



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년09월12일
(11) 등록번호 10-1306074
(24) 등록일자 2013년09월03일

(51) 국제특허분류(Int. Cl.)
H04W 12/12 (2009.01) H04W 88/18 (2009.01)
(21) 출원번호 10-2012-0103860
(22) 출원일자 2012년09월19일
심사청구일자 2012년09월19일
(56) 선행기술조사문헌
KR101059558 B1*
KR1020100068786 A*
KR1020110039629 A
KR101172876 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
강철구
인천광역시 남동구 남동대로692번길 13-5 ,2
동401호(구월동, 골드맨션)
(72) 발명자
강철구
인천광역시 남동구 남동대로692번길 13-5 ,2
동401호(구월동, 골드맨션)
(74) 대리인
홍중원

전체 청구항 수 : 총 14 항

심사관 : 장상배

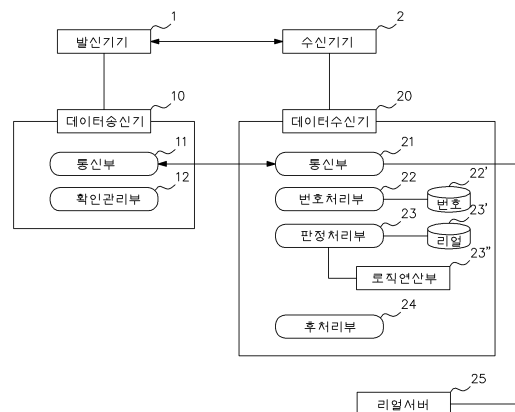
(54) 발명의 명칭 피싱방지방법 및 피싱방지시스템

(57) 요약

[과제] 개인정보 유출의 위험을 현격히 낮추고, 런타임으로 입증할 수 있는 인증데이터를 확인하여, 피싱을 방지한다.

[해결수단] 통신을 통하여 음성통화와 문자대화 중 적어도 하나의 대화를 요청하는 발신기기가, 상기 요청에 응답하는 수신기기에 대하여, 피싱(phishing)을 하지 못하도록 하는 피싱방지방법에 있어서, 상기 발신기기에 연결된 데이터송신기로부터 상기 수신기기에 연결된 데이터수신기에, 확인용 데이터가 전송되는 **데이터 전송단계**와, 상기 발신기기에 할당된 전화번호 또는 아이디가, 피싱인지의 여부를 확인할 필요가 있다고 상기 수신기기에 미리 등록되어 있는 관심대상의 전화번호 또는 아이디에 해당되는 경우에, 상기 발신기기가 확인대상으로 결정되는 **번호처리단계**와, 상기 확인대상에 대하여, 상기 확인용 데이터가 별도의 경로로 취득된 검증용 데이터인 리얼데이터와 상응되지 않는 경우에, 상기 발신기기가 피싱기기로 판정되는 **판정처리단계**와, 상기 피싱기기에 대하여, 미리 정해져 있는 후속조치가 취하여지는 **후처리단계**를 구비한다.

대표도 - 도1



특허청구의 범위

청구항 1

통신을 통하여 음성통화와 문자대화 중 적어도 하나의 대화를 요청하는 발신기기가, 상기 요청에 응답하는 수신기기에 대하여, 피싱(phishing)을 하지 못하도록 하는 피싱방지방법에 있어서,

상기 대화의 개시 이전, 개시 초기, 또는 개시 후의 시점에, 상기 대화와 별개로 백그라운드 실행되는 제1 데이터통신 또는 전화통신을 통하여, 상기 발신기기에 연결된 데이터송신기로부터 상기 수신기기에 연결된 데이터수신기에, 확인용 데이터가 전송되는 **데이터 전송단계**와,

상기 발신기기에 할당된 전화번호 또는 아이디가, 피싱인지의 여부를 확인할 필요가 있다고 상기 수신기기에 미리 등록되어 있는 관심대상의 전화번호 또는 아이디에 해당되는 경우에, 상기 데이터수신기에 의하여 상기 발신기기가 확인대상으로 결정되는 **번호처리단계**와,

상기 확인대상에 대하여, 상기 대화와 별개로 실행되는 제2 데이터통신을 통하여 또는 내부 로직연산결과로부터 취득된 검증용 데이터인 리얼데이터와 상기 확인용 데이터가 상응되지 않는 경우에, 상기 데이터수신기에 의하여 상기 발신기기가 피싱기기로 판정되는 **판정처리단계**와,

상기 피싱기기에 대하여, 상기 수신기기에 의하여 미리 정해져 있는 후속조치가 취하여지는 **후처리단계**를 구비함을 특징으로 하는 피싱방지방법.

청구항 2

청구항 1에 있어서,

상기 확인용 데이터는, 확인용 **키 또는 패스워드 또는 메시지**임을 특징으로 하는 피싱방지방법.

청구항 3

청구항 1 또는 청구항 2에 있어서,

상기 데이터 전송단계의 이전에, 상기 데이터수신기로부터 상기 데이터송신기로, 확인용 데이터 전송요청을 전달하는 **전송요청단계**가 더욱 구비됨

을 특징으로 하는 피싱방지방법.

청구항 4

청구항 1 또는 청구항 2에 있어서,

상기 데이터송신기는, 상기 데이터수신기에 데이터를 푸시할 수 있는 **푸시서버**나, 상기 데이터수신기에 데이터를 전송할 수 있는 **전송서버**로 구성되고,

상기 확인용 데이터는, 상기 발신기기로부터의 발신요청에 따라 상기 푸시서버로부터 푸시되거나 상기 전송서버로부터 전송됨

을 특징으로 하는 피싱방지방법.

청구항 5

청구항 1 또는 청구항 2에 있어서,

상기 데이터송신기는, 상기 발신기기로부터 상기 수신기기에 대하여 행하여진 발신이력을 저장하고 관리하는 **발신이력서버**로 구성되고,

상기 확인용 데이터는, 상기 데이터수신기로부터의 발신이력의 조회에 따른 응답메시지로서 상기 발신이력서버로부터 발송됨

을 특징으로 하는 피싱방지방법.

청구항 6

청구항 1 또는 청구항 2에 있어서,

상기 리얼데이터는,

상기 데이터수신기 또는 상기 데이터수신기에 연결된 **리얼서버**에 저장되어 있다가 인출되어 취득되거나, 또는

상기 확인용 데이터의 생성과 동일한 로직으로 상기 리얼데이터를 생성시키도록 구성된 **로직연산부**에 의하여 연산되어 취득됨

을 특징으로 하는 피싱방지방법.

