침해사고대응매뉴얼

문서번호: 가비아-MN-10

개정번호: VERSION 1.8

정보보호 책임자	정보보호 최고책임자

문서개정이력

개정번호	제/개정일자	담당자	개정내용
Ver 1.0	2017.03.09	안광해	정보보호최고책임자 승인/매뉴얼 시행
Ver 1.1	2017.04.19	안광해	이행심사 조치 사항 처리 제7조 침해사고 대응 절차 내용 개정 제8조 2항 예외적용 책임자 변경 기존: 정보보호관리자, 개정: 정보보호최고책임자
Ver 1.2	2017.10.11	안광해	조직 체계 변경으로 인한 침해사고 대응 체계 변경
Ver 1.3	2018.07.09	안광해	별지1. 침해사고 비상 연락망 유관기관 연락처 변경
Ver 1.4	2018.09.04	안광해	별지1. 침해사고 비상 연락망 변경
Ver 1.5	2019.02.26	안광해	조직체계 변동으로 인한 내용 변경 별지1. 침해사고 비상 연락망 변경
Ver 1.6	2019.08.27	안광해	조직체계 변동으로 인한 내용 변경 별지1. 침해사고 비상 연락망 변경
Ver 1.7	2020.02.24	정명도	조직체계 변동으로 인한 내용 변경 별지1. 침해사고 비상 연락망 변경
Ver 1.8	2020.11.16	정명도	퇴사자로 인한 내용 변경 별지 1. 침해사고 비상 연락망

목 차

제 1 조 (목적)

본 매뉴얼은 g 클라우드에서 발생하는 사이버 침해사고를 신속하게 대응하기 위한 준비와 대응을 기술하여 침해사고로부터의 피해를 최소화하고 후속 보안대책을 세울 수 있도록 하는데 그 목적이 있다.

제 2 조 (정의 및 범위)

적용 범위는 g 클라우드를 운영(기술) / 개발 / 관리하는 모든 직원을 포함하며, 이에 사고접수, 조치, 대응을 할 수 있는 정보보안팀, 보안 IDC 운영팀을 포함한다.

① "침해사고"라 함은 정보통신시스템을 대상으로 관련 규정에 위배되는 사건이나 해킹, 컴퓨터 웜.바이러스, 서비스거부, 비인가된 접근, 정보시스템의 오남용(비인가된 사용) 등을 말하며 정상적인 업무에 지장을 초래하는 사고를 말한다.

② "사이버침해사고대응팀"이라 함은 CERT(Computer Emergency Response Team)라고도 하며 해킹 또는 바이러스 사고 발생에 사고의 분석, 처리, 사후복구, 사후 예방 조치 등을 주요 업무로 하는 정보보안 조직을 말한다.

③ "사이버 공격"이라 함은 해킹.컴퓨터 바이러스. 논리폭탄. 메일폭탄. 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법 침입. 교란. 마비. 파괴하거나 정보를 절취. 훼손하는 일체의 사이버공격 행위를 말한다.

④ "백도어(Backdoor)"이라 함은 시스템의 보안설정을 우회할 수 있는 비밀 통로로서 서비스 술자나 유지보수개발자들의 접근편의를 위해 고의적으로 만들어 놓은 것을 말하며 악의적인 목적을 가진 공격자가 시스템 보안 후 해당 시스템의 재 보안을 목적으로 만들어 놓은 것을 포함한다.

