(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년12월05일
(11) 등록번호 10-0782411
(24) 등록일자 2007년11월29일

(51) Int. Cl.
G06F 15/00 (2006.01) *G06F 17/00* (2006.01)
G06F 3/12 (2006.01)
(21) 출원번호 10-2006-0087830
(22) 출원일자 2006년09월12일
심사청구일자 2006년09월12일
(65) 공개번호 10-2007-0030146
(43) 공개일자 2007년03월15일
(30) 우선권주장
JP-P-2005-00264424 2005년09월12일 일본(JP)
(56) 선행기술조사문헌
특2001-0114190
전체 청구항 수 : 총 19 항

(73) 특허권자
캐논 가부시끼가이샤
일본 도꾜도 오오따꾸 시모마루꼬 3쪼메 30방 2고
(72) 발명자
키시모토 히로아키
일본국 도꾜도 오오따꾸 시모마루꼬 3쪼메 30방 2고 캐논가부시끼가이샤 나이
(74) 대리인
권태복, 이화익

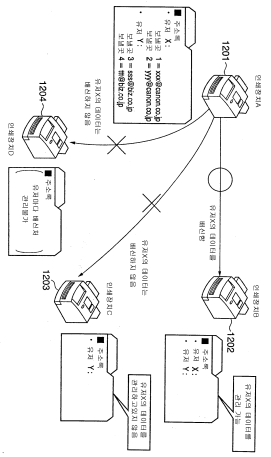
심사관 : 장대근

(54) 데이터 배신장치 및 데이터 배신방법

(57) 요 약

인쇄장치A에는, 주소록 데이터로서, 유저X에 액세스가 허용된 보낼곳 1, 보낼곳 2가 등록되고, 유저Y에 액세스가 허용된 보낼곳 3, 보낼곳 4가 등록되어 있다. 인쇄장치A로부터 주소록 데이터를 배신하는 경우, 배신처의 인쇄장치가 유저마다 주소록 데이터를 관리하는 기능을 갖는 것인가 아닌가가 판정된다. 인쇄장치B는, 상기 기능을 갖고, 게다가 유저X,Y가 함께 주소록 데이터에 등록되어 있다. 그래서, 인쇄장치A는, 유저X, Y와 관련된 보낼곳 데이터를 모두 인쇄장치B에 배신할 수 있다. 이에 대하여, 인쇄장치D는, 주소록 데이터를 유저마다 관리하는 기능을 갖지 않는다. 그래서, 인쇄장치A는, 주소록 데이터를 인쇄장치D에 배신할 수 없거나, 또는 권한이 있는 조작자에 의해 배신 조작된 경우에만 배신할 수 있다.

대표도 - 도12



특허청구의 범위

청구항 1

이용자를 특정하는 이용자 데이터와, 상기 이용자에 의한 액세스가 허가 또는 제한된 데이터가 관련지어진 제한 액세스 데이터를 격납하는 격납 수단(205)과,

상기 제한 액세스 데이터의 송신처 장치가, 상기 제한 액세스 데이터에 대한 액세스를 이용자마다 허가 또는 제한하는 액세스 관리기능을 갖는 것인가 아닌가 판정하는 기능 판정 수단(203; S602)과,

상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖지 않는다고 판정된 경우에, 인증 정보의 입력을 요구하고, 입력된 인증 정보를 사용해서 인증 처리를 행하는 인증 수단(203; S603-S604)과,

상기 인증 수단에 의한 인증처리가 성공한 경우에, 상기 제한 액세스 데이터를 상기 송신처 장치에 송신하는 송신 제어 수단(203; S605)을 구비한 것을 특징으로 하는 데이터 배신장치.

청구항 2

제 1 항에 있어서,

상기 기능 판정 수단에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 가진다고 판정된 경우에, 상기 격납 수단에 격납된 이용자 데이터 중에서, 상기 송신처 장치에서 격납된 이용자 데이터와 대응하는 공통 이용자 데이터를 판별하는 판별 수단(203; S608)을 더 구비하고,

상기 인증 수단은, 상기 격납수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터와 관련된 데이터를 송신할 때에, 인증 정보의 입력을 요구하고, 입력된 인증 정보를 사용해서 인증처리를 행하고,

상기 송신 제어 수단은, 상기 인증 처리가 성공한 경우에, 상기 격납 수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터와 관련된 데이터를 상기 송신처 장치에 송신하는 것을 특징으로 하는 데이터 배신장치.

청구항 3

제 2 항에 있어서,

상기 송신 제어 수단은, 상기 공통 이용자 데이터와 관련된 데이터를, 상기 인증 처리 없이 상기 송신처 장치에 대하여 송신하는 것을 특징으로 하는 데이터 배신장치.

청구항 4

제 1 항에 있어서,

상기 기능 판정 수단에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 가진다고 판정된 경우에, 상기 격납 수단에 격납된 이용자 데이터 중에서, 상기 송신처 장치에서 격납된 이용자 데이터와 대응하는 공통 이용자 데이터를 판별하는 판별 수단(203; S1101)과,

상기 격납 수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터를, 상기 송신처 장치에 등록하는 등록 수단(203; S1103)을 더 구비하고,

상기 송신 제어 수단은, 상기 기능 판정 수단에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 가진다고 판정된 경우에, 상기 인증 처리 없이 상기 송신처 장치에 대하여 제한 액세스 데이터 전체를 송신하는 것을 특징으로 하는 데이터 배신장치.

청구항 5

제 1 항 내지 제 4 항 중 어느 한 항에 있어서,

상기 제한 액세스 데이터는, 데이터를 송신하는 보낼곳 정보를 포함하고, 이용자마다 액세스가 허가 또는 제한되는 주소록 데이터인 것을 특징으로 하는 데이터 배신장치.

청구항 6

제 1 항 내지 제 4 항 중 어느 한 항에 있어서,

화상의 하드카피를 형성하는 화상형성수단(207)을 더 구비한 것을 특징으로 하는 데이터 배신장치.

청구항 7

격납 수단(205)에 격납된, 이용자를 특정하는 이용자 데이터와, 상기 이용자에 의한 액세스가 허가 또는 제한된 데이터가 관련지어진 제한 액세스 데이터를 배신하는 데이터 배신방법이며,

상기 제한 액세스 데이터의 송신처 장치가, 상기 제한 액세스 데이터에 대한 액세스를 이용자마다 허가 또는 제한하는 액세스 관리기능을 갖는 것인가 아닌가 판정하는 기능 판정 스텝(S602)과,

상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖지 않는다고 판정된 경우에, 인증 정보의 입력을 요구하고, 입력된 인증 정보를 사용해서 인증 처리를 행하는 인증 스텝(S603; S604)과,

상기 인증 스텝에 의한 인증 처리가 성공한 경우에, 상기 제한 액세스 데이터를 상기 송신처 장치에 송신하는 송신제어 스텝(S605)을 포함한 것을 특징으로 하는 데이터 배신방법.

청구항 8

제 7 항에 있어서,

상기 기능 판정 스텝에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 가진다고 판정된 경우에, 상기 격납 수단에 격납된 이용자 데이터 중에서, 상기 송신처 장치에 격납된 이용자 데이터와 대응하는 공통 이용자 데이터를 판별하는 판별 스텝(S608)을 더 포함하고,

상기 인증 스텝은, 상기 격납 수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터와 관련된 데이터를 송신할 때에 인증 정보의 입력을 또 요구하고, 입력된 인증 정보를 사용해서 인증 처리를 행하고,

상기 송신 제어 스텝은, 상기 인증 처리가 성공한 경우에, 상기 격납 수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터와 관련된 데이터를 상기 송신처 장치에 송신하는 것을 특징으로 하는 데이터 배신방법.

청구항 9

제 8 항에 있어서,

상기 송신 제어 스텝은, 상기 공통 이용자 데이터와 관련된 데이터를, 상기 인증 처리 없이 상기 송신처 장치에 대하여 송신하는 것을 특징으로 하는 데이터 배신방법.

청구항 10

제 7 항에 있어서,

상기 기능 판정 스텝에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 가진다고 판정된 경우에, 상기 격납 수단에 격납된 이용자 데이터 중에서, 상기 송신처 장치에서 격납된 이용자 데이터와 대응하는 공통 이용자 데이터를 판별하는 판별 스텝(S1102)과,

상기 격납 수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터를, 상기 송신처 장치에 등록하는 등록 스텝(S1103)을 더 구비하고,

상기 송신 제어 스텝은, 상기 기능 판정 스텝에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리 기능을 가진다고 판정된 경우에, 상기 인증 처리 없이 상기 송신처 장치에 대하여 제한 액세스 데이터 전체를 송신하는 것을 특징으로 하는 데이터 배신방법.

청구항 11

제 7 항 내지 제 10 항 중 어느 한 항에 있어서,

상기 제한 액세스 데이터는, 데이터를 송신하는 보낼곳 정보를 포함하고, 이용자마다 액세스가 허가 또는 제한된 주소록 데이터인 것을 특징으로 하는 데이터 배신방법.

청구항 12

이용자를 특정하는 이용자 데이터와, 상기 이용자에 의한 액세스가 허가 또는 제한된 데이터가 관련지어진 제한 액세스 데이터를 격납하는 격납 수단(205)과,

상기 제한 액세스 데이터의 송신처 장치가, 상기 제한 액세스 데이터에 대한 액세스를 이용자마다 허가 또는 제한하는 액세스 관리기능을 갖는 것인가 아닌가 판정하는 기능 판정 수단(203; S602)과,

상기 기능 판정 수단의 판정에 의해, 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖지 않는 경우에는, 상기 제한 액세스 데이터의 송신을 금지하고, 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖는 경우에는, 상기 제한 액세스 데이터를 상기 송신처 장치에 송신하는 송신 제어 수단(203; S605; S606-1)을 구비한 것을 특징으로 하는 데이터 배신장치.

청구항 13

격납 수단(205)에 격납된, 이용자를 특정하는 이용자 데이터와, 상기 이용자에 의한 액세스가 허가 또는 제한된 데이터가 관련지어진 제한 액세스 데이터를 배신하는 데이터 배신방법이며,

상기 제한 액세스 데이터의 송신처 장치가, 상기 제한 액세스 데이터에 대한 액세스를 이용자마다 허가 또는 제한하는 액세스 관리기능을 갖는 것인가 아닌가 판정하는 기능 판정 스텝(S602)과,

상기 기능 판정 스텝의 판정에 의해, 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖지 않은 경우는, 상기 제한 액세스 데이터의 송신을 금지하고, 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖는 경우에는, 상기 제한 액세스 데이터를 상기 송신처 장치에 송신하는 송신 제어 스텝(S605; S606-1)을 구비한 것을 특징으로 하는 데이터 배신방법.

청구항 14

컴퓨터에 로드되어서 실행되었을 때에, 이용자를 특정하는 이용자 데이터와, 상기 이용자에 의한 액세스가 허가 또는 제한된 데이터가 관련지어진 제한 액세스 데이터를 배신하는 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체로서, 상기 방법은,

상기 제한 액세스 데이터의 송신처 장치가, 상기 제한 액세스 데이터에 대한 액세스를 이용자마다 허가 또는 제한하는 액세스 관리기능을 갖는 것인가 아닌가 판정하는 기능 판정 스텝과,

상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖지 않는다고 판정된 경우에, 인증 정보의 입력을 요구하고, 입력된 인증 정보를 사용해서 인증 처리를 행하는 인증 스텝과,

상기 인증 스텝에 의한 인증 처리가 성공한 경우에, 상기 제한 액세스 데이터를 상기 송신처 장치에 송신하는 송신 제어 스텝을 구비한 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체.

청구항 15

제 14 항에 있어서,

상기 방법은, 상기 기능 판정 스텝에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 가진다고 판정된 경우에, 상기 격납 수단에 격납된 이용자 데이터 중에서, 상기 송신처 장치에서 격납된 이용자 데이터와 대응하는 공통 이용자 데이터를 판별하는 판별 스텝을 더 구비하고,

상기 인증 스텝은, 상기 격납 수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터와 관련된 데이터를 송신할 때에 인증 정보의 입력을 더 요구하고, 입력된 인증 정보를 사용해서 인증 처리를 행하고,

상기 송신 제어 스텝은, 상기 인증 처리가 성공한 경우에, 상기 격납 수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터와 관련된 데이터를 상기 송신처 장치에 송신하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체.

청구항 16

제 15 항에 있어서,

상기 송신 제어 스텝은, 상기 공통 이용자 데이터와 관련된 데이터를, 상기 인증 처리 없이 상기 송신처 장치에 대하여 송신하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체.