청구항 7

청구항 1 또는 청구항 2에 있어서,

상기 후속조치는,

상기 수신기기에 경고를 발하는 **경고조치**,

대화를 차단하는 **차단조치** 및

미리 정해져 있는 전화번호나 아이디에 상기 발신기기에 관한 정보와 피싱 발생사실을 전송하는 **신고조치**

중 적어도 하나를 포함함을 특징으로 하는 피싱방지방법.

청구항 8

통신을 통하여 음성통화와 문자대화 중 적어도 하나의 대화를 요청하는 발신기기가, 상기 요청에 응답하는 수신기기에 대하여, 피싱(phishing)을 하지 못하도록 하는 피싱방지시스템에 있어서,

상기 발신기기에 연결되어 있는 **데이터송신기**와,

상기 수신기기에 연결되어 있고, 상기 대화의 개시 이전, 개시 초기, 또는 개시 후의 시점에, 상기 대화와 별개로 백그라운드 실행되는 제1 데이터통신 또는 전화통신을 통하여, 상기 데이터송신기로부터 확인용 데이터를 전송받는 **데이터수신기**와,

상기 발신기기에 할당된 전화번호 또는 아이디가, 피싱인지의 여부를 확인할 필요가 있다고 상기 수신기기에 미리 등록되어 있는 관심대상의 전화번호 또는 아이디에 해당되는 경우에, 상기 데이터수신기가 상기 발신기기를 확인대상으로 결정하는 **번호처리부**와,

상기 확인대상에 대하여, 상기 대화와 별개로 실행되는 제2 데이터통신을 통하여 또는 내부 로직연산결과로부터 취득된 검증용 데이터인 리얼데이터와 상기 확인용 데이터가 상응되지 않는 경우에, 상기 데이터수신기가 상기 발신기기를 피싱기기로 판정하는 **판정처리부**와,

상기 피싱기기에 대하여, 상기 수신기기가 미리 정해져 있는 후속조치를 취하는 **후처리부**

를 구비함을 특징으로 하는 피싱방지시스템.

청구항 9

청구항 8에 있어서,

상기 확인용 데이터는, 확인용 **키** 또는 **패스워드** 또는 **메시지임**

을 특징으로 하는 피싱방지시스템.

청구항 10

청구항 8 또는 청구항 9에 있어서,

상기 확인용 데이터의 전송 이전에, 상기 데이터수신기는, 상기 데이터송신기로 **확인용 데이터 전송요청**을 전달

함

을 특징으로 하는 피싱방지시스템.

청구항 11

청구항 8 또는 청구항 9에 있어서,

상기 데이터송신기는, 상기 데이터수신기에 데이터를 푸시할 수 있는 **푸시서버**나 상기 데이터수신기에 데이터를 전송할 수 있는 **전송서버**로 구성되고,

상기 확인용 데이터는, 상기 발신기기로부터의 발신요청에 따라 상기 푸시서버로부터 푸시되거나 상기 전송서버로부터 전송됨

을 특징으로 하는 피싱방지시스템.

청구항 12

청구항 8 또는 청구항 9에 있어서,

상기 데이터송신기는, 상기 발신기기로부터 상기 수신기기에 대하여 행하여진 발신이력을 저장하고 관리하는 **발신이력서버**로 구성되고,

상기 확인용 데이터는, 상기 데이터수신기로부터의 발신이력의 조회에 따른 응답메시지로서 상기 발신이력서버로부터 발송됨

을 특징으로 하는 피싱방지시스템.

청구항 13

청구항 8 또는 청구항 9에 있어서,

상기 리얼데이터는,

상기 데이터수신기 또는 상기 데이터수신기에 연결된 **리얼서버**에 저장되어 있다가 인출되어 취득되거나, 또는

상기 확인용 데이터의 생성과 동일한 로직으로 상기 리얼데이터를 생성시키도록 구성된 **로직연산부**에 의하여 연산되어 취득됨

을 특징으로 하는 피싱방지시스템.

청구항 14

청구항 8 또는 청구항 9에 있어서,

상기 후속조치는,

상기 수신기기에 경고를 발하는 **경고조치**,

대화를 차단하는 **차단조치** 및

미리 정해져 있는 전화번호나 아이디에 상기 발신기기에 관한 정보와 피싱 발생사실을 전송하는 **신고조치**

중 적어도 하나를 포함함을 특징으로 하는 피싱방지시스템.

명세서

기술분야

[0001] 본 발명은, 피싱방지방법 및 피싱방지시스템에 관한 것으로서, 보다 상세히는, 전화를 통한 보이스피싱이나 문자대화서비스(단문메시지, 카카오톡 등을 포함함)를 통한 메시지피싱 등을 미연에 방지할 수 있는 방법 및 시스템에 관한 것이다.

