코드서명 인증서 보안 가이드

미래창조과학부
Ministry of Science, ICT and Future Planning

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

제1장
개요

제1장 개요

1.1 배경

개발회사에서 인터넷 상으로 소프트웨어를 배포하는 경우 사용자에게 신뢰할 만한 프로그램임을 알리기 위해 1)코드 서명한 소프트웨어를 배포한다. 코드 서명한 소프트웨어는 인증기관에서 일종의 디지털 도장을 받은 프로그램과 같다. 웹에서 소프트웨어를 다운로드 할 때 코드서명이 되지 않은 소프트웨어인 경우, 알 수 없는 게시자가 배포한 것임을 알리는 보안경고창이 뜬다. 이에 반해 코드 서명 된 경우는 개발회사 정보를 보여줌으로써 안심하고 다운받을 수 있는 인증 역할을 수행한다.

그러나 최근 APT 공격을 통해 제조사가 보관하고 있는 코드서명 인증서를 탈취하여, 악성코드를 해당 인증서로 서명, 배포하는 사례가 발생하고 있다. 코드서명 된 악성코드는 사용자 입장에서 개발 회사를 통해 정상적으로 배포된 파일로 인식되기 때문에 파급력이 크다. 이는 대부분 코드서명 인증서 관리 미흡으로 인해 발생한다. 공격자는 인증서 관리가 취약한 부분을 악용하여 악성코드 삽입을 통해 인증서를 탈취한다. 최종적으로 악성코드를 코드서명 한 후 전파시키는 방식의 사례가 나타하고 있다. 관리 미흡으로 인해 침해사고 사례가 발생하는 것이니만큼 보안 관리 및 침해사고 대응체계를 업데이트 시킬 필요가 있다.

이에 본 가이드에서는 코드서명 인증서 관리 미흡으로 인해 발생하는 침해사고 위협 사례를 다루어 그 위험성을 인지하도록 한다. 또한 개발회사에서 코드서명 인증서 관리시 반영하여야 할 사항을 제공함으로써 사고 예방 및 피해를 최소화하고자 한다.

1) 코드서명 : 인터넷 환경 또는 컴퓨터에 사용되는 소프트웨어 개발사를 인증하는 전자 서명 방법

1.2 가이드 목적 및 구성

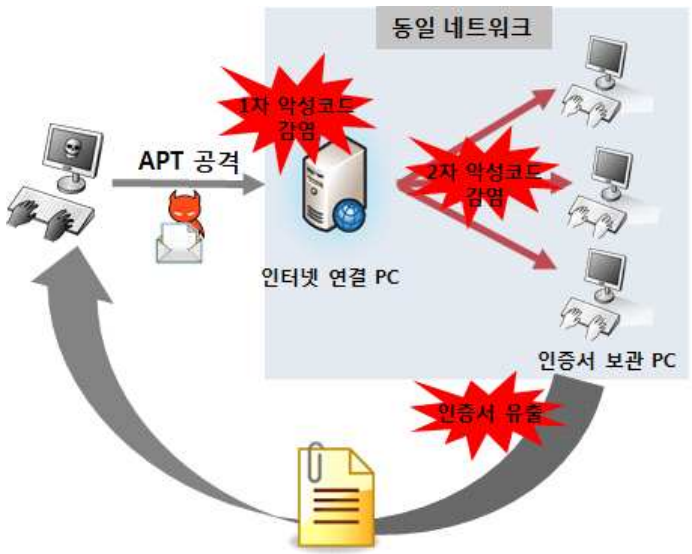
목적	- 코드서명 인증서 관리 위협 심각성 인지를 통한 보안 인식 제고 - 안전한 코드서명 관리를 위한 침해사고 예방 및 피해 최소화
대상	- 코드서명 인증서 관리자
범위	- 코드서명 관리 시 지켜야 할 사항
구성	- [1장] 개요 1.1 배경 1.2 가이드 목적 및 구성 - [2장] 인증서 관리 미흡 악용 사례 - [3장] 코드서명 인증서 보안 가이드 3.1 인증서 관리 3.2 인증서 관리 시스템 3.3 보안 업데이트 체계 3.4 침해사고 발생 시 사고대응체계 - [4장] 코드서명 인증서 보안 가이드 해설서

제2장
인증서 관리 미흡 악용 사례

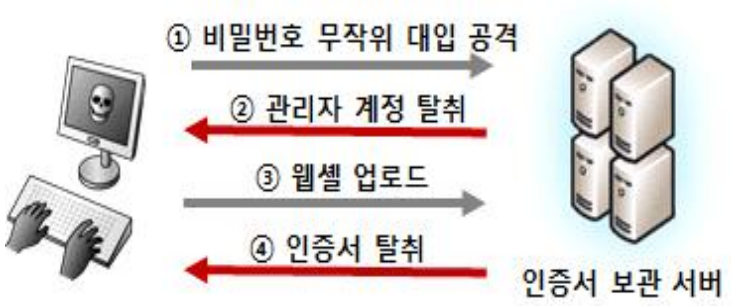
제2장 인증서 관리 미흡 악용 사례

코드서명 인증서를 개발자 PC에서 관리하거나 사내 인터넷망 내에서 인증서 PC를 관리하는 경우, 인증서를 탈취하는 사례가 발생하였다. 공격자는 사내 PC 중 하나를 악성코드에 감염시켰다. 이후 같은 망에서 사용하는 공용 솔루션 취약점 등을 악용하여 인증서 PC에 접근함으로써 인증서를 탈취한 사례이다. 또 인증서 보관을 웹서버에서 하고 있는 경우 공격자가 웹사이트 관리자 페이지에 접근하여 계정 무작위 대입 공격을 통해 인증서 탈취, 악성코드 위장 배포에 악용한 사례가 존재한다.

