발간사

최근 인터넷을 비롯한 정보 통신 인프라의 발전은 정보혁명을 더욱 가속화시킴과 동시에 과학, 사회, 경제, 문화 심지어 정치영역까지 큰 영향을 미치고 있으며, 이와 더불어 홈페이지 서버들도 개인이 보유할 정도로 보급이 확산되고 있어, 그 중요도도 나날이 증가하고 있습니다.

특히, 최근 급증하고 있는 홈페이지 해킹은 국가 경쟁력을 좌우하는 첨단과학기술관련국가 중요 시설 및 정보지원에 대한 정보 침해가 빈번하게 발생하고, 홈페이지가 정보화의 기반요소로 자리 매김 해 가고 있는 현 시점에서 크나큰 걸림돌로 작용할 수 있습니다.

이러한 홈페이지 해킹에 대비하여 웹 방화벽, 웹 스캐너등 웹 전용 보안장비 도입 · 운영하여 홈페이지 강화에 많은 노력을 기울이고 있으나, 홈페이지 운영 · 관리에 대한 프로세스가 정립되지 않아서 한계성을 조금씩 보이고 있습니다.

이에 과학기술정보보호센터(S&T-SEC)는 홈페이지 보안 프로세스 정립을 위하여 웹 서버 운영체제와 운영에 관련 된 보안 준수사항을 기술하고자 하며, 특히 기 구축 운영 중인 홈페이지 뿐만 아니라 개편 및 재개발 예정인 홈페이지에 대한 보안 프로세스 정립을 위하여 웹 어플리케이션 개발 단계부터 홈페이지 개발자들에게 반드시 필요한 보안 사항을 제시 하고자 합니다.

2007. 11. 30

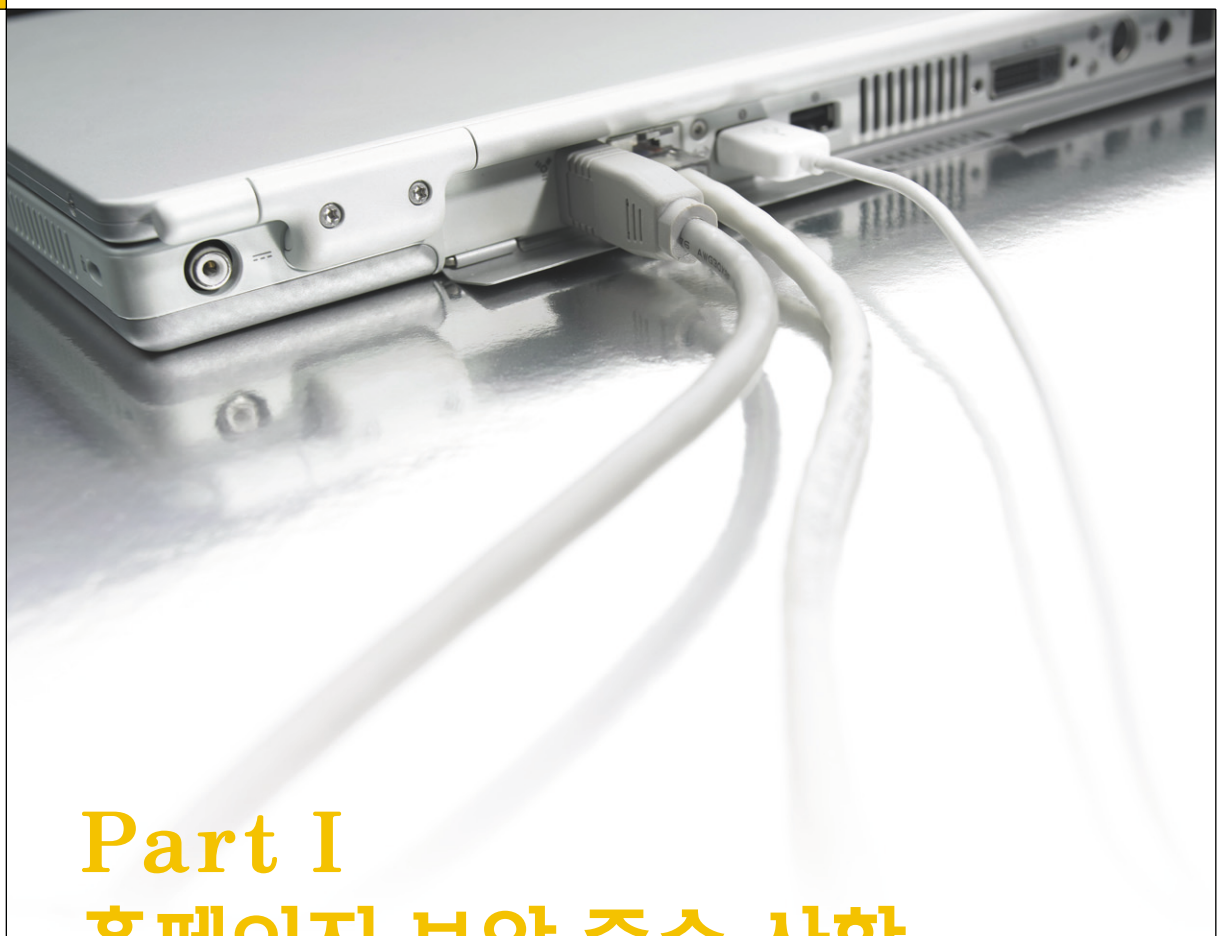
과학기술정보보호센터장

황 일 선

본 가이드는 최신 해킹 기술 및 침해시도 사례를 기반으로 과학기술 분야 특성에 맞는 안전한 홈페이지 운영 및 관리를 위하여 과학기술정보보호센터의 연구원들이 참여하여 제작 되었습니다.

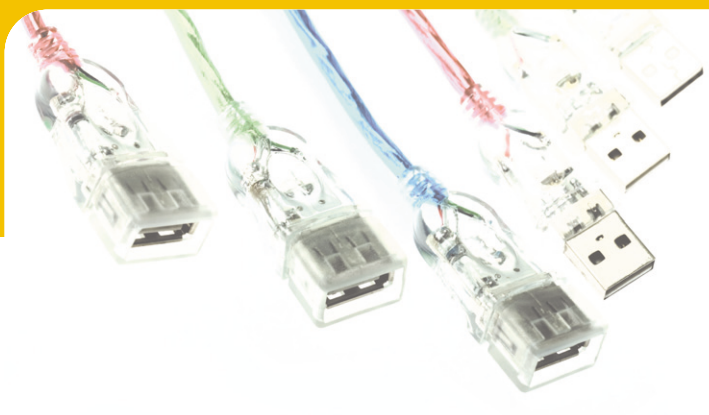
2007년 11월 30일

주관연구기관명 : 한국과학기술정보연구원
주관연구책임자 : 황일선 (고성능연구망사업단 단장)
참 여 연 구 원 : 이혁로(선임기술원) 박학수(선임연구원)
이행곤(선임연구원) 정기문(연 구 원)
최상수(연 구 원) 이호선(연 구 원)
김주범(연 구 원)



Part I
홈페이지 보안 준수 사항

Part Ⅰ 홈페이지 보안 준수 사항



1. 개요

가. 개요

미국의 보안 전문가인 브루스 슈나이어(Bruce Schneier)는 자신의 저서 '비밀과 거짓말(Secrets and lies)' 에서 다음과 같이 강조했다.

"Security is a process, not a product"

이것은 프로세스 관점에서의 보안을 역설한 것으로, 보안은 몇몇 보안 제품이나 물리적 장치를 통해서 해결될 수 있는 것이 아니며 보안 모델링, 정책 수립, 훈련 및 실행 · 통제를 통한 지속적인 투자를 필요로 하고, 보안은 과정이며 언제나 진행형이라는 것이다.

이러한 관점에서 볼 때, 많은 기관 및 기업에서는 홈페이지 보안성 강화를 위하여 웹 방화벽을 도입 · 운영하고, 정보보호 컨설팅을 통한 주기적인 홈페이지 취약점 진단을 수행하고 있는 것은 분명히 그 한계점이 존재한다는 점을 암시하고 있다고 할 수 있다.

따라서, 『보안 책임자』는 최선의 보안 기술을 구현하고 지속적인 패치를 통해 기술적 취약점을 해결하는 것은 언제나 중요한 일이라고 할 수 있다. 그러나, 이러한 이면에 존재하는 위험이나 위협이 없는지 찾아내고 분석하고 이에 대한 대응책을 강구하는 것과 모델링 및 위험 평가 등을 통해 보안 프로세스를 정립하는 것이 지금의 『보안 책임자』가 가져야 할 중요한 임무이다

나. 적용범위

과학기술부 산하 정보보호 대상기관에서 기 구축 운영중인 홈페이지와 향후 개편 및 재개발 예정인 홈페이지를 대상으로 한다.

다. 활용방법

본 장에서는 홈페이지 보안 프로세스 정립을 위하여 웹 서버 운영체제와 운영에 관련된 보안 준수사항을 기술하고자 하며, 특히 기 구축 운영 중인 홈페이지 뿐만 아니라 개편 및 재개발 예정인 홈페이지에 대한 보안 프로세스 정립을 위하여 웹 어플리케이션 개발 단계부터 홈페이지 개발자들에게 필요한 보안 준수 사항을 제시 하고자 한다.

라. 용어정의

1) OS(Operating System) : 컴퓨터의 하드웨어와 소프트웨어를 제어하여, 사용자가 컴퓨터를 쓸 수 있게 만들어주는 프로그램을 말한다.
2) 업로드(Upload) : 소규모의 시스템에서 대규모의 시스템으로 데이터를 담고 있는 파일을 이동하는 작업.
3) 인증 : 컴퓨터에서 전자화된 정보로 상대편의 신원을 확인하는 방법.
4) SSL(secure sockets layer) : 인터넷 상거래시 필요한 개인 정보를 보호하기 위한, 개인 정보 유지 프로토콜이다.
5) TLS(전송 계층 보안, Transport Layer Security) : 현재 널리 사용되고 있는 SSL(Secure Sockets Layer)을 대신하는 차세대 안전 통신 규약. SSL에 비해 강력한 암호화를 실현할 수 있고 폭이 넓은 망의 통신 규약에 대응하는 점에서 주목을 끌고 있다. 암호화에는 3개의 다른 데이터 암호화 표준(DES) 키를 사용한 트리플 DES 기술이 응용되고 있다. SSL은 TCP/IP에만 대응하지만 전송 계층 보안(TLS)은 네트웨어나 순차 패킷 교환(SPX), 애플토크(Apple-Talk) 등의 통신망 통신 규약에도 대응하고 있다. 또 오류 메시지 처리 기능이 다소 개선된 것으로 평가되고 있으며 미국 마이크로소프트사, 넷스케이프 커뮤니케이션스사가 TLS의 대응을 진행시켰다.

2. 운영체제 보안 준수 사항

웹 서버를 설치하기 전에 호스트 OS의 보안을 먼저 확실히 해두어야 한다. 아무리 웹 서버를 안전하게 설정 및 운영한다 해도, 웹 서버가 설치될 OS가 안전하지 않다면 결코 웹 서버의 안전을 보장할 수 없다.

(1) OS에 대한 최신 패치 적용

OS 벤더사이트나 보안 취약점 정보사이트를 주기적으로 방문하여 현재 사용하고 있는 OS에 대한 최신 취약점 정보를 수집하고, 패치 등 관련된 보안대책을 신속하게 적용하도록 한다[1].

