(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0018678
(43) 공개일자 2013년02월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *G06F 15/16* (2006.01)
G06F 17/00 (2006.01)
(21) 출원번호 10-2012-7023108
(22) 출원일자(국제) 2011년03월02일
심사청구일자 없음
(85) 번역문제출일자 2012년09월04일
(86) 국제출원번호 PCT/US2011/026898
(87) 국제공개번호 WO 2011/109543
국제공개일자 2011년09월09일
(30) 우선권주장
12/718,843 2010년03월05일 미국(US)

(71) 출원인
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
파나슈크 아나톨리
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
바블라니 기리쉬
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(뒷면에 계속)
(74) 대리인
제일특허법인

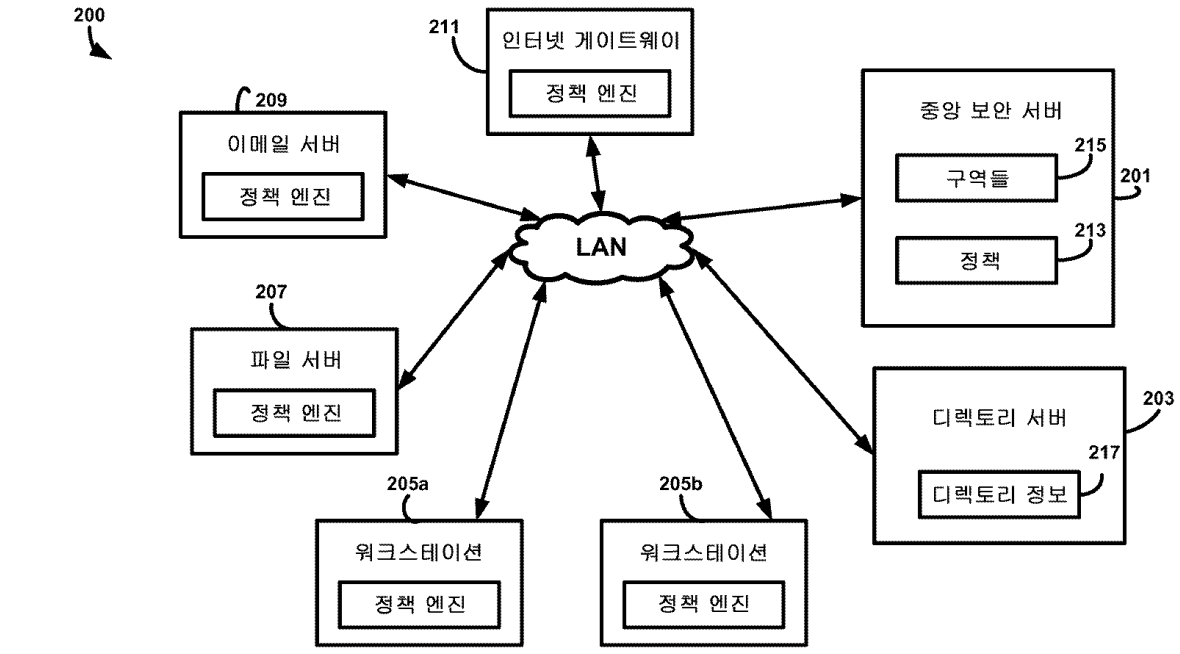
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **구역들을 이용한 정보 보호**

(57) 요 약

일부 실시예들은 정보 공간 내에 있는 장치들, 사용자들, 및 도메인들이 구역들로 그룹화될 수 있는 정보 보호 방안에 관한 것이다. 정보가 어떤 구역의 경계를 지나 전달될 때, 전달이 허용되어야 할지, 차단되어야 할지 여부 및/또는 어떤 다른 정책적 조치들이 취해져야 할지 여부(예를 들어, 암호화 요구, 사용자에게 계획된 전달에 대한 승인 촉구, 또는 어떤 다른 조치)를 결정하기 위해 정보 보호 규칙들이 적용될 수 있다.

대 표 도



(72) 발명자

맥콜간 찰스

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

파르사사라시 크리쉬나 쿠마르

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

특허청구의 범위

청구항 1

적어도 한 개의 프로세서 및 적어도 한 개의 유형의 메모리를 포함하는 컴퓨터에 의해 수행되는 정보 보호를 위한 방법 - 상기 컴퓨터는 복수의 사용자, 장치, 및/또는 도메인의 구역을 포함하는 정보 공간 안에서 동작하며, 상기 복수의 구역 각각은 사용자, 장치, 및/또는 도메인의 논리적 그룹임 - 으로서,

정보의 전달의 개시에 대응하여, 상기 정보의 전달이 상기 정보가 상기 복수의 구역 중 둘 사이의 구역 경계를 지나게 할 것인지 여부를 판단하는 단계,

상기 전달이 상기 정보가 상기 구역 경계를 지나게 하지 않을 것이라고 판단될 경우, 상기 전달을 허용하는 단계,

상기 전달이 상기 정보가 상기 구역 경계를 지나게 할 것이라고 판단될 경우:

정보 보호 규칙을 액세스하는 단계,

정책적 조치가 수행되어야 할지 여부를 결정하기 위해 상기 정보 보호 규칙을 상기 전달에 적용하는 단계, 및

상기 정책적 조치가 수행되어야 한다고 결정될 경우, 상기 정책적 조치를 수행하는 단계를 포함하는

방법.

청구항 2

제1항에 있어서,

상기 정보의 전달이 상기 정보가 구역 경계를 지나게 할 것인지 여부를 판단하는 단계는

보안 서버로부터, 상기 복수의 구역 중 상기 전달을 개시한 사용자나 장치가 그룹화되는 제1구역 및 상기 복수의 구역 중 상기 정보의 전달의 의도된 수신자인 사용자나 장치가 그룹화는 제2구역을 나타내는 구역 정보를 수신하는 단계를 더 포함하는

방법.

청구항 3

제2항에 있어서,

상기 보안 서버는 상기 컴퓨터와 별개의 장치인

방법.

청구항 4

제2항에 있어서,

상기 복수의 구역 중 상기 제1구역 및 상기 복수의 구역 중 상기 제2구역이 상기 복수의 구역 중 동일한 구역인지 여부를 판단하는 단계,

상기 복수의 구역 중 상기 제1구역 및 상기 복수의 구역 중 상기 제2구역이 상기 복수의 구역 중 동일한 구역이라고 판단될 경우, 상기 전달이 상기 정보가 상기 구역 경계를 지나게 하지 않을 것이라고 판단하는 단계, 및

상기 복수의 구역 중 상기 제1구역 및 상기 복수의 구역 중 상기 제2구역이 상기 복수의 구역 중 동일한 구역이 아니라고 판단될 경우, 상기 전달이 상기 정보가 상기 구역 경계를 지나게 할 것이라고 판단하는 단계를 더 포

함하는

방법.

청구항 5

제1항에 있어서,

상기 정보 보호 규칙을 액세스하는 단계는

상기 정보 보호 규칙을 저장한 보안 서버로부터 상기 정보 보호 규칙을 액세스하되, 상기 보안 서버는 상기 컴퓨터와 별개의 장치인 단계를 더 포함하는

방법.

청구항 6

적어도 한 개의 프로세서 및 적어도 한 개의 유형의 메모리를 포함하는 컴퓨터 상에서 실행될 때, 복수의 사용자, 장치, 및/또는 도메인의 구역을 포함하는 정보 공간에서 방법을 수행하는 명령어로 인코딩된 적어도 한 개의 컴퓨터 판독 가능 매체 - 상기 복수의 구역 각각은 사용자, 장치, 및/또는 도메인의 논리적 그룹이며, 상기 컴퓨터는 상기 복수의 구역 중 한 개로 그룹화됨 - 로서,

상기 방법은

상기 컴퓨터에서 문서를 생성하는 단계,

상기 문서에 대해 제1분류를 자동으로 결정하는 단계,

상기 결정된 제1분류를 식별하는 정보를 상기 문서 내에 삽입하는 단계,

상기 문서에 대해 제2분류를 식별하는 사용자 입력을 수신하는 단계,

상기 사용자 입력에 대응하여, 상기 문서로부터 상기 제1분류를 식별하는 정보를 제거하고 상기 제2분류를 식별하는 정보를 상기 문서 내에 삽입함으로써 상기 제2분류로 상기 제1분류를 무효화하는 단계를 포함하는

적어도 한 개의 컴퓨터 판독 가능 매체.

청구항 7

제6항에 있어서,

상기 문서에 대해 제1분류를 자동으로 결정하는 단계는 상기 컴퓨터가 그룹화되는 상기 복수의 구역 중 상기 한 개에 적어도 일부 기초해서 상기 제1분류를 결정하는 단계를 포함하는

적어도 한 개의 컴퓨터 판독 가능 매체.