<그림 2-1> 인증서 보관 PC를 혼용해서 사용 했을 경우



<그림 2-2> 인증서 보관 서버를 웹서버로 사용 했을 경우



제3장

코드서명 인증서 보안 가이드

제3장 코드 서명 인증서 보안 가이드

3.1 인증서 관리

- **(별도의 인증서 관리 시스템 유무)** 서명 작업을 수행하는 시스템 및 인증서 관리 시스템은 일반 업무 PC와 혼용하여 사용할 수 없다.
- **(시스템 망 분리)** 서명 작업을 수행하는 시스템은 망 분리가 이루어져야 하며, 타임스탬프 포트를 제외한 모든 포트를 차단해야 한다.
- **(시스템 접근통제)** 서명 작업을 수행하는 시스템은 지정된 관리자 외 접근을 차단해야 한다.
- **(인증서 접근통제 및 승인)** 인증서에는 관리자 혹은 관리자가 지정한 사람만 접근 가능해야 하며, 인증서 복사·변경·삭제 등의 작업 수행 전 관리자 승인이 있어야 한다.
- **(인증서 보관의 안정성)** 인증서는 별도의 안전한 매체에 저장해야 하며, 매체 접근 시 패스워드를 요구해야 한다. 또한 지정된 매체 외 보관된 인증서는 삭제해야 한다.
- **(패스워드 변경 주기)** 패스워드는 분기별 1회 이상 변경해야 한다. 또한, 패스워드 변경 이력을 기록해야 한다.
- **(패스워드 조합 구성)** 패스워드는 숫자, 대소문자, 특수문자를 포함하여 2조합 10자 이상 또는 3조합 8자 이상으로 구성해야 한다.
- **(인증서 사용 로그 기록 및 승인)** 코드 서명을 위해 인증서 사용 시 작업 일지를 기록해야 하고, 관리자의 승인을 받아야 한다.
- **(인증서 작업일지 검토)** 관리자는 주 1회 이상 작업일지의 이상 유무를 검토해야 한다.

o **(보안성 검토 수행)** 서명 작업 시스템과 인증서 관리 시스템에 대해 반기별 1회 이상 자체적으로 취약점 점검을 수행해야 한다.

3.2 인증서 관리 시스템

o **(취약한 패스워드 설정)** 시스템 계정의 패스워드는 2조합 10글자 또는 3조합 8글자 이상으로 설정해야 한다.

o **(패스워드 복잡도 정책 설정)** 시스템의 패스워드 복잡도(2조합 10글자 또는 3조합 8글자) 정책을 설정해야 한다.

o **(주기적인 패스워드 변경)** 패스워드는 분기별 1회 이상 변경해야 한다.

o **(자동 로그인 금지)** 시스템 계정은 자동 로그인으로 설정해서는 안 된다.

o **(불필요한 계정 삭제)** 임시로 생성한 계정 등의 불필요한 계정은 제거하고, 실제 사용하는 계정만 남겨둬야 한다.

o **(공용 계정 삭제)** 관리자가 사용하는 계정은 다른 직원과 공용으로 사용되어서는 안 된다.

o **(최소한의 관리자 계정 사용)** 관리자 계정은 실제 사용하는 계정만 설정하여 최소한으로 사용해야 한다.

o **(인터넷 접속 차단)** 관리 시스템은 외부 인터넷 접속을 허용해서는 안 되며, 관리에 필요한 포트만 화이트리스트 기반으로 관리해야 한다.

o **(공유 폴더 차단)** 시스템 내 공유 폴더를 생성해서는 안 된다.

o **(불필요한 서비스 삭제)** 시스템 내 모든 불필요한 서비스는 제거해야 한다.

o **(불필요한 프로그램 삭제)** 메신저, 원격제어 프로그램 등 불필요한 프로그램을 사용할 수 없다.

o **(백신 프로그램 설치)** 백신 프로그램을 한 개 이상 설치해야 한다.

o **(백신 프로그램의 최신 업데이트)** 백신 프로그램은 최신 업데이트를 주기적으로 수행하여 최신버전으로 유지해야 한다.

o **(최신 패치 적용)** 시스템에 설치된 소프트웨어 버전을 최신버전으로 유지해야 한다.

o **(USB 등의 미디어 자동 실행 차단)** USB 등의 미디어가 자동으로 실행되지 않도록 설정해야 한다.

o **(화면 보호기 설정)** 시스템에 화면 보호기를 설정해야 한다.

o **(윈도우 이벤트 로그 및 리눅스 로그 설정 여부)** 시스템 로그는 최소 6개월 이상 로그를 기록하도록 설정해야 한다.

