실증단지 보안 취약성 점검 리스트

번호	문항	배점	점검(해당항목에 V표)

1. 관리적 보안

<1.1 정보보안 담당조직>

	1.1.1 운영센터는 시스템 및 네트워크 보안을 담당하기 위한 조직을 운영하는가	배점	점검(해당항목에 V표)
1	1 정보보호 업무를 담당하는 조직이 있으며, 담당자가 상주한다	3	
	2. 정보보호 업무와 실증단지 운영을 함께하는 담당자가 상주한다	2	
	3. 정보보호 업무를 원격으로 수행하는 보안 담당자가 있다	1	
	4. 정보보호 업무 담당자가 없다	0	
	증빙자료 : 정보보호 업무 조직도, 보안업무 담당자 지정 근거서류 등		

<1.2 침해사고 대응체계 수립>

	1.2.1 침해사고 대응과 관련한 절차서를 수립하였는가	배점	점검(해당항목에 V표)
2	1. 침해사고 대응 절차서를 수립하였으며, 관련 조직을 운영하고 년 1회 갱신한다	3	
	2. 침해사고 대응 절차서를 수립하였으며, 관련 조직을 운영한다	2	
	3. 침해사고 대응 절차서를 수립하였다	1	
	4. 해당 절차서가 없다	0	
	증빙자료 : 침해사고 대응 절차서, 정보보호 업무 조직도, 침해사고 대응 절차서 갱신 내역서 등		

	1.2.2 운영센터 침해사고 발생시 신속한 대응을 위해 비상연락체계를 수립하였는가	배점	점검(해당항목에 V표)
3	1. 비상연락체계를 수립하였다	3	
	2. 비상연락체계를 수립하지 않았다	0	
	증빙자료 : 비상연락체계도		

	1.2.3 침해사고 대응 및 복구 훈련 계획을 수립하고 시행하는가	배점	점검(해당항목에 V표)
4	1. 침해사고 대응 및 복구 훈련 계획을 수립하였으며, 년 1회 시행한다	3	
	2. 침해사고 대응 및 복구 훈련 계획을 수립하였다	1.5	
	3. 침해사고 대응 및 복구 훈련 계획을 수립하지 않았다	0	
	증빙자료 : 침해사고 대응 및 복구 훈련 계획서, 훈련 시행 근거 서류 등		

	1.2.4 자체 보안점검 계획을 수립하고 시행하는가	배점	점검(해당항목에 V표)
5	1. 자체 보안점검 계획을 수립하였으며, 년 1회 시행한다	3	
	2. 자체 보안점검 계획을 수립하였다	1.5	
	3. 자체 보안점검 계획을 수립하지 않았다	0	
	증빙자료 : 보안점검 계획서, 보안점검 수행 내역기록 등		

	1.2.5 주기적인 보안 취약성 분석을 수행하는가	배점	점검(해당항목에 V표)
6	1. 년 1회 보안 취약성 분석을 수행하고, 결과에 따라 적절한 조치 적용 후 이행 점검을 수행한다	3	
	2. 년 1회 보안 취약성 분석 후 결과에 따른 적절한 조치를 적용한다	2	
	3. 년 1회 보안 취약성을 분석한다	1	
	4. 보안 취약성 분석을 수행하지 않는다	0	
	증빙자료 : 취약성 분석 계획서, 이행 점검표, 취약성 분석 결과 보고서 등		

<1.3 정보보안 교육>

	1.3.1 네트워크·시스템 관리자 및 사용자에 대해 정보보호 교육을 실시하는가	배점	점검(해당항목에 V표)
7	1. 정보보호담당자에 대해서 정보보호 전문교육을 연 1회 이상 실시하며, 관리자 및 사용자에 대한 정보보호 교육을 연 1회 이상 실시한다	3	
	2. 정보보호담당자에 대해서 정보보호 전문교육을 연 1회 이상 실시한다	2	
	3. 이메일, 게시판 등을 이용한 정보보호 제고 교육을 연 1회 이상 실시한다	1	
	4. 정보보호 교육을 수행하지 않는다	0	
	증빙자료 : 정보보호 교육 계획 및 관련 근거서류 등		

<1.4 보안관제>

	1.4.1 운영센터는 관할 네트워크 및 정보시스템에 대한 보안관제를 실시하는가	배점	점검(해당항목에 V표)
8	1. 보안 로그 수집 및 실시간 모니터링을 수행하고 지속적인 히스토리(history)를 관리한다	3	
	2. 보안 로그 수집, 보안 이벤트 관련 경보 발생시에만 담당자가 해당 경보를 확인한다	2	
	3. 수집된 보안 로그를 통합보안관제 센터로 전송한다	1	
	4. 보안관제를 수행하지 않는다	0	
	5. 해당없다	평가제외	
	증빙자료 : 보안로그, 히스토리 기록, 보안관제 구성도 등		

	1.4.2 정보시스템, 정보보호시스템, 네트워크 장비 등의 보안 로그를 저장하는가	배점	점검(해당항목에 V표)
9	1. 시스템 및 서비스 로그를 6개월 이상 저장한다	3	
	2. 시스템 및 서비스 로그를 3개월 이상 저장한다	2	
	3. 시스템 및 서비스 로그를 3개월 미만 저장한다	1	
	4. 저장하지 않는다	0	
	증빙자료 : 정보시스템, 정보보호시스템, 네트워크 장비 및 로그 서버에 기록된 로그 등		

