



등록특허 10-2312087



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년10월14일
(11) 등록번호 10-2312087
(24) 등록일자 2021년10월06일

- (51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01) *G06F 21/45* (2013.01)
G06K 9/00 (2006.01) *H04L 9/32* (2006.01)
- (52) CPC특허분류
G06F 21/32 (2013.01)
G06F 21/45 (2013.01)
- (21) 출원번호 10-2018-0074532
- (22) 출원일자 2018년06월28일
심사청구일자 2019년12월03일
- (65) 공개번호 10-2019-0002351
- (43) 공개일자 2019년01월08일
- (30) 우선권주장
JP-P-2017-128048 2017년06월29일 일본(JP)
- (56) 선행기술조사문헌
US20070168674 A1*

*는 심사관에 의하여 인용된 문헌

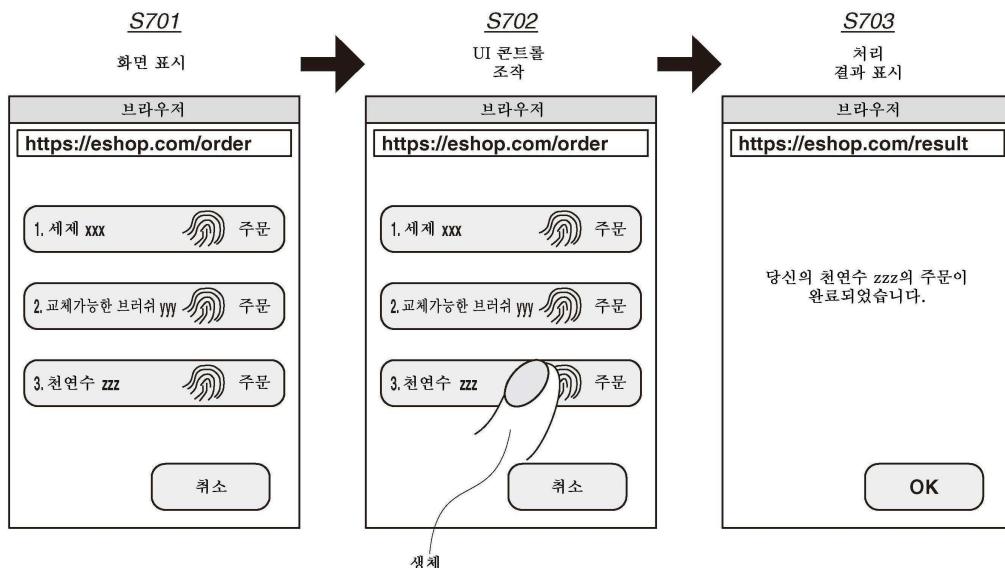
전체 청구항 수 : 총 7 항

심사관 : 문남두

(54) 발명의 명칭 정보 처리 장치 및 방법

(57) 요 약

정보 처리 장치는, 사용자 조작을 접수하기 위한 콘트롤의 생성 명령들에 기초하여 콘트롤을 표시하여, 생체 인증이 요구되는 것을 나타내는 정보가 콘트롤에 부가되게 하고, 표시된 콘트롤에 대한 사용자 조작이 검출될 때에, 콘트롤에 대응하는 처리 요구를 실행하게 하고, 정보 처리 장치에 의해 판독된 생체 정보와 저장되는 생체 정보를 사용하여 생체 인증의 결과에 기초하는 데이터를, 처리 요구의 요구처에 송신하게 한다. 처리 요구 및 생체 인증의 결과에 기초하는 데이터에 기초하여, 콘트롤에 대응하는 처리에 관한 정보가 표시된다.

대 표 도

(52) CPC특허분류

G06K 9/00006 (2013.01)

H04L 9/3231 (2013.01)

명세서

청구범위

청구항 1

생체 인증을 위한 인증 모듈, 템퍼 저항성을 갖는 저장 영역, 디스플레이, 그리고, 사용자의 생체 정보를 판독하는 생체 정보 센서이며 상기 디스플레이 상의 조작 영역 중 적어도 일부인 판독 가능 영역 내의 생체 정보를 판독하도록 구성된 생체 정보 센서를 포함하는 정보 처리 장치로서,

사용자 조작을 접수하기 위한 콘트롤의 생성 명령에 따라, 상기 생체 인증이 요구되는 것을 나타내는 정보가 부가되는 상태에서의 상기 콘트롤을, 상기 디스플레이에 표시하는 표시 수단으로, 상기 콘트롤의 상기 생성 명령은 네트워크를 통해 상기 정보 처리 장치와 통신하는 웹 애플리케이션으로부터 제공되는 표시 수단;

상기 표시된 콘트롤에 대한 상기 사용자 조작이 검출될 때에, 상기 콘트롤에 대응하는 처리 요구를 상기 웹 애플리케이션을 포함하는 시스템에 송신하는 요구 수단; 및

사용자 조작 대상인 상기 콘트롤이 표시되는 위치에서 상기 생체 정보 센서를 통해 판독된 생체 정보와, 상기 저장 영역에 저장되는 상기 생체 정보를 사용하여 상기 인증 모듈에 의해 실행된 상기 생체 인증의 결과에 기초하는 데이터를, 상기 시스템에 송신하는 송신 수단

을 포함하고,

상기 처리 요구 및 상기 생체 인증의 상기 결과에 기초하는 데이터에 따라, 상기 콘트롤에 대응하는 처리에 관한 정보가 상기 디스플레이에 표시되고,

상기 표시된 콘트롤은 상기 생체 정보 센서의 상기 판독 가능 영역 내에 배치 및 표시되는, 정보 처리 장치.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 콘트롤에 대한 상기 사용자 조작에 응답하여 생성된 제1 검증 데이터가 상기 처리 요구에 부가되고,

상기 처리 요구의 요구처로부터 상기 제1 검증 데이터를 포함하는 인증 요구가 만들어진 경우에, 상기 인증 모듈에 의해 상기 생체 인증이 실행되는, 정보 처리 장치.

청구항 4

제3항에 있어서,

상기 생체 정보가 저장되는 때 생성된 비밀 키가 상기 저장 영역에 저장되고,

상기 비밀 키에 대응하는 공개 키가 상기 처리 요구의 상기 요구처가 되는 시스템에 등록되고,

상기 인증 요구는 상기 시스템에 의해 생성된 제2 검증 데이터를 포함하고,

상기 생체 인증의 상기 결과에 기초하는 상기 데이터는, 상기 인증 모듈에 의해 실행된 상기 생체 인증이 성공한 경우에 상기 저장 영역으로부터 추출되는 상기 비밀 키와, 상기 제2 검증 데이터를 사용하여 생성된 서명 데이터를 포함하고,

상기 서명 데이터는 상기 공개 키를 사용하여 상기 시스템 의해 검증되는, 정보 처리 장치.

청구항 5

제1항에 있어서,

상기 콘트롤의 상기 생성 명령을 따르는 상기 생체 인증이 요구되는 것을 나타내는 상기 정보가 부가되는 상태

에서 표시되어야 할 상기 콘트롤의 표시 영역에서, 상기 생체 정보 센서에 의해 상기 생체 정보가 판독될 수 없는 경우에, 상기 생체 인증이 요구되는 것을 나타내는 상기 정보를 부가하지 않고 상기 콘트롤이 표시되고, 상기 콘트롤에 대한 상기 사용자 조작이 검출된 경우에, 상기 사용자로부터 상기 생체 인증을 요구하기 위한 화면이 추가적으로 표시되는, 정보 처리 장치.

청구항 6

삭제

청구항 7

삭제

청구항 8

제1항에 있어서,

상기 생체 정보는 상기 사용자의 지문에 관한 정보인, 정보 처리 장치.

청구항 9

생체 인증을 위한 인증 모듈, 템퍼 저항성을 갖는 저장 영역, 디스플레이, 그리고, 사용자의 생체 정보를 판독하는 생체 정보 센서이며 상기 디스플레이 상의 조작 영역 중 적어도 일부인 판독 가능 영역 내의 생체 정보를 판독하도록 구성된 생체 정보 센서를 포함하는 정보 처리 장치에 대한 방법으로서,

사용자 조작을 접수하기 위한 콘트롤의 생성 명령에 따라, 상기 생체 인증이 요구되는 것을 나타내는 정보가 부가되는 상태에서의 상기 콘트롤을, 상기 디스플레이에 표시하는 단계로, 상기 콘트롤의 상기 생성 명령은 네트워크를 통해 상기 정보 처리 장치와 통신하는 웹 애플리케이션으로부터 제공되는 단계;

상기 표시된 콘트롤에 대한 상기 사용자 조작이 검출될 때, 상기 콘트롤에 대응하는 처리 요구를 상기 웹 애플리케이션을 포함하는 시스템에 송신하는 단계; 및

상기 사용자 조작의 대상인 상기 콘트롤이 표시되는 위치에서 상기 생체 정보 센서를 통해 판독된 생체 정보와, 상기 저장 영역에 저장되는 상기 생체 정보를 사용하여 상기 인증 모듈에 의해 실행된 상기 생체 인증의 결과에 기초하는 데이터를, 상기 시스템에 송신하는 단계

를 포함하고,

상기 처리 요구 및 상기 생체 인증의 상기 결과에 기초하는 상기 데이터에 따라, 상기 콘트롤에 대응하는 처리에 관한 정보가 상기 디스플레이에 표시되고,

상기 표시된 콘트롤은 상기 생체 정보 센서의 상기 판독 가능 영역 내에 배치 및 표시되는, 정보 처리 장치에 대한 방법.

청구항 10

컴퓨터가, 생체 인증을 위한 인증 모듈, 템퍼 저항성을 갖는 저장 영역, 디스플레이, 그리고, 사용자의 생체 정보를 판독하는 생체 정보 센서이며 상기 디스플레이 상의 조작 영역 중 적어도 일부인 판독 가능 영역 내의 생체 정보를 판독하도록 구성된 생체 정보 센서를 포함하는 정보 처리 장치에 대한 방법을 실행하게 하기 위한 컴퓨터 프로그램이 저장된 비일시적 컴퓨터 판독 가능 저장 매체로서, 상기 방법은,

사용자 조작을 접수하기 위한 콘트롤의 생성 명령에 따라, 상기 생체 인증이 요구되는 것을 나타내는 정보가 부가되는 상태에서의 상기 콘트롤을, 상기 디스플레이에 표시하는 단계로, 상기 콘트롤의 상기 생성 명령은 네트워크를 통해 상기 정보 처리 장치와 통신하는 웹 애플리케이션으로부터 제공되는 단계;

상기 표시된 콘트롤에 대한 상기 사용자 조작이 검출될 때, 상기 콘트롤에 대응하는 처리 요구를 상기 웹 애플리케이션을 포함하는 시스템에 송신하는 단계; 및

상기 사용자 조작의 대상인 상기 콘트롤이 표시되는 위치에서 상기 생체 정보 센서를 통해 판독된 생체 정보와, 상기 저장 영역에 저장되는 상기 생체 정보를 사용하여 상기 인증 모듈에 의해 실행된 상기 생체 인증의 결과에

기초하는 데이터를, 상기 시스템에 송신하는 단계

를 포함하고,

상기 처리 요구 및 상기 생체 인증의 상기 결과에 기초하는 상기 데이터에 따라, 상기 콘트롤에 대응하는 처리에 관한 정보가 상기 디스플레이에 표시되고,

상기 표시된 콘트롤은 상기 생체 정보 센서의 상기 판독 가능 영역 내에 배치 및 표시되는, 비일시적 컴퓨터 판독 가능 저장 매체.

발명의 설명

기술 분야

[0001]

본 개시내용은 생체 인증을 사용하여 서비스를 이용할 때의 제어에 관한 것이다.

배경 기술

[0002]

최근, 스마트폰들이나 태블릿 컴퓨터들 등의 휴대형 디바이스들이 널리 보급되어 오고 있다. 또한, 이들 모바일 디바이스들 등의 정보 처리 장치에 설치되는 디스플레이들, 센서들 및 프로세서들 등의 컴포넌트들의 기술 개발도 진보해 왔다.

[0003]

최근, 스마트폰들 등의 디바이스들의 후방 측 또는 다른 위치들에서 지문 센서가 표준 장비로서 장착되어, 사용자의 것에 의해, 생체 인증의 인증 수단이 더 빈번히 사용되어 왔다. 스마트폰들, 태블릿 컴퓨터들 및 기타 디바이스들에는, 사용자들이 주로 사용자의 손가락에 의해 이를 디바이스들을 조작할 수 있게 하는 표준 장비로서 터치 패널 디스플레이를 사용하는 사용자 인터페이스(UI)가 제공된다.

[0004]

패스워드 시스템 등의 레거시 인증을 사용하는 스마트폰들, 태블릿 컴퓨터들 및 기타 디바이스들에서, 생체 인증은 보안 및 편리성을 향상시키는 인증 시스템을 제공한다. 예를 들어, 애플리케이션 스토어에서 애플리케이션을 구입할 경우, 다음 단계들을 포함하는 절차가 수행된다:

1. 구입 지시(UI 조작),

2. 인증(레거시 인증 또는

생체 인증), 및

3. 구입 처리 결과 표시.

[0009]

단계 2에서는, 레거시 인증 및 생체 인증 양자 모두가 이용될 수 있다.

