스마트그리드 실증단지
보안가이드라인

2010. 05.

국가보안기술연구소

목 차

1. 개요

1.1 목적

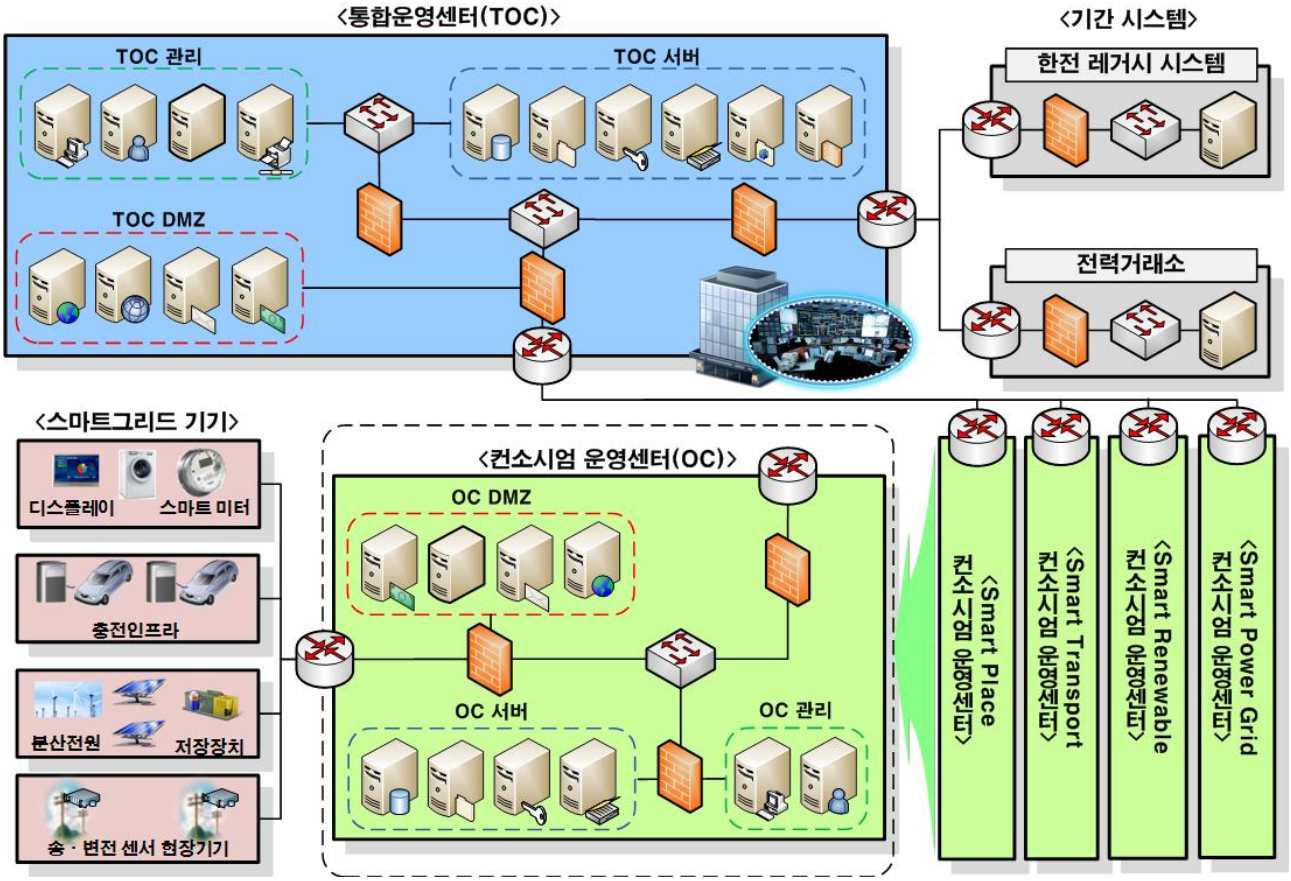
본 가이드라인은 스마트그리드 실증단지의 사이버 보안위협을 식별하고 이에 대한 보안대책을 제시하는 것을 목적으로 한다. 이를 통해, 스마트그리드 실증단지에 대한 사이버 보안위협을 최소화하여, 성공적 스마트그리드 실증단지 운영과 안전한 국가 스마트그리드 구축에 도움이 되고자 한다.

1.2 가이드라인 적용대상

본 가이드라인은 통합운영센터(TOC, Total Operation Center), 컨소시엄 운영센터(OC, Operation Center), 스마트그리드 기기 및 연계구간에 대한 사이버 보안위협과 보안대책을 제시한다.

연계구간에는 통합운영센터↔컨소시엄 운영센터, 통합운영센터↔기간시스템, 컨소시엄 운영센터↔스마트그리드 기기 구간 및 실증단지 외부 연계구간을 의미한다.

실증단지 외부 연계구간은 [그림 1]에 표시된 통합운영센터, 컨소시엄 운영센터, 스마트그리드 기기, 기간시스템 간의 연계구간을 제외한 연계구간을 의미한다.



[그림 1] 가이드라인 적용대상

1.3 가이드라인 구성

본 가이드라인의 구성은 다음과 같다.

- 1장은 가이드라인의 목적 및 적용대상에 대해 기술한다.
- 2장은 스마트그리드 실증단지의 사이버 보안위협에 대해 기술한다.
- 3장은 스마트그리드 실증단지의 사이버 보안대책에 대해 기술한다.