청구항 17

제 14 항에 있어서,

상기 방법은, 상기 기능 판정 스텝에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 가진다고 판정된 경우에, 상기 격납 수단에 격납된 이용자 데이터 중에서, 상기 송신처 장치에서 격납된 이용자 데이터와 대응하는 공통 이용자 데이터를 판별하는 판별 스텝과,

상기 격납 수단에 격납된 이용자 데이터 중 상기 공통 이용자 데이터 이외의 이용자 데이터를, 상기 송신처 장치에 등록하는 등록 스텝을 더 구비하고,

상기 송신 제어 스텝은, 상기 기능 판정 스텝에 의해 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 가진다고 판정된 경우에, 상기 인증 처리 없이 상기 송신처 장치에 대하여 제한 액세스 데이터 전체를 송신하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체.

청구항 18

제 14 항에 있어서,

상기 제한 액세스 데이터는, 데이터를 송신하는 보낼곳 정보를 포함하고, 이용자마다 액세스가 허가 또는 제한된 주소록 데이터인 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체.

청구항 19

컴퓨터에 로드되어서 실행되었을 때에, 이용자를 특정하는 이용자 데이터와, 상기 이용자에 의한 액세스가 허가 또는 제한된 데이터가, 관련지어진 제한 액세스 데이터를 배신하는 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체로서, 상기 방법은,

상기 제한 액세스 데이터의 송신처 장치가, 상기 제한 액세스 데이터에 대한 액세스를 이용자마다 허가 또는 제한하는 액세스 관리기능을 갖는 것인가 아닌가 판정하는 기능 판정 스텝과,

상기 기능 판정 스텝의 판정에 의해, 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖지 않는 경우는, 상기 제한 액세스 데이터의 송신을 금지하고, 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖는 경우에는, 상기 제한 액세스 데이터를 상기 송신처 장치에 송신하는 송신 제어 스텝을 구비한 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<17> 본 발명은, 정보의 동기의 유지, 및 정보의 배신을 행할 때에 정보의 시큐리티를 유지를 행할 수 있는 데이터 배신장치 및 데이터 배신방법에 관한 것이다.

<18> 최근, 네트워크에는, 복수의 프린터나 복사기, 팩시밀리, 또는 이 기능들을 갖는 복합기 등이 때때로 접속된다. 네트워크에 접속된 이들 장치(네트워크 장치라고 부른다.), 특히 팩시밀리와 복합기에는, 네트워크 설정에 관한 데이터와, E메일 및 팩시밀리의 보낼곳 정보를 포함하는 주소록 데이터 등, 여러 가지 데이터가 축적되어 있다. 또한, 네트워크 장치에는, 주소록 데이터를 이용자마다 관리하는 기능을 구비하는 것도 있다. 이용자마다 주소록을 관리하는 기능이란, 액세스 가능한 주소록 데이터를 이용자마다 제한하기 위한 기능이다. 그 기능을 갖는 장치는, 이용자가 주소록 데이터에의 액세스를 시험해 본 때는, 이용자에게 패스워드 입력을 요구해서 그 인증을 행한다. 인증이 성공한 경우에만 해당 이용자에 의해 액세스가 허용되어 있는 범위에서 주소록 데이터에의 액세스를 허용한다. 복수의 네트워크 장치에 의해 주소록을 공유하기 위한 기술로서, 네트워크 장치에 최신의 주소록 데이터를 송신하고, 그것에 의해서 각 장치가 갖는 주소록 데이터를 동기시키는 방법이 있다.

예를 들면, 일본국 공개특허공보 2002-232585호에는, 전자메일을 사용해서 전화번호부를 갱신하는 방법이 제안되어 있다. 이 방법에서는, 송신원으로 전자메일 본문에 전화번호부를 기재해서 송신하면, 수신한 장치는, 전자메일 본문에 포함되는, 상대편 정보에 대응하는 특정한 식별자를 검출한다. 그리고, 그 장치는, 그 식별자에 이어지는 텍스트 정보를 상대편 정보로서 전화번호부에 등록한다.

<19> 배신된 데이터가 액세스의 제한이 필요한 데이터, 예를 들면 개인 데이터일 경우이어도, 일본국 공개특허공보 2002-232585호에 기재되어 있는 기술을 사용해서 데이터의 배신을 행하면, 배신처의 네트워크 장치로는, 배신된 데이터에의 액세스를 제한할 수 없는 경우가 있다. 예를 들면, 배신처의 네트워크 장치가, 이용자마다 주소록에의 액세스의 제한을 행하는 기능, 즉 이용자마다의 관리기능을 갖지 않으면, 수신한 데이터를 주소록에 등록되었다고 하여도, 그 주소록에는 누구나 제한 없이 액세스할 수 있다.

<20> 상술한 것처럼, 각 네트워크 장치가 이용자마다 주소록 데이터를 관리할 수 있다고 하여도, 그 데이터를 다른 장치에 배신함에 의해, 주소록 데이터의 이용자마다의 관리가 깨진다. 이러한 문제점은, 주소록 데이터에 한정하지 않고, 액세스 제한을 필요로 하는 다른 종류의 데이터, 예를 들면 개인 데이터 등의 배신시에도 마찬가지로 생긴다. 또한, 네트워크 장치는, 복사기, 팩시밀리, 인쇄장치 또는 복합기에 한정하지 않고, 액세스 제한을 필요로 하는 데이터를 관리하는 다른 종류의 장치에 관해서도 마찬가지로, 이 문제는 생긴다.

발명이 이루고자 하는 기술적 과제

<21> 본 발명은, 상기 종래의 문제점을 해결하기 위한 것으로서, 액세스가 제한되어 있는 데이터를 하나의 장치로부터 다른 장치에 송신할 경우에, 배신처 장치가 갖는 기능에 따라 배신을 제한하고, 그것에 의해서 배신되는 데이터에의 액세스의 제한을 유지할 수 있는 데이터 배신장치 및 데이터 배신방법 및 그것을 실현하기 위한 프로그램을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

<22> 상기 목적을 달성하기 위해서 본 발명의 제 1의 국면에 의하면, 데이터 배신장치는,

<23> 이용자를 특정하는 이용자 데이터와, 상기 이용자에 의한 액세스가 허가 또는 제한된 데이터가 관련지어진, 제한 액세스 데이터를 격납하는 격납 수단과,

<24> 상기 제한 액세스 데이터의 송신처 장치가, 상기 제한 액세스 데이터에 대한 액세스를 이용자마다 허가 또는 제한하는 액세스 관리기능을 갖는 것인가 아닌가 판정하는 기능 판정 수단과,

<25> 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖지 않는다고 판정되었을 경우에, 인증 정보의 입력을 요구하고, 입력된 인증 정보를 사용해서 인증 처리를 행하는 인증 수단과,

<26> 상기 인증 수단에 의한 인증 처리가 성공한 경우에, 상기 제한 액세스 데이터를 상기 송신처 장치에 송신하는 송신 제어 수단을 구비한다.

<27> 또한, 상기 목적을 달성하기 위해서 본 발명의 제 2 국면에 의하면, 데이터 배신장치는,

<28> 이용자를 특정하는 이용자 데이터와, 상기 이용자에 의한 액세스가 허가 또는 제한된 데이터가 관련지어진 제한 액세스 데이터를 격납하는 격납 수단과,

<29> 상기 제한 액세스 데이터의 송신처 장치가, 상기 제한 액세스 데이터 에 대한 액세스를 이용자마다 허가 또는 제한하는 액세스 관리기능을 갖는 것인가 아닌가 판정하는 기능 판정 수단과,

<30> 상기 기능 판정 수단의 판정에 따라, 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖지 않는 경우에는, 상기 제한 액세스 데이터의 송신을 금지하고, 상기 제한 액세스 데이터의 송신처 장치가 액세스 관리기능을 갖는 경우에는, 상기 제한 액세스 데이터를 상기 송신처 장치에 송신하는 송신 제어 수단을 구비한다.

<31> 본 발명의 또 다른 특징은, (첨부된 도면을 참조하여) 예시적인 실시예에 관한 아래의 설명으로부터 명백해질 것이다.

<32> (실시예)

<33> 우선, 도 12를 참조해서 본 발명의 개략을 설명한다. 도 12에 있어서, 인쇄장치A(1201)에는, 주소록 데이터로서, 유저X에 액세스가 허용된 보낼곳 1, 보낼곳 2가 등록되고, 유저Y에 액세스가 허용된 보낼곳 3, 보낼

곳 4가 등록되어 있다. 인쇄장치A(1201)로부터 주소록 데이터를 송신하는 경우, 배신처의 인쇄장치가 유저마다 주소록 데이터를 관리하는 기능을 갖는 것인가 아닌가가 판정된다. 배신처인 인쇄장치B(1202)는 유저마다 주소록 데이터를 관리하는 기능을 가진다. 게다가, 유저X, Y가 함께 주소록 데이터에 등록되어 있다. 그 때문에, 유저X, Y와 관련된 보낼곳 데이터를 모두 인쇄장치A(1201)는 인쇄장치B(1202)에 배신할 수 있다. 이에 대하여, 인쇄장치D(1204)는 주소록 데이터를 유저마다 관리하는 기능을 갖지 않는다. 그래서, 인쇄장치A(1201)는 주소록 데이터를 인쇄장치D(1204)에 배신할 수 없는지, 또는 권한이 있는 조작자에 의해 배신 조작된 경우에만 배신할 수 있다. 조작자의 권한은 패스워드 등의 인증 정보를 사용해서 확인된다. 또 인쇄장치C(1203)는, 주소록 데이터를 유저마다 관리하는 기능을 갖지만, 주소록 데이터에 등록된 유저는 유저 Y뿐이다. 그 때문에, 유저X와 관련된 보낼곳 데이터는 인쇄장치C에는 배신할 수 없거나, 또는 권한이 있는 조작자에 의해 배신 조작된 경우에만 배신할 수 있다. 이하, 본 발명에 대해서 보다 자세한 설명을 행한다.

<34> [제1실시예]

<35> 도 1은, 본 발명의 제1실시예에 따른 정보배신 시스템을 나타낸다. 본 제1실시예에서는 이용자마다 액세스가 허가 또는 제한된 제한 액세스 데이터를 정보배신의 대상으로 삼는다. 그 제한 액세스 데이터의 일례로서, 제1 실시예는, 네트워크 장치인 복사 장치에 보존되어 있는 주소록 데이터를 예시한다. 주소록 데이터에 포함되는 보낼곳 데이터는, 복사 장치로 문서를 스캔한 문서 데이터나, 복사 장치 내에 보존하고 있는 문서 데이터를 팩시밀리나 전자메일(E 메일)등의 송신 수단을 사용해서 송신할 때에, 송신의 보낼곳으로서 이용된다.

<36> 도 1은, 복사 장치(101~103)의 접속 형태를 도시한 도면이다. 복사 장치 101은, 복사 장치 101에 격납된 주소록 데이터를, 네트워크(100)를 통해서, 복사 장치 102, 복사 장치 103에 송신할 수 있다. 즉, 주소록 데이터는 복사기 사이에 호환성을 가지고 있다. 호환성은, 각 복사 장치에 보존되는 주소록 데이터의 형식을 통일하여 유지할 수 있다. 또한, 보존되는 형식이 달라 있어도, 배신되는 데이터 형식에 호환성이 있으면 배신은 가능하다. 그 배신을 위한 일 방법으로서, XML을 사용해서 주소록 데이터에 포함되는 보낼곳 데이터 및 유저 데이터를 나타내는 태그를 정의해 두는 방법이 있다. 유저 데이터란, 유저의 액세스권과 인증 정보를 정의한 데이터이다. 그리고, 송신되는 정보의 의미를 태그로 나타냄으로써, 그 XML데이터를 수신한 복사 장치는 각 태그를 식별해서 주소록 데이터를 재구성할 수 있다. 복사 장치는 태그의 의미를 공유할 필요가 있지만, 이름공간을 별도로 정의해 두는 것으로 그것은 실현 가능하다. 보존되는 주소록 데이터도 XML로 기술해도 좋다. 이렇게 하여 주소록 데이터의 배신은 가능해지고 있다.

<37> 여기서, 복사 장치 101 및 복사 장치 102는, 유저마다 보낼곳 데이터를 관리할 수 있다. 즉, 주소록 데이터는, 유저의 액세스권을 특정하는 유저 데이터와, 각 유저에 의한 액세스가 허가된 보낼곳 데이터가 관련지어진 데이터베이스이다. 그 때문에, 복사 장치 101 및 복사 장치 102는, 유저마다 액세스를 허용하는 보낼곳 데이터를 제한할 수 있다. 본 제1실시예에서는, 이와 같이 액세스가 제한된 데이터를 제한 액세스 데이터라고 부른다. 또한, 본 제1실시예의 주소록 데이터에서는, 유저와 그 유저에 액세스가 허가된 보낼곳 데이터가 서로 관련되어 있다. 이에 대해, 유저와 그 유저에 의한 액세스가 금지된 보낼곳 데이터가 서로 관련되어도 된다. 여하간에, 유저와 그 액세스할 수 있는 범위는, 서로 관련되어야 한다. 또한, 복사 장치 101 및 복사 장치 102에서는, 모든 보낼곳 데이터가 이용자마다 액세스 제한되어 있다고는 할 수 없다. 불특정 유저가 액세스 가능한 보낼곳 데이터가 주소록 데이터에 포함되어도 된다.

