개인정보보호 정상화 대책

-기본이 지켜지는 개인정보보호-

2014. 7. 31.

관계부처 합동

순 서

Ⅰ. 추진배경 ····· 1

Ⅱ. 개인정보보호 현황과 문제점 ····· 2

1. 실태점검 결과 ····· 2
2. 사고사례 분석 ····· 8
3. 종합평가 ····· 10

Ⅲ. 정상화 대책 ····· 16

□ 핵심제도 선진화 대책 ····· 17

1. 권리구제 및 책임성 강화 ····· 17
2. 주민등록번호 관리제도 개선 ····· 20

□ 유출된 개인정보 대응 대책 ····· 23

1. 유출된 개인정보 삭제·파기 ····· 23
2. 체계적인 불법정보 단속·적발 ····· 25
3. 유출정보를 활용한 금융사기 방지 ····· 26

□ 유출 예방 · 방지 및 사이버안전 대책 ····· 27

1. 현장 중심 관리체계 정비 ····· 27
2. 개인정보 유출 예방 · 방지를 위한 투자 촉진 ····· 33
3. 사이버안전 및 기술기반 강화 ····· 36

Ⅳ. 과제별 추진계획 ····· 41

참고 1. 공공기관 개인정보 보유실태 ····· 47
2. 주요사항별 실태점검 결과 총계 ····· 48
3. 주요 용어설명 ····· 49

< 수립경과 >

◇ **범정부 TF**를 중심으로 **국회, 민간전문가 의견수렴**을 거쳐 **전반적 실태점검, 제도·기술·금융 등 분야별 개선과제** 수립과정을 진행

□ 정부내 논의과정

○ **국무총리 주재 관계장관회의(1.26) :** 근본적 재발방지 **대책 수립 지시 및 기본방향** 결정

○ **국조실장 주재 범정부 TF회의 :** 실태점검계획 수립 및 중간점검, 개선대책 등 총괄·조정(2.7 구성)

- **분야별 실무TF :** 운영TF(국무2차장), 제도개선 TF(안행부 1차관), 기술TF(미래부 2차관)

< 범정부 TF 추진 경과 >

□**1차**(2.7) : 부처별 점검단 구성 및 계획 확정 등

□**2차**(2.24) : 금융관련대책 논의(금융위), 민간부문 점검계획(안행부, 방통위), 해킹 등 보안기술관련 '기술TF' 신설(팀장 : 미래부 제2차관) 등

□**3차**(3.18) : 현장조사 중간점검, 법제도·기술분야 검토방향 논의 등

* 운영TF 개최: 1차(2.14), 2차(3.5), 3차(3.13), 4차(3.21), 5차(4.7), 6차(6.26), 7차(7.28)

□ 국회 논의과정

○ **국정조사**(2.5~28)

○ **4월 국회 : 정보통신망법 개정안(미방위) 통과**(5.2)

* 의원실 주관 토론회(3.21 강은희의원, 3.27 김영주 의원), 당정협의(3.21, 4.16), 새누리당 개인정보 특위 등에서도 지속적으로 논의

□ 민간전문가 등 의견수렴

○ 교수, 변호사 등 개인정보보호 **민간전문가 간담회**

* 학계(3.7일, 5.2일, 6.18일), 법조계(3.19일), IT전문가(3.26일)

○ **업계 간담회 :** IT업계(2.28일), 이통사(3.7일), 금융권(3.28일)

Ⅰ. 추진배경

□ **개인정보보호**는 **사생활**(Privacy) **비밀 보장** 및 **행복추구**를 위해 보장되어야 하는 **헌법적 가치**

* 개인정보자기결정권은 사생활의 비밀과 자유, 인간의 존엄과 가치 및 행복추구권, 자유민주적 기본질서, 국민주권 등을 이념적 기초로 하는 기본권(헌재, 99헌마513)

○ 또한, **IT기반** 경제구조 하에서 개인정보는 **경제질서의 근간**

* 인터넷쇼핑 이용자 2,604만명, 인터넷뱅킹 이용자 1,857만명 (2013 정보화통계집)

□ 그러나, 개인정보보호법 제정('11.3월) 등 그간의 노력에도 불구하고 **개인정보 유출사고**가 지속적으로 발생

* 주요 유출사고 : KT 1,170만건('14.3월), 카드3사 8,700만건('14.1월), SK 컴즈 3,500만명('11.7월), 옥션 1,860만명('08.2월), 넥슨 1,320만명 유출('11.11월), GS칼텍스 1,150만명('08.9월) 등

○ 특히, 우리나라는 **발전된 IT 인프라**와 함께 **주민번호 중심의 개인식별체계**가 운영되고 있어 **정보유출에 따른 피해가 큰 상황**

* 개인정보 유출 피해규모는 5년간 37억불, GDP 0.4% 수준에 달하는 상황 ('12년, 인터넷진흥원)

□ 카드3사 개인정보 유출사고(1.8)를 계기로 **공공 및 민간부문 실태점검** 및 **근본적 재발방지대책 마련 추진**(1.26, 관계장관회의 총리지시)

○ **국조실장**(팀장) **및 18개 기관 차관(급)**으로 **범정부 TF**를 구성(2.7), 근본적 재발방지 대책 마련 추진

- 분야별 검토를 위해 범정부 TF 내 **기술 TF, 법·제도 TF 구성·운영**

○ 각 부처별 「**개인정보보호 실태점검단**」을 구성, 부처·산하기관 등의 개인정보보호법 준수 여부를 점검

Ⅱ. 개인정보보호 현황과 문제점

1. 실태점검 결과

(1) 공공부문

< 점검개요 >

◇ 「개인정보보호 실태점검단(단장: 각 부처 차관)」을 구성하여 **개인정보보호법** 준수 여부를 점검(2월~6월말)

○ **점검대상 :** 16개 부처* 및 청·지자체·시도교육청 등 소속·산하기관과 공사·공단을 포함한 총 **1,234개 기관**

* 기재부, 미래부, 교육부, 법무부, 안행부, 문체부, 농식품부, 산업부, 복지부, 환경부, 고용부, 여가부, 국토부, 해수부, 방통위, 금융위(14부+2위원회)

○ **점검방식 : 서면 전수조사** 후 취약한 **998개 기관 현장점검**

○ **점검항목 :** 개인정보보호법상 점검토록 된 13개 분야* 64개 항목

* 수집·이용시 동의 및 최소수집, 개인정보 제3자 제공 제한, 개인정보 파기, 동의받는 방법, 민감정보 및 고유식별정보 처리제한, 취급자 감독, 안전조치의무 등 (참고3)

□ **보유실태 :** 국가행정기관(중앙·지방·교육)이 관리하는 **개인정보 파일* 목록은 약 34만여개, 개인정보 수는 1,031억건**('13년)

* 중앙행정기관 1.7만개, 지방자치기관 16.8만개, 교육기관 15.1만개
(예시 : 주민등록정보, 공직자재산등록 정보, 보험료 납부내역, 과세내역 등)

□ 점검결과(총괄)

○ **서면조사時**에는 전체 점검항목 중 **위반항목 비율이 3% 수준**이었으나, **현장점검 결과 7% 수준**

구분	기관수	시스템*수	총점검 항목수**	개선필요 항목수	점검항목 중 위반항목 비율
서면(전수조사)	1,234개	12,175개	779,826개	25,994개	3.3%
현장(취약분야)	998개	6,410개	413,026개	30,501개	7.4%

* 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터베이스 (예 : 민원처리시스템 등)
** 총점검 항목수는 대략적으로 "시스템수×점검항목수(64)"

□ **부처별 점검결과**(현장점검 기준)

○ 부처별 점검기관 및 점검 건수는 **교육부**(40.6%), **안행부**(38.5%) 등 2개 기관이 **약 80%**를 차지

부처명	교육부	안행부	산업부	복지부	농식품부	기타 (11개 부처)	합계
기관수	398	390	55	19	12	124	998
점검항목 비중	40.6%	38.5%	3.8%	2.7%	2.2%	12.3%	100%

○ 부처별 점검항목 중 위반항목의 비율이 **전체부처 평균(7.4%) 이상**인 경우는 **7개**, 그 **이하**인 경우는 **9개** 부처로 파악

점검항목 대비 개선필요 비율	평균(7.4%) 이상	평균(7.4%) 미만
부처수(16개)	7개	9개
부처명	고용부, 교육부, 법무부, 산업부, 환경부, 여가부, 문체부	농식품부, 국토부, 해수부, 미래부, 기재부, 안행부, 금융위, 방통위, 복지부

□ **분야별 점검결과**(현장점검 기준)

○ **관리체계, 보안기술, 인프라** 전반에서 **문제점 발견**

- **정보**를 관행적으로 **과다수집**하고, **보존기간을 과도하게 장기로 설정**하거나 **파기 지연** 등 **관리감독 미흡**

- 인사이동에 따른 **시스템 접근권한 변경 미실시**, 개인정보 암호화 등 **기술적 관리체계 미비**

- 분야별로는, **업무위탁時 준수사항 위반**(15.7%), **수집·이용 동의 위반**(10.1%), **안전조치 위반**(8.1%), 파기절차 미준수(8.1%) 등 順

< 분야별 위반항목 중 상위 5개 항목(현장점검 기준) >

순위	분야	위반항목 비율
1	업무위탁에 따른 처리 제한	15.7%
2	필수사항 고지 등 개인정보의 수집·이용 동의	10.1%
3	안전조치 의무	8.1%
4	즉시파기, 복구불가능한 방법 등 개인정보 파기 절차	8.1%
5	개인정보취급자에 대한 감독	7.5%

주요 위반 유형 및 사례

□ 업무위탁

- ▸ 위탁업체가 **연이어 계약될 경우** 매년 해야 하는 위탁업체 **교육 미실시**
- ▸ **PC 유지보수 등 외부위탁 계약** 시 개인정보보호 관련 내용을 미포함
- ▸ 업무 위탁 계약시 **문서에 의한 계약 처리 미흡** 등

□ 수집・이용

- ▸ 매년 대다수의 초・중등학교에서 **관행적으로 각종 조사서식**을 이용하여 주거현황, 부모 직업 등 **개인정보를 과다 수집**
- ▸ 교육활동에 수반되는 각종 개인정보 **수집양식에 동의 절차, 필수고지 항목 누락, 제3자 제공**에 따른 별도 **동의여부 미준수** 등

□ 안전조치 의무

- ▸ **시스템 접속기록**이 대부분 **기본사항**(ID·접속시간 등)만 **관리**되고 유출 확인에 필요한 **업무수행내역**(열람·출력 등)은 **미관리**
- ▸ 인사이동 시 시스템 **접근권한을 즉시 변경하지 않고 상당기간 유지**
- ▸ **주민등록번호** 등 고유 식별정보 내부 저장시 **암호화 조치 미흡** 등

□ 개인정보 파기

- ▸ 학생・학부모로부터 수집한 개인정보 **수집동의서**(종이) 등 **파기관리 소홀**
- ▸ 분쟁 대비 등을 이유로 **보존기간을 장기**로 설정 및 관행적으로 **파기 지연** 등

□ 개인정보 취급자 감독

- ▸ 취급자·수탁자, 시스템 담당자 등에 대한 **교육 및 관리·감독이 미흡**하고 정기 또는 수시 **실태조사 및 점검 미실시** 등

□ 현장점검時 제기된 주요 애로 및 건의사항

○ 개인정보보호 담당 **인력, 예산 및 전문성** 부족

- 부처의 경우, 정보화담당관실에서 개인정보보호 업무를 겸임하고, 학교의 경우 전산담당교사 1인이 수업・학생지도 등 여러 업무를 병행
- 개인정보보호 업무를 처리할 수 있는 시스템 구축에 필요한 예산 등 지원 미흡

* PC의 업무망/인터넷 망 분리가 기본적으로 전제되어야 하나 지자체, 공공기관 등의 경우 관련예산이 거의 미반영

* SW의 경우에도 신속하게 적기에 업그레이드되어야 하나 관련 예산 확보에 애로

(2) 민간부문 실태점검 결과

< 점검개요 >

◇ 안행부, 방통위 등 소관 부처별로 점검단을 구성하여 실태점검 실시(1월~6월말)

○ **점검대상 :** 침해신고 및 언론보도 등을 토대로 **개인정보보호 취약 업체로 지목된 191개 업체 대상**

* 유통 · 서비스 · 제조업 등 **일반분야 97개 업체**(안행부)와 **ICT분야 94개 업체**(방통위)

○ **점검방식 :** 온라인 점검 및 현장점검 병행(안행부), 현장점검(방통위)

○ **점검사항 :** 개인정보보호법 및 정보통신망법상 규정 준수 여부

□ 점검결과(총괄)

○ 점검대상 191개 업체 중 **6월말 현재 점검결과가 정리된 것은 총 120개 업체이며, 이 중 116개 업체에서 198건**을 적발*

* 공공부문의 전수조사와 달리 민간부문의 경우 경미한 사항은 현장개선을 유도하고 처분대상인 위법행위를 중심으로 점검하여 적발건수 분류기준이 상이함

* SMS 대량발송업체, 포털사 등 71개 업체는 위반사항 조사 및 결과 정리중

○ 관리·유통, 보안 기술, 인프라 측면 등 **전반에 걸쳐 취약성 노출**

□ 대상별 점검결과

○ **일반분야**는 77개 **업체**에서 **117건 위반사항 적발, ICT 분야**는 **39개 업체**에서 **81건 위반사항 적발**

< 점검결과 개요 >

분야	일반								ICT						총계
	협회/단체	증권사	마트 등 생활 밀착형	전문대/사이버대	병원	게임 업체	화장품 업체	소계	통신사 영업점	온라인 쇼핑몰 게임업체	대량 SMS 발송업체	포털사	정보유출 사업자	소계	
업체수	12	7	30	16	10 (2)	6 (2)	16	97 (4)	33	6	9	4	42	94	191 (4)
적발건수	20	12	53	17	9	6	진행중	117	73	8	진행중			81	198

