(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년07월13일
(11) 등록번호 10-2420497
(24) 등록일자 2022년07월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 21/60* (2013.01)
G06F 21/62 (2013.01)
(52) CPC특허분류
H04L 9/0877 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2017-0088830
(22) 출원일자 2017년07월13일
심사청구일자 2019년01월14일
(65) 공개번호 10-2018-0015076
(43) 공개일자 2018년02월12일
(30) 우선권주장
JP-P-2016-152288 2016년08월02일 일본(JP)
(56) 선행기술조사문헌
KR1020150057980 A*
KR1020140104370 A*
JP2001312486 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
캐논 가부시끼가이샤
일본 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고
(72) 발명자
카쿠타니 나오야
일본국 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고 캐논 가부시끼가이샤 나이
(74) 대리인
권태복

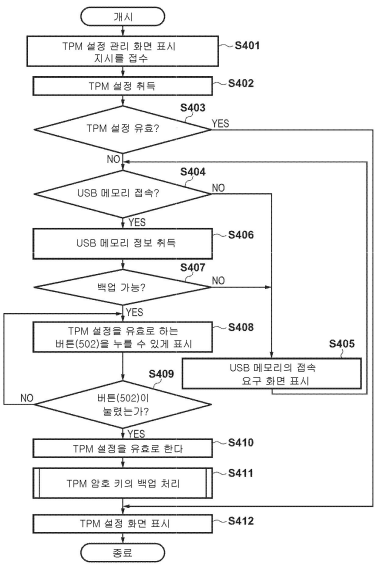
전체 청구항 수 : 총 8 항 심사관 : 강민성

(54) 발명의 명칭 **정보 처리장치와 그 제어방법, 및 기억매체**

(57) 요 약

하드웨어 시큐리티 모듈(HSM)을 갖는 정보 처리장치에 있어서, HSM의 암호 키의 백업이 가능한 것을 조건으로, HSM의 암호 키를 이용해서 데이터의 암호화 및 복호화를 가능하게 하는 HSM 기능을 유효하게 설정할 수 있다.

대 표 도 - 도4



(52) CPC특허분류
G06F 21/62 (2013.01)

명 세 서

청구범위

청구항 1

하드웨어 시큐리티 모듈(HSM)을 갖는 정보 처리장치로서,

상기 HSM의 암호 키를 보존하는 외부 메모리가 접속되어 있는지 아닌지, 또는 상기 외부 메모리가 상기 HSM의 상기 암호 키를 보존할 수 있는 비어 있는 기억 영역을 가지고 있는지 아닌지에 근거하여, 상기 HSM의 상기 암호 키의 백업이 가능한지 아닌지를 판정하도록 구성된 판정부와,

상기 HSM의 상기 암호 키의 백업이 가능하다고 판정되는 조건에서, 상기 암호 키를 이용해서 데이터의 암호화 및 복호화를 행하는 HSM 기능을 유효로 하는 지시를 접수 가능하도록 제어를 행하도록 구성된 제어부와,

상기 HSM 기능을 유효로 하는 지시가 접수되는 것에 따라 상기 HSM 기능을 유효로 설정하도록 구성된 설정부와,

상기 설정부에 의해 상기 HSM 기능이 유효로 설정되는 것에 따라 상기 암호 키를 백업하도록 구성된 백업부를 구비하고,

상기 제어부는, 상기 판정부에 의해 상기 HSM의 상기 암호 키의 백업이 가능하지 않은 것으로 판정되는 경우, 조작부를 통해서 상기 HSM 기능을 유효로 하는 지시를 접수하지 않도록 제어를 행하는 정보 처리장치.

청구항 2

삭제

청구항 3

삭제

청구항 4

제 1항에 있어서,

상기 HSM 기능을 유효로 하는 지시를 내리는 지시부를 표시하도록 구성된 표시부를 더 구비하고,

상기 표시부는, 상기 HSM 기능을 유효로 하는 지시가 접수 가능한 경우에는, 상기 지시부를 조작 가능하게 표시하고, 상기 HSM 기능을 유효로 하는 지시가 접수 가능하지 않은 경우에는, 상기 지시부를 조작할 수 없도록 표시하는 정보 처리장치.

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

하드웨어 시큐리티 모듈(HSM)을 갖는 정보 처리장치의 제어방법으로서,

상기 HSM의 암호 키를 보존하는 외부 메모리가 접속되어 있는지 아닌지, 또는 상기 외부 메모리가 상기 HSM의 상기 암호 키를 보존할 수 있는 비어 있는 기억 영역을 가지고 있는지 아닌지에 근거하여, 상기 HSM의 상기 암호 키의 백업이 가능한지 아닌지를 판정하는 단계와,

상기 HSM의 상기 암호 키의 백업이 가능하다고 판정되는 조건에서, 상기 암호 키를 이용해서 데이터의 암호화 및 복호화를 행하는 HSM 기능을 유효로 하는 지시를 접수 가능하도록 제어를 행하는 단계와,

상기 HSM 기능을 유효로 하는 지시가 접수되는 것에 따라 상기 HSM 기능을 유효로 설정하는 단계와,

상기 설정하는 단계에서 상기 HSM 기능이 유효로 설정되는 것에 따라 상기 암호 키를 백업하는 단계를 포함하고,

상기 제어를 행하는 단계에서는, 상기 판정하는 단계에서 상기 HSM의 상기 암호 키의 백업이 가능하지 않은 것으로 판정되는 경우, 조작부를 통해서 상기 HSM 기능을 유효로 하는 지시를 접수하지 않도록 제어를 행하는 정보 처리장치의 제어방법.

청구항 12

프로세서가, 하드웨어 시큐리티 모듈(HSM)을 갖는 정보 처리장치의 제어방법을 실행하게 하는 프로그램을 기억한 컴퓨터 판독가능한 기억매체로서,

상기 제어방법은,

상기 HSM의 암호 키를 보존하는 외부 메모리가 접속되어 있는지 아닌지, 또는 상기 외부 메모리가 상기 HSM의 상기 암호 키를 보존할 수 있는 비어 있는 기억 영역을 가지고 있는지 아닌지에 근거하여, 상기 HSM의 상기 암호 키의 백업이 가능한지 아닌지를 판정하는 단계와,

상기 HSM의 상기 암호 키의 백업이 가능하다고 판정되는 조건에서, 상기 암호 키를 이용해서 데이터의 암호화 및 복호화를 행하는 HSM 기능을 유효로 하는 지시를 접수 가능하도록 제어를 행하는 단계와,

상기 HSM 기능을 유효로 하는 지시가 접수되는 것에 따라 상기 HSM 기능을 유효로 설정하는 단계와,

상기 설정하는 단계에서 상기 HSM 기능이 유효로 설정되는 것에 따라 상기 암호 키를 백업하는 단계를 포함하고,

상기 제어를 행하는 단계에서는, 상기 판정하는 단계에서 상기 HSM의 상기 암호 키의 백업이 가능하지 않은 것으로 판정되는 경우, 조작부를 통해서 상기 HSM 기능을 유효로 하는 지시를 접수하지 않도록 제어를 행하는 컴퓨터 판독가능한 기억매체.

청구항 13

제 1항에 있어서,

상기 조작부를 더 구비하고,

상기 지시는 상기 조작부를 거쳐 접수되는, 정보 처리장치.

청구항 14

제 1항에 있어서,

상기 HSM 기능이 유효하다는 것을 나타내는 설정 정보를 메모리에 보존하도록 구성된 보존부를 더 구비하고,

상기 설정 정보가 상기 메모리에 보존되는 경우에, 상기 판정부는 상기 HSM의 상기 암호 키의 백업이 가능한지 아닌지를 판정하지 않는, 정보 처리장치.

청구항 15

삭제

청구항 16

제 11항에 있어서,

상기 지시는 상기 정보 처리장치의 상기 조작부를 거쳐 접수되는, 정보 처리장치의 제어방법.

청구항 17

제 11항에 있어서,

상기 HSM 기능이 유효하다는 것을 나타내는 설정 정보를 메모리에 보존하는 단계를 더 포함하고,

상기 설정 정보가 상기 메모리에 보존되는 경우에, 상기 HSM의 상기 암호 키의 백업이 가능한지 아닌지를 상기 판정하는 단계에서 판정하지 않는, 정보 처리장치의 제어방법.

청구항 18

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은, 정보 처리장치, 그 제어방법, 및 기억매체에 관한 것이다.

배 경 기 술

[0002] 일반적으로, PC(personal computer)와, 인쇄 기능을 갖는 MFP(multi-function peripheral/digital multi-function peripheral) 등의 정보 처리장치에서는, 기밀 데이터가 암호화되어 보존된다.

[0003] 최근, 이 정보 처리장치 내에 포함된 기밀 데이터를 암호화/복호화하는 경우, 정보 처리장치에 물리적으로 접속된 외부의 하드웨어 시큐리티 모듈(HSM)에 격납된 암호 키를 이용하는 정보 처리장치도 있다. 예를 들면, 이 HSM은, TCG(Trusted Computing Group)의 규격에 준거한 TPM(Trusted Platform Module)을 이용한다. TPM은, 암호화 키를 안전하게 관리하는 것이 가능한 내탬퍼성(tamper resistance)을 구비한 시큐리티 칩이다.

[0004] 일반적으로, TPM을 구비한 기기는, 기밀 데이터를 암호화하고, 그 암호화에 이용한 키를 TPM 내에서 관리함으로써, 안전한 기밀 데이터의 관리를 실현하고 있다. 이러한 정보 처리장치의 TPM을 이용한 암호화/복호화를 이하에서는 "TPM 기능"이라고 부른다. 이 TPM 기능을 채용한 경우, 예를 들면, TPM의 고장이나 분실 등이 발생하면, TPM의 교환이 행해지는 일이 있다.

[0005] 지금, 예를 들면, 고장에 의해 TPM을 새로운 TPM로 교환하는 경우, 새로운 TPM 칩 내의 TPM 암호 키는,

고장전의 오래된 TPM 내의 TPM 암호 키와는 다르다. 이 때문에, 오래된 TPM 내의 TPM 암호 키를 사용하여 암호화한 정보 처리장치 내의 기밀 데이터는, 그 새로운 TPM에 의해 복호화해서 이용할 수는 없다. 그 때문에, TPM에 의해 관리하는 암호화 키(이하, TPM 암호 키)의 백업이 필요하게 된다. TPM 암호 키의 백업은, 그 장치에 USB 등의 외부 스토리지를 접속하고, 그 접속한 외부 스토리지에 TPM 암호 키를 보존함으로써 행해지는 경우가 많다. 예를 들면, TPM이 고장난 경우, 그 장치의 TPM을 새로운 TPM으로 교환하고, 원래의 TPM 암호 키가 보존되어 있는 외부 스토리지를 그 장치에 접속하고, 이 외부 스토리지에 기억되어 있는 TPM 암호 키를 사용해서 새로운 TPM으로 TPM 암호 키를 리스토어한다.

[0006] 일본국 특개 2015-122720호 공보에는, TPM 기능을 이용하는 기기의 TPM 암호 키의 백업에 관한 기술이 기재되어 있다. 이 기술에 따르면, TPM 암호 키는 TPM 기능이 유효된 후에 생성되기 때문에, 기기를 사용하는 유저는 TPM 기능을 유효로 한 후에, USB 메모리 등의 외부 스토리지에 대하여 TPM 암호 키의 백업을 실행하고 있다.

[0007] 그렇지만, 유저가 기기에 대하여 TPM 기능을 유효로 한 후 TPM 암호 키의 백업을 잊어버리는 경우가 있다. 이것에는, 예를 들면, TPM 기능을 유효로 했을 때에, 백업을 위한 USB 메모리를 준비하지 않았거나, 또는 TPM 기능을 유효로 하는 유저와, TPM 암호 키를 백업해서 관리하는 유저가 다른 경우가 생각된다. 또한, 백업 기능의 존재를 몰랐던 유저가 TPM 기능을 유효로 한 경우도 생각된다. 이렇게 해서 TPM 암호 키가 백업되지 않은 채 TPM이 교환되어 버리면, 오래된 TPM의 TPM 암호 키를 사용하여 암호화한 기기 내부의 기밀 데이터를 복호화해서 이용할 수 없게 된다는 과제가 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명의 일면은 종래기술과 관련된 전술한 문제를 해소하는 것이다.

[0009] 본 발명의 특징은, 유저가 HSM 암호 키를 백업하는 잊어버리는 것을 방지하는 기술을 제공하는 것에 있다.

