(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년04월04일
(11) 등록번호 10-1718277
(24) 등록일자 2017년03월14일

(51) 국제특허분류(Int. Cl.)
H04L 12/66 (2006.01) *G06F 21/55* (2013.01)
G06F 21/62 (2013.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
H04L 12/66 (2013.01)
G06F 21/554 (2013.01)
(21) 출원번호 10-2015-7033810
(22) 출원일자(국제) 2013년06월28일
심사청구일자 2015년11월26일
(85) 번역문제출일자 2015년11월26일
(65) 공개번호 10-2016-0004360
(43) 공개일자 2016년01월12일
(86) 국제출원번호 PCT/US2013/048545
(87) 국제공개번호 WO 2014/209357
국제공개일자 2014년12월31일
(56) 선행기술조사문헌
US20030195859 A1*
US20060059564 A1*
US20090150991 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인텔 코포레이션
미합중국 캘리포니아 95054 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
네이쉬투트 알렉스
이스라엘 갠 야브네 80700 하다간 10/3
벤-샬롬 오메르
이스라엘 리숀 레-티젼 75503 버렌스타인 스트리트 55
리 홍
미국 캘리포니아주 95762 엘도라도 힐스 킹키드 코트 245
(74) 대리인
제일특허법인

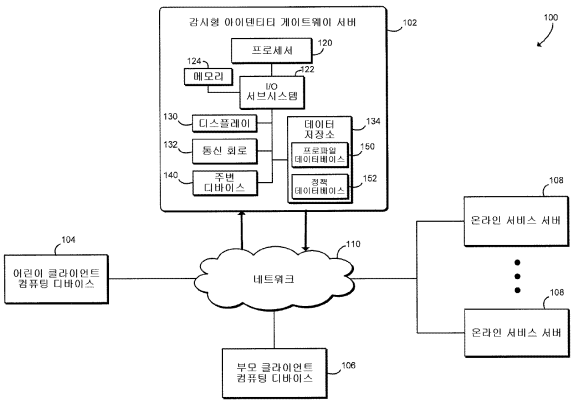
전체 청구항 수 : 총 25 항 심사관 : 김대성

(54) 발명의 명칭 **감시형 온라인 아이덴티티**

(57) 요 약

온라인 아이덴티티의 감시를 가능하게 하는 기법은 "어린이" 클라이언트 컴퓨터 디바이스의 사용자에 의해 온라인 서비스에 대한 액세스를 가능하게 하고 모니터링하는 게이트웨이 서버를 포함한다. 게이트웨이 서버는 클라이언트 컴퓨팅 디바이스로부터 온라인 서비스에 대한 액세스를 위한 요청을 수신하고, 온라인 서비스에 대한 액세스 정보를 검색하고, 액세스 정보를 사용하여 클라이언트 컴퓨팅 디바이스를 위한 온라인 서비스에 대한 액세스를 가능하게 한다. 액세스 정보는 사용자로부터 기밀로 유지된다. 게이트웨이 서버는 또한 정책 데이터베이스의 정책 규칙 세트에 기초하여 클라이언트 컴퓨팅 디바이스와 온라인 서비스 사이의 활동을 제어하는 활동 모니터 모듈을 포함할 수 있다. 게이트웨이 서버는 리뷰 및/또는 승인을 위해 그러한 활동에 관한 통지를 "부모" 클라이언트 컴퓨팅 디바이스에 송신할 수 있고, 이는 정책 데이터베이스를 업데이트하는데 또한 사용될 수 있다.

대 표 도



(52) CPC특허분류
G06F 21/629 (2013.01)
H04L 63/0823 (2013.01)
H04L 63/102 (2013.01)
H04L 63/105 (2013.01)
G06F 2221/2137 (2013.01)
G06F 2221/2149 (2013.01)

명 세 서

청구범위

청구항 1

온라인 아이덴티티(online identity)의 감시(supervision)를 가능하게 하는 게이트웨이 서버로서,

클라이언트 컴퓨팅 디바이스의 사용자의 온라인 서비스에 대한 액세스 정보를 저장하는 프로파일 데이터베이스(profile database) - 상기 액세스 정보는 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스 가능하지 않음 - 와,

상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이에서 허가된 활동을 정의하는 정책 규칙 세트를 저장하는 정책 데이터베이스(policy database)와,

(i) 상기 클라이언트 컴퓨팅 디바이스로부터 수신된 새로운 온라인 서비스를 등록하라는 요청에 응답하여 상기 새로운 온라인 서비스에 액세스하는 새로운 액세스 정보를 생성 - 상기 새로운 액세스 정보는 상기 게이트웨이 서버에 의해 무작위로(randomly) 생성되는 패스워드를 포함함 - 하고, (ii) 상기 클라이언트 컴퓨팅 디바이스로부터 상기 새로운 온라인 서비스에 대한 액세스를 위한 요청을 수신하고, (iii) 상기 요청에 응답하여, 상기 프로파일 데이터베이스로부터 상기 새로운 온라인 서비스에 대한 상기 새로운 액세스 정보를 검색(retrieve)하고, (iv) 상기 새로운 액세스 정보를 사용하여 상기 클라이언트 컴퓨팅 디바이스를 위한 상기 새로운 온라인 서비스에 대한 액세스를 가능하게 하는, 아이덴티티 관리자 모듈(identity manager module)과,

상기 정책 규칙 세트에 기초하여 상기 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하는 활동 모니터 모듈(activity monitor module)

을 구현하는 하드웨어 프로세서를 포함하는

게이트웨이 서버.

청구항 2

제 1 항에 있어서,

상기 새로운 온라인 서비스에 대한 액세스를 가능하게 하는 것은, 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 액세스 정보를 사용하여 상기 새로운 온라인 서비스에 로깅하면서 상기 클라이언트 컴퓨팅 디바이스로부터 상기 새로운 액세스 정보를 비밀로 유지하는 것을 포함하는

게이트웨이 서버.

청구항 3

제 1 항에 있어서,

상기 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하는 것은, 상기 정책 데이터베이스의 액세스 제어 정책에 따라 상기 클라이언트 컴퓨팅 디바이스에 의한 상기 새로운 온라인 서비스에 대한 액세스를 제어하는 것을 포함하는

게이트웨이 서버.

청구항 4

제 1 항에 있어서,

상기 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하는 것은, 경고 이벤트

(alert event)의 발생을 위해 상기 활동을 모니터링하는 것 및 상기 경고 이벤트의 발생에 응답하여 경고를 생성하는 것을 포함하는

게이트웨이 서버.

청구항 5

제 4 항에 있어서,

상기 경고 이벤트는, (ⅰ) 상기 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티 프로파일 정보에 대한 상기 새로운 온라인 서비스에 의한 요청, (ii) 구매 거래의 개시, 또는 (iii) 콘텐츠 정책에 기초하여 수락가능하지 않은 것으로 식별된 상기 새로운 온라인 서비스에 의한 콘텐츠 전달(delivery) 중 적어도 하나를 포함하는

게이트웨이 서버.

청구항 6

제 4 항에 있어서,

상기 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하는 것은,

상기 경고 이벤트를 차단(block)하는 것과,

다른 클라이언트 컴퓨팅 디바이스의 사용자에게 상기 경고 이벤트의 발생을 알리는 통지(notification)를 상기 다른 클라이언트 컴퓨팅 디바이스로 송신하는 것을 더 포함하는

게이트웨이 서버.

청구항 7

제 6 항에 있어서,

상기 활동 모니터 모듈은, 또한,

상기 통지의 송신에 응답하여 상기 다른 클라이언트 컴퓨팅 디바이스로부터 상기 경고 이벤트에 대한 허가(authorization)를 수신하고,

상기 허가의 수신에 응답하여 상기 경고 이벤트가 발생하도록 허용하는

게이트웨이 서버.

청구항 8

제 1 항에 있어서,

상기 아이덴티티 관리자 모듈은, 또한,

상기 새로운 액세스 정보가 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스 가능하지 않도록 상기 프로파일 데이터베이스 내에 상기 새로운 액세스 정보를 저장하고,

상기 새로운 액세스 정보를 사용하여 상기 클라이언트 컴퓨팅 디바이스의 사용자를 상기 새로운 온라인 서비스에 등록하는

게이트웨이 서버.

청구항 9

제 1 항에 있어서,

상기 아이덴티티 관리자 모듈은, 또한,

다른 클라이언트 컴퓨팅 디바이스로부터 관리 액세스 요청(management access request)을 수신하고,

상기 다른 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티를 검증(verify)하고,

상기 다른 클라이언트 컴퓨팅 디바이스로부터 수신된 데이터에 기초하여 상기 정책 데이터베이스 내에 저장된 정책 규칙 세트를 업데이트하는

게이트웨이 서버.

청구항 10

복수의 인스트럭션이 저장된 하나 이상의 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 복수의 인스트럭션은, 실행에 응답하여 게이트웨이 서버로 하여금,

클라이언트 컴퓨팅 디바이스로부터 수신된 새로운 온라인 서비스를 등록하라는 요청에 응답하여 상기 새로운 온라인 서비스에 액세스하는 새로운 액세스 정보를 생성하게 하고 - 상기 새로운 액세스 정보는 상기 게이트웨이 서버에 의해 무작위로 생성되는 패스워드를 포함함 - ,

클라이언트 컴퓨팅 디바이스로부터 상기 새로운 온라인 서비스에 대한 액세스를 위한 요청을 수신하게 하고,

상기 요청에 응답하여, 상기 게이트웨이 서버의 프로파일 데이터베이스로부터 상기 새로운 온라인 서비스에 대한 상기 새로운 액세스 정보를 검색하게 하고,

상기 새로운 액세스 정보를 사용하여 클라이언트 컴퓨팅 디바이스의 사용자를 위한 상기 새로운 온라인 서비스에 대한 액세스를 가능하게 하고 - 상기 새로운 액세스 정보는 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스 가능하지 않음 - ,

상기 게이트웨이 서버의 정책 데이터베이스 내에 저장된 정책 규칙 세트에 기초하여 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하게 하는

컴퓨터 판독가능 저장 매체.

청구항 11

제 10 항에 있어서,

상기 새로운 온라인 서비스에 대한 액세스를 가능하게 하는 것은, 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 액세스 정보를 사용하여 상기 새로운 온라인 서비스에 로깅하면서 상기 클라이언트 컴퓨팅 디바이스로부터 상기 새로운 액세스 정보를 비밀로 유지하는 것을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 12

제 10 항에 있어서,

상기 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하는 것은, 상기 게이트웨이 서버의 액세스 제어 정책에 따라 상기 클라이언트 컴퓨팅 디바이스에 의한 상기 새로운 온라인 서비스에 대한 액세스를 제어하는 것을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 13

제 10 항에 있어서,

상기 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하는 것은, 경고 이벤트의 발생을 위해 상기 활동을 모니터링하는 것 및 상기 경고 이벤트의 발생에 응답하여 경고를 생성하는 것을 포함하는

컴퓨터 판독가능 저장 매체.

청구항 14

제 13 항에 있어서,

상기 경고 이벤트는, (ⅰ) 상기 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티 프로파일 정보에 대한 상기 새로운 온라인 서비스에 의한 요청, (ⅱ) 구매 거래의 개시, 또는 (ⅲ) 콘텐츠 정책에 기초하여 수락가능하지 않은 것으로 식별된 상기 새로운 온라인 서비스에 의한 콘텐츠 전달 중 적어도 하나를 포함하는

컴퓨터 판독가능 저장 매체.

청구항 15

제 13 항에 있어서,

상기 복수의 인스트럭션은, 또한, 상기 게이트웨이 서버로 하여금,

상기 경고 이벤트를 차단하게 하고,

다른 클라이언트 컴퓨팅 디바이스의 사용자에게 상기 경고 이벤트의 발생을 알리는 통지를 상기 다른 클라이언트 컴퓨팅 디바이스로 송신하게 하는

컴퓨터 판독가능 저장 매체.

청구항 16

제 15 항에 있어서,

상기 복수의 인스트럭션은, 또한, 상기 게이트웨이 서버로 하여금,

상기 통지의 송신에 응답하여 상기 다른 클라이언트 컴퓨팅 디바이스로부터 상기 경고 이벤트에 대한 허가를 수신하게 하고,

상기 허가의 수신에 응답하여 상기 경고 이벤트가 발생하도록 허용하게 하는

컴퓨터 판독가능 저장 매체.

청구항 17

제 10 항에 있어서,

상기 복수의 인스트럭션은, 또한, 상기 게이트웨이 서버로 하여금,

상기 새로운 액세스 정보가 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스 가능하지 않도록 상기 게이트웨이 서버 상에 상기 새로운 액세스 정보를 저장하게 하고,

상기 새로운 액세스 정보를 사용하여 상기 클라이언트 컴퓨팅 디바이스의 사용자를 상기 새로운 온라인 서비스에 등록하게 하는

컴퓨터 판독가능 저장 매체.

청구항 18

제 10 항에 있어서,

상기 복수의 인스트럭션은, 또한, 상기 게이트웨이 서버로 하여금,

다른 클라이언트 컴퓨팅 디바이스로부터 관리 액세스 요청을 수신하게 하고,

상기 다른 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티를 검증하게 하고,

상기 다른 클라이언트 컴퓨팅 디바이스로부터 수신된 데이터에 기초하여 상기 정책 데이터베이스 내에 저장된 정책 규칙 세트를 업데이트하게 하는

컴퓨터 판독가능 저장 매체.

청구항 19

온라인 아이덴티티를 감시하기 위한 방법으로서,

게이트웨이 서버에 의해, 클라이언트 컴퓨팅 디바이스로부터 수신된 새로운 온라인 서비스를 등록하라는 요청에 응답하여 상기 새로운 온라인 서비스에 액세스하는 새로운 액세스 정보를 생성하는 단계 - 상기 새로운 액세스 정보는 상기 게이트웨이 서버에 의해 무작위로 생성되는 패스워드를 포함함 - 와,

상기 게이트웨이 서버 상에서, 클라이언트 컴퓨팅 디바이스로부터 새로운 온라인 서비스에 대한 액세스를 위한 요청을 수신하는 단계와,

상기 요청에 응답하여, 상기 게이트웨이 서버의 프로파일 데이터베이스로부터 상기 새로운 온라인 서비스에 대한 상기 새로운 액세스 정보를 검색하는 단계와,

상기 게이트웨이 서버를 사용하여, 상기 새로운 액세스 정보를 사용하여 상기 클라이언트 컴퓨팅 디바이스의 사용자를 위한 상기 새로운 온라인 서비스에 대한 액세스를 가능하게 하는 단계 - 상기 새로운 액세스 정보는 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스 가능하지 않음 - 와,

상기 게이트웨이 서버를 사용하여, 상기 게이트웨이 서버의 정책 데이터베이스에 저장된 정책 규칙 세트에 기초하여 상기 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하는 단계를 포함하는

온라인 아이덴티티 감시 방법.

청구항 20

제 19 항에 있어서,

상기 새로운 온라인 서비스에 대한 액세스를 가능하게 하는 단계는, 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 액세스 정보를 사용하여 상기 새로운 온라인 서비스에 로깅하면서 상기 클라이언트 컴퓨팅 디바이스로부터 상기 새로운 액세스 정보를 비밀로 유지하는 단계를 포함하는

온라인 아이덴티티 감시 방법.

청구항 21

제 19 항에 있어서,

상기 클라이언트 컴퓨팅 디바이스와 상기 새로운 온라인 서비스 사이의 활동을 제어하는 단계는, 경고 이벤트의 발생을 위해 상기 활동을 모니터링하는 단계 및 상기 경고 이벤트의 발생에 응답하여 경고를 생성하는 단계를

포함하는

온라인 아이덴티티 감시 방법.

청구항 22

제 21 항에 있어서,

상기 경고 이벤트는, (ⅰ) 상기 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티 프로파일 정보에 대한 상기 새로운 온라인 서비스에 의한 요청, (ii) 구매 거래의 개시, 또는 (iii) 콘텐츠 정책에 기초하여 수락가능하지 않는 것으로 식별된 상기 새로운 온라인 서비스에 의한 콘텐츠의 전달 중 적어도 하나를 포함하는

온라인 아이덴티티 감시 방법.

청구항 23

제 21 항에 있어서,

상기 경고 이벤트를 차단하는 단계와,

상기 경고 이벤트의 발생을 다른 클라이언트 컴퓨팅 디바이스의 사용자에게 알리는 통지를 상기 다른 클라이언트 컴퓨팅 디바이스에 송신하는 단계를 더 포함하는

온라인 아이덴티티 감시 방법.

청구항 24

제 23 항에 있어서,

상기 통지를 송신하는 것에 응답하여 상기 다른 클라이언트 컴퓨팅 디바이스로부터 상기 경고 이벤트에 대한 허가를 수신하는 단계와,

상기 허가의 수신에 응답하여 상기 경고 이벤트가 발생하도록 허용하는 단계를 더 포함하는

온라인 아이덴티티 감시 방법.

청구항 25

제 19 항에 있어서,

상기 새로운 액세스 정보가 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스가능하지 않도록 상기 게이트웨이 서버 상에 상기 새로운 액세스 정보를 저장하는 단계와,

상기 새로운 액세스 정보를 사용하여 상기 새로운 온라인 서비스에 상기 클라이언트 컴퓨팅 디바이스의 사용자를 등록하는 단계를 더 포함하는

온라인 아이덴티티 감시 방법.

