특정감사

감 사 보 고 서

- 국가 사이버안전 관리 실태 -

2016. 3.

감 사 원

목 차

Ⅰ 감사실시 개요

1. 감사 배경 및 목적

최근 사이버 테러, 해킹 등 사이버 공격은 갈수록 지능화·은밀화 되고 있고 원전·전력망 등 국가 핵심 제어시스템을 마비, 파괴시키는 사이버공격, 공공아이핀 부정발급, 금융·의료정보 등 대규모 개인정보 유출 등에 따라 경제적 손실[1]은 물론이고 사회혼란과 국민불안을 초래하고 국가안보까지 위협받게 되는 문제에 직면하고 있다.

또한, 공공아이핀의 부정 발급(2015년), 카드사의 금융정보 유출(2014년) 및 병원·약국의 의료정보 유출(2014년, 2015년) 등 개인정보 무단 유출 등의 보안사고도 지속적으로 발생하고 있다.

따라서 감사원에서는 국가 사이버안전 관리체계, 행정·금융·보건의료 관련 소관별 정보보호 업무 실태 등을 종합 점검하여 문제점 및 그 근본적인 원인을 파악하고 개선방안을 제시함으로써 효과적인 국가 사이버안전 관리체계를 구축하고, 행정·금융·보건의료 관련 소관별 정보보호 강화 등을 통해 국가 사이버안전을 강화할 필요가 있었다.

이에 따라 '국가 사이버안전 관리 실태' 감사를 2015년 감사계획에 반영하고 이번 감사를 실시하게 되었다.

2. 감사 중점 및 대상

이번 감사에서는 [표 1]과 같이 국가 차원의 사이버안전 관리체계의 적정성을

1) 사이버 침해사고로 인한 경제적 피해는 자연재해로 인한 연간 피해액 1.7조 원의 2배가 넘는 연간 3.6조 원 수준임

점검하고, 다량의 개인정보를 취급하거나 개인정보 유출 사고가 많이 발생하는 행정·금융·보건의료 부문을 대상으로 소관별 정보보호 업무 추진의 적정성을 주로 점검하였다.

[표 1] 분야별 감사 중점

관리체계 분야	소관별 정보보호 업무 분야		
	행정부문	금융부문	보건의료부문
▪ 주요정보통신기반시설 지정·관리의 적정성 ▪ 정보보호인력 양성 시책 추진의 적정성 ▪ 정보보호 관련 인증제도 운영의 적정성 등	▪ 아이핀 제도 운영의 적정성 - 민간아이핀 운영의 적정성 - 공공아이핀 운영의 적정성 ▪ 공공아이핀 부정발급 사고처리의 적정성 - 공익감사청구사항 포함 ▪ 본인확인제도 운영의 적정성	▪ 자율보안 책임체계 전환 및 관리의 적정성 ▪ 금융 이용자의 보호 강화 시책 추진의 적정성 - 부정거래탐지시스템 구축 및 운영 등	▪ 개인정보(의료정보) 보호·관리의 적정성 - 요양급여 비용 심사청구 소프트웨어 등 - 폐업의료기관의 의료정보 보호의 적정성 ▪ 의료정보 활용체계의 적정성

3. 감사실시 과정

이번 감사는 2015. 6. 8.부터 7. 3.까지 언론보도 사항, 국회 정책자료, 연구용역 자료 등 관련 자료를 수집·분석하는 등 감사를 준비하였고, 2015. 7. 6.부터 7. 17.까지 10일간 관련 분야의 전문가 면담 등을 포함한 예비조사를 실시한 후 같은 해 8. 24.부터 10. 14.까지 감사인원 21명을 투입하여 실지감사를 실시하였다.

그리고 이번 감사에 필요한 전문성을 보완하고 객관성 및 신뢰성을 제고하기 위해 2차에 걸쳐 산·학·연 관련 분야의 전문가를 대상으로 전문가 자문회의를 개최하였다.

또한 행정부문의 아이핀 제도 및 본인확인 제도의 운영 실태와 개선방안에 관련하여서는 전문기관을 활용하여 연구용역과 설문조사를 실시하였고, 금융·

복지 부문에 대하여도 산·학·연 전문가의 자문을 구하는 등 전문성·객관성을 확보하기 위해 최대한 노력하였다.

4. 감사결과 처리

감사결과 위법·부당사항 및 개선 사항과 관련하여 2015. 10. 14. 보건복지부, 같은 해 10. 23. 미래창조과학부, 방송통신위원회, 금융위원회, 같은 해 11. 11. 행정자치부 등 주요 감사대상기관의 차관 등이 참석한 가운데 감사마감회의를 개최하여 감사에서 나타난 문제점 등에 대한 대상기관의 의견 및 개선방안 등에 대해 논의하였다.

그리고 감사원에서는 감사결과 지적사항에 대하여 대상기관과 질문·답변 과정을 거쳐 의견을 수렴·반영한 후 감사원의 내부 검토과정을 거쳐 2016. 3. 17. 감사위원회의의 의결로 감사결과를 최종 확정하였다.

Ⅱ 감사대상 현황[2)]

1. 주요 기관의 역할·임무

국가정보원, 미래창조과학부, 금융위원회 등 주요 기관의 역할·임무는 [표 2]와 같다.

[표 2] 주요 기관의 역할·임무

기관명	주요 역할·임무
국가정보원	▪ 「정보통신기반 보호법」, 「전자정부법」, 「국가정보화 기본법」, 「국가사이버안전관리규정」 등 관계 법령에 따라 국가·공공기관에 대한 정보보안 업무를 총괄 ▪ 국가 차원의 종합적·체계적인 예방·대응을 위해 2004년 2월 국가사이버안전센터를 설립하여 국가 사이버안전 정책 수립, 해킹 및 악성코드 유포 등 사이버공격에 대한 탐지·대응, 각급기관 정보통신망에 대한 보안진단, 공공 분야 주요정보통신기반시설의 보호 업무, 공공 분야 사이버위기 경보 발령, 사고 조사·분석 및 대응복구 등 사이버안전 총괄 기관의 역할을 담당
미래창조과학부	▪ 2013년 구 안전행정부, 산업통상자원부, 방송통신위원회의 정보보호 관련 업무를 이관받아 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다), 「국가정보화 기본법」, 「전자서명법」, 「정보통신기반 보호법」, 「정보보호산업의 진흥에 관한 법률」 등 관계법령에 따라 민간 분야 주요정보통신기반시설의 보호, 민간 분야 침해사고 예방·대응체계 마련, 전자인증 및 정보보호산업 관련 정책의 수립 및 추진 등 민간 분야의 정보보호 및 정보보호산업 진흥 업무를 총괄
금융위원회	▪ 「전자금융거래법」, 「신용정보의 이용 및 보호에 관한 법률」 등 관계 법령에 따라 전자금융거래 이용자 보호 및 전자금융 분야 정보보안 정책의 수립 및 제도개선 등의 업무를 수행
행정자치부	▪ 「국가정보화 기본법」, 「전자정부법」, 「개인정보 보호법」 등 관계 법령에 따라 전자정부의 사이버 침해에 대한 예방·대응체계 마련 및 공공 분야 등 개인정보보호 정책 업무를 수행
방송통신위원회	▪ 정보통신망법 등에 따라 개인정보 침해사고의 사전예방, 유·노출 사고 대응 등 정보통신망 관련 개인정보보호 정책 업무를 수행 ▪ 주민등록번호 대체수단으로 아이핀·범용공인인증서·휴대폰인증 등을 도입·운영
한국인터넷진흥원	▪ 정보통신망법 제52조에 따라 민간 분야 정보통신망의 침해사고 예방 및 대응, 개인정보보호 등을 목적으로 설립된 인터넷 정보보호 전문기관
국가보안기술연구소	▪ 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따라 공공 분야의 사이버안전을 위한 연구·개발, 국가 암호기술 연구, 해킹 대응 등 각종 정보보안기술 개발 및 정책 연구 등을 위해 한국전자통신연구원의 부설 연구소로 설립된 정보보호 전문연구기관
한국지역정보개발원	▪ 「전자정부법」 제72조에 따라 전자지방정부 구현 및 지역정보화 촉진을 위하여 지방자치단체에서 추진하는 정보화사업, 이와 관련하여 관계 중앙행정기관 또는 지방자치단체가 위탁하는 사무, 지방자치단체의 취약점 분석, 보안관제, 침해사고 대응 등 정보보호 업무도 수행

자료: 법령자료 등 재구성

2) 이 부분은 감사결과 지적된 문제점의 종합적 이해를 돕기 위해 감사대상 업무의 현황을 기술한 것으로, 감사대상 기관이 제출한 자료를 바탕으로 작성되었으며 현장조사 등 감사의 방법으로 검증한 내용이 아님

2. 관계 법령 현황

공공부문 사이버안전 총괄 업무는 「국가사이버안전관리규정」에 규정되어 있으며, 민간부문 사이버 침해사고 예방 및 대응 업무는 정보통신망법에 규정되어 있고, 주요정보통신기반시설 보호 업무는 「정보통신기반 보호법」에 규정되어 있는 등 [표 3]과 같이 다수 법규에 기관별·업무별로 규정되어 있다.

[표 3] 기관별 관련 법령 현황

구분	근거 법령 명칭	담당 업무
국무조정실	· 「정보통신기반 보호법」	· 정보통신기반보호위원회 운영
미래창조과학부	· 정보통신망법 · 「정보통신기반 보호법」 · 「정보보호산업의 진흥에 관한 법률」	· 민간부문 침해사고 대응(한국인터넷진흥원) · 민간부문 주요정보통신기반시설 보호 · 정보보안산업 육성
국가정보원	· 「국가사이버안전관리규정」 · 「정보통신기반 보호법」	· 공공부문 사이버안전 업무 총괄, 공공부문 침해사고 대응(국가사이버안전센터) · 공공부문 주요정보통신기반시설 보호
행정자치부	· 「개인정보 보호법」 · 「전자정부법」	· 개인정보보호 총괄 · 전자정부 정보보호
방송통신위원회	· 정보통신망법	· 정보통신망의 개인정보보호 및 스팸 대응
금융위원회	· 「전자금융거래법」 · 「신용정보의 이용 및 보호에 관한 법률」	· 전자금융거래 안정성 확보 · 금융정보 보호

자료: 미래창조과학부 등 제출자료 재구성

3. 예산 현황

국가 정보보호 예산은 [표 4]와 같이 2015년 2,543억 원으로 정보화 예산 4조 1,070억 원의 6.2% 수준이고, 2010년 8.0%, 2011년 9.4%, 2012년 8.3%에 비해 다소 낮아졌다.

[표 4] 정보화 예산 및 정보보호 예산 현황

(단위: 억 원, %)

구분	2010년	2011년	2012년	2013년	2014년	2015년
정보화 예산(A)	20,783	21,562	27,063	29,977	39,404	41,070
정보보호 예산(B)	1,670	2,019	2,248	1,489	2,460	2,543
정보보호 예산 비율(B/A)	8.0	9.4	8.3	5.0	6.2	6.2

자료: 미래창조과학부 제출자료 재구성

4. 보안관제센터 현황

최근 사이버공격이 고도화·지능화됨에 따라 정부는 행정·에너지·금융 등 국가 주요 정보통신시스템 등에 대한 공격 징후를 조기 탐지하고 대응하기 위하여 분야별 보안관제센터를 구축·운영하고 있는데, [표 5]와 같이 2015년 현재 중앙행정부처 단위에서 31개의 보안관제센터가 운영되고 있다.

[표 5] 보안관제센터 현황

부문	기관	관제센터	부문	기관	관제센터
행정	행정자치부	정부통합전산센터(대전)	국세	국세청	국세 관제센터
		정부통합전산센터(광주)	방위산업	방위사업청	방위사업 관제센터
		시도 사이버침해대응 지원센터	재정	기획재정부	재정 관제센터
국방	국방부	국군사이버사령부	문화	문화체육관광부	문화체육관광 관제센터
외교	외교부	외교 사이버안전센터	기상	기상청	기상 관제센터
국토교통	국토교통부	국토교통 사이버안전센터	노동	고용노동부	노동 관제센터
보건의료	보건복지부	보건의료 사이버안전센터	환경	환경부	환경 관제센터
교육	교육부	교육 사이버안전센터	법무	법무부	법무 관제센터
에너지	산업통상자원부	산업통상 사이버안전센터	통일	통일부	통일 관제센터
통신과학	미래창조과학부	미래창조 사이버안전센터	농식품	농림수산식품부	농식품부 사이버안전센터
		과학기술 정보보호센터	검찰	대검찰청	대검 사이버안전센터
		KISA 인터넷침해대응센터	병무	병무청	병무청 사이버안전센터
금융	금융위원회	금융보안원	해양	해양수산부	해양수산 사이버안전센터
치안	경찰청	경찰 전산보호센터	중소기업	중소기업청	중기청 사이버안전센터
특허	특허청	특허 관제센터	공정위	공정거래위원회	공정위 사이버안전센터
관세	관세청	관세 관제센터			

자료: 미래창조과학부 등 제출자료 재구성

5. 주요정보통신기반시설 현황

국가·사회적으로 중요한 제어시설에 대한 해킹 시도로 공공안전이 위협을 받는 상황이 빈번하게 발생됨에 따라 정부는 2001년부터 국가·사회적으로 중요한 정보통신기반시설을 주요정보통신기반시설로 지정하여 중점 보호·관리하고 있으며, [표 6]과 같이 2015년 2월 현재 정보통신, 행정, 금융, 교통수송, 에너지, 보건의료 등의 분야에서 17개 관계 중앙행정기관, 205개 관리기관 등 354개 시설이 주요정보통신기반시설로 지정·관리되고 있다.

[표 6] 연도별 주요정보통신기반시설 지정 현황(2015년 10월)

(단위: 개)

구분	'01년	'02년	'04년	'05년	'06년	'07년	'08년	'09년	'10년	'11년	'12년	'13년	'14년
신규지정	23	66	7	1	5	10	11	21	28	33	23	85	63
지정취소 등	-	-	△3	△1	△4	△3	△3	△4	△1	-	-	△2	△1
누계	23	89	93	93	94	101	109	126	153	186	209	292	354

자료: 미래창조과학부 제출자료

6. 주요 해킹사고 발생 현황

최근 발생한 주요 해킹사고 현황은 [표 7]과 같다.

