「차례」

Chapter 1 정보보안과 위험관리(Information Security and Risk Management)

Section 01 정보보안과 위험관리 정의와 주요 개념 18
1. 정보보안 관리 개요 18
2. 정보보안 관리에 사용되는 용어 19
Section 02 정보 보안의 핵심 원칙 24
1. 기밀성(Confidentiality) 24
2. 무결성(Integrity) 24
3. 가용성(Availability) 24
4. NIST(NIST SP 800-33) 25
5. NIST에서 말하는 핵심원칙 사이의 의존 관계(NIST SP 800-33) 25
Section 03 정보보호 거버넌스 26
1. 정보보호 거버넌스의 배경 26
2. 보안정책, 절차, 표준, 지침, 기준선 28
3. 준거(Compliance)에 대한 프레임워크 31
Section 04 기업과 조직의 행동양식 38
1. 조직 구조의 진화 38
2. 정보보안 관점에서 조직과 직원 관리의 모범사례/규준 38
3. 정보보안 관리자 40
4. 보고 체계 모델 41
5. 전사적 보안 감독 위원회(Enterprise wide Security Oversight Committee) 43
6. 정보보안 계획 및 인적보안 46
Section 05 보안인식 활동/훈련/교육 48
1. 보안 교육의 종류 48
2. 보안인식 48
3. 보안인식 활동 49
4. 보안 훈련 및 교육 50
Section 06 위험관리 51
1. 위험관리 개념 51
2. 자산의 식별 52
3. 정성적 위험 분석(Qualitative Risk Analysis) 54
4. 정량적 위험 분석(Quantitative Risk Analysis) 55
5. 위험에 대한 대책 56
6. 위험 분석 57
Section 07 윤리 58

연습문제 / 60

Chapter 2 접근통제(Access Control)

Section 01 접근통제의 정의 및 주요 개념 68
1. 접근통제의 정의 68
2. 접근통제의 구성 용어 68
3. 접근통제 절차 68
4. 접근통제 원칙 70
5. 정보 분류(Data Classification) 70
Section 02 접근통제 카테고리와 유형 71
1. 접근통제 카테고리 71
2. 접근통제 유형 72
3. 접근통제 카테고리와 유형의 예 72
Section 03 접근통제에 대한 위협 73
1. 서비스 거부 공격(DoS) 73
2. 스팸 메일 79
3. 버퍼 오버플로(Buffer Overflow) 80
4. 모바일 코드 80
5. 악성 소프트웨어 81
6. 패스워드 크래커(Password Cracker) 82
7. 스푸핑(Spoofing) 83
8. 스니퍼 /중간자 공격(Man-in-the-middle attacks) 85
9. 세션 하이재킹(Session Hijacking) 86
10. 방사(Emanation) 87
11. 어깨넘어 훔쳐보기와 백도어/트랩도어 88
12. 사회공학 88
Section 04 시스템에 대한 접근 90
1. 식별 및 인증 90
2. 패스워드(Password) 91
3. 스마트카드 94
4. 생체인증(Biometrics) 97
Section 05 접근 통합 인증 체계 100
1. SSO(Single Sign On) 100
2. 커베로스(Kerberos) 102
3. 세사미(SESAME) 103
Section 06 데이터에 대한 접근 104
1. 인가의 유형 104
Section 07 중앙집중형 접근통제 107
1. 중앙집중형 접근통제 107
2. 래디우스(RADIUS) 107
3. TACACS/TACACS+ 108
4. RAIUS를 개선한 다이어미트(DIAMETER) 109
5. 원격 접근 시 사용되는 프로토콜 109
6. 분산화된 접근통제 110
7. 혼합 접근통제 111
Section 08 침입 방지 시스템 113
1. 침입 방지 시스템(IPS, Intrusion Prevention System) 113

Section 09 접근통제 보증 116
1. 침투 테스트 116
2. 테스트의 유형 117
3. 은닉채널(Covert Channel) 118
4. 예방 통제 기술 허니팟(HoneyPot) 119