발명의 설명

배 경 기 술

[0001] 온라인 서비스의 액세스 및 인기가 증가함에 따라, 사용자, 특히 미성년자에게 제기되는 온라인 서비스와 같은 위험은 계속 증가하는 문제이다. 예를 들어, 많은 부모들은 소셜 네트워킹, 웹 서핑, 및 게임 서비스와 같은 온라인 서비스에 대한 액세스를 자신의 아이들에게 허용하지만, 부모들은 아이들에 의한 온라인 서비스의 잠재적 오용(misuse) 및/또는 온라인 서비스 및/또는 알려지지 않는 제 3 자에 의한 온라인 남용(abuse)(예를 들어, 신용 사기(scamming), 부적절한 콘텐츠 등)에 아이들이 노출되는 것을 걱정한다. 온라인 서비스에 대한 액세스를

제어하는 것은 어린이가 집 컴퓨터, 스마트폰, 태블릿 컴퓨터 등과 같은 다양한 다른 디바이스들을 통해 온라인 서비스에 액세스하는 상황들에서 복잡하다. 추가적으로, 일부 환경에서, 부모들은 온라인 서비스의 액세스에 관한 제어 시에(예를 들어, 어린이가 그러한 서비스에 액세스할 수 있는 시간, 또는 기간을 제어하는 것) 더 많은 단위를 원할 수 있고/있거나 어린이의 온라인 경험의 다른 측면들을 제어하는 것을 원할 수 있다.

[0002] 전형적인 부모 제어 기법은 상이한 컴퓨팅 디바이스들 및 위치들에 걸쳐 액세스를 제어하는 기능으로 종종 제한된다. 예를 들어, 일부 부모 제어 메커니즘은 디바이스 기반으로 구현되며, 이는 부모 제어 소프트웨어를 사용하여 업데이트되는 각각의 보호형 컴퓨팅 디바이스를 요구한다. 다른 부모 제어 메커니즘은 홈 기반 또는 클라우드 기반일 수 있다. 그러나, 다시 한 번, 그러한 메커니즘은 어린이가 집 또는 클라우드 제어 외부에서 원격의 컴퓨팅 디바이스를 사용하고 있는 상황에서 어린이의 온라인 행동 및/또는 경험을 제어하는 것으로 제한된다.

본 발명에 대한 종래 기술의 예로는 미국 특허출원공개공보 제 2009/0177514 호가 있다.

도면의 간단한 설명

[0003] 본원에서 설명되는 개념들은 예시의 방법으로 설명되며 첨부된 도면으로 제한되지 않는다. 설명의 명료성 및 단순성을 위해, 도면들에 도시된 구성요소들은 반드시 축적에 따라 도시되는 것은 아니다. 적절한 것으로 고려되는 경우, 대응하거나 유사한 구성요소들을 나타내기 위해 도면들 중에서 참조 부호가 반복될 수 있다.

도 1은 온라인 아이덴티티를 감시하기 위한 시스템에 관한 적어도 하나의 실시예의 간략화된 블록도이다.

도 2는 온라인 아이덴티티를 감시하기 위한 시스템에 관한 적어도 하나의 추가 실시예의 간략화된 블록도이다.

도 3은 도 1 또는 도 2의 시스템의 감시형 아이덴티티 게이트웨이 서버의 환경에 관한 적어도 하나의 실시예의 간략화된 블록도이다.

도 4 내지 도 6은 도 1 내지 도 3의 감시형 아이덴티티 게이트웨이 서버에 의해 실행될 수 있는 온라인 아이덴티티를 감시하기 위한 방법에 관한 적어도 하나의 실시예의 간략화된 흐름도이다.

도 7은 감시형 아이덴티티 게이트웨이 서버에 의해 수행되는 온라인 아이덴티티의 감시를 관리하기 위한 방법의 적어도 하나의 실시예의 간략화된 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0004] 본 개시물의 개념들은 다양한 수정 및 대안적인 형태를 허용할 수 있고, 이들의 특정 실시예들은 도면에서 예시에 의해 도시되며 본원에 상세히 설명될 것이다. 그러나, 본 개시물의 개념을 개시된 특정 형태로 제한하고자 하는 것이 아니며, 그와 대조적으로 본 개시물 및 첨부된 특허청구항과 일치하는 모든 수정, 균등물, 및 대안을 포함하고자 한다는 것이 이해되어야 한다.

[0005] "하나의 실시예", "일 실시예", "예시적인 실시예" 등에 대한 본 명세서에서의 참조는 개시된 실시예가 특정한 특징, 구조, 또는 특성을 포함할 수 있다는 것을 나타내지만, 모든 실시예들이 그러한 특정한 특징, 구조, 또는 특성을 포함할 수 있거나 반드시 포함하지 않을 수 있다. 더욱이, 그러한 문구는 일부 실시예들을 반드시 지칭하는 것은 아니다. 또한, 특정한 특징, 구조, 또는 특성이 일 실시예와 관련되어 도시될 때, 이는 명시적으로 설명되든지 안 되든지 다른 실시예들과 관련하여 그러한 특징, 구조, 또는 특성을 가져오는 것은 본 기술분야의 당업자의 지식 내에 존재한다는 것이 제안된다.

[0006] 개시된 실시예들은 일부 경우들에서, 하드웨어, 펌웨어, 소프트웨어, 또는 이들의 임의의 조합으로 구현될 수 있다. 개시된 실시예들은 또한 하나 이상의 프로세서에 의해 판독되고 실행될 수 있는 일시적 또는 비일시적 머신 판독가능(예를 들어, 컴퓨터 판독가능) 저장 매체에 의해 실행되거나 저장되는 인스트럭션으로서 구현될 수 있다. 머신 판독가능 저장 매체는 임의의 저장 디바이스, 메커니즘, 또는 머신에 의해 판독가능한 형태(예를 들어, 휘발성 또는 비휘발성 메모리, 매체 디스크, 또는 다른 매체 디바이스)로 정보를 저장 또는 송신하기 위한 다른 물리적 구조로 구현될 수 있다.

[0007] 도면에서, 일부 구조적 또는 방법 특징들은 특정 배치 및/또는 순서로 도시될 수 있다. 하지만, 그러한 특정 배치 및/또는 순서가 필수적인 것은 아니라는 것이 이해되어야 한다. 오히려, 일부 실시예들에서, 그러한 특징들은 예시적인 도면에 도시된 것과 상이한 방식 및/또는 순서로 배치될 수 있다. 따라서, 특정 도면 내의 구조적 또는 방법 특징의 포함은 그러한 특징이 모든 실시예들에 요구되는 것을 내포하는 것을 의미하지 않으며, 일부

실시예들에서는, 포함되지 않을 수 있거나 다른 특징들과 조합될 수 있다.

[0008] 이제 도 1을 참조하면, 예시적인 실시예에서, 온라인 아이덴티티를 감시하기 위한 시스템(100)은 감시형 아이덴티티 게이트웨이 서버(102), "어린이(child)" 클라이언트 컴퓨팅 디바이스(104), "부모(parental)" 클라이언트 컴퓨팅 디바이스(106), 및 하나 이상의 온라인 서비스 서버(108)를 포함한다. 사용 시, 아래에서 더 상세히 설명되는 바와 같이, 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 온라인 아이덴티티를 관리하고, 네트워크(110)를 통해 사용자를 위한 온라인 서비스 서버들(108) 중 하나 이상에 대한 액세스를 가능하게 한다. 그렇게 하기 위해, 게이트웨이 서버(102)는 등록된 온라인 서비스 서버들(108)의 각각에 대한 액세스 정보를 유지한다. 액세스 정보는 온라인 서비스 서버들(108) 중 하나 이상에 의해 호스팅되는 특정 온라인 서비스에 클라이언트 컴퓨팅 디바이스(104)의 사용자를 로그인시키는 게이트웨이 서버(102)에 의해 사용 가능하다. 예를 들어, 액세스 정보는 클라이언트 컴퓨팅 디바이스(104)의 사용자에 의해 액세스 가능하지 않고 기밀로 유지되는, 특정 온라인 서비스에 대한 사용자 패스워드를 포함할 수 있다. 이러한 방법에서, 게이트웨이 서버(102)는, 게이트웨이 서버(102)가 민감한 정보(예를 들어, 사용자의 아이덴티티 정보)에 대한 제어 양을 유지하도록 허용하는, 클라이언트 컴퓨팅 디바이스(104)의 사용자에 의해 소비되는 특정 온라인 서비스에 대한 브로커(broker)로서 역할을 한다.

[0009] 추가적으로, 게이트웨이 서버(102)는 클라이언트 컴퓨팅 디바이스(104)와 온라인 서비스 서버(108) 사이의 온라인 활동(activity)을 모니터링 및 제어한다. 예를 들어, 아래에서 더 상세히 설명되는 바와 같이, 게이트웨이 서버(102)는 액세스 제어 정책(예를 들어, 날짜, 기간, 화이트/블랙 리스트, 구매 양, 콘텐츠 타입 등)에 기초하여 어떤 온라인 서비스, 콘텐츠, 및/또는 활동이 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에게 액세스 가능한지를 제어할 수 있다. 일부 실시예들에서, 게이트웨이 서버(102)는 경고 이벤트(예를 들어, 클라이언트 컴퓨팅 디바이스(104)의 사용자로부터 기밀 정보를 요청하는 서비스, 제한 콘텐츠에 관한 액세스 등)에 대하여 모니터링할 수 있고 그러한 경고 이벤트의 검출에 응답하여 "부모" 클라이언트 컴퓨팅 디바이스(106)로 통지할 수 있다.

[0010] 감시형 아이덴티티 게이트웨이 서버(102)는 본원에서 설명되는 기능을 수행할 수 있는 임의의 타입의 서버 컴퓨팅 디바이스, 또는 디바이스들의 집합으로 포함될 수 있다. 예를 들어, 게이트웨이 서버(102)는 단일 서버 컴퓨터 또는 복수의 서버 컴퓨터로 포함될 수 있다. 추가적으로, 일부 실시예들에서, 게이트웨이 서버(102)는 네트워크(110)에 걸쳐 분산된 복수의 컴퓨팅 디바이스로부터 형성된 "가상 서버"로서 포함될 수도 있다. 예를 들어, 게이트웨이 서버(102)에 의해 제공되는 기능은 일부 실시예들에서 클라우드 기반 서비스의 일부로서 제공될 수 있다. 따라서, 게이트웨이 서버(102)가 도 1에 도시되고 단일 서버 컴퓨팅 디바이스로서 포함되는 것으로 후술되지만, 게이트웨이 서버(102)는 후술되는 기능을 가능하게 하도록 함께 협력하는 복수의 디바이스로서 포함될 수 있다. 추가적으로, 일부 실시예들에서, 감시형 아이덴티티 게이트웨이 서버(102), 또는 이들의 기능의 부분들은 집 또는 사업체 내에 위치될 수 있다.

[0011] 도 1에 도시된 바와 같이, 감시형 아이덴티티 게이트웨이 서버(102)는 프로세서(120), 입력/출력 서브시스템(122), 메모리(124), 디스플레이(130), 통신 회로(132), 데이터 저장 디바이스(134), 및 하나 이상의 주변 디바이스(140)를 포함한다. 물론, 다른 실시예들에서, 게이트웨이 서버(102)는 서버 또는 다른 컴퓨터에서 흔히 발견되는 것(예를 들어, 다양한 입력/출력 디바이스)과 같은 다른 또는 추가적인 컴포넌트를 포함할 수 있다. 추가적으로, 일부 실시예들에서, 예시적인 컴포넌트들 중 하나 이상은 다른 컴포넌트 내에 통합될 수 있고, 아니면 다른 컴포넌트의 일 부분을 형성할 수도 있다. 예를 들어, 메모리(124), 또는 이들의 일부분은 일부 실시예들에서 프로세서(120) 내에 통합될 수 있다.

[0012] 프로세서(120)는 본원에서 설명되는 기능들을 수행할 수 있는 임의의 타입의 프로세서로서 포함될 수 있다. 예를 들어, 프로세서(120)는 싱글 또는 멀티 코어 프로세서(들), 디지털 신호 프로세서, 마이크로컨트롤러, 또는 다른 프로세서 또는 처리/제어 회로로서 포함될 수 있다. 이와 마찬가지로, 메모리(124)는 본원에서 설명되는 기능들을 수행할 수 있는 임의의 타입의 휘발성 또는 비휘발성 메모리 또는 데이터 저장소로서 포함될 수 있다. 동작 시, 메모리(124)는 운영 체제, 애플리케이션, 프로그램, 라이브러리, 및 드라이버와 같이, 게이트웨이 서버(102)의 동작 동안 사용되는 다양한 데이터 및 소프트웨어를 저장할 수 있다. 메모리(124)는 프로세서(120), 메모리(124), 및 게이트웨이 서버(102)의 다른 컴포넌트로서 포함될 수 있는, I/O 서브시스템(122)을 통해 프로세서(120)에 통신가능하게 연결된다. 예를 들어, I/O 서브시스템(122)은 메모리 제어기 허브, 입력/출력 제어 허브, 펌웨어 디바이스, 통신 링크(즉, 포인트 투 포인트 링크, 버스 링크, 와이어, 케이블, 광 가이드, 인쇄 회로 기판 트레이스 등) 및/또는 다른 컴포넌트 및 입력/출력 동작을 가능하게 하는 서브시스템으로 구현되거나 아니면 이들을 포함할 수 있다. 일부 실시예들에서, I/O 서브시스템(122)은 시스템 온 칩(SoC)의 일 부분을 형

성할 수 있고, 프로세서(120), 메모리(124), 및 게이트웨이 서버(102)의 다른 컴포넌트들과 함께 단일 집적 회로 칩 상에 통합될 수 있다.

[0013] 게이트웨이 서버(102)의 디스플레이(130)는, 액정 디스플레이(LCD), 발광 디스플레이(LED), 플라즈마 디스플레이, 음극선관(CRT), 또는 다른 타입의 디스플레이 디바이스와 같이, 디지털 정보를 디스플레이할 수 있는 임의의 타입의 디스플레이로서 포함될 수 있다. 일부 실시예들에서, 디스플레이(130)는 사용자 인터랙션을 가능하게 하는 터치 스크린과 연결될 수 있다.

[0014] 게이트웨이 서버(102)의 통신 회로(132)는, 네트워크(110)를 통해 게이트웨이 서버(102)와, "어린이" 클라이언트 컴퓨팅 디바이스(104), "부모" 클라이언트 컴퓨팅 디바이스(106), 및/또는 하나 이상의 온라인 서비스 서버(108) 사이의 통신을 인에이블할 수 있는, 임의의 통신 회로, 디바이스, 또는 이들의 집합으로 포함될 수 있다. 통신 회로(132)는 임의의 하나 이상의 통신 기법(예를 들어, 무선 또는 유선 통신) 및 연관 프로토콜(예를 들어, 이더넷, 블루투스®, Wi-Fi®, WiMAX 등)을 사용하도록 구성되어 그러한 통신을 달성할 수 있다.

[0015] 데이터 저장 디바이스(134)는, 예를 들어, 메모리 디바이스 및 회로, 메모리 카드, 하드 디스크 드라이브, 고체 상태 드라이브, 또는 다른 데이터 저장 디바이스와 같이, 데이터를 단기 또는 장기 저장하도록 구성된 임의의 타입의 디바이스 또는 디바이스들로 포함될 수 있다. 도 1의 예시적인 실시예에서, 데이터 저장소(134)는 감시형 아이덴티티 게이트웨이 서버(102)와 통합된 것으로 도시되지만, 다른 실시예들에서, 데이터 저장소(134)는 게이트웨이 서버(102)로부터 따로 떨어져 있지만 게이트웨이 서버와 통신할 수 있다. 예를 들어, 데이터 저장소(134)는 개별 데이터 서버 등에 의해 유지될 수 있다.

[0016] 데이터 저장소(134)는 프로파일 데이터베이스(150) 및 정책 데이터베이스(152)를 저장한다. 아래에서 더 상세히 설명되는 바와 같이, 프로파일 데이터베이스(150)는, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자가 대응 온라인 서비스에 로그인하도록 게이트웨이 서버(102)에 의해 사용가능한, 다양한 온라인 서비스 서버(108)에 대한 서비스 액세스 정보(330)(도 3 참조)를 저장한다. 프로파일 데이터베이스(150)는 또한 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 온라인 아이덴티티 프로파일(332)(도 3 참조)을 또한 저장한다. 온라인 아이덴티티 프로파일(332)은 사용자의 아이덴티티 정보를 포함하며, 이들 중 일부는 온라인 서비스 서버(108)와 공유되지 않고 보안이 유지될 수 있다.

[0017] 정책 데이터베이스(152)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)와 온라인 서비스 서버(108) 사이의 온라인 활동을 제어하도록 게이트웨이 서버(102)에 의해 사용되는 정책 규칙(350)(도 3 참조) 세트를 저장한다. 정책 규칙(350)은, 예를 들어, 온라인 서비스에 관한 화이트/블랙 리스트, 액세스 제어 정책, 구매 거래(purchase transaction) 정책, 및/또는 다른 정책 및 규칙을 포함하는 그러한 활동을 모니터링 및 제어하도록 게이트웨이 서버(102)에 의해 사용가능한 임의의 타입의 정책 규칙으로 포함될 수 있다.