<1.5 보안위해물품>

	1.5.1 보안위해물품 관리를 수행하는가	배점	점검(해당항목에 V표)
10	1. 방문자 및 내부자 모두에 대해서 보안위해물품 반출입 신청절차를 통해 보안위해물품을 관리한다	3	
	2. 방문자에 대해서만 보안위해물품 반출입 신청절차를 통해 보안위해물품을 관리한다	1.5	
	3. 보안위해물품 관리 보안대책이 없다	0	
	증빙자료 : 보안위해물품 반출입 신청서(실 기록내역) 등		

	1.5.2 USB 및 보조기억매체 보안대책을 수립하고 시행하는가	배점	점검(해당항목에 V표)
11	1. USB 및 보조기억매체 사용을 금지한다	3	
	2. 관리대장 및 솔루션을 통해 지정된 시스템에서만 인가된 USB 및 보조기억매체 사용을 허가한다	2	
	3. 관리대장 및 솔루션을 통해 인가된 USB 및 보조기억매체 사용을 허가한다	1	
	4. 보안대책이 마련되어 있지 않다	0	
	증빙자료 : 보조기억매체 관리지침, USB 및 보조기억매체 관리 솔루션 도입현황, USB 및 보조기억매체 관리대장 등		

	1.5.3 ODD 장비 사용제한을 시행하는가	배점	점검(해당항목에 V표)
	1. 모든 ODD 장비를 목록화 하여 관리하고, 지정된 기기에 대해서만 쓰기를 허용한다	3	
	2. ODD 장비 사용제한이 마련되어 있지 않다	0	
12			
	증빙자료 : 보조기억매체 관리지침, ODD 장비 목록, ODD 보안대책 계획서 등		

<1.6 개인정보보호>

	1.6.1 개인정보보호를 위한 보안대책이 마련되어 있는가	배점	점검(해당항목에 V표)
	1. 개인정보보호 관리 책임자를 지정하고, 개인정보보호를 위한 개인정보 암호화, 사용자 동의서 등의 보안대책이 마련되어있다	3	
	2. 개인정보보호를 위한 개인정보 암호화, 사용자 동의서 등의 보안대책이 마련되어 있다	1.5	
13	3. 개인정보보호 대책이 마련되어 있지 않다	0	
	4. 해당없다	평가제외	
	증빙자료 : 개인정보보호 관리 책임자 지정 내역, 개인정보보호 암호화 및 사용자 동의서, 기타 개인정보 보호대책 근거 서류 등		

<1.7 시설보호>

	1.7.1 운영센터 내 중요 시설에 대해 보호구역을 지정하고 관리하는가	배점	점검(해당항목에 V표)
	1. 중요 시설에 대해 보호구역(중요, 일반구역)으로 지정하고, 출입 제한 조치를 적용하여 관리한다	3	
	2. 중요 시설에 대해 보호구역(중요, 일반구역)으로만 지정하여 관리한다	1.5	
14	3. 중요 시설에 대한 보호조치가 없다	0	
	증빙자료 : 보호구역 지정서, 보호구역 표지 부착, 보호구역 보호대책 현황 등		

<1.8 전자기파 보호>

	1.8.1 고출력 전자기파 공격에 대처하기 위한 보안대책을 수립하고 시행하는가	배점	점검(해당항목에 V표)
	1. 고출력 전자기파 공격을 막기 위한 보안대책을 수립하고 시행한다	3	
	2. 고출력 전자기파 공격에 대한 보안대책이 마련되어 있지 않다	0	
15			
	증빙자료 : 고출력 전자기파 보안대책 등		

2. 운영센터 보안

<2.1 계정관리>

	2.1.1 정보시스템의 사용자 계정을 관리하는가	배점	점검(해당항목에 V표)
16	1. 정보시스템 운영에 불필요한 계정은 삭제 또는 비활성화하며, 사용자별 독립 계정을 설정하여 사용한다	3	
	2. 정보시스템 운영 필수 계정을 여러 사용자가 함께 사용한다	1.5	
	3. 정보시스템 사용자 계정 관리가 이루어지지 않고 있다	0	
	증빙자료 : 정보시스템 목록 및 네트워크 구성도, 정보시스템 계정 운영 절차, 계정 리스트(계정 별 발급 목적 명시) 등		

	2.1.2 정보시스템에 대한 로그인 절차를 사용하는가	배점	점검(해당항목에 V표)
17	1. 계정, 패스워드를 이용한 로그인 절차를 사용하고, 이석시 자동로그아웃 기능이 활성화 되어 있다	3	
	2. 계정, 패스워드를 이용한 로그인 절차만을 사용한다	1.5	
	3. 정보시스템에 대한 로그인 절차가 없다	0	
	증빙자료 : 정보시스템 목록 및 네트워크 구성도, 점검시 정보시스템 로그인 절차, 자동로그아웃 설정 등 점검		

	2.1.3 안전한 패스워드를 사용하는가	배점	점검(해당항목에 V표)
18	1. 숫자, 문자, 특수문자를 조합하여 최소 8자 이상으로 사용하며, 90일 이내 1회 이상 변경 사용한다	3	
	2. 숫자, 문자, 특수문자를 조합하여 최소 8자 이상으로 사용한다	2	
	3. 숫자, 문자를 조합하여 8자 이상으로 사용하되, 유추할 수 없는 문자 및 숫자를 사용한다	1	
	4. 기관명, 생일 등 유추 가능한 문자 및 숫자 사용, 짧은 패스워드 사용 등을 사용한다	0	
	증빙자료 : 정보시스템 목록 및 네트워크 구성도, 패스워드 정책, 시스템 패스워드 정책 설정 및 패스워드 직접 점검 수행		

