

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일

2022 년 1 월 13 일 (13.01.2022)



(10) 국제공개번호

WO 2022/010039 A1

- (51) 국제특허분류:
G06F 21/57 (2013.01) *G06F 21/86* (2013.01)
G06F 21/55 (2013.01) *H04L 29/06* (2006.01)
- (21) 국제출원번호: PCT/KR2020/013835
- (22) 국제출원일: 2020 년 10 월 12 일 (12.10.2020)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2020-0085599 2020 년 7 월 10 일 (10.07.2020) KR
10-2020-0130540 2020 년 10 월 8 일 (08.10.2020) KR
- (71) 출원인: 고려대학교 산학협력단 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION)
[KR/KR]: 02841 서울시 성북구 안암로 145, Seoul (KR).
- (72) 발명자: 강수영 (KANG, Sooyoung); 02794 서울시 성북구 월곡로14길 26, 108동 1302호, Seoul (KR). 김승주 (KIM, Seungjoo); 06218 서울시 강남구 도곡로57길 12, 103동 503호, Seoul (KR).
- (74) 대리인: 이대호 등 (LEE, Dae Ho et al.); 06120 서울시 강남구 강남대로 476 11층, 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK,

MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

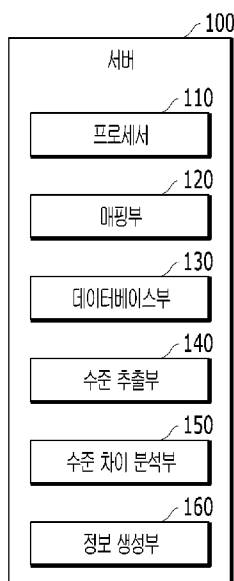
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(54) Title: SECURITY BY DESIGN APPROACH USING EVIDENCE-BASED SECURITY TECHNIQUE

(54) 발명의 명칭: 증거 기반 보안 기법을 활용한 보안내재화 방법론



100...Server
110...Processor
120...Mapper
130...Database unit
140...Level extractor
150...Level difference analyzer
160...Information generator

(57) Abstract: Disclosed according to some embodiments of the present disclosure is a method for security by design. The method for security by design may comprise the steps of: mapping security by design approaches and evidence-based security approaches to each other; and storing the results of the mapping in a database.

(57) 요약서: 본 개시의 몇몇 실시예에 따른, 보안내재화 방법이 개시된다. 상기 보안내재화 방법은 보안내재화 방법론과 증거 기반 보안 방법론을 매핑하는 단계; 및 매핑 결과를 데이터베이스에 저장하는 단계를 포함할 수 있다.

WO 2022/010039 A1

명세서

발명의 명칭: 증거 기반 보안 기법을 활용한 보안내재화 방법론 기술분야

- [1] 본 개시는 보안내재화 방법론에 관한 것으로, 구체적으로 증거 기반 보안 기법을 활용한 보안내재화 방법론에 관한 것이다.

[2]

배경기술

- [3] 미국 정부는 1970년대부터 모의해킹을 통해 컴퓨팅 제품의 개선을 수행하였다. 그러나, 모의해킹을 통한 방법은 모의해킹팀의 역량 및 수행 기간에 따라 취약점 유무가 결정되며, 취약점이 발견되지 않았다고 해서 대상 제품에 취약점이 없음을 보장하는 것이 아니라는 문제가 있었다.
- [4] 이후 미국은 제품의 보안 품질을 향상시키기 위해서는 취약점을 찾고 패치하는 것에만 의존할 것이 아니라 개발 프로세스 자체가 체계적이고 엄격하게 관리되어야 함을 인식하고, 보안내재화(Security by Design)와 관련된 각종 개발 방법론 및 평가조달 체계 관련 표준들을 발표하기 시작했다.
- [5] 여기서, 보안내재화란 제품의 요구사항 분석 및 설계와 같이 개발 초기 단계부터 보안을 고려함으로써 제품의 복잡도를 감소시키고 신뢰성을 달성하기 위한 것일 수 있다. 그리고, 이러한 보안내재화가 포함된 개발 프로세스를 “Secure SDLC(Secure Software Development Life Cycle)” 또는 “보안공학 프로세스(Security Engineering Process)”라고 할 수 있다.
- [6] 그러나 현재 공개되어 있는 Secure SDLC 들의 표준 및 가이드라인들은 추상적인 보안 활동 목록들만 나열하고 있기 때문에 실제 현장에서 Secure SDLC를 구축하는 것은 쉽지 않다.
- [7] 따라서, 기업체가 원하는 수준에 맞게 Secure SDLC를 구체화하기 위한 보안내재화 방법론에 대한 수요가 존재한다.

[8]

발명의 상세한 설명

기술적 과제

- [9] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 증거 기반 보안 기법을 활용한 보안내재화 방법을 제공하고자 한다.
- [10] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

[11]

과제 해결 수단

- [12] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 일 실시예에 따라, 컴퓨팅

장치의 프로세서를 이용한 보안내재화 방법론을 구체화하는 방법으로서, 상기 방법론: 보안내재화 방법론과 증거 기반 보안 방법론을 매핑하는 단계; 및 매핑 결과를 데이터베이스에 저장하는 단계; 를 포함할 수 있다.

- [13] 또한, 상기 매핑 결과는, 적어도 하나의 보안 단계, 적어도 하나의 보안 활동, 적어도 하나의 세부 보안 활동 및 산출물을 포함할 수 있다.
- [14] 또한, 상기 적어도 하나의 보안 단계는, 보안 교육과 관련된 제 1 단계, 착수 및 계획과 관련된 제 2 단계, 요구사항 분석과 관련된 제 3 단계, 획득과 관련된 제 4 단계, 설계와 관련된 제 5 단계, 구현과 관련된 제 6 단계, 검증과 관련된 제 7 단계, 배포와 관련된 제 8 단계, 운영과 관련된 제 9 단계 및 폐기와 관련된 제 10 단계 중 적어도 하나를 포함할 수 있다.
- [15] 또한, 기업체의 특성 및 상기 기업체의 보안내재화 방법론 현황을 인식하는 단계; 상기 보안내재화 방법론 현황에 기초하여, 상기 기업체의 보안내재화 방법론 수준을 인식하는 단계; 상기 특성 및 보안내재화 방법론 현황에 기초하여 상기 기업체와 관련된 경쟁사를 인식하는 단계; 상기 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 단계; 및 상기 경쟁사의 평균 보안내재화 방법론 수준 및 상기 기업체의 상기 보안내재화 방법론 수준에 기초하여, 상기 경쟁사와 상기 기업체의 보안내재화 방법론 수준 차이를 정량적으로 분석하여 제 1 정보를 제공하는 단계; 를 더 포함할 수 있다.
- [16] 또한, 상기 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 단계는, 상기 경쟁사가 수행한 정보 보호 제품의 보안성 표준에 대한 현황 정보를 획득하는 단계; 및 상기 현황 정보에 기초하여 상기 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 단계; 를 포함할 수 있다.
- [17] 또한, 상기 매핑 결과는, 상기 적어도 하나의 보안 활동 각각에 포함되는 복수의 세부 보안 활동 각각에 부여되는 보안내재화 방법론 수준이 기록된 보안내재화 방법론 수준 정보를 포함하고, 상기 매핑 결과 및 상기 보안내재화 방법론 현황에 기초하여, 상기 기업체의 보안내재화 방법론 수준을 인식하는 단계는, 상기 보안내재화 방법론 수준 정보와 상기 보안내재화 방법론 현황에 기초하여, 상기 적어도 하나의 보안 활동 각각에 대한 상기 기업체의 상기 보안내재화 방법론 수준을 인식하는 단계; 를 포함할 수 있다.
- [18] 또한, 상기 제 1 정보를 제공한 이후, 상기 기업체가 원하는 수준의 적정 보안내재화 방법론 수준을 수신하는 단계; 및 상기 매핑 결과에 포함된 적어도 하나의 보안 활동 중 상기 적정 보안내재화 방법론 수준과 관련된 적어도 하나의 필수 보안 활동에 대한 제 2 정보를 제공하는 단계; 를 포함할 수 있다.
- [19] 또한, 상기 제 2 정보는, 상기 적어도 하나의 필수 보안 활동이 포함된 적어도 하나의 필수 보안 단계 각각에 매핑된 적어도 하나의 필수 산출물을 포함할 수 있다.
- [20] 또한, 상기 제 1 정보는, 그래프 형식으로 상기 보안내재화 방법론 수준 차이를 정량적으로 나타낼 수 있다.

- [21] 또한, 상기 그래프는, 상기 적어도 하나의 세부 보안 활동 각각을 나타내는 x축, 상기 적어도 하나의 세부 보안 활동 각각에 대한 보안내재화 방법론 수준을 나타내는 y축, 상기 경쟁사의 평균 보안내재화 방법론 수준을 나타내는 제 1 선 및 상기 기업체의 보안내재화 방법론 수준을 나타내는 제 2 선을 포함할 수 있다.
- [22] 또한, 상기 그래프는, 상기 제 1 선 및 상기 제 2 선 사이의 간극에 의해 형성되는 차이(gap)에 기초하여, 상기 경쟁사 및 상기 기업체의 상기 보안내재화 방법론 수준 차이를 정량적으로 나타낼 수 있다.
- [23] 또한, 보안내재화 방법론과 증거 기반 보안 방법론을 매핑하는 매핑부; 및 매핑 결과를 저장하는 데이터베이스부; 를 포함할 수 있다.
- [24] 또한, 기업체의 특성 및 상기 기업체의 보안내재화 방법론 현황을 인식하고, 상기 보안내재화 방법론 현황에 기초하여, 상기 기업체의 보안내재화 방법론 수준을 인식하고, 상기 특성 및 보안내재화 방법론 현황에 기초하여 상기 기업체와 관련된 경쟁사를 인식하고, 상기 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 수준 추출부; 상기 경쟁사의 평균 보안내재화 방법론 수준 및 상기 기업체의 상기 보안내재화 방법론 수준에 기초하여, 상기 경쟁사와 상기 기업체의 보안내재화 방법론 수준 차이를 정량적으로 분석하여 제 1 정보를 제공하는 수준 차이 분석부; 및 상기 매핑 결과에 포함된 적어도 하나의 보안 활동 중 상기 기업체가 원하는 수준의 적정 보안내재화 방법론 수준과 관련된 적어도 하나의 필수 보안 활동에 대한 제 2 정보를 제공하는 정보 생성부; 를 더 포함할 수 있다.
- [25]
- [26] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

[27]

발명의 효과

- [28] 본 개시의 몇몇 실시예에 따르면, 사용자의 보안 수준의 문제점을 쉽게 파악할 수 있는 보안내재화 방법론을 제공할 수 있도록 한다.
- [29] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

[30]

도면의 간단한 설명

- [31] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의

총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 특정 세부사항들 없이 실시될 수 있음은 명백할 것이다. 다른 예시들에서, 공지의 구조들 및 장치들이 하나 이상의 양상들의 기재를 용이하게 하기 위해 블록도 형태로 도시된다.

[32]

[33] 도 1은 본 개시의 몇몇 실시예에 따른 서버의 일례를 설명하기 위한 블록 구성도이다.

[34] 도 2는 본 개시의 몇몇 실시예에 따른 서버가 매핑 결과를 데이터베이스에 저장하는 방법의 일례를 설명하기 위한 흐름도이다.

[35] 도 3은 본 개시의 몇몇 실시예에 따른 데이터베이스부에 저장된 매핑 결과의 일례를 설명하기 위한 도면이다.

[36] 도 4는 본 개시의 몇몇 실시예에 따른 매핑 결과의 일례를 설명하기 위한 도면이다.

