(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년07월30일
(11) 등록번호 10-0848991
(24) 등록일자 2008년07월22일

(51) Int. Cl.
G06F 17/00 (2006.01) *G06F 15/00* (2006.01)
(21) 출원번호 10-2006-0097233
(22) 출원일자 2006년10월02일
심사청구일자 2006년10월02일
(65) 공개번호 10-2007-0040719
(43) 공개일자 2007년04월17일
(30) 우선권주장
JP-P-2005-00297079 2005년10월12일 일본(JP)
JP-P-2005-00362592 2005년12월16일 일본(JP)
(56) 선행기술조사문헌
JP17227331 A*
US20030101339 A1
US20030167314 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
가부시키가이샤 히타치세이사쿠쇼
일본국 도쿄토 치요다쿠 마루노우치 1초메 6반 6고
(72) 발명자
다니모또 고우이찌
일본 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 가부시키가이샤히타치세이사쿠쇼 지적재산권본부 내
히라까와 도모히로
일본 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 가부시키가이샤히타치세이사쿠쇼 지적재산권본부 내
(뒷면에 계속)
(74) 대리인
구영창, 장수길

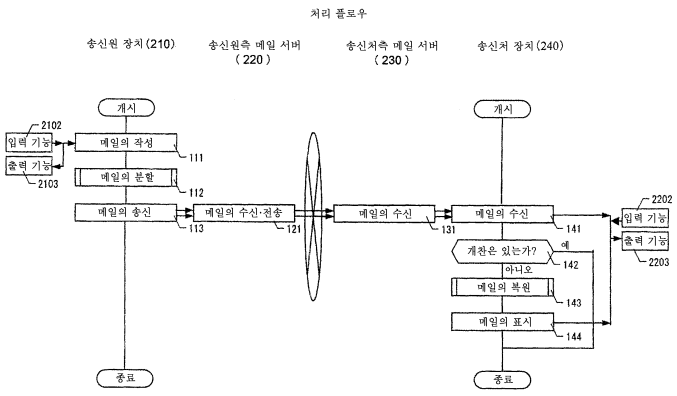
전체 청구항 수 : 총 18 항 심사관 : 김명찬

(54) 전자 데이터 송수신 방법 및 전자 데이터 송수신 시스템

(57) 요 약

본 발명은, 종래, 전자 데이터를 송수신할 때에, 경로 상에서의 도청 및 복원의 위험성을 저하시키는 것, 및, 가령, 네트워크 상에서 개찬 등의 조작이 행하여진 경우에도, 개찬의 검지를 용이하게 행하는 것을 가능하게 하는 것이다. 비밀 분산법을 이용하여 전자 데이터를 송수신하는 것으로, 송신원 장치가, 비밀 분산법을 이용하여, 전자 데이터를 소정수의 부분 데이터로 분할하고, 소정수의 부분 데이터에 대응하는 부속 데이터로서, 해당 부속 데이터와 부분 데이터의 총수를 산정하기 위해 필요한 정보를 갖는 부속 데이터를 임의 수 생성하고, 네트워크를 통하여 전자 데이터의 송신처인 송신처 장치에 이들을 송신하고, 송신처 장치는, 복수의 부분 데이터 및 상기 부속 데이터를 포함하는 수신 데이터를 기억 장치에 저장하고, 부속 데이터를 이용하여, 부분 데이터 및 부속 데이터에 대한 개찬이 없는 경우, 부분 데이터로부터 분할 전의 원 데이터인 전자 데이터를 복원한다.

대표도 - 도1



(72) 발명자

구마모또 마사히로

일본 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 가부시키가이샤히타치세이사쿠쇼 지적재산권본부 내

다니구찌 가즈히꼬

일본 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 가부시키가이샤히타치세이사쿠쇼 지적재산권본부 내

특허청구의 범위

청구항 1

비밀 분산법을 이용하여 전자 데이터를 송수신하는 전자 데이터 송수신 방법으로서,

상기 전자 데이터의 송신원인 송신원 장치가, 비밀 분산법을 이용하여, 상기 전자 데이터를 소정수의 부분 데이터로 분할하는 스텝,

상기 송신원 장치가, 상기 소정수의 부분 데이터에 대응하는 부속 데이터이고, 해당 부속 데이터와 상기 부분 데이터를 합한 개수를 나타내는 개수 정보를 나타내는 정보를 포함하는 부속 데이터를 생성하는 스텝,

상기 송신원 장치가, 네트워크를 통하여 상기 전자 데이터의 송신처인 송신처 장치에, 상기 부분 데이터 및 부속 데이터를 송신하는 스텝,

상기 송신처 장치는, 상기 부분 데이터 및 상기 부속 데이터를 수신하는 스텝,

상기 송신처 장치는, 상기 부분 데이터 및 상기 부속 데이터를 포함하는 수신 데이터를 기억 장치에 저장하는 스텝,

상기 송신처 장치는, 상기 부속 데이터를 이용하여, 상기 부분 데이터 및 상기 부속 데이터에 대한 개찬의 유무를 검지하는 스텝, 및

상기 송신처 장치는, 상기 부분 데이터로부터 상기 전자 데이터를 복원하는 스텝

을 포함하고,

상기 송신원 장치는, 상기 전자 데이터를 복수의 부분 데이터로 분할하는 전자 데이터 송수신 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 송신원 장치는, 상기 부분 데이터 및 상기 부속 데이터의 각각에, 복원 대상으로 되는 다른 부분 데이터 혹은 부속 데이터를 식별하는 정보를 포함시키는 전자 데이터 송수신 방법.

청구항 4

제1항에 있어서,

상기 송신원 장치는, 상기 부속 데이터를 1개 이상 생성하는 전자 데이터 송수신 방법.

청구항 5

제1항에 있어서,

상기 송신처 장치는, 상기 개수 정보를 이용하여, 개찬의 유무를 검지하는 전자 데이터 송수신 방법.

청구항 6

제5항에 있어서,

상기 송신원 장치 및 상기 송신처 장치의 각각은, 소정의 정보열을 기억해 두고,

상기 송신원 장치는, 상기 부분 데이터 및 상기 부속 데이터의 각각에 대하여, 해당 데이터의 소정 위치에, 소정 규칙에 따라서 상기 정보열을 구성하는 부호를 삽입하고,

상기 송신처 장치는, 상기 부호를 집합함으로써 상기 정보열을 구성하고, 미리 기억되어 있는 정보열과 비교함으로써 상기 부분 데이터 및 상기 부속 데이터에 대한 개찬의 유무를 검지하는 전자 데이터 송수신 방법.

청구항 7

제1항에 있어서,

상기 송신원 장치는, 상기 부분 데이터 및 상기 부속 데이터의 각각을, 소정 시간의 간격을 두고 연속적으로 송신함으로써,

서로 다른 통신 경로로 상기 부분 데이터 및 상기 부속 데이터의 각각을 송신할 가능성을 높이는 전자 데이터 송수신 방법.

청구항 8

제7항에 있어서,

상기 송신원 장치는, 상기 소정 시간으로서, 일정한 간격으로, 상기 부분 데이터 및 상기 부속 데이터의 각각을, 송신하는 전자 데이터 송수신 방법.

청구항 9

제1항에 있어서,

상기 송신원 장치는, 분할된 복수의 부분 데이터 및 부속 데이터 중 일부를 상기 송신처 장치 이외의 중개 장치에, 다른 것을 상기 송신처 장치에 송신하고,

상기 송신처 장치는, 상기 중개 장치에 액세스하여, 그 중개 장치에 송신된 부분 데이터 혹은 부속 데이터를 다운로드하고, 다운로드된 부분 데이터와 부속 데이터와 상기 송신처 장치에 송신된 부분 데이터와 부속 데이터를, 상기 전자 데이터로 복원하는 전자 데이터 송수신 방법.

청구항 10

비밀 분산법을 이용하여 전자 데이터를 송수신하는 전자 데이터 송수신 방법으로서,

상기 전자 데이터의 송신원인 송신원 장치가, 비밀 분산법을 이용하여, 상기 전자 데이터를 소정수의 부분 데이터로 이루어지는 부분 데이터군으로 분할하는 스텝,

상기 송신원 장치가, 상기 부분 데이터군을 제1 부분 데이터군과 제2 부분 데이터군으로 분류하는 스텝,

상기 송신원 장치가, 상기 제1 부분 데이터군의 부분 데이터에 대응하고, 상기 부분 데이터군의 부분 데이터로부터 상기 전자 데이터로 복원하기 위한 부속 데이터이고, 상기 제2 부분 데이터군의 저장 위치에 관련되는 위치 관련 정보를 포함하는 부속 데이터를 생성하는 스텝,

상기 송신원 장치가, 네트워크를 통하여 상기 전자 데이터의 송신처인 송신처 장치에 상기 부속 데이터 및 상기 제1 부분 데이터군을, 상기 네트워크를 통하여 데이터 서버에 상기 제2 부분 데이터군을 송신하는 스텝,

상기 송신처 장치가, 상기 제1 부분 데이터군 및 상기 부속 데이터를 수신하는 스텝,

상기 송신처 장치가, 상기 부속 데이터를 이용하여, 상기 제2 부분 데이터군의 저장 위치를 특정하는 스텝,

상기 송신처 장치가, 특정된 상기 저장 위치에 액세스하여, 상기 데이터 서버로부터 상기 제2 부분 데이터군의 부분 데이터를 읽어들이는 스텝, 및

상기 송신처 장치가, 읽어들여진 상기 제2 부분 데이터군의 부분 데이터와 수신한 상기 제1 부분 데이터군의 부분 데이터로부터, 상기 부속 데이터를 이용하여, 상기 전자 데이터를 복원하는 스텝

을 포함하고,

상기 송신원 장치는, 상기 제1 부분 데이터에 대응하는 개수의 상기 부속 데이터를 생성하는 전자 데이터 송수신 방법.