3.3 보안 업데이트 체계

o **(보안 업데이트 무결성 검증)** 실행파일, 비실행파일, 업데이트 정책 파일 등 업데이트 관련 파일 무결성을 검증해야 한다.

o **(안전한 무결성 검증 기술 사용)** 무결성 검증 시 CRC 등 우회가 가능한 방법을 사용해서는 안 된다.

o **(보안 업데이트 서버 IP, URL 변조 확인)** 공격자가 업데이트 설정 파일 등의 서버 주소 변조를 대비하여 변조 여부를 확인해야 한다.

o **(업데이트 클라이언트, 서버 간 상호 인증)** 위장 업데이트 서버를 구축할 경우 정상 업데이트 서버로 오인하여 업데이트가 수행할 수 있기 때문에 상호 인증을 수행해야 한다.

o **(클라이언트 원격 업데이트 포트 상시 오픈 제한)** 클라이언트의 업데이트 포트가 상시로 오픈되어 있어서는 안 된다.

o **(안전한 암호화 알고리즘 및 키 관리)** 보안 업데이트 관련 파일 보호에 적용한 암호화 시 취약한 알고리즘을 사용하면 안 된다.

o **(안전한 보안 업데이트 업로드 소프트웨어 계정 사용)** 업데이트 파일 업로드 및 파일 동기화 소프트웨어의 불필요한 계정은 제거해야 하며, 안전한 패스워드를 사용해야 한다.

o **(보안 업데이트 파일 업로드 시 사용자 인증)** 보안 업데이트 파일 업로드 시 신뢰된 사용자만 업로드 할 수 있도록 인증 방식이 구현되어 있어야 한다.

o **(보안 업데이트 파일 업로드 전 관리자 승인 실시)** 관리자가 승인한 후에만 보안 업데이트 파일을 업로드 할 수 있도록 하는 승인 절차가 존재해야 한다.

o **(보안 업데이트 업로드 소프트웨어 ID, 패스워드 암호화 전송)** 보안 업데이트 파일 업로드 소프트웨어의 ID, 패스워드 전송 시 암호화를 해야 한다.

o **(보안 업데이트 업로드 소프트웨어 접근통제 설정)** 보안 업데이트 파일 업로드 소프트웨어에 대한 접근통제를 수행해야 한다.

o **(보안 업데이트 관련 관리자 지정)** 보안 업데이트 파일을 업로드하는 관리자를 별도로 지정해야 한다.

o **(보안 업데이트 파일 코드 서명)** 실행파일, 비실행파일 등 업데이트 관련 파일의 코드 서명을 수행해야 한다.

o **(보안 업데이트 파일의 인증서 상태(유효기간, 인증 경로, 해지 여부 등) 검사)** 코드 서명에 사용한 인증서 유효기간 만료 여부 등을 확인해야 한다.

o **(코드 서명 생성 서버와 업데이트 서버 분리 사용)** 코드 서명은 업데이트 서버가 아닌 별도의 시스템에서 수행해야 한다.

3.4 침해사고 발생 시 사고대응체계

- **(인증서 폐기 절차 마련)** 인증서 유출 또는 위험 발생을 대비하여 인증서 폐기 절차에 대한 지침을 마련해야 한다.

- **(비상연락망 구축)** 사고 발생 시 대응 연락망을 구축하여 신속한 대응이 가능하도록 해야 한다.

- **(로그 관리)** 서명 작업 시스템 및 인증서 관리 시스템 로그는 6개월 이상 보관해야 한다.

제4장
코드서명 인증서
보안 가이드 항목 해설서

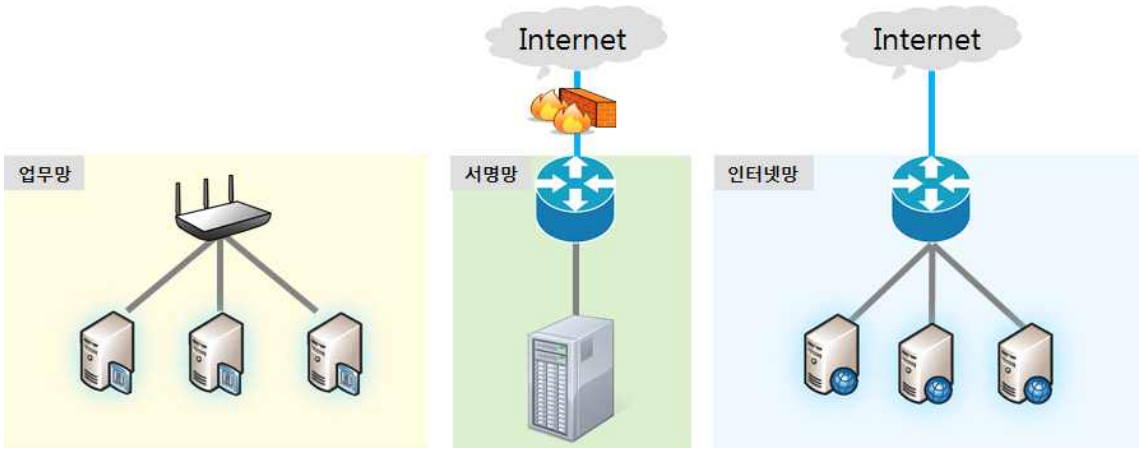
제4장 코드서명 인증서 관리 보안 가이드 항목 해설서

■ 인증서 관리

① 서명 작업을 수행하는 시스템 및 인증서 관리 시스템은 일반 업무 PC와 혼용하여 사용할 수 없다. ② 서명 작업을 수행하는 시스템은 망 분리가 이루어져야 하며, 타임스탬프 포트를 제외한 모든 포트를 차단해야 한다.

