(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년12월09일
(11) 등록번호 10-1575282
(24) 등록일자 2015년12월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01)
(21) 출원번호 10-2011-0124760
(22) 출원일자 2011년11월28일
심사청구일자 2014년03월26일
(65) 공개번호 10-2013-0058813
(43) 공개일자 2013년06월05일
(56) 선행기술조사문헌
JP2006504178 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
안개일
대전광역시 서구 둔산북로 215, 13동 1203호 (둔산동, 가람아파트)
서대희
충청남도 홍성군 홍성읍 월계천길 41-11, 103동 901호 (홍성향촌현대아파트)
(뒷면에 계속)
(74) 대리인
한양특허법인

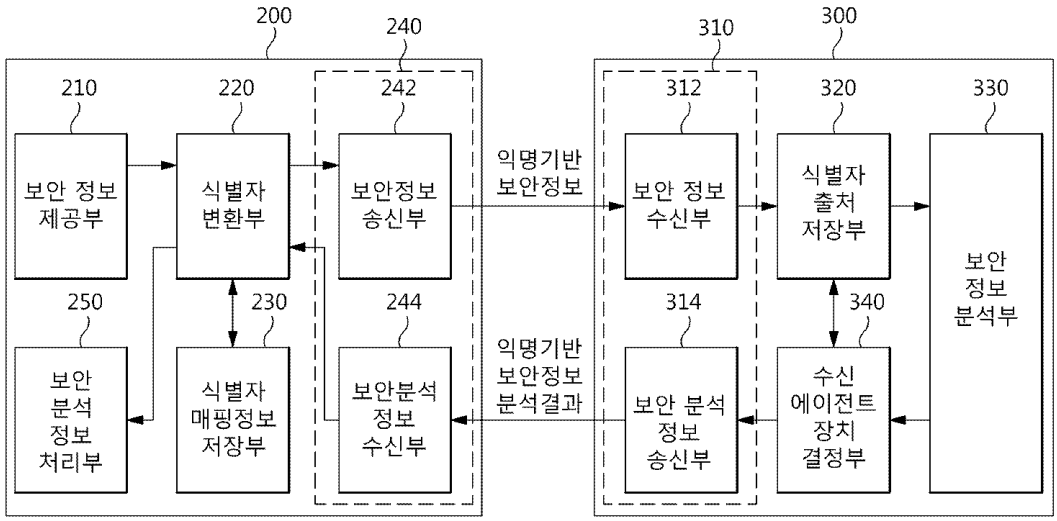
전체 청구항 수 : 총 10 항 심사관 : 이복현

(54) 발명의 명칭 **보안관리 도메인들 간에 익명 식별자 기반의 보안정보를 공유하기 위한 에이전트 장치 및 방법**

(57) 요 약

본 발명은 보안관리 도메인들 간에 익명 식별자 기반의 보안정보를 공유하기 위한 에이전트 장치 및 방법에 관한 것이고, 보다 상세하게는 보안정보 공유를 원하는 보안관리 도메인들이 신뢰할 수 있는 도메인에 존재하는 보안분석 대행 에이전트 장치를 통해 개인정보를 추출할 수 없는 해쉬 식별자를 사용하여 보안정보를 공유하게 함으로써, 공유되는 보안정보에 포함된 개인정보를 효과적으로 보호할 수 있도록 하는 보안관리 도메인들 간에 익명 식별자 기반의 보안정보를 공유하기 위한 에이전트 장치 및 방법에 관한 것이다.

대 표 도



(72) 발명자

김종현

대전광역시 유성구 엑스포로123번길 65-38 (도룡동)

임선희

경기도 성남시 분당구 내정로 186, 롯데아파트 127-904 (수내동, 파크타운)

이성원

대전광역시 서구 대덕대로 248, 넥서스밸리 A-407 (둔산동)

김기영

대전광역시 유성구 엑스포로123번길 65-38, 503동 3102호 (도룡동, 스마트시티)

서동일

대전광역시 유성구 엑스포로 448, 305동 1204호 (전민동, 엑스포아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호	10914-06002
부처명	방송통신위원회
연구관리전문기관	한국방송통신전파진흥원
연구사업명	방송통신기술개발사업(**원천기술개발사업)
연구과제명	전역적 협력기반의 통합보안제어 시스템 개발
기 여 율	1/1
주관기관	한국전자통신연구원
연구기간	2010.03.01 ~ 2013.02.28

명 세 서

청구범위

청구항 1

복수의 보안관리 도메인들 각각에 위치하여 보안정보를 수집하고 보안관리 도메인의 외부로 상기 보안정보를 전송하는 보안정보 공유 에이전트 장치로서,

상기 보안정보에 포함된 실명 식별자를 익명 식별자로 변환함으로써 실명 식별자 기반의 보안정보를 익명 식별자 기반의 보안정보로 변환하되, 단방향 해쉬(Hash) 함수를 이용하여 상기 보안정보에 포함된 실명 식별자를 상기 익명 식별자인 해쉬 식별자로 변환하는 식별자 변환부;

상기 복수의 보안관리 도메인들이 보안정보를 공유하도록 상기 식별자 변환부에 의해 변환된 익명 식별자 기반의 보안정보를 상기 보안관리 도메인 외부로 전송하는 보안정보 통신부; 및

상기 보안정보에 포함된 실명 식별자와 상기 실명 식별자로부터 변환된 익명 식별자 간의 매핑정보를 저장하는 식별자 매핑정보 저장부;를 포함하고,

상기 식별자 변환부는, 상기 식별자 매핑정보 저장부에 저장된 매핑정보를 이용하여, 보안분석 대행 에이전트 장치로부터 수신한 보안정보 분석결과에 포함된 익명 식별자를 실명 식별자로 변환하는 것을 특징으로 하는, 보안정보 공유 에이전트 장치.

청구항 2

삭제

청구항 3

청구항 1에 있어서,

상기 보안정보에 포함된 실명 식별자를 해쉬 식별자로 변환하기 위한 해쉬 함수의 알고리즘과 키(Key)는 보안정보 공유 에이전트 장치들 사이에서만 공유되는 것을 특징으로 하는, 보안정보 공유 에이전트 장치.

