개인정보보호 실태점검단 교육

교육 개요

○ 일　　시 : 2014.2.28(금), 13:30~16:00
○ 장　　소 : 정부서울청사 별관 2층 강당
○ 참석대상 : 부처별 점검단 담당자

교육 시간표

시 간		주 요 내 용	비 고
13:00~13:30	30’	ㅇ 교육생 등록	
13:30~13:40	10‘	ㅇ 국민의례 및 인사말씀	안전행정부 개인정보보호과
13:40~16:00	140‘	개인정보보호 실태점검 지침 (가이드라인)	

개인정보처리시스템별 점검 항목(결과)표

(000 시스템)

* 13개 분야 64개 항목

분야 (해당 법 조항)	세부 점검 항목	양호	개선 필요	해당 없음
제15조(개인정보의 수집·이용 동의)	1. 온·오프라인 회입가입 시 동의 여부			
	2. 각종 게시판, 기타 개인정보 수집 시 동의 여부			
	3. 정보주체 동의 시 필수 고지항목(4개*) 고지 여부			
	4. 필수 고지항목(4개*) 내용의 적정 여부 * 4개 : 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			
제16조(최소 수집 및 서비스 제공 거부)	5. 목적에 필요한 최소한의 개인정보 수집 여부			
	6. 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부			
제17조(개인정보의 제공)	7. 제3자에게 개인정보 제공 시 정보주체 동의 여부			
	8. 정보주체 동의 시 필수 고지항목(5개*) 고지 여부			
	9. 필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			
제18조(개인정보의 이용·제공 제한)	10. 개인정보 수집 당시 정보주체의 이용·제공 동의 범위를 초과하여 이용·제공 여부			
	11. 개인정보 제공 시 제공 목적범위 내 이용, 안전조치 실시, 목적 달성 후 파기 등 요청 여부			
	12. 동의에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개*) 고지 여부			
	13. 필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			
제21조(개인정보의 파기)	14. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부			
	15. 개인정보 파기 시 복구 또는 재생되지 않도록 조치 여부			
	16. 임시파일 및 출력자료 등에 대한 즉시 파기 여부			
	17. 법령에 따라 보존할 경우 별도 분리 보관 여부			
제22조(동의를 받는 방법)	18. 최소 개인정보와 그 외의 개인정보 구분 동의 여부			
	19. 동의가 필요한 정보(필수정보)와 동의 없이 처리할 수 있는 정보(선택정보)의 구분 동의 여부			
	20. 홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부			
	21. 선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부			

분야 (해당 법 조항)		세부 점검 항목	양호	개선 필요	해당 없음
제23조(민감정보의 처리 제한)		22. 사상, 정치, 건강 등 민감정보의 동의에 의한 수집 및 제공 시 구분 동의 여부			
		23. 정보주체 동의 시 필수 고지항목(수집 4개, 제공 5개) 고지 여부			
		24. 필수 고지항목(4개 또는 5개) 내용의 적정 여부			
제24조(고유식별정보의 처리 제한)		25. 고유식별정보*의 동의에 의한 수집 및 제공 시 구분 동의 여부 * 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호			
		26. 주민등록번호 외 회원가입 방법 제공 여부			
제26조(업무위탁에 따른 처리 제한		27. 위탁 계약 시 문서(계약서)에 의한 계약 여부			
		28. 문서(계약서)에 필수 반영사항(6개*) 포함 여부 * 6개 : 목적외 처리금지, 기술 관리적 보호조치, 목적·범위, 재위탁 제한, 접근제한 등 안전조치, 관리·감독사항			
		29. 수탁자에 대한 교육 실시 여부			
		30. 처리현황 점검 등 수탁자 관리·감독 여부			
제28조(개인정보취급자에 대한 감독)		31. 개인정보취급자에 대한 관리·감독(접근권한 관리, 통제 등 포함) 여부			
		32. 개인정보취급자에 대한 보안서약서 징구 여부			
		33. 개인정보취급자에 대한 정기적인 교육 실시 여부			
제29조(안전조치의무)	내부관리계획 수립·시행	34. 내부관리계획 수립·시행 여부			
		35. 내부관리계획의 필수 반영사항(4개*) 포함 여부 * 4개 : 보호책임자 지정, 보호책임자/취급자의 역할·책임, 안전성 확보 조치, 취급자 교육			
	접근권한 관리 및 접근통제	36. 시스템에 대한 접근권한을 필요 최소한의 범위로 업무 담당자에 따라 차등 부여 여부			
		37. 전보·퇴직 등 인사이동으로 취급자가 변경될 경우 접근권한 변경 또는 말소 여부			
		38. 접근권한의 부여·변경·말소 내역의 기록관리 및 최소 3년간 보관 여부			
		39. 취급자별로 개별 계정 발급 여부			
		40. 안전한 비밀번호 작성규칙의 수립·적용 여부			
		41. 불법적 접근 및 침해사고 방지를 위한 시스템 설치·운영 여부			
		42. 외부에서 정보통신망을 통한 접속 시 가상사설망, 전용선 등 안전한 접속수단 제공 여부			
		43. P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단 실시 여부			
		44. 인터넷 홈페이지의 개인정보 노출 방지를 위한 보안조치 실시 여부			

분야 (해당 법 조항)		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	개인정보의 암호화	45. 개인정보 암호화계획 수립·시행 여부			
		46. 비밀번호의 외부 송·수신 시 암호화 조치 여부			
		47. 비밀번호의 내부 저장 시 일방향 암호화 조치 여부			
		48. 바이오정보의 외부 송·수신 시 암호화 조치 여부			
		49. 바이오정보의 내부 저장 시 암호화 조치 여부			
		50. 고유식별정보의 외부 송·수신 시 암호화 조치 여부			
		51. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 암호화 조치 여부			
		52. 고유식별정보의 내부 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부			
	접속기록의 보관	53. 취급자의 접속기록을 최소 6개월 이상 보관·관리 여부			
		54. 접속기록의 항목(4개*)이 적정한지 여부 * 4개 : ID, 날짜 및 시간, 접속자 IP 주소, 수행 업무(열람, 수정, 삭제, 인쇄, 입력 등)			
		55. 접속기록이 위·변조 및 도난, 분실되지 않도록 접속기록의 안전하게 보관 여부			
	보안프로그램 설치·운영	56. 보안 프로그램의 설치·운영 여부			
		57. 보안 프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부			
	물리적 접근 방지	58. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 수립·운영 여부			
		59. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부			
제30조(개인정보 처리방침의 수립·공개)		60. 개인정보 처리방침의 수립 여부			
		61. 개인정보 처리방침에 필수 항목(8개*) 포함 여부 * 8개 : 처리 목적, 처리 및 보유기간, 제3자 제공 사항(해당 시), 위탁 사항(해당 시), 정보주체 권리·의무 및 행사 방법, 처리항목, 파기 사항, 안전성 확보 조치 사항			
		62. 개인정보 처리방침의 홈페이지 등 공개 여부			
제31조(개인정보 보호책임자의 지정)		63. 개인정보 보호책임자 지정 여부			
		64. 개인정보 보호책임자의 업무 범위, 자격요건 등 적정 여부			

1 개인정보의 수집·이용 동의(법 제15조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제15조(개인정보의 수집·이용 동의)	1. 온·오프라인 회원 가입 시 동의 여부			
	2. 각종 게시판, 기타 개인정보 수집 시 동의 여부			
	3. 정보주체 동의 시 필수 고지항목(4개*) 고지 여부			
	4. 필수 고지항목(4개*) 내용의 적정 여부 * 4개 : 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

1. 온·오프라인 회원 가입 시 동의 여부

❍ 온라인 회원 가입 서식 및 오프라인 상으로 회원 가입신청서 등을 통해 정보주체의 개인정보를 수집·이용하는 경우로서,

- 서식에 개인정보 수집·이용에 관한 명시적 '동의' 표시(체크) 여부 확인

※ 법령 상의 규정이나 의무 수행을 위한 경우에는 명시적으로 '동의' 표시 행위로서 동의 여부를 확인하지 않아도 되며, 점검 항목표에는 '해당 없음'에 체크
다만, 법령 상 규정 등에도 불구하고 동의를 받는 경우에는 '양호'에 체크

2. 각종 게시판, 기타 개인정보 수집 시 동의 여부

❍ 홈페이지 운영 시 각종 게시판(예: 칭찬합시다, 건의사항, 자유게시판, 민원, 상담 등)을 통해 개인정보를 수집하는 경우와 회원 가입이 아닌 형태의 모든 개인정보를 수집하는 서식으로,

- 서식에 개인정보 수집·이용에 관한 명시적 '동의' 표시(체크) 여부 확인

☞ **홈페이지 회원가입은 대부분 동의를 받고 있으나, 게시판은 동의 받지 않는 사례 다수 있음**

3. 정보주체 동의 시 필수 고지항목(4개) 고지 여부

❍ 온·오프라인 회원 가입 서식과 홈페이지 게시판, 기타 서식을 통해 개인정보를 동의 받고 수집·이용하는 경우 필수 고지항목(4개)를 고지하고 동의 받는지를 확인