[0010]

과제의 해결 수단

[0011] 본 발명의 제1면에 따르면, 하드웨어 시큐리티 모듈(HSM)을 갖는 정보 처리장치로서, 상기 HSM의 암호 키를 보존하는 외부 메모리가 접속되어 있는지 아닌지, 또는 상기 외부 메모리가 상기 HSM의 상기 암호 키를 보존할 수 있는 비어 있는 기억 영역을 가지고 있는지 아닌지에 근거하여, 상기 HSM의 상기 암호 키의 백업이 가능한지 아닌지를 판정하도록 구성된 판정부와, 상기 HSM의 상기 암호 키의 백업이 가능하다고 판정되는 조건에서, 상기 암호 키를 이용해서 데이터의 암호화 및 복호화를 행하는 HSM 기능을 유효로 하는 지시를 접수 가능하도록 제어를 행하도록 구성된 제어부와, 상기 HSM 기능을 유효로 하는 지시가 접수되는 것에 따라 상기 HSM 기능을 유효로 설정하도록 구성된 설정부와, 상기 설정부에 의해 상기 HSM 기능이 유효로 설정되는 것에 따라 상기 암호 키를 백업하도록 구성된 백업부를 구비하고, 상기 제어부는, 상기 판정부에 의해 상기 HSM의 상기 암호 키의 백업이 가능하지 않은 것으로 판정되는 경우, 조작부를 통해서 상기 HSM 기능을 유효로 하는 지시를 접수하지 않도록 제어를 행하는 정보 처리장치가 제공된다.

[0012] 본 발명의 제2면에 따르면, 하드웨어 시큐리티 모듈(HSM)을 갖는 정보 처리장치로서, HSM의 암호 키의 백업이 가능한지 아닌지를 판정하도록 구성된 제1 판정부와, 상기 HSM의 상기 암호 키의 백업이 가능하다고 상기 제1 판정부에 의해 판정되는 조건에서, 상기 암호 키를 이용해서 데이터의 암호화 및 복호화를 행하는 HSM 기능을 유효로 하는 지시를 접수 가능하도록 제어를 행하도록 구성된 접수부와, 상기 HSM 기능이 유효인지 아닌지를 판정하도록 구성된 제2 판정부와, 상기 HSM의 상기 암호 키가 백업되었는지 아닌지를 판정하도록 구성된 제3 판정부와, 상기 HSM 기능이 유효하다고 상기 제2 판정부에 의해 판정되고, 상기 HSM의 상기 암호 키가 백업되지 않았다고 상기 제3 판정부에 의해 판정되는 경우, 상기 HSM의 상기 암호 키를 백업하도록 제어를 행하도록 구성된 제어부를 구비하고, 상기 제어부는, 상기 제 1 판정부에 의해 상기 HSM의 상기 암호 키의 백업이 가능하지 않은 것으로 판정되는 경우, 조작부를 통해서 상기 HSM 기능을 유효로 하는 지시를 접수하지 않도록 제어를 행하는 정보 처리장치가 제공된다.

[0013] 본 발명의 제3면에 따르면, 하드웨어 시큐리티 모듈(HSM)을 갖는 정보 처리장치의 제어방법으로서, 상

기 HSM의 암호 키를 보존하는 외부 메모리가 접속되어 있는지 아닌지, 또는 상기 외부 메모리가 상기 HSM의 상기 암호 키를 보존할 수 있는 비어 있는 기억 영역을 가지고 있는지 아닌지에 근거하여, 상기 HSM의 상기 암호 키의 백업이 가능한지 아닌지를 판정하는 단계와, 상기 HSM의 상기 암호 키의 백업이 가능하다고 판정되는 조건에서, 상기 암호 키를 이용해서 데이터의 암호화 및 복호화를 행하는 HSM 기능을 유효로 하는 지시를 접수 가능하도록 제어를 행하는 단계와, 상기 HSM 기능을 유효로 하는 지시가 접수되는 것에 따라 상기 HSM 기능을 유효로 설정하는 단계와, 상기 설정하는 단계에서 상기 HSM 기능이 유효로 설정되는 것에 따라 상기 암호 키를 백업하는 단계를 포함하고, 상기 제어를 행하는 단계에서는, 상기 판정하는 단계에서 상기 HSM의 상기 암호 키의 백업이 가능하지 않은 것으로 판정되는 경우, 조작부를 통해서 상기 HSM 기능을 유효로 하는 지시를 접수하지 않도록 제어를 행하는 정보 처리장치의 제어방법이 제공된다.

[0014] 본 발명의 제4면에 따르면, 프로세서가, 하드웨어 시큐리티 모듈(HSM)을 갖는 정보 처리장치의 제어방법을 실행하게 하는 프로그램을 기억한 컴퓨터 판독가능한 기억매체로서, 상기 제어방법은, 상기 HSM의 암호 키를 보존하는 외부 메모리가 접속되어 있는지 아닌지, 또는 상기 외부 메모리가 상기 HSM의 상기 암호 키를 보존할 수 있는 비어 있는 기억 영역을 가지고 있는지 아닌지에 근거하여, 상기 HSM의 상기 암호 키의 백업이 가능한지 아닌지를 판정하는 단계와, 상기 HSM의 상기 암호 키의 백업이 가능하다고 판정되는 조건에서, 상기 암호 키를 이용해서 데이터의 암호화 및 복호화를 행하는 HSM 기능을 유효로 하는 지시를 접수 가능하도록 제어를 행하는 단계와, 상기 HSM 기능을 유효로 하는 지시가 접수되는 것에 따라 상기 HSM 기능을 유효로 설정하는 단계와, 상기 설정하는 단계에서 상기 HSM 기능이 유효로 설정되는 것에 따라 상기 암호 키를 백업하는 단계를 포함하고, 상기 제어를 행하는 단계에서는, 상기 판정하는 단계에서 상기 HSM의 상기 암호 키의 백업이 가능하지 않은 것으로 판정되는 경우, 조작부를 통해서 상기 HSM 기능을 유효로 하는 지시를 접수하지 않도록 제어를 행하는 컴퓨터 판독가능한 기억매체가 제공된다.

[0015] 본 발명의 또 다른 특징은 첨부도면을 참조하여 주어지는 이하의 실시형태의 상세한 설명으로부터 명백해질 것이다.

도면의 간단한 설명

[0016] 명세서에 포함되고 명세서의 일부를 구성하는 다음의 첨부도면은, 본 발명의 예시적인 실시형태, 특징 및 국면을 예시하며, 상세한 설명과 함께, 본 발명의 원리를 설명하는 역할을 한다.

도 1은, 본 발명의 제1 실시예에 따른 복합기의 하드웨어 구성의 개략을 설명하는 블록도이다.

도 2는, 제1실시예에 따른 TPM과 HDD가 취급하는 암호 키와 기밀 데이터의 개략 구성을 설명하는 블록도이다.

도 3은, 제1실시예에 따른 복합기의 기동 처리를 설명하는 흐름도이다.

도 4는, 제1실시예에 따른 복합기에 있어서의 TPM 기능을 유효로 하는 처리를 설명하는 흐름도이다.

도 5a 내지 도 5c는, 제1실시예에 따른 복합기의 조작부에 표시되는 TPM 설정 관리 화면의 일례를 도시한 도면이다.

도 6은, 제1실시예에 따른 복합기에 의해 행해지는 도 4의 스텝 S411에서의 TPM 암호 키의 백업 처리를 설명하는 흐름도이다.

도 7은, 제1실시예에 따른 복합기의 조작부에 표시되는 TPM 암호 키의 백업용의 패스워드를 입력하는 화면의 일례를 도시한 도면이다.

도 8은, 제2실시예에 따른 복합기의 기동 처리를 설명하는 흐름도이다.

도 9는, 제2실시예에 따른 복합기가 제공하는 기능의 메인메뉴 화면의 일례를 도시한 도면이다.

도 10은, 제2실시예에 따른 복합기에 의해 행해지는 유저 인증 처리를 설명하는 흐름도이다.

도 11은, 본 발명의 제3실시예에 따른 복합기에 의해 행해지는 HSM 기능을 유효로 하는 처리와 백업 처리를 설명하는 흐름도이다.

도 12a 내지 도 12c는, 제3실시예에 따른 복합기의 조작부에 표시되는 HSM 설정 관리 화면의 일례를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하, 첨부도면을 참조하여 본 발명의 실시예를 상세히 설명한다. 이하의 실시예는 본 발명의 청구범위를 제한하도록 의도된 것이 아니며, 이하의 실시예에 따라 서술되는 국면의 모든 조합이 본 발명에 따른 문제를 해결하는 수단에 대해 반드시 필요한 것은 아니라는 것은 자명하다.

[0018] 본 실시예에서는, 정보 처리장치에 물리적으로 접속된 외부의 하드웨어 시큐리티 모듈(HSM)은 TPM(Trusted Platform Module)을 이용하는 것으로 가정한다. 본 실시예에서, TPM을 접속/이용가능하고 유저 인증 기능을 갖는 정보 처리장치의 일례로서, 복합기(multi-function peripheral/digital multi-function peripheral)를 설명한다. 그렇지만, 본 발명은, 이러한 복합기에 한정되지 않고, TPM 등의 HSM을 접속/이용가능하고 유저 인증 기능을 갖는 정보 처리장치를 채용할 수 있다.

[0019] 제1실시예

[0020] 도 1은, 본 발명의 제1실시예에 따른 복합기(100)의 하드웨어 구성의 개략을 설명하는 블록도다.

[0021] 제어부(101)는, 화상 입력 디바이스인 스캐너부(102)와 화상 출력 디바이스인 프린터부(103)와 접속하고, 네트워크(104) 또는 공중회선(105)과 접속함으로써 화상정보나 디바이스 정보의 입출력을 행한다.

[0022] CPU(106)은 복합기(100) 전체를 제어하는 프로세서다. RAM(107)은 CPU(106)이 동작하기 위한 시스템 워크 메모리를 제공하고, 또한 화상 데이터, 유저 정보나 패스워드 등을 일시 기억하기 위한 메모리이다. ROM(108)은 부트 ROM이며, 부트 프로그램을 격납하고 있다. HDD(109)은 하드디스크 드라이브이며, CPU(106)에 의해 실행되는 프로그램, 어플리케이션, 화상 데이터 등을 격납한다. 또한, 실시예에 따른 후술하는 흐름도를 실행하기 위한 프로그램도 이 HDD(109)에 격납되어 있다. 실시예에 따른 흐름도의 각 스텝은, CPU(106)이 HDD(109)에 기억된 프로그램을 RAM(107)에 전개해서 프로그램을 실행함으로써 달성된다. 단, 이 CPU(106) 이외의 프로세서가 상기 흐름도의 각 스텝을 실행하거나, 또는, CPU(106)과 다른 프로세서가 협동해서 상기 흐름도의 처리를 실행해도 된다.

[0023] 조작부 인터페이스(110)는, 터치패널을 갖는 조작부(111)와의 인터페이스를 제어하여, 조작부(111)에 표시할 화상 데이터를 조작부(111)에 출력하고, 또한 조작부(111)를 거쳐 유저가 입력한 정보를 CPU(106)에 전하는 역할을 한다. 네트워크 인터페이스(112)는 네트워크(104)에 접속하고, 네트워크(104)를 거쳐 정보의 입출력을 행한다. 모뎀(113)은 공중회선(105)에 접속하고, 공중회선(105)을 거쳐 다른 기기와 정보의 입출력을 행한다. SRAM(114)은 고속에서 동작가능한 불휘발성의 기록 매체다. RTC(115)은 리얼 타임 클록이며, 제어부(101)에 전원이 공급되지 않는 상태에서도 현재의 시간을 계속해서 카운트하는 처리를 행한다. 이상의 디바이스가 시스템 버스(116) 위에 배치된다.

[0024] 이미지 버스 I/F(117)는, 시스템 버스(116)와 화상 데이터를 고속으로 전송하는 화상 버스(118)를 접속하고, 데이터 구조를 변환하는 버스 브리지다. 화상 버스(118)는, PCI 버스 또는 IEEE1394로 구성되고, 이 화상 버스(118) 상에는 이하의 디바이스가 배치된다. RIP부(119)는 래스터 이미지 프로세서이며, PDL 코드를 비트맵 이미지로 전개한다. 디바이스 I/F부(120)는, 스캐너부(102), 프린터부(103)와 제어부(101)를 접속하고, 화상 데이터에 대해 동기계 및 비동기계 사이의 변환을 행한다. 스캐너 화상처리부(121)는, 스캐너부(102)로부터 입력한 화상 데이터에 대해 보정, 가공 및 편집을 행한다. 프린터 화상처리부(122)는, 프린터부(103)에 출력하는 화상 데이터에 대하여, 보정, 해상도 변환 등을 행한다. TPM(123)은, TPM 암호 키의 이용(TPM 기능)을 허용한다. USB 접속부(124)는, USB 메모리(125)(외부 메모리)에 접속하고, 그 USB 메모리(125)와의 사이에서 데이터의 입출력을 행한다.