청구항 4

삭제

청구항 5

삭제

청구항 6

보안분석 도메인에 위치하는 보안분석 대행 에이전트 장치로서,

복수의 보안관리 도메인들 각각에 위치하는 보안정보 공유 에이전트 장치에서 단방향 해쉬(Hash) 함수를 이용하여 보안정보에 포함된 실명 식별자를 익명 식별자인 해쉬 식별자로 변환된 익명 식별자 기반의 보안정보를 수신하는 보안정보 수신부;

상기 보안정보 수신부에 의해 수신된 익명 식별자 기반의 보안정보를 분석하여 익명 식별자 기반의 보안정보 분석결과를 산출하는 보안정보 분석부;

상기 보안정보 분석부에 의해 산출된 익명 식별자 기반의 보안정보 분석결과를 상기 보안정보 공유 에이전트 장치로 전송하는 보안분석정보 송신부;

상기 보안정보 공유 에이전트 장치로부터 수신한 보안정보에 포함된 익명 식별자와 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치 간의 매핑정보를 저장하는 식별자 출처 저장부; 및

상기 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정하기

위한 수신 에이전트 장치 결정부;를 포함하고,

상기 수신 에이전트 장치 결정부는, 상기 식별자 출처 저장부에 저장된 매핑정보를 이용하여, 상기 익명 식별자를 포함하는 보안정보로부터 분석된 보안정보 분석결과를 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치로 전송하도록, 상기 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정하는 것을 특징으로 하는, 보안분석 대행 에이전트 장치.

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

청구항 6에 있어서,

상기 수신 에이전트 장치 결정부는, 상기 보안정보 분석결과를 익명 식별자 별로 분류하고, 상기 식별자 출처 저장부에 저장된 매핑정보에서 각 익명 식별자를 포함하는 보안정보를 전송한 보안정보 공유 에이전트 장치를 검색함으로써, 상기 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정하는 것을 특징으로 하는, 보안분석 대행 에이전트 장치.

청구항 11

복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법에 있어서,

상기 복수의 보안관리 도메인들 각각에 위치하는 보안정보 공유 에이전트 장치가 보안관리 도메인의 보안정보에 포함된 실명 식별자를 익명 식별자로 변환하는 단계;

상기 보안정보 공유 에이전트 장치가 상기 보안정보에 포함된 실명 식별자와 상기 실명 식별자로부터 변환된 익명 식별자 간의 매핑정보를 저장하는 단계;

상기 보안정보 공유 에이전트 장치가 익명 식별자 기반의 보안정보를 보안분석 대행 에이전트 장치로 전송하는 단계;

상기 보안분석 대행 에이전트 장치가 상기 보안정보 공유 에이전트 장치로부터 수신한 익명 식별자 기반의 보안정보를 분석하는 단계;

상기 보안분석 대행 에이전트 장치가 익명 식별자 기반의 보안정보 분석결과를 상기 보안정보 공유 에이전트 장치로 전송하는 단계; 및

상기 보안정보 공유 에이전트 장치가 상기 보안정보에 포함된 실명 식별자와 상기 실명 식별자로부터 변환된 익명 식별자 간의 매핑정보를 이용하여, 상기 보안분석 대행 에이전트 장치로부터 수신한 보안정보 분석결과에 포함된 익명 식별자를 실명 식별자로 변환하는 단계;를 포함하고,

상기 실명 식별자를 익명 식별자로 변환하는 단계는

단방향 해쉬 함수를 이용하여 상기 보안정보에 포함된 실명 식별자를 상기 익명 식별자인 해쉬 식별자로 변환하는 것을 특징으로 하는, 보안정보 공유 방법.

청구항 12

삭제

청구항 13

청구항 11에 있어서,

상기 보안정보에 포함된 실명 식별자를 해쉬 식별자로 변환하기 위한 단방향 해쉬 함수의 알고리즘과 키는 보안정보 공유 에이전트 장치 사이에서만 공유되는 것을 특징으로 하는, 보안정보 공유 방법.

청구항 14

삭제

청구항 15

삭제

청구항 16

청구항 11에 있어서,

상기 보안분석 대행 에이전트 장치가 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정하는 단계를 더 포함하는 것을 특징으로 하는, 보안정보 공유 방법.

청구항 17

청구항 16에 있어서,

상기 보안분석 대행 에이전트 장치가 상기 보안정보 공유 에이전트 장치로부터 수신한 보안정보에 포함된 익명 식별자와 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치 간의 매핑정보를 저장하는 단계를 더 포함하는 것을 특징으로 하는, 보안정보 공유 방법.

청구항 18

청구항 17에 있어서,

상기 보안정보 공유 에이전트 장치를 결정하는 단계는,

상기 보안분석 대행 에이전트 장치가 상기 보안정보 공유 에이전트 장치로부터 수신한 보안정보에 포함된 익명 식별자와 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치 간의 매핑정보를 이용하여, 상기 익명 식별자를 포함하는 보안정보로부터 분석된 보안정보 분석결과를 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치로 전송하도록, 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정하는 것을 특징으로 하는, 보안정보 공유 방법.

청구항 19

청구항 18에 있어서,

상기 보안정보 공유 에이전트 장치를 결정하는 단계는,

상기 보안정보 분석결과를 익명 식별자별로 분류하고, 상기 식별자 출처 저장부에 저장된 상기 매핑정보에서 각 익명 식별자를 포함하는 보안정보를 전송한 보안정보 공유 에이전트 장치를 검색하는 단계를 포함하는 것을 특징으로 하는, 보안정보 공유 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안관리 도메인들 간에 익명 식별자 기반의 보안정보를 공유하기 위한 에이전트 장치 및 방법에 관한 것이고, 보다 상세하게는 보안정보 공유를 원하는 보안관리 도메인들이 신뢰할 수 있는 도메인에 존재하는 보안분석 대행 에이전트 장치를 통해 개인정보를 추출할 수 없는 해쉬 식별자를 사용하여 보안정보를 공유하게 함으로써, 공유되는 보안정보에 포함된 개인정보를 효과적으로 보호할 수 있도록 하는 보안관리 도메인들 간에 익명 식별자 기반의 보안정보를 공유하기 위한 에이전트 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷의 확산으로 인해 개인의 인터넷 뱅킹, 전자상거래 이용이 급속히 증가하고 있으며, 기업, 정부, 은행의 서비스 및 마케팅이 인터넷 쇼핑몰, 홈페이지 등을 중심으로 빠른 속도로 증가하고 있다. 이러한 상황에서 개인정보와 신용카드 등 금융신용정보와 기업의 마케팅, 신 제품 개발정보를 부당하게 취득하거나, 대규모 인터넷 서비스의 중단 또는 서비스 불능사태를 유발하기 위한 각종 불법적인 행위들이 만연하고 있다.

[0003] 이러한 불법적인 행위, 예를들어, 불법적인 해킹이나 불특정 다수를 겨냥한 웜/바이러스의 유포 등과 같은 사이버 공격을 효과적으로 방어하기 위해, 인터넷 서비스를 제공하는 기관/회사의 보안관리 도메인은 신뢰정보공유 네트워크(Trusted Information Sharing Network)를 구축하여, 다른 인터넷 서비스 제공자의 보안관리 도메인과 해킹, 바이러스, 웜, 사이버테러, 네트웍스파이, 정보전 등의 침해사고 및 취약성 정보와 같은 보안정보를 공유하고 있다.

