情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

제어시스템 보안성 평가 방법에 관한 연구

최 명 길[†‡]
중앙대학교

A Study on Security Evaluation Methodology for Industrial Control Systems

Myeonggil Choi[†‡]
Chung-Ang University

요 약

주요 국가기반 산업분야에서 운용중인 제어시스템은 다양한 제어 기능을 수행하고 있으며, 최근 제어시스템에 가해지는 다양한 위협이 가해지고 있는 실정이다. 제어시스템의 안전한 운용을 보증하기 위하여 제어시스템의 안전성을 검증할 수 있는 보증방법의 개발이 절실히 필요하다. 본 연구는 제어시스템의 특성을 반영한 정보보안평가 절차 및 방법론을 제시하고, 체크리스트로 구현을 통해서 절차 및 방법론의 효과성을 검증한다. 동 연구가 제시하는 제어시스템의 정보보안 평가 절차 및 점검체크리스트는 제어시스템 운용자 및 보증 평가자가 제어시스템의 개발 과정 및 운용의 안전성을 담보할 수 있는 보증 활동시에 사용할 수 있다.

ABSTRACT

Industrial Control systems which are operated in the industrial infrastructure adopts the various functions and face various threats in these days. To assure the security of the industrial control systems, the security evaluation methodology should be necessarily developed. This study suggests the processes and methodology for evaluating control systems, verifies the effectiveness of processes and methodologies through development of security checklists. The results of the study will be utilized for operators, evaluators and obtainers of industrial controls and be basis for developing and assuring the industrial controls systems.

Keywords: Security Assurance, Security Evaluation, Evaluation Methodology, Security Checklists, Industrial Control Systems

I. 서 론

주요기반시설을 관리하는 제어시스템(industrial control systems)이 폐쇄 네트워크(closed network)에서 인터넷 기반 네트워크(Internet-based network)로 변화되면서 다양한 보안 위협 및 취약성이 증가되고 있다. 국가주요기반시설을 제어하는 제어시스템이 사이버 공격이나 침해를 당하는 경우 안보, 경제 및 국민생활에 막대한 피해를 일으킬 수 있어 국가주요기반시설의 보안의 중요성이 강화되고 있다.

제어시스템의 안전한 개발 및 운용을 위해서 제어시스템 보안을 위한 다양한 보안대책이 제안되고 있다. 제어시스템의 보안 대책의 효과적인 운영을 위하여 제어시스템의 보안성에 대한 보증(security assurance)이 필요하고, 제어시스템의 보안성을 보증할 수 있는 보안평가 절차 및 방법이 필요하다. 제어시스템의 보안성 평가 절차 및 방법은 제어시스템의 보증은 제어시스템 획득, 운용절차, 운용 정책 및 조

접수일(2013년 2월 18일), 수정일(2013년 4월 9일), 게재확정일(2013년 4월 9일)
† 주저자, mgchoi@cau.ac.kr
‡ 교신저자, mgchoi@cau.ac.kr

직, 제어시스템을 구성하는 디바이스의 취약성 점검 및 보안대책 수립, 제어시스템에 연동된 네트워크의 안전성 평가 및 제어시스템 전체에 대한 위험 관리 등을 포함할 수 있어야 한다. 제어시스템의 보안성 평가와 일반 정보시스템의 보안성 평가와 유사한 측면이 존재하지만, 제어시스템의 고유한 특성을 반드시 고려해야 한다. 제어시스템은 환경, 구성 디바이스, 제어시스템 연동 방식, 제어시스템이 오작동 발생할 수 있는 파급력 등을 감안할 때, 현존하는 보안성 평가 절차 및 방법론을 적용하기 어렵다. 따라서 제어시스템의 획득 절차, 제어시스템의 운용 환경, 제어시스템의 기능, 제어시스템의 시스템 특성, 조직 등을 고려한 제어시스템의 보안성 보증을 위한 보안 평가 절차 및 방법론의 연구가 필요하다. 따라서 본 연구는 제어시스템의 획득절차, 운용 환경, 컴포넌트 기능, 컴포넌트 특성 등에 적합한 정보보안 평가 프로세스 및 정보보안 보증 체크리스트를 연구한다.

본 연구가 제안하는 정보보호 평가 프로세스 및 체크리스트는 제어시스템 정책 및 조직, 제어시스템 보호프로파일, 제어시스템의 위험 관리 및 제어시스템을 구성하는 각종 디바이스의 취약성 점검 체크리스트 등을 포함한다.

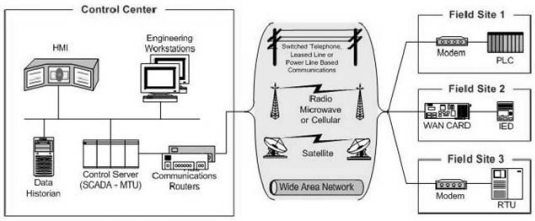
본 연구가 제안하는 제어시스템 보안 평가 방법론은 제어시스템의 개발자, 운용자 및 보안 평가자 등이 채용할 수 있으며, 본 연구의 결과는 제어시스템의 보안성 보증을 위한 제어시스템의 보호프로파일 개발, 보안대책 개발, 제어시스템의 취약성 점검 및 제어시스템의 보안성 평가에 활용될 수 있다.

본 연구는 구성은 다음과 같다. 2장은 제어시스템의 디바이스 및 제어시스템의 구성을 고찰한다. 3장은 제어시스템 특유의 취약성 및 보안 평가시 고려사항을 제시한다. 4장은 제어시스템의 보안성 평가 프로세스를 개발하고, 5장은 제어시스템 보안성 평가를 위한 체크리스트를 제시한다.

II. 제어시스템 특성 및 보안고려사항

2.1. 제어시스템의 특성

제어시스템은 필드로부터 운영되는 데이터와 센서 측정 결과를 수집하고, 정보를 표시하고, 지역·원격 장비를 순차적 제어 명령을 수행한다. 제어시스템은 장치마다 상호 연결 또는 외부 기기와 연결하여 각 장치에 대한 원격 접근과 제어가 가능하고, 명령 및 조작을 할 수 있는 양방향 통신서비스 환경을 구축한다. 이러한 환경은 DSC(distributed control system) SCADA이다. DSC는 제어시스템으로 작은 지역에서 하나의 프로세서나 플랜트에 적용된 시스템이며, SCADA는 제어시스템의 일종으로 광역, 분산된 동작을 수행하는 플랜트들에 적용하는 분산시스템을 포함하는 광의의 용어이다[15]. 일반적인 제어시스템의 구성은 다음 [그림 1]과 같다[15].



