【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19年3月29日(2007.3.29)

【公表番号】特表2003-527782(P2003-527782A)
【公表日】平成15年9月16日(2003.9.16)
【出願番号】特願2001-528775(P2001-528775)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｑ　20/00　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０６Ｋ　19/10　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｄ
Ｇ０６Ｆ　17/60　４１０Ｚ
Ｇ０９Ｃ　1/00　６４０Ｄ
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０６Ｋ　19/00　Ｒ

【手続補正書】
【提出日】平成19年2月6日(2007.2.6)
【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】　セキュリティモジュールが文書作成者に知られない秘密を発生し、
秘密が、セキュリティモジュールが本物であるかどうかを通知する情報と共に、暗号化されて認証個所に伝送され、
認証個所が秘密を解読し、かつセキュリティモジュールが本物であるかどうかを確認し、そして検査個所だけが解読できるように、秘密が、文書作成者を確認する情報と共に暗号化されて文書作成者に伝送され、
文書作成者は、固有のデータをセキュリティモジュールに伝送し、
セキュリティモジュールが、文書作成者自身によって挿入されたデータを秘密に不可逆的に結合し、
この場合、秘密を推定することができない、
セキュリティモジュールを使用して偽造防止した文書又はデータセットを作成するための方法において、
文書作成者によって挿入されたデータと秘密の不可逆的な結合の結果が、文書に転記され、文書作成者自身によって挿入されたデータ及び認証個所の暗号化された情報が、文書を構成することを特徴とする方法。
【請求項２】　認証個所から引き渡された他の情報が、文書作成者本人であるかどうかの情報及び文書作成者によって作成された文書の有効期間に関する情報を有することを特徴とする請求項１に記載の方法。
【請求項３】　文書の真性を検査する方法において、検査個所が認証個所で暗号化された他の情報と秘密を解読することにより、文書作成者によって挿入されたデータと秘密からなる不可逆結合の結果が文書に転記されたかどうかを検査することと、検査個所が偽造防止文書の作成のために使用されるセキュリティモジュールと同じ方法で、文書作成者によって文書に挿入されたデータを、解読された秘密と不可逆的に結合すること、及び、

検査個所がそれ自体が行った不可逆の結合の結果を、文書作成者が行い文書に転記された不可逆の結合の結果と比較することを特徴とする方法。

【請求項４】　文書作成者によって文書に挿入されたデータが偽造されたかどうかが、比較によって確かめられることを特徴とする請求項３記載の方法。