* ( )안은 점검시 미적발 업체 수

□ 분야별 점검결과

○ 주요 위반내용은 **안전성 확보의무** 위반(35.4%), **부당 수집·이용** 위반(17.2%), **파기의무** 위반(12.6%) 등의 順

위반분야	안전성 확보	개인정보 수집이용	파기	개인정보 처리위탁	동의받는 방법	기타	계
일반(건)	42	16	4	19	13	23	117
ICT(건)	28	18	21	-	2	12	81
계(건)	70	34	25	19	15	35	198
비중(%)	35.4	17.2	12.6	9.6	7.6	17.6	100.0

부문별 주요 위반사례

□ 일반분야

▸ **(협회/단체)** 개인정보 수집 동의, 정보처리 위탁과 접근통제 및 권한관리, 암호화 조치 등 **안전성확보 조치**가 미흡하고, 특히 일부는 **개인정보를 동의 없이 수집·제공한 사실이 확인**

▸ **(증권사)** 개인정보 수집·제공 동의시 **필수 고지사항 누락, 고유식별정보 수집**과 **상품판매 권유에 대한 동의 획득**시 **구분 동의가 미흡**하며, **안전성확보 조치 관련 사항도 미흡**

▸ **(생활밀착형 업체) 중·소규모 기업**이 많고, **관련법 이해도**가 **낮아 현장적용 미흡**

▸ **(전문대/사이버대/대형병원/게임업체)** 개인정보 **처리 위탁 시 준수사항과 안전성 확보 조치**에 대한 사항이 미흡

□ ICT 분야

▸ **(통신사 영업점) 보호조치 위반, 주민번호 이용금지 위반, 목적 달성이 된 개인정보 미파기** 등

▸ **(온라인쇼핑몰·게임)** 개인정보 취급자 관리·감독 미흡, 안전조치의무 소홀, 홍보·판매권유 정보구분 동의 미실시 등

(3) 점검결과 조치

□ 노출된 개인정보 삭제, 임시파일 파기, 현장 시정교육 실시 등 **인력·예산투입 없이 개선 가능한 사항은 즉시 조치 완료**

○ 과태료 등 제재사항은 조사 완료 후 위원회 의결 등 관련 절차에 따라 진행

○ **법령 개정 및 인력·예산 조치가 선행**되어야 하는 **중장기 과제는 금번 대책에 포함시켜 추진**

* 접속기록 관리 시스템 확충, 암호화 시스템 마련 등

현장점검 결과 즉시조치 및 중장기 개선사항(예시)

기간별	주요 개선사항
즉시 시정	o 홈페이지, 수기대장 등의 불필요한 개인정보 삭제 및 파기
	o 직원, 수탁자, 취급자 등 개인정보 관련 담당자 교육 실시
	o 관리자, 담당자 접근권한 현행화 또는 보안서약서 징구
	o 개인정보 수집 및 제3자 제공시 동의절차, 항목 개선 등
중장기 개선	o 개인정보 보관 및 관리를 위한 계획·매뉴얼 등 기준 마련
	o 파일별 수집항목, 보유기간 재검토 등
	o 주민번호 수집 근거 마련 또는 대체 수단 도입
	o 개인정보 암호화 조치
	o 시스템 접근권한 개선, 접근기록 보관, 접속기록 보존 연장 등
	o 보안 솔루션/SW 도입
	o 개인정보 통합관리시스템 구축

2. 사고사례 분석

(1) 주요 사고사례

□ 최근 대규모 유출사고가 지속적으로 반복
(같은 회사에서 반복 유출된 경우도 존재)

○ **해킹, 내부유출, 위탁업체 관리 소홀** 등이 주요 원인

○ **유출정보는 대부분 주민등록번호**를 포함하고 있으며, 최근 **신용정보 유출도 증가** 추세

○ 사고발생 이후 유출기업에 대한 **제재조치 및 피해자 권리구제** 등은 **피해규모에 비해 미흡**

< 주요 사고 사례 원인 및 피해규모 >

시기	발생기업	발생원인	피해규모	유출정보	제재조치 등
'08. 2	옥션	해킹	1,860만명	주민번호, 이메일 등	-
'08. 4	하나로텔레콤	불법제공	600만명	주민번호, 전화번호 등	40일 영업정지, 과징금 1억5천만 등
'10. 3	신세계몰 등 25개 업체	해킹	2,000만명	주민번호, ID, 비밀번호 등	업체별 유출수준에 따라 과태료부과
'11. 7	SK컴즈	해킹	3,500만명	암호화된 주민번호와 비밀번호 등	-
'11. 8	삼성카드	내부 유출	80만명	주민번호 앞자리 2개 등	기관주의 및 유출직원 면직
'12. 7	KT	해킹	870만건	주민번호, 휴대폰 번호, 요금제 등	과징금 7억5천만, 시정조치 명령
'14. 1	카드3사 (KB·롯데·NH카드)	위탁업체 유출	8,700만건	주민번호, 신용카드 번호, 결제계좌 등	3개월 영업정지 및 각 사에 과태료 600만원부과
'14. 3	KT	해킹	1,170만건	주민번호, 유심카드 번호 등	과징금 7천만, 과태료 1천5백만, 시정명령

* 이 외에도 신용카드 결제 단말기(POS) 소프트웨어 개발관리업체가 카드 결제정보 등을 보관하는 Server를 부실 관리하여 개인정보 해외유출 (14.3) 및 커피판매점 등의 POS단말기에서 신용카드 및 포인트 카드 비밀정보가 유출되어 카드 위조 및 현금인출 사고 발생 (14.4월) 등

(2) 주요 범죄유형 (개인정보범죄 정부합동수사단)

□ (정보수집 · 공급 측면) 거래시 **개인정보를 동의 없이 수집하여 보관·이용**하거나 제3자 **불법제공, 해킹 등 발생**

○ 결제승인 대행업체(VAN社) 및 신용카드 결제 단말기(POS) **소프트웨어 개발업체**가 **카드정보 등을 보관·이용**하다 **해킹 등을 통해 정보 유출**

○ **통신사 대리점, 휴대폰 판매점** 등에서 회원정보의 불법 보관·이용

○ 인터넷 블로그를 통해 **유출된 개인정보를 판매**하거나 해커와 연계하여 특정 개인정보를 해킹하여 제공

□ (정보 활용 · 수요 측면) 이미 유출된 개인정보를 **유통 시장**을 통해 **불법적으로 판매**하여 수익을 얻거나, **영업 · 사기** 등에 활용

○ 대출권유인 · 보험설계사 등이 **휴대폰 문자메시지(SMS) 및 텔레마케팅** 등 **비대면 방식 영업**을 위해 **임의로 개인정보 유출**

○ 유출정보를 활용하여 **보이스피싱, 스미싱**에 활용

○ **불법도박 사이트**의 회원유치를 위해 경쟁 사이트의 회원정보를 해킹하여 대량문자발송 등 영업

○ 도용된 ID를 활용하여 **불법 게임아이템을 대량생산**하여 아이템 거래시장에서 현금 환전 후 **인터넷 전자상품권으로 현금화**

□ (관리측면) **보안프로그램 해지·미설치** 등으로 접근권한 제한 조치를 위반하거나 **암호화 조치**를 미적용

3. 종합평가

※ 앞서 분석한 실태점검과 사고사례 등을 바탕으로 권리구제와 주민등록번호 등 핵심제도와 개인정보 **불법유통·유출방지시스템의 문제점을 종합평가**

(1) 개인정보보호 핵심 제도 측면

권리구제 및 책임성 확보 관련제도

□ 현행법*은 손해배상시 **피해자는 피해 및 피해액을 입증**하고, **유출기관은 고의·과실여부를 입증**토록 규정

* 개인정보보호법 제39조, 정보통신망법 제32조 및 신용정보법 제43조

○ 그러나, 피해자가 **피해액을 입증하기 쉽지 않고** 소송 절차가 번거로워 **배상액도 낮은 실정** → 피해구제의 **실효성이 낮고 기업이 경각심**을 갖기에는 **미흡**

< 개인정보 피해구제 국내사례 >

	ㅇㅇ은행	ㅇㅇ전자
피해유형	이메일, 주민번호 유출	사진, 성명, 주민번호, 주소, 병역 사항, 대학교 성적, 가족관계 등
재판기간	06.3~07.11월 (589일)	06.10~08.11월 (772일)
참가자/ 피해자	414명 / 3만 2천여명	259명 / 3천여명
배상금액	1인당 20만원 (총 8,280만원 : 20만원×414명)	1인당 30만원 (총 7,770만원, 30만원×259명)

해외 피해구제 사례(미국)

ㅇ 공정신용평가법(Fair Credit Reporting Act)에 의한 징벌적 손해배상 인정('14.1월)
: 오레곤 주 연방지방법원은 Equifax社 사건에서 실제 피해액이 18만 달러 상당이었으나, 징벌적 손해배상액을 160만 달러로 결정

ㅇ 비디오 프라이버시 보호법(Video Privacy Protection Act)상 법정 손해배상제도
: 비디오테입서비스 제공자가 고의로 개인정보를 타인에게 공개한 경우, 실손해와 함께 2,500달러를 넘지 않는 정액손해배상을 규정

□ 최고경영자 등 **임원의 개인정보보호에 대한 책임이 미흡**하고, 일부 실무자만 책임을 지는 경향

주민등록번호 관리제도

□ 모든 국민에게 **의무적으로 고유번호(13자리)가 부여**되고 한번 부여되면 **변경이 제한**되며, 공공·민간에서 **광범위하게 사용**

□ **온라인 상**에서는 **'12.8월**부터 **법령상 근거없는 주민번호 수집이 금지**(정보통신망법), **'14.8.7일부터는 오프라인으로 전면 확대**(개인정보보호법)

* 위반시 3,000만원 이하의 과태료 부과

○ 이러한 규제에도 불구하고 **실제로는 과도하게 수집**되는 경향

* 공공기관의 88.1%, 민간사업자의 61.5%가 주민번호를 수집하고 있으며, 정보주체의 75%는 과도한 수집이라고 응답(2013 개인정보보호 실태조사)

○ 주민번호 **수집이 허용되는 법령**도 **866개 수준**('14.1월 기준)으로 **지나치게 광범위**

□ 주민번호는 **여타 개인정보**(주소, 전화번호 등)**를 연결하는 핵심키** 역할을 하기 때문에 **유출시 명의도용 등 피해우려**가 큰 상황

* 개인정보 침해 관련 전체 민원(166,801건) 중 83.8%(139,724건)가 주민등록번호와 관련(인터넷진흥원, '12년)

< 주민등록번호 관련 국가별 비교 >

미국	사회보장서비스를 위한 **사회보장번호(SSN)**가 공공부문 뿐만 아니라 일부 민간부문(의료·교육·금융 등)에서도 활용
영국	**국가보험번호**와 **국민건강서비스번호**가 공공부문에서 사용
유럽	**기관별 개인식별번호**(독일), **비강제적 국가주민등록제도**(프랑스)
일본	주거등록제도 상 **주민표코드**가 공공기관 업무에 한정하여 활용

◇ 정보유출 피해특성을 감안한 **효과적인 권리구제수단 도입** 필요

◇ 국민적 불안감이 큰 대규모 **주민등록번호 유출**사고가 반복되면서 **근본적인 제도 개선방안**이 필요한 상황

(2) 유출정보 불법유통 측면

□ (국내) **대출·통신·텔레마케팅** 등 중심으로 금전적 이득을 위한 **개인정보 불법유통 시장**이 광범위하게 형성된 것으로 추정

○ 전화번호 정보는 건당 10원 ~ 50원, 대출기록이 포함된 개인정보는 건당 5000원 ~ 2만원에 판매('14.01.08, 서울신문)

* 개인정보 불법유통 게시물 검색건수(인터넷진흥원): '13년 18,994건, '14년 6월 20,192건

□ (해외) 국내뿐만 아니라 **해외로 유통시장이 확대**되고 있으며, 특히 중국 등 주변국을 중심으로 주민번호 해외노출이 심각

* 우리나라 주민번호 해외노출 국가순위('13년, 인터넷진흥원)
: 총 6,572건 중 중국 5,612건(85.5%), 미국 660건(10.0%), 일본 24건(0.4%)

□ (피해현황) 유출정보를 이용한 **보이스피싱, 파밍, 스미싱 등 급증**

○ 지난 3년간 **사이버 금융사기로 피해**를 입은 누적 건수는 **약 5만 4천건, 피해금액은 총 2천 4백억원 수준**(경찰청, '13.12)

* 피해건수: '11년 8,244건 → '12년 7,891건 → '13년 37,744건
피해금액: '11년 1,019억원 → '12년 601억원 → '13년 775억원

- 기존 보이스피싱 피해 외에 스미싱(Smishing) 등 신종기법을 악용한 소액결제 사기 등으로 인한 **신규 피해 증가**

* 보이스피싱 피해액(건수) : '11년 1,019억원(8,244건)→'12년 595억원(5,709건)→'13년 553억원(4,765건)
* 스미싱 피해액(건수) : '12년 6억원(2,182건)→'13년 57억원(29,575건)

