

발명의 설명

발명의 명칭: 보안 제어와 비용 통제 최적화 시스템 및 방법

기술분야

- [1] 발명은 선박 사이버보안 아키텍처를 구성함에 있어서 적절한 보안 제어에 대한 통제 비용의 적정성을 시뮬레이션하는 시스템에 관한 것으로, 선택되는 보안 제어에 포함되는 통제 정책에 따라서 통제 비용을 산출하며, 통제 비용에 따라 수용가능한 통제 위험을 파악하여 자동으로 최적의 보안 비용을 제시하여 새롭게 구축되는 기업, 조직, 선박의 보안 기준을 개선할 수 있도록 판단할 수 있는 보안과 비용의 시뮬레이션 방법과 시스템에 관한 것이다.

배경기술

- [2] 최근에는 사이버 보안 위협이 다양화, 지능화되면서 위협 대응을 위한 다양한 보안 기술과 제품이 출시되고 있다. 위협 대응에는 보안 제어를 통해 적절한 수준의 보안 비용 산출이 요구된다.
- [3] 일반적으로, 보안 비용 산출에 영향을 받는 조건은 요구사항, 컴플라이언스, 환경분석 결과, 완화대책에 따라 구성된다.
- [4] 예를들어 국제선급협회(IACS) UR E26의 Protect 요구사항을 이행하기 위해서 해당하는 선박의 선주 요구사항, 준수해야 하는 물과 환경분석 결과로 탑재되는 CBS의 제작사, 모델, 기반 네트워크의 속도/수용량(Bandwidth), 시스템의 Core 수량, 애플리케이션의 종류, 네트워크 구성 등으로 구성된다.
- [5] 이에 따라 완화대책은 방화벽, 침입탐지시스템, 로깅 등으로 구현된다.
- [6] 그러나 보안 제어를 위해서는 시스템, 네트워크, 애플리케이션, 모바일, 소스코드 등과 같은 기술적 대책과 보안 조직, 정책, 사용자 및 관리자와 같은 정책적 대책이 동시에 요구되지만 제어를 강하게 할수록 보안제어 비용이 증가한다.
- [7] 따라서, 보안 요구사항에 따라 구현하여야 하는 보안 제어와 보안 제어에 투자되는 비용은 적정수준에서 선택되어야 한다.
- [8] 그러나 현재는 적정수준의 보안 제어를 선택하기 위한 보안 제어에 필요한 상세 통제 비용을 산출하고 시뮬레이션할 방법이 없으며, 적절치 않은 보안 통제 수준 선택으로 과대 비용 지출 또는 과소 집행으로 통제 우회 문제점이 있었다.
- [9] 관련 선행문헌으로는 대한민국 공개특허 제10-2020-0029266호(2020.03.18.)가 공개되어 있다.

발명의 내용

기술적 과제

- [10] 본 발명의 목적은 선박 사이버보안 아키텍처를 구성함에 있어서, 선택되는 보안 제어에 포함되는 통제 정책에 따라서 통제 비용을 산출하여, 통제 비용에 따라 수용가능한 통제 위험을 파악하여 자동으로 최적의 보안 비용을 제시하여 새롭게 구축되는 기업, 조직, 선박의 보안 기준을 개선할 수 있도록 보안과 비용의

시뮬레이션을 통해 판단할 수 있는 보안 제어와 비용 통제 최적화 시스템과 방법을 제공하는 것을 목적으로 한다.

