

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014年2月13日(13.02.2014)



(10) 国際公開番号
WO 2014/024265 A1

- (51) 国際特許分類:
H04L 9/14 (2006.01) G06F 21/62 (2013.01)
G06F 17/50 (2006.01)
- (21) 国際出願番号: PCT/JP2012/070143
- (22) 国際出願日: 2012年8月8日(08.08.2012)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人(米国を除く全ての指定国について): 株式会社日立製作所(HITACHI, LTD.) [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目6番6号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 塩野谷 友隆(SHIONOYA Tomotaka) [JP/JP]; 〒1858601 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所 中央研究所内 Tokyo (JP). 勝 康夫

(SUGURE Yasuo) [JP/JP]; 〒1858601 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所 中央研究所内 Tokyo (JP).

(74) 代理人: 井上 学, 外(INOUE Manabu et al.); 〒1008220 東京都千代田区丸の内一丁目6番1号 株式会社日立製作所内 Tokyo (JP).

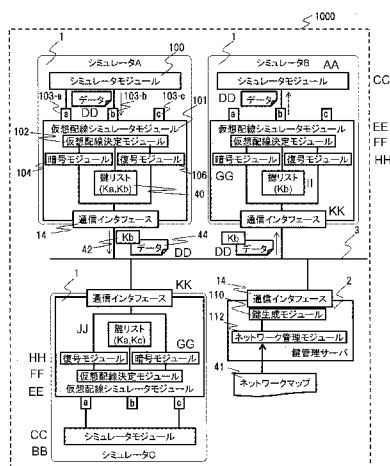
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

(54) Title: METHOD FOR COMMUNICATION BETWEEN SIMULATORS, AND SIMULATION SYSTEM

(54) 発明の名称: シミュレータ間の通信方法およびシミュレーションシステム

[図1]



- 1 Simulator A
- 2 Key management server
- 14, KK Communication interface
- 40 Key list (Ka, Kb)
- 41 Network map
- 44, DD Data
- 100, CC Simulator module
- 101, EE Virtual connection simulator module
- 102, FF Virtual connection determination module
- 104, GG Encryption module
- 106, HH Decryption module
- 110 Key generation module
- 112 Network management module
- AA Simulator B
- BB Simulator C
- II Key list (Kb)
- JJ Key list (Ka, Kc)

(57) Abstract: In a test which uses simulators corresponding to each component to be simulated, communication between components can be easily observed and therefore protecting information that should be concealed is becoming difficult. The present invention solves the above problem by, in communication between simulators operating upon a plurality of information processing devices connected with a network, providing for each simulator a set of keys corresponding to virtual connections of each simulator to other simulators, whereupon a first simulator among the plurality of simulators, when transmitting data to one among the virtual connections to the first simulator, encrypts the data with a key corresponding to the one connection among the set of keys provided to the first simulator, and transmits the encrypted data to the network.

(57) 要約: シミュレーション対象の各コンポーネントに対応するシミュレータを用いたテストにおいては、コンポーネント同士の通信が容易に観測可能であるという点において、秘匿されるべき情報の保護が困難になっている。本発明は、ネットワークで接続されている複数の情報処理装置上で動作するシミュレータ間の通信において、各シミュレータに、各シミュレータが接続される他のシミュレータへの仮想配線に対応する鍵のセットを与え、複数のシミュレータの内の第1シミュレータが、データを第1シミュレータに接続されている仮想配線の内の一に送信する際に、第1シミュレータに与えられている鍵のセットの内、該一に対応する鍵で該データを暗号化し、ネットワークに送信することで、前述の課題を解決する。



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

シミュレータ間の通信方法およびシミュレーションシステム

技術分野

[0001] 本発明は、ソフトウェア上でハードウェアの動作を模擬的に試験するシミュレーションに係り、特にシミュレータ同士の通信に関する。

背景技術

[0002] 近年のハードウェアライフサイクルの短ピッチ化に伴って、ハードウェアを構成するコンポーネントあるいはハードウェアそのもののテスト工程の短期間化が求められている。その一方で、ハードウェアに対する機能要求が高まっており、よしんば故障したとしても安全に停止、あるいは安定状態になるまで継続駆動するためのフェイルオーバ性やフォールストレラント性が重視される傾向にあり、テスト項目数は増加している。かといって、ハードウェアの中には車両や工具機器といった大型な機器も含まれるため、テスト品質の低下によるテスト工程の短期間化は許容されない。

[0003] こうした背景において、手戻りの発生が多い初期テスト段階において、シミュレータを用いたテストが一般化してきている。しかしながら、従来のハードウェアを用いたテストと異なり、シミュレータを用いたテストにおいては、コンポーネント同士の通信が容易に観測可能であるという点において、秘匿されるべき情報の保護が困難になっている。コンポーネントが有するノウハウは、企業にとっての生命線であるため、これらの情報が危険にさらされるシミュレーション環境は極めて利用可能性の低いものとなる。

[0004] コンピュータ間の通信を隠蔽する技術として、特許文献1に記載されている技術がある。

先行技術文献

特許文献

[0005] 特許文献1：国際公開第2008／146639号

発明の概要

発明が解決しようとする課題

[0006] 特許文献1記載の技術は、プロジェクト管理サーバをネットワークに接続し、そのプロジェクト管理サーバが、ユーザが属するプロジェクトに基づいてネットワークに接続しているコンピュータに通信用の鍵を配布し、それぞれのコンピュータあるいはそのコンピュータ上で動作している仮想マシンが配布された鍵を用いて通信することで、プロジェクトグループごとに秘匿された通信を実現するものである。しかしながら、テストの対象となるコンポーネントやハードウェアのそれぞれに対応するシミュレータに対してプロジェクトグループによる管理を適用すると、プロジェクトに対する鍵によるプロテクトが突破されると、すべてのシミュレータ間の通信が漏えいする。これを防ぐためにはプロジェクト管理サーバのプロテクトをより強固にする必要があり、運用コストが増加してしまう。

[0007] 本発明は上記課題を鑑みて為されたものであって、シミュレータ間の通信の秘匿性の向上を目的としている。

課題を解決するための手段

[0008] 本発明は、ネットワークで接続されている複数の情報処理装置上で動作するシミュレータ間の通信において、各シミュレータに、各シミュレータが接続される他のシミュレータへの仮想配線に対応する鍵のセットを与え、複数のシミュレータの内の第1シミュレータが、データを第1シミュレータに接続されている仮想配線の内の一に送信する際に、第1シミュレータに与えられている鍵のセットの内、該一に対応する鍵で該データを暗号化し、ネットワークに送信することで、前述の課題を解決する。

発明の効果

[0009] 仮想配線に対応する鍵セットによるプロテクトにより、仮想配線毎に鍵で通信が秘匿化され、シミュレータ間の通信の秘匿性が向上する。

図面の簡単な説明

[0010] [図1]本発明の実施例であるシミュレーションシステムの機能ブロック図である。

[図2]本発明の実施例であるシミュレーションシステムに含まれるシミュレータ装置の一例を示す図である。

[図3]本発明の実施例であるシミュレーションシステムに用いられる鍵リストの一例を示す図である。

[図4]本発明の実施例であるシミュレーションシステムに含まれる鍵管理サーバ装置の一例を示す図である。

[図5]ネットワークマップの例を示す図である。

[図6]鍵管理サーバによる初期鍵発行処理の一例を示す図である。

[図7]データ送信処理の実装例を示す図である。

[図8]データ受信処理の実装例を示す図である。

[図9]本発明の実施例であるシミュレーションシステムに適用可能な鍵変更手順の一例を示す図である。

[図10]本発明の実施例であるシミュレーションシステムに適用可能な外乱の付与手順の一例を示す図である。

[図11]本発明の実施例であるシミュレーションシステムに適用可能な外乱管理に用いる表の一例を示す図である。

[図12]本発明の実施例であるシミュレーションシステムに適用可能な鍵管理方法の一例を示す図である。

[図13]データ受信処理の実装例を示す図である。

[図14]本発明の実施例であるシミュレーションシステムに適用可能な鍵分割割当て手順の一例を示す図である。

発明を実施するための形態

実施例 1

[0011] 本明細書においては同一番号が割り当てられた構成要素は同一の構成要素を表す。また、バリエーションがある構成要素に関しては、1-a、1-bのように、“-”とアルファベット一文字で同種だが異なる役割を果たす構

成要素であることを表す。

[0012] 図1は、本発明の実施例であるシミュレーションシステム1000の機能ブロック図である。シミュレーションシステム1000は、1台以上のシミュレータ1と1台の鍵管理サーバ2がネットワーク3を接続した回路上で実現される。図1では、説明の簡単化のために、シミュレーションシステム1000は、シミュレータA、シミュレータB、およびシミュレータCの3台のシミュレータ1を有するとして説明する。

[0013] シミュレーションシステム1000の環境を構築するための装置については、図2、3を用いて説明する。図2は、シミュレータ1を実現するシミュレータ装置1'の構成例を示す図である。シミュレータ装置1'は、プロセッサ装置10と、メモリ装置12と、通信インタフェース14と、これらの構成要素を接続する通信バス16と、を有する装置である。シミュレータ装置1'は、情報処理装置であり、例えばサーバ装置である。

[0014] 通信インタフェース14は、ネットワーク3を介して接続された他の装置に対して命令及びデータ44を送信、或いは当該他の装置からの命令及びデータ44を受信するための装置である。このネットワーク3は、物理的なケーブルで実現してもよいし、無線技術を用いて実現してもよい。また、ネットワーク3をローカルエリアネットワーク(Local Area Network)やワイドエリアネットワーク(Wide Area Network)などを利用して実現してもよい。通信インタフェース14は必ずしも各シミュレータ装置1'に1台である必要はなく、ネットワーク3の種類が多岐に渡る場合、それらに対応した通信インタフェース14を複数搭載しても構わないし、専用のネットワーク3の確保などを目的として、同一ネットワーク3に複数の通信インタフェース14を接続しても構わない。以降、シミュレータ1と他の装置の間におけるデータ44の送受信において特に断りがない場合は、暗黙的に通信インタフェース14とネットワーク3を介して送受信を実現することとする。

[0015] プロセッサ装置10は、メモリ装置12に格納されているプログラムを実

行、あるいはメモリ装置 12 に対するデータ 44 を読み書きする装置である。プロセッサ装置 10 は、各シミュレータ装置 1' に複数台搭載されていても構わない。

[0016] メモリ装置 12 は、装置が使用する処理手段を格納および情報を記憶するための装置であり、モジュール本体など、モジュール実行中には内容の書換が強く制限されるモジュール領域 60 と、モジュールが扱う一時データなど、モジュール実行中において適切に内容が書き換えられるデータ領域 61 とを内包している。但し、これらの領域を必ずしも全ての状態で実現する必要はなく、便宜上図示しているにすぎないことに注意すべきである。

[0017] メモリ装置 12 には、ダイナミックラム (DRAM) などの揮発メモリによって構成される高速な読み書きが可能な記憶装置が適用されるが、アプリケーションが許すならば、ハードディスクドライブや SSD (Solid State Disk) などの不揮発性の大容量記憶装置を適用してもよいし、または CD-R (Compact Disk Recordable) などのライトワンスメディアを適用しても構わない。また、メモリ装置 12 は、単一の装置から構成されている必要は無く、複数台、複数種の記憶装置を RAID (Redundant Arrays of Inexpensive Disks) のような並列構成あるいは JBOD (Just a Bunch Of Disks) のような直列構成に接続して実現しても構わない。

[0018] メモリ装置 12 のモジュール領域 60 には、コンポーネントの挙動をシミュレートするシミュレータモジュール 100 とコンポーネント間の通信をシミュレートするための仮想配線シミュレータモジュール 101 とが格納されている。仮想配線シミュレータモジュール 101 は、仮想的な通信路 (仮想配線 42' (図 1 には図示せず)) のうち、使用する仮想配線 42' を決定する仮想配線決定モジュール 102 と、仮想配線 42' に送信する情報を暗号化する暗号モジュール 104 と、前記暗号モジュール 104 によって暗号化された情報を復号し、情報の参照を実現するための復号モジュール 106

と、を含む。

[0019] 一方、データ領域 6 1 には、シミュレータ間の通信で用いられる暗号鍵 4 2 を含む鍵リスト 4 0 が格納されている。また、データ領域 6 1 には、シミュレータ間で通信されるデータ 4 4 が格納される。