[표 7] 주요 해킹사고 발생 현황

사건명	사건일자	사건 내용	피해 상황
7.7 DDoS	2009. 7. 7.	▪ 7월 7일부터 9일까지 대규모 DDoS 공격으로 청와대 등 주요 정부기관과 민간기업 홈페이지가 마비	공격대상: 국내외 36개 기관, 좀비PC: 약 11만대
3.4 DDoS	2011. 3. 4.	▪ 3월 4일부터 7일까지 국내 주요 사이트를 대상으로 대규모 DDoS 공격 ▪ 웹하드 설치 프로그램 변조를 통해 동시 다발적으로 대량 악성코드 유포·감염	공격대상: 국내 40개 기관, 좀비PC: 약 11만대
○○ 해킹	2011. 4. 12.	▪ 해킹 공격으로 ○○ 내부 전산망 시스템이 파괴 ▪ ○○ 외주 전산관리 직원의 노트북이 악성코드에 감염되어 내부 전산망 공격에 악용	서버 및 업무용 PC 270대 파괴 (4월 30일까지 ○○ 전산망 마비)
3.20 사이버공격	2013. 3. 20.	▪ 3월 20일 국내 주요 언론사와 금융권의 전산망이 악성코드에 감염되어 동시에 마비 * 중앙 관리서버가 해킹당하여 동시에 다수의 시스템에 악성코드 감염	PC/서버 등 약 48,800대 파괴 (정상복구까지 최대 10일 소요)
6.25 사이버공격	2013. 6. 25.	▪ 6월 25일부터 7월 1일 사이에 언론사 전산망 파괴, 청와대 등 정부기관 홈페이지 변조, 정부통합전산센터 DNS 대상 DDoS 공격으로 사회적 혼란 야기	69개 기관 대상 복합적인 연쇄 사이버 공격
●● 해킹	2014. 3. 6.	▪ '고객서비스계약번호'에 대한 본인 여부를 검증하는 절차가 없는 취약점을 해커가 악용하여 홈페이지의 타인 정보를 조회·유출 * 인천광역수사대에서 개인정보 불법 유통 단속과정에서 유출 정황 확인	약 982만 명 고객정보 유출
◇◇ DNS DDoS	2014. 11. 29.	▪ ◇◇ DNS(서최DC, 동작IDC) 대상으로 3차례 DDoS 공격 * 보안이 취약한 공유기가 악성코드에 감염되어 DDoS 공격 트래픽 발생	3차례 총 32분 DDoS 공격
⊛⊛ 해킹	2014. 12. 9.	▪ 12월 9일부터 12일까지 ⊛⊛(주) 직원을 대상으로 악성코드 이메일을 발송하여 시스템 파괴 시도 * 원전가동 중단 협박을 통한 사이버 심리전으로 사회혼란 야기	원전 설계도면 등 유출 (시스템 파괴 공격은 실패)
공공아이핀 해킹	2015. 2. 28.	▪ 2월 28일부터 3월 2일까지 공인인증서 우회 인증 및 법정대리인 취약점을 해커가 악용하여 공공아이핀을 부정 발급	공공아이핀 82만 건 부정발급

자료: 미래창조과학부 등 제출자료 재구성

7. 주요 개인정보 유출 등 사고 발생 현황

최근 개인정보 유출 등 사고는 [표 8]과 같이 주민등록번호, 성명 이외에도 카드번호, 계좌번호 등 금융 개인정보와 환자 조제정보, 진료정보 등 의료 개인정보까지 광범위하게 발생하고 있는 실정이다.

[표 8] 주요 개인정보 유출 등 사고 발생 현황

사고 기관명	사고 일자	피해 규모	유출 정보	소관 부문
◆◆	2011. 11. 28.	1,322만 건	주민등록번호, 성명 등	행정
●●	2012. 7. 30.	1,170만 건	주민등록번호, 성명, 계좌번호 등	행정
□□카드	2014. 1. 8.	1,967만 건	주민등록번호, 계좌정보, 카드번호 등	금융
■■카드	2014. 1. 8.	4,449만 건	주민등록번호, 계좌정보, 전화번호 등	금융
○○카드	2014. 1. 10.	2,426만 건	주민등록번호, 계좌정보, 카드번호 등	금융
●●	2014. 3. 7.	981만 건	주민등록번호, 신용카드번호 등	행정
△△	2014. 4. 11.	277만 건	주민등록번호, 성명 등	행정
▲▲	2014. 7. 28.	7억 건	환자 조제정보, 주민등록번호 등	보건의료
▲▲	2015. 7. 23.	43억 건	환자 조제정보, 주민등록번호 등	보건의료
▽▽	2015. 7. 23.	7억 건	환자 진료·처방정보, 성명 등	보건의료
▼▼	2015. 7. 23.	7,802만 건	환자 처방정보, 성명 등	보건의료

자료: 행정자치부 등 제출자료 재구성

8. 주요 정보보호 업무 연혁

[표 9]와 같이 2001년에는 「정보통신기반 보호법」이 제정되었고, 구 「정보통신망 이용촉진 등에 관한 법률」(2001. 7. 1. 법률 제6360호 정보통신망법으로 개정되기 전의 것)에 정보보호업무가 추가되어 정보통신망법으로 개편되었으며, 2003년에는 구 한국정보보호진흥원(현 한국인터넷진흥원) 내에 인터넷침해사고대응지원센터를 설립하였고, 2004년에는 국가정보원 내에 국가사이버안전센터를 설립하였다.

2005년에는 공공 분야의 사이버안전 관리 업무를 위해 「국가사이버안전관리규정」을 제정하였고, 2008년에는 범국가적 차원의 보안관제체계를 구축하였으며 2010년에는 국군사이버사령부가 창설되었다.

한편, 사이버공격에 효과적으로 대응하기 위해 2009년, 2011년, 2013년, 2015년 정부의 사이버위기 종합대책을 각각 마련하여 시행하고 있다.

[표 9] 주요 정보보호 업무 연혁

연도	주요 추진 내용
2001	▪ 「정보통신기반 보호법」 제정 ▪ 「전자정부구현을 위한 행정업무 등의 전자화 촉진에 관한 법률」 제정 ▪ 「정보통신망 이용촉진 등에 관한 법률」이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 개편 ▪ 한국정보보호센터가 한국정보보호진흥원(KISA)으로 승격
2003	▪ 1.25 인터넷 대란 발생 ▪ KISA 인터넷침해사고대응지원센터 설립
2004	▪ 국가사이버안전센터 설립 ▪ 「국기 위기관리 기본 지침」(대통령 훈령) 및 국가사이버위기관리 매뉴얼 제정
2005	▪ 「국가사이버안전관리규정」(대통령훈령) 제정
2007	▪ 정보보호제품 민간 평가기관 지정 ▪ 「전자정부구현을 위한 행정업무 등의 전자화 촉진에 관한 법률」을 「전자정부법」으로 개정
2008	▪ 정부조직 개편에 따라 각 정부부처에서 정보보호 관련기능 분담 수행 – 방송통신위원회: 통신사업자 등 민간부문 정보보호 – 행정안전부: 행정전자서명제도 운영, 주요정보통신기반시설 보호, 공공 분야 개인정보보호 – 지식경제부: 정보보호산업 육성 및 기술개발, 정보보호 전문인력 양성 ▪ 범국가 차원의 보안관제체계 구축 – 국방·외교·행정 등 10대 핵심부문 보안관제센터 설립
2009	▪ 7.7 DDoS 침해사고 발생 ▪ 국가 사이버위기 종합대책 수립 ▪ 한국인터넷진흥원(KISA) 출범(한국정보보호진흥원, 한국인터넷진흥원, 정보통신국제협력진흥원 통합)
2010	▪ 국군사이버사령부 설립 ▪ 전자금융거래 공인인증수단 다양화 ▪ 「전자정부법」 전부 개정(전자정부 관련 기능과 법령 통폐합)
2011	▪ 「개인정보 보호법」 제정 및 개인정보보호위원회 출범 ▪ 3.4 DDoS 침해사고 발생 ▪ 국가 사이버안보 마스터플랜 수립 및 시행
2013	▪ 3.20 사이버테러, 6.25 사이버공격 발생 ▪ 국가 사이버안보 종합대책 발표 ▪ 인터넷상 주민번호 수집 및 사용 제한제도 시행
2014	▪ 카드사 및 통신사 고객정보 유출, 개인정보보호 정상화 대책 발표 ▪ ●●, ⊛⊛ 해킹사고 및 ◇◇ DNS DDoS 침해사고 발생
2015	▪ 국가 사이버안보 태세 강화 종합대책 발표

자료: 미래창조과학부 등 제출자료

Ⅲ 감사결과

1. 감사결과 총괄

감사결과 [표 10]과 같이 국가 사이버안전 관리체계 분야, 행정·금융·보건의료 관련 소관별 주요 정보보호 업무 추진 분야에서 23건의 위법·부당 및 제도 개선 사항이 확인되었고, 그 외에 모범사례 1건을 발굴하였다.

[표 10] 지적사항 총괄

(단위: 건)

구분	합계	징계·문책	시정	주의	권고	통보	통보(모범)	현지조치
건수	24	2	-	5	-	15	1	1

감사결과 확인된 주요 문제점은 다음과 같다.

가. 국가 사이버안전 관리체계 분야

① **(기반시설 관리)** 중앙행정기관은 주요정보통신기반시설을 지정하고, 관리기관은 취약점을 평가한 후 보호대책을 수립·이행하여야 하며, 미래창조과학부는 주요정보통신기반시설 지정을 권고하고 관리기관이 수립한 보호대책의 이행을 점검하도록 되어 있는데 미래창조과학부에서 2014년 10월 "지정평가기준"을 마련하면서 제어시스템은 사이버침해 시 제어 불능이 문제이나 피해정도를 '정보유출 여부'로 평가하는 등 기반시설의 특성을 고려하지 않은 일률적인 지표로 평가하도록 되어 있어 ▶▶ 등 도시가스 3개사에 대해 2010년부터 2014년까지 4회에 걸쳐 지정권고를 하였는데도 기반시설 지정 여부에 대한 이견으로 미래창조과학부의 지정권고와 중앙행정기관의 미지정 결정이 반복되어 지정권고의 실효성이 떨어지고 있다.

② **(인력관리)** 행정자치부에서 정부 종합대책에 따라 정보보호 강화를 위해 2011년부터 2015년까지 미래창조과학부 등 40개 부처의 정보보호 전담인력 124명을 증원하는 등 정보보호 인력에 대한 관리를 하면서 15개 부처에서는 정보보호 전담인력 44명을 증원하고도 이 중 16명만 충원하고 28명은 미충원 또는 타 부서에

배치하거나 정보보호 업무 이외의 타 업무를 처리하고 있고, 36개 부처에서는 충원인력 81명 중 45명(55.6%)을 자격증 미소지자 또는 경력 미달자 등 비전문 인력으로 충원하였다.

한편, 미래창조과학부에서 민간 분야의 정보보호인력 양성시책을 추진하면서 2014년 7월 "고용창출지원사업"(고용노동부)을 통해 정보보호 인력을 채용한 중소기업을 지원(월 90만 원/인)하기로 계획하고도 미래창조과학부와 고용노동부에서 정보보호 인력 범위 등에 대한 상호 간의 협의가 지연되어 1년여 동안 시행되지 못하였다.

⇨ **이에 대하여**

○ **미래창조과학부장관에게 기반시설의 개별특성을 제대로 반영하도록 주요정보통신기반시설의 지정기준을 개선하고, 지정권고만 반복하고 있는데 대하여 정보통신기반보호위원회에 지정여부를 결정하는 방안을 마련하도록 통보하였으며**

○ **행정자치부장관에게 정보보호 전담인력을 증원한 데 대하여 각 중앙 부처에서 미충원 또는 타 부서에 배치하거나 타 업무를 병행하여 처리하지 못하도록 하는 등 효율적인 정보보호 인력 관리 방안을 마련하도록 통보하였고, 미래창조과학부장관과 고용노동부장관에게 정보보호 인력양성 시책이 지연·시행되는 일이 없도록 상호 간의 협의를 적기에 추진하는 등 정책 추진을 위한 협의 업무를 철저히 하도록 주의촉구하였다.**

나. 행정 · 금융 · 보건의료 소관별 주요 정보보호 업무 추진 분야

① **(행정)** 인터넷 상 주민등록번호 대체수단으로 방송통신위원회에서는 2005년 민간 아이핀, 행정자치부에서는 2008년 공공아이핀을 각각 도입하였는데, 2015년 3월 공공아이핀 75만 건이 부정 발급되었고, 2015년 6월 현재 349개 사이트에서 아이핀의 불법 거래가 이루어지고 있는데도 감독부처인 행정자치부와 방송통신위원회는 부정 발급되거나 도용된 아이핀 규모와 원인조차 파악하지 못하고 있는 실정이다.

또한, 아이핀 발급 시 법원행정처의 가족관계등록 전산정보자료가 연계되지 않는 점을 악용하여 법정대리인이 아닌 자가 만 14세 미만자의 법정대리인으로 행사하여 아이핀 8만 건을 무단 발급받아 현재 사용 중에 있으며, 사망자·영유아 등 인터넷 취약자에게도 아이핀 20만 건이 발급되었다.

한편, 행정자치부에서는 2015년 산하 한국지역정보개발원에서 관리하고 있는 공공아이핀 발급시스템을 통해 공공아이핀 75만 건이 부정 발급되는 해킹사고에 대한 사고처리를 하면서 위 75만 건 전부를 삭제하여 도용을 차단하였다고 발표하고 2차 암호를 도입하는 등 "아이핀 부정발급 재발방지 대책"도 수립하였다.

그런데 위 75만 건 외에 공공아이핀 7만여 건이 추가로 법정대리인을 통해 부정발급된 사실을 확인하고도 이를 은폐하였고, 이 중 2.7만 건에 대해서는 삭제요청 등 사후조치를 하지 않은 채 방치하였을 뿐만 아니라 위 대책 수립 시 법정대리인 여부를 확인하지 못하는 문제를 알고도 위 대책에서 누락시켰다.

② **(금융)** 금융위원회에서 전자금융 이용자 보호를 위해 금융사고에 대한 부정거래 탐지시스템(FDS)을 도입하고 준비금을 적립하도록 하는 등 사후책임을 강화하고 있으나 FDS를 구축한 32개 은행·증권·전자금융업자 중 13개 업체만 전담조직을 운영하고 있고, 50개 금융기관 중 47개 업체가 금융사고 시 준비금의 세부 지급기준을 마련하지 않고 있다.

또한, 2014년 5월 전자금융 이용자 편의성 제고를 위해 지급결제대행업체(PG, Payment Gateway)에 카드정보 저장을 허용하여 간편 결제하는 등의 방안을 마련·추진하고 있으나 「전자금융거래법」에는 PG사가 카드정보를 저장할 수 있는 '전자금융업자'로 규정되어 있는 반면 「여신전문금융업법」에는 PG사가 '결제대행업체'(신용카드 가맹점 지위)로 규정되어 있고 「신용카드 가맹점 표준약관」에는 카드사 허용 시에만 PG사가 카드정보를 저장 가능하도록 되어 있어 현재 40개 PG사 중 1개 사만 카드정보를 저장하고 있다.

③ **(보건의료)** 의료기관은 건강보험심사평가원에 요양급여비용 청구 시 위 평가원에서 인증한 청구소프트웨어를 통해 주민등록번호, 진료기록 등 환자의 의료정보를 제출하는데, 보건복지부에서 2013년 청구소프트웨어 개발업체인 ▲▲의 환자 의료정보 유출 사건 시 청구소프트웨어 등을 통해 의료정보가 유출될 수 있다는 사실을 인지하고도 청구소프트웨어 인증 시 보안기능 검사 등 의료정보 유출 재발방지 방안을 마련하지 않아 2015년 또다시 ▲▲ 등을 통해 조제정보 43억 건과 진료정보 7억 건이 불법 수집·유출되는 사고가 발생하게 되었다.

