



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년12월27일
(11) 등록번호 10-0788904
(24) 등록일자 2007년12월18일

(51) Int. Cl.

H04Q 7/38 (2006.01) H04L 9/32 (2006.01)

H04Q 7/24 (2006.01)

(21) 출원번호 10-2006-0122912

(22) 출원일자 2006년12월06일

심사청구일자 2006년12월06일

(56) 선행기술조사문헌

JP2006106928 A

(뒷면에 계속)

(73) 특허권자

한국전자통신연구원

대전 유성구 가정동 161번지

(72) 발명자

전중홍

대전 유성구 전민동 엑스포아파트 209동 1603호

이원석

대전 서구 도마2동 경남아파트 114동 506호

(뒷면에 계속)

(74) 대리인

유미특허법인

전체 청구항 수 : 총 15 항

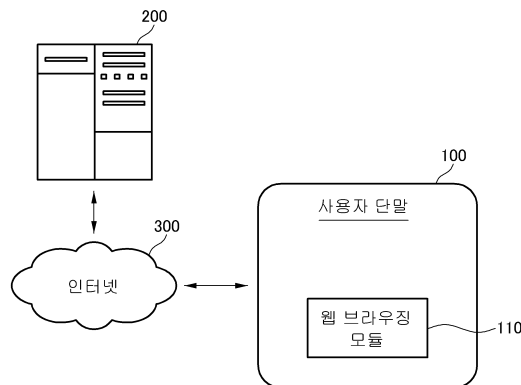
심사관 : 마정윤

(54) 신뢰 링크 인증 시스템과 그의 인증 방법 및 인증 표시방법

(57) 요약

신뢰 링크 인증 시스템에서, 단말은 웹 서버로부터 수신된 웹 페이지를 파싱하여 신뢰 링크에 대한 마크업 정보를 추출한다. 그리고 추출된 마크업 정보를 신뢰 링크 인증 서버로 전송한다. 신뢰 링크 인증 서버는 단말로부터 전송된 신뢰 링크의 마크업 정보로부터 신뢰 링크에 대한 인증 확인을 수행한 후 인증 확인 결과를 단말로 전송한다. 단말은 신뢰 링크 인증 서버로부터 수신한 인증 확인 결과에 따라 인증 확인된 신뢰 링크에는 신뢰 마크를 표시하고 웹 페이지를 렌더링하여 사용자에게 표시한다.

대표도 - 도1



(72) 발명자

이강찬

대전 중구 태평2동 버드내아파트 217동 904호

이승윤

대전 유성구 지족동 열매마을아파트 202동 808호

인민교

대전 유성구 가정동 236-1

유태완

대전 유성구 노은동 499-5번지 401호

장인동

대전 유성구 신성동 140-12

(56) 선행기술조사문헌

KR100704000 B1

KR1020000036707 A

KR1020020020400 A

JP2006313517 A

특허청구의 범위

청구항 1

단말이 웹 서버로부터 요청한 웹 페이지에 인증된 신뢰 링크를 표시하는 방법에 있어서,
 상기 웹 페이지를 파싱하여 신뢰 링크에 대한 마크업 정보를 추출하는 단계;
 상기 추출된 마크업 정보를 이용하여 상기 신뢰 링크에 대한 인증 확인을 요청하는 단계;
 상기 인증 확인된 신뢰 링크에 신뢰 마크를 표시하는 단계; 및
 상기 신뢰 마크가 표시된 신뢰 링크를 포함하는 웹 페이지를 렌더링하여 표시하는 단계
 를 포함하는 신뢰 링크 인증 표시 방법.

청구항 2

제1항에 있어서,
 상기 인증 확인이 되지 않은 신뢰 링크에 대해 비신뢰 마크를 표시하는 단계
 를 더 포함하는 신뢰 링크 인증 표시 방법.

청구항 3

제2항에 있어서,
 상기 인증 확인 여부에 따라 상기 신뢰 링크를 포함하는 웹 페이지의 URL(Uniform Resource Locator) 주소 표시
 창에 신뢰 마크 또는 비신뢰 마크를 표시하는 단계
 를 더 포함하는 신뢰 링크 인증 표시 방법.

