정 보 보 호 학 회 지
제24권 제1호, 2014. 2

전력신뢰도 관리기구의 사이버보안 활동 동향 및 국내 적용방안 고찰

김 성 호*, 김 신 규*, 서 정 택*

요 약

전력계통의 안정성이 무너질 경우 정전의 발생으로 국가적인 경제적 손실과 더불어 사회적 혼란이 야기될 수 있다. 따라서 전력계통의 신뢰성 보장을 위해 국가 차원의 제도마련 및 운영이 필요하다. 이에 미국에서는 전력운용의 신뢰성 보장을 전담하는 기구를 통해 전력사의 전력계통 운영을 감시 및 감사함으로써 전력계통 신뢰도 보장에 힘쓰고 있다. 본 고에서는 전력계통의 신뢰성 침해의 다양한 원인 중 최근 큰 이슈가 되고 있는 사이버 보안 침해에 대응하기 위한 전력계통 신뢰도 관리 기구의 활동을 살펴보고, 국내에 전력신뢰도 관리기구 및 관련 관리체계 구축 시에 사이버 보안 측면에서 고려되어야할 사항들에 대해 살펴보고자 한다.

Ⅰ. 서 론

2011년 9월 15일 국내에서 발생된 순환정전 사건은 국내도 블랙아웃의 위험에서 더 이상 안전하지 않다는 것을 보여주었다. 전력 수요의 급증 및 예비전력 부족으로 유발된 순환정전은 국내 전력계통의 신뢰도 관리가 미비했다는 것을 보여주었으며, 이로 인해 경제적 피해 및 사회적 혼란이 유발되었다[1]. 이후 국가적으로 전력계통 신뢰도에 대한 중요도 인식이 높아지고 있으며, 2013년 지식경제부(현 산업통상자원부)에서 공고된 “제 6차 전력수급기본계획” [2] 에는 국내에 북미전력계통 신뢰도관리기구(North American Electric Reliability Corporation, NERC)와 같은 전력계통 신뢰도 관리 기구가 설립을 위한 계획이 포함되어 있다.

한편, 현재의 전력산업 및 전력신뢰도 관리 기술들은 IT기술에 의존적으로 되고 있으며, 이러한 특성으로 인해 국내에서도 전력계통에 대한 사이버 보안위협이 제기되고 있다 [3] . 이러한 상황은 미국에서도 동일하게 받아들여지고 있으며, 이에 NERC에서는 전력계통 신뢰도 침해의 주요 원인 중 하나로 사이버 침해를 지목하고, 전력계통을 대상으로 한 사이버 보안 위협에 대응하기 위한 일련의 역할들을 수행하고 있다.

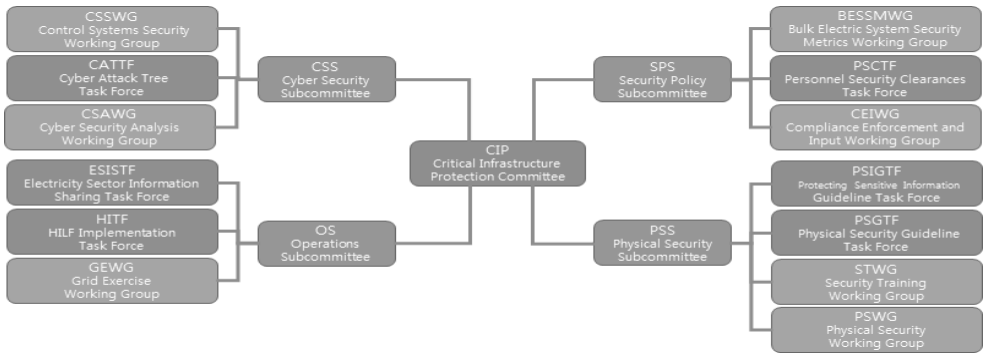
본 고에서는 NERC에서 수행하고 있는 전력계통에 대한 사이버보안 역할들을 살펴보고, 국내에 설립될 전력계통 신뢰도 관리기구가 수행해야 할 사이버 보안의 역할들에 대해 논의해 보고자 한다.

