(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3686080号
(P3686080)
(45)発行日　平成17年8月24日(2005.8.24)　(24)登録日　平成17年6月10日(2005.6.10)

(51)Int.Cl.[7]	F I		
G06F 11/00	G06F	9/06	660N
G06F 12/14	G06F	12/14	560C
G09C 1/00	G09C	1/00	640A
H04L 9/32	H04L	9/00	675A

請求項の数 39　(全 18 頁)

(21)出願番号　特願平7-504087
(86)(22)出願日　平成6年7月1日(1994.7.1)
(65)公表番号　特表平9-502550
(43)公表日　平成9年3月11日(1997.3.11)
(86)国際出願番号　PCT/US1994/007480
(87)国際公開番号　WO1995/002293
(87)国際公開日　平成7年1月19日(1995.1.19)
審査請求日　平成13年7月2日(2001.7.2)
(31)優先権主張番号　08/089,014
(32)優先日　平成5年7月8日(1993.7.8)
(33)優先権主張国　米国(US)

(73)特許権者
アレン、ローレンス　スィー.、ザ　サード
アメリカ合衆国　８７０５９　ニューメキシコ州　ティヘラス　テソロテ　ロード　５６
(73)特許権者
フォレスト、スティファニー
アメリカ合衆国　８７１０６　ニューメキシコ州　アルバカーキ　アムハースト　エヌ．イー．４４０

最終頁に続く

(54)【発明の名称】デジタル信号集合体に対する改変検出方法

(57)【特許請求の範囲】

【請求項１】

コンピュータの記憶装置に格納される、第２の複数の連続的なデジタル信号（以下、オリジナルストリングという）を保護するために、前記オリジナルストリングに改変が存在するのかを判断するため、コンピュータの演算装置により前記オリジナルストリングと比較される、第１の複数の連続的なデジタル信号（以下、保護ストリングという）を前記演算装置を用いて生成する保護ストリング生成方法において、

テスト用の複数の連続的なデジタル信号（以下、テストストリングという）を前記演算装置を用いて生成するステップ（ａ）と、

前記テストストリングが前記オリジナルストリングにマッチするのかを前記演算装置を用いて試すステップ（ｂ）と、

前記ステップ（ｂ）にてマッチするときは、前記テストストリングを捨てて、異なるテストストリングを前記演算装置を用いて生成するために前記ステップ（ａ）に戻るステップ（ｃ１）と、

前記ステップ（ｂ）にて非マッチであるときは、前記テストストリングを前記記憶装置内の前記保護ストリング内へ前記演算装置を用いて格納するステップ（ｃ２）と

を備えることを特徴とする保護ストリング生成方法。

【請求項２】

前記ステップ（ｃ２）は、さらに、前記演算装置を用いてステップ（ａ）の手順に戻り、複数の非マッチテストストリングが前記記憶装置内の前記保護ストリング内に格納された

後、この手順を終了することを特徴とする請求項１記載の保護ストリング生成方法。
【請求項３】
さらに、前記オリジナルストリングをそれぞれ複数の連続的なデジタル信号からなる複数のセグメントに前記演算装置を用いて分解するステップを備えることを特徴とする請求項１記載の保護ストリング生成方法。
【請求項４】
前記マッチを試すステップ（ｂ）は、それぞれのテスト用の複数の連続的なテストストリングが前記オリジナルストリングのそれぞれの前記セグメントの前記複数の連続的なデジタル信号にマッチするのかを前記演算装置を用いて試すことを特徴とする請求項３記載の保護ストリング生成方法。
【請求項５】
前記ステップ（ａ）にあってテストストリングは前記演算装置を用いてランダムに生成されることを特徴とする請求項１記載の保護ストリング生成方法。
【請求項６】
コンピュータの記憶装置に格納される、第１の複数の連続的なデジタル信号（以下、オリジナルストリングという）の改変を検出するオリジナルストリングの改変検出方法において、
前記記憶装置には前記オリジナルストリングに関連する第２の複数の連続的なデジタル信号（保護ストリングという）を有し、
前記保護ストリングは複数のテストストリングを有し、
それぞれの前記テストストリングは、前記保護ストリングが作成されたときには前記オリジナルストリングに非マッチの複数の連続的なデジタル信号を有し、
前記保護ストリングの一つの前記テストストリングの複数の連続的なデジタル信号を前記オリジナルストリングの複数の連続的なデジタル信号と前記コンピュータの演算装置を用いて比較するステップ（ａ）と、
前記ステップ（ａ）にて非マッチであるときは、前記演算装置を用いて前記保護ストリング内の前記全てのテストストリングが試験されるまで前記ステップ（ａ）の手順に戻り、かつ、異なるテストストリングを選択するステップ（ｂ１）と、
前記ステップ（ａ）にて前記テストストリングとオリジナルストリングとの間にマッチがあるときは、前記手順を終わらせ、前記演算装置を用いて前記オリジナルストリングに改変が存在すると判断するステップ（ｂ２）と
を備えることを特徴とするオリジナルストリングの改変を検出するオリジナルストリングの改変検出方法。
【請求項７】
前記記憶装置に格納される前記保護ストリングは、それぞれ複数の連続的なデジタル信号からなる複数のセグメントに分解されることを特徴とする請求項６記載のオリジナルストリングの改変検出方法。
【請求項８】
前記比較ステップ（ａ）は、前記保護ストリングの一つのテストストリングの複数の連続的なデジタル信号を、前記オリジナルストリングのそれぞれのセグメントの複数の連続的なデジタル信号と前記演算装置を用いて比較することを特徴とする請求項７記載のオリジナルストリングの改変検出方法。
【請求項９】
コンピュータの記憶装置に格納される、第１の複数の連続的なデジタル信号（以下、オリジナルストリングという）を保護するオリジナルストリングの保護方法において、
第２の複数の連続的なデジタル信号（以下、テストストリングという）を前記コンピュータの演算装置を用いて生成するステップ（ａ）と、
前記テストストリングの前記第２の複数の連続的なデジタル信号を、前記オリジナルストリングの前記複数の連続的なデジタル信号と前記演算装置を用いて比較するステップ（ｂ）と、

前記比較ステップ（ｂ）の比較の結果、前記テストストリングの前記第２の複数の連続的なデジタル信号と、前記オリジナルストリングの前記第１の複数の連続的なデジタル信号とがマッチするときは、前記演算装置を用いて異なるテストストリングに関して前記ステップ（ａ）の手順へ戻るステップ（ｃ１）と、
前記比較ステップ（ｂ）の比較の結果が非マッチであるときは、前記演算装置を用いて前記テストストリングを前記記憶装置内の前記保護ストリングに格納すると共に、前記保護ストリングに複数の非マッチテストストリングが格納されるまで前記ステップ（ａ）の手順に戻るステップ（ｃ２）と、
前記保護ストリングの一つのテストストリングの複数の連続的なデジタル信号を、前記オリジナルストリングの複数の連続的なデジタル信号と前記演算装置を用いて比較するステップ（ｄ）と、
前記比較ステップ（ｄ）の比較の結果が非マッチであるときには、前記演算装置を用いて前記保護ストリングに格納された全てのテストストリングがテストされるまで、前記ステップ（ｄ）に戻り、かつ異なるテストストリングを選択するステップ（ｅ１）と、
前記比較ステップ（ｄ）の比較の結果、前記テストストリングと前記オリジナルストリングとがマッチするときは、前記演算装置を用いて前記手順を終わらせて、オリジナルストリングに改変が存在することを判断するステップ（ｅ２）と
を備えることを特徴とするオリジナルストリングの保護方法。

