국가기반시설 정보보안 관리체계 프로그램 개발

배지효*, 이동선**, 전하정***,
*성신여자대학교 융합보안공학과
** 동덕여자대학교 컴퓨터학전공
***숙명여자대학교 컴퓨터과학전공
e-mail : bjh1460@naver.com, slsle144@naver.com, vane815@sookmyung.ac.kr

Development of an national infrastructure Information Security Management System Program

Jihyo Bae*, Dongsun Lee **, Hajeong Jeon***
*Dept. of Convergence Security Engineering, Sung-Shin Women's University
** Dept. of Computer Science, Dong-Duk Women's University
***Division of Computer Science, Sook-Myung Women's University

요 약

최근 국가기반시설을 대상으로 하는 사이버 공격이 증가하고 있다. 이에 따라 국내외에서는 시설의 침해영향도를 고려하여 자산을 분류하고 관리적/기술적/물리적 보안조치를 수행하도록 지침 및 정책을 제시하고 있다. 그러나 국내 지침은 자산 특성을 고려치 않아 운영 측면의 효율성을 저하하고 있다. 이에 본 논문은 기존 문서의 내용을 보완한 국가기반시설 정보보안 관리체계 프로그램을 제안한다.

1. 서론

국내의 국가기반시설은 재난 및 안전관리 기본법에 따라 재난이 발생할 경우 국가안전보장과 경제·사회에 미치는 피해 규모 및 범위를 고려하여 지정한다.[1] 이러한 국가기반시설의 장비들이 점차 아날로그에서 디지털로 변경되면서 기술적인 공격에 대한 공격 벡터가 증가하고 있다.[2] 이에 따라 국외에서는 *<RG 5.71>*와 *<NEI 08-09>*에 국가기반시설의 장비들을 보호하기 위한 지침을 규정하고 있다. 국내에서도 *<KINAC/RS-015>*를 통해 필수시스템과 필수디지털자산을 식별하고 기술적/관리적/운영적 보안조치 항목을 적용하여 위협에 대비하고 있다.

그러나 위 지침들은 자산의 특성을 고려하지 않은 보안조치 항목을 동일하게 적용하고 있어 운영적인 측면에서 효율성이 저하되고 있다.[3]

이에 본 논문은 기존 지침의 필수시스템 및 필수디지털자산 식별 알고리즘과 기술적 보안조치 항목을 보완하여 국내 국가기반시설에 적합한 프로세스를 제시하고, 아래의 목표를 충족하는 국가기반시설 정보보안 관리체계 프로그램을 제안한다.

첫째, 필수시스템(CS, Critical System)과 필수디지털자산(CDA, Critical Digital Asset)을 식별 및 분류하는 기능을 제공한다. 새로운 식별 기준을 수립하여 세부적으로 자산을 분류하고 이를 체계적으로 관리할 수 있도록 한다.

둘째, 기술적 보안조치 항목을 관리하는 기능을 제공한다. 자산의 특성을 반영한 점검 항목을 정하고 상세 내용을 매핑하여 자산에 따라 차등적인 보안조치를 수행한다.

마지막으로 기술적 보안성 평가를 통해 자산별 기술적 보안조치의 요건 만족 여부를 점검하고 요건을 만족하지 못하는 자산에 대해 추가적인 조치를 수행하여 사각지대를 해소한다.

