Hanbit RealTime 128

Max의 해킹과 보안 시리즈

네트워크 보안 시스템 구축과 보안 관제

장상근 지음

– 보안 관제편 –

한빛미디어 Hanbit Media, Inc.

Max의 해킹과 보안 시리즈

네트워크 보안 시스템 구축과 보안 관제

장상근 지음

– 보안 관제편 –

한빛미디어 Hanbit Media, Inc.

Max의 해킹과 보안 시리즈 **네트워크 보안 시스템 구축과 보안 관제** – 보안 관제편 –

초판발행 2016년 4월 15일

지은이 장상근(맥스) / **펴낸이** 김태헌
펴낸곳 한빛미디어(주) / **주소** 서울시 마포구 양화로 7길 83 한빛미디어(주) IT출판부
전화 02-325-5544 / **팩스** 02-336-7124
등록 1999년 9월 30일 제10-1779호
ISBN 978-89-6848-804-7 15000 / **정가** 12,000원

총괄 전태호 / **책임편집** 김창수 / **기획·편집** 정지연
디자인 표지/내지 여동일, 조판 최송실
마케팅 박상용, 송경석, 변지영 / **영업** 김형진, 김진불, 조유미

이 책에 대한 의견이나 오탈자 및 잘못된 내용에 대한 수정 정보는 한빛미디어(주)의 홈페이지나 아래 이메일로 알려주십시오.
한빛미디어 홈페이지 www.hanbit.co.kr / **이메일** ask@hanbit.co.kr

Published by HANBIT Media, Inc. Printed in Korea
Copyright ⓒ 2016 장상근 & HANBIT Media, Inc.
이 책의 저작권은 장상근과 한빛미디어(주)에 있습니다.
저작권법에 의해 보호를 받는 저작물이므로 무단 복제 및 무단 전재를 금합니다.

지금 하지 않으면 할 수 없는 일이 있습니다.
책으로 펴내고 싶은 아이디어나 원고를 메일(ebookwriter@hanbit.co.kr)로 보내주세요.
한빛미디어(주)는 여러분의 소중한 경험과 지식을 기다리고 있습니다.

저자 소개

지은이_ **장상근(맥스)**

현재 KBS(한국방송공사)에서 정보보호 업무를 하고 있다. 1998년 중학교 시절부터 해킹과 보안 분야에 관심을 가졌으며 고등학교 때에는 충북 지역 정보보안 연구 모임(충북 해커스랩)에서 활동했다. 대학에 입학해서는 세종대 정보보안 소모임(S.S.G)에서 활동했고, 육군 정보보호기술(CERT)병 및 자이툰 파병으로 군 복무를 했다. 제대 후 2008년도 대학정보보호동아리 연합회(KUCIS) 회장직을 맡았고, 국내 보안 업체들에서 악성코드 분석, 모바일 보안과 보안 취약점 분석 등 선행 보안 기술 연구 활동을 했다. 그 외 활동으로 해킹과 보안 커뮤니티(Haru) 및 SECUINSIDE 보안 컨퍼런스 등에도 참여하고 있으며, 사물인터넷, 인공지능, 첨단 농업 등에 관심이 많다.

- **홈페이지:** http://maxoverpro.org
- **이메일:** maxoverpro@gmail.com

저자 서문

현재 시중에 있는 해킹과 보안 관련 책은 웹 해킹, 리버스 엔지니어링, 모의해킹 등 공격 및 분석에 초점이 맞춰 있고, 방어의 관점에서 저술된 책은 상대적으로 적다는 생각이 문득 들었습니다. 사실, 보안 업체와 일반 기업에서는 공격이 목표가 아니라 어떻게 하면 서버, 네트워크, PC 등 자신의 자산을 안전하게 보호할 수 있을까를 고민합니다. 하지만 자체적으로 보안 조직을 구성해 보안 시스템을 운영 및 유지보수하고 보안 관제하면서 사이버 침해사고에 대응할 수 있는 능력을 갖춘 곳은 생각보다 많지 않습니다.