< 동의 여부 획득 시 필수 고지사항 >

① 개인정보의 수집·이용 목적 ② 수집하려는 개인정보의 항목 ③ 개인정보의 보유 및 이용 기간 ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

☞ **정보통신망법에 따라 ①~③번은 고지하나, 상당수 홈페이지에서 ④은 고지하지 않고 있음, 또한 개인정보처리방침 전체를 고지하여 ④가 미포함된 상태로 고지하지 않는 사례 다수 있음**

4. 필수 고지항목(4개) 내용의 적정 여부

❍ 온·오프라인 회원 가입 서식과 홈페이지 게시판, 기타 서식을 통해 개인정보 동의 획득 시 고지하는 항목(4)의 내용을 확인

- 개인정보의 수집·이용 목적이 적정한지 여부 확인
- 수집하려는 개인정보의 항목과 보유 및 이용기간 설정이 수집 목적 달성을 위해 적합하게 설정되었는지 여부 확인
- 동의 거부 시 불이익 사항을 적시 하는 경우 그 적정성 확인

※ 필수항목, 선택항목에 따른 수집 목적을 명확히 하고, 목적 달성을 위해 불필요한 수집항목과 보유기간 등은 수집·이용하는 목적에 맞게 조정 필요

2 최소 수집 및 서비스 제공 거부(법 제16조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제16조(최소 수집 및 서비스 제공 거부)	5. 목적에 필요한 최소한의 개인정보 수집 여부			
	6. 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부			

□ 점검 방법 및 평가 기준

5. 목적에 필요한 최소한의 개인정보 수집 여부

❍ 온·오프라인 상에서 필수정보로 개인정보를 수집하는 경우, 목적 달성을 위해 반드시 수집하여야 하는 최소한의 개인정보인지 여부 확인

- 필수정보는 아니나, 추가적인 서비스 제공 등을 위해 필요한 선택정보로 수집하는 경우에도 목적 달성을 위한 최소한의 정보인지 여부를 확인

※ 최소한의 개인정보 수집 여부에 대한 입증 책임은 개인정보처리자가 부담

6. 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부

❍ 온라인 회원 서식 또는 오프라인 각종 서식 등을 통해 정보주체의 동의 획득 시 최소한의 정보(필수정보) 외의 개인정보 수집에 동의하지 않는다는 이유로 회원 가입 또는 기본적인 서비스 제공이 가능한지 여부 확인

- 특히, 홈페이지 회원 가입 시 필수정보가 아닌, 선택정보로 되어 있는 개인정보를 미입력 시 회원가입 진행을 하지 못하는 경우 확인

☞ **홈페이지에서 선택정보이나, 동의 체크하지 않으면 다음으로 넘어가지 않은 사례 있음**

3 개인정보의 제공(법 제17조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제17조(개인정보의 제공)	7. 제3자에게 개인정보 제공 시 정보주체 동의 여부			
	8. 정보주체 동의 시 필수 고지항목(5개*) 고지 여부			
	9. 필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

7. 제3자에게 개인정보 제공 시 정보주체 동의 여부

❍ 온·오프라인 회원 가입 서식 또는 각종 서식을 통해 수집한 개인정보를 제3자에게 제공 시 동의를 받고 있는지 여부를 확인

- 서식에 개인정보 제공에 관한 명시적 '동의' 표시(체크) 여부 확인

※ 법령 상의 규정이나 의무 수행을 위한 경우에는 명시적으로 '동의' 표시 행위로 동의 여부를 획득하지 않아도 되며, 점검항목표에는 '해당 없음'에 체크 바람
다만, 법령 상 규정 등에도 불구하고 동의 받는 경우에는 '양호'에 체크 바람

※ 고유식별정보, 민감정보의 경우 법령 상 제공하여 처리할 수 있는 규정이 있는 경우 동의 없이 제공 가능하며, 그렇지 않은 경우에는 동의 받고 제공할 수 있음
다만, 고유식별정보 중 주민등록번호는 법령 규정 외에는 처리 할 수 없음

8. 정보주체 동의 시 필수 고지항목(5개) 고지 여부

❍ 온·오프라인 회원 가입 서식 또는 각종 서식을 통해 수집한 개인정보를 제3자에게 제공하는 경우 필수 고지항목(5개)을 고지하고 동의를 받는지 여부를 확인

< 동의 여부 획득 시 필수 고지사항 >

① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

☞ **홈페이지에서 제공 동의 획득 시 ⑤번에 대한 고지 없이 동의 받는 사례 있음**

9. 필수 고지항목(5개) 내용의 적정 여부

❍ 온·오프라인 회원 가입 서식과 홈페이지 게시판, 기타 서식을 통해 개인정보 제3자 제공의 동의 획득 시 고지하는 항목(5)의 적정 여부를 확인

- 개인정보를 제공받는 자가 모두 포함되어 있는지 여부 확인
- 제공받는 자의 개인정보 이용목적이 적정한지 여부 확인
- 제공하려는 개인정보의 항목과 제공받는 자의 보유 및 이용기간 설정이 이용 목적 달성을 위해 불가피하게 설정되었는지 여부
- 동의 거부 시 불이익 사항을 적시 하는 경우 그 적정성 확인

※ 법령 상 규정 또는 의무 이행을 위해 제공하는 경우 동의 획득하지 않고 제공할 수 있음, 다만, 법령에서 정한 목적 및 범위 내에서만 처리해야하며, 제공하는 사항에 대해 개인정보처리방침을 통해 공개해야 함

☞ **법령 상 정한 목적 및 범위를 초과하여 이용제공 하는 경우 처벌 받을 수 있음**

4 개인정보의 이용·제공 제한(법 제18조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제18조(개인정보의 이용·제공 제한)	10. 개인정보 수집 당시 정보주체의 이용·제공 동의 범위를 초과하여 이용·제공 여부			
	11. 개인정보 제공 시 제공 목적범위 내 이용, 안전조치 실시, 목적 달성 후 파기 등 요청 여부			
	12. 동의에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개*) 고지 여부			
	13. 필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

10. 개인정보 수집 당시 정보주체의 이용·제공 동의 범위를 초과하여 이용·제공 여부

❍ 온·오프라인 회원 가입 또는 기타 서식을 통해 개인정보 수집 시 획득한 동의 범위를 초과하여 이용하거나, 제3자에게 제공하는 경우 확인

- 최초 동의 획득 시 이용·제공의 목적, 항목 등을 초과하여 다른 목적으로 이용하거나, 제공하는 경우가 있는지 확인

11. 개인정보 제공 시 제공 목적범위 내 이용, 안전 조치 실시, 목적 달성 후 파기 등 요청 여부

❍ 목적 외의 용도로 법 제18조 2항에 따라 제3자에게 제공하는 경우 제공받는 자에게 제공받은 개인정보를 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하여야 하며,

- 안전성 확보를 위해 필요한 구체적인 조치를 마련하도록 문서로 요청해야하며, 목적 외로 제공된 개인정보의 목적달성 또는 보유기간 경과 후 파기 여부 등도 문서로 확인 받고 있는지 확인

※ 당초 목적 범위 내로 제3자에게 제공한 경우에는 해당하지 않음

12. 동의에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개) 고지 여부

❍ 정보주체의 동의에 의한 목적 외 이용 및 제3자 제공 시 필수 고지항목(5개)을 고지하고 동의 받는지 여부를 확인

< 동의 여부 획득 시 필수 고지사항 >

① 개인정보를 제공받는 자
② 개인정보의 이용목적(제공 시 제공받는 자의 개인정보 이용 목적)
③ 이용 또는 제공하는 개인정보의 항목
④ 개인정보의 보유 및 이용기간(제공 시 제공 받는 자의 보유 및 이용 기간)
⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

13. 필수 고지항목(5개) 내용의 적정 여부

❍ 목적 외 자체 이용 또는 제3자 제공을 목적으로 동의 획득 시 필수 고지하는 항목(5)의 적정 여부를 확인

- 개인정보를 제공받는 자가 모두 포함되어 있는지 여부 확인
- 제공받는 자의 개인정보 이용 목적이 적정한지 여부 확인
- 제공하려는 개인정보의 항목과 제공받는 자의 보유 및 이용기간 설정이 이용 목적 달성을 위해 불가피하게 설정되었는지 여부
- 동의 거부 시 불이익 사항을 적시 하는 경우 그 적정성 확인

5 개인정보의 파기(법 제21조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제21조(개인정보의 파기)	14. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부			
	15. 개인정보 파기 시 복구 또는 재생되지 않도록 조치 여부			
	16. 임시파일 및 출력자료 등에 대한 즉시 파기 여부			
	17. 법령에 따라 보존할 경우 별도 분리 보관 여부			

□ 점검 방법 및 평가 기준

14. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부

❍ 온·오프라인 회원 가입 또는 기타 서식을 통해 수집하여 보유하고 있는 개인정보(파일)의 당초 수집목적이 달성되었거나, 보유기간이 경과된 경우에는 지체 없이(보유기간 종료일로부터 5일 이내) 파기하는지 여부 확인