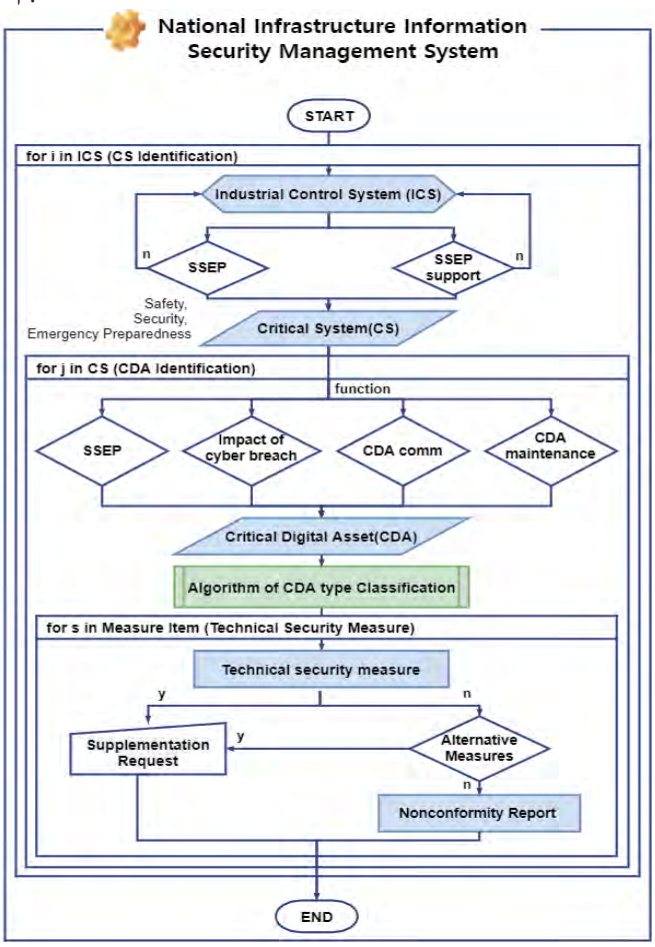
2. 국가기반시설 정보보안 관리체계 프로그램

2.1 프로그램 알고리즘

그림 1은 국가기반시설 정보보안 관리체계 프로그램의 전체 알고리즘이다. 프로그램은 세부적으로 필수시스템 식별(CS Identification), 필수디지털자산 식별(CDA Identification), 필수디지털자산 유형 분류(Algorithm of CDA type Classification), 보안성 평가(Security Evaluation) 단계로 진행된다.

필수시스템 식별(CS Identification) 단계는 국가기반시설의 산업제어시스템을 대상으로 수행한다. 산업제어시스템(ICS, Industrial Control System)이 안전(Safety), 보안(Security), 비상 대응(Emergency Preparedness) 기능, 즉 SSEP 기능을 수행하거나 필수시스템의 SSEP 기능을 지원하는 경우, 필수시스템(CS)으로 식별한다. 안전 기능(Safety)은 원자력 발전소의 원자로, 터빈 등의 안전성을 유지하고, 보안 기능(Security)은 물리적 방호를 유지하며, 비상 대응 기능(Emergency Preparedness)은 방사선적 영향을 일으키는 사고 및 사건에 대응하기 위한 기능으로 원자력 시설에 직접적인 영향을 끼칠 수 있는 설비들을 필수시스템(CS)으로 식별하고 있

다.



(그림 1) 국가기반시설 정보보안 관리체계 프로그램 알고리즘

필수디지털자산 식별(CDA Identification) 단계는 필수시스템(CS)의 디지털자산(Digital Asset)을 대상으로 아래의 네 가지 특성 중 해당하는 항목이 있을 경우, 필수디지털자산(CDA)으로 식별한다.

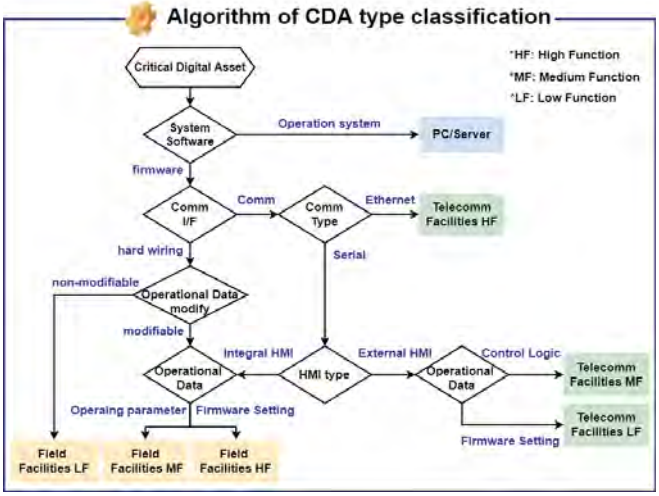
A. SSEP(Safety, Security, Emergency Preparedness) 기능
B. 사이버공격 침해 시 영향(Impact of cyber breach)
C. 필수디지털자산과 통신 연결 기능(CDA comm)
D. 필수디지털자산 유지 보수 기능(CDA maintenance)

식별된 필수디지털자산은 유형 분류 알고리즘(Algorithm of CDA type classification)을 거쳐 필수디지털자산의 유형을 분류하게 된다. 해당 알고리즘은 2.2 필수디지털자산 유형 분류 알고리즘에서 상세히 설명한다.