[그림 1] 제어시스템의 구성

제어시스템의 구조는 일반적인 컴퓨터 네트워크와 다른 점이 존재하며[2][7], 이 차이점은 보안요구사항에 영향을 미친다. 가장 큰 차이점은 시스템의 구성이 광범위한 지역에 센서, 로봇, 제어기, 컴퓨터가 유선, 무선, 인공위성을 통해 연결되고 있어 신호방식이 디지털과 아날로그가 동시에 수용된다.

2.2. 제어시스템 보안 평가시 고려사항

제어시스템은 일반적인 정보시스템과 많은 부분이 상이하다. 제어시스템의 보안성 평가는 일반적인 보안성 평가와 다르다. 특히 제어시스템의 보안 평가 기술은 아직 초기 수준에 머물러 있으며, 대부분의 취약성 평가는 정보시스템의 취약성 평가 절차를 따르고 있다. 본 연구는 제어시스템 보안성 평가 방법론의 개발을 위해 제어시스템 고유의 특성을 반영한 보안평가 고려사항을 식별한다.

2.2.1. 제어시스템의 취약성

첫째, 제어시스템의 보안위협과 취약점을 살펴본다. 제어시스템의 구조는 특정회사의 제품을 주문제작하여 다른 시스템과 연동하지 않고 독립적으로 구축 및 운영을 한다. 그러나 최근 정보공유와 신속한 의사결정을 통해 경쟁력 향상을 위하여 비즈니스 시스템과 통합하여 운영이 되고 있다[2].

비즈니스 시스템과의 통합은 제어시스템의 개발형 시스템으로 전환이 요구되고, 따라서 폐쇄망으로 유지되어 노출되지 않은 각종 취약점이 제어시스템에 전이되어 위협이 증가하게 된다.

제어시스템의 제어 네트워크는 성능, 안전성, 유연성, 안전성 등에서 우수한 반면, 보안성은 취약하다.

2.2.2. 네트워크 분리 문제

대부분의 제어시스템은 근본적으로 회사 공동 네트워크 이전에 구축되거나 종종 분리되어 구축된다. 결과적으로 IT관리자는 회사 공동 네트워크나 원격접속 포인트를 통해서 자신의 제어 네트워크로 접근할 수 없다는 가정 하에 운영된다. 그러나 실제 제어시스템 네트워크와 회사 정보시스템은 핵심적인 정보관리상의 이유로 종종 연결되어 운영된다[16].

원격지 접속이 필요하다는 요구사항은 많은 전력회사의 제어시스템 엔지니어가 자사의 공동 네트워크상에서 제어시스템을 모니터링하고, 제어가 가능하도록 시스템을 연계한다.

전력회사는 공동 네트워크와 제어시스템 네트워크 간 연계를 통해 회사 정책결정자가 운용 시스템으로부터 핵심적인 데이터를 즉시 얻을 수 있도록 하였다. 이러한 연동은 보안 위험에 대한 충분한 이해 없이 이루어졌다. 사실, 전력회사의 공동 네트워크에 대한 보안 정책은 위와 같은 접근을 통해 제어시스템에 대한 승인되지 않은 접근이나 제어를 하는 것을 막을 수 없다.

2.2.3. 상이한 시스템 사이의 연동 문제

회사 공동 네트워크와 제어시스템간 연동을 위해서 서로 다른 통신 프로토콜을 가진 시스템간 통합이 필요하다. 통합은 두 개의 상이한 시스템간 데이터 통신이 가능한 인프라를 구축하게 한다. 네트워크 기술자는 통신의 복잡성으로 보안 문제를 해결하지 못하기도 한다. 따라서 제어시스템을 타 네트워크의 승인받지 않은 접근으로부터 보호하기 위해 설계된 접근제어는 제대로 동작하지 못하게 한다. 원인은 일반적으로 네트워크 관리자가 네트워크를 연결하는 핵심 접근 포인트를 간과함으로 비롯된다. 비록 내부적으로 방화벽과 침입탐지시스템, 강력한 패스워드의 효과적이 조합은 제어시스템으로 들어오는 모든 진입점을 보호할 수 없다.

2.2.4. 기타 네트워크 취약성 문제

회사 공동 네트워크와 제어시스템은 종종 연계 운영된다. 따라서 제어시스템의 보안수준이 자사 공동 네트워크의 보안수준과 같아진다. 탈규제에 따라 개방 접속에 대한 압력으로 공동 네트워크의 보안성은 급속도록 취약해진다. [표 1]은 기타 보안 취약점을 요약한다[6][7][8][9].

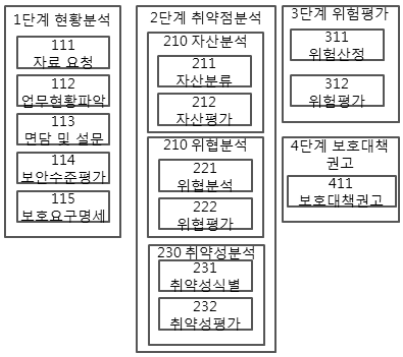
[표 1] 기타 제어시스템 보안 취약점

구분	취약점
정보노출	많은 정보는 단순한 쿼리를 통해 제공
불완전한 네트워크 아키텍처	네트워크 아키텍처상의 설계가 잘못은 제어시스템 문제로 발전 가능
실시간 모니터링 부재	DDoS 등과 같은 공격에 대한 탐지 및 복구 시스템 부재

III. 제어시스템 보안성 평가 방법론

3.1.1. 제어시스템 보안 평가 프로세스

일반 정보시스템을 대상으로 이루어지는 보안성 평가 프로세스는 [그림 3]과 같다[3].



[그림 2] 사이버 보안성 평가 프로세스

제어시스템의 보안성 평가 점검 프로세스는 제어시스템의 시스템 구성과 기능, 통신 프로토콜 등의 내외부적 요인이 있어 발생하는 위협이 크다. 본 연구는 제어시스템의 환경에 적합한 변경된 제어시스템의 보안 평가 프로세스를 제안한다. 개발된 제어시스템 보안성 평가 프로세스는 [그림 2]과 같다.