<2.2 정보시스템>

	2.2.1 정보시스템 보호를 위하여 보안패치 및 백신 업데이트를 주기적으로 수행하는가	배점	점검(해당항목에 V표)
19	1. 월 1회 이상 보안패치 목록 확인 및 보안패치를 수행하며, 주기적인 백신 업데이트를 수행한다	3	
	2. 보안패치 및 백신 업데이트를 수행한다	1.5	
	3. 보안패치 및 백신 업데이트가 이루어지지 않고 있다	0	
	증빙자료 : 정보시스템 목록 및 네트워크 구성도, 점검시 보안패치, 백신 엔진의 최신 업데이트 여부 점검		

	2.2.2 백신 프로그램을 이용하여 주기적으로 악성코드 검사를 실행하는가	배점	점검(해당항목에 V표)
20	1. 백신 프로그램의 실시간 검사기능을 활용하며, 주 1회 이상 악성코드를 주기적으로 검사한다	3	
	2. 주 1회 이상 주기적으로 악성코드를 검사한다	2	
	3. 비정기적으로 악성코드를 검사한다	1	
	4. 악성코드를 검사하지 않는다	0	
	증빙자료 : 정보시스템 목록 및 네트워크 구성도, 백신 프로그램의 점검 기록, 실시간 감시 설정 여부		

	2.2.3 보안패치 및 백신 업데이트를 안전하게 수행하는가	배점	점검(해당항목에 V표)
21	1. 인터넷과 연결되지 않은 실증단지 내부에 패치관리시스템 또는 백신업데이트 시스템을 운영하여 사용한다	3	
	2. 오프라인으로 보안패치 및 백신업데이트를 수행한다	2	
	3. 인터넷과 연계하여 보안패치 및 백신 업데이트를 수행한다	1	
	4. 보안패치 및 백신 업데이트를 수행하지 않는다	0	
	증빙자료 : 정보시스템 목록 및 네트워크 구성도, 보안패치 및 백신 업데이트 수행 방안, 보안패치 서버 및 백신 업데이트 서버 구성도 등		

<2.3 정보보호시스템>

	2.3.1 침입탐지시스템 및 침입방지시스템 탐지 규칙을 관리하는가	배점	점검(해당항목에 V표)
22	1. 최신 탐지 규칙을 유지한다	3	
	2. 최신 탐지 규칙을 유지하지 않는다	0	
	증빙자료 : 정보보호시스템 목록 및 네트워크 구성도, 침입탐지시스템, 침입방지시스템의 탐지규칙에 대한 최신 업데이트 여부 점검		

	2.3.2 침입차단시스템의 정책 변경을 위한 절차를 수립 및 시행하는가	배점	점검(해당항목에 V표)
23	1. 정책 가이드라인 마련, 정보보호 관리자의 승인 등을 통해 변경하고, 변경기록을 관리한다	3	
	2. 정책 가이드라인 마련, 정보보호 관리자의 승인 등을 통해 변경한다	2	
	3. 정보보호 관리자를 통해 변경한다	1	
	4. 정책 변경에 대한 절차가 없다	0	
	증빙자료 : 정보보호시스템 목록 및 네트워크 구성도, 침입차단시스템 정책 변경 절차, 정책 변경 내역 등		

	2.3.3 침입차단시스템 관리가 이루어지는가	배점	점검(해당항목에 V표)
24	1. 콘솔에서 직접관리하거나 지정된 IP를 통해서 암호화 통신으로 관리하고, 로그인시 인증절차를 사용한다	3	
	2. 전용 프로그램을 사용하여 관리하고, 암호화 통신 및 로그인시 인증절차를 사용한다	2	
	3. 웹 기반의 서비스를 이용하여 관리하고, 암호화 통신 사용 및 로그인시 인증절차를 사용한다	1	
	4. 보안대책이 없다	0	
	증빙자료 : 정보보호시스템 목록 및 네트워크 구성도, 점검시 침입차단시스템 관리에 대하여 직접 점검		

	2.3.4 침입차단시스템의 침입차단 규칙을 수립하였는가	배점	점검(해당항목에 V표)
25	1. All Deny를 기본으로 설정하고, 필요 서비스 및 필수 허용 대상에 대해서만 허용규칙을 Inbound/Outbound로 구분하여 설정한다	3	
	2. All Deny를 기본으로 설정하고, 필요 서비스 및 필수 허용 대상에 대해서만 허용규칙을 설정한다	2	
	3. All Deny를 기본으로 설정하였으나, 정책 중복성 존재하고 불필요한 서비스가 허용으로 설정되어 있다	1	
	4. All Deny를 기본으로 설정하지 않고 있다	0	
	증빙자료 : 정보보호시스템 목록 및 네트워크 구성도, 침입차단시스템 정책 리스트(object 목록 포함), 시스템 별 운영 서비스 목록(포트번호 포함), 네트워크 구성도(IP 주소 포함) 등		

<2.4 네트워크 장비>

	2.4.1 네트워크 장비의 운영체제 업데이트를 수행하는가	배점	점검(해당항목에 V표)
26	1. 운영체제 업데이트를 수행한다	3	
	2. 운영체제 업데이트를 수행하지 않는다	0	
	증빙자료 : 네트워크 장비 목록 및 네트워크 구성도, 점검시 네트워크 운영체제 버전의 최신 여부 확인		

