(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4932108号
(P4932108)

(45)発行日　平成24年5月16日(2012.5.16)　(24)登録日　平成24年2月24日(2012.2.24)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675Z
H04L	9/10	(2006.01)	H04L	9/00	621A
G09C	1/00	(2006.01)	G09C	1/00	660D

請求項の数 24　(全 29 頁)

(21)出願番号	特願2001-500933 (P2001-500933)
(86)(22)出願日	平成12年5月25日 (2000.5.25)
(65)公表番号	特表2003-501915 (P2003-501915A)
(43)公表日	平成15年1月14日 (2003.1.14)
(86)国際出願番号	PCT/GB2000/001996
(87)国際公開番号	WO2000/073879
(87)国際公開日	平成12年12月7日 (2000.12.7)
審査請求日	平成19年5月22日 (2007.5.22)
(31)優先権主張番号	99304164.9
(32)優先日	平成11年5月28日 (1999.5.28)
(33)優先権主張国	欧州特許庁 (EP)

(73)特許権者　398038580
ヒューレット・パッカード・カンパニー
HEWLETT－PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　３０００
(74)代理人　100087642
弁理士　古谷　聡
(74)代理人　100076680
弁理士　溝部　孝彦
(74)代理人　100063897
弁理士　古谷　馨

最終頁に続く

(54)【発明の名称】文書にデジタル署名するためのシステム

(57)【特許請求の範囲】

【請求項１】

文書をデジタル署名するシステムであって、

文書(505)を表わす画像データを生成し、該画像データをフレームバッファメモリ(315)に記憶する手段(500)と、

前記フレームバッファメモリ(315)から前記画像データを読み出し、表示可能な画像データを生成し、表示手段へ伝送することにより、前記表示手段に前記表示可能な画像データを表示させる手段(320)と、

前記フレームバッファメモリ(315)から前記画像データを読み出し、該画像データによって表される文書(505)に関連するデジタル署名を生成する手段(300,520)と、

デジタル署名処理中は、少なくとも前記文書の画像データを含む前記フレームバッファメモリ(315)の部分に対するアクセス権を有しないアプリケーション又はプロセスの書込みアクセスを拒絶し、それによって、前記デジタル署名処理中は、前記フレームバッファメモリの対応する部分に記憶された前記文書の画像データ、及び、従って前記表示手段上に表示される前記文書の表示可能な画像データを、前記アクセス権を有しないアプリケーション又はプロセスの書込みアクセスにより変更することが出来ないようにする手段(520)と

からなるシステム。

【請求項２】

前記文書を表示するためのグラフィック信号を生成する主処理手段(200)を更に含み、

前記表示可能な画像データを生成する手段(320)は、前記主処理手段(200)によって生成されたグラフィック信号に基づいて前記表示可能な画像データを生成するように構成され、

前記フレームバッファメモリから画像データを読み出す手段(320)は、前記画像データをその実際の画像を前記表示手段上に表示するのに適した信号に変換し、該信号を表示可能な画像データとして前記表示手段(105)へ伝送するように構成される、請求項１に記載のシステム。

【請求項３】

前記画像データ、又は該画像データを表わすものを受信し、対応するデジタル署名を生成するトークン処理手段(400)を含むリムーバブルトークン(122)を更に含む、請求項１、又は請求項２に記載のシステム。

【請求項４】

前記文書(505)をデジタル署名するための要求信号を生成する手段(110,115,500)を更に含み、

前記画像データによって表される文書に関連するデジタル署名を生成する手段(300,520)は、前記主処理手段(200)及び前記トークン処理手段(400)から独立した処理手段(300)を含む高信用コンポーネント(260)として構成され、

前記トークン処理手段(400)は、前記要求信号の受信時に、ユーザに関連するデジタル署名を生成するように構成され、

前記フレームバッファメモリ(315)、前記画像データを読み出し、表示可能な画像データを生成する手段(320)、及び前記表示手段(105)は、合わせて１つの表示システムを構成し、前記表示システムは、前記デジタル署名処理の際に、前記高信用コンポーネントによってのみ制御される、請求項２、又は請求項３に記載のシステム。

【請求項５】

前記高信用コンポーネント(260)は、高信用画像データを取得、及び／又は生成する手段と、前記デジタル署名処理の際に、前記表示システムを制御し、前記高信用画像データを使用して、デジタル署名すべき表示された前記文書画像をハイライトする手段とを更に含み、前記高信用画像データは、ユーザを一意に特定する、請求項４に記載のシステム。

【請求項６】

前記高信用画像データは、前記高信用画像を表わすピクスマップデータ、又は前記高信用画像を形成するための命令を含む、請求項５に記載のシステム。

【請求項７】

前記表示システムを制御し、デジタル署名すべき表示された前記文書画像をハイライトする手段は、

前記高信用画像によって特徴付けられ、前記文書画像の周囲の少なくとも一部に配置された境界、又は境界を規定する１又は複数のインジケータ、

前記文書画像の背景の少なくとも一部を形成する前記高信用画像によって特徴付けられた背景パターン、

前記文書画像内に形成された前記高信用画像によって特徴付けられた画像、及び

前記文書画像内に、又は前記文書画像の近くに形成された前記高信用画像によって特徴付けられたテキストメッセージ

のうちの１以上を前記表示手段上に生成することによって、前記表示システムを制御する、請求項５、又は請求項６に記載のシステム。

【請求項８】

前記高信用コンポーネント(260)は、リムーバブルトークン(122)から高信用画像データを取得、及び／又は生成する手段を含む、請求項５～７のうちのいずれか一項に記載のシステム。

【請求項９】

前記高信用コンポーネント(260)は、前記表示システムを制御し、ユーザに対してメッセージを表示させる手段を更に含む、請求項４に記載のシステム。

【請求項１０】
高信用入力手段を更に含み、それによってユーザは、安全な態様でメッセージに応答することが可能である、請求項９に記載のシステム。
【請求項１１】
前記高信用入力手段は、安全な通信路を介して前記高信用コンポーネント(260)に接続されたスイッチ(135)を含む、請求項１０に記載のシステム。
【請求項１２】
前記高信用コンポーネント(260)と前記リムーバブルトークン(122)は、さらなる対話を行う前に相互認証プロセスを実施する、請求項４～８のうちのいずれか一項に記載のシステム。
【請求項１３】
前記高信用コンポーネント(260)は、前記表示システムの一体部分を形成する、請求項４に記載のシステム。
【請求項１４】
前記表示システムは、前記高信用コンポーネント(260)が、前記主処理手段(200)と前記フレームバッファメモリ(315)の間に物理的、及び機能的に配置され、前記主処理手段(200)が、前記高信用コンポーネントの機能によって間接的にしか前記フレームバッファメモリ(315)にアクセスできないように構成される、請求項１３に記載のシステム。
【請求項１５】
デジタル署名動作を要約するデータを生成する手段を更に含む、請求項１～１５のうちのいずれか一項に記載のシステム。
【請求項１６】
文書をデジタル署名するためにコンピュータにより実施される方法であって、
文書(505)のデジタル画像データを生成し、フレームバッファ(315)内の前記デジタル画像データを更新するステップと、
前記フレームバッファメモリから前記デジタル画像データを読み出し、該デジタル画像データを視覚表示手段の駆動に適した信号に変換し、該信号を視覚表示手段(105)へ伝送し、前記文書の画像を表示させるステップと、
デジタル署名の要求に応じて、前記フレームバッファメモリ(315)から前記デジタル画像データを読み出し、表示する際に、前記文書に関連するデジタル署名を生成するステップと、
前記デジタル署名の生成中は、アクセス権を有しないプロセスによる前記フレームバッファメモリに対する書込みアクセスを一時的に拒絶し、それによって、デジタル署名処理中は、前記フレームバッファに記憶された前記デジタル画像データ、及び、従って前記視覚表示手段を駆動するために前記デジタル画像データから変換された信号を、アクセス権を有しないプロセスにより変更することが出来ないようにするステップと
からなるコンピュータにより実施される方法。
【請求項１７】
高信用画像データを取得、及び／又は生成し、該高信用画像データを使用して、表示された前記文書画像をハイライトするステップを更に含み、前記高信用画像データは、ユーザを一意に特定する、請求項１６に記載のコンピュータにより実施される方法。
【請求項１８】
前記表示された文書画像をハイライトするステップは、
前記高信用画像によって特徴付けられ、前記文書画像の周囲の少なくとも一部に配置された境界、又は境界を規定する１又は複数のインジケータ、
前記文書画像の背景の少なくとも一部を形成する前記高信用画像によって特徴付けられた背景パターン、
前記文書画像内に形成された前記高信用画像によって特徴付けられた画像、及び
前記文書画像内に、又は前記文書画像の近くに形成された前記高信用画像によって特徴付けられたテキストメッセージ

のうちのいずれか１つ、又は複数の視覚的効果を前記視覚表示手段上に生成することにより達成される、請求項１７に記載のコンピュータにより実施される方法。
【請求項１９】
前記高信用画像データは、リムーバブルトークン(122)から取得される、請求項１７、又は請求項１８に記載のコンピュータにより実施される方法。
【請求項２０】
請求項１６～１９のうちのいずれか一項に記載のコンピュータにより実施される方法にしたがって文書をデジタル署名するように構成されたシステム。
【請求項２１】
複数の閲覧可能なページを有する文書をデジタル署名するためにコンピュータにより実施される方法であって、
前記複数の閲覧可能なページのそれぞれについて、請求項１６～１９のうちのいずれか一項に記載のコンピュータにより実施される方法にしたがって、そのページに関連するデジタル署名を生成するステップと、
前記複数の閲覧可能なページ全てのデジタル署名に関連するさらに別のデジタル署名を生成するステップと
からなるコンピュータにより実施される方法。
【請求項２２】
請求項１６～１９のうちのいずれか一項に記載のコンピュータにより実施される方法にしたがって、第１のユーザによって既に署名され、前記第１のユーザの秘密鍵を使用して生成された第１のデジタル署名が添付された文書を第２のユーザが副署名するためにコンピュータにより実施される方法であって、
前記第１のデジタル署名の完全性を検証するステップと、
前記第２のユーザの秘密鍵を使用し、請求項１６～１９のうちのいずれか一項に記載のコンピュータにより実施される方法にしたがって、前記文書に関連する第２のデジタル署名を生成するステップと
からなるコンピュータにより実施される方法。
【請求項２３】
請求項１６～１９のうちのいずれか一項に記載のコンピュータにより実施される方法にしたがって、第１のユーザによって既に署名され、前記第１のユーザの秘密鍵を使用して生成された第１のデジタル署名が添付された文書を第２のユーザが副署名するためにコンピュータにより実施される方法であって、
前記第１のデジタル署名の完全性を検証するステップと、
前記第２のユーザの秘密鍵を使用し、請求項１６～１９のうちのいずれか一項に記載のコンピュータにより実施される方法にしたがって、前記第１のデジタル署名に関連する第２のデジタル署名を生成するステップと
からなるコンピュータにより実施される方法。
【請求項２４】
前記高信用コンポーネントは、改竄に対する耐性を有するように製造される、請求項４～１４のいずれか一項に記載のシステム。
【発明の詳細な説明】
【０００１】
【技術的背景】
本発明は、署名者が署名しようと思う文書が実際に署名する文書であるよう署名者に高度な信用を提供するように、画像データ、特に文書にデジタル署名する装置及び方法に関する。
【０００２】
【背景技術】
従来の先行技術による量販市場コンピューティングプラットフォームには、周知のパーソナルコンピュータ（ＰＣ）及びＡｐｐｌｅ　Ｍａｃｈｉｎｔｏｓｈ（登録商標）等の競合

製品、及び既知のパームトップ及びラップトップパーソナルコンピュータの急増がある。一般に、これらのマシンの市場は２つのカテゴリ、すなわち家庭用または消費者用と企業用に分けられる。家庭用または消費者使用のコンピューティングプラットフォームの一般的な要件は、比較的高い処理能力、インターネットアクセス機能、及びコンピュータゲームを扱うのためのマルチメディア機能である。この種のコンピューティングプラットフォームの場合、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）９５及び９８オペレーティングシステム製品及びＩｎｔｅｌプロセッサ、いわゆるＷｉｎＴｅｌプラットフォームが市場を独占している。

【０００３】

一方、ビジネスでの使用の場合、零細企業から多国籍組織まで様々な組織向けに利用可能な、製造販売独占権を有する極めて多くのコンピュータプラットフォームが存在している。これらアプリケーションの多くは、サーバプラットフォームが、中央集中化されたデータ記憶装置及びアプリケーション機能を、複数のクライアントステーションに対して提供する。ビジネスでの使用の場合、他の重要な評価尺度としては、信頼性、リモートアクセス機能、ネットワーキング機能、及びセキュリティ機能等がある。このようなプラットフォームについては、ＵＮＩＸはもちろんＭｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ　ＮＴ４．０（登録商標）オペレーティングシステムが一般的であり、さらに最近ではＬｉｎｕｘオペレーティングシステムも用いられる。

【０００４】

Ｗｉｎｄｏｗｓタイプのオペレーティングシステムは、ユーザが別個のウィンドウで別個のアプリケーションを実行することを可能にしており、いわゆるＷＩＭＰ（ウィンドウ、アイコン、メニュー、及びポインタ）インタフェースを提供する。これによって、ユーザは通常キーボードを用いてデータを入力し、マウスを用いてオプションを選択することによりアプリケーションと対話を行い、また、ダイアログボックス及びドロップダウン（またはプルアップ）メニューを介してアプリケーションを制御する。

