平成２９年８月３１日判決言渡　同日原本領収　裁判所書記官

平成２７年（ワ）第３６９８１号　虚偽事実の告知・流布差止等本訴請求事件

平成２８年（ワ）第１７５２７号　特許権侵害差止等反訴請求事件

口頭弁論の終結の日　平成２９年５月２９日

判　　決

本訴原告（反訴被告）　株式会社シー・エス・イー

（以下「原告」という。）

同訴訟代理人弁護士　田　中　伸　一　郎

同　佐　竹　勝　一

同　奥　村　直　樹

同　山　本　飛　翔

同訴訟代理人弁理士　近　藤　直　樹

同補佐人弁理士　山　崎　貴　明

本訴被告（反訴原告）　パスロジ株式会社

（以下「被告」という。）

同訴訟代理人弁護士　笠　原　基　広

同　坂　生　雄　一

同　中　村　京　子

同補佐人弁理士　塩　谷　英　明

主　　文

１　被告は，文書，口頭若しくはインターネットを通じて，別紙原告製品目録記載１の認証用ソフトウェアにおけるパスワード登録シス

テムの使用が，特許第４４５５６６６号に係る特許権を侵害し，又は，侵害するおそれがある旨を，需要者，原告の取引関係者その他の第三者に告知し，流布してはならない。

２　被告は，原告に対し，３００万円及びこれに対する平成２８年１月１３日から支払済みまで年５分の割合による金員を支払え。

３　原告のその余の本訴請求をいずれも棄却する。

４　被告の反訴請求をいずれも棄却する。

５　訴訟費用は，本訴反訴を通じてこれを１０分し，その１を原告の負担とし，その余を被告の負担とする。

６　この判決は，第２項に限り，仮に執行することができる。

事　実　及　び　理　由

第１　請求

１　本訴請求

⑴　主文第１項同旨

⑵　被告は，原告に対し，１０００万円及びこれに対する平成２８年１月１３日（本訴状送達の日の翌日）から支払済みまで年５分の割合による金員を支払え。

⑶　被告は，朝日新聞，読売新聞，毎日新聞，日本経済新聞及び産経新聞の各朝刊全国版の社会面広告欄に，別紙謝罪広告目録記載の広告文を同目録記載の条件で，各１回ずつ掲載せよ。

２　反訴請求

⑴　原告は，別紙原告製品目録記載１のソフトウェア製品（以下「原告ソフトウェア」という。）及び同目録記載２のシステム製品（以下「原告システム」といい，原告ソフトウェアと併せて「原告製品」と総称する。）の生産，譲渡又は譲渡の申出をしてはならない。

⑵　原告は，前項記載のソフトウェア製品及びシステム製品を廃棄せよ。

⑶　原告は，被告に対し，１０００万円及びこれに対する平成２８年６月４日（反訴状送達の日の翌日）から支払済みまで年５分の割合による金員を支払え。

第２　事案の概要

本件本訴事件は，原告が，「原告ソフトウェアにおけるパスワード登録システムの使用が特許第４４５５６６６号に係る被告の特許権を侵害し，又は侵害するおそれがある」旨を告知・流布する被告の行為が不正競争防止法２条１項１５号に該当する旨主張して，被告に対し，①同法３条１項に基づき，上記告知・流布の差止めを，②同法４条に基づき，損害賠償金の一部である１０００万円及びこれに対する不法行為の日の後である平成２８年１月１３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，③不正競争防止法１４条に基づき，謝罪広告の掲載を，それぞれ求める事案である。

本件反訴事件は，発明の名称を「ユーザ認証方法およびユーザ認証システム」とする３つの特許（特許第４４５５６６６号，特許第４２７５０８０号，特許第３８０９４４１号。以下，順に「本件特許１」などといい，併せて「本件各特許」と総称する。）に係る各特許権（以下，順に「本件特許権１」などといい，併せて「本件各特許権」と総称する。）を有する被告が，主位的に，①原告による原告ソフトウェアの生産，販売及び販売の申出（以下，併せて「販売等」ともいう。）が，本件特許権１及び本件特許権２を侵害するものとみなされる行為（特許法１０１条１号，２号，４号）並びに本件特許権３を侵害する行為に当たり，②原告による原告製品の販売等が，本件各特許権を侵害するものとみなされる行為（特許法１０１条１号，２号，４号，５号）に当たると主張し，予備的に，原告製品の購入者が原告製品と端末装置等とを組み合わせてワンタイムパスワード導出パターンの登録方法を構築する行為等が本件各特許権の侵害に当たり，原告はこれを教唆又は幇助していると主張して，原告に対

し，①特許法１００条１項に基づき，原告製品の生産，譲渡又は譲渡の申出の差止めを，②同条２項に基づき，原告製品の廃棄を，③不法行為に基づく損害賠償金（特許法１０２条３項）の一部である１０００万円及びこれに対する不法行為後である平成２８年６月４日（反訴状送達日の翌日）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，それぞれ求める事案である。

１　前提事実（当事者間に争いがない事実及び証拠上明らかな事実）

⑴　当事者

ア　原告は，各種情報処理に関するシステム分析，開発及びプログラミング等を目的とする株式会社である。

イ　被告は，コンピュータに関するハードウェア・ソフトウェアの開発，製造，販売，リースならびに保守サービス等を目的とする株式会社である。

被告の代表取締役は，Ａ（以下「Ａ」という。）である。

なお，被告の変更前の商号は，株式会社セキュアプロバイダである（以下，商号変更前も含めて，単に「被告」という。）。

⑵　被告の特許権

被告は，次の各特許権（本件各特許権）を有している（なお，本件各特許に係る明細書を，順に「本件明細書１」などという。）。

ア　本件特許権１

（ア）　特許番号　第４４５５６６６号

（イ）　発明の名称　ユーザ認証方法およびユーザ認証システム

（ウ）　出 願 日　平成２１年９月２４日

（エ）　登 録 日　平成２２年２月１２日

イ　本件特許権２

（ア）　特許番号　第４２７５０８０号

（イ）　発明の名称　ユーザ認証方法およびユーザ認証システム

（ウ） 出 願 日　平成１７年１月３１日

（エ） 登 録 日　平成２１年３月１３日

ウ　本件特許権３

（ア） 特許番号　第３８０９４４１号

（イ） 発明の名称　ユーザ認証方法およびユーザ認証システム

（ウ） 出 願 日　平成１５年２月１３日

（エ） 登 録 日　平成１８年５月２６日

⑶　特許請求の範囲の記載

本件各特許に係る特許請求の範囲の記載は次のとおりである。

ア　本件特許１に係る請求項８（以下，この発明を「本件発明１」という。）

端末装置と，前記端末装置と通信回線を介して接続されたサーバとを含む，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録システムであって，

前記端末装置は，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを表示し，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すための手段と，

前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返す手段と，を有し，

前記端末装置と通信回線を介して接続されたサーバは，

前記特定されたパスワード導出パターンを登録させるための手段を備える，

パスワード導出パターンの登録システム。

イ　本件特許２に係る請求項１（以下，この発明を「本件発明２」という。）

ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録方法であって，

サーバが，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成ステップと，

サーバが，前記生成した提示用パターンを前記ユーザに提示して，前記提示パターンについての特定の要素に割り当てられたキャラクタの入力を促す入力ステップと，

サーバが，前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，前記生成ステップおよび前記入力ステップを繰り返す特定ステップと，

サーバが，前記特定したパスワード導出パターンを登録する登録ステップと，

を備えることを特徴とするパスワード導出パターンの登録方法。

ウ　本件特許３に係る請求項２６（以下，この発明を「本件発明３」という。）

コンピュータを，

所定のパターンを構成する要素群の中から選択された特定の要素に基づくパスワード導出パターンを，ユーザに対応づけて登録する登録手段，

前記ユーザの情報端末装置から送信された，利用対象システムに割り当てられたシステム識別情報を受け付ける受付手段，

前記情報端末装置から前記システム識別情報を受け付けた場合に，前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成手段，

前記情報端末装置に，前記生成した提示用パターンを送信する送信手段，

前記利用対象システムからキャラクタを受け付け，前記提示用パターンと前記ユーザのパスワード導出パターンとに基づいて，前記受け付けたキャラクタが正当であるか否かを判断する第１の判断手段，

前記情報端末装置から受け付けたシステム識別情報に基づいて，前記キャラクタを受け付けた前記利用対象システムが正当であるか否かを判断する第２の判断手段，

前記第１の判断手段が判断した結果を前記利用対象システムに通知する通知手段，

として機能させるためのプログラム。

エ　本件特許３に係る請求項２５（以下，この発明を「本件発明４」といい，本件発明１ないし４を併せて「本件各発明」という。）

所定のパターンを構成する要素群の中から選択された特定の要素に基づくパスワード導出パターンを，ユーザに対応づけて登録する登録手段と，

前記ユーザの情報端末装置から送信された，利用対象システムに割り当てられたシステム識別情報を受け付ける受付手段と，

前記情報端末装置から前記システム識別情報を受け付けた場合に，前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成手段と，

前記情報端末装置に，前記生成した提示用パターンを送信する送信手段と，

前記利用対象システムからキャラクタを受け付け，前記提示用パターンと前記ユーザのパスワード導出パターンとに基づいて，前記受け付けたキャラクタが正当であるか否かを判断する第１の判断手段と，

前記情報端末装置から受け付けたシステム識別情報に基づいて，前記キャラクタを受け付けた前記利用対象システムが正当であるか否か

を判断する第２の判断手段と，

前記第１の判断手段が判断した結果を前記利用対象システムに通知する通知手段と，

を備えることを特徴とするユーザ認証装置。

⑷　本件各発明の構成要件

本件各発明を構成要件に分説すると，次のとおりである（以下，分説した構成要件をそれぞれの符号に従い「構成要件１Ａ」のようにいう。）。

ア　本件発明１

１Ａ：端末装置と，前記端末装置と通信回線を介して接続されたサーバとを含む，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録システムであって，

１Ｂ：前記端末装置は，

１Ｂ－１：複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを表示し，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すための手段と，

１Ｂ－２：前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し，

１Ｂ－３：これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返す手段と，を有し，

１Ｃ：前記端末装置と通信回線を介して接続されたサーバは，前記特定されたパスワード導出パターンを登録させるための手段を備える，

１Ｄ：パスワード導出パターンの登録システム。

イ　本件発明２

２Ａ：ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録方法であって，

２Ｂ：サーバが，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成ステップと，

２Ｃ：サーバが，前記生成した提示用パターンを前記ユーザに提示して，前記提示パターンについての特定の要素に割り当てられたキャラクタの入力を促す入力ステップと，

２Ｄ：サーバが，前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，前記生成ステップ及び前記入力ステップを繰り返す特定ステップと，

２Ｅ：サーバが，前記特定したパスワード導出パターンを登録する登録ステップと，

２Ｆ：を備えることを特徴とするパスワード導出パターンの登録方法。

ウ　本件発明３

３Ａ：コンピュータを，

３Ｂ：所定のパターンを構成する要素群の中から選択された特定の要素に基づくパスワード導出パターンを，ユーザに対応づけて登録する登録手段，

３Ｃ：前記ユーザの情報端末装置から送信された，利用対象システムに割り当てられたシステム識別情報を受け付ける受付手段，

３Ｄ：前記情報端末装置から前記システム識別情報を受け付けた場合に，前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成手段，

３Ｅ：前記情報端末装置に，前記生成した提示用パターンを送信する

送信手段，

３Ｆ：前記利用対象システムからキャラクタを受け付け，前記提示用パターンと前記ユーザのパスワード導出パターンとに基づいて，前記受け付けたキャラクタが正当であるか否かを判断する第１の判断手段，

３Ｇ：前記情報端末装置から受け付けたシステム識別情報に基づいて，前記キャラクタを受け付けた前記利用対象システムが正当であるか否かを判断する第２の判断手段，

３Ｈ：前記第１の判断手段が判断した結果を前記利用対象システムに通知する通知手段，

３Ｉ：として機能させるためのプログラム。

エ　本件発明４

４Ａ：所定のパターンを構成する要素群の中から選択された特定の要素に基づくパスワード導出パターンを，ユーザに対応づけて登録する登録手段と，

４Ｂ：前記ユーザの情報端末装置から送信された，利用対象システムに割り当てられたシステム識別情報を受け付ける受付手段と，

４Ｃ：前記情報端末装置から前記システム識別情報を受け付けた場合に，前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成手段と，

４Ｄ：前記情報端末装置に，前記生成した提示用パターンを送信する送信手段と，

４Ｅ：前記利用対象システムからキャラクタを受け付け，前記提示用パターンと前記ユーザのパスワード導出パターンとに基づいて，前記受け付けたキャラクタが正当であるか否かを判断する第１の判断手段と，

４Ｆ：前記情報端末装置から受け付けたシステム識別情報に基づいて，前記キャラクタを受け付けた前記利用対象システムが正当であるか否かを判断する第２の判断手段と，

４Ｇ：前記第１の判断手段が判断した結果を前記利用対象システムに通知する通知手段と，

４Ｈ：を備えることを特徴とするユーザ認証装置。

オ　なお，本件発明３と本件発明４は，前者が「プログラム」に関する発明であるのに対し，後者は「ユーザ認証装置」に関する発明である点で相違するが，その余の構成要件は実質的に同一である。

⑸　原告の行為

原告は，業として原告製品の製造，販売及び販売の申出等を行っている。

⑹　原告製品の構成及び構成要件充足性

ア　原告ソフトウェアに用いられているワンタイムパスワード導出パターンの登録システム（以下「本件登録システム」という。）は，構成要件１Ａ，１Ｂ－１及び１Ｄを充足する（なお，被告は，原告システムにも本件登録システムが用いられている旨主張している。）。

イ　本件登録システムの登録方法（以下「本件登録システム方法」という。）は，構成要件２Ａ及び２Ｅを充足する。

ウ　原告ソフトウェアで用いられているユーザ認証システム（以下「本件ユーザ認証システム」といい，その認証方法を「本件ユーザ認証システム方法」という。）に用いられるプログラム（以下「本件ユーザ認証システムプログラム」という。）は，構成要件３Ａ，３Ｂ，３Ｆ及び３Ｈを充足する。

エ　本件ユーザ認証システムに用いる装置（以下「本件ユーザ認証システム装置」という。）は，構成要件４Ａ，４Ｅ及び４Ｇを充足する。

⑺　被告の行為

ア　被告は，平成２６年３月頃，原告ソフトウェアのディストリビュータ及びユーザ等に対し，「ワンタイムパスワード認証技術のご紹介及び特許ライセンスの件」と題する書状（甲６。以下「本件書状１」という。）を送付した。

本件書状１には，「パスロジ社からライセンスを受けずに販売されている同様のワンタイムパスワード認証製品を利用されますと，それが特許侵害品である場合は，ユーザーも特許侵害に問われる可能性がありますので，ご留意ください。」，「３．日本国特許第４２７５０８０号，第４４５５６６６号〈抜き出し位置登録方法〉」，「パスロジック方式では，抜き出し位置を本人確認のための情報とします。そのため，抜き出し位置をユーザが自分で登録することが望ましいのですが，その登録時のユーザビリティを高め，確実性を高め，さらにチュートリアルも含めることができる方式として開発した技術です。」，「※特許発明に係わるサービス・製品を正当な権限なく実施すること（第三者から購入してエンドユーザとして利用する場合や，自社開発により実施する場合も含む）は，特許権侵害となります。」などと記載されている。

イ　被告は，同年７月頃，原告製品のディストリビュータ及びユーザである１１社に対し，「ワンタイムパスワード認証技術のご紹介及び特許ライセンスの件」と題する書状（甲７。以下「本件書状２」という。）を送付した。

本件書状２には，本件書状１とほぼ同旨の内容が記載されている。

ウ　被告は，平成２７年４月８日付けで，原告製品のユーザであるニフティ株式会社（以下「ニフティ」という。）に対し，書状（甲８。以下「本件書状３」という。）を送付した。

本件書状３には，「今回，貴社の『ニフティクラウドサービス』の中で提供されているパターン認証のためのパスワード登録システムを拝見した

ところ，パスロジ社が所有するワンタイムパスワード関連特許（例えば，第４４５５６６６号の請求項８）をご使用されていると認識しております…。」「パスロジ社としましては，貴社が上記特許をお使いになることはワンタイムパスワード技術の普及のためには大変好ましいことと考えております。但し，貴社とは未だ正式なライセンス契約を結んでおりませんので，今回ぜひ正式に契約書を交わしていただきたく存じます。」との内容が記載されているとともに，ニフティが提供するパスワード登録システムが本件発明１の技術的範囲に属する旨記載された事実実験公正証書が添付されていた。

エ　被告は，同年６月２５日付けで，ニフティに対し，「ワンタイムパスワード特許の件」と題する書状（甲９。以下「本件書状４」といい，本件書状１ないし本件書状４を「本件各書状」と総称する。）を送付した。

