중앙 관리 소프트웨어 보안 가이드

2016. 11

미래창조과학부

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

제1장
개요

제1장 개요

1.1 배경

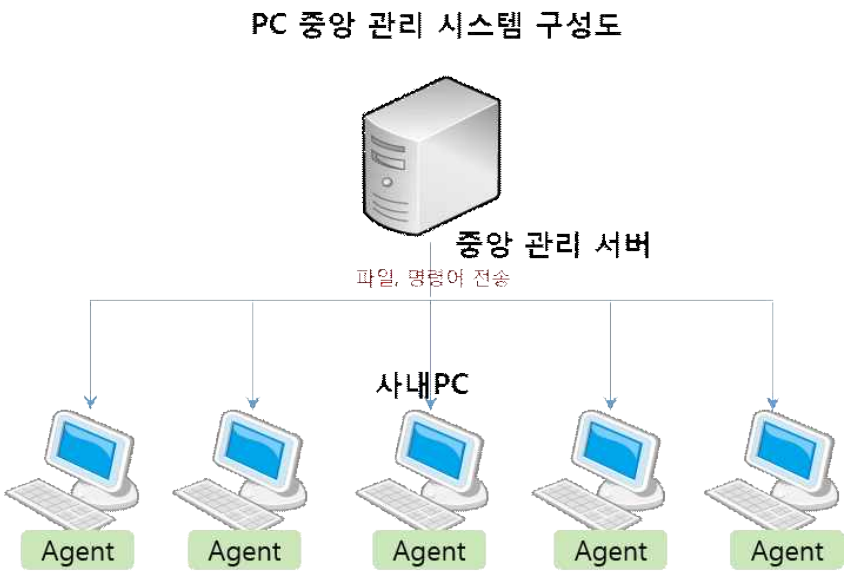
최근 공격자는 APT 공격을 통해 피해 대상을 쉽게 확산시키기 위한 방법으로 기업내에서 주로 이용하는 중앙 관리형 소프트웨어의 특징을 이용하여 공격하고 있다. 각 기업에서 도입 및 운영하고 있는 중앙 관리형 소프트웨어는 패치관리, 자산관리, 보안관리 등 다양한 목적을 위하여 사용되고 있으며, 특정 명령어를 통해 일괄적으로 패치 또는 정책을 설정하는 시스템을 말한다.

중앙 관리형 소프트웨어는 크게 PC 등 자산을 관리하기 위한 관리 서버와 에이전트로 구성된다.

o **(관리 서버)** PC를 중앙에서 제어하기 위한 시스템으로 시스템 관리자는 관리자 페이지에 접속하여 PC에 일괄적으로 파일 및 명령어 전송을 수행할 수 있다.

o **(에이전트)** 관리 서버에서 송신하는 파일, 명령어를 처리하기 위해 PC내에 설치되는 소프트웨어로써 사내 보안 프로그램 설치, 업데이트 설치, 자산관리 등을 위해 사용된다.

<그림 1-1> 중앙 관리형 소프트웨어 시스템 구성도



기업에서 주로 이용하는 중앙 관리형 소프트웨어 종류는 다음과 같다.

- **백신** : 바이러스 패턴 파일, 백신 업데이트 파일을 중앙에서 연결된 PC로 전송
- **NAC(네트워크접근제어)** : 사내 네트워크 보안 솔루션으로 필수 보안 프로그램 파일을 PC로 전송하는 시스템
- **자산관리 시스템** : 중앙에서 일괄적으로 사내 자산을 관리하기 위한 시스템
- **PMS(패치관리시스템)** : 중앙에서 PC에 업데이트 파일을 전달하여 패치하는 시스템
- **PC보안솔루션** : DLP(데이터유출방지), 매체제어, 불법소프트웨어 차단 등 PC 보안을 위해 설치하는 프로그램
- **기타** : 윈도우 Active Directory, 메신저, 그룹웨어 등

이러한 중앙 관리형 소프트웨어에 취약점이 존재하는 경우, 연결된 다수의 PC에 악성코드를 쉽게 감염시켜 장악 할 수 있게 된다. 다수의 PC를 감염시키면 효과적인 공격 대상인 시스템 관리자 PC, 개인정보 관리자 PC 등을 찾기 용이해지고 기업에 큰 피해를 입힐 수 있는 경로를 쉽게 찾을 수 있게 된다. 과거 발생한 대규모 침해사고도 마찬가지로 기업내 중앙 관리형 소프트웨어 중 하나인 업데이트 체계의 취약점을 악용하여 악성코드를 감염 및 확산 시킨 후 피해를 유발하였다.

이에 본 가이드에서는 중앙 관리형 소프트웨어로 인해 발생하는 침해사고 위협 사례를 다루어 그 위험성을 인지하도록 한다. 또한 중앙관리형 소프트웨어를 개발하는 기업과 도입하여 운영하는 기관에서 주의해야 할 항목들을 제공함으로써 사고 예방 및 피해를 최소화하고자 한다.

1.2 가이드 목적 및 구성

목적	- 중앙 관리 소프트웨어의 위협 심각성 인지를 통한 보안 인식 제고 - 안전한 중앙 관리 소프트웨어 개발 및 운영을 통한 침해사고 예방 및 피해 최소화
대상	- 중앙 관리 소프트웨어 개발자 및 이용자
범위	- 중앙 관리 소프트웨어 개발 및 운영 시 지켜야 할 사항
구성	- [1장] 개요 1.1 배경 1.2 가이드 목적 및 구성 - [2장] 보안 위협 2.1 중앙 관리 소프트웨어 악용 사례 - [3장] 중앙 관리 소프트웨어 보안가이드 - [4장] 중앙 관리 소프트웨어 보안가이드 항목 해설서

제2장
보안 위협

제2장 중앙 관리 소프트웨어 악용 사례

기업은 직원 PC를 일괄적으로 관리·제어하기 위해 패치관리시스템(PMS), 자산관리시스템, 보안 솔루션 등을 사용하고 있다. 공격자는 이러한 중앙 관리 프로그램이 피해 대상을 쉽게 확산·전이시킬 수 있기 때문에 악성코드를 퍼트리는 매개체로 이용한다. 이러한 중앙 관리 프로그램 내 취약점 및 운영상 미흡한 부분을 찾아 침해사고로 악용하는 사례가 지속적으로 발생하고 있다.

