(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년02월25일
(11) 등록번호 10-2081492
(24) 등록일자 2020년02월19일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *G06F 16/00* (2019.01)
(52) CPC특허분류
G06F 21/577 (2013.01)
G06F 16/258 (2019.01)
(21) 출원번호 10-2017-0171242
(22) 출원일자 2017년12월13일
심사청구일자 2017년12월13일
(65) 공개번호 10-2019-0070583
(43) 공개일자 2019년06월21일
(56) 선행기술조사문헌
KR1020170035248 A*
US20160366174 A1*
KR1020170135495 A
KR1020160119678 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
건국대학교 산학협력단
서울특별시 광진구 능동로 120, 건국대학교내 (화양동)
(72) 발명자
김기천
서울특별시 서초구 방배로 270, 다동 504호 (방배동, 신삼호아파트)
진정하
경기도 용인시 기흥구 보정로 30, 118동 902호(보정동, 행원마을동아솔레시티아파트)
유요셉
서울특별시 노원구 공릉로 320, 401동 304호(하계동, 하계동청구빌라)
(74) 대리인
특허법인 무한

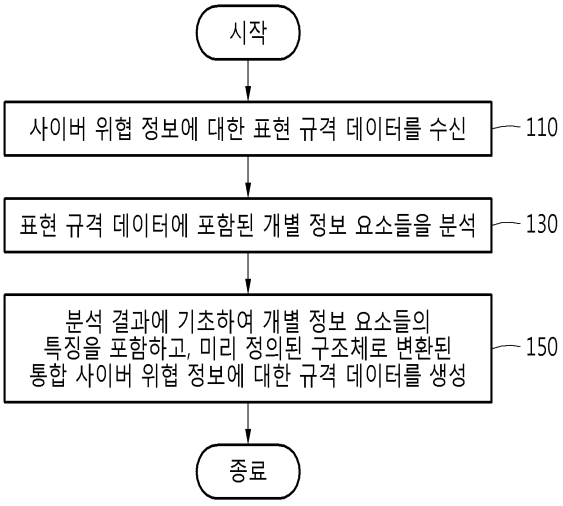
전체 청구항 수 : 총 17 항 심사관 : 구대성

(54) 발명의 명칭 **사이버 위협 정보에 대한 통합 표현 규격 데이터 생성 방법 및 장치**

(57) 요 약

사이버 위협 정보에 대한 통합 표현 규격 데이터 생성 방법 및 장치가 개시된다. 통합 표현 규격 데이터 생성 방법은 사이버 위협 정보에 대한 표현 규격 데이터를 수신하는 단계, 상기 표현 규격 데이터에 포함된 개별 정보 요소들을 분석하는 단계, 및 상기 분석 결과에 기초하여, 상기 개별 정보 요소들의 특징을 포함하고, 미리 정의된 구조체로 변환된 상기 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성하는 단계를 포함할 수 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 1711050943
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발 (R&D)사업
연구과제명 블록체인 기반 침해 사고 대응 시스템
기 여 율 0.5/1
주관기관 건국대학교 산학협력단
연구기간 2017.04.01 ~ 2017.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711055567
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발 (R&D)사업
연구과제명 안전한 IoT 전용망 구축을 위한 LPWAN 침해 방지 기술 개발
기 여 율 0.5/1
주관기관 콘벨라(주)
연구기간 2017.04.01 ~ 2017.12.31

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

사이버 위협 정보에 대한 표현 규격 데이터를 수신하는 단계;

상기 표현 규격 데이터에 포함된 개별 정보 요소들을 분석하는 단계; 및

상기 분석 결과에 기초하여, 상기 개별 정보 요소들의 특징을 포함하고, 미리 정의된 구조체로 변환된 상기 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성하는 단계

를 포함하고,

상기 통합 표현 규격 데이터를 생성하는 단계는,

상기 개별 정보 요소들의 특징 중 공통되는 특징 또는 상기 개별 정보 요소들에게 필수적으로 요구되는 특징을 상기 통합 표현 규격 데이터의 일 특징으로 결정하는, 통합 표현 규격 데이터 생성 방법.

청구항 2

제1항에 있어서,

상기 사이버 위협 정보에 대한 표현 규격 데이터 표현 규격 데이터는,

STIX(The Structured Threat Information eXpression)인, 통합 표현 규격 데이터 생성 방법.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 통합 표현 규격 데이터를 생성하는 단계는,

상기 개별 정보 요소의 특징들 중 유사한 역할을 수행하는 서로 다른 명칭의 특징을 상기 통합 표현 규격 데이터 상의 동일한 특징으로 결정하는, 통합 표현 규격 데이터 생성 방법.

청구항 5

제1항에 있어서,

상기 통합 표현 규격 데이터를 생성하는 단계는,

상기 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 상기 통합 표현 규격 데이터 상의 일 특징으로 결정하는, 통합 표현 규격 데이터 생성 방법.

청구항 6

제5항에 있어서,

상기 분석 도구는,

머신 러닝(machine learning)을 포함하는, 통합 표현 규격 데이터 생성 방법.

청구항 7

제1항에 있어서,

상기 통합 표현 규격 데이터는,

상기 개별 정보 요소의 유형에 대한 정보 및 상기 개별 정보 요소의 식별자에 대한 정보를 일 특징으로 포함하는, 통합 표현 규격 데이터 생성 방법.

청구항 8

제1항에 있어서,

상기 통합 표현 규격 데이터는,

상기 개별 정보 요소에 포함되는 세부 정보 요소에 대한 정보를 일 특징으로 포함하는, 통합 표현 규격 데이터 생성 방법.