【０００５】

「Ｅ－コマース」として知られるインターネットを介して取引が行われる商業活動の増大に伴い、従来技術では、インターネットを介してコンピュータプラットフォーム間のデータトランザクションを可能にすることに大きな関心があった。特に、現在標準的に用いられている手書きで署名した紙の契約書を必要とせずに、ユーザがインターネット越しに契約の締結へ入れることが重要であると認識されている。しかし、電子データの不正や改竄の可能性があるため、このような提案では、完全にトランスペアレントで効率的な市場に要求される広範囲規模での遠隔地にいる見知らぬ相手との完全に自動化された取引は、今まで控えられていた。このような取引を行うための根本的な問題は、ユーザとコンピュータプラットフォームとの間、及び対話を行うコンピュータプラットフォーム間の信用の問題である。

【０００６】

コンピュータプラットフォームのセキュリティ及び信用度の増大を目的とするいくつかの従来技術による方式がある。主に、これらはアプリケーションレベルでのセキュリティ機能の追加によるものであり、言い換えるなら、セキュリティ機能はオペレーティングシステムのカーネルに最初から埋め込まれてはおらず、コンピューティングプラットフォームの基本的なハードウェアコンポーネントに内蔵されてはいない。スマートカードを備えたポータブルコンピュータ装置がすでに市場に出回っており、これらのスマートカードは、コンピュータのスマートカードリーダへ入力されるユーザ固有のデータを保持している。現在、このようなスマートカードは従来のパーソナルコンピュータへの増設機器のレベルにあり、周知のコンピュータの筐体に内臓されている場合もある。これらの従来技術による方式はコンピュータプラットフォームのセキュリティをいくらか向上させるが、従来技術による方式によって得られるセキュリティ及び信用度のレベルは、コンピュータプラットフォーム間での自動化された取引のアプリケーションを普及させるには不十分であると思われる。ビジネスにおいて大きな価値ある取引が広範規模の電子商取引にさらされる前

に、基礎的な技術についてさらに大きな信用度が必要とされるであろう。
【０００７】
２０００年２月１５日付で出願された本出願人の同時係属国際特許出願ＰＣＴ／ＧＢ００／００５２８「Trusted Computing Platform」、及び２０００年３月３日付で出願されたＰＣＴ／ＧＢ００／００７５２「Smartcard User Interface for Trusted Computing Platform」は、ここで参照することによって全内容を取り入れるものとする。これらには、内蔵型ハードウェアコンポーネントの形態で「高信用コンポーネント」を有するコンピュータプラットフォームから成る「高信用コンピュータプラットフォーム」の概念が開示されている。各々がこのような高信用コンポーネントを備える２つのコンピュータエンティティは、互いに高い「信用」度で対話することができる。すなわち、第１及び第２のコンピュータエンティティが互いに対話する場合、対話のセキュリティは、高信用コンポーネントが存在しない場合と比較して拡張される。これは次のような理由による。・コンピュータエンティティのユーザは、自分自身のコンピュータエンティティの完全性及び機密性に関して、及び他の相手に属するコンピュータエンティティの完全性及び機密性に関して、高い信用度を有する。
・各々のエンティティは、前記他のエンティティが実際に目的とするエンティティであるということに関して、信用がある。
・これらのエンティティの一方または両方が、トランザクション、例えばデータ転送トランザクションに対する相手を表す場合、内蔵された高信用コンポーネントによって、このエンティティと対話する第三者のエンティティは、このエンティティが実際にそのような相手を表すということに関して、高度の信用度を有する。
・高信用コンポーネントは、高信用コンポーネントによって実施される検証及び監視プロセスを通して、このエンティティ自体の固有の機密性を増大させる。
・コンピュータエンティティが予期されるように振る舞う可能性がより高くなる。
【０００８】
上述したように、文書に署名する従来の方法は、文書の画像が再現される媒体（通常は紙）上へ物理的に署名するというものである。この方法は、署名されている対象が明確であること、及びこの署名された画像が署名された対象の証明になるという利点を有する。しかし、このことは電子商取引の必要性には合致しない。
【０００９】
今日では、従来のコンピュータプラットフォーム及び標準的な暗号化技術を用いて文書にデジタル署名することも可能である。しかし、本発明者らは、従来のコンピュータプラットフォームにおいて、デジタル署名された文書の電子翻訳は通常、ユーザが目にすることができる文書と同じ翻訳ではないと認識している。したがって、ユーザが、署名を意図するデータとは異なるデータにうっかり署名してしまう可能性がある。従来では、ユーザがデータに故意に署名を行い、この署名されたデータはコンピュータプラットフォームによって自分に表示されたものに一致しないということを、後から不正に主張することも可能である。このような問題は、上述した高信用プラットフォームが用いられた場合であっても依然として存在する。
【００１０】
従来の電子的な署名方法は、当業者にとって周知である。本質的に、デジタルデータは、例えばハッシュ関数の使用によってダイジェストに圧縮される。次に、このダイジェストが、秘密鍵（または単に「秘密」とも呼ばれる）によって初期化されたある暗号化方法の使用によって暗号化される。これは、通常、ＰＣ等のコンピュータプラットフォーム上で行われる。一つの実施としては、コンピュータプラットフォームに取り付けられたスマートカードリーダに挿入されるユーザのスマートカード内に機密に保持された秘密鍵を用いて、データに署名するというものである。テキスト文書という特定の場合、デジタルデータはＭｉｃｒｏｓｏｆｔのＮｏｔｅｐａｄ、Ｗｏｒｄｐａｄ、またはＷｏｒｄ等のワードプロセッサアプリケーションによって生成されるファイルであることができる。通常、署名という動作は、署名者が署名されたデータの意味に対して法的な責任を受諾することを

意味している。

【００１１】

ハッシュ関数は従来技術において周知であり、この関数は比較的大量の入力データから比較的少量の出力データを生成することのできる一方向関数であり、入力データのわずかな変更によって出力データは大幅に異なってくる。よって、ハッシュ関数が適用されるデータファイルは、第１のダイジェストデータ（ハッシュ関数の出力）を生じる。わずかな変更、例えばオリジナルデータファイル内の単一ビットを変更すると、この変更されたデータファイルにハッシュ関数が再度適用された場合、大幅に異なる出力を生じる。このようにして、数メガバイトのデータを含むデータファイルをハッシュ関数に入力すると、１２８～１６０ビット長のデジタル出力が、結果のダイジェストデータとして生じる。データファイルから生成した比較的小量のダイジェストデータを予約されたディレクトリへ保管することは、高信用コンポーネントがより少ないメモリ空間及びより少ない処理能力の使用で動作することになるため有益である。

【００１２】

既知の署名プロセス中、ユーザは通常、文書がコンピュータのモニタに通常の倍率及び解像度でレンダリングされる際に、その文書を解釈する。既存のアプリケーションにおいて、ユーザのスマートカードは、文書を作成または操作あるいはその両方を行うために使用されるアプリケーションが文書を表現する形式でデータに署名する。しかし、本発明者らは、ソフトウェアには、ユーザが画面を閲覧しているときに、ユーザが知っているものとは異なる意味を持つスマートカードへデータを送信してしまう可能性があると考える。この可能性は、人々に解釈される文書の電子的表現物にデジタル署名する従来の方法の有効性に疑念を導入するのに十分な理由でありうる。

【００１３】

【発明の開示】

本発明は、人々に解釈されるデジタル署名された文書の信用を向上するシステム及び方法からなる。該システム及び方法は必然的に、他の目的に使用可能なデータの信用のある表示も含んでいる。

【００１４】

第１の態様によれば、本発明は、文書を表すデジタル署名を生成するように構成されるデータ処理システムであって、

デジタル署名する文書を格納するための主記憶手段と、

文書を表示するためのグラフィック信号を生成する手段を含む、少なくとも１つのアプリケーションプロセスを実行するための主処理手段と、

前記署名する文書に対して要求信号を生成するための手段と、

フレームバッファメモリと、

前記グラフィック信号に基づいて前記文書を表すデジタル画像データを生成し、このデジタル画像データを前記フレームバッファメモリに格納するための手段と、

前記フレームバッファメモリから前記デジタル画像データを読み出し、このデータを、実際の画像の表示するのに適した信号へ変換し、この信号を表示手段へ転送する手段と、からなる表示システムと、

前記デジタル画像データを表すデジタル署名を生成するため、前記要求信号に応答して動作可能な、独立した処理手段を含む高信用コンポーネントと、

からなるデータ処理システムを提供する。ここで、デジタル署名は、文書をユーザに表示するために用いられるデータを基にして生成される。

【００１５】

好ましい実施形態において、高信用コンポーネントは、あらゆるアクセス権の無いアプリケーションまたはプロセスが、文書のデジタル画像データを保持している前記フレームバッファメモリの少なくとも一部へ書き込みアクセスを行うことを拒絶するための手段と、フレームバッファメモリの各々の部位がデータの書き込みについてアクセス不可能である間にデジタル画像データを表すデジタル署名を生成するための手段と、からなる。

【００１６】
好ましい実施形態において、データ処理システムは、フレームバッファメモリからデジタル画像データもしくはこれを表すものを受信し、それぞれののデジタル署名を生成するための処理手段からなるリムーバブルトークンをさらに含む。便利な例としては、リムーバブルトークンは、適切にプログラムされたスマートカードである。
【００１７】
好ましい実施形態において、高信用コンポーネントは、高信用画像データを取得または生成あるいはその両方を行うための手段と、高信用画像データを用いて表示された文書画像をハイライトさせるために表示システムを制御するための手段と、からなる。この手段は、高信用コンポーネントが動作の制御下にあることの視覚的なフィードバックをユーザへ提供する。
【００１８】
高信用画像データは、高信用画像または高信用画像を形成するための命令を表すピクスマップデータを含みうる。好ましくは、高信用コンポーネントは、リムーバブルトークンから高信用画像データを取得または生成あるいはその両方を行う手段を含む。高信用コンポーネントは、メッセージをユーザに表示するよう表示システムを制御する手段をさらに備えることが好ましい。
【００１９】
好ましい実施形態において、データ処理システムは、ユーザが安全にメッセージに応答可能な高信用入力手段をさらに備える。高信用入力手段は、安全な通信路を介して高信用コンポーネントに接続されるスイッチを備えうる。
【００２０】
好ましい実施形態において、高信用コンポーネント及びセキュアトークンは、さらなる対話に先立って相互認証プロセスを実行する。
【００２１】
好ましい実施形態において、高信用コンポーネントは表示システムの一部分を形成する。例えば、表示システムは、主処理手段のみが高信用コンポーネントの機能を通して間接的にフレームバッファメモリにアクセスできるように、高信用コンポーネントが物理的及び機能的に主処理手段とフレームバッファメモリの間に配置されるように構成可能である。好ましくは、高信用コンポーネントは、デジタル署名動作を要約するデータを生成する手段をさらに含む。
【００２２】
本発明の他の態様及び実施形態は、以下の説明、特許請求の範囲及び図面から明らかになろう。
【００２３】
【発明を実施する最適な形態および産業的応用】
好ましい実施形態は、本出願人の同時継続出願中の欧州特許出願第９９３０１１００．６に記載の「高信用コンポーネント」の特徴のいくつかを最も便利に使用する高信用コンポーネントを利用する。この出願において、高信用コンポーネントは、ホストコンピュータの完全性メトリックを測定してこれを完全性メトリックの真値と比較し、ホストコンピュータの完全性をユーザまたは他のホストコンピュータに通知するように（するかどうかは別として）プログラムされたプロセッサを備えたハードウェアデバイスである。この高信用コンポーネントと本明細書における好ましい実施形態での高信用コンポーネントの間の重要な共通点は、次のようなことである。
・双方とも暗号化プロセスを用いるが、好ましくは暗号化プロセスに対して外部インタフェースを設けないこと。
・双方とも、少なくとも正規のユーザの知識なしでは、これらの動作を覆すことができないように、不正変更防止能力及び不正変更検出能力の両方を有すること。
・双方とも、取りつけられるホストコンピュータとは物理的及び機能的に独立した１つの物理的なハードウェアコンポーネントからなることが好ましいこと。

このような独立性は、高信用コンポーネントが自身に処理能力とメモリを有することによって達成される。

【００２４】

不正変更防止に関連する技術は、セキュリティの分野における当業者には周知である。これらの技術としては、不正変更に影響されないための方法（高信用デバイスの適切なカプセル化等）、不正変更を検出するための方法（仕様外の電圧、Ｘ線、高信用デバイスのケーシングにおける物理的な完全性の損失、等の検出）、及び不正変更が検出された場合にデータを消去する方法が含まれる。適切な技術のさらなる考察は、http://www.cl.cam.ac.uk/~mgk25/tamper.htmlに見られる。タンパープルーフィング（いたずら防止）が、本発明の最も望ましい特徴であるが、これは本発明の通常動作には含まれないため、本発明の範囲を越えたものであることが理解されよう。

【００２５】

この説明において「高信用」という用語は、物理的または論理的なコンポーネント、動作、またはプロセスに関連して用いられる場合、その振る舞いが様々な動作環境下で予測可能であり、かつ、外部要因、例えば破壊的なアプリケーションソフトウェア、ウィルス、物理的妨害等による干渉または破壊に対して高い耐性を有しているという意味を内包している。

【００２６】

本明細書で用いる「ホストコンピュータ」という用語は、少なくとも１つのデータプロセッサ、少なくとも１つの形態のデータ記憶装置、及びいくつかの形態の外部エンティティと対話するための通信能力とを有するデータ処理装置を指して用いており、この通信は、外部装置のような外部エンティティ、ユーザ及び他のコンピュータまたはその両方が、ローカルにあるいはインターネットを介して行うものである。「ホストコンピュータシステム」という用語は、ホストコンピュータ自体に加え、ホストコンピュータに取り付けられるキーボード、マウス、ＶＤＵ等の標準的な外部装置を含む。