[0010]

일본 미심사 특허 출원 공개 공보(PCT 출원의 번역) 제2008-523460호에서, 지문 판독기는 의료 시스템과 의료 스태프를 인터페이스-접속하기 위한 다이내믹 디스플레이 및 터치 스크린 입력을 포함한 사용자 인터페이스에서, 다이내믹 디스플레이의 후방 측에 하나 이상의 지문 스캐너를 가동식으로 배치하는 것을 포함한다. 사용자 인터페이스로 터치 조작이 입력된 경우에, 터치 위치를 식별하고, 식별된 위치로 이동한 지문 스캐너에 의해 판독된 지문을 사용하여, 사용자 식별 및 인증을 제공하는 기술이 개시된다.

[0011]

스마트폰, 태블릿 컴퓨터 및 기타 디바이스들에 대하여 인증이 필요한 웹 서비스를 제공할 때에도, 생체 인증을 이용할 수 있다. 이 예에서는, 구입 지시가 주어질 때 생체 인증이 요구된다. 생체 인증을 요구하는 웹 서비스에 대해서는, 사용자 입력을 접수하기 위해서 단말기에 표시되는 몇 가지의 오브젝트(버튼들 등의 UI 콘트롤들)에의 조작들 중에서, 기동이나 구입 등의 특정 처리를 위한 조작이 수행되는 경우에 인증이 요구된다. 해당 조작에 한하여, 단말기 내에서의 인증이 완료될 때까지 사용자로 하여금 사용자의 생체 정보를 의도적으로 입력하게 하기 위한 높은 조작성의 메커니즘이 요구된다.

발명의 내용

[0012]

본 개시내용의 양태에 따르면, 생체 인증을 위한 인증 모듈, 탭퍼 저항성을 갖는 저장 영역, 사용자의 생체 정보를 판독하는 생체 정보 센서 및 디스플레이를 포함하는 정보 처리 장치는, 사용자 조작을 접수하기 위한 콘트롤의 생성 명령에 따라, 생체 인증이 요구되는 것을 나타내는 정보가 부가되는 상태에서의 콘트롤을, 디스플레이에 표시하는 표시 수단, 표시된 콘트롤에 대한 사용자 조작이 검출될 때에, 콘트롤에 대응하는 처리 요구를

행하는 요구 수단, 및 사용자 조작 대상인 콘트롤이 표시되는 위치에서 생체 정보 센서를 통해 판독된 생체 정보와, 저장 영역에 저장되는 생체 정보를 사용하여 인증 모듈에 의해 실행된 생체 인증의 결과에 기초하는 데이터를, 처리 요구의 요구처에 송신하는 송신 수단을 포함하고, 처리 요구 및 생체 인증의 결과에 기초하는 데이터에 따라, 콘트롤에 대응하는 처리에 관한 정보가 디스플레이에 표시된다.

[0013] 추가적인 특징들은 첨부 도면들을 참고한 예시적인 실시예들에 대한 이하의 설명으로부터 명확해질 것이다.

도면의 간단한 설명

[0014] 도 1은 예시적인 실시예에 따른 시스템 구성 예를 도시한다.

도 2a 및 도 2b는 정보 처리 장치의 하드웨어 구성 예들을 도시한다.

도 3은 예시적인 실시예에 따른 시스템 내의 각 디바이스들의 소프트웨어 및 하드웨어 구성 예들을 도시한다.

도 4는 컴퓨터에 의해 제공되는 사용자 인터페이스 예를 도시한다.

도 5는 도 4에서 나타내는 사용자 인터페이스의 구현 예를 설명하기 위한 도면이다.

도 6은 도 4에서 나타내는 사용자 인터페이스의 생성 처리를 설명하기 위한 플로우차트이다.

도 7은 컴퓨터의 사용자 인터페이스 화면 천이 예를 도시한다.

도 8은 컴퓨터 및 서버에 의한 전반적인 처리의 시퀀스를 도시한다.

도 9a 및 도 9b는 컴퓨터의 하드웨어 사양들에 의존한 사용자 인터페이스 예들을 도시한다.

도 10은 제2 변형예에 따른 사용자 인터페이스 화면 천이 예를 도시한다.

도 11은 제2 변형예에 따른 컴퓨터와 서버에 의한 전반적인 처리의 시퀀스를 도시한다.

도 12는 예시적인 실시예에 따른 적용 예의 사용자 인터페이스의 구현 예를 예시하는 도면이다.

도 13은 생체 인증의 실행 설정 화면을 도시한다.

도 14는 적용 예의 컴퓨터와 서버에 의한 전반적인 처리의 시퀀스를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0015] 이하, 본 개시내용을 실시하기 위한 예시적인 실시예들이 도면들을 참조하여 설명될 것이다.

[0016] 도 1은, 본 예시적인 실시예에 따른 시스템 구성의 일례를 나타낸다.

[0017] 네트워크(101)는, 인터넷 및 인트라넷을 포함한다. 네트워크(105)는, 사설 네트워크 또는 로컬 영역 네트워크(LAN)를 포함한다. 네트워크(105)는, 컴퓨터들 등의 디바이스들을 접속하는 말단의 네트워크이고, 유선 통신 네트워크 또는, 무선 LAN이나 휴대 전화 통신 네트워크 등의 무선 통신 네트워크일 수 있다. 컴퓨터(111)는, 개인용 컴퓨터들, 랩탑 컴퓨터들, 태블릿 컴퓨터들, 및 스마트폰들 등의 다양한 형태들 및 타입들을 포함한다. 컴퓨터(111)는, 디지털 카메라들, 프린터들, 차량 탑재 디바이스들(카 내비게이션 시스템들), 및 홈 어시스턴스 로봇 또는 간호 로봇 등의, 웹 서비스와 통신하고, 터치 패널이 구비된 디바이스들을 포함한다. 서버(121)는 네트워크를 통해 웹 사이트들 및 웹 애플리케이션들 등의 웹 서비스들을 제공한다.

[0018] 도 2a는 컴퓨터(111)를 포함하는 정보 처리 장치 하드웨어의 모듈 구성 예를 도시한다. 도 2b는 서버(121)를 포함하는 정보 처리 장치 하드웨어의 모듈 구성 예를 나타낸다.

[0019] 도 2a에서, 네트워크 인터페이스(202)는 LAN 등의 네트워크에 접속되어, 다른 컴퓨터들 및 네트워크 디바이스들과 통신한다. 접속은 유선 또는 무선일 수 있다. 판독 전용 메모리(ROM)(204)는 내장 프로그램 및 데이터를 저장한다. 랜덤 액세스 메모리(RAM)(205)는 임시 메모리 영역으로서 사용되는 메모리이다. 2차 저장 디바이스(206)는 예를 들어, 하드 디스크 드라이브(HDD)나 플래시 메모리에 의해 대표되는 저장 디바이스이다. 중앙 처리 유닛(CPU)(203)은 ROM(204), RAM(205), 또는 2차 저장 디바이스(206)로부터 판독된 프로그램을 실행한다. 2차 저장 디바이스(206)는, 후술하는 플로우차트들에서 처리를 구현하기 위한 소프트웨어 프로그램을 또한 저장한다. 사용자 인터페이스(201)는, 사용자가 키보드, 마우스, 버튼 등을 사용하여 정보나 신호를 입력할 수 있게 한다. 이러한 하드웨어를 포함하지 않는 컴퓨터는, 원격 테스크톱이나 원격 셸을 통해, 다른 컴퓨터에 접속될 수 있고 다른 컴퓨터를 통해 조작될 수 있다. 디스플레이(210)는 하나의 사용자 인터페이스이다. 터치 패

널(211)은 다른 사용자 인터페이스이다. 터치 패널(211)은, 접촉 센서, 압력 센서 등을 통해, 사용자 조작의 조작 위치/방향, 조작 거리 및 조작 압력 등을 검출한다. 생체 정보 센서(212)는 사용자의 지문, 정맥, 홍채, 음성 및 얼굴 화상에 관한 생체 정보를 판독한다. TPM(Trusted Platform Module)(221)은, 운영 체제 및 다른 하드웨어에 독립하여 기능하는 보안 칩이고, 탬퍼 저항성이고, 기밀 정보를 처리 및 저장하기 위한 저장 유닛으로서 역할을 한다. 본 개시내용에서는, 생체 인증에 이용하는 사용자의 생체 정보, 또는 그 특징량 및 후술되는 인증 처리에 요구되는 비밀 키가 TPM(221)에 저장된다. TPM의 대안으로서, 탬퍼 저항성은 1개의 칩 상에서 기타 메모리 공간들로부터 격리된 보안 메모리 공간을 확보하고, 그 메모리 공간에서 사용자의 생체 정보, 또는 그 특징량, 및 비밀 키를 관리하기 위한 저장 유닛을 제공하는 방법에 의해 구현될 수 있다. 각 유닛은 입력/출력 인터페이스(207)를 통해 접속된다.

[0020] 본 실시예에서, 디스플레이(210), 터치 패널(211) 및 생체 정보 센서(212)가 일체로 구성된다. 더 구체적으로, 이를 하드웨어 컴포넌트들이 서로 겹쳐져서, 디스플레이(210) 상의 터치 조작이 터치 패널(211)에 의해 검출되고 제어되고, 터치 패널(211) 상의 임의의 위치에 대한 생체 정보의 입력, 즉, 터치와 연관된 지문 정보의 판독이 생체 정보 센서(212)에 의해 검출되고 제어된다.

[0021] 도 2b는, 도 2a에서의 하드웨어 구성과 유사한 하드웨어 구성을 도시한다. 서버(121)로서 동작하기 위해서 요구되는 구성만이 도시되고, 도 2a에서의 동일한 참조 부호들을 참조하여 설명되는 구성의 기능들과 유사한 기능들은 생략된다. 제공되는 예시는 단지 일례이며, 디스플레이 등의, 다른 일반적인 하드웨어 구성들이 또한 포함될 수 있다.

[0022] 도 3은, 본 시스템의 각 디바이스들의 소프트웨어의 모듈 구성들을 도시하는 도면이다. 도 2a 및 도 2b를 참조하여 설명되는 하드웨어 구성들이 또한 부분적으로 도시된다. 도시된 소프트웨어의 모듈 구성들 각각은, CPU(203)에 의해 본 개시내용에 특유한 프로그램을 실행함으로써 구현되고, 네트워크 접속의 화살표들에 의해 도시한 바와 같이, 서로 통신할 수 있다.

[0023] 먼저, 서버(121)의 구성에 대해서 설명할 것이다.

[0024] 웹 애플리케이션(311)은, 서버(121)에 설치된다. REST(Representational State Transfer) API(Application Programming Interface)(312)는 웹 애플리케이션(311)에 의해 제공된다. 웹 UI(313)은, 웹 애플리케이션(311)에 의해 제공된다. 데이터 스토어(314)는, 웹 애플리케이션(311)이 사용하는 데이터를 보존 및 저장한다. 웹 애플리케이션(311)은, 클라이언트로부터의 HTTP 요구의 콘텐츠에 기초하여, 웹 UI(313)를 통해 HTML(HyperText Markup Language)이나 JavaScript®의 콘텐츠 파일로 응답하거나, REST API(312)를 통해 XML(extended markup language)이나 JSON(JavaScript Object Notation) 데이터로 응답한다.

[0025] 인증 서버(321)는, 서버(121)에 설치된다. 데이터 스토어(322)는, 인증 서버(321)가 사용하는 데이터를 보존 및 저장한다. 인증 서버(321)는, 사용자의 각각의 어카운트에 사용될 수 있는 인증 시스템, 예를 들어, 인증자 정보를 등록 및 관리하여 인증 어설션을 검증한다. 인증 서버(321)는 사용자의 생체 정보 또는 생체 정보의 특징량을 직접적으로 저장 및 관리하지 않는다. 인증 서버(321)는 또한 서버(121) 외부에 위치될 수 있다, 즉 네트워크 상으로 서버(121)에 접속될 수 있다.

[0026] 이어서, 컴퓨터(111)의 구성에 대해서 설명할 것이다.

[0027] 운영 체제(351)(이후, OS로서 지칭됨)는, 컴퓨터(111)에 설치된다. OS(351)는, 컴퓨터(111)의 각 하드웨어를 관리 및 제어하여 각종 프로그램의 실행을 관리하는 기본 소프트웨어이다. 플랫폼 API(352)는, OS(351)에 포함되고, OS(351)를 통해 각 하드웨어와의 상호작용을 제어한다. 그래픽 드라이버(353)는 디스플레이(210)를 제어한다. 터치 패널 콘트롤러(354)는, 터치 패널(211)로부터의 예를 들어, 접촉, 위치 및 압력의 신호들을 검출 및 처리한다. 터치 패널 디스플레이의 경우, OS(351)가 디스플레이(210)에 UI 콘트롤들을 묘사하고, 터치 패널(211)이 사용자에 의해 수행되는 UI 콘트롤 조작을 검출하고, OS(351)에 피드백을 제공한다.

[0028] 인증자(355)는, 생체 정보 센서(212)로부터 판독된 생체 정보에 기초하여 사용자를 인증한다. 본 개시내용에서, 인증자(355)는 인증 모듈로서 정의된다. 생체 정보 센서(212) 및 인증자(355)의 조합이 인증 모듈로서 지정될 수 있다. 인증자(355)는, 예를 들어 TPM(221)의 보안 영역에 암호 키를 저장하고, 판독된 생체 정보 또는 그 특징량 등의 기밀 정보를 그 암호키를 사용하여 2차 저장 디바이스(206)에 암호화 데이터로서 저장한다. 사용자가 생체 인증을 시도한 때, 인증자(355)는 저장되는 생체 정보 또는 그 특징량을, 사용자에 의해 제공되는 생체 정보와 정합하여, 생체 인증이 성공했는지를 판정한다.