【請求項１０】
さらに、前記オリジナルストリングを、それぞれ複数の連続的なデジタル信号からなる複数の連続的なセグメントに前記演算装置を用いて分解するステップを備えることを特徴とする請求項９記載のオリジナルストリングの保護方法。

【請求項１１】
前記比較ステップ（ｂ）は、前記テストストリングの、前記第２の複数の連続的なデジタル信号と前記オリジナルストリングの前記セグメントの各々の、前記複数の連続的なデジタル信号とのマッチを前記演算装置を用いて試すことを特徴とする請求項１０記載のオリジナルストリングの保護方法。

【請求項１２】
前記比較ステップ（ｄ）は、前記テストストリングの前記第２の複数の連続的なデジタル信号と前記オリジナルストリングの前記各セグメントの各々の、前記複数の連続的なデジタル信号とのマッチを前記演算装置を用いて試すことを特徴とする請求項１０記載のオリジナルストリングの保護方法。

【請求項１３】
前記テストストリングは前記演算装置を用いてランダムに生成されることを特徴とする請求項９記載のオリジナルストリングの保護方法。

【請求項１４】
複数のコンピュータに格納される、複数の同一のオリジナルコンピュータファイルを保護するためのコンピュータファイル保護方法において、
それぞれの前記オリジナルコンピュータファイルは複数の連続的なデジタル信号を有しており、各コンピュータにて、
テスト用の複数の連続的なデジタル信号（以下、テストストリングという）をランダムにコンピュータの演算装置を用いて生成するステップ（ａ）と、
前記テストストリングの前記テスト用の複数の連続的なデジタル信号を前記オリジナルコンピュータファイルの前記複数の連続的なデジタル信号と前記演算装置を用いて比較するステップ（ｂ）と、
前記比較ステップ（ｂ）の比較の結果、前記テストストリングの前記複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの前記複数の連続的なデジタル信号とがマッチするときは、前記演算装置を用いて前記ステップ（ａ）に戻るステップ（ｃ１）と、
前記比較ステップ（ｂ）の比較の結果が非マッチであるときは、前記演算装置を用いて前

記テストストリングをコンピュータ保護ファイルに格納し、さらに前記コンピュータ保護ファイルに複数の非マッチテストストリングが格納されるまで前記ステップ（ａ）の手順に戻るステップ（ｃ２）と、
前記コンピュータ保護ファイルの一つのテストストリングの複数の連続的なデジタル信号をオリジナルコンピュータファイルの複数の連続的なデジタル信号と前記演算装置を用いて比較するステップ（ｄ）と、
前記比較ステップ（ｄ）の比較の結果が非マッチであるときには、前記演算装置を用いて前記コンピュータ保護ファイルの全ての前記テストストリングがテストされるまで前記ステップ（ｄ）に戻り、かつ異なるテストストリングを選択するステップ（ｅ１）と、
前記比較ステップ（ｄ）の比較の結果、前記テストストリングと前記オリジナルコンピュータファイルとがマッチするときは、前記演算装置を用いて前記手順を終わらせ、前記オリジナルコンピュータファイルに改変が存在することを判断するステップ（ｅ２）と
を備えることを特徴とするコンピュータファイル保護方法。
【請求項１５】
さらに、前記オリジナルコンピュータファイルを、それぞれ複数の連続的なデジタル信号からなる複数の連続的なセグメントに前記演算装置を用いて分解するステップを備えることを特徴とする請求項１４記載のコンピュータファイル保護方法。
【請求項１６】
前記比較ステップ（ｂ）は、前記テストストリングのテスト用の複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの前記各セグメントの各々の複数の連続的なデジタル信号とのマッチを前記演算装置を用いて試すことを特徴とする請求項１５記載のコンピュータファイルの保護方法。
【請求項１７】
前記比較ステップ（ｄ）は、前記コンピュータ保護ファイルの一つのテストストリングのテスト用の複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの前記各セグメントの各々の複数の連続的なデジタル信号とを前記演算装置を用いて比較することを特徴とする請求項１５記載のコンピュータファイルの保護方法。
【請求項１８】
前記複数のコンピュータは、ネットワークに相互接続されていることを特徴とする請求項１４記載のコンピュータファイルの保護方法。
【請求項１９】
コンピュータの記憶装置に格納される、第２の複数の連続的なデジタル信号（以下、オリジナルストリングという）を保護するために、前記オリジナルストリングに改変が存在するのかを判断するため、コンピュータの演算装置により前記オリジナルストリングと比較される、第１の複数の連続的なデジタル信号（以下、保護ストリングという）を生成する保護ストリング生成方法において、
前記オリジナルストリングの前記複数の連続的なデジタル信号よりも少ない数のテスト用の複数の連続的なデジタル信号（以下、テストストリングという）を前記演算装置を用いて生成するステップ（ａ）と、
前記テストストリングの前記テスト用の複数の連続的なデジタル信号と前記オリジナルストリングの前記第２の複数の連続的なデジタル信号とのマッチを前記演算装置を用いて試すステップ（ｂ）と、
前記ステップ（ｂ）の結果が非マッチであるときには、前記演算装置を用いて前記テストストリングを破棄し、かつ異なるテストストリングに関して前記ステップ（ａ）に戻るステップ（ｃ１）と、
前記ステップ（ｂ）の結果がマッチであるときには、前記演算装置を用いて前記テストストリングを前記記憶装置内の前記保護ストリングに格納するステップ（ｃ２）と
を備えることを特徴とする保護ストリングの生成方法。
【請求項２０】
前記ステップ（ｃ２）は、さらに、前記演算装置を用いてステップ（ａ）の前記手順に戻

り、複数のマッチテストストリングが前記保護ストリング内に格納された後、前記手順を終了することを特徴とする請求項１９記載の保護ストリングの生成方法。
【請求項２１】
さらに、前記オリジナルストリングを、それぞれ複数の連続的なデジタル信号からなる複数のセグメントに前記演算装置を用いて分解するステップを備えることを特徴とする請求項１９記載の保護ストリング生成方法。
【請求項２２】
前記マッチを試すステップ（ｂ）は、前記テストストリングの前記テスト用の複数の連続的なテストストリングが前記オリジナルストリングのそれぞれの前記セグメントの前記複数の連続的なデジタル信号にマッチするのかを前記演算装置を用いて試すことを特徴とする請求項２１記載の保護ストリング生成方法。
【請求項２３】
前記格納ステップ（ｃ２）は、さらに、前記テストストリングが前記オリジナルストリングとマッチした前記オリジナルストリングの前記第２の複数の連続的なデジタル信号内の位置のロケーションを前記演算装置を用いて前記記憶装置に格納することを特徴とする請求項１９記載の保護ストリング生成方法。
【請求項２４】
前記ステップ（ａ）にあってテストストリングはランダムに前記演算装置を用いて生成されることを特徴とする請求項１９記載の保護ストリング生成方法。
【請求項２５】
コンピュータの記憶装置に格納される、第１の複数の連続的なデジタル信号（以下、オリジナルストリングという）の改変を検出するオリジナルストリングの改変検出方法において、
前記オリジナルストリングに関連する第２の複数の連続的なデジタル信号（以下、保護ストリングという）を前記記憶装置に有し、
前記保護ストリングは複数のテストストリングを有し、
前記保護ストリングが前記演算装置を用いて生成されたとき、前記オリジナルストリングの複数の連続的なデジタル信号の一部分にマッチする方法であり、
前記保護ストリングの一つのテストストリングの複数の連続的なデジタル信号を、前記オリジナルストリングの複数の連続的なデジタル信号と前記演算装置を用いて比較するステップ（ａ）と、
前記比較ステップ（ａ）の比較がマッチであるときは、前記演算装置を用いて前記ステップ（ａ）の手順に戻り、前記保護ストリング内の前記全てのテストストリングがテストされるまで異なるテストストリングを選択するステップ（ｂ１）と、
前記比較ステップ（ａ）の比較結果が前記テストストリングとオリジナルストリングが非マッチであるときは、前記演算装置を用いて前記手順を終了し、オリジナルストリングに改変が存在すると判断するステップ（ｂ２）と
を備えることを特徴とするオリジナルストリングの改変検出方法。
【請求項２６】
前記保護ストリングは、それぞれ複数の連続的なデジタル信号からなる複数のセグメントに前記演算装置を用いて分解されることを特徴とする請求項２５記載のオリジナルストリングの改変検出方法。
【請求項２７】
前記比較ステップ（ａ）は、前記保護ストリングの一つのテストストリングの複数の連続的なデジタル信号を、前記オリジナルストリングのそれぞれのセグメントの複数の連続的なデジタル信号と前記演算装置を用いて比較することを特徴とする請求項２６記載のオリジナルストリングの改変検出方法。
【請求項２８】
コンピュータの記憶装置に格納された複数の連続的なデジタル信号を有するオリジナルコンピュータファイルを保護するコンピュータファイル保護方法において、