■ 취약한 관리자 비밀번호 사용

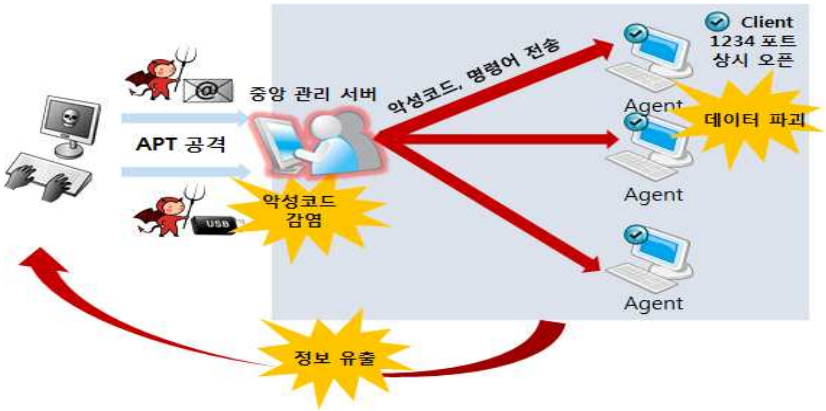
최근 취약한 관리자 비밀번호를 악용하여 공격한 사례가 있다. 공격자는 사전에 피싱 메일 등을 통해 관리자 PC를 감염시킨다. 이 후, 중앙관리 프로그램 관리자 계정이 추측하기 쉬운 비밀번호를 되어 있는 점을 악용하여 비밀번호 무작위 대입 등을 통해 관리자 계정을 탈취한다. 탈취한 계정으로 중앙관리 프로그램에 접속한다. 최종적으로 공격자는 중앙 관리 프로그램을 통해 악성코드를 사내 망에 연결돼있는 모든 PC에 전송하여 감염시킨 사례라고 볼 수 있다.

<그림 2-1> 취약한 관리자 비밀번호를 사용하는 경우

■ 시스템 명령 및 파일 실행 취약점 악용(상시 오픈포트 이용)

중앙 관리 프로그램(에이전트) 취약점을 찾아 악용하는 사례도 발견되고 있다. 한 사례로, 에이전트와 서버 간 업데이트 파일 및 설치 프로그램 전송 등을 위해 사용되는 상시 오픈 포트(Port)에 실행 파일 또는 명령어를 전송할 경우 상호 인증을 수행하지 않는 취약점을 이용한 사례가 있다. 이를 통해 공격자는 사전에 감염시킨 PC를 관리자 서버인척 위장하여, 관리 다른 PC들의 해당 포트로 정상파일이 아닌 악성파일을 전송해 악성코드를 감염시킬 수 있다.

<그림 2-2> 상시 오픈 포트를 운영 중인 에이전트에 취약점이 존재하는 경우

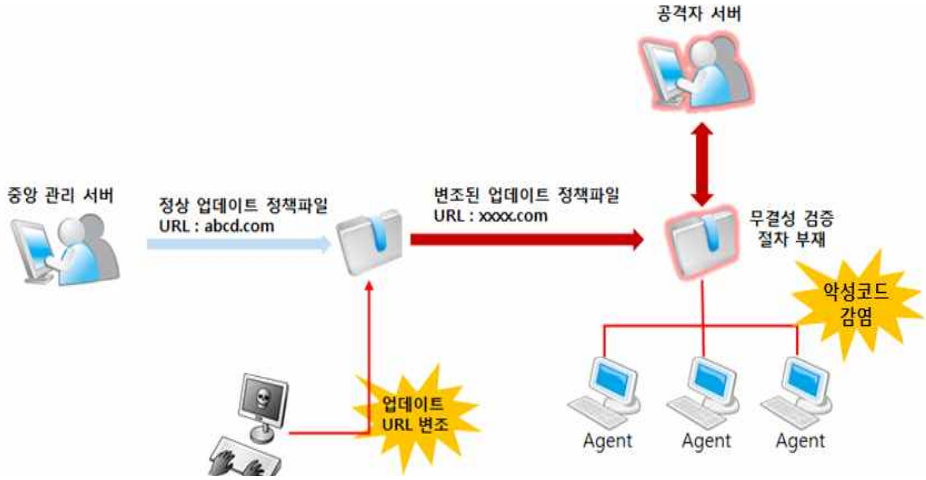


■ 파일 무결성 검증 절차 부재

에이전트에서 업데이트 파일을 받을 때 업데이트 URL이 정상 URL인지 확인하지 않는 경우가 있다. 공격자는 이를 악용하여 MITM[1] 또는 ARP Spoofing[2]을 통해 중앙 관리 서버 업데이트 URL을 악성코드 유포 URL로 변조할 경우 사내 PC에서 악성 사이트에 접속하여 악성코드가 다운로드 되어 실행된다. 업데이트 URL이 변조되더라도 최종적으로 받은 파일이 정상파일인지 아닌지 확인하는 무결성 검증 절차가 있다면 악성코드 실행은 불가능하다. 여기서 무결성 검증이란, 서버가 업데이트 파일의 고유한 값(해쉬 등)을 개인키로 암호화하여 전송하고 에이전트에서는 암호화한 값을 공용키로 해독하여 실제 받은 파일의 고유한 값과 동일한지 비교하는 절차이다. 이러한 검증 절차가 부재할 경우, 중앙 관리 서버 또는 Fake 서버에서 악성파일을 배포해도 사내 PC에서 의심 없이 실행하게 된다.

<그림 2-3> 무결성 검증을 하지 않는 경우

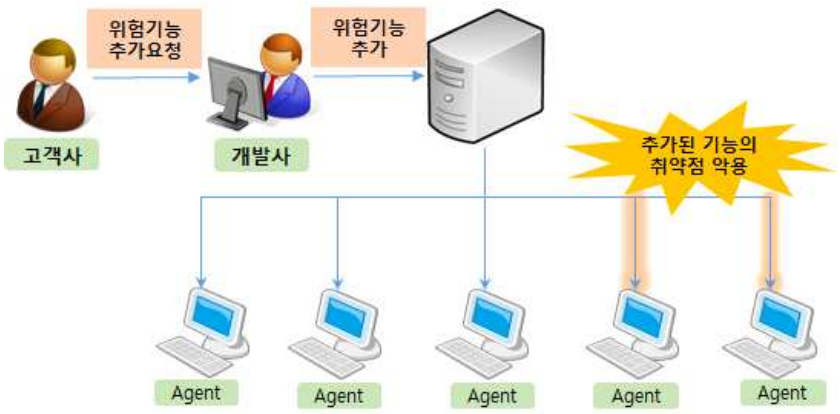
1) MITM(Man In The Middle) : 네트워크 통신 중간에서 제3자가 통신 내용을 도청하거나 조작하는 공격 기법
2) ARP Spoofing : 근거리 네트워크 망에서 ARP 프로토콜을 이용해 망에 연결된 사용자의 데이터를 가로채거나 조작하는 공격 기법



