(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 15/00

(11) 공개번호 특1999-0058372
(43) 공개일자 1999년07월15일

(21) 출원번호 10-1997-0078472
(22) 출원일자 1997년12월30일

(71) 출원인 삼성전자 주식회사 윤종용
경기도 수원시 팔달구 매탄3동 416
(72) 발명자 김영식
서울특별시 종로구 명륜동2가 4번지
장화선
서울특별시 서초구 서초3동 1468-1
(74) 대리인 감동훈

심사청구 : 있음

(54) 스마트 카드를 이용한 컴퓨터의 보안 방법

요약

본 발명은 보안 기능이 뛰어난 스마트 카드를 이용함으로써 데이터를 보호하고 사용자의 접근을 제한할 수 있도록 한 스마트 카드를 이용한 컴퓨터의 보안 방법을 제공함에 그 목적이 있다. 전술한 목적을 달성하기 위한 본 발명의 스마트 카드를 이용한 컴퓨터의 보안 방법은 컴퓨터 시스템 전체에 전원을 인가받은 후 상기 시스템의 기본 입출력 장치에서 자기 진단을 수행하여 상기 시스템에 구비되어 있는 장치들을 점검하여 상기 시스템의 오류 여부를 확인하는 단계; 상기 시스템에 스마트 카드가 장착되었는 지를 판단하고 상기 스마트 카드가 장착 되었을 경우에는 상기 장착된 스마트 카드가 상기 컴퓨터에 사용될 적당한 카드인 지를 판별하는 단계; 상기 판별결과 상기 스마트 카드가 사용 가능한 것일 경우에는 암호를 입력받아 상기 입력받은 암호가 기설정된 암호와 일치하는 지를 판단하는 단계; 상기 판단결과 상기 입력받은 암호와 상기 기설정된 암호가 일치하는 경우에는 상기 스마트 카드에 저장되어 있는 컴퓨터의 환경 설정 데이터를 읽어들여 상기 컴퓨터 시스템의 메모리에 저장된 컴퓨터의 환경 설정 데이터와 일치하는 지를 판단하는 단계; 및 상기 스마트 카드에서 읽어들인 컴퓨터의 환경 설정 데이터와 상기 컴퓨터 시스템의 메모리에 저장된 컴퓨터의 환경 설정 데이터가 일치하는 경우에는 상기 컴퓨터 시스템의 정상적인 시동 과정을 수행하는 단계를 구비하여 이루어진다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 본 발명의 보안 방법이 적용되는 스마트 카드 단말기 인터페이스 시스템의 구성을 개략적으로 보인 시스템 블록도,

도 2는 본 발명의 스마트 카드를 이용한 컴퓨터의 보안 방법을 설명하기 위한 플로우챠트이다.

*** 도면의 주요 부분에 대한 부호의 설명 ***

10. 스마트 카드 소켓부, 20. 스마트 카드 인터페이스부,
30. 마이콤, 40. 메모리부,
50. 데이터 송수신부, 60. 제어부,
70. 비교기, 80. 버퍼부,
90. 컴퓨터 슬롯

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 스마트 카드를 이용한 컴퓨터의 보안 방법에 관한 것으로서, 더욱 상세하게는 보안 기능이 뛰

어난 스마트 카드를 이용함으로써 데이터를 보호하고 사용자의 접근을 제한할 수 있도록 한 스마트 카드를 이용한 컴퓨터의 보안 방법에 관한 것이다.

일반적으로 개인용 컴퓨터(Presonal Computer;이하, PC라 한다), 팜탑 컴퓨터(Palmtop Computer), 노트북 컴퓨터(Notebook Computer) 등과 같은 시스템들은 시스템에 저장되어 정보의 유출을 방지하고자 다른 사용자들이 쉽게 접근할 수 없게 하기 위한 여러 가지 방안이 강구되고 있다.

종래의 컴퓨터는 컴퓨터에 내장되어 있는 금속 산화막 반도체(complementary metal oxide semiconductor;이하, CMOS라 한다) 메모리에 사용자의 암호를 부여받아 저장하고 있다가 컴퓨터 가동시 사용자로부터 암호를 입력받아 CMOS에 저장된 암호값을 비교하여 맞으면 컴퓨터를 가동하도록 하고, 사용자가 입력한 암호와 CMOS 메모리에 저장된 값이 맞지 않으면 컴퓨터의 가동이 더 이상 진행되지 않도록 하였다.