◇ 불법정보 유통을 효과적으로 억제하기 위하여 **취약부문에 대한 구조적 관리 방안 마련 필요**

◇ 광범위한 불법유통시장에 대한 **체계적·지속적 단속, 신속한 정보회수 방안** 및 **금융사기피해 방지조치** 강화 등 필요

(3) 개인정보 유출 방지 측면

법률·조직·관리 체계

□ (법률체계) 일반법인 개인정보보호법과 함께, 분야별로 개별법(정보통신망법, 신용정보법 등)에 따른 별도의 규제체계 존재

* **개인정보보호법 :** 기본원칙, 정책체계, 권리구제 등을 포괄적으로 규정
신용정보법, 정보통신망법 : 금융 분야, 정보통신 분야 각각 규정

○ 법률간 적용대상이 명확하지 않아 현장에서 법적용 혼란

* 예) 꽃집에서 인터넷 주문·배달을 겸하는 경우 개인정보보호법 및 정보통신망법 모두 적용

○ 일반법인 개인정보보호법보다 개인정보보호 필요성이 높은 신용정보법·정보통신망법 등 개별법의 제재수준이 낮은 경우도 존재

< 법률간 제재수준 차이 >

위반유형	개인정보보호법	정보통신망법	신용정보법
선택정보 수집에 미동의시 서비스 제공 거부시 과태료	3천만원	3천만원	없음
개인정보 유출시 과징금 상한	5억원 (주민번호 유출시)	매출액 3%	없음
제3자 제공 미동의시 서비스 제공 거부시 과태료	3천만원	1천만원	없음

□ (관리체계) 현장에서 제대로 집행되지 않고 관리 사각지대도 발생

○ 통신사 대리점, 텔레마케팅업체, 신용카드 결제시스템 등 기존 체계에서 관리되기 힘든 구조적 취약부문 존재

○ 불필요한 정보까지 수집, 파기 없이 장기보관·이용하는 관행이 지속

* 일반적으로 약 20여개(예: 전화번호, 주소) 많은 경우 약 50여개 항목 수집

○ 정보업무 처리자, 시스템 담당자, 위탁수행자 등에 대한 **관리감독 및 교육 체계가 미비**하고 실제 실행되지 않는 경우 다수

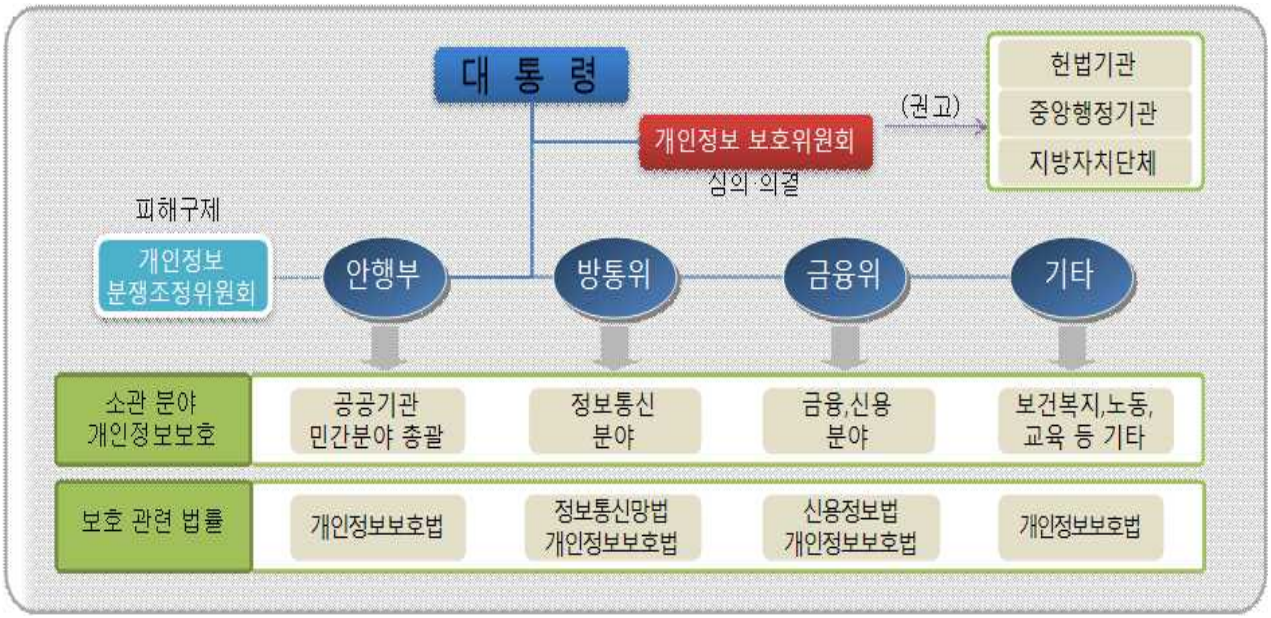
* 카드3사가 카드 부정사용 방지시스템(FDS) 개발을 코리아크레딧뷰로(KCB)에 위탁 → KCB 직원이 수탁업무 수행과정에서 입수한 정보 외부 유출 ('14.1)

○ 법 적용대상에 비해 **관련조직 및 인력규모가 취약**해 제대로 된 관리감독이 힘든 상황

* 온라인사업자, 금융기관 등 전체 개인정보처리자는 약 380만개 수준이나, 관련 감독조직은 안행부, 방통위, 금융위 등 50여명 수준에 불과

□ **(행정시스템) 개인정보보호위원회**가 주요정책을 심의·의결하고, 안행부가 정책을 총괄, **소관부처는** 금융·통신 등 **분야별로 감독**

○ 그동안 카드사 등 정보유출 사태시 **부처간 조정**이나 구조적인 **사각지대 해소** 대응 등에 있어 한계 노출



◇ 일반법-개별법 체계상 발생가능한 **법률간 정합성 문제 해소** 필요

◇ 현장에서 법 규정이 제대로 작동하도록 **실행력을 확보할 필요**

정보보호 기술 인프라

□ (인력) 기업에서 정보보호 업무는 **비선호분야로 취급**되어 **우수 인력 유치가 곤란**

* 정보보호 최고책임자 전담 비율은 12.7%, 전담조직 운영 비율은 9.8% 수준이며, 인력공급 부족은 약 1.3만명 규모(인터넷진흥원)

□ (투자) 민간기업의 경우, IT투자 중 정보보호 분야에 5% 이상 투자하는 기업의 비율은 '12년 기준 **약 3%**에 불과(미국 40%, 영국 50%)(인터넷진흥원)

○ 공공부문 **정보보호 예산**은 정보화예산의 7~8% 수준에 불과

* 미국의 경우, 정보화예산 대비 정보보호예산 비율은 9.7%(13년)

< 정보화예산 대비 정보보호 예산 추이 > (단위 : 억원)

구 분	2009	2010	2011	2012	2013
정보화 예산	31,378	32,869	32,897	33,053	32,967
정보보호 예산	1,742	2,702	2,035	2,633	2,402
정보보호 예산비율	5.6%	8.2%	6.2%	8.1%	7.3%

□ (기술) 최근 **보안사고의 상당수가 해킹에 의해 발생**

* 사이버위협 국가순위 : 1위 미국, 2위 한국, 3위 캐나다(13.8월 파이어아이사(FireEye))

○ 그러나, 단순 해킹도 막지 못하는 등 해킹에 대응할 수 있는 **기술력이 낮고**, 기술 및 보안제품 **개발 노력도 미흡**

* 선진국과 기술격차는 1.8년 수준이나, 급속도로 발전하는 해킹기술 특성상 작은 격차에도 해킹방지기술 효과는 크게 저하('13년, 인터넷진흥원)
* 국가전체 R&D 중 정보보호 분야('13년, 인터넷진흥원)
  : 미국 0.47%(7천억원), 한국 0.17%(288억원)

◇ 정보보호를 위한 **인적·물적 투자를 확대**하고, 기업 스스로 **자발적인 노력을 촉진할 수 있는 여건조성** 필요

◇ 해킹방지 기술 및 정보보호 단계별 필요기술 등 **정보보호 기술인프라가 세계적 수준으로 신속하게 발전**토록 지원 필요

Ⅲ. 정상화 대책

< 개 요 >

기본 방향

- ✓ 정보관리, 제도, 기술, 권리구제를 포괄하는 **종합적 접근**
- ✓ 국민이 체감하고 개인정보 시스템이 정상화되는 **근본대책**
- ✓ 정보보호를 위해 노력하고 책임지는 **문화와 시스템 정착**

핵심제도 선진화

① 권리구제 및 책임성 강화
- ✓ 징벌적손해배상,법정손해배상
- ✓ 관리책임성, 이용자편의 제고

② 주민등록번호 관리제도 개선
- ✓ 주민번호 변경 허용방안 마련
- ✓ 대체 및 수집 최소화

유출된 개인정보 대응

① 유출된 개인정보 삭제 · 파기
- ✓ 대청소기간 설정
- ✓ 유출정보 신속탐지•삭제
- ✓ 해외유출 정보 대응

② 체계적인 불법정보 단속 · 적발
- ✓ 집중단속 실시
- ✓ 협력체계 확충

③ 유출정보 활용한 금융사기 방지
- ✓ 사이버사기 대응체계 강화
- ✓ 본인확인 강화 등 기발표 대책 이행

유출 예방•방지 및 사이버안전

① 현장 중심 관리체계 정비
- ✓ 취약분야 구조적 관리
- ✓ 관리단계별 강화
- ✓ 법률 및 행정시스템 정비

② 유출 예방•방지를 위한 투자 촉진
- ✓ 민간·공공 투자 확충
- ✓ 기업의 기술적 자율성 제고

③ 사이버안전 및 기술기반 강화
- ✓ 보안기술 강화
- ✓ 신ICT산업 분야 정보보호 체계정비
- ✓ 전문인력양성

1 핵심제도 선진화 대책

1. 권리구제 및 책임성 강화

◇ 국민들이 **쉽게 피해구제**를 받고, **불편을 최소화**토록 개선
◇ 개인정보보호를 소홀히 하는 기관은 **책임을 분명히 지도록 제도화**

(1) 권리구제 강화

□ **징벌적 손해배상제도**를 신규 도입하고 **법정손해배상제도**를 확대 도입

* 피해자는 2가지 손해배상제도 중 적용 요건, 피해배상 가능성 등을 감안하여 선택가능

※ 기업 등이 **제도변화에 대비**할 수 있도록 **유예기간(예 : 1년) 부여**

① 징벌적 손해배상제도

○ 고의·중과실로 개인정보를 유출한 기관에 대해 **가중된 책임**을 물어 **피해액의 최대 3배까지 배상액을 중과**

○ **개인정보보호법, 정보통신망법, 신용정보법**에 도입('14년)

② 법정손해배상 제도

○ 개인정보 유출피해시 구체적 피해액 입증 없이도 법원 판결을 통해 **정해진 일정금액**(300만원 이내)**을 간편하게 보상받는 제도**

○ '14.5월 도입된 정보통신망법 상 법정손해배상제도를 **개인정보보호법, 신용정보법으로 확대 적용**('14년)

< 양 제도 비교 및 도입방안 >

구분	징벌적 손해배상제도	법정 손해배상제도
적용요건	기업의 고의·중과실로 개인정보 유출 또는 동의없이 활용하여 피해 발생	기업의 고의·과실로 개인정보가 분실·도난·유출된 경우
입증책임	기업이 고의·중과실 없음을 입증 피해액은 피해자가 입증	기업이 고의·과실 없음을 입증 피해자에 대한 피해액 입증책임 면제
구제범위	재산 및 정신적 피해 모두 포함	사실상 피해입증이 어려운 정신적 피해
배상규모	실제 피해액의 3배 이내 배상	300만원 이하의 범위에서 상당한 금액
적용시기	개정법 시행이후 유출사고	
적용법률	개인정보보호법, 정보통신망법, 신용정보법	

* 법적 안정성 차원에서 법 시행 이전 유출사고에 대해서는 양 제도 적용을 배제, 다만, 카드3사 유출사고 등 법 시행이전 피해자들에 대해서는 피해입증 자료 등을 감독기관에서 적극 지원

□ 이와 함께 **금융기관**의 경우, 거액의 손해배상 발생에 대비하여 **보험 가입 또는 준비금 적립**을 의무화 (신용정보법 개정, '14년)

* 금융기관의 경우, 손해배상이 금융기관 자체의 부담으로 끝나는 것이 아니라 공적 자금 등 국민부담으로 전가될 우려가 있으므로 일정부분 이에 대한 대비 필요

(2) 관리 책임성 확보

□ 개인정보 유출 등 범죄자에 대해 처벌 강화('14년)

유출자 처벌 강화

구분	현행	개선(안)	비고
①범죄로 취득한 수익 몰수·추징	(신설)	사안을 고려하여 형사벌에 병과	개인정보보호법
②부정한 방법으로 개인정보를 영리 등의 목적으로 타인에게 제공	징역 5년, 벌금 5천만원	징역 10년, 벌금 1억원	개인정보보호법
③악성프로그램 유포 등 침해행위	징역 5년, 벌금 5천만원	징역 7년, 벌금 7천만원	정보통신망법
	징역 5년, 벌금 5천만원	징역 7년, 벌금 7천만원	신용정보법
④정당한 권한없이 정보통신망 침입	징역 3년, 벌금 3천만원	징역 5년, 벌금 5천만원	정보통신망법 신용정보법
⑤안전성 조치 미비로 개인정보 유출	(신설)	징역 2년, 벌금 2천만원,	신용정보법

□ 개인정보 유출기관에 대해서는 과징금 기준 상향 조정('14년)