청구항 8

제6항에 있어서,

상기 문서에 대해 제1분류를 자동으로 결정하는 단계는 상기 컴퓨터의 사용자가 그룹화되는 상기 복수의 구역 중 상기 한 개에 적어도 일부 기초해서 상기 제1분류를 결정하는 단계를 포함하는

적어도 한 개의 컴퓨터 판독 가능 매체.

청구항 9

제6항에 있어서,

상기 문서에 대해 제1분류를 자동으로 결정하는 단계는 상기 문서의 콘텐츠에 적어도 일부 기초해서 상기 제1분류를 결정하는 단계를 포함하는

적어도 한 개의 컴퓨터 판독 가능 매체.

청구항 10

컴퓨터 시스템 내 컴퓨터로서,

적어도 한 개의 유형의 메모리, 및

프로세서 실행 가능 명령어를 실행하는 적어도 한 개의 하드웨어 프로세서를 포함하며, 상기 명령어는

사용자, 장치, 및/또는 도메인을 논리적 구역으로 그룹화하는 제1정보의 사용자 입력에 대응하여, 상기 제1정보를 상기 적어도 한 개의 유형의 메모리에 저장하며,

상기 정보가 논리적 구역 사이의 경계를 지나게 할 정보의 전달의 개시에 대응하여 적용될 정보 보호 규칙을 특정하는 제2정보의 사용자 입력에 대응하여, 상기 제2정보를 상기 적어도 한 개의 유형의 메모리에 저장하는 것인

컴퓨터.

명 세 서

배 경 기 술

[0001] 조직 내에서 정보는 빈번하게 생성되며 공유된다. 예를 들어, 작업자들은 조직 내 다른 작업자들과 조직 밖의 사람들 양방에게 이메일을 작성하여 전송한다. 또한, 작업자들은 문서들을 생성하고, 그 문서들을 내부 파일 서버들로 업로드하고, 그것들을 휴대형 저장 매체(예를 들어, 착탈 가능 플래시 메모리 드라이브들)로 전달하며, 그것들을 조직 밖의 다른 사용자들에게 전송한다.

[0002] 조직 내 작업자들에 의해 생성된 정보의 일부는 기밀이거나 민감한 것일 수 있다. 따라서, 그러한 정보를 보유한 작업자들이 오로지 정보 액세스 권한이 있는 사람들하고만 정보를 공유하게 하며/하거나, 작업자들이 그러한 정보를 액세스 권한이 없는 어떤 사람에게 우발적으로 전달하는 위험을 줄이는 것이 요망될 수 있다.

발명의 내용

과제의 해결 수단

[0003] 발명자들은 정보가 공유될 때 정보 액세스 권한이 없거나 정보에 액세스하도록 의도되지 않은 어떤 사람에게 종종 정보가 전송되거나 정보에 액세스할 권한이 없는 어떤 사람에 의해 악의적으로 탈취될 수 있다는 것을 인식해 왔다.

[0004] 따라서, 일부 실시예들은 정보 공간 내 장치들, 사용자들 및 도메인들이 구역들로 그룹화될 수 있는 정보 보호 방안에 관한 것이다. 정보가 어떤 구역의 경계를 지나 전달될 때, 전달이 허용되어야 할지 또는 차단되어야 할지 여부, 및/또는 어떤 다른 정책적 조치들이 취해져야 할지 여부(예를 들어, 암호화 요구, 사용자에게 의도된 전달에 대한 승인 촉구, 또는 어떤 다른 조치)를 결정하기 위해 정보 보호 규칙들이 적용될 수 있다.

[0005] 일 실시예는 적어도 한 개의 프로세서 및 적어도 한 개의 유형의 메모리를 포함하는 컴퓨터에 의해 수행되는 정보 보호 방법에 관한 것으로서, 컴퓨터는 복수의 사용자들, 장치들, 및/또는 도메인들의 구역들을 포함하는 정보 공간 안에서 동작하고, 복수의 구역들 각각은 사용자들, 장치들, 및/또는 도메인들의 논리적 그룹이며, 상기 방법은 정보의 전달의 개시에 응답하여, 정보의 전달이 정보가 복수의 구역들 중 둘 사이의 구역 경계를 지나게 하는 것인지 여부를 판단하는 단계; 전달이 정보가 구역 경계를 지나게 하지 않을 것이라고 판단될 때, 전달을 허용하는 단계; 전달이 정보가 구역 경계를 지나게 하는 것이라고 판단될 때, 정보 보호 규칙들을 액세스하는

단계; 정책적 조치가 수행되어야 할지 여부를 판정하기 위해 정보 보호 규칙들을 전달에 적용하는 단계; 및 정책적 조치가 수행되어야 한다고 결정될 때, 정책적 조치를 수행하는 단계를 포함한다.

[0006] 또 다른 실시예는 적어도 한 개의 프로세서 및 적어도 한 개의 유형의 메모리를 포함하는 컴퓨터 상에서 실행될 때 복수의 사용자들, 장치들, 및/또는 도메인들의 구역들을 포함하는 정보 공간 안에서 방법을 수행하는 명령어들로 부호화된 적어도 한 개의 컴퓨터 판독 가능 매체에 관한 것으로서, 복수의 구역들 각각은 사용자들, 장치들, 및/또는 도메인들의 논리적 그룹이고, 컴퓨터는 복수의 구역들 중 하나로 그룹화되며, 상기 방법은 컴퓨터에서 문서를 생성하는 단계; 문서에 대해 제1분류를 자동으로 결정하는 단계; 결정된 제1분류를 식별하는 정보를 문서 안에 삽입하는 단계; 문서에 대해 제2분류를 식별하는 사용자 입력을 수신하는 단계; 사용자 입력에 대응하여, 문서로부터 제1분류를 식별하는 정보를 제거하며 제2분류를 식별하는 정보를 문서 안에 삽입함으로써 제2분류로 제1분류를 무효화하는 단계를 포함한다.

[0007] 또 다른 실시예는 적어도 한 개의 유형의 메모리; 및 프로세서 실행 가능 명령어들을 실행하는 적어도 한 개의 하드웨어 프로세서를 포함하는 컴퓨터 시스템 내 컴퓨터에 관한 것으로서, 상기 명령어들은 사용자들, 장치들, 및/또는 도메인들을 논리적 구역들로 그룹화하는 제1정보의 사용자 입력에 대응하여, 제1정보를 적어도 한 개의 유형의 메모리에 저장하며, 정보가 논리적 구역들 사이의 경계를 가로지르게 할 정보의 전달의 개시에 대응하여 적용될 정보 보호 규칙들을 특정하는 제2정보의 사용자 입력에 대응하여, 제2정보를 적어도 한 개의 유형의 메모리에 저장하는 것이다.

도면의 간단한 설명

[0008] 첨부된 도면들은 축척에 맞게 도시되도록 의도된 것이 아니다. 도면에서, 다양한 도면에 도시된 각각의 동일하거나 거의 동일한 구성요소는 동일한 참조부호를 통해 표시된다. 명료성을 위해, 모든 도면에서 모든 구성요소에 참조번호가 부여되지 않을 수 있다.

도 1은 일부 실시예들에 따라 복수의 구역들로 논리적으로 분할된 정보 공간의 블록도이다.

도 2는 본 발명의 실시예들의 정보 보호 기법들이 구현될 수 있는 컴퓨터 시스템의 블록도이다.

도 3은 일부 실시예들에 따라 복수의 구역들로 논리적으로 분할된 정보 공간에서 정보 보호를 지원하기 위한 프로세스의 흐름도이다.

도 4는 일부 실시예들의 양태들이 구현될 수 있는 컴퓨터 시스템의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0009] 발명자들은 조직 내 작업자들이 기밀이거나 민감한 전자 정보를 생성하며/하거나 액세스할 때, 작업자들이 무심코 혹은 악의적으로 그 정보의 보안을 위태롭게 하는 상황들이 일어날 수 있다는 것을 인식해왔다. 예를 들어, 어떤 작업자가 전자 정보를 그 정보를 액세스할 권한이 없는 어떤 사람에게 본의 아니게 전송하거나, 안전하지 않은 장소(예를 들어, 정보를 액세스할 권한이 없는 어떤 사람이 액세스할 수 있는 파일 서버)에 그 전자 정보를 저장할 수 있다. 또 다른 예로서, 작업자가 기밀 전자 정보를 (암호화하기보다) 평문으로 공유함으로써 그 정보를 정보 액세스 권한이 없는 어떤 사람이 가로채게 하는 보다 큰 위험에 그 정보가 놓여지게 하거나, 정보의 보안을 위태롭게 하는 다른 조치들을 취할 수 있다.