그러나 전술한 바와 같이 COMS 메모리를 사용하여 보안을 행할 경우에는 컴퓨터의 구조상 암호는 항상 특정한 위치와 주소를 가지고 있어서, 누구나가 침범하여 조작 및 변경이 가능하다. 또한 CMOS 메모리에 연결된 전원을 차단함으로써 CMOS 메모리에 저장된 암호를 삭제할 수 있다.

따라서, 암호를 삭제한 후에는 더 이상 사용자의 암호가 유효하지 않으므로 누구나가 접근이 가능하여 실질적으로 컴퓨터의 보안이 이루어질 수 없어 컴퓨터의 도난 사고가 빈번하게 일어나고 컴퓨터에 저장된 데이터의 유출 및 손실이 발생하는 문제점이 있다.

특히, 이동이 간편하고 많은 량의 데이터를 생성, 편집 및 저장이 가능한 노트북 컴퓨터의 경우 귀중한 정보의 손실과 아울러 물질적 손실이 많아지고 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 전술한 문제점을 해결하기 위해 안출된 것으로서, 보안 기능이 뛰어난 스마트 카드를 이용함으로써 데이터를 보호하고 사용자의 접근을 제한할 수 있도록 한 스마트 카드를 이용한 컴퓨터의 보안 방법을 제공함에 그 목적이 있다.

전술한 목적을 달성하기 위한 본 발명의 스마트 카드를 이용한 컴퓨터의 보안 방법은 컴퓨터 시스템 전체에 전원을 인가받은 후 상기 시스템의 기본 입출력 장치에서 자기 진단을 수행하여 상기 시스템에 구비되어 있는 장치들을 점검하여 상기 시스템의 오류 여부를 확인하는 단계; 상기 시스템에 스마트 카드가 장착되었는 지를 판단하고 상기 스마트 카드가 장착 되었을 경우에는 상기 장착된 스마트 카드가 상기 컴퓨터에 사용될 적당한 카드인 지를 판별하는 단계; 상기 판별결과 상기 스마트 카드가 사용 가능한 것일 경우에는 암호를 입력받아 상기 입력받은 암호가 기설정된 암호와 일치하는 지를 판단하는 단계; 상기 판단결과 상기 입력받은 암호와 상기 기설정된 암호가 일치하는 경우에는 상기 스마트 카드에 저장되어 있는 컴퓨터의 환경 설정 데이터를 읽어들여 상기 컴퓨터 시스템의 메모리에 저장된 컴퓨터의 환경 설정 데이터와 일치하는 지를 판단하는 단계; 및 상기 스마트 카드에서 읽어들인 컴퓨터의 환경 설정 데이터와 상기 컴퓨터 시스템의 메모리에 저장된 컴퓨터의 환경 설정 데이터가 일치하는 경우에는 상기 컴퓨터 시스템의 정상적인 시동 과정을 수행하는 단계를 구비하여 이루어진다.

발명의 구성 및 작용

이하에서는 첨부한 도면을 참조하여 본 발명의 양호한 실시예에 따른 스마트 카드를 이용한 컴퓨터의 보안 방법에 대해서 상세하게 설명한다.

도 1은 본 발명의 보안 방법이 적용되는 스마트 카드 단말기 인터페이스 시스템의 구성을 개략적으로 보인 시스템 블록도이다. 이 도면에 도시하는 바와 같이, 본 발명이 적용되는 스마트 카드 단말기 인터페이스 시스템은 스마트 카드에 장착된 칩상의 접점을 스마트 카드 단말기와 연결하며 스마트 카드의 삽입을 위한 삽입구를 구비한 스마트 카드 소켓부(10), ISO 규격에 따라 스마트 카드에서 필요로 하는 신호를 소정의 레벨과 타이밍을 갖는 신호로 변환하는 스마트 카드 인터페이스부(20), 인터페이스 장치의 전체 제어를 수행하고 필요에 따라 연산을 행하는 마이콤(30), 마이콤(30)으로부터 보내지는 데이터를 저장하는 메모리부(40), 컴퓨터에서 보내지는 데이터를 마이콤(30)으로 보내고 마이콤(30)에서 보내지는 데이터를 컴퓨터쪽으로 보내는 데이터 송수신부(50), 시스템 전체를 제어하는 제어부(60), 인터페이스 장치를 제어하기 위한 어드레스를 컴퓨터로부터 인가받아 제어부(60)로 보내는 비교기(70), 데이터의 송수신을 나타내는 컴퓨터 슬롯의 어드레스 최하위 비트(SA0), I/O 읽기 신호(IOR), I/O 쓰기 신호(IOW)를 마이콤(30)으로 전달해 주는 버퍼부(80) 및 컴퓨터 본체 내부에 있는 것으로 스마트 카드를 데이터 통로로 접속하기 위한 삽입구를 구비한 컴퓨터 슬롯(90)를 구비하여 이루어진다.