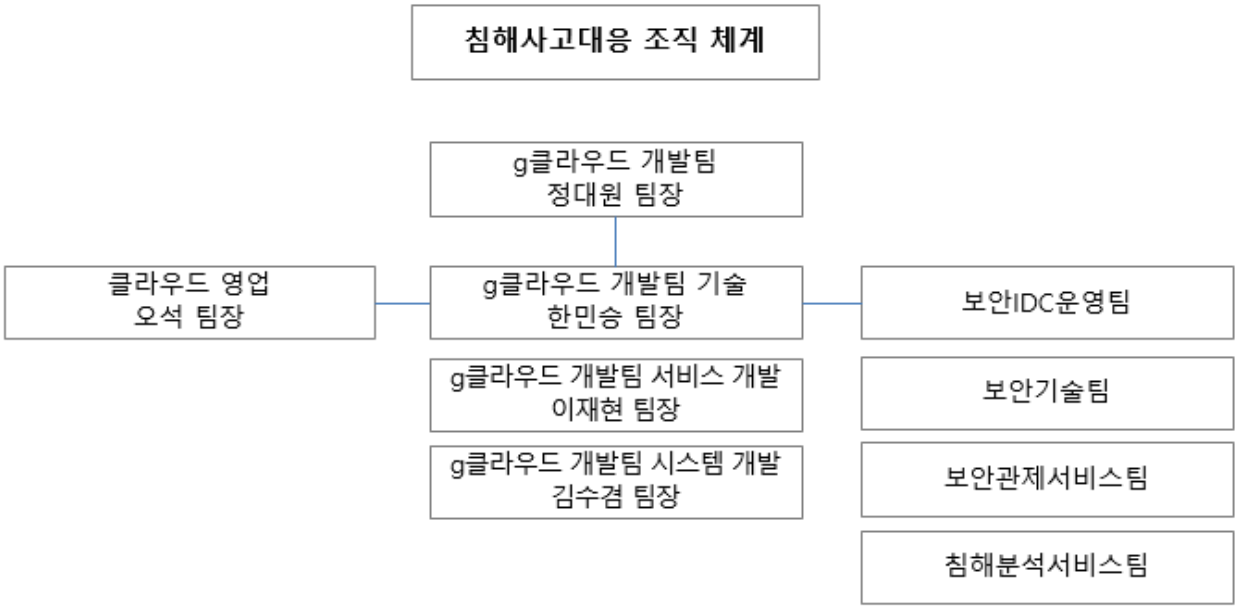
제 3 조 침해사고 대응 조직체계

① 침해사고 대응팀은 보안IDC운영팀의 보안기술팀과 보안 관제 서비스팀, 침해 분석 서비스팀으로 구성한다

② g클라우드 운영(기술) 및 개발팀은 침해사고 대응팀의 보안정책 및 요구사항에 대해서 적극적으로 협력하여 침해사고와 관련된 보안사고에 대해서 대응할 수 있도록 한다.

③ 클라우드IDC사업팀는 관련 사고 발생 시 고객 응대, 제반 시설 등을 지원할 수 있도록 한다.

④ 정보보안팀은 필요에 따라 원인 분석을 같이 하고 이후 재발방지를 위한 방안을 마련한다



구분	업무 요약
클라우드 영업	- 고객 안내 및 상황 전파
클라우드 기술	- 침해사고 대응팀 업무지원 - 관련 로그 증적 확보 - 사고 조치
보안IDC운영팀	- 사고접수, 원인 조사, 및 조치 가이드라인 - 클라우드 사업본부 보고

제 4 조 인력 구성 책임

① 보안IDC 운영팀의 팀장은 실무책임자로 침해사고대응 업무를 총괄하여 빠른 사고대응 업무가 가능하도록 한다. 회사 내의 타 부서 및 관계 기관과의 업무조율 역할과 대내외의 침해사고 대응팀과의 협력관계를 구축하여야 한다.

1) 기관의 대내외 업무 조율을 위한 실무 대표자 역할을 하며, 주로 사고 대응을 위한 대내외 협력 업무에 대한 연락처로써의 역할을 수행한다.

2) 해킹 및 바이러스 등의 침해사고 접수, 사고 할당, 사고 접수 자료에 대한 관리 및 보안사고의 초기 접수에서 사고 여부의 초기 판단 업무를 수행 한다.

3) 해킹사고 발생 시, 해당사고를 정확히 분석하고 대응할 수 있는 사고분석 전문 역할을 수행한다.

② 클라우드 영업(클라우드IDC사업팀)은 보안IDC운영팀 및 클라우드 기술 업무에 필요한 인적・물적 자원을 지원 하여야 하며, 고객의 침해사고 대응 안내 및 회사 내 상황전파를 통해 확산에 방지하는 역할을 수행한다.

③ 클라우드 운영(기술)은 침해사고에 필요한 로그 증적 자료 확보, 서버 네트워크 격리, 침해사고조치 등 침해사고대응팀이 필요한 업무를 적극적으로 지원하며, 사고 상황 등급에 따라 비상연락망 체계를 가동하여 피해를 최소화 할 수 있도록 지원 업무를 수행한다.

제5조 침해사고의 종류

침해사고의 종류에는 비 인가된 시스템 사용 또는 사용자의 계정 도용, 악성코드 유입 및 실행, 정보서비스의 방행 등이 해당되며, 다음과 같이 종류를 구분할 수 있다.

① 악성프로그램 유포 : 제작자가 의도적으로 다른 정보시스템 이용자에게 피해를 주는 악의적 목적으로 만든 프로그램 및 실행 가능한 코드를 의미한다.
"악성코드"라 표현하기도 하며, E-mail, 메신저, 문서의 매크로 기능 등을 이용하여 악성 프로그램을 실행시키고 공격에 사용한다. 주요 형태로는 컴퓨터 바이러스, 인터넷 웜, 트로이 목마 등이 공격에 이용된다.

