방송통신위원회
KOREA COMMUNICATIONS COMMISSION

망법 시행령 개정 방향 주요 내용

2012. 3. 30(금)

Contents

Ⅰ 추진 배경

1. 추진 배경

기업 정보보호의 시급성 및 중요성

- 세계 최고 수준의 정보통신 인프라를 기반으로 신규 IT서비스가 급속히 활성화 되고 있으나, 사이버 침해사고도 고도화되어 점점 조직적·기능적으로 진화
  ※ APT(Advanced Persistent Threat) : 특정 대상자의 고객정보 등 정보 자산을 탈취하는 공격 기법
- 기업 정보보호 사고 발생 시, 기업은 매출 감소·주가 하락 등 존폐 위기를 맞으며, 이용자는 서비스 이용의 불편과 개인정보 2차 피해(피싱, 스팸, 불법대출 등) 경험
  ※ '11년 : 농협 전산망 장애(4월), SK컴즈 개인정보 유출(7월), 넥슨 해킹(11월) 등 침해사고 발생
- 전 세계 27개국 2,100개 기업을 대상으로 조사한 결과, '09년 기업의 75%가 사이버공격을 경험한 것으로 조사되었으며, 피해 규모는 기업당 연 2백만 달러 (약 23억원)로 추정(출처 : 2010 State of Enterprise Security Report, 시만텍)

정보보호 제도 일원화로 기업의 정보보호 수준 향상

- '03년 1.25 인터넷 대란 이후 최소한의 정보보호 조치를 위하여 시행되었던 기존의 안전진단 제도는 고도화된 침해사고 예방에 태생적 한계 노출
  ※ 안전진단 제도의 실효성에 대한 지속적인 문제제기(2010 국정감사 지적사항)
- 따라서 보안성이 강화된 정보보호관리체계(ISMS) 인증제도로 일원화함으로써 정보통신망의 안정성·신뢰성을 제고하고, 기업의 사회적 책임 강화 및 고객의 정보보호 서비스 선택권 제공

2. 추진 경과

정보통신망법 개정 경과

- 2011. 3월 진성호 의원 정보통신망법 개정(안) 발의
- 2011. 12월 국회 문방위 및 법사위 의결
- 2011. 12월 국회 본회의 통과(12.29)
- 2012. 2월 정부 이송(2.3) 및 공포(2.17)
- 2013. 2월 개정 정보통신망법 시행(2.18)

3. 법 개정에 따른 신규 제도

정보보호 안전진단 제도 폐지	• (목적) 실효성 및 중복성 논란을 해소하기 위하여, 안전진단 제도를 폐지하고 정보보호관리체계 인증 제도로 일원화 • (내용) '13년 2월 이후 제도 폐지
정보보호관리체계 인증 의무 대상자 지정	• (목적) 기존 안전진단 대상자는 정보보호관리체계(ISMS) 인증을 의무적으로 받도록 하여, 기업의 정보보호 수준 유지 및 향상 • (내용) 의무 대상자 지정 기준, 미인증 시 과태료 1천만원 부과
정보보호 관리등급 제도	• (목적) 이용자가 확인 가능하도록 기업에 관리등급을 부여하여, ISMS 인증 기업이 상위의 정보보호 활동을 수행하도록 유도 • (내용) 등급 기준, 방법 및 절차, 유효기간 등
정보보호 사전점검	• (목적) 정보통신서비스 운영 이전에 계획, 설계단계부터 정보보호를 고려하여 비용효과적으로 안전한 서비스 제공 • (내용) 정보보호 사전점검 권고 및 기준, 방법, 절차, 수수료 등
정보보호 최고책임자 지정	• (목적) 정보통신서비스 제공자가 정보보호 최고책임자(CISO)를 임원급으로 지정·운영하여 체계적인 정보보호 활동 유도 • (내용) CISO 역할, CISO 협의회 수행 사업 등

Ⅱ 시행령 개정 방향 주요 내용

Ⅱ-1 정보보호 안전진단 제도 폐지

1. 근거 법령

법 부칙 제1조, 제3조

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 제45조, 제45조의2, 제45조의3, 제46조의3, 제47조, 제47조의2, 제47조의3, 제47조의5, 제76조제3항 제6호부터 제9호까지의 개정규정은 공포 후 1년이 경과한 날부터 시행한다.

제3조(정보보호 안전진단의 폐지에 따른 경과조치) 이 법 시행 당시 종전의 규정에 따라 정보보호 안전진단을 받은 사업자는 정보보호 안전진단을 받은 당해연도에는 제47조제2항에 따른 정보보호 관리체계 인증을 받은 사업자로 본다.