[37] 도 5는 본 개시의 몇몇 실시예에 따른 서버가 제 2 정보를 제공하는 방법의 일례를 설명하기 위한 흐름도이다.

[38] 도 6은 본 개시의 몇몇 실시예에 따른 서버가 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 방법의 일례를 설명하기 위한 흐름도이다.

[39] 도 7은 본 개시의 몇몇 실시예에 따른 서버가 기업체와 경쟁사의 차이점을 분석하기 위해 생성하는 그래프의 일례를 설명하기 위한 도면이다.

[40] 도 8은 본 개시내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도를 도시한다.

[41]

발명의 실시를 위한 최선의 형태

[42] 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 감지될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다. 구체적으로, 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다.

[43] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에

개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.

- [44] 비록 제 1, 제 2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제 1 소자나 구성요소는 본 발명의 기술적 사상 내에서 제 2 소자나 구성요소 일 수도 있음은 물론이다.
- [45] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [46] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.
- [47] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.
- [48] 더불어, 본 명세서에서 사용되는 용어 "정보" 및 "데이터"는 종종 서로 상호교환 가능하도록 사용될 수 있다.
- [49] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다.
- [50] 이하의 설명에서 사용되는 구성 요소에 대한 접미사 "모듈" 및 "부"는 명세서

작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

- [51] 본 개시의 목적 및 효과, 그리고 그것들을 달성하기 위한 기술적 구성들은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 본 개시를 설명하는데 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로써 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다.
- [52] 그러나 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있다. 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [53]
- [54] 도 1은 본 개시의 몇몇 실시예에 따른 서버의 일례를 설명하기 위한 블록 구성도이다.
- [55] 도 1을 참조하면, 서버(100)는 프로세서(110), 매핑부(120), 데이터베이스부(130), 수준 추출부(140), 수준 차이 분석부(150) 및 정보 생성부(160)를 포함할 수 있다. 다만, 상술한 구성 요소들은 서버(100)를 구현하는데 있어서 필수적인 것은 아니어서, 서버(100)는 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.
- [56] 서버(100)는, 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [57] 한편, 프로세서(110)는 통상적으로 서버(100)의 전반적인 동작을 처리할 수 있다. 프로세서(110)는 서버의 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 데이터베이스부(130)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.
- [58] 한편, 매핑부(120)는 보안내재화 방법론과 증거 기반 보안 방법론을 매핑할 수 있다. 여기서, 보안내재화 방법론은 Secure SDLC 표준 및 가이드라인을 포함할 수 있다. 일례로, 보안내재화 방법론은 Microsoft SDL, NIST SSDLC, CSA SDF, OWASP CLASP, McGraw, Touchpoints, SAFECODE, OWASP BSIMM, OWASP SAMM, NIST RMF 및 SAEJ3061 등의 Secure SDLC 표준 및 가이드라인을 포함할 수 있다. 다만, 이에 한정되는 것은 아니다. 한편, 증거 기반 보안 방법론은 표준은 ISO/IEC 15408-CC(Common Criteria), ISO/IEC 27001 ISMS(Information

Security Management System), ISO/IEC 27701-PIMS(Privacy Information Management System) 및 ISO/IEC 8405-CEM(Common Evaluation Methodology) 등을 포함할 수 있다. 다만, 이에 한정되는 것은 아니다. 이하, 매핑부(120)에 대한 설명은 도 2를 통해 후술한다.

- [59] 한편, 본 개시의 몇몇 실시예에 따르면 매핑부(120)는 상기 보안내재화 방법론에 포함된 단계를 비교 분석할 수 있다.
- [60] 구체적으로, 매핑부(120)는 상기 보안내재화 방법론에 포함된 복수개의 Secure SDLC 표준 및 가이드라인 각각에 포함된 보안 활동 중 중복된 보안 활동을 합칠 수 있다. 예를 들어, 매핑부(120)는 10 종의 Secure SDLC의 각 단계들을 비교 분석하여 10개의 단계로 정규화 및 일반화할 수 있다. 그리고, 매핑부(120)는 각 단계에서 수행해야하는 보안 활동을 모두 합한 후 중복되는 보안 활동을 도출함으로써 하나의 보안내재화 방법론으로 통합할 수 있다. 일례로, 매핑부(120)는 10개의 단계와 66개의 보안 활동을 갖는 매핑 결과를 생성할 수 있다. 다만, 이에 한정되는 것은 아니다. 이하, 매핑부(120)가 매핑 결과를 생성하는 방법의 일례는 도 3을 통해 후술한다.
- [61] 한편, 데이터베이스부(130)는 상술한 보안내재화 방법론 및 증거 기반 보안 방법론들이 사전 저장되어 있을 수 있다. 다만, 이에 한정되는 것은 아니고, 향후 공신력 있는 Secure SDLC가 학술 및 산업계에 소개될 경우 관련 데이터를 추가하여 프레임워크를 확장할 수도 있다.
- [62] 한편, 본 개시에서 데이터베이스부(130)는 매핑부(120)에 의해 매핑된 매핑 결과를 저장할 수 있다. 이하, 데이터베이스부(130)에 대한 설명은 도 2를 통해 후술한다.
- [63] 한편, 본 개시의 몇몇 실시예에 따르면, 데이터베이스부(130)의 스키마(schema)는 복수개의 테이블로 구성될 수 있다. 여기서, 스키마는 데이터베이스부(130)를 구성하는 레코드의 크기, 키(key)의 정의, 레코드와 레코드의 관계, 검색 방법 등일 수 있다. 다만, 이에 한정되는 것은 아니다.
- [64] 한편, 데이터베이스부(130)에 포함된 복수개의 테이블 중 제 1 테이블에는 통합된 보안내재화 방법론의 10개의 단계들이 저장되어 있을 수 있다. 또한, 제 2 테이블에는 각 단계 별로 수행해야 하는 66개의 보안 활동들이 저장되어 있을 수 있다. 또한, 제 3 테이블에는 ISO/IEC 15408-CC 3부 및 ISO/IEC 8405-CEM에 정의되어 있는 보증요구사항 컴포넌트 63개, ISO/IEC 27001 ISMS에 정의되어 있는 세부 점검 항목 104개, ISO/IEC 27701-PIMS에 정의되어 있는 세부 평가 항목 54개를 합하여 총 221개의 세부 보안 활동들이 저장되어 있을 수 있다. 그리고, 제 4 테이블에는 ISO/IEC 15408-CC 및 ISO/IEC 8405-CEM의 보증 요구사항 항목과 매핑한 결과인 산출해야 할 문서들의 템플릿이 저장되어 있을 수 있다. 다만, 이에 한정되는 것은 아니다.
- [65] 한편, 데이터베이스부(130)는 메모리 및/또는 영구저장매체를 포함할 수 있다. 메모리는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk

type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다.

- [66] 한편, 수준 차이 분석부(150)는 수준 추출부(140)로부터 생성된 수준에 기초하여, 경쟁사와 기업체의 차이를 정량적으로 분석해주기 위한 것일 수 있다.
- [67] 구체적으로, 수준 차이 분석부(150)는 경쟁사의 평균 보안내재화 방법론 수준 및 기업체의 보안내재화 방법론 수준에 기초하여, 경쟁사와 기업체의 보안내재화 방법론 수준 차이를 정량적으로 분석하여 제 1 정보를 제공할 수 있다. 여기서, 제 1 정보는 그래프 형식으로 보안내재화 방법론 수준 차이를 정량적으로 나타내는 정보일 수 있다. 다만, 이에 한정되는 것은 아니다.
- [68] 예를 들어, 수준 차이 분석부(150)는 기업체 및 기업체의 경쟁사가 선정된 경우, 기업체와 경쟁사의 보안내재화 방법론 수준 차이를 정량적으로 나타내기 위한 그래프를 생성할 수 있다. 이 경우, 사용자는 보안내재화 방법론 활동 중 미흡한 단계 및 보안 활동을 한눈에 파악할 수 있으며, 기업체의 보안내재화 방법론 활동의 문제점을 파악하는데 용이할 수 있다. 이하, 수준 차이 분석부(150) 및 수준 차이 분석부(150)에 의해 생성된 그래프와 관련된 내용은 도 6을 통해 후술한다.
- [69] 한편, 본 개시에서 보안내재화 방법론 수준은 정확성(functional correctness), 안정성(safety integrity) 및 보안성(security assurance)을 고려한 지표로서, 복수개의 단계로 구성될 수 있다.
- [70] 예를 들어, 보안내재화 방법론 수준은 7개의 단계로 구성될 수 있으며, 높은 단계일수록 보안내재화 방법론 수준이 체계적이고 엄격하게 관리된다는 것을 의미할 수 있다.
- [71] 한편, 본 개시에서, 수준 추출부(140)는 정확성, 안정성 및 보안성 중 하나의 속성만 매핑할 경우, 해당 속성의 수준을 산정할 수 있다. 또는, 수준 추출부(140)는 2개 이상의 속성이 매핑될 경우, 보안 활동 수행 현황을 통해 수준이 조율될 수 있다. 이러한 과정을 통해 산출되는 수준은 보안 활동 별로 도출될 수 있다. 그리고 그 결과는 그래프 형식으로 출력되어 보안내재화 방법론 수준을 한눈에 파악할 수 있도록 할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [72] 한편, 정보 생성부(160)는 매핑 결과에 포함된 적어도 하나의 보안 활동 중 기업체가 원하는 수준의 적정 보안내재화 방법론 수준과 관련된 적어도 하나의 필수 보안 활동에 대한 제 2 정보를 제공할 수 있다.
- [73] 예를 들어, 정보 생성부(160)는 수준 차이 분석부(150)에서 생성되는 결과에 기초하여, 기업체가 원하는 수준의 보안내재화 방법론 수준, 보안 활동, 세부 보안 활동 및 산출해야 할 문서 중 적어도 하나를 도출할 수 있다. 다만, 이에

한정되는 것은 아니다. 이하, 정보 생성부(160)가 제공하는 제 2 정보에 대한 내용은 도 5를 통해 후술한다.

[74] 한편, 본 개시의 몇몇 실시예에 따르면, 정보 생성부(160)는 기업체와 경쟁사 간의 보안내재화 방법론 수준 차이가 너무 큰 경우 한 번에 경쟁사 수준에 도달하기 어렵기 때문에, 기업체의 현재 상황을 고려하여 기업체가 원하는 수준의 보안내재화 방법론 수준을 구축할 수 있다. 다만, 이에 한정되는 것은 아니다.

[75] 한편, 본 개시에서, 서버(100)는 사용자 입력부 또는 통신부를 통해 사용자로부터 기업체 및 경쟁사에 대한 정보를 입력 받을 수 있다. 이 경우, 정보 생성부(160) 기업체 및 경쟁사의 특성에 기초하여, 매핑부(120)를 통해 생성된 66개의 보안 활동 중 기업체 및 경쟁사와 관련된 보안 활동들을 선택할 수 있다. 그리고, 정보 생성부(160)는 기업체로부터 수신되는 정보에 기초하여, 기업체가 원하는 보안내재화 방법론 수준을 달성하기 위한 세부 보안 활동 및 산출해야 할 문서 등을 생성할 수 있다. 이 경우, 산출해야 할 문서가 쉽게 도출됨으로써 추적성을 확보할 수 있다. 또한, 현장에서 보안 문제가 발생했을 경우 원인을 파악하고 신속하게 대응할 수 있다. 다만, 이에 한정되는 것은 아니다.

[76]

[77] 도 2는 본 개시의 몇몇 실시예에 따른 서버가 매핑 결과를 데이터베이스에 저장하는 방법의 일례를 설명하기 위한 흐름도이다.

[78] 도 2를 참조하면, 서버(100)의 매핑부(120)는 보안내재화 방법론과 증거 기반 보안 방법론을 매핑할 수 있다(S110).