청구항 4

제2항에 있어서,
 상기 인증 확인 여부에 따라 상기 웹 페이지에 포함된 전송 버튼에 신뢰 마크 또는 비신뢰 마크를 표시하는 단
 계
 를 더 포함하는 신뢰 링크 인증 표시 방법.

청구항 5

제2항에 있어서,
 상기 비신뢰 마크가 표시된 신뢰 링크의 링크 연결을 차단하는 단계
 를 더 포함하는 신뢰 링크 인증 표시 방법.

청구항 6

제2항에 있어서,
 상기 비신뢰 마크가 표시된 신뢰 링크를 포함하는 웹 페이지에서 사용자 정보가 입력되는 입력창에 경고 문구를
 표시하는 단계
 를 더 포함하는 신뢰 링크 인증 표시 방법.

청구항 7

다수의 단말과 인터넷을 통해 접속되어 있는 신뢰 링크 인증 서버에서 상기 단말로부터 요청된 웹 페이지의 신
 뢰 링크를 인증하는 방법에 있어서,
 상기 다수의 단말 중 상기 신뢰 링크 등록자의 단말로부터 상기 인터넷을 통해 입력받은 상기 웹 페이지의 신뢰

링크 인증 정보를 등록하는 단계;

상기 다수의 단말 중 상기 신뢰 링크 인증 요청자의 단말로부터 상기 신뢰 링크에 대한 인증 확인을 요청받는 단계;

상기 등록된 신뢰 링크 인증 정보에 기초하여 상기 단말이 요청한 신뢰 링크에 대한 인증 확인을 수행하는 단계; 및

상기 인증 확인 결과를 상기 단말로 전송하는 단계

를 포함하는 신뢰 링크 인증 방법.

청구항 8

제7항에 있어서,

상기 신뢰 링크 인증 정보를 등록하는 단계는,

상기 신뢰 링크 등록자에 대한 사용자 인증을 수행하는 단계;

상기 인증된 신뢰 링크 등록자로부터 신뢰 링크 인증 정보를 입력받는 단계;

상기 입력된 신뢰 링크 인증 정보의 중복 여부를 확인하는 단계; 및

상기 입력된 신뢰 링크 인증 정보가 중복되지 않을 경우 상기 신뢰 링크 인증 정보를 등록하는 단계

를 포함하는 신뢰 링크 인증 방법.

청구항 9

제8항에 있어서,

상기 입력된 신뢰 링크 인증 정보가 중복되는 경우 상기 신뢰 링크 인증 정보의 수정 여부에 따라 상기 신뢰 링크 인증 정보를 수정하는 단계

를 더 포함하는 신뢰 링크 인증 방법.

청구항 10

제7항 내지 제9항 중 어느 한 항에 있어서,

상기 신뢰 링크 인증 정보는 링크 연결 IP 목록, 링크 연결 키워드 목록, 허가된 웹 서버의 IP 목록 및 허가된 웹 서버의 URL(Uniform Resource Locator) 목록 중 적어도 하나를 포함하는 신뢰 링크 인증 방법.

청구항 11

웹 서버로부터 요청한 웹 페이지에 신뢰 링크를 표시하는 단말에 있어서,

상기 웹 페이지를 파싱하여 신뢰 링크를 추출하고, 인증이 확인된 신뢰 링크에 신뢰 마크를 표시하고, 인증이 확인되지 않은 신뢰 링크에 비신뢰 마크를 표시하는 렌더링 엔진부;

상기 추출된 신뢰 링크에 대한 인증 확인을 요청하고, 인증 확인 결과를 상기 렌더링 엔진부로 전달하는 신뢰 링크 확인부; 및

상기 렌더링 엔진부에 의해 신뢰 마크가 표시된 신뢰 링크를 포함하는 웹 페이지를 표시하는 그래픽 인터페이스부

를 포함하는 단말.

청구항 12

제11항에 있어서,

상기 렌더링 엔진부는,

상기 신뢰 마크가 표시된 신뢰 링크를 포함하는 웹 페이지의 URL(Uniform Resource Locator) 주소 입력창에 신

뢰 마크를 표시하고, 비신뢰 마크가 표시된 신뢰 링크를 포함하는 웹 페이지의 URL 주소 입력창에 비신뢰 마크를 표시하는 단말.