[0029] 애플리케이션(361)은, 컴퓨터(111)에 설치되고, 2개의 카테고리: 네이티브 애플리케이션들과 브라우저들로 분할

될 수 있다. 네이티브 애플리케이션은, OS 상에서 직접 실행 가능한 코드로 기술된 애플리케이션이다. 네이티브 애플리케이션은, OS(351)가 제공하는 각 기능에 플랫폼 API(352)를 통해 액세스한다. 브라우저는, HTML 및 JavaScript®를 표시 및 실행하는 애플리케이션이다. JavaScript®(372)는 브라우저 상에서 실행된다. 브라우저는, 네트워크를 통해, 서버(121)에서 실행되는 웹 애플리케이션(311)으로부터 HTML, JavaScript®(372) 등을 취득, 실행 및 표시한다. 브라우저 API(373)는, 브라우저 상에서 실행되는 JavaScript®(372)에 의해 OS(351)이 제공하는 기능에 액세스할 수 있도록 브라우저에 포함된다. 네이티브 애플리케이션이 네트워크 상의 기능 및 데이터를 사용하는 경우에는, 웹 애플리케이션(311)에 접속되어, REST API(312)를 통해 데이터를 송신 및 수신한다.

[0030] 일부 경우에서, 애플리케이션(361)에 의해 웹 애플리케이션(311)에 접속되고, 특정한 기능이나 데이터에 액세스하기 위해서 사용자 인증이 요구된다. 본 개시내용에 의해 사용되는 1개의 인증 방식일 수 있는 FIDO® 얼라이언스로부터의 FIDO®(Fast IDentity Online)에 따르면, 웹 인증에 생체 인증을 사용하기 위한 표준 사양들이 공개되어 있다. 이하의 절차에 의해 웹 인증에 사용하는 생체 인증용 인증자(355)를 인증 서버(321)에 등록한다.

[0031] (1) 애플리케이션(361)으로부터, 웹 애플리케이션(311)에 액세스하고, 인증 서버(321)에서의 레거시 인증, 예를 들어, 사용자 이름 및 패스워드의 입력에 기초하여, 로그인한다.

[0032] (2) 애플리케이션(361)으로부터, 웹 애플리케이션(311)에 등록 개시 요구를 송신하는 경우, 인증 서버(321)는 챌린지(Challenge) 데이터를 생성하고, 챌린지 데이터를 애플리케이션(361)에 반환한다.

[0033] (3) 애플리케이션(361)은, 인증자(355)에 크리덴셜 생성 요구를 송신한다.

[0034] (4) 크리덴셜 생성 요구에 응답하여 사용자의 생체 인증 처리의 성공에 기초하여, 인증자(355)는 비밀 키 및 공개 키의 페어를 생성한다.

[0035] (5) 인증자(355)에 의해, 비밀 키 및 공개 키의 페어는, 웹 애플리케이션(311)에 로그인한 사용자 정보와 연관한다. 비밀 키는, 컴퓨터(111) 내의 TPM(221) 등의 보안 영역에 저장된다.

[0036] (6) 인증자(355)는 등록용 크리덴셜 정보를 생성한다. 등록용 크리덴셜 정보는, 인증자(355)를 개별로 식별하기 위한 크리덴셜과, 공개 키 및 전술한 챌린지로부터 비밀 키를 사용하여 생성된 서명을 포함한다.

[0037] (7) 인증자(355)는 생성된 등록용 크리덴셜 정보를 인증 서버(321)에 송신한다.

[0038] (8) 인증 서버(321)는, 수신된 등록용 크리덴셜 정보에 포함되는 공개 키를 사용하여 유사하게 포함되는 서명을 검증하고, 인증자를 식별하는 정보, 공개 키 등을, 사용자 정보와 연관하여 저장한다.

[0039] 등록 처리 이후, 애플리케이션(361)이 웹 애플리케이션(311)에 액세스할 때, 인증 서버(321)에 의해 생성된 검증 데이터로서 챌린지를 포함하고, RP ID(relying party identifier) 등이 지정된 생체 인증 요구(어설션 요구)가 애플리케이션(361)에 송신된다. 이 때, 컴퓨터(111) 내에 대응하는 인증자가, 생체 인증을 실행함으로써 얻어지는 비밀 키와 그 챌린지를 사용하여 서명을 생성한다. 그 후, 서명을 검증하는 인증 서버(321)에 의해, 웹 애플리케이션(311)에 로그인하기 위한 인증 처리가 실현된다. 즉, 본 사양들에 기초하여, 네트워크를 통해 인증을 위한 생체 정보가 흐르지 않는다. 또한, 등록 처리 이후, 패스워드 및 기타 수단을 사용한 레거시 인증이 불필요하다.

[0040] 도 4는 본 개시내용에서, 컴퓨터(111)의 디스플레이(210)에 표시되는 통합된 생체 인증의 UI 콘트롤의 표시 예를 나타낸다.

[0041] 영역(401)은, 컴퓨터(111)에 포함되고 터치 패널(211)로서 또한 역할을 하는 디스플레이(210)의 예이다. 도 4에서 흑색 도포된 영역은 터치 패널 디스플레이의 표시 가능 범위 및 터치 조작 검출 가능 영역을 나타낸다. 영역(402)은, 디스플레이(210)의 동일 면에서 생체 정보 센서(212)의 생체 정보, 예컨대 지문의 검출 가능 영역을 나타낸다. UI(410)는, 영역(401) 상에 표시된 애플리케이션(361)의 UI 예를 나타낸다. 콘트롤들(411 내지 414)은, UI(410)에 배치된 UI 콘트롤들(버튼 오브젝트들)의 예이다. 콘트롤들(411 내지 413)은, 통합된 생체 인증의 UI 콘트롤들이다. 표준 UI 콘트롤(414)은, 생체 인증을 필요로 하지 않는다. 통합된 생체 인증의 UI 콘트롤들은, 생체 정보 센서(212)의 검출 가능 영역(402) 내에 임의인 위치에 배치될 수 있다.

[0042] 도 5 및 도 6을 참조하여, 도 4에서 나타내는 UI 콘트롤들을 표시하는 방법 및 처리 플로우의 예들이 설명될 것이다.

[0043] 도 5에서의 영역(500)은, 애플리케이션(361)의 일례로서 웹 브라우저(브라우저)에 표시되는 마크업 언어(예를

들어, HTML)에서 기술된 데이터의 일부를 나타낸다. HTML 요소들(501 및 502)은, UI 콘트롤들을 표시하기 위한 생성 명령들을 나타낸다.

[0044] HTML 요소(502)는, 표준 UI 콘트롤에 대응한다. HTML 요소(501)는, 통합된 생체 인증의 UI 콘트롤에 대응한다. 생체 인증을 지정하기 위해서, HTML5의 커스텀 데이터 속성 data-*을 이용한 예가 가정된다. 커스텀 데이터 속성 data-bioauth=""required""는, 콘트롤이 통합된 생체 인증의 UI 콘트롤인 것을 나타낸다. 유사하게, data-bioauth-rpid 속성에, 웹 애플리케이션(311)을 식별하기 위한 RP ID로서 도메인명을 지정한다.

[0045] 영역(510)은, 브라우저에서의 HTML(500)의 UI 표시 결과를 나타낸다. 콘트롤(511)은, HTML 요소(501)에 의해 지정된 통합된 생체 인증의 UI 콘트롤이다. 콘트롤(513)은, HTML 요소(502)에 의해 지정된 표준의 버튼 콘트롤이다. 생체 인증 아이콘(512)은, 커스텀 데이터 속성 data-bioauth=""required""에 의해, UI 콘트롤(511)이 생체 인증용 특별한 콘트롤인 것을 나타내도록 의도된다. 사용자는 생체 인증 아이콘(512)에 기초하여, 조작에 생체 인증이 요구되는 것을 인식할 수 있다. 또한, 생체 인증 아이콘(512)을 포함하는 UI 콘트롤(511)을 조작할 때, 통상의 콘트롤에 대한 조작(버튼 누름)에 비하여, 카메라나 센서 등의 생체 정보 센서(212)에 의한 생체 정보를 판독하기 위해, 어느 정도의 긴 누름 조작이 요구될 수 있다. 지문 정보가 판독되는 경우에, 사용자의 손가락이 생체 인증 아이콘(512) 부분에 터치되고 있는 동안에 사용자의 손가락의 지문 정보가 센서에 의해 판독된다. 얼굴 화상 인증 등을 위한 얼굴 화상을 판독하기 위해서는, 생체 인증 아이콘(512) 부분에 터치되는 동안에 컴퓨터(111)의 카메라(도시하지 않음)를 통해 사용자의 화상을 캡처함으로써 얼굴 화상이 판독된다. 판독이 완료되고, 생체 인증이 성공한 경우에, 구입 수속 완료 화면 등의 다음 화면으로의 천이가 수행된다.

[0046] 도 6은, 도 5에서 나타낸 HTML 데이터의 판독 및 묘화에 관한 처리를 설명하는 플로우차트이다. 이 처리는 브라우저를 위한 애플리케이션(361)을 CPU(203)이 실행함으로써 구현된다.

[0047] 단계 S601에서, 브라우저는, HTML(500) 내의 HTML 요소를 1개씩 판독한다. 단계 S602에서, 브라우저는 HTML 요소 내에, 속성 data-bioauth=""required""로, 생체 인증 요구가 지정되는지를 판정한다. 단계 S602에서 생체 인증 요구가 지정되는 것으로 판정된 경우에(단계 S602에서 예), 처리는 단계 S603으로 진행한다. 생체 인증 요구가 지정되지 않는 것으로 판정된 경우에(단계 S602에서 아니오), 처리는 단계 S604로 진행한다.

[0048] 단계 S603에서, 브라우저는, 지정된 좌표 및 크기에서 OS(351)에 UI 콘트롤의 묘화를 요구한다. OS(351)는, 생체 인증 아이콘(512)을 포함하는 UI 콘트롤(511)을 디스플레이(210)에 묘화한다. 단계 S604에서, 브라우저는, OS(351)에 표준 콘트롤의 묘화를 요구하고, OS(351)는 표준 콘트롤을 묘화한다. HTML내의 모든 요소가 묘화를 완료하는 경우, 도시된 루프 처리가 종료되고, 단계 S605에서, UI(510)에 모든 UI 콘트롤의 표시가 완료된다.

[0049] 도 5 및 도 6은 애플리케이션(361)이 브라우저인 예이지만, 애플리케이션(361)이 네이티브 애플리케이션인 경우에 유사한 처리가 수행된다. 애플리케이션(361)이 네이티브 애플리케이션인 경우에는, 프로그램내에서 OS(351)가 제공하는 UI 콘트롤들이 직접 묘화될 수 있다. 전술한 예에서 HTML의 커스텀 데이터 속성을 이용한 경우에서와 같이, OS(351)에 대한 UI 콘트롤 묘화 명령들에 생체 인증을 나타내는 속성을 부가함으로써, 네이티브 애플리케이션이 OS(351)에 생체 인증용 특별한 콘트롤을 묘화하도록 요구한다.

[0050] 도 7 및 도 8을 참조하여, 통합된 생체 인증의 UI 콘트롤의 사용자 조작들에 기초한 처리 플로우가 설명된다.

[0051] 도 8은, 사용자 조작들을 포함하는, 컴퓨터(111) 및 서버(121)에 의한 전반적인 처리의 시퀀스를 설명하는 도면이다.

[0052] 단계 S801에서, 사용자는, 애플리케이션(361)을 조작하여, 애플리케이션의 기동, 또는, 화면 표시를 요구한다. 단계 S802에서, 조작 대상인 애플리케이션(361)으로서 브라우저가, 웹 애플리케이션(311)에 웹 콘텐츠 요구를 송신한다.

[0053] 단계 S803에서, 웹 애플리케이션(311)은, 웹 콘텐츠로서 HTML 데이터나 JavaScript®로 응답한다. 생체 인증이 필요한 UI 콘트롤에 대해서는, 도 5를 참조하여 전술한 커스텀 데이터 속성들을 부가한다. 조작 대상의 애플리케이션(361)이 네이티브 애플리케이션인 경우에는, 단계 S802 및 단계 S803을 실행하는 대신에 프로그램 내에서 묘화되는 UI 콘트롤이 지정된다.

[0054] 단계 S804에서, 애플리케이션(361)은, HTML 데이터를 터치 패널 디스플레이(210) 상에서 묘화 처리를 수행한다. 애플리케이션(361)은, 플랫폼 API(352)를 통해 좌표 및 크기를 지정함으로써 UI 콘트롤을 묘화하도록 OS(351)에 요구한다. 이 때, 생체 인증은 API의 확장 파라미터 등을 이용함으로써 지정된다. 단계 S805에서, OS(351)는, 애플리케이션(361) 상에 요구된 UI 콘트롤을 표시한다. 이 때, 통합된 생체 인증의 UI 콘트롤에는, 생체 인증

아이콘(512)을 표시한다. 단계 S806에서, 애플리케이션(361)은, OS(351)에 대하여, 관련 UI 콘트롤에 대한 이벤트 청취자를 설정한다. 이 때, 통합된 생체 인증의 UI 콘트롤에는, 지정된 웹 애플리케이션(311)의 RP ID를 이벤트 청취자의 확장 파라미터로서 부가한다. OS(351)는 또한 RP ID를 OS(351)의 로컬 저장 영역에 기록한다.