보안성 평가(Security Evaluation) 단계는 필수디지털자산 유형에 따라 기 등록한 기술적 보안조치 항목의 수행 여부를 순차적으로 확인한다. 해당 필수디지털자산이 기술적 보안조치 요건을 모두 만족하는 경우, 보안성 평가를 완료한 것으로 처리한다. 이때, 보완요청 사항(Supplementation Requests)을 작성하여 추가적인 조치를 이행할 수 있다. 기술적 보안조치 항목을 하나라도 만족하지 않으면 각 항목에 1 대 1로 매핑되는 대안조치(Alternative Measures) 수행 여부를 확인하여 이를 수행한 경우에는 위와 동일하게 보안성 평가를 완료한 것으로 처리한다. 대안조치를 수행하지 않은 경우에는 부적합 보고서(Nonconformity Report)를 필수적으로 작성하여 필요한 조치 내용을 기간 내에 이행할 수 있도록 한다.

위 과정을 통해 보호 대상인 필수디지털자산을 식별하고 최소한의 보안 요구 사항을 충족할 수 있도록 체계적으로 관리한다.

2.2 필수디지털자산 유형 분류 알고리즘



(그림 2) 필수디지털자산(CDA) 유형 분류 알고리즘

기존 *<NEI 13-10>*에서 제시하고 있는 알고리즘은 자산이 수행하는 기능을 기준으로 유형을 구분한다. 6개의 유형을 A와 B로 구별하고, 같은 범주 내에서는 번호로 구별하고 있다. 이는 자산의 기능을 반영하지 않는 방식으로 용어를 통해 의미를 파악하기 어렵다.

본 논문에서는 자산의 특성과 기능을 고려하여 자산 유형을 칭하는 용어를 정의하였다. 이에 따라 필수디지털자산의 유형을 분류하는 알고리즘에 분기점을 수정 및 추가하여 제안한다.

그림 2 알고리즘의 첫 번째 분기점은 System Software의 종류로 OS(Operating System)과 firmware로 분류된다. OS를 운용하는 PC/Server 자산 유형을 추가하여 많은 공격 벡터가 있는 자산에 대해 적절한 기술적 보안조치를 수행하도록 한다. 이외의 자산은 Firmware이며, 해당 자산을 분류하는 분기점인 Communication Interface 방식에 따라 자산 유형의 용어를 크게 2개로 정의하였다. Communication 방식은 설비들이 중간 매개체를 이용한 간접 연결 방식(indirect connection)이라는 점을 반영하여 Telecommunication Facilities로 정의하였다. Hard wiring 방식은 대상 설비와 이를 제어하는 설비가 일 대 일로 연결되는 직접 연결 방식(direct connection)이며 현장에서 제한적으로 사용할 수 있

으므로 Field Facilities(현장 설비)로 정의하였다. 같은 범주에 있는 자산은 세부 기능을 수행하는 범위에 따라 HF(High Function, MF(Medium Function, LF(Low Function)로 정의한다. Telecomm Facilities(통신 설비)는 Comm type 분기점에서 Ethernet과 Serial 방식으로 나누어진다. Ethernet 통신을 하는 설비는 Telecomm Facilities HF로 분류한다. Serial 통신 설비는 HMI type 분기점이 External HMI일 때, Telecomm Facilities MF, LF로 분류한다. Operational Data 분기점에서 Control Logic을 수정할 수 있으면 Telecomm Facilities MF, Firmware Setting이 가능하면 Telecomm Facilities LF로 분류한다. Field Facilities는 Operational Data modify 분기점에 의해 non-modifiable이면 Field Facilities LF로 분류한다. modifiable 설비는 Integral HMI를 통해 Operational Data 분기점에서 Operating parameter를 변경할 수 있으면 Field Facilities MF, Firmware Setting을 수정할 수 있으면 Field Facilities HF로 분류한다.

위 알고리즘을 통해 필수디지털자산의 유형을 세부적으로 분류함으로써 상대적으로 공격 벡터가 많은 자산에 적절한 기술적 보안조치를 적용하여 보안성을 제고할 수 있다.