■ 커스터마이징 기능 악용

중앙 관리 소프트웨어를 도입하는 고객사 측에서 해당 소프트웨어에 특정 기능을 개발사에 요구하여 추가하는 경우가 존재한다. 추가 요청 기능이 UI 수정이나 기본 기능 등과 같은 기존 소프트웨어에 존재하는 기능이라면 문제가 되지 않지만, 기존에 존재하지 않던 파일 배포 기능, 에이전트에 시스템 명령을 실행시킬 수 있는 등의 기능을 개발사에 추가 요청하여 커스터마이징 하는 경우 문제가 될 수 있다. 이러한 추가 기능 중 해킹에 악용 가능한 위험 기능이 있을 수 있고, 추가 기능이라 보안성 검토가 충분히 이뤄지지 않을 수 있으므로 위험기능 추가는 하지 않는 것이 좋다.

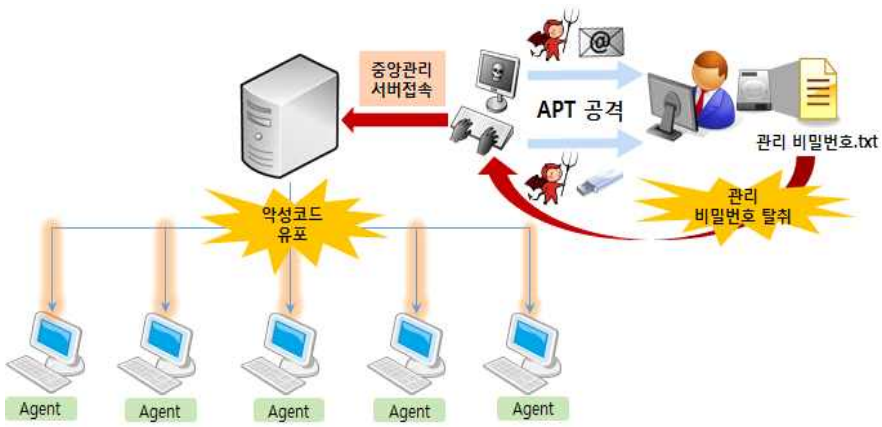
<그림 2-4> 고객의 요청에 의해 위험기능을 추가하여 운영하는 경우



■ 비밀번호 기록 파일 보관

내부 망에 침투한 공격자는 보통 내부 망 에이전트들을 한 번에 공격하기 위한 방법을 찾게 된다. 이때, 효과적인 수단 중 하나가 중앙 관리 소프트웨어를 이용한 방법이다. 중앙 관리 기능을 이용해 에이전트를 감염시킬 수 있기 때문에 관리자 PC에 대한 APT 공격을 성공한 공격자는 중앙 관리 서버에 접속하기 위한 비밀번호를 알아내기 위해 노력한다. 만약, 관리 · 시스템 비밀번호 등을 파일에 저장하여 관리한다면 해커에 의해 쉽게 유출되어 시스템 접근을 허용하는 최악의 상황을 제공할 수 있다.

<그림 2-5> 관리 비밀번호를 파일에 저장하여 운영하는 경우



이러한 사례들처럼 침해사고가 실제 발생하고 있어, 대응방법을 알고 보안설정지침을 적용하는 것이 무엇보다 중요하다.

제3장

중앙 관리 소프트웨어 보안가이드

제3장 1절 중앙 관리 소프트웨어 개발 보안가이드

3.1 중앙 관리 소프트웨어 보안 체계

- **(파일 무결성 검증)** 실행·비실행, 설치, 업데이트, 정책 파일 등 파일에 대한 무결성 검증을 수행해야 한다.
- **(안전한 방법의 무결성 검증기술 사용)** 무결성 검증은 에이전트에 하드코딩 된 값 또는 CRC 비교가 아닌 공개키 방식 등 안전한 방법으로 검증해야 한다.
- **(안전한 암호화 알고리즘 및 키 관리)** 파일 전송, 통신 구간 등은 안전한 암호화 알고리즘 사용 및 키 관리를 수행해야 한다.
- **(에이전트 프로그램 상시 오픈포트 제거) 에이전트** 프로그램에서 명령어 또는 파일을 수신하기 위해 사용하는 상시 오픈 포트를 제거해야 한다.
- **(원격 시스템 명령어 처리 기능 제거)** 관리 서버에서 원격으로 에이전트에 시스템 명령 실행 기능을 제거해야 한다.
- **(고객 요청 기능 시)** 고객의 요청에 의해 기본 제품의 기능 외 추가적인 기능을 제공해야 할 때, 보안을 고려하여 기능을 제공하여야 한다.
- **(정책 설정 보안 관리)** 서버와 에이전트간의 정책 설정은 지정된 관리자만 수행할 수 있도록 구현해야 한다.
- **(중앙 관리 서버 IP, URL 변조 불가)** 중앙 관리 서버 IP, URL의 변조가 불가능하도록 구성되어 있어야 한다.
- **(서버↔에이전트 간 안전한 상호 인증)** 서버↔에이전트 간 안전한 상호 인증 절차가 존재해야 한다.
- **(관리 S/W ID, PW 암호화)** 관리자 ID, PW에 대해 통신 구간 암호화가 적용되어 있어야 한다.

3.2 관리 프로그램 보안

o **(계정 관리)** 개발사에서 관리 목적으로 만든 불필요한 계정이 없어야 한다.

o **(패스워드 관리)** 관리자 계정 생성 시 비밀번호 복잡도(2조합 10글자 또는 3조합 8글자)를 만족하도록 설정해야 하며, 최초 설치 시 사용자에게 패스워드를 설정하도록 유도해야 한다.

o **(접근통제)** 접근 가능한 관리자 IP 지정 등을 통한 중앙 관리 프로그램에 대한 접근 통제 기능을 제공해야 한다.

o **(세션 타임 아웃 설정)** 관리 프로그램을 일정 시간 동안 사용하지 않을 경우, 로그아웃 되도록 세션 타임아웃 기능을 제공해야 한다.

o **(자동 접속 제한)** 관리 프로그램에 대한 자동 로그인 기능을 제공해서는 안 된다.

o **(ID/PW 평문 전송 서비스 미사용)** 평문으로 패킷이 전송되는 서비스 기능을 제공해서는 안 된다.

o **(로그 관리)** 접속 로그, 설정 변경 로그를 기록하는 기능 등 시스템 로그는 최소 3개월 이상 로그를 기록하도록 제공 한다.

