금융회사 침해사고 준비도 가이드

2016. 12. 21.

목 차

Ⅰ. 개 요

1. 작성 배경

□ 전자적 침해사고의 예방 및 피해 최소화 필요성 증가

- IT기술을 사용하는 업무 비중이 늘어나면서 전자적 침해사고에 의한 대규모 피해발생 가능성이 증가
- 침해사고와 관련된 디지털 증거가 없어지거나 위변조 되면 사고원인 파악이 어렵고 많은 시간이 소요되어 재발 및 피해확산 가능성 증가

□ 전자적 침해사고 조사에 고비용 발생

- 공격기술이 고도화되면서 침해사고 원인을 조사하기 위해 소요되는 비용이 과다하게 발생할 수 있어 조사비용의 절감방안 필요

□ 전자적 침해사고와 관련된 법적 분쟁에 대비

- 침해사고 증가와 고객정보의 중요성에 대한 사회적 인식이 높아지면서 관련 법적분쟁의 발생 가능성이 증가하여 이에 대한 대비 필요

2. 작성 목적

「금융회사 침해사고 준비도 가이드」(이하 '가이드')는 금융회사가 침해사고 예방 및 피해규모 최소화, 유사시 사고조사 비용의 절감 및 디지털 증거의 법적 증거능력 확보를 위하여 사전에 갖추어야 할 사항을 안내함으로써 금융회사가 수행하는 침해사고 대응업무 지원을 목적으로 함

3. 가이드의 구성

가이드는 총 3장과 참고자료로 구성

① Ⅰ장은 가이드가 작성된 배경, 목적, 가이드 내용의 구성, 가이드 활용과 관련된 내용을 포함

② Ⅱ장은 아직은 생소한 침해사고 준비도(이하 '준비도') 및 디지털 포렌식의 개념, 필요사항, 국내외 현황 등을 간략하게 소개

③ Ⅲ장은 금융회사가 침해사고 준비도를 구축함에 있어 사용할 수 있는 필요사항에 대한 현황 정보, 관련기술 안내, 업무절차 등을 예시함으로써 IT보안 담당자가 업무에 활용할 수 있는 준비도 참조 모델을 제시

④ 참고자료는 IT보안 담당자가 침해사고 준비도를 자체 점검해볼 수 있도록 하는 체크리스트 등을 제공

4. 가이드의 활용

□ 침해사고 준비도 구축 업무 수행에 참조

– 본 가이드는 신속한 침해사고 조사를 위하여 금융회사가 갖추어야 할 준비도 참조모델을 포함하고 있으므로 금융회사 IT보안 담당자가 이를 참조하거나 회사별 상황에 맞춰 일부 수정하여 업무에 활용

□ 정보보호 프로세스 개선에 활용

– 기존 복구 중심의 침해사고 대응 프로세스를 신속한 사고원인 조사를 통한 재발방지 및 피해 최소화 프로세스를 추가하여 개선하는데 본 가이드를 활용

5. 가이드의 개정

연단위 개정을 원칙으로 하며 작성일 및 버전을 표지에 명시하여 최신 가이드를 확인할 수 있도록 함(다만, 환경변화가 없으면 개정을 생략)

Ⅱ. 침해사고 준비도 소개

1. 「침해사고 준비도*」 개념

* 포렌식 준비도라 불리기도 하며, 본 가이드는 침해사고 대응에 중점을 두기 위하여 침해사고 준비도라는 용어를 사용

□ **정의** : 침해사고와 관련된 디지털 증거를 법적 증거능력을 갖는 방식으로 수집·분석(디지털 포렌식)하기 위한 계획 및 시스템과 인적 자원에 대한 조직적 준비

【참 고】 디지털 포렌식 연구자 논문 등에 명시된 정의

□ Tan

침해사고 대응에 필요한 포렌식 비용을 최소화하고 증거 데이터에 대한 사용가능성을 최대화하기 위하여 신뢰할 수 있는 증거를 수집할 수 있는 환경능력을 극대화 시키는 것

□ Rowlingson

사전에 잠재적인 디지털 증거를 수집할 수 있도록 조직의 정보시스템을 설정하고 조직의 정책, 인력, 절차를 이에 맞게 조정하는 것으로 사후 분석에 필요한 증거의 가용성 및 품질을 향상시키는 것

□ Nikkel

디지털 포렌식 업무를 수행하기 사전에 절차와 도구, 훈련된 인력을 마련하고 포렌식 능력을 IT 기반시설과 어플리케이션의 초기 설계 요소로 구현하는 것

□ 백승조, 임종인

잠재적 디지털 증거를 법적 증거능력을 유지하는 방식으로 수집·분석하기 위한 준비를 갖추는 수준으로 잠재적 증거를 신속하게 확보하기 위한 계획을 사전에 수립하고 시스템적, 인적 준비를 조직적으로 갖추는 것

※ 출처 : 「개인정보보호 강화를 위한 포렌식 준비도 모델 및 도입방안 연구」 (저자 : 백승조, 임종인; 2015년 5월)

□ 특징

- 침해사고가 발생하기 전에 디지털 증거를 신속하고 효과적으로 수집하고 분석할 수 있도록 IT 인프라 및 프로세스를 구축하는 사전적 침해사고 대응 전략
- 업무 복구 중심의 기존 침해사고 대응계획과는 달리 신속한 사고원인 파악으로 침해사고의 재발 및 피해확산 방지계획도 포함
- 무결성, 신뢰성이 보장된 상태로 디지털 증거를 수집·분석하여 법적 증거능력을 확보할 것을 요구

□ 도입 장점

- 신속한 사고원인 파악을 통한 적시 대응으로 업무연속성 확보 및 사고조사 지연에 따른 피해 최소화
- 침해사고가 발생할 경우 침해사고 조사에 필요한 비용과 시간을 최소화
- 디지털 증거의 법적 증거능력 확보로 침해사고 관련 법적 분쟁에서 면책 가능성 증가
- 합리적 보호조치를 취하고 있음을 보여줌으로써 기업의 정보보호 시스템에 대한 신뢰도 제고
- 침해사고 대응을 위해 요구되는 IT규제를 효과적으로 준수

금융회사는 기존 복구중심의 침해사고 대응 계획에 침해사고 준비도 개념을 포함하는 것이 필요

2. 「디지털 포렌식*」 개념

* 법의학에서 사용하는 포렌식이라는 용어를 디지털 영역에 접목한 용어

□ **정의** : 침해사고의 근본 원인을 밝히기 위하여 디지털 증거를 적법한 방법으로 식별, 분석, 보존, 제출하는 일련의 과정

【참 고】 위키피디아 정의

- 전자적 증거물 등을 사법기관에 제출하기 위해 데이터를 수집, 분석 및 보고서를 작성하는 일련의 작업
- 사이버 해킹 공격 및 사이버 범죄시 범죄자들이 컴퓨터, 이메일, IT기기, 스마트폰 등의 운영체제, 어플리케이션, 메모리 등에 다양한 전자적 증거를 남기게 되므로 사이버 범죄자 추적 및 조사에 핵심적 요소

□ 디지털 증거의 특징

– 저장매체의 영향을 받지 않고 원본과 사본의 생산, 이전, 삭제, 수정이 가능하여 원본과 사본의 구별 및 위변조 확인이 곤란

– 디지털 형태로 저장되기 때문에 인간이 직접 내용을 인지할 수 없어 가독성을 위하여 변환과정이 필요하며 이를 위해 전문가 참여가 필요

□ 디지털 포렌식의 유형

– 목적에 따른 분류

· 정보추출 포렌식(Information Extraction Forensics)
디지털 저장매체에 기록되어 있는 데이터를 복구하거나 검색하여 찾아냄으로써 증거를 발견하거나 확보하는 포렌식
· 사고대응 포렌식(Incident Response Forensics)
침해행위와 관련된 시스템의 로그, 해킹기록 등을 조사하여 사고의 원인, 피해내용, 공격자 등을 파악할 목적으로 수행하는 포렌식

– 수집 및 분석대상에 따른 분류

· 휘발성 증거에 대한 포렌식

레지스터, 캐시, 메모리의 내용이나 네트워크 연결상태, 실행중인 프로그램 상태, Swap 파일시스템 내용, 파일 및 디렉터리의 시간속성 정보 등 시스템 종료 및 임의 접근으로 본래의 데이터가 사라지거나 훼손되는 데이터에 대한 포렌식

· 비휘발성(디스크) 증거에 대한 포렌식

하드디스크, USB메모리 등과 같이 비휘발성 저장매체로 부터 디지털 증거를 획득·분석하는 포렌식

· 네트워크 증거에 대한 포렌식

네트워크상에서 전송중인 패킷정보 등 디지털 증거를 획득·분석하는 포렌식

· 프로그램 소스(Source) 포렌식

프로그램 원시코드나 리버스 엔지니어링(Reverse Engineering) 등을 통해 확보된 프로그램 소스의 작동방식 및 결과를 분석하는 포렌식

3. 침해사고 준비도 필요 사항

필요 사항	금융회사 관련 현황
① 침해사고 및 디지털 증거 식별	□ 보호자산 식별 - 금융회사 주요 보호자산은 전자금융 서비스, 개인(금융)정보, 업무정보, 내부(업무)망, 인터넷망 등 - 특히, 개인(금융)정보는 유출, 위변조, 삭제 등 다양한 침해위협이 있고 공격자의 주요 목표가 될 수 있음
	□ 침해사고 유형 분류 - 전자금융감독규정 시행세칙*은 6개 유형으로 침해사고를 분류(디도스 공격, 전산자료/프로그램 조작, 정보유출, 시스템 위변조, 내부망 해킹, 악성코드 감염) *정보기술부문 및 전자금융 사고보고 양식
	□ 침해사고 관련 디지털 증거 식별 - 금융회사의 보호자산과 연관된 정보처리시스템, 정보보호시스템, 네트워크, 단말기(PC 등), 웹서비스 서버 등의 디지털 기록이 디지털 증거 - 저장된 로그, 이벤트 기록 등 비휘발성 정보뿐만 아니라 시스템을 종료하면 사라지는 휘발성 정보(메모리, 네트워크 연결정보 등)도 중요한 디지털 증거