제어시스템의 보안성 평가 프로세스는 다음과 같

다. 첫째, 사전준비 단계이다. 둘째, 현황분석 단계에서 자산분석과 위협분석을 수행함과 동시에, 제어시스템의 기능 및 환경설정 검토 단계를 제안한다.

셋째, 취약점평가 단계에서 제어시스템 고유의 취약성 평가를 위한 세부 단계로 구성한다. 넷째, 취약점 보고, 완화 및 대책 수립 단계에서 경영자를 대상으로 하는 요약 보고서 작성 단계가 추가되었다. 제어시스템 취약성 점검 프로세스의 상세한 내용을 살펴보면 다음과 같다.

〔그림 3〕 제어시스템 보안성 평가 프로세스

3.1. 사전준비 단계

사전준비 단계는 제어시스템 평가 절차 이전에 필요한 작업들로 구성된다.

3.1.1. 대상시스템 기본정보 파악

개략적인 자산의 현황 파악은 상위 수준의 시스템 구조를 파악하는 단계이다. 파악해야 하는 시스템/네트워크/물리적 구성은 다음과 같다.

- 시스템 구성 파악
- 네트워크 구성 파악

정보시스템의 주 업무를 파악하기 위한 내용 분석을 실시한다. 업무 파악에서는 업무 분류 및 시스템 분류와 함께 다음의 작업을 수행한다.

- 업무현황조사 면담대상자 선정 및 일정 확정
- 업무현황면담
- 업무파악

3.1.2. 보안 평가 수준 결정

보안 평가 수준 결정 단계에서는 평가 수준을 5등급으로 분류한다. 〔표 2〕는 보안 평가 대상과 평가 방법을 서술한다.

〔표 2〕 보안 평가의 대상과 평가 방법

수준	보안평가 대상	보안 평가 방법	예상 기간
1	• 핵심 업무 수행에 필요한 서버 • 외부망과 연동하는 회사 네트워크 장비 • 주요 웹 응용프로그램	• 개략 자산분석(서버및네트워크장비) • 개략 네트워크 분석 • 취약점분석 도구를 이용한 기술적 취약점 분석 • 개략 모의침투 수행 • 취약점평가 및 즉시 조치사항제시	1-2 개월
2	• 수준 1 포함 • 핵심 업무 수행과 관련되는 내부 네트워크 장비(DMZ) 및 정보보호시스템 • Control Center에 위치한 SCADA • 핵심 업무 수행에 관련된 주요 데이터 및 DB	• 수준 1 포함 • 개략 자산분석 • 상세 네트워크 분석 • 점검표 활용 • 관리적/물리적 취약점 분석 • 모의침투 수행 • 취약점 평가 및 보안대책 수립	2-3 개월
3	• 수준 2 포함 • 개인 PC • SCADA 통제 네트워크 및 정보보호시스템	• 수준 2 포함 • 자산분석(PC) • 상세 관리적/물리적 취약점 분석 • 보안대책 및 추진계획 수립	3-5 개월
4	• 수준 3 포함 • 핵심 업무 백업에 필요한 서버 • 내부 행정 업무 관련 네트워크 장비 • 핵심 업무 수행과 관련된 백업용 데이터 및 백업 DB • 기타 웹 응용프로그램 • SCADA 필드장치	• 수준 3 포함 • 상세 자산분석 • 보안전략계획 수립 및 즉시 조치사항 이행확인 • 위험평가	4-6 개월
5	• 수준 4와 동일	• 수준 4 포함 • 위험 평가 • 기대 효과 분석	6개월 이상

3.1.3. 평가팀 결성

자산 소유자는 평가팀을 선정한다. 선정될 평가팀의 정보는 다음과 같다.

- 팀 구성원에 관한 정보는 평가를 수행하는 기관이 제공한다.
- 대부분의 평가팀 구성원은 학위나 자격증을 보유하지 않으며, 경험적인 지식을 축적한다.
- 자산 소유자는 평가팀이 적절한 제어 시스템 경험을 가지고 있는지 확인하기 위해 팀원의 공식

적인 증빙 서류를 확인한다.
- 평가팀 구성원의 역할과 책임을 명확히 정의하고, 자산 소유자에게 통보해야 한다.

3.1.4. 자료 및 인터뷰 요청

자료 및 인터뷰 요청 단계에서는 기관 특성과 기관 현황 파악을 위한 자료 도출을 위해 자료 및 인터뷰를 요청한다.

요구 자료는 조직구성도, 네트워크 구성도 및 장비 현황, 시스템 구성도 및 장비 현황, 업무구성도 및 업무설명자료, 정보보호정책서, 지침서 및 설명 자료로 구성된다. 기관 조직도 및 업무 담당자 연락처 도출과 자료 요청 문서 발송/구두 요청을 수행한다.

현행 정보보호현황 및 요구사항 분석을 위하여 관련 부서 설문지 작성을 한다. 면담은 면담자 선정, 면담 일시 및 장소 확정, 면담 대상자를 위한 설명자료 작성의 절차로 진행된다.

면담 및 설문 준비가 완료되면 면담 및 설문을 실시한다. 각 면담은 경영자 면담, IT관리자 면담, - 제어시스템 운영자 면담 등으로 이루어진다.

- 조직구성원 면담

3.1.5. 취약점 평가 계획서 작성

평가 계획의 세부사항 정의를 수행한다. 자산 소유자는 자세한 평가 계획을 만족하지만, 평가팀은 자세한 계획 수립에 필요한 시간과 비용은 계획은 방해가 됨을 인지한다.

평가 진행 중에는 시스템 구성을 고정하여야 한다. 또한 자산 소유자와 운영자는 평가팀과 논의 없이 테스트 중에 시스템 변경 금지를 반드시 숙지한다. 그리고 제어 시스템 관리자(또는 적절한 인력)가 평가팀을 감시하며 시험에 참여하고, 관리자는 평가팀과의 협력을 통해 정보 자원의 시험 결과를 자산 소유자에게 전달해주는 역할을 수행한다.

평가팀의 평가 활동과 관련된 제약사항 (평가팀의 안전사항, 평가과정에서 발생하는 민감한 정보의 처리 사항, 평가대상 시스템의 무결성)을 확인한다. 평가 예산은 평가 소요 시간에 의해서 산출되며, 평가 소요시간, 소요 인력 비용, 행정지원비용 등으로 구성된다.

3.2. 현황분석 단계

현황 단계에서는 일반적인 취약점 분석 방법론과 거의 동일한 단계를 거치나, 앞서 언급한 바와 같이 제어 시스템 고유의 특성에 맞춘 단계를 추가/수정하였다.