[0010] 따라서, 일부 실시예들은 사용자들 및 장치들이 "구역들(zones)"이라 불리는 논리적 그룹들로 분할되는 컴퓨터 시스템에 관한 것이다. 전자 정보가 한 구역 안의 사용자나 장치로부터 다른 구역 안의 사용자나 장치에게 전달될 때, 그 정보는 구역의 경계를 지났다고 간주된다. 정보가 구역의 경계를 지나게 하는 정보의 전달이 개시될 때, 그 전달이 허용되는지 여부나 전달이 허용되기 전에 어떤 조치(예를 들어, 작업자가 전달을 개시하도록 촉구하는 것, 전달을 감사 로깅(audit logging)하는 것, 전달을 허용하기 전에 정보의 암호화를 요구하는 것, 또는 어떤 다른 조치)가 취해져야 하는지 여부를 결정하기 위해 정보 제어 규칙들이 적용될 수 있다.

[0011] 일부 실시예들에서, 정보 제어 규칙들은 전달되는 정보의 타입을 고려할 수 있다. 예를 들어, 기밀 정보를 제1구역에서 제2구역으로 전달하고자 할 때 비기밀 정보를 제1구역에서 제2구역으로 전달하고자 할 때와는 다른 정보 제어 규칙들이 적용될 수 있다. 따라서, 일부 실시예들에서 전자 정보가 생성될 때, 그것에 정보의 민감도 및/또는 정보의 다른 특성들을 가리키는 분류가 (예를 들어, 자동적으로나, 반자동적으로나, 수동적으로) 태깅될 수 있다. 분류 규칙들은 전자 정보의 분류, 및 정보가 구역의 경계를 지나 전달되도록 시도될 때 정보가 전

달되는 구역을 고려할 수 있다.

[0012] 이러한 기법은 다수의 이점을 제공할 수 있다. 첫째, 그것은 일정한 보안 정책이 규정되게 하고 각종 다양한 채널들에 걸쳐 적용될 수 있게 한다. 즉, 동일한 분류 규칙들의 집합이 이메일 전달, 월드 와이드 웹을 통한 콘텐츠 전달, 조직 내부의 파일 서버로의 파일 전달, 및/또는 어떤 다른 타입의 전자 정보나 정보 채널에 적용될 수 있다. 둘째, 그것은 민감하거나 기밀 정보에 대해 보장될 수 있는 규칙들의 제한적인 집합이 그러한 규칙들의 제한적인 집합이 보장되지 않는 정보에 적용될 필요가 없도록, 정보 제어 규칙들이 적용되는 정보의 타입에 기초해서 정보 제어 규칙들이 맞춤화될 수 있게 한다.

[0013] 선행 기술의 여러 문제 및 상기 논의된 기법들에 의해 제공되는 여러 이점이 위에서 확인되었다. 그러나, 본 발명은 그러한 문제들 전체나 어느 한 가지에 대처하거나 그러한 이점들 전체나 어느 한 가지를 제공하는 데 국한되지 않는다. 즉, 일부 실시예들이 그러한 문제들의 일부나 전체에 대처하며 그러한 이점들의 일부나 전체를 제공할 수 있는 한편, 일부 실시예들은 그러한 문제들 중 어느 하나에 대처하거나 그러한 이점들 중 어느 하나를 제공하지 못할 수 있다.

[0014] 도 1은 구역들로 분류될 수 있는 정보 공간의 예를 도시한다. 도 1에 도시된 바와 같이, 조직(100)은 다수의 장치들을 포함하는 컴퓨터 시스템을 가질 수 있다. 그 장치들 중 일부는 조직의 엔지니어링 부서에 의해 사용될 수 있으며, 일부는 PR(public relations) 부서에 의해 사용될 수 있다. 엔지니어링 부서로부터의 문서들이나 다른 콘텐츠 부분들이 상당량의 기밀 및/또는 민감한 정보를 포함할 가능성이 높은 한편, PR 부서에서 생성된 문서들이나 다른 콘텐츠 부분들은 그러한 정보를 포함할 가능성이 적으므로, 엔지니어링 부서에 의해 사용되는 장치들이 하나의 구역으로 그룹화되며 PR 부서에 의해 사용되는 장치들은 다른 구역으로 그룹화될 수 있다. 따라서, 도 1에 도시된 바와 같이, 조직 내 모든 장치들은 LAN(local area network)(125)을 통해 물리적으로 연결되지만, 엔지니어링 파일 서버(103), 엔지니어링 이메일 서버(105), 및 워크 스테이션들(107a, 107b, 및 107c)은 엔지니어링 부서 구역(101)으로 논리적으로 그룹화될 수 있는 한편, PR 파일 서버(109), PR 이메일 서버(111), 및 워크 스테이션들(113a, 113b, 및 113d)은 PR 부서 구역(115)으로 함께 논리적으로 그룹화된다.

[0015] 또한, 도 1의 예에서 조직(100) 외부에 있는 조직(121)이 한 구역으로 논리적으로 그룹화될 수 있다. 예를 들어, 조직(121)이 조직(100)의 신뢰하는 파트너라면, 다른 정보 제어 규칙들을 조직(121)에 적용하는 것이 요망되며, 그 결과 (예를 들어, 인터넷(117)을 통해) 조직(121)으로 전송되고 그로부터 수신되는 정보가 조직(100) 밖에 있는 다른 개체들의 정보와는 다르게 취급된다. 따라서, 조직(121)은 신뢰하는 파트너 구역(119)으로 논리적으로 그룹화될 수 있지만, (예를 들어, 인터넷(117)을 통해) 조직(100) 외부의 다른 개체들로 전송되며 그로부터 수신되는 정보는 일반 인터넷 구역(123)으로 전송되며 그로부터 수신되는 것으로 취급될 수 있다. 위에서 논의되는 바와 같이, 정보가 한 구역에서 다른 구역으로 전송될 때, 정보 보호 규칙들이 적용될 수 있으며, 보증되는 경우 그 정보 보호 규칙들에 기초하여 조치가 취해질 수 있다.

[0016] 도 1의 예에서, 조직(100) 안의 장치들은 두 개의 구역으로 논리적으로 그룹화된다. 조직은 어떤 적절한 개수의 구역들을 포함할 수 있으므로 이것은 단지 예시적인 것이라는 점이 이해되어야 한다. 예를 들어, 조직 내의 모든 장치들과 사용자들이 한 개의 구역으로 그룹화되거나, 그러한 장치들과 사용자들이 셋 이상의 여러 구역으로 그룹화될 수도 있다. 또한, 도 1의 예에서는, 장치들만이 구역으로 논리적으로 그룹화되는 것으로 도시된다. 그러나, 사용자들(예를 들어, 조직(100)의 피고용자들, 다른 작업자들, 또는 다른 사람들)이나 도메인들 역시 구역으로 논리적으로 그룹화될 수 있다. 예를 들어, 엔지니어링 부서에서 일하는 조직(100)의 피고용자들은 엔지니어링 부서 구역(101)으로 그룹화될 수 있으며, PR 부서 안에서 일하는 피고용자들은 PR 부서 구역(115)으로 그룹화될 수 있다.

[0017] 따라서, 발명자들은 한 구역으로 그룹화되는 사용자가 다른 구역으로 그룹화되는 장치를 사용하는 상황이 일어날 수 있다는 것을 인식해왔다. 그러므로, 사용자가 그 장치로부터 정보를 전송하거나 그 장치에서 정보를 수신할 때, 정보는 사용자의 구역이나 장치의 구역으로부터 전송되거나 수신된 것으로서 취급될 수 있다. 그에 따라, 예컨대 엔지니어링 구역으로 그룹화된 엔지니어링 부서의 어떤 피고용자가 PR 부서 구역으로 그룹화된 워크스테이션(113a)에 로그인하여 작업하는 경우, 그 피고용자는 엔지니어링 파일 서버(103)로 문서를 업로드하려고 시도할 수 있다. 이 문서는 엔지니어링 부서 구역이나 PR 부서 구역으로부터 보내진 것으로 취급될 수 있다.