[0018] 일부 실시예들에서, 게이트웨이 서버(102)는 하나 이상의 주변 디바이스(140)를 더 포함할 수 있다. 그러한 주변 디바이스(140)는 서버 컴퓨팅 디바이스에서 공통으로 발견되는 임의의 타입의 주변 디바이스, 예컨대, 하드웨어 키보드, 입력/출력 디바이스, 주변 통신 디바이스, 및/또는 다른 주변 디바이스를 포함할 수 있다.

[0019] "어린이" 클라이언트 컴퓨팅 디바이스(104) 및 "부모" 클라이언트 컴퓨팅 디바이스(106)는 본원에서 설명되는 기능을 수행할 수 있는 임의의 타입의 컴퓨팅 디바이스로서 포함될 수 있다. 예를 들어, 클라이언트 컴퓨팅 디바이스들(104, 106)의 각각은 컴퓨터, 데스크톱 컴퓨터, 워크스테이션, 랩톱 컴퓨터, 노트북 컴퓨터, 태블릿 컴퓨터, 스마트폰, 분산형 컴퓨팅 시스템, 멀티프로세서 시스템, 소비자 전자 장치, 스마트 텔레비전, 스마트 어플라이언스, 및/또는 다른 컴퓨팅 디바이스로 포함될 수 있으나 이로 제한되지 않는다. 클라이언트 컴퓨팅 디바이스들(104, 106)의 각각은 전술된 감시형 아이덴티티 게이트웨이 서버(102)의 컴포넌트들과 유사한, 프로세서, 메모리, 및 I/O 서브시스템과 같은 컴포넌트들을 포함할 수 있다. 본 설명의 명료성을 위해 도 1에 도시되지 않거나 본원에서 별도로 설명되지 않은, 게이트웨이 서버(102)의 그러한 컴포넌트들에 관한 설명은 클라이언트 컴퓨팅 디바이스들(104, 106)의 대응 컴포넌트에 동일하게 적용한다.

[0020] 예시적인 실시예에서, 클라이언트 컴퓨팅 디바이스(104)는 어린이, 또는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자에 의존하는 다른 사람에 의해 동작된다. 이와 같이, "어린이" 및 "부모"에 관한 명칭은 클라이언트 컴퓨팅 디바이스(104) 및 클라이언트 컴퓨팅 디바이스(106) 각각에 관하여 본 명세서 전체에 걸쳐 사용될 수 있다. 그러나, "어린이" 클라이언트 컴퓨팅 디바이스(104)는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자의 어린이로 제한되지 않는다는 것이 이해되어야 한다. 이와 마찬가지로, "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 부모로 제한되지 않는다. 오히려,

클라이언트 디바이스들(104, 106)의 사용자는 어린이-부모가 아닌 관계를 가질 수 있다. 즉, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자에 의해 모리터링/제어될 온라인 아이덴티티 및 활동의 임의의 사용자일 수 있다. 예를 들어, 다른 실시예들에서, 클라이언트 컴퓨팅 디바이스(104)의 사용자는 클라이언트 컴퓨팅 디바이스(106)의 사용자의 직원일 수 있거나 아니면 어린이-부모가 아닌 관계를 가질 수 있다.

[0021] 도 1의 예시적인 시스템(100)은 하나의 "어린이" 클라이언트 컴퓨팅 디바이스(104) 및 하나의 "부모" 클라이언트 컴퓨팅 디바이스(106)만을 포함하지만, 다른 실시예들에서 시스템(100)은 추가적인 "어린이" 클라이언트 컴퓨팅 디바이스(104) 및/또는 "부모" 클라이언트 컴퓨팅 디바이스(106)를 포함할 수 있다. 예를 들어, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자는 하나의 위치(예를 들어, 집) 내의 제 1 클라이언트 컴퓨팅 디바이스 및 제 2 위치(예를 들어, 친구 집) 내의 제 2 클라이언트 컴퓨팅 디바이스를 동작시킬 수 있다. 그러한 실시예들에서, "어린이"에 의해 사용되는 각각의 클라이언트 컴퓨팅 디바이스는 게이트웨이 서버(102)를 통해 온라인 서비스 서버(108)에 액세스하는데 사용되는, "어린이" 클라이언트 컴퓨팅 디바이스(104)를 포함한다. 이와 같이, 게이트웨이 서버(102)에 의해 제공되는 감시형 아이덴티티 및 활동 모니터링은 특정 "어린이" 클라이언트 컴퓨팅 디바이스(104)로 제한되지 않는다.

[0022] 온라인 서비스 서버들(108)은 본원에서 설명되는 기능을 수행할 수 있는, 임의의 타입의 서버 컴퓨팅 디바이스, 또는 디바이스들의 집합으로서 포함될 수 있다. 예를 들어, 온라인 서비스 서버들(108)의 각각은 단일 서버 컴퓨터 또는 복수의 서버 컴퓨터로서 포함될 수 있다. 추가적으로, 일부 실시예들에서, 각각의 온라인 서비스 서버(108)는 네트워크(110)에 걸쳐 분산된 복수의 컴퓨팅 디바이스들로부터 형성되는 "가상 서버"로서 포함될 수 있다. 각각의 온라인 서비스 서버(108)는 감시형 아이덴티티 게이트웨이 서버(102)를 통해 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 의해 액세스될 수 있는, 대응 온라인 서비스를 제공한다. 온라인 서비스 서버(108)는 소셜 네트워킹, 네트워크 서칭, 게임, 정보 검색 및 보급(dissemination), 사업, 및/또는 다른 온라인 서비스를 포함하는 임의의 타임의 온라인 서비스를 제공할 수 있으나 이로 제한되지 않는다.

[0023] 네트워크(110)는 임의의 개수의 다양한 유선 및/또는 무선 통신 네트워크로서 포함될 수 있다. 이와 같이, 네트워크(110)는 하나 이상의 네트워크, 라우터, 스위치, 컴퓨터, 및/또는 다른 중간 디바이스를 포함할 수 있다. 예를 들어, 네트워크(110)는 하나 이상의 셀룰러 네트워크, 전화 통신망(telephone network), 근거리 또는 광역 통신망, 공개 이용가능 글로벌 네트워크(publicly available global networks)(예를 들어, 인터넷), 또는 이들의 임의의 조합으로 포함되거나 아니면 포함할 수 있다.

[0024] 도 1의 시스템(100)에서, 감시형 아이덴티티 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104) 및 "부모" 클라이언트 컴퓨팅 디바이스(106)로부터 원격으로 위치된다. 예를 들어, 일부 실시예들에서, 게이트웨이 서버(102)는 "클라우드" 내에 위치하고 네트워크(110)(예를 들어, 인터넷)를 통해 액세스가능하다. 그러나, 도 2에 도시된 바와 같은 다른 실시예들에서, 감시형 아이덴티티 게이트웨이 서버(102)는 로컬 서버로서 포함될 수 있다. 예를 들어, 게이트웨이 서버(102)는 클라이언트 컴퓨팅 디바이스들(104, 106)의 사용자들로서 동일한 거주지 또는 집 내에 위치될 수 있다. 그러한 실시예들에서, 게이트웨이 서버(102)는, 적합한 통신 기술 및 프로토콜(예를 들어, 이더넷, Wi-Fi, TCP/IP 등)을 사용하여 근거리 통신망(LAN)으로서 포함될 수 있는, 로컬 네트워크(200)를 통해 클라이언트 컴퓨팅 디바이스들(104, 106)에 의해 액세스가능할 수 있다.

[0025] 추가적으로, 일부 실시예들에서, 도 2의 로컬 감시형 아이덴티티 게이트웨이 서버(102)는, 클라이언트 컴퓨팅 디바이스들(104, 106)이 게이트웨이 서버로부터 원격으로 위치된 때조차도 액세스가능할 수 있다. 예를 들어, 도 2에 도시된 바와 같이, "어린이" 클라이언트 컴퓨팅 디바이스(104)는 감시형 아이덴티티 게이트웨이 서버(102)로부터 원격으로 위치될 수 있지만 네트워크(110) 및 로컬 네트워크(200)를 통해 감시형 아이덴티티 게이트웨이 서버에 액세스할 수 있다. 이러한 방법으로, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자는 감시형 아이덴티티 게이트웨이 서버(102)로부터 원격에 있을 때(예를 들어, 게이트웨이 서버(102)에 의해 서비스되는 홈으로부터 원격에 있을 때)조차도 게이트웨이 서버(102)를 통해 온라인 서비스 서버(108)에 계속 액세스할 수 있다. 물론, 다른 실시예들에서, 다른 시스템 토폴로지가 사용될 수도 있다. 임의의 그러한 토폴로지에서, 감시형 아이덴티티 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 의해 액세스가능하고 이로써 아래에서 더 상세히 설명되는 바와 같은 감시 방식으로 온라인 서비스 서버들(108)에 액세스한다.

[0026] 이제 도 3을 참조하면, 사용 시, 감시형 아이덴티티 게이트웨이 서버(102)는 환경(300)을 수립한다. 환경(300)은 아이덴티티 관리자 모듈(302), 활동 모니터 모듈(304), 프로파일 데이터베이스(150), 및 정책 데이터베이스

(152)를 포함한다. 아이덴티티 관리자 모듈(302), 활동 모니터 모듈(304), 및 환경(300)의 다른 모듈들의 각각은 소프트웨어, 펌웨어, 하드웨어, 또는 이들의 임의의 조합으로서 포함될 수 있다.

[0027] 아이덴티티 관리자 모듈(302)은, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 온라인 아이덴티티를 관리하고 등록 및 로그인 절차를 포함하면서 사용자의 원하는 온라인 아이덴티티를 유지하는 액세스를 온라인 서비스 서버들(108)과 가능하게 한다. 아이덴티티 관리자 모듈(302)은 서비스 액세스 모듈(310) 및 관리 모듈(312)을 포함한다. 서비스 액세스 모듈(310)은 정책 데이터베이스(152)에 저장된 정책 규칙(350)(예를 들어, 화이트/블랙 리스트)에 기초하여 온라인 서비스 서버들(108)에 의해 호스팅되는 원하는 온라인 서비스들에 등록 및 액세스한다. 예를 들어, "어린이" 컴퓨팅 디바이스(104)의 사용자가 새로운 온라인 서비스(예를 들어, 새로운 소셜 네트워킹 서비스)에 등록하기 원하는 경우, 서비스 액세스 모듈(310)은 새로운 온라인 서비스에 대한 등록 프로세스를 가능하게 한다. 그렇게 하여, 서비스 액세스 모듈(310)은 프로파일 데이터베이스(150)에 저장되는, 새로운 온라인 서비스에 대한 서비스 액세스 정보(330)를 생성한다. 서비스 액세스 정보(330)는, 예를 들어, 대응 온라인 서비스 서버(108)의 서비스 및/또는 위치(예를 들어, URL(Uniform Resource Locator), 인터넷 프로토콜 어드레스 등)를 식별하는 서비스 식별(340), 특정 서비스에 대한 사용자이름, 온라인 서비스 서버(108)에 로그인하는데 사용되는 패스워드를 포함할 수 있다. "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에 관한 감시를 인에이블하기 위해, 패스워드(344)(및 일부 실시예에서의 사용자이름(342))는 사용자에게 기밀하고 비밀스러운 것으로 유지된다. 즉, 패스워드(344) 및 온라인 서비스에 액세스하는데 사용되는 다른 정보는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에 의해 액세스 가능하지 않다. 일부 실시예들에서, 감시형 아이덴티티 게이트웨이 서버(102)는 패스워드(344) 및/또는 사용자이름(342)을 생성한다. 예를 들어, 게이트웨이 서버(102)는 패스워드(344)를 무작위로 생성할 수 있고 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에 의해 발견가능하지 않은 방식으로 패스워드(344)를 생성하는 일부 다른 기능 또는 방법을 사용할 수 있다. 추가적으로, 아래에서 더 상세히 설명되는 바와 같이, 게이트웨이 서버(102)는 새로운 온라인 서비스에 등록하고자 시도하는 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 응답하여 "부모" 클라이언트 컴퓨팅 디바이스(106)로 통지 또는 경고 메시지를 송신할 수 있다. 그러한 통지는 요청된 새로운 온라인 서비스가 아래에서 설명되는 바와 같은 정책 데이터베이스(152)에 기초하여 수락가능하지 않다는 결정에 대한 응답일 수 있다. 추가적으로 또는 대안적으로, 일부 실시예들에서, 모든 새로운 등록 요청은 등록 이전에 확인을 위해 "부모" 클라이언트 컴퓨팅 디바이스(106)에 송신된다. 이러한 방법으로, 감시형 아이덴티티 게이트웨이 서버(102)는 아래에서 더 상세히 설명되는 바와 같이 사용자의 온라인 아이덴티티 프로파일 및 활동에 대한 제어를 유지한다.

[0028] 등록 프로세스 동안, 관리 모듈(312)은 프로파일 데이터베이스(150)에 저장된 어린이 아이덴티티 프로파일(332) 및 정책 데이터베이스(152)에 저장된 정책 규칙(350)에 기초하여 특정 온라인 서비스에 대한 온라인 아이덴티티의 생성을 관리할 수 있다. 일부 실시예들에서, 어린이 아이덴티티 프로파일(332)은 일부 또는 모든 온라인 서비스로부터 비밀로 유지될, 이를 테면, 등록 프로세스에서 사용되지 않는, 아이덴티티 정보를 포함할 수 있다. 대안적으로, 디폴트 또는 애매모호한 정보는 특정 아이덴티티 정보로 사용될 수 있다. 이러한 방법에서, 관리 모듈(312)은 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 아이덴티티 정보의 보급에 대한 제어를 유지할 수 있고, 일부 실시예들에서는, 다양한 온라인 서비스들에 걸쳐 일관된 온라인 아이덴티티(consistent online identity)를 유지할 수 있다.

[0029] 온라인 서비스가 성공적으로 등록된 이후, 서비스 액세스 모듈(310)은 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터의 요청에 응답하여 등록된 온라인 서비스에 대한 액세스를 가능하게 할 수 있다. 그렇게 해서, 서비스 액세스 모듈(310)은 요청된 온라인 서비스에 액세스하기 위해 서비스 액세스 정보(330)를 이용한다. 물론, 그러한 액세스는 요청된 온라인 서비스의 시간(time of day), 기간(length of time), 또는 다른 액세스 파라미터를 기술할 수 있는, 정책 데이터베이스(152) 내에 정의된 정책 규칙(350)에 의존한다. 관리 모듈(312)은 또한 "부모" 클라이언트 컴퓨팅 디바이스(106)로부터의 요청에 응답하여 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 온라인 아이덴티티를 관리하고, 정책 데이터베이스(152) 내에 정의된 정책을 관리하고, 클라이언트 컴퓨팅 디바이스(104)의 활동 로그(activity logs)를 리뷰하고, 및/또는 게이트웨이 서버(102)에 의해 제공되는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 활동에 관한 온라인 감시의 관리를 가능하게 할 수 있다.

[0030] 활동 모니터 모듈(304)은 "어린이" 클라이언트 컴퓨팅 디바이스(104)와 온라인 서비스 서버들(108) 사이의 온라인 활동을 모니터링 및 제어한다. 그렇게 해서, 활동 모니터 모듈(304)은 어린이 모니터 모듈(322) 및 서비스 모니터 모듈(324)을 포함한다. 어린이 모니터 모듈(322)은 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 온라인 활동을 모니터링하고, 서비스 모니터 모듈(324)은 온라인 서비스 서버들(108)의 온라인 활동을 모니터링한다.

활동 모니터 모듈(304)은 정책 데이터베이스(152)에 저장된 정책 규칙(350)에 따라 그러한 활동을 모니터링 및 제어한다.

[0031] 앞서 설명된 바와 같이, 정책 데이터베이스(152)는 아이덴티티 식별 관리자 모듈(302) 및 활동 모니터 모듈(304)에 의해 실시되는(enforced) 액세스 및 활동 정책을 정의하는, 정책 규칙(350)을 포함한다. 각각의 정책 규칙(350)은 "어린이" 클라이언트 컴퓨팅 디바이스(104) 및/또는 온라인 서비스 서버들(108)의 온라인 활동을 모니터링 및 제어하도록 모듈들(302, 304)에 의해 사용가능한 임의의 타입의 정책 규칙으로서 포함될 수 있다. 예를 들어, 예시적인 실시예에서, 정책 규칙(350)은 화이트 리스트(352) 및 블랙 리스트(354)를 포함한다. 화이트 리스트(352)는 게이트웨이 서버(102)에 의해(즉, "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자에 의해) 수락가능한 것으로 여겨진 온라인 서비스들을 식별하고, 블랙 리스트(354)는 게이트웨이 서버(102)에 의해 수락가능하지 않은 것으로 여겨지는 온라인 서비스를 식별한다. 이와 같이, 아이덴티티 관리자 모듈(302)은, 블랙 리스트(354) 상에 나열된 온라인 서비스에 등록하려는 임의의 요청을 무시할 것이고 화이트 리스트(352) 상에 나열된 임의의 온라인 서비스의 등록을 허가할 것이다. 요청된 새로운 온라인 서비스에 관한 임의의 그러한 거절 또는 허가는, 부모 통지 정책(364)에 관하여 아래에서 더 상세히 설명되는 바와 같이, 게이트웨이 서버(102)로 하여금 "부모" 클라이언트 컴퓨팅 디바이스(106)로 대응 통지를 송신하게 할 수 있다.

