㈜ OO 웹하드
정보통신설비 운영 지침

2014. 12

㈜OO웹하드

㈜OO 웹하드 정보통신설비 운영지침

본 지침은 ㈜OO웹하드의 정보통신설비 운영에 관련된 제반 사항이 수록되어 있으므로 ㈜OO웹하드의 허가 없이 상용 정보통신망에 게재를 삼가 해 주시고, 보안 관리상 외부로의 반출을 금지하오니 유의하시기 바랍니다.

※ 본 지침은 웹하드 업체의 정보통신설비의 보안관리에 대한 이해를 돕기 위하여 작성된 예시 지침이며, 본 지침의 적용 시 업체의 현황에 맞도록 수정할 것을 권고함

문서 개정 이력

개정번호	조항번호	개 정 내 용 요 약	개정일자	담당자	확인자
1.00	-	신규 제정	2014.12.31		

목 차

I. 개 요

1. 목 적

본 지침은 ㈜OO웹하드(이하 회사)의 정보시스템 및 정보시스템 운영과 관련된 절차를 기록·관리하여 체계적인 업무 수행이 가능하도록 지속적으로 관리하는 것을 목적으로 한다.

2. 적용 대상 및 범위

본 지침은 회사의 정보시스템 및 정보보호시스템 운영과 관련된 조직 또는 장비 전반에 적용한다.

3. 시행일

본 지침은 결재일로부터 시행한다.

4. 예외적용

다음 각 호에 해당하는 경우에는 본 규정에서 명시한 내용일지라도 정보보안 담당자의 승인을 받아 예외 취급할 수 있다.

- 기술 환경의 변화로 적용이 불가능할 경우
- 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있을 경우
- 기타 재해 등 불가항력적인 상황일 경우

II. 서버 보안

1. 일반사항

1.1. 목적

UNIX, Windows 계열 서버 시스템을 다양한 보안 위협 및 취약성으로부터 안전하게 보호하고, 운용 관리 하는데 그 목적이 있다.

2. 서버 시스템 운영 시 관리

2.1. 운영 관리

- 서버에 설치된 소프트웨어의 현황을 목록으로 만들고 변경 현황을 관리한다.
- 담당자는 소프트웨어의 변경 및 하드웨어 변경 시, 이에 대한 충분한 검토를 실시하여 “[별첨 1] 시스템실 작업 계획서”를 작성하고, 책임자의 승인을 받아 작업을 수행한다.
- 작업 완료 후 “[별첨 2] 시스템 작업 결과 보고서”를 작성하여 작업 이상 유무를 책임자에게 보고하도록 한다.
- 책임자는 서버 운영 상 설치를 허용하는 소프트웨어 및 유틸리티 목록을 검토하여 승인해야 하고, 허용하지 않는 소프트웨어 또는 유틸리티가 설치되지 않도록 통제하여야 한다.
- 담당자는 서버에 설치된 소프트웨어 및 유틸리티의 적정성을 수시로 점검하도록 하여, 설치된 허가되지 않은 소프트웨어 및 유틸리티가 존재할 경우 이를 책임자에게 보고토록 해야 한다.
- 서버에 설치된 소프트웨어 패키지의 임의적 변경은 기능상의 오류를 발생시킬 위험이 있으므로 임의의 변경을 하지 않는 것을 원칙으로 한다. 다만, 필요한 경우 책임자 및 제품공급자와 협의 하에 변경한다.
- 담당자는 서버 변경 시 발생할 수 있는 위험에 대응하기 위해 서버 변경에 대한 문서화 작업이 이루어지도록 한다.
- 담당자는 서버의 하드웨어 및 소프트웨어의 지속적인 가용성과 무결성 확보를 위해 정기적 혹은 필요한 경우 수시로 예방점검을 한다.
- 담당자는 서버시스템의 세부 운영 절차와, 장애 발생 시의 처리 절차를 연 1회 검토하여 별도 작성 관리하고, 그 절차에 따르도록 한다.
- 담당자는 내부 직원의 비상연락망 및 서버시스템 유지보수 업체의 비상 연락망을 관리하여야, 장애 발생 등의 예기치 못한 비상 상황에 대처할 수 있도록 대비한다.

2.2. 패스워드 관리

2.2.1. 패스워드 관리 정책

- 신규 사용자에게 시스템 사용 권한을 부여할 때에는 반드시 패스워드를 부여 받도록 해야 한다.
- 패스워드는 최소 3개월 주기로 변경하여야 한다.
- 사용자는 자신의 패스워드를 기억 하고 패스워드 보안을 철저히 해야 한다.
- 모든 사용자는 패스워드 인증을 통해서만 시스템을 사용할 수 있어야 한다.
- 모든 사용자의 패스워드는 8자 이상으로 한다.
- 직전의 패스워드로 변경이 허용되지 않아야 한다.
- 루트 권한을 갖은 사용자가 퇴직 및 인사발령 등의 사유로 루트 권한을 인계할 때는 인수자는 즉시 기존에 사용했던 패스워드를 변경해야 한다.
- 패스워드를 전자우편으로 전달하지 않는다.
- UNIX 시스템은 Shadow 패스워드 시스템을 사용하여 보안을 강화한다.
- UNIX 시스템의 담당자는 수시로 패스워드 파일의 접근권한을 점검한다.
- 시스템 최초 설치 후 공급업체에서 미리 설정한 특정 계정과 패스워드는 인수시험 완료 후 즉시 삭제하거나 변경한다.

2.2.2. 패스워드 이력 관리

- 서버 시스템의 패스워드 변경 시 변경되는 신규 패스워드는 담당자에게 제출되어야 한다.
- 담당자는 관리 대장에 각 시스템의 패스워드에 대한 이력을 대외비로 분류하고 관리하여 안전하게 보관한다.

2.2.3. 패스워드 사용 규칙

- 필수 사항
  - 최소 8자 이상 이어야 한다.
  - 사용자 계정 이름을 그대로 패스워드로 사용해서는 안 된다.

- 선택 사항
  - 사전에 있는 단어나 거꾸로 철자화한 단어를 패스워드로 사용해서는 안 된다.
  - 사용자 자신의 관련 정보를 이용한 패스워드를 사용해서는 안 된다.
  - 키보드의 일렬화된 배열 패스워드를 사용해서는 안 된다. (예: asdfghjk 등)
  - 사용자 계정과 유사한 패스워드를 사용해서는 안 된다.
  - 빨리 입력하기 어려운 패스워드는 사용하지 않는다.
  - 서로 관련 없는 문자들을 혼합한 패스워드를 사용한다.
  - 한글의 특성을 최대한 활용한 패스워드를 사용한다.
  - 대소문자, 특수문자를 혼합한 패스워드를 사용한다.

※ 패스워드 생성 시 참고

[개인정보의 안전성 확보조치 기준 및 해설서 제5조(비밀번호 관리) 규정]

· 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 2종류 이상으로 구성한 경우

· 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9개, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성한 경우

2.2.4. 패스워드의 책임성

- 담당자는 다음 사항을 수행하여야 한다.
  - 최초 로그인에 대한 패스워드를 설정한다.
  - 패스워드의 변경 주기를 설정한다.
  - 퇴직 및 인사발령 등으로 사용하지 않는 사용자 계정을 삭제한다.
  - 패스워드는 3개월 주기로 변경하도록 하며, 이·퇴직/발령 등의 사유로 인해 담당자가 변경되는 경우 즉시 계정에 대한 패스워드를 변경해야 한다.
  - 주기적으로 보안도구 등을 이용해 패스워드 보안을 점검해야 한다.
  - 여러 명의 담당자가 하나의 계정을 공유하는 것을 금지한다.

- 모든 사용자는 다음 사항을 준수해야 한다.
  - 항상 패스워드의 보안성을 유지하여야 한다.
  - 최초 패스워드를 부여 받으면 즉시 다른 패스워드로 변경하여야 한다.
  - 의심스러운 패스워드 위반 등이 발생하면 즉시 책임자에 보고해야 한다.
  - 다른 사람이 지켜보고 있을 때에 패스워드를 입력하지 않아야 한다.
  - 여러 서버에 계정이 있을 경우는 각각 다른 패스워드를 사용해야 한다.
  - 장시간 사용하지 않거나 퇴직 시에는 계정의 사용 중지를 요청하여야 한다.

3. 유닉스 시스템 보안관리

3.1. 계정 관리

3.1.1. 계정 보호

- 패스워드를 미설정하거나 패스워드와 계정이 동일한 계정을 허용해서는 안 된다.
- 담당자와 책임자를 제외하고 UID가 '0'인 계정이 존재해서는 안 된다.
- 모든 계정의 PATH환경 설정에 "."이 존재해서는 안 된다.
- 특별한 경우(응용프로그램용 ID, 시스템 유틸리티용 ID 등) 이외에 하나의 ID는 동시에 하나의 세션만 로그인 할 수 있다.
- home 디렉토리는 소유자 이외의 사용자에게 write 권한을 부여해서는 안 된다.
- 사용자의 .profile, .cshrc, .login 등은 소유자 이외의 다른 사용자에게 write 권한을 부여해서는 안 된다.

3.1.2. 계정 생성

- ".profile" 파일은 적절한 path값과 제한된 umask(022)를 설정해야 한다.
- 임시파일 디렉토리는 사용자 path 변수에 포함하지 않아야 한다.
- 모든 사용자의 로그인 ID와 UID는 서로 다르게 사용하여야 한다.
- 패스워드는 3개월 주기로 변경하여 사용해야 하며 변경사항을 관리하여야 한다.
- UNIX 시스템 담당자 이외의 사용자(응용프로그램 개발자 등)들은 제한된 shell을 사용하며 아래와 같은 사항에 대해서 제한을 받을 수 있다.
  - 디렉토리의 사용은 자신의 디렉토리에 국한된다.
  - 자신의 디렉토리와 서브 디렉토리내의 파일만 접근할 수 있다.
  - 담당자에 의해 지정된 path 내의 명령어만을 실행할 수 있다.
- 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.

3.1.3. 계정 사용 중지

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

3.1.4. 정지된 계정 재사용

- 정지된 계정을 다시 사용하는 사용자는 새로운 패스워드를 부여받고, 최초 로그인할 때 즉시 패스워드를 변경하도록 해야 한다.

3.1.5. 계정 폐쇄

- 사용자의 home 디렉토리에 있는 모든 파일과 하위 디렉토리 등을 제거한다.
- 사용자가 소유의 모든 파일을 조사하여 불필요한 파일은 없애야 한다.
- 사용자가 만들어 놓은 관련 파일을 조사하여 제거한다.
- 사용자 계정이 관리 권한 밖의 다른 시스템 내에 존재하고 있을 경우, 해당 담당자에게 그 계정에 대한 제거를 의뢰하여야 한다.

3.1.6. 계정 이동

- 계정의 이동 시에는 사용자의 UID와 GID가 있는지를 조사하여, 만일 존재할 경우에는 새로운 UID와 GID를 부여하여야 한다.
- 계정에 대한 사용자 파일을 새로운 시스템으로 복사한다.
- 이전의 계정은 폐쇄하거나 정지한다.

3.1.7. 그룹 생성

- 사용 목적이 유사하거나 같은 프로젝트 내에 있는 계정들을 동일 그룹에 둔다.
- 새로운 프로젝트가 생길 경우는 프로젝트와 관련된 사용자별로 그룹을 만든다.
- /etc/group과 /etc/passwd내에 있는 그룹과 사용자 ID는 일치하여야 한다.
- 특별히 보안이 필요한 사용자 계정들을 별도 그룹으로 지정하여야 한다.

3.1.8. 그룹 폐쇄

- 사용하지 않거나, 구성원이 없는 사용자 생성 그룹은 삭제한다.

3.2. 접근 통제

3.2.1. 네트워크를 통한 접근통제

- 네트워크 파일은 group과 other 사용자에게 write 권한을 부여하지 않아야 한다.
- 네트워크 파일 내의 필요하지 않는 호스트명은 삭제해야 한다.
- 사용하지 않고 불필요한 네트워크 서비스는 삭제한다. (RPC, NFS 등)
- 시스템의 사용자나 네트워크 사용 상태정보 등을 외부로 유출시킬 수 있는 프로그램을 제한한다. (finger, talk, ftp, r서비스 등)
- 네트워크 파일시스템 NFS(Network File System)을 통제한다.
  - export할 파일시스템을 제한해야 하고 파일시스템을 마운트할 수 있도록 허용된 호스트명이 명시되어 있어야 한다.
- sendmail은 항상 최신 version을 사용하고 통제하여야 한다.
  - sendmail과 관련된 환경설정 파일은 접근을 제한하여야 한다.
  - sendmail을 통해 사용자의 상태정보를 확인할 수 있는 expn, vrfy 등의 명령은 사용을 제한하여야 한다.
- 기타 필요한 네트워크 서비스 및 네트워크 관련 설정은 적절한 보안이 강구되어야 한다.
- 관리자는 내부의 지정된 위치 외에서는 접근을 할 수 없도록 한다.

3.2.2. 로그인 접근 통제

- 로그온 절차 성공 전에는 시스템 또는 응용프로그램의 식별이 가능한 식별자 표시를 금지한다.
- 로그온 시 불법접근 및 비인가 사용자의 접근을 경고하는 보안 경고 문구가 표시되도록 설정한다.
- 로그온 시 비인가된 사용자에게 시스템 관련 정보를 제공해서는 안 된다.
- 오류 발생에 대해 상세내역을 출력을 하지 않는다.
- 성공하지 못한 로그온 시도 횟수를 10회 이하로 설정하며, 연속 로그인을 실패한 로그인에 대해서 다음과 같이 조치한다.
  - 연결을 해제한다.

- 성공하지 못한 로그온 시도에 대해 로그를 남긴다.
- 성공 로그온에 대해서 이전 로그온 날짜 및 시간, 이전 로그온 이후의 성공하지 못한 로그온 정보를 표시한다.
- 서버 로그인시 텔넷(telnet) 접속을 지양하도록 설정/사용 하도록 하고, 가능한 SSH를 사용토록 한다. 이 때, 원격 접속에 서비스 포트 설정은 기본설정을 반드시 변경하여 사용하여야 한다.

3.3. 보안 패치 관리

- 보안패치는 각종 소프트웨어, 운영체제 등에서 발견되는 보안상의 취약성을 보완해주는 프로그램으로 새로운 패치가 발표되는 즉시 시스템 적용성을 검토한 후 즉시적용 하여 보안조치를 취함으로서 보안 사고를 사전에 예방할 수 있도록 한다.
- 회사 내의 패치 적용 대상 시스템, 소프트웨어별로 다음 사항을 포함하도록 관리 한다.
  - 각 서버에서 사용되는 소프트웨어 목록 및 버전 정보 목록 관리
  - 패치 설치 후 서버의 정상적인 운영상태 확인
- 기타 보안패치 관리 작업을 자동화 해주는 소프트웨어를 사용할 경우, 위 사항들을 만족하고 있는지 주기적으로 검토한다.

3.4. 백업 및 복구

3.4.1. 백업

- 서비스 제공 및 업무 수행과 직접적인 관계가 있는 주요정보는 물리적 재난이나 정보통신설비의 오류 발생의 긴급 상황이 발생할 경우, 즉각적으로 복구할 수 있도록 주기적으로 백업을 수행하고 백업 매체를 안전한 곳에 보관하도록 한다.
- 위험분석 등의 방법을 통하여 자체적으로 중요도에 따라 관리가 필요한 주요 정보를 식별하고 주요정보에 대한 백업 계획을 마련한다. 정보의 중요성 및 특성을 고려하여 백업의 방법 및 횟수 등의 백업 계획을 마련한다.
- 백업은 백업될 데이터의 성격에 따라 백업시기, 백업주기, 백업방법, 백업데이터의 보관방식 및 보존기간 등을 포함하여 백업 담당자, 백업 및 복구 방법・절차・주기 등을 기록/관리 한다.

3.4.2. 백업 방식

- 백업 방식은 데이터의 성격, 데이터의 양, 그리고 정보통신설비 자원의 가동시간 등을 고려하여 결정한다.
- 백업은 백업된 데이터의 기록매체에 따라 디스크 백업과 테이프 백업으로 구분되며, 백업이 신속하게 이루어져야 할 경우에는 디스크 백업방식을 채택한다.

