

실증단지 사이버 보안지침

제 1 장 총 칙

제1조 (목표) 본 지침은 제주 스마트 그리드 실증단지의 구축 및 운영에 관한 사이버 보안 확보를 목표로 한다.

제2조 (정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “기간시스템”이라 함은 한전과 전력거래소에서 실증단지 구축 이전부터 제주도 전력 공급을 위해서 운영되던 DAS¹⁾, EMS, CBP 등의 시스템을 말한다.
2. “사이버 공격”이라 함은 네트워크를 통해 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 해킹·웬바이러스 등 악성코드 유포·서비스방해·도청 등을 수행하는 행위를 말한다.
3. “사이버 보안”이라 함은 사이버 공격으로부터 실증단지 기기, 정보시스템, 정보통신망을 보호하기 위한 조치를 말한다.
4. “기기”라 함은 스마트그리드 실증단지에 설치되는 스마트미터(DCU 포함), 스마트가전(홈디스플레이 포함), 전기차, 전기차 충·방전장치, 정보수집 센서, 풍력·태양력 등 신재생 발전기기를 말한다.
5. “정보시스템”이라 함은 서버, PC 등 단말기, 보조기억매체, 네트워크 장치, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어와 소프트웨어를 말한다.
6. “정보통신망”이라 함은 유·무선, 광선, 위성 등을 매개로 하는 다양한 정보통신수단에 의하여 부호, 문자, 음향, 영상 등의 정보를 수집·가공·저장·검색·송수신하는 정보 전달체계를 말한다.
7. “기기 인증”이라 함은 정보시스템에 접근하는 기기가 사용이 허가된 기기임을 정보시스템이 확인하는 것을 말한다.
8. “컨소시엄 운영센터”라 함은 실증단지 내에서 Place, Transportation, Renewable, Power Grid 각 분야의 스마트그리드 기술 및 비즈니스 모델의 실증을 담당하는 곳을 말한다.
9. “통합보안 관제센터”라 함은 실증단지 내에서 침해사고, 취약점, 위협 정보

1) DAS : Distribution Automation System

등에 대한 관제·대응 및 조기 예·경보 발행 역할을 담당하며 통합운영센터에서 운영하는 곳을 말한다.

10. “실증단지 보안센터”라 함은 보안 취약점 분석, 사이버 모의훈련, 이기종 네트워크 정보보안대책 수립, 사이버 위기상황 대응체계 수립 등의 침해사고 대응 및 사이버보안 점검 활동을 담당하는 곳을 말한다.

제3조 (역할) 실증사업 관련 기관과 사업자의 제주 스마트그리드 실증단지내 사이버 보안 확보를 위한 역할은 다음 각 호와 같다.

1. 한국스마트그리드사업단은 제주 스마트그리드 실증사업을 총괄하며, 보안 전문가로 구성된 보안 워킹그룹을 운영한다.
2. 국가보안기술연구소는 제주 스마트그리드 실증단지에서 실증단지 보안센터를 운영하며, 사이버보안 점검 활동 등을 통해 스마트그리드 실증단지의 사이버 보안을 총괄한다.
3. 통합운영센터는 통합운영센터와 연계 구간에 대한 사이버 보안 대책을 수립·적용 한다.
4. 사업자는 컨소시엄 운영센터, 기기, 운영센터와 기기간 정보통신망 및 인터넷을 통한 실증 서비스 통신망에 대한 사이버 보안 대책을 수립·적용 한다.

제4조 (사이버 보안 활동) 통합운영센터와 각 컨소시엄 운영센터는 사이버 보안을 위하여 다음 각 호의 활동을 수행한다.

1. 사이버 보안 대책 수립 및 시행
2. 보안 취약성 분석
3. 실증단지 보안센터에서 수행하는 사이버보안 점검 지원

제5조 (사이버 보안 점검) ① 실증단지 보안센터는 스마트그리드 실증단지를 대상으로 연 1회 이상 다음 각 호의 사이버 보안 점검을 실시하고, 그 결과를 한국스마트그리드사업단에 통보 한다.

1. 보안 취약성 분석
 2. 모의훈련
 3. 실증단지 사이버 보안지침 준수 여부
- ② 실증단지 보안센터는 스마트그리드 실증단지내 모든 정보시스템, 정보통신망, 기기에 대해서 사이버보안 점검을 수행할 수 있다.

제6조 (정보보호제품 도입) 정보보호제품을 도입하고자 하는 사업자는 국가 정보보안기본지침에 의거 국제공통평가기준(CC)에 따라 인증된 정보보호제품 또는 국가용 암호제품으로 지정된 암호제품을 설치해야 한다. 단, 국제공통평가기준 또는 국가용 암호제품에 포함되지 않은 정보보호제품을 설치해야 하는 경우에는 국가정보원의 보안적합성 검증을 받아야 한다.