前記オリジナルコンピュータファイルの前記複数の連続的な信号よりも少ない数の、複数の連続的なデジタル信号を持つテストストリングをコンピュータの演算装置を用いて生成するステップ（ａ）と、
前記テストストリングの前記複数の連続的なデジタル信号を前記オリジナルコンピュータファイルの前記複数の連続的なデジタル信号と前記演算装置を用いて比較するステップ（ｂ）と、
前記比較ステップ（ｂ）の比較の結果が、前記テストストリングの前記複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの前記複数の連続的なデジタル信号とが非マッチであるときには、異なるテストストリングに関して前記演算装置を用いて前記ステップ（ａ）に戻るステップ（ｃ１）と、
前記比較ステップ（ｂ）の比較の結果がマッチであるときには、前記演算装置を用いて前記テストストリングを前記記憶装置内の前記保護ファイルに格納し、複数のマッチテストストリングが前記保護ファイルに格納されるまでステップ（ａ）に戻るステップ（ｃ２）と、
前記保護ファイルの一つのテストストリングの複数の連続的なデジタル信号を前記オリジナルコンピュータファイルの複数の連続的なデジタル信号と前記演算装置を用いて比較するステップ（ｄ）と、
前記比較ステップ（ｄ）の比較の結果がマッチであるときには、前記保護ファイルの全ての前記テストストリングがテストされるまで前記演算装置を用いて前記ステップ（ｄ）に戻り、かつ異なるテストストリングを選択するステップ（ｅ１）と、
前記テストストリングとオリジナルコンピュータファイルとが非マッチであれば、前記演算装置を用いて前記手順を終了し、前記オリジナルコンピュータファイルに改変が存在することを判断するステップ（ｅ２）と
を備えることを特徴とするコンピュータファイル保護方法。

【請求項２９】
さらに、前記オリジナルコンピュータファイルを、それぞれ複数の連続的なデジタル信号からなる複数の連続的なセグメントに前記演算装置を用いて分解するステップを備えることを特徴とする請求項２８記載のコンピュータファイル保護方法。

【請求項３０】
前記比較ステップ（ｂ）は、前記テストストリングの複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの前記各セグメントの各々の複数の連続的なデジタル信号とのマッチを前記演算装置を用いて試すことを特徴とする請求項２９記載のコンピュータファイルの保護方法。

【請求項３１】
前記比較ステップ（ｄ）は、前記テストストリングの複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの前記各セグメントの各々の複数の連続的なデジタル信号とのマッチを前記演算装置を用いて試すことを特徴とする請求項２９記載のコンピュータファイルの保護方法。

【請求項３２】
前記格納ステップ（ｃ２）は、さらに、前記テストストリングが前記オリジナルコンピュータファイルとマッチした前記オリジナルコンピュータファイルの前記複数の連続的なデジタル信号内の位置のロケーションを前記演算装置を用いて前記記憶装置に格納することを特徴とする請求項３２記載のコンピュータファイルの保護方法。

【請求項３３】
前記ステップ（ａ）にあってテストストリングはランダムに前記演算装置を用いて生成されることを特徴とする請求項２８記載のコンピュータファイルの保護方法。

【請求項３４】
複数のコンピュータに格納された複数の同一のオリジナルコンピュータファイルを保護するためのコンピュータファイル保護方法において、
前記オリジナルコンピュータファイルの各々は複数の連続的なデジタル信号を有しており

、各コンピュータにて、
前記オリジナルコンピュータファイルの前記複数の連続的な信号よりも少ない数の、複数の連続的なデジタル信号を持つテストストリングをランダムに前記コンピュータの演算装置を用いて生成するステップ（ａ）と、
前記テストストリングの前記複数の連続的なデジタル信号を前記オリジナルコンピュータファイルの前記複数の連続的なデジタル信号と前記演算装置を用いて比較するステップ（ｂ）と、
前記比較ステップ（ｂ）にあって前記テストストリングの前記複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの前記複数の連続的なデジタル信号とが非マッチであるとき、前記演算装置を用いて前記ステップ（ａ）の手順に戻るステップ（ｃ１）と、
前記比較ステップ（ｂ）の比較結果がマッチであるときには、前記テストストリングをコンピュータの記憶装置内の保護ファイルに前記演算装置を用いて格納し、複数のマッチテストストリングが前記コンピュータ保護ファイルに格納されるまでステップ（ａ）に戻るステップ（ｃ２）と、
前記コンピュータ保護ファイルの一つのテストストリングの複数の連続的なデジタル信号を前記オリジナルコンピュータファイルの連続的なデジタル信号と前記演算装置を用いて比較するステップ（ｄ）と、
前記比較ステップ（ｄ）の比較の結果がマッチであるときには、前記コンピュータ保護ファイルの全ての前記テストストリングがテストされるまで、前記演算装置を用いて前記ステップ（ｄ）の手順に戻り、かつ異なるテストストリングを選択するステップ（ｅ１）と、
前記テストストリングと前記オリジナルコンピュータファイルとが非マッチであれば、前記演算装置を用いて前記手順を終了し、前記オリジナルコンピュータファイルに改変が存在することを判断するステップ（ｅ２）と
を備えることを特徴とするコンピュータファイル保護方法。
【請求項３５】
さらに、前記オリジナルコンピュータファイルを、それぞれ複数の連続的なデジタル信号からなる複数の連続的なセグメントに前記演算装置を用いて分解するステップを備えることを特徴とする請求項３４記載のコンピュータファイル保護方法。
【請求項３６】
前記比較ステップ（ｂ）は、前記テストストリングのテスト用の複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの各セグメントの各々の複数の連続的なデジタル信号とのマッチを前記演算装置を用いて試すことを特徴とする請求項３５記載のコンピュータファイルの保護方法。
【請求項３７】
前記比較ステップ（ｄ）は、前記テストストリングのテスト用の複数の連続的なデジタル信号と前記オリジナルコンピュータファイルの前記各セグメントの各々の複数の連続的なデジタル信号とのマッチを前記演算装置を用いて試すことを特徴とする請求項３５記載のコンピュータファイルの保護方法。
【請求項３８】
前記複数のコンピュータは、ネットワークと相互接続されていることを特徴とする請求項３４記載のコンピュータファイルの保護方法。
【請求項３９】
前記格納ステップ（ｃ２）は、さらに前記テストストリングが前記オリジナルコンピュータファイルとマッチした前記オリジナルコンピュータファイルの前記複数の連続的なデジタル信号内の位置のロケーションを前記演算装置を用いて前記記憶装置に格納することを特徴とする請求項３４記載のコンピュータファイルの保護方法。
【発明の詳細な説明】
技術分野