【００２７】

本明細書で用いる「文書」という用語は、ホストコンピュータシステムを用いて視覚化することの可能なあらゆるデータの集合を含んでいる。通常、文書は契約書などのテキスト文書である。しかし、文書には、テキストだけでなく、あるいはテキストの代わりに、グラフィックまたはピクチャを含むこともできる。一般に、文書は単一ページまたは複数ページを含むことができる。

【００２８】

本明細書で用いる「ピクスマップ」という用語は、単色画像またはカラー（またはグレースケール）画像のいずれかを定義するデータを含むように広く用いられる。「ビットマップ」という用語は単色画像にのみ関連付けられ、例えば、ピクセルが「オン」であるか「オフ」であるかに応じて１または０にセットされる。これに対し、「ピクスマップ」はより総称的な用語であり、単色画像及びカラー画像を双方とも含み、この場合、カラー画像は最大で２４ビットが必要とされ、単一ピクセルの色合い、飽和度、及び強度を定義するためにはさらにそれ以上のビットが必要とされる。

【００２９】

後述で明らかにされるが、本明細書における好ましい実施形態による高信用コンポーネントは、安全なユーザインタフェースを提供し、特に、ホストコンピュータの表示機能の少なくともいくつかを制御する。本明細書における高信用コンポーネントには、本出願人の同時継続出願中の特許出願における高信用コンポーネントによる完全性メトリックを得ても得なくてもよいが、完全性メトリックの獲得は本明細書では考慮されない。

【００３０】

好ましい実施形態は本質的には、ユーザが、ユーザのスマートカードの秘密鍵または暗号化コプロセッサ等他の形態のセキュアトークンを用いて、ユーザがホストコンピュータ上に格納された文書にデジタル署名することを可能にする。署名は、画面で閲覧中の文書が実際にスマートカードが署名している文書である、という高度な信用をユーザに提供する

状況下で、ホストコンピュータの高信用表示プロセッサ（すなわち高信用コンポーネント）によって行われる。特に、スマートカードは、高信用画像データあるいは「シール」を収容する。この高信用画像データあるいは「シール」は、署名手続き中に安全な通信路を介してホストコンピュータへ渡され高信用コンポーネントによって表示される。これらは前記高信用画像の部分的な表示であって、通常ユーザ対して一意であり、前記高信用コンポーネントが署名動作を制御していることの信用をユーザに提供する。さらに、この好ましい実施形態においては、ホストコンピュータには、高信用表示プロセッサへ直接接続される高信用入力装置が設けられ、これによりユーザは、このホストコンピュータの他の機能によって妨害されることなく、ホストコンピュータと対話することができる。

【００３１】

さらに詳しくは、同様の効果を有した高信用表示プロセッサあるいは表示装置は、ホストコンピュータの標準ソフトウェアによって操作することの出来るデータだけでなく、ビデオ処理の段階にあるビデオデータへも関連付けられる。これにより、ホストコンピュータのソフトウェアによって干渉または改竄されることなく、高信用表示プロセッサはデータを表示表面に表示することができる。したがって、高信用表示プロセッサは、どの画像が現在ユーザに対して表示されているかを特定することができる。これは、ユーザが署名している画像（ピクスマップ）を明確に識別するために用いられる。これによる副次的な効果は、従来の特許出願の完全性メトリック、ユーザステータスメッセージ、プロンプト等を含むあらゆるデータを、高信用表示プロセッサが表示画面上に高い信用度で表示可能なことである。

【００３２】

図１は、好ましい実施形態によるホストコンピュータシステムを示しており、この図で、ホストコンピュータは、Ｗｉｎｄｏｗｓ　ＮＴ（登録商標）オペレーティングシステムの下で動作するパーソナルコンピュータすなわちＰＣである。図１によれば、ホストコンピュータ１００は、視覚表示ユニット（ＶＤＵ）１０５、キーボード１１０、マウス１１５、及びスマートカードリーダ１２０、及びローカルエリアネットワーク（ＬＡＮ）１２５に接続され、ＬＡＮ１２５は次にインターネット１３０に接続される。本明細書ではスマートカードリーダは独立したユニットであるが、キーボードの一部分を成すように一体化されてもよい。さらに、ホストコンピュータは、高信用入力装置を備える。この図では高信用スイッチ１３５がキーボードに一体化されている。ＶＤＵ、キーボード、マウス、及び高信用スイッチは、ホストコンピュータのヒューマン／コンピュータインタフェース（ＨＣＩ）として考えられる。特に、高信用スイッチ及びディスプレイは、信用のおける制御下で動作する場合、後述するように、「高信用ユーザインタフェース」として考えられる。図１は、後述する本実施形態で用いるためのスマートカード１２２も図示している。

【００３３】

図２は、図１のホストコンピュータのハードウェアアーキテクチャを示しており、この図において、ホストコンピュータ１００は、ＲＡＭ２０５とＲＯＭ２１０からなる主記憶装置へ接続された中央演算処理装置（ＣＰＵ）２００または主処理装置からなり、これらの構成要素のすべてはホストコンピュータ１００上のマザーボード２１５上に取り付けられている。この例では、ＣＰＵはＰｅｎｔｉｕｍ（登録商標）プロセッサである。ＣＰＵはＰＣＩ（Peripheral Component Interconnect）ブリッジ２２０を介して、ホストコンピュータ１００の他の主要なコンポーネントを取り付けるためのＰＣＩバス２２５に接続される。ＰＣＩバス２２５は、適切な制御部分、アドレス部分、及びデータ部分を含むが、これらについては本明細書において詳述しない。本発明の説明の範囲を越えるＰｅｎｔｉｕｍプロセッサ及びＰＣＩアーキテクチャの詳細な説明については、Hans-Peter Messmerによる書籍「The Indispensable PC Hardware Handbook」第３版（Addison-Wesley発行、ＩＳＢＮ０－２０１－４０３９９－４）を参照して欲しい。もちろん、本実施形態は決してＰｅｎｔｉｕｍプロセッサ、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステム、またはＰＣＩバスを用いての実施に限定されるものではない。

【００３４】

ＰＣＩバス２２５に取り付けられるホストコンピュータ１００のその他の主要なコンポーネントは、ＳＣＳＩバス２３５を介してハードディスクドライブ２４０及びＣＤ－ＲＯＭドライブ２４５へ接続されるＳＣＳＩ（Small computer system interface）アダプタと、ホストコンピュータ１００をＬＡＮ１２５に接続するためのＬＡＮ（ローカルエリアネットワーク）アダプタ２５０と、キーボード１１０・マウス１１５・及びスマートカードリーダ１２０を取り付けるためのＩＯ（入出力）装置２２５と、高信用表示プロセッサ２６０と、を含み、前記コンピュータ１００は、前記ＬＡＮアダプタを介してファイルサーバ、プリントサーバ、または電子メールサーバ等の他のホストコンピュータ（図示せず）及びインターネット１３０と通信できるようになっている。この高信用表示プロセッサは、以下で説明するように、すべての標準表示機能に加えてさらに複数のタスクを処理する。この標準表示機能は、あらゆる標準的なホストコンピュータ１００が通常有していると思われる機能であり、Ｗｉｎｄｏｗｓ　ＮＴ（登録商標）オペレーティングシステムの下で動作するＰＣについて言うならば、オペレーティングシステムまたはアプリケーションソフトウェアに関連する画像を表示するための機能である。ここで、キーボード１１０は、高信用表示プロセッサ２６０への直接接続されるだけでなく、ＩＯ装置２５５へも接続されている点に留意されたい。

【００３５】

主要なコンポーネントはすべて、特に高信用表示プロセッサ２６０は、ホストコンピュータ１００のマザーボード２１５上にまとめて設けられることが好ましいが、ＬＡＮアダプタ２５０及びＳＣＳＩアダプタ２３０はプラグインタイプであってもよい。

【００３６】

図３は、高信用表示プロセッサ２６０の好ましい物理的なアーキテクチャを示す。好ましい実施形態によれば、高信用表示プロセッサ２６０は、高信用コンポーネントの特徴を有するハードウェアコンポーネントであり、表示プロセッサの標準的な表示機能と、デジタル署名を生成するための追加的な非標準機能と、高信用ユーザインタフェースとを提供する。当業者には、これらの機能を代替として物理的に２つ以上の個別の物理的なコンポーネントへ分割できることが理解できるであろう。しかし、以下の説明を読めば、すべての機能を単一の高信用コンポーネントに統合することが、最も洗練された有用な解決策を提供することが分かるであろう。

【００３７】

図３によれば、高信用プロセッサ２６０は、

マイクロコントローラ３００と、

マイクロコントローラ３００の動作を制御するための各々の制御プログラム命令（ファームウェア）を含む不揮発性メモリ３０５、例えばフラッシュメモリと（別の方法としては、高信用表示プロセッサ２６０をＡＳＩＣ(特定用途向けＩＣ）で実施することも可能であり、この場合、通常大量生産よって高いパフォーマンスとコスト効率を提供するが、開発はさらに高価であり柔軟性は低い）、

高信用プロセッサ２６０をＰＣＩバスへ接続し、後述するように、ＣＰＵ２００から画像データ（すなわちグラフィックスプリミティブ）を受信すると共に、スマートカード１２２から高信用画像データも受信するためのインタフェース３１０と、

少なくとも１つの完全な画像フレーム（最大１６７０万色をサポートする１２８０×７６８のスクリーン解像度の場合、典型的なフレームバッファメモリ３１５の大きさは１～２メガバイトである）の格納に十分なＶＲＡＭ（ビデオＲＡＭ）を有するフレームバッファメモリ３１５と、

ピクスマップデータを、ビデオインタフェース３２５を介してビデオＤＡＣへ接続されてる（アナログ）ＶＤＵを動作させるためのアナログ信号へ変換するためのビデオＤＡＣ（デジタル／アナログコンバータ）３２０と、

高信用スイッチ１３５から信号を直接受信するためのインタフェース３３０と、

状態情報、特に受信した暗号鍵を格納すると共に、マイクロコントローラ３００に作業エリアを提供するための不揮発性メモリ３３５（例えばＤＲＡＭ（ダイナミックＲＡＭ）ま

たはもっと高価なＳＲＡＭ（スタティックＲＡＭ））と、
より詳細に後述するように、高信用表示プロセッサ２６０に暗号の識別機能、及び認証、完全性、信用度、及び再生攻撃からの保護、デジタル署名の作成、及び電子証明書の使用、を提供するように設けられたハードウェア暗号化アクセラレータ及びソフトウェア暗号化アクセラレータまたはその両方からなる暗号化プロセッサ３４０と、
高信用表示プロセッサ２６０の識別子I_{DP}（例えば、単純なテキスト文字列の記号）と、
高信用表示プロセッサ２６０の秘密鍵S_{DP}と、高信用表示プロセッサ２６０を署名公開鍵－秘密鍵の対及び機密の公開鍵－秘密鍵の対に結び付けると共に、高信用表示プロセッサ２６０の対応する公開鍵を含む、ＶｅｒｉＳｉｇｎ　Ｉｎｃ．等の第三者信用機関によって署名されて提供される証明書$Cert_{DP}$と、を格納する不揮発性メモリ３４５、例えばフラッシュメモリと、
から構成される。

【００３８】
証明書は通常このような情報を含むが、認証局（ＣＡ）の公開鍵は含まない。この公開鍵は、通常、「公開鍵インフラストラクチャ」（ＰＫＩ）を用いて利用できるようになる。ＰＫＩの動作は、セキュリティの分野の当業者にとって周知である。

【００３９】
証明書$Cert_{DP}$は、公開鍵の出所及びこの公開鍵が正当な公開鍵－秘密鍵の対の一部であることを第三者が信用できるような方法で、高信用表示プロセッサ２６０の公開鍵を第三者へ供給するために用いられる。ここで、第三者は、高信用表示プロセッサ２６０の公開鍵を事前に知る、または事前に取得する必要はない。

【００４０】
高信用表示プロセッサ２６０は、自身の識別と高信用プロセスをホストコンピュータへ提供し、また、高信用表示プロセッサは、不正変更防止能力、耐偽造性、及び耐偽作によってこれらの特性を有する。適切な認証機構を有する選ばれたエンティティのみが、この高信用表示プロセッサ２６０内で実行されているプロセスに影響を及ぼすことができる。ホストコンピュータの通常のユーザも、ネットワークを介してホストコンピュータに接続されるあらゆる通常ユーザまたはあらゆる通常のエンティティも、高信用表示プロセッサ２６０内で実行されているプロセスにアクセスまたは干渉することはできない。高信用表示プロセッサ２６０は、「不可侵な」特性を有する。

【００４１】
まず、高信用表示プロセッサ２６０は、ホストコンピュータ１００のマザーボードにインストールされた後、高信用表示プロセッサ２６０との安全な通信により、その識別、秘密鍵、及び証明書を用いて初期化される。証明書を高信用表示プロセッサ２６０へ書き込む方法は、スマートカードに秘密鍵を書き込むことによってスマートカードを初期化する方法に類似している。前記安全な通信は、信用できる第三者（及びホストコンピュータの製造業者）にのみ知られている「マスターキー」によって確保されており、このマスターキーは、製造時に高信用表示プロセッサ２６０へ書き込まれ、高信用表示プロセッサ２６０へのデータの書き込みを可能にするために用いられる。したがって、マスターキーを知らずに高信用表示プロセッサ２６０に対してデータを書き込むことは不可能である。