서명 작업에 사용되는 인증서는 외부로 유출 되어서는 안 되며, 외부에서 접근하지 못하도록 관리해야 한다. 이를 위해 서명 작업을 수행하는 시스템은 개발용 PC, 인터넷용(업무용) PC와는 별도의 네트워크 망에 구축되어야 한다. 하지만, 코드 서명 작업 시 필요한 타임스탬프 정보를 위해 인터넷에 연결하거나, 업무용 PC에 인증서를 저장하여 사용하는 경우가 있다. 이렇게 망을 혼용함으로 인해 외부에서 접근이 가능할 경우, 내부 자원을 유출하는 악성코드 감염 등 위험이 높아질 수 있다.

<그림 4-1> 인증서 서명 작업 시스템의 별도 망 구성

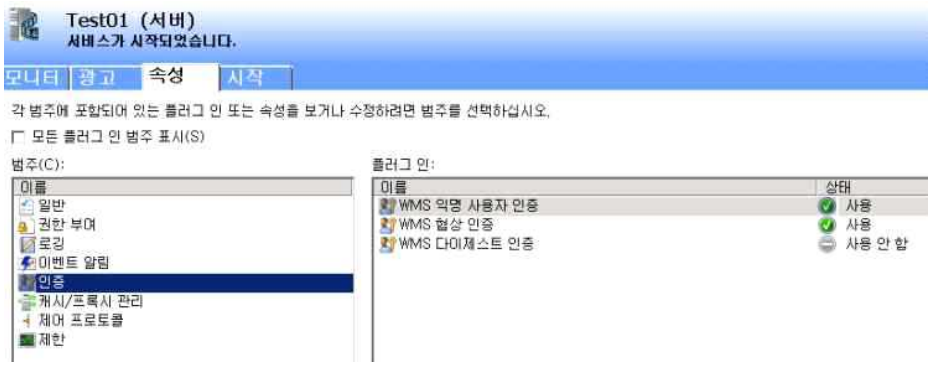


이에 서명 작업을 수행하기 위한 인증서를 보관함에 있어 업무용, 인터넷용 PC를 별도의 네트워크 망에 연결하고 타임스탬프 포트를 제외한 모든 포트를 차단하도록 해야 한다.

③ 서명 작업을 수행하는 시스템은 지정된 관리자 외 접근을 차단해야 한다.
④ 인증서에는 관리자 혹은 관리자가 지정한 사람만 접근 가능해야 하며, 인증서 복사·변경·삭제 등의 작업 수행 전 관리자 승인이 있어야 한다.
⑤ 인증서는 별도의 안전한 매체에 저장해야 하며, 매체 접근 시 패스워드를 요구해야 한다. 또한 지정된 매체 외에 보관된 인증서는 삭제해야 한다.

일부 업체에서는 관리 편의를 위해 개발자들 개개인이 인증서를 가지고 있거나 필요시 마다 USB에 무분별하게 인증서를 복사하여 서명을 하는 경우가 존재한다. 안전한 인증서 보관 방법과 접근통제를 수행하지 않으면 침해사고가 발생할 경우, 인증서 유출 여부를 명확하게 인지할 수 없다. 따라서 인증서는 관리자 또는 관리자가 지정한 사람만 접근 가능해야 하며, 매체에 보관 시 패스워드나 지문을 인식하는 등 보안 설정이 가능한 매체에 보관해야 한다.

<그림 4-2> 익명 사용자가 해당 시스템에 접근 가능하도록 설정되어 있는 경우



⑥ 패스워드는 분기별 1회 이상 변경해야 한다. 또한, 패스워드 변경 이력을 기록해야 한다.
⑦ 패스워드는 숫자, 대소문자, 특수문자를 포함하여 2조합 10자 이상 또는 3조합 8글자 이상으로 구성해야 한다.

코드 서명 시 사용하는 패스워드는 외부 유출에 대비하여 주기적인 관리가 필요하다. 관리자는 패스워드가 악성코드에 의해 타인에게 알려진 사실을 인지하지 못하더라도 분기별로 패스워드를 변경하게 되면, 유출된 패스워드에 의해 지속적으로 악용되는 상황을 피할 수 있다. 이에 패스워드는 분기별로 변경해야하며, 변경 이력을 기록해 관리해야 한다. 패스워드 복잡도는 다음과 같은 구성으로 어려운 패스워드를 사용하도록 한다.

<그림 4-3> 패스워드 복잡도 설정방법

⑧ 코드 서명을 위해 인증서 사용 시 작업일지를 기록해야 하고, 관리자의 승인을 받아야 한다.
⑨ 관리자는 주 1회 이상 작업일지의 이상 유무를 검토해야 한다.