청구항 13

제12항에 있어서,

상기 웹 페이지에는 상기 웹 페이지를 기술하는 마크업 언어에 상기 신뢰 링크를 나타내는 특정 태그 또는 속성 정보가 표시되어 있으며,

상기 렌더링 엔진부는 상기 특정 태그 또는 속성값으로부터 상기 신뢰 링크를 추출하는 단말.

청구항 14

단말로부터 요청된 웹 페이지의 신뢰 링크를 인증하는 신뢰 링크 인증 서버에 있어서,

상기 신뢰 링크의 등록을 요청하는 신뢰 링크 등록자를 인증하는 사용자 인증부;

상기 신뢰 링크 등록자 정보 및 신뢰 링크 인증 정보를 저장하고 있는 등록 정보 저장부;

상기 신뢰 링크 등록자로부터 상기 신뢰 링크 인증 정보를 입력받아 상기 등록 정보 저장부에 저장하는 등록 정보 입력부; 및

상기 저장된 신뢰 링크 인증 정보에 기초하여 상기 단말로부터 요청된 웹 페이지의 신뢰 링크를 인증하여 상기 단말로 알려주는 신뢰 링크 인증 처리부

를 포함하는 신뢰 링크 인증 서버.

청구항 15

제14항에 있어서,

상기 등록 정보 입력부는,

상기 신뢰 링크 등록자로부터 입력받은 상기 신뢰 링크 인증 정보의 중복 여부를 확인하고, 상기 신뢰 링크 인증 정보를 수정하는 신뢰 링크 인증 서버.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <9> 본 발명은 신뢰 링크 인증 시스템과 그의 인증 방법 및 인증 표시 방법에 관한 것이다.
- <10> 오늘날 많은 사람들은 데스크탑을 비롯하여 휴대폰, TV에 이르기까지 다양한 단말을 이용하여 인터넷을 이용하고 있다. 사용자는 브라우징 페이지의 주소 입력 창에 URL(Uniform Resource Locator)을 입력하거나, 사용자에게 전달된 전자 우편의 링크를 클릭하여 인터넷 상의 여러 웹 사이트에 접속할 수 있다. 이러한 접속을 통해 생성된 웹 페이지는 사용자에게 사용자 아이디, 비밀번호, 이름, 신용 카드 번호, 주민등록번호 등과 같은 개인 정보를 입력하도록 요구하게 된다. 그런데 이러한 개인 정보를 속임수에 의한 방법으로 가로채어 악용하기 위한 피싱(phishing)과 같은 악의적인 방법들이 등장하기 시작했다.
- <11> 피싱은 특정한 사이트 또는 웹 페이지를 유사하게 만든 사이트 또는 웹 페이지로 사용자들을 유도하고, 사용자들에게 암호, 카드 비밀번호와 같은 중요한 개인 정보를 입력하도록 유도함으로써 사용자 정보를 가로채기 위한 방법이다.
- <12> 일반적으로 웹 브라우징은 특정 웹 페이지 내의 내용들을 렌더링하여 보여주면서 이미지, 동영상, 텍스트 등의 내용과 함께 하이퍼링크로 표현된 링크들을 보여주게 된다. 그러나 웹 브라우징에서 하이퍼링크를 표현할 때, 하이퍼링크에 대한 URI(Universal Resource Identifier)와 함께 표현되도록 지정된 단어 또는 문장을 주로 표현하게 되며, 링크된 URI에 대한 정보는 부가 정보로 표현하게 된다. 따라서 사용자는 현재 보여지고 있는 웹 사

이트가 합법적인 콘텐츠를 표현하고 있는 합법적인 웹 사이트인지, 특정 하이퍼링크가 합법 서버를 지정하고 있는 링크인지를 쉽게 판단할 수 없다. 이러한 상태에서 피싱의 방법을 사용하여 사용자로 하여금 불법 웹 사이트로 접속을 유도하면, 사용자는 쉽게 불법 웹 사이트에 접속할 수 있다. 이로 인하여 개인 식별 정보가 쉽게 유출될 수가 있다.