필요 사항	금융회사 관련 현황
② 법적, 기술적, 인적 요구사항 식별	□ 법적 요구사항 및 제한사항 식별 - 금융회사 침해사고와 관련된 주요 법률인 전자금융거래법, 정보통신기반보호법, 정보통신망법, 개인정보보호법의 요구사항 및 제한사항 식별 - 전자금융감독규정, 위협대응 행동매뉴얼 등 관련 감독규정 및 매뉴얼 포함 필요
	□ 기술적 요구 사항 식별 - 신뢰성 있는 디지털 증거의 수집, 분석, 보존 기술 식별 · 디지털 포렌식 도구 확보 및 검증제도 확인
	□ 인적 요구사항 식별 - 디지털 포렌식 전문인력 확보(내/외부) · 디지털 포렌식 전문가 자격 검증제도 확인
③ 침해사고 준비도에 따른 IT인프라 구축	□ 디지털 증거 수집·분석 및 보존 정책 수립 - 디지털 증거 수집 및 분석에 대한 절차적 매뉴얼 수립 - 디지털 증거 보존 방법 및 보존 기간에 대한 정책 수립
	□ 시스템 아키텍처 정의 및 구현 - 중요도에 따라 네트워크 구간 분리, 분리된 네트워크 구간별 접속 제한, 정보보호시스템 설치 등 디지털 포렌식 친화적인 시스템 아키텍처 구현
	□ 테스트 및 평가 - 침해사고 유형별로 식별된 디지털 증거의 수집, 분석 가능성을 훈련 등을 통해 테스트 및 평가
	□ 디지털 증거 수집 및 보존 - 디지털 증거가 정해진 정책에 따라 수집·보존이 이루어질 수 있도록 디지털 증거의 수집과 보존을 위한 프로세스 및 인프라를 구축

필요 사항	금융회사 관련 현황
④ 지속적 관리	□ 준비도 정책 관리 체계 수립 - 연간 정보보호 계획 수립시 준비도 정책 관리를 포함 · 준비도 관련 정보보호 규정, 매뉴얼, 가이드 등을 갱신
	□ 지속적인 직원 교육 및 인식 제고 - 직원 정보보호 교육 및 인식제고 프로그램에 침해사고 준비도 관련 프로그램 내용을 반영
	□ 지속적인 모니터링 및 감사 - 정보보호 점검 등의 프로세스에 준비도와 관련된 지속적인 모니터링 및 감사 활동을 포함

4. 금융보안원을 활용한 침해사고 준비도 구축

□ 침해사고 준비도 구축을 위한 디지털 포렌식 전문인력과 전문도구 확보가 어려운 금융회사는 **침해사고 조사 시 침해사고 조사 역량을 갖추고 있는 금융보안원을 적극 활용하여 조사 수행**

□ **금융보안원은 침해사고(포렌식) 전문 인력 및 도구, 방법론을 갖추고 있으며** 침해사고 발생 시 부터 **금융회사와 증거수집 및 포렌식 분석 등 원활한 합동 조사 진행 가능**

※ **침해사고 발생 즉시 증거수집, 포렌식 분석 수행이 되지 않을 경우 신속한 사고원인 파악 및 피해확산 방지에 영향을 줌**

□ 금융보안원 침해사고 대응 연락처

– 전 화 : 02 - 3495 - 9494

– 이메일 : cert@fsec.or.kr

5. 국내·외 침해사고 준비도 현황

가. 해외 현황

국가명	관련 현황
미 국	□ NIST*에서 포렌식과 관련된 표준 가이드를 제공 * NIST(National Institute of Standards and Technology) : 미국 상무부 기술관리국이 운영하는 국립표준기술연구소 - Guide to Integrating Forensic Techniques into Incident Response · 침해사고 대응과 관련된 포렌식 기술 및 포렌식 분석 시나리오 제공 - Computer Security Incident Handling Guide · 침해사고 대응 절차 및 조직 구성, 사고처리 절차, 정보공유 원칙 등을 제시 □ 일부 보안전문 업체에서 침해사고 준비도 개념을 포함한 평가, 진단 및 컨설팅 서비스를 제공 - FireEye : 침해사고 대응 전략, 대응 조직의 역할 및 책임, 탐지·분석 메커니즘 등을 테스트 후 개선방안을 제공 - Symantec : 침해사고 대응 관리적, 기술적 준비도를 평가하고 테스트 후 개선방안을 제공
영 국	□ 정부의 정보취급기관은 의무적으로 포렌식 준비도를 갖추도록 제도화 - 정부 보안정책 프레임워크에 포렌식 준비도를 명시 · (내용) 정보시스템에서 산출되는 데이터를 보존, 분석할 수 있는 **포렌식 준비도 정책이 포함된 정보자산 감사능력**을 갖추어야 함 □ 민간에도 GPG(Good Practice Guide)를 통해 정책 샘플이나 기술적/인적 요구사항, 우수사례 등을 제공

나. 국내 현황

□ 체계적으로 **제도화된 침해사고 준비도 관련 법조항은 없으나**, 정보보호 관련 법률 및 각종 정보보호 평가 및 인증 제도에서 침해사고 대응, 로그관리 등 침해사고 준비도 내용을 다수 포함

— 관련법률 : 전자금융거래법, 전자금융감독규정, 개인정보보호법, 정보통신기반보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등

□ 특히, 금융권은 전자금융거래법, 전자금융감독규정 및 위기대응행동매뉴얼 등에 **침해사고 준비도 개념이 포함되어 있어 침해사고 준비도를 상당부분 구축**

— 전자금융감독규정(12조~18조)은 정보기술 보호대책(단말기, 전산자료 보호대책, 정보처리시스템), 방지대책(해킹, 악성코드 감염) 및 관리대책(공개용 웹서버, IP주소) 규정에서 디지털 증거(로그 등) 획득 및 보존을 명시

— 금융회사 위기대응행동매뉴얼은 침해사고 대응을 위한 조직, 프로세스, 보고 및 정보공유 절차 등을 포함

□ 그러나, 침해사고 대응이 복구중심으로 되어 있어 효과적인 디지털 포렌식을 통한 **신속한 사고원인 파악 및 디지털 증거의 증거능력 확보를 위한 디지털 포렌식 수집과 분석 내용은 보완** 필요

Ⅲ. 금융회사 침해사고 준비도 참조 모델

1. 침해사고 및 디지털 증거 식별

가. 보호자산 식별

구 분	작성 방법
업무 현황	- 기 작성한 업무현황 리스트 활용 가능 · 업무연속성계획(BCP), 인증자료, 업무 참고자료 등 - 자료가 없으면 업무중요도를 고려하여 신규 작성
고객정보 현황	- 기 작성한 고객정보 보유 현황 활용 가능 · 개인정보취급방침, 개인정보영향평가, 업무 참고자료 등 - 자료가 없으면 신규 작성 · 주민번호, 계좌번호, 카드번호 등 중요 정보 보유 현황 포함은 필수
시스템 및 네트워크 현황	- 기 작성한 시스템 및 네트워크 현황 활용 가능 - 자료가 없으면 신규 작성 · 내부망, 인터넷망 및 서버망, 단말기망 등 네트워크 분리를 알아볼 수 있고 정보보호 시스템 및 솔루션 확인이 가능할 수 있도록 작성

나. 침해사고 유형분류

구 분	침해사고 내용
전산자료/ 프로그램 조작	전산시스템에 저장된 데이터 및 프로그램을 조작, 파괴, 은닉하는 행위
정보유출사고	내부직원 또는 협력직원의 악의적인 목적 및 과실에 의해 발생한 정보유출 사고
내부망 해킹	내부 시스템 취약점 또는 연계된 시스템의 취약점으로 발생한 정보유출 및 시스템 마비 사고 등
시스템 위변조	전산시스템을 위변조하여 정상적인 서비스를 방해하는 행위(홈페이지 위변조 등)
디도스 공격	다양한 서비스 거부 공격을 통하여 금융회사의 서비스 구간을 마비시키는 사고

※ '전자금융감독규정 시행세칙' 정보기술부문 및 전자금융사고 보고양식 사고 유형 준용

다. 침해사고 관련 디지털 증거 식별

1) 침해사고 유형별 디지털 증거

사고유형	디지털 증거 및 기록
공통	□ 정보처리 시스템, 네트워크, 단말기 현황 □ 정보보호 시스템, 네트워크, 솔루션 현황 □ 침입 탐지·차단시스템 이벤트 및 탐지 패킷 로그 □ 침입 탐지·차단시스템 정책 및 패치 기록 □ 침해사고 관련 내/외부 네트워크 통신 기록 □ 백신 로그 및 패치 기록 □ 정보처리시스템 시스템 로그 및 패치 기록 □ 정보처리시스템 계정별 접근 및 사용 기록 □ 어플리케이션 설치 및 사용 포트 기록 □ 어플리케이션 로그 및 패치 기록 □ 단말기 하드디스크 이미지 □ 단말기 메모리 정보 등
전산자료/ 프로그램 조작	□ 데이터/프로그램 무결성 검증 기록 등
정보유출사고	□ 전산자료 및 중요파일 접근 기록 □ 이동식저장매체 접속 기록 □ 정보유출방지 시스템 탐지 로그 □ 망간 자료연계 시스템 탐지 로그 □ 인터넷/웹메일 접속 기록 □ 디지털저작권관리시스템/매체제어시스템 감사로그 등
내부망 해킹	□ 스팸 탐지 기록 □ 악성코드 감염 기록 □ 아웃바운드 트래픽 기록 등
시스템 위변조 (웹변조)	□ 웹서버 접속 로그 □ 웹페이지 위변조 확인 기록 □ 웹서버 계정 내역 및 접근 로그 □ 시스템 무결성 검증 기록 □ DB 쿼리 로그 등
디도스 공격	□ 디도스 대응 시스템 정책 및 탐지차단 로그 □ 공격 네트워크 트래픽 샘플 □ 웹서버 접속 로그 등