- 다만, 법령에 따라 보존하여야 하는 경우에는 보존 할 수 있음

※ 법령에 따라 보존 필요 시 기존 개인정보(파일)과 분리하여 보관하여야 함

☞ **수집 목적이 달성되고, 보유기간이 경과된 후에도 보관 중인 경우 다수 사례 있음**

15. 개인정보 파기 시 복구 또는 재생되지 않도록 조치 여부

❍ 개인정보(파일)의 당초 수집목적이 달성되었거나, 보유기간이 경과되어 파기 시 복원이 불가능한 방법으로 영구 삭제했는지 여부 확인

- 기록물, 인쇄물, 서면 등의 경우 파쇄 또는 소각 여부 확인 필요

16. 임시파일 및 출력자료 등에 대한 즉시 파기 여부

❍ 업무 수행 상 보존 필요성은 없으나, 임시적으로 생성된 파일이나 출력 자료를 사용 후 즉시 파기하는지 여부 확인

17. 법령에 따라 보존할 경우 별도 분리 보관 여부

❍ 다른 법령에 따라 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하는지 여부 확인

- 접근권한은 소송 담당자 등 필수 요원으로 접근권한을 엄격히 제한 필요

☞ **법령에 따라 분리 보관한다는 의미는 소송, 민원 등 특정한 상황이 아니면 접근할 필요가 없다는 것이며, 파기 시 삭제하지 않고 단순히 테이블 필드에 플래그 형태로 남기는 사례 있음**

6 동의를 받는 방법(법 제22조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제22조(동의를 받는 방법)	18. 동의 사항의 구분 동의 여부			
	19. 동의가 필요한 정보와 동의 없이 처리할 수 있는 정보의 구분 동의 여부			
	20. 홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부			
	21. 선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부			

□ 점검 방법 및 평가 기준

18. 동의 사항의 구분 동의 여부

❍ 동의의 내용과 의미를 명확하게 인지한 상태에서 동의 여부를 결정할 수 있도록 통상의 동의와 구분해서 동의 받고 있는지 여부 확인

< 구분 동의가 필요한 경우 >

① 개인정보의 수집·이용 동의(제15조 제1항 제1호)
② 제3제 제공 동의(제17조 제1항 제1호)
③ 국외 제3자 제공 동의(제17조 제3항)
④ 목적 외 이용·제공 동의(제18조 제2항 제1호)
⑤ 마케팅 목적 처리 동의(제22조 제3항)
⑥ 법정대리인의 동의(제22조 제5항)
⑦ 민감정보의 처리 동의(제23조 제1항 제1호)
⑧ 고유식별정보 처리 동의(제24조 제1항 제1호)

☞ **고유식별정보, 마케팅 정보 동의 시 구분동의 받지 않고 일괄 동의 사례 다수 있음**

19. 동의가 필요한 정보와 동의 없이 처리할 수 있는 정보의 구분 동의 여부

❍ 정보주체의 동의가 필요 없는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하는지 확인

< 동의가 필요 없는 개인정보 >

① 계약의 체결 및 이행을 위해 필수적인 정보 ② 급박한 생명·신체·재산상 이익보호를 위해 필요한 정보 ③ 법령상 의무 준수를 위해 불가피한 정보 ④ 개인정보처리자의 정당한 이익을 위해 필요한 정보 등

- 고유식별정보 및 민감정보의 경우에는 계약의 체결 이행 등을 위해 필요하다고 해도 제24조, 제23조에 의거, 별도 동의 받거나 관련 법령에 의해 처리를 허용하고 있는지 여부 확인

- 개인정보처리자가 자신의 정당한 이익을 위해 동의 없이 처리한 경우 개인정보처리자가 이를 입증*할 수 있는지 확인

* 동의 없이 처리할 수 있는 개인정보라는 입증은 개인정보처리자가 해야하며, 입증하지 못하는 경우 동의 받지 않고 수집하는 것으로 처벌될 수 있음

※ 대부분 기관에서 동의 없이 수집 가능한 경우에도 추후 분쟁 등을 피하거나, 법령상 목적 외에 부가적인 목적 달성을 위해 필수사항에 포함하여 동의를 받고 있음

20. 홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부

❍ 재화나 서비스를 홍보하거나 판매를 권유하기 위한 동의 획득 시 일반적인 개인정보 동의 여부와 구분하고 있는지 확인

☞ **홈페이지 회원 가입 시 수집목적에 '신재품 소개 및 안내' 등 홍보 목적의 동의를 구분하지 않고 일괄 동의 받는 사례 있음(※ 동의 받고, 실제 홍보하지 않는 경우가 많음)**

21. 선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부

❍ 선택정보를 수집하거나, 홍보 권유를 위한 개인정보 동의에 대해 미동의 이유로 홈페이지 회원 가입 등 기본적인 재화 또는 서비스 제공을 거부하고 있는지 확인

< 기본적인 서비스 제공과 관계없는 동의 사항 >

① 선택정보의 처리에 대한 동의
② 직접 마케팅에 대한 동의
③ 목적외 이용·제공에 대한 동의

☞ **홈페이지에서 마케팅 목적 또는 선택정보 미동의시 회원가입이 안되는 사례 있음**

7 민감정보의 처리 제한(법 제23조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제23조(민감정보의 처리 제한)	22. 사상, 정치, 건강 등 민감정보의 동의에 의한 수집 및 제공 시 구분 동의 여부			
	23. 정보주체 동의 시 필수 고지항목(수집 4개, 제공 5개) 고지 여부			
	24. 필수 고지항목(4개 또는 5개) 내용의 적정 여부			

□ 점검 방법 및 평가 기준

22. 사상, 정치, 건강 등 민감정보의 동의에 의한 수집 및 제공 시 구분 동의 여부

❍ 민감정보를 수집 및 제공 시 일반적인 개인정보의 처리 동의와 구분하여 별도 동의 받고 있는지 여부 확인

※ 법령의 특별한 규정에 따라 민감정보를 처리하는 경우 세부점검 항목에 '해당 없음' 표시

< 민감정보의 구분 >

① 사상·신념에 관한 정보 ② 노동조합·정당의 가입·탈퇴에 관한 정보 ③ 정치적 견해에 관한 정보 ④ 건강, 성생활에 관한 정보 ⑤ 유전자 검사 결과로 얻어진 유전정보 ⑥ 범죄경력자료에 해당하는 정보

23. 정보주체 동의 시 필수 고지항목(수집 4개, 제공 5개) 고지 여부

❍ 세부점검항목표 3번, 8번을 참고, 필수 고지사항(수집4, 제공5) 고지 여부

24. 필수 고지항목(4개 또는 5개) 내용의 적정 여부

❍ 세부점검항목표 4번, 9번을 참고, 필수 고지항목(수집4, 제공5) 적정 여부

8 고유식별정보의 처리 제한(법 제24조)

□ 세부점검항목(표)

분야 (해당 법 조항)	세부 점검 항목	양호	개선 필요	해당 없음
제24조(고유식별정보의 처리 제한)	25. 고유식별정보*의 동의에 의한 수집 및 제공 시 구분 동의 여부 * 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호			
	26. 주민등록번호 외 회원가입 방법 제공 여부			

□ 점검 방법 및 평가 기준

25. 고유식별정보의 동의에 의한 수집 및 제공 시 구분 동의 여부

❍ 고유식별정보를 수집 및 제공 시 일반적인 개인정보의 처리 동의와 구분하여 별도 동의 받고 있는지 여부 확인

※ 법령의 특별한 규정에 따라 고유식별정보를 처리하는 경우 세부점검 항목에 '해당 없음' 표시

< 고유식별정보 현황 >

① 주민등록번호* ② 여권번호 ③ 운전면허번호 ④ 외국인등록번호 * '14.8.7일 이후 법령 상 처리가 허용된 경우만 처리 할 수 있으며, 보유하고 있는 정보는 2년 이내 파기

26. 주민등록번호 외 회원가입 방법 제공 여부

❍ 공공기관 및 공공기관 외의 인터넷 홈페이지를 운영하는 자로 전년도말 기준 직전 3개월간 인터넷 홈페이지를 이용자 수가 하루 평균 1만명 이상인 경우

- 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(예: I-PIN, 공인인증서, 휴대전화 인증 등)을 제공하고 있는지 확인

9 업무위탁에 따른 처리 제한(법 제26조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제26조(업무위탁에 따른 처리 제한	27. 위탁 시 필수사항(7) 포함한 문서(계약서)에 의한 계약 여부 * 6개 : 목적외 처리금지, 기술 관리적 보호조치, 목적 범위, 재위탁 제한, 접근제한 등 안전조치, 관리·감독사항			
	28. 수탁자 공개 여부			
	29. 수탁자에 대한 교육 실시 여부			
	30. 처리현황 점검 등 수탁자 관리·감독 여부			

□ 점검 방법 및 평가 기준

27. 위탁 시 필수사항(7) 포함한 문서(계약서)에 의한 계약 여부

❍ 개인정보 처리에 관한 업무를 제3자에게 위탁하는 경우 필수사항(7)을 포함한 문서(계약서)에 의한 계약을 체결하는지 확인

- 보안 약정서, 협약서 등의 형태의 계약 부속서류라 하더라도 필수사항(7)이 모두 포함되어 있는 경우에는 인정됨

< 위탁계약 시 문서에 포함될 필수사항 >

① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
② 개인정보의 기술적·관리적 보호조치에 관한 사항
③ 위탁업무의 목적 및 범위
④ 재위탁 제한에 관한 사항
⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
⑦ 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