[79] 구체적으로, 매핑부(120)는 보안내재화 방법론에 포함된 복수의 Secure SDLC 표준 및 가이드라인 각각의 단계를 비교 분석할 수 있다. 그리고, 매핑부(120)는 상기 보안내재화 방법론에 포함된 보안 활동 중 중복된 보안 활동을 합칠 수 있다. 예를 들어, 매핑부(120)는 10 종의 Secure SDLC의 각 단계들을 비교 분석하여 10개의 단계로 정규화 및 일반화할 수 있다. 그리고, 매핑부(120)는 각 단계에서 수행해야 하는 보안 활동을 모두 합한 후 중복되는 보안 활동을 도출함으로써 하나의 보안내재화 방법론으로 통합할 수 있다. 이 경우, 매핑부(120)는 10개의 단계와 66개의 보안 활동을 갖는 보안내재화 방법론을 생성할 수 있다. 이하, 10개의 단계와 66개의 보안 활동을 갖는 보안내재화 방법론에 대해서는 도 3을 통해 후술한다.

[80] 한편, 매핑부(120)는 보안내재화 방법론이 통합되어 생성된 경우, 보안내재화 방법론에 증거 기반 보안 방법론을 매핑할 수 있다.

[81] 구체적으로, 매핑부(120)는 상기 증거 기반 보안 방법론 중 가장 먼저 ISO/IEC 15408-CC의 3부 및 ISO/IEC 8405-CEM에 정의되어 있는 63개의 보증요구사항을 이용하여, 보안내재화 방법론에 매핑을 수행할 수 있다.

[82] 한편, 서버(100)의 매핑부(120)에 의해 생성된 66개의 보안 활동 중, ISO/IEC 15408-CC에서는 다루지 않는 항목이 존재할 수 있다. 예를 들어, 보안 및

개인정보보호 관련 교육, 보안 교육과 관련된 일정 계획 및 보안 교육 로드맵 수립 등은 ISO/IEC 15408-CC에는 포함되어 있지 않을 수 있다. 따라서, 매핑부(120)는 ISO 27001-ISMS에 정의되어 있는 104개의 세부 점검 항목을 활용하여, 보안내재화 방법론에 매핑을 수행할 수 있다.

- [83] 한편, 매핑부(120)에 의해 생성된 66개의 보안 활동 중, ISO/IEC 15408-CC 및 ISO 27001-ISMS에서 다루지 않는 항목이 더 존재할 수 있다. 예를 들어, 개인정보보호 영향평가 등은 ISO/IEC 15408-CC 및 ISO 27001-ISMS에는 포함되어 있지 않을 수 있다. 따라서, 매핑부(120)는 개인정보보호 관점에서 수행되어야 하는 보안 활동들은 ISO/IEC 27701-PIMS에 정의되어 있는 54개의 세부 평가 항목을 활용하여, 보안내재화 방법론에 매핑을 수행할 수 있다.
- [84] 결과적으로, 매핑부(120)는 ISO/IEC 15408-CC의 보증요구사항 컴포넌트 63개, ISO 27001-ISMS의 세부 점검 항목 104개, ISO/IEC 27701-PIMS의 세부 평가 항목 54개를 합하여 총 221개의 세부 항목들과 66개의 보안 활동 간 매핑을 수행함으로써, 세부 보안 활동 및 산출해야 할 문서 등을 생성할 수 있다. 다만, 이에 한정되는 것은 아니다. 한편, 본 개시에 따른 매핑부(120)가 66개의 보안 활동에 매핑을 수행한 221개의 세부 보안 활동들에 대해선 도 4를 통해 후술한다.
- [85] 한편, 본 개시의 몇몇 실시예에 따르면, 서버(100)의 매핑부(120)는 보안내재화 방법론에 증거 기반 보안 방법론 표준을 매핑하여, 산출물 목록을 도출할 수 있다. 여기서, 산출물은 기존 소프트웨어 공학에서 산출하는 문서에, 보안과 관련된 항목을 추가한 것일 수 있다. 다만, 이에 한정되는 것은 아니다.
- [86] 한편, 66개의 보안 활동들이 대표적인 증거 기반 보안 방법론 표준인 ISO/IEC 15408-CC와 매핑되어 산출물까지 모두 도출된 경우, 조직이나 개인 정보에 대한 보안 활동은 ISO 27001-ISMS 및 ISO/IEC 27701-PIMS로 보완될 수 있다.
- [87] 구체적으로, ISO/IEC 15408-CC는 보안성을 평가하기 위한 2부의 보안요구사항, 보증 수준을 평가하기 위한 3부 및 ISO/IEC 8405-CEM의 보증요구사항을 포함할 수 있다. 여기서, ISO/IEC 15408-CC의 3부 및 ISO/IEC 8405-CEM의 보증요구사항은 요구사항 분석, 개발, 설치 및 운영, 생명주기 지원, 테스트 및 취약점 분석 단계로 분류될 수 있다. 그리고, 보증요구사항은 보안내재화 방법론의 단계와 유사하기 때문에 대부분의 보안 활동들을 커버할 수 있다. 또한 보증요구사항은 각 단계별로 수행해야 하는 세부 항목들을 포함하고 있으며, 산출해야 할 문서들이 충족해야 하는 상세한 요구 조건들이 포함되어 있을 수 있다. 따라서, 이를 활용하여 상세 세부 보안 활동들을 정의하고 산출해야 할 문서들의 템플릿을 생성할 수 있다. 여기서, 템플릿은 산출물과 관련된 문서를 생성하기 위한 양식 등이 포함된 샘플 문서 일 수 있다. 다만, 이에 한정되는 것은 아니다. 다만, 이에 한정되는 것은 아니다.
- [88] 상술한 바와 같이, 서버(100)의 매핑부(120)가 보안내재화 방법론과 증거 기반 보안 방법론을 매핑하는 경우, 적어도 하나의 보안 단계, 적어도 하나의 보안

활동, 적어도 하나의 세부 보안 활동 및 산출물을 포함하는 매핑 결과가 생성될 수 있다. 다만, 이에 한정되는 것은 아니다.

[89] 한편, 서버(100)의 프로세서(110)는 매핑 결과를 데이터베이스에 저장할 수 있다(S120). 이하, 본 개시에 따른 매핑 결과에 대한 내용은 도 3 및 도 4를 통해 후술한다.

[90] 한편, 본 개시의 몇몇 실시예에 따르면, 매핑 결과는 보안내재화 방법론 수준 정보를 포함할 수 있다. 이 경우, 수준 추출부(140)는 보안내재화 방법론 수준 정보에 기초하여, 기업체의 보안내재화 방법론 수준을 인식할 수 있다. 이하, 수준 추출부(140)가 매핑 결과에 포함된 보안내재화 방법론 수준 정보에 기초하여, 기업체의 보안내재화 방법론 수준을 인식하는 방법은 도 5를 통해 후술한다.

[91]

[92] 도 3은 본 개시의 몇몇 실시예에 따른 데이터베이스부에 저장된 매핑 결과의 일례를 설명하기 위한 도면이다.

[93] 도 3을 참조하면, 서버(100)의 데이터베이스부(130)에 저장된 보안내재화 방법론의 매핑 결과는 적어도 하나의 보안 단계, 적어도 하나의 보안 활동 및 산출물을 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[94] 제 1 단계는 보안 교육(Security Training)에 대한 단계일 수 있다. 그리고, 제 1 단계에는 3개의 보안 활동이 포함될 수 있다.

[95] 구체적으로, 제 1 단계의 보안 활동은 기본 보안 교육, 심화 보안 교육 및 보안 교육 관련 일정 계획 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[96] 한편, 제 1 단계에서는 교육 일정, 교육을 받아야 하는 대상, 교육 커리큘럼 등에 대한 계획과 해당 교육을 이수한 사람의 명단을 포함하였으나, 보안이 고려됨에 따라 기존 교육에서 보안과 관련된 교육 내용이 추가될 수 있다. 따라서, 제 1 단계의 산출물 목록은 보안 교육 계획서 및 교육 참석자 명단 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[97] 한편, 제 2 단계는 착수 및 계획(Initiation)에 대한 단계일 수 있다. 그리고, 제 2 단계에는 9개의 보안 활동이 포함될 수 있다.

[98] 구체적으로, 제 2 단계의 보안 활동은 프로젝트 범주화, 역할 식별, 프로젝트에 사용될 도구 선정, 보안 요구사항 출처 식별, 최소 품질 및 보안 수준 정의, 보안 이슈 처리에 대한 보상 체계 마련, 보안 일정 계획 및 관리, 보안 목표 설정 및 보안 목표의 일관성 및 완전성 검증의 보안 활동 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[99] 한편, 제 2 단계에서, 현행 프로세스 분석서 및 현행 시스템 분석서는 기존의 보안내재화 방법론과 동일하게 산출될 수 있다. 다만, 프로젝트 일정, 프로젝트 범위, 역할 등에 대한 계획을 다루는 프로젝트 계획서와 사용자의 요구사항을 명세한 요구사항 정의서는 보안을 고려해야 하는 범위를 산정하고, 보안 기능

요구사항을 추가적으로 포함되어야 할 수 있다. 따라서, 제 2 단계의 산출물 목록은 현행 프로세스 분석서, 현행 시스템 분석서, 프로젝트 계획서 및 요구사항 정의서 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[100] 한편, 제 3 단계는 요구사항 분석(Requirements Analysis)에 대한 단계일 수 있다. 그리고, 제 3 단계에는 9개의 보안 활동이 포함될 수 있다.

[101] 구체적으로, 제 3 단계의 보안 활동은 프로젝트 보안 분석 범위 산정, 영향평가서, 인터페이스 정의서, 개인정보보호 영향평가, 사업상 영향평가, 안전성 영향평가, 기존 소프트웨어 평가, 기능 요구사항 도출, 보안 요구사항 도출, 분야별 요구사항에 대한 적합성 및 충돌 여부 판단 및 보안 목표에 따른 요구사항 검증 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[102] 한편, 제 3 단계에서 기존의 보안내재화 방법론은 사업 영향도만 분석할 수 있었다. 다만, 본 개시에서는 보안 및 프라이버시 영향도를 추가적으로 분석한 영향평가서가 산출될 수 있다. 또한, 기존 인터페이스에 대한 식별자, 목적, 사용 방법 등을 명세한 인터페이스 정의서는 보안 기능을 수행하는 정도(직접 수행, 간접 수행 등)에 따라 인터페이스를 분류하여 명세될 수 있다. 따라서, 제 3 단계의 산출물 목록은 영향평가서 및 인터페이스 정의서 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[103] 한편, 제 4 단계는 획득(Acquisition)에 대한 단계일 수 있다. 그리고, 제 4 단계에는 3개의 보안 활동이 포함될 수 있다.

[104] 구체적으로, 제 4 단계의 보안 활동은 획득 범위 및 계획 수립, Third-party 구성요소에 대한 보안 요구사항 정의, Third-party 구성요소에 대한 보안 요구사항 평가 및 테스트 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[105] 한편, 제 4 단계에서는 third-party가 개발한 구성요소에 대해 검수하는 획득 검수서가 산출되어야 한다. 따라서, 제 4 단계의 산출물 목록은 획득 검수서를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[106] 제 5 단계는 설계(Design)에 대한 단계일 수 있다. 그리고, 제 5 단계에는 12개의 보안 활동이 포함될 수 있다.