[0025] 도 2는, 제1실시예에 따른 TPM(123)과 HDD(109)이 취급하는 암호 키와 기밀 데이터의 개략 구성을 설명하는 블록도다. 도 2의 상부는 TPM(123)의 개략 구성을 나타내고, TPM 루트 키(TPM root key)(201), TPM 암호 키(202) 및 TPM 레지스터(203)를 갖고 있다. 또한, 도 2 하부는 TPM 기능에 관련되고 HDD(109)에 기억되어 있는 데이터의 개략 구성을 나타내고, 이 데이터는 디바이스 암호 키(211), 디바이스 암호 키 블롭(blob)(212) 및 암호화된 데이터(213)를 포함하고 있다.

[0026] 제1실시예에서는, 복합기(100)가 다루는 기밀 데이터는 디바이스 암호 키(211)를 사용하여 암호화된다. 이 기밀 데이터는, 복합기(100)의 화상 데이터와 주소록 등의 개인 데이터 뿐만 아니라, 복합기(100)의 어플리케이션 소프트웨어가 취급하는 각각의 암호 키와 증명서, 유저 인증 기능의 패스워드 등도 포함하지만, 특별하게 한정은 하지 않는다.

[0027] 디바이스 암호 키(211)는, TPM 암호 키(202)를 사용하여 암호화된다. 또한, 이 TPM 암호 키(202)는, TPM 루트 키(201)를 사용하여 암호화된다. 이 TPM 루트 키(201)는, 외부에서의 접근에 의해 덮어쓰거나, 삭제하거나, 추출이 불가능하며, 암호화를 위해서만 사용될 수 있다. 이 일련의 암호 키의 체인에 의해, 내탬퍼성을 갖는 강고한 시큐리티를 실현할 수 있다. 또한, 공장 출하시 등 TPM(123)을 처음으로 복합기(100)에 접속하는 경우, TPM(123) 내부에는 TPM 암호 키(202)가 존재하지 않는다. 복합기(100)가 최초로 기동시에, CPU(106)이 암호 키를 생성하고, TPM 암호 키로서 이 암호화 키를 TPM(123)에 입력한다. 이렇게 해서, TPM(123) 내에서, TPM 암호 키(202)가 TPM 루트 키(201)를 사용하여 암호화되어, TPM 루트 키(201)와 관련된다. CPU(106)이 TPM 암호 키(202)를 TPM(123)에 입력할 때, TPM 레지스터(203)에 정보가 보존되고, 또한, TPM(123)은 CPU(106)에 암호 키 블롭을 출력한다. 이들 항목은 TPM 암호 키(202)의 정당성의 검증에 사용되며, 후술하는 도 3의 처리의 설명에서 설명한다.

[0028] 이때, 제1실시예에 있어서의 이들 키의 구성은 어디까지나 일례이며, 본 발명을 한정하는 것은 아니다. 예를 들면, TPM 내에 TPM 루트 키가 존재하지 않고, TPM 암호 키 만 격납하는 구성을 채용하거나, 또는, TPM 루트 키와 TPM 암호 키 이외의 암호 키를 사용하여 보다 견고하게 TPM 내의 암호 키를 보호하는 구성을 채용해도 된다. 또한, HDD(109)의 기밀 데이터가, TPM 암호 키로 암호화된 디바이스 암호 키로 암호화되는 것이 아니라, TPM 암호 키로 직접 암호화되는 구성을 채용해도 된다.

[0029] 다음에, 제1실시예에 따른 복합기(100)의 기동시에 행해지는 TPM(123)의 암호 키의 정당성의 검증 제어에 대해서 도 1 내지 도 3을 참조하여 설명한다. 이때, 본 실시예에 따른 복합기(100)의 처리는, 복합기(100) 내의 CPU(106)에 의해 제어된다.

[0030] 도 3은, 제1실시예에 따른 복합기(100)의 기동 처리를 설명하는 흐름도다. 이때, 이 처리는, CPU(106)이, 예를 들면, HDD(109)에 격납되어 있는 프로그램을 RAM(107)에 전개해서 이 프로그램을 실행함으로써 달성된다.

[0031] 우선, 스텝 S301에서 CPU(106)은, SRAM(114)로부터 복합기(100)의 TPM 설정을 취득한다. 이 TPM 설정은, 복합기(100)의 TPM 기능이 유효인지 또는 무효인지를 표시하는 설정 정보다. 다음에, 스텝 S302로 절차를 진행하여, CPU(106)은, 스텝 S301에서 취득한 TPM 설정이 유효인지 아닌지 판정한다. 스텝 S302에서 CPU(106)이 TPM 설정이 무효라고 판정하면, 이 처리를 종료한다. 한편, 스텝 S302에서 CPU(106)이 TPM 설정이 유효라고 판정한 경우에는 스텝 S303으로 절차를 진행하여, CPU(106)은, 암호 키의 정당성을 검증한다.

[0032] 제1실시예에서는, TPM(123)의 TPM 암호 키(202)와 디바이스 암호 키(211)는 정당성을 검증의 대상으로 설정된다. 정당성의 검증은, TPM 암호 키(202)가 HDD(109)의 디바이스 암호 키(211)를 TPM 루트 키(201)를 사용하여 암호화하여 얻어진 키이기 때문에, TPM 암호 키(202)를 TPM 루트 키(201)로 복호화해서 디바이스 암호 키(211)가 얻어지는지 아닌지 확인하는 것을 말한다. 전술한 바와 같이, TPM(123)의 TPM 암호 키(202)는 CPU(106)에 의해 입력되고, TPM 루트 키(201)로 암호화된다. 이때, CPU(106)가 TPM 암호 키(202)를 생성해서 TPM 암호 키(202)를 TPM(123)에 보존할 때, CPU(106)은 TPM(123)으로부터 암호 키 블롭(212)을 취득해서 이 암호 키 블롭(212)을 HDD(109)에 보존한다. 이때, 이 암호 키 블롭(212)을 TPM(123)과 관련시키는 정보도, TPM(123)의 TPM 레지스터(203)에 보존된다. 따라서, 스텝 S303에서, CPU(106)은 HDD(109)에 격납되어 있는 암호 키 블롭(212)을 TPM(123)에 입력한다. 이에 따라, TPM(123)은, 그 입력된 암호 키 블롭(212)과 TPM 레지스터(203)에 보존하고 있는 관련 정보를 비교한다. 이것들이 일치하면, TPM(123)의 TPM 암호 키(202)와, HDD(109)에 보존하고 있는 디바이스 암호 키(211)가 관련되어 있다고 확인한다.

[0033] 이때, 이 암호 키의 정당성의 확인 처리는 어디까지나 일례이며, 이 처리에 한정되지 않는 것으로 한다. 예를 들면, TPM 레지스터(203)에 디바이스 암호 키의 카피를 유지하고, CPU(106)이 디바이스 암호 키(211)를 TPM(123)에 입력하고, 디바이스 암호 키(211)를 TPM 레지스터(203)에 유지되어 있는 디바이스 암호 키와 비교한다. 이렇게 해서, HDD(109)의 디바이스 암호 키(211)와 TPM(123)의 TPM 암호 키(202)가 관련되어 있는지 아닌지 확인해도 된다.

[0034] 스텝 S303의 처리후, 스텝 S304로 절차를 진행하여, CPU(106)는 암호 키의 정당성의 검증에 의해, CPU(106)이 취급하는 암호 키를 정상적으로 이용할 수 있는지 아닌지 판정한다. 스텝 S304에서 CPU(106)이 암호 키의 정당성의 검증에 의해 그 암호 키를 정상적으로 이용가능하다고 판정한 경우에는, 이 처리를 종료한다. 한편, 스텝 S304에서 CPU(106)이 암호 키의 정당성의 검증에 의해 취급할 암호 키를 정상적으로 이용할 수 없다고 판정한 경우에는, 스텝 S305로 절차를 진행하여, CPU(106)은 조작부(111)에 에러 화면(여기에서는 도시하지 않

는다)을 표시하고, 이 처리를 종료한다.

[0035] 전술한 처리가 복합기(100)의 기동 처리시의 TPM 암호 키의 정당성 검증 처리다. 이때, 스텝 S305와 같이 암호 키를 정상적으로 이용할 수 없는 경우의 예로는, TPM 칩의 고장이나 TPM 칩이 접속되거나 TPM 칩이 내장되는 메인 보드의 고장에 의해 칩/메인 보드를 교환하고, 그후 복합기(100)를 기동하는 경우를 들 수 있다.

[0036] 다음에, 제1실시예에 따른 TPM 기능을 유효로 하는 제어에 대해 도 1, 도 4 및 도 5a 내지 도 5c를 참조하여 설명한다.

[0037] 도 4는, 제1실시예에 따른 복합기(100)에 있어서의 TPM 기능을 유효로 하는 처리를 설명하는 흐름도다. 이때, 이 처리는, CPU(106)이, 예를 들면, HDD(109)에 격납되어 있는 프로그램을 RAM(107)에 전개해서 이 프로그램을 실행함으로써 달성된다.

[0038] 우선, 스텝 S401에서 CPU(106)은, 조작부(111)로부터 TPM 설정 관리 화면(도 5a 내지 5c)의 표시 지시를 접수한다. 다음에, 스텝 S402로 절차를 진행하여 CPU(106)은, SRAM(114)에 보존되어 있는 TPM 설정을 취득한다. 다음에, 스텝 S403으로 절차를 진행하여 CPU(106)은, 그 취득한 TPM 설정이 유효로서 설정되어 있는지를 판정한다. TPM 설정이 유효인 것으로 판정되면, 절차가 스텝 S412로 진행하지만, 그렇지 않을 때는 스텝 S404로 절차를 진행하여, CPU(106)은, USB 접속부(124)에 USB 메모리(125)가 접속되어 있는지를 판정한다. 스텝 S404에서 CPU(106)이, USB 접속부(124)에 USB 메모리(125)가 접속되지 않고 있다고 판정한 경우에는, 스텝 S405로 절차를 진행한다. 스텝 S405에서 CPU(106)은, 유저에 대하여, USB 접속부(124)에 USB 메모리(125)를 접속하도록 요구하는 메시지를 조작부(111)에 표시하고, 스텝 S404로 절차를 진행한다.

[0039] 도 5a는, 제1실시예에 따른 복합기(100)의 조작부(111)에 표시되는 TPM 설정 관리 화면의 일례를 도시한 도면이다.

[0040] 여기에서는, TMP 설정을 유효로 하기 위해서, TPM 암호 키를 백업할 수 있는 USB 메모리(125)를 USB 접속부(124)에 접속하도록 유저에게 요구하는 메시지가 표시된 예를 나타내고 있다. 이 화면은, 현재의 TPM 설정의 항목(501)과, TPM 설정을 유효로 하는 버튼(502)을 포함하고 있다. 스텝 S405의 상태에서의 도 5a에서는, USB 메모리(125)가 접속되어 있지 않기 때문에, TPM 설정을 유효로 하는 버튼(502)은 이 버튼(502)을 누를 수 없도록, 그레이아웃해서 표시되어 있다.

[0041] 스텝 S404에서 CPU(106)이, USB 접속부(124)에 USB 메모리(125)가 접속되어 있다고 판정한 경우에는, 스텝 S406으로 절차를 진행하여, CPU(106)은, 그 USB 메모리(125)의 정보를 취득하고, 스텝 S407로 절차를 진행한다. 스텝 S407에서 CPU(106)은, USB 메모리(125)의 기억 영역에 TPM 암호 키를 백업할 수 있는지 아닌지 판정한다. 스텝 S407에서 TPM 암호 키를 백업할 수 없다고 판정한 경우에는 스텝 S405로 절차를 진행한다. 여기에서, TPM 암호 키를 백업할 수 없는 상태는, 예를 들어, USB 메모리(125)에 비어 있는 기억 영역이 없는 경우나, 유저가 그 기억 영역에 기록할 수 있는 권한을 갖지 않을 때, USB 메모리(125)에 TPM 암호 키를 기록할 수 없는 경우를 말한다.