청구항 9

제1항에 있어서,

상기 통합 표현 규격 데이터는,

사이버 위협에 대한 대응 방안에 대한 정보를 일 특징으로 포함하는, 통합 표현 규격 데이터 생성 방법.

청구항 10

사이버 위협 정보를 수신하는 단계;

상기 사이버 위협 정보에 대한 표현 규격 데이터에 기초하여, 상기 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성하는 단계; 및

상기 통합 표현 규격 데이터에 기초하여, 상기 사이버 위협 정보를 가공하는 단계

를 포함하고,

상기 통합 표현 규격 데이터를 생성하는 단계는,

개별 정보 요소들의 특징 중 공통되는 특징 또는 상기 개별 정보 요소들에게 필수적으로 요구되는 특징을 상기 통합 표현 규격 데이터의 일 특징으로 결정하는, 사이버 위협 정보 가공방법.

청구항 11

제10항에 있어서,

상기 사이버 위협 정보를 가공하는 단계는,

상기 통합 표현 규격 데이터에 포함되는 특징들에 기초하여 상기 사이버 위협 정보를 분류하는, 사이버 위협 정보 가공 방법.

청구항 12

제10항에 있어서,

상기 통합 표현 규격 데이터를 생성하는 단계는,

상기 사이버 위협 정보에 대한 표현 규격 데이터에 포함된 개별 정보 요소의 특징에 대한 정보를 획득하는 단계; 및

상기 개별 정보 요소의 특징에 대한 정보에 기초하여, 상기 개별 정보 요소의 특징을 모두 포함하고, 미리 정의된 구조체로 변환된 상기 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성하는 단계

를 포함하는, 사이버 위협 정보 가공방법.

청구항 13

삭제

청구항 14

제12항에 있어서,

상기 통합 표현 규격 데이터를 생성하는 단계는,

상기 개별 정보 요소의 특징 중 유사한 역할을 수행하는 서로 다른 명칭의 특징을 통합 사이버 위협 표현 규격 데이터 상의 동일한 특징으로 결정하는, 사이버 위협 정보 가공방법.

청구항 15

제12항에 있어서,

상기 통합 표현 규격 데이터를 생성하는 단계는,

상기 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 상기 통합 표현 규격 데이터 상의 일 특징으로 결정하는, 사이버 위협 정보 가공방법.

청구항 16

사이버 위협 정보에 대한 표현 규격 데이터를 수신하는 수신부;

상기 표현 규격 데이터에 포함된 개별 정보 요소의 특징에 대한 정보를 획득하는 특징 정보 획득부; 및

상기 개별 정보 요소의 특징에 대한 정보에 기초하여, 상기 개별 정보 요소의 특징을 모두 포함하고, 미리 정의된 구조체로 변환된 통합 표현 규격 데이터를 생성하는, 통합 표현 규격 데이터 생성부

를 포함하고,

상기 통합 표현 규격 데이터 생성부는,

상기 개별 정보 요소의 특징 중 공통되는 특징 또는 상기 개별 정보 요소들에게 필수적으로 요구되는 특징을 상기 통합 표현 규격 데이터의 일 특징으로 결정하는, 통합 표현 규격 데이터 생성 장치.

청구항 17

삭제

청구항 18

제16항에 있어서,

상기 통합 표현 규격 데이터 생성부는,

상기 개별 정보 요소의 특징 중 유사한 역할을 수행하는 서로 다른 명칭의 특징을 상기 통합 표현 규격 데이터 상의 동일한 특징으로 결정하는, 통합 표현 규격 데이터 생성 장치.

청구항 19

제16항에 있어서,

상기 통합 표현 규격 데이터 생성부는,

상기 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 상기 통합 표현 규격 데이터 상의 일 특징으로 결정하는, 통합 표현 규격 데이터 생성 장치.

청구항 20

제1항, 제2항, 제4항 내지 제12항, 제14항 및 제15항 중 어느 한 항의 방법을 구현하기 위한 프로세서에 의해 실행되는 프로그램이 기록된 컴퓨터로 읽을 수 있는 기록 매체.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 사이버 위협 정보에 대한 통합 표현 규격 데이터 생성 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] STIX(The Structured Threat Information eXpression)은 미국 국토안보부에서 사이버 정보 위협에 대한 내용을 표준화하고 구조화시킨 것으로서, 사이버 위협에 대해 일관적인 분석 및 자동화된 해석을 가능하게 하는 표현 규격 데이터이다. STIX는 등록된 사이버 위협 정보에 대해서는 자동화된 해석을 지원할 수 있지만 새로운 공격에 대한 사이버 위협 정보를 자동으로 추가하는 방식을 지원할 수는 없다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0003] 일 실시예에 따른 통합 표현 규격 데이터 생성 방법은 사이버 위협 정보에 대한 표현 규격 데이터를 수신하는 단계; 상기 표현 규격 데이터에 포함된 개별 정보 요소들을 분석하는 단계; 및 상기 분석 결과에 기초하여, 상기 개별 정보 요소들의 특징을 포함하고, 미리 정의된 구조체로 변환된 상기 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성하는 단계를 포함할 수 있다.

[0004] 일 실시예에 따른 통합 표현 규격 데이터는 STIX(The Structured Threat Information eXpression)일 수 있다.

[0005] 일 실시예에 따른 통합 표현 규격 데이터를 생성하는 단계는 상기 개별 정보 요소들의 특징 또는 상기 개별 정보 요소들에게 필수적으로 요구되는 특징 중 공통되는 특징 또는 상기 개별 정보 요소들에게 필수적으로 요구되는 특징을 상기 통합 표현 규격 데이터의 일 특징으로 결정할 수 있다.