[0032] 예시적인 정책 규칙(350)은 또한 액세스 정책(356), 콘텐츠 정책(358), 및 구매 정책(360)을 포함한다. 액세스 정책(356)은 집단적으로 또는 개별적으로 온라인 서비스 서버들(108)에 대한 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 의한 액세스를 허용하는 다양한 액세스 파라미터를 규정하는 정책 규칙을 정의한다. 예를 들어, 액세스 정책(356)은 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 의해 액세스가능한 시간, 온라인 서비스가 액세스가능한 기간, 및/또는 온라인 서비스에 대한 액세스 파라미터를 규정하는 다른 정책을 정의하는 정책 규칙을 포함할 수 있다. 이와 마찬가지로, 콘텐츠 정책(358)은 어떤 콘텐츠가 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터 송신 및/또는 수신되도록 수락가능한/수락가능하지 않은지를 규정하는 정책 규칙을 정의한다. 콘텐츠 정책(358)은, 예를 들어, 콘텐츠 타입, 콘텐츠와 연관된 메타데이터, 콘텐츠 소스, 및/또는 다른 콘텐츠 파라미터를 포함하는, 임의의 파라미터를 사용하여 수락가능한/수락가능하지 않은 콘텐츠를 식별할 수 있다. 활동 모니터 모듈(304)은 온라인 서비스 서버(108)가 수락가능하지 않은 콘텐츠를 전달하고자 시도하고 있고 및/또는 "어린이" 클라이언트 컴퓨팅 디바이스(104)가 수락가능하지 않은 콘텐츠를 송신하고자 시도하고 있다고 결정한 경우, 활동 모니터 모듈(304)은 아래에서 더 상세히 설명되는 바와 같이 그러한 콘텐츠를 차단(block)하고/하거나 다른 수단을 취한다. 이와 마찬가지로, 구매 정책(360)은 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에 의해 수행될 수 있는 온라인 구매 거래에 관한 파라미터를 규정하는 정책 규칙을 정의한다. 예를 들어, 구매 정책(360)은 임의의 온라인 구매에 대한 금액 한도(monetary limit)를 정의할 수 있고, "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자에 의한 허가를 요청하는 금액 제한을 정의하거나, 구매 거래가 수락가능한/수락가능하지 않은 온라인 서비스를 정의하거나, 및/또는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에 의해 수행될 수 있는 온라인 구매 거래의 타입을 제어하는 다른 정책 규칙을 정의할 수 있다.

[0033] 정책 규칙(350)은 또한 프로파일 정책(362)을 포함한다. 프로파일 정책(362)은 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 어떤 아이덴티티 정보가 온라인 서비스 서버들(108) 및/또는 그러한 온라인 서비스의 다른 사용자들과 공유될 수 있는지를 규정하는 정책 규칙을 정의한다. 앞서 설명된 바와 같이, 어린이 아이덴티티 프로파일(332)은 온라인 서비스들과 공유되지 않거나, 특정 온라인 서비스들과 공유되지 않는 정보를 포함할 수 있다. 공유하도록 수락가능한 특정 아이덴티티 정보, 및 아이덴티티 정보의 보급과 관련된 임의의 다른 파라미터는 프로파일 정책(360)에 의해 식별될 수 있다.

[0034] 일부 실시예들에서, 정책 규칙(350)은 또한 부모 통지 정책(364)을 포함할 수 있다. 부모 통지 정책(364)은, 감시형 아이덴티티 게이트웨이 서버(102)로 하여금 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자에게 통지하게 하고/하거나 그러한 경고 이벤트에 응답하여 다른 예방조치(precautions)(예를 들어, 데이터를 로깅(logging))를 행하게 할 수 있는, 다양한 경고 이벤트(alert events)를 정의한다. 부모 통지 정책(364)에 의해 정의되는 경고 이벤트는 정책 데이터베이스(152) 내에 저장된 다른 정책 규칙(350)에 기초할 수 있다. 예를 들어, 콘텐츠 정책(358)에 의해 수락가능하지 않는 것으로 식별된 콘텐츠가 "어린이" 클라이언트 컴퓨팅 디바이스(104)로 또는 그로부터 송신되도록 시도되는 경우, 부모 통지 정책(364)은 통지가 "부모" 클라이언트 컴퓨팅 디바이스(106)에 송신되는 것을 규정할 수 있다. 이와 마찬가지로, "어린이" 클라이언트 컴퓨팅 디바이스(104)가 블랙 리스트(354)에 나열된 온라인 서비스에 등록하고자 시도하거나, 액세스 정책(356)에 대한 온라인 서비스 카운터에 액세스하고자 시도하거나, 및/또는 구매 정책(360) 내에 식별된 한도보다 많은 온라인 구매 거래를 수행하고자 시도하는 경우, 부모 통지 정책(364)은 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자가 그러한

시도들을 통지받는 것을 규정할 수 있다. 물론, 부모 통지 정책(364)은 언제 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자가 통지받을지를 규정하는 임의의 추가적 또는 다른 타입의 정책 규칙을 포함할 수 있다. 즉, 일부 실시예들에서, 경고 통지/확인(confirmation)은 부모 통지 정책(364)에 기초하는 이벤트별 기저로 "부모" 클라이언트 컴퓨팅 디바이스(106)에 송신될 수 있다(즉, 부모 통지 정책(364)은 이벤트가 허용되기 이전에 부모 통지 및/또는 확인을 요청하는 각각의 이벤트를 정의할 수 있다). 그러한 통지는, 이메일, 문자 메시지, 녹음 전화 통화 또는 음성메일, 및/또는 다른 통지를 포함하나 이로 제한되지 않는 임의의 타입의 통지로 포함될 수 있다.

[0035] 이제 도 4를 참조하면, 사용 시, 감시형 아이덴티티 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 온라인 아이덴티티 및 활동을 감시하기 위한 방법(400)을 실행할 수 있다. 방법(400)은 감시형 아이덴티티 게이트웨이 서버(102)가 온라인 서비스에 대한 액세스를 위한 요청이 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 의해 수신되었는지 여부를 결정한다. 그러한 경우, 방법(400)은 게이트웨이 서버(102)가 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자를 식별하는 블록 404로 진행한다. 예를 들어, 블록 406에 도시된 바와 같이, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자는 사용자이름 및 패스워드 또는 다른 로그인 방법(예를 들어, 생체인증, 암호화 토큰 등)을 사용하여 게이트웨이 서버(102)에 로그인할 수 있다. 그 이후, 블록 408에서, 게이트웨이 서버는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 아이덴티티가 검증되는지 여부를 결정한다. 그렇지 않은 경우, 방법(400)은 블록 410으로 진행하여 게이트웨이 서버(102)가 원하는 온라인 서비스에 대한 액세스를 위한 요청을 거절한다. 그 이후 방법은 온라인 서비스에 대한 액세스를 위한 추가 요청을 대기하는 블록 402로 되돌아 간다.

[0036] 그러나, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자가 블록 408에서 검증되는 경우, 방법(400)은 감시형 아이덴티티 게이트웨이 서버(102)가 새로운 온라인 서비스에 등록하는 요청이 클라이언트 컴퓨팅 디바이스(104)로부터 수신되었는지 여부를 결정하는 블록 412로 진행한다. 예시적인 실시예에서, 새로운 온라인 서비스는 그러한 온라인 서비스가 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에게 이용가능하기 전에 감시형 아이덴티티 게이트웨이 서버(102)에 등록되어야 한다. 새로운 온라인 서비스에 등록하려는 요청이 수신되는 경우, 방법(400)은 요청된 새로운 온라인 서비스를 위한 식별 데이터는 게이트웨이 서버(102)에 의해 수신되는 블록 414로 진행한다. 식별 데이터는, 새로운 온라인 서비스를 식별하는 임의의 타입의 데이터로서 포함될 수 있고 게이트웨이 서버(102)(즉, 온라인 서비스를 호스팅하는 온라인 서비스 서버(108))가 온라인 서비스에 액세스할 수 있는 메커니즘을 제공한다. 예를 들어, 예시적인 실시예에서, 식별 데이터는 서비스를 호스팅하는 온라인 서비스 서버(108)에 대한 URL 및/또는 인터넷 프로토콜(IP) 어드레스를 포함한다. 물론, 다른 실시예들에서, 식별 데이터는 서비스의 이름과 같은 다른 데이터를 포함할 수 있다.

[0037] 새로운 온라인 서비스 식별 데이터가 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터 수신된 경우, 게이트웨이 서버(102)는 블록 416에서 새로운 온라인 서비스를 검증한다. 그렇게 하여, 게이트웨이 서버(102)의 아이덴티티 관리자 모듈(302)은 정책 데이터베이스(152)의 정책 규칙(350)을 사용하여 새로운 온라인 서비스가 허가되는지를 검증할 수 있다. 예를 들어, 아이덴티티 관리자 모듈(302)은 새로운 온라인 서비스에 관한 식별 데이터를 블랙 리스트(354)와 비교하여 요청된 새로운 온라인 서비스가 사전에 제한되지 않았다는 것을 보장할 수 있다. 추가적으로, 아이덴티티 관리자 모듈(302)은 요청된 새로운 온라인 서비스로부터 이용가능한 콘텐츠를 콘텐츠 정책(358)과 비교하여 콘텐츠가 수락가능한 것인지를 보장할 수 있다. 물론, 아이덴티티 관리자 모듈(302)은 요청된 새로운 온라인 서비스가 허가되는지 여부를 검증하기 위해 정책 규칙(350) 중 임의의 하나 이상을 이용할 수 있다. 일부 실시예들에서, 블록 418에서, 아이덴티티 관리자 모듈(302)은 새로운 온라인 서비스에 대한 요청이 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터 수신되었다고 통지하기 위해 "부모" 클라이언트 컴퓨팅 디바이스(106)와 통신할 수 있다. 그러한 실시예들에서, 아이덴티티 관리자 모듈(302)은 요청된 새로운 온라인 서비스가 허가되는 "부모" 클라이언트 컴퓨팅 디바이스(106)로부터의 인스트럭션 또는 확인에 응답하여 새로운 온라인 서비스의 등록을 허가할 수 있다.

[0038] 블록 420에서 게이트웨이 서버(102)가 요청된 새로운 온라인 서비스가 허가되지 않는다고 결정한 경우, 방법(400)은 새로운 온라인 서비스에 대한 요청이 거절되는 블록 410으로 진행한다. 추가적으로, 일부 실시예들에서, 게이트웨이 서버(102)는 새로운 온라인 서비스에 대한 요청이 거절되었다는 통지를 "부모" 클라이언트 컴퓨팅 디바이스(106)로 송신할 수 있다.

[0039] 하지만, 블록 420에서 요청된 새로운 온라인 서비스가 허가되는 경우, 방법(400)은 게이트웨이 서버(102)가 새로운 온라인 서비스에 대한 액세스 정보를 생성하는 블록 422로 진행한다. 온라인 서비스에 액세스하는데 요구되는 정보(예를 들어, 온라인 서비스의 URL) 외에, 액세스 정보는 또는 사용자이름 및/또는 패스워드를 또한 포

함할 수 있다. 게이트웨이 서버(102)는 액세스 정보를 생성하는 임의의 적합한 알고리즘 또는 방법을 이용할 수 있다. 예를 들어, 블록 424에 도시된 바와 같이, 게이트웨이 서버(102)는 요청된 온라인 서비스를 위한 사용자 이름 및/또는 패스워드를 무작위로 생성할 수 있다. 다른 실시예들에서, 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자에 의해 제공된 사전결정된 데이터(예를 들어, 사전허가된 패스워드)에 기초하여 사용자이름 및 패스워드를 생성할 수 있다. 추가적으로, 액세스 정보의 생성은 요청된 온라인 서비스의 필요조건(예를 들어, 패스워드 길이 및 캐릭터 필요조건)에 의존할 수 있다. 일부 실시예들에서, 게이트웨이 서버(102)는 패스워드를 생성하지만 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자이름을 수신할 수 있다. 그럼에도 불구하고, 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자로부터 기밀이고 비밀로 유지되는 액세스 정보를 수신한다는 것을 유념해야 한다. 이와 같이, 액세스 정보는 사용자에게 알려지지 않기 때문에, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자는 친구의 컴퓨팅 디바이스와 같은 다른 메커니즘을 통해 온라인 서비스(예를 들어, 새로 생성된 계정)에 액세스하지 못할 수 있다.

[0040] 블록 428에서, 감시형 아이덴티티 게이트웨이 서버(102)는 프로파일 데이터베이스 내에 새로운 온라인 서비스에 대한 액세스 정보를 저장한다. 다시, 액세스 정보는 액세스 정보가 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에 의해 액세스가능하지 않은 방식으로 게이트웨이 서버(102) 상에 저장된다. 블록 430에서, 게이트웨이 서버(102)는 블록 422에서 생성된 액세스 정보를 사용하여 새로운 온라인 서비스에 계정을 등록한다. 추가적으로, 일부 실시예들에서, 온라인 서비스의 타입에 따라, 게이트웨어 서버(102)는 블록 432에서 "어린이" 클라이언트 컴퓨팅 디바이스의 사용자를 위해 온라인 서비스 상에 공개 프로파일을 수립할 수 있다. 그렇게 하여, 게이트웨이 서버(102)는 프로파일 데이터베이스(150)의 어린이 아이덴티티 프로파일(332)에 포함된 정보를 이용할 수 있다. 추가적으로, 게이트웨이 서버(102)는 정책 데이터베이스(152)의 정책 규칙(350)(예를 들어, 프로파일 정책(362))에 기초하여 공개 프로파일을 수립하기 위해 어린이 아이덴티티 프로파일(332)의 어떤 정보를 사용할지를 결정할 수 있다. 이러한 방법에서, "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에 관한 더 많은 아이덴티티 정보는 신뢰되는 온라인 서비스에 제공될 수 있고, 더 적은 아이덴티티 정보는 덜 신뢰되는 서비스에 제공된다.

[0041] 감시형 아이덴티티 게이트웨이 서버(102)가 블록 430에서 새로운 온라인 서비스에 등록한 이후에, 블록 434에서 게이트웨이 서버(102)는 새롭게 등록된 온라인 서비스에 대한 온라인 서비스 명단(online service roster)을 업데이트한다. 온라인 서비스 명단은 "어린이" 클라이언트 컴퓨팅 디바이스의 사용자가 액세스하도록 허가된 등록 온라인 서비스의 리스트로서 포함될 수 있다. 게이트웨이 서버(102)는 프로파일 데이터베이스(150)에 온라인 서비스 명단을 저장할 수 있다.

[0042] 블록 430에서 새로운 온라인 서비스가 온라인 서비스 명단에 추가된 이후에, 방법(400)은 블록 412로 진행하고 여기서 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자가 추가적인 새로운 온라인 서비스에 등록하기 원하는지 여부를 결정한다. 원하는 경우, 방법(400)은 다시 블록 414로 진행하여 앞서 설명된 바와 같이 요청된 새로운 온라인 서비스를 등록한다. 그러나, 온라인 서비스의 등록이 블록 412에서 요청되지 않은 경우, 방법(400)은 블록 500(도 5)으로 진행한다. 블록 500에서, 감시형 아이덴티티 게이트웨이 서버(102)는 허가된 온라인 서비스에 액세스하는 요청이 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터 수신되었는지를 결정한다. 그렇지 않다면, 방법(400)은 게이트웨이 서버(102)가 온라인 서비스에 액세스하는 요청이 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터 수신되었는지를 결정하는 도 4의 블록 402로 되돌아간다. 그러나, 허가된 온라인 서비스에 액세스하는 요청이 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터 수신된 경우, 방법(400)은 블록 502로 진행한다.

[0043] 블록 502에서, 감시형 아이덴티티 게이트웨이 서버(102)는 프로파일 데이터베이스(150)로부터 허가된 온라인 서비스의 온라인 서비스 명단을 검색하고 사용자에게 디스플레이하기 위해 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 허가된 온라인 서비스의 명단을 송신한다. "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자는 명단으로부터 액세스될 원하는 허가된 온라인 서비스를 선택할 수 있다. "어린이" 클라이언트 컴퓨팅 디바이스(104)의 기능에 따라, 원하는 허가된 온라인 서비스를 선택하는데 임의의 적합한 선택 방법이 사용될 수 있다.

[0044] 블록 504에서 게이트웨이 서버(102)가 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터 허가된 온라인 서비스의 선택에 관한 통지를 수신하는 경우, 방법(400)은 게이트웨이 서버(102)가 선택된 허가된 온라인 서비스에 대한 액세스 정보를 검색하는 블록 506으로 진행한다. 앞서 설명된 바와 같이, 액세스 정보는, 프로파일 데이터베이스에 저장될 수 있고 일부 실시예들에서 서비스 식별정보(340)(예를 들어, URL 또는 IP 어드레스), 사용자이름(342), 및 패스워드(344)를 포함할 수 있다. 추가적으로, 앞서 설명된 바와 같이, 액세스 정보 또는 그의 일

부분(예를 들어, 패스워드(344))은 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에게 비밀로 유지된다.

[0045] 선택된 허가된 온라인 서비스에 대한 액세스 정보가 블록 506에서 검색된 후에, 감시형 아이덴티티 게이트웨이 서버(102)는 액세스 정보를 사용하여 요청된 온라인 서비스로의 로그인 프로세스를 가능하게 한다. 예를 들어, 일부 실시예들에서, 게이트웨이 서버(102)는 블록 508에서 액세스 정보를 사용하여 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자가 로그인하도록 선택된 온라인 서비스의 온라인 서비스 서버(108)와 통신할 수 있다. 그러한 실시예들에서, 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)를 위한 프록시로서 역할을 한다. 그러나, 앞서 설명된 바와 같이, 액세스 정보(또는 그것의 부분)는 로그인 프로세스 동안 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에게 기밀로 유지된다.