배경기술

- [0002] 일반적으로, '피싱(phishing)'이란, 실제 웹사이트를 본떠 만든 가짜 웹사이트에 접속하도록 하고, 개인정보를 입력하도록 하여, 이 입력된 개인정보를 사취하는 불법행위를 말한다. 이렇게 사취된 개인정보는, 불법 계좌이체 등 후속의 다양한 불법행위에 사용된다. 따라서, 피싱의 피해를 입지 않도록, 인터넷의 사용자들은 주의를 하여야 한다.
- [0003] 한편, 최근에는, 상기 피싱과 유사하게, 실제 전화 발신처인 것처럼 속이면서 가짜 전화 발신처에서 전화를 걸어서, 역시 개인정보를 사취하는 불법행위가 기승을 부리고 있다. 이러한 행위는, 일명 '보이스피싱'이라고 한다. 이 보이스피싱은, 발신번호 변경기능을 이용하는 경우가 많아서, 전화 수신측에서는, 전화번호만 가지고는 식별이 불가능한 것이 현실이며, 역시 그 피해를 입지 않도록, 전화 사용자들은 주의를 하여야 한다. 가짜 발신처로서는, 은행, 카드사, 보험사 등의 금융기관, 경찰서, 국정원, 국세청 등의 국가기관, 한전, 가스공사 등의 공기업 등이 흔히 이용되고, 자녀들이나 배우자, 부모님 등 가족의 전화로 위장되는 경우도 있다.
- [0004] 그리고, 음성을 통하지 않고, 문자를 통하여 서로간에 대화를 주고 받을 수 있는 다양한 서비스들이 최근에 많이 등장하였다. 예컨대, 전화망을 이용하는 단문서비스(SMS)의 문자대화는 물론이고, MSN, 네이트온 등의 컴퓨터 인터넷망을 통한 문자대화서비스나, 카카오톡이나 마이피플 등 모바일 인터넷망을 통한 문자대화서비스도 왕성하게 서비스되고 있다.
- [0005] 그리고, 피싱은 이러한 각종 문자대화서비스 분야에도 퍼지고 있다. 즉, 문자대화서비스에서는 상대방을 대면하여 확인할 수 있는 상태가 아니므로, 이러한 점을 악용하여, 착각을 유도하여 특정인인 것처럼 속이면서 문자대화 함으로써, 개인정보를 사취하는 불법행위가 기승을 부리고 있다. 이를 '메시지피싱'이라 하기로 한다.
- [0006] 종래에는, 특허문헌 1과 같이, 발신전화의 과금정보와 가입자정보를 저장함과 함께, 보이스피싱에 대한 블랙리스트를 저장하고 관리함으로써, 피싱여부를 판별하는 방식의 기술이 개시되어 있었다.

선행기술문헌

특허문헌

- [0007] (특허문헌 0001) 특허공개 제10-2009-0129179호 공보

발명의 내용

해결하려는 과제

- [0008] 그런데, 특허문헌 1에 개시된 기술은, 통화시작시간, 발신자번호, 착신자번호, 통화종료시간 등의 과금정보는 물론이고, 전화명의, 주소, 요금납부방법, 납부계좌 등의 가입자정보까지 저장하고 있으므로, 그 데이터베이스의 규모는 가히 엄청난 크기가 되지 않으면 안된다. 따라서, 그 정보의 구축에 드는 시간과 비용도 문제가 되거니와, 이러한 거대한 데이터베이스를 가동시켜서 어떤 특정 정보를 조회하는데 걸리는 시간과 비용도 엄청나서, 반응속도가 극히 느린 시스템이 될 것으로 판단된다. 게다가, 이러한 과금정보나 가입자정보는, 통신회사 이외에는 함부로 축적하는 것이 금지되는 개인정보에 해당되고, 이러한 개인정보가 만에 하나 유출되었을 경우에는, 그 피해는 이루 말할 수 없는 큰 경제적, 사회적 대형사고를 초래하고 말 것이다.
- [0009] 게다가, 특허문헌 1에 개시된 기술은, 블랙리스트를 저장 및 관리하는 구성인데, 이는 과거에 보이스피싱의 경력이 있어서, 블랙리스트에 등재된 전화번호를 집중적으로 조사하여 보이스피싱 여부를 판단한다는 것을 의미한다. 따라서, 새로운 전화번호로 시도되는 보이스피싱에는 무력하다. 즉, 보이스피싱의 범피자들은, 전화번호를 수시로 바꾸기 때문에, 바뀐 새로운 전화번호에는, 블랙리스트는 현실적으로 아무런 효과를 내지 못한다. 또한, 초범인 경우에도, 특허문헌 1의 기술은 효력이 없다.
- [0010] 따라서, 본 발명은, 발신자의 과금정보나 가입자정보와 같은 극히 개인적인 정보를 별도로 추출, 저장 및 관리하지 않는 방식을 채택함으로써, 개인정보 유출의 위험을 현격히 낮춘 피싱방지방법 및 피싱방지시스템을 제공하고자 하는 것이다.
- [0011] 또한, 과거의 범피를 바탕으로 한 블랙리스트 대신에, 현재 런타임으로 입증할 수 있는 인증데이터를 확인함으로써, 과거의 전화번호나 아이디 뿐만 아니라 신규의 전화번호나 아이디에도 동일하게 통일적으로 적용할 수 있는 피싱방지방법 및 피싱방지시스템을 제공하고자 하는 것이다.