	2.4.2 네트워크 장비의 기본 패스워드 및 배너를 변경하였는가	배점	점검(해당항목에 V표)
	1. 패스워드 및 배너 변경을 수행한다	3	
	2. 패스워드 및 배너 변경을 수행하지 않는다	0	
27			
	증빙자료 : 네트워크 장비 목록 및 네트워크 구성도, 점검시 Default 패스워드 여부 및 배너 변경 여부 확인		

	2.4.3 네트워크 장비의 불필요한 서비스를 제거하는가	배점	점검(해당항목에 V표)
	1. 불필요한 서비스를 제거한다	3	
	2. 불필요한 서비스를 제거하지 않는다	0	
28			
	증빙자료 : 네트워크 장비 목록 및 네트워크 구성도, 네트워크 장비 별 서비스 리스트 등		

	2.4.4 네트워크 장비들 간 시간동기화를 수행하는가	배점	점검(해당항목에 V표)
	1. 시간동기화를 수행한다	3	
	2. 시간동기화를 수행하지 않는다	0	
29			
	증빙자료 : 네트워크 장비 목록 및 네트워크 구성도, 네트워크 장비 시간 설정 덤프, 점검시 시간 동기화 확인		

<2.5 응용 프로그램 및 서비스 관리>

	2.5.1 정보시스템의 서비스를 관리하는가	배점	점검(해당항목에 V표)
	1. 정보시스템에 필요한 필수 서비스만을 운영하며, TCP Wrapper 등을 통해 접근 차단한다	3	
	2. TCP Wrapper 등을 통해 접근 차단 하거나 필수 서비스만 운영한다	1.5	
30	3. 정보시스템 서비스를 관리하지 않는다	0	
	증빙자료 : 정보시스템 별 서비스 리스트, 접근 제한 정책, TCP Wrapper 등의 접근 제한 솔루션 현황 등		

	2.5.2 웹 서버와 DB 서버를 분리하여 운영하는가	배점	점검(해당항목에 V표)
	1. 웹 서버와 DB 서버를 별도 하드웨어로 운영하고, DMZ 영역에서 운영한다	3	
	2. 웹 서버와 DB 서버를 별도 하드웨어로 운영하되, 기타 정보시스템과 동일 네트워크에서 운영한다	1.5	
31	3. 웹 서버와 DB 서버를 하나의 하드웨어로 통합하여 운영한다	0	
	4. 해당없다	평가제외	
	증빙자료 : 웹, DB 서버 구성도 및 현황 등		

	2.5.3 웹 응용프로그램 취약점 공격에 대한 보안 대책을 수립 및 시행하는가	배점	점검(해당항목에 V표)
	1. 웹 응용프로그램 방화벽을 추가 구성하여 보호하고, 웹 응용프로그램 취약점을 분석하고 제거한다	3	
	2. 웹 응용프로그램 취약점을 분석하고 제거한다	1.5	
32	3. 웹 응용프로그램 취약점 공격에 대한 보안대책이 없다	0	
	증빙자료 : 웹 응용프로그램 방화벽 현황, 웹 취약점 점검 보고서 및 보안대책 현황 등		

	2.5.4 서비스 운영시 사용되는 중요 데이터(개인정보, 전력과금 정보)를 암호화하여 DB에 저장하는가	배점	점검(해당항목에 V표)
	1. DB보안 솔루션을 이용하여 중요 데이터를 암호화한다	3	
	2. 중요 필드 값들만 암호화한다	1.5	
33	3. 중요 데이터를 암호화하여 저장하지 않는다	0	
	증빙자료 : 시스템 별 서비스 목록, 서비스 별 사용 데이터 목록, DB보안 솔루션 현황, DB 암호화 현황, 점검시 중요 필드들에 대한 암호화 여부 점검		

	2.5.5 DB 운영시 DB 보안대책을 수립 및 시행하는가	배점	점검(해당항목에 V표)
	1. 데이터 연동을 위한 DB 계정과 DB 관리자 계정을 분리하여 관리하고, 작업기록 및 트랜잭션에 대한 로그를 관리한다	3	
	2. 데이터 연동을 위한 DB 계정과 DB 관리자 계정을 분리하여 관리한다	1.5	
34	3. DB 보안대책이 수립되어 있지 않다	0	
	증빙자료 : 데이터 연동 DB 계정 및 관리자 계정 ID 리스트(덤프), 작업기록 및 트랜잭션 로그 등		

<2.6 네트워크 구성 및 접근제어>

	2.6.1 제어시스템을 물리적으로 분리된 네트워크에서 운영하고 있는가	배점	점검(해당항목에 V표)
	1. 다른 네트워크와 물리적으로 분리된 네트워크에서 운영한다	3	
	2. 다른 네트워크와 일방향으로 연결하여 운영한다	2	
35	3. 침입차단시스템을 통해 다른 시스템과 연계하여 차단한다	1	
	4. 네트워크가 분리되어 있지 않다	0	
	5. 해당없다	평가제외	
	증빙자료 : 네트워크 구성도 및 침입차단시스템 구성도, 침입차단시스템 정책 목록 등		

	2.6.2 운영센터 네트워크에서 인터넷 사용을 제한하고 있는가	배점	점검(해당항목에 V표)
	1. 인터넷 사용을 제한하고 있다	3	
	2. 인터넷 사용을 제한하지 않는다	0	
36			
	증빙자료 : 네트워크 구성도, 점검시 운영센터 네트워크에서 인터넷 사용 여부 점검		