[0046] 대안적으로, 다른 실시예들에서, 감시형 아이덴티티 게이트웨이 서버(102)는 블록 510에서 액세스 정보에 기초하여 로그인 인증서(login certificate)를 생성함으로써 로그인 프로세스를 가능하게 할 수 있고 블록 512에서 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 생성된 로그인 인증서를 송신한다. "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자는 로그인 인증서를 이용하여 요청된 온라인 서비스 서버(108)에 로그인할 수 있다. 그러한 실시예들에서, 게이트웨이 서버(102)는 임의의 적합한 암호화 방법을 이용하여 액세스 정보에 기초한 로그인 인증서를 생성할 수 있다. 물론, 로그인 인증서는 액세스 정보(또는 그의 일부)에 관한 비밀(secrecy)을 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자로부터 유지한다. 추가적으로, 일부 실시예들에서, 생성된 로그인 인증서는 사전결정된 횟수 이후에는 만료되도록 구성되는 일회용 인증서로 포함될 수 있고, 및/또는 다른 보호 메커니즘을 포함할 수 있다.

[0047] "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자가 요청된 온라인 서비스에 로그인 한 이후에, 감시형 아이덴티티 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)와 요청된 온라인 서비스의 온라인 서비스 서버(108) 사이의 통신을 가능하게 한다. 그와 같이, 일부 실시예들에서, "어린이" 클라이언트 컴퓨팅 디바이스(104)와 온라인 서비스 서버(들)(108) 사이의 모든 통신은 게이트웨이 서버(102)를 통해 전송(tranfer)되거나 아니면 게이트웨이 서버(102)에 의해 액세스가능하다. 그러한 통신을 가능하게 하면서, 게이트웨이 서버(102)는 통신에 기초하여 블록 516에서 임의의 경고 이벤트를 모니터링한다. 그렇게 하여, 게이트웨이 서버(102)는 정책 데이터베이스(152)의 정책 규칙(350)을 사용하여 그러한 경고 이벤트에 대한 통신을 분석할 수 있다.

[0048] 블록 518에서, 게이트웨이 서버(102)는 정책 규칙(350)을 사용하여 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 온라인 활동(activity)을 모니터링함으로써 경고 이벤트에 대해 모니터링할 수 있다. 예를 들어, 게이트웨이 서버(102)는 블록 522에서 액세스 정책(356)을 실시할 수 있다. 앞서 설명된 바와 같이, 액세스 정책(356)은 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자가 특정 허가된 온라인 서비스에 액세스할 수 있는 때, 사용자가 허가된 온라인 서비스에 액세스할 수 있는 기간, 및/또는 "어린이 클라이언트 컴퓨팅 디바이스(104)의 사용자에 의한 허가된 온라인 서비스의 액세스가능성(accessibility)을 제어하는 다른 기준을 규정(dictate)할 수 있다. 추가적으로, 블록 524에서, 게이트웨이 서버(102)는 프로파일 정책(362)을 사용하여 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 아이덴티티 데이터의 노출을 모니터링 및 제어할 수 있다. 그렇게 하여, 게이트웨이 서버(102)는 프로파일 정책(362)(예를 들어, 어드레스 정보, 전체 성명 등)에 기초하여 제한되도록 결정되는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자에 관한 식별정보 데이터를 포함하는 것들에 대하여 "어린이" 클라이언트 컴퓨팅 디바이스(104)로부터 송신되는 통신을 모니터링할 수 있다. 추가적으로, 블록 526에서, 게이트웨이 서버(102)는 구매 정책(360)에 기초하여 온라인 구매 및 결제 거래를 제어할 수 있다. 예를 들어, 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 의한 임의의 온라인 구매가 구매 정책(360)에 의해 규정된 임계 금액 미만인 것을 보장할 수 있다. 일부 실시예들에서, 게이트웨이 서버(102)는 블록 528에서 "어린이" 클라이언트 컴퓨팅 디바이스의 사용자의 온라인 활동을 또한 기록할 수 있다. 예를 들어, 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)에 의해 수신되고 송신된 통신을 기록할 수 있다. 온라인 활동에 관한 그러한 기록은 정책 규칙(350)에 기초할 수 있고 연속으로 또는 정책 규칙(350)에 의해 정의되는 바와 같이 경고 이벤트의 검출에 응답하여 발생할 수 있다.

[0049] 블록 520에서, 게이트웨이 서버(102)는 정책 규칙을 사용하여 온라인 서비스 서버(108)의 온라인 활동을 모니터링함으로써 경고 이벤트를 또한 모니터링할 수 있다. 예를 들어, 게이트웨이 서버(102)는 블록 530에서 온라인 서비스에 의해 제공된 콘텐츠에 대한 액세스를 모니터링 및/또는 제어할 수 있다. 그렇게 하여, 게이트웨이 서버(102)는 온라인 서비스 서버(108)에 의해 전달된 콘텐츠를 모니터링하여 그러한 콘텐츠가 콘텐츠 정책(358)에 기초하여 미허가 콘텐츠(예를 들어, 성인 콘텐츠)인지 여부를 결정할 수 있다. 추가적으로, 블록 532에서, 게이트웨이 서버(102)는 정책 데이터베이스(152)의 프로파일 정책(362)에 기초하여 "어린이" 클라이언트 컴퓨팅 디

바이스(104)의 사용자의 아이덴티티 데이터에 대한 요청들을 모니터링 및/또는 제어할 수 있다. 예를 들어, 게이트웨이 서버(102)는 제한되거나 사적인(private) 것(예를 들어, 어드레스 정보, 전체 성명 등)으로 식별되었던 어린이 아이덴티티 프로파일(332)의 식별정보 데이터에 관한 요청들을 모니터링할 수 있다.

[0050] 물론, 게이트웨이 서버(102)는 정책 데이터베이스의 임의의 정책 규칙(350)에 기초하여 온라인 서비스 서버(들)(108) 및/또는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 활동을 모니터링하여 경고 이벤트가 블록 516에서 발생했는지 여부를 결정할 수 있다는 것이 이해되어야 한다. 블록 534에서, 게이트웨이 서버(102)가 어떠한 경고 이벤트도 발생하지 않았다고 결정하는 경우, 방법(400)은 게이트 서버(102)가 "어린이" 클라이언트 컴퓨팅 디바이스(104)와 온라인 서비스 서버(108) 사이의 통신을 계속해서 가능하게 하는 블록 514로 되돌아간다. 그러나, 게이트웨이 서버(102)가 경고 이벤트가 발생했다고 결정하는 경우, 방법(400)은 블록 600(도 6)으로 진행한다. 블록 600에서, 게이트웨이 서버(102)는 경고 이벤트를 생성하는 활동이 차단되어야 하는지 결정한다. 즉, 정책 규칙(350)은 경고 이벤트를 프롬프팅하는 활동이 차단될 것인지 여부를 규정할 수 있다. 예를 들어, 게이트웨이 서버(102)가 콘텐츠 정책(358)에 기초하여 온라인 서비스 서버(108)로부터 허가되지 않은 콘텐츠가 송신된다고 결정하는 경우, 게이트웨이 서버(102)는 그러한 차단 조치를 지시하는 콘텐츠 정책(358)에 응답하여 블록 602에서 콘텐츠를 차단할 수 있다.

[0051] 경고 이벤트를 생성하는 활동이 블록 600에서 차단되지 않거나 활동이 블록 602에서 차단된 이후에, 방법(400)은 블록 604로 진행하고 여기서 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)에 경고 이벤트를 통지할지 여부를 결정한다. "부모" 클라이언트 컴퓨팅 디바이스(106)의 통지는 부모 통지 정책(364) 및/또는 정책 데이터베이스(152)의 정책 규칙(350)의 다른 정책에 의해 정의될 수 있다. 이와 같이, 일부 경고 이벤트들은 "부모" 클라이언트 컴퓨팅 디바이스(106)의 통지를 트리거링할 수 있지만, 다른 경고 이벤트들은 하지 않는다. 블록 604에서 게이트웨이 서버(102)가 "부모" 클라이언트 컴퓨팅 디바이스(106)에 통지할 것이라고 결정하는 경우, 방법(400)은 블록 606으로 진행하고 여기서 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)에 통지를 송신한다. 그러한 통지는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자에게 경고 이벤트가 발생 및/또는 차단된 것을 통지할 수 있다. 일부 실시예들에서, "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자는 블록 608에서 경고 이벤트의 차단을 중단하거나 아니면 경고 이벤트를 프롬프팅하는 활동을 허가할 수 있다. "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자가 경고 이벤트를 프롬프팅하는 활동을 허가한 경우, 방법(400)은 게이트웨이 서버(102)가 활동을 허용하는 블록 610으로 진행한다. 예를 들어, 게이트웨이 서버(102)가 활동을 차단했던 경우에, 활동은 블록 610에서 차단되지 않는다. 활동이 610에서 허용되었거나 활동이 블록 608에서 허가되지 않은 이후에, 방법(400)은 게이트웨이 서버(102)가 "어린이" 클라이언트 컴퓨팅 디바이스(104)와 온라인 서비스 서버(들)(108) 사이의 통신을 계속 가능하게 하는 블록 514(도 5)로 되돌아 간다.

[0052] 이제 도 7을 참조하면, 일부 실시예들에서, 감시형 아이덴티티 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)에 의한 아이덴티티 감시의 관리를 가능하게 할 수 있다. 그렇게 하여, 게이트웨이 서버(102)는 온라인 아이덴티티의 감시를 관리하기 위한 방법(700)을 실행할 수 있다. 방법(700)은 게이트웨이 서버(102)가 액세스에 대한 요청이 "부모" 클라이언트 컴퓨팅 디바이스(106)로부터 수신되었는지를 결정하는 블록 702에서 시작한다. 그렇다면, 방법(700)은 블록 704로 진행하고 여기서 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자를 식별한다. 예를 들어, 블록 706에 도시된 바와 같이, "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자는 사용자이름 및 패스워드 또는 다른 로그인 방법(예를 들어, 생체인증, 암호화 토큰 등)을 사용하여 게이트웨이 서버(102)에 로그인할 수 있다. 그 이후, 블록 708에서, 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자가 검증되는지를 결정한다. 그렇지 않다면, 액세스에 대한 요청은 거절되고, 방법(700)은 블록 702로 되돌아가서 액세스에 대한 추가 요청을 기다린다.

[0053] 그러나, 블록 708에서 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자가 검증되는 경우, 방법(700)은 블록 710 및 블록 730으로 진행한다. 블록 710에서, 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자가 정책 데이터베이스(152)의 정책 규칙(350)을 업데이트하기 원하는지 결정한다. 원하는 경우, 방법(700)은 블록 712로 진행하고 여기서 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)로부터 업데이트된 정책 데이터를 수신한다. 예를 들어, 게이트웨이 서버(102)는 블록 714에서 업데이트된 화이트 및/또는 블랙 리스트 정책 데이터, 블록 716에서 업데이트된 액세스 정책 데이터, 블록 718에서 업데이트된 콘텐츠 정책 데이터, 블록 720에서 업데이트된 구매 정책 데이터, 블록 722에서 업데이트된 프로파일 정책 데이터, 블록 724에서 업데이트된 부모 통지 정책 데이터, 및/또는 블록 726에서 업데이트된 다른 정책 데이터를 나열할 수 있다. 특정 업데이트된 정책 데이터 및 이들의 포맷은 업데이트되는 특정 정책 및/또는 다른 기준에 의존할 수 있다. 그럼에도 불구하고, 블록 728에서, 게이트웨이 서버(102)는 정책 데이터베이스(152)에 업데

이트된 정책 데이터를 저장한다. 업데이트된 정책 데이터가 국부적으로 저장된 이후에, 방법(700)은 블록들(710, 730)로 되돌아 간다.

[0054] 블록 730에서, 게이트웨이 서버(102)는 "부모" 클라이언트 컴퓨팅 디바이스(106)의 사용자가 게이트웨이 서버에 의해 기록된 활동 로그(activity logs)에 액세스하기 원하는지 여부를 결정한다. 앞서 설명된 바와 같이, 게이트웨이 서버(102)는 "어린이" 클라이언트 컴퓨팅 디바이스(104)의 사용자의 온라인 활동 및/또는 액세스된 온라인 서비스를 기록할 수 있다. 그러한 활동은, 예를 들어, "어린이" 클라이언트 컴퓨팅 디바이스(104)와 온라인 서비스 서버(108) 사이의 통신을 포함할 수 있다. 블록 730에서 활동 로그에 대한 요청이 수신되는 경우, 블록 732에서 게이트웨이 서버는 요청된 활동 로그를 검색하고 블록 734에서 "부모" 클라이언트 컴퓨팅 디바이스(106)로 활동 로그를 송신한다. 그 이후 방법(700)은 블록들(710, 730)로 되돌아 가서 앞서 설명된 바와 같이 정책 데이터베이스(152)를 업데이트하고 활동 로그에 액세스하는 요청을 모니터링한다.

[0055] 예시

[0056] 본원에서 설명되는 기법들에 관한 실례가 되는 예시들은 아래에서 제공된다. 기법들에 관한 일 실시예는 아래에서 설명되는 예시들 중 임의의 하나 이상의 예시, 및 이들의 임의의 조합을 포함할 수 있다.

[0057] 예시 1은 온라인 아이덴티티의 감시를 가능하게 하는 게이트웨이 서버를 포함하고, 상기 게이트웨이 서버는 클라이언트 컴퓨팅 디바이스의 사용자의 온라인 서비스에 대한 액세스 정보를 저장하는 프로파일 데이터베이스 - 상기 액세스 정보는 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스가능하지 않음 - 와; 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 허가된 활동을 저의하는 정책 규칙 세트를 저장하는 정책 데이터베이스와; (ⅰ) 상기 클라이언트 컴퓨팅 디바이스로부터 온라인 서비스에 대한 액세스를 위한 요청을 수신하고, (ii) 상기 요청에 응답하여, 상기 프로파일 데이터베이스로부터 상기 온라인 서비스에 대한 액세스 정보를 검색하고, (iii) 상기 액세스 정보를 사용하여 상기 클라이어트 컴퓨팅 디바이스을 위해 상기 온라인 서비스에 대한 액세스를 가능하게 하는 아이덴티티 관리자 모듈과; 상기 정책 규칙 세트에 기초하여 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 활동 모니터 모듈을 포함한다.

[0058] 예시 2는 예시 1의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 위한 요청을 수신하는 것은, 상기 게이트웨이 서버의 데이터베이스로부터 이용가능한 허가된 온라인 서비스에 관한 식별 데이터를 검색하는 것과; 상기 클라이언트 컴퓨팅 디바이스로 상기 이용가능한 허가된 온라인 서비스의 식별 데이터를 송신하는 것과; 상기 클라이언트 컴퓨팅 디바이스로부터 상기 이용가능한 허가된 온라인 서비스 중 하나의 선택을 수신하는 것을 포함한다.

[0059] 예시 3은 예시 1 및 2 중 임의의 예시의 요지를 포함하고, 상기 액세스 정보를 검색하는 것은, 상기 온라인 컴퓨팅 디바이스의 사용자가 상기 온라인 서비스에 로그인하도록 상기 게이트웨이 서버에 의해 사용가능한 로그인 정보를 검색하는 것을 포함한다.

[0060] 예시 4는 예시 1 내지 예시 3 중 임의의 예시의 요지를 포함하고, 상기 로그인 정보는 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 온라인 서비스에 로그인하는데 사용가능한 사용자 이름 또는 패스워드 중 적어도 하나를 포함한다.

[0061] 예시 5는 예시 1 내지 예시 4 중 임의의 예시의 요지를 포함하고, 상기 사용자이름 또는 상기 패스워드 중 적어도 하나는 상기 게이트웨이 서버에 의해 무작위로 이전에 생성된 것이다.

[0062] 예시 6은 예시 1 내지 예시 5 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스는 상기 액세스 정보를 사용하여 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 온라인 서비스에 로깅하면서 상기 액세스 정보를 상기 클라이언트 컴퓨팅 디바이스로부터 비밀로 유지하는 것을 포함한다.

[0063] 예시 7은 예시 1 내지 예시 6 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 가능하게 하는 것은 상기 액세스 정보에 기초하여 로그인 인증서를 생성하는 것을 포함하고, 상기 로그인 인증서는 상기 온라인 서비스에 로깅하기 위해 상기 클라이언트 컴퓨팅 디바이스에 의해 사용가능하다.

[0064] 예시 8은 예시 1 내지 예시 7 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 가능하게 하는 것은 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 네트워크 통신을 가능하게 하는 것을 포함한다.

[0065] 예시 9는 예시 1 내지 예시 8 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 것은 상기 정책 데이터베이스의 액세스 제어 정책에 따라 상기 클라이언트

컴퓨팅 디바이스에 의한 상기 온라인 서비스에 대한 액세스를 제어하는 것을 포함한다.

[0066] 예시 10은 예시 1 내지 예시 9 중 임의의 예시의 요지를 포함하고, 상기 액세스 제어 정책은 (ⅰ) 상기 클라이언트 컴퓨팅 디바이스가 상기 온라인 서비스에 액세스할 수 있는 기간 또는 (ii) 상기 클라이언트 컴퓨팅 디바이스가 상기 온라인 서비스에 액세스할 수 있는 시간 중 적어도 하나를 정의한다.