Ⅱ. 미국 전력 신뢰도 관리 기구

1965년 미국에서 발생된 광역정전을 통해 FPC(Federal Power Commission)는 전력계통 신뢰도 문제가 발생할 경우 개별 전력회사 차원에서는 해결이 불가능하다고 판단하였으며, 전력계통 신뢰도 보장을 위해 전력회사들 간에 통일된 계통운영 및 계획을 수립해 줄 수 있는 기구가 필요하다는 결론에 도달하게 되었다. FPC의 제안에 의해 북미 전력회사들은 북미신뢰도위원회(North America Reliability Council, NERC)을 설립하게 되었으며, 이후 35년간 자발적인 전력계통 신뢰도 기준을 수립하여 운영해 왔다[4].

하지만 2003년 북미 대정전 사건을 계기로 자율적인

본 연구는 2012년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (2012101050004A)
* ETRI 부설 연구소({night12, skkim, seojt}@ensec.re.kr)



〔그림 1〕 CIPC 조직 구성도

계통 신뢰도 기준보다는 강제성을 띄는 계통 신뢰도 기준이 필요하다는 의견에 도달하였다. 이에 미국 에너지 정책법(Energy Policy Act of 2005)에서는 FERC(Federal Energy Regulatory Commission)가 ERO(Electric Reliability Organization)를 지정하도록 명시하고 있다. 또한 미국 연방전력법(Frderal Power Act) 215조 e항과 18 C.F.R. 39.7 등에는 ERO가 전력시스템의 신뢰성과 관련된 조사, 평가, 분석, 감사 등의 업무를 수행하도록 명시하고 있다.

2006년 FERC는 북미전력계통 신뢰도관리기구인 NERC를 ERO로 지정하였으며, 이후 NERC는 북미 대규모 전력시스템 운영 주체들의 신뢰도 보장을 위한 노력을 및 표준 준수를 위해 다음과 같은 활동을 수행하고 있다.

- o 신뢰도 표준 개발 : 대규모 전력시스템 신뢰성 확보를 보장하기 위한 신뢰도 표준 제정
- o 신뢰성 평가 및 성능 분석 : 전력 공급과 수요에 대한 분석을 통해 전력시스템의 적절성 및 신뢰성에 대한 평가를 하며, 문제에 대한 대책을 고민
- o 신뢰성 위험 관리 : 전력설비, 발전시설, 시스템, 사람 등에 대한 실시간 감시를 통해 신뢰성 및 적절성에 대한 감사 역할 수행하며, 감사결과를 바탕으로 신규 신뢰도 표준 개발 및 기존 신뢰도 표준의 개정 여부를 식별
- o 신뢰도 표준 준수 및 시행 : 표준 준수에 대한 감시 및 규정위반에 대한 제제 등을 시행
- o 훈련 및 운영자 자격증 : 신뢰도 표준, 규제 등에 대한 교육을 시행하고, 전력시스템 운영자 자격증 제도를 시행

미국의 NERC는 비영리 단체로 운영조직 및 위원회들로 구성되어 있다. 특히 위원회는 전력산업계 각 분야의 전문가들로 구성되어 있으며, 북미 대규모 전력시스템(Bulk Power System)의 안전성 확보에 기여하는 것을 목표로 활동하고 있다. 위원회에서는 NERC에서 수행되는 모든 활동에 대한 자문활동을 수행하고 있으며 6개의 기술위원회, 1개의 집행위원회, 21개의 하위위원회, 24개의 워킹그룹, 15개의 태스크포스가 존재한다.

6개의 기술위원회 중 사이버 및 물리 보안과 관련하여 CIPC(Critical Infrastructure Protection Committee)가 운영되고 있다. CIPC는 북미 대규모 전력시스템의 사이버 및 물리적 보안성 제고를 위한 역할을 수행한다. [그림 1]과 같이 CIPC는 4개의 하위위원회와 7개의 워킹그룹, 6개의 태스크포스로 현재 구성되어 있다.