	2.6.3 운영센터 정보시스템들을 별도 서브넷으로 구성하여 접근제어를 수행하는가	배점	점검(해당항목에 V표)
	1. 기능, 보안 중요도 별로 세분화해 구성하고, 필요 서비스만 접근 허용하도록 접근제어를 수행한다	3	
	2. 서버영역, 운영요원 PC 영역, DMZ만 별도 구성하여 접근제어를 수행한다	2	
37	3. DMZ 영역만 별도 구성하여 접근제어를 수행한다	1	
	4. 접근제어를 수행하고 있지 않다	0	
	증빙자료 : 네트워크 구성도, 시스템 목록, 시스템 별 서비스 목록, 서브넷 구성도, DMZ 구성도 및 접근제어 현황 등		

	2.6.4 안전하지 않은 시스템(비인가 시스템 및 악성코드 감염 시스템) 및 보안정책을 따르지 않는 시스템에 대해 네트워크 사용제한을 수행하는가	배점	점검(해당항목에 V표)
38	1. NAC를 사용하여 안전하지 않은 시스템의 네트워크 사용을 제한한다	3	
	2. MAC 주소 및 백신 소프트웨어 등을 사용하여 안전하지 않은 시스템의 네트워크 사용을 제한한다	2	
	3. MAC 주소를 이용하여 안전하지 않은 시스템의 네트워크 사용을 제한한다	1	
	4. 네트워크 사용제한을 수행하고 있지 않다	0	
	증빙자료 : 네트워크 구성도, 시스템 목록, 시스템 별 서비스 목록, NAC 구성 현황, 네트워크 사용 제한 대책서 등		

	2.6.5 정보시스템 자원은 권한에 따라 사용자 접근제한을 수행하는가	배점	점검(해당항목에 V표)
39	1. SecureOS 등을 사용하여 시스템 자원에 대한 사용자 접근을 제한한다	3	
	2. SecureOS 등을 사용하여 시스템 자원에 대한 사용자 접근을 제한하지 않는다	0	
	증빙자료 : Secure OS등의 시스템 접근제한 솔루션 현황, 접근제한 리스트 등		

	2.6.6 운영센터 내부에서 무선 네트워크를 사용하고 있는가	배점	점검(해당항목에 V표)
40	1. 무선 네트워크를 사용하지 않는다	3	
	2. 무선 네트워크를 사용하며 WPA2 이상의 보안대책으로 관리한다	1.5	
	3. 무선 네트워크를 사용하나 보안대책이 안전하지 않다	0	
	증빙자료 : 무선 네트워크 운영 현황, AP의 무선 네트워크 보안 설정		

3. 연계구간 보안

<3.1 통합운영센터와 컨소시엄 운영센터 연계구간>

	3.1.1 통합운영센터와 컨소시엄 운영센터 연계시 DMZ를 구성하는가	배점	점검(해당항목에 V표)
41	1. DMZ를 구성한다	3	
	2. DMZ를 구성하고 있지 않다	0	
	증빙자료 : 네트워크 구성도		

	3.1.2 통합운영센터와 컨소시엄 운영센터 연계구간 (임차)전용선을 사용하는가	배점	점검(해당항목에 V표)
42	1. 전용선을 사용하거나, 임차전용선을 사용하면서 VPN 적용 등의 통신 보안대책이 있다	3	
	2. 임차전용선을 사용하고 있다	1.5	
	3. (임차)전용선을 사용하고 있지 않다	0	
	증빙자료 : 네트워크 구성도(전용선, VPN 장비현황 등 표시), 임차전용선 임대 계약서		

	3.1.3 통합운영센터와 컨소시엄 운영센터 연계구간에서 인증, 데이터 무결성 및 기밀성 제공 등에 표준 암호 알고리즘을 사용하는가	배점	점검(해당항목에 V표)
43	1. 128 비트 이상 수준의 표준 암호 알고리즘을 사용한다	3	
	2. 128 비트 미만 수준의 표준 암호 알고리즘을 사용한다	2	
	3. 비표준 암호 알고리즘을 사용한다	1	
	4. 암호 알고리즘 사용하고 있지 않다	0	
	5. 해당없다 (전용선 사용의 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.1.4 통합운영센터와 컨소시엄 운영센터 연계구간에서 통신 주체간 인증을 수행하는가	배점	점검(해당항목에 V표)
44	1. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 상호인증을 수행한다	3	
	2. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 단방향 인증(클라이언트 또는 서버)을 수행한다	2	
	3. 기기 고유 주소 또는 MAC 주소를 사용하여 인증을 수행한다	1	
	4. 인증을 수행하고 있지 않다	0	
	5. 해당없다 (전용선 사용의 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.1.5 통합운영센터와 컨소시엄 운영센터 연계구간에서 대칭키(사전공유비밀키) 또는 공개키(인증서) 사용에 대한 보안대책이 마련되어 있는가	배점	점검(해당항목에 V표)
45	1. (사전공유비밀키 기반의 경우) 초기 기기 설정은 오프라인, 갱신은 안전한 프로토콜을 사용하여 온라인으로 수행 등의 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 내에 설치된 공개키(인증서) 서버를 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	3	
	2. (사전공유비밀키 기반의 경우) 초기 기기 설정 및 갱신을 오프라인으로 수행하는 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 마련과 함께 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	2	
	3. (사전공유비밀키 기반의 경우) 초기 기기 설정된(오프라인) 사전공유비밀키를 갱신없이 계속 사용하면서 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등의 관리 방안 없이, 초기 설정된 개인키 및 공개키 쌍을 사용한다 또는, 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 없이 운영한다	1	
	4. 보안대책이 없다	0	
	5. 해당없다 (전용선 사용의 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.1.6 통합운영센터와 컨소시엄 운영센터 연계구간에서 데이터 무결성 및 기밀성을 제공하는가	배점	점검(해당항목에 V표)
46	1. 데이터 무결성 및 기밀성을 모두 제공한다	3	
	2. 데이터 무결성 또는 기밀성을 제공한다	1.5	
	3. 모두 제공하고 있지 않다	0	
	4. 해당없다 (전용선 사용의 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