발명이 이루고자 하는 기술적 과제

- <13> 본 발명이 이루고자 하는 기술적 과제는 사용자의 개인 정보의 유출을 방지할 수 있는 신뢰 링크 인증 시스템과 그의 인증 방법 및 인증 표시 방법을 제공하는 것이다.

발명의 구성 및 작용

- <14> 본 발명의 한 실시 예에 따르면, 단말이 웹 서버로부터 요청한 웹 페이지에 신뢰 링크를 표시하는 방법이 제공된다. 이 방법은 상기 웹 페이지를 파싱하여 신뢰 링크에 대한 마크업 정보를 추출하는 단계; 상기 추출된 마크업 정보를 이용하여 상기 신뢰 링크에 대한 인증 확인을 요청하는 단계; 상기 인증 확인된 신뢰 링크에 신뢰 마크를 표시하는 단계; 및 상기 신뢰 마크가 표시된 신뢰 링크를 포함하는 웹 페이지를 렌더링하여 표시하는 단계를 포함한다.
- <15> 본 발명의 다른 실시 예에 따르면, 다수의 단말과 인터넷을 통해 접속되어 있는 신뢰 링크 인증 서버에서 상기 단말로부터 요청된 웹 페이지의 신뢰 링크를 인증하는 방법이 제공된다. 이 방법은, 상기 다수의 단말 중 상기 신뢰 링크 등록자의 단말로부터 상기 인터넷을 통해 입력받은 상기 웹 페이지의 신뢰 링크 인증 정보를 등록하는 단계; 상기 다수의 단말 중 상기 신뢰 링크 인증 요청자의 단말로부터 상기 신뢰 링크에 대한 인증 확인을 요청받는 단계; 상기 등록된 신뢰 링크 인증 정보에 기초하여 상기 단말이 요청한 신뢰 링크에 대한 인증 확인을 수행하는 단계; 및 상기 인증 확인 결과를 상기 단말로 전송하는 단계를 포함한다.
- <16> 본 발명의 또 다른 실시 예에 따르면, 웹 서버로부터 요청한 웹 페이지에 신뢰 링크를 표시하는 단말이 제공된다. 이 단말은 상기 웹 페이지를 파싱하여 신뢰 링크를 추출하고, 인증이 확인된 신뢰 링크에 신뢰 마크를 표시하고, 인증이 확인되지 않은 신뢰 링크에 비신뢰 마크를 표시하는 렌더링 엔진부; 상기 추출된 신뢰 링크에 대한 인증 확인을 요청하고, 인증 확인 결과를 상기 렌더링 엔진부로 전달하는 신뢰 링크 확인부; 및 상기 렌더링 엔진부에 의해 신뢰 마크가 표시된 신뢰 링크를 포함하는 웹 페이지를 표시하는 그래픽 인터페이스부를 포함한다.
- <17> 본 발명의 또 다른 실시 예에 따르면, 단말로부터 요청된 웹 페이지의 신뢰 링크를 인증하는 신뢰 링크 인증 서버가 제공된다. 이 신뢰 링크 인증 서버는 상기 신뢰 링크의 등록을 요청하는 신뢰 링크 등록자를 인증하는 사용자 인증부; 상기 신뢰 링크 등록자 정보 및 신뢰 링크 인증 정보를 저장하고 있는 등록 정보 저장부; 상기 신뢰 링크 등록자로부터 상기 신뢰 링크 인증 정보를 입력받아 상기 등록 정보 저장부에 저장하는 등록 정보 입력부; 및 상기 저장된 신뢰 링크 인증 정보에 기초하여 상기 단말로부터 요청된 웹 페이지의 신뢰 링크를 인증하여 상기 단말로 알려주는 신뢰 링크 인증 처리부를 포함한다.
- <18> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- <19> 명세서 및 청구범위 전체에서, 어떤 부분이 어떤 구성 요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 각 블록은 특정한 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.
- <20> 이제 본 발명의 실시 예에 따른 신뢰 링크 인증 시스템과 그의 인증 방법 및 인증 표시 방법에 대하여 도면을 참고로 하여 상세하게 설명한다.
- <21> 도 1은 본 발명의 실시 예에 따른 신뢰 링크 인증 시스템을 개략적으로 나타낸 도면이고, 도 2는 도 1에 도시된 웹 브라우징 모듈(110)을 개략적으로 나타낸 도면이다. 그리고 도 3은 도 1에 도시된 신뢰 링크 인증 서버를 개략적으로 나타낸 도면이다.

