(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3877782号
(P3877782)
(45)発行日　平成19年2月7日(2007.2.7)　(24)登録日　平成18年11月10日(2006.11.10)

(51)Int.Cl.		F I		
H04L 29/04	(2006.01)	H04L	13/00	303Z
H04M 3/493	(2006.01)	H04M	3/493	
H04M 11/00	(2006.01)	H04M	11/00	302

請求項の数 16　(全 8 頁)

(21)出願番号	特願平10-541347
(86)(22)出願日	平成10年3月30日(1998.3.30)
(65)公表番号	特表2001-517396(P2001-517396A)
(43)公表日	平成13年10月2日(2001.10.2)
(86)国際出願番号	PCT/IB1998/000468
(87)国際公開番号	WO1998/044693
(87)国際公開日	平成10年10月8日(1998.10.8)
審査請求日	平成17年3月28日(2005.3.28)
(31)優先権主張番号	97650011.6
(32)優先日	平成9年4月1日(1997.4.1)
(33)優先権主張国	欧州特許庁(EP)

(73)特許権者
テレフオンアクチーボラゲツト　エル　エム　エリクソン
スウエーデン国エス―１２６　２５　ストツクホルム（番地なし）
(74)代理人
弁理士　浅村　皓
(74)代理人
弁理士　浅村　肇
(74)代理人
弁理士　林　鈺三
(74)代理人
弁理士　清水　邦明

最終頁に続く

(54)【発明の名称】機密保護データ通信のための方法および装置

(57)【特許請求の範囲】

【請求項１】

互いに離れているデータ処理システム（２、３）によって実行され、一つのシステムから機密保護チャンネル経由で他のシステムへ機密保護データを送信するステップを含むデータ通信方法（１）であって、さらに

データカテゴリーの識別、すなわち機密保護データか、一般データかの識別（３４）をシステムで行うステップと、

前記機密保護チャンネルから少なくとも一部は物理的に分離された一般チャンネル経由で前記システムから一般データを送信（３６）するステップと、

前記機密保護チャンネルおよび前記一般チャンネルを経由する機密保護データと一般データの双方を受信側システム（３）で受信して併合（４０）するステップとを含むことを特徴とする前記方法。