<38> 이에 대하여, 복사 장치 103은 유저마다 보낼곳 데이터를 관리할 수 없다. 즉, 복사 장치 103에 보존된 주소록 데이터는, 불특정 유저에 의해 액세스 가능하다.

<39> <복사 장치의 구성>

<40> 도 2는 복사 장치의 블록도이다. 도 2에 있어서, 입력 화상 처리부(201)는, 종이 원고 등을 스캐너(209) 등의 화상 판독장치로 판독하여, 판독된 화상 데이터를 화상 처리한다. NIC(Network Interface Card)부/RIP부(202)는 NIC부와 RIP부를 포함한다. NIC부는 네트워크에 접속하기 위한 인터페이스이며, 네트워크를 통해서 입력된 화상 데이터(주로 PDL데이터)를 RIP부에 건네주거나, MFP내부의 화상 데이터나 장치 정보를 네트워크 경유로 외부에 송신한다. RIP 부는, 입력된 PDL(Page Description Language) 데이터를 해독하고, RIP(Raster Image Processor)전개를 수행한다(즉, 라스터 형식의 비트 맵 데이터(이하, 간단히 화상 데이터라고 부른다.)를 생성한다). RIP 부로 처리된 화상 데이터, 혹은 입력된 화상 데이터는, MFP제어부(203)에 보내진다.

<41> MFP제어부(203)는, 입력 데이터와 출력 데이터를 제어하는 역할을 한다. 또한, MFP제어부(203)에 입력된 화상 데이터는, 임시로 메모리부(205)에 격납된다. 격납된 화상 데이터는, 필요에 따라서 판독된다. MFP 제

어부(203)에는 (미도시된) 프로세서가 내장되어 있다. 이 프로세서에 의해 프로그램을 실행함으로써, 주소록 데이터의 관리, 주소록 데이터에 포함되는 보낼곳에 대한 전자메일의 송신, 주소록 데이터에 포함되는 팩시밀리 번호에 대한 팩시밀리 송신 등의 처리를 행한다. 주소록 데이터의 관리에는, 주소록 데이터의 편집 이외, 주소록 데이터의 다른 복사 장치에의 배신(도 6에서 설명한다.)과, 주소록 데이터의 수신(도 7에서 설명한다.) 등의 처리가 포함된다.

<42> 메모리부(205)에는, 주소록 데이터(205a), 그 주소록 데이터(205a) 관리를 위한 프로그램(205b)(도 6, 도 7a 및 도 7b의 순서를 포함한다.), 주소록 데이터 배신시에 참조되는 인증 정보(또는 그 일부)인 패스워드 데이터(205c)등이 격납되어 있다. 패스워드 데이터(205c)는, 유저가 주소록에 액세스하기 위한 인증 정보가 아니고, 주소록 데이터의 관리용의 정보이다. 메모리부(205)에는, 배신처 정보(205d)도 격납되어 있다. 배신처 정보(205d)에는, 배신처의 복사 장치를 특정하는 디바이스 식별 정보와, 그 배신처 복사장치의 기능을 나타내는 기능 정보가 등록되어 있다. 등록된 기능 정보에는, 해당 복사 장치가 주소록 기능을 갖는 것인가 아닌가, 및 주소록 기능을 갖는 경우에는, 액세스 관리기능을 갖는 것인가 아닌가를 나타내는 정보가 포함된다. 여기서, 액세스 관리기능이란, 주소록 데이터 등의 제한 액세스 데이터에 대한 액세스를 유저마다 허가 또는 제한하는 기능이다. 이러한 정보는, 2치 정보이고 플래그 등으로 나타낼 수 있다. 각 복사 장치는 각각을 특정하는 디바이스 식별 정보, 예를 들면 주소(IP 주소)로 나타내어진다. 그 주소와 상기 플래그를 관련시켜서 보존함으로써, 배신처의 복사 장치와 그 기능을 대응시킬 수 있다. 디바이스 식별 정보 및 기능 정보를 포함하는 배신처 정보(205d)는, 조작부(204)로부터 관리자 등에 의해 입력되어 메모리부(205)에 보존된다. 패스워드 데이터(205c)도, 미리 조작부(204)로부터 등록되어 메모리부(205)에 보존된다. 물론, 패스워드 데이터(205c)는, 네트워크를 거쳐서 퍼스널컴퓨터 등으로부터 등록될 수도 있다.

<43> 출력 화상 처리부(206)는, 프린트하기 위한 화상처리를 화상 데이터에 대하여 시행하고, 그 처리된 화상 데이터를 프린터부(207)에 보낸다. 화상처리에는, 예를 들면 양자화(2치화)와 유사 계조화라고 한 처리가 포함된다. 프린터부(207)에서는, 시트를 급지하고, 출력 화상 처리부(206)에서 처리된 화상 데이터를 그 시트 위에 순차로 형성한다. 화상이 형성된 시트는 후 처리부(208)에 보내지고, 시트의 구분 처리, 시트의 마무리 처리 등이 행해진다. 프린터부(207)에는, 그 동작을 제어하기 위한 프린터 제어부(210)가 구비되어 있다. 조작부(204)는, 이용자가 여러 가지 기능 등을 선택하고 조작 지시하기 위한 것이다.

<44> 조작부(204)는, 키 입력부와 터치 패널부로 이루어진다. 유저가 터치패널을 소정의 시퀀스로 조작하는 경우, 전자메일을 송신하거나, 혹은 팩시밀리 송신할 수 있다. 보낼곳을 입력할 때는, 유저는 주소록 데이터를 참조할 수 있다. 그러나, 유저가 참조할 수 있는 것은, 그 유저에 대하여 액세스가 허가되어 있는(혹은 액세스가 금지되어 있지 않은) 보낼곳 데이터에 한정된다. 불특정 유저가 참조 가능한 보낼곳 데이터(무제한 액세스 보낼곳 데이터라고 부른다.)에 관해서는 특히 유저 인증은 필요없다. 이와 대조하여, 액세스가 제한된 보낼곳 데이터에 관해서는, 유저에 의해 입력된 인증 정보, 예를 들면, 유저 식별자와 패스워드를, 미리 격납되어 있는 인증 정보와 대조한다. 그리고, 양자의 인증 정보가 일치하면, 즉 인증이 성공하면, 해당 유저에게 허용된 범위에서 보낼곳 데이터를 터치 패널부에 표시한다. 유저는 그 표시된 보낼곳 데이터 중에서 원하는 보낼곳을 선택하고, 전자메일이나 팩시밀리를 송신할 수 있다. 설치상은, 주소록 데이터의 참조가 유저에 의해 지시되었을 경우, 유저 식별자 및 패스워드 등의 인증 정보의 입력을 요구한다. 인증이 실패한 경우 혹은 인증하지 않은 취지가 입력되었을 경우에는, 무제한 액세스 보낼곳 데이터만을 표시한다. 한편, 인증이 성공하면, 그 무제한 액세스 보낼곳 데이터에 더해서 해당 유저가 액세스 가능한 보낼곳 데이터를 표시한다. 물론, 이것은 일례이며, 제한된 보낼곳 데이터를, 인증되지 않은 유저에 액세스시키지 않으면, 설치 형태로서는 여러 가지의 형태를 취득할 수 있다.

<45> 도 3은, 도 1의 복사 장치(101)의 조작부(204)에 표시된 주소록 데이터의 관리 화면이다. 복사 장치(101)의 주소록 데이터는 유저마다 관리된다. 이 경우에, 유저 A~F와 관련된 보낼곳 데이터가 격납되어 있다. 유저A~F의 각 유저는, 자신에게 관련지어진 보낼곳 데이터에 한해서 참조할 수 있다. 도 3의 화면(300)에는, 유저 표시란(302)이 표시되어 있다. 유저가 그 란을 선택하면, 유저에 의한 인증 정보의 입력이 요구된다. 인증이 성공하면, 선택된 보낼곳 데이터가 화면에 표시된다. 사용자가 배신 버튼(301)을 누르면, 주소록 데이터가 배신처 정보(205d)에 의해 특정되는 다른 복사 장치에 대하여 배신된다.

<46> 도 4는, 도 1의 복사 장치(102)의 조작부(204)에 표시된 주소록의 관리 화면이다. 복사 장치(102)의 주소록 데이터에는, 유저A, B, C의 보낼곳 데이터가 격납되어 있지만, 유저D, E, F의 보낼곳 데이터는 격납되어 있지 않다. 즉, 유저D, E, F는, 각각의 유저 자신이 보낼곳 데이터를 등록하지 않으면, 복사 장치(102)에 있어

서 보낼곳 데이터를 이용할 수는 없다.

<47> 도 5는, 도 1의 복사 장치(103)의 조작부(204)에 표시되는 주소록이다. 복사 장치(103)의 주소록 데이터는 유저마다 관리되고 있지 않고, 모든 보낼곳 데이터는, 복사 장치(103)를 이용하는 유저가 누구나 참조 및 이용할 수 있다. 즉, 복사 장치(103)의 주소록 데이터는 무제한 액세스 데이터이다. 본 제1실시예에서는, 복사 장치(103)는 액세스 관리기능을 갖지 않고, 유저마다 보낼곳 데이터를 관리할 수 없다.

<48> <데이터의 구성>

<49> 도 9a~도 9c는, 제1 실시예의 주소록 데이터의 구성 예를 나타내고, 도 9d는 배신처 정보(205d)의 일례를 나타낸다. 도 9a는, 복사 장치 101 및 복사 장치 102에 보존되는 주소록 데이터의 예이다. 주소록 데이터는 각각의 유저에 대응하는 유저 블록(911)마다 분할되어 있다. 유저 블록(911)은, 유저와 그 유저가 액세스할 수 있는 보낼곳 데이터가 관련시켜져 있다. 하나의 유저 블록에는, 유저를 특정하기 위한 데이터(유저 데이터) 910과, 그 유저와 관련된 보낼곳 데이터 912가 포함된다. 유저 데이터(910)에는, 유저를 식별하는 유저 식별자(유저ID)와, 거기에 대응해서 미리 등록된 패스워드가 포함된다. 보낼곳 데이터(912)에는, 보낼곳의 이름과 그 전자메일 주소 및 팩시밀리 번호가 포함된다. 이 데이터들은, 각 유저에 대해서 보존된다. 또한, 유저 데이터만 관련하는 보낼곳 데이터가 포함되지 않는 유저 블록도 생각할 수 있다.

<50> 도 9b는, 유저 블록에 더해서, 공유 블록(921)이 포함된 주소록 데이터의 예이다. 공유 블록에의 액세스는 제한되지 않는다. 공유 블록에는, 유저 데이터에 해당하는 영역에, 그것이 유저와 관련된 보낼곳 데이터에서는 없는 것을 나타내는 소정의 공유 식별정보가 보존되어 있다. 그 공유 식별정보와 관련된 보낼곳 데이터는 불특정 유저에 의해 이용할 수 있다.

<51> 도 9c는, 복사 장치(103)에 의해 보존되어 있는 주소록 데이터의 예이다. 복사 장치(103)가 액세스 관리기능을 갖지 않기 때문에, 유저 데이터는 불필요하다. 그래서, 주소록 데이터는 보낼곳 데이터를 검색 가능하게 모은 구성을 가진다. 도 9a, 도 9b 및 도 9c에서 주소록 데이터는 테이블 포맷으로 나타내지만, 전술한 바와 같이 XML등으로 정의한 태그를 사용하여 나타낼 수도 있다.

<52> 도 9d는, 배신원의 복사 장치(101)가 보존하는 배신처 정보(205d)의 일례를 나타낸다. 배신처 정보에는, 디바이스 식별 정보(941)와 기능 정보(942)가 포함된다. 디바이스 식별 정보(941)와 기능 정보(942)는 관련시켜져 있고, 기능 정보(942)는 관련지어진 배신처 장치의 기능을 나타낸다. 도 9d의 예에서는, 디바이스 식별 정보로서, 복사 장치 102의 주소와 복사 장치 103의 주소가 보존되어 있다. 그리고, 복사 장치 102와 관련된 기능 정보는 액세스 관리기능이 있는 것을 나타내는 반면에, 복사 장치 103과 관련된 기능 정보는 액세스 관리기능이 없는 것을 보이고 있다.

