(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 12 월 13 일 (13.12.2012)

WIPO | PCT

(10) 국제공개번호
WO 2012/169862 A2

(51) 국제특허분류:
G06F 21/24 (2006.01) *G06F 21/20* (2006.01)

(21) 국제출원번호: PCT/KR2012/004601

(22) 국제출원일: 2012 년 6 월 11 일 (11.06.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0055544 2011 년 6 월 9 일 (09.06.2011) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **삼성전자 주식회사 (SAMSUNG ELECTRONICS CO., LTD.)** [KR/KR]; 경기도 수원시 영통구 삼성로 129, 443-742 Gyeonggi-do (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **김은아 (KIM, Eun Ah)** [KR/KR]; 경기도 용인시 기흥구 삼성 2 로 97 삼성종합기술원 내, 446-712 Gyeonggi-do (KR). **김대엽 (KIM, Dae Youb)** [KR/KR]; 경기도 용인시 기흥구 삼성 2 로 97 삼성종합기술원 내, 446-712 Gyeonggi-do (KR). **이병준 (LEE, Byoung Joon)** [KR/KR]; 경기도 용인시 기흥구 삼성 2 로 97 삼성종합기술원 내, 446-712 Gyeonggi-do (KR). **허미숙 (HUH, Mi Suk)** [KR/KR]; 경기도 용인시 기흥구 삼성 2 로 97 삼성종합기술원 내, 446-712 Gyeonggi-do (KR).

(74) 대리인: **특허법인 무한 (MUHANN PATENT & LAW FIRM)**; 서울시 강남구 논현동 51-8 명림빌딩 2, 5, 6 층, 135-814 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

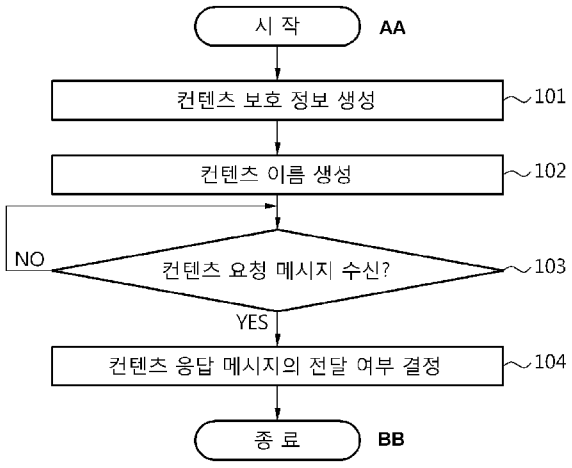
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC,

[다음 쪽 계속]

(54) **Title**: CONTENT NAME-BASED NETWORK DEVICE AND METHOD FOR PROTECTING CONTENT

(54) **발명의 명칭** : 컨텐츠 이름 기반의 네트워크 장치 및 컨텐츠 보호 방법

[Fig. 1]



AA ... start
BB ... end
101 ... generate content protection information
102 ... generate content name
103 ... Has the content request message been received?
104 ... decide whether to forward content response message

(57) **Abstract**: Disclosed is a method for protecting content in content name-based networking. The method for protecting content generates content protection information on contents which a contents generator wishes to protect; and generates a name for the contents, which indicates the location of the contents in a content name-based network, on the basis of the content protection information. At this stage, the content protection information comprises at least one of: marking information which indicates whether the contents are protected; and policy information which indicates the scope of the disclosure of the contents.

(57) **요약서**: 컨텐츠 이름 기반의 네트워킹에서 컨텐츠 보호 방법이 개시된다. 컨텐츠 보호 방법은, 컨텐츠 생성자가 보호하고자 하는 컨텐츠에 대한 컨텐츠 보호 정보를 생성하고, 컨텐츠 보호 정보에 기초하여 컨텐츠 이름 기반의 네트워크에서 컨텐츠의 위치를 나타내는 컨텐츠 이름을 생성할 수 있다. 여기서, 컨텐츠 보호 정보는, 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함할 수 있다.

WO 2012/169862 A2

MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

명세서

발명의 명칭: 컨텐츠 이름 기반의 네트워크 장치 및 컨텐츠 보호 방법

기술분야

[1] 아래의 설명은 컨텐츠 중심 네트워크(Content Centric Network) 또는 정보 중심 네트워크(Information Centric Network)에서 컨텐츠 및 컨텐츠와 관련된 정보를 보호하는 기술에 관한 것이다.

배경기술

[2] 컨텐츠 중심 네트워크(Contents Centric Network)에서의 데이터 통신(예를 들어, 컨텐츠 전송)은 컨텐츠의 이름에 기반하여 이루어 진다. 인터넷 프로토콜(Internet Protocol: IP) 기반 네트워크에서 IP 주소를 이용하여 통신 대상(host)을 찾아가는 것과는 달리, 컨텐츠 중심 네트워크에서는 컨텐츠 이름을 이용하여 컨텐츠를 찾아간다. 이하에서, 컨텐츠는 네트워크에서 전송되는 데이터 또는 정보를 포함할 수 있다.

[3] 컨텐츠 중심 네트워킹(Content Centric Networking: CCN) 방법은 다음과 같다. 먼저, 임의의 네트워크 장치는 원하는 컨텐츠의 이름을 포함하는 요청 메시지를 이웃 네트워크 장치들로 전송할 수 있다. 그리고, 요청 메시지를 수신한 이웃 네트워크 장치들 중 요청 메시지에 명시된 컨텐츠를 저장하고 있는 네트워크 장치는 해당 컨텐츠를 포함하는 응답 메시지를 요청 메시지를 송신한 네트워크 장치로 전송할 수 있다.

[4] 이처럼, 컨텐츠 중심 네트워킹은 요청과 응답의 형태를 나타낸다. 즉, 컨텐츠 중심 네트워킹은 송신자가 통신을 시작, 제어하는 구조가 아닌, 수신자가 통신을 시작하는 구조 (receiver based communication)를 나타낸다. 이러한 수신자가 통신을 시작하는 구조 아래에서는, 컨텐츠를 저장하고 있는 네트워크 장치나 컨텐츠 생성자(content source or publisher)의 의도와 상관 없이 컨텐츠가 다른 네트워크 장치의 요청에 의하여 전송될 수 있다. 예를 들어, 특정 네트워크 도메인(domain) 내부에서만 공유되어야 할 컨텐츠가 도메인 외부의 네트워크 장치의 요청에 의하여 외부로 전송될 수 있다. 단, 컨텐츠의 암호화 기술을 이용하여 접근 권한이 없는 수신자가 컨텐츠 내용(content object)을 식별하지 못하도록 할 수는 있으나, 컨텐츠의 전송을 방지할 수는 없다.

[5] 또한, 컨텐츠 이름을 이용하여 컨텐츠 요청 메시지를 전송하고, 이에 대응하는 응답 메시지를 수신하는 방식으로, 컨텐츠 이름, 컨텐츠가 생성된 네트워크 도메인에 대한 정보, 및 컨텐츠 소유자에 대한 정보 등을 식별할 수 있다. 이러한 방식은 컨텐츠 및 컨텐츠와 관련된 정보의 유출 문제, 및 컨텐츠 생성자에 대한 프라이버시 침해 문제를 발생시킬 수 있다.

[6] 따라서, 컨텐츠 중심 네트워크에서 컨텐츠에 대한 접근 권한이 없는 네트워크

장치 또는 사용자에게 컨텐츠 내용(content object) 뿐만 아니라, 컨텐츠 이름, 네트워크의 도메인 이름 등의 컨텐츠 관련 정보가 유출되지 않도록 컨텐츠를 보호하는 기술이 필요하다.

발명의 상세한 설명

과제 해결 수단

[7] 일실시예에 따른 컨텐츠 보호 방법은 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함하는 컨텐츠 보호 정보를 생성하는 단계; 및 상기 컨텐츠 보호 정보에 기초하여 컨텐츠 이름 기반의 네트워크에서 컨텐츠의 위치를 나타내는 컨텐츠 이름을 생성하는 단계를 포함할 수 있다.

[8] 일실시예에 따른 컨텐츠 보호 방법은 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신하는 단계; 및 컨텐츠 보호 정보에 기초하여 상기 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계를 더 포함할 수 있다.

[9] 또한, 일실에에 따른 상기 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계는 상기 컨텐츠 요청 메시지가 가리키는 컨텐츠의 저장 여부를 확인하는 단계; 및 상기 컨텐츠가 저장된 것으로 확인됨에 따라, 상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠를 포함하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계를 포함할 수 있다.

[10] 또한, 일실에에 따른 상기 컨텐츠를 포함하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계는 상기 마킹 정보에 기초하여 상기 컨텐츠가 접근 보호가 설정된 컨텐츠인지 여부를 확인하는 단계; 및 상기 컨텐츠에 대한 접근 보호가 확인됨에 따라, 상기 정책 정보에 기초하여 상기 컨텐츠 응답 메시지를 전달할 다음 네트워크 장치가 상기 공개 범위 내에 포함되는지 여부를 확인하는 단계를 포함할 수 있다.

[11] 일실시에에 따른 네트워크 장치는 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함하는 컨텐츠 보호 정보를 생성하는 컨텐츠 보호 정보 생성부; 및 상기 컨텐츠 보호 정보에 기초하여 컨텐츠 이름 기반의 네트워크에서 컨텐츠의 위치를 나타내는 컨텐츠 이름을 생성하는 컨텐츠 이름 생성부를 포함할 수 있다.

[12] 일실시에에 따른 네트워크 장치는 상기 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신하는 메시지 수신부; 및 상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 결정부를 더 포함할 수 있다.

[13] 또한, 일실에에 따른 상기 결정부는 상기 컨텐츠 요청 메시지가 가리키는 컨텐츠의 저장 여부를 확인하는 확인부; 및 상기 컨텐츠가 저장된 것으로 확인됨에 따라, 상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠를 포함하는

컨텐츠 응답 메시지의 전달 여부를 결정하는 전달 결정부를 포함할 수 있다.

[14] 다른 실시예에 따른 컨텐츠 보호 방법은 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신하는 단계; 및 컨텐츠 보호 정보에 기초하여 설정된 태그 정보를 이용하여 상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계를 포함할 수 있고, 상기 컨텐츠 보호 정보는, 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함할 수 있다.

[15] 또한, 다른 실시예에 따른 상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계는 상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계는, 상기 컨텐츠 요청 메시지가 가리키는 컨텐츠의 저장 여부를 확인하는 단계; 및 상기 컨텐츠가 저장되지 않은 것으로 확인됨에 따라, 상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계를 포함할 수 있다.

[16] 다른 실시예에 따른 네트워크 장치는 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신하는 메시지 수신부; 및 컨텐츠 보호 정보에 기초하여 설정된 태그 정보를 이용하여 상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 결정부를 포함할 수 있고, 상기 컨텐츠 보호 정보는, 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함할 수 있다.

[17] 또한, 다른 실시예에 따른 상기 결정부는 상기 컨텐츠 요청 메시지가 가리키는 컨텐츠의 저장 여부를 확인하는 확인부; 및 상기 컨텐츠가 저장되지 않은 것으로 확인됨에 따라, 상기 컨텐츠 보호 정보와 전달 정보 베이스(Forwarding Information Base: FIB)에 기록되어 있는 정책 정보에 기초하여 상기 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달할지 여부를 결정하는 전달 결정부를 포함할 수 있다.

[18] 다른 실시예에 따른 컨텐츠 보호 방법은 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함하는 컨텐츠 보호 정보를 생성하는 단계; 및 상기 컨텐츠 보호 정보에 기초하여 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계를 포함할 수 있다.

도면의 간단한 설명

[19] 도 1은 컨텐츠를 생성한 네트워크 장치에서 컨텐츠를 보호하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[20] 도 2는 컨텐츠를 저장하고 있는 네트워크 장치에서 컨텐츠를 보호하기 위해 컨텐츠 응답 메시지를 전달할지 여부를 결정하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[21] 도 3은 네트워크 장치에서 컨텐츠 응답 메시지의 전송을 제어하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[22] 도 4는 네트워크 장치에서 컨텐츠 요청 메시지의 전송을 제어하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[23] 도 5는 네트워크 장치의 세부 구성을 도시한 블록 다이어그램이다.

[24] 도 6은 네트워크 장치에서 컨텐츠 요청 메시지를 중계하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[25] 도 7은 컨텐츠 요청 메시지를 중계하는 네트워크 장치의 세부 구성을 도시한 블록 다이어그램이다.

발명의 실시를 위한 형태

[26] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다. 본 컨텐츠 보호 방법은 네트워크 장치에 의해 수행될 수 있다.