【請求項２】

請求項１記載の方法において、自動的にデータカテゴリを識別するための手段（５）を送信側システムに設けた前記方法。

【請求項３】

請求項２記載の方法において、送信側システム（２）が受信側システムから最初に受信したプログラム（３３）にしたがって自動的にデータカテゴリを認識する前記方法。

【請求項４】

前記請求項のいずれかに記載の方法において、終端点で一般チャンネルと対応する信号チ

ャンネルを前記機密保護チャンネルとした前記方法。
【請求項５】
請求項４記載の方法において、前記機密保護チャンネルの帯域幅を前記一般チャンネルよりも狭くした前記方法。
【請求項６】
前記請求項のいずれかに記載の方法において、前記受信側システムから前記送信側システムへ機密保護チャンネルアドレスを送信（３２）するステップを追加した前記方法。
【請求項７】
前記請求項のいずれかに記載の方法において、前記送信側システム（２）に接続された交換機（８）によって機密保護データと一般データの両方を受信し、前記交換機が通信リンク（２０）を経由する前記受信側システム（３）への経路指定を機密保護データのために行う方法。
【請求項８】
請求項７記載の方法において、前記交換機（８）が管理機能（２１）を経由する前記受信側システム（３）への経路指定を機密保護データのために行う前記方法。
【請求項９】
請求項８記載の方法において、前記交換機（８）が専用線（１１）を経由する前記管理機能（２１）への経路指定を機密保護データのために行う前記方法。
【請求項１０】
請求項８または９記載の方法において、前記管理機能（２１）が前記専用線（１３）を経由するシステムへの経路指定を機密保護データのために行う前記方法。
【請求項１１】
請求項７から９のいずれかに記載の方法において、交換機とシステムの間のプロトコルのアドレスとシステムで使用される遠隔データ処理システムアドレスとの相関を示すマトリクスが前記管理機能（２１）に含まれる前記方法。
【請求項１２】
前記請求項のいずれかに記載の方法において、前記機密保護チャンネルとしてＩＳＤＮ接続のＤチャンネルが含まれ、前記一般チャンネルとしてＩＳＤＮ接続のＢチャンネルが含まれる前記方法。
【請求項１３】
ユーザシステム（２）とリモートホストシステム（３）によって実行され、前記ユーザシステムから前記機密保護チャンネル経由で前記リモートシステムへ機密保護データを送信するステップを含むデータ通信方法であって、
前記機密保護チャンネルとしてＩＳＤＮ接続（７）のＤチャンネルが含まれ、
データのカテゴリ、すなわち機密保護データか一般データかがユーザシステムで識別され、
ユーザシステムからＩＳＤＮのＢチャンネル経由で一般データが送信され、ユーザシステムに接続されたデジタル交換機（８）が、非機密保護経路を経由する前記ホストシステムへの経路指定を一般データのために行うと共に、物理的に分離された通信リンクを経由する前記ホストシステムへの経路指定を機密保護データのために行い、
前記ホストシステムで機密保護データと一般データの両方を受信して、それらを併合することを特徴とする前記データ通信方法。
【請求項１４】
請求項１３記載の方法において、デジタル交換機（８）が管理機能（２１）を経由する前記ホストシステムへの経路指定を機密保護データのために行う前記方法。
【請求項１５】
請求項１４記載の方法において、前記ユーザシステムから要求される複数のホストシステムとの通信を可能にするアドレシングマトリクスが前記管理機能（２１）に含まれる前記方法。
【請求項１６】

機密保護チャンネル（７、２０）経由で遠隔データ処理システムに機密保護データを送信するための手段を有するデータ処理システム（２）であって、さらに
データのカテゴリ、すなわち機密保護データか一般データかを識別し、
少なくとも一部は前記機密保護チャンネルから物理的に分離されている一般チャンネル経由で一般データを送信する手段を含むことを特徴とする前記システム。

【発明の詳細な説明】

序論

発明の分野

本発明は機密保護チャンネル（ｓｅｃｕｒｅ　ｃｈａｎｎｅｌ）を介してデータ処理システム間で機密保護データ（ｓｅｃｕｒｅ　ｄａｔａ）の伝送を行うデータ通信に関するものである。ここで「機密保護データ」とは、部外者のアクセスから最大限に保護されるべき極秘データを意味する。

従来技術の説明

電話音声チャンネル、ファックス通信、あるいは電話でＤＴＭＦトーンを使用してクレジットカード番号などの機密保護データがごく日常的に伝送されている。この種の通信は限られた意味では有効である。例えば、２４時間自動オンラインバンキング用のＤＴＭＦ対話通信の使用は増加し続けている。このタイプの通信はかなり安全性が高いと考えられる。

しかしながら、このタイプの通信はかなり限定的なもので、ホストシステムにパーソナルコンピュータを接続したようなシステム、例えばインターネットサービスプロバイダーに接続したシステムで提供される範囲のサービスと柔軟性は望めない。

また、ＧＢ２１５４１０８（Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｐａｔｅｎｔｓ　Ｌｉｍｉｔｅｄ）に記載されているように機密保護データを同報システムで伝送することも知られている。この明細書に記載されている構成によれば、加入者は暗号化データ送信専用の機密保護チャンネルを選択し、自分の端末と機密保護チャンネルの一時接続を行う。そのチャンネルは暗号化キー通信用として使用される。システムはチャンネルセレクタと、機密保護チャンネル信号発生器と、先端部の機密保護チャンネル選択検出器を備えている。ユーザ側は受信機、チャンネルセレクタコントローラ、解読器、アルゴリズムメモリ、暗号器を備えている。このシステムでは、通信確立のために多くのシグナリングが伴い、また特別なハードウェアも必要である。また、伝送データの大半が必ずしも機密保護データであるとも限らない一般的な通信に必要な多様性は提供し得ないようである。