【００４２】
図３から明らかなように、フレームバッファメモリ３１５は高信用表示プロセッサ２６０自身によってのみアクセス可能になっており、ＣＰＵ２００からはアクセスできない。ＣＰＵ２００、もっと重大なものとしては破壊的なアプリケーションプログラムやウィルスが、高信用動作中にピクスマップを変更できないことが不可欠であるため、このことは好ましい実施形態の重要な特徴である。もちろん、ＣＰＵ２００がフレームバッファメモリ３１５に直接アクセス可能である場合であっても、ＣＰＵ２００がフレームバッファメモリ３１５にアクセスする可能性があるときに、高信用表示プロセッサ２６０が絶対的な制御を有するように構成されるならば、同じレベルのセキュリティを提供することは可能であろう。明らかに、後者の方式の方が実施するのは難しいと思われる。

【００４３】
次に、話の背景として、グラフィックスプリミティブがホストコンピュータ１００によって生成される典型的なプロセスについて説明する。まず、特定の画像を表示したいアプリケーションプログラムが、グラフィカルＡＰＩ（アプリケーションプログラミングインタフェース）を介してオペレーティングシステムに対して適切な呼び出しを行う。画像を表示する目的のため、ＡＰＩは通常、アプリケーションプログラムに対して、Ｗｉｎｄｏｗｓ　ＮＴ（登録商標）によって提供されているように、特有の基礎的な関数にアクセスするための標準的なインタフェースを提供する。ＡＰＩの呼び出しによって、オペレーティングシステムが各グラフィックスドライバライブラリルーチンを呼び出し、その結果、表示プロセッサ、この例では高信用表示プロセッサ２６０に特有のグラフィックスプリミティブが生成される。これらのグラフィックスプリミティブは、最終的にはＣＰＵ２００によって高信用表示プロセッサ２６０へ渡される。グラフィックスプリミティブの例としては、「ポイントｘからポイントｙまで太さｚで線を引く」または「ポイントｗ、ｘ、ｙ、ｚで囲まれた領域を色ａで塗りつぶす」等がありうる。
【００４４】
マイクロコントローラ３００の制御プログラムは、マイクロコントローラを制御して、受信したグラフィックスプリミティブを処理するための標準的な表示機能を提供する。具体的には次のように行われる：ＣＰＵ２００からグラフィックスプリミティブを受信し、これを処理して、ＶＤＵ１０５の画面に表示される画像を直接表すピクスマップデータを形成する。ここでピクスマップデータは、一般に、ＶＤＵ１０５の画面上でアドレス指定可能なピクセルの赤色ドット、緑色ドット、及び青色それぞれのドットに対する強度値を有する；このピクスマップデータをフレームバッファメモリ３１５へ格納する；定期的に、例えば１秒当たり６０回、フレームバッファメモリ３１５からピクスマップデータを読み出し、ビデオＤＡＣを用いてこのデータをアナログ信号へ変換し、このアナログ信号をＶＤＵ１０５に送信して、要求された画像を画面上に表示する。
【００４５】
標準表示機能以外に、制御プログラムは、ＣＰＵ２００からだまし取った表示画像データを高信用画像データと組み合わせて、単一のピクスマップを形成する機能を有する。さらに制御プログラムは、暗号化プロセッサ及び高信用スイッチ１３５との対話の管理も行う。
【００４６】
高信用表示プロセッサ２６０は、ホストコンピュータ１００の「表示システム」全体の一部を形成しており、その他の部分は通常オペレーティングシステムの表示機能であって、その他の部分は、アプリケーションプログラムにより「呼び出す」ことが可能になっていて、グラフィックスプロセッサ及びＶＤＵ１０５の標準表示機能へアクセスする。言い換えれば、ホストコンピュータ１００の「表示システム」は、画像を表示することに関係するあらゆるハードウェアまたは機能を含んでいる。
【００４７】
すでに述べたように、本実施形態は、高信用表示プロセッサ２６０とユーザのスマートカード１２２との間の対話に依存している。好ましい実施形態による使用に適したスマートカードの処理エンジンは、図４に示される。この処理エンジンは、データのデジタル署名及びどこか別の場所から受信した署名の検証を補助するために、標準的な暗号化及び復号化の関数を実行するためのプロセッサ４００を備える。本実施形態において、このプロセッサ４００は、内蔵型オペレーティングシステムを有し、ＩＳＯ７８１６－３、４、Ｔ＝０、Ｔ＝１、及びＴ＝１４規格に規定される非同期プロトコルを介して外部の世界と通信するよう構成される８ビットマイクロコントローラである。スマートカードはまた、不揮発メモリ４２０例えばフラッシュメモリを含み、この不揮発メモリは、スマートカード１２２の識別子I_{SC}、データにデジタル署名するのに使用される秘密鍵S_{SC}、及び第三者信用機関によって提供されこのスマートカードを公開鍵－秘密鍵の対に結び付けると共にスマートカード１２２の対応する公開鍵（高信用表示プロセッサ２６０の証明書$Cert_{DP}$

と同じ性質）を含む証明書$Cert_{SC}$を含む。さらに、スマートカードは、不揮発性メモリ４２０に「シール」データＳＥＡＬを含み、より詳細に後述するように、このシールデータは、プロセスがユーザのスマートカードを用いて安全に動作しているということをユーザへ示すために、高信用表示プロセッサ２６０によってグラフィックで表現される。好ましい実施形態において、シールデータＳＥＡＬは、一意の識別子としてユーザによって最初に選択された画像、例えばユーザ自身の画像のピクスマップの形態であり、周知の技術を用いてスマートカード１２２にロードされる。プロセッサ４００は、状態情報（受信した鍵等）を格納するため、及びプロセッサ４００にワークエリアを提供するために、揮発性メモリ４３０例えばＲＡＭへアクセスし、また、スマートカードリーダと通信するために、インタフェース４４０例えば電気的な接点へアクセスする。

【００４８】

シール画像は、ピクスマップとして格納される場合、比較的大量のメモリを使用する可能性がある。これは、記憶容量が比較的限られているスマートカード１２２に画像を格納する必要がある状況では、明らかに欠点となりうる。メモリ要件は、いくつかの異なる技術によって低減することができる。例えば、シール画像は次のものを含みうる：高信用表示プロセッサ２６０によって解凍できるように圧縮された画像；高信用表示プロセッサ２６０によって生成される反復モザイクの基本要素を形成するサムネイル画像；高信用表示プロセッサ２６０が単一の大きな画像として表示できるような、または上記のようにサムネイル画像として使用できるような英数字キャラクタ集合等の普通に圧縮された画像。あらゆる代替的方法において、シールデータ自体は暗号化形態であってもよく、表示可能になる前には、高信用表示プロセッサ２６０がデータを復号化する必要がある。あるいは、シールデータは、ホストコンピュータ１００またはネットワークサーバに格納されうる多くの画像のうち１つを識別する暗号化されたインデックスであってもよい。この場合、インデックスは、安全な通信路を介して高信用表示プロセッサ２６０によって取り込まれ、正しい画像を取得して表示するために復号化される。さらに、シールデータは、画像を生成するために、適切にプログラムされた高信用表示プロセッサ２６０によって解釈することができる命令（例えば、ＰｏｓｔＳｃｒｉｐｔ（登録商標）命令）を含むこともできる。

【００４９】

図５は、高信用署名動作を実施する状況におけるホストコンピュータ１００、高信用表示プロセッサ２６０、及びスマートカード１２２の機能間の論理的な関係を示す。高信用署名動作に関わるプロセスを明確に表現するため、ホストコンピュータ１００内への論理的な分離から離れ、表示プロセッサ２６０またはスマートカード１２２の各機能が物理的なアーキテクチャから独立して表現されている。さらに、「標準表示機能」は、高信用機能から線ｘ－ｙによって分けられ、この線の左側にある機能は高信用機能であることを明示している。図において、機能は楕円で表され、機能が作用する「不変の」データ（署名処理中の文書画像を含む）はボックスで示される。単に明確化したいという理由から、状態データまたは受信された暗号鍵等の動的データは図示されない。楕円間及び楕円とボックスの間の矢印は、それぞれ論理的な通信路を表す。

【００５０】

図５によれば、ホストコンピュータ１００は次のものを含みうる：文書への署名を要求するアプリケーションプロセス５００、例えばワードプロセッサプロセス；文書データ５０５；オペレーティングシステムプロセス５１０；アプリケーションプロセス５００から表示呼び出しを受信するためのＡＰＩ５１１プロセス；キーボード１１０からアプリケーションプロセス５００への入力を提供するためのキーボードプロセス５１３；マウス１１５からアプリケーションプロセス５００への入力を提供するためのマウスプロセス５１４；ＡＰＩプロセス５１１を介してアプリケーションプロセスから受信した呼び出しに基づいてグラフィックスプリミティブを生成するためのグラフィックスプリミティブプロセス５１５。ＡＰＩプロセス５１１、キーボードプロセス５１３、マウスプロセス５１４、及びグラフィックスプリミティブプロセス５１５は、オペレーティングシステムプロセス５１０の最上部に構築され、オペレーティングシステムプロセス５１０を介してアプリケーシ

ョンプロセスと通信する。

【００５１】

ホストコンピュータ１００の残りの機能は、高信用表示プロセッサ２６０によって提供される機能である。これらの機能は次のものを含む：高信用表示プロセッサ２６０のすべての動作を統合させるため、及びグラフィックスプリミティブプロセスからグラフィックスプリミティブを受信するため、及びアプリケーションプロセス５００から署名要求を受信するための制御プロセス５２０；制御プロセス５２０からの要求に応答して文書署名手順を表す署名された要約を生成するための要約プロセス５２２；スマートカード１２２からピクスマップのデジタル署名を取得するための署名要求プロセス５２３；スマートカード１２２からシールデータ５４０を取得するためのシールプロセス５２４；要約プロセス５２２、署名要求プロセス５２３、及びシールプロセスによって要求された呼び掛け／応答及びデータ署名タスクを行うため、スマートカード１２２との対話を行うスマートカードプロセス５２５；格納されているピクスマップデータ５３１を読み出し、このピクスマップデータを署名要求プロセス５２３へ渡すように署名要求プロセス５２３によって要求された場合、これを行うためのピクスマップ読み出しプロセス５２６；制御プロセス５２０から受信したグラフィックスプリミティブ及びシール画像データに基づいてピクスマップデータ５３１を生成するためのピクスマップ生成プロセス５２７；ピクスマップデータを読み出してこれをアナログ信号へ変換し、変換した信号をＶＤＵ１０５へ送信するための画面リフレッシュプロセス５２８；高信用スイッチ１３５がユーザによって起動されたか否かを監視するための高信用スイッチプロセス５２９。スマートカードプロセス５２５は、高信用表示プロセッサの識別データI_{DP}、秘密鍵S_{DP}データ、及び証明書$CERT_{DP}$データ５３０へアクセスできるようになっている。実際に、スマートカード及び高信用表示プロセッサは、標準的なオペレーティングシステムの呼び出しを介して互いに対話する。

【００５２】

スマートカード１２２は、シールデータ５４０と、高信用表示プロセッサ２６０と対話して呼び掛け／応答及びデータ署名タスクを行うための表示プロセッサプロセス５４２と、スマートカード識別データI_{SC}・スマートカード秘密鍵データS_{SC}・スマートカード証明書データ$Cert_{SC}$５４３と、を有する。

【００５３】

次に、図１～５に示す構成を用いて文書に署名するための好ましいプロセスについて、図６の流れ図を参照して説明する。まず、ステップ６００において、ユーザはアプリケーションプロセス５００を制御して、文書にデジタル署名するための「署名要求」を起動する。アプリケーションプロセス５００は、専用ソフトウェアプログラム、あるいはＭｉｃｒｏｓｏｆｔ　Ｗｏｒｄ等の標準的なワードプロセッサのパッケージへの追加、例えばマクロ等、によって実現することができる。いずれの場合であっても、署名要求またはアプリケーションプロセス５００はどちらも安全である必要はない。ユーザが署名要求を開始するとき、画面全体がすでに署名された文書で満たされていないならば、ユーザは署名したい文書の指定も行う。例えば、この署名したい文書は、画面全体の領域の一部に表示される場合もあれば、特定のウィンドウに表示される場合もある。画面上の特定エリアの選択は単純なタスクであり、（ＷＩＭＰ環境を用いた）いくつかの方法、例えばある領域を画定するユーザ定義のボックスを描画すること、あるいは単に座標を指定することによって、達成することができる。

【００５４】

次に、ステップ６０２において、アプリケーションプロセス５００は、画面上の（画定されたエリアまたはウィンドウ内に）表示されている画像に署名するため、制御プロセス５２０を呼び出し、制御プロセス５２０はこの呼び出しを受信する。これと同時に、図示されていないが、制御プロセス５２０は、グラフィックスプリミティブプロセスから任意のグラフィックスプリミティブを受信し、これをピクスマップ生成プロセス５２７へ転送する。文書に署名するためのアプリケーションプロセス５００からの呼び出しは、文書のエッジの座標（ａ、ｂ、ｃ、ｄ）を含む。この座標の送信によって、画面の表面全体、ある

完結したウィンドウ、または画面の任意の部分等に広く署名できるようになることに留意して欲しい。次に、アプリケーションプロセス５００は、制御プロセス５２０が画像の署名を返すのを待つ。