- [11] 본 발명의 다른 목적은 보안 제어를 위한 구성요소를 정형화할 수 있고, 정형화된 데이터 기반의 보안 통제 비용을 산출할 수 있으며, 다양한 완화대책 방안에 대한 시뮬레이션을 수행할 수 있는 보안 제어와 비용 통제 최적화 시스템과 방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

- [12] 상기한 목적을 달성하기 위한 본 발명의 일측면에 따른 보안 제어와 비용 통제 최적화 방법은, 사이버보안 데이터베이스와 연동되며 보안제어와 비용 통제 프로그램을 탑재한 서버가 인터넷을 통해 복수의 사용자 단말 장치와 접속되어 통신하되, 사용자 단말 장치를 이용하여 서버에 접속하는 서버 접속 단계; 서버에서 사이버보안 요구사항과 메뉴를 제공하고, 선택된 메뉴에 대한 사이버보안 조건을 입력할 수 있는 입력창을 제공하는 입력창 제공 단계; 상기 입력창 제공 단계를 통해 서버로부터 제공된 입력창에 선택 기본정보와 CBS 조건 정보를 사용자 단말 장치를 이용하여 입력하는 정보 입력 단계; 서버는 상기 정보 입력 단계를 통해 입력된 데이터를 기반으로 보안제어와 비용 통제 프로그램을 통해 사이버보안 데이터베이스와 연동하여 선택 사이버보안 요구사항 분석을 통한 통제 정책에 따른 통제 비용을 산출하고, 통제 비용에 따라 수용가능한 통제 위험을 추출하는 추출 단계; 및 상기 추출 단계를 통해 추출된 결과를 사용자 단말 장치에 제공하는 결과 제공 단계를 포함할 수 있다.
- [13] 또한, 본 발명의 일측면에 따른 보안 제어와 비용 통제 최적화 방법은, 상기 정보 입력 단계에서, CBS 조건 정보는 선택 CBS, 네트워크, 문서 및 온보드테스트 정보 중 적어도 하나를 포함할 수 있다.
- [14] 또한, 본 발명의 일측면에 따른 보안 제어와 비용 통제 최적화 방법에서, 상기 추출 단계는, 선택 사이버보안 요구사항을 분석하고 보안 제어 방법과 이에 종속되는 통제 기술과 통제 정책을 적용하기 위해 소요되는 비용을 산출하고, 입력값에 해당하는 데이터를 시뮬레이션하여 통제 비용에 따라 수용가능한 통제 위험을 추출하는 것을 특징으로 한다.
- [15] 또한, 본 발명의 일측면에 따른 보안 제어와 비용 통제 최적화 방법에서, 상기 제공 단계는, 사이버보안 데이터베이스와 연동하여, 보안 제어의 복수 항목에 대한 특징을 나타내는 축 그래프로 제공될 수 있으며; 각 보안 제어 항목의 기준 축 그래프가 채워진 상태를 확인하여, 보안 제어가 필요한 항목과 보안 제어 수준을 확인할 수 있는 것을 특징으로 한다.
- [16] 또한, 본 발명의 다른 측면에 따른 보안 제어와 비용 통제 최적화 시스템은, 사이버보안 데이터베이스와 연동되며 보안제어와 비용 통제 프로그램을 탑재한 서버에 통신 접속하여 보안 요구사항, 규제사항을 포함하는 사이버보안에 필요한 요구사항을 입력하는 사용자 단말 장치; 상기 사용자 단말 장치를 통해 접속

할 수 있으며, 사이버보안 요구사항과 메뉴를 제공하고, 선택된 메뉴에 대한 사이버보안 조건을 입력할 수 있는 입력창을 제공하는 서버; 및 상기 서버와 연동되며, 보안 요구사항, 규제사항 등 선택에 필요한 사이버보안 정보가 저장되는 사이버보안 데이터베이스를 포함하며; 상기 서버는, 상기 사용자 단말 장치를 통해 입력되는 선택 기본정보와 CBS 조건 정보를 포함하는 입력 데이터를 기반으로 사이버보안 데이터베이스와 연동하여 보안제어와 비용 통제 프로그램을 통해 보안 제어를 분석하여 통제 정책에 따른 통제 비용을 산출하고, 통제 비용에 따라 수용가능한 통제 위험을 추출하며; 상기 서버는, 추출된 결과를 사용자 단말 장치에 제공하는 것을 특징으로 한다.