本発明は、コンピュータにおいて格納されもしくは使用されるようなデジタル信号集合体に対する改変を検出する方法に関する。また、特に、本発明は、例えば、ウイルスや他の形態による不当な改ざんにより生じたコンピュータファイル内の改変を検出する方法に関する。

発明の背景

ハードウェアはネットワークを介して相互に関係付けられ、一方ソフトウェアはコンピュータプログラム及びデータの携帯性という面から相互に関係付けられるというように、コンピュータシステムやソフトウェアが益々相互に関連してくるにつれて、例えばウイルスのような不当な利用者や不当な改ざん者による不当な侵入から守ることは益々困難なものとなってきている。更に、コンピュータが益々相互に関係付けられるにつれて、一旦コンピュータネットワークのあるノードでそのような侵入が起こるとその侵入から（他の装置を）離隔させるのは益々困難になってきている。

この技術分野においては、ウイルス検出プログラムがよく知られている。典型的な従来のウイルス検出プログラムにおいては、コンピュータの副構成要素である記憶媒体（メモリ又はディスク）内に寄生する特定のウイルスを追跡してその存在を判断することがプログラムにより行われている。しかしながら、かかる従来の対ウイルス・プログラムは単に既知のウイルスを検出するにすぎない。新しいウイルスが創作されてコンピュータプログラムに侵入するような場合、その対ウイルス・プログラムでは新しいウイルスは特定できないので、そのような新規に侵入するウイルスの存在を検出することはできない。それ故、従来において対ウイルス・プログラムが次々と出現してきた理由の一つとしては、新たに創作されたウイルスを特定するために対ウイルス・プログラムは随時更新されなければならなかったからである。

同様に、従来の対ウイルス・プログラムの他の問題点としては次のようなものがある。即ち、ネットワーク上のあるコンピュータのあるノードからあるウイルスが侵入し、対ウイルス・プログラムがそれを検出できなかった場合、ネットワーク上の他のすべてのコンピュータに同じ対ウイルス・プログラムが備わっていたとしても、そのウイルスは検出されないままネットワーク上の他のすべてのコンピュータに拡散してしまう。その結果、新しいウイルスであれば、コンピュータネットワーク上のあるノードに一旦侵入すれば、全コンピュータネットワークに侵入拡散できることが事実上確証される。

コンピュータ技術分野において、対ウイルス・プログラムと同じように、その改変を検出するためにあるファイルを他のファイルと比較するプログラムというのはよく知られている。加えて、例えばチェックサムのようなファイル認証方法もこの技術分野においてはよく知られている。

生物学の分野においては、免疫システム細胞というものがよく知られている。Ｔ細胞がその免疫システムの一部を構成している。Ｔ細胞は抗原を検出する受容体をその表面に有している。これらの受容体は疑似ランダム遺伝的過程を経て構成され、いくつかの受容体は生体からの分子もしくは「自己分子」を検出することができる高い可能性を有している。Ｔ細胞は胸腺において消極的選択と呼ばれる検閲過程を経る。消極的選択において、自己分子もしくは生体にとって通常の分子、又はペプチドである分子を認識したＴ細胞は、破壊され胸腺に抑留される。自己ペプチドを検出しなかったＴ細胞は、胸腺を離れ、外部からの抗原に対する免疫による保護についての一基礎を提供する。

発明の概要

本発明においては、オリジナル・コンピュータ・ファイルを保護するために、複数の隣接デジタル信号を有するコンピュータ保護ファイルを生成する方法が開示されている。その方法においては先ずテストファイルが生成される。テストファイルは複数の隣接デジタル信号を有する。その方法においては、テストファイルにおける複数の隣接デジタル信号とオリジナル・コンピュータ・ファイルにおける複数の隣接デジタル信号とのマッチングが調べられる。そこで、マッチしていた場合、そのテストファイルは破棄され、その手順はもとに戻って前のテストファイルと異なる他のテストファイルを生成する。一方、マッチしていなかった場合、そのテストファイルは格納される。

本発明には、オリジナル・コンピュータ・ファイルに対する改変を検出する方法も含まれており、その方法においてはオリジナル・コンピュータ・ファイルは関連保護ファイルを有している。オリジナル・コンピュータ・ファイルは複数の隣接デジタル信号を有している。関連コンピュータ保護ファイルも複数のテストファイルを有しており、それらのテストファイルの各々は複数の隣接デジタル信号を有している。また、その複数の隣接デジタル信号は、オリジナル・コンピュータ保護ファイルが生成されたときにおいては、オリジナル・コンピュータ・ファイルにおける複数の隣接デジタル信号とはマッチしない信号である。そこで、この方法においては、コンピュータ保護ファイルの１つのテストファイルの複数の隣接デジタル信号とオリジナル・コンピュータ・ファイルにおける複数の隣接デジタル信号とが比較される。非マッチの場合には、コンピュータ保護ファイルにおけるすべてのテストファイルが検証されるまで、異なるテストファイルが選択され、手順は比較のステップまで戻る。一方、テストファイルとオリジナル・コンピュータ・ファイルがマッチした場合には、その手順は終了し、オリジナル・コンピュータ・ファイルに改変が検出されたことになる。

【図面の簡単な説明】

図１ａ及び１ｂは、コンピュータ保護ファイルを生成し、そのコンピュータ保護ファイルが生成された後のオリジナル・コンピュータ・ファイルに対する改変を検出するという本発明の好適な実施例における２つの方法のそれぞれのフローチャートである。

図２ａ及び２ｂは、それぞれ図１ａ及び１ｂに示された方法の他の実施例のフローチャートである。

図３は、コンピュータのネットワークの概略図であり、それぞれのコンピュータは、ネットワークのあるノードからウイルスが侵入した場合にその拡散を防御するためのオリジナル・コンピュータ・ファイルと関連した異なるコンピュータ保護ファイルを有している。

発明の詳細な説明

本発明は、オリジナルのコンピュータ・ファイルを保護するため、コンピュータ保護（protection）ファイルを生成する方法に関する。明細書中で、請求の範囲を含めて、使われているように、「ファイル」という用語は、デジタル情報の集まり（collection）を意味する。このようなデジタル情報の集まりには、コンピュータのディスクドライブ等の、ある格納メディア（storage medium）上に物理的に格納された物理的なファイルや、他の物理的ファイルの一部である論理的ファイルが該当し得る。「ファイル」という用語が示すものは、オリジナルのコンピュータ・ファイル内に含まれているコンピュータ保護ファイルのように、エンコードされ、他の「ファイル群」内に含まれることさえある。要するに、用語「ファイル」は、他の物理的集まりから分離された物理的集まりに限定されず、単にデジタル情報の集まりが該当する。