연습문제 / 120

Chapter 3 암호학(Cryptography)

Section 01 암호학의 기본개념 및 역사 128
1. 암호학(Cryptography)의 기본개념 128
2. 암호화의 주요 개념 및 용어 129
3. 암호학의 역사 130
Section 02 암호화 방식 132
1. 입력데이터 처리에 따른 암호화의 구분 132
2. 위치에 따른 암호화의 구분 133
Section 03 암호 시스템 135
1. 대치 암호(Substitution ciphers) 135
2. 전치 암호(Transposition ciphers) 138
3. 기타 암호 139
Section 04 암호 알고리즘 142
1. 블록기반 암호화 모드 142
2. 대칭 알고리즘 146
3. 비대칭 알고리즘 149
4. 하이브리드 암호화 152
Section 05 키 관리 방법 154
1. 키 관리 154
2. 암호화 방식에 따른 키 관리 154
3. PKI 156
Section 06 메시지 무결성 통제 및 디지털 서명 159
1. 체크섬(Checksum) 159
2. MAC(Message Authentication Code) 161
3. 디지털 서명 163
Section 07 암호해독과 공격 165
1. 암호해독 공격 유형 165
2. 사회공학기법 168
3. 공격의 유형 168
Section 08 암호화의 용도 171
1. 암호화를 이용한 이메일 보안 171
2. 인터넷과 네트워크 보안 172
3. 기타 참고 174

연습문제 / 176

Chapter 4 물리적 보안(Physical Security)

Section 01 물리적 보안 개요와 도전 과제 182
1. 물리적 보안의 주제 182
2. 물리적(환경적) 보안의 도전 과제 183
3. 물리적 보안의 통제 기법 185
4. 계층화된 방어 모델 185
Section 02 시설 위치 및 설계 182
1. 시설 위치 187
2. 시설 설계 188
Section 03 건물과 외곽 경계 190
1. 건물 190
2. 외곽 경계(Outermost perimeter) 192
Section 04 내부 지원 시스템 197
1. 전력 197
2. 화재예방, 탐지, 억제 199
Section 05 입구 통제 및 자산 보호 202
1. 입구 통제 202
2. 자산 보호 205
Section 06 정보보호와 관리서비스 및 기타 206
1. 유지보수와 서비스 사안 206
2. 물리적 접근의 감사 207
3. 범죄예방을 위한 환경 설계 방안 207

연습문제 / 210

Chapter 5 보안 아키텍처와 설계(Security Architecture and Design)

Section 01 보안 아키텍처의 개요 216
1. 기업 측면에서의 보안 아키텍처의 필요성 216
2. 보안 아키텍처의 구성 217
Section 02 컴퓨터 아키텍처 218
1. 하드웨어 218
2. 소프트웨어 227
Section 03 일반적인 아키텍처 프레임워크 230
1. 자크만 프레임워크(Zachman Framwork) 230
2. SABSA(Sherwood Applied Business Architecture) Framework 231
3. TOGAF(The Open Group Architecture Framework) 232
4. DoDAF 232
5. ITIL(IT Infrastructure Library) 233
6. 좋은 보안 아키텍처의 특징 233
Section 04 보안 디자인 컴포넌트와 원칙 234
1. 보호링(Protection ring) 234
2. 계층화와 데이터 숨김 235
3. 프로세스 격리(Process Isolation) 235
4. 보안 도메인 236
5. 신뢰 컴퓨팅 베이스(TCB, Trusted Computer Base) 236

6. 참조 모니터 및 보안 커널 237
Section 05 보안 모델과 아키텍처 이론 238
1. 보안 정책과 모델 238
2. 접근통제 239
3. 벨라파둘라 모델(BLP, Bell – LaPadula Confidentiality Model) 242
4. 비바 무결성 모델(Biba Integrity Model) 243
5. 클락–윌슨 무결성 모델(Clark – Wilson Integrity Model) 245
6. 기타 기본 모델 245
7. 보안 운영 모드 247
Section 06 보안 제품 평가 방법 및 기준 248
1. TCSEC 248
2. ITSEC 250
3. 공통평가기준(CC, Common Criteria) 250
4. CMMI(Capability Maturity Model Integration) 253
5. 보안 프레임워크 : ISO/IEC 17799:2005, BS7799:2, ISO 27001 254
6. COSO(Committee of Sponsoring Organizations) 255
7. 인증 및 인가 256