유출기관 과징금 강화

구분	현행	개선(안)	비고
안전성 조치 미비로 개인정보 유출	(신설)	매출액의 3%	신용정보법
	과징금 1억원	매출액의 3%	정보통신망법

○ 개인정보 보호책임자(CPO)를 **임원급으로 지정**하고, **최고경영자(CEO)에게 보고**토록 하여 기업 책임성 강화 (개인정보보호법 개정, '14년)

* 개인정보 보호책임자의 보고의무 위반시 제재조치(과태료 2천만원) 부과 규정 신설

- 개인정보관련 법 위반시 **CEO 등에 대한 해임 등 징계권고** 대상 확대 (개인정보보호법, 신용정보법 → 정보통신망법까지 확대)

□ 개인정보 유출시 유출기관에게 **피해자 불편과 경제적 부담을 최소화하는 규정**을 신설 (표준개인정보보호지침 등 개정, '14년)

○ 카드 재발급, 정보 수정서비스 제공 등을 **유출기관이 책임지고 이행**토록 조치

* (예시) 원칙적으로 신용정보 유출시 신용카드를 재발급하고 피해자 불편이 없는 방식으로 신용정보 수정서비스 제공, 수신자부담 전화를 통한 카드 재발급신청 등 상담 실시

(3) 이용자 편의 제고

□ 개인정보 처리에 대한 동의를 받을 경우 **동의서의 중요 내용**을 보다 **명확히 알기 쉽게 작성**토록 개선
(개인정보보호법 시행령 개정, '14년)

* 시행령 제17조: 개인정보 제공 동의서, 전화, 이메일 등 동의방법만 명시 → (변경) 필수·선택정보의 구분, 동의서를 소비자 입장에서 알기쉽게 작성할 의무 부과(글자크기, 색깔 등)

□ 알기쉬운 동의방법의 세부방안을 명시한 **'온라인 개인정보 수집·이용·제공 등 가이드라인' 마련** ('14년, 방통위)

○ "필수사항"과 "선택사항"을 **별도 페이지로 구분하고, 필수사항에 동의하면** 서비스 제공

* 선택사항에 동의하지 않는다고 서비스 제공이 거부되지 않도록 함

○ 제3자 정보제공의 경우 **포괄적 동의를 금지, 정보제공의 대상·목적별로 그룹화**하여 **각각 동의**를 받도록 개선

○ **글자 크기, 줄 간격 등을 확대**하여 **읽기 쉽게 개선**

□ 개인정보 처리방침에 **열람·처리정지·파기 등 요구권 행사방법 및 의무적 공개 항목을 구체적으로 기재**하여 공개토록 규정
(개인정보보호법 개정, '14년)

* 구체적인 개인정보 처리방침 작성방안은 안전행정부장관 고시로 제시

□ 회원탈퇴시 가입시보다 과도한 절차 요구 금지 및 **개인정보 처리정지·삭제 요구 절차를 간소화**하도록 법 개정 (개인정보보호법 개정, '14년)

* 정보통신망법에는 기반영(제30조6항)

2. 주민등록번호 관리제도 개선

◇ 과거에 유출된 주민번호를 악용한 2차 피해를 방지하고 국민 불안을 해소하기 위해 **불가피한 경우 주민번호 변경허용 방안을 마련**

◇ 일상생활에서 **주민번호 제공이 필요치 않도록** 주민번호 **수집 최소화 및 대체수단** 마련을 통해 수요 최소화

(1) 주민번호의 제한적 변경 허용 방안

□ 주민번호가 유출되어 신체·재산상 중대한 **피해를 입거나 피해를 입을 우려가 큰 경우** 등에 대해 예외적으로 **제한적 변경을 허용** (주민등록법 개정, '14년)

○ 악용될 소지가 있고 사회적 혼란이 있을 수 있으므로 **일정한 요건을 충족**할 경우에 **제한적으로 인정**

기존		개선(예시)
· 한번 부여된 주민등록번호는 **가족관계등록부 사항의 변동**이나 번호에 **오류**가 있는 경우 **정정 가능**	➡	· 아래 요건 추가 ① 개인정보 침해사고 등으로 주민번호가 유출되고 도용되거나 변조되어 **생명·신체를 해치거나 재산상 중대한 피해를 입을 것이 확실한 것**으로 인정되는 사람 ② **성폭력 피해자**로서 **주민등록번호 유출로 피해를 입을 가능성이 클 것**으로 인정되는 사람 등

* 현재는 시행령에 의해 제한적으로 인정하고 있으나, 향후 법률개정 사항으로 상향(국민 권리·의무 관련성 감안)

○ **시행시기**는 신청절차, 세부 적용기준 등 **구체적 시행 방안 준비, 주민등록법 개정** 등이 **완료된 이후** 시행

□ **주민번호 관리체계 전면 개편 문제**

○ **국민적 합의가 필요한 사항**인 만큼 공청회(9월) 등 의견수렴을 충분히 거쳐 결론 ('14년, 안행부)

(2) 대체 방안

□ 개인식별수단의 하나로서 **I-PIN**을 오프라인에서도 본인인증 수단으로 사용 가능하도록 개선 (안행부)

○ **1단계** : 현재 온라인만 적용되는 I-PIN 서비스를 오프라인으로 확대 실시('14.8월)

○ **2단계** : 민간 I-PIN 발급기관*에서는 주민번호를 보관하지 않도록 개편('15년)

* 서울신용평가정보(사이렌24), 코리아크레딧뷰로(KCB), NICE평가정보 등

□ 주민번호 外 **다양한 개인식별 수단 도입방안** 검토 ('15년, 안행부)

(3) 수집 최소화 방안

□ **주민등록번호 수집 근거 법령 정비 및 적정성 심사체계 구축**

○ **주민번호 수집을 요구**하는 업무에 대한 **전수조사**(~8월) 실시(안행부 등)

- 수집 불가피성을 전면 재검토하여 주민번호가 불필요한 경우 법령 근거 삭제 추진

※ 주민번호 수집이 불가피한 경우 소관 부처별 법령상 근거 마련 병행

- **민간분야**는 필요성이 낮은 분야를 대상으로 주민번호 수집대상에서 단계적으로 축소 (예시: 전자상거래 분야)

○ 개인정보보호위원회에 **'주민번호 근거법령 정비 소위'**를 구성하여 법령상 허용되는 주민번호 수집 적정성 사전·사후 심사('15년)

□ 주민번호 수집·관리에 대한 업종별 **매뉴얼 배포 및 캠페인**을 통해 관행과 의식 개선('14년~, 안행부)

* 인사·노무·교육·의료·금융·보건복지 등 10개 분야별 가이드라인 마련·既배포(안행부, '11.9~'13.12월)

□ **주민번호 불법 수집 신고창구** 운영(8월~, 안행부)

○ 수집이 허용되는 구체적 업무·사례를 모바일 앱 등으로 **전국민에게 공개**

(4) 안전조치 강화 방안

□ **'16년 1월 주민번호 암호화 조치 의무화에 대비**하여 차질없이 시행 준비

* 주민번호 암호화 비율은 공공부문 63.5%, 민간부문 22.7%에 불과('13년 기준)

○ 업종별 특성 등을 고려하여 **적용대상·시기 기준**을 **마련**하고, 개인정보보호법 **시행령** 및 **고시 개정 추진** ('15년, 안행부)

□ 주민번호 암호화 등 **보호조치의 실제 운영 여부를** 기업 스스로 **점검할 수 있는 도구** 개발·보급 ('15년, 방통위·안행부)

○ 영세사업자의 경우, **개인정보보호 법규 준수를 지원하는 SW와 주민번호 수집금지·파기기술을 지원**

2 유출된 개인정보 대응 대책

◇ 지난 4월부터 **'개인정보범죄 합동수사단'**을 구성하여 실시한 집중단속 결과, **115명의 정보유출 사범 적발** 및 **44명이 구속**

○ 향후에도 **정보 유출 사실이 계속 드러날** 것으로 예상

⇒ 국민 불안이 해소될 때까지 **유출된 개인정보의 단속·회수·폐기** 등을 **대폭 강화**

1. 유출된 개인정보 삭제 · 파기

□ 개인정보 **"대청소 기간"**('14.9월~12월)을 **설정**하여 검색 가능한 **불법 유통정보를 최대한 삭제**

○ 전 국민이 스스로 개인정보를 삭제·폐기하고 불법 유통되는 개인정보를 신고하는 운동 전개

▸ 추진기관 : 방통위, 개인정보보호위, 인터넷진흥원 + 안행부, 미래부, 금융위, 합동수사단(검·경), 금감원 등 공공기관 + 포털 등 민간기관
▸ 추진방식 : 인터넷진흥원의 국민신고센터(☏118, privacy.kisa.or.kr) + 금감원의 개인정보불법유통 신고센터(☏1332, fss.or.kr) 등에 신고하여 삭제하거나 자진 삭제
▸ 청소대상(예시)
□ 법령 근거 없이 수집되는 주민번호 (도서관, 쇼핑몰 등 회원 가입시 수집)
□ 방치 개인정보 (수년간 관리하지 않은 미니홈피 등에 게시된 주소·생년월일)
□. 필요한 범위를 넘어 수집된 개인정보 (입사원서에 기재하는 소득·종교·가족)
□. 불법 유통 개인정보 (해킹한 신용정보 및 환자 진료기록 등의 판매) 등

- '대청소 기간' 중 신고자* 및 자진신고자**에 대해 인센티브 부여

* 금감원 및 개인정보보호협회 포상제 활용
** 개인정보 범죄자가 자진신고하는 경우 수사과정에서 양형에 참작

□ 인터넷진흥원에서 수행하고 있는 **인터넷상 노출 개인정보**에 대한 **검색·탐지 기능 강화**

○ **중요 웹사이트의 검색 주기**를 현재 **2주→3일로 대폭 단축**('15년)

* 중요 웹사이트(약 2만개) : 노출이 빈번하거나 홈페이지 일일이용자가 1천명 이상인 웹

□ 검색된 개인정보에 대하여는 **2개월 이내 삭제**토록 조치하고, **삭제조치의 실효성을 확보하기 위한 방안** 추진('14년, 방통위)

개인정보 삭제조치 실효성 확보방안

① **법적근거 마련** : 개인정보 불법유통 게시글 차단·삭제('14년, 방통위)

○ 이용자 또는 방통위(인터넷진흥원 포함)는 이용자의 **주민등록번호**, 계좌정보 등 **금융정보**가 공개된 웹사이트에 노출된 경우

- 웹사이트 또는 검색사이트 운영자에게 **삭제 등 필요한 조치를 요청**할 수 있도록 하고, 이 경우 운영자는 필요한 조치를 하도록 **법적 근거 마련**

○ 개인정보 불법유통을 근절하기 위하여 **웹사이트 및 검색사이트에 공개된 "개인정보 불법유통 게시글"**을 **불법정보로 명시하여 차단·삭제**할 수 있는 근거 마련

* 현재 정보통신망법 제44조의7에서 불법정보의 유통금지 등을 규정하고 있으므로, 불법 개인정보를 노출시키고 있는 게시물도 불법정보에 포함토록 개정

② **인프라 확충** : 개인정보 검색·조회·삭제 시스템 확충('14년, 안행부·방통위)

○ 개인정보 유출사고 발생시 이용량 폭주 등에 대비하여 주민번호 이용내역 검색 서비스인 「**주민번호 클린센터**」 **시스템** 장비증설(H/W) 및 시스템(S/W) 개선

□ **개인정보 노출 검색대상**을 현행 웹사이트에서 페이스북, 트위터 등 **사회관계망서비스(SNS)로 확대** ('14년, 방통위)

□ **해외에 유출된 개인정보 삭제·파기** 적극 추진
('14년~, 방통위, 정부합동수사단 등)

* 해외검색프로그램의 경우 자동검색 시스템(일정주기)을 통해 각종정보(노출정보 포함)를 수집·보관하고 있어 미삭제시 노출정보를 그대로 제공

○ 해외에서 불법유통되는 개인정보를 줄이기 위해 **한-중 수사협의체 구성 등 사법공조를 강화** ('14년, 방통위, 정부합동수사단)

* 한-중 수사협의체 구성을 위한 MOU를 旣체결(4.29)

○ 해외유출 정보 처리를 위한 개인정보보호 **협력센터 확대**

* 현재 베이징에 한중인터넷협력센터 1개소 설치(인터넷진흥원)

○ 해외 포털서비스의 노출정보를 검색하는 서비스에 대해 인터넷진흥원 등 관계기관이 노출정보를 검색·삭제할 수 있도록 **해외 포털 서비스와의 협력 강화**

2. 체계적인 불법정보 단속적발

□ 개인정보 침해 및 불법유통에 대한 범정부적인 **집중단속 전개** ('14.4월~'15.4월, 정부합동수사단)

* 정부합동수사단 구성: 검·경, 미래부, 안행부, 방통위, 국세청, 금감원, 인터넷진흥원 등

< 집중단속 대상 >

- ▸ 상거래 과정에서의 **개인정보 불법수집, 기업 수집 개인정보의 외부 무단제공, 개인정보 해킹 등**
- ▸ 개인정보 **유출 원인** 및 **관리주체의 책임소재**
- ▸ 불법 개인정보를 활용한 **대출알선, 보이스피싱** 등 **신종 금융사기, 도박사이트 회원유치, 대포폰·대포통장 제작** 등

□ 불법유통 게시물 등에 대한 탐지 후 즉시 조사 및 수사할 수 있도록 **정보공유 및 협업체계 강화**('15년, 방통위, 검·경 등)

3. 유출정보를 활용한 금융사기 방지

□ 새로운 기술로 진화하고 있는 **피싱·스미싱·파밍 등** 신종사기 수법에 대한 대응능력 제고 (미래부)