☞ **계약서에 비밀 누설 금지 등만 포함하고, 필수사항(7개)을 누락한 사례 다수 있음**

28. 수탁자 공개 여부

❍ 개인정보의 처리 업무를 위탁하는 경우 수탁자를 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하고 있는지 여부 확인

- 인터넷 홈페이지에 공개할 수 없는 경우 다른 방법으로 공개 필요

< 인터넷 홈페이지가 없는 경우 수탁자 공개 방법 >

① 사업장의 보기 쉬운 장소에 게시
② 관보 또는 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
③ 정보주체에게 배포하는 각종 소식지에 포함하여 연 2회 이상 발행
④ 계약서 등에 실어 발급하는 방법

☞ **수탁사를 누락하거나, 업무 단위로 묶어 개별 수탁사를 파악하기 어려운 사례 있음**

29. 수탁자에 대한 교육 실시 여부

❍ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하는지 확인

☞ **수탁사를 누락하거나, 업무 단위로 묶어 개별 수탁사를 파악하기 어려운 사례 있음**

30. 처리현황 점검 등 수탁자 관리·감독 여부

❍ 위탁자는 수탁자가 개인정보처리자로서 준수해야할 사항*과 문서(계약서) 포함된 필수사항**의 준수 여부를 관리·감독하는지 확인

* 개인정보 수집 시 적법한 동의 획득 여부, 목적 달성 후 파기 여부 등 법 준수사항

** 문서에 포함될 필수사항은 점검항목 27번의 표 참조

☞ **위탁기간이 종료되고, 처리된 개인정보가 실제 파기되었는지 여부 미확인 사례 있음**

10 개인정보 취급자에 대한 감독(법 제28조)

□ 세부점검항목(표)

분야 (해당 법 조항)	세부 점검 항목	양호	개선 필요	해당 없음
제28조(개인정보취급자에 대한 감독)	31. 개인정보취급자에 대한 관리·감독(접근권한 관리, 통제 등 포함) 여부			
	32. 개인정보취급자에 대한 보안서약서 징구 여부			
	33. 개인정보취급자에 대한 정기적인 교육 실시 여부			

□ 점검 방법 및 평가 기준

31. 개인정보취급자에 대한 관리·감독(접근권한 관리, 통제 등 포함) 여부

❍ 개인정보취급자(임직원, 파견·시간제근로자)의 개인정보처리시스템에 대한 접근권한을 업무의 성격에 따라 최소한의 범위로 차등 부여하는 등 접근권한을 관리·감독하고 있는지 확인

32. 개인정보취급자에 대한 보안서약서 징구 여부

❍ 개인정보취급자로 하여금 보안서약서를 징구하는지 여부 확인

33. 개인정보취급자에 대한 정기적인 교육 실시 여부

❍ 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하고 있는지 확인

☞ **임시직, 계약직 등에 대한 교육을 실시하지 않은 사례 있음**

11-1 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	내부관리계획 수립·시행	34. 내부관리계획 수립·시행 여부			
		35. 내부관리계획의 필수 반영사항(4개*) 포함 여부 * 4개 : 보호책임자 지정, 보호책임자/취급자의 역할·책임, 안전성 확보 조치, 취급자 교육			

□ 점검 방법 및 평가 기준

34. 내부관리계획 수립·시행 여부

❍ 개인정보의 안전한 처리를 위한 내부관리계획을 수립·시행하고 있는지 확인(단, 소상공인은 내부관리계획을 수립하지 아니할 수 있음)

- 내부관리계획이라는 명칭 이외의 다른 명칭(예: 개인정보보호정책 등)으로 수립하여도 점검항목 35의 사항이 모두 포함된 경우 내부관리계획으로 인정됨

< 소상공인 및 상시근로자 정의 >

▸ 소상공인 : 「소기업 및 소상공인 지원을 위한 특별조치법」 제2조제2호에 의거 '광업·제조업·건설업 및 운수업'의 경우 상시근로자의 수가 10인 미만인 사업자, 그 외의 업종인 경우 상시근로자 수가 5인 미만인 사업자를 말함

▸ 상시근로자 : 「중소기업기본법 시행령」 제4조 및 제5조에 의거, 근로자 중에서 '임원', '일용근로자', '3개월 이내의 기간을 정하여 근로하는자', '기초연구진흥 및 기술개발지원에 관한 법률' 제14조에 해당하는 기업부설연구소의 연구전담요원을 제외한 근로자

35. 내부관리계획의 필수 반영사항(4개) 포함 여부

❍ 내부관리계획을 수립 시 보호책임자 지정 등 필수사항(4)을 모두 반영하여 수립하였는지 확인

< 내부관리계획 필수 항목(4) >

① 개인정보 보호책임자 지정에 관한 사항
② 개인정보 보호책임자 및 개인정보취급자의 역할·책임에 관한 사항
③ 개인정보의 안전성 확보에 필요한 조치에 관한 사항
④ 개인정보취급자에 대한 교육에 관한 사항
⑤ 그 밖의 개인정보 보호를 위하여 필요한 사항(예: 개인정보파일 보유기간 등)

개인정보 내부관리계획 목차 (예시)

제1장 총칙
제1조(목적)
제2조(적용범위)
제3조(용어 정의)

제2장 내부관리계획의 수립 및 시행
제4조(내부관리계획의 수립 및 승인)
제5조(내부관리계획의 공표)

제3장 개인정보보호책임자의 의무와 책임
제6조(개인정보보호책임자의 지정)
제7조(개인정보보호책임자의 의무와 책임)
제8조(개인정보취급자의 범위 및 의무와 책임)

제4장 개인정보의 처리단계별 기술적·관리적 안전조치
제9조(개인정보취급자 접근 권한 관리 및 인증)
제10조(접근통제)
제11조(개인정보의 암호화)
제12조(접근기록의 위변조 방지)
제13조(보안프로그램의 설치 및 운영)
제14조(물리적 접근제한)

제5장 개인정보보호 교육

제6장 개인정보 침해대응 및 피해구제

11-2 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	접근권한 관리 및 접근통제	36. 시스템에 대한 접근권한을 필요 최소한의 범위로 업무 담당자에 따라 차등 부여 여부			
		37. 전보·퇴직 등 인사이동으로 취급자가 변경될 경우 접근권한 변경 또는 말소 여부			
		38. 접근권한의 부여·변경·말소 내역의 기록관리 및 최소 3년간 보관 여부			
		39. 취급자별로 개별 계정 발급 및 계정 미공유 여부			
		40. 안전한 비밀번호 작성규칙의 수립·적용 여부			
		41. 불법적 접근 및 침해사고 방지를 위한 시스템 설치·운영 여부			
		42. 외부에서 정보통신망을 통한 접속 시 가상사설망, 전용선 등 안전한 접속수단 제공 여부			
		43. P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단 실시 여부			
		44. 인터넷 홈페이지의 개인정보 노출 방지를 위한 보안조치 실시 여부			

□ 점검 방법 및 평가 기준

36. 시스템에 대한 접근권한을 필요 최소한의 범위로 업무 담당자에 따라 차등 부여 여부

❍ 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 확인

- 업무 성격에 따라 접근 권한의 팀별, 개인별 차등 부여 여부 확인

☞ **개발 초기 시 부여된 관리자 권한, 디폴트 권한 등으로 일괄 부여된 사례 있음**

37. 전보·퇴직 등 인사이동으로 취급자가 변경될 경우 접근권한 변경 또는 말소 여부

❍ 개인정보취급자의 전보 또는 퇴직 등 인사이동 발생 시 개인정보처리시스템의 접근권한을 즉시 변경 또는 말소하는지 확인

☞ **퇴직자의 계정을 삭제하지 않고 남겨 놓은 사례 있음**

38. 접근권한의 부여·변경·말소 내역의 기록관리 및 최소 3년간 보관 여부

❍ 개인정보취급자의 접근권한 부여 및 전보 또는 퇴직에 따른 변경, 말소에 대한 기록은 최소 3년간 보관하고 있는지 확인

※ 변경 이력을 시스템에 자동으로 남기지 않는 경우 수기로 작성, 관리 여부 확인

☞ **권한 변경 이력을 보관하지 않은 사례 있음**

39. 취급자별로 개별 계정 발급 여부

❍ 개인정보처리시스템에 접속 할 수 있는 사용자 계정을 발급하는 경우, 취급자 별로 한 개의 사용자 계정을 발급하는지 확인

- 사용자 계정(ID)을 다수의 사용자가 공유하는지 여부 확인

☞ **업무 편의상 하나의 계정(ID)을 다수의 사용자가 공유하는 사례 있음**

40. 안전한 비밀번호 작성규칙의 수립·적용 여부

❍ 개인정보취급자 또는 정부주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립·적용하는지 확인

※ 내부관리계획의 안전성확보 조치 사항으로 포함하여 작성 할 수 도 있으며, 별도 비밀번호 작성규칙을 작성하여 운영할 수 있음

☞ **비밀번호 작성규칙에 불구하고 취급자 등이 시스템 접속 시 반영하지 않은 사례 있음**

41. 불법적 접근 및 침해사고 방지를 위한 시스템 설치·운영 여부

❍ 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 접근통제시스템*을 설치 운영하는지 확인

* · 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는 시스템(방화벽 등)