[0006] 일 실시예에 따른 상기 통합 표현 규격 데이터를 생성하는 단계는 상기 개별 정보 요소의 특징 중 유사한 역할을 수행하는 서로 다른 명칭의 특징을 상기 통합 표현 규격 데이터 상의 동일한 특징으로 결정할 수 있다.

[0007] 일 실시예에 따른 통합 표현 규격 데이터를 생성하는 단계는 상기 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 상기 통합 표현 규격 데이터 상의 일 특징으로 결정할 수 있다.

[0008] 일 실시예에 따른 분석 도구는 머신 러닝(machine learning)을 포함할 수 있다.

[0009] 일 실시예에 따른 통합 표현 규격 데이터는 상기 개별 정보 요소의 유형에 대한 정보 및 상기 개별 정보 요소의 식별자에 대한 정보를 포함할 수 있다.

[0010] 일 실시예에 따른 통합 표현 규격 데이터는 상기 개별 정보 요소에 포함되는 세부 정보 요소에 대한 정보를 포함할 수 있다.

[0011] 일 실시예에 따른 통합 표현 규격 데이터는 사이버 위협에 대한 대응 방안에 대한 정보를 포함할 수 있다.

[0012] 일 실시예에 따른 사이버 위협 정보 가공 방법은 사이버 위협 정보를 수신하는 단계; 사이버 위협 정보에 대한 표현 규격 데이터에 기초하여, 상기 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성하는 단계; 및 상기 통합 표현 규격 데이터에 기초하여, 상기 사이버 위협 정보를 가공하는 단계를 포함할 수 있다.

[0013] 일 실시예에 따른 상기 사이버 위협 정보를 가공하는 단계는 상기 통합 표현 규격 데이터에 포함되는 특징들에 기초하여 상기 사이버 위협 정보를 분류할 수 있다.

[0014] 일 실시예에 따른 통합 표현 규격 데이터를 생성하는 단계는 상기 사이버 위협 정보에 대한 표현 규격 데이터에 포함된 개별 정보 요소의 특징에 대한 정보를 획득하는 단계; 및 상기 개별 정보 요소의 특징에 대한 정보에 기초하여, 상기 개별 정보 요소의 특징을 모두 포함하고, 미리 정의된 구조체로 변환된 상기 사이버 위협 정보에

대한 통합 표현 규격 데이터를 생성하는 단계를 포함할 수 있다.

[0015] 일 실시예에 따른 통합 표현 규격 데이터를 생성하는 단계는 상기 개별 정보 요소의 특징 중 공통되는 특징 또는 상기 개별 정보 요소들에게 필수적으로 요구되는 특징을 상기 통합 표현 규격 데이터의 일 특징으로 결정할 수 있다.

[0016] 일 실시예에 따른 통합 표현 규격 데이터를 생성하는 단계는 상기 개별 정보 요소의 특징 중 유사한 역할을 수행하는 서로 다른 명칭의 특징을 상기 통합 사이버 위협 표현 규격 데이터 상의 동일한 특징으로 결정할 수 있다.

[0017] 일 실시예에 따른 상기 통합 표현 규격 데이터를 생성하는 단계는 상기 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 상기 통합 표현 규격 데이터 상의 일 특징으로 결정할 수 있다.

[0018] 일 실시예에 따른 통합 표현 규격 데이터 생성 장치는 사이버 위협 정보에 대한 표현 규격 데이터를 수신하는 수신부; 상기 표현 규격 데이터에 포함된 개별 정보 요소의 특징에 대한 정보를 획득하는 특징 정보 획득부; 및 상기 개별 정보 요소의 특징에 대한 정보에 기초하여, 상기 개별 정보 요소의 특징을 모두 포함하고, 미리 정의된 구조체로 변환된 통합 표현 규격 데이터를 생성하는, 통합 표현 규격 데이터 생성부를 포함할 수 있다.

[0019] 일 실시예에 따른 통합 표현 규격 데이터 생성부는 상기 개별 정보 요소의 특징 중 공통되는 특징 또는 상기 개별 정보 요소들에게 필수적으로 요구되는 특징을 상기 통합 표현 규격 데이터의 일 특징으로 결정할 수 있다.

[0020] 일 실시예에 따른 통합 표현 규격 데이터 생성부는 상기 개별 정보 요소의 특징 중 유사한 역할을 수행하는 서로 다른 명칭의 특징을 상기 통합 표현 규격 데이터 상의 동일한 특징으로 결정할 수 있다.

[0021] 일 실시예에 따른 상기 통합 표현 규격 데이터 생성부는 상기 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 상기 통합 표현 규격 데이터 상의 일 특징으로 결정할 수 있다.

도면의 간단한 설명

[0022] 도 1은 일 실시예에 따른 통합 표현 규격 데이터 생성 방법을 설명하기 위한 흐름도이다.

도 2a는 일 실시예에 따른 사이버 위협 정보에 대한 표현 규격 데이터의 형태를 설명하기 위한 도면이다.

도 2b는 일 실시예에 따른 일 개별 정보 요소의 표현 형태의 일례를 도시하는 도면이다.

도 3a는 일 실시예에 따른 사이버 위협 정보에 대한 통합 표현 규격 데이터의 형태를 설명하기 위한 도면이다.

도 3b는 일 실시예에 따른 통합 표현 규격 데이터의 표현 형태의 일례를 도시하는 도면이다.