(2) OS 취약점 점검

정기적으로 취약점 점검 도구와 보안 체크리스트를 활용하여 호스트 OS의 보안 취약점을 점검한다. 발견된 취약점들은 보완조치하고 조치사항은 이력관리를 위해 기록해 둔다.

(3) 웹 서버 전용 호스트로 구성

웹 서버의 중요도를 고려하여 가급적이면 웹 서버 전용 호스트로 구성하도록 한다. 웹 서비스 운영에 필요한 최소한의 프로그램들만 남겨두고, 불필요한 서비스들은 반드시 제거하도록 한다. 시스템 사용을 목적으로 하는 일반 사용자 계정들은 모두 삭제하거나 최소의 권한만 할당하여 오직 관리자만이 로그인이 가능하도록 한다.

[참고] Anonymous FTP 사용시 주의

만약 동일 서버에서 웹 서비스와 anonymous FTP를 동시에 사용해야 한다면, 웹 서비스의 문서 디렉토리가 anonymous FTP를 통해 접근이 불가능하도록 설정해야 한다. 웹 문서에 대해 설정한 접근제어가 anonymous FTP에 의해 위배될 수 있다.

[참고] 개발도구 제거

웹 서버를 구축한 후에는 컴파일러 같은 소프트웨어 개발 도구들은 공격자가 서버에 침입한 후에 익스플로잇 코드를 컴파일 하는 등 권한 상승을 위해 사용될 수 있기 때문에 제거 하도록 한다.

(4) 서버에 대한 접근 제어

관리목적의 웹 서버 접근은 콘솔 접근만을 허용하는 것이 가장 좋다. 만일 원격 접근이 필요하다면 관리자가 사용하는 PC의 IP만 접근이 가능하도록 접근제어를 수행한다.

(5) DMZ 영역에 위치

웹 서버를 DMZ 영역에 위치시키도록 한다. 웹 서버를 방화벽에 의해서 보호 받도록 하고[2], 웹 서버가 침해 당하더라도 웹 서버를 경유해서 내부 네트워크로의 침입은 불가능하도록 구성한다.

(6) 강력한 관리자 계정 패스워드 사용

관리자 계정의 패스워드 보안은 모든 보안의 기본이다. 하지만 이런 기본이 지켜지지 않아서 여전히 해킹사고가 많이 발생하고 있다. 패스워드 보안은 모든 보안의 기본이자 가장 중요한 필수 보안 사항이다.

관리자 계정의 패스워드는 유추가 불가능하고 패스워드 크랙 시 쉽게 알아낼 수 없는 강력한 패스워드를 사용하도록 한다. 패스워드는 길이가 최소한 8자 이상이고, 이름이나 계정명으로 유추할 수 없는 것이어야 한다. 또한 사전에 없는 단어를 사용하도록 하고, 기호문자를 최소 한 개 이상 포함시키도록 한다.

[1] 가급적이면 운영중인 서버에 직접 적용하지 말고 별도의 테스트 서버를 이용하여 충분한 테스트를 거친 후에 적용하는 것이 좋다.
[2] 웹 서비스가 방화벽을 통해 보호받을 수는 없지만, 방화벽을 통해 같은 서버에 존재하는 다른 서비스의 취약점을 이용한 공격은 막을 수 있다.

(7) 파일 접근권한 설정

관리자 계정이 아닌 일반 사용자 계정으로 관리자 계정이 사용하는 파일들을 변경할 수 없도록 해야 한다. 만약 관리자 계정보다 권한이 낮은 일반 계정으로 관리자가 실행하거나 쓰기를 수행하는 파일들을 변경할 수 있다면 관리자 권한 획득이 가능하다.

3. 웹 서버 설치 시 보안 준수 사항

(1) 소스코드 형태의 배포본 설치

웹 서버 소프트웨어가 소스코드와 바이너리 형태로 배포되는 경우, 보안상 가장 좋은 것은 소스코드를 다운로드 받아 필요한 기능만 설치하는 것이다.

(2) 설치시 네트워크 접속 차단

웹 서버를 설치하기 전부터 보안설정을 안전하게 끝낼 때까지 호스트의 네트워크 접속을 차단하도록 한다. 보안설정이 완전히 끝나지 않은 상태에서 웹 서버가 외부에 노출될 경우 쉽게 해킹 당할 수 있으며, 그 이후에 취해지는 보안 조치들이 의미가 없게 될 수 있다.

(3) 웹 프로세스의 권한 제한

시스템 전체적인 관점에서 웹 프로세스가 웹 서비스 운영에 필요한 최소한의 권한만을 갖도록 제한한다. 이렇게 하여 웹사이트 방문자가 웹 서비스의 취약점을 이용해 시스템에 대한 어떤 권한도 획득할 수 없도록 한다.

(4) 로그 파일의 보호

로그 파일은 침입 혹은 침입시도 등 보안 문제점을 파악하는데 중요한 정보를 제공한다. 이러한 로그 파일이 노출, 변조 혹은 삭제되지 않도록 불필요한 접근으로부터 보호한다.

(5) 웹 서비스 영역의 분리

웹 서비스 영역과 시스템(OS)영역을 분리시켜서 웹 서비스의 침해가 시스템 영역으로 확장될 가능성을 최소화한다. 웹 서버의 루트 디렉토리와 OS의 루트 디렉토리를 다르게 지정한다.

웹 컨텐츠 디렉토리와 시스템 디렉토리는 물론 가급적 다른 웹 서버 디렉토리와도 분리시킨다. 또한 로그 디렉토리와 설정 디렉토리는 웹 서비스를 통해 접근이 불가능한 곳에 위치시키도록 한다.

(6) 링크 사용금지

공개 된 웹 컨텐츠 디렉토리 안에서 서버내의 다른 디렉토리나 파일들에 접근할 수 있는 심볼릭 링크, 앨리어스, 바로가기 등을 사용하지 않는다.

(7) 자동 디렉토리 리스팅 사용중지

디렉토리 요청시 디렉토리 내에 존재하는 파일 목록을 보여주지 않도록 설정한다.디렉토리 내에 존재하는 DB 패스워드 파일이나 웹 어플리케이션 소스 코드 등 중요한 파일들에 대해 직접 접근이 가능하면 보안상 매우 위험하다. 이를 막기 위해 자동 디렉토리 리스팅 기능의 사용을 중지시킨다.

(8) 기본 문서 순서 주의

웹 서버에서는 디렉토리 요청시 기본적으로 보여지는 파일들을 지정할 수 있도록 되어 있다. 이 파일 목록을 올바로 지정하여 기본 문서가 악의적인 목적의 다른 파일로 변경되지 않도록 한다.

(9) 샘플 파일, 매뉴얼 파일, 임시 파일의 제거

웹 서버를 설치 시 기본적으로 설치되는 샘플 파일이나 매뉴얼 파일은 시스템 관련 정보를 노출하거나 해킹에 악용될 수 있다. 따라서 웹 서버 설치 후에 반드시 이러한 파일들을 찾아서 삭제하도록 한다.

만약 관리 등의 이유로 웹을 통해 설명문서에 접근해야 한다면 접근제어를 통해 꼭 필요한 사용자만 접근을 허용하고 그 외의 사용자들은 접근하지 못하도록 설정한다.

또한 웹 서버를 정기적으로 검사하여 임시 파일들을 삭제하도록 한다. 특히 웹 서비스의 업데이트나 유지보수시 생성되는 백업파일이나 중요한 파일 등은 작업이 끝난 후 반드시 삭제하도록 한다.

정확한 관리를 위해 폴더와 파일의 이름과 위치, 개수 등이 적혀있는 별도의 문서를 관리하는 것이 좋다. 그래서 문서에 등록되지 않은 불필요한 파일들을 점검해서 삭제하도록 한다.

(10) 웹 서버에 대한 불필요한 정보 노출 방지

웹 서버 종류, 사용 OS, 사용자 계정 이름 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 한다. 이러한 정보가 사소한 것처럼 보일 수 있지만, 이러한 정보를 아는 것만으로도 공격에 필요한 나머지 정보를 수집하는데 도움이 될 수 있다.

뉴스그룹이나 메일링 리스트를 통해 웹 서버 운영에 대한 질의를 할 경우에도, 조직의 네트워크와 시스템에 대한 상세정보가 유출되지 않도록 주의한다[3].

(11) 업로드 제어

불필요한 파일 업로드는 허용하지 않는것이 안전하다. 만일 파일 업로드를 허용해야 한다면, 대량의 업로드로 인한 서비스 불능상태가 발생하지 않도록 해야 하고 업로드를 허용해야 하는 파일의 종류를 지정하여 그 외 종류의 파일들은 업로드가 불가능하도록 한다. 업로드 된 파일은 웹 서버에 의해 바로 처리되지 못하도록 해야 하며 처리되기전에 반드시 수동이나 자동으로 파일의 보안성 검토를 수행하도록 한다.

---

[3] 실제로 한 보안 컨설팅 회사는 인터넷에 공개된 정보를 기반으로 CIA의 네트워크에 대한 상세한 지도를 그릴 수 있었다. 이 정보가 비록 기밀성이 떨어지는 정보일지는 몰라도 해킹을 위한 좋은 출발점이 될 수 있다.
(http://www.computerworld.com/printthis/2002/0,4814,68961,00.html)

(12) 인증과 접근제어의 사용

웹 서버에서 제공하는 인증 기능과 접근제어 기능을 필요한 곳에 적절하게 활용한다. 웹 서버에서는 사용자 아이디/패스워드 기반의 인증 기능과 특정 IP나 도메인에 대한 접근제어 기능을 제공한다.

(13) 패스워드 설정 정책 수립

웹 서버의 인증 기능을 이용하는 경우에, 유추가 불가능한 패스워드를 사용하도록 한다. 패스워드 길이와 사용 문자에 대한 최소 복잡도를 설정하도록 하고, 사용자의 개인정보나 회사 공개정보를 이용한 비밀번호 사용을 금지하도록 한다. 또한 사용자들에게 웹사이트의 패스워드와 다른 중요한 것들의 패스워드(예를 들어, 은행이나 주식 관련 비밀번호)를 다르게 사용하도록 권장한다. 웹 서버 보안이 100% 완벽할 수 없기 때문에, 이렇게 함으로써 웹 서버 침해로 인한 더 큰 피해를 막을 수 있다.

(14) 동적 컨텐츠 실행에 대한 보안 대책 수립

동적 컨텐츠 처리 엔진들은 웹 서버의 일부로서 실행되면서 웹 서버와 동일한 권한으로 실행된다. 따라서 각 엔진 사용시 발생할 수 있는 모든 보안 취약점들을 파악하고 이와 관련된 보안 기능들을 설정해야 한다.

동적 컨텐츠와 관련된 기능 중 사용하지 않는 기능들은 제거를 하고 예제 파일들은 반드시 삭제한다. 가능하다면 동적 컨텐츠가 실행될 수 있는 디렉토리를 특정 디렉토리로 제한시키도록 하고, 컨텐츠의 추가 권한은 관리자로 제한하도록 한다.

(15) 설치 후 패치 수행

웹 서버 기본 설치 후 알려진 취약점을 바로잡기 위해 취약점 정보사이트나 벤더사이트를 방문해서 웹 서버와 관련된 취약점 정보를 수집하고, 패치나 업그레이드를 수행한다.