· 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하는 시스템(IDS 또는 IPS 등)

☞ **웹호스팅 시 방화벽 등 보안장비 이용에 추가 비용이 들어 설치하지 않은 사례 있음**

42. 외부에서 정보통신망을 통한 접속 시 가상사설망, 전용선 등 안전한 접속수단 제공 여부

❍ 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 시 안전한 접속수단(가상사설망, 전용선 등)을 통해서만 접속하는지 확인

☞ **홈페이지 관리자페이지 접속 시 단순 ID/패스워드로만 접속 가능한 사례 있음**

43. P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단 실시 여부

❍ P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 PC에 조치를 취하고 있는지 확인

44. 인터넷 홈페이지의 개인정보 노출 방지를 위한 보안조치 실시 여부

❍ 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 PC에 조치를 취해야함

☞ **웹서버 설정이 미흡하여 게시판 등에 올린 개인정보가 구글 등에 노출되는 사례 있음**

11-3 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	개인정보의 암호화	45. 개인정보 암호화계획 수립·시행 여부			
		46. 비밀번호의 외부 송·수신 시 암호화 조치 여부			
		47. 비밀번호의 내부 저장 시 일방향 암호화 조치 여부			
		48. 바이오정보의 외부 송·수신 시 암호화 조치 여부			
		49. 바이오정보의 내부 저장 시 암호화 조치 여부			
		50. 고유식별정보의 외부 송·수신 시 암호화 조치 여부			
		51. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 암호화 조치 여부			
		52. 고유식별정보의 내부 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부			

□ 점검 방법 및 평가 기준

45. 개인정보 암호화계획 수립·시행 여부

❍ 고유식별정보, 비밀번호, 바이오정보 등이 포함된 개인정보처리 시스템을 운영하는 경우 암호화 계획을 수립하여 시행했는지 확인

46. 비밀번호의 외부 송·수신 시 암호화 조치 여부

❍ 비밀번호를 홈페이지 회원 가입, 로그인 및 개인정보 변경 시 정보통신망을 통해 송·수신하는 경우 암호화하는지 확인

※ SSL 보안서버 구축을 하였으나, 실제 페이지의 소스 수정을 하지 않아 전송 시 암호화되지 않는 경우도 있어 실제 확인 필요

☞ **wire shark 등 프로그램을 통해 전송되는 패킷의 암호화 검사 시 암호화하지 않은 사례 있음**

47. 비밀번호의 내부 저장 시 일방향 암호화 조치 여부

❍ 홈페이지를 포함한 개인정보처리시스템 사용자의 비밀번호는 복호화 되지 아니하도록 일방향 암호화(해시함수)하여 저장하는지 확인

- 일방향 암호화 여부, 안전한 알고리즘으로 암호화 여부 등은 DB쿼리 결과, 암호화 솔루션 및 암호 알고리즘 등을 확인

☞ **안전하지 않은 알고리즘(MD5, SHA-1, 자체 함수제작 등) 및 양방향 암호화 방식으로 암호화한 사례 있음**

48. 바이오정보의 외부 송·수신 시 암호화 조치 여부

❍ 바이오정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하는지 확인

49. 바이오정보의 내부 저장 시 암호화 조치 여부

❍ 바이오정보를 개인정보처리시스템 및 PC 저장 시 암호화하는지 확인

50. 고유식별정보의 외부 송·수신 시 암호화 조치 여부

❍ 고유식별정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통해 전달하는 경우에는 이를 암호화하는지 확인

- 특히, 홈페이지 실명확인 및 회원가입 시 전송하는 고유식별정보를 암호화하여 전송하는지 확인

- 또한, USB 등 각종 매체를 통해 전달하거나, 이메일 등에 첨부파일로 전송하는 경우에도 응용프로그램에서 제공하는 암호화 등을 적용하여 전송하고 있는지 확인

☞ **고유식별정보가 첨부파일에 포함된 이메일 전송 시 암호화하지 않고 전송한 사례 있음**

51. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 암호화 조치 여부

❍ 고유식별정보를 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ)에 저장하는 경우 암호화하여 저장하는지 확인

52. 고유식별정보의 내부 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부

❍ 내부망에 고유식별정보를 저장하는 경우에는 암호화의 적용여부 및 적용범위를 정하여 시행하고 있는지 확인

- 영향평가 대상이 되는 공공기관의 경우 개인정보영향평가의 결과에 따라 암호화 적용여부 및 범위를 정할 수 있음

- 영향평가 대상이 되는 공공기관의 경우를 제외하고는 위험도 분석에 따른 결과에 따라 암호화 적용여부 및 범위를 정함

< 개인정보 영향평가의 대상 >

① 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일

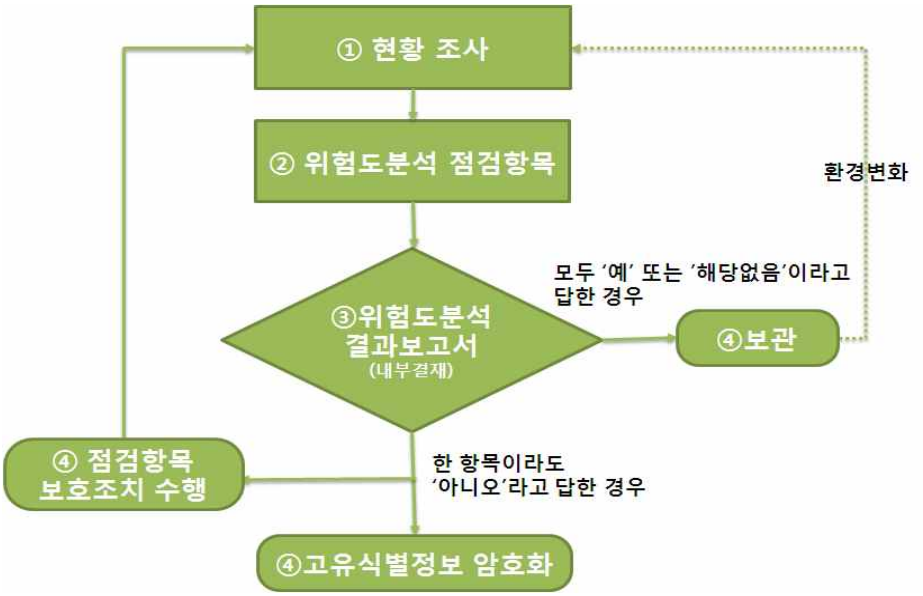
② 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일

③ 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일

④ 법 제33조 제1항에 따른 개인정보영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일

< 위험도 분석 절차 및 내용 >

① 위험도 분석을 위해 개인정보 파일 및 고유식별정보 보유 여부 등 현황조사
② 개인정보 파일단위별로 위험도 분석 항목별 점검을 수행
③ 위험도 분석 결과보고서를 작성하여 내부결재 후 보관
④ 점검 결과에 따라 고유식별정보 암호화 등을 수행



구 분	점 검 항 목
DB 및 Application 기반	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?
	13. DB서버 내에 불필요한 서비스 포트를 차단하고 있습니까?
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?
	15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?
	16. DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사이동 발생 시 지체 없이 DB 접근권한을 변경하고 있습니까?
	19. DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?
	20. DB접속자 및 개인정보취급자의 비밀번호 입력 시 5회 이상 연속 입력오류가 발생한 경우 계정 잠금 등 접근을 제한하고 있습니까?
	21. DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?
	22. DB 및 DB접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용 시 관리자 승인 후 사용하고 있습니까?
	23. DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?
	24. HDD등 DB 저장매체의 불용 처리 시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?
웹(Web) 기반 ※웹사이트 운영시	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?

