

(19)대한민국특허청(KR) (12) 등록특허공보(B1)

(51) 。 Int. Cl.⁷
G06F 17/30

(45) 공고일자 2004년12월29일
(11) 등록번호 10-0462829
(24) 등록일자 2004년12월10일

(21) 출원번호 10-2004-0041620
(22) 출원일자 2004년06월08일

(65) 공개번호
(43) 공개일자

(73) 특허권자 엔에이치엔(주)
서울특별시 강남구 역삼동 737 스타타워빌딩 34층

(72) 발명자 하정수
서울특별시 영등포구 여의도동 은하아파트 D-403

김정수
서울특별시 관악구 봉천7동 1617-23 2층

이우성
서울특별시 양천구 신월2동 615-6 대경연립 나동 103호

(74) 대리인 천성진

심사관 : 이영수

(54) 명령어의 유효성 판단 방법 및 그 시스템

요약

본 발명은 사용자의 단말기로부터 입력된 명령어의 유효성 판단 방법에 대한 것으로, 더욱 상세하게는 사용자로부터 입력된 명령어 중에서 소정의 규칙을 만족하는 명령어는 유효 또는 무효로 확정하고, 상기 규칙을 만족하지 않는 명령어에 대해서는 선정된 판단 방법에 따라 추가적인 유효성 판단 과정이 수행되도록 할 수 있는 명령어의 유효성 판단 방법에 대한 것이다.

본 발명에 따른 명령어의 유효성 판단 방법은, 허용 네트워크 주소 정보 및 상기 허용 네트워크 주소와 연관된 하나 이상의 차단 키워드를 포함하는 허용 데이터베이스를 유지하는 단계, 사용자의 단말기로부터 요청 내용을 포함하는 명령어를 입력 받는 단계, 상기 명령어에 포함된 상기 요청 내용 또는 네트워크 주소 정보를 추출하는 단계, 상기 허용 데이터베이스를 참조하여 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인지 판단하는 단계, 판단 결과 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인 경우, 상기 허용 데이터베이스를 참조하여 상기 요청 내용이 상기 허용 네트워크 주소 정보와 연관된 상기 하나 이상의 차단 키워드와 연관되어 있는지 판단하는 단계, 및 판단 결과 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있는 경우 선정된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 단계를 포함한다.

대표도

도 2

색인어

명령어, 유효성, 허용 네트워크 주소, 차단 키워드, 필터링.

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 명령어의 유효성 판단 방법을 수행하는 판단 시스템의 네트워크 연결을 도시한 도면이다.
 도 2는 본 발명의 일실시예에 따른 명령어의 유효성 판단 방법을 도시한 흐름도이다.
 도 3은 본 발명의 일실시예에 있어서, 허용 데이터베이스의 일례를 도시한 도면이다.
 도 4는 본 발명의 일실시예에 있어서, 소정의 검색 시스템이 사용자에게 제공하는 검색 결과 리스트의 일례이다.
 도 5는 본 발명의 또 다른 실시예에 따른 명령어의 유효성 판단 방법을 도시한 흐름도이다.
 도 6은 본 발명의 또 다른 실시예에 있어서, 선정된 판단 방법에 따라 명령어의 유효성 여부를 판단하는 과정을 도시한 흐름도이다.
 도 7은 본 발명의 또 다른 실시예에 있어서 로그 데이터베이스에 기록되는 로그 정보의 일례를 도시한 도면이다.
 도 8은 본 발명의 또 다른 실시예에 따른 판단 시스템을 도시한 블록도이다.
 도 9는 본 발명에 따른 명령어의 유효성을 판단하는 방법을 수행하는 데 채용될 수 있는 범용 컴퓨터 장치의 내부 블록도이다.

<도면의 주요 부분에 대한 부호의 설명>

800 : 판단 시스템
 801 : 제1 판단 시스템
 8011: 명령어 입력부 8012 : 데이터 추출부
 8013: 제1 판단부 8014: 제2 판단부
 8015: 제3 판단부
 802 : 제2 판단 시스템
 803: 허용 데이터베이스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 사용자의 단말기로부터 입력된 명령어의 유효성 판단 방법에 대한 것으로, 더욱 상세하게는 사용자로부터 입력된 명령어 중에서 소정의 규칙을 만족하는 명령어는 유효 또는 무효로 확정하고, 상기 규칙을 만족하지 않는 명령어에 대해서는 선정된 판단 방법에 따라 유효성 판단 과정이 수행되도록 할 수 있는 명령어의 유효성 판단 방법에 대한 것이다.

서버/클라이언트 모델에 있어서, 클라이언트는 통신망을 통해 서버에 접속하여 소정의 요청을 입력하고 상기 서버는 상기 사용자 단말기로 상기 요청에 대응하는 응답을 한다.

그런데, 상기 사용자는 상기 응답을 얻기 위해서가 아니라 다른 목적으로 상기 요청을 입력하는 경우가 있다.

예를 들면, 검색 서비스를 제공하는 검색 서버는 사용자의 선호도에 따른 검색 결과 목록을 제공하기 위해 사용자의 검색 요청을 통계적으로 분석하여 검색 결과 목록을 생성하는데 이용할 수 있다. 소정의 검색 결과 목록을 제공 받은 사용자가 '자주' 선택하는 검색 결과는 검색 요청과의 관련성이 높고 또한 사용자의 선호도도 높다고 생각할 수 있으므로, 상기 검색 서버는 상기 검색 결과에 우선권을 부여하여 추후에도 상기 검색 요청에 대해서는 상기 검색 결과가 우선적으로 사용자에게 제공되도록 할 수 있다.

이 경우 상기 사용자의 '검색 결과 선택'은 한편으로는 '상기 검색 결과와 연관된 정보를 제공 받거나 상기 검색 결과와 연관된 웹 페이지에 접속하기 위한 요청'으로 사용되었지만, 다른 한편으로는 '검색 결과 목록을 생성하는 기준'으로서 사용되며, 이러한 사실을 알고 있는 사용자는 소정의 검색 쿼리에 응답하여 제공된 검색 결과 목록 중 동일한 검색 결과를 반복적으로 선택함으로써, 자신이 선택한 검색 결과의 우선권이 부여되도록 할 수 있다. 물론 이와 같이 상기 사용자가 악의적인 의도로 검색 결과를 반복적으로 선택하여 상기 검색 결과에 우선권이 부여된 경우에는, 검색 결과와 관련성이 높고 사용자들이 선호하는 검색 결과를 우선권으로 제공하고자 하는 원래의 목적은 달성될 수 없게 된다.

따라서, 검색 서버는 사용자가 검색 결과를 선택하는 요청을 입력하는 경우 상기 요청이 악의적인 의도로 입력되었는지 여부를 판단할 필요가 있다. 판단 결과 상기 요청이 악의적인 의도로 입력된 경우에는 상기 요청에 따라 검색 결과와 연관된 정보는 제공되지, 상기 요청을 검색 결과 목록을 생성하는 기준으로는 사용하지 않는 것이 바람직할 것이다. 이와 같이, 소정 시스템으로 입력되는 사용자의 '요청'이 상기 시스템이 목적인 바와 다른 사용자의 악의적인 의도에 의해 발생한 것인지 여부를 판단하는 것이 필요한 경우가 있다.

이하, 본 명세서에서 사용되는 '명령'이라는 용어는 소정의 서버 시스템에서 소정의 동작이 수행되도록 하기 위한 사

용자의 '요청', 상기 서버 시스템으로 소정의 정보를 제공하기 위한 사용자의 '대화', 또는 상기 '정보' 자체를 포함하는 포괄적인 개념으로 사용되었으며, 상기 '명령'은 상기 사용자의 단말기로부터 상기 서버 시스템으로 '명령어'를 전송함으로써 상기 서버 시스템에 전달될 수 있다.

한국특허출원 제10-2002-7010554호('발명의 명칭: 네트워크 상에서의 대화의 유효성 결정을 위한 시스템 및 방법' 이하 '출원 발명'이라고 함)는 사용자의 명령의 유효성 여부를 판단하는 방법 중 하나를 제시하고 있다. 상기 한국특허출원은 출원 명세서에서 사용자의 악의적인 의도로 입력된 대화를 '불법 대화'라고 칭하고 있다.

상기 출원 발명은 1) 추정된 사용자에 관한 '집합적 방식 데이터'와 '고유 특징 데이터'를 포함하는 데이터를 네트워크 상의 사용자 대화로부터 수집하고, 2) 데이터베이스에 데이터를 저장하며, 3) 네트워크와의 불법 대화를 식별하기 위해 집합적 방식 및 고유 특징 데이터로 예측 모델을 구축하고, 4) 예측 모델을 이용하여 데이터베이스 내 불법 대화를 식별하는 단계를 포함한다.

상기 출원 발명은 '집합적 방식 데이터'로서 '검색 목록 클릭/단위 시간당 고유 사용자 ID의 숫자', '진입 소스/단위 시간당 고유 사용자 ID의 수', '어떤 청구 가능한 클릭을 수용하는 광고자/단위 시간당 고유 사용자 ID의 수' 등을 개시하고 있다.

또한, 상기 출원 발명은 '고유 특징 데이터'로서 '수입을 발생시킨 클릭의 날짜', '수입을 발생시킨 클릭의 시간 스탬프' 등을 개시하고 있다.

그런데, 상기 출원 발명은 하나의 대화가 입력될 때마다 상기 예측 모델을 이용하여 상기 대화가 유효한지 여부를 판단한다. 즉, 『하나의 대화에 대해』 '수용할 수 있으나 드문 클래스(ABUC) 값', '정상적 행동양식의 클래스(NBC) 값', '수용할 수 없는 클래스(UC) 값'을 각각 계산하고, 그 중 가장 큰 값을 갖는 클래스에 상기 대화가 속한다고 판단한다.

따라서, 대화의 패턴 상, 또는 현재까지 수집된 정보를 분석한 결과 상기 대화가 무효임을 용이하게 판단할 수 있는 경우에도 동일한 시스템 자원을 사용하여 ABUC 값, NBC 값, 및 UC값을 각각 산출, 비교한 후 대화가 무효임을 판단하게 되어 시스템 자원을 불필요하게 많이 소모하게 된다는 문제가 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 소정의 규칙에 따라 사용자로부터 입력된 명령어의 유효성을 간단하게 결정하고, 상기 규칙에 따라 상기 명령어의 유효성을 결정할 수 없는 경우에만 선정된 판단 방법에 따른 추가적인 유효성 판단을 할 수 있는 명령어의 유효성 판단 방법 및 그 시스템을 제공하는 것을 목적으로 한다. 즉, 본 발명은 허용 데이터베이스 또는 차단 데이터베이스에 기록되어 있는 정보에 부합하는 명령어 또는 부합하지 않는 명령어는 소정의 규칙에 따라 유효 또는 무효로 판단하고 추가적인 유효성 판단 과정을 생략할 수 있는 명령어의 유효성 판단 방법 및 그 시스템을 제공한다.

또한, 본 발명은 명령어의 유효성 판단 과정을 명령어가 소정의 규칙에 부합하는지 여부를 판단하는 제1 과정과, 규칙에 부합하지 않는 명령어에 대해서는 선정된 판단 방법에 따라 그 유효성을 판단하는 제2 과정으로 이분화하여, 간단하고 빠르게 유효 여부가 판단 가능한 명령어는 제1 과정만으로 명령어의 유효성 판단 과정이 종료되도록 함으로써, 명령어의 유효성 판단을 수행하는 시스템의 부하를 감소시키고 명령어의 유효성 판단 속도를 향상시킬 수 있는 명령어의 유효성 판단 방법 및 그 시스템을 제공한다.

또한, 본 발명은 관리자, 개발자 또는 관리자의 단말기의 네트워크 주소로부터 입력되는 명령어, 또는 관공서나 대기업의 단말기의 네트워크 주소로부터 입력되는 명령어와 같이, 신뢰할 수 있으면서 알려진 네트워크 주소 또는 네트워크 그룹으로부터 입력되는 명령어는 유효로 판단하여 추가적인 유효성 판단 과정을 생략할 수 있는 명령어의 유효성 판단 방법 및 그 시스템을 제공하는 것을 목적으로 한다.

한편, 본 발명은 관공서나 대기업의 단말기로부터 입력되는 명령어라고 하더라도 상기 관공서 등이 입력할 가능성이 희박한 요청 내용을 포함하는 명령어에 대해서는 유효성 판단 과정을 생략하지 않도록 하여 보다 정확하게 명령어의 유효성 여부를 판단할 수 있는 명령어의 유효성 판단 방법 및 그 시스템을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

상기의 목적을 달성하고, 상술한 종래 기술의 문제점을 해결하기 위하여, 본 발명에 따른 명령어의 유효성 판단 방법은, 허용 네트워크 주소 정보 및 상기 허용 네트워크 주소와 연관된 하나 이상의 차단 키워드를 포함하는 허용 데이터베이스를 유지하는 단계, 사용자의 단말기로부터 요청 내용을 포함하는 명령어를 입력 받는 단계, 상기 명령어에 포함된 상기 요청 내용 또는 네트워크 주소 정보를 추출하는 단계, 상기 허용 데이터베이스를 참조하여 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인지 판단하는 단계, 판단 결과 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인 경우, 상기 허용 데이터베이스를 참조하여 상기 요청 내용이 상기 허용 네트워크 주소 정보와 연관된 상기 하나 이상의 차단 키워드와 연관되어 있는지 판단하는 단계, 및 판단 결과 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있는 경우 선정된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 단계를 포함한다.

또한, 본 발명의 일측에 따르면, 상기 판단 방법은 판단 결과 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있지 않은 경우 상기 명령어를 유효로 판단하는 단계를 더 포함한다.

본 명세서에서 사용되는 용어의 정리

1) 네트워크 주소 정보

본 명세서에서 사용된 네트워크 주소는 IP 주소를 포함하여 단말기의 네트워크 상에서의 위치를 식별하기 위해 사용되며, 네트워크 주소에 대한 정보를 '네트워크 주소 정보'로 정의한다.