(16) 설정 파일 백업

웹 서버를 인터넷에 연결하기 전에 초기 설정 파일을 백업 받아서 보관해 둔다. 또한 변경이 있을 때마다 설정 파일을 백업하여 해킹이나 실수가 발생해도 빠르게 복구할 수 있도록 한다.

(17) SSL/TLS 사용

보안과 기밀성이 요구되는 경우 SSL이나 TLS를 사용하도록 한다[4]. 대부분의 경우에 SSL/TLS는 웹 서버에서 사용할 수 있는 가장 훌륭한 인증 및 암호 방법이다.

[4] modssl 사이트(www.modssl.or.kr) 및 MS사의 웹 서버에서 SSL 설정 문서 (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/ko/library/iis/56bdf977-14f8-4867-9c51-34c346d48b04.mspx?mfr=true) 참조

4. 웹 서버 운영 시 보안 준수 사항

(1) 파일 무결성 점검 도구의 사용

웹 서버 설정 파일, 패스워드 파일, 스크립트 파일 등을 보호하기 위해 파일 무결성 점검을 수행하도록 한다. 업그레이드나 내용 변경시 파일 무결성 체크섬(checksum)을 업데이트 한다. 체크섬을 한번만 쓰기가 가능한 보호된 미디어에 저장하고, 정기적으로 체크섬을 비교하도록 한다.

(2) 새로운 보안 취약점에 대한 지속적인 모니터링

웹 보안 취약점 정보사이트를 주기적으로 방문하여 취약점 정보를 얻고, 새로운 취약점이 발표되면 패치 등 권고된 보안대책을 적용하도록 한다.

(3) 주기적인 로그 점검 및 백업

웹 서버 로그와 OS 로그를 주기적으로 점검하여 침입 혹은 침입시도, 보안 문제점 등을 파악하도록 한다.(권고사항 : 매일)

로그 점검시 다음과 같은 사항을 주의 깊게 검토하도록 한다.

- 불법적인 로그인 시도
- 접근이 제한된 파일에 대한 접근 시도
- 존재하지 않는 파일에 대한 접근 시도
- 허용되지 않은 PUT 메소드를 이용한 파일 업로드 시도
- 부적절한 입력값이 포함된 접근 시도
- 단시간 동안 특정 IP로부터의 다량 접근 시도
- 웹 서버의 뜻하지 않은 멈춤 혹은 시작

디스크 풀(full)을 막고 로그관리를 편하게 하기 위해 웹 서버 로그를 주기적으로 백업하도록 한다.

(4) 안전한 동적 컨텐츠의 사용

모든 동적 컨텐츠들은 충분히 테스트되고 안전하다고 판단된 후에 운영중인 웹 서버에 설치해서 사용하여야 한다.

(5) 웹 컨텐츠 승인 절차 수립

웹 컨텐츠 공개에 대한 승인 절차를 마련하여, 웹 서버 관리자나 개발자가 임의로 웹 컨텐츠를 추가 및 변경하지 못하도록 하고 새로운 웹 컨텐츠를 공개하기 전에 불필요한 정보나 기밀성이 요구되는 정보가 없는지 검토하도록 한다.

(6) 웹 컨텐츠 접근 매트릭스 관리

웹 컨텐츠 접근 매트릭스를 만들어, 웹컨텐츠 디렉토리안에 어떤 폴더와 어떤 파일들이 존재하고, 각각이 누구에 의해 접근이 가능하고 접근이 제한되어야 하는지 정의하도록 한다.

(7) 관리자 PC에 대한 보안

관리자 PC에 대한 해킹은 곧 웹 서버에 대한 해킹과 동일한 결과를 가져올 수 있기 때문에 웹 서버 보안에 못지 않게 관리자 PC에 대한 보안에도 신경을 쓰도록 한다.

5. 웹 어플리케이션 개발 시 보안 준수 사항

웹 어플리케이션 보안을 위해 가장 중요한 것은 어플리케이션 설계 당시부터 보안을 고려하는 것이다. 훌륭한 개발자에 의해 성능 좋은 어플리케이션이 개발되어도 기본적인 보안 의식이 없이 프로그래밍 되어 있다면 웹 어플리케이션이 안전하게 동작함을 보장할 수 없다. 웹 어플리케이션의 취약성과 이에 대한 공격 기법은 매우 다양하고 고도화 되고 있으나 현재 웹 어플리케이션 취약점 점검도구는 시스템이나 네트워크 자체에 대한 취약점을 점검하는 도구들에 비해 공격 기법을 따라가지 못하고 있다. 따라서 가장 효율적인 방어는 웹 어플리케이션 설계 당시부터 보안을 고려하는 것이다.

(1) 유효한 사용자 입력값

웹 어플리케이션을 쉽게 공격하는 방법 중 한가지는 사용자 입력값의 조작이라고 할 수 있다. 일단 모든 사용자 입력을 의심해야 하고, 값의 유효성을 판단하기 위해 다중의 보안장치를 설계해야 한다.

URL 창, 로그인 창, 웹 게시판 등 사용자 입력값을 처리하는 모듈에서는 값을 입력하는 순간부터 철저한 유효성 검사(Validation Check)를 수행하도록 설정한다. 그리고, 입력될 수 없는 값을 체크하기 보다는 입력할 수 있는 값을 체크하여 필터링 하도록 설계한다.

그리고 클라이언트측에서 수행하는 유효성 검사를 신뢰해서는 안된다. 반드시 서버측에서도 입력값에 대한 유효성을 점검해야 한다.

(2) 안전한 오류 환경 설계

어플리케이션이 오류로 인해 동작할 수 없을 경우, 기본적으로 어플리케이션의 상태를 서비스 거부(denial of service) 상태로 설계해야 한다. 예를 들어, 방화벽이 동작할 수 없을 경우 입출력 인터페이스의 모든 패킷이 폐기 되는것과 비슷하다. 따라서 오류 상태의 어플리케이션에서는 사용자 로그인이 제한되거나, 서비스 이용이 불가능하도록 설계한다.

(3) 간단하고 강력한 통제 인터페이스 설계

사용자 편의성을 고려하지 않는다면, 보안 통제는 일상화 되기 어렵다. 따라서 어플리케이션의 사용자와 관리자를 위한 통제 인터페이스는 가능한 사용하기 쉽게 설계되어야 한다.

(4) 다중 보안 장치 적용

웹 어플리케이션의 안전성을 제고하기 위해서는 다중의 보안 장치가 고려되어야 한다. 현재의 웹 어플리케이션에 대한 공격 기법은 매우 다양하고 고도화 되어 있다. 따라서 일회적인 보안 장치로는 어플리케이션의 보안을 안전성을 보장하기 어렵다.

예를 들어, 일단 로그인이 성공한 사용자라 할지라도, 개인정보를 변경하거나 보안이 요구되는 서비스를 이용할 경우 패스워드를 재확인 하는 등 추가적인 인증과정을 거치도록 설계한다.

(5) 최소한의 권한

어플리케이션은 최소한의 권한으로 작동할 수 있도록 설계한다. 최소한의 권한으로 운영되는 어플리케이션은 공격 받을 경우 어플리케이션의 손상을 제한할 수 있기 때문이다.

또한, 사용자의 경우 허가된 서비스만 사용 가능하도록 접근을 제한하도록 한다.

(6) 권한 분리

프로세스나 자원에 대한 접근은 두가지 이상의 조건에 의존해 판단해야 한다. 그래야 한가지 통제장치가 무력화 되어도 시스템에 대한 불법적인 접근을 차단 할 수 있기 때문이다.

웹 사이트 또한 제한영역과 공개영역으로 구분하여 설계한다.

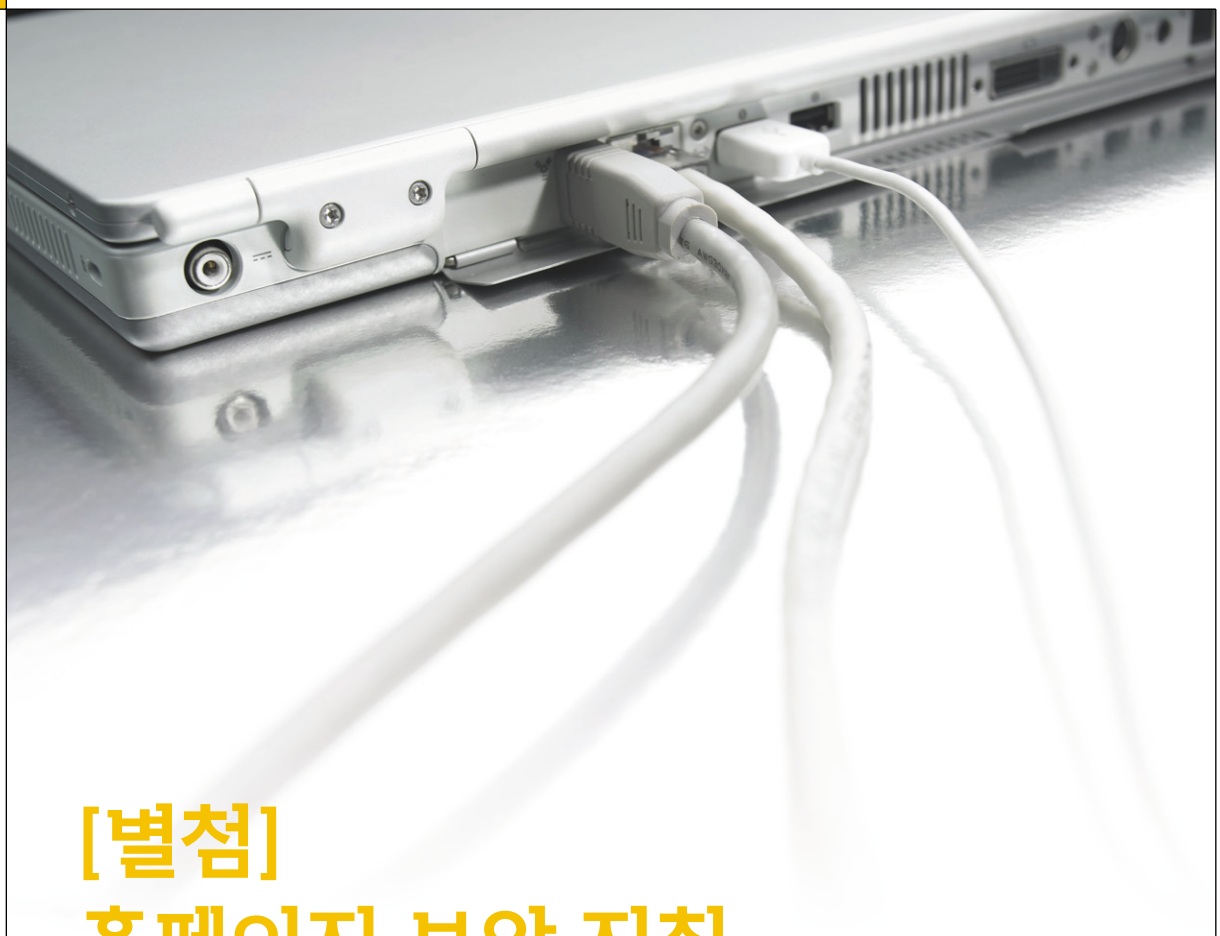
(7) 검증된 암호 모듈 사용

검증된 암호 알고리즘이라 할지라도 자체적으로 구현할 경우, 예상할 수 있는 취약성 검토가 어렵고 발견된 취약성에 대해서도 개발 지식이 있는 사람만이 패치 개발이 가능하기 때문에 가급적 공개적으로 보안성이 검증된 암호 모듈을 사용하도록 한다.