[0055] 상기의 처리의 결과로서, 컴퓨터(111)의 터치 패널 디스플레이(210) 상에 도 7의 단계 S701의 애플리케이션(361)의 UI 화면이 표시된다.

[0056] 단계 S807에서, 사용자가, 도 7의 단계 S701에서 나타내는 화면 상의 UI 콘트롤들 중 하나를 조작한다. 더 구체적으로, 도 7의 단계 S702에 도시하는 바와 같이, 사용자는 통합된 생체 인증의 UI 콘트롤을, 예를 들어, 사용자의 손가락으로 터치한다(누른다).

[0057] 단계 S808에서, OS(351)는, UI 콘트롤들 중 하나의 조작을 검출한 경우, 1회의 난수 넌스(Nonce)를 생성하고, 넌스를 OS(351)의 로컬 저장 영역에 기록한다. 넌스는, 생체 인증이 어느 UI 콘트롤을 기점으로서 실행되는지를 추적 및 검증하기 위한 검증 데이터로서 사용된다. 단계 S809에서, OS(351)는, 애플리케이션(361)에 UI 콘트롤 조작 이벤트를 통지한다. 이 때, 생성된 넌스를 이벤트에 부가한다.

[0058] 단계 S810에서, 애플리케이션(361)은, OS(351)로부터 수신한 이벤트를 해석하여, 생체 인증 요구가 지정된 콘트롤에 대한 조작 이벤트인지를 판정한다. 단계 S811에서, 단계 S810에서의 판정이 아니오인 경우에(단계 S810에서 아니오), 이벤트는 통상의 UI 콘트롤 조작 이벤트로서 처리된다. 도 7의 예는 취소 버튼이 조작된 경우이므로, 생체 인증 등을 수행하지 않고, 초기 화면으로의 천이 등의 처리가 수행될 것이다. 단계 S810에서의 판정이 예인 경우에(단계 S810에서 예), 처리는 단계 S812로 진행한다.

[0059] 단계 S812에서, 애플리케이션(361)은, 단계 S807에서 검출되고, 단계 S702에서 나타내는 사용자 조작에 의해 요구된 처리가 수행되는 URL(uniform resource locator)을 수신처로서 설정하고, 웹 애플리케이션(311)에 대한 처리 요구로서, 인증 개시 요구를 송신한다. 이 때, OS(351)로부터 수신한 넌스를 요구에 부가한다.

[0060] 단계 S813에서, 웹 애플리케이션(311)은, 인증 개시 요구의 수신에 응답하여, 인증 서버(321)에 인증 개시 트리거를 송신한다. 인증 서버(321)는, 단계 S814에서 검증 데이터로서 챌린지를 생성하고, 단계 S815에서 생성된 챌린지로 웹 애플리케이션(311)에 응답한다. 단계 S816에서, 웹 애플리케이션(311)은, 애플리케이션(361)에 생성된 챌린지, RP ID 및 넌스로 응답한다. 본 개시내용에서, 인증 서버(321)로부터 웹 애플리케이션(311)을 통해 송신되는 인증 요구(어설션 요구)에, 챌린지 및 RP ID에 더하여, 넌스가 부가된다.

[0061] 단계 S817에서, 애플리케이션(361)은, 인증 요구의 수신에 응답하여, 플랫폼 API(352)를 통해 OS(351)에 어설션 요구를 송신한다. 이 때, 챌린지, RP ID 및 넌스를 요구에 부가한다.

[0062] 단계 S818에서, OS(351)는, 단계 S817에서 수신된 RP ID와 넌스가, 단계 S806 및 단계 S808에서 기록된 것들과 정합하는지를 판정한다. 단계 S818에서의 판정 결과로서, 그것들이 정합되지 않는 경우에(단계 S818에서 아니오), 단계 S819에서 애플리케이션(361)은 여러 응답을 표시하여 처리를 중단한다. 단계 S818에서의 판정 결과로서 그것들이 정합되는 경우(단계 S818에서 예), 처리는 단계 S820으로 진행한다. 단계 S820에서, OS(351)는 인증자(355)에 챌린지를 포함하는 생체 인증 요구를 송신한다. 이 때, 확장 파라미터로서, 관련 UI 콘트롤의 표시 영역에 대응하는 생체 정보 센서의 영역을 지정한다.

[0063] 단계 S807 내지 단계 S820 사이의 짧은 기간에, 도 7의 단계 S702에서 나타내는 UI 콘트롤에 대한 사용자 조작이 수행된다. 이 동안에, 사용자는 생체 정보를 컴퓨터(111)에 입력한다.

[0064] 단계 S821에서, 인증자(355)는, 확장 파라미터로서 지정되고 UI 콘트롤의 표시 영역에 대응하는 영역으로부터 생체 정보 센서(212)에 의해 판독된 생체 정보를 사용하는 생체 인증의 결과를 취득한다. 미리 TPM(221)에 저장된 생체 정보 또는 그 특징량과, 생체 정보 센서(212)에 의해 판독된 생체 정보 또는 그 특징량의 정합도가 높은 경우에 생체 인증이 성공했다고 판정된다. 단계 S823에서, 인증자(355)는, 인증 결과를 검증하고, 인증이 성공한 경우에는, TPM(221)으로부터, 관련 생체 정보에 대응하는 비밀 키를 추출한다. 단계 S824에서, 인증자(355)는, 추출한 비밀 키와, 단계 S820에서 수신한 챌린지를 사용해서 서명 데이터를 생성한다. 단계 S825에서, 인증자(355)는, 인증 응답으로서 생성한 서명 데이터를 포함하는 어설션을 OS(351)에 반환한다. 단계 S826에서, OS(351)는, 인증 응답으로서 생성된 서명 데이터를 포함하는 어설션을 애플리케이션(361)에 반환한다.

[0065] 단계 S827에서, 애플리케이션(361)은, 웹 애플리케이션(311)에, 단계 S824에서 생성된 서명 데이터를 포함하는 어설션을 송신한다.

- [0066] 단계 S828에서, 웹 애플리케이션(311)은, 인증 서버(321)에 수신된 어설션을 송신하여, 그 검증을 요구한다.
- [0067] 단계 S829에서, 인증 서버(321)는, 인증자가 등록될 때 저장되는 공개 키를 사용하는 것에 의해, 어설션에 포함되는 서명 데이터를 검증한다. 단계 S830에서, 인증 서버(321)는, 단계 S829의 어설션 검증에 기초하여, 성공 또는 실패의 인증 결과로 응답한다. 더 구체적으로는, 인증 서버(321)는, 공개 키를 사용하는 것에 의해 서명 데이터로부터 챤린지를 추출하고, 단계 S814에서 생성된 챤린지와 동일한지를 확인한다. 확인 결과로서 챤린지들이 정합하는 경우에는, 웹 애플리케이션(311)은 인증 결과로서 성공을 통지받는다.
- [0068] 단계 S831에서, 웹 애플리케이션(311)은, 인증이 성공한 경우에, 단계 S812의 요구 콘텐츠를 처리한다. 예를 들어, 단계 S702의 예에서, 처리는 사용자에 의해 조작된 UI 콘트롤에 의해 지정된 상품의 주문 처리이다.
- [0069] 단계 S832에서, 웹 애플리케이션(311)은, 애플리케이션(361)에, 인증 결과로 응답한다. 인증 결과가 성공인 경우에, 단계 S831의 인증이 성공한 경우의 처리 결과를 포함하는 콘텐츠 데이터가 제공된다.
- [0070] 단계 S833에서, 애플리케이션(361)은, 인증 결과 및 처리 결과의 정보를 포함하는 콘텐츠를 컴퓨터(111)의 터치 패널 디스플레이(210) 상에 표시하여, 이를 결과들을 사용자에게 통지한다. 이 표시는 도 7의 단계 S703에 나타낸 바와 같고, 단계 S702의 주문 처리 요구에 대한 처리 결과가 표시된다.
- [0071] <제1 변형 예>
- [0072] 도 9a 및 도 9b는, 도 4의 구성과는 상이하고, 생체 정보 센서의 영역이 터치 패널 디스플레이 영역 내의 일부에 존재하는 경우의 구성 예들을 나타낸다.
- [0073] 도 9a에서, 검출 가능 영역(901)은 생체 정보 센서(212)가 생체 정보를 검출할 수 있는 영역이다. 터치 패널 디스플레이의 표시 가능 범위 및 터치 조작 검출 가능 영역(401) 중, 높이 H까지의 부분이 생체 정보 센서(212)의 검출 가능 영역이다.
- [0074] UI(910)는, 애플리케이션(361)의 UI 예이다. 콘트롤들(911 내지 913)은 UI 콘트롤들의 예들이다. 콘트롤(911)은, 생체 정보 센서(212)의 검출 가능 영역 외부에 있기 때문에, 표준 UI 콘트롤이 배치된다. 콘트롤들(912, 913)은, 생체 정보 센서(212)의 검출 가능 영역 내부에 있기 때문에, 통합된 생체 인증의 UI 콘트롤이 배치될 수 있다.
- [0075] <제2 변형 예>
- [0076] 도 9b에서, 검출 가능 영역(921)은 생체 정보 센서(212)의 검출 가능 영역이 보다 한정적인 예이다.
- [0077] UI(930)는 애플리케이션(361)의 UI 예이다. 영역(931)은, 콘트롤들(912 및 913)과 같이, 통합된 생체 인증의 UI 콘트롤이다. 이러한 방식으로, 생체 정보 센서(212)의 검출 가능 영역이 한정적일 경우에는, 통합된 생체 인증의 UI 콘트롤이 배치될 수 있는 위치 및 그 수가 한정된다.
- [0078] 생체 정보 센서(212)의 검출 가능 영역이 한정되어 있는 경우, 또는, 생체 정보 센서(212)가 터치 패널 디스플레이의 터치 조작 검출 가능 영역(401) 및 표시 가능 범위와 관련되지 않은 위치에 독립적으로 제공되는 경우에는, 문제가 일어날 수 있다. 더 구체적으로, 원하는 위치에 통합된 생체 인증의 UI 콘트롤을 배치하는 것, 및 도 7 및 도 8을 참조하여 설명한 통합된 생체 인증의 UI 콘트롤 처리를 적용하는 것이 곤란할 수 있다. 이 문제는, 컴퓨터(111)의 생체 정보 센서(212)의 설치 위치 및 검출 가능 영역과 같은 하드웨어 사양들에 따라 상이하다.
- [0079] 도 10 및 도 11은, 전술한 바와 같이 컴퓨터(111)의 하드웨어 사양들의 차이들로 인해, 통합된 생체 인증의 UI 콘트롤이 사용될 수 없는, 즉 그러한 UI 콘트롤의 구현이 곤란한 경우의 대안의 처리 플로우를 설명한다.
- [0080] 도 11은, 제2 변형 예에서 설명되는 컴퓨터(111) 및 서버(121)에 의한 사용자 조작들을 포함하는 전반적인 처리의 시퀀스를 설명하는 도면이다.
- [0081] 단계 S1101에서, 사용자는 애플리케이션(361)을 조작하여, 애플리케이션의 기동, 또는, 화면 표시를 요구한다. 단계 S1102 내지 단계 S1104는, 도 8을 참조하여 설명한 단계 S802 내지 단계 S804와 유사하므로, 그 설명을 생략한다.
- [0082] 단계 S1105에서, OS(351)는, 컴퓨터(111)의 하드웨어 사양들로서, 통합된 생체 인증의 UI 콘트롤들의 표시 영역에 생체 정보 센서(212)가 있는지를 판정한다. 단계 S1105에서의 판정이 아니오(생체 인증을 통합하는 UI 콘트롤들의 표시 영역에 생체 정보 센서(212)가 없음)인 경우, 단계 S1106에서, 애플리케이션(361)에 UI 콘트롤 묘

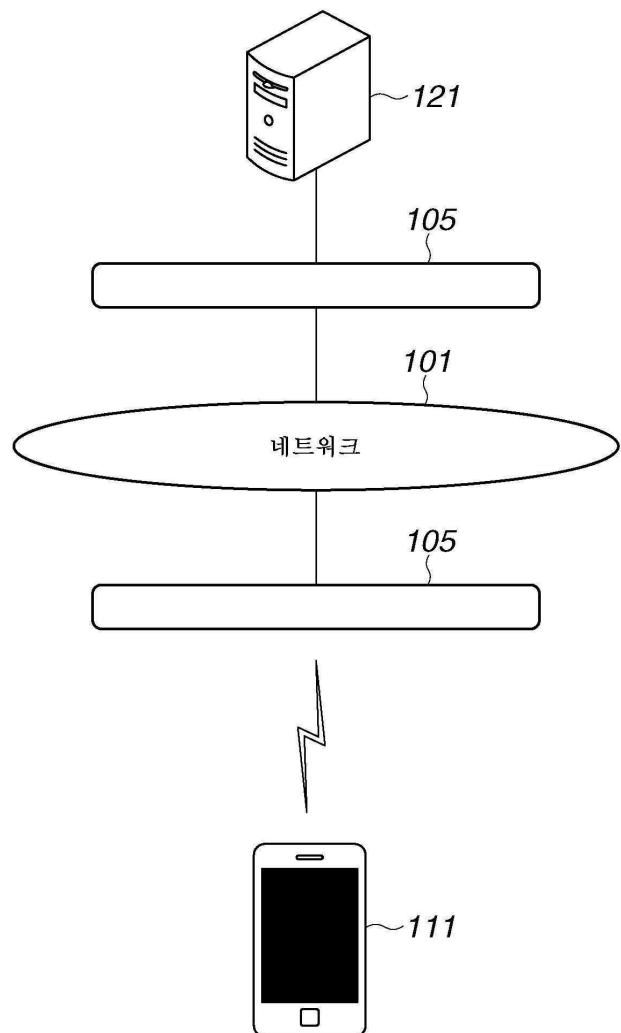
화 요구에 대하여 에러 응답이 반환된다.