2) 데이터베이스

본 명세서에서 사용된 허용 데이터베이스, 차단 데이터베이스 또는 로그 데이터베이스 등은 데이터베이스의 일종이며, 상기 '데이터베이스'는 각 데이터들의 연관 관계가 용이하게 파악될 수 있도록 기록 장치에 체계적으로 기록된 데이터의 집합을 의미한다.

3) 제1 판단 시스템 및 제2 판단 시스템

본 발명에 따른 판단 시스템은 제1 판단 시스템 및 제2 판단 시스템을 포함한다. 이러한 구분은 기능에 따라 이루어진 것으로 제1 판단 시스템 및 제2 판단 시스템은 동일 장치에 의해 구현될 수도 있다. 본 명세서에서의 '제1 판단 시스템'은 소정의 간단한 규칙을 만족하는 명령어를 유효 또는 무효로 판단한다. 상기 규칙을 만족하지 않는 명령어는 그 유효 또는 무효가 결정될 수 없기 때문에, 제2 판단 시스템은 선정된 판단 방법을 사용하여 상기 규칙을 만족하지 않는 명령어에 대해 보다 정교한 유효성 판단을 수행한다.

즉, '제2 판단 시스템'에서 유효성 판단의 대상이 되는 명령어는 제1 판단 시스템에 의해 '필터링'된 명령어뿐이다.

4) 선정된 판단 방법

본 명세서에서 사용된 '선정된 판단 방법'이라는 용어는 상기 제2 판단 시스템에서 명령어의 유효성을 판단하기 위해 사용되는 판단 방법을 의미한다.

이하 첨부된 도면을 참조하여 본 발명을 상세히 설명하기로 한다.

도 1은 본 발명에 따른 명령어의 유효성 판단 방법을 수행하는 판단 시스템의 네트워크 연결을 도시한 도면이다. 판단 시스템(100)은 제1 판단 시스템(101), 제2 판단 시스템(102), 허용 데이터베이스(103), 차단 데이터베이스(104), 및 로그 데이터베이스(105)를 포함하고, 판단 시스템(100)은 사용자의 단말기(110 등)와 유무선 통신망을 통하여 연결될 수 있다. 판단 시스템(100)은 사용자로부터 입력된 명령어를 처리하고 처리 결과에 따른 응답을 상기 사용자에게 제공할 수 있다.

또한, 이하에서는 판단 시스템(100)이 검색 시스템(120)과 연동하여, 검색 시스템(120)을 이용하는 사용자(110)로부터 입력된 명령어의 유효성을 판단하는 경우를 예로 들어 설명한다. 다만, 검색 시스템(120)은 예시적인 것이며, 본 발명의 범위는 사용자들로부터 명령어를 입력 받아 소정의 서비스(게임 서비스, 예약 서비스, 지식 제공 서비스 등)를 제공하는 모든 서비스 시스템에 대해 미친다. 또한, 판단 시스템(100)과 검색 시스템(120)은 동일한 장치로 구현될 수 있으며 이 경우에도 본 발명의 범위에 포함된다.

또한, 이하에서는 네트워크 주소로서 IP 주소를 사용하는 경우를 예로 들어 설명한다.

도 2는 본 발명의 일 실시예에 따른 명령어의 유효성 판단 방법을 도시한 흐름도이다. 단계(201)에서 제1 판단 시스템(101)은 허용 데이터베이스(103)를 유지한다.

본 발명의 일 실시예에 따르면, 허용 데이터베이스(103)에는 허용 IP 주소 정보 또는 허용 네트워크 그룹 정보를 포함한다. 허용 IP 주소 정보는 관공서의 IP 주소 정보, 또는 국내 대기업의 IP 주소 등, 불법적인 명령어를 입력할 가능성이 낮으면서도 잘 알려져 있는 IP 주소 정보일 수 있다.

도 3은 허용 데이터베이스(103)의 일례를 도시한 도면이다. 도 3의 도면 부호(301)은 신뢰할 만한 국내 대기업인 '삼성'과 연관된 IP 주소 정보를 나타내고, 도면 부호(302)는 '삼성'과 연관된 차단 키워드 '꽃배달'을 나타낸다.

단계(202)에서 검색 시스템(120)은 사용자의 단말기(110)로부터 명령어를 입력 받고, 단계(203)에서 제1 판단 시스템(101)은 상기 명령어에 포함된 IP 주소 정보를 추출한다.

단계(204)에서 판단 시스템(101)은 허용 데이터베이스(102)를 참조하여 상기 추출된 IP 주소 정보가 허용 IP 주소 정보인지 여부를 판단한다. 예를 들면, 상기 추출된 IP 주소 정보가 '254.254.254.254'이라면, 도 3의 허용 데이터베이스(103)로부터 상기 추출된 IP 주소 정보는 허용 IP 주소 정보라는 것을 알 수 있다.

또는, 단계(205)에서 판단 시스템(101)은 상기 IP 주소 정보를 이용하여 상기 IP 주소와 연관된 네트워크 그룹에 대한 네트워크 그룹 정보를 식별한다.

네트워크 그룹의 일례로서 IPv4에 따른 네트워크 클래스(Network Class)를 예로 들 수 있다. 네트워크 클래스는 IP 주소 공간을 분할하는 메커니즘에 대한 것이다. 8bit를 갖는 4개의 옥텟(Octet)으로 구성되어 있는 IPv4에 따른 IP 주소 체계에 있어서 IP 주소 정보로부터 상기 IP 주소를 갖는 단말기가 접속되는 네트워크를 식별할 수 있다. 예를 들면, 클래스 C 네트워크는 192.0.0.0부터 223.255.255.0까지의 IP 주소를 갖고, 앞에서부터 3개의 옥텟이 네트워크 번호를 나타내기 위해 사용되었다.

따라서, 제1 판단 시스템(101)은 IP 주소로부터 상기 IP 주소와 연관된 네트워크 그룹을 식별할 수 있다. 또한, 상기 실시예에서는 IPv4 방식을 예로 들어 설명했으나, 이 외에도 IP 주소 공간을 하나 이상의 집단으로 분류하는 방식을 채택하는 IP 주소 방식에 대해서도 본 발명이 적용될 수 있음은 당연하다.

단계(206)에서 제1 판단 시스템(101)은 허용 데이터베이스(103)를 참조하여 상기 식별된 네트워크 그룹 정보가 허용 네트워크 그룹 정보인지 여부를 판단한다. 예를 들면, 추출된 IP 주소 정보가 254.254.254.254인 경우에 상기 식별된 네트워크 그룹 정보는 '254.254.254.xxx'이다. 기호 'xxx'에는 0 내지 255 중의 임의의 숫자가 들어갈 수 있다. 도 3의 허용 데이터베이스(103)로부터 상기 식별된 네트워크 그룹 정보 '254.254.254.xxx'는 허용 네트워크 그룹 정보라는 것을 알 수 있다.

또한 본 발명의 또 다른 실시예에 따르면, 제1 판단 시스템(101)은 단계(204)에서의 판단 결과 상기 추출된 IP 주소 정보가 허용 IP 주소 정보가 아닌 경우에만 단계(205 및 206)를 수행할 수도 있다.

단계(204)에서의 판단 결과 상기 추출된 IP 주소 정보가 허용 IP 주소 정보이거나, 또는 단계(206)에서의 판단 결과 상기 식별된 네트워크 그룹 정보가 허용 네트워크 그룹 정보인 경우 제1 판단 시스템(101)은 상기 명령어를 유효로

결정한다(단계(209)).

이와 같이 제1 판단 시스템(101)에서 유효로 결정된 명령어에 대해서는 제2 판단 시스템(102)은 상기 선정된 판단 방법에 따른 유효성 판단을 수행하지 않는다. 즉, 제1 판단 시스템(101)은 관공서나 대기업 등 불법적이고 악의적인 명령어를 입력하지 않을 가능성이 높은(신뢰성이 인정되는) 것으로 알려진 IP 주소에 대한 IP 주소 정보를 허용 데이터베이스(103)에 기록하여 두고 이를 이용하여 일부 명령어에 대해서는 유효성 여부를 간단하게 결정할 수 있다.

따라서, 일정한 규칙을 만족하는 명령어는 제1 판단 시스템(100)에서 간단하게 유효로 결정되고, 후술하는 바와 같이 제2 판단 시스템(200)에서의 복잡한 판단 과정은 생략되므로, 판단 시스템(100)에서의 전체 연산량 또는 기록해야 하는 데이터량이 감소되어 판단 시스템(100)의 부하가 감소될 수 있다.

또한, 본 발명의 또 다른 실시예에 따르면, 허용 데이터베이스(103)는 허용 IP 주소 정보 또는 허용 네트워크 그룹과 연관된 하나 이상의 차단 키워드를 더 기록하고 있다. 예를 들면 도 3에서 도시한 바와 같이, 허용 IP 주소 정보 '123.123.123.123'과 연관된 차단 키워드는 차단 키워드 '꽃배달'이다.

본 실시예에서 제1 판단 시스템(101)은 허용 IP 주소 정보 또는 허용 네트워크 주소 정보뿐만 아니라, 차단 키워드를 이용하여 명령어를 보다 정확하게 필터링 할 수 있다. 즉, 신뢰성이 인정되는 IP 주소를 갖는 단말기로부터 입력되는 명령어라고 하더라도, 상기 차단 키워드를 이용하여 상기 명령어가 유효 또는 무효인지 여부를 한번 더 판단할 수 있다.

단계(203)에서 제1 판단 시스템(101)은 명령어로부터 IP 주소 정보뿐만 아니라 요청 내용도 더 추출한다. 예를 들면, 사용자는 '꽃배달'이라는 키워드를 검색 시스템(120)으로 입력하면, 검색 시스템(120)은 이에 응답하여 도 4에 도시한 바와 같은 검색 결과 리스트를 상기 사용자에게 제공한다. 상기 사용자는 상기 검색 결과 리스트 중에서 검색 결과(예를 들면, 검색 결과(401))를 선택하기 위한 명령어를 입력한다. 이러한 명령어는 상기 사용자가 자신의 단말기(110)의 웹 브라우저에서 디스플레이 되는 검색 결과를 마우스 클릭하여 생성될 수 있다.

본 실시예에서는 단계(202)에서 입력되는 명령어가 검색 결과(401)를 마우스 클릭하여 생성되는 명령어인 경우를 예로 들어 설명한다. 즉, 상기 명령어에 포함된 요청 내용은 검색 결과(401)를 선택하는 것으로서, 보다 구체적으로는 검색 결과(401)과 연관된 웹 페이지로의 링크 요청일 수 있다.

상기 추출된 IP 주소 정보가 허용 IP 주소 정보인 경우, 단계(207)에서 제1 판단 시스템(101)은 허용 데이터베이스(103)를 참조하여 상기 허용 IP 주소 정보와 연관된 차단 키워드를 검색한다. 또는 식별된 네트워크 그룹 정보가 허용 네트워크 그룹 정보인 경우, 단계(207)에서 제1 판단 시스템(101)은 허용 데이터베이스(103)를 참조하여 상기 허용 네트워크 그룹 정보와 연관된 차단 키워드를 검색한다. 예를 들면, 상기 추출된 IP 주소 정보가 '123.123.123.123'인 경우, 상기 추출된 IP 주소 정보는 허용 IP 주소 정보이고, 도 3으로부터 상기 허용 IP 주소 정보와 연관된 차단 키워드는 '꽃배달'임을 알 수 있다.

이와 같이, 검색 결과 하나 이상의 차단 키워드가 검색되는 경우, 단계(208)에서 제1 판단 시스템(101)은 상기 요청 내용과 상기 차단 키워드가 연관되어 있는지 여부를 판단한다. 예를 들면, 제1 판단 시스템(101)은 차단 키워드와 요청 내용이 소정의 규칙에 부합하는 경우 연관성이 있다고 판단할 수 있으며 상기 규칙은 실시예에 따라 판단 시스템(100)의 관리자에 의해 적절하게 선택, 저장될 수 있다.

단계(207)에서 검색된 차단 키워드가 '꽃배달'이고, 단계(203)에서 추출된 요청 내용이 '꽃배달'에 대한 검색 요청에 따라 제공된 검색 결과 리스트 중 하나의 검색 결과를 선택하기 위한 것이기 때문에, 본 실시예에서 제1 판단 시스템(101)은 상기 차단 키워드 '꽃배달'과 상기 요청 내용은 연관되어 있다고 판단할 수 있다.

이와 같이 차단 키워드와 상기 요청 내용이 연관되어 있는 경우, 즉 상기 명령어가 신뢰할 만한 IP 주소 또는 신뢰할 만한 네트워크 그룹에 포함되는 IP 주소로부터 입력된 경우에도, 상기 명령어에 포함된 요청 내용이 차단 키워드와 연관되어 있는 경우에는 상기 명령어를 바로 유효로 판단하지 않고 제2 판단 시스템(102)에서 상기 선정된 판단 방법에 따른 추가적인 유효성 판단이 수행되도록 하여 보다 정확하게 명령어의 유효성을 판단할 수 있도록 한다. 제2 판단 시스템(102)에서의 유효성 판단 과정은 도 6을 이용하여 후술한다.

한편, 단계(207)에서 상기 허용 IP 주소 정보 또는 상기 허용 네트워크 그룹 정보와 연관된 차단 키워드가 검색되지 않는 경우, 또는 하나 이상의 차단 키워드가 검색되었으나 단계(208)에서의 판단 결과 검색된 차단 키워드와 상기 요청 내용 사이의 연관성이 인정되지 않는 경우, 예를 들면, 상기 요청 내용은 키워드 '마케팅'에 대한 키워드 검색을 요청하기 위한 것이고 상기 검색된 차단 키워드는 '꽃배달'인 경우, 제1 판단 시스템(101)은 상기 명령어를 유효로 판단하고(단계(209)), 제2 판단 시스템(102)은 상기 명령어에 대한 유효성 판단을 수행하지 않는다.