연습문제 / 257

Chapter 6 재난복구와 비즈니스 연속성(Disaster Recovery & Business Continuity)

Section 01 비즈니스 연속성 계획과 재난 복구 262
1. 보안의 기본 원칙 262
2. 비즈니스 연속성 계획 262
3. 재난 복구 계획 263
4. 위험 분석 및 관리 개요 264
Section 02 BCP 프로세스 266
1. BCP 단계(NIST) 266
2. 비상 계획 정책 수립 267
3. 업무 환경 분석 268
4. BCP 프로젝트 개시 268
Section 03 비즈니스 영향 분석 270
1. 비즈니스 영향 분석 270
2. 비즈니스 영향 분석 프로세스(NIST) 271
3. 위험 분석 272
4. 상호 의존 273
5. 예방적 방법 273
Section 04 전략개발단계 274
1. 복구 전략 274
2 비즈니스 프로세스 복구 275
3. 시설물 복구 276
4. 공급과 기술적 복구 279
5. 사용자 환경 복구 281
6. 데이터 복구 281
7. RAID 282

8. 데이터 백업과 중복 288
9. 데이터 백업을 위한 기술 288
Section 05 데이터의 복구와 회복 292
1. BCP/DRP 단계 293
2 BCP/DRP 전략 계획 294
3. BCP/DRP 테스트 295
4. BCP 관리 297

연습문제 / 298

Chapter 7 통신 및 네트워크 보안(Telecommunications and Network Security)

Section 01 기본개념 304
1. 네크워크 분류 304
2. OSI 참조 모델 306
3. 주요 네트워크 기반 공격기법 및 방어 대책 308
Section 02 Layer 1 : 물리적 계층 311
1. 개념과 아키텍처 311
2. 네트워크를 위한 장비 314
3. 위협과 대응책 318
4. 무선 랜(Wireless LAN) 보안 기술 318
Section 03 Layer 2 : 데이터링크 계층 320
1. 개념과 아키텍처 320
2. 기술과 구현 323
3. 프로토콜 324
4. 위협 및 대응책 326
Section 04 Layer 3 : 네트워크 계층 328
1. 개념과 아키텍처 328
2. 기술과 구현 333
3. 프로토콜 345
4. 위협과 대응책 346
Section 05 Layer 4 : 전송 계층 349
1. 개념과 아키텍처 349
2. 기술과 구현 349
3. 프로토콜 350
4. 위협 및 대응책 351
Section 06 Layer 5 : 세션 계층 354
1. 개념과 아키텍처 354
2. 기술 및 구현 354
3. 프로토콜 355
4. 위협 및 대응책 355
Section 07 Layer 6 : 프레젠테이션 계층 357
1. 개념과 아키텍처 357
2. 기술과 구현 357
3. 프로토콜 357
4. 위협과 대응책 358

Section 08 Layer 7 : 응용 계층 262
1. 개념과 아키텍처 359
2. 기술과 구현 359
3. 프로토콜 361
4. 위협과 대응책 363
Section 09 스마트폰 기반의 보안 위협 및 대응책 262
1. 스마트폰 환경에 대한 이해 366
2 스마트폰 기반의 취약성과 위협 및 해결책 366

연습문제 / 372

Chapter 8 응용프로그램 보안(Application Security)