청구항 11

삭제

청구항 12

제10항에 있어서,

상기 송신원 장치는, 상기 제1 부분 데이터군의 부분 데이터 각각과 생성된 상기 부속 데이터의 각각을 대응시켜, 상기 송신처 장치에 송신하는 전자 데이터 송수신 방법.

청구항 13

제12항에 있어서,

상기 송신처 장치는, 상기 부속 데이터의 각각을 결합함으로써, 상기 위치 관련 정보로부터 상기 제2 부분 데이터군의 저장 위치를 나타내는 위치 정보를 생성하는 전자 데이터 송수신 방법.

청구항 14

제13항에 있어서,

상기 위치 정보는, URL인 전자 데이터 송수신 방법.

청구항 15

제14항에 있어서,

상기 제2 부분 데이터군은, 1개의 부분 데이터로 구성되는 전자 데이터 송수신 방법.

청구항 16

제15항에 있어서,

상기 송신원 장치는, 상기 부속 데이터이고, 해당 부속 데이터와 상기 부분 데이터를 합한 개수를 나타내는 정보를 포함하는 부속 데이터를 생성하고,

상기 송신처 장치는, 상기 부속 데이터를 이용하여, 상기 부분 데이터 및 상기 부속 데이터에 대한 개찬의 유무를 검지하는 전자 데이터 송수신 방법.

청구항 17

제16항에 있어서,

상기 송신처 장치는, 상기 개찬이 검지되지 않았던 경우, 상기 전자 데이터의 복원을 실행하는 전자 데이터 송수신 방법.

청구항 18

비밀 분산법을 이용하여 전자 데이터를 송수신하는 전자 데이터 송수신 시스템으로서,

비밀 분산법을 이용하여, 상기 전자 데이터를 소정수의 부분 데이터로 분할하는 분할 수단, 상기 소정수의 부분 데이터에 대응하는 부속 데이터이고, 해당 부속 데이터와 상기 부분 데이터를 합한 개수를 나타내는 개수 정보를 나타내는 정보를 포함하는 부속 데이터를 생성하는 생성 수단, 및, 네트워크를 통하여 상기 전자 데이터의 송신처인 송신처 장치에, 상기 부분 데이터 및 부속 데이터를 송신하는 송신 수단으로 이루어지는 송신원 장치, 및

상기 부분 데이터 및 상기 부속 데이터를 수신하는 수신 수단, 상기 부분 데이터 및 상기 부속 데이터를 포함하는 수신 데이터를 기억 장치에 저장하는 저장 수단, 상기 부속 데이터를 이용하여, 상기 부분 데이터 및 상기 부속 데이터에 대한 개찬의 유무를 검지하는 검지 수단, 및, 상기 부분 데이터로부터 상기 전자 데이터를 복원하는 복원 수단으로 이루어지는 송신처 장치를 포함하고,

상기 분할 수단은, 상기 전자 데이터를 복수의 부분 데이터로 분할하는 전자 데이터 송수신 시스템.

청구항 19

삭제

청구항 20

제18항에 있어서,

상기 송신원 장치는, 상기 부분 데이터 및 상기 부속 데이터의 각각에, 복원 대상으로 되는 다른 부분 데이터 혹은 부속 데이터를 식별하는 정보를 포함시키는 수단을 더 포함하는 전자 데이터 송수신 시스템.

청구항 21

제18항에 있어서,

상기 생성 수단은, 상기 부속 데이터를 1개 이상 생성하는 전자 데이터 송수신 시스템.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<26> 본 발명은, 소위 비밀 분산법을 이용하여 전자 데이터를 취급하는 기술에 관한 것이다. 그 중에서도, 전자 메일을 포함하는 전자 데이터의 송수신을 행하는 기술에 관한 것이다.

<27> 전자 데이터의 수수나 보관 시의 안전성을 높이는 기술로서, 비밀 분산법이 있다. 이것은, 전자 데이터를 그것 단독으로는 의미가 없는 부분 데이터로 분할하고, 특정한 프로그램에 의해 또한 부분 데이터가 소정수(혹은 모두) 갖추어져야 비로소 원래의 전자 데이터로 복원되는 기술이다.

<28> 이 비밀 분산법에 관한 종래 기술로서, 일본 특개 2004-53969호 공보(종래 기술 1)가 있다. 본 종래 기술 1에서, 고도의 기밀성을 갖고 신뢰성이 높은 전자 부절을 간단히 생성하기 위한 기술이 기재되어 있다. 이 때문에, 종래 기술 1에서는, 취급하는 데이터인 평문을 읽어내어 압축 부호화하여 용장의 비트 패턴을 제거한 부호어를 생성하고, K개의 엘리먼트로 잘게 잘라, 각 엘리먼트를 난수에 기초하여 M개의 부절 파일로 배분하여 저장하고, 그 배분 방법을 엘리먼트 할당 테이블에 기록하고, 엘리먼트 할당 테이블을 M개로 분할하여 부절 파일에 클로즈 헤더로서 추가하고, 부절 파일마다의 클로즈 헤더에 분배된 엘리먼트 할당 테이블의 분할편의 배치 리스트를 오픈 헤더로서 부절 파일에 추가함으로써, 부절 파일에 전자 부절을 생성하여 필요에 따라서 출력한다.

<29> 또한, 이 비밀 분산법을 이용하여, 네트워크를 경유해서, 전자 데이터를 배송하는 기술로서, 일본 특개 2003-132229호 공보 및 일본 특개 2003-132234호 공보(종래 기술 2 및 3)가 있다. 종래 기술 2에서는, 서버가, 전자 데이터를, 제1 및 제2 부절 정보로 분할하고, 제1 부절 정보를 제1 통신로를 통해서 센터 머신에 송신하고, 제2 부절 정보를 클라이언트에게 제2 통신로를 통해서 송신하며, 클라이언트는 제1 부절 정보를 모아, 제2 부절 정보와 통합하여, 원래의 전자 데이터를 복원하는 것이 기재되어 있다. 또한, 복원에 필요한 정보를 할당 대응표 T에 규정하는 것이 기재되어 있다. 또한, 종래 기술 3에서는, 센터 머신을 경유하지 않고 서버 머신으로부터 유저 머신에, 복수의 전자 부절의 각각을, 서로 다른 통신 수단(포함한다 : 서로 다른 시각)으로 송신하는 것이 기재되어 있다. 또한, 이 서로 다른 시각이란, 동일한 통신 경로로 송신하는 것을 의식하고 있다(0025항).

발명이 이루고자 하는 기술적 과제

<30> 그러나, 종래 기술 1에서는, 비밀 분산법의 알고리즘에 관해서, 상세하게 검토가 이루어져 있지만, 전자 데이터를 네트워크를 통하여 송수신하는 것에 관해서는 거의 고려되어 있지 않다. 이 때문에, 예를 들면 네트워크 상에서 분할된 부분 데이터에 개찬이 이루어진 경우에는 전자 데이터를 복원할 수 없게 된다는 네트워크 상에서 송수신하는 경우의 과제가 남게 된다. 또한, 종래 기술 2, 3에서는, 네트워크를 이용하여 송수신하는 것은 기재되어 있지만, 네트워크 상에서 개찬 등의 조작이 행하여진 경우에는, 분할 전의 원 데이터를 복원할 수 없다고 하는 문제는 고려되어 있지 않다.

발명의 구성 및 작용

<31> 따라서, 본 발명에서는, 전자 데이터를 비밀 분산법으로 분할한 부분 데이터와 함께 임의 수의 부속 데이터를

송수신하는 구성으로 하였다. 여기서, 각 부분 데이터 및 각 부속 데이터에는, 복원 대상으로 되는 다른 부분 데이터, 다른 부속 데이터를 식별하는 정보를 포함시켜 두어도 된다. 또한, 부분 데이터, 부속 데이터의 총수를 산정하기 위해 필요한 정보를 포함시켜 두어도 된다.

<32> 보다 구체적인 양태로서는, 이하의 구성이 본 발명에 포함된다. 비밀 분산법을 이용하여 전자 데이터를 송수신하는 전자 데이터 송수신 방법에서, 상기 전자 데이터의 송신원인 송신원 장치가, 비밀 분산법을 이용하여, 상기 전자 데이터를 소정수의 부분 데이터로 분할하고, 상기 송신원 장치가, 상기 소정수의 부분 데이터에 대응하는 부속 데이터로서, 해당 부속 데이터와 상기 부분 데이터의 총수를 산정하기 위해 필요한 정보를 갖는 부속 데이터를 임의 수 생성하고, 상기 송신원 장치가, 네트워크를 통하여 상기 전자 데이터의 송신처인 송신처 장치에, 상기 부분 데이터 및 부속 데이터를 송신하고, 상기 송신처 장치는, 상기 부분 데이터 및 상기 부속 데이터를 수신하고, 상기 송신처 장치는, 상기 복수의 부분 데이터 및 상기 부속 데이터를 포함하는 수신 데이터를 기억 장치에 저장하고, 상기 송신처 장치는, 상기 부속 데이터를 이용하여, 상기 부분 데이터 및 상기 부속 데이터에 대한 개찬의 유무를 검지하고, 상기 송신처 장치는, 상기 부분 데이터로부터 분할 전의 원 데이터인 상기 전자 데이터를 복원한다.

<33> 또한, 이 전자 데이터 송수신 방법에서, 상기 송신원 장치는, 상기 부분 데이터를 2개 이상의 부분 데이터로 분할하는 것도 본 발명에 포함된다.