3.2.1. 자료검토 및 인터뷰

동 단계에서 기술 자료 검토를 수행한다. 기술적 문서 검토 대상은 시스템 인벤토리, 아키텍처 다이어그램, 프로세스 다이어그램, 절차 및 프로세스 문서 등을 통해 제어 시스템 검토 등이다.

자료 검토에서는 시스템/네트워크/물리적 환경 검토를 수행한다. 자세한 내용은 다음과 같다.
- 시스템 구성 검토
- 네트워크 구성 검토
- 제어시스템 구성 검토

직원 인터뷰의 대상은 제어 시스템 직원인 프로세스 엔지니어, 운영자, 벤더, 통합업체, 개발자, 소유자, 관리자이다. 직원 인터뷰의 목적은 제어 시스템 프로세스 및 절차에 대한 이해와 통찰력 획득과 팀은 시스템 설계 방식이나 운영 방식에 있는 보안 취약점을 발견하기 위하여 시스템 운영자와 인터뷰를 수행할 수 있음에 있다.

3.2.2. 제어 시스템 기능 및 환경 설정 검토

제어 시스템 기능 및 환경 설정 파악의 목적은 다음과 같다.
- 평가팀은 기능을 확인하고 시스템의 환경 설정을 점검함으로 제어 시스템을 검사할 수 있다.
- 점진적으로 디바이스의 기능 및 제어 시스템 특징을 점검해야 한다.
- 평가팀은 제어 시스템 컴포넌트의 환경 설정을 체크해야 한다.

제어 시스템 기능 및 환경 설정 검토의 장점은 다음과 같다.
- 평가팀이 제어 시스템의 고유한 요구사항과 특성을 이해하는 데 도움이 된다.
- 이 활동은 프로세스를 최적화 될 수 있는 영역을 식별하게 한다.
- 운용 중인 시스템 컴포넌트와 네트워크 평가 및 안전하게 하는 유일한 방법이다.

반면 단점은 시스템을 실제로 테스트하지 않고, 침투 테스트는 운용중인 제어 시스템에 대해서 행해져야 한다.

3.2.3. 보안요구 명세서

보안요구명세서는 현재 시스템의 정보보호상태에 비추어 기밀성, 무결성, 가용성을 만족시키기 위하여 필요한 일련의 행동, 제도정비나 보안도구의 설치 등과 같은 것을 명세한다.

관리적, 물리적, 기술적 부문의 보안요구명세서 작성이 요구되며, 경영자, 관리자, 담당자와의 면담 및 설문 내용을 토대로 보안요구명세 작성한다. 보안요구명세서에서 조직의 보안요구사항 분석은 다음 자료를 통해서 이루어진다.

- 보안수준평가를 위한 경영자, 관리자, 담당자, 일반직원 등과의 면담 및 설문 내용
- 법적 규정, 내부 규정 또는 다른 조직과 맺은 계약으로 조직이 상대방을 만족시키는 정보보호요구사항
- 조직의 운영을 지원하기 위하여 개발된 정보처리 체계의 원칙, 목적 등을 만족시키기 위한 정보보호요구사항

3.2.4. 공격 대상 식별

공격 대상 식별을 위해, 공격 대상 리스트 작성이 요구된다. 이 단계에서는 공격 대상이 되는 특정 기능이나 네트워크 침투 대상 설정과 평가 계획에 초기 공격 벡터의 집합을 자세하게 서술하지만, 평가팀이 공격 대상을 정의하고, 공격 방법을 자세하게 서술하지 않는다.

공격 대상의 리스트를 토대로 우선순위를 작성한다. 생성된 공격 벡터의 목록을 참고하여 제어 시스템의 잠재적인 손상 정도에 따라 공격 대상의 우선순위가 결정된다. 손상정도가 높은 공격 제어 시스템부터 공격 대상으로 설정한다. 평가 계획에 포함되는 공격 설명은 의도적으로 모호할 수 있다. 즉 실제 공격 벡터는 설명보다 더 좋은 효과를 낼 수 있다. 상위 수준의 설명은 평가팀이 공격자의 공격 방식에 얽매이지 않고, 문제 탐구에 필요한 유연성을 가지게 한다. 공격 벡터 설명은 애매하지만, 공격 대상의 우선 순위화는 목표를 위한 추가적인 세부사항을 정의해야 한다.

예상 가능한 초기 공격 벡터의 목록은 다음과 같다.

- Attack the FEP from the field equipment side (manipulate the RTU or PLC connection)
- Attack the FEP from the control system network side
- Attack the application server (e.g. the HMI)
- Attack the real-time database server
- Attack the historian server

3.2.5. 자산분석

자산 분류자산 범위 산정은 현행 분석 시스템, 네트워크, 응용 구성도 등을 참조하여 대상 범위 정의한다.

자산 조사는 자산 분류 기준에 관련 담당자들의 협조를 받아 조사하며, 자산항목별 분류 및 자산범위에 따른 선별하고 업무처리와 조직을 고려한 자산조사를 수행한다. 점검 대상의 자산을 분류할 수 있다. 우선 첫 번째로 자산의 속성에 대해 분류하면 다음과 같다.

- 정보/데이터: 조직 및 인사정보, 자금정보 등 조직의 중요한 정보자산
- 하드웨어: 조직의 업무, 서비스를 수행하기 위한 H/W
- 소프트웨어: 조직의 업무, 서비스를 수행하기 위해 필요한 S/W
- OS: 제어 시스템 고유 OS
- 인력: 제어 시스템 관련 인력
- 환경: 물리적 환경

식별된 자산에 대하여 각 자산의 중요도 분석을 수행한다. 자산 중요도 분석에서는 현행 분석 시스템, 네트워크, 응용 구성도 등을 참조하여 대상 범위 정의하고, 자산가중치, 외부네트워크에서 접근 가능성(n), 침해시 파급효과(a), 처리업무의 중요도 (b), 정성적 기준, 기밀성(C), 무결성(I), 가용성(A) 등을 고려하여 결정한다. 자산의 중요도는 정성적인 기준을 사용한다.

각 자산의 중요도 등급을 계상한다. 등급의 세부사항은 다음과 같다.