11-4 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	접속기록의 보관	53. 취급자의 접속기록을 최소 6개월 이상 보관·관리 여부			
		54. 접속기록의 항목(4개*)이 적정한지 여부 * 4개 : ID, 날짜 및 시간, 접속자 IP 주소, 수행 업무(열람, 수정, 삭제, 인쇄, 입력 등)			
		55. 접속기록이 위·변조 및 도난, 분실되지 않도록 접속기록의 안전하게 보관 여부			

□ 점검 방법 및 평가 기준

53. 취급자의 접속기록을 최소 6개월 이상 보관·관리 여부

❍ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하고 있는지 확인

☞ **홈페이지 관리자 페이지 접속 시 접속 기록을 남기지 않은 사례 있음**

54. 접속기록의 항목(4개)이 적정한지 여부

❍ 개인정보처리시스템에 접속 시 필수항목(4)을 남기는지 확인

< 접속기록에 포함되어야 할 필수 항목 >

필수 기록 항목	설 명
① ID	개인정보취급자 식별 정보
② 날짜 및 시간	접속 일시
③ 접속자 IP 주소	접속지 정보
④ 수행 업무	열람, 수정, 삭제, 입력, 인쇄 등

※ 개인정보취급자 1명(Root, Admin 등)이 개인정보처리시스템을 관리하는 경우, 전자적 로그를 남기지 않고, 접속 기록을 수기로 작성하여 상급자의 승인을 받아도 가능

55. 접속기록이 위·변조 및 도난, 분실되지 않도록 접속기록의 안전하게 보관 여부

❍ 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관하고 있는지 확인

- 접속기록에 대한 위·변조를 방지하기 위해 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직함

- 접속기록을 수정 가능한 매체(HDD 또는 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리할 수 있음

11-5 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	보안프로그램 설치·운영	56. 보안 프로그램의 설치·운영 여부			
		57. 보안 프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부			

□ 점검 방법 및 평가 기준

56. 보안 프로그램의 설치·운영 여부

❍ 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하고 있는지 확인

57. 보안 프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부

❍ 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하고 있는지 확인

- 악성 프로그램관련 경보가 발령된 경우
- 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 업데이트를 하고 있는지 확인

☞ **백신프로그램 업데이트 및 OS 최신 패치 확인 시 업데이트를 미실시하는 사례 있음**

11-6 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	물리적 접근 방지	58. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 수립·운영 여부			
		59. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부			

□ 점검 방법 및 평가 기준

58. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 수립·운영 여부

❍ 전산실·자료보관실을 별도로 두고 있는 경우에는 비인가자의 접근으로 인한 개인정보의 절도, 파괴 등의 물리적 위협으로부터 정보자산을 보호하기 위해 출입통제 절차를 수립하는지 확인

- 비밀번호 기반 출입통제 장치, 스마트카드 기반 출입 통제장치 등 물리적 접근통제 장치를 설치·운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하고 있는지 확인

59. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부

❍ 개인정보가 포함된 서류나 보조기억매체(USB, CD 등) 등은 잠금장치가 부착되어 있는 금고 또는 잠금장치가 있는 캐비넷 등에 안전하게 보관하고 있는지 확인

☞ **개인정보가 포함된 서류 등을 캐비넷에 보관하지 않고 책상에 방치하는 사례 있음**

12 개인정보 처리방침의 수립·공개 (법 제30조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제30조(개인정보 처리 방침의 수립·공개)	60. 개인정보 처리방침의 수립 여부			
	61. 개인정보 처리방침에 필수 항목(8개*) 포함 여부 * 8개 : 처리 목적, 처리 및 보유기간, 제3자 제공 사항(해당 시), 위탁 사항(해당 시), 정보주체 권리 의무 및 행사 방법, 처리항목, 파기 사항, 안전성 확보 조치 사항			
	62. 개인정보 처리방침의 홈페이지 등 공개 여부			

□ 점검 방법 및 평가 기준

60. 개인정보 처리방침의 수립 여부

❍ 개인정보 처리에 관한 '개인정보처리방침'을 수립하고 있는지 확인

61. 개인정보 처리방침에 필수 항목(8개) 포함 여부

❍ 개인정보처리방침 공개 시 필수 항목을 포함하여 공개하는지 확인

< 개인정보처리 방침 필수 항목 >

① 개인정보의 처리 목적	② 개인정보의 처리 및 보유 기간
③ 개인정보의 제3자 제공에 관한 사항	④ 개인정보 처리의 위탁에 관한 사항
⑤ 정보주체의 권리·의무 및 행사방법에 관한 사항	
⑥ 처리하는 개인정보의 항목	⑦ 개인정보의 파기에 관한 사항
⑧ 안전성 확보 조치에 관한 사항	

62. 개인정보 처리방침의 홈페이지 등 공개 여부

❍ '개인정보처리방침'을 홈페이지에 공개해고 있는지, 홈페이지가 없는 경우 사업장의 보기 쉬운 장소에 게시하는 방식 등으로 공개하는지 확인

13 개인정보 보호책임자의 지정 (법 제31조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제31조(개인정보 보호 책임자의 지정)	63. 개인정보 보호책임자 지정 여부			
	64. 개인정보 보호책임자의 업무 범위, 자격요건 등 적정 여부			

□ 점검 방법 및 평가 기준

63. 개인정보 보호책임자 지정 여부

❍ 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호 책임자를 지정하고 있는지 확인

- 공공기관이 아닌 사업주는 대표자, 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람을 개인정보 보호책임자로 지정하고 있는지 확인

- 공공기관은 다음의 자격 요건에 맞게 지정하고 있는지 확인

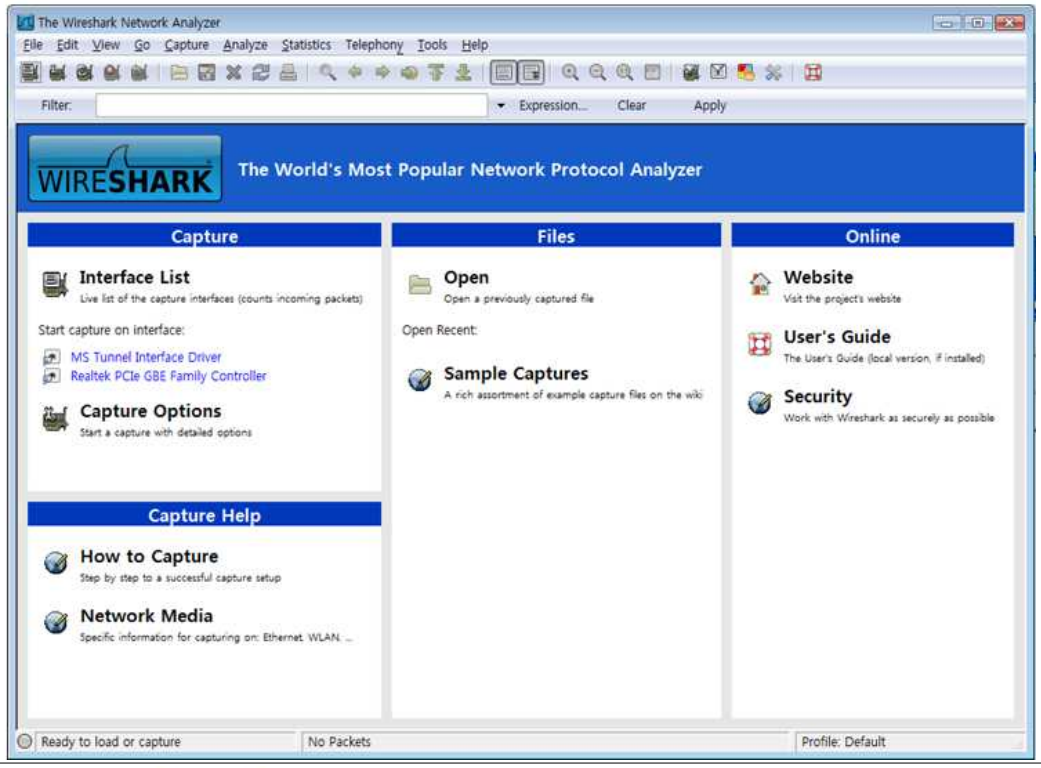
< 공공기관 개인정보보호책임자 자격 요건 >

공공 기관		자격 요건
①	국회, 법원, 헌법재판소, 중앙선관위, 중앙행정기관	고위공무원단
②	① 외 정무직공무원을 장으로 하는 국가기관	3급 이상 공무원
③	①, ② 외 고위·3급 공무원을 장으로 하는 국가기관	4급 이상 공무원
④	①~③ 외의 국가기관	개인정보 처리 업무 담당 부서장
⑤	시·도 및 시·도 교육청	3급 이상 공무원
⑥	시·군· 및 자치구	4급 이상 공무원
⑦	각급 학교	행정사무 총괄자
⑧	①~⑦ 외 공공기관	개인정보 처리 업무 담당 부서장