【００５５】

署名要求に応答し、ステップ６０４において、制御プロセス５２０は、要求時からプロセスが完了するまで、強制的に署名する画像を「スタティック（静的）」にする。ここで、「スタティック」とは、文書画像が高信用表示プロセッサ２６０以外によっては変更不可能なことを意味する。これにより、ユーザは、署名処理中常に、自身が見ているものが署名してるものであると確信を得ることができる。本実施形態では、制御プロセス５２０は、それ以上のグラフィックスプリミティブを「受け付けない」すなわち処理しないことによって、「スタティック」表示を達成する。状況によっては、グラフィックスプリミティブプロセス（またはその均等物）は、制御プロセス５２０がさらなるグラフィックスプリミティブを受信できるよう準備されるまで、グラフィックスプリミティブを「バッファリング」してもよい。他の状況によっては、署名される画像のグラフィックスプリミティブを単純に失われてもよい。文書画像が全画面を満たしている場合、画像をスタティックにすることは、単にいずれのグラフィックスプリミティブも処理しない場合である。しかし、署名する画像が全画面の一部分、例えばウィンドウのみを形成する場合、制御プロセス５２０は、受信したグラフィックスプリミティブが「スタティック」領域に影響するか否かを決定し、影響するものを拒絶する必要がある。このようにして、フレームバッファメモリ３１５内のスタティック文書画像のピクスマップは、この文書画像がスタティックである間、グラフィックスプリミティブプロセスからのあらゆる命令、またはＣＰＵ２００上で実行されている他のあらゆるプロセスによって変更されないよう保持される。

【００５６】

いったん文書画像がスタティックになると、ステップ６０６において、図１０ｃを参照してより詳細に後述するように、制御プロセス５２０は、署名する文書をハイライトするようにピクスマップを修正するため、アプリケーションプロセス５００によって提供される座標（ａ、ｂ、ｃ、ｄ）を含めた呼び出し命令をピクスマップ生成プロセス５２７へ送る。次に、ステップ６０８において、スマートカードプロセス５２５が判定を行ったときに、スマートカード１２２がまだスマートカードリーダ１２０に挿入されていないと判定された場合には、制御プロセス５２０は、ユーザにスマートカード１２２を挿入するよう求めるグラフィックメッセージを表示するようピクスマップ生成プロセスへ命令する。このメッセージには、１０秒のカウントダウンタイマＣＯＵＮＴが付加される。スマートカード１２２を受け取らなかった結果、カウントダウンタイマが切れる（すなわち、ゼロに達する）と、ステップ６１４において、制御プロセスは署名動作をキャンセルし、例外信号をアプリケーションプロセス５００へ返す。これに応答し、ステップ６１６において、アプリケーションプロセス５００は適切なユーザメッセージを表示する。スマートカード１２２が時間内に挿入される場合、またはすでに存在していた場合、プロセスは継続する。

【００５７】

次に、ステップ６１８において、制御プロセス５２０はシールプロセス５２４を呼び出し、シールプロセス５２４はスマートカードプロセス５２５を呼び出し、スマートカード１２２からシールデータ５４０を取得する。追加的に、制御プロセス５２０は、ピクスマップ生成プロセス５２７を呼び出し、ユーザにシールデータ５４０の回復を試行中であることを示す別のメッセージを表示することもできる。ステップ６１８及び６２０において、高信用表示プロセッサ２６０のスマートカードプロセス５２５及びスマートカード１２２の表示プロセッサプロセス５４２が、相互認証を行うために周知の「呼び掛け／応答」技術を用いて対話を行い、シールデータ５４０をスマートカードから制御プロセス５２０へ返す。次に、この相互認証プロセス及びシールデータ５４０の受け渡しの詳細について、図７を参照して説明する。

【００５８】

図７によれば、スマートカードプロセス５２５は、シールデータＳＥＡＬ５４０を返送し

てもらうための要求ＲＥＱ１をスマートカード１２２へ送信する。表示プロセッサプロセス５４２はナンスR_1を生成し、これをスマートカードプロセス５２５への呼びかけのときに送信する。スマートカードプロセス５２５はナンスR_2を生成し、これをナンスR_1と連結し、連結$R_1 \| R_2$をスマートカードの秘密鍵で署名して署名sS_{DP}（$R_1 \| R_2$）を生成し、連結$R_1 \| R_2$、署名sS_{DP}（$R_1 \| R_2$）、及び証明書$Cert_{DP}$をスマートカード１２２の表示プロセッサプロセス５４２へ返す。表示プロセッサプロセス５４２は、証明書$Cert_{DP}$から高信用表示プロセッサ２６０の公開鍵を抽出し、これをナンスR_1及び署名sS_{DP}（$R_1 \| R_2$）に用いて、連結$R_1 \| R_2$と比較することにより認証し、シール要求が所望の高信用表示プロセッサ２６０からきたものであること、及び高信用表示プロセッサ２６０がオンラインであることを確認する。ナンスは、古くから繰り返される信用できないプロセスより引き起こされる本物の署名を用いた不正（「再生攻撃」と呼ばれる）から、ユーザを保護するするために用いられる。

【００５９】

次に、スマートカード１２２の表示プロセッサプロセス５４２は、R_2をそのスマートカードのシールデータＳＥＡＬ５４０と連結し、秘密鍵S_{SC}を用いて連結$R_2 \| SEAL$に署名して署名sS_{SC}（$R_2 \| SEAL$）を生成し、秘密鍵S_{SC}を用いてシールデータＳＥＡＬ５４０を暗号化して暗号化シールデータ５４０sS_{SC}（ＳＥＡＬ）を生成し、ナンスR_2、暗号化シールデータsS_{SC}（ＳＥＡＬ）、署名sS_{SC}（$R_2 \| SEAL$）、及びスマートカードの証明書$Cert_{SC}$を、高信用表示プロセッサ２６０のスマートカードプロセス５２５へ送信する。スマートカードプロセス５２５は、証明書$Cert_{SC}$からスマートカードの公開鍵を抽出し、これを用いてナンスR_2及び署名sS_{SC}（$R_2 \| SEAL$）を検証し、暗号化シールデータ５４０sS_{SC}（ＳＥＡＬ）からシールデータＳＥＡＬ５４０を復号化し、最終的にこのシールデータＳＥＡＬ５４０を、シールプロセス５２４を介して制御プロセス５２０へ返す。

【００６０】

図６に戻り、ステップ６２２において、制御プロセス５２０はシールデータＳＥＡＬ５４０を受信すると、このデータをピクスマップ生成プロセス５２７へ転送し、図１０ｄを参照して後述するように、シール画像を生成し、これを用いて署名する文書をハイライトするように、ピクスマップ生成プロセス５２７へ命令する。次に、ステップ６２４において、制御プロセス５２０は、署名動作を続けたいか否かをユーザに尋ねるメッセージを表示するように、ピクスマップ生成プロセスへ命令する。このメッセージには、１０秒のカウントダウンタイマＣＯＵＮＴが付加される。ステップ６２６において、ユーザから応答を受信しなかった結果カウントダウンタイマが切れると、ステップ６２８において、制御プロセスは署名動作をキャンセルし、例外信号をアプリケーションプロセス５００へ戻す。これに応答して、アプリケーションプロセス５００は、ステップ６２９において、適切なユーザメッセージを表示する。ステップ６３０において、ユーザが、１０秒の時間期限内に高信用スイッチ１３５を起動することによって明示的に応答した場合、プロセスは継続する。継続の許可は、代替として、適当なレベルの認証が用いられるなれば、高信用スイッチ１３５を用いることによる方法だけではなく、信用度の低い通信路を介して、さらには適切なソフトウェアルーチンを用いることによっても提供することができる。あるいは、信用のおけるスマートカードが単に存在することで、署名を行うための十分な認証と成り得ると判断されるかもしれない。このような代替は、セキュリティポリシーの問題である。

【００６１】

次に、ステップ６３２において、制御プロセス５２０は、文書画像の署名を要求するように署名要求プロセス５２３へ命令し、署名要求プロセス５２３がピクスマッププロセス５２６を呼び出して、署名する文書のピクスマップデータのダイジェストを返すよう要求し、ピクスマップ読み出しプロセス５２６は各ピクスマップデータを読み出し、ハッシュアルゴリズムを用いてピクスマップデータのダイジェストD_{PIX}を生成し、このダイジェストを署名要求プロセス５２３へ返す。さらに、ピクスマップ読み出しプロセス５２６は「

表示フォーマットデータ」ＦＤを生成する。ＦＤには、後にピクスマップデータからテキストベースの文書を再構築するために必要とされる情報が含まれ（文書テキストを再構築する必要がない場合もあるため、ＦＤは必須ではない）、これを同様に署名要求プロセス５２３へ返す。例えば、この表示フォーマットデータＦＤには、「１０２４×７６８」等の画面上のピクセル数及びその割り当て、文書のテキストに用いられるフォントタイプ及びサイズ（文書がテキストベースの場合）等が含まれる（後述するように、少なくともこの情報のいくつかは、置換または追加として、文書の「要約」に含まれる可能性がある）。ステップ６３４及び６３６において、署名要求プロセス５２３は、周知の呼び掛け／応答プロセスを用いてスマートカード１２２の表示プロセッサプロセス５４２と対話し、文書の個々の署名を生成する。これについて、次に図８の流れ図を参照して詳細に説明する。

【００６２】

図８において、スマートカードプロセス５２５は、前記ダイジェストD_{PIX}及び表示フォーマットデータＦＤの署名を生成するため、スマートカード１２２に対して要求ＲＥＱ２を生成する。スマートカード１２２の表示プロセッサプロセス５４２は、ナンスR_3を生成し、これをダイジェストD_{PIX}及び表示フォーマットデータＦＤを返送してもらうための呼びかけと共にスマートカードプロセス５２５へ送信することによって、応答する。スマートカードプロセス５２５は、ダイジェストD_{PIX}を表示フォーマットデータＦＤ及びナンスR_3と連結し、この連結D_{PIX}‖ＦＤ‖R_3に署名して署名sS_{DP}（D_{PIX}‖ＦＤ‖R_3）を生成する。次に、スマートカードプロセス５２５は、連結D_{PIX}‖ＦＤ‖R_3及び各々の署名sS_{DP}（D_{PIX}‖ＦＤ‖R_3）をスマートカード１２２の表示プロセッサプロセス５４２へ送信する。表示プロセッサプロセス５４２は、高信用表示プロセッサの公開鍵（シールデータ５４０の交換においてすでに受信している）を用いて、高信用表示プロセッサの署名sS_{DP}（D_{PIX}‖ＦＤ‖R_3）及びナンスR_3を検証し、このダイジェストが現在の画像のダイジェストであることを証明する。表示プロセッサプロセス５４２は、秘密鍵を用いてピクスマップD_{PIX}のダイジェスト及び表示フォーマットデータＦＤに署名し、２つの署名sS_{SC}（D_{PIX}）とsS_{SC}（ＦＤ）をそれぞれ生成する。次に、スマートカードの表示プロセッサプロセス５４２は、署名されたダイジェストsS_{SC}（D_{PIX}）及び署名された表示フォーマットデータsS_{SC}（ＦＤ）を高信用表示プロセッサ２６０のスマートカードプロセス５２５へ返す。スマートカードプロセス５２５は、次に、スマートカードの公開鍵（シールデータ５４０の交換の結果すでにある）を用いてこのダイジェストD_{PIX}及び表示フォーマットデータＦＤを検証すると共に、スマートカードの署名を検証し、スマートカードがいまだにオンラインであることを証明する。

【００６３】

図６へ戻り、ステップ６３８において、高信用表示プロセッサ２６０のスマートカードプロセス５２５は、ピクスマップＰＩＸ、スマートカードのピクスマップダイジェストの署名されたものsS_{SC}（D_{PIX}）、及び表示フォーマットデータの署名されたものsS_{SC}（ＦＤ）を連結して画像の個々の署名ＰＩＸ‖sS_{SC}（D_{PIX}）‖sS_{SC}（ＦＤ）を形成し、署名要求プロセス５２３を介してこれを制御プロセス５２０へ返す。制御プロセス５２０は、この個々の署名をアプリケーションプロセス５００へ返す。次に、アプリケーションプロセス５００は、ステップ６４０においてこの個々の署名を格納し、ステップ６４２において署名動作を「要約する」ために、制御プロセス５２０へさらなる呼び出しを行うことによって応答する。要約の目的は署名を完了させることにあり、これについては、図９の流れ図及び以下の要約の例を参照して説明する。

```
1   TC-88503-00.01
2   Access time: Thu 06-May-1999,11:18
3   Pages: 2

4   Image01 | 560 x 414 (187,190) [1024 x 768]
5   -----署名始まり-----
6   PmftitUGoWZh6SLDgqQAvGZZY47Fp8wx5ZqE5HS8bGrSV3RD7LKw0kyXPY6yhGDpVNUc/R2
    +Gr4mm0LqS/twYuPdskyL4uk3no0w3LG2+f+/vzC4cKMPeY/LhbazZScvhK3CJ+apQxyikj
    cY5rTC563klovOPTBI/IyqZPxRnic=
7   -----署名終わり-----

8   Image02 | 670 x 379 (201,228) [1024 x 768]
9   -----署名始まり-----
10  UV1w5Rgr5F0iAjvUW4GP28NKAA+tOy42uBbP78JeQ5w20MI1afTYkSNtfn9VykYMPIfZLwM
    7ZZV+4fFttuSgOZI4n5iBkSEwtEj0z6ik/np6paq+0lGQZhhJCbq8OaX97Gmdg3AoBq4x+D
    hujmqkCJO+Dz6+x8kE24Z8YFXLPOI=
11  -----署名終わり-----

12  要約署名
13  -----署名始まり-----
14  ciZDZL2+41FsFci2cPjWFsfltkyXrfHBUM1kAEyudaZcVxD3XczTN7txSazInM2deJL9qnA
    een2DW1ZGjp1EESNkhoZXj0kT5TYNv2ylYFk0lSN+JVF09bmc9GdYLo/hSOWyYG/U29Mzqz
    ktaTdTqY/gPh1GajrSJGqRms+we/c=
15  -----署名終わり-----
```