[0004] 도 1은 복수의 보안관리 도메인들이 자신의 도메인에서 수집한 보안정보를 상호 공유하도록 하기 위한 일반적인 보안정보 공유 시스템을 나타내는 도면이다.

[0005] 도 1에 도시된 바와 같이, 인터넷 서비스를 제공하는 기관/회사의 보안관리 도메인들(10a, 10b)은, 보안정보를 수집하고 이를 서로 간에 공유하기 위해 다른 보안관리 도메인으로 전송하는 보안정보 공유 에이전트 장치(100a, 100b)를 각각 포함한다. 여기서, 제1 보안관리 도메인(10a)과 제2 보안관리 도메인(10b)이 사전 합의에 따라 보안정보를 공유하기로 결정함에 따라, 상기 제1 보안관리 도메인(10a) 내의 제1 보안정보 공유 에이전트 장치(100a)와 상기 제2 보안관리 도메인(10b) 내의 제2 보안정보 공유 에이전트 장치(100b)는 자신의 보안관리 도메인에서 수집한 보안정보를 유·무선통신을 통해 간에 교환함으로써, 보안관리 도메인들(10a, 10b) 간의 보안정보 공유가 이루어지게 진다.

[0006] 여기서, 보안정보 공유 에이전트 장치(100a, 100b)들이 자신이 속한 보안관리 도메인에 대하여 수집한 보안정보(침해사고 정보, 보안로그, 사이버공격 탐지 정보, 보안취약성 정보, 보안평가 정보 등)에는 인터넷 서비스를 사용하는 고객 개인을 식별할 수 있는 실명 식별자(IP 주소 등)가 포함될 수 있는데, 특정한 보안관리 도메인에서 수집된 보안정보에 포함된 실명 식별자가 보안정보 공유에 의해 다른 보안관리 도메인으로 전송되게 되면 고객의 프라이버시가 노출될 수 있다.

[0007] 이러한, 고객의 프라이버시 노출 문제 때문에 종래에는 보안관리 도메인 간에 공유하는 보안정보를 실명 식별자가 포함되지 않은 보안통계정보(분당 사이버 공격 건수, 트래픽량, 사이버공격의 심각도 등)로 국한하고 있으나, 실명 식별자가 포함되지 않은 보안정보는 보안관리 도메인 사이에서 공유가 되어도 보안정보를 식별할 수 있는 키(Key)가 없기 때문에 보안정보 상호 간의 연관성 및 상관관계를 분석하기 어려운 바, 의미있는 보안정보의 분석이 거의 불가능한 실정이다.

[0008] 따라서, 보안관리 도메인 간에 식별자를 포함하는 보안정보를 공유하면서도 고객 개인의 프라이버시를 보호할 수 있는 보안정보 공유 시스템의 도입이 필요하다.

발명의 내용

해결하려는 과제

[0009] 본 발명의 목적은, 복수의 보안관리 도메인들이 침해사고, 보안로그, 보안 취약성 정보 등의 보안정보를 공유할 때, 보안정보에 포함된 개인 식별자가 보안관리 도메인 외부로 유출되지 않도록 함으로써, 공유되는 보안정보에 포함된 개인정보를 보호할 수 있는 보안정보 공유 기술을 제공하고자 함에 있다.

과제의 해결 수단

[0010] 상기한 목적을 달성하기 위한 본 발명에 따른 복수의 보안관리 도메인들 각각에 위치하여 보안정보를 수집하고 보안관리 도메인의 외부로 상기 보안정보를 전송하는 보안정보 공유 에이전트 장치는, 상기 보안정보에 포함된 실명 식별자를 익명 식별자로 변환함으로써 실명 식별자 기반의 보안정보를 익명 식별자 기반의 보안정보로 변환하는 식별자 변환부; 및 상기 복수의 보안관리 도메인들이 보안정보를 공유하도록 상기 식별자 변환부에 의해 변환된 익명 식별자 기반의 보안정보를 상기 보안관리 도메인 외부로 전송하는 보안정보 통신부를 포함하는 것을 특징으로 한다.

[0011] 이때, 상기 식별자 변환부는, 단방향 해쉬(Hash) 함수를 이용하여 상기 보안정보에 포함된 실명 식별자를 상기 익명 식별자인 해쉬 식별자로 변환할 수 있다.

[0012] 이때, 상기 보안정보에 포함된 실명 식별자를 해쉬 식별자로 변환하기 위한 해쉬 함수의 알고리즘과 키(Key)는 보안정보 공유 에이전트 장치들 사이에서만 공유될 수 있다.

[0013] 이때, 상기 보안정보에 포함된 실명 식별자와 상기 실명 식별자로부터 변환된 익명 식별자 간의 매핑정보를 저장하는 식별자 매핑정보 저장부를 더 포함할 수 있다.

[0014] 이때, 상기 식별자 변환부는, 상기 식별자 매핑정보 저장부에 저장된 매핑정보를 이용하여, 보안분석 대행 에이전트 장치로부터 수신한 보안정보 분석결과에 포함된 익명 식별자를 실명 식별자로 변환할 수 있다.

[0015] 또한, 상기한 목적을 달성하기 위한 본 발명에 따른 보안분석 도메인에 위치하는 보안분석 대행 에이전트 장치는, 복수의 보안관리 도메인들 각각에 위치하는 보안정보 공유 에이전트 장치로부터 익명 식별자 기반의 보안정보를 수신하는 보안정보 수신부; 상기 보안정보 수신부에 의해 수신된 익명 식별자 기반의 보안정보를 분석하여 익명 식별자 기반의 보안정보 분석결과를 산출하는 보안정보 분석부; 및 상기 보안정보 분석부에 의해 산출된 익명 식별자 기반의 보안정보 분석결과를 상기 보안정보 공유 에이전트 장치로 전송하는 보안분석정보 송신부를 포함하는 것을 특징으로 한다.

[0016] 이때, 상기 보안분석 대행 에이전트 장치는, 상기 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정하기 위한 수신 에이전트 장치 결정부를 더 포함할 수 있다.

[0017] 이때, 상기 보안분석 대행 에이전트 장치는, 상기 보안정보 공유 에이전트 장치로부터 수신한 보안정보에 포함된 익명 식별자와 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치 간의 매핑정보를 저장하는 식별자 출처 저장부를 더 포함할 수 있다.

[0018] 이때, 상기 수신 에이전트 장치 결정부는, 상기 식별자 출처 저장부에 저장된 매핑정보를 이용하여, 상기 익명 식별자를 포함하는 보안정보로부터 분석된 보안정보 분석결과를 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치로 전송하도록, 상기 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정할 수 있다.