Ⅲ. NERC 사이버보안 활동

3.1. 보안관련 신뢰성 표준 개발 및 적용

앞서 설명한 바와 같이 NERC는 전력계통 운영사가 준수해야 하는 신뢰성 표준을 개발한다. 사이버 및 물리 공격을 통해 전력계통의 안정성이 파괴되는 것을 막기 위해 NERC는 보안관련 신뢰성 표준을 개발하여 발표한다. 보안관련 신뢰성 표준이 바로 CIP(Critical Infrastructure Protection)다. 각 전력계통 운영사는 CIP를 준수하여 사이버 위협에 대응해야 한다. CIP에 대해서는 다음 절에서 자세히 다루도록 한다.

NERC의 역할은 CIP를 개발하는데만 그치지 않는다. NERC는 각 전력사가 CIP를 정확히 준수하는지에 대해 분석, 조사, 평가, 감사를 수행한다. 또한 NERC는

〔표 1〕 CIP 각 항별 주요 내용

신뢰성 기준	내용
CIP-002 : 중요 사이버 자산 식별 (Critical Cyber Asset Identification)	위험기반 평가방법을 통해 기업의 중요 사이버 자산 식별 방안 및 체계 제시
CIP-003 : 보안관리 통제 (Security Management Controls)	중요 사이버 자산을 보호하기 위해 정책, 접근제어, 정보보호 등에 대한 최소한의 보안관리 통제사항 제시
CIP-004 : 인사 및 교육 (Personnel & Training)	보안인식 고취, 보안 교육, 사원의 위험성 평가 등을 통한 중요 자산에 접근하는 직원에 대한 적정 수준의 보안수준 유지방안 제시
CIP-005 : 전자적 보안경계 (Electronic Security Perimeters)	중요 사이버 자산이 존재하는 전자적 보안경계의 보호를 위해 경계 식별, 접근제어, 관제, 취약점 점검 등의 보안 통제사항 제시
CIP-006 : 중요 사이버 자산의 물리적 보안 (Physical Security of Critical Cyber Asset)	전자적 보안 경계 내에 있는 모든 사이버 자산이 물리적으로 안전할 수 있도록 계획을 세우고 관리하기 위한 방안 제시
CIP-007 : 시스템 보안 관리 (System Security Management)	전자적 보안 경계 내에서 사이버 자산으로 인식되는 시스템의 보안을 강화하기 위한 방법과 절차 제시
CIP-008 : 사고 보고와 대응책 기획 (Incident Reporting and Response Planning)	중요 사이버 자산과 관련된 사이버보안 사고를 확인, 분류, 대응, 보고하는 절차 제시
CIP-009 : 중요 사이버 자산의 복구 계획 마련 (Recovery Plans for Critical Cyber Assets)	기업의 재난 복구 기술 및 지침을 통해 중요 사이버 자산 복구 계획 마련 방안 제시

신뢰성 표준을 준수하지 않은 위반사항에 대해 제제를 가한다. 신뢰성 표준 위반사항에 대한 제제는 위반 시 위험도, 위반의 심각성, 위반 기간 등을 종합하여 결정한다.

3.2. CIP (Critical Infrastructure Protection)

CIP 표준은 NERC에서 개발되는 전력시스템 사이버보안 표준으로 기반시설에 포함된 정보시스템과 자산을 보호하며, 사이버보안 신뢰성을 충족시키기 위해 제시되고 있다. CIP는 002 ~ 009항의 세부 항목으로 나누어져 개발되고 있으며 각 항별 주요 내용은 [표 1]과 같다.

CIP 사이버보안 표준은 버전 1에서 버전 5까지 개발되었다. CIP 버전 5는 2013년 11월 22일[5] FERC에서 최종 승인되었으며, CIP 버전 3에서 버전 4를 거치지 않고 버전 5로 적용될 예정이다. CIP 버전 5에서는 대량 전기시스템(Bulk Electric System)에 대한 CIP 표준 항목들이 확장되었으며, [표 2]와 같이 2개의 항이 추가되었다.