<34> 또한, 이들 전자 데이터 송수신 방법에서, 상기 송신원 장치는, 상기 부속 데이터를 1개 이상의 어느 것을 생성하는 것도 본 발명에 포함된다.

<35> 또한, 이들 전자 데이터 송수신 방법에서, 상기 송신처 장치는, 상기 복원 대상으로 되는 다른 부분 데이터 및 다른 부속 데이터를 식별하는 정보, 각 부분 데이터를 부호화한 정보 등을 이용하여, 개찬의 유무를 검지하는 것도 본 발명에 포함된다.

<36> 또한, 이 전자 데이터 송수신 방법에서, 상기 송신원 장치 및 상기 송신처 장치의 각각은, 소정의 정보열을 기억해 두고, 상기 송신원 장치는, 상기 부분 데이터 및 상기 부속 데이터의 각각에 대하여, 해당 데이터의 소정 위치에, 소정 규칙에 따라서 상기 정보열을 구성하는 부호를 삽입하고, 상기 송신처 장치는, 상기 부호를 집합함으로써 상기 정보열을 구성하고, 미리 기억되어 있는 정보열과 비교함으로써 상기 부분 데이터 및 상기 부속 데이터에 대한 개찬의 유무를 검지하는 것도 본 발명에 포함된다.

<37> 또한, 이들 전자 데이터 송수신 방법에서, 상기 송신원 장치는, 상기 부분 데이터 및 상기 부속 데이터의 각각을, 소정 시간의 간격을 두고 연속적으로 송신함으로써, 서로 다른 통신 경로로 상기 부분 데이터 및 상기 부속 데이터의 각각을 송신할 가능성을 높이는 것도 본 발명에 포함된다.

<38> 또한, 이 전자 데이터 송수신 방법에서, 상기 송신원 장치는, 상기 소정 시간으로서, 예를 들면 30초 이상 3분 이하의 시간의 간격으로, 상기 부분 데이터 및 상기 부속 데이터의 각각을, 송신하는 것도 본 발명에 포함된다.

<39> 또한, 상술한 전자 데이터 송수신 방법에서, 상기 송신원 장치는, 분할된 복수의 부분 데이터 및 부속 데이터 중 일부를 상기 송신처 장치 이외의 중개 장치에, 다른 것을 상기 송신처 장치에 송신하고, 상기 송신처 장치는, 상기 중개 장치에 액세스하여, 해당 중개 장치에 송신된 부분 데이터를 다운로드하고, 다운로드된 부분 데이터와 상기 송신처 장치에 송신된 부분 데이터를, 상기 전자 데이터로 복원하는 것도 본 발명에 포함된다. 이 양태로서, 이하의 처리도 본 발명에 포함된다.

<40> 비밀 분산법을 이용하여 전자 데이터를 송수신하는 전자 데이터 송수신 방법에서, 상기 전자 데이터의 송신원인 송신원 장치가, 비밀 분산법을 이용하여, 상기 전자 데이터를 소정수의 부분 데이터로 이루어지는 부분 데이터군으로 분할하고, 상기 송신원 장치가, 상기 부분 데이터군을 제1 부분 데이터군과 제2 부분 데이터군으로 분류하고, 상기 송신원 장치가, 상기 제1 부분 데이터군의 부분 데이터에 대응하여, 상기 부분 데이터군의 부분 데이터로부터 상기 전자 데이터로 복원하기 위한 부속 데이터로서, 상기 제2 부분 데이터군의 저장 위치에 관련되는 위치 관련 정보를 포함하는 부속 데이터를 생성하고, 상기 송신원 장치가, 네트워크를 통하여 상기 전자 데이터의 송신처인 송신처 장치에 상기 부속 데이터 및 상기 제1 부분 데이터군을, 상기 네트워크를 통하여 데이터 서버에 상기 제2 부분 데이터군을 송신하고, 상기 송신처 장치가, 상기 제1 부분 데이터군 및 상기 부속 데이터를 수신하고, 상기 송신처 장치가, 상기 부속 데이터를 이용하여, 상기 제2 부분 데이터군의 저장 위치를 특정하고, 상기 송신처 장치가, 특정된 상기 저장 위치에 액세스하여, 상기 데이터 서버로부터 상기 제2 부분 데이터군의 부분 데이터를 읽어들이고, 상기 송신처 장치가, 읽어들인 상기 제2 부분 데이터군의 부분 데이터와

수신한 상기 제1 부분 데이터군의 부분 데이터로부터, 상기 부속 데이터를 이용하여, 상기 전자 데이터를 복원한다.

<41> 또한, 이 처리에서, 상기 송신원 장치는, 상기 제1 부분 데이터에 대응하는 개수의 상기 부속 데이터를 생성하는 것도 본 발명에 포함된다. 또한, 이 처리에서, 상기 송신원 장치는, 상기 제1 부분 데이터군의 부분 데이터 각각과 생성된 상기 부속 데이터의 각각을 대응시켜, 상기 송신처 장치에 송신하는 것도 본 발명에 포함된다.

<42> 또한, 상기 송신처 장치는, 상기 부속 데이터의 각각을 결합함으로써, 상기 위치 관련 정보로부터 상기 제2 부분 데이터군의 저장 위치를 나타내는 위치 정보를 생성하는 것도 본 발명에 포함된다. 여기서, 상기 위치 정보는, URL이다.

<43> 또한 상기 제2 부분 데이터군은, 1개의 부분 데이터로 구성되는 것도 본 발명에 포함된다.

<44> 또한, 상기 송신원 장치는, 상기 부속 데이터로서, 해당 부속 데이터와 상기 부분 데이터를 합한 개수를 나타내는 정보를 포함하는 부속 데이터를 생성하고, 상기 송신처 장치는, 상기 부속 데이터를 이용하여, 상기 부분 데이터 및 상기 부속 데이터에 대한 개찬의 유무를 검지하는 것도 본 발명에 포함된다. 여기서, 상기 송신처 장치는, 상기 개찬이 검지되지 않았던 경우, 상기 전자 데이터의 복원을 실행하는 것도 본 발명에 포함된다.

<45> 또한, 본 발명에는, 상술한 각 처리를 컴퓨터에서 실행시키는 프로그램, 이 프로그램을 저장한 기억 매체, 이들의 방법도 포함된다.

<46> 본 발명에 따르면, 보다 안전하게 간이한 시스템 구성으로 전자 데이터의 송수신이 가능하게 된다.

<47> <실시예>

<48> 본 발명의 실시 형태(제1 실시예)에 대해서, 전자 데이터의 송수신을 전자 메일의 이용에 의해 행하는 경우를 예로, 도면을 이용하여 설명한다.

<49> 이하, 제1 실시예의 처리 내용에 대해서, 설명한다.

<50> 도 1은, 본 발명의 제1 실시예를 도시하는 처리 플로우도이다. 도 2는, 본 실시예를 실현하기 위한 장치 구성을 포함하는 전자 데이터 송수신 시스템의 전체 이미지도이다.

<51> 우선, 도 2에 도시하는 전자 데이터 송수신 시스템의 전체 이미지도에 관해서 설명한다. 전자 데이터 송수신 시스템은, 송신원 장치(210)와, 송신원측 메일 서버(220)와, 송신처측 메일 서버(230)와, 송신처 장치(240)가, 통신 네트워크(250)로 접속된 시스템이다.

<52> (1) 송신원 장치(210)의 장치 구성

<53> 송신원 장치(210)란, 메일의 송신자가, 송신 대상인 전자 메일에 관한 각종 정보의 입력을 행할 때에 이용하는 기기이다. 그 예로서는, 퍼스널 컴퓨터나 메일 송수신 기능을 가진 휴대 전화, PDA(휴대 정보 단말기) 등이며, 설치형, 휴대형의 구별은 문제삼지 않는다.

<54> 송신원 장치(210)는, 제어 기능(2101)에, 입력 기능(2102), 출력 기능(2103), 통신 기능(2104) 등의 기능으로 구성된다. 각 기능은, 송신원 장치(210)의 처리 내용에 따라, 적절하게, 제휴해서 처리를 행한다. 입력 기능(2102)은, 키보드(21021), 마우스(21022), USB 메모리(21023) 등으로 구성된다. USB 메모리(21023)에는, 메일 소프트, 송수신자를 특정하기 위한 정보 등(송수신자의 메일 어드레스, 송수신자 ID)이 저장되어 있다. 송신원 장치(210)는, 메모리, 하드 디스크를 포함하는 기억 장치, CPU 등의 처리 장치를 갖고, 기억 장치에 저장된 프로그램에 따라서, 처리 장치가 정보 처리를 실행하는 것이다.

<55> 여기서, USB 메모리(21023) 내에 기억되는 송수신자 ID는, 송수신자의 메일 어드레스에 대응하여, 송수신자 쌍방의 식별에 이용하는 것이다. 통상적으로, 메일의 송신 시에는, 메일 헤더 부분에 기재된 메일 어드레스에 기초하여, 메일 서버간에서의 송수신이 행하여지지만, 상기 송수신자 ID는, 메일의 송수신자를 특정하기 위해서, 메일 보디 부분에 기재되는 내부 정보의 위치 결정이다. 또한, 상기 송수신자 ID는, USB 메모리 내의 재기입 불가능한 에리어에 저장하거나, 혹은, 재기입 가능한 에리어에 저장되는 경우에도, 재기입 시에 특별한 장치를 필요로 하거나 하여, 용이하게 변경할 수 없도록 하는 것이 바람직하다.