3.4.3. 복구

- 수립한 백업 및 복구 방법·절차는 다음과 같은 단계에 따라 수행되도록 한다.

- 장애발생 상황인지 및 보고
- 복구 우선순위의 결정
- 사후 점검 및 원인분석
- 장애 및 복구기록 유지관리 등

- 복구는 가장 믿을만한 백업매체를 사용해야 한다. 피해 시점 또는 문제발생 시점 이전의 백업본을 사용하도록 한다. 백업·복구의 관리를 위해 관리대장을 만들고 기록할 수 있도록 한다.

3.5. 감사 및 로그 기록

사용자가 사용한 명령들에 대해 로깅이 필요한 서버에 대해서만 로그를 기록하고, 기타 서버들은 요약 파일만 관리한다.

3.5.1. 로그 기록 관리

다음의 사항들은 기본적으로 로그를 기록하여야 할 내용들이다.

- 가장 최근에 로그인한 사용자 정보
- 사용자의 로그인 성공/실패 정보
- 사용자별 로그인/로그아웃 정보(날짜와 시간)
- 접근 IP주소, 접속 터미널 정보
- 시스템 접근의 성공 및 실패 기록(비권한자 침입시 침입자 이름/일시 등)
- 데이터 및 기타 접근의 성공 및 실패 기록을 시스템이 지원하는 경우에 한해 추가 기록하도록 한다.
- 패스워드 변경 등과 같은 중요 시스템 명령의 수행 내역 로그
- 사용자의 접속 가능 수준 이상의 정보를 얻으려는 시도에 관한 로그
- 기본 응용프로그램 구동 관련 로그 (메일 로그, 파일 전송 로그, 웹서버 로그 등)

3.5.2. 로그 보관 주기

- 로그는 최소 3개월 이상, 업무의 중요도에 따라 적절한 방법으로 보관되어야 한다.

3.5.3. 로그 데이터 관리

- 로그 데이터는 적절하게 관리되어야 한다.
- 사용자나 이벤트 등 감사할 대상을 선택할 때 각 감사 대상들이 적정한가를 판단해야 한다.
- 로그 파일이 수용치를 넘을 때는 테이프 등에 보관하고 로그 파일을 초기화 또는 삭제해야 한다.
- 관리자는 서버 접속 로그 등에 대한 내·외부의 문서화된 요청 시, 관련 법률에 근거하여 제공한다. 다만, 법률에 근거하지 않은 불가피한 경우 책임자의 승인 후 제공한다.

※ 관련 서식은 “[별첨 7] 서버 장비 설정/로그 백업 관리대장”을 참조

4. Windows 계열 시스템 보안관리

4.1. 계정 관리

4.1.1. 패스워드 관리

- 패스워드는 최소 8자 이상으로 하며, 연속 4자 동일 문자의 사용을 금지하고 ID와 동일한 패스워드 사용을 금지한다.
- 패스워드는 3개월 주기로 변경하여 사용해야 한다. 유출된 경우, 즉시 변경한다.
- 기존 패스워드는 최대 12개월 이내, 업무의 중요도에 따라 6개월 이내 재사용을 금지한다.
- 사용자가 자신의 패스워드를 바꾸기 위해선 반드시 로그온 해야 한다.
- 단순 패스워드를 사용하지 않도록 해야 한다.

4.1.2. 사용자 관리

- 신규 사용자 및 사용자 그룹을 생성시킬 때 사용 목적, 사용자 정보, 사용 기간 등을 정확히 고려하여 생성하여야 한다.
- 그룹의 등록 정보 및 접근 권한 등은 그룹 내의 모든 구성원에게 허용되므로 그룹과 사용자 계정 설정 시 특별히 주의하여야 한다.
- 사용자가 소속된 그룹을 확인하여 적합한 그룹에 속해 있는지 확인 후 불필요한 그룹에 속해 있을 경우 삭제한다.
- 사용자별로 서버에 접속할 수 있는 날짜와 시간을 설정하며 설정된 시간 이외에는 로그온을 금지시킨다.
- 사용자는 사용자의 업무에 필요한 시스템에만 접속할 수 있도록 한다.
- 담당자는 사용자 계정의 유효기간을 설정해야 한다. 또 임시 계정은 반드시 사용 기간이 경과된 후 사용할 수 없도록 설정한다.

4.1.3. 관리자와 관리자 그룹 관리

- 관리자(Administrator Account)와 관리자 그룹(Administrators Group)은 접근 권한의 제한이 없으므로 특별히 주의하여 설정되어야 한다.
- 사용자 그룹 중 특별한 권한을 갖는 그룹은 그룹의 구성원을 검토하여 불필요한 사용자 계정은 삭제한다.
- 기존 시스템에 새로운 담당자가 선임되었다면 시스템 담당자는 즉시 담당자 패스워드를 변경하여야 한다.
- 관리작업용, 일반작업용 계정을 구분하여 관리한다.
- 모든 운영자 계정으로의 실패한 로그온 시도는 기록되어야 한다.
- “Domain Admins Group”과 “Administrator Group”의 구성원을 확인하여 불필요한 사용자는 모두 삭제한다.

4.1.4. Guest 계정과 Everyone Group 관리

- Guest 계정은 허용하지 않는다.
- 일시적으로 Guest계정을 사용해야 할 경우 사용 환경을 신중히 설정한다.

4.1.5. Login Parameter

- 자동 로그온 기능을 제거하여야 한다.
- 로그온 시 불법 접근의 제한 및 사용자의 권한 한계 등을 알리는 경고를 한다.

4.2. 접근 통제

4.2.1. 네트워크통한 접근통제

- 네트워크를 통한 시스템 접근 권한은 원격 로그온이 반드시 필요한 Group에만 설정하도록 한다.
- 관리자 그룹만이 로컬컴퓨터(Local Computer)에 로그온을 할 수 있도록 하여야 하며 이외의 사용자들은 로컬컴퓨터에 접속을 금지하여야 한다.
- 보안로그와 감사는 관리자 그룹(Administrators Group)만이 관리하여야 한다.
- 도메인내의 로컬그룹(Local Group)에 부여된 사용 권한을 점검하여야 한다.
- 공유 폴더의 필요성을 검토하여 불필요한 공유 기능을 제거하여야 한다.
- 시스템에 설치된 서비스를 조사하여 불필요한 서비스는 제거하여야 한다.
- NetBIOS 접근을 제한하여야 한다.

※ 관련 양식 “[별첨 3] 보안정책 변경 요청서” 참고

4.2.2. 로그인 접근 통제

- 로그온 절차 성공 전에는 시스템 또는 응용프로그램의 식별자 표시를 금지한다.
- 로그온 시 불법접근 및 비인가 사용자의 접근을 경고하는 보안 경고 문구가 표시되도록 설정한다.
- 로그온 시 비인가 된 사용자에게는 시스템에 대한 정보를 제공하지 않는다.
- 성공하지 못한 로그온 시도 횟수를 10회 이하로 설정하며, 연속 로그인을 실패한 로그인에 대해서 다음과 같이 조치한다.
  - 연결을 해제한다.
  - 일정 시간 로그온을 할 수 없도록 로그인 화면을 잠근다.
  - 성공하지 못한 로그온 시도에 대해 로그를 남긴다.
- 윈도우 서버의 터미널서비스의 원격접속서비스 포트를 반드시 변경하여 설정/사용 하도록 한다.

4.3. 보안 패치 관리

4.3.1. 보안패치

- 보안패치는 각종 소프트웨어, 운영체제 등에서 발견되는 보안상의 취약성을 보완해주는 프로그램으로 새로운 패치가 발표되는 즉시 시스템 적용성을 검토한 후 즉시적용 하여 보안조치를 취함으로서 보안 사고를 사전에 예방할 수 있도록 한다.
- 회사 내의 패치 적용 대상 시스템, 소프트웨어별로 보안패치 방법 및 절차를 정리하여 패치 적용 정보를 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
  - 패치 설치 후 서버의 정상적인 운영상태 확인
- 기타 보안패치 관리 작업을 자동화 해주는 소프트웨어를 사용할 경우, 위 사항들을 만족하고 있는지 주기적으로 검토한다.

4.4. 백업 및 복구

4.4.1. 백업

- 서비스 제공 및 업무 수행과 직접적인 관계가 있는 주요정보는 물리적 재난이나 정보통신설비의 오류 발생으로 긴급 상황이 발생할 경우, 즉각적으로 복구할 수 있도록 주기적으로 백업을 수행하고 백업 매체를 안전한 곳에 보관하도록 한다.
- 위험분석 등의 방법을 통하여 자체적으로 중요도에 따라 관리가 필요한 주요 정보를 식별하고 주요정보에 대한 백업 계획을 마련한다. 정보의 중요성 및 특성을 고려하여 백업의 방법 및 횟수 등의 백업 계획을 마련한다.
- 백업은 백업될 데이터의 성격에 따라 백업시기, 백업주기, 백업방법, 백업데이터의 보관방식 및 보존기간 등을 포함하여 백업 담당자, 백업 및 복구 방법・절차・ 주기 등을 기록/관리 한다.

4.4.2. 백업 방식

- 백업 방식은 데이터의 성격, 데이터의 양, 그리고 정보통신 설비 자원의 가동시간 등을 고려하여 결정한다.
- 백업은 백업된 데이터의 기록매체에 따라 디스크 백업과 테이프 백업으로 구분되며, 백업이 신속하게 이루어져야 할 경우에는 디스크 백업방식을 채택한다.

4.4.3. 복구

- 수립한 백업 및 복구 방법・절차는 다음과 같은 단계에 따라 수행되도록 한다.
  - 장애발생 상황인지 및 보고
  - 복구 우선순위의 결정

  - 사후 점검 및 원인분석
  - 장애 및 복구기록 유지관리 등
- 복구는 가장 믿을만한 백업매체를 사용해야 한다. 피해 시점 또는 문제발생 시점 이전의 백업본을 사용하도록 한다.

4.5. 감사 및 로그 기록

4.5.1. 로그 기록 관리

- 아래 사항을 참고로 하여 자원과 이벤트를 감사한다.
  - 감사정책은 시스템의 사정에 맞게 유연하게 관리할 수 있도록 정의한다.
  - Users 그룹 대신에 Everyone 그룹을 감사하여 로컬 사용자 외에 네트워크에 연결하는 모든 사용자들을 감사한다.
  - 경향 분석을 위해 감사로그를 정기적으로 보관한다.
- 담당자는 수시로 보안 감사 정책을 확인하여야 하며 보안 감사 이벤트 로그는 다음의 내용을 기록 하도록 감사 정책을 설정하여야 한다.
  - 사용자 계정 관리 성공/실패 정보
  - 사용자 로그온, 로그오프 성공/실패 정보
  - 시스템 이벤트 (시스템 종료 및 재시작 정보 등) 성공/실패 정보
  - 보안 정책 변경 성공/실패 정보
  - 사용자 권한 획득 및 사용에 관한 성공/실패 정보
  - 개체 접근에 대한 성공/실패 정보
- 보안 관련 감사를 위해 로그온 및 로그오프, 보안정책 변경에 대해서는 반드시 로그기록을 해야 한다.
- 기타 항목에 대해서는 자원의 중요도에 따라 선택적으로 로그를 기록한다.
- 중요 시스템 파일이나 데이터에 대해서는 별도 감사항목을 설정하여 확인한다.

4.5.2. 로그 보관 주기

- 로그는 최소 3개월 이상, 업무의 중요도에 따라 적절한 방법으로 보관되어야 한다.

4.5.3. 로그 데이터 관리

- 로그 데이터는 적절하게 관리되어야 한다.
- 로그기록에 접근할 수 있는 권한을 담당자로 제한하여야 한다.
- 사용자나 이벤트 등 감사할 대상을 선택할 때 각 감사 대상들이 적정성을 판단해야 한다.
- 로그 파일이 수용치를 넘을 때는 테이프 등에 보관하고 로그 파일을 초기화해야 한다.
- 모든 로그기록은 충분한 크기의 값을 설정하여 겹쳐 쓰지 않도록 하여야 한다.

5. 점검 및 로깅

5.1. 주기적 모니터링

담당자는 다음 각 호와 같은 서버의 사용 현황 및 이상 유무를 주기적으로 모니터링해야 하며, 이상 상황 발생 시 신속히 책임자에게 보고한다.

1) 서버 용량 (CPU, 메모리 등)
2) 파일시스템 용량초과
3) 사용자 접속현황

5.2. 로그내용

담당자는 정보보호 사고 또는 오류 발생 시 추적성을 확보하기 위해 중요 서버에 대하여 다음 각항과 같은 로그를 기록하도록 설정해야 한다.

1) 중요 정보의 기록
   중요 정보를 취급하는 서버의 경우 비밀정보의 추가/수정/삭제 및 보안 위반사항들에 대해여 로그를 기록하여야 한다.

2) 사용자 보안관련 활동의 로그 기록
   사용자 책임성을 확보하기 위해 사용자의 모든 보안관련 활동은 로그에 기록되어야 한다.

1) 감사에 필요한 보안사항의 로그 기록
   서버 보안 관련 사항의 로그는 보안대책의 효과성 또는 준수성을 종합적으로 점검하기 위한 내용을 포함하여야 한다.

2) 시스템에 영향을 줄 수 있는 명령어의 로그 기록
   시스템 담당자에 의해 실행되는 시스템 관련 명령어는 로그를 통해 추적할 수 있도록 해야 한다.

5.3. 로그 관리

1) 시각 동기화
   사건의 정확한 기록을 위해 네트워크에 연결된 사내의 모든 서버는 내부 시각을 일치시켜야 한다.

2) 로그변조 행위에 대한 대응
   서버는 로그 파괴, 변조에 대응할 수 있는 정보보호 기능을 보유하여야 한다.

3) 로그파일 접근 제한
책임자의 사전 승인이 없는 한 모든 시스템과 응용 프로그램의 로그는 비인가자가 접근할 수 없어야 한다.

4) 로그 공개 제한
시스템 접속내역을 기록한 로그는 사용자의 서면동의나 법률에 의한 관련기관의 협조요청에 의하지 않고는 타인에게 공개할 수 없다.

5) 정보보호 관련 로그의 보존
서버의 정보보호 관련 로그 및 접근권한에 관한 기록은 최소 3개월 동안 로그의 누설이나 수정을 할 수 없는 곳에 안전하게 보관한다.

5.4. 로그 분석

1) 로그의 정기적 검토
정보보호 침해 예방 활동을 위해 담당자는 주기적으로 정보보호에 관련된 로그 기록을 검토 및 조치하고 그 결과를 관리한다.

2) 로그 기록과 통계 유지
의심스러운 사건이 발생했을 때 경고 및 적발이 가능하도록 사용자의 활동 관련 기록과 통계들을 유지하고 있어야 한다.

※ 관련 서식은 “[별첨 7] 서버 장비 설정/로그 백업 관리대장”을 참조

III. 네트워크 보안

1. 일반사항

1.1. 목적

네트워크를 통한 접근 프로세스를 확립하고 효과적으로 접근을 통제하기 위한 보안 요구사항을 정의함으로써, 내부 사용자들의 합법적인 네트워크 사용을 유도하고 내·외부의 불법적인 침입과 위협으로부터 내부 정보자산을 보호하는데 그 목적이 있다.

2. 네트워크 운영 시 관리

2.1. 운영 관리

- 네트워크의 전체 라우팅 및 필터링 등의 설정 정책에 대한 현황을 유지하고 변경 현황을 관리한다.
- 담당자는 네트워크 시스템의 하드웨어 및 소프트웨어의 지속적인 가용성과 무결성 확보를 위해 정기적 혹은 필요한 경우 수시로 예방점검을 한다.
- 담당자는 네트워크시스템의 세부 운영 절차와, 장애 발생 시의 처리 절차를 연 1회 검토 및 작성 관리하고, 그 절차에 따르도록 한다.
- 담당자는 내부 직원의 비상연락망 및 네트워크시스템 유지보수 업체의 비상 연락망을 관리하여야 하며, 장애 발생 등의 예기치 못한 비상 상황에 대처할 수 있도록 대비한다.
- 침해사고의 대응 및 추적성을 높이기 위해서 모든 네트워크시스템의 시간을 시간서버와 동기화 시키도록 한다.