한편, 의료기관 휴·폐업 시 진료기록부 등을 보건소에 이관하되, '진료기록부 등 보관계획' 허가 시 의료기관 개설자도 보관 가능하도록 되어 있어 강남구 보건소 등 20개 보건소를 확인한 결과, 진료기록부 관리인력 부족 등으로 진료기록부 등이 안전성 확보 조치가 되지 않은 채 보관되고 있었고, 의료인의 가족 등 진료기록부 보관자격이 없는 자가 보관하는 등 부실하게 작성된 '진료기록부 보관계획'을 그대로 인정하였을 뿐만 아니라 사후점검도 실시하지 않고 있었다.

⇨ **이에 대하여**

○ **행정자치부장관 및 방송통신위원장에게 아이핀의 부정 발급·불법 거래 및 도용 등 문제에 대한 실효성 있는 해결 방안을 마련하도록 통보하였고, 행정자치부장관에게 공공아이핀의 대규모 부정발급 사고를 부당 처리하고 법정대리인을 통한 부정발급 문제를 은폐한 관련자에 대하여 징계처분하도록 요구하였으며**

○ **금융위원장에게 FDS 전담조직 운영을 활성화하는 방안과 금융사고 시 준비금을 지급할 수 있는 세부기준을 마련하고, PG사도 카드정보를 저장할 수 있도록 하기 위해 「여신전문금융업법」 및 「신용카드 가맹점 표준약관」을 개정하는 방안을 마련하도록 통보하였고**

○ **보건복지부장관에게 청구소프트웨어 등을 통해 의료정보가 유출되지 않도록 의료정보 보호 업무를 철저히 하도록 주의촉구하였으며, 안전성 확보조치가 미흡한 채 부실하게 관리되고 있는 휴·폐업 의료기관의 진료기록부 등에 대한 관리 개선 방안을 마련하도록 통보하였다.**

(3) 정보보호 인증제도 운영

실태

미래창조과학부 등에서 기업 등이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립·관리·운영하는 정보보호 관리체계를 평가하여 정보보호 수준을 측정하는 정보보호 인증제도로 [표 36]과 같이 정보보호 관리체계(ISMS[23]), 개인정보보호 관리체계(PIMS[24]), 개인정보보호(PIPL[25]) 인증 등을 운영하고 있다.

[표 36] ISMS, PIMS, PIPL 등 인증제도 비교

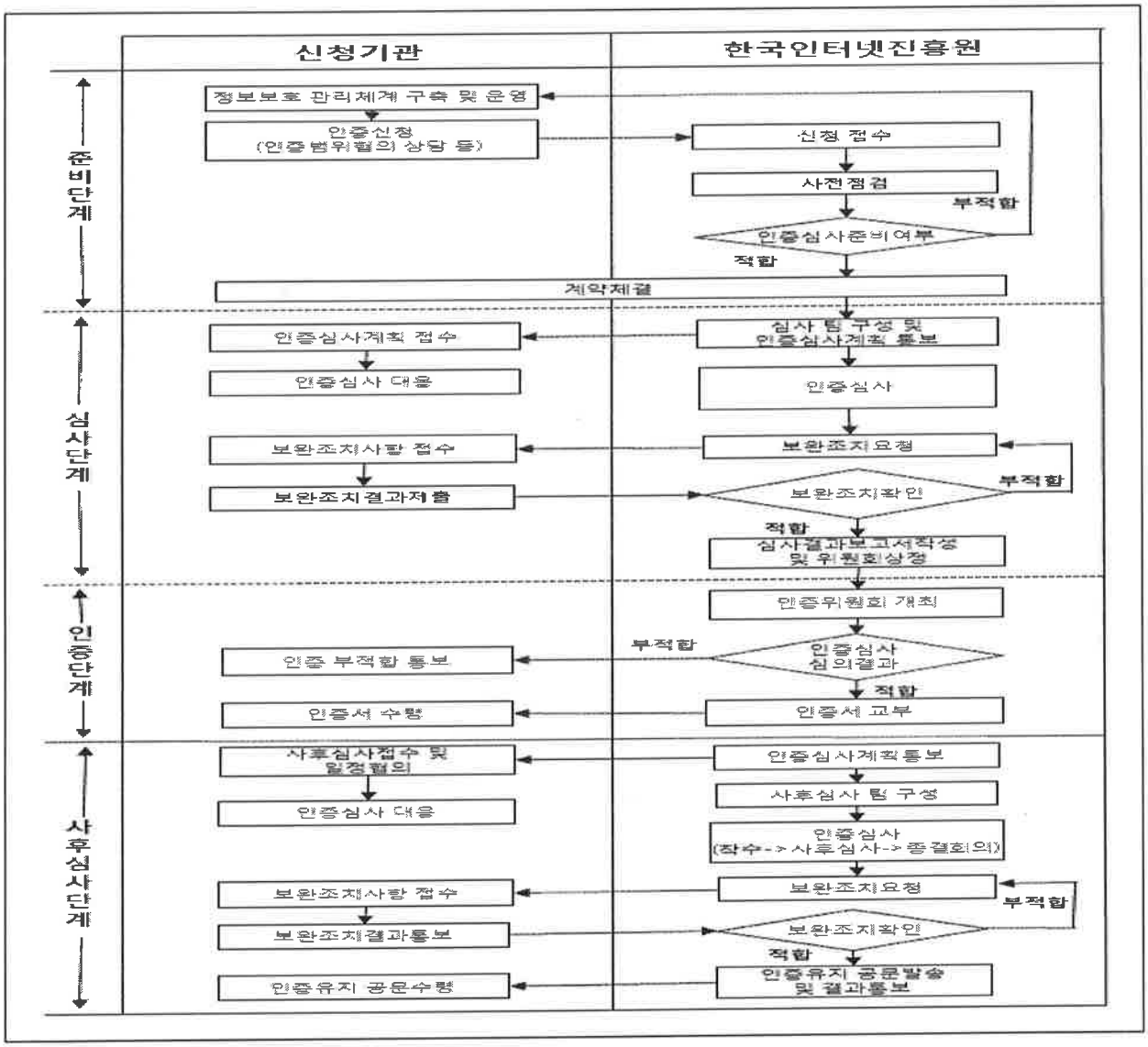
구 분	정보보호관리체계 인증 (ISMS, 미래창조과학부)	개인정보보호 관리체계 인증 (PIMS, 방송통신위원회)	개인정보 보호 인증 (PIPL, 행정자치부)
시행	2002년	2010년	2013년
제도성격	의무	임의	임의
도입목적	정보통신시스템으로 제공하는 서비스의 안정·신뢰성	정보통신시스템 내 개인정보처리 시스템을 통한 개인정보의 안전한 관리	개인정보의 안전한 관리
법적근거	「정보통신망법」 제47조	「정보통신망법」 제47조의3	「개인정보 보호법」 제13조의3
대상	정보통신서비스 제공 기업(기관) ※ 의무대상: ISP(인터넷서비스제공자), IDC(데이터센터) 및 연간 매출액 100억 이상 또는 일평균 이용자 수 100만 명 이상 기업	개인정보 수집· 취급 기업(기관) 암묵적으로 적용대상을 다음과 같이 구분 -PIMS: 정보통신서비스 제공 사업자(「정보통신망법」) -PIPL: 모든 개인정보처리자 대상(「개인정보 보호법」)	
점검 기준항목	미래창조과학부 고시	방송통신위원회 고시	행정자치부 고시
	104개	124개	최대 65개
인증기관	한국인터넷진흥원	한국인터넷진흥원	한국정보화진흥원
유효기간	3년	3년	3년
인증 현황	○○은행 등 392개 기업(기관) ('15년 9월 기준)	▼▼(주) 등 29개 기업(기관) ('15년 9월 기준)	♡♡등 13개 기업(기관) ('15년 9월 기준)
과태료	1,000만 원 (의무대상자)	-	-

자료: 한국인터넷진흥원 제출자료 재구성

23) Information System Management System의 약자
24) Personal Information Management System의 약자
25) Personal Information Protection Level의 약자

한편 ISMS 인증을 받고자 하는 기업 등은 「정보보호 관리체계 인증 등에 관한 고시」에 따라 [그림 3]과 같이 한국인터넷진흥원 등 인증기관과 인증범위를 협의한 후 인증심사를 준비하고, 인증기관에서는 인증심사팀을 구성하여 인증심사 및 보완조치를 확인한 후 인증위원회 심의·의결을 거쳐 인증서를 교부[26]한다.

[그림 3] ISMS 인증심사 및 사후심사 절차



자료: 한국인터넷진흥원 제출자료

26) 통상적인 ISMS 인증신청에서 인증서 교부까지는 4개월 소요(심사준비 30일, 인증심사 5일, 보완조치 30일, 인증위원회 심의준비 30일 등)되고 인증신청을 위해서는 ISMS를 구축한 후 최소 2개월 이상 운영하여 신청하여야 함

또한 위 인증기관에서는 ISMS 인증의 실효성 제고를 위하여 관리체계를 지속 유지하도록 매년 사후심사를 실시하며 미흡한 부분에 대한 보완조치를 확인한 후 인증을 유지하고 있다.

ISMS 인증심사는 서면심사와 현장심사로 진행되고 정보보호 관리과정(정보보호 정책 수립, 범위설정, 위험관리, 구현 및 사후관리로 연결되는 과정)과 정보보호 대책(정보보호 관리과정에 따라 수립한 통제사항)에 대하여 심사하며, 인증심사기준은 정보보호 관리과정 5개 분야에 대한 12개 통제항목과 정보보호 대책 13개 분야 92개 통제항목으로 구성된다.

ISMS 인증 의무대상자가 인증을 받지 아니하면 과태료 1천만 원이 부과되고 인증을 받은 기업은 공공 분야 정보시스템 사업 등의 기술성 평가 시 가점, 기업신용평가 시 가점 등 가산점 혜택을 가지며 ISMS 인증을 받은 내용을 기업 홍보에 이용할 수 있다.

이와 같은 ISMS 인증 시 인센티브, 인증 의무대상자 확대 및 정보보호에 대한 인식 제고 등으로 ISMS 인증을 받은 업체 수는 [표 37]과 같이 지속적으로 증가하여 2015년 10월 현재 392개 업체 등이 ISMS 인증을 유지하고 있고, 이 중 의무대상자는 276개 업체에 달한다.

[표 37] ISMS 인증 유지 현황(2011~2015년)

(단위: 개)

구분	2011년	2012년	2013년	2014년	2015년(10월)
인증업체 수	119	152	272	377	392
의무대상업체 수	-	-	134	271	276

자료: 한국인터넷진흥원 제출자료 재구성

문제점

가-(3)-1 정보보호 및 개인정보보호 인증제도 통합 추진 부적정

미래창조과학부(이하 "미래부"라 한다)와 방송통신위원회(이하 "방통위" 라 한다) 등에서 2014. 8. 5. 기업 등의 정보보호 수준을 측정하고 점검 항목도 서로 유사한 ISMS, PIMS, PIPL 인증제도를 중복 운영함으로써 발생하는 기업부담 가중 등의 문제를 해결하기 위해 개선방안을 마련하였다.

위 개선방안에 따르면 PIMS와 PIPL 인증제도는 주관부처, 인증기관 등이 상이하나 인증목적, 주요내용은 유사하여 부처 협의를 통해 2016년부터 통합 운영하는 것으로 결정되었다. 그리고 방통위와 행정자치부 간 협의 진행을 통해 2015. 7. 21. "공동고시 제정초안"을 마련하는 등 PIMS와 PIPL 인증제도의 통합이 정상적으로 추진되고 있었다.

한편 ISMS와 PIMS 인증제도는 정보보호 관리체계이나 규제성격, 인증목적, 심사내용, 심사관점 등이 다르므로 통합하지 아니하고 심사 시 유사중복 부분을 상호 인정해주는 것으로 결정하였다.

미래부와 방통위에서 ISMS와 PIMS 등 상호 유사한 정보보호 인증제도에 대한 통합운영 여부를 결정할 때에는 세부 심사항목별 중복성 정도에 대한 검토결과, 통합운영에 따른 장·단점 분석결과 등을 토대로 객관적·합리적으로 결정하는 것이 바람직하다.

이에 감사원 감사기간(2015. 8. 24.~10. 14.) 중 ISMS와 PIMS의 인증제도 간 운영과 관련하여 검토한 결과, 위 두 관서에서는 ISMS와 PIMS 인증제도에

대해 2015년 1월부터 인증범위가 중복되는 영역에 한하여 상호 인정을 시행하고 있었으나 다음과 같은 문제가 발견되었다.

① ISMS와 PIMS의 심사항목과 평가기준 상호 유사

위 두 관서에서 두 인증제도의 심사항목이 상이하다고 검토[27](2014. 8. 5.)하였으나 감사원 감사기간 중 ISMS와 PIMS의 심사항목 중복성을 검토한 결과 [별표 3] "ISMS와 PIMS 심사항목 중복 현황(2015. 9. 9.)"과 [표 38]과 같이 두 인증제도의 심사항목 평균 74%가 유사·중복[28]된 것으로 나타났다.

[표 38] ISMS와 PIMS 심사항목 중복성 검토 결과

(단위: 개)

ISMS 고유항목	PIMS 고유항목	동일항목	유사항목주)	합계
19	41(생명주기 등)	42	44	146

주: 유사항목은 ISMS 기준 43개, PIMS 기준 41개이며, 두 기준의 합집합은 44개(세부 내용은 [별표 3] 참조)
자료: 한국인터넷진흥원 제출자료 재구성

② ISMS와 PIMS 간 연계운영 필요성에 대한 검토 미흡

[그림 4]와 같이 ISMS의 경우에는 인증범위 내 시스템과 서비스의 안정성·신뢰성 차원에서 깊이 있는 심사가 이루어지나 인증범위 밖에서의 개인정보 흐름을 고려하지 못하고 있다.