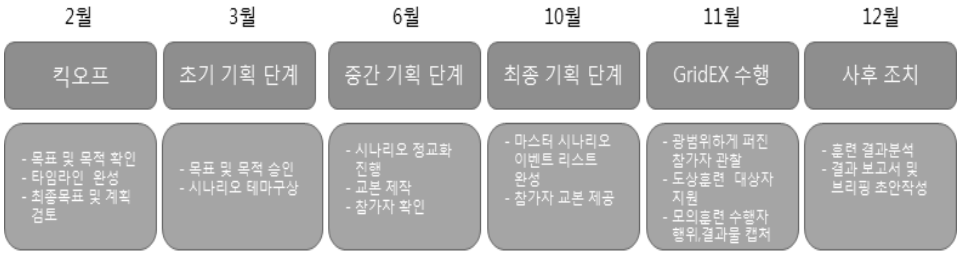
〔표 2〕 CIP 버전 5 추가 항목

신뢰성 기준	내용
CIP-010 : 설정변경 관리 및 취약점 평가 (Configuration Change Management and Vulnerability Assessments)	승인되지 않은 설정변경 방지 및 탐지와 취약성 평가 방안 제시
CIP-011 : 정보보호 (Information Protection)	정보시스템 대상 승인되지 않은 접근방지 방안 제시

3.3. ES-ISAC 운영

NERC의 ES-ISAC에서는 북미의 대규모 전력시스템 관련 사이버보안 정보공유를 위해 운영되고 있으며, 미국 에너지부와 NERC의 ESCC(Electricity Sector Coordinating Council)와 상호 협력하고 있다. ES-ISAC에서 수행되는 주요 업무는 다음과 같다.

- o 전력 서비스, 인프라스트럭처 및 중요 전력자원 보호와 관련된 사항들에 대한 식별, 우선순위 설정, 상호 협력관계 조정
- o 물리적 사이버 위협, 취약점, 보안사고, 잠재적인 보호조치 및 사이버 모의훈련 등과 관련된 정보공유
- o 보안위협, 보안취약성, 보안동향 및 영향도 평가와 관련된 데이터를 DoE, FERC, DHS와 협력하여 분석



〔그림 2〕 GridEx 진행프로세스

- o BPS(Bulk Power System)와 관련된 사이버 보안 사고 조사 데이터를 분석하여 보고서 작성
- o 관련 정부기관 및 유관기관들과 보안경계, 보안경고, 보안권고 등의 정보 공유
- o 전력계통과 관련된 교육 및 정보프로그램 시행

ES-ISAC에서는 NERC Alert이라는 이메일 기반의 정보메시지 형태로 대규모 전력시스템의 사이버보안과 관련된 중요 정보들을 제공하고 있으며, NERC 경보(Alert)는 다음과 같이 구분된다.

- o Industry Advisory : 문제로 이어질 가능성이 있거나 이슈가 될 수 있는 사항에 대해 정보 제공
- o Recommendation to Industry : 경보에 발령에 따른 전력사별 대응 행위가 수반되어야 하는 경보
- o Essential Action : 대형 전력시스템의 안정성을 유지하기 위해서 반드시 수행해야 하는 행위를 식별하여 알리는 경보로 이사회의 승인을 거쳐 발령

3.4. 사이버 모의훈련

GridEx는 NERC에서 주관하는 대규모 전력시스템 대상 사이버 침투대응 모의훈련으로, 북미의 전력사, 공공기관, 산업체, 학계 등 전력계통과 관련된 대부분의 기관들이 참여하고 있다. GridEx는 전력계통 사이버보안 대책으로 수립된 대응책 훈련 및 훈련결과를 바탕으로 파생된 관련 정보들을 공유하기 위한 목적으로 수행된다. 해당 훈련은 사전 정의된 시나리오에 따라 가상으로 진행되며, 실제 전력계통에 영향을 끼치지 않도록 수행된다[6]. 2011년 16~17일 GridEx가 수행되었으며, 2년 뒤인 2013년 11월 13~14일 GridEx II가 수행되었다. GridEx, GridEx II는 약 8개월가량의 준비기간을 거친 후에 수행되었으며, GridEx의 진행 프로세스는 [그림 2]와 같다.