과제의 해결 수단

- [0012] 상기 과제를 해결하기 위한 본 발명의 피싱방지방법은, 통신을 통하여 음성통화와 문자대화 중 적어도 하나의 대화를 요청하는 발신기기가, 상기 요청에 응답하는 수신기기에 대하여, 피싱(phishing)을 하지 못하도록 하는 피싱방지방법에 있어서, 상기 발신기기에 연결된 데이터송신기로부터 상기 수신기기에 연결된 데이터수신기에, 확인용 데이터가 전송되는 **데이터 전송단계**와, 상기 발신기기에 할당된 전화번호 또는 아이디가, 피싱인지의 여부를 확인할 필요가 있다고 상기 수신기기에 미리 등록되어 있는 관심대상의 전화번호 또는 아이디에 해당되는 경우에, 상기 데이터수신기에 의하여 상기 발신기기가 확인대상으로 결정되는 **번호처리단계**와, 상기 확인대상에 대하여, 상기 확인용 데이터가 별도의 경로로 취득된 검증용 데이터인 리얼데이터와 상응되지 않는 경우에, 상기 데이터수신기에 의하여 상기 발신기기가 피싱기기로 판정되는 **판정처리단계**와, 상기 피싱기기에 대하여, 상기 수신기기에 의하여 미리 정해져 있는 후속조치가 취하여지는 **후처리단계**를 구비한다.
- [0013] 여기서, 상기 확인용 데이터는, 데이터통신 또는 전화통신을 통하여 전송되는 확인용 **키 또는 패스워드 또는 메시지**일 수 있다.
- [0014] 또한, 상기 데이터 전송단계의 이전에, 상기 데이터수신기로부터 상기 데이터송신기로, 확인용 데이터 전송요청을 전달하는 **전송요청단계**가 더욱 구비되어도 좋다.
- [0015] 또한, 상기 데이터송신기는, 상기 데이터수신기에 데이터를 푸시할 수 있는 **푸시서버**나, 상기 데이터수신기에 데이터를 전송할 수 있는 **전송서버**로 구성되고, 상기 확인용 데이터는, 상기 발신기기로부터의 발신요청에 따라 상기 푸시서버로부터 푸시되거나 상기 전송서버로부터 전송되어도 좋고,
- [0016] 상기 데이터송신기는, 상기 발신기기로부터 상기 수신기기에 대하여 행하여진 발신이력을 저장하고 관리하는 **발신이력서버**로 구성되고, 상기 확인용 데이터는, 상기 데이터수신기로부터의 발신이력의 조회에 따른 응답메시지로서 상기 발신이력서버로부터 발송되어도 좋다.
- [0017] 그리고, 상기 리얼데이터는, 상기 데이터수신기 또는 상기 데이터수신기에 연결된 **리얼서버**에 저장되어 있다가 인출되어 취득되거나, 또는 상기 확인용 데이터의 생성과 동일한 로직으로 상기 리얼데이터를 생성시키도록 구성된 **로직연산부**에 의하여 연산되어 취득되도록 구성될 수 있다.
- [0018] 그리고, 상기 후속조치는, 상기 수신기기에 경고를 발하는 **경고조치**, 대화를 차단하는 **차단조치** 및 미리 정해져 있는 전화번호나 아이디에 상기 발신기기에 관한 정보와 피싱 발생사실을 전송하는 **신고조치** 중 적어도 하나를 포함할 수 있다.
- [0019] 한편, 상기 과제를 달성하기 위한 본 발명의 시스템은, 통신을 통하여 음성통화와 문자대화 중 적어도 하나의 대화를 요청하는 발신기기가, 상기 요청에 응답하는 수신기기에 대하여, 피싱(phishing)을 하지 못하도록 하는 피싱방지시스템에 있어서, 상기 발신기기에 연결되어 있는 **데이터송신기**와, 상기 수신기기에 연결되어 있고, 상기 데이터송신기로부터 확인용 데이터를 전송받는 **데이터수신기**와, 상기 발신기기에 할당된 전화번호 또는 아이디가, 피싱인지의 여부를 확인할 필요가 있다고 상기 수신기기에 미리 등록되어 있는 관심대상의 전화번호 또는 아이디에 해당되는 경우에, 상기 데이터수신기가 상기 발신기기를 확인대상으로 결정하는 **번호처리부**와, 상기 확인대상에 대하여, 상기 확인용 데이터가 별도의 경로로 취득된 검증용 데이터인 리얼데이터와 상응되지 않는 경우에, 상기 데이터수신기가 상기 발신기기를 피싱기기로 판정하는 **판정처리부**와, 상기 피싱기기에 대하여, 상기 수신기기가 미리 정해져 있는 후속조치를 취하는 **후처리부**를 구비한다.
- [0020] 여기서, 상기 확인용 데이터는, 데이터통신 또는 전화통신을 통하여 전송되는 확인용 **키 또는 패스워드 또는 메시지**일 수 있다.
- [0021] 그리고, 상기 확인용 데이터의 전송 이전에, 상기 데이터수신기는, 상기 데이터송신기로 **확인용 데이터 전송요청**을 전달하여도 좋다.
- [0022] 또한, 상기 데이터송신기는, 상기 데이터수신기에 데이터를 푸시할 수 있는 **푸시서버**나 상기 데이터수신기에 데이터를 전송할 수 있는 **전송서버**로 구성되고, 상기 확인용 데이터는, 상기 발신기기로부터의 발신요청에 따라 상기 푸시서버로부터 푸시되거나 상기 전송서버로부터 전송되도록 하거나,
- [0023] 상기 데이터송신기는, 상기 발신기기로부터 상기 수신기기에 대하여 행하여진 발신이력을 저장하고 관리하는 **발신이력서버**로 구성되고, 상기 확인용 데이터는, 상기 데이터수신기로부터의 발신이력의 조회에 따른 응답메시지로서 상기 발신이력서버로부터 발송되도록 하여도 좋다.

[0024] 그리고, 상기 리얼데이터는, 상기 데이터수신기 또는 상기 데이터수신기에 연결된 **리얼서버**에 저장되어 있다가 인출되어 취득되거나, 또는 상기 확인용 데이터의 생성과 동일한 로직으로 상기 리얼데이터를 생성시키도록 구성된 **로직연산부**에 의하여 연산되어 취득되도록 할 수 있다.

[0025] 그리고, 상기 후속조치는, 상기 수신기기에 경고를 발하는 **경고조치**, 대화를 차단하는 **차단조치** 및 미리 정해져 있는 전화번호나 아이디에 상기 발신기기에 관한 정보와 피싱 발생사실을 전송하는 **신고조치** 중 적어도 하나를 포함할 수 있다.

발명의 효과

[0026] 본 발명에 의하면, 대화의 요청시에 발신기기에 연결된 데이터송신기로부터 수신기기에 연결된 데이터수신기가 확인용 데이터를 받고, 이를 별도의 안전한 경로를 통하여 획득한 리얼데이터와 비교하는 과정을 거칠 뿐이므로, 종래기술과 같이 발신자의 과금정보나 가입자정보와 같은 극히 개인적인 정보를 별도로 추출, 저장 및 관리하는 방식이 아니다. 따라서, 개인정보 유출의 위험이 현격히 낮아진다.

[0027] 또한, 확인용 데이터를 매번 대화의 요청시마다 수신하여, 그 전화번호 또는 아이디와 상응되는 진정한 리얼데이터와 비교하므로, 종래기술과 같이 과거의 범위를 바탕으로 한 블랙리스트를 관리하는 것이 아니다. 대신에, 현재 런타임으로 입증할 수 있는 인증데이터를 확인하는 것이므로, 과거의 전화번호나 아이디 뿐만 아니라 런타임의 신규의 전화번호나 아이디에도 동일하게 통일적으로 적용할 수 있다는 현저한 효과가 있다.

도면의 간단한 설명

[0028] 도 1은, 본 발명의 피싱방지방법이 적용되는 피싱방지시스템의 대략 블록구성도이다.

도 2는, 본 발명의 피싱방지방법이 실행되는 흐름을 나타내는 플로우차트이다.

