

기업의 정보보호 통제항목 간 결함발생 영향분석 및 심각도 측정 연구	
1	<div> <div>요약</div> <p>기존의 정보보호수준측정 방법론의 한계를 개선하기 위해서 선행 연구들의 면밀한 고찰을 통해 기업의 수준 측정항목, 측정항목의 결함 영향도, 객관적 가중치 산정 근거 등 수준측정 항목 및 방법론의 객관적이고 실증적인 방법을 모색하고 정책수립 시 기초자료로 활용하기 위해 분석함</p> <p>기업의 정보보호 수준측정을 위해 통계적 기법과 Case-Control 기법을 활용한 계층분석법을 적용하려 K-ISMS 보안통제항목의 결함중심의 위험도 및 가중치를 산정하고 검증함</p> </div> <div> <div>결론</div> <p>정보보호 수준측정에 용이하고, 적합한 방법을 찾고, 실용적 접근방법 측면에서 기업의 보안수준 측정방식을 일정 기준선의 합격 여부에서 결함 위험도 중심의 수준측정 방법론 제시함</p> <p>이로 인해 국내 정보보호 인증제도 통합, 분야별 인증기준 신설 및 개정 등 정보보호정책수립과 집행을 위한 객관적 근거자료로 활용 가능</p> </div> <div> <div>키워드</div> <p>ISMS / 보안 결함 심각도 측정 / 정보보호수준측정</p> </div>
효율적인 개인정보관리체계(PIMS) 인증제도 도입방안 연구	
2	<div> <div>요약</div> <p>국내 정보보호관리체계 인증제도(ISMS), ePrivacy, PIA제도와 PIMS의 중복성을 연구하고, 중복성 해소방안 제시</p> <p>또한 ISMS와 PIMS의 중복성을 제거하는 심사항목의 모듈화 방안을 제안하고, 이를 적용한 새로운 PIMS 인증체계 제시</p> </div> <div> <div>결론</div> <p>중복성과 유사성 개념 고찰과 제도적 중복과 방법론적 중복의 개념정의를 기반으로 두 인증제도간의 중복성을 평가하기 위한 방법론 제시, 중복평가 수행 후 새로운 PIMS 인증체계 방안 제시</p> <p>이로 인해 조직은 보다 효율적으로 정보보호와 개인정보관리 활동을 수행할 수 있고, 비용-효과적이고 차별화된 인증제도 도입이 가능함</p> </div> <div> <div>키워드</div> <p>ISMS / PISMS / 정보보호 중복성 해소</p> </div>
소기업에 특화된 정보보호 점검 항목에 관한 연구 (중소기업의 업종과 규모를 중심으로)	
3	<div> <div>요약</div> <p>전문적인 정보보호 인력 및 솔루션을 도입하기 어려운 실정의 소규모 기업의 정보보호 인식 수준 상향을 위한 가이드를 제시하고, 적용 가능한 최소의 정보보호 항목만을 도출하는 것을 목표로함</p> <p>정보보호를 수행하기 어려운 점으로 조사된 항목을 주요 문제점으로 선별하고, 그 문제점을 해결하기 위한 방안으로 정보보호관리체계, 개인정보관리체계 그리고 정보보호준비도 평가의 평가항목을 비교 분석하여 중복되는 항목을 추출함</p> <p>추출된 항목의 실효성 검증을 위해 국내 중소기업에 종사하는 임직원 및 경영자를 대상으로 설문조사를 실시하여 최종적인 관리 항목 도출</p> <p>소기업 기준 최소점검항목으로 최종 20개 항목을 도출하였고, '최소 점검 모듈'이라는 개념 제안</p> </div>

	결론	중소기업 보안의 문제점에 대한 해결 방안을 모색하고, 중소기업의 정보보호 애로사항 중 비용과 인력 그리고 정보보호에 대한 지식이나 수행방법의 부재에 대한 해결방안으로 비용 발생을 최소화하고, 자체인력으로 수행할 수 있는 점검항목 도출
	키워드	ISMS / 소기업 특화 정보보호 / 정보보호 점검 항목 타당성 조사
4	중소기업에 적합한 정보보안관리체계	
	요약	국내외의 대표적인 정보보호 인증제도인 K-ISMS, ISO27001 두 개의 인증 제도를 비교 분석하고, 분속한 정보를 통해 문제점 도출하고, 이를 개선하고자 중소기업에 적합한 정보보호 인증 제도인 L-ISMS를 설계 제안하고, 새로운 인증 제도를 통해 기존 인증제