[0020] 鍵リスト 4 0 の構成例を図 3 に示す。鍵リスト 4 0 は、各シミュレータが用いる暗号鍵 4 2 の一次元の配列として実装され、図 3 の例では先頭から K a、K b、K c の順序で格納されている。ただし、これはあくまで実装の一例であり、暗号鍵 4 2 のそれぞれに対して一意に識別するためのキーと、キーをアドレスに指定する関数による連想配列などを用いてもよいし、順序性を持たない集合として扱ってもよいし、必要があればキューやスタックといった、参照・格納順に制約を設けたデータ構造で実装しても構わない。いずれにせよ、鍵リスト 4 0 に対して、キーを用いた暗号鍵参照は有限の時間で完了されればよい。

[0021] これらのモジュールあるいはデータ 4 4 はメモリ装置 1 2 に常に格納されている必要はなく、実行する際にネットワーク 3 を介して接続されたストレージ装置などの別の装置からロードされても構わないし、コンパイルモジュールを有する状態であれば、実行する際にプロセッサ装置 1 0 が解釈できるネイティブコードにソースファイルから変換して、メモリ装置 1 2 に配置しても構わない。メモリ装置 1 2 に格納されている各モジュールに関しては、各構成要素の説明後別途説明する。

[0022] 通信バス 1 6 は、シミュレータ 1' 装置内の構成要素間でのデータ 4 4 の送受信を実現するための装置であり、CPUバスやアドレスバスなどの内部バスと Serial ATA や PCI Express などの拡張バスを接続して構成される装置である。有線の通信バスの例を挙げたが、配線の簡素化などを目的として無線で通信バス 1 6 を構成しても構わない。以降、メモリ装置 1 2、プロセッサ装置 1 0、及び通信インタフェース 1 4 間の通信において特に断りが無い場合は、暗黙的に通信バス 1 6 を介して送受信を実現する。

＜各モジュールの説明＞

以下、メモリ装置１２に格納される各モジュールについて説明する。

- [0023] シミュレータモジュール１００は、コンポーネントの状態や信号の送受信を、モジュール内部の状態変化やＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍ Ｉｎｔｅｒｆａｃｅ）の呼び出しなどで代替し、ソフトウェア上でコンポーネントの動作を模擬的に実行するモジュールである。このシミュレータモジュール１００が有する内部的情報や通信状況は企業ノウハウを多分に含んでいる。本実施例のシミュレーションシステム１０００では、シミュレータモジュール１００同士の通信を、仮想配線４２'を介して行うことで、仮想配線４２'に接続されていない他のシミュレータモジュール１００やシミュレーションシステム１０００に含まれないアプリケーションに対してデータ４４が隠蔽される。仮想配線４２'を実現するためのモジュールが、次に説明する仮想配線シミュレータモジュール１０１である。
- [0024] 仮想配線シミュレータモジュール１０１は、複数のＡＰＩ１０３を有するモジュールである。ＡＰＩ１０３－ａ，ｂ，ｃ・・・のそれぞれは、コンポーネントに接続されている配線のそれぞれに対応する。シミュレータモジュール１００は、その通信の用途に応じて自身が生成した信号をいずれかのＡＰＩ１０３に選択して入力する。
- [0025] 仮想配線決定モジュール１０２は、復号モジュール１０６によって復号された信号が正しく復号されているかどうか、確認するためのモジュールである。こうした復号の確認は、例えばチェックサムを用いる方法などが挙げられる。
- [0026] 暗号モジュール１０４は、入力された信号を一定の規則に従って変換し、復号手段を持たない装置から情報を抽出できなくするモジュールである。暗号には暗号表を用いた文字列置換方法や、素因数分解などの一方向性関数がある、逆関数の計算が困難であることを利用した変換方法を用いてもよい。
- [0027] 復号モジュール１０６は、入力された信号を一定の規則に従って変換し、

別の信号に変換するモジュールである。ここで注意すべきは、復号モジュール 106 自身は復号が成功したかどうか判定せず、入力された信号をただ規則に従って変換し出力するモジュールであることである。

- [0028] 鍵リスト 40 は、暗号モジュール 104 と復号モジュール 106 によってそれぞれ参照される、暗号化に用いる暗号鍵 42 を番号づけて管理したデータである。以降、本明細書においては、鍵リスト 40 中の i 番目の暗号鍵 42 は K_i と表現する。暗号モジュール 104 が K_i を用いて暗号化した情報は復号モジュール 106 が K_i を用いて暗号化前の情報として復号可能であると、また、異なる暗号鍵 K_j ($i \neq j$) では復号し得ないものとする。

<鍵管理サーバ装置 2' の説明>

図 4 に、鍵管理サーバ 2 を実現する鍵管理サーバ装置 2' の構成例を示す。鍵管理サーバ装置 2' はシミュレータ装置 1' と同じくプロセッサ装置 10 と、メモリ装置 12 と、通信インタフェース 14 と、これらの構成要素を接続する通信バス 16 と、を有する装置である。鍵管理サーバ装置 2' は、情報処理装置であり、例えばサーバ装置である。

- [0029] それぞれの装置の動作はシミュレータ装置 1' を構成する装置と同等であるため、説明を省略する。

<各モジュールの説明>

鍵管理サーバ装置 2' のメモリ装置 12 に格納されるモジュールについて説明する。鍵生成モジュール 110 は、シミュレータ 1 が情報を暗号化あるいは復号する際に使用する暗号鍵 42 を生成するモジュールである。鍵生成モジュール 110 によって発行される暗号鍵 42 は、少なくともシミュレーション環境に実現される仮想配線 42' にそれぞれユニークな値が割り振られるように構築されるようにする。

- [0030] ネットワーク管理モジュール 112 は、ネットワークマップ 41 を参照し、仮想配線 42' を定義するモジュールである。仮想配線 42' とは、コンポーネント同士の配線による接続を仮想的に記録した情報である。具体的には、仮想配線 42' は、あるコンポーネントと接続している全てのコンポー

ネットの識別情報（ID）の集合として定義される。特にこの集合のサイズが2の場合、2つのコンポーネントはそれぞれが相互に接続され、また他のコンポーネントが接続されていない1：1の関係として接続されていることが示される。

[0031] ネットワークマップ41は、こうした仮想配線42'を人間が可視しやすい情報として記録された情報である。回路図のように幾何的に表されていてもよいし、何らかの言語で記述されていてもよい。

[0032] シミュレータ装置1'および鍵管理サーバ装置2'をそれぞれネットワーク接続し、起動することで、各装置のモジュールが相互に連携し、図1に示したようなシミュレーション環境が実現される。

<シミュレータの接続>

図1に示したシミュレーション環境において、鍵管理サーバ2が仮想配線42'を定義し、シミュレータの接続を確立する手順を説明する。

[0033] 図5は、ネットワークマップ41の一例であり、図1に示したシミュレーション環境に対応したものである。図5のネットワークマップ41においては、3つのシミュレータ1が有するシミュレータモジュール100のそれぞれによってシミュレートされる3つのコンポーネント100'が、仮想バスA、仮想バスB、及び仮想専用線の3本の仮想配線42'で接続されている。このように、仮想配線42'には、コンポーネントを接続する仮想バス及び仮想専用線が含まれる。また、有線配線ではなく、ワイヤレスLANのように無線配線を含んでいてもよい。また、コンポーネントAはシミュレータAで、コンポーネントBはシミュレータBで、コンポーネントCはシミュレータCで、それぞれ模擬される。すなわち、各シミュレータは、シミュレーション対象の各コンポーネントに対応している。

[0034] 図6は、シミュレーション環境において初期状態を構成するための初期鍵発行処理S1の一例をフローチャートで示したものである。ステップS11では、鍵管理サーバ2のネットワーク管理モジュール112は、ネットワークマップ41を走査し、仮想配線42'のそれぞれに識別情報（ID）を割

当てる。ステップS 1 2では、鍵管理サーバ2のネットワーク管理モジュール1 1 2は、ネットワーク3に接続している全てのシミュレータ1とそれぞれセキュアなセッションを構築する。

[0035] ステップL 1 0～L 1 1では、全ての仮想配線4 2' に対して以下のステップS 1 3、S 1 4を実行する。ステップS 1 3では、仮想配線4 2' に対して鍵管理サーバ2の鍵生成モジュール1 1 0がユニークな暗号鍵4 2を生成する。ステップS 1 4では、鍵管理サーバ2の鍵生成モジュール1 1 0は、対象の仮想配線4 2' に接続している全てのシミュレータ1に、ステップS 1 3で生成した鍵を送信する。以上のステップで、鍵管理サーバ2は、シミュレータ間の仮想配線4 2' による接続に対応付けられた暗号鍵4 2のセットを各シミュレータ1に送信する。

[0036] 図5に示した例では、シミュレーション環境は3本の仮想配線4 2' を有している。以降、便宜上、図5の仮想専用線を仮想配線4 2' -aと、仮想バスAを仮想配線4 2' -bと、仮想バスBを仮想配線4 2' -cと、それぞれ呼ぶ。図1および図5に示したシミュレーション環境においては、仮想配線4 2' -aに対して独自の暗号鍵4 2であるK aが発行され、また、仮想配線4 2' -aに対して、仮想配線シミュレータモジュール1 0 1が、API 1 0 3-aを割当てる。仮想配線4 2' -b、cに対しても同様に、独自の暗号鍵4 2であるK b、K cがそれぞれ発行され、また、仮想配線4 2' -b、cに対して、仮想配線シミュレータモジュール1 0 1が、API 1 0 3-b、cをそれぞれ割当てる。図1および図5に示したシミュレーション環境においては、シミュレータAは仮想配線4 2' -a、bに、シミュレータBは仮想配線4 2' -bに、シミュレータCは仮想配線4 2' -a、cにそれぞれ接続されている。これを実現するため各シミュレータ1のシミュレータモジュール1 0 0は、自身が有する各配線への入出力信号を、各シミュレータ1の仮想配線シミュレータモジュール1 0 1のAPI 1 0 3にそれぞれ接続する。

[0037] 図1に示した例では、シミュレータAの鍵リスト4 0には、K aとK bが

含まれ、シミュレータ A のシミュレータモジュール 100 は、仮想配線シミュレータモジュール 101 の API 103-a、b に接続されている。シミュレータ B の鍵リスト 40 には、K b が含まれ、シミュレータ B のシミュレータモジュール 100 は、仮想配線シミュレータモジュール 101 の API 103-b に接続されている。また、シミュレータ C の鍵リスト 40 には、K a、K c が含まれ、シミュレータ C のシミュレータモジュール 100 は、仮想配線シミュレータモジュール 101 の API 103-a、c に接続されている。このように、各シミュレータ 100 の鍵リスト 40 に、暗号鍵 42 のセットが配置される。

[0038] 鍵管理サーバ 2 は、上述のようにネットワークマップ 41 はメモリ装置 12 に保持しているが、生成した暗号鍵 42 はメモリ装置 12 に保持しない。これにより、鍵管理サーバ 2 のプロテクトが突破された場合でも、シミュレーションシステム 1000 に配置されている鍵 42 が読み取られることを防ぐことができる。

[0039] シミュレーションシステム 1000 のデータ 44 の送受信方法を、図 7、8 を用いて説明する。図 7 は、データ送信処理 S5 の実装例である。ステップ S51 では、仮想配線決定モジュール 102 は、自身が有する API 103 を監視し、シミュレータモジュール 100 から送信されてくる信号を検知する。ステップ C51 では、仮想配線決定モジュール 102 は、信号を受信した API 103 に対応した暗号鍵 42 が鍵リスト 40 に格納されているか確認する。

[0040] ステップ C51 で API 103 に対応する暗号鍵 42 である K i が鍵リスト 40 に格納されている場合、ステップ S52 で、仮想配線決定モジュール 102 は API 103 から取得したデータ 44 を暗号モジュール 104 に渡し、暗号モジュール 104 は K i を用いてデータ 44 を暗号化する。さらに、ステップ S53 で、暗号モジュール 104 は、暗号化したデータ 44 を通信インタフェース 14 を介し、接続しているネットワーク 3 にブロードキャストする。そして、ステップ S510 で、データ送信処理 S5 を終了する。