(8) 최소한의 공통 메커니즘

어플리케이션의 공유 메커니즘, 예를 들어 /tmp 나 /temp, /var/tmp 등의 사용을 최소화 한다. 공유 메커니즘은 의도하지 않은 상호작용을 포함하기 때문에 위험 할 수 있다.

세션의 경우, 공유 메커니즘을 통해 타인의 세션 ID 획득이 가능하기 때문에 설계시 이를 피할 수 있는 방법이 고려되어야 한다.



[별첨]
홈페이지 보안 지침

보안 담당자	보안 관리자	보안 책임자

홈페이지 보안 지침

문서번호 :

개정번호 : 1.00

개정 이력

개정번호	개 정 내 용 요 약	개정일자	담당자
1.00	신규 제정	2007.00.00	

목 차

목 차

1. 총칙

가. 목적

본 지침은 과학기술 분야 정부출연 연구기관의 (이하 "연구기관"이라 함) 정보통신 시스템(홈페이지)에 대한 개발 및 운영 시 각 영역의 보안사항을 규정함으로써 연구기관의 홈페이지 보안관리를 보다 안정적이고 효율적으로 하는데 그 목적이 있다.

나. 적용 범위

본 지침은 연구기관 내의 보안관련 조직 및 정보시스템 운영조직과 홈페이지 시스템에 대하여 적용된다.

다. 용어 정의

1) 정보보호

정보의 비밀성, 무결성, 가용성을 보장하기 위한 관리적, 기술적, 물리적 수단 또는 그러한 수단으로 이루어지는 행위를 말한다.

2) 보안정책

조직의 정보보호를 위하여 정보보호 정의 및 목표, 정보보호 중요성을 명시한 최상위 정보보호 방침을 나타내는 문서를 말한다.

3) 보안지침서

정보보호 방침을 뒷받침하는 세부적인 정보보호 규칙을 정하는 문서를 말한다.

4) 보안절차서

정보보호를 위하여 따라야하는 활동을 순차적으로 표시한 문서를 말한다.

5) 정보시스템

컴퓨터의 본체, 주변장치 및 단말장치 등의 전부 또는 일부로서 구성되는 하드웨어 및 소프트웨어를 총칭한다.

6) 전자적침해행위

해킹, 컴퓨터바이러스, 논리적 메일폭탄, 서비스거부 또는 고출력 전자기파 등을 사용하여 컴퓨터 시스템이나 인터넷 망을 공격하는 행위를 말한다.

7) 침해사고 대응

침해사고를 분석하고 해결책을 제시하여 보안 위협에 대응 할 수 있도록 하는 업무를 말한다.

8) 침해사고

비 인가된 접근, 전산 시스템의 오남용(비 인가된 사용)을 의미한다. 또한 해킹사고뿐만 아니라 바이러스 사고도 포함한다.

9) 침해사고대응팀

해킹 또는 바이러스 사고 발생에 따른 사고의 분석, 처리, 사후 복구, 사후 예방 조치 등을 주요 업무로 하는 보안팀을 말한다.

10) DB(Database)

DBMS 내의 테이블, 뷰, 스토어드 프로시져, 데이터 등의 집합체를 나타내는 구조를 말한다.

11) DBMS(Database Management System)

DB를 관리하는 소프트웨어 시스템으로, 다수의 컴퓨터 사용자들이 DB 안에 데이터를 기록하거나 접근할수 있도록 해주는 프로그램이다.

2. 정보보호 조직 지침

본 지침은 연구기관의 홈페이지 개발 및 보안 업무 수행을 위한 보안 조직을 구성하여 운영하도록 하며 보안조직의 구성은 보안심의위원회, 보안 담당부서를 구성하여 연구기관 내 보안활동을 수행하도록 한다.

가. 보안조직 구성

연구기관은 기관의 정보보호 업무 수행을 위한 보안조직인 보안 심의위원회, 보안팀 및 각 팀별 보안담당자를 지정하고 보안활동을 수행한다.

1) 보안 심의위원회

보안 심의위원회는 CEO, 임원, 각 팀장, 보안 책임자 등의 구성원으로 하며, 정보보호 관련 최고 의사 결정 기구 역할을 한다.

2) 보안 팀

기관의 보안 담당부서는 기관 전체에 대한 정보보호 활동 및 보안감사 기능을 수행하며, 보안 책임자, 보안 관리자, 보안 담당자를 구성한다.

3) 팀별 보안 담당자

팀별 보안 담당자는 보안활동에 있어서 부서 간 이견 발생 시 협의체 역할 및 보안 담당부서와의 대응 창구로써 팀 내 정보보호 활동을 주관한다.

나. 보안 조직의 역할

연구기관은 기관의 정보보호 업무 수행을 위한 구성 조직 별 역할은 다음과 같다.

1) 보안 심의위원회

보안 심의위원회의 주요 수행 업무는 다음과 같다.

- ◆ 정보보호 활동 계획 및 예산 심의
- ◆ 정보보호 방침/지침/절차 등 규정의 검토 및 승인

◆ 주요 정보보호 이슈에 대한 대책 결정
◆ 중대 정보보호 사고에 대한 검토 및 협의

2) 보안 팀

보안 팀은 연구기관 전체에 대한 보안활동을 위한 다음의 업무를 수행한다.

◆ 기관의 보안활동 수행 및 감사 수행
◆ 임직원을 대상으로 년간 정보보호 교육 및 홍보 계획을 수립 및 팀별 정보보호 담당자와 협력을 통한 교육을 시행 후 교육내용 및 참석자에 대한 기록을 관리

3) 보안 책임자

보안 책임자는 기관 정보보호 활동을 총괄하고 정보보호담당부서를 관리하며 주요 수행 업무는 다음과 같다.

◆ 보안 총괄 및 책임
◆ 보안심의위원회 회의 소집, 안건상정
◆ 보안 정책 및 지침, 계획, 절차 등의 승인
◆ 침해사고 등 비상상황 시 수행 총괄
◆ 보안 담당부서 관리

4) 보안 관리자

보안 관리자는 보안 책임자의 정보보호 업무를 보좌하고, 위임받아 정보보호 활동 실무 총괄하고, 보안 담당자를 관리하며 주요 수행 업무는 다음과 같다.

◆ 정보보호 실무 총괄 및 보안 담당자 관리
◆ 회사 사업방향에 기초한 정보보호 계획 수립 및 수행
◆ 정보보호 관련 소요 예산 편성/집행
◆ 유관기관의 정보보호 관련 법, 규정 검토 준수 총괄
◆ 침해사고 등 비상상황 시 제반사항 이행 및 관리
◆ 정보보호 인식제고를 위한 교육 계획의 수립 및 실시총괄
◆ 보안감사 및 취약성 점검 계획 수립 및 주관

5) 보안 담당자

보안 담당자는 보안 관리자의 지시 하에 연간 정보보호 활동 및 감사 계획을 수립하고, 보안 책임자의 승인을 득하며 주요 수행 업무는 다음과 같다.

- 정보보호 지침, 절차의 제정 · 개정 · 폐기 주관
- 정보보호 사고 예방 및 대응 지원
- 시스템 도입 또는 개발시 보안성 확인 시행
- 임직원에 대한 정보보호 교육 및 인식제고 프로그램 주관
- 정기, 비정기적 정보보호 감사 수행
- 주기적인 기술적 보안 취약성 점검
- 자산에 대한 위험평가 수행

6) 팀별 보안 담당자

팀별 보안 담당자는 부서 내 보안 관련사항 전달 및 홍보를 수행하며 보안사고 발생시 보안 담당부서와 협력하여 이를 처리하며 주요 수행업무는 다음과 같다.

- 보안 팀과 협업 체계를 통해 부서 내 정보보호 활동 및 홍보 수행
- 부서 내 자산 관리
- 부서 내 보안사고 발생시 보안 담당부서와 협력하여 이를 처리
- 기관의 보안에 대한 팀 내 의견 수렴 및 전달
- 새로운 시스템 또는 서비스에 대한 보안기능 구현 시 부서 내 적정성 평가 및 지원

3. 침해사고 대응 지침

본 지침은 각 기관에서 발생 가능한 침해사고에 신속하게 대응하기 위한 준비와 대응절차를 기술하여 침해사고로부터의 피해를 최소화하고 후속 보안 대책 수립을 목적으로 하며 보안 관리자는 본 지침을 참조하여 침해사고 발생 및 침해사고 탐지 시 이에 신속하게 대응할 수 있는 준비를 갖추어야 한다.

가. 침해사고 대응팀 구성

(1) 인력 구성

침해사고 대응팀은 침해사고 대응팀장, 연락담당자, 사고접수 담당으로 구성하여 관련 업무를 수행하도록 한다.

1) 침해사고대응팀장

침해사고 대응팀의 실무 책임자로 침해사고대응 업무를 총괄하여 빠른 사고대응 업무가 가능하도록 한다. 회사 내에서는 타 부서 및 경영진과의 업무 조율 역할과 대외적으로는 국내 침해사고대응팀과의 협력관계를 구축한다.

2) 연락담당자(Representative)

회사의 대내외 업무 조율을 위한 실무 대표자 역할을 한다. 주로 사고대응을 위한 대내외 협력 업무에 대한 연락처로써의 역할을 수행한다.

3) 사고접수 담당

해킹 및 바이러스 등의 침해사고 접수, 사고 할당, 사고 접수자료에 대한 관리를 담당한다. 보안사고의 초기 접수에서 사고여부의 초기 판단 업무를 수행하고 이를 각 관련 담당자에게 이관한다.

4) 침해사고 처리 담당

해킹사고 발생 시, 해당 사고를 정확히 분석하고 대응할 수 있는 사고 분석 전문가 역할을 수행한다. 이러한 업무를 담당하는 사람은 기관 내의 시스템 및 네트워크 관

리 그리고 서비스 운영에 대한 지식을 갖고 있어야 한다. 하지만 필요에 따라 IT 부서에 근무하는 각 분야의 전문가의 도움을 얻을 수 있도록 하는 것이 중요하다. 다음과 같은 업무를 수행한다.

- ◆ 사고노트 작성 배포
- ◆ 특정 중요 사안에 대한 기술문서 작성 배포
- ◆ 해킹사고 탐지 및 방지를 위한 프로그램 개발 참여

5) 취약성 분석/테스트 담당

새로운 취약성에 대한 분석, 사이트에 대한 위협 여부 평가, 취약성 테스트 등의 업무를 담당한다. 항상 새로운 취약성의 발표 자료를 검토하고 각 사이트에 적용 여부를 판단하여야 한다. 다음과 같은 업무를 수행한다.

- ◆ 보안권고문 작성 배포
- ◆ 기술 문서 작성 및 배포
- ◆ 보안 가이드 라인 작성 및 배포 등

나. 침해사고의 범위

침해사고란 정보통신시스템에 대한 비 인가된 행위 또는 위협을 의미한다. 비 인가된 시스템 사용 또는 사용자의 계정 도용, 악성코드 유입 및 실행, 정보 서비스의 방해 등이 해당된다. 또한 회사의 보안정책에 위반되는 행위 역시 침해사고로 정의한다. 침해사고 대응팀은 본 침해사고의 범위에 정의된 사고를 중심으로 대응조치를 취하도록 한다.