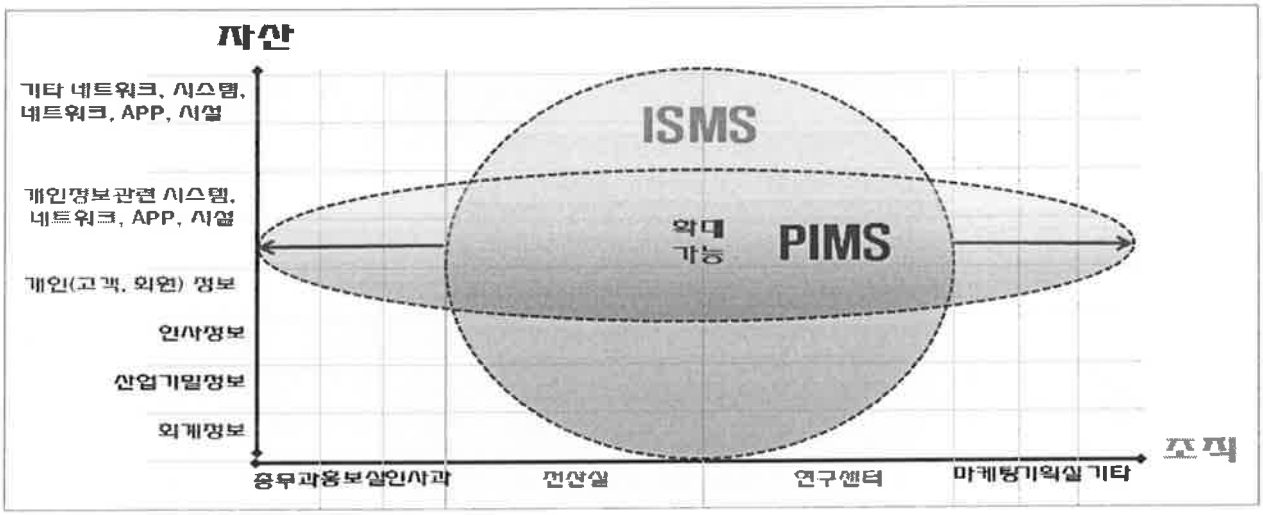
또한, PIMS는 전사 범위에서 개인정보의 흐름을 고려하고 있지만 시스템과 서비스의 안정성·신뢰성 측면에서 ISMS에 비해 심도 있게 다루지 못하는 문제가 있다.

---

27) 당시 미래부와 방통위에서 검토한 내용을 확인한 결과 각각의 심사항목을 구체적으로 비교·분석하지 아니한 채 유사항목은 점검항목에서 제외하였다는 사유로 동일항목(37%)만 검토하여 심사항목이 다른 것으로 검토됨

28) PIMS 인증기준(124개) 중 ISMS와 동일하거나 유사한 인증기준의 비율은 67%(83개)이고, ISMS 인증기준(104개) 중 PIMS와 동일하거나 유사한 인증기준의 비율은 81.7%(85개)이며, 두 비율의 평균은 74%. 그리고 PIMS 인증기준에서 생명주기(32개)를 제외할 경우 90%가 중복

[그림 4] ISMS 및 PIMS 인증범위 중복 현황



자료: 한국인터넷진흥원 제출자료 재구성

그리고 감사원 감사기간 중 한국인터넷진흥원에서 제출한 최근 5년간(2011~2015년) 주요 개인정보 유출사고를 분석한 결과 [별표 4] "최근 5년간 개인정보 침해사고 분석 결과"와 같이 전체 50건 중 31건[29](62%)이 웹 서버 등에서 웹쉘 등을 통해 우회적으로 유출되는 해킹사고로 발생되는 등 개인정보 보호는 정보통신시스템 정보보호 활동과 밀접한 관계가 있었다.

또한, ISMS 인증만 받을 경우 정보통신시스템에 대한 침해 활동으로 개인정보가 유출될 우려가 있는 등 개인정보에 대한 보호는 담보할 수 없다.

【정보통신시스템 해킹이 개인정보 유출로 이어진 사고 사례】

▪ 2014년 3월 ㈜●●에서 발생한 982만 명의 개인정보 유출사고의 경우

- ㈜●●가 2013년 12월 정보통신서비스 인프라운영 등에 대해 ISMS 인증심사를 받았으나 개인정보 보호 부문에 해당하는 ●●의 ♥♥ 홈페이지는 점검대상이 아니어서 해킹에 취약(고객서비스계약번호에 대한 검증 없이 DB정보를 조회)한 상태로 운영하다가 개인정보 유출사고 발생

29) 나머지 19건은 관리자 실수, 프로그램 오류 등에 의해 유출

이와 같이 ISMS나 PIMS를 상호 연계하지 않은 채 개별적으로 점검할 경우 고조되는 사이버 침해행위로부터 안전을 담보하기 어렵다.

③ ISMS와 PIMS 중복운영에 따른 기업부담 완화 곤란

감사원 감사기간 중 위 두 인증제도를 동시에 인증받은 기업을 대상으로 인증범위가 중복되는지 확인한 결과 [별표 5] "ISMS/PIMS 동시 인증기업의 인증범위 중복 현황"과 같이 PIMS 인증을 받은 사업자 총 29개 중 23개 사업자(79%)가 ISMS와 PIMS 인증을 동시에 취득하고 있었고 23개 사업자의 ISMS와 PIMS 인증범위의 평균 81.3%가 중복되는 것으로 나타났다.

위 "①항" 내지 "③항"와 같이 종합적인 정보보호 관리체계 확보가 어려울 뿐 아니라 ISMS와 PIMS 인증을 모두 취득하고자 하는 기업에 대하여 경제적[30]·행정적 부담 등을 줄 우려가 있다.

관계기관 의견 미래부와 방통위에서는 감사결과에 별다른 이견을 제기하지 않으면서 상호 협의하여 ISMS와 PIMS를 통합하는 방안을 마련하겠다는 의견을 제시하였다.

조치할 사항 **미래창조과학부장관**과 **방송통신위원회 위원장**은 서로 협의하여 기업부담을 최소화하면서 개인정보 보호를 포함하는 종합적인 정보보호 관리체계를 수립하기 위해 ISMS와 PIMS 인증제도를 통합하는 방안을 마련하시기 바랍니다.**(통보)**

---

30) 인증신청기업의 종업원 수 300명, 서버급 컴퓨터 100대, 심사일수 9일 기준으로 ISMS인증에 소요되는 비용은 15백여만 원, PIMS인증에 소요되는 비용은 23백여만 원(사후관리 1·2차 포함, 수수료 감면 혜택 30% 적용 시)

나. 행정·금융·보건의료 소관별 주요 정보보호 업무 추진 분야

(1) 행정 부문

실태

(가) 아이핀 제도 개요

국가 행정업무의 효율성을 제고하고 국민에게 편리한 행정서비스를 제공하고자 도입한 주민등록번호(이하 "주민번호"라 한다)는 금융, 통신 등 다양한 민간분야에서 활용되었고, 인터넷이 활성화되면서 본인 식별수단으로 회원 가입, 결제, 게시판 등의 서비스를 이용할 때 실명 확인, 성인인증의 수단으로 광범위하게 사용되었다.

그런데 개인을 고유하게 식별할 수 있고 평생 변동이 없는 주민번호는 그 특성 때문에 일단 노출될 경우, 변경이 어렵고 인터넷을 통해 무한 복제될 수 있어 계정 도용, 금융사기 등의 피해가 지속적으로 발생하고 있다.

특히 국내 주요 포털, 인터넷 쇼핑몰은 물론 금융기관 등 각종 사업장에서 수집한 주민번호가 관리 소홀이나 해커 공격으로 유출되는 사고가 빈발함에 따라 인터넷 상에서 주민번호의 안전성에 대한 불안이 심화되었다.

이에 따라 인터넷상에서 주민번호를 대체하는 본인확인 수단으로 본인이 원하는 경우 언제든지 변경이 가능한 아이핀(I-PIN, Internet Personal Identification Number) 제도를 도입하게 되었다.

(나) 아이핀 제도 추진 경과

① 민간아이핀

방송통신위원회(구 정보통신부, 이하 "방통위"라 한다)에서 2005년 10월 주민번호

도용 및 유출에 대응하기 위해 「주민번호 대체수단 가이드라인」을 제정한 후 주민번호를 대체하는 본인확인 수단으로 아이핀을 개발·보급하였다.

그리고 방통위에서는 2008. 6. 13. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다) 제23조의2 제1항에서 정보통신서비스 이용자가 회원으로 가입할 때 주민번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하도록 정함에 따라 2009. 1. 28. 같은 법 시행령 제9조의2 제1항에서 일평균 이용자 수를 기준으로 일반 웹사이트는 1만 명 이상, 포털은 5만 명 이상인 경우에는 주민번호를 이용하지 않은 회원가입수단을 의무적으로 제공하도록 "주민번호 대체수단 의무제공 사업자 기준"을 마련하였다.

또한 방통위에서는 2009. 3. 31. "인터넷상 주민번호 대체수단(I-PIN) 이용 활성화 기본계획" 수립 및 「본인확인기관의 지정 및 관리에 관한 지침」을 제정[33] 하여 인터넷 상에서 주민번호를 대체하는 아이핀의 보급 확대를 위해 한국인터넷진흥원에서 아이핀 계정(ID) 통합관리시스템[34]을 개발하고 본인확인 관련 법령이 마련되는 2011년 4월까지 위 지침을 아이핀 발급·관리 업무에 적용하도록 하는 등 민간분야에서 아이핀을 전면적으로 확산할 수 있도록 추진하였다.

이후 2011. 4. 5. 본인확인기관 지정을 위한 근거를 마련하고자 정보통신망법을 개정하고 같은 해 10. 4. 본인확인기관 3곳[35]을 지정하면서 본격적으로 아이핀 제도를 시행하게 되었다.

2012. 2. 17. 정보통신망법에서 법령이 이용자의 주민번호 수집 또는 이용을

33) 2005년 10월 본인확인기관(5개사)별 I-PIN 서비스가 개시되어 이용자들이 I-PIN을 사용할 수 있었지만 본인확인기관에 대한 법령은 미비

34) 이용자가 아이핀 이용 시 아이핀을 발급받은 본인확인기관을 기억하지 않고도 사용할 수 있도록 하는 시스템

35) ◐◐(주), ◑◑(주), ♨♨(주)

허용하는 경우와 주민번호 수집·이용이 불가피한 경우를 제외하고는 주민번호 수집을 금지하면서 [표 40]과 같이 전체 아이핀 발급량이 증가하고 있고, 그동안 민간아이핀 발급 건수는 [표 41]과 같다.

[표 40] 연도별 아이핀 발급 증가 추세

(단위: 건)

구분	2008~2011년	2012년	2013년	2014년
민간	3,408,310	1,847,307	6,610,087	3,380,949
공공	1,061,173	617,179	892,771	1,525,888

자료: 한국인터넷진흥원, 한국지역정보개발원 제출자료 재구성

[표 41] 아이핀 가입자 수(누적 발급건수 기준)

(단위: 만 건)

본인확인기관	2011년	2012년	2013년	2014년
◐◐(주)	180	284	636	815
◑◑(주)	147	212	416	531
♨♨(주)	14	30	134	178
계	341	526	1,186	1,524

주: 공공아이핀 발급건수는 409만 건(2014년 기준)
자료: 한국인터넷진흥원 제출자료 재구성

② 공공아이핀

구 행정안전부에서는 구 「공공기관의 개인정보보호에 관한 법률」(2010. 3. 22. 법률 제10142호, 「개인정보 보호법」으로 개정되기 전의 것) 제9조에서 '공공기관의 장은 개인정보가 분실·도난·누출되지 않도록 안전성 확보 조치를 해야 한다'고 정한 데 따라 [표 42]와 같은 절차를 거쳐 2007년 12월 한국지역정보개발원과 'G-PIN 센터운영사업 위·수탁업무수행 계약'을 맺는 등으로 공공아이핀 제도를 도입·시행하였다.

[표 42] 공공아이핀 도입 추진 현황

연월	추진 내역	내용
2006. 5.	공공기관 홈페이지 개인정보 노출 방지대책 수립·시행	- 개인정보의 홈페이지 게재 방지 - 홈페이지상 개인정보 노출 여부를 각종 평가에 반영
2006. 5.	행정자치부 정책조정회의	- 본인확인을 할 수 있도록 공인인증서 활용 등 보완대책 - '07년 이후 전 공공기관으로 서비스 확대 실시
2006. 6.	대전광역시 시범사업 착수	- 대전광역시를 시범기관으로 선정 - '06년 말까지 사업 완료 및 시험 운영
2006. 8.	인터넷 통합ID관리 서비스 추진계획	- 온라인상에서 본인확인을 위한 새로운 기술 도입 - 민간 유료서비스를 대체할 수 있는 효율적 수단 확보
2007. 8.	통합ID관리센터 구축사업 추진계획	- 인터넷상 본인확인수단으로 주민번호 대체서비스 개발·보급 - 국민의 개인정보를 안전·편리하게 사용하도록 정보보호 환경 조성

자료: 행정자치부 제출자료 재구성

이후 구 행정안전부에서는 2011. 5. 6.「개인정보 보호법」 제24조 제2항(2011. 3. 29. 제정)과 정보통신망법 제44조의5 제1항의 규정에 따라 국가, 지방자치단체 등 공공기관이 운영하는 웹사이트에서 회원 가입을 할 때 주민번호 대신 공공아이핀을 사용하게 하는「공공기관 I-PIN 의무도입 적용 지침」을 마련하는 등으로 공공아이핀 제도를 시행하였다.

그동안 공공아이핀 운영 관련 예산과 이용 현황은 [표 43] 및 [표 44]와 같다.

[표 43] 공공아이핀 예산 현황

(단위: 백만 원)

아이핀 업무 수행기관	합계	2011년 이전	2012년	2013년	2014년	2015년
한국지역정보개발원	14,088	8,850	1,331	1,279	1,314	1,314
한국인터넷진흥원[주)]	1,696	897	195	170	210	224
합계	15,784	9,747	1,526	1,449	1,524	1,538

주: 민간아이핀과의 통합ID 관리를 위하여 공공아이핀 연동시스템을 구축·운영

자료: 행정자치부 및 한국인터넷진흥원 제출자료 재구성

[표 44] 공공아이핀 이용 현황

(단위: 건)

구분	합계	2011년 이전	2012년	2013년	2014년	2015년 5월
보급건수	13,474	7,108	5,247	793	258	68
발급건수	5,049,990	1,061,173	617,179	892,771	1,525,888	952,979
이용건수	21,706,339	3,405,252	2,861,372	4,074,570	6,339,545	5,025,600

자료: 한국지역정보개발원 제출자료 재구성

감사원 감사기간(2015. 8. 24.~10. 14.) 중 확인한 결과, 아이핀을 발급받을 때 필수 입력 사항은 [표 45]와 같고, 아이핀 발급 시 본인 확인 수단은 [표 46]과 같이 주로 휴대폰(65.3%)과 공인인증서(15.6%)로 이루어지고 있다.

[표 45] 아이핀 발급 시 확인사항

구분	필수 입력사항			본인 확인 방법				
	주민번호	아이디	비밀번호	공인인증서	휴대폰	주민등록발급일자	방문신청	법정대리인주)
민간아이핀	○	○	○	○	○	×	○	○
공공아이핀	○	○	○	○	×	○	○	○

주: 만 14세 미만 아동에게 아이핀을 발급할 때 법정대리인의 주민등록발급일자, 공인인증서, 휴대폰을 사용

[표 46] 아이핀 발급 시 본인확인 수단별 현황(2015. 8. 31.)