- [17] 또한, 본 발명의 다른 측면에 따른 보안 제어와 비용 통제 최적화 시스템에서, 상기 사용자 단말 장치는, 서버의 입력창을 통해 선택 기본정보와 CBS 조건 정보를 포함하여 입력하며; 상기 CBS 조건 정보는 선택 CBS, 네트워크, 문서 및 온보드 테스트 정보 중 적어도 하나를 포함할 수 있다.
- [18] 또한, 본 발명의 다른 측면에 따른 보안 제어와 비용 통제 최적화 시스템에서, 상기 서버는, 선택 사이버보안 요구사항을 분석하고 보안 제어 방법과 이에 종속되는 통제 기술과 통제 정책을 적용하기 위해 소요되는 비용을 산출하고, 입력값에 해당하는 데이터를 시뮬레이션하여 통제 비용에 따라 수용가능한 통제 위험을 추출하는 것을 특징으로 한다.
- [19] 또한, 본 발명의 다른 측면에 따른 보안 제어와 비용 통제 최적화 시스템에서, 상기 서버는, 사이버보안 데이터베이스와 연동하여 추출된 데이터를 보안 제어의 복수 항목에 대한 특징을 나타내는 축 그래프로 사용자 단말 장치에 제공될 수 있으며; 각 보안 제어 항목의 기준 축 그래프가 채워진 상태를 확인하여, 보안 제어가 필요한 항목과 보안 제어 수준을 확인할 수 있는 것을 특징으로 한다.

발명의 효과

- [20] 본 발명에 따르면 선택 사이버보안 아키텍처를 구성함에 있어서, 선택되는 보안 제어에 포함되는 통제 정책에 따라서 통제 비용을 산출하여, 통제 비용에 따라 수용가능한 통제 위험을 파악하여 자동으로 최적의 보안 비용을 제시하여 새롭게 구축되는 기업, 조직, 선택의 보안 기준을 개선할 수 있도록 보안과 비용의 시뮬레이션을 통해 판단할 수 있는 효과를 갖는다.
- [21] 또한, 본 발명에 따르면 보안 제어를 위한 구성요소를 정형화할 수 있고, 정형화된 데이터 기반의 보안 통제 비용을 산출할 수 있으며, 다양한 완화대책 방안에 대한 시뮬레이션을 수행할 수 있는 효과를 갖는다.

도면의 간단한 설명

- [22] 도 1은 본 발명에 따른 보안 제어와 비용 통제 최적화 시스템의 구성을 나타내는 도면이다.
- [23] 도 2는 본 발명에 따른 보안 제어와 비용 통제 최적화 방법을 나타내는 순서도이다.

- [24] 도 3은 본 발명에 따른 보안 제어와 비용 통제 최적화 방법의 추출 단계에서 통제 비용 산출 과정을 나타내는 도면이다.
- [25] 도 4는 본 발명에 따른 보안 제어와 비용 통제 최적화 방법에서 정보 입력 단계와 추출 단계를 나타내는 도면이다.
- [26] 도 5는 본 발명에 따른 보안 제어와 비용 통제 최적화 시스템에서 선박 사이버 보안 데이터베이스의 구성을 나타내는 도면이다.
- [27] 도 6은 본 발명에 따른 보안 제어와 비용 통제 최적화 방법에서 입력창 제공 단계를 나타내는 도면이다.
- [28] 도 7은 본 발명에 따른 보안 제어와 비용 통제 최적화 방법에서 정보 입력 단계에서 입력되는 정보를 나타내는 도면이다.
- [29] 도 8은 본 발명에 따른 보안 제어와 비용 통제 최적화 방법에서 추출된 결과를 제공하는 결과 제공 단계를 나타내는 도면이다.