- 매우 높음(VH): 자산의 피해 발생 시에 국가 전체의 마비가 오는 극심한 피해
- 높음(H): 자산의 피해 발생 시 업무를 계속할 수 없는 극심한 피해의 상태
- 중간(M) :자산의 피해발생시 업무 기능의 현저한 저하 및 직원이나 시스템 운용자가 업무에 심각한 지장을 초래
- 낮음(L) :자산 피해발생시 업무 기능의 저하 및 운영자의 작업 효율성을 감소시킴

3.2.6. 위협분석

위협 분석에서는 위협을 식별하고, 위협의 영향과 발생가능성을 고려하여 위협 평가를 실시한다.

위협 식별의 조사항목은 위협 유형별 분류, 알려진 위협 조사, 위협시나리오에 의한 위협 조사, 위협영향, 위협발생주기의 과정을 거친다.

위협 식별 과정에서 자산에 대하여 발생했거나 발생할 가능성이 있는 보안 관리에 관한 위협을 조사하고, 성질 유형에 따라 분류한다. 그리고 IT분야의 자산과 취약성과의 관계를 고려하여 위협을 정보/데이터, 문서 및 서류, OS, 인력, 환경, 하드웨어, 소프트웨어 등으로 분류한다. 마지막으로 피해규모를 산출하기 위해 발생빈도, 피해종류, 발생가능성, 피해대상(자산) 등을 모두 고려한다.

위협 식별 과정에서는 위협 시나리오를 고려한다. 위협 시나리오는 파악되지 않은 위협을 발견하기 위한 가상적인 위협환경을 설정하고, 발생 가능한 위협을 유추하여 위협을 탐색하는 방법이다.

위협 식별방법은 다음과 같이 정리할 수 있다.

- 자산에 대한 행위자: 인간과 비인간으로 분류, 인간은 내부자, 외부자, 제3자로 분류, 비인간은 기술, 환경(사회적 문제), 자연 (자연재해) 등으로 분류
- 자산접근경로: 네트워크를 통해서 접근, 물리적으로 직접 접근
- 자산접근동기: 우연은 목적 없이 우연이 접근, 고의는 어떤 목적을 달성하기 위해 접근

식별된 위협을 바탕으로 위협 평가를 실시한다. 위협 평가의 기준은 위협에 의한 영향과 발생주기 또는 가능성에 따라 달라진다. 〔표 3〕는 위협 평가 기준을 서술한 것이다.

위협 영향과 발생주기에 따라 위협 정도와 위협 등급이 산출된다. 위협평가 매트릭스는 〔표 4〕와 같다.

〔표 3〕 위협 평가 기준

평가	발생주기 또는 가능성
매우 높음 (VH):4	시스템의 수명주기 동안 매우 자주 발생함 (3개월)
높음(H):3	시스템의 수명주기 동안 5번 이상 발생할 수 있는 상태 (6개월)
중간(M):2	시스템 자산이 수명주기 동안 2-3차례 손해를 입을 수 있는 상태 (1년 이내)
낮음(L):1	자산의 수명주기 동안 거의 발생하지 않음

〔표 4〕 위협 평가 매트릭스

위협 영향	L				M				H				VH			
발생 주기	L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
위협 정도	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
위협 등급	1	2	2	3	2	2	3	3	2	3	3	4	3	3	4	4

위협평가는 위협에 의한 영향과 위협 발생주기를 함께 고려하여 작성한 위협평가기준표와 위협평가 매트릭스에 의한 등급에 의해 산출한다.

3.3. 취약점 평가 단계

취약점 평가 단계에서는 제어시스템에 적합한 취약점 평가 절차를 거쳐 최종적인 제어시스템 취약점 등급을 산출한다.

3.3.1. 실험실 평가

실험실 평가는 제어 시스템이 운용 중인 시스템과 동일한 제어 시스템을 구성하여 분리된 네트워크에서 수행한다. 여기에서 동일하게 복제된 시스템은 최대한 운용 중인 시스템과 기능이 동일해야 한다. 시험은 운용 중인 시스템의 환경 등을 최대한 유사하게 구비하여 수행한다. 자산 소유자는 평가를 위한 제어 시스템을 사전에 구성된 개발 시설을 활용해야 하며, 최소한도의 장비는 구성되어야 한다.

실험실 평가는 제어 시스템을 구성하는 프로세스와 프로토콜 내에 있는 취약성을 찾을 때 가장 효과적이다. 만약 자산소유자가 식별된 취약성을 완화시킬 수 없다면 효과가 매우 낮다. 동 시험은 제어 시스템 공급자가 보안에 매우 적극적이고, 보고된 취약성에 대한 패치를 신속하게 내놓을 때 적합하다. 자산 소유자는 시험 시작 전 보안패치에 대한 강제조항이 있을 때 비용이 낭비되지 않는다는 사실을 인식해야 한다.

3.3.2. 운용중인 시스템 평가

운용중인 제어 시스템의 보안평가는 운용중인 제어 시스템을 운용 장소에서 시험하는 것이며, 시험을 위해서 제어 시스템의 모든 특성이 존재해야 되고, 활성화되어야 한다.

특히 운용중인 시스템 평가는 신중히 수행되어야 한다. 제어 시스템 파괴에 따른 잠재적인 영향은 심각하며, 시험 활동은 트래픽과 이벤트를 관찰하는 것을 위주로 해야 한다. 팀이 공격 벡터를 시험할 때는 대상 컴포넌트를 일시적으로 운용중인 시스템에서 분리할 수 있는지를 제어 시스템 관리자와 협의해야 한다. 만약 긍정적인 답변을 얻을 수 없다면, 긍정적인 답변을 얻을 때까지 공격 벡터를 사용해서는 안 된다.

운용중인 시스템 평가를 수행할 때, 평가팀은 운용중인 제어 시스템에서 평가 대상을 엄격하게 선정해야 한다. 평가 결과는 해커가 제어 시스템에 접근권한을 획득하는 것을 막는 보호대책도 평가를 해야 한다. 자산소유자와 평가팀이 동 시험의 의미를 이해한다면, 참가자는 프로세스에 영향을 주지 않고, 중요한 사항에 초점을 둘 수 있다. 운용중인 시스템 평가는 사이트에서 공격자가 시행할 수 있는 공격을 설명할 수 있다. 사이트 보안 평가는 실험실 평가를 수행한 후 또는 제어 시스템을 시험할 수 있는 다른 방법이 부재할 때 사용이 가능하다.

