックが内蔵されており、クロックが計時する時刻データとシードから、トークンコード・アルゴリズムに従って、一定時間ごとに変化する認証用データ（トークンコード）が生成され（Ｓ１０１）、トークンの表示部に表示される（Ｓ１０２）。この一定時間（一期間）は３０秒、６０秒、１２０秒のいずれかである。クロックの計時する時刻が変化しても、一期間内であれば認証用データは同一である。

２　パスコード方式の場合（第３図参照）

各利用者が所持するＳｅｃｕｒＩＤ ピンパッドタイプトークン（製品(5)）には、シード、トークンコード・アルゴリズム、パスコード・アルゴリズム（パスコード生成のための乱数発生プログラム。当該認証システムを利用するすべての利用者が所持するトークンとＡＣＥ／Ｓｅｒｖｅｒに同じプログラムが内蔵されている）及びクロックが内蔵され、クロックが計時する時刻データとシードから、トークンコード・アルゴリズムに従って、一期間ごとに変化するトークンコードが生成され（Ｓ２０１）、トークンの表示部に表示されるようになっており（Ｓ２０２）、利用者が認証要求時にＰＩＮ（Personal Identification Number、各利用者に割り当てられた固有の識別番号）をトークンに入力すると、ＰＩＮと前記トークンコードから、パスコード・アルゴリズムに従って認証用データ（パスコード）が生成され（Ｓ２０４）、トークンの表示部に表示される（Ｓ２０５）。クロックの計時する時刻が変化しても、一期間内であれば認証用データは同一である。

３　ソフトウェアトークン方式の場合（第４図参照）

(1) ＳｅｃｕｒＩＤ ソフトウェアトークン（製品(6)）のみが使用される場合

ＳｅｃｕｒＩＤ ソフトウェアトークン（製品(6)）には、シード、トークンコード・アルゴリズム及びパスコード・アルゴリズムが内蔵されており、ＳｅｃｕｒＩＤ ソフトウェアトークンがインストールされた利用者のコンピュータのクロックが計時する時刻データとシードから、トークンコード・アルゴリズムに従って、一期間ごとに変化するトークンコードが生成され、利用者のコンピュータの画面上に表示されるようになっており、利用者が認証要求時にＰＩＮを利用者のコンピュータのキーボードから入力すると、ＰＩＮと前記トークンコードから、パスコード・アルゴリズムに従って認証用データ（パスコード）が生成され、利用者のコンピュータの画面上に表示される。クロックの計時する時刻が変化しても、一期間内であれば認証用データは同一である。

なお、ＳｅｃｕｒＩＤ ソフトウェアトークン（製品(6)）には、オプションとして、現在時刻を表示する機能を付けることができる。但し、この場合、現在時刻表示機能を利用中は認証用データは表示できない。

(2) ＳｅｃｕｒＩＤ ソフトウェアトークン（製品(6)）、ＳｅｃｕｒＩＤ スマートカード（製品(7)）、ＳｅｃｕｒＩＤ カードリーダー（製品(8)）が３つとも使用される場合

ＳｅｃｕｒＩＤ スマートカードにはシードが、ＳｅｃｕｒＩＤ ソフトウェアトークンにはトークンコード・アルゴリズム及びパスコード・アルゴリズムが内蔵されており、ＳｅｃｕｒＩＤ ソフトウェアトークンがインストールされた利用

者のコンピュータのクロックが計時する時刻データとＳｅｃｕｒＩＤ カードリーダーを介してＳｅｃｕｒＩＤ スマートカードから利用者のコンピュータに伝送されるシードから、トークンコード・アルゴリズムに従って、一期間ごとに変化するトークンコードが生成され、利用者のコンピュータの画面上に表示されるようになっており、利用者が認証要求時にＰＩＮを利用者のコンピュータのキーボードから入力すると、ＰＩＮと前記トークンコードから、パスコード・アルゴリズムに従って認証用データ（パスコード）が生成され、利用者のコンピュータの画面上に表示される。クロックの計時する時刻が変化しても、一期間内であれば認証用データは同一である。

