https://doi.org/10.33778/kcsa.2024.24.3.003

단독망 자료유출 방지를 위한 정보자산 인증 방안

김 일 한*, 이 주 승**, 김 현 수**

요 약

정보보호는 외부 사이버공격으로부터의 보호와 더불어 내부자료 유출 위험요인을 사전에 식별하여 차단하는 것이 중요하다. 이를 위해 많은 기업과 기관에서는 자료(파일) 자체를 암호화해 외부로 유출 시 내용확인을 불가능하게 DRM(Digital Rights Management) 문서보안 솔루션과 전산장비의 USB포트 등 매체제어를 통해 데이터 유출방지를 위한 DLP(Data Loss Prevention) 솔루션을 대표적으로 운용하고 있다. 이와 같이 내부 자료유출 방지 노력이 중요한 시점에서 관리 사각지대에 놓일 수 있는 단독망 환경의 정보자산 식별과 매체제어와 같은 통제정책 운용이 요구된다. 본 연구에서는 내부 업무망에도 연결되지 않는 단독망 정보자산의 인증을 통해 해당 정보자산에 유일하게 적용되는 매체통제정책 생성-배포-적용 모델을 제시하였으며, 이를 위해 정보자산 획득 시 자동으로 등록되는 자산관리시스템 정보와 연계한 인증기법을 개발하여 정확한 정보자산 식별 및 유연한 매체통제가 가능한 시스템을 설계 및 구축하였다.

Information Asset Authentication Method for Preventing Data Leakage in Separated Network Environments

Ilhan Kim*, Juseung Lee**, Hyunsoo Kim***

ABSTRACT

Information security is crucial not only for protecting against external cyber-attacks but also for identifying and blocking internal data leakage risks in advance. To this end, many companies and institutions implement digital rights management(DRM) document security solutions, which encrypt files to prevent content access if leaked, and data loss prevention(DLP) solutions, which control devices such as USB ports on computing equipment to prevent data leaks. At a time when efforts to prevent internal data leaks are crucial, there is a growing need for control policies such as device control and the identification of information assets in standalone network environments, which could otherwise fall into unmanaged domains. In this study, we propose a Generation-Distribution-Application model for device control policies that are uniquely applied to standalone information assets that are not connected to internal networks. To achieve this, we developed an authentication technique linked with the asset management system, where information assets are automatically registered upon acquisition. This system allows for precise identification of information assets and enables flexible device control, and we have designed and implemented a system based on these principles.

Key words : Data Loss Prevention, Digital Rights Management, Information Asset Authentication, Isolated Network

접수일(2024년 08월 19일), 수정일(1차: 2024년 09월 09일), (2차: 2024년 09월 20일), 게재확정일(2023년 09월 23일)

* 국방과학연구소(주저자)
** 국방과학연구소

1. 서 론

산업의 고도화와 IT 기술의 발전으로 국가 경쟁력이 향상되고 공공 연구기관과 기업에서도 첨단 기술 보유 비중이 지속적으로 증가하고 있으나 산업기술 자료의 무단유출에 의한 경제적 피해 또한 증가하고 있다. 이와 같이 첨단 산업기술 유출 방지를 위해서는 국가차원의 정부정책과 관련 정보보호 기술연구가 필요하다[1]. 특히 방위산업분야에서는 무기체계 연구개발 등 첨단 기술자료 유출 시 국가적 손실로 이어지기 때문에 방위산업기술 보호법을 제정하여 체계적인 기술 보호대책 및 절차를 지원하고 있다.

방위산업기술 보호체계의 하나로 방위산업기술 정보에 접근하는 시스템 및 컴퓨터 등에 외부망 접속 차단 체계를 요구하고 있으며[2], 이에 따라, 정보보호 부서에서는 외부로부터의 접근 보안성이 높은 망분리 환경을 구축하여 방위산업기술 정보에 대한 보호체계를 유지하고 있다. 주요 업무로는 외부 인터넷을 통한 사이버침해시도 차단과 망분리 환경의 내부 업무망에 연결되어 있는 EndPoint 정보자산을 대상으로 정보보호 활동을 수행하고 있으며, 이외에 내부 업무망에도 연결되지 않는 시험용도 등의 단독망 정보자산에 대한 정보보호 활동 또한 전문적인 관리가 필요하다. 단독망 정보자산의 경우 저장매체 통제가 중요한 만큼 본 논문에서는 내부 업무망의 자료유출방지시스템과 연계하여 단독망 정보자산 별로 유연한 매체통제정책 생성을 위한 정보자산 인증 기법을 제안한다.