도 3은, 본 발명의 피싱방지방법이 적용된 피싱방지시스템의 일례인 스마트폰 화면의 예시도로서, (a)는, 피싱방지에 대한 관심대상 리스트(관리리스트)의 설정 및 입력화면의 예시도, (b)는, 전화수신시에 가로챈 전화번호가 관심대상이 아닌 경우의 화면의 예시도, (c)는, 전화수신시에 가로챈 전화번호가 관심대상이기는 하지만 확인용 데이터가 리얼데이터와 상응되어서 피싱이 아니라고 판단된 경우의 화면의 예시도, (d)는, 전화수신시에 가로챈 전화번호가 관심대상인데, 확인용 데이터가 리얼데이터와 상응되지 않아서 피싱이라고 판단된 경우의 화면의 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 이하, 본 발명에 대하여, 첨부도면을 참조하면서 상세히 설명한다. 다만, 동일구성에 의하여 동일기능을 행하는 요소에 대해서는, 도면이 바뀌더라도 동일부호를 유지함으로써 상세한 설명을 생략하는 경우가 있다.

[0030] 도 1은, 본 발명의 피싱방지방법이 적용되는 피싱방지시스템의 대략 블록구성도이다. 도 2는, 본 발명의 피싱방지방법이 실행되는 흐름을 나타내는 플로우차트이다.

[0031] 본 발명의 피싱방지시스템은, 통신을 통하여 음성통화와 문자대화 중 적어도 하나의 대화를 요청(S10)하는 발신기기(1)가, 상기 요청에 응답(S10)하는 수신기기(2)에 대하여, 피싱(phishing)을 하지 못하도록 하는 피싱방지방법을 구현하기 위한 시스템이다. 이 피싱방지시스템은, **데이터송신기(10)**와, **데이터수신기(20)**와, **번호처리부(22)**와, **판정처리부(23)**와, **후처리부(24)**를 구비하고, 이는 본 발명의 피싱방지방법의, **데이터 전송단계**와, **번호처리단계**와, **판정처리단계**와, **후처리단계**에 대응된다. 개략하여, 본 발명은, 음성통화 또는 문자대화의 개시 이전, 개시 초기, 또는 개시 후의 시점(통화나 대화 도중)에, 통화나 대화를 멈추고 또는 통화나 대화와 동시에 백그라운드 실행으로, 발신측으로부터 수신측이 확인용 데이터를 받아서, 이를 발신측의 전화번호나 아이디에 대응시켜서 미리 확보하고 있는 리얼데이터와 비교함으로써, 발신측의 피싱여부를 확인하는 구성으로 되어 있다. 다만, 이하의 설명에서는, 통화나 대화의 개시 전에 확인용 데이터를 검증하여, 피싱이 아닌 경우에만 통화나 대화를 연결하는 경우에 대하여 설명하지만, 통화나 대화의 개시 후에 검증 및 피싱에 대한 처리를 하는 경우에도 마찬가지로 적용할 수 있음은 자명하다. 이하, 구체적으로 설명한다.

[0032] 상기 **데이터송신기(10)**는, 상기 발신기기(1)에 연결되어 있고, 상기 발신기기(1)의 본연의 기능, 즉 음성대화나 문자대화를 수행하는 기능 이외에 본 발명의 구현을 위하여 추가로 구비된 데이터처리기기이다. 다만, 이는, 상기 발신기기(1)에 포함되는 모듈로서 구현되어도 좋다.

[0033] 또한, 상기 **데이터수신기(20)**는, 상기 수신기기(2)에 연결되어 있고, 상기 수신기기(2)의 본연의 기능, 즉 음성

대화나 문자대화를 수행하는 기능 이외에 본 발명의 구현을 위하여 추가로 구비된 데이터처리기기이다. 다만, 이는, 상기 수신기기(2)에 포함되는 모듈로서 구현되어도 좋다. 이는, 상기 데이터송신기(10)로부터 확인용 데이터를 전송(S30)받는다. 이로써, **데이터 전송단계**가 수행된다.

[0034] 여기서, 상기 발신기기(1)와 수신기기(2)는, 전화 또는 정보통신기기일 수 있다. 상기 전화는, 유선전화와 무선 전화, 휴대폰, 스마트폰, VoIP전화 뿐 아니라 가까운 미래에 출현될 모든 형태의 음성대화기기를 포함한다. 상기 정보통신기기는, 휴대폰 등에서 가능한 단문서비스(SMS)가 구현되는 기기, 컴퓨터통신을 이용한 메신저기능이 구현되는 기기, 모바일 인터넷을 이용한 카카오톡, 마이피플 등의 문자대화서비스가 구현되는 기기 뿐 아니라 가까운 미래에 출현될 모든 형태의 문자대화기기를 포함한다.

[0035] 상기 발신기기(1)는, 예컨대 은행, 카드사, 보험사 등의 금융기관, 경찰서, 국정원, 국세청 등의 국가기관, 한전, 가스공사 등의 공기업 등의 전화 또는 정보통신기기일 수 있다. 이 경우, 범죄자는 이러한 기관이나 회사를 가장하여 대화 요청을 해 와서, 개인정보를 빼내어가기 때문에, 이러한 피싱을 방지할 수 있도록 하여야 한다. 또는, 상기 발신기기(1)는, 예컨대 자녀들이나 배우자, 부모님 등 가족의 전화 또는 정보통신기기일 수 있다. 이 경우, 범죄자는 이러한 가족의 유괴나 사고 등을 가장하여 대화 요청을 해 와서, 개인정보를 빼내어가기 때문에, 이러한 피싱을 방지할 수 있도록 하여야 한다.

[0036] 여기서, 상기 확인용 데이터는, 상기 발신기기(1) 측에서 피싱이 아니라는 것을 증명하기 위하여 수신기기(2) 측에 전송하는 데이터인데, 이는 데이터통신 또는 전화통신을 통하여 전송되는 확인용 **키 또는 패스워드 또는 메시지**로서 구성되어도 좋다. 상기 키(key), 패스워드, 그리고 메시지는, 표현은 다르지만, 결국 판정을 위하여 사용되는 짧은 문구(short phrase)를 의미한다는 점에서 서로 유사한 바가 있다. 상기 메시지는, 단문서비스(SMS)의 메시지나 모바일인터넷용 대화서비스(카카오톡 등)의 메시지 뿐만 아니라, 앞으로 가까운 미래에 출현할 모든 형태의 메시지를 포함하며, 문자, 텍스트, 음성디지털데이터, 화상디지털데이터 등을 포함한다.

[0037] 여기서, 보다 구체적인 구현예를 들어본다면, 상기 데이터송신기(10)는, 푸시서버나 전송서버로 구현될 수도 있고, 발신이력서버로 구현될 수도 있다.