三　認証用データの送受信（第５図参照）

１　トークンコード方式の場合

利用者名、ＰＩＮ及び前記二１によって生成された認証用データ（トークンコード）が、被認証側の利用者のコンピュータから、ＡＣＥ／Ａｇｅｎｔが組み込まれたコンピュータを経由してＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータへ送信され（Ｓ５０１）、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータはこれを受信する。そして、ＡＣＥ／Ｓｅｒｖｅｒによる認証結果（第６図のＳ６０２参照）が返信される（Ｓ５０２）。なお、トークンコード方式の場合は、ＰＩＮとトークンコードとを合わせたものをパスコードと呼んでいる。

２　パスコード方式（及びソフトウェアトークン方式）の場合

利用者名及び前記二２（あるいは３）によって生成された認証用データ（パスコード方式及びソフトウェアトークン方式の場合、これをパスコードと呼んでいる）が、被認証側の利用者のコンピュータから、ＡＣＥ／Ａｇｅｎｔが組み込まれたコンピュータを経由してＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータへ送信され（Ｓ５０１）、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータはこれを受信する。そして、ＡＣＥ／Ｓｅｒｖｅｒによる認証結果（第６図のＳ６０２参照）が返信される（Ｓ５０２）。

四　認証側装置における認証（適否判定）の仕組み（第６、７、８図参照）

１　トークンコード方式の場合

⑴ 時刻誤差自動許容範囲内の認証

①　前記三１によって利用者名、ＰＩＮ及び前記二１によって生成された認証用データ（トークンコード）をＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータが受信すると（Ｓ６０１）、ＡＣＥ／Ｓｅｒｖｅｒは、その利用者名に対応するシード、ＰＩＮ、オフセット値（後記五参照）等の情報を、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのデータベースから読み出す（Ｓ６０３）。

②　そして、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのクロックが計時する時刻をＵＴＣ（協定世界時間）に変換して（Ｓ６０７）前記オフセット値を加え（Ｓ６１０，Ｓ７０４）、そのオフセット加算した時刻データと前記データベースから読み出されたシードとから、トークンコード・アルゴリズムに従って、比較用トークンコードを生成する（Ｓ６１１，Ｓ７０５）。

③　被認証側と認証側のクロックは別個独立のものであり、双方のクロックが計時する時刻に誤差が生じることは避けられないので、前回認証時以降に生じた双方のクロックが計時する時刻の誤差（被認証側から送られて来たトークンコードに用いられている時刻データと、認証側において、そのトークンコードが受信された時刻にオフセット値を加えた時刻データであって、比較用トークンコードの生成に用いられた時刻データとの差）が±１期間（合計３期間。１期間は３０秒、６０秒、１２０秒のいずれか）の範囲内である場合には自動的に認証を許容するようにするため（Ｓ９０５）、前記②の比較用トークンコードは、前記②のＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのクロックが計時する時刻をＵＴＣ（協定世界時間）に変換して前記オフセット値を加えた時刻データを中心とするその前後±１期間の時刻データ（３つの時刻データ）によって３種類生成される（Ｓ６１１，Ｓ７０５）。

④　この３種類の比較用トークンコードのいずれかと被認証側のコンピュータから送信されてきた認証用データ（トークンコード）が一致した場合には、Ｓ６１２によりＹＥＳの判断がなされて、ＰＩＮが一致することを条件としてＳ６１３によりＹＥＳの判断がなされ、認証する旨の判定をして、被認証側にアクセスを許容する旨の返答を行う（Ｓ６１４）。

⑤　なお、被認証側から送信されて来たトークンコードが、前回の認証時に送信されて来たトークンコードと同じものであった場合には、Ｓ６０９によりＹＥＳの判断がなされて否認証である旨の返答がなされる（Ｓ６０２）。

⑵　時刻誤差自動許容範囲の段階的拡張

認証間隔があいた場合には、被認証側と認証側のクロックが計時する時刻の誤差が前記⑴③の±１期間に収まらない確率が高まる。そこで、前記⑴③の時刻誤差自動許容範囲は、前回の認証時からの間隔が１週間あく毎に±１期間ずつ、最大±１０期間まで拡張されるようになっており、これに応じて前記⑴③の比較用トークンコードの数も２つずつ増加する（Ｓ９２２）。