본 논문의 구성은 2~3장에서 정보자산 관리환경 분석 및 자료유출방지시스템에 대한 기술동향과 상용 솔루션 기능에 대해 살펴보고 4장에서 단독망 환경의 정보자산 인증 방안과 보안규정을 충족할 수 있는 기술을 검토하여 시스템 설계를 제시한다. 5장에서는 단독망 정보자산 인증을 통해 생성된 매체통제 정책의 동작 검증 및 기존 솔루션과 비교를 통해 본 연구의 시사점을 제시하고 6장에서 결과에 대해 논의한다.

2. 관련 연구

2.1 정보자산 관리

정보자산은 업무수행을 지원하는 모든 일련의 대상이라고 할 수 있으며, 한정된 인력과 자원으로 기업의 핵심정보 보호를 위해서는 중요 정보자산을 식별하고 그에 따른 정보보호 대책이 수립되어야 한다[3][4].

정보자산 관리는 보유 정보자산과 관련된 모든 변경 이력정보, 획득비용, 계약자료 등의 자료를 관리하는 것으로 IT 자산관리와 PC 자산관리로 구분할 수 있으며 자산의 현재 상태, 지속적인 서비스 요구수준, 어느 자산의 위험(중요) 여부, 최적의 운영관리 전략 및 자금투자 계획, 최적의 장기적 자금전략 5가지 요소의 검토가 필요하다[5]. 세부적으로는 하드웨어, 소프트웨어, 미들웨어, 기반시설, 네트워크, OA기기 등으로 분류할 수 있으며, 체계적인 관리를 위해 종류별, 목적별 등의 관리항목과 타 시스템과의 연계까지 고려한 자산분류체계에 기반하여 관리되어야 한다[6]. 이를 위해 범정부 EA(Enterprise Architecture)에서도 정보자산의 도입·운영·개선·폐기 및 평가 등 정보자산 관리 업무를 명시하고 있으며, 체계적인 관리를 위해 정보자산관리시스템(IT Asset Management System) 구축을 통해 자산정보 추적 수준을 넘어 IT Governance 의사결정에 필요한 정보를 제공하고 있다[5][7]. EA와 ITAM의 주요개념을 요약하면 <표 1>과 같다.

<표 1> EA 및 ITAM 비교[8][9][10]

구분	EA	ITAM
정의	조직의 비즈니스, 관리 프로세스, 정보기술 구성요소 간 상호연계에 대한 현재와 목표의 명시적인 기록	경영목표 달성을 위해 조직의 IT자원 및 연계된 데이터의 전수명주기를 관리하는 체계 및 기법
필요성	정보자원에 대한 공유 및 중복투자 방지 효율적인 관리체계 구축을 통한 통합적인 관리	외부의 규제강화·비용상승·생산성 약화 개선을 위한 IT 자산관리 체계화 및 투명성 강화
주요기능	업무·데이터·응용·기술 아키텍처 정의	자산이력관리, 재무관리, 구매 및 계약관리 업무 지원
기대효과	IT Governance 의사결정 지원 IT 정보의 일관성, 정확성, 적시성 향상	전사 자원의 파악 및 관리를 통한 중복투자 방지 IT Governance 자원관리체계 구축