[0038] 상기 데이터송신기(10)가, 상기 데이터수신기(20)에 데이터를 푸시할 수 있는 **푸시서버**나, 상기 데이터수신기(20)에 SMS나 일반데이터를 전송할 수 있는 **전송서버**로 구성되는 경우에, 상기 확인용 데이터는, 상기 발신기기(1)로부터의 발신요청에 따라 상기 푸시서버로부터 푸시되거나, 상기 전송서버로부터 전송되도록 구성될 수도 있다.

[0039] 예컨대, 푸시서버로 구현되는 경우, 발신기기(1)의 대화의 요청에 이어서, 푸시서버가 자동으로 데이터수신기(20)에 확인용 데이터를 푸시할 수 있다.

[0040] 또는, 발신기기(1)의 대화의 요청에 이어서, 미리 정해진 시간 내에 확인용 데이터의 푸시가 이루어지지 않으면, 데이터수신기(20)가 푸시서버에 푸시의 요청을 하고, 이에 따라서 푸시서버가 데이터수신기(20)에 확인용 데이터를 푸시할 수 있다.

[0041] 예컨대, 전송서버로 구현되는 경우, 발신기기(1)의 대화의 요청에 이어서, 전송서버가 자동으로 데이터수신기(20)에 확인용 데이터를 전송할 수 있다. 예컨대 이 데이터는, 단문메시지의 형식을 가질 수도 있고, 예컨대 그 메시지의 내용 중 특정 부분이 확인용 데이터에 해당될 수도 있다.

[0042] 또는, 발신기기(1)의 대화의 요청에 이어서, 미리 정해진 시간 내에 확인용 데이터의 전송이 이루어지지 않으면, 데이터수신기(20)가 전송서버에 전송의 요청을 예컨대 단문메시지 형식으로 행하고, 이에 따라서 전송서버가 데이터수신기(20)에 확인용 데이터를 예컨대 단문메시지 형식으로 전송할 수 있다.

[0043] 다만, 전송서버의 경우, 단문메시지 형식의 데이터의 전송이 반드시 필수인 것은 아니며, 일반 서버와 클라이언트 사이의 데이터의 전송과 같은 데이터통신을 이용하더라도 상관없다.

[0044] 한편, 상기 데이터송신기(10)가, 상기 발신기기(1)로부터 상기 수신기기(2)에 대하여 행하여진 발신이력을 저장하고 관리하는 **발신이력서버**로 구성되는 경우에, 상기 확인용 데이터는, 상기 데이터수신기(20)로부터의 발신이력의 조회에 따른 응답메시지로서 상기 발신이력서버로부터 발송되도록 구성될 수도 있다.

[0045] 예컨대, 발신이력서버로 구현되는 경우, 발신기기(1)의 수신기기(2)에 대한 모든 대화의 요청이 발신이력서버에 기록되고 있다. 이 상태에서, 발신기기(1)의 대화의 요청이 발생된 경우, 수신기기(2)는, 미리 정해진 시간, 예컨대 최근 5초 이내에 발신기기(1)로부터 수신기기(2)로 발신한 이력이 존재하는지의 여부를 발신이력서버에 조

회하고, 이로부터 응답을 받을 수 있고, 이 응답이 확인용 데이터로서 기능한다.

- [0046] 이와 같이 상기 데이터송신기(10)가 발신이력서버로 구성된 경우에, 상기 데이터 전송단계에 있어서의 확인용 데이터는 응답메시지가 되고, 이 응답메시지의 전송 이전에, 상기 데이터수신기(20)는, 상기 데이터송신기(10)로 **확인용 데이터 전송요청**이 되는 조회메시지를 전달하도록 하는 **전송요청단계**를 더욱 구비하도록 구성되는 것으로 이해할 수 있다.
- [0047] 상기 **번호처리부(22)**는, 상기 데이터수신기(20)에 구비되어, 발신기기(1)에 대하여 피싱여부의 판정을 행할 필요가 있는지를 필터링하는 모듈이다. 즉, 모든 발신기기(1)에 대하여 피싱여부를 판정하는 것은 처리시간과 전원 등의 자원의 낭비를 초래할 수 있으므로, 피싱여부의 판정을 선별적으로 수행하기 위함이다. 발신기기(1)의 전화번호나 아이디는, 발신기기(1)의 대화의 요청시에, 수신기기(2)나 데이터수신기(20)에서 공지의 기술에 의하여 용이하게 입수할 수 있다.
- [0048] 상기 번호처리부(22)는, 상기 발신기기(1)에 할당된 전화번호 또는 아이디가, 피싱인지의 여부를 확인할 필요가 있다고 상기 수신기기(2)에 미리 등록되어 있는 관심대상의 전화번호 또는 아이디에 해당되는 경우에, 상기 발신기기(1)를 확인대상으로 결정(S20)한다. 이로써, **번호처리단계**가 수행된다.
- [0049] 상기 관심대상은, 도 3의 (a)에 예시되어 있는 바와 같이, 수신기기(2)의 사용자가 임의로 설정할 수 있도록 하여도 좋다. 즉, '피싱관리 리스트' 메뉴에는, 미리 관공서, 금융기관 등의 이름과 전화번호 또는 아이디가 체크박스에 체크를 하는지의 여부에 의하여 선택되도록 구비되어 있을 수가 있다. 또한, 이와 더불어, 사용자가 임의로 타이핑하거나 주소록에서 불러와서, 친구나 가족 등 관심대상의 이름과 전화번호 또는 아이디를 입력 및 관리할 수 있도록 '사용자지정 리스트' 메뉴가 구비되어도 좋다.
- [0050] 상기 **판정처리부(23)**는, 상기 데이터수신기(20)에 구비되어, 상기 확인대상에 대하여, 상기 확인용 데이터가 별도의 경로로 취득된 검증용 데이터인 리얼데이터와 상응되는지를 비교(S40)하여, 상응되지 않는 경우(S50)에, 상기 발신기기(1)를 피싱기기로 판정(S70)한다. 이로써, **판정처리단계**가 수행된다.
- [0051] 여기서, 상기 리얼데이터는, 진정(genuine) 데이터를 의미하고, 상기 발신기기(1)로부터 입수된 전화번호 또는 아이디에 해당되는 진정 발신자에 의하여 만들어져서 상기 수신기기(2)측에 입수되는 데이터이다. 예컨대, 확인대상인 발신기기(1)가 한국전력에 해당되는 전화번호를 통하여 수신기기(2)에 대화의 요청, 즉 발신을 하고, 확인용 데이터를 전송한 경우, 이를 착신한 수신기기(2)는, 상기 한국전력의 전화번호에 상응하는 리얼데이터를 진정 발신자인 상기 한국전력의 신뢰할 수 있는 소스로부터 입수하여, 이를 상기 확인대상인 발신기기(1)로부터 받은 상기 확인용 데이터와 비교하게 되는 것이다.
- [0052] 여기서, 상기 리얼데이터는, 완성된 형태로 전달되어 저장되어 있도록 할 수도 있지만, 프로그램화된 생성 로직이 구현되어 있어도 좋다. 완성된 형태로 전달된 리얼데이터인 경우에는, 상기 데이터수신기(20) 또는 상기 데이터수신기(20)에 연결된 **리얼서버(25)**에 예컨대 데이터베이스의 형태로 미리 저장되어 있다가, 본 발명의 방법의 작동시에 인출되어 취득될 수도 있다. 그리고, 생성 로직이 구현된 프로그램의 형태인 경우에는, 상기 프로그램이 상기 데이터수신기(20) 또는 상기 데이터수신기(20)에 연결된 **리얼서버(25)**에 예컨대 **로직연산부(23')**의 형태로 미리 구현되어 있다가, 본 발명의 방법의 작동시에 상기 프로그램이 구동되어, 리얼데이터가 생성되어 취득될 수도 있다. 예컨대 OTP(One Time Password; 일회용 패스워드)의 생성과 같이, 상기 확인용 데이터의 생성과 동일한 로직으로 상기 리얼데이터를 생성시키도록 구성된 로직연산부(23')가 구현될 수 있다.
- [0053] 마지막으로, 상기 **후처리부(24)**는, 상기 데이터수신기(20)에 구비되어, 상기 피싱기기에 대하여, 미리 정해져 있는 후속조치(S70)를 취한다. 이로써, **후처리단계**가 수행된다.
- [0054] 여기서, 상기 후속조치는, 상기 수신기기(2)에 예컨대 시각적 또는 청각적 경고를 발하는 **경고조치**, 대화를 차단하는 **차단조치** 및 미리 정해져 있는 전화번호나 아이디에 상기 발신기기(1)에 관한 정보와 피싱 발생사실을 전송하는 **신고조치** 중 적어도 하나를 포함함이 바람직하다.
- [0055] <동작>
- [0056] 이하, 상기와 같은 구성을 가지는 본 발명의 피싱방지시스템을 이용하여 이루어지는 피싱방지방법에 대하여 예를 들어서 설명한다.
- [0057] 도 3은, 본 발명의 피싱방지방법이 적용된 피싱방지시스템의 일레인 스마트폰 화면의 예시도로서, (a)는, 피싱방지에 대한 관심대상 리스트(관리리스트)의 설정 및 입력화면의 예시도, (b)는, 전화수신시에 가로챈 전화번호가 관심대상이 아닌 경우의 화면의 예시도, (c)는, 전화수신시에 가로챈 전화번호가 관심대상이기는 하지만 확