2) 시스템 종류별 디지털 증거

가. 공통

항 목	디지털 증거 및 기록	확인방법
기본 정보	- OS 정보, 패치정보 - 디스크 정보 - 시스템 시간(CMOS 시간)	운영체제(OS) 기본 명령어
활성 데이터	- 프로세스 정보 - 네트워크 정보	운영체제(OS) 기본 명령어
	- 메모리 덤프	전문 수집도구 이용
비활성 정보	- 설치 프로그램 정보	전문 수집도구 이용
	- 정보보안 프로그램	전문 수집도구 이용
	- 사용자 계정 정보 (예 : 윈도우 : net user/linux : /etc/passwd)	운영체제(OS) 기본 명령어
	- 네트워크 패킷	전문 수집도구 이용

나. 윈도우(Windows)

항 목	디지털 증거 및 기록
레지스트리	설치프로그램 목록, 최근 사용 문서 파일, USB 저장장치 사용 기록, 최근 접근 문서, 최근 접속 인터넷 주소, 최근 실행 명령어, 자동실행 항목 등(system, sam, security, software, default, NTUSER.dat) - 저장 : %SYSTEMROOT%₩System32₩config, C₩Users₩사용자명₩
이벤트 로그	보안/설치/시스템/응용프로그램/하드웨어/PowerShell 이벤트 등 로그 - 저장 : %SYSTEMROOT%₩System32₩winevt
계정(Account) 사용 기록	계정 현황, Last Login, Last Failed Login, Last Password Change, Group Membership, Sucess/Fail Logins, Logon Types, RDP Usage, 비인가계정(Rogue Local Accounts) 등 - 저장 : %SYSTEMROOT%₩System32₩config, C₩Users₩사용자명₩,%SYSTEMROOT%₩System32₩winevt
파일 및 디렉터리 정보	윈도우즈 파일시스템(FAT, NTFS)의 디렉터리 및 파일에 대한 접근, 생성, 수정된 정보 등($MFT, $LogFile, $UsnJrnl) - 포렌식 전문도구로 확인
실행파일 기록	프리패치(Prefetch), 슈퍼패치(Superfetch) - 저장 : %SYSTEMROOT%₩Prefetch
인터넷 접속 기록	웹 히스토리, 쿠키(Cookie), 세션(Session) 정보, 캐시(Cache), download 등 - 저장 : %Profile%AppData₩Local₩Microsoft₩Windows₩
이메일 사용 기록	웹메일, 마이크로소프트 아웃룩(Outlook) 이메일(pst,ost,eml)
파일 복구	크래시 덤프(Crash Dump), 시스템 복원지점(System Restore Point) 복사본 등 - 저장 : %SYSTEMROOT%₩MEMORY.dmp, 시스템 복원 폴더

다. Linux/Unix

항 목	디지털 증거 및 기록
디렉터리 구성 및 파일	기본 실행 파일 및 실행 기록(/bin), 부팅에 필요한 파일(/boot), 시스템 장치 파일(/dev), 시스템 설정 파일(/etc), 사용자 홈 디렉터리(/home), 시스템 공유 라이브러리(/lib), 장치 마운트 경로(/mnt), 시스템 프로세스 특수 파일(/proc), 사용자 설치 경로(/usr), 관리자 홈 디렉터리(/root), 관리자 실행 파일(/sbin), 로그, 프린터 스풀 등 가변 파일(/var)
중요한 서비스 설정 기록	운영체제 및 시스템 서비스(/etc), 개별 어플리케이션은 각각 확인 - 저장 : /etc/passwd, /etc/shadow, /etc/groups, /etc/hosts
작업 스케줄러 (주기적 실행)	cron, at - 저장 : /var/log/cron, /var/spool/at
시스템 로그	접근로그, 에러로그, 감사로그 - 저장 : /usr/adm(AIX), /var/adm(HP-UX), /var/log(SunOS), /var/log(Linux), /secure
사용자별 실행 명령 기록	acct, pacct - 저장 : /var/account/pacct
로그인 기록	사용자별 최종 로그인 시간 기록(lastlog), 로그인 실패 기록(loginlog) - 저장 : /var/log/lastlog
시스템 콘솔 출력 및 syslog 기록	messages - 저장 : /var/log/message
su 명령 사용 기록	sulog - 저장 : /var/log/sulog
현재 로그인 사용자 정보	utmp(x), w 또는 who 명령 - 저장 : /var/log/utmp
로그인/아웃, 시스템 시작/종료 시간 등	wtmp(x), last - 저장 : /var/log/wtmp
FTP 접근기록	xferlog - 저장 : /var/log/xferlog
사용자별 수행한 명령어	history - 저장 : /root/.bash_history

라. 네트워크(Network) 시스템

1) 네트워크 장비 설정 값 및 로그

구 분	디지털 증거 및 기록
스위치	- CAM(Content Addressable Memory) 테이블
라우터	- 라우팅 테이블 - 차단 트래픽 로그(ACL) - 트래픽 량
DHCP 서버	- DHCP 로그 • IP 주소를 할당 받은 장비의 MAC 주소, IP 주소 할당 및 갱신 시간, 호스트 네임 등
네임서버	- DNS 로그 • 조회 시간 및 조회 내역 등
웹프록시	- 웹서핑 로그 - 클라이언트(IP) 별 웹서핑 패턴 - 캐싱된 웹페이지

2) 네트워크 전송 데이터 추출 값

구 분	추출방법	디지털 증거 및 기록
통신케이블	- 케이블 탭핑(Tapping) - 포트 미러링(Mirroring)	- 데이터 통신 패킷 - 관리용 통신 패킷
무선	- 무선인터넷 전송규약 WAP*을 이용하여 수집 * Wireless Application Protocol	- 데이터 통신 패킷 - 관리용 통신 패킷
전문도구	- 전문도구로 우회 통신 환경을 구축하여 데이터 추출	- 데이터 통신 패킷 - 관리용 통신 패킷

마. 정보보호시스템

구 분	디지털 증거 및 기록
공통사항	- 감사 로그(시스템 로그인 정보 등)
침입탐지시스템(IDS)	- 침입 탐지 및 차단 로그 - 패킷 헤더와 플로우 기록 정보, 패킷 페이로드 - 출발지/목적지 IP 주소, TCP/UDP 포트, 네트워크 이벤트 발생 시간
방화벽(F/W)	- 허용 및 차단 정책 - 접근 및 에러 로그
네트워크 접근 제어(NAC 등)	- 네트워크 비정상 행위 탐지 로그(Spoofing 등) - 업데이트 파일 배포 로그 등
서버보안(Secure OS 등)	- 시스템 접속 로그, 중요 파일 실행 로그 - 서버보안 데몬 실행 로그
디도스 대응 시스템	- 트래픽 발생 추이 - 디도스 공격 패킷
USB 통제	- USB 연결 정보
백신	- 악성프로그램 탐지, 삭제 로그
데이터유출방지 시스템(DLP)	- 프로그램 설치 정보, 응용 프로그램 접속 로그, 매체 사용로그
문서암호화관리 시스템(DRM)	- 프로그램 설치 정보, 응용 프로그램 접속 로그, 매체 사용로그
APT탐지시스템	- APT 탐지 로그(유입 실행파일 관련 정보)
DB보안	- 질의 및 응답 관련 로그 - DB 변경 관련 로그
패치관리 서버	- 파일 배포 정보
무선침입방지시스템(WIPS)	- 무선 침입 탐지 및 차단 로그
인증서버	- 로그인 성공/실패 로그 등 인증 관련 로그
이메일 보안	- 비정상 파일이 포함된 이메일 송수신 로그

바. 정보처리시스템

구 분	디지털 증거 및 기록
전자금융 거래 로그	- 전자금융 서비스와 관련한 로그
어플리케이션 로그	- 자체 또는 외주 개발되어 사용하고 있는 어플리케이션 로그
Web	- 웹 접속 및 에러 로그
WAS	- 통신 로그
DB	- 감사 및 질의/응답 로그
Mail	- 메일 필터링 로그
미들웨어	- 미들웨어 로그
SSO	- 계정 정보 및 로그인/아웃 로그

2. 요구사항 식별

가. 법적 요구사항 식별

□ 전자금융감독규정의 침해사고 준비도 관련 규정

구 분	요구사항 주)	전자금융감독 규정 주)
단말기 보호대책	무단조작 방지	제12조 제1호
	단말기 보호	제12조 제2호
	중요단말기 보호	제12조 제3호
	보조기억매체 통제	제12조 제4호
전산자료 보호대책	전산자료 현황 관리	제13조 제1항 제3호
	반출·반입 통제	제13조 제1항 제5호
	보조기억매체 관리	제13조 제1항 제7호
	백업자료 관리	제13조 제1항 제8호
	정보시스템 가동 기록 보존	제13조 제1항 제11호, 제13조 제4항
정보처리시스템 보호대책	장애 기록 관리	제14조 제3호
	모니터링 시스템 구축	제14조 제4호
	중요 패치 수행	제14조 제7호, 제15조 제1항 제2호
	백업·소산 관리	제14조 제8호
정보보호시스템 설치 및 운영	보안정책 승인·적용 이력 보관	제15조 제2항 제3호, 제15조 제3항
	내부통신망과 외부통신망 분리 차단	제15조 제1항 제5호