【００６４】

ステップ６４４において、制御プロセス５２０は、画像の数（上記要約例では２つ）に加え、画像の個々の署名（例の６、１０行目）、高信用表示装置を識別するラベル（例の１行目）、現在時刻と日付（例の２行目）、及びこの要約自体の署名されたダイジェスト（例の１４行目）、を含む要約メッセージ全体を生成するために、要約プロセス５２２を呼び出す。各々の画像に対して、この要約は、ピクセル表現の画像サイズ（例えば画像１の場合５６０×４１４）、ピクセル表現の画面の原点からのオフセット（例えば画像１の場合１８７,１９０）、及びピクセル表現の表示解像度（例えば画像１の場合１０２４×７６８）も含んでいる。

【００６５】

次に、ステップ６４６において、要約プロセス５２２は、要約のダイジェストD_{SUM}を生成し、呼び掛け／応答プロセスを用いてスマートカード１２２と対話することにより要約ダイジェストD_{SUM}の署名を生成するために、高信用表示プロセッサ２６０のスマートカードプロセス５２５を呼び出す。これについては、次に図９を参照して説明する。

【００６６】

図９において、スマートカードプロセス５２５は、要約のダイジェストD_{SUM}の署名を生成するため、スマートカード１２２に対して要求REQ_3を生成する。スマートカードの表示プロセッサプロセス５４２はナンスR_4を生成し、要約のダイジェストD_{SUM}を返送してもらうための呼びかけの際に送信する。スマートカードプロセス５２５は、ダイジェストD_{SUM}をナンスR_4と連結し、この連結$D_{SUM} \| R_4$に署名して署名$sS_{DP}(D_{SUM} \| R_4)$を生成する。次に、高信用表示プロセッサ２６０のスマートカードプロセス５２５は、連結$D_{SUM} \| R_4$及び各々の署名$sS_{DP}(D_{SUM} \| R_4)$を表示プロセッサプロセス５４２へ送信する。次に、表示プロセッサプロセス５４２は、高信用表示プロセッサの公開鍵（シールデータ５４０の交換からすでにある）を用いて高信用表示プロセッサの署名及びナンスR_4を検証し、この要約が現在の要約であることを証明する。次に、表示プロセッサプロセス５４２が、秘密鍵を用いて要約のダイジェストD_{SUM}に署名し、署名されたダイジェスト$sS_{SC}(D_{SUM})$をスマートカードプロセス５２５へ送信する。高信用表示プロセッサ２６０のスマートカードプロセス５２５は、スマートカードの公開鍵を用いてこのダイジェストを検証すると共に、スマートカードの署名を検証し、スマートカードがいまだにオンラインであることを証明する。

【００６７】

図６へ戻り、ステップ６５２において、スマートカードプロセス５２５は、要約プロセス５２２を介して、署名された要約のダイジェストｓＳ$_{SC}$（Ｄ$_{SUM}$）と連結された要約ＳＵＭ（結果、連結ＳＵＭ‖ｓＳ$_{SC}$（Ｄ$_{SUM}$）を形成する）を制御プロセス５２０へ返し、制御プロセス５２０がこの要約ＳＵＭ‖ｓＳ$_{SC}$（Ｄ$_{SUM}$）をアプリケーションプロセス５００へ返す。ステップ６５４において、アプリケーションプロセス５００がこの要約を受信する。

【００６８】

格納もしくは他のエンティティへの送信のため、この個々の署名及び要約は、アプリケーションプロセス５００、または契約書の証明方法として本発明に記載している範囲以外の様々な方法でホストコンピュータ１００で実行されている任意の他のプロセスによっても、使用することができる。

【００６９】

最後に、ステップ６５６において、制御プロセス５２０が、文書画像に関連するグラフィックスプリミティブの受信及び処理を再開することにより画面の静止化を解除し、これによって実際に、画面の制御をアプリケーションアプリケーションプロセス５００または他のアプリケーションソフトウェアへ返す。別な方法として、ユーザが、典型的には別のユーザメッセージに応答して、再び高信用スイッチ１３５を起動するまで、制御がアプリケーションプロセス５００に戻されないようにすることも可能であり、この場合タイムアウト時間は設けられない。これによって、ホストコンピュータが標準の動作すなわち高信用でない動作へ戻る前に、ユーザにスタティック文書画像を見直すためのより多くの時間を与えることができる。

【００７０】

署名された文書を検証するためには、個々の署名ＰＩＸ‖ｓＳ$_{SC}$（Ｄ$_{PIX}$）‖ｓＳ$_{SC}$（ＦＤ）及び要約ＳＵＭ‖ｓＳ$_{SC}$（Ｄ$_{SUM}$）の双方が検証されなければならない。このような検証方法は、セキュリティの分野における当業者には周知である。例えば、ピクスマップのダイジェストに対する署名ｓＳ$_{SC}$（Ｄ$_{PIX}$）は公開鍵を用いて検証される。この公開鍵は、公的に入手可能であり、好ましくは認証局（ＣＡ）によって供給されるデジタル証明書Ｃｅｒｔ$_{SC}$内に含まれる。次に、検証されたダイジェストは、ピクスマップからダイジェストを再計算することによって得られる値と比較される。この場合、ダイジェストは標準的な周知の定義されたハッシュ関数を用いて生成される。この照合が正確に一致する場合、署名の検証は完了する。要約を含む他の署名についても同様の方法で照合される。

【００７１】

人が署名された文書の表現方法を検証できるようにするための好ましい方法は、ピクスマップを変換して画像内へ戻すことである。このためには、アプリケーション、実際には高信用表示プロセッサ２６０が、ピクスマップデータＰＩＸを各ホストコンピュータ１００のフレームバッファメモリ３１５内へロードする必要がある。これにより、署名者によって既に署名された文書を人が閲覧することができるようになる。

【００７２】

ここでは、署名する文書をハイライトする段階について、図１０ａ～１０ｄを参照して説明する。好ましい実施形態において、シールデータＳＥＡＬは、高信用画像のピクスマップからなる。例えば、図１０ａに示されるように、シールデータ５４０のピクスマップは、「スマイリーフェース」１０００を定義する。図１０ｂは、画面（図示せず）のウィンドウ１０１０内の例示的なこれから署名される文書Ｄｏｃ１の画像１００５を示す。ハイライトを行う最初のステップでは、画像がスタティックになった後であってシールデータを受信する前の段階で、高信用表示プロセッサ２６０が、図１０ｃに示すように、フレーム１０２０を文書画像１００５の周囲へ付加することによって、署名する文書をハイライトする。また、スマートカード１２２がない場合には、これもまた図１０ｃに示されるように、ユーザにスマートカードを挿入するよう求めるユーザメッセージ１０３０が、１０秒カウントダウンタイマ１０３５と共に表示される。次に、スマイリーフェースのピクスマップ画像がスマートカード１２２から取得されると、図１０ｄに示されるように、高信

用表示プロセッサ２６０が、スマイリーフェースの複数のインスタンス１０４５またはモザイクを用いてフレーム１０４０を装飾する。さらに、図１０ｄに示すように、高信用表示プロセッサ２６０は、署名プロセスを継続したいか否かをユーザに尋ねるさらなるユーザメッセージ１０５０を、１０秒カウントダウンタイマ１０５５と共に生成する。装飾されたフレーム１０４０は、ユーザに対して、適切なスタティック画像領域が選択されていることを示すと共に、高信用表示プロセッサ２６０が完全にその署名プロセスの制御中であることの高レベルの信用をユーザへ与える。また、ユーザ自身のシール画像の存在は、メッセージが、なにか別の（おそらく破壊的な）ソフトウェアアプリケーションまたはハードウェアデバイスからではなく高信用表示プロセッサ２６０からのものであるという信用をユーザに提供する。

【００７３】

図１０ｅ及び図１０ｇは、図１０ｃ及び図１０ｄに示される「フレーム」の視覚的作用の代替を示す。図１０ｅでは、４つの単一のシール画像１０６０が、アプリケーションプロセス５００によって提供される座標を用いてスタティック文書画像の角に配置され、スタティック画像領域を画定している。図１０ｆでは、このスタティック画像は、単一のシール画像を示すように背景を変更することで画定される。図１０ｇでは、スタティック画像は、シール画像のモザイクを示すように背景を変更することで画定される。当業者は、本発明の記載を鑑みて、静的画像をハイライトすることの可能な他の視覚的作用を思いつくことができるであろう。さらに、例えば、「現在、シールデータ５４０取得中．．．」、「現在、文書署名作成中．．．」等、署名動作中にさらなる状態メッセージを含めることが望ましいこともある。

【００７４】

高信用表示プロセッサ２６０には、シール画像及びメッセージを画面上の正しい場所に表示可能であることが要求されることが理解されよう。シール画像及びメッセージ画像は、署名プロセス中に現れその後は消失するという点において、明らかに一時的なものである。第１の画像を第２の画像で覆い、これによって第１の画像の一部を隠してから、第２の画像を除去し、その後第１の画像の隠された部分を復元するという周知の標準的な表示技術がある。このような技術は当然のこととして、通常のウィンドウ環境、例えば複数のウィンドウが互いに重なりあうよう環境において用いられる。高信用表示プロセッサ２６０は、シール画像及びメッセージ画像を標準ディスプレイに重ねるという目的のため、これらの標準技術の１つまたは複数を実施するように構成される。

【００７５】

状況によっては、文書が大きすぎてそのすべてが一度にＶＤＵ１０５の画面に収まりきらなくても、なお容易に読める場合がある。明らかに、本実施形態を実用的にするためには、ユーザが、署名する前にその文書を極めてはっきりと読めることが重要である。そのため、次に説明するように、文書を複数の画面ページに分割することも可能であり、この場合、各々のページが署名されて前のページの署名と暗号的に結び付けられることが必要とされる。

【００７６】

まず、アプリケーションプロセス５００が第１ページの画像を表示させ、上述したように、署名を行うため高信用表示プロセッサ２６０に対して呼び出しを行う。高信用表示プロセッサ２６０が、要約を要求する代わりに個々の署名を返すと、アプリケーションプロセス５００が高信用表示プロセッサ２６０に第２ページの画像を表示し、その画像に署名するよう命令する。明らかに、この場合、高信用表示プロセッサ２６０は、アプリケーションプロセス５００によるこのような要求を補助するように構成される。すべての画像が署名され、アプリケーションプロセス５００に返された後にのみ、アプリケーションプロセス５００は要約の要求を行う。そして、この要約は、上述の２ページの要約内に例示されるように、マルチページ文書において署名された画像の数を含む。

【００７７】

マルチページ文書の最初のページは単一ページと同じ方法で署名され、その結果個々の署

名が返される。しかし、署名を行うため後続する画像が存在する場合、高信用表示プロセッサ２６０は、先行する署名要求後に要約要求を受信しなかったことから、これらがマルチページ文書の一部であることを認識する。その結果、高信用表示プロセッサ２６０は、後続のページに署名を行うための許可を求める別のメッセージをユーザに対して表示する。これに応答して、マルチページ文書に署名中のユーザは、前述と同様の信用のおける許可された通信路（例えば、高信用スイッチ１３５）を用いて、このページが前のページに関連していること及びこれにも署名すべきであることを高信用表示プロセッサ２６０に対して承認する。高信用表示プロセッサ２６０がこのマルチページ承認を受信すると、以前に署名されたページの署名を現在のページのピクスマップと連結し、連結のダイジェストを作成し、これを署名のためスマートカードへ送信する。これは、現在のピクスマップだけのダイジェストの送信に代えて行われる。このプロセスは、後続のページを前のページに暗号的に「連鎖」させ、検出なしではページを再構成不可能なように、また検出なしでは中間ページを挿入または削除不可能なようにする。

【００７８】

最初のページの正当性は、単一ページとまったく同じ方法でチェックすることができる。後続ページの正当性は、現在のピクスマップのダイジェストが、連結された前の署名及び現在のピクスマップのダイジェストで置換されること以外は、単一ページの場合と同じ方法を用いてチェックすることができる。

【００７９】

後続のページを前のページに暗号的に連鎖させる多くの方法があることが理解されよう。これらの方法は、本説明の記載を鑑みて、セキュリティの分野における当業者には明白であろう。

【００８０】

さらにセキュリティを強化するため、マルチページ文書の各ページの画像は、従来のフッタ「ｘページ／ｙ」を含むように構成することができる。ここで、「ｘ」はページ番号であり、「ｙ」は総ページ数である。これは、単に文書を読むことで、なくなった文書を容易に検出できるようにする。

【００８１】

本発明の文書署名方式の大きな利点は、署名された文書が、再署名または副署名された文書であってもよいという点である。そのため、文書の要約は監査証跡を含むことが好ましい。再署名及び副署名に関しては多くの変形が存在するが、とは言え（明らかに）さらに署名する前に、電子的な完全性チェックを常に行うべきである。極端な例としては、新しい署名者が、各々の署名された画像について閲覧・承認・再署名を順に行い、効率的に元の署名を新しい署名に置きかえることが可能である。例えばこの方法は、あるユーザが、誰か別の人によってそのユーザのために用意した文書を署名する場合に用いられる。他の極端な例としては、新しい署名者が文書をまったく閲覧する必要がない場合、元の要約に署名することによって、元の署名を単に「十分検討せずに認可する」こともできる。これは、信用のおける従業員の成果を管理者が副署名するのに便利である。