인용 데이터가 리얼데이터와 상응되어서 피싱이 아니라고 판단된 경우의 화면의 예시도, (d)는, 전화수신시에 가로챈 전화번호가 관심대상인데, 확인용 데이터가 리얼데이터와 상응되지 않아서 피싱이라고 판단된 경우의 화면의 예시도이다.

[0058] 본 발명의 피싱방지방법은, 확인대상으로서 예컨대 도 3 (a)의 '피싱관리 리스트'란이나 '사용자지정 리스트'란에 등재된 경우에만 작동된다.

[0059] 따라서, 도 3 (b)와 같이, 예컨대 010-1111-XXXX 번호가 확인대상 리스트에 지정되어 있지 않은 상태라면, 그런 경우에는, 그 전화번호로부터 전화가 수신기기(2)에 착신되어도, 피싱여부의 판정을 수행하지 않는다. 따라서, 별도의 조치 없이 통화연결을 하면서, 디스플레이에 단순히 '피싱관리 대상이 아닙니다'라는 식의 메시지만 표시하는데, 이 전화는 실제로 피싱인지 아닌지를 알 수가 없다.

[0060] 반대로, 도 3 (c)나 (d)와 같이, 예컨대 010-1111-XXXX 번호가 확인대상 리스트에 지정되어 있는 상태라면, 그런 경우에는, 그 전화번호로부터 전화가 수신기기(2)에 착신되는 경우에, 일단 통화연결을 보류한 채로, 피싱여부의 판정을 먼저 수행하게 된다. 그리고, 그 발신기기(1)로부터 받은 확인용 데이터와 그 전화번호로부터 파악되는 국가보훈처 등의 진정 발신자로부터 입수한 신뢰할 수 있는 진정 데이터인 리얼데이터를 비교하게 된다. 그 비교결과에 따라서 피싱이 아니라고 판정된 경우에는 도 3 (c)와 같이 '안전하다'는 점을 표시하면서, 통화연결을 하면 된다. 그리고, 그 비교결과가 피싱이라고 판정된 경우에는 도 3 (d)와 같이 '피싱이다'라는 점을 표시하면서, 설정내용에 따라서는 미리 정해져 있는 전화번호 등을 통하여 피싱신고를 자동으로 하도록 하고, 통화연결을 금지하는 등의 조치를 취하면 된다.

[0061] 이상, 전화의 보이스피싱에 대하여 구체적 예시를 들어서 설명하였으나, 문자대화서비스에 대한 메시지피싱에 대해서도 비슷한 방식으로 적용할 수 있다. 예컨대, 문자대화서비스가 수행되고 있는 수신기기(2)에 있어서, 발신기기(1) 측에서 문자대화를 요청해오면, 대화창에 표시된 그 발신기기(1)의 아이디가 취득될 수 있고, 또한, 그 발신기기(1)로부터 확인용 데이터를 취득할 수 있다. 이와 함께, 그 발신기기(1)의 아이디가 확인대상에 해당되면, 그 발신기기(1)의 아이디에 해당되는 진정 발신자의 리얼데이터를 취득하고, 이를 확인용 데이터와 비교함으로써, 피싱의 여부를 판정할 수 있다. 만일 피싱인 경우에는, 대화의 종료 및 경고의 표시, 신고 등을 수행하도록 할 수 있다.