- <22> 도 1에 나타난 바와 같이, 신뢰 링크 인증 시스템은 웹 브라우징 모듈(110)을 탑재하는 사용자 단말(100) 및 신뢰 링크 인증 서버(200)를 포함한다. 이때, 사용자 단말(100)과 신뢰 링크 인증 서버(200)는 인터넷(300)을 통해 접속될 수 있다.
- <23> 그리고 도 2를 보면, 웹 브라우징 모듈(110)은 렌더링 엔진부(111), 신뢰 링크 확인부(112) 및 그래픽 인터페이스부(113)를 포함한다. 렌더링 엔진부(111)는 인터넷을 통해 수신된 웹 페이지를 파싱하여 신뢰 링크만을 추출한다. 즉, 웹 페이지에는 웹 페이지를 기술하는 마크업 언어인 HTML(HyperText Markup Language), XHTML(eXtensible HTML), cHTML(compact HTML), WML(Wireless Markup Language) 등에 신뢰 링크를 표현하는 특정한 태그 또는 속성 값이 표시되어 있다. 따라서, 렌더링 엔진부(111)는 파싱된 웹 페이지에서 신뢰 링크를 표현하는 마크업 정보에 기초하여 신뢰 링크를 추출할 수 있다.
- <24> 그리고 렌더링 엔진부(111)는 인증 확인된 신뢰 링크에 신뢰 마크를 표시하고, 인증 확인이 되지 않은 신뢰 링크에 비신뢰 마크를 표시한다. 이때, 렌더링 엔진부(111)는 비신뢰 마크가 표시된 신뢰 링크에 대해서는 링크 연결이 되지 않도록 링크 연결을 차단할 수도 있으며, 상기 비신뢰 마크가 표시된 신뢰 링크를 포함하는 웹 페이지에서 사용자 정보가 입력되는 입력창에 경고 문구를 표시할 수도 있다. 신뢰 링크 확인부(112)는 추출된 신뢰 링크에 대한 인증 확인을 신뢰 링크 인증 서버(200)로 요청하고, 신뢰 링크 인증 서버(200)로부터 인증 확인 결과를 렌더링 엔진부(111)로 전달한다. 그래픽 인터페이스부(113)는 신뢰 마크가 표시된 신뢰 링크를 사용자 화면에 표시한다.
- <25> 신뢰 링크 인증 서버(200)는 신뢰 링크에 대한 인증 정보를 기록, 보관 및 제공하는 기능을 수행한다. 이러한 신뢰 링크 인증 서버(200)는 도 3에 나타난 바와 같이, 신뢰 링크 인증 서버(200)는 사용자 인증부(210), 등록 정보 입력부(220), 신뢰 링크 인증 처리부(230) 및 인증 정보 저장부(240)를 포함한다.
- <26> 사용자 인증부(210)는 신뢰 링크에 대한 인증 등록 요청 페이지를 요청한 신뢰 링크 등록자에 대한 인증을 수행한다. 등록 정보 입력부(220)는 인증이 확인된 신뢰 링크 등록자로부터 신뢰 링크 인증 정보를 입력받고, 입력받은 신뢰 링크 등록 정보의 중복 여부를 확인한 후 인증 정보 저장부(240)에 신뢰 링크 인증 정보를 저장한다. 신뢰 링크 인증 처리부(230)는 신뢰 링크 확인부(112)로부터 신뢰 링크에 대한 인증 확인을 요청받아 신뢰 링크에 대한 인증 확인을 수행한 후, 그 결과를 신뢰 링크 확인부(112)로 전달한다. 인증 정보 저장부(240)는 등록된 사용자 정보 및 신뢰 링크 인증 정보를 저장하고 있다. 신뢰 링크 인증 정보에는 링크 연결 IP 목록, 링크 연결 키워드 목록, 허가된 웹 서버의 IP 목록, 허가된 웹 서버의 URL 목록 및 사용 제한 여부 정보 등이 있을 수 있다.