- [0041] ステップC 5 1でA P I 1 0 3に対応する暗号鍵4 2であるK iが鍵リスト4 0に格納されていない場合、ステップS 5 4で、仮想配線決定モジュール1 0 2は受信したデータ4 4を破棄し、続いて、ステップS 5 1でA P I 1 0 3の監視を再開する。
- [0042] 次に、データ4 4の受信処理について説明する。
- [0043] 図8は、データ受信処理S 6の実装例である。ステップS 6 1で、復号モジュール1 0 6は、通信インタフェース1 4を介して、暗号化されたデータ4 4を受信する。ステップS 6 2で、復号モジュール1 0 6は、受信した暗号化されたデータ4 4を、自身が属するシミュレータ1に与えられて鍵リスト4 0に含まれている暗号鍵4 2を用いて、復号することを試みる。本実施例においては、この復号処理を鍵リスト4 0に含まれている全ての暗号鍵4 2について並列実行することで、同クロックに復号されたデータ4 4を取得することを期待しているが、それぞれの復号処理が十分短時間で終了し、鍵リスト4 0の最初と最後に格納された暗号鍵4 2を用いた復号結果が同時に終了したとみなせるのであれば、逐次的処理で実装しても構わない。ステップS 6 3で、仮想配線決定モジュール1 0 2は、それぞれの復号処理を施されたデータ4 4の復号成功可否を判定する。
- [0044] ステップC 6 1で復号に成功したデータ4 4がある場合、ステップS 6 4で、復号に成功した暗号鍵4 2に対応するA P I 1 0 3の出力信号を変更し、データ受信処理S 6を終了する（ステップS 6 1 0）。これにより、シミュレータ1は復号されたデータ4 4を受信することができる。一方、ステップC 6 1で復号に成功したデータ4 4がない場合、ステップS 6 1 0でデータ受信処理S 6を終了する。
- [0045] データ送信処理S 5とデータ受信処理S 6の2つの処理を用いて、各シミュレータモジュール1 0 0は、仮想配線4 2' 上での通信を実現する。各シミュレータ1から他のシミュレータ1に送信されるデータ4 4はブロードキャストで発行され、受信するシミュレータ1が受信可否を決定するため、仮想配線4 2' に送信されたデータ4 4は、その仮想配線4 2' に接続されて

いる機器を模したシミュレータ全てにほぼ同時に到着する。このほぼ同時にデータ 4 4 が到着する特長は、それぞれが独自のクロックで動作する複雑なコンポーネントの組合せのシミュレーションにとって有用である。

[0046] なお、各シミュレータモジュール 1 0 0 は、元来接続する必要のない仮想配線 4 2' に接続してもよい。例えば図 1 および図 5 の例では、シミュレータ C が、仮想配線シミュレータモジュール 1 0 1 が提供する A P I 1 0 3 - b に接続してもよい。なぜなら、仮想配線 4 2' - b を流れるデータ 4 4 を暗号化している K b が鍵管理サーバ 2 によってシミュレータ C には発行されていないため、シミュレータ C は観測している情報を復号できないため、結果的に、仮想配線 4 2' - b からは断絶される。

[0047] 一方、他のシミュレータモジュール 1 0 0 の妨害などを目的として、接続する必要のない仮想配線 4 2' に対して、無作為に情報を流すような場合においては、送信元のシミュレータ 1 の鍵リスト 4 0 に、対応する暗号鍵 4 2 が無い限り、ネットワーク 3 への情報送信が許可されない。よしんば、暗号鍵 4 2 が無い状態でのデータ 4 4 送信が許容される様態であったとしても、その場合は、受信側が正しく復号できないため、データ 4 4 は受理されず破棄される。これらの処理によって、本発明によるシミュレーション方法においては、データ 4 4 の隠ぺいと、安全性を確保する。

[0048] 本実施例のシミュレーションシステムでは、各仮想配線に対してユニークな鍵が与えられる。したがって、仮にそのうちの一つの鍵によるプロテクトが突破されたとしても、すべてのシミュレータ間の通信が漏えいすることにはならない。このように、本実施例のシミュレーションシステムは、高い安全性を提供することができる。

実施例 2

[0049] 実施例 1 で説明したシミュレーションシステムで各仮想配線に対して与えられている鍵毎に、鍵交換をして鍵を更新し、さらに高い安全性を実現する実施例を説明する。

<鍵交換処理>

実施例 1 では、データ 4 4 の送受信の安全性について説明したが、その中で説明したように任意のシミュレータ 1 は、自身が接続していない仮想配線 4 2' 上のデータ 4 4 を受信することが可能である。それぞれのシミュレータ 1 は仮想配線シミュレータモジュール 1 0 1 によって、復号確認の手段を有しているため、ブルートフォースアタックなどの暗号突破手段を用いれば、一定の計算量で任意の仮想配線 4 2' 上のデータ 4 4 を復号可能である。そこで、本実施例においては鍵交換プロセスによるセキュリティレベルの担保について説明する。

[0050] 図 9 に、図 1 に示したシミュレーション環境に適用可能な鍵交換処理の一例として、鍵交換処理 S 7 を示す。各シミュレータ 1 がある時刻において、鍵リスト 4 0 に格納している暗号鍵 4 2 をカッコ内に示す。また、ブロードキャストについては実線の矢印で示すのに対して、対象を指定するユニキャストあるいはマルチキャストに関しては、一点鎖線の矢印を用いて表現する。

[0051] 初期状態においては、図 1 で説明した状態と同様である。以下、仮想配線 4 2' - b に接続するための暗号鍵 4 2 である K b を異なる鍵 K b' に変更するプロセスを示す。

[0052] 既に述べたように、鍵管理サーバ 2 は自身のプロテクトが突破された際に全ての暗号鍵 4 2 が読みとられることを防止するために、仮想配線 4 2' に接続されているシミュレータ 1 についてはネットワークマップ 4 1 に記録しているが、その仮想配線 4 2' に接続するための暗号鍵 4 2 は記録していない。

[0053] そこで、鍵管理サーバ 2 は、暗号鍵 4 2 の取得を実施するために、ネットワークマップ 4 1 を参照し、対象とする仮想配線 4 2' に接続している任意のシミュレータ 1（本実施例においてはシミュレータ A）に対して、暗号鍵 4 2 である K b の変更要求を発行する（P 7 1）。K b の変更要求を受信したシミュレータ A は、鍵管理サーバ 2 に K b を送信する（P 7 2）。このプロセスは例えば公開鍵交換プロセスなどの十分セキュアなアルゴリズムで実

現すればよい。鍵管理サーバ2は、鍵生成機能を用いてK bに換わるK b'を生成する(S 7 2 1)。

[0054] 鍵管理サーバ2は、生成したK b'を暗号鍵4 2であるK bを用いて暗号化しブロードキャストする(P 7 3)。このプロセスによって、K b'を取得できるのはK bをあらかじめ有している、シミュレータA、Bのみである。それぞれのシミュレータ1は、K b'を受信したことを鍵管理サーバ2にユニキャストする(P 7 4)。鍵管理サーバ2は、ネットワークマップ4 1を参照し、仮想配線4 2' - bに接続しているすべてのシミュレータ1がK b'を受信したかどうかを確認できるまで、すなわちP 7 4での各シミュレータ1からのユニキャストの送信を受信できるまで、次の処理を待機する(S 7 2 2)。この処理によって、鍵交換処理S 7によって仮想配線4 2'からシミュレータ1が除外されることを防止することができる。

[0055] 鍵管理サーバ2は、暗号鍵4 2であるK bを用いて鍵変更指示をブロードキャストする(P 7 9)。鍵変更の指示を復号できたシミュレータ1は、鍵リスト4 0に格納されている、該当する暗号鍵4 2であるK bをK b'に変更する(S 7 1 1)。以降、シミュレーション環境において、K bは無効となる。最後に、鍵管理サーバ2は、鍵管理サーバ2内にあるK bを破棄し、鍵交換処理S 7を終了する(S 7 2 3)。

実施例 3

[0056] 昨今のハードウェアテストにおいては、故障時のフェイルオーバー性やフォールストレラント性の確認も要求されている。故障の一つとして、配線の故障による送受信信号の変化あるいは断絶がある。本実施例においては、実施例2で説明した鍵交換処理を用いて、配線故障をシミュレーションする方法について説明する。

[0057] 図1 0に、実施例2で説明した鍵交換処理S 7を用いて配線故障シミュレーションを実現する処理のシーケンスの一例として、鍵交換処理S 7'を示す。実施例2の鍵交換処理S 7と同様に、鍵管理サーバ2は鍵変更(K bに対して)を要求し(P 7 1)、任意のシミュレータ1(図1 0ではシミュレ

ータ 1 A) が対象となる暗号鍵 4 2 (K b) を鍵管理サーバ 2 に送信し (P 7 2)、その後鍵管理サーバ 2 が新たな暗号鍵 4 2 (K b') を生成する (S 7 2 1)。

[0058] P 7 3' からが実施例 2 の鍵交換処理 S 7 と異なる処理である。実施例 2 では新しい暗号鍵 4 2 (K b') を古い暗号鍵 4 2 (K b) を用いて暗号化し、ブロードキャストしていたが、本実施例では任意のシミュレータ 1 にユニキャストあるいはマルチキャストする (P 7 3')。新しい暗号鍵 4 2 を受信し、復号できたシミュレータ 1 (図 10 ではシミュレータ A) は、実施例 2 の鍵交換処理 S 7 と同様に、K b' の受信確認を鍵管理サーバ 2 に送信する (P 7 4)。その一方で、鍵管理サーバ 2 は、生成した新しい暗号鍵 4 2 (K b') にノイズ N を加えて、K b'' を生成する (S 7 2 1)。

[0059] この K b'' の特徴は次の (1)、(2) の 2 つである。(1) K b' とノイズ N を用いて一意に生成可能である。(2) K b' で暗号化されたデータ 4 4 を K b'' で復号した際、復号成功と判定されるが、元データ 4 4 が正しく取得できることは保証されない。

[0060] このような K b'' の特性を実現するには、例えば排他的論理和 (XOR) を使ってデータ 4 4 を変換する方法などを用いればよい。例えば、8 ビットのデータ 4 4 に対して 8 ビットの復号成功信号を末尾に付与し、16 ビットの暗号鍵 4 2 の K' と XOR した結果を暗号化されたデータ 4 4 とする方法においては、8 ビットのノイズ N を生成し、K' の上位 8 ビットと XOR 演算などの論理演算を施すことで、上述の (1) と (2) の特徴を実現する K b'' を提供できる。

[0061] 鍵管理サーバ 2 は、P 7 3' で暗号鍵 4 2 である K b' を送付しなかったシミュレータ 1 (図 10 ではシミュレータ B) に、ノイズ N を付与した暗号鍵 4 2 である K b'' を K b で暗号化し、ユニキャストもしくはマルチキャストする (P 7 5)。K b'' を受信したシミュレータ B は、受信確認を鍵管理サーバ 2 へ送信する (P 7 6)。P 7 4 と P 7 6 により、実施例 2 と同様に、鍵管理サーバ 2 が、仮想配線 4 2' - b に接続しているシミュレータ 1 の

全てが暗号鍵42を受信できたかを確認できる(S722)。その後、鍵管理サーバ2は、実施例2と同様に、各シミュレータ1に鍵の変更を指示し(P79)、元の暗号鍵42であるKbを破棄する(S723)。

[0062] 鍵管理サーバ2は、ノイズNを、ノイズNを与えた仮想配線42'とシミュレータ1を一意に特定できる情報とともに、鍵管理サーバ装置2'のメモリ装置12に格納しておく。格納方法の一例としてノイズデータベース30を図11に示す。ノイズデータベース30は、仮想配線42'とシミュレータ1がそれぞれID管理されている場合に、どのシミュレータ1の暗号鍵42にどのようなノイズNが付与されているか関連付けて記録するためのデータベースである。図11のノイズデータベースでは、仮想配線ID31、シミュレータID32、およびノイズ33の組をエントリとしており、仮想配線ID31には仮想配線42'-bを示す「b」が、シミュレータIDにはシミュレータBを示す「B」が、ノイズ33には8ビットのノイズNの「00010000」が格納されている。このノイズデータベース30を用いれば、再び仮想配線42'-bの暗号鍵42を変更する際に、受信したKb」とノイズNを参照し、Kb'を再度生成することで、シミュレータBに与えた配線故障を回復したり、他のシミュレータ1にノイズを付与したりするなどを実現できる。