주) 상세 내용은 「금융IT 보안 컴플라이언스 가이드」(2015. 6.30, 금융보안원) 및 본 가이드 <참고 2> 「전자금융감독규정의 준비도 관련 요구사항 식별」 참조

구 분	요구사항 주)	전자금융감독 규정 주)
악성코드 감염 방지 대책	악성코드 검색 및 치료 프로그램의 최신상태 유지	제16조 제1항 제1호, 제2호
	중요단말기 악성코드 감염 일일 점검	제12조 제3호, 제16조 제1항 제4호
공개서버 보안	공개용 웹서버의 설치 및 접근 통제	제17조 제1항 제1호
	공개용 웹서버 거래로그 관리	제17조 제1항 제4호
	공개용 웹서버 해킹 방지	제17조 제4항
IP주소 관리	내부 IP 주소체계 보안	제18조 제1호, 제2호
	인터넷 접속내역 기록·보관	제18조 제3호
계정 및 권한 관리	사용자 계정 통제	제13조 제1항 제1호, 제4호, 제14호, 제13조 제2항
	외주사용자 계정 통제	제13조 제1항 제2호
정보처리시스템 관리자 통제	정보처리시스템 관리자 통제장치 마련·운용	제13조 제5항
	정보처리시스템 관리자 주요 업무 관련 행위 감시	제13조 제5항, 제28조 제2항
내부사용자 비밀번호 관리	비밀번호 설정·운영	제32조 제1호, 제2호
	비밀번호 시도횟수 제한 및 재부여 절차	제32조 제3호
이용자 비밀번호 관리	이용자 비밀번호 조회 관리	제33조 제1항
	비밀번호 시도횟수 제한 및 재부여 절차	제33조 제2항 제3호
전산원장 통제	부적합 관련기록 보존	제27조 제4항
	작업자 및 작업내용 기록 보존	제27조 제5항

주) 상세 내용은 「금융IT 보안 컴플라이언스 가이드」(2015. 6.30, 금융보안원) 및 본 가이드 <참고 2> 「전자금융감독규정의 준비도 관련 요구사항 식별」 참조

구 분	요구사항 주)	전자금융감독 규정 주)
일괄작업 통제	작업내용 기록·관리	제30조 제4호
	주요업무 관련 행위 모니터링	제30조 제5호
프로그램 통제절차 수립	프로그램 변경 기록·관리	제29조 제2호
전자금융거래 기록·보존	전자금융거래 기록·보존	제38조 전자금융거래법 제22조 제1항, 제2항 전자금융거래법 시행령 제12조 제1항, 제2항
	거래기록 보존 및 보관 요건 준수	전자금융거래법 제22조 제1항 전자금융거래법 시행령 제12조 제3항, 제4항
	보존기관 경과 전자금융거래 기록 파기	전자금융거래법 제22조 제2항, 제3항 전자금융거래법 시행령 제12조 제5항, 제6항

주) 상세 내용은「금융IT 보안 컴플라이언스 가이드」(2015. 6.30, 금융보안원) 및 본 가이드 <참고 2> 「전자금융감독규정의 준비도 관련 요구사항 식별」 참조

나. 기술적 요구사항 식별

1) 디지털 포렌식 도구 검증 제도

가) NIST(미) CFTT(Computer Forensics Tool Test Program)

* NIST(National Institute of Standards and Technology)
: 미국 상무부(United States Department of Commerce) 기술관리국이 운영하는 국립표준기술연구소

□ NIST에서 운영하는 컴퓨터 포렌식 도구 신뢰성 확인 프로그램

□ 목적

— 제조사가 도구를 개선하기 위해 필요한 정보 제공

— 사용자가 포렌식 도구를 선택하는데 필요한 정보 제공

— 사법 등의 분야에서 포렌식 도구 성능을 이해하는데 참조

□ 참조 웹사이트 : http://www.cftt.nist.gov

— 테스트 방법론 및 포렌식 도구 테스트 결과 등 조회 가능

□ 기 타

— 미, 국토안보국(Department of Homeland Security)에서 지원

나) 국내 검증 제도

□ 국내는 법원이나 대검찰청에서 공식적으로 인정하는 포렌식 도구는 없음

□ 2008년 10월 국가디지털포렌식센터가 설립된 이후 EnCase*(미국, Guidance Software社)* 등 검증된 포렌식 전문도구를 이용한 디지털 증거가 법정에 제출되거나 증거로 인정받고 있음

* 검찰, 경찰 등 수사기관에서 주로 사용하고 있으며 금융보안원도 디지털 포렌식 전문도구로 EnCase 등을 사용

2) 주요 포렌식 도구

가) 통합 포렌식 도구

도구명	운영체제	제조사	라이선스
EnCase Forensic	Windows	Guidance Software(미)	상용
FTK	Windows	AccessData (미)	상용
Forensic Explorer	Windows	GetData(미)	상용

나) 활성데이터 수집/분석(Live Forensic) 도구

도구명	운영체제	제조사	라이선스
Argos DFAS	Windows	더존(한국)	상용
Live Response	Windows	e-fense(미)	상용
MIR	Windows	Mandiant(미)	상용

다) 디스크 이미징(복제) 도구

도구명	운영체제	제조사	라이선스
Falcon	-	Logicube(미)	상용
Image MASter Series	-	Intelligent Computer Solution(미)	상용

라) 모바일 포렌식 도구

도구명	운영체제	제조사	라이선스
XRY Series	-	Micro Systemation(미)	상용
UFED	-	Cellebrite(미)	상용

마) 데이터 복구 도구

도구명	제조사	라이선스
Recover My Files Pro	GetData(미)	상용
R-Studio	R-Tools Technology(미)	상용
FinalData	파이널데이터(한국)	상용

3) 공격자 관련 정보획득 사이트

웹사이트	획득정보(무료)
http://whois.kisa.or.kr/kor/	국내 IP 관련 정보
http://www.ip-tracker.org/	해외 IP 관련 정보
https://www.shodan.io/	IP 조회 및 외부 오픈 서비스 정보
http://domainbigdata.com/	도메인, IP, E_mail 관련 정보

다. 인적 요구사항 식별

1) 디지털 포렌식 전문인력 확보 현황

□ 내부 전문인력 : 디지털 포렌식 자격증 소지자 및 관련 경력자 현황 확인

□ 외부 전문인력

- 금융보안원 : 디지털 포렌식 전문역량 보유
  (전문인력, 전문도구 및 방법론 등)
- 정보보호 전문업체(전문인력, 전문도구 보유 확인 필요)

2) 디지털 포렌식 관련 교육 프로그램

기관명	웹사이트	교육과정	자격증
금융보안원	edu.fsec.or.kr	포렌식 기초 및 심화	-
SANS	www.sans.or.kr	포렌식 분석 및 대응 등	GCFA
더존 정보보호 서비스	www.dforensic.co.kr	디지털포렌식 전문가 2급, AccessData(FTK) 공인 교육기관	디지털포렌식 전문가 2급, ACE(FTK)
제트코	www.jetco.co.kr	EnCase 공인 교육기관, FTK 활용 교육 등	EnCE (EnCase)

* 기타 다수 정보보호교육기관에서 디지털 포렌식 교육을 개설

다. 디지털 포렌식 자격 인증제도

(2016년 10월 현재)

구분	자격증	주관기관	특징
국내	디지털 포렌식 전문가 1·2급 (민간자격)	한국포렌식 학회	- 응시자격 : 2급(없음), 1급(디지털 포렌식 전문가 자격증 2급 보유하고, 유관 경력 2년) - 응 시 료 : 2급(필기/실기) : 6만원/12만원 1급(필기/실기) : 10만원/20만원 - 합격기준 : 2급(필기/실기) : 60점/60점 1급(필기/실기) : 60점/60점 - 자격유지 : 2급(1년 유효), 1급(미정)
국외	CCFP	한국 사이버 포렌식협회 (CFPA)	- 응시자격 : IT보안등 관련 경력 3년 이상 - 응 시 료 : US$549 - 합격기준 : 필기(700점) - 자격유지 : 3년
국외	GCFA	GIAC (교육:SANS)	- 응시자격 : 별도 자격 없음 - 응 시 료 : USD 659(교육 포함) - 합격기준 : 필기(69%) - 자격유지 : 3년 유효
국외	ACE	AccessData	- 응시자격 : 별도 자격 없으나, 포렌식 도구(FTK) 기능 및 지식 필요 - 응 시 료 : 교육비에 포함 - 합격기준 : 필기(80%) - 자격유지 : 1년 유효(1년뒤 실기 시험)
국외	EnCE	Guidance Software	- 응시자격 : EnCase 포렌식 교육 64시간 수료 또는 경력 1년 이상 - 응 시 료 : USD 225 - 합격기준 : 필기(80%), 실기(85%) - 자격유지 : 3년 유효