○ 현재 **주요 공공기관, 은행** 등을 대상으로 실시 중인 보이스 피싱, 파밍 **차단서비스 대상기관 확대** ('15년)

* 보이스피싱 차단(326개→500개 기관), 파밍 차단서비스(91개→150개 기관)

○ 스미싱 수집 채널을 확대하고, 분석능력을 강화하여 스미싱 의심문자를 알려주는 **스미싱 확인 서비스** 실시 ('14년)

* 이용자가 의심 문자를 인터넷진흥원으로 전송(☎118)하면, 스미싱 여부 검증 후 문자로 통보

○ 스마트폰에 악성앱 감염 사실을 알려주고 치료 방법을 안내하는 **모바일 사이버 치료서비스 구축** ('14년)

○ 전화번호를 도용한 **발신번호 임의변경 문자 차단 서비스를 현재 공공기관·은행에서 개인으로 확대** ('14.7월)

* 개인이 이통사에 번호도용 문자 차단 서비스를 신청하면, 신청자가 등록한 전화번호가 스미싱 발신 번호로 사용될 경우 자동차단

□ 유출사고 발생시 **신속한 대응**을 통해 피해 발생 가능성 최소화

○ 개인정보를 취급하는 공공기관 및 일정규모 이상의 민간기관은 사고발생시 신속하게 대응조치(예:7일이내)를 할 수 있도록 **「개인정보 유출사고 대응매뉴얼」 마련을 의무화**
(표준개인정보보호지침 등 개정, '14년, 안행부, 방통·금융위)

* 통지·조회절차, 영업점·인터넷회선 확충 등 고객민원 대응 조치, 현장혼잡 최소화 조치, 고객불안 해소 조치, 피해자 구제 조치 등 포함

□ 본인확인 강화 등 **기발표 대책***(3.10)**을 차질없이 이행**(금융위)

* 사기 피해 방지를 위한 입금계좌지정 서비스, 일정금액 이상 카드 문자알림 서비스 무료화, 비인증 결제방식에 대한 이중인증 의무화 등

3 유출 예방·방지 및 사이버 안전 대책

1. 현장 중심 관리체계 정비

◇ **개인정보유출**이 반복되고 있는 취약분야는 **집중관리체계** 구축

◇ **꼭 필요한 정보만 수집**하고 **수집된 정보는 철저히 보호**토록 개인정보관리 시스템 개선

(1) 통신사 대리점 등 취약분야 구조적 관리

□ **(통신사 대리점·판매점)** 개인정보 보유를 최소화하고 정보유통 보안을 강화하는 등 통신사별 관리책임을 제고('15년, 방통위)

○ 대리점 또는 영업점이 **통신사에 의무적으로 등록**토록 하고, 미등록 및 불법행위 적발시 **퇴출수단***을 마련

* 미등록 판매점과 거래한 대리점은 투아웃제(영업정지 ⇒ 계약해지) 도입, 영업점의 개인정보 관련 불법행위시 5년간 등록금지 등

○ 통신사 **'개인정보 관리수준 평가제도'**를 도입, 개별 통신사의 개인정보보호 **관리 현황, 활동 등을 평가**한 후 **결과를 공개**

* 평가위 구성 등 추진, 평가결과는 이통사 이용자보호 업무평가에 반영 (인터넷진흥원)

○ 개인정보 무단조회 방지를 위한 **SMS 본인인증제도*** 시행

* 영업점 고객정보 조회시 통신사가 가입자에게 SMS로 인증번호를 전송하고, 영업점은 전송받은 인증번호를 가입자가 알려주어야 가입자 정보를 조회할 수 있는 서비스

○ 서비스 가입신청 시 **'전자 청약 시스템'** 적용 추진

* 서식지 형태의 가입신청을 본사와 직접 연결된 별도의 단말기를 통하여 이용자가 직접 개인정보를 입력하고 서명하는 형태로 전환 검토

□ **(신용카드 단말기(POS 등) 관리업체)** 관리·감독체계를 명확하게 정비

○ 지정된 보안규정을 준수한 단말기만을 사용토록 하고, 위반시 **가맹점을 처벌**하는 등 **관리시스템* 구축** ('14년~, 금융위)

* 그동안 소관부처가 명확하지 않아 관리 사각지대 존재
→ 금융위가 정한 보안규정을 준수하도록 규정하고, 미준수시 벌금부과(500만원)

○ **신용카드 결제망 관리회사(VAN사) 등록제** 운영, **IC 단말기 전환** 등 기발표 대책(금융위) 차질없는 이행

□ **(텔레마케팅(TM) 업체)** 개인정보를 **합법적으로 이용하는 업무 관행(Business Rule)이 정착**되도록 제도적 여건 개선

○ TM영업시 사전동의를 받지 않은 경우, 수신인에게 **개인정보 수집출처를 고지**하도록 의무화 ('14년, 방통위)

* 누구든지 광고성 정보를 전송하려면 수신자의 사전동의를 받아야 하나, 전화권유판매업은 사전동의의 예외로 인정(정통망법 제50조)

○ **TM수신거부시스템(www.donotcall.go.kr) 이용을 활성화** ('14년, 공정위)

* 방문판매법에 따라 TM업체는 월 1회이상 시스템에 접속하여 수신거부 소비자를 영업대상에서 제외하여야 하나, 이용률이 7.7%(372개/4811개)에 불과('14.4월)

○ TM에 대한 **민간의 자율적 개인정보보호 관리체계 확충**('14년, 방통위)

- 현재 인터넷사이트 대상으로 적용되는 **개인정보보호 인증 마크제***(ePRIVACY)를 **TM업체**에 확대 적용

* 개인정보보호 정책 및 관리수준을 평가하여 기준을 충족할 경우 인증마크 부여(개인정보보호협회)

- 불법 TM신고 제도(개인정보보호협회)를 **이동통신서비스에서 전 업종으로 확대**하고, 활성화 추진(포상금 10→20만원 상향 등)

○ 불법 TM의 **전화번호 이용 정지를 위해 관련 법률 개정** 추진 (전기통신사업법 등, '14년)

* 불법 대부광고에 사용된 전화번호 이용중지 요청을 규정한 대부업법 旣 개정(3.18)

□ **영세·중소기업의 정보보호 역량 강화**를 위해 **지방 권역별 정보보호 지원센터** 확충('14년~, 미래부)

* 전문가 컨설팅, 온라인 상담 등 서비스 제공('14년 2개소 / 대구, 인천)

(2) 개인정보 관리단계별 강화

□ **(수집단계) 개인정보 최소수집원칙**이 현장에서 실질적으로 **정착**될 때까지 점검·개선

○ 이번 실태점검시 파악된 **개인정보 과다수집 사례 등에 대해 일제 정비** (~'15.3월, 안행부)

* 전 공공기관 대상 개인정보 수집 자체 실태조사 실시 및 서식 개선(12월말), 안행부는 개인정보파일 보유실태 및 개선에 대한 정기 점검 실시(연1회)

○ 지속적으로 공공·민간이 스스로 **최소수집 원칙을 점검하고 정비할 수 있는 체계**를 구축

- **(공공부문)** 일정 규모 이상 개인정보 보유 공공기관은 자체계획 수립, 매년 수집·보유 필요성 및 적정성에 대한 실태조사 후 개선

- **(민간부문) 업권별 협회**에서 자율적으로 정보제공·이용동의서 **등을 정비,** 필요시 소관부처·안행부가 **합동점검**하여 시정조치

* 개인정보 보유건수 기준으로 매년(예: 1천만명 이상), 격년(5백만명 이상), 5년주기(1백만명 이상) 등 검사주기를 차등화하여 점검

□ **(관리단계)** 개인정보 출처 관리 시스템을 구축하고, 취약 분야로 지적되어온 **위·수탁관계를 명확히 정립**('14년, 안행부)

○ 개인정보 다수 처리 기관은 **제3자로부터 제공받은 개인정보에 대해 수집출처 및 목적을 관리**하도록 의무화

* 개인정보 보유건수가 일정수준(예 : 1백만건) 이상인 공공기관·기업 대상 적용 (개인정보보호법 개정)

○ 개인정보 **처리방침**에 수탁자의 담당자 연락처 등 **위탁에 관한 사항을 보다 구체적으로 작성**토록 개선 (표준 작성지침 마련)

* (예시) 위탁시 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등

○ 위·수탁자 모두에게 손해배상을 청구할 수 있도록 명시하여 **정보주체의 배상청구권 및 수탁자 책임 강화**(개인정보보호법 개정)

□ **(파기단계)** 법령상 근거에 따라 **필요최소한 기간만 보존 후 파기**토록 관련 규정 재정비('14년, 전부처)

* 업무분야에 따라 보존기간이 달라질 수 있으므로 **소관부처별로 정비** (예 : 부동산 거래 및 출생관련 의료정보는 장기간 보유 필요)

○ 개인정보 파기시, **복구 또는 재생되지 않게 조치**하도록 하는 규정 신설(신용정보법 개정, '14년)

* 개인정보보호법, 정보통신망법의 경우 관련 규정 기설치

□ **(잊혀질 권리 등)** 전문가 의견수렴 등을 통해 잊혀질 권리*, 디지털 유산** 등에 대한 법제도 구축방안 검토('15년, 방통위)

* 잊혀질 권리 : 정보주체가 포털 등 정보통신서비스 제공자에게 자신과 관련된 정보를 삭제하거나 확산을 방지토록 요청할 수 있는 권리
* 디지털 유산 : 사망시 보유하고 있던 모든 디지털 형태의 재산에 관한 권리·의무

(3) 법률 및 행정시스템 정비

□ **(법률)** 현장에서 법적용 혼란과 사각지대가 발생하지 않도록 **법률간 정합성**을 제고 (개인정보보호법·정보통신망법·신용정보법, '14년)

		정보통신망법 적용대상	신용정보법 적용대상	개인정보보호법 적용대상
현행	대상	정보통신망을 영리로 사용하는자	신용정보 이용·제공자	모든 개인정보처리자 *개별법 적용대상 제외 여부 불명확
	대상수	약 273만개 사업자 + 160만개 스마트폰앱	약 7만개 사업자	약 380만개 사업자
개선	대상	개인정보보호 조항을 전기통신사업자(KT 등)와 통신판매사업자(옥션 등)로 한정	금융기관, 신용정보회사 등으로 한정	모든 개인정보처리자 *개별법 적용사업자는 각 소관부처에 위임·위탁
	대상수	약 37만개 사업자 +160만개 스마트폰앱	약 3천5백개 사업자	약 340만개 사업자

○ **개인정보보호법을 기준**으로 제재수준 정비

○ 개인정보보호위를 통해 **상시적으로 관련 법령간 정합성을 유지**하는 체계를 구축(법령심사소위 설치 등)

제재수준 정비방안

위반유형		개인정보 보호법	정보통신망법		신용정보법	
			기존	개선안	기존	개선안
수집·이용·제공	민감정보처리 금지 위반 (징역)	5년	좌동	좌동	3년	5년
	(벌금)	5천만원	좌동	좌동	3천만원	5천만원
	해킹 등 침해행위로 인한 수집 (징역)	5년	좌동	좌동	3년	5년
	(벌금)	5천만원	좌동	좌동	3천만원	5천만원
	선택정보 수집 미동의시 서비스 제공 거부 (과태료)	3천만원	좌동	좌동	-	5천만원
	제3자 제공 미동의시 서비스 제공 거부 (과태료)	3천만원	1천만원	3천만원	-	3천만원
	수집 목적외 용도 이용 또는 제3자 제공 (징역)	5년	좌동	좌동	좌동	좌동
	(벌금)	5천만원	좌동	좌동	좌동	좌동
	(과징금)	없음	매출액 1%	매출액 3%	-	-
위탁업무	위탁업무범위 위반 (징역)	5년	-	-	-	5년
	(벌금)	5천만원	-	-	-	5천만원
	마케팅 위탁시 수탁자 미고지 (징역)	-	5년	좌동	-	-
	(벌금)	-	5천만원	좌동	-	-
	(과태료)	3천만원	-	-	-	3천만원
	위탁교육 및 중요사항 계약시 반영의무 위반 (과태료)	1천만원	-	-	-	1천만원
안전성확보	안전성 조치 미비로 유출 (징역)	2년	좌동	좌동	-	2년
	(벌금)	1천만원	좌동	2천만원	-	2천만원
	(과징금)	5억원 (주민번호 유출시)	매출액 1% 또는 1억원	매출액 3%	-	매출액 3%
	식별정보 암호화 (과태료)	3천만원	좌동	좌동	-	3천만원
	내부관리계획 미수립 (과태료)	3천만원	좌동	좌동	5백만원	3천만원
이용자권리	개인정보 열람 및 정정청구 거부 (과태료)	3천만원	좌동	좌동	1천만원	3천만원
	개인정보 제공·이용동의 철회 및 삭제요구시 삭제의무 위반 (과태료)	3천만원	좌동	좌동	1천만원	3천만원
	유출통지 및 신고 미이행 (과태료)	3천만원	좌동	좌동	-	3천만원

□ **(행정시스템)** 새로운 기구를 신설하기보다는 기존 조직체계 보강을 통해 **조정·점검 - 감독·집행 - 지원기능**을 강화

○ 개인정보보호위가 **실질적인 역할**을 할 수 있도록 강화 ('14년, 안행부)