[107] 구체적으로, 제 5 단계의 보안 활동은 보안 기능 설계 및 명세, 설계 모범사례 및 원칙 준수, 통합 과정에 대한 구조 설계, 자산 식별, 데이터 흐름도 작성, 위협 도출, 공격 라이브러리 수집, 위험 분석, 완화방안 도출, 개인정보보호 분석, 사용 및 오용 사례 식별 및 요구사항에 따른 설계 검증 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[108] 한편, 제 5 단계에서는 클래스, 컴포넌트, 데이터베이스 등에 대한 설계를 명세하는 설계 명세서가 보안 기능을 수행하는 정도에 따라 모듈을 분류하여 명세되어야 할 수 있다. 또한, 소프트웨어 아키텍처 설계서 및 시스템 아키텍처

설계서는 보안 정책에 따라 보안 기능이 정확하게 동작하며 우회 경로가 없음을 입증하도록 명세되어야 할 수 있다. 또한, 모듈을 설계하며 모듈 간 통합을 검증하기 위한 통합 테스트 계획서 및 테스트 시나리오는 보안 모듈 간 통합 내용을 추가적으로 포함해야 할 수 있다. 따라서, 제 5 단계의 산출물 목록은 설계 명세서, SW 아키텍처 설계서, 시스템 아키텍처 설계서 및 통합 테스트 계획서 및 통합 테스트 시나리오 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

- [109] 제 6 단계는 구현(Implementation)에 대한 단계일 수 있다. 그리고, 제 6 단계에는 3개의 보안 활동이 포함될 수 있다.
- [110] 구체적으로, 제 6 단계의 보안 활동은 코딩 가이드라인 준수, 배포 가이드 문서 및 도구 생성 및 설계에 따른 구현 검증 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [111] 한편, 제 6 단계에서는 보안을 고려한 보안 코딩 가이드라인을 준수하여 개발한 소스코드가 산출되어야 하며, 보안 모듈을 테스트하기 위한 단위 테스트 계획서 및 테스트 시나리오가 산출되어야 할 수 있다. 따라서, 제 6 단계의 산출물 목록은 소스코드, 단위 테스트 계획서 및 테스트 시나리오 및 단위 테스트 결과서 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [112] 한편, 제 7 단계는 검증(Verification)에 대한 단계일 수 있다. 그리고, 제 7 단계에는 8개의 보안 활동이 포함될 수 있다.
- [113] 구체적으로, 제 7 단계의 보안 활동은 수동 정적 분석, 자동 정적 분석, 동적 분석, 통합 및 인수 테스트, 침투 테스트, 위협 모델 검토 및 업데이트, 최소 품질 및 보안 수준 검토 및 보안 문서 검토 및 업데이트 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [114] 한편, 제 7 단계에서는 보안을 고려한 통합, 시스템, 인수 테스트에 대한 테스트 계획서 및 테스트 시나리오가 산출되어야 할 수 있다. 또한, 기존 개발 프로세스에서는 수행하지 않았던 취약성 분석을 수행함에 따라 취약성 분석서가 산출되어야 할 수 있다. 따라서, 제 7 단계의 산출물 목록은 통합/시스템/인수 테스트 계획서 및 테스트 시나리오, 통합/시스템/인수 테스트 결과서 및 취약성 분석서 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [115] 제 8 단계는 배포(Release)에 대한 단계일 수 있다. 그리고, 제 8 단계에는 7개의 보안 활동이 포함될 수 있다.
- [116] 구체적으로, 제 8 단계의 보안 활동은 최종 보안 검토, 최종 개인정보보호 검토, 생산을 위한 요구사항 도출, 생산 절차 결정, 생산에 대한 검증, 비상 사고 대응계획 및 배포 과정에 대한 보안 검토 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [117] 한편, 제 8 단계는 기존에는 품질을 최종 검토했던 반면 보안 및 프라이버시에 대한 최종 검토 내용이 추가됨에 따라 리허설 계획서 및 리허설 결과서가

산출되어야 할 수 있다. 또한, 기존 배포 과정에 물리적 보안 대책과 논리적 보안 대책이 모두 고려된 배포 요청서가 산출되어야 할 수 있다. 더하여, 제 8 단계의 산출물 목록에는 배포 이후 비상 사고를 대비하여 비상 사고 대응 계획서와 비상 사고 대응 결과서가 산출되어야 할 수 있다. 따라서, 제 8 단계의 산출물 목록은, 리허설 계획서 및 리허설 결과서, 배포 요청서, 비상 사고 대응 계획서 및 비상 사고 대응 결과서 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

- [118] 한편, 제 9 단계는 운영(Operation)에 대한 단계일 수 있다. 그리고, 제 9 단계에는 7개의 보안 활동이 포함될 수 있다.
- [119] 구체적으로, 제 9 단계의 보안 활동은 모니터링 대상 지표 및 데이터 수집, 보고 전략 식별, 지속적인 모니터링, 취약점 보고, 취약점에 대한 평가, 해결방안 수립, 취약점 공개 및 업데이트 관리 및 배포 이후 형상관리 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [120] 한편, 제 9 단계에서는 보안상 안전한 설치 및 운영 지침과 공격자에게 정보를 제한하기 위한 오류 메시지, 운영환경에서 충족되어야 하는 보안 대책 등이 포함된 설치 결과서, 운영자 지침서, 사용자 지침서가 산출되어야 할 수 있다. 또한, 운영 단계에서 발생한 취약점에 대해 대응 계획서 및 패치 결과가 산출되어야 할 수 있다. 따라서, 제 9 단계의 산출물 목록은 설치 결과서, 운영자 지침서, 사용자 지침서, 취약점 대응 계획서 및 취약점 패치 결과서 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [121] 한편, 제 10 단계는 폐기(Disposal)에 대한 단계일 수 있다. 그리고, 제 10 단계에는 5개의 보안 활동이 포함될 수 있다.
- [122] 구체적으로, 제 10 단계의 보안 활동은 폐기 및 전이 계획 수립, 중요정보 보존, 매체 완전 소거, 하드웨어 및 소프트웨어 폐기 및 시스템 종료 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [123] 한편, 제 10 단계에서는 프로젝트 수행에 있어 시스템 사용에 대해 계획하고 이행하며, 시스템을 이관하거나 폐기하는 것에 대해 계획하고 이행하는 시스템 이행계획서와 이행결과서가 산출되어야 할 수 있다. 따라서, 제 10 단계의 산출물 목록은 시스템 이행계획서 및 시스템 이행결과서 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [124] 한편, 본 개시에서, 데이터베이스부(130)에는 각 단계의 추적성을 확보하기 위한 증거 기반 보안 방법론 표준의 출처를 포함하는 매핑표가 포함되어 있을 수 있다.
- [125] 예를 들어, 보안내재화 방법론에 포함된 10개의 단계 중 제 3 단계는 '요구사항 분석 단계'일 수 있다. 그리고, 제 3 단계에 포함된 19번째 보안 활동은 '보안 요구사항 도출'일 수 있다. 이때, '보안 요구 사항 도출' 보안 활동의 경우, ISO/IEC 15408-CC의 'ASE_REQ.1 보안요구사항' 보증요구사항 컴포넌트 및 ISO/IEC 27001 ISMS의 '8.1.1 보안요구사항 정의' 세부 점검 항목과 매핑될 수 있다. 이

경우 제 3 단계인 '요구사항 분석 단계'에서 산출해야 하는 문서는 '보안이 고려된 SRS(Software Requirement Specification)'일 수 있다. 그리고, 상기 문서의 템플릿에는 인터페이스와 보안기능요구사항 간 매핑표가 포함되어 있어, 두 요소 간 추적성을 확보할 수 있다. 따라서, 실제 현장에서 보안 문제가 발생하면 매핑표를 통해 원인을 파악하고 신속하게 보안 대책을 강구할 수 있다. 다만, 이에 한정되는 것은 아니다.

- [126] 상술한 바와 같이, 본 개시에 따른 보안내재화 방법론은 10개의 단계, 66개의 보안 활동 및 산출물 목록을 포함할 수 있다.
- [127] 한편, 본 개시의 몇몇 실시예에 따르면, 매핑 결과에는 적어도 하나의 세부 보안 활동이 더 포함될 수 있다. 이하, 도 4를 통해 본 개시에 따른 매핑 결과에 대해 좀 더 설명한다.
- [128]
- [129] 도 4는 본 개시의 몇몇 실시예에 따른 매핑 결과의 일례를 설명하기 위한 도면이다.
- [130] 도 4를 참조하면, 서버(100)의 매핑부(120)는 증거 기반 보안 방법론에 포함된 세부 항목을 활용할 수 있다. 일례로, 매핑부(120)는 ISO/IEC 15408-CC, ISO 27001-ISMS 및 ISO/IEC 27701-PIMS 등 3개의 표준에 포함된 세부 항목을 활용할 수 있다.
- [131] 구체적으로, 매핑부(120)는 ISO/IEC 15408-CC 표준에 포함된 63개의 보증요구사항 컴포넌트를 활용할 수 있다. 좀 더 구체적으로, 매핑부(120)는 보안목표명세서 분류에 포함된 10개의 컴포넌트, 개발 분류에 포함된 19개의 컴포넌트, 설치 및 운영 분류에 포함된 2개의 컴포넌트, 생명주기 지원 분류에 포함된 18개의 컴포넌트, 테스트 및 취약점 평가 분류에 포함된 9개의 컴포넌트 등의 보증요구사항 컴포넌트를 활용할 수 있다.
- [132] 한편, 매핑부(120)는 ISO 27001-ISMS 표준에 포함된 104개의 세부 점검 항목을 활용할 수 있다. 구체적으로, 매핑부(120)는 정보보호 정책에 포함된 6개의 세부 점검 항목, 정보보호 조직에 포함된 4개의 세부 점검 항목, 외부자 보안에 포함된 3개의 세부 점검 항목, 정보자산 분류에 포함된 3개의 세부 점검 항목, 정보보호 교육에 포함된 4개의 세부 점검 항목, 인적 보안에 포함된 5개의 세부 점검 항목, 물리적 보안에 포함된 9개의 세부 점검 항목, 시스템 개발 보안에 포함된 10개의 세부 점검 항목, 암호 통제에 포함된 2개의 세부 점검 항목, 접근 통제에 포함된 14개의 세부 점검 항목, 운영 보안에 포함된 22개의 세부 점검 항목, 침해사고 관리에 포함된 7개의 세부 점검 항목, IT 재해복구에 포함된 3개의 세부 점검 항목 및 정보보호 관리에 포함된 12개의 세부 점검 항목 등의 세부 점검 항목을 활용할 수 있다.
- [133] 한편, 매핑부(120)는 ISO/IEC 27701-PIMS 표준에 포함된 54개의 세부 평가 항목을 활용할 수 있다. 구체적으로, 매핑부(120)는 대상기관 개인정보보호 관리체계에 포함된 8개의 세부 평가 항목, 대상 시스템의 개인정보보호

관리체계에 포함된 6개의 세부 평가 항목, 개인정보처리 단계별 보호 조치에 포함된 12개의 세부 평가 항목, 대상 시스템의 기술적 보호 조치에 포함된 19개의 세부 평가 항목 및 특정 IT 기술 활용 시 개인정보보호 정보보호에 포함된 9개의 세부 평가 항목 등의 세부 평가 항목을 활용할 수 있다.

[134] 결과적으로, 매핑부(120)는 3개의 표준으로부터 도출된 221개의 세부 항목들과 66개의 보안 활동들에 대한 매핑을 수행함으로써, 적어도 하나의 세부 보안 활동들을 정의하고 산출해야 할 문서 등을 생성할 수 있다. 다만, 이에 한정되는 것은 아니다.

[135]

[136] 도 5는 본 개시의 몇몇 실시예에 따른 서버가 제 2 정보를 제공하는 방법의 일례를 설명하기 위한 흐름도이다.

