

CONTENTS

제1장 기업 리스크 평가와 분석

제1절 리스크 관리 개론	14
1. 리스크 관리의 개념	16
2. 보안 리스크	20
3. 리스크 관리자	21
4. 리스크 관리의 목표	23
5. 리스크 관리의 중요성	24
제2절 리스크 평가 모델	26
1. 자산평가	29
자산정보원 / 영향력 수준결정	
2. 위협평가	34
위협요인 데이터의 수집	
3. 취약성 평가	40
4. 리스크 평가	41
5. 대책 선정	42
6. 지속적인 평가	43
7. 리스크 관리방법	45
리스크의 회피 / 리스크의 전가 / 리스크의 경감 / 리스크의 분산 / 리스크의 보유	
8. 리스크 관리의 최적화	48
보안의 비용효과성 / 주기적인 검토 / 보안 파일	
제3절 비용편익 분석	50
1. 대응책의 선정	51
2. 대응책의 비용결정	53
대응책의 가격결정요소 / 불편함에 대한 비용측정 / 대응책의 우선순위	
3. 의사결정 프로세스	56
체계화된 의사결정 / 한계편익의 분석 / 리스크 평가의 실시 / 대응책의 선정시 고려사항	
4. 리스크 분석 모델	62
정량적 리스크 분석 / 정성적 리스크 분석	
제4절 보 험	66
1. 보안과 보험산업의 역사	68
2. 범죄보험과 보증보험	69
3. 가택침입과 납치	71
4. 화재보험	73
5. 보험적용범위	73

제2장 기업 보안조사와 감사

제1절 보안조사	76
1. 시설물의 보안	78
2. 기업 부서별 평가	80
인사부서 / 회계부서 / 데이터 처리 / 구매부서 / 선적 및 검수 / 조사보고서 / 운영감사와 프로그램화된 조사 /	
손실 가능성 / 손실 위험성 / 가능성, 위험성, 취약성 매트릭스	

3. 현장 보안조사 절차	88
관찰 / 질문 / 분석 / 사실 확인 / 조사 / 평가	
제2절 기초 보안진단(취약성 분석)	92
1. 환경과 구성	92
지리적 환경과 기온 / 규모와 구성 / 사회적·정치적 환경 / 사업장 내부 활동	
2. 보호 시스템	94
물리적 보호조치 / 화재와 재난 / 통제 시스템 / 보상 시스템	
제3절 회계감사	
1. 회계관리	96
내부 통제 질문서 / 손실예방 감사 / 회계의 전산화	
2. 책임 추적성	101
증거 수집 / 손실예방 관련 주요 기록 / 구매관리 / 재고관리	
제4절 분식회계의 유형과 대책	108
1. 급여와 인사활동	108
가공의 종업원 / 가공의 노무시간	
2. 구매와 대금지급활동	110
가공의 매입거래 / 구매거래의 누락 / 매입거래와 입고물품의 차이 / 기간의 부채	
3. 제조와 재고자산 보관활동	111
원가계산방법 악용 / 재고자산 실물분실 및 도난 / 재고자산 평가 미실시	
4. 매출과 대금회수 활동	113
가공 고객과 미적송된 매출 / 실제 발생한 매출거래의 누락 / 매출 거래와 선적물품의 차이 / 매출의 기간귀속 오류 / 현금수입의 기록누락 / 랩핑 / 회수불능 채권상각	
5. 재무활동	115
실제하는 차입금의 누락 / 우발채무의 미계상 / 카이팅	
제3장 기업 보안 취약성 분석	
제1절 리스크 매트릭스	118
1. 문제의 정의	119
손실의 유형 / 손실의 개연성과 빈도 / 개연성의 요인 / 역사적 경험	
2. 개연성 요소분석	124
매트릭스 기법 / 개연성 등급의 설정 / 등급별 표시 / 손실발생의 치명성 / 치명성의 개념	
3. 다양한 비용요소	129
영구적인 대체비용 / 일시적인 대체비용 / 추가적인 후속비용 / 수입의 감소 / 비용의 감소 / 보안손실액의 산정방식 / 치명성 등급설정 / 손실영향력 산정방법 / 우선순위의 결정	
제2절 위협분석	135
1. 위협분석 모델	135
2. 위협분석의 연계성	137
제3절 대응책 수립	138
1. 대응책 수립기준	138
2. 시스템 평가기법	140
3. 구성요소의 선정	140
4. 시스템의 운영방법	141
제4절 보안의 경제적 타당성	142
1. 비용절감	143
2. 손실관리	143
3. 손실회복	145
4. 보안비용의 측정	147
5. 보안비용의 구성	148