전술한 구성의 마이콤(30)은 스마트 카드 소켓부(10)로부터 스마트 카드의 유무를 읽고 스마트 카드 인터페이스부(20)로 Vcc 인가 시점 제어, LED 제어, 리세트 신호 제어 신호를 인가하고 결함상태를 읽기도 한다. 또한 스마트 카드와 인터페이스 장치 간의 인증을 위한 계산과 컴퓨터 시스템에서 명령을 인가 받아 해석한 후 처리하여 결과를 컴퓨터로 돌려주는 기능도 수행한다.

전술한 스마트 카드는 카드에 바코드나 필름막 대신에 IC (Integrated Cir- cuit;집적회로)를 집어넣은 것으로써, 이는 크레디트 카드 사이즈에 중앙처리장치(CPU)와 8~32kbyte의 IC 메모리를 넣은 IC 카드, 수mm정도 두께의 카드에 대용량 LSI(Large Scale Integration;대규모 집적회로)메모리만을 넣은 IC 메모리 카드 및 외부와 무선으로 데이터를 송수신할 수 있는 와이어레스(wireless) 카드 등의 세 가지로 크게 분류될 수 있다.

이러한 스마트 카드 중에서 마이크로 프로세서와 메모리를 내장하는 카드는 카드 내에서 연산하는 능력이 있기 때문에 암호 번호의 확인이나 암호 처리 등이 카드 내에서 가능하다. 한편, 이러한 스마트 카드는 은행의 캐시(cash) 카드 등에 이용하면 보안 향상과 함께 데이터를 짧은 부호로 보내서, 데이터 전송량을 절감할 수 있는 이점이 있으며, 스마트 카드라는 명칭 이외에 IC 카드, 칩 카드(chip card), 인텔리젼트 카드 등으로 불려진다.

도 2는 본 발명의 스마트 카드를 이용한 컴퓨터의 보안 방법을 설명하기 위한 플로우챠트이다. 이 도면에 도시하는 보와 같이, 먼저 단계(S10)에서 전원을 인가받은 후 단계(S12)로 진행하여 컴퓨터의 기본 입출력 장치에서 자기 진단을 수행하여 컴퓨터에 구비되어 있는 중앙 처리부, 메모리 및 각종 입출력 장치들을 점검하여 시스템의 오류 여부를 확인한다. 이후 단계(S14)에서는 스마트 카드 소켓부(10)에 스마트 카드가 장착되었는 지를 판단한다. 단계(S14)의 판단결과 스마트 카드가 장착되어 있지 않을 경우에는 단계(S15)로 진행하여 시스템 오류 메시지를 출력하고 동작을 중지시키고, 스마트 카드가 장착되었을 경우에는 단계(S16)로 진행하여 장착된 스마트 카드가 사용 가능한 것인 지를 판별하기 위한 스마트 카드의 고유 번호를 읽어들인다. 다음 단계(S18)에서는 단계(S16)에서 읽어들인 스마트 카드의 고유 번호가 유효한 것인 지를 판단한다. 단계(S18)의 판단결과 단계(S16)에서 읽어들인 고유 번호가 유효한 것이 아닐 경우는 스마트 카드 소켓부(10)에 장착된 스마트 카드가 컴퓨터에 사용될 적당한 스마트 카드가 아니므로 단계(S19)로 진행하여 적당한 스마트 카드가 아님을 알리는 오류 메시지를 출력하고 단계(S10)로 진행하여 다시 전원을 인가받아 자기 진단을 수행한다. 단계(S16)에서 읽어들인 고유 번호가 유효한 것일 경우에는 단계(S20)로 진행하여 스마트 카드의 사용자가 확실한 지를 인증하기 위하여 사용자로부터 암호를 입력받는다. 다음 단계(S22)에서는 단계(S20)에서 입력받은 암호가 기설정된 값과 일치하는 지를 판단한다. 단계(S22)의 판단결과 암호가 일치하지 않을 경우에는 단계(S23)로 진행하여 컴퓨터의 가동이 더 이상 진행되지 않도록 컴퓨터의 동작을 중지시킨다. 단계(S22)의 판단결과 암호가 일치하여 스마트 카드의 사용자가 확실하다는 인증 절차가 완료되면 CMOS 메모리에 접근할 수 있도록 하며 단계(S24)로 진행하여 스마트 카드에 저장되어 있는 컴퓨터의 환경 설정 데이터를 읽어들인다. 이때 CMOS 메모리에는 컴퓨터의 사용자 인증에 필요한 응용 프로그램과 암·복호 알고리즘이 추가되어 있어야 한다. 다음 단계(S26)에서는 단계(S24)에서 읽어들인 스마트 카드에 저장되어 있는 컴퓨터의 환경 설정 데이터와 컴퓨터에 있는 CMOS 메모리에 저장된 컴퓨터의 환경 설정 데이터가 일치하는 지를 판단한다. 단계(S26)의 판단결과 단계(S24)에서 읽어들인 환경 설정 데이터와 CMOS 메모리에 저장된 컴퓨터의 환경 설정 데이터가 일치하지 않을 경우에는 단계(S16)로 진행하여 다시 스마트 카드 및 사용자의 인증 절차를 거쳐 CMOS 메모리에 저장된 환경을 변경할 수 있는 권한을 부여하고, 스마트 카드에서 읽어들인 내용과 CMOS 메모리에 저장된 컴퓨터의 환경 설정 데이터와 스마트 카드에 저장된 내용이 일치할 경우에는 단계(S28)로 진행하여 컴퓨터 기동 절차를 수행하게 한다.