즉, 제1 판단 시스템(101)은 명령어에 포함된 IP 주소 정보 및 요청 내용과, 허용 데이터베이스(103)에 기록되어 있는 데이터를 이용하여 간단하게 유효로 판단할 수 있는 명령어를 필터링(filtering)한다. 또한, 제1 판단 시스템(101)은 명령어에 포함된 IP 주소 정보 및 요청 내용과, 허용 데이터베이스(103)에 기록되어 있는 데이터만을 이용해서는 간단하게 유효로 판단할 수 없는 명령어에 대해서는 제2 판단 시스템(102)에서 보다 정교한 유효성 판단이 수행되도록 한다.

또한, 본 발명의 또 다른 실시예에 따르면, 허용 데이터베이스(103)에 허용 IP 주소 정보 또는 허용 네트워크 그룹 정보와 연관하여 차단 키워드 대신 허용 키워드가 기록되어 있을 수도 있다.

제1 판단 시스템(101)은 소정의 명령어에 포함된 IP 주소 정보가 허용 IP 주소 정보인 경우, 허용 데이터베이스(103)에서 상기 허용 IP 주소 정보와 연관된 허용 키워드를 검색한다. 제1 판단 시스템(101)은 상기 명령어에 포함된 요청 내용과 상기 허용 키워드가 연관되어 있는 경우에는 상기 명령어를 유효로 판단하고, 상기 요청 내용과 상기 허용 키워드의 연관성이 인정되지 않는 경우에는 상기 명령어의 유효 여부를 판단할 수 없으므로 제2 판단 시스템(102)에서 상기 명령어에 대한 유효성 판단이 수행되도록 한다.

또한, 도 3에 도시한 바와 같이, 허용 데이터베이스(103)에는 어떤 허용 IP 주소 정보(또는 허용 네트워크 그룹 정보)에 대해서는 차단 키워드, 다른 허용 IP 주소 정보(또는 허용 네트워크 그룹 정보)에 대해서는 허용 키워드가 연관되어 기록되어 있을 수도 있다. 예를 들면, 제1 허용 IP 주소 정보와 연관해서는 차단 키워드가 기록되어 있고, 제2 허용 IP 주소 정보와 연관해서는 허용 키워드가 기록되어 있을 수도 있다.

이때, 제1 판단 시스템(101)은 상기 제1 허용 IP 주소로부터 입력되는 명령어에 대해서는 상기 명령어에 포함된 요청 내용이 상기 차단 키워드와 연관되어 있지 않은 경우, 상기 제2 허용 IP 주소로부터 입력되는 명령어에 대해서는 상기 명령어에 포함된 요청 내용이 상기 허용 키워드와 연관되어 있는 경우, 각각 해당 명령어를 유효로 판단하며, 그 반대의 경우에는 제2 판단 시스템(102)에서 해당 명령어에 대한 추가적인 유효성 판단이 수행되도록 한다.

이하, 본 발명의 또 다른 실시예에 따른 명령어의 유효성 판단 방법에 대해 설명한다. 본 실시예에 있어서 제1 판단 시스템(101)은 소정의 허용 키워드와 연관된 명령어는 유효로 판단하고, 상기 명령어에 대해서는 제2 판단 시스템(102)에서 추가적인 유효성 판단이 수행되지 않도록 한다.

제1 판단 시스템(101)의 관리자는 정치, 사회적인 이슈(issue)와 연관된 키워드, 경품 또는 이벤트와 연관된 키워드 등, 일정 기간 동안 사용자들의 관심이 급증하는 대상과 연관된 키워드를 허용 키워드로서 허용 데이터베이스(103)에 기록한다.

제1 판단 시스템(101)은 사용자로부터 입력된 명령어에 포함된 요청 내용을 추출하고 상기 요청 내용이 상기 허용 키워드와 연관되어 있는지 여부를 판단한다. 판단 결과, 상기 요청 내용이 상기 허용 키워드와 연관되어 있는 경우 제1 판단 시스템(101)은 상기 명령어를 무효로 유효로 판단한다.

반대로, 상기 요청 내용이 상기 허용 키워드와 연관되어 있지 않은 경우에는 제1 판단 시스템(101)은 제2 판단 시스템(102)에서 상기 명령어에 대한 유효성 판단이 수행되도록 한다.

본 실시예는 상술한 바와 같이 사용자들의 관심이 급증한 대상과 연관된 키워드를 허용 키워드로 설정하여, 상기 명령어가 제2 판단 시스템(102)에서의 판단 결과 평소에 비해 비정상적으로 다수 입력되는 명령어로서 불법적인 의도로 입력되는 명령어로 오인되는 것을 방지한다.

또한, 본 발명의 또 다른 실시예에 따르면, 제1 판단 시스템(101)은 선정된 허용 키워드와 연관된 명령어의 기간 별 입력 횟수를 산출하고, 상기 기간 별 입력 횟수를 이용하여 허용 데이터베이스(103)를 갱신한다. 예를 들면 상기 기간 별 입력 횟수가 소정값 이하로 떨어지는 경우에는 상기 허용 키워드와 연관된 대상에 대한 사용자들의 관심이 감소하고 있다고 판단할 수 있고, 이러한 판단에 따라 지금까지는 허용 키워드였던 상기 키워드를 더 이상 허용 키워드로서 유지하는 것은 바람직하지 않다. 즉, 상기 허용 키워드는 허용 데이터베이스(103)로부터 제거된다.

이하, 도 5를 참조하여 본 발명의 또 다른 실시예에 따른 명령어의 유효성 판단 방법에 대해 설명한다. 본 실시예에 있어서, 허용 데이터베이스(103)에는 허용 IP 주소 정보, 허용 네트워크 그룹 정보가 기록되어 있고, 차단 데이터베이스(104)에는 차단 IP 주소 정보, 차단 네트워크 그룹 정보가 기록되어 있다. 허용 데이터베이스(103) 및 차단 데이터베이스(104)는 동일한 장치로 구현될 수 있다.

허용 데이터베이스(103)에 기록되는 허용 IP 주소 정보 또는 허용 네트워크 그룹 정보는 정상적인 명령어를 입력할 것으로 인정되는 단말기의 IP 주소 또는 상기 IP 주소가 포함되는 네트워크 그룹에 대한 것이다.

차단 데이터베이스(104)에 기록되는 차단 IP 주소 정보 또는 차단 네트워크 그룹 정보는, 소정의 IP 주소 또는 소정의 네트워크 그룹으로부터 입력되는 명령어는 유효로 판단하지 않는 것이 바람직한 경우의 상기 IP 주소 또는 상기 네트워크 그룹에 대한 것이다. 예를 들면, 제1 판단 시스템(101)은 검색 시스템(120)에서 제공하는 서비스에 부합되지 않는 불법적/악의적 의도로 명령어를 입력할 가능성이 높다고 인정되는 단말기의 IP 주소(또는 상기 IP 주소가 포함되는 네트워크 그룹)에 대한 IP 주소 정보(또는 네트워크 그룹 정보)를 차단 IP 주소 정보(또는 네트워크 그룹 정보)로 선정할 수 있다. 이러한 단말기로부터 입력되는 명령어는 무효인 경우가 많으므로 제2 판단 시스템(102)에서의 복잡한 명령어 판단 과정을 거치지 않고도 바로 무효로 결정함으로써 판단 시스템(100)에서의 부하를 감소시키고 상기 단말기의 사용자가 새로운 방식으로, 예를 들면 새로운 방식의 불법 명령어 자동 입력 프로그램을 사용하여 이제까지와는 다른 패턴을 갖는 불법적인 명령어를 입력하고자 하는 경우 이를 원천적으로 차단하고자 한 것이다.

또한, 본 발명의 또 다른 실시예에 따르면, 제1 판단 시스템(101)은 판단 시스템(100)의 개발자 또는 관리자의 단말기의 IP 주소에 대한 IP 주소 정보를 차단 IP 주소 정보로 선정할 수 있다. 상기 개발자 등은 검색, 검색 결과 선택 등 판단 시스템(100)이 예상한 원래의 목적으로 검색 시스템(120)에 명령어를 입력하는 것이 아니라, 판단 시스템(100)이 제대로 동작하고 있는지 시험해보기 위해 명령어를 입력하는 경우가 많다. 따라서, 상기 개발자 등의 명령어 입력을 유효로 판단하고, 상기 유효인 명령어에 기초하여 검색 시스템(120)에서의 광고를 의뢰한 광고주에게 소정의 광고비를 과금하는 것은 바람직하지 않다. 제1 판단 시스템(101)은 상기 개발자 등의 단말기에 대한 IP 주소 정보 또는 네트워크 그룹 정보를 차단 IP 주소 정보 또는 차단 네트워크 그룹 정보로 선정함으로써 이러한 문제를 방지한다.

또한, 검색 시스템(120)이 검색과 관련하여 소정의 광고 서비스를 제공하는 경우, 이러한 광고 서비스를 이용하는 광고주의 단말기의 IP 주소, 또는 상기 IP 주소가 포함되는 네트워크 그룹 역시 차단 IP 주소 또는 차단 네트워크 그룹으로 결정될 수 있다. 광고주 역시 검색, 검색 결과 선택 등 원래의 목적으로 소정의 명령어를 입력하기 보다는 검색 시스템(120)에서의 광고가 제대로 수행되고 있는지 여부를 확인하기 위해 명령어를 입력하는 경우가 많기 때문이다. 단계(502)에서 제1 판단 시스템(101)은 사용자의 단말기(110)로부터 명령어를 입력 받고, 단계(503)에서 제1 판단 시스템(101)은 상기 명령어에 포함된 IP 주소 정보를 추출한다.

단계(504)에서 판단 시스템(101)은 허용 데이터베이스(103)를 참조하여 상기 추출된 IP 주소 정보가 허용 IP 주소 정보인지 여부를 판단한다.

또는, 단계(505)에서 판단 시스템(101)은 상기 IP 주소 정보를 이용하여 상기 IP 주소와 연관된 네트워크 그룹에 대한 네트워크 그룹 정보를 식별한다. 단계(506)에서 제1 판단 시스템(101)은 허용 데이터베이스(102)를 참조하여 상

기 식별된 네트워크 그룹 정보가 허용 네트워크 그룹 정보인지 여부를 판단한다. 한편, 본 발명의 또 다른 실시예에 따르면, 제1 판단 시스템(101)은 단계(504)에서의 판단 결과 상기 추출된 IP 주소 정보가 허용 IP 주소 정보가 아닌 경우에만 단계(505 및 506)를 수행할 수도 있다.

단계(504)에서의 판단 결과 상기 추출된 IP 주소 정보가 허용 IP 주소 정보이거나, 또는 단계(506)에서의 판단 결과 상기 식별된 네트워크 그룹 정보가 허용 네트워크 그룹 정보인 경우 제1 판단 시스템(101)은 상기 명령어를 유효로 결정한다(단계(510)). 이 경우 제2 판단 시스템(102)은 상기 명령어에 대한 유효성 판단을 수행하지 않는다.

판단 결과 상기 추출된 IP 주소 정보가 허용 IP 주소 정보가 아니고, 상기 식별된 네트워크 그룹 정보가 허용 네트워크 그룹 정보도 아닌 경우, 단계(507)에서 제1 판단 시스템(101)은 차단 데이터베이스(104)를 참조하여 상기 추출된 IP 주소 정보가 차단 IP 주소 정보인지 여부를 판단한다.

또는, 단계(508)에서 제1 판단 시스템(101)은 차단 데이터베이스(104)를 참조하여 상기 식별된 네트워크 그룹 정보가 차단 네트워크 그룹 정보인지 여부를 판단한다. 한편, 본 발명의 또 다른 실시예에 따르면, 제1 판단 시스템(101)은 단계(507)에서의 판단 결과 상기 추출된 IP 주소 정보가 허용 IP 주소 정보가 아닌 경우에만 단계(508)를 수행할 수도 있다.

판단 결과 상기 추출된 IP 주소 정보가 차단 IP 주소 정보인 경우, 또는 상기 식별된 네트워크 그룹 정보가 차단 네트워크 그룹 정보인 경우, 단계(509)에서 제1 판단 시스템(101)은 상기 명령어를 무효로 결정한다. 이 경우 제2 판단 시스템(102)은 상기 명령어에 대한 유효성 판단을 수행하지 않는다.

본 실시예에 따라 제1 판단 시스템(101)에서 유효성이 결정되지 않은 명령어는, 제2 판단 시스템(102)에서 그 유효성이 판단된다. 즉, 제1 판단 시스템(101)에서는 소정의 규칙을 만족하는 명령어는 간단하게 유효 또는 무효로 결정하고, 유효 또는 무효 여부가 결정되지 않은 명령어에 대해서만 제2 판단 시스템(102)에서 추가적인 유효성 판단이 수행되도록 함으로써, 판단 시스템(100)에서의 시스템 부하를 감소시키고 있다.

이하, 제2 판단 시스템(102)에서 제1 판단 시스템(101)에 의해 필터링된 명령어에 대해 선정된 판단 방법에 따라 유효성 여부를 판단하는 과정을 도 6을 참조하여 구체적으로 설명한다.

제2 판단 시스템(102)은 단계(601)에서 상기 입력된 명령어의 요청 형식을 해석하고, 단계(602)에서 상기 요청 형식에 기초하여 상기 명령어의 유효성을 판단한다.

본 발명의 또 다른 실시예에 따르면, 요청 형식에 기초하여 판단한 결과 상기 명령어가 무효라고 판단되는 경우에는, 상기 명령어에 대해 단계(603) 이하의 판단 과정은 수행하지 않을 수 있다.

단계(603)에서 판단 시스템(100)은 상기 명령어와 연관된 로그(log) 정보를 생성한다. 상기 로그 정보는 상기 추출된 IP 주소 정보, 상기 명령어가 검색 시스템(120)로 입력된 시점에 대한 입력 시점 정보, 상기 명령어에 포함된 요청 내용 등을 포함할 수 있다.