<3.2 통합운영센터와 기간시스템 연계구간>

	3.2.1 통합운영센터와 기간시스템 연계시 DMZ를 구성하는가	배점	점검(해당항목에 V표)
47	1. DMZ를 구성한다	3	
	2. DMZ를 구성하고 있지 않다	0	
	3. 해당없다	평가제외	
	증빙자료 : 네트워크 구성도		

	3.2.2 통합운영센터와 기간시스템 연계구간 (임차)전용선을 사용하는가	배점	점검(해당항목에 V표)
48	1. 전용선을 사용하거나, 임차전용선을 사용하면서 VPN 적용 등의 통신 보안대책이 있다	3	
	2. 임차전용선을 사용하고 있다	1.5	
	3. (임차)전용선을 사용하고 있지 않다	0	
	4. 해당없다 (적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도(전용선, VPN 장비현황 등 표시), 임차전용선 임대 계약서		

	3.2.3 통합운영센터와 기간시스템 연계구간에서 인증, 데이터 무결성 및 기밀성 제공 등에 표준 암호 알고리즘을 사용하는가	배점	점검(해당항목에 V표)
49	1. 128 비트 이상 수준의 표준 암호 알고리즘을 사용한다	3	
	2. 128 비트 미만 수준의 표준 암호 알고리즘을 사용한다	2	
	3. 비표준 암호 알고리즘을 사용한다	1	
	4. 암호 알고리즘 사용하고 있지 않다	0	
	5. 해당없다 (전용선을 사용하거나, 적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.2.4 통합운영센터와 기간시스템 연계구간에서 통신 주체간 인증을 수행하는가	배점	점검(해당항목에 V표)
50	1. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 상호인증을 수행한다	3	
	2. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 단방향 인증(클라이언트 또는 서버)을 수행한다	2	
	3. 기기 고유 주소 또는 MAC 주소를 사용하여 인증을 수행한다	1	
	4. 인증을 수행하고 있지 않다	0	
	5. 해당없다 (전용선을 사용하거나, 적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.2.5 통합운영센터와 기간시스템 연계구간에서 대칭키(사전공유비밀키) 또는 공개키(인증서) 사용에 대한 보안대책이 마련되어 있는가	배점	점검(해당항목에 V표)
51	1. (사전공유비밀키 기반의 경우) 초기 기기 설정은 오프라인, 갱신은 안전한 프로토콜을 사용하여 온라인으로 수행 등의 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 내에 설치된 공개키(인증서) 서버를 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	3	
	2. (사전공유비밀키 기반의 경우) 초기 기기 설정 및 갱신을 오프라인으로 수행하는 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 마련과 함께 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	2	
	3. (사전공유비밀키 기반의 경우) 초기 기기 설정된(오프라인) 사전공유비밀키를 갱신없이 계속 사용하면서 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등의 관리 방안 없이, 초기 설정된 개인키 및 공개키 쌍을 사용한다 또는, 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 없이 운영한다	1	
	4. 보안대책이 없다	0	
	5. 해당없다 (전용선을 사용하거나, 적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.2.6 통합운영센터와 기간시스템 연계구간에서 데이터 무결성 및 기밀성을 제공하는가	배점	점검(해당항목에 V표)
52	1. 데이터 무결성 및 기밀성을 모두 제공한다	3	
	2. 데이터 무결성 또는 기밀성을 제공한다	1.5	
	3. 모두 제공하고 있지 않다	0	
	4. 해당없다 (전용선을 사용하거나, 적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

<3.3 운영센터와 기기 연계구간>

	3.3.1 운영센터와 스마트그리드 기기 연계시 DMZ를 구성하는가	배점	점검(해당항목에 V표)
53	1. DMZ를 구성한다	3	
	2. DMZ를 구성하고 있지 않다	0	
	3. 해당없다 (적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도		