제3장 2절 중앙 관리 소프트웨어 운영 보안가이드

3.3 중앙 관리 소프트웨어 운영 보안

- o **(초기 비밀번호 변경)** 소프트웨어 초기 설치 시 관리자 비밀번호를 변경 후 사용해야 한다.
- o **(위험기능 추가 지양)** 운영의 편리함을 위해 존재하지 않는 기능 중 위험 기능을 개발사에 추가 요구하여 도입하는 것은 지양해야 한다.
- o **(비밀번호 파일 저장 금지)** 관리 비밀번호와 같은 중요 정보를 파일에 기록하여 보관해서는 안 된다.
- o **(주기적인 로그 확인)** 중앙 관리 소프트웨어의 이용 로그를 주기적으로 확인해야 한다.
- o **(패스워드 복잡도 설정)** 계정의 패스워드 복잡도(2조합 10글자 또는 3조합 8글자)를 설정해야 한다.
- o **(공용 계정 삭제)** 다른 사람과 공용으로 사용 되는 계정은 없어야 한다.
- o **(최소한의 관리자 계정 사용)** 관리자 계정은 실제 사용하는 계정만 설정하여 최소한으로 사용해야 한다.
- o **(접근 통제)** 관리자 PC 및 서버는 접근 가능한 IP를 지정하고 인터넷 차단 등 물리적으로 독립된 네트워크를 구성하여 관리하여야 한다.
- o **(공유 폴더 차단)** 공유 폴더를 생성해서는 안 된다.
- o **(불필요한 서비스 삭제)** 사용 용도와 상관없는 불필요한 서비스는 제거해야 한다.
- o **(불필요한 프로그램 삭제)** 메신저, 원격제어 서비스 등 불필요한 프로그램은 삭제하여야 한다.

- **(최신 패치 적용)** 시스템에 설치된 소프트웨어 버전을 최신버전으로 유지해야 한다.
- **(백신 프로그램 설치)** 백신 프로그램을 설치해야 하며, 백신 프로그램은 최신 업데이트를 주기적으로 수행하여 최신버전으로 유지해야 한다.
- **(USB 등의 미디어 자동 실행 차단)** USB 등의 미디어가 자동으로 실행되지 않도록 설정해야 한다.
- **(화면 보호기 설정)** 화면 보호기를 설정해야 한다.

제4장
중앙 관리 소프트웨어
보안가이드 항목 해설서

제4장 중앙 관리 소프트웨어 개발 보안가이드 항목 해설서

■ 중앙 관리 소프트웨어 보안 체계 강화

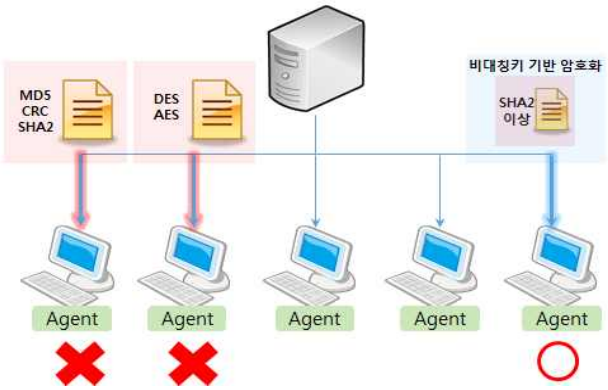
① 실행·비실행, 설치, 업데이트, 정책 파일 등 파일에 대한 무결성 검증을 수행해야 한다.
② 무결성 검증은 에이전트에 하드코딩 된 값, CRC 비교가 아닌 공개키 방식 등 안전한 방법으로 검증해야 한다.

중앙 관리 서버 또는 프로그램에서 에이전트와 통신하는 과정 중 사용되는 파일(실행, 비실행, 설치, 업데이트, 정책 등)에 대해 무결성 검증을 수행해야 한다. 에이전트에 푸쉬하는 실행파일은 무결성을 검증하지만 정책 파일이나 업데이트 파일에 대한 무결성은 검사하지 않는 경우가 있다. 무결성 검증을 일부 파일만 하게 될 경우, 검증 절차가 누락된 종류의 파일을 이용해 악성코드가 유포될 수 있다. 이를 위해 서버와 에이전트 간 주고 받는 파일에 대한 무결성 검증을 수행하여, 중간에서 공격자가 파일을 변조하더라도 사용자 PC에까지 피해가 발생하지 않도록 해야 한다.

또한, 파일 무결성을 안전한 방법을 사용해 검증해야 한다. 파일에 대한 무결성을 MD5, SHA256 등과 같은 해쉬 알고리즘만을 이용하여 파일과 해쉬 값을 같이 전송하는 방식으로 단순 해쉬 값 비교를 통해 변조 유무를 확인하거나, 파일 전송 과정에서 누락된 데이터의 유무를 확인하기 위해 CRC를 체크하는 정도의 무결성 검증만을 수행하는 경우가 있다. 이러한 방법들로 무결성을 검증한다면 중앙 서버나 관리자 PC가 장악 될 경우, 푸쉬할 파일이나 업데이트 파일을 악성코드로 만들고 악성코드에 대한 해쉬 값과 CRC 값을 생성하여 전송하는 방식으로 무결성 검증을 우회할 수 있다. 이런 우회 가능성을 제거하기 위해 AES256과 같은 대칭키를 이용해 파일을 암호화하는 방법으로 무결성 검증을 수행하는 경우도 있지만, 이는 대칭키가 서버와 에이전트 양측에 존재해야 하므로 에이전트 프로그램의 역공학을 통해 키가 유출 될 수 있는 위험이 있다.

따라서, 안전한 무결성 검증을 위해선 파일에 대한 해쉬 값을 SHA256 이상의 알고리즘으로 생성 후 해쉬 값을 공개키 기반의 알고리즘을 이용해 서버의 개인키로 암호화하는 방식이 안전하다. 이렇게 암호화된 해쉬 값과 파일을 함께 전송하고, 에이전트에서는 서버의 공개키로 복호화하는 방식으로 파일의 해쉬 값을 비교하면 서버의 개인키가 유출되지 않는 이상 무결성 검증 절차를 우회하기 어렵다.