[0063] 以上の処理により、一部にはノイズが付与された信号が到着あるいは発信されるシミュレータ1が仮想配線42'に接続され、配線故障を模擬することができる。すなわち、シミュレータ1に与えられた鍵のセットに含まれる鍵の一部の鍵を変更することで、通信故障を模擬することができる。この配線故障の導入は、実施例2の鍵交換と同様に行われるので、セキュリティのレベルを高く保ちつつ、実行することができる。

実施例 4

[0064] 実施例1では、シミュレーション環境において、各シミュレータ1に信号が到着する時刻の同時性について、述べてきた。しかしながら、実際のハードウェア回路においては、配線長に応じた到着時刻のズレや信号の立ち上が

りなどで個々のコンポーネントへの信号到着時刻に厳密には遅れが生じる。
こうした信号到着の遅れを模擬する方法を述べる。

[0065] 図12は、本実施例の鍵リスト40の実現例である。図12の各暗号鍵42は、任意の数に分割され、分割されて記録される。ここで、 K_n の部分暗号鍵である $K_{n,1} \sim K_{n,m}$ のそれぞれを暗号化されたデータ44に対して適用して逐次復号すれば、 K_n で復号されたものと同じデータ44が再現できるものとする。たとえば、8bitのXOR暗号鍵42を用いる実装においては、暗号鍵42を最大8個にまで分割し、各ビット情報を $K_{n,1}$ 、 $K_{n,2} \dots$ 、 $K_{n,8}$ として記録すればよい。これらの $K_{n,1} \sim K_{n,8}$ を暗号化されたデータ44にそれぞれXOR演算することで、元の暗号鍵42である K_n で復号したのと同様の復号結果を得られる。

[0066] なお、鍵リスト40に対してキーを用いて暗号鍵42を参照する際、任意の数に分割された暗号鍵42を集合として取得することができるのであれば、本実施例のように必ずしも2次元の配列として記録する必要はなく、それぞれが連想配列として記録されていてもよいし、順序を持たない集合として記録されていてもよい。

[0067] 図13に本実施例のデータ受信処理S6'を示す。本実施例においても、図8に示したデータ受信処理S6と同様に、受信されたデータ44は各暗号鍵42で並列復号されるが、この際に暗号鍵42が分割されている場合、逐次的に復号処理が実施される(S62')。各復号処理に係るクロックが同等であれば、2つに分割された暗号鍵42である K_b での復号は任意の分割されていない K_i での復号処理に比べて処理完了に2倍の時間を要する。この処理時間の違いが、ネットワーク遅延として再現される。

[0068] 図14に、鍵分割プロセスを含む鍵交換処理S7''を示す。実施例2および実施例3と同様に、鍵管理サーバ2が特定の仮想配線42' (図14では仮想配線42'-b) に属する任意のシミュレータ1 (図14ではシミュレータA) に対して、鍵変更を要求し、暗号鍵42である K_b を取得し(P72)、新しい暗号鍵42である K_b' を生成する(S721)。こうして生

成された新しい暗号鍵 4 2 である Kb' は第 3 実施例と同様に、一部のシミュレータ 1 に対して、ユニキャストあるいはマルチキャストされる (P 7 3')。新しい暗号鍵 4 2 を受信し、復号できたシミュレータ 1 (図 1 4 ではシミュレータ A) は、実施例 2 の鍵交換処理 S 7 と同様に、 Kb' の受信確認を鍵管理サーバ 2 に送信する (P 7 4)。

[0069] 次に、鍵生成モジュール 1 1 0 は、暗号鍵 4 2 (図 1 4 では Kb') を任意の数に分割する。分割数の決定は、ネットワークマップ 4 1 に記載された配線長などから決定してもよいし、各シミュレータ 1 のハードウェア的处理速度の違いなどから決定してもよい。そして、ネットワーク遅延を再現したいシミュレータ 1 (図 1 4 ではシミュレータ B) に対して、分割された鍵を送信する。分割された鍵を受信したシミュレータ B は、受信確認を鍵管理サーバ 2 へ送信する (P 7 8)。

[0070] 以降、実施例 2 および実施例 3 と同様に、仮想配線 4 2' - b に属するシミュレータ 1 全てに対して受信を確認し (S 7 2 2)、鍵変更を指示し (P 7 9)、古い暗号鍵 4 2 である Kb を破棄して (S 7 2 3)、鍵交換処理 S 7 を終了する。

[0071] 以上の処理により、一部には遅延のある信号が到着あるいは発信されるシミュレータ 1 が仮想配線 4 2' に接続され、信号遅延を模擬することができる。すなわち、シミュレータ 1 に与えられた鍵のセットに含まれる鍵の一部の鍵を分割することで、信号遅延を模擬することができる。この信号遅延の導入は、実施例 2 の鍵交換と同様に行われるので、セキュリティのレベルを高く保ちつつ、実行することができる。

符号の説明

[0072] 1 : シミュレータ、2 : 鍵管理サーバ、3 : ネットワーク、1 0 0 : シミュレータモジュール、1 0 1 : 仮想配線シミュレータモジュール、4 0 : 鍵リスト、4 2 : 暗号鍵、4 4 : データ、S 5 : データ送信処理、S 6 : データ受信処理、S 7 : 鍵交換処理

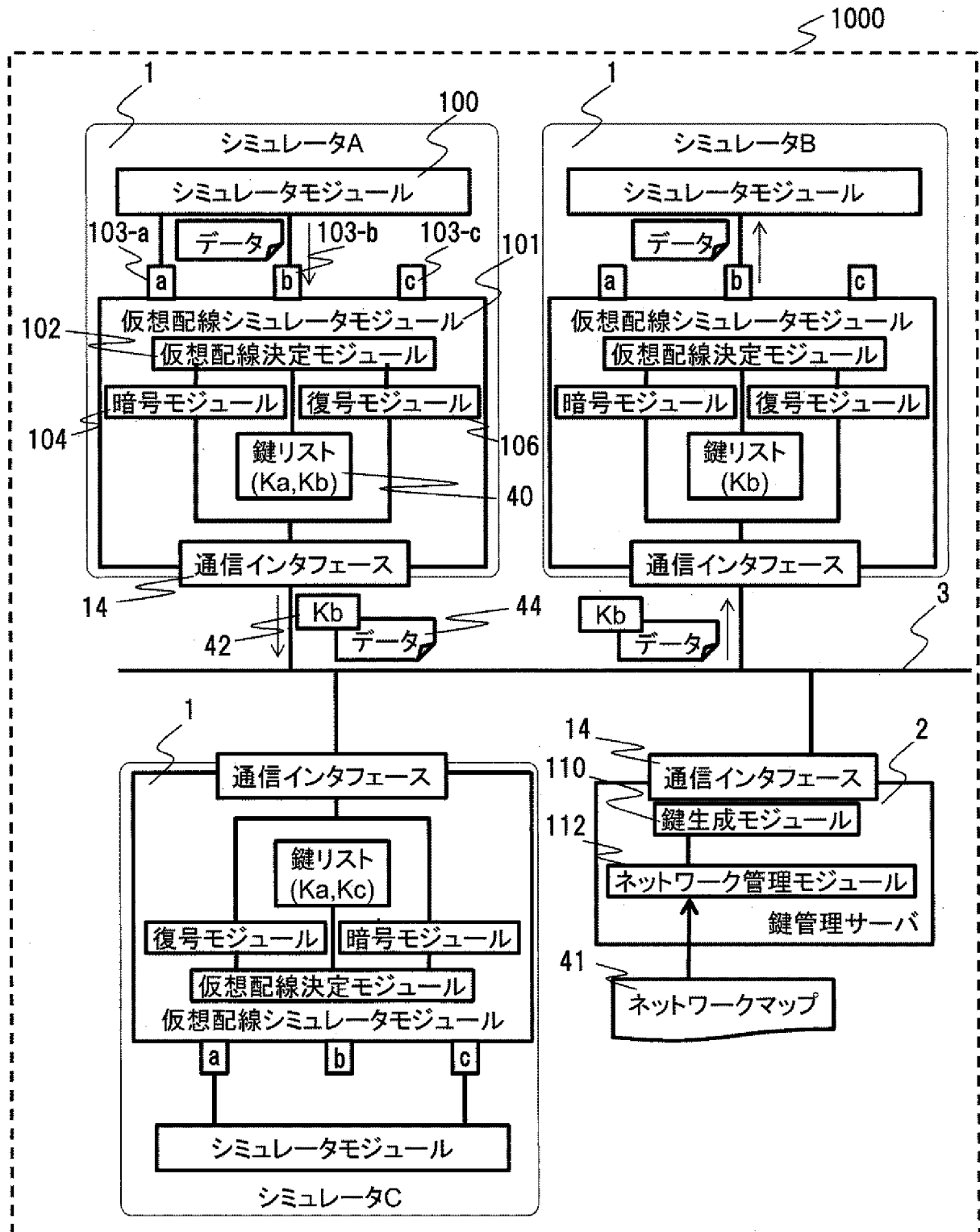
請求の範囲

- [請求項1] ネットワークで接続されている複数の情報処理装置上で動作するシミュレータ間の通信方法であって、
- 各シミュレータに、各シミュレータが接続される他のシミュレータへの仮想配線に対応する鍵のセットを与え、
- 前記複数のシミュレータの内の第1シミュレータが、データを前記第1シミュレータに接続されている仮想配線の内の一に送信する際に、前記第1シミュレータに与えられている前記鍵のセットの内、該一に対応する鍵で該データを暗号化し、前記ネットワークに送信することを特徴とするシミュレータ間の通信方法。
- [請求項2] 請求項1に記載のシミュレータ間の通信方法であって、
- 前記複数のシミュレータの内の第2シミュレータに与えられた鍵のセットに含まれる鍵の内の一部の鍵を変更することで、通信故障を模擬することを特徴とするシミュレータ間の通信方法。
- [請求項3] 請求項1に記載のシミュレータ間の通信方法であって、
- 前記複数のシミュレータの内の第2シミュレータに与えられた鍵のセットに含まれる鍵の内の一部の鍵を分割することで、信号到着遅れを模擬することを特徴とするシミュレータ間の通信方法。
- [請求項4] 請求項1に記載のシミュレータ間の通信方法であって、
- 各シミュレータは、シミュレーション対象の各コンポーネントに対応していることを特徴とするシミュレータ間の通信方法。
- [請求項5] 複数の情報処理装置上で動作するシミュレーションシステムであって、
- 前記複数の情報処理装置の内の一で実行される鍵管理サーバを有し、
- 前記鍵管理サーバは、前記複数の情報処理装置で実行される複数のシミュレータ間の接続に対応付けられた暗号鍵のセットを各シミュレータに送信することを特徴とするシミュレーションシステム。