2.3 필수디지털자산 유형별 기술적 보안조치 수행

기존 지침의 기술적 보안조치 항목은 산재되어 있어 내용이 복잡하고 효율성이 저하되고 있다.

본 논문에서는 <*KINAC/RS-015*>의 기술적 보안조치 항목을 다음과 같은 4가지 대분류로 정의하고 점검 상세 내용을 분류하였다. 필수디지털자산의 유형과 점검 항목은 1:N 관계이다.

- 계정 및 권한 관리
- 접근 통제 및 인증
- 로그관리 및 추적
- 시스템 및 통신 보안

1.1.12 네트워크 접근 통제(점검 항목)
가. MAC(Media Access Control) 주소 잠금
나. 물리적 혹은 논리적 네트워크 분리
다. 정적 테이블 주소 유지
라. 패스워드 등 중요정보 전송 시, 암호화
마. 모니터링

1.1.12 네트워크 접근 통제 (상세 내용)
가. MAC(Media Access Control) 주소를 변경할 수 없게 고정
나. 물리적 스위치 또는 VLAN 기술을 사용하여 이더넷 트래픽 분리
다. ARP Table을 정적으로 고정하여 ARP Cache Poisoning 공격 방지
라. 인가된 사용자만이 정보에 접근, 주요 정보를 암호화하여 MITM(Man-in-the-Middle) 공격에 대응
마. 지속적인 모니터링을 통해 악의적인 접근 감시

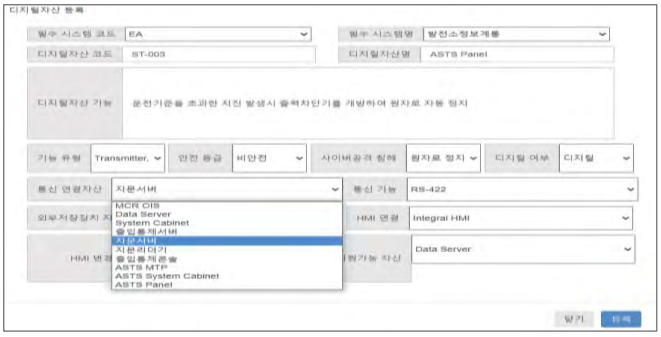
1.1.12 네트워크 접근 통제 (대안조치)
기술적 및 물리적 접근 통제를 수립하여 이행하고, 주기적인 감사를 통해 취약점 분석을 수행하여 위협을 제거한다.

(그림 3) 기술적 보안조치 항목 예시

그림 3은 <*KINAC/RS-015*>의 한 항목을 발췌하여 점검 분류를 「접근 통제 및 인증」로 정의하고 점검 상세 내용과 대안조치를 작성한 것이다.[4] 해당 항목은 TCP/IP 프로토콜 또는 NAC(Network Access Control)를 통해 네트워크에 접근하는 자산에 적용할 수 있는 내용이다. 즉, Ethernet 방식으로 통신하는 PC/Server, Telecomm Facilities HF 자산이 수행해야 하는 항목이다. 이러한 필수디지털자산의 유형별 특성을 고려한 기술적 보안조치 항목의 적용은 불필요한 과정을 제거하여 효율성을 높일 수 있다. 또한 관리자가 항목을 등록하여 새롭게 등장하는 사이버 위협에 대비할 수 있다. 이는 필수디지털자산에 영향을 미칠 수 있는 취약점을 제거하고 안전하게 관리하기 위함이다.

3. 프로그램 구현 결과

(그림 4) 필수시스템(CS) 식별 및 등록 화면



(그림 5) 필수디지털자산(CDA) 식별 및 등록 화면

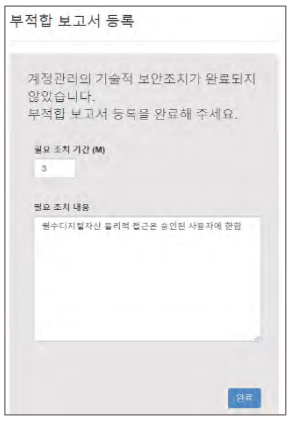
그림 4는 산업제어시스템 조회 화면에서 등록 버튼을 선택하면 나타나는 필수시스템 등록 화면이다. 이때, 필수시스템 식별 기준에 따라 필수시스템(CS)과 비필수시스템(Non-CS)으로 식별한다.