2. 보안위협

본 장에서는 통합운영센터, 컨소시엄 운영센터를 포함하는 운영센터와 스마트 그리드 기기를 대상으로 발생 가능한 사이버 보안위협들을 기술한다.

2.1 운영센터 보안위협

운영센터 내부 및 연계구간에서 발생가능한 보안위협에 대해 기술한다.

2.1.1 외부에서의 침입

2.1.1.1 공격자는 정보시스템의 원격접속서비스(Telnet, FTP, Web, RPC 등)의 계정을 추측하여 정보시스템에 침입할 수 있다.

2.1.1.2 공격자는 정보시스템의 원격접속서비스의 취약점을 이용하여 정보시스템에 침입할 수 있다.

2.1.1.3 공격자는 웹, 서버/클라이언트 응용프로그램 등의 응용프로그램 취약점을 이용하여 정보시스템에 침입할 수 있다.

2.1.1.4 공격자는 운영센터에서 운영하는 무선 네트워크의 인증을 우회하거나, 취약점을 이용하여 운영센터에 침입할 수 있다.

2.1.2 악성코드 감염

2.1.2.1 운영센터 내 정보시스템에서 인터넷을 사용할 경우 웹 브라우저, ActiveX 등의 취약점을 이용한 악성코드에 감염될 수 있다.

2.1.2.2 운영센터 내 정보시스템에서 수신한 전자메일의 악성 첨부파일 실행을 통해 악성코드에 감염될 수 있다.

2.1.2.3 악성코드에 감염된 USB 메모리 등의 보조기억매체를 정보시스템에서 이용할 경우 악성코드에 감염될 수 있다.

2.1.3 중요정보 유출

2.1.3.1 운영센터 내 DB 서버 등에 저장되는 전력운영정보 및 개인정보 등이 암호화되어 있지 않을 경우, DB 서버의 중요정보가 유출될 수 있다.

2.1.3.2 내부자가 정보시스템에 보조기억매체를 연결하여 중요정보를 유출할 수 있다.

2.1.3.3 내부자가 정보시스템의 정보를 프린터 등을 이용하여 출력물 형태로 중요정보를 유출할 수 있다.

2.1.3.4 공격자는 네트워크에 전송되는 패킷을 수집하여 중요정보를 획득·유출할 수 있다.

2.1.4 중요정보 변조·파괴

2.1.4.1 공격자가 정보시스템에 침투하여 중요정보를 변조·파괴할 수 있다.

2.1.4.2 공격자는 네트워크에 전송되는 데이터를 가로채고, 위·변조된 데이터를 전송할 수 있다.

2.1.5 침입 전이

2.1.5.1 공격자는 침입한 정보시스템을 거점으로 이용해 다른 정보시스템으로 침입할 수 있다.

2.1.5.2 하나의 정보시스템이 웜·바이러스에 감염될 경우 다른 정보시스템으로 감염이 전파될 수 있다.

2.1.6 불법 제어명령 전송

2.1.6.1 공격자는 제어명령을 위·변조하여 불법 제어명령을 스마트그리드 기기로 전송할 수 있다.

2.1.7 서비스 거부 공격

2.1.7.1 공격자는 다량의 트래픽을 발생, 다수의 접속시도, 취약점 등을 이용해 정보시스템 및 네트워크에 대한 서비스 거부 공격을 할 수 있다.

2.1.8 고출력 전자기파 공격

2.1.8.1 공격자는 운영센터에 고출력의 전자기파(EMP, Electromagnetic Pulse)를 방사하여 운영센터 내 정보시스템을 파괴할 수 있다.

2.2 스마트그리드 기기 보안위협

2.2.1 스마트그리드 기기 침입

2.2.1.1 공격자는 스마트그리드 기기가 가지고 있는 관리용 통신장치를 통해 패스워드를 추측하거나 응용프로그램 취약점을 이용하여 스마트그리드 기기에 침입할 수 있다.

2.2.1.2 공격자는 스마트그리드 기기가 가지고 있는 무선통신 장치를 통해 패스워드를 추측하거나 응용프로그램 취약점을 이용하여 스마트그리드 기기에 침입할 수 있다.

2.2.2 스마트그리드 기기 복제 및 변조

2.2.2.1 공격자는 다른 스마트그리드 기기의 식별자, 암호키, 인증 데이터 등의 보안 정보를 공격자의 기기에 저장하여 스마트그리드 기기를 복제할 수 있다.

2.2.2.2 공격자는 스마트그리드 기기에 저장된 정보를 변경하여 스마트그리드 기기를 변조할 수 있다.

2.2.3 스마트그리드 기기 위장

2.2.3.1 공격자는 복제되거나 변조된 스마트그리드 기기를 이용해 정상 스마트그리드 기기로 위장할 수 있다.

2.2.3.2 공격자는 정상 스마트그리드 기기로 위장하여 다른 스마트그리드 기기나 운영센터에 접근할 수 있다.

2.2.4 악성코드 감염

2.2.4.1 공격자는 원격으로 배포되는 소프트웨어를 변조하여 스마트그리드 기기에 악성코드를 설치할 수 있다.

2.2.5 중요 정보 유출

2.2.5.1 공격자는 스마트그리드 기기에서 송·수신되는 정보를 수집하여 중요 정보를 획득·유출할 수 있다.

2.2.5.2 공격자는 스마트그리드 기기에 접근하여 기기의 메모리 또는 저장 공간에서 중요 정보를 획득·유출할 수 있다.