발명의 실시를 위한 형태

- [30] 본 발명의 목적과 기술적 구성 및 그에 따른 작용 및 효과에 관한 자세한 사항은 본 발명의 명세서에 첨부된 도면에 의거한 상세한 설명에 의해 보다 명확하게 이해될 것이다.
- [31] 본 명세서에서 사용되는 용어는 단지 특정한 실시예를 설명하기 위해 사용되는 것으로 본 발명을 한정하려는 의도가 아니다. 예컨대, 본 명세서에서 사용되는 '구성된다' 또는 '포함한다' 등의 용어는 발명에 기재된 여러 구성요소들 또는 여러 단계들을 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성요소들 또는 일부 단계들을 포함하지 않거나 또는 추가적인 구성요소들 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다. 또한, 본 명세서에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함한다.
- [32] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써 본 발명을 상세히 설명한다. 이하에서 설명되는 실시예들은 본 발명의 기술사상을 당업자가 용이하게 이해할 수 있도록 제공되는 것으로서, 이에 의해 본 발명이 한정되는 것으로 해석되어서는 안되며, 본 발명의 실시예들은 이 분야의 통상의 기술자에게 다양한 응용을 가질 수 있음은 당연하다.
- [33] 본 발명은 선박 사이버보안 아키텍처를 구성함에 있어서 적절한 보안 제어에 대한 통제 비용의 적정성을 시뮬레이션하는 시스템에 관한 것으로, 선택되는 보안 제어에 포함되는 통제 정책에 따라서 통제 비용을 산출하며, 통제 비용에 따라 수용가능한 통제 위험을 파악하여 자동으로 최적의 보안 비용을 제시하여 새롭게 구축되는 기업, 조직, 선박의 보안 기준을 개선할 수 있도록 판단 할 수 있는 보안과 비용의 시뮬레이션 방법과 시스템에 관한 것이다.
- [34] 도 1을 참조하면, 본 발명에 따른 보안 제어와 비용 통제 최적화 시스템은, 사이버보안 데이터베이스(150)와 연동되며 보안제어와 비용 통제 프로그램을 탑재

한 서버에 통신 접속하여 보안 요구사항, 규제사항을 포함하는 사이버보안에 필요한 요구사항을 입력하는 사용자 단말 장치(10)와, 사용자 단말 장치(10)를 통해 접속할 수 있으며, 사이버보안 요구사항(Requirements)과 메뉴를 제공하고, 선택된 메뉴에 대한 사이버보안 조건을 입력할 수 있는 입력창을 제공하는 서버(100); 및 서버(100)와 연동되며, 보안 요구사항, 규제사항 등 선택에 필요한 사이버보안 정보가 저장되는 사이버보안 데이터베이스(DB, 150)를 포함할 수 있다.

[35] 서버(100)는, 사용자 단말 장치(10)를 통해 입력되는 선택 기본정보와 선택(CBS: Computer Based System) 조건 정보를 포함하는 입력 데이터를 기반으로 사이버보안 데이터베이스(150)와 연동하여 보안제어와 비용 통제 프로그램을 통해 보안 제어를 분석하여 통제 정책에 따른 통제 비용을 산출하고, 통제 비용에 따라 수용가능한 통제 위험을 추출할 수 있다.

[36] 또한, 서버(100)는, 추출된 결과를 사용자 단말 장치에 제공할 수 있으며, 사이버보안 데이터베이스(150)와 연동하여 추출된 데이터를 보안 제어의 복수 항목에 대한 특징을 나타내는 축 그래프로 사용자 단말 장치(10)에 제공될 수 있으며, 각 보안 제어 항목의 기준 축 그래프가 채워진 상태를 확인하여, 보안 제어가 필요한 항목과 보안 제어 수준을 확인할 수 있는 것을 특징으로 한다.

[37] 이때 사용자 단말 장치(10)는 복수의 사용자 단말 장치(11, 12)가 인터넷을 통해 서버에 접속되어 통신할 수 있다.

[38] 또한, 사용자 단말 장치(10)는, 서버(100)의 입력창(110)을 통해 선택 기본정보와 CBS 조건 정보를 포함하여 입력하고, CBS 조건 정보는 선택 CBS, 네트워크(network), 문서(Documents) 및 온보드 테스트(Onboardtest) 정보 중 적어도 하나를 포함할 수 있다.