図１ａを参照すると、オリジナルのコンピュータ・ファイル１０を保護するためにコンピュータ保護ファイル１６を生成する本発明の方法のフローチャートが示されている。オリジナルのコンピュータ・ファイル１０は、複数の隣接するデジタル信号を有するファイル又はストリングとして表されている。本発明の方法は一般に、コンピュータ・システム内で保護されるデジタル情報の集まりに関するので、オリジナルのストリング１０は、バイナリ信号又は、バイトやキャラクタによってベースとされるより大きな信号であり得る。コンピュータは、テスト・ストリング（R_0）１２として表されるテスト・ファイルをランダムに生成する。テスト・ストリング１２は、また、隣接するデジタル信号を複数有する。次に、ランダムに生成されたテスト・ストリング１２の、オリジナル・ストリング１０の一部に対する比較（match）が試みられる。これから詳細に説明されるように、テスト・ストリングR_0の複数の隣接するデジタル信号は、オリジナル・ストリング１０の複数の隣接するデジタル信号と比較が試みられる。マッチ（以後、詳細に議論される基準）の場合、テスト・ストリング１２は、捨てられ（rejected）、そして、当該方法は続けて、別のランダム・テスト・ストリング１２を生成し、前記のステップを続ける。マッチしない（non-match）場合、テスト・ストリング１２はコンピュータ保護ファイル１６又は抗体セット（Ｒ）１６内に保持される。好ましい実施の形態では、これまでに記載された

方法が、複数の非マッチング（non-matching）・テスト・ファイル１２が抗体セット（Ｒ）１６内に、コンピュータ保護ファイルとして格納されるまで、続けられる。
ランダムに生成されたテスト・ストリング１２の複数の隣接するデジタル信号の、オリジナル・ストリング１０の複数の隣接するデジタル信号への比較を試みるため、オリジナル・ストリング１０はまず、それぞれが複数の隣接デジタル信号から構成される、複数の隣接セグメントに構文解析され（parsed）、又は、論理的に分解される。好ましい実施の形態では、オリジナル・ストリング１０は、等しいサイズのセグメントに、構文解析又は分解される。しかしながら、これは必須の制限ではなく、単に便宜上のものである。例えば、オリジナル・ストリング１０が、
00101000100100000100001010010011
から成る３２ビット・ストリングである場合、上記記載の３２ビット・ストリングは、以下のように、それぞれ４つの隣接デジタル・ビットから構成される８つのセグメントに構文解析・分解される。
0010｜1000｜1001｜0000｜0100｜0010｜1001｜0011
オリジナル・ストリングが、それぞれ４つの隣接デジタル・ビットを有する８つのセグメントに構文解析・分解されると、ランダムに生成されるテスト・ストリング１２のそれぞれも、その長さが４つの隣接するデジタル・ビットになる。テスト・ストリング１２は、それから、テスト・ストリング１２のデジタル信号のそれぞれを、各セグメントのデジタル信号に対してテストすることによって、セグメントのそれぞれと比較される。従って、テスト・ストリング１２が隣接デジタル信号「１０００」を含む場合、テスト・ストリング１２と第２セグメントとの間にマッチが見出される。その場合、当該方法は続いて、ランダムに異なるテスト・ストリング１２を生成し、そのテスト・ストリング１２の、オリジナル・ストリング１０のセグメントのそれぞれに対する比較が試みられる。
ランダムに生成されたテスト・ストリング１２が、オリジナル・ストリング１０のセグメントのいずれにもマッチしないことが分かった場合、例えば、テスト・ストリングが「０１１１」である場合、そのテスト・ストリング１２は抗体セット（Ｒ）１６内に格納される。好ましい実施の形態では、それぞれがオリジナル・ストリング１０のセグメントのいずれにもマッチしない、複数のテスト・ストリング１２が抗体セット（Ｒ）１６内に格納されるまで、別のテスト・ストリング１２がランダムに生成され、オリジナル・ストリング１０の各セグメントに対してテストされる。
図１ｂを参照すると、本発明のもう一つの方法のフローチャートが示されており、ここでは、一旦、前記方法において判断されるように、マッチしない複数のテスト・ストリングが見出され、抗体セット（Ｒ）１６内に格納されると、抗体セット（Ｒ）１６は、テストされるストリング１８内に改変が生じているか否かを判断するのに使われる。テストされるストリング１８は、テストされたオリジナル・ストリング１０と関連を有する。オリジナル・ストリング又はオリジナル・コンピュータ・ファイル１０の許可されていない侵入又は侵略（unauthorized intrusion or invasion）が発生しなかった場合、テストされるストリング１８は、オリジナル・ストリング１０と一致する。しかしながら、抗体セット（Ｒ）１６が生成されてから、オリジナル・ストリング１０がウイルス等によって変更、又は侵された場合、テストされるストリング１８はオリジナル・ストリング１０の変形物（variation）である。図１ｂに描かれた本発明の方法は、テストされるストリング１８が、オリジナル・ストリング１０である確率が高いのか、その変更された変形物であるかの判断をする。
好ましい実施の形態においては、テストされるストリング１８も、それぞれ複数の隣接デジタル信号で構成される複数のセグメントに構文解析又は分解される。再び、好ましい実施の形態においては、セグメントの長さは等しく、かつ、抗体セット（Ｒ）１６の生成に使われたセグメントの長さに等しい。上の例で続けると、ストリング１８は、それぞれ４ビット長の８つのセグメントに構文解析・分解される。４ビット長である、抗体セット（Ｒ）１６からのテスト・ストリングのそれぞれは、ストリング１８のセグメントのそれぞれに対して比較される。抗体セット（Ｒ）１６からのテスト・ストリング１２がストリン

グ１８からのセグメントのいずれにもマッチしない場合、抗体セット（Ｒ）１６から次のテスト・ストリング１２が使われる。これは、抗体セット（Ｒ）１６からのテスト・ストリングのすべてがテストされ、ストリング１８がオリジナル・ストリング１０と同じである確率が高いことが明らかにされるまで、続く。
一方、抗体セット（Ｒ）１６からのテスト・ストリングのいずれかが、ストリング１８のセグメントのいずれかにマッチする場合は、ストリング１８は、オリジナル・ストリング１０と一致せず、オリジナル・ストリング１０への変更が発生したことが明らかにされる。
図３には、ネットワーク化された複数のコンピュータ２０（Ａ－Ｄ）の概略図が示されている。本発明の前記方法による効果は、図３を参照することにより明らかになる。もし、それぞれのコンピュータ２０が各々のオリジナルのコンピュータ・プログラムあるいはストリング１０を遂行すると仮定するならば、図１ａを用いて説明された方法により、各コンピュータ２０（Ａ－Ｄ）は連携されたコンピュータ保護ファイルあるいは他のコンピュータ２０により生成されたものとは異なる抗体セット（Ｒ）１６を生成する。各保護ファイル１６はランダムに生成されたテスト・ストリング１２に基づいて作成されるため、コンピュータ２０Ａと連携され、R_1とラベルされた保護ファイル１６は、コンピュータ２０Ｂにより生成されたオリジナルのストリング１０と連携されたR_2とラベルされた保護ファイル１６とは異なる。それゆえ、各コンピュータ２０にとって、オリジナルファイル１０と連携された保護ファイル１６は別のものである。
ここで、コンピュータ・ノードの１つ、すなわちコンピュータ２０Ａに発生したウイルスあるいは不許可の指令を想定してみよう。さらに、コンピュータ２０Ａで動くオリジナルのコンピュータ・ファイル１０と連携されたコンピュータ保護ファイルR_1は、ウイルスの指令を検出できないと仮定しよう。さらに、ウイルスは連結に沿ってコンピュータ２０Ｂに伝播する。同じウイルスであるから、コンピュータ２０Ａで動くオリジナルのストリング１０を冒したのと同じように、コンピュータ２０Ｂで動くオリジナルのコンピュータ・ファイルあるいはオリジナルのストリング１０を冒す。コンピュータ２０Ｂのオリジナルのファイルと連携されたコンピュータ保護ファイルあるいは抗体セット１６R_2は、コンピュータ２０Ａのコンピュータ保護ファイルとは異なるから、コンピュータ２０Ａのコンピュータ保護ファイルR_1がウイルスの指令を検出できなかったとしても、前述のテスト方法によればオリジナルのコンピュータ・ファイル１０の変化によりウイルスの存在を検出するかも知れない。それゆえ、ウイルスが全体のコンピュータネットワークに侵入するためには、ウイルスはコンピュータ２０Ａのコンピュータ保護ファイルR_1ばかりでなく、コンピュータ２０Ｂの保護ファイルR_2，コンピュータ２０Ｃの保護ファイルR_3，コンピュータ２０Ｄの保護ファイルR_4にもまた打ち勝たねばならない。お分かりのように、ネットワーク上のコンピュータの数が増えるにつれ、増加するネットワーク上の異なる保護ファイルに対応して検出を避けるウイルスの能力も減少する。それゆえ、本発明の方法において、オリジナルのストリング１０へのウイルスの指令の検出は、確率的根拠のある決定である。