<53> 복사 장치 101은 주소록 데이터의 배신처리를 행하기 전에, 복사 장치 102 및 103이 액세스 제어기능을 갖는지의 여부를, 복사 장치 102 및 103에 대하여 네트워크를 통해서 문의할 수도 있다. 복사 장치가 액세스 제어기능을 갖는 것인가 아닌가의 판정에는, SNMP(Simple Network Management Protocol)등의 프로토콜을 사용할 수 있다.

<54> <주소록 데이터의 배신처리>

<55> 다음에, 도 1의 복사 장치 101로부터 복사 장치 102에 주소록 데이터를 배신하는 처리에 대해서 도 6, 도 7a 및 도 7b의 흐름도를 참조해서 설명한다. 도 6은, 복사 장치 101로부터 주소록 데이터를 복사 장치 102에 배신하는 경우의, 복사 장치 101의 MFP제어부(203)에 의해 실행되는 처리의 흐름도다. 이 흐름도는, 도 3의 배신 버튼(301)이 눌린 경우에 개시된다.

<56> 스텝S601에 있어서, 우선 배신처 정보(205d)를 참조해서 주목 배신처의 기능을 체크한다. 주목 배신처란, 배신처 정보(205d)에 있어서, 예를 들면, 그 정렬 순으로 선택한 하나의 배신처이다. 따라서, 최초는 배신처 정보(205d)의 선두에 등록된 디바이스 식별 정보에 의해 특정되는 배신처가 주목 배신처가 된다. 도 9d의 예에서는 최초의 주목 배신처는 복사 장치(102)이다. 그리고, 그 주목 배신처와 관련된 기능 정보를 읽는다.

<57> 스텝S601에서는, 판독한 기능 정보에 의해, 주목 배신처에 액세스 관리기능이 있는지 판정한다. 액세스 관리기능이 있다고 판정되면, 스텝S608로 분기되고, 주목 배신처에서는, 배신원 장치에 보존된 주소록 데이터에 포함되는 전체 보낼곳 데이터를 유저별로 관리하고 있는지 판정한다. 즉, 도 9b와 같이 공유 ID가 주소록 데이터에 포함되어 있으면, 전체 보낼곳 데이터가 유저별로 관리되지 않고 있다고 판단할 수 있다. 이 판정 때문에, 이하의 방법을 취할 수 있다. 즉, 주목 배신처에 대하여, 주소록 데이터에 포함되는 유저 데이터의 리스트의 요

구를 송신한다. 그리고, 주목 배신처의 장치로부터 그 요구에 대한 응답을 수신했다면, 수신한 유저 데이터의 리스트에 포함되는 유저 데이터와, 송신원의 복사 장치의 주소록 데이터에 포함되는 유저 데이터를 대조한다. 조회의 결과, 만약 수신한 유저 데이터의 리스트가, 송신원 복사 장치에 보존된 주소록 데이터에 포함되는 유저 데이터를 포함하고 있으면, 주목 배신처에서는 송신원 장치의 주소록의 전체 보낼곳을 유저별로 관리하고 있다고 판단할 수 있다. 이때, 한 사람의 유저이어도, 패스워드는 장치마다 다른 가능성이 있기 때문에, 대조의 대상에 패스워드는 포함되지 않는다.

<58> 스텝S608에 있어서, 주목 배신처에서는 송신원 장치의 주소록의 전체 보낼곳을 유저별로 관리하고 있다고 판정된 경우, 스텝S605로 분기되어서 주소록 테이블을 주목 배신처에 송신한다. 주소록 데이터는, 본 예에서는 XML형식으로 하고, 배신처는 배신처 정보에 등록된 주소이다. 그러나, 설명상은, 도 9a, 9b, 9c 등을 참조해서 설명한다.

<59> 한편, 스텝S608에 있어서, 주목 배신처에서는 송신원 장치의 주소록의 전체 보낼곳을 유저별로 관리하고 있지 않다고 판정된 경우, 스텝S603으로 분기되어서 인증 정보, 예를 들면 전송용 패스워드의 입력을 요구한다. 스텝S602에 있어서, 주목 배신처에 액세스 관리기능이 없다고 판정된 경우에도, 스텝S603으로 분기되어서 전송용 패스워드의 입력을 요구한다.

<60> 주소록 데이터의 배신조작을 행한 관리자에 의해 전송용 패스워드가 입력되면, 패스워드 데이터(205c)와 대조되어, 일치하면 인증 성공인 취지를 나타내는 정보가 일시적으로 메모리부(205)에 보존된다. 일치하지 않을 경우, 혹은 패스워드 입력이 스킵되었을 경우에는, 인증 실패인 취지를 나타내는 정보가 일시적으로 메모리부에 보존된다.

<61> 스텝S604에서는 인증이 성공한 것인가 아닌가 판정한다. 성공이면, 스텝S605로 분기되어서 주소록 테이블을 주목 배신처 장치에 송신한다. 그러나, 스텝S602에 있어서 NO라고 판정되어 있는 경우에는, 주목 배신처의 장치는 유저 데이터를 필요로 하지 않는다. 그래서 이 경우에는 유저 데이터를 송신할 필요가 없다.

<62> 스텝S604에 있어서 인증이 실패했다고 판정된 경우에는, 스텝S606-1로 분기된다. 스텝S606-1에 있어서는, 주목 배신처의 복사 장치에 의해 유저별 관리가 되는 보낼곳 데이터가 있으면, 그 보낼곳 데이터와 관련되는 유저 데이터를, 주목 배신처에 송신한다. 예를 들면, 송신원이 도 3의 주소록 데이터를, 주목 송신처가 도 4의 주소록 데이터를 격납하고 있는 것으로 한다. 이 경우, 유저A, B, C에 관련되는 보낼곳 데이터는, 주목 배신처에 있어서도 각각의 유저에 대해서 관리된다. 이에 대하여 유저D, E, F는, 주목 배신처의 주소록 데이터에는 등록되어 있지 않고, 이 유저들과 관련된 보낼곳 데이터는 각각의 유저에 대해서 관리되지 않는다. 그래서, 스텝S604에 있어서 인증에 실패했다고 판정되면, 스텝S606-1에서는, 유저A, B, C에 관련되는 보낼곳 데이터만이 주목 배신처에 송신된다. 물론, 주목 배신처의 장치에 액세스 관리기능이 없으면 스텝S606-1에 있어서 송신해야 할 데이터는 없다. 그리고, 스텝S606-2에 있어서는, 스텝S606-1에서 송신된 데이터 이외의 데이터를 송신할 수 없는 취지를 조작부(204)에 표시한다. 전술한 도 4 및 도 5의 예에서는, 유저D, E, F와 관련된 보낼곳 데이터는 송신할 수 없으므로, 스텝S606-2에서는 그 취지가 표시된다.

<63> 스텝S606-2, 혹은 스텝S605 후에는 스텝S607로 분기된다. 스텝S607에서는, 배신처 정보(205d)에 등록되어, 아직 주목되지 않고 있는 배신처가 아직 있는지 판정한다. 있으면, 다음(미배신의) 배신처는 주목 배신처로서 설정되고, 스텝S601로 분기된다.

<64> 이상과 같이, 배신처의 장치에 의해 유저마다 관리되지 않는 보낼곳 데이터를 배신할 때에는, 인증 정보의 입력을 요구하고, 인증 정보가 입력되지 않은 경우에는 배신을 행하지 않는다. 이 때문에, 배신처의 장치에 있어서 주소록 데이터가 무제한으로 액세스 가능해지는 사태를 사전에 방지할 수 있다.

<65> 도 7a는, 액세스 관리기능을 갖는 배신처 복사 장치(예를 들면, 복사 장치 102)가, 도 6의 스텝S605 또는 스텝S606-1에 의해 송신된 주소록 데이터를 수신했을 때의 처리를 나타내는 흐름도이다. 스텝S701에 있어서, 우선 수신한 주소록 데이터에 포함되는 유저 데이터 중, 선두의 유저 데이터, 특히 유저 ID에 주목한다. 그리고, 그 주목 유저 ID가, 배신처 장치가 갖는 주소록 데이터에 등록되어 있는지 판정한다(S702). 등록되어 있으면, 수신한 주소록 데이터에 포함되고, 주목 유저 데이터와 관련된 보낼곳 데이터를, 배신처 복사 장치가 갖는 주소록 데이터에 등록한다(S704). 등록된 보낼곳 데이터는, 주목 유저 데이터의 유저 ID와 동일한 유저 ID를 갖는 유저 데이터와 관련된다. 이때, 추가적으로 등록할지, 덮어 쓰기적으로 등록할지는 관리자에게 선택하게 하여도 된다. 이와는 달리, 등록방법은, 미리 결정되어도 된다.

<66> 한편, 스텝S702에 있어서, 주목 유저 데이터가, 배신처 장치의 주소록 데이터에 등록되지 않고 있는 경

우에는, 스텝S703으로 분기된다. 스텝S703에서는, 수신한 주소록 데이터에 포함되고, 주목 유저 데이터와 관련된 보낼곳 데이터를, 공유 ID에 관련지어서, 배신처 복사 장치가 갖는 주소록 데이터에 등록한다. 즉, 배신처 장치에서 관리되지 않고 있는 유저와 관련된 보낼곳 데이터가 배신된 경우, 그 보낼곳 데이터에 대한 액세스 제한은 해제된다.

<67> 스텝S703 및 S704 후에는, 스텝S705에 있어서, 수신한 주소록 데이터에, 주목 유저 데이터의 이외의 미주목의 유저 데이터가 있는지 판정한다. 있으면, 다음 유저 데이터에 주목해서(S706), 스텝S702부터 반복한다.

<68> 수신한 주소록 데이터에 포함되는 태그에 의해 유저 데이터와 그 유저 데이터에 관련된 보낼곳 데이터가 표시되어 있기 때문에, 유저 데이터와 보낼곳 데이터를 수신한 주소록 데이터로부터 추출할 수 있다. 태그가 아니더라도, 미리 정의된 필드 코드 등을 송신원 장치와 송신처 장치가 공유하고 있으면, 데이터를 공유할 수 있다.

<69> 배신원 장치와 배신처 장치에서 공통되는 유저 데이터(공통 유저 데이터)가 있으면, 공통 유저 데이터에 관련되는 보낼곳 데이터는, 배신처 장치에서도 유저마다 관리된다. 즉, 유저마다 액세스가 허가되거나 혹은 제한된다.

<70> 도 7b는, 액세스 관리기능을 갖지 않는 복사 장치, 예를 들면 복사 장치(103)가, 주소록 데이터를 수신했을 때의 처리 순서의 예를 나타낸다. 스텝S711에서는, 수신한 주소록 데이터에 포함되는 보낼곳 데이터를, 모두 주소록 데이터에 등록한다. 등록이 추가인지 덮어쓰기인지는 관리자에게 선택되거나, 미리 결정해 둔다.

<71> <주소록 데이터에의 액세스>

<72> 도 8은, 액세스 관리기능을 갖는 복사 장치에 있어서, 주소록 데이터에 액세스할 때의 처리 순서를 나타낸다. 예를 들면, 도 8은, 도 3의 표시 화면에서, 유저 표시란(302)을 누르는 등의 조작이 행해지고, 특정한 유저와 관련된 보낼곳 데이터에의 액세스가 요구된 경우의 수순을 나타낸다.

<73> 우선, 액세스가 요구된 유저에 대응하는 액세스용 인증 정보, 예를 들면, 패스워드의 입력을 요구한다. 액세스가 요구된 유저는, 눌려진 유저 표시란에 대응한다. 도 9a에서 설명한 바와 같이, 주소록 데이터에 포함되는 유저 데이터에는, 유저마다의 인증 정보(대조용의 패스워드)도 보존되어 있다. 이 패스워드는, 주소록 데이터에 유저를 등록할 때에 등록된다. 스텝S801에서는, 요구에 따라 패스워드가 입력되면, 입력된 패스워드와, 액세스가 요구된 유저의 유저 데이터의 일부로서 주소록 데이터에 보존된 패스워드를 대조한다. 일치하면, 인증은 성공이며, 일치하지 않으면 실패이다. 스텝S802에서는, 인증이 성공했는지 실패했는지를 판정한다. 성공이면, 해당 유저와 관련된 보낼곳 데이터를 주소록 데이터로 판독해서 표시한다(스텝S803). 한편, 인증에 실패한 경우에는, 에러 표시를 하고 처리를 종료한다(스텝S804).

<74> 스텝S803에서 표시된 보낼곳 데이터로부터, 전자메일 주소 혹은 팩시밀리 번호 등이 선택되어서, 선택된 송신처에 붙여서 전자메일이나 팩시밀 리가 송신된다. 또는, 선택된 보낼곳 데이터의 편집 처리 등이 행해진다.