컴퓨터의 기동 수행시 스마트 카드에 저장된 개인의 고유의 킷값을 이용하여 하드 디스크의 데이터를 암·복호화하여 스마트 카드를 이용하지 않고 접근한 타인에게 정보가 유출되는 것을 방지할 수 있으며, 컴퓨터에 장착된 사용자의 스마트 카드는 언제든지 탈착이 가능하여 사용자가 본인의 컴퓨터에 장착된 스마트 카드를 타인이 사용하지 못하게 하거나 사용자가 이동을 할 경우 또는 도난의 염려가 있을 경우에는 컴퓨터에 장착된 스마트 카드를 빼내어 사용자가 소지하고 다니면 정보의 유출이나 시스템의 도난을 효과적으로 방지할 수 있다.

본 발명의 스마트 카드를 이용한 컴퓨터의 보안 방법은 전술한 실시예에 국한되지 않고 본 발명의 기술사상이 허용하는 범위 내에서 다양하게 변형하여 실시할 수 있다. 예를 들어, 제품 생산 시작전 단계에서 일련의 번호를 부여받고 생산 공정 각 진행 단계마다 진행 여부 및 결과를 스마트 카드에 기록한 다음 생산 완료 단계에서 스마트 카드에 저장된 고유 번호와 각 생산 공정에서 나온 결과를 읽어 그 결과를 애프터 서비스 시스템에 데이터 베이스화하여 관리할 수 있도록 한다.

발명의 효과

이상에서 설명한 바와 같은 본 발명의 스마트 카드를 이용한 컴퓨터의 보안 방법에 따르면, 보안성이 뛰어난 스마트 카드를 이용하여 사용자 인증 절차를 거쳐 컴퓨터의 가동 허락을 얻음으로써 정보의 유출을 차단하고 사용자의 접근을 제한할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1

컴퓨터 시스템 전체에 전원을 인가받은 후 상기 시스템의 기본 입출력 장치에서 자기 진단을 수행하여 상기 시스템에 구비되어 있는 장치들을 점검하여 상기 시스템의 오류 여부를 확인하는 단계;

상기 시스템에 스마트 카드가 장착되었는 지를 판단하고 상기 스마트 카드가 장착 되었을 경우에는 상기 장착된 스마트 카드가 상기 컴퓨터에 사용될 적당한 카드인 지를 판별하는 단계;