3. 네트워크 보안 관리

3.1. 사용 관리

3.1.1. 사용 권한

- 내부망은 인가된 직원에 한하여 접근 단말장치(PC 등)에 필요한 보안설정을 완료한 후 인가된 범위 내에서 이용할 수 있다.
- 비인가자나 외부인의 외부망 사용을 위해서는 보안서약서를 작성 후, 네트워크 담당자로부터의 네트워크 사용 승인을 득한 후 네트워크를 이용할 수 있다.
- 비인가자나 외부인이 내부망을 사용해야 할 경우, 네트워크담당자의 승인을 받아 접근이 필요한 단말장치(PC등)에 필요한 보안설정 완료한 후, 네트워크 담당자로부터의 네트워크 사용 승인을 득한 후 이용할 수 있다.

- 사용기간이 만료되었거나 사용 종료된 네트워크 자원은 즉시 회수 한다.

3.1.2. 사용자 준수사항

- 네트워크 통신망을 업무 이외의 사적인 용도로 이용할 수 없다.
- 통신망을 이용하여 비밀 및 대외비 이상의 정보자산을 사전 승인 없이 외부에 공개하거나 발신할 수 없다.
- 통신망을 이용하여 유해정보를 유포하거나 비인가 사이트에 대한 불법침입, 해킹 등의 행위에 사용할 수 없다.
- 타인의 PC, 전자메일 시스템, 정보시스템에 허가 없이 접근하거나, 다른 사용자의 네트워크 사용을 방해 하여서는 안 된다.
- 외부로부터 음란성 파일을 취득, 유포하거나 타인을 비방, 선동하거나 성적 수치심 및 성차별 내용의 메일을 유포할 수 없다.
- 개인 사용자는 통신망을 불법 도청하거나 보안 통제장비를 우회하기위해 어떠한 장비도 통신망에 접근시키거나 설치할 수 없다.
- 내부 망 사용자들의 모든 행위에 대해 정보자산 보호를 목적으로 로깅, 감시하거나 차단할 수 있다.
- 인터넷상에서 다운로드 되는 모든 소프트웨어와 파일들은 사용 전에 바이러스 탐지 도구로 검색 및 테스트 되어야 한다.
- 외부 네트워크에서 인터넷을 통하여 내부 네트워크로 접속하고자 하는 모든 사용자는 내부 네트워크로 접속하기 전에 침입차단시스템 또는 VPN과 같은 접근통제시스템에서 인증을 받아야 한다.
- 기밀 정보를 인터넷 등의 외부 네트워크를 통해 전송할 때에는 암호화하여야 한다.
- 인터넷상에서 암호화 등의 안전한 정보보호기술을 이용하지 않는 한 텔넷(telnet) 접속은 금지한다.
- 내부직원은 보안성이 확보되지 않은 장소에서 회사의 통신망에 접속해서는 안 된다.
- 원격 접속시스템과 내부망의 연결이 필요할 경우 접근통제 기능을 적용하여 제한된 서비스만을 사용할 수 있도록 통제되어야 한다.
- 원격 접속시스템의 사용자는 보안성 강화를 위하여 패스워드를 주기적으로 변경하여야 한다.

3.2. 네트워크 연결 통제

3.2.1. 외부로부터의 네트워크 실시간 접속

외부로부터의 회사 내부 네트워크 또는 정보시스템으로의 네트워크 접속은 모두 차단하는 것을 기본 원칙으로 한다. 다만, 내부 네트워크를 이용하기 위해서는 다음과 같은 보안 절차에 따라 접근을 허용하도록 통제한다.

- 내부 네트워크로의 접근은 가상사설망(VPN)을 통해 사용자 인증을 반드시 거치도록 한다.
- 정보보호시스템의 접근차단 정책을 허용해야 하는 경우, 책임자의 승인을 받아 필요한 서비스에 대해서만 접근을 허용하도록 명시적인 침입차단시스템 정책을 수립할 수 있다.

외부로부터 회사 내부 네트워크 또는 정보시스템으로의 네트워크 접속은 침입차단시스템 등의 부가적인 네트워크 접근통제 장치를 통해서만 이루어져야 한다.

3.2.2. 불필요한 네트워크 접속 금지

불필요한 통신장비나 네트워크 세그먼트는 모두 물리적으로 네트워크에서 분리시킨다.

3.2.3. 사용하지 않는 세션 차단

사용하지 않는 유휴 세션이 장시간 유지되지 않도록 최대 10분 이상 유지되는 세션은 자동으로 연결이 해제되어야 한다.

3.3. 장비 및 설정 관리

3.3.1. 네트워크 시스템 및 장비 보안

- 네트워크 장비는 도입 후 기본으로 제공되는 초기 값을 즉시 변경하여야 하며, 시스템의 설치 목적 기능을 제외한 모든 기능을 해제(불필요한 서비스 및 포트 제거)하고 필요시 책임자의 승인(보안성 검토)을 득한 후 적용한다.
- 네트워크 장비는 물리적으로 접근 통제할 수 있는 안전한 곳에 설치하며, 허가된 사용자 이외에 접근을 통제한다.
- 네트워크 보안장비의 소프트웨어는 안정성이 입증된 가장 안전한 버전을 사용하여야 하고, 모든 취약점이 제거된 이후에 네트워크와 연결한다.
- 네트워크 장비에 대한 원격접속은 허가된 내부 담당자 이외에 모두 통제한다.
- 네트워크 장비의 장애처리를 위하여 인터넷을 통한 외부인의 접근은 일체 불허하며 부득이한 경우 책임자의 승인을 득하여 허용한다.
- 장비에 할당된 IP 주소 및 환경정보, 구성도 등은 대외비 자료로 관리한다.
- 모든 통신 케이블 배선은 도청이나 손상으로부터 보호받을 수 있도록 지하 매설 또는 전용 관로를 이용하고 비인가자의 접근을 통제한다.
- 전원케이블과 통신케이블은 상호 간섭을 방지하기 위해 분리 설치한다.
- SNMP community는 RO(Read Only)만 설정하여 사용하는 것을 원칙으로 하되 필요시 책임자의 승인 후 에 RW(Read Write) community를 한시적으로 설정하여 사용할 수 있다.
- 시스템 원격 접속이 오랫동안 유지될 경우의 해킹 위험성을 제거하기 위한 connection time-out(3분 이내)을 설정하여 사용한다.
- 시스템 접속 시 비인가 접속을 경고 하는 안내 문구를 반드시 표시한다.
- 사용 중인 운영체제의 보안 취약점 및 버그 발견 시 관련 기관 또는 업체에 통보하여 적절한 운영체제로 신속히 업그레이드해야 한다.

3.3.2. 계정 및 사용자 권한관리

- 시스템 공급 시 제공되는 디폴트 ID 및 패스워드를 즉시 변경해야 한다.
- 모든 패스워드는 영문자/숫자를 조합하여 8자리 이상으로 한다.
- 패스워드는 최소 3개월 주기로 변경하여야 한다.
- 퇴직자, 계약해지자 등 무자격자 ID는 사유 발생 일에 즉시 삭제한다.
- 원격 접속시스템을 운영할 때는 사용자 인증, 패스워드 사용기준(자리 수, 변경주기, 사용기간 등) 및 사용기록 로깅 등 보안기능이 있는 제품을 사용한다.
- 사용자의 로그온 기록 및 사용이력은 로그 기록 후 3개월 이상 유지한다.
- 외부 제3자의 원격 또는 현장 작업 및 운영관련 업무 수행 후 사용된 계정은 즉시 삭제하거나 공용계정인 경우 패스워드를 즉시 변경한다.

3.4. 보안 패치 관리

3.4.1. 보안패치

- 보안패치는 각종 소프트웨어, 운영체제 등에서 발견되는 보안상의 취약성을 보완해주는 프로그램으로 새로운 취약성에 대한 보안패치가 발표되는 즉시 시스템에 적용하여 보안조치를 취함으로서 보안 사고를 사전에 예방할 수 있도록 한다.
  - 보안패치 정보를 주기적으로 입수하고 적용
  - 주요 보안패치에 대해서는 적용일 등 패치정보를 기록・관리
- 조직 내의 패치 적용 대상 시스템, 소프트웨어별로 보안패치 방법 및 절차를 정리하여 패치 적용 정보를 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 시스템에 사용되는 소프트웨어 목록 및 버전 정보 목록 관리
  - 각 소프트웨어 또는 시스템 제공업체 확인하여 최신버전 보안패치 목록 및 패치 방법 확인
  - 패치 설치 후 서버의 정상적인 운영상태 확인
- 기타 보안패치 관리 작업을 자동화 해주는 소프트웨어를 사용할 경우, 위 사항들을 만족하고 있는지 주기적으로 검토한다.

3.5. 백업 및 복구

3.5.1. 백업

- 서비스 제공 및 업무 수행과 직접적인 관계가 있는 주요정보는 물리적 재난이나 정보통신설비의 오류 발생으로 긴급 상황이 발생할 경우, 즉각적으로 복구할 수 있도록 주기적으로 백업을 수행하고 백업 매체를 안전한 곳에 보관하도록 한다.
- 위험분석 등의 방법을 통하여 자체적으로 중요도에 따라 관리가 필요한 주요정보를 식별하고 주요정보에 대한 백업 계획을 마련한다. 정보의 중요성 및 특성을 고려하여 백업의 방법 및 횟수 등의 백업 계획을 마련한다.

- 백업은 백업될 데이터의 성격에 따라 백업 시기, 백업주기, 백업방법, 백업데이터의 보관방식 및 보존기간 등을 포함하여 백업 담당자, 백업 및 복구 방법・절차・주기 등을 기록/관리 한다.

3.5.2. 복구

- 수립한 백업 및 복구 방법·절차는 다음과 같은 단계에 따라 수행되도록 한다.
  - 장애발생 상황인지 및 보고
  - 복구 우선순위의 결정
  - 사후 점검 및 원인분석
  - 장애 및 복구기록 유지관리 등
- 복구는 가장 믿을만한 백업매체를 사용해야 한다. 피해 시점 또는 문제발생 시점 이전의 백업본을 사용하도록 한다. 백업·복구의 관리를 위해 관리대장을 만들고 기록할 수 있도록 한다.

3.6. 트래픽 모니터링

네트워크 모니터링 도구를 이용하여 백본망 및 주요노드 구간, 외부망과 연결되는 주요회선에서 소통되는 트래픽을 24시간 모니터링 해야 한다.

3.6.1. 자체적으로 모니터링을 수행하는 경우

- 웹하드 서비스를 제공하는 네트워크 진입점(백본, 진입노드)에서 24시간 트래픽 모니터링을 수행하여야 한다.
- 모니터링 대상은 In-Bound, Out-Bound 트래픽을 모두 포함하여야 하며, 담당자를 지정하여 수행하여야 한다.
- 모니터링을 위한 도구(NMS, MRTG, NetFlow, Cflowd/arts++ 등)를 이용할 수 있다.

3.6.2. 모니터링을 위탁 운영하는 경우

- 모니터링 담당자는 위탁 운영 업체로부터 네트워크 트래픽에 대한 정기적인 보고를 받아야 한다.
- 모니터링 결과를 원격으로 확인 가능한 경우 담당자는 주기적(1일 1회)으로 네트워크 모니터링 결과를 확인하여야 한다.
- 이상 발생 시 위탁운영업체로부터 보고 받을 수 있는 체계를 마련하여야 한다.

3.7. 무선네트워크 보안

- 업무상 무선네트워크를 사용하는 경우 사용자 인증, 데이터 암호화 등 보안 조치를 마련하여 적용하여야 한다.
- 무선 네트워크의 사용은 허가된 임직원을 대상으로 하며, 외부인에게 제공할 경우 담당자의 허가를 득하여야 한다.

3.7.1. 사용자 인증 및 접근제어

- 무선 네트워크를 사용할 경우 아래와 같은 사용자 인증 및 접근제어를 위한 조치를 취하여야 한다.
  - 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅을 중지
  - 추측이 어려운 복잡한 SSID 및 네트워크 키(Key) 값을 사용

3.7.2. 데이터 암호화

- 일반적인 무선공유기에서 제공하는 보안기술은 아래의 표와 같으며, 안전한 WPA2을 사용하여야 한다.

구분	WEP (Wired Equvalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access2)
인증	사전 공유된 비밀 키 사용 (64비트, 128비트)	사전에 공유된 비밀 키를 사용하거나 별도의 인증 서버를 이용	사전에 공유된 비밀 키를 사용하거나 별도의 인증 서버를 이용
암호방법	고정 암호 키 사용 RC4 알고리즘 사용	암호 키 동적 변경(TKIP) RC4 알고리즘 사용	암호 키 동적 변경 AES 등 강력한 암호 알고리즘 사용
보안성	가장 취약하여 널리 사용되지 않음	WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	가장 강력한 보안기능 제공

- 업무 환경에 따라 필요 시 모바일 용 VPN을 사용할 수 있다.

3.7.3. 무선 네트워크 장치 관리

- 무선 네트워크의 사용을 위한 장치는 연 1회 이상 보안 조치에 대한 점검을 수행하여야 하고, 그 기록을 유지·관리하여야 한다.
- 무선 네트워크 장치는 월 1회 이상 펌웨어의 업데이트 유무를 확인하고, 안정성 유지를 위하여 최신의 펌웨어로 유지·관리하여야 한다.

3.8. 라우터(Router) /스위치 보안

3.8.1. 접근제어

- 콘솔을 통한 라우터/스위치 접근을 차단하기 위해 라우터가 설치된 랙은 잠금장치를 하거나 물리적인 접근통제가 실시되는 곳에 설치하여야 한다.
- 라우터/스위치를 이용한 원격지 접근을 차단하기 위해 터미널 접근에 대한 접근제어 목록을 운영하거나 대체 수단을 강구하여 운용자를 제외한 다른 사용자의 원격지 접근을 차단하여야 한다.
- 라우터/스위치 운용자의 사용이력을 로깅 하여야 하며, 강화된 인증 및 중앙 집중적 사용자 관리를 위해 인증시스템을 운영할 수도 있다.
- 라우터/스위치 접근에 사용되는 모든 패스워드는 패스워드 관련 규정을 준수 하여야 한다.

- 예방점검 및 장비장애로 인해 외부 엔지니어의 라우터 접근이 필요할 경우에는 담당자가 동행하여 업무를 수행한다.
- 네트워크의 운영 상태만을 조회하는 사용자에게는 구성 변경이 불가능 하도록 낮은 등급의 접근 권한을 부여하여야 한다.

3.8.2. 라우팅 정보관리

- 라우터/스위치의 라우팅 테이블은 주기적으로 점검하여 비인가된 라우팅 정보나 불필요한 라우팅 정보를 감시 및 삭제하여야 한다.
- 외부 네트워크와 특별히 라우팅 테이블 교환이 불필요한 경우에는 가능하면 정적 (Static) 라우팅을 사용한다.
- 모든 라우터/스위치에는 IP스푸핑 공격을 가능하게 해주는 소스 라우팅 기능을 업무에 필요에 의한 경우를 제외하고는 모두 제거하여야 한다. 부득이 소스 라우팅 기능을 사용해야하는 경우 IP스푸핑 공격을 무력화 시킬 수 있는 대체 방어 수단이 적용되어야 한다.

3.8.3. 라우터/스위치의 보안설정

- 패스워드는 암호화하여 저장되도록 환경을 설정하며, SNMP 읽기 모드와 쓰기 모드의 패스워드를 동일하게 사용하지 않는다.
- 패스워드는 최소 3개월을 주기로 변경하여야 한다.
- SNMP Community String으로 기본적으로 제공되는 Public이나 Private을 사용해서는 안되며, SNMP 권한은 특별한 경우를 제외하고는 Read-Only로 운영하도록 한다. 또한 SNMP는 ACL을 적용하여 서비스 접근을 제한한다.
- 특별한 경우를 제외하고 라우터/스위치에서 Directed Broadcast 및 ICMP Redirect 기능을 제거한다.
- Banner에 보안 경고를 설정한다. 라우터 관련 정보는 나타내지 않아야 한다.
- 라우터/스위치 운영에 불필요한 모든 서비스를 제거하여야 한다. (Cisco Discovery Protocol, Tcp Udp Small 서비스, Http, R-Service, Finger, CDP, Proxy ARP, Bootp 등)
- 유해 트래픽으로 네트워크 장애가 발생할 경우 침해/장애대응 프로세스에 따라 적절하게 대응하여야 한다.