[0019] 이때, 상기 수신 에이전트 장치 결정부는, 상기 보안정보 분석결과를 익명 식별자 별로 분류하고, 상기 식별자 출처 저장부에 저장된 매핑정보에서 각 익명 식별자를 포함하는 보안정보를 전송한 보안정보 공유 에이전트 장치를 검색함으로써, 상기 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정할 수 있다.

[0020] 또한, 상기한 목적을 달성하기 위한 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법은, 상기 복수의 보안관리 도메인들 각각에 위치하는 보안정보 공유 에이전트 장치가 보안관리 도메인의 보안정보에 포함된 실명 식별자를 익명 실별자로 변환하는 단계; 상기 보안정보 공유 에이전트 장치가 익명 식별자 기반의 보안정보를 보안분석 대행 에이전트 장치로 전송하는 단계; 상기 보안분석 대행 에이전트 장치가 상기 보안정보 공유 에이전트 장치로부터 수신한 익명 식별자 기반의 보안정보를 분석하는 단계; 및 상기 보안분석 대행 에이전트 장치가 익명 식별자 기반의 보안정보 분석결과를 상기 보안정보 공유 에이전트 장치로 전송하는 단계를 포함하는 것을 특징으로 한다.

[0021] 이때, 상기 실명 식별자를 익명 실별자로 변환하는 단계는, 단방향 해쉬 함수를 이용하여 상기 보안정보에 포함된 실명 식별자를 상기 익명 식별자인 해쉬 식별자로 변환할 수 있다.

[0022] 이때, 상기 보안정보에 포함된 실명 식별자를 해쉬 식별자로 변환하기 위한 단방향 해쉬 함수의 알고리즘과 키는 보안정보 공유 에이전트 장치 사이에서만 공유될 수 있다.

[0023] 이때, 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법은, 상기 보안정보 공유 에이전트 장치가 상기 보안정보에 포함된 실명 식별자와 상기 실명 식별자로부터 변환된 익명 식별자 간의 매핑정보를 저장하는 단계를 더 포함할 수 있다.

[0024] 이때, 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법은, 상기 보안정보 공유 에이전트 장치가 상기 보안정보에 포함된 실명 식별자와 상기 실명 식별자로부터 변환된 익명 식별자 간의 매핑정보를 이용하여, 상기 보안분석 대행 에이전트 장치로부터 수신한 보안정보 분석결과에 포함된

익명 식별자를 실명 식별자로 변환하는 단계를 더 포함할 수 있다.

[0025] 이때, 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법은, 상기 보안분석 대행 에이전트 장치가 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정하는 단계를 더 포함할 수 있다.

[0026] 이때, 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법은, 상기 보안분석 대행 에이전트 장치가 상기 보안정보 공유 에이전트 장치로부터 수신한 보안정보에 포함된 익명 식별자와 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치 간의 매핑정보를 저장하는 단계를 더 포함할 수 있다.

[0027] 이때, 상기 보안정보 공유 에이전트 장치를 결정하는 단계는, 상기 보안분석 대행 에이전트 장치가 상기 보안정보 공유 에이전트 장치로부터 수신한 보안정보에 포함된 익명 식별자와 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치 간의 매핑정보를 이용하여, 상기 익명 식별자를 포함하는 보안정보로부터 분석된 보안정보 분석결과를 상기 익명 식별자를 포함하는 보안정보를 전송한 해당 보안정보 공유 에이전트 장치로 전송하도록, 익명 식별자 기반의 보안정보 분석결과를 전송하는 대상이 되는 보안정보 공유 에이전트 장치를 결정할 수 있다.

[0028] 이때, 상기 보안정보 공유 에이전트 장치를 결정하는 단계는, 상기 보안정보 분석결과를 익명 식별자별로 분류하고, 상기 식별자 출처 저장부에 저장된 상기 매핑정보에서 각 익명 식별자를 포함하는 보안정보를 전송한 보안정보 공유 에이전트 장치를 검색하는 단계를 포함할 수 있다.

발명의 효과

[0029] 본 발명에 따르면, 보안정보의 공유를 원하는 보안정보 공유 에이전트 장치들이 신뢰할 수 있는 도메인에 존재하는 보안분석 대행 에이전트 장치를 통해 개인정보를 추출할 수 없는 해쉬 기반의 식별자를 사용하여 상호 간에 보안정보를 공유하게 함으로써, 공유되는 보안정보에 포함된 개인정보가 외부로 유출되는 것을 방지할 수 있다.

도면의 간단한 설명

[0030] 도 1은 복수의 보안관리 도메인들이 자신의 도메인에서 수집한 보안정보를 상호 공유하도록 하기 위한 종래의 보안정보 공유 시스템을 나타내는 도면이다.

도 2는 본 발명에 따른 보안정보 공유 시스템의 개념을 나타내는 도면이다.

도 3은, 본 발명에 따른 보안정보 공유 시스템의 보안정보 공유 에이전트 장치와 보안분석 대행 에이전트 장치 각각의 구성을 나타내는 블록도이다.

도 4는 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법을 설명하기 위한 흐름도이다.

도 5는 보안정보 공유 에이전트 장치 측에서 본 발명에 따른 보안정보 공유 방법을 수행하는 과정을 보다 구체적으로 설명하기 위한 흐름도이다.

도 6은 보안분석 대행 에이전트 장치 측에서 본 발명에 따른 보안정보 공유 방법을 수행하는 과정을 보다 구체적으로 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 본 발명을 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다. 여기서, 반복되는 설명, 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능, 및 구성에 대한 상세한 설명은 생략한다. 본 발명의 실시형태는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[0032] 이하에서는 본 발명의 실시예에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 시스템의 구성 및 그 동작에 대하여 설명하도록 한다.

[0033] 도 2는 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 시스템의 개념을 나타내는 도면이다.

[0034] 도 2를 참조하면, 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 시스템은, 보안정보를 공유하기 위한 보안관리 도메인들(20a, 20b) 각각에 위치하는 보안정보 공유 에이전트 장치들(200a, 200b)과, 보안분석 도메인(30)에 위치하는 보안분석 대행 에이전트 장치(300)로 구성된다. 여기서, 상기 보안분석 대행 에이전트 장치(300)가 위치하는 보안분석 도메인(30)은 복수의 보안관리 도메인들(20a, 20b) 모두가 신뢰할 수 있는 도메인인 것이 바람직하다. 설명의 편의를 위해, 도 1에는 비록 2개의 보안정보 공유 에이전트 장치만을 도시하였으나, 본 발명에 따른 보안정보 공유 시스템에서의 보안정보 공유 에이전트 장치의 수는 이에 한정되지 아니한다.