- <27> 도 4는 도 1에 도시된 웹 브라우징 모듈(110)의 동작을 나타낸 도면이고, 도 5a 및 도 5b는 각각 신뢰 마크 및 비신뢰 마크가 표시된 신뢰 링크를 나타낸 도면이다. 도 6a 및 도 6b는 각각 신뢰 마크 및 비신뢰 마크가 표시된 CGI 제출 버튼을 나타낸 도면이다. 도 7a 및 도 7b는 각각 신뢰 마크 및 비신뢰 마크가 표시된 웹 페이지의 주소 표시창을 나타낸 도면이다.
- <28> 도 4에 나타난 바와 같이, 렌더링 엔진부(111)는 인터넷을 통해 웹 서버로부터 요청한 웹 페이지를 수신하고 수신된 웹 페이지를 파싱한다(S400-S410). 그리고 신뢰 링크 확인부(111)는 신뢰 링크에 대한 마크업 정보가 포함되어 있는지 확인한다(S420). 이때, 신뢰 링크 확인부(112)는 신뢰 링크에 대한 마크업 정보가 포함되어 있을 경우, 해당 마크업 정보를 신뢰 링크 인증 서버(200)로 전송하여 신뢰 링크에 대한 인증 확인을 요청한다(S430). 신뢰 링크 인증 서버(200)에 의해 신뢰 링크에 대한 인증이 확인되면, 렌더링 엔진부(111)는 도 5a에 도시된 바와 같이 신뢰 링크(111a)에 신뢰 마크(T, 111b)를 표시한다(S440). 또한 렌더링 엔진부(111)는 단계(S440)에서 인증 확인 요청된 신뢰 링크에 대해 신뢰 링크 인증 서버(200)로부터 인증이 확인되지 않는 경우, 도 5b에 도시된 바와 같이 신뢰 링크에 비신뢰 마크(F, 112b)를 표시하고, "파싱 주의" 등의 파싱 위험 표시를 위한 경고 문구를 표시한다(S450). 그리고 단계(S420)에서 확인한 결과, 웹 페이지에서 신뢰 링크에 대한 마크업 정보가 포함되어 있지 않으면, 또는 신뢰 링크 확인부(112)에서 신뢰 링크에 신뢰 마크 또는 비신뢰 마크 표시가 완료되면, 렌더링 처리부(111)는 해당 웹 페이지에 대한 렌더링 처리를 수행한다(S460).
- <29> 그래픽 인터페이스부(113)는 단계(S460)를 거쳐 렌더링 처리부(111)에서 렌더링 처리가 완료된 웹 페이지를 사용자 화면에 표시한다(S470).
- <30> 한편, 렌더링 처리부(111)는 신뢰 링크(111a)에 신뢰 마크(T, 111b) 표시와 함께 도 6a에 도시된 바와 같이 신뢰 링크 값을 가진 CGI 제출 버튼(111d)에 신뢰 마크(T, 111b)를 표시할 수 있으며, 마찬가지로 렌더링 처리부(111)는 비신뢰 링크(1111a)에 비신뢰 마크(F, 111c) 표시와 함께 도 6b에 도시된 바와 같이 비신뢰 링크 값을