検出の確率

検出は確率的なものであるため、次に保護ファイル１６のテスト・ストリングおよびオリジナルのストリング１０の異なる構成に対する確率について説明する。最初は、同じ長さの２つのストリング間の完全なマッチングは、ストリングの各場所で、デジタル信号（バイナリ信号、あるいはバイト信号やキャラクタ信号のようなバイナリ信号の集まり）が同一であることを意味することに注意すべきである。１つの実施例においては、もし対応する場所におけるシンボルの隣接マッチングが起こるならば、マッチングが起こると思われる。さらに、もしストリングの長さがｌでありｍがアルファベットのシンボルの数（シンボルがバイナリ１であり、１０４の順位にある場合、ＳＰＡＲＣプロセッサからの指令セットに対しｍ＝２，そして中間値に対しｍ＝５０）であるならば，マッチングの確率は次のように決定される。
もし、次の用語を定義するならば、

N_{R0}＝テスト・ストリングの最初の数（マッチングを行う前）
N_R＝マッチングを行った後のテストストリングの数
N_S＝オリジナルのストリングのセグメントの数
P_M＝２つのランダム・ストリングのマッチングの確率
ｆ＝N_Sオリジナルのストリングのいずれもマッチングしないランダム・ストリングの確率
＝（１－P_M）^{NS}
P_f＝N_R抗体が指令を検出しない確率
もし、P_Mが小さくN_Sが大きいならば、

$$f \approx e^{-P_M N_S}$$

そして、

$$N_R = N_{R_0} \times f$$

$$P_f = (1 - P_M)^{N_R}$$

$$\approx e^{-P_M N_R}$$

上記をN_Rについて解くと、
$\ln P_f = N_R \ln(1-P_M)$
あるいは、

$$N_R = \frac{\ln P_f}{\ln (1-P_M)}$$

ｆは、ほぼ

$$e^{-P_M N_S} = (1 - P_M)^{N_S}$$

であるから、
$-P_M N_S = N_S \ln(1-P_M)$
あるいは、
$-P_M = \ln(1-P_M)$
あるいは、

$$N_R = \frac{\ln P_f}{-P_M} = \frac{-\ln P_f}{P_M}$$

そこで、次の式を得る。

$$N_R = N_{R_0} \times f$$

あるいは、

$$N_{R_0} = \frac{-\ln P_f}{P_M \times f}$$

$$= \frac{-\ln P_f}{P_M \times (1-P_M)^{N_S}}$$

この式により、検出の確率（１－P_f）の関数として指令を検出することが求められる最初のストリング（N_{R0}）の数、保護されるオリジナルのストリングのセグメントの数（N_S）、およびマッチングルール（P_M）を予測することができる。R_0は、次式のようなマッチングルールを選択することにより最小化される。

$$P_M = \frac{1}{N_s}$$

これは所望の検出の確率を選択することができ、N_Sの大きさ（保護されるべきストリングの数）の関数として求められる抗体ストリングの数を概算することができることを示している。

検出の確率の増大はコンピュータ費用の増加に結び付くため（R_0およびRの大きさが増大するため）、（ａ）１つの侵入行為がいかに致命的であるか、そして（ｂ）システムにどれほど冗長性が存在するか（すなわち、どれほど検出アルゴリズムのコピーが存在するか）を決定することにより所望の検出の確率を選択することができる。検出の確率は独立の検出アルゴリズムの数により指数関数的に増加することに注意すべきである。もし、N_t＝アルコリズムのコピーの数であるならば、

$$P_{\text{system fails to detect}} = (P_f)^{N_t}$$

以下の表の値は、異なったアルファベットサイズ、すなわちｍから対応するｒおよびｌの値を求めたものである。

アルファベットサイズ＝２

	P_M		
r\l	16	32	50
1	1.0	1.0	1.0
2	1.0	1.0	1.0
3	0.938	1.0	1.0
4	0.438	0.938	1.0
5	0.203	0.453	0.734
6	0.094	0.218	0.359
7	0.043	0.105	0.176
8	0.020	0.051	0.086

アルファベットサイズ＝５０

	P_M		
r\l	16	32	50
1	0.314	0.628	0.984
2	0.006	0.012	0.019
3	1.10E-04	2.35E-04	3.76E-04
4	2.04E-06	4.55E-06	3.98E-06
5	3.77E-08	8.79E-08	3.75E-07
6	6.91E-10	1.69E-09	3.52E-19
7	1.26E-11	3.26E-11	3.31E-11
8	2.26E-13	6.28E-13	3.11E-12

アルファベットサイズ＝１０４

	P_M		
r\l	16	32	50
1	0.152	0.305	0.476
2	0.001	0.003	0.004
3	0.123E-05	2.64E-05	4.23E-05
4	1.1E-07	2.46E-07	3.98E-07
5	9.78E-10	2.28E-09	3.75E-09
6	8.62E-12	2.11E-11	3.52E-11
7	7.53E-14	1.96E-13	3.31E-13
8	6.52E-16	1.81E-15	3.11E-15

前述の表は、式に対して概算により求めたものである。結局、正確な式を用いて、以下の

表の値を求めた。

アルファベットサイズ＝２

r\l	P_M 16	32	50
1	1.000	1.000	1.000
2	0.961	0.999	1.000
3	0.702	0.922	0.983
4	0.395	0.665	0.827
5	0.197	0.390	0.552
6	0.093	0.205	0.315
7	0.043	0.103	0.165
8	0.020	0.050	0.084

アルファベットサイズ＝５０

r\l	P_M 16	32	50
1	0.276	0.476	0.636
2	0.006	0.012	0.019
3	1.021E-04	2.353E-04	3.764E-04
4	1.885E-06	4.550E-06	7.373E-06
5	3.456E-08	8.787E-08	1.443E-07
6	6.285E-10	1.695E-09	2.824E-09
7	1.132E-11	3.264E-11	5.522E-11
8	2.012E-13	6.277E-13	1.079E-12