3.3.3. End-to-End 침투 평가

End-to-End 침투평가의 목적은 공격자가 얼마나 깊이 침투할 수 있는지를 실질적으로 파악하는 것이다. 침투평가에서 얻어지는 정보는 실질적인 취약점 평가에 도움이 된다. 예를 들면, 평가팀이 회사의 LAN에 있는 공격자가 DMZ 서버를 훼손하고, 다른 DMZ 서버를 오용할 수 있다면, 공격자가 공격 대상을 원격에서 통제할 수 있다는 추론이 가능하다. 침투평가는 시간과 비용이 많이 소모되는 관계로 주어진 평가예산 내에서 최대한 자원을 활용해야 한다.

침투 평가는 자산소유자에게 보호대책이 사이버 공격에 얼마나 취약한지를 보여주고, 사이버 평가팀이 한 네트워크에서 다른 네트워크로 침투를 불가능하게 하는 격리는 네트워크 경계선의 안전성을 나타낸다. 반면에 시험과 관련된 많은 시간이 제어 시스템에 직접 관련되지 않은 영역에서 소비될 수 있고, 인터넷에서 제어 시스템으로의 침투할 수 있는 탐색을 개발하고, 연결하는 시간을 낭비한다.

보안평가팀은 제어 시스템에 연결된 경계선의 연결부분과 제어 시스템을 구현한 프로세스와 프로토콜에 초점을 두고 평가해야 한다.

결론적으로, end-to-end 평가는 공격자가 회사 네트워크에 접근할 수 있는지를 여부를 평가하며, 동 평가는 제어 시스템에 존재하는 취약성에 접근을 막는 제어 시스템 경계 방어의 효과성을 시험한다. 그리고 제어 시스템 평가시 평가팀은 공격자가 통제 네트워크에 접근할 수 있는 방법을 찾을 수 있다고 가정해야 하며, 실험실 평가는 제어 시스템 소프트웨어에 초점을 두고 있으며, 운용중인 시스템 평가는 위험에 노출시키지 않고 제어 시스템 네트워크와 호스트에 초점을 둔다.

3.3.4. 취약점 평가

취약점 평가는 자동점검, 체크리스트 등에 의한 점검결과에 대해 분석하고, 시스템 보안현황을 파악한다. 취약점 평가는 다음의 단계를 따른다[7,8,9].

첫째, 기존보호대책을 분석한다. 관리적, 물리적, 기술적 취약성에 대해 기존 보호대책이 어떻게 적용되고 있는지를 분석한다.

둘째, 메트릭을 활용한 취약점 분류를 수행한다. 취약점이 식별되면, 다음 해야 할 작업은 취약점의 영향을 결정하는 것이다. 평가팀이 취약점에 대해 하나 이상의 공격을 만드는 주된 이유 중 하나는 취약점 영향을 이해하기 위함이다.

일반 취약점 점수시스템(CVSS)은 개별 조직의 독특한 환경에 대한 위험을 나타내는 방식으로 취약점 점수를 표준화한 방법이다. CVSS v2 점수 방법은 취약점이 조직에 미치는 실제 위험도에 따라 우선순위를 매기는 사이버 보안 업계 표준이다.

셋째, 취약점을 평가한다. 취약성 데이터베이스(NVD)는 CVSS v2 점수를 부여하고, 취약점 심각도 등급에 따라 점수를 부여한다. NVD는 CVSS 점수에 심각도 등급 '낮음', '중간', '높음'을 추가하여 제공하고, 질적 순위는 CVSS 점수를 매핑한다. [표 5]는 CVSS 점수와 질적 순위 간의 매핑을 보여준다.

[표 5] NVD 보안 등급

CVSS Score	NVD severity rating
7.5-10.0	매우 높음(VH):4
5.0-7.4	높음(H):3
2.5-4.9	중간(M):2
0.0-2.4	낮음(L):1

3.3.5. 위험 평가

위험 평가에서는 위험도를 산정하고 제어시스템 위

험 등급을 결정한다. 위험 산정에서는 위험 시나리오 작성 및 분석, 자산/위협/취약성 매트릭스 작성과 기 분석 결과를 기반으로 주요자산 위험수준을 결정한다.

위험 산정은 자산, 위협, 취약성 상호간의 작용을 평가해서 위험도를 산정해야 한다. 위험 평가는 제어 시스템이 공격받을 수 있다는 가능성을 수치적으로 결정한다. 이 방법은 침투 테스트에 비해 더 적은 시간과 자원이 필요하다. 이 방법은 팀의 작업이 시스템 운영에 관해 수동적임으로 안전한 생산 시스템에서 수행할 수 있다. 제어 시스템의 위험 평가 등급 결정은 〔표 6〕을 통해 이루어진다.

〔표 6〕 제어 시스템의 위험 평가 등급 결정

위협		L				M				H				VH			
취약성		L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
자산	L	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7
	M	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
	H	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9
	VH	4	5	6	7	5	6	7	8	6	7	8	9	7	8	9	10

3.4. 취약점 보고, 완화 및 대책 수립 단계

요약 보고서는 취약성뿐만 아니라 문제를 완화하는 데 필요한 노력을 서술한다. 취약점이나 기타 보안 문제는 조직의 치료 노력을 우선 순위화하여 선정한다. 요약은 시험한 제어 시스템의 평가된 항목이 서술되어야 한다. 평가 결과 보고서는 다음의 내용을 포함한다.

- 발견된 취약점의 요점을 반복하고, 완화의 가능성을 식별한다.
- 자산 소유자는 제어 시스템의 사이버 보안 평가에 대한 취약점 점수를 사용한다.
- 취약성 및 식별된 보안 문제는 조직의 치료 능력에 따라 우선순위화 하여야 한다.
- 취약점 완화 내용을 서술한다.

IV. 제어시스템 보안성 평가 점검 체크리스트

제어시스템의 보안성 평가 프로세스를 진행하기 위하여 구체적인 보안성 평가 체크리스트의 구현이 필요하다. 보안성 평가 점검 체크리스트는 제어시스템 보안성 평가 점검 프로세스에서 제어시스템 개발자, 운용자 및 평가자가 수행해야 할 중요한 활동을 나열한다.〔7,8,9〕

4.1. 제어시스템 보안성 평가 체크리스트

4.1.1. 제어시스템 정책 및 절차 평가 체크리스트

〔표 7〕은 제어시스템의 정책과 절차를 평가하는 체크리스트이다.