発明の概要

本発明は互いに離れているデータ処理システムによって実行されるデータ通信方法を提供する。これは、あるシステムが機密保護チャンネル経由で他のシステムへ機密保護データを送信するステップを含む方法であって、さらに
データカテゴリーの識別、すなわち機密保護データか、一般データかの識別をシステムで行うステップと、
機密保護チャンネルから少なくとも一部は物理的に分離された一般チャンネル経由で前記システムから一般データを送信するステップと、
機密保護チャンネルおよび一般チャンネル経由の機密保護データと一般データの双方を受信側システムで受信して併合（ｍｅｒｇｅ）するステップとを含むことを特徴とする。

このように、本発明のシステムでは機密保護データと一般データの両方を扱い、両タイプを同時に送信することができるので、柔軟性が大きくなる。また、シリアル通信に伴う遅延が生じないため、高速応答が得られる。したがって本発明によれば、例えば、インターネットアクセスプログラムを使用してサービスプロバイダーなどのリモートシステムにパーソナルコンピュータを接続することが可能であって、広範で柔軟性に富んだサービスが実現されると共に、機密保護経路を介した機密保護データ伝送が保証される。１回の通信セッションの間でも随時、受信および翻訳の各システムの役割を逆にすることが可能である。これにより、機密保護データの双方向通信が可能になる。

一実施例では、送信側システムは自動的にデータカテゴリを識別するための手段を含む。

一実施例では、送信側システムは受信側システムから最初に受け取ったプログラムにしたがって自動的にデータのカテゴリを認識する。
機密保護チャンネルは終端点で一般チャンネルに対応する信号チャンネルであることが好ましい。
一実施例では、機密保護チャンネルは一般チャンネルより帯域幅が狭い。
別の実施例の方法では更に、例えば一般チャンネル経由で受信側システムから送信側システムに機密保護チャンネルアドレスを送信するステップが含まれる。
一実施例では、送信側システムに接続された交換機で機密保護データと一般データの両方を受信し、交換機は通信リンクを経由する受信側システムへの経路指定を機密保護データのために行う。
一実施例では、交換機は管理機能を経由する受信側システムへの経路指定を機密保護データのために行う。
一実施例では、交換機は専用線を経由する管理機能への経路指定を機密保護データのために行う。
別の実施例では、管理機能は専用線を経由するシステムへの経路指定を機密保護データのために行う。
交換機とシステムの間のプロトコルのアドレスとシステムで使用される遠隔データ処理システムアドレスとの関連を示すマトリクスが管理機能に含まれることが好ましい。
一実施例では、機密保護チャンネルとしてＩＳＤＮ接続のＤチャンネルが含まれ、一般チャンネルとしてＩＳＤＮ接続のＢチャンネルが含まれる。
別のアスペクトにおいて、本発明はユーザシステムとリモートホストシステムによって実行されるデータ通信方法であって、ユーザシステムが機密保護チャンネル経由でリモートシステムへ機密保護データを送信するステップを含む通信方法を提供する。この通信方法は、
機密保護チャンネルとしてＩＳＤＮ接続のＤチャンネルが含まれること
データのカテゴリ、すなわち機密保護データか一般データかをユーザシステムで識別すること
ユーザシステムからＩＳＤＮのＢチャンネル経由で一般データを送信し、
ユーザシステムに接続されたデジタル交換機からホストシステムに対して、一般データを非機密保護経路経由で送信すると共に、機密保護データを物理的に分離された通信リンク経由で送信すること
機密保護データと一般データの両方をホストシステムで受信して、それを併合することを特徴とする。
一実施例では、デジタル交換機は管理機能を経由するホストシステムへの経路指定を機密保護データのために行う。
一実施例では、管理機能はユーザシステムから要求される複数のホストシステムとの通信を可能にするアドレシングマトリクスを備えている。
また、本発明は機密保護チャンネル経由で機密保護データを遠隔データ処理システムし送信するための手段を含むデータ処理システムを提供する。このデータ処理システムは、
データのカテゴリ、すなわち機密保護データか一般データかを識別するステップと、
少なくとも一部は機密保護チャンネルから物理的に分離されている一般チャンネル経由で一般データを送信するステップとを含むことを特徴とする。
発明の詳細な説明
本発明を更に明確に理解するため、以下に付図と単なる例示的実施例を用いて説明を行う。
図１はユーザシステムと、リモートホストシステムと、その両者間の通信方法を示す概要図。
図２は複数のリモートホストシステムと複数のユーザシステムの間で通信を可能にする方法を示す図。
図３は図１のユーザシステムの動作を説明する図。