(단위: 건, %)

구분	계	휴대폰	공인인증서	신용카드	주민등록발급일자	방문신청	법정대리인	여권, 아이핀
계	21,823,783 (100)	14,252,442 (65.3)	3,396,449 (15.6)	1,072,621 (4.9)	1,454,241 (6.7)	189,078 (0.9)	1,401,450 (6.4)	57,502 (0.2)
한국지역정보개발원	5,463,000 (25)	-	2,897,965 (53.1)	-	1,454,241 (26.6)	182,277 (3.3)	921,616 (16.9)	6,901 (0.1)
◐◐(주)	8,939,115 (41)	7,596,915 (85.0)	255,764 (2.9)	596,013 (6.7)	-	2,805 (0.0)	440,092 (4.9)	47,526 (0.5)
◑◑(주)	5,466,215 (25)	4,879,279 (89.3)	191,170 (3.5)	357,848 (6.5)	-	2,352 (0.0)	32,491 (0.6)	3,075 (0.1)
♨♨(주)	1,955,453 (9)	1,776,248 (90.8)	51,550 (2.6)	118,760 (6.1)	-	1,644 (0.1)	7,251 (0.4)	-

주: 공공아이핀 법정대리인의 경우 사용된 본인확인 수단은 공인인증서 45.5%, 주민번호발급일자 52.1%임
자료: 한국지역정보개발원 및 민간아이핀 발급기관 제출자료 재구성

그리고 2010년 9월부터 공공아이핀 서비스와 민간아이핀 서비스가 통합·연계 운영됨에 따라 공공아이핀 발급기관(한국지역정보개발원)과 민간아이핀 발급기관[36]은 서로 다르나, 사용자 입장에서는 아이핀을 적용하는 웹사이트에서 공공아이핀 또는 민간아이핀 구분 없이 아이핀을 사용할 수 있게 되었다.

(다) 웹사이트 회원 가입 시 본인확인 현황

우리나라는 1990년대 후반 본격적으로 인터넷이 보급되고 이용자가 급증하여

36) ◐◐(주), ◑◑(주), ♨♨(주)

2015년 현재 인터넷 보급률이 세계 최고로 개인생활에 일대 변혁을 맞이했으나 2005년경 인터넷상에서 개인의 신상정보 공개 및 언어폭력 등으로 인한 피해 사례들이 잇달아 발생하는 등 인터넷 상에서의 언어폭력, 명예훼손, 개인정보 유출 등의 역기능이 발생하였다.

이에 방통위에서는 2007. 1. 26. 정보통신망법 제44조의5의 규정을 신설하는 등으로 본인확인제도를 도입하였는데, 그 취지는 인터넷상에서 본인확인정보를 이용하여 이용자를 안전하게 식별·인증하기 위한 것이다.

문제점

나-(1)-1 아이핀 제도 운영·관리 부적정

아이핀은 주민등록번호(이하 "주민번호"라 한다)를 대체하기 위해 도입된 본인확인수단으로서 인터넷 웹사이트에서 회원가입·연령확인(성인인증)·게시판 글쓰기 등을 하고자 하는 이용자가 주민번호 대신 아이핀을 사용할 경우, 다음과 같은 장점 또는 기대효과가 있다.

주민번호는 개인을 고유하게 식별할 수 있는 정보로서 평생 변동이 없는 특성 때문에 일단 노출될 경우 변경이 어렵고 인터넷을 통해 무한 복제될 수 있어 계정 도용, 금융사기 등의 피해가 지속적으로 발생하는 데 반해 아이핀은 무료로 공공·민간 웹사이트에서 본인확인을 할 수 있는 서비스로 아이핀이 유출되더라도 언제든 폐기하고 재발급을 받을 수 있으므로 아이핀 도용의 위험을 줄이면서 온라인에서 주민번호를 대체할 수 있다.

그러나 부정 이용자가 타인 명의로 아이핀을 부정 발급받을 경우, 유출된 사실을 본인이 알 수 없어 폐기·재발급 요청을 하기 어렵고, 명의가 도용된 사람은 개인정보 유출로 인해 심각한 피해를 입을 수 있다.

따라서 행정자치부(이하 "행자부"라 한다)와 방송통신위원회(이하 "방통위"라 한다)에서는 아이핀이 부정 발급되거나 불법 거래되지 않도록 제도 운영상 부작용과 문제점은 없는지 상시 점검하여 문제점이 있는 경우 이에 대한 개선방안을 마련하는 등 아이핀 제도 운영에 대한 관리·감독을 철저히 하여야 한다.

그런데 이번 감사원 감사기간 중 아이핀 제도 운영실태를 점검한 결과 다음과 같은 문제점이 있었다.

① 아이핀 부정 발급 및 불법 거래

한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)에서는 인터넷상에서 타인 명의 아이핀을 불법 거래하는 웹사이트를 [표 47]과 같이 '아이핀 대량', '아이핀 판매' 등의 검색어로 검출한 후 삭제하고 있다.

[표 47] 아이핀 불법 거래 관련 노출 검색 및 삭제 현황(2015. 3. 1.~6. 24.)

(단위: 건, %)

검색어	국내			국외			삭제율 (B/A)
	검출	정탐(A)	삭제(B)	검출	정탐(A)	삭제(B)	
아이핀_대량	2,220	15	13	137	9	-	54.17
아이핀_판매	2,422	257	72	134	73	32	31.52
아이핀_구매	1,323	3	3	69	-	-	100.00
아이핀_팝니다	1,291	184	98	141	51	28	53.62
아이핀_아이디_거래	1,478	10	9	62	1	1	90.91
아이핀판매	70	2	2	3	1	1	100.00
I-PIN	116	-	-	39	-	-	0.00
아이핀_거래	729	-	-	49	-	-	0.00
아이핀_삽니다	463	2	-	35	-	-	0.00
합계	**10,112**	**473**	**197(42)**	**669**	**135**	**62(46)**	**42.60**

주: 정탐은 아이핀을 불법으로 판매하는 것으로 확인된 웹사이트임
자료: 한국인터넷진흥원 제출자료 재구성

그러나 인터넷진흥원에서는 2015년 6월 현재 아이핀을 불법 판매하는 608개 웹사이트를 확인하고도 직접 삭제할 권한이 없어 해당 웹사이트에 자진 삭제를 요청하기만 한 결과 608개 중 259개 웹사이트만 자진 삭제하였고 나머지 349개 웹사이트에서 아이핀이 여전히 불법 판매되고 있으며 아이핀 불법거래 웹사이트 서버 608개 중 135개가 미국 등 국외에 위치하고 있어 웹사이트가 삭제되기 어려운 실정이다.

한편 2015. 2. 27.부터 같은 해 3. 2.까지 해커가 보유하고 있던 개인정보(이름, 주민번호)를 공인인증서 승인값과 함께 서버로 계속 전송하여 아이핀 75만여 건을 부정 발급받는 사고가 발생하였을 뿐 아니라 이번 감사원 감사기간 중 확인 결과 문제점 "②항" 내지 "③항"과 같이 가짜 법정대리인이 14세미만 미성년자 명의로 79,275건의 아이핀을 부정 발급받았거나 사망자에게도 794건이 발급되는 등 아이핀 부정 발급이 이루어지고 있었다.

또한 아이핀을 부정 발급한 원인을 규명하기 위해 인터넷진흥원에 조사 의뢰한 결과 부정 발급된 아이핀들이 '정상 발급된 아이핀으로 현재로는 부정 발급의 원인을 파악할 수 없다'고 회신하였다.

이와 같이 아이핀 불법 거래 사이트에서 쉽게 부정 발급된 아이핀을 구매할 수 있고, 위 아이핀이 어떤 경위로 부정 발급되었는지에 대해 정보보호 전문기관인 인터넷진흥원에서도 파악할 수 없는데도 행자부와 방통위에서는 타인 명의로 발급되어 도용되고 있는 아이핀이 어느 정도 규모인지와 그 원인은 무엇인지에 대해 제대로 파악하지 않고 있다.

② 법정대리인 검증 없이 만 14세 미만 아동에 대해 아이핀 발급

행자부와 방통위에서는 아이핀 발급 사업자로 하여금 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제31조와 「개인정보 보호법」 제22조 제5항의 규정에 따라 만 14세 미만 아동은 법정대리인의 동의를 받아 아이핀을 발급하여 주도록 하고 있다.

그러나 행자부와 방통위에서는 대법원에서 운영하는 가족관계등록부와 아이핀 시스템을 연계하지 않고 있어 법정대리인의 진위 여부를 알 수 없는데도 이러한 문제를 근본적으로 해결하지 않고 있으며, 법정대리인을 통한 아이핀 발급을 보류하거나 중단하는 등의 책임 있는 조치는 하지 않은 채 법정대리인 1명당 만 14세 미만 아동에게 5건까지 아이핀을 발급해 주고 있다.

이에 감사원에서 만 14세 미만 아동 명의로 발급된 아이핀 1,325,455건에 대하여 대법원 가족관계등록부에 조회한 결과 [표 48]과 같이 가짜 법정대리인이 79,275건의 아이핀을 부정 발급받은 것으로 확인되었다.

[표 48] 법정대리인 명의(만 14세 미만 아동) 아이핀 발급 실태(2015. 8. 31.)

(단위: 건)

구분	계	법정대리인	법정대리인과 무관		
			소계	법정대리인 확인 불가	기타주)
총계	1,325,455	1,246,180	79,275	76,272	3,003
한국지역정보개발원	916,863	875,319	41,544	40,840	704
◐◐(주)	369,241	335,882	33,359	32,566	793
◑◑(주)	32,100	29,018	3,082	2,255	827
♨♨(주)	7,251	5,961	1,290	611	679

주: 아동과 법정대리인 동일, 미존재 주민번호 등 시스템 오류인 경우와 외국인인 경우
자료: 한국지역정보개발원 및 민간아이핀 발급기관 제출자료 재구성

③ 사망자와 인터넷 취약자(만 7세 이하, 만 80세 이상) 등에 대한 아이핀 발급

아이핀의 부정 발급 실태를 파악하기 위해 한국지역정보개발원 등 4개 아이핀

발급기관에서 2014. 1. 1.부터 2015. 6. 30. 사이에 발급한 아이핀 7,588,688건에 대하여 분석·점검하였다.

그런데 [표 49]와 같이 사망 후에도 아이핀 794건이 발급되고, 사망 후에도 1,158건이 사용하고 있었으며, 인터넷 취약계층인 만 7세 이하인 자에게 186,197건, 80세 이상 고령자에게도 14,437건의 아이핀이 발급되는 등 사망자 등을 포함한 계 202,586건 대부분의 아이핀이 부정 발급되어 다른 사람이 사용하는 것으로 추정되었다.

[표 49] 사망자와 만 7세 이하 영유아 등에 대한 아이핀 발급 현황(2014. 1. 1.~2015. 6. 30.)

(단위: 건)

구분	합계	사망자			7세 이하	80세 이상
		소계	사망 후 발급자	사망 후 사용자		
한국지역정보개발원	162,519	104	29	75	159,112	3,303
◐◐(주)	25,305	977	401	576	19,967	4,361
◑◑(주)	13,635	765	317	448	6,964	5,906
♨♨(주)	1,127	106	47	59	154	867
합계	202,586	1,952	794	1,158	186,197	14,437

자료: 한국지역정보개발원 및 민간아이핀 발급기관 제출자료 재구성

<사망자, 7세 이하 영유아 등의 아이핀 발급 및 사용 사례>

- A(아이디: 目目, 1974년생)는 2014. 8. 15. 공공아이핀을 발급받은 후 같은 해 12. 11. 사망, 그런데 사망 74일 후인 2015. 2. 23.까지 법무부 홈페이지에서 교정본부 수용자에게 인터넷 서신을 보내거나 화상접견 예약을 하는 등 사망 후 141차례 본인 확인
- B(아이디: 皿皿, 1928년생)은 88세 때인 2014. 5. 10. 민간아이핀을 발급, 청소년용 게임과 게임아이템 거래 웹사이트 등에 106차례 본인 확인, 같은 해 11. 16. 사망 후에도 스포츠 게임 등에서 42차례 본인 확인
- C(아이디: 冊冊, 2011년생)는 4살 때인 2015. 2. 26. 공공아이핀을 발급, 같은 날부터 육군 군수사령부(www.logcmd.mil.kr)에 접속하여 11차례에 걸쳐 본인 확인을 하였으나, 웹사이트에는 성명만 남아 있어 아이핀 이용목적 확인 불가

한편 위와 같은 문제점과 관련하여 감사원에서 2015. 11. 4. 정보보호 관련 산·학·연 전문가 자문회의를 개최한 결과, 6명 중 4명의 전문가가 아이핀 제도

개선 및 재검토 등이 필요하다는 의견을 제시하였다.

<사이버보안 전문가 2차 자문 결과>

- 아이핀 폐지 및 본인 확인 최소화 필요 (D 박사, 전 국군사이버사령관)
- 아이핀 제도 전면 재검토, 주민번호 수집·사용 최소화 필요 (E ㅎㅎ대학교 교수)
- 휴대폰 인증 등 대체수단 검토 필요 (F 한국인터넷진흥원 ○본부장)
- 아이핀 용도가 의문시, 본인확인 최소화 정책과 연계 검토 필요 (G ◎연구소 소장)

그리고 감사원에서 2015. 10. 8.부터 같은 해 12. 17.까지 △△대학교 산학협력단에 "인터넷 본인확인 및 아이핀 제도 관련 진단과 개선방안"에 대한 연구를 의뢰한 결과 아이핀은 아이디와 패스워드를 기반으로 하는 인증 방식이므로 인터넷상에 아이디와 패스워드가 노출되거나 탈취될 경우 명의 도용 및 개인정보 유출 문제가 발생할 가능성이 높다고 하였다.

또한 아이핀을 통한 본인확인 기술시장의 국가 개입은 특정 본인확인 기술을 유리하게 취급하거나 사용을 강제하게 되므로 휴대폰 인증기술, 범용공인인증서 기술 등 다른 본인확인 기술이 아이핀 기술과 공정하게 경쟁할 수 없도록 하는 등 기술중립성[37] 위반이 발생한다고 하였다.

관계기관 의견 및 검토결과 행자부와 방통위에서는 아이핀의 경우 주민번호와 달리 도용 또는 유출되더라도 쉽게 폐기·재발급되기 때문에 피해를 최소화할 수 있다고 주장한다.

그러나 아이핀은 주민번호를 기반으로 생성·발급되는데 아이핀을 부정 발급받는 경우 유출된 사실을 본인이 알 수 없어서 폐기·재발급 요청을 하기

37) 기술 중립성이란 시장 참여자에게 가장 적합한 기술의 선택권을 부여하기 위하여 기술과 관련된 정책에서 특정 기술을 유리하게 취급하거나 특정 기술 사용의무를 부과하지 말아야 한다는 원칙(EU FrameWork Directive 2002/21)

어려우므로 이같은 주장은 받아들이기 어렵다.

그리고 행자부에서는 2015. 10. 6. 만 14세 미만 아동에 대한 아이핀 발급 시 법정대리인 여부를 주민등록시스템을 통해 검증하도록 개선하였으며, 사망자나 인터넷 취약자에게 발급된 아이핀은 사망자 유가족, 부모 등 가족이 사용하기 때문에 부정 사용이라고 단정할 수 없다고 주장한다.