3. 침해사고 준비도에 따른 IT인프라 구축

가. 디지털 증거 수집·분석 정책 수립

1) 디지털 증거처리 표준/디지털 포렌식 가이드라인

가) 디지털 포렌식 절차

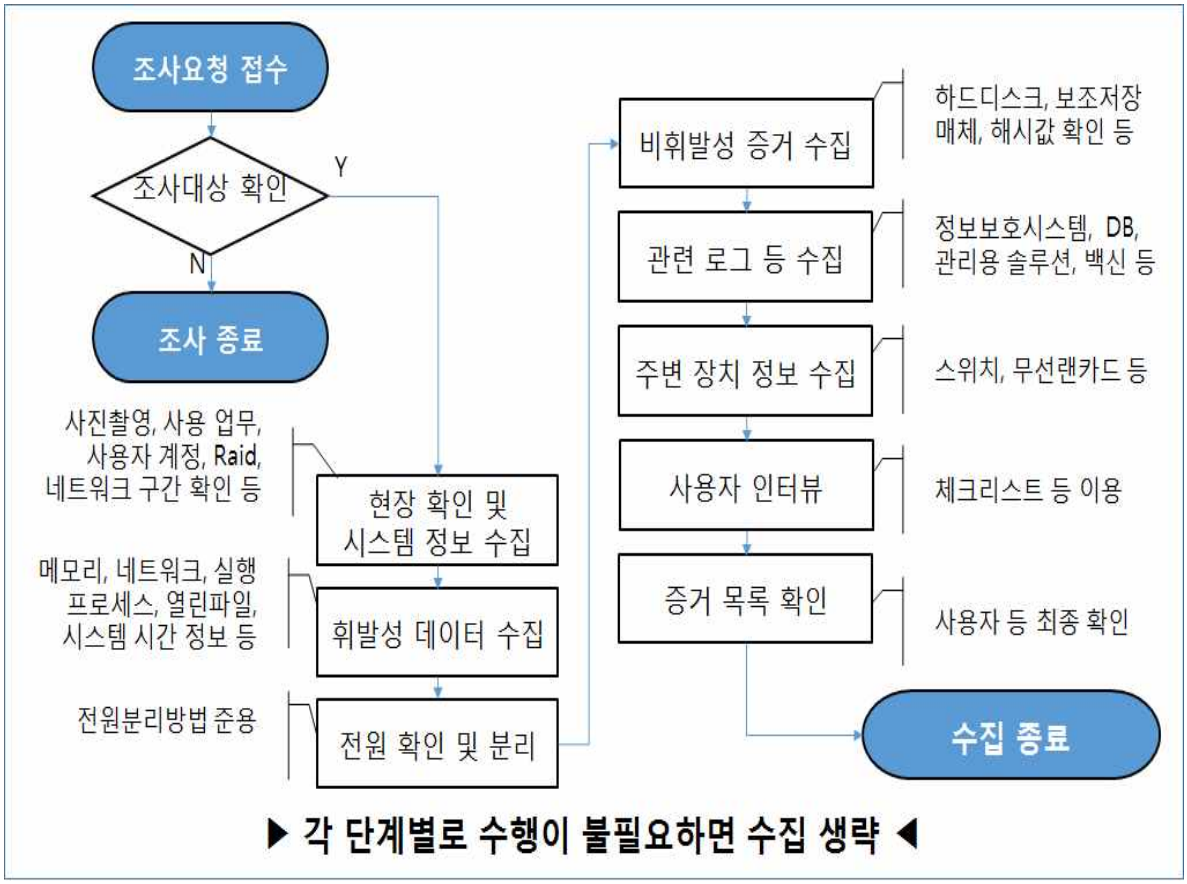
① 사전 준비	- 디지털 포렌식 도구 준비 - 조사 및 증거수집 대상 확인 등
② 디지털 증거 수집	- 디지털 증거 획득 - 원본 확인 및 사본 생성 등
③ 디지털 증거 보관 및 이동	- 안전한 장소에 보관 - 분석 및 보관을 위한 안전한 장소로 이동 등
④ 조사 분석	- 자료복구, 타임라인 확인 및 시그니처 등 분석 - 해시값 생산 및 확인, 관련 로그 분석 등
⑤ 보고서 작성	- 증거 분석결과 확인, 전문가 소견 - 무결성 확인, 담당자/입회인 확인 등

나) 증거수집

□ 기본원칙

적법한 절차의 준수	침해사고 조사에 필요한 범위 내에서 내외부 법률 및 규정에 적법한 절차로 수집
원본의 안전한 보존	쓰기방지장치 등을 이용하여 원본의 변경을 차단하여 수집하고 이송시에는 손상을 방지
증거의 무결성 확보	증거의 변조가 없음을 입증하기 위해 원본과 사본의 해시 값을 생산하여 입회인이 확인

□ 디지털 증거 수집 일반 절차

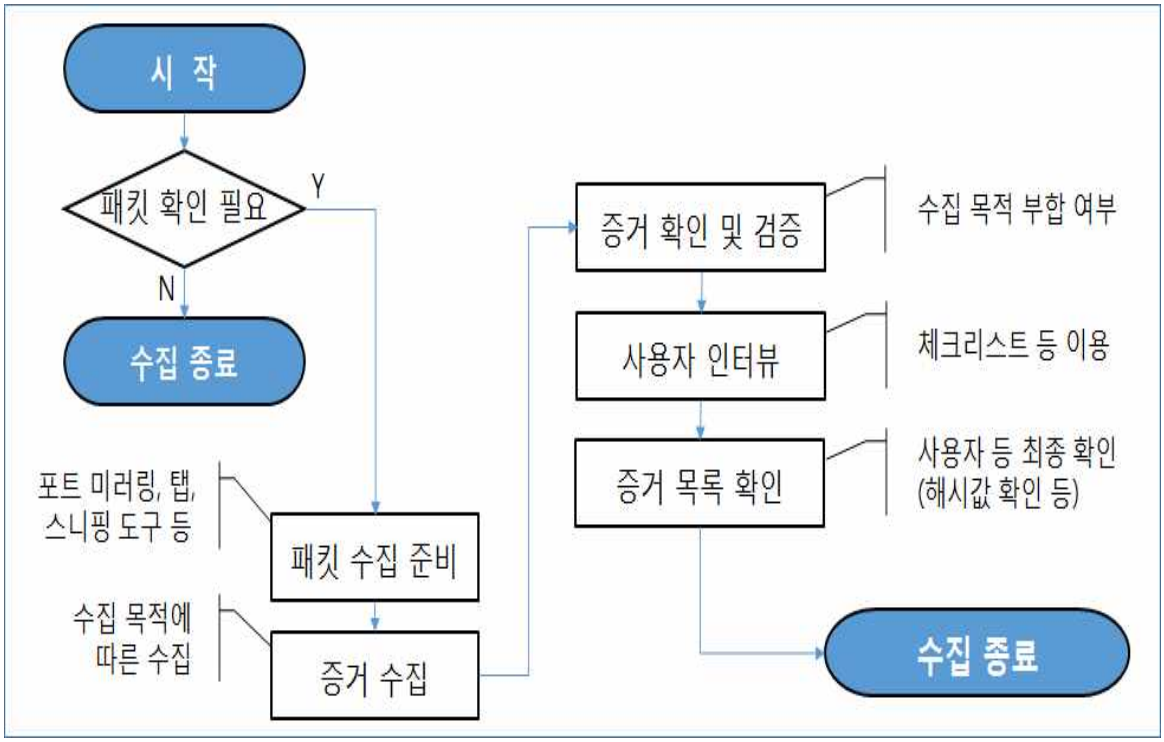


※ 시스템 운영체제별 전원분리방법

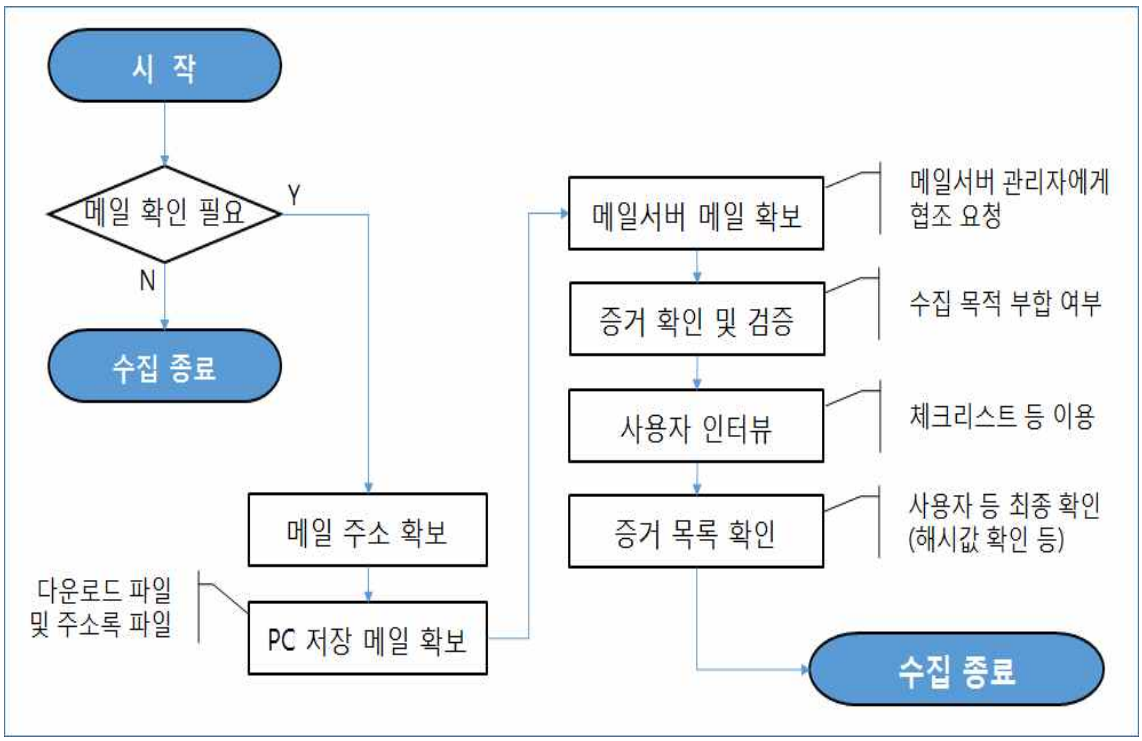
OS	전원분리 방법	비 고
Windows (PC용)	전원 플러그 바로 분리 주)	전원플러그 분리시에는 시스템 본체의 플러그를 제거 (UPS 사용 시스템의 임시데이터 삭제 방지)
Windows (서버)	정상종료 후 전원플러그 분리	
Linux	정상종료 후 전원플러그 분리	
Unix	정상종료 후 전원플러그 분리	
Macintosh	전원 플러그 바로 분리 주)	