제 2 장 사이버 보안

제7조 (통합운영센터와 기간시스템 연계 구간 보호) ① 통합운영센터는 통합 운영센터와 연계되는 다음 각 호를 포함한 기간시스템 연계 구간에 대한 보안조치를 수행해야 한다.

1. 실증단지가 위치한 제주지역 전력거래소 EMS 등의 연계 구간
2. 실증단지가 위치한 제주지역 한전 송·변전시스템 연계 구간
3. 실증단지가 위치한 제주지역 한전 배전시스템 연계 구간

② 제1항에서 규정한 보안조치라 함은 다음 각 호를 의미한다.

1. 통합운영센터와 기간시스템과의 연결을 일원화하고, 접점에 침입차단시스템을 설치하여 통합운영센터로부터 기간시스템으로의 침입을 차단한다.
2. 망간의 연결에 있어 중간에 DMZ 구간을 설치 운영한다.

제8조 (정보통신망 보호) 통합운영센터와 컨소시엄 운영센터는 통합운영센터와 컨소시엄 운영센터간의 연결에 있어 다음 각 호의 사항을 포함한 보안조치를 수행해야 한다.

1. 송·수신 데이터의 위·변조를 방지하여야 한다.
2. 침입차단시스템을 설치하여 접근통제를 수행한다.
3. 침입탐지시스템 또는 침입방지시스템을 설치하여 유해트래픽의 탐지 또는 차단 기능을 수행한다.

제9조 (정보시스템 보호) 통합운영센터와 컨소시엄 운영센터는 사이버 공격으로부터 각각의 운영센터 정보시스템을 보호하기 위하여 다음 각 호의 사항을 포함한 보안조치를 수행해야 한다.

1. 정보시스템에 악성코드 탐지 소프트웨어를 설치·운영한다.
2. 정보시스템 운영체제 및 응용 소프트웨어의 보안패치 상태를 최신으로 유지한다.
3. 정보시스템 운영에 필요한 서비스 외에 불필요한 서비스는 제거한다.

4. 정보시스템에 접근하는 사용자에게 대해서 인증을 수행한다.

제10조 (컨소시엄 운영센터와 기기 연계 구간 보호) 각 컨소시엄은 실증을 위해 설치하는 스마트미터 또는 스마트미터의 모뎀, 전기충전기, 신재생 발전기기, 정보수집 센서 등을 포함한 기기 및 기기와의 통신을 보호하기 위한 기기 인증을 수행하고, 송·수신 메시지의 위·변조를 방지한다.

제 3 장 사이버 공격 대응 및 조치

제11조 (관제) ① 통합운영센터는 실증단지 내의 악의적인 사이버 공격을 모니터링 및 분석하고, 사고 대응을 수행할 수 있도록 통합보안관제를 수행해야 한다.

② 컨소시엄 운영센터는 컨소시엄에서 운영하는 기기, 정보통신망, 정보시스템에 대한 악의적인 사이버 공격을 모니터링 및 분석하고, 사고 대응을 수행할 수 있도록 보안관제를 수행할 수 있으며, 통합운영센터의 통합보안관제를 위한 체계를 지원해야 한다.

③ 제 1항과 제 2항에 의한 보안관제는 다음 각 호의 기능을 제공해야 한다.

1. 실증단지 내의 정보통신망 및 정보시스템 보안 설비의 이벤트 로그 등의 보안 로그를 수집 할 수 있다.

2. 보안 로그는 일정기간(6개월) 이상 저장 관리한다.

3. 수집된 보안 로그로부터 침해사고 및 이상행위를 실시간 탐지한다.

④ 통합운영센터와 각 컨소시엄 운영센터는 기기, 정보시스템 및 정보통신망에 대한 사이버 공격 인지시 피해실태를 파악하고 관련 로그자료를 보존하여야 하며, 필요시 정보시스템을 정보통신망과 분리하는 등의 초동조치를 취하여야 한다.

⑤ 통합운영센터와 각 컨소시엄 운영센터는 정보통신망 마비 또는 자료유출 등 중대사고 발생시에는 초동조치를 취하고, 즉시 실증단지 보안센터에 사고를 통보하여야 한다.

⑥ 실증단지 보안센터는 신고된 사이버 보안 사고에 대해 조사를 실시할 수 있으며, 재발방지를 위한 보안대책을 권고할 수 있다.

부 칙 (2010. 1. 1)

제1조 (다른 지침과의 관계) 본 지침에서 명시하지 않은 사항은 관련 법규에서

정하는 바에 따르며, 그 이외의 사항은 “스마트그리드 실증단지 보안가이드라인”을 참조하여 조치한다.

제2조 (보안가이드라인) “스마트그리드 실증단지 보안가이드라인”은 2010년 5월 31일까지 제정한다.

제3조 (사이버 보안 점검 시행일) 본 지침 제5조의 사이버 보안 점검은 제주 스마트그리드 실증단지가 구축되는 2011년1월 1일 이후부터 수행한다.