그러나 주민등록시스템으로는 법원 가족관계등록시스템과 달리 만 14세 미만 아동에 대하여 세대주가 부모인 경우에만 검증되는 한계가 있으므로 주민등록시스템과 연계하였다고 하여 법정대리인의 문제점을 해결하였다고 보기 어렵고, 주민등록시스템이 해킹에 취약한 아이핀 시스템과 연계되어 해킹을 당할 경우 주민등록번호 유출 등 또다른 피해가 발생할 우려가 있다.

그리고 유가족 등이 인터넷 취약자에 발급한 아이핀을 사용하였다고 단정할 수 없고, 가족이 사용하였다고 하더라도 본인이 아니라면 문제의 소지가 있을 수 있으므로 가족의 아이핀을 사용하는 것은 부정 사용이 아니라는 주장도 받아들이기 어렵다.

조치할 사항 **행정자치부장관**과 **방송통신위원회 위원장**은 아이핀의 부정 발급·불법 거래 및 도용 등의 문제에 대한 실효성 있는 해결 방안을 마련하시기 바랍니다.**(통보)**

나-(1)-2	해킹에 의한 대규모 아이핀 부정 발급 사건 부당 처리

① 사건개요 및 진행사항

기관을 한국지역정보개발원으로 정한 「개인정보 보호법 시행령」 제62조 제2항을 개정하여 전문성과 역량을 갖춘 전문기관에 공공아이핀 관리업무를 위탁할 예정이라는 의견을 제시하였다.

그러면서도 위 시행령 개정안에는 '한국지역정보개발원 또는 한국인터넷진흥원 등에 위탁할 수 있다'라고 되어 있어 행자부의 산하기관인 한국지역정보개발원을 배제하지 않고 여전히 위탁할 수 있는 여지를 남겨 두고 있다.

조치할 사항 **행정자치부장관**은 공공아이핀 관리업무를 설립 취지 등에 맞지 않고 전문 인력 등 역량·전문성이 떨어지는 기관에 위탁하는 일이 없도록 하고 공공아이핀 관리 위탁업무를 철저히 하시기 바랍니다.**(주의)**

나-(1)-4 인터넷상의 불필요한 본인확인 요구 개선 미흡

인터넷상에서의 본인확인은 민간·공공 인터넷 웹사이트 이용자가 회원가입, 온라인 쇼핑 시 결재 등을 할 때에 본인인지 여부를 확인하는 것으로서 상당수의 웹사이트에서 본인확인을 요구하고 있고, 본인확인을 하지 않을 경우 해당 인터넷 웹사이트에서 제공하는 서비스를 이용할 수가 없다.

미국 등 외국의 경우 감사원에서 2015. 8. 24.부터 같은 해 10. 14.사이에 ⊗⊗ 등 18개 외국의 주요 웹사이트에 접속하여 회원가입 등을 할 때에 본인확인을 요구하는지 여부에 대해 직접 확인한 결과, [표 52]와 같이 회원가입 단계 등에서 개인정보를 수집하거나 본인 확인을 하는 절차는 없었다.

[표 52] 외국 주요 웹사이트의 본인확인 절차 운영 실태

구분	웹사이트명	운영 국가	본인확인 여부			
			회원가입 단계	게시판 이용	아이디/비밀번호 조회	주요 기능 이용
구매 웹사이트	-	미국	×	-주)	×	-
	-	일본	×	-	×	-
	-	스웨덴	×	-	×	-
	-	중국	×	-	×	-
포털	-	미국	×	×	×	-
	-	미국	×	×	×	-
	-	일본	×	-	×	-
	-	중국	×(메일 인증)	×	×	×
공공기관	-	미국	×	×	×	×
	-	독일	×	×	×	×
	-	영국	×	×	×	×
	-	일본	×	×	×	×
게임 웹사이트	-	미국	×	-	×	-
	-	일본	×	-	×	-
	-	미국	×	-	-	-
	-	미국	×	-	-	-
문화 웹사이트	-	미국	×	×	×	×
	-	미국	×	-	×	-

주: '-'의 경우 웹 게시판에 해당 메뉴가 없어 확인 불가

또한 국내의 경우에도 감사원 감사기간(2015. 8. 24.~10. 14.) 중 개인정보 수집이나 본인확인 절차 없이 인터넷 상에서 티켓구매가 가능한 ㅏㅏ과 ⓜⓜ에 대하여 웹사이트 운영상의 어려움이 있는지를 문의한 결과 "고령자나 인터넷 미숙자들을 위해 아무런 정보를 제공받지 않았고, 사업 수행에는 전혀 지장이 없다"고 확인해 주었다.

한편, 2014년도 한 해 동안의 국내 온라인 쇼핑 거래액은 45조 2,440억 원으로 전년도(38조 4,980억 원)에 비해 17.5% 증가하였으며, 온라인 쇼핑 거래액 중 모바일 쇼핑 거래액은 14조 8,090억 원으로 전년대비 125.8% 증가하는 등 [표 53]과 [그림 6]과 같이 매년 10%대 이상 성장하는 등 인터넷을 활용한 산업이

새로운 형태의 시장으로 자리 잡고 있어 온라인 쇼핑 시 본인확인 절차로 인해 이용자에게 불편을 초래하거나 이용자의 접근에 장애가 되는 일이 없도록 하는 것이 중요하다.

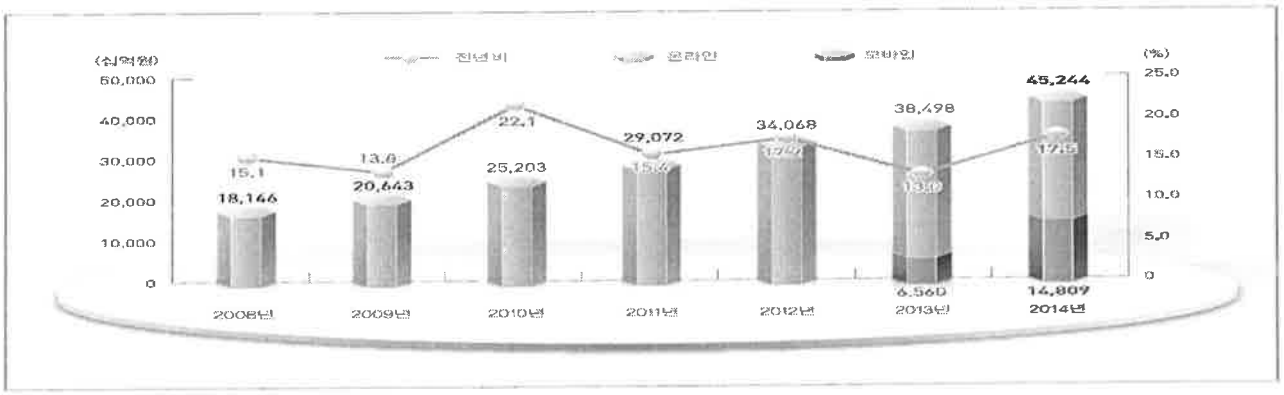
[표 53] 국내 온라인 쇼핑 거래액 동향

(단위: 십억 원, %)

구분	2008년	2009년	2010년	2011년	2012년	2013년	2014년
◦ 총거래액	18,146	20,643	25,203	29,072	34,068	38,498	45,244
모바일 거래액	-	-	-	-	-	6,560	14,809
- 전년대비 증가율	15.1	13.8	22.1	15.4	17.2	13.0	17.5

자료: 통계청 보도자료 재구성

[그림 6] 온라인쇼핑 거래규모 추이



자료: 통계청 보도자료 재구성

그러나 [표 54]와 같이 2014년 국내에서 외국 인터넷 쇼핑몰을 이용한 것은 15,530천 건, 1,544,915천 달러인 데 비하여 국외에서 국내 인터넷 쇼핑몰을 이용한 것은 106천 건에 36,824천 달러로 건수로는 146.5배 차이가 발생하고 금액으로는 41.9배 차이가 발생하였다.

[표 54] 우리나라 전자상거래 수출입 현황

(단위: 천 건, 천 달러)

구분	2010년		2011년		2012년		2013년		2014년	
	건수	금액	건수	금액	건수	금액	건수	금액	건수	금액
수입 (직접구매)	3,579	274,231	5,602	472,277	7,944	707,206	11,159	1,040,038	15,530	1,544,915
수출 (역직접구매)	7	2,105	20	4,420	36	10,638	69	23,960	106	36,824
차이	3,572	272,126	5,582	467,857	7,908	696,568	11,090	1,016,078	15,424	1,508,091

자료: 관세청 제출자료 재구성

또한 2015. 1. 9. 한국무역투자진흥공사에서 발표한 '주요국 온라인 해외직접구매 시장 동향'에 따르면 우리나라 해외 직접구매와 역직접구매 간 무역격차는 2011년 5,150억 원, 2012년 7,705억 원, 2013년 1조 1,244억 원, 2014년 10월 기준 1조 3,342억 원으로 매년 벌어지고 있다. 이와 같은 현상은 국내 인터넷 쇼핑몰에서의 과도한 본인확인 요구가 하나의 원인으로 작용한 것으로 판단된다.

이와 관련하여 박근혜 대통령도 제1차 및 제2차 규제개혁장관회의[52]에서 "우리나라에서만 요구하고 있는 공인인증서가 국내 쇼핑몰의 해외진출에 걸림돌이 되고 있다"고, "전자상거래 부문과 관련해서 확실하게 모든 규제를 풀고, 국제기준에 맞게 할 것"이라고 말씀하였다.

따라서 외국인의 경우 공인인증서 등 국내용 본인확인 수단을 갖고 있지 않아 국내 인터넷 쇼핑몰 이용 시 본인확인을 할 수 없는 등 본인확인제도가 전자상거래의 활성화에 저해요인으로 작용하고 있고, 내국인의 경우에도 사업수행을 위하여 반드시 본인확인이 필요하지 않으므로, 방통위에서는 인터넷 사용자의 편의성 및 접근성을 제한하지 않도록 인터넷상에서 본인확인은 필요최소한의 경우(개인정보가 반드시 있어야만 정상적 서비스를 제공할 수 있는 경우)에만 요구하도록 하기 위한 실효성 있는 방안을 마련하는 것이 바람직하다.

이와 관련하여 방통위, 미래부 등에서는 2014. 9. 22. 구성한 '범정부 전자상거래 규제개선 태스크포스'에서 인터넷 쇼핑몰 회원가입 시 본인확인 절차 폐지를 주요 과제로 설정하여 ♧♧(◓◓에서 운영)은 2015. 4. 21., ◒◒은 같은 해 7. 30. 회원가입 시 본인확인 절차를 폐지하는 등 [표 55]와 같이 2015년 7월 현재 주요 쇼핑몰 20개 업체 중 15개 업체가 본인확인 절차를 폐지하였다.

52) 제1차 규제개혁장관회의는 2014. 3. 20. 개최, 제2차 규제개혁장관회의는 2014. 9. 3. 개최

[표 69] 주요 20개 쇼핑몰 본인확인 절차 폐지 현황

번호	쇼핑몰	인증 여부	번호	쇼핑몰	인증 여부	번호	쇼핑몰	인증 여부	번호	쇼핑몰	인증 여부
1	-	X	6	-	X	11	-	O	16	-	O
2	-	X	7	-	X	12	-	X	17	-	O
3	-	X	8	-	X	13	-	X	18	-	X
4	-	X	9	-	X	14	-	X	19	-	O
5	-	X	10	-	X	15	-	X	20	-	O

자료: 미래창조과학부 제출자료 재구성

그러나 이와 같은 노력이후 방통위에서 온라인 쇼핑몰 등으로 하여금 필요 최소한의 경우에만 본인확인을 요구하도록 유도하기 위한 실효성 있는 대책을 마련하지 않고 있어 다수의 온라인 쇼핑몰에서 본인확인이 불필요한데도 여전히 본인확인을 요구하고 있는 실정이다.

이에 대하여 구체적으로 살펴보면 다음과 같다.

공정거래위원회에서 국고보조금 사업으로 2014. 9. 25.부터 같은 해 10. 24.까지 온라인 쇼핑몰 이용 시 본인확인 실태를 조사한 결과에 따르면 [별표 8] "온라인 쇼핑몰 이용 시 본인확인 실태조사 결과" 및 [표 56]과 같이 조사대상 100개 업체 중 2개 업체만 개인정보 수집이나 본인확인 절차 없이 구매가 가능한 것으로 나타났다.

[표 56] 국내에 개설된 온라인 쇼핑몰 이용 시 본인확인 실태조사 결과

(단위: 개)

구분 (업체 수)	회원, 비회원 요구 없음	회원가입 요구 (업체 수: 98)			비회원 구매 가능 (업체 수: 63)		필수 수집 정보							
		회원 가입	본인확인		본인확인		아이디	비밀 번호	이름	성별	생년 월일	이메일	휴대폰	주소
			여	부	여	부								
국내 웹사이트 (82)	2	80	66 (불분명 5 제외)	9	22	23	66	71	70	30	38	72	64	49
외국계 웹사이트(18)	-	18	8	10	1	17	11	17	14	2	7	14	8	5
계(100)	2	98	74	19	23	40	77	88	84	32	45	86	72	54

자료: 공정거래위원회 국고보조금 사업 결과 재구성

그리고 나머지 98개 업체 중 회원가입 시 본인확인을 요구한 업체가 74개[53] 이었고, 비회원으로도 구매 가능한 것으로 확인된 63개 업체도 그중 23개 업체가 본인확인을 해야만 회원가입이나 구매가 가능하게 운영하는 것으로 조사되었으며, 18개 외국계 웹사이트 중 8개 업체(44.4%)에서 회원가입 시 본국 웹사이트에서는 본인확인을 하지 않는 것과 달리 국내에서 웹사이트를 운영할 때는 본인확인을 하고 있는 것으로 나타났다.

그리고 감사원에서 위 조사를 실시한 날로부터 약 1년 후인 2015년 10월에 회원가입 시 본인확인을 요구한 위 74개 업체에 대하여 본인확인 실태를 점검하였다.

그런데 [별표 8] "온라인 쇼핑몰 이용 시 본인확인 실태조사 결과"와 같이 위 74개 업체 중 55개(74.3%) 업체가 여전히 회원가입시 본인확인을 요구하였고 나머지 19개(25.7%) 업체는 회원가입 시 본인확인을 요구하지 않았다.

한편 감사원에서 2015. 10. 8.부터 같은 해 12. 17.까지 ㅇㅇ대학교 산학협력단에 '인터넷 본인확인 및 아이핀 제도 관련 진단과 개선방안'에 대한 연구를 의뢰한 결과 강제적 본인확인제[54] 및 수많은 자발적 본인확인 관행이 발생하고 있어 인터넷을 통한 소통을 제약하므로 서비스의 내용과 관계없이 요구되는 강제적 본인확인제를 최대한 폐지해야 할 필요가 있는 것으로 나타났다.