<56> (2) 송신원측 메일 서버(220), 및, 송신처측 메일 서버(230)의 장치 구성

<57> 송신원측 메일 서버(220), 및, 송신처측 메일 서버(230)는, 송신원 장치(210), 및, 송신처 장치(240)간에서 메

일의 송수신을 행할 때의 중개 장치로서 동작하고, 제어 기능, 입력 기능, 출력 장치, 통신 기능 등으로 구성된다.

<58> 또한, 동일한 기업이나 부서, 프로바이더 등 내에서 메일의 송수신을 행할 때에는, 송신원측 메일 서버(220), 및, 송신처측 메일 서버(230)는, 단일의 장치로 되는 경우도 있다.

<59> (3) 송신처 장치(240)의 장치 구성

<60> 송신처 장치(240)는, 메일의 수신자가, 수신 대상인 전자 메일에 관한 각종 정보의 입출력을 행할 때에 이용하는 기기로서, 송신원 장치(210)와 마찬가지로, 퍼스널 컴퓨터나 메일 송수신 기능을 가진 휴대 전화가 그 예이다. 송신처 장치(240)를 구성하는 각 기능은, 기본적으로, 송신원 장치(210)와 마찬가지이므로, 상세한 설명은 생략한다.

<61> (4) 통신 네트워크(250)의 장치 구성

<62> 송신원 장치(210), 송신원측 메일 서버(중개 장치)(220), 송신처측 메일 서버(중개 장치)(230), 및, 송신처 장치(240)간의 통신을 행하기 위한 통신 네트워크(250)는, 전용선이나 인터넷 등의 통신 회선 등이며, 유선, 무선의 구별은 문제삼지 않는다.

<63> 다음으로, 도 2를 인용하면서, 도 1의 처리 플로우에 따라, 본 실시예에서의 처리 동작을 설명한다.

<64> (1) 송신원 장치(210)의 처리 동작

<65> 입력 기능(2102)으로부터, 송신 대상인 전자 메일에 관한 각종 정보(메일의 수신처, 텍스트 본문, 첨부 파일 등의 입력, 화면 상의 버튼의 선택 등)를 입력하여, 메일의 작성을 행한다(스텝 111).

<66> 작성한 메일로부터, 비밀 분산법을 이용하여 복수의 부절 데이터를 생성함으로써, 복수의 메일로 분할한다(스텝 112).

<67> 분할한 원 메일의 송수신에 필요로 되는 각종 정보를 메일의 헤더 부분 및 보디 부분에 기재한 복수의 전자 메일(부분 메일 및 부속 메일)을 생성하고, 통신 네트워크(250)를 통하여, 송신원측 메일 서버(220)에 송신한다(스텝 113).

<68> (2) 송신원측 메일 서버(220)의 처리 동작

<69> 송신원 장치(210)로부터 송신된 전자 메일을 수신하고, 송신처측 메일 서버에, 수신한 메일을 전송한다(스텝 121).

<70> (3) 송신처측 메일 서버(230)의 처리 동작

<71> 송신원측 메일 서버(220)로부터 송신된 전자 메일을 수신한다(스텝 1311).

<72> (4) 송신처 장치(240)의 처리 동작

<73> 입력 기능(2102)으로부터, 수신 대상인 전자 메일에 관한 각종 정보(메일의 수신자에 관한 정보, 화면 상의 버튼의 선택 등)를 입력하여, 복수의 메일의 수신을 행한다(스텝 141).

<74> 수신한 메일의 개찬의 유무에 관하여, 체크를 행한다(스텝 142).

<75> 개찬이 없는 경우에는, 메일의 복원을 행하고(스텝 143), 있는 경우에는, 처리를 종료한다. 복원한 메일을, 출력 장치(240)에 표시한다(스텝 113).

<76> 이하에, 실시예의 각 처리 스텝의 일부에 관하여, 상세하게 설명한다.

<77> [송신원 장치(210):스텝 111]

<78> 도 3은, 송신원 장치(210)로부터의 메일의 입력 화면을 나타내는 이미지도이다. 출력 장치(2103) 상의 화면은, 4개의 에리어(메일의 작성, 보존, 표시 등에 관한 처리 종별의 입력을 접수하기 위한 기본 메뉴 선택 에리어(301), 송신 대상인 메일의 편집에 관한 처리 종별을 접수하기 위한 편집 메뉴 선택 에리어(302), 수신처나 제명 등의 입력을 접수하기 위한 헤더 정보 입력 에리어(303), 메일 본문의 입력을 접수하기 위한 본문 입력 에리어(304), 메일에 첨부하는 첨부 파일의 리스트를 표시하는 첨부 파일 표시 에리어(305))로 분할되어 있다.

<79> 유저는, 송신 대상으로 되는 메일에 관한 각종 정보를, 송신 헤더 정보 입력 에리어(303), 본문 입력 에리어(304) 등에 입력함과 함께, 필요에 따라, 편집 메뉴 선택 에리어(302) 내의 첨부 파일 버튼을 눌러, 첨부 파일

을 선택하거나, 메일의 분할에 관한 정보(메일 분할수, 분할 룰 등)나 송신 간격, 부분 메일과 부속 메일의 각 총수에 관한 정보 등의 입력을 행한다. 여기서, 분할 룰이란, 복수의 메일로 분할할 때의 룰을 규정하는 것으로, 예를 들면 모든 분할 메일의 사이즈를, 특정한 사이즈로 분할하는 경우나, 첨부 파일의 사이즈가 큰 경우에, 텍스트 부분이 주로 되는 분할 메일과, 첨부 파일 부분이 주로 되는 분할 메일로 분할하는 경우 등에 이용하는 룰을 가리킨다.

<80> [송신원 장치(210):스텝 112]

<81> 도 4는, 메일의 분할 처리 플로우를 도시하는 이미지도이다.

<82> 원 메일의 메일 본문, 첨부 파일 등을 부절화하기 위해서, 부호화를 행한다. 통상적으로, 원 메일의 본문 부분은, 텍스트 형식의 정보가 기재되고, 첨부 파일 부분은, BASE64로 대표되는 부호화 방식에 의해 부호화된다. 여기서는, 비밀 분산법에 의해, 본문이나 첨부 파일 등의 정보를 부절 암호화하기 위해, 특정한 부호화 방식에 의해 부호열을 생성(인코드)한다. 부호화 알고리즘은, 메일 소프트 내에 저장되어 있다(스텝 1121).

<83> 비밀 분산법을 이용하여, 상기 부호열을 부절 암호화하여, 부절 데이터를 생성한다. 이 때, 생성하는 부절 데이터의 총수나 사이즈는, 스텝 111에서 입력한 수치를 이용한다. 또한, 비밀 분산법에 의한 부절 암호화 알고리즘은, 메일 소프트 내에 저장되어 있다(스텝 1122).

<84> 메일의 보디 부분에, 상기 부절 암호화한 부절 데이터 및 송신자 ID, 수신자 ID, 분할 메일 ID, 해당 부분 데이터 이외의 부분 데이터를 식별하는 페어 데이터 ID 등을 저장한 부분 메일을 생성한다. 메일의 헤더 부분은, 통상의 메일의 송수신에 사용하는 송수신자 어드레스나 제명 등을 기재한다(스텝 1123).

<85> 메일의 보디 부분에, 상기한 각 부절 데이터에 관한 정보열(예를 들면 해시 함수에 의해 산출한 메시지 다이제스트) 및 송신자 ID, 수신자 ID, 분할 메일 ID, 해당 부속분 데이터 이외의 부속 데이터를 식별하는 페어 데이터 ID 등을 저장한 부속 메일을 생성한다. 메일의 헤더 부분은, 통상의 메일의 송수신에 사용하는 송수신자 어드레스나 제명 등을 기재한다(스텝 1124).

<86> 도 5는, 부분 메일(510), 및, 부속 메일(520)의 개요를 도시하는 이미지도이다.

<87> 부분 메일(510)은, 메일 서버간에서의 송수신에 필요로 되는 헤더 정보(511), 분할 메일 ID, 및, 해당 부분 메일 이외의 부분 메일을 나타내는 페어 메일 ID 등을 기재하는 영역(512), 각 부절 데이터 및 송수신자 ID 등을 기재하는 영역(513)으로 구성된다.

<88> 부속 메일(520)은, 메일 서버간에서의 송수신에 필요로 되는 헤더 정보(521), 분할 메일 ID, 및, 해당 부속 메일 이외의 부속 메일을 나타내는 페어 메일 ID 등을 기재한 영역(522), 각 부절 데이터에 관한 정보열 및 송수신자 ID 등을 기재하는 영역(513)으로 구성된다.

<89> 또한, 비밀 분산법에 의한 부절 암호화의 대상으로서, 스텝 1121 및 스텝 1122의 설명에서는, 원 메일의 텍스트 본문 부분 및 첨부 파일 부분을 그 예로 하였지만, 상기 송신자 ID나 상기 수신자 ID 및 상기 분할 메일 ID나 상기 페어 메일 ID 등도 그 대상으로 하는 것도 생각된다. 이 경우, 후술하는 분할 메일의 개찬 체크(스텝 142) 및 메일의 복원(스텝 143)의 처리 플로우의 상세 부분에 약간의 변경이 발생하지만, 개요 플로우에는 영향은 없다.

<90> [송신처 장치(240):스텝 142]

<91> 도 6은, 송신처 장치(240)에서의 개찬 체크를 도시하는 이미지도이다.

<92> 부속 메일의 개수회분(이 경우에는, m)까지, 메일을 읽어들인다(스텝 1421). 각 부속 메일에 기재되어 있는 송수신자 ID를 읽어들인다(스텝 1422).

<93> 각 부속 메일 내의 각 부절 데이터에 관한 정보열을 읽어들인다(스텝 1423). 읽어들이는 대상의 부속 메일이 없어질 때까지, 반복하고, 스텝 1425로 천이한다(스텝 1424).