② 서비스거부 공격(DoS, Denial of Service) : 시스템 또는 네트워크 서비스의 정상적인 운영을 방해하는 공격으로, 시스템을 다운시키거나 네트워크에 과부하의 트래픽을 유발 시켜 사용자들이 서비스를 이용하지 못하게 하는 공격이다.

③ 시스템 침입(비 인가된 접근) : 시스템 또는 네트워크의 취약성을 이용하여 시스템을 침입 하는 공격이다. 보통 특정 취약점을 공격하는 해킹프로그램을 이용하거나, 잘못된 서버 운영상의 문제를 이용하여 시스템에 침입한다.

④ 오·남용 : 시스템 및 네트워크 자원을 허가 받지 않은 방법으로 사용하거나 악용하는 공격 이다. 스팸메일을 보낼 때 다른 사이트의 시스템을 이용하는 방법이나 다른 사람의 계정을 도용하는 행위 등이 대표적인 예이다.

⑤ 정보수집 : 특정 사이트의 시스템 및 네트워크에 대한 정보를 수집하기 위한 공격으로 포트스캔, 전화번호 스캔 등이 있다. 공격자는 정보수집을 통해 특정 사이트에 어떠한 시스템이 존재하는지, 어떠한 서비스가 제공되는지, 어떠한 네트워크 구조를 갖고 있는지, 그리고 어떠한 취약성이 있는지를 조사하게 된다.

제 6 조 침해사고 판단 기준

① 웜/바이러스 및 해킹 등의 공격에 의해 피해 받은 대상 및 피해범위의 확산 범위를 기준으로 사용한다.

② 피해범위의 분류는 다음과 같다.

1) 개별 시스템(PC 및 정보시스템 포함)

2) 단일 네트워크 내의 시스템군

3) 2개 이상 개별 네트워크 내의 시스템군

③ 피해상황과 업무영향에 따라 다음과 같이 침해사고 등급을 정한다.