- [0083] 단계 S1107에서, 애플리케이션(361)은, 생체 인증용 UI 콘트롤의 생성이 성공했는지를 판정한다. OS(351)로부터 에러 응답이 반환된 경우에, 생체 인증용 UI 콘트롤의 생성이 실패한 것으로 판정된다. 단계 S1107에서의 판정이 아니오인 경우에는, 단계 S1108에서, 애플리케이션(361)은 OS(351)에, 좌표 및 크기가 동일한 채, 표준 UI 콘트롤을 묘화하도록 요구한다.
- [0084] 단계 S1109에서, OS(351)는, 표준 UI 콘트롤을 터치 패널 디스플레이(210)에 묘화한다.
- [0085] 단계 S1110에서, 애플리케이션(361)은, OS(351)에 대하여 관련 UI 콘트롤에 대한 이벤트 청취자를 설정한다.
- [0086] 상기의 처리의 결과로서, 컴퓨터(111)의 터치 패널 디스플레이(210) 상에 도 10의 단계 S1001의 애플리케이션(361)의 UI 화면이 표시된다. 생체 인증 아이콘(512)이 UI 콘트롤들의 임의의 것에 존재하지 않고, 이는 도 7의 단계 S701에서 나타내는 화면과 상이하다.
- [0087] 단계 S1111에서, 사용자가, 도 10의 단계 S1001에서 나타내는 화면 상의 UI 콘트롤들 중 임의의 하나를 조작한다. 더 구체적으로, 도 10의 단계 S1002에서 도시하는 바와 같이, 사용자는 UI 콘트롤을 사용자의 손가락으로 터치한다(누른다).
- [0088] 단계 S1112에서, OS(351)는, 애플리케이션(361)에 UI 콘트롤에의 조작 이벤트를 통지한다. 단계 S1113에서, 애플리케이션(361)은, 이벤트 통지에 응답하여, 사용자 조작의 UI 콘트롤 대상에 대응하는 처리가 수행되는 URL을 수신처로 설정하고, 웹 애플리케이션(311)에 인증 개시 요구를 송신한다.
- [0089] 단계 S1114 내지 단계 S1116은 전술한 단계 S813 내지 단계 S815와 유사하므로, 그 설명을 생략한다. 단계 S1117에서, 웹 애플리케이션(311)은, 애플리케이션(361)에 챌린지 및 RP ID로 응답한다.
- [0090] 단계 S1118에서, 애플리케이션(361)은, 플랫폼 API(352)를 통해 OS(351)에 어설션 요구를 송신한다. 이 때, 챌린지 및 RP ID가 요구에 부가된다.
- [0091] 단계 S1119에서, OS(351)는, 인증자(355)에 생체 인증 요구를 송신한다.
- [0092] 단계 S1120에서, 인증자(355)는, 도 10의 단계 S1003에서 나타낸 바와 같이, 사용자로부터 생체 인증을 요구하기 위한 화면을 컴퓨터(111)의 터치 패널 디스플레이(210) 상에 추가적으로 표시한다. 도 10의 단계 S1004에서 나타낸 바와 같이, 사용자는, 컴퓨터(111)의 생체 정보 센서(212)로 하여금 예를 들어, 사용자의 지문을 판독하게 한다. 사용자의 생체 정보의 입력 작업에 응답하여, 단계 S1121에서 생체 인증이 실행된다. 이후, 단계들은 도 8의 단계 S823 내지 단계 S833과 유사하므로, 그 설명을 생략한다. 본 시퀀스에서, 생체 인증의 결과로서, 처리 결과는 단계 S833에서와 같이, 도 10의 단계 S1005에서 나타낸 바와 같이 표시된다.
- [0093] <적용 예>
- [0094] 이어서, 도 12, 도 13 및 도 14를 참조하여, 생체 인증을 통합한 전술한 UI 콘트롤들이 다른 사용 사례들에 적용되는 적용 예들이 설명된다.
- [0095] 데스크톱 또는 홈 화면의 UI(1200)는, 컴퓨터(111)의 터치 패널 디스플레이(210) 상에 OS(351)에 의해 제공 및 표시된다. 버튼들(1201, 1202)은 버튼형 UI 콘트롤들이다. 버튼(1201)은, 애플리케이션(361)의 기동 버튼이다. 버튼(1202)은, URL 쇼트컷의 기동 버튼이다. 아이콘(1203)은, 도 5를 참조하여 설명된 생체 인증 아이콘(512)이다. 생체 인증 아이콘(1203)의 유/무는 애플리케이션 기동 버튼 또는 URL 쇼트컷 기동 버튼이, 통합된 생체 인증의 UI 콘트롤인지를 나타낸다.
- [0096] UI(1300)는, 애플리케이션 기동 버튼 또는 URL 쇼트컷 기동 버튼에 대하여 생체 인증의 실행을 설정하기 위한 UI이다. 영역(1301)은, "App1"이라고 하는 애플리케이션(361)의 기동 버튼에 대하여 생체 인증의 실행이 설정되는 예이다. "App1"이라고 하는 애플리케이션(361)은, 웹 애플리케이션(311)의 도메인 "foo.com"을, RP ID로서 사용하는 것에 의해 생체 인증 플로우를 사용할 수 있다. 본 실시예에서, 생체 인증의 실행 설정이 오프이어서, UI(1200)의 "App1"의 기동 버튼에는, 생체 인증 아이콘(1203)은 표시되지 않는다. 영역(1302)은, "URL3"이라고 하는 URL 쇼트컷의 기동 버튼에 대하여 생체 인증의 실행이 설정되는 예이다. 영역(1302)에서, "URL3"의 쇼트컷의 수신처 URL은, "https://cn-shop.com/authn"이다. 본 실시예에서, 생체 인증의 실행 설정은 온이어서, UI(1200)의 "URL3"의 기동 버튼에는, 생체 인증 아이콘(1203)이 표시된다. "설정 불가"가 표시되는 애플리케이션 기동 버튼 또는 URL 쇼트컷 기동 버튼은, 생체 인증을 사용하지 않는다.

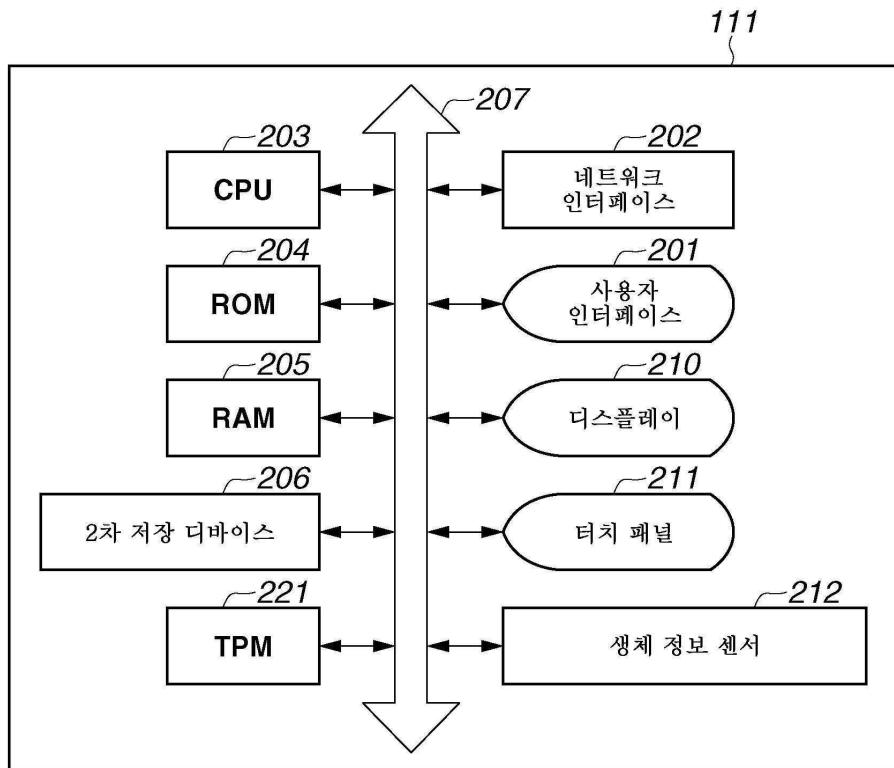
- [0097] 도 14는 애플리케이션 기동 버튼 또는 URL 쇼트컷 기동 버튼이, 통합된 생체 인증의 UI 콘트롤로서 처리되는 경우의 플로우를 설명한다.
- [0098] 단계 S1401에서, OS(351)는, 데스크톱 또는 홈 화면에 표시되는 애플리케이션 또는 URL 쇼트컷의 기동 버튼을 판독하고 또한 UI(1300)에서 나타낸 생체 인증의 실행 설정을 판독한다. 단계 S1402에서, OS(351)는, 생체 인증의 실행 설정이 온으로 설정된 버튼에 대해서는, 생체 인증 아이콘(1203)을 포함한 UI 콘트롤을, 컴퓨터(11 1)의 터치 패널 디스플레이(210) 상에 묘화 및 표시한다. 표시 결과는 도 12에서의 UI(1200)이다.
- [0099] 단계 S1403에서, 사용자는, 애플리케이션 기동 버튼(1201) 또는 URL 쇼트컷 기동 버튼(1202)을 조작하여, 애플리케이션을 기동하거나, 또는 브라우저에 의해 URL 쇼트컷을 개방하도록 요구한다.
- [0100] 단계 S1404에서, 전술한 단계 S808에서와 같이, OS(351)는 넌스를 생성한다. 단계 S1405에서, OS(351)는, 애플리케이션(361)에 UI 콘트롤 조작 이벤트를 통지한다. 이 때, 생성된 넌스가 이벤트에 부가된다.
- [0101] 단계 S1406에서, 애플리케이션(361)은, UI(1300)의 생체 인증의 실행 설정에 기초하여, 관련 기동 버튼의 생체 인증의 실행 설정이 온인 경우, 웹 애플리케이션(311)에 처리 요구로서의 인증 개시 요구를 송신한다. 이 때, 수신된 넌스를 요구에 부가한다. 단계들은 도 8을 참조하여 설명한 단계 S813 내지 단계 S833과 유사하다. 생체 인증 아이콘(1203)의 위치에 대응하는 생체 정보 센서(212)에 의해 판독된 생체 정보에 기초한 생체 인증이 성공적이고, 인증 서버(321)에 의한 검증에도 성공한 경우에, 단계 S1403에서 사용자에 의해 지정된 애플리케이션(361)이 기동되고, 초기 화면이 표시된다.
- [0102] 전술한 바와 같이, 터치 패널 디스플레이 내에 생체 인증 센서가 포함된 부품 디바이스가 사용 가능한 경우, UI 조작과 생체 인증을, 직관적이고 이해하기 쉬운 하나의 UI 조작으로 통합하는 유닛이 제공될 수 있다. 특히, 지정된 UI 콘트롤의 표시 영역 상에 있어서의 조작들에 대해서만, 동시에 생체 인증을 실행하는 유닛이 제공될 수 있다. 따라서, 생체 인증 조작이 수행될 때의 사용자 편리성 및 조작성이 향상될 수 있다.
- [0103] 다른 실시예들
- [0104] 실시예(들)는, 전술한 실시예(들) 중 하나 이상의 기능을 실행하기 위해 저장 매체(보다 완전하게는 '비일시적 컴퓨터 판독가능 저장 매체'라 칭할수도 있음)에 기록된 컴퓨터 실행가능 명령어들(예를 들어, 하나 이상의 프로그램)을 판독 및 실행하고 그리고/또는 전술한 실시예(들) 중 하나 이상의 기능을 실행하는 하나 이상의 회로(예를 들어, 주문형 집적 회로(ASIC))를 포함하는 시스템 또는 장치의 컴퓨터에 의해, 그리고 예를 들어 전술한 실시예(들) 중 하나 이상의 기능을 실행하기 위해 저장 매체로부터 컴퓨터 실행가능 명령어들을 판독 및 실행함으로써 그리고/또는 전술한 실시예(들) 중 하나 이상의 기능을 실행하기 위해 하나 이상의 회로를 제어함으로써 시스템 또는 장치의 컴퓨터에 의해 실행되는 방법에 의해 실현될 수도 있다. 컴퓨터는 하나 이상의 프로세서(예를 들어, 중앙 처리 유닛(CPU), 마이크로 처리 유닛(MPU))를 포함할 수 있고 컴퓨터 실행가능 명령어들을 판독 및 실행하기 위한 별도의 컴퓨터들 또는 별도의 프로세서들의 네트워크를 포함할 수 있다. 컴퓨터 실행가능 명령어들은 예를 들어 네트워크 또는 저장 매체로부터 컴퓨터에 제공될 수 있다. 저장 매체는, 예를 들어 하드 디스크, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 분산형 컴퓨팅 시스템들의 스토리지, 광 디스크(예컨대, 콤팩트 디스크(CD), 디지털 다기능 디스크(DVD) 또는 블루레이 디스크(BD)TM), 플래시 메모리 디바이스, 메모리 카드 등 중 하나 이상을 포함할 수 있다.
- [0105] (기타의 실시예)
- [0106] 본 발명은, 상기의 실시형태의 1개 이상의 기능을 실현하는 프로그램을, 네트워크 또는 기억 매체를 개입하여 시스템 혹은 장치에 공급하고, 그 시스템 혹은 장치의 컴퓨터에 있어서 1개 이상의 프로세서가 프로그램을 읽어 실행하는 처리에서도 실현가능하다.
- [0107] 또한, 1개 이상의 기능을 실현하는 회로(예를 들어, ASIC)에 의해서도 실행가능하다.
- [0108] 예시적인 실시예를 설명하였지만, 개시내용은 개시된 예시적인 실시예들로 한정되지 않음을 이해해야 한다. 이하의 청구항들의 범위는 이러한 모든 변형과 동등한 구조 및 기능을 포함하도록 최광의로 해석되어야 한다.