(1) 악성 프로그램 유포

악의적인 사용자 또는 해커가 의도적으로 다른 정보통신 이용자에게 피해를 주고자 하는 악의적 목적으로 만든 프로그램 및 실행 가능한 코드를 의미한다. "악성코드"라 표현하기도 하며, E-mail, 메신저, 문서의 매크로 기능 등을 이용하여 악성프로그램을 유포시키고 공격에 사용한다. 주요 형태로는 컴퓨터 바이러스, 인터넷 웜, 트로이목마 등이 공격에 이용된다.

(2) 서비스거부 공격(D●S, Denial ●f Service)

시스템 또는 네트워크 서비스의 정상적인 운영을 방해하는 공격으로, 시스템을 다운시키거나, 네트워크에 과부하의 트래픽을 유발시켜 사용자들이 서비스를 이용하지 못하게 하는 공격이다.

(3) 시스템 침입(비 인가된 접근)

시스템 또는 네트워크의 취약성을 이용하여 시스템에 침입하는 공격이다. 보통 특정 취약점을 공격하는 해킹프로그램을 이용하거나, 잘못된 서버운영상의 문제(예, 디폴트 패스워드를 사용하는 경우 등)를 이용하여 시스템에 침입한다.

(4) 오남용(비 인가된 사용)

시스템 및 네트워크 자원을 허가받지 않은 방법으로 사용하거나 악용하는 공격이다. 스팸메일을 보낼 때 다른 사이트의 시스템을 이용하는 방법이나 다른 사람의 계정을 도용하는 행위 등이 대표적인 예이다.

(5) 정보수집

특정 사이트의 시스템 및 네트워크에 대한 정보를 수집하기 위한 공격으로 포트스캔, 전화번호 스캔 등이 있다. 공격자는 정보 수집을 통해 특정 사이트에 어떠한 시스템이 존재하는지, 어떠한 서비스가 제공되는지, 어떠한 네트워크 구조를 갖고 있는지, 그리고 어떠한 취약성이 있는지를 조사하게 된다.

(6) 보안 정책 위반

보안 운영의 가이드라인에 위배되는 행위 또는 고의적인 위반행위 또한 침해사고로 정의하고 각 경우에 대해서 조사한다.

다. 침해사고 대응절차

(1) 침해사고 점검

보안 담당자는 로그 점검 혹은 정보보호 시스템의 실시간 모니터링을 수행할 때 다음 사항에 주의하여 침입흔적을 확인하며 침입의 흔적을 발견 시 그 원인이 정보시스템 운영 및 개발 담당 부서의 관리 담당자나 프로그래머의 실수 때문인지 확인한다.

① 같은 사용자 이름으로 두명 이상 동시 로그인이 되고 있는지 확인한다.
② 정규 시간외의 시스템 사용자를 확인한다.
③ 관리자 권한 외의 작업수행 시도가 있었는지 점검한다.
④ 보안 관련 파일의 수정 및 수정 시도가 불법적으로 이루어졌는지 점검한다.
⑤ 허가가 안된 파일, 서비스 및 기타 자원의 접근 시도를 확인한다.
⑥ 일반 사용자의 홈 디렉토리에 시스템 파일이 존재하는지 확인한다.
⑦ 계정 관련 시스템 파일에 관리자 이외의 접근 시도가 있었는지 점검한다.
⑧ 네트워크 전송량을 증가시키는 비정상적인 프로그램 실행 작업이 있는지 점검한다.
⑨ 한 사용자가 많은 외부 접속을 시도하고 있는지 점검한다.
⑩ 허가된 모뎀 사용자가 아닌데 모뎀으로 로그인을 하려는 시도 및 접속을 점검한다.
⑪ 시스템의 비정상적인 동작이 있다면 외부의 불법적인 침입이 있는지의 여부를 점검한다.

(2) 침해사고 탐지

① 보안담당자는 침입자가 시스템 내에서 활동하고 있는 것으로 판단될 때 보안 관리자에게 즉시 보고를 한다.
② 보안관리자는 필요시 관련 국가기관(KISA, CERT)의 협조를 받기 위한 절차를 준비한다. 이때, 협조 의뢰의 최종 결정은 정보보호 책임자가 한다.
③ 침입자의 시스템 내 활동을 발견시 세부 처리 절차는 다음과 같다.
④ 내부 단말기에서 침투한 경우 현재의 단말 위치를 확인한다.
⑤ 현재 침입자가 시스템 내에 있다면, 가능한 도구나 명령어를 이용하여 침입자에 관련된 정보를 수집한다.

⑥ 침입자가 수행하고 있는 명령어를 파일로 저장하거나 기록한다.
⑦ 중요한 데이터에 접근을 할 경우 또는 침입자를 추적할 자신이 없을 경우 침입자의 연결을 끊는다.
⑧ 보안담당자는 침입자의 시스템 내 활동에 대한 절차 적용 후 보안사고 및 대응결과를 보안 관리자에게 보고를 한다.

(3) 침해흔적 발견 시 조치절차

1) 로그 파일의 분석 등을 통해 침입한 흔적이 발견된 경우 보안진단 도구나 체크리스트를 이용하여 다음과 같은 사항을 점검한다.
① 새로운 계정이 생성되어 있는지 확인한다.
② 패스워드 파일이 변경되었는지 확인한다.
③ 주요 설정 및 실행 파일 등이 변경되었는지 확인한다.
④ 특정 파일의 접근 모드가 변경되었는지 확인한다.
⑤시스템 유틸리티가 변경 및 수정되었는지 확인한다.

2) 데이터의 변조나 불법 접근의 흔적이 있을 경우 해당 서비스를 중지시킨다.

3) 침입자를 식별하기 위한 증거 수집을 한다.

4) 백업 등을 이용하여 복구한다.

5) 보안담당자는 침입흔적 발견 후 피해상황을 파악하여 보안사고 및 대응결과서를 작성한 뒤 보안관리자에게 보고한다.

라. 보안 담당자의 역할

1) 침해사고 발생시 보안관리자의 세부 처리 절차는 다음과 같다.
① 침해사고의 피해 상황을 파악한다.
② 침입자를 식별하기 위한 증거를 수집한다.
③ 시스템의 복구를 지원한다.

④ 문제점을 파악하여 대책을 제시한다.
⑤ 필요 시 정보보호센터 및 보안관련 수사기관에 침해사고에 대한 수사를 의뢰한다.

2) 보안사고 및 대응결과서와 보안사고 발견 및 조치 결과서를 작성하여 보안 관리자의 승인을 득한다.

3) 보안사고 기록은 비밀로 분류하고 3년 이상 보관한다.

4) 교육 및 홍보를 강화하고 동일 문제가 재발하지 않도록 한다.

4. 웹 서버 보안지침

본 지침은 각 기관에서 웹 서버 구축 및 보안 설정 시 구축 및 운영에 필요한 사항을 규정함으서 웹 서버 시스템의 보안성을 강화하고 비인가자의 침입의 악의적인 접근을 차단하는 목적으로 작성 되었으며 보안 관리자 및 시스템 관리자는 본 지침을 웹 서버 구축 및 운영 하는데 있어 이를 참조한다.

가. 웹 서버 구축

(1) 소프트웨어 업그레이드 및 패치 설치

항상 최신 버전의 소프트웨어를 사용하고 보안과 관련된 패치를 설치하여야 한다. 이는 인터넷 공격에 대응하기 위한 가장 간편하고 효과적인 방법이다. 특히 주기적으로 웹 서버에서 사용되는 어플리케이션에 대한 새로운 업데이트 및 보안패치를 확인하도록 한다.

(2) 단독 목적의 웹 서버 사용

웹 서버 관리자는 반드시 웹 서비스만을 위한 단독 서버를 구축하여 운영하여야 한다. 하나의 시스템에 웹 서버, 메일서버, DNS 서버, 데이터베이스 서버를 운영하는 경우가 있는데 이는 웹 서버를 포함하여 데이터베이스 서버까지도 위험하게 한다. 일반적으로 하나의 서비스가 추가될 때마다 그만큼 더 위협이 증가하게 된다.

특히, 중요한 정보를 다루는 데이터베이스 서버의 경우 가능한 웹 서버와 분리하여 서로 다른 시스템에서 운영하도록 한다.

(3) 불필요한 어플리케이션 제거

웹 서버에서 사용되지 않는 모든 불필요한 소프트웨어는 반드시 제거한다. 디폴트로 시스템을 설치하게 되면 많은 경우 다양한 종류의 소프트웨어들이 설치되고 실행되게 된다. 그리고 이러한 소프트웨어의 취약점으로 인하여 해킹을 당하게 된다.

(4) 침입차단시스템(Firewall) 사용

라우터와 침입차단시스템을 이용하여 DMZ 구간 네트워크를 구성한다. 그리고 웹 서버를 비롯한 일반 인터넷 서비스를 제공하는 시스템을 이곳에 설치하도록 한다. 이 경우 웹 서버를 포함하여 DMZ 구간의 시스템에서 중요 내부 서버나 네트워크로 접속하지 못하도록 접근제어를 하도록 한다.

이는 만약의 경우, 웹 서버가 해킹을 당할 경우에 공격자가 웹 서버를 통하여 또 다른 서버나 내부 시스템으로 침입을 하지 못하도록 하는데 목적이 있다.

(5) 원격 접근 제한

웹 서버 관리의 편리성을 위해 관리자는 콘솔을 이용하기보다는 원격지에서 웹 서버로 접속하는 경우가 많다. 이 경우, 네트워크 도청 등의 공격을 통하여 공격자는 관리자의 ID나 패스워드를 획득하고 시스템에 접근할 수 있다. 따라서 가능한 원격 접근을 최소화하거나 하지 않도록 한다.

(6) 웹 트랜잭션 보안

웹 서버를 통하여 금융정보, 개인정보, 회원정보, 그리고 ID, 패스워드와 같은 정보를 일반 사용자(클라이언트)와 통신할 경우에는 그 정보가 노출되는 위협이 발생한다. 따라서 웹 서버에서 중요한 정보를 다룰 경우에는 반드시 SSL/TLS 암호화를 지원하도록 한다.

나. 웹 서버 운영

(1) 파일 무결성 점검

웹 서버 설정파일, 패스워드 파일, 스크립트 파일, 그리고 OS의 중요 설정 · 시스템 파일에 대해서 주기적으로 무결성 점검을 수행하도록 한다. 가능한 경우, 무결성 점검의 체크섬 값은 한번만 쓰기 가능한 미디어에 저장하도록 하여 변조를 방지하도록 한다.

(2) 새로운 보안 취약점에 대한 모니터링 및 적용

웹 서버와 관련된 신규 취약점 정보, 웹 어플리케이션과 관련된 신규 취약점 정보를 지속적으로 모니터링 한다. 새로운 취약점이 발표되면 이에 대한 패치를 웹 서버에 적용하도록 한다.

(3) 주기적인 로그 점검

웹 서버 로그와 OS 로그를 주기적(매일)으로 점검하여 침입, 침입시도, 또는 보안 문제점을 발견하도록 한다.