[0018] 일부 실시예들에서, 사용자의 구역이 사용자가 사용하고 있는 장치의 구역보다 우선할 수 있다. 따라서, 상기 예에서 엔지니어링 부서의 피고용자가 워크스테이션(113a)으로부터 엔지니어링 파일 서버(103)로 문서를 업로드할 때, 그 문서는 엔지니어링 부서 구역으로부터 엔지니어링 부서 구역으로 보내지는 것으로(즉, 구역의 경계를

지나지 않는 것으로) 취급될 수 있다. 그러나, 본 발명은 어떤 실시예들에서는 장치의 구역이 그 장치를 사용하는 사용자의 구역에 우선할 수 있으며 어떤 실시예들에서는 사용자의 구역이 우선할지 장치의 구역이 우선할지 여부가 조직의 관리자에 의해 설정될 수 있으므로 그 점에 국한되는 것은 아니다.

[0019] 위에서 논의된 바와 같이, 정보 보호 규칙들은 정보가 구역의 경계를 지나 전달될 때 정보가 전달되고 있는 구역, 정보를 전달하고 있는 구역, 및 전달되고 있는 정보의 분류에 기초하여 조치가 수행되어야 하는지 여부 및 어떤 조치들이 수행되어야 하는지를 규정할 수 있다. 정보는 다양한 방식들 중 어느 하나에 따라 분류될 수 있으며, 정보의 분류는 정보 생성 및 공유 프로세스 시 다양한 시점들 중 어느 한 시점에서 수행될 수 있다. 예를 들어, 분류는 자동적으로나 반자동적으로나 수동적으로 수행될 수 있고, 정보가 생성될 때, 정보가 저장될 때, 정보가 전달될 때, 및/또는 어떤 다른 적절한 시점에 수행될 수 있다.

[0020] 예를 들어, 일부 실시예들에서, 문서(예를 들어, 이메일이나 다른 문서)를 생성하기 위한 응용 프로그램이 사용될 때, 그 응용 프로그램은 문서를 자동으로 분류할 수 있다. 응용 프로그램은 어떤 적절한 기준들이나 기준에 기초하여 문서를 분류할 수 있다. 예를 들어 응용 프로그램은 사용자 및/또는 장치가 그룹화되어 있던 구역에 기초하거나 문서 내 키워드들이나 패턴들에 기초하여 문서를 자동으로 분류할 수 있다. 따라서, 예를 들어 텍스트의 어떤 키워드들이나 패턴들을 포함하는 문서들에 소정 분류들이 할당될 수 있다. 일부 실시예들에서 문서들은 해시 함수(예를 들어, SHA1이나 어떤 다른 적절한 해시 함수)를 이용하여 문서를 해싱하고, 해시 값을 저장된 해시 값들의 집합과 비교하며, 비교결과에 기초하여 문서들에 분류를 할당함으로써 분류될 수 있다. 일부 실시예들에서 문서들은 유사도 검출을 위해 문서들(또는 문서들의 일부)에 대한 퍼지(fuzzy) 해싱을 나타내기 위해 쉥글링(shingling) 기법들을 이용하는 퍼지 매칭을 이용하여 분류될 수 있다. 일부 실시예들에서, 문서는 문서가 생성되었던 템플릿에 기초해서 분류되거나, 문서를 생성하거나 편집하는데 사용되는 그 응용 프로그램과 관련된 디폴트 분류나 어떤 다른 디폴트 분류를 할당받을 수 있다. 응용 프로그램은 문서가 문서의 최초 생성시, 문서가 저장될 때마다, 문서가 완성될 때, 및/또는 어떤 다른 적절한 시점에 분류될 수 있다.

[0021] 일부 실시예들에서는 문서를 생성하는 데 사용되는 응용 프로그램이 분류를 수행하는 것 대신, 혹은 그에 더하여 문서를 생성하는데 사용된 컴퓨터 상에서 실행되는 정보 보호 에이전트나 다른 소프트웨어 프로그램에 의해 분류가 수행될 수 있다. 그러한 소프트웨어 프로그램은 위에서 논의된 기준들 중 어느 하나(또는 기준들의 어떤 조합)에 기초하여 문서의 분류를 수행할 수 있으며, 문서의 최초 생성 후 어떤 적절한 시점에 문서의 분류를 수행할 수 있다. 예를 들어, 그러한 에이전트나 다른 소프트웨어 프로그램은 배경 프로세스로서 컴퓨터 상에 저장된 문서들을 분류하거나, 컴퓨터 외부에서 문서들의 전달의 개시에 따라 문서들을 분류하거나, 어떤 다른 적절한 시점에 분류할 수 있다.

[0022] 위의 예들에서, 문서들은 그들이 생성된 컴퓨터 상에서 분류된다. 그러나, 일부 실시예들에서 문서를 수신하는 개체에 의해 문서가 분류될 수 있으므로 본 발명이 그러한 점에 국한되는 것은 아니다. 예를 들어, 문서가 전달되는 경우, 그 문서를 수신하는 장치가 예컨대 전달이 허용되어 완료되어야 하는지, 허용되지 않고 중단되어야 하는지 여부를 결정하기 위한 정보 제어 규칙들을 적용하기 전에 문서의 분류를 수행할 수 있다. 예를 들어, 워크스테이션 상에서 실행되는 이메일 클라이언트는 의도된 수신자들에게로의 전달을 위해 조직 내 이메일 서버로 이메일을 전송할 수 있다. 일부 실시예들에서, 이메일 서버는 그 이메일의 분류를 수행할 수 있다. 또한, 조직 밖의 개체로부터 수신된 이메일들이나 다른 문서들은 그들이 조직 내 어떤 장치에 의해 수신될 때까지 분류되지 않을 것이며, 이는 외부 개체들이 문서들을 분류하기 위해 동일한 정보 보호 모델을 사용하지 않을 것이기 때문이다. 따라서, 이 문서들에 대한 분류는 문서들이 조직 안에서 수신된 후에 수행될 수 있다. 예를 들어, 이메일 서버가 외부 발신자들로부터 수신된 이메일들의 분류를 수행할 수 있거나, 내부 파일 서버가 외부 발신자들로부터 업로드된 문서들의 분류를 수행할 수 있다.

[0023] 문서에 대한 알맞은 분류가 결정되면, 그 분류가 다양한 방식들 중 어느 하나를 통해 저장될 수 있다. 일부 실시예들에서, 분류는 문서 자체에 내장될 수 있다(예를 들어, 태그나 라벨로서). 예를 들어, 이메일에 대한 분류는 이메일 헤더 안에 내장될 수 있으며, 다른 타입의 문서에 대한 분류는 그 문서에 포함된 메타데이터 안에 내장될 수 있다.

[0024] 위에서 논의된 예들에서, 문서들의 분류는 자동적으로 수행된다. 그러나, 본 발명이 이 점에 국한되지 않으며, 이는 일부 실시예들에서 문서들의 분류는 문서에 분류가 자동으로 할당될 수 있지만 사용자가 그 자동 분류를 무효로 할 수 있으며 다른 분류를 그 문서에 할당하는 능력을 가지도록 반자동적으로 수행될 수 있기 때문이다.

[0025] 일부 실시예들에서, 어떤 사용자들이 문서들에 분류를 할당할 권한이 있으며 어떤 사용자들이 앞서 할당된 분류를 무효화하도록 허용되는지를 나타내는 정책들이 정의될 수 있다. 예를 들어, 일부 실시예들에서는 다음 사용

자가 최초 사용자의 관리자이거나 상사인 경우, 다음 사용자가 최초 사용자에 의해 앞서 할당된 분류를 무효화하도록 허용될 수 있다. 다음 사용자가 최초 사용자의 관리자이거나 상사인지 여부에 관한 판단은 예를 들어 디렉토리 서버의 디렉토리 정보에 저장된 조직 차트(org 차트)를 이용하여 이루어질 수 있다.

[0026] 일부 실시예들에서, 문서들의 분류는 사용자들이 각 문서에 할당되어야 할 분류를 수동적으로 특정하도록 수동으로 수행될 수 있다. 그러한 실시예들에서, 분류가 할당되었던 문서가 구역의 경계를 지나 전달되는 경우, 정보 보호 규칙들이 적용될 수 있도록 그 문서에 디폴트 분류가 할당될 수 있다.

[0027] 문서들을 분류하기 위한 어떤 적절한 분류 방식이 사용될 수 있다. 일부 실시예들에서, 문서에 할당되는데 사용 가능한 분류는 조직의 관리자에 의해 설정될 수 있다. 사용될 수 있는 분류의 예들로는 "회사 기밀", "개인", "기밀 아님", "금전적 데이터", 및/또는 어떤 다른 적절한 분류가 포함될 수 있다.

