㈜클라우드 침해사고관리지침은 클라우드컴퓨팅서비스를 제공하기 위한 운영문서로서 검토되고 승인됨	구분	직위	성명	일자	서명
	승인	정보보호 최고책임자	홍길동	2019.01.01	
	검토	정보보호 담당자	장길산	2019.01.01	

㈜클라우드
침해사고 관리지침

2019. 01. 01

㈜클라우드

문서 제·개정 이력				
번호	날짜	쪽	내용	담당자
1	2019-01-01	-	최초 작성	홍길동

본 문서는 침해사고관리지침에 대한 예시이며, 클라우드컴퓨팅서비스 제공자는 자사의 서비스 형태, 운영환경 등을 고려하여 작성하여야 한다.

제1장 총칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 침해사고에 대한 관리에 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 지침은 ㈜클라우드의 클라우드컴퓨팅서비스 업무에 종사하는 임직원 및 ㈜클라우드와 계약을 맺어 클라우드컴퓨팅서비스 업무를 수행하는 외부업체 직원 모두에게 적용된다.

제3조(용어정의) 이 지침에서 사용되는 용어 정의는 다음 각 호와 같다.

1. “침해사고”라 함은 보안정책에 위배되는 모든 사고를 말하며 보안 침해사고, 소프트웨어 이상 및 오류, 악성코드 등으로 인한 정보자산의 손상 등을 포함한다.
2. “악성코드”라 함은 컴퓨터바이러스와 달리 다른 파일을 감염시키지는 않지만, 악의적인 용도로 사용될 수 있는 유해 프로그램을 말한다.
3. “백도어”라 함은 시스템의 정상적인 보호 수단을 우회할 수 있는 숨겨진 메커니즘을 의미한다.

제2장 침해사고 대응절차 및 체계

제4조(침해사고 대응 절차 수립) ① 침해사고의 정의 및 범위, 긴급연락체계 구축, 침해사고 발생시 보고 및 대응 절차, 사고 복구조직의 구성 등을 포함한 침해사고 대응절차를 수립하여야 한다.

② 침해사고를 유형 및 중요도에 따라 분류하고 분류에 따른 이에 따른 보고체계를 정의하여야 한다.

③ 침해사고 대응체계를 외부 기관을 통해 구축한 경우 수립된 침해사고 대응절차 및 체계를 계약서에 반영하여야 한다.

④ 침해사고의 모니터링, 대응 및 처리와 관련되어 외부 전문가, 전문업체, 전문기관(KISA) 등과의 연락 및 협조체계를 수립하여야 한다.

제5조(침해사고 예방) ① 정보시스템별 담당자는 필요 시 국가정보원과 협의하여 현장방문 또는 원격 측정을 통하여 사이버안전대책 이행 여부와 정보통신망의 안정성 여부를 확인한다.

② 정보시스템별 담당자는 보안관제시스템 또는 오프라인 등을 통해 사이버 위협 정보를 인지한 경우에는 초동조치 후 관련 기관에게 신속히 통지한다.

③ 정보시스템별 담당자는 보안정보, 보안권고문, 또는 취약점 분석정보를 수시로 수집하여 보안업데이트 및 대응조치를 수행하고, 직원들에게 배포한다.

제6조(침해사고 대응 훈련) ① 침해사고 대응절차에 관한 연 1회 이상 모의훈련 계획을 수립하고 이에 따라 주기적으로 훈련 실시 및 적정성과 효과성을 평가하여야 한다.

② 이용자가 클라우드 서비스 제공자의 침해사고 대응 모의훈련의 결과를 요청할 경우 이를 문서화하여 제공하여야 한다.

제7조(침해사고 보고) ① 외부로부터의 침해시도가 의심되는 이상징후를 지체없이 인지할 수 있도록 다음과 같은 항목이 포함된 모니터링 절차를 수립하여 이행하여야 한다.

1. 모니터링 대상범위 : 침해시도 탐지 및 차단하기 위한 각종 정보보호시스템 이벤트 로그 등
2. 모니터링 방법 : 외부 전문업체를 통한 모니터링, 자체 모니터링 체계 구축 등
3. 담당자 및 책임자 지정
4. 모니터링 결과 보고체계
5. 침해시도 발견 시 대응절차 등

② 클라우드컴퓨팅서비스 상의 침해사고 징후 또는 침해사고 발생을 인지한 경우 침해사고 보고절차에 따라 신속하게 보고하여야 한다.