그 결과 본인확인 수단이 없는 외국인이나 번잡한 본인 확인절차를 요구하는 국내 웹사이트에 접속하기를 꺼려하는 내국인 사용자의 경우 국내 온라인 쇼핑몰

53) 감사기간 중인 2015. 10. 5. 본인확인 여부를 다시 확인한 결과 74개 업체 중 55개 업체가 회원가입 시 본인확인을 요구하였고, 나머지 19개 업체는 회원가입 시 본인확인을 요구하지 않는 것으로 개선하였음

54) 정보통신망법 제44조의5에 따른 공공기관 게시판실명제, 「청소년보호법」 제16조에 따른 청소년유해물 실명제, 「게임산업진흥에 관한 법률」 제12조의3에 따른 인터넷 게임 실명제 등

에서 상품을 구매하기가 곤란해지는 등 국내 인터넷 웹사이트에 대한 접근성 및 편의성이 저하되고, 인터넷 웹사이트에서 본인 확인을 통해 개인정보를 수집할 경우 [표 57]과 같이 해킹 등에 의해 개인정보가 대규모로 유출될 우려도 있다.

[표 57] 본인확인을 요구하는 웹사이트의 개인정보 유출 사고 사례

(단위: 만 명)

사고 일자	유출 사고 업체명	유출규모(주민등록번호 포함)
2011년 11월	◆◆	1,322
2012년 7월	(주)●●	873
2013년 12월	(주)◓◓은행	101
2014년 1월	□□카드(주), (주)■■카드, ○○은행(주) 등 3개 카드사	8,358
2014년 3월	(주)●●	1,170
2014년 4월	(주)△△	277
2014년 6월	(주)▽▽	171
2014년 7월	(주)●●	104
2014년 7월	⊗⊗(주)	123
계		12,499

자료: 행정자치부 및 방송통신위원회, 한국인터넷진흥원 제출자료 재구성

관계기관 의견 방송통신위원회에서는 감사결과에 별다른 이의를 제기하지 않으면서 회원가입 시 본인확인 절차로 인해 외국인을 포함한 해외거주 이용자 등이 국내 웹사이트를 이용할 수 없어 산업활성화 저해요소로 지적받고 있기 때문에 본인확인을 강제하지 못하도록 유도하고 있으며, 산업활성화 차원에서 본인확인을 제한하는 법령의 신설을 검토할 필요가 있다는 의견을 제시하였다.

조치할 사항 **방송통신위원회 위원장**은 인터넷상에서의 서비스 제공을 위해 개인정보를 반드시 제공받아야 하는 경우를 제외하고는 본인확인 절차를 없애도록 하기 위한 실효성 있는 방안을 마련·시행하시기 바랍니다.**(통보)**

[별표 3]

ISMS와 PIMS 심사항목 중복 현황(2015. 9. 9.)

ISMS 심사항목			PIMS 심사항목	분류(세부항목)		
				동일	유사	고유
심사항목 (계: 146개)				42	44	60
정보보호관리과정	1.정보보호 정책수립 및 범위설정	1.1 정보보호정책의 수립	1.1 개인정보보호정책의 수립		O	
		1.2 범위설정	1.2 범위설정		O	
			1.3 개인정보 흐름 파악			O
	2.경영진의 책임 및 조직구성	2.1 경영진 참여	2.1 경영진 참여		O	
		2.2 정보보호 조직 구성 및 자원 할당	2.2 개인정보보호 조직 구성 및 자원 할당		O	
	3.위험관리	3.1 위험관리 방법 및 계획 수립	3.1 위험관리 방법 및 계획 수립		O	
		3.2 위험식별 및 평가	3.2 위험식별 및 평가		O	
		3.3 정보보호대책 선정 및 이행계획 수립	3.3 개인정보보호대책 선정 및 이행계획 수립		O	
	4.정보보호 대책구현	4.1 정보보호대책의 효과적 구현	4.1 개인정보보호대책의 효과적 구현		O	
		4.2 내부 공유 및 교육	4.2 내부 공유 및 교육		O	
	5.사후관리	5.1 법적요구사항 준수검토	5.1 법적요구사항 준수검토		O	
		5.2 정보보호 관리체계 운영 현황 관리	5.2 개인정보보호 관리체계 운영 현황 관리		O	
		5.3 내부감사	5.3 내부감사		O	
정보보호대책	1.정보보호 정책	1.1.1 정책의 승인	1.1.1 정책의 승인	O		
		1.1.2 정책의 공표	1.1.2 정책의 공표	O		
		1.2.1 상위 정책과의 연계성	1.2.1 상위 정책과의 연계성	O		
		1.2.2 정책시행 문서수립	1.2.2 정책시행 문서수립	O		
		1.3.1 정책의 검토	1.3.1 정책검토	O		
		1.3.2 정책 문서 관리	1.3.2 정책 문서 관리	O		
	2.정보보호 조직	2.1.1 정보보호 최고책임자 지정	2.1.1 개인정보보호관리책임자(CPO) 지정		O	
		2.1.2 실무조직 구성	2.1.2 실무조직 구성		O	
			2.1.3 부서별 개인 정보취급 책임자 및 담당자 지정			O
		2.1.3 정보보호위원회	2.1.4 개인정보보호 의사결정 기구 구성 및 운영		O	
		2.2.1 역할 및 책임	2.2.1 역할 및 책임		O	
			2.2.2 보고 및 의사소통 체계		O	
	3.외부자 보안	3.1.1 외부자 계약 시 보안요구 사항				O
		3.2.1 외부자 보안 이행관리				O
		3.2.2 외부자 계약 만료 시 보안				O
	4.정보자산 분류	4.1.1 정보자산 식별	3.1.1 개인정보 식별 및 관리 자산별 책임 할당		O	
		4.1.2 정보자산별 책임할당			O	
		4.2.1 보안등급과 취급	3.2.1 개인정보 및 자산별 보안등급과 취급		O	
	5.정보보호 교육	5.1.1 교육계획	4.1.1 교육계획		O	
		5.1.2 교육대상	4.1.2 교육대상		O	
		5.1.3 교육내용 및 방법	4.1.3 교육내용 및 방법		O	
		5.2.1 교육 시행 및 평가	4.2.1 교육 시행 및 평가		O	
	6.인적보안	6.1.1 주요 직무자 지정 및 감독	5.1.1 개인정보취급자 지정 및 감독		O	
		6.1.2 직무 분리	7.3.2 직무 분리		O	
		6.1.3 비밀유지서약서				O
			5.1.2 개인정보보호 서약			O
		6.2.1 퇴직 및 직무변경 관리	5.1.3 퇴직 및 직무변경 관리		O	
		6.2.2 상벌규정	5.1.4 상벌규정		O	
	7.물리적 보안	7.1.1 보호구역 지정	8.1.1 보호구역 지정	O		
		7.1.2 보호설비	8.1.2 보호설비	O		
		7.1.3 보호구역 내 작업	8.1.3 보호구역 내 작업	O		
		7.1.4 출입통제	8.1.4 출입통제	O		
		7.1.5 모바일기기 반출입	8.1.5 모바일 기기 반출입	O		
		7.2.1케이블보안				O

ISMS 심사항목			PIMS 심사항목	분류(세부항목)		
				동일	유사	고유
		7.2.2 시스템배치및관리				O
		7.3.1 개인업무 환경보안	8.2.1 개인업무 환경 보안	O		
		7.3.2 공용업무 환경보안	8.2.2 고용업무 환경 보안	O		
			8.3.1 영상정보처리기기 이용제한, 안내판 설치, 관리			O
	8.시스템 개발보안	8.1.1 보안 요구사항 정의	7.5.1 분석 및 설계 보안	O		
		8.1.2 인증 및 암호화 기능				O
		8.1.3 보안로그 기능				O
		8.1.4 접근권한 기능				O
		8.2.1 구현 및 시험	7.5.2 구현 및 시험	O		
		8.2.2 개발과 운영환경 분리	7.5.3 개발과 운영 환경 분리	O		
		8.2.3 운영환경 이관	7.5.4 운영 환경 이관	O		
		8.2.4 시험 데이터 보안	7.5.5 시험 데이터 보안	O		
		8.2.5 소스 프로그램 보안	7.5.6 소스 프로그램 보안	O		
		8.3.1 외주개발 보안	7.5.7 외주 개발 보안	O		
	9.암호통제	9.1.1 암호정책 수립	7.2.1 암호정책 수립 및 이행	O		
		9.2.1 암호키 생성 및 이용	7.2.2 암호키 생성 및 이용	O		
	10.접근통제	10.1.1 접근통제 정책 수립	7.1.1 접근통제 정책 수립	O		
			7.1.2 개인정보취급자 등록			O
		10.2.1 사용자 등록 및 권한부여	7.1.3 개인정보취급자 권한관리		O	
		10.2.2 관리자 및 특수권한 관리	7.1.8 특수권한 관리		O	
		10.2.3 접근권한 검토	7.1.4 개인정보취급자 접근권한 검토		O	
		10.3.1 사용자 인증	7.1.5 개인정보취급자 인증 및 식별		O	
		10.3.2 사용자 식별			O	
			7.1.6 개인정보취급자 책임			O
		10.3.3 사용자 패스워드 관리	7.1.7 개인정보취급자 및 사용자 패스워드 관리		O	
		10.3.4 이용자 패스워드 관리			O	
		10.4.1 네트워크 접근	7.1.9 네트워크 접근	O		
		10.4.2 서버 접근	7.1.10 서버 접근	O		
		10.4.3 응용 프로그램 접근	7.1.11 응용프로그램 접근	O		
		10.4.4 데이터베이스 접근	7.1.12 데이터베이스 접근	O		
		10.4.5 모바일기기 접근	7.1.13 모바일 기기 접근	O		
		10.4.6 인터넷 접속	7.1.14 인터넷 접속 통제	O		
	11.운영보안	11.1.1 운영절차 수립	7.3.1 운영절차 수립	O		
		11.1.2 변경관리	7.3.3 변경관리	O		
		11.2.1 정보시스템 인수				O
		11.2.2 보안시스템 운영				O
		11.2.3 성능 및 용량관리				O
		11.2.4 장애관리				O
		11.2.5 원격운영 관리	7.3.4 원격운영 관리	O		
		11.2.6 스마트워크 보안	7.3.5 스마트워크 보안	O		
		11.2.7 무선네트워크 보안	7.3.6 무선네트워크 보안	O		
		11.2.8 공개서버 보안	7.3.7 공개서버 보안	O		
		11.2.9 백업관리	7.3.10 백업관리	O		
		11.2.10 취약점 점검	7.3.11 취약점 점검	O		
		11.3.1 전자거래 보안				O
		11.3.2 정보전송 정책 수립 및 협약 체결				O
		11.4.1 정보시스템 저장매체 관리	7.4.1 개인정보처리시스템 저장매체 관리	O		
		11.4.2 휴대용 저장매체 관리	7.4.2 휴대용 저장매체 관리	O		
		11.5.1 악성코드 통제	7.3.8 악성코드 통제	O		
		11.5.2 패치관리	7.3.9 패치관리	O		
		11.6.1 시각동기화	7.6.1 시각동기화	O		
		11.6.2 로그기록 및 보존	7.6.2 개인정보처리시스템 접속기록 저장		O	
			7.6.3 개인정보처리시스템 접속기록의 위·변조 방지			O

ISMS 심사항목			PIMS 심사항목	분류(세부항목)		
				동일	유사	고유
		11.6.3 접근 및 사용 모니터링	7.6.4 개인정보 처리활동 모니터링 및 점검		O	
		11.6.4 침해시도 모니터링				O
			7.7.1 개인정보 출력 용도의 특정 및 보호대책			O
			7.8.1 개인정보 마스킹			O
	12.침해사고 관리	12.1.1 침해사고 대응절차 수립	6.1.1 침해사고 대응절차 수립		O	
		12.1.2 침해사고 대응체계 구축	6.1.2 침해사고 대응체계 구축		O	
		12.2.1 침해사고 훈련	6.2.1 침해사고 대응훈련		O	
		12.2.2 침해사고보고	6.2.2 침해사고 보고		O	
		12.2.3 침해사고 처리 및 복구	6.2.3 침해사고 처리 및 복구		O	
		12.3.1 침해사고 분석 및 공유	6.3.1 침해사고 분석 및 정보공유		O	
		12.3.2 재발방지	6.3.2 침해사고 재발방지		O	
	13.IT재해 복구	13.1.1 IT재해복구체계 구축				O
		13.2.1 영향분석에 따른 복구대책 수립				O
		13.2.2 시험 및 유지관리				O
생명주기요구사항	1.개인정보 수집에 따른 조치		1.1.1 서비스 제공을 위해 필요한 최소한의 정보수집			O
			1.1.2 중요 개인정보 수집 제한			O
			1.1.3 간접 수집 시 조치			O
			1.1.4 주민등록번호 수집·이용 제한			O
			1.1.5 주민등록번호 대체수단			O
			1.2.1 이용자 동의			O
			1.2.2 법정대리인 동의 획득 및 고지			O
			1.2.3 동의기록 보관			O
			1.2.4 고유식별번호 별도 동의			O
			1.3.1 개인정보취급방침 마련 및 게시			O
	2.개인정보 이용 및 제공에 따른 조치		2.1.1 목적 내 개인정보 이용			O
			2.2.1 이용자의 불만 처리			O
			2.2.2 열람정정 요구권 보장 및 처리			O
			2.2.3 동의철회			O
			2.2.4 개인정보 이용내역 통지			O
			2.2.5 개인정보 누출 등 통지·신고 절차 및 방법			O
			2.2.6 개인정보 누출 등 대책 마련			O
			2.3.1 이용자 고지 및 동의			O
			2.3.2 위탁자 책임			O
			2.3.3 외부위탁 관리 감독			O
			2.3.4 외부위탁 계약 시 보안요구사항			O
			2.4.1 제3자 제공 시 동의			O
			2.4.2 제공받은 개인정보의 관리			O
			2.4.3 제3자 보안			O
			2.5.1 개인정보 이전 시 보호조치			O
			2.5.2 해외 이전 시 보호조치			O
	3.개인정보 관리 및 파기에 따른 조치		3.1.1 개인정보의 저장 및 관리			O
			3.1.2 파기규정			O
			3.1.3 파기시점			O
			3.1.4 파기방법			O
			3.1.5 목적 달성 후 보유			O
			3.1.6 휴면 이용자의 개인정보 파기			O

자료: 한국인터넷진흥원 제출자료 재구성

[별표 4]

최근 5년간 개인정보 침해사고 분석 결과

(단위: 만 건)