[0067] 예시 11은 예시 1 내지 예시 10 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 것은 상기 정책 데이터베이스의 프로파일 공개 정책(profile disclosure policy)에 기초하여 상기 온라인 서비스에 대한 상기 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티 프로파일 정보의 공개를 제어하는 것을 포함한다.

[0068] 예시 12는 예시 1 내지 예시 11 중 임의의 예시의 요지를 포함하고, 상기 아이덴티티 프로파일 정보의 공개를 제어하는 것은 상기 온라인 서비스로부터 수신된 아이덴티티 프로파일 정보에 대한 요청을 차단하는 것을 포함한다.

[0069] 예시 13은 예시 1 내지 예시 12 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 것은 상기 정책 데이터베이스의 구매 거래 정책에 기초하여 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 온라인 구매 거래를 제어하는 것을 포함한다.

[0070] 예시 14는 예시 1 내지 예시 13 중 임의의 예시의 요지를 포함하고, 상기 온라인 결제 거래를 제어하는 것은 상기 온라인 결제 거래의 통화량(currency amount)이 상기 구매 거래 정책에 정의된 임계 통화량(threshold currency amount)을 넘는다는 결정에 응답하여 상기 온라인 결제 거래를 차단하는 것을 포함한다.

[0071] 예시 15는 예시 1 내지 예시 14 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 것은 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 표시하는 데이터 로그(data log)를 생성하는 것을 포함한다.

[0072] 예시 16은 예시 1 내지 예시 15 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 것은 상기 정책 데이터베이스의 콘텐츠 정책에 기초하여 온라인 서비스에 의해 전달된 콘텐츠를 제어하는 것을 포함한다.

[0073] 예시 17은 예시 1 내지 예시 16 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 의해 전달된 콘텐츠를 제어하는 것은 상기 콘텐츠 정책에서 식별된 참조 콘텐츠와 관련되는 콘텐츠에 응답하여 상기 클라이언트 컴퓨팅 디바이스에 의한 상기 콘텐츠에 대한 액세스를 차단하는 것을 포함한다.

[0074] 예시 18은 예시 1 내지 예시 17 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 것은 경고 이벤트의 발생에 대하여 상기 활동을 모니터링하는 것 및 상기 경고 이벤트의 발생에 응답하여 경고를 생성하는 것을 포함한다.

[0075] 예시 19는 예시 1 내지 예시 18 중 임의의 예시의 요지를 포함하고, 상기 경고 이벤트는, (ⅰ) 상기 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티 프로파일 정보에 대한 상기 온라인 서비스에 의한 요청, (ii) 구매 거래의 개시(initiation), 또는 (iii) 콘텐츠 정책에 기초하여 수락가능하지 않은 것으로 식별된 상기 온라인 서비스에 의한 콘텐츠의 전달 중 적어도 하나를 포함한다.

[0076] 예시 20은 예시 1 내지 예시 19 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 것은 상기 경고 이벤트를 차단하는 것을 더 포함한다.

[0077] 예시 21은 예시 1 내지 예시 20 중 임의의 예시의 요지를 포함하고, 상기 경고를 생성하는 것은 다른 컴퓨팅 디바이스의 사용자에게 상기 경고 이벤트의 발생을 알리는 통지를 상기 다른 컴퓨팅 디바이스로 송신하는 것을 포함한다.

[0078] 예시 22는 예시 1 내지 예시 21 중 임의의 예시의 요지를 포함하고, 상기 활동 모니터 모듈은 또한, 상기 통지의 송신에 응답하여 상기 다른 컴퓨팅 디바이스로부터 상기 경고 이벤트에 대한 허가를 수신하고; 상기 허가의 수신에 응답하여 상기 경고 이벤트가 발생하도록 허용한다.

[0079] 예시 23은 예시 1 내지 예시 22 중 임의의 예시의 요지를 포함하고, 상기 아이덴티티 관리자 모듈은 또한, 상기 클라이언트 컴퓨팅 디바이스로부터 새로운 온라인 서비스를 상기 게이트웨이 서버에 등록하라는 요청을 수신하고; 상기 새로운 온라인 서비스를 식별하는 식별 데이터를 수신하고; 상기 새로운 온라인 서비스에 액세스하는 새로운 액세스 정보를 생성하고; 상기 새로운 액세스 정보가 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해

액세스가능하지 않도록 상기 새로운 액세스 정보를 상기 프로파일 데이터베이스 내에 저장한다.

[0080] 예시 24는 예시 1 내지 예시 23 중 임의의 예시의 요지를 포함하고, 상기 새로운 액세스 정보를 생성하는 것은 상기 새로운 온라인 서비스에 액세스하는데 사용가능한 패스워드를 무작위로 생성하는 것을 포함한다.

[0081] 예시 25는 예시 1 내지 예시 24 중 임의의 예시의 요지를 포함하고, 상기 새로운 액세스 정보를 생성하는 것은 상기 패스워드와 연관된 사용자이름을 무작위로 생성하는 것을 포함한다.

[0082] 예시 26은 예시 1 내지 예시 25 중 임의의 예시의 요지를 포함하고, 상기 아이덴티티 관리자 모듈은 또한 상기 새로운 액세스 정보를 사용하여 상기 클라이언트 컴퓨팅 디바이스의 사용자를 상기 새로운 온라인 서비스에 등록한다.

[0083] 예시 27은 예시 1 내지 예시 26의 요지를 포함하고, 상기 아이덴티티 관리자 모듈은 또한 상기 정책 데이터베이스의 정책 규칙 및 상기 식별 데이터에 기초하여 상기 새로운 온라인 서비스가 허가되는지 여부를 결정한다.

[0084] 예시 28은 예시 1 내지 예시 27 중 임의의 예시의 요지를 포함하고, 상기 아이덴티티 관리자 모듈은 또한 다른 클라이언트 컴퓨팅 디바이스로부터 관리 액세스 요청을 수신하고; 상기 다른 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티를 검증하고; 상기 다른 클라이언트 컴퓨팅 디바이스로부터 수신된 데이터에 기초하여 상기 정책 데이터베이스에 저장된 정책 규칙 세트를 업데이트한다.

[0085] 예시 29는 예시 1 내지 예시 28 중 임의의 예시의 요지를 포함하고, 상기 아이덴티티 관리자 모듈은 또한 상기 다른 클라이언트 컴퓨팅 디바이스로부터 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동의 활동 로그에 대한 요청을 수신하고; 상기 활동 로그를 상기 다른 클라이언트 컴퓨팅 디바이스에 송신한다.

[0086] 예시 30은 온라인 아이덴티티를 감시하기 위한 방법을 포함하고, 상기 방법은, 클라이언트 컴퓨팅 디바이스로부터 온라인 서비스에 대한 액세스를 위한 요청을 게이트웨이 서버 상에서 수신하는 단계와; 상기 요청에 응답하여, 상기 게이트웨이 서버의 프로파일 데이터베이스로부터 상기 온라인 서비스에 대한 액세스 정보를 검색하는 단계와; 상기 액세스 정보를 사용하여 상기 클라이언트 컴퓨팅 디바이스의 사용자를 위해 상기 온라인 서비스에 대한 액세스를 가능하게 하는 단계 - 상기 액세스 정보는 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스가능하지 않음 - 와; 상기 게이트웨이 서버를 사용하여, 상기 게이트웨이 서버의 정책 데이터베이스에 저장된 정책 규칙 세트에 기초하여 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 단계를 포함한다.

[0087] 예시 31은 예시 30의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 위한 요청을 수신하는 단계는 상기 게이트웨이 서버의 데이터베이스로부터 이용가능한 허가된 온라인 서비스의 식별 데이터를 검색하는 단계와; 상기 이용가능한 허가된 온라인 서비스의 식별 데이터를 상기 클라이언트 컴퓨팅 디바이스로 송신하는 단계와; 상기 클라이언트 컴퓨팅 디바이스로부터 상기 이용가능한 허가된 온라인 서비스들 중 하나의 선택을 수신하는 단계를 포함한다.

[0088] 예시 32는 예시 30 및 예시 31 중 임의의 예시의 요지를 포함하고, 상기 액세스 정보를 검색하는 단계는 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 온라인 서비스에 로그인하도록 상기 게이트웨이 서버에 의해 사용가능한 로그인 정보를 검색하는 단계를 포함한다.

[0089] 예시 33은 예시 30 내지 예시 32 중 임의의 예시의 요지를 포함하고, 상기 로그인 정보는 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 온라인 서비스에 로그인하는데 사용가능한 사용자이름 또는 패스워드 중 적어도 하나를 포함한다.

[0090] 예시 34는 예시 30 내지 예시 33 중 임의의 예시의 요지를 포함하고, 상기 사용자이름 또는 패스워드 중 적어도 하나는 상기 게이트웨이 서버에 의해 이전에 무작위로 생성된다.

[0091] 예시 35는 예시 30 내지 예시 34 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 가능하게 하는 단계는 상기 액세스 정보를 사용하여 상기 온라인 서비스에 상기 클라이언트 컴퓨팅 디바이스의 사용자를 로깅하면서 상기 액세스 정보를 상기 클라이언트 컴퓨팅 디바이스로부터 비밀로 유지하는 단계를 포함한다.

[0092] 예시 36은 예시 30 내지 예시 35 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 가능하게 하는 단계는 상기 액세스 정보에 기초하여 로그인 인증서를 생성하는 단계를 포함하고, 상기 로그인 인증서는 상기 클라이언트 컴퓨팅 디바이스가 상기 온라인 서비스에 로그인하는데 사용가능하다.

[0093] 예시 37은 예시 30 내지 예시 36 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 가능하게 하는 단계는 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 네트워크 통신을 가능하게 하는 단계를 포함한다.

[0094] 예시 38은 예시 30 내지 예시 37 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 단계는 상기 게이트웨이 서버의 액세스 제어 정책에 따라 상기 클라이언트 컴퓨팅 디바이스에 의한 상기 온라인 서비스에 대한 액세스를 제어하는 단계를 포함한다.

[0095] 예시 39는 예시 30 내지 예시 38 중 임의의 예시의 요지를 포함하고, 상기 액세스 제어 정책은, (ⅰ) 상기 클라이언트 컴퓨팅 디바이스가 상기 온라인 서비스에 액세스할 수 있는 기간 또는 (ii) 상기 클라이언트 컴퓨팅 디바이스가 상기 온라인 서비스에 액세스할 수 있는 시간 중 적어도 하나를 정의한다.

[0096] 예시 40은 예시 30 내지 예시 39 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 단계는 상기 게이트웨이 서버의 프로파일 공개 정책에 기초하여 상기 온라인 서비스로의 상기 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티 프로파일 정보의 공개를 제어하는 단계를 포함한다.

[0097] 예시 41은 예시 30 내지 예시 40 중 임의의 예시의 요지를 포함하고, 상기 아이덴티티 프로파일 정보의 공개를 제어하는 단계는 상기 온라인 서비스로부터 수신된 아이덴티티 프로파일 정보에 대한 요청을 차단하는 단계를 포함한다.

[0098] 예시 42는 예시 30 내지 예시 41 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 단계는 상기 게이트웨이 서버의 구매 거래 정책에 기초하여 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 온라인 결제 거래를 제어하는 단계를 포함한다.

[0099] 예시 43은 예시 30 내지 예시 42 중 임의의 예시의 요지를 포함하고, 상기 온라인 결제 거래를 제어하는 단계는 상기 구매 거래 정책에서 정의된 임계 통화량보다 더 큰 상기 온라인 결제 거래의 통화량에 응답하여 상기 온라인 결제 거래를 차단하는 단계를 포함한다.

[0100] 예시 44는 예시 30 내지 예시 43 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 단계는 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 표시하는 데이터 로그를 생성하는 단계를 포함한다.

[0101] 예시 45는 예시 30 내지 예시 44 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 단계는 상기 게이트웨이 서버의 콘텐츠 정책에 기초하여 온라인 서비스에 의해 전달되는 콘텐츠를 제어하는 단계를 포함한다.

[0102] 예시 46은 예시 30 내지 예시 45 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 의해 전달되는 콘텐츠를 제어하는 단계는 상기 콘텐츠 정책에 식별된 참조 콘텐츠에 관련된 콘텐츠에 응답하여 상기 클라이언트 컴퓨팅 디바이스에 의한 상기 콘텐츠에 대한 액세스를 차단하는 단계를 포함한다.

[0103] 예시 47은 예시 30 내지 예시 46 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하는 단계는 경고 이벤트의 발생을 위해 상기 활동을 모니터링하는 단계 및 상기 경고 이벤트의 발생에 응답하여 경고를 생성하는 단계를 포함한다.

[0104] 예시 48은 예시 30 내지 예시 47 중 임의의 예시의 요지를 포함하고, 상기 경고 이벤트는, (ⅰ) 상기 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티 프로파일 정보에 대한 상기 온라인 서비스에 의한 요청, (ii) 구매 거래의 개시, 또는 (iii) 콘텐츠 정책에 기초하여 수락가능하지 않는 것으로 식별된 상기 온라인 서비스에 인한 콘텐츠의 전달 중 적어도 하나를 포함한다.

[0105] 예시 49는 예시 30 내지 예시 48 중 임의의 예시의 요지를 포함하고, 상기 경고 이벤트를 차단하는 단계를 더 포함한다.

[0106] 예시 50은 예시 30 내지 예시 49 중 임의의 예시의 요지를 포함하고, 상기 경고를 생성하는 단계는 다른 컴퓨팅 디바이스의 사용자에게 상기 경고 이벤트의 발생을 알리는 통지를 상기 다른 클라이언트 컴퓨팅 디바이스로 송신하는 단계를 포함한다.

[0107] 예시 51은 예시 30 내지 예시 50 중 임의의 예시의 요지를 포함하고, 상기 통지를 송신하는 것에 응답하여 상기 다른 컴퓨팅 디바이스로부터 상기 경고 이벤트에 대한 허가를 수신하는 단계와; 상기 경고 이벤트가 상기 허가

의 수신에 응답하여 발생하도록 허용하는 단계를 더 포함한다.

[0108] 예시 52는 예시 30 내지 예시 51 중 임의의 예시의 요지를 포함하고, 상기 게이트웨이 서버를 사용하여 새로운 온라인 서비스에 등록하라는 요청을 상기 클라이언트 컴퓨팅 디바이스로부터 수신하는 단계와; 상기 새로운 온라인 서비스에 액세스하도록 새로운 액세스 정보를 생성하는 단계와; 상기 새로운 액세스 정보가 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스가능하지 않도록 상기 게이트웨이 서버 상에 상기 새로운 액세스 정보를 저장하는 단계를 더 포함한다.

[0109] 예시 53은 예시 30 내지 예시 52 중 임의의 예시의 요지를 포함하고, 새로운 액세스 정보를 생성하는 단계는 상기 새로운 온라인 서비스에 액세스하는데 사용가능한 패스워드를 무작위로 생성하는 단계를 포함한다.

[0110] 예시 54는 예시 30 내지 예시 53 중 임의의 예시의 요지를 포함하고, 새로운 액세스 정보를 생성하는 단계는 상기 패스워드와 연관된 사용자이름을 무작위로 생성하는 단계를 포함한다.

[0111] 예시 55는 예시 30 내지 예시 54 중 임의의 예시의 요지를 포함하고, 상기 새로운 액세스 정보를 사용하여 상기 새로운 온라인 서비스에 상기 클라이언트 컴퓨팅 디바이스의 사용자를 등록하는 단계를 더 포함한다.

[0112] 예시 56은 예시 30 내지 예시 55 중 임의의 예시의 요지를 포함하고, 상기 게이트웨이 서버에 의해 유지되는 정책 데이터베이스의 정책 규칙 및 상기 식별 데이터에 기초하여 상기 새로운 온라인 서비스가 허가되는지 여부를 결정하는 단계를 더 포함한다.

[0113] 예시 57은 예시 30 내지 예시 56 중 임의의 하나의 예시의 요지를 포함하고, 상기 게이트웨이 서버 상에서, 다른 클라이언트 컴퓨팅 디바이스로부터 관리 액세스 요청을 수신하는 단계와; 상기 다른 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티를 검증하는 단계와; 상기 다른 클라이언트 컴퓨팅 디바이스로부터 수신된 데이터에 기초하여 상기 정책 데이터베이스에 저장된 정책 규칙 세트를 업데이트하는 단계를 더 포함한다.

[0114] 예시 58은 예시 30 내지 예시 57 중 임의의 하나의 예시의 요지를 포함하고, 상기 게이트웨이 서버 상에서, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동의 활동 로그에 대한 요청을 수신하는 단계와; 상기 다른 클라이언트 컴퓨팅 디바이스로 상기 활동 로그를 송신하는 단계를 더 포함한다.

[0115] 예시 59는 프로세서, 복수의 인스트럭션이 저장된 메모리를 포함하는 컴퓨팅 디바이스를 포함하고, 상기 복수의 인스트럭션은 상기 프로세서에 의해 실행될 때 상기 컴퓨팅 디바이스로 하여금 예시 30 내지 예시 58 중 임의의 예시의 방법을 수행하게 한다.