- 침해사고가 조직에 미치는 영향이 심각할 경우 최고 경영진에게 신속히 보고
- 침해사고 초기 대응 및 증거 보존 조치

③ 침해사고 발생 시 법률이나 규정 등에 따라 관계기관에 신고하여야 하며 개인정보와 관련한 침해사고는 이용자(정보주체)에게 신속하게 통지하여야 한다.

제8조(침해사고 대응) ① 정보보호 침해사고 접수 후 정보시스템별 담당자는 침해사고 유형별로 다음 각 호의 절차에 따라 대응한다.

1. 침해사고가 확대되지 않도록 침해당한 서버의 네트워크 분리, 공격 포트의 차단 등 필요한 응급조치를 먼저 취한다.
2. 침해사고의 확산을 막기 위해 해당 정보시스템의 중단이 통계청 전체 업무에 영향을 미치는 경우 업무시간 종료 후에 서비스를 중단하며, 해당 정보시스템의 중단이 일부 업무에 영향을 미치는 경우에는 해당 업무부서와 협의 후 즉시 해당 정보시스템을 중단시킨다.
3. 응급조치 후 정보보호 침해사고의 원인 분석 및 증거확보를 위하여 해당 침해사고 관련 로그 및 제반 증거자료를 수집 및 확보해야 한다.
4. 국가정보원 등에서 권고하는 유형별 대응 조치를 취하고, 추후 재발방지를 위한 교육 등 대응책을 마련해야 한다.

② 정보보호 침해사고 유형에 따라 다음과 같이 구분한다.

1. 악성코드 공격
2. 서비스거부 공격
3. 비인가접근 공격

4. 복합구성 공격

제9조(비상연락체계 구축) ① 업무별 시스템 담당자 및 관련 외부 사업자(PM)의 이름과 연락처를 상시 관리하여야 하며, 정보보호 관련 상주 근무자, 외부 유지보수 협력업체, 유관기관 등 비상연락체계를 비치하고, 주기적으로 비상연락망을 점검한다.

제10조(침해사고 분석) ① 정보보호 관리자는 보안사고로 인한 피해를 최소화하기 위해 보안사고 유형 및 등급에 따라 보안사고 대응팀을 구성하고, 정보보호 최고책임자의 승인을 받는다.

② 보안사고 대응팀은 다음 각 호에 따라 보안사고 분석 및 로그 수집을 수행한다.

- 서버 및 네트워크 담당자와 정보보호 담당자는 보안사고 내용을 분석하여 침입 사실, 사고원인 등을 파악한다.
- 서버 및 네트워크 담당자는 증거확보를 위해 현재 보유하고 있는 로그 중 침입흔적을 담은 모든 로그를 백업한다.
- 파일시스템은 상세한 수준으로 덤프를 받은 후, 서명, 일시 등을 기록하고, 덤프파일은 안전한 곳에 보관한다.
- 정보보호 담당자는 정보보호시스템 로그를 점검하여 관련기록을 모두 백업받고 안전한 곳에 보관한다.
- 재침입의 위험이 있다고 판단될 때에는 네트워크 접속을 끊거나 단일 사용자(Single-User)모드에서 작업해야 한다.

③ 침입자가 현재 시스템에 침투해 해킹을 하고 있는 것으로 판단된 경우에는 다음과 같은 조치를 즉시 취한다.

- 정보보호 담당자는 정보보호 관리자에게 보고함과 동시에 즉시 해당 시스템을 네트워크와 분리한 후, 정보보호 최고책임자의 결정에 따라 추적여부를 결정한다.
- 침입 후 활동하는 내용이 치명적이지 않다고 판단되는 경우 정보보호 최고책임자의 승인하에 로그 분석을 통하여 침입위치 및 침입대상을 추적한다.
- 침입자를 추적할 수 없거나, 해킹으로부터 시스템의 보호가 우선이라고 판단되는 경우 접속을 차단하여야 한다.

④ 정보보호 관리자는 보안사고 분석 및 대응 업무 수행 중 필요에 따라 외부기관의 협조를 받을 수 있다. 이때 협조 의뢰의 최종결정은 정보보호 최고책임자가 한다.