그림 5는 디지털자산 조회 화면의 등록 버튼을 선택하여 필수디지털자산을 등록하는 화면이다. 드롭다운 메뉴에서 필수시스템을 선택하면 해당 필수시스템의 디지털 자산이 선택된다. 자산의 특성과 수

행 기능을 선택하면 필수디지털자산(CDA)과 비필수디지털자산(Non-CDA)으로 식별하고 유형을 분류하여 등록한다.

(그림 6) 필수디지털자산 보안성 평가 등록 화면

그림 6은 보안성 평가 조회 화면에서 각 필수디지털자산 행의 등록 버튼을 선택하면 나타나는 화면으로 필수디지털자산의 보안성 평가를 수행한다. 해당 화면에서는 기 등록한 기술적 보안조치 항목과 대안조치 수행 여부를 체크리스트 방식으로 확인하고 추가적으로 수행할 점검 내용을 작성할 수 있다. 이때, 기술적 보안조치 항목이 Yes일 경우, 대안조치 항목은 disable 되어 선택할 수 없다.



(그림 7) 부적합 보고서 등록 화면

(그림 8) 부적합 보고서 추적 화면

그림 7은 위의 기술적 보안조치와 대안조치를 완료하지 못한 항목이 있을 때 나타나는 부적합 보고서 등록 화면이다. 부적합 내용을 해소하기 위해 필요한 조치를 작성할 수 있다.

그림 8은 기술적 보안조치 항목과 대안조치를 만족하지 못한 자산을 대상으로 발행한 부적합 보고서를 관리하는 화면이다. 각 필수디지털자산의 조회 버튼을 통해 부적합 내용과 필요 조치 등에 대한 상세 내용을 조회 및 수정할 수 있다. 필요한 조치를 모두 이행한 자산에 대해 완료 컬럼의 '미완료'를 선택하면 '완료' 로 변경되어 지속적으로 추적 및 관리할 수 있다.

4. 결론

국가기반시설을 대상으로 국가발 사이버 공격이 증가하여 범국가적인 피해가 우려되고 있다. 이에 따라 국내 상황을 고려한 지침의 필요성이 대두되고 있다.

본 논문에서는 기존 문서의 문제점을 제시하고 이를 보완하는 알고리즘 및 프로세스를 제안한다. 해당 프로그램의 기대효과는 다음과 같다. 첫 번째, 자산의 특성을 반영한 유형 분류 알고리즘을 제안하여 자산을 효율적으로 관리할 수 있다. 두 번째, 산재된 기술적 보안조치 항목들을 통합할 수 있는 기준을 제시하여 자산별로 적합한 조치를 수행한다. 이는 상대적으로 공격 벡터가 많은 자산은 기술 보안성을 제고하고, 적은 자산은 최소한의 보안성을 충족시키며 불필요한 처리를 방지할 수 있도록 한다. 세 번째, 자산별로 추가적인 조치 사항을 작성하여 보안성이 결여된 자산의 사각지대를 해소할 수 있다. 또한 자산의 변경 사항을 지속적으로 추적할 수 있다. 이러한 프로세스는 관리자의 편리성을 증진시키고 국가기반시설의 체계적인 관리를 통해 기술적 보안성을 강화할 수 있을 것으로 기대된다.

5. 참고 문헌

[1] 재난 및 안전관리 기본법 제26조 제1항
[2] 최윤혁, 이상진, "원자력시설의 필수디지털자산에 대한 기술적 보안조치항목에 대한 연구, 한국정보보호학회, 제29권, 제4호, 877-884, 2019.
[3] 김인경, 변예은, 권국희, "원전디지털자산 사이버보안 규제 요건 개발을 위한 보안조치 적용 방안에 대한 분석, 한국정보보호학회, 제29권 제5호, 1077-1088, 2019.
[4] 김나영 외, "원자력시설 사이버보안 규제기준 측면의 기술적 보안조치에 대한 이행방안 연구", 한국정보보호학회, 제27권 제2호, 57-68, 2017.

본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.