【００８２】

再署名操作の場合、アプリケーションプロセス５００は再署名要求を発し、署名された文書（及び個々の署名と要約）を高信用表示プロセッサ２６０へ送信する。高信用表示プロセッサ２６０は、署名された文書を署名者の公開鍵を用いて検証し、文書（または文書の各ページの）のピクスマップを復元し、この検証された画像を、署名要求アプリケーションからの元の画像であるかのように、正しい順序で新しいユーザに対して表示する。ユーザは、例えば前述のように高信用スイッチ１３５を用いて個々の各画像の受け入れを承認し、新しいユーザが所有するスマートカードによって上述のように画像に署名させる。この結果、新しいユーザが所有するスマートカードにより署名されたことを除き、元の文書と同じ署名された文書が生成される。

【００８３】

同様に、副署名操作の場合、アプリケーションプロセス５００は、副署名要求を発し、署

名された文書（及び個々の署名と要約）を高信用表示プロセッサ２６０へ送信する。高信用表示プロセッサ２６０は署名された文書を検証し、検証された各画像を、アプリケーションプロセス５００からの元の画像であるかのように、正しい順序で新しいユーザに対して表示する。ユーザは、各々の個々の画像の受け入れを承認し、高信用表示プロセッサ２６０が、新しいユーザが所有するスマートカードを用いて元の要約に署名する。オプションとして、新しいユーザは、新しいユーザによって署名された前ユーザの公開鍵の証明書を提供し、後の署名の検証に関連する処理オーバヘッドを軽減する。

【００８４】

明らかに、再署名及び副署名の実施に関しては様々な変形があり、これらは本発明の記載に鑑みて当業者にとって明らかとされるであろう。

【００８５】

文書は署名、再署名、及び/または副署名の履歴を持つことが可能なため、本実施形態は、文書の要約の一部を形成する監査情報を便利に提供する。この監査情報は、文書の署名履歴を追跡できるようにする。この監査情報には、文書の以前の状態に関するデータ及び文書の新しい状態を生成するために新しいユーザによって行われた操作（行動）が含まれる。監査情報は、ユーザから独立していなければならないため、監査情報は高信用表示プロセッサ２６０によって署名される。監査情報には、常にあらゆる以前の要約情報（以前の署名者によるその要約情報の署名を含む）が含まれる。署名された文書が初めから作成された場合、高信用表示プロセッサ２６０の識別ラベルI_{DP}が監査ルートとして挿入される。また、監査情報は、新しいユーザによってどの個々の画像が閲覧されて承認されたか、及び、文書が初めから作成されたのかあるいは新しいユーザによって再署名または副署名されたかどうか、の指示も有することが好ましい。監査情報を含む要約を作成するため、スマートカードには、前記要約の内容だけのダイジェストではなく、前記要約の内容と連結した監査情報のダイジェストが送信される。残りのプロセスは、前述した通りである。

【００８６】

文書を署名するためのプロセスの拡張としては、ピクスマップデータに署名を行う前に、高信用表示プロセッサ２６０が可逆的圧縮アルゴリズムを用いてピクスマップを圧縮し、個々の署名の格納及び送信に関連するオーバヘッドを低減させる方法もある。

【００８７】

ピクスマップは、標準的な圧縮アルゴリズム、例えばＬＺ－１もしくはＬＺ－２圧縮を応用した符号語ベースのアルゴリズムによって圧縮することができる。あるいは、ピクスマップの圧縮に、ＯＣＲ（光学文字認識）に類似した技術を使用することもできる。この場合、状況は、従来のＯＣＲよりも低い解像度であるとはいえ、入力データが完全に「走査」される点において従来のＯＣＲとは異なる。ピクスマップのＯＣＲ圧縮されたものは、ピクスマップ用のアルファベットを生成するために「ＢＬＯＢマッチング」を用いて生成することができる。ピクスマップは、このアルファベットの各々の文字のピクスマップを構成し、メッセージが元のピクスマップを表現するように、これらの文字を用いてメッセージを形成する。このことは、ピクスマップが新しいアルファベットへ圧縮され、メッセージがこの新しいアルファベットで書かれる場合があるということを意味している。ピクスマップをそのアルファベットで書かれた新しいアルファベット及びメッセージに圧縮された可能性もあることを意味する。明らかに、このピクスマップデータには誤りも曖昧さも無いので、これは可逆圧縮方法である。

【００８８】

画像ピクスマップの大きさを小さくする別の方法は、この画像を純粋な黒と白で表現することである。この方法は、ピクセルが黒か白かを定義するために、０または１にセットされる単一ビットのみが必要される。別の状況では、文書画像は、各々のピクセルが通常最大２４ビットを必要としうるフルカラー画像として表現される。明らかに、この技術は、単純な白黒のテキストベースの文書に適している。しかし、カラーの文書または画像には適していない。

【００８９】
随時、文書画像は、ＯＣＲタイプのプロセスを用いて変換してテキストベースの文書へ戻され、文書の標準的なデジタルテキスト表現を再構築することができる。この技術は、テキストマッピングが不正確である可能性があるため、署名に使用することはできないが、続く機械処理のために標準的なデジタルテキスト表現（ＡＳＣＩＩ等）へ変換し戻すために、署名された文書の受信者が使用することはできる。好ましい実施形態では、高信用表示プロセッサ２６０は、ＯＣＲ文書の復元を行うために設けられる。
【００９０】
ＯＣＲを実施するため、ＯＣＲアルファベットが標準的な方法で生成され、次に、格納されているフォントと対応付けられ、これを基にして標準の文字集合へ変換される。従来のＯＣＲのように、対応の曖昧な文字はピクスマップのまま保持し、ユーザによる変換を行えるようフラグ設けることができる（これはめったに起こらない状況である。特にフォントタイプ及びサイズ情報が表示用形式のデータＦＤで供給されているならば、データに誤りがないため）。極度に注意する場合には、この再構築された文書全体は、署名者が署名することを意図する文書の見栄えに対して人間により手動でチェックされるべきである。好ましくは、すべての文書再構築プロセスは、信用のおけるプロセスによって行われる。
【００９１】
上述した好ましい実施形態は、フレームバッファメモリ３１５に格納されているビデオデータがオペレーティングシステムを含むホストコンピュータ１００のソフトウェアにより操作されうるポイントを超えて、高信用表示プロセッサ２６０がこのビデオデータに直接的及び専用のアクセスを有するという前提に基づいている。これは、高信用表示プロセッサ２６０が変更を行わない限り、ビデオデータが変更されないことを意味している。
【００９２】
すべてのコンピュータアーキテクチャがこのように構成されるわけではないことは理解されよう。例えば、コンピュータアーキテクチャによっては、フレームバッファメモリがメインメモリ（主記憶手段）の一部を形成するように設けられ、これによって単一アドレス空間（ＳＡＳ）表示システムを形成するものもある。このようなシステムの１つの利点は、ＣＰＵと表示プロセッサが両方ともフレームバッファメモリへアクセスすることができ、グラフィックス操作のオーバヘッドを共有することによって、グラフィックスパフォーマンスが向上することである。明らかに、このようなＳＡＳシステムで本発明を実施することは、ＣＰＵがメモリにアクセス出来てしまうため、署名中に安全であるという前提に基づかない。しかしながら、本発明を実施を提供するようにこのようなＳＡＳシステムを変更することのできる多くの方法がある。例えば、署名動作中にＣＰＵからのデータによってメモリが更新されないように、メモリに高信用表示プロセッサからの制御線を設けることができる。記憶装置自体は、この機能を実行するための特別な論理を備えるように変更されることが好ましい。あるいは、メモリへのアクセスは、別の論理回路をメモリの通常の制御パスに挿入することよってブロックされる。したがって、このようなシステムは、高信用表示プロセッサの許可がある場合にのみ、フレームバッファメモリ内のビデオデータを高信用表示プロセッサ以外によって変更できる、という変更された前提に基づく。明らかに、システムが真に安全である限り、この前提は最初の前提と同じくらい安全な動作に対して適切である。
【００９３】
他のアーキテクチャ、例えば単純なグラフィックス環境では、表示プロセッサの機能がオペレーティングシステム自体の一部を形成することも可能であり、これによって別個の表示プロセッサハードウェアを設ける必要がなくなる。明らかに、この場合、ＣＰＵにかかるグラフィックスオーバヘッドは、別個の表示プロセッサハードウェアを用いるシステムよりも大きくなり、これによってプラットフォームのグラフィックスパフォーマンスが制限される。明らかに、そのような状況では「高信用表示プロセッサ」を設ける余地はない。しかしながら、高信用表示プロセッサによって提供されるフレームバッファメモリを保護する機能、及びスマートカードと対話する機能と同等の機能は、署名中に表示システム

（いずれの形態であっても）を制御する適切な高信用コンポーネントを用いて実施できることが当業者には明白であろう。

【００９４】

本発明の他の実施形態では、高信用スイッチ１３５の機能をソフトウェアで置き換えることができる。高信用スイッチプロセス５２９が起動されると（ステップ６３０のように）、専用スイッチの動作を待つ代わりに、高信用コンポーネント２６０は、乱数発生能力を用いて文字列の形態でナンスを生成する。次に、この文字列は、「動作を承認するために＜文字列＞を入力して下さい」という形態のメッセージで、高信用ディスプレイに表示される。ここでアクションを承認するためには、ユーザがキーボード１１０を用いて与えられた文字列を入力しなければならない。この文字列は毎回異なり、他のソフトウェアはこの文字列に対するアクセスを持たないため（文字列は高信用プロセッサ３００とディスプレイの間のみでやり取りされる）、悪意のあるソフトウェアがこの承認プロセスを害することは不可能である。

【００９５】

本発明の他の実施形態では、付加的にまたは代替的に、高信用表示プロセッサ（または同等物）は、高信用ディスプレイを起動するためのインタフェースを備える。高信用ディスプレイは、例えば、ＬＣＤパネルディスプレイでありうる。高信用スイッチが高信用表示プロセッサとの対話のための高信用手段をユーザに提供するのと同様の方法により、高信用ディスプレイは、標準ＶＤＵを介する以外に、ユーザに情報をフィードバックするための高信用手段を提供することができる。例えば、高信用ディスプレイは、上述した署名動作に関連するユーザ状態メッセージを提供するのに使用することができる。ここで、ディスプレイは高信用表示プロセッサに直接接続される、またはある形態の高信用通信路を介して接続されるため、標準的なホストコンピュータで実行されているアプリケーションは、高信用ディスプレイにアクセス不可能であるべきである。本質において、このような高信用ディスプレイは、上述したいわゆる「高信用インタフェース」に対する追加である。実際には高信用ディスプレイは一つの例であり、他の形態の高信用フィードバック装置を追加あるいは代替として含められない理由はない。例えば、ある形態の高信用音声装置が可聴フィードバックを提供するのに有用であるということもありうる。

【図面の簡単な説明】

【図１】　本発明の好ましい実施形態による動作に適したコンピュータシステムを示す図である。

【図２】　本発明の好ましい実施形態による動作に適したホストコンピュータのハードウェアアーキテクチャを示す図である。

【図３】　本発明の好ましい実施形態による動作に適した高信用ディスプレイプロセッサのハードウェアアーキテクチャを示す図である。

【図４】　本発明の好ましい実施形態による動作に適したスマートカード処理エンジンのハードウェアアーキテクチャを示す図である。

【図５】　本発明の好ましい実施形態による動作に適した高信用ディスプレイプロセッサ及びスマートカードを備えるホストコンピュータの機能的アーキテクチャを示す図である。

【図６】　文書の個々の署名の生成に関わるステップを示す系統線図である。

【図７】　スマートカードからシール画像データを復元するための高信用ディスプレイプロセッサとスマートカードとの間のメッセージのシーケンスを示す図である。

【図８】　文書画像の署名を生成するための高信用ディスプレイプロセッサとスマートカードの間のメッセージのシーケンスを示す図である。

【図９】　文書画像署名プロセスの要約の署名を生成するための高信用ディスプレイプロセッサとスマートカードの間のメッセージのシーケンスを示す図である。

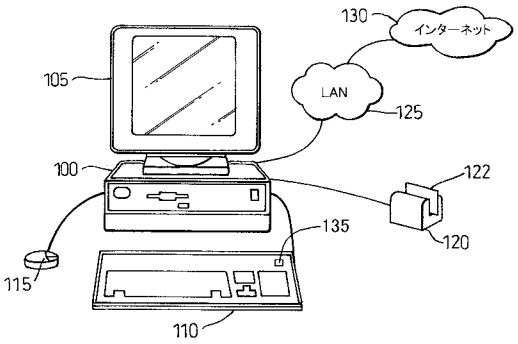
【図１０ａ】　例示的な高信用画像を示す図である。

【図１０ｂ～１０ｄ】　文書画像の署名における視覚的なステップを示す図である。

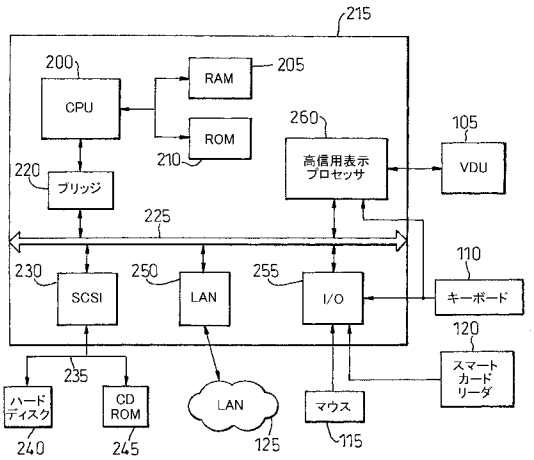
【図１０ｅ～１０ｇ】　署名される文書の画像をハイライトする代替方法を示す図である