Section 01 기본 개념 378
1. 소프트웨어 개발 환경 378
2. 오픈소스(Open Source) 379
3. 응용프로그램 개발 보안 및 통제 380
Section 02 응용프로그램 환경에서의 보안 위협 및 대책 389
1. 응용프로그램 환경에서의 위협 389
2. 응용프로그램 환경에서의 보안 대책 392
Section 03 악성 코드(Malware) 397
1. 악성코드의 유형 397
2. 악성코드로부터 보호 400
Section 04 감사, 보증 메커니즘 402
1. 인증(Certification) 402
2. 인가(Accreditation) 402
3. 변경 관리(Change Management) 402
4. 구성 관리(Configuration Management) 403
Section 05 데이터베이스(Database) 404
1. DBMS 아키텍처 404
2. DB 인터페이스 언어 406
3. DW(Data Warehousing) 407
4. 데이터베이스 취약점 및 위협 408
5. DBMS 통제 409
6. 지식관리(Knowledge Management) 410
Section 06 웹 응용프로그램 환경 411
1. 웹 응용프로그램에 대한 위협과 보호 411

연습문제 / 414

Chapter 9 운영 보안(Operation Security)

Section 01 운영보안의 개요와 특권 개체 통제 420
1. 운영보안(Operation Security)의 개요 420
2. 특권 개체 통제(Privileged Entity Controls) 420

Section 02 자원보호(Resource Protection) 422
1. 시설 422
2. 하드웨어 422
3. 소프트웨어 422
4. 문서 및 운영 위협 423
5. 통제유형 및 방법 423
6. 물리적 접근 제어(Physical Access Control) 426
7. 매체의 보안 제어 426
Section 03 운영연속성(Continuity of operations) 428
1. 결함 허용성(Fault Tolerance) 428
2. 데이터 보호 428
3. 시설 429
4. 문제관리(Problem Management) 429
5. 운영공격 유형 430
6. 시스템복구(System Recovery) 433
7. 취약성 스캐닝(Vulnerability scanning) 434
8. 감사(Auditing) 434
9. 침투 테스팅 기법 436
10. 위반 분석(Violation Analysis) 436
Section 04 변경 통제 관리 262
1. 형상 관리(Configuration Management) 437
2. 변경 통제 프로세스 437
3. 라이브러리 유지 438
4. 패치 관리 438

연습문제 / 439

Chapter 10 법, 컴플라이언스, 조사(Legal, Regulations, Compliance and Investigations)

Section 01 컴퓨터 범죄 446
1. 컴퓨터 범죄의 개요 446
2. 컴퓨터 범죄의 대표적인 유형 447
3. 컴퓨터 범죄자의 분류 448
4. 컴퓨터 범죄의 구성요소 449
5. 범죄 예방을 위한 기업 내에서의 요구사항(Due Care) 449
Section 02 주요 법률 체계 450
1. 법 개요 450
2. 지적 재산권 450
3. 소프트웨어 저작권 451
4. 개인정보보호법 451
5. 법, 명령 그리고 규정 453
Section 03 윤리 및 의무 456
1. $(ISC)^2$의 윤리강령 456
2. Computer Ethics Institute의 윤리 강령 10계명 456
3. IAB(Internet Activities Board)의 비윤리적이고 용인되지 않는 행위 457
4. 윤리적 오류의 사례 457
5. 하향 책임(Downstream Liability) 457

Section 04 컴퓨터 범죄 조사 458
1. 사건 대응 458
2. 컴퓨터 범죄 감식과 적절한 증거 수집 458
3. 사고 처리 459
4. 감시, 수색 그리고 압수 459
5. 디지털/전자적 증거물 460
Section 05 컴퓨터 포렌식 462
1. 디지털 증거물의 개념 462
2. 디지털 증거의 특성 462
3. 포렌식의 원칙 462
4. 포렌식의 절차 463
5. 디지털 증거 수집의 절차 463
6. 포렌식의 분류 및 기술 464
7. 디지털 포렌식 도구 464
8. 디스크 복사와 디스크 이미징의 비교 465
9. 컴퓨터 포렌식의 Anti-Forensic 기법 465
10. 포렌식 담당자별 역할 465
Section 06 CERT(Computer Emergency React Team) 466
1. CERT 직원이 갖춰야 할 기술력 466
2. 침해사고 대응 기능 466
3. CERT에서 많이 사용하는 정보확인 기법 467

연습문제 / 468