[0035] 제1 보안관리 도메인(20a)에 위치하는 제1 보안정보 공유 에이전트 장치(200a)는 제2 보안관리 도메인(20b)에 위치하는 제2 보안정보 공유 에이전트 장치(200b)와 직접 통신하지 아니하고, 신뢰할 수 있는 보안분석 도메인(30)에 위치하는 보안분석 대행 에이전트 장치(300)를 통해서만 간접적으로 자신이 속한 보안관리 도메인에서 수집한 보안정보를 공유한다. 여기서, 제1 보안정보 공유 에이전트 장치(200a)는 제1 보안관리 도메인(20a)에서 수집한 보안정보를 보안분석 대행 에이전트 장치(300)로 전송하고자 할 때, 상기 보안정보에 개인을 식별할 수 있는 실명 식별자(IP 주소 등)가 포함되어 있는 경우, 실명 식별자를 개인을 식별할 수 없는 익명 식별자로 변환함으로써 실명 식별자 기반의 보안정보를 익명 식별자 기반의 보안정보로 바꾸어 보안분석 대행 에이전트 장치(300)로 전송한다. 제2 보안정보 공유 에이전트 장치(200b) 역시 제2 보안관리 도메인(20b)에서 수집한 보안정보를 보안분석 대행 에이전트 장치(300)로 전송하고자 할 때, 상기 보안정보에 개인을 식별할 수 있는 실명 식별자(IP 주소 등)가 포함되어 있는 경우, 실명 식별자를 개인을 식별할 수 없는 익명 식별자로 변환함으로써 실명 식별자 기반의 보안정보를 익명 식별자 기반의 보안정보로 바꾸어 보안분석 대행 에이전트 장치(300)로 전송한다. 그리고, 제1 보안정보 공유 에이전트 장치(200a)와 제2 보안정보 공유 에이전트 장치(200b)로부터 익명 식별자 기반의 보안정보들을 수신한 보안분석 대행 에이전트 장치(300)는 상기 익명 식별자 기반의 보안정보를 해당 보안정보 공유 에이전트 장치 별로 필요한 방식으로 가공/분석한 익명 식별자 기반의 보안정보 분석결과를 제1 보안정보 공유 에이전트 장치(200a)와 제2 보안정보 공유 에이전트 장치(200b)로 각각 전송한다.

[0036] 도 3은, 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 시스템에서의 보안정보 공유 에이전트 장치와 보안분석 대행 에이전트 장치 각각의 구성을 나타내는 블록도이다.

[0037] 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 시스템에서의 보안정보 공유 에이전트 장치(200)는, 도 3을 참조하면, 보안정보 제공부(210), 식별자 변환부(220), 식별자 매핑정보 저장부(230), 보안정보 통신부(240) 및 보안분석정보 처리부(250)로 구성된다.

[0038] 보안정보 제공부는(210), 보안정보 공유 에이전트 장치(200)가 속한 보안관리 도메인의 보안정보를 수집하고, 수집된 보안정보를 식별자 변환부(220)로 전송한다.

[0039] 식별자 변환부(220)는, 상기 보안정보 제공부(210)로부터 수신한 보안정보에 개인을 식별할 수 있는 실명 식별자가 포함된 경우, 상기 실명 식별자를 개인을 식별할 수 없는 익명 식별자로 변환하고, 변환된 익명 식별자 기반의 보안정보를 보안정보 교환부로 전송한다.

[0040] 개인을 식별할 수 있는 실명 식별자에서 개인을 식별할 수 없는 익명 식별자로의 변환은 해쉬 함수(Hash function)를 사용함으로써 이루어질 수 있는데, 상기 익명 식별자로의 변환을 위해 사용되는 해쉬 함수는 역함수가 존재하지 않는 단방향 함수(One-way function)로서 'H(실명 식별자|키) = 해쉬 식별자'에 따른다. 상기 식별자 변환부(220)가 결과값으로부터 입력값을 계산할 수 없는 해쉬 함수를 이용하여 보안정보에 포함된 실명 식별자를 해쉬 식별자인 익명 식별자로 변환함으로써, 보안정보 공유 에이전트 장치(200)는 익명 식별자 기반의 보안정보를 보안분석 대행 에이전트 장치(300)로 전송하게 되고, 그에 따라 상기 보안정보 공유 에이전트 장치(200)와 보안분석 대행 에이전트 장치(300)가 익명 식별자 기반의 보안정보를 공유하게 되어 개인 프라이버시 노출 문제를 해결할 수 있게 된다. 여기서, 식별자 변환부(220)에서 실명 식별자를 익명 식별자인 해쉬 식별자로 변환하기 위한 해쉬 함수의 알고리즘 및 키는 보안분석 대행 에이전트 장치(300) 이외의 모든 보안정보 공유 에이전트 장치 사이에서 동일한 것이 바람직하다. 이하의 설명에서 익명 식별자는 해쉬 식별자를 지칭할 수 있고, 물론, 청구항에 기재된 익명 식별자 역시 해쉬 식별자를 지칭할 수 있음은 당연하다.

[0041] 또한, 상기 식별자 변환부(220)는, 보안정보 공유 에이전트 장치(200)의 분석결과 수신부(244)가 보안분석 대행 에이전트 장치(300)로부터 익명 식별자 기반의 보안정보 분석결과를 수신하면, 식별자 매핑정보 저장부(230)에 저장된 실명 식별자와 익명 식별자 간의 매핑정보를 이용하여, 상기 보안정보 분석결과에 포함된 익명 식별자를 실명 식별자로 변환한다.

[0042] 식별자 매핑정보 저장부(230)는, 상기 식별자 변환부(220)가 보안정보에 포함된 실명 식별자를 익명 식별자로 변환하면, 상기 실명 식별자와 익명 식별자 간의 매핑정보를 저장한다.

[0043] 보안정보 통신부(240)는, 상기 식별자 변환부(220)에 의해 변환된 익명 식별자 기반의 보안정보를 보안분석 대행 에이전트 장치(300)로 전송하는 보안정보 송신부(242)와 상기 보안분석 대행 에이전트 장치(300)로부터 익명 식별자 기반의 보안정보 분석결과를 수신하는 보안분석정보 수신부(244)를 포함하여, 보안정보 공유 에이전트 장치(200)와 보안분석 대행 에이전트 장치(300) 사이에 익명 식별자 기반의 보안정보와 그 분석결과를 교환하도록 한다.

[0044] 보안분석정보 처리부(250)는, 상기 식별자 변환부(220)에 의해 보안분석 대행 에이전트 장치(300)로부터 수신된 익명 식별자 기반의 보안정보 분석결과가 실명 식별자 기반의 보안정보 분석결과로 변환되면 이를 처리한다.

[0045] 한편, 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 시스템에서의 보안분석 대행 에이전트 장치(300)는, 도 3을 참조하면, 보안정보 분석결과 통신부(310), 식별자 출처 저장부(320), 보안정보 분석부(330) 및 수신 에이전트 장치 결정부(340)를 포함한다.