本件書状４には，「ぜひご検討賜り，ライセンス契約書を交わしていただきたくお願い申し上げます。」との内容が記載されているとともに，ニフティが提供するパスワード登録システムが本件発明１の技術的範囲に属する旨の弁理士の意見が記載された鑑定意見書が添付されていた。

オ　被告は，同年９月１０日，ニフティ担当者に対して電子メール（甲１０。以下「本件メール」という。）を送信した。

本件メールには，「当方は，貴社のご意向に沿うべく，再度ＣＳＥ社と本件について交渉をいたしました。…当方は誠意をもって，なぜ侵害になるのかを再度説明いたしました。」などと記載されている。

⑻　無効審判請求等

ア　原告は，平成２７年１１月２７日，特許庁長官に対し，本件特許１に係る無効審判請求を提起した（無効２０１５－８００２１８）。

イ　特許庁は，平成２９年４月１０日付けで，本件特許１を特許法２９条の２及び１２３条１項２号により無効とする旨の審決の予告をし，同月１３

日，被告に送達された（甲３６。弁論の全趣旨）。

ウ　被告は，訂正請求するための期間として定められた同月１３日から６０日以内に訂正請求をすることを前提に，本件訴訟において，訂正による対抗主張を提出したが，当裁判所は，同年５月１６日の第１０回弁論準備手続において，同主張を時機に後れた攻撃防御方法であると判断して却下した。

２　争点

【反訴について】

(1)　原告製品は本件各発明の技術的範囲に属するか（争点１）

ア　本件登録システムは本件発明１の技術的範囲に属するか（争点１－１）

具体的には，構成要件１Ｂ－２，１Ｂ－３，１Ｃの充足性

イ　本件登録システム方法は本件発明２の技術的範囲に属するか（争点１－２）

具体的には，構成要件２Ｂ，２Ｃ，２Ｄ，２Ｆの充足性

ウ　本件ユーザ認証システムプログラムは本件発明３の技術的範囲に属するか（争点１－３）

具体的には，構成要件３Ｃ，３Ｄ，３Ｅ，３Ｇ，３Ｉの充足性

エ　本件ユーザ認証システム装置は本件発明４の技術的範囲に属するか（争点１－４）

具体的には，構成要件４Ｂ，４Ｃ，４Ｄ，４Ｆ及び４Ｈの充足性

(2)　本件特許１の無効理由の有無（争点２）

ア　特許法２９条の２違反（争点２－１）

イ　公然実施（争点２－２）

(3)　原告による間接侵害の成否（争点３）

(4)　直接侵害の教唆・幇助行為による原告の不法行為の成否（争点４）

(5)　被告の損害額（争点５）

【本訴について】

(6)　本件各書状及び本件メールの送付等は，原告の「営業上の信用を害する」ものか（争点６）

(7)　本件各書状及び本件メールの内容は「虚偽」であるか（争点７）

(8)　被告の行為の違法性・違法性阻却事由の有無（争点８）

(9)　被告の過失の有無（争点９）

(10)　原告の損害額（争点１０）

(11)　信用回復措置の必要性の有無（争点１１）

３　争点に関する当事者の主張（反訴について）

(1)　争点１（原告製品は本件各発明の技術的範囲に属するか）について

ア　争点１－１（本件登録システムは本件発明１の技術的範囲に属するか）について

【被告の主張】

原告製品に用いられている本件登録システムは，次のとおり，本件発明１の技術的範囲に属する。

（ア）　構成要件１Ｂ－２の充足性について

ａ　「入力されたキャラクタに基づいてパスワード導出パターンが特定される」の意義について

「基づく」とは，「①基礎にする。よりどころにする。②基として起こる。起因する。」等を意味する。

また，本件明細書１には，要素の１回の入力によって要素を絞り込み，新たなキャラクタを割り振るとのパスワード導出パターンの特定方法の一実施形態が記載されている（段落【００８９】ないし【００９４】）が，入力されたキャラクタに起因して要素を特定する一方法が記載されているにすぎない。他方で，本件明細書１には，２回入力されたキャラクタの組み合わせで要素を特定するとの一実

施形態が開示されている（段落【００９６】）。

そうすると，「入力されたキャラクタに基づいてパスワード導出パターンが特定される」とは，「提示用パターン」として提示された「要素」に割り当てられた「キャラクタ」が入力されることにより，入力された「キャラクタ」に起因して要素が特定され，ユーザが登録しようとするパスワード導出パターンが特定されることを意味する。

b　「特定されるまで，新たな提示用パターンを表示する処理を繰り返す」の意義について

「提示用パターン」とは，構成要件１Ｂ－１の「提示用パターン」と同様に，「複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた」ものを意味する。２回目以降に提示される「提示用パターン」は，その要素に割り当てられたキャラクタの入力に基づいてパスワード導出パターンを特定するために提示され，所定のパターンを構成する「要素」に割り当てられた「キャラクタ」が，前に提示された「提示用パターン」と異なるものを意味し，構成要件１Ｂ－２には，「要素」に割り当てられた「キャラクタ」が異なるために，構成要件１Ｂ－１の「提示用パターン」とは異なる「新たな提示用パターン」と記載されている。

また，２回目以降に提示される「提示パターン」において，所定のパターンを構成する要素にどのようなキャラクタを割り当てるかについては，特に限定されていない。

そうすると，「特定されるまで，新たな提示用パターンを表示する処理を繰り返す」とは，パスワード導出パターンが特定されるまで，「要素」に割り当てられた「キャラクタ」が異なる「提示用パターン」を表示する処理を繰り返す，という意味であるというべきである。

c　本件登録システムでは，サーバが，１回目と２回目のマトリクス表に対して入力されたキャラクタを確認し，それによってユーザが選択したマス目の位置と順番を特定しており，入力された数字に基づいてパスワードとなる位置と順番を特定するため，新しい数字が割り当てられたマトリクス表が表示される。

本件登録システムにおける「マトリクス表」は，「数字の乱数表」であるから，本件登録システムにおいて提示される新しい数字が割り当てられたマトリクス表は，最初に提示されたマトリクス表とは異なるマトリクス表であり，構成要件１Ｂ－２の「新たな提示用パターン」に該当する。また，本件登録システムが，パスワードとなる位置と順番を特定するために最初に表示したものとは異なる数字が割り当てられたマトリクス表を表示することは，構成要件１Ｂ－２の「パスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返」すことに該当する。

したがって，本件登録システムは，構成要件１Ｂ－２を充足する。

仮に，本件登録システムにおいて，全体マトリクスの「要素」であるすべてのマスに数字が表示された「マトリクス表」がユーザに対して２回提示され，２回の提示の両方に対して，ユーザが選択した「位置」「順番」に従ってマトリクス表中の数字を都度入力し，２回分の入力結果を組み合わせることによってユーザが選択したワンタイムパスワード導出のための位置と順番の特定を行っているとしても，本件登録システムでは，「マトリクス表」に対する入力結果２回分に起因して，ユーザの選択したマス目を特定しているから「入力されたキャラクタに基づいてパスワード導出パターンが特定される」を充足し，２回目の数字の入力で特定するにあたり，マス目に割り当てられる数字が１回目のマトリクス表とは異なるマトリクス表を表示しているから，構成要件１Ｂ－２

の「特定されるまで，新たな提示用パターンを表示する処理を繰り返す」を充足する。

（イ） 構成要件１Ｂ－３の充足性について

構成要件１Ｂ－３の「新たな提示用パターン」は構成要件１Ｂ－２の「新たな提示用パターン」と同義である。

そして，本件登録システムは，ユーザに新たに表示されたマトリクス表から特定のマス目に割り当てられた数字を抜き出させ，その数字を入力する入力フォームを表示する再表示機能部を有し，新たに提示されたマトリクス表及びパスワード入力欄を有する入力フォームを新たに表示するところ，数字を入力する入力フォームを表示することは，構成要件１Ｂ－３の「キャラクタの入力を促す処理」に該当し，新しい入力フォームを表示する再表示機能部は，構成要件１Ｂ－３の「新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返す手段」に該当する。

したがって，本件登録システムは，構成要件１Ｂ－３を充足する。

（ウ） 構成要件１Ｃの充足性について

本件登録システムでは，パソコン，携帯電話，スマートフォン等の端末装置と通信回線を介して接続されたセキュアマトリクス認証サーバが，特定されたパスワードとなる位置と順番を登録するパターン登録機能部を有しており，セキュアマトリクス認証サーバは，ユーザの端末装置と通信回線を通じて接続され，ユーザの２回の数字の入力を受け付けてパスワードとなる位置と順番を特定し，それを登録する。

そして，「パスワードとなる位置と順番」は，構成要件１Ｃの「パスワード導出パターン」に該当し，「特定されたパスワードとなる位置と順番を登録するパターン登録機能部」は，構成要件１Ｃの「特定されたパスワード導出パターンを登録させるための手段」に該当する。

したがって，本件登録システムは，構成要件１Ｃを充足する。

【原告の主張】

本件登録システムは，次のとおり，本件発明１の技術的範囲に属しない。

（ア） 構成要件１Ｂ－２の充足性について

ａ 「入力されたキャラクタに基づいてパスワード導出パターンが特定される」の意義について

特許請求の範囲や本件明細書１の一般的な説明に係る記載部分（段落【００１６】【００１７】）を見ても，構成要件１Ｂ－２の技術的意義は不明である。

しかし，本件明細書１の実施例に関する記載（段落【００８９】ないし【００９４】，【図１８】及び【図１９】）によれば，本件発明１の技術思想は，登録しようとするパスワード導出パターンに対応する要素値の入力を繰り返すことによって提示用パターンの要素を絞り込み，ユーザが意図しているパスワード導出パターンを特定し，当該特定は，提示した提示用パターンのうち，入力された要素値を持つ該当要素数と入力された要素数と等しいかどうかで判断するというものといえる。

そうすると，「入力されたキャラクタに基づいてパスワード導出パターンが特定」とは，入力された最終のＮ回目に表示された「提示用パターン」によりユーザが入力したキャラクタ（数字等。要素値）を持つ該当要素数と入力された要素数と等しいことにより判断されるのであり，当該「提示用パターン」とユーザが入力したキャラクタそのものに基づき，「パスワード導出パターン」が一義的に特定されることを意味する。

ｂ 「特定されるまで，新たな提示用パターンを表示する処理を繰り返す」の意義について

上記ａで述べた本件発明１の技術思想に照らせば，「特定されるまで，新たな提示用パターンを表示する処理を繰り返す」とは，ある特定のパターンに対して入力されたキャラクタにより要素の場所とその順番からなる「パスワード導出パターン」が特定されるまで，キャラクタが割り当てられる要素の異なる新しい提示用パターンを表示することを意味する。そして，「新たな提示用パターン」（Ｎ回目の表示）が，（Ｎ－１）回目に表示された「提示用パターン」と要素自体を同一としつつ，要素に割り当てられたキャラクタだけを異にする「提示用パターン」を表示したのでは，当該パターンに対して入力されたキャラクタにより，要素の場所とその順番からなる「パスワード導出パターン」が特定することはできないから，２回目以降に表示される「新たな提示用パターン」は，提示が重ねられるごとに要素が絞り込まれ，従前の「提示用パターン」とは異なるものである。

ｃ　原告ソフトウェアに用いられている本件登録システムでは，全体マトリックスの「要素」であるすべてのマスに数字が表示された「マトリクス表」がユーザに対して２回提示され，いずれの提示においても，ユーザが選択した「位置」「順番」に従ってマトリクス表中の数字を都度入力し，２回分の入力結果を組み合わせることによってユーザが選択したワンタイムパスワード導出のための位置と順番情報の特定を行っており，本件発明１の「パスワード導出パターン」に対応する「ワンタイムパスワード」の「位置」と「順番」情報の特定は，「マトリクス表」をユーザに二度提示し，二度の提示に対してユーザが選択した「位置」のキャラクタを選択した「順番」を都度入力し，当該２回分の入力結果を組み合わせることによって行っている。そして，この二度提示される「マトリクス表」は，キャラクタは異なるが，それが割り当てられる要素は全く同一であり，１回目の入力結果に基づ

く絞込みによる数字の表示される要素の特定は行われていない。

このように，本件登録システムでは，「ワンタイムパスワード」の「位置」と「順番」の情報は，最終の「マトリクス表」への入力結果でなく，二度提示される「マトリクス表」への２回分の入力結果の組合せによって特定されているから，「前記入力されたキャラクタに基づいてパスワード導出パターンが特定される」ものではない。

また，本件登録システムでは，二度提示される「マトリクス表」への入力により「パスワード導出パターン」が特定されるが，いずれの「マトリクス表」の要素のパターンは全く同一であって「新たな」ものではないから，「パスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返す」ものでもない。

したがって，本件登録システムは，構成要件１Ｂ－２を充足しない。

（イ）　構成要件１Ｂ－３の充足性について

上記(ア)のとおり，本件登録システムには「新たな提示用パターン」は存在しないから，本件登録システムは，構成要件１Ｂ－３を充足しない。

（ウ）　構成要件１Ｃの充足性について

上記(ア)のとおり，本件登録システムには「前記入力されたキャラクタに基づいてパスワード導出パターンが特定」されていないから，本件登録システムは，構成要件１Ｃを充足しない。

イ　争点１－２（本件登録システム方法は本件発明２の技術的範囲に属するか）について

【被告の主張】

本件登録システム方法は，原告製品に用いられており，その構成は別紙「本件登録システム方法の構成（被告主張)」のとおりである。本件登録システム方法は，次のとおり，本件発明２の技術的範囲に属する。

（ア） 構成要件２Ｂの充足性について

ａ 構成要件２Ｂは，提示用パターンの生成主体が「サーバ」である旨規定しているが，「サーバ自身」が単体で上記生成を行わなければならないと解すべきではない。本件明細書２の実施例に関する記載（段落【００８３】ないし【００８５】）によれば，提示用パターンの生成や提示に関してサーバ自身がすべて行わければならないものではなく，クライアント端末において認証サーバの指示に従って処理が実行されることは排除されていないといえる。

本件登録システムでは，セキュアマトリクス認証サーバがマトリクス表を生成するところ，上記「マトリクス表」は，「４×４」×４表（又は３表）の数字の乱数表であるから，構成要件２Ｂの「複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターン」に該当する。そして，上記「要素」はマトリクス表の「マス目」に，マス目に割り当てられた「所定のキャラクタ」は「数字」に該当する。

よって，本件登録システム方法は，構成要件２Ｂを充足する。

ｂ 仮に，本件登録システム方法の構成が原告主張のとおりであるとしても，本件登録システム方法では，ＳＭＸ認証サーバが，ユーザＩＤを受けて「パスワード変更用マトリクス」を生成する基となる情報の「パスワード変更用Ｓｅｅｄ」を生成し，クライアント端末に送信している。そして，「パスワード変更用マトリクス」は，「パスワード変更用Ｓｅｅｄ」以外は，ＳＭＸ認証サーバとクライアント端末とで共有された情報によって生成され，「パスワード変更用Ｓｅｅｄ」が送信されることによって，一意に決定される。

したがって，本件登録システム方法では，ＳＭＸ認証サーバが「パスワード変更用マトリクス」を生成しているといえる。

また，ＳＭＸ認証サーバは，既に保持しているユーザＩＤと組み合せ，自ら「パスワード変更用マトリクス」（クライアントで発生させている１回目と２回目のパスワード変更用マトリクスと同一のもの）を生成する。

そうすると，原告主張の構成によっても，本件登録システム方法は，構成要件２Ｂを充足する。

（イ） 構成要件２Ｃの充足性について

a 構成要件２Ｃは，提示用パターンの生成主体及び提示主体が「サーバ」である旨規定しているが，上記(ア)ａのとおり，本件明細書２の実施例に関する記載（段落【００８３～００８５】）によれば，クライアント端末において認証サーバの指示に従って，提示用パターンの生成又は提示が実行されることは排除されていないから，サーバ自身が単体で上記生成及び提示を行わなければならないと解すべきではない。

本件登録システム方法では，セキュアマトリクス認証サーバが，マトリクス表を生成し，生成したマトリクス表をユーザに提示し，マトリクス表から特定のマス目に割り当てられた数字を抜き出させ，その数字を入力する入力フォームを表示する。

そして，ユーザに，マトリクス表から特定のマス目に割り当てられた数字を抜き出させ，その数字を入力する入力フォームを表示することは，構成要件２Ｃの「提示パターンについての特定の要素に割り当てられたキャラクタの入力を促す入力ステップ」に該当する。

よって，本件登録システム方法は，構成要件２Ｃを充足する。

b 仮に，本件登録システム方法の構成が原告主張のとおりであるとしても，上記(ア)ｂのとおり，本件登録システム方法において，ＳＭＸ認証サーバは，「パスワード変更用マトリクス」の生成を決定付ける

「パスワード変更Ｓｅｅｄ」をクライアント端末に送信し，同端末にユーザＩＤと組み合わせて「パスワード変更用マトリクス」を生成させ，ユーザに対し，それを提示し，ユーザが登録しようとする「ワンタイムパスワード導出ルール」に基づき，マトリクス表のマス目に割り当てられた数字を入力するよう促している。ここで，上記提示に係る「パスワード変更用マトリクス」は，ＳＭＸ認証サーバで生成された「パスワード変更用マトリクス」と同一である。