2. 법 개정 취지 및 시행령 규정사항

법 개정 취지

새로운 IT서비스 활성화 및 해킹기법의 고도화에 따라 안전진단의 실효성 및 정보보호제도의 중복성 논란을 해소하기 위하여, 보안성이 높은 정보보호관리체계 인증 제도로 일원화

시행령 규정사항

정보보호 안전진단 제도 관련 규정의 삭제(제39조 ~ 제46조)

II-2 ISMS 인증 의무 대상자 지정

1. 근거 법령(1/2)

법 제47조, 제76조

제47조(정보보호 관리체계의 인증) ① 방송통신위원회는 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 **종합적 관리체계**(이하 **"정보보호 관리체계"**라 한다)를 수립·운영하고 있는 자에 대하여 제3항에 따른 기준에 적합한지에 관하여 **인증**을 할 수 있다.

② 정보통신서비스 제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 **인증을 받아야 한다.**

1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 **정보통신망서비스를 제공하는 자**
2. **집적정보통신시설 사업자**
3. **연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자**

<생략>

④ 제1항에 따른 정보보호 관리체계 **인증의 유효기간**은 **3년**으로 한다.

1. 근거 법령(2/2)

법 제47조, 제76조

⑤ 방송통신위원회는 **한국인터넷진흥원** 또는 **방송통신위원회가 지정한 기관**(이하 **"정보보호 관리체계 인증기관"**이라 한다)으로 하여금 제1항 및 제2항에 따른 **인증에 관한 업무를 수행**하게 할 수 있다.

⑥ 한국인터넷진흥원 및 정보보호 관리체계 인증기관은 정보보호 관리체계의 실효성 제고를 위하여 **연 1회 이상 사후관리**를 실시하고 그 결과를 방송통신위원회에 통보하여야 한다.

제76조(과태료) ③ 다음 각 호의 어느 하나에 해당하는 자에게는 **1천만원 이하의 과태료**를 **부과**한다.

6. 제47조제2항을 위반하여 **정보보호 관리체계 인증**을 받지 아니한 자
7. 제47조제7항 및 제47조의3제3항을 위반하여 **인증 받은 내용을 거짓으로 홍보**한 자

2. 법 개정 취지 및 시행령 규정사항

법 개정 취지

기존 안전진단 대상자는 정보보호관리체계(ISMS) 인증을 의무적으로 받도록 하여 정보통신서비스 제공자의 정보보호 체계를 유지 및 향상

시행령 규정사항

ISMS 인증 의무 대상자 범위, ISMS 인증 업무 범위, 인증의 사후관리, 인증 표시 및 홍보, 인증 취소의 방법 및 절차, 인증기관의 지정 기준・절차・유효기간・사후관리

3. ISMS 인증 의무 대상자 지정(1/4)

인증 의무 대상자 범위

1. 법 제47조제2항제1호 : 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자 중 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자

2. 법 제47조제2항제3호 :
   ① 정보통신서비스부문 전년도(법인의 경우에는 전 사업연도) 매출액이 100억원 이상으로서 방송통신위원회가 고시하는 기준에 해당하는 자
   ② 전년도 말 기준 3개월간의 일일평균 이용자 수가 100만명 이상으로서 방송통신위원회가 고시하는 기준에 해당하는 자

3. 법 제47조제2항제2호 : 집적정보통신시설사업자(IDC)가 마련한 시설의 일부를 임대하여 집적정보통신시설사업을 하는 자(VIDC)에 대해서는 2번 기준(100억 이상, 100만명 이상) 적용

2. ISMS 인증 의무 대상자 지정(2/4)

정보보호관리체계 인증 제도

정의 : 인증대상기관이 수립·운영하고 있는 정보보호관리체계(ISMS)가 인증심사 기준(방통위 고시)에 적합한지를 한국인터넷진흥원 또는 방송통신위원회가 지정하는 기관이 심사하여 인증하는 제도

대상 : 인증 희망 기업(ISMS를 수립·운영하고 있는 자), 의무 대상자

인증기관 : 한국인터넷진흥원, 방송통신위원회가 지정한 기관(ISMS 인증기관)

심사 방법 : 서면심사, 현장심사

인증 유효 기간 : 3년(최초 심사, 사후관리 심사)

정보보호관리체계 인증 절차

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2. ISMS 인증 의무 대상자 지정(3/4)