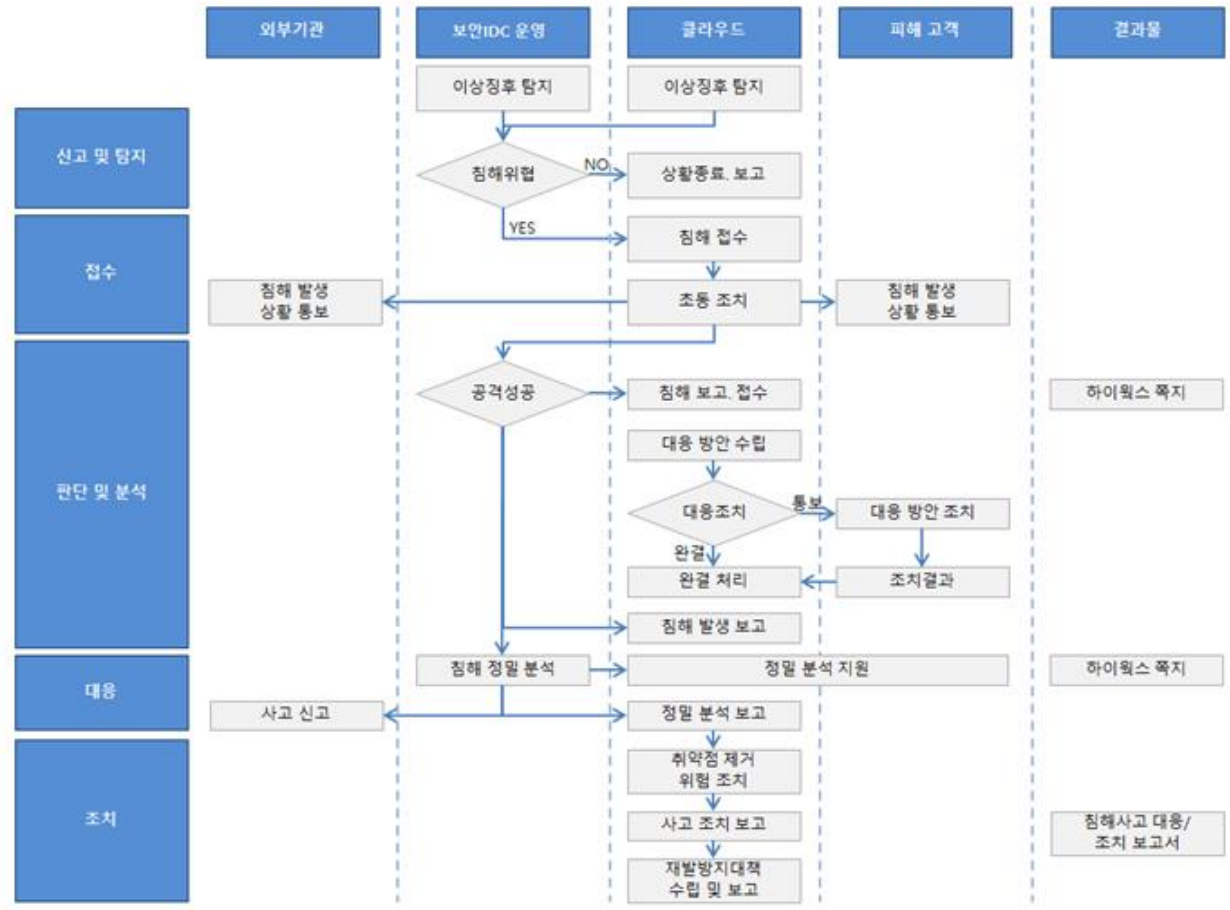
구분	피 해 상 황	업무 영향	보고범위
1등급 (심각)	- 국가적 차원의 네트워크 및 정보시스템 이용 불가 - 전체 정보시스템에 대한 침해사고나 지속적인 공격 발생 - 서버렉, 건물 화재 또는 붕괴 - 정전 또는 인터넷 회선 장애(12시간 이상) - 주요 정보통신기반시설 침해사고 발생	핵심서비스 업무중단 또는 전체업무에 중대한 영향초래	정대원 팀장 오석 팀장 한민승 팀장 장기훈 팀장 김상태 팀장
2등급 (경계)	- 개별서버에 대한 침해사고나 지속적인 공격 발생 - 일부기관에서 침해사고 발생, 다수기관으로 확산 - 외부기관(NIS, KISA) 침해사고조사 - 언론 부정적보도(정보유출, 해킹, 위변조 등) - 정전 또는 인터넷 회선 장애(1~12시간) - 주요 정보통신기반시설 운영기관 침해사고 발생	기관업무중단 또는 일부업무 활동 영향 초래	오석 팀장 한민승 팀장 장기훈 팀장
3등급 (주의)	- 업무에 지속적인 영향 없고 정보시스템에 일시적 문제발생 - 외부기관(KISA, NIS) 자료요청 - 해외 사이버공격 피해 확산으로 국내 유입 우려 상황 전파 - 정전 또는 인터넷 회선 장애(60분이내)	기관업무영향 없으나 시스 템 문제발생,	한민승 팀장 장기훈 팀장
4등급 (관심)	- 해외 사이버공격 피해 확산으로 국내 유입 우려 상황 전파 - 위험도가 높은 바이러스, 취약점 및 해킹기법 출현 - 개인PC의 랜섬웨어, 악성코드 등 이상징후 발견	침해사고 이상징후 탐 지	한민승 팀장 보안 기술팀 보안관제서비스팀 침해사고분석서비스팀

④ 침해사고 등급에 따른 주요 조치사항은 다음과 같다.

구분	주요 조치사항	비 고
1등급 (심각)	. 침해사고 긴급 대응팀 구성.운영 . 피해발생 가능성이 높은 네트워크 단절 . 전기관 PC 사용 최소화 권고 . 공격대상 서비스 포트 자체 차단	
2등급 (경계)	. 침해사고 긴급 대응팀 구성.운영 . 집중 모니터링 대상에 대한 보안취약점 재점검 . 서비스거부 공격에 대한 이상 징후 포착 시 공격 차단 . 정보시스템 긴급 백업	
3등급 (주의)	. 사고 발생 정보자산 감시 . 정보보호시스템 보안정책 점검 및 유해 패턴 경로 감시 . 정보시스템 긴급 백업 . 사이버보안관제 운영 강화 및 유관기관 공조체계 점검	
4등급 (관심)	. 주기적인 악성코드 점검 . 새로운 악성코드, 취약점, 악용공격도구 정보 파악 . 취약점이 발표된 소프트웨어는 보안패치 적용 또는 업데이트 . 불필요한 서비스 점검.차단 및 백신프로그램 최신 업데이트	

제 7 조 침해사고 대응 절차

① 침해사고 대응 세부 업무 흐름도



② 신고 및 탐지

가. 사고 신고

- g클라우드 개발팀의 클라우드 기술(운영)팀이 보안IDC운영팀의 보안기술팀 등에게 침해사고 신고를 한다.