[39] 또한, 서버(100)는, 선택 사이버보안 요구사항을 분석하고 보안 제어 방법과 이에 종속되는 통제 기술과 통제 정책을 적용하기 위해 소요되는 비용을 산출하고, 입력값에 해당하는 데이터를 시뮬레이션하여 통제 비용에 따라 수용가능한 통제 위험을 추출할 수 있다.

[40] 즉, 보안 제어와 비용 통제 최적화 시스템은 보안 요구사항, 규제사항 등 선택에 필요한 사이버보안 데이터베이스(DB)와 연동되며 보안제어와 비용 통제 프로그램을 탑재한 서버(100)가 인터넷을 통해 복수의 단말 장치(11, 12)와 접속되어 통신하고 선택 사이버보안 요구사항 분석을 통한 보안 제어 방법과 이에 종속되는 통제 기술과 통제 정책, 이를 적용하기 위해 소요되는 비용을 제공할 수 있다.

[41] 도 2를 참조하여, 본 발명의 일측면에 따른 보안 제어와 비용 통제 최적화 방법을 살펴보면, 사이버보안 데이터베이스와 연동되며 보안제어와 비용 통제 프로그램을 탑재한 서버가 인터넷을 통해 복수의 사용자 단말 장치와 접속되어 통신하되, 사용자 단말 장치를 이용하여 서버에 접속하는 서버 접속 단계(S100)와, 서버에서 사이버보안 요구사항과 메뉴를 제공(S110)하고, 선택된 메뉴에 대한 사이버보안 조건을 입력할 수 있는 입력창을 제공하는 입력창 제공 단계(S120)와,

입력창 제공 단계(S120)를 통해 서버로부터 제공된 입력창에 선택 기본정보와 CBS 조건 정보를 사용자 단말 장치를 이용하여 입력하는 정보 입력 단계(S130)와, 서버(100)는 정보 입력 단계(S130)를 통해 입력된 데이터를 기반으로 보안 제어와 비용 통제 프로그램을 통해 사이버보안 데이터베이스(150)와 연동하여 선택 사이버보안 요구사항 분석을 통한 통제 정책에 따른 통제 비용을 산출하고, 통제 비용에 따라 수용가능한 통제 위험을 추출하는 추출 단계(S140) 및 추출 단계(S140)를 통해 추출된 결과를 사용자 단말 장치에 제공하는 제공 단계(S150)를 포함할 수 있다.

- [42] 즉, 사용자 단말 장치(10)를 이용하여 서버(100)에 접속하고, 서버(100)가 사용자 단말 장치(10)에 대해 사이버보안에 필요한 요구사항 메뉴를 제공하며, 사용자 단말 장치(10)에서 메뉴를 선택하면 서버(100)는 그에 따른 사이버보안 조건 입력창을 제공할 수 있다.
- [43] 이어서, 사용자 단말 장치(10)를 통해 입력창에 선택 기본정보와 선택을 구성하는 CBS 조건을 입력하면, 서버(100)가 보안제어와 비용 통제 프로그램의 동작에 의해 입력된 조건에 따라 선택 사이버보안 데이터베이스(150)로부터 데이터를 추출하여 입력값에 해당하는 정보를 사용자 단말 장치에 제공할 수 있다.
- [44] 또한, 도 3을 참조하여 추출 단계에서 통제 비용 산출 과정을 살펴보면, 사이버보안 요구사항을 분석하여 허용 가능한 위험인지 여부를 확인하고, 허용 가능한 위험인 경우 종료되고, 허용 가능한 위험이 아닌 경우 보안 제어가 수행될 수 있도록 하며, 이에 따른 보안 제어 수행 비용을 산출할 수 있다.
- [45] 도 4는 본 발명에 따른 보안 제어와 비용 통제 최적화 방법에서 정보 입력 단계와 추출 단계를 나타내는 도면으로, 정보 입력 단계(S120)에서는 사이버보안에 필요한 요구사항을 입력하고, 입력 정보를 확인할 수 있다.
- [46] 또한, 선택 CBS, 네트워크, 문서 정보 및 온보드 테스트(onboard test)를 포함하는 CBS 조건 정보와 선택 기본정보를 입력할 수 있고, 입력 정보를 확인할 수 있다.
- [47] 이어서 서버(100)에서는 입력 정보를 분석하여 사이버보안 데이터베이스와 연동하여 통제 정책에 따른 통제 비용을 산출하고, 통제 비용에 따라 수용가능한 통제 위험을 추출할 수 있으며, 추출된 결과를 사용자 단말에 제공할 수 있다.
- [48] 결과 제공 방식은 메시지 또는 이메일 발송을 통해 제공될 수 있으며, 제공 시 보안 제어의 복수 항목에 대한 특징을 나타내는 축 그래프로 제공될 수 있고, 각 보안 제어 항목의 기준 축 그래프가 채워진 상태를 확인하여, 보안 제어가 필요한 항목과 보안 제어 수준을 용이하게 한번에 확인할 수 있는 것을 특징으로 한다.
- [49] 도 5는 본 발명에 따른 보안 제어와 비용 통제 최적화 시스템에서 선택 사이버보안 데이터베이스의 구성을 나타내는 도면으로, 선급 및 참고기관에 대한 종류 테이블과 Notation 테이블 및 사이버보안 요구사항 테이블이 저장되어 연동될 수 있다.