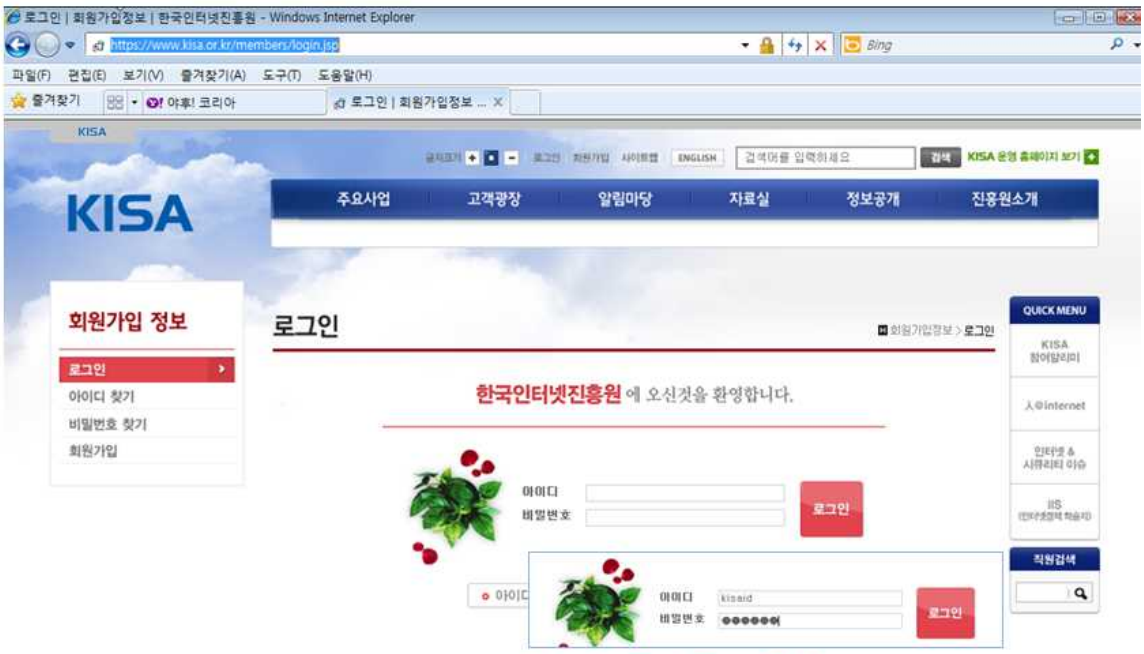
붙임 네트워크 전송 구간 암호화 여부 검사 방법(wireshark 사용법)

※ WireShark 프로그램은 프리웨어로 인터넷에 검색하여 설치 할 수 있음

① WireShark 구동

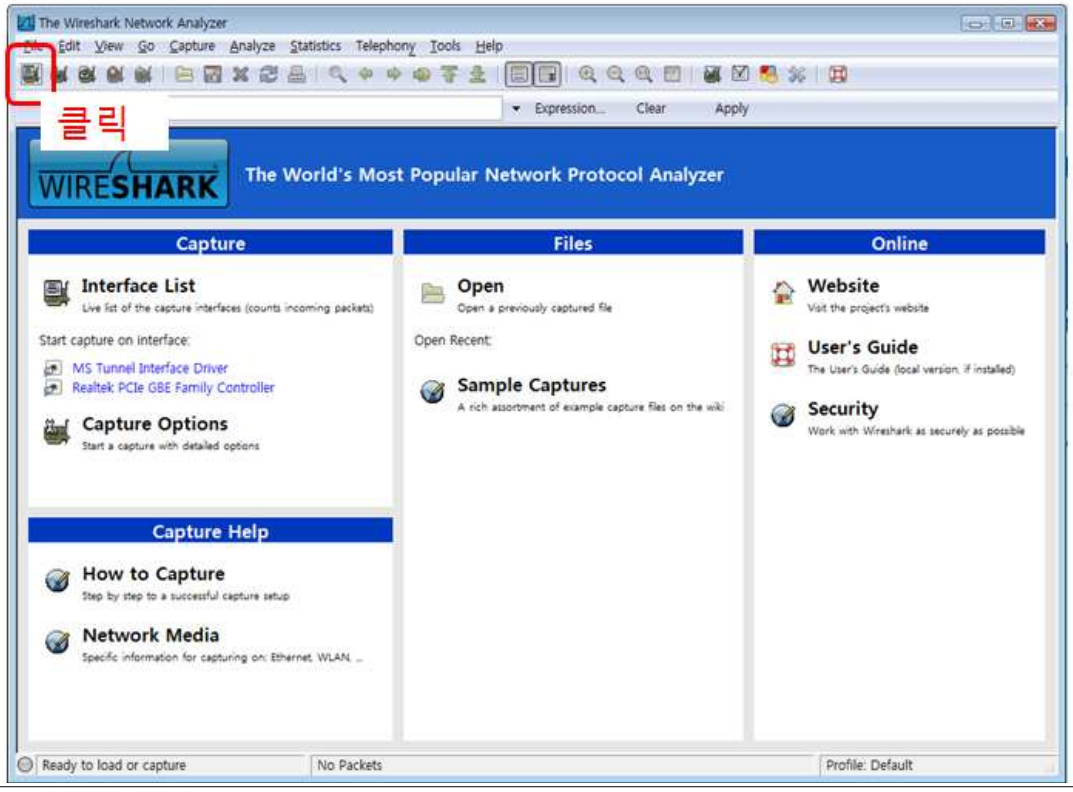


② 점검대상 웹페이지 접속(ex: https://www.kisa.or.kr/members/login.jsp)

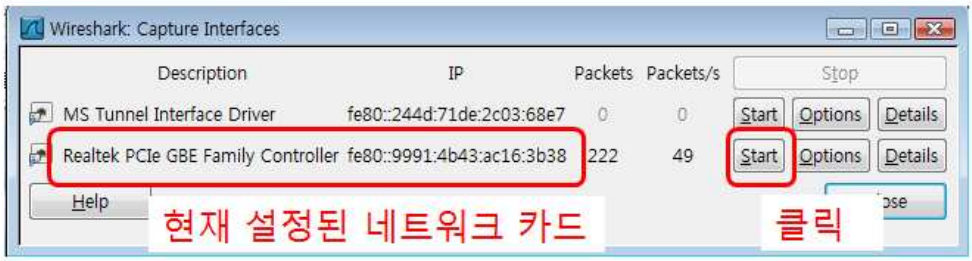


③ 암호화 필요정보 입력
(ex: ID는 kisaid, PW는 kisapw)

③ 패킷캡쳐 인터페이스 설정



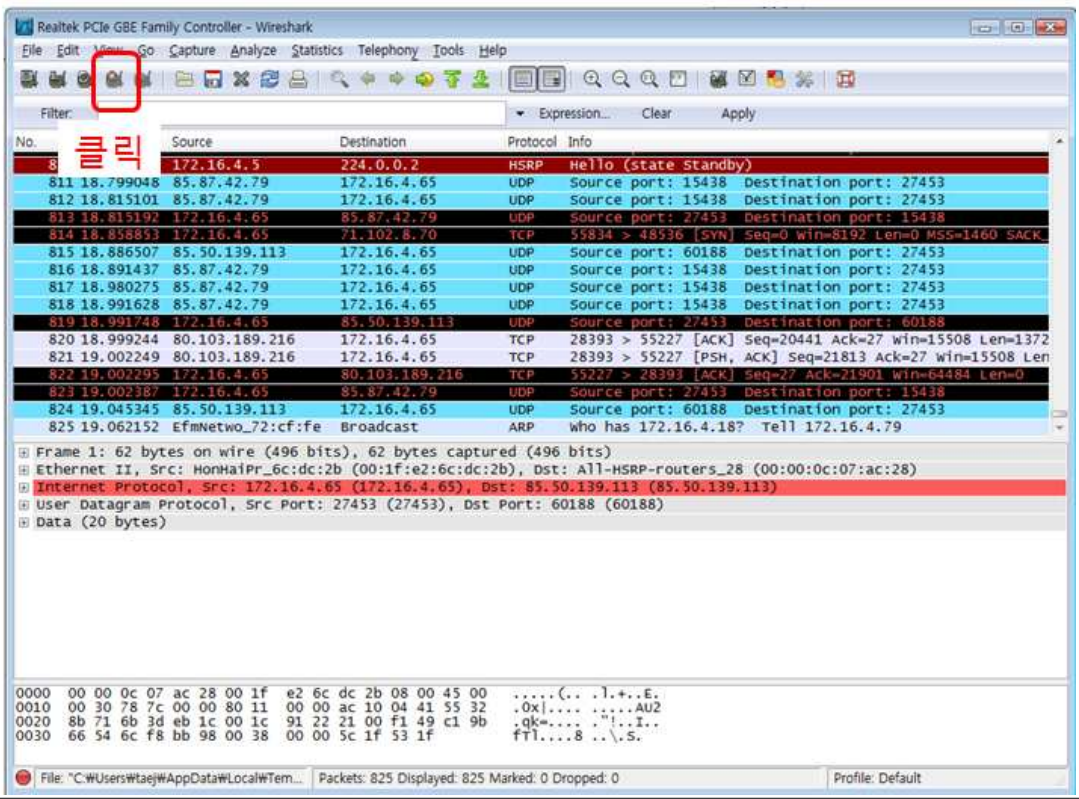
④ 패킷캡쳐 시작



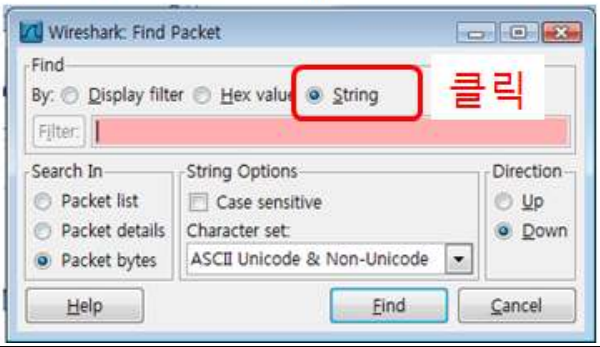
※ packets/s의 수치가 증가하는 것이 현재 설정된 네트워크 카드임

⑤ 점검대상 웹페이지에서 패킷발송(ex: 로그인 버튼 클릭)