<94> 부분 메일의 개수회(이 경우에는, n)까지, 메일을 읽어들인다(스텝 1425). 각 부분 메일에 기재되어 있는 송수신자 ID를 읽어들인다(스텝 1426).

<95> 각 부분 메일 내의 부절 데이터로부터, 각각에 대응하는 정보열을 산출한다. 산출 시에는, 스텝 1124에서 이용한 알고리즘과 동일한 것을 이용한다(스텝 1427).

<96> 부속 데이터 내의 송수신자 ID 및 각 부절 데이터에 대응하는 정보열과 일치하는지의 여부를 판단하고(스텝

1428), 일치하는 경우에는, 스텝 1428로 상태를 옮기고, 일치하지 않는 경우에는 처리를 종료한다(스텝 1428). 읽어들이는 대상의 메일이 없어질 때까지, 반복한다(스텝 1429).

<97> [송신처 장치(240):스텝 143]

<98> 도 7은, 송신처 장치(240)에서의 원 메일의 복원 플로우의 개요를 도시하는 이미지도이다.

<99> 부분 메일의 개수회분(이 경우에는, n)까지, 메일을 읽어들인다(스텝 1431). 각 부분 메일 내의 부절 데이터를 기억 장치에 읽어들인다(스텝 1432). 읽어들이는 대상의 각 메일에 대해서, 반복한다(스텝 1433).

<100> 읽어들인 각 부절 데이터를 비밀 분산법에 이용한 알고리즘을 이용하여 통합한다. 비밀 분산법에 의한 부절 복호화 알고리즘은, 메일 소프트 내에 저장되어 있다(스텝 1434).

<101> 통합한 데이터(부호화열)를 디코드하여, 메일 본문, 첨부 파일 등의 데이터를 복원한다. 디코드에 필요한 알고리즘은, 메일 소프트 내에 저장되어 있다(스텝 1435).

<102> 이상 설명한 바와 같이, 본 실시예에 따르면, 전자 데이터를, 네트워크를 통하여 송수신할 때에, 비밀 분산법의 알고리즘을 이용하여 복수의 메일로 분할 송신함으로써 경로 상에서의 도청 및 복원의 위험성을 저하시킬 수 있으며, 또한, 가령, 네트워크 상에서 개찬 등의 조작이 행하여진 경우에도, 개찬의 검지를 용이하게 행하는 것이 가능하게 된다.

<103> 또한, 본 실시예에서는, 분할한 전자 메일의 송신처를 단일의 송신처 장치로서 설명하였지만, 원 메일의 특징(첨부 파일의 유무나 규모, 수신자측의 환경 등)을 가미하여, 복수의 송신처 장치에 대하여, 전자 메일을 송신하는 것도 생각된다. 예를 들면, 첨부 파일이, 설계 도면으로 대표되는 이미지 데이터나, 음악 파일 등인 경우에는, 원 메일의 텍스트 부분(예로서, 첨부 파일의 개요나, 지시 내용 등을 기재)을 주로 하는 부분 메일 및 부속 메일을 상기 실시예에 나타낸 송신처 장치(메일 서버)에 송신하고, 원 메일의 첨부 파일 부분을 주로 하는 부분 메일을 상기 송신처 장치 이외의 서버에 송신하는 형태가 생각된다. 이 내용에 관해서는, 이하, 제2 실시예로서 설명한다.

<104> 제1 실시예에 나타낸 부분 데이터(메일이나 파일 등을 비밀 분산법으로 분할한 부분 데이터) 중의 1개 이상의 부분 데이터를, 송신처 장치 이외의 서버에 송신하는 제2 실시예에 대해서, 설명한다.

<105> 도 8은, 본 발명의 제2 실시예를 도시하는 처리 플로우도이다. 도 9는, 본 실시예를 실현하기 위한 장치 구성을 포함하는 전자 데이터 송수신 시스템의 전체 이미지도이다.

<106> 우선, 도 9에 도시하는 전자 데이터 송수신 시스템의 전체 이미지도에 관해서 설명한다. 전자 데이터 송수신 시스템은, 송신원 장치(210)와, 송신원측 메일 서버(220)와, 송신처측 메일 서버(230)와, 송신처 장치(240)와, Web 서버(260)가, 통신 네트워크(250)로 접속된 시스템이다.

<107> 송신원 장치(210)와, 송신원측 메일 서버(220)와, 송신처측 메일 서버(230)와, 송신처 장치(240)의 장치 구성에 대해서는, 제1 실시예에서 설명하였으므로, 여기서는 생략한다.

<108> Web 서버(260)는, 송신원 장치가 작성한 부분 데이터를 저장하는 장치로서, 부분 데이터 저장용 영역을 갖고, 제어 기능, 입력 기능, 출력 기능 등으로 구성된다.

<109> 송신원 장치(210), 송신원측 메일 서버(220), 송신처측 메일 서버(230), 송신처 장치(240), 및 Web 서버(260)간의 통신을 행하기 위한 통신 네트워크(250)는, 전용선이나 인터넷 등의 통신 회선 등이며, 유선, 무선의 구별은 문제삼지 않는다.

<110> 다음으로, 도 9를 인용하면서, 도 8의 처리 플로우에 따라, 본 실시예에서의 처리 동작을 설명한다.

<111> (1) 송신원 장치(210)의 처리 동작

<112> 입력 기능(2102)이, 이용자의 조작에 따른 송신 대상인 전자 메일에 관한 각종 정보(메일의 수신처, 텍스트 본문, 첨부 파일 등의 입력, 화면 상의 버튼의 선택 등)의 입력을 접수한다. 그리고, 제어 기능에 의해, 이 내용에 따른 메일의 작성을 행한다(스텝 811). 처리의 상세에 대해서는, 전술한 스텝 111과 마찬가지이다.

<113> 작성된 메일로부터, 비밀 분산법을 이용하여 복수의 부절 데이터를 생성함으로써, 복수의 메일(부분 메일)로 분할한다. 다음으로, 작성한 부분 메일에 대해서, 송신처 장치(240)에 송신하기 위한 제1 부분 메일군(여기서는, n개의 부분 메일로 이루어짐)과, Web 서버(260)에 송신하기 위한 제2 부분 메일군(여기서는, s개의 부분 메일로 이루어짐)으로 분류한다. 또한, 개찬의 검지에 필요한 정보, 분할수 등 부분 메일로부터 원래의 메일로 복원하

기 위해 필요한 정보, 및 제2 부분 메일군의 저장 장소(URL 등)에 관한 정보를 분산해서 포함하는 1개 이상의 부속 메일(여기서는, m개의 부속 메일)을 작성한다(스텝 812). 여기서, 저장 장소는, 송신원 장치마다 미리 정해 두어도 되고, 송신원 장치의 지정에 의해 정해도 된다. 또한, 제2 부분 데이터군의 저장 장소는, 제1 부분 메일군의 영역(513)에 기재해도 되고, 제1 부분 메일군의 영역(513)과 부속 메일의 영역(523)으로 나누어 기재해도 된다.

<114> 송신원 장치(210)와 송신처 장치(240)의 송수신에 필요로 되는 각종 정보를 헤더 부분 및 보디 부분에 기재한 복수의 전자 메일(스텝 812에서 작성한 제1 부분 메일군 및 부속 메일군)을, 통신 네트워크(250)를 통하여, 송신원측 메일 서버(220)에 송신한다(스텝 813).

<115> 스텝 812에서 작성한 제2 부분 메일군을, 통신 네트워크(250)를 통하여, Web 서버(260)에 송신한다(스텝 814). 또한, 스텝 814에서는, 스텝 812에서 특정된 저장 위치에 대하여 저장하도록 요구하는 정보도 송신한다.

<116> 또한, 부분 메일의 작성에서, 메일 본문과 첨부 파일을 합한 것을 1개의 데이터로 하여, 비밀 분산법을 이용하여, 부분 메일을 작성해도 되고, 메일 본문과 첨부 파일을 따로따로 하여, 각각 비밀 분산법을 이용하여 부분 메일, 부분 파일을 작성해도 된다. 메일 본문과 첨부 파일을 따로따로 분할 처리하는 경우, 첨부 파일을, 비밀 분산법을 이용하여 분할하여, 제1 부분 파일군과 제2 부분 파일군으로 분류한 후, 제2 부분 파일군을, 스텝 813의 메일 송신보다 전에(나중이라도 됨), 통신 네트워크(250)를 통하여, Web 서버(260)에 송신·저장해 두어도 된다. 메일 본문과 첨부 파일을 따로따로 분할 처리한 경우에는, 송신처 장치는, 메일 본문만 복원하고, 메시지를 확인한 후에, 첨부 파일의 제2 부분 파일을 Web 서버(260)에 취득하러 가는 것도 가능하게 된다.

<117> (2) 송신원측 메일 서버(220)의 처리 동작

<118> 송신원 장치(210)로부터 송신된 전자 메일을 수신하고, 송신처측 메일 서버에, 수신한 메일을 전송한다(스텝 821).

<119> (3) 송신처측 메일 서버(230)의 처리 동작

<120> 송신원측 메일 서버(220)로부터 송신된 전자 메일을 수신한다(스텝 831).

<121> (4) Web 서버(260)의 처리 동작

<122> 송신원 장치(210)로부터 제2 부분 메일군을 수취한다(스텝 851).

<123> 수취한 제2 부분 메일군을, 소정의 장소에 저장한다. 저장 장소는, 스텝 814에서 송신되는 정보에 따라서, 즉, 스텝 812에서 특정된 저장 장소에 저장한다(스텝 852).