3.8.4. 로그관리

- 라우터 및 스위치 장비의 인증 로그, 자산목록에 의해 발생된 로그는 별도 로그 서버에 저장하며 해당 로그는 3개월 이상 보관하여야 한다.
- 발생된 로그는 실시간으로 모니터링 하며, 실시간으로 로그를 수집/보관하여야 한다.

※ 관련 서식은 “[별첨 8] 네트워크 장비 설정/로그 백업 관리대장”을 참조

3.8.5. 유지관리

- 라우터의 가용성 보장을 위해 유지보수를 수행하며, 정기점검을 실시하여야 한다.
- 네트워크 운용자는 라우터의 안정적인 운영을 위해 최신 운영체제 중 가장 안전한 버전을 사용해야 하며, 새로운 운영체제 적용 시에는 모든 보안취약점을 제거해야 한다.
- 유지보수 수행으로 인해 보안의 허점이 발생하지 않도록 해야 하며, 유지보수를 위해 방문하는 외부 인력은 사전 승인된 인력이어야 한다.
- 유지보수 계약을 체결하지 않는 경우에는 자체적으로 주기적인 점검을 수행하여 그 기록을 남긴다.

IV. 웹, DNS, DHCP 서버 보안

1. 일반사항

1.1. 목적

웹서버 및 DNS, DHCP, DB 서버의 안전한 운영을 위해 필요한 지침을 제공하는데 그 목적이 있다.

2. 웹서버 보안

2.1. 웹서버 구축

- 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 웹서버에서 사용되는 어플리케이션에 대한 새로운 업데이트 및 보안 패치를 확인하도록 한다.

- 단독 목적의 웹 서버 사용
  웹서버 관리자는 반드시 웹 서비스만을 위한 단독 서버를 구축하여 운영 하여야 한다. 하나의 시스템에 웹서버, 메일서버, DNS 서버, 데이터베이스 서버를 운영하는 경우가 있는데 이는 웹서버를 포함하여 데이터베이스 서버 까지도 위험하게 한다. 일반적으로 하나의 서비스가 추가될 때마다 그만큼 더 위협이 증가하게 된다.
  특히, 중요한 정보를 다루는 데이터베이스 서버의 경우 웹서버와 분리하여 서로 다른 시스템에서 운영하도록 한다.

- 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.
- 침입차단시스템(Firewall) 사용
  라우터와 침입차단시스템을 이용하여 DMZ 구간 네트워크를 구성한다. 그리고 웹서버를 비롯한 일반 인터넷 서비스를 제공하는 시스템을 이곳에 설치하도록 한다. 이 경우 웹서버를 포함하여 DMZ 구간의 시스템에서 중요 내부 서버나 네트워크로 접속하지 못하도록 접근제어를 하도록 한다. 특히 접근제어의 경우 외부에서 내부로의 접근제어와 내부에서 외부로의 접근제어가 모두 구현되도록 한다.
  이는 만약의 경우, 웹서버가 해킹을 당할 경우에 공격자가 웹서버를 통하여 또 다른 서버나 내부 시스템으로 침입을 하지 못하도록 하는데 목적이 있다.

- 원격 접근 제한
  웹서버 관리의 편리성을 위해 관리자는 종종 콘솔을 이용하기보다는 원격지에서 웹서버로 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.

- 웹 트랜잭션 보안

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

2.2. 웹서버 운영

- 새로운 보안 취약점에 대한 모니터링 및 적용

  웹서버와 관련된 신규 취약점 정보, 웹 어플리케이션과 관련된 신규 취약점 정보를 지속적으로 모니터링 한다. 새로운 취약점이 발표되면 바로 웹서버에 적용하도록 한다. 알려진 취약점에 대해서는 유관기관의 웹 보안 취약점관리 방안을 따른다.

- 주기적인 로그 점검
  웹 서버 로그와 운영체제 로그를 주기적(월 1회 이상)으로 점검하여 침입, 침입시도, 또는 보안 문제점을 발견하도록 한다.

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

※ 관련 양식 [별첨 4] 백업 관리 보고서 참조

3. DNS 서버 보안

3.1. DNS 서버 구축

- 소프트웨어 업그레이드 및 패치 설치
  운영체계를 포함한 최신 버전의 DNS 서버를 설치하고 보안과 관련된 모든 패치를 설치하여야 한다.

- DNS 서버 보안 설정
  DNS 서버에 대한 각종 오남용을 예방하기 위하여 다음과 같은 보안설정을 하도록 한다.

- DNS spoofing 방지(no recursion 설정)
- Zone Transper 제한
- DNS 서버는 내부용으로만 제한하여 과도한 정보 유출 방지
- 백업용 DNS 서버 운영

- 침입차단시스템(Firewall) 사용
  라우터와 침입차단시스템을 이용하여 구성한 DMZ 구간 네트워크에 DNS 서버를 설치한다. 그리고 다음과 같은 사항의 접근제어를 하도록 한다.
  - 내부 네트워크, 외부 네트워크로부터 DNS 서버로의 비 인가된 접근을 통제한다.
  - DNS 서버로부터 중요 내부 서버나 네트워크로 비 인간된 접근을 통제한다.

3.2. DNS 서버 운영

- DNS 서버 설정파일 백업
  DNS 서버 장애로 인하여 시스템의 복구가 필요한 경우를 위해서 DNS 설정파일에 대한 백업을 주기적으로 실시하도록 한다.

※ 관련 양식 참조

- DNS 서버 과부하 대책 마련
  DNS 서버의 오남용 공격 또는 과도한 질의로 인한 장애에 대비하기 위하여 주기적으로 DNS 서버의 CPU, 메모리, 네트워크 트래픽 량 등에 대해서 모니터링 하도록 한다. 가능한 경우 1차, 2차 DNS 서버로 구성하여 운영하고, 부하분산 대책을 사용하도록 한다.

- 새로운 보안 취약점에 대한 모니터링 및 적용
  DNS 서버와 관련된 신규 취약점 정보를 지속적으로 모니터링 한다. 새로운 취약점이 발표되면 가능한 빠르게 DNS 서버에 적용하도록 한다.

- 주기적인 로그 점검
  DNS 서버 로그와 운영체제 로그를 주기적(월 1회 이상)으로 점검하여 침입, 침입시도, 또는 보안 문제점을 발견하도록 한다.

4. DHCP 서버 보안

4.1. DHCP 서버 운영

- DHCP서버에 문제가 발생할 경우 DHCP를 이용하는 인터넷 접속서비스에 큰 불편을 야기할 수 있으므로 아래와 같은 보안대책을 적용하여 가용성과 기밀성을 확보하고 시스템 과부하에 대비하여야 한다.
  - 과부하에 대비한 부하분산 대책을 마련
  - 설정파일 백업 실시

- IP 할당 상황 등에 대한 로그기록 유지・관리

• DHCP 서버의 용량 및 사용도 등을 주기적으로 측정하여야 한다.
  - 월 1회 이상 DHCP 서버의 용량 및 사용도 등을 측정하여야 한다.
  - DNS 서버의 용량 및 사용도 측정은 DHCP 서버 CPU 부하량, 메모리 사용량, 트래픽량 등의 성능을 모니터링하여 확인하여야 한다.

• DHCP 서버의 부하분산 방안을 수립하여 적용하여야 한다.
  - DHCP 서버의 과부하에 대비하고 가용성을 확보하기 위한 부하분산 방안을 적용하여야 한다.
  - 부하분산 방안으로 로드밸런싱 및 이중구조의 사용, 공개된 외부 DHCP 서버의 사용 등의 방안이 적용되어야 한다.

• DHCP 서버의 환경변수 설정 및 설정 파일 정보에 대한 기록을 정기적으로 백업하여야 한다.
  - DHCP서버의 핵심 서비스는 DHCP서버를 사용하여 IP 주소 및 관련된 기타 세부구성 정보(서브넷 마스크(subnet mask), 게이트웨이(gateway), DNS 주소 등)를 DHCP사용자에게 동적으로 할당하는 서비스를 제공하는 것으로 필요한 환경변수 설정 및 설정파일에 대한 정보 기록이 유지・관리될 수 있도록 주기적으로 백업을 수행하여야 한다.
  - DHCP사용자에 대한 IP 주소 할당 정보를 가지고 있는 DB를 주기적으로 백업하여야 한다.
• DHCP 서버의 감사로그 기능을 활성화하여 사용자별 할당된 IP 주소, Mac 주소, 사용시간 등을 로깅하여야 한다.
  - 시스템 오동작, 침해사고, 서비스 이용 내역 분석 등을 위하여 DHCP서비스 이용에 대한 정보가 유지될 수 있도록 감사 로그(audit log)와 로그(log) 추적 기능을 활성화하여 운영하여야 한다.
  - 침해사고 발생 시 추적이 용이하도록 DHCP서버의 감사 로그 기능을 활성화하여 시간대, MAC주소, 사용자 별로 할당한 IP 주소를 기록・관리하여야 한다.

V. DBMS 보안

1. 일반사항

1.1. 목적

DBMS에 대한 다양한 보안 위협 및 취약성으로부터 안전하게 보호하고, 운용 관리 하는데 그 목적이 있다.

2. DBMS 운영 시 보안

2.1. DBMS 서버 구축

- DB서버는 외부로부터의 직접 접속을 차단하기 위하여 침입차단시스템 내부에 설치하며, 특히 웹서버가 위치한 구역으로부터 분리 설치되어야 한다.
- 성능과 용량을 충분히 확보하도록 하고 불필요한 서비스를 제거하고 운영 하도록 한다.

2.2. DBMS 운영 관리

2.2.1. 사용자 인증

1) 계정과 패스워드를 통한 시스템 접근

- DB에 계정을 가진 사용자들은 반드시 ID와 패스워드를 사용하도록 하며 주기적으로 패스워드를 변경하도록 한다.
- 매우 중요한 데이터를 저장하고 있는 DB는 토큰이나 암호화된 ID와 패스워드 또는 생체인식 등을 이용한 강화된 사용자 인증 방법을 사용할 수 있을 것이다.

2) 자동 로그오프

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

3) DBMS 로그인 화면 관리

- 로그인 화면은 반드시 필요한 로그인 관련 정보만 표시해야 한다.
- 회사나, 시스템 운영체제, 네트워크 환경, 내부적인 사항과 같은 정보는 성공적인 로그인 후에 표시 되어야 한다.

2.2.2. 권한 관리

1) 사용자 추가

- DBMS ID가 필요한 사용자는 담당자에게 “[별첨 5] DBMS ID(생성/변경/삭제) 신청서”를 작성하여 ID 생성/변경/삭제 신청 승인을 받아야 한다.
- 담당자는 신청서를 참조하여 ID 및 패스워드를 부여한다.
- 담당자는 발행한 ID 내역을 “[별첨 6] 데이터베이스 권한 부여 관리대장”에 기록 하도록 한다.

2) 접근 권한 변경 절차

- DB에 대한 접근권한 변경이 필요할 경우 담당자로부터의 승인을 득하기 위해 “[별첨 5] DBMS ID(생성/변경/삭제) 신청서”를 작성한다.
- 승인 후 담당자는 신청서의 요청 양식에 따라 접근 권한을 부여하고 “[별첨 6] 데이터베이스 권한 부여 관리대장”에 기록 하도록 한다.

3) 사용자 삭제 절차

- 사용자의 이직·퇴직·발령 등 인사이동 사항이 통보되거나 외주 업무가 종료되는 경우 이를 담당자에게 통보해야 한다.
- 이직·퇴직·발령 등 인한 인사이동을 통보 받은 담당자는 ID삭제의 적합성을 검토하도록 한다.
- ID삭제 검토가 완료된 사용자에 대해서 DBMS 내의 계정을 삭제하고 “[별첨 6] 데이터베이스 권한 부여 관리대장”에서 삭제 하여야 한다.

4) 불법 행위에 따른 접근권한의 취소

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

5) 사용자 권한의 주기적 재평가

- 사용자에게 부여된 권한은 주기적으로 재평가하여 책임자의 승인을 받는다. 이를 위해 담당자는 “[별첨 6] 데이터베이스 권한 부여 관리대장”을 통해 권한 목록을 관리한다.

6) 사용자 임무 변경 통보

- 각 팀 책임자는 해당 내부직원의 업무나 업무환경 변화에 따른 ID 및 권한의 변경을 담당자는 즉시 반영하여 관리한다.

7) DBMS 및 응용시스템 담당자의 권한 제한

- 실 운영 DB의 백업 등의 단순한 업무를 정해진 절차에 의해 수행하는 DB 관리시스템의 담당자나 응용시스템의 담당자에게는 직무수행을 위해 필요한 권한 이상의 접근권한을 부여하지 않는다.

8) 응용시스템 개발자의 실 운영 정보 접근 제한

- 운영 단계의 실 운영 시스템 DB에 대해, 응용시스템 개발자는 개발중인 응용시스템의 테스트 시 개발과 관련된 실 운영 정보 이외 가능한 한 접근할 수 없도록 해야 하며 권한 부여시는 최소한의 권한만 부여되어야 한다. 테스트 완료 후 해당 권한을 즉시 취소한다.

9) 실 운영 정보의 직접 수정 금지

- 실 운영 시스템의 DB 데이터의 수정은 정상적인 인증방법 외의 방법을 통한 직접 수정을 절대 금해야 한다. 단, 필요시는 수립된 절차에 따라 인가된 사람에 의해 책임자의 승인 하에 이루어져야 한다.

10) 응용시스템을 통한 실 운영 정보의 수정

- 개발자나 담당자를 포함한 모든 DB사용자는 적합한 절차를 거치지 않고는 실 운영 정보를 수정할 수 없어야 한다.

2.3. DBMS 접근 통제

2.3.1. DB의 시스템 파일에 대한 변경 권한과 접근통제

DBMS 설치 소프트웨어 라이브러리 또는 DB의 운영체제 파일(데이터 파일, 환경구성 파일, 로그 파일 등)을 변경할 수 있는 권한은 담당자만이 가지고 있어야 하며 이를 위해 별도의 디렉터리를 지정 보관해야 한다.

2.3.2. 여러 장소에서의 다중 접속 제한

하나의 DB 계정을 이용하여 여러 터미널(장소)에서 동시에 다수의 온라인 세션을 연결해서는 안 된다.

2.3.3. 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.

2.4. DBMS 보안 관리

2.4.1. 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.

2.4.2. DB의 암호화

데이터의 유형과 비밀성에 따라 개인정보 및 기밀정보인 경우 데이터는 가능한 암호화하여 보관해야 한다.

2.5. 감사 추적성 확보를 위한 로깅

2.5.1. 로그 기록

1) 기밀정보를 저장하는 DB의 로그 기록

비밀 정보를 저장하고 있는 DB는 비밀 정보의 추가, 수정, 삭제와 관련된 사용자 ID의 변경 전·후의 데이터 등에 대해 감사를 수행 하여야 한다.

2) 감사에 필요한 보안 사항의 로그 기록

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

3) 담당자에 대한 로그 기록

담당자의 활동에 대한 로그기록을 남기도록 한다.

2.5.2. 로그 기록의 관리

1) 로그의 정기적 검토 및 보고

보안 침해 예방 활동을 위해 담당자는 정기적으로 보안관련 로그 기록을 검토하고 이상 발견 시 책임자에게 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) 로그 기록 공개 제한

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

2.5.3. 보안위반 사건의 사용자 통보

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

2.5.4. 승인에 따른 로그 접근 인가

책임자의 사전 승인이 없는 한 사용자의 DB 접근에 관한 모든 로그 기록은 비인가자가 접근할 수 없어야 한다.

2.5.5. 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.

2.6. 복구를 위한 DBMS 로그 기록

2.6.1. DBMS의 로그 기능 설치

DBMS는 필수적으로 시스템 복구를 위한 로그 기능을 적용하여야 한다.

2.6.2. 실 운영 정보의 변경에 대한 복원

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

2.6.3. 로그파일의 백업

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

2.6.4. 로그파일 모니터링

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

2.7. 백업 절차

2.7.1. 데이터별 백업에 대한 규정의 문서화

데이터가 상실/파괴 되었을 때, 이를 복구하기 위해 데이터별 정기적인 백업이 이루어져야 하며 백업에 대해 다음 사항들이 문서화되어 최신의 정보로 유지되어야 한다.