도 4는 일 실시예에 따른 통합 표현 규격 데이터에 기초하여 사이버 위협 정보를 가공하는 가공방법을 설명하기 위한 흐름도이다.

도 5는 일 실시예에 따른 통합 표현 규격 데이터 생성 장치의 전체적인 구성을 도시하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0023] 실시예들에 대한 구조적 또는 기능적 설명들은 단지 예시를 위한 목적으로 개시된 것으로서, 다양한 형태로 변경되어 실시될 수 있다. 따라서, 본 명세서의 범위는 개시된 실시예들의 특정한 형태로 한정되는 것이 아니라 설명한 기술적 사상에 포함되는 변경, 균등물, 또는 대체물을 포함한다.

[0024] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 이런 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 해석되어야 한다. 예를 들어, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[0025] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.

[0026] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 설명된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함으로 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0027] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 해당 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0028] 한편, 어떤 실시예가 달리 구현 가능한 경우에 특정 블록 내에 명기된 기능 또는 동작이 순서도와 다르게 수행될 수 있다. 예를 들어, 연속하는 두 블록들이 실제로는 실질적으로 동시에 수행될 수도 있고, 관련된 기능 또는 동작에 따라서는 해당 블록들의 순서가 뒤바뀌어 수행될 수도 있다.

[0029] 이하, 실시예들을 첨부된 도면들을 참조하여 상세하게 설명한다. 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조 부호를 부여하고, 이에 대한 중복되는 설명은 생략하기로 한다.

[0030] 사이버 위협 정보를 표현하는 STIX(The Structured threat Information eXpression)을 토대로 머신 러닝(Machine Learning)을 통해 새로운 사이버 위협 정보를 추출하기 위하여, 자동화된 빅데이터 분석을 수행하기 위해서는, 머신 러닝에 대한 입력으로써 단일 형태의 입력 데이터가 요구된다. STIX의 데이터는 서로 다른 형태의 개별 정보 요소를 포함하기 때문에, 머신 러닝을 통한 데이터 분석을 위해서는 STIX에 포함된 데이터를 단일 형태의 데이터로 변환할 필요가 있다. 통합 표현 규격 데이터 생성 시스템은 데이터 분석을 위한 단일 형태의 입력 데이터 생성을 위하여 통합 표현 규격 데이터를 생성하고, 생성된 통합 표현 규격 데이터를 통해 사이버 위협 정보를 가공할 수 있다. 가공된 사이버 위협 정보는 머신 러닝을 위한 초기 입력으로 사용될 수 있고, 머신 러닝을 통한 데이터 분석을 통해 새로운 사이버 위협 정보가 추출될 수 있다. 본 명세서에서 사용되는 사이버 위협 정보라는 용어는 다양한 형태의 사이버 공격에 대한 내용을 포함하는 정보를 의미할 수 있다.

[0031] 도 1은 일 실시예에 따른 통합 표현 규격 데이터 생성 방법을 설명하기 위한 흐름도이다.

[0032] 도 1을 참조하면, 단계(110)에서 통합 표현 규격 데이터 생성 장치는 사이버 위협 정보에 대한 표현 규격 데이터를 수신할 수 있다. 일 실시예에 따르면, 사이버 위협 정보에 대한 표현 규격 데이터는 STIX일 수 있다. STIX는 미국의 국토안보부에서 사이버 위협 정보를 표준화한 것으로, STIX는 지속적인 업데이트를 통해 변화하는 사이버 공격에 대한 사이버 위협 정보가 반영될 수 있다. 통합 표현 규격 데이터 생성 장치는 업데이트가 진행된 현재 버전의 STIX를 수신하고, 수신한 STIX를 토대로 통합 표현 규격 데이터를 생성할 수 있다.

[0033] 단계(130)에서 통합 표현 규격 데이터 생성 장치는 수신한 표현 규격 데이터에 포함된 개별 정보 요소들을 분석할 수 있다. 사이버 위협 정보에 대한 표현 규격 데이터는 공격에 대한 공격자의 행태 양식에 대한 개별 정보 요소, 위협 탐지를 위한 패턴에 대한 개별 정보 요소와 같이 복수 개의 개별 정보 요소를 포함할 수 있다.

[0034] 일 실시예에 따르면, 개별 정보 요소들은 모든 개별 정보 요소들이 공통으로 포함하는 특징을 포함할 수 있다. 예를 들어, 모든 개별 정보 요소들이 공통으로 포함하는 특징은 개별 정보 요소의 유형에 대한 특징, 개별 정보 요소의 유형에 대한 식별자에 대한 특징, 개별 정보 요소가 생성된 날짜에 대한 정보를 포함할 수 있지만, 공통으로 포함되는 특징은 제시된 예시에 한정되지 않을 수 있다.

[0035] 일 실시예에 따르면, 개별 정보 요소는 개별 정보 요소마다 정의된 특징을 포함할 수 있다. 개별 정보 요소마다 정의된 특징은 해당 특징에 대한 특징 값이 반드시 필요한 특징, 선택적으로 포함할 수 있는 특징, 미래에 사용될 것으로 대비하여 할당되는 특징으로 유형이 분류될 수 있다.

[0036] 일 실시예에 따르면 개별 정보 요소는 일부 개별 정보 요소와 연관되는 특징을 포함할 수 있다. 예를 들어, 개별 정보 요소가 포함하는 일 특징은 일부의 개별 정보 요소들에는 포함되지만, 나머지 개별 정보 요소에는 포함되지 않을 수 있다.