2.2 단독망 정보보호 솔루션 운영 환경

단독망 정보자산은 온라인상의 Server-Agent에 의해 통제가 불가하여 SW 설치를 위해 USB 등을 통해 별도로 설치하여 운영된다. 외부망에서 단독망으로 SW 반입 시 고려해야할 사항으로 SW 패키지의 보안 취약점을 사전에 식별 할 수 있는 단독망 전용의 패키지 관리 도구 개발과 Read-Only 상태를 지원하는 저장장치를 이용한 반입, 단독망 내의 패키지에 대해서도 주기적인 백업, 패키지의 업그레이드/다운그레이드 패치에 대한 일괄처리 방안이 필요하다[11]. 이와 같이 외부 SW 반입 시에도 보안대책을 준수하여야 하며, 단독망 정보자산의 내부자료 유출 방지를 위해 USB 포트 등 매체제어 기능을 수행하는 자료유출방지시스템, 문서암호화시스템 및 백신 등의 정보보호 솔루션을 운영하고 있다. 하지만 단독망 환경 특성상 정보보호 솔루션의 사용자 로그인 인증이나 통제정책을 온라인상에서 실시간으로 인증 및 갱신 할 수 없어 일반적으로 동일한 통제정책이 적용되도록 Agent를 설계한다. 예를 들어 단독망 정보자산 매체통제정책에 대해 USB 포트만 허용하고, 그 외의 모든 포트는 차단하는 등의 일괄적인 정책을 적용한다. 이후 예외정책이 필요한 경우 솔루션 제조사를 통해 별도의 기술지원으로 서비스가 가능하다. 이 경우 모든 단독망 정보자산의 인증 정보가 동일하여 자료유출 등의 문제 발생 시 사후 로그 추적 등 데이터 분석이 요구되는 경우 실제 사용자와 정보자산을 특정하기에 제한이 있어 정보보호 시스템의 관리적 역할을 충족하기 어렵게 된다. 이러한 단독망 환경의 제약사항을 위한 단독망 내부자료 유출방지 대책이 필요하다.

3. 자료유출 방지 기술 및 시스템 동향

3.1 자료유출 방지 기술 동향

자료유출 방지 기술(Data Loss Prevention)은 조직 내부 정보와 같은 민감정보, 기술정보 등 보호되어야 할 자료의 무단 유출을 차단하는 기술이다. [12]의 연구에서는 자료유출의 경로 및 취약점으로 보조기억매체(USB, CD, DVD 등) 이용, 무선통신과 같은 자료전송장치 이용, 자료암호화(Digital Rights Management) 해제 취약점, 보안프로그램 프로세스의 서비스 임의종료 취약점, OS의 안전모드 진입 취약점, 가상화 솔루션 자료유출 보안취약점, PC 부팅 직후 시간차 우회 취약점, 자료 확장명 변경 등을 제시하며 이러한 취약점으로부터 안전한 자료유출방지 시스템 운영을 위해 CD나 USB를 통한 부팅 차단, PC 본체의 잠금장치 설치, 보안 관리자의 시스템 기능 교육, 안전한 장소에서 관리서버 운영, 감사로그 저장 공간 확보 방안을 제안하고 있다. [13]의 연구에서도 개인정보와 같은 민감정보나 내부 기밀파일에 시그니처를 삽입하고, 이를 USB에 이동 및 저장 시 시그니처를 탐지하여 유출을 차단하고 로그 증적을 통해 향후 유출사고 조사 시 활용될 수 있는 시스템을 제안하고 있다. 이와 같이 온·오프라인 상에서 내부 자료유출 경로 및 방법은 <표 2>와 같이 요약할 수 있으며, 이와 더불어 단독망 환경의 자료유출방지를 위한 정보보호시스템 통제정책 운영에 대한 연구가 필요하다.

<표 2> 자료유출 경로 및 방법

구분	자료유출 경로	자료유출 방법
온라인	웹메일, 웹사이트, FTP, SNS 등	내용 및 파일 온라인 전송 등
오프라인	전산장비, 저장매체 연결 등	장비, 저장매체, 출력물 반출 등

3.2 자료유출 방지(DLP) 시스템 동향

자료유출방지시스템은 자료유출 방지를 위해 데이터 및 탐지규칙의 일치 여부와 같은 특정 패턴 탐지기술에 기반하여 EndPoint 정보자산에서 자료전송, 자료사용, 민감 데이터를 탐지하는 기술이다. 즉, 이메일, 웹사이트, 보조기억매체, 클라우드 앱 등을 통해 발생할 수 있는 민감 데이터의 유출을 사전에 차단하는 것이라 할 수 있다[14]. 자료유출방지시스템의 평가기준 요소로는 소스코드의 취약점을 이용하여 보안정책을 우회할 수도 있으므로 내부 소스코드의 보호 수단이 필수적인 요구사항이라고 할 수 있다[15]. 또한 트래픽 용량과 관계없이 이상 패턴탐지 및 정확한 작동과 네트워크 및 EndPoint 탐지 기능, 정책설정, 그룹별 접근권한 설정지원, 정책의 적용 용이성, 탐지증거 증적 등을 들 수 있다[16].