나. (보안IDC운영팀 보안 기술팀 및 보안관제서비스팀) 이상징후 탐지

- 보안IDC운영팀 보안 기술팀 및 보안관제서비스팀은 침해예방 활동을 위한 모니터링을 상시 수행

하며 이상징후를 탐지한다.

다. (g클라우드 개발팀 클라우드 기술(운영)팀) 이상징후 탐지

- g클라우드 개발팀 클라우드 기술(운영)팀은 침해예방 활동을 위한 모니터링을 상시 수행하며 이상징후를 탐지한다.
- g클라우드 개발팀 클라우드 기술(운영)팀은 보안IDC운영팀의 보안 기술팀 등에게 이를 유선 또는 E-mail로 통지하고, 침해위협 여부 확인을 의뢰한다.

라. 침해위협 여부 판단

- 보안IDC운영팀의 보안 기술팀 등은 침해위협 여부를 판단한다.
- 침해위협이 아닐 경우, 보안IDC운영팀의 보안 기술팀 등은 이상징후 탐지를 교정하고, "위험도: 관심으로 E-mail을 g클라우드 개발팀 클라우드 기술(운영)팀에게 보내며, 상황을 종료 한다.

마. 지침에 따른 통지

- 침해사고가 발생하면 보안IDC운영팀 보안 기술팀 등은 '침해사고대응지침 제11조(대외업무)'에 따라 이용자 통지, 유관기관 연락 등을 진행해야 한다. 실제 외부기관을 포함한 비상연락망은 별지 1. 침해사고비상연락망을 참고한다.

※. 참고) 침해위협 모니터링 판단 CASE

- 권한 없는 사용자의 지속적인 인증 시도
- 지속적인 1:1 프로토콜 취약점 공격 발생
- 의심스러운 행동
- 취약점 탐색 행위
- IDS 이벤트 조합을 통한 탐지
- 기타 외부 기관과 사전 협의된 이벤트

③ 접수

가. 침해 접수

- "신고 및 탐지" 단계에서 침해위협이 발생하였다고 판단한 경우, 보안IDC운영팀 보안 기술팀 등은 g클라우드 개발팀 클라우드 기술(운영)팀에게 침해 접수 내용을 유선 또는 E-mail로 통보한다.

나. 초동 조치

- g클라우드 개발팀 기술(운영)팀은 해당 시스템 피해고객에 침해위협 발생 사실을 통보하고, 원칙적으로 네트워크를 차단하며, 시스템을 최대한 유지, 보존하도록 안내한다.
- 네트워크 차단은 물리적으로 해당 시스템의 네트워크 포트를 제거하거나, 방화벽에서 송수신을 차단한다.

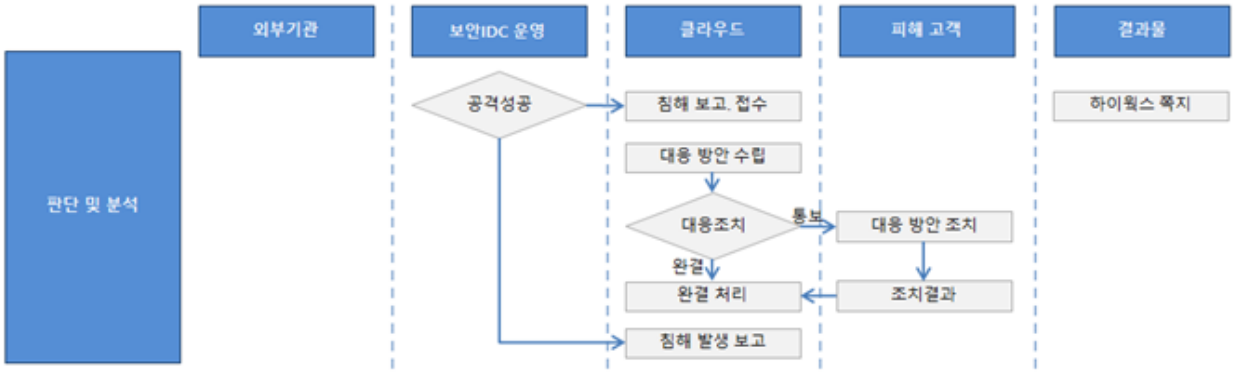
다. 공격성공 여부 의뢰

- g클라우드 개발팀 기술(운영)팀은 접수된 침해위협에 대하여 공격이 성공하였는지 여부를 보안IDC 운영팀 보안기술팀 등에게 의뢰한다.
- g클라우드 개발팀 기술(운영)팀은 침해대상 시스템에 대한 정보를 최대한 제공한다.