[0037] 통합 표현 규격 데이터 생성 장치는 단계(110)에서 수신한 표현 규격 데이터에 포함된 개별 정보 요소들에 모두에 포함된 공통 특징들 및 개별 정보 요소에 대하여 고유하게 정의된 특징들을 분류하고, 개별 정보 요소에 고유하게 정의된 특징들의 유형을 분류함으로써, 표현 규격 데이터에 포함된 개별 정보 요소들을 분석할 수 있다.

[0038] 단계(150)에서, 통합 표현 규격 데이터 생성 장치는 단계(130)의 분석 결과에 기초하여 개별 정보 요소들의 특징을 모두 포함하고, 미리 정의된 구조체로 변환된 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성할 수 있다.

[0039] 일 실시예에 따르면, 통합 표현 규격 데이터 생성 장치는 개별 정보 요소들의 특징 중 공통되는 특징 또는 개별

정보 요소들에게 필수적으로 요구되는 특징을 통합 표현 규격 데이터의 일 특징으로 결정할 수 있다. 예를 들어, 통합 표현 규격 데이터 생성 장치는 개별 정보 요소의 유형에 대한 특징과 같이 모든 개별 정보 요소가 포함하거나 개별 정보 요소들에게 필수적으로 요구되는 특징을 통합 표현 규격 데이터의 일 특징으로 결정할 수 있다.

[0040] 일 실시예에 따르면, 통합 표현 규격 데이터 생성 장치는 개별 정보 요소의 특징들 중 유사한 역할을 수행하는 서로 다른 명칭의 특징을 통합 표현 규격 데이터 상의 동일한 특징으로 결정할 수 있다. 예를 들어, 개별 정보 요소가 생성된 날짜에 대한 특징이 일 개별 정보 요소와 다른 개별 정보 요소에서 서로 다른 명칭으로 정의되어 있는 경우, 통합 표현 규격 데이터 생성 장치는 서로 다른 명칭으로 정의된 특징을 동일한 명칭을 통해 통합 표현 규격 데이터 상에 일 특징으로 통합시킬 수 있다.

[0041] 일 실시예에 따르면, 통합 표현 규격 데이터 생성 장치는 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 통합 표현 규격 데이터 상의 일 특징으로 결정할 수 있다. 예를 들어, 통합 표현 규격 데이터 생성 장치는 사이버 위협 정보를 분석하는 분석 도구로써 사용되는 머신 러닝에서 데이터 분석에 필수적으로 사용되는 특징을 통합 표현 규격 데이터의 일 특징으로 결정할 수 있다.

[0042] 도 2a는 일 실시예에 따른 사이버 위협 정보에 대한 표현 규격 데이터의 형태를 설명하기 위한 도면이다.

[0043] 도 2a를 참조하면, 표현 규격 데이터는 공격에 대한 공격자의 행태 양식에 개별 정보 요소, 대상에 대한 공격 행동의 그룹에 대한 개별 정보 요소, 공격에 대응하기 위한 조치에 대한 개별 정보 요소, 공격 및 위협요소를 나타내는 ID에 대한 개별 정보 요소, 위협 탐지를 위한 패턴에 대한 개별 정보 요소, 공통된 속성의 공격 set에 대한 개별 정보 요소, 악성 코드 정보에 대한 개별 정보 요소, 시스템/네트워크에서 관찰된 정보에 대한 개별 정보 요소, 위협 정보 모음에 대한 개별 정보 요소, 악의적인 행위자로 간주되는 주체에 대한 개별 정보 요소, 공격에 사용될 수 있는 도구에 대한 개별 정보 요소, 소프트웨어의 실수로 발생하는 취약점에 대한 개별 정보 요소를 포함할 수 있다. 표현 규격 데이터에 포함되는 개별 정보 요소는 제시된 예시에 한정되지 않고, 사이버 위협 정보와 관련된 임의의 정보 요소를 포함할 수 있다.

[0044] 도 2b는 일 실시예에 따른 일 개별 정보 요소의 표현 형태의 일례를 도시하는 도면이다.

[0045] 도 2b에는 소프트웨어의 실수로 발생하는 취약점에 대한 개별 정보 요소인 'Vulnerability'에 포함되는 특징들 및 특징들에 대응되는 특징 값을 포함하는 데이터 구조체가 도시된다. 개별 정보 요소 'Vulnerability'는 특징으로 'type', 'id', 'created', 'modified', 'name' 및 'external_references'를 포함할 수 있고, 제시된 특징들에 대한 특징 값들은 특징들에 대응하여 데이터 구조체 상에 제시될 수 있다.

[0046] 도 3a는 일 실시예에 따른 사이버 위협 정보에 대한 통합 표현 규격 데이터의 형태를 설명하기 위한 도면이다.

[0047] 일 실시예에 따르면, 통합 표현 규격 데이터 생성 장치는 개별 정보 요소들의 특징 중 공통되는 특징 또는 개별 정보 요소들에게 필수적으로 요구되는 특징을 통합 표현 규격 데이터의 일 특징으로 결정할 수 있고, 개별 정보 요소의 특징들 중 유사한 역할을 수행하는 서로 다른 명칭의 특징들을 통합 표현 규격 데이터 상의 동일한 특징으로 결정할 수 있고, 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 통합 표현 규격 데이터 상의 일 특징으로 결정할 수 있다.