단계(604)에서 제2 판단 시스템(102)은 상기 로그 정보를 로그 데이터베이스(105)에 기록한다. 도 7은 로그 데이터베이스(105)에 기록되는 로그 정보의 일례를 도시한 도면이다. 도 7에 도시한 바와 같이, 본 발명의 또 다른 실시예에 따르면, 상기 로그 정보는 명령어의 입력 시점에 따라 정렬되거나, 상기 IP 주소 정보와 연관하여 체계적으로 기록될 수 있다. 또한, 로그 데이터베이스(105)에는 사용자로부터 입력된 명령어에 대응하는 로그 정보 외에도, 상기 사용자가 검색 시스템(120)에 접속한 경우 상기 접속과 관련된 로그 정보(701), 검색 시스템(120)이 상기 사용자에게 제공한 정보와 연관된 로그 정보(예를 들면, 상기 사용자에게 제공된 검색 결과 목록과 관련된 로그 정보(702))도 기록될 수 있다.

단계(605)에서 제2 판단 시스템(102)은 상기 로그 정보를 이용하여 상기 명령어의 유효성을 판단한다. 제2 판단 시스템(102)은 상기 명령어와 연관하여 생성된 로그 정보만을 이용할 수도 있고, 로그 데이터베이스(105)에 기록된 하나 이상의 로그 정보를 더 이용하여 상기 명령어의 유효성을 판단할 수도 있다.

이하에서는, 실시예에 따라 요청 형식에 기초하여 명령어의 유효성을 판단하는 과정(단계(602)), 및 로그 정보를 이용하여 명령어의 유효성을 판단하는 과정(단계(605))을 구체적으로 설명한다.

1. 명령어의 요청 형식에 기초하여 상기 명령어의 유효성을 판단하는 과정

(1) 명령어의 HTTP 버전에 기초하여 명령어의 유효성을 판단하는 경우

본 실시예에 따르면, 상기 요청 형식은 상기 명령어를 작성하기 위해 사용된 HTTP(Hyper Text Transfer Protocol)의 버전(version)이다.

검색 시스템(120)에 악의적인 의도로 명령어를 입력하기 위해, 사용자는 명령어를 수동으로 발생시키지 않고, 소정의 명령어가 '자동적으로' 생성되도록 하는 프로그램을 이용하는 경우가 있다.

일반적으로 인터넷 상에서 명령어는 HTTP에 따라 작성되며, HTTP의 버전이 낮을수록 그 내용이 단순하고 널리 알려져 있기 때문에, 최신 버전보다는 낮은 버전을 이용하여 상기 프로그램을 작성하는 경우가 많다. 이와 같이, 일반적으로 사용되지 않는 버전의 HTTP에 의해 명령어가 작성된 경우에는 상기 명령어가 무효일 가능성이 높다.

예를 들면, HTTP/1.1 버전이 일반적으로 사용되는 경우, 판단 서버(101)는 상기 HTTP/1.1 버전을 유효 버전으로 선정하고, 상기 명령어의 HTTP 버전을 식별하여 상기 명령어가 유효 버전(즉, HTTP/1.1) 이외의 버전, 예를 들면 HTTP/1.0 버전이나, HTTP/1.1 이후의 버전으로 작성된 경우 단계(203)에서 상기 명령어가 무효일 가능성이 높다고 판단할 수 있다. 명령어의 유효성을 판단하기 위한 기준이 되는 유효 버전은 시간의 흐름에 따라 변경될 수 있다.

(2) 명령어에 포함된 부가 정보에 기초하여 명령어의 유효성을 판단하는 경우

본 실시예에 따르면, 상기 요청 형식은 상기 명령어에 포함된 부가 정보의 유무이다. 예를 들면, 상기 부가 정보는 상기 단말기에 설치된 웹 브라우저의 브라우저 정보 또는 상기 단말기가 직전에 접속한 웹 페이지의 URL 정보이다.

일반적으로 웹 브라우저는 검색 시스템(120)의 검색 서버 등의 서버에 접속하여 명령어를 전송하는 경우 HTTP에 따라 상기 서버에 웹 브라우저의 종류 또는 버전에 대한 웹 브라우저 정보를 상기 명령어에 포함시켜 전송하는 경우가

많다. 또한, 웹 브라우저는 상기 웹 브라우저가 직접에 접속한 웹 페이지의 URL 정보를 HTTP에 따라 상기 명령어에 포함시켜 전송하는 경우가 많다.

따라서, 상기와 같은 부가 정보가 포함되지 않은 명령어는 명령어 자동 생성 프로그램에 의해 자동적으로 생성되었을 가능성이 높다. 따라서, 제2 판단 시스템(102)은 상기 부가 정보가 상기 명령어에 포함되어 있는지 여부를 상기 명령어의 유효성 판단에 반영할 수 있다.

(3) 명령어에 포함된 식별 정보에 기초하여 명령어의 유효성을 판단하는 경우

제2 판단 시스템(102)은 명령어에 요청 내용 및 단말기의 IP 주소 정보 별로 식별 정보가 포함되도록 한다. 따라서, 상기 식별 정보를 포함하는 명령어의 입력 횟수를 산출하면, 동일 IP 주소 정보를 갖는 단말기로부터 동일 요청 내용을 포함하는 명령어가 몇 번 입력되었는지 여부를 판단할 수 있다.

사용자는 특정 요청을 하기 위한 명령어, 예를 들면 검색 결과를 선택하기 위한 명령어는 한번 입력하는 것이 일반적일 것이다. 따라서, 판단 서버(101)는 동일 식별 정보를 갖는 명령어가 소정값, 예를 들면 두 번 이상 입력되는 경우 상기 식별 정보를 포함하는 명령어는 무효라고 판단할 수 있다.

(4) 소정의 이벤트가 발생한 이후 일정 시간 내에 명령어가 입력된 경우

제2 판단 시스템(102)은 소정의 이벤트가 발생하고, 상기 이벤트에 따라 생성되는 명령어가 상기 이벤트 발생 이후 너무 짧은 시간 이내에 입력되는 경우 상기 명령어를 무효로 판단할 수 있다.

예를 들면, 상기 이벤트는 검색 시스템(102)이 사용자의 검색 요청에 따라 소정의 검색 결과 목록을 상기 사용자에게 제공하는 것이다. 상기 검색 결과 목록을 제공 받은 사용자는 상기 검색 결과 목록에 포함된 특정 검색 결과를 선택하기 위한 명령어를 입력할 수 있다.

이때, '사람'이 상기 명령어를 입력하기 위해서는 '상기 검색 결과 목록을 인식하고, 적절한 검색 결과를 파악하고 선택하는' 등의 일련의 과정을 거쳐야 하며, 이러한 과정을 수행하기 위해서는 일정한 시간이 필요하다.

따라서, 상기 검색 결과 목록을 제공한 시점으로부터 상기 사용자가 검색 결과를 선택하는 명령어를 입력하기까지의 시간 간격이 너무 짧은 경우(예를 들면 0.5 초인 경우)에는 제2 판단 시스템(102)은 상기 명령어를 무효로 판단할 수 있다.

(5) 암호화/복호화 방법을 이용하여 명령어의 유효성을 판단하는 경우

판단 시스템(100)은 검색 시스템(120)의 검색 서버 등 서비스 서버로 사용자가 명령어를 입력하는 경우, 상기 명령어에 암호화된 정보가 포함되도록 제어한다.

예를 들면, 상기 명령어에 어떤 채널을 통해 입력된 경인지, 상기 채널의 어떤 정보와 연관되어 입력됐는지 여부에 대한 정보를 암호화 하여 포함시킬 수 있다.

실시예에 따라, 상기 암호화 방법은 HTTP에서 제공하는 암호화 규약에 따른 것일 수 있다. 또한, 본 발명의 또 다른 실시예에 따르면, 판단 시스템(100)은 상기 암호화 알고리즘을 포함하는 프로그램을 플러그 인(plug-in) 형태로 단말기(110)에 제공할 수 있고, 단말기(110)는 상기 프로그램을 설치하여 상기 암호화 알고리즘에 따라 명령어를 암호화할 수도 있다.

제2 판단 시스템(102)은 상기 암호화 된 명령어를 입력 받아 복호화 한다.

제2 판단 시스템(102)은 상기 명령어가 암호화 되어 있지 않거나, 상기 명령어가 상기 복호화 방법에 의해 해독되지 않는다면, 상기 명령어가 무효라고 판단한다.

2. 로그 정보를 이용하여 명령어의 유효성을 판단하는 과정

(1) '특정 IP 주소 정보'를 포함하는 명령어가 일정한 시간 간격으로 입력되는 경우와 같이 명령어의 입력 시점이 소정의 규칙성을 갖는 경우

제2 판단 시스템(102)은 로그 데이터베이스(105)에 기록된 로그 정보 중에서, 상기 명령어에 포함된 IP 주소 정보를 포함하는 로그 정보를 검색한다. 본 발명의 또 다른 실시예에 따르면, 제2 판단 시스템(102)은 상기 IP 주소 정보를 포함하는 로그 정보 중 일정 기간 내 기록된 로그 정보만을 검색할 수도 있다.

상기 검색된 로그 정보를 제1 로그 정보라 하면, 제2 판단 시스템(102)은 상기 제1 로그 정보에 포함된 입력 시점 정보를 추출하고, 상기 추출된 입력 시점 정보의 전부 또는 일부가 소정의 규칙에 따른 연관성을 갖는 경우 상기 명령어를 무효로 판단한다.

예를 들면, 상기 명령어가 입력된 시점이 '2004/04/02, 09:00:30'이고 상기 제1 로그 정보에 포함된 입력 시점 정보가 각각 '2004/04/02, 08:50:30', '2004/04/02, 08:40:30', '2004/04/02, 08:30:30', '2004/04/02, 08:20:30'...인 경우, 상기 제1 로그 정보와 연관된 명령어가 10분 간격으로 검색 시스템(120)으로 입력되었다는 사실을 알 수 있다. 상기 규칙성은, 이와 같이 명령어가 입력된 입력 시점의 시간 간격이 일정한 경우 외에도, 예를 들면 상기 시간 간격이 등차 수열 또는 등비 수열로 증가하는 경우 등과 같이 수학적인 규칙성이 발견되는 경우를 모두 포함할 수 있다.

이와 같이, 특정한 IP 주소 정보를 포함하는 명령어의 입력 시점에 규칙성이 인정되는 경우, 상기 명령어는 명령어를 자동적으로 발생시키는 프로그램 등을 이용하여 발생한 명령어일 가능성이 크기 때문에, 제2 판단 시스템(102)은 상기 명령어를 무효로 판단한다.

본 발명의 또 다른 실시예에 따르면, 제2 판단 시스템(102)은 상기 검색된 입력 시점 정보들 중에서 소정의 규칙을 따르는 입력 시점 정보의 수가 일정 개수 이상인 경우에만 상기 명령어를 무효로 판단할 수 있다.

또한, 본 발명의 또 다른 실시예에 따르면, 제2 판단 시스템(102)은 상기 규칙을 따르는 입력 시점 정보를 포함하는 로그 정보를 식별하고, 상기 식별된 로그 정보와 연관된 명령어를 모두 무효로 판단할 수 있다. 즉, 소정의 IP 주소를 갖는 단말기로부터 입력된 명령어의 입력 시점에 규칙성을 갖는 것이 판명된 명령어들의 집합은 모두 무효로 처리한다.

(2) '특정 요청 내용'을 포함하는 명령어가 일정한 시간 간격으로 입력되는 경우와 같이 명령어의 입력 시점이 소정의 규칙성을 갖는 경우

제2 판단 시스템(102)은 로그 데이터베이스(105)에 기록된 로그 정보 중에서, 상기 명령어에 포함된 요청 내용을 포함하는 로그 정보를 검색한다. 본 발명의 또 다른 실시예에 따르면, 제2 판단 시스템(102)은 상기 IP 주소 정보를 포함하는 로그 정보 중 일정 기간 내 기록된 로그 정보만을 검색할 수도 있다.

상기 검색된 로그 정보를 제1 로그 정보라 하면, 제2 판단 시스템(102)은 상기 제1 로그 정보에 포함된 입력 시점 정보를 추출하고, 상기 추출된 입력 시점 정보의 전부 또는 일부가 소정의 규칙에 따른 연관성을 갖는 경우 상기 명령어를 무효로 판단한다.

예를 들면, 상기 명령어가 입력된 시점이 '2004/04/02, 09:00:30'이고 상기 제1 로그 정보에 포함된 입력 시점 정보가 각각 '2004/04/02, 08:50:30', '2004/04/02, 08:40:30', '2004/04/02, 08:30:30', '2004/04/02, 08:20:30'...인 경우, 상기 제1 로그 정보와 연관된 명령어가 10분 간격으로 검색 시스템(120)로 입력되었다는 사실을 알 수 있다. 상기 규칙성은, 이와 같이 명령어가 입력된 입력 시점의 시간 간격이 일정한 경우 외에도, 예를 들면 상기 시간 간격이 등차 수열 또는 등비 수열로 증가하는 경우 등과 같이 수학적인 규칙성이 발견되는 경우를 모두 포함할 수 있다.

이와 같이, 특정한 요청 내용을 포함하는 명령어의 입력 시점에 규칙성이 인정되는 경우, 상기 명령어는 명령어를 자동적으로 발생시키는 프로그램 등을 이용하여 발생한 명령어일 가능성이 크기 때문에, 판단 서버(101)는 상기 명령어를 무효로 판단한다.

본 발명의 또 다른 실시예에 따르면, 제2 판단 시스템(102)은 상기 검색된 입력 시점 정보들 중에서 소정의 규칙을 따르는 입력 시점 정보의 수가 일정 개수 이상인 경우에만 상기 명령어를 무효로 판단할 수 있다.