<124> 또한, 송신원 장치(210)로부터 Web 서버(260)의 저장 영역에 액세스(예를 들면 직접적으로 액세스)하여, 제2 부분 메일군을 저장해도 된다. 이 경우, 스텝 851과 스텝 852는, 동일 스텝으로서 실행해도 된다.

<125> (5) 송신처 장치(240)의 처리 동작

<126> 입력 기능(2102)이, 이용자의 조작에 따른 수신 대상인 전자 메일에 관한 각종 정보(메일의 수신자에 관한 정보, 화면 상의 버튼의 선택 등)의 입력을 접수한다. 그리고, 제어 기능이 복수의 메일(제1 부분 메일군, 부속 메일군)의 수신을 행한다(스텝 841).

<127> 스텝 841에서 취득한 부속 메일군에, 제2 부분 메일군의 저장 장소에 관한 정보가 포함되어 있는 경우, 그 정보에 기초하여, Web 서버(260)에 액세스하여, 제2 부분 메일군을 취득한다(스텝 842).

<128> 수신한 제1 부분 메일군, 및 취득한 제2 부분 메일군의 개찬의 유무에 관하여, 체크를 행한다(스텝 843). 개찬이 없는 경우에는, 메일의 복원을 행하고, 개찬이 있는 경우에는, 처리를 종료한다(스텝 844). 그리고, 복원한 메일을, 출력 장치(2403)에 표시한다(스텝 845).

<129> 또한, 송신원 장치에서, 메일 본문과 첨부 파일을 따로따로 분할 처리하고 있는 경우(부분 메일군과 부분 파일군을 작성한 경우)에는, 상기 스텝 842를 행하기 전에, 부분 메일군에 대해서, 개찬의 유무를 체크한 후, 메일 본문의 복원을 행하여, 메일 본문을 확인해도 된다. 이 경우, 그 후에, 스텝 842에서, 부속 메일에 포함되는 제2 부분 파일군의 저장 장소에 관한 정보에 기초하여, Web 서버(260)에 액세스하여, 제2 부분 파일군을 취득하고, 그 후에 스텝 843에서, 제2 부분 파일군의 개찬의 유무에 관하여, 체크를 행하고, 스텝 844에서, 첨부 파일의 복원을 행한다.

<130> 이하에, 본 실시예의 각 처리 스텝의 일부에 관하여, 상세하게 설명한다.

<131> [송신원 장치(210):스텝 812]

<132> 도 10은, 본 실시예에서의 메일의 분할 처리 플로우를 도시하는 이미지도이다.

<133> 원 메일의 메일 본문, 첨부 파일 등을 부절화하기 위해서, 부호화를 행한다. 통상적으로, 원 메일의 본문 부분은, 텍스트 형식의 정보가 기재되며, 첨부 파일 부분은, BASE64로 대표되는 부호화 방식에 의해 부호화된다. 여기서는, 비밀 분산법에 의해, 본문이나 첨부 파일 등의 정보를 부절 암호화하기 위해서, 특정한 부호화 방식에 의해 부호열을 생성(인코드)한다. 부호화 알고리즘은, 메일 소프트 내에 저장되어 있다(스텝 8121).

<134> 비밀 분산법을 이용하여, 상기 부호열을 부절 암호화하여, 부절 데이터를 생성한다. 이 때, 생성하는 부절 데이터의 총수나 사이즈는, 스텝 811에서 입력한 수치를 이용한다. 또한, 비밀 분산법에 의한 부절 암호화 알고리즘은, 메일 소프트 내에 저장되어 있다(스텝 8122).

<135> 메일의 보디 부분에, 상기 부절 암호화한 부절 데이터 및 송신자 ID, 수신자 ID, 분할 메일 ID, 해당 부분 데이터 이외의 부분 데이터를 식별하는 페어 데이터 ID 등을 저장한 부분 메일군(1개 이상의 부분 메일로 이루어짐)을 생성한다. 메일의 헤더 부분은, 통상의 메일의 송수신에 사용하는 송수신자 어드레스나 제명 등을 기재한다(스텝 8123).

<136> 작성한 부분 메일군에 대해서, 송신처 장치(240)에 송신하기 위한 제1 부분 메일군(1개 이상의 부분 메일로 이루어짐)과, Web 서버(260)에 송신하기 위한 제2 부분 메일군(1개 이상의 부분 메일로 이루어짐)으로 분류한다. 구체적으로는, 예를 들면, 각 부분 메일에 대해서, 각 부분 메일에 기재되어 있는 분할 메일 ID와, 배분 정보(제1인지 제2인지)를 기록한 관리 테이블을 작성한다. 여기서, 제1 부분 메일군과 제2 부분 메일군의 개수는, 도 3의 입력 화면의 편집 메뉴에 추가하여, 거기에서 설정하도록 해도 되고, 설정 파일 등에 미리 기재해 두고, 그것을 읽어들여 설정하도록 해도 된다(스텝 8124).

<137> 제1 부분 메일군의 구성은, 도 5에 도시하는 바와 같이, 메일 서버간에서의 송수신에 필요로 되는 헤더 정보(511), 분할 메일 ID, 및, 해당 부분 메일 이외의 부분 메일을 나타내는 페어 메일 ID 등을 기재하는 영역(512), 각 부절 데이터 및 송수신자 ID 등을 기재하는 영역(513)으로 구성된다. 제2 부분 메일군의 구성은, 제1 부분 메일의 구성과 마찬가지이어도 되고, 헤더 정보(511)를 제외한 구성으로 해도 된다.

<138> 메일의 보디 부분에, 상기한 각 부절 데이터에 관한 정보열(예를 들면 해시 함수에 의해 산출한 메시지 다이제스트)이나, 제2 부분 메일군의 저장 장소에 관한 정보, 분할수 등 부분 메일로부터 원래의 메일로 복원하기 위해 필요한 정보, 및 송신자 ID, 수신자 ID, 분할 메일 ID, 해당 부속분 메일 이외의 부속 메일을 식별하는 페어 데이터 ID 등을 저장한 1개 이상의 부속 메일을 생성한다. 메일의 헤더 부분은, 통상의 메일의 송수신에 사용하는 송수신자 어드레스나 제명 등을 기재한다. 여기서, 부속 메일에 저장하는 제2 부분 메일군의 저장 장소는, 도 3의 입력 화면의 편집 메뉴에 추가하여, 거기에서 설정하도록 해도 되고, 설정 파일 등에 미리 기재해 두고, 그것을 읽어들여 설정하도록 해도 된다(스텝 8125).

<139> 부속 메일의 구성은, 도 5에 도시하는 바와 같이, 메일 서버간에서의 송수신에 필요로 되는 헤더 정보(521), 분할 메일 ID, 및, 해당 부속 메일 이외의 부속 메일을 나타내는 페어 메일 ID 등을 기재한 영역(522), 각 부절 데이터에 관한 정보열, 제2 부분 메일군의 저장 장소에 관한 정보, 분할수 등 부분 메일로부터 원래의 메일로 복원하기 위해 필요한 정보, 및 송수신자 ID 등을 기재하는 영역(513)으로 구성된다.

<140> [송신처 장치(240):스텝 842, 스텝 843]

<141> 도 11은, 송신처 장치(240)에서의 제2 부분 메일군의 취득, 및 개찬 체크를 도시하는 이미지도이다.

<142> 수신한 부속 메일의 개수회분(이 경우에는, m)까지, 메일을 읽어들이고, 각 부속 메일에 포함되는 각 부절 데이터에 관한 정보열, 분할수 등 부분 메일로부터 원래의 메일로 복원하기 위해 필요한 정보, 제2 부분 메일군의 저장 장소에 관한 정보, 및 송신자 ID, 수신자 ID, 분할 메일 ID, 해당 부속분 메일 이외의 부속 메일을 식별하는 페어 데이터 ID를 읽어들인다(스텝 8421).

<143> 스텝 8421에서 읽어들인 각 부속 메일에 기재되어 있는 제2 부분 메일군의 저장 장소에 관한 정보로부터, 제2 부분 메일군의 저장 장소를 특정한다(스텝 8422).

<144> 상기 특정한 저장 장소에 네트워크(250)를 경유해서 액세스하여, 제2 부분 메일군을 취득한다(스텝 8423).

<145> 수신한 제1 부분 메일의 개수회(이 경우에는, n)까지, 메일을 읽어들이고, 각 부분 메일에 포함되는 부절 데이터 및 송신자 ID, 수신자 ID, 분할 메일 ID, 해당 부분 데이터 이외의 부분 데이터를 식별하는 페어 데이터 ID를 읽어들인다(스텝 8431).

<146> 취득한 제2 부분 메일의 개수회(이 경우에는, s)까지, 부분 메일을 읽어들이고, 각 부분 메일에 포함되는 부절 데이터 및 송신자 ID, 수신자 ID, 분할 메일 ID, 해당 부분 데이터 이외의 부분 데이터를 식별하는 페어 데이터 ID를 읽어들인다(스텝 8432).

<147> 제1 부분 메일군, 및 제2 부분 메일군의 각 부분 메일 내의 부절 데이터로부터, 각각에 대응하는 정보열을 산출한다. 산출 시에는, 스텝 8125에서 이용한 알고리즘(예를 들면, 해시 함수)과 동일한 것을 이용한다(스텝 8433).

<148> 스텝 8433에서 산출한 각 부절 데이터의 정보열과, 스텝 8421에서 읽어들인 각 부속 메일 내의 각 부절 데이터에 대응하는 정보열이 일치하는지의 여부를 판단하고, 일치하는 경우에는, 스텝 844로 상태를 옮기고, 일치하지 않는 경우에는, 예를 들면 에러 화면을 표시하고 처리를 종료한다(스텝 8434).