A사의 솔루션은 비인가자 및 자료 생산자의 악의적인

정보유출 차단과 유출 가능성을 사전에 근절하기 위해 중앙집중 통합보안 관리 메커니즘으로 기업에 일관성 있는 보안정책 수립과 관리를 지원하고 있다. 웹메일, 웹하드, 웹게시판, FTP, 메신저, P2P, SNS 등 온라인 보안과, USB 메모리, 휴대폰, CD/DVD 같은 오프라인 보안, 사용자 PC의 보안설정을 통제하는 PC보안, 개인정보 유출 통제, 로그 감사기능 등을 수행하는 통합 EndPoint 자료유출방지 기능을 제공하고 있다[17].

B사는 암호화된 패킷의 복호화를 통한 전송 데이터에 개인정보, 기밀정보의 전송차단과 로그증적을 통해 SSL 통신의 트래픽을 처리하는 네트워크 DLP와 맥 OS, 리눅스 OS를 지원하는 EndPoint DLP, 서버 내의 취약점 점검, 악성코드 차단, 개인정보/기밀정보 유출 통제 기능을 제공하는 서버군 DLP 제품을 제공하고 있다[18][19][20].

C사의 솔루션은 통합 PC보안 솔루션으로 정보유출 방지, 민감정보 관리, 웹/소프트웨어 차단, PC취약점 점검, IT 자산관리, 문서백업, 출력물 보안 7가지 보안 이슈에 대한 서비스를 제공하고 있으며, 정보유출방지 기능에서는 이동식 저장매체 차단, 인터넷 파일첨부 차단, 메신저, 웹하드 등을 통한 소프트웨어 파일반출 차단, 무선 인터넷 접속 차단, 화면캡처/공유폴더 차단, 로그 및 원본저장의 기능을 지원하고 있다[21]. 이와 같이 상용 시스템의 주요기능은 <표 3>과 같이 요약할 수 있으며, 중앙 집중·통합형의 관리로 온라인상의 관리시스템에 의한 운영을 기본으로 하고 있으나 본 논문에서 제안하는 정보자산 인증 기법은 정보자산 별 고유한 인증 값을 추출 후 내부 업무망의 자료유출방지시스템과 연계하여 인증을 통해 사용자와 정보자산을 연계하여 단독망 정보자산별로 맞춤형 통제정책을 제공 한다.

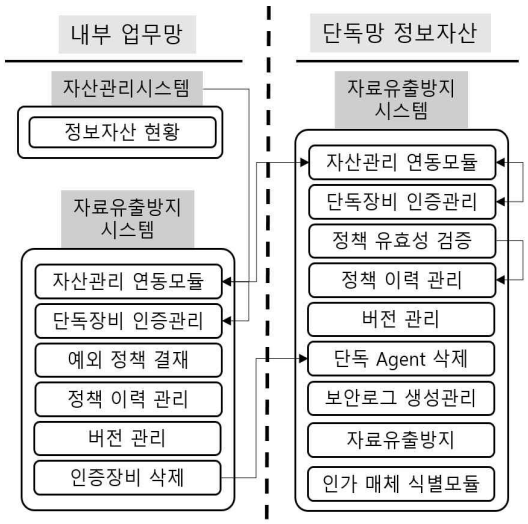
<표 3> 상용 시스템 주요기능 비교

구분	주요기능
A사	온·오프라인 보안, PC 보안, 개인정보 보안, 보안관리 및 감사
B사	네트워크 보안, EndPoint 보안, 서버 보안
C사	정보유출방지, 민감정보관리, 웹/소프트웨어 차단, PC 취약점 점검, IT자산관리, 문서백업, 출력물 보안

4. 단독망 정보자산 인증 설계

4.1 시스템 구성

단독망 정보자산의 내부자료 유출 방지를 위하여 매체통제를 수행하는 자료유출방지시스템과 자산관리 시스템을 연계하여 정보자산의 인증을 수행하고 인증 여부에 따라 USB 포트 등 매체제어 통제정책을 생성-배포-적용을 통해 통제정책 이외의 수단으로 내·외부자의 정보유출을 사전에 차단한다. 이 인증정보는 보안저장매체관리시스템과 같은 타 솔루션에 API를 통해 제공이 가능하여 여러 활용 용도가 있다. 내부 업무망의 자산관리시스템, 자료유출방지시스템, 단독망 자료유출방지시스템까지 시스템 구성은 (그림 1)과 같다.