코드 서명 관리자 또는 관리자의 승인을 받은 사람은 코드 서명 시 작업일지를 기록해 서명 작업 이력을 남겨 놓아야 한다. 작업일지는 관리자가 주기적으로 검토하여 승인 받지 않은 사용 내역을 검토해야 한다. 이러한 승인 절차 및 이상 유무 검토는 사고 발생 시 이상 사항을 적발하는데 도움이 될 수 있다.

⑩ 서명 작업 시스템과 인증서 관리 시스템에 대해 반기별 1회 이상 자체적으로 취약점 점검을 수행해야 한다.

인증서 관리 시스템은 폐쇄망에서 운영하지 않을 경우, 외부에서 서버 취약점을 통해 침투할 가능성이 존재한다. 또한, 분리된 망에서 운영하더라도 악성코드가 취약점을 악용한 2차 침투가 발생할 수 있기 때문에 개발사는 서명 작업 시스템과 인증서 관리 시스템에 대해 자체적으로 보안성 검토를 수행해야 한다. 자체적으로 보안성 검토가 어려운 경우, 외부 컨설팅을 받을 때 해당 시스템들도 포함시켜 점검을 받도록 해야 한다.

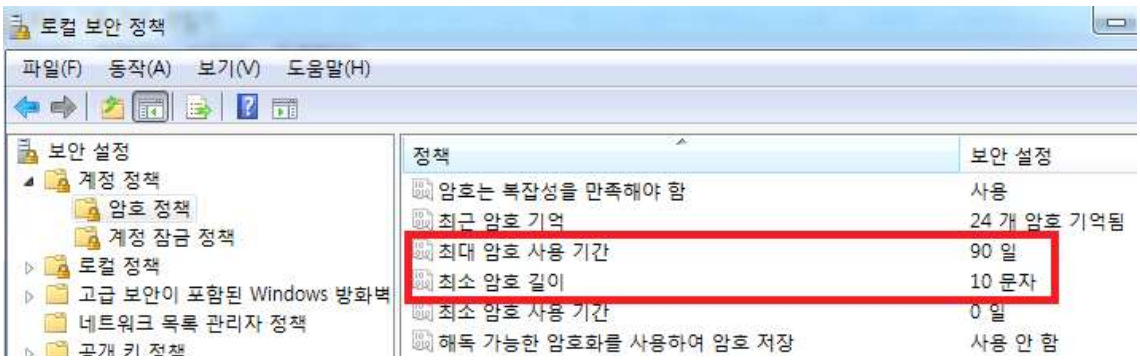
■ 인증서 관리 시스템

① 시스템 계정의 패스워드는 2조합 10글자 또는 3조합 8글자 이상으로 설정해야 한다.
② 시스템의 패스워드 복잡도(2조합 10글자 또는 3조합 8글자) 정책을 설정해야 한다.
③ 패스워드는 분기별 1회 이상 변경해야 한다.
④ 시스템 계정은 자동 로그인으로 설정해서는 안 된다.

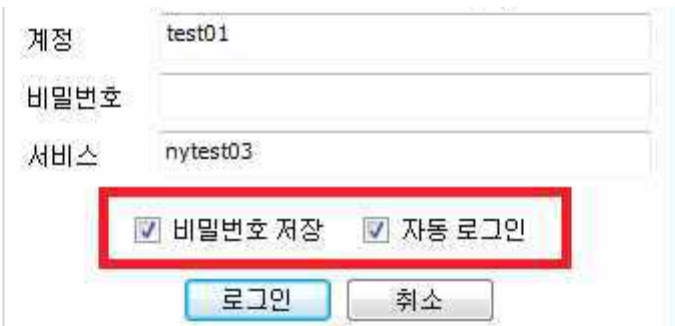
시스템 계정 설정 시 ID/패스워드를 admin/admin 또는 패스워드가 12345678 등과 같이 유추하기 쉽게 설정되어 있는 상태는 암호화 설정을 하지 않은 보안수준에 해당한다. 이에 ID/패스워드의 경우 설정 없이 접속할 수 없도록 기본 설정으로 하여야 한다. 그리고 아래 그림과 같이 2조합 10글자 또는 3조합 8글자 길이의 패스워드를 설정하여야 한다. 또한 시스템 계정의 패스워드는 최소 분기별 1회 이상 변경하여, 기존 담당자의 이직/퇴사 등 패스워드가 알려졌을 경우에 대한 대책을 마련해야 한다.

관리할 시스템이 많을 경우 관리 편의성을 위해 관리 페이지나 시스템에 접속하는 계정에 대해 자동 로그인 설정을 하는 경우가 많다. 이는 ID/패스워드를 설정하지 않은 것과 같으므로 자동 로그인 기능이 있다 하더라도 반드시 자동 로그인 설정을 해지해야 한다.

<그림 4-4> 패스워드 정책 설정



<그림 4-5> 자동 로그인으로 설정되어 있는 경우



⑤ 임시로 생성한 계정 등의 불필요한 계정은 제거하고, 실제 사용하는 계정만 남겨둬야 한다.
⑥ 관리자가 사용하는 계정은 다른 직원과 공용으로 사용 되어서는 안 된다.
⑦ 관리자 계정은 실제 사용하는 계정만 설정하여 최소한으로 사용해야 한다.