(4) 웹 서버 설정파일 백업

웹 서버 장애로 인하여 시스템의 복구가 필요한 경우를 위해서 설정파일에 대한 백업을 주기적으로 실시하도록 한다.

5. 시스템 보안 지침

본 지침은 UNIX, Windows 계열 서버 시스템을 다양한 보안 위협 및 취약성으로부터 안전하게 보호하고, 운용 관리를 위하여 기관 소유의 모든 UNIX, Windows 계열의 서버 시스템을 그 적용 범위로 하고, 적용 범위 내의 모든 장비와 그 부대시설물을 포함하는 모든 자원 및 동 자원을 이용하여 업무를 수행하는 모든 사용자를 대상으로 한다

가. 시스템 도입/운영/폐기 보안관리

(1) 서버 시스템 도입 시 보안성 검증

① 서버 시스템 신규 도입 및 설치 시 보안성 검증을 통하여 안정성을 확인한 후 서비스가 운영 될 수 있도록 보안성에 대한 검토가 이루어지도록 한다.
② 보안전담 조직에서는 서버 시스템 보안성 검증 후 인증에 통과한 시스템만을 서비스 운영 허가를 주도록 하며, 보안성 검증을 통과하지 못한 경우에는 보안성 강화를 통하여 재검증을 받도록 체계화 한다.

(2) 서버 시스템 운영관리

① 서버에 설치된 소프트웨어의 현황을 목록으로 만들고 변경현황을 관리한다.
② 서버에 설치된 상용 소프트웨어의 임의적 변경은 기능상의 오류를 발생시킬 위험이 있으므로 필요한 경우 해당 부서장 및 제품공급자와 협의 하에 변경한다.
③ 서버 담당자는 서버 변경 시 발생할 수 있는 위험에 대응하기 위해 서버 변경에 대한 문서화 작업이 이루어지도록 한다.
④ 서버 담당자는 서버의 하드웨어 및 소프트웨어의 지속적인 가용성과 무결성 확보를 위해 정기적 혹은 필요한 경우 수시로 예방점검을 한다.

(3) 서버 시스템 폐기관리

① 서버의 매각이나 폐기를 위한 반출 전에 해당 서버 담당자는 해당 서버의 저장장치를 분리하여 별도 파기하거나 로우레벨로 초기화한다.

② 보안전담조직은 사용자 정보, 중요 거래 정보, 중요 컨텐츠 등 민감한 내용이 보관된 서버의 경우 처리결과에 대해 사후검토를 실시할 수 있다.

나. Unix시스템 보안관리

(1) 계정관리

1) 계정 보호

① 패스워드 미설정이나 패스워드와 계정이 동일한 계정을 허용해서는 안 된다.
② 시스템운용자와 보안담당자를 제외하고 UID가 '0' 인 계정이 존재해서는 안 된다.
③ 모든 계정의 path에 "."이 존재할 경우, path의 마지막에 존재하여야 한다.
④ 특별한 경우(응용프로그램용 ID, 시스템 유틸리티용 ID 등) 이외에 하나의 ID는 한번만 로그인 할 수 있다.
⑤ home 디렉토리는 소유자 이외의 사용자에게 write 권한을 부여해서는 안 된다.
⑥ 사용자의 .profile, .cshrc, .login 등은 소유자 이외의 다른 사용자에게 write 권한을 부여해서는 안 된다.

2) 계정 생성

① /etc/passwd 파일의 5번째 필드인 comment 필드에는 비상시 연락하기 위하여 사용자 확인 및 연락이 가능한 정보를 넣는다.
② ".profile" 파일은 적절한 path값과 제한된 umask(022)를 설정해야 한다.
③ 패스워드는 1개월 주기로 변경하여 사용해야 하며 변경사항을 관리하여야 한다.
④ 사용자 ID 부여기준

- 사용자 계정은 고유한 ID를 사용해야 하며, 수행하는 작업의 특성에 따라 불가피한 경우에만 그룹 ID를 사용할 수 있다.
- 사용자의 권한은 업무 목적과 보안정책에 최소한의 권한만을 부여해야 한다.
- 사용자의 권한 남용을 방지하기 위해 직무 원칙에 따라 권한을 분리 부여한다.

3) 계정 사용 중지

① 특정 계정 사용을 정지시킬 경우는 해당 사용자가 현재 로그인 중인지 확인해야 하고, 사용 중일 때는 반드시 로그아웃 하도록 한 후 정지시켜야 한다.

② 계정 사용을 정지시키기 전에, 해당 계정과 동일 그룹 내에 있는 다른 사용자에게 통보하여 필요한 파일들을 복사하도록 해야 한다.

(2) 패스워드 관리

1) 패스워드 관리 정책

① 신규 사용자에게 시스템 사용 권한을 부여할 때에는 반드시 패스워드를 부여 받도록 해야 한다.
② 패스워드는 최소 3개월 주기로 변경하여야 한다.
③ 사용자는 자신의 패스워드를 기억 하고, 패스워드 보안을 철저히 해야 한다.
④ 모든 사용자는 패스워드 인증을 통해서만 시스템을 사용할 수 있어야 한다.
⑤ 모든 사용자의 패스워드는 영문자/숫자를 조합하여 8자리 이상으로 한다.
⑥ 패스워드 입력 제한은 10회로 하고, 10회 실패 시 연결이 자동 해제(disconnected)되며 30분 동안 벌칙(penalty)을 적용한다.
⑦ 루트 권한을 갖은 사용자가 이/퇴직 등의 사유로 루트 권한을 이양할 때는 인수자는 즉시 기존에 사용했던 패스워드를 변경해야 한다.

(3) 접근 통제

1) 네트워크를 통한 접근통제

① 네트워크 파일 내의 필요하지 않는 호스트명은 삭제해야 한다.
② 사용하지 않고 불필요한 네트워크 서비스는 삭제한다.(RPC, NFS 등)
③ 시스템의 사용자나 네트워크 사용 상태정보 등을 외부로 유출시킬 수 있는 프로그램을 제한한다. (finger, talk, ftp, r서비스 등)
④ 네트워크 파일시스템 NFS(Network File System)을 통제한다.
◆ export할 파일시스템을 제한해야 하고 파일시스템을 마운트할 수 있도록 허용된 호스트명을 명시되어 있어야 한다.

2) 터미널 로그인 접근통제

① 로그온 절차 성공 전에는 시스템 또는 응용프로그램의 식별자 표시를 금지한다.
② 로그온 시 비 인가된 사용자에게 시스템 관련정보를 제공해서는 안된다.

③ 오류 발생에 대해 상세내역을 출력을 하지 않는다.
④ 성공하지 못한 로그온 시도 횟수를 10회 이하로 설정하며 다음과 같이 조치한다.
◆ 연결을 해제한다.
◆ 로그온 실패 이후, 시도에 대해서는 30분 동안 로그온 절차를 진행하지 않는다.
◆ 성공하지 못한 로그인 시도에 대해 로그를 남긴다.

⑤ 로그온 절차에 소요되는 최소 · 최대 허용시간을 설정하며, 초과 시 로그온 절차를 중지한다. (최소 1초, 최대 10초)
⑥ 성공 로그온에 대해서 이전 로그온 날짜 및 시간, 이전 로그온 이후의 성공하지 못한 로그온 정보를 표시한다.

(4) 보안 패치

1) 보안패치는 각종 소프트웨어, 운영체제 등에서 발견되는 보안상의 취약성을 보완해주는 프로그램으로 새로운 취약성에 대한 보안패치가 발표되는 즉시 시스템에 적용하여 보안조치를 취함으로서 보안사고를 사전에 예방할 수 있도록 한다.
① 보안패치 정보를 주기적으로 입수하고 적용
② 주요 보안패치에 대해서는 적용일 등 패치정보를 기록 · 관리
③ 보안패치 정보를 주기적으로 입수하고 적용

2) 조직 내의 패치 적용 대상 시스템, 소프트웨어별로 보안패치 방법 및 절차를 정리하여 패치 적용 정보를 기록 · 관리하도록 하고 다음 사항을 포함하도록 한다.
① 시스템 성능 및 환경의 문제로 패치를 하지 못하는 경우에는 해당 사유와 이를 보완하기 위해 적용한 대체수단이나 방법을 기록한다.
② 각 서버에서 사용되는 소프트웨어 목록 및 버전 정보 목록 관리
③ 각 소프트웨어 또는 시스템 제공업체의 홈페이지를 확인하여 최신버전의 보안패치 목록 및 패치 방법 확인
④ 패치 설치 후 서버의 정상적인 운영상태 확인

(5) 감사와 로깅

1) 사용자가 사용한 명령들에 대해 로깅이 필요한 서버(보안툴 관리서버 등)에 대해서만 로깅하고, 기타 서버들은 Summary 파일만 관리한다.

2) 다음의 사항들은 기본적으로 로깅 하여야 할 내용들이다.
① 가장 최근에 로그인한 사용자 정보
② 사용자별(사용자 ID) 로그인 시간 정보
③ 사용자별 로그인 · 로그아웃 정보(날짜와 시간)
④ 가능한 경우, 접속 터미널 ID와 위치
⑤ 시스템 접근의 성공 및 실패 기록(비권한자 침입시 침입자 이름 · 일시 등)
⑥ 데이터 및 기타 접근의 성공 및 실패 기록

3) 로그는 최소 1개월 이상, 업무의 중요도에 따라 적절한 방법으로 보관한다.

다. Windows 계열 시스템 보안관리

(1) 계정 관리

1) 패스워드 관리
① 패스워드는 영문자와 숫자를 혼합하여 최소 8자 이상으로 하며, 연속 4자 동일 문자의 사용을 금지하고 ID와 동일한 패스워드 사용을 금지한다.
② 패스워드는 3개월 주기로 변경하여 사용해야 한다. 유출된 경우, 즉시 변경한다.
③ 기존 패스워드는 최대 12개월 이내, 업무의 중요도에 따라 6개월 이내 재사용을 금지한다.
④ 최대 10회의 로그온 실패 후에는 계정이 잠기게(Lock-out) 한다.
⑤ 시스템 운용자만이 잠긴 계정을 풀도록(Unlock) 한다.
⑥ 사용 시간이 제한된 사용자의 경우 정해진 사용 시간이 경과되면 강제로 로그오프시켜 사용을 중지시킨다.
⑦ 사용자가 자신의 패스워드를 바꾸기 위해선 반드시 로그온해야 한다.
⑧ 단순 패스워드를 사용하지 않도록 해야 한다.

⑨ Default 관리자 계정을 그대로 사용해서는 안된다.

2) 사용자 관리

① 신규 사용자 및 사용자 그룹을 생성시킬 때 사용 목적, 사용자 정보, 사용 기간 등을 정확히 고려하여 생성하여야 한다.
② 그룹의 등록 정보 및 접근 권한 등은 그룹 내의 모든 member에게 허용되므로 그룹과 사용자 계정 설정시 특별히 주의하여야 한다.
③ 사용자가 소속된 그룹을 확인하여 적합한 그룹에 속해 있는자 확인 후 불필요한 그룹에 속해 있을 경우 삭제한다.
④ 사용자별로 서버에 접속할 수 있는 날짜와 시간을 설정하며 설정된 시간 이외에는 로그온을 금지시킨다.
⑤ 사용자는 사용자의 업무에 필요한 시스템에만 접속할 수 있도록 한다.
⑥ 시스템 운용자는 사용자 계정의 유효기간을 설정해야 한다. 또 임시 계정은 반드시 사용 기간이 경과된 후 사용할 수 없도록 설정한다.
⑦ 사용자 계정의 생성 시 긴 이름과 설명을 기록하여야 한다.