[0042] 이때, 제1실시예에서는, TPM 암호 키의 백업처를 USB 메모리로 가정하고 있지만, 백업처는 USB 메모리 이외의 스토리지이어도 되고, 특별하게 한정은 하지 않는다. 예를 들면, USB-HDD 및 SD 카드 등의 메모리 미디어, 네트워크를 거친 SMB, 클라우드 스토리지 영역 등을 사용해도 된다.

[0043] 한편, 스텝 S407에서 CPU(106)이 USB 메모리(125)의 기억 영역에 TPM 암호 키를 백업할 수 있다고 판정한 경우에는 스텝 S408로 절차를 진행하여, CPU(106)은, 전술한 TPM 설정 관리 화면의 TPM 설정을 유효로 하는 버튼(502)을 누름 가능하게 해서 표시한다. 도 5b는, TPM 설정 관리 화면에서, TPM 설정을 유효로 하는 버튼(502)의 그레이아웃 상태를 해제하고, 누름 가능하게 버튼(502)을 표시한 예를 나타내고 있다.

[0044] 다음에, 스텝 S409로 절차를 진행하여, CPU(106)은, TPM 설정을 유효로 하는 버튼(502)이 눌러졌는지 아닌지를 판정한다. 스텝 S409에서 CPU(106)가 그 버튼(502)이 눌러졌다고 판정한 경우에는 스텝 S410으로 절차를 진행하여, CPU(106)은 TPM 설정을 유효로 한다. 그후, 스텝 S411에서 CPU(106)은, TPM 암호 키의 백업 처리를 실행한다.

[0045] 제1실시예에서는, TPM 설정이 유효로 되면 CPU(106)은 TPM(123)에 대하여 TPM 암호 키의 생성 지시를 출력한다. 이에 따라, TPM(123)은 TPM 암호 키를 생성하고, CPU(106)에 암호 키 블롭(212)을 출력한다. 이 TPM 기능의 설정이 유효로 되어 있는 것을 표시하는 설정 정보는 CPU(106)에 의해 SRAM(114)에 보존된다.

[0046] 이 스텝 S404 내지 스텝 S411에서 유저가 TPM 기능을 유효로 하면, 미리 TPM 암호 키를 백업할 수 있는

것을 조건으로, TPM 암호 키의 생성 처리가 실행된다. 이에 따라, 유저가 TPM 암호 키를 백업하는 것을 잊는 것을 방지하는 효과가 있다.

[0047] 다음에, 스텝 S411에 있어서, TPM 암호 키의 백업 처리를 도 1, 도 6, 도 7을 참조하여 설명한다.

[0048] 도 6은, 제1실시예에 따른 복합기(100)에 의해 행해지는 도 4의 스텝 S411의 TPM 암호 키의 백업 처리를 설명하는 흐름도다.

[0049] 스텝 S601에서 CPU(106)은, 조작부(111)에 TPM 암호 키의 백업용의 패스워드를 입력하기 위한 화면을 표시하고, TPM 암호 키의 백업시의 패스워드의 입력을 접수한다.

[0050] 도 7은, 제1실시예에 따른 복합기(100)의 조작부(111)에 표시되는 TPM 암호 키의 백업용의 패스워드를 입력하는 화면의 일례를 도시한 도면이다.

[0051] 조작부(111)로부터 입력된 패스워드는, "*"로 마스크되어서 패스워드의 입력 프레임(701)에 표시된다. 여기에서, 유저가 OK 버튼(702)을 누르면, CPU(106)은, TPM 암호 키의 백업용의 패스워드와 함께, TPM 암호 키의 백업 실행 지시를 접수한다. 제1실시예에서는, 이 패스워드 정보는 CPU(106)에 의해 SRAM(114)에 유지된다. 또한, 제1실시예에서는, 오설정 방지를 위해 동일한 패스워드가 2회 입력되는 것으로 가정한다.

[0052] 이렇게 해서 스텝 S602에서 CPU(106)가 패스워드의 입력이 완료했다고 판정하면, 스텝 S603으로 절차를 진행하여, CPU(106)은, SRAM(114)에 유지한 패스워드를 기초로 TPM 암호 키를 암호화해서, 스텝 S604로 절차를 진행한다. 제1실시예에 있어서의 패스워드를 사용한 암호화는, PKCS#12(public Key Cryptography Standard #12) 포맷으로 행하는 것으로 가정한다. 이때, 제1실시예에서는, TPM 암호 키의 백업은, 유저가 지정한 패스워드 정보를 기초로 한 패스워드 암호화 방식에 의해 행해지지만, 본 발명은 이것에 한정되지 않는다. 예를 들면, 미리 복합기(100)에 유지한 고정 패스워드, 공통 키, 또는 PKI 메카니즘을 사용한 공개 키와 비밀 키로 TPM 암호 키를 보호해도 된다.

[0053] 다음에, 스텝 S604로 절차를 진행하여, CPU(106)은, 암호화한 TPM 암호 키를 백업하기 위해서 암호화한 TPM 암호 키를 출력 파일 형식으로 정형하고, 파일을 아카이브해서, 스텝 S605로 절차를 진행한다. 제1실시예에서는, 후술하는 TPM 암호 키의 리스토어를 행하기 전에, 암호화한 TPM 암호 키의 파일인 것을 식별하기 위해, 출력할 파일을 이 파일에 식별 헤더를 붙여 아카이브한다. 제1실시예에서는, 이 데이터를 TPM 암호 키 백업 데이터로 칭한다.

[0054] 스텝 S605에서, CPU(106)은, 아카이브화한 TPM 암호 키 백업 데이터를 USB 메모리(125)에 기록한다. 다음에, 스텝 S606으로 절차를 진행하여, CPU(106)은, TPM 암호 키 백업 데이터를 USB 메모리(125)에 정상으로 기록할 수 있었는지 아닌지 판정하여, USB 메모리(125)에의 기록에 실패했다고 판정한 경우에는, 스텝 S607로 절차를 진행한다. 스텝 S607에서, CPU(106)은, 조작부(111)에 기록 에러를 표시하고, 스텝 S601로 절차를 진행하여, 백업 처리를 반복한다.

[0055] 한편, 스텝 S606에서 USB 메모리(125)에의 백업에 성공했다고 판정한 경우에는 스텝 S608로 절차를 진행하여, CPU(106)은 SRAM(114)에 백업 완료 플래그를 보존하고, 스텝 S609로 절차를 진행한다. 스텝 S609에서, CPU(106)은, 조작부(111)에 TPM 암호 키의 백업이 완료한 것을 나타내는 메시지를 표시하고, 이 TPM 암호 키 백업처리를 종료한다.

[0056] 이때, 제1실시예에서는, TPM 설정을 유효로 하는 버튼(502)이 눌러졌을 때에, 자동적으로 도 7의 TPM 암호 키 백업용의 패스워드의 입력 화면으로 화면이 전환되는 것으로 가정한다. 그러나, 자동적으로 화면이 천이하지 않고, 유저의 지시에 따라 화면이 천이해서 백업이 행해지는 구성을 채용하여도 된다.

[0057] 다음에, 도 4의 설명으로 되돌아간다.

[0058] 이렇게 해서 TPM 암호 키의 백업이 완료하면, 도 4의 스텝 S412로 절차를 진행하여, CPU(106)은, 조작부(111)에 TPM 설정이 유효로 된 것을 나타내는 메시지를 표시한다.

[0059] 도 5c는, TPM 설정이 유효로 되었을 때의 TPM 설정 화면의 일례를 도시한 도면이다.

[0060] 도 5c에는, 현재의 TPM 설정 항목(501)이 "ON"으로 변경되고, TPM 설정을 유효로 하는 버튼(502)을 그레이아웃으로 표시해서 누를 수 없도록 하는 예를 나타내고 있다.

[0061] 이때, 제1실시예에 따른 TPM 설정의 유효화와 TPM 암호 키의 백업을 관리자 권한을 갖는 유저만 행할

수 있다는 것을 상정하고 있다. 그 때문에, 도 5a 내지 도 5c에 나타낸 TPM 설정 관리 화면은, 관리자 권한이 있는 유저가 로그인한 경우에만 표시된다.

[0062] 이상에서 설명한 바와 같이, 제1실시예에 따르면, TPM 기능을 갖는 정보 처리장치에서, TPM 암호 키를 백업할 수 있다는 것을 조건으로, 유저가 TPM 설정을 무효인 상태로부터 유효인 상태로 변경할 수 있다. 이에 따라, TPM 설정을 유효로 한 후에, 유저가 TPM 암호 키의 백업을 잊는 것을 방지할 수 있다.

[0063] 제2실시예

[0064] 다음에, 본 발명의 제2실시예에 대해 설명한다. 전술한 제1실시예에서는, 복합기(100)의 TPM 설정을 유효로 할 때, 유저가 조작부(111)를 거쳐 조작하는 것을 전제로 하고 있었다. 그렇지만, 이러한 로컬 UI로부터의 설정에 의해 TPM 설정 만을 유효로 하는 것 대신에, 리모트로 TPM 설정을 유효로 하는 경우도 있다. 한가지 예는, 복합기(100)의 TPM 설정을 포함하는 관리자 설정이 데이터로서 네트워크를 거쳐 임포트되는 경우이다. 이러한 경우, 제1실시예와 같이, 리모트로 지시가 주어진다면, USB 메모리 등의 스토리지를 접속하지 않고 있으면, TPM 기능을 유효로 할 수 없다고 하는 것은 현실적이지 않다. 한편, 스토리지가 접속되지 않고 있어도, 리모트로 TPM 설정을 유효화할 수 있도록 하는 구성이 채용되는 경우, TPM 암호 키가 백업되지 않는다는 사태가 발생할 가능성이 있다.

[0065] 이에 따라, 제2실시예에서는, 네트워크를 거쳐 리모트 장치로부터 TPM 설정을 유효로 하는 지시를 받은 경우에, 스토리지가 접속되지 않고 있어도 TPM 설정을 유효화하는 것을 허가한다. TPM 암호 키가 백업되지 않고 있는 상태에서 TPM 설정이 유효로 된 복합기(100)의 기동시, 또는 이와 같은 상태에서 복합기(100)에서의 유저 인증시에, TPM 암호 키를 백업하도록 유저에게 촉구하여, 유저가 TPM 암호 키의 백업을 잊는 것을 억제한다. 이때, 제2실시예에 따른 복합기(100) 및 TPM(123)의 구성, TPM 암호 키 백업 처리 등에 관해, 제2실시예에서 설명하지 않는 개소는 제1실시예에서와 같다. 이하에서는, 리모트 장치로부터 TPM 설정을 유효로 하는 지시를 받았을 때 TPM 설정이 유효화되는 경우의 처리에 대해 설명한다. 제2실시예에 있어서도, 유저가 복합기(100)의 조작부(111)로부터 TPM 설정을 유효화하려고 시도하는 경우에는, 복합기(100)는 제1실시예의 처리를 실행한다.

[0066] 도 8은, 제2실시예에 따른 복합기(100)의 기동 처리를 설명하는 흐름도다. 이때, 이 처리는 CPU(106)이 예를 들면, HDD(109)에 격납되어 있는 프로그램을 RAM(107)에 전개해서 이 프로그램을 실행함으로써 달성된다. 이 도 8의 처리는, 전술한 제1실시예에 따른 도 3의 흐름도와, 스텝 S806 및 S807의 처리가 추가되어 있는 점에서 다르다. 이 추가되는 처리는, TPM 암호 키가 백업되지 않은 경우에 백업 지시를 표시하는 처리이지만, 그것의 상세에 대해서는 후술한다. 제2실시예에 따른 도 8의 흐름도의 스텝 S801 내지 S805의 처리는, 제1실시예의 도 3의 스텝 S301 내지 스텝 S305의 처리와 유사하기 때문에, 그것들의 설명을 생략한다.

[0067] 스텝 S804에서 CPU(106)이 암호 키의 정당성의 검증에 의해 CPU(106)이 취급하는 암호 키가 정상적으로 이용가능하다고 판정한 경우에는, 스텝 S806으로 절차를 진행한다. 스텝 S806에서, CPU(106)은, SRAM(114)에 보존되어 있는 백업 완료 플래그를 참조하여, TPM 암호 키가 백업되었는지 아닌지 판정한다. 이 백업 완료 플래그는, 전술한 제1실시예의 스텝 S608에서 CPU(106)에 의해 SRAM(114)에 보존한 정보이다. 이렇게 해서 스텝 S806에서 CPU(106)이, TPM 암호 키가 백업되었다고 판정한 경우에는, 이 처리를 종료한다. 한편, 스텝 S806에서 CPU(106)이, TPM 암호 키가 백업되지 않았다고 판정한 경우에는, 스텝 S807로 절차를 진행하여, CPU(106)은 조작부(111)에 TPM 암호 키의 백업을 지시하는 화면을 표시하고, 이 처리를 종료한다.