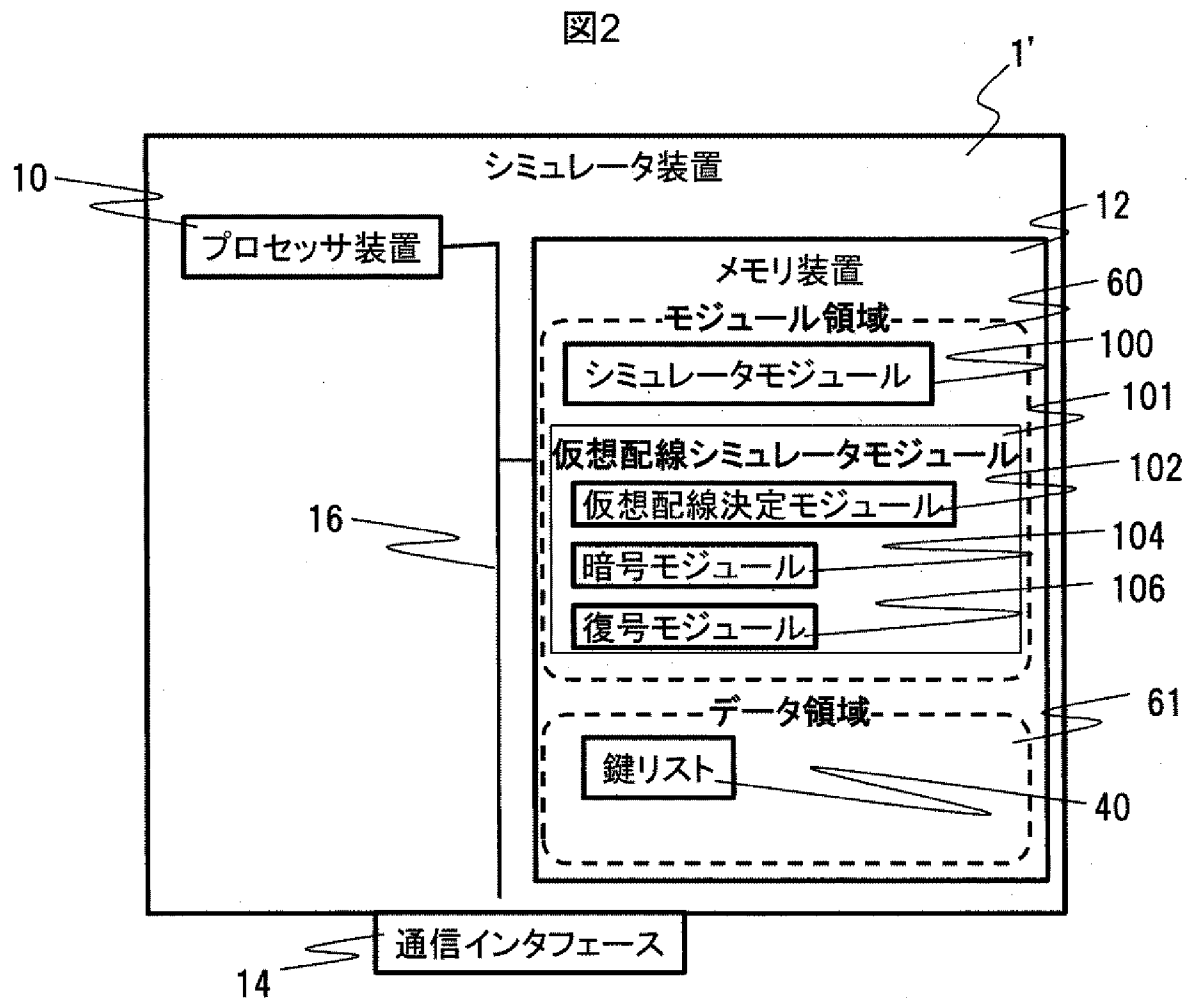
- [請求項6] 請求項5に記載のシミュレーションシステムであって、
前記鍵管理サーバは、前記複数のシミュレータの内の第1シミュレータに与えられた鍵のセットに含まれる鍵の一部の鍵を変更することで、通信故障を模擬することを特徴とするシミュレーションシステム。
- [請求項7] 請求項5に記載のシミュレーションシステムであって、
前記複数のシミュレータの内の第1シミュレータに与えられた鍵のセットに含まれる鍵の一部の鍵を分割することで、信号到着遅れを模擬することを特徴とするシミュレーションシステム。
- [請求項8] 請求項5に記載のシミュレーションシステムであって、
前記鍵管理サーバは、前記複数のシミュレータの内の任意のシミュレータ間の接続に対応付けられている鍵を更新することを特徴とするシミュレーションシステム。

[図1]

図1

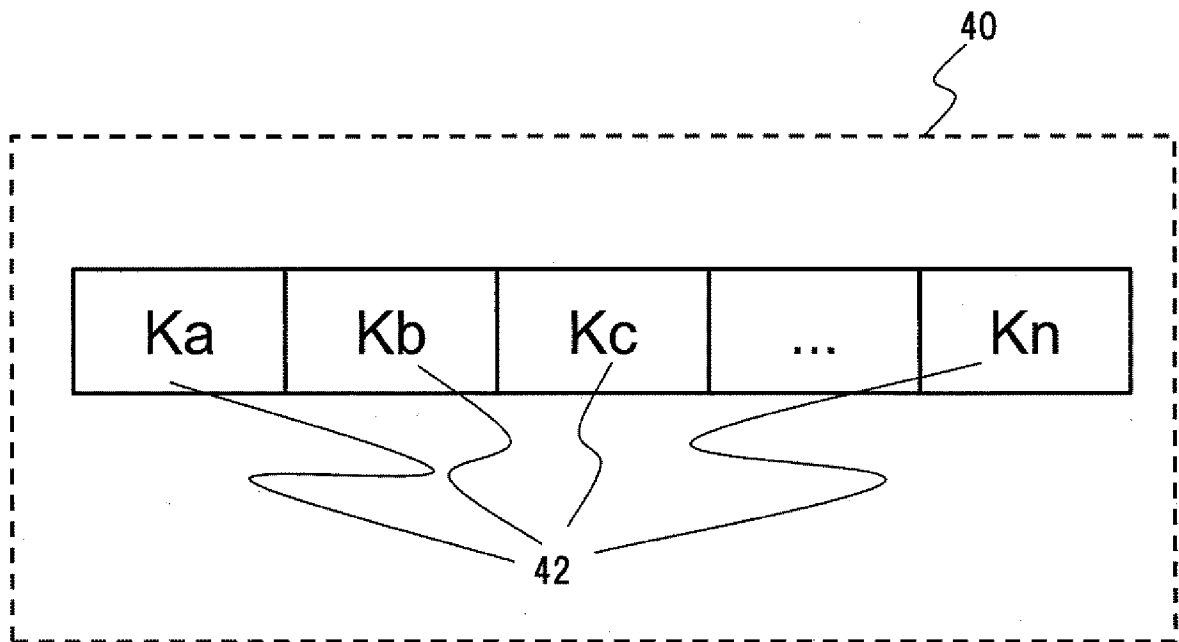


[図2]

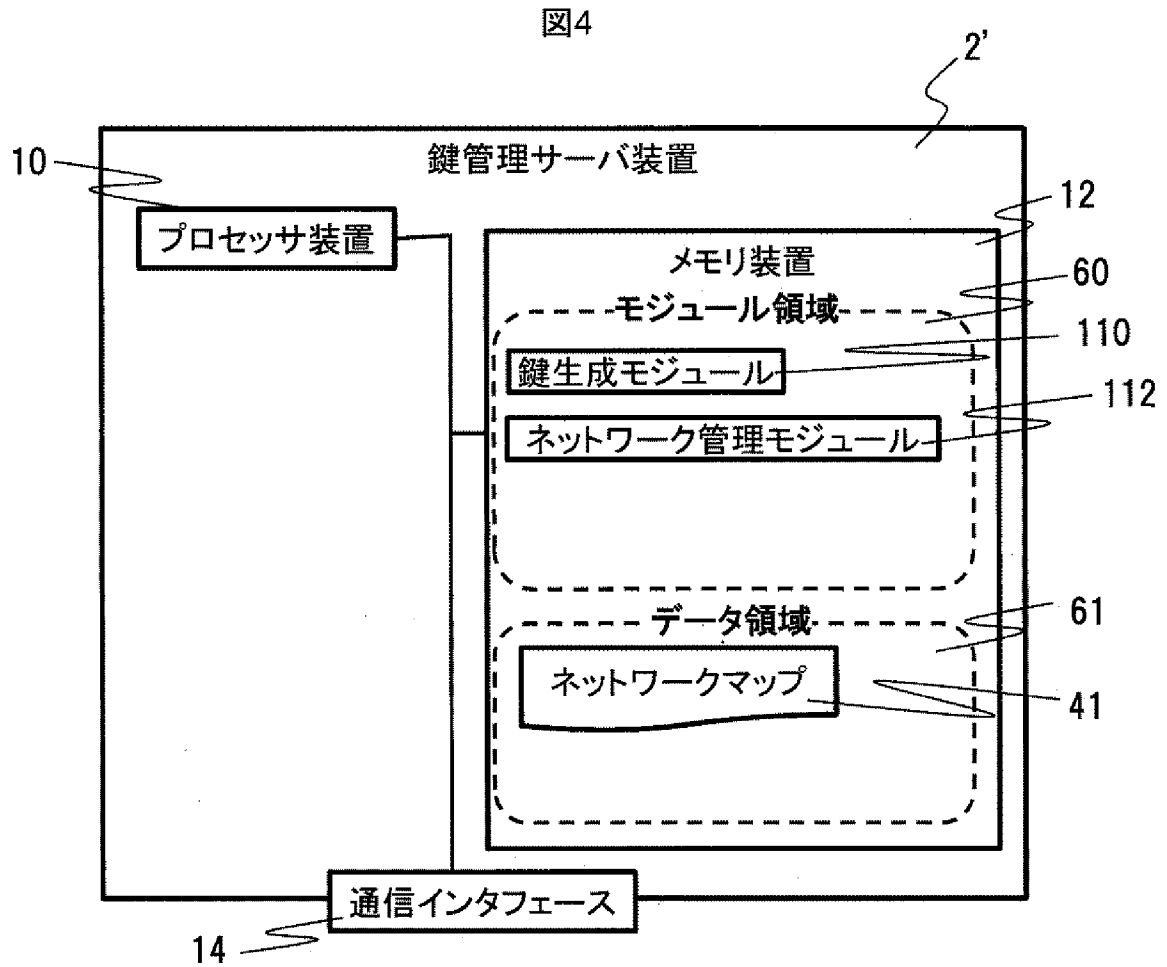


[図3]

図3

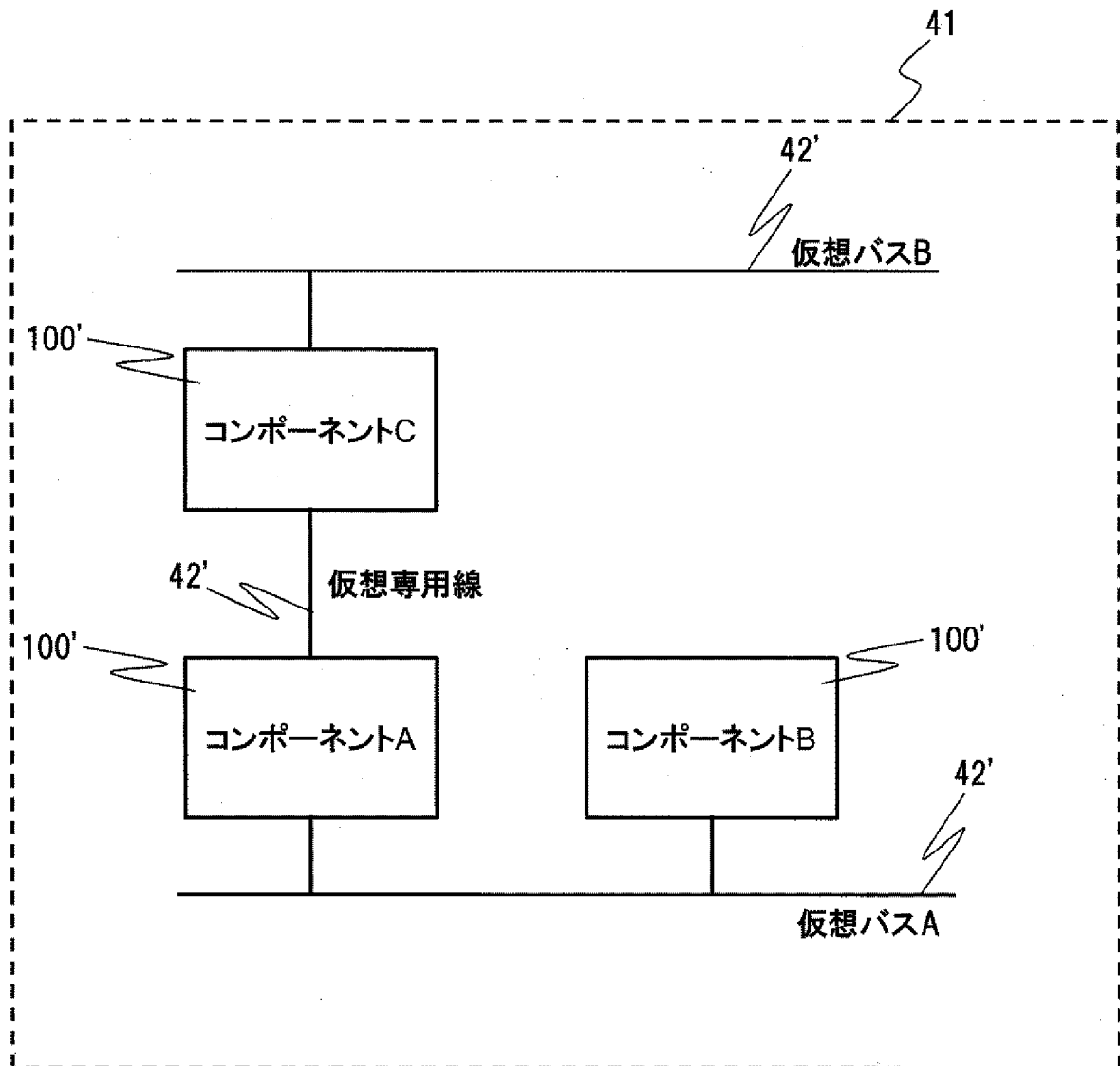


[図4]