[27] 도 1은 컨텐츠를 생성한 네트워크 장치에서 컨텐츠를 보호하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[28] 도 1에 따르면, 101 단계에서, 네트워크 장치는, 컨텐츠를 생성하면서 컨텐츠 보호 정보를 함께 생성할 수 있다. 여기서, 컨텐츠 보호 정보는, 다른 네트워크 장치에게 컨텐츠에 대한 접근을 허용 할지 여부에 관한 정책이 컨텐츠 이름에 포함되어 있음을 나타내는 마킹 정보(marking information), 및 컨텐츠가 전달될 수 있는 공개 범위를 나타내는 정책 정보(policy information)를 포함할 수 있다. 여기서, 다른 네트워크 장치에는, 동일한 네트워크 도메인(network domain)에 속하는 네트워크 장치, 동일한 네트워크 도메인에 속하지 않는 외부 네트워크 장치, 또는 인터넷을 통해 연결된 네트워크 장치 등이 포함될 수 있다.

[29] 이때, 네트워크 장치는, 문자 코드 또는 숫자 코드 등의 형태로 마킹 정보를 생성할 수 있다. 마킹 정보는 태그(tag)로서 컨텐츠 보호 여부를 표시할 수 있다. 그리고, 네트워크 장치는 문자 코드, 숫자 코드, 오프셋(offset), 또는 리스트(list) 등의 형태로 정책 정보를 생성할 수 있다. 또는 네트워크 장치는 문자 코드, 숫자 코드, 오프셋, 또는 리스트가 혼합된 형태로 정책 정보를 생성할 수도 있다.

[30] 102 단계에서, 네트워크 장치는, 컨텐츠 보호 정보에 기초하여 컨텐츠 이름을 생성할 수 있다.

[31] 컨텐츠 이름은 컨텐츠 중심 네트워크에서 해당 컨텐츠를 식별할 수 있는 유일한 식별자가 될 수 있다. 또한, 컨텐츠 이름은, 복수의 컴포넌트(component)로 구성될 수 있고, 계층 구조를 가질 수도 있다. 예를 들어, AAA회사의 BBB조직에서 news.jpg 라는 컨텐츠를 생성한 경우, /AAA.com/BBB/news.jpg와 같은 컨텐츠 이름이 생성될 수 있고, 위 컨텐츠 이름은 3개의 컴포넌트로 구성될 수 있다.

[32] 또한, 컨텐츠 이름은, 컨텐츠와 관련된 정보(예를 들어, 컨텐츠가 생성되었거나 저장되어 있는 네트워크 도메인)의 이름을 나타내거나 컨텐츠의 고유 이름, 컨텐츠의 버전(version) 정보, 컨텐츠의 세그먼트(segment) 번호, 및 컨텐츠 보호 정보 중 적어도 하나를 포함할 수 있다. 각 컴포넌트에는 컨텐츠와 관련된

정보의 이름, 컨텐츠 고유 이름, 버전 정보, 세그먼트 번호, 컨텐츠 보호 정보가 위치할 수 있다. 예를 들어, 컨텐츠 이름은 계층적 네트워크 도메인 구조를 표현하거나 계층적 네트워크 도메인에 속한 컨텐츠를 나타낼 수 있다.

[33] 이때, 네트워크 장치는, 복수의 컴포넌트들 중 어느 하나의 컴포넌트에 컨텐츠 보호 정보가 포함되도록 컨텐츠 이름을 생성할 수 있다.

[34] 네트워크 장치는 컨텐츠 보호 정책에 따라 컨텐츠 보호 정보를 컨텐츠 이름 내 임의의 위치에 위치시킬 수 있다. 예를 들어, 네트워크 장치는 네트워크 도메인 컴포넌트와 네트워크 도메인 컴포넌트 사이에 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다. 또는, 네트워크 장치는 네트워크 도메인 컴포넌트와 컨텐츠 고유 이름 컴포넌트 사이에 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다. 그리고, 네트워크 장치는 컨텐츠 고유 이름 컴포넌트와 컨텐츠 버전 정보 컴포넌트 사이에 위치하도록 컨텐츠 이름을 생성할 수도 있다.

[35] 이 때, 컨텐츠 보호 정보는 컨텐츠 응답 메시지에서 생성하는 전자 서명이 적용되는 범위 내에 위치할 수 있다.

[36] 또한, 네트워크 장치는, 컨텐츠 보호 정보를 컨텐츠 이름 내 임의의 위치에 포함되도록 컨텐츠 이름을 생성할 수 있다. 이 때, 컨텐츠 보호 정보는 컨텐츠 응답 메시지에서 생성하는 전자 서명이 적용되는 컨텐츠 이름 범위 내에 위치할 수 있다. 또한, 컨텐츠 이름 내 컨텐츠 보호 정보의 위치에 따라 보호 대상이 달라질 수 있다. 일례로, 특정 네트워크 도메인 및 도메인에 속하는 컨텐츠 이름에 대하여 다른 네트워크 장치의 접근을 허용하지 않은 경우, 네트워크 장치는 아래의 표 1과 같이, 보호하고자 하는 네트워크 도메인의 이름 컴포넌트 이후에 연속하여 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다.

[37] 【표 1】

컨텐츠 이름		
도메인 이름	컨텐츠 보호 정보	컨텐츠 파일 이름 (optional)
/AAA.xxx/BBB/CCC/DDD	/Security_info (=marking info.+policy info.)	/EEE.zzz

[38] 표 1에 따르면, 네트워크 장치는 보호하고자 하는 도메인 이름, 또는 이를 포함하는 컨텐츠 이름에 대한 요청 메시지를 수신한 경우, 컨텐츠 보호 정보에 기초하여 도메인 이름을 다른 네트워크 장치로 전송하지 않을 수 있다. 예를 들어, 컨텐츠 중심 네트워킹(CCN)에서, 요청 메시지는

인터레스트(INTEREST)로 표현될 수 있다.

[39] 표 1에 따라 네트워크 장치가 /AAA.xxx/BBB/CCC/DDD 이름을 갖는 네트워크 도메인 또는 /AAA.xxx/BBB/CCC/DDD/EEE/zzz 이름을 갖는 컨텐츠를 요청하는 인터레스트를 수신한 경우, 네트워크 장치는 도메인 이름 /AAA.xxx/BBB/CCC/DDD 이름 이후에 컨텐츠 보호 정보가 위치하는 것을 식별할 수 있다. 이에 따라, 네트워크 장치는 컨텐츠 보호 정보에 기초하여 도메인 이름 또는 컨텐츠를 다른 네트워크 장치로 전송하지 않을 수 있다. 이때, 네트워크 장치는, 도메인 이름 별로 컨텐츠 보호 정보를 생성할 수도 있다. 예를 들어, 네트워크 장치는 도메인 BBB에 대한 컨텐츠 보호 정보, 도메인 CCC에 대한 컨텐츠 보호 정보, 도메인 DDD에 대한 컨텐츠 보호 정보를 각각 생성할 수도 있다.

[40] 표 1에 따르면, 컨텐츠 이름 및 네트워크 도메인 이름을 구성하는 복수의 컴포넌트들은, 슬래시(/) 마다 하나의 컴포넌트로 구분될 수 있다. 예를 들어, /AAA.xxx/BBB/CCC/DDD/Security_info로 구성된 경우, AAA.xxx는 컴포넌트 1, BBB는 컴포넌트 2, CCC는 컴포넌트 3, DDD는 컴포넌트 4, Security_info는 컴포넌트 5에 해당할 수 있다. 그러면, 표 1에서, 도메인 이름은 5개의 컴포넌트로 구성될 수 있다.

[41] 다른 예로, 특정 컨텐츠 이름을 가진 컨텐츠에 대하여 다른 네트워크 장치의 접근을 허용하지 않은 경우, 네트워크 장치는, 아래의 표 2와 같이, 보호하고자 하는 컨텐츠 파일 이름 컴포넌트 이후에 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다.

[42] **【표 2】**

[43]

컨텐츠 이름				
도메인 이름	컨텐츠 파일 이름	버전 정보	컨텐츠 보호 정보	세그먼트 번호
/AAA.xxx/BBB/CCC/DDD	EEE.zz z	Version #	Security_info	Segment #

[44] 표 2에 따르면, 도메인 이름은, 컨텐츠가 저장되어 있거나 생성된 네트워크 도메인을 계층적으로 나타내는 정보일 수 있고, 컨텐츠 파일 이름은, 컨텐츠 생성자가 생성한 컨텐츠 자체의 이름을 나타낼 수 있고, 버전 정보는, 생성한 컨텐츠의 버전을 나타내는 정보일 수 있고, 세그먼트 번호는, 생성한 컨텐츠가 복수개의 세그먼트로 분할됨에 따라, 분할된 세그먼트에서 해당하는 번호를 나타내는 정보일 수 있다.

[45] 그리고, 표 2에 따르면, 네트워크 장치는, 복수의 컴포넌트들 중 컨텐츠에 대한 전자 서명이 적용되는 범위에 해당하는 컴포넌트에 컨텐츠 보호 정보가

위치하도록 컨텐츠 이름을 생성할 수 있다. 예를 들어, 네트워크 장치는, 전자 서명이 적용되는 버전 정보와 세그먼트 정보 사이에 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다.

[46] 이때, 컨텐츠 보호 정보는, 복수의 컴포넌트들 중 전자 서명이 적용되는 범위에 해당하는 어느 하나의 컴포넌트에 위치해도 상관없다. 여기서, 컴포넌트는, 컨텐츠 이름에 포함된 각 정보들을 구분하는 단위로서, 컨텐츠 보호 정보는 하나의 컴포넌트로 구성될 수 있다. 이때, 표 2와 같이, 도메인 이름이 4개의 계층적인 네트워크 도메인의 이름으로 구성된 경우, 도메인 AAA.xxx, 도메인 BBB, 도메인 CCC, 및 도메인 DDD 각각은 하나의 컴포넌트로 구성될 수 있다. 다시 말해, 표 2에서 도메인 이름은 4개의 컴포넌트로 구성될 수 있다. 또한, 컨텐츠 파일 이름, 버전 정보, 세그먼트 번호도 각각 하나의 컴포넌트로 구성될 수 있다. 이때, 네트워크 장치는, 컨텐츠 파일 이름 이후에 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다.

[47] 그리고, 103 단계에서, 네트워크 장치는, 컨텐츠 요청 메시지를 수신할 수 있다. 예를 들어, 네트워크 장치는, 컨텐츠 응답 메시지를 전달할 다음 네트워크 장치로부터 컨텐츠 요청 메시지를 수신할 수 있다. 컨텐츠 응답 메시지를 전달할 다음 네트워크 장치는 상위 네트워크 도메인에 존재하는 네트워크 장치일 수 있다.

[48] 여기서, 컨텐츠 요청 메시지는, 컨텐츠 내용, 컨텐츠 파일 이름, 컨텐츠가 속한 네트워크 도메인 이름, 특정 네트워크 도메인에 속하는 컨텐츠들을 포함하는 컨텐츠 리스트 및 정보, 도메인 구조(domain hierarchy) 정보 중 적어도 하나를 포함할 수 있다. 그리고, 컨텐츠 내용 (object)은, 컨텐츠 생성자가 생성한 파일(file)을 의미하고, 도메인 구조(domain hierarchy) 정보는, 하나 이상의 네트워크 도메인 간의 계층적 연결 관계를 나타내는 정보일 수 있다.

[49] 일례로, 아래의 표 3과 같이, 네트워크 장치는 도메인 DDD 관련 정보를 요청하는 컨텐츠 요청 메시지를 수신할 수 있다.

[50] 【표 3】

컨텐츠 요청 메시지	
컨텐츠 보호 프로토콜 이용	ccns_Interest://AAA.xxx/BBB/CCC/DDD

[51]

컨텐츠 보호 프로토콜 미이용	ccn_Interest://AAA.xxx/BBB/CCC/DDD

[52] 표 3에 따르면, 컨텐츠 요청 메시지는 네트워크 내에서 컨텐츠 보호 프로토콜을 이용하는지 여부를 알리기 위하여, 프로토콜 명시자(indicator)를 두 가지로 사용할 수 있다. 예를 들어, 도메인 DDD의 하위 도메인 리스트 또는 컨텐츠 리스트와 같은 도메인 DDD와 관련 정보의 전송을 요청하는 네트워크 장치가

컨텐츠 보호 프로토콜을 이용함을 알리기 위해, 프로토콜 명시자로 ccns_Interest 형태를 가질 수 있다. 또한, 컨텐츠 요청 메시지는, 네트워크 장치가 컨텐츠 보호 프로토콜을 이용하지 않음을 알리기 위해, ccn_Interest 형태를 가질 수 있다. 다시 말해, http 및 https 프로토콜이 호환되어 사용하는 것과 같이, 네트워크 장치는, ccn 및 ccns 프로토콜을 호환하여 사용할 수 있다. 여기서, 컨텐츠 보호 프로토콜은, 컨텐츠 보호 정보에 기초하여 컨텐츠를 다른 네트워크 장치와 공유하거나, 또는 공유하지 않음을 정의한 규약일 수 있다.

