정 보 보 호 학 회 지
제24권 제5호, 2014. 10

에너지 기업에 대한 정보보호 관리체계 발전방향

유 영 인*, 정 수 연**, 이 경 호***

요 약

국내 IT 인프라 수준은 세계 최고임에도 불구하고 그에 미치지 못하는 정보보안체계로 많은 사이버 위협에 노출되어 있다. 이는 산업제어시스템 또한 점차 온라인상으로 제어되기 시작하면서, 국가 기반 시설인 에너지 기업에도 문제가 확대되고 있다. 산업제어시스템인 원자력 발전소 SCADA 시스템의 경우 최근 이란에서 스턱스넷 공격으로 인해 발전소 가동이 중단되는 사태가 발생하기도 하였다. 이러한 사이버 보안 위협 에 대응하기 위해 현재 도입된 정보보안체계는 다양한 분야별로 충분한 이해를 바탕으로 그 성격에 맞게 적용이 되어야 하지만 획일화 된 기준과 평가방식으로 비효율적인 결과를 만들고 있다. 이러한 문제를 인식하고 에너지 분야에 초점을 맞추어 그에 적합한 특화된 정보보호 관리체계를 수립하는 동시에 평가지수의 제도화 및 활성화를 제안하고자 한다. 이 제안을 통해 에너지기반 시설 위험을 방지하고 각종 위협에 대처능력이 향상 될 것을 기대한다.

Ⅰ. 서 론

전 세계적으로 고도화된 사이버공격이 예상되고 있는 가운데 각 나라별로 위협에 대한 피해를 미리 방지하기 위해 정보보호 관리체계를 적용하고 있다. 현재 우리나라도 위험공격을 대비하고자 정보보호 관리체계를 도입하여 실행하고 있지만 가장 기본이 되는 정보보호에 대한 인식의 부재, 획일화된 기준, 단편적인 평가 방식 등의 한계점을 가지고 있다. 또한 빠르게 발전하는 사이버 공격 기법 속도에 비해 정보보호 기술의 발전 속도는 현저히 느리고 공격위협의 성격이 지능화, 첨단화 되면서 위험노출 범위가 더욱 확대되고 있다.

현재 국정원 진단, 미래부 평가, K-ISMS 등 중복된 관리체계의 운용으로 인해 과도한 업무 중복으로 여러 가지 위험이 발생될 가능성에 노출되어 있다. 그 중 가장 시급한 문제는 국내 정보보호 관리체계 기준은 에너지 산업의 환경 및 업무의 특성을 고려하지 않고 실행되고 있다는 것이다. 이러한 문제점들은 향후 전력, 가스 등 국가주요기반시설에 대한 사이버 위협이 현실화 될 가능성을 높이고 있고 그로 인해 발생 가능한 많은 피해들이 예상된다. 본 연구는 에너지 산업 분야의 환경 및 특성을 고려하여 특화된 정보보호 관리체계를 수립하고 조직의 정보보호 수준을 평가할 수 있는 지수를 개발하는 것에 관한 방법을 제시하고 있다.

정보보호 관리체계 설립 시 사전준비, 통제기반/위험기반 측정 및 분석, 평가, 검토, 모니터링, 개선 과 같은 체계적인 프로세스를 기반으로 통제항목을 적용하여 위험을 감소시키고 투입비용대비 효과를 최적하며, 개발된 관리체계와 평가지수를 제도화하고 활성화 하여 발생 가능한 각종 위협에 대해 대비하고 위험대처 능력의 향상을 기대한다.

Ⅱ. 산업제어시스템(ICS)분석

2.1. 산업제어시스템(Industrial Control System)개요

2.1.1. ICS 정의

산업 제어 시스템(Industrial Control System)은 산업 분야 또는 주요 기반시설에서 사용하는 관리 제어 및 데이터 취득(SCADA)시스템, 분산 제어 시스템(DCS), 프로그래밍 가능한 논리 제어기(PLC) 등을 포함한 여

* 고려대학교 정보보호대학원 (crenius@korea.ac.kr)
** 고려대학교 정보보호연구원 (46sooyun@gmail.com)
*** 고려대학교 정보보호대학원 (kevinlee@korea.ac.kr)

러 제어 시스템 유형을 포괄하는 일반적인 용어다.