또한, 본 발명의 또 다른 실시예에 따르면, 제2 판단 시스템(102)은 상기 규칙을 따르는 입력 시점 정보를 포함하는 로그 정보를 식별하고, 상기 식별된 로그 정보와 연관된 명령어를 모두 무효로 판단할 수 있다. 즉, 소정의 IP 주소를 갖는 단말기로부터 입력된 명령어의 입력 시점에 규칙성을 갖는 것이 판명된 명령어들의 집합은 모두 무효로 처리한다.

(3) 일정 기간 동안 특정 IP 주소를 갖는 단말기로부터의 명령어의 수가 비정상적으로 다수 입력되는 경우

제2 판단 시스템(102)은 로그 데이터베이스(105)에 제1 기간 동안 기록된 로그 정보를 이용하여 각 단말기로부터 상기 제1 기간 동안 입력된 명령어의 제1 개수를 산출한다. 각 단말기를 식별하기 위해 네트워크 주소가 사용될 수 있다. 즉, 동일 네트워크 주소를 갖는 단말기로부터 입력된 명령어는 하나의 단말기로부터 입력된 것으로 볼 수 있다. 단, 상기 네트워크 주소가 프락시 서버 또는 공유기의 네트워크 주소인 경우에는 예외로 한다.

제2 판단 시스템(102)은 로그 데이터베이스(105)에 제2 기간 동안 기록된 로그 정보를 이용하여 상기 명령어에 포함된 상기 네트워크 주소를 갖는 단말기로부터 상기 제2 기간 동안 입력된 명령어의 제2 개수를 산출한다.

상기 제1 기간은 상기 제2 기간과 동일할 수도 있으나, 상기 제1 기간은 상기 제2 기간에 비해 큰 값으로 선정하는 것이 바람직하다. 또한, 상기 제2 기간은 오전, 오후, 저녁, 심야, 새벽 등 특정 시기의 기간을 선정함으로써 특정 시기별로 명령어가 입력되는 패턴을 고려하여 명령어의 유효성을 판단할 수 있다. 예를 들면, 새벽 4시경에는 명령어가 입력되는 횟수가 현저히 감소하기 때문에 이를 반영하여 유효성 판단을 할 수도 있다.

제2 판단 시스템(102)은 상기 단말기 별 제1 개수와 상기 제2 개수를 이용하여 상기 명령어의 유효성을 판단할 수 있다.

예를 들면, 제2 판단 시스템(102)은 상기 단말기 별 제1 개수의 평균값을 산출하여 상기 제2 개수와 상기 평균값을 비교하여 상기 명령어의 유효성을 판단한다. 제2 판단 시스템(102)은 상기 제2 개수가 상기 평균값을 초과하는 경우, 또는 상기 평균값에 소정값을 더한 값을 초과하는 경우 상기 명령어를 무효로 판단할 수 있다. 또한, 제2 판단 시스템(102)은 상기 평균값과 상기 제2 개수의 비율을 산출하여 상기 비율이 소정값을 초과하는 경우 상기 명령어를 무효로 판단할 수도 있다.

또한, 제2 판단 시스템(102)은 상기 단말기 별 제1 개수 중 최대값을 산출하거나, 또는 상기 단말기 별 제1 개수의 분산값을 산출하고 상기 최대값 또는 상기 분산값과 상기 제2 개수를 비교하여 상기 명령어의 유효성을 판단할 수도 있다.

한편, 상기에서는 상기 단말기 별 제1 개수, 또는 이들의 평균값 등을 이용하는 경우를 구체적으로 예로 들어 설명했으며, 이러한 방식은 후술하는 각 판단 과정에서 제1 개수와 제2 개수를 비교하여 제2 개수에 비해 제1 개수가 비정상적으로 많은지 여부를 판단하는 경우에 모두 적용될 수 있다. 또한, 상술한 바와 같은 제1 개수와 제2 개수를 비교하는 구체적인 방법은 예시적인 것에 불과하며, 본 발명의 범위는 이에 한정되지 않고 소정의 의미를 갖는 제1 개수와 또 다른 소정의 의미를 갖는 제2 개수를 비교하여 명령어의 유효성을 판단하는 모든 판단 방법에 미친다.

(4) 일정 기간 동안 입력된 특정 명령어의 수가 비정상적으로 다수인 경우

제2 판단 시스템(102)은 로그 데이터베이스(105)에 제1 기간 동안 기록된 로그 정보를 이용하여 상기 제1 기간 동안 입력된 명령어의 제1 개수를 요청 내용에 따라 각각 산출한다. 즉, 상기 제1 기간 동안 입력된 명령어 주에서 동일 요청 내용을 포함하는 명령어의 수를 각각 산출한다.

제2 판단 시스템(102)은 로그 데이터베이스(105)에 제2 기간 동안 기록된 로그 정보를 이용하여 상기 명령어에 포함된 요청 내용을 포함하는 로그 정보의 제2 개수를 산출한다. 상기 제2 개수는 상기 제2 기간 동안 입력된 명령어 중에서 상기 명령어와 동일한 요청 내용을 포함하는 명령어의 개수이다.

제2 판단 시스템(102)은 상기 요청 내용 별 제1 개수와 상기 제2 개수를 이용하여 상기 명령어의 유효성을 판단할 수 있다. 즉, 제2 판단 시스템(102)은 상기 단말기 별 그리고 상기 요청 내용 별 제1 개수와 상기 제2 개수를 비교하여 상기 제2 개수가 상기 제1 개수에 비해 비정상적으로 크다고 판단되는 경우 상기 명령어를 무효로 판단할 수 있다. 상기 제1 개수와 상기 제2 개수의 비교 방법의 구체적인 예는 상술한 바와 같다.

(5) 일정 시간 동안 특정 IP 주소를 갖는 단말기로부터의 특정 요청을 하기 위한 명령어의 수가 비정상적으로 다수 입력되는 경우

제2 판단 시스템(102)은 로그 데이터베이스(105)에 제1 기간 동안 기록된 로그 정보를 이용하여 각 단말기로부터 상기 제1 기간 동안 입력된 명령어의 제1 개수를 요청 내용 별로 산출한다. 즉, 소정의 단말기로부터 소정의 요청 내용이 포함된 명령어가 상기 제1 기간 동안 몇 개 입력되었는지 각각 산출한다. 각 단말기를 식별하기 위해 IP 주소가 사용될 수 있다. 즉, 동일 IP 주소로부터 입력된 명령어는 하나의 단말기로부터 입력된 것으로 볼 수 있다.

제2 판단 시스템(102)은 로그 데이터베이스(105)에 제2 기간 동안 기록된 로그 정보를 이용하여 상기 명령어에 포함된 상기 IP 주소를 갖는 단말기로부터 상기 제2 기간 동안 입력된 명령어 중 상기 요청 내용을 포함하는 명령어의 제2 개수를 산출한다.

상기 제1 기간은 상기 제2 기간과 동일할 수도 있으나, 상기 제1 기간은 상기 제2 기간에 비해 큰 값으로 선정하는 것이 바람직하다. 또한, 상기 제2 기간은 오전, 오후, 저녁, 심야, 새벽 등 특정 시기의 기간을 선정함으로써 특정 시기별로 명령어가 입력되는 패턴을 고려하여 명령어의 유효성을 판단할 수 있다. 예를 들면, 새벽 4시경에는 명령어가 입력되는 횟수가 현저히 감소하기 때문에 이를 반영하여 유효성 판단을 할 수도 있다.

제2 판단 시스템(102)은 상기 단말기 별 그리고 상기 요청 내용 별 제1 개수와 상기 제2 개수를 비교하여 상기 제2 개수가 상기 제1 개수에 비해 비정상적으로 크다고 판단되는 경우 상기 명령어를 무효로 판단할 수 있다.

(6) 2차 명령어와 연관된 1차 정보가 존재하지 않는 경우

검색 시스템(120)은 사용자로부터 검색 쿼리를 입력 받고 상기 검색 쿼리에 대응하는 검색 결과 목록을 생성하여 상기 사용자에게 제공한다. 상기 검색 결과 목록을 제공 받은 상기 사용자는 상기 검색 결과 목록 중 검색 결과를 선택하고, 검색 시스템(120)은 상기 선택된 검색 결과에 대응하는 정보를 제공하거나, 상기 검색 결과와 연관된 웹 페이지로 상기 사용자가 접속하도록 중계한다. 이와 같이 검색 시스템(120) 또는 판단 시스템(100)과 사용자의 단말기(110) 사이에는 여러 정보들이 송수신(통신)된다.

본 명세서에서는 검색 시스템(120) 또는 판단 시스템(100)과 사용자 사이에서 통신되는 정보가 순차적인 인과 관계를 갖고 있는 경우, 원인이 되는 정보는 1차 정보, 상기 1차 정보에 기초하여 생성되는 결과 정보는 2차 정보로 정의한다. 또한, 상기 정보는 명령어를 포함한다.

예를 들면, 상기 검색 결과 목록은 상기 검색 쿼리에 기초하여 생성되는 것으로, 상기 검색 쿼리는 1차 명령어, 상기 검색 결과 목록은 2차 정보로 정의할 수 있다. 또한, 사용자가 상기 검색 결과를 선택하는 명령어를 입력하고 상기 선택 명령에 대응하여 상기 정보가 제공되는 경우, 상기 명령어는 1차 명령어, 상기 정보는 2차 정보로 정의할 수 있다.

제2 판단 시스템(102)은 사용자의 상기 단말기와 통신하는 정보에 대응하는 로그 정보를 생성하여 로그 데이터베이스(105)에 기록한다. 상기 로그 정보는 상기 정보 또는 상기 정보의 송수신 시점에 대한 정보를 포함한다.

제2 판단 시스템(102)은 상기 단말기로부터 입력된 명령어가 그 요청 내용으로 보아 2차 명령어로 판단된 경우, 로그 데이터베이스(105)를 참조하여 상기 명령어와 연관된 1차 정보(또는 1차 명령어)에 대응하는 로그 정보를 검색한다. 상기 명령어와 연관된 1차 정보에 대응하는 상기 로그 정보는 상기 2차 명령어에 포함된 질의의 내용, 상기 2차 명령어에 포함된 IP 주소 정보를 참조하여 검색될 수 있다.

2차 명령어는 1차 정보에 기초하여 발생되므로, 상기 1차 정보에 대응하는 로그 정보가 검색되지 않는다면, 상기 명령어는 정상적인 절차에 따라 입력된 명령어가 아니라고 할 수 있으므로, 제2 판단 시스템(102)은 상기 명령어를 무효로 판단할 수 있다.

(7) 2차 명령어와 연관된 1차 정보가 존재하지 않는 경우 - 명령어 자체에 포함된 정보를 이용하는 경우

정상적인 절차에 따라 명령어가 입력되는지 여부, 예를 들면 사용자의 웹 페이지 제공 요청에 따라 소정의 웹 페이지를 제공하고, 상기 사용자로부터 상기 웹 페이지에 포함된 정보를 이용한 추가 요청을 입력 받는 것과 같이, 정상적인 절차에 따르는 경우 상기 추가 요청은 상기 웹 페이지의 제공을 전제로 한다.

따라서, 제2 판단 시스템(102)은 명령어의 유효성을 판단하기 위해 명령어 자체에 상기와 같은 이력(history) 정보가 포함되도록 할 수 있다. 상기 이력 정보는 이후 상기 명령어의 유효성을 판단하는 기준이 되므로, 상기 이력 정보는 암호화되어 상기 명령어에 포함되도록 제어하는 것이 바람직하다.

제2 판단 시스템(102)은 사용자의 단말기로부터 제1 명령어를 입력 받고, 상기 제1 명령어에 따라 상기 사용자에게 소정의 정보를 포함하는 웹 페이지를 제공한다.

상기 사용자는 상기 정보에 기초하여 제2 명령어를 입력할 수 있다. 예를 들면, 상기 제1 명령어는 소정의 검색 쿼리를 포함한 검색 요청이며, 상기 제2 명령어는 검색 결과 목록 중 소정의 검색 결과를 선택하는 명령일 수 있다.

이때, 제2 판단 시스템(102)은 상기 제2 명령어에 이력 정보가 포함되도록 한다. 상기 이력 정보는 상기 단말기가 직전에 접속한 웹 페이지의 URL 정보(이러한 URL 정보는 웹 브라우저로부터 제공 받을 수도 있음), 상기 단말기의 제1 IP 주소, 또는 상기 제1 명령어를 입력한 단말기의 제2 IP 주소 등이다. 정상적인 경우 상기 단말기의 제2 IP 주소와 상기 제1 명령어를 입력한 단말기의 제1 IP 주소는 일치할 것이다.

이와 같은 구성에 따르면, 제2 판단 시스템(102)은 소정의 명령어가 입력되는 경우, 상기 명령어에 포함된 이력 정보를 이용하여 상기 명령어의 유효성 여부를 판단할 수 있게 된다.

예를 들면, 제2 판단 시스템(102)은 상기 명령어에 현재 또는 이전 웹 페이지에 대응하는 URL 정보가 포함되어 있지 않는 경우 상기 명령어를 무효로 할 수 있다.

또는, 제2 판단 시스템(102)은 상기 명령어에 URL 정보가 포함되어 있는 경우, 상기 URL이 정상적으로 상기 단말기가 명령어를 입력하기 위해 현재 접속 중, 또는 이전에 접속했어야 하는 웹 페이지의 URL이 아닌 경우에는 상기 명령어를 무효로 판단한다.

또한, 제2 판단 시스템(102)은 제1 명령어의 입력을 전제로 하여 생성될 수 있는 제2 명령어에, 제1 명령어를 입력한 단말기의 제1 IP 주소 정보가 포함되어 있지 않은 경우 상기 명령어를 무효로 판단할 수 있다.

또한, 제2 판단 시스템(102)은 상기 제2 명령어에 포함된 제1 IP 주소 정보와 제2 IP 주소 정보를 비교하여 일치하지 않는 경우 상기 제2 명령어를 무효로 판단한다.