	결론	새로운 인증제도를 통해서 관리적, 재무적 측면에서 큰 이점을 확보하며 기존 정보보호 인증 제도의 장점을 계승하여 정보보호의 기밀성, 무결성, 가용성을 유지
	키워드	ISMS / 정보보호 인증제도 비교 분석 / 정보보호수준평가
5	정보보호 관리체계와 개인정보보호 관리체계 인증제도의 효과적인 운영방안	
	요약	정보보호 관리체계와 개인정보보호 관리체계를 동시에 운영 할 수 있는 여러 가지 운영방안을 제시하고, 각 운영 방안별로 소요되는 비용과 통제항목을 비교하여 가장 효율적인 인증제도의 운영방안을 도출하며 유사제도의 통합 사례를 살펴보고, 선행연구를
	결론	향후 정보보호 관리체계와 개인정보보호 관리체계의 인증제도 운영방안 개선에서 시간과 비용 비교의 근거로 활용될 수 있음 정보보호 관리체계와 개인정보보호 관리체계 운영 시 인증심사 준비에 필요한 시간과 비용을 절감할 수 있는 인증제도의 운영방안을 찾아보고, 선행연구의 검토를 통해서 기존 연구에서는 두 제도가 함께 운영 되고자 할 때 인증서 취득을 위한 소요 시간과 비용을 절감해 줄 수 있는 연구가 부재하다는 결론을 냄 위 문제점 해결을 위해서 4가지 인증제도 운영방안과 3가지 인증 심사원 운영방안을
	키워드	ISMS / ISMS와PIMS의 통합 관리 / 통합 ISMS-PIMS 인증제도 운영방안 제안
6	침해사고 대응을 위한 디지털 포렌식 도구 활용 지침 적용 수행 방안 연구 (ISMS와 ISO27001 통합을 중심으로)	
	요약	조직내의 체계화된 지침과 지표들의 필요성을 위해 기업의 디지털 포렌식을 ISMS와 ISO27001의 점검 항목 표준화를 이용해서 적용함 디지털포렌식 도구의 활용 사례 검토를 통해서 도구 현황을 파악하고, 관리체계의 절차 및 통제항목을 점검하여 디지털 포렌식 지침 수립에 적합한 점검 항목을 도출하며 도출된 세부 점검 항목에 대한 유효성 검증을 통해 디지털 포렌식 지침을 적용
	결론	정보보호관리체계와 ISO27001을 기반으로 디지털 포렌식 지침 수립에 적합한 점검 항목을 도출하였으며 도출된 세부 점검 항목에 대한 유효성 검증을 통해 디지털 포렌식 지침 적용 유효성을 확인함 또한 오픈소스인 GRR Rapid Response 사용법과 윈도우 이벤트 로그 분석 절차 연구를
	키워드	ISMS&ISO270001 / 디지털포렌식 / 디지털포렌식과 통제항목 비교분석
7	의료기관 KISA-ISMS 인증항목과 ISO 27799 비교 분석 및 개선방안	
	요약	의료정보보호 국제 표준인 ISO 27799와 KISA-ISMS를 비교 분석하여 의료기관의 현재 정책이 반영되어 있으면서 ISMS기준을 만족하는 항목들로 인증을 받게 함으로써 인증
	결론	정보자산분류에서 자산의 소유권, 인적보안에서 고용 전 적격심사, 인적보안에서 고용 계약조건, 접근 통제에서 접근권한 검토, 운영 보안에서 원격근무의 제한 이하 다섯개의 항목들에 대한 개선방안을 제시하고, 의료정보 국제 표준과 비교한 뒤 추가 가능한
	키워드	ISMS / 의료정보 국제 표준 ISO 27799 / 국내 의료정보보안체계 강화

8	정보보호관리체계를 이용한 네트워크 인프라 보안 개선 방안 연구	
	요약	네트워크 인프라와 정보보호관리체계의 정의와 특징, 현황, 선행연구 등을 분석하고, ISMS기반의 네트워크 인프라 운영 보안지침 개선의 필요성과 개선 영역을 정의한다. 또한 ISMS기반의 네트워크 인프라 영역 별 보안지침 개선 항목을 정의하고, 설문조사를 통해서 보안지침 개선안을 검증함
	결론	네트워크 인프라 보안을 위한 ISMS를 이용하여 네트워크 인프라 보안 개선에 대한 연구를 수행하고, ISMS의 절차와 통제 그리고 네트워크 인프라 보안 개선 항목을 검증 하면서 네트워크 인프라 보안 개선 방안을 제안한다. 또한 이를 통해서 기업의 네트워크 인프라 보안에 대해 보다 체계적으로 접근하고, 기업의 보안담당자들의 보안 프로세스 표준화 및 체계화에 대한 전략적 대안을 제시 하였다.