アルファベットサイズ＝１０４

r\l	P_M 16	32	50
1	0.143	0.266	0.383
2	0.001	0.003	0.004
3	1.233E-05	2.642E-05	4.227E-05
4	1.101E-07	2.456E-07	3.980E-07
5	9.776E-10	2.280E-09	3.745E-09
6	8.617E-12	2.114E-11	3.523E-11
7	7.533E-14	1.958E-13	3.312E-13
8	6.520E-16	1.810E-15	3.112E-15

他の実施例

図２ａには、図１ａに示された本願発明の方法の他の実施例のフローチャートが示されている。図２ａのフローチャートでは、オリジナル・ストリングは１１０として記載されている。本願発明の方法を実行しているコンピュータは、ランダムなテスト・ストリング１１２を生成する。図１ａに示されるオリジナル・ストリング１０と同様なオリジナル・ストリング１１０は、複数のセグメントとして細かに調べられる。好ましい実施例では、セグメントのすべては複数の隣接デジタル信号からなる各々のセグメントと等価である。ついで、コンピュータはランダムに生成させたテスト・ストリング１１２をオリジナル・ストリング１１０の各々のセグメントとのマッチングを行う。結局、マッチしないと、テスト・ストリング１１２は廃棄される。

結局、テスト・ストリング１１２がオリジナル・ストリング１１０のセグメントとマッチすると、テスト・ストリング１１２は、抗体セット（Ｒ）１１６の一部として保護ファイル１１６に保持される。抗体セット（Ｒ）１１６の生成は、図１ａで示され記述された抗体セット（Ｒ）１６の正確に相補的なロジックとなる。しかしながら、テスト・ストリング１１２はオリジナル・ストリング１１０のひとつ以上のセグメントとマッチするので、テスト・ストリング１１２がオリジナル・ストリング１１０とマッチする特定のひとつの

場所かまたは複数の場所もまた抗体セット（Ｒ）１１６に格納される。また、テスト・ストリング１１２がオリジナル・ストリング１１０のセグメントとマッチした回数に関するデータも抗体セット（Ｒ）１１６に記録されなければならない。
図２ａに示したフローチャートと同じように、図２ｂのフローチャートは、図１ｂのフローチャートに示された方法の別の実施例である本願発明の方法を示している。一旦、抗体セット（Ｒ）ファイル１１６が作られると、抗体セット（Ｒ）ファイルはストリング１１８に対してテストされる。それは抗体セット１１６からのテスト・ストリング１１２がストリング１１８に対してマッチすると仮定される各々の場所で、抗体セット１１６からのテスト・ストリング１１２をテストされるべきストリング１１８に対してマッチングを試みることになる。もし、マッチしなければ、ストリング１１８はオリジナル・ストリング１１０と同一ではなく、オリジナル・ストリング１１０に対する変化が検出される。
もし抗体セット１１６からのテスト・ストリング１１２がストリング１１８のセグメントとマッチすれば、コンピュータはテスト・ストリング１１２をマッチが起こると想定されているすべての場所がテストされるかまたは必要とされるマッチ数になるまで、残りのすべてのセグメントに対して比較を行う。これは、もし複数のマッチがあったり、オリジナル・ストリング１１０のセグメントのひとつのみにウイルスが感染したような場合、マッチングテストは抗体セット１１６からのテスト・ストリング１１２をオリジナル・ストリング１１０の想定されたマッチングセグメントのすべてに対して、変更が生じていないことを確かめるため比較しなければならないため必要なことである。もし、抗体セット１１６からのテスト・ストリング１１２が、ストリング１１８のセグメントの必須の回数や必須の場所でマッチすれば、第２のテスト・ストリング１１２が抗体セット１１６から検索され、すべてのテスト・ストリング１１２がテストされるまで、別のマッチングテストが実行される。結局、すべてのテスト・ストリング１１２が必須の場所および回数でストリング１１８のセグメントとマッチし、ストリング１１８はオリジナル・ストリング１１０と同一であるという高い信頼性を有するようになる。
図２ａおよび２ｂに述べられ示されたオリジナル・ファイルでの変化を確実に検知するという点における本発明の方法の有利な点は、同様に、図３に述べられ示されるようなネットワークに適用することができる。ネットワークの各々のコンピュータ２０（Ａ－Ｄ）は他のコンピュータ２０の抗体セット１１６とは異なるそれ自身の抗体セット１１６を生成するので、ウィルスを逃しコンピュータネットワーク全体に広がってしまう確率は、ネットワークにおけるコンピュータの数が増加するにつれて減少するであろう。

その他の考察

前述において論じたように、本発明は物理的な”ファイル”の作成またはテストに限定されない。用語”ファイル”の使用は、デジタル信号、キャラクタ信号による又はバイトによるような２進数あるいはそれ以上のグループ化(grouping)の集合体を備え得るデジタル情報の集合を定義するには明かに手不足である。
更に、前述において論じたように、”マッチ”の概念は、各場所において完全同一であるマッチに限定されない。上記において記載される一例は単に、”ｒ＜ｌとなるようなストリング長ｌにおいて、対応する位置における信号間での隣接するｒ個のマッチ”である。他の実施例は単に、”ｒ＜ｌとなるようなストリング長ｌにおいて、対応する位置における信号間でのｒ個のマッチ”である。この実施例は、対応する位置における信号間のマッチは隣接するマッチでなければならないという要件を緩和する。他の形態のマッチには相補形態(complementary form)のような論理等価物が含められる。故に、例えば、２進法のストリング”０１１１”は”１０００”に対するマッチと考えられる。というのは、この２つは論理的に相補的等価物であるからである。
更に、図１ａに示され記載されるようなコンピュータ保護ファイル１６の発生において、オリジナル・ストリング１０に”マッチしない”テスト・ストリング１２を保持することによって、対応する場所、例えば１つのシンボル、にマッチがなければテスト・ストリング１２は拒絶される必要はない。言い換えれば、コンピュータ保護ファイル１６は、複数の”純粋な”テスト・ストリング１２であってどのストリングもオリジナル・ストリング

１０における対応するシンボルとマッチする単一シンボルは有しないようなものを備える必要はない。低レベルのマッチが許容され得る。
従って、テストされるストリング１８に対してコンピュータ保護ファイル１６の各テスト・ストリング１２をテストするに当たり、図１ｂに示され記載されるように、対応する場所における単一シンボルのマッチのような低レベルのマッチはオリジナル・ストリング１０が変更された旨の宣言に至る必要はない。
同様に、コンピュータ保護ファイル１１６の発生において、図２ａに示され記載されるように、オリジナル・ストリング１１０に”マッチする”テスト・ストリング１１２を保持することによって、対応する場所に例えば１つのシンボルがマッチしないならテスト・ストリング１１２は拒絶される必要はない。言い換えれば、コンピュータ保護ファイル１１６は、複数の”純粋な”テスト・ストリング１１２であってどのストリングもオリジナル・ストリング１１０における対応するシンボルとマッチしない単一シンボルは有しないようなものを備える必要はない。低レベルの非マッチングが許容され得る。
加えて、コンピュータ保護ファイル１６の各テスト・ストリング１２をテストするに当り、図２ｂに示され記載されるように、対応する場所における単一シンボルがマッチしないような低レベルの非マッチはオリジナル・ストリング１０が変更された旨の宣誓に至る必要はない。
故に、クレームを含めて、ここで用いるように、用語”マッチ”は、上述の方法のいかなるものをも含むものであり、場合に応じて低レベルの”マッチ”又は”非マッチ”を含むが、これらに限定されるものではない。
低レベルの”マッチ”又は”非マッチ”の許容の論拠は、単一シンボル（ビットまたはバイト）における変更のような幾つかの変更のみを生じるウイルスは蔓延しないだろうということである。ウイルスが複写するならば、多くの変化が起きウイルスが検出されるだろう。低レベルのウイルス攻撃を許容するための二律背反性は、オリジナル・ストリングを保護するアルゴリズムが速く実行するだろうが保護の低下を伴うということである。これは、人間の免疫系において低レベルのウイルス攻撃は必ずしも免疫応答を引き起こさないことと類似している。
最後に、テスト・ストリング１２又は１１２の発生は、図１ａ及び図２ｂに示され記載される方法においてランダムに発生しなくてもよい。次に発生するテスト・ストリング１２又は１１２が先に発生するテスト・ストリング１２又は１１２と異なる限りにおいて、本発明の方法は同様に機能するだろう。