そうすると，原告主張の構成によっても，本件登録システム方法は，構成要件２Ｃを充足する。

（ウ） 構成要件２Ｄの充足性について

a 構成要件２Ｄは，「サーバが，前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，前記生成ステップ及び前記入力ステップを繰り返す特定ステップ」と規定しているから，「生成ステップ」と「入力ステップ」は，それぞれパスワード導出パターンが特定されるまで繰り返されれば足り，「生成ステップ」とは，提示用パターンを生成するものであればよく，「入力ステップ」とは，上記提示用パターンをユーザに提示し，キャラクタの入力を促すものであればよい。そして，本件明細書２の実施例に係る記載（段落【００９２】）も勘案すると，「入力ステップ」と「生成ステップ」との間において，「パスワード導出パターンが特定され」たか否かの判断を必ず要するものではない。

本件登録システム方法では，セキュアマトリクス認証サーバが，入力された数字に基づいてパスワードとなる位置と順番を特定し，再度，新しい数字が割り当てられたマトリクス表を生成し，生成したマトリクス表から特定のマス目に割り当てられた数字を抜き出させ，その数字を入力する入力フォームを表示するところ，「数字」及び「パスワ

ードとなる位置と順番」は，それぞれ，構成要件２Ｄの「キャラクタ」及び「パスワード導出パターン」に該当する。また，上記(ア)及び(イ)の生成ステップ及び入力ステップの意義に照らせば，最初に提示したものとは異なる数字が割り当てられたマトリクス表を生成してユーザに提示し，同表から抜き出した特定のマス目に割り当てられた数字を入力する入力フォームを再度表示することは，構成要件２Ｄの「パスワード導出パターンが特定されるまで，前記生成ステップ及び前記入力ステップを繰り返す」ことに該当する。

よって，本件登録システム方法は，構成要件２Ｄを充足する。

b　仮に，本件登録システム方法の構成が，原告主張のとおりであるとしても，本件登録システム方法では，ＳＭＸ認証サーバが，「パスワード変更用Ｓｅｅｄ」をクライアント端末に送信し，クライアント端末に，ユーザＩＤと組み合わせ，２回分への入力結果で「ワンタイムパスワード導出ルール」が特定される「パスワード変更用マトリクス」を２回分同時に発生させ，異なる「パスワード変更用マトリクス」を生成させている。また，本件登録システム方法では，上記のとおり，ＳＭＸ認証サーバが，「パスワード変更用Ｓｅｅｄ」をクライアント端末に送信し，同端末に，１回目及び２回目の「パスワード変更用マトリクス」を生成させて順次ユーザに提示し，ユーザに対し，登録しようとする「ワンタイムパスワード導出ルール」に基づいてマトリクス表のマス目に割り当てられた数字を入力するように促し，２回の入力結果によってユーザが登録しようとする「ワンタイムパスワード導出ルール」は特定される。

したがって，本件登録システム方法では，「入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで」，「入力ステップ」を「繰り返」されている。

そうすると，原告主張の構成によっても，本件登録システム方法は，構成要件２Ｄを充足する。

（エ）　構成要件２Ｆの充足性について

上記(ア)ないし(ウ)に加えて，構成要件２Ａ及び２Ｅの充足性は争いがないから，本件登録システムは，構成要件２Ｆを充足する。

【原告の主張】

本件登録システム方法は，原告ソフトウェアに用いられており，その構成は，別紙「本件登録システム方法の構成（原告主張)」のとおりであるところ，次のとおり，本件発明２の技術的範囲に属しない。

（ア）　構成要件２Ｂの充足性について

構成要件２Ｂは，「サーバが，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する」と規定し，「サーバ」が「提示用パターン」を生成してユーザに提示するものとしている。

本件登録システム方法では，「パスワード変更用マトリクス」はクライアント端末で生成され，クライアント端末にインストールされたソフトウェアによってユーザに提示されており，「サーバ」は「提示用パターン」の「生成」及び「提示」を行っていない。

したがって，本件登録システム方法は，構成要件２Ｂを充足しない。

（イ）　構成要件２Ｃの充足性について

構成要件２Ｃは，「サーバが，前記生成した提示用パターンを前記ユーザに提示して，前記提示パターンについての特定の要素に割り当てられたキャラクタの入力を促す」と規定し，認証サーバ自身が「提示用パターン」を生成し，かつユーザに提示することを要件としている。

本件登録システム方法では，「パスワード変更用マトリクス」はクライアント端末で生成され，クライアント端末にインストールされたソフ

トウェアによってユーザに提示されており，「サーバ」は「提示用パターン」の「生成」及び「提示」を行っていない。

したがって，本件登録システム方法は，構成要件２Ｃを充足しない。

（ウ） 構成要件２Ｄの充足性について

構成要件２Ｄは，「サーバ」が，「入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで」「前記生成ステップ及び前記入力ステップを繰り返す」ことを規定している。また，本件発明２の特許請求の範囲には，「生成ステップ」（構成要件２Ｂ）の後に「入力ステップ」（構成要件２Ｃ）に関する記載があり，その前後関係を明らかにした上で，前の入力ステップで「入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで」，「前記生成ステップおよび前記入力ステップを繰り返す特定ステップ」をサーバが行う（構成要件２Ｄ）と記載されているから，構成要件２Ｄは，特許請求の範囲の文言上，認証サーバが，「『生成ステップ』→『入力ステップ』→『入力されたキャラクタに基づいてパスワード導出パターンが特定され』たかの判断→（特定されなかった場合に）『生成ステップ』→『入力ステップ』→『入力されたキャラクタに基づいてパスワード導出パターンが特定され』たかの判断…」という過程で，「パスワード導出パターンが特定」されるまで「生成ステップ」と「入力ステップ」が交互に繰り返されることを規定している。

本件登録システム方法では，クライアント端末が，「ＳＭＸ認証サーバ」から送信された１つの「パスワード変更用ｓｅｅｄ」をユーザＩＤと組み合わせ，「パスワード変更用マトリクス」を一度に２回分生成し，生成された２回分の「パスワード変更用マトリクス」をユーザに順次提示して入力を促す入力ステップを行っている。すなわち，本件登録システム方法では，サーバではなくクライアント端末で「パスワード変更用

マトリクス」の生成又は提示が行われており，また，１回目に提示された「パスワード変更用マトリクス」に「入力されたキャラクタに基づいてパスワード導出パターンが特定」されるか否かに関係なく２回目の「パスワード変更用マトリクス」の生成は１回目の提示前に生成されており，さらに，「（１回目の提示用パターンに対して）入力されたキャラクタ」をサーバに送付せず，その入力結果「に基づいてパスワード導出パターンが特定され」たか否かに関係なく，２回目の「パスワード変更用マトリクス」の提示が行われている。加えて，本件登録システム方法では，１回目も２回目も提示される「パスワード変更用マトリクス」は，それに対して「入力されたキャラクタに基づいてパスワード導入パターンが特定される」ものではない上，２回の入力結果を組み合わせてユーザが意図したパスワード導出パターンを特定できない場合は存在せず，当該パターンを特定できない場合が存在することを前提とした本件発明２の「特定ステップ」が存在するとはいえない。

以上によれば，本件登録システム方法は，「サーバが，前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，前記生成ステップおよび前記入力ステップを繰り返す特定ステップ」の構成を有しないから，構成要件２Ｄを充足しない。

（エ）　構成要件２Ｆの充足性について

上記(ア)ないし(ウ)によれば，本件登録システム方法は，構成要件２Ｆを充足しない。

ウ　争点１－３（本件ユーザ認証システムプログラムは本件発明３の技術的範囲に属するか）について

【被告の主張】

本件ユーザ認証システムは，①原告ソフトウェアが「ＶＭＷａｒｅ」と組み合わせて使用される場合のユーザ認証システム（クライアントコンピ

ュータから仮想デスクトップにアクセスする際のユーザ認証に用いられるシステム），及び，②ＲＡＤＩＵＳプロトコル（ネットワーク上の利用者の認証や権限の付与，利用状況の記録などを行うための通信プロトコルの一つ）が利用可能な機器及びシステム（以下「ＲＡＤＩＵＳ対応機器」という。）と組み合わせ使用される場合のユーザ認証システム（ＳＭＸ認証サーバをＲＡＤＩＵＳによって連携してユーザ認証に用いられるシステム）である。本件ユーザ認証システムプログラムの構成の概要は，別紙「本件ユーザ認証システムプログラムの構成（被告主張）」の第１記載のとおりであり，上記①のシステムのプログラム構成は，同第２記載のとおりであり，上記②のシステムのプログラム構成は，別紙「本件ユーザ認証システムプログラム構成（原告主張）」のとおり（ただし，「ログインＩＤは，ＳＭＸ認証サーバにおいて，各利用システム毎に付されるものではなく，ユーザ固有の番号である。」点を除く。）である。

本件ユーザ認証システムプログラムは，次のとおり，本件発明３の技術的範囲に属する。

（ア）　構成要件３Ｃの充足性について

ａ　本件ユーザ認証システムプログラムにおいて，セキュアマトリクスの認証サーバは，ユーザのマトリクス表取得クライアントから送信された，ログインＩＤを受け付けるログインＩＤ情報受付部を有するところ，マトリクス表取得クライアントは，構成要件３Ｃの「情報端末装置」に該当する。

また，構成要件３Ｃの「システム識別情報」とは，システム固有の情報である必要はなく，「利用対象システムに割り当てられたシステム識別情報」であれば足りるところ，例えば，本件明細書３（段落【００５８】）には，本件ユーザ認証システムのログインＩＤはシステム識別情報として利用対象システムに紐付けて事前に告知されたも

のとして利用し得ることが記載されている。そして，原告ソフトウェアの運用ガイド（乙３５，３６）によれば，ユーザを識別する「ＵｓｅｒＩＤ」とは別個に認証時に使用される「ＬｏｇｉｎＩＤ」を設定することとされ，１つのＵｓｅｒＩＤに対して最大１０個のＬｏｇｉｎＩＤを設定することができ，ＳＭＸ認証サーバに登録されていないＬｏｇｉｎＩＤを入力すると「ログインＩＤが登録されていません。」又はダミーマトリクス表が表示されるとされており，ＳＭＸ認証サーバが，ログインＩＤを受け付けることでユーザ認証を要求している利用対象システムの有無を識別しているといえる。また，上記運用ガイド（乙３５）によれば，「ＬｏｇｉｎＩＤ（エイリアス）」を複数登録することによって場所や用途に応じて「ＬｏｇｉｎＩＤ」を使い分けることができるとされており，ユーザは，利用対象システムごとにログインＩＤを付与し，当該ログインＩＤを使い分けることで，複数の利用対象システムに対して異なるパスワードポリシーのマトリクス認証システムを用いることが可能となる。加えて，上記運用ガイド（乙３５）によれば，本件ユーザ認証システムでは，ログインＩＤにレルム（特定のグループを意味する識別子）を付与することができるとされており，ログインＩＤに利用対象システムを意味するレルムを付与すればログインＩＤのレルムによって利用対象システムを識別することができる。

以上によれば，本件ユーザ認証システムプログラムにおけるログインＩＤは，構成要件３Ｃの「システム識別情報」に該当する。

したがって，本件ユーザ認証システムプログラムは，構成要件３Ｃを充足する。

ｂ　なお，本件発明３の特許請求の範囲には，「情報端末装置」と「利用対象システム」は物理的に別個の端末であることは記載されていな

い。また，「情報端末装置」と「利用対象システム」が論理的に別個のシステムであって，ユーザからの認証要求の経路が「情報端末装置」経由のものと「利用対象システム」経由のものの２つ以上から構成されていれば，ワンタイムパスワードを生成する提示用パターンの送信先である「情報端末装置」からの認証手続開始メッセージを受け付け，提示用パターンから得られるキャラクタを受け付ける「利用対象システム」からの認証要求を受けることによって「利用対象システム」単体の不正アクセスを排除するという作用効果（本件明細書３・段落【００６７】）を奏することができるから，使用端末装置が物理的に同一であるか否かは問題とはならない。したがって，本件発明３は，「情報端末装置」と「利用対象システム」とが物理的に別個のものであることを前提としていない。この点を措くとしても，本件ユーザ認証システムの上記①の構成の場合（ＶＭＷａｒｅを用いてサーバの仮想化を行い，仮想デスクトップを利用する場合），「情報端末装置」と「利用対象システム」は物理的に別個である。

（イ）　構成要件３Ｄの充足性について

本件ユーザ認証システムプログラムでは，マトリクス表取得クライアントからログインＩＤを受け付けた場合に，セキュアマトリクス認証サーバがマトリクス表を生成する基となるｓｅｅｄを生成するマトリクス表生成ｓｅｅｄ生成部を有する。

上記(ア)によれば，上記「マトリクス表取得クライアント」，「ログインＩＤ」及び「マトリクス表を生成する基となるｓｅｅｄ」は，それぞれ，構成要件３Ｄの「情報端末装置」，「システム識別情報」及び「前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パターン」に該当する。また，上記(ア)のとおり，本件ユーザ認証システムにおいて，ＳＭＸ認証サーバが，ログインＩＤを受け

てマトリクス表を生成する基となるｓｅｅｄを生成するところ，マトリクス表生成ｓｅｅｄの生成とマトリクス表の生成は技術的に同義である。

以上によれば，本件ユーザ認証システムプログラムは，構成要件３Ｄを充足する。

（ウ） 構成要件３Ｅの充足性について

本件ユーザ認証システムプログラムは，セキュアマトリクス認証サーバが，マトリクス表取得クライアントに対し，生成したマトリクス表生成ｓｅｅｄを送信するマトリクス表送信部を有する。

そして，上記(イ)のとおり，「マトリクス表取得クライアント」及び「マトリクス表生成ｓｅｅｄ」は，それぞれ，構成要件３Ｅの「情報端末装置」及び「提示用パターン」に該当する。

したがって，本件ユーザ認証システムプログラムは，構成要件３Ｅを充足する。

（エ） 構成要件３Ｇの充足性について

本件ユーザ認証システムプログラムは，マトリクス表取得クライアントから受け付けたログインＩＤに基づいて，数字が入力されたユーザのＲＡＤＩＵＳ対応機器が正当であるか否かを判断する対象ＲＡＤＩＵＳ対応機器判断部を有する。

上記(ア)のとおり，「マトリクス表取得クライアント」及び「ログインＩＤ」は，それぞれ，構成要件３Ｇの「情報端末装置」及び「システム識別情報」に該当し，「数字」及び「ＲＡＤＩＵＳ対応機器」は，それぞれ，構成要件３Ｇの「キャラクタ」及び「利用対象システム」に該当する。

また，本件ユーザ認証システムプログラムでは，ＳＭＸ認証サーバが，マトリクス表に基づくパスワードの他に，ＲＡＤＩＵＳ対応機器から送信を受けたログインＩＤとマトリクス表取得クライアントから受けたロ

グインＩＤを照合してユーザ認証を行っており，ユーザがログインＩＤを利用対象システムに紐付けて用いる場合には，ログインＩＤは利用対象システムの識別情報として機能しているから，ＳＭＸ認証サーバは，ログインＩＤを識別することにより，ログインＩＤに基づいて，パスワードが入力されたＲＡＤＩＵＳ対応機器の正当性を判断している。さらに，ＳＭＸ認証サーバは，ＲＡＤＩＵＳ対応機器と通信する際，ＲＡＤＩＵＳ対応機器のＩＰアドレス及びＲＡＤＩＵＳ対応機器に対応して事前に設定されたシークレットキーをＲＡＤＩＵＳ対応機器から受け取り，それらがＳＭＸ認証サーバに事前に登録されたものであるか否かを判断する機能を備えており，ユーザ認証の際，これらの情報をログインＩＤ及びパスワードと共に受け取ることで，パスワードが入力されたＲＡＤＩＵＳ対応機器の正当性の判断をより個別的に行うことができる。

以上によれば，本件ユーザ認証システムプログラムは，構成要件３Ｇを充足する。

（オ）　構成要件３Ｉの充足性について

上記(ア)ないし(エ)に加えて，構成要件３Ａ，３Ｂ，３Ｆ及び３Ｈの充足性に争いがないことによれば，本件ユーザ認証システムプログラムは，構成要件３Ｉを充足する。

【原告の主張】

本件ユーザ認証システムプログラムの構成は，別紙「本件ユーザ認証システムプログラム（原告主張)」のとおりであるところ，本件ユーザ認証システムプログラムは，次のとおり，本件発明３の技術的範囲に属しない。

（ア）　構成要件３Ｃの充足性について

ａ　本件明細書３の記載（段落【００２４】，【００４５】，【００６７】，【図１】）や拒絶理由通知書に対する意見書の内容に照らせば，本件発明３は，「情報端末装置」と「利用対象システム」が物理的に別の