- 백업 대상(테이블스페이스, 테이블, 도는 로그 기록 파일 등)
- 백업 주기
- 백업 수행시간
- 백업 수행방법
- 백업파일의 명명규칙

2.7.2. 기밀정보의 백업주기

장애로부터 중요 데이터와 소프트웨어를 보호하기 위해 가능한 자주 정규적인 백업이 시행되어야 한다.

2.7.3. 백업본의 원격지(OFF-SITE) 보관

백업본은 재난으로 인한 손실에서 벗어날 수 있도록 원본과 물리적으로 충분히 떨어진 장소에 보관하여야 하며, 물리적으로 비인가자의 접근이 통제되어야 한다.

2.7.4. 원격지(OFF-SITE)에 저장된 정보의 디렉터리 관리

원격 저장소에 보관되어 있는 백업파일은 백업일자 목록을 유지/관리 한다.

2.8. 복구 절차

2.8.1. 복구계획의 수립

자연재해, 사고, 설비상의 문제, 고의적인 행위, 서비스 제공의 손실, 유용성의 손실로부터 초래되는 IT 서비스 중단 위협을 최소화하기 위해 DBMS와 DB의 복구 계획을 수립한다.

2.8.2. 복구 우선순위에 따른 정보자원의 분류

담당자는 비상사태에 대비하여 데이터베이스의 복구순위를 수립하고, 이의 적합성을 주기적으로 평가하여야 한다. 특히 중요한 테이블의 목록을 정리하여 그 복구우선 순위를 정하는 것이 중요하다.

2.8.3. 복구 전 DB 백업

DB 복구상황이 발생할 경우 복구 작업을 수행하기 전 상황의 DB에 대한 백업이 이루어져야 한다. 이는 복구 실패에 대한 정보의 손실을 최소화하기 위해 필요하다.

VI. 정보보호시스템 보안

1. 일반사항

1.1. 목적

침입차단시스템(Firewall), 침입방지시스템(IPS), 가상 사설망(VPN), 서버보안 (SecureOS), 웹방화벽, 통합관제시스템, 종합분석시스템 등의 정보보호시스템의 운영 및 관리를 위한 보안 요구사항을 정의함으로써, 효과적인 정보보호시스템 운영을 통해 실수나 고의로 외부 네트워크로부터 내부 시스템 및 데이터 등의 자원에 접근하여 정보의 유출, 손상, 파괴 등 일련의 불법적 행위를 방어하고 탐지하는데 그 목적이 있다.

1.2. 운영 관리

1.2.1. 정보보호 시스템 도입 및 운영

- 외부망과 연계되는 구간에는 침입차단시스템, 침입탐지시스템 등 네트워크의 안전성을 제고할 수 있는 정보보호시스템을 설치·운영하여야 한다.
- 또한, 운영 중인 웹 서버를 보호하기 위한 웹방화벽 또는 웹쉘탐지제품을 설치·운영하여야 하며, 최신의 패턴에 대한 업데이트를 실시하여야 한다.
- 정보보호시스템은 적절한 접근제어 및 탐지 정책을 반영하고 설정에 대한 현황을 관리하여야 한다.
- 정보보호시스템은 이상 징후 탐지 시 관리자에게 이메일, SNS, 경보 등 가용한 수단을 사용하여 실시간 통보하도록 설정하여 운영하여야 한다.
- 인터넷망에서 내부망으로의 접근은 모두 차단하여야 하며, 웹 서버, 백업서버, 관리자의 접근만 허용하여야 한다.
- 정보보호시스템 담당자는 정보보호시스템의 하드웨어 및 소프트웨어의 지속적인 가용성과 무결성 확보를 위해 정기적(월 1회) 혹은 필요한 경우 수시로 예방점검을 한다.
- 사후 추적성을 높이기 위해 모든 정보보호시스템의 시간을 시간서버와 동기화 설정을 하도록 한다. 다만, 시간 서버와 시간 동기화에 필요한 네트워크 연결이 불가한 시스템은 담당자에 의해 수시로 시간서버와의 동기화 적용을 하도록 한다.

1.2.2. 정보보호 모니터링

주요시스템・네트워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지 확인하기 위해 모니터링 시스템 구축 또는 위탁운영을 통하여 침해사고 탐지・대응 체계를 구축하여야 한다.

- 정보보호시스템의 운영절차를 수립하여야 한다.
  - 정보보호시스템(방화벽, 웹방화벽, 웹쉘탐지제품 등) 운영을 위한 지침 또는 운영절차를 수립하여야 한다.
  - 정보보호시스템을 위탁 운영하는 경우 위탁운영에 대한 지침이 포함되어야 한다.

- 정보보호시스템의 성능 및 용량 등 운영 현황을 지속적으로 모니터링 하기위한 절차를 수립・이행 하여야 한다.
  - 정보보호시스템의 유지보수 및 운영 현황 모니터링을 위한 절차를 마련하여야 하고, 사용자 수 및 트래픽 양의 변화를 모니터링하여 적절한 성능을 지원하는 제품을 사용하여야 한다.
  - 최소 월 1회 이상 정보보호시스템의 하드웨어 자원에 대한 성능을 모니터링 하여야 한다.

- 이상 징후를 지체 없이 인지할 수 있도록 모니터링 체계 및 절차를 수립하여야 한다.
  - 자체적인 모니터링 체계를 구축하여 운영하는 경우 모니터링 요원, 모니터링 시스템, 모니터링 절차를 포함한 지침을 마련하여야 한다.
  - 이상 징후 발생 시 대응할 수 있도록 담당자 및 책임자를 지정하고 각 담당자의 역할 및 책임을 정의하여야 한다.
  - 이상 징후 조치 후 재발방지를 위한 조치를 취하기 위한 대책을 마련하여야 한다.

1.2.3. 주기적 점검

- 정보보호시스템 보안기능(비정상 트래픽 차단 등)의 정상 작동 여부를 주기적(월 1회 이상)으로 점검 한다.
- 통신망 장애에 대비하여 특정 트래픽 차단 기능, 불필요한 서비스에 대한 차단 정책, 네트워크 보안 설정, 암호화 등 보안 기능에 대한 정상 작동 유무를 주기적(월 1회 이상)으로 점검한다.
  - 위탁 운영을 하는 경우 주기적인 보고를 받을 수 있도록 해당 내용을 계약 또는 협약서의 내용에 포함하여야 하고, 위탁 운영 업체 및 유관기관과의 연락체계가 갖추어져 있어야 한다.

2. 침입차단시스템 보안 관리

2.1. 보안 정책

- 침입차단시스템 구성 시 서버의 등급 분류와 현재 내부에서 사용하고 있는 네트워크도 보안등급에 맞게 적절히 분류가 이루어져야 한다.
- 침입차단시스템을 이용해서 내부의 네트워크를 적절한 보안등급으로 나누어서 구성하고, 시스템의 보안등급에 따라 적절한 위치에 시스템을 배치해야 한다.

2.2. 운영 관리

2.2.1. 서비스별 정책(Rule) 설정

- 침입차단시스템이 지원하는 특성을 최대한 활용하여 각 인터넷 서비스별 접근제어 규칙을 정의해야 한다. 접근규칙 정의방법은 기본적으로 인터넷 서비스들이 가지고 있는 발신지/수신지 주소, 발신지/수신지 포트를 이용하여 패킷 필터링한다.
- 예를 들면 가능한 아웃바운드 정책은 차단으로 관리하며 필요시 오픈한다. 또한 외부자의 관리 목적의 원격 내부 접근 (Telnet, 원격 데스크탑 서비스 등)은 원칙적으로 불허하며

필요시 방문 작업을 원칙으로 한다.

- 외부자의 관리 또는 개발을 목적으로 하는 원격 내부 접근이 필요한 경우 내부 시스템의 보안을 유지하기 위하여 반드시 담당자의 승인을 거쳐 야 한다.
- 원격 접근 시 주간 접근 허용을 기본으로 하며, 야간 접근이 필요한 경우 사용시간의 기재 후 접속을 신청한다.
- 접근차단 정책은 침입차단시스템의 용량과 한계 그리고 IP통신의 약점과 위협에 대한 충분한 고려 하에 설계 되어야 한다. 침입차단시스템은 일반적으로 아래의 기본 정책을 적용 한다.

명백히 허용되지 않은 모든 서비스는 접근을 거부 한다.

- 위 정책은 기본적으로 모든 정책을 거부하고 필요한 서비스에 대해서만 접근을 허용하는 기본 정책으로, 정보보안의 모든 영역에서 전통적인 접근 모델로 쓰이고 있다.

- 정책 설계를 하는 사람은 아래 사항을 반드시 고려해야 한다.
  - 어떤 인터넷 서비스를 사용할 예정인가?
  - 서비스가 사용되는 위치가 어디인가?
  - 암호화 또는 다이얼 업과 같은 요구가 발생하는가? 또 이를 지원해야 하는가?
  - 이런 서비스와 접근을 제공할 때 어떤 위험이 따르는가?
  - 네트워크의 유용함을 통제하고 제한하는 것과 보호하는데 드는 비용은?
  - 보안과 유용성간에 어떤 합의가 도출되어 있는가?

- 네트워크로 연결된 사용하지 않는 TCP 유휴 세션이 장시간 유지되지 않도록 최대 10분 이상 유지되는 TCP 세션은 강제로 연결을 해제 하도록 한다. 다만, 네트워크담당자와 충분한 협의를 거쳐 지속적인 세션 연결 유지를 필요로 하는 서비스에 대해서는 예외 적용을 하도록 한다.

2.2.2. 보안정책 등록/변경 절차

- 보안정책 등록
  외부에서 침입차단시스템을 경유하여 내부의 자원에 접근하려는 보안정책의 변경이 요구되어지면 다음 절차를 거쳐야 한다.
  - 관리 담당자는 “[별첨 3] 보안정책 변경 요청서”를 작성한다.
  - 관리 담당자는 결재를 득한 후 보안 정책의 설정을 실행하고 변경된 결과를 저장한다.
  - 책임자는 “[별첨 3] 보안정책 변경 요청서”에 대해서 내부 및 외부의 불법적인 또는 불필요한 접속을 차단하기 위하여 서비스 정책에 대하여 검토한 후 적정한 경우 승인한다.

- 보안정책 변경
  - 서비스의 내용 변경으로 인해 보안정책을 변경할 경우 침입차단시스템 “[별첨 3] 보안정책 변경 요청서”를 작성한다.
  - 승인절차는 등록절차에 준한다.

- 보안정책 폐지
  - 별다른 통보가 없을 경우 담당자는 사용 기간이 만료된 정책에 대해서는 침입차단시스템의 정책 목록에서 삭제 또는 중지한다.
  - 요청기한 이전에 서비스가 불필요해진 경우 요청자는 반드시 보안정책 폐지를 요청하여야 한다.

2.2.3. 보안 정책 검증

- 일반적으로 정책의 검증은 정책에 의거한 보안시스템의 변화와 시스템이 구축된 환경의 변화, 상위 정책의 변화, 보안 침해사고 등에 의하여 요구된다.
- 정기적인 보안정책 검증을 수행하고 불필요하거나 기존 정책 중 수정이 필요한 부분을 확인하여 지속적인 관리를 수행한다.

· 네트워크의 규모가 확장 또는 변경될 때	· 네트워크 보안 담당자의 교체시
· 네트워크 트래픽이 변화할 경우	· 침입차단시스템의 업그레이드시
· 필터링 규칙의 재조정시	· 네트워크 시스템을 감사할 때
· 상위 정책이 변화할 때	· 신규 시스템이 가동될때
· 설치된 침입차단 기술이 낙후된 것일 때	· 보안 침해사례가 리포트될 때

· 회사 전체 혹은 부분이 사용할 새로운 네트워크 서비스가 적용될 때

2.2.4. 로그관리

- 내부에 접속하는 침입시도는 반드시 로그가 남도록 해야 하며, 로그는 다음의 사항이 포함되도록 한다.
  - 로그의 시작과 종료
  - 출발지/목적지 IP, 프로토콜, 포트(서비스), Action
  - 불법적인 침입시도
  - 침입차단시스템의 구성파일 및 로그파일에 대한 모든 접근
  - 침입차단시스템 정지와 재기동
- 로그는 주기적으로 분석하고 특이사항 발생 시 내용을 분석 및 검토하여 적절한 조치 후 그 내역 및 결과를 기록 하도록 한다.
- 시스템의 로그는 1주일 단위로 백업을 받고 대장에 기록한다.
- 로그는 용량 도달 시 수동 디스크 또는 테이프 백업이 수행될 수 있도록 한다.
- 백업된 로그의 보관주기는 3개월 이상으로 한다.

※ 관련 서식은 “[별첨 9] 정보보호시스템 장비 설정/로그 백업 관리대장”을 참조

2.2.5. 관리자 접근 경로 통제

- 담당자는 시스템 관리자, 네트워크 관리자 등 관리자 권한을 가진 사용자를 지정하고 관리하도록 한다.

- 관리자 권한을 가진 사용자는 침입차단시스템의 정책을 이용하여 내부의 지정된 특정 위치에서, 특정 경로를 통해서만 접속이 가능하도록 통제한다.
- 관리자 권한을 가진 사용자의 모든 행동은 가능한 한 시스템에 기록되고 모니터링 하도록 한다.
- 관리자 권한을 가진 사용자의 외부 네트워크로부터의 접근은 담당자가 허용하는 범위를 제외한 그 어떠한 경우라도 모두 차단 되도록 한다.

3. 침입방지시스템 보안 관리

3.1. 보안 정책

침입방지시스템을 구성하고자 하는 데에 있어서 중요한 기준 또한 보안정책이며, 정책에 따라 기술적으로 지원하는 제품을 선정 할 수도 있다.

- 일반적인 보안 목표(무결성, 기밀성, 가용성) 뿐 아니라 보다 일반적인 관리 목표(개인정보보호, 장애에 대한 보호, 관리효율성)을 고려하면 명확한 목표를 설정한다.

- 각 기능에 요구되는 데이터 및 네트워크에 접근하는 내용 뿐 아니라 시스템 사용자의 일반적인 업무 기능(단일 사용자에게 할당된 일반적인 기능들)을 조사한다.

- 정책이 위반된 것을 침입방지시스템이 방지하였을 때, 회사의 명백한 처리 및 대응 방안이 필요하다. 침입방지시스템의 운영자는 적극적으로 경보를 다루기 위하여 회사의 대응 정책을 숙지하여야 한다.

3.2. 운영 관리

3.2.1. 구성

침입방지시스템을 배치하는 데에 있어서 담당자들이 경험을 쌓고 모니터링과 유지보수를 위하여 얼마나 많은 자원이 필요한지 고려하여 전략을 수립하여야 한다. 자원은 다양한 침입방지시스템의 특성을 고려하여 시스템 환경에 맞도록 설정하는 데에 필요하다.

우선 일반적으로 설치 및 유지가 간편한 네트워크 기반 침입방지시스템을 사용하는 데에 있어서 효과적인 배치를 위한 전략을 수립하여야 한다.

3.2.2. 배치

네트워크 기반 침입방지시스템을 배치할 때 발생되는 문제는 시스템 센서를 어디에 위치시켜야 하는지 찾아내는 것이다. 각각의 위치에 따라 다른 장점을 가질 수 있으며 네트워크 기반 침입방지시스템을 위치시키는 데에 많은 옵션이 있다.

- DMZ 네트워크의 각 외부 방화벽 뒤 위치
- 외부 방화벽의 바깥쪽 위치
- 중요 네트워크 백본 위치
- 중요 네트워크 서브넷 위치

3.2.3. 이벤트 경보 운영 관리

결과적으로 침입방지시스템이 배치되고 나면 어떠한 형태의 경보를 사용하고 언제 중요한 이슈를 다룰 것인가에 대한 문제점에 부딪히게 된다. 대부분의 침입방지시스템은 경보 설정에 있어 매우 다양한 옵션을 가지고 있다. 예를 들어 전자메일, 무선 호출, 네트워크 관리 프로토콜 트랩, 공격 원천주소에 대한 자동차단 등이 있다.