3) 관리자와 관리자 그룹 관리

① 관리자(Administrator Account)와 관리자 그룹(Administrators Group)은 접근 권한의 제한이 없으므로 특별히 주의하여 설정되어야 한다.
② 사용자 그룹 중 특별한 권한을 갖는 그룹은 그룹의 member를 검토하여 불필요한 사용자 계정은 삭제한다.
③ 기존 시스템에 새로운 운영자가 선임되었다면 시스템 운용자는 즉시 운영자 계정명과 패스워드를 변경하여야 한다.
④ 모든 운영자용 계정은 두 개의 계정(관리 작업용, 일반 작업용)을 사용한다.
⑤ 모든 운영자 계정으로의 실패한 로그온 시도는 기록되어야 한다.
⑥ Domain Admins Group과 Administrator Group의 member를 확인하여 불필요한 사용자는 모두 삭제한다.

(2) 접근 통제

1) 네트워크 접근통제

① 네트워크를 통한 시스템 접근 권한은 원격 로그온이 반드시 필요한 Group에만 설정하도록 한다.

② 관리자 그룹만이 local computer에 로그온을 할 수 있도록 하여야 하며 이외의 사용자들은 local computer에 접속을 금지하여야 한다.

③ 보안로그와 감사는 관리자 그룹만이 관리하여야 한다.

④ 공유 폴더의 필요성을 검토하여 불필요한 공유 기능을 제거하여야 한다.

⑤ TCP/IP의 「보안사용」기능을 사용하여 시스템에서 사용 가능한 TCP port, UDP port, IP Protocol을 설정하여야 한다.(필요한 IP Port만 허용)

⑥ 시스템에 설치된 서비스를 조사하여 불필요한 서비스는 제거하여야 한다.

⑦ RPC(Remote Procedure Call) 서비스는 제거해야 한다.

⑧ NetBIOS 접근을 제한하여야 한다.

2) 시스템 로그인

① 로그온 절차 성공 전에는 시스템 또는 응용프로그램의 식별자 표시를 금지한다.

② 로그온 시 다음과 같은 초기 보안 메세지를 삽입한다. “임직원을 위한 시스템으로써 인가된 분만 사용할 수 있습니다. 불법 사용 시에는 법적 제제를 받을 수 있습니다.”

③ 로그온 시 비인가 된 사용자에게는 시스템에 대한 정보를 제공하지 않는다.

④ 오류 발생에 대한 상세내역을 출력하지 않는다.

⑤ 성공하지 못한 로그인 시도에 대해 로그를 남긴다.

⑥ 성공 로그온에 대해서 이전 로그온 날짜 및 시간, 이전 로그온 이후의 성공하지 못한 로그온 정보를 표시한다.

(3) 보안 패치 관리

1) 보안패치

① 보안패치는 각종 소프트웨어, 운영체제 등에서 발견되는 보안상의 취약성을 보완해주는 프로그램으로 새로운 취약성에 대한 보안패치가 발표되는 즉시 시스템에 적용

하여 보안조치를 취함으로서 보안사고를 사전에 예방할 수 있도록 한다.

◆ 보안패치 정보를 주기적으로 입수하고 적용
◆ 주요 보안패치에 대해서는 적용일 등 패치정보를 기록 · 관리
◆ 보안패치 정보를 주기적으로 입수하고 적용

② 조직 내의 패치 적용 대상 시스템, 소프트웨어별로 보안패치 방법 및 절차를 정리하여 패치 적용 정보를 기록 · 관리하도록 하고 다음 사항을 포함하도록 한다.

◆ 시스템 성능 및 환경의 문제로 패치를 하지 못하는 경우에는 해당 사유와 이를 보완하기 위해 적용한 대체수단이나 방법을 기록한다.
◆ 각 서버에서 사용되는 소프트웨어 목록 및 버전 정보 목록 관리
◆ 각 소프트웨어 또는 시스템 제공업체의 홈페이지를 확인하여 최신버전의 보안패치 목록 및 패치 방법 확인
◆ 패치 설치 후 서버의 정상적인 운영상태 확인

③ 기타 보안패치 관리 작업을 자동화 해주는 소프트웨어를 사용할 경우, 위 사항들을 만족하고 있는지 주기적으로 검토한다.

(4) 감사와 로깅

① 아래 사항을 참고로 하여 자원과 이벤트를 감사한다.

◆ 감사정책은 시스템의 사정에 맞게 유연하게 관리할 수 있도록 정의한다.
◆ Users 그룹 대신에 Everyone 그룹을 감사하여 local 사용자 외에 네트워크에 연결하는 모든 사용자들을 감사한다.
◆ 감사로그를 분석하는 스케줄을 정한다.
◆ 경향 분석을 위해 감사로그를 정기적으로 보관한다.

② 로그기록에 접근할 수 있는 권한을 시스템 운용자로 제한하여야 한다.
③ 보안 관련 감사를 위해 로그온 및 로그오프, 파일 및 개체 접근, 보안정책 바꾸기에 대해서는 반드시 로깅을 해야 한다.
④ 기타 항목에 대해서는 자원의 중요도에 따라 선택적으로 로깅한다.
⑤ 중요 시스템 파일이나 데이터에 대해서는 별도 감사항목을 설정하여 확인한다.

⑥ 보안 로그(Security Log)는 보안관제부서에서 점검할 때까지 보관되어야 한다.

⑦ 서버 운용자는 수시로 보안 이벤트 로그를 확인하여야 하며 로그는 다음의 내용을 남겨야 한다.

- 사용자 로그온, 로그오프 기록
- 파일 및 객체 액세스 실패 기록
- 시스템 종료 및 재시작 기록
- 보안 정책 변경 기록

⑧ 모든 로그기록은 충분한 크기의 값을 설정하여 겹쳐 쓰지 않도록 하여야 한다.

⑨ 주기적으로 로그 백업을 받아야 하고 감사 로그는 최소 1개월 이상, 업무의 중요도에 따라 적절한 기한 및 방법으로 보관되어야 한다.

6. DB 보안지침

본 지침은 DBMS 및 DB의 안전한 운용을 위해 준수하여야 할 업무절차를 정의함으로써 해당 정보자산에 대한 불법 사용을 제한하고 보호하는 것을 목적으로 한다.

가. DB 서버 설치

① DB서버는 외부로부터의 직접접속을 차단하기 위하여 침입차단시스템 내부에 설치하도록 한다.
② 성능과 용량을 충분히 확보하도록 하고 불필요한 서비스를 제거하고 운영하도록 한다
③ DB 담당자는 DBMS를 설치하는 경우 “DBMS 설치 · 폐기 계획서” 작성한다.
④ DB 담당자는 IT운영팀장에게 “DBMS 설치 · 폐기 계획서”의 승인을 받은 후 설치한다.
⑤ DB 담당자는 설치된 DBMS에 대한 보안 설정을 수행하고, 이를 근거로 “DBMS 보안성 검토 요청서”를 작성하여 정보보호 관리자에게 승인을 받도록 한다.

나. DB 운영 관리

(1) 변경 관리

1) DBMS 의 변경

DB 관련 소프트웨어 또는 DB의 변경은 공식적인 변경 절차를 통해 수행되어야 하며, 다음 사항을 준수해야 한다.

① DB담당자는 변경하기 전에 적절한 백오프 절차를 수립하여야 한다.
② 비상시의 DB변경은 복사본에서 우선 실시하도록 하고, 변경 후 변경내용, 변경자, 변경사유 등을 문서화하여 관리하여야 한다.
③ 상용 소프트웨어(DB 관리용 유틸리티)의 임의적 변경은 기능상의 오류를 발생 시킬 위험이 있으므로 꼭 필요할 경우 공급자 및 사용자와 협의 하에 변경하도록 한다.
④ 소프트웨어 변경이 필요한 경우, 변경에 대한 영향분석을 실시하여 변경으로 인해 발생 가능한 위험과 취약성에 대한 적절한 문서화와 테스트 대책이 수립되어야 한다.

2) DB 변경

정해진 응용프로그램에 의해 수정하는 경우 외에 DB에 수록된 중요 데이터를 수정할 필요가 있는 경우에는 다음과 같은 절차를 준수하여야 한다.

① 데이터 수정의 요청 : 데이터의 정확성 문제로 비즈니스에 문제가 발생한 경우 비즈니스 담당자는 팀장의 승인을 획득한 후 '데이터 수정 요청서'를 작성하여, DB 담당자에게 데이터의 수정을 요청할 수 있다.

② 데이터의 수정

◆ DB 담당자는 데이터 수정 요청사항에 대하여 IT운영부서장에게 보고하고 승인을 획득한다.

◆ DB 담당자는 DBMS를 이용하여 데이터를 수정하고 그 결과를 요청자 및 IT운영부서장에게 보고한다.

③ 데이터 수정 내역의 기록 : IT운영부서장은 데이터의 수정에 대해 수정 요청자, 수정자, 수정일자, 수정내역 등을 기록하여 보관한다.

(2) 사용자 인증

1) 계정과 패스워드를 통한 시스템 접근

① DB에 계정을 가진 사용자들은 반드시 ID와 패스워드를 사용하도록 하며 주기적으로 패스워드를 변경하도록 한다.

② 매우 중요한 데이터를 저장하고 있는 DB라면 토큰이나 암호화된 ID와 패스워드 또는 생체인식 등을 이용한 강화된 사용자 인증 방법을 사용하도록 한다.

2) 자동 로그오프

사용자나 타 정보 시스템으로부터 일정시간(30분)동안 어떤 입력도 일어나지 않으면 자동적으로 로그오프 시키거나 세션을 중단시켜야 한다.

3) DBMS 로그인 화면 관리

① 로그인 화면은 단지 로그인 관련 정보만 표시해야 한다.

② 조직이나, 시스템 운영체제, 네트워크 환경, 내부적인 사항과 같은 정보는 성공적인 로그인 후에 표시 되어야 한다.

(3) 권한 관리

1) 사용자 추가

DBMS에 사용자를 추가할 경우 다음의 절차를 따라 사용자 ID를 추가한다.

① ID 가 필요한 사용자는 "DBMS ID 생성 · 변경 · 삭제 신청서"를 작성한 후 DB담당자로부터 승인을 받는다.

② DB담당자는 승인받은 신청서를 참조하여 ID 및 패스워드를 부여한다.

③ DB담당자는 "DBMS 사용자 현황"에 발행한 ID 및 부여한 권한 내역을 기록한다.

④ DB담당자는 생성한 ID와 패스워드를 시스템 사용에 따른 지침 상의 주의사항과 함께 신청한 사용자에게 송부한다.

2) 접근권한 변경 절차

DB에 대한 사용자 접근권한을 변경할 필요성이 있을 때 다음과 같은 절차를 따라 수행한다.

① DB에 대한 추가 접근권한이 필요할 때 필요한 자가 "DBMS 접근권한 신청서"를 작성한다.

② 작성한 "DBMS 접근권한 신청서"를 DB 담당자에게 송부하여 승인을 받는다.

③ 승인 후 DB담당자가 "DBMS 접근권한 신청서"에 따라 접근 권한을 부여한다.

④ DB담당자는 "DBMS 사용자 현황"에 권한 변경 사항을 갱신한다.