도면

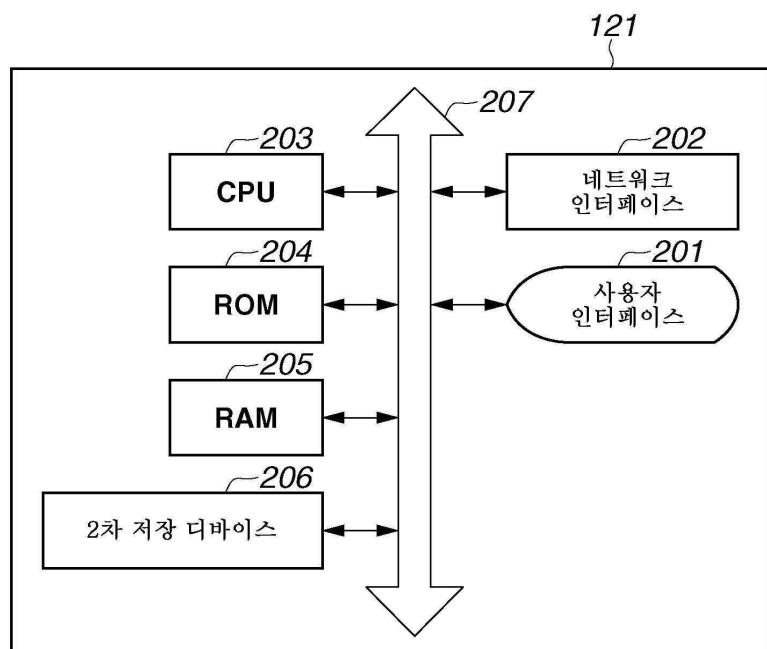
도면1



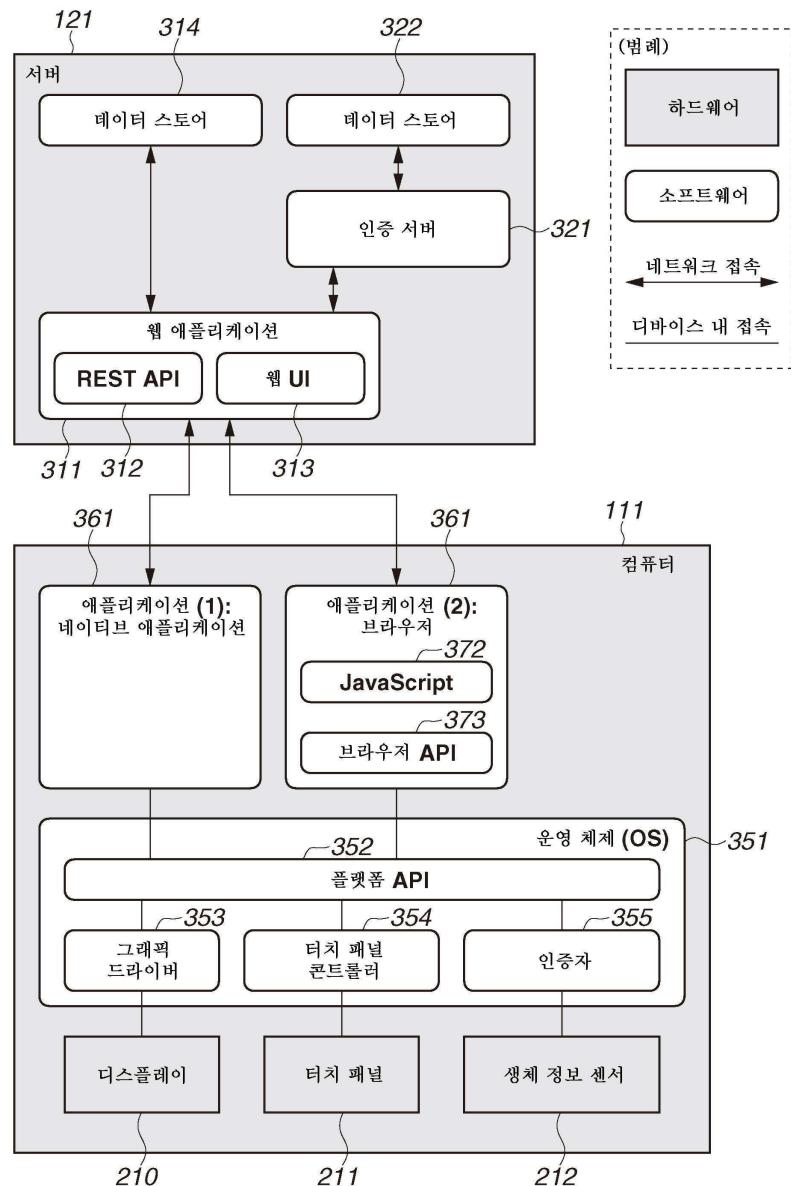
도면2a



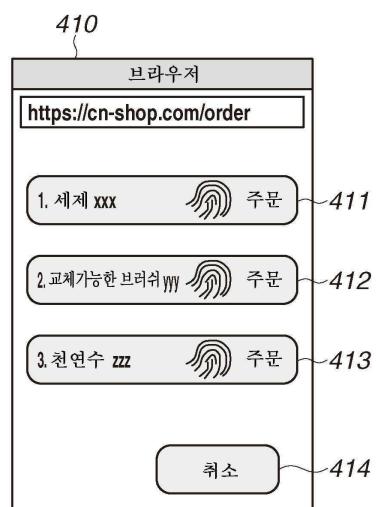
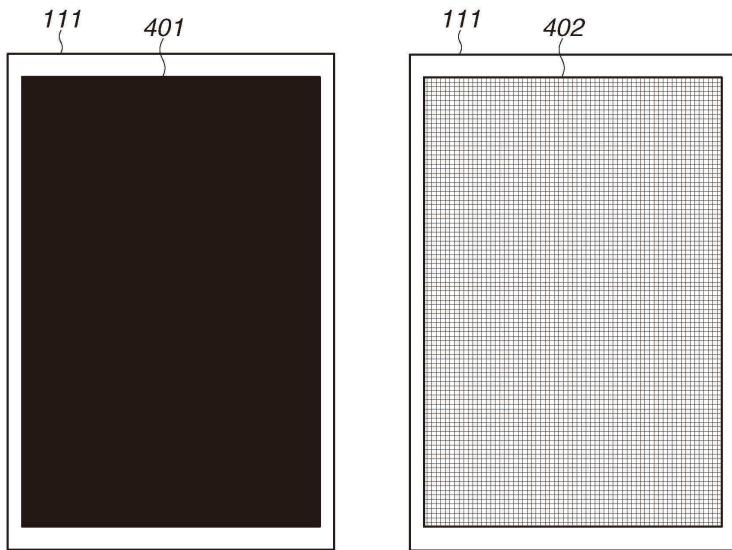
도면2b



도면3



도면4



도면5

500 ~

```
<div align="center">
  <p>“C사의 CameraShot GX”를 ¥59000에 주문했습니다.<br>
  당신이 당신의 주문을 확인하기를 원하는 경우, 당신의 계좌에 등록된 생체 인증을 수행해주세요.<br>
</p>
```

501 ~

```
<input type="button" name="button1" value="주문 확인" style="WIDTH: 120px; HEIGHT: 120px" data-bioauth="required" data-bioauth-pid="cr-shop.com" onclick="callBioauthn()"/>
```

502 ~

```
<input type="button" name="button2" value="CANCEL" onclick="location.href='cancelledhtml'">
</div>
```