※. 참고) 침해대상 시스템 제공 정보, 하이웍스 쪽지 요약 보고

- O.S.타입
- Patch 여부
- 버전 정보
- Application S/W 사용여부 및 종류
- 방화벽, IPS, IDS 상관관계

④ 판단 및 분석



가. 공격성공 여부 판단

- 보안IDC운영팀 보안 기술팀은 침해위협에 대하여 공격성공 여부를 판단한다.

나. 침해 보고 접수

- 보안IDC운영팀 보안 기술팀 등은 공격이 성공하였다고 판단될 경우, 즉시 g클라우드 개발팀 기술(운영)팀에 침해 보고를 접수하고, 동시에 "대응" 단계로써 보안IDC운영팀 침해분석서비스팀에 정밀 분석을 의뢰한다.

다. 대응방안 수립

- g클라우드 개발팀 기술(운영)팀은 접수 받은 침해위협발생에 대한 대응방안을 수립한다.

라. (클라우드 기술(운영)팀) 대응방안 조치)

- 해당 시스템이 g클라우드 개발팀 기술(운영)팀에서 관리 하에 있는 경우, 클라우드 기술(운영)팀은 해당 대응방안 조치를 직접 수행한다.

마. (피해고객) 대응방안 조치 및 결과 통보

- 해당 시스템이 g클라우드 개발팀 기술(운영)팀에서 관리 하지 않는 있는 경우, g클라우드 개발팀 기술(운영)팀은 해당 침해위협발생 사실을 피해고객에게 전달하고, 대응방안 조치를 안내하며, 결과통보를 의뢰한다.

바. 침해 발생 보고

- 보안IDC운영팀 보안기술팀 등은 공격이 실패하였다고 판단될 경우, g클라우드 개발팀 기술(운영)팀에게 "위험도:관심"의 침해 발생 사항을 유선 또는 E-mail로 보고한다.

⑤ 대응

가. (침해사고대응팀) 침해사고 분석/대응

- 보안IDC운영팀 침해분석서비스팀은 침해사고 정밀 분석을 실시한다. 분석 중에 필요하다고 판단되면 바로 처리(대응)한다. 처리(대응)은 피해 프로그램 제거, 피해상황 원복 등이 있다.
- 침해사고 분석 및 대응은 해당 사고의 판단되는 위험도에 따라 방문처리 또는, 원격에서의 처리 등이 있다.
- 침해사고 "위험도:경계"의 경우, 방화벽에서 제한적으로 해당 시스템에 접근하도록 하여 원격에서 처리할 수 있다.
- 침해대응 위험도가 가장 높은 단계인 "위험도:위험"의 경우, 해당 시스템은 네트워크 접근을 봉쇄하고, 방문하여 처리함을 원칙으로 한다.

나. (g클라우드 개발팀 기술(운영)팀/피해고객) 침해사고분석 지원

- g클라우드 개발팀 기술(운영)팀과 피해고객은 보안IDC운영팀 보안 기술팀 등의 침해사고 분석을 지원한다.
- 침해사고분석 지원은 시스템에 대한 통제, 처리(대응), 정보제공 그리고, 피해고객과의 유기적인 협조 유지 등이 있다.

다. 침해사고 정밀 분석 보고

- 보안IDC운영팀 침해분석서비스팀의 침해사고 정밀 분석이 완료되면, 보안IDC운영실 보안 기술팀은 침해사고 정밀 분석 보고서를 g클라우드 개발팀 기술(운영)팀에 제공한다.
- 침해사고 내역 중 이용자 정보가 유출된 경우, '침해사고대응지침 제11조(대외업무)'에 따라 이용자

통지, 외부기관 연락 등을 진행해야 한다. 실제 외부기관을 포함한 비상연락망은 별지 1. 침해사고 비상연락망을 참고한다.

※. 참고) 별지 3. 침해사고 처리결과 보고서

⑥ 조치

가. 취약점 제거

- 접수한 정밀 분석 보고서에 따라 취약점을 제거한다.
- 이때, 서비스 수행에 영향을 주지 않으면서 취약점을 제거하거나, 부득이 영향을 끼칠 수밖에 없다면 그것을 최소화하여야 한다.
- 이 과정에서 서비스 불가 상황, 복구를 위한 백업데이터나 시스템 정보를 보유하고 있지 않는 상황이 발생(또는, 파악)될 수 있으며, 이 경우에는 서비스 중요도와 복구 소요 시간 등을 감안하여 수행계획을 수립하고 조치하여야 한다.