[0116] 예시 60은 복수의 인스트럭션이 저장된 하나 이상의 머신 판독가능 저장 매체를 포함하고, 상기 복수의 인스트럭션은 실행되는 것에 응답하여 컴퓨팅 디바이스가 예시 30 내지 예시 58 중 임의의 예시의 방법을 수행하게 한다.

[0117] 예시 61은 예시 30 내지 예시 38 중 임의의 예시의 방법을 수행하기 위한 수단들을 포함하는 컴퓨팅 디바이스를 포함한다.

[0118] 예시 61은 온라인 아이덴티티의 감시를 가능하게 하는 컴퓨팅 디바이스를 포함하고, 상기 컴퓨팅 디바이스는, 클라이언트 컴퓨팅 디바이스로부터 온라인 서비스에 대한 액세스를 위한 요청을 수신하기 위한 수단과; 상기 게이트웨이 서버의 프로파일 데이터베이스로부터 상기 온라인 서비스에 대한 액세스 정보를 검색하기 위한 수단과; 상기 액세스 정보를 사용하여 상기 클라이언트 컴퓨팅 디바이스의 사용자에 대하여 상기 온라인 서비스에 대한 액세스를 가능하게 하기 위한 수단 - 상기 액세스 정보는 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스가능하지 않음 - 과; 상기 게이트웨이 서버의 정책 데이터베이스 내에 저장된 정책 규칙 세트에 기초하여 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하기 위한 수단을 포함한다.

[0119] 예시 62는 예시 61의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 위한 요청을 수신하기 위한 수단은 상기 게이트웨이 서버의 데이터베이스로부터 이용가능한 허가된 온라인 서비스에 관한 식별 데이터를 검색하기 위한 수단과; 상기 이용가능한 허가된 온라인 서비스의 식별 데이터를 상기 클라이언트 컴퓨팅 디바이스로 송신하기 위한 수단과; 상기 클라이언트 컴퓨팅 디바이스로부터 상기 이용가능한 허가된 온라인 서비스 중 하나에 관한 선택을 수신하기 위한 수단을 포함한다.

[0120] 예시 63은 예시 61 및 예시 62의 요지를 포함하고, 상기 액세스 정보를 검색하기 위한 수단은 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 온라인 서비스에 로그인하도록 상기 게이트웨이 서버에 의해 사용가능한 로그인 정보를 경색하기 위한 수단을 포함한다.

[0121] 예시 64는 예시 61 내지 예시 63 중 임의의 예시의 요지를 포함하고, 상기 로그인 정보는 상기 클라이언트 컴퓨팅 디바이스의 사용자가 상기 온라인 서비스에 로그인하는데 사용가능한 사용자이름 또는 패스워드 중 적어도 하나를 포함한다.

[0122] 예시 65는 예시 61 내지 예시 64 중 임의의 예시의 요지를 포함하고, 상기 사용자이름 또는 상기 패스워드 중 적어도 하나는 상기 게이트웨이 서버에 의해 이전에 무작위로 생성된다.

[0123] 예시 66은 예시 61 내지 예시 65 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 가능하게 하기 위한 수단은 상기 액세스 정보를 사용하여 상기 온라인 서비스에 상기 클라이언트 컴퓨팅 디바이스의 사용자를 로깅하면서 상기 액세스 정보를 상기 클라이언트 컴퓨팅 디바이스로부터 비밀로 유지하기 위한 수단을 포함한다.

[0124] 예시 67은 예시 61 내지 예시 66 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 가능하게 하기 위한 수단은 상기 액세스 정보에 기초하여 로그인 인증서를 생성하기 위한 수단을 포함하고, 상기 로그인 인증서는 상기 온라인 서비스에 로그인하도록 상기 클라이언트 컴퓨팅 디바이스에 의해 사용가능하다.

[0125] 예시 68은 예시 61 내지 예시 67 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 대한 액세스를 가능하게 하기 위한 수단은 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 네트워크 통신을 가능하게 하기 위한 수단을 포함한다.

[0126] 예시 69는 예시 61 내지 예시 68 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하기 위한 수단은 상기 게이트웨이 서버의 액세스 제어 정책에 따라 상기 클라이언트 컴퓨팅 디바이스에 의한 상기 온라인 서비스에 대한 액세스를 제어하기 위한 수단을 포함한다.

[0127] 예시 70은 예시 61 내지 예시 69 중 임의의 예시의 요지를 포함하고, 상기 액세스 제어 정책은, (ⅰ) 상기 클라이언트 컴퓨팅 디바이스가 상기 온라인 서비스에 액세스할 수 있는 기간 또는 (ii) 상기 클라이언트 컴퓨팅 디바이스가 상기 온라인 서비스에 액세스할 수 있는 시간 중 적어도 하나를 정의한다.

[0128] 예시 71은 예시 61 내지 예시 70 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하기 위한 수단은 상기 게이트웨이 서버의 프로파일 공개 정책에 기초하여 상기 온라인 서비스로의 상기 클라이언트 디바이스의 사용자에 관한 아이덴티티 프로파일 정보의 공개를 제어하기 위한 수단을 포함한다.

[0129] 예시 72는 예시 61 내지 예시 71 중 임의의 예시의 요지를 포함하고, 상기 아이덴티티 프로파일 정보의 공개를 제어하기 위한 수단은 상기 온라인 서비스로부터 수신된 아이덴티티 프로파일 정보에 대한 요청을 차단하기 위한 수단을 포함한다.

[0130] 예시 73은 예시 61 내지 예시 72 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하기 위한 수단은 상기 게이트웨이 서버의 구매 거래 정책에 기초하여 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 온라인 결제 거래를 제어하기 위한 수단을 포함한다.

[0131] 예시 74는 예시 61 내지 예시 73 중 임의의 예시의 요지를 포함하고, 상기 온라인 결제 거래를 제어하기 위한 수단은 상기 구매 거래 정책에 정의된 임계 통화량보다 더 큰 상기 온라인 결제 거래의 통화량에 응답하여 상기 온라인 결제 거래를 차단하기 위한 수단을 포함한다.

[0132] 예시 75는 예시 61 내지 예시 74 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하기 위한 수단은 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 표시하는 데이터 로그를 생성하기 위한 수단을 포함한다.

[0133] 예시 76은 예시 61 내지 예시 75 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하기 위한 수단은 상기 게이트웨이 서버의 콘텐츠 정책에 기초하여 온라인 서비스에 의해 전달된 콘텐츠를 제어하기 위한 수단을 포함한다.

[0134] 예시 77은 예시 61 내지 예시 76 중 임의의 예시의 요지를 포함하고, 상기 온라인 서비스에 의해 전달된 콘텐츠를 제어하기 위한 수단은 상기 콘텐츠 정책에서 식별된 참조 콘텐츠와 관련 있는 콘텐츠에 응답하여 상기 클라이언트 컴퓨팅 디바이스에 의한 상기 콘텐츠에 대한 액세스를 차단하기 위한 수단을 포함한다.

[0135] 예시 78은 예시 61 내지 예시 77 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동을 제어하기 위한 수단은 경고 이벤트의 발생을 위해 상기 활동을 모니터링하는 수단

및 상기 경고 이벤트의 발생에 응답하여 경고를 생성하기 위한 수단을 포함한다.

[0136] 예시 79는 예시 61 내지 예시 78 중 임의의 예시의 요지를 포함하고, 상기 경고 이벤트는, (ⅰ) 상기 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티 프로파일 정보에 대한 상기 온라인 서비스에 의한 요청, (ii) 구매 거래의 개시, 또는 (iii) 콘텐츠 정책에 기초하여 수락가능하지 않는 것으로 식별된 상기 온라인 서비스에 의한 콘텐츠의 전달 중 적어도 하나를 포함한다.

[0137] 예시 80은 예시 61 내지 예시 79 중 임의의 예시의 요지를 포함하고, 상기 경고 이벤트를 차단하기 위한 수단을 더 포함한다.

[0138] 예시 81은 예시 61 내지 예시 80 중 임의의 예시의 요지를 포함하고, 상기 경고를 생성하기 위한 수단은 다른 컴퓨팅 디바이스의 사용자에게 상기 경고 이벤트의 발생을 알리는 통지를 상기 다른 클라이언트 컴퓨팅 디바이스에 송신하기 위한 수단을 포함한다.

[0139] 예시 82는 예시 61 내지 예시 81 중 임의의 예시의 요지를 포함하고, 상기 통지를 송신하는 것에 응답하여 상기 다른 컴퓨팅 디바이스로부터 상기 경고 이벤트에 대한 허가를 수신하기 위한 수단과; 상기 경고 이벤트가 상기 허가의 수신에 응답하여 발생하도록 허용하는 수단을 포함한다.

[0140] 예시 83은 예시 61 내지 예시 82 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스로부터, 상기 게이트웨이 서버를 사용하여 새로운 온라인 서비스에 등록하라는 요청을 수신하기 위한 수단과; 상기 새로운 온라인 서비스를 식별하는 식별 데이터를 수신하기 위한 수단과; 상기 새로운 온라인 서비스에 액세스하는 새로운 액세스 정보를 생성하기 위한 수단과; 상기 새로운 액세스 정보가 상기 클라이언트 컴퓨팅 디바이스의 사용자에 의해 액세스가능하지 않도록 상기 게이트웨이 서버 상에 상기 새로운 액세스 정보를 저장하기 위한 수단을 포함한다.

[0141] 예시 84는 예시 61 내지 예시 83 중 임의의 예시의 요지를 포함하고, 새로운 액세스 정보를 생성하기 위한 수단은 상기 새로운 온라인 서비스에 액세스하는데 사용가능한 패스워드를 무작위로 생성하기 위한 수단을 포함한다.

[0142] 예시 85는 예시 61 내지 예시 84 중 임의의 예시의 요지를 포함하고, 새로운 액세스 정보를 생성하기 위한 수단은 상기 패스워드와 연관된 사용자이름을 무작위로 생성하기 위한 수단을 포함한다.

[0143] 예시 86은 예시 61 내지 예시 85 중 임의의 예시의 요지를 포함하고, 상기 새로운 액세스 정보를 사용하여 상기 새로운 온라인 서비스에 상기 클라이언트 컴퓨팅 디바이스의 사용자를 등록하기 위한 수단을 더 포함한다.

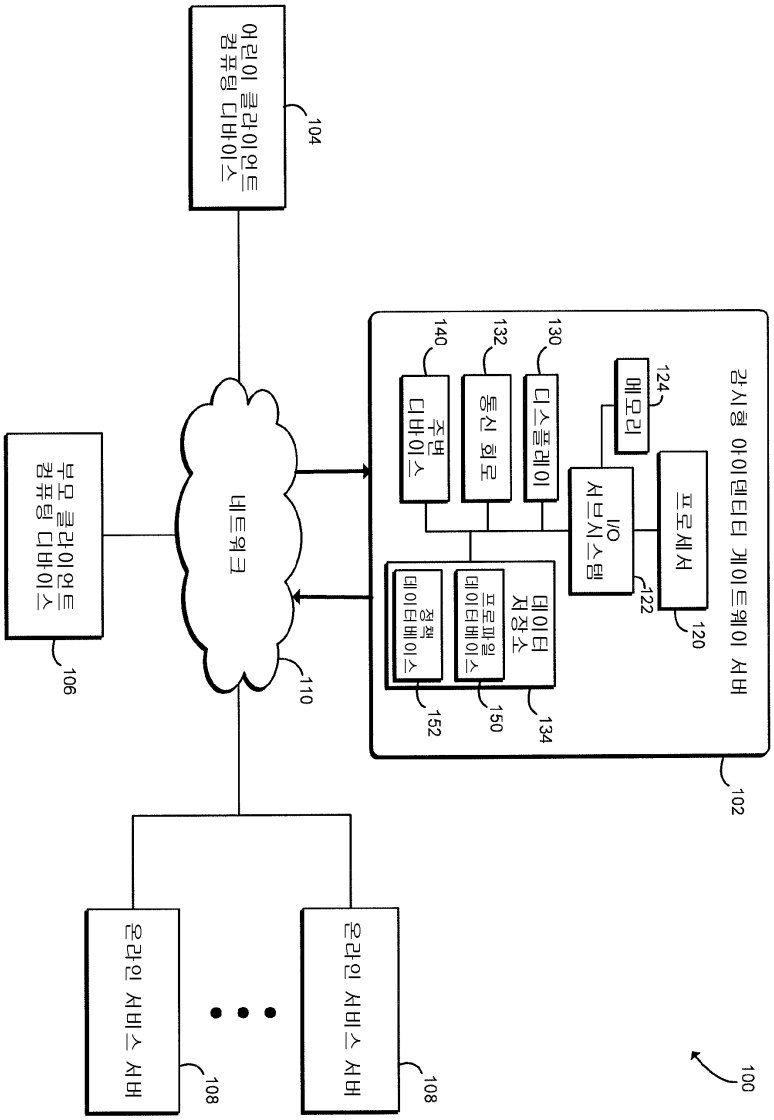
[0144] 예시 87은 예시 61 내지 예시 86 중 임의의 예시의 요지를 포함하고, 상기 게이트웨이 서버에 의해 유지되는 정책 데이터베이스의 정책 규칙 및 상기 식별 데이터에 기초하여 상기 새로운 온라인 서비스가 허가되는지 여부를 결정하기 위한 수단을 더 포함한다.

[0145] 예시 88은 예시 61 내지 예시 87 중 임의의 예시의 요지를 포함하고, 다른 클라이언트 컴퓨팅 디바이스로부터 관리 액세스 요청을 수신하기 위한 수단과; 상기 다른 클라이언트 컴퓨팅 디바이스의 사용자의 아이덴티티를 검증하기 위한 수단과; 상기 다른 클라이언트 컴퓨팅 디바이스로부터 수신된 데이터에 기초하여 상기 정책 데이터베이스에 저장된 정책 규칙 세트를 업데이트하기 위한 수단을 더 포함한다.

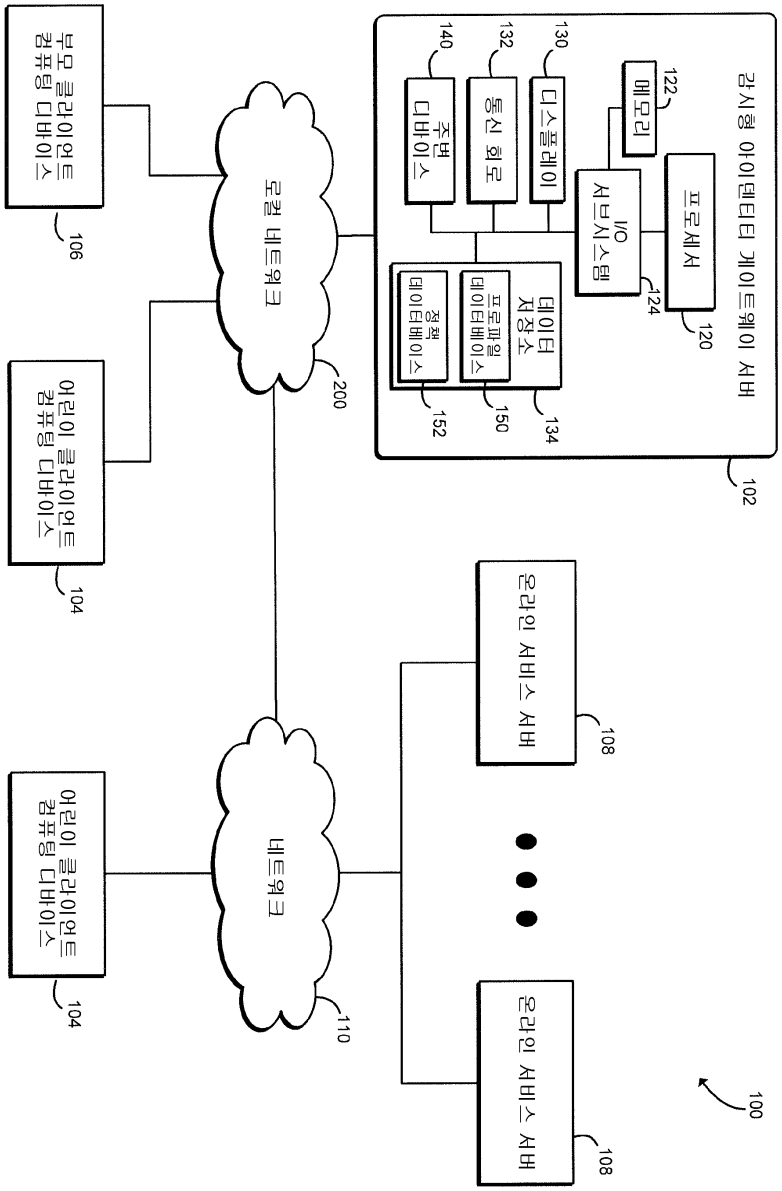
[0146] 예시 89는 예시 61 내지 예시 88 중 임의의 예시의 요지를 포함하고, 상기 클라이언트 컴퓨팅 디바이스와 상기 온라인 서비스 사이의 활동에 관한 활동 로그에 대한 요청을 수신하기 위한 수단과; 상기 활동 로그를 상기 다른 클라이언트 컴퓨팅 디바이스로 송신하기 위한 수단을 더 포함한다.