⑶　ネクストトークンコードモードでの認証

①　前記⑴⑵の時刻誤差自動許容範囲内の認証が一定回数以上失敗した場合、Ｓ９０９でＹＥＳの判断がなされ、被認証側と認証側のクロックが計時する時刻の前回認証時以降に生じた誤差が±１０期間（合計２１期間）の範囲内である場合には認証を許容できるように、ＡＣＥ／Ｓｅｒｖｅｒは時刻誤差許容範囲を拡大する。具体的には、Ｓ９１１によりネクストトークンコードモードＯＮとなり、Ｓ０２によりＹＥＳの判断がなされ、Ｓ０３，Ｓ９１２と進み、時刻誤差許容範囲をＳ９２４に示す最大許容可能範囲にする。

②　そして、被認証側のコンピュータから送信されてきた認証用データ（トークンコード）と拡大された時刻誤差許容範囲内の時刻データから生成される２１種類の比較用トークンコードのいずれかが一致した場合にはＳ９１３によりＹＥＳとなり、認証側のＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータから被認証側のコンピュータに、一定時間が経過して前記認証用データ（トークンコード）から変化した次の期間の認証用データ（ネクストトークンコード）の送信を要求する（Ｓ６２０，Ｓ９１４）。

③　その要求に従って被認証側のコンピュータから送信されてきたネクストトークンコードと、前記②で一致した比較用トークンコードの次期間の比較用トークンコード（Ｓ０４）が一致した場合には、Ｓ６２１，Ｓ９１５でＹＥＳの判断がなされて認証する旨の判定をして、被認証側にアクセスを許容する旨の返答を行う（Ｓ６１４，Ｓ９１７）。

２　パスコード方式の場合

⑴　時刻誤差自動許容範囲内の認証

①　前記三２によって利用者名及び前記二２によって生成された認証用データ（パスコード）をＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータが受信すると（Ｓ６０１）、ＡＣＥ／Ｓｅｒｖｅｒは、その利用者名に対応するシード、ＰＩＮ、オフセット値（後記五参照）等の情報を、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのデータベースから読み出す（Ｓ６０３）。

②　そして、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのクロックが計時する時刻をＵＴＣ（協定世界時間）に変換して（Ｓ６０７）前記オフセット値を加え（Ｓ６１０，Ｓ７０４）、そのオフセット加算した時刻データと前記データベースから読み出されたシード及びＰＩＮから、パスコード・アルゴリズムに従って、比較用パスコードを生成する（Ｓ６１７，Ｓ７０５）。

③　被認証側と認証側のクロックは別個独立のものであり、双方のクロックが計時する時刻に誤差が生じることは避けられないので、前回認証時以降に生じた双方のクロックが計時する時刻の誤差（被認証側から送られて来たトークンコードに用いられている時刻データと、認証側において、そのトークンコードが受信された時刻にオフセット値を加えた時刻データであって、比較用トークンコードの生成に用いられた時刻データとの差）が±２期間（合計５期間。１期間は３０秒、６０秒、１２０秒のいずれか）の範囲内である場合には自動的に認証を許容するようにするため（Ｓ９０５）、前記②の比較用パスコードは、前記②のＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのクロックが計時する時刻をＵＴＣ（協定世界時間）に変換して前記オフセット値を加えた時刻データを中心とするその前後±２期間の時刻データ（５つの時刻データ）によって５種類生成される（Ｓ６１７，Ｓ７０５）。

④　この５種類の比較用パスコードのいずれかと被認証側のコンピュータから送信されてきた認証用データ（パスコード）が一致した場合には、Ｓ６１８によりＹＥＳの判断がなされて認証する旨の判定をして、被認証側にアクセスを許容する旨の返答を行う（Ｓ６１４）。

⑤　なお、被認証側から送信されて来たパスコードが、前回の認証時に送信

されて来たパスコードと同じものであった場合には、Ｓ６０９によりＹＥＳの判断がなされて否認証である旨の返答がなされる（Ｓ６０２）。

⑵ 時刻誤差自動許容範囲の段階的拡張

認証間隔があいた場合には、被認証側と認証側のクロックが計時する時刻の誤差が前記⑴③の±２期間に収まらない確率が高まる。そこで、前記⑴③の時刻誤差自動許容範囲は、前回の認証時からの間隔が１週間あく毎に±１期間ずつ、最大±１０期間まで拡張されるようになっており、これに応じて前記⑴③の比較用トークンコードの数も２つずつ増加する（Ｓ９２２）。