인증 업무 범위

1. 인증 신청인이 수립한 정보보호 관리체계의 심사
2. 인증의 사후관리
3. 제1호에 따른 심사결과의 심의
4. 인증서 발급·관리
5. 제1호부터 제4호까지 인증에 관한 업무와 관련된 부대업무

인증의 사후관리

1. 사후관리는 연 1회 이상 서면심사 및 현장심사로 수행
2. 사후관리 시, 인증 취소 사유가 발견되면 인증위원회에서 심의 후 방통위 통보

인증 취소 사유 및 과태료

1. 거짓이나 부정한 방법으로 인증 취득
2. 인증기준에 미달
3. 사후관리를 거부 또는 방해

※ 의무 대상자가 인증을 받지 않은 경우, 1천만원 이하 과태료 부과

2. ISMS 인증 의무 대상자 지정(4/4)

인증 수수료

인증신청자의 종업원 수, 정보통신설비 규모, 인증 심사 일수 등에 따라 산정(고시 예정)

인증기관의 지정 기준

1. 인증심사업무를 전담하는 직원(인증심사원) 5명 이상 보유(기존 10명)
2. 방통위의 업무수행요건·능력심사에서 적합하다고 인정(기존 업무수행능력심사)

※ 인증심사원의 자격 요건, 교육·자격 관리, 업무수행요건, 능력심사 세부 기준(고시 예정)

인증위원회

정의 : 한국인터넷진흥원 또는 ISMS 인증기관에서 정보보호에 관한 학식과 경험이 풍부한 자를 위원으로 설치·운영

역할 : 최초 심사 결과 심의, 사후관리 심사에서 인증 취소 사유 발견 시 심의

인증기관의 사후관리

인증기관은 지정기준 변경사항 및 인증실적 보고서를 다음 연도 1월말까지 방송통신위원회에 제출

방송통신위원회는 인증기관 지정 취소 여부 확인 시, 자료 제출 요구 및 현장 실사 가능

Ⅱ-3 정보보호 관리등급 제도

1. 근거 법령

법 제47조의5

제47조의5(정보보호 관리등급 부여) ① 제47조에 따라 **정보보호 관리체계 인증을 받은 자**는 기업의 통합적 정보보호 관리수준을 제고하고 이용자로부터 정보보호 서비스에 대한 신뢰를 확보하기 위하여 방송통신위원회로부터 **정보보호 관리등급을 받을 수 있다.**

② 방송통신위원회는 **한국인터넷진흥원**으로 하여금 제1항에 따른 **등급 부여**에 관한 **업무를 수행**하게 할 수 있다.

<생략>

⑤ 제1항에 따른 등급 부여의 심사기준 및 등급 부여의 방법·절차·수수료, 등급의 유효기간, 제4항에 따른 등급취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

2. 법 개정 취지 및 시행령 규정사항

법 개정 취지

정보통신서비스사업자의 정보보호 수준을 이용자가 직접 확인 가능하도록 등급을 부여하여, 기업의 사회적 책임성 강화를 통한 정보보호 수준 향상을 유도하고, 고객에게는 객관적인 기업 선택의 기준 제시

시행령 규정사항

등급 심사 기준(고시 예정), 심사 방법, 등급 심사 수행 인력 자격, 등급의 유효 기간

3. 정보보호 관리등급 제도

정보보호 관리등급 제도

ISMS 인증 취득 기업이 우수한 수준의 정보보호 활동을 수행하여 등급 부여를 신청하면, 신청기업의 정보보호 체계·활동이 등급 심사 기준에 적합한지 심사하여 등급을 부여하는 제도(우수/최우수)

등급 심사 기준

정보보호 관리등급 부여를 위한 세부 심사 기준(고시 예정)

등급 부여 방법 및 절차

심사 방법 : 서면심사, 현장심사
심사원 : ISMS 인증심사원
기타 : 등급 부여 신청, 심사, 증명서 발급 등 세부 사항(고시 예정)

등급의 유효 기간

유효 기간 : 1년(유효 기간 동안 ISMS 인증 취득으로 인정)

Ⅱ-4 정보보호 사전점검

1. 근거 법령

법 제45조의2

제45조의2(정보보호 사전점검) ① 정보통신서비스 제공자는 **새로이 정보통신망을 구축하거나 정보통신서비스를 제공**하고자 하는 때에는 그 계획 또는 설계에 정보보호에 관한 사항을 고려하여야 한다.