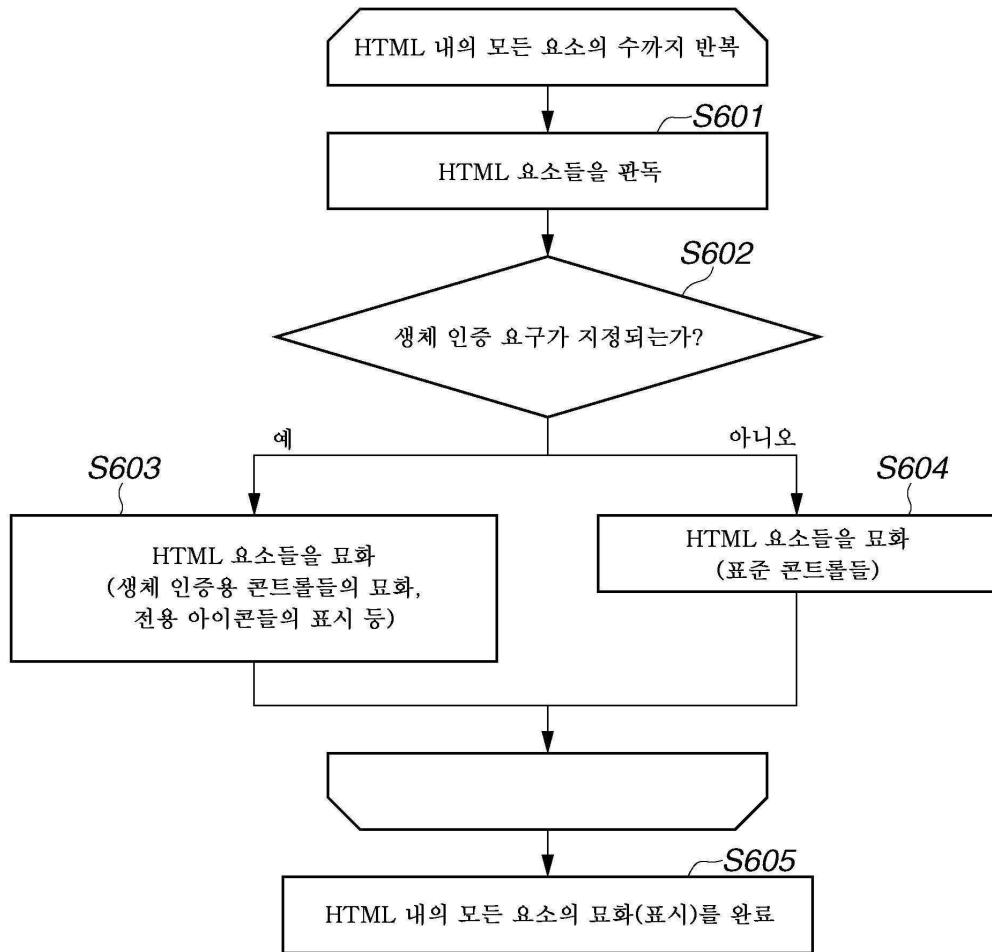
510 ~

https://cr-shop.com/confirm	브라우저
---	------

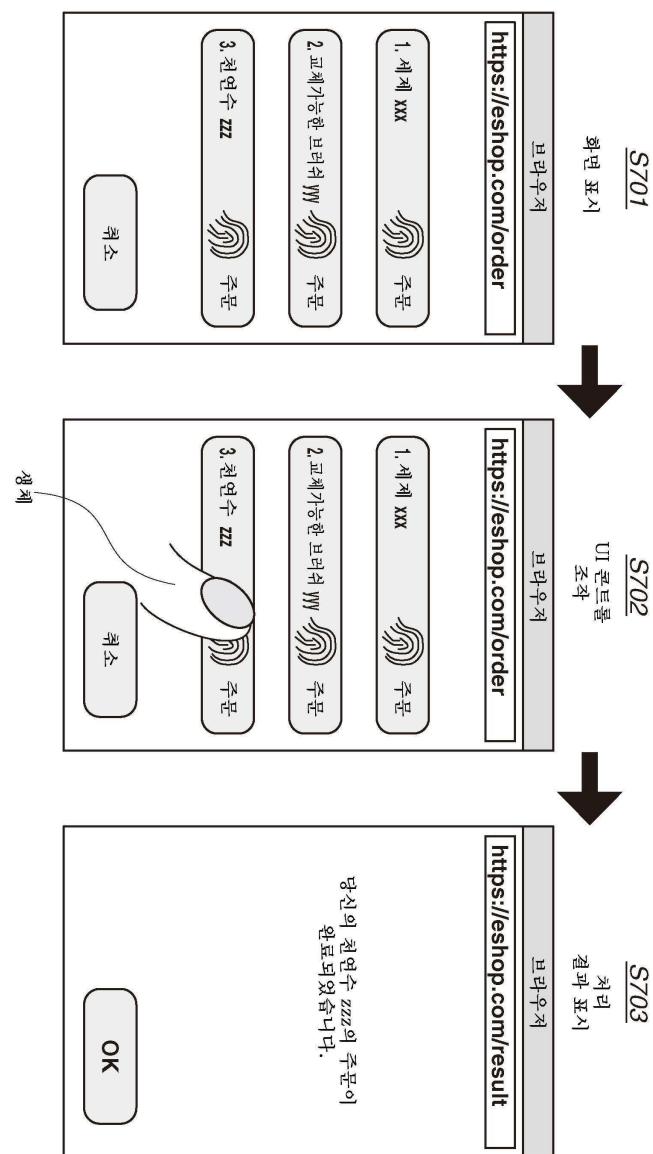
512 ~

511 513

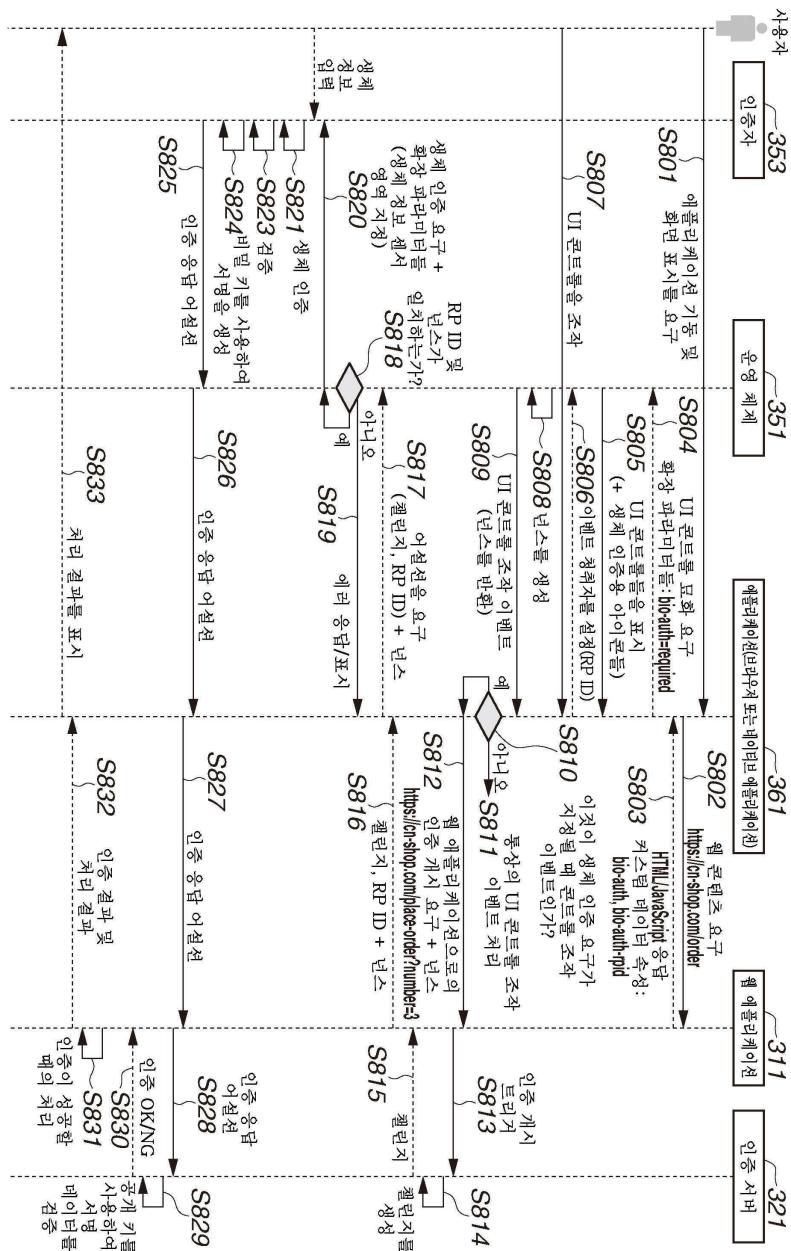
도면6



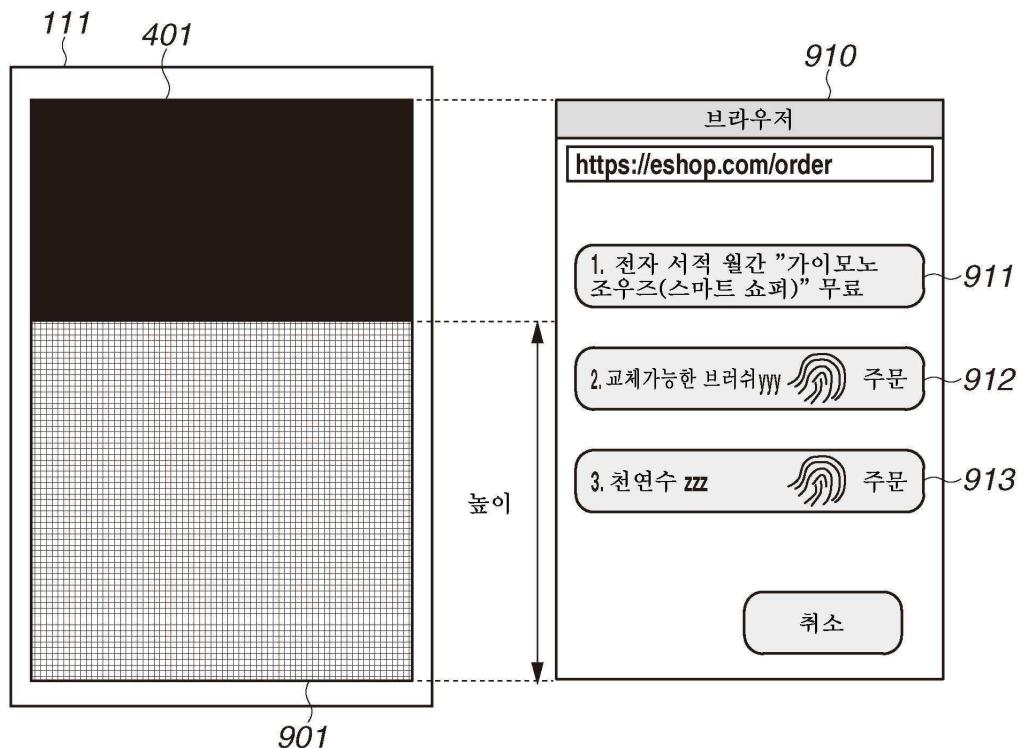
도면7



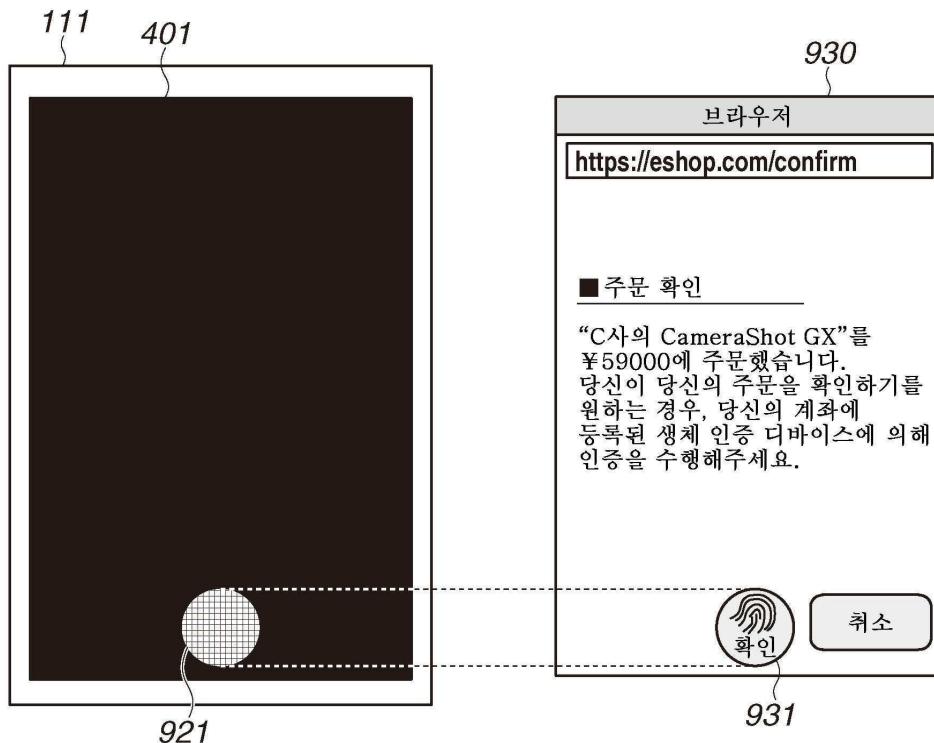
도면8



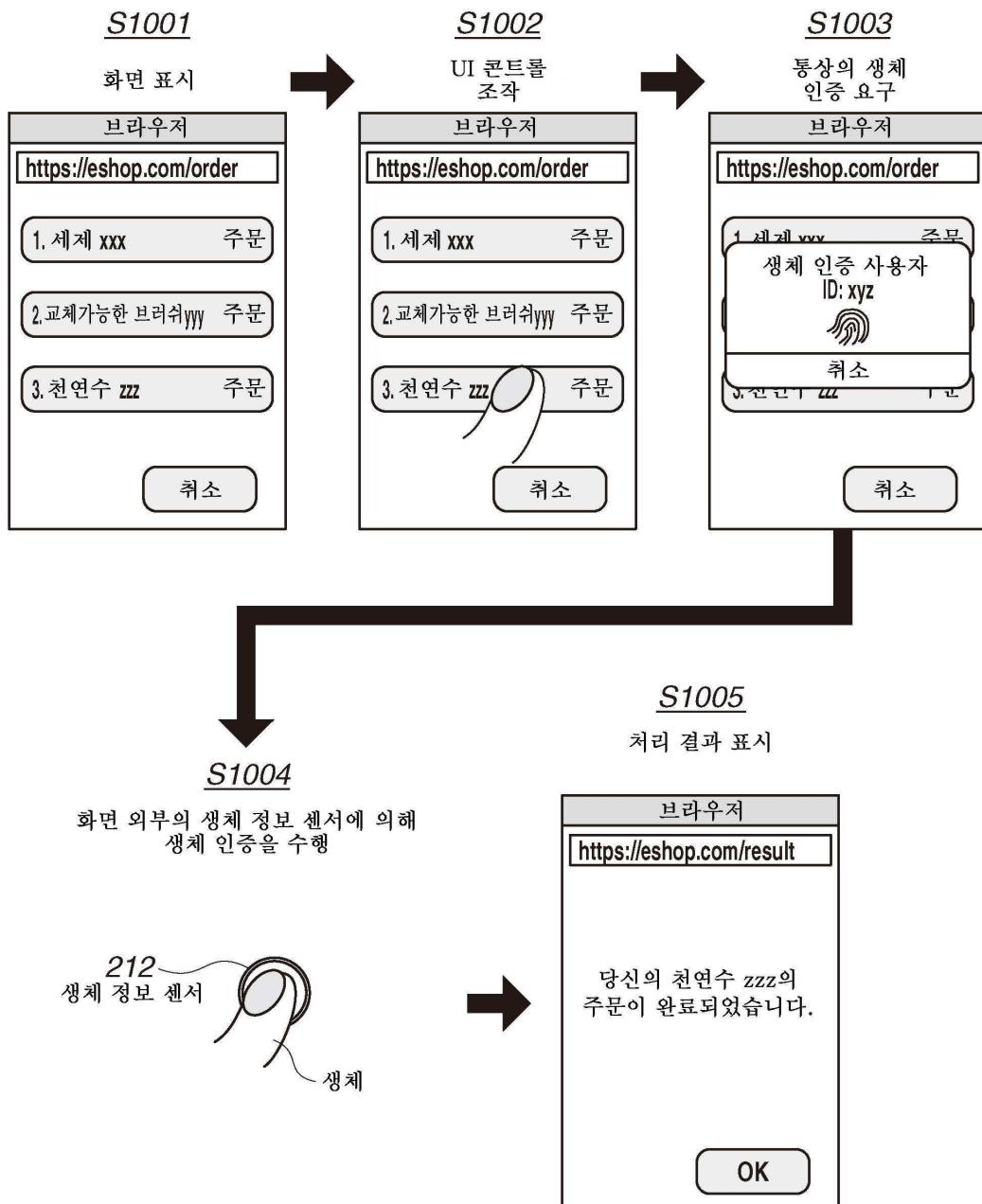
도면9a



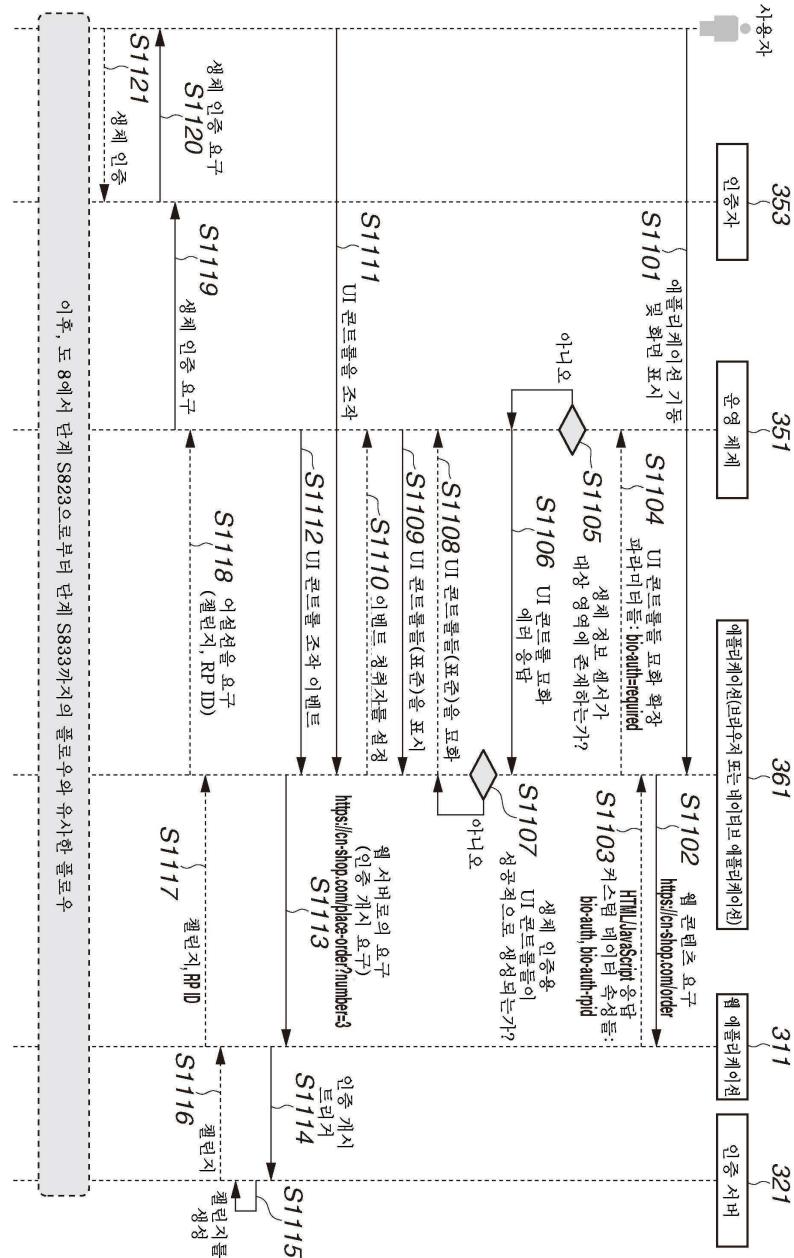
도면9b



도면10

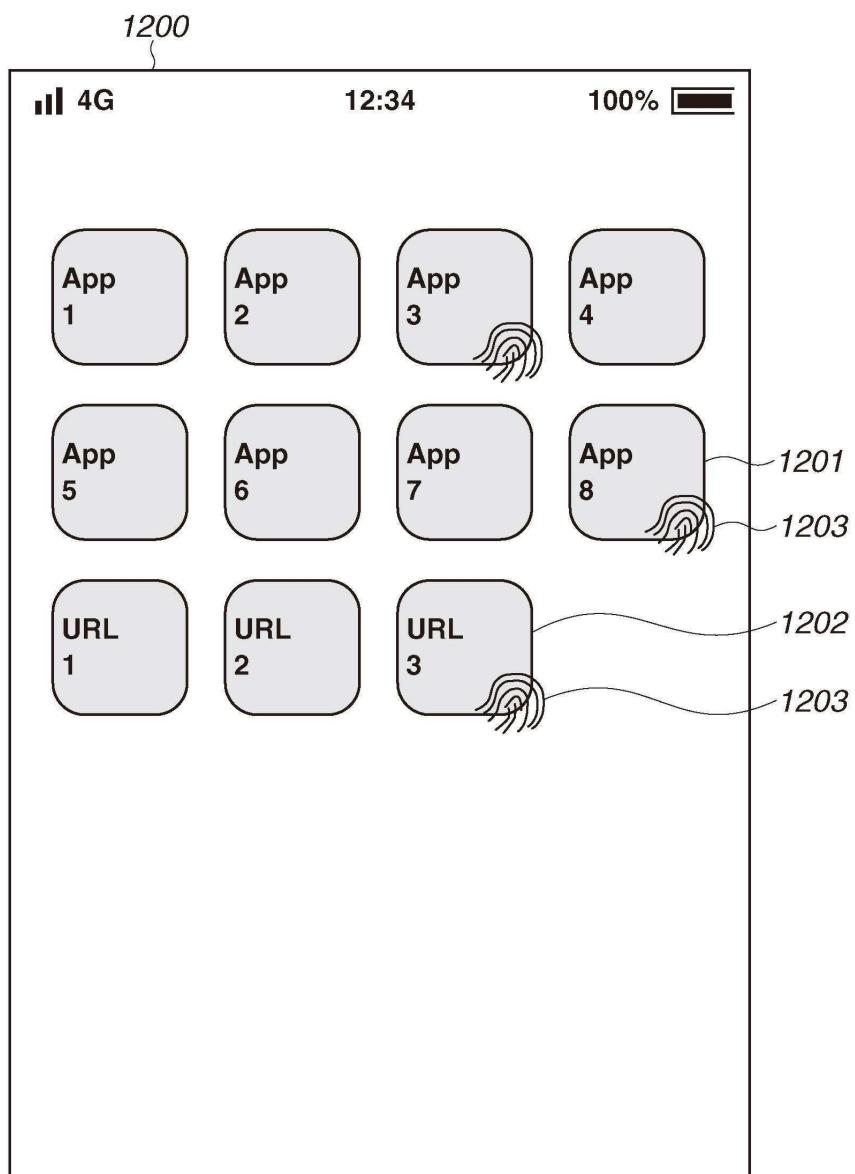


도면11



이후, 도 8에서 단계 S823으로부터 단계 S833까지의 플로우와 유사한 플로우

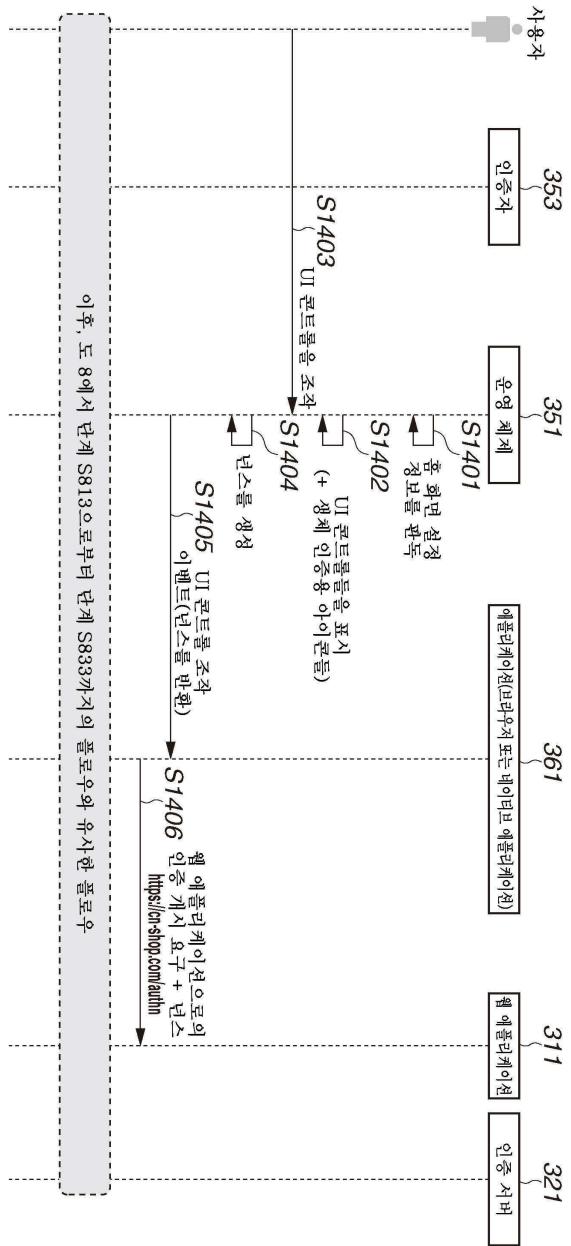
도면12



도면13

1300	
1301～	
1302～	
4G	12:34
100%	
< 설정	생체 인증의 실행
애플리케이션 기동 버튼	
App1 RPID: foo.com	<input checked="" type="checkbox"/> <small>온</small> <small>오프</small>
App2	설정 불가
App3 RPID: bar.com	<input checked="" type="checkbox"/> <small>온</small> <small>오프</small>
App4 RPID: dot.com	<input checked="" type="checkbox"/> <small>온</small> <small>오프</small>
App5	설정 불가
App6	설정 불가
App7	설정 불가
App8 RPID: cn-shop.com	<input checked="" type="checkbox"/> <small>온</small> <small>오프</small>
URL 쇼트컷	
URL1 https://vit.ly/wn89y	설정 불가
URL2 https://raku-shop.com	<input checked="" type="checkbox"/> <small>온</small> <small>오프</small>
URL3 https://cn-shop.com/authn	<input checked="" type="checkbox"/> <small>온</small> <small>오프</small>

도면14



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 3

【변경점】

제1학기에 있어서

상기 콜트롤에 대한 상기 사용자 조작에 응답하여 생성된 제1 결론 데이터가 상기 첫째 요구에 부가되고

상기 처리 요구의 상기 요구처로부터 상기 제1 검증 데이터를 포함하는 인증 요구가 만들어진 경우에, 상기 인증 모듈에 의해 상기 생체 인증이 실행되는 정보 처리 장치

【별경후】

제1항에 있어서.

상기 쿠트롤에 대한 상기 사용자 조작에 응답하여 생성된 제1 결합 데이터가 상기 처리 용도에 복가되고,

상기 처리 요구의 요구처록부터 상기 제1 검증 데이터를 포함하는 임출 요구가 만들어진 경우에, 상기 임

증 모듈에 의해 상기 생체 인증이 실행되는, 정보 처리 장치.