[53] 이어, 104 단계에서, 네트워크 장치는, 컨텐츠 보호 정보에 기초하여 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지의 전달 여부를 결정할 수 있다

[54] 이하에서는 도 2를 참조하여 컨텐츠 응답 메시지의 전달 여부를 결정하는 구성에 대해 상세히 설명하기로 한다.

[55] 도 2는 컨텐츠를 저장하고 있는 네트워크 장치에서 컨텐츠를 보호하기 위해 컨텐츠 응답 메시지를 전달할지 여부를 결정하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[56] 도 2에 따르면, 201 단계에서, 네트워크 장치는, 컨텐츠 요청 메시지를 수신함에 따라 컨텐츠 저장 여부를 확인할 수 있다.

[57] 예를 들어, 네트워크 장치는, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 컨텐츠 스토어(Contents Store: CS)에 저장되어 있는지 여부를 확인할 수 있다. 여기서, 컨텐츠 스토어는, 컨텐츠를 저장하는 캐쉬(cache)일 수 있으며, 네트워크 장치는, 하나 이상의 컨텐츠들이 저장된 데이터 저장부(미도시)를 별도로 구비할 수 있다.

[58] 이어, 컨텐츠 스토어에 컨텐츠가 저장된 것으로 확인된 경우, 네트워크 장치는, 저장된 컨텐츠에 해당하는 컨텐츠 보호 정보에 기초하여 컨텐츠 응답 메시지를 전달할지 여부를 결정할 수 있다.

[59] 이를 위해, 먼저, 202 단계에서, 네트워크 장치는, 컨텐츠 보호 정보에 포함된 마킹 정보를 확인할 수 있다. 이때, 네트워크 장치는, 마킹 정보에 기초하여 컨텐츠가 접근 보호가 설정된 컨텐츠인지 여부를 확인할 수 있다. 여기서, 마킹 정보는 문자 코드 또는 숫자 코드 형태의 태그(tag) 로 표현될 수 있다.

[60] 일례로, 마킹 정보가 문자 코드 형태의 'S' (secure)를 포함하는 경우, 네트워크 장치는, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 접근 보호가 설정된 컨텐츠임을 확인할 수 있다.

[61] 다른 예로, 마킹 정보가 문자 코드 형태의 'NS'(non-secure)를 포함하는 경우, 네트워크 장치는, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 접근 허용이 마킹된 컨텐츠임을 확인할 수 있다. 다시 말해, 네트워크 장치는, 다른 네트워크 장치가 컨텐츠로 접근할 수 있도록 허용된 컨텐츠임을 확인할 수 있다.

[62] 또 다른 예로, 마킹 정보가 숫자 형태의 '1'을 포함하는 경우, 네트워크 장치는, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 접근 보호가 설정된 컨텐츠임을 확인할 수 있다.

[63] 또 다른 예로, 마킹 정보가 숫자 형태의 '0'을 포함하는 경우, 네트워크 장치는, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 접근 허용이 설정된 컨텐츠임을 확인할 수 있다.

[64] 이어, 203 단계에서, 마킹 정보를 확인한 경우, 네트워크 장치는, 컨텐츠 보호 정보에 포함된 정책 정보를 확인할 수 있다. 이때, 네트워크 장치는, 정책 정보에 기초하여 응답 메시지를 전달할 (forwarding) 다음 (next hop) 네트워크 장치가 공개 범위 내에 포함되는지 여부를 확인할 수 있다. 여기서, 정책 정보는, 오프셋(offset), 문자 코드, 숫자 코드 및 유사코드, 또는 도메인 리스트(domain list) 형태로 표현된 컨텐츠를 공개하고자 하는 도메인의 수 또는 범위 등을 나타낼 수 있다. 이때, 도메인의 수는, 컨텐츠가 속한 최상위 네트워크 도메인(루트(root, /)로 표현하기도 함), 또는 컨텐츠 자신을 기준으로 계층적으로 연결된 네트워크 도메인의 수를 의미할 수 있다.

[65] 일례로, 루트 도메인을(최상위 네트워크 도메인) 기준으로 하며, 정책 정보가 오프셋 형태의 '2'를 포함하는 경우, 네트워크 장치는, 루트 도메인을 기준으로 두 번째 하위 도메인까지 컨텐츠를 공유 또는 노출할 수 있음을 확인할 수 있다. 예를 들어, 컨텐츠 요청 메시지 ccn_Interest://AAA.xxx/BBB/CCC/DDD가 DDD 도메인의 네트워크 장치로 수신되고, DDD 도메인이 실제로 컨텐츠 보호 정책을 가진 네트워크 도메인일 때, DDD 도메인의 네트워크 장치는 컨텐츠 보호 정책에 따라 컨텐츠 응답 메시지를 전송할 수 있다. 이 때, DDD 도메인의 이름은 /AAA.xxx/BBB/CCC/DDD/DDD의 컨텐츠 보호정보(정책 정보) 가 될 수 있고, DDD의 정책 정보가 '2'를 포함하는 경우, 네트워크 장치는, 루트인 AAA.xxx를 기준으로 '2'에 해당하는 도메인 BBB에 해당하는 네트워크 장치와 루트에는 DDD의 도메인 구조를 공유 또는 노출할 수 없고, 도메인 CCC에 해당하는 네트워크 장치에게는 DDD의 도메인 구조를 공유 또는 노출할 수 있음을 확인할 수 있다.

[66] 그리고, 204 단계에서, 네트워크 장치는, 정책 정보의 확인 여부에 기초하여 컨텐츠 응답 메시지를 전달(forwarding)할 수 있다.

[67] 일례로, 정책 정보에 기초하여 컨텐츠 응답 메시지를 전달할 다음 네트워크 장치가 공개 범위 내에 포함되는 않는 것으로 확인된 경우, 네트워크 장치는, 컨텐츠 응답 메시지를 컨텐츠 응답 메시지를 전달할 다음 네트워크 장치로 전달하지 않을 수 있다. 다시 말해, 컨텐츠 요청 메시지를 무시하고 응답하지 않을 수 있다. 이에 따라, 보호하고자 하는 컨텐츠가 공유 또는 노출을 원하지 않는 네트워크 장치에 전송되는 것을 방지할 수 있다.

[68] 다른 예로, 정책 정보에 기초하여 컨텐츠 응답 메시지를 전달할 다음 네트워크 장치가 공개 범위 내에 포함되는 경우, 네트워크 장치는, 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지를 컨텐츠 응답 메시지를 전달할 다음 네트워크 장치로 전달할 수 있다. 여기서, 컨텐츠 응답 메시지는, 도메인 이름, 컨텐츠 파일 이름, 버전 정보, 세그먼트 번호, 컨텐츠 보호 정보, 및 파일 형태의 컨텐츠

데이터 중 적어도 하나를 포함할 수 있다.

[69] 한편, 네트워크 도메인 별로 컨텐츠 보호 정보가 다르게 설정된 경우, 네트워크 장치는 우선 순위에 기초하여 컨텐츠를 다른 네트워크와 공유 또는 노출할지 여부를 결정할 수 있다.

[70] 예를 들어, 상위 도메인에서 하위 도메인 이름 및 컨텐츠들을 외부 도메인과 공유 또는 노출하지 않도록 컨텐츠 보호 정보 1을 생성하고, 하위 도메인에서는 하위 도메인에 속하는 컨텐츠들을 외부 도메인과 공유 또는 노출하도록 컨텐츠 보호 정보 2를 생성한 경우, 상위 도메인에 대한 컨텐츠 보호 정보 1의 우선 순위가 하위 도메인에 대한 컨텐츠 보호 정보 2의 우선 순위보다 높을 수 있다. 다시 말해, 네트워크 장치는, 컨텐츠 보호 정보 1의 우선 순위가 높기 때문에, 하위 도메인에 속하는 컨텐츠를 외부 도메인에 해당하는 다른 네트워크 장치와 공유 또는 노출하지 않을 수 있다.

[71] 이상의 도 2에서는, 네트워크 장치가 마킹 정보를 확인하여 컨텐츠 응답 메시지의 전달 여부를 결정하는 것에 대해 설명하였으나, 이는 실시예에 해당되며, 네트워크 장치는 마킹 정보의 존재 여부에 기초하여 컨텐츠 응답 메시지의 전달 여부를 결정할 수도 있다.

[72] 일례로, 202 단계에서, 네트워크 장치는, 컨텐츠 이름을 구성하는 컴포넌트들 중 마킹 정보가 위치하는 컴포넌트가 존재하는지 여부를 결정할 수 있다. 이때, 마킹 정보가 존재하지 않는 것으로 결정된 경우, 네트워크 장치는, 보안 정책을 실행하지 않아도 되기 때문에 컨텐츠 응답 메시지를 전달하는 것으로 바로 결정할 수 있다. 그리고, 마킹 정보가 존재하는 경우, 네트워크 장치는, 마킹 정보 이후에 연속하는 내용이 정책 정보임을 확인할 수 있다. 그러면, 네트워크 장치는, 정책 정보에 따라 보안 정책을 실행해야 함을 알 수 있다. 이에 따라, 네트워크 장치는, 앞의 203 및 204 단계에서 설명한 바와 같이, 정책 정보에 기초하여 컨텐츠의 공개 범위를 확인하고, 컨텐츠 응답 메시지의 전달 여부를 결정할 수 있다.

[73] 이상의 도 1 및 도 2에서 설명한 이그레스 필터링(Egress Filtering)에 대한 자세한 설명은, 도 3을 참조하여 후술하기로 한다.

[74] 도 3은 네트워크 장치에서 컨텐츠 응답 메시지의 전송을 제어하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[75] 도 3에 따르면, 네트워크 장치는, 컨텐츠 보호 정보에 기초하여 컨텐츠 요청 메시지에 해당하는 컨텐츠를 상위 도메인에 해당하는 네트워크 장치로 전송할지 여부를 제어할 수 있다. 이때, 보호하고자 하는 컨텐츠에 대한 컨텐츠 요청 메시지가 발생한 경우, 컨텐츠 요청 메시지를 컨텐츠가 저장된 네트워크 장치까지 전달한 후, 컨텐츠가 저장된 네트워크 장치부터 루트 도메인에 해당하는 네트워크 장치들 각각은 컨텐츠 보호 정보, FIB에 포함된 태그 정보 또는 CS에 포함된 태그 정보에 기초하여 컨텐츠를 상위 도메인에 해당하는 네트워크 장치 또는 인터넷을 통해 외부 네트워크 장치로 전달할지 여부를

제어할 수 있다. 이처럼, 컨텐츠가 저장된 네트워크 장치부터 루트 도메인에 해당하는 네트워크 장치까지 계층 별로 컨텐츠를 포함하는 컨텐츠 응답 메시지를 전송할지 여부를 결정하는 것은 IP 기반 네트워크의 방화벽이 수행하는 기능인 이그레스 필터링(Egress Filtering)과 유사할 수 있다. 이에 따라, 이러한 이그레스 필터링을 이용하는 경우, 컨텐츠가 저장된 네트워크 장치 및 컨텐츠가 저장된 네트워크 장치의 상위 도메인들은 컨텐츠 요청 메시지를 모두 수신할 수는 있으나, 컨텐츠 요청 메시지가 공개 범위에 포함되지 않는 네트워크 장치와 공유 또는 노출되는 것을 차단할 수 있다.

[76] 도 3에서, 루트에 해당하는 네트워크 장치 1(302)은, 인터넷(303)을 통해 외부 네트워크 장치로부터 파일 형태의 EEE.zzz에 대한 전송을 요청하는 컨텐츠 요청 메시지를 수신할 수 있다. 예를 들어, 네트워크 장치 1(302)은, ccns_Interest://AAA.xxx/BBB/CCC/DDD/EEE.zzz 형태의 컨텐츠 요청 메시지(301)를 수신할 수 있다.

[77] 이어, 네트워크 장치 1(302)은 컨텐츠 스토어(Contents Store: CS) 1에 컨텐츠 요청 메시지(301)에 해당하는 컨텐츠가 저장되어 있는지 여부를 확인할 수 있다. 이때, CS 1에 컨텐츠가 저장되지 않은 것으로 확인된 경우, 네트워크 장치 1(302)은 자신의 펜딩 인터레스트 테이블(Pending Interest Table: PIT) 1에 컨텐츠 요청 메시지를 기록할 수 있다.