2.2.6 중요 정보 변조·파괴

2.2.6.1 공격자는 스마트그리드 기기에 네트워크를 통해 침입하여 중요 정보를 변조·파괴할 수 있다.

2.2.6.2 공격자는 스마트그리드 기기에 물리적으로 접근하여 기기의 메모리 또는 저장 공간에 저장된 중요 정보를 변조·파괴할 수 있다.

2.2.6.3 공격자는 운영센터 및 다른 스마트그리드 기기로 위·변조된 정보를 전달할 수 있다.

2.2.7 재사용 공격을 통한 권한 획득

2.2.7.1 공격자는 획득한 정보를 재사용(Replay)하여 스마트그리드 기기 및 운영센터에 대한 접근권한을 획득할 수 있다.

2.2.8 침입 전이

2.2.8.1 공격자는 침입한 스마트그리드 기기를 거점으로 이용해 다른 스마트그리드 기기 또는 운영센터로 침입할 수 있다.

2.2.8.2 하나의 스마트그리드 기기가 웜·바이러스에 감염될 경우 다른 스마트그리드 기기로 감염이 전파될 수 있다.

3. 보안대책

본 장에서는 운영센터, 스마트그리드 기기에 대한 보안위협을 해결하기 위해 필요한 사이버 보안대책을 기술한다.

3.1 암호 알고리즘

인증, 무결성, 기밀성, 부인방지 서비스를 제공하기 위해 사용가능한 암호 알고리즘에 대해 기술한다.

3.1.1 권장 암호 알고리즘

국내·외에서 안전성이 입증된 암호 알고리즘은 다음과 같다.

3.1.1.1 국내표준 암호 알고리즘을 사용해야 하며, 필요한 경우 국제표준 암호 알고리즘을 사용할 수 있다.

<표 1> 권장 암호 알고리즘

대칭키 암호 알고리즘		ARIA, SEED, AES
해쉬함수		HAS-160, SHA-1/224/256/384/512
공개키 암호 알고리즘	인수분해 방식	RSA
	이산대수 방식	KCDSA, DSA, DH, MQV
	타원곡선 방식	EC-KCDSA, ECDSA, ECDH, ECMQV

3.1.1.2 대칭키 암호 알고리즘 보안강도는 128 비트 이상을 만족해야 하며, 공개키 암호 알고리즘 보안강도는 112 비트 이상을 만족해야 한다.

<표 2> 보안강도 128 bit인 알고리즘별 키 길이

보안강도	대칭키 암호 알고리즘	인수분해 방식	이산대수 방식		타원곡선방식
			공개키	개인키	
112 bits	-	2048 bits	2048 bits	224 bits	224-225 bits
128 bits	128 bits	3072 bits	3072 bits	256 bits	256-383 bits

* 출처 : NIST SP 800-57 'Recommendation for Key Management-Part 1'

3.2 인증 및 키관리

운영센터 내 정보시스템, 스마트그리드 기기 등의 통신 주체 간에 데이터 통신시 사용되는 인증 및 키관리에 대한 보안 요구사항을 기술한다.

3.2.1 인증

통신 주체 간 인증은 다음 사항을 만족해야 한다.

3.2.1.1 통신 주체 간에 인증 및 키 교환이 필요한 경우, 비밀키 또는 공개키 기반의 상호인증을 수행해야 한다.

3.2.1.2 비밀키 기반의 인증일 경우, 정보시스템 및 기기에 오프라인 또는 보안대책이 강구된 온라인 방식을 사용하여 사전공유비밀키(Pre-shared key)를 설정해야 하고, 사전공유비밀키를 인증 또는 데이터 무결성 및 기밀성 제공 용도로 직접 사용해서는 안 된다.

3.2.1.3 공개키 기반의 인증일 경우, 정보시스템 및 기기의 식별자와 공개키 매핑 일치 여부 확인이 가능해야 하고, 공개키 생성·변경·파기 등의 관리 수준은 인증서 관리의 보안 수준을 만족해야 한다.

3.2.1.4 정보시스템 및 기기의 공개키(인증서) 관리는 실증단지 내 공개키(인증서) 서버들을 통해서 이루어져야 한다.

3.2.1.5 사전공유비밀키 및 공개키(인증서)는 필요시 갱신할 수 있도록 해야 하며, 실증단지 사업 수행기간 동안 최소 1번의 갱신을 수행해야 한다.[1)]

3.2.2 키 교환 및 관리

통신 주체 간 상호 인증 수행 후, 데이터 보호를 위한 키 교환·분배를 위해 다음 사항을 준수해야 한다.

3.2.2.1 키 생성 시 안전한 난수발생기[2)]를 이용해야 한다.

---

1) 최대 2년까지 사용가능하나 실증단지 사업 기간 내에 인증서, 사전 공유키 교체 과정을 통해서 발생할 수 있는 문제를 조기에 파악하고 개선하기 위해 1년 마다 인증서 및 사전공유비밀키를 변경

2) 난수발생기에 대한 상세한 설명은 암호검증기준 (KS X ISO/IEC 19790)과 국정원 IT보안인증사무국 홈페이지 참조

3.2.2.2 키 교환·분배 과정을 위한 암호 알고리즘은 ‘3.1.1 권장 암호 알고리즘‘을 참조한다.

3.2.2.3 키 교환·분배 과정에서 키가 노출되지 않도록 암호화를 하거나 상호 교환되는 파라미터들이 위·변조되지 않도록 인증 기능을 제공해야 한다.