(그림 1) 시스템 기능 구성도

4.2 자료유출방지시스템을 통한 단독망 정보자산 인증관리

단독망 정보자산은 내부 업무망과 단절되어 운영되는 장비로서 담당자 변경이나, 자료유출방지시스템 통제정책 등의 변경이 있을 시 내부 자산관리시스템에서 업데이트된 정보 및 정책이 단독망 정보자산에는 업데이트가 연계되지 않는 단절이 있다. 이는 물리적 망분리 환경의 특성상 정보자산의 관리적 측면에서 정보의 불일치와 같은 데이터 정합성에 취약하다고 할 수 있

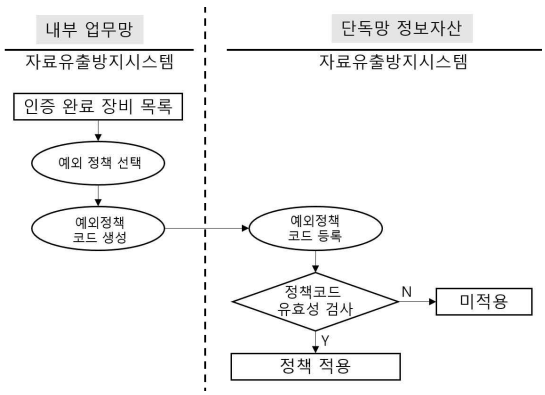
다. 이를 위해 단독망 정보자산 Machine-ID 등의 식별자를 통해 인증코드를 생성하여 내부 업무망의 자료유출방지시스템에 인증 코드를 등록하고 자산관리시스템과 연계하여 인증한다. 자산인증이 완료되면 단독망 정보자산 활성화 코드가 생성되며 이 코드를 단독망 정보자산에 입력하면 기본 통제정책으로 활성화 된다. 인증 코드와 활성화 코드는 <표 4>와 같은 정보로 구성되어 있으며, 자료유출방지시스템을 통한 단독망 정보자산 인증 흐름은 (그림 2)와 같다.

<표 4> 자료유출방지시스템 인증 구성 요소

인증 코드	정책 발급을 위한 Machine-ID 등 식별자
활성화 코드	정보자산식별번호, 서버시간, 등록코드

4.3 단독망 정보자산 예외정책 적용

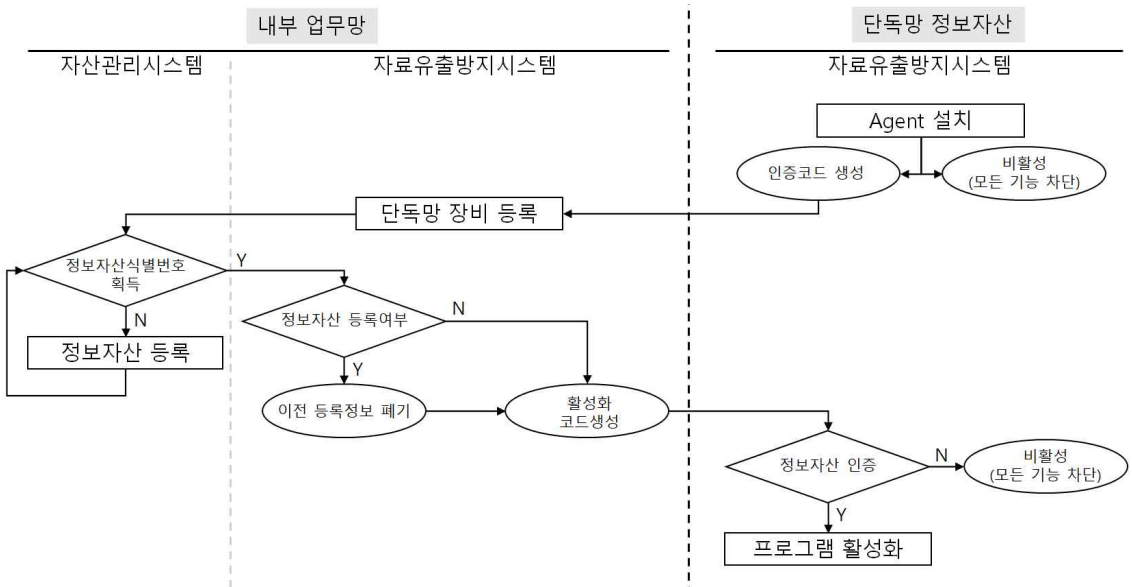
단독망 정보자산에 자료유출방지시스템 Agent가 설치되면 매체제어 등의 통제정책이 활성화되어 USB 포트, 인터넷 연결 등 모든 매체가 차단된다. 다만, 차단된 기능 중 허용이 필요한 경우 그림(3)과 같은 절차로 단독망 정보자산에 예외정책을 적용할 수 있다. 내부 업무망 자료유출방지시스템에서 단독망 정보자산