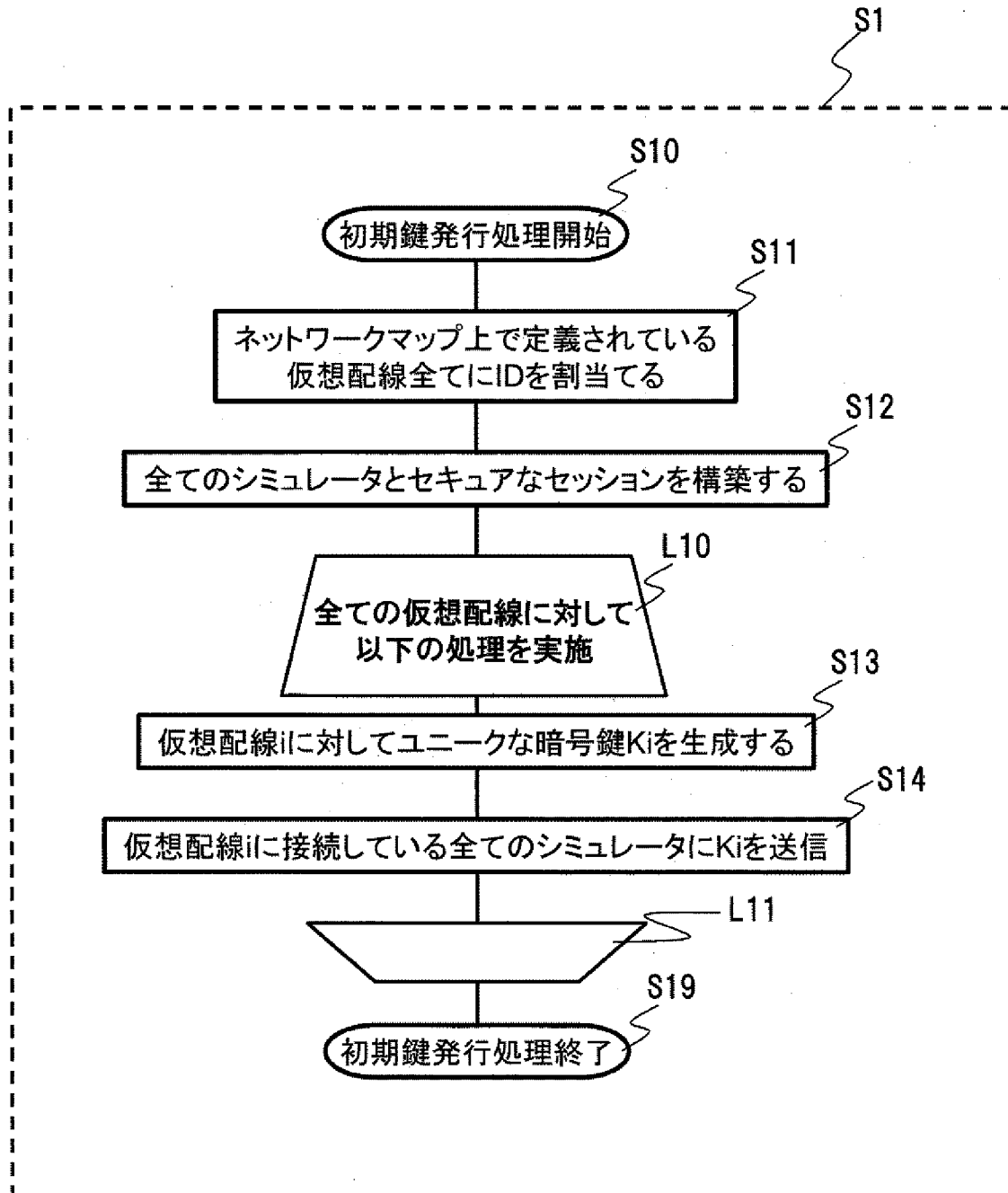
[図5]

図5

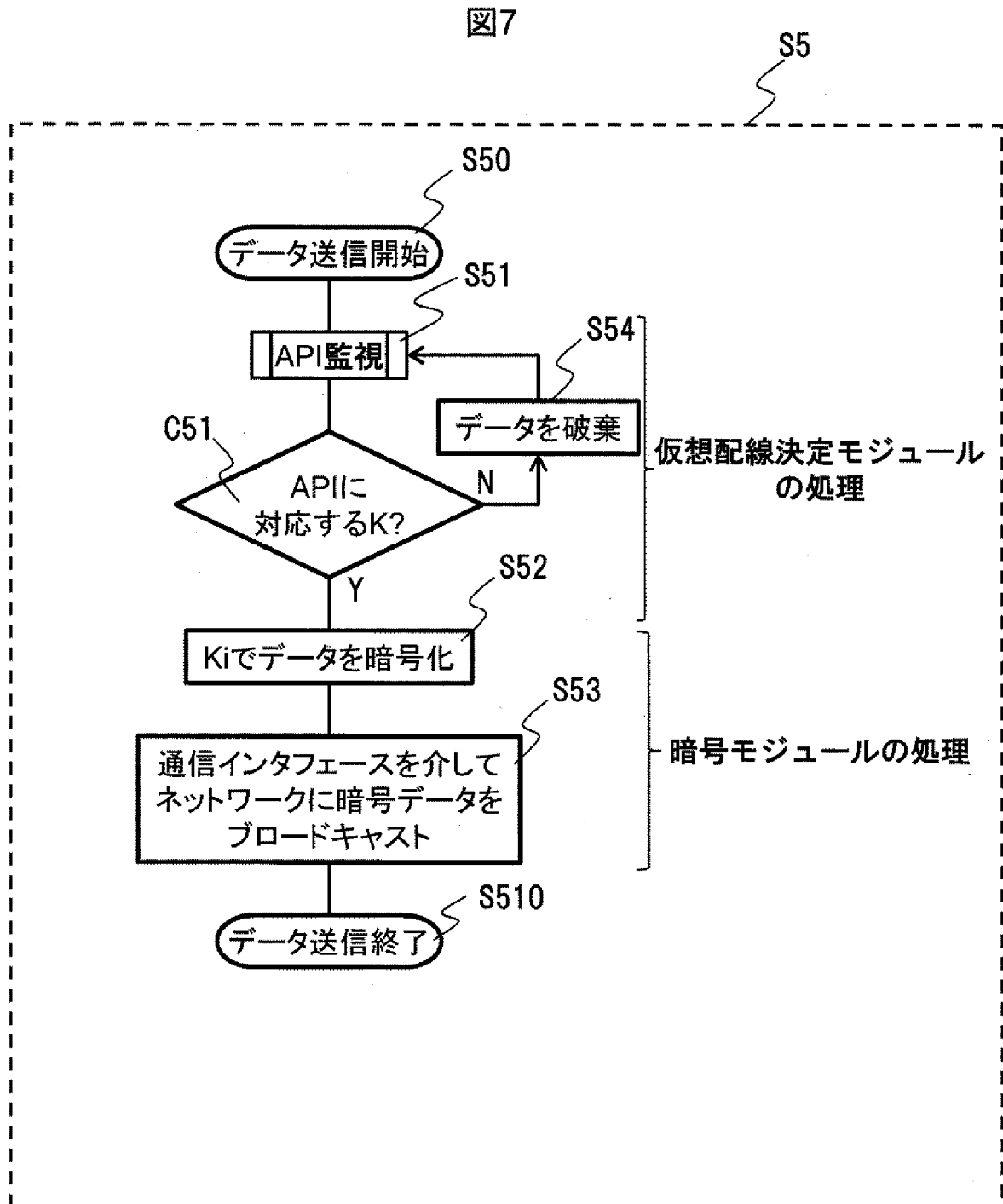


[図6]

図6

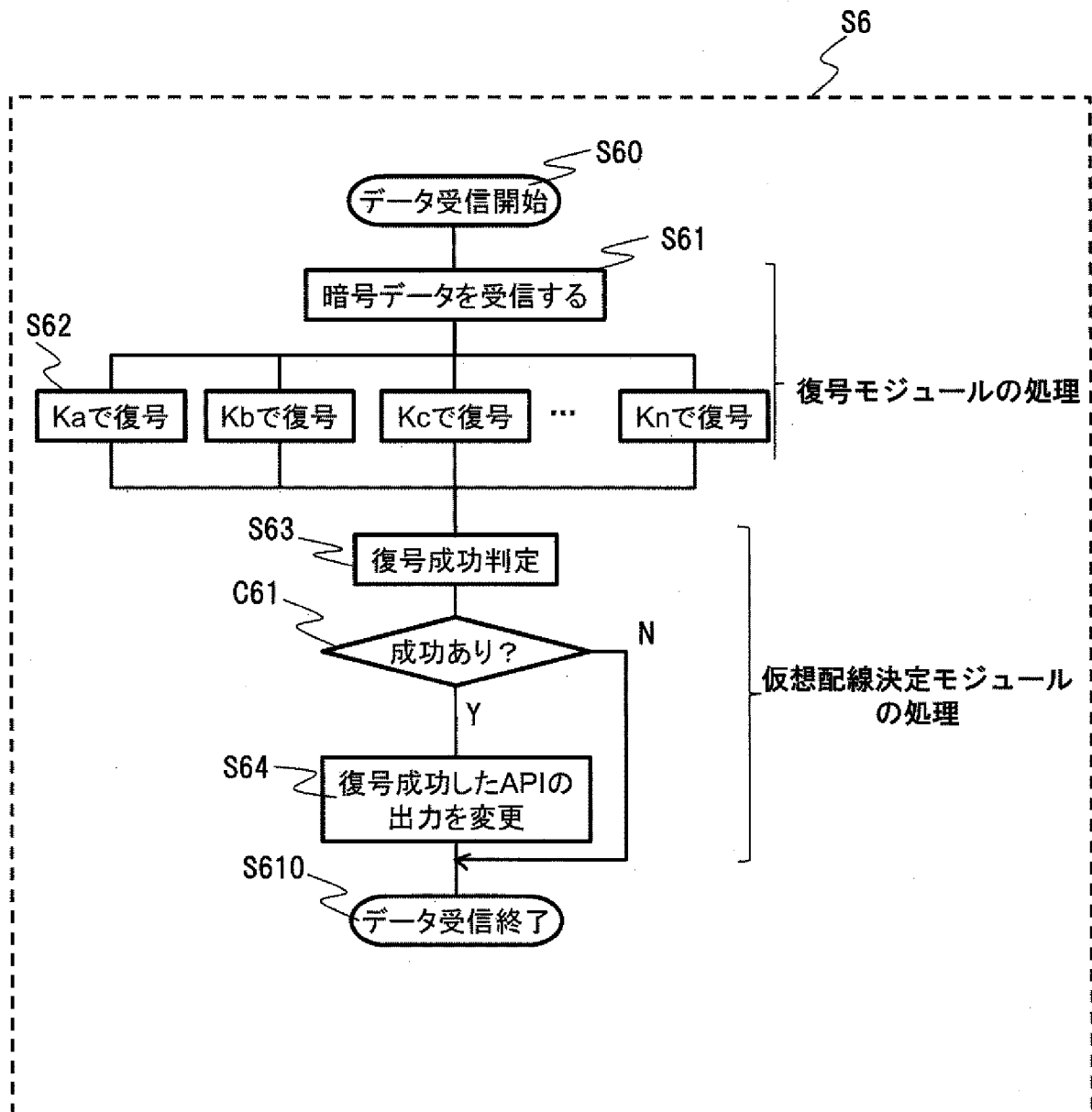


[図7]