< 개인정보보호위원회 기능강화 >

현행		개선
· 안행부가 기본계획 수립, 분쟁조정위원 임명, 사무국 운영 등 담당	➡	· 개인정보보호위가 담당
-	➡	< 개인정보보호위 권한 추가 > ① 심의·의결 안건에 대한 사실조사권 ② 정책·제도 개선권고 및 이행 점검 ③ 법령간 정합성 유지 ④ 민간부문 위법사항 조사요구권

○ 개인정보보호 관련 주요 부처의 업무량 및 수요 분석을 통해 **조직 및 전문인력 보강**('15년, 안행부)

* 중앙부처, 지자체 및 공공기관 개인정보보호 인력을 현재 대비 2배 수준 확대 검토

□ **인터넷 진흥원**을 범정부적 **개인정보 정책지원 전문기관**으로 확충 ('15년, 미래부·기재부)

○ 유사한 기능을 수행하는 여타 정책지원기관의 **개인정보보호 기능**을 **인터넷진흥원**으로 **통합 검토**

○ 실태점검·사고조사·사이버사기 대응 등 관련 기능 확대 및 인력보강

* 이번 대책으로 인터넷진흥원의 역할이 3~5배 증가 예상

○ 전 부처에 대한 정보보호서비스 지원이 될 수 있도록 이사회에 관계부처가 참여토록 개선

2. 개인정보 유출 예방·방지를 위한 투자 촉진

◇ 급변하는 기술환경 변화에 신속히 대응하기 위해서는 **스스로 정보보호에 투자하는 여건**을 조성하는 것이 중요

○ **정보보호 투자에 대한 인센티브**를 강화하고, 기술기준 등에 대한 **기업의 자율성 제고** 필요

* 규정만 지키면 정보보안사고에 대해 면책될 경우, 오히려 기술발전이나 투자동기를 저해할 우려

(1) 민간·공공 투자 확충

□ 민간분야

민간분야 인센티브 확대방안

① **중소기업**의 정보보호 시설·제품 등 **직접 투자 비용**에 대한 **조세감면 연장**('14→'17년) **및 확대**(7% → 10%)

② 중소기업의 **정보보호서비스 컨설팅 비용에 대한 조세감면(25%) 제도 홍보 강화**

* 정보보호서비스 컨설팅 비용이 연구·인력개발비 세액공제(조특법 제10조) 대상 비용 중 기술자문료(시행령 별표6)에 해당한다는 내용을 잘 모르는 기업들이 다수

③ **중소기업**의 정보보호 신규인력 채용시 **인건비 보조**(월 최대 90만원/1인)

* 고용노동부의 '고용창출지원사업'에 정보보호분야 추가

④ **'정보보호 우수기업'**으로 **선정** 시 **정부·공공조달 및 국가 연구개발 사업** 참여時 **가점**(0.5～1점) 부여

⑤ 기업이 **정보보호 관련보험* 가입** 시 보험료 할인(5～15%)을 받을 수 있도록 **관련기관 및 업계의 협력** 추진

* 개인정보보호 배상책임보험, 전자금융거래 배상책임보험, e-Biz 배상 책임보험 등

⑥ 보안투자 및 법규준수 등 보안역량 강화를 위한 기업의 준비·노력(Readiness) 정도를 평가하는 민간자율 **'정보보호 준비도 평가' 도입** 추진

□ 공공분야

공공분야 인센티브 확대방안

① **정보보호예산이 일정비율(예:10%수준)을 유지**하도록 가이드라인 제시

* 정보보호예산 편성 가이드라인(미래부, 기재부)

② 정보보호 **R&D 투자를 단계적으로 확대**(미래부, 기재부)

* '14년 ICT 기술개발예산 (7,429억원) 중 정보보호예산은 3.6% 수준

③ **각 부처 평가시 정보보호 투자를 평가에 반영 검토**('15년)

④ **공공기관 경영평가**에서 정보보호노력이 평가될 수 있도록 **기준 구체화**(기재부)

⑤ **정보보호 제값받기 문화정착**

- **정보보호 제품·서비스 비용**을 '하자 보수'를 위한 유지관리 대가가 아닌 **'서비스 대가'로 전환**(기재부, 미래부)

  * **대가 비용**(현 정보보호제품 구입비의 9%→15%, '17년)을 **확대**하고, 제품·서비스의 **활용특성에 따라 차등지급**할 수 있도록 **'서비스 대가 산정 가이드라인'** 개발·보급

- 가이드라인에 따라 **무상유지보수 기간 단축**(1년→6개월) **검토**

- **분리발주** 등이 **시행**될 수 있도록 **'정보보호 표준계약서' 마련**·보급

⑥ 정보보호가 생활화 될 수 있도록 캠페인 지원(미래부)

□ 정보보호 **산업기반 조성 추진** ('14년, 미래부)

○ **정보보호산업 진흥법** 제정 추진 ('14년)

* 주요 내용 : 정보보호 수요에 맞는 정보보호 전문인력 양성, 기술개발, 산업체 지원 강화, 정보보호 산업진흥계획 수립, 산업진흥 기반 조성, 정보보호기업 지원 등

○ ICT 융합에 대응한 융합보안시장 등 신산업을 육성하고, 글로벌 시장을 선점하기 위한 **10대 전략제품** 발굴·육성을 구체화 ('14~'18년)

* ① 해킹(APT) 공격대응 ② 사이버블랙박스 ③ 지능형 영상감시 ④ 사용자 친화형 얼굴-홍채 인식 ⑤ 유해콘텐츠 차단 ⑥ 무선침입탐지 ⑦ 스마트단말 보안칩 ⑧ 산업용 통합보안 ⑨ 차세대 암호기술 ⑩ 유니버셜 인증 등

(2) 기업의 기술적 자율성 제고

□ **지나치게 세부적으로 규정**된 개인정보보호 관련 기술적 조치 제도(고시)를 개정하여 **기업의 자율성**을 부여 ('15년, 방통위, 금융위)

○ 세부적인 조치사항까지 강제하는 방식에서 기본원칙과 필요 최소한 조치만 규정하고 **개별적 수단 선택은 재량**을 인정

* '개인정보의 기술적·관리적 보호조치 기준'(방통위), '전자금융감독규정'(금융위) 개정

관련규정 정비방향 예시
① **인증수단 등 접근통제 관련** (개인정보의 기술적 · 관리적 보호조치 기준) · '공인인증서 등 안전한 인증수단' → '안전한 인증수단'으로 개정하여 사업자의 자율적 선택권 보장하는 방안 검토 * '14.5.20부터 온라인 카드결제시 공인인증서 의무사용은 旣폐지 (전자금융감독규정 시행세칙) ② **안전성 확보를 위한 보호조치 관련** (개인정보의 기술적 · 관리적 보호조치 기준) · 사업자가 개인정보 보유규모 등을 고려하여 보호조치 내용을 결정할 수 있도록 관련 규정 수정 검토 ③ **전자금융거래 보호조치 관련** (전자금융감독규정) · 단말기 보호대책, 전자금융거래시 준수사항 등과 관련하여 특정기술을 강제하지 않도록 관련 규정을 수정하는 방안 검토

○ 장기적으로 보호조치 기준에 세부적 조치사항을 규정하지 않고, **보호목표**를 **규정**하여 **기업의 자율성**을 부여하는 체계로 전환 검토 (안행부, 미래부, 방통위, 금융위 등)

□ 정부의 **직접규제 대신 인증시험을 활용**할 수 있도록 제도 개선

○ 안행부, 미래부, 방통위 등이 각각 운영하는 **유사인증제도간 중복을 해소**하고 상호 인정범위 확대 추진 ('14.12월, 안행부, 미래부, 방통위)

3. 사이버 안전 및 기술기반 강화 (미래부)

◇ 빠르게 발전하는 해킹기술에 대응하여 **예방·탐지·분석·치료 등 단계별 보안기술을 개발·보급**

◇ **신ICT산업 분야 정보보호 대책**을 마련하고, **전문인력을 양성**

(1) 보안기술 강화

□ 암호화 기술개발

○ 개인정보 암호화로 인한 시스템 성능저하 우려를 감안, 스마트폰 등에서 **효율적으로 관리 가능한 경량 암호화 기술** 개발 ('16년)

□ 해킹탐지체계 고도화

○ **스피어 피싱 대응을** 위해 **이메일 악성코드 유포 탐지시스템 구축**('15년)

* 이메일 스팸 트랩 시스템(임의의 계정을 개설하여 해당 주소로 유입되는 모든 메일을 수집)등을 통해 수집된 이메일을 검사하여 스피어 피싱용 악성코드 추출·분석

○ 악성코드 은닉사이트 탐지 강화를 위해 **탐지대상 홈페이지 확대** (15만개→50만개)('14년)

○ 가상 ID 10만개를 통해 해커를 유인하는 **사이버트랩 시스템** 개발('15년)

* 허니팟(해커를 속이기 위해 가상 개인정보를 활용해 공격을 유도)용 개인정보를 공개하여 SNS 등으로 사이버사기 공격을 유도한 후, 수신되는 메시지를 자동 수집하여 필요시 수사기관 제공

○ 민간·공공 **주요정보통신기반시설에 대한 정기적 모의해킹·훈련 실시 근거 마련**(연1회이상) 및 이행점검 강화 (정보통신기반보호법개정, '14년)

○ 개별 침해사고 정보를 종합분석하기 위한 **사이버 위협 정보 분석·공유시스템**(C-TAS) 구축 및 운영 (‘14년)

* C-TAS(Cyber Threats Analysis System) : 사이버 위협정보를 체계적으로 수집 → 정보분석 → 공유하는 시스템

○ 비행기 블랙박스처럼 사이버 침해사고를 신속하게 분석하고 증거를 보존하는 기술인 **사이버 블랙박스 개발** (’16년)

- 개별기관에 사이버 블랙박스를 설치하여 **자체 보안관제를 강화** (‘16년)

□ 악성코드 대응 체계 강화

○ **좀비PC 방역체계 사각지대**에 있는 중소인터넷 서비스업체 및 학교·공공기관의 공용 PC 등에 대해 사이버 치료체계 적용 (‘14년)

○ **PC 자가진단** 도구인 **SW 원클릭 안심서비스*** 구축·시범운영 (‘15년)

* PC에 설치된 주요 소프트웨어의 버전을 확인할 수 있고 최신 버전으로 업데이트 하기 위한 정보 제공 서비스

○ SW 업데이트시 유포되는 악성코드를 탐지하는 체계 확대 (현재 웹하드 업체 대상 → 모든 상용 SW로 확대, ~‘17년)

□ 스마트폰 보안 강화

○ 분실시 **개인데이터 삭제기능(킬스위치)뿐만 아니라, 스미싱 차단앱** 등을 모든 스마트폰 출고시 **기본탑재 추진**

* 킬스위치 : 팬택(’13.2월), 애플(’13.9월), 삼성(’14.4월), LG(’14.5월) 적용
* 스미싱 차단앱 기본탑재, 보안설정 옵션 및 인터페이스 가이드 개발(’14.10월)

○ 폰키퍼(스마트폰 보안앱) 일일 보안공지 용량 확대 (월 20만명→100만명, ‘14.11월)

○ **악성앱 모니터링** 대상 확대 (‘15년)

* 구글, 해외 블랙마켓(5곳) → 이동통신사 등 국내 주요 앱 마켓으로 확대

□ 유출정보 탐지

○ 신종·변종 악성앱(스마트폰내 비인가된 정보 접근 등)에 대한 **정보 유출행위 탐지 기술 신규 개발**('15년~)

○ 정보보호 취약점을 분석 및 대응서비스를 제공하는 **정보공유분석 센터(ISAC)**를 **주요 산업분야**(의료, 에너지 등)**로 확대·구축** 지원 ('15년~)

* 현재 정보통신, 은행, 증권, 지자체 등 4개 분야에 ISAC 구축

(2) 신ICT산업 분야 정보보호 체계 정립

□ (인증환경 및 전자서명기술 개선) 공인인증서 이용환경 개선 및 **새로운 전자서명 신기술** 도입 추진

○ 특정기술(액티브X)에 지나치게 의존하는 환경개선을 위해 웹 표준 기반 공인인증서비스 기술개발 ('14년)

* 현재는 MS사 인터넷 익스플로어에서만 액티브X 이용 가능

○ 공인인증서 유출방지를 위하여 보안토큰 등 **안전한 저장매체 확대** 추진('14년)

* 보안토큰, USIM 등 안전한 저장매체 내 인증서의 유효기간을 현재 1년에서 3년까지 연장

○ ATM, 의료정보 시스템 등 ICT 융복합기기에 대한 **보안성 강화**를 위한 사전연구('15년)를 거쳐 인증서비스 개발·도입 ('16년)

○ 정보시스템의 설계단계에서 정보보호를 고려토록 하는 사업 모델(Business Model)을 확산('14년~)

* 사전 설계단계시 보안을 고려하도록 안내서 개발 및 홍보활동('14년), 사전 점검 및 시큐어 코딩을 위한 가이드 개발·보급 ('15년) 등도 추진

□ **(신ICT산업) 빅데이터, 클라우드, 사물인터넷 등** 신기술 분야별로 개인정보보호와 산업발전을 조화할 수 있는 대책 마련(미래부, 방통위)

○ **(빅데이터) 개인정보보호 가이드라인**을 제공('14.8월)하고, **개인정보보호 기술개발 및 상용화** 지원 ('14년~)

- 개인정보 처리 대행 전문기업 및 개인정보 침해 문제해결 지원을 위한 **클리어링 하우스*** 도입 검토 ('14년)

* 빅데이터 활용에 따른 개인정보 침해, 품질·가치 훼손 등 문제해결 지원 전담기관

- 장기적으로는 개인정보 제공시 사전동의를 받도록 하는 방식을 **중요성이 높지 않은 경우 사후동의 방식*** 허용 검토 ('16년)