[0046] 보안정보 분석결과 통신부(310)는, 보안정보 공유 에이전트 장치(200)로부터 익명 식별자 기반의 보안정보를 수신하는 보안정보 수신부(312)와 상기 보안정보 수신부(312)를 통해 수신된 익명 식별자 기반의 보안정보를 분석한 보안정보 분석결과를 상기 보안정보 공유 에이전트 장치(200)로 전송하는 보안분석정보 송신부(314)를 포함하여, 보안정보 공유 에이전트 장치(200)와 보안분석 대행 에이전트 장치(300) 사이에 익명 식별자 기반의 보안정보와 그 분석결과를 교환하도록 한다.

[0047] 식별자 출처 저장부(320)는, 상기 보안정보 분석결과 통신부(310)의 보안정보 수신부(312)를 통해 보안정보 공유 에이전트 장치(200)로부터 수신한 익명 식별자 기반의 보안정보에서 익명 식별자를 추출하고, 추출된 익명 식별자와 상기 익명 식별자 기반의 보안정보를 전송한 해당 보안정보 공유 에이전트 장치 간의 매핑정보를 저장한다.

[0048] 보안정보 분석부(330)는, 상기 보안정보 분석결과 통신부(310)의 보안정보 수신부(312)를 통해 보안정보 공유 에이전트 장치들로부터 수신한 익명 식별자 기반의 보안정보들을 분석하여 익명 식별자 기반의 보안정보 분석결과를 도출한다. 상기 보안정보 분석부(330)는 각종 보안정보를 여러가지 분류로 검색 및 가공할 수 있도록 정규화하여 데이터베이스로 구축하고, 데이터마이닝 또는 지식기반의 분석 알고리즘을 적용함으로써, 웜, 바이러스의 전파경로 분석, 주요 분포 시간, 주요 공격자, 공격 종류, 분석 가능한 패턴 정보, 위험도별 대응 조치 등과 같은 보안정보 분석결과를 도출할 수 있다.

[0049] 수신 에이전트 장치 결정부(340)는, 상기 보안정보 분석부(330)에 의해 도출된 익명 식별자 기반의 보안정보 분석결과를 어떠한 보안정보 공유 에이전트 장치(200)로 전송할 것인지를 결정한다. 보다 구체적으로, 상기 수신 에이전트 장치 결정부(340)는, 상기 보안정보 분석부(330)에 의해 도출된 익명 식별자 기반의 보안정보 분석결과를 익명 식별자 별로 분류하고, 상기 식별자 출처 저장부(320)에 저장된 매핑정보에서 각 익명 식별자를 포함하는 보안정보를 송신한 보안정보 공유 에이전트 장치를 검색하며, 검색된 보안정보 공유 에이전트 장치에게 해당 익명 식별자 기반의 보안정보 분석결과만을 송신하도록 결정한다.

[0050] 이하에서는 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법에 대하여 설명하도록 한다.

[0051] 도 4는 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법을 설명하기 위한 흐름도이다.

[0052] 도 4를 참조하면, 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방

법은, 먼저 보안정보 공유 에이전트 장치(200)의 보안정보 제공부(210)가 자신이 속한 보안관리 도메인의 보안정보를 수집한다(S400).

[0053] 그 다음으로, 보안정보 공유 에이전트 장치(200)의 식별자 변환부(220)는 보안정보 제공부(210)에 의해 수집된 보안정보에 포함된 실명 식별자를 개인을 식별할 수 없는 익명 식별자로 변환하고(S410), 보안정보 송신부(242)는 식별자 변환부(220)에 의해 변환된 익명 식별자 기반의 보안정보를 보안분석 대행 에이전트 장치(300)의 보안정보 수신부(312)로 송신한다(S420).

[0054] 한편, 보안분석 대행 에이전트 장치(300)의 보안정보 수신부(312)는 보안정보 공유 에이전트 장치(200)의 보안정보 송신부(242)로부터 익명 식별자 기반의 보안정보를 수신하고(S430), 보안정보 분석부(330)는 보안정보 수신부(312)를 통해 수신된 익명 식별자 기반의 보안정보에 대한 분석을 수행하여 익명 식별자 기반의 보안정보 분석결과를 도출한다(S440).

[0055] 그 다음으로, 보안분석 대행 에이전트 장치(300)의 수신 에이전트 장치 결정부(340)는 보안정보 분석부(330)에 의해 도출된 익명 식별자 기반의 보안정보 분석결과에서 어떠한 정보를 어떠한 보안정보 공유 에이전트 장치(200)로 송신할 것인지를 결정하고(S450), 보안분석정보 송신부(314)는 상기 S450 단계에서 결정된 보안정보 공유 에이전트 장치(200)로 해당하는 익명 식별자 기반의 보안정보 분석결과를 송신한다(S460).

[0056] 이때, 보안정보 공유 에이전트 장치(200)의 보안분석정보 수신부(244)는 보안분석 대행 에이전트 장치(300)의 보안분석정보 송신부(314)로부터 익명 식별자 기반의 보안정보 분석결과를 수신하여(S470), 이를 식별자 변환부(220)로 전송한다.

[0057] 식별자 변환부(220)는 전송된 익명 식별자 기반의 보안정보 분석결과에서 익명 식별자를 실명 식별자로 변환하고(S480), 보안분석정보 처리부(250)가 변환된 실명 식별자 기반의 보안정보 분석결과를 처리한다(S490).

[0058] 도 5는 보안정보 공유 에이전트 장치 측에서 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법을 수행하는 과정을 보다 구체적으로 설명하기 위한 흐름도이다.

[0059] 도 5를 참조하면, 먼저 본 발명에 따른 보안정보 공유 에이전트 장치(200)는 식별자 변환부(220)에 의해 자신이 속한 보안관리 도메인에서 수집된 보안정보에 개인을 식별할 수 있는 실명 식별자(IP 주소 등)가 포함되어 있는지 여부를 판단하고, 수집된 보안정보에 실명 식별자가 포함되어 있다면, 단방향 해쉬 함수를 사용하여 상기 실명 식별자를 개인을 식별할 수 없는 익명 식별자인 해쉬 식별자로 변환한다(S510).

[0060] 그 다음으로, 보안정보 공유 에이전트 장치(200)는 보안정보에 포함된 실명 식별자와 해당 실명 식별자로부터 변환된 해쉬 식별자 간의 매핑정보를 식별자 매핑정보 저장부(230)에 저장한 후(S520), 보안분석 대행 에이전트 장치(300)로 해쉬 식별자 기반의 보안정보를 전송한다(S530).