비록 이러한 특징이 주의를 끌 수 있지만 주어진 환경 안에서 안정된 침입방지시스템의 설치와 동작이 안정화 될 때 까지 보수적인 관점에서 사용하는 것이 중요하다. 몇 몇 전문가는 침입방지시스템의 설치 후에, 수개월이 지난 후에나 경보 기능을 활성화 할 것을 권장하고 있다.

경보가 발생되었을 때 자동적으로 공격에 대응하는 기능이 포함되어 있을 경우(특히 침입방지시스템이 직접 방화벽과 연동되어 공격 소스에 대한 트래픽을 차단하는 방법을 사용할 때) 공격자의 위장 혹은 남용에 의해 합법적인 사용자의 접근이 거부되는 등의 피해가 발생되지 않도록 각별한 주의가 필요하다.

3.2.4. 공격이벤트 대응 관리

사고 대응 계획 및 절차를 가지고 있으며, 바이러스, 시스템의 내부자 남용, 그리고 해킹과 같은 회사의 보안 사고를 취급하는 절차를 포함한다.

이 사고 대응 계획 및 절차는 유관 부서에 대해 최소한의 역할과 책임을 할당하며 사고가 발생되었을 때 취할 행동에 대하여 명시하고, 사고 대응 절차에 따라 모든 사람이 책임을 가져야 할 부분에 대해 훈련 내용과 시간 계획을 수립한다. 나아가서 소방훈련과 유사하게 절차에 대하여 주기적으로 테스트를 실시하며 부서의 책임과 임무가 전달되어 지도록 하여야 한다. 또한 사고 대응 절차에 따라 침입방지시스템 운영자에 대하여 훈련을 실시하여야 한다.

만일 보안 기반 구조에 있어서 추가적으로 침입방지시스템의 보고서에서 나온 사항에 대한 행동 절차를 앞당기고자 한다면, 침입방지시스템의 역할을 충분히 고려하여 재검토 할 시간이 필요하다. 특히 침입방지시스템에 의해 제공된 메시지에 따라 절차를 수립하여 행동을 취할 수

있게 계획을 수립하는 것이 좋다.

3.2.5. 로그관리

- 내부에 접속하는 침입시도는 반드시 로그가 남도록 해야 하며, 로그는 다음의 사항이 포함되도록 한다.
  - 로그의 시작과 종료
  - 접근 IP
  - 불법적인 침입시도
  - 침입방지시스템의 구성파일 및 로그파일에 대한 모든 접근
  - 침입방지시스템 정지와 재 기동
- 로그는 주기적으로 분석하고 특이사항 발생 시 내용을 분석 및 검토하여 적절한 조치 후 그 내역 및 결과를 기록 하도록 한다.
- 시스템의 로그는 1주일 단위로 백업을 받고 대장에 기록한다.
- 로그는 용량 도달 시 수동 디스크 또는 테이프 백업이 수행될 수 있도록 한다.
- 백업된 로그의 보관주기는 3개월 이상으로 한다.

3.2.6. 업그레이드

- 침입방지시스템의 운용상 가장 중요한 부분 중의 하나가 최신 탐지 정책을 유지하는 것이다.
- 효과적인 침입방지시스템의 운영을 위해 항상 최신의 침입방지 규칙을 유지하고 필요시에는 자체적으로 탐지 정책을 제작하여 추가하도록 한다.
- 상시 업그레이드를 수행하되 주기적으로 업그레이드 수행기록을 유지한다.
- 정보보호시스템을 최신 기능을 가진 버전으로 업그레이드 하거나 트래픽 탐지패턴을 수시로 업데이트하여 정보통신 망에 대한 장애 및 정보통신설비에 대한 침해사고에 신속 하게 대응할 수 있도록 한다.

4. VPN 보안 관리

4.1. 보안 정책

- DMZ망의 공개된 서비스를 제외한 모든 내부 네트워크로의 접근은 가상사설망(VPN)의 사용자 인증을 성공하여야만 이용이 가능하다.
- 가상사설망(VPN)의 사용자 관리는 책임자의 승인을 받아 네트워크 담당자(VPN 담당자)에 의해 이루어지도록 한다.
- 관리자는 가상사설망을 거쳐 관리자 권한을 획득 및 이용할 수 없다.

4.2. 운영 절차

4.2.1. 사용자 계정 신청

- 정보시스템 원격지 사용을 위한 VPN 계정신청은 임직원으로 제한한다.
- 원격 근무를 하고자 하는 내부 직원은 VPN계정 사용 신청을 하여야 한다.
- 담당자는 VPN 계정 사용 신청을 접수하여 확인하고, 책임자가 VPN 계정신청을 승인한다.

4.2.2. 원격 접속 이용

- 원격지 근무자는 승인된 VPN계정을 이용하여 정보보호팀에서 정한 VPN연결 절차에 따라 사용자 인증을 거친 후 내부 네트워크로의 접근이 가능하다.
- 원격지 근무자는 VPN연결 전 정보보호팀에서 정하는 PC보안절차에서 요구하는 보안소프트웨어 설치 및 보안설정을 정확히 적용 후 내부네트워크에 접근하도록 하여야 하며, 이를 따르지 않음으로 인해 내부 네트워크에 애기치 않은 손상을 발생시켰을 경우 적합한 절차에 따라 징계를 받을 수 있다.

VII. 관리용 단말 보안

1. 목적

관리목적을 위한 단말기(PC)에 대한 다양한 보안 위협 및 취약성으로부터 안전하게 보호하고, 운용 관리 하는데 그 목적이 있다.

1.1. 관리용 단말 보안

1.1.1. 관리용 단말의 용도

- 정보통신설비, 정보보호시스템, 네트워크 장비를 관리하기 위한 관리용 단말은 전용으로 운영하여야 한다.
  ※ 관리용 단말은 관리대상에 접근하는 모든 단말(위탁운영 업체의 관리용 단말 및 개발 PC)이 포함되어야 한다.
- 즉, 관리용 단말은 일반 사무용 등 기타 용도로 사용되어서는 안된다.
- 서비스 업데이트, 패치 등을 이유로 개발용 단말에서 운영 중인 정보통신설비(웹서버, DB서버, 컨텐츠 서버 등), 네트워크 장비, 정보보호시스템에 접근이 가능한 경우 개발용 단말도 관리용 단말에 준하여 관리되어야 한다.
- 웹 하드 서비스에 대한 위탁을 통행 운영 중인 경우 위탁업체의 관리용 단말도 동일한 기준을 적용하여 운영하여야 한다.
- 관리용 단말에서 운영 중인 시스템에 접근하는 경우 안전한 채널(VPN, SSH, SSL, SFTP 등)을 사용해야 한다.

1.1.2. 관리용 단말의 인터넷 사용 통제

- 관리용 단말에서는 관리대상인 정보통신설비, 정보보호시스템, 네트워크 장비로의 접근만을 허용하고 그 외의 접속은 모두 차단하여야 한다.
  - 외부인터넷의 웹 접속뿐 아니라 메신저나 타 프로토콜(telnet, ftp 등)을을 이용하여 외부 네트워크에 접근하는 모든 것을 차단하여야 한다.
- 정보통신설비, 정보보호시스템, 네트워크 장비에 대한 관리자는 지정되어 있어야 하며, 관리용 단말은 지정된 관리자만 사용할 수 있어야 한다.
  - 관리용 단말의 계정 및 패스워드 관리 필요
  - 관리자 패스워드에 대한 복잡도, 변경주기, 패스워드 길이 등 관리

1.1.3. 관리용 단말의 보안관리

- 관리용 단말은 악성코드 방지를 위해 백신이 설치하여야 한다.
- 관리용 단말은 관리대상 시스템을 관리하기 위한 프로그램 외의 불필요한 어플리케이션은 설치하지 않아야 한다.

- 관리용 단말의 운영체제, 설치된 백신은 주기적으로 패치하여야 한다.
- 설치된 백신은 항상 동작하도록 설정되어야 하며, 최신 업데이트를 적용하여야 한다.
- 관리용 단말은 파일공유, 네트워크 공유 등을 설정하여 사용하면 안된다.

VIII. 접근통제 및 보안설정 관리

1. 일반 사항

1.1. 목적

회사의 정보통신설비에는 인가된 자만 시스템에 접속할 수 있어야 하고, 인터넷 등을 통해 외부에서 접속할 경우 일회용 패스워드 사용 등의 인가 절차를 강화하는데 목적이 있다.

2. 접근통제 및 보안설정 관리

- 정보통신설비는 인가된 접속지로부터 인가된 사용자만 접속할 수 있도록 통제하여야 한다.
  - 정보통신설비(웹서버, DB서버, 네트워크 장치, 어플리케이션 서버, 백업서버 등)는 인간된 사용자만 접근이 가능하도록 통제하여야 한다.
  - 침입차단시스템(방화벽)의 보안정책은 정보통신설비에 접근하는 모든 트래픽에 대하여 통제를 수행하여야 한다.
    ※ 인가된 IP/Port 기반 접근통제 및 인가된 프로토콜(SSH, SSL 등) 기반 보안정책을 적용하여야 한다.
  - 정보통신설비는 인가된 사용자만을 허용하기 위하여 ID/Password를 반드시 설정하여야 한다.

- 인가된 사용자만 정보통신설비에 접속할 수 있는지 주기적으로 점검하여야 한다.
  - 비인가된 사용자의 접근을 확인하기 위하여 정보통신설비의 접근이력을 주기적(월 1회 이상)으로 검토하여야 한다.
  - 침입차단시스템의 로그를 기반으로 정보통신 접근이력을 검토하고, 운영체제가 제공하는 로그를 검토하여 비인가자의 접근이 시도되었는지 검토하여야 한다.
  - 퇴사자, 보직이동 등으로 인가된 사용자의 변경이 발생한 경우 계정 삭제, 접근 IP 변경을 통하여 비인가된 사용자의 접근을 차단하여야 한다.
  - 유지보수 등을 위하여 물리적으로 시스템에 접근하여 콘솔로 접근하는 경우 반드시 관리자가 동행하여 유지보수 직원의 작업내역을 확인하여야 하며, 유지보수 등을 위한 별도의 계정을 발급하고 유지보수용 계정에 과도한 권한을 부여하지 않아야 한다.
  - 유지보수용 계정의 경우 평소에는 계정을 중지시켜 사용하지 못하도록 하고, 필요시에 관리자의 허락 하에 사용할 수 있도록 한다.

- 인터넷 등을 통해 외부에서 접속할 경우 일회용 패스워드(OTP) 또는 VPN 등을 사용하여야 한다.
  - 네트워크를 통해 정보통신설비에 접속하는 경우 일회용 패스워드를 사용하거나 VPN, SSH, SSL을 사용하여 안전한 통신채널을 확보하여야 한다.

- 정보통신설비에서 서비스를 제공하기 위해 반드시 필요한 프로토콜을 제외한 프로토콜 및 서비스는 중지 또는 제거하여야 한다.
  - 각 서버(웹서버, DB서버, 백업서버, 어플리케이션 서버)는 각 용도를 제외한 서비스 및 프로토콜을 제공하지 않아야 한다.

IX. 관리자 계정관리

1. 일반사항

1.1. 목적

정보통신설비의 관리자 계정 비밀번호가 유추하기 어려운 패스워드로 설정하여, 외부자로부터 접근을 막는 것을 목적으로 한다.

2. 관리자 계정의 비밀번호 관리

- 정보통신설비의 관리자 계정이 비밀번호는 8자리 이상으로 설정하여야 한다.
  - 정보통신설비에 대한 관리를 수행하는 관리자 계정의 비밀번호는 8자리 이상으로 설정하여야 한다.
  - 단, 시스템 상의 한계로 비밀번호를 8자리 이상으로 설정이 불가능한 경우 해당 시스템이 제공하는 최대 길이의 비밀번호를 사용하여야 한다.
  - 관리자 계정의 비밀번호는 영문자, 숫자, 특수문자를 혼합하여 사용하여야 한다.
  - 관리자의 변경이 발생하는 경우 반드시 계정 및 비밀번호를 변경하여야 한다.
  - 비밀번호 변경 시 바로 이전 비밀번호를 재사용하지 않아야 한다.
  - 정보보호시스템, DB, 웹 어플리케이션 등 제조사에서 제공하는 디폴트 계정 및 비밀번호는 제품 사용 전에 변경하여야 하며, 불필요한 계정은 모두 삭제하여야 한다.
  - 비밀번호 생성 시에 추측하기 어려운 조합구조를 갖도록 하여야 한다.

  ※ 사전에 정의된 단어, 웹하드 사이트 명, 전화번호, 생일 등의 정보를 이용한 비밀번호 생성 금지

- 정보통신설비의 관리자 계정의 비밀번호는 적어도 3개월마다 1회 이상 변경하여야 한다.
  - 관리자 계정의 비밀번호는 최대 사용기간이 90일을 초과하지 않아야 한다.
  - 관리자 계정의 비밀번호 변경에 대한 이력을 기록하여야 한다.
  - 관리자의 계정 및 패스워드를 공유하여 사용하지 않아야 한다.

  ※ 패스워드 생성 시 참고

  [개인정보의 안전성 확보조치 기준 및 해설서 제5조(비밀번호 관리) 규정]
  - 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 2종류 이상으로 구성한 경우
  - 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9개, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성한 경우

X. 로그관리

1. 일반사항

1.1. 목적

정기적으로 로그를 분석하여 정보통신설비의 침입시도 및 이상징후 등에 대한 분석 및 침입유무 확인을 목적으로 한다.

2. 로그 관리

- 정보통신설비의 침입시도 및 이상징후 등에 대해 분석하고 능동적으로 대응하기 위해 기록 관리되어야 할 중요 로그를 식별하여야 한다.
  - 웹 어플리케이션, 정보보호시스템, DB에서 침입시도 및 이상징후를 의미하는 로그가 생성되어 기록될 수 있도록 식별하여야 한다.
  - 각 시스템에서 생성되어야 하는 로그를 분류하기 위한 기준을 마련해야 한다.
  - 웹 어플리케이션에서 생성되어야 하는 로그의 예는 허용되지 않은 페이지 접근 시도, 소스코드 다운로드 시도, Brute Force Attack 등에 대한 로그를 생성할 수 있어야 한다.
  - 정보보호시스템에서 생성되어야 하는 로그의 예는 우회접근, 보안정책 우회, 관리자 권한 획득 시도 등에 대한 로그를 생성할 수 있어야 한다.
  - DB에서 생성되어야 하는 로그의 예는 대량 데이터 다운로드, 비인가자의 접근 시도, 관리자 권한 획득 시도 등에 대한 로그를 생성할 수 있어야 한다.
  - 각 시스템에서 생성된 로그는 관리자가 해석하기에 적합해야 한다.

  ※ 로그는 접근 시도자(계정정보, IP정보, Port정보, 시간정보 등)의 정보가 포함되어야 한다.
  - 관리자는 로그 분석을 통하여 침입시도 및 데이터 유출에 대한 공격이 있었는지 확인하기 위하여 주기적인 로그 분석을 수행하여야 한다.

- 정보통신설비의 식별된 중요 로그는 1개월 이상 보존・관리되어야 한다.
  - 웹 어플리케이션, DB, 네트워크 장치에서 생성된 로그는 최소한 1개월 이상 보존하여야 한다.

- 정보보호시스템의 로그는 3개월 이상 기록・관리되어야 한다.
  - 침입차단시스템(방화벽), 웹방화벽, 웹쉘탐지제품 등의 정보보호시스템에서 생성된 로그는 최소한 3개월 이상 보존하여야 한다.

XI. 중요정보 암호화

1. 일반사항

1.1. 목적

모든 시스템 내 중요정보(주민등록번호, 신용카드번호, 계좌번호, 등)은 암호화 되어야 하며, 안전한 알고리즘의 사용을 목적으로 한다.

2. 중요정보 암호화

- 모든 시스템의 비밀번호를 복호화 되지 않도록 일방향 암호화하여 저장하여야 한다.
  - 웹서버, DB서버, 어플리케이션 서버 등 웹하드 서비스를 운영하는데 구축된 모든 시스템의 패스워드는 모두 일방향 암호화(해쉬 함수)를 이용하여 저장하여야 한다.
  - 운영체제, DB에서는 패스워드 저장 시 일방향 암호화를 기본적으로 지원하지만 웹하드 회원의 패스워드는 DB에 데이터로 저장되므로 별도의 일방향 암호화를 수행하여 저장하여야 한다.
  - 일방향 암호화(해쉬 함수)는 SHA-256 이상의 함수를 적용하여야 한다.