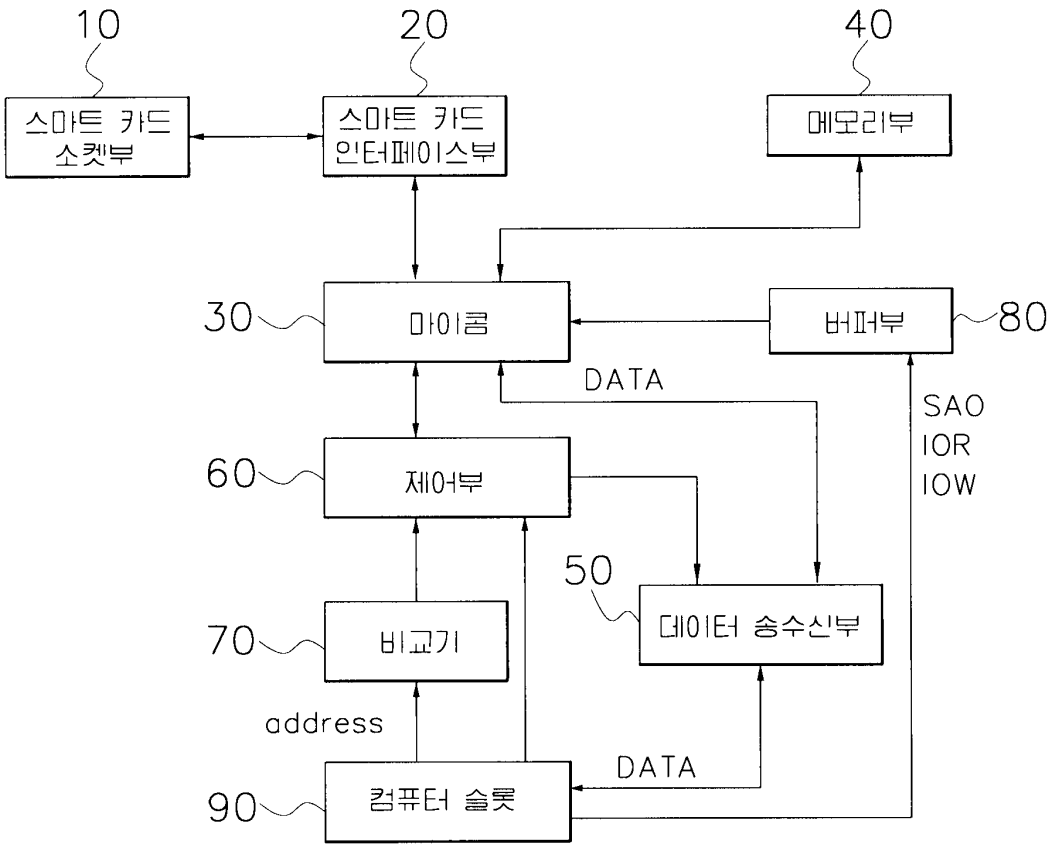
상기 판별결과 상기 스마트 카드가 사용 가능한 것일 경우에는 암호를 입력받아 상기 입력받은 암호가 기설정된 암호와 일치하는 지를 판단하는 단계;

상기 판단결과 상기 입력받은 암호와 상기 기설정된 암호가 일치하는 경우에는 상기 스마트 카드에 저장되어 있는 컴퓨터의 환경 설정 데이터를 읽어들여 상기 컴퓨터 시스템의 메모리에 저장된 컴퓨터의 환경 설정 데이터와 일치하는 지를 판단하는 단계; 및