〔표 7〕 정책 및 절차 평가 체크리스트

평가대상	
정보보호정책	보안 훈련과 인식
문서화된 보안 훈련	보안지침
장비 구현 지침	관리 메커니즘
제어시스템의 보안 감사	재해 복구 계획
제어시스템 구성 변경 관리	감사 및 책임
정보보호조직	인적 보안
외부자 보안	자산 분류
매체 관리	교육 및 훈련
접근통제	운영 관리
업무 연속성	사고 대응
감사	

4.1.2. 제어시스템 플랫폼 평가 체크리스트

〔표 8〕는 제어시스템에 대한 플랫폼 보안성 평가 체크리스트이다.

〔표 8〕 플랫폼 보안성 평가 체크리스트

평가대상	
보안아키텍처 설계 적합성	소프트웨어의 보안 패치
보안형상관리 및 유지 보수	
기본 구성	
구형 OS 및 프로그램 취약점평가	
제어시스템 소프트웨어 보안구성관리 및 유지보수	
휴대 장치에 저장된 데이터	암호정책.
암호 취약점	암호 노출
암호 추측	암호문 관리.
부적절한 접근 제어	허가, 권한, 접근 통제

4.1.3. 제어시스템 플랫폼 하드웨어 평가 체크리스트

제어시스템의 플랫폼 하드웨어와 내포된 취약점을 평가할 수 있는 평가 체크리스트는 〔표 9〕와 같다.

〔표 9〕 플랫폼 하드웨어 평가 체크리스트

취약점	
부적절한 테스트	부적절한 물리 보호
인증되지 않은 직원의 장비에 물리적인 접근	안전하지 않은 원격 접속
문서화 되지 않은 자산	전자-자기 펄스(EMP)
백업 전원의 부족	중요구성요소슬랙부족

4.1.4. 제어시스템 플랫폼 소프트웨어 평가 체크리스트

제어시스템의 소프트웨어 취약점을 분류하고, 내용을 제시하면 〔표 10〕과 같다.

〔표 10〕 제어시스템 플랫폼 소프트웨어 평가 취약점

평가대상	
버퍼 오버플로우	입력값 범위체크
커맨드 인젝션	SQL 인젝션
제한된 디렉터리에 대한 경로명의 부적절한 제한	
LDAP인젝션	운영체제명령실행
포맷스트링	SSI 인젝션
XPath인젝션	디렉토리인덱싱
정보누출	악성콘텐츠
약한문자열강도	보안 기능 비활성화
서비스 거부(DoS)	잘못된 처리
낮은 수준의 코드 품질	승인, 권한부여 및 접근통제
OLE for Process Control (OPC)	
민감한 정보 관리	일반 텍스트
불필요한 서비스	구성 및 S/W 불충분한 인증
유지보수 매뉴얼 및 독점 소프트웨어	
소스코드, 시스템 수정파일	로그 비유지
사고 비탐지	공통적인 취약점
위치공개	데이터 평문전송
쿠키변조	

4.1.5. 제어시스템 플랫폼 악성코드 평가 체크리스트

플랫폼 악성 코드 방어 취약점은 플랫폼을 악성 코드로부터 방어할 때 정상적으로 방어를 가로 막는 취약점이다. 체크리스트는 〔표 11〕과 같다.

〔표 11〕 플랫폼 악성 코드 방어 평가 체크리스트

평가대상
악성코드 방지 소프트웨어의 미설치
악성코드 방지 소프트웨어 최신 업데이트
충분한 테스트를 거치지 않은 악성코드 보호 소프트웨어

4.1.6. 제어시스템 네트워크 취약점 평가 체크리스트

제어시스템의 취약점은 네트워크의 결함, 잘못된 구성, 잘못된 관리에서 발생할 수 있다. 이러한 취약점은 다양한 보안 제어를 통해 제어하거나 완화할 수 있다. 〔표 12〕는 제어시스템의 네트워크 취약점과 관련된 체크리스트이다.

〔표 12〕 제어시스템 네트워크 평가 체크리스트

평가대상	
취약한 네트워크 아키텍처	보안 파이미터 미정의
DMZ의 기능적 불완전성	네트워크 분리의 불완전성
방화벽 우회	방화벽 부적절한 구성
데이터 접근제어	기본 구성사용
감사 및 책임	네트워크 장치설정
비암호전송	암호의 공개
접근제어 적용문제	취약한 방화벽 정책
적절하지 못한 인증	

4.1.7. 제어시스템 네트워크 하드웨어 평가 체크리스트

제어시스템의 취약점은 네트워크 하드웨어와 관련된 잘못된 구성, 잘못된 관리에서 발생할 수 있다. 〔표 13〕은 네트워크 하드웨어와 관련된 취약점 점검리스트이다.

〔표 13〕 네트워크 하드웨어 평가 체크리스트

평가대상	
네트워크 장비 물리적 보호	안전하지 않은 물리 포트
제어시스템 네트워크 컴포넌트 구성관리	
환경 제어 손실	비인증된 인원의 접근
네트워크의 슬랙 점검	계정 관리
접근 관리	패치 관리
기능 관리	로그 관리

4.1.8. 제어시스템 네트워크 경계 평가 체크리스트

제어시스템 네트워크 경계 평가 체크리스트는 3단계 취약성 평가 단계의 운용중인 시스템평가, 취약점 평가, 및 4단계 취약점 보고,완화 및 대책수립 단계에서 완화조치분석, 완화전략 확인 및 테스트 등의 프로세스에서 수행하는 평가 활동이다. 〔표 14〕는 네트워크 경계 평가 리스트이다.

〔표 14〕 네트워크 경계 평가 체크리스트

평가대상	설명
보안 경계 미정의	방화벽 및 라우터 로그
비제어 트래픽이 제어 네트워크 사용	
제어 네트워크 서비스가 없음	
방화벽의 부재, 적절치 못한 구성	
네트워크 보안 감시	

4.1.9. 제어시스템 통신 평가 체크리스트

제어시스템의 통신시에 많은 취약점이 발생한다. 제어시스템 통신 시의 체크리스트는 〔표 15〕와 같다.

〔표 15〕 통신 평가 체크리스트

취약점	
통신 무결성 검사	주요 제어 경로 미정의
통신 프로토콜 사용	인증 비표준화
데이터 인증에 대한 불인정	
클라이언트와 접속장치간 데이터 보호	
클라이언트와 접속장치 사이의 부적절한 인증	

4.1.10. 제어시스템 물리적 평가 체크리스트

제어시스템을 둘러싸고 있는 물리적 보호대책은 다양하다. 제어시스템은 외부의 침입으로부터 기본적으로 안전하게 보호되어야 한다. 제어시스템의 물리적 평가 체크리스트는 〔표 16〕과 같다.