<75> 이상과 같이 하여, 유저마다 관리된 주소록 데이터를 다른 장치에 대하여 배신할 수 있다. 그리고, 배신시에, 배신처에서 유저마다의 관리가 행해지지 않는 보낼곳 데이터, 즉 액세스의 제한이 없어지는 보낼곳 데이터에 대해서는, 그 조작을 요구한 조작자에 대하여 인증을 행하고, 일정한 권한이 있는 조작자에게 대해서만 배신을 허용한다. 주소록 데이터의 관리를 배신원에 있어서 엄격하게 행할 수 있다.

<76> <변형>

<77> 보낼곳 데이터는, 보낼곳의 명칭과 팩시밀리 번호 및 전자메일 주소를 대응시킨 데이터이며, 주소록 데이터는, 보낼곳 데이터와 명칭에 의해 검색 가능한 구성한 데이터베이스이다. 따라서, 보낼곳 데이터는 개인을 특정할 수 있는 개인정보이며, 컴퓨터에 의해 검색 가능한 형식으로 데이터베이스에 등록된 개인 데이터이다. 본 발명은, 보낼곳 데이터에 한정하지 않고, 일정한 권한을 갖는 사람에 대하여 액세스가 허용되어 있는 개인 데이터 일반에 대해서 적용할 수 있다. 예를 들면, 퍼스널 컴퓨터 등에 인스톨된 전자메일 프로그램에 의해 관리되는 주소록에 관해서도 완전히 마찬가지로 적용할 수 있다. 또한, 우편물의 보낼곳 인쇄 프로그램에 의해 관리되는 주소록이나, 명함관리 프로그램에 의해 관리되는 정보도 개인정보를 포함한다. 또한, 본 발명은, 이것들 데이터에 적용할 수 있다.

<78> 또한, 개인정보에 추가하여, 본 실시예는 소정의 액세스 권한을 갖는 유저에 대해서만 액세스가 허용된 문서 데이터 등에 적용될 수 있다. 그 문서 데이터 전체 혹은 그 일부의 송신시에, 그 문서 데이터를 관리할 수

없는 장치에의 송신을 제한할 수 있다. 즉, 개인정보에 추가하여 제한 액세스 데이터 일반에 관해서도 본 발명을 적용할 수 있다. 이것은, 제 2 실시예에도 적용한다.

<79> 또한, 제 1 실시예에서는 주소록 데이터 전체의 배신에 관하여 설명했다. 본 발명은, 주소록 데이터의 일부, 예를 들면 선택된 유저 데이터와 관련된 보낼곳 데이터를 배신하는 경우에도 적용할 수 있다. 이 경우에는, 송신되는 데이터는 주소록 데이터 전체가 아니고, 선택된 데이터의 일부인 점에서 상기 제 1 실시예와 다르다. 그러나, 데이터의 구성과 처리 순서는, 본 제 1 실시예에서 설명한 바와 같다. 이때, 주소록 데이터의 일부의 배신은, 제 2 실시예에 관해서도 마찬가지로 적용할 수 있다.

<80> [제 2 실시예]

<81> 도 11은, 도 2의 복사 장치(102)로 관리되지 않고 있는 유저의 보낼곳 데이터를 배신할 때에, 복사 장치(102)의 주소록 데이터에, 해당 유저를 새롭게 등록하고, 그 유저에 관련지어서 보낼곳 데이터도 등록하기 위한 순서를 나타낸다. 또한, 도 6과 공통되는 스텝에 관해서는, 도 6과 동일한 부호를 나타내고, 이 스텝들의 설명은 생략한다.

<82> 스텝S602에 있어서 주목 배신처에 액세스 관리기능이 있다고 판정된 경우, 스텝S1101로 분기된다. 스텝S1101에서는, 주목 배신처의 장치는, 배신원 장치에 보존된 주소록 데이터에 포함되는 전체 보낼곳 데이터를 유저별로 관리하고 있는지 판정한다. 판정 내용은 도 6과 마찬가지이다. 그러나, 도 11에 있어서는, 스텝S1101에서 NO라고 판정된 경우에는 스텝S1102로 분기한다는 점에서 스텝S608과는 다르다. 스텝S1102에서는, 주목 배신처의 장치에 보존된 주소록 데이터에, 새롭게 유저 데이터를 추가하는지, 조작자에게 확인을 재촉한다. 이를 위해, 확인 메시지와, 사용자 데이터를 추가할 것인가 아닌가를 선택하기 위한 버튼을 조작부(204)에 표시한다. 이 예를 도 10에 나타낸다. "예" 버튼(1001)이 눌려서 추가가 선택되면, 스텝S1102로부터 스텝S1103으로 분기한다. 그리고, 주목 배신처에 새로운 유저 데이터를 추가한다(스텝S1103). 유저 데이터의 추가는, 배신원 장치로부터, 배신하는 주소록 데이터에 포함되는 유저 데이터를 읽고, 그것을 송신처 장치에 송신하여 행해진다. 유저 데이터를 수신한 배신처 장치는, 수신한 유저 데이터에 포함되고, 게다가 배신처 장치의 주소록 데이터에 포함되어 있지 않은 유저 데이터를, 주소록 데이터에 추가한다. 그 때 추가된 유저 데이터에 관련되는 보낼곳 데이터는, 스텝S605에서 등록되므로, 스텝S1103에서는 보낼곳 데이터는 존재하지 않는다. 스텝S1102에서 유저 데이터의 추가가 선택되지 않았던 경우, 스텝S603으로 분기한다. 스텝S603, 스텝S604, 스텝S605, 스텝S606-1, 스텝S606-2, 스텝S607은, 제1 실시예와 같다.

<83> 이때, 유저 데이터의 추가를 유저 어카운트의 추가라고도 부른다. 도 10에서는 유저 어카운트로서 표시되어 있다.

<84> 또한, 도 11의 예에서는, 유저 데이터의 추가와 관련된 보낼곳 데이터의 추가를 별도의 페이즈에서 행하고 있다. 그러나, 유저 데이터의 추가와, 관련된 보낼곳 데이터의 추가를 단일 페이즈에서 행할 수도 있다. 그 경우, 스텝S1103에서는, 배신원 장치가 갖는 주소록 데이터 전체를 배신처에 송신한다. 그리고, 주소록 데이터를 수신한 장치는, 수신한 주소록 데이터에 포함되는 유저 데이터를 모두 등록하고, 관련된 보낼곳 데이터도 이어서 등록한다. 등록되는 유저 데이터에는, 액세스 제한을 위해 액세스용 패스워드가 포함되어 있는 것이 바람직하다. 이것은, 액세스용 패스워드가 등록되지 않으면, 액세스가 제한되어 있지 않은 경우이기 때문이다. 기존의 유저 데이터는, 추가할 필요가 없다. 이 경우, 보낼곳 데이터를 별도로 송신할 필요가 없기 때문에, 송신 후에는 스텝S607로 분기하게 된다.

<85> 이상과 같이 하여, 배신처의 장치가 보존하는 주소록 데이터에 등록되어 있지 않은 유저 데이터에 관해서는, 주소록 데이터를 배신할 때에 등록할 수 있다. 액세스 관리기능을 갖는 복사 장치로부터, 액세스 관리기능을 갖는 복사 장치에의 주소록 데이터를 배신하는 경우, 액세스가 제한된 보낼곳 데이터 전체를, 액세스 제한을 첨부한 채 배신처 장치에 송신할 수 있다.

<86> 또한, 제1 및 제2 실시예에서는, 주소록 데이터의 송신시에는, 데이터를 암호화하는 것이 바람직하다. 특히, 제2 실시예에서는, 유저 데이터의 등록을 위한 패스워드도 송신하고, 암호화는 필수이다.

<87> 또한, 상기 실시예에서는, 배신처 정보는 관리자가 손수 입력하는 것으로 설명했다. 한편, 소정 형식으로 각 복사 장치에 배신처 정보가 보유되어 있는 경우, 예를 들면, 동일 기종의 복사 장치가 접속된 시스템이면, 배신원의 복사 장치가 배신처의 각 복사 장치로 보존되어 있는 배신처 정보를 폴링한다. 이에 따라, 배신처 정보를 송신원 장치에 수집할 수 있다.

<88> <기타 실시예>

<89> 주목하는 것은, 본 발명이, 단일 소자 또는 복수의 소자로 이루어진 시스템을 구비한 장치에 적용될 수 있다는 것이다.

<90> 또한, 본 발명은, 상술한 실시예의 각 기능을 실현하는 소프트웨어 프로그램을, 시스템 혹은 장치에 대하여 직접 또는 간접적으로 공급하고, 그 시스템 또는 장치의 컴퓨터가 상기 공급된 프로그램 코드를 판독해서, 실행하는 것에 의해서 구현될 수 있다. 이 경우에, 상기 시스템 또는 장치가 그 프로그램의 기능을 가지고 있으면, 실행 모드는 프로그램에 의존할 필요가 없다.

<91> 따라서, 본 발명의 기능을 컴퓨터로 실현하기 때문에, 상기 컴퓨터에 인스톨되는 프로그램 코드 자체도 본 발명을 실현하는 것이다. 즉, 본 발명의 청구항은, 본 발명의 기능을 실현하기 위한 컴퓨터 프로그램도 포함한다.

<92> 이 경우에, 상기 시스템 또는 장치가 프로그램의 기능을 가지고 있으면, 예를 들면, 오브젝트 코드, 인터프리터에 의해 실행되는 프로그램 또는 오페레이팅 시스템에 공급된 스크립트 데이터와 같은, 임의의 형태로 프로그램을 실행해도 된다.

<93> 프로그램을 공급하는데 사용될 수 있는 기록 매체로서는, 예를 들면, 플로피 디스크, 하드디스크, 광디스크, 광자기디스크, CD-ROM, CD-R, CD-RW, 자기테이프, 비휘발성 메모리 카드, ROM 및 DVD(DVD-ROM, DVD-R)가 있다.

<94> 또한, 프로그램을 공급하는 방법에 관해서는, 클라이언트 컴퓨터의 브라우저를 사용해서 인터넷의 웹사이트에 접속될 수 있고, 본 발명의 컴퓨터 프로그램, 혹은 압축되어 자동 인스톨 기능을 포함하는 프로그램의 파일을 하드디스크 등의 기록 매체에 다운로드할 수 있다. 또한, 본 발명의 프로그램은, 그 프로그램을 구성하는 프로그램 코드를 복수의 파일로 분할하고, 각각의 파일을 다른 웹사이트로부터 다운로드하여서 공급될 수 있다. 즉, 본 발명의 기능을 컴퓨터로 실현하기 위한 프로그램 파일을 복수의 유저에 대하여 다운로드시키는 WWW(World Wide Web) 서버도, 본 발명의 청구항에 의해 포함된다.

<95> 또한, 본 발명의 프로그램을 암호화해서 CD-ROM등의 기억매체에 격납해서 유저에게 배포하고, 소정 조건을 만족시키는 유저에게, 인터넷을 거쳐서 웹사이트로부터 암호화를 푸는 열쇠정보를 다운로드시켜, 그 열쇠정보로 암호화된 프로그램을 복호해서 실행하여, 프로그램을 사용자 컴퓨터에 인스톨하여도 된다.

<96> 또한, 컴퓨터가, 판독한 프로그램을 실행함으로써, 전술한 실시예의 기능이 실현되는 경우에다가, 또한, 컴퓨터 상에서 가동하고 있는 오페레이팅 시스템 등은, 실제의 처리의 전부 또는 일부를 행해도 되어, 전술한 실시예의 기능이 그 처리에 의해 실현될 수 있다.

<97> 아울러, 기록 매체로부터 판독된 프로그램이, 컴퓨터에 삽입된 기능 확장 보드나 컴퓨터에 접속된 기능 확장 유닛에 구비되는 메모리에 기록되어도 된 후, 그 기능 확장 보드나 기능 확장 유닛에 구비되는 CPU등이 실제의 처리의 일부 또는 전부를 행하여, 전술한 실시예의 기능이 상기 처리에 의해 실현될 수 있다.

<98> 본 발명을 예시적 실시예를 참조하여 설명하였지만, 본 발명은 상기 개시된 예시적 실시예에 한정되지 않는다는 것을 알 수 있다. 이하의 청구범위는, 이러한 모든 변형 및 동등한 구성 및 기능을 포함하도록 아주 넓게 해석되어야 한다.

발명의 효과

<99> 이상과 같은 본 발명은, 배신되는 데이터에의 액세스의 제한을 유지할 수 있다. 구체적으로는, 본 발명은, 액세스 관리기능을 갖는 장치에 대하여 제한 액세스 데이터를 배신하는 경우에는, 배신처 장치에 대하여 이용자의 액세스권을 새롭게 등록함으로써 제한 액세스 데이터의 시큐리티를 유지하고, 무권한의 이용자에 의한 액세스를 방지할 수 있다.