⑶ ネクストトークンコードモードでの認証

① 前記⑴⑵の時刻誤差自動許容範囲内の認証が一定回数以上失敗した場合、Ｓ９０９でＹＥＳの判断がなされ、被認証側と認証側のクロックが計時する時刻の前回認証時以降に生じた誤差が±１０期間（合計２１期間）の範囲内である場合には認証を許容できるように、ＡＣＥ／Ｓｅｒｖｅｒは時刻誤差許容範囲を拡大する。具体的には、Ｓ９１１によりネクストトークンコードモードＯＮとなり、Ｓ０２によりＹＥＳの判断がなされ、Ｓ０３，Ｓ９１２と進み、時刻誤差許容範囲をＳ９２４に示す最大許容可能範囲にする。

② そして、被認証側のコンピュータから送信されてきた認証用データ（パスコード）と拡大された時刻誤差許容範囲内の時刻データから生成される２１種類の比較用パスコードのいずれかが一致した場合にはＳ９１３によりＹＥＳとなり、認証側のＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータから被認証側のコンピュータに、一定時間が経過して前記認証用データ（パスコード）から変化した次の期間の認証用データ（ネクストトークンコード）の送信を要求する（Ｓ６２２，Ｓ９１４）。

③ その要求に従って被認証側のコンピュータから送信されてきたネクストパスコードと、前記②で一致した比較用パスコードの次期間の比較用パスコードが一致した場合には、Ｓ６２３によりＹＥＳの判断がなされて認証する旨の判定をして、被認証側にアクセスを許容する旨の返答を行う（Ｓ６１４）。

３ ソフトウェアトークン方式の場合

⑴ 時刻誤差自動許容範囲内の認証

① 前記三２によって利用者名及び前記二３によって生成された認証用データ（パスコード）をＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータが受信すると（Ｓ６０１）、ＡＣＥ／Ｓｅｒｖｅｒは、その利用者名に対応するシード、ＰＩＮ、オフセット値（後述）等の情報を、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのデータベースから読み出す（Ｓ６０３）。

② そして、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのクロックが計時する時刻をＵＴＣ（協定世界時間）に変換して（Ｓ６０７）前記オフセット値を加え（Ｓ６１０，Ｓ７０４）、そのオフセット加算した時刻データと前記データベースから読み出されたシード及びＰＩＮから、パスコード・アルゴリズムに従って、比較用パスコードを生成する（Ｓ６１１又はＳ６１７，Ｓ７０５）。

③ 被認証側と認証側のクロックは別個独立のものであり、双方のクロックが計時する時刻に誤差が生じることは避けられないので、前回認証時以降に生じた双方のクロックが計時する時刻の誤差（被認証側から送られて来たトークンコードに用いられている時刻データと、認証側において、そのトークンコードが受信された時刻にオフセット値を加えた時刻データであって、比較用トークンコードの生成に用いられた時刻データとの差）が±１０期間（合計２１期間。１期間は３０秒、６０秒、１２０秒のいずれか）の範囲内である場合には自動的に認証を許容するようにするため（Ｓ９０５）、前記②の比較用パスコードは、前記②のＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのクロックが計時する時刻をＵＴＣ（協定世界時間）に変換して前記オフセット値を加えた時刻データを中心とするその前後±１０期間の時刻データ（２１個の時刻データ）によって２１種類生成される（Ｓ９２２）。

④ この２１種類の比較用パスコードのいずれかと被認証側のコンピュータから送信されてきた認証用データ（パスコード）が一致した場合には、認証する旨の判定をして、被認証側にアクセスを許容する旨の返答を行う（Ｓ６１４）。

⑤ なお、被認証側から送信されて来たパスコードが、前回の認証時に送信されて来たパスコードと同じものであった場合には、Ｓ６０９によりＹＥＳの判断がなされて否認証である旨の返答がなされる（Ｓ６０２）。