[0028] 도 2는 구역들 및 정보 분류에 기초하여 정보 보호 규칙들이 이용될 수 있는 조직에 대한 컴퓨터 시스템(200) 블록도이다. 컴퓨터 시스템(200)은 구역 정보(215) 및 정책 정보(213)를 저장하는 중앙 보안 서버(201)를 포함한다. 구역 정보(215)는 (예를 들어, 네트워크 관리자에 의해) 규정되어 있던 구역들 및 규정된 구역들 각각으로 그룹화된 장치들, 사용자들, 및/또는 도메인들을 가리킨다. 정책 정보(213)는 구역 경계를 지나 정보가 전달될 때 적용되어야 하는 정보 보호 규칙들(예를 들어, 관리자에 의해 규정되어 있던 규칙들)을 특정한다.

[0029] 컴퓨터 시스템(200)은 또한 디렉토리 정보(217)를 저장하는 디렉토리 서버(203)를 포함할 수 있다. 디렉토리 정보(217)는 컴퓨터 시스템의 사용자들 및 그 안의 장치들에 대한 정보를 포함한다. 또한, 디렉토리 정보는 조직 유닛들이나 사용자들과 장치들의 그룹들을 규정할 수 있다. 예를 들어, 디렉토리 정보(217)는 엔지니어링 부서의 사용자들 및/또는 장치들을 포함하는 "엔지니어링 그룹"을 규정할 수 있고, PR 부서의 사용자들 및/또는 장치들을 포함하는 "PR 그룹"을 규정할 수 있다.

[0030] 일부 실시예들에서, 디렉토리 정보(217)는 사용자들, 장치들, 및/또는 도메인들을 구역들로 그룹화하는데 사용될 수 있다. 예를 들어, 구역 정보(215)는 "엔지니어링 그룹" 내 모든 사용자나 장치가 "엔지니어링 부서" 구역으로 그룹화되고 "PR 그룹" 내 모든 사용자나 장치가 "PR 부서" 구역으로 그룹화됨을 나타내도록 구성될 수 있다.

[0031] 발명자들이 어떤 개체(예를 들어, 조직)가 컴퓨터 시스템(200)을 운영하는 조직 밖에 있을 때, 컴퓨터 시스템(200)의 관리자는 외부 조직의 사용자들 및 장치들을 식별하는디렉토리 정보에 액세스할 수 없다는 것을 인식해 왔다. 따라서, 외부 조직을 어떤 구역으로 그룹화하는 것이 요망되는 경우, 그 조직의 도메인 이름이 사용될 수 있다. 예를 들어, "Contoso, Inc."라는 이름의 외부 조직이 도메인 이름 "contoso.com"을 사용하며 이 조직을 어떤 구역(예를 들어, "신뢰하는 파트너" 구역)으로 그룹화하는 것이 요망하는 경우, 구역 정보는 도메인 이름 "contoso.com"을 이 구역에 속하는 것으로서 식별할 수 있다. 일부 실시예들에서, 디렉토리 정보(217)는 외부 개체들의 도메인 이름들을 포함하는 신뢰하는 파트너들의 그룹을 규정할 수 있으며, 구역 정보는 그 그룹 내 도메인 이름들 전체가 특정 구역(예를 들어, "신뢰하는 파트너" 구역)으로 그룹화됨을 표시할 수 있다.

[0032] 컴퓨터 시스템(200)은 또한 여러 다른 장치들을 포함할 수도 있다. 예를 들어 도 2에서, 컴퓨터 시스템(200)은 이메일 서버(209), 파일 서버(207), 워크스테이션들(205a 및 205b), 및 인터넷 게이트웨이(211)를 포함한다. 인터넷 게이트웨이(211)는 컴퓨터 시스템(200) 내 장치들을 위한 인터넷으로의 게이트웨이 역할을 할 수 있으며, 컴퓨터 시스템(200) 내 장치들은 LAN(218)을 통해 서로 통신할 수 있다.

[0033] 장치들(205a, 205b, 207, 209 및 211) 각각은 정책 엔진을 포함한다. 이 장치들 각각의 정책 엔진은 정보가 다른 장치로부터 수신되거나 다른 장치로 전달될 때, 정보가 구역의 경계를 언제 지났거나 전달의 경우 언제 지날지를 결정하도록 동작할 수 있다. 그렇다면, 정책 엔진은 정보 보호 규칙들에 기초해서 어떤 정책적 조치가 보장되는지를 판달할 수 있으며, 그 정책적 조치를 수행할 수 있다.

[0034] 도 2의 예에서, 장치들(205a, 205b, 207, 209, 및 211) 각각은 정책 엔진을 실행한다. 그러나 본 발명은 이러한 점에 국한되지 않는다. 즉, 일부 실시예들에서, 구역의 경계에 있는 장치들(예를 들어, 다른 구역으로 정보를 직접 전송하거나 그로부터 정보를 수신할 수 있는 장치들)만이 정책 엔진을 실행할 수 있다. 따라서, 그러한 실시예들이 도 2의 예에서 사용되었으며 컴퓨터 시스템(200) 내 장치들 및 사용자들 모두가 하나의 구역으로 그룹화되었다면, 인터넷 게이트웨이(211) 만이 정책 엔진을 실행할 필요가 있다.

[0035] 도 3은 정보 보호 규칙들을 구현하기 위해 컴퓨터 시스템(200)과 같은 컴퓨터 시스템 안에서 사용될 수 있는 예시적 정보 보호 프로세스를 보여준다. 프로세스는 콘텍츠(예를 들어, 문서)가 생성되거나 수신되는 단계(301)

에서 시작된다. 이어서, 프로세스는 콘텍츠가 분류되고 콘텐츠에 대한 분류가 저장되는 단계(303)로 계속된다.

[0036] 단계(303) 이후에, 프로세스는 다른 장치로의 콘텐츠의 전달이 개시되는 단계(305)로 계속된다. 그 후, 프로세스는 그 전달이 콘텐츠를 구역의 경계를 지나게 하는지 혹은 지나게 할 것인지가 결정되는 단계(307)로 계속된다. 단계(307)는 예를 들어 콘텐츠를 전달 개시하는 장치상이거나 전달을 개시했던 장치로부터 콘텐츠가 전달된 후 콘텐츠를 수신하는 다른 장치상에서 정책 엔진에 의해 수행될 수 있다.

[0037] 정책 엔진은 그 전달이 정보를 구역의 경계를 지나게 하는지 혹은 지나게 할 것인지 여부를 다양한 방식들 중 어느 하나에 의해 결정할 수 있다. 예를 들어, 일부 실시예들에서, 정책 엔진은 전달을 개시했던 장치나 사용자의 구역 및 전달의 의도된 수신자인 장치나 사용자의 구역을 결정하기 위해 중앙 보안 서버(201)(위에서 논의한 바와 같이 구역 정보(215)를 저장함)와 통신할 수 있다. 대안적으로, 일부 실시예들에서 이 구역 정보의 일부나 전체가 장치 상에 내부적으로 캐싱될 수 있으며, 정책 엔진은 전달을 개시했던 장치나 사용자의 구역 및 의도된 수신자인 장치나 사용자의 구역을 결정하기 위해 그 내부적으로 캐싱된 정보를 이용할 수 있다. 전달을 개시했던 장치나 사용자의 구역과 콘텐츠에 대해 의도된 수신자인 장치나 사용자의 구역이 동일하다면, 그 전달은 콘텐츠가 구역의 경계를 넘게 하지 않는다고 판단될 것이며, 프로세스가 종료될 수 있다.

[0038] 전달을 개시했던 장치나 사용자의 구역과 콘텐츠에 대해 의도된 수신자인 장치나 사용자의 구역이 상이하다면, 그 전달은 콘텐츠가 구역의 경계를 지나게 하거나 지나게 할 것이라고 판단될 것이며, 프로세스는 단계(309)로 계속될 수 있다. 단계(309)에서 정책 엔진은 어떤 정책적 조치들이 의도된 전달의 결과로서 취해져야 할지 여부를 결정하며, 그 정책적 조치들을 수행할 수 있다. 정책 엔진은 어떤 정책적 조치들이 어떤 적절한 방식으로 취해져야 하는지 여부를 결정할 수 있다. 예를 들어, 정책 엔진은 정책 정보(213)에 저장된 정보 보호 규칙들을 결정하기 위해 중앙 보안 서버(201)와 통신할 수 있으며, 해당 전달에 그러한 규칙들을 적용할 수 있다. 대안적으로, 일부 실시예들에서 정책 정보(213)에 저장된 규칙들의 일부나 전부가 장치 상에서 내부적으로 캐싱될 수 있으며, 정책 엔진은 분류 규칙들을 결정하기 위해 그 내부적으로 캐싱된 정보를 이용할 수 있다.

