【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年1月5日(2006.1.5)

【公表番号】特表2001-527333(P2001-527333A)
【公表日】平成13年12月25日(2001.12.25)
【出願番号】特願2000-526026(P2000-526026)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/16　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｈ０４Ｌ　9/00　６４３

【手続補正書】
【提出日】平成17年9月15日(2005.9.15)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ディジタル的にエンコードされたデータを配信する方法であって：
ａ）前記データを多数のフレームに分割することと；
ｂ）前記フレームをエンクリプトすることと；
ｃ）前記データフレームの多数のコピーを多数のユーザへ配信することであって、各フレームは制御フィールドと共に配信されるものと；
ｄ）キー生成のためのシード値を多数のユーザの各々のところに位置するそれぞれの安全保護モジュールへ通信することと；
ｅ）安全保護モジュールへ通信されたシード値から導き出されたキーを使用して各ユーザにおいてデータフレームをデコードすることであって、該安全保護モジュールは、前記制御フィールドが該安全保護モジュールへ送られているときのみ、それぞれのフレームの復号を可能にするように構成されているものと；
ｆ）選択された１以上のユーザにおいて、安全保護モジュールへ該制御フィールド内の制御メッセージを送ることと；
ｇ）該または各選択されたユーザにおいて、前記制御メッセージに応答して、前記シード値から生成されたキーの使用可能度を制御して、ユーザによる前記データへのアクセスを選択的に制御することと、を含む方法。
【請求項２】
各データフレームがフレーム識別フィールドを含み、安全保護モジュールによって生成された各キーが前記フィールドによって識別される１つのフレームに指定される請求項１に記載の方法。
【請求項３】
前記データの多数のコピーを配信するステップが、通信ネットワークを介して複数のユーザへデータパケットをマルチキャストすることを含む請求項１または請求項２に記載の方法。
【請求項４】
制御メッセージがデータフレームで多数のユーザに配信され、選択されたユーザまたは

ユーザグループを識別するユーザ識別フィールドが制御メッセージ内に含まれ、制御メッセージが、前記ユーザ識別フィールドによって識別されるユーザまたはユーザグループのみによって実行される請求項１ないし請求項３の何れか１項に記載の方法。

【請求項５】

制御メッセージが停止フラグを含み、停止フラグに応答して、該または各選択されたユーザにおけるキーの生成が停止される請求項１ないし請求項４の何れか１項に記載の方法。

【請求項６】

安全保護モジュールから制御メッセージの源へ応答信号を戻すことを含む請求項１ないし請求項５の何れか１項に記載の方法。

【請求項７】

制御メッセージが接触送信者フラグを含み、接触送信者フラグが設定されたときに、安全保護モジュールから応答信号を戻すステップが実行される請求項６に記載の方法。

【請求項８】

前記応答信号を受取ったときに、別の制御メッセージをユーザへ送ることを含む請求項６または請求項７に記載の方法。

【請求項９】

データ通信システム内の顧客端末を動作する方法であって：

ａ）顧客端末においてそれぞれが制御フィールドを有する多数のエンクリプトされたデータフレームを受取ることと；

ｂ）顧客端末においてキー生成のためのシード値を受取ることと；

ｃ）キー生成のための前記シード値を、顧客端末に位置する安全保護モジュールへ送ることと；

ｄ）安全保護モジュールにおいてデータフレームのデクリプションのためのキーをシード値を使用して生成することと；

ｅ）前記キーを使用して制御フィールドが受取られたそれぞれのデータフレームのみをデクリプトすることと；

ｆ）該制御フィールド内の受取った制御メッセージを前記安全保護モジュールへ送ることと；

ｇ）前記制御メッセージに応答して、前記シード値を使用して生成されたキーの使用可能度を制御し、それによって顧客端末のユーザによる顧客端末で受取られたデータへのアクセスを制御することと、を含む方法。

【請求項１０】

データ通信システムであって：

ａ）複数のフレームを出力するように構成された遠隔のデータ源と；

ｂ）複数のフレームをそれぞれ異なるキーでエンクリプトするためのエンクリプション手段と；

ｃ）それぞれが制御フィールドを有するエンクリプトされたデータフレームの多数のコピーを配信するように構成された通信チャンネルと；

ｄ）該制御フィールドを有するエンクリプトされたデータフレームのそれぞれのコピーを通信チャンネルから受取るように構成された多数の顧客端末と；

ｅ）顧客端末に位置し、データフレームをデクリプトするのに使用するシード値のキーから生成するようにプログラムされているキー生成装置と；

ｆ）キー生成装置に接続されたキー制御手段であって、

該制御フィールドを受取るインターフェイスと、

制御フィールドが受取られたそれぞれのフレームを復号化するためのキーのみをリリースするように構成された制御手段と、

該制御フィールド内の制御メッセージに応答して、シード値から生成されたキーのユーザに対する使用可能度を制御するように構成された制御手段と、を含むキー制御手段と；

ｇ）キー生成装置に接続され、通信チャンネルから顧客端末において受取られるデータフレームをデクリプトするように構成されたデクリプション手段と、
を含むデータ通信システム。
【請求項１１】
通信チャンネルがパケット交換データネットワークである請求項１０に記載のデータ通信システム。
【請求項１２】
請求項１ないし請求項１１の何れか１項に記載の方法において使用する顧客端末であって：
ａ）データ通信チャンネルへ接続するためのデータインターフェイスと；
ｂ）データフレームをデクリプトするときに使用するためのキーをシード値から生成するようにプログラムされたキー生成装置と；
ｃ）該データインターフェイスと該キー生成装置とに接続され、該データインターフェイスを介して受取られるデータフレームをデクリプトするように構成されたデクリプション手段と、
ｄ）該キー生成装置に接続されたキー制御手段であって、
制御フィールドを受取るためのインターフェイスと、
制御フィールドを有する受取られたそれぞれのデータフレームをデクリプトするためのキーのみをリリースするように構成された制御手段と、
該制御フィールド内の制御メッセージに応答し、シード値から生成されるキーのユーザに対する使用可能度を制御するように構成された制御手段と、を含むキー制御手段と、
を含む顧客端末。
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図２
【補正方法】変更
【補正の内容】

【図２】