[137] 도 5를 참조하면, 서버(100)의 수준 추출부(140)는 기업체의 특성 및 기업체의 보안내재화 방법론 현황을 인식할 수 있다(S210).

[138] 일례로, 수준 추출부(140)는 사용자 입력부(미도시) 또는 통신부(미도시)를 통해 기업체로부터 수신된 정보에 기초하여, 기업체의 특성 및 현황을 파악할 수 있다. 여기서, 기업체의 특성은 기업체가 수행하고 있는 업무의 업종 또는 업태 동일 수 있다. 다만, 이에 한정되는 것은 아니다.

[139] 한편, 서버(100)의 수준 추출부(140)는 보안내재화 방법론 현황에 기초하여, 기업체의 보안내재화 방법론 수준을 인식할 수 있다(S220).

[140] 구체적으로, 수준 추출부(140)는 기업체가 수행하고 있는 보안내재화 방법론 현황을 정량적으로 분석한 후 기업체의 보안내재화 방법론 수준을 인식할 수 있다. 여기서, 보안내재화 방법론 수준은 정확성(functional Correctness), 안정성(safety Integrity) 및 보안성(security Assurance)을 고려한 지표로서, 복수개의 단계로 구성될 수 있다.

[141] 예를 들어, 보안내재화 방법론 수준은 7개의 단계로 구성될 수 있으며, 높은 단계일수록 보안내재화 방법론 수준이 체계적이고 엄격하게 관리된다는 것을 의미할 수 있다. 다만, 이에 한정되는 것은 아니다.

[142] 한편, 본 개시의 몇몇 실시예에 따르면, 서버(100)의 데이터베이스부(130)에 저장된 매핑 결과는 보안내재화 방법론 수준 정보를 포함하고 있을 수 있다. 이때, 보안내재화 방법론 수준 정보는 적어도 하나의 보안 활동 각각에 포함되는 복수의 세부 보안 활동 각각에 부여되는 보안내재화 방법론 수준일 수 있다. 이 경우, 수준 추출부(140)는 상기 보안내재화 방법론 수준 정보와 상기 보안내재화 방법론 현황에 기초하여, 상기 적어도 하나의 보안 활동 각각에 대한 상기 기업체의 상기 보안내재화 방법론 수준을 인식할 수 있다. 다만, 이에 한정되는 것은 아니다.

[143] 한편, 본 개시의 몇몇 실시예에 따르면, 서버(100)의 수준 추출부(140)는 매핑 결과에 포함된 10개의 단계 중 적어도 하나의 단계 또는 적어도 하나의 보안 활동에 대한 기업체의 보안내재화 수준을 인식할 수도 있다.

- [144] 예를 들어, 수준 추출부(140)는 매핑 결과에 포함된 적어도 하나의 단계와 관련된 내용을 기업체가 수행하고 있는 경우, 해당 단계 및 보안 활동을 선택할 수 있다. 다른 일례로, 수준 추출부(140)는 매핑 결과에 포함된 적어도 하나의 단계와 관련된 내용을 기업체가 수행하고 있지 않은 경우, 해당 단계 및 보안 활동을 선택할 수 있다.
- [145] 한편, 서버(100)의 수준 차이 분석부(150)는 기업체의 특성 및 보안내재화 방법론 현황에 기초하여 기업체와 관련된 경쟁사를 인식할 수 있다(S230).
- [146] 일례로, 수준 차이 분석부(150)는 기업체의 특성에 기초하여, 유사한 업종 또는 업태를 갖는 업체를 경쟁사로 인식할 수 있다.
- [147] 다른 일례로, 수준 차이 분석부(150)는 사용자 입력부 또는 통신부를 통해 기업체로부터 경쟁사에 대한 정보를 입력 받을 수 있다. 다만, 이에 한정되는 것은 아니다.
- [148] 또 다른 일례로, 수준 차이 분석부(150)는 기존에 분석한 적어도 하나의 경쟁사의 보안내재화 방법론 수준에 대한 정보가 저장되어 있는 경우, 기존의 경쟁사 중 보안내재화 방법론 수준이 유사한 경쟁사를 인식할 수도 있다. 다만, 이에 한정되는 것은 아니다.
- [149] 한편, 서버(100)의 수준 추출부(140)는 경쟁사의 평균 보안내재화 방법론 수준을 인식할 수 있다(S240).
- [150] 구체적으로, 수준 추출부(140)는 경쟁사가 수행한 정보 보호 제품의 보안성 표준에 대한 현황 정보를 획득하여, 경쟁사의 평균 보안내재화 방법론 수준을 인식할 수 있다. 다만, 이에 한정되는 것은 아니다. 이하, 수준 추출부(140)가 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 방법은 도 6을 통해 후술한다.
- [151] 한편, 본 개시에서, 서버(100)의 수준 추출부(140)는 통신부 또는 사용자 입력부를 통해 기업체로부터 경쟁사의 평균 보안 내재화 방법론 수준에 대한 정보를 수신할 수도 있다. 다만, 이에 한정되는 것은 아니다.
- [152] 한편, 서버(100)의 수준 차이 분석부(150)는 경쟁사의 평균 보안내재화 방법론 수준 및 기업체의 보안내재화 방법론 수준에 기초하여, 경쟁사와 기업체의 보안내재화 방법론 수준 차이를 정량적으로 분석하여 제 1 정보를 제공할 수 있다(S160).
- [153] 구체적으로, 수준 차이 분석부(150)는 그래프 형식으로 기업체의 보안내재화 방법론 수준과 경쟁사의 보안내재화 방법론 수준 차이를 나타내는 제 1 정보를 제공할 수 있다. 다만, 이에 한정되는 것은 아니다. 이하, 본 개시에 따른 제 1 정보에 대한 내용은 도 7을 통해 후술한다.
- [154] 한편, 본 개시에서 서버(100)의 수준 차이 분석부(150)는 제 1 정보가 생성된 경우, 디스플레이부(미도시)를 통해 제 1 정보를 출력할 수 있다. 다른 일례로, 수준 차이 분석부(150)는 제 1 정보가 생성된 경우, 제 1 정보를 기업체와 관련된 단말로 전송할 수도 있다. 다만, 이에 한정되는 것은 아니다.

- [155] 한편, 제 1 정보를 제공한 이후, 서버(100)의 정보 생성부(160)는 기업체가 원하는 수준의 적정 보안내재화 방법론 수준을 수신할 수 있다(S260).
- [156] 일례로, 정보 생성부(160)는 사용자 입력부 또는 통신부를 통해 기업체로부터 기업체가 원하는 수준의 적정 보안내재화 방법론 수준을 수신할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [157] 한편, 서버(100)의 정보 생성부(160)는 매핑 결과에 포함된 적어도 하나의 보안 활동 중 적정 보안내재화 방법론 수준과 관련된 적어도 하나의 필수 보안 활동에 대한 제 2 정보를 제공할 수 있다(S270). 여기서, 제 2 정보는 적어도 하나의 필수 보안 활동이 포함된 적어도 하나의 필수 보안 단계 각각에 매핑된 적어도 하나의 필수 산출물을 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [158] 한편, 본 개시에서, 정보 생성부(160)는 기업체가 원하는 수준의 적정 보안내재화 방법론 수준에 기초하여, 데이터베이스부(130)에 보안내재화 방법론의 10개의 단계 중 적어도 하나의 필수 보안 단계를 선택할 수 있다. 이 경우, 적어도 하나의 필수 보안 단계에 매핑된 적어도 하나의 필수 산출물이 산출될 수 있다. 그리고, 정보 생성부(160)는 적어도 하나의 필수 산출물에 기초하여, 기업체에 제공할 템플릿을 생성할 수 있다. 여기서, 템플릿은 산출물과 관련된 문서를 생성하기 위한 양식 등이 포함된 샘플 문서 일 수 있다. 다만, 이에 한정되는 것은 아니다.
- [159] 한편, 본 개시에서 서버(100)의 정보 생성부(160)는 제 2 정보가 생성된 경우, 제 2 정보를 기업체와 관련된 단말로 전송할 수도 있다. 다만, 이에 한정되는 것은 아니다.
- [160]
- [161] 도 6은 본 개시의 몇몇 실시예에 따른 서버가 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 방법의 일례를 설명하기 위한 흐름도이다.
- [162] 도 6을 참조하면, 서버(100)의 수준 추출부(140)는 경쟁사가 수행한 정보 보호 제품의 보안성 표준에 대한 현황 정보를 획득할 수 있다(S241).
- [163] 일례로, 수준 추출부(140)는 사용자 입력부 또는 통신부를 통해 기업체로부터 현황 정보를 수신할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [164] 한편, 서버(100)의 수준 추출부(140)는 현황 정보에 기초하여 경쟁사의 평균 보안내재화 방법론 수준을 인식할 수 있다(S242).
- [165] 구체적으로, 수준 추출부(140)는 현재 경쟁사가 수행하고 있는 정보 보호 제품의 보안성 표준에 대한 현황 정보에 따라, 평균 보안내재화 방법론 수준을 생성할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [166] 좀 더 구체적으로, 데이터베이스부(130)에는 7단계의 보안내재화 방법론 수준에 대한 기 설정된 값이 저장되어 있을 수 있다. 이 경우, 수준 추출부(140)는 매핑부(120)에 의해 기 생성된 매핑 결과와, 경쟁사가 수행하고 있는 현황 정보를 비교할 수 있다. 그리고, 수준 추출부(140)는 비교된 결과와 기 설정된 값을 이용하여, 경쟁사의 보안내재화 방법론 수준을 생성할 수 있다. 다만, 이에

한정되는 것은 아니다.

[167]

[168] 도 7은 본 개시의 몇몇 실시예에 따른 서버가 기업체와 경쟁사의 차이점을 분석하기 위해 생성하는 그래프의 일례를 설명하기 위한 도면이다. 도 7에 도시된 그래프의 x축은 적어도 하나의 세부 보안 활동 각각을 나타낼 수 있고, y축은 적어도 하나의 세부 보안 활동 각각에 대한 보안내재화 방법론 수준을 나타낼 수 있다. 그리고, 도 7의 제 1 선은 경쟁사의 평균 보안내재화 방법론 수준을 나타내기 위한 선일 수 있고, 제 2 선은 기업체의 보안내재화 방법론 수준을 나타내기 위한 선일 수 있다. 도 7의 g1 및 g2는 제 1 선 및 제 2 선 사이의 간극에 의해 형성되는 차이(gap)를 설명하기 위한 것일 수 있다.

[169] 도 7에서는, 서버(100)의 수준 차이 분석부(150)가 상기 기업체는 개발 초기 단계부터 배포 및 운영단계까지 모두 수행하고 있다고 인식한 경우, 수준 차이 분석부(150)는 이와 유사한 특징을 가진 경쟁사가 대표적인 소프트웨어 개발사인 Microsoft 사라고 인식할 수 있다. 이하, 경쟁사가 Microsoft 사라고 가정하고 이하 설명한다.

[170] 한편, 서버(100)의 수준 추출부(140)는 Microsoft 사의 평균 보안내재화 수준을 인식할 수 있다.

[171] 구체적으로, 수준 추출부(140)는 Microsoft가 기존에 ISO/IEC 15408-CC 인증을 획득한 사례를 기반으로 Microsoft 사의 평균 보안내재화 수준을 산정할 수 있다.

[172] 예를 들어, Microsoft 사의 최근 5년간 표준은 ISO/IEC 15408-CC 인증 사례는 데이터베이스 제품 5종과 운영체제 7종에 대한 사례일 수 있다. 이 경우, 수준 추출부(140)는 상기 인증 사례에 기초하여, Microsoft 사의 평균 보안내재화 수준이 4레벨이라고 인식할 수 있다.