(8) 일정 시간 동안 일정한 네트워크 그룹에서 특정한 질의의 수가 비정상적으로 다수인 경우

제2 판단 시스템(102)은 상기 식별된 네트워크 그룹 정보를 이용하여 상기 명령어의 유효성 여부를 판단한다.

판단 서버(101)는 로그 데이터베이스(102)에 기록된 로그 정보를 이용하여 제1 기간 동안 각 단말기로부터 입력된 명령어의 제1 개수를 요청 내용 별로 각각 산출한다. 제2 판단 시스템(102)은 동일 IP 주소를 갖는 단말기로부터 입력된 명령어는 하나의 단말기로부터 입력된 것으로 결정할 수 있다. 단, 상기 네트워크 주소가 프락시 서버 또는 공유기의 IP 주소인 경우에는 예외로 한다.

제2 판단 시스템(102)은 로그 데이터베이스(105)에 기록된 로그 정보를 이용하여 제2 기간 동안 동일 네트워크 그룹 정보와 연관되고 상기 요청 내용을 포함하는 명령어의 제2 개수를 산출한다.

제2 판단 시스템(102)은 상기 제1 개수 및 상기 제2 개수를 비교하여 상기 제2 개수가 상기 제1 개수에 비해 비정상적으로 다수인 경우 상기 명령어를 무효로 판단할 수 있다.

따라서, 본 실시예에 따르면, 동일 네트워크 클래스 등 동일 네트워크 그룹에 접속되어 있는 다수의 단말기를 이용하여 악의적인 의도로 소정의 명령어를 입력하는 경우 이를 감지할 수 있게 된다.

(9) 명령어에 포함된 식별 정보가 동일한 명령어가 중복적으로 입력되는 경우

본 실시예에 있어서, 제2 판단 시스템(102)은 사용자의 단말기로부터 소정의 정보를 요청하는 명령어를 입력 받는 경우, 상기 명령어에 상기 정보 또는 상기 단말기의 IP 주소와 연관된 식별 정보가 포함되도록 제어한다.

또한, 제2 판단 시스템(102)은 상기 명령어에 포함된 식별 정보를 참조하여 상기 식별 정보를 포함하는 명령어의 입력 횟수를 판단하고, 판단 결과 상기 식별 정보를 포함하는 명령어가 복수 개 입력된 경우에는 상기 명령어를 무효로 판단한다.

상기 구성에 따르면, 제2 판단 시스템(102)은 동일 단말기의 사용자가 동일 정보를 반복적으로 요청하는지 여부를 판단할 수 있게 되고, 한번 제공 받은 정보를 불필요하게 반복적으로 요청하는 명령어는 악의적인 의도로 입력된 명령어로 간주할 수 있을 것이다.

또한, 본 발명의 또 다른 실시예에 따르면, 제2 판단 시스템(102)은 동일한 식별 정보를 포함하는 모든 명령어를 무효로 판단할 수도 있고, 상기 식별 정보를 포함하는 명령어 중 시간적으로 가장 먼저 입력된 명령어를 제외한 명령어를 무효로 판단할 수도 있다.

이상, 제1 판단 시스템(101)에서 필터링 된 명령어에 대해 제2 판단 시스템(102)에서 수행되는, 요청 형식에 기초하여 명령어의 유효성을 판단하는 과정(단계(602)), 및 로그 정보를 이용하여 명령어의 유효성을 판단하는 과정(단계(605))을 구체적으로 설명했다. 제2 판단 시스템(102)은 상기와 같은 선정된 판단 방법을 하나 이상 채택할 수 있으며, 각 판단 방법에 따른 판단 결과를 종합적으로 검토하여 상기 명령어의 유효성 여부를 판단할 수도 있다. 또한, 제2 판단 시스템(102)은 각 판단 결과에 가중치를 부여하여 산출한 전체 판단 결과를 이용하여 상기 명령어의 유효성 여부를 판단할 수도 있다.

본 발명의 또 다른 실시예에 따르면, 제1 판단 시스템(101)에서의 차단 데이터베이스(104)는 제2 판단 시스템(102)에서의 유효성 판단 결과에 따라 갱신될 수 있다.

즉, 판단 시스템(100)은 상기 2. (1) 내지 (3), 및 (5)에서의 판단 결과 상기 명령어가 무효로 판단되는 경우 상기 명령어를 입력한 단말기에 대한 IP 주소 정보를 식별한다.

판단 시스템(100)은 상기 IP 주소 정보를 포함하고 소정의 기간 동안 입력되는 명령어의 제1 개수를 산출한다. 또한, 판단 시스템(100)은 상기 명령어 중에서 제2 판단 시스템(102)에 의해 무효로 판단된 명령어의 제2 개수를 산출한다. 판단 시스템(100)은 상기 제1 개수 및 상기 제2 개수를 이용하여 상기 단말기가 '비정상적으로 다수의 명령어를 악의적인 의도로 입력'하는지 여부를 가늠할 수 있다.

즉, 입력된 명령어 중 다수가 무효로 판단되는 경우, 상기 단말기의 사용자는 악의적인 의도로 명령어를 빈번하게 입력한다고 판단할 수 있다. 따라서, 이후 상기 단말기로부터 입력되는 명령어 역시 무효일 가능성이 높기 때문에, 판단 시스템(100)은 상기 단말기에 대한 IP 주소 정보를 차단 IP 주소 정보로 선정하여 차단 데이터베이스(104)에 기록하여 차단 데이터베이스(104)를 갱신함으로써, 상기 단말기로부터 입력되는 명령어는 상기 선정된 판단 방법을 이용하여 유효성 여부를 판단하지 않고 바로 무효로 결정한다.

제1 개수에 비해 제2 개수가 상대적으로 많은지 여부는 제1 개수와 제2 개수의 비율을 산출하여 소정값 이상인지 판단하는 방식 등, 상술한 바와 같은 다양한 방식이 사용될 수 있으며, 본 발명의 범위는 이러한 방식의 종류에 제한되지 않는다.

또한, 본 발명의 또 다른 실시예에 따르면, 판단 시스템(100)은 상기 제1 개수 및 상기 제2 개수를 이용하여 판단한 결과, 상기 IP 주소 정보를 차단 IP 정보로 선정할 정도는 아니지만, 이후 지속적으로 무효인 명령어를 입력할 경우 차단 IP 정보로 선정될 가능성이 높은 IP 주소 정보는 무효 의심 IP 주소 데이터베이스(도시하지 않음)에 기록하고 보다 집중적으로 관리할 수 있다. 또한, 본 발명의 또 다른 실시예에 따르면, 무효 의심 IP 주소 데이터베이스는 복수 개 존재할 수 있으며, 이에 따라 소정의 IP 주소를 차단 IP 주소로 결정하기까지 2단계 이상의 판단 과정을 수행할 수도 있다.

이와 같은 구성에 따르면, 이제까지 입력된 명령어에 대한 로그 정보만으로는 상기 명령어를 입력한 단말기의 IP 주소 정보가 차단 IP 주소 정보인지 판단하기 어려운 경우에는, 상기 IP 주소 정보를 무효 의심 IP 주소 정보로 결정하고 이후에 상기 IP 주소 정보를 포함하는 명령어를 더 관찰함으로써 상기 IP 주소 정보를 차단 IP 주소 정보로 결정할지

여부를 판단함으로써 소정의 명령어가 무효인지 여부를 더욱 정확하게 판단할 수 있게 된다.

또한, 본 발명의 또 다른 실시예에 따르면, 판단 시스템(100)의 관리자는 로그 데이터베이스(105)에 기록된 정보 등 수집된 정보에 따라 허용 데이터베이스(103) 또는 차단 데이터베이스(104)를 갱신할 수도 있다.

또한, 본 발명의 또 다른 실시예에 따르면, 판단 시스템(100)은 허용 데이터베이스(103) 또는 차단 데이터베이스(104)를 주기적으로 갱신할 수 있다. 예를 들면, 판단 시스템(100)은 소정의 기준에 따라 허용 데이터베이스(103)에 기록된 허용 키워드가 더 이상 허용 키워드로서 기능하지 못한다고 판단되는 경우 상기 허용 키워드를 삭제하여 허용 데이터베이스(103)를 갱신한다.

한편, 판단 시스템(100)은 상기와 같은 구성에 따라 무효로 판단된 명령어에 대해서도 소정의 효과는 발생하도록 할 수도 있다. 예를 들면, 상기 명령어가 검색 시스템(120)이 제공한 검색 결과 목록 중에서 검색 결과를 선택하기 위한 요청인 경우, 검색 시스템(120)은 상기 명령어가 무효인지 여부와 관계없이 상기 선택된 검색 결과와 연관된 정보를 상기 단말기로 전송할 수 있다. 다만, 상기 명령어가 상기 검색 결과와 연관하여 광고를 제공하는 광고주에게 과금하기 위한 기준, 또는 상기 검색 결과를 선택하는 사용자의 선호도를 판단하기 위한 기준 등으로도 사용되는 경우, 무효로 판단된 상기 명령어는 상기 기준으로는 사용하지 않는 것이 바람직할 것이다.

또한, 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체에 기록되는 프로그램은 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

이하에서는, 본 발명의 또 다른 실시예에 따른 명령어의 유효성을 판단하는 판단 시스템(100)에 대해 설명한다. 도 8은 판단 시스템(100, 800)의 내부 구성을 도시한 블록도이다. 판단 시스템(800)은 제1 판단 시스템(801), 제2 판단 시스템(802), 허용 데이터베이스(803)를 포함한다.

또한, 제1 판단 시스템(801)은 명령어 입력부(8011), 데이터 추출부(8012), 제1 판단부(8013), 제2 판단부(8014), 및 제3 판단부(8015)를 포함한다.

허용 데이터베이스(803)는 허용 네트워크 주소 정보 및 상기 허용 네트워크 주소와 연관된 하나 이상의 차단 키워드를 포함하며, 허용 데이터베이스(803)에 기록되는 데이터의 일례는 도 3에 도시한 바와 같다.

명령어 입력부(8011)는 사용자의 단말기(110)로부터 요청 내용을 포함하는 명령어를 입력 받고, 데이터 추출부(8012)는 상기 명령어에 포함된 상기 요청 내용 또는 IP 주소 정보를 추출한다.

제1 판단부(8013)는 허용 데이터베이스(103)를 참조하여 상기 추출된 IP 주소 정보가 허용 IP 주소 정보인지 판단한다.

제2 판단부(8014)는 판단 결과 상기 추출된 IP 주소 정보가 허용 IP 주소 정보인 경우, 허용 데이터베이스(103)를 참조하여 상기 요청 내용이 상기 허용 IP 주소 정보와 연관된 상기 하나 이상의 차단 키워드와 연관되어 있는지 판단한다.

제3 판단부(8015)는 판단 결과 상기 요청 내용이 상기 차단 키워드와 연관되어 있지 않은 경우 상기 명령어를 유효로 판단한다.

한편, 판단 결과 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있는 경우에는, 제2 판단 시스템(802)는 선정된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행한다.

선정된 판단 방법에 따라 명령어의 유효성을 판단하는 구체적인 구성은 상술한 실시예에서 설명했으므로 본 실시예에서는 그 자세한 설명은 생략한다.

도 9는 본 발명에 따른 명령어의 유효성을 판단하는 방법을 수행하는 데 채용될 수 있는 범용 컴퓨터 장치의 내부 블록도이다.

컴퓨터 장치(900)는 램(RAM: Random Access Memory)(920)과 롬(ROM: Read Only Memory)(930)을 포함하는 주기억장치와 연결되는 하나 이상의 프로세서(910)를 포함한다. 프로세서(910)는 중앙처리장치(CPU)로 불리기도 한다. 본 기술분야에서 널리 알려져 있는 바와 같이, 롬(930)은 데이터(data)와 명령(instruction)을 단방향성으로 CPU에 전송하는 역할을 하며, 램(920)은 통상적으로 데이터와 명령을 양방향성으로 전송하는 데 사용된다. 램(920) 및 롬(930)은 컴퓨터 판독 가능 매체의 어떠한 적절한 형태를 포함할 수 있다. 대용량 기억장치(Mass Storage)(940)는 양방향성으로 프로세서(910)와 연결되어 추가적인 데이터 저장 능력을 제공하며, 상기된 컴퓨터 판독 가능 기록 매체 중 어떠한 것일 수 있다. 대용량 기억장치(940)는 프로그램, 데이터 등을 저장하는데 사용되며, 통상적으로 주기억장치보다 속도가 느린 하드 디스크와 같은 보조기억장치이다. CD 롬(960)과 같은 특정 대용량 기억장치가 사용될 수도 있다. 프로세서(910)는 비디오 모니터, 트랙볼, 마우스, 키보드, 마이크로폰, 터치스크린 형 디스플레이, 카드 판독기, 자기 또는 종이 테이프 판독기, 음성 또는 필기 인식기, 조이스틱, 또는 기타 공지된 컴퓨터 입출력장치와 같은 하나 이상의 입출력 인터페이스(950)와 연결된다. 마지막으로, 프로세서(910)는 네트워크 인터페이스(970)를 통하여 유선 또는 무선 통신 네트워크에 연결될 수 있다. 이러한 네트워크 연결을 통하여 상기된 방법의 절차를 수행할 수 있다. 상기된 장치 및 도구는 컴퓨터 하드웨어 및 소프트웨어 기술 분야의 당업자에게 잘 알려져 있다.

상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있다.

지금까지 본 발명에 따른 구체적인 실시예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서는 여러 가지 변형이 가능함은 물론이다.

그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안되며, 후술하는 특허 청구의 범위뿐 아니라 이 특허 청구의 범위와 균등한 것들에 의해 정해져야 한다.

이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허 청구 범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

발명의 효과

본 발명에 따르면, 소정의 규칙에 따라 사용자로부터 입력된 명령어의 유효성을 간단하게 결정하고, 상기 규칙에 따라 상기 명령어의 유효성을 결정할 수 없는 경우에만 선정된 판단 방법에 따른 추가적인 유효성 판단을 할 수 있는 명령어의 유효성 판단 방법 및 그 시스템이 제공된다.