端末であることを前提としているといえるが，本件ユーザ認証システムにおける情報端末装置と利用対象システムは，物理的に別の端末ではない。

したがって，本件ユーザ認証システムプログラムが本件発明３の技術的範囲に属するとの被告の主張は理由がない。

ｂ　この点を措くとしても，構成要件３Ｃの「システム識別情報」とは，「利用対象システム１１は，固有のシステムＩＤ（システム識別情報）を内部のＲＯＭに記憶して」（本件明細書３・段落【００２４】）おり，利用対象となるシステムを識別するためのシステム固有の情報と解すべきである。

本件ユーザ認証システムプログラムにおけるログインＩＤは，利用システムごとに異なるものではなく，利用対象システムを識別するものでもなく，ＳＭＸ認証サーバにおけるユーザ固有の番号であるから，本件発明３の「利用対象システムに割り当てられたシステム識別情報」に該当しない。そもそも，本件ユーザ認証システムプログラムにおけるＳＭＸ認証サーバは，対象の利用システムを特定することなく，１組のログインＩＤ及びパスワードのみによって複数の利用システムに関するユーザ認証を行い，「システム識別情報」を受け付けていない。

したがって，本件ユーザ認証システムプログラムは，構成要件３Ｃを充足しない。

ｃ　なお，被告は，ＬｏｇｉｎＩＤ（エイリアス）やレルム付きＵｓｅｒＩＤ又はレルム自体が「利用対象システムに割り当てられたシステム識別情報」に該当する旨主張するが，ＬｏｇｉｎＩＤ（エイリアス）は利用システムを識別するものではない。また，複数のレルム付きＵｓｅｒＩＤは，ＳＭＸ認証サーバにおいて，全く別個のＵｓｅｒＩＤとして扱われ，利用対象システムを識別するものではない。

（イ）　構成要件３Ｄの充足性について

上記(ア)のとおり，本件発明３における「システム識別情報」とは，利用対象となるシステムを識別するためのシステム固有の情報である。また，構成要件３Ｄの「前記情報端末装置から前記システム識別情報を受け付けた場合に，前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する」とは，その文言及び本件明細書３の記載（段落【００３７】等）によれば，コンピュータが，利用対象システムのシステム識別情報を受け付けることを条件として，提示用パターンを生成することを意味している。また，構成要件３Ｄは，コンピュータを「…所定のキャラクタを割り当てた提示用パターンを生成する生成手段」として機能させるプログラムを規定しているから，「提示用パターン」は，コンピュータで生成されるものである。

この点，上記(ア)のとおり，本件ユーザ認証システムにおけるログインＩＤ（ＬｏｇｉｎＩＤ（エイリアス），レルム付きＵｓｅｒＩＤ又はレルム自体を含む。）は，いずれも利用対象システムを識別するものではなく「利用対象システムに割り当てられたシステム識別情報」に該当しない。また，本件ユーザ認証システムプログラムは，ＶＭＷａｒｅを識別する固有の情報を受領することなく，ユーザ固有の情報であるログインＩＤの入力を受けてＳＭＸ認証サーバがマトリクス表の基となるｓｅｅｄを生成している。

よって，本件ユーザ認証システムプログラムは，「前記情報端末装置から前記システム識別情報を受け付けた場合に，前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成手段」を充足せず，構成要件３Ｄを充足しない。

（ウ）　構成要件３Ｅの充足性について

上記(イ)によれば，構成要件３Ｅの「前記生成した提示用パターン」とは，コンピュータが生成した提示用パターンであるところ，本件ユーザ認証システムプログラムでは，「提示用パターン」に相当するマトリクス表を生成するのはセキュアマトリクス認証サーバではなくクライアント端末である。

よって，本件認証システムプログラムは，構成要件３Ｅを充足しない。

(エ)　構成要件３Ｇの充足性について

構成要件３Ｇのユーザが情報端末装置から入力したシステム識別情報に基づき「前記キャラクタを受け付けた前記利用対象システムが正当であるか否か」の判断を行うとは，「前記利用対象システム」が当該システム識別情報で特定されたものかどうかを確認することを意味している。また，構成要件３Ｇは，利用対象システムと物理的に別個の端末である情報端末装置において，利用対象システムの利用に係る認証を受けるために，提示用パターンを受けるために対象システムに割り当てられたシステム識別情報を送信する構成を前提としている。

この点，本件ユーザ認証システムプログラムでは，ＶＭＷａｒｅの対象システムは，事前に特定されることによってＶＭＷａｒｅ　Ｖｉｅｗが呼び出され，当該ＶＭＷａｒｅ　Ｖｉｅｗでユーザ名とパスワードが入力されるから，システム認証の必要性はない。

よって，本件ユーザ認証システムプログラムは，「(コンピュータが)前記情報端末装置から受け付けたシステム識別情報に基づいて，前記キャラクタを受け付けた前記利用対象システムが正当であるか否かを判断する第２の判断手段」を充足しないから，構成要件３Ｇを充足しない。

(オ)　構成要件３Ｉの充足性について

上記(ア)ないし(エ)によれば，本件ユーザ認証システムプログラムは，構成要件３Ｉを充足しない。

エ　争点１－４（本件ユーザ認証システム装置は本件発明４の技術的範囲に属するか）について

【被告の主張】

本件発明４は，本件発明３が「プログラム」に関する発明であるのに対し，「ユーザ認証装置」に関する発明であり，この点において本件発明３と相違するが，その他の構成要件は実質的に同一である。

よって，上記ウ【被告の主張】と同様の理由により，本件ユーザ認証システムに用いられる装置である本件ユーザ認証システム装置は，本件発明４の技術的範囲に属する。

【原告の主張】

上記ウ【原告の主張】と同様の理由により，本件ユーザ認証システム装置は，構成要件４Ｂないし４Ｄ，４Ｆ及び４Ｈを充足しない。

(2)　争点２（本件特許１の無効理由の有無）について

ア　争点２－１（特許法２９条の２違反）について

【原告の主張】

（ア）　本件発明１と特開２００２－３６６５１７公報（以下「甲１１公報」という。）に開示された発明（以下「甲１１発明」という。）の同一性について

本件特許１の出願日前に出願され，本件特許１の出願後に出願公開された甲１１公報には，次の発明（甲１１発明）が開示されている。

①　携帯電話機等の端末装置１と，前記端末装置と移動体通信網２を介して接続された処理センタ装置４（データベース，認証サーバ，ウエブサーバを含む）とを含む，ユーザ認証に用いるワンタイムパスワードを導出するためのワンタイムパスワード情報の登録システム。

②　前記端末装置１は，認証サーバ４２から送られた，ランダムパスワード表を表示する。ユーザは，送られたランダムパスワード表の中か

ら，例えば４つの位置を選択し，選択した４つの位置に記載された数値について，図３中の「パスワード」と表示された箇所に，「６」「３」「４」「１」として順次入力する（一度目のパスワード入力)。

認証サーバ４２から再度送られる，表示された数字のみが異なる２回目のランダムパスワード表を表示し，ユーザは，表示されたパスワード表から，上記と同じ４つの位置に記載された数値「３」「２」「０」「２」を，再度，順次入力する（二度目のパスワード入力)。

③　認証サーバは，ユーザによる二度の入力に基づき，ユーザによって選択されたランダムパスワードの位置を確定し，確定した位置情報をユーザ情報としてデータベースに登録する。

そして，本件発明１の「端末装置」は甲１１発明の「携帯電話機等の端末装置」に，「端末装置と通信回線を介して接続されたサーバ」は「前記端末装置と移動体通信網を介して接続された処理センタ装置」に，「ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録システム」は「ユーザ認証に用いられるワンタイムパスワードを導出するためのワンタイムパスワード情報の登録システム」に，「複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターン」は，１回目に表示されるランダムパスワード表に，それぞれ相当する。仮に，甲１１発明のユーザによる２度の入力に基づき，ユーザにより選択されたランダムパスワードの位置を確定することが，本件発明１の「前記入力されたキャラクタに基づいてパスワード導出パターンが特定される」ことに該当し，かつ，数字のみが異なる甲１１発明の２回目に表示されるランダムパスワード表が，前者の「新たな提示用パターン」に該当するのであれば，本件発明と甲１１発明の構成要件はすべて一致する。

よって，本件発明１は甲１１発明と同一であり，特許法２９条の２本

文により特許を受けることができないから，本件特許１は，同法１２３条１項２号により無効とされるべきものである。

（イ） 本件発明１と甲１１発明の発明者の同一性について

甲１１発明の発明者はＡのみではないから，本件発明１と甲１１発明の発明者は完全に同一ではない。

すなわち，甲１１発明は，エヌ・ティ・ティ・コミュニケーションズ株式会社（以下「ＮＴＴコム」という。）が，Ｂ（以下「Ｂ」という。）を中心とする同社スタッフの下，同社からより高度な認証システムの設計開発の依頼を受けたＣ（以下「Ｃ」という。）が代表取締役を務めるベーステクノロジー株式会社（以下「ベース社」という。）や被告が加わって進めたモバイルコネクトサービスの開発（以下，同開発に係るプロジェクトを「本件プロジェクト」という。）において考案された発明である。本件プロジェクトでは，Ｂが携帯電話端末だけで，パスワードの登録と認証を済ませるとの設計思想を着想して同思想に沿って要件定義をし，ベース社及び被告が具体的設計と開発を分担しており，被告における具体的な開発担当者はＡではなくＤ（以下「Ｄ」という。）であった。このように，甲１１発明に係る開発には，多数の人物が関与している。

また，Ａが，ＯＦＦＩＣベース・ワンタイムパスワードの登録方法として平成１２年１２月２２日付け資料（乙７）を作成してＮＴＴコムに提供したことはない。そもそも，上記資料に記載された方式（以下，単に「方式Ｃ」という。）のうち，甲１１発明の構成に関する部分は，同年１１月２２日付けのＣ作成の資料（乙５）に記載されており，Ａが初めて着想したものではない。

したがって，Ａのみが甲１１発明の発明者であるとはいえない。

【被告の主張】

（ア） 本件発明１と甲１１発明の同一性について

本件発明１は「パスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し」との構成を有するが，甲１１発明に係る明細書の【図４】によれば，段落【００１８】ないし【００２１】に記載された２回の入力によってランダムパスワードの位置は一意に確定しないとされているから，甲１１発明は，少なくとも上記構成を有していない。

したがって，本件発明１と甲１１発明は同一ではないから，本件発明１は，特許法２９条の２により特許を受けることができないものではない（なお，被告は，当初，本件発明１と甲１１発明が同一であると主張していたが，被告第４準備書面において同主張を撤回した。）。

（イ） 本件発明１と甲１１発明の発明者の同一性について

仮に，本件発明１が甲１１発明と同一であるとしても，その発明者はいずれもＡであるから，本件発明１は，特許法２９条の２括弧書きにより，特許を受けることができないものに該当しない。

すなわち，Ａは，平成９年頃，ブラウザ画面上に表示されたマトリクス状の文字や数字からあらかじめ登録した位置と順番で文字や数字を抜き出し，それをワンタイムパスワードとして入力するシステム（以下「パスロジック方式」という。）を開発した。Ａが代表取締役を務めていた有限会社メディアコネクト（以下「メディア社」という。）は，平成９年７月２８日，パスロジック方式を採用したパスワード認証システム「ＯＦＦＩＣ」の販売を開始し，その関連事業を被告に承継させた。被告は，平成１２年１０ないし１１月頃，ＮＴＴコムから，携帯電話サービス「ｉモード」のユーザ認証システムに「ＯＦＦＩＣ」を採用したいと依頼され，同月から，ベース社と共同してシステム開発を進めた（本件プロジェクト）。同プロジェクトでは，被告がＯＦＦＩＣを用い

たユーザのパスワード認証技術を，ベース社がｉモードとＯＦＦＩＣとの連携技術を担当した。

Ａは，ＮＴＴコムから，ワンタイムパスワード登録方法の提案を依頼され，入力位置がユーザの意図するものに推察されるまで，ＯＦＦＩＣ画面を携帯電話が表示する処理を繰り返し行い，これにより，ＯＦＦＩＣ画面についての抜き出し位置の数字の入力を促す処理を繰り返すことを特徴的部分とする方式Ｃを着想し，同年１２月２２日付けで，方式Ｃを記載した「ｉモードでのＯＦＦＩＣ利用開始手順案」（乙７。以下「本件手順案」という。）を作成し，ＮＴＴコムに提供した。

この点，方式Ｃの上記特徴的部分と甲１１発明の特徴的部分（位置情報が確定されるまで，縦４個×横１２個の新たなランダムパスワードを端末装置が表示する処理を繰り返し行い，これにより，縦４個×横１２個の新たなランダムパスワードについての特定の座標位置に配置されているパスワードの入力を促す処理を繰り返すこと）は同一である。

このように，甲１１発明の発明者はＡであって本件発明１の発明者と同一であるから，本件発明１は，特許法２９条の２に該当しない。

なお，ＢやＣ，Ｄらは甲１１発明の発明者ではない。すなわち，ＮＴＴコムの従業員であったＢについては，本件プロジェクトの実務責任者として，甲１１発明に係る特許出願前に，被告から同発明の内容を知得する機会があったにすぎない。また，Ｃについては，ベース社と被告の上記役割分担に照らせば，Ｃらベース社の担当者は，ＯＦＦＩＣに関するパスワード認証技術の設計には直接関与していない。被告と業務委託契約を締結していた株式会社アクロネット（以下「アクロネット社」という。）の社員のＤについては，Ａの指示を受けてＮＴＴコムとの窓口を担当していたにすぎない。

イ　争点２－２（公然実施）について

【原告の主張】

本件発明１は，本件特許１の優先日（平成１４年２月１３日）以前からＮＴＴコムが提供していたモバイルコネクトサービス（以下「本件サービス」という。）において公然と実施されていた。

すなわち，ＮＴＴコムは，平成１３年６月５日には本件サービスをリリースしていたところ，本件サービスで用いられているパスワード登録方法は，数字が表記されるマトリクス表に対して，ユーザが登録を希望するイメージパスワードに基づき，携帯電話等で数字を入力する操作を２回繰り返し，２回の入力結果に基づき，認証サーバ側でパスワードを特定して登録するという方法であって，甲１１公報に開示されたパスワード登録方法と同一方式である。

よって，本件発明１は，特許法２９条１項２号により，特許を受けることができないから，本件特許１は無効である。

【被告の主張】

携帯端末だけでパスワードの登録から認証まで完結する仕組み，特に，方式Ｃが本件サービスに実装され，一般利用者に提供されるようになったのは，平成１４年３月ないし５月頃である。

なお，原告が，本件特許１の優先日前に本件発明１が公然と実施されていたとして提出する証拠（甲１９ないし２１）は，信用性がない，又は，パスワード登録方法の実施に関する記載が含まれないから，いずれも原告の主張を裏付けるものではない。

(3)　争点３（原告による間接侵害の成否）について

【被告の主張】

原告製品は，本件発明１のシステムの「生産にのみ用いられる物」（特許法１０１条１号），本件発明２の方法の「使用にのみ用いる物」（同条４号）及び本件発明４のユーザ認証装置の「生産に用いる物…であつてその発明に

よる課題の解決に不可欠なもの」（同条２号）に該当する。

また，原告システムは，本件発明１の「生産に用いる物…であつてその発明による課題の解決に不可欠なもの」（同条２号）及び本件発明２の方法の「使用に用いる物…であつてその発明による課題の解決に不可欠なもの」（同条５号）にも該当する。

そして，上記(1)【被告の主張】のとおり，本件登録システムは本件発明１の技術的範囲に属し，本件登録システム方法は本件発明２の技術的範囲に属し，本件ユーザ認証システム装置は本件発明４の技術的範囲に属する。

したがって，原告による原告製品の販売等は，本件各特許権を侵害するものとみなされる。

【原告の主張】

上記(1)【原告の主張】のとおり，本件登録システム，本件登録システム方法及び本件ユーザ認証システム装置は，それぞれ本件発明１，本件発明２，本件発明４の技術的範囲に属しないから，間接侵害は成立しない。

(4)　争点４（直接侵害の教唆・幇助行為による原告の不法行為の成否）について

【被告の主張】

仮に，上記(3)の間接侵害の成立が認められないとしても，原告製品の購入者は，業として保有するシステムのユーザ認証システムに利用する目的を有する事業者であると解され，業として，原告ソフトウェアをサーバ等にインストールし，又は，原告システムを用いて本件登録システムを構築し，本件登録システム方法を使用し，本件ユーザ認証システム装置を生産し，本件ユーザ認証システム方法を使用し，本件各特許権を侵害している。