3.2.2.4 데이터 기밀성 및 무결성, 키 암호화 등을 위한 비밀키는 해쉬함수 등으로 별도의 서브키를 생성한 후 사용해야 하며, 주기적으로 변경 사용해야 한다.

3.2.2.5 키 사용 만료 시, 시스템 및 기기는 공격자가 키를 획득하여 재사용할 수 없도록 파기해야 한다.

3.3 관리적 보안

운영센터에서 사이버 보안을 위해 관리적으로 수행해야 하는 정보보호 체계, 인적 보안, 시설 보안 등에 대해 기술한다.

3.3.1 정보보호 체계

정보보호 업무 관리, 보안관제, 침해사고 대응, 보안 점검을 위하여 다음의 요구사항을 만족해야 한다.

3.3.1.1 운영센터는 정보보호 업무를 총괄하는 정보보호 담당자를 지정해야 한다.

3.3.1.2 운영센터는 관할 네트워크, 정보시스템 등에 대해 보안관제를 실시해야 한다.

3.3.1.3 운영센터는 침해사고 발생 시 원인 추적 및 보안수준 향상을 위한 자료로 이용하기 위해 시스템 및 서비스 로그를 6개월 이상 유지해야 한다.

3.3.1.4 운영센터는 침해사고 발생 시 대응하기 위한 침해사고 대응 절차서를 수립·시행해야 한다.

3.3.1.5 운영센터는 침해사고 발생 시 신속하게 대응하기 위해 비상연락체계를 수립 및 운영해야 한다.

3.3.1.6 운영센터는 침해사고 대응 및 복구 훈련 계획을 수립하고, 연 1회 이상 침해사고 대응 및 복구 모의훈련을 실시해야 한다.

3.3.1.7 운영센터는 연 1회 이상 자체 보안점검 계획을 수립하여 실시해야 한다.

3.3.2 인적 보안

네트워크, 정보시스템, 정보보호시스템에 대한 접근제한, 교육 및 외부 인력 관리를 위하여 다음 요구사항을 만족해야 한다.

3.3.2.1 네트워크, 정보시스템, 정보보호시스템의 관리자 및 사용자에 대한 접근권한 체계를 수립·시행해야 한다.

3.3.2.2 관리자 및 사용자에 대해 연 1회 이상의 정보보호 교육을 실시해야 한다.

3.3.2.3 운영센터의 상주 직원 외 외부 인력을 통한 시스템 개발, 설치, 운영, 정비 시 정보보호 교육을 수행해야 하고, 시스템에 대한 접근권한 제한 등의 보안 조치를 시행해야 한다.

3.3.3 시설(물리적) 보안

운영센터 시설보안을 위하여 다음 요구사항을 만족해야 한다.

3.3.3.1 운영센터는 물리적 보안 중요도에 따라 보호구역을 설정한다.

3.3.3.2 운영센터는 보호구역에 대해 인가받지 아니한 자의 출입을 제한할 수 있는 물리적 보안대책을 수립·시행해야 한다.

3.3.4 고출력 전자기파 보안

스마트그리드 실증단지 정보시스템에 대한 고출력 전자기파 공격에 대한 대책으로 다음 요구사항을 만족해야 한다.

3.3.4.1 운영센터는 정보시스템에 대한 고출력 전자기파 공격에 대처하기 위한 보안 대책을 수립·시행해야 한다.

3.3.5 보조기억매체 보안

보조기억매체 관리를 위하여 다음 요구사항을 만족해야 한다.

3.3.5.1 인가되지 않은 USB 및 보조기억매체가 정보시스템 또는 기기에 연결되는 것을 차단해야 한다.

3.3.5.2 운영센터 내 모든 정보기기의 CD, DVD 드라이브 등 ODD (Optical Disc Drive) 장비들에 대하여 기기등록을 수행하고, 인가 인원에 대해서만 사용을 허가해야 한다.

3.3.6 보안위해물품 관리

운영센터에서 반출·입되는 보안위해물품을 관리하기 위하여 다음 요구사항을 만족해야 한다.

3.3.6.1 운영센터 방문자에 대하여 노트북, USB 메모리, 카메라 등의 보안위해물품 소지 여부를 검사하고, 이에 대한 반출·입 제한을 수행해야 한다.

3.3.6.2 보안위해물품의 반출·입이 필요한 경우 물품 반출·입 신청서를 제출하고 반출·입 물품에 대한 보안검색을 수행해야 한다.

3.3.6.3 운영센터 내부에서 사진촬영을 하고자 할 때는 사진촬영 허가신청서를 보안 담당자에게 제출하여 보안 조치를 거쳐야 한다.

3.3.7 개인정보보호

운영센터에서 취급하는 개인정보를 보호하기 위하여 다음의 요구사항을 만족해야 한다.

3.3.7.1 운영센터에서 취급하는 개인정보를 보호하기 위하여 개인정보보호 관리 책임자를 지정해야 한다.

3.3.7.2 운영센터의 개인정보보호 관리 책임자는 분실, 도난, 누출, 변조로부터 개인정보를 보호하기 위한 기술적, 관리적 조치를 강구해야 한다.

3.4 운영센터 보안

운영센터의 안전한 구축과 운영을 위한 정보시스템, 네트워크, 정보보호시스템, 통신 보안 및 네트워크 연계구간 보안에 대해서 기술한다.

3.4.1 네트워크 구성

운영센터의 네트워크 구성은 다음 요구사항을 만족해야 한다.

3.4.1.1 운영센터는 인터넷과 연결된 망과 물리적으로 연결을 차단해야 한다.