[0039] 분류 규칙들은 분류 규칙들에 기초해서 어떤 적절한 정책적 조치를 특정할 수 있다. 예를 들어, 정책 엔진은 전달을 차단하고, 전달을 완료하기 위해 콘텐츠의 암호화를 요구하고, 전달의 감사 로그 엔트리를 생성하고, 전달을 완료하기 전에 사용자에게 승인을 촉구하고, 전달이 요망되는 정보의 사본을 생성하고, 사용자나 관리자에게 전달에 대해 통지하는 경보를 보내며/거나, 어떤 다른 적절한 조치를 취할 수 있다.

[0040] 도 4는 본 발명의 양태들이 구현될 수 있는 예시적 컴퓨터(400)의 개략적 블록도를 도시한다. 명료성을 목적으로 컴퓨터(400) 중 예시적 부분들만이 식별되며, 이들이 어떤 식으로든 본 발명의 양태들을 한정하는 것은 아니다. 예를 들어, 컴퓨터(400)는 한 개 이상의 추가적 휘발성 혹은 비휘발성 메모리들(저장 매체라고도 칭할 수 있음), 한 개 이상의 추가적 프로세서들, 어떤 다른 사용자 입력 장치들, 및 여기 기술된 기능을 수행하기 위해 컴퓨터(400)에 의해 실행될 수 있는 어떤 적절한 소프트웨어나 다른 명령어들을 포함할 수 있다.

[0041] 예시된 실시예에서, 컴퓨터(400)는 중앙 처리 유닛(402)(한 개 이상의 범용 프로그래머블 컴퓨터 프로세서들을 포함할 수 있음), 유형의 메모리(404), 비디오 인터페이스(406), 사용자 입력 인터페이스(408), 및 네트워크 인터페이스(412) 사이의 통신을 가능하게 하는 시스템 버스(410)를 포함한다. 네트워크 인터페이스(412)는 네트워크 접속(420)을 통해 적어도 한 개의 원격 컴퓨팅 장치(418)에 연결될 수 있다. 사용자 입출력 장치들 외에, 모니터(422), 키보드(414), 및 마우스(416)와 같은 주변기기들 역시 컴퓨터 시스템에 포함될 수 있으며, 본 발명이 이러한 것에 한정되는 것은 아니다.

[0042] 일부 실시예들에서, 위에 예시되고 기술된 장치들은 컴퓨터(400)와 같은 컴퓨터들로서 구현될 수 있다. 예를 들어, 일부 실시예들에서 장치들(201, 203, 205a, 205b, 207, 209 및 211)은 각각 컴퓨터(400)와 같은 컴퓨터로서 구현될 수 있다. 이에 관해, 이 장치들의 상술한 기능이 그 기능을 수행하는 소프트웨어 명령어들을 실행하는 중앙 처리 유닛(402)에 의해 구현될 수 있으며 그 장치들에 저장되는 것으로 위에서 기술된 정보는 메모리(404)에 저장될 수 있다는 점이 이해되어야 한다.

[0043] 본 발명의 적어도 일 실시예에 대한 여러 양태들이 전술한 바와 같이 기술되었으나, 다양한 치환, 변경, 및 개선이 용이하게 당업자에게 일어날 수 있다는 점이 이해되어야 한다.

[0044] 그러한 치환, 변경, 및 개선은 이 개시의 일부가 되도록 의도되며, 본 발명의 개념 및 범위 안에 있도록 의도된다. 따라서, 상술한 설명과 도면들은 단지 예일 뿐이다.

[0045] 상술한 본 발명의 실시예들은 수많은 방식 중 어느 하나로 구현될 수 있다. 예를 들어, 실시예들은 하드웨어, 소프트웨어, 또는 그 조합을 이용하여 구현될 수 있다. 소프트웨어로 구현될 때, 소프트웨어 코드는 단일 컴퓨

터 내에 제공되거나 여러 컴퓨터들 사이에 분산되는지 여부와 관계없이 어떤 적절한 프로세서나 프로세서들의 집합 상에서 실행될 수 있다.

[0046] 또한, 컴퓨터는 랙에 탑재된 컴퓨터, 데스크탑 컴퓨터, 랩탑 컴퓨터, 또는 태블릿 컴퓨터와 같은 여러 형태 중 어느 하나를 통해 구현될 수 있다는 점이 이해되어야 한다. 추가적으로, 컴퓨터는 PDA(Personal Digital Assistant), 스마트폰, 또는 어떤 다른 적절한 휴대형 또는 고정형 전자 기기를 포함하여, 일반적으로 컴퓨터라고 간주되지 않지만 적절한 프로세싱 능력을 가지는 장치 안에 내장될 수 있다.

[0047] 또한, 컴퓨터는 한 개 이상의 입출력 장치들을 가질 수 있다. 이 장치들은 다른 무엇보다 사용자 인터페이스를 제공하기 위해 사용될 수 있다. 사용자 인터페이스를 제공하기 위해 사용될 수 있는 출력 장치들의 예들에는 출력에 대한 시각적 표현을 위한 프린터나 디스플레이 스크린 및 출력에 대한 청각적 표현을 위한 스피커나 기타 소리 생성 장치들이 포함된다. 사용자 인터페이스를 위해 사용될 수 있는 입력 장치들의 예들에는 키보드 및 마우스, 터치 패드 및 디지타이징 태블릿과 같은 포인팅 장치들이 포함된다. 또 다른 예로서, 컴퓨터는 음성 인식이나 다른 청각 형식을 통해 입력 정보를 수신할 수 있다.

[0048] 그러한 컴퓨터들은 기업망이나 인터넷과 같은 광역 네트워크(WAN)나 랜(LAN) 같은 것을 포함하는 어떤 적절한 형식으로 한 개 이상의 네트워크들에 의해 서로 연결될 수 있다. 그러한 네트워크들은 어떤 적절한 기술에 기반할 수 있고, 어떤 적절한 프로토콜에 따라 동작할 수 있으며, 무선 네트워크, 유선 네트워크 또는 광섬유 네트워크를 포함할 수 있다.

[0049] 또한, 여기에 약술된 다양한 방법들이나 프로세스들은 다양한 운영체제들이나 플랫폼들 중 어느 하나를 이용하는 한 개 이상의 프로세서들 상에서 실행될 수 있는 소프트웨어로서 코딩될 수 있다. 또한, 그러한 소프트웨어는 여러 적절한 프로그래밍 언어 및/또는 프로그래밍이나 스크립트 툴 중 어느 하나를 이용하여 작성될 수 있으며, 프레임워크나 가상 머신 상에서 실행되는 실행 가능한 기계어 코드나 중간 코드로서 컴파일될 수도 있다.

[0050] 이 점에 관해, 본 발명은 한 개 이상의 컴퓨터들이나 다른 프로세서들 상에서 실행될 때 상기 논의된 본 발명의 다양한 실시예들을 구현하는 방법들을 수행하는 한 개 이상의 프로그램들을 이용하여 부호화된 컴퓨터 판독 가능 매체(또는 여러 컴퓨터 판독 가능 매체들)(예를 들어, 컴퓨터 메모리, 한 개 이상의 플로피 디스크, 컴팩트 디스크(CD), 광 디스크, 디지털 비디오 디스크(DVD), 자기 테이프, 플래시 메모리, 필드 프로그래머블 게이트 어레이들의 회로 구성이나 다른 반도체 소자들, 또는 다른 일시적이지 않은 유형의 컴퓨터 저장 매체)로서 실시될 수 있다. 컴퓨터 판독 가능 매체나 매체들은 그 매체 상에 저장된 프로그램이나 프로그램들이 상기 논의된 바와 같은 본 발명의 다양한 양태들을 구현하기 위해 한 개 이상의 다양한 컴퓨터들이나 다른 프로세서들 상으로 로드될 수 있도록 운반 가능한 것일 수 있다.

[0051] "프로그램"이나 "소프트웨어"라는 용어들은 일반적인 맥락에 따라 여기에서 위에서 논의된 바와 같은 본 발명의 다양한 양태들을 구현하기 위해 컴퓨터나 다른 프로세서를 프로그래밍하기 위해 사용될 수 있는 컴퓨터 코드나 일련의 컴퓨터 실행 가능 명령어들의 어떤 유형을 지칭하는 것으로 사용된다. 또한, 이 실시예의 한 양태에 따르면, 실행될 때 본 발명의 방법들을 수행하는 한 개 이상의 컴퓨터 프로그램들은 한 개의 컴퓨터나 프로세서 상에 상주할 필요는 없으며, 본 발명의 다양한 양태들을 구현하기 위해 여러 다양한 컴퓨터들이나 프로세서들 사이에서 모듈 방식으로 분산될 수 있다.