나. 위험 조치

- 최종 위험 조치를 시행하고 서비스 재개를 결정하여 실행한다.
- 위험 조치는 해당 시스템에 대하여 유사한 방법에 의한 또 다른 침해사고가 발생하지 않도록 하는 모든 예방활동을 말한다.

다. 침해사고 조치 보고

- 해당 침해사고조치 결과에 대하여 "침해사고 조치 보고"를 간략히 작성하여 내부에 보고한다.

라. 재발방지대책 수립 및 보고

- 차후 동일 사안으로 침해사고가 발생하지 않도록 재발방지대책을 수립하고 내부에 보고한다.

제 8 조 침해사고 통지 내용 및 방법

① 침해사고의 통지

다음 각 호에 해당하는 경우, 지체없이 그 사실을 이용자에게 알려야 한다.

가. 정보통신망 이용척진 및 정보보호 등에 관한 법률에 따른 침해사고 발생 시

나. 이용자 정보가 유출 된 때

② 통지방법

침해사고 발생 시, 다음의 방법 중 또는 이와 유사한 방법 중 하나를 선택하여 이용자에게 지체없이 통보하여야 한다.

가. 유/무선 전화
나. 우편
다. 전자우편
라. 문자메시지
마. 클라우드컴퓨팅서비스 접속 화면 게시

③ 통지내용

가. 침해사고에 대한 통지 시, 침해사고의 발생경위, 피해범위, 복구예정시간 등을 안내하고 피해확산 방지를 위한 g클라우드의 조치사항과 이용자가 취할 수 있는 방안에 대하여 안내를 해야한다.
나. 침해사고에 대한 문의, 신고 등을 접수할 수 있는 담당부서 및 연락처를 안내해야한다.
다. 개인정보침해사고 시에는 다음의 각 호의 내용을 통지하여야 한다.
- 유출된 개인정보의 항목
- 유출된 시점과 그 경위
- 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
- 유출사고에 대한 g클라우드 대응조치 및 피해구제절차
- g클라우드 이용자에게 피해가 발생한 경우 신고 등을 접수 할 수 있는 담당부서 및 연락처

④ 피해확산 방지를 위한 g클라우드 및 g클라우드 이용자의 조치

가. g클라우드는 피해확산 방지를 위하여 침해사고 범위의 네트워크를 차단하여 피해확산 방지를 위한 조치 수행한다.
나. g클라우드는 침해사고 범위의 상/하단으로 침해확산 방지를 위한 보안시스템의 차단룰에 대하여 검토하고 적용할 수 있도록 해야한다.
다. g클라우드는 침해사고 범위에 있는 시스템의 계정/패스워드 정보를 갱신하여 피해범위의 확산을 방지해야한다.
라. g클라우드는 피해확산 방지 및 복구를 위하여 관련 백업정보를 확인하고 복원할 수 있도록 준비해야한다.

마. g클라우드 이용자는 서비스의 계정 및 패스워드 정보를 갱신하여 피해범위의 확산을 방지해야한다.

제 9 조 부칙

① 시행일

본 매뉴얼은 정보보호최고책임자의 승인일부터 시행된다.

② 예외적용

다음 각 호에 해당하는 경우에는 본 매뉴얼에 명시한 내용일지라도 정보보호 최고 책임자의 승인을 받아 예외 취급할 수 있다.

1) 기술환경의 변화로 적용이 불가능할 경우
2) 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있을 경우
3) 기타 재해 등 불가항력적인 상황일 경우

별지 1. 침해사고 비상 연락망

침해사고 비상연락망

1. 정보보안팀

담당업무	담당자	연락처
정보보안팀	김상태 팀장	010-5671-5081
정보보안팀 보안정책팀	정명도 팀장	010-4402-8862
정보보안팀 보안정책팀	김문선	010-2077-2657
정보보안실 보안정책팀	최성원	010-2711-0434
정보보안실 보안정책팀	안광해	010-4708-9249
정보보안팀 보안분석팀	정윤성 팀장	010-6773-6663
정보보안팀 보안분석팀	김민주	010-7652-2530
정보보안팀 보안분석팀	이유희	010-4388-8834
정보보안팀 보안분석팀	최진열	010-2948-2324