<그림 4-1> 안전한 무결성 검증 방법 예시



③ 파일 전송, 통신 구간 등은 안전한 암호화 알고리즘 사용 및 키 관리를 수행해야 한다.

소프트웨어를 최신 버전으로 업데이트하는 것처럼 암호화에 사용되는 암호화 알고리즘이나 키 관리를 취약한 알고리즘을 사용하게 되면, 알려진 공격으로 인해 키가 유출될 위협이 있다. 일부 업체에서는 통신 구간에 이용되는 프로토콜을 자체 프로토콜로 만들고, 통신 구간을 AES와 같은 대칭키로 암호화한 후, 키를 에이전트 프로그램에 하드코딩하는 경우가 있다. 이 경우도 마찬가지로 프로그램 역공학을 통한 키 유출 위험이 있으므로 통신 구간은 공개키 기반의 SSL 통신을 수행하는 것이 안전하며, 키 관리는 서버에 존재하는 개인키에 대한 접근통제 정책을 수립하여 외부에 유출되지 않도록 관리해야 한다. 또한 개인키는 중앙 관리 서버가 아닌 별도의 시스템 또는 금고 등에 보관하는 것이 더 안전하다.

<그림 4-2> 안전한 암호화 알고리즘 및 키 관리

④ 에이전트 프로그램에서 명령어 또는 파일을 수신하기 위해 사용하는 상시 오픈 포트를 제거해야 한다.
⑤ 관리 서버에서 원격으로 에이전트에 시스템 명령 실행 기능을 제거해야 한다.
⑥ 고객의 요청에 의해 기본 제품의 기능 외 추가적인 기능을 제공해야 할 때, 보안을 고려하여 기능을 제공해야 한다.

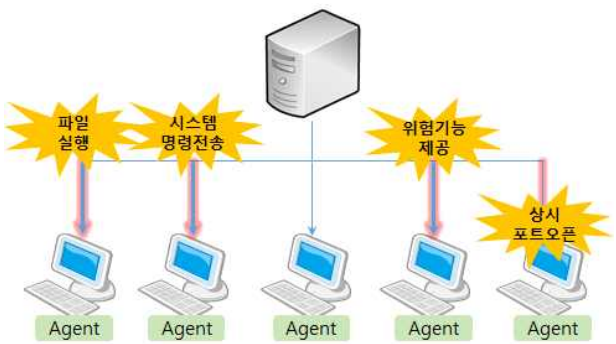
중앙 관리 서버에서 에이전트를 제어하거나 관리하기 위한 기능을 악용하는 사례가 자주 발생하고 있다. 과거 사고 사례를 보면 대부분 이런 에이전트를 일괄 제어하는 기능이 보안에 미흡하여 발생하였다.

중앙 관리형 소프트웨어의 특징 상 서버와 에이전트 간 통신하기 위해 연결 포트가 존재한다. 하지만, 이런 연결 포트를 에이전트에 상시 오픈하고 있는 것 보다는 연결이 필요할 때마다 에이전트에서 먼저 서버에 요청하여 세션을 맺는 방식이 더 안전하다. 불가피하게 에이전트에서 명령 처리를 위해 포트를 상시 오픈해야 한다면 이를 최소화하고 에이전트끼리 명령 송수신이 불가하도록 서버와 에이전트간 상호 인증을 통한 접근 통제 절차가 반드시 들어가야 한다.

또한 중앙 서버에서 에이전트를 제어하는 기능 중 파일 실행, 복사, 삭제, 시스템 종료 등과 같은 시스템 명령어를 실행시킬 수 있는 기능이 존재하는 경우가 있다. 이러한 기능들은 공격자에 의해 악성코드를 실행하게 하거나 시스템의 주요 파일들을 삭제하는 행위와 같은 악의적인 동작이 가능할 수 있어 제거해야 한다.

PC에 일괄적으로 설치파일을 강제 푸쉬하는 기능과 같은 위험한 기능이 최초 구축 시 존재하지 않았지만, 운영 중 필요하여 기능을 추가하는 경우도 있다. 하지만, 추가 요청한 기능에 대해 보안성이 고려되지 않아 위험할 수 있으며, 이런 기능의 존재 자체가 공격자에 의해 악용될 가능성이 높으므로 제공 또는 적용하지 않는 것이 안전하다.

<그림 4-3> 공격자에게 악용될 수 있는 기능 예시



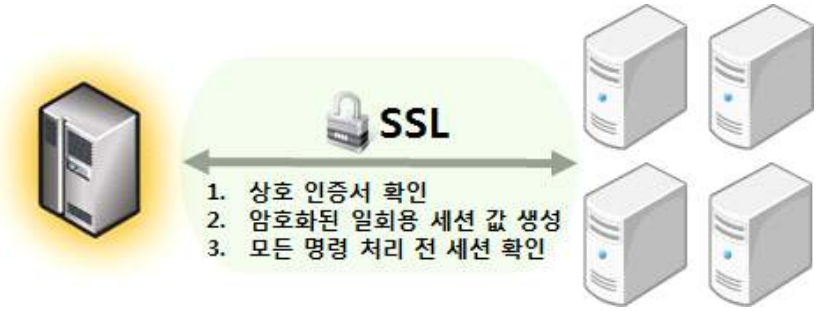
⑦ 서버와 에이전트간의 정책 설정은 지정된 관리자만 수행할 수 있도록 구현해야 한다.

중앙 관리형 소프트웨어는 중앙 관리 목적 별 중앙에서 에이전트를 제어하기 위한 정책 설정 기능이 존재한다. 이런 정책 설정을 지정된 관리자 프로그램만으로 제어가 가능하도록 구현해야 한다. 관리 프로그램이 없더라도 통신 프로토콜이 암호화되어 있지 않다면 동일한 패킷을 만들어 전송하여 정책 변경을 할 수 있으므로 통신 구간 암호화를 통해 지정된 관리 프로그램만이 정책 설정이 변경 가능하도록 구현해야 한다. 또한 정책 설정 파일의 무결성 보호를 위해 암호화 적용을 관리자 서버에서 수행한다면 관리자 서버가 장악될 경우 암호화된 정책파일이 변조될 수 있어 별도의 관리 시스템에서 암호화 적용과 키 관리를 수행하는 것이 더 안전하다.