。

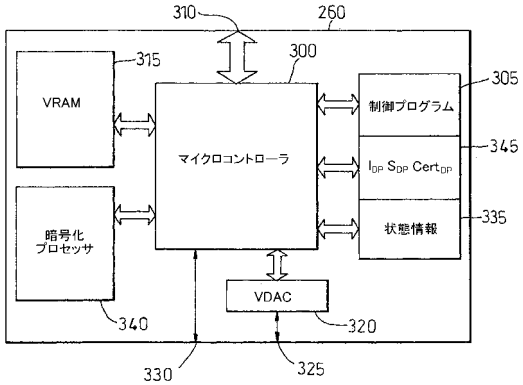
【図１】


130
インターネット
105
LAN
125
100
122
135
120
115
110

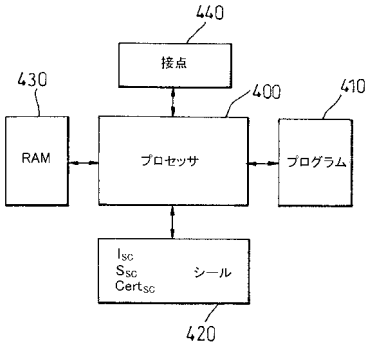
【図２】


215
200
CPU
RAM
205
ROM
210
260
高信用表示プロセッサ
105
VDU
220
ブリッジ
225
230
SCSI
250
LAN
255
I/O
110
キーボード
120
スマートカードリーダ
235
ハードディスク
240
CD ROM
245
LAN
125
マウス
115

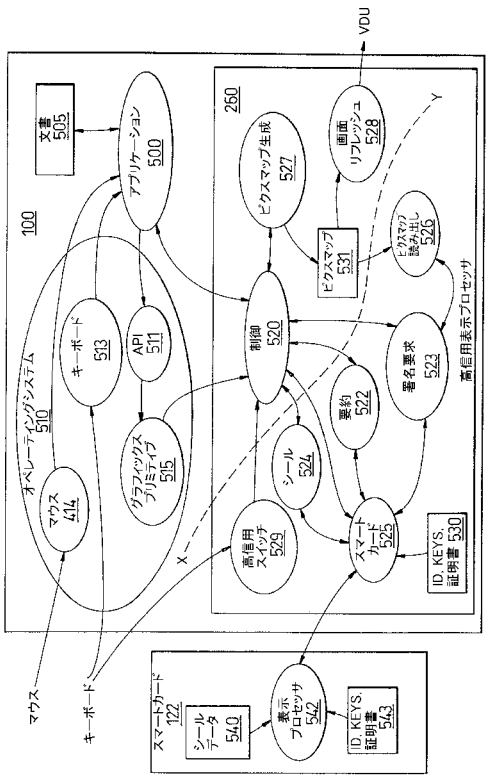
【図３】


310
260
315
300
VRAM
マイクロコントローラ
制御プログラム
305
I_{DP} S_{DP} $Cert_{DP}$
345
暗号化プロセッサ
状態情報
335
VDAC
340
320
330
325

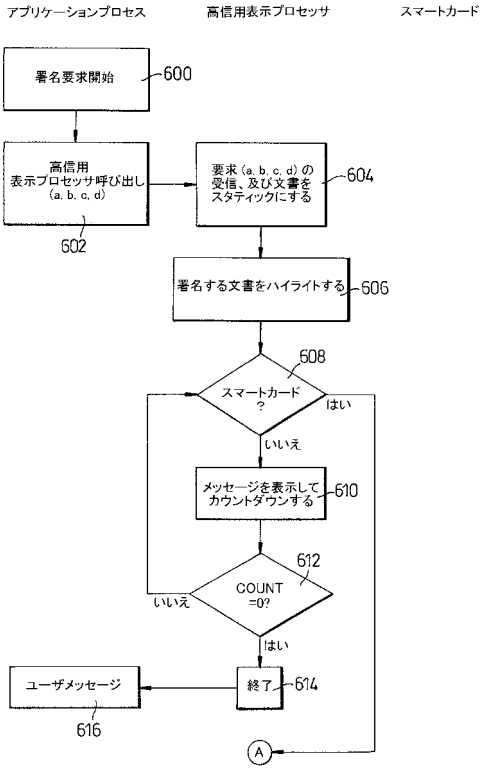
【図４】


440
接点
430
400
410
RAM
プロセッサ
プログラム
I_{SC}
S_{SC}
$Cert_{SC}$
シール
420

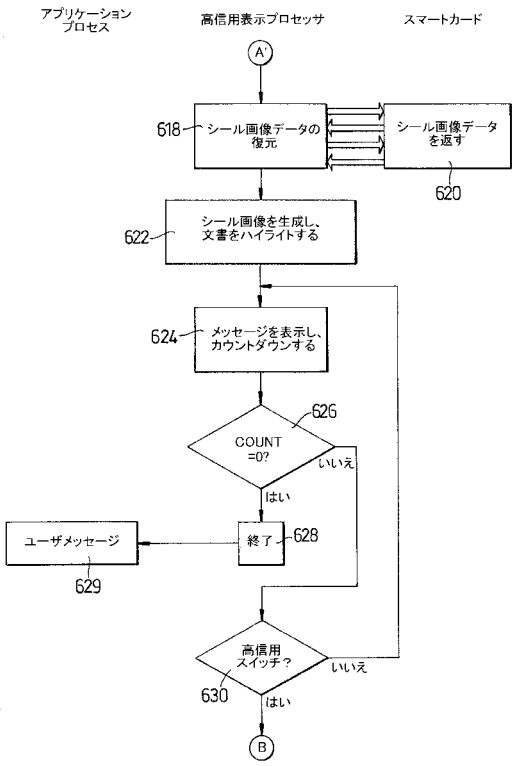
【図５】


VDU
100
オペレーティングシステム 510
アプリケーション 500
文書 505
API 511
キーボード 513
グラフィックス プリミティブ 515
マウス 414
250
ビクスマップ生成 527
画面 リフレッシュ 528
ビクスマップ 531
ビクスマップ読み出し 525
制御 520
署名要求 522
要約 522
シール 524
スマートカード 525
高信用スイッチ 529
ID, KEYS, 証明書 530
高信用表示プロセッサ
X
Y
マウス
キーボード
スマートカード 122
シールデータ 540
表示プロセッサ 542
ID, KEYS, 証明書 543

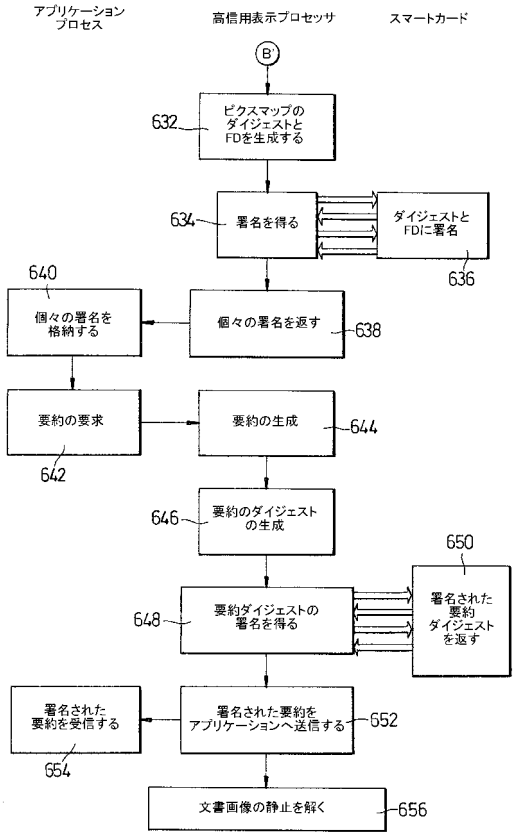
【図６】


アプリケーションプロセス
高信用表示プロセッサ
スマートカード
署名要求開始 600
高信用表示プロセッサ呼び出し (a, b, c, d) 602
要求 (a, b, c, d) の受信、及び文書をスタティックにする 604
署名する文書をハイライトする 606
スマートカード？ 608
はい
いいえ
メッセージを表示してカウントダウンする 610
COUNT =0? 612
いいえ
はい
終了 614
ユーザメッセージ 616
A

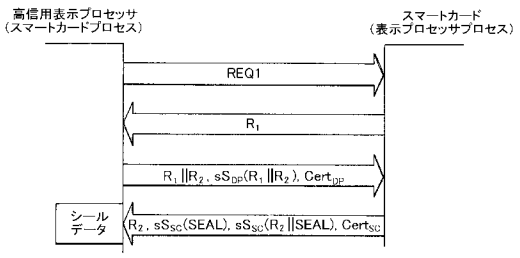
【図６－１】


アプリケーションプロセス
高信用表示プロセッサ
スマートカード
A'
シール画像データの復元 618
シール画像データを返す 620
シール画像を生成し、文書をハイライトする 622
メッセージを表示し、カウントダウンする 624
COUNT =0? 626
いいえ
はい
終了 628
ユーザメッセージ 629
高信用スイッチ？ 630
いいえ
はい
B

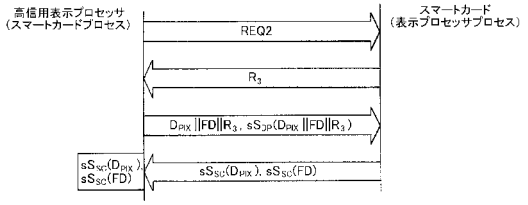
【図６－２】


アプリケーションプロセス
高信用表示プロセッサ
スマートカード
B'
ビクスマップのダイジェストとFDを生成する 632
署名を得る 634
ダイジェストとFDに署名 636
個々の署名を返す 638
個々の署名を格納する 640
要約の要求 642
要約の生成 644
要約のダイジェストの生成 646
要約ダイジェストの署名を得る 648
署名された要約ダイジェストを返す 650
署名された要約をアプリケーションへ送信する 652
署名された要約を受信する 654
文書画像の静止を解く 656

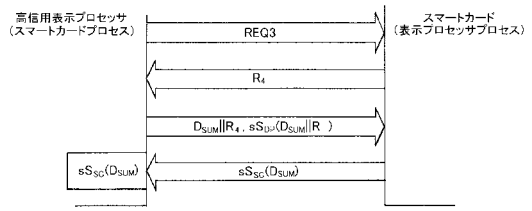
【図７】



【図８】



【図９】



【図１０ａ】

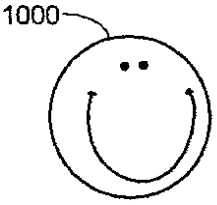
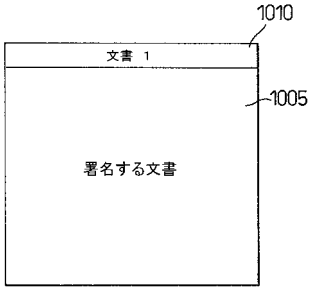
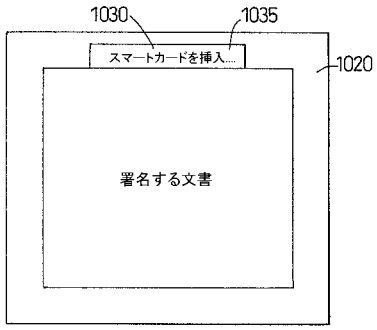


FIGURE 10a

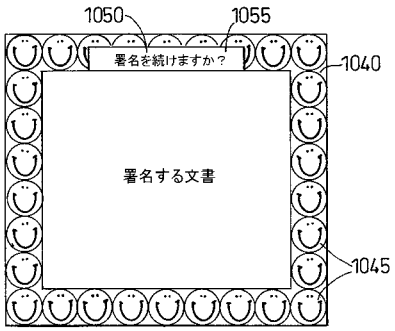
【図１０ｂ】



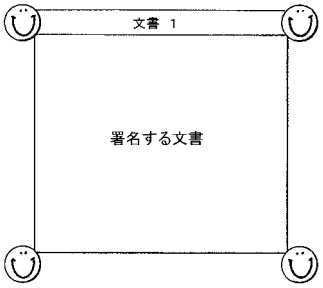
【図１０ｃ】



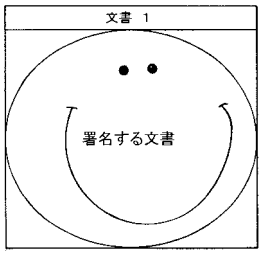
【図１０ｄ】



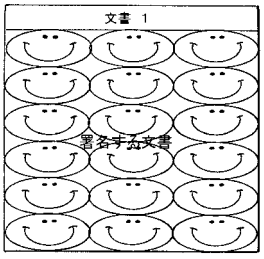
【図１０ｅ】



【図１０ｆ】



【図１０ｇ】



フロントページの続き

(72)発明者　プラウドラー，グレーム，ジョン
イギリス国ブリストル・ビーエス３４・８エックスキュー，ストーク・ガイフォード，タッチストーン・アベニュー・５
(72)発明者　バラチェフ，ボリス
イギリス国ブリストル・ビーエス８・４エルティー，ホットウェルズ，グランビィ・ヒル，ラットランド・ハウス・７
(72)発明者　チェン，リクン
イギリス国ブリストル・ビーエス３２・９ディーキュー，ブラッドレイ・ストーク，ハーベスト・クローズ・１

審査官　青木　重徳

(56)参考文献　特開平０６－０９５５９１（ＪＰ，Ａ）
特開平１０－１４３４３９（ＪＰ，Ａ）
特開平１０－２２４５８８（ＪＰ，Ａ）
特開平０８－１６０８５６（ＪＰ，Ａ）
特開平０８－００６８３６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/32
G09C　1/00
H04L　9/10