3.5. 기타 사항

NERC에서는 CIP에 명시된 사이버 및 물리적 보안 통제사항에 대한 이행 정도를 측정하기 위한 기준을 개발하여 대규모 전력 시스템에 대한 보안성을 측정하며, 개발된 측정기준을 이용해 매년 “보안 분석 보고서”를 발간하고 있다. 또한 대규모 전력시스템의 안정성 확보를 위해 사이버 및 물리적 보안 가이드라인을 지속적으로 개발, 검토, 갱신하고 있다. 전력분야 정보에 대한 비밀공개 요구가 있을 시 관련 근거 식별 이후 공개여부를 결정하며, 민간 및 공공기관 간 안전한 정보공유 체계를 수립하고 있다.

NERC에서는 CIP 표준 개발과 더불어 해당 표준을 분석한 보고서인 CIP-CAR(Compliance Analysis Report)를 발간하며, 기기 또는 어플리케이션이 CIP 표준을 준수하였는지 여부를 평가하는 보고서인 CIP-CAN(Compliance Application Notices)를 발간하고 있다.

Ⅳ. 국내 전력계통 신뢰성기구 사이버보안 고려사항

4.1. 사이버보안 표준 제정 및 관리

국내 전력계통 신뢰도와 관련된 정책 및 관련 규정들은 지식경제부(현 산업통상자원부) 고시[7]를 통해 제공되고 있다. “전력계통 신뢰도 및 전기품질 유지기준” 고시 중 제45조(전력IT설비 보안기준 수립)에서는 전력계통에서의 사이버보안과 관련된 사항들을 제시하고 있으며, 전기사업법을 통해 해당 사항들을 준수하도록 하고 있다.

하지만 전력계통 사이버보안 표준인 CIP을 체계적으로 개발하고 이를 준수하도록 한 NERC에 비해 국내

전력계통 신뢰도 사이버보안 준수사항은 그 내용이 추상적으로 서술되어 있으며, 이는 전력계통과 관련된 사이버보안 준수 사항들을 강제하기에는 어려움이 따른다. 이러한 문제점들을 극복하기 위해서 국내 전력계통 신뢰성기구는 사이버보안과 관련하여 다음과 같은 역할을 수행해야 한다.

- o 전력계통 사이버보안 표준 제정 및 관리
  - 법규, 정책, 가이드라인 등을 집대성한 보안 표준 제시
  - 전력계통 사이버보안 표준이 실질적 규제가 될 수 있도록 관련 법규 및 정책 개편
  - 전력계통 운영환경 변화에 대응할 수 있도록 지속적인 갱신 및 개발
- o 전력계통 사이버보안 표준 준수 및 시행 모니터링
  - 준수 사항에 대한 점검, 분석, 평가, 감사 등을 통해 전력 시스템이 제정된 사이버보안 표준을 정확하게 준수할 수 있도록 관리
  - 표준 준수를 위한 지속적인 교육 프로그램 개발 및 운영

4.2. 전력계통 사이버침해 대응 및 정보 공유

한국전력거래소 내의 전력계통 보안관제 센터에서는 계통운영시스템과 시장운영시스템을 사이버침해로부터 보호하기 위해 설립되었으며, 24시간 관제업무를 수행중에 있다. 또한 침해사고 대응 모의훈련 및 민간발전사 제어담당자들을 대상으로 정보보안 교육을 실시하며 전력계통을 대상으로 한 사이버위협에 대응하고 있다. 또한 한국전력거래소 정보기술처 정보보호팀은 직제상 주요정보 통신기반시설 및 정보보안 보호정책 수립 및 운영, 전력계통 보안관제 센터 운영 및 보안시스템 유지관리, 개인정보 보호, 사이버 침해 대책 수립 및 대응, 보안설비 구축정책 수립 및 관리, 정보보안 관련 대내외 업무 등을 수행하고 있다.