도면의 간단한 설명

<1> 도 1은 본 발명의 실시예에 따른 정보배신 시스템의 구성을 나타내는 도면,

<2> 도 2는 본 발명에 따른 복사 장치의 블록도,

<3> 도 3은 본 발명의 정보배신 시스템에서의 복사 장치(101)의 주소록 관리 화면을 도시한 도면,

<4> 도 4는 본 발명의 정보배신 시스템에서의 복사 장치(102)의 주소록 관리 화면을 도시한 도면,

<5> 도 5는 본 발명의 정보배신 시스템에서의 복사 장치(103)의 주소록 화면을 도시한 도면,

<6> 도 6은 본 발명의 제1실시예에서의 배신원 복사 장치에 의한 배신처리의 흐름도,

<7> 도 7a는 본 발명의 제1실시예에서의 배신처 복사 장치에 의한 수신 처리의 흐름도,

<8> 도 7b는 본 발명의 제1실시예에서의 배신처 복사 장치에 의한 수신 처리의 흐름도,

<9> 도 8은 본 발명의 복사 장치에 있어서 주소록 데이터에 액세스하는 처리의 흐름도,

<10> 도 9a는 주소록 데이터 및 배신처 정보의 일례를 도시한 테이블,

<11> 도 9b는 주소록 데이터 및 배신처 정보의 다른 예를 도시한 테이블,

<12> 도 9c는 주소록 데이터 및 배신처 정보의 또 다른 예를 도시한 테이블,

<13> 도 9d는 주소록 데이터 및 배신처 정보의 또 다른 예를 도시한 테이블,

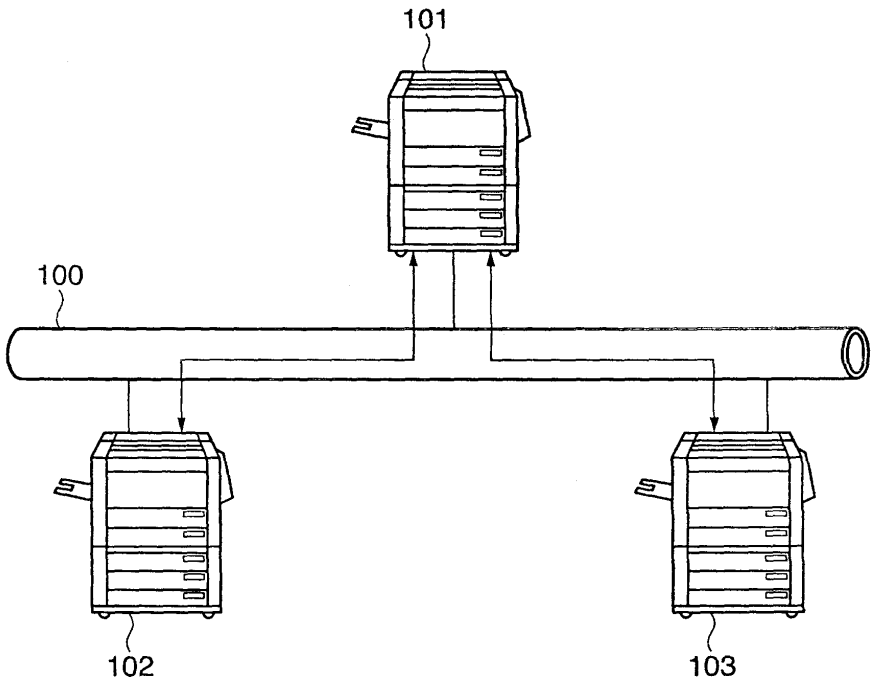
<14> 도 10은 본 발명의 제2실시예에서의 배신원 복사 장치에 표시되는 확인 화면의 일례를 도시한 도면,

<15> 도 11은 본 발명의 제2실시예에서의 배신원 복사 장치에 의한 배신처리의 흐름도,

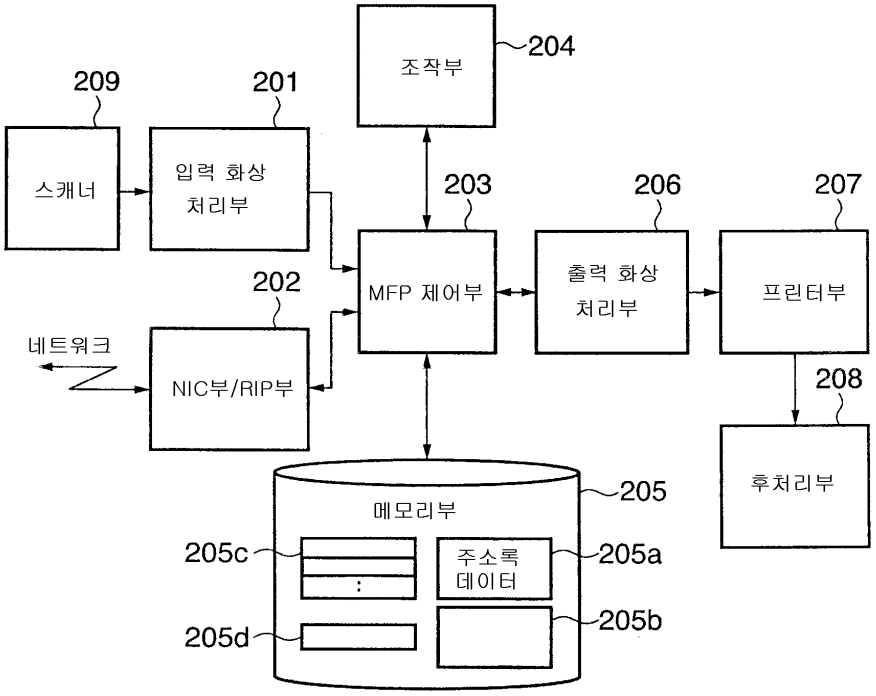
<16> 도 12는 본 발명의 개략을 설명하기 위한 도면이다.

도면

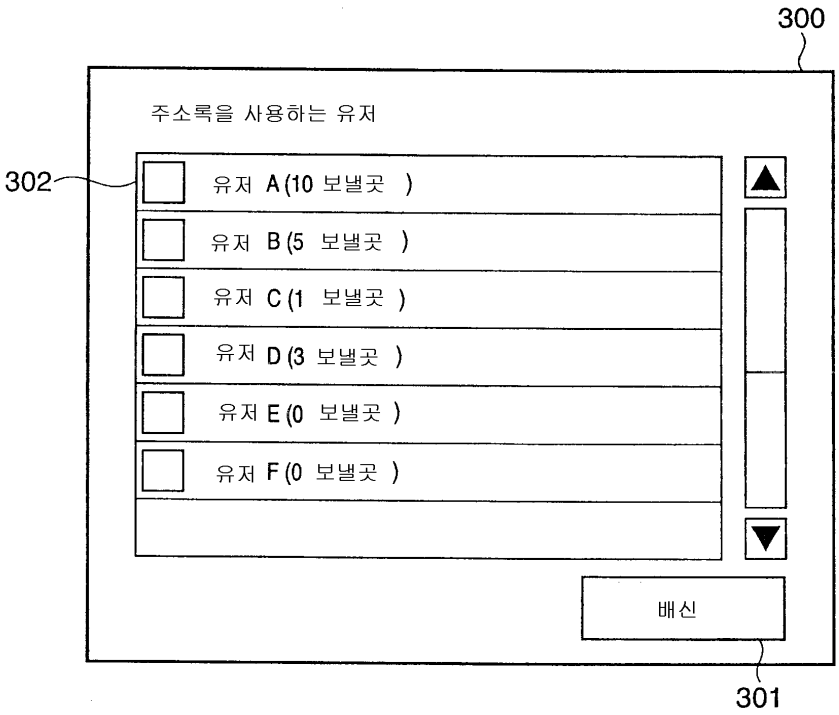
도면1



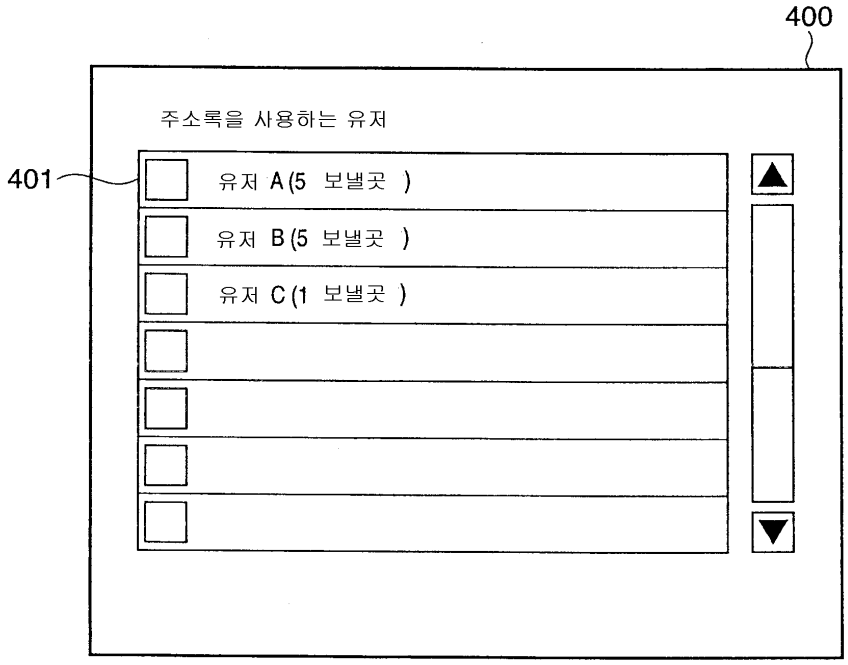
도면2


조작부
204
209
201
스캐너
입력 화상 처리부
203
206
207
MFP 제어부
출력 화상 처리부
프린터부
202
네트워크
NIC부/RIP부
208
후처리부
205
메모리부
205c
주소록 데이터
205a
205d
205b

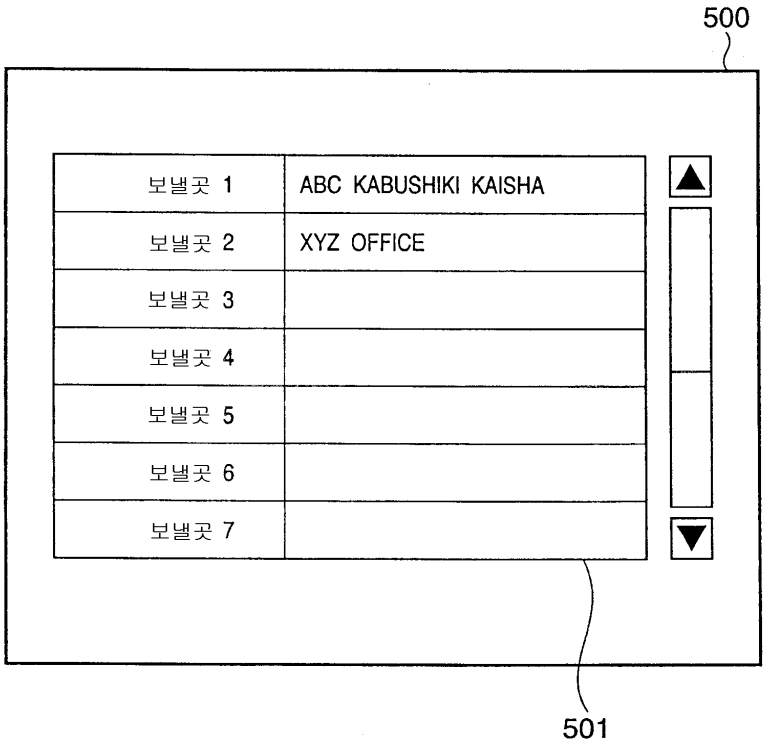
도면3


300
주소록을 사용하는 유저
302
유저 A(10 보낼곳)
유저 B(5 보낼곳)
유저 C(1 보낼곳)
유저 D(3 보낼곳)
유저 E(0 보낼곳)
유저 F(0 보낼곳)
배신
301