[173] 한편, 서버(100)의 수준 차이 분석부(150)는 기업체가 수행하고 있는 보안내재화 방법론 현황에 기초하여, 기업체의 보안내재화 방법론 수준을 결정할 수 있다. 그리고, 수준 추출부(140)는 데이터베이스부(130)에 저장된 매핑 결과에 기초하여, 기업체와 연관된 단계 및 보안 활동 목록을 선택할 수 있다.

[174] 예를 들어, 수준 추출부(140)는 매핑 결과에 포함된 10개의 단계 중 보안 교육, 착수 및 계획, 요구사항 분석, 설계, 구현, 검증, 배포 및 운영 단계 등의 총 8개의 단계를 선택할 수 있다. 또한, 수준 추출부(140)는 66개의 보안 활동 중 58개의 보안 활동을 선택할 수 있다. 그리고, 수준 추출부(140)는 58개의 보안 활동 각각에 대한 보안내재화 수준을 생성할 수 있다.

[175] 한편, 수준 차이 분석부(150)는 기업체 및 경쟁사의 보안내재화 수준이 생성된 경우, 기업체와 경쟁사의 정량적 차이를 나타내기 위한 그래프를 생성할 수 있다. 그리고, 생성된 그래프는 도 7과 같이 나타낼 수 있다.

[176] 도 7을 참조하면, 그래프는 제 1 선 및 제 2 선 사이의 간극에 의해 형성되는 차이(gap)에 기초하여, 경쟁사 및 기업체의 보안내재화 방법론 수준 차이를 정량적으로 나타낼 수 있다. 여기서, 제 1 선은 경쟁사의 평균 보안내재화 방법론

수준을 나타내고 제 2 선은 기업체의 보안내재화 방법론 수준을 나타낼 수 있다. 다만, 이에 한정되는 것은 아니다.

[177] 예를 들어, g1을 참조하면, 착수 및 계획 단계에 대한 단계인 2단계 중 프로젝트에 사용될 도구 선정과 관련된 보안 활동의 경우, 기업체의 보안내재화 방법론 수준은 2이고, 경쟁사의 보안내재화 방법론 수준은 4일 수 있다.

[178] 다른 예를 들어, g2을 참조하면, 요구사항 분석에 대한 단계인 3단계 중 사업상 영향평가와 관련된 보안 활동의 경우, 기업체의 보안내재화 방법론 수준은 0이고, 경쟁사의 보안내재화 방법론 수준은 4일 수 있다. 다만, 이에 한정되는 것은 아니다.

[179] 한편, 본 개시에서 기업체와 경쟁사 간의 보안내재화 수준에 대한 차이가 분석된 경우, 서버(100)의 정보 생성부(160)는 기업체가 원하는 보안내재화 방법론 수준 달성하기 위한 제 2 정보를 제공할 수 있다.

[180] 일례로, 서버(100)의 정보 생성부(160)는 기업체의 현재 보안내재화 방법론 수준은 Microsoft 사의 보안내재화 방법론 수준에 도달하기 어렵다고 인식할 수 있다. 이 경우, 정보 생성부(160)는 기업체의 보안내재화 방법론 수준에 기초하여, 기 설정된 레벨에 도달할 수 있도록 하는 적어도 하나의 필수 보안 단계 각각에 매핑된 적어도 하나의 필수 산출물을 생성할 수도 있다.

[181] 다른 일례로, 정보 생성부(160)는 적어도 하나의 보안 활동 각각에 대한 보안내재화 방법론 수준의 편차가 줄어들 수 있도록 하는 적어도 하나의 세부 보안 활동 및 산출물 등을 생성할 수도 있다. 다만, 이에 한정되는 것은 아니다.

[182]

[183] 상술한 바를 통해 살펴본 바와 같이, 현재 대표적으로 활용되고 있는 보안내재화 방법론의 Secure SDLC 표준이나 가이드라인들은 너무 일반적이며 구체적인 내용들이 포함되어 있지 않기 때문에 실제 현장에서 활용하기가 매우 어려울 수 있다. 특히, 각 단계들 간 추적성을 확보하기 위해 반드시 필요한 산출 문서의 경우 예시 템플릿이 공개되지 않거나 템플릿의 내용이 구체적이지 않을 수 있다. 반면, 본 발명에 따르면 보안내재화 방법론을 기업체가 원하는 수준에 맞게 구체화시키기 위하여 보안내재화 방법론 수준 기반 보안내재화 프레임워크를 제공할 수 있다.

[184] 또한, 본 발명에 따른 보안내재화 방법론 기반 보안내재화 프레임워크를 사용할 경우, 자사와 경쟁사 간 갭 분석을 통해 보안내재화 수준 차이를 정량적으로 분석할 수 있다. 또한, 보안내재화를 필요로 하는 조직이 원하는 수준의 보안내재화를 구축하는데 필요한 상세한 세부 보안 활동 및 산출해야 하는 문서에 대한 예시 템플릿 등을 제공하여 실제 현장에서의 보안내재화를 구축할 때 활용이 용이하도록 할 수 있다.

[185]

[186] 도 8은 본 개시내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한

일반적인 개략도를 도시한다.

- [187] 본 개시내용이 일반적으로 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어와 관련하여 전술되었지만, 당업자라면 본 개시내용 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로서 구현될 수 있다는 것을 잘 알 것이다.
- [188] 일반적으로, 본 명세서에서의 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로시저, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된 장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.
- [189] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘다에 위치할 수 있다.
- [190] 컴퓨터는 통상적으로 다양한 컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체로서, 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다.
- [191] 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는 데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.
- [192] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터등을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선

매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것의 조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.

- [193] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.
- [194] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇 가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.
- [195] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA)—이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 새시(도시 생략) 내에서 외장형 용도로 구성될 수 있음—, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 예를 들어, USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘 다를 포함한다.
- [196] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 저장 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 zip 드라이브(zip drive), 자기 카세트, 플래쉬 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 저장 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가

본 개시의 방법들을 수행하기 위한 컴퓨터 실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.

- [197] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부분이 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.
- [198] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.
- [199] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.
- [200] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 서버 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원거리 통신망(WAN)(1154)에의 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크, 예를 들어, 인터넷에 연결될 수 있다.
- [201] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 서버에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을

설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(1142)를 통해 시스템 버스(1108)에 연결된다. 네트워크화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[202] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순히 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[203] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서도 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a,b,g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5 GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

[204] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 "소프트웨어"로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식으로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

[205] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조 물품(article)으로 구현될 수 있다. 용어 "제조

물품"은 임의의 컴퓨터-판독가능 장치로부터 액세스 가능한 컴퓨터 프로그램 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장 매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트립, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 용어 "기계-판독가능 매체"는 명령(들) 및/또는 데이터를 저장, 보유, 및/또는 전달할 수 있는 무선 채널 및 다양한 다른 매체를 포함하지만, 이들로 제한되는 것은 아니다.

[206]

[207] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

청구범위

- [청구항 1] 컴퓨팅 장치의 프로세서를 이용한 보안내재화 방법론을 구체화하는 방법으로서, 상기 방법은:
 보안내재화 방법론과 증거 기반 보안 방법론을 매핑하는 단계; 및
 매핑 결과를 데이터베이스에 저장하는 단계;
 를 포함하는,
 보안내재화 방법.
- [청구항 2] 제 1 항에 있어서,
 상기 매핑 결과는,
 적어도 하나의 보안 단계, 적어도 하나의 보안 활동, 적어도 하나의 세부 보안 활동 및 산출물을 포함하는,
 보안내재화 방법.
- [청구항 3] 제 2 항에 있어서,
 상기 적어도 하나의 보안 단계는,
 보안 교육과 관련된 제 1 단계, 착수 및 계획과 관련된 제 2 단계, 요구사항 분석과 관련된 제 3 단계, 획득과 관련된 제 4 단계, 설계와 관련된 제 5 단계, 구현과 관련된 제 6 단계, 검증과 관련된 제 7 단계, 배포와 관련된 제 8 단계, 운영과 관련된 제 9 단계 및 폐기와 관련된 제 10 단계 중 적어도 하나를 포함하는,
 보안내재화 방법.
- [청구항 4] 제 2 항에 있어서,
 기업체의 특성 및 상기 기업체의 보안내재화 방법론 현황을 인식하는 단계;
 상기 보안내재화 방법론 현황에 기초하여, 상기 기업체의 보안내재화 방법론 수준을 인식하는 단계;
 상기 특성 및 보안내재화 방법론 현황에 기초하여 상기 기업체와 관련된 경쟁사를 인식하는 단계;
 상기 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 단계; 및
 상기 경쟁사의 평균 보안내재화 방법론 수준 및 상기 기업체의 상기 보안내재화 방법론 수준에 기초하여, 상기 경쟁사와 상기 기업체의 보안내재화 방법론 수준 차이를 정량적으로 분석하여 제 1 정보를 제공하는 단계;
 를 더 포함하는,
 보안내재화 방법.
- [청구항 5] 제 4 항에 있어서,
 상기 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 단계는,
 상기 경쟁사가 수행한 정보 보호 제품의 보안성 표준에 대한 현황 정보를

획득하는 단계; 및

상기 현황 정보에 기초하여 상기 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 단계;

를 포함하는,

보안내재화 방법.

[청구항 6]

제 4 항에 있어서,

상기 매핑 결과는,

상기 적어도 하나의 보안 활동 각각에 포함되는 복수의 세부 보안 활동 각각에 부여되는 보안내재화 방법론 수준이 기록된 보안내재화 방법론 수준 정보를 포함하고,

상기 매핑 결과 및 상기 보안내재화 방법론 현황에 기초하여, 상기 기업체의 보안내재화 방법론 수준을 인식하는 단계는,

상기 보안내재화 방법론 수준 정보와 상기 보안내재화 방법론 현황에 기초하여, 상기 적어도 하나의 보안 활동 각각에 대한 상기 기업체의 상기 보안내재화 방법론 수준을 인식하는 단계;

를 포함하는,

보안내재화 방법.

[청구항 7]

제 4 항에 있어서,

상기 제 1 정보를 제공한 이후, 상기 기업체가 원하는 수준의 적정 보안내재화 방법론 수준을 수신하는 단계; 및

상기 매핑 결과에 포함된 적어도 하나의 보안 활동 중 상기 적정 보안내재화 방법론 수준과 관련된 적어도 하나의 필수 보안 활동에 대한 제 2 정보를 제공하는 단계;

를 포함하는,

보안내재화 방법.

[청구항 8]

제 7 항에 있어서,

상기 제 2 정보는,

상기 적어도 하나의 필수 보안 활동이 포함된 적어도 하나의 필수 보안 단계 각각에 매핑된 적어도 하나의 필수 산출물을 포함하는,

보안내재화 방법.

[청구항 9]

제 4 항에 있어서,

상기 제 1 정보는,

그래프 형식으로 상기 보안내재화 방법론 수준 차이를 정량적으로 나타내는,

보안내재화 방법.

[청구항 10]

제 9 항에 있어서,

상기 그래프는,

상기 적어도 하나의 세부 보안 활동 각각을 나타내는 x축, 상기 적어도

하나의 세부 보안 활동 각각에 대한 보안내재화 방법론 수준을 나타내는 y축, 상기 경쟁사의 평균 보안내재화 방법론 수준을 나타내는 제 1 선 및 상기 기업체의 보안내재화 방법론 수준을 나타내는 제 2 선을 포함하는, 보안내재화 방법.

[청구항 11] 제 10 항에 있어서,

상기 그래프는,

상기 제 1 선 및 상기 제 2 선 사이의 간극에 의해 형성되는 차이(gap)에 기초하여, 상기 경쟁사 및 상기 기업체의 상기 보안내재화 방법론 수준 차이를 정량적으로 나타내는,

보안내재화 방법.