인사보안 / 시설보안 / 정보보안 / 전문적인 교육, 훈련과 예방 프로그램 / 보안관리, 감독과 기획

제5절 취약성 평가를 위한 팀 기법	152
1. 협력의 중요성	152
2. 보안업무의 중복확인	154
3. 태스크 포스팀	154
팀의 정규 구성원 / 태스크 포스 운영팀장 / 프로그램의 운영	
4. 모임의 구성	157
위협 정의 / 브레인 스토밍 / 위협분석 / 대응책 / 추가감사	
5. 프로그램의 연속성	160

제4장 기업 시설보안검사

제1절 보안검사 프로그램	162
1. 보안시스템의 목표	163
2. 프로그램의 수립	165
3. PSI팀의 조직과 업무	167
4. 프로그램의 방법론	168
1단계 / 2단계 / 3단계	
5. 검사 필요성의 판단	170
6. 준비 목적과 목표	171
사업장의 데이터 수집 / 목적 / 책임 / 의무 / 정책과 절차	
7. 보안검사의 태도	175
보안관리기획과 프로그래밍 / 보안 프로그램의 모니터링	
8. 현장 프로그램관리	178
제2절 시설보안검사 프로세스	179
1. 사전 검사계획	180
2. 재조사	181
관리적 준비과정 / 주요 고려사항 / 자료수집	
3. 검사진행과 사실확인	185
사업장 취약성 테스트 / 사업장 검사공정	
4. 사전검사의 개요	188
사업장 검사의 시행 / 최종 요약보고	
5. 데이터 분석과정	190
6. 검사보고서의 작성	191
결점과 권고사항 / 보안검사 체크리스트	
7. 시설보안 대책	196
테러리즘 대책 / 기술적 보안대책 / 범죄 대응책(외부) / 범죄 대응책(내부)	
제3절 시설보안진단 보고서	200
1. 요약문	200
2. 개요와 범위	202
개요 / 범위	
3. 사실 확인	202
4. 결론	203
5. 권고사항	204

제5장 기업 재난관리

제1절 재난의 전개	208
1. 재난관리와 BCP	208
기업업무의 연속성 / 재난관리	
2. 재난의 예상	212
3. 재난의 대비	213
4. 예방과 대응	215
5. 응급 의료체제	216
제세동기 / 응급처리 지침 / 에이즈와 B형 간염	
6. 표준운영절차	220
7. 미디어의 역할	221
제2절 재난복구 프로세스	
1. 인위재난	225
폭탄위협과 폭발 / 파업 / 시민의 소요 / 사보타주와 정전 / 구조물 붕괴	
2. 자연재난	229
태풍 / 홍수 / 눈보라 / 지진	
3. 비상계획과 재난복구	235
4. 시설물의 안전성	237
건물 / 건물내 주요 시설 / 출입통제 / 보안 서비스의 활용	
5. 방화 프로세스	240
화재감시원 / 화재진압팀 / 보안요원 / 구성원	