[78] 그리고, 네트워크 장치 1(302)은 전달 정보 베이스(Forwarding Information Base: FIB) 1를 참조하여 컨텐츠 요청 메시지를 전달할 네트워크 장치 2(304)에 해당하는 인터페이스(305)를 결정할 수 있다. 여기서, CCN에서 인터페이스(interface)는 페이스(face)로 표현될 수 있으며, 포트 번호(port number)를 포함할 수 있다. 예를 들어, 네트워크 장치 1(302)은, FIB 1에 기록된 메시지들과 컨텐츠 요청 메시지 간의 롱기스트 매칭(longest matching)을 이용하여 인터페이스(305)를 결정할 수 있다. 그리고, 네트워크 장치 1(302)은 결정된 인터페이스(305)를 통해 컨텐츠 요청 메시지(301)를 네트워크 장치 2(304)로 전달할 수 있다. 이때, CCN에서 컨텐츠 응답 메시지는 데이터(DATA)로 표현될 수도 있다.

[79] 동일한 방법으로, 네트워크 장치 2(304)는 컨텐츠 요청 메시지(301)를 다음 네트워크 장치 3(306)으로 전달할 수 있다. 마찬가지로, 네트워크 장치 3(306)은 컨텐츠 요청 메시지(301)을 네트워크 장치 4(307)로 전달하고, 네트워크 장치 4(307)는 컨텐츠 요청 메시지(301)을 네트워크 장치 5(308)로 전달할 수 있다. 그러면, 네트워크 장치 4(307)는 컨텐츠 스토어(CS) 4에 컨텐츠 요청 메시지(301)에 해당하는 컨텐츠가 저장되어 있는지 여부를 확인할 수 있다.

[80] 이때, CS 4에 컨텐츠가 저장된 것으로 확인된 경우, 네트워크 장치 4(307)는 CS 4의 태그 정보에 기초하여 컨텐츠의 공개 범위를 확인할 수 있다.

[81] 예를 들어, 컨텐츠에 해당하는 태그 정보가 '1'로 설정(311)된 경우, 네트워크 장치 4(307)는 컨텐츠 요청 메시지에 해당하는 컨텐츠가 보호가 설정된

컨텐츠임을 확인할 수 있다. 그러면, 네트워크 장치 4(307)는 컨텐츠에 대한 컨텐츠 보호 정보에 기초하여 컨텐츠를 네트워크 장치 3(306)으로 전달할지 여부를 결정할 수 있다.

[82] 예를 들어, 컨텐츠 요청 메시지에 해당하는 컨텐츠의 정책 정보가 '3'을 포함하는 경우, 네트워크 장치 4(307)는 루트부터 세 번째 도메인에 해당하는 네트워크 장치 3(306)까지 컨텐츠를 공유 또는 노출할 수 있음을 확인할 수 있다. 이에 따라, 네트워크 장치 4(307)는 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지를 네트워크 장치 3(306)으로 전달(312)할 수 있다.

[83] 여기서, 컨텐츠 응답 메시지는 도메인 이름, 컨텐츠 파일 이름, 컨텐츠 보호 정보, 및 컨텐츠 데이터를 포함할 수 있다. 이때, 컨텐츠 데이터가 여러 버전을 가지고 있으며, 복수의 세그먼트로 분할된 경우, 컨텐츠 응답 메시지는 버전 정보 및 세그먼트 정보를 더 포함할 수 있다.

[84] 동일한 방법으로, 네트워크 장치 3(306)은 컨텐츠 응답 메시지에 포함된 컨턴츠 보호 정보에 기초하여 수신한 컨텐츠에 해당하는 태그 정보를 설정할 수 있다. 이때, 수신한 컨텐츠가 보호 컨텐츠로 확인된 경우, 네트워크 장치 3(306)은 정책 정보에 기초하여 컨텐츠의 공개 범위가 루트부터 세 번째 도메인에 해당하는 네트워크 장치 3(306)까지 임을 확인할 수 있다. 다시 말해, 네트워크 장치 3(306)은 정책 정보에 기초하여 컨텐츠의 공개 범위에 네트워크 장치 2(304)가 포함되지 않는 것을 확인할 수 있다.

[85] 그러면, 네트워크 장치 3(306)은 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지를 네트워크 장치 2(304)로 전달하지 않을 수 있다(313). 이에 따라, 컨텐츠 요청 메시지에 해당하는 컨텐츠의 공개 범위에 포함되지 않는 네트워크 장치로는 컨텐츠 응답 메시지가 전달되지 않음에 따라, 컨텐츠 생성자가 보호를 원하는 컨텐츠는 보호될 수 있다.

[86] 도 4는 네트워크 장치에서 컨텐츠 요청 메시지의 전송을 제어하는 방법을 설명하기 위해 제공되는 플로우 차트이다.

[87] 도 4에 따르면, 네트워크 장치는, FIB 또는 FIB에 포함된 태그 정보에 기초하여 컨텐츠 요청 메시지를 다음 네트워크 장치로 전송할지 여부를 제어할 수 있다. 여기서, 다음 네트워크 장치는 하위 네트워크 도메인에 존재하는 네트워크 장치일 수 있다.

[88] 이처럼, 보호하고자 하는 컨텐츠에 대한 컨텐츠 요청 메시지가 발생한 경우, 컨텐츠 응답 메시지를 전달할 다음 네트워크 장치가 먼저 다음 네트워크 장치로 컨텐츠 요청 메시지가 전송되는 것을 차단할 수 있는데, 이는 IP 기반 네트워크의 방화벽이 수행하는 기능인 인그레스 필터링(Ingress Filtering)과 유사하다. 여기서, 다음 네트워크 장치는 상위 네트워크 도메인에 존재하는 네트워크 장치일 수 있다.

[89] 이에 따라, 이러한 인그레스 필터링을 이용하는 경우, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 저장된 네트워크 장치는 컨텐츠 요청 메시지가 발생한 사실

자체를 모를 수도 있다.

[90] 도 4에서, 루트에 해당하는 네트워크 장치 1(402)은, 인터넷(403)을 통해 외부 네트워크 장치로부터 파일 형태의 EEE.zzz에 대한 전송을 요청하는 컨텐츠 요청 메시지를 수신할 수 있다. 예를 들어, 네트워크 장치 1(402)은, ccns_Interest://AAA.xxx/BBB/CCC/DDD/EEE.zzz 형태의 컨텐츠 요청 메시지(401)를 수신할 수 있다.

[91] 이어, 네트워크 장치 1(402)은 컨텐츠 스토어(Contents Store: CS) 1에 컨텐츠 요청 메시지(401)에 해당하는 컨텐츠가 저장되어 있는지 여부를 확인할 수 있다.

[92] 이때, CS 1에 컨텐츠가 저장되지 않은 것으로 확인된 경우, 네트워크 장치 1(402)은 자신의 펜딩 인터레스트 테이블(Pending Interest Table: PIT) 1에 컨텐츠 요청 메시지를 기록할 수 있다.

[93] 그리고, 네트워크 장치 1(402)은 전달 정보 베이스(Forwarding Information Base: FIB) 1를 참조하여 컨텐츠 요청 메시지(401)를 전달할 네트워크 장치 2(404)에 해당하는 인터페이스(405)를 결정할 수 있다. 여기서, CCN에서 인터페이스(interface)는 페이스(face)로 표현될 수 있으며, 포트 번호(port number)를 포함할 수 있다. 예를 들어, 네트워크 장치 1(402)은, FIB 1에 기록된 메시지들과 컨텐츠 요청 메시지 간의 롱기스트 매칭(longest matching)을 이용하여 인터페이스(405)를 결정할 수 있다.

[94] 그리고, 네트워크 장치 1(402)은 결정된 인터페이스에 해당하는 태그 정보에 기초하여 컨텐츠 요청 메시지를 결정된 인터페이스(405)를 통해 다음 네트워크 장치 2(403)로 전달할지 여부를 결정할 수 있다. 여기서, 다음 네트워크 장치는 하위 네트워크 도메인에 존재하는 네트워크 장치일 수 있다. 예를 들어, 결정된 인터페이스(405)에 해당하는 태그 정보가 '0'인 경우, 네트워크 장치 1(402)은 태그 정보에 기초하여 도메인 이름 '/AAA.xxx/BBB/CCC'는 보호 컨텐츠로 설정되지 않음을 확인할 수 있다. 그러면, 네트워크 장치 1(402)은 결정된 인터페이스(405)를 통해 컨텐츠 요청 메시지를 네트워크 장치 2(404)로 전달할 수 있다.

[95] 동일한 방법으로, 네트워크 장치 2(404)는 컨텐츠 요청 메시지를 수신함에 따라, 컨텐츠 스토어 2에 컨텐츠 요청 메시지(401)에 해당하는 컨텐츠가 저장되어 있는지 여부를 확인할 수 있다. 이때, CS 2에 컨텐츠가 저장되지 않은 것으로 확인된 경우, 네트워크 장치 2(404)는 자신의 펜딩 인터레스트 테이블(PIT) 2에 컨텐츠 요청 메시지(401)를 기록할 수 있다. 이어, 네트워크 장치 2(404)는 전달 정보 베이스(FIB) 2를 참조하여 컨텐츠 요청 메시지(401)를 전달할 네트워크 장치 3(406)에 해당하는 인터페이스(407)를 결정할 수 있다. 그리고, 네트워크 장치 2(404)은 결정된 인터페이스(407)를 통해 컨텐츠 요청 메시지를 네트워크 장치 3(406)으로 전달할 수 있다.

[96] 그리고, 네트워크 장치 2(404)는 결정된 인터페이스(407)에 해당하는 태그 정보에 기초하여 컨텐츠 요청 메시지를 결정된 인터페이스(407)를 통해 하위

도메인에 해당하는 네트워크 장치 3(406)으로 전달할지 여부를 결정할 수 있다. 이때, 네트워크 장치 3(406)으로 전달 가능한 것으로 결정된 경우, 네트워크 장치 2(404)는 컨텐츠 요청 메시지를 인터페이스(407)를 통해 네트워크 장치 3(406)으로 전달할 수 있다(410).

[97] 동일한 방법으로, 네트워크 장치 3(406)은 FIB 3에서 롱기스트 매칭을 이용하여 컨텐츠 요청 메시지(401)를 전달할 네트워크 장치 4(409)에 해당하는 인터페이스(408)를 결정할 수 있다. 그리고, 네트워크 장치 3(406)는 결정된 인터페이스(408)에 해당하는 태그 정보에 기초하여 컨텐츠 요청 메시지를 하위 도메인에 해당하는 네트워크 장치 4(409)로 전달할지 여부를 결정할 수 있다.

[98] 예를 들어, FIB 3에서, 결정된 인터페이스(408)에 해당하는 태그 정보가 '1'로 설정된 경우, 네트워크 장치 3(406)은 '/AAA.xxx/CCC/DDD'가 보호가 설정된 컨텐츠 임을 확인할 수 있다. 그러면, 네트워크 장치 3(406)은 컨텐츠 요청 메시지(401)를 하위 도메인에 해당하는 네트워크 장치 4(409)로 전달하지 않을 수 있다(411). 이처럼, 네트워크 장치 3(406)은 IFB 4에서 태그 정보에 기초하여 컨텐츠 요청 메시지(401)를 무시하고, 네트워크 장치 4(409)로 전달하지 않음에 따라, 결국 네트워크 장치 4(409) 는 컨텐츠 요청 메시지를 수신하지 않을 수 있고, 네트워크 장치 4에 저장된 컨텐츠(412) 또한 전송하지 않을 수 있다. 이에 따라, 컨텐츠 요청 메시지(401)에 해당하는 컨텐츠(412)는 컨텐츠의 공개 범위에 포함되는 네트워크 장치 4(409), 및 네트워크 장치 3(406)까지만 공유 또는 노출될 수 있으며, 컨텐츠는 공개 범위에 포함되지 않는 다른 네트워크 장치들과는 공유 또는 노출되지 않을 수 도 있다.

[99] 도 5는 네트워크 장치의 세부 구성을 도시한 블록 다이어그램이다.

[100] 도 5에 따르면, 네트워크 장치(500)는 컨텐츠 보호 정보 생성부(501), 컨텐츠 이름 생성부(502), 메시지 수신부(503), 결정부(505), 및 컨텐츠 스토어(507)를 포함할 수 있다.