2.2. ICS분류 및 특성

ICS는 각 시스템의 구성과 기능에 따라 크게 다음과 같이 구분 된다.

2.2.1. SCADA

SCADA는 지리적으로 분산된 자산을 제어하는데 사용하는 시스템이다. 스카다 제어 센터는 원거리 통신 네트워크에 대한 제어를 수행하며 현장에 배치된 장치들의 밸브작동과 센서 시스템으로부터 정보수집, 지역 환경과 경보 상태를 모니터링하는 역할을 한다. 적용 분야로는 수도 공급, 폐기물 수집 시스템, 천연 가스 파이프라인, 전력 그리도, 철도 교통 등 다양하게 이용 된다.

2.2.2. DAS

DAS는 전기가 안정적으로 생산,공급 될 수 있도록 실시간으로 감시하거나 제어 및 계측하는 전력계통자동화시스템의 일부로 통신장치를 통해 배전설비의 현장정보(상태정보, 전류·전압, 고장유무 등)를 실시간으로 취득·모니터링하고 원격으로 제어함으로써 정전구간 축소 및 고장 정전시간을 단축할 수 있는 종합 시스템이다.

2.2.3. DCS

DCS는 산업 공정을 제어하는데 사용하고 하위 시스템과 결합된 장비들을 감독하고 제어하는 장비이다. 제품과 프로세스 제어는 제품 또는 프로세스 상태에 따라 피드백과 피드포워드 제어 반복을 통해 이루어진다. 적용 분야는 프로세스 기반 산업에 광범위하게 사용된다.

2.2.4. PLC

PLC는 산업 장비 또는 프로세스를 제어하는 컴퓨터 기반 반도체 회로 장치이다. 이는 제어 시스템 보조 컴포넌트이지만 소규모 제어 시스템 설정에서는 주요 컴포넌트 역할을 수행하고 거의 모든 산업 공정에 사용되는 장치이다.

2.3. 에너지 제어 시스템 특성 도출

산업 제어 시스템(ICS)의 목표는 성능, 신뢰성, 안정성, 유연성 보장이다. 하지만 기존의 ICS 보안은 단순히 네트워크와 시스템은 제어하는 콘솔을 물리적으로 보안하는 데 머물러 있었다. 이러한 한계를 극복하기 위해 ICS개발은 꾸준히 이루어졌으며 그로 인해 새로운 유형의 위협을 가져다주었고 시스템 침해 가능성을 높였다.

2.3.1. IT 시스템과 ICS

IT시스템과 ICS의 특성들은 에너지 제어 시스템에 맞는 관리체계를 구축하기 위해 알아 둘 필요가 있고 이 두 가지 특성을 비교함으로써 ICS에서 요구되는 보안 기준 및 통제 항목을 도출해야 한다. 기존 IT 시스템과 ICS의 차이는 다음 [표 1]과 같다.

〔표 1〕 IT시스템과 제어 시스템의 차이점〔4〕

분류	IT 시스템	제어시스템
성능 요구	비 실시간, 지속적 응답, 고속 처리량, 지연 및 지터 허용	실시간, 신속한 응답, 적당한 처리량 허용, 지연 및 지터는 불허
가용성 요구	재부팅 허용, 시스템 운영 요구사항에 따라 가용성 결함 허용	재부팅 불허용, 높은 가용성 요구, 여분의 시스템 필요, 계획된 가동 정지, 철저한 사전 배치 테스팅
위험 관리 요구	데이터 기밀성과 무결성이 가장 중요, 고장방지의 중요도 낮음(일시적인가동 중지 허용), 비즈니스 운영 지연이 최대 위험 요소임	인명의 안정성이 가장 중요, 고장방지 필수(일시적인 가동 중지 불허용), 규정의 불이행, 환경의 영향, 인명 및 장비 혹은 생산 능력의 손실이 최대위험
보안 구조	IT 자산 및 저장/전송되는 정보 보호, 중앙 서버 보안	제어장치와 PLC 같은 필드 장치 보호, 중앙 서버 보안
보안 솔루션	통상적인 IT시스템을 대상으로 설계	제어시스템 운영을 침해하지 않도록 보안 툴(of-line) 테스트 필요
시간 민감성	비상사태 시 상호작용에 덜 민감, 보안 정도에 따라 시스템에 대한 엄격한 접근 통제 적용 가능	비상사태 시 사람 혹은 다른 상호작용에 대한 대응이 매우 중요, 시스템에 대한 접근이 엄격히 규제되어야 함(그러나 HMI와 상호작용을 방해해서는 안됨)