특정 작업을 위해 계정을 임시로 생성하였으나, 작업 후 계정을 삭제하지 않아 관리되지 않는 경우가 발생할 수 있다. 이런 불필요한 계정은 공격자에 의해 악용될 가능성이 있기에 실제 사용하는 계정만 남겨두어야 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 4-6> 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 관리 시스템은 외부 인터넷 접속을 허용해서는 안 되며, 관리에 필요한 포트만 화이트리스트 기반으로 관리해야 한다.
⑨ 시스템 내 공유 폴더를 생성해서는 안 된다.

인증서를 관리하는 시스템은 외부에 노출 되어서는 안 되며, 외부에서 접근하지 못하도록 관리해야 한다. 관리 시스템을 통해 외부 인터넷 접속을 할 경우, 악성코드에 감염될 가능성이 더욱 높아지며 인증서 유출 위협이 증가하게 된다. 또한, 관리의 편의를 위해 시스템 내 공유 폴더를 생성하여 사용하거나 외부 인터넷 접속이 가능한 시스템을 사용할 경우 악성코드에 감염되는 등의 위협이 존재할 수 있다. 따라서 시스템 관리를 위해 업데이트 등 필요한 포트만 화이트리스트 기반으로 접근 통제하여 안전하게 관리 하도록 해야 한다.

<그림 4-7> 외부 접속 PC 악성코드 감염 후, 내부 PC로의 2차 감염 사례

<그림 4-8> 네트워크 및 공유 센터에서 파일 / 공용 폴더 공유 끄기

⑩ 시스템 내 모든 불필요한 서비스는 제거해야 한다. ⑪ 메신저, 원격제어 프로그램 등 불필요한 프로그램을 사용할 수 없다.

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

⑫ 백신 프로그램을 한 개 이상 설치해야 한다.
⑬ 백신 프로그램은 최신 업데이트를 주기적으로 수행하여 최신버전으로 유지해야 한다.
⑭ 시스템에 설치된 소프트웨어 버전을 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 한 개 이상의 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.

⑮ 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. 내부망 침해를 목적으로 제작된 악성코드를 외부 저장매체에 담아 사회공학적 기법 등을 통해 악성코드가 담겨져 있는 USB 사용을 유도할 수 있다. 이러한 위협을 예방하기 위해, USB 자동 실행을 허용하지 않도록 설정해야 한다.

<그림 4-9> 자동 실행 방지

⑯ 시스템에 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 4-10> 화면 보호기 설정

⑰ 시스템 로그는 최소 6개월 이상 로그를 기록하도록 설정해야 한다.

침해사고가 발생한 경우, 정확한 사고분석을 위해 반드시 필요한 시스템 로그는 최소 6개월 이상 기록하고 보관해야 한다. 정확한 사고분석이 이루어지지 않으면, 어떻게 공격이 이루어졌는지, 어떠한 정보가 유출됐는지 파악하기 어려워지게 된다. 시스템 로그를 활용한 사고분석을 통해 어떻게 공격이 이루어졌는지 파악하고 사고 재발 방지를 위해 시스템 로그 기록을 유지해야 한다.

<그림 4-11> 시스템 로그 보관 기간 설정

■ 보안 업데이트 체계

① 실행파일, 비실행파일, 업데이트 정책 파일 등 업데이트 관련 파일의 무결성을 검증해야 한다.
② 무결성 검증 시 CRC 등 우회가 가능한 방법을 사용해서는 안 된다.
③ 공격자가 업데이트 설정 파일 등 서버 주소 변조를 대비하여 변조 여부를 확인해야 한다.
④ 위장 업데이트 서버를 구축할 경우 정상 업데이트 서버로 오인하여 업데이트가 수행되기 때문에 상호 인증을 수행해야 한다.

기능 추가, 취약점 보완 등을 통한 업데이트 시 파일 무결성 검증을 통해, 인가되지 않은 제 3자에 의하여 수정 또는 삭제되는 것을 방지해야 한다.

무결성 검증 시 사용되는 알고리즘은 SHA-2와 같은 안전한 검증 기법을 사용하는 것이 좋다.

<그림 4-12> 각 해시 알고리즘 특징

구분	MD5 (Message-Digest algorithm 5)	SHA-1 (Secure Hash Algorithm-1)	SHA-2 (Secure Hash Algorithm-2)
검증	• 128비트 체크섬 확인	• 160 비트 체크섬 확인	• 224/256/384/512 비트 체크섬 확인
암호화	• xor, and, or 연산으로 암호화	• +, and, or, xor, rotl 연산으로 암호화	• +, and, or, xor, rotr, shr 연산으로 암호화
보안성	• 설계상 결함이 있음	• 공격법이 존재	• 아직 공격법이 발견되지 않음

지난 3.20 사이버테러 사건과 같이 APT 공격에 의해 업데이트 서버가 악성코드 유포지로 악용되는 것을 방지하기 위해 업데이트 서버 주소가 변조되어있는지 변조 여부를 확인해야 한다. 또한, 공격자가 위장 업데이트 서버를 구축하여 악성코드를 유포할 가능성이 있기 때문에, 클라이언트와 정상 업데이트 서버 간 상호 인증을 수행해야 한다.

⑤ 클라이언트의 업데이트 포트가 상시로 오픈되어 있어서는 안 된다.