[0068] 도 9는, 제2실시예에 따른 복합기(100)가 제공하는 기능의 메인 메뉴 화면의 일례를 도시한 도면이다. 이 화면은, 복합기(100)의 기동시에 CPU(106)에 의해 조작부(111)에 표시된다. 제2실시예에서는, 이 메인 메뉴 화면의 스테이터스 라인(901)의 영역에 백업 지시 메시지(902)를 표시하고, 유저에게 TPM 암호 키를 백업하도록 촉구하는 화면을 표시한다.

[0069] 이에 따라, 복합기(100)의 유저가 TPM 암호 키가 백업되지 않은 것을 알아차리고, 적절한 대처를 행할 수 있게 된다.

[0070] 다음에, 복합기(100)에 대하여 관리자가 유저 인증을 행한 경우의 제어에 대해 설명한다.

[0071] 도 10은, 제2실시예에 따른 복합기(100)에 의한 유저 인증 처리를 설명하는 흐름도다. 이때, 이 처리는, CPU(106)이, 예를 들면, HDD(109)에 격납되어 있는 프로그램을 RAM(107)에 전개해서 이 프로그램을 실행함으로써 달성된다.

[0072] 우선, 스텝 S1001에서 CPU(106)은, 조작부(111)에게 로그인 화면을 표시시키고, 스텝 S1002로 절차를

진행한다. 스텝 S1002에서 CPU(106)은, 조작부(111)를 거쳐 유저로부터의 유저 정보와 패스워드의 입력을 접수한다. 이렇게 해서 입력된 유저 정보와 패스워드는, RAM(107)에 유지된다. 제2실시예에서는, 유저 정보와 패스워드를 일시 기억하기 위해서 RAM(107)을 사용하고 있지만, HDD(109) 등 데이터를 기억 가능한 다른 장치를 사용해도 되고, 한정은 하지 않는다. 후술하는 제3실시예에 관해서도 마찬가지로 한정은 하지 않는다. 또한, 제2실시예에서는, CPU(106)은 유저 인증을 위한 유저 정보와 관련된 패스워드를, 디바이스 암호 키(211)를 사용하여 암호화해서 이 패스워드를 HDD(109)에 기억한다.

[0073] 다음에, 스텝 S1003으로 절차를 진행하여 CPU(106)은, 입력된 유저 정보와 관련하여 암호화되어 있는 패스워드 정보를 HDD(109)로부터 취득하고, 이 패스워드 정보를 복호화하고, 패스워드 정보를 입력된 패스워드와 비교하여, 패스워드가 올바른 패스워드인지 아닌지를 검증하고, 스텝 S1004로 절차를 이행한다. 제2실시예에서는, 이 CPU(106)에 의한 암호화된 패스워드의 복호화는 디바이스 암호 키(211)를 사용해서 행한다. 또한, 디바이스 암호 키(211)는, TPM(123)의 TPM 암호 키(202)를 사용하여 암호화된다. CPU(106)은 TPM(123)에 암호화된 디바이스 암호 키(211)를 입력함으로써 TPM 암호 키(202)로 복호화된 디바이스 암호 키를 취득해서 이용한다. 또한, 이 TPM 암호 키(202)는 TPM 루트 키(201)로 암호화되어 있고, TPM 암호 키(202)를 이용할 때는, TPM 루트 키(201)를 사용하여 TPM 암호 키(202)가 복호화된다.

[0074] 스텝 S1004에서 CPU(106)은, 스텝 S1002에서 입력된 유저 정보와 패스워드를 사용하여 유저에 대해 인증을 행하고 그 결과 인증에 실패한 경우에는, 조작부(111)에 에러를 표시하고, 스텝 S1002로 절차를 이행한다. 한편, 스텝 S1004에서 CPU(106)이, 입력된 유저 정보와 패스워드가 올바르다고 판정해서 유저의 인증에 성공한 경우에는, 스텝 S1005로 절차를 진행하여, CPU(106)은, 그 유저가 복합기(100)에 로그인하는 것을 허가한다. 다음에, 스텝 S1006으로 절차를 진행하여, CPU(106)은, 그 로그인한 유저의 유저 정보를 RAM(107)이 유지하게 하고, 스텝 S1007로 절차를 진행한다. 스텝 S1007에서 CPU(106)은, SRAM(114)로부터 TPM 설정을 취득해서 스텝 S1008로 절차를 이행한다.

[0075] 스텝 S1008에서 CPU(106)은, SRAM(114)로부터 취득한 TPM 설정이 유효로 설정되어 있는지 아닌지를 판정한다. 여기에서, CPU(106)이, TPM 설정이 무효라고 판정한 경우에는, 이 처리를 종료한다. 한편, 스텝 S1008에서 CPU(106)이 TPM 설정이 유효로 설정되어 있다고 판정한 경우에는, 스텝 S1009로 절차를 진행하여, CPU(106)은 SRAM(114)로부터 TPM 암호 키가 백업되었는지 아닌지 판정한다. 이때, 제1실시예에서 설명한 바와 같이, SRAM(114)에 보존되어 있는 백업 완료 플래그가 온인지 아닌지에 따라, TPM 암호 키가 백업되었는지 아닌지 판정한다. 여기에서, TPM 암호 키가 백업되었다고 판정한 경우에는, 이 처리를 종료한다. 한편, 스텝 S1009에서 CPU(106)이, TPM 암호 키가 백업되지 않았다고 판정한 경우에는, 스텝 S1010으로 절차를 진행하여, CPU(106)은 로그인한 유저가 관리자 권한을 갖는지 아닌지 판정한다. 여기에서, 그 유저가 관리자 권한을 갖는다고 판정한 경우에는 스텝 S1011로 절차를 진행하여, CPU(106)은, TPM 암호 키의 백업을 유저에게 촉구하는 화면을 표시하게 한다. 제2실시예에서는, 전술한 도 7에 나타낸 TPM 암호 키 백업용의 패스워드의 입력 화면을 조작부(111)에 표시한다. 그후의 TPM 암호 키 백업 처리는, 전술한 제1실시예에서의 처리와 유사하다. 스텝 S1012에서, CPU(106)은, 전술한 도 6의 흐름도와 유사하게, TPM 암호 키의 백업 처리를 실행하고, 이 처리를 종료한다.

[0076] 이러한 처리에 의해, 로그인한 유저가 관리자이고 TPM 암호 키가 백업되지 않은 경우에, 유저에게 TPM 암호 키의 백업을 촉구하는 것에 의해, 유저가 TPM 암호 키를 백업하는 것을 잊는 것을 억제할 수 있다. 이때, 제2실시예에서는, 유저의 인증 직후에 백업을 촉구하는 화면을 조작부(111)에 표시하고 있었지만, 본 발명은 이것에 한정되지 않는다. 예를 들면, 유저가 복합기(100)의 관리 설정을 조작할 때에, 조작부(111)의 표시가 관리 화면으로 천이할 때 이와 같은 화면을 표시하도록 하는 구성을 채용하여도 된다.

[0077] 스텝 S1010에서 CPU(106)이, 로그인한 유저가 관리자 권한을 갖지 않는다고 판정한 경우에는, 이 처리를 종료한다. 제2실시예에서, 이것은, TPM 암호 키의 백업이 관리자 권한을 갖는 유저에 의해서만 실행되는 것을 상정하고 있기 때문이다.

[0078] 이때, 제2 실시예에서는, TPM 암호 키의 백업을 행하지 않아도, 복합기(100)가 제공하는 카피 기능 등의 다른 기능을 실행할 수 있다. 그렇지만, TPM 암호 키의 백업을 하지 않으면, 도 9의 메인 메뉴 화면에서 제공하는 카피 버튼 등의 버튼을 조작할 수 없게 해서, 소정의 기능의 실행이 허용되지 않는 사양을 채용해도 되고, 특별하게 한정은 하지 않는다.

[0079] 이상에서 설명한 바와 같이, 제2실시예에 따르면, TPM 암호 키가 백업되지 않은 상태에서 TPM 설정이 유효로 되어 있는 복합기(100)가 기동되거나, 또는 이 상태에서 유저를 인증할 때에, TPM 암호 키의 백업을 유저에게 촉구하고 있다. 이에 따라, 유저가 TPM 설정을 제1실시예와는 달리, 예를 들면, 리모트로 유효로 하는

경우에, 유저가 TPM 암호 키를 백업하는 것을 잊어버리는 것을 억제할 수 있다.

[0080] 제3실시예

[0081] 다음에, 본 발명의 제3실시예에 대해 설명한다. 전술한 제1 및 제2실시예에서는, TPM 기능을 갖는 복합기(100)에 있어서, TPM 암호 키는 TPM 설정을 유효로 한 후에 생성되기 때문에, 백업도 TPM 설정을 유효로 한 후에만 행할 수 있다. 그렇지만, 기능(이하, HSM 기능)을 유효로 하기 전에 암호 키(이하, HSM 암호 키)를 생성하는 다른 HSM(Hardware Security Module)이 존재할 수 있다. 이에 따라, 제3실시예에서는, HSM 암호 키가 HSM 기능을 유효로 하기 전에 생성/백업 가능한 복합기(100)에 있어서, 유저가 HSM 암호 키를 백업하는 것을 잊는 것을 억제하는 제어에 대해 설명한다. 이하, 제3실시예에서는, 전술한 제1 및 제2실시예와의 차이를 설명한다.

[0082] 도 11은, 본 발명의 제3실시예에 따른 복합기(100)에 의해 행해지는 HSM 기능을 유효로 하는 처리와 백업 처리를 설명하는 흐름도이다. 이때, 이 처리는, CPU(106)이, 예를 들면, HDD(109)에 격납되어 있는 프로그램을 RAM(107)에 전개해서 이 프로그램을 실행함으로써 달성된다.

[0083] 우선, 스텝 S1101에서 CPU(106)은, 조작부(111)로부터 HSM 설정 관리 화면의 표시 지시를 접수한다. 다음에, 스텝 S1102로 절차를 진행하여 CPU(106)은, SRAM(114)으로부터 HSM 설정을 취득한다. 다음에, 스텝 S1103에서 CPU(106)은, SRAM(114)로부터 취득한 HSM 설정이 유효한지를 판정한다. 스텝 S1103에서 CPU(106)은, 취득한 HSM 설정이 무효라고 판정하면, 스텝 S1104로 절차를 진행하여, CPU(106)은 조작부(111)에 HSM 암호 키를 사전에 백업하도록 유저에게 요구하는 메시지를 표시하고, 스텝 S1105로 절차를 진행한다.

[0084] 스텝 S1105에서, CPU(106)은, HSM 암호 키가 백업되었는지 아닌지를 판정한다. 이 경우도, 전술한 스텝 S806과 마찬가지로, SRAM(114)에 보존되어 있는 백업 완료 플래그가 온인지 아닌지에 따라, HSM 암호 키가 백업되었는지 아닌지 판정한다. 여기에서, HSM 암호 키가 백업되지 않았다고 판정한 경우에는, 스텝 S1106으로 절차를 진행하여, CPU(106)은 HSM 암호 키의 백업을 접수하고, 스텝 S1107로 절차를 진행한다.

[0085] 도 12a는, 도 11의 스텝 S1106에서 복합기(100)의 조작부(111)에 표시되는 HSM 설정 관리 화면의 일례를 도시한 도면이다. 여기에서는, HSM 암호 키를 사전에 백업하도록 유저에게 요구하는 메시지가 표시되어 있고, 현재의 HSM 설정(1203)이 오프이다. 여기에서는, 도 12a에 나타낸 것과 같이, HSM 암호 키의 백업의 실행을 지시하는 버튼(1202)은 조작가능한 상태로 표시되어 있고, HSM 설정을 유효로 하는 버튼(1201)은 조작할 수 없도록 그레이아웃하여 표시되어 있다.

[0086] 스텝 S1107에서, CPU(106)은, 버튼(1202)을 조작하여 HSM 암호 키의 백업의 실행이 지시되었는지 아닌지를 판정하여, HSM 암호 키의 백업의 실행이 지시되었다고 판정했을 때는 스텝 S1108로 절차를 진행하고, HSM 암호 키의 백업 처리를 실시한다. 이 HSM 암호 키의 백업 처리에서는, TPM 암호 키의 백업이 HSM 암호 키의 백업으로 변경된 것 뿐으로, 이 처리는 기본적으로는 상기한 제1실시예의 스텝 S411과 유사하다.