분류	IT 시스템	제어시스템
시스템 운영	일반적인 운영체제 사용하도록 설계, 갱신은 자동화된 도구를 이용해 쉽게 가능	특화된 운영체제와 표준 운영체제 사용(흔히 보안 기능 결여), 소프트웨어 변경은 세심한 주의 필요 (보통 벤더에 의해 수행)
자원 제약성	보안 솔루션과 같은 제3자 어플리케이션의 추가를 지원하는 충분한 자원 이용가능	프로세스에 최적화된 설계로 보안 기능 추가를 위한 메모리 용량 및 컴퓨팅 자원 제한 존재
통신	표준 통신 프로토콜, 주로 지역 무선 기능을 가진 유선 네트워크 사용, 통상적인 IT 네트워크 기반으로 구축	많은 전용 및 표준 통신 프로토콜, 전용 유선 및 무선과 같은 다양한 형태의 매체 사용, 네트워크가 복잡하고 전력시스템에 대한 전문성 요구
변화 관리	소프트웨어 변경은 보안 정책 및 절차에 따라 주기적으로 진행(보통 자동화 도구 이용)	소프트웨어 변경은 제어 시스템의 무결성 보장을 위해 단계적으로 진행, 대부분 더 이상 지원되지 않는 OS 사용으로 패치 불가
관리 지원	다양한 지원형태 가능	보통 단일 벤더를 통해서만 가능
시스템 생명 주기	3~5년의 짧은 생명주기	15~20년의 긴 생명주기
컴포넌트 접근성	지역에 설치되고 접근용이	고립되어 있고 원격지에 설치되어 있어 접근이 어려움

ICS의 성능 요구사항은 개별 설치에 의해 받아들여진 지연 및 지터의 허용 수준에 대한 기준으로 실시간 응답은 시간임계적이고 보통 처리량은 높은 지연을 수용 가능하나 지터는 수용가능하지 않다. 또한 많은 ICS 프로세스들은 중복 시스템을 필요로 할 수 있고 정전은 사전에 일/주 단위로 계획, 예정되어야 하며 고가용성은 철저한 사전-배포 검사를 요구한다. 구성요소에 대한 재시작과 같은 응답은 프로세스 가용성 요구사항 때문에 허용 가능하지 않다. 위험관리 요구사항에서 사람의 안전은 프로세스의 보호에 이어서 무엇보다 중요하며 주요 위험 영향으로는 규제 미 준수, 환경적 영향, 제품, 장비 또는 생명의 손실 등이 있고 내고장성은 순간 정지시간이 허용되지 않더라도 필수적이다. 아키텍처 보안 초점의 주요 목표는 최종 클라이언트를 보호하는 것이고 중앙 서버의 보호 또한 중요하다. 의도하지 않은 결과가 나올 경우 보안도구는 보통의 ICS 운영에 방해가 되지 않음을 보장하는 검사를 받아야만 한다. 또한 사람과 그 응급 상호작용에 대한 응답이 중요한데 ICS에 대한 접근은 인간-기계 상호작용을 방해하거나 해를 입혀서는 안 된다. 시스템 운영에 있어서 소프트웨어 변화는 소프트웨어 벤더들에 의해 신중하게 이루어져야 하며, 보안 기능이 내장되어 있지 않은 경우도 있다.