한국전력거래소도 NERC와 같이 전력계통 신뢰도 관련 사이버 보안 위협에 대응하기 위해 노력하고 있지만, 규모의 한계로 인하여 NERC에서 추진되는 Grid-Ex, ES-ISAC 등과 같은 활동에 비해 제한적으로 수행되고 있다. 이러한 이유로 국내 전력계통 신뢰성 기구는 전력계통 사이버 침해 대응을 위해 다음과 같은 역할을 강화해야 한다.

- o ES-ISAC 운영 확장을 통한 사이버 침해사고 대응 및 정보 공유
  - 지속적인 사이버보안 교육 프로그램 개발 및 운영
  - 전력시스템 대상 사이버 침해관련 정보수집 및 분석
  - 전력시스템 대상 사이버공격 정보, 취약점 정보, 사례 등에 대한 정보 제공
  - 사이버 침해관련 주요 경보발령 및 관련 정보 제공
  - 사이버 모의훈련 확장을 통해 APT(Advanced Persistent Threat)과 같은 보안위협으로 발생되는 침해사고에 대한 대응능력 제고

Ⅴ. 결론

본 고에서는 미국의 NERC에서 운영되는 사이버관련 조직 및 활동들을 통해 국내 전력계통 신뢰도 관리기구 설립 시 고려되어야 사항들에 대해 살펴보았다. 국내에서도 전력계통 신뢰성 운영과 관련된 전문성 있는 독립기구 설립이 예상되고 있으며, 전력계통 신뢰성 운영과 사이버보안은 밀접한 관계를 맺고 있기 때문에 기구 설립 시부터 전력계통에 대한 사이버 보안 사항들이 고려되어야 한다.

참고문헌

[1] 이근준, “2011. 9. 15 순환정전발생과 오차 분석”, 2012 대한전기학회 전력기술부문회 추계학술대회 논문집, 대한전기학회, pp. 323-325, 10월 2012년.

[2] 지식경제부, “제6차 전력수급기본계획”, 2월 2013년.

[3] 강순의, 손윤태, 김성학, “우리나라 전력계통의 사이버테러 대응방안 고찰”, 대한전기학회 전력기술부문회 추계학술대회 논문집, pp. 124-126, 11월 2007년.

[4] 전기위원회, “2003년 북미 정전 보고서 요약”, 5월 2005년

[5] FREC, “Version 5 Critical Infrastructure Protection Reliability Standards”, https://www.ferc.gov/whats-new/comm-meet/2013/112113/E-2.pdf

[6] NERC, “2011 NERC Grid Security Exercise“,

After Action Report, 3월 2012년
[7] 지식경제부, “전력계통 신뢰도 및 전기품질 유지기준 (지식경제부고시 제2012-67호, 2012.3.26., 타법개정)”

〈저 자 소 개〉

사 진

김 성 호 (SungHo Kim)
정회원

2009년 2월 : 인하대학교 컴퓨터공학과 졸업
2012년 2월 : 인하대학교 정보통신공학과 석사
2012년 9월~현재 : ETRI 부설연구소 연구원
<관심분야> 스마트그리드 보안, 시스템보안, 네트워크 보안, 취약점 분석

사 진

김 신 규(Sinkyu Kim)
정회원

2000년 2월 : 연세대학교 기계전자공학부 졸업
2002년 2월 : 연세대학교 컴퓨터과학과 석사
2007년 8월 : 연세대학교 컴퓨터과학과 박사수료
2003년 12월~현재 : ETRI 부설연구소 선임연구원/실장
<관심분야> 스마트그리드 보안, 국가기반시설 보안, 취약점 분석

사 진

서 정 택 (JungTaek Seo)
종신회원

1999년 2월 : 충주대학교 컴퓨터공학과 졸업
2001년 2월 : 아주대학교 컴퓨터공학과 석사
2006년 2월 : 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 11월~현재 : ETRI 부설연구소 선임연구원/부장
<관심분야> 제어시스템 보안, 취약성 분석ㆍ평가, 스마트그리드 보안, 원자력 사이버 보안, DDoS 공격 탐지 및 대응