② 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 대통령령으로 정하는 **정보보호 사전점검기준에 따라 보호조치를 하도록 권고**할 수 있다.

1. 이 법 또는 다른 법령에 따라 **방송통신위원회의 인가·허가를 받거나 등록·신고를 하도록 되어 있는 사업**으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업

2. **방송통신위원회가 사업비의 전부 또는 일부를 지원하는 사업**으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업

③ 제2항에 따른 정보보호 **사전점검의 기준·방법·절차·수수료** 등 필요한 사항은 대통령령으로 정한다.

2. 법 개정 취지 및 시행령 규정사항

법 개정 취지

정보통신서비스 개시 이전에 계획, 설계단계부터 정보보호를 고려하여 정보통신망의 침해사고를 예방하고, 비용효과적으로 안전한 서비스를 제공하기 위해 정보보호 사전점검 제도를 신설

시행령 규정사항

정보보호 사전점검의 대상, 정보보호 사전점검 기준, 방법 및 절차, 수수료를 명시하고 세부적인 사항은 고시로 정함

3. 정보보호 사전점검(1/3)

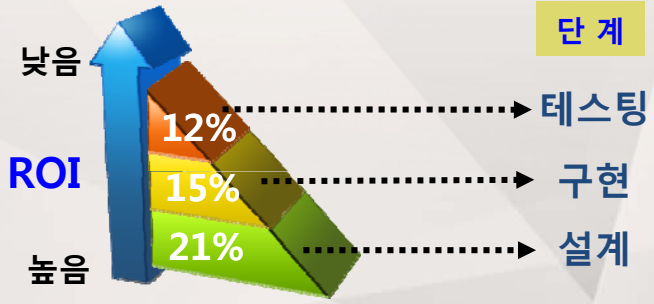
정보보호 사전점검의 개념

IT 서비스의 구축 단계(계획・설계・구현・테스트)에서 정보보호 위협, 취약점, 위험 분석 등의 진단을 통해 사전에 취약점을 제거하고, 보호대책을 수립·적용하는 일련의 보안 컨설팅 활동

[서비스 Life-Cycle]

단계별 취약점 조치 비용

단계별 사전점검 투자 vs 효과



3. 정보보호 사전점검(2/3)

정보보호 사전점검 조문

< 정보보호 사전점검의 기준 >

- 대상 서비스의 아키텍처, 서비스 운영 환경, 보호대상 식별 및 위험성, 보호대책 도출 및 구현 현황을 고려하여 고시로 정하도록 함

< 정보보호 사전점검 권고 대상 >

1) 방통위의 인가·허가, 등록·신고 대상 사업 중 투자규모 5억 이상인 사업 (단순 HW, SW 구입비 제외)

2) 방통위가 신규 서비스 또는 사업의 발굴 · 육성을 위해 사업비를 지원하는 시범사업

3. 정보보호 사전점검(3/3)

정보보호 사전점검 조문

< 정보보호 사전점검의 방법 절차 등 >

- 방법 : 서면점검, 현장점검, 원격점검
- 절차 : ① 사전점검 준비 → ② 설계 검토 → ③ 보호대책 적용 → ④ 현장 점검 → ⑤ 사전점검 결과 정리
- 수행인력 요건 : 시행령 별표 2에 따른 기술인력 요건
- 교육 요건 : 방통위가 지정하는 기관에서 실시하는 교육 이수자만이 수행
- 수행 주체 : 대상기관이 자체적으로 수행하거나 KISA 또는 외부 전문기관
- 기타 : 기타 세부사항은 방통위 고시로 정함

< 수수료 >

- 사전점검 대상 사업의 규모, 사전점검 참가자의 전문성, 사전점검 기간을 고려하여 구체적인 산정기준을 방통위 고시로 정함

Ⅱ-5 정보보호 최고책임자 제도

1. 근거 법령

법 제45조의3

제45조의3(정보보호 최고책임자의 지정 등) ① **정보통신서비스 제공자**는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 **임원급의 정보보호 최고책임자**를 **지정**할 수 있다.

② 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.

1. 정보보호관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선

<생략>

③ 정보통신서비스 제공자는 침해사고에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 정보보호 최고책임자를 구성원으로 하는 **정보보호 최고책임자 협의회**를 **구성·운영**할 수 있다.

④ 정부는 제3항에 따른 협의회의 활동에 필요한 경비의 전부 또는 일부를 지원할 수 있다.