또한 시스템은 특정 산업 프로세스를 지원하기 위해 설계되었고 보안 기능의 추가를 지원하기에 충분한 메모리 및 컴퓨팅 자원이 없을 수도 있다. 산업 제어 시스템의 통신은 독점적이고 기본적인 통신 프로토콜로 통신 매체의 여러 유형의 전용 유선 및 무선을 포함하여 사용되며 경우에 따라서는 제어 기술자들의 전문지식을 요구한다. 또한 소프트웨어 변경은 철저히 테스트되고 제어 시스템의 무결성이 유지되도록 시스템 전반에 점진적으로 배치되어야 한다. ICS정전은 자주(주 단위)로 계획되고 예정되어야 하며, 지원이 멈춘 OS를 사용할 수도 있다. 서비스 지원은 개인 벤더를 통해 이루어지며 구성요소의 생명주기는 보통 15년에서 20년 정도이고 구성요소들은 보통 고립되어 있어 관리가 어렵다.

반면 정보통신 시스템의 비-실시간 응답은 일관성을 가져야 하며 일반적으로 높은 처리율을 요구하고 일반적으로 지연과 지터의 얼마간의 수준에 저항 할 수 있다. 또한 재시작과 같은 응답은 허용가능하고 가용성 부족은 시스템의 운영 요구사항에 따라 허용될 수 있다. IT시스템에서는 데이터 기밀성과 무결성은 가장 중요하며 주요 위험 영향은 비즈니스 운영의 지연이다. 아키텍처 보안의 주요 초점은 IT자산의 동작을 보호하는 중앙 집중도는 분산 여부 및 정보를 저장하거나 자산 간에 전송하며 중앙 서버는 더 많은 보호를 요구할 수 있다. 보안 솔루션은 일반적인 IT시스템 전반에 설계되어 있고 IT 시스템에서는 환경과 물리적 상호작용이 없다. 또한 시스템은 일반 운영 시스템과 함께 사용하기 위해 설계되며 업그레이드는 자동화된 배포 도구로 가능하여 복잡하지 않다. 또한 타사 응용 프로그램의 추가를 지원하기에 충분한 자원을 지정하며, IT통신은 국소화된 무선기능을 가진 주요 유선 네트워크이다. 보안패치를 포함하는 IT 시스템에서의 소프트웨어 업데이트는 보안 정책과 절차를 기반으로 적용되는데 이러한 절차들은 서버 기반 도구를 사용함으로써 자동화 된다. 일반적인 IT시스템들은 상호 연결된 기술 아키텍처를 지원하거나 다양한 지원 스타일을 허용 할 수 있고 구성요소의

생명주기는 3년에서 5년 정도이며 구성요소들은 보통 지역적이고 접근이 용이하다.

Ⅲ. 에너지 특화 관리체계

에너지 특화 관리체계는 에너지 분야(전력, 가스 등) 기반시설의 특성을 반영한 발전된 정보보호 관리체계이다. 이는 에너지 제어시스템을 보유한 조직의 효과적인 보안 관리를 위한 평가체계로 크게 네 단계로 구성된다.

사전준비 단계에서 비즈니스/보안 요구사항 검토 및 정보보호의 범위를 정의한다. 이후 운영 단계에서 실직적인 평가가 에너지 기업의 특성이 맞추어 수행된다. 다음 검토 단계에서 평가 단계의 결과를 하나의 지수로 도출하여 조직의 보안 수준을 검토하고 모니터링 하게 된다. 마지막 개선 단계에서 위 결과를 토대로 개선의 수요를 조직에 반영하게 된다. 위 프로세스는 각 조직의 보안 관리에 대해 효율성과 효과성을 보장해 주는 것을 목표로 하며, 구체적인 수행내용은 다음과 같다.

〔그림 1〕 에너지 특화 관리체계 단계

3.1. 에너지 특화 관리체계: 준비

준비 단계에서는 현재 및 미래에 대한 비즈니스/보안 요구사항을 정의하고 문서화 하는 단계이다. 이는 비즈니스/보안 요구사항 검토를 통해 에너지 기업이 지향하는 보안 목표 및 목적을 파악하고 실무자의 요구사항을 파악하여 관리 범위를 정의함을 말한다.

