

**보도자료**

2010년 11월 15일(월) 배포시점부터 보도하여 주시기 바랍니다.

문의 : 네트워크정책국 개인정보보호윤리과 김광수 과장(☎750-2770)  
개인정보보호윤리과 한지혜 사무관(☎750-2773) han@kcc.go.kr**개인정보관리 안전기업 인증!****- 개인정보보호 관리체계 (PIMS) 인증제 도입 -**

방송통신위원회(이하 방통위)는 계속되는 개인정보 대량 유출 사고를 방지하고 기업의 사회적 책임을 강화하기 위한 일환으로 기업 스스로 고객의 개인정보를 보호할 수 있는 관리체계를 수립하여 지속적인 보호활동을 수행할 수 있도록 "개인정보보호 관리체계(PIMS) 인증제" 도입을 의결하였다.

※ PIMS(Personal Information Management System) : 개인정보보호 관리체계

“개인정보보호 관리체계 인증제”란 개인정보를 취급하는 기업이 전사차원에서 개인정보 보호 활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 것으로, 고객의 개인정보 보호를 위해 필요한 법적인(정보통신망법 등) 요구사항을 포함한 총 3개 분야 119개 통제항목에 대한 점검 과정을 거치게 된다. 특히 인증제도의 신뢰성과 공정성 확보를 위하여 방송통신위원회가 인증제를 직접 관리·감독하고, 한국인터넷진흥원이 인증 신청 기업의 심사를 수행할 예정이다.

방통위 관계자는 “인증제도 도입으로 법률에 명시된 최소한의 보호 대책만으로 개인정보 침해사고 방지에 어려움을 겪었던 기업들에게 체계적 개인정보 보호활동을 위한 세부 기준과 방법이 제시되었으며, 국민들에게는 개인정보를 안전하게 관리하는 기업을 객관적으로 식별할 수 있는 기준이 마련되었다는 점에서 의미가 크다”고 밝혔다.

또한 방통위는 12월중에 사업자를 대상으로 인증제 설명회를 개최할 계획이며, 인증 신청 및 심사는 2011년부터 수행할 예정이다.

## 개인정보보호 관리체계 (PIMS) 인증제

### □ 도입 배경

- 기업의 개인정보 이용 확산에 따른 대량 개인정보 유출 사고 증가
    - ※ 신세계 쇼핑몰('10.3), GS 칼텍스('08.9), 옥션('08.2) 등 1천만건 이상의 개인정보 유출사고가 지속적으로 발생
  - 법률에 명시된 최소한의 보호대책만으로 기업의 다양한 서비스에 사용되고 있는 개인정보 침해사고 예방이 어려운 상황
- ⇒ 기업의 자율적인 개인정보보호 활동을 유도하고, 국민들에게 개인정보를 안전하게 관리하는 기업을 손쉽게 식별할 수 있도록 개인정보보호관련 국가공인 인증제도 도입이 필요

### □ 도입경과

- 개인정보보호관리체계 인증제도 기반 요소 개발(2009년도)
  - 개인정보보호관리체계 인증 심사항목 및 인증 체계(안) 마련 : 상반기
  - 대량 개인정보 취급 사업자 대상 모의 인증 수행(SKT) : 하반기
- 개인정보보호관리체계 인증제(안) 검증(2010년도)
  - 중소기업 이용 편의성 확대를 위한 심사항목 경량화 : '10. 3월
  - 심사항목 검증을 위한 기업규모별 모의 인증 수행 : '10. 4월
  - ※ 대상 : NHN(대기업), 인크루트(중기업), 인터넷교차로(소기업)
  - 분야별 의견 수렴을 위한 인증제 도입 공청회 : '10. 8월