도면

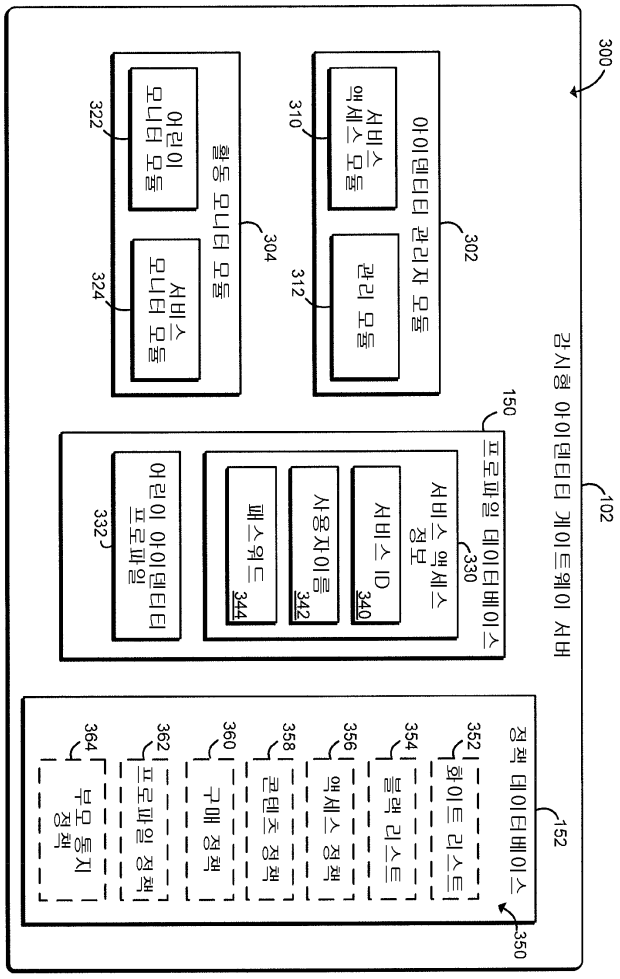
도면1


어린이 클라이언트 컴퓨팅 디바이스
104
부모 클라이언트 컴퓨팅 디바이스
106
네트워크
110
감시형 아이덴티티 게이트웨이 서버
102
주변 디바이스
140
통신 회로
132
디스플레이
130
메모리
124
I/O 서브시스템
122
프로세서
120
데이터 저장소
134
프로파일 데이터베이스
150
정책 데이터베이스
152
온라인 서비스 서버
108
온라인 서비스 서버
108
100

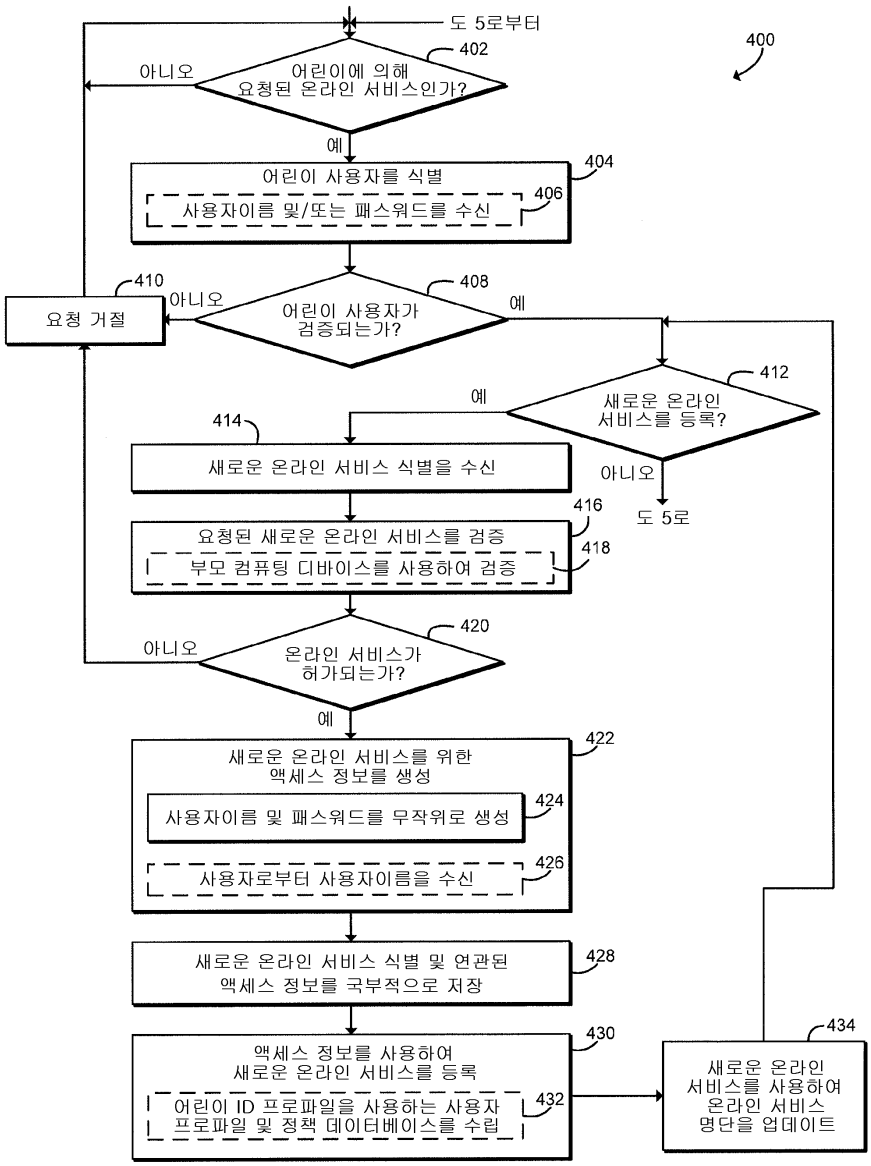
도면2


감시형 아이덴티티 게이트웨이 서버
102
프로세서
120
메모리
122
I/O 서브시스템
124
디스플레이
130
통신 회로
132
주변 디바이스
140
데이터 저장소
134
프로파일 데이터베이스
150
정책 데이터베이스
152
로컬 네트워크
200
부모 클라이언트 컴퓨팅 디바이스
106
어린이 클라이언트 컴퓨팅 디바이스
104
어린이 클라이언트 컴퓨팅 디바이스
104
네트워크
110
온라인 서비스 서버
108
온라인 서비스 서버
108
100

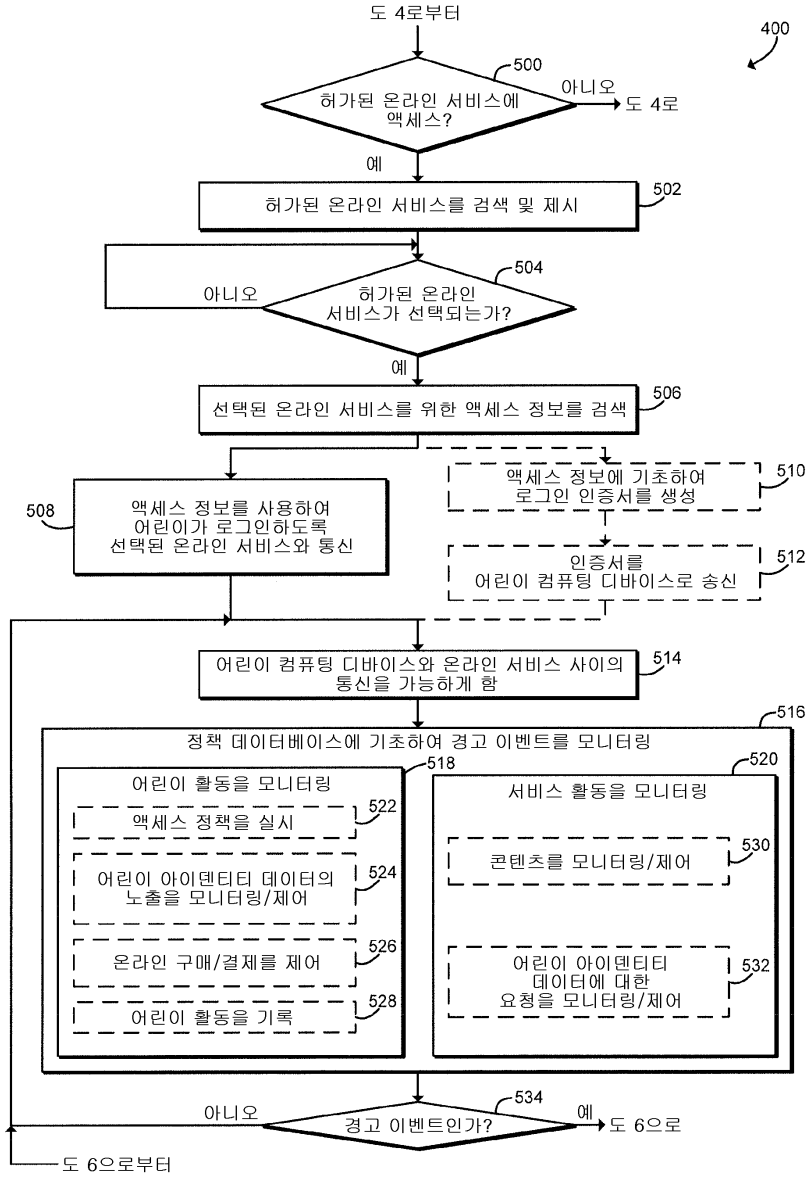
도면3


300
감시형 아이덴티티 게이트웨이 서버
102
아이덴티티 관리자 모듈
302
서비스 액세스 모듈
310
관리 모듈
312
활동 모니터 모듈
304
어린이 모니터 모듈
322
서비스 모니터 모듈
324
프로파일 데이터베이스
150
서비스 액세스 정보
330
서비스 ID
340
사용자이름
342
패스워드
344
어린이 아이덴티티 프로파일
332
정책 데이터베이스
152
350
화이트 리스트
352
블랙 리스트
354
액세스 정책
356
콘텐츠 정책
358
구매 정책
360
프로파일 정책
362
부모 통지 정책
364

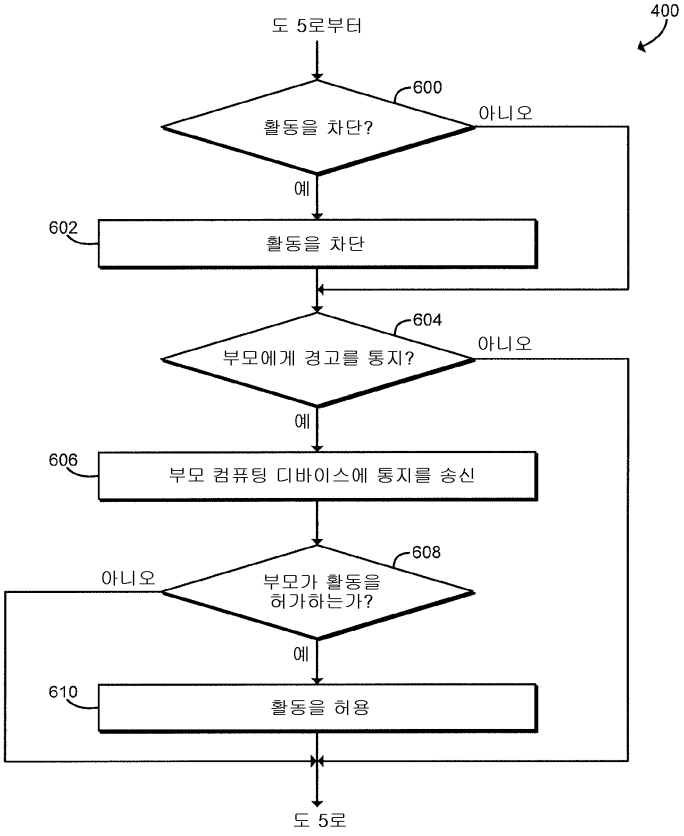
도면4


도 5로부터
400
402
어린이에 의해 요청된 온라인 서비스인가?
아니오
예
404
어린이 사용자를 식별
406
사용자이름 및/또는 패스워드를 수신
408
어린이 사용자가 검증되는가?
410
요청 거절
아니오
예
412
새로운 온라인 서비스를 등록?
예
414
새로운 온라인 서비스 식별을 수신
아니오
도 5로
416
요청된 새로운 온라인 서비스를 검증
418
부모 컴퓨팅 디바이스를 사용하여 검증
420
온라인 서비스가 허가되는가?
아니오
예
422
새로운 온라인 서비스를 위한 액세스 정보를 생성
424
사용자이름 및 패스워드를 무작위로 생성
426
사용자로부터 사용자이름을 수신
428
새로운 온라인 서비스 식별 및 연관된 액세스 정보를 국부적으로 저장
430
액세스 정보를 사용하여 새로운 온라인 서비스를 등록
432
어린이 ID 프로파일을 사용하는 사용자 프로파일 및 정책 데이터베이스를 수립
434
새로운 온라인 서비스를 사용하여 온라인 서비스 명단을 업데이트

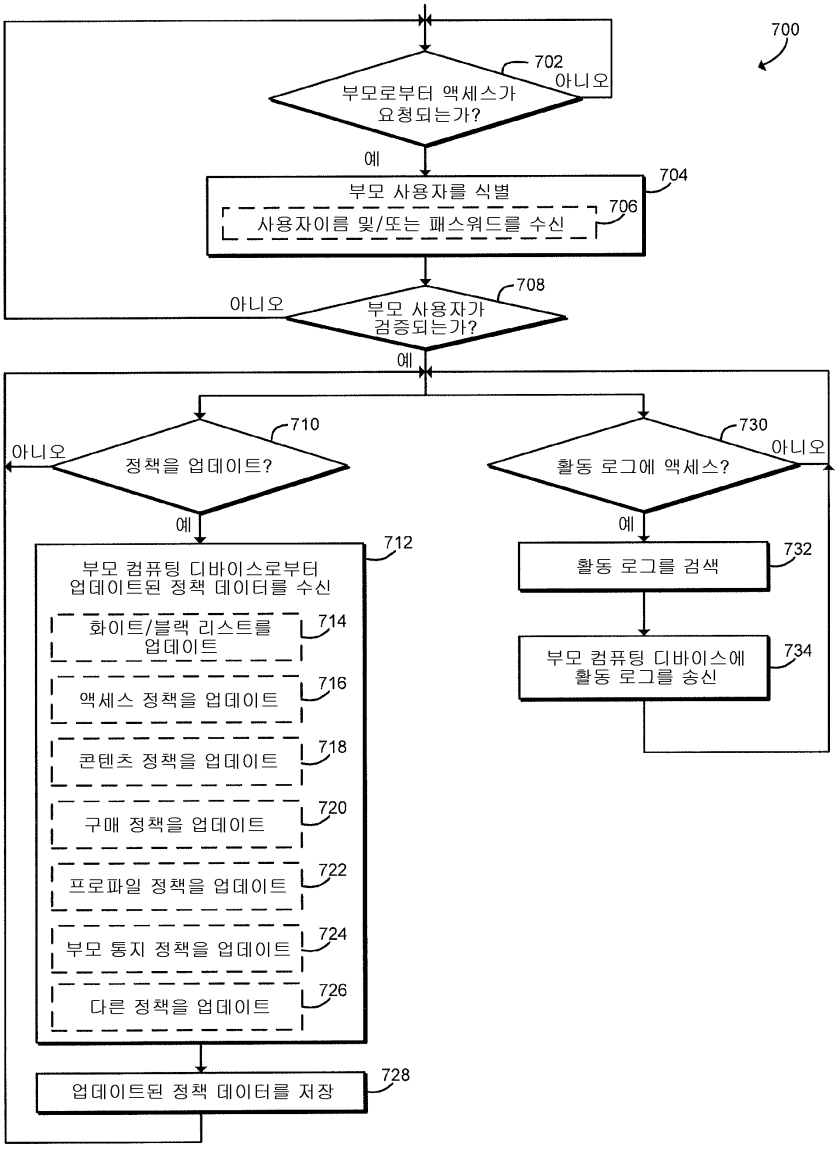
도면5


도 4로부터
400
500
허가된 온라인 서비스에 액세스?
아니오
도 4로
예
502
허가된 온라인 서비스를 검색 및 제시
504
아니오
허가된 온라인 서비스가 선택되는가?
예
506
선택된 온라인 서비스를 위한 액세스 정보를 검색
508
액세스 정보를 사용하여 어린이가 로그인하도록 선택된 온라인 서비스와 통신
510
액세스 정보에 기초하여 로그인 인증서를 생성
512
인증서를 어린이 컴퓨팅 디바이스로 송신
514
어린이 컴퓨팅 디바이스와 온라인 서비스 사이의 통신을 가능하게 함
516
정책 데이터베이스에 기초하여 경고 이벤트를 모니터링
518
어린이 활동을 모니터링
522
액세스 정책을 실시
524
어린이 아이덴티티 데이터의 노출을 모니터링/제어
526
온라인 구매/결제를 제어
528
어린이 활동을 기록
520
서비스 활동을 모니터링
530
콘텐츠를 모니터링/제어
532
어린이 아이덴티티 데이터에 대한 요청을 모니터링/제어
534
아니오
경고 이벤트인가?
예
도 6으로
도 6으로부터

도면6


400
도 5로부터
600
활동을 차단?
아니오
예
602
활동을 차단
604
부모에게 경고를 통지?
아니오
예
606
부모 컴퓨팅 디바이스에 통지를 송신
608
아니오
부모가 활동을
허가하는가?
예
610
활동을 허용
도 5로

도면7



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 제10항

【변경전】

상기 클라이언트 컴퓨팅 디바이

【변경후】

클라이언트 컴퓨팅 디바이