- [50] 또한, 선박 CBS 인벤토리, 응용 시스템 목록, 정보 저장 테이블이 저장되고 연동될 수 있다.
- [51] 따라서, 해당 데이터를 포함하여 사이버보안 요구사항을 분석할 수 있도록 서버와 연동될 수 있다.
- [52] 도 6은 본 발명에 따른 보안 제어와 비용 통제 최적화 방법에서 입력창 제공 단계를 나타내는 도면으로 도 6(a)에 고객사 정보 입력, 도 6(b)에 선박 사이버보안 건적요청내용을 입력, 도 6(c) 내지 도 6(e)에 적용 시스템 및 문서를 입력할 수 있는 입력창이 제공될 수 있다.
- [53] 도 7은 본 발명에 따른 보안 제어와 비용 통제 최적화 방법에서 정보 입력 단계에서 입력되는 정보를 나타내는 도면으로, 선박 기본정보와 요청사 정보가 제공되며, 선박사이버보안 요청사항과 문서, 네트워크 및 온보드 테스트 자료가 세부적으로 입력될 수 있도록 한다.
- [54] 즉, 정보 입력 단계(S130)에서, CBS 조건 정보는 선박 CBS, 네트워크, 문서 및 온보드테스트 정보 중 적어도 하나를 포함할 수 있다.
- [55] 또한, 추출 단계(S140)는, 선박 사이버보안 요구사항을 분석하고 보안 제어 방법과 이에 종속되는 통제 기술과 통제 정책을 적용하기 위해 소요되는 비용을 산출하고, 입력값에 해당하는 데이터를 시뮬레이션하여 통제 비용에 따라 수용가능한 통제 위험을 추출하는 것을 특징으로 한다.
- [56] 또한, 도 8은 본 발명에 따른 보안 제어와 비용 통제 최적화 방법에서 추출된 결과를 제공하는 결과 제공 단계를 나타내는 도면이다.
- [57] 즉 보안 제어의 복수 항목에 대한 특징을 나타내는 축 그래프로 제공될 수 있고, 도 8에서는 식별(IDENTIFY), 보호(PROTECT), 감지(DETECT), 회복(RECOVERY), 응답(RESPOND)으로 5개의 특징에 각 보안 제어 항목의 기준 축 그래프가 채워진 상태를 확인(축 그래프가 중심에서 외측으로 채워지는 형태)하여, 보안 제어가 필요한 항목과 보안 제어 수준을 용이하게 한번에 확인할 수 있는 것을 특징으로 한다.
- [58] 또한, 제공 단계(S150)에서는 필요한 사이버보안에 대한 추천 항목을 여러가지 경우의 수의 따라 제공될 수 있다.
- [59] 전술된 식별(IDENTIFY), 보호(PROTECT), 감지(DETECT), 회복(RECOVERY) 및 응답(RESPOND)에서 보안 제어 수준을 변경하여 어느 특징 하나를 중점적으로 보안 제어하는지에 따라 각 항목별 추천 상품을 제안하여 제공될 수 있다.
- [60] 따라서, 본 발명에 따르면 선박 사이버보안 아키텍처를 구성함에 있어서, 선택되는 보안제어에 포함되는 통제 정책에 따라서 통제 비용을 산출하여, 통제 비용에 따라 수용가능한 통제 위험을 파악하여 자동으로 최적의 보안 비용을 제시하여 새롭게 구축되는 기업, 조직, 선박의 보안 기준을 개선할 수 있도록 보안과 비용의 시뮬레이션을 통해 판단할 수 있는 효과를 갖는다.