〔표 16〕 물리적 평가 체크리스트

평가대상	설명
접근 통제	주요 시스템에 대한 별도의 출입통제를 실시하거나 이중의 보호 장치 설치 여부 평가
감시 통제	주요시설의 출입구와 전산실 및 통신장비실 내부에 CCTV를 설치 여부를 평가
전력 보호	전원 공급 이상이나 기타 전기 관련 사고로부터 장비가 보호됨을 평가
환경 통제	물리적 중요도에 따라 제한구역, 통제구역 등으로 분류하는 다단계 보호 대책을 평가

4.2. 제어시스템의 잠재적 위협원

제어시스템에 대한 위협은 적대적인 기관, 테러 집단, 산업스파이, 내부자 위협, 악의적인 침입자와 같은 적대적인 출처, 시스템 복잡도, 인간의 실수와 사고, 장비 고장, 자연 재해와 같은 자연적인 출처에서 발생한다. 제어시스템에 대한 적대적인 위협(자연적인 위협)원을 살펴보면 〔표 9〕와 같다.

〔표 17〕 제어시스템의 잠재적 위협원

위협 요소	
공격자	봇-네트워크 운영자
범죄 집단	국제정보 서비스
내부자	피셔
스패머	악성프로그램 제작자
테러리스트	산업 스파이

V. 결 론

제어시스템은 국가주요인프라, 산업주요시설 등의 다양한 환경에서 개발 및 운용되고 있지만, 보안에 대한 인식 및 보안 기술에 대한 연구·개발 수준이 매우 낮은 상황이다. 제어시스템의 보안대책이 제시되어 운용되고 있지만, 보안성에 대한 보증은 이루어지지 않은채 운용되고 있어 보안 대책의 유효성을 판단하기 어려운 상황이다.

제어시스템의 사이버 보안 평가 기술은 아직 초기 수준에 머물러 있는 실정이다. 제어시스템의 사이버 보안 평가 기술이 기존의 보안 평가 기술과 근본적인 차이점은 제어시스템이 다양한 형태의 필드 디바이스와 정보시스템을 포함하고 있고, 이해 당사자가 다양하다는 점이다. 제어시스템의 보안 취약성은 일반 IT 정보시스템과 비교할 때 다양한 형태로 존재할 수 있다.

본 연구는 제어시스템의 다양한 형태의 취약성을 식별해야 하는 당위성을 제공하고, 평가자가 점검할 수 있는 객관적이며, 타당성 있는 점검 프로세스를 제공한다. 제어시스템의 설계, 개발, 운용 전 수명주기의 관점에서 제어시스템의 보안성을 보증할 수 있는 기술의 개발은 제어시스템의 보안 대책의 실효성을 판단하여 적절한 보안 대책의 추가 개발 또는 현존하는 제어시스템의 보안성을 확인해주는 역할을 수행한다.

본 연구는 제어시스템의 환경, 구성 디바이스 및 운용 등의 특성을 감안하여 제어시스템에 적합한 보안성 평가 방법론 및 제크리스트를 제시하고 있다. 본 연구가 제시하는 평가 방법론 및 체크리스트는 제어시스템의 보안성을 보증할 수 있는 전체적인 내용을 서술하고 있지만, 구체성에 있어서 추가적인 연구가 더 필요하다. 동 연구의 한계는 제안된 방법론을 검증할 수 있는 사례가 없어 유용성을 검증하지 못했다는 점이다.

동 연구가 제시하는 내용은 제어시스템 획득자, 개발자, 평가자가 제어시스템 보안대책의 계획 및 구현, 제어시스템의 국내외 획득, 제어시스템에 대한 보안평가시에 가이드라인으로 활용할 수 있다.

참고문헌

〔1〕 이철수, "산업제어시스템 정보보안 감리 프레임워크 연구," *한국정보보호학회논문지*, 18(1),

pp.139-148, 2008년 12월.
〔2〕 최명균, 이동범, 곽진, "제어 시스템에 대한 보안정책 동향 및 보안 취약점 분석," *한국정보보호학회논문지*, 21(5), pp.55-64, 2011년 8월.
〔3〕 한국정보보호진흥원, "취약점 분석·평가 모델," December 2002.
〔4〕 ANSI/ISA-99.00.01-2007, "Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models," pp.69-73, October 2007.
〔5〕 CPNI, "Cyber Security Assessments of Industrial Control Systems," November 2010.
〔6〕 DHS, "Recommended Practice for Patch Management of Control Systems, Department of Homeland Security," December, 2008.
〔7〕 DHS, "Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments," July, 2009.
〔8〕 DHS, "Common Cybersecurity Vulnerabilities in Industrial Control Systems," May 2011.
〔9〕 DHS, "Recommended Practice:Improv-ing Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," October, 2009.
〔10〕 ISA, "Security for Industrial Automa-tion and Control Systems Part 1: Terminology, Concepts, and Models, International Society for Automation," October 29, 2007
〔11〕 Lee, Kathy, et al., "U.S. Department of Energy Office of Electricity Delivery and Energy Reliability," NSTB ICCP Security Assessment, February 2010.
〔12〕 Mell, Peter, Scarfone, Karen, and Romanosky, Sasha, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," June 2007
〔13〕 MITRE, "Common Attack Pattern Enumeration and Classification (CAPEC),"http://measurablesecurity.mitre.org/directory/areas/softwareassurance.html.
〔14〕 MITRE, "CWE(Common Weaknesses Enumeration)," Department of Homeland Security, January 11, 2009.
〔15〕 NIST, NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security, Final Public Draft, National Institute of Standards and Technology," September 29, 2008.
〔16〕 NIST, NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," September 2008.

〈著者紹介〉

최 명 길(Myeonggil Choi) 종신회원
1988년~1993년: 부산대학교 학사
2004년: 한국과학기술원 박사
1995년~2000년: 국방과학연구소 연구원
2000년~2005년: 국가보안기술연구소 선임연구원
2005년~2007년: 인제대 교수
2008년~현재: 중앙대 교수
〈관심분야〉 보안성평가, 정보보호정책 및 관리, 개인정보보호