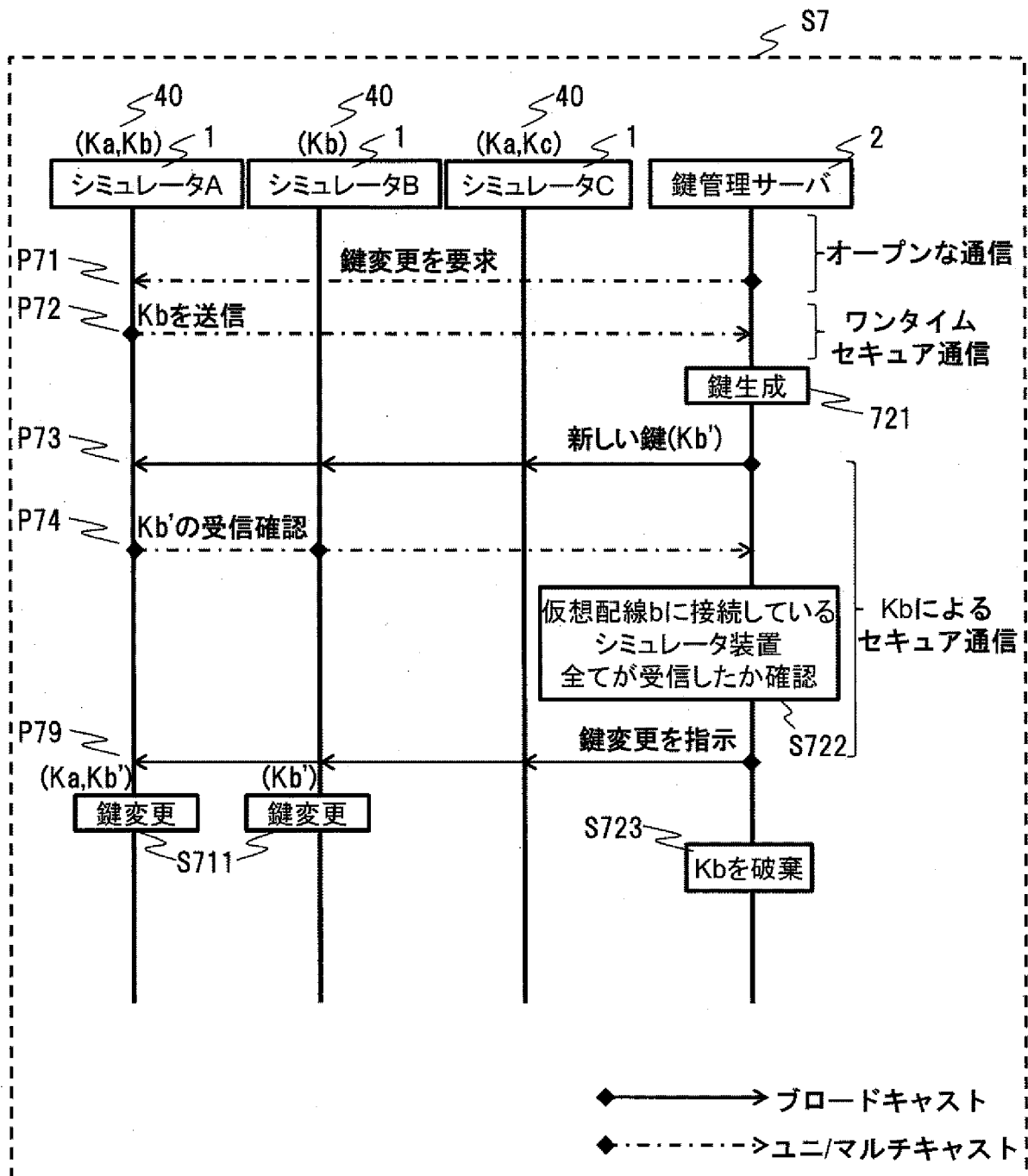
[図8]

図8



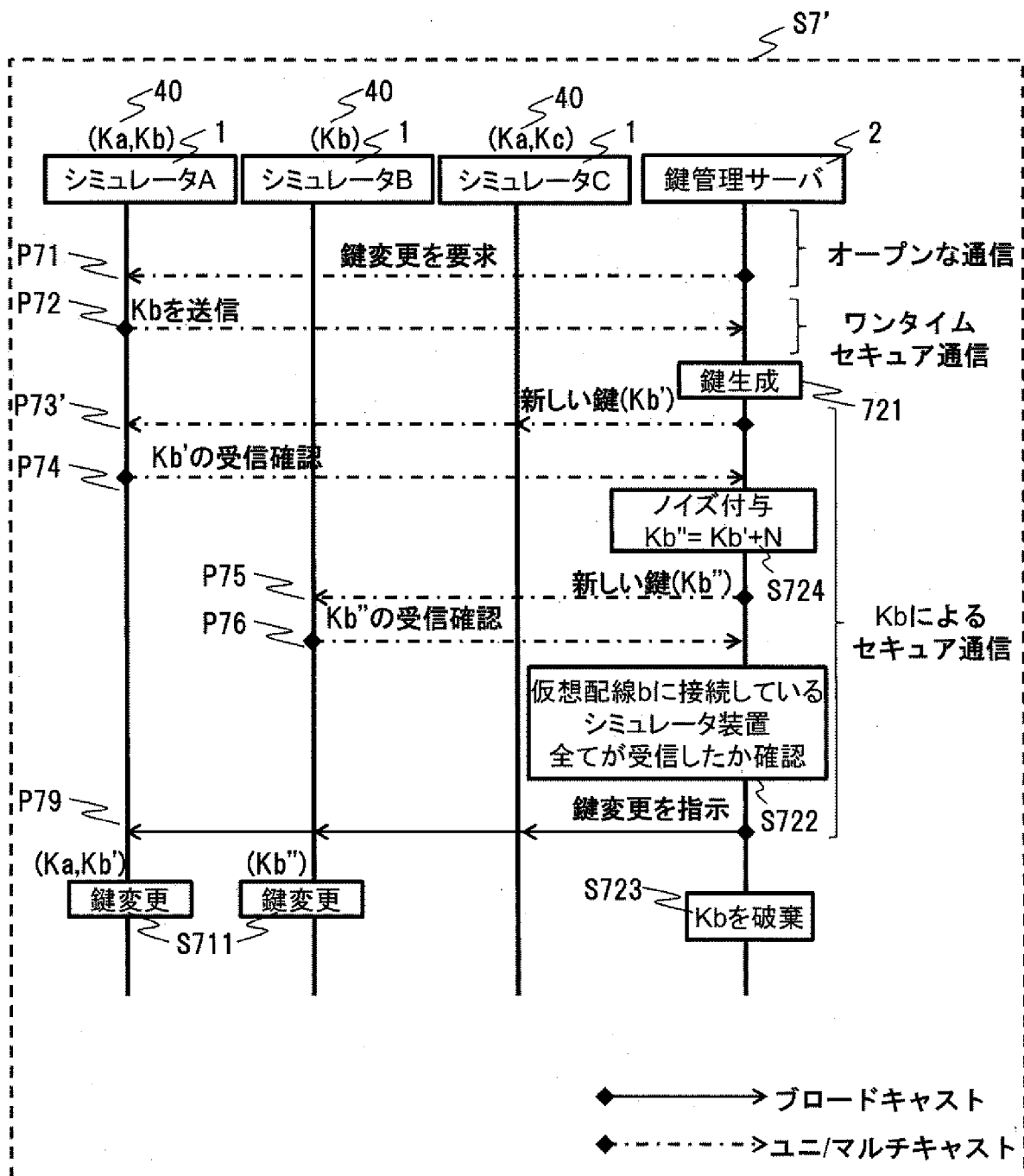
[図9]

図9



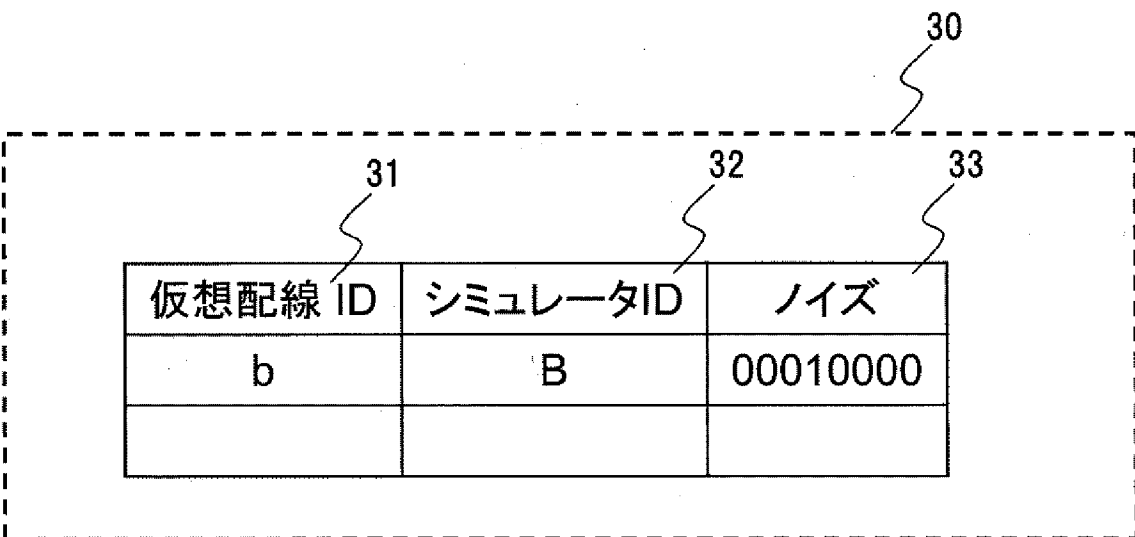
[図10]

図10



[図11]

図11

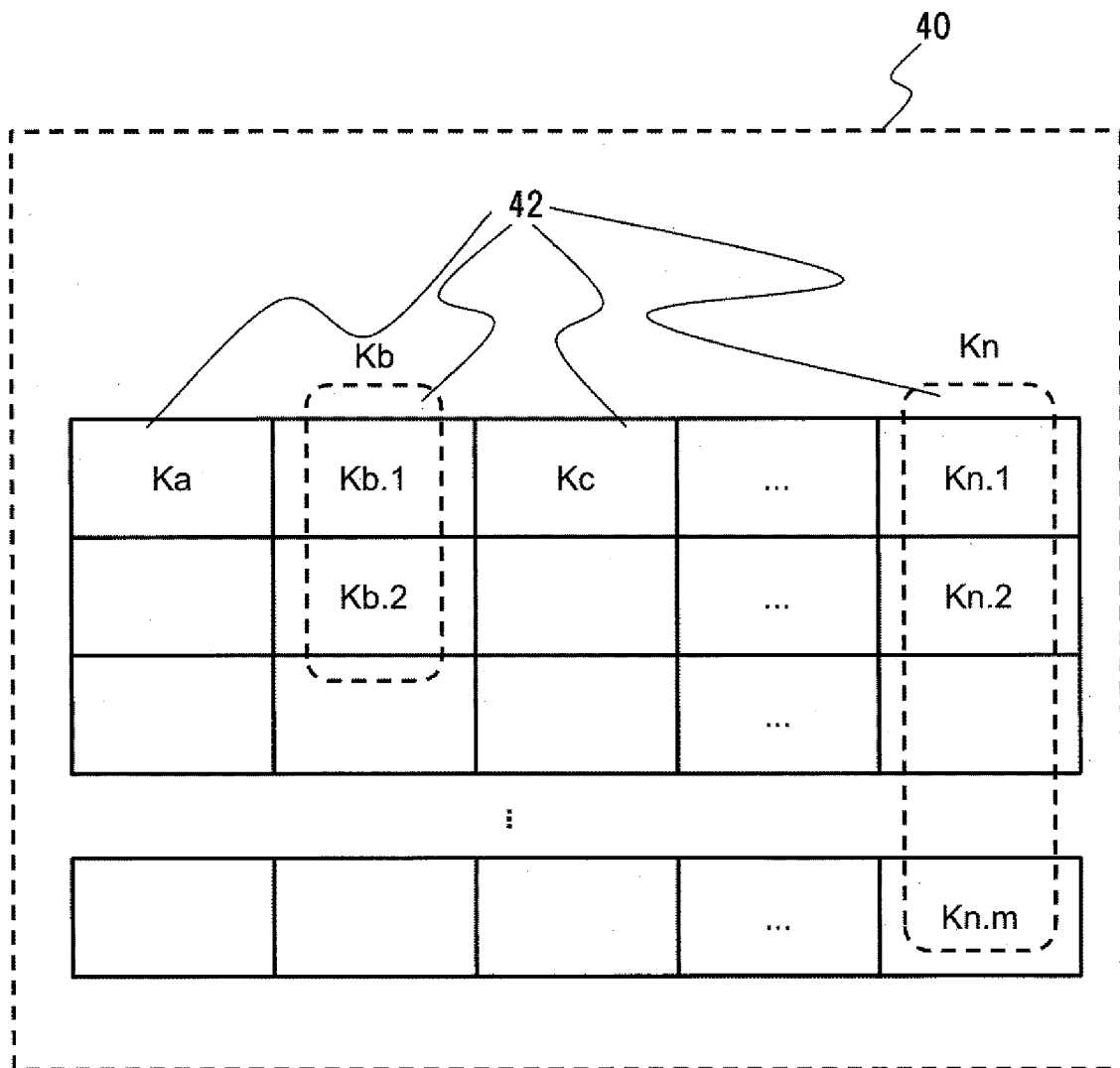


The diagram shows a table with three columns and three rows, enclosed in a dashed rectangular box. The columns are labeled '仮想配線 ID' (Virtual Wiring ID), 'シミュレータID' (Simulator ID), and 'ノイズ' (Noise). The first row contains the values 'b', 'B', and '00010000'. The second and third rows are empty. Reference numerals 30, 31, 32, and 33 point to the dashed box, the first column, the second column, and the third column, respectively.