- [61] 또한, 본 발명에 따르면 보안 제어를 위한 구성요소를 정형화할 수 있고, 정형화된 데이터 기반의 보안 통제 비용을 산출할 수 있으며, 다양한 완화대책 방안에 대한 시뮬레이션을 수행할 수 있는 효과를 갖는다.
- [62] 이상 설명된 본 발명에 따른 실시예는 다양한 컴퓨터 구성요소를 통하여 실행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 판독 가능한 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium) 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위하여 하나 이상의 소프트웨어 모듈로 변경될 수 있으며 그 역도 마찬가지이다.
- [63] 이상에서 설명되는 실시예들은 본 발명의 기술사상을 당업자가 용이하게 이해할 수 있도록 제공되는 것으로서, 이에 의하여 본 발명이 한정되는 것으로 해석되어서는 안되며, 본 발명의 실시예들은 본 발명의 사상 및 범위를 벗어나지 않는 범위 내에서 다양하게 수정 및 변형될 수 있음은 이 기술의 분야에서 통상의 지식을 가진 자에게 자명하다. 따라서 그러한 수정예 또는 변형예들은 본 발명의 특허청구범위에 속한다 하여야 할 것이다.

서열목록

- [64] 10: 사용자 단말 장치
- [65] 50: 인터넷
- [66] 100: 서버
- [67] 110: 요구 입력 프로그램
- [68] 120: 보안 제어 분석 프로그램
- [69] 150: 사이버보안 데이터베이스