주) 정상적인 시스템 종료절차를 수행하면 임시 데이타가 삭제됨

□ 네트워크 증거 수집 절차



□ 이메일 증거 수집 절차



□ 증거수집 준수사항

- 현장도착시 준수사항
  · 수집 시스템이 확인되었으면 각 시스템별 현재 시각과 시스템 시간 일치 여부 확인
  · 수집 시스템에 설치된 소프트웨어 확인
  · 하드웨어나 네트워크를 파악하고 원본의 손상을 방지
  · 수집대상 목록을 검토·확인하여 신속하게 수집

- 증거물 수집시 준수사항
  · 시스템 전원의 On/Off 상태, Raid 구성 여부 등을 확인하여 디지털 증거가 손상되지 않도록 수집
  · 사용자 간섭을 최소화 하여 디지털 증거의 수정을 최소화
  · 활성데이터는 휘발성이 높은 것부터 우선적으로 수집
  · 수집된 데이터나 수행된 작업에 대한 기록은 수집과정이 끝난 후 증거 무결성을 위해 해시값 기록
  · 입회인 등 제3자에 의한 확인을 증빙할 수 있도록 기록

다) 증거분석 의뢰

□ 디지털 증거 분석의뢰
- 디지털 증거물이 변경 내지 멸실되지 않았음을 증명할 수 있도록 조치
- 증거 수집, 이송 과정에서 발생한 상황은 문서화

□ 디지털 증거물 운반 및 이동시 주의사항
- 증거물 유형에 따라 변조나 손상이 되지 않도록 조치를 취한 후 운반 및 이동

라) 증거분석

□ 기본원칙
- 증거원본의 안전한 보존 및 무결성 확보
- 증거분석 기법과 도구의 신뢰성 확보
- 증거분석 과정의 기록
- 증거분석 결과의 신뢰성 확보
  · 제3자가 재분석해도 결과가 일치하여야 함

□ 준비사항
- 분석 장비
  · 증거분석 전용 시스템을 사용하고, 데이터의 무결성 유지를 위하여 인터넷 접속 금지
  · 쓰기방지 장치 등으로 위변조 방지
  · 사용에 익숙하고 신뢰성이 검증된 전문 분석 도구만을 사용
  · 분석결과물을 저장 할 안전한 저장장치를 준비하여 사용
- 분석대상 및 범위 결정
  · 사건개요, 증거물 수집 과정, 분석의 목적 등을 파악하여 분석 대상 및 범위를 결정
- 증거분석 표준 절차
  · 분석대상 디지털 증거물의 유형에 따라 적절한 자료추출 및 분석 표준절차에 따라 증거분석을 실시

마) 결과보고서 작성

□ 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리 정연하게 작성
□ 추정을 배제하고 사실관계를 중심으로 작성
□ 객관적 사실, 설명 내용, 분석가 의견을 구분하여 작성
□ 증거 발견방법 및 분석 과정을 명확하게 기록
□ 분석 및 처리과정을 사진 및 화면캡처 등으로 기록
□ 분석에 사용한 하드웨어 및 소프트웨어는 반드시 기록
□ 법정 증거능력이 필요한 분석결과는 수정이 불가능한 문서자료 형태로 부본을 작성하여, 안전한 장소에 보관

나. 디지털 증거 보존 정책

1) 법규에서 규정한 디지털 증거 보존 기간

대상 로그	법규명	보존기간	비 고
전자금융 거래 기록	전자금융거래법 시행령 (제12조)	5년간 (1만원초과) 1년간 (1만원이하)	
정보처리시스템 가동기록 - 접속, 사용, 자료처리, 오류 기록 등	전자금융 감독규정 (제13조)	1년 이상	금융보안원 취약점 분석평가 점검 항목
이용자 정보조회 내역 - 사용자, 사용일시, 변경 및 조회 내역, 접속방법 등	전자금융 감독규정 (제13조)	1년 이상	금융보안원 취약점 분석평가 점검 항목
OS 및 설정내용 등의 백업, 소산 및 백업자료	전자금융 감독규정 (제14조)	1년 이상	금융보안원 취약점 분석평가 점검 항목
정보보호시스템 책임자 지정운영 및 운영 결과	전자금융 감독규정 (제15조)	1년 이상	금융보안원 취약점 분석평가 점검 항목
내외부 IP 주소의 인터넷 접속 내용	전자금융 감독규정 (제18조)	1년 이상	금융보안원 취약점 분석평가 점검 항목
중요원장의 조회, 수정, 삭제, 삽입한 작업자와 작업내용 기록	전자금융 감독규정 (제27조)	5년 이상	금융보안원 취약점 분석평가 점검 항목
개인정보처리자가 개인정보처리시스템에 접속한 기록	개인정보의 안전성 확보 조치 기준(제8조)	6개월 이상	

2) 기타 침해사고 조사 관련 디지털 증거 보존 권고 기간

대상 로그	보존권고 기 간	보존방법
인터넷 접속 관련 로그	1년 이상	위변조 및 도난 분실이 되지 않도록 안전하게 보관*
개인(금융)정보 접속 관련 로그	1년 이상	〃
정보보호시스템 탐지 로그	1년 이상	〃
서버 및 PC 내 로그	-	시스템 내 자동 보관되며, 중요 시스템은 해당 로그 비활성화 금지 필요
업무용 중요 응용프로그램 로그	1년 이상	위변조 및 도난 분실이 되지 않도록 안전하게 보관

* 로그 중앙관리 시스템, 서면, 마이크로필름, 디스크 또는 자기테이프 등에 보관하며, 해시값 등을 적용하여 원본임을 확인할 수 있도록 하는 조치를 권고

다. 시스템 아키텍처 정의 및 구현

1) 네트워크 구간 분리 및 접근기록 관리

□ 네트워크는 중요도에 따라 분리하고, 분리된 구간 사이는 침입차단시스템 등 정보보호시스템을 설치하여 접근통제 및 접근내역을 기록(Logging)

□ 금융회사 네트워크 구간 분리

번호	네트워크 명칭*	용 도
1	인터넷 연결 구간	주요 전자금융 서비스를 제공하기 위하여 ISP 인터넷과 연결되는 구간
2	DMZ 구간	전자금융 서비스 제공을 위한 웹서버 등이 위치하는 구간
3	전자금융서버구간	DMZ 구간에 위치한 서버들과 통신하는 전자금융 서버들이 위치하는 구간
4	계정계 구간	계정계 HOST 서버 등이 위치하는 구간
5	내부서버 구간	대외에 공개될 필요가 없는 내부 사용자 업무에 필요한 서버들이 위치한 구간
6	개발서버 구간	업무테스트 및 개발을 위한 테스트 서버들이 위치하는 구간
7	내부사용자 구간	내외부 직원 PC(단말기) 등이 위치하는 구간
8	대외연결 구간	각종 금융 서비스의 원활한 제공을 위하여 대외기관이 연결된 구간
9	DR 구간	장애 발생시를 대비하여 구성한 DR센터 구간
10	인터넷 망	직원 인터넷 접속 네트워크로 내부(업무)망과 망분리된 네트워크

*** 금융보안원 금융분야 보안 취약점 점검가이드(네트워크) 준용**

□ 로그는 일정 수준 이상이 누적되면 이전 로그는 삭제되므로 정보보호시스템, NMS 및 EMS 등에 저장된 로그에 대해 관리 실시

예) 정기적 백업 수행, 2차 백업 등

2) 서버 및 어플리케이션 정보 및 운영기록 관리

□ 서버 정보 : 운영체제 버전 및 업데이트, 보안패치, 계정 및 비밀번호, 사용 서비스, 디렉터리 정보

□ 각종 S/W : 버전 및 업데이트, 보안패치, 로그 정보

— Web, WAS, DBMS, Mail, 미들웨어

□ 어플리케이션 : 버전 및 업데이트, 감사 및 로그 정보

— 업무용 어플리케이션

라. 테스트 및 평가

□ 침해사고 대응훈련 시 침해사고 발생을 가정한 침해사고 조사 업무를 포함하고 그 결과를 평가

□ 주요 포함사항

— 침해사고조사팀 구성

— 침해사고 조사에 필요한 기초자료 확보

· 시스템 및 네트워크 현황, 개인(금융)정보 현황, 계정 정보

— 침해사고 조사에 필요한 디지털 증거(로그 등) 확보

· 휘발성/비휘발성 디지털 증거, 네트워크 트래픽 디지털 증거 확보 포함

· 디지털 증거 보존기간의 적정성

— 침해사고 조사·분석 전문인력, 분석장비(H/W, S/W) 확보

— 디지털 증거 수집·분석 및 보고 매뉴얼(절차 및 체크리스트, 비상연락망 등) 존재 등

마. 디지털 증거 수집 및 보존

□ 디지털 증거 수집 및 보존 정책에 따라 디지털 증거를 수집 및 보존하고 주기적으로 테스트 및 평가

4. 지속적 관리

가. 준비도 정책 관리 체계 수립

□ 매년 정보계획 수립 내용에 준비도 정책관리 포함
— 준비도 관련 규정, 매뉴얼, 가이드 등을 갱신
— 디지털 포렌식에 필요한 인력, 도구, 프로세스를 갱신
— 준비도 관련 테스트 및 평가 결과를 반영