이 책은 중소기업, 스타트업, 학교, 게임방 등 소규모 조직에서 오픈소스를 활용해 적은 예산으로도 자체적으로 보안 시스템을 구축하고 보안 관제 중 발생할 수 있는 다양한 사이버 공격 유형에 대응할 수 있도록 내용을 구성했습니다.

보안 관제는 보안 관제 시스템을 구축하는 것이 끝이 아니라 제대로 된 보안을 위한 시작입니다. 점점 고도화되는 사이버 공격에 대응할 수 있게 이 책이 작지만 큰 도움이 되었으면 합니다. 또한, 최신 사이버 공격을 분석하고 보안 시스템에 적용해 침해사고를 예방할 수 있도록 스스로 노력이 필요함을 잊지 않았으면 합니다.

이 책이 나오는 데 많은 도움을 주신 한빛미디어 관계자분들께 감사의 말씀을 드리며 항상 응원하고 격려해 주시는 부모님과 가족, 동료, 친구들에게 감사의 말을 전합니다. 마지막으로 책을 쓰는 동안 책의 내용을 검토해 주는 등 세심하게 배려해 준 여자친구에게 사랑한다는 말을 전합니다.

대상 독자 및 참고사항

이 책은 보안 시스템을 구축하고 보안 관제를 하려는 기업과 공공기관의 보안 담당자, 보안 시스템 구축과 보안 관제를 배우려는 학생을 대상으로 합니다. 이 책은 네트워크와 운영체제(Linux)에 대한 기본적인 내용을 알면 좀 더 쉽게 이해할 수 있습니다.

이 책은 어떻게 보안 조직과 보안 관제 센터를 만들어야 할지 그리고 보안 관제 시스템 구축과 운용에 대한 기본적인 내용 등을 이해하고 실제 사이버 공격 유형에 따른 대응 방법을 익혀 실제 보안 관제 업무에 도움을 주는 것을 목표로 합니다.

이 책에서 사용하는 웹 해킹 실습 예제는 http://maxoverpro.org/pds/webhack.zip 에서 다운로드하기 바랍니다. 그 밖에 이 책과 관련해 궁금한 점은 필자의 홈페이지나 이메일로 문의해 주기 바랍니다.

차례

chapter 6 웹 방화벽 011

6.1 웹 방화벽 설치 011
6.2 웹 방화벽 정책 관리 012
6.2.1 웹 방화벽 정책 적용 013
6.2.2 웹 방화벽 정책 설정 015
6.3 정리 017

chapter 7 네트워크 접근 제어 시스템 019

7.1 네트워크 접근 제어 시스템의 필요성 019
7.2 네트워크 접근 제어 시스템 구축 020
7.2.1 NAC 구축 방식 020
7.2.2 NAC 설치 022
7.2.3 In-Line 방식의 PacketFence 환경 구축 026
7.2.4 Out-of-Band 방식의 PacketFence 환경 구축 032
7.3 PacketFence 운영 034
7.3.1 단말기 네트워크 접근 제어 035
7.3.2 사용자 관리 037
7.4 정리 038

chapter 8 보안 관제 시스템 039

8.1 보안 관제 구성 039
8.2 데이터 분석과 검색을 위한 Elasticsearch 040
8.2.1 Elasticsearch 설치 041
8.2.2 Elasticsearch 설정과 구동 042
8.2.3 Elasticsearch 플러그인 044

8.3 로그 수집을 위한 Logstash 045
8.3.1 Logstash 설치와 설정 045
8.3.2 Logstash-forwarder 설치와 설정 050
8.4 데이터 시각화를 위한 Kibana 052
8.4.1 Kibana 설치와 설정 052
8.4.2 Kibana를 이용한 데이터 분석 055
8.4.3 Kibana를 이용한 데이터 시각화 057
8.5 정리 061

chapter 9 보안 취약점 점검을 위한 도구 활용법 063

9.1 netstat 064
9.2 tcpdump 065
9.3 WireShark 067
9.3.1 특정 패킷만 수집하기 068
9.3.2 패킷 데이터 필터링 070
9.3.3 패킷 데이터 파일 저장 072
9.3.4 패킷 데이터로부터 파일 추출 073
9.4 EtherApe 074
9.5 Bit-Ttwist 076
9.5.1 네트워크 패킷 재전송 076
9.5.2 네트워크 패킷 수정 078
9.6 Nmap 079
9.6.1 Nmap을 이용한 네트워크 점검 080
9.6.2 Nmap 스크립트 엔진을 이용한 네트워크 취약점 점검 082
9.7 OpenVAS 082
9.7.1 OpenVAS 설치와 설정 083
9.7.2 OpenVAS를 통한 취약점 점검 084