データ処理・通信システム１が図１および図２に示されている。システム１は複数のユーザシステム２と、複数のリモートホストシステムを含む。この実施例において、リモートホストシステムはインターネットサービスプロバイダー３である。代替的に、互いに通信する二者のみを含むシステムであってもよい。
それぞれのユーザシステム２はデータプロセッサ５として従来のマイクロコンピュータデータプロセッサを含むと共に、この実施例では加入者通信回路６としてデジタルＩＳＤＮ回路を含んでいる。一般にデータプロセッサは請求書の支払い、オンラインバンキングの支払い等に通信が利用可能なようにプログラムされる。
このプログラムはデータのカテゴリ、すなわち機密保護データか一般データかを識別する。機密保護データはＩＳＤＮ回線７のＤチャンネル、一般データは従来のＢチャンネルで送信される。ＩＳＤＮ回線７で回路６とデジタル交換機８が接続される。交換機８は全く従来通りのものであり、Ｂチャンネルデータとは別個にＤチャンネル経由で送信されるデータの経路指定を行う。したがって、一般データはＩＳＤＮ回線７のＢチャンネルとインターネット経由で従来通りの方法で送信される。しかし、機密保護データはＩＳＤＮ回線７のＤチャンネルと、交換機８をサービスプロバイダー３に接続する通信ネットワークとを含む安全な経路で送信される。通信ネットワークリンクはインターネットリンクよりも安全性がかなり高い。
つぎに図３は、システム１によって実行される通信方式をフローチャートで図示している。ステップ３１で、データプロセッサ５はＩＳＤＮ回路６経由でサービスプロバイダー３からプログラムを受け取る。ステップ３２で、データプロセッサは更に、機密保護経路を介して機密保護データを送信するためにサービスプロバイダーの通信アドレスを受け取る。あるいは、このアドレスはサービスへの登録後に手紙か電話による連絡を受けた後、ユーザが自分のシステムに入力することも可能である。したがって、このとき使用される普通のインターネット通信アドレスに加えて、加入者データプロセッサ５はまた、機密保護データ通信に使用し得る通信アドレスを持っている。
ステップ３３で、プロセッサ５はユーザ入力データを受信し、サービスプロバイダー３からあらかじめ受信したプログラムを使用してそのデータを処理する。これらの入力データとして、例えば商品のオンラインショッピングに関連するものも含まれる。この例では、財務アカウントデータは機密保護データとみなすことができる。ステップ３４で、データプロセッサ５はデータ内の機密保護データフィールドを識別する。例えば、特定のフィールドで機密保護データを表し、残りフィールドで一般データを表すテンプレートをサービスプロバイダーから受け取り、これを利用して上記識別を行うことができる。あるいは、ユーザがデータ入力時にフラグを入力することによって機密保護データであることを示してもよい。重要な点は、データのカテゴリ、すなわち機密保護データか、一般データかをデータプロセッサ５によって識別することである。
プロセッサ５は、ステップ３５におけるＩＳＤＮのＤチャンネルを経由する機密保護データ伝送と、ステップ３６におけるＩＳＤＮのＢチャンネルを経由する一般データ伝送とを含むデータアップロードをサービスプロバイダー３に対して実行するためにＩＳＤＮ回路６の動作を指示する。Ｄチャンネルは呼設定や呼終了などに使用される狭帯域信号チャンネルである。しかしながら、このチャンネルには、極秘の財務キーデータまたは暗号化キーデータなどの機密保護データを挿入する程度の十分な帯域幅がある。
ステップ３７で、デジタル交換機５の中のフレームハンドラーはＤチャンネルの機密保護データを取り込む。
ステップ３８において一般データは従来通りの方法でインターネット１２へ経路指定される。交換機８とインターネット１２の第１ノード間の接続はダイヤルアップ接続で確立することができる。インターネット１２とサービスプロバイダー３間の最終接続には専用線１３を使用することができる。上記の最初と最後のリンクは安全性がかなり高いが、インターネット１２のノード経由で送信されるデータは通信ネットワークリンク経由で送信されるデータと比べて一般に安全性が低いと考えられる。しかし、機密保護データでなければ、これは問題にならない。