나. 지속적인 직원 교육 및 인식 제고

□ 주기적으로 실시하는 정보보호 교육 프로그램에 준비도 관련 내용 포함
— 침해사고 발생시 디지털 증거 보존 및 수집 방법 등
□ 디지털 포렌식 전문인력 양성을 위한 교육프로그램 운영
— 금융보안원 교육센터 등 외부 전문 교육프로그램 활용

다. 지속적인 모니터링 및 감사

□ 정보보호 점검 및 감사활동에 준비도 관련 내용 포함
□ 취약점 분석평가 등 외부 전문가를 통한 준비도 관련 점검 실시

<참고자료 1>

금융회사 침해사고 준비도 체크리스트(안)

Ⅰ. 침해사고 및 디지털 증거 식별 - 1

점검 항목	점검내용	비 고
1. 보호자산 식별		
가. 업무현황	① 업무현황을 문서 및 시스템 조회로 확인할 수 있는가?	
	② 업무현황이 최신 현황으로 관리되고 있는가?	
	③ 업무현황은 중요도에 따라 구분(분류)되어 있는가?	
	④ 업무별 담당자 및 연락처를 확인할 수 있는가?	
나. 고객정보 보유 현황	① 고객정보 보유 현황을 문서 및 시스템 조회로 확인할 수 있는가?	
	② 고객정보 보유 현황이 최신 현황으로 관리되고 있는가?	
	③ 주민번호, 금융정보 등 중요정보 보유현황을 확인할 수 있는가?	
다. 시스템 및 네트워크 현황	① 시스템 및 네트워크 현황을 문서 및 시스템 조회로 확인할 수 있는가?	
	② 시스템 및 네트워크 현황이 최신 현황으로 관리되고 있는가?	
	③ 시스템 및 네트워크 현황이 네트워크 구간별로 확인되는가?	
	④ 시스템 및 네트워크 담당자 현황이 확인되는가?	
2. 침해사고 유형 분류		
–	① 침해사고 유형이 분류/정의되어 있는가?	
	② 침해사고 유형별 조사 방법이 정리되어 있는가?	

Ⅰ. 침해사고 및 디지털 증거 식별 - 2

점검 항목		점검내용	비 고
3. 침해사고 관련 디지털 증거 식별			
가. 침해사고 유형별 디지털 증거	공 통	① 정보시스템 및 어플리케이션에서 획득할 수 있는 디지털 증거가 식별되어 있는가?	
		② 식별된 디지털 증거의 획득이 가능한가?	
	사고 유형별	① 사고 유형별로 침해사고 조사에 필요한 디지털 증거를 식별하고 있는가?	
		② 식별된 디지털 증거의 획득이 가능한가?	
나. 시스템 종류별 디지털 증거 (계 속)	공 통	① 시스템 및 OS 종류별로 디지털 증거는 식별되어 있는가?	
		② 시스템 및 OS 종류별로 디지털 증거가 기본정보, 활성 및 비활성 정보로 구분되어 있는가?	
		③ 시스템 및 OS 종류별 디지털 증거 수집 방법 및 방안을 마련하고 있는가?	
		④ 시스템 및 네트워크 장비 시간이 동기화 되고 있는가?	

Ⅰ. 침해사고 및 디지털 증거 식별 - 3

점검 항목		점검내용	비 고
나. 시스템 종류별 디지털 증거 (계 속)	운영체제(OS)	① 시스템 로그(운영체제, 이벤트, 감사, 접속 등)를 정상적으로 기록하고 있는가?	
		② 시스템 로그가 사용자(계정) 및 사용 내역을 식별할 수 있도록 기록하고 있는가?	
		③ 시스템 로그의 보존기간은 적정한가?	
		④ 시스템 로그를 주기적으로 백업하고 있는가?	
	네트워크	① 네트워크 로그를 정상적으로 기록하고 있는가?	
		② 네트워크 통신 기록, 관리용 통신 기록의 보존기간은 적정한가?	
		③ 네트워크 전송 데이터 값을 추출할 수 있는 방안은 있는가?	
		④ 네트워크 구간에 대해 접근 내역을 확인할 수 있는 방안이 마련되어 있는가?	

Ⅰ. 침해사고 및 디지털 증거 식별 - 4

점검 항목		점검내용	비 고
나. 시스템 종류별 디지털 증거 (계 속)	정보보호 시스템	① 정보보호시스템 로그를 정상적으로 기록하고 있는가?	
		② 정보보호시스템별로 정책 및 탐지 로그 확인이 가능한가?	
		③ 정보보호시스템 로그를 주기적으로 백업하고 있는가?	
	정보처리 시스템	① 전자금융 거래 로그를 정상적으로 기록하고 있는가?	
		② 전자금융 거래 로그의 임의 변조를 방지하고 있는가?	
		③ 전자금융 거래 로그의 보존기간은 적정한가?	
		④ 전자금융 거래 로그를 주기적으로 백업하고 있는가?	
		⑤ 정보처리시스템별로 로그 확인이 가능한가?	
		⑥ 정보처리시스템 로그의 보존기간은 적정한가?	
		⑦ 정보처리시스템 로그를 주기적으로 백업하고 있는가?	

Ⅱ. 요구사항 식별

점검 항목	점검내용	비 고
1. 법적 요구사항 식별		
–	① 법적(관련 규정) 요구사항이 식별하고 있는가?	
	② 법적 요구사항의 충족여부를 확인하고 있는가?	
2. 기술적 요구사항 식별		
–	① 디지털 포렌식 기술적 요구사항을 파악하고 있는가?	
	② 기술적으로 검증받은 디지털 포렌식 전문 도구를 갖추고 있는가?	
	③ 용도별 디지털 포렌식 도구를 보유하고 있는가?	
3. 인적 요구사항 식별		
–	① 디지털 포렌식 전문 인력 자격(자격증, 경력)은 정하고 있는가?	
	② 디지털 포렌식 전문 인력 확보방안은 가지고 있는가?	
	③ 디지털 포렌식 전문가 육성을 위한 교육은 계획하고 있는가?	

Ⅲ. 침해사고 준비도에 따른 IT인프라의 구축 - 1

점검 항목	점검내용	비 고
1. 디지털 증거 수집·분석 정책 수립		
가. 디지털 포렌식 절차	① 디지털 포렌식 절차는 수립되어 있는가?	
	② 디지털 포렌식 절차에 업무 담당자는 지정되어 있는가?	
나. 증거수집	① 디지털 증거의 수집절차는 수립되어 있는가?	
	② 디지털 증거 수집시 지켜야할 준수사항은 정리되어 있는가?	
	③ 디지털 증거 수집절차에 안전한 전원 분리방법은 포함되어 있는가?	
다. 증거분석	① 디지털 증거분석 매뉴얼은 수립되어 있는가?	
	② 디지털 증거분석에 필요한 장비는 준비되어 있는가?	
라. 결과보고서 작성	① 결과보고서 작성 방법은 수립되어 있는가?	
	② 결과보고서에 내용이 누락되지 않고 포함될 수 있도록 하고 있는가?	

Ⅲ. 침해사고 준비도에 따른 IT인프라의 구축 - 2

점검 항목	점검내용	비 고
2. 디지털 증거 보존 정책		
–	① 법규에서 정한 디지털 증거 보존 기간을 준수하고 있는가?	
	② 법규에 포함되지 않은 디지털 증거의 유형을 정의하고 보존기간을 준수하고 있는가?	
	③ 디지털 증거의 보존 방법이 있는가?	
3. 시스템 아키텍처 정의 및 구현		
가. 네트워크 구간 분리 및 접근기록 관리	① 중요도에 따라 네트워크 구간이 분리되어 있는가?	
	② 네트워크 구간별 접근이 통제되고 접근기록을 확인할 수 있는가?	
	③ 네트워크 구간별 접근 기록이 내외부 규정에 따라 보존되고 있는가?	
나. 서버 및 어플리케이션 정보 및 운영기록 관리	① 서버 및 S/W, 업무용 어플리케이션 정보는 파악되어 있는가?	
	② 서버, S/W, 업무용 어플리케이션의 운영기록은 정확하게 관리되고 있는가?	
4. 테스트 및 평가		
–	① 침해사고 조사업무의 원활한 수행을 테스트하고 있는가?	
	② 침해사고 조사업무의 테스트 결과를 평가하고 있는가?	
	③ 침해사고 조사업무의 평가 결과가 조사 업무에 반영되고 있는가?	

Ⅳ. 지속적 관리

점검 항목	점검내용	비 고
1. 준비도 정책 관리체계 수립		
–	① 매년 준비도 정책관리를 하고 있는가?	
	② 준비도 정책관리 내용이 개선되고 있는가?	
2. 지속적인 직원 교육 및 인식 제고		
–	① 침해사고 준비도 관련 교육 계획을 수립하고 있는가?	
	② 주기적으로 침해사고 준비도 관련 교육이 실시되고 있는가?	
	③ 침해사고 준비도 교육 내용은 적정한가?	
3. 지속적인 모니터링 및 감사		
	① 침해사고 준비도를 주기적으로 점검 및 평가하고 있는가?	
	② 침해사고 준비도 점검결과가 업무에 반영되고 있는가?	
	③ 침해사고 준비도 업무수행 결과를 주기적으로 점검/관리 하고 있는가?	

<참고자료 2>

전자금융감독규정의 준비도 관련 요구사항 식별

1) 전자금융감독규정 제12조(단말기 보호대책)

또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다.

1. 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것
2. 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것
3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것
4. 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제할 것

【관련 로그】

□ F/W, IDS, PC보안, 백신 등 정보보호시스템 로그
□ 단말기 OS 및 어플리케이션 로그
□ 단말기 사용자 및 계정별 사용내역, 접근 성공 및 실패 기록
□ 단말기 패치기록 및 로그
□ 단말기 사용 보조기억매체 및 휴대용 전산장비 사용 기록

【관련 현황】

□ 중요단말기 지정 현황
□ 단말기 H/W 및 S/W 현황, 네트워크 구성도
□ 단말기 사용자 및 계정 현황
□ 단말기 사용 보조기억매체 및 휴대용 전산장비 사용 현황

2) 전자금융감독규정 제13조(전산자료 보호대책)

① 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.