[0048] 도 3a를 참조하면, 통합 표현 규격 데이터는 개별 정보 요소의 유형에 대한 정보, 개별 정보 요소의 식별자에 대한 정보, 처음 생성된 날짜에 대한 정보, 포함된 세부 정보 요소의 세부적 유형에 대한 정보, 세부 정보 요소의 식별자에 대한 정보, 위협에 대한 대응 및 예방할 수 있는 행동에 대한 정보, 위협에 대하여 관찰되는 패턴에 대한 정보, 목적 및 목표에 대한 정보, 핵심 특징을 포함하는 자세한 설명에 대한 정보, 세부 정보 요소에 대한 내용의 외부 참조에 대한 정보를 일 특징으로 포함할 수 있다. 통합 표현 규격 데이터에 포함되는 특징에 대한 정보는 제시된 예시에 한정되지 않고, 임의의 사이버 위협에 대한 정보 및 사이버 위협 정보의 분석을 위한 정보를 포함할 수 있다.

[0049] 도 3b는 일 실시예에 따른 통합 표현 규격 데이터의 표현 형태의 일례를 도시하는 도면이다.

[0050] 도 3b에는 소프트웨어의 실수로 발생하는 취약점에 대한 개별 정보 요소인 'Vulnerability'에 대한 데이터를 통합 표현 규격 데이터를 통해 표현한 데이터 구조체의 일례를 도시하는 도면이다. 개별 정보 요소 'Vulnerability'는 특징으로 'type', 'id', 'created', 'labels', 'name', 'action', 'pattern', 'goal', description 및 'references'를 포함할 수 있고, 제시된 특징들에 대한 특징 값들은 특징들에 대응하여 데이터 구조체 상에 제시될 수 있다.

[0051] 도 4는 일 실시예에 따른 통합 표현 규격 데이터에 기초하여 사이버 위협 정보를 가공하는 가공방법을 설명하기 위한 흐름도이다.

[0052] 단계(410)에서 사이버 위협 정보 가공 장치는 사이버 위협 정보를 수신할 수 있다.

[0053] 단계(430)에서 사이버 위협 정보 가공 장치는 수신한 사이버 위협 정보에 대한 표현 규격 데이터에 기초하여 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성할 수 있다.

[0054] 일 실시예에 따르면, 사이버 위협 정보 가공 장치는 사이버 위협 정보에 대한 표현 규격 데이터에 포함된 개별 정보 요소의 특징에 대한 정보를 획득하고, 획득한 개별 정보 요소의 특징에 대한 정보에 기초하여 개별 정보 요소의 특징을 모두 포함하고, 미리 정의된 구조체로 변환된 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성할 수 있다.

[0055] 일 실시예에 따르면, 개별 정보 요소의 특징 중 공통되는 특징 또는 개별 정보 요소들에게 필수적으로 요구되는 특징은 통합 표현 규격 데이터 상의 일 특징으로 결정될 수 있다. 개별 정보 요소의 특징 중 유사한 역할을 수행하는 서로 다른 명칭의 특징들은 통합 사이버 위협 표현 규격 데이터 상의 동일한 특징으로 결정될 수 있다. 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징은 통합 표현 규격 데이터 상의 일 특징으로 결정될 수 있다.

[0056] 단계(450)에서 사이버 위협 정보 가공 장치는 생성된 통합 표현 규격 데이터에 기초하여 사이버 위협 정보를 가공할 수 있다. 사이버 위협 정보 가공 장치는 통합 표현 규격 데이터에 포함되는 특징들에 기초하여 사이버 위협 정보를 분류함으로써 사이버 위협 정보를 가공할 수 있다. 예를 들어, 도 2b에 도시된 사이버 위협 정보는 가공을 통해 도 3b에 제시된 데이터로 변환됨으로써, 단일 형태의 데이터 구조체가 형성될 수 있다.

[0057] 도 5는 일 실시예에 따른 통합 표현 규격 데이터 생성 장치의 전체적인 구성을 도시하는 도면이다.

[0058] 도 5를 참조하면, 통합 표현 규격 데이터 생성 장치(500)는 사이버 위협 정보에 대한 표현 규격 데이터를 수신하는 수신부(510), 표현 규격 데이터에 포함된 개별 정보 요소의 특징에 대한 정보를 획득하는 특징 정보 획득부(530), 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성하는 통합 표현 규격 데이터 생성부(550) 및 생성된 통합 표현 규격 데이터를 저장하는 데이터 베이스(570)를 포함할 수 있다.

[0059] 일 실시예에 따르면 통합 표현 규격 데이터 생성부(550)는 특징 정보 획득부(530)를 통해 획득한 개별 요소의 특징에 대한 정보에 기초하여 개별 정보 요소의 특징을 모두 포함하고, 미리 정의된 구조체로 변환된 통합 규격 데이터를 생성할 수 있다. 예를 들어, 사이버 위협 정보에 대한 표현 규격 데이터는 STIX일 수 있고, 통합 표현 규격 데이터 생성부(550)는 표현 규격 데이터에 포함된 개별 정보 요소의 특징들 중 공통되는 특징 또는 개별 정보 요소들에게 필수적으로 요구되는 특징을 통합 표현 규격 데이터의 일 특징으로 결정할 수 있다. 통합 표현 규격 데이터 생성부(550)는 개별 정보 요소의 특징 중 유사한 역할을 수행하는 서로 다른 명칭의 특징을 통합 표현 규격 데이터 상의 동일한 특징으로 결정할 수 있다. 또한, 통합 표현 규격 데이터 생성부(550)는 사이버 위협 정보를 분석하는 분석 도구에서 사용되는 특징을 통합 표현 규격 데이터 상의 일 특징으로 결정할 수 있다.