[0061] 그 다음으로, 보안정보 공유 에이전트 장치(200)는 보안분석 대행 에이전트 장치(300)로부터 해쉬 식별자 기반의 보안정보를 분석한 해쉬 식별자 기반의 보안정보 분석결과를 수신하고(S540), 식별자 매핑정보 저장부(230)에 저장된 실명 식별자와 해쉬 식별자 간의 매핑정보를 이용하여 수신한 보안정보 분석결과에 포함된 해쉬 식별자를 실명 식별자로 변환(S550)함으로써, 해쉬 식별자 기반의 보안정보 분석결과를 실명 식별자 기반의 보안정보 분석결과로 변환한다.

[0062] 도 6은 보안분석 대행 에이전트 장치 측에서 본 발명에 따른 복수의 보안관리 도메인들 간에 보안정보를 공유하기 위한 보안정보 공유 방법을 수행하는 과정을 보다 구체적으로 설명하기 위한 흐름도이다.

[0063] 도 6을 참조하면, 먼저 본 발명에 따른 보안분석 대행 에이전트 장치(300)는 보안정보 공유 에이전트 장치(200)로부터 해쉬 식별자 기반의 보안정보를 수신하고(S610), 해쉬 식별자와 해당 해쉬 식별자 기반의 보안정보를 전송한 보안정보 공유 에이전트 장치(200) 간의 매핑정보를 식별자 출처 저장부(320)에 저장한다(S620).

[0064] 그 다음으로, 보안정보 분석부(330)를 통해 해쉬 식별자 기반의 보안정보에 대한 분석을 수행하여 해쉬 식별자 기반의 보안정보 분석결과를 도출한다(S630). 그리고, 수신 에이전트 장치 결정부(340)를 통해 상기 S630 단계에서 도출된 해쉬 식별자 기반의 보안정보 분석결과를 해쉬 식별자 별로 분류하고(S640), 식별자 출처 저장부(320)에 저장된 매핑정보를 이용하여 각 해쉬 식별자 기반의 보안정보를 전송한 보안정보 공유 에이전트 장치(200)를 검색한다(S650).

[0065] 마지막으로, 상기 S650 단계에서 검색된 보안정보 공유 에이전트 장치(200)로 해당하는 해쉬 식별자 기반의 보안정보 분석결과를 송신한다(S660).

[0066] 이상에서와 같이 도면과 명세서에서 최적의 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0067] 200: 보안정보 공유 에이전트 장치