そして，原告は，上記業者に対し，上記各行為をさせることを目的として原告製品の販売等を行い，上記各行為を容易ならしめている。

したがって，原告は，原告製品の販売等により，上記業者による本件各特

許権の侵害行為を教唆又は幇助しており，当該行為は，間接侵害行為と同等の違法性を有する不法行為に該当するというべきである。

【原告の主張】

争う。

(5)　争点５（被告の損害額）について

【被告の主張】

原告製品の平成２４年度における売上高は，１１億円を下らないところ，本件各特許権の実施料率は６．３％を下らないから，原告製品の販売等に係る本件各特許権の年間実施料相当額の合計額は，少なくとも，年間６９００万円を下らない（１１億円×６．３％＝６９３０万円)。そして，上記実施料相当額における各特許権の割合は，「本件特許権１：本件特許権２：本件特許権３＝１：１：２」であると解されるから，本件各特許権の年間実施料相当額は，少なくとも，以下の金額を下回らない。

①　本件特許権１：６９００万円×１／４＝１７２５万円

②　本件特許権２：６９００万円×１／４＝１７２５万円

③　本件特許権３：６９００万円×１／２＝３４５０万円

原告は，遅くとも平成２５年５月３０日から原告製品の販売等を行い，現在も継続していることからすれば，被告が，特許法１０２条３項に基づき「受けるべき金額に相当する額」は，次のとおり，合計２億０７００万円を下らない。

①　本件特許権１：１７２５万円×３年間＝　　５１７５万円

②　本件特許権２：１７２５万円×３年間＝　　５１７５万円

③　本件特許権３：３４５０万円×３年間＝１億０３５０万円

よって，被告は，原告に対し，上記損害金の一部として１０００万円及びこれに対する遅延損害金の支払を求める。

【原告の主張】

争う。

4　争点に関する当事者の主張（本訴について）

⑴　争点６（本件各書状及び本件メールの送付等は，原告の「営業上の信用を害する」ものか）

【原告の主張】

ア　本件書状１及び本件書状２について

上記各書状には，原告ソフトウェアにおける本件登録システムの使用が本件特許権１を含む被告の特許権を侵害する行為に該当する旨が記載されており，特許権侵害に基づく差止請求や損害賠償請求を行うことを示唆する内容である。実際，原告ソフトウェアを利用する原告の顧客らは，上記各書状の受領後，直ちに原告ソフトウェアの使用等が被告の特許権を侵害している旨指摘されていると理解し，原告に説明を求めている。また，被告は，送付先に原告の顧客が含まれることを認識した上で上記各書状を送付している。

このような上記各書状の内容及び送付の態様に照らせば，単に被告製品の導入及びライセンス契約締結の検討を促すための販促文書であるとはいえず，上記各書状の送付は，原告の営業上の信用を害するものである。

イ　本件書状３，本件書状４及び本件メールについて

本件書状３は，被告が，原告より優位な競争上の地位に立つために，原告ソフトウェアのユーザであるニフティに対し，同社の「ニフティクラウドサービス」で提供されているパスワード登録システム（以下「ニフティシステム」という。）の使用が被告の特許権を侵害する行為であるとして，同社にライセンス契約の締結を求める内容である。また，被告は，ニフティが原告ソフトウェアのユーザであることを確定的に認識した後，ニフティシステムが本件発明１の技術的範囲に属する旨記載された鑑定意見書を添付するなどし，本件書状３と同旨の内容の本件書状４及び本件メールを

送付している。

したがって，本件書状３，本件書状４及び本件メールの送付は，原告の営業上の信用を害するものである。

【被告の主張】

ア　本件書状１及び本件書状２について

上記各書状は，被告製品の普及及び上記ライセンス契約締結の営業活動の一環として作成した販促文書であり，特許権侵害に係る記載は，特許権侵害に関する一般的な説明にすぎない。また，上記各書状には，一切，原告及び原告製品に関する記載はなく，その送付先は，知的財産権に関心を有する大企業である。

このような，上記各書状の内容や送付態様に照らせば，上記各書状は，直ちに原告製品が本件特許権１を侵害するものと認識されるものとはいえないから，これらの送付は，原告の営業上の信用を害するものではない。

イ　本件書状３，本件書状４及び本件メールについて

本件書状３は，被告が，ニフティシステムを同社が独自に開発したとの考えに基づき，同社に対し，同システムが本件発明１の技術的範囲に属するとして，正当な権利行使の一環としてライセンス契約の締結を申し入れた文書であり，原告の営業上の信用を害するような内容は一切記載されておらず，本件書状４及び本件メールも同様である。

したがって，本件書状３，本件書状４及び本件メールの送付は，原告の営業上の信用を害するものではない。

⑵　争点７（本件各書状及び本件メールの内容は「虚偽」であるか）について

【原告の主張】

前記争点１－１のとおり，本件登録システムは，本件発明１の技術的範囲に属しない。また，前記争点２のとおり，本件特許１には無効理由がある。したがって，本件各書状及び本件メールの内容は「虚偽」である。

【被告の主張】

仮に，本件各書状及び本件メールが原告ソフトウェアに言及したものと解されるとしても，前記争点１－１のとおり，本件登録システムは，本件発明１の技術的範囲に属する。また，前記争点２のとおり，本件特許１には無効理由はない。したがって，本件各書状及び本件メールの内容は「虚偽」ではない。

(3)　争点８（被告の行為の違法性・違法性阻却事由の有無）について

【被告の主張】

ア　本件書状１及び本件書状２の送付について

被告は，上記各書状の送付にあたって，複数の弁理士に依頼して，原告ソフトウェアの運用ガイドと本件発明１の各要素を逐一対比する鑑定書を作成するなどしていた。また，本件特許１には明らかな無効理由が存在していたといえない。

このように，被告は，上記各書状の送付にあたり，特許権侵害訴訟を提起するために通常必要とされる事実調査及び法律的検討を尽くしているから，上記送付について，違法性は認められない。

イ　本件書状３，本件書状４及び本件メールの送付について

被告は，複数の弁理士に侵害鑑定を依頼した上で，ニフティシステムが本件特許権１の侵害品であるとの確信に至り，ライセンス契約交渉を開始するために，本件書状３をニフティに送付し，ニフティシステムが原告ソフトウェアを利用したものであることを認識した後，原告と交渉しても進展しないと考え，ニフティに対し，本件書状３と同旨の内容の本件書状４及び本件メールを送付した。

また，被告は，上記各書状及びメールの送付に当たって，甲１１公報の存在を認識していなかった。

そうすると，仮に，原告ソフトウェアが本件発明１の技術的範囲に属さ

ない，又は，本件特許１に無効理由があるとしても，本件書状３，本件書状４及び本件メールの送付は，ニフティに対して，本件特許権の行使を前提として，社会通念上必要と認められる範囲の内容及び態様で，訴訟提起に先立って直接の交渉を行うための行為であるから，本件特許権１の正当な権利行使の一環としてされた正当行為であり，違法性が阻却される。

【原告の主張】

争う。

(4)　争点９（被告の過失の有無）について

【原告の主張】

被告は，根拠もなく，原告ソフトウェアが本件特許権１を侵害すると誤信して，本件各書状及び本件メールの送付を行ったものであるから，過失が認められる。

【被告の主張】

被告は，本件各書状及び本件メールの送付につき，特許権侵害訴訟を提起するために通常必要とされる事実調査及び法律的検討を尽くしているから，当該送付について，被告に過失はない。

(5)　争点１０（原告の損害額）について

【原告の主張】

本件書状３，本件書状４及び本件メールの送付という被告の行為により，原告は，次のとおり，１８８５万８８９８円を下らない損害を被ったので，その一部である１０００万円及びこれに対する訴状送達の日の翌日からの遅延損害金の支払を求める。

ア　原告ソフトウェアの使用が本件特許権１等を侵害するものではない旨をニフティらに対して説明するために要した費用は，１１４万円を下らない。

（ア）　原告の社員の人件費　　６４万円

（イ）　弁護士費用　　５０万円以上

イ　無効審判請求事件及び本件訴訟のために支出した弁護士費用・弁理士費用等は，１６７１万８８９８円である。

ウ　経済的信用棄損により生じた無形損害は，１００万円を下らない。

【被告の主張】

否認ないし争う。

原告の主張する上記ア及びイの損害は，本件書状３，本件書状４及び本件メールの送付との間に相当因果関係がない。また，原告の主張する上記ウの損害については，上記送付により原告の経済的信用が棄損された事実はない。

(6)　争点１１（信用回復措置の必要性の有無）について

【原告の主張】

原告は，被告の不正競争行為によって，金銭賠償では填補されない程度にその営業上の信用を著しく害されており，原告の信用を回復するためには，謝罪広告の掲載を命じる必要性がある。

【被告の主張】

争う。

第３　当裁判所の判断

【反訴について】

１　争点２（本件特許１の無効理由の有無）について

事案に鑑み，争点２から判断する。

⑴　争点２－１（特許法２９条の２違反）について

ア　本件発明１と甲１１発明の同一性について

（ア）　被告は，当初，本件発明１と甲１１発明が同一であることを認めていたが，後に，自白を撤回し，甲１１発明に係る明細書の記載（【図４】）によれば，明細書記載の２回の入力（段落【００１８】ないし【００２１】）によってランダムパスワードの位置は確定されないから，甲１１発明は，本件発明１の有する「パスワード導出パターンが特定されるま

で，新たな提示用パターンを表示する処理を繰り返し」との構成を少なくとも有しない旨主張するに至った。

そこで，以下，甲１１発明が「パスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し」との構成を有するか否かについて検討する。

（イ） 甲１１発明に係る明細書には，以下の記載がある。

「以下，ワンタイムパスワード発行の手順について説明する。最初に，端末装置１から前記ユーザ情報をデータベース４５に登録する初期登録時点において，認証サーバ４２は，ウエブサーバ４３を介してアクセス元の端末装置１に初期ワンタイムパスワード情報登録ＵＲＬを通知する電子メールを送信する。」（段落【００１８】）

「端末装置１のユーザは，初期ワンタイムパスワード情報登録ＵＲＬにおいて，認証サーバ４２からウエブサーバ４３を介して送られた図３のようなウエブページを見て，縦４個×横１２個のランダムパスワードの中から例えば４つを選択し，選択したパスワードを図３の「パスワード」と表示された箇所に入力する。縦４個×横１２個の各ランダムパスワードには，図４（ａ）に示すように，（Ａ，１）から（Ｄ，１２）までの座標が付与されている。」（段落【００１９】）

「端末装置１のユーザは，例えば座標（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を位置登録したい場合，これらの各座標位置に配置されているランダムパスワード，すなわち「６」，「３」，「４」，「１」を入力する。次に，認証サーバ４２からは図４（ｂ）に示すような２回目のランダムパスワードが送られる。端末装置１のユーザは，図４（ｂ）のランダムパスワードの配置を見て，前述の座標位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）に配置されているランダムパスワード，すなわち「３」，「２」，「０」，「２」を入力する。認証サーバ４２

は，２回の入力により，ユーザによって選択されたランダムパスワードの位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を確定し，確定した位置情報を前記ユーザ情報としてデータベース４５に登録する。」（段落【００２０】）

「最後に，認証サーバ４２は，アクセス元の端末装置１のユーザ毎及びアクセス先のサービス提供者装置３－１～３－３毎に異なる前記第１のＵＲＬを通知する電子メールを，ウエブサーバ４３を介してアクセス元の端末装置１に送信する。以上で，初期登録が終了する。」（段落【００２１】）

（ウ） 上記(イ)の明細書の記載によれば，甲１１発明においては，認証サーバから２回のランダムパスワードが送られ，端末装置のユーザによる２回の入力によってユーザにより選択されたランダムパスワードの位置が確定し，確定した位置情報の登録を経てワンタイムパスワードの発行に係る初期登録が行われるものと解される。そして，上記明細書の記載において引用された【図４】は，認証サーバから送られるランダムパスワードについて，各座標位置に数字がランダム配置されていることを示す一例にすぎないというべきであるから，仮に，【図４】を前提に，２回の入力によって特定される座標が複数存在し得る結果になるとしても，直ちに上記初期登録の手順が否定されることにならないと解すべきである。

そうすると，甲１１発明は，ワンタイムパスワードの導出パターンの座標が特定されるために，２回にわたりパターン（ランダムパスワード）を表示する処理が行われているといえるから，甲１発明の有する「パスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し」との構成を有すると認められる。

そして，他の構成においても，甲１発明と甲１１発明に異なる点はな

いから，両発明は同一であると認められる。

イ　本件発明１と甲１１発明の発明者の同一性について

（ア）　後掲各証拠及び弁論の全趣旨によれば，以下の事実が認められる。

ａ　Ａは，平成９年頃，ブラウザ画面上に表示されたマトリクス状の文字や数字から，あらかじめ登録した位置と順番で文字や数字を抜き出し，ワンタイムパスワードとして入力するシステム（パスロジック方式）を開発した。（乙１３，３７）

ｂ　Ａが代表取締役を務めていたメディア社は，同年７月２８日，パスロジック方式を採用したパスワード認証システム「ＯＦＦＩＣ」の販売を開始し，その後，ＯＦＦＩＣ関連の事業はメディア社から被告に承継された。（乙１３，３７）

ｃ　ＮＴＴコムによるモバイルコネクトサービスの開発に係るプロジェクト（本件プロジェクト）は，平成１１年頃に立ち上がり，同社従業員のＢが同プロジェクトチーム約２０名のトップの立場を務めた。（乙２７，２８）

ｄ　ＮＴＴコムは，モバイルコネクトサービスのユーザ認証システムにＯＦＦＩＣを利用することを考え，同サービスの開発を分担していたベース社に開発を委託し，ベース社が被告に再委託し，開発が進められた。（乙２７，２８，３８）

本件プロジェクトの開発会議には，ＮＴＴ社のプロジェクトチームメンバーのほか，Ｃ（ベース社の代表取締役）やＡ（被告の代表取締役）も参加しており，Ｃが開発会議において，モバイルコネクトサービスに関するアイデアを提示することもあった。なお，ＮＴＴコムとベース社との契約により，モバイルコネクトサービスの開発に関するベース社のアイデアは，すべてＮＴＴコムに帰属することとなっていた。（乙２７，２８）

ｅ　Ｃは，被告からＯＦＦＩＣのＰｅｒｌ言語のロジックの開示を受け，平成１２年１１月２２日付けで「モバイルプラットフォームプロジェクト　ワンタイムパスワード：ＯＦＦＩＣ連携について」と題する文書（以下「本件Ｃ文書」という。）を作成した。同文書には，「２．初回の登録方式」として，以下の内容が記載されている。（乙５）

「方式（手順）

①　ワンタイムパスワードを登録する為の，固定パスワードをユーザ数ランダムに発生させ，ＵＲＬと共にｅ－ｍａｉｌで利用者の携帯電話端末へ通知する。

②　各利用者は，ＵＲＬをアクセスし，固定パスワードを使って認証を通過する。

③　認証後，ＯＦＦＩＣのワンタイムパスワードを登録する画面において，自分のパスワード位置と順序を指定し，確認後，登録する。

④　ワンタイムパスワード登録完了したことを，ＵＲＬと共にｅ－ｍａｉｌで利用者の携帯端末へ通知する。（このＵＲＬは本番用）

⑤　本番ＵＲＬへアクセスすると，ＯＦＦＩＣの乱数列が表示され，ワンタイムパスワードを入力して，本番アプリケーションに入る。

分担

ＳＰ（引用者注：被告）殿：②～④

ＢＴＩ（引用者注：ベース社）：①，⑤，ユーザＤＢ設計」

ｆ　被告の担当者であったＤは，同年１２月２６日頃，ＮＴＴコムに対し，被告作成名義の同月２２日付けの「ｉモードでのＯＦＦＩＣ利用開始手順案」（本件手順案）をメールで送信し，同手順案はＮＴＴコム内で回覧された。（乙７，８）

本件手順案には，「方式Ａ」から「方式Ｄ」までの４つの方式が記

載されており，「方式Ｃ」の内容は，次のとおりである。（乙７）

「１．　利用者の携帯電話にメールを送付し，パスワード設定をするためのＵＲＬ（ＩＤ付き）を連絡する。

２．　利用者は，ＵＲＬにアクセスし，表示されたＯＦＦＩＣ画面（特定のパターンで数字が並んでいるもの）から，抜き出したい位置の数字を入力する。これを２回くりかえす。

３．　サーバー側では，数字の変化から，入力位置を推察し，画面に抜き出しパターンを表示する。意図するものであれば，本登録をする。」

ｇ　Ａは，平成１３年１月２２日，Ｃに対し，本件手順案をメールで送信した（乙３１の１及び２）。

ｈ　その後，本件プロジェクトにおいて，本件手順案等の検討が進められ，ＮＴＴコムは，ビジネスモデル特許として，発明者をＢとし，甲１１発明について特許出願をした（甲１１，乙２７，３８）。

(イ)　上記(ア)の認定事実によれば，本件プロジェクトには，ＮＴＴコムのプロジェクトチームメンバーの他，Ｃをはじめとするベース社のメンバーやＡをはじめとする被告のメンバーが関与し，Ａ以外の者（例えば，Ｃ）からも新たなパスワード登録方法に関するアイデアが出される中で，同プロジェクトの成果物として甲１１発明が完成し，発明者をＢとする特許出願がされたことが認められる。