제6장 BIA와 BCP

제1절 비즈니스 영향분석	246
1. BIA의 목적	246
2. 리스크 분석과 BIA	250
수용과 타당성 / 지원 / 중요성	
3. BIA 방법론	253
4. 데이터의 수집	255
목적 / 지침 / 내용	
5. 사례연구	259
수입원 / 재정영향 / 총 손실의 산정 / 추가 비용 / 업무 사이클 / 비즈니스 영향 / 심각성 산정 / 복귀시간 / 필요 자원 / 대체시간	
6. 질문지 형식	263
임직원 / 내·외부 협력자 / 고객과 소프트웨어 / 장비 / 문서형식과 보급품 / 핵심 기록물	
7. 데이터 분석과 제안	266
데이터 분석 / 데이터 제안	
제2절 비즈니스 연속성 기획	269
1. BCP 계획	269
계획의 필요성 / BCP의 구성요소 / BCP의 기초 / BCM의 진화 / BCP 4단계 방법론 / BCP의 구성요소 / 성공적인 BCP의 수립 / BCP의 기대효과	
2. 연속성 계획	279
3. 기획수립 과정	281
4. 프로젝트의 관리	283
코디네이터와 경영진의 지원 / 범위와 기획 방법론의 정의 / 리스크 규명과 감사의 이행	
5. 복구전략의 개발	287
수동기법으로 전환 / 대체전원 / 통신장비	
6. 대체장소와 데이터 복구	291
대체계약 / 핫 사이트 / 웜 사이트 / 콜드 사이트 / 반사 데이터와 원격 저널링 / 정책과 절차 / 데이터 백업	

7. 제3자 제조	295
8. 기록물 관리	296
9. 시설물 복원	297

제7장 보안교육 프로그램과 발전방안

제1절 보안교육 프로그램	300
1. 보안실무자 교육 프로그램	301
보안요원을 위한 세미나(보안요원이나 조사원) / 보안관리자를 위한 강의와 세미나	
2. 최고 보안관리자를 위한 교육 프로그램	302
프로그램의 개요 / Wharton 접근법 : 교육을 통한 효과 / 핵심 강의 주제	
3. 보안교육 프로그램의 트렌드	304
4. 보안실무자 핵심과정	305
보안 리스크 분석 / 보안 디자인 / 보안운영 관리 / 경계구역 보안 / 건물보안과 디자인 / CCTV / 보안조사 / 출입통제와 확인 / 범죄와 직원의 모니터링 / 증거보존과 수사 / 인사관리와 리더십 / IT(컴퓨터) 보안 / 인명보호와 요인보안 / 위기관리 / 정보보안 / 기술적 감시대책 / 폭발물과 폭발장치	
5. 대학원 교과과정	313
산업보안 정책론 / 기업 보안관리론 / 기업 자산보호 / 산업보안 관련법 / 리스크 관리론 / 시설 보안론 / 정보시스템 보안 / 범죄 수사론 / 범죄학 / 테러리즘	
제2절 한국 산업보안 발전방안	322
1. 서론	322
2. 한국 산업보안의 현황	323
산업보안의 정의 / IT 보안이 산업기밀유출보호인가?	
3. 한국 산업보안의 문제점	326
보안 관련 용어 혼란 / 산업보안전문가가 없다 / 산업보안은 산업기술유출방지가 아니다 / 한국의 기업보안부서에는 부정행위 조사업무가 없다	
4. 한국 산업보안의 발전방안	335
산업보안은 위험관리에서 출발해야 / 산업보안협회의 설립 / 산업보안대학원 설립 / 산업보안 자격제도의 시행 / CSO 체제의 구축	
5. 결론	346
참고문헌	348

APPENDIX _기업 보안실무 체크리스트

시설보안진단 체크리스트	352
절도·사기·횡령의 징후	369
화물보안 체크리스트	383
비상계획 프로그램	393
한국기업(주) 보안정책과 절차	404
산업기술의 유출방지 및 보호에 관한 법률	419
산업기술의 유출방지 및 보호에 관한 법률 시행령	431
산업기술의 유출방지 및 보호에 관한 법률 시행규칙	441
기업보안관리자용 PT 제안 자료 예시	443
찾아보기(INDEX)	455