[0060] 실시예들에서 설명된 구성요소들은 하나 이상의 DSP (digital signal processor), 프로세서, 컨트롤러, ASIC (application specific integrated circuit), FPGA (field programmable gate array)와 같은 프로그래머블 논리 소자, 다른 전자 기기들 및 이것들의 조합 중 하나 이상을 포함하는 하드웨어 구성 요소에 의해 구현될 수 있다. 실시예들에서 설명된 과정들 또는 기능들 중 적어도 일부는 소프트웨어에 의해 구현될 수 있고, 해당 소프트웨어는 기록 매체에 기록될 수 있다. 실시예들에서 설명된 구성요소들, 기능들 및 과정들은 하드웨어와 소프트웨어의 조합에 의해 구현될 수 있다.

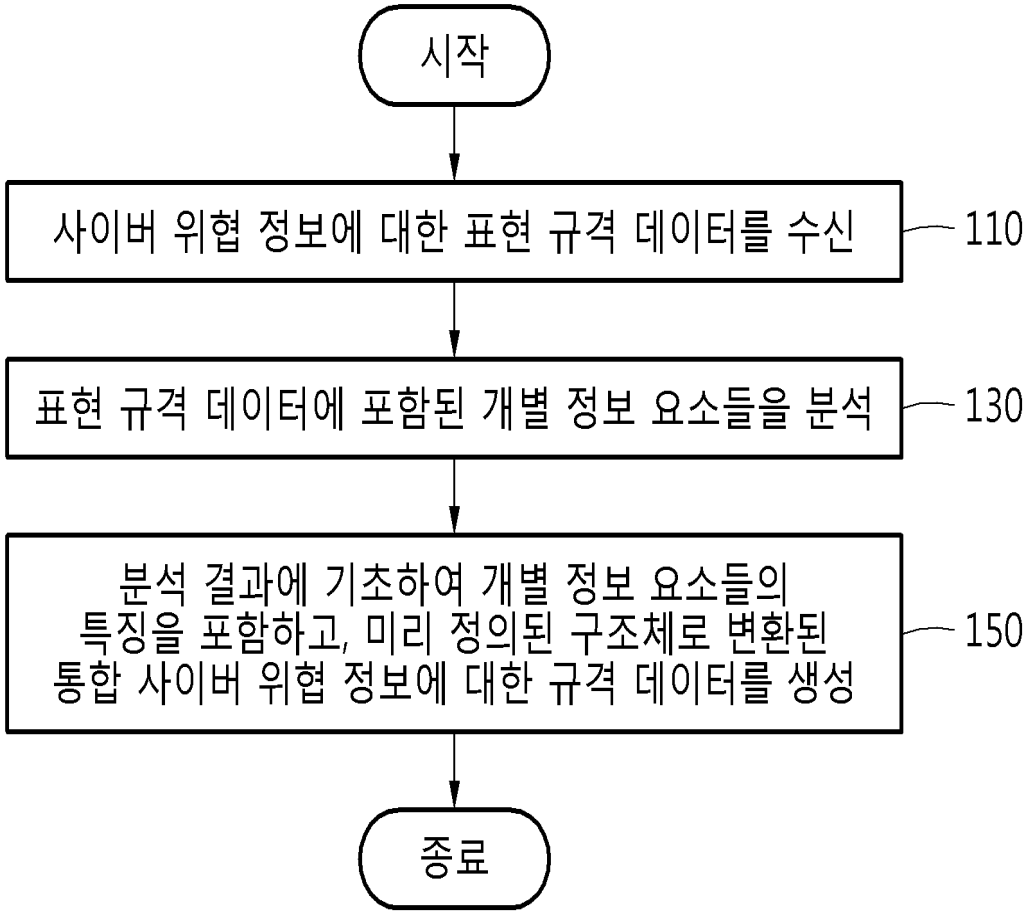
[0061] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 컴퓨터 판독 가능 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과

같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0062] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기를 기초로 다양한 기술적 수정 및 변형을 적용할 수 있다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

도면

도면1



도면2a

Attack Pattern	공격에 대한 공격자의 행태 양식
Campaign	대상에 대한 공격 행동의 그룹
Course of Action	공격에 대응하기 위한 조치
Identity	공격 및 위협요소를 나타내는 ID
Indicator	위협 탐지를 위한 패턴
Intrusion Set	공통된 속성의 공격 set
Malware	악성코드 정보
Observed Data	시스템/네트워크에서 관찰된 정보
Report	위협 정보 모음
Threat Actor	악의적인 행위자로 간주되는 주체
Tool	공격에 사용될 수 있는 도구
Vulnerability	SW 실수로 발생하는 취약점

도면2b


```
{
  "type":  "vulnerability",
  "id":  "vulnerability-0c7b88",
  "created":  "2017-09-12-T13:09:27.000Z",
  "modified":  "2017-09-12T13:09:27.000Z",
  "name":  "CVE-2017-1234",
    "external_references":  [
        {
            "source_name":  "cve",
            "ecternal_id":  "CVE-2017-1234"
        }
    ]
}
```