  ※ 단, 운영체제 및 DB 로그인 패스워드의 경우 운영체제나 DB에서 제공하는 패스워드 암호화 방식을 적용한다.

- 주민등록번호, 신용카드번호, 계좌번호 등을 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
  - 주민등록번호, 신용카드번호, 계좌번호 등 웹하드 회원의 개인정보를 DB에 저장하는 경우 안전한 암호알고리즘을 이용하여 암호화하여야 한다.
  - 안전한 암호알고리즘은 키 길이가 128bit 이상을 지원하는 블록암호알고리즘이다.
  - 키 길이가 128bit를 지원하는 암호알고리즘은 SEED, AES가 대표적이며, 암호화에 사용된 키는 안전하게 보관하여야 한다.

  ■ 키 관리의 예

  1. 키가 저장된 폴더에 대한 접근통제 적용 및 숨김 폴더 설정

  2. 사용자 입력 값을 seed로 하여 암호 키를 생성하여 메모리에서만 사용하고 사용 후 메모리에서 삭제하는 방식 적용

  ※ 암호화에 사용되는 키가 웹 소스에 하드코딩하여 사용하는 경우가 있는데 이는 암호키의 노출 가능성이 매우 높으므로 웹 소스에 키를 하드코딩하는 것은 금지하여야 한다.

XII. 취약점 점검

1. 일반 사항

1.1. 목적

정보통신시스템에 대한 주기적인 보안 점검을 수행함으로써 주요 자산의 위협에 대한 노출을 최소화하는데 그 목적이 있다.

2. 취약점 점검

취약점 점검은 웹서버, 메일서버, DNS서버, 인증, DB서버 등의 서버 시스템과, 라우터/스위치 등의 네트워크 시스템 및 정보보호시스템 등을 대상으로 한다.

또한, 취약점 점검은 정보통신설비의 보호를 위하여 연 1회 이상 실시하고 발견된 취약점을 보완하여야 한다.

2.1. 취약점 점검 방법 결정

취약점 점검은 상용 혹은 공개 취약점 점검도구에 의한 진단 및 수작업에 의한 점검, 외부 정보보호업체 등을 통하여 수행할 수 있다. 취약점 점검도구의 이용은 특정한 소수의 취약점 탐지보다는 다수의 취약점 항목을 자동으로 점검할 수 있다.

또한, 취약점점검 업무의 외부위탁 및 정보자산에 대한 제3자의 접근을 허용하는 경우 보안요구사항을 관련 계약에 명시하여야 한다.

2.1.1. 취약점 점검도구 선정

기 도입한 취약점 점검도구를 사용하거나, 또는 취약점 점검도구를 도입하여 진행한다.

2.1.2. 취약점 점검도구 관리

- 취약점 점검도구의 사용 및 관리는 책임자로 제한한다.
- 책임자는 취약점 점검도구의 접근통제에 대한 관리책임을 갖으며, 새로운 취약점이 발견될 경우 취약점 점검도구의 정책업데이트를 실시한다.

2.2. 취약점 점검항목 선정

정보시스템에 문제가 발생하거나 또는 발생할 수 있는 위협요인을 식별하고, 점검에 필요한

취약점 점검항목을 선정한다.

- 시스템 운영체제 상의 취약점
- 시스템 내 주요설정이 잘못됨으로 인한 취약점
- 시스템 내 운용되는 기본 프로그램에 대한 취약점
- 시스템 내 사용자 및 파일시스템의 취약점
- 시스템의 네트워크 서비스 및 데몬 프로그램 관련 취약점
- 시스템 내 설치된 응용프로그램의 취약점 등

2.3. 취약점 점검 수행

취약점 점검도구를 이용하거나 수동으로 점검항목에 대한 기술적 취약점을 탐지하며 가능한 수동점검(보안장비 우회에 대한 중점 점검 등)을 통하여 취약점 점검을 수행한다.

- 정보통신망 및 네트워크 구성 식별 : ping이나 포트 스캔을 이용하여 네트워크에서 동작중인 서버, 네트워크 장비, 정보보호시스템 등 정보통신 시스템에 대한 구성정보를 파악한다.
- 응용 프로그램(서비스) 취약점 점검 : 포트 스캔 등의 기법을 이용하여 네트워크상의 정보통신시스템에 활성화되어 있는 서비스 포트를 확인한다. 이 경우 불필요한 서비스가 동작 중이라면 제거하는 것이 좋다.
- 네트워크 취약점 점검 : ID, 비밀번호 및 데이터 등의 가로채기, 스푸핑, 서비스거부공격 등 기술적인 위협들에 대해 점검한다.
- 시스템취약점 점검 : 정보통신시스템에 대한 내부적 취약점, 즉 운영체제 및 어플리케이션의 보안 취약점을 상세하게 파악한다.
- 무결성 점검 : 중요 파일에 대한 변경 및 손상 여부를 알기 위해 무결성 점검도구를 이용하여 원본 파일 정보와 일치하는지 검사한다.

점검 수행 후 에는 과거에 발생했던 취약점이 다시 발견되었는지, 조치사항에 대한 변경관리를 하고 있는지 등을 확인하기 위하여 일정기간 이상 취약점 점검결과를 DB, 보고서, 하드 카피 등의 형태로 보관할 수 있도록 한다.

2.4. 발견된 취약점 조치

- 취약점 점검을 통해 발견된 취약점에 대해서 적절한 조치와 해결책을 마련한다.
- 취약점 점검결과에 대해 기존 정보보호대책의 적정성, 효율성 및 문제점을 평가하고 분석한다.
- 새로 보완되어야 할 정보보호대책(방침, 절차, 시스템) 등을 기존 대책과 연계하여 효과성, 경제성을 바탕으로 가장 효율적인 대책과 추진방법을 선정한다.
- 책임자는 취약점 분석・평가 결과 발견된 정보보호 취약점들 중에서 시정할 수 있는 항목은 즉시 시정하여 정보보호 취약성을 제거하도록 하고, 즉시 시정할 수 없는 부분은 필요한 보안대책을 수립하여 시정조치 계획서에 반영하도록 한다.
- 책임자는 취약점 시정조치 계획을 기록하여 적절한 시정조치가 이루어 졌는지

추적·관리한다.

- 아래의 방법에 따라 시정조차 할 수 있도록 한다.
  - 정보시스템 관리자 개별 면담을 통한 우선 조치사항 결정
  - 불필요 서비스는 확인 후 차단정책 적용하여 잠재적 취약성 제거
  - 서비스 영향을 최소화하도록 패치 및 업데이트 일정을 별도 수립 후 시행

2.5. 예외적용

다음 각 호에 해당하는 경우에는 본 규정에서 명시한 내용일지라도 정보보안 담당자의 승인을 받아 예외 취급한다.

- 기술 환경의 변화로 적용이 불가능할 경우
- 관리적, 기술적인 이유로 지침의 적용을 보류할 긴급한 사유가 있을 경우
- 기타 재해 등 불가항력적인 상황일 경우

XIII. 침해사고 대응

1. 일반사항

1.1. 목적

침해사고에 신속하게 대응하기 위한 준비와 대응절차를 기술하여 침해사고로 부터의 피해를 최소화하고 후속 보안 대책을 세울 수 있도록 하는데 그 목적이 있다.

적절하지 못한 사고대응은 지속적인 침해사고를 야기하게 되며, 이에 따른 고비용 및 회사 이미지의 손상을 초래하게 된다. 따라서 보안 관리자는 침해사고가 발생했을 때 또는 공격을 탐지했을 때 이에 신속하게 대응할 수 있는 준비를 갖추어야 한다.

1.2. 인력 구성 및 비상 연락 체계

1.2.1. 인력 구성

일반적으로 책임자, 담당자 등으로 구성한다.

- 책임자 : 침해사고 대응조직의 실무 관리자로 침해사고대응 업무를 총괄하여 빠른 사고대응 업무가 가능하도록 한다. 회사 내에서는 타 부서와의 업무 조율 역할과 대외적으로는 국내 정보보호 유관기관과의 협력 관계를 구축한다.
  또한, 회사의 대내외 업무 조율을 위한 실무 대표자 역할을 한다. 주로 사고대응을 위한 대내외 협력 업무에 대한 연락처로써의 역할을 수행한다.

- 담당자 : 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 이관하는 작업을 수행한다.
- 침해사고 처리 담당은 침해사고 발생 시 해당 사고를 정확히 분석하고 대응 할 수 있는 사고 분석 전문가 역할을 수행한다. 이러한 업무를 담당하는 사람은 조직 내의 시스템 및 네트워크 관리 그리고 서비스 운영에 대한 지식을 갖고 있어야 한다. 하지만 필요에 따라 산업정보평생과에 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
  - 침해사고 탐지 및 방지를 위한 프로그램 개발 참여

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

- 보안권고문 작성 배포
- 기술 문서 작성 및 배포
- 보안 가이드라인 작성 및 배포 등

1.2.2. 비상 연락망

비상연락망은 전 직원의 업무 사무분장을 기반으로 하여 연락처, 비상 연락처를 포함 한다.

1.3. 침해사고의 범위

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

1.3.1. 침해사고의 종류

- 악성 프로그램 유포 : 제작자가 의도적으로 다른 정보통신 이용자에게 피해를 주고자하는 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 인터넷 웜, 트로이목마 등이 공격에 이용된다.

- 서비스거부 공격(DoS, Denial of Service) : 시스템 또는 네트워크 서비스의 정상적인 운영을 방해하는 공격으로, 시스템을 다운시키거나, 네트워크에 과부하의 트래픽을 유발시켜 사용자들이 서비스를 이용하지 못하게 하는 공격이다.

- 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.

- 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.

- 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.

- 보안 정책 위반 : 회사의 보안에 위배되는 행위 또는 고의적인 위반행위 또한 침해사고로 정의하고 각 경우에 대해서 조사한다.

1.4. 제공 서비스

침해사고대응조직은 새로운 침해사고 및 취약성에 대한 경고를 제공하고, 사고처리를 위한 업무를 하게 된다.

1.5. 대외 업무

책임자는 회사를 대표하여 보안과 관련된 외부조직과의 많은 대외업무를 필요로 한다. 담당자는 침해사고 발생 시 신속한 조치를 위하여 해킹·바이러스 관련 사고대응기관과 협조 체재를 유지한다.

2. 침해사고 대응 및 복구

2.1. 침해사고 신고 접수 요령

2.1.1. 접수 방법 및 수단

침해사고 접수방법에는 긴급한 사항인 경우 주로 전화를 이용하며 일반적으로는 전자우편을 통해 접수받는다. 침해사고로 전자우편을 이용할 수 없거나 폐쇄망을 사용하는 경우는 팩스를 이용한다. 침해사고 접수자는 사고 보고자와 연락하여 다음 사항을 주지시키고 확인하도록 한다.

- 제공된 정보를 어떻게 취급할 것인지를 신고기관 담당자에게 주지시킨다.

- 침해사고 피해기관의 담당자에게 침해사고 접수자의 신분정보를 제공한다.
  - 침해사고 신고자가 정보보호팀의 접수자를 확인할 수 있도록 이름, 전화번호, E-mail주소를 알려준다.

- 신고기관의 연락처 및 신고자의 신분 확인
  - 침해사고 접수자는 신고자의 연락처로 연락하여 신고기관 및 신고자의 신분을 확인하여 거짓 신고 및 사기성 신고를 방지한다.

- 침해사고에 대하여 수사기관에 신고할 것인가 여부를 확인한다.

[접수 수단]

- 전　화 :　XXX) XXX-XXXX
- 팩　스 :　XXX) XXX-XXXX
- E-Mail :　admin@XXX.co.kr

2.1.2. 접수 및 전달 절차

침해사고 보고 경로는 E-mail을 기본으로 하며, “사고신고” 양식에 따라 침해사고 신고를 적절히 할 수 있도록 양식을 사전 배포 또는 게시토록 한다.

사고가 보고될 경우, 다음과 같은 지침에 따라 사고를 처리하도록 한다.

- 침해사고 보고기관(사람)의 신분을 확인한다.
- 관련 담당자에게 사고접수 내용(E-mail등)을 전달한다.
- 침해사고 신고기관(사람)에게 침해사고 접수확인 메일을 전송한다.

답장 메일 전송 시 침해사고 신고 접수 확인 및 할당된 사고번호를 메일의 제목에 명시하고, 사고번호 관리를 통해 연락 및 정보 교류를 원활히 할 수 있도록 한다.

2.1.3. 침해사고 처리 절차

- 침해사고 신고 접수한자는 침해사고 접수 후 신속히 책임자에게 보고 후 관련담당자에게 사고 내역을 인계토록 한다.

- 침해사고와 관련된 시스템의 담당자는 침해사고 유형에 따라 우선순위를 부여하고 각 사고의 트래킹을 위해 사고번호를 부여한다. 만일, 침해사고로 처리하지 않아도 되는 잘못된 신고일 경우 신고자에게 해당 사실을 통지하고 사고를 종결한다.

- 침해사고를 처리한 담당자는 “사고 조치 결과” 양식에 따라 정보보안 담당자에게 사고 개요를 보고하고 사고처리를 진행한다.

2.2. 침해사고 처리 요령

2.2.1. 초기분석 및 사고대응전략 수립

사고번호가 할당되면, 사고를 처리할 담당자를 지정하고 사고를 처리한다. 사고분석 담당자는 먼저 보고된 기본 자료를 검토하고 구체적인 처리 방향을 설정한다. 보고된 자료만으로도 침해사고의 여부를 정확히 판단하기 힘든 경우에는 사고와 관련된 담당자와 연락을 취하고 추가적인 정보를 획득하거나 초기 분석을 한다.

사고처리 방향을 결정하는데 여러 고려사항이 있을 수 있다. 담당자는 무엇보다 어떤 결정을 하는데 있어 가능한 피해시스템의 관리자와 협의를 하는 것이 우선되어야 한다.

2.2.2. 분석방법 고려사항

피해시스템을 네트워크에 연결된 상태 그대로 분석을 할 것인가(라이브 분석), 또는 피해시스템을

격리시켜서 분석할 것인가를(격리분석) 결정해야 한다. 각각의 분석방법에 따라 장단점이 있으며, 침해사고의 상황에 따라서 방법이 결정된다. 일반적으로는 라이브 시스템에서 초기분석을 한 후에 결과에 따라서 라이브 시스템에 대한 분석을 할지 아니면 격리분석을 할지 결정한다.

- 라이브 시스템 분석 : 현재 네트워크에 연결되어 서비스를 제공하고 있는 라이브한 피해시스템을 분석하는 것이다. 이처럼 살아있는 시스템을 분석할 경우에는 현재 실행되고 있는 프로세스에 대한 분석, 메모리 내용의 분석, 네트워크 활동 정보, 임시파일 등을 분석할 수 있는 장점이 있다. 그리고 무엇보다 공격자의 활동을 지속적으로 감시할 수 있는 장점도 있다. 반면, 분석 도중에 침입 흔적이 손상되거나, 공격자에게 노출될 수 있는 위험이 있다. 주로 다음과 같은 상황에서 라이브 시스템을 분석한다.

  - 피해시스템에서 제공하는 서비스를 대체할 만한 백업 시스템이 없을 경우,
  - 빠른 사고분석 및 대응을 해야 할 경우
  - 라이브한 공격정보를 얻기 위해 격리분석을 원하지 않을 경우
  - 공격자 또는 공격 프로그램의 지속적인 모니터링이 필요한 경우
  - 피해 여부가 확실하지 않아 확인을 위한 분석을 할 경우
  - 특별히, 격리분석을 필요로 하지 않을 경우

- 격리분석 : 공격흔적을 보존하기 위해 피해시스템의 디스크 이미지를 복사하고 복사본을 분석하거나, 또는 부팅 가능한 분석용 CD-ROM으로 피해시스템을 부팅시킨후 피해시스템의 디스크를 읽기 전용으로 마운트해서 분석한다. 사고로 인한 피해를 확산시키지 않으며, 피해시스템의 상태를 훼손하지 않고, 파일시스템에 대한 세밀한 분석을 할 수 있는 장점이 있다. 반면, 라이브 시스템에서만 획득할 수 있는 많은 정보를 놓치게 된다. 또한 지속적으로 공격자를 모니터링 할 수 없는 단점이 있다. 따라서 격리분석이 필요한 경우에는 먼저 라이브시스템에 대한 기본적인 정보를 빠르게 수집하고 나서 격리하는 것이 바람직하다. 주로 다음과 같은 상황에서 격리분석을 하게 된다.