연번	보도 일자	사업자명	사고 경위	유출항목	건수
1	2011. 11.	-	해킹	이름, 암호화된 주민등록번호 등	1,322
2	2012. 2.	-	해킹	메일계정, 암호	18
3	2012. 5.	-	해킹	이름, 암호화되지 않은 비밀번호 등	422
4	2012. 7.	-	프로그램 오류	이름, 주소 등	3
5	2012. 7.	-	해킹	이름, 주민등록번호(법인번호) 등	873
6	2012. 9.	-	구글링	이름, 주민등록번호 등	16
7	2012. 11.	-	해킹	이름, 생년월일 등	285
8	2012. 11.	-	해킹	이름, 생년월일 등	353
9	2012. 11.	-	해킹	이름, 주소, 전화번호 등	9
10	2012. 11.	-	구글링	이름, 학번 등	2
11	2013. 2.	-	내부 유출	이름, 주소 등	198
12	2013. 5.	-	내부 유출	이름, 휴대폰번호 등	16
13	2013. 6.	-	해킹	이름, 주소 등	10
14	2013. 11.	-	해킹	이름, 주민등록번호 등	1
15	2013. 12.	-	내부 유출	이름, 휴대폰번호 등	4
16	2013. 12.	-	내부 유출	이름, 주민등록번호 등	10
17	2014. 1.	-	내부 유출	이름, 휴대폰번호 등	10,000
18	2014. 2.	-	해킹	이름, 주소 등	42
19	2014. 2.	-	해킹	이름, 주소, 전화번호 등	75.9
20	2014. 2.	-	해킹	이름, 주민등록번호, 휴대폰번호 등	190
21	2014. 2.	-	해킹	이름, 비밀번호 등	15.6
22	2014. 2.	-	내부 유출	이름, 주민등록번호 등	13
23	2014. 3.	-	해킹	이름, 생년월일, 휴대폰번호 등	113
24	2014. 3.	-	해킹	이름, 계좌번호, 주민등록번호 등	1,170
25	2014. 3.	-	관리자 실수	이름, 이메일계정 등	1.9
26	2014. 4.	-	해킹	성명, 전화번호, 이메일계정 등	미확인
27	2014. 4.	-	내부 유출	이름, 주민등록번호 등	3
28	2014. 4.	-	원인미상	이름, 주민등록번호 등	277
29	2014. 4.	-	내부 유출	이름, 주민등록번호 등	3
30	2014. 4.	-	구글링	이름, 주민등록번호 등	1
31	2014. 4.	-	원인미상	이름, 주민등록번호 등	55
32	2014. 5.	-	해킹	이름, 비밀번호 등	50
33	2014. 7.	-	해킹	이름, 생년월일, 이메일계정 등	미확인
34	2014. 7.	-	해킹	이름, 주민등록번호 등	105
35	2014. 7.	-	해킹	이름, 주민등록번호 등	22.5
36	2014. 7.	-	해킹	이름, 비밀번호 등	128
37	2014. 7.	-	해킹	이름, 주민등록번호 등	94
38	2014. 7.	-	해킹	이름, 주민등록번호 등	52
39	2014. 9.	-	해킹	이름, 생년월일, 휴대폰번호 등	11
40	2014. 10.	-	해킹	이름, 주소, 직장 등	75
41	2014. 10.	-	해킹	이름, 주민등록번호, 주소 등	21
42	2014. 10.	-	해킹	이름, 생년월일, 주소 등	11
43	2014. 12.	-	해킹	이름, 생년월일 등	13
44	2014. 12.	-	해킹	이름, 이메일계정 등	85
45	2014. 12.	-	해킹	이름, 이메일계정, 전화번호 등	1
46	2015. 1.	-	내부 유출	이름, 전화번호	23
47	2015. 2.	-	내부 유출	이름, 휴대폰번호 등	2,400
48	2015. 2.	-	해킹	이름, 비밀번호(암호화) 등	2
49	2015. 2.	-	내부 유출	이름, 휴대폰번호 등	561
50	2015. 4.	-	관리소홀	이름, 주민등록번호 등	3

자료: 한국인터넷진흥원 제출자료 재구성

[별표 5]

ISMS/PIMS 동시 인증기업의 인증범위 중복 현황

(단위: %)

구분	업체명	인증범위	인증유형	인증범위 중복률
1	-	-	P	100
		-	I	
2	-	-	P	100
		-	I	
3	-	-	P	100
		-	I	
4	-	-	P	60
		-	I	
5	-	-	P	50
		-	I	
6	-	-	P	100
		-	I	
7	-	-	P	80
		-	I	
8	-	-	P	80
		-	I	
9	-	-	P	100
		-	I	
10	-	-	P	80
		-	I	
11	-	-	P	80
		-	I	
12	-	-	P	100
		-	I	
13	-	-	P	80
		-	I	
14	-	-	P	100
		-	I	
15	-	-	P	60
		-	I	
16	-	-	P	80
		-	I	
17	-	-	P	20
		-	I	
18	-	-	P	80
		-	I	
19	-	-	P	100
		-	I	
20	-	-	P	100
		-	I	
21	-	-	P	60
		-	I	
22	-	-	P	100
		-	I	
23	-	-	P	60
		-	I	
기업수	23	중복률 평균		81.3

주: I: ISMS, P: PIMS

자료: 한국인터넷진흥원 제출자료 재구성

[별표 8]

온라인 쇼핑몰 이용 시 본인 확인 실태조사 결과

번호	분류	사이트명	홈페이지 주소	국내외	회원		비회원		본인확인			필수 수집 정보									'15. 10. 5. 기준 본인확인 여부
					회원 가입	본인 확인	비회원 구매	본인 확인	인증방식	휴대폰	아이핀	아이디	비밀 번호	이름	성별	생년 월일	이메일	휴대폰	전화	주소	
1	종합 쇼핑몰 (10)	-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀, 공인인증서	-	-	○	○	○			○		○	○	X
2		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-		○	○	○	○	○	○	○	○	서비스 종료
3		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○	○	○			○	○			X
4		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀, 안심체크	-	-	○	○	○			○	○	○	○	○
5		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○	○	○			○	○			○
6		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀, 이메일	-	-	○	○	○			○	○		○	X
7		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○		○	이메일 인증
8		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○		○	○
9		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀, 공인인증서	-	-	○	○	○	○	○	○			○	이메일 인증
10		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○	○	○				○		○	X
11	오픈 마켓 (4)	-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○	○	○	X
12		-	-	해외	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○			X
13		-	-	해외	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○			X
14		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○	○	○			○	○	○	○	○
15	백화점 (5)	-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○		○	○	○		○	이메일 인증
16		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○	○	○			○	○	○		○
17		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○	○	○			○	○	○	○	X
18		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○	○	○			○	○	○	○	○ (간편 회원가입 동시 제공)
19		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○		○	이메일 인증

번호	분류	사이트명	홈페이지 주소	국내외	회원		비회원		본인확인			필수 수집 정보									'15. 10. 5. 기준 본인확인 여부
					회원 가입	본인 확인	비회원 구매	본인 확인	인증방식	휴대폰	아이핀	아이디	비밀번호	이름	성별	생년월일	이메일	휴대폰	전화	주소	
20	대형마트 (4)	-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○		○	이메일 인증
21		-	-	국내	○	본인확인	가능	본인확인	휴대폰, 아이핀	-	-	○	○	○			○	○		○	○
22		-	-	국내	○	본인확인	가능	본인확인	휴대폰, 아이핀	-	-	○	○	○			○	○	○	○	이메일 인증
23		-	-	국내	○	본인확인	가능	본인확인	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○		○	○
24	소셜커머스 (4)	-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀	-	-		○	○	○	○	○	○			○
25		-	-	국내	○	×	불가능	×	×			○	○				○	○			X
26		-	-	국내	○	×	불가능	×	×			○	○	○		○		○			X
27		-	-	국내	○	본인확인	불가능	×	휴대폰	-		○	○	○			○				X
28	슈퍼마켓 (2)	-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○		○	○
29		-	-	국내	○	본인확인	가능	본인확인	휴대폰, 아이핀	-	-	○	○	○			○	○	○	○	○
30	의류 (8)	-	-	국내	○	본인확인	가능	×	아이핀		-	○	○	○		○	○	○	○	○	○
31		-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○	○	○	○
32		-	-	국내	○	본인확인	가능	본인확인	휴대폰, 아이핀	-	-	○	○	○			○	○		○	X
33		-	-	해외	○	본인확인	불가능	×	휴대폰, 아이핀	-	-			○			○	○		○	○
34		-	-	해외	○	본인확인	가능	×	휴대폰, 아이핀, 공인인증서	-	-	○	○	○		○	○	○	○	○	○
35		-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀, 외국인등록증	-	-	○	○	○			○	○		○	○
36		-	-	국내	○	본인확인	가능	본인확인	휴대폰, 아이핀	-	-	○	○	○			○		○	○	X
37		-	-	해외	○	×	가능	×	×			○	○			○			○	○	X
38	서점 (5)	-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○		○	이메일 인증
39		-	-	해외	○	본인확인	가능	본인확인	휴대폰, 아이핀	-	-	○	○	○		○	○	○		○	○
40		-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○			○
41		-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○		○	○

번호	분류	사이트명	홈페이지 주소	국내외	회원		비회원		본인확인			필수 수집 정보									'15. 10. 5. 기준 본인확인 여부
					회원 가입	본인 확인	비회원 구매	본인 확인	인증방식	휴대폰	아이핀	아이디	비밀번호	이름	성별	생년월일	이메일	휴대폰	전화	주소	
42		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀, SMS, 이메일	-	-	○	○	○	○	○	○		○	○	○
43	음원 (4)	-	-	국내	○	×	불가능	×	×			○	○	○			○				이메일 인증
44		-	-	국내	○	불분명	불가능	×	휴대폰, 이메일	-	-	○	○	○	○	○	○				이메일 인증
45		-	-	국내	○	×	불가능	×	×				○				○				X
46		-	-	국내	○	×	불가능	×	페이스북, 카카오톡	-	-	○	○		○	○	○				X
47	여행 (5)	-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-			○	○	○	○	○			○
48		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀	-	-	○		○			○	○			○
49		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-			○			○	○	○	○	○
50		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀, 공인인증서	-	-			○	○	○	○	○		○	○
51		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○		○	○	○		○		○	○
52	콘도 (2)	-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀, 공인인증서	-	-	○	○	○	○		○	○		○	○
53		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○		○	○
54	항공 (3)	-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○	○	○	○
55		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○	○		○		○	○	○
56		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○		○	○		○		○
57	교통 (3)	-	-	국내	×	×	가능	×	×												×
58		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-		○	○	○	○	○	○			○
59		-	-	국내	×	×	가능	×	×												×
60	영화 (4)	-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀, 공인인증서	-	-	○	○	○		○	○	○	○	○	○
61		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○	○	○	○
62		-	-	국내	○	본인 확인	가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○			○
63		-	-	국내	○	본인 확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○		○	○

번호	분류	사이트명	홈페이지 주소	국내외	회원		비회원		본인확인			필수 수집 정보									'15. 10. 5. 기준 본인확인 여부
					회원 가입	본인 확인	비회원 구매	본인 확인	인증방식	휴대폰	아이핀	아이디	비밀번호	이름	성별	생년월일	이메일	휴대폰	전화	주소	
64	온라인 게임 (4)	-	-	해외	○	본인확인	불가능	×	휴대폰, 아이핀	-	-		○				○				○
65		-	-	해외	○	본인확인	불가능	×	휴대폰, 아이핀	-	-	○	○				○	○			○
66		-	-	국내	○	×	불가능	×	이메일				○				○				×
67		-	-	국내	○	×	불가능	×	이메일				○			○	○				×
68	가전 (4)	-	-	국내	○	본인확인	가능	본인확인	휴대폰, 아이핀	-	-	○	○	○		○	○		○		○
69		-	-	해외	○	본인확인	가능	×	휴대폰, 아이핀	-	-	○	○	○		○		○		○	○
70		-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○		○	○
71		-	-	국내	○	본인확인	가능	×	휴대폰, 아이핀	-	-	○	○	○		○	○	○		○	○
72	케이블 방송 (5)	-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○			○
73		-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○	○	○		○	○
74		-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀, 공인인증서	-	-	○	○	○		○	○	○	○	○	○
75		-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀, 공인인증서	-	-	○	○	○	○	○	○	○	○	○	○
76		-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○		○	○	○	×
77	놀이 공원 (3)	-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○	○	○	○
78		-	-	국내	○	×	불가능	×	이메일			○	○	○	○	○	○	○		○	이메일 인증
79		-	-	국내	○	불분명	불가능	×	휴대폰, 아이핀	-	-	○	○				○	○			○
80	온라인 캐시 (3)	-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○		○	○	○			○
81		-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀, 이메일	-	-	○	○	○	○	○	○	○			○
82		-	-	국내	○	본인확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○			○	○			○
83	해외 쇼핑 (6)	-	-	해외	○	×	불가능	×	×				○	○			○				×
84		-	-	해외	○	×	불가능	×	×			○	○	○	○	○	○	○	○	○	×
85		-	-	해외	○	×	가능	×	×				○	○			○				×
86		-	-	해외	○	×	가능	×	×			○	○	○			○				×

번호	분류	사이트명	홈페이지 주소	국내외	회원		비회원		본인확인			필수 수집 정보									'15. 10. 5. 기준 본인확인 여부
					회원 가입	본인 확인	비회원 구매	본인 확인	인증방식	휴대폰	아이핀	아이디	비밀 번호	이름	성별	생년 월일	이메일	휴대폰	전화	주소	
87	구매 대행 (2)	-	-	해외	○	×	가능	×	×				○	○			○				×
88		-	-	해외	○	×	가능	×	×				○	○			○				×
89		-	-	국내	○	×	불가능	×	×				○	○			○				×
90		-	-	국내	○	본인 확인	가능	본인 확인	휴대폰, 아이핀		-	○	○	○			○	○	○	○	○
91	공공 사이트 (3)	-	-	국내	○	본인 확인	불가능	×	공인인증서, 공공아이핀 가입용번호, 세무서방문			○	○	○			○	○	○		○
92		-	-	국내	○	×	가능	본인 확인	공인인증서 (서비스 이용 시)			○	○	○			○	○		○	○
93		-	-	국내	○	본인 확인	불가능	×	주민등록번호 인증			○	○	○			○		○		○
94	앱마켓 (4)	-	-	국내	○	본인 확인	불가능	×	×												×
95		-	-	해외	○	×	불가능	×	×			○	○	○	○	○					×
96		-	-	국내	○	본인 확인	불가능	×	휴대폰, 아이핀	-	-	○	○	○	○	○		○			○
97		-	-	해외	○	×	불가능	×	×				○			○	○				×
98	모바일 메신저 (3)	-	-	국내	○	불분명	불가능	×	휴대폰	-								○			×
99		-	-	국내	○	불분명	불가능	×	휴대폰	-								○			×
100		-	-	국내	○	불분명	불가능	×	휴대폰	-								○			×

자료: 공정거래위원회 국고보조금 사업결과 재구성

감사결과 처분요구와 통보사항 일람표

○ 방송통신위원회

일련번호	관계기관	분야	제 목	처분요구 등 종류	문제점 및 명세서 번호
1	방송통신위원회	소관 정보보호 분야	아이핀 제도 운영·관리 부적정	통보	나-(1)-1
2	방송통신위원회	〃	인터넷상의 불필요한 본인확인 요구 개선 미흡	통보	나-(1)-4
3	〃	관리체계 분야	정보보호 및 개인정보보호 인증 제도 통합 추진 부적정	통보	가-(3)-1