2. 보안IDC운영팀

담당업무	담당자	연락처
보안 IDC 운영실 보안관제대표번호	-	02-2039-5337
보안 IDC 운영팀 실무조직 구성원	장기훈 팀장	010-6345-5137
보안 IDC 운영팀 실무조직 구성원	신준호	010-9722-2283
보안 IDC 운영팀 실무조직 구성원	정한영	010-4533-2475
보안 IDC 운영팀 실무조직 구성원	최재호	010-2744-6495
보안 IDC 운영팀 실무조직 구성원	양민철	010-2005-2256
보안 IDC 운영팀 실무조직 구성원	김영규 팀장	010-3745-9684
보안 IDC 운영팀 실무조직 구성원	이준석	010-9533-6744
보안 IDC 운영팀 실무조직 구성원	장미희	010-2265-6685
보안 IDC 운영팀 실무조직 구성원	한창훈	010-8985-5984
보안 IDC 운영팀 실무조직 구성원	장관희	010-9697-7110
보안 IDC 운영팀 실무조직 구성원	윤태균	010-9268-5042
보안 IDC 운영팀 실무조직 구성원	여선수	010-9095-5998
보안 IDC 운영팀 실무조직 구성원	성창경	010-2695-9733

보안 IDC 운영팀 실무조직 구성원	손현구	010-8493-1257
보안 IDC 운영팀 실무조직 구성원	이종진	010-4846-8067
보안 IDC 운영팀 실무조직 구성원	배재영	010-7753-9131
보안 IDC 운영팀 실무조직 구성원	박성민	010-8425-0759
보안 IDC 운영팀 실무조직 구성원	신규아	010-2045-2901
보안 IDC 운영팀 실무조직 구성원	유준현	010-9315-9309
보안 IDC 운영팀 실무조직 구성원	하혜민	010-2686-4306
보안 IDC 운영팀 실무조직 구성원	홍완의	010-2089-3804
보안 IDC 운영팀 실무조직 구성원	신동수	010-3847-3914
보안 IDC 운영팀 실무조직 구성원	전득상 팀장	010-8867-3767

3. g클라우드 개발팀

부서	담당자	연락처
g클라우드 개발팀	정대원 팀장	010-7315-8446
g클라우드 개발팀 클라우드 기술팀	한민승 팀장	010-3132-4351
g클라우드 개발팀 클라우드 서비스개발팀	이재현 팀장	010-3426-6804
g 클라우드 개발팀 클라우드 시스템개발팀	김수겸 팀장	010-2513-7285

4. 클라우드 IDC 사업팀

부서	담당자	연락처
클라우드 IDC 사업팀 사업2팀	오석 팀장	010-5095-5769

5. 유관 기관 연락망

기관	담당자	연락처(E-mail, HP, office)	URL
KISA	대표전화	118	https://www.kisa.or.kr https://www.krcert.or.kr
경찰청 사이버안전국	대표전화	182	http://cyberbureau.police.go.kr
방통위	대표전화	02-2110-2114	www.kcc.go.kr
관할 경찰서(분당)	대표전화	031-786-5233 (사이버과)	-
관할 소방서(분당)	대표전화	119 우선/ 031-8018-3114	-
CONCERT	대표전화	02-3474-2490	https://www.concert.or.kr
과학기술정보통신부	대표전화	1335 / 야간: 02-2110-2152~3	https://www. msit.go.kr
국가정보원	대표전화	111	https://www.nis.go.kr:4016

별지 2. 침해사고 관리목록

침해사고 관리목록

침해사고 번호	접수일자	처리일자	상태	처리자	담당자	비고

별지 3. 침해사고 처리결과 보고서

침해사고 처리결과 보고서

승인	정보보호담당자	정보보호관리자

1. 개요

1.1 사고 개요

발생일시	
최초 보고일시	
최초 보고자(성명/소속)	
사고 내용	
사고 대응 시작일시	
사고 대응 종료일시	

1.2 사고 총평

2. 수행 내역

2.1. 점검 기간

0000년 00월 00일

2.2 점검 인력

소 속	직 급	이 름	연 락 처
㈜ 가비아 0000	대리	홍 길 동	02-829-3000

2.3 점검 대상

번호	IP 주소	용 도	OS	비 고
1	111.111.111.111	XXXX	XXXXXXX	-

2.4 점검 결과

번호	점검 항목	점검 결과
1	공격자 정보	XXXXXXX
2	웹 로그	XXXXXXX
3	시스템 로그	XXXXXXX
4	악성파일	XXXXXXX
5	취약점	XXXXXXX

2.5 침해사고 처리 경과(Time Table)

시간	수행 작업
09:00	사고 인지(최초 인지부서: 00000)

3. 상세 분석 및 발생원인/재발방지 대책