[청구항 12] 보안내재화 방법론과 증거 기반 보안 방법론을 매핑하는 매핑부; 및

매핑 결과를 저장하는 데이터베이스부;

를 포함하는,

보안내재화 장치.

[청구항 13] 제 12 항에 있어서,

기업체의 특성 및 상기 기업체의 보안내재화 방법론 현황을 인식하고,

상기 보안내재화 방법론 현황에 기초하여, 상기 기업체의 보안내재화

방법론 수준을 인식하고, 상기 특성 및 보안내재화 방법론 현황에

기초하여 상기 기업체와 관련된 경쟁사를 인식하고, 상기 경쟁사의 평균 보안내재화 방법론 수준을 인식하는 수준 추출부;

상기 경쟁사의 평균 보안내재화 방법론 수준 및 상기 기업체의 상기

보안내재화 방법론 수준에 기초하여, 상기 경쟁사와 상기 기업체의

보안내재화 방법론 수준 차이를 정량적으로 분석하여 제 1 정보를

제공하는 수준 차이 분석부; 및

상기 매핑 결과에 포함된 적어도 하나의 보안 활동 중 상기 기업체가

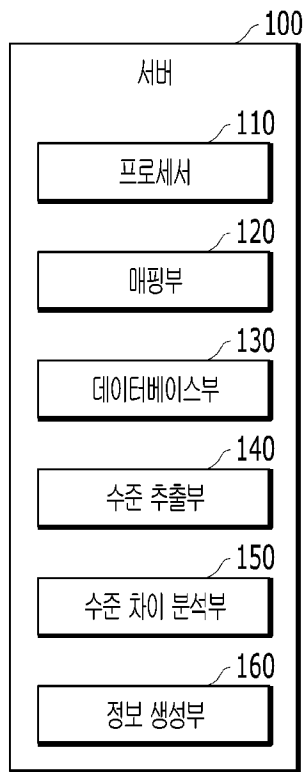
원하는 수준의 적정 보안내재화 방법론 수준과 관련된 적어도 하나의

필수 보안 활동에 대한 제 2 정보를 제공하는 정보 생성부;

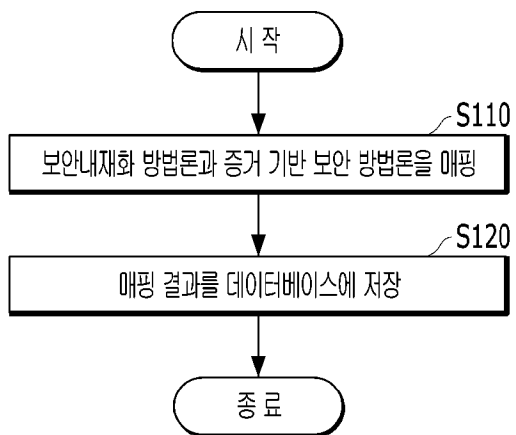
를 더 포함하는,

보안내재화 장치.

[도 1]



[도 2]



[도 3]

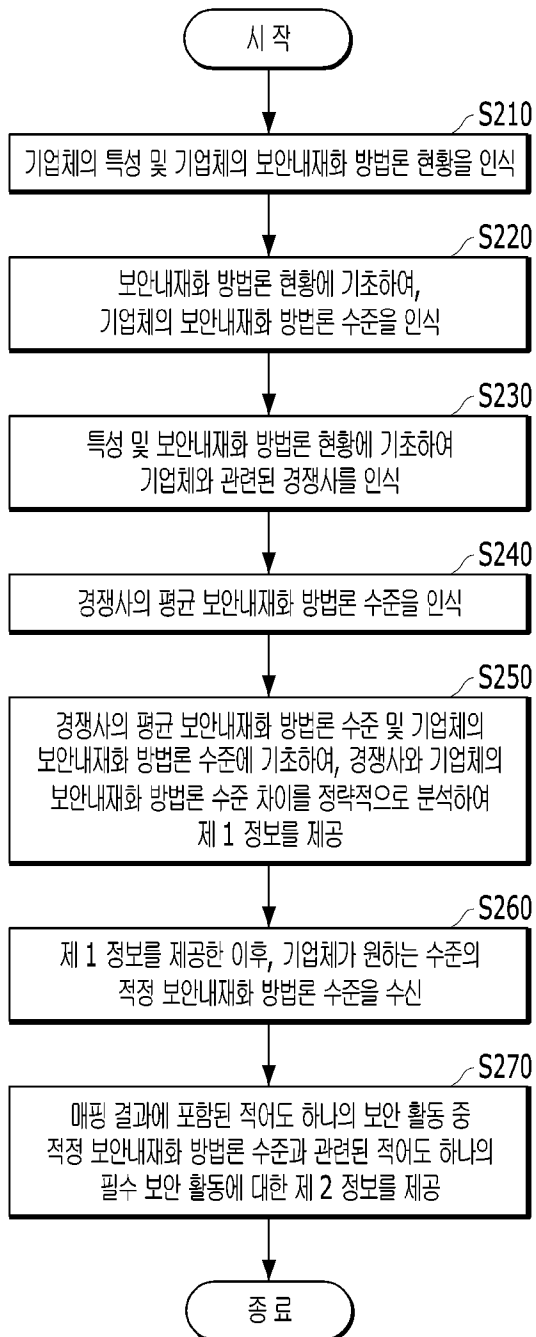
6. 구현 (Implementation)	37	코딩 가이드라인 준수	- 시스템 - 단위 테스트 계획서 및 테스트 시나리오 - 단위 테스트 결과서
	38	배포 가이드 문서 및 도구 생성	
	39	설계에 따른 구현 검증	
	40	수동 정적 분석	
7. 검증 (Verification)	41	자동 정적 분석	- 통합/시스템/인수 테스트 계획서 및 테스트 시나리오 - 통합/시스템/인수 테스트 결과서 - 취약성 분석서
	42	동작 분석	
	43	통합 및 인수 테스트	
	44	정수 테스트	
8. 배포 (Release)	45	위험 모델 검토 및 업데이트	
	46	최소 품질 및 보안 수준 검토	
	47	보안 문서 검토 및 업데이트	
	48	최종 보안 검토	- 리허설 계획서 및 리허설 결과서 - 배포 요청서
9. 운영 (Operation)	49	최종 개인정보보호 검토	
	50	생산을 위한 요구사항 도출	
	51	생산 절차 결정	
	52	생산에 대한 검증	- 비상 사고 대응 계획서 - 비상 사고 대응 결과서
10. 폐기 (Disposal)	53	비상 사고 대응 계획	
	54	배포 과정에 대한 보안 검토	
	55	모니터링 대상 지표 및 데이터 수집, 보고 전략 수립	
	56	지속적인 모니터링	- 설치 결과서 - 운영자 지침서 - 사용자 지침서 - 취약점 대응 계획서 - 취약점 패치 결과서
10. 폐기 (Disposal)	57	취약점 보고	
	58	취약점에 대한 평가	
	59	해결 방안 수립	
	60	취약점 공개 및 업데이트 관리	
10. 폐기 (Disposal)	61	배표 이후 생산라인	
	62	폐기 및 전이 계획 수립	
	63	중요정보 보존	
	64	매체 완전 소거	
10. 폐기 (Disposal)	65	하드웨어 및 소프트웨어 폐기	
	66	시스템 종료	- 시스템 이행계획서 및 시스템 이행결과서

단계	No	보안 활동	신출물
1. 보안 교육 (Security Training)	1	기본 보안 교육	- 보안 교육 계획서 - 교육 참석자 명단
	2	심화 보안 교육	
	3	보안 교육 관련 일정 계획	
	4	프로젝트 검토회	
2. 착수 및 계획 (Initiation)	5	역할 식별	
	6	프로젝트에 사용될 도구 선정	- 위험 프로세스 분석서 - 위험 시스템 분석서 - 프로젝트 계획서 - 요구사항 정의서
	7	보안 요구사항 출처 식별	
	8	최소 품질 및 보안 수준 정의	
3. 요구사항 분석 (Requirements Analysis)	9	보안 이슈 처리에 대한 보안 체계 마련	
	10	보안 일정 계획 및 관리	
	11	보안 목표 설정	
	12	보안 목표의 일관성 및 완전성 검증	
4. 획득 (Acquisition)	13	프로젝트 보안 분석 범위 선정	
	14	개인정보보호 영향평가	
	15	사업상 영향평가	- 영향평가서 - 인더테이션 정의서
	16	안전성 영향평가	
5. 설계 (Design)	17	기준 소프트웨어 설계	
	18	기능 요구사항 도출	
	19	보안 요구사항 도출	
	20	분리별 요구사항에 대한 객관성 및 충돌 여부 판단	
5. 설계 (Design)	21	보안 목표에 따른 요구사항 검증	
	22	획득 범위 및 계획 수립	
	23	Third-party 구성요소에 대한 보안 요구사항 정의	
	24	Third-party 구성요소에 대한 보안 요구사항 평가 및 테스트	
5. 설계 (Design)	25	보안 기능 설계 및 명세	
	26	설계 모범사례 및 원칙 준수	
	27	통합 과정에 대한 구조 설계	
	28	자산 식별	
5. 설계 (Design)	29	데이터 흐름도 작성	- 설계 명세서 - SW 아키텍처 설계서 - 시스템 아키텍처 설계서 - 통합 테스트 계획서 및 통합 테스트 시나리오
	30	위험 도출	
	31	공격 라이브리러리 수집	
	32	위험 분석	
5. 설계 (Design)	33	완화방안 도출	
	34	개인정보보호 분석	
	35	사용 및 오용 사례 식별	
	36	요구사항에 따른 설계 검증	

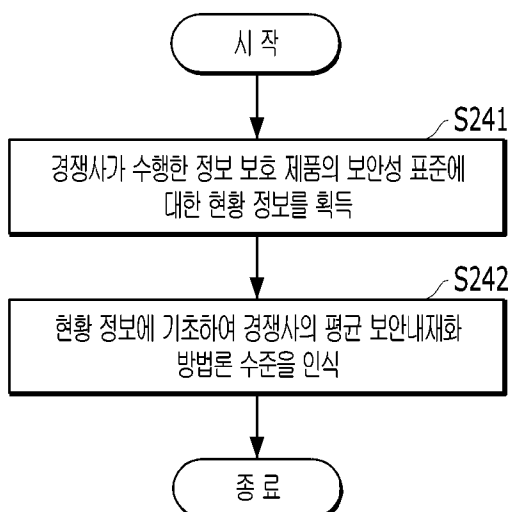
[도4]

표준	분류	개수
ISO/IEC 15408 - CC	1. 보안목표명세서	10
	2. 개발	19
	3. 설치 및 운영	2
	4. 생명주기 지원	18
	5. 테스트	9
	6. 취약점 평가	5
CC 합계	63개의 보증요구사항 컴포넌트	
ISO 27001 - ISMS	1. 정보보호 정책	6
	2. 정보보호 조직	4
	3. 외부자 보안	3
	4. 정보자산 분류	3
	5. 정보보호 교육	4
	6. 인적 보안	5
	7. 물리적 보안	9
	8. 시스템 개발 보안	10
	9. 암호 통제	2
	10. 접근 통제	14
	11. 운영 보안	22
	12. 침해사고 관리	7
	13. IT 재해복구	3
	14. 정보보호 관리	12
ISMS 합계	104 세부 점검 항목	
ISO/IEC 27701 - PIMS	1. 대상기관 개인정보보호 관리체계	8
	2. 대상 시스템의 개인정보보호 관리체계	6
	3. 개인정보처리 단계별 보호 조치	12
	4. 대상 시스템의 기술적 보호 조치	19
	5. 특정 IT 기술 활용 시 개인정보보호	9
PIMS 합계	54 세부 평가 항목	
총 합계	221 세부 보안 활동	