2. 법 개정 취지 및 시행령 규정사항

법 개정 취지

정보통신서비스 제공자에 대해 정보보호를 체계적으로 구축하고 관리할 수 있도록 정보보호 최고책임자를 임원급으로 지정, 관리 유도

시행령 규정사항

정보보호 최고책임자 협의회가 수행하는 사업의 범위

3. 정보보호 최고책임자 제도

정보보호 최고책임자(CISO)

정의 : 정보통신서비스 제공자(기업)의 정보보호 담당 임원으로 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리 등의 업무를 수행

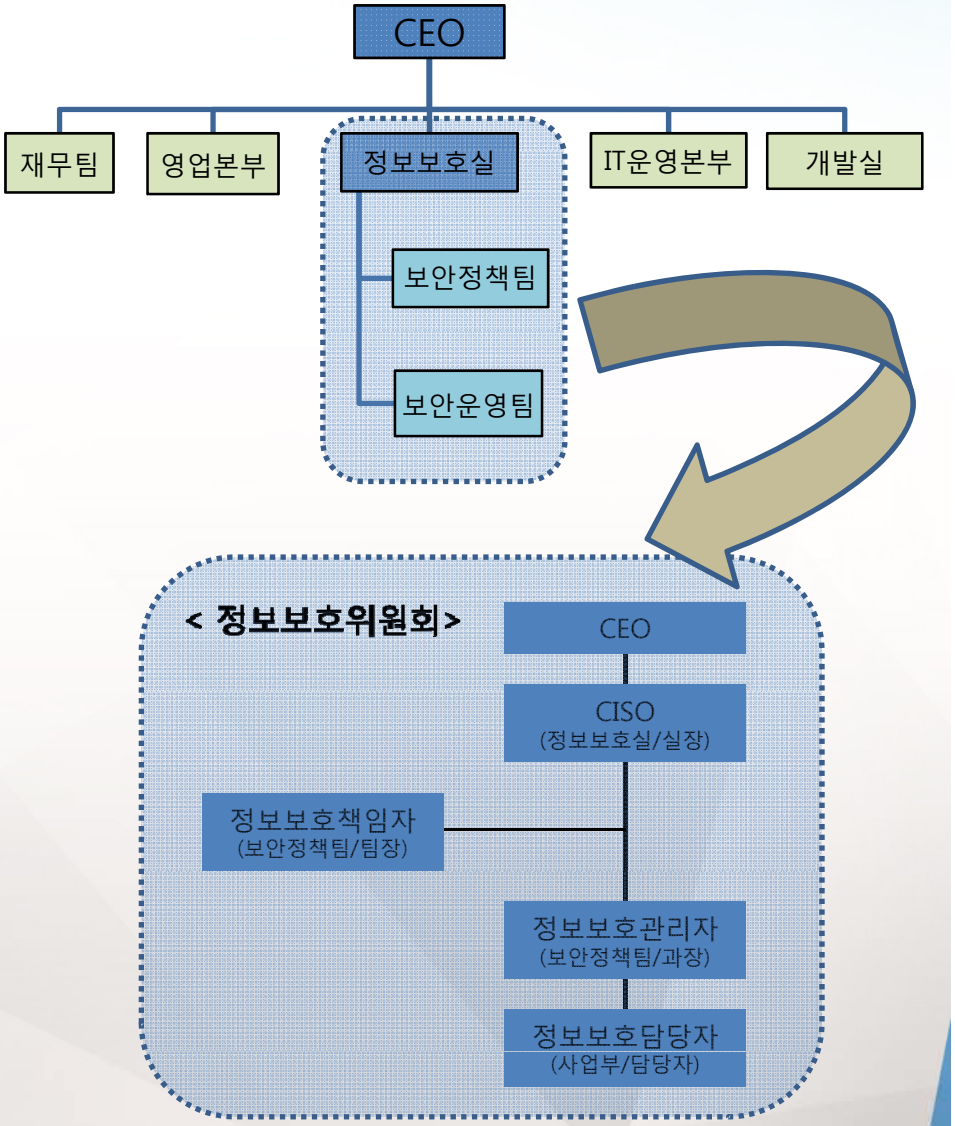
CSO, CISO 비교 : CSO는 건물, 인력에 대한 경비를 포함한 물리적 보안책임자이며, CISO는 정보통신시스템을 담당하는 정보보호 최고책임자

※ CSO(Chief Security Officer, 보안최고책임자)

※ CISO(Chief Information Security Officer, 정보보호 최고책임자)