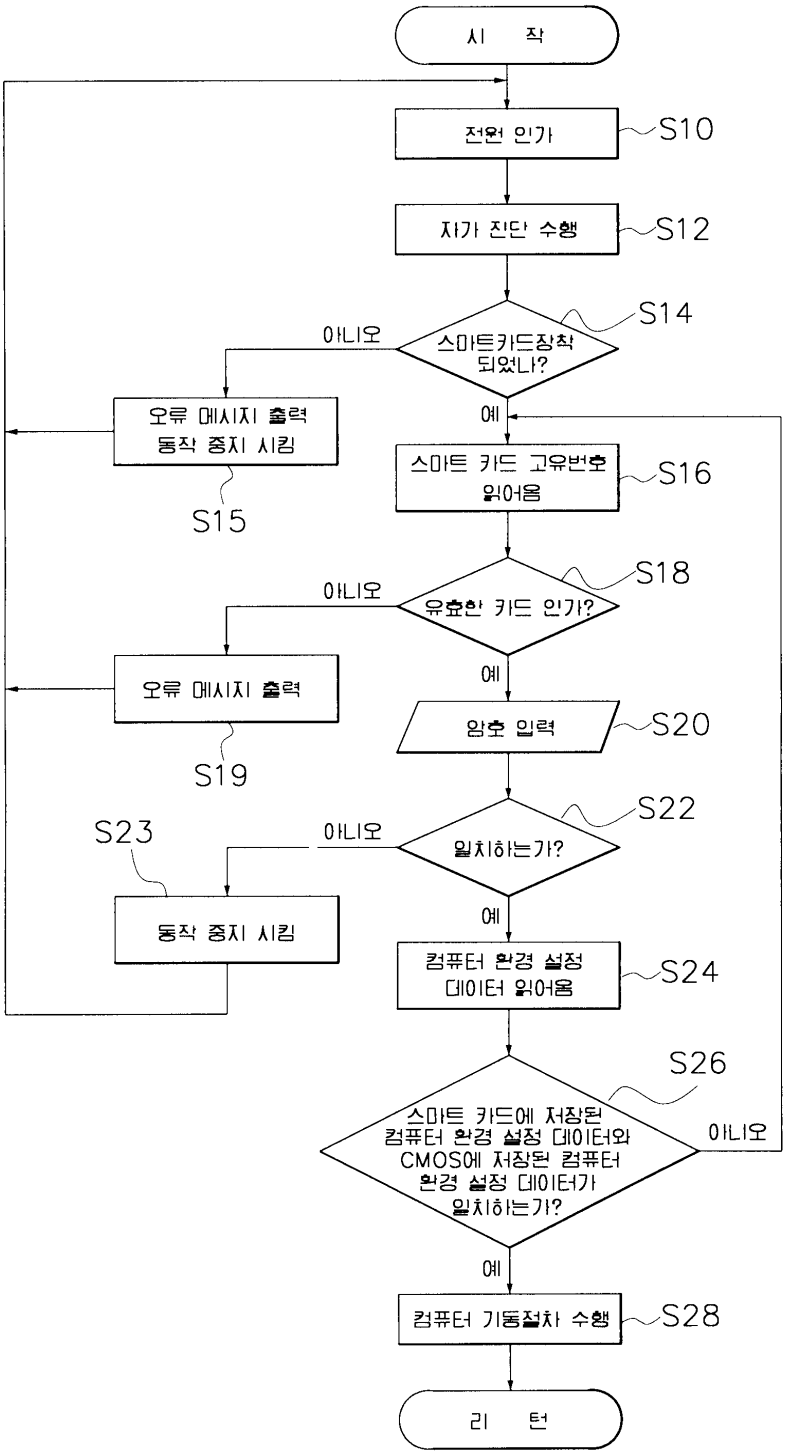
상기 스마트 카드에서 읽어들인 컴퓨터의 환경 설정 데이터와 상기 컴퓨터 시스템의 메모리에 저장된 컴퓨터의 환경 설정 데이터가 일치하는 경우에는 상기 컴퓨터 시스템의 정상적인 시동 과정을 수행하는 단계를 구비하여 이루어지는 스마트 카드를 이용한 컴퓨터의 보안 방법.

도면

도면1


10
스마트 카드 소켓부
20
스마트 카드 인터페이스부
40
메모리부
30
마이콤
버퍼부
80
DATA
SAO
IOR
IOW
60
제어부
50
데이터 송수신부
70
비교기
address
DATA
90
컴퓨터 슬롯

도면2


시 작
전원 인가
S10
자가 진단 수행
S12
스마트카드장착 되었나?
S14
아니오
예
오류 메시지 출력 동작 중지 시킴
S15
스마트 카드 고유번호 읽어옴
S16
유효한 카드 인가?
S18
아니오
예
오류 메시지 출력
S19
암호 입력
S20
일치하는가?
S22
S23
아니오
예
동작 중지 시킴
컴퓨터 환경 설정 데이터 읽어옴
S24
스마트 카드에 저장된 컴퓨터 환경 설정 데이터와 CMOS에 저장된 컴퓨터 환경 설정 데이터가 일치하는가?
S26
아니오
예
컴퓨터 기동절차 수행
S28
리 턴