3.1.1. 관리범위 정의 기준

정보보호 관리 범위는 비즈니스/보안 요구사항 검토를 통해 도출된 내용을 고려하여 설정한다. 정보보호 관리체계의 시작점으로 조직의 특성에 따라 다양한 형태를 가지게 된다. 또한 세부사항 주요 목적들에 대한 측정 가능한 기준을 포함하여야 한다. 이는 국제적으로 널리 사용되는 일반적인 고려기준[1]을 기반으로 대상 기관에 대한 현장 답사 및 실무자 인터뷰를 통하여 조직의 실정과 환경에 적합한 정보보호 관리 범위를 설정한다. 정보보호 관리 범위 설정 시 국제적으로 상용되는 일반적인 고려 기준은 다음과 같다.

〔표 2〕 정보보호 관리 범위 설정 시 고려사항

고려사항	세부내용
보안 사고의 영향과 손실 비용을 최소화	고객 서비스 제공 시간 지연
	직원의 도덕성, 생산성, 효율성 감소
	계약, 판매, 주문, 이익의 손실
	고객 손실
	신뢰와 자신감 손실
	자산 손실
	법적 제재
	운영 제어 능력 손실
보안 사고 발생 빈도 낮춤	인적 오류
	서비스 방해
	회사 자원의 잘못된 사용/남용
	절취, 사기 등 범죄
	기기 오작동, 시스템 실패, 시스템 다운 시간
법과 규제 준수 측면	유럽 연합에서 제시하는 데이터 프라이버시 지침
	미국에서 제시하는 샤베인스 옥슬리(SoX) 규제
	회사 조직이 속한 국가에서 요구하는 규제 및 지침 기준
서비스를 구분하는 시장 척도	데이터 복구, 미디어 저장과 같은 오프라인 서비스
	인터넷 뱅킹과 같은 온라인 서비스
고객과 비즈니스 파트너 관계	고객과의 계약적 의무 준수를 위해 고려해야 할 사항들
비즈니스 가치 강화	비즈니스 기회 및 투자를 극대화
	보안 위험에 대한 의사결정에 필요한 정보 제공
	위험 인지 ,관리, 정보 보안, 조직의 민감도와 주요 자산에 대한 효율적인 관리 방안
	정보 보안 위험 관리 문화 촉진
조직의 핵심 서비스	해당 조직의 목표와 결부된 서비스

3.1.2. 에너지 특화 관리체계 범위 설정

에너지 기업이 정보보호 관리체계 범위 설정 기준을

모두 준수해야 하는 것은 아니다. 하지만 반드시 고려해야 할 사항들은 따를 필요가 있다. 관리 범위에 포함하지 않을 경우 위험 평가 단계에서 결정된 보안 요구사항을 준수하는 것이 어려워 조직의 책임에 영향을 줄 수 있기 때문이다. ISO/IEC 27001 구현 지침서에서 필수적으로 포함해야 할 정보보호 관리 범위는 다음과 같다.

- 정보보호관리 운영에 참여하는 인원
- 업무 관리체계 내에서 사용되는 프로세스와 서비스
- 관리체계 수행에 필요한 정보 및 정보 시스템
- 관리체계 인터페이스와 연결 방법
- 관리체계를 위한 ICT 인프라 지원
- 관리체계의 물리적 위치

위 기준과 함께 에너지 제어시스템을 보유한 조직의 정보보호 관리 범위는 실시간 응답, 높은 가용성, 예측 가능성, 신뢰성 등의 특징을 포함한다. 즉 에너지 제어 시스템이 지원 할 수 없거나 각 에너지 기업이 보안상 추천하지 않는 항목에 대해서 관리 범위를 조정한다. 또한 관리 범위 조율 시 다음과 같이 에너지 기업에 요구되는 항목을 참고하여 수행한다.

- 공공의 건강과 안전에 대한 위험 최소화
- 환경에 대한 피해 최소화
- 국가 경제와 주요기능에 대한 생산성 중단, 감소의 방지
- 사이버 공격과 인적 위협으로부터 주요 기반시설을 보호

위 항목을 고려하여 에너지 제어시스템에 필수적으로 포함해야 할 정보보호 관리 범위는 다음과 같다.