	3.3.2 운영센터와 스마트그리드 기기 연계구간에서 인증, 데이터 무결성 및 기밀성 제공 등에 표준 암호 알고리즘을 사용하는가	배점	점검(해당항목에 V표)
54	1. 128 비트 이상 수준의 표준 암호 알고리즘을 사용한다	3	
	2. 128 비트 미만 수준의 표준 암호 알고리즘을 사용한다	2	
	3. 비표준 암호 알고리즘을 사용한다	1	
	4. 암호 알고리즘 사용하고 있지 않다	0	
	5. 해당없다 (적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.3.3 운영센터와 스마트그리드 기기 연계구간에서 통신 주체간 인증을 수행하는가	배점	점검(해당항목에 V표)
55	1. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 상호인증을 수행한다	3	
	2. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 단방향 인증(클라이언트 또는 서버)을 수행한다	2	
	3. 기기 고유 주소 또는 MAC 주소를 사용하여 인증을 수행한다	1	
	4. 인증을 수행하고 있지 않다	0	
	5. 해당없다 (적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.3.4 운영센터와 스마트그리드 기기 연계구간에서 대칭키(사전공유비밀키) 또는 공개키(인증서) 사용에 대한 보안대책이 마련되어 있는가	배점	점검(해당항목에 V표)
56	1. (사전공유비밀키 기반의 경우) 초기 기기 설정은 오프라인, 갱신은 안전한 프로토콜을 사용하여 온라인으로 수행 등의 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 내에 설치된 공개키(인증서) 서버를 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	3	
	2. (사전공유비밀키 기반의 경우) 초기 기기 설정 및 갱신을 오프라인으로 수행하는 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 마련과 함께 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	2	
	3. (사전공유비밀키 기반의 경우) 초기 기기 설정된(오프라인) 사전공유비밀키를 갱신없이 계속 사용하면서 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등의 관리 방안 없이, 초기 설정된 개인키 및 공개키 쌍을 사용한다 또는, 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 없이 운영한다	1	
	4. 보안대책이 없다	0	
	5. 해당없다 (적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.3.5 운영센터와 스마트그리드 기기 연계구간에서 데이터 무결성 및 기밀성을 제공하는가	배점	점검(해당항목에 V표)
57	1. 데이터 무결성 및 기밀성을 모두 제공한다	3	
	2. 데이터 무결성 또는 기밀성을 제공한다	1.5	
	3. 모두 제공하고 있지 않다	0	
	4. 해당없다 (적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

<3.4 운영센터와 외부 네트워크 연계구간>

	3.4.1 운영센터와 외부 네트워크 연계시 DMZ를 구성하는가	배점	점검(해당항목에 V표)
	1. DMZ를 구성한다	3	
	2. DMZ를 구성하고 있지 않다	0	
58	3. 해당없다 (적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도		

	3.4.2 운영센터와 외부 네트워크 연계구간 (임차)전용선을 사용하는가	배점	점검(해당항목에 V표)
	1. 전용선을 사용하거나, 임차전용선을 사용하면서 VPN 적용 등의 통신 보안대책이 있다	3	
	2. 임차전용선을 사용하고 있다	1.5	
59	3. (임차)전용선을 사용하고 있지 않다	0	
	4. 해당없다 (적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도(전용선, VPN 장비현황 등 표시), 임차전용선 임대 계약서		

	3.4.3 운영센터와 외부 네트워크 연계구간에서 인증, 데이터 무결성 및 기밀성 제공 등에 표준 암호 알고리즘을 사용하는가	배점	점검(해당항목에 V표)
	1. 128 비트 이상 수준의 표준 암호 알고리즘을 사용한다	3	
	2. 128 비트 미만 수준의 표준 암호 알고리즘을 사용한다	2	
60	3. 비표준 암호 알고리즘을 사용한다	1	
	4. 암호 알고리즘 사용하고 있지 않다	0	
	5. 해당없다 (전용선을 사용하거나, 적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.4.4 운영센터와 외부 네트워크 연계구간에서 통신 주체간 인증을 수행하는가	배점	점검(해당항목에 V표)
61	1. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 상호인증을 수행한다	3	
	2. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 단방향 인증(클라이언트 또는 서버)을 수행한다	2	
	3. 기기 고유 주소 또는 MAC 주소를 사용하여 인증을 수행한다	1	
	4. 인증을 수행하고 있지 않다	0	
	5. 해당없다 (전용선을 사용하거나, 적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.4.5 운영센터와 외부 네트워크 연계구간에서 대칭키(사전공유비밀키) 또는 공개키(인증서) 사용에 대한 보안대책이 마련되어 있는가	배점	점검(해당항목에 V표)
62	1. (사전공유비밀키 기반의 경우) 초기 기기 설정은 오프라인, 갱신은 안전한 프로토콜을 사용하여 온라인으로 수행 등의 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 내에 설치된 공개키(인증서) 서버를 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	3	
	2. (사전공유비밀키 기반의 경우) 초기 기기 설정 및 갱신을 오프라인으로 수행하는 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 마련과 함께 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	2	
	3. (사전공유비밀키 기반의 경우) 초기 기기 설정된(오프라인) 사전공유비밀키를 갱신없이 계속 사용하면서 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등의 관리 방안 없이, 초기 설정된 개인키 및 공개키 쌍을 사용한다 또는, 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 없이 운영한다	1	
	4. 보안대책이 없다	0	
	5. 해당없다 (전용선을 사용하거나, 적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	3.4.6 운영센터와 외부 네트워크 연계구간에서 데이터 무결성 및 기밀성을 제공하는가	배점	점검(해당항목에 V표)
63	1. 데이터 무결성 및 기밀성을 모두 제공한다	3	
	2. 데이터 무결성 또는 기밀성을 제공한다	1.5	
	3. 모두 제공하고 있지 않다	0	
	4. 해당없다 (전용선을 사용하거나, 적용 구간이 없을 경우)	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

4. 스마트그리드 기기 보안

<4.1 스마트그리드 기기>

	4.1.1 기기 설치시 확인된 기기만을 설치하도록 절차를 수립하고 시행하는가	배점	점검(해당항목에 V표)
64	1. 기기 설치시 운영센터에 등록된 기기인지 확인 후 설치한다	3	
	2. 등록 기기 여부를 확인하지 않고 설치한다	0	
	3. 해당없다	평가제외	
	증빙자료 : 기기 설치 절차서, 기기 설치 및 등록 내역서 등		