가진 CGI 제출 버튼(111d)에 비신뢰 마크(F, 111c)를 표시할 수 있다. 이때, 사용자 정보가 입력되는 입력창에 경고 문구(피싱 주의)를 표시할 수도 있다.

- <31> 또한 렌더링 처리부(111)는 도 7a에 도시된 바와 같이 신뢰 링크를 가지는 있는 웹 페이지에 대한 주소 표시창(111f)에 신뢰 마크(T, 111b)를 표시할 수도 있다. 마찬가지로, 렌더링 처리부(111)는 도 7b에 도시된 바와 같이 비신뢰 링크를 가지는 있는 웹 페이지에 대한 주소 표시창(111f)에 비신뢰 마크(F, 111c)를 표시할 수도 있다.
- <32> 도 8은 도 3에 도시된 신뢰 링크 인증 서버(200)의 등록 정보 입력부(210)의 동작 과정을 나타낸 도면이다.
- <33> 도 8에 나타낸 바와 같이, 등록 정보 입력부(220)는 사용자로부터 신뢰 링크 인증 등록 페이지를 요청받는다(S800). 그러면, 사용자 인증부(210)는 사용자에게 사용자 인증 처리를 수행한다(S810). 이때, 사용자가 신뢰 링크 인증 서버(200)에 등록되어 있으면, 등록 정보 입력부(210)는 사용자로부터 신뢰 링크 인증 정보를 입력받는다(S820). 한편, 단계(S710)에서 사용자가 신뢰 링크 인증 서버(200)에 등록되어 있지 않은 경우 사용자 인증부(210)는 신규 사용자 등록 처리를 수행하여 등록한다(S830-S840).
- <34> 그리고 등록 정보 입력부(220)는 신뢰 링크 등록자로부터 입력받은 신뢰 링크 인증 정보로부터 중복 등록 여부를 판단한다(S850). 이때, 중복 등록이 아닌 경우, 등록 정보 입력부(220)는 신뢰 링크 인증 정보를 인증 정보 저장부(240)에 저장하여 신규 신뢰 링크 인증 정보를 등록한다(S860). 만약, 중복 등록으로 판단된 경우, 등록 정보 입력부(220)는 중복 등록에 대한 권한 확인과 함께 신뢰 링크 등록자로부터 신뢰 링크 인증 정보의 수정 여부를 확인하여 신뢰 링크 인증 정보를 수정한다(S870-S880). 이때, 중복 등록에 대한 권한이 없거나 신뢰 링크 등록자가 신뢰 링크 인증 정보의 수정을 원하지 않을 경우 또는 단계(S830)에서 사용자가 신규 사용자 등록을 원하지 않을 경우 등록 정보 입력부(220)는 오류 메시지를 생성하고 신뢰 링크 인증 정보 입력이 종료된다(S890).
- <35> 이상에서 설명한 본 발명의 실시 예는 장치 및 방법을 통해서만 구현되는 것은 아니며, 본 발명의 실시 예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시 예의 기재로부터 본 발명이 속하는 기술 분야의 전문가라면 쉽게 구현할 수 있는 것이다.
- <36> 그리고 본 발명의 권리 범위는 상술한 실시 예에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리 범위에 속하는 것이다.

발명의 효과

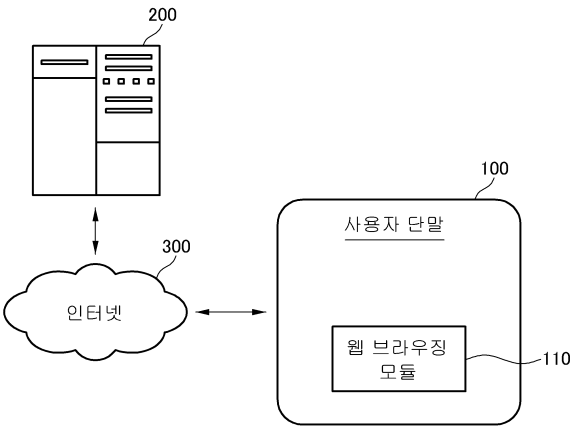
- <37> 이와 같이 본 발명의 실시 예에 의하면, 링크에 대한 신뢰도가 높아지고 이와 아울러 링크를 제공하는 웹 서버와 웹 페이지에 대한 신뢰도가 높아질 수 있다. 또한 이로 인하여 개인 정보 유출과 신뢰도 하락을 방지할 수가 있다.