[0052] 컴퓨터 실행 가능 명령어들은 한 개 이상의 컴퓨터들이나 다른 장치들에 의해 실행되는 프로그램 모듈들과 같은 많은 형태들로 되어 있을 수 있다. 일반적으로 프로그램 모듈은 특정 작업을 수행하거나 특정한 추상적 데이터 유형들을 구현하는 루틴, 프로그램, 오브젝트, 컴포넌트, 데이터 구조를 포함한다. 통상적으로, 프로그램 모듈들의 기능은 다양한 실시예들에서 원하는 바대로 결합되거나 분산될 수 있다.

[0053] 또한, 데이터 구조들이 어떤 적절한 형식으로 컴퓨터 판독 가능 매체 안에 저장될 수 있다. 예시의 단순성을 위해, 데이터 구조들은 데이터 구조 상의 위치를 통해 관련된 필드들을 가지는 것으로 도시될 수 있다. 그러한 관계가 마찬가지로 필드들 사이의 관계를 전달하는 컴퓨터 판독 가능 매체 내에 위치를 가진 필드들에 대해 저장소를 할당함으로써 달성될 수 있다. 그러나, 포인터들, 태그들, 또는 데이터 요소들 사이의 관계를 설정하는 다른 메커니즘들을 포함하는 어떤 적절한 메커니즘이 데이터 구조의 필드들 안의 정보들 사이의 관계를 설정하기 위해 사용될 수 있다.

[0054] 본 발명의 다양한 양태들이 단독으로 또는 조합하여 상술한 내용에서 기술된 실시예들에서 특정하여 논의되지 않은 다양한 구성들로 사용될 수 있으며, 그에 따라 적용에 있어서 상술한 내용에 언급되거나 도면에 예시된 구성요소들의 세부내용 및 구성에 국한되는 것은 아니다. 예를 들어, 일 실시예에서 기술된 양태들이 다른 실시

예들에서 기술된 양태들과 함께 어떤 방식으로 결합될 수 있다.

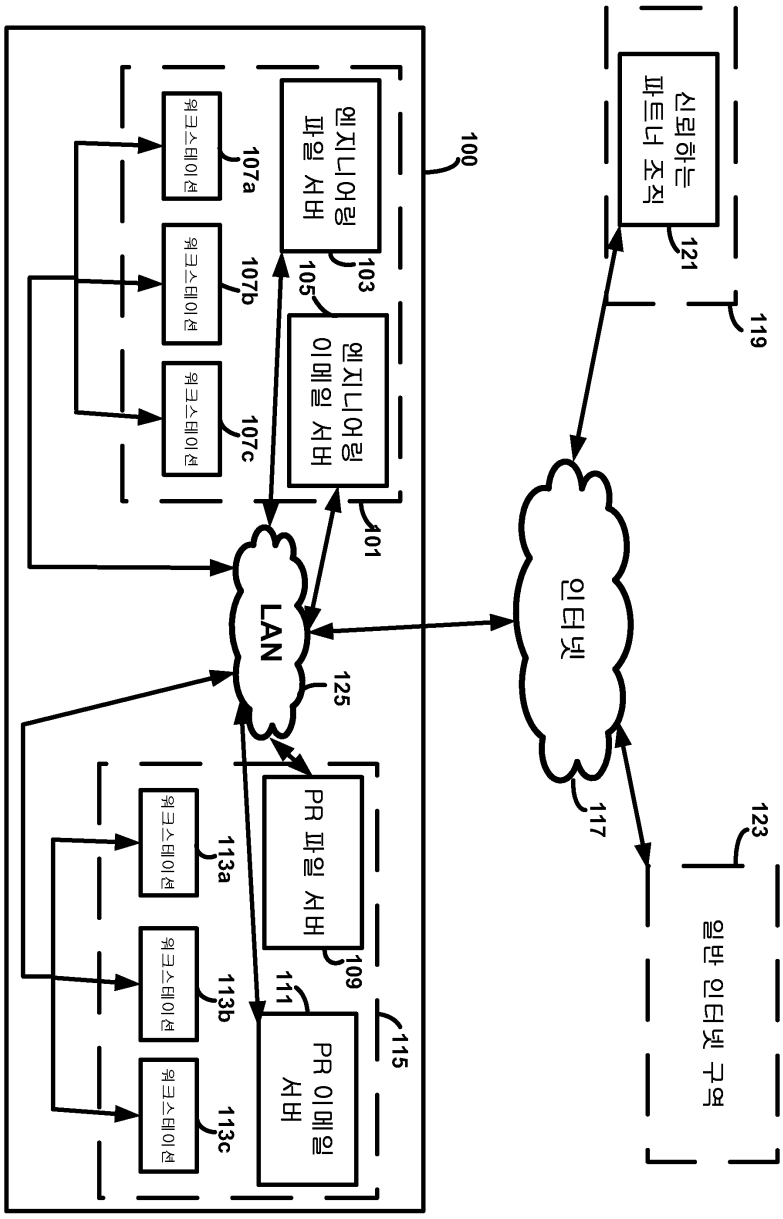
[0055] 또한, 본 발명은 일 예가 제공되었던 방법으로서 구현될 수 있다. 방법의 일부로서 수행되는 단계들은 어떤 적절한 방식으로 순서화될 수 있다. 그에 따라, 도시된 실시예들에서는 순차적 단계들로 도시되었지만, 단계들이 도시된 것과 다른 순서로 수행되며 일부 단계들을 동시에 수행하는 것을 포함할 수 있는 실시예들이 구성될 수 있다.

[0056] 청구항 구성 요소를 변경하기 위해 청구범위 내에서 "제1(first)", "제2(second)", "제3(third)" 등과 같은 순서적인 용어를 사용하는 것은 그 자체로 어떤 우선순위, 서열, 또는 다른 청구항 구성 요소에 대한 한 청구항 구성 요소의 순서나 방법의 단계들이 수행되는 시간적 순서를 내포하는 것이 아니며, 단지 청구항 구성 요소들을 구분하기 위해 소정 명칭을 가진 하나의 청구항 구성 요소를 동일한 명칭을 가진 다른 구성 요소와 구분하기 위한 (그러나 순서적 용어의 사용을 위한) 표식으로서 사용된다.

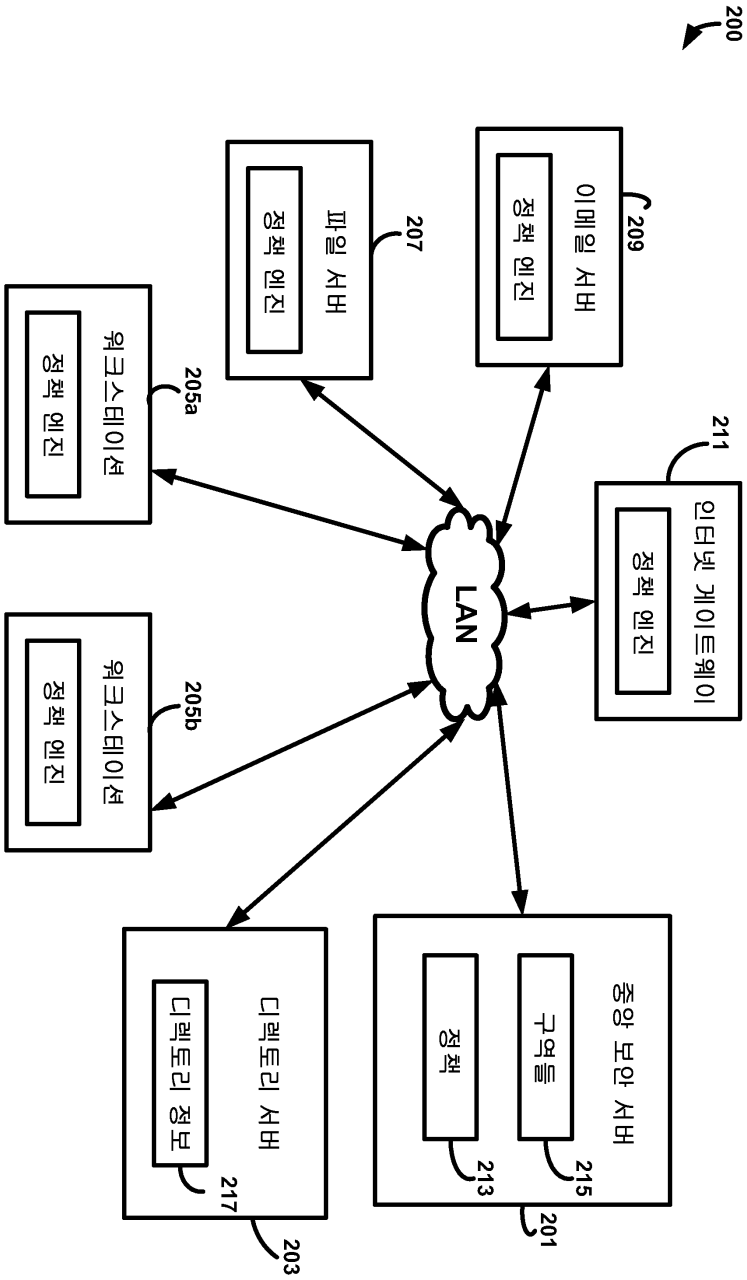
[0057] 또한, 여기에 사용된 표현과 용어는 설명을 목적으로 하는 것이며, 한정하는 것으로 간주되지 않아야 한다. "포함한다(including)", "구비한다(comprising)", 또는 "가진다(having)", "내포한다(containing)", "수반한다(involving)", 및 여기에 있는 이들의 파생어들의 사용은 그 뒤에 나열되는 항목들 및 그 균등물들뿐만 아니라 추가 항목들을 포괄하는 것을 의미한다.