(그림 3) 단독망 정보자산 예외정책 적용 흐름도

에 대한 예외정책 코드를 생성하고 해당 코드를 단독망 정보자산에 등록을 통해 예외정책을 활성화 시켜 USB 포트 등 차단된 기능을 사용할 수 있다.

예외정책 적용 대상 단독망 정보자산의 자료유출방지시스템 Agent는 해당 정책 적용을 위해 정보자산식별번호 일치여부, 인증만료 여부, 정보자산의 날짜 및 시간 일치여부, 정책의 중복사용 여부를 확인하여 유효성 검사를 수행한다. 내부 업무망에서 발급된 예외정책은 사용자 기준이 아닌 정보자산식별번호를 기준으로 생성되며 단독망 자료유출방지시스템에 인증된



(그림 2) 단독망 정보자산 인증 흐름도

정보자산식별번호가 일치하지 않거나 장비사용 인증 기간이 만료된 경우 해당 정책을 등록하지 않고 폐기 처리한다. 예외정책 발급 시 해당 정책의 유효기간을 설정하게 되며, 해당 기간은 내부 업무망의 서버 시간을 기준으로 정책이 생성된다. 그러나 정책 사용대상인 단독망 정보자산의 경우 날짜 및 시간 관리는 OS 자체적으로 설정되고, 이는 사용자의 임의 변경이 가능하게 되며, 내부 업무망 서버와의 일치 여부를 보장할 수 없게 된다. 따라서 내부 업무망에서 예외정책이 발급될 때 정책의 최대 유효기간을 설정하여 해당 기간 내에 있는 경우 정책의 사용을 가능하게 하고, 정책 유효기간이 벗어난 경우 해당 예외정책은 폐기된다. 이와 더불어 예외정책 코드는 내부 업무망에서 결재를 통해 일회성 사용을 기준으로 발급된다. 단독망 정보자산의 날짜 및 시간은 사용자가 임의 변경이 가능함에 따라 계속적으로 재사용이 가능하여 일회성 사용 기준 원칙을 우회할 수 있는 문제가 발생할 수 있다. 따라서 내부 업무망에서 해당 예외정책에 대한 정책관리 번호를 추가 요소로 적용하여 단독망 정보자산의 시간 및 날짜 변경에 따른 정책 우회 취약점에 대한 방어 방안을 마련하고 단독망 자료유출방지시스템 Agent에서는 등록하여 사용했던 등록코드의 이력 관리를 통해 정책에 대한 중복사용을 방지할 수 있도록 한다.

5. 시스템 구현

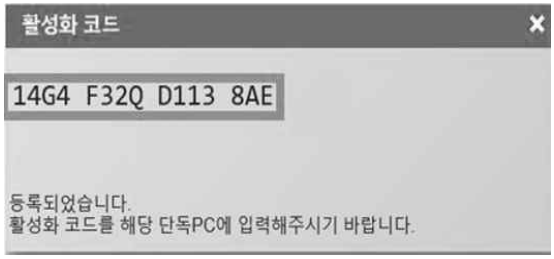
5.1 단독망 정보자산 인증

단독망 정보자산에 단독망 자료유출방지시스템 Agent를 설치하면 모든 매체를 차단하며, (그림 4)와 같이 가장먼저 PC 인증을 요하고 있다. PC 인증은 단독망 정보자산의 Machine-ID와 같은 고윳값을 이용하여 인증코드를 생성하며, 이 인증코드를 (그림 5)와 같이 내부 업무망의 자료유출방지시스템에 정보자산 소유자 정보, 자산관리시스템의 정보자산 식별번호를 입력함으로써 인증이 완료된다. 정보자산식별번호는 내부 업무망의 자산관리시스템과 연계되어 자산 소유자 사번에 등록된 정보자산등록 번호를 자동으로 선택하여 등록할 수 있다.