	키워드	ISMS / 네트워크 인프라 / 보안지침 개선
9	ISMS-P 기반의 스마트팩토리 보호대책 개선연구	
	요약	제어시스템 보안 국제표준규격 IEC62443 의 개요와 항목별로 상세사항을 분석하고, KISA 스마트 공장 중요정보 유출 방지 가이드와 비교분석을 진행한다. 또한 분석한 내용을 바탕으로 국내 ISMS-P 정보보호 관리체계의 개선 사항을 제안한
	결론	국제 표준인 IEC62443과 KISA에서 제공하는 스마트공장 중요정보 유출방지 가이드를 서로 비교하여 위협관리 측면인 항목들을 서로 매핑한다. 이에 도출된 유사항목 및 키워드를 국내 정보보안 관리체계와 한번 더 매핑하여 보호대책 항목에 대한 내용추가
	키워드	ISMS-P / 제어시스템 보안 국제표준규격 IEC62443 / 스마트팩토리
10	사물인터넷을 이용한 기업정보 유출 방지대책에 대한 연구	
	요약	사물인터넷 기술을 이용한 기업 정보 유출, 즉 산업기밀 보호 측면의 검토가 매우 약한 상황에서 사물인터넷 기기를 활용한 기업정보 유출 보안위험을 파악하고, 대응하기 위한 연구를 진행한다. 또한 기존 운영 중인 또는 신규 보안체계 프로세스 및 솔루션을 융합하여 기업정보를 보호하기 위한 방안을 제시한다. 사물인터넷 기술에 대해 새로운 기업정보 유출 경로로 악용될 수 있는 보안위험을 분석하고, 보안관리 체계 구축에 적합한 운영모델을 도출하기 위해 각 위협요인들에 대한
	결론	기업에서는 보안담당자의 역량 확보를 위한 노력을 강화할 필요가 있으며 보안 투자가 '성과 없는 투자' 가 아닌 기업의 가치를 높여주는 '미래지향적 투자'라는 인식으로의 전환이 필요하고, 기업 내의 협조적인 보안체계 구축 필요성과 자발적으로 보안을 준수하
	키워드	IoT / 기업정보보호 / IoT를 이용한 기업정보 유출 방지대책
11	정보보호관리체계(ISMS)를 이용한 네트워크 인프라 보안 개선 방안 연구	
	요약	네트워크 인프라와 ISMS의 이론적 배경(정의, 특징, 인증심사 현황 선행연구 등)을 통해서 네트워크 인프라 보안 지침 개선의 필요성과 영역의 정의하고 보안지침 개선안의 검증을 설문조사 방법과 표본 응답자 구성으로 설문 결과 확인
	결론	네트워크 인프라 보안 시 보안 매뉴얼에 따라 시스템 장애와 외부의 침입에 매뉴얼대로 대처할 수 있는지를 확인하고 관리하는 것이 중요하다. 또한 해커의 침입을 통해 악성코드 배포와 전산시스템 마비 그리고 개인정보 및 중요정보가 유출이 되는 문제들을 미리 차단할 수 있는 체계를 마련해야 한다.