또한, 본 발명에 따르면, 명령어의 유효성 판단 과정을 명령어가 소정의 규칙에 부합하는지 여부를 판단하는 제1 과정과, 규칙에 부합하지 않는 명령어에 대해서는 선정된 판단 방법에 따라 그 유효성을 판단하는 제2 과정으로 이분화하여, 간단하고 빠르게 유효 여부가 판단 가능한 명령어는 제1 과정만으로 명령어의 유효성 판단 과정이 종료되도록 함으로써, 명령어의 유효성 판단을 수행하는 시스템의 부하를 감소시키고 명령어의 유효성 판단 속도를 향상시킬 수 있는 명령어의 유효성 판단 방법 및 그 시스템이 제공된다.

또한, 본 발명에 따르면, 무효로 판단되는 명령어를 상습적으로 입력하는 불량 사용자로부터 입력된 명령어가 유효로 판단되는 것을 원천적으로 차단할 수 있는 명령어의 유효성 판단 방법 및 그 시스템이 제공된다. 즉, 차단 네트워크 주소 정보 또는 차단 네트워크 그룹 정보를 이용하여 소정의 명령어를 필터링하는 방법은, 소정의 단말기를 사용하여 악의적인 의도로 명령어를 입력한 바 있는 사용자가 다른 방법을 사용하여 악의적인 의도를 은폐하여 불법적인 명령어를 다시 입력하고자 하는 경우에도 차단 네트워크 주소를 갖는(또는 차단 네트워크 그룹에 포함된 네트워크 주소를 갖는) 단말기로부터 입력된 명령어는 모두 무효로 판단함으로써 악의적인 의도로 상기 단말기로부터 입력된 명령어를 모두 무력화할 수 있다.

또한, 본 발명에 따르면, 관리자, 개발자 또는 관리자의 단말기의 네트워크 주소로부터 입력되는 명령어, 또는 관공서나 대기업의 단말기의 네트워크 주소로부터 입력되는 명령어와 같이, 신뢰할 수 있으면서 알려진 네트워크 주소 또는 네트워크 그룹으로부터 입력되는 명령어는 유효로 판단하여 추가적인 유효성 판단 과정을 생략할 수 있는 명령어의 유효성 판단 방법 및 그 시스템이 제공된다.

또한, 본 발명에 따르면, 관공서나 대기업의 단말기로부터 입력되는 명령어라고 하더라도 상기 관공서 등이 입력할 가능성이 희박한 요청 내용을 포함하는 명령어에 대해서는 유효성 판단 과정을 생략하지 않도록 하여 보다 정확하게 명령어의 유효성 여부를 판단할 수 있는 명령어의 유효성 판단 방법 및 그 시스템이 제공된다.

(57) 청구의 범위

청구항 1.

명령어의 유효성 판단 시스템에서의 명령어의 유효성 판단 방법에 있어서,
상기 유효성 판단 시스템은 허용 데이터베이스, 명령어 입력부, 데이터 추출부, 제1 판단 시스템 및 제2 판단 시스템을 포함하고,
상기 제1 판단 시스템은 제1 판단부 및 제2 판단부를 포함하고,
상기 허용 데이터베이스에 허용 네트워크 주소 정보 및 상기 허용 네트워크 주소와 연관된 하나 이상의 차단 키워드를 유지하는 단계;
상기 명령어 입력부에서 사용자의 단말기로부터 요청 내용을 포함하는 명령어를 입력 받는 단계;
상기 데이터 추출부에서 상기 명령어에 포함된 상기 요청 내용 또는 네트워크 주소 정보를 추출하는 단계;
상기 제1 판단부에서 상기 허용 데이터베이스를 참조하여 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인지 판단하는 단계;
상기 제2 판단부에서 판단 결과 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인 경우, 상기 허용 데이터베이스를 참조하여 상기 요청 내용이 상기 허용 네트워크 주소 정보와 연관된 상기 하나 이상의 차단 키워드와 연관되어 있는지 판단하는 단계; 및
상기 제2 판단 시스템에서 판단 결과 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있는 경우 선정된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 단계를 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 2.

제1항에 있어서,
상기 제1 판단 시스템은 제3 판단부를 더 포함하고,
상기 제3 판단부에서 판단 결과 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있지 않은 경우 상기 명령어를 유효로 판단하는 단계를 더 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 3.

명령어의 유효성 판단 시스템에서의 명령어의 유효성 판단 방법에 있어서,
상기 유효성 판단 시스템은 허용 데이터베이스, 명령어 입력부, 데이터 추출부, 제1 판단 시스템 및 제2 판단 시스템

을 포함하고,
 상기 제1 판단 시스템은 제1 판단부 및 제2 판단부를 포함하고,
 상기 허용 데이터베이스에 허용 네트워크 주소 정보 및 상기 허용 네트워크 주소와 연관된 하나 이상의 허용 키워드를 유지하는 단계;
 상기 명령어 입력부에서 사용자의 단말기로부터 요청 내용을 포함하는 명령어를 입력 받는 단계;
 상기 데이터 추출부에서 상기 명령어에 포함된 상기 요청 내용 또는 네트워크 주소 정보를 추출하는 단계;
 상기 제1 판단부에서 상기 허용 데이터베이스를 참조하여 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인지 판단하는 단계;
 상기 제2 판단부에서 판단 결과 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인 경우, 상기 허용 데이터베이스를 참조하여 상기 요청 내용이 상기 허용 키워드와 연관되어 있는지 판단하는 단계; 및
 상기 제2 판단 시스템에서 판단 결과 상기 추출된 요청 내용이 상기 허용 키워드와 연관되어 있지 않은 경우 선전된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 단계를 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 4.

제3항에 있어서,
 상기 제1 판단 시스템은 제3 판단부를 더 포함하고,
 상기 제3 판단부에서 판단 결과 상기 추출된 요청 내용이 상기 허용 키워드와 연관되어 있는 경우 상기 명령어를 유효로 판단하는 단계를 더 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 5.

명령어의 유효성 판단 시스템에서의 명령어의 유효성 판단 방법에 있어서,
 상기 유효성 판단 시스템은 허용 데이터베이스, 명령어 입력부, 데이터 추출부, 제1 판단 시스템 및 제2 판단 시스템을 포함하고,
 상기 허용 데이터베이스에 하나 이상의 허용 키워드를 유지하는 단계;
 상기 명령어 입력부에서 사용자의 단말기로부터 명령어를 입력 받는 단계;
 상기 데이터 추출부에서 상기 명령어에 포함된 요청 내용을 추출하는 단계;
 상기 제1 판단 시스템에서 상기 허용 데이터베이스를 참조하여 상기 추출된 요청 내용이 허용 키워드와 연관되어 있는지 여부를 판단하는 단계; 및
 상기 제2 판단 시스템에서 판단 결과 상기 추출된 요청 내용이 허용 키워드와 연관되어 있지 않은 경우 선정된 판단 방법에 따라 상기 명령어의 유효성을 판단하는 단계를 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 6.

제5항에 있어서,
 상기 제1 판단 시스템에서 상기 허용 키워드와 연관된 명령어의 기간 별 입력 횟수를 산출하는 단계; 및
 상기 제1 판단 시스템에서 상기 기간 별 입력 횟수가 소정값 미만으로 산출되는 경우 상기 허용 키워드를 상기 허용 데이터베이스에서 제거하도록 상기 허용 데이터베이스를 갱신하는 단계를 더 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 7.

명령어의 유효성 판단 시스템에서의 명령어의 유효성 판단 방법에 있어서,
 상기 유효성 판단 시스템은 허용 데이터베이스, 명령어 입력부, 데이터 추출부 및 제1 판단 시스템을 포함하고,
 상기 허용 데이터베이스에 하나 이상의 허용 네트워크 주소 정보를 포함하는 허용 데이터베이스를 유지하는 단계;
 상기 명령어 입력부에서 사용자의 단말기로부터 명령어를 입력 받는 단계;
 상기 데이터 추출부에서 상기 명령어에 포함된 네트워크 주소 정보를 추출하는 단계;
 상기 제1 판단 시스템에서 상기 허용 데이터베이스를 참조하여 상기 추출된 네트워크 주소 정보에 대응하는 허용 네트워크 주소 정보가 존재하는지 판단하는 단계; 및
 상기 제1 판단 시스템에서 상기 추출된 네트워크 주소 정보에 대응하는 허용 네트워크 주소가 존재하는 경우, 상기 명령어를 유효로 판단하는 단계를 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 8.

제7항에 있어서,
 상기 유효성 판단 시스템은 제2 판단 시스템을 더 포함하고,
 상기 허용 데이터베이스는 하나 이상의 허용 네트워크 그룹 정보를 포함하는 허용 네트워크 그룹 정보를 더 포함하고,
 상기 제1 판단 시스템에서 상기 추출된 네트워크 주소 정보를 이용하여 상기 추출된 네트워크 주소 정보가 포함되는 네트워크 그룹 정보를 식별하는 단계;
 상기 제1 판단 시스템에서 상기 허용 데이터베이스를 참조하여 상기 식별된 네트워크 그룹 정보에 대응하는 허용 네트워크 그룹 정보가 존재하는지 판단하는 단계; 및
 상기 제2 판단 시스템에서 상기 식별된 네트워크 그룹 정보에 대응하는 허용 네트워크 그룹 정보가 존재하지 않는 경

우 선정된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 단계를 더 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 9.

제7항에 있어서,
상기 유효성 판단 시스템은 차단 데이터베이스를 더 포함하고,
상기 차단 데이터베이스에 하나 이상의 차단 네트워크 주소 정보를 유지하는 단계;
명령어 입력부에서 사용자의 단말기로부터 명령어를 입력 받는 단계;
상기 데이터 추출부에서 상기 명령어에 포함된 네트워크 주소 정보를 추출하는 단계;
상기 제1 판단 시스템에서 상기 차단 데이터베이스를 참조하여 상기 추출된 네트워크 주소 정보에 대응하는 차단 네트워크 주소 정보가 존재하는지 판단하는 단계; 및
상기 제2 판단 시스템에서 상기 추출된 네트워크 주소 정보에 대응하는 차단 네트워크 주소 정보가 존재하지 않는 경우 선정된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 단계를 더 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 10.

제7항에 있어서,
상기 차단 네트워크 주소 정보는 상기 유효성 판단 시스템의 관리자 또는 개발자가 사용하는 단말기, 또는 소정의 광고주의 단말기의 네트워크 주소 정보인 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 11.

제7항에 있어서,
상기 제2 판단 시스템에서 상기 추출된 네트워크 주소 정보에 대응하는 차단 네트워크 주소 정보가 존재하지 않는 경우 소정의 기간 동안 입력되고 상기 추출된 네트워크 주소 정보를 포함하는 제1 명령어의 제1 개수를 산출하는 단계;
상기 제2 판단 시스템에서 상기 제1 명령어 중에서 상기 판단 방법에 따라 유효성을 판단한 결과 무효로 판단된 제2 명령어의 제2 개수를 산출하는 단계; 및
상기 제2 판단 시스템에서 상기 제1 개수와 상기 제2 개수의 비가 소정값을 초과하는 경우 상기 추출된 네트워크 주소 정보를 상기 차단 데이터베이스에 기록하는 단계를 더 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 12.

제7항에 있어서,
상기 제2 판단 시스템에서 상기 추출된 네트워크 주소 정보에 대응하는 차단 네트워크 주소 정보가 존재하지 않는 경우 소정의 기간 동안 입력되고 상기 추출된 네트워크 주소 정보를 포함하는 제1 명령어 중에서 상기 판단 방법에 따라 유효성을 판단한 결과 무효로 판단된 제2 명령어의 제2 개수를 산출하는 단계; 및
상기 제2 판단 시스템에서 상기 제2 개수가 소정값을 초과하는 경우 상기 추출된 네트워크 주소 정보를 상기 차단 데이터베이스에 기록하는 단계를 더 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 13.

제7항에 있어서,
상기 차단 데이터베이스는 하나 이상의 차단 네트워크 그룹 정보를 포함하는 차단 네트워크 그룹 정보를 더 포함하고,
상기 제1 판단 시스템에서 상기 추출된 네트워크 주소 정보를 이용하여 상기 추출된 네트워크 주소 정보가 포함되는 네트워크 그룹 정보를 식별하는 단계;
상기 제1 판단 시스템에서 상기 차단 데이터베이스를 참조하여 상기 식별된 네트워크 그룹 정보에 대응하는 차단 네트워크 그룹 정보가 존재하는지 판단하는 단계;
상기 제2 판단 시스템에서 상기 식별된 네트워크 그룹 정보에 대응하는 차단 네트워크 그룹 정보가 존재하지 않는 경우 선정된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 단계를 더 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 14.

명령어의 유효성 판단 시스템에서의 명령어의 유효성 판단 방법에 있어서,
상기 유효성 판단 시스템은 허용 데이터베이스, 명령어 입력부, 데이터 추출부, 제1 판단 시스템 및 제2 판단 시스템을 포함하고,
상기 허용 데이터베이스에 허용 네트워크 그룹 정보와 연관된 하나 이상의 차단 키워드를 유지하는 단계;
상기 명령어 입력부에서 사용자의 단말기로부터 요청 내용을 포함하는 명령어를 입력 받는 단계;
상기 데이터 추출부에서 상기 명령어에 포함된 상기 요청 내용 또는 네트워크 주소 정보를 추출하는 단계;
상기 제1 판단 시스템에서 상기 네트워크 주소 정보를 포함하는 네트워크 그룹 정보를 식별하는 단계;
상기 제1 판단 시스템에서 상기 허용 데이터베이스를 참조하여 상기 식별된 네트워크 그룹 정보가 허용 네트워크 그룹 정보인지 판단하는 단계;
상기 제1 판단 시스템에서 판단 결과 상기 식별된 네트워크 그룹 정보가 허용 네트워크 그룹 정보인 경우 상기 허용 데이터베이스를 참조하여 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있는지 판단하는 단계; 및
상기 제2 판단 시스템에서 판단 결과 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있는 경우 선정된 판단

방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 단계
를 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 15.