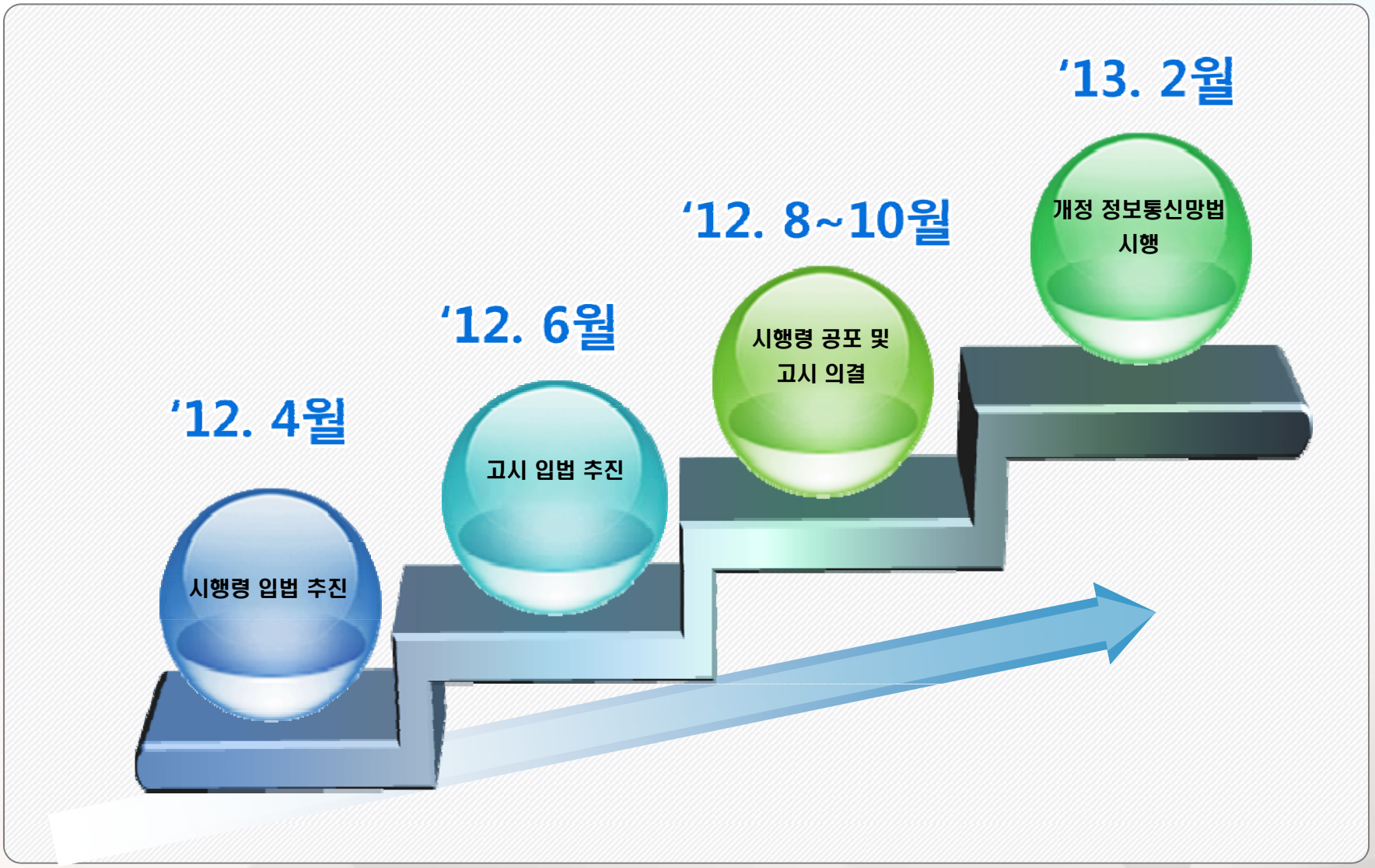
CISO 역할 : ① 정보보호관리체계의 수립 및 관리·운영, ② 정보보호 취약점 분석·평가 및 개선, ③ 침해사고의 예방 및 대응, ④ 사전 정보보호대책 마련 및 보안조치 설계·구현 등

정보보호 최고책임자 협의회 : CISO로 구성하는 협의회로 침해사고 공동 예방 및 대응, 필요한 정보의 교류, 그 밖의 공동 사업 수행



Ⅲ 향후 추진 일정

향후 추진일정


'12. 4월
시행령 입법 추진
'12. 6월
고시 입법 추진
'12. 8~10월
시행령 공포 및
고시 의결
'13. 2월
개정 정보통신망법
시행

감사합니다