(그림 4) 단독망 정보자산 인증코드 생성화면

(그림 5) 단독망 정보자산 등록화면

단독망 정보자산이 내부 업무망 문서유출방지시스템에 정상적으로 인증이 완료되면 (그림 6)과 같이 기본 통제정책을 내장한 활성화 코드가 생성되고, 이 코드값을 단독망 정보자산에 등록하면 해당 단독망 정보자산은 인증 및 활성화 과정이 완료된다.



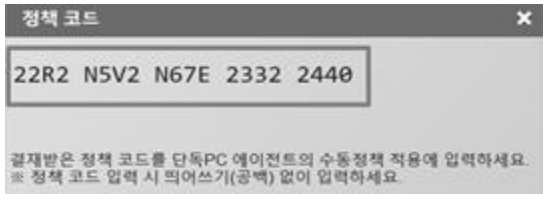
(그림 6) 단독망 정보자산 활성화 코드 생성화면

(그림 7) 단독망 정보자산 예외정책 신청 화면

5.2 예외정책 신청-생성-적용

단독망 정보자산이 등록된 이후 해당 단독망 정보자산에서 USB포트, CD 등 접속허용이 필요한 경우 내부 업무망 자료유출방지시스템의 (그림 7) 화면에서 예외정책 신청 및 승인요청을 거쳐 승인이 완료되면 신청된 예외정책이 (그림 8)과 같이 20자리 코드 값으로 생성 된다. 이 코드 값을 단독망 정보자산의 자료유출방지시스템에 수동으로 등록하면 코드에 기록되어 있는 예외정책이 활성화되어, 해당 단독망 정보자산은 USB 포트 등 예외허용 된 정책에 대해 차단이 해제된다. 예외정책 코드에는 예외허용 항목정보, 단독망 정보자산식별번호, 예외정책 적용기간 등의 정보를 포함하고 있다. 이 일련의 과정은 (그림 1)의 정책이력관리, 버전관리, 보안로그생성관리 모듈에 의해 모두 암호화된 형태로 특정 영역에 저장되어 저장매체로 이동-복사 등의 모든 로그를 기록한다.

이와 같이 상용 자료유출방지시스템에서는 추가 개발을 통해 별도의 예외정책을 제공하는 방식에서 단독망 정보자산의 Unique한 고윳값을 통해 인증을 거쳐 해당 정보자산 별로 필요한 통제정책을 유연하게 생성할 수 있고 신속하게 적용하여 자료유출방지시스템의 운영 편리성을 개선하였다.



(그림 8) 예외정책 코드 생성화면

6. 결론

민간과 공공부문에 구분 없이 제품 기술도면, 연구개발 산출물, 실험데이터, 개인정보, 계약서류 등 내부 민감 자료 보호의 중요성은 금전적인 문제 외에도 국제관계 문제까지 확대될 수 있는 중요한 사안이다. 내·외부자에 의한 자료 무단유출방지를 위해서는 정책적, 기술적, 관리적 수단의 조화를 통한 내부통제와 사용 불편 개선을 위한 시스템 편의성 또한 지속적인 연구가 필요하다. 상용 자료유출방지시스템에서도 단독망 정보자산의 자료유출 방지를 위해 매체통제 정책을 일부 지원하는 것으로 확인되었으나, 본 연구에서는 기존 시스템의 기능을 확대하여 단독망 환경에서도 특화된 서비스를 위해 다음의 현안들을 고안하였다. 첫째, 단독망 정보자산 자산관리에 있어 정확한 정보자산 식

별을 위해 정보자산 인증기법을 개발하여 관리 사각지대에 놓일 수 있는 자산관리에 투명성을 개선하였다. 둘째, 정보자산 인증정보를 API를 통해 타 정보보호 솔루션에 제공하여 솔루션별로 추가 인증수단 개발 공수를 절감과 같은 상호운용성을 향상시켰다. 셋째, 단독망 정보자산 인증코드, 활성화코드, 예외정책코드 개념을 도입하여, 각각의 단독망 정보자산별로 USB 포트, 네트워크 포트, 무선네트워크 장치, 시리얼 장치, 휴대용 장치(Media Transfer Protocol), 적외선 장치 등 허용/차단 정책을 유연하게 적용할 수 있는 시스템을 설계 · 구축하여 사용편의성을 개선하였다. 마지막으로 정보자산 인증 및 매체통제 정책 운용으로 단독망 환경의 정보자산 내부자료 관리에 보안성을 한층 더 강화하였다.