청구범위

- [청구항 1] 사이버보안 데이터베이스와 연동되며 보안제어와 비용 통제 프로그램을 탑재한 서버가 인터넷을 통해 복수의 사용자 단말 장치와 접속되어 통신 하되,
 사용자 단말 장치를 이용하여 서버에 접속하는 서버 접속 단계;
 서버에서 사이버보안 요구사항과 메뉴를 제공하고, 선택된 메뉴에 대한 사이버보안 조건을 입력할 수 있는 입력창을 제공하는 입력창 제공 단계;
 상기 입력창 제공 단계를 통해 서버로부터 제공된 입력창에 선택 기본정보와 CBS 조건 정보를 사용자 단말 장치를 이용하여 입력하는 정보 입력 단계;
 서버는 상기 정보 입력 단계를 통해 입력된 데이터를 기반으로 보안제어와 비용 통제 프로그램을 통해 사이버보안 데이터베이스와 연동하여 선택된 사이버보안 요구사항 분석을 통한 통제 정책에 따른 통제 비용을 산출하고, 통제 비용에 따라 수용가능한 통제 위험을 추출하는 추출 단계; 및
 상기 추출 단계를 통해 추출된 결과를 사용자 단말 장치에 제공하는 결과 제공 단계를 포함하는, 보안 제어와 비용 통제 최적화 방법.
- [청구항 2] 청구항 1에 있어서,
 상기 정보 입력 단계에서, CBS 조건 정보는 선택 CBS, 네트워크, 문서 및 온보드테스트 정보 중 적어도 하나를 포함하는, 보안 제어와 비용 통제 최적화 방법.
- [청구항 3] 청구항 1에 있어서,
 상기 추출 단계는,
 선택된 사이버보안 요구사항을 분석하고 보안 제어 방법과 이에 종속되는 통제 기술과 통제 정책을 적용하기 위해 소요되는 비용을 산출하고, 입력값에 해당하는 데이터를 시뮬레이션하여 통제 비용에 따라 수용가능한 통제 위험을 추출하는 것을 특징으로 하는, 보안 제어와 비용 통제 최적화 방법.
- [청구항 4] 청구항 1에 있어서,
 상기 제공 단계는,
 사이버보안 데이터베이스와 연동하여, 보안 제어의 복수 항목에 대한 특징을 나타내는 축 그래프로 제공될 수 있으며;
 각 보안 제어 항목의 기준 축 그래프가 채워진 상태를 확인하여, 보안 제어가 필요한 항목과 보안 제어 수준을 확인할 수 있는 것을 특징으로 하는, 보안 제어와 비용 통제 최적화 방법.
- [청구항 5] 사이버보안 데이터베이스와 연동되며 보안제어와 비용 통제 프로그램을 탑재한 서버에 통신 접속하여 보안 요구사항, 규제사항을 포함하는 사이버보안에 필요한 요구사항을 입력하는 사용자 단말 장치;

상기 사용자 단말 장치를 통해 접속할 수 있으며, 사이버보안 요구사항과 메뉴를 제공하고, 선택된 메뉴에 대한 사이버보안 조건을 입력할 수 있는 입력창을 제공하는 서버; 및

상기 서버와 연동되며, 보안 요구사항, 규제사항 등 선택에 필요한 사이버보안 정보가 저장되는 사이버보안 데이터베이스를 포함하며;

상기 서버는, 상기 사용자 단말 장치를 통해 입력되는 선택 기본정보와 CBS 조건 정보를 포함하는 입력 데이터를 기반으로 사이버보안 데이터베이스와 연동하여 보안제어와 비용 통제 프로그램을 통해 보안 제어를 분석하여 통제 정책에 따른 통제 비용을 산출하고, 통제 비용에 따라 수용가능한 통제 위험을 추출하며;

상기 서버는, 추출된 결과를 사용자 단말 장치에 제공하는 것을 특징으로 하는, 보안 제어와 비용 통제 최적화 시스템.

[청구항 6]

청구항 5에 있어서,

상기 사용자 단말 장치는, 서버의 입력창을 통해 선택 기본정보와 CBS 조건 정보를 포함하여 입력하며;

상기 CBS 조건 정보는 선택 CBS, 네트워크, 문서 및 온보드테스트 정보 중 적어도 하나를 포함하는, 보안 제어와 비용 통제 최적화 시스템.

[청구항 7]

청구항 5에 있어서,

상기 서버는,

선택 사이버보안 요구사항을 분석하고 보안 제어 방법과 이에 종속되는 통제 기술과 통제 정책을 적용하기 위해 소요되는 비용을 산출하고, 입력값에 해당하는 데이터를 시뮬레이션하여 통제 비용에 따라 수용가능한 통제 위험을 추출하는 것을 특징으로 하는, 보안 제어와 비용 통제 최적화 시스템.

[청구항 8]

청구항 5에 있어서,

상기 서버는,

사이버보안 데이터베이스와 연동하여 추출된 데이터를 보안 제어의 복수 항목에 대한 특징을 나타내는 축 그래프로 사용자 단말 장치에 제공될 수 있으며;

각 보안 제어 항목의 기준 축 그래프가 채워진 상태를 확인하여, 보안 제어가 필요한 항목과 보안 제어 수준을 확인할 수 있는 것을 특징으로 하는, 보안 제어와 비용 통제 최적화 시스템.