3.4.1.2 Wi-Fi 등과 같은 무선 네트워크를 운영센터 네트워크로 구성하거나, 연결하는 것을 금지해야 한다.

3.4.1.3 운영센터 정보시스템들을 기능, 보안 중요도에 따라 서버영역, DMZ영역, 관리영역 등의 별도 서브넷으로 구성하여 접근제어를 수행해야 한다.

3.4.1.4 비인가 시스템, 악성코드 감염 시스템, 보안패치 및 업데이트 등의 보안 정책을 따르지 않는 시스템에 대하여 네트워크 연결과 사용을 제한해야 한다.

3.4.2 정보시스템 보안 관리

정보시스템의 계정, 패스워드 및 접근권한 관리를 위하여 다음 요구사항을 만족해야 한다.

3.4.2.1 정보시스템 운영에 필수적인 계정 이외의 계정은 삭제 또는 비활성화해야 한다.

3.4.2.2 시스템 사용자별로 독립적인 계정을 사용해야 한다.

3.4.2.3 사용자의 시스템 사용을 위해서는 계정, 패스워드 등을 이용한 안전한 로그인 절차를 수행해야 한다.

응용 시 유의사항 : 자리 이석시 보안대책으로 화면 보호기 및 화면 보호기 해제를 위한 패스워드를 설정해야 한다.

3.4.2.4 패스워드는 복잡도 및 사용기간 제한 등을 통하여 안전하게 관리해야 한다.

응용 시 권장사항 : 패스워드는 숫자/문자/특수문자를 조합하여 최소 8자리 이상으로 사용하고, 최소 90일 이내 1회 이상 변경한다.

3.4.2.5 정보시스템 자원(디렉토리, 프로세스 등)은 권한에 따라 사용자 접근을 제한해야 한다.

3.4.3 정보시스템 서비스 관리 및 접근제어

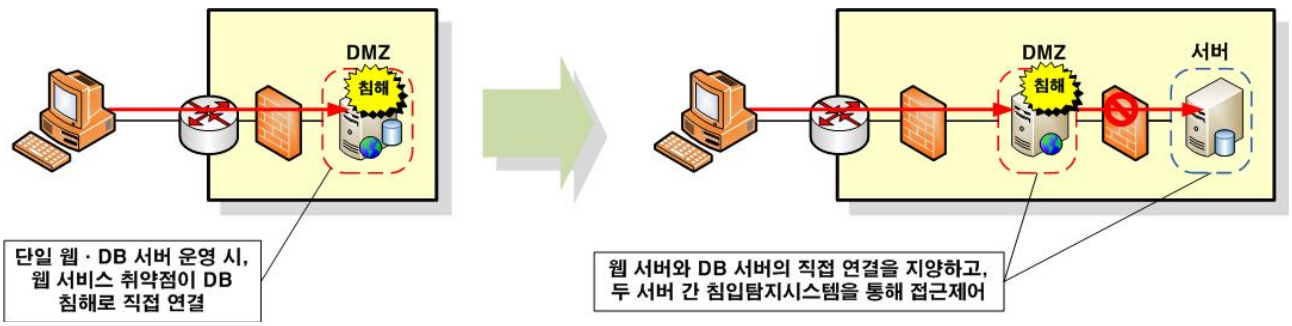
정보시스템 서비스, 웹, DB 관리를 위하여 다음 요구사항을 만족해야 한다.

3.4.3.1 시스템 운영과 관리에 필요하지 않은 서비스를 제거해야 한다.

<표 3> 불필요한 서비스 제거를 위한 업무 수행 절차

① 시스템에서 사용하는 모든 서비스 목록 작성 ② 해당 서비스가 시스템 운영에 필요한 서비스인지 검토 ③ 식별된 불필요한 서비스 제거 ④ 시스템 관리를 위해서 필요한 서비스는 최소 권한, 최소 시스템으로 제한 ⑤ 시스템 운영에 필요한 서비스는 암호화 등의 보안대책 적용

3.4.3.2 운영센터는 웹, DB 서버가 구동되는 시스템을 하드웨어적으로 분리하고, 운영에 필요한 경우 외에는 두 시스템 간 접근을 제한해야 한다.



[그림 2] 웹, DB 서버 분리를 통한 안전한 구성 예

3.4.3.3 웹 서비스 운영 시 웹 응용프로그램 취약점 공격에 대한 보안대책을 수립·시행해야 한다.

응용 시 권장사항 : 웹, WAS(Web Application Server)는 기존의 일반적인 침입차단시스템 외에 웹 응용프로그램 방화벽을 추가로 구성하여 보호할 수 있다.

3.4.3.4 서비스 운영시 사용되는 개인정보, 전력과금 등과 같은 중요 데이터는 암호화하여 DB에 저장해야 한다.

응용 시 유의사항 : DB 암호화시 '3.1.1 권장 암호 알고리즘'을 만족하여야 한다.

3.4.3.5 DB 운영 시 데이터 보호를 위한 DB 보안대책을 수립·시행해야 한다.

응용 시 권장사항 : 자료제공 및 데이터 연동을 위한 DB 계정은 DB 관리자 계정과 분리되어야 하며, DB 관리자 작업 기록, DB 생성·수정·삭제 등의 기록, DB 쿼리에 대한 로그기록을 6개월 이상 저장해야 한다.

3.4.3.6 정보시스템 내 서비스에 대한 접근을 최소한으로 제한하여야 한다.