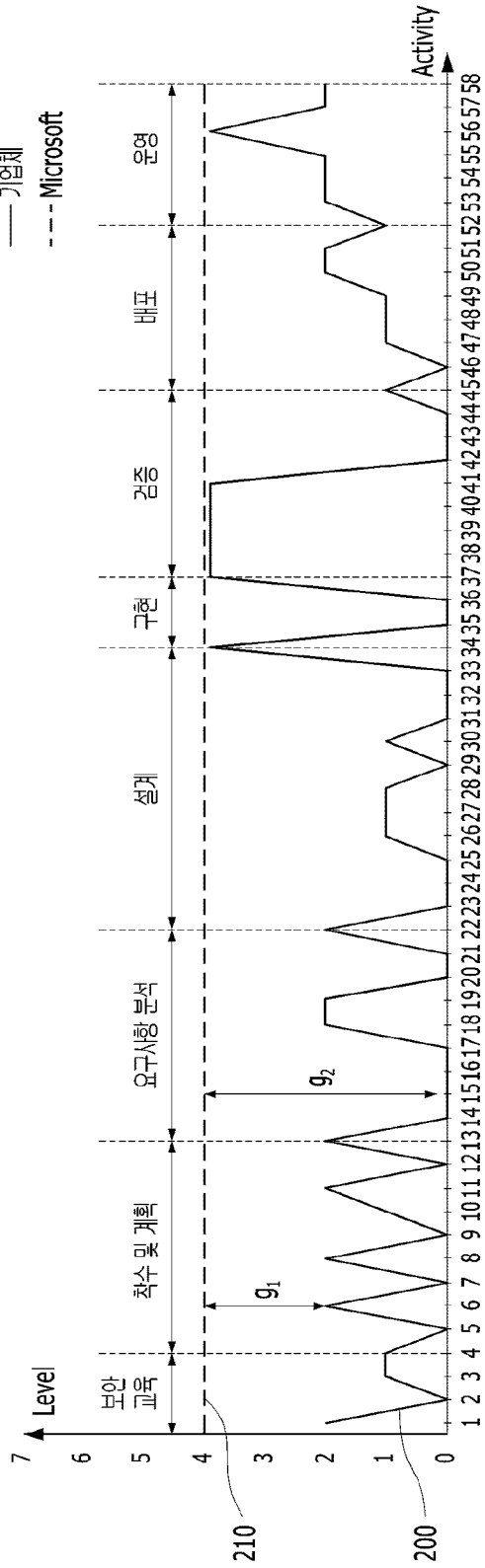
[도5]



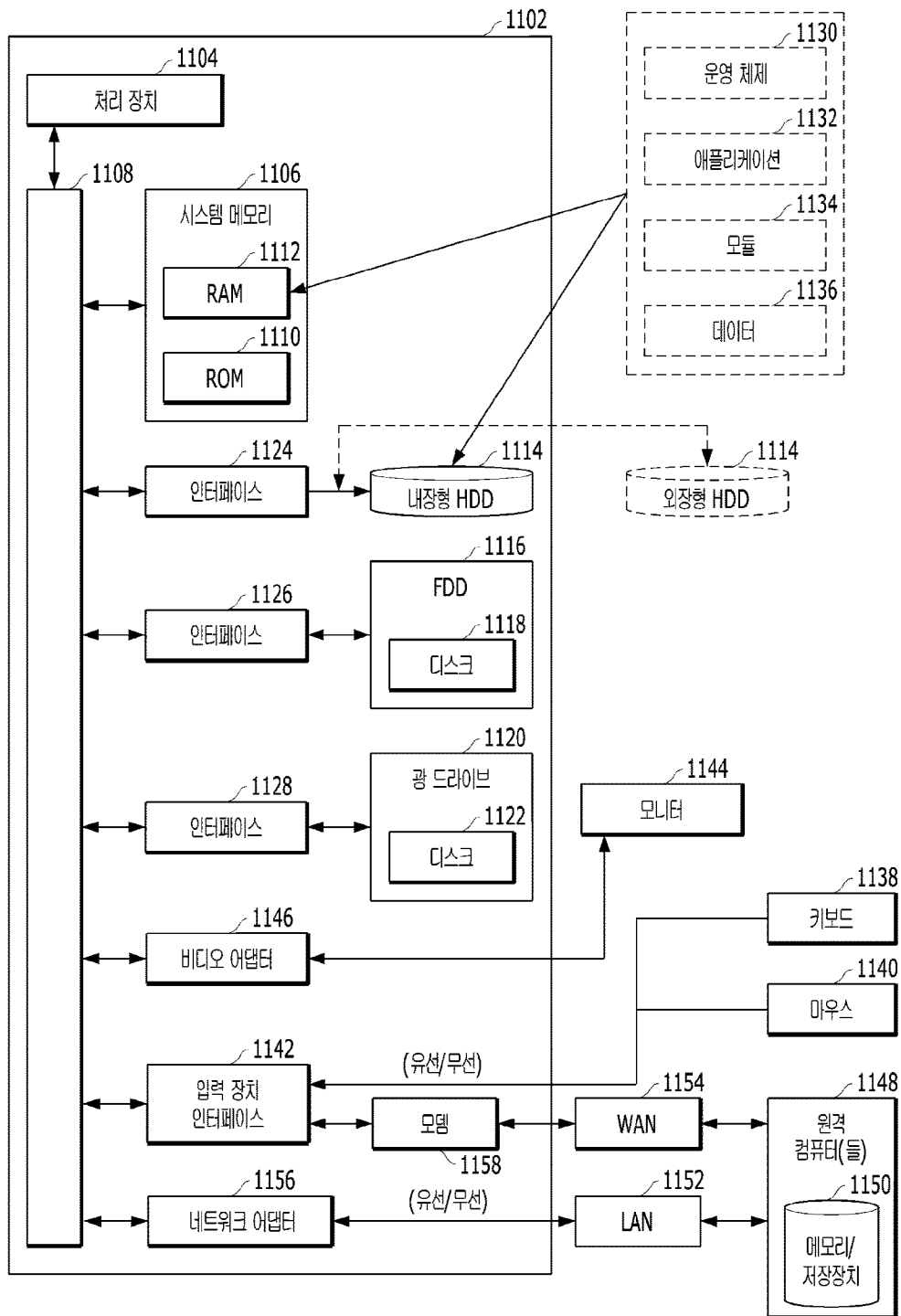
[도6]



[도7]



[도8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2020/013835

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57(2013.01)i; G06F 21/55(2013.01)i; G06F 21/86(2013.01)i; H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/57(2013.01); G06F 15/16(2006.01); G06F 21/55(2013.01); G06F 9/44(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above

Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 보안내재화(Security by Design), secure SDLC(Secure Software Development Life Cycle), 증거 기반 보안 방법론(ISO/IEC), 기업(enterprise), 수준(level)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	PARK, Jin Seok. Combining Secure Software Development Lifecycle with Common Criteria. Department of Information Security Graduate School of Information Security Korea University. pp. 1-28, December 2013. See pages 19-21.	1,12 2-11,13
Y	WO 2013-054961 A1 (RHEE, Seung Woo et al.) 18 April 2013 (2013-04-18) See paragraphs [0005], [0024] and [0027]; claims 1-2; and figure 1.	1,12
A	LEAL, Rhand. How to integrate ISO 27001 A.14 controls into the system/software development life cycle (SDLC). pp. 1-8, 24 February 2017. [Retrieved on 19 March 2021]. Retrieved from <https://advisera.com/27001academy/blog/2017/01/24/how-to-integrate-iso-27001-a-14-controls-into-the-system-software-development-life-cycle-sdlc>. See pages 1 and 4.	1-13
A	US 2019-0114435 A1 (2509757 ONTARIO INC.) 18 April 2019 (2019-04-18) See paragraphs [0047] and [0054]; and figure 1.	1-13

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“D” document cited by the applicant in the international application

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

02 April 2021

Date of mailing of the international search report

07 April 2021

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon Building 4, 189 Cheongsaro, Seo-gu, Daejeon 35208

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2020/013835

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009-0064087 A1 (ISOM, Pamela K.) 05 March 2009 (2009-03-05) See paragraph [0005]; and claim 1.	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2020/013835

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2013-054961	A1	18 April 2013	None			
US	2019-0114435	A1	18 April 2019	AU	2018-349089	A1	18 April 2019
				CA	3076262	A1	18 April 2019
				EP	3695338	A1	19 August 2020
				US	10706156	B2	07 July 2020
				US	2020-0285756	A1	10 September 2020
				US	2020-0285757	A1	10 September 2020
				WO	2019-071354	A1	18 April 2019
US	2009-0064087	A1	05 March 2009	US	8122426	B2	21 February 2012

A. 발명이 속하는 기술분류(국제특허분류(IPC)) G06F 21/57(2013.01)i; G06F 21/55(2013.01)i; G06F 21/86(2013.01)i; H04L 29/06(2006.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) G06F 21/57(2013.01); G06F 15/16(2006.01); G06F 21/55(2013.01); G06F 9/44(2006.01) 조사된 기술분야에 속하는 최소문헌 이외의 문헌 한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우)) eKOMPASS(특허청 내부 검색시스템) & 키워드: 보안내재화(Security by Design), secure SDLC(Secure Software Development Life Cycle), 증거 기반 보안 방법론(ISO/IEC), 기업(enterprise), 수준(level)		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y A	PARK JIN SEOK, 'Combining Secure Software Development Lifecycle with Common Criteria', Department of Information Security Graduate School of Information Security Korea University, pp. 1-28, 2013.12 페이지 19-21	1,12 2-11,13
Y	WO 2013-054961 A1 (RHEE, SEUNG WOO 등) 2013.04.18 단락 [0005], [0024], [0027]; 청구항 1-2; 및 도면 1	1,12
A	RHAND LEAL, 'How to integrate ISO 27001 A.14 controls into the system/software development life cycle (SDLC)', pp. 1-8, 2017.02.24 [검색일: 2021.03.19]. 출처 <https://advisera.com/27001academy/blog/2017/01/24/how-to-integrate-iso-27001-a-14-controls-into-the-system-software-development-life-cycle-sdlc> 페이지 1, 4	1-13
A	US 2019-0114435 A1 (2509757 ONTARIO INC.) 2019.04.18 단락 [0047], [0054]; 및 도면 1	1-13
☒ 추가 문헌이 C(계속)에 기재되어 있습니다. ☒ 대응특허에 관한 별지를 참조하십시오.		
* 인용된 문헌의 특별 카테고리: "A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌 "D" 본 국제출원에서 출원인이 인용한 문헌 "E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 "L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 "O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 "P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 "T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 "X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다. "Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. "&" 동일한 대응특허문헌에 속하는 문헌		
국제조사의 실제 완료일 2021년04월02일(02.04.2021)		국제조사보고서 발송일 2021년04월07일(07.04.2021)
ISA/KR의 명칭 및 우편주소 대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-481-8578		심사관 양정록 전화번호 +82-42-481-5709

C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2009-0064087 A1 (PAMELA K. ISOM) 2009.03.05 단락 [0005]; 및 청구항 1	1-13

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
WO 2013-054961 A1	2013/04/18	없음	
US 2019-0114435 A1	2019/04/18	AU 2018-349089 A1	2019/04/18
		CA 3076262 A1	2019/04/18
		EP 3695338 A1	2020/08/19
		US 10706156 B2	2020/07/07
		US 2020-0285756 A1	2020/09/10
		US 2020-0285757 A1	2020/09/10
		WO 2019-071354 A1	2019/04/18
US 2009-0064087 A1	2009/03/05	US 8122426 B2	2012/02/21