- ICS 네트워크 및 네트워크 활동에 대한 논리적 접근 통제
- ICS 네트워크 및 장치에 대한 물리적 액세스 제한
- 모든 비인가 행위에 대한 모니터링
- 모든 조건(자연재해 등)으로부터 ICS의 기능 유지
- 사고 후 시스템 복원

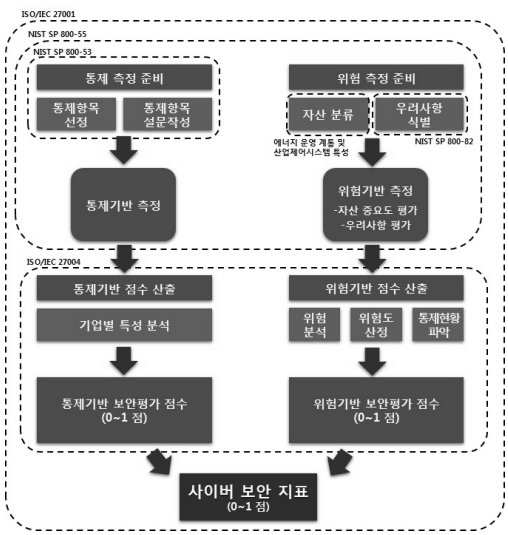
정의 된 범위 내에서 제시하는 항목에 대한 관리에 대해 각 기관은 동등한 보안 역량을 제공하지 못할 경우 그 이유에 대한 근거를 제공해야 한다.

3.2. 에너지 특화 관리체계: 운영

운영 단계는 실질적인 평가가 수행된다. 평가는 통제기반 측정 및 분석, 위험기반 측정 및 분석으로 나뉜다.[5] 통제 및 위험 기반 평가에서 측정된 결과는 사이버 보안 지표 점수로 환산되며, 다음과 같은 과정을 통해 산출된다.

통제기반 측정 및 분석은 조직의 보안 통제 수준을 측정하고 분석하는 단계를 의미한다. 크게 통제 측정 준비, 통제기반 측정, 통제기반 점수 산출, 통제항목 이행 현황 분석 과정으로 구성된다. 통제 측정 준비 단계에서는 조직의 특성에 맞는 통제 항목 선택과 실제 측정에 사용될 설문지 작성 등을 수행한다. 설문지 작성 시 사용되는 통제 항목은 미국국립표준기술연구소의 NIST SP 800-53를 참조한다. NIST SP 800-53은 정부 기관 정보 시스템을 보호하기 위한 보안 통제 항목 선택과 관련된 가이드라인을 제공한다. 이 문서에서 제공하는 산업 제어 시스템에 특화된 통제 항목들을 참조하여 구성하게 된다. 통제 기반 측정은 설문지를 배포하고 수집하는 단계를 의미한다. 회수된 설문지를 분석해 통제 기반 점수를 산출하고, 마지막으로 여러 가지 분석 방법을 통해 통제 항목 이행 현황 분석을 수행하게 된다.

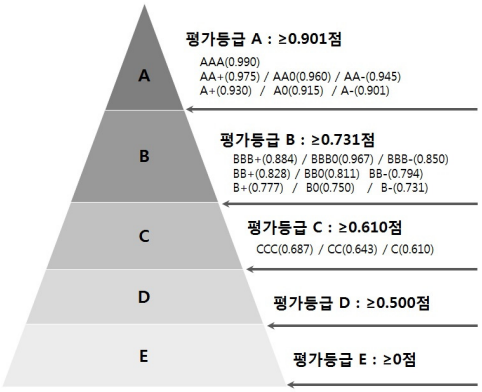
위험기반 측정 및 분석은 조직이 보유한 자산의 가치를 평가하고 해당 자산에 대한 위험을 식별해 현재 조



〔그림 2〕 사이버 보안 지표 산출

직이 처한 상황을 측정하고 분석하는 단계를 의미한다. 자산은 현황에서 언급한 SCADA, DAS, DCS 등의 장비로 분류 한다. 다음 위협, 취약성 평가는 분류된 자산의 취약점-위협 기반으로 위험도를 산출하는 일반적인 정보보호 관리체계와 달리 '우려사항'이라는 개념을 도입한다. 우려사항은 산업용 제어시스템의 보안 가이드 문서인 NIST SP 800-82가 제공하는 제어시스템 보안에 대한 위협의 식별 및 취약점 기준을 참조하여 도출한다. 이 우려사항은 단편적인 Yes / No 형식의 취약점 점검의 한계를 넘어서 해당 조직에서 실제로 발생 가능한 다양한 시나리오를 실무자가 직접 평가하고 고민해 볼 수 있는 시야를 갖게 해 준다.