デジタル交換機８のフレームハンドラーはステップ３９において、通信リンク２０上のサービスプロバイダー３への機密保護データの経路指定を行う。これは物理的に分離された全く別個の経路である。
上記を達成する方法について、図２に従って詳細に述べる。この実施例では、通信リンクに管理機能２１が含まれる。管理機能２１は送信アイデンティティと端末終点識別子（ＴＥＩ）値の組み合わせを０と３６の間に設定する。管理機能２１は無制限な数のサービスプロバイダー３から最終的な宛先を選択するマトリクスを備えていて、専用線経由でそれを宛先に送信する。
交換機８とサービスプロバイダー３とのリンクは、機密保護データ用と一般データ用で完全に異なっている。最初にユーザシステムに送信される通信アドレスは管理機能マトリクスで適切なサービスプロバイダーを識別するために使用される。この経路は一般データ経路から独立して制御される。これは機密通信において非常に重要な意味を持っている。
図３のステップ４０で、サービスプロバイダー３は機密保護データおよび一般データを併合して必要なトランザクション処理を完了する。
別の実施例において、交換機フレームハンドラーはデータの管理機能２１への経路指定を行うための信号として特定値のＳＡＰＩ（Ｓｅｒｖｉｃｅ　Ａｃｃｅｓｓ　Ｐｏｉｎｔ　Ｉｄｅｎｔｉｆｉｅｒ）を認識する。このように、フレームハンドラーの動作は、さらに一般的なパケット交換構成と統合することが可能であって、その場合、管理機能２１を使用すべきか、Ｘ．２５ネットワークなどの一般的なパケット交換網を使用すべきかを決定するためにＳＡＰＩ値を利用することができる。多くの可能性があるが、重要な点は機密保護データが交換機で受信されるときに異なったチャンネルを経由するので分別処理が可能であり、物理的に分離された別のリンクを経由する宛先サービスプロバイダーへの経路指定をすることができる。これは、単に機密保護データを識別してＤチャンネルで送信するだけで達成される。交換機を変更する必要はない。
ユーザシステムとサービスプロバイダーの間で使用するものとして発明を記述したが、さらに一般的には、相互に機密保護データを送信する２つのデータ処理システムの間で実施することも考えられる。一つの例として、一般データの同報と機密保護データの送信を平行して実行することができる。その場合の機密保護データには同報信号を解読するためのコードまたはキーを含めることができる。
更に拡張して、機密保護チャンネルを双方向通信で使用することもできる。
また、ＩＳＤＮのＤチャンネル、Ｂチャンネル以外で、機密保護データおよび一般データ用の経路を使用することも考えられる。例えば、インターネット上で送信される一般データとは別に、機密保護データはダイヤルアップか専用線で送信することができる。
本発明は上記実施例に制限されず、また請求の範囲に応じて構成と詳細内容は変化する。