[0062] 또한, 상기 리얼데이터는, 진정 발신자로부터 수신기기(1)의 데이터수신기(20)로 한번 전송되도록 하여도 되지만, 보안력의 향상을 위하여 주기적으로 또는 수시로 리얼데이터가 업데이트되도록 운영하여도 좋다.

[0063] 그리고, 본 발명의 범위는, 상기 구체적 실시예에 의하여 제한되지 않으며, 청구범위에 기재된 발명사상의 범위 내에서 이루어진 변형, 변경 및 개량은, 모두 본 발명의 범위에 속하는 것으로 해석되어야 한다.

산업상 이용가능성

[0064] 본 발명은, 전화를 통한 보이스피싱이나 문자대화서비스를 통한 메시지피싱 등을 미연에 방지할 수 있는 방법 및 시스템에 적용할 수 있다.

부호의 설명

- [0065]
1. 발신기기
 2. 수신기기
 10. 데이터송신기
 11. 통신부
 12. 확인관리부
 20. 데이터수신기
 21. 통신부
 22. 번호처리부
 - 22'. 번호데이터베이스
 23. 판정처리부

23'. 리얼데이터베이스

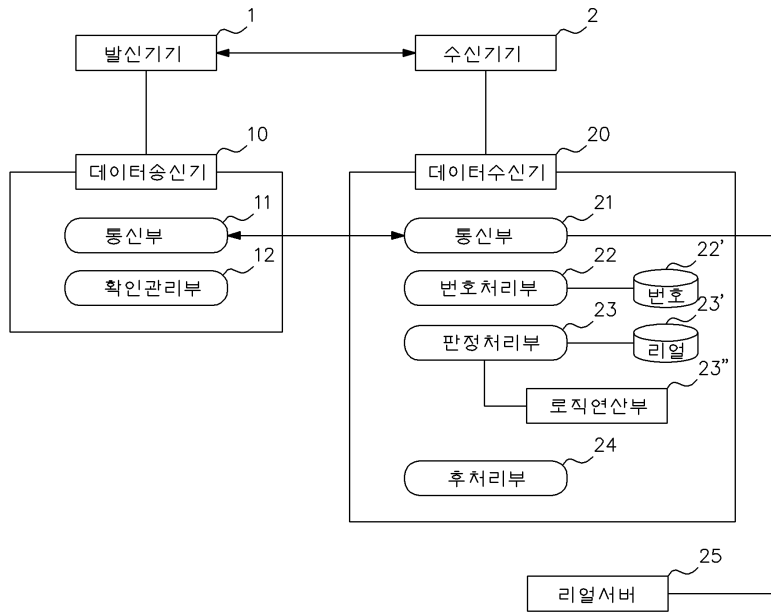
23''. 로직연산부

24. 후처리부

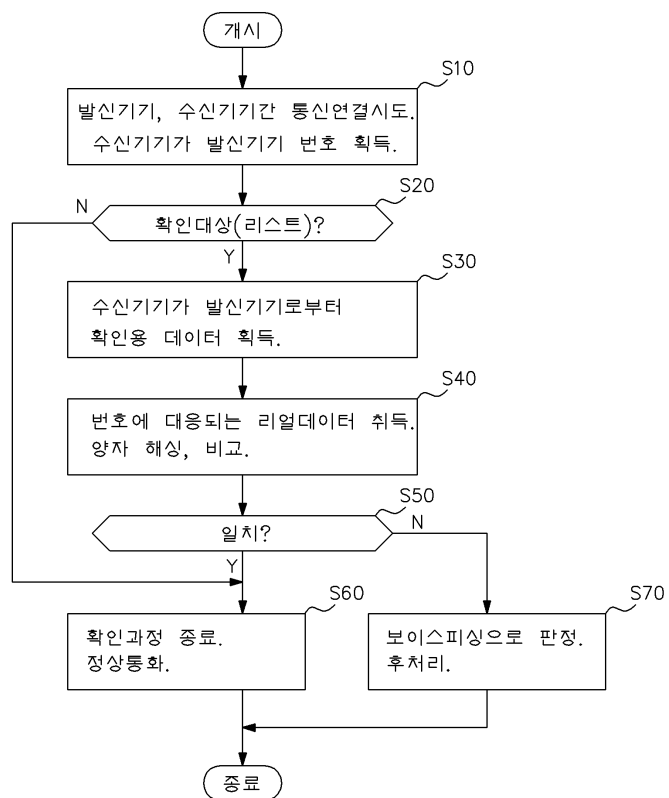
25. 리얼서버

도면

도면1

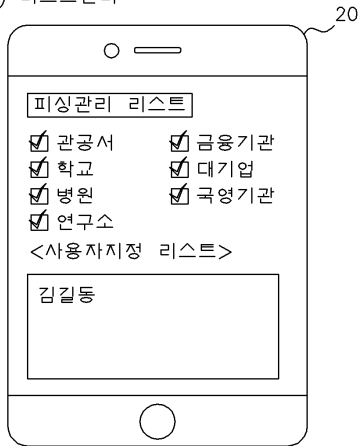


도면2

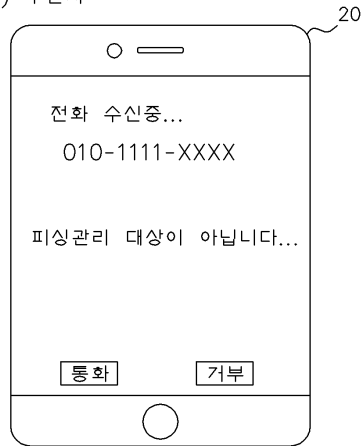


도면3

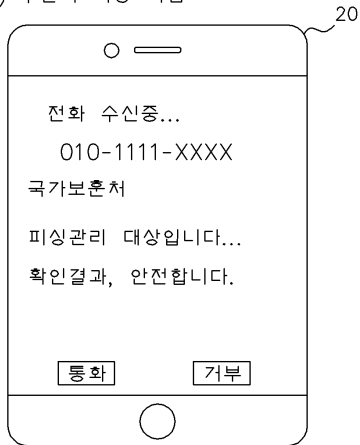
(a) 리스트관리



(b) 수신시



(c) 수신시-피싱 아님



(d) 수신시-피싱