⑧ 중앙 관리 서버 IP, URL의 변조가 불가능하도록 구성되어 있어야 한다.
⑨ 서버↔에이전트 간 안전한 상호 인증 절차가 존재해야 한다.

에이전트에서 관리 서버와 통신하기 위한 IP나 URL은 보통 프로그램 내 하드코딩 되어 있거나 설정 파일을 통해 관리된다. 하지만, 설정 파일의 내용이 변조되거나 ARP, DNS 스푸핑 공격에 의해 지정된 관리 프로그램과 통신하지 않고 공격자가 만든 가짜 서버와 통신하게 하여 정상 업데이트 파일이 아닌 악성코드를 내려 받아 실행하거나 잘못된 정책 파일을 받아와 적용하게 하는 등의 공격이 가능하다. 이런 가짜 서버와의 통신을 유도한 공격을 예방하기 위해선 에이전트에서 서버와 통신 시 상호 인증하는 기능이 존재해야 한다. 서버와 에이전트 간 세션이 생성되기 전에 서로 정상 서버와 에이전트가 맞는 지 확인하는 절차가 있어야 하며, 이런 인증 절차를 단순히 자체 제작한 프로토콜이 맞는 지 여부만 체크하는 게 아니라 암호화된 인증 방법으로 양쪽 모두 인증해야 한다. 예를 들면, SSL 통신을 하고 초기 세션 생성 시 인증서를 확인하는 절차를 포함시켜 인증하게 하거나 각각의 서버 및 에이전트가 개별로 만든 공개키, 개인키로 인증 값을 세션 생성 시마다 다르게 생성해 확인하는 절차가 있는 등의 인증과정이 있어야 한다.

<그림 4-4> 안전한 상호 인증 방법



⑩ 관리자 ID, PW에 대해 통신 구간 암호화가 적용되어 있어야 한다.

관리 서버에 접속 시 사용되는 ID, PW를 평문으로 서버에 전송하여 인증하는 경우, 중간에 스니핑을 통해 관리자 계정을 알아내 접속할 수 있다. 이렇게 스니핑한 관리자 계정으로 관리 프로그램에 접속하여 악성코드 유포, 정책 설정 변경 등이 가능하므로 스니핑이 어렵도록 ID, PW를 통신 구간에서 암호화해야 한다.

■ 관리 프로그램 보안 강화

① 개발사에서 관리 목적으로 만든 불필요한 계정이 없어야 한다. ② 관리자 계정 생성 시 비밀번호 복잡도(2조합 10글자 또는 3조합 8글자)를 만족하도록 설정해야 하며, 최초 설치 시 사용자에게 패스워드를 설정하도록 유도해야 한다.

프로그램 계정 설정 시 ID/패스워드를 admin/admin 또는 패스워드가 12345678 등과 같이 유추하기 쉽게 설정되어 있는 상태이다. 이에 ID/패스워드의 경우 설정 없이 접속할 수 없도록 사용자에게 아래 그림과 같이 2조합 10글자 또는 3조합 8글자 길이의 패스워드를 설정하도록 유도해야 한다. 또한 시스템 계정의 패스워드는 최소 분기별 1회 이상 변경하여, 기존 담당자의 이직/퇴사 등 패스워드가 알려졌을 경우에 대한 대책을 마련해야 한다.

<그림 4-5> 패스워드 복잡도 설정방법

③ 접근 가능한 관리자 IP 지정 등을 통한 중앙 관리 프로그램에 대한 접근 통제 기능을 제공해야 한다.

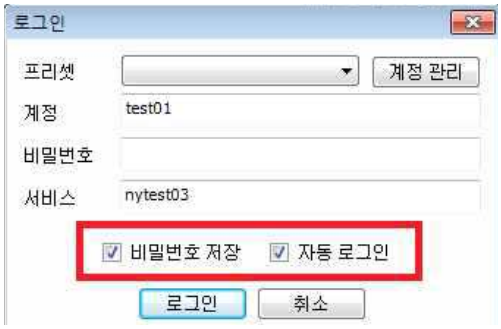
중앙 관리 프로그램 구축 시 관리자로 지정한 IP 이외에 다른 IP에서는 정상 관리 프로그램을 이용해 접속하더라도 접속하지 못하도록 접근을 통제하는 기능이 있어야 한다. 또한, 실제 에이전트로의 패킷을 전송하는 관리 서버에도 직접적인 접근을 제한할 수 있도록 지정된 관리 프로그램으로만 접근할 수 있도록 제공해야 한다. 또한 서버 간 접근이 불가하도록 접근통제를 실시한다.

④ 관리 프로그램을 일정 시간 동안 사용하지 않을 경우, 로그아웃 되도록 세션 타임아웃 기능을 제공해야 한다.
⑤ 관리 프로그램에 대한 자동 로그인 기능을 제공해서는 안 된다.

관리자가 관리 프로그램에 로그인 하고 다른 업무를 보는 동안 세션이 끊기지 않도록 하여 업무의 연속성을 지원해주는 경우가 있다. 이는 관리자에게 편의는 제공하지만, 관리자가 자리를 비운 사이 타인이 접근해 관리 프로그램의 기능을 악용할 수 있으므로 보안상 위험하다. 따라서 특정 시간(5~10분) 동안 기능을 사용하지 않는다면 자동 로그아웃이 되도록 타임아웃 기능을 제공해야 한다.

관리해야 하는 프로그램 및 시스템이 많을수록 관리의 편리성 때문에 관리 페이지나 관리 프로그램에 접속하는 계정에 대해 자동 로그인 기능을 제공하는 경우가 있다. 이는 계정을 모르는 허용되지 않은 자가 관리자 프로그램에 로그인 할 수 있도록 하므로 제공해서는 안 된다.

<그림 4-6> 자동 로그인으로 설정되어 있는 경우



⑥ 평문으로 패킷이 전송되는 서비스 기능을 제공해서는 안 된다.

관리 서버에 접속하기 위한 터미널 프로그램은 사용하지 않고 관리 프로그램만을 이용해 접속을 허용하는 것이 안전하다. 예를 들어 텔넷은 평문 서비스이기 때문에 제공하지 않는 것이 안전하다. 또한, 파일 전송 서비스도 FTP는 평문 서비스이므로 제공할 경우 공격자에 의해 파일이 유출되거나 주요 정보가 노출될 수 있다. 그러므로 파일 전송에는 FTP 보다 SFTP와 같이 보안이 강화된 서비스를 제공해야 한다.