응용 시 권장사항 : 서비스 이용이 필요한 대상 시스템에 한하여 통신을 허용해야 한다.

3.4.4 정보시스템 보안패치 및 백신

정보시스템의 보안패치 및 백신 업데이트는 다음의 요구사항을 만족해야 한다.

3.4.4.1 월 1회 이상 운영체제, 응용프로그램의 최신 보안패치 목록을 확인하고 보안패치를 수행해야 한다.

3.4.4.2 백신 프로그램을 설치하고, 주 1회 이상 최신 검사엔진으로 업데이트를 수행하여, 주기적으로 악성코드 감염 여부를 점검해야 한다.

3.4.4.3 보안패치 및 백신 업데이트는 인터넷과 연결되지 않은 실증단지 내부의 패치관리시스템(PMS), 백신업데이트시스템(VMS) 등을 이용하거나 오프라인으로 수행해야 한다."

3.4.5 네트워크 장비 보안 설정

네트워크 장비 취약점 제거 및 사고분석을 위하여 다음 요구사항을 만족해야 한다.

3.4.5.1 네트워크 장비를 최신 운영체제로 업데이트해야 한다.

3.4.5.2 기본으로 설정된 패스워드 및 배너를 변경해야 한다.

3.4.5.3 네트워크 장비 운영 및 관리에 필요하지 않은 서비스를 제거해야 한다.

3.4.5.4 침해사고 및 네트워크 장비 장애 시 정확한 사고분석을 위해 네트워크 장비의 시간을 동일하게 설정해야 한다.

3.4.6 정보보호시스템

정보보호시스템 설치, 탐지규칙 설정은 다음 요구사항을 만족해야 한다.

3.4.6.1 침입탐지시스템 및 침입방지시스템 탐지규칙은 월1회 이상 확인 및 점검해야 하며, 최신 업데이트를 유지해야 한다.

3.4.6.2 침입차단시스템의 정책 변경은 반드시 정보보호 관리자의 승인을 얻어 시행하고, 변경 기록을 관리해야 한다.

3.4.6.3 침입차단시스템 관리는 콘솔에서 직접관리 또는 지정된 IP 주소에서만 가능해야 하며, 관리자 로그인시 인증절차를 거쳐야 한다.

3.4.6.4 침입차단시스템의 침입차단 규칙은 모두 차단(All Deny)으로 설정하고 통신허용 대상에 대해서만 허용규칙을 설정해야 한다.

3.4.7 제어시스템

제어시스템 네트워크는 다음 요구사항을 만족해야 한다.

3.4.7.1 제어시스템이 설치된 네트워크는 다른 네트워크와 물리적으로 분리되어야 한다.

3.4.7.2 제어시스템 운영정보 활용을 위하여 부득이 다른 네트워크와 통신이 필요한 경우, 일방향 통신 방법을 사용해야 한다.

3.4.7.3 제어시스템과 원격감시·제어 대상과의 통신시 전용선을 사용하고 전용선을 사용하더라도 안전성이 보장되지 않을 경우 VPN 등을 적용하여 전송 데이터의 기밀성과 무결성을 보장해야 한다.

3.4.8 정보시스템 간 통신

통합운영센터, 컨소시엄 운영센터의 정보시스템이 다른 정보시스템과 통신 시 다음 요구사항을 만족해야 한다.

3.4.8.1 통합운영센터 내 정보시스템과 컨소시엄 운영센터 내 정보시스템 간 통신 시 응용프로그램 계층에서 종단 간(End-to-End) 암호화 통신을 수행해야 한다.

3.4.8.2 운영센터 내 정보시스템 간 통신시 중요정보(제어명령, 요금정보 등)의 경우 응용프로그램 계층에서 종단 간 기밀성 및 무결성을 제공해야 한다.

3.4.9 실증단지 외부 연계구간

실증단지 외부 연계구간 보안은 다음 요구사항을 만족해야 한다.

3.4.9.1 운영센터는 실증단지 외부 네트워크와 연계하지 않는 것을 원칙으로 한다.

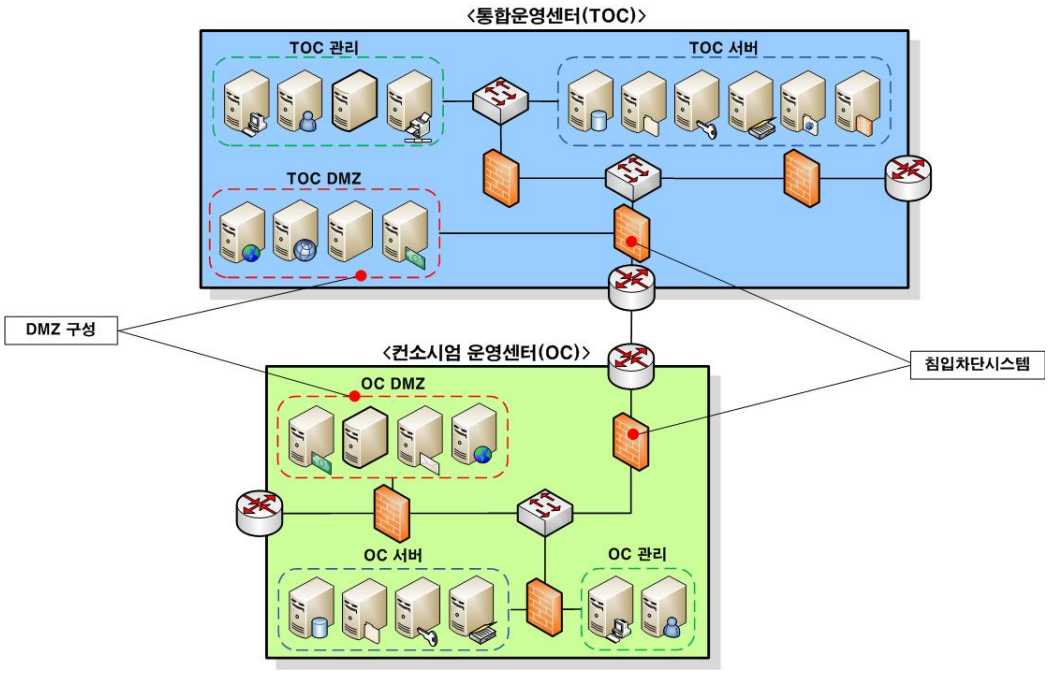
3.4.9.2 실증단지 운영정보 활용을 위하여 부득이 실증단지 외부 네트워크와 연계되어야 할 경우, 일방향 통신 방법을 사용해 외부 네트워크에서의 침입을 차단해야 한다.