[101] 먼저, 컨텐츠 보호 정보 생성부(501)는 컨텐츠를 생성하면서, 생성하는 컨텐츠의 보호 여부를 나타내는 마킹 정보 및 컨텐츠의 공개 범위를 나타내는 정책 정보를 포함하는 컨텐츠 보호 정보를 생성할 수 있다. 여기서, 마킹 정보는, 다른 네트워크 장치 및 외부 네트워크 장치 중 적어도 하나에게 생성한 컨텐츠에 대한 접근을 허용할지 또는 접근을 막고 보호할지 여부에 대한 정책이 컨텐츠 이름에 포함되어 있음을 나타내는 정보일 수 있다. 그리고, 정책 정보는, 계층적 구조를 가지고 있는 각 도메인에 해당하는 네트워크 장치들 중에서 생성한 컨텐츠가 전달되어 공유 또는 노출될 수 있는 공개 범위를 나타내는 정보일 수 있다. 예를 들어, 컨텐츠 보호 정보 생성부(501)는 정책 정보를 오프셋, 숫자나 문자 코드, 유사 코드, 또는 네트워크 도메인 리스트 형태로 생성할 수 있다.

[102] 컨텐츠 이름 생성부(502)는 컨텐츠 보호 정보에 기초하여 컨텐츠 이름 기반의 네트워크(CCN)에서 컨텐츠의 위치(즉, 경로)를 나타내는 컨텐츠 이름을 생성할 수 있다. 여기서, 컨텐츠 이름은, 도메인 이름 정보, 컨텐츠 이름 정보, 버전 정보,

컨텐츠 보호 정보, 및 세그먼트 정보 중 적어도 하나를 포함할 수 있다.

[103] 이때, 컨텐츠 이름은 복수의 컴포넌트(component)로 구분될 수 있으며, 컨텐츠 보호 정보는 복수의 컴포넌트들 중 하나의 컴포넌트로 구성될 수 있다. 다시 말해, 컨텐츠 이름 생성부(502)는 복수의 컴포넌트들 중 어느 하나의 컴포넌트에 컨텐츠 보호 정보가 포함되도록 컨텐츠 이름을 생성할 수 있다. 이때, 컨텐츠 이름 생성부(502)는 복수의 컴포넌트들 중에서 컨텐츠에 대한 전자 서명이 적용되는 범위 내에 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다.

[104] 일례로, 도메인 이름 및 도메인에 속하는 컨텐츠 이름을 보호하고자 하는 경우, 컨텐츠 이름 생성부(502)는 복수의 컴포넌트들 중에서 도메인 이름 정보가 위치하는 컴포넌트 이후에 연속하여 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다.

[105] 다른 예로, 컨텐츠 이름을 보호하고자 하는 경우, 컨텐츠 이름 생성부(502)는 복수의 컴포넌트들 중에서 컨텐츠 이름 정보가 위치하는 컴포넌트 이후에 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다. 예를 들어, 생성한 컨텐츠에 대한 버전 정보와 세그먼트 정보가 존재하는 경우, 컨텐츠 이름 생성부(502)는 버전 정보와 세그먼트 정보 사이에 컨텐츠 보호 정보가 위치하도록 컨텐츠 이름을 생성할 수 있다.

[106] 메시지 수신부(503)는 다른 네트워크 장치로부터 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신할 수 있다. 예를 들어, 메시지 수신부(503)는 다음 네트워크 장치로부터 컨텐츠 요청 메시지를 수신할 수 있다. 여기서, 컨텐츠 요청 메시지는, 컨텐츠 데이터, 컨텐츠 이름 정보, 도메인 이름 정보, 도메인 구조(domain hierarchy) 정보, 컨텐츠 리스트 정보 중 적어도 하나를 포함할 수 있다.

[107] 그러면, 결정부(504)는 컨텐츠 보호 정보에 기초하여 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지를 다른 네트워크 장치로 전달할지 여부를 결정할 수 있다. 여기서, 결정부(504)는 컨텐츠 요청 메시지가 가리키는 컨텐츠가 컨텐츠 스토어(507)에 저장되어 있는지 여부를 확인하는 확인부(505), 및 컨텐츠 보호 정보에 기초하여 컨텐츠를 포함하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 전달 결정부(506)를 포함할 수 있다.

[108] 일례로, 컨텐츠 스토어(507)에 컨텐츠 요청 메시지에 해당하는 컨텐츠가 저장된 것으로 확인된 경우, 확인부(505)는 마킹 정보에 기초하여 컨텐츠에 대한 접근 보호 여부를 확인할 수 있다. 이때, 컨텐츠가 보호 컨텐츠로 확인된 경우, 확인부(505)는 정책 정보에 기초하여 컨텐츠 요청 메시지에 해당하는 컨텐츠의 공개 범위를 확인할 수 있다. 다시 말해, 확인부(505)는 상위 도메인에 해당하는 네트워크 장치가 공개 범위 내에 포함되는지 여부를 확인할 수 있다. 이때, 네트워크 장치가 공개 범위 내에 포함되는 것으로 확인된 경우, 전달 결정부(506)는 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지를 상위

도메인에 해당하는 네트워크 장치로 전달할 수 있다.

[109] 반면, 상위 도메인에 해당하는 네트워크 장치가 공개 범위 내에 포함되지 않는 것으로 확인된 경우, 전달 결정부(506)는 컨텐츠 응답 메시지를 네트워크 장치로 전달하지 않는 것으로 결정할 수 있다. 여기서, 컨텐츠 응답 메시지는, 도메인 이름, 컨텐츠 이름, 컨텐츠 보호 정보, 버전 정보, 세그먼트 정보 및 컨텐츠 데이터 중 적어도 하나를 포함할 수 있다. 이에 따라, 컨텐츠 보호 정보에 기초하여 컨텐츠 응답 메시지를 상위 도메인에 해당하는 네트워크 장치로 전달하지 않는 경우, 공개 범위에 포함되지 않는 네트워크 장치들로 컨텐츠가 공유 또는 노출되는 것을 보호할 수 있다.

[110] 도 6은 네트워크 장치에서 컨텐츠 요청 메시지를 중계하는 방법을 설명하기 위해 제공되는 플로우 차트이다. 도 6에서, 네트워크 장치는 컨텐츠 중심 네트워킹(CCN)을 수행하는 네트워크 장치들 중 컨텐츠 요청 메시지를 전달하는 중계 네트워크 장치일 수 있다.

[111] 도 6에 따르면, 601 단계에서, 네트워크 장치는 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신할 수 있다. 여기서, 컨텐츠 요청 메시지는, 컨텐츠 데이터 자체, 컨텐츠 파일 이름, 도메인 이름, 도메인에 속하는 컨텐츠들을 포함하는 컨텐츠 리스트 정보, 및 도메인 구조(domain hierarchy) 정보 중 적어도 하나를 포함할 수 있다.

[112] 이어, 602 단계에서, 네트워크 장치는, 컨텐츠 보호 정보에 기초하여 설정된 태그 정보를 이용하여 컨텐츠 요청 메시지의 전달 여부를 결정할 수 있다. 여기서, 컨텐츠 보호 정보는, 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 컨텐츠의 공개 범위를 나타내는 정책 정보를 포함할 수 있다. 이때, 네트워크 장치는, 컨텐츠의 마킹 정보에 기초하여 CS의 태그 정보 및 FIB의 태그 정보를 설정할 수 있다. 여기서, 태그 정보는, 마킹 정보에 기초하여 컨텐츠 요청 메시지에 해당하는 컨텐츠가 보호 컨텐츠인지 여부가 설정된 정보이다.

[113] 일례로, 네트워크 장치는, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 컨텐츠 스토어에 저장되어 있는지 여부를 확인할 수 있다. 그리고, 컨텐츠가 저장되지 않은 것으로 확인된 경우, 네트워크 장치는, 컨텐츠 요청 메시지를 팬딩 인터레스트 테이블(PIT)에 기록할 수 있다. 이어, 네트워크 장치는, 전달 정보 베이스(FIB)의 태그 정보에 기초하여 다음 네트워크 장치로 컨텐츠 요청 메시지를 전달할지 여부를 결정할 수 있다. 여기서, 다음 네트워크 장치는 하위 네트워크 도메인에 존재하는 네트워크 장치일 수 있다.

[114] 이때, 태그 정보에 기초하여 컨텐츠가 보호 컨텐츠로 결정된 경우, 네트워크 장치는, 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달하지 않는 것으로 결정할 수 있다. 반면, 태그 정보에 기초하여 컨텐츠가 보호 컨텐츠가 아닌 것으로 결정된 경우, 네트워크 장치는 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달하는 것으로 결정할 수 있다. 이러한 인그레스 필터링(Ingress Filtering)에 대한 설명은 앞의 도 4에서 자세히 설명하였으므로 중복되는 설명은

생략하기로 한다.

[115] 도 7은 컨텐츠 요청 메시지를 중계하는 네트워크 장치의 세부 구성을 도시한 블록 다이어그램이다.

[116] 도 7에 따르면, 네트워크 장치(700)는 메시지 수신부(701), 결정부(702), 및 컨텐츠 스토어(705)를 포함할 수 있다.

[117] 먼저, 메시지 수신부(701)는 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신할 수 있다. 예를 들어, 메시지 수신부(701)는 상위 도메인에 해당하는 네트워크 장치로부터 컨텐츠 요청 메시지를 수신할 수 있다.

[118] 결정부(702)는 컨텐츠 보호 정보에 기초하여 설정된 태그 정보를 이용하여 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달할지 여부를 결정할 수 있다. 여기서, 컨텐츠 보호 정보는, 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 컨텐츠의 공개 범위를 나타내는 정책 정보를 포함할 수 있다. 이때, 결정부(702)는 확인부(703) 및 전달 결정부(704)를 포함할 수 있다.

[119] 전달 결정부(704)는 컨텐츠 보호 정보에 기초하여 컨텐츠 요청 메시지의 전달 여부를 결정할 수 있다. 전달 결정부(704)는 컨텐츠에 대한 접근 보호가 확인됨에 따라, 정책 정보와 전달 정보 베이스(Forwarding Information Base: FIB)에 기록되어 있는 정책 정보에 기초하여 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달할 필요가 있는지 여부를 결정할 수 있다. 여기서, 다음 네트워크 장치는 하위 네트워크 도메인에 존재하는 네트워크 장치일 수 있다. 전달 결정부(704)는 컨텐츠 요청 메시지가 가리키는 컨텐츠가 저장되지 않은 것으로 확인됨에 따라, 컨텐츠 보호 정보에 기초하여 컨텐츠 요청 메시지의 전달 여부를 결정할 수 있다.

[120] 전달 결정부(704)는 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달할 필요가 없는 것으로 확인되는 경우, 컨텐츠 요청 메시지를 다음 네트워크로 전달하지 않는 것으로 결정할 수 있다.

[121] 또한, 전달 결정부(704)는, 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달할 필요가 있거나, 불필요함을 확인하지 못한 경우, 컨테츠 요청 메시지를 다음 네트워크 장치로 전달하는 것으로 결정할 수 있다.

[122] 확인부(703)는 컨텐츠 요청 메시지가 수신됨에 따라, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 컨텐츠 스토어(CS: 705)에 저장되었는지 여부를 확인할 수 있다. 이때, 저장되지 않은 것으로 확인된 경우, 네트워크 장치는, 컨텐츠 요청 메시지를 PIT에 기록할 수 있다. 또는 확인부(703)는 마킹 정보에 기초하여 컨텐츠가 접근 보호가 설정된 컨텐츠 인지 여부를 확인할 수 있다.

[123] 그리고, CS에 컨텐츠 요청 메시지에 해당하는 컨텐츠가 저장되지 않은 것으로 확인된 경우, 네트워크 장치는, FIB의 태그 정보에 기초하여 다음 네트워크 장치로 컨텐츠 요청 메시지를 전달할 지 여부를 결정할 수 있다. 반면, 저장된 것으로 확인된 경우, CS의 태그 정보에 기초하여 다음 네트워크 장치로 컨텐츠 요청 메시지를 전달할 지 여부를 결정할 수 있다. 여기서, 태그 정보는, 마킹

정보에 기초하여 컨텐츠 요청 메시지에 해당하는 컨텐츠가 보호 컨텐츠인지 여부가 설정된 정보일 수 있다.

[124] 이때, 컨텐츠 요청 메시지에 해당하는 컨텐츠가 보호 컨텐츠인 경우, 네트워크 장치는, 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달하지 않는 것으로 결정할 수 있다. 반면, 컨텐츠가 보호 컨텐츠가 아닌 경우, 네트워크 장치는, 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달하는 것으로 결정할 수 있다. 이러한 인그레스 필터링(Ingress Filtering)에 대한 설명은 앞의 도 4에서 자세히 설명하였으므로 중복되는 설명은 생략하기로 한다.