산출된 통제기반 보안평가 점수와 위험기반 보안평가 점수는 0~1점 사이로 환산되며, 이는 사이버 보안 지표가 된다. 사이버 보안 지표는 다음과 같은 등급으로 나뉘며, 부여받은 등급은 조직의 현 보안수준을 의미한다.



〔그림 3〕 사이버 보안 등급표

3.3. 에너지 특화 관리체계: 검토

검토 단계는 기관에 맞게 구축하고 적용한 측정/평가 방법이 기관에 적절히 이용되도록 이끄는 데 목적이 있다. 단발성으로 측정하고 분석하는 것은 기관의 개별 자산 보안에 대한 투자적절성, 투자효율성을 특성에 맞게 정확히 파악했다고 보기 어렵다. 따라서 기관 전체 자산 보안에 대한 투자적절성 및 투자 효율성을 파악하기 위해서는 각 측정값 간의 관계를 파악하고, 이에 대한 피드백이 행해져야 한다. 이를 위해 보안 전문가와 각 자산을 담당하는 실무자의 평가 위원회를 구성하고, 의견을 수렴하여 산출된 사이버 보안 지표를 기반으로

〔표 3〕 ISO/IEC 27001에서 요구되는 필수 모니터링 항목〔1〕

번호	ISO/IEC 27001 요구사항에서 정의된 필수 모니터링 항목
1	효과성과 기능성에 대한 모니터링
2	변화에 대한 모니터링
3	위험과 업무 영향도, 정보보호 관리의 과정, 사고 조절 과정에 대한 모니터링
4	사람들 인식, 경쟁, 정보보호 관리체계의 활용에 관한 모니터링
5	ICT, 네트워크, 인터넷 사용, 웹 사이트에 대한 모니터링
6	제3자 서비스와 SLA에 대한 모니터링
7	기업 정책과 절차의 준수, 계약 의무, 법과 규제에 대한 모니터링

MBO, MBI를 셋팅한다. MBO, MBI는 현재 측정결과 및 전체적인 프로세스에 반영 가능하도록 해야 한다.

지속적인 개선을 통해 정보보호를 효과적으로 달성하기 위해서 적합한 모니터링이 필요하다. 일반적으로 ISO/IEC에서 요구하는 조직의 필수 모니터링 사항은 다음과 같다.

일반적인 기업과 에너지 기업의 환경은 차이가 존재한다. 따라서 에너지 기업에 필요한 주기적인 고려사항과 조치가 필요하다. 에너지 기업은 다음 항목들을 참고하여 에너지 특화 관리체계에 대한 주기적인 모니터링을 수행하고 체크해야 한다.

모니터링은 위 항목을 참조하여 모니터링 구축, 권고사항 확립과 대응방안 계획, 모니터링 수행과 문서작성, 후속조치의 총 네 단계를 거쳐 수행한다.

〔표 4〕 에너지 특화 관리체계에 대한 모니터링 항목

번호	에너지 특화 관리체계의 모니터링 항목
1	기관은 관리체계의 효과성을 위협, 취약성, 위험과 영향의 관점에서 모니터링 하고 있는가?
2	사업 확장, 다른 기술 도입 등 새로운 기업 요구사항의 측면에서 관리체계의 효과성을 모니터링하고 있는가?
3	조직은 비즈니스 프로세스에 연관시켜서 정보 보호의 효과성을 모니터링 하고 있는가?
4	조직은 직원들이 정보 보호와 관련된 업무 기능과 역할을 수행하는 데 있어서 효과적으로 수행하고 있는지 모니터링 하고 있는가?
5	조직은 사고 처리 과정의 효율성을 모니터링 하고 있는가?