3) 사용자 삭제 절차

① 사용자의 퇴직 등 인사관련 변경 사항이 통보되거나 외주 업무의 종료, 팀 이동 등으로 인해 서버에서 ID를 삭제할 필요가 있을 경우 ID 사용자는 "DBMS ID 생성 · 변경 · 삭제 신청서"를 작성한다.

② DB 담당자에게 "DBMS ID 생성 · 변경 · 삭제 신청서"의 승인을 받는다.

③ DB 담당자는 사용자에게 부여되었던 ID를 삭제한다.

④ DB 담당자는 "DBMS 사용자 현황"을 갱신한다.

4) 접근등급 분류 및 권한 목록 유지

DB 관리시스템과 DB의 오브젝트에 대하여 접근 가능한 사용자를 분류하고, 사용자 별 권한의 허용범위를 기술한 접근권한 관리목록을 유지하되 이는 항상 최신의

현황으로 관리해야 한다.

5) 불법 행위에 따른 접근권한의 취소

DB담당자는 DB 또는DBMS의 정상적인 운영을 방해하거나, 다른 사용자의 시스템 사용을 저해하는 등의 악영향을 끼치는 행위가 발견되거나 의심이 될 때 사용자의 모든 권한을 취소할 수 있다.

6) 사용자 권한의 주기적 재평가

사용자에게 부여된 권한은 일정기간(6개월)마다 각 팀 정보보호 담당자에 의해 재평가되어야 한다. 이를 위해 DB담당자는 권한 리스트를 발행하여 각 팀 정보보호 담당자에게 송부하여야 한다.

7) 사용자 임무 변경 통보

각 팀 보안 담당자는 해당 팀원의 업무나 고용 현황 변화에 따른 ID 및 권한의 변경을 DBA에게 즉시 통보해야 하고 DB담당자는 즉시 이를 반영해야 한다.

8) DBMS 및 응용시스템 운영자의 권한 제한

실운용 DB의 백업 등의 단순한 업무를 정해진 절차에 의해 수행하는 DB 관리시스템의 운영자나 실운용 응용시스템의 운영자에게는 직무수행을 위해 필요한 권한 이상의 접근권한을 부여하지 않는다.

9) 응용시스템 개발자의 실운용 정보 접근 제한

운영 단계의 실운용 시스템 DB에 대해, 응용시스템 개발자는 개발중인 응용시스템의 테스트 시 개발과 관련된 실운용 정보 이외의 어떠한 실운용 정보에도 접근할 수 없도록 해야 하며 권한 부여시는 '읽기'와 '복사' 권한만 부여되어야 한다. 테스트 완료 후 해당 권한을 즉시 취소한다.

10) 실 운용 정보의 직접 수정 금지

실운용 시스템의 DB 데이터의 수정은 정상적인 인증방법 외의 방법을 통한 직접 수정을 절대 금해야 한다. 단, 필요시는 수립된 절차에 따라 인가된 사람에 의해 각 운영부서장의 승인 하에 이루어져야 한다.

11) 응용시스템을 통한 실운용 정보의 수정

개발자나 DB담당자를 포함한 일반 사용자들은 승인된 응용시스템을 통하지 않고는 실운용 정보를 수정할 수 없어야 한다.

다. DBMS 접근 통제

(1) DB의 시스템 파일에 대한 변경 권한과 접근통제

DBMS 설치 소프트웨어 라이브러리 또는 DB의 운영체제 파일(데이터 파일, 환경 구성파일, 로그 파일 등)을 변경할 수 있는 권한은 DB담당자와 업무 백업을 하는 다른 한 사람만이 가지고 있어야 하며 이를 위해 별도의 디렉터리를 지정 보관해야 한다.

(2) 여러 장소에서의 다중 접속 제한

하나의 DB 계정을 이용하여 여러 터미널(장소)에서 동시에 여러 온라인 세션(Session)을 연결해서는 안 된다.

(3) 인가된 내부자의 고의 또는 실수에 의한 정보 침해 방지

특별한 관리가 요구되는 기밀정보는 인가된 내부자의 고의 또는 실수에 의한 중요 데이터의 유출, 변조, 혹은 파괴의 위협을 방지하도록 추가적인 인증 절차가 시스템상에 구현되어야 한다.

라. DB 보안 관리

(1) 정보의 속성에 대한 기밀성 유지

DB 내부구조를 파악할 수 있는 사용자나 오브젝트 등의 구성정보가 포함된 데이터(예, DB2 catalog, 데이터 사전 등)에의 접근은 업무적으로 접근할 필요가 있는 사람에게만 접근을 허용하여야 한다.

(2) DB의 암호화

데이터의 유형과 비밀성에 따라 기밀정보인 경우 데이터를 암호화하여 보관해야 한다.

마. 감사 추적성 확보를 위한 로깅

(1) 로깅

1) 기밀정보를 저장하는 DB의 로그 기록

기밀 정보를 저장하고 있는 DB는 기밀 정보의 추가, 수정, 삭제와 관련된 사용자의 ID, 변경 전후 데이터 등에 대해 감사기능을 적용하여 그 기록을 유지하여야 한다.

(2) 감사에 필요한 보안 사항의 로그 기록

DB 보안관련 사항의 로그는 보안대책의 효과성 또는 준수성을 종합적으로 점검하기 위한 내용을 포함하여야 한다.

1) DB담당자에 대한 로그 기록

DB담당자의 활동에 대한 로그기록을 남기도록 한다.

(3) 로그 기록의 관리

1) 로그의 정기적 검토 및 보고

보안 침해 예방 활동을 위해 DB담당자는 정기적으로 보안관련 로그 기록을 검토하고 이상 발견 시 정보보호담당자에게 보고하여야 한다.

2) 로그 기록과 통계 유지

의심스러운 사건이 발생했을 때 경고 및 적발이 가능하도록 응용 프로그램과 DBMS는 사용자의 활동 관련 기록과 통계들을 유지하고 있어야 한다.

3) 보안사항과 접근통제 권한 로그의 보존

사내 다중 사용자 시스템과 네트워크상의 사용자들의 보안사항과 접근권한에 관한 기록이 일정기간(최소 3개월 이상)동안 유지되어야 한다.

4) 로그 기록 공개 제한

DB에 접근 내역을 기록한 로그는 당사자의 서면 동의나 법률에 의한 사직당국의 협조 요청에 의하지 않고는 타인에게 공개할 수 없다.

(4) 보안위반 사건의 사용자 통보

DB 사용자는 어떤 행위가 보안위반과 관계있는 것인지 숙지해야 하고 DB담당자는 보안 위반사항이 기록된다는 사실을 사용자에게 인지시켜야 한다.

(5) 승인에 따른 로그 접근 인가

각 팀별 정보보호 관리자의 사전 승인이 없는 한 사용자의 DB 접근에 관한 모든 로그 기록은 비인가자가 접근할 수 없어야 한다.

(6) 컴퓨터 범죄 의심 시 필요 정보 확보

컴퓨터 범죄나 오남용이 발생했다고 의심될 때 조사 시 필요한 모든 증거 확보를 위해 관련 정보를 즉시 안전하게 확보해야 한다.

바. 복구를 위한 DBMS 로깅

(1) DBMS의 로그 기능 설치

DBMS는 필수적으로 시스템 복구를 위한 로그 기능을 적용하여야 한다.

(2) 중요시스템 활동의 신속한 재개를 위한 로그

중요한 응용시스템에서 사용하는 DB는 즉각적인 시스템 활동을 재개할 수 있도록 보다 자세한 로그 기록을 하여야 한다.

(3) 실운용 정보의 변경에 대한 복원

실운용 기밀정보의 오류 및 부당한 수정을 원래대로 복원될 수 있도록 자세한 로그가 기록되어야 하며 안전하게 보관되어야 한다.

(4) 로그파일의 백업

로그파일은 DB의 데이터 백업이 이루어지는 것과는 별개의 백업주기를 정하여 백업을 수행하여야 한다.

(5) 로그파일 모니터

다음 사항을 항상 모니터 하여야 한다.

- ◆ 로그파일의 저장 공간(디스크, 자기테이프 등)
- ◆ 로그파일의 저장 현황

7. 부칙

가. 시행일

본 지침은 2007. 00. 00부터 시행한다.

8. 관련서식

[첨부 1] 보안패치 관리대장
[첨부 2] 계정 관리대장
[첨부 3] 침해사고 보고 양식
[첨부 4] 백업 관리대장
[첨부 5] 로그 점검 관리대장

[첨부 1] 보안패치 관리대장

보안패치 관리대장

서버담당자	정보보호관리자

서버명	
작성일	년 월 일

NO	패치명	Patch ID	용도	패치일	담당자	비고
1	-	100123	취약점패치	2007.1.10	홍길동	
2						
3						

[첨부 2] 계정 관리대장

계정 관리대장

서버담당자	정보보호관리자

서버명	
작성일	년 월 일

NO	계정	패스워드	등록일	용도	책임자	비고
1	root	-	2007.1.1	관리	운용팀장	기한 등

* 본 양식은 작성 후 밀봉 후 정보보호관리자에게 제출한다.
* 정보보호관리자는 시건 장치가 있는 안전한 장소에 보관한다.

[첨부 3] 침해사고 보고 양식

침해사고 보고 양식

침해사고 처리 담당자	침해사고 번호
	Ex) IN-040304-3212
신고기관 정보	
기관 이름	
신고자 이름	
전화번호	
E-mail	
피해 시스템 정보	
IP 주소	
호스트 명	
운영체제	
추정 피해 시간	
시스템 운영 환경	
공격 시스템 정보	
IP 주소	
호스트 명	
사고에 대한 설명(간단히 작성)	
사고발견 경위, 피해현황 등	

관련 기관(부서) 통지	
기관(부서)명	통지 내용

[첨부 4] 백업 관리대장

백업 관리대장

서버담당자	정보보호관리자

NO	백업일자	서버명	백업 정책	백업 내용	담당자
1	2007. 1. 1	DNS	Full backup	모든 디렉토리/파일	홍길동
2	2007. 1. 7	DNS	Incremental Backup	LOG 파일	홍길동
3					

[첨부 5] 로그 점검 관리대장

로그 점검 관리대장

서버담당자	정보보호관리자

작성일	년 월 일

서버명	로깅 관리	접근 로그	실패 로그	관리자 로그	보안 로그

◆ 로그 관리 점검 결과 (이상/문제 발생시 작성)

문제 발생 시스템	
문제 내역	
조치 내용/결과	
향후 대책	
정보보호 담당자 검토 의견	
서버 담당자 검토 의견	

◆ 세부 로그 관리 점겸 항목

구분	세부 점검 항목	점검 결과
로깅 관리	로그인/접근 로그 로깅 여부	
	주요 시스템 로그 로깅 여부	
접근 로그 관리	로그인 사용자 정보 확인	
	로그인/로그아웃 시간 및 정보	
	사용자별 접근 서비스 정보	
실패 로그 관리	로그인 실패 로그	
	정보 접근 실패 로그	
	권한 접근 실패 로그	
관리자 로그 관리	관리자 권한 로그인 로그	
	관리자 작업 수행 로그	
보안 로그 관리	취약점 공격 및 침해사고 관련 로그	
	공격자 작업 수행 로그	

* 세부 점검 항목은 서버 용도 및 서비스 특성에 맞추어 작성 필요