(2) 時刻誤差自動許容範囲の段階的拡張

認証間隔があいた場合には、被認証側と認証側のクロックが計時する時刻の誤差が前記(1)③の±１０期間に収まらない確率が高まる。そこで、前記(1)③の時刻誤差自動許容範囲は、前回の認証時からの間隔が１週間あく毎に±１０期間ずつ、最大±７０期間まで拡張されるようになっており、これに応じて前記(1)③の比較用トークンコードの数も２０つずつ増加する（Ｓ９２２）。

(3) ネクストトークンコードモードでの認証

① 前記(1)(2)の時刻誤差自動許容範囲内の認証が一定回数以上失敗した場合、被認証側と認証側のクロックが計時する時刻の前回認証時以降に生じた誤差が±７０期間（合計１４１期間）の範囲内である場合には認証を許容できるように、ＡＣＥ／Ｓｅｒｖｅｒは時刻誤差許容範囲を拡大する。具体的には、Ｓ９１１によりネクストトークンコードモードＯＮとなり、Ｓ０２によりＹＥＳの判断がなされ、Ｓ０３，Ｓ９１２と進み、時刻誤差許容範囲をＳ９２４に示す最大許容可能範囲にする。

② そして、被認証側のコンピュータから送信されてきた認証用データ（パスコード）と拡大された時刻誤差許容範囲内の時刻データから生成される１４１種類の比較用パスコードのいずれかが一致した場合にはＳ９１３によりＹＥＳとなり、認証側のＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータから被認証側のコンピュータに、一定時間が経過して前記認証用データ（パスコード）から変化した次の期間の認証用データ（ネクストトークンコード）の送信を要求する（Ｓ９１４）。

③ その要求に従って被認証側のコンピュータから送信されてきたネクストパスコードと、前記②で一致した比較用パスコードの次期間の比較用パスコードが一致した場合には、Ｓ６２３によりＹＥＳの判断がなされて認証する旨の判定をして、被認証側にアクセスを許容する旨の返答を行う（Ｓ６１４）。

五　認証側装置によるオフセット処理（第９図参照）

１　利用者から初めて認証要求があった際、ＡＣＥ／Ｓｅｒｖｅｒは、ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのクロックが計時する時刻をＵＴＣ（協定世界時間）に変換した時刻データを中心とするその前後±７２０期間（１期間は３０秒、６０秒、１２０秒のいずれか）の時刻データに基づき、１４４１個の比較用トークンコード（あるいは比較用パスコード）を生成させ、当該利用者から送られてきた認証用データと比較して、期間のズレを認識し、認証後直ちに、当該被認証側（利用者）の情報として、認証側のＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのデータベースに記憶させる（オフセット処理）。

２　当該利用者が２回目の認証を受けようとする場合、ＡＣＥ／Ｓｅｒｖｅｒは、前記１によってデータベースに記憶されたオフセット値を読み出して（Ｓ９０２）、認証側のクロック（ＡＣＥ／Ｓｅｒｖｅｒが組み込まれたコンピュータのクロック）が計時する現在時刻に前記オフセット値を加え（Ｓ９０３）、そのオフセット加算したものを時刻データとして用いて、比較用トークンコード（あるいは比較用パスコード）を生成する（Ｓ９０４：前記四１(1)②、四２(1)②、四３(1)②参照）。

３　２回目の認証が行われた場合、前回認証時に認証側コンピュータのデータベースに記憶されたオフセット値に、前回認証時から今回認証時までに新たに生じた期間のズレを加算して、これを認証側のコンピュータのデータベースに記憶させる（Ｓ９０７：オフセット更新）。

４　３回目以降の認証後のオフセット更新も同様である。

六　ＳｅｃｕｒＩＤとＡＣＥ／Ｓｅｒｖｅｒとの時間同期処理

１　利用者が保持するＳｅｃｕｒＩＤトークンにはカード内臓時計があり、そのトークンの時刻（Ｓ１０００）をもとに所定のアルゴリズムでパスコードが生成される（Ｓ１００１）。利用者はこのパスコードを利用者名と共にアクセスの許容を求めるべくＡＣＥ／Ｓｅｒｖｅｒに送信する（Ｓ１００２）。

