【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2月15日(2007.2.15)

【公開番号】特開2000-196584(P2000-196584A)
【公開日】平成12年7月14日(2000.7.14)
【出願番号】特願平11-362358
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｇ０７Ｂ　17/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ｚ
Ｇ０７Ｂ　17/00

【手続補正書】
【提出日】平成18年12月21日(2006.12.21)
【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】　暗号化オペレーションを実行する暗号化デバイスにより誘導されるエミッションを制限する方法において、
前記暗号化デバイスを物理的に安全な環境に格納し、
前記暗号化デバイスに、前記物理的に安全な環境の外部にある第１電源から電力を供給し、
前記物理的に安全な環境内に第２電源を配置し、
少なくともプロセッサーが暗号化オペレーションを実行しているとき、前記第２電源から前記暗号化デバイス内の前記プロセッサーに電力を供給するステップを備えることを特徴とする方法。
【請求項２】　前記電力を供給するステップは、
前記プロセッサーが暗号化オペレーションを実行しているとき、前記第１電源から前記第２電源へ切換え、
前記プロセッサーが暗号化オペレーションを実行していないとき、前記第２電源から前記第１電源へ切換えるステップを備える請求項１に記載した方法。
【請求項３】　前記第２電源は電力貯蔵回路であり、前記電力貯蔵回路は、暗号化オペレーションが実行されていないとき、前記電力貯蔵回路は前記第１電源から電力を貯蔵し、暗号化オペレーションが実行されているとき、前記プロセッサーに電力を供給する請求項１に記載した方法。
【請求項４】　前記暗号化オペレーションは複数のセグメントに分けられ、前記第２電源は、前記複数のセグメントの間に、前記第１電源から電力を貯蔵する請求項３に記載した方法。
【請求項５】　暗号化オペレーションを実行する暗号化デバイスにより誘導されるエミッションを制限する方法において、
前記暗号化デバイスを物理的に安全な環境に格納し、
前記暗号化デバイスに、前記物理的に安全な環境の外部にある第１電源から電力を供給し、
前記物理的に安全な環境内に第２電源を配置し、
少なくとも前記暗号化デバイスが暗号化オペレーションを実行しているとき、前記第２

電源から前記暗号化デバイスに電力を供給するステップを備えることを特徴とする方法。

【請求項６】　前記電力を供給するステップは、

前記暗号化デバイスが暗号化オペレーションを実行しているとき、前記第１電源から前記第２電源へ切換え、

前記暗号化デバイスが暗号化オペレーションを実行していないとき、前記第２電源から前記第１電源へ切換えるステップを備える請求項５に記載した方法。

【請求項７】　前記第２電源は電力貯蔵回路であり、前記電力貯蔵回路は、暗号化オペレーションが実行されていないとき、前記電力貯蔵回路は前記第１電源から電力を貯蔵し、暗号化オペレーションが実行されているとき、前記プロセッサーに電力を供給する請求項５に記載した方法。

【請求項８】　暗号化オペレーションを実行する暗号化システムにおいて、

暗号化オペレーションを実行する少なくとも１つのプロセッサー、

前記暗号化オペレーションを実行するのに使用するため、前記プロセッサーに結合したメモリー手段、

前記暗号化オペレーションで計算され使用された情報を記憶し検索するため、前記プロセッサーに結合した記憶手段、

前記暗号化オペレーションへの直接のアクセスを防止するための、前記プロセッサーと前記メモリー手段と前記記憶手段との安全格納手段、

前記プロセッサーと前記メモリー手段と前記記憶手段とに結合し、これらに電力を供給するための、前記安全格納手段の外部にある第１電源、

少なくとも前記プロセッサーに結合し、これに電力を供給するための、前記安全に格納する手段の内部にある第２電源、及び、

暗号化オペレーションが実行されているとき、前記第１電源から前記第２電源へ切換え、非暗号化オペレーションが実行されているとき、前記第２電源から前記第１電源へ切換える手段を備えることを特徴とするシステム。

【請求項９】　前記第２電源はバッテリーである請求項８に記載したシステム。

【請求項１０】　前記第２電源は電力貯蔵回路である請求項８に記載したシステム。

【請求項１１】　前記電力貯蔵回路はキャパシターを備え、前記キャパシターは非暗号化オペレーションの間に充電され、暗号化オペレーションの間に少なくとも前記プロセッサーに電力を供給するため放電する請求項１０に記載したシステム。

【請求項１２】　前記暗号化オペレーションは複数のセグメントに分けられ、前記第２電源は、前記複数のセグメントの間に再充電される請求項８に記載したシステム。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】００２７

【補正方法】変更

【補正の内容】

【００２７】

図２に、本発明による暗号化デバイス10と共に使用することが出来る電力貯蔵回路（全体を40で示す）を示す。電力貯蔵回路40は、ライン36で電力ライン30に接続され、キャパシターＣ１、トランジスターＱ１、3つの抵抗器Ｒ1、Ｒ2、Ｒ3を備える。外部の電力入力ライン30と、暗号プロセッサー22の間に電力貯蔵回路40を置くことにより、プロセッサー20は、暗号プロセッサー22へ、電力ライン30で外部電力入力から供給するか、又は貯蔵デバイス（この場合キャパシターＣ１）から供給するかを制御することが出来る。本発明の好適な実施例では、Ｃ1＝0.04Ｆ、Ｒ1＝680Ω、Ｒ2＝47Ω、Ｒ3＝10ｋΩである。対応する実施のため、これらは相互に変えることが出来る。