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 10

【변경전】

컴퓨터가, 생체 인증을 위한 인증 모듈, 템퍼 저항성을 갖는 저장 영역, 디스플레이, 그리고, 사용자의 생체 정보를 판독하는 생체 정보 센서이며 상기 디스플레이 상의 조작 영역 중 적어도 일부인 판독 가능 영역 내의 생체 정보를 판독하도록 구성된 생체 정보 센서를 포함하는 정보 처리 장치에 대한 방법을 실행하게 하기 위한 컴퓨터 프로그램이 저장되는 비일시적 컴퓨터 판독 가능 저장 매체로서, 상기 방법은,

사용자 조작을 접수하기 위한 콘트롤의 생성 명령에 따라, 상기 생체 인증이 요구되는 것을 나타내는 정보가 부가되는 상태에서의 상기 콘트롤을, 상기 디스플레이에 표시하는 단계로, 상기 콘트롤의 상기 생성 명령은 네트워크를 통해 상기 정보 처리 장치와 통신하는 웹 애플리케이션으로부터 제공되는 단계;

상기 표시된 콘트롤에 대한 상기 사용자 조작이 검출될 때, 상기 콘트롤에 대응하는 처리 요구를 상기 웹 애플리케이션을 포함하는 시스템에 송신하는 단계; 및

상기 사용자 조작의 대상인 상기 콘트롤이 표시되는 위치에서 상기 생체 정보 센서를 통해 판독된 생체 정보와, 상기 저장 영역에 저장되는 상기 생체 정보를 사용하여 상기 인증 모듈에 의해 실행된 상기 생체 인증의 결과에 기초하는 데이터를, 상기 시스템에 송신하는 단계

를 포함하고,

상기 처리 요구 및 상기 생체 인증의 상기 결과에 기초하는 상기 데이터에 따라, 상기 콘트롤에 대응하는 처리에 관한 정보가 상기 디스플레이에 표시되고,

상기 표시된 콘트롤은 상기 생체 정보 센서의 상기 판독 가능 영역 내에 배치 및 표시되는, 비일시적 컴퓨터 판독 가능 저장 매체.

【변경후】

컴퓨터가, 생체 인증을 위한 인증 모듈, 템퍼 저항성을 갖는 저장 영역, 디스플레이, 그리고, 사용자의 생체 정보를 판독하는 생체 정보 센서이며 상기 디스플레이 상의 조작 영역 중 적어도 일부인 판독 가능 영역 내의 생체 정보를 판독하도록 구성된 생체 정보 센서를 포함하는 정보 처리 장치에 대한 방법을 실행하게 하기 위한 컴퓨터 프로그램이 저장되는 비일시적 컴퓨터 판독 가능 저장 매체로서, 상기 방법은,

사용자 조작을 접수하기 위한 콘트롤의 생성 명령에 따라, 상기 생체 인증이 요구되는 것을 나타내는 정보가 부가되는 상태에서의 상기 콘트롤을, 상기 디스플레이에 표시하는 단계로, 상기 콘트롤의 상기 생성 명령은 네트워크를 통해 상기 정보 처리 장치와 통신하는 웹 애플리케이션으로부터 제공되는 단계;

상기 표시된 콘트롤에 대한 상기 사용자 조작이 검출될 때, 상기 콘트롤에 대응하는 처리 요구를 상기 웹 애플리케이션을 포함하는 시스템에 송신하는 단계; 및

상기 사용자 조작의 대상인 상기 콘트롤이 표시되는 위치에서 상기 생체 정보 센서를 통해 판독된 생체 정보와, 상기 저장 영역에 저장되는 상기 생체 정보를 사용하여 상기 인증 모듈에 의해 실행된 상기 생체 인증의 결과에 기초하는 데이터를, 상기 시스템에 송신하는 단계

를 포함하고,

상기 처리 요구 및 상기 생체 인증의 상기 결과에 기초하는 상기 데이터에 따라, 상기 콘트롤에 대응하는 처리에 관한 정보가 상기 디스플레이에 표시되고,

상기 표시된 콘트롤은 상기 생체 정보 센서의 상기 판독 가능 영역 내에 배치 및 표시되는, 비일시적 컴퓨터 판독 가능 저장 매체.