２　ＡＣＥ／Ｓｅｒｖｅｒでは、利用者名とパスコードとを受信し（Ｓ１００３）、受信された利用者名に基づいて利用者毎にそのオフセットが格納されているデータベースから当該利用者のオフセットを取得する（Ｓ１００４）。サーバー内蔵の時計から得た時刻データに対してこのオフセットで加減算して（Ｓ１００５）修正時刻を得る（Ｓ１００６）。次に修正時刻をもとに利用者側と同様のアルゴリ

ズムでパスコードを生成する（Ｓ１００７）。
　３　このサーバーパスコードと送信されてきた利用者のパスコードとを比較して、誤差許容範囲内であればアクセス許可の認証を行う（Ｓ１００８）。次に修正時刻とトークン時刻との間に誤差があるか否かが確認される（Ｓ１００９）。誤差がない場合には同期処理は終了する。一方、誤差がある場合には、オフセットを修正した後（Ｓ１０１０）これをデータベースに上書き保存して（Ｓ１０１１）同期処理は終了する。
　４　なお、実施品では、パスコードの誤差許容時間の範囲内における認証を行うために、修正時刻に対応するパスコードを生成すると共にその前後の時刻に対するパスコードも併せて生成して、これらのパスコード群と利用者のパスコードとを比較するようにしている。そして、その中のいずれかのパスコードが一致すれば、誤差許容範囲内であるとしてアクセス許可の認証を行う。そして、一致したパスコードに対応するオフセットをデータベースに上書き保存して次回のアクセスに備えるものである。

第三　図面の説明
　第１図は、認証システムの全体構成図である。
　第２図は、被認証側装置Ｉのトークンコード方式装置②の処理フロー図である。
　第３図は、パスコード方式装置③の処理フロー図である。
　第４図は、ソフトウェアートークン方式装置④の処理フロー図である。
　第５図は、認証側装置Ⅱの信号の流れの説明図である。
　第６図は、ＡＣＥ／Ｓｅｒｖｅｒの認証の処理フロー図である。
　第７図は、トークンコード比較の説明図である。
　第８図は、ネクストトークンコードモードの処理フロー図である。
　第９図は、ＡＣＥ／Ｓｅｒｖｅｒの時刻データのオフセット更新の処理フロー図である。
　第１０図は、ＳｅｃｕｒＩＤとＡＣＥ／Ｓｅｒｖｅｒとの時間同期処理のフロー図である。

以　上

第１図　第２図　第３図　第４図　第５図　第６図　第７図　第８図　第９図　第１０図

（別紙）　　Ｋｅｏｎ説明書

一　製品名
　　Ｋｅｏｎ

二　製品の説明
　　Ｋｅｏｎは、公開鍵方式暗号を利用した電子証明書に基づく電子署名による認証を必要とする各種利用者アプリケーションに対し、電子証明書の発行管理・暗号鍵の管理機能などを提供する、以下の複数のプログラム及び機器からなる製品系列の総称である。
　　Keon Certificate Server（ＫＣＳ）
　　利用者からの要求に基づき電子証明書の発行、有効期限管理などを行うプログラム。
　　Keon Security Server（ＫＳＳ）
　　電子証明書を持つ利用者の証明書・暗号鍵の保管、利用者のアプリケーション利用権限情報の管理などを行なうプログラム。
　　Keon Desktop（ＫＤＴ）
　　利用者の使用するパーソナルコンピュータ（ＰＣ）上で稼動し、KCSやKSSと通信しながら、利用者の電子証明書や暗号鍵をＰＣ上で利用可能にするためのプログラム。利用者ＰＣ上に保管してあるデータの暗号化にも利用可能。
　　Keon Agent（群）
　　各種利用者アプリケーションの利用権限を利用者に自動的に与えるためKDT及びKSSと通信しながら電子証明書や利用権限情報のやり取りを行なうためのプログラム。

Keon SecurID3100

利用者の電子証明書や暗号鍵を利用者が手元に保存するためのスマートカード。

なお、Ｋｅｏｎにおいては、前述したＫＳＳやＫＤＴ等で管理される各種情報へのアクセスを認証する手段として前述した別紙「ＲＳＡシステム説明書」記載のアクセス制御システムを用いる場合がある。

以　上