<149> [송신처 장치(240):스텝 844]

<150> 도 12는, 송신처 장치(240)에서의 원 메일의 복원 플로우의 개요를 도시하는 이미지도이다.

<151> 제1 부분 메일의 개수회분(이 경우에는, n)까지, 메일을 읽어들인다. 또한, 스텝 8423에서 취득한 제2 부분 메일을, 개수회분(이 경우에는, s) 읽어들인다(스텝 8441).

<152> 제1 부분 메일, 제2 부분 메일의 각 부분 메일 내의 부절 데이터를 기억 장치에 읽어들인다(스텝 8442). 읽어들인 각 부절 데이터를 비밀 분산법에 기초한 알고리즘을 이용하여 통합한다. 비밀 분산법에 의한 부절 복호화 알고리즘은, 메일 소프트 내에 저장해 둔다(스텝 8443). 통합한 데이터(부호화열)를 디코드하여, 메일 본문, 첨부 파일 등의 데이터를 복원한다. 디코드에 필요한 알고리즘은, 메일 소프트 내에 저장되어 있다(스텝 8444).

<153> 또한, 본 실시예에서는, 제1 부분 메일군과, 제2 부분 메일군으로 분류하고, 제2 부분 메일군을 1개의 Web 서버에 저장하는 경우에 대해서 설명하였지만, 분류수를 늘려서 제3, 제4 부분 메일군을 작성하고, 각각 서로 다른 Web 서버 상에 각각 저장하도록 해도 된다. 이 경우, 제1 부분 메일군에 각 Web 서버의 저장 위치를 포함시킨다. 또한, 제1 부분 메일군에, 제2 부분 메일군의 저장 위치를 포함시키고, 제2 부분 메일군에 제3 부분 메일군의 저장 장소를 포함시키는 등으로 순차적으로 저장 장소를 포함시키는 구성으로 해도 된다. 또한, 제1 부분 메일군과 제2 부분 메일군을 합해서야 비로소 제3 부분 메일군의 저장 장소를 특정할 수 있도록 구성해도 된다.

<154> 또한, 시스템의 부하나 메일 내용에 따라서, 부분 메일을 읽어들이는 타이밍을 변경하거나, 개찬 검지에 관한 스텝을 생략해서 실시하는 것도 가능하다.

<155> 또한, 부분 메일이나 부속 메일의 구조는, 제1 실시예에 기초하고 있으므로, 메일 소프트를 교체하지 않고, 송신처 장치에 따라서, 제1 실시예와 같은 실시 형태를 취하거나, 본 실시예와 같은 실시 형태를 취하거나 하는 것도 가능하다. 예를 들면, 부속 메일 중에, 제2 부분 메일군에 관한 위치 정보(URL이나 Web 서버에의 액세스권 등)가 없는 경우에는, 제1 실시예에 기재한 처리를 행하고, 위치 정보가 존재하는 경우에는, 본 실시예에 기재한 처리를 행한다.

<156> 제2 부분 메일군의 저장 장소는, 부속 메일군 내에 기재되어 있으므로, 제2 부분 메일군의 취득은, 메일 소프트에 의해 행하여져, 송신처 장치 및 그 조작자는, Web 서버의 존재나 장소를 의식하지 않고, 전자 데이터의 수신, 표시를 행할 수 있다.

<157> 또한, 인증에 관한 이하의 기능을 추가함으로써, 보다 안전하게 메일 및 첨부 파일의 송수신을 행할 수 있다. 인증에 관한 실시예를, 이하에 기재한다.

<158> 송신처 장치(210)는, 인증용 데이터를 작성하고, 비밀 분산법을 이용하여 분할하여, 인증용 부분 데이터(인증용 부분 데이터 A, 인증용 부분 데이터 B)를 작성한다. 여기서, 비밀 분산법에 의한 부절 암호화 알고리즘은, 메일 소프트 내에 저장해 둔다. 또한, 여기서 작성하는 인증용 데이터는, 송신처 장치마다 고정의 ID를 준비하고, 그것에 기초하여 작성해도 되며, 송신할 때마다 매회 ID를 작성하고, 그것에 기초하여 작성해도 된다. 또는, 송신원 장치나 송신처 장치에서, 공개 키 암호 방식에 의해 전자 서명을 작성하고, 그것에 기초하

여 인증용 데이터를 작성해도 된다. 다음으로, 송신처 장치(210)는, 인증용 부분 데이터 A는 자신이 보관하고, 인증용 부분 데이터 B는, 송신처 장치에 송부한다(송부 시에는, 암호화해서 송부, 혹은, IC 카드 등의 매체를 이용하여 직접 건네주는 것이 바람직하다).

<159> 송신원 장치, 및 송신처 장치가 서로를 인증할 때에는, 자신이 갖는 인증용 부분 데이터와 상대가 갖는 인증용 부분 데이터를 비밀 분산법에 기초한 알고리즘을 이용하여 통합하고, 원래의 인증용 데이터가 복원 가능한지의 여부로 인증을 행한다.

<160> 본 실시예와 같이, Web 서버를 이용하는 경우, 송신원 장치는, 인증용 부분 데이터 A를 Web 서버에 등록해 두고, 제2 부분 데이터 취득을 위해 송신처 장치로부터 Web 서버에 액세스가 있었을 때에, 상기 인증용 부분 데이터를 이용한 인증에 의해 액세스를 제어할 수 있다. 구체적으로는, 송신처 장치에 대하여, 인증용 부분 데이터 B의 제시를 재촉하는 처리를 행하고, 비밀 분산법에 기초한 알고리즘을 이용하여, Web 서버에 등록된 인증용 부분 데이터 A와 통합하여, 원래의 인증용 데이터를 복원할 수 있는 경우에, 액세스를 허가한다.

<161> 또한, 본 발명에는 상술한 실시예 이외의 양태도 포함되는 것은 분명할 것이다.

<162> 본 발명에 의해, 보다 안전하게 간이한 시스템 구성으로 전자 데이터의 송수신이 가능하게 된다.

발명의 효과

<163> 본 발명에 따르면, 보다 안전하게 간이한 시스템 구성으로 전자 데이터의 송수신이 가능하게 된다.

도면의 간단한 설명

<1> 도 1은 본 발명을 실시하기 위한 기본적인 흐름을 도시하는 처리 플로우 개요도.

<2> 도 2는 전자 데이터 송수신 시스템의 전체 이미지도.

<3> 도 3은 송신원 장치(210)로부터의 메일의 입력 화면을 도시하는 도면.

<4> 도 4는 메일의 분할 처리 플로우를 도시하는 도면.

<5> 도 5는 분할 메일의 이미지를 도시하는 도면.

<6> 도 6은 개찬 체크의 처리 플로우를 도시하는 도면.

<7> 도 7은 메일의 복원 처리 플로우를 도시하는 도면.

<8> 도 8은 본 발명의 제2 실시예를 실시하기 위한 기본적인 흐름을 도시하는 처리 플로우 개요도.

<9> 도 9는 본 발명의 제2 실시예에서의 전자 데이터 송수신 시스템의 전체 이미지도.

<10> 도 10은 본 발명의 제2 실시예에서의 메일 분할 처리 플로우를 도시하는 도면.

<11> 도 11은 본 발명의 제2 실시예에서의 제2 부분 메일군의 취득, 및 개찬 체크의 처리 플로우를 도시하는 도면.

<12> 도 12는 본 발명의 제2 실시예에서의 메일의 복원 처리 플로우를 도시하는 도면.