  - 공격의 피해가 계속 확산될 것으로 판단되는 경우, 바로 네트워크를 차단한다.
  - 여분의 백업 시스템이 있으며, 시간을 갖고 자세히 분석하고 싶을 경우
  - 라이브 시스템에 대한 분석이후, 파일시스템에 대한 보다 자세한 분석을 할 경우
  - 공격 증거를 보존하기 위해 피해시스템을 훼손하지 말아야 할 경우

2.2.3. 대응방법 고려사항

대응측면은 주로 공격자의 추적여부, 복구를 어떻게 할 것인가, 보안조치를 언제 할 것인지에 대한 결정, 그리고 법적 대응을 할 것인지 등에 대한 결정이 따른다. 마찬가지로 모든 결정은 침해사고의 상황과 분석자의 판단에 따르게 된다.

- 공격자 추적 : 공격자를 추적하기 위해서는 공격자 모니터링, 외부기관의 협력 등 많은 시간과 자원을 필요로 한다. 사고 범위, 피해 규모, 그리고 내부 자원의 역량에 따라서 추적 여부를 결정한다. 무엇보다 고객사와 협의를 통해서 하도록 한다.

- 복구 : 침해사고의 성격, 피해 범위에 따라 복구의 시기, 방법, 범위가 달라진다. 이는 피해시스템 분석에도 영향을 준다. 예를 들면, 매우 중요한 사고이며 서비스가 계속 제공되어야 하는 경우 일차적인 초기분석을 통해 시스템을 먼저 복구해야 한다. 하지만 이러한 복구 과정에서 많은 공격흔적이 훼손될 수 있다.

- 법적 대응 : 사고의 경중에 따라서 법적인 대응을 할 것인지 고려한다. 만약 침해사고로 인한 피해가 있다면 법적인 대응을 적극 고려해 볼 수 있다. 만약 법적 대응을 결정한 경우에는 최대한 피해시스템을 보존하도록 해야 한다.

  - 피해시스템 통제: 더 이상의 피해를 받지 않기 위해 외부로부터 시스템을 차단한다.
  - 시스템의 처리: 가능한 시스템을 직접 분석하지 않고 원본 상태로 보관한다. 긴급 시에는 서버를 이미지복사 한 후에 시스템 복구 작업을 하도록 한다.
  - 위와 같이 처리한 다음 수사기관(국가사이버안젠센터/검찰청 인터넷 범죄 수사센터 등)에 신고하여 피해상담 및 복구, 법률적인 대응방안에 대해서 조력을 받도록 한다.

2.2.4. 피해 시스템 분석

사고분석의 목적은 피해시스템을 분석해서 다음과 같은 사실을 밝히기 위해서 이다. 항상 모든 사항을 밝혀낼 수는 없으나, 이를 밝히기 위해 최선을 다해 분석해야 한다.

- 사고가 발생한 원인 및 공격방법 : 공격자가 시스템에 어떻게 침입했는지에 대해서 분석한다. 주로 특정 어플리케이션의 취약성, 시스템의 잘못된 설정, 그리고 계정 도용 등을 이용하여 침입한다.

- 사고의 발생 시간 : 공격자가 언제 처음으로 시스템에 침입했는지 분석하고, 최초 침입 이후 재 침입이 언제 있었는지 등에 대해서 분석한다.

- 사고의 발생 범위 : 보통 사이트 내에 하나의 시스템이 공격을 당했으면, 다른 시스템도 해킹을 당했을 경우가 많다. 따라서 사이내의 다른 모든 시스템, 그리고 피해시스템과 관련된 시스템에 대해서 피해여부를 확인해야 한다.

- 공격자 출처 : 공격자의 IP주소를 찾아내고, 해당 IP를 사용하는 기관 정보를 분석한다.

- 공격의 목적 : 공격자가 피해시스템에서 어떠한 활동을 했는지 분석함으로서 공격의 목적을 확인한다. 주로 정보유출, 단순한 침입, 공격시스템으로 사용 등의 목적이 있을 수 있다.

- 사고복구를 위한 긴급조치와 장기조치 방법: 사고를 분석하면서 긴급하게 취할 수 있는 예방조치방법을 찾아보고 필요할 경우 예방조치를 취한다. 그리고 완전한 사고분석이 끝나면 향후 비슷한 유형의 사고를 예방하고 탐지할 수 있는 대책을 마련한다.

다음은 사고를 처리하는 담당자가 유의해야 할 사항이다.

- 가능한 침입흔적을 있는 그대로 보존한다.
- 분석과정에서 수집된 데이터를 별도 시스템에 백업, 관리 한다.
- 침해시스템 복구 시 침해 관련된 파일 및 프로세스는 삭제와 별도로 침해 흔적 파일 보관 또는 시스템 이미지 백업을 수행한다.

- 분석하는 모든 과정을 기록한다. 분석방법, 내용, 분석시간, 그리고 해당 분석을 한 이유 등에 이르는 가능한 모든 내용을 적는 것이 좋다. 이러한 자료가 축적되면서 사고대응 능력이 획기적으로 높아지게 된다.
- 각각의 침입흔적에 대한 설명과 발견된 위치·시간 등을 기록하고 보존한다.
- 시스템 로그, 침입차단시스템 및 침입방지시스템의 로그, 분석과정에서 생성된 기록 등 피해시스템에서 발견된 파일, 해당 사고와 관련되어 다른 사이트에서 발견된 흔적들 최대한 수집 및 백업을 수행한다.
- 사고와 직접적으로 관련되지 않은 사람에게 관련 정보를 공개하지 않는다.

2.2.5. 모니터링

사고분석 후에 추가적인 공격정보의 획득 또는 공격자 추적을 위해서 모니터링을 할 수 있다. 모니터링 대상은 공격자 또는 공격 프로그램의 활동이 될 수도 있다. 모니터링 방법은 네트워크 모니터링과 피해 시스템 모니터링을 통하여 수행한다.

2.3. 침해사고 대응 및 복구

사고대응 및 복구 단계에서는 취약성 제거, 피해시스템 복구, 관련자 통지, 보안대책 구현, 등의 작업을 수행한다.

- 취약성 제거
  - 공격에 이용된 취약성을 제거한다.
  - 피해시스템뿐 아니라 피해시스템과 똑같은 종류의 시스템에 대해서 모두 분석하고 같은 취약성이 발견되면 이를 제거한다.
  - 이러한 작업은 사고분석 결과 조직 내의 관련된 담당자에게 배포함으로서 각 담당자가 직접 수정하도록 유도 한다.
- 피해시스템 복구
  - 취약성 제거를 한 다음, 정상적인 서비스가 이루어지도록 시스템을 복구한다.
  - 만약 분석이 완벽하게 이루어지지 않았다고 판단된다면, 되도록 시스템을 다시 설치하는 것이 바람직하다.
  - 그리고 시스템 복구 시에는 가장 믿을만한 백업 버전으로 복구를 한다.
- 관련자 통지
  - 사고와 관련된 모든 사람에게 분석결과를 통지해 준다. 이 경우, 사고와의 관련성에 따라 주는 정보의 깊이가 달라져야 한다.

- 외부 기관에 주는 정보는 피해기관의 세부 정보가 포함되지 않아야 하며, 상대방이 필요로 하는 정보만을 전달하도록 한다.
- 단기 및 중장기 대응 방안 수립을 통한 재발 방지 및 해당 사고 전파 여부를 결정하고 전파를 통한 동일사례 재발방지 활동을 수행한다.

2.4. 침해사고 보고 절차 및 방법

2.4.1. 침해사고의 유형

- 악성 소프트웨어(바이러스, 백도어, 트로이 목마, 백오리피스 등)에 의한 침해
- 네트워크/시스템 침해 및 징후 포착
- 자산의 도난, 분실, 파손 및 파괴
- 정보 자산의 유출 및 변조
- 대내외의 비인가된 해킹 시도
- 기타 발견된 보안취약성, 소프트웨어 오동작, 시스템 오류 등

2.4.2. 침해사고의 긴급성 판단 기준

- 분산서비스거부공격(DDoS)을 당하고 있어 시스템의 정상 동작이 불가능한 경우
- 침입자에 의해 서버의 중요 파일이 삭제되고 있는 경우
- 백도어, 백오리피스 등의 악성프로그램이 실행되어 정상적인 접근제어를 실시하더라도 다른 경로를 통한 침입자의 지속적인 공격 시도가 있는 경우
- 자산의 절취 및 도난 등의 현장을 목격한 경우
- 비인가자에 의한 정보자산의 유출 및 변조 현장을 목격한 경우

2.4.3. 침해사고의 감시 및 보고

- 침해사고 감시
  각 시스템 담당자는 다음 각 호의 방법으로 보안사고 또는 보안위협 시도를 확인하기 위하여 보안사고 징후를 감시한다.
  - 사용자 ID 로그인의 로그 검토
  - 외부로부터의 접속 로그 검토
  - 침입차단시스템(방화벽) 로그 검토
  - 침입탐지시스템의 실시간 경보 감시
  - 침입탐지시스템의 로그 검토
  - 백신 프로그램의 주기적 수행을 통해 바이러스 감염 감시

- 침해사고 감시 실행 주기
  - 각 담당자는 사용자 ID 로그인 로그 검토를 매월 시행
  - 외부로부터의 접속 로그 검토는 매월 시행
  - 침입차단시스템 로그 검토는 매월 시행
  - 침입탐지시스템의 실시간 경보 감시 기능은 365일 24시간 작동으로 유지
  - 침입탐지시스템에 대한 로그 검토는 특별한 보안 경고가 발생했을 때 시행

- 백신 프로그램을 이용한 바이러스 검색은 매주 시행

- 침해사고 보고 및 처리 절차
  - 사고분석 및 대응이 종료되면, 사고에 대한 보고서를 작성하며 종합분석 시스템의 침해대응메뉴의 보고서 및 위협경보 보고서를 통하여 정보보안 담당자 및 상위기관에 대응 결과 및 요청 사항에 대한 회신을 수행한다.
  - 보고서 내용은 사고분석 및 대응 과정의 모든 내용과, 비슷한 유형의 사고를 방지하기 위한 보안시스템의 개선방향 등에 대해서 작성한다.
  - 작성된 보고서는 조직 내의 책임자에게 보고되고 책임자의 결정에 따라 현재의 시스템 또는 네트워크에 그 결과가 반영 되어야 한다.

관련 서식

[별첨 1] 시스템실 작업 계획서

정보시스템 작업 계획서

년 월 일

제 목			
목적 및 근거			
대상시스템			
작업일시			
작 업 자			
작업내용	작업계획		
	작업환경		
복구계획			
영향성평가			
공지사항	중단서비스		
	공지내용		
특이사항			

결재	담당자	책임자

[별첨 2] 시스템 작업 결과 보고서

정보시스템 작업 결과 보고서

년 월 일

제 목	
목적 및 근거	
대상시스템	
작업일시	
담당자/작업자	
작업내용	
작업결과	
중단서비스	
기타사항	

결재	담당자	책임자

[별첨 3] 보안정책 변경 요청서

보안정책 변경 요청서

담당자	책임자

신 청 자	소속	직급	성명	연락처
사 유 (작업내용)				
사용기간	□ 영구 □ 임시 (~)			
사용시간	시간 :		요일 :	
등록구분	□ 신규 □ 변경 □ 삭제			
행 위	□ 허용 □ 거부			
출 발 지		IP		
목 적 지		IP		
접근포트		사용계정		
처리일시		처리자	(인)	
기 타	작업자 소속 :	성명 :	연락처 :	

본인은 회사 침입차단시스템 및 서버보안, DB보안 정책 변경을 상기와 같이 요청합니다.

년 월 일

신청자 : (서명)

[별첨 3] 보안정책 변경 요청서 - 작성 요령

보안정책 변경 요청서 작성 요령

1. 작성시기

- 회사 내외부 사용자가 회사에서 운영 중인 정보시스템 장비에 원격 접속이 필요하여 방화벽, 서버보안, DB보안 정책 수정을 요할 시 신청자(업무 담당자)가 작성

2. 작성 및 처리요령

가. 신청부서

1) 신 청 자 : 신청자 소속, 직급, 성명, 연락처 기재
2) 사유 : 원격 접속 신청 사유(작업내용 등) 기재
3) 사용기간 : 영구/임시 여부, 임시 룰셋일 경우 해당 날짜 기재
4) 사용시간 : 원격접속이 필요한 시간 기재
5) 요일 : 원격접속이 필요한 요일 기재
6) 등록구분 : 요청 룰셋의 신규, 변경, 삭제 여부 표기
7) 행위 : 원격 접속의 허용, 거부 여부 표기
8) 출발지 : 접속자의 설명, IP 기재
9) 목적지 : 접속대상의 설명, IP, 사용 서비스 포트 기재
10) 사용계정 : 원격 접속 시 사용 OS계정, DB계정 기재
11) 기타 : 작업자의 소속, 성명, 연락처 기재
12) 신청 : 하단에 신청일자와 신청자 기재 후 서명
13) 결재 : 좌측 상단에 해당 장비담당자 및 팀장(담당) 서명

나. 처리부서

1) 결재 : 우측 상단에 보안담당자 및 책임자 확인 서명
   (책임자는 책임자에게 원격접속 승인권한을 위임 전결 한다.)
2) 처리 : 보안정책 적용 후 처리일시와 처리자(보안장비담당자) 기재 및 서명

3. 작성 후 관리

- 보안 룰셋 변경 요청서(철)에 보관하여 관리

[별첨 4] 백업 관리 보고서

백업 관리 보고서

장비명		Full백업일			
			직급	성명	서명
		담 당 자			
백업방법		책 임 자			

1. 백업 현황

백업대상서버	데이터 종류	성공 여부							Full Backup 세부사항					
		월	화	수	목	금	토	일	백업 미디어	용량 (GB)	시간 (시:분)	백업 주기	보관 주기	보관 장소
합 계														

2. 복구 사항 및 장애 사항

복구 수행	
장애 및 조치 내역	

3. 특이 사항

특이사항 및 기타 사항	

[별첨 5] DBMS ID(생성/변경/삭제) 신청서

DBMS ID(생성/변경/삭제) 신청서

담당자	책임자

신청자	소속	성명	직위
종류	□ 개인 ID □ 공용 ID		
기본정보	신청 ID	신청 DBMS	유효기간
추가사항 (생성할 경우만)	패스워드 (없을 시 초기 패스워드)	필요권한	
생성 및 폐기의 필요내역			

위와 같이 접근권한을 요청하오니 검토 후 재가하여 주시기 바랍니다.

년 월 일

신청자 : (인)

[별첨 6] 데이터베이스 권한 부여 관리대장

데이터베이스 권한부여 관리대장

계정명	요청권한	업무명	요청대상	요청사유	권한부여일	권한해제일	신청자	확인자

[별첨 7] 서버 장비 설정/로그 백업 관리대장

서버 장비 설정/로그 백업 관리대장

담당자	책임자

NO	백업일자	장비명	백업 내용	비고
1	2014.00.00	server#1	모든 설정 백업	
2				
3				

[별첨 8] 네트워크 장비 설정/로그 백업 관리대장

네트워크 장비 설정/로그 백업 관리대장

담당자	책임자

NO	백업일자	장비명	백업 내용	비고
1	2014.00.00	Router#1	모든 설정 백업	
2				
3				

[별첨 9] 정보보호시스템 설정/로그 백업 관리대장

정보보호시스템 설정/로그 백업 관리대장

관리 담당자	책임자

NO	백업일자	시스템명	백업 정책	백업 내용	담당자
1	2014.00.00	Firewall	Full Backup	모든 정책 백업	홍길동
2	2014.00.00	Firewall	Incremental Backup	로그 파일	홍길동
3					