1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것
2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것
3. 전산자료의 보유현황을 관리하고 책임자를 지정·운영할 것
4. 전산자료의 입·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것
5. 전산자료 및 전산장비의 반출·반입을 통제할 것
6. 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것
7. 정기적으로 보조기억매체의 보유 현황 및 관리실태를 점검하고 책임자의 확인을 받을 것
8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것
9. 주요 백업 전산자료에 대하여 정기적으로 검증할 것
10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보사용 금지
11. 정보처리시스템의 가동기록은 1년 이상 보존할 것
12. 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것
13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것
14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것

② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.

③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.

④ 1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다.

1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록
3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록

⑤ 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중확인 및 모니터링을 하여야 한다.

【관련 로그】

□ 전산자료(단말, 서버 등)와 관련된 F/W, IDS, DRM, 보안OS, DB보안, 접근관리 등 정보보호시스템 로그
□ 전산자료 사용자 및 계정별 사용내역, 접근 성공 및 실패 기록
□ 전산자료와 패치기록 및 로그
□ 단말기 사용 보조기억매체 및 휴대용 전산장비 사용 기록

【관련 현황】

□ 전산자료 보유 현황(백업 및 소산 내역 포함)
□ 전산자료 관련 H/W 및 S/W 현황, 네트워크 구성도
□ 전산자료 관련 사용자 및 계정 부여, 변경, 삭제 현황
□ 전산자료 입·출 현황(테스트시 사용 포함)
□ 전산자료 관련 보조기억배체 사용 현황

3) 전자금융감독규정 제14조(정보처리시스템 보호대책)

또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다.

1. 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것
2. 데이터베이스관리시스템(Database Management System : DBMS)·운영체제·웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성·보관할 것
3. 정보처리시스템의 장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세하게 작성·보관할 것
4. 정보처리시스템의 정상작동여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능한 모니터링시스템을 갖출 것
5. 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수할 것
6. 정보처리시스템의 책임자를 지정·운영할 것
7. 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 할 것
8. 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록·관리할 것
9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것
10. 정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하고, 이상징후 발생 시 필요한 통제 조치를 즉시 시행할 것

【관련 로그】

☐ F/W, IDS, PC보안, 백신 등 정보보호시스템 로그
☐ 단말기 OS 및 어플리케이션 로그
☐ 단말기 사용자 및 계정별 사용내역, 접근 성공 및 실패 기록
☐ 단말기 패치기록 및 로그
☐ 단말기 사용 보조기억매체 및 휴대용 전산장비 사용 기록

【관련 현황】

☐ 중요단말기 지정 현황
☐ 단말기 H/W 및 S/W 현황, 네트워크 구성도
☐ 단말기 사용자 및 계정 현황
☐ 단말기 사용 보조기억매체 및 휴대용 전산장비 사용 현황

4) 전자금융감독규정 제15조(해킹 등 방지대책)

① 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)
4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)

② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 삭제
2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것
3. 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것
4. 정보보호시스템의 원격관리를 금지하고 주기적으로 작동 상태를 점검할 것
5. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것

③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.

④ 금융회사 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.

⑤ 삭제

⑥ 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다.

1. 무선통신망 이용 업무는 최소한으로 국한하고 법 제21조의2에 따른 정보보호최고책임자의 승인을 받아 사전에 지정할 것
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것
4. 비인가 무선접속장비(Access Point : AP) 설치·접속여부, 중요 정보 노출 여부를 주기적으로 점검할 것

【관련 로그】

☐ F/W, IDS, PC보안, 백신 등 정보보호시스템 로그
☐ NMS, WIPS 등 유무선 네트워크 관리 및 정보보호시스템 로그
☐ 디도스 대응 시스템 정책 및 차단 로그

【관련 현황】

☐ 네트워크 망분리 현황
☐ 서비스 및 포트 허용 정책 현황
☐ 내부 네트워크 파일 배부 및 무결성 검증 현황
☐ 무선 통신 사용 현황
☐ 무선 통신 보안대책 적용 현황
☐ 패치 적용 및 관리 현황
☐ 원격관리 금지 및 작동 상태 점검 현황
☐ 백업 및 복구 절차 수립 시행 현황
☐ 보안정책의 등록, 변경 및 삭제에 대한 이력 현황
☐ 비인가 무선접속장비(Access Point : AP) 설치·접속 현황
☐ 중요 정보 노출여부를 주기적 점검 현황

5) 전자금융감독규정 제16조(악성코드 감염 방지대책)

① 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다.

1. 응용프로그램을 사용할 때에는 악성코드 검색프로그램 등으로 진단 및 치료 후 사용할 것
2. 악성코드 검색 및 치료프로그램은 최신상태로 유지할 것
3. 악성코드 감염에 대비하여 복구 절차를 마련할 것
4. 제12조제3호에 따른 중요 단말기는 악성코드 감염여부를 매일 점검할 것

② 금융회사 또는 전자금융업자는 악성코드 감염이 발견된 경우 악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치를 신속하게 취하여야 한다.

【관련 로그】

□ 안티바이러스 시스템 및 프로그램(백신 등) 로그

□ NMS, WIPS 등 유무선 네트워크 관리 및 정보보호시스템 로그

【관련 현황】

□ 안티바이러스 시스템 및 프로그램 적용 현황

□ 안티바이러스 프로그램 패치 현황

□ 악성코드 대응 방안

□ 악성코드 점검 및 감염시 조치 현황

6) 전자금융감독규정 제17조(홈페이지 등 공개용 웹서버 관리대책)

① 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간")에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것
2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것 (다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.

1. 게시자료에 대한 사전 내부통제 실시
2. 무기명 또는 가명에 의한 게시 금지
3. 홈페이지에 자료를 게시하는 담당자의 지정·운용
4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치

③ 삭제

④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다.

⑤ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

【관련 로그】

□ F/W, IDS, PC보안, 백신 등 정보보호시스템 로그

□ 단말기 외부인터넷 접속 로그

【관련 정보】

□ 공개용 웹서버 운영 및 추가 인증 수단 적용 현황

□ 공개용 웹서버 제공 서비스 현황

□ 홈페이지 자료게시 담당자 현황

□ 웹서버 해킹 대응 및 단말기 악성 사이트 접근 통제대책 현황

7) 전자금융감독규정 제18조(IP주소 관리대책)

또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다.

1. 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소 사용 등으로 보안을 강화하며 내부 IP주소체계의 외부유출을 금지할 것
2. 개인별로 내부 IP주소를 부여하여 유지·관리할 것
3. 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관할 것
4. 정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP주소를 사용할 것. 다만, 외부직원 등과의 공동작업 수행 등 네트워크의 분리가 어렵다고 금융감독원장이 정하는 경우에는 업무특성별로 접근권한을 분리하여 IP주소를 사용할 수 있다.
5. 내부통신망은 다른 기관 내부통신망과 분리하여 사용할 것

【관련 로그】

□ 내부 IP주소 및 외부 IP주소의 인터넷 접속내용 로그(1년 이상)

【관련 정보】

□ IP주소 관리 및 부여 현황

□ 내부통신망과 다른 기관 내부통신망 분리·사용 현황

<참 고> 정보보호 관련 법률 현황

법령·법규 명	관련 내용
정보통신기반 보호법	제4장 주요정보통신기반시설의 보호 및 침해사고 대응에서 침해사고의 통지(제13조), 복구조치(제14조), 대책본부 구성(제15조), 정보공유·분석센터(제16조) 등 침해대응 관련 내용을 규정하고 시행령에 세부 절차 및 방법을 규정
정보통신망 이용촉진 및 정보보호 등에 관한 법률	법, 제27조의 3(개인정보 누출 등의 통지·신고), 제48조의 2(침해사고의 대응 등), 제48조의 3(침해사고의 신고 등), 제48조의 4(침해사고의 원인 분석)에서 침해사고 관련 통지·신고 및 대응업무 내용을 규정하고 시행령에 세부 절차 및 방법을 규정
개인정보 보호법	제34조(개인정보 유출 통지 등)에서 개인정보 유출 사고 발생 시 통지 및 신고 관련 내용을 규정하고 시행령에 세부 절차 및 방법을 규정
전자금융 거래법	제21조의 5(침해사고의 통지 등), 제21조의 6(침해사고의 대응)에서 침해사고 발생 시 통지 및 대응 관련 내용을 규정하고 시행령에 세부 절차 및 방법을 규정
전자금융 감독규정	제15조(해킹 등 방지대책), 제16조(악성코드 감염 방지대책), 제23조(비상대책 등의 수립·운용), 제24조(비상대응 훈련 실시), 제37조의 4(침해사고대응기관 지정 및 업무범위 등), 제73조(정보기술부문 및 전자금융 사고보고)에서 침해사고 관련 통지 및 대응업무 내용을 규정하고 시행세칙에 세부 절차 및 방법을 규정
<금융위원회> 금융전산분야 위기대응 실무매뉴얼	국가위기관리기본지침, 재난 및 안전관리기본법, 전자금융거래법, 정보통신기반보호법에 근거하여 위기 유형별로 위기경보 수준별 조치사항, 위기대응 조치 및 절차를 규정한 금융위원회 실무 매뉴얼
<각 금융회사> 위기대응 행동매뉴얼	[금융위원회] 금융전산분야 위기대응 실무매뉴얼에 근거하여 위기 유형별로 각 참가기관의 위기경보 수준별 조치사항, 위기대응 조치 및 절차를 규정한 개별 금융회사 위기대응 실무 매뉴얼