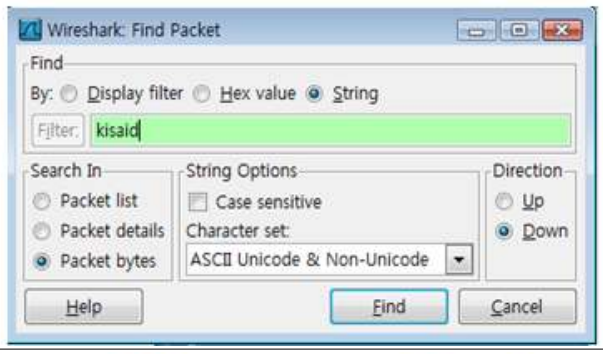
⑥ 캡쳐된 패킷을 확인 (ex: 로그인 버튼 클릭)



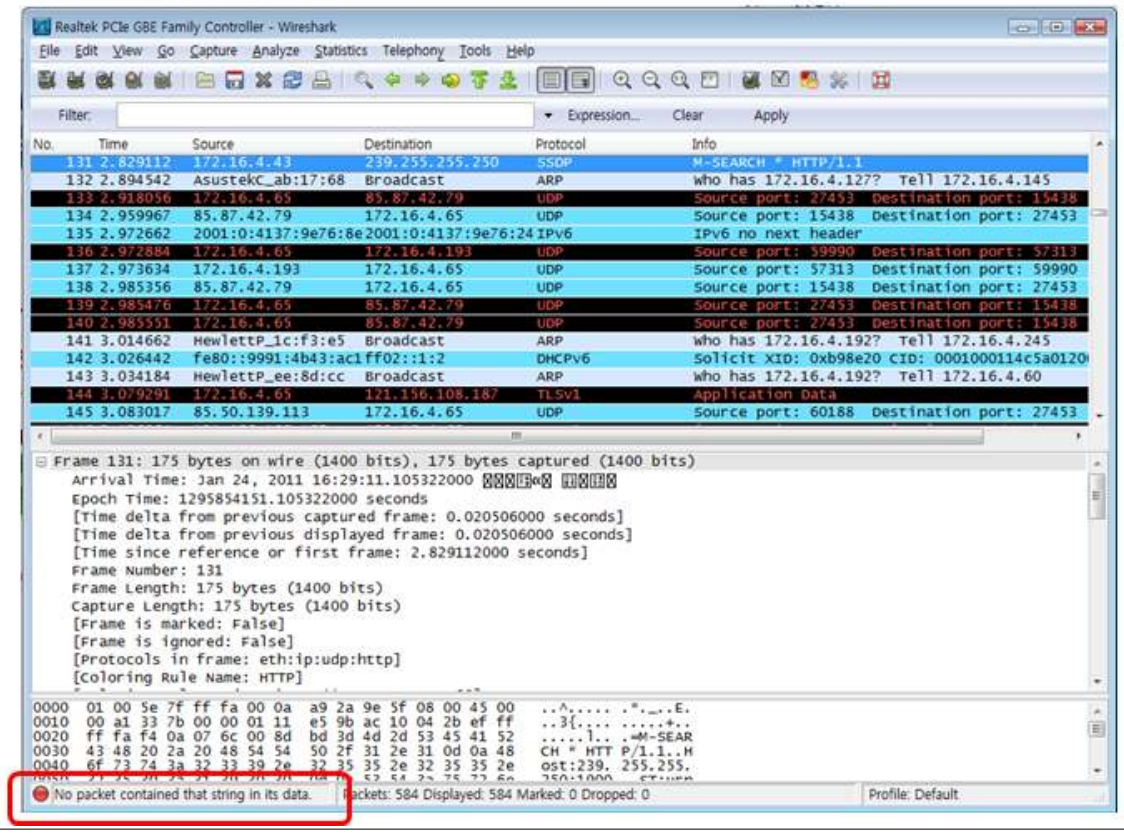
⑦ 캡쳐된 패킷의 확인화면(⑦)에서 단축키 Ctrl + F 클릭



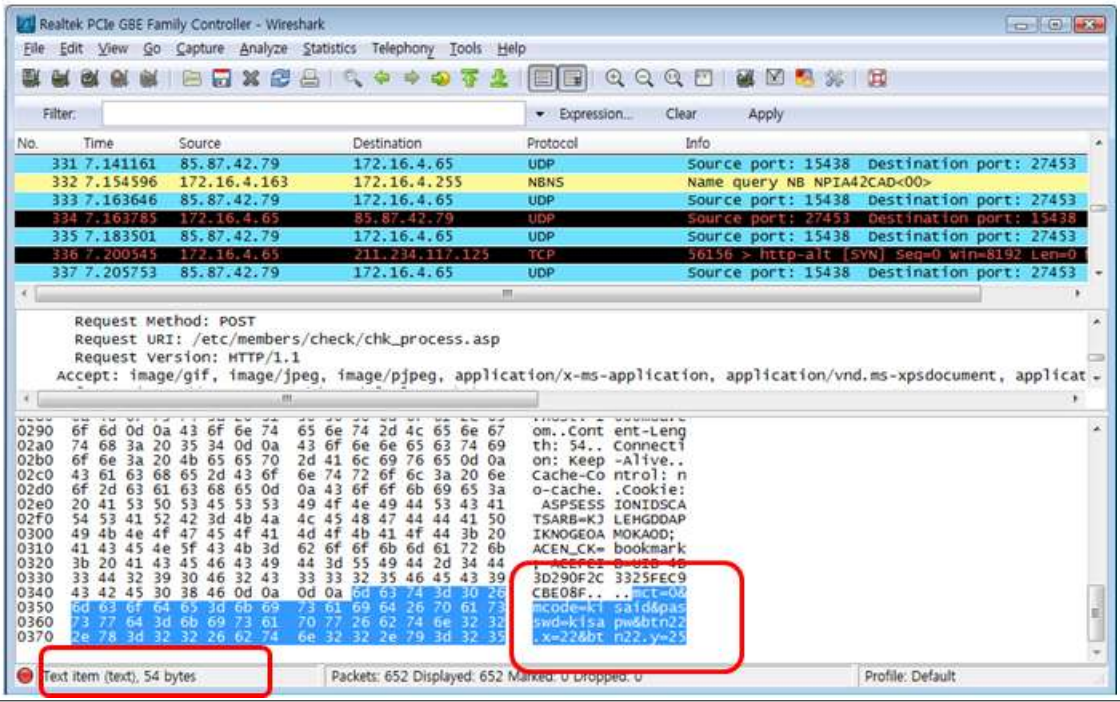
⑧ 암호화 필요 정보 입력 (③의 문자열 입력)



⑨ 암호화 된 정보는 검색이 되질 않음을 확인



⑩ 암호화가 되지 않은 경우 ID(kisaid), PW(kisapw) 확인 가능

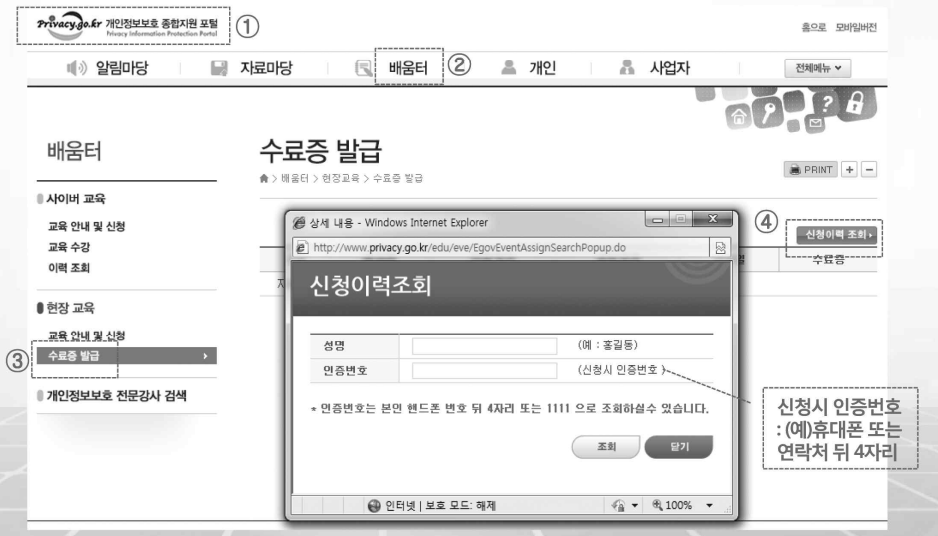


교육 수료증 발급 안내

- 교육신청 및 상시학습 인정(※ 별도 수료통보 없음)
- 수료증 출력 방법
  - 개인정보보호 종합지원 포털(privacy.go.kr) >> 배움터 >> 현장교육 >> 수료증 발급

※ 주의사항 : '신청이력조회' 시 인증번호는 현장교육 신청 시 등록 인증번호 입력

(예 : 휴대폰 또는 연락처 뒤 4자리)



- 문의처(개인정보보호 종합지원 포털) : 02) 2100 – 3343, 3344

메모

메모

메모