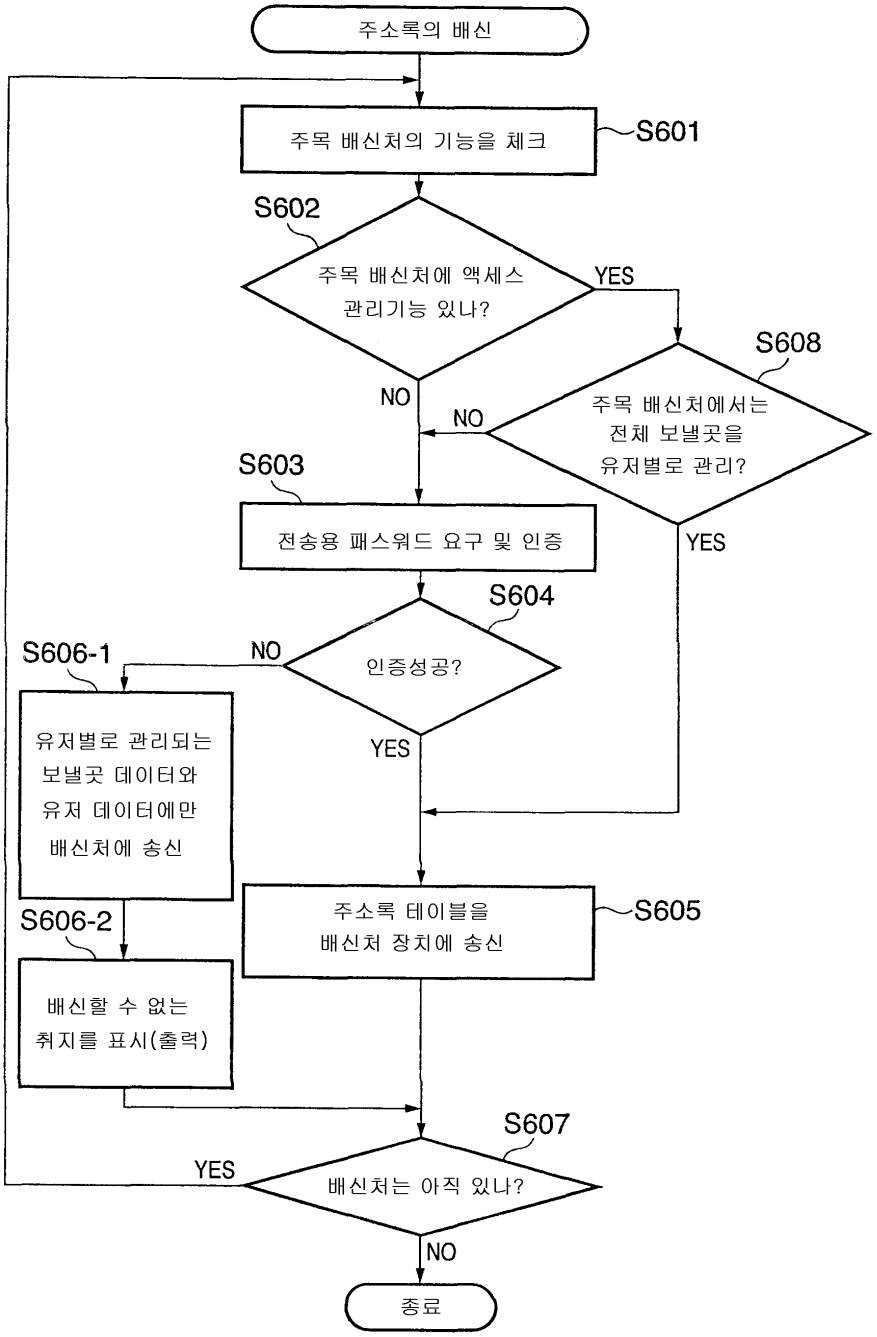
도면4


400
주소록을 사용하는 유저
401
유저 A(5 보낼곳)
유저 B(5 보낼곳)
유저 C(1 보낼곳)

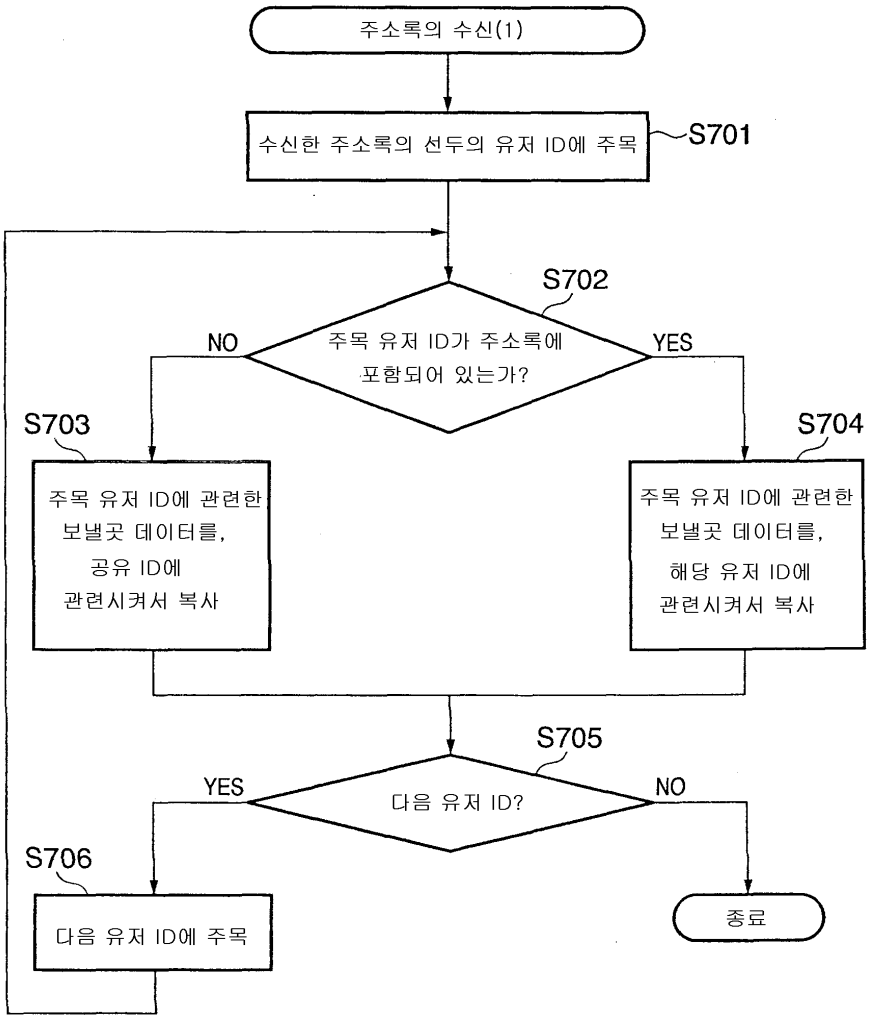
도면5


500
보낼곳 1
ABC KABUSHIKI KAISHA
보낼곳 2
XYZ OFFICE
보낼곳 3
보낼곳 4
보낼곳 5
보낼곳 6
보낼곳 7
501

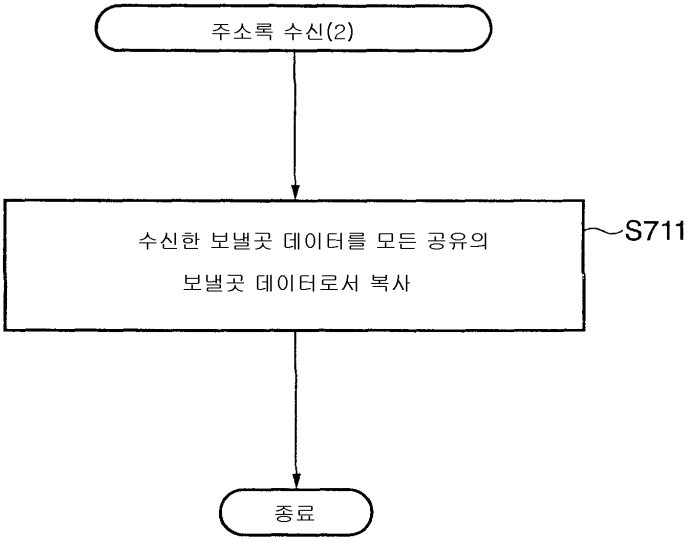
도면6


주소록의 배신
주목 배신처의 기능을 체크
S601
S602
주목 배신처에 액세스 관리기능 있나?
YES
NO
S608
주목 배신처에서는 전체 보낼곳을 유저별로 관리?
NO
YES
S603
전송용 패스워드 요구 및 인증
S604
인증성공?
NO
YES
S606-1
유저별로 관리되는 보낼곳 데이터와 유저 데이터에만 배신처에 송신
S606-2
배신할 수 없는 취지를 표시(출력)
주소록 테이블을 배신처 장치에 송신
S605
S607
배신처는 아직 있나?
YES
NO
종료

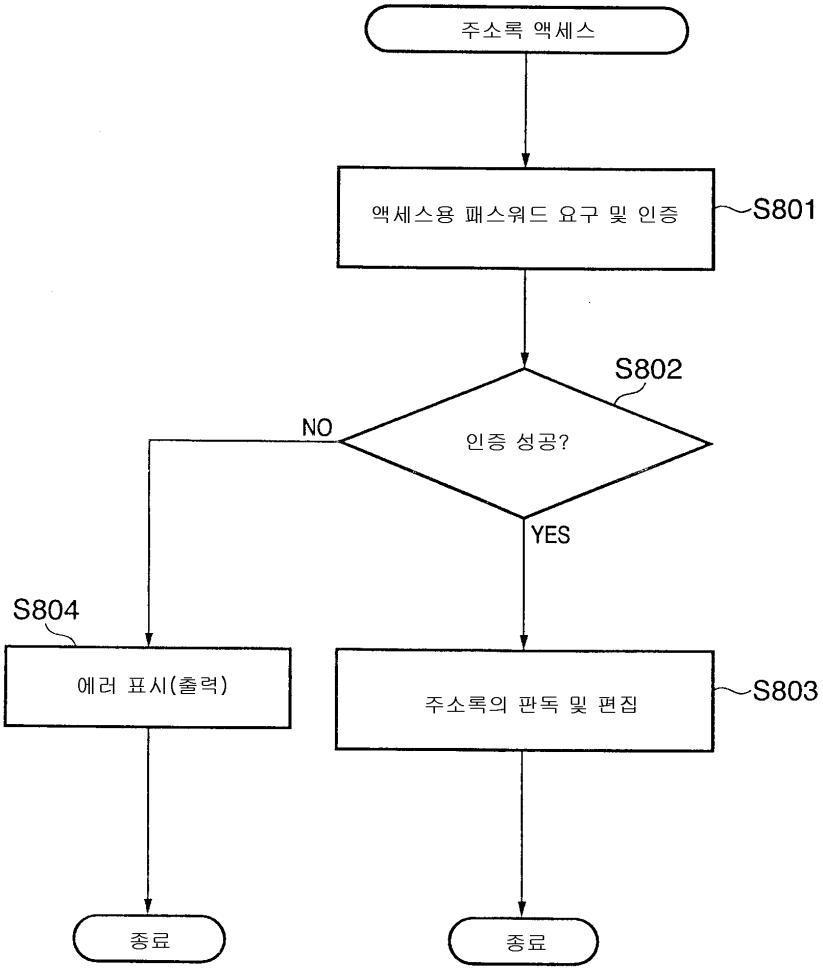
도면7a


주소록의 수신(1)
수신한 주소록의 선두의 유저 ID에 주목
S701
S702
주목 유저 ID가 주소록에 포함되어 있는가?
NO
YES
S703
주목 유저 ID에 관련한 보낼곳 데이터를, 공유 ID에 관련시켜서 복사
S704
주목 유저 ID에 관련한 보낼곳 데이터를, 해당 유저 ID에 관련시켜서 복사
S705
다음 유저 ID?
YES
NO
S706
다음 유저 ID에 주목
종료

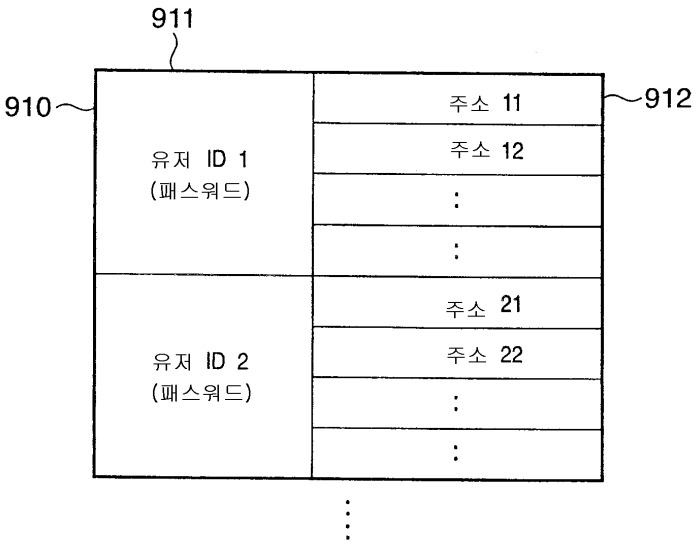
도면7b


주소록 수신(2)
수신한 보낼곳 데이터를 모든 공유의 보낼곳 데이터로서 복사
S711
종료

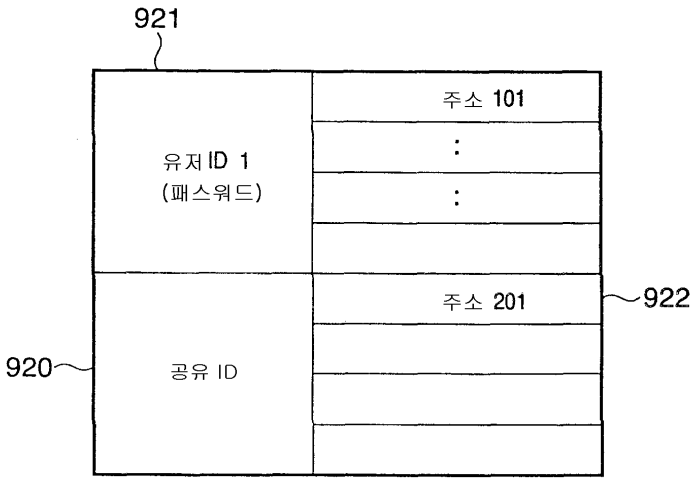
도면8


주소록 액세스
액세스용 패스워드 요구 및 인증
S801
S802
인증 성공?
NO
YES
S804
에러 표시(출력)
주소록의 판독 및 편집
S803
종료
종료