[0087] 한편, 스텝 S1105에서 CPU(106)이, HSM 암호 키가 백업되었다고 판정한 경우에는, 스텝 S1109로 처리를 진행하여, CPU(106)은, HSM 설정을 유효로 하는 지시를 접수하고, 스텝 S1110으로 절차를 진행한다.

[0088] 도 12b는, 도 11의 스텝 S1109에서, 복합기(100)의 조작부(111)에 표시되는 HSM 설정 관리 화면의 일례를 도시한 도면이다.

[0089] 여기에서는, HSM 암호 키가 백업되었기 때문에, HSM 설정을 유효로 하는 버튼(1201)의 그레이아웃 상태가 해제되어, 버튼(1201)을 누를 수 있다. 또한, 도 12b에서는, HSM 암호 키의 백업의 실행을 지시하는 버튼(1202)은 조작할 수 없도록 그레이아웃으로 표시되어 있다.

[0090] 스텝 S1110에서, CPU(106)은, HSM 설정을 유효로 하는 버튼(1201)을 누름으로써, HSM 설정을 유효로 하도록 지시되었는지 아닌지 판정한다. 여기에서, CPU(106)은, HSM 설정을 유효로 하는 버튼(1201)이 눌러졌다고 판정한 경우에는, 스텝 S1111로 절차를 진행하여, HSM 설정을 유효하게 하고, 스텝 S1112로 절차를 진행한다. 이러한 처리에 의해, HSM 암호 키를 반드시 백업하지 않으면 HSM 설정을 유효로 할 수 없는 구성을 채용함으로써, 유저가 HSM 암호 키의 백업을 잊는 것을 억제할 수 있다.

[0091] 다음에, 스텝 S1112에서, CPU(106)은, HSM 설정 관리 화면에, HSM 기능의 설정이 유효로 되어 있는 상태를 표시한다.

[0092] 도 12c는, 도 11의 스텝 S1112에서, 복합기(100)의 조작부(111)에 표시되는 HSM 설정 관리 화면의 일례를 도시한 도면으로, 여기에서는 HSM 설정이 유효로 된 것을 나타내는 화면의 예를 나타낸다.

[0093] 도 12c에서는, HSM 설정이 유효이고 HSM 암호 키가 백업되었기 때문에, 현재의 HSM 설정(1203)이 ON으로 설정되고, HSM 설정을 유효로 하는 버튼(1201)이 조작할 수 없도록 그레이아웃으로 표시되어 있다. 또한, HSM 암호 키의 백업의 실행을 지시하는 버튼(1202)은 조작할 수 없도록 그레이아웃으로 표시되어 있다.

[0094] 이상에서 설명한 바와 같이, 제3실시예에 따르면, HSM 설정이 유효해지기 전에 HSM 암호 키를 백업할 수 있는 복합기에 있어서, HSM 암호 키를 반드시 백업을 실행하지 않으면 HSM 설정을 유효로 할 수 없는 구성을 채용할 수 있다. 이에 따라, HSM 설정을 유효로 했을 때에, 유저가 HSM 암호 키의 백업을 잊어버리는 것을 억제할 수 있다.

[0095] 기타 실시예

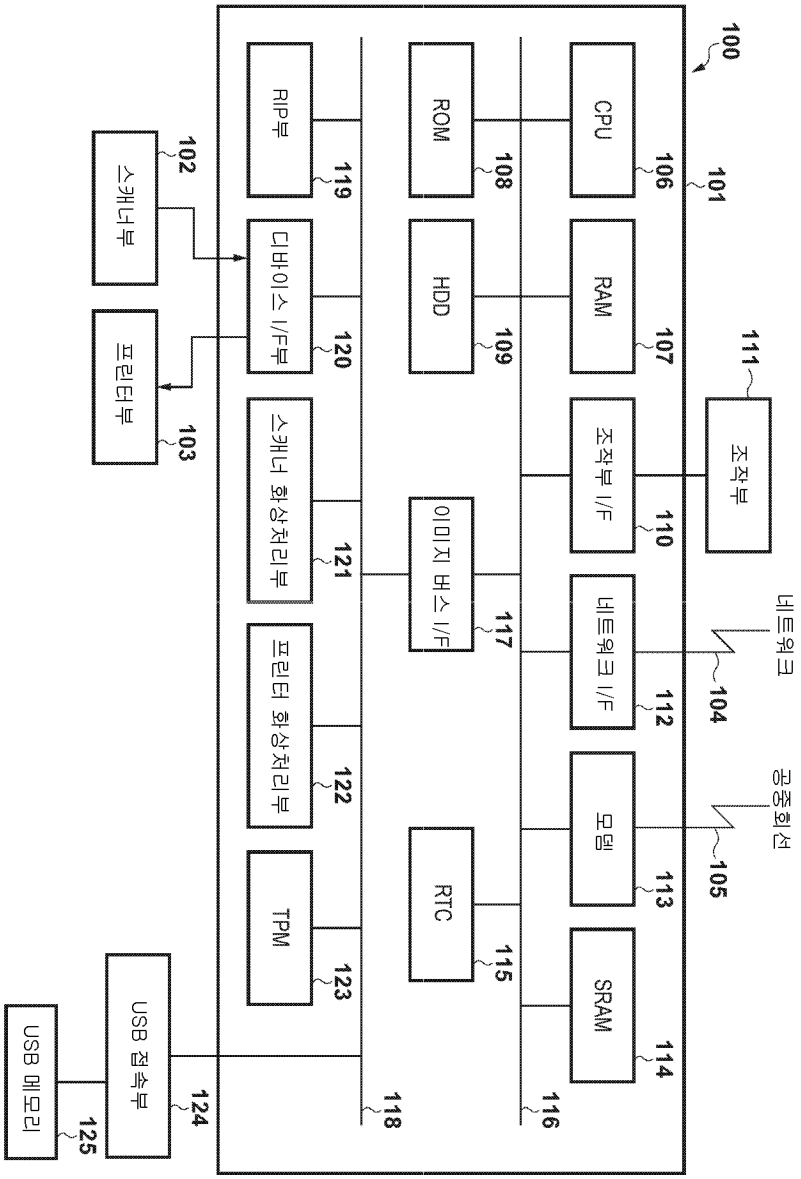
[0096] 본 발명의 실시형태는, 본 발명의 전술한 실시형태(들)의 1개 이상의 기능을 수행하기 위해 기억매체('비일시적인 컴퓨터 판독가능한 기억매체'로서 더 상세히 언급해도 된다)에 기록된 컴퓨터 실행가능한 명령(예를 들어, 1개 이상의 프로그램)을 판독하여 실행하거나 및/또는 전술한 실시예(들)의 1개 이상의 기능을 수행하는 1개 이상의 회로(예를 들어, 주문형 반도체 회로(ASIC)를 포함하는 시스템 또는 장치의 컴퓨터나, 예를 들면, 전술한 실시형태(들)의 1개 이상의 기능을 수행하기 위해 기억매체로부터 컴퓨터 실행가능한 명령을 판독하여 실행함으로써, 시스템 또는 장치의 컴퓨터에 의해 수행되는 방법에 의해 구현될 수도 있다. 컴퓨터는, 1개 이상의 중앙처리장치(CPU), 마이크로 처리장치(MPU) 또는 기타 회로를 구비하고, 별개의 컴퓨터들의 네트워크 또는 별개의 컴퓨터 프로세서들을 구비해도 된다. 컴퓨터 실행가능한 명령은, 예를 들어, 기억매체의 네트워크로부터 컴퓨터로 주어져도 된다. 기록매체는, 예를 들면, 1개 이상의 하드디스크, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 분산 컴퓨팅 시스템의 스토리지, 광 디스크(콤팩트 디스크(CD), 디지털 다기능 디스크(DVD), 또는 블루레이 디스크(BD)™ 등), 플래시 메모리소자, 메모리 카드 등을 구비해도 된다.

[0097] 본 발명은, 상기한 실시형태의 1개 이상의 기능을 실현하는 프로그램을, 네트워크 또는 기억매체를 개입하여 시스템 혹은 장치에 공급하고, 그 시스템 혹은 장치의 컴퓨터에 있어서 1개 이상의 프로세서가 프로그램을 읽어 실행하는 처리에서도 실행가능하다. 또한, 1개 이상의 기능을 실현하는 회로(예를 들어, ASIC)에 의해서도 실행가능하다.

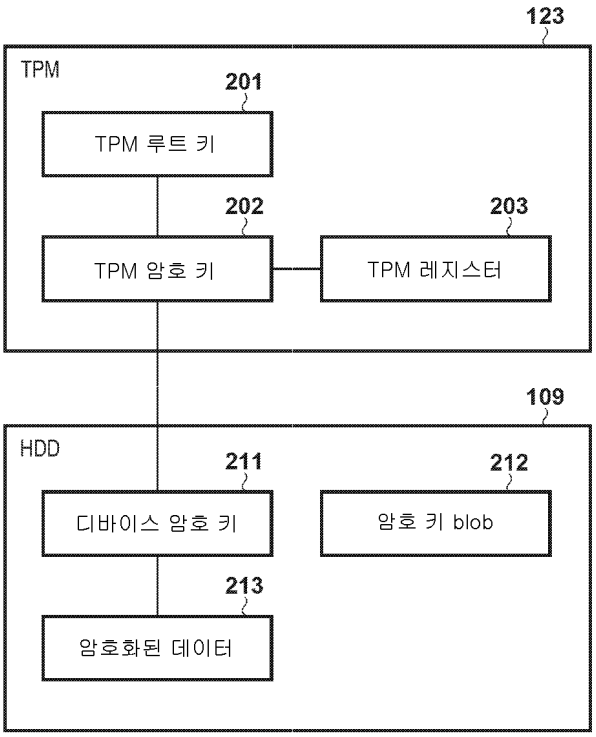
[0098] 예시적인 실시형태들을 참조하여 본 발명을 설명하였지만, 본 발명이 이러한 실시형태에 한정되지 않는다는 것은 자명하다. 이하의 청구범위의 보호범위는 가장 넓게 해석되어 모든 변형, 동등물 구조 및 기능을 포괄하여야 한다.

도면

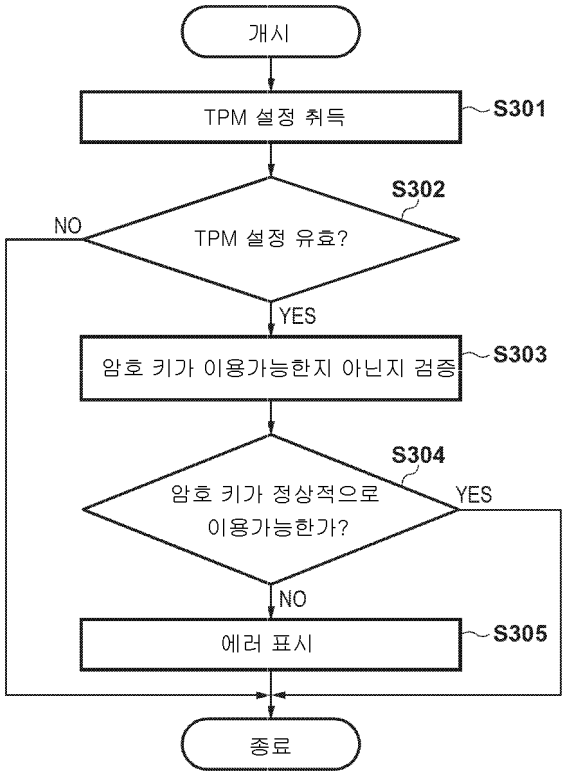
도면1


100
101
CPU
106
RAM
107
조작부 I/F
110
네트워크 I/F
112
모뎀
113
SRAM
114
조작부
111
네트워크
104
공중회선
105
ROM
108
HDD
109
이미지 버스 I/F
117
RTC
115
116
RIP부
119
디바이스 I/F부
120
스캐너 화상처리부
121
프린터 화상처리부
122
TPM
123
118
스캐너부
102
프린터부
103
USB 접속부
124
USB 메모리
125