【図１Ａ】

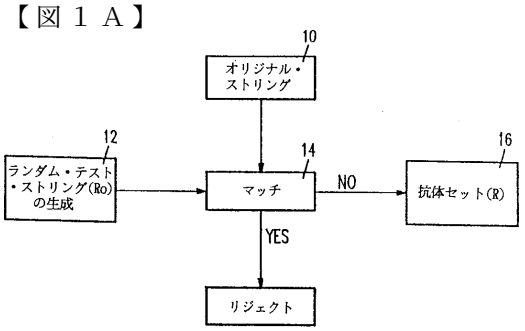

FIG. 1A

【図１Ｂ】

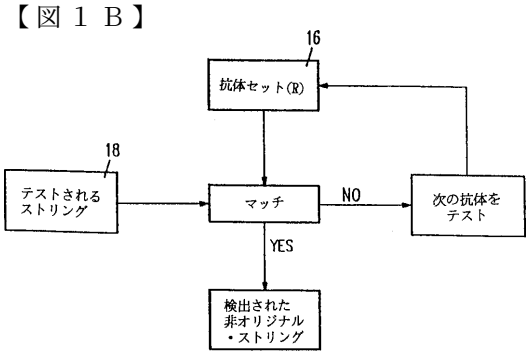

FIG. 1B

【図２Ａ】

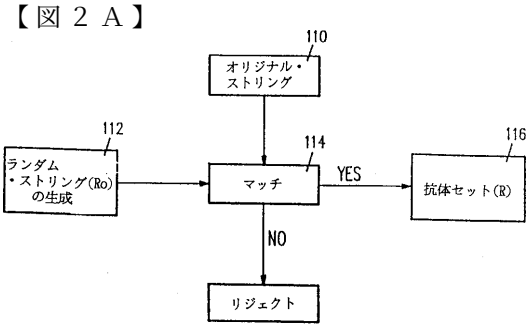

FIG. 2A

【図２Ｂ】

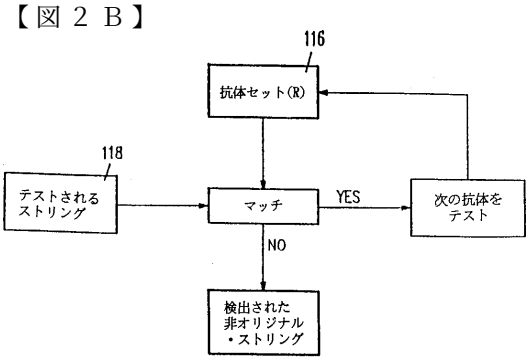

FIG. 2B

【図３】

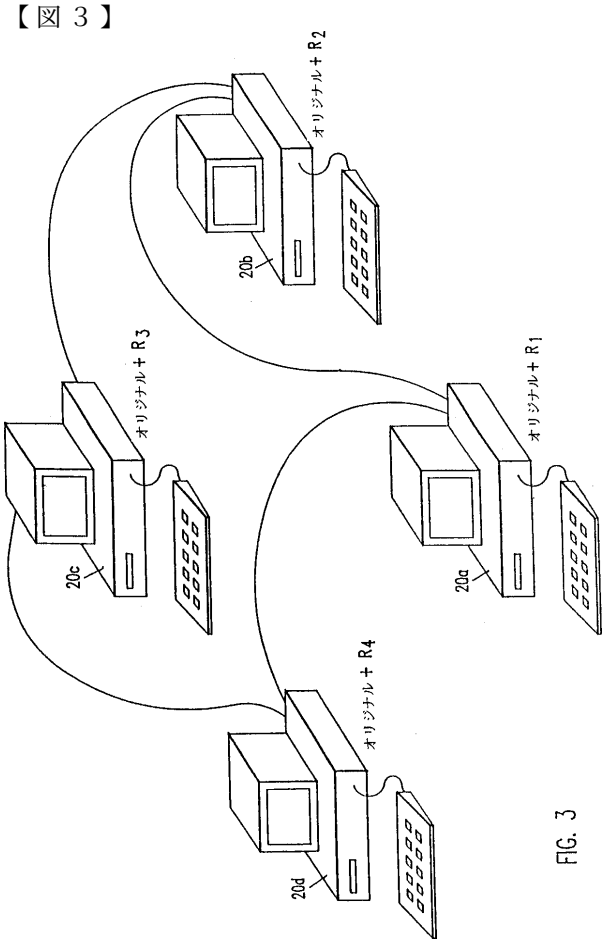

FIG. 3

フロントページの続き

(73)特許権者
ペレルソン、アラン　エス.
アメリカ合衆国　８７５０１　ニューメキシコ州　サンタフェ　ロス　アルボレス　レイン　８２０
(74)代理人
弁理士　三好　秀和
(72)発明者　アレン、ローレンス　スィー. 、ザ　サード
アメリカ合衆国　８７０５９　ニューメキシコ州　ティヘラス　テソロテ　ロード　５６
(72)発明者　フォレスト、スティファニー
アメリカ合衆国　８７１０６　ニューメキシコ州　アルバカーキ　アムハースト　エヌ. イー. ４４０
(72)発明者　ペレルソン、アラン　エス.
アメリカ合衆国　８７５０１　ニューメキシコ州　サンタフェ　ロス　アルボレス　レイン　８２０

審査官　久保　光宏

(56)参考文献　特開平４－１３９５３４（ＪＰ，Ａ）
特開平６－３３７７８１（ＪＰ，Ａ）
特開平６－３３４６４８（ＪＰ，Ａ）
特開平４－３３８８２３（ＪＰ，Ａ）
岡本栄司，「暗号技術の応用　認証、零知識証明方式」，ｂｉｔ，日本，共立出版株式会社，１９９１年１２月　１日，Vol.23，No.13，pp.99-111，ISSN:0385-6984
Tom Madej，”AN APPLICATION OF GROUP TESTING TO THE FILE COMPARISON PROBLEM”，Proc. of 1989 IEEE 9th Int. Conf. on Distributed Computing Syatems，１９８９年，pp.237-243，JST資料番号：C0487B
W. KENT FUCHS，et.al.，”Comparison and Diagnosis of Large Replicated Files”，IEEE Transactions on Software Engineering，１９８７年，Vol.SE-13，No.1，pp.15-22，JST資料番号：D0480D，ISSN:0098-5589

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G06F　9/06
G06F 12/00
G06F 12/14
G09C　1/00
H04L　9/32
JSTファイル(JOIS)
CSDB(日本国特許庁)
WPI/L(DIALOG)
INSPEC(DIALOG)