	주제	ISMS기반의 네트워크 인프라 운영 보안지침 개선안

ISMS-P 인증심사원의 핵심 직무역량 모델링	
12	<div> <div>요약</div> <p>정보보안 관련 전문 인력인 ISMS-P 인증심사원에 초점을 맞추어 ISMS-P 인증심사원에 요구되는 핵심 직무 특성 및 개인적 특징을 추출하고 1차 전문가 리뷰를 통한 항목 선별 작업을 거쳐, 2차 ISMS-P 인증심사원 설문 조사를 통해 역량 모델링을 진행</p> </div> <div> <div>결론</div> <p>1차 전문가 리뷰를 통해 선별된 항목 46개에서 직무 지식 3개, 직무 기술 1개, 개인 특성 3개를 제거한 39개의 역량 항목을 최종적으로 도출하였고 이것을 바탕으로 개인 역량을 파악할 수 있는 역량 모델링 개발</p> </div> <div> <div>주제</div> <p>ISMS-P 인증심사원의 핵심 직무 역량을 파악해 이를 평가할 수 있는 역량 모델링 진행</p> </div>
방송사 정보보호 활동이 종사자의 준수태도와 의도에 미치는 영향 - 정보보호 관리체계(ISMS) 중심으로	
13	<div> <div>요약</div> <p>지상파방송사, IPTV사업자 등 25개 방송사 직원을 대상으로 본 설문조사를 진행해, 수집된 17부를 최종 표본으로 분석하였고 실증조사를 통해서 수집된 자료의 처리는 SPSS 22.0을 사용하여 각 변수에 대한 빈도분석, 상관관계분석 및 회귀분석을 실시하였다. 구조방정식 Amos22를 사용해서 정보보호활동과 정보보호인식, 정보보호 준수태도와 의도간 인과 관계를 확인적 요인분석을 실시하였다</p> </div> <div> <div>결론</div> <p>관리적 정보보호활동은 업무관련 인식에 영향을 미치지 않는 것으로 나타났고, 정보보호활동으로 받는 업무관련 인식은 정보보호 준수태도에 부(-)의 영향을 미치는 것으로 나타났고, IT직원과 비IT직원간 기술적 정보보호가 업무관련 인식에 미치는 영향은 차이가 있는 것으로 나타났고, 방송사 직종별 정보보호활동이 정보보호 준수태도와 의도에 미치는 차이가 있는 것으로 나타났다</p> </div> <div> <div>주제</div> <p>방송사 정보보호 활동이 종사자의 준수태도와 의도에 미치는 영향</p> </div>
정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도의 효과적인 운영방안	
14	<div> <div>요약</div> <p>정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)는 인증제도의 준비를 위해 소요되는 시간과 비용을 줄여 달라는 요구에 따라 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도로 통합되었다. 그러나 모든 유형의 인증 대상기관에 동일한 인증기준을 적용하면서 생기는 인증 대상기관별 인증기준 적용기준의 모호성과 인증 대상기관에게 과도한 관리체계 운영을 요구하는 인증기준 통제항목의 모호성, 인증 대상기관에 적용해야 할 법적 근거가 모호한 문제점이 발생. 사례 연구를 통해 인증제도의 운영을 위한 방안 제언</p> </div> <div> <div>결론</div> <p>인증기준을 적용하는 인증 대상기관의 유형을 구분하고 유형에 따라 인증심사 시 적용하는 통제항목이나 세부 점검항목을 다르게 적용함으로써 인증 대상기관별 인증기준 적용의 모호성을 개선할 수 있는 방안 ISMS 인증만을 취득하려는 기관에 대해서는 ISMS 인증기준 통제항목에서 개인정보 보호항목이나 ISMS-P 인증 취득 시 적용되는 통제항목의 요구사항을 제외하고 인증심사를 진행하도록 하여 인증기준 통제항목의 모호성을 개선할 수 있는 방안 정보통신망법의 준용 대상이 아닌 인증 대상기관은 해당 기관이 준용해야 하는 법을 기준으로 인증심사를 진행하게 되면 인증 심사 시 적용해야 하는 법의 모호성에 대한 문제점을 개선할 수 있는 방안</p> </div> <div> <div>주제</div> <p>정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도의 효과적인 운영방안을 위해 사례연구</p> </div>