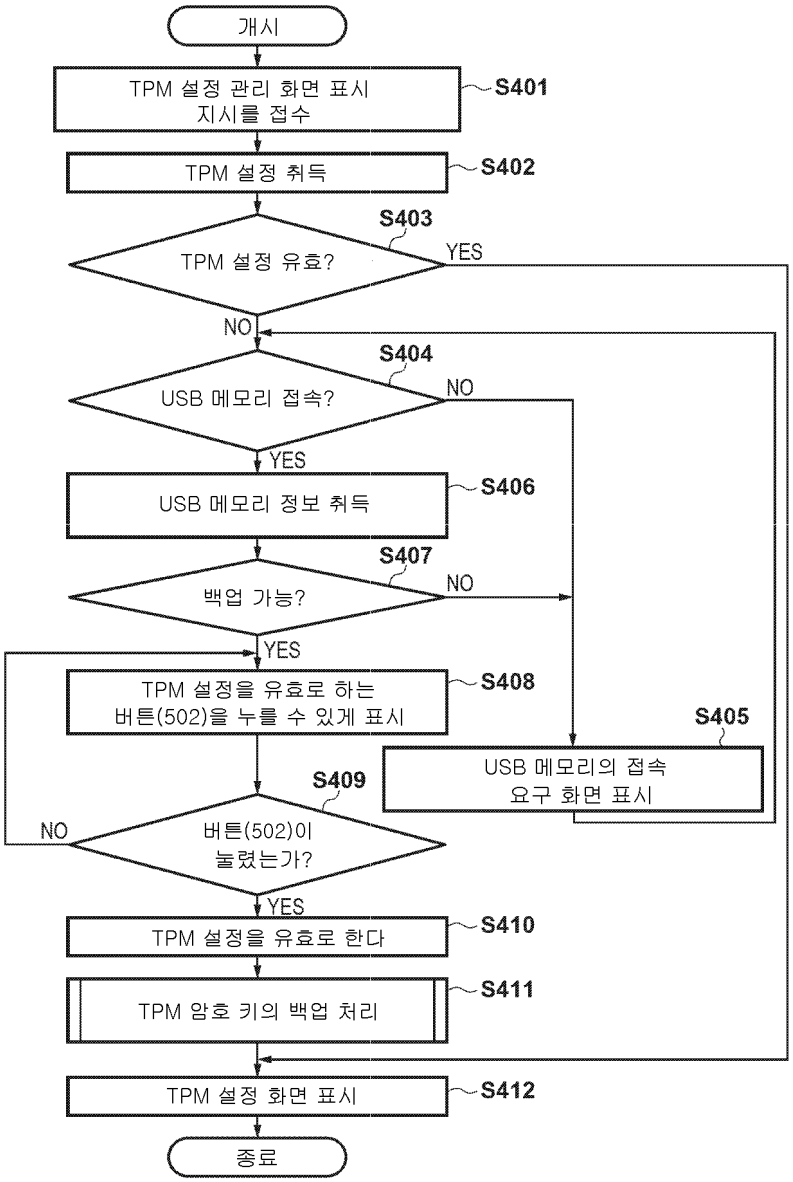
도면2


123
TPM
201
TPM 루트 키
202
203
TPM 암호 키
TPM 레지스터
109
HDD
211
212
디바이스 암호 키
암호 키 blob
213
암호화된 데이터

도면3

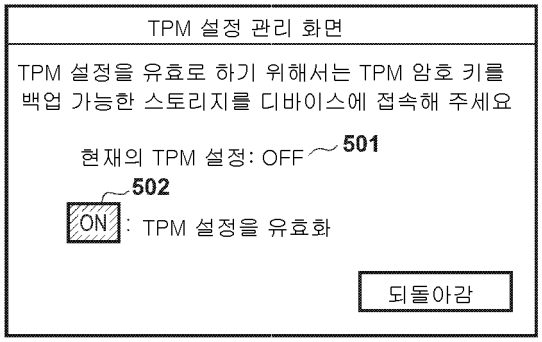

개시
TPM 설정 취득
S301
S302
NO
TPM 설정 유효?
YES
암호 키가 이용가능한지 아닌지 검증
S303
S304
암호 키가 정상적으로
이용가능한가?
YES
NO
에러 표시
S305
종료

도면4

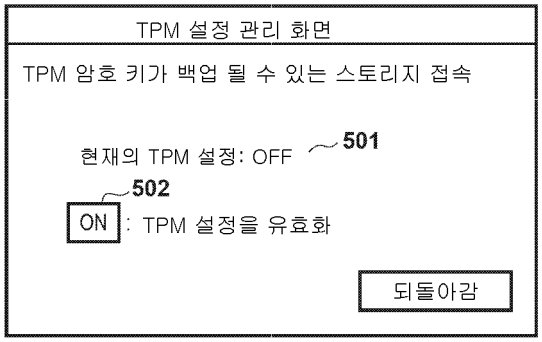

개시
TPM 설정 관리 화면 표시 지시를 접수
S401
TPM 설정 취득
S402
S403
TPM 설정 유효?
YES
NO
S404
USB 메모리 접속?
NO
YES
USB 메모리 정보 취득
S406
S407
백업 가능?
NO
YES
TPM 설정을 유효로 하는 버튼(502)을 누를 수 있게 표시
S408
S405
USB 메모리의 접속 요구 화면 표시
S409
NO
버튼(502)이 눌렸는가?
YES
TPM 설정을 유효로 한다
S410
TPM 암호 키의 백업 처리
S411
TPM 설정 화면 표시
S412
종료

도면5

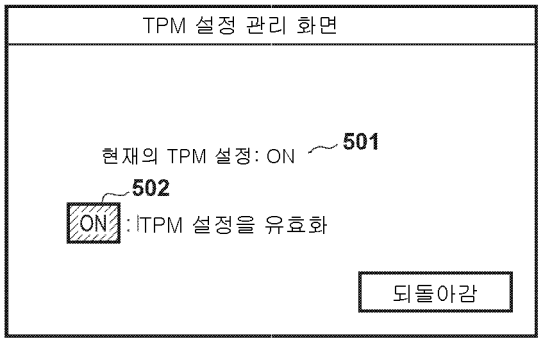
(a)


TPM 설정 관리 화면
TPM 설정을 유효로 하기 위해서는 TPM 암호 키를 백업 가능한 스토리지를 디바이스에 접속해 주세요
현재의 TPM 설정: OFF
501
502
ON
: TPM 설정을 유효화
되돌아감

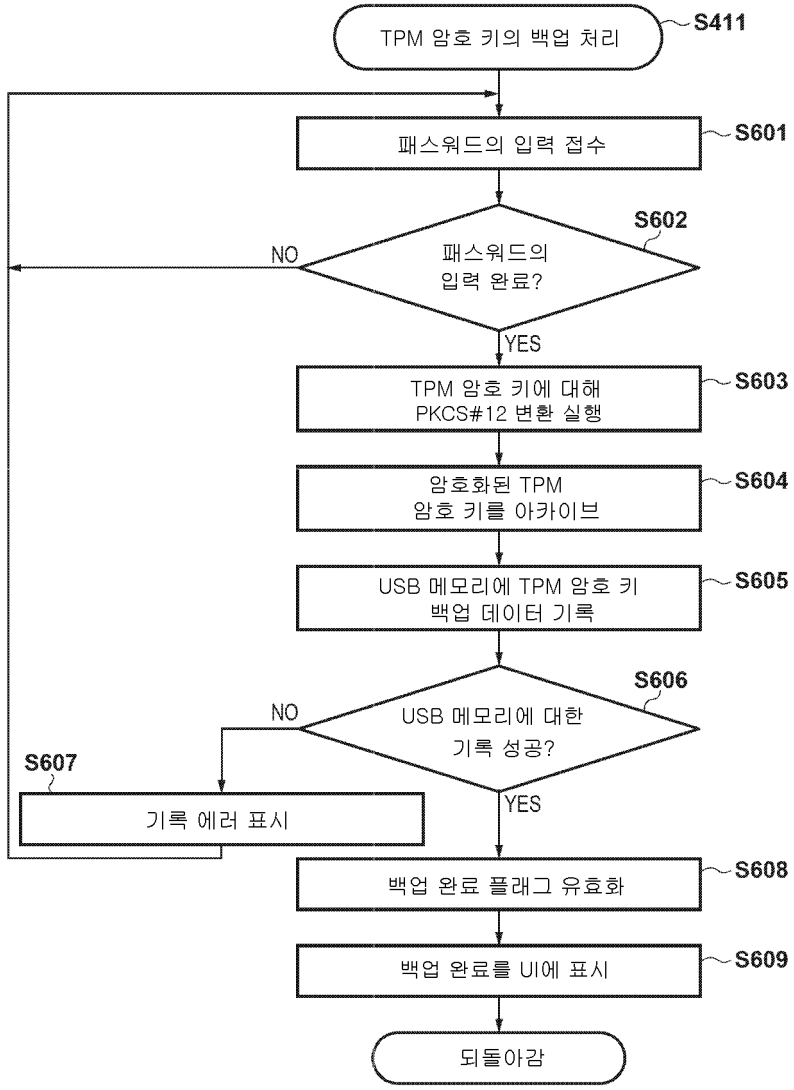
(b)


TPM 설정 관리 화면
TPM 암호 키가 백업 될 수 있는 스토리지 접속
현재의 TPM 설정: OFF
501
502
ON
: TPM 설정을 유효화
되돌아감

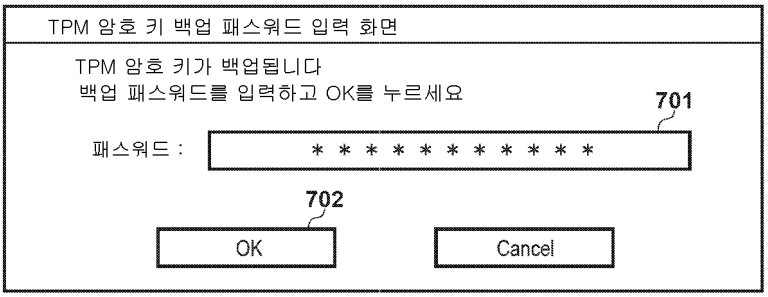
(c)


TPM 설정 관리 화면
현재의 TPM 설정: ON
501
502
ON
: TPM 설정을 유효화
되돌아감

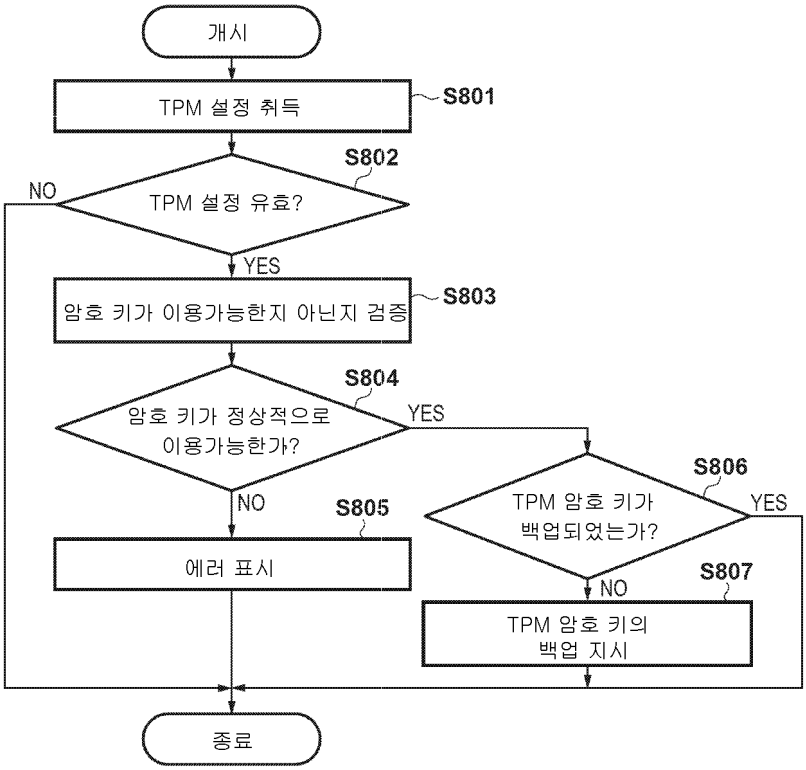
도면6


TPM 암호 키의 백업 처리
S411
패스워드의 입력 접수
S601
S602
NO
패스워드의
입력 완료?
YES
TPM 암호 키에 대해
PKCS#12 변환 실행
S603
암호화된 TPM
암호 키를 아카이브
S604
USB 메모리에 TPM 암호 키
백업 데이터 기록
S605
S606
NO
USB 메모리에 대한
기록 성공?
S607
기록 에러 표시
YES
백업 완료 플래그 유효화
S608
백업 완료를 UI에 표시
S609
되돌아감