제11조(증거수집 및 보존) ① 서버 및 네트워크 담당자와 정보보호 담당자는 제10조에서 분석 및 수집한 증거를 정보보호 관리자에게 전달한다.

② 정보보호 관리자는 침입자 처벌 및 법률적 대응을 위해, 수집된 증거를 사고발생 후 공소시효까지 안전하게 보존하여야 한다.

제12조(결과보고 및 공유) ① 침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알려야 한다. 또한 유사한 침해사고에 대한 신속한 처리를 위해 침해사고 관련 정보 및 발견된 취약점을 관련 조직 및 임직원과 공유하여야 한다.

② 정보보호 담당자는 보안사고대응팀의 각 관련 부서에서 조치결과를 취합하여 그 결과를 정보보호 관리자에게 보고하며, 정보보호 관리자는 보안사고 1, 2급에 대하여 보안사고 조치 보고서를 다음 각 호와 같이 작성하여 정보보호 최고책임자에게 사고 경과와 조치사항을 보고한다.

- 보안사고 분석결과
- 보안사고 대응내역
- 조치계획 및 조치내역
- 재발방지 방안 및 계획

③ 개인정보 사고의 경우 보안사고대응팀은 사고 종료 시까지 다음 각 호의 사항에 대해 상시 모니터링 및 대응을 수행한다.

- 고객이나 언론의 동향 분석
- 법률 Risk 파악
- 피해고객 구제방안 모색 등 사고대응 활동

④ 개인정보 유출사고의 경우 개인정보관리 담당자는 해당 정보주체에게 다음 각 호의 사항을 포함하여 유출사실을 통보하여야 한다.

- 유출 등이 된 개인정보 항목
- 유출 등이 발생한 시점과 그 경위
- 정보주체가 취할 수 있는 조치
- 회사의 대응조치 및 피해 구제절차
- 정보주체가 상담 등을 접수할 수 있는 부서 및 연락처

⑤ 정보주체의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 제3항 각 호의 통보항목을 인터넷 홈페이지에 30일 이상 게시하여야 한다.

제13조(사후관리) ① 정보보호 관리자는 유사한 사고의 재발 방지를 위하여 관련 정책 및 지침의 개정, 정보보호시스템 도입, 유관기관 협조체계 구축 등 효과적인 재발방지 대책을 수립하여야 하고, 필요 시 보안사고 대응절차에 대한 내용을 변경하여야 한다.

② 정보보호 관리자는 수립된 재발방지 대책을 보고하여 동일 또는 유사 사고의 재발에 대비하여야 하며 보안사고의 대응 및 복구가 완료되었음을 확인하여야 한다.

③ 정보보호 담당자는 1, 2 등급의 보안사고 관련된 기록을 대외비 이상 등급으로 분류하고, 이를 보존・관리하여야 한다.

④ 법적 또는 규정상 보안사고 관련하여 대외기관의 요청이 있는 경우 대외협력 관련부서는 정보보호 관리자와 협의 후 대응하여야 한다.

⑤ 정보보호 관리자는 보안사고에 대한 정보와 발견된 취약점들을 관련 부서 및 임직원들에게 공유 및 전파하여야 한다.

[별지 제1호 서식]침해사고 대응결과 보고서

침해사고 대응결과 보고서

결재	정보보호 관리자	정보보호 책임자	정보보호 최고책임자

침해사고 대응 보고서에는 다음과 같은 내용이 포함되어 작성되어야 한다.

□ 침해사고 발생 일시/종료 일시

□ 침해사고 발견 및 피해사항

□ 침해사고 조치 내용

✓침입시도 IP Address

✓침입시도 방법

✓침해사고 분석 방법

✓침해사고 복구 방법

□ 침해사고 영향 범위 (침해사고가 발생한 시스템/피해내역)

□ 침해사고 예방 및 재발방지 대책

[별지 제2호 서식]비상연락망

비상연락망

1. 보안사고대응팀 연락망

담당업무	담당자	연락처

2. 관련부서연락망

부서명	담당자	담당업무	연락처

3. 관련업체 연락망

업체명	담당자	담당업무	연락처

4. 관계기관 연락망

기관명	담당자	담당업무	연락처