そして，甲１１発明のパスワードの初期登録に係る部分は，①認証サーバがウェブサーバを介してアクセス元の端末装置に初期ワンタイムパスワード情報登録ＵＲＬを通知する電子メールを送信し，②端末装置のユーザは，上記ＵＲＬにおいて，認証サーバからウェブサーバを介して送られたウェブページを見て，縦４個×横１２個のランダムパスワードの中から選択し，選択したパスワードを入力し，③認証サーバから送ら

れた２回目のランダムパスワードに対し，端末装置のユーザがランダムパスワードを入力し，④認証サーバが，２回の入力によりユーザにより選択されて確定されたランダムパスワードの位置情報をユーザ情報としてデータベースに登録し，⑤認証サーバが，ＵＲＬを通知する電子メールをウェブサーバを介してアクセス元の端末装置に送信する，というものであると認められる（甲１１発明に係る明細書の段落【００１８】ないし【００２１】参照）ところ，上記部分を具体的に着想，提示した主体（甲１１発明のパスワードの発明者）がＡのみであると認めるに足りる証拠はないから，本件発明１と甲１１発明の発明者が同一であるとは認められない。

（ウ）　これに対し，被告は，甲１１発明の特徴的部分は「位置情報が確定されるまで，縦４個×横１２個の新たなランダムパスワードを端末装置１が表示する処理を繰り返し行い，これにより，縦４個×横１２個の新たなランダムパスワードについての特定の座標位置に配置されているパスワード（すなわち数字）の入力を促す処理を繰り返すこと」にあるところ，これと同一の特徴的部分を有する方式Ｃの記載された本件手順案をＡが作成し，ＮＴＴコムに送付したことに照らせば，甲１１発明の発明者はＡである旨主張する。

この点，本件手順案のデータに係るプロパティには作成者として「(省略)」と記載されている（乙３１の３）が，これをもって直ちにＡのみが本件手順案の内容を着想したと推認することはできず，かえって，本件手順案より前にＣにより作成された本件Ｃ文書にも，「③認証後，ＯＦＦＩＣのワンタイムパスワードを登録する画面において，自分のパスワード位置と順序を指定し，確認後，登録する。④ワンタイムパスワード登録完了したことを，ＵＲＬと共にｅ－ｍａｉｌで利用者の携帯端末へ通知する。(このＵＲＬは本番用)」といった記載があることによれ

ば，本件手順案の内容の一部は，Ａが本件手順案を作成するよりも前に既に本件プロジェクト内において着想されていたものと認められる。したがって，被告の上記主張を採用することはできない。

ウ　小括

以上によれば，本件発明１は特許法２９条の２によって特許を受けられないから，本件特許１には無効理由が認められる。

⑵　したがって，争点２－２（公然実施）について判断するまでもなく，本件特許１は無効とされるべきものである。

２　争点１（原告製品は本件各発明の技術的範囲に属するか）について

⑴　争点１－１（本件登録システムは本件発明１の技術的範囲に属するか）について

上記１のとおり，本件特許１には無効理由が認められるから，争点１－１（本件登録システムは本件発明１の技術的範囲に属するか）については判断を要しない。

⑵　争点１－２（本件登録システム方法は本件発明２の技術的範囲に属するか）について

ア　構成要件２Ｃの充足性について

（ア）　本件明細書２の記載

ａ　【課題を解決するための手段】

本発明は，ユーザごとのパスワード導出パターンを認証サーバに予め登録しておき，ユーザによる利用対象システムの利用の際に，認証サーバが提示用パターンを生成してユーザに提示して，この提示用パターンについてユーザ自身のパスワード導出パターンに対応するキャラクタ列を入力させ，認証サーバは，提示した提示用パターンとユーザ自身のパスワード導出パターンとに基づいて，入力されたキャラクタ列に対して認証を行い，その認証結果を利用対象システムに通知す

るユーザ認証方法およびユーザ認証システムである。（段落【００１６】）

b　【発明を実施するための最良の形態】

(a) 次に，ユーザは，そのシステムＩＤを携帯電話機１３に入力し，認証サーバ１２に送信する（図中(3)）。認証サーバ１２は，これを受けて，乱数表を生成し，これを提示用パターンとしてユーザの携帯電話機１３に送信する（図中(4)）。ユーザは，携帯電話機１３上に表示される提示用パターンを参照して，利用対象システム１１に対して，自身のパスワード導出パターンに割り当てられた要素値のシーケンス（数字列）をパスワードとして入力する。これにより，利用対象システム１１は認証サーバ１２にパスワードを送信する（図中(5)）。(段落【００３７】)

(b) 図１８は，本実施形態に係るパスワード導出パターンの登録方法の処理の流れを説明するためのフローチャートである。このような処理は，携帯電話機１３と認証サーバ１２とによるクライアント／サーバモデルにおけるそれぞれのプログラムによって実現することができるが，本実施形態では，このような処理を実現するための所定のプログラムを含むページデータを認証サーバ１２から携帯電話機１３に送信し，携帯電話機１３においてこれを実行することにより実現している。（段落【００８３】）

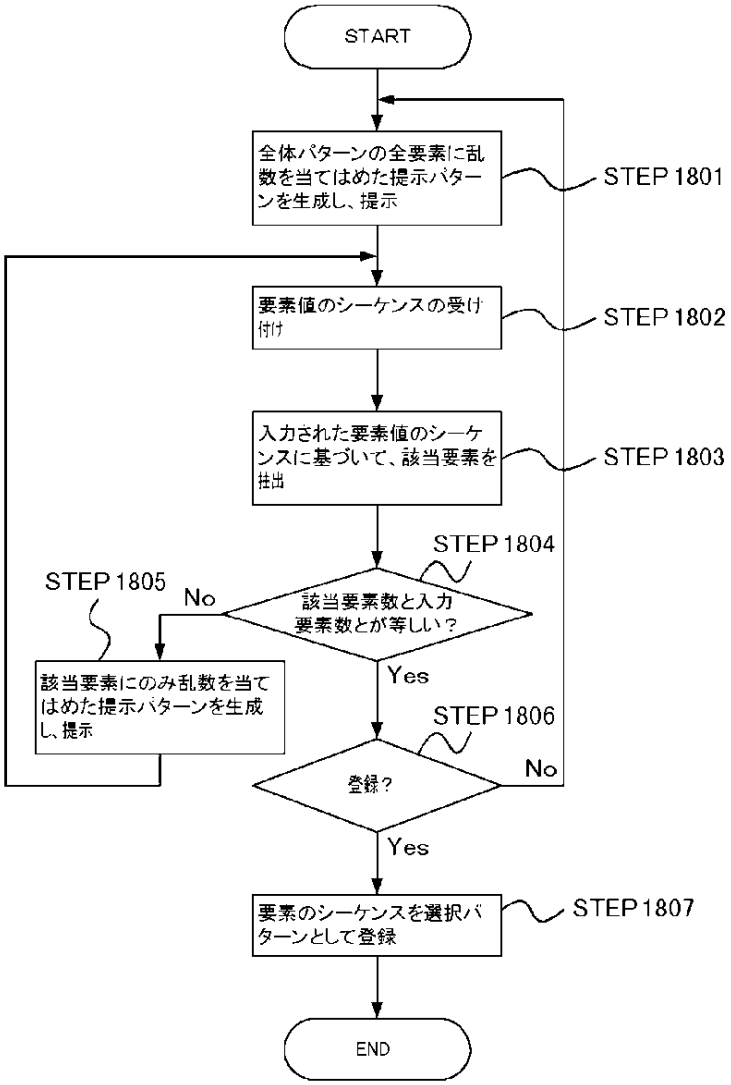
(c) 上記実施形態と同様に，例えば，利用対象システム１１に対するユーザアカウントが登録された時点で，認証サーバ１２は，この登録画面を構成するページデータのＵＲＬを含むメールコンテンツをユーザの携帯電話機１３に対してメールで送信し，これを受信したユーザが携帯電話機１３上に表示されたメールコンテンツ中のＵＲＬを選択する。これにより，認証サーバ１２は，所定のプログラム

を含むページデータを携帯電話機１３に送信する。（段落【００８４】）

(d) ページデータを受信した携帯電話機１３は，そのページデータを解釈して，そこに含まれる所定のプログラムに従って図１８に示す処理を実行し，登録画面を表示する。すなわち，携帯電話機１３は，まず，全体パターン３４の要素群のすべてに対して，乱数発生関数により発生させた乱数をそれぞれ割り当てて提示用パターンを生成し，他の画面要素と相まってパスワード導出パターン登録画面として表示して，ユーザに入力を促す（ＳＴＥＰ１８０１）。ユーザは，この登録画面に対して，登録しようとするパスワード導出パターンの要素に割り当てられた数字を入力する。携帯電話機１３は，ユーザから要素のシーケンスを受け付けると（ＳＴＥＰ１８０２），提示した提示用パターンのうち，入力された要素値を持つ要素を該当要素として抽出し，その数を保持しておく（ＳＴＥＰ１８０３）。次に，携帯電話機１３，抽出した該当要素の数が入力された要素数と等しいか否かを判断し（ＳＴＥＰ１８０４），等しくないと判断する場合には，要素の絞り込みを行うため，全体パターン３４中の該当要素のみに乱数を割り当てて提示用パターンを生成し，同様に，登録画面として表示して，ユーザに入力を促す（ＳＴＥＰ１８０５）。一方，抽出した該当要素の数が入力された要素数と等しいと判断する場合，携帯電話機は，要素の絞り込みができたものとして，登録確認画面を提示して，ユーザに確認を促す（ＳＴＥＰ１８０６）。そして，ユーザによって例えば「ＯＫ」ボタンが選択された場合には（ＳＴＥＰ１８０７のＹｅｓ），携帯電話機１３は，要素のシーケンスをパスワード導出パターンとして登録するため，登録要求を認証サーバ１２に送信し（ＳＴＥＰ１８０６），処理を終了

する。（段落【００８５】）

c　本発明の一実施形態に係るパスワード導出パターンの登録方法の処理の流れを説明するためのフローチャート（【図１８】）は，次のとおりである。



（イ）　構成要件２Ｃの充足性について

本件発明２の構成要件２Ｂは，「サーバが，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成ステップと，」というものであり，構成要件２Ｃは，「サーバが，前記生成した提示用パターンを前記ユ

ーザに提示して，前記提示パターンについての特定の要素に割り当てられたキャラクタの入力を促す入力ステップと，」というものである。

これらの構成要件の文言を踏まえれば，上記構成要件２Ｃは，提示用パターンの生成主体がサーバであることを規定すると共に，サーバが自ら生成した提示用パターンをユーザに提示することを規定していると解するのが相当である。上記ア(ア)の本件明細書２の記載も上記解釈を裏付けるものである。

一方，原告による特許出願の内容（甲２５）及び弁論の全趣旨によれば，本件登録システム方法の構成は，別紙「本件登録システム方法の構成（原告主張)」のとおりであると認められる（この点，被告は，上記構成が別紙「本件登録システム方法の構成（被告主張)」のとおりであると主張するが，その内容は抽象的であるし，これを認めるに足りる証拠もない。)。

そして，別紙「本件登録システム方法の構成（原告主張)」の②ないし④記載のとおり，本件登録システム方法においては，次のとおりの構成が採られている。

「②クライアント端末は,「パスワード変更用ｓｅｅｄ」を受信すると同端末にインストールされたプログラムにより，ユーザが入力するユーザＩＤを同「パスワード変更用ｓｅｅｄ」と組み合わせ，ユニークで，且つ当該２回分への入力結果で「ワンタイムパスワード導出ルール」が特定される「パスワード変更用マトリクス」をクライアントにおいて発生規則に従って２回分同時に（「パスワード変更用マトリクス」１回目及び２回目）発生させる。　③クライアント端末は，ユーザに「パスワード変更用マトリクス」（１回目）を提示し，ユーザが登録しようとする「ワンタイムパスワード導出ルール」に基づきマトリクス表のマス目に割り当てられた数字を入力するようにユーザに促す（１回目の提示。

ユーザによる１回目の入力)。　④ユーザによる１回目の数字入力終了後，クライアント端末は既に発生させている「パスワード変更用マトリクス」（２回目）をユーザに提示し，「ワンタイムパスワード導出ルール」に基づきマトリクス表のマス目に割り当てられた数字の入力を促す（２回目の提示。ユーザによる２回目の入力　→　これにより「ワンタイムパスワード導出ルール」が特定される。)。」

そうすると，本件登録システム方法においては，クライアント端末は，ユーザが入力するユーザＩＤを，受信した「パスワード変更用ｓｅｅｄ」と組み合わせて，「パスワード変更用マトリクス」（１回目及び２回目）を発生させ，これをユーザに対して提示するものである。つまり，ユーザに対して提示用パターンに相当する「パスワード変更用マトリクス」（１回目及び２回目）を提示するのは，「ＳＭＸ認証サーバ」ではなく「クライアント端末」であるから，本件登録システム方法は，構成要件２Ｃを充足しないというべきである。

なお，被告は，サーバ自身が単体でユーザに対する提示用パターンの提示を行われければならないと解すべきではない旨主張するが，特許請求の範囲の記載や本件明細書２の記載（段落【００８３】ないし【００８５】）を見ても，そのような解釈を導くことはできず，他に上記主張を裏付ける根拠は見当たらないから，上記主張を採用することはできない。

イ　小括

以上によれば，その余の点について検討するまでもなく，本件登録システム方法は，本件発明２の技術的範囲に属すると認めることはできない。

⑶　争点１－３（本件ユーザ認証システムプログラムは本件発明３の技術的範囲に属するか）について

ア　構成要件３Ｃの充足性について

（ア） 構成要件３Ｃは，「前記ユーザの情報端末装置から送信された，利用対象システムに割り当てられたシステム識別情報を受け付ける受付手段，」というものであるところ，同構成要件の充足性については，①同構成要件における「情報端末装置」と「利用対象システム」が物理的に別個の端末であることが必要であるかという点，②本件ユーザ認証システムにおける「情報端末装置」と「利用対象システム」が物理的に別個であるかという点，③構成要件３Ｃの「システム識別情報」がシステム固有の情報である必要があると解すべきであるかという点において，当事者間に争いがある。

一方，構成要件３Ｃの「システム識別情報」が利用対象となるシステムを識別するための情報であると解されること，及び，原告ソフトウェアの本件ユーザ認証システムにおける認証サーバが，ユーザのマトリクス表取得クライアントから送信されたログインＩＤを受け付けるログインＩＤ情報受付部を有することについては，当事者間に争いがない。

（イ） そこで，まず，上記の当事者間に争いがない事実を前提に，本件ユーザ認証システムプログラムにおけるログインＩＤが，利用対象となるシステムを識別する「システム識別情報」に該当するか否かについて検討すると，本件全証拠を検討しても，本件ユーザ認証システムプログラムにおけるログインＩＤが利用対象システムを識別する機能を有していることを認めるに足りる証拠はないから，上記ログインＩＤは，構成要件３Ｃの「システム識別情報」に該当するとはいえない。

（ウ） この点，被告は，原告ソフトウェアの運用ガイド（乙３５，３６）には，①ユーザを識別するＵｓｅｒＩＤに対して，認証時に使用される最大１０個のＬｏｇｉｎＩＤを設定することができ，ＳＭＸ認証サーバに登録されていないＬｏｇｉｎＩＤを入力すると「ログインＩＤが登録されていません。」又はダミーマトリクス表が表示されること，②Ｌｏ

ｇｉｎＩＤ（エイリアス）を複数登録することによって「ＬｏｇｉｎＩＤ」を使い分けられ，ユーザは，利用対象システムごとにログインＩＤを付与することにより，複数の利用対象システムに対して異なるパスワードポリシーのマトリクス認証システムを用いられること，③ログインＩＤに利用対象システムを意味するレルムを付与すればログインＩＤのレルムによって利用対象システムを識別することができること，以上の点が記載されているから，ログインＩＤは利用対象システムを識別している旨主張する。

しかしながら，上記①については，上記運用ガイド（乙３６）には，「ダミーマトリクス機能は，攻撃者に対し，ＳＭＸのＬｏｇｉｎＩＤの登録有無を分からないようにするための機能となります。ダミーマトリクス機能を使用していない場合には，ＳＭＸに登録されていないＬｏｇｉｎＩＤを入力した際,「ログインＩＤが登録されていません。」と表示されますが，ダミーマトリクス機能を使用することにより，ＳＭＸに登録されていないＬｏｇｉｎＩＤが入力された場合でも，ダミーのマトリクス表が表示される動作となります。」との記載があり，ＳＭＸ認証サーバがログインＩＤの登録の有無を判断した上で「ログインＩＤが登録されていません。」との文言又はダミーマトリクス表を表示することは記載されているが，ログインＩＤにより利用対象システムの有無を識別することを裏付ける記載は見当たらない。上記②については，運用ガイド（乙３５）には,「ＬｏｇｉｎＩＤ（エイリアス）を複数登録することにより，場所や用途に応じてログインＩＤを使い分けることができます。ＬｏｇｉｎＩＤ（エイリアス）は，ＵｓｅｒＩＤ毎に最大１０個まで作成することが可能です。」との記載があるが，複数の利用対象システムに対して異なるログインＩＤを設定することができることを裏付ける記載は見当たらない。上記③については，運用ガイド（乙３５）には,