⑦ 접속 로그, 설정 변경 로그를 기록하는 기능 등 시스템 로그는 최소 3개월 이상 로그를 기록하도록 제공 한다.

중앙 관리형 소프트웨어는 침해사고에 악용될 가능성이 높은 프로그램이다. 이런 프로그램은 공격자에게 장악될 경우, 많은 행위가 가능한 종류의 프로그램이기 때문에 사후 대응을 위해 사용 로그를 기록해야 한다. 접속 로그는 해커의 관리 프로그램 장악 시점을 파악할 수 있도록 도움을 주며, 설정 변경 로그는 중앙 관리형 프로그램을 통해 악성코드나 악의적인 행위 시점을 제공한다. 해커의 해킹 공격을 추적하는 것뿐만 아니라 관리자에 대한 감사 증적에도 필요하므로 로그 기록은 상세하게 기록될 수 있도록 제공해야 한다.

■ 중앙 관리 소프트웨어 운영 보안 강화

① 소프트웨어 초기 설치 시 관리자 비밀번호를 변경 후 사용해야 한다.
② 운영의 편리함을 위해 존재하지 않는 기능 중 위험 기능을 개발사에 추가 요구하여 도입하는 것은 지양해야 한다.
③ 관리 비밀번호와 같은 중요 정보를 파일에 기록하여 보관해서는 안 된다.
④ 중앙 관리 소프트웨어의 이용 로그를 주기적으로 확인해야 한다.

중앙관리 소프트웨어 초기 도입 시 개발사에서는 고객사에 방문하여 설치 및 환경 설정을 도와준다. 이 때, 개발사에서 관리자 기본 비밀번호(admin/admin, root/root 등)를 설정하고 관리자에게 추후 비밀번호 변경이 필요하다는 것을 안내한다. 하지만 많은 운영자들이 초기 비밀번호를 변경하지 않은 상태로 운영을 하고 있다. 중앙 관리 소프트웨어의 관리자 프로그램에서 초기 비밀번호를 변경해야만 사용 가능하도록 구현되어 있으면 상관없지만, 그렇지 않은 경우에는 초기 비밀번호를 변경 후 사용해야 한다. 초기 비밀번호를 변경하지 않은 상태로 공격자가 내부 망에 침투한다면 관리자 비밀번호를 추측하여 관리자 기능을 악용 할 수 있으므로 초기 비밀번호는 바로 변경해야 한다.

또한, 중앙 관리 소프트웨어 도입 시 개발사에게 해당 소프트웨어를 통해 특정 기능을 사용할 수 있도록 구현을 요청하는 경우가 있다. 개발사에서 기본적으로 제공하는 기능이 아닐 경우에는 고객사의 요청에 의해 추가 개발 작업이 들어가야 하는데, 이런 추가 개발 작업 과정은 보안성 검토가 충분히 이루어지지 않을 수 있다. 따라서 되도록 위험 기능을 요청하지 않는 것이 안전하다.

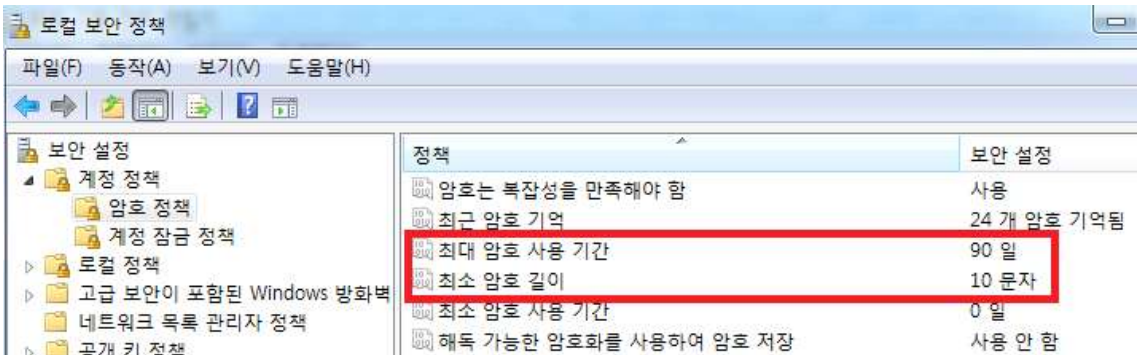
관리 소프트웨어 운영자들은 관리 소프트웨어뿐만 아니라 다른 소프트웨어 및 서버를 관리하는 경우가 많아 비밀번호를 기억하지 못하는 경우가 있다. 그래서 일부 운영자는 비밀번호를 기억하기 위해 파일에 비밀번호를 기록해두는 경우가 있는데 이는 내부 망에 침투한 해커에 의해 노출될 가능성이 있다. 이를 방지하기 위해 비밀번호를 파일에 기록해서는 안 되며, 불가피한 경우 본인만 알 수 있는 내용으로 기록 후 암호를 걸어놓는 것이 안전하다.

위의 사항들은 사고를 예방하기 위한 사전 보안 강화라면 사후 대안 또한 고려해야 한다. 사후 대비를 위해선 주기적인 로그 검토는 필수적이다. 최근 침해사고 유형을 보면 내부 망에 침투한 공격자가 오랜 시간 시스템을 모니터링 한 후에 공격을 시도하고, 공격에는 내부 직원들 PC에 영향을 끼칠 수 있는 중앙 관리 소프트웨어를 타깃으로 은밀히 이뤄지는 경우가 많다. 이런 은밀한 공격을 탐지하기 위해서는 소프트웨어의 로그를 주기적으로 확인해야 하고, 확인된 로그를 바탕으로 공격 유무를 판단할 수 있도록 숙지해야 한다.

⑤ 계정의 패스워드 복잡도(2조합 10글자 또는 3조합 8글자) 정책을 설정해야 한다.
⑥ 다른 사람과 공용으로 사용 되는 계정은 없어야 한다.
⑦ 관리자 계정은 실제 사용하는 계정만 설정하여 최소한으로 사용해야 한다.

관리자의 PC 비밀번호를 관리자 프로그램 비밀번호와 마찬가지로 복잡도를 만족하도록 생성해야 한다. 외부 사람이 관리자 PC에 접근 가능한 경우, 설정된 비밀번호가 유추 가능한 비밀번호와 같이 쉬운 비밀번호로 되어 있으면 PC 로그인이 가능할 수 있기 때문에 비밀번호 정책을 만들어 지키는 것이 안전하다. 또한 계정의 비밀번호는 분기별 1회 이상 변경하여 해킹 공격 등으로 유출된 비밀번호를 사용하지 않도록 해야 한다.