* 현재는 모든 개인정보에 대해 정보제공시 사전동의(opt-in)를 받는 방식

○ **(클라우드 컴퓨팅)** 클라우드컴퓨팅법 제정 등 이용자가 **클라우드에 저장하는 각종 정보**에 대한 **제도적 보호장치 마련** ('14년)

○ **(사물인터넷)** 보안, 프라이버시 등 역기능 대응을 위한 **'정보보호 로드맵'** 마련 ('14년)

○ **(영상정보처리기기)** 보호제도* 마련을 위한 **전문가 검토 등 추진** ('14년, 안행부)

* 개인영상정보의 처리기준과 절차, 영상정보처리기기의 관리·보호 요건, 영상정보주체의 권리보장 등 규정

(3) 전문인력 양성

□ 초중고, 대학, 군대 등 **연속성 있는 인력양성 체계 구축**

○ **(초중고)** SW과목을 교과과정에 포함토록 추진하고, **정보보호 영재교육원** 신설·운영('14년 4개), 특성화고(6개→10개) 및 **마이스터고** (1개→2개) **정보보호과정 확대** 추진('17년)

* 향후, 대학입시 선택과목 반영 등 대학입시와 연계여부 검토 추진(교육부)

○ **(대학) 정보보호 특성화 대학 지정** 및 **정보보호학과 설치** 확대 (28개→'17년 35개)

- 사이버 안전관련 대학의 연구기능 강화를 위해 **사이버시큐리티 연구센터*** 설치·운영(5개, '14년)

* 사이버관련 연구시설, 시스템 지원 및 연구활동비 지원 사업

○ **(군복무)** 사이버보안을 전문으로 하는 사관(30명, '16년~), 부사관·병 양성('15년~) 및 예비군 창설 추진

□ **맞춤형 인력양성**

○ **(최정예 인력 양성 등)** 2017년까지 차세대 보안리더 등 국가 사이버 위기시 대응이 가능한 우수인력 5,000여명 양성

○ **(실무인력 양성)** 금융, 의료 등 다양한 산업분야에서 필요한 실무 인력 양성('16년)

* 금융 및 일반기업 정보보호책임자(CISO)(각 4회, 240명), 보안관제(6회, 180명) 과정 확대

○ **(개인정보보호책임자(CPO)과정 신설)** 공무원, 기업 CEO, CPO 등 산업현장의 수요를 반영한 개인정보보호 전문과정 신설 추진('16년~)

Ⅳ. 과제별 추진계획

연번	과제 내용	소관	일정
□ 핵심제도 선진화 대책			
1. 책임 및 권리구제 강화			
(1) 권리구제 강화			
1	법정손해배상 제도 도입 - 개인정보보호법, 신용정보법 개정	안행부 금융위	14년
2	징벌적 손해배상제도 도입 - 개인정보보호법, 정보통신망법, 신용정보법 개정	안행부 방통위 금융위	14년
3	거액의 손해배상 발생에 대비한 금융기관 보험가입 의무화 - 신용정보법 개정	금융위	14년
(2) 관리 책임성 확보			
4	개인정보 유출 등 범죄자 처벌 강화 - 개인정보보호법, 신용정보법 개정	안행부 방통위 금융위	14년
5	개인정보 유출기관에 대한 과징금 기준 상향	방통위 금융위	14년
6	개인정보 보호책임자(CPO)를 임원급으로 지정하고, 최고경영자에게 보고를 의무화 - 개인정보보호법 개정	안행부	14년
7	법위반시 정보통신서비스 제공자의 대표자 등에 대한 해임 등 징계권고 규정 마련 - 정보통신망법 개정	방통위	14년
8	개인정보유출시 피해자 불편과 경제적 부담을 최소화토록 의무화 - 표준개인정보보호지침 등 개정	안행부	14년
(3) 이용자 중심 시스템 개선			
9	개인정보 제공 동의서를 알기쉽게 작성해야할 의무를 보다 구체화 - 개인정보보호법 시행령 개정	안행부	14년
10	‘온라인 개인정보 수집·이용·제공 등 가이드라인’ 마련	방통위	14년
11	개인정보 처리방침에 열람·처리정지·파기 등 요구권 행사방법 및 의무적 공개항목을 구체화 - 개인정보보호법 개정	안행부	14년
12	정보 처리정비·삭제 요구 절차를 간소화 - 개인정보보호법 개정	안행부	14년

연번	과제 내용	소관	일정
2. 주민등록번호 관리제도 개선			
(1) 주민번호 변경 허용 방안			
13	피해를 입거나 피해를 입을 우려가 큰 경우 주민번호 변경 허용 - 주민등록법 개정	안행부	14년
14	주민번호 전면개편 방향 검토	안행부	14년
(2) 대체 방안			
15	I-PIN 서비스 오프라인 확대실시	안행부	14년
16	민간 I-PIN 발급기관이 주민번호를 보관하지 않도록 개편	안행부	15년
17	주민번호 外 다양한 개인식별수단 도입 방안 검토	안행부	15년
(3) 수집 최소화 방안			
18	주민번호 수집업무에 대한 전수조사 실시 및 수집 근거법령 정비	안행부	14년
19	민간분야 주민번호 수집대상 단계적 축소	안행부	계속
20	개인정보보호위원회에 주민번호 근거법령 정비 소위 구성하여 주민번호 수집 적정성 사전·사후 심사	개보위	15년
21	매뉴얼 배포 및 캠페인을 통한 의식과 관행 개선 - 개인정보보호 매뉴얼, 분야별 가이드라인 등 지속 보완·배포 - 민·관 공동 주민번호 미수집 합동 캠페인 전개	안행부	14년~
22	주민번호 불법수집 신고창구 운영	안행부	14년~
(4) 안전조치 강화 방안			
23	주민번호 암호화 조치 의무화에 대비 - 업종별 특성을 고려한 적용대상·시기기준 등 마련	안행부	15년
24	기업 스스로 점검할 수 있는 도구 개발·보급 - 영세사업자에 대한 SW 및 주민번호 수집금지·파기기술 지원	안행부 방통위	15년
□ 유출된 개인정보 대응대책			
1. 유출된 개인정보 삭제·파기			
25	개인정보 "대청소 기간" 설정, 불법 유통정보 삭제 조치 등	방통위 개보위	14년
26	중요웹사이트에 대해 개인정보 노출 탐지·삭제 강화	방통위	15년
27	개인정보 삭제조치 실효성 확보 - 정보통신망법 개정 및 인프라 확충	방통위 안행부	14년
28	탐지대상을 웹사이트 → 페이스북, 트위터 등 SNS로 확대	방통위	14년
29	해외 유출 개인정보 삭제·파기 추진 - 한-중 수사협의체 구성 등 사법공조를 강화 - 해외포털 서비스와의 협력 강화 - 개인정보보호 협력센터 확대	방통위 합수단	14년~

연번	과제 내용	소관	일정
2. 체계적인 불법정보 단속·적발			
30	대대적인 개인정보 침해 및 불법유통에 대한 집중단속	합수단	14.4월~15.4월
31	방송통신심의위, 검·경 등 간의 정보공유 및 협업체계 확충	방통위 검·경	15년
3. 유출정보를 활용한 금융사기 방지			
32	보이스피싱, 파밍 차단서비스 대상기관 확대	미래부	15년
33	스미싱 확인 서비스 실시	미래부	14년
34	모바일 사이버 치료서비스 구축	미래부	14년
35	발신번호 임의변경 문자 차단 서비스 확대	미래부	14년
36	「정보유출 사고 대응매뉴얼」 마련 의무화를 위한 관련 규정 개정	안행부 방통위 금융위	14년
□ 개인정보 예방·유출방지 및 사이버안전 대책			
1. 현장 중심 관리체계 정비			
(1) 통신사·대리점 등 취약분야 구조적 관리			
37	하위영업점 통신사등록 의무화, 미등록 및 불법행위 퇴출수단 마련	방통위	15년
38	통신사 '개인정보 관리수준 평가제도' 도입 및 평가결과 공개	방통위	15년
39	SMS 본인인증제도 시행	방통위	15년
40	서비스 가입신청 시 '전자 청약 시스템' 적용 추진	방통위	15년
41	신용카드 결제 단말기 관리업체 관리·감독체계 정비	금융위	14년
42	TM시 개인정보 수집 출처를 수신인에게 사전고지토록 의무화	방통위	14년
43	TM수신거부시스템 이용안내 등 활성화	공정위	14년
44	TM에 대한 민간 자율적 개인정보보호 관리체계 확충 - 개인정보보호 인증마크제*(ePRIVACY)를 TM업체로 확대 - 민간자율 불법 TM신고 제도를 전 업종으로 확대	방통위	15년
45	불법 TM의 전화번호 이용 정지를 위한 관련법률 개정	미래부	14년
46	지방 권역별 정보보호 지원센터 확충	미래부	14년
(2) 개인정보 관리단계별 강화			
47	실태점검시 파악된 개인정보 과다수집 사례 등 정비	안행부	~15.3월
48	최소수집원칙을 점검하고 정비할 수 있는 체계 구축 및 추진	안행부	계속
49	개인정보 다수 처리 기관은 제3자로부터 제공받은 개인정보에 대해 수집출처 및 목적을 관리하도록 의무화 - 개인정보보호법 개정	안행부	14년

연번	과제 내용	소관	일정
50	수탁자의 담당자 연락처 등 위탁에 관한 사항을 보다 구체화 - 표준 작성지침 마련	안행부	14년
51	위·수탁자 모두에게 손해배상을 청구할 수 있도록 명시 - 개인정보보호법 개정	안행부	14년
52	법령상 근거에 따라 필요최소한 기간만 보존 후 파기토록 규정 재정비	전부처	14년
53	개인정보 파기시, 복구 또는 재생되지 않게 조치 - 신용정보법 개정	금융위	14년
54	전문가 의견수렴 등을 통해 잊혀질 권리, 디지털 유산 등에 대한 법제도 구축방안 검토	방통위	15년
(3) 법률 및 행정시스템 정비			
55	법적용 명확화 및 제재수준 정비 등 법률간 정합성 제고 - 적용대상 명확화 - 개별법상 상충되는 규정 및 제재수준 정비 - 개별법상 별도규정이 없는 경우, 개인정보보호법 준용토록 명문화	안행부 방통위 금융위	14년
56	개인정보보호위를 통해 상시적으로 관련 법령간 정합성을 유지하는 체계를 구축(법령심사소위 설치 등)	개보위	14년
57	개인정보보호위가 부처에 대한 실질적인 조정·점검 기능을 수행할 수 있도록 조사요구권 부여, 점검권한 등 신설	안행부	14년
58	개인정보보호 관련 조직 및 전문인력 보강	안행부	15년
59	범정부적 개인정보 정책지원 전문기관 확충 추진	미래부 기재부	15년
2. 유출예방 · 방지를 위한 정보보호 투자 촉진			
(1) 민간·공공 투자 확충			
60	민간 및 공공분야 인센티브 확대 추진	미래부, 기재부 고용부 등	~17년
61	정보보호산업 진흥을 위한 법적 근거 마련 추진	미래부	14년
62	10대 전략제품 핵심기술개발 로드맵을 통해 제품 발굴·육성	미래부	14~18
(2) 기업의 기술적 자율성 제고			
63	개인정보보호 관련 기술적 조치제도(고시)를 개정하여 기업의 자율성을 부여	방통위 금융위	14년 15년
64	장기적으로 보호조치 기준에 세부적 조치사항을 규정하지 않고, 보호목표를 규정하여 기업의 자율성을 부여하는 체계로 전환 검토	안행부 방통위 금융위	15년

연번	과제 내용	소관	일정
65	유사인증제도간 중복 해소 및 상호 인정범위 확대 추진	미래부 안행부 방통위	14년
3. 사이버안전 및 기술기반 강화			
(1) 보안기술 강화			
66	경량 암호화 기술 개발	미래부	16년
67	이메일 악성코드 유포 탐지시스템 구축	미래부	15년
68	악성코드 은닉사이트 탐지 강화를 위해 탐지대상 홈페이지 확대	미래부	14년
69	가상 ID 10만개를 통해 해커를 유인하는 사이버트랩 시스템 개발	미래부	15년
70	주요정보통신기반시설에 대한 정기적 모의해킹·훈련 근거 마련 - 정보통신기반보호법 개정	미래부	14년
71	사이버 위협 자동분석시스템(C-TAS) 개발 및 운영	미래부	14.7월
72	비행기 블랙박스처럼 사이버 침해사고를 신속하게 분석하고 증거를 보존하는 기술인 사이버 블랙박스 개발	미래부	16년
73	중소인터넷 서비스업체 및 학교 등 공용 PC 등에 대해 사이버 치료체계 적용	미래부	14년
74	PC 자가진단 도구 보급 및 SW 원클릭 안심서비스 구축·운영	미래부	15년
75	SW 업데이트시 유포되는 악성코드 탐지체계 확대	미래부	17년
76	스미싱 차단앱 등을 스마트폰 출고시 기본탑재 추진	미래부	14년~
77	폰키퍼(스마트폰 보안앱) 일일 보안공지 용량 확대	미래부	14년
78	악성앱 모니터링 대상 확대	미래부	15년
79	신종·변종 악성앱에 대한 정보 유출행위 탐지기술 개발	미래부	15년~
80	정보공유분석센터(ISAC)를 주요 산업분야로 확대·구축 지원	미래부 관계부처	15년~
(2) 신ICT산업분야 정보보호 체계 정립			
81	웹표준 기반 공인인증서비스 기술개발	미래부	14년
82	공인인증서 유출방지를 위하여 보안토큰 등 안전한 저장매체 확대 추진	미래부	14년
83	ICT 융복합기기에 대한 보안성 강화를 위한 사전연구('15년)를 거쳐 인증서비스 개발·도입	미래부	16년