210: 보안정보 제공부 220: 식별자 변환부

230: 식별자 매핑정보 저장부 240: 보안정보 통신부

242: 보안정보 송신부 244: 보안분석정보 수신부

250: 보안분석정보 처리부

300: 보안분석 대행 에이전트 장치

310: 보안정보 분석결과 통신부

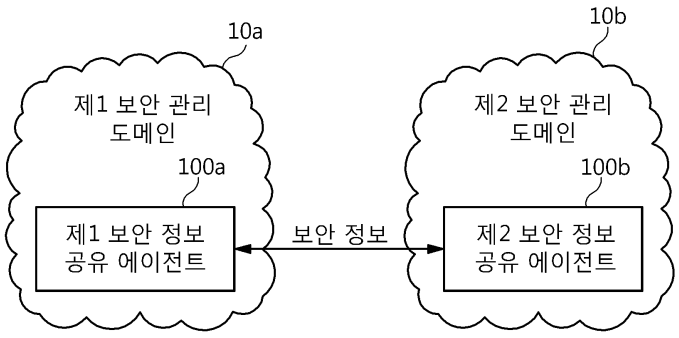
312: 보안정보 수신부 314: 보안분석정보 송신부

320: 식별자 출저 저장부 330: 보안정보 분석부

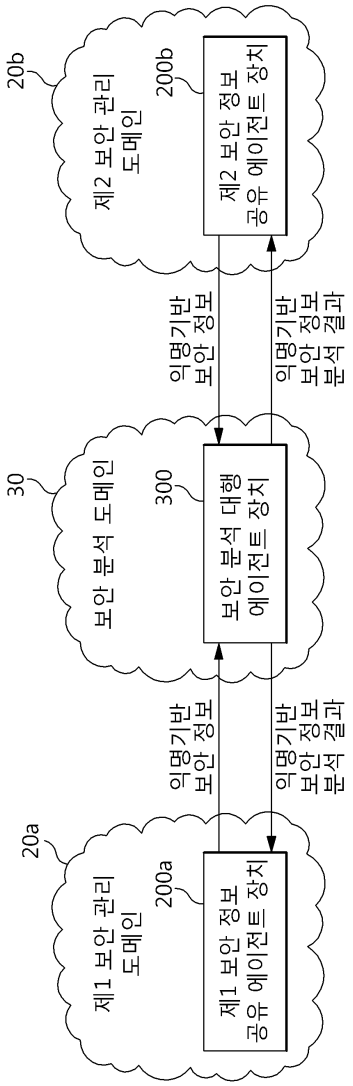
340: 수신 에이전트 장치 결정부

도면

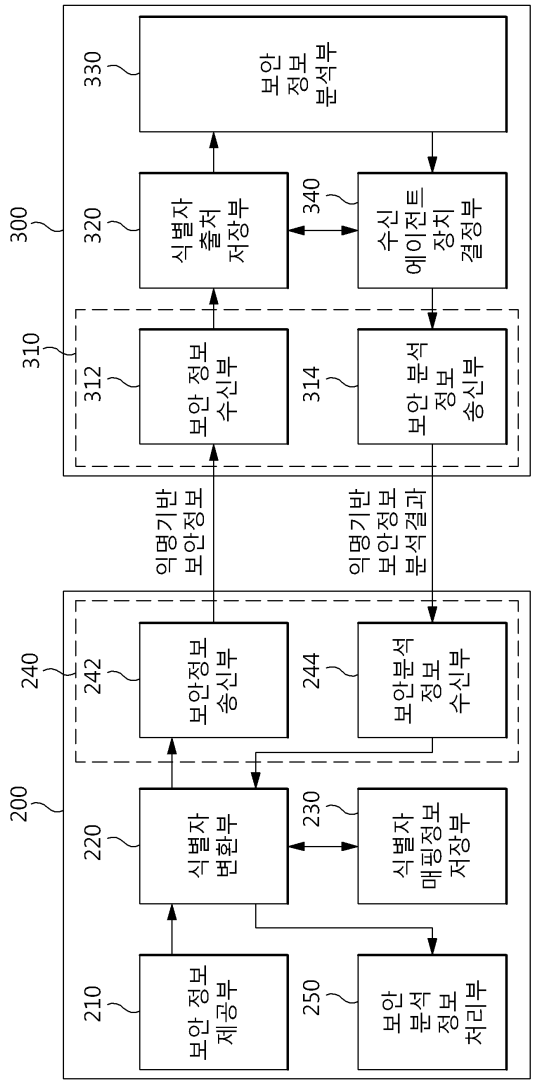
도면1



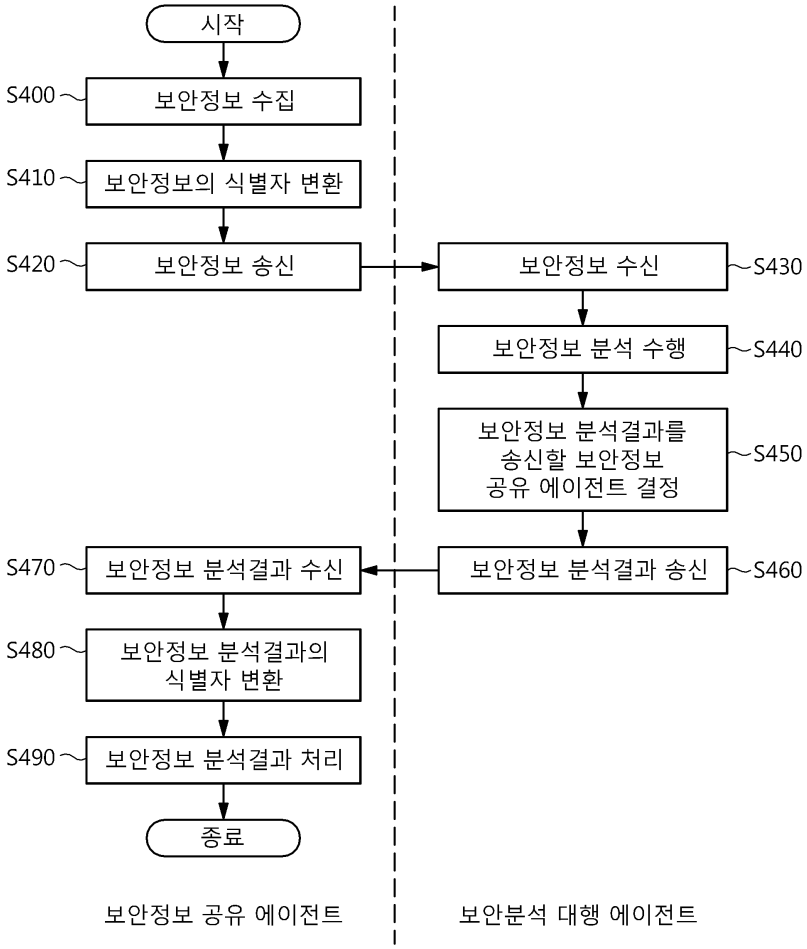
도면2


20b
제2 보안 관리
도메인
200b
제2 보안 정보
공유 에이전트 장치
익명기반
보안정보
익명기반
보안정보결과
30
보안 분석 도메인
300
보안 분석 대행
에이전트 장치
익명기반
보안정보
익명기반
보안정보결과
20a
제1 보안 관리
도메인
200a
제1 보안 정보
공유 에이전트 장치

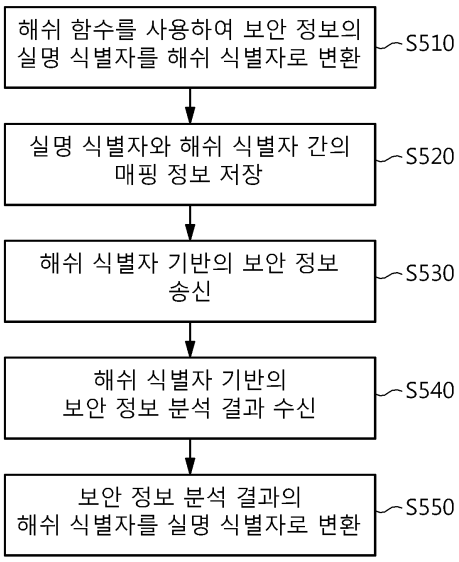
도면3


200
210
보안 정보 제공부
220
식별자 변환부
230
식별자 매핑정보 저장부
240
242
보안정보 송신부
244
보안분석 정보 수신부
250
보안 분석 정보 처리부
익명기반 보안정보
익명기반 보안정보 분석결과
300
310
312
보안 정보 수신부
314
보안 분석 정보 송신부
320
식별자 출처 저장부
340
수신 에이전트 장치 결정부
330
보안 정보 분석부

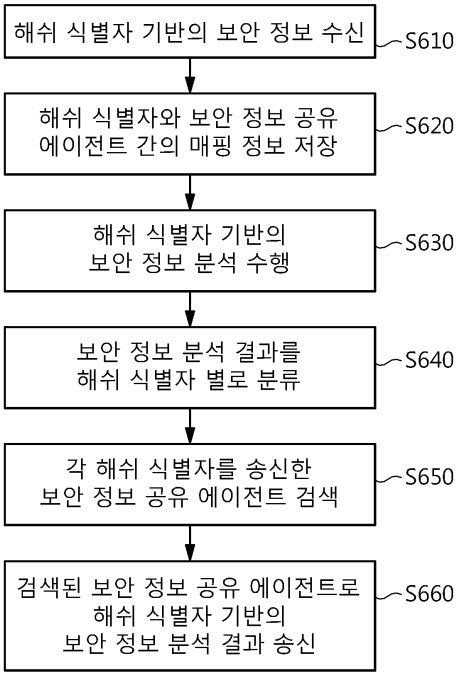
도면4


시작
S400
보안정보 수집
S410
보안정보의 식별자 변환
S420
보안정보 송신
보안정보 수신
S430
보안정보 분석 수행
S440
보안정보 분석결과를
송신할 보안정보
공유 에이전트 결정
S450
보안정보 분석결과 송신
S460
S470
보안정보 분석결과 수신
S480
보안정보 분석결과의
식별자 변환
S490
보안정보 분석결과 처리
종료
보안정보 공유 에이전트
보안분석 대행 에이전트

도면5


해쉬 함수를 사용하여 보안 정보의
실명 식별자를 해쉬 식별자로 변환
S510
실명 식별자와 해쉬 식별자 간의
매핑 정보 저장
S520
해쉬 식별자 기반의 보안 정보
송신
S530
해쉬 식별자 기반의
보안 정보 분석 결과 수신
S540
보안 정보 분석 결과의
해쉬 식별자를 실명 식별자로 변환
S550

도면6


해쉬 식별자 기반의 보안 정보 수신
S610
해쉬 식별자와 보안 정보 공유 에이전트 간의 매핑 정보 저장
S620
해쉬 식별자 기반의 보안 정보 분석 수행
S630
보안 정보 분석 결과를 해쉬 식별자 별로 분류
S640
각 해쉬 식별자를 송신한 보안 정보 공유 에이전트 검색
S650
검색된 보안 정보 공유 에이전트로 해쉬 식별자 기반의 보안 정보 분석 결과 송신
S660