방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2011.10.13.(목
丶

보도자료

2011년10월13일(목) 배포 시점부터 보도하여 주시기 바랍니다.

문의 : 네트워크정책국 네트워크정보보호팀 이상훈 팀장(☎750-2750)
네트워크정보보호팀 송미라 사무관(☎750-2757)

방통위, '클라우드 보안' 안내서 마련 · 배포

- 안전한 클라우드 서비스 제공·이용을 위한 『클라우드 서비스 정보보호 안내서』 발간 -

방송통신위원회와 한국인터넷진흥원은 클라우드 서비스를 안전하게 제공·이용하기 위해 고려해야 할 보안대책을 담은 「클라우드 서비스 정보보호 안내서」를 발간한다고 밝혔다.

클라우드 서비스는 '11년 상반기에 개인 이용자가 1,030만 명을 넘는 등 최근 국내외 각종 설문조사에서 가장 주목받고 있는 IT기술로 손꼽히고 있으며 미래 IT의 핵심산업으로 주목받고 있다.

그러나 아마존, 구글, 마이크로소프트 등 해외 클라우드 서비스에서 서비스 중단과 같은 장애 사고가 발생함에 따라 클라우드 서비스의 안정적 운영과 이용에 대한 요구가 증대되고 있는 실정이다.

이에 따라 방통위는 클라우드 서비스 제공자와 이용자가 실질적으로 활용할 수 있는 클라우드 서비스 정보보호 안내서를 산·학·연 클라우드 전문가들과의 논의를 통해 마련하게 되었다.

안내서는 서비스 제공 측면에서 ▲네트워크 이중화 및 인증, 이용자 데이터의 암호화 등을 포함한 기술적/관리적 보안대책을 담고 있다. 또한 서비스 이용 측면에서 ▲서비스 선택 기준, 사업자별 보안정책

확인 사항, 안전한 이용방법 등을 포함하고 있다.

방통위는 클라우드 정보보호 안내서 발간을 통해 정보보호기준을 제시함으로써 사업자와 이용자의 자발적 보안대책 마련과 클라우드 보안에 대한 인식을 높이는데 기여할 것으로 기대하고 있다.

아울러 방송통신위원회와 한국인터넷진흥원은 안전한 클라우드 서비스의 보급 활성화를 위해 연말까지 국내 클라우드 서비스 실태 파악을 위한 사업자 정보보호 현황조사를 완료할 계획이며, 보안원천기술 개발 및 산업체 기술이전 등 사업자 지원책을 지속적으로 모색해 나갈 예정이다.

※ 동 안내서는 클라우드 서비스 사업자, 기업이용자에게 배포할 예정이며, KISA 홈페이지(www.kisa.or.kr) 자료실에서 다운로드 받을 수 있음

붙임 : 클라우드 서비스 정보보호 안내서 주요내용 및 목차

<붙임>

「클라우드 서비스 정보보호 안내서」 주요 내용

□ 개요

o 안전한 클라우드 서비스 환경 조성을 위한 서비스 제공자 및 이용자의 정보보호 고려사항을 제시

□ 안내서 주요 내용

o **(보안위협)** 가상화, 자원공유, 정보위탁, 접속단말의 다양성 등 클라우드 서비스의 특성으로 인한 대규모 서비스 장애, 정보 유출 등의 위협 존재

- 서비스 장애에 따른 연계 서비스의 연쇄적 중단 등 피해 대규모화
- IT자원 공유 특성에 따른 해킹, 설정 오류로 인한 정보 유출 및 손실
- 복수 사용자의 IT자원 공유에 따른 악성코드 감염 확산·가속화
- 다양한 접속 단말 등에 따라 비인가 사용자의 불법적 자원접근 가능성

o **(제공자 대책)** 클라우드 서비스 장애 및 침해사고 발생 가능성을 최소화하고 피해확산 방지를 위한 관리적·기술적 정보보호 대책 마련

- 제공자의 보안관리 책임 등 클라우드 서비스 모델(IaaS, PaaS, SaaS)의 특성에 따른 정보보호정책 수립
- 이용자 정보처리 서버 및 스토리지 위치, 관련 준거법률 등을 포함한 이용약관 수립·게시
- 지리적으로 분리된 데이터센터간의 안전한 데이터 송·수신을 위한 네트워크 보안 강화
- 가상화 환경의 정보보호 모니터링 및 시스템 보안 강화기술 적용

o **(기업 이용자 대책)** 기업의 운영 목표 및 IT환경에 적합한 클라우드 서비스를 선택하고 업무 연속성을 고려한 단계적 도입 적용

- 기업 규모 및 부서별 IT환경, 기존 시스템과의 호환성 등을 고려하여 클라우드 서비스 도입 형태 및 범위 정의
- 기업 중요 정보의 국외이전, 사내 정책과의 불일치 등으로 인한 문제 발생을 최소화하는 클라우드 서비스 제공자 선택
- 클라우드 서비스 오류 및 장시간 서비스 장애 등에 대비한 정기적 백업 및 중요 정보의 암호화 적용
- 클라우드 서비스 변경 및 해지에 따른 기업 정보유출 방지를 위해 기업 정보의 회수 및 삭제 확인서의 확보

o **(개인 이용자 대책)** 이용 목적에 따라 클라우드 서비스 모델을 선택하고 개인 단말기의 안전한 관리 및 올바른 서비스 이용방법 준수

- 이용자 정보처리방침 및 보상대책, 침해사고 대응 절차 등의 명확한 고지여부를 확인하고 정보보호 관련 인증을 취득한 클라우드 서비스 선택
- 정보 공유 및 접근 권한 설정 등 올바른 서비스 이용방법 준수
- 서비스 변경에 따른 기존 서비스와의 접근권한 설정기준 및 호환성 보장여부 등 이용조건 확인

□ 활용방안

o 클라우드 서비스 제공자

- 안전한 클라우드 서비스 제공을 위한 관리적·기술적 구축 기준 마련
- 자사 클라우드 서비스 보안수준에 대한 이용자 홍보 및 안내

o 클라우드 서비스 기업 및 개인 이용자

- 클라우드 서비스 및 정보보호에 대한 기본 지식 습득
- 자신의 IT환경에 적합하고 안전한 클라우드 서비스 선택 기준 마련

<참고>

〈 클라우드 정보보호 안내서 목차 〉