불필요한 포트 오픈은 공격자 입장에서 공격을 시도할 수 있는 수단과 방법이 늘어나게 되는 것과 같다. 업데이트는 자주 이루어지는 작업이 아니기 때문에, 필요할 때만 포트를 오픈하며 업데이트를 하지 않을 때는 포트를 닫아두는 것이 안전하다.

<그림 4-13> 불필요한 포트가 오픈된 상태

⑥ 보안 업데이트 관련 파일 보호에 적용한 암호화 시 취약한 알고리즘을 사용하면 안 된다.

소프트웨어를 최신 버전으로 업데이트하는 것처럼, 업데이트 파일 암호화 시 취약한 알고리즘을 사용할 경우 키가 유출될 위협이 있다. 따라서 안전한 알고리즘(비대칭키 등)을 사용하여 암호화를 수행해야 한다.

⑦ 업데이트 파일 업로드 소프트웨어 및 파일 동기화 소프트웨어의 불필요한 계정은 제거해야 하며, 안전한 패스워드를 사용해야 한다.

불필요한 계정이 많으면 많을수록 공격자의 수단과 방법이 늘어나게 되는 것과 같기 때문에 실제 사용하는 계정만 남겨두어야 한다. 또한 앞에서 설명했던 것처럼 2조합 10글자 또는 3조합 8글자 길이의 패스워드를 설정하여야 한다.

⑧ 보안 업데이트 파일 업로드 시 신뢰된 사용자만 업로드 할 수 있도록 인증 방식이 구현되어 있어야 한다.
⑨ 관리자가 승인한 이후에 보안 업데이트 파일을 업로드 할 수 있도록 하는 승인 절차가 존재해야 한다.
⑩ 보안 업데이트 파일 소프트웨어의 ID/패스워드에 대한 전송 시 암호화를 해야 한다.
⑪ 보안 업데이트 파일 업로드 소프트웨어에 대한 접근통제를 수행해야 한다.
⑫ 보안 업데이트 파일을 업로드 하는 관리자를 별도로 지정해야 한다.

보안 업데이트 파일을 업로드 할 때에는 인가된 사용자만 업로드 할 수 있도록 조치해야 한다. 비인가 된 사용자가 보안 업데이트 파일을 악성코드 삽입하여 업로드하게 될 경우, 업데이트 체계가 악성코드 유포지로 악용될 위협이 있다. 그러므로 신뢰된 사용자만 업로드 할 수 있도록 인증 방식을 구현해야 한다. 사용자에 대한 인증을 제공할 때에는 아래와 같이 각 유형의 인증 방법을 2개 이상 결합하여 Multi-Factor 인증으로 제공해야 안전하다. 이 때, 같은 유형(ex: Type1 + Type1)의 인증으로 2개 이상 결합하면 약간의 안전성을 보장받을 수 있지만, 다른 유형(ex : Type1 + Type 3)의 인증 결합 방식보다는 안전성이 떨어진다.

또한, 신뢰된 사용자라 하더라도 관리자 승인 절차를 마련하여, 신뢰된 사용자의 실수 혹은 변심에 따른 악성코드 유포에 대한 대비를 마련해야 한다.

<그림 4-14> 각 유형별 인증 수단

유형	인증수단
Type 1 (지식기반)	PIN, ID, 패스워드, 계좌번호 등
Type 2 (소유기반)	IC 카드, 토큰, 디지털 인증서, 인증 디바이스
Type 3 (신체기반)	지문, 홍채, 망막, 정맥, 얼굴

보안 업데이트 소프트웨어에 로그인, 패스워드 변경 등 ID/패스워드 인증 절차가 있을 때 암호화를 하고 전송해야 한다. 평문으로 전송 될 경우 계정정보가 유출되어 비인가 된 사용자가 권한 탈취, 악성코드 유포지로 활용할 위협이 있다.

<그림 4-15> ID/패스워드를 평문으로 전송하는 경우

보안 업데이트 소프트웨어를 이용할 때는 사용자 그룹(업무 단위 등)마다 사용 권한을 세분화하여 지정하며 관리자를 별도 지정해야 한다. 여기서 중요한 점은 부여하는 사용 권한을 최소한으로 해야 한다는 것이다. 예를 들어, 보안 업데이트 소프트웨어에 접근하여 읽기·쓰기·업데이트 실행 권한 등과 같이 권한 설정을 세분화 한다면 위험을 더욱 줄일 수 있다. 접근 권한은 이직/퇴사 또는 인사이동 등에 의한 사용자의 담당 업무 변경에 따른 규정이 정해져 있는 것이 중요하다.

⑬ 실행파일, 비실행파일 등 업데이트 관련 파일의 코드 서명을 수행해야 한다.
⑭ 코드 서명에 사용한 인증서의 유효기간 만료 여부 등을 확인해야 한다.

업데이트에 대한 파일에도 마찬가지로 코드 서명 절차를 수행해야 한다. 코드 서명을 통해 클라이언트 측에서 안심하고 업데이트를 진행할 수 있도록 인증 역할을 부여해 줘야한다. 코드 서명에 사용되는 인증서의 유효기간을 사전에 파악, 유효기간이 만료된 인증서로 코드 서명이 이루어지는 일이 없도록 해야 한다.

⑮ 코드 서명은 업데이트 서버가 아닌 별도의 시스템에서 수행해야 한다.