ISMS 프로젝트 시 프로젝트 관리 영역이 ISMS 프로젝트 성과에 미치는 영향	
15	<div> <div>요약</div> <div>ISMS 프로젝트 경험자를 대상으로 ISO21500에서 제시하고 있는 프로젝트 관리 영역인 통합, 이해 관계자, 범위, 자원, 시간, 예산, 리스크, 품질, 조달, 의사소통이 ISMS 프로젝트 성과에 어떠한 영향을 미치는 지를 분석. 또한, 이를 통해 ISMS 프로젝트 시 어떠한 프로젝트 영역에 중점을 두고 수행해야 할지 에 대한 방안을 제시하고자 하였다. 더불어, ISMS 컨설팅 수행역량이 프로젝트 관리 영역과 ISMS 프로젝트 성과 간에 조절효과를 일으킴으로써, ISMS 컨설팅의 효과성에 대해서도 검증하고자 하였다</div> </div> <div> <div>결론</div> <div>ISMS 프로젝트 시 시간 관리 영역이 ISMS 프로젝트 성과에 매우 중요한 영향을 미친다는 것을 보여주고 있다. 무엇보다도 ISMS 프로젝트 시에 의사소통 관리가 ISMS 프로젝트 성과에 가장 중요한 영향을 미친다는 것을 보여주고 있다</div> </div> <div> <div>주제</div> <div>프로젝트 관리에 대한 국제 표준인 ISO21500의 10개의 관리 영역이 ISMS 프로젝트 성과에 미치는 영향에 있어서 컨설팅 조절변수의 효과가 나타나는지를 살펴봄</div> </div>
ISMS-P를 이용한 모바일 앱 진단 항목 연구	
16	<div> <div>요약</div> <div>ISMS-P를 이용한 모바일 앱 보안 체크리스트 개선안을 만들어 해당 체크리스트 개선안을 검증받기 위해 설문조사를 이용</div> </div> <div> <div>결론</div> <div>정량화된 정보보호 및 개인정보보호 관리체계 인증 항목을 모바일 보안 진단에 사전 적용함으로써 정보 주체의 중요정보와 개인정보를 보호함과 동시에 침해사고에 대한 예방을 충분히 할 수 있다</div> </div> <div> <div>주제</div> <div>모바일 앱 보안 진단 항목 개선을 위하여 정보보호 및 개인정보보호 관리체계(ISMS-P)를 이용한 모바일 앱 보안 진단 항목 개선에 대한 연구를 진행</div> </div>
보안 7대 위협을 이용한 ISMS-P 인증효과에 관한 연구 : 기업규모와 경력 중심으로	
17	<div> <div>요약</div> <div>한국인터넷진흥원이 발표한 보안 7대 위협에 대해 자신의 회사를 얼마나 보호할 수 있는지에 대한 효과와 관련하여 설문을 수집하고, 이를 바탕으로 분산분석과 회귀분석을 통해 정보보호 관리체계의 효과성에 대해 분석을 진행. 연구의 결과가 기업의 ISMS-P 인증의 중요성과 체계 도입을 위한 근거자료가 되며, 또한 정보보호 가이드라인 수립이 어려운 스타트업 기업, 중소기업의 보안 체계 수립을 위해 도움이 되기를 희망</div> </div> <div> <div>결론</div> <div>실무자의 경력과 회사규모와 상관없이 ISMS-P의 모든 요소는 기업의 보안 실무자 또는 IT 분야 종사자들이 중요하게 생각하고 있다는 것을 알 수 있었다</div> </div> <div> <div>주제</div> <div>경력과 회사규모가 다른 IT 종사자 50명에게 정보보호 표준인 ISMS-P의 보안요소가 한국인터넷진흥원이 발표한 보안 7대 위협에 대해 자신의 회사를 얼마나 보호할 수 있는지에 대한 효과</div> </div>