3.4.10 통합운영센터와 컨소시엄 운영센터 연계구간

통합운영센터와 컨소시엄 운영센터 연계구간은 다음 요구사항을 만족해야 한다.

3.4.10.1 통합운영센터와 컨소시엄 운영센터 간 통신 시 외부의 침입을 차단할 수 있는 전용선, VPN 등을 사용해야 한다.

3.4.10.2 통합운영센터와 컨소시엄 운영센터 간 연계 시 침입차단시스템을 이용하여 DMZ를 구성한 후 중계서버를 이용하여 통신해야 한다.



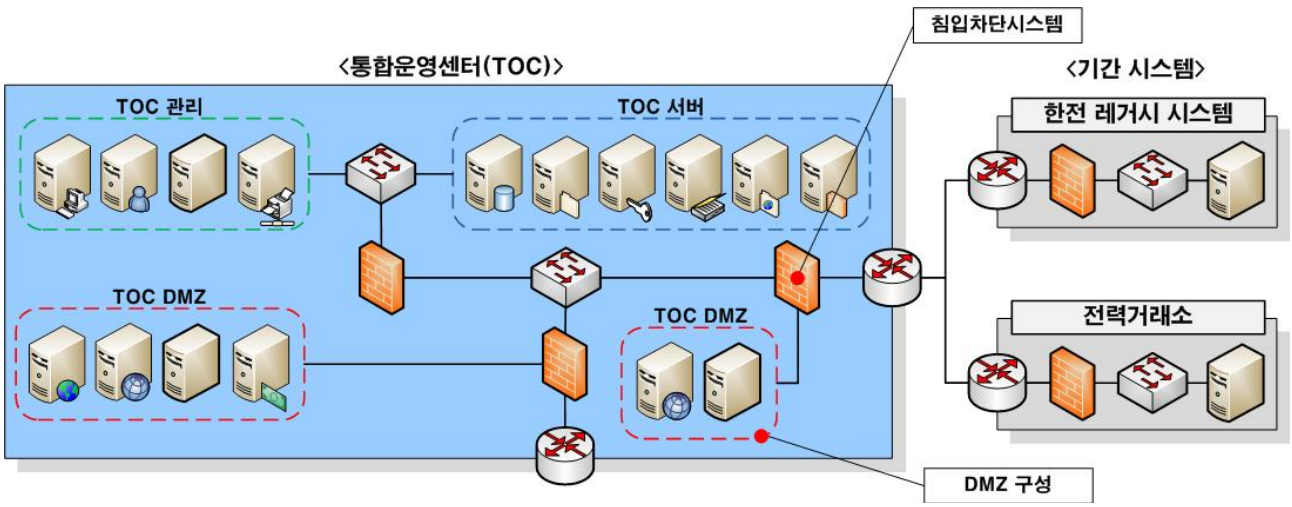
[그림 3] 운영센터 연계구간 침입차단시스템 및 DMZ 구성

3.4.11 통합운영센터와 기간시스템 연계구간

통합운영센터와 기간시스템 연계구간은 다음 요구사항을 만족해야 한다.

3.4.11.1 통합운영센터와 기간시스템 간 통신 시 외부에서의 침입을 차단하기 위하여 전용선, VPN 등의 통신 수단을 사용해야 한다.

3.4.11.2 통합운영센터와 기간시스템 간 연계 시 침입차단시스템을 이용하여 DMZ를 구성한 후 중계서버를 이용하여 통신해야 한다.



[그림 4] 통합운영센터와 기간시스템 연계구간 침입차단시스템 및 DMZ 구성

3.4.12 컨소시엄 운영센터와 스마트그리드 기기 연계구간

컨소시엄 운영센터와 스마트그리드 기기 연계구간은 다음 요구사항을 만족해야 한다.

3.4.12.1 스마트그리드 기기 설치 시 컨소시엄 운영센터에서 인증을 수행하여야 한다.

3.4.12.2 컨소시엄 운영센터 또는 데이터 수집장치에서 기기에 대한 네트워크 접근제어를 수행해야 한다.

3.4.12.3 컨소시엄 운영센터와 기기 간 연계 시 침입차단시스템을 이용하여 DMZ를 구성한 후 중계서버를 이용하여 통신해야 한다.

3.4.12.4 컨소시엄 운영센터와 기기 간에 전달되는 전력 및 개인 정보 등의 중요 데이터를 암호화해야 한다.