<그림 4-7> 패스워드 정책 설정



특정 작업을 위해 계정을 임시로 생성하였으나, 작업 후 계정을 삭제하지 않아 관리되지 않는 경우가 발생할 수 있다. 이러한 불필요한 계정이나 다른 사람과 공용으로 사용되고 있는 계정은 공격자에 의해 악용될 가능성이 있기에 실제 사용하는 계정만 남겨두어야 하며, 만약 공용 계정이 존재한다면 삭제해야 한다. 그리고 사용 용도에 따라 계정의 권한을 최소한만으로 설정해야 하며, 하나의 계정에 모든 권한을 부여해서는 안 된다. 모든 권한을 갖고 있는 관리자 계정에 대해서는 별도 관리를 해야 하며, 최소한으로 사용해야 한다.

<그림 4-8> 특정 서비스가 root(관리자 계정)으로 실행되고 있는 경우

```
stat     15268     1  2 Mar21 ?        05:54:01 /usr/local/stat/stmn/jdk/jre/bin/java -Djava.ut
root     15285     1  0 Mar21 ?        00:00:23 /usr/local/stat/stmn/apache/bin/httpd -k start
daemon   15690 15285  0 11:54 ?        00:00:00 /usr/local/stat/stmn/apache/bin/httpd -k start
daemon   15728 15285  0 11:54 ?        00:00:00 /usr/local/stat/stmn/apache/bin/httpd -k start
daemon   20203 15285  0 11:59 ?        00:00:00 /usr/local/stat/stmn/apache/bin/httpd -k start
daemon   20863 15285  0 12:00 ?        00:00:00 /usr/local/stat/stmn/apache/bin/httpd -k start
daemon   20864 15285  0 12:00 ?        00:00:00 /usr/local/stat/stmn/apache/bin/httpd -k start
daemon   27300 15285  0 12:07 ?        00:00:00 /usr/local/stat/stmn/apache/bin/httpd -k start
daemon   27301 15285  0 12:07 ?        00:00:00 /usr/local/stat/stmn/apache/bin/httpd -k start
```

⑧ 관리자 PC 및 서버는 접근 가능한 IP를 지정하고 인터넷 차단 등 물리적으로 독립된 네트워크를 구성하여 관리하여야 한다.

관리자 PC 및 에이전트를 관리하는 시스템은 해당 시스템에 접근 가능한 IP를 별도로 지정해야 하며, 인터넷 등 외부와의 연결이 차단된 네트워크 망을 구성하여 운영·관리해야 한다. 최근 공격 사례를 보면, 하나의 시스템이 장악되었을 때, 인터넷에 연결되어 있는 경우 다수의 시스템에 빠르게 2차 감염이 진행된 사례가 존재한다.

⑨ 공유 폴더를 생성해서는 안 된다.

외부 인터넷 접속이 가능한 인터넷망에서 관리의 편의를 위해 시스템 내 공유 폴더를 생성하여 사용할 경우 악성코드에 감염 및 동일 네트워크로 2차 감염 진행 등 위협이 존재할 수 있다. 따라서 별도의 독립적인 망을 사용하더라도 공유 폴더는 되도록 생성하지 않는 것이 좋으며, 외부와 연결되어 있는 인터넷망을 사용할 경우에는 공유 폴더를 생성해서는 안 된다.

<그림 4-9> 네트워크 및 공유 센터에서 파일 / 공용 폴더 공유 끄기

⑩ 사용 용도와 상관없는 불필요한 서비스는 제거해야 한다.
⑪ 메신저, 원격제어 프로그램 등 불필요한 프로그램을 사용할 수 없다.

사용 용도와 상관없는 불필요한 서비스, 편의성을 위한 메신저, 원격제어 프로그램 등 불필요한 프로그램을 사용하게 되면 다른 보안 설정이 잘 갖춰져 있다 하더라도 악성코드에 감염 될 위협이 증가하게 된다. 불필요한 서비스나 프로그램은 공격자의 입장에서 공격을 시도할 수 있는 수단과 방법이 늘어나게 되는 것과 같으므로 삭제, 제거해야한다.

⑫ 시스템에 설치된 소프트웨어 버전을 최신버전으로 유지해야 한다.
⑬ 백신 프로그램을 설치해야 한며, 백신 프로그램은 최신 업데이트를 주기적으로 수행하여 최신버전으로 유지해야 한다.

백신 프로그램은 시스템을 보호할 수 있는 최소한의 예방 수단이다. 백신 프로그램을 설치하지 않으면 악성코드 위협에 무방비로 노출되어 악성코드 감염이 쉽게 발생할 수 있다. 그러므로 악성코드 감염을 기본적으로 대비하기 위해 백신 프로그램 설치는 필수이며, 주기적으로 업데이트하여 신규 악성코드에 대한 대비를 해야 한다.

또한, 시스템에 설치되어 있는 소프트웨어를 주기적으로 업데이트하여 해당 소프트웨어의 버전을 항상 최신버전으로 유지해야 한다. 소프트웨어 버전을 최신버전으로 유지함으로써 해당 소프트웨어의 알려진 취약점을 이용한 공격에 예방할 수 있다.

⑭ USB 등 미디어가 자동으로 실행되지 않도록 설정해야 한다.

USB와 같은 외부 저장매체는 인터넷, 이메일과 마찬가지로 공격자 입장에서 내부망 공격에 유용한 접근 경로가 될 수 있다. 내부 망 침해를 목적으로 제작된 악성코드를 외부 저장매체에 담아 사회 공학적 기법 등을 통해 악성코드가 담겨져 있는 USB 사용을 유도할 수 있다. 이러한 위협을 예방하기 위해, USB 자동 실행을 허용하지 않도록 설정해야 한다.

<그림 4-10> 자동 실행 방지

⑮ 화면 보호기를 설정해야 한다.

시스템 관리 권한을 가진 사용자가 작업 중에 잠시 동안 자리를 비운 경우, 화면 보호기를 설정해 놓지 않으면 권한을 갖고 있지 않은 비인가 사용자가 시스템 관리 권한을 갖게 되는 경우가 발생할 수 있다. 이를 예방하기 위해 시스템에 화면 보호기를 설정하여 다시 로그인 시도 절차를 진행하도록 해야 한다.

<그림 4-11> 화면 보호기 설정