	4.1.2 기기에 저장하는 비밀번호, 패스워드 등을 보호하는가	배점	점검(해당항목에 V표)
65	1. 비밀번호 또는 패스워드를 해시 알고리즘 등을 사용하여 보호한다	3	
	2. 비밀번호 또는 패스워드를 평문으로 저장한다	0	
	3. 해당없다	평가제외	
	증빙자료 : 기기 비밀번호, 패스워드 등의 암호화 저장 여부 확인		

	4.1.3 스마트그리드 기기 내 저장되는 데이터를 보호하는가	배점	점검(해당항목에 V표)
66	1. 국가정보원이 시행하는 암호검증 절차를 마친 암호모듈을 사용하여 암호화하고, 최소한의 정보만 기기에 저장한다	3	
	2. 자체 개발한 암호모듈을 사용하여 암호화하고, 최소한의 정보만 기기에 저장한다	1.5	
	3. 암호화 하지 않고 기기에 데이터를 저장한다	0	
	4. 해당없다	평가제외	
	증빙자료 : 기기 저장 데이터 목록, 저장 방법 확인, 기기 내장 암호모듈명 및 인증서 등		

	4.1.4 스마트그리드 기기 펌웨어 및 소프트웨어를 설치 및 업데이트시 보안대책을 수립 및 시행하는가	배점	점검(해당항목에 V표)
67	1. 펌웨어 및 소프트웨어 기능 및 안전성 점검하고, 설치전 펌웨어 및 소프트웨어에 대한 무결성 검사 등을 수행한 후 인증된 펌웨어 및 소프트웨어를 설치한다	3	
	2. 펌웨어 및 소프트웨어 기능 및 안전성 점검을 수행한 후 설치한다	1.5	
	3. 보안대책이 없다	0	
	4. 해당없다	평가제외	
	증빙자료 : 펌웨어와 소스트웨어의 설치 및 업데이트 절차서, 설치/업데이트시의 보안대책서 등		

	4.1.5 스마트그리드 기기 복제 방지 대책을 수립 및 시행하는가	배점	점검(해당항목에 V표)
68	1. Anti-tampering, Tamper-proofing 등의 복제방지 대책 수립 및 시행한다	3	
	2. 복제방지 대책이 없다	0	
	3. 해당없다	평가제외	
	증빙자료 : 스마트그리드 기기 복제 방지 대책안, 기기에 적용된 복제방지 기술 현황 등		

<4.2 스마트그리드 기기 연계구간>

	4.2.1 스마트그리드 기기 간 통신에서 인증, 데이터 무결성 및 기밀성 제공 등에 표준 암호 알고리즘을 사용하는가	배점	점검(해당항목에 V표)
69	1. 128 비트 이상 수준의 표준 암호 알고리즘을 사용한다	3	
	2. 128 비트 미만 수준의 표준 암호 알고리즘을 사용한다	2	
	3. 비표준 암호 알고리즘을 사용한다	1	
	4. 암호 알고리즘 사용하고 있지 않다	0	
	5. 해당없다	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	4.2.2 스마트그리드 기기 간 통신에서 통신 주체간 인증을 수행하는가	배점	점검(해당항목에 V표)
70	1. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 상호인증을 수행한다	3	
	2. 대칭키(사전공유비밀키) 또는 공개키(인증서) 기반의 단방향 인증(클라이언트 또는 서버)을 수행한다	2	
	3. 기기 고유 주소 또는 MAC 주소를 사용하여 인증을 수행한다	1	
	4. 인증을 수행하고 있지 않다	0	
	5. 해당없다	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	4.2.3 스마트그리드 기기 간 통신에서 대칭키(사전공유비밀키) 또는 공개키(인증서) 사용에 대한 보안대책이 마련되어 있는가	배점	점검(해당항목에 V표)
71	1. (사전공유비밀키 기반의 경우) 초기 기기 설정은 오프라인, 갱신은 안전한 프로토콜을 사용하여 온라인으로 수행 등의 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 내에 설치된 공개키(인증서) 서버를 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	3	
	2. (사전공유비밀키 기반의 경우) 초기 기기 설정 및 갱신을 오프라인으로 수행하는 보안대책을 통해 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 마련과 함께 운영하며, 발급된 공개키(인증서)를 통해 상호 인증을 수행한다	2	
	3. (사전공유비밀키 기반의 경우) 초기 기기 설정된(오프라인) 사전공유비밀키를 갱신없이 계속 사용하면서 상호 인증을 수행한다 (공개키 기반의 경우) 공개키(인증서) 생성/변경/파기 등의 관리 방안 없이, 초기 설정된 개인키 및 공개키 쌍을 사용한다 또는, 공개키(인증서) 생성/변경/파기 등을 실증단지 외부에 설치된 공개키(인증서) 서버를 외부 연계에 대한 보안대책 없이 운영한다	1	
	4. 보안대책이 없다	0	
	5. 해당없다	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		

	4.2.4 스마트그리드 기기 간 통신에서 데이터 무결성 및 기밀성을 제공하는가	배점	점검(해당항목에 V표)
72	1. 데이터 무결성 및 기밀성을 모두 제공한다	3	
	2. 데이터 무결성 또는 기밀성을 제공한다	1.5	
	3. 모두 제공하고 있지 않다	0	
	4. 해당없다	평가제외	
	증빙자료 : 네트워크 구성도, 인증 및 암호화 등의 보호 대책 계획서, 인증 및 암호화 솔루션 현황 등		