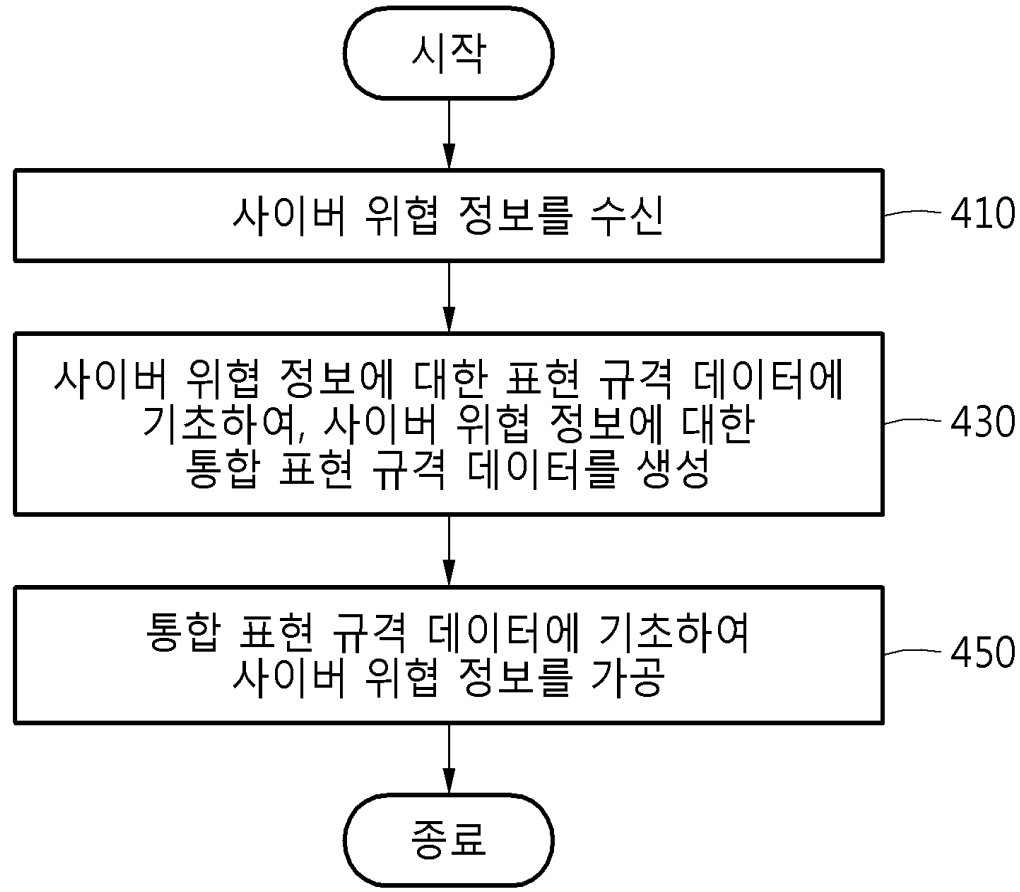
도면3a

Type	정보 요소의 유형
Id	정보 요소에서의 식별자
Created	처음 생성된 날짜
Labels	세부적 유형
Name	세부 정보 요소의 식별자
Action	대응 및 예방할 수 있는 행동
Pattern	관찰되는 패턴
Goal	목적 및 목표
Description	핵심 특징을 포함한 자세한 설명
Reference	세부 정보 요소에 대한 내용의 외부 참조

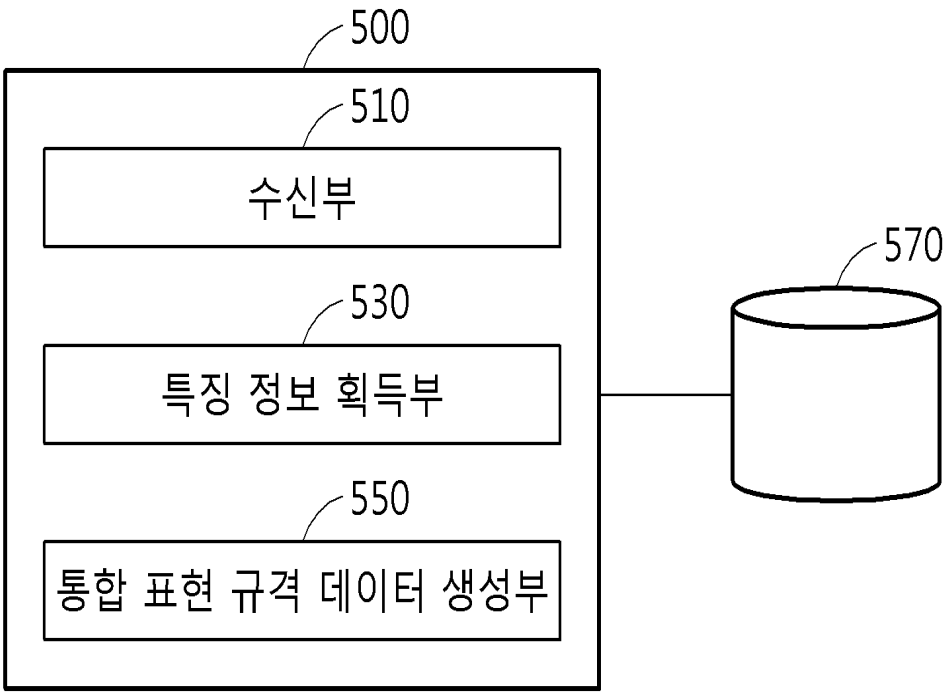
도면3b


```
{
  "type":  "vulnerability",
  "id":  "vulnerability-0c7b88",
  "created":  "2017-09-12T13:09:27.000Z",
  "labels":  "Failure to Handle Exceptional Conditions",
  "name":  "CVE-2017-1234",
  "action":  null,
  "pattern":  null,
  "goal":  null,
  "description":  "http://www.securityfocus.com/bid/99310",
  "reference":  null
}
```

도면4


시작
사이버 위협 정보를 수신
410
사이버 위협 정보에 대한 표현 규격 데이터에 기초하여, 사이버 위협 정보에 대한 통합 표현 규격 데이터를 생성
430
통합 표현 규격 데이터에 기초하여 사이버 위협 정보를 가공
450
종료

도면5


500
510
수신부
530
특징 정보 획득부
550
통합 표현 규격 데이터 생성부
570