3.5 스마트그리드 기기 보안

스마트그리드 기기를 보안위협으로부터 보호하기위한 보안대책에 대해 기술한다.

3.5.1 암호 지원

스마트그리드 기기에 사용되는 암호화모듈은 다음의 요구사항을 만족해야 한다.

3.5.1.1 스마트그리드 기기에 저장되는 정보는 동일한 평문에 대해 동일한 암호문이 생성되지 않도록 한다.

3.5.2 암호 통신

스마트그리드 기기 간 및 스마트그리드 기기와 운영센터 간 안전한 데이터 전송을 위해 다음 요구사항을 만족해야 한다.

3.5.2.1 물리적으로 분리된 스마트그리드 기기 간 전송되는 데이터는 무결성 및 기밀성이 보장되어야 한다.

3.5.2.2 물리적으로 분리된 스마트그리드 기기와 운영센터 간 전송되는 데이터는 무결성 및 기밀성이 보장되어야 한다.

3.5.3 스마트그리드 기기 내 데이터 저장 및 보호

스마트그리드 기기에 저장되는 데이터의 보호를 위해서 다음 요구사항을 만족해야 한다.

3.5.3.1 서비스 제공을 위해 필요한 최소 정보만 기기 내 저장하며, 서비스 제공을 위해 필요한 기간 동안만 저장되어야 한다.
3.5.3.2 스마트그리드 기기에 저장되는 중요 정보는 안전성이 확인된 암호모듈[1]을 통해 암·복호화 되어야 한다.
3.5.3.3 인증 및 암·복호화 모듈에 사용되는 기기 비밀번호 또는 패스워드는 해시 알고리즘을 사용하여 보호해야 한다.

3.5.4 스마트그리드 기기 식별 및 인증

인가된 스마트그리드 기기의 식별 및 인증을 위해서는 다음 요구사항을 만족해야 한다.

3.5.4.1 기기 설치 및 네트워크 등록 시 운영센터와 스마트그리드 기기 간 상호 인증이 가능해야 한다.
3.5.4.2 네트워크 운영 주체는 정상적으로 등록된 안전한 스마트그리드 기기를 식별할 수 있어야 한다.
3.5.4.3 인증 데이터의 재사용 공격을 방지해야 한다.

1) 국가정보원에서 시행 중인 암호검증 절차를 마친 검증필 암호모듈을 의미한다.

3.5.5 네트워크 접근통제

안전하지 않은 기기의 실증단지 네트워크 접근을 막기 위해서는 다음 요구사항을 만족해야 한다.

3.5.5.1 운영센터에 의해 인증을 마친 기기에 한해서 네트워크 가입, 통신 연결, 데이터 전송 등을 허락해야 한다.
3.5.5.2 실증단지 네트워크에 대한 기기 접근통제는 기기 식별자, 기기 주소, 목적지 주소 등의 조건별로 제한할 수 있어야 한다.

3.5.6 스마트그리드 기기 접근통제

암호화된 정보, 암호키 등 스마트그리드 기기에 저장된 중요 데이터에 대한 권한이 없는 사용자에 대한 접근을 통제하기 위해서는 다음 요구사항을 만족해야 한다.

3.5.6.1 기기 유·무선 로컬 인터페이스를 통한 원격 접근 또는 현장에서의 물리적 접근 시 사용자를 인증해야 한다.
3.5.6.2 사용자의 스마트그리드 기기에 대한 접근통제는 기기 관리 목적, 사용자 권한 등의 조건별로 제한할 수 있어야 한다.
3.5.6.3 현장 관리요원이 기기 유지·보수장비를 분실한 경우 운영센터는 해당 장비의 스마트그리드 기기 접근을 즉시 차단할 수 있어야 한다.

3.5.7 스마트그리드 기기 펌웨어 및 소프트웨어 설치 보안

스마트그리드 기기의 안전성 유지를 위한 펌웨어 및 소프트웨어 설치 시 보안 위협을 차단하기 위해 다음의 요구사항을 만족해야 한다.

3.5.7.1 기기 취약점이 노출된 경우, 취약점을 제거하기 위한 펌웨어 및 소프트웨어 업데이트를 실시해야 한다.
3.5.7.2 기기 펌웨어 및 소프트웨어는 설치(업데이트) 이전에 반드시 기능과 보안성이 검증되어야 한다.

3.5.7.3 악의적인 펌웨어 및 소프트웨어 설치(업데이트)를 무결성 보장, 인증, 접근제어 등을 통해 방지할 수 있어야 한다.

3.5.8 스마트그리드 기기 복제 방지

스마트그리드 기기를 불법 복제 후 정상 기기처럼 네트워크에서 동작하는 것을 차단하기 위해 다음의 요구사항을 만족해야 한다.

3.5.8.1 기기의 고유 식별자, 인증, 암호 등 관련 중요정보에 대한 복제 방지 대책을 수립해야 한다.

3.5.9 스마트그리드 기기와 외부 네트워크 연결 차단

네트워크 및 다른 기기를 통한 스마트그리드 기기 침입 및 정보유출을 차단하기 위해 다음의 요구사항을 만족해야 한다.

3.5.9.1 스마트그리드 기기는 실증단지 외부에 존재하는 기기 및 네트워크와 연계하지 않는 것을 원칙으로 한다.

3.5.9.2 실증 목적상 필요에 의해 스마트그리드 기기가 외부와 연계될 경우 침입을 차단할 수 있도록 별도의 보안 대책을 강구해야 한다.