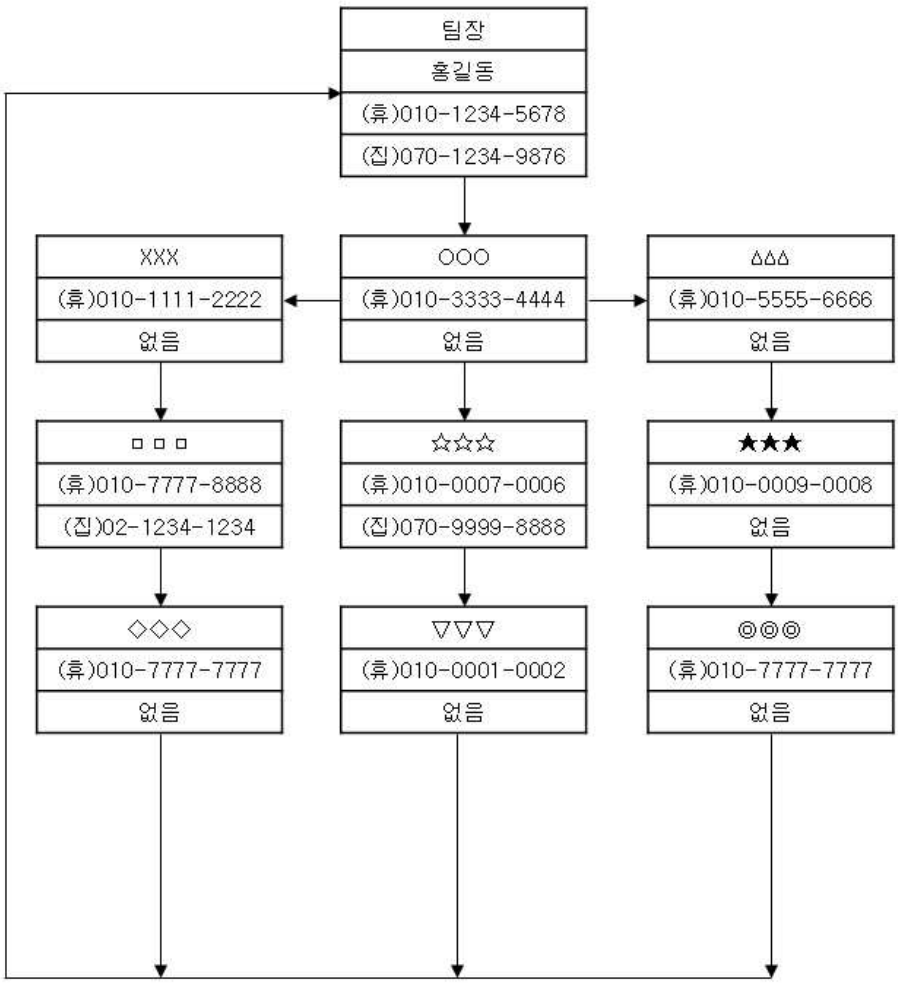
일부 업체에서는 편의를 위해 서버를 용도별로 구분하여 사용하지 않고, 하나의 서버에 업데이트와 코드 서명을 같이 진행하고 있다. 이러한 경우, 악성코드에 감염되었을 경우 피해가 더욱 커질 위협이 있다. 따라서 업데이트 서버와 코드 서명을 진행하는 시스템을 별도로 구분하여 관리 · 운영해야 한다.

■ 침해사고 발생 시 사고대응체계

① 인증서 유출 또는 위험 발생을 대비하여 인증서 폐기 절차에 대한 지침을 마련해야 한다.
② 사고 발생 시 대응 연락망을 구축하여 신속한 대응이 가능하도록 해야 한다.

인증서가 유출 되었을 경우, 즉시 인증서를 폐기하고 인증서 재발급 절차를 진행한다. 배포된 소프트웨어를 재발급한 인증서로 코드 서명하여 재배포하는 등 인증서 관련된 침해사고 발생 시 사고대응 체계 수립이 필요하다. 인증서 폐기 절차에 대한 지침을 마련하여 인증서로 코드 서명한 악성코드 대응이 늦어지지 않도록 해야 한다. 또한 사고 발생 시 비상 대응 연락망을 구축하여 신속한 대응이 가능하도록 해야 한다.

<그림 4-16> 사고 발생 시 비상 대응 연락망 예시



③ 서명 작업 시스템 및 인증서 관리 시스템 로그는 6개월 이상 보관해야 한다.

침해사고 발생 시 가장 먼저 해야 할 일과, 가장 중요한 일은 로그 분석이다. 로그가 없으면 원인규명 및 공격자 식별이 불가능하다. 그렇기 때문에 로그 관리가 무엇보다 중요하다. 따라서 발생한 보안 이벤트들의 상황 및 피해 여부 등의 로그를 기록하고 안전한 곳에 보관해야 한다. 이를 통해 해당 환경의 취약점을 파악할 수 있고, 사고 로그를 통하여 사고 발생 시점 이후 사건의 추적성을 확보할 수 있다. 또한, 유사한 사례가 발생하였을 경우 사고 로그 관리를 통하여 악의적인 사용자의 추적 및 대응에 활용 할 수 있다.