도면의 간단한 설명

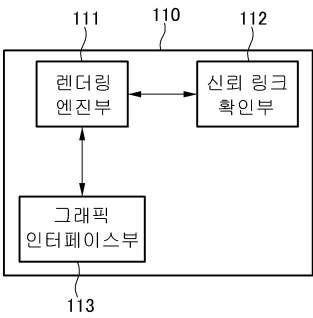
- <1> 도 1은 본 발명의 실시 예에 따른 신뢰 링크 인증 시스템을 개략적으로 나타낸 도면이다.
- <2> 도 2는 도 1에 도시된 웹 브라우징 모듈을 개략적으로 나타낸 도면이다.
- <3> 도 3은 도 1에 도시된 신뢰 링크 인증 서버를 개략적으로 나타낸 도면이다.
- <4> 도 4는 도 1에 도시된 웹 브라우징 모듈(110)의 동작을 나타낸 도면이다.
- <5> 도 5a 및 도 5b는 각각 신뢰 마크 및 비신뢰 마크가 표시된 신뢰 링크를 나타낸 도면이다.
- <6> 도 6a 및 도 6b는 각각 신뢰 마크 및 비신뢰 마크가 표시된 CGI 제출 버튼을 나타낸 도면이다.
- <7> 도 7a 및 도 7b는 각각 신뢰 마크 및 비신뢰 마크가 표시된 웹 페이지의 주소 표시창을 나타낸 도면이다.
- <8> 도 8은 도 3에 도시된 신뢰 링크 인증 서버(200)의 등록 정보 입력부(210)의 동작 과정을 나타낸 도면이다.

도면

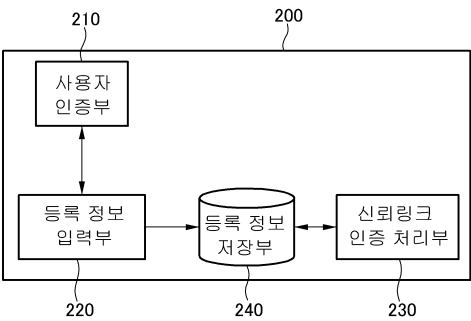
도면1



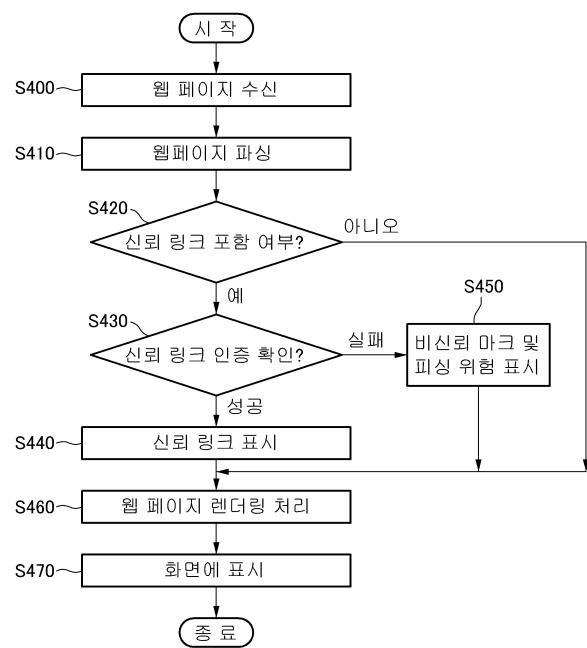
도면2



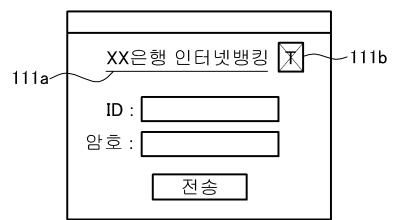
도면3



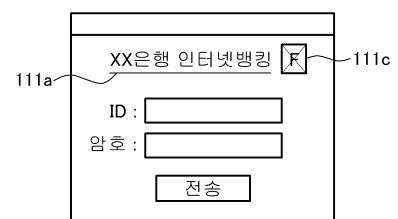
도면4



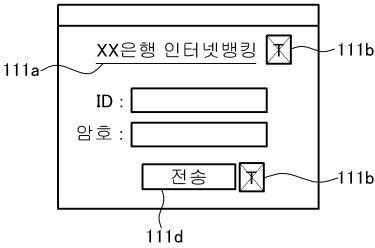
도면5a



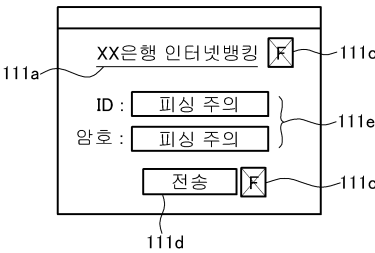
도면5b



도면6a



도면6b



도면7a



도면7b



도면8