ユーザ新規登録の「設定項目一覧」の「ＵｓｅｒＩＤ」欄に「ユーザのＩＤを入力します。レルム付きＵｓｅｒＩＤはシステムで一意の値である必要があります。レルム付きＵｓｅｒＩＤは『〔ＵｓｅｒＩＤ〕〔レルムセパレータ〕〔レルム〕』で構成されます。」との記載があり，また，「ＬｏｇｉｎＩＤ」欄に「ユーザのＬｏｇｉｎＩＤを入力します。ＬｏｇｉｎＩＤは認証時に使用されるＩＤです。レルム付きＬｏｇｉｎＩＤはシステムで一意の値である必要があります。レルム付きＬｏｇｉｎＩＤは『〔ＬｏｇｉｎＩＤ〕〔レルムセパレータ〕〔レルム〕』で構成されます。」との記載があるが，レルム付きＬｏｇｉｎＩＤ又はレルムが利用対象システムを識別することをうかがわせる記載は見当たらない。

したがって，被告の上記主張は採用できない。

イ　小括

上記アによれば，本件ユーザ認証システムプログラムは，構成要件３Ｃを充足しないから，その余の点について判断するまでもなく，本件ユーザ認証システムプログラムは，本件発明３の技術的範囲に属するとは認められない。

⑷　争点１－４（本件ユーザ認証システム装置は本件発明４の技術的範囲に属するか）について

本件発明４は，本件発明３が「プログラム」に関する発明であるのに対し，「ユーザ認証装置」に関する発明であり，この点において本件発明３と相違するが，その他の構成要件は実質的に同一であるところ，上記⑶と同様の理由により，本件ユーザ認証システム装置は，本件発明４の構成要件４Ｂを充足しないから，本件発明４の技術的範囲に属するとは認められない。

３　争点３（原告による間接侵害の成否）及び争点４（直接侵害の教唆・幇助行為による原告の不法行為の成否）について

上記１及び２で検討したところによれば，原告による間接侵害ないし直接侵

害の教唆・幇助行為による不法行為はいずれも成立しない。

４　まとめ

以上のとおり，被告の反訴請求はいずれも理由がない。

【本訴について】

５　争点６（本件各書状及び本件メールの送付等は，原告の「営業上の信用を害する」ものか）について

⑴　本件書状１及び本件書状２について

本件書状１及び本件書状２の記載内容は，前記第２の１（前提事実）⑺ア及びイのとおりであり，被告の開発したマトリクス型ワンタイムパスワード「ＰａｓｓＬｏｇｉｃ®」製品及び同製品に採用されている代表的な特許技術の紹介，被告からライセンスを受けずに販売されている特許侵害品を利用した場合にはユーザも特許侵害に問われる可能性がある旨の特許侵害に関する一般的な指摘，並びに，ＰａｓｓＬｏｇｉｃの導入又は特許のライセンスに関する連絡先の案内を内容とするものである（甲６，７）。

このような上記各書状の記載内容に照らせば，上記各書状の送付先に原告のディストリビュータやユーザが含まれているとしても，上記各書状は，被告の製品に関する一般的な販促文書にすぎないと解すべきである。

したがって，上記各書状の送付は，原告の「営業上の信用を害する」ものとはいえない。

⑵　本件書状３，本件書状４及び本件メールについて

本件書状３，本件書状４及び本件メールは，いずれも原告ソフトウェアのユーザであるニフティに対するものである。また，上記書状等の記載内容は，前記第２の１（前提事実）⑺ウないしオのとおり，いずれも，ニフティシステムの使用が本件特許権１を侵害する行為であって同社とのライセンス契約の締結を求めるというものである上，本件書状３には，上記侵害の事実が存在する旨の公証人作成の事実実験公正証書（甲８）が，本件書状４には同旨

の弁理士作成の鑑定意見書（甲９）が添付されている。そして，ニフティシステムの使用は原告ソフトウェアの使用を意味する（弁論の全趣旨）。

上記各書状及び本件メールの送付先及びその内容に照らせば，これらの書状等に原告に関する直接的な記載が見当たらないことを考慮しても，当該書状等について，一般的な被告の製品の販促文書であると解することはできず，原告ソフトウェアの使用が本件特許権１などの特許権を侵害する旨を原告ソフトウェアのユーザに指摘する文書であると解するのが相当である。

したがって，上記各書状及び本件メールは，原告の「営業上の信用を害するもの」に該当する。

６　争点７（本件各書状及び本件メールの内容は「虚偽」であるか）について

上記５のとおり，本件書状３，本件書状４及び本件メールは，原告ソフトウェアの使用が本件特許権１などの特許権を侵害する旨を原告ソフトウェアのユーザに指摘する文書であると解される。そして，被告は原告ソフトウェアにおける本件登録システムが本件発明１の技術的範囲に属する旨主張しているところ，前記１のとおり，本件発明１に係る本件特許１には無効理由があると認められるから，本件書状３，本件書状４及び本件メールの内容は「虚偽の事実」の告知に当たると認められる。

７　争点８（被告の行為の違法性・違法性阻却事由の有無）について

被告は，複数の弁理士に特許権侵害の鑑定を依頼するなどしてニフティシステムの利用が特許権侵害であると確信した上で，ニフティに対し，ライセンス交渉を求めるために本件書状３，本件書状４及び本件メールを送付したのであり，その内容及び態様は，社会通念上必要と認められる範囲であるから，被告の行為には違法性がない，又は，正当な権利行使の一環として違法性が阻却される旨主張する。

しかしながら，証拠（甲８，９）によれば，被告が侵害鑑定依頼をした弁理士は被告の当時の代理人弁理士を含めて３名にすぎないと認められ，しかも，

本件全証拠によっても，本件特許１の無効理由について調査した事実は認められないから，被告が特許権侵害の有無について十分な法的検討をした上で上記各書状等を送付したと認めることはできない。また，上記各書状等の内容は，専らニフティシステムの利用が特許権侵害に該当することを前提にライセンス契約の締結を求めるというものであり，少なくとも，本件書状４及び本件メールは，被告が，ニフティを自社製品の製造者ではなく原告ソフトウェアのユーザという第三者であることを確定的に認識した上で，同社に対して送付したものである。

このような上記各書状等の送付に至る経緯に照らせば，その内容及び態様が社会通念上必要と認められる範囲であるとも，正当な権利行使の一環であるとも認めることはできないから，被告の上記主張を採用することはできない。

８　争点９（被告の過失の有無）について

上記７で説示したとおり，被告が本件書状３，本件書状４及び本件メールの送付に先立って侵害鑑定依頼をした弁理士は被告の当時の代理人弁理士を含めて３名にすぎず，しかも，被告が本件特許１の無効理由について調査した事実も認められないから，被告が，特許権侵害の有無について十分な法的検討をした上で上記各書状等を送付したと認めることはできない。したがって，被告には上記各書状等の送付につき過失があったと認められる。

９　争点１０（原告の損害額）について

原告は，被告による本件書状３，本件書状４及び本件メールの送付により，①ニフティらに対する説明費用として，人件費６４万円及び弁護士費用５０万円以上，②無効審判請求事件及び本件訴訟に係る弁護士費用及び弁理士費用として１６７１万８８９８円，③無形損害として，少なくとも１００万円の損害が生じた旨主張する。

⑴　①及び②の損害について

ア　人件費について

証拠（甲３２ないし３５）によれば，原告の従業員が原告ユーザに対して特許権侵害の事実がない旨を説明したことは認められるが，本件全証拠によっても，当該対応に係る人件費として６４万円の損害が生じた事実を認めるに足りる証拠はない。

イ　弁護士費用及び弁理士費用について

後掲各証拠及び弁論の全趣旨によれば，原告が，①の費用として弁護士費用５４万４０２０円（甲４２。ただし，源泉所得税控除額を除く。以下同じ。），②の費用として弁護士費用等１６７１万８８９８円（甲４３の１ないし６，甲４４の１及び２）の請求を受けたことは認められるところ，被告の不正競争行為と相当因果関係のある損害としては，本件訴訟の内容や性質，経緯等に照らして，上記②のうち，本件訴訟に係る弁護士費用のうち２００万円と認めるのが相当であり，他の損害については相当因果関係を認めるに足りない。

(2)　③の損害について

原告は，被告による本件書状３，本件書状４及び本件メールのニフティに対する送付により，その信用が毀損されたと認められるところ，上記信用棄損による損害を填補する足りる金額は，上記各書状等の内容，送付先，送付回数等の諸般の事情を総合すると，少なくとも１００万円であると認めるのが相当である。

(3)　小括

以上によれば，原告の損害額は３００万円と認めるのが相当である。

１０　争点１１（信用回復措置の必要性の有無）について

上記５ないし９で説示した全ての事情を考慮すると，本件全証拠によっても，原告の求める謝罪広告を命じる必要性までは認められない。

１１　まとめ

以上によれば，原告の本訴請求は，原告ソフトウェアの開発，製造及び販売

が本件特許権１を侵害する行為である旨の告知・流布の差止め，並びに損害賠償金３００万円及びこれに対する遅延損害金の支払を求める限度で理由がある。

【結論】

１２　よって，原告の本訴請求は主文の限度で理由があるからその限度で認容してその余を棄却し，被告の反訴請求はいずれも理由がないからこれらを棄却することとして，主文のとおり判決する。

東京地方裁判所民事第４７部

裁判長裁判官　　沖　　中　　康　　人

裁判官　　矢　　口　　俊　　哉

裁判官島田美喜子は，差支えにより署名押印できない。

裁判長裁判官　　沖　　中　　康　　人

（別紙）

原告製品目録

１　認証用ソフトウェア「ＳＥＣＵＲＥＭＡＴＲＩＸ」

２　認証セキュリティシステム

「ＳＥＣＵＲＥＭＡＴＲＩＸ　Ａｌｌ－ｉｎ－Ｏｎｅ　Ｍｏｄｅｌ」

以上

（別紙）

謝罪広告目録

１　広告文

（１）見出し

謝罪広告

（２）本文（ただし，日付は広告掲載の日とする。）

当社は，平成２６年３月頃，平成２６年７月頃及び平成２７年８月頃にかけて，貴社の取引先に対して，貴社が開発販売する認証用ソフトウェア「ＳＥＣＵＲＥＭＡＴＲＩＸ」について，特許第４４５５６６６号を侵害するおそれがあるかのような記載をした文書を送付しましたが，これは当社の誤った認識によるものでした。

当社は，ここに前記文書の記載を撤回するとともに，貴社の信用を害したことを謝罪致します。

平成　　年　　月　　日

パスロジ株式会社

株式会社シー・エス・イー御中

２　掲載条件

（１）掲載条件

ア　縦　２段

イ　横　１０センチメートル

（２）活字の大きさ

前記紙面に見出し及び本文を掲載し得る範囲で最大限の活字

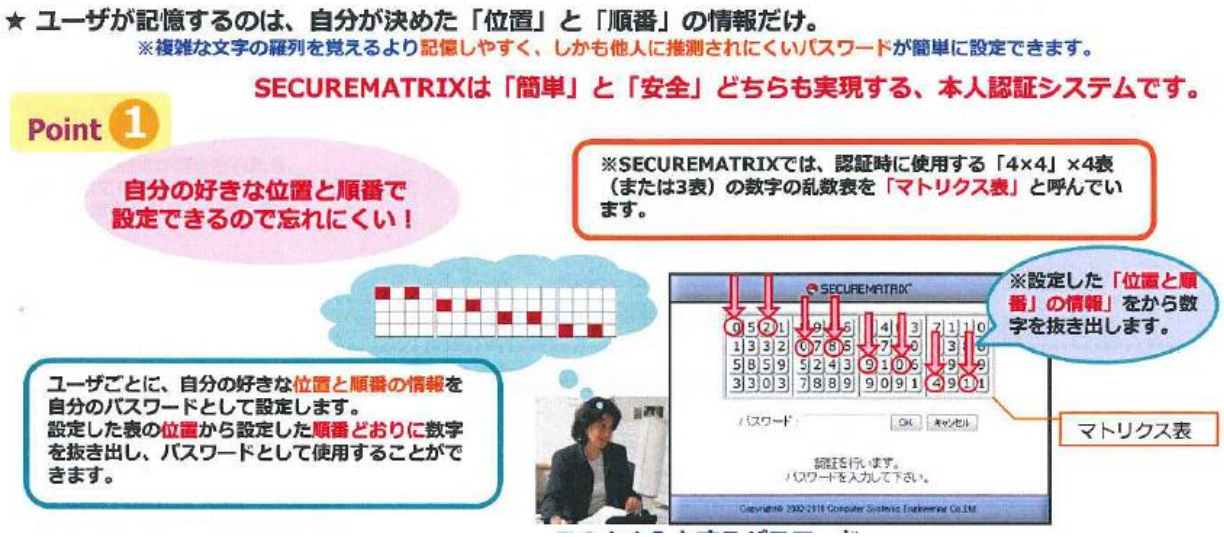
以　　上

（別紙）

本件登録システム方法の構成（被告主張）

１．パスワードとなる位置と順番の決定

ユーザは，「４×４」×４表（または３表）の数字の乱数表（以下「マトリクス表」という。）を構成するマス目から，ユーザのパスワードとして使用する，特定のマス目の位置と順番を決定する。



２．抜き出した数字の入力（１回目）

ユーザは，パソコン，携帯電話，スマートフォン等の端末装置の画面上に提示されたマトリクス表から，パスワードとなる位置と順番のマス目に割り当てられた数字を抜き出し，入力フォームに抜き出した数字列を入力する。

３．抜き出した数字の入力（２回目）

数字列の入力を受け付けると，ユーザの端末装置の画面上に，新しい数字が割り当てられたマトリクス表が表示される。ユーザは，再度，パスワードとなる位置と順番のマス目に割り当てられた数字を抜き出し，入力フォームに抜き出した数字列を入力する。

４．設定されたパスワードの確認

２回目の入力によって，セキュアマトリクス認証サーバがパスワードとなる位置と順番を特定し，それをマトリクス表の上に反映して，ユーザに提示する。ユーザは，これが自分の設定したものと合っていることを確認して，「ＯＫ」をクリックする。


Step 6
（設定した位置と順番が合っているのでOKね！）
SECUREMATRIX
設定した「位置と順番」の情報がマトリクス表の上に反映されていることを確認してから、「OK」をクリック。
パスワード変更中（ログインID:emoizumi01）
あなたの選択したパスワード情報は以下のとおりです。
パスワード情報 ********
'*' の部分は位置情報です。マトリクス表の数字を参照して下さい。
確認後よければ、OKを押して下さい。
OK
キャンセル
この画面を早く閉じて下さい
Copyright© 2002-2010 Computer Systems Engineering Co.,Ltd.