[125] 지금까지, 마킹 정보 및 정책 정보를 포함하는 컨텐츠 보호 정보를 이용하여 컨텐츠를 생성한 네트워크 장치가 다른 네트워크 장치 및 외부 네트워크 장치 중 적어도 하나와 컨텐츠를 공유 또는 노출을 제어하는 구성에 대해 설명하였다. 여기서, 마킹 정보(marking information)는, 다른 네트워크 장치 또는 외부 네트워크 장치 중 적어도 하나에게 컨텐츠에 대한 접근을 허용 할지 또는 컨텐츠에 대한 접근을 보호할지 여부에 대한 정책이 컨텐츠 이름에 포함되어 있음을 나타내는 정보일 수 있다.

[126] 즉, 마킹 정보는, 컨텐츠가 보호 컨텐츠로 설정되었는지 또는 비보호 컨텐츠로 설정되었는지 여부를 나타내는 정보일 뿐만 아니라, 마킹 정보 이후에 위치하는 문자열, 데이터 등이 정책 정보임을 나타내는 정보를 의미할 수 있다.

[127] 일례로, 컨텐츠 이름이 /AAA.xxx/BBB/CCC/_SS_정책1/_Version_2.0인 경우, 네트워크 장치는 슬래시(/)로 단위마다 컨텐츠 이름을 해석(parsing)할 수 있다. 여기서, 컨텐츠 이름은, 컨텐츠 전체 이름을 나타낼 수 있다.

[128] 그러면, 네트워크 장치는, 파싱을 통해 AAA.xxx, BBB, CCC는 컨텐츠 이름 정보 및 도메인 이름 정보를 의미하는 정보이고,_Version_과 연속하여 위치하는 숫자가 2.0이므로 컨텐츠의 버전이 2.0임을 확인할 수 있다. 그리고, 네트워크 장치는, 파싱을 통해 _SS_와 연속하여 위치하는 정책1을 실행해야 함을 확인할 수 있다. 이처럼, 마킹 정보는, 마킹 정보와 연속하여 위치하는 문자열, 데이터 형태의 내용을 정책 정보로 활용해야 함을 네트워크 장치에게 알려주기 위한 정보일 수 있다.

[129] 다시 말해, 네트워크 장치는, 컨텐츠 이름 내에 마킹 정보가 존재하는지 여부에 기초하여 보안 정책을 수행할지, 수행하지 않을지 여부를 결정할 수 있다. 이에 따라, 컨텐츠 이름 내에 마킹 정보가 포함된 컴포넌트가 없는 경우, 네트워크 장치는, 컨텐츠 보호를 위한 보안 정책을 수행하지 않을 수 있다. 그리고, 마킹 정보가 포함된 컴포넌트가 존재하는 경우, 네트워크 장치는, 마킹 정보 이후에 연속하여 위치하는 내용이 정책 정보임을 확인하고, 정책 정보에 따라 컨텐츠 보호를 위한 정책을 수행할 수 있다.

[130] 이상에서 설명한 바와 같이, 본 발명의 일실시예에 따르면, 컨텐츠 보호 정보에 기초하여 컨텐츠에 대한 접근 허용을 제어함에 따라, 컨텐츠 생성자가 컨텐츠 공유를 원하지 않는 사용자 또는 네트워크 장치로부터 컨텐츠를 보호할 수 있다.

[131] 본 발명의 실시 예에 따른 방법들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[132] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[133] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

청구범위

[청구항 1] 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함하는 컨텐츠 보호 정보를 생성하는 단계; 및
상기 컨텐츠 보호 정보에 기초하여 컨텐츠 이름 기반의 네트워크에서 컨텐츠의 위치를 나타내는 컨텐츠 이름을 생성하는 단계
를 포함하는 컨텐츠 보호 방법.

[청구항 2] 제1항에 있어서,
상기 컨텐츠 보호 정보를 생성하는 단계는,
상기 컨텐츠를 생성하면서, 상기 컨텐츠 보호 정보를 함께 생성하고,
상기 마킹 정보는, 다른 네트워크 장치 및 외부 네트워크 장치 중 적어도 하나에게 상기 컨텐츠에 대한 접근을 허용할지 또는 상기 컨텐츠에 대한 접근을 보호할지 여부에 대한 정책이 컨텐츠 이름에 포함되어 있음을 나타내는 정보인 컨텐츠 보호 방법.

[청구항 3] 제1항에 있어서,
상기 컨텐츠 보호 정보를 생성하는 단계는,
상기 정책 정보를 오프셋(offset), 숫자, 유사코드, 또는 도메인 리스트(domain list) 형태로 생성하고,
상기 정책 정보는,
상기 컨텐츠가 전달될 수 있는 공개 범위를 나타내는 정보인 컨텐츠 보호 방법.

[청구항 4] 제1항에 있어서,
상기 컨텐츠 이름은, 복수의 컴포넌트(component)로 구분되며,
상기 컨텐츠 보호 정보는, 하나의 컴포넌트로 구성되어 상기 컨텐츠 이름 내에 포함되는 컨텐츠 보호 방법.

[청구항 5] 제4항에 있어서,
상기 컨텐츠 이름을 생성하는 단계는,
상기 복수의 컴포넌트들 중 컨텐츠에 대한 전자 서명이 적용되는 범위 내에 상기 컨텐츠 보호 정보가 위치하도록 상기 컨텐츠 이름을 생성하는 컨텐츠 보호 방법.

[청구항 6] 제1항에 있어서,
상기 컨텐츠 이름을 생성하는 단계는,
도메인 이름 정보가 위치하는 컴포넌트 이후에 연속하여 상기 컨텐츠 보호 정보가 위치하도록 상기 컨텐츠 이름을 생성하는 컨텐츠 보호 방법.

[청구항 7] 제1항에 있어서,
상기 컨텐츠 이름을 생성하는 단계는,
컨텐츠 이름 정보가 위치하는 컴포넌트 이후에 상기 컨텐츠 보호 정보가 위치하도록 상기 컨텐츠 이름을 생성하는 컨텐츠 보호 방법.

[청구항 8] 제1항에 있어서,
상기 컨텐츠 이름을 생성하는 단계는,
상기 컨텐츠 보호 정보가 버전 정보 및 세그먼트 정보 사이에 위치하도록 상기 컨텐츠 이름을 생성하는 컨텐츠 보호 방법.

[청구항 9] 제1항에 있어서,
상기 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신하는 단계; 및
상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계
를 더 포함하는 컨텐츠 보호 방법.

[청구항 10] 제9항에 있어서,
상기 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계는,
상기 컨텐츠 요청 메시지가 가리키는 컨텐츠의 저장 여부를 확인하는 단계; 및
상기 컨텐츠가 저장된 것으로 확인됨에 따라, 상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠를 포함하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계
를 포함하는 컨텐츠 보호 방법.

[청구항 11] 제10항에 있어서,
상기 컨텐츠를 포함하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계는,
상기 마킹 정보에 기초하여 상기 컨텐츠가 접근 보호가 설정된 컨텐츠인지 여부를 확인하는 단계; 및
상기 컨텐츠에 대한 접근 보호가 확인됨에 따라, 상기 정책 정보에 기초하여 상위 도메인에 해당하는 네트워크 장치가 상기 공개 범위 내에 포함되는지 여부를 확인하는 단계
를 포함하는 컨텐츠 보호 방법.

[청구항 12] 제11항에 있어서,
상기 컨텐츠를 포함하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계는,
상기 상위 도메인에 해당하는 네트워크 장치가 공개 범위 내에 포함되지 않는 것으로 확인됨에 따라, 상기 컨텐츠 응답 메시지를 전달하지 않는 것으로 결정하는 컨텐츠 보호 방법.

[청구항 13] 제11항에 있어서,
상기 컨텐츠를 포함하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계는,
상기 상위 도메인에 해당하는 네트워크 장치가 공개 범위 내에 포함되는 것으로 확인됨에 따라, 상기 컨텐츠 응답 메시지를 상기 상위 도메인에 해당하는 네트워크 장치로 전달하는 것으로 결정하는 컨텐츠 보호 방법.

[청구항 14] 제9항에 있어서,
상기 컨텐츠 요청 메시지는,
컨텐츠 이름, 컨텐츠 내용(object), 컨텐츠 네트워크의 도메인 이름, 컨텐츠 네트워크의 도메인 구조(domain hierarchy), 및 특정 컨텐츠 네트워크의 도메인에 포함된 컨텐츠 리스트 중 적어도 하나를 포함하는 컨텐츠 보호 방법.

[청구항 15] 제1항에 있어서,
상기 컨텐츠 이름은,
컨텐츠 네트워크의 도메인(domain) 이름, 컨텐츠의 고유 이름, 컨텐츠의 버전(version) 정보, 상기 컨텐츠 보호 정보, 및 세그먼트(segment) 정보 중 적어도 하나를 포함하는 컨텐츠 보호 방법.

[청구항 16] 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함하는 컨텐츠 보호 정보를 생성하는 컨텐츠 보호 정보 생성부; 및
상기 컨텐츠 보호 정보에 기초하여 컨텐츠 이름 기반의 네트워크에서 컨텐츠의 위치를 나타내는 컨텐츠 이름을 생성하는 컨텐츠 이름 생성부
를 포함하는 네트워크 장치.

[청구항 17] 제16항에 있어서,
상기 컨텐츠 보호 정보 생성부는,
상기 컨텐츠를 생성하면서, 상기 컨텐츠 보호 정보를 함께 생성하고,
상기 마킹 정보는, 다른 네트워크 장치 및 외부 네트워크 장치 중 적어도 하나에게 상기 컨텐츠에 대한 접근을 허용할지 또는 상기 컨텐츠에 대한 접근을 보호할지 여부에 대한 정책이 컨텐츠 이름에 포함되어 있음을 나타내는 정보인 네트워크 장치.

[청구항 18] 제16항에 있어서,
상기 컨텐츠 보호 정보 생성부는,
상기 정책 정보를 오프셋(offset), 숫자, 유사코드, 또는 도메인 리스트(domain list) 형태로 생성하고,

상기 정책 정보는,
상기 컨텐츠가 전달될 수 있는 공개 범위를 나타내는 정보인 네트워크 장치.

[청구항 19] 제16항에 있어서,
상기 컨텐츠 이름은, 복수의 컴포넌트(component)로 구분되며,
상기 컨텐츠 보호 정보는, 하나의 컴포넌트로 구성되어 상기 컨텐츠 이름 내에 포함되는 네트워크 장치.

[청구항 20] 제19항에 있어서,
상기 컨텐츠 이름 생성부는,
상기 복수의 컴포넌트들 중 컨텐츠에 대한 전자 서명이 적용되는 범위 내에 상기 컨텐츠 보호 정보가 위치하도록 상기 컨텐츠 이름을 생성하는 네트워크 장치.

[청구항 21] 제16항에 있어서,
상기 컨텐츠 이름 생성부는,
도메인 이름 정보가 위치하는 컴포넌트 이후에 연속하여 상기 컨텐츠 보호 정보가 위치하도록 상기 컨텐츠 이름을 생성하는 네트워크 장치.

[청구항 22] 제16항에 있어서,
상기 컨텐츠 이름 생성부는,
컨텐츠 이름 정보가 위치하는 컴포넌트 이후에 상기 컨텐츠 보호 정보가 위치하도록 상기 컨텐츠 이름을 생성하는 네트워크 장치.

[청구항 23] 제16항에 있어서,
상기 컨텐츠 이름 생성부는,
상기 컨텐츠 보호 정보가 버전 정보 및 세그먼트 정보 사이에 위치하도록 상기 컨텐츠 이름을 생성하는 네트워크 장치.

[청구항 24] 제16항에 있어서,
상기 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신하는 메시지 수신부; 및
상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 결정부를 더 포함하는 네트워크 장치.

[청구항 25] 제24항에 있어서,
상기 결정부는,
상기 컨텐츠 요청 메시지가 가리키는 컨텐츠의 저장 여부를 확인하는 확인부; 및
상기 컨텐츠가 저장된 것으로 확인됨에 따라, 상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠를 포함하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 전달 결정부

를 포함하는 네트워크 장치.

[청구항 26] 제25항에 있어서,
상기 확인부는,
상기 컨텐츠가 저장된 것으로 확인됨에 따라, 상기 마킹 정보에 기초하여 상기 컨텐츠가 접근 보호가 설정된 컨텐츠인지 여부를 확인하고, 상기 컨텐츠에 대한 접근 보호가 확인됨에 따라, 상기 정책 정보에 기초하여 상위 도메인에 해당하는 네트워크 장치가 상기 공개 범위 내에 포함되는지 여부를 확인하는 네트워크 장치.