3.4. 에너지 특화 관리체계: 개선

개선단계에서는 평가 위원회를 구성하고 이를 중심으로 에너지 특화 관리체계에 조직의 변화(조직 구조 및 인력 구조 개편, 신규 장비 도입, 정책의 변화 등) 및 개선사항을 재 반영하는 과정을 말한다. 평가 위원회는 사업부서, 주관부서, 시스템 운영부서, 관리책임자, 기업 내 최고의자결정권자, 외부 전문가 등으로 구성한다. 해당 인원은 정책 및 전략수립 지식, 기술 및 시스템 분석 지식, 위험평가 및 보안관련 지식, 운영 프로그램 및 사업계획에 대한 지식 등의 요건이 요구되며, 이때 해당 능력이나 경험이 있는 내부 직원의 존재 여부 등을 파악하여 자체적으로 평가 위원회를 구성 할 것인지 외부 인력을 활용할 것인지를 판단해야 한다. 또한 여러 부서와 연관되는 경우에는 별도의 외부 전문 기관이 대행하여 수행토록 해야 한다.

개선 수행 시 모든 절차의 내용과 결과를 문서화 하며, 잔존 위험이나 이해관계자 간의 의견충돌이 있는 경우에는 최고의사결정권자를 참여시킴으로 합의를 도출한다. 평가위원회는 보고서를 최종적으로 승인 할 수 있는 국가기관에 보고해야한다.

마지막으로 검증 결과에 따라 위험을 제거하기 위한 개선조치사항을 충실히 이행하고, 개선조치 사항의 이행 여부를 점검할 수 있는 별도의 내부 절차가 마련되어야 한다.

Ⅳ. 결 론

사이버 공격이 점차 고도화 되고 있는 가운데, 국내의 기존 정보보호 관리체계는 획일적이며, 단편적인 평가만을 수행하고 있다. 또한 국정원, 미래부 등 중복된 평가 수행으로 인해 과도 한 업무량이 부여되어 여러 가지 문제가 발생 가능하다. 이를 극복하기 위해 본 논문에서는 산업제어시스템 및 에너지 기업의 특성을 반영한 관리체계를 제안하였다. 이는 해당 조직이 속한 분야의 계통 특성을 고려해 정보보호를 수행 하는 것으로 에너지 기업 정보보호의 핵심인 연속성 확보, 침해사고 최소화, 조직 관리에 대한 비용 절감 등을 성취 가능하고 현재 일률적인 보안 준수를 목표로 하는 기존의 관리체계의 한계점을 극복 가능하다.

이 관리체계는 에너지 기업에 정착 후 장기적으로 항공, 철도, 해양 등 전반적인 국가 주요 기반시설에 대해서도 해당 기관의 특성을 고려한 실효성 있는 정보보호 관리체계 구축을 기대 할 수 있다.

참 고 문 헌

[1] International Organization for Standardization, ISO 27001 (2013).

[2] National Institute of Standards and Technology, NIST Special Publication 800-53 (2009).

[3] National Institute of Standards and Technology, NIST Special Publication 800-55 (2007).

[4] National Institute of Standards and Technology, NIST Special Publication 800-82 (2011).

[5] 양선웅, “에너지분야 사이버안전지표 구현에 대한 실증연구”, *고려대학교 정보보호대학원*, June 2013.

[6] WEISS, Joe. “Industrial Control System (ICS) Cyber Security for Water and Wastewater Systems”. In: *Securing Water and Wastewater Systems*. Springer International Publishing, pp. 87-105, 2014.

〈저 자 소 개〉

유 영 인 (Young in You)
정회원

2013년 8월 : 서울시립대학교 수학과 졸업
2013년 9월 ~ 현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 정보보호, 위험관리, ISMS

정 수 연 (Su Yun Jung)
비회원

2013년 2월 : 덕성여자대학교 식품영양학 졸업
2013년 9월~현재 : 고려대학교 정보보호 연구원
관심분야 : 정보보호

이 경 호 (Kyung Ho Lee)
종신회원

1989년 8월 : 서강대학교 수학과 학사
1997년 8월 : 서강대학교 정보통신대학원 석사 졸업
2009년 8월 : 고려대학교 정보보호대학원 박사 졸업
1994년 2월~현재 : 삼성그룹, nhn, 시큐베이스 등 근무
2011년 9월~현재 : 고려대학교 정보보호대학원 부교수
관심분야 : 정보보호, 위험관리, 정보보호컨설팅, 개인정보보호 정책