【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27年3月19日(2015.3.19)

【公表番号】特表2014-533445(P2014-533445A)
【公表日】平成26年12月11日(2014.12.11)
【年通号数】公開・登録公報2014-068
【出願番号】特願2014-518465(P2014-518465)
【国際特許分類】
Ｈ０４Ｌ　9/14　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６４１

【手続補正書】
【提出日】平成27年1月27日(2015.1.27)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
N人の内部者に関連するN個のネットワーク・セグメントを含むネットワーク・システムが在り、
前記ネットワーク・セグメントのゲートウエイとして機能するN個の順序の有るプロキシーの集合と、
前記内部者に関連するN個のランダムに選ばれた鍵Knの集合が在り（記号nを１とNを含む１～Nの間の整数である）、
任意のn番目のプロキシーは、
j-1回鍵を掛けられた暗号文C_{j-1}を受け取り（ここで、記号jを１とNを含む１～Nの間の整数であり、又、ｊ＝１のC_{j-1}は原文C_0を表わす）、
前記暗号文C_{j-1}に前記n番目のプロキシーの鍵Knで鍵を掛けるプロセスを実行し、下記の(1)式で表わされる暗号文C_jを作り、
暗号文 $C_j \equiv eKn(C_{j-1})$ -------(1)
ここでeKn()は鍵Knの設定された関数を表わす；
前記プロキシーの集合は鍵を順番にj回掛ける順序を決める集合を実装しており、これに依り原文C_0の集合からj>2に派生する暗号文C_jの集合を提供する一方、
各々の暗号文C_jは、原文C_0について、前記プロキシーの集合に依り、(2)式のjの整数n_1，n_2，…，n_jの組み合わせで与えられており、
暗号文 $C_j = Kn_j(\cdots Kn_2(Kn_1(C_0))\cdots)$ -------(2)
ここで(1)式のeKn()を(2)式のKn()で書き換えている；
内部者各々の鍵Kn_jが
上記(2)式との等号を満足する下記のような一つの暗号文$Y(C_0)$の鍵Yを計算し決定することは困難であることと
(2) = $Y(C_0)$-------(3)
計算困難性のゆえに、もはや号鍵としては機能しないこと
を特徴とする鍵を罠に掛けるネットワーク・システムである。なお、鍵Kn()は鍵Knを持つ変換関数の罠に掛かった状態を表わす。
【請求項２】
請求1に従う暗号文C_jの集合は、鍵を掛ける順序を定義しているネットワーク経路の個

数を含むこと
を特徴とする請求１記載の鍵を罠に掛けるネットワーク・システムである；ここで、鍵を掛ける順序とは、jの整数n_1，n_2，…，n_jの順列組合せに相当するj!に等しい一方、逆順に鍵を掛ける経路(4)式の個数が前記j整数の円順列に相当する(j-1)!に等しいことを言う；

$$C_j \text{ ---> } C_{j-1} \text{ ---> } \cdots \text{ ---> } C_1 \equiv eKn_1(C_0) \text{ ---> } C_0 \text{ -------(4)}$$