도면

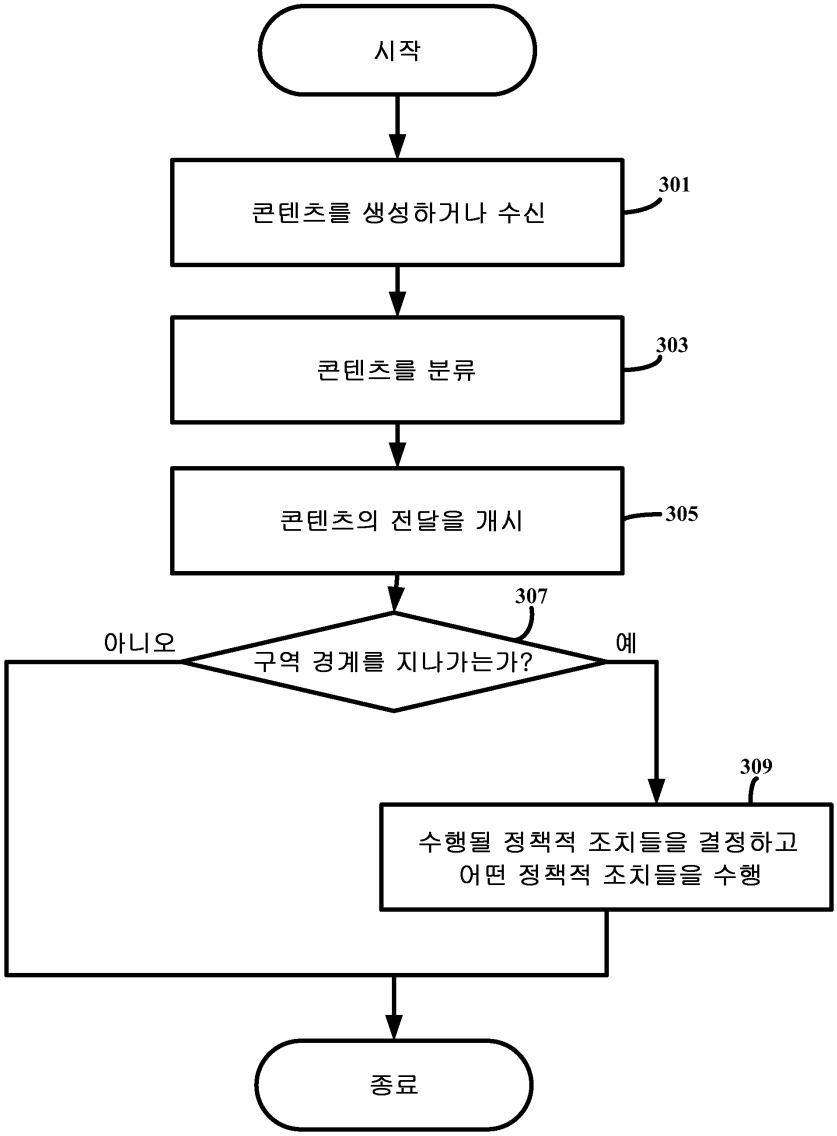
도면1


신뢰하는
파트너 조직
121
119
엔지니어링
파일 서버
103
105
엔지니어링
이메일 서버
101
100
워크스테이션
107a
워크스테이션
107b
워크스테이션
107c
LAN
125
인터넷
117
123
일반 인터넷 구역
PR 파일 서버
109
111
PR 이메일
서버
115
워크스테이션
113a
워크스테이션
113b
워크스테이션
113c

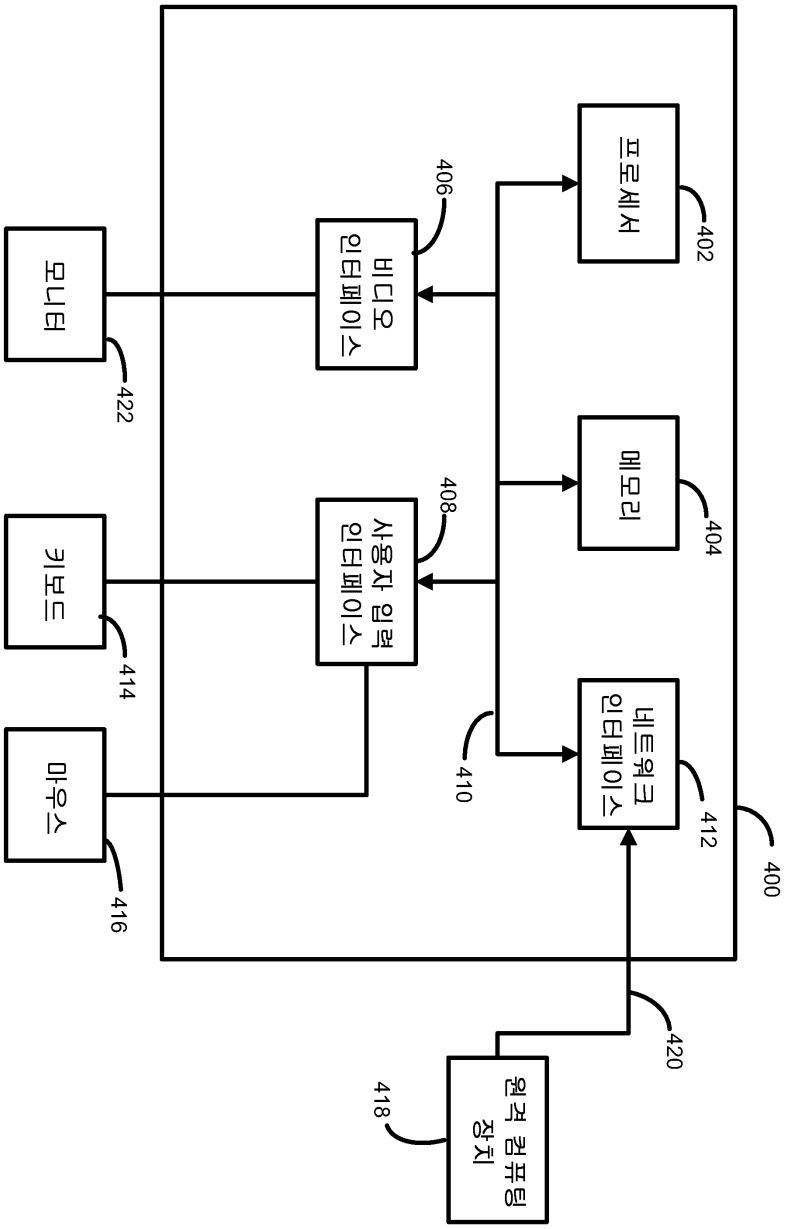
도면2


200
이메일 서버
정책 엔진
209
파일 서버
정책 엔진
207
워크스테이션
정책 엔진
205a
워크스테이션
정책 엔진
205b
LAN
인터넷 게이트웨이
정책 엔진
211
중앙 보안 서버
정책
213
구역들
215
201
디렉토리 서버
디렉토리 정보
217
203

도면3


시작
콘텐츠를 생성하거나 수신
301
콘텐츠를 분류
303
콘텐츠의 전달을 개시
305
307
아니오
구역 경계를 지나가는가?
예
309
수행될 정책적 조치들을 결정하고
어떤 정책적 조치들을 수행
종료

도면4


프로세서
402
메모리
404
네트워크 인터페이스
412
400
410
비디오 인터페이스
406
사용자 입력 인터페이스
408
모니터
422
키보드
414
마우스
416
420
원격 컴퓨팅 장치
418