<13> <도면의 주요 부분에 대한 부호의 설명>

<14> 210 : 송신원 장치

<15> 220 : 송신원측 메일 서버

<16> 230 : 송신처측 메일 서버

<17> 240 : 송신처 장치

<18> 250 : 통신 네트워크

<19> 2101 : 제어 기능

<20> 2102 : 입력 기능

<21> 2103 : 출력 기능

<22> 2104 : 통신 기능

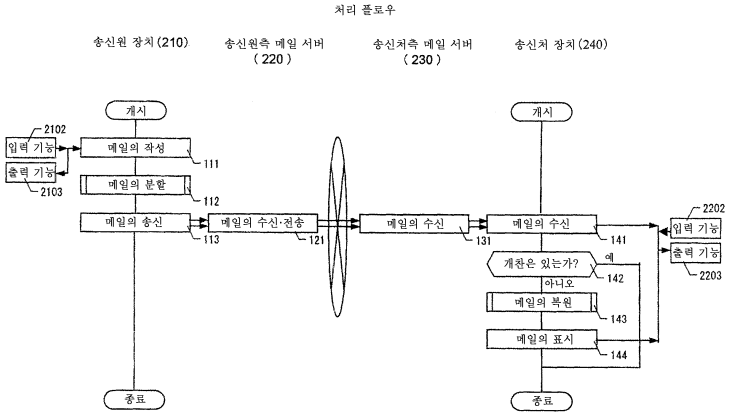
<23> 21021 : 키보드

<24> 21022 : 마우스

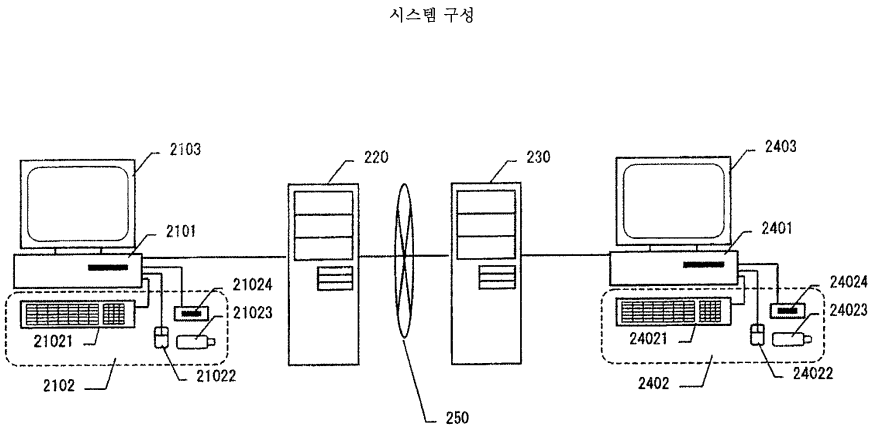
<25> 21023 : USB 메모리

도면

도면1

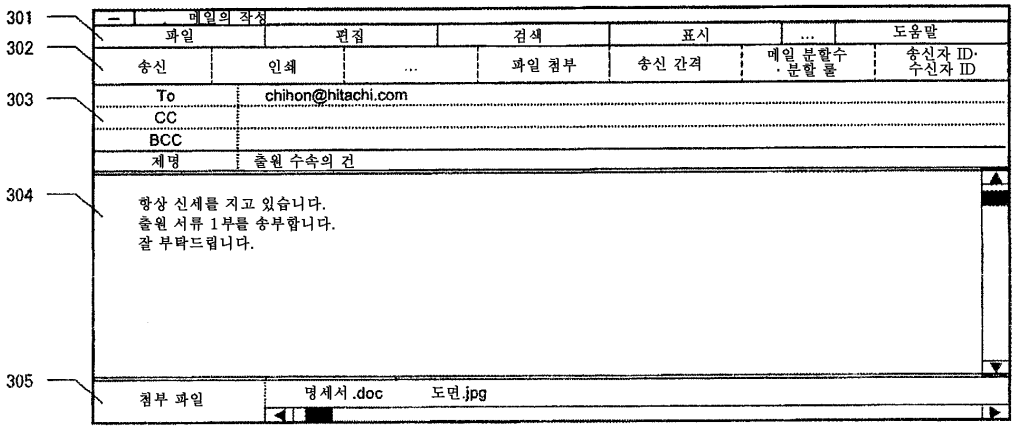


도면2



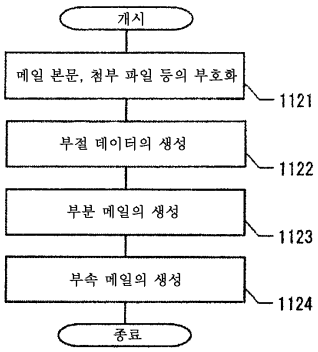
도면3

입력 화면



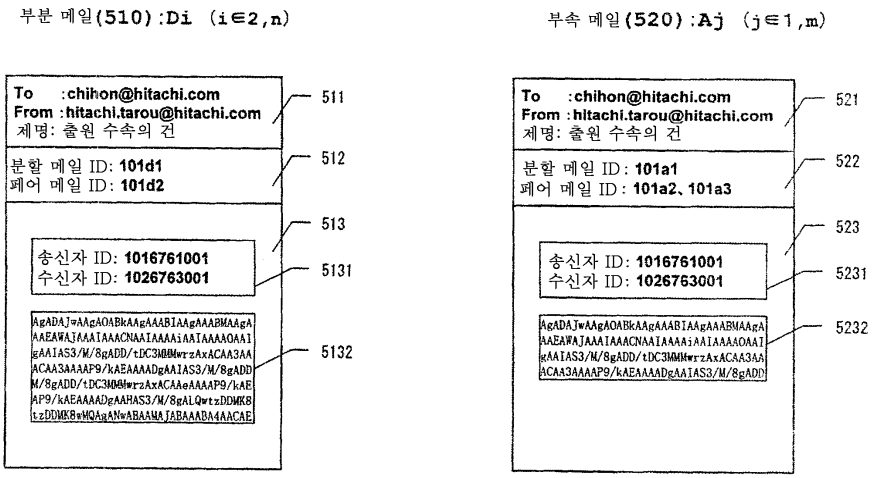
도면4

메일의 분할 처리 플로우



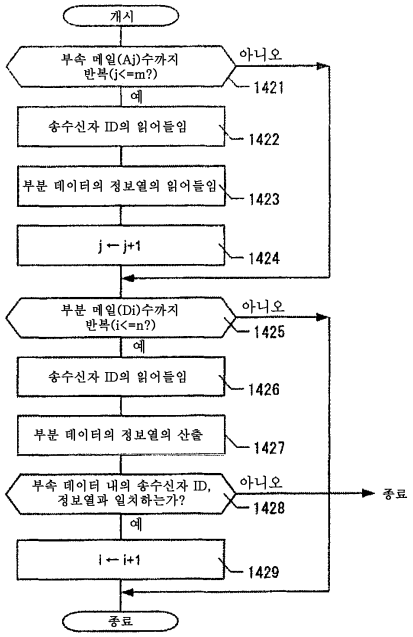
도면5

분할 메일



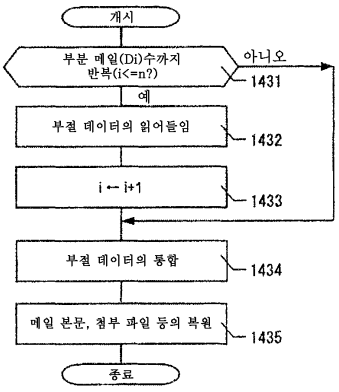
도면6

개찬 체크의 처리 플로우



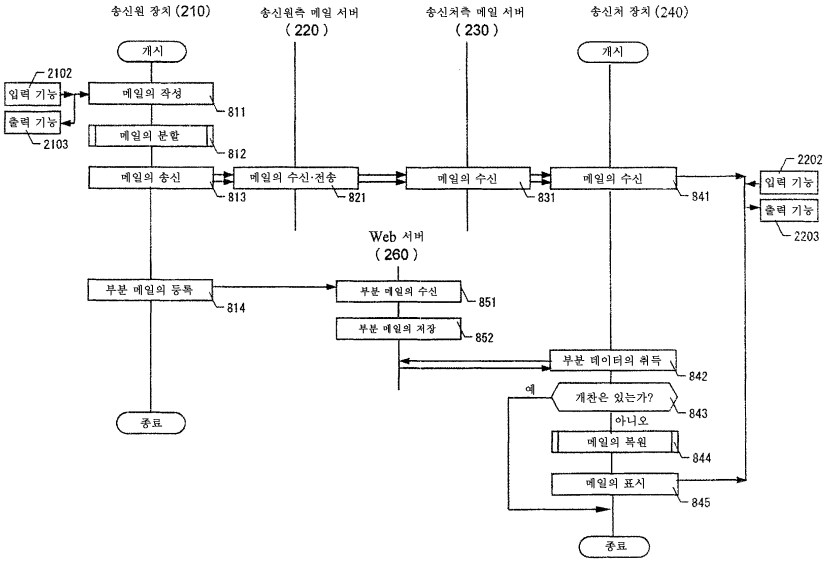
도면7

메일의 복원 플로우



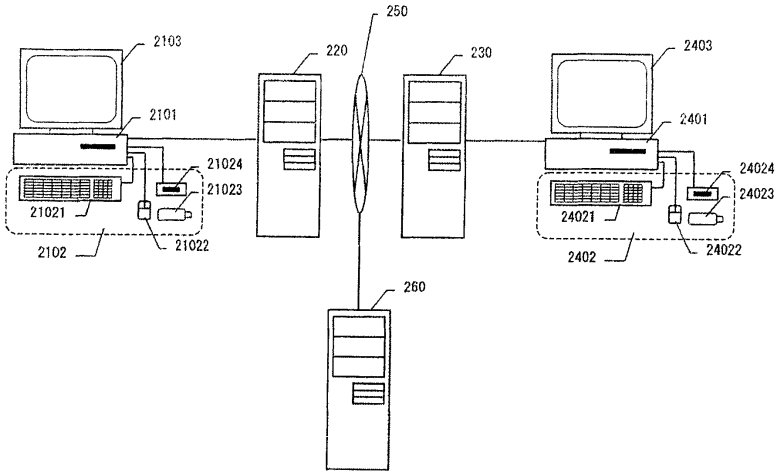
도면8

처리 플로우



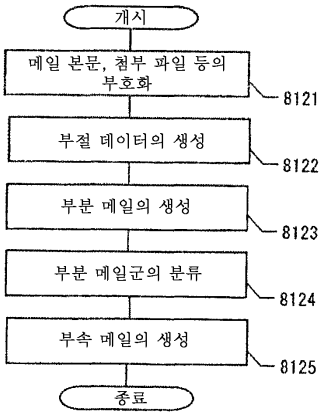
도면9

시스템 구성(제2 실시예)



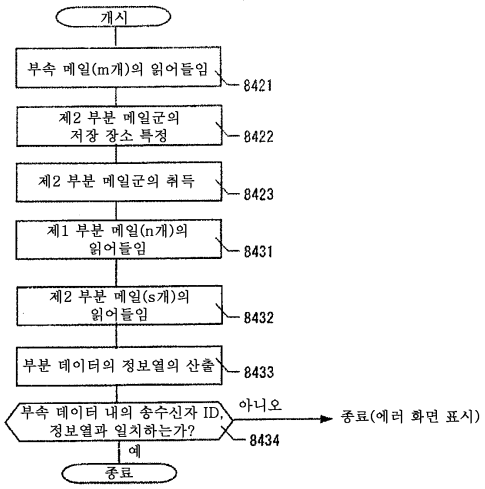
도면10

메일의 분할 처리 플로우(제2 실시예)



도면11

제2 부분 메일군의 취득, 개찬 체크의 처리 플로우



도면12

메일의 복원 플로우