[청구항 27] 제26항에 있어서,
상기 전달 결정부는,
상기 상위 도메인에 해당하는 네트워크 장치가 공개 범위 내에 포함되지 않는 것으로 확인됨에 따라, 상기 컨텐츠 응답 메시지를 전달하지 않는 것으로 결정하는 네트워크 장치.

[청구항 28] 제26항에 있어서,
상기 전달 결정부는,
상기 상위 도메인에 해당하는 네트워크 장치가 공개 범위 내에 포함되는 것으로 확인됨에 따라, 상기 컨텐츠 응답 메시지를 상기 상위 도메인에 해당하는 네트워크 장치로 전달하는 것으로 결정하는 네트워크 장치.

[청구항 29] 제24항에 있어서,
상기 컨텐츠 요청 메시지는,
컨텐츠 이름, 컨텐츠 내용, 컨텐츠 네트워크의 도메인 이름, 컨텐츠 네트워크의 도메인 구조, 및 특정 컨텐츠 네트워크의 도메인에 포함된 컨텐츠 리스트 중 적어도 하나를 포함하는 네트워크 장치.

[청구항 30] 제16항에 있어서,
상기 컨텐츠 이름은,
컨텐츠 네트워크의 도메인 이름, 컨텐츠의 고유 이름, 컨텐츠의 버전 정보, 상기 컨텐츠 보호 정보, 및 세그먼트 정보 중 적어도 하나를 포함하는 네트워크 장치.

[청구항 31] 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신하는 단계;
및
컨텐츠 보호 정보에 기초하여 설정된 태그 정보를 이용하여 상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계
를 포함하고,
상기 컨텐츠 보호 정보는, 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함하는 컨텐츠 보호 방법.

[청구항 32] 제31항에 있어서,

상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계는,
상기 컨텐츠 요청 메시지가 가리키는 컨텐츠의 저장 여부를 확인하는 단계; 및
상기 컨텐츠가 저장되지 않은 것으로 확인됨에 따라, 상기 컨텐츠 보호 정보에 기초하여 상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계
를 포함하는 컨텐츠 보호 방법.

[청구항 33] 제32항에 있어서,
상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계는,
상기 컨텐츠가 저장되지 않은 것으로 확인됨에 따라, 상기 컨텐츠 요청 메시지를 팬딩 인터레스트 테이블에 기록하는 컨텐츠 보호 방법.

[청구항 34] 제31항에 있어서,
상기 태그 정보는,
상기 마킹 정보에 따라 상기 컨텐츠가 보호 컨텐츠인지 여부가 설정된 정보인 컨텐츠 보호 방법.

[청구항 35] 제34항에 있어서,
상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계는,
상기 태그 정보에 기초하여 상기 컨텐츠가 보호 컨텐츠로 설정된 것으로 결정됨에 따라, 상기 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달하지 않는 컨텐츠 보호 방법.

[청구항 36] 제34항에 있어서,
상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 단계는,
상기 태그 정보에 기초하여 상기 컨텐츠가 보호 컨텐츠로 설정되지 않은 것으로 결정됨에 따라, 상기 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달하는 컨텐츠 보호 방법.

[청구항 37] 컨텐츠의 전달을 요청하는 컨텐츠 요청 메시지를 수신하는 메시지 수신부; 및
컨텐츠 보호 정보에 기초하여 설정된 태그 정보를 이용하여 상기 컨텐츠 요청 메시지의 전달 여부를 결정하는 결정부
를 포함하고,
상기 컨텐츠 보호 정보는, 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함하는 네트워크 장치.

[청구항 38] 제37항에 있어서,
상기 결정부는,
상기 컨텐츠 요청 메시지가 가리키는 컨텐츠의 저장 여부를 확인하는 확인부; 및

상기 컨텐츠가 저장되지 않은 것으로 확인됨에 따라, 상기 컨텐츠 보호 정보와 전달 정보 베이스(Forwarding Information Base: FIB)에 기록되어 있는 정책 정보에 기초하여 상기 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달할지 여부를 결정하는 전달 결정부를 포함하는 네트워크 장치.

[청구항 39] 제38항에 있어서,
상기 전달 결정부는,
상기 컨텐츠가 저장되지 않은 것으로 확인됨에 따라, 상기 컨텐츠 요청 메시지를 팬딩 인터레스트 테이블에 기록하는 네트워크 장치.

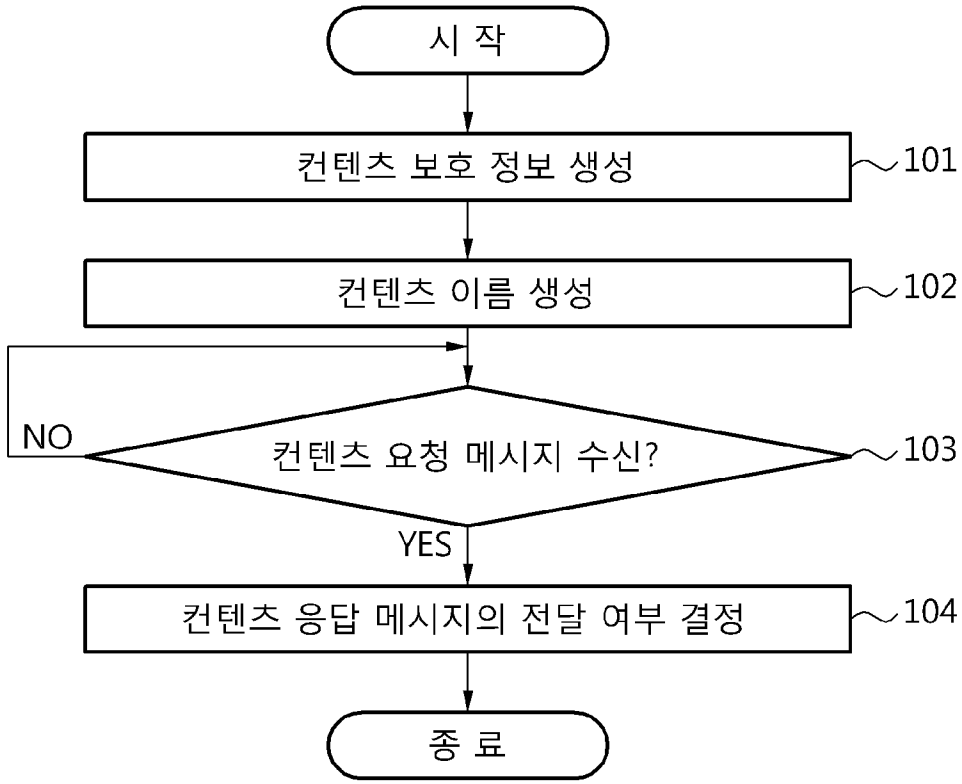
[청구항 40] 제37항에 있어서,
상기 태그 정보는,
상기 마킹 정보에 따라 상기 컨텐츠가 보호 컨텐츠 인지 여부가 설정된 정보인 네트워크 장치.

[청구항 41] 제40항에 있어서,
상기 전달 결정부는,
상기 태그 정보에 기초하여 상기 컨텐츠가 보호 컨텐츠로 설정된 것으로 결정됨에 따라, 상기 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달하지 않는 네트워크 장치.

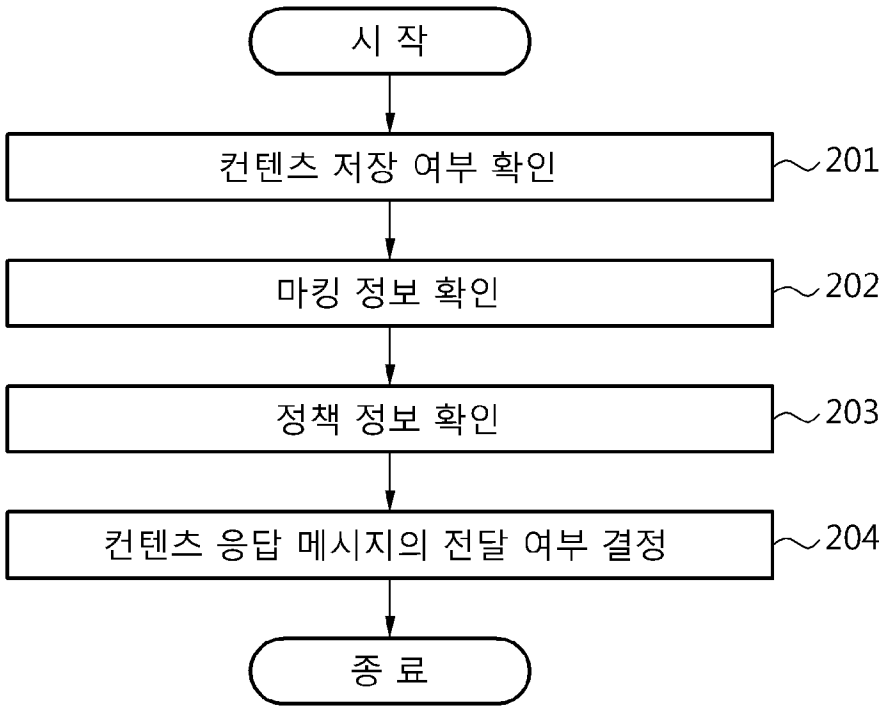
[청구항 42] 제40항에 있어서,
상기 전달 결정부는,
상기 태그 정보에 기초하여 상기 컨텐츠가 보호 컨텐츠로 설정되지 않은 것으로 결정됨에 따라, 상기 컨텐츠 요청 메시지를 다음 네트워크 장치로 전달하는 네트워크 장치.

[청구항 43] 컨텐츠의 보호 여부를 나타내는 마킹 정보, 및 상기 컨텐츠의 공개 범위를 나타내는 정책 정보 중 적어도 하나를 포함하는 컨텐츠 보호 정보를 생성하는 단계; 및
상기 컨텐츠 보호 정보에 기초하여 컨텐츠 요청 메시지에 대응하는 컨텐츠 응답 메시지의 전달 여부를 결정하는 단계를 포함하는 컨텐츠 보호 방법.

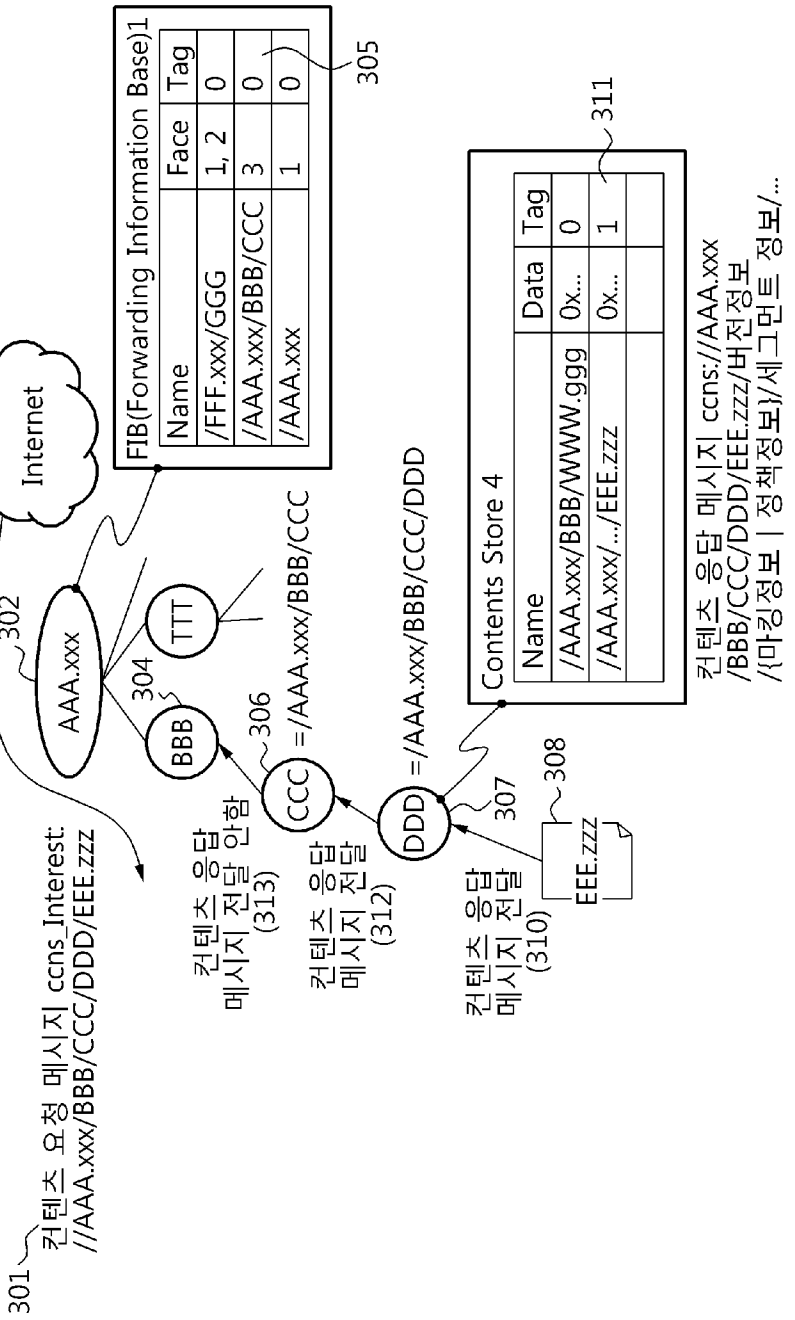
[Fig. 1]