향후 연구로는 단독망 정보자산에서 운용되는 자료유출방지시스템의 유실 없는 안정적인 로그저장 방법과 이 로그를 내부 업무망 자료유출방지시스템으로 이관하여 로그분석을 통한 이상행위 탐지 고도화 방안 연구가 필요하다.

참고문헌

[1] 이대성, 김재성, 김귀남, “정보 유출 방지 연구기술 동향,” 정보보호학회지, 제20권, 제2호, pp.56-65, 2010.

[2] 방위산업기술 보호법 시행령.

[3] 김명훈, “정보자산의 선별 절차에 관한 연구,” 디지털문화아카이브지, 제6권, 제2호, pp.55-74, 2023.

[4] 강종구, 임재환, 이홍주, 장항배, “소규모 IT 서비스 기업 비즈니스 특성을 고려한 정보자산 유형분류 설계연구,” 한국전자거래학회지, 제16권, 제4호, pp.97-108, 2011.

[5] 최동진, “IT 자산관리에 관한 연구,” 한국컴퓨터정보학회 동계학술대회 논문집, 제30권, 제1호, pp.141-143, 2022.

[6] 김재생, 신화성, “웹기반 IT 자산관리 시스템의 구축,” 디지털정책연구, 제10권, 제8호, pp.193-200, 2012.

[7] 행정안전부, 정보기술아키텍처 도입·운영 지침.

[8] 네이버 블로그, https://blog.naver.com/365blackstar/223458145025.

[9] 네이버 블로그, https://blog.naver.com/365blackstar/223458465355.

[10] 정재화, 김현수, “정보기술아키텍처 구축 사례 연구,” 한국SI학회지, 제5권, 제1호, pp.111-128, 2006.

[11] 안건희, 안상혁, 임동균, 정수환, 김재우, 신영주, “폐쇄망에서의 안전하고 효율적인 소프트웨어 패키지 관리 방안,” 정보처리학회논문지, 제11권, 제4호, pp.119-126, 2022.

[12] 김선미, 홍순오, 이강석, “자료유출방지 시스템의 안전한 운영 방안,” 한국통신학회 학술대회논문집, 제6호, pp.1639-1640, 2009.

[13] 신규진, 정구현, 양동민, 이봉환, “내부 기밀파일 유출 방지를 위한 USB DLP 기법,” 한국정보통신학회논문지, 제21권, 제12호, pp.2333-2340, 2017.

[14] 유승재, “내부정보유출방지를 위한 DLP 시스템 연구,” 융합보안논문지, 제18권, 제5호, pp.121-126, 2018.

[15] Andrada Coos, “Keeping Source Code Safe with Data Loss Prevention,” 2018, https://www.endpointprotector.com/blog/keep-source-code-safewith-dlp.

[16] 이호균, 이승민, 남택용, 장종수, “기밀정보 유출 방지 기술 동향,” 정보통신연구진흥원 주간기술동향, 제1256호, pp.1-12, 2006.

[17] 워터월 DLP 솔루션, https://www.wwsystems.co.kr/product/dlp.

[18] 소만사 DLP 솔루션, https://www.somansa.com/wp-content/uploads/2024/07/Mail-i-_20230629_page.pdf.

[19] 소만사 DLP 솔루션, https://www.somansa.com/wp-content/uploads/2024/03/Privacy-i_20240229.pdf.

[20] 소만사 DLP 솔루션, https://www.somansa.com/wp-content/uploads/2023/01/20221129_server-i.pdf.

[21] 지란지교소프트 DLP 솔루션, https://www.officekeeper.co.kr/product/function/dlp.

〔저자소개〕

김 일 한 (Ilhan Kim)
2008년 8월 충남대학교 석사
2021년 2월 충북대학교 박사
현 재 국방과학연구소 선임기술원
정보보호팀장

email : ilhan2676@hanmail.net

이 주 승 (Juseung Lee)
2012년 12월 Shepherd University B.S.
2018년 8월 아주대학교 석사
현 재 국방과학연구소 선임기술원

email : ljs-1212@hanmail.net

김 현 수 (Hyunsoo Kim)
2010년 5월 Carnegie Mellon University B.S.
2013년 2월 연세대학교 석사
현 재 국방과학연구소 선임연구원

email : rmffpd@gmail.com