【図１】

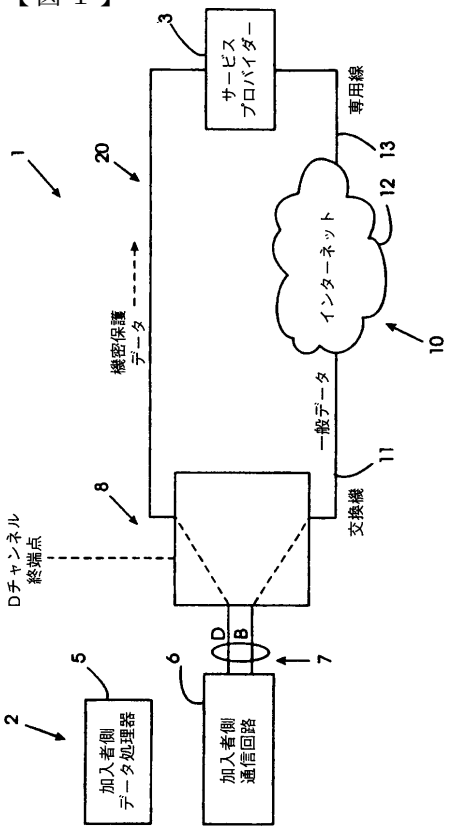

Fig. 1

【図２】

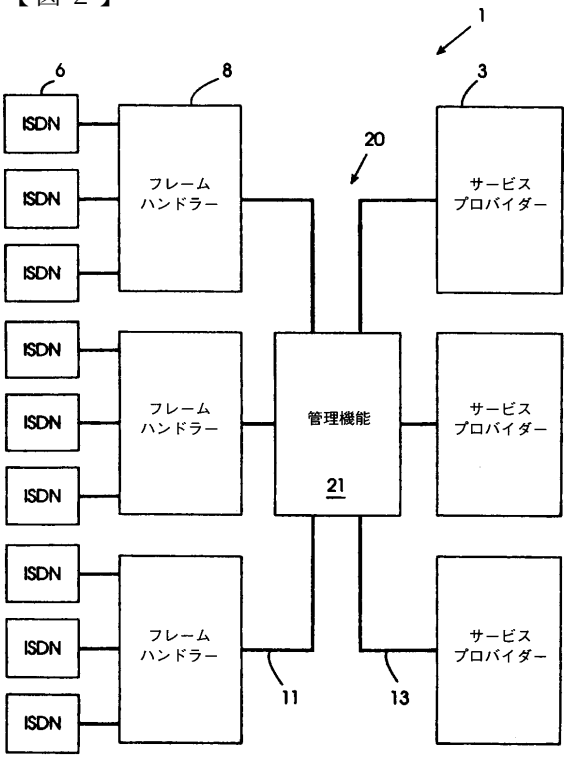

Fig. 2

【図３】

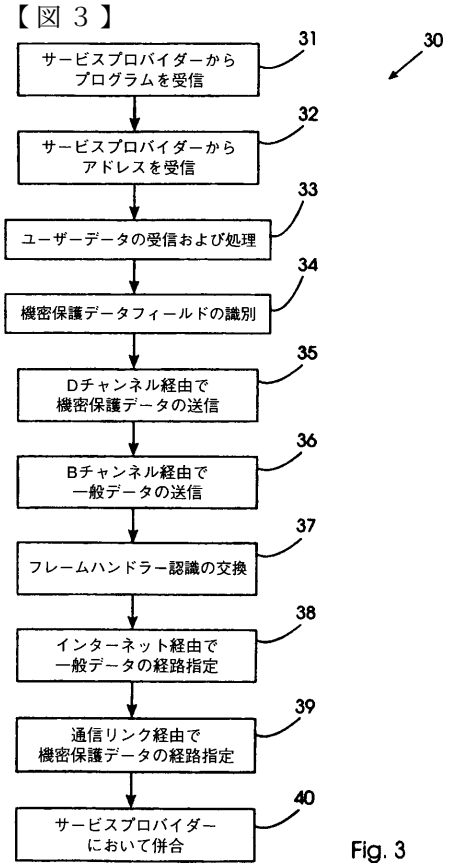

Fig. 3

フロントページの続き

(72)発明者　グルネル，オベ
アイルランド国，ダブリン　１４，チャーチタウン，ウッドローン　パーク　３

審査官　安藤　一道

(56)参考文献　欧州特許出願公開第５１１４９７（ＥＰ，Ａ１）
欧州特許出願公開第６０３５９６（ＥＰ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 29/04
H04M 3/493
H04M 11/00