仮想配線 ID	シミュレータID	ノイズ
b	B	00010000

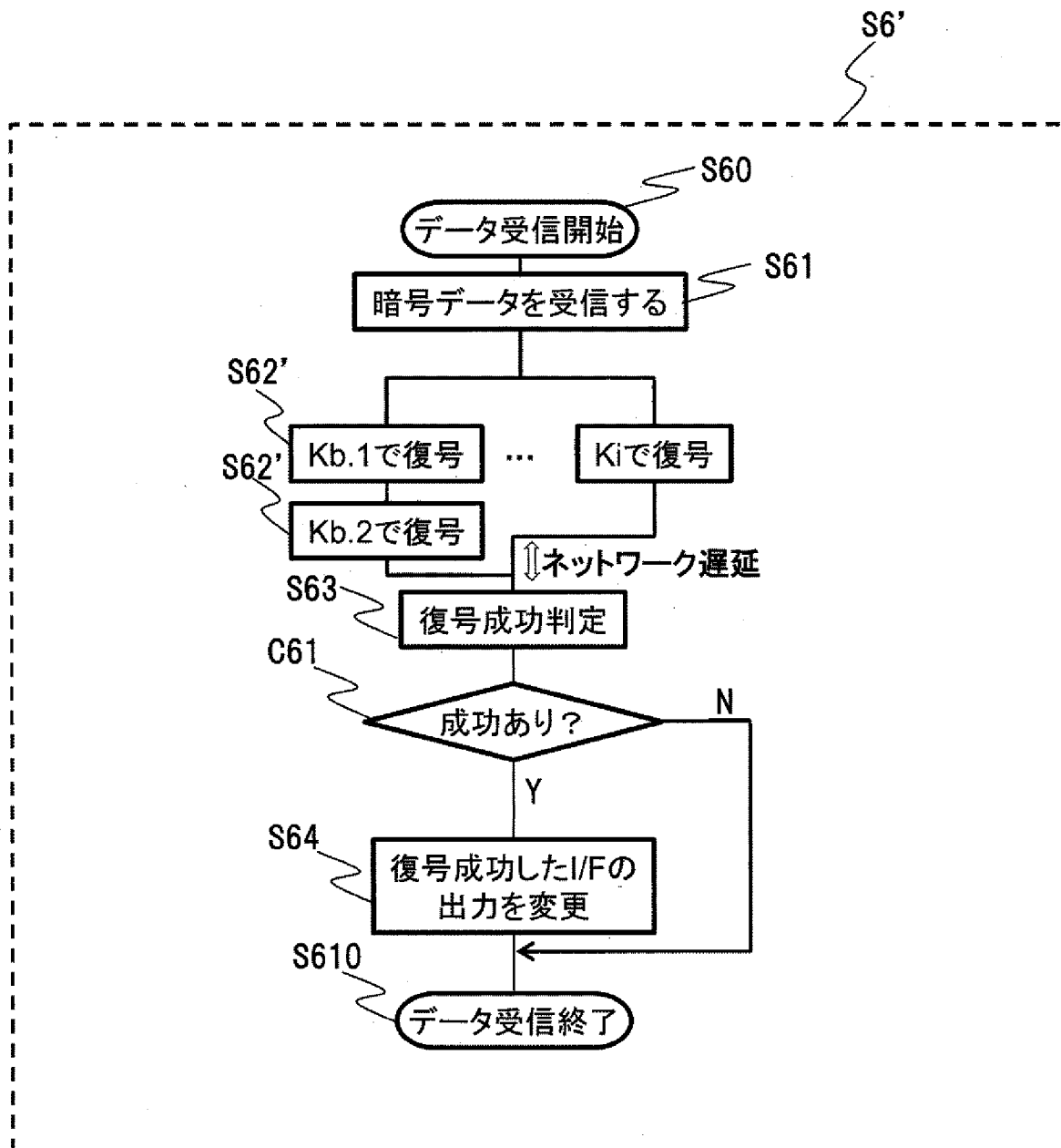
[図12]

図12



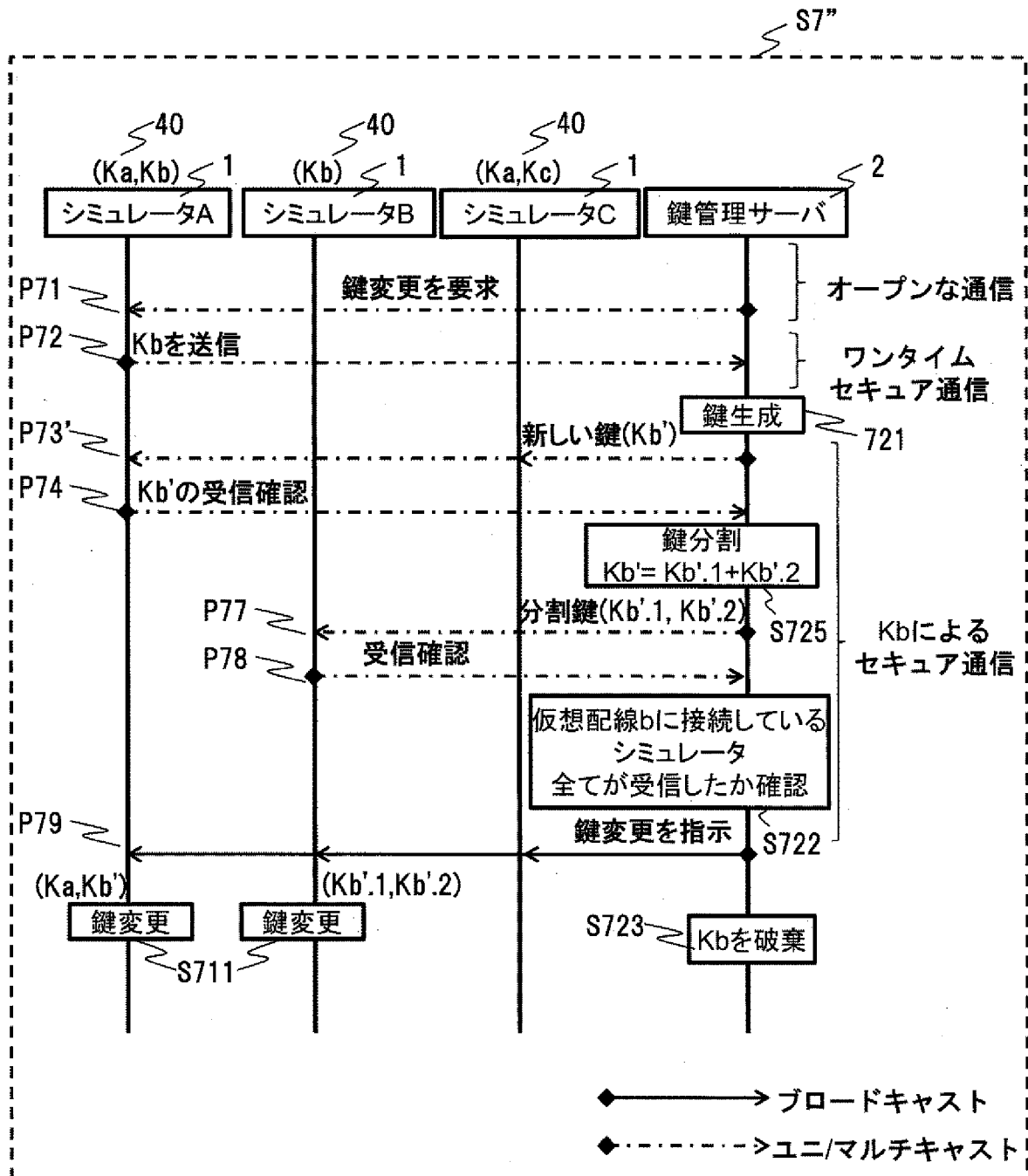
[図13]

図13



[図14]

図14



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/070143

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/14(2006.01) i, G06F17/50(2006.01) i, G06F21/62(2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/14, G06F17/50, G06F21/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2012

Kokai Jitsuyo Shinan Koho 1971-2012 Toroku Jitsuyo Shinan Koho 1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JSTPlus/JMEDPlus/JST7580(JDreamII), SHIMYURESHON ANGO (in Japanese)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Stytz, M. R. and Banks, S. B., ENABLING DISTRIBUTED SIMULATION MULTI-LEVEL SECURITY USING VIRTUAL MACHINE AND VIRTUAL PRIVATE NETWORK TECHNOLOGY, PROCEEDINGS OF SPIE, Vol.6570, 2007, p.65700B-1 - 12, especially 3. Using VMs and VPNs for Simulation Security	1, 4, 5, 8 2, 3, 6, 7
Y	JP 2011-22702 A (International Business Machines Corp.), 03 February 2011 (03.02.2011), paragraphs [0001] to [0010], [0047] to [0074]	1, 4, 5, 8
Y	JP 2009-545785 A (Intel Corp.), 24 December 2009 (24.12.2009), paragraphs [0044] to [0056]	1, 4, 5, 8



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

12 December, 2012 (12.12.12)

Date of mailing of the international search report

25 December, 2012 (25.12.12)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2012/070143

JP 2011-22702 A	2011.02.03	US 2011/0015916 A1
JP 2009-545785 A	2009.12.24	US 2008/0005586 A1
		EP 2041687 A2
		WO 2008/008623 A2
		CN 101454783 A

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/14(2006.01)i, G06F17/50(2006.01)i, G06F21/62(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. H04L9/14, G06F17/50, G06F21/24

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 2 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 2 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 2 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580(JDreamII) シミュレーション 略号

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	Stytz, M. R. and Banks, S. B., ENABLING DISTRIBUTED SIMULATION MULTI-LEVEL SECURITY USING VIRTUAL MACHINE AND VIRTUAL PRIVATE NETWORK TECHNOLOGY, PROCEEDINGS OF SPIE, Vol.6570, 2007, p.65700B-1 - 12, especially 3. Using VMs and VPNs for Simulation Security	1, 4, 5, 8 2, 3, 6, 7
Y	JP 2011-22702 A（インターナショナル・ビジネス・マシーンズ・コーポレーション）2011.02.03, 1-10, 47-74 段落	1, 4, 5, 8
Y	JP 2009-545785 A（インテル・コーポレーション）2009.12.24, 44-56 段落	1, 4, 5, 8

C 欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

1 2 . 1 2 . 2 0 1 2

国際調査報告の発送日

2 5 . 1 2 . 2 0 1 2

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

中里 裕正

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

5 S

9 3 6 4

国際調査報告
パテントファミリーに関する情報

国際出願番号 PCT/J P 2 0 1 2 / 0 7 0 1 4 3

JP 2011-22702 A	2011. 02. 03	US 2011/0015916 A1
JP 2009-545785 A	2009. 12. 24	US 2008/0005586 A1
		EP 2041687 A2
		WO 2008/008623 A2
		CN 101454783 A