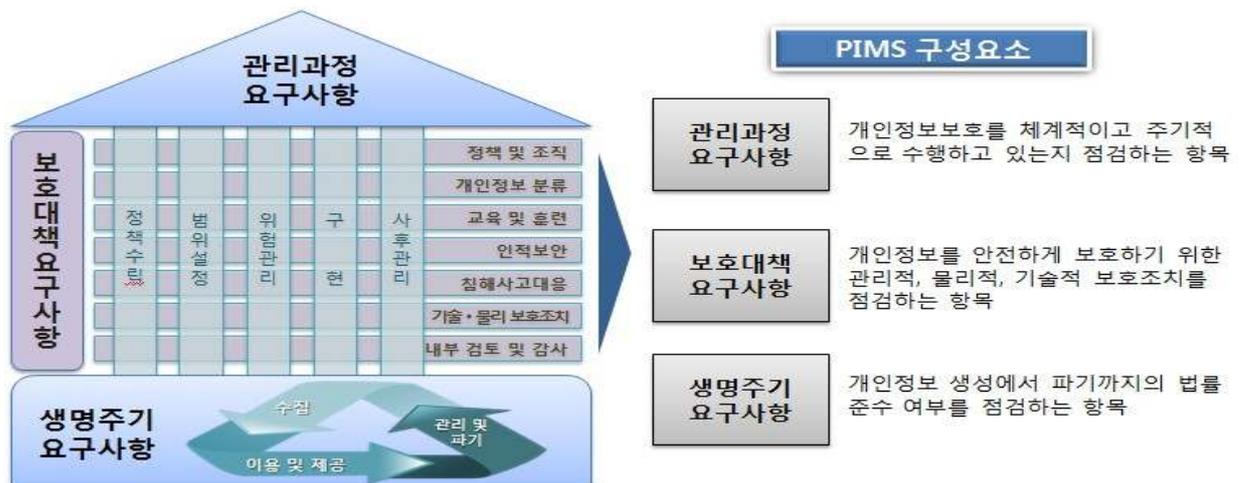
### □ 인증체계 구성 및 운영

- (인증체계)인증제도의 객관성 및 신뢰성 확보를 위해 인정기관, 인증위원회, 인증기관을 분리하여 운영
  - 인증제도를 관리·감독하는 인정기관을 방송통신위원회가 직접 수행
  - 산업계, 학계, 정부의 전문가로 인증위원회를 구성하여 인증결과를 심의
  - 한국인터넷진흥원을 인증기관으로 지정하여 심사의 객관성 확보