시 작
컨텐츠 보호 정보 생성
101
컨텐츠 이름 생성
102
NO
컨텐츠 요청 메시지 수신?
103
YES
컨텐츠 응답 메시지의 전달 여부 결정
104
종 료

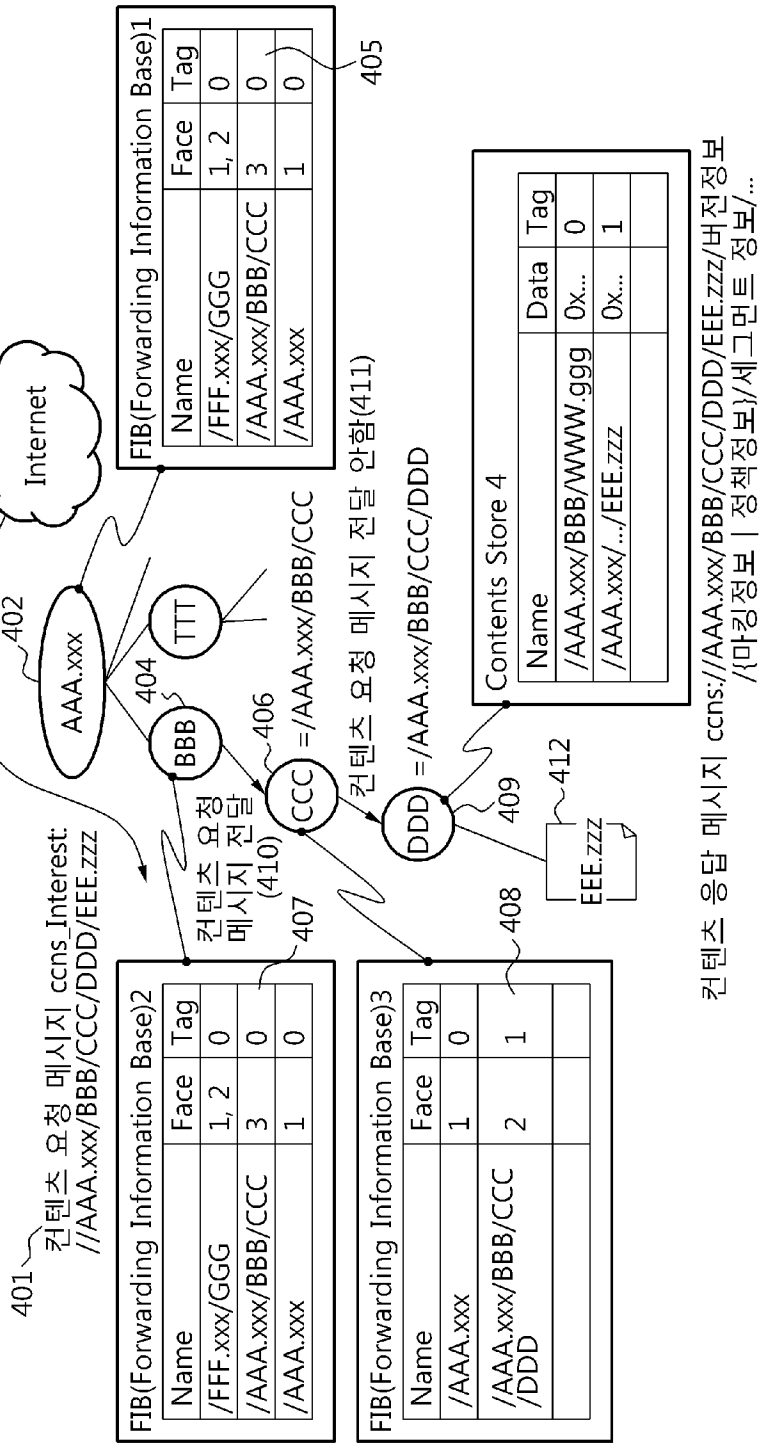
[Fig. 2]


시 작
컨텐츠 저장 여부 확인
201
마킹 정보 확인
202
정책 정보 확인
203
컨텐츠 응답 메시지의 전달 여부 결정
204
종 료

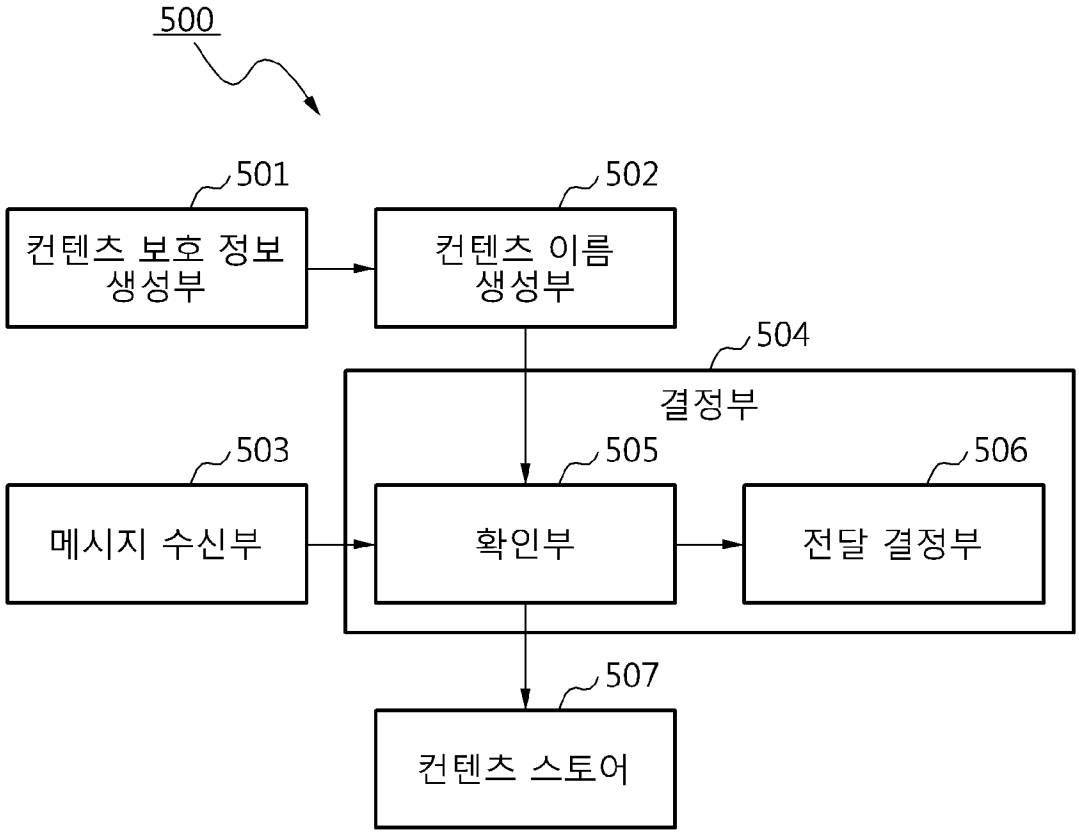
[Fig. 3]


303
Internet
302
AAA.xxx
304
BBB
TTT
306
CCC =/AAA.xxx/BBB/CCC
DDD =/AAA.xxx/BBB/CCC/DDD
307
308
EEE.zzz
301
컨텐츠 요청 메시지 ccns_Interest:
//AAA.xxx/BBB/CCC/DDD/EEE.zzz
컨텐츠 응답
메시지 전달 안함
(313)
컨텐츠 응답
메시지 전달
(312)
컨텐츠 응답
메시지 전달
(310)
FIB(Forwarding Information Base)1
Name | Face | Tag
/FFF.xxx/GGG | 1, 2 | 0
/AAA.xxx/BBB/CCC | 3 | 0
/AAA.xxx | 1 | 0
305
Contents Store 4
Name | Data | Tag
/AAA.xxx/BBB/WWW.ggg | 0x... | 0
/AAA.xxx/.../EEE.zzz | 0x... | 1
311
컨텐츠 응답 메시지 ccns://AAA.xxx
/BBB/CCC/DDD/EEE.zzz/버전정보
/{마킹정보 | 정책정보}/세그먼트 정보/...

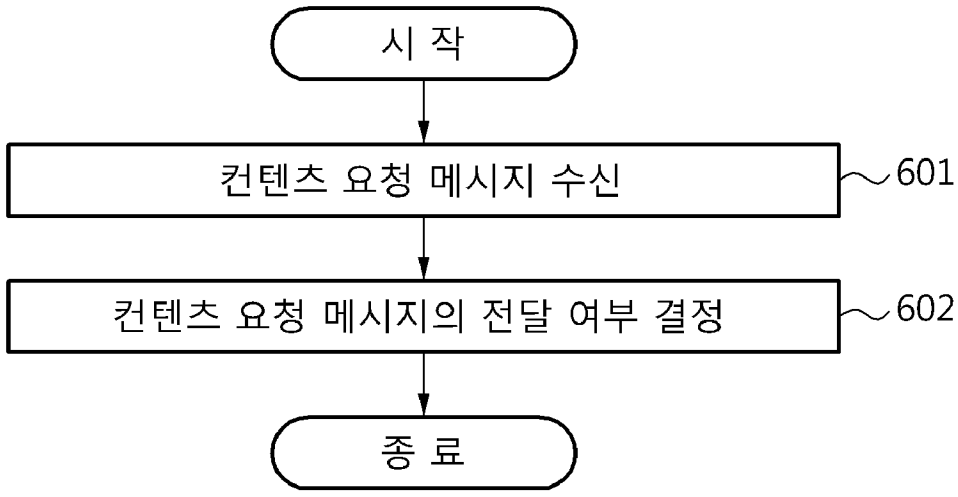
[Fig. 4]


403
Internet
402
AAA.xxx
TTT
404
BBB
406
CCC
=/AAA.xxx/BBB/CCC
DDD
=/AAA.xxx/BBB/CCC/DDD
409
412
EEE.zzz
408
407
401
컨텐츠 요청 메시지 ccns_Interest:
//AAA.xxx/BBB/CCC/DDD/EEE.zzz
컨텐츠 요청 메시지 전달
(410)
컨텐츠 요청 메시지 전달 안함(411)
405
FIB(Forwarding Information Base)1
Name | Face | Tag
/FFF.xxx/GGG | 1, 2 | 0
/AAA.xxx/BBB/CCC | 3 | 0
/AAA.xxx | 1 | 0
FIB(Forwarding Information Base)2
Name | Face | Tag
/FFF.xxx/GGG | 1, 2 | 0
/AAA.xxx/BBB/CCC | 3 | 0
/AAA.xxx | 1 | 0
FIB(Forwarding Information Base)3
Name | Face | Tag
/AAA.xxx | 1 | 0
/AAA.xxx/BBB/CCC/DDD | 2 | 1
Contents Store 4
Name | Data | Tag
/AAA.xxx/BBB/WWW.ggg | 0x... | 0
/AAA.xxx/.../EEE.zzz | 0x... | 1
컨텐츠 응답 메시지 ccns://AAA.xxx/BBB/CCC/DDD/EEE.zzz/버전정보
/{마킹정보 | 정책정보}/세그먼트 정보/...

[Fig. 5]


500
501
컨텐츠 보호 정보 생성부
502
컨텐츠 이름 생성부
504
결정부
503
메시지 수신부
505
확인부
506
전달 결정부
507
컨텐츠 스토어

[Fig. 6]


시 작
컨텐츠 요청 메시지 수신
601
컨텐츠 요청 메시지의 전달 여부 결정
602
종 료

[Fig. 7]