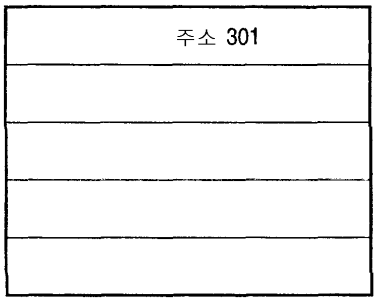
도면9a


911
910
912
유저 ID 1
(패스워드)
주소 11
주소 12
:
:
유저 ID 2
(패스워드)
주소 21
주소 22
:
:

도면9b



도면9c

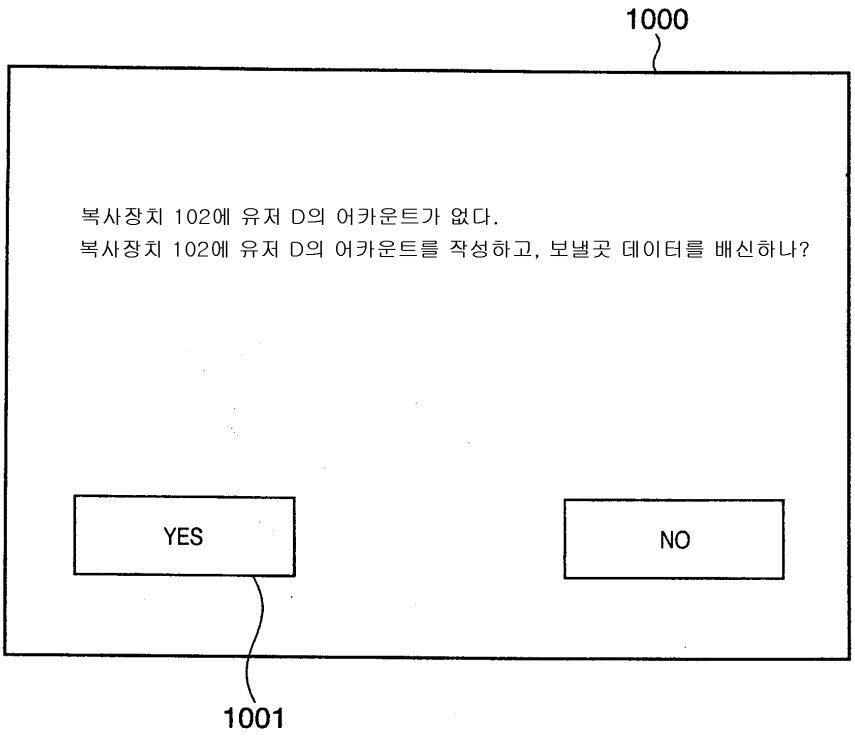


도면9d

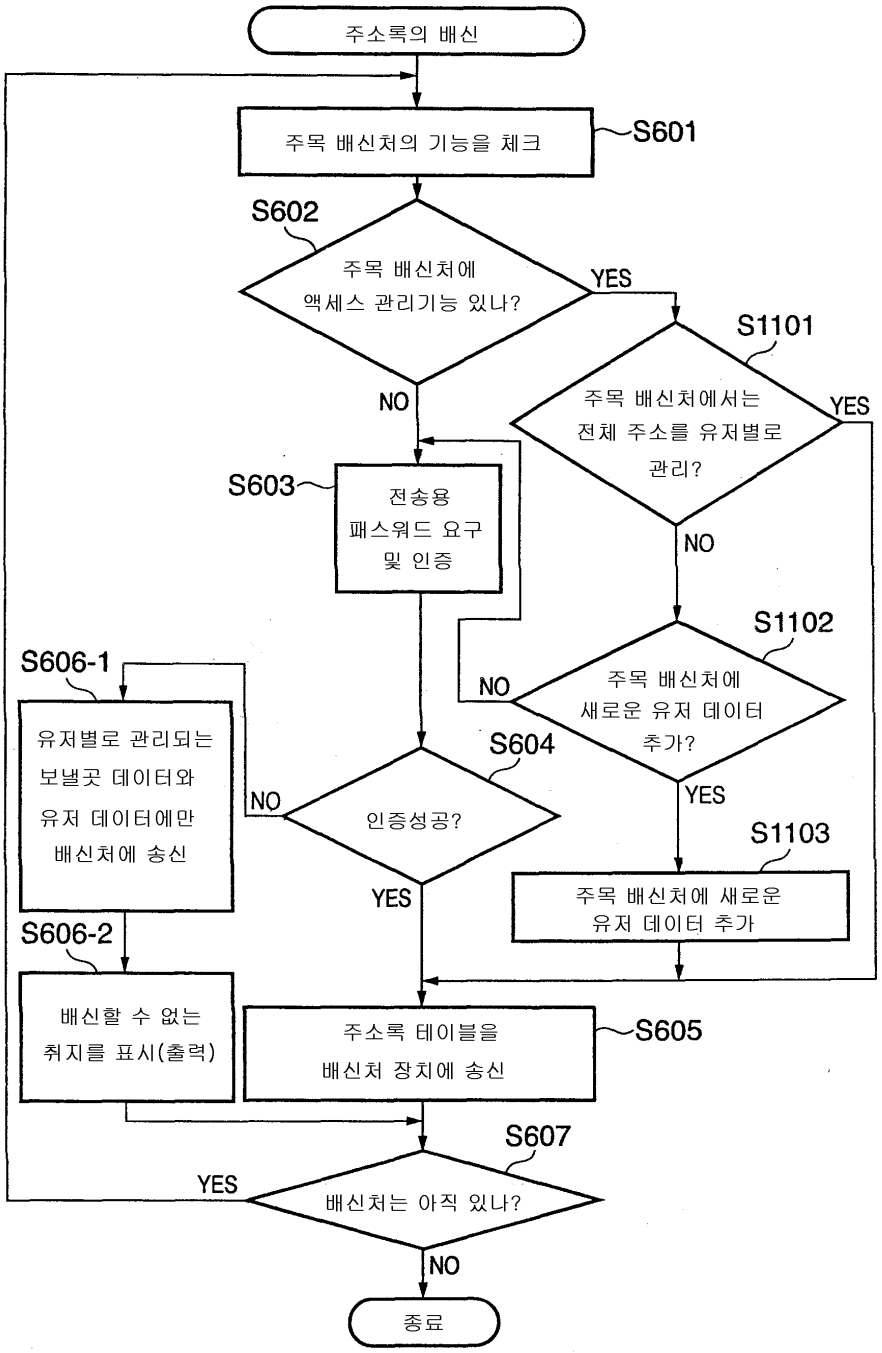
941
942

디바이스 식별정보	기능정보
복사 장치 102의 주소	액세스 관리기능 있음
복사 장치 103의 주소	엑세스 관리기능 없음

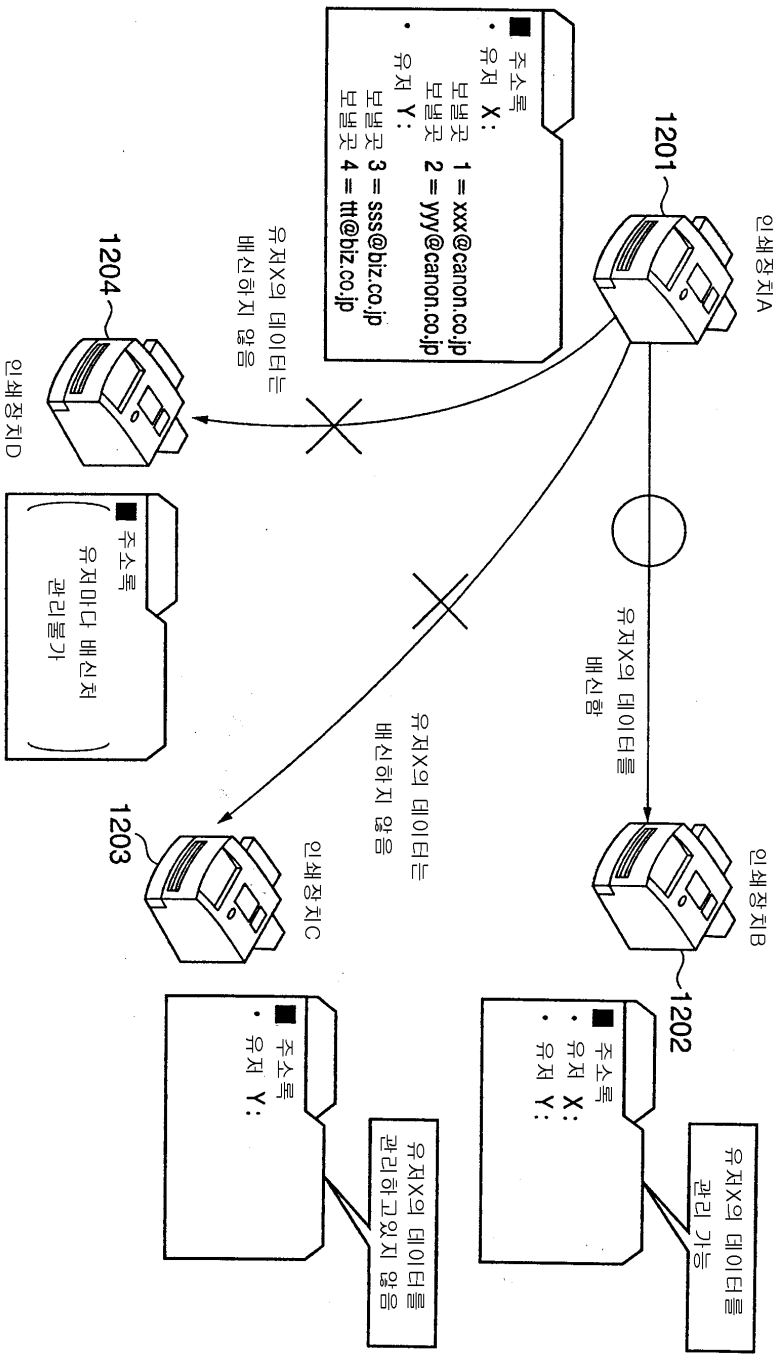
도면10


1000
복사장치 102에 유저 D의 어카운트가 없다.
복사장치 102에 유저 D의 어카운트를 작성하고, 보낼곳 데이터를 배신하나?
YES
NO
1001

도면11


주소록의 배신
주목 배신처의 기능을 체크
S601
S602
주목 배신처에
액세스 관리기능 있나?
YES
NO
S1101
주목 배신처에서는
전체 주소를 유저별로
관리?
YES
NO
S603
전송용
패스워드 요구
및 인증
S1102
주목 배신처에
새로운 유저 데이터
추가?
NO
YES
S606-1
유저별로 관리되는
보낼곳 데이터와
유저 데이터에만
배신처에 송신
S604
인증성공?
NO
YES
S1103
주목 배신처에 새로운
유저 데이터 추가
S606-2
배신할 수 없는
취지를 표시(출력)
주소록 테이블을
배신처 장치에 송신
S605
S607
YES
배신처는 아직 있나?
NO
종료

도면12


인쇄장치A
1201
주소록
• 유저 X:
보낼곳 1 = xxx@canon.co.jp
보낼곳 2 = yyy@canon.co.jp
• 유저 Y:
보낼곳 3 = sss@biz.co.jp
보낼곳 4 = ttt@biz.co.jp
유저X의 데이터를
배신함
인쇄장치B
1202
주소록
• 유저 X:
• 유저 Y:
유저X의 데이터를
관리 가능
유저X의 데이터는
배신하지 않음
인쇄장치C
1203
주소록
• 유저 Y:
유저X의 데이터를
관리하고있지 않음
유저X의 데이터는
배신하지 않음
인쇄장치D
1204
주소록
유저마다 배신처
관리불가