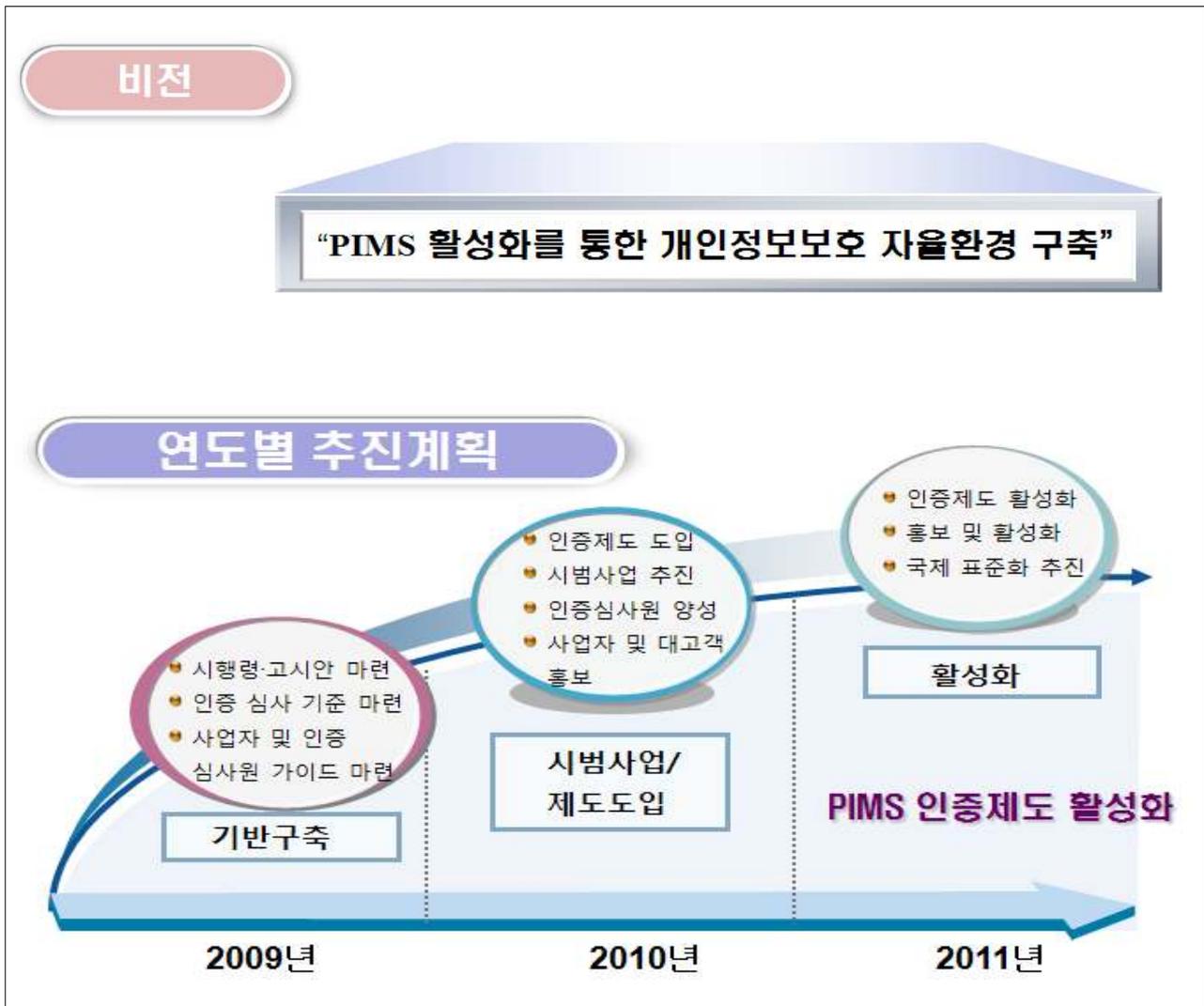
## 【 인증 체계 구성 및 운영 】



- **(인증운영)**개인정보보호관리체계(PIMS) 인증은 기업 자율제도로 운영
  - 개인정보보호관리체계를 구축·운영하는 기업이 자율적으로 심사를 신청하고, 인증기관이 검증후 일정 수준 이상이 기업에 인증을 부여
- **(인증 절차)** 국내외 주요 인증제도의 심사 절차를 준용한 4단계로 구성
  - ① 준비 단계 : 인증 절차 상담 및 신청 서류 준비
  - ② 심사 단계 : 관리체계 운영 검증을 위한 문서 심사 및 현장 심사
  - ③ 인증 단계 : 인증심사 결과를 근거로 인증 적합성 심사
  - ④ 사후관리 단계 : 인증 취득후 1년 단위로 사후관리 심사를 수행
- **(심사항목 구성)** 기업의 체계적이고 지속적인 개인정보보호활동과 법률 준수를 보장할 수 있도록 3개 분야의 119개 통제항목, 325개의 세부 점검 사항으로 구성



## □ 비전 및 향후 계획



- 개인정보 침해사고 사업자 등을 대상으로 설명회 : '10. 12월  
※ 대량 개인정보 취급 사업자, 개인정보 침해사고 사업자를 우선 선정
- 주요 정보통신서비스 제공 사업자 대상 인증심사 : '11. 1~12월
- 개인정보보호관리체계 구축 방법 등 사업자 교육 : '11. 3월
- 개인정보보호관리체계 인증 심사원 양성교육 : '11. 6월
- 개인정보보호관리체계 자가진단 도구 개발 : '11. 9월