以上

（別紙）

本件登録システム方法の構成（原告主張）

原告ソフトウェアによる本件登録システム方法は，以下の方法により，ワンタイムパスワードを導出するためのマトリクス表中のマス目の位置及び順番を，ワンタイムパスワード導出ルールとして登録するものである。

① ＳＭＸ認証サーバが，クライアント端末においてユーザに提示される「パスワード変更用マトリクス」を生成する際に使用される情報である「パスワード変更用ｓｅｅｄ」を生成する。この「パスワード変更用ｓｅｅｄ」は，入力ユーザＩＤと組み合わされることで「パスワード変更用マトリクス」に含まれるパターン要素をユニークに決定する情報である（特許第３９３９７３６号明細書（甲２５）段落【００３１】参照。当該特許のシード値は認証のための１つのパターンを特定するものであるが，本件登録システムの「パスワード変更用ｓｅｅｄ」は当該特許のシード値を以下のように拡張し，１つの「パスワード変更用ｓｅｅｄ」が登録のための２つのパターンを特定するものとし，なおかつ，２回のパターンの提示で必ずパスワードを特定できるパターンの組を生成する数値を選抜したものである。）。

「パスワード変更用ｓｅｅｄ」は，乱数発生アルゴリズムによって発生した所定範囲内の数値であり，それのみでは「パスワード変更用マトリクス」をユニークに決定することはできない（段落【００３３】参照）。

② クライアント端末は，「パスワード変更用ｓｅｅｄ」を受信すると同端末にインストールされたプログラムにより，ユーザが入力するユーザＩ

Ｄを同「パスワード変更用ｓｅｅｄ」と組み合わせ，ユニークで，且つ当該２回分への入力結果で「ワンタイムパスワード導出ルール」が特定される「パスワード変更用マトリクス」をクライアントにおいて発生規則に従って２回分同時に（「パスワード変更用マトリクス」１回目及び２回目）発生させる。

③　クライアント端末は，ユーザに「パスワード変更用マトリクス」（１回目）を提示し，ユーザが登録しようとする「ワンタイムパスワード導出ルール」に基づきマトリクス表のマス目に割り当てられた数字を入力するようにユーザに促す（１回目の提示。ユーザによる１回目の入力)。

④　ユーザによる１回目の数字入力終了後，クライアント端末は既に発生させている「パスワード変更用マトリクス」（２回目）をユーザに提示し，「ワンタイムパスワード導出ルール」に基づきマトリクス表のマス目に割り当てられた数字の入力を促す（２回目の提示。ユーザによる２回目の入力　→　これにより「ワンタイムパスワード導出ルール」が特定される。)。

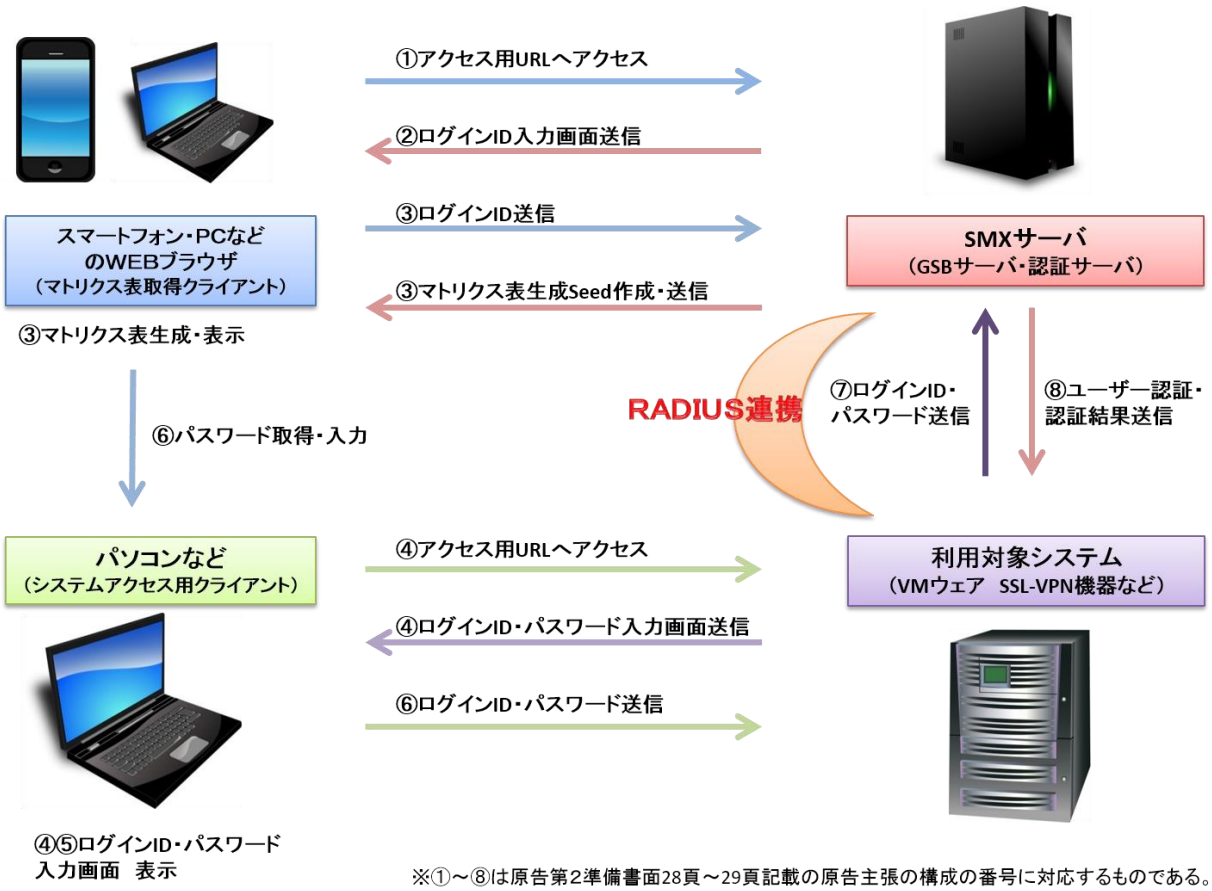
⑤　ユーザによる上記２回の数字入力結果（ユーザによる１回目の入力結果及び２回目の入力結果）が，「ＳＭＸ認証サーバ」に送信される。「ＳＭＸ認証サーバ」は，クライアント端末から送信された２回の数字入力結果と，自ら「パスワード変更用ｓｅｅｄ」から生成した１回目と２回目のパスワード変更用マトリクス（クライアントで発生させた１回目と２回目のパスワード変更用マトリクスと同じ）から，ユーザにより選択，特定された「ワンタイムパスワード導出ルール」を取得し，パスワードポリシー違反の有無などを確認する。

⑥ 「ＳＭＸ認証サーバ」の確認後，クライアント端末において，入力されたパターンを表わす変更パスワード確認用マトリクスを表示し，ユーザがクライアント端末においてパスワードが正しく入力されたことの確認を行う。クライアント端末から確認を受け，「ＳＭＸ認証サーバ」がパスワード（マス目の位置と順番）を登録する。

（別紙）

本件ユーザ認証システムプログラムの構成（被告主張）

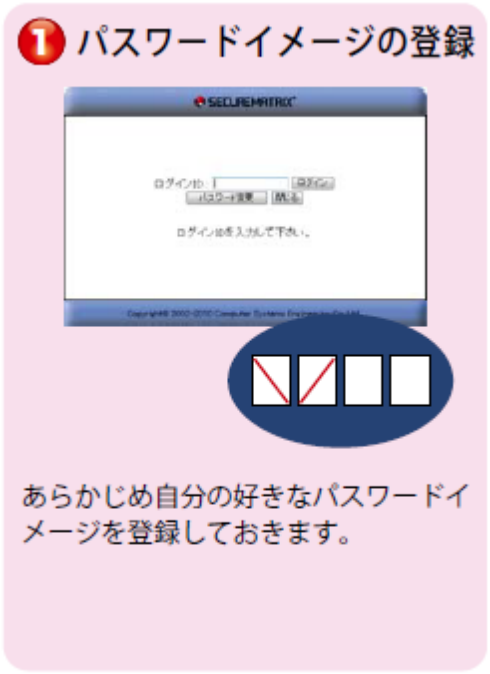
第１　構成図



第２　原告ソフトウェアが「ＶＭＷａｒｅ」と組み合わせて使用される場合

１　パスワードイメージの登録

ユーザは，あらかじめ，セキュアマトリクス認証サーバに，パスワードとなるマトリクス表上のマス目の位置と順番（以下「パスワードイメージ」という。）を，別紙「本件登録システム方法の構成（被告主張）」に記載した方法で登録する。



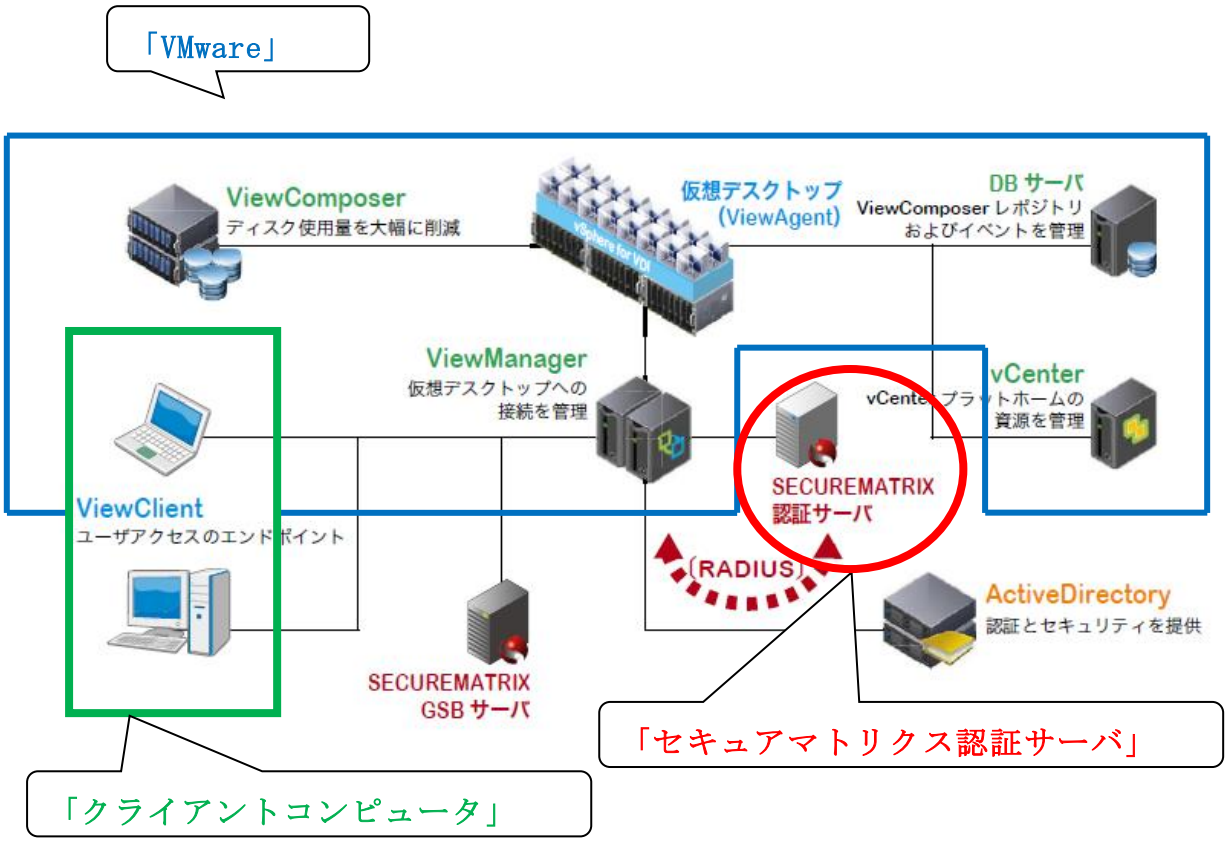
2　マトリクス表の生成

以下の説明においては，仮想化環境[1]構築用ソフトウェア「VMware View（ヴイエムウェア・ビュー)」[2]によって構築されたシステム（下図に示された「View Client」「View Composer」「View Manager」「仮想デスクトップ[3]（View Agent)」「View Center」「DB サーバ」を含むシステム）を総称して，「VMware（ヴイエムウェア)」と呼ぶ。

ユーザは，「VMware」のクライアントソフトウェア「View Client（ビュー・クライアント)」がインストールされているユーザの端末（以下「クライアン

1 コンピュータ上にソフトウェアによって仮想的に構築されたコンピュータ（仮想マシン）が備える仕様や機能の総体のこと。
2　米国 VMware 社が提供する，仮想化技術のうち仮想デスクトップ方式を実現する製品群を総称して「VMware View」と呼ぶ。
3 仮想デスクトップとは，企業の情報システムなどで，デスクトップ環境を仮想化してサーバ上に集約すること。利用者はクライアント機からネットワークを通じてサーバ上の仮想マシンに接続し，デスクトップ画面を呼び出して操作する。

トコンピュータ」という。）から「VMware」に関する識別情報を送信する。それをセキュアマトリクス認証サーバが受け付けると，当該クライアントコンピュータからの要求に応じマトリクス表を生成する。



3　マトリクス表の表示

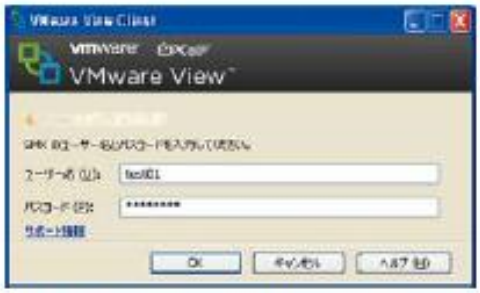
セキュアマトリクス認証サーバは，生成したマトリクス表の情報をクライアントコンピュータに送信し，ブラウザを使って表示させ，ユーザに対し提示する。

①ブラウザを使ってマトリクス表を表示します。

4　「View Client」へのユーザ名・パスワード入力

「View Client」は，ユーザに対し，ユーザ名と，ブラウザに表示したマトリクス表から，あらかじめ登録したパスワードイメージに従って抜き出した数字列を入力するよう入力フォームを表示する。

ユーザは，「View Client」の入力フォームに，ユーザ名のほか，ブラウザに表示されたマトリクス表を見ながら，パスワードイメージに従って数字を抜き出し，抜き出した数字列を入力する。



5　「Active Directory」のパスワード入力

ユーザが，「View Client」にユーザ名と，パスワードイメージに従って抜き出した数字列を入力すると，「View Client」は，ユーザに対し，さらに「Active Directory」[4]のユーザ名とパスワードを入力するよう入力フォームを表示する。ユーザは，「View Client」に，「Active Directory」のユーザ名とパスワードの入力を行う。

[4] Microsoft 社のサーバコンピュータ向け OS の製品「Windows Server」の機能の一つで，管理するネットワーク上に存在する様々な資源やその利用者の情報や権限などを一元管理することができるもの。

③ActiceDirectory のユーザー名とパスワードを入力します。

6　仮想デスクトップへの接続

上記３及び４にてユーザが「View Client」に入力した各ユーザ名・パスワードが正当であれば，Windows7 デスクトップ（仮想デスクトップ）へ接続がなされ，Windows7 デスクトップが起動する。

④仮想デスクトップに接続します。　⑤　～デスクトップ起動中画面～

7　仮想デスクトップへの接続完了

Windows7 デスクトップの起動が完了する。このときクライアントコンピュータの画面上に起動する Windows7 デスクトップは，仮想デスクトップである。

⑥デスクトップの起動が完了しました。

以上

（別紙）

本件ユーザ認証システムプログラムの構成（原告主張）

① ユーザが，クライアント端末においてＳＭＸ認証画面へのアクセス用ＵＲＬを入力し，クライアントからＳＭＸ認証サーバへ，同ＵＲＬが送信される。なお，係るアクセスＵＲＬは，ユーザが利用を望むシステムが VMWare の場合でも，他のシステムの場合でも変わらない同一のものである。

② ①によりアクセスＵＲＬを受けたＳＭＸ認証サーバは，ログインＩＤ入力用の画面を生成し，クライアント端末へと送信する。ログインＩＤは，ＳＭＸ認証サーバにおいて，各利用システム毎に付されるものではなく，ユーザ固有の番号である。

③ クライアント端末に表示されたログインＩＤ入力画面において，ユーザがログインＩＤを入力すると，クライアント端末からＳＭＸ認証サーバへとログインＩＤが送付される。ログインＩＤを受けたＳＭＸ認証サーバは，マトリクス表を生成する基となるｓｅｅｄを生成し，クライアント端末へと送信する。クライアント端末では送信を受けたｓｅｅｄとログインＩＤに基づきマトリクス表を生成・表示する。これが，乙２１の利用イメージにおいては「①ブラウザを使ってマトリクス表を表示します。」とされる画面である。

④ 上記①～③の動作とは別途に，ユーザは，VMware View の「ユーザ名及びパスコード」入力画面を表示するため，当該入力画面の該当ＵＲＬをクライアント端末へと入力する。これにより，クライアント端末から VMware サーバへとアクセスがなされ，同サーバからクライアント端末へ「ユーザ名及びパスコード」の入力画面が送信される。クライアント端末においては，送信を

受けた「ユーザ名及びパスコード」入力画面が表示される。これが，乙２１の利用イメージにおいて「②ユーザ名と，マトリクス表から抜き出したパスワードをパスコード欄に入力します」として表示されている画面である。

⑤ このように，クライアント端末には，ＳＭＸ認証サーバから上記③のマトリクス表が，VMware View から「ユーザ名及びパスコード」入力画面が，それぞれ送信されることになるが，ユーザは，クライアント端末のブラウザ上で，適宜切り替えて各画面を表示することになる。

⑥ ユーザは，「ユーザ名及びパスコード」入力画面に対して，上記マトリクス表から得られたパスワード及びログインＩＤを入力する（このログインＩＤは，上記②で用いられたログインＩＤと同一の番号のものが用いられる）。ユーザにより入力されたログインＩＤ及びパスワードは，クライアント端末から VMware サーバへと送信される。

⑦ クライアント端末からログインＩＤとパスワードの送信を受けた VMware サーバは，これらをＳＭＸ認証サーバへと送付する。

⑧ ＳＭＸ認証サーバは，送信を受けたログインＩＤ及びパスワードと上記③においてＳＭＸ認証サーバがクライアント端末から受けたログインＩＤ及びＳＭＸ認証サーバが生成したマトリクス表に基づくパスワードとに基づきユーザ認証を行う。上記②で述べた通り，ＳＭＸ認証サーバにおいて，ログインＩＤは，各利用システムに付されるものではなく，ユーザに固有の番号であるから，ＳＭＸ認証サーバでは，１組のログインＩＤ及びパスワードのみによって，複数の利用システムでユーザ認証を行うことができる。

以上