제1항, 제3항, 제5항, 제8항, 제9항, 제13항 또는 제14항 중 어느 한 항에 있어서,
상기 제2 판단 시스템은 로그 데이터베이스를 포함하고,
상기 선정된 판단 방법에 따라 상기 명령어에 대한 유효성 판단을 수행하는 상기 단계는,
상기 제2 판단 시스템에서 상기 명령어와 연관된 로그 정보를 생성하는 단계 - 상기 로그 정보는 상기 명령어에 포함
된 네트워크 주소 정보, 상기 명령어에 포함된 요청 내용, 및 상기 명령어의 입력 시점에 대한 입력 시점 정보 중 어느
하나 이상을 포함함 -;
상기 제2 판단 시스템에서 상기 로그 정보를 상기 로그 데이터베이스에 기록하는 단계;
상기 제2 판단 시스템에서 상기 로그 데이터베이스에 기록된 로그 정보 중에서, 상기 네트워크 주소 정보를 포함하는
로그 정보를 검색하는 단계;
상기 제2 판단 시스템에서 상기 검색된 로그 정보에 포함된 입력 시점 정보를 추출하는 단계; 및
상기 추출된 입력 시점 정보의 전부 또는 일부가 소정의 규칙에 따른 연관성을 갖는 경우, 상기 명령어를 무효로 판단
하는 단계
를 포함하는 것을 특징으로 하는 명령어의 유효성 판단 방법.

청구항 16.

삭제

청구항 17.

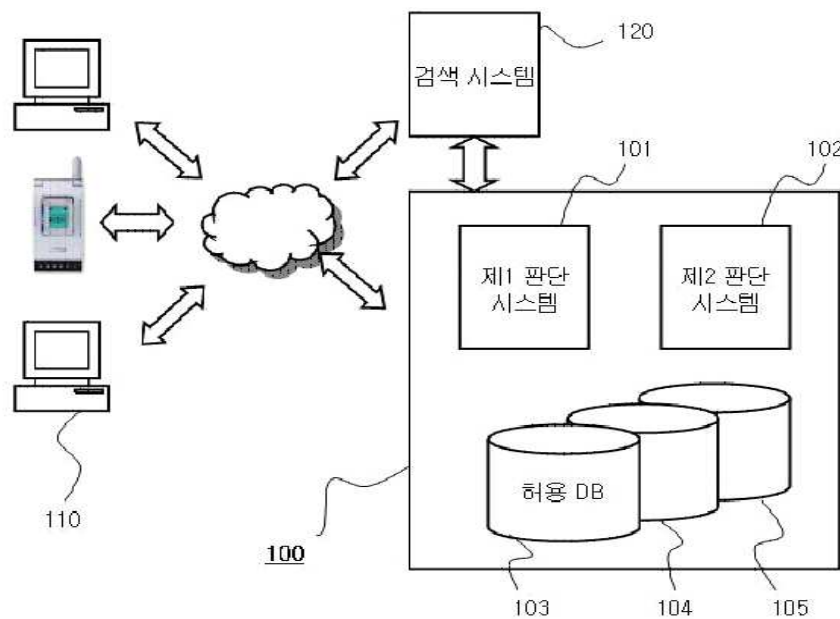
제1항 내지 제14항 중 어느 한 항의 방법을 실행시키기 위한 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

청구항 18.

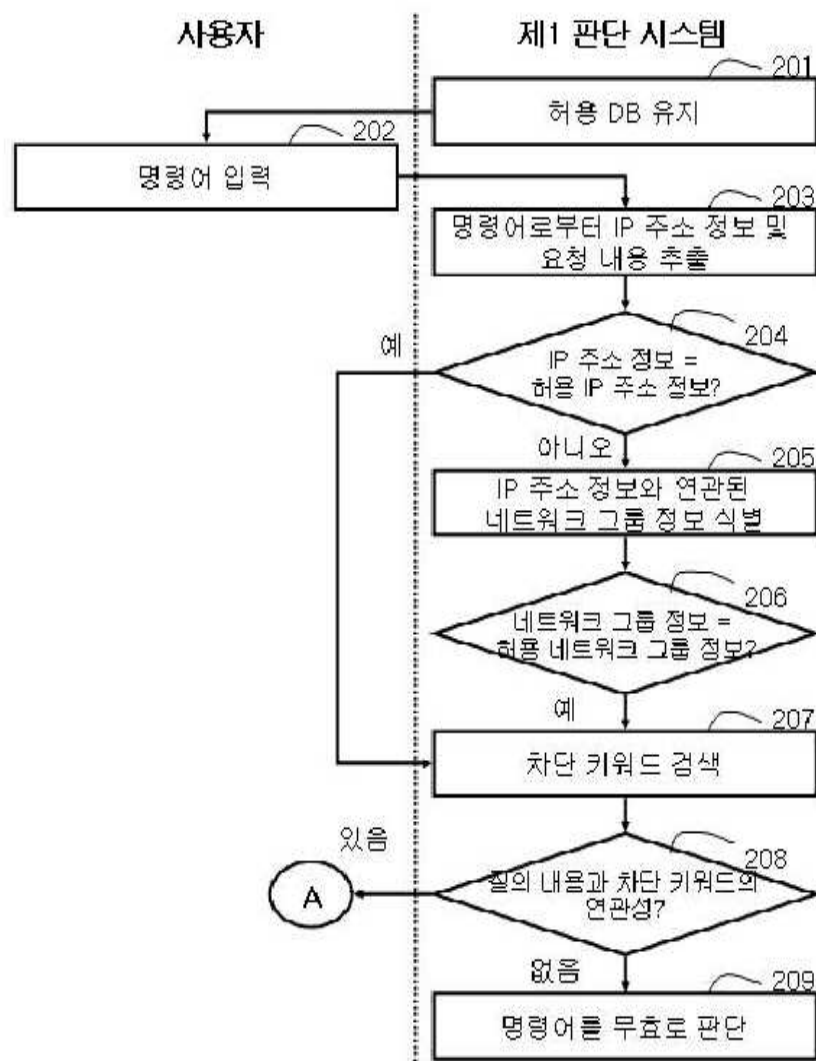
명령어의 유효성을 판단하는 판단 시스템에 있어서,
허용 네트워크 주소 정보 및 상기 허용 네트워크 주소와 연관된 하나 이상의 차단 키워드를 포함하는 허용 데이터베
이스;
사용자의 단말기로부터 요청 내용을 포함하는 명령어를 입력 받는 명령어 입력부;
상기 명령어에 포함된 상기 요청 내용 또는 네트워크 주소 정보를 데이터 추출부;
상기 허용 데이터베이스를 참조하여 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인지 판단하는 제1
판단부;
판단 결과 상기 추출된 네트워크 주소 정보가 허용 네트워크 주소 정보인 경우, 상기 허용 데이터베이스를 참조하여
상기 요청 내용이 상기 허용 네트워크 주소 정보와 연관된 상기 하나 이상의 차단 키워드와 연관되어 있는지 판단하
는 제2 판단부;
판단 결과 상기 요청 내용이 상기 차단 키워드와 연관되어 있지 않은 경우 상기 명령어를 유효로 판단하는 제3 판단
부를 포함하는 제1 판단 시스템; 및
판단 결과 상기 추출된 요청 내용이 상기 차단 키워드와 연관되어 있는 경우 선정된 판단 방법에 따라 상기 명령어에
대한 유효성 판단을 수행하는 제2 판단 시스템을 포함하는 것을 특징으로 하는 명령어의 유효성 판단 시스템.

도면

도면1



도면2



도면3

허용 IP 주소 정보 (또는 허용 네트워크 그룹 정보)	종류	차단 키워드	허용 키워드
123.123.123.123	삼성	꽃배달, ..., ...	無
254.254.254.xxx	한국특허청	無	특허, 상표, ...
...	...	...	...
...	...	...	...
...	...	...	...

도면4

401

봄봄플라워 - 전국 3시간내 **꽃배달**, ok캐쉬백포인트적립, 회원마일리지적립, 기념일관리, 디카촬영,
상품안내 꽃배달, 꽃다발, 꽃바구니, 플라워 박스, 동서양난, 경조 화환, 개업 화분,
<http://bangflower.co.kr>

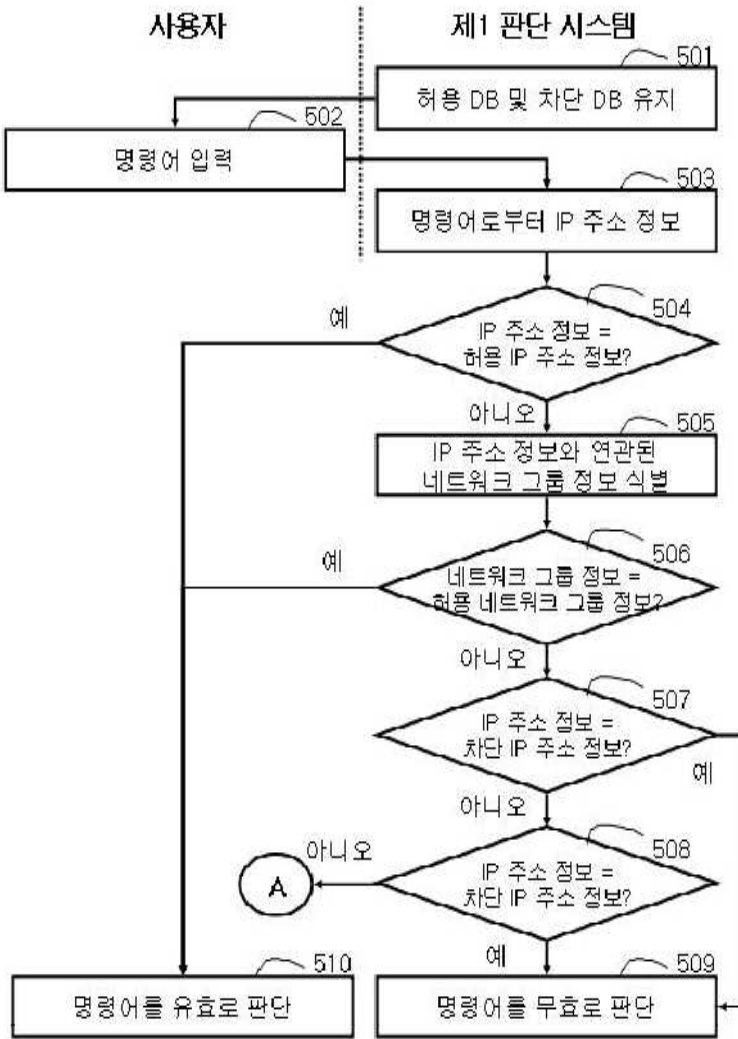
이지플라워 - 전국 2,3시간내 할인 **꽃배달**, 무료**꽃배달**이벤트, 기업회원 현금전환서비스 제공,
이벤트/경품 무료 꽃배달에 지금 도전하세요!
<http://www.easyflower.co.kr>

sk전국꽃배달 - 전국2~3시간 **꽃배달**서비스, ok캐쉬백적립, 계산서, 이벤트, 선물, 꽃집, 화원,
제품소개 여배미날, 스승의날, 카네이션바구니, 성년의날 제품
<http://www.sk-flower.com>

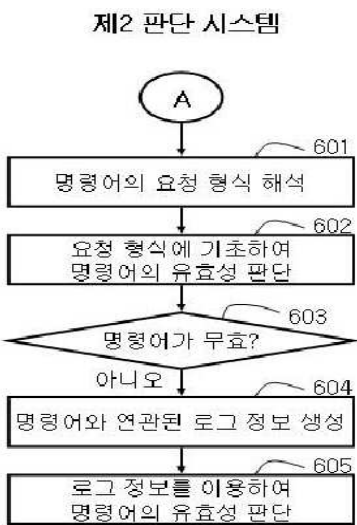
...

...

도면5



도면6



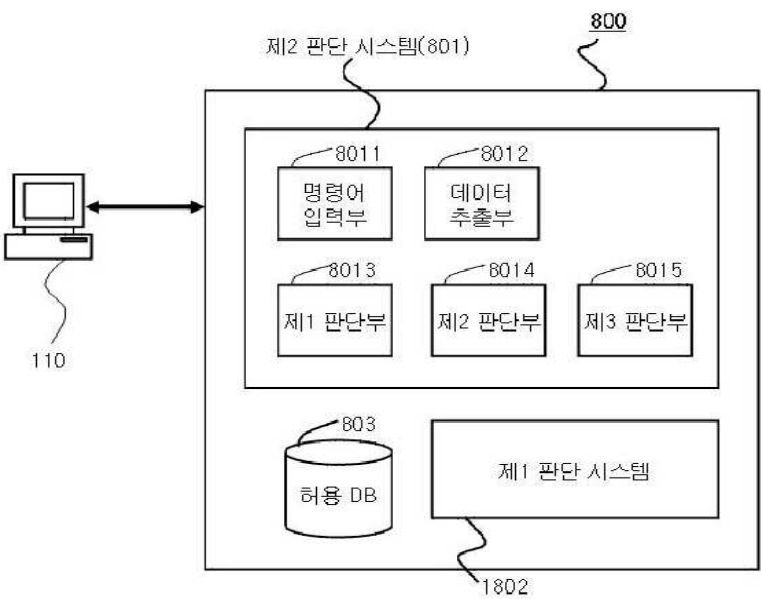
도면7

701

IP 주소 정보	입력 시점 정보	내용 정보(요청 내용 포함)	...
123.123.123.123	2004/04/16, 02:30:25	메인 페이지 접속	...
	2004/04/16, 02:31:02	검색 쿼리 입력	...
	2004/04/16, 02:31:40	검색 결과 목록 제공	...
	2004/04/16, 02:32:16	검색 결과 선택	...
	...	...	...

702

도면8



도면9