연번	과제 내용	소관	일정
84	정보시스템의 설계단계에서 정보보호를 고려토록 하는 사업모델(Business Model)을 확산	미래부	14년~
85	빅데이터 관련 개인정보보호 가이드라인 제공	방통위	14.8월
86	개인정보보호 기술개발 및 상용화 지원	미래부	14년~
87	클리어링 하우스 도입 검토	미래부	14년
88	장기적으로는 현행 사전동의 방식(opt-in)을 분야에 따라 일부 사후동의 방식(opt-out)으로 전환 검토	방통위	16년
89	클라우드에 저장하는 각종 정보에 대한 제도적 보호장치 마련 - 클라우드컴퓨팅법 제정	미래부	14년
90	보안, 프라이버시 등 역기능 대응을 위한 '정보보호 로드맵' 마련	미래부	14.9월
91	개인영상정보 보호제도 마련을 위한 전문가 검토 등 추진	안행부	14년
(3) 전문인력 양성			
92	대학과 연계한 정보보호 영재교육원을 신설・운영	미래부, 교육부	14년
93	특성화고(6개→10개) 및 마이스터고(1개→2개) 정보보호과정 확대 추진	미래부, 교육부	17년
94	정보보호 특성화 대학 지정 및 정보보호학과 설치 확대	미래부, 교육부	17년
95	사이버전문사관(30명, '16년~), 부사관·병 양성('15년~) 및 사이버보안 예비군 창설 추진 등 민군 연계 인력관리	미래부 국방부	15년~
96	국가 사이버 위기시 대응이 가능한 우수인력 5,000여명 양성	미래부	17년
97	금융, 의료 등 다양한 산업분야에서 필요한 실무 인력 양성	미래부 금융위 복지부	16년
98	산업현장의 수요를 반영한 정보보호 전문과정 신설 추진	미래부 방통위	16년~

참고1 공공기관 개인정보 보유실태

□ 국가행정기관(중앙행정, 지방자치, 교육기관)이 보유·관리하는 **개인정보파일* 목록 수는 약 34만여개, 개인정보 수**는 1,031억건**('13년)

* 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물 (예시: 보험료 납부내역)

** 주민등록번호 등 개별 개인정보의 주체(사람)를 말하며, 하나의 개인정보파일 내에 동일한 사람 중복포함 가능 (예시: 개인별 보험료 납부내역)

○ 개인정보보호법에 따라 보유현황 인터넷 공개(www.privacy.go.kr)

< 연도별 개인정보파일 목록 수 >

연도	총계	중앙행정	지방자치	교육기관
2009	375,441	4,883	78,928	291,630
2010	309,355	5,682	67,800	235,873
2011	261,725	9,796	89,033	162,896
2012	323,425	14,356	151,400	157,669
2013	336,820	16,971	168,424	151,425
2014. 6월	339,875	17,109	171,471	151,295

□ 주요 개인정보파일 보유현황 예시

○ **(안행부)** 공직자재산등록정보*, 주민등록정보 등 개인정보파일 146개

* 주요항목: 재산등록항목(성명, 주민번호, 직급 등), 정보제공동의서(성명, 동의자 인적사항 등), 고지거부 신청서(성명, 생년월일, 등) 등 30여개

○ **(복지부)** 건강보험공단의 보험료 납부내역* 등 개인정보파일 670개

* 주요항목: 인적정보, 납부금액, 납부자명, 고지이력일련번호, 자동이체금액 등 220여개

○ **(국세청)** 부가가치세 과세*, 사업자등록 등 개인정보파일 19개

* 주요항목: 사업장 주소, 상호, 성명, 사업장등록번호, 매입세액, 소득종류 등 10개

참고2 주요사항별 실태점검 결과 총계

13개 분야 (법 해당 조항)	항목수	서면조사 결과		현장점검 결과		점검항목 중 개선필요 비율*(%)
		양호	개선필요	양호	개선필요	
제15조(개인정보의 수집·이용 동의)	4	30,877	**2,253**	13,949	**2,580**	**10.1**
제16조(최소 수집 및 서비스 제공 거부)	2	17,927	398	8,772	592	4.6
제17조(개인정보의 제공)	3	18,030	941	6,394	964	5.0
제18조(개인정보의 이용·제공 제한)	4	26,021	869	9,630	801	3.1
제21조(개인정보의 파기)	4	36,725	**1,491**	16,532	**2,074**	**8.1**
제22조(동의를 받는 방법)	4	23,567	1,284	9,158	**1,445**	**5.7**
제23조(민감정보의 처리 제한)	3	10,989	504	2,853	440	2.3
제24조(고유식별정보의 처리 제한)	2	11,176	554	4,265	571	4.5
제26조(업무위탁에 따른 처리 제한	4	25,309	**1,887**	12,838	**4,033**	**15.7**
제28조(개인정보취급자에 대한 감독)	3	30,999	**1,502**	16,333	1,433	7.5
제29조(안전 조치 의무)	26	208,286	**12,582**	113,258	**13,534**	**8.1**
제30조(개인정보 처리방침의 수립·공개)	3	30,382	1,270	16,041	1,373	7.1
제31조(개인정보 보호책임자의 지정)	2	21,717	459	11,604	423	3.3
기타(기관별 자체 추가 항목)	일부	435	0	1,630	279	7.0
13개 분야	**64개**	**492,440**	**25,994**	**243,257**	**30,542**	**7.4**

* 개선필요 비율 : 개선필요 항목수 / 총 점검 항목수(양호+개선필요+기타)

참고3 주요 용어설명

용어	내용	쪽
개인정보 자기결정권	정보주체가 개인정보의 공개와 이용 등에 관하여 스스로 결정할 수 있는 권리	1
개인식별체계	개인을 다른 사람과 구분하거나 구별할 수 있는 방식 (예시: 주민번호, 여권번호 등과 같은 고유식별정보)	1
부정사용 방지시스템(FDS)	카드거래 내역 분석을 통해 의심거래 이상 징후에 대하여 회원과 통화하는 등 확인하여 사고를 예방하는 시스템	14
개인정보 보호책임자(CPO)	개인정보 처리에 관한 업무를 총괄하여 책임지는 권한을 가진 자	18
아이핀(I-PIN)	인터넷에서 주민번호를 대신하여 개인을 식별하는 수단	21
사회관계망서비스 (SNS)	인터넷 이용자들이 새로운 인맥을 쌓거나 기존 인맥관계 강화를 돕는 서비스 (예시: 페이스북, 트위터, 싸이월드 등)	24
주민번호 클린센터	이용자 주민번호의 인터넷 이용내역을 간편하게 조회할 수 있도록 안전행정부와 KISA가 제공하는 무료 서비스	24
개인정보보호 협력센터	국외 웹사이트 상에서 불법 거래되는 개인정보의 삭제·단속 강화를 위해 협력센터 운영 및 국제공조 도모 * 한중인터넷협력센터(중국, '12.11월 설립)	25
보이스피싱	전화 등을 통해 신용카드 번호 등의 개인정보를 알아내어 범죄에 이용하는 전화금융사기 수법	26
파밍	합법적인 도메인을 탈취하거나 도메인네임시스템(DNS), 서버 주소를 변조하여 개인정보를 훔치는 컴퓨터 범죄 수법	26
모바일 사이버 치료서비스	스마트폰에 악성앱 감염 사실을 알려주고 치료 방법을 안내 서비스 제공	26
피싱	금융기관 등으로부터 개인정보를 불법적으로 알아내 이를 이용하는 사기수법	26

용어	내용	쪽
스미싱	스마트폰 문자메시지를 통해 소액 결제를 유도하는 피싱 사기 수법	26
전자청약시스템	상품설명서, 가입설계서, 청약서 등의 종이서류 없이 본사와 직접 연결된 전용 단말기와 전자서명만으로 청약이 가능한 서비스	27
판매시점정보 관리시스템(POS)	금전등록기기와 컴퓨터 단말기의 기능을 결합한 시스템	28
텔레마케팅(TM)	소비자의 구매 이력 등을 근거로 전화 매체 등을 이용한 판매 방식	28
TM수신거부시스템 (www.donotcall.go.kr)	전화권유판매 수신거부의사 등록시스템에서 간단한 휴대폰 인증을 통해 무분별한 텔레마케팅 차단 및 신고 서비스 제공	28
개인정보보호 인증마크제 (ePRIVACY)	기업(기관) 홈페이지 이용자의 개인정보보호 수준을 관계 법령에 근거하여 심사하고, 일정수준 도달시 인증마크를 부여하는 민간자율인증제도 * OPA(개인정보보호협회) 발급	28
신용카드 결제망 관리회사(VAN社)	신용카드 결재승인, 가맹점 단말기 설치, 전표매입 등을 대행하는 업체	28
권역별 정보보호지원센터	지역별 맞춤형 정보보호 상담 및 컨설팅 수행을 위해 지방 권역별 센터를 설립하여 서비스 제공	28
개인정보파일	개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열 및 구성한 개인정보의 집합물 (예시: 보험료 납부내역 등)	29
한국인터넷진흥원 (KISA)	인터넷서비스활성화, 해킹·바이러스 대응, 개인정보보호, 방송통신 국제협력 등을 위한 미래창조과학부 산하 공공기관	32
APT 공격	악성코드 이메일을 통해 PC를 감염시키고, 감염된 좀비PC를 통해 정보를 유출하는 해킹공격 방법의 하나	34
유니버셜 인증	웨어러블 컴퓨터에 적용 가능한 인증 및 암호화	34

용어	내용	쪽
개인정보인증제도 ISMS PIMS PIPL	공공기관과 민간 기업이 일정 기준 이상의 개인정보보호 수준을 갖추면 정부가 이를 인증해주고 외부에 공개할 수 있게 하는 제도 * ISMS(정보보호관리체계, 미래부) : 정보통신서비스제공자 대상 * PIMS(개인정보보호관리체계, 방통위) : 개인정보취급 정보통신서비스제공자 대상 * PIPL(개인정보보호인증제, 안행부) : 모든 개인정보처리자 대상	35
스피어피싱	잘 아는 지인이 보내는 것처럼 위장한 이메일을 특정인에게 발송하여 악성코드에 감염시킨 후 정보 유출	36
사이버트랩 시스템	가상 ID 등을 통해 해커를 유인하는 미끼도구	36
허니팟	해커를 속이기 위해 가상의 개인정보를 활용해 의도적으로 설치해두어 공격을 유도하는 시스템	36
사이버위협 자동분석시스템 (C-TAS)	각종 사이버침해사고 정보를 실시간 종합적 수집·분석·공유 가능한 시스템으로 수집→분석→공유 절차를 거침 * 현재 KISA에서 시범 운영중('14.5월)	37
좀비PC	바이러스에 감염됐지만 스스로 인지하지 못한 채 스팸을 보내는 등 원격 조종당하는 PC	37
PC 자가진단 도구	자가 PC의 취약점 점검 서비스 (예시: SW업데이트 정보 제공, 비밀번호 안전정도 점검 등)	37
SW 원클릭 안심서비스	PC에 설치된 주요 소프트웨어의 버전을 확인할 수 있고 최신 버전으로 업데이트하기 위한 정보 제공 서비스	37
킬스위치	스마트폰을 분실하는 경우 원격으로 조작해 개인 데이터를 삭제하고 사용을 막는 일종의 자폭 기능	37
사이버블랙박스	비행기 블랙박스처럼 사이버 침해사고를 신속하게 분석하고 증거를 보존하는 기술	37
정보공유분석센터 (ISAC)	사이버테러 대응을 위해 보안취약점, 침해요인 등의 정보를 공유하고 사고발생 시 즉시 분석	38

용어	내용	쪽
액티브-X (Active-X)	일반 응용프로그램과 웹의 연결을 돕는 기술로서, MS사의 익스플로러를 통해 지원	38
웹표준 방식	웹사이트 개발시 익스플로러, 사파리, 크롬 등 어떤 브라우저를 사용해도 같은 결과가 나타나도록 국제웹표준화기구(W3C)의 표준에 맞추어 개발하는 방식	38
보안토큰	전자서명생성키 등의 비밀정보를 안전하게 저장·보관하기 위하여 키 생성·전자서명 생성 등이 기기 내부에서 처리되도록 구현된 하드웨어 기기	38
USIM	이용자 식별정보 등이 저장된 장치로 이동통신단말기기 등에 삽입하여 사용	38
ATM (자동거래금융단말기)	현금지급, 입금, 계좌이체 등을 처리할 수 있는 기기	38
빅데이터	디지털 환경에서 생성되는 방대한 양의 데이터로서, 다양한 형태로 집적되어 분석 및 예측이 가능	39
클라우드 컴퓨팅	인터넷상의 서버를 통하여 데이터 저장, 네트워크, 콘텐츠 사용 등 IT 관련 서비스 이용이 가능한 컴퓨터 환경	39
사물인터넷	사물을 유무선 네트워크로 연결하여 정보를 공유하는 환경으로, 다양한 사물에 구현되어 최근에는 만물인터넷의 개념이 등장 (예시: 구글 글라스, 심장박동 모니터링 기계 등)	39
클리어링 하우스	복수 통신사업자의 로밍 및 인증, 정산 등을 위한 서비스	39
정보보호 최고책임자(CISO)	기업(기관)에서 정보보안 업무에 관련된 총괄 책임을 지는 임직원	40