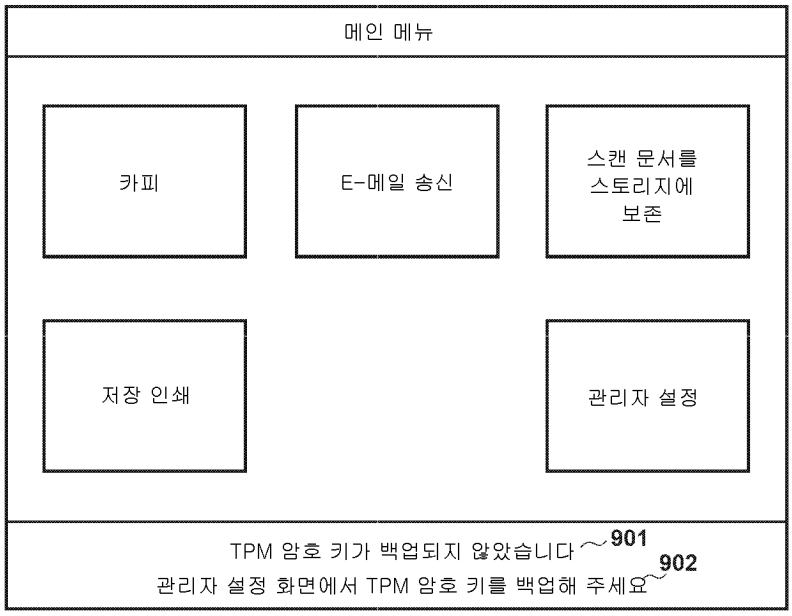
도면7


TPM 암호 키 백업 패스워드 입력 화면
TPM 암호 키가 백업됩니다
백업 패스워드를 입력하고 OK를 누르세요
701
패스워드 :
* * * * * * * * * * *
702
OK
Cancel

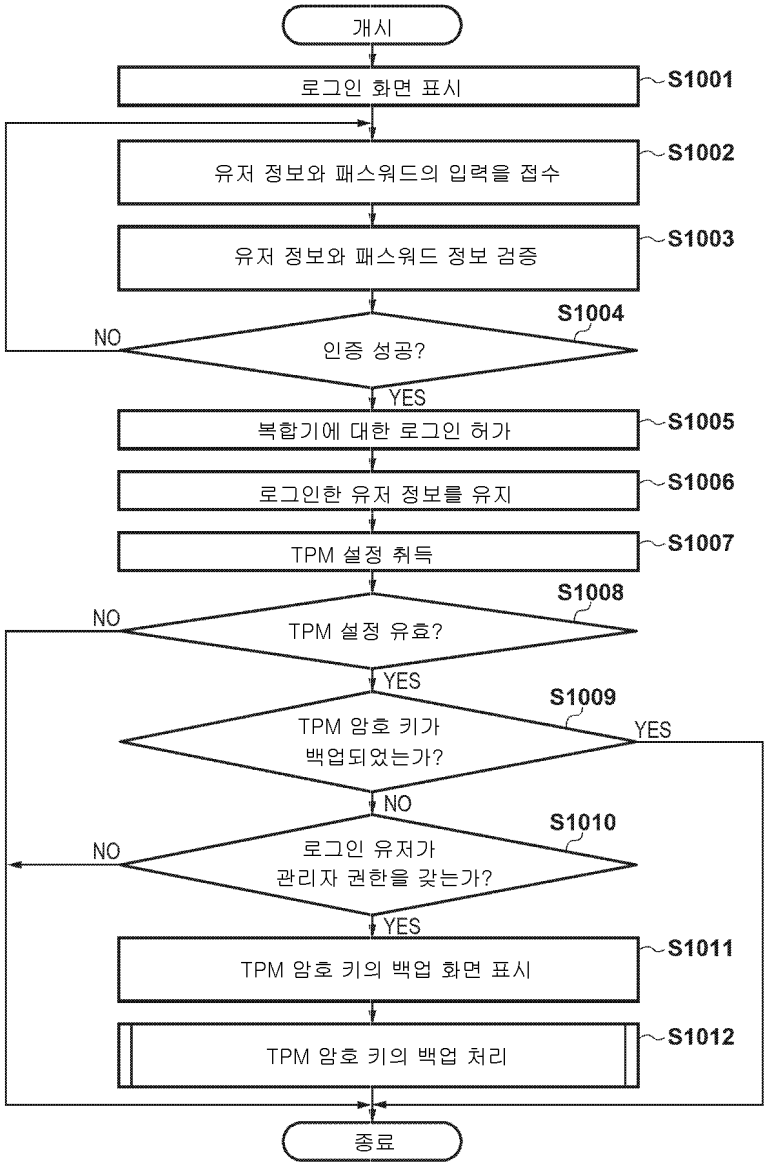
도면8


개시
TPM 설정 취득
S801
S802
TPM 설정 유효?
NO
YES
암호 키가 이용가능한지 아닌지 검증
S803
S804
암호 키가 정상적으로 이용가능한가?
YES
NO
S805
에러 표시
S806
TPM 암호 키가 백업되었는가?
YES
NO
S807
TPM 암호 키의 백업 지시
종료

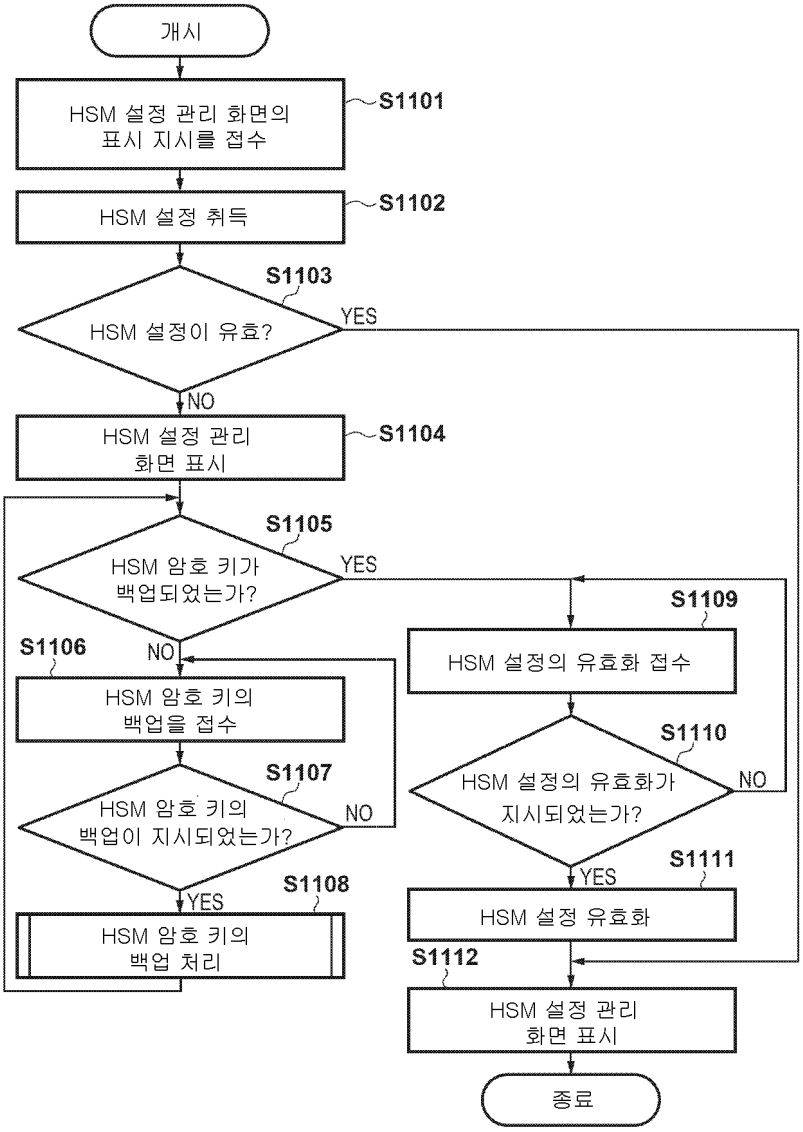
도면9


메인 메뉴
카피
E-메일 송신
스캔 문서를 스토리지에 보존
저장 인쇄
관리자 설정
TPM 암호 키가 백업되지 않았습니다
901
관리자 설정 화면에서 TPM 암호 키를 백업해 주세요
902

도면10

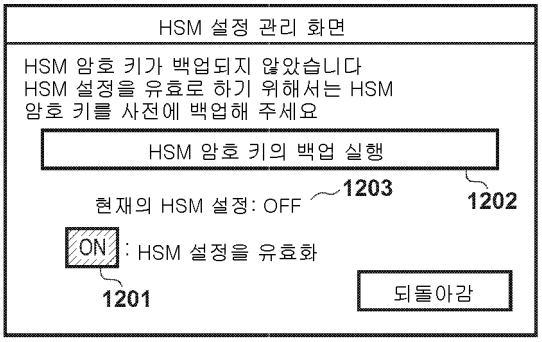

개시
로그인 화면 표시
S1001
유저 정보와 패스워드의 입력을 접수
S1002
유저 정보와 패스워드 정보 검증
S1003
인증 성공?
S1004
NO
YES
복합기에 대한 로그인 허가
S1005
로그인한 유저 정보를 유지
S1006
TPM 설정 취득
S1007
TPM 설정 유효?
S1008
NO
YES
TPM 암호 키가
백업되었는가?
S1009
YES
NO
로그인 유저가
관리자 권한을 갖는가?
S1010
NO
YES
TPM 암호 키의 백업 화면 표시
S1011
TPM 암호 키의 백업 처리
S1012
종료

도면11

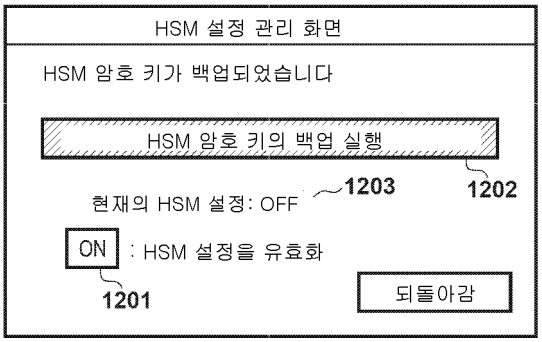

개시
HSM 설정 관리 화면의 표시 지시를 접수
S1101
HSM 설정 취득
S1102
S1103
HSM 설정이 유효?
YES
NO
HSM 설정 관리 화면 표시
S1104
S1105
HSM 암호 키가 백업되었는가?
YES
NO
S1106
HSM 암호 키의 백업을 접수
S1107
HSM 암호 키의 백업이 지시되었는가?
NO
YES
S1108
HSM 암호 키의 백업 처리
S1109
HSM 설정의 유효화 접수
S1110
HSM 설정의 유효화가 지시되었는가?
NO
YES
S1111
HSM 설정 유효화
S1112
HSM 설정 관리 화면 표시
종료

도면12

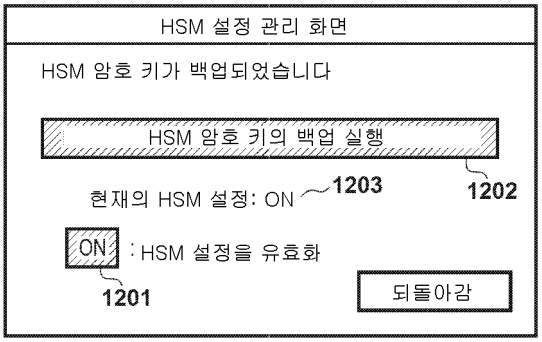
(a)


HSM 설정 관리 화면
HSM 암호 키가 백업되지 않았습니다
HSM 설정을 유효로 하기 위해서는 HSM
암호 키를 사전에 백업해 주세요
HSM 암호 키의 백업 실행
1202
현재의 HSM 설정: OFF
1203
ON
: HSM 설정을 유효화
1201
되돌아감

(b)


HSM 설정 관리 화면
HSM 암호 키가 백업되었습니다
HSM 암호 키의 백업 실행
1202
현재의 HSM 설정: OFF
1203
ON
: HSM 설정을 유효화
1201
되돌아감

(c)


HSM 설정 관리 화면
HSM 암호 키가 백업되었습니다
HSM 암호 키의 백업 실행
1202
현재의 HSM 설정: ON
1203
ON
: HSM 설정을 유효화
1201
되돌아감