9.8 정리 088

chapter 10 실전 보안 관제 089

10.1 보안 관제 기본 운영 090
10.1.1 IP/Port 기반 공격 탐지와 대응 090
10.1.2 프로토콜 기반 공격 탐지와 대응 092
10.1.3 시그니처 기반 공격 탐지와 대응 094
10.2 임계치 기반 공격 탐지와 대응 094
10.2.1 트래픽 과부하 공격 094
10.2.2 무작위 대입 공격 095
10.3 유해 및 악성 사이트 탐지와 대응 097
10.3.1 블랙 리스트 097
10.3.2 유해 콘텐츠 분석 기반 탐지/차단 099
10.3.3 유해 및 악성코드 배포 IP 조사와 추적 100
10.4 웹 해킹 탐지와 대응 103
10.4.1 인젝션 103
10.4.2 인증 및 세션 관리 취약점 106
10.4.3 크로스 사이트 스크립팅 108
10.4.4 보안 설정 오류 109
10.4.5 민감한 데이터 노출 110
10.4.6 크로스 사이트 요청 변조 111
10.4.7 알려진 취약점이 있는 컴포넌트 112
10.4.8 홈페이지 위·변조 및 웹셸을 이용한 침해사고 과정과 대응 113
10.5 공격 코드 탐지와 대응 116
10.5.1 Exploit 116
10.5.2 Shellcode 118
10.6 서버 및 엔드포인트 공격 탐지와 대응 118

10.6.1 서버 보안 이벤트 분석 ——— 119
10.6.2 네트워크 접근 제어를 통한 엔드포인트 보안 위협 차단 ——— 120
10.7 정리 ——— 122

chapter 11 보안 관제의 미래 ——— 123

11.1 보안 관제 트렌드의 변화 ——— 123
11.1 보안 관제 트렌드 변화에 따른 고려사항 ——— 124
11.2 보안 관제 인력의 전문성 ——— 125
11.3 보안 시스템 구축 시 체크 리스트 ——— 126
11.5 정리 ——— 127

chapter 6

웹 방화벽

웹을 통한 침해사고(정보 유출 및 금전적 피해)가 지속해 발생하면서 웹 보안의 필요성과 중요도가 높아졌다. 하지만 웹 애플리케이션에 존재하는 취약점은 네트워크 영역에서 발생하는 것이 아니라 내부의 웹 서버나 DB에서 다양한 형태로 발생할 수 있어서 기존의 방화벽과 IDS/IPS로는 네트워크 영역에서 정교한 형태의 웹 해킹을 탐지하기 어려웠다. 이에 따라 웹 해킹에 대응할 수 있는 특화된 웹 방화벽WAF, Web Application Firewall이라는 보안 시스템이 나타났다.

이 장에서는 호스트 기반 웹 방화벽인 'ModSecurity'를 설치하고 이를 운영하는 방법에 대해 알아보겠다.

6.1 웹 방화벽 설치

ModSecurity는 Apache 웹 서버에서 적용할 수 있는 오픈소스 웹 방화벽으로, 실시간으로 웹 애플리케이션의 모니터링과 로그를 확인할 수 있고 웹 공격에 대한 침입 탐지와 방지 기능을 갖추고 있어 중·소형 규모의 웹 서비스를 운영하는 곳이라면 웹 보안을 강화하는 데 유용하게 사용할 수 있다. Apache 외에도 Nginx, IIS 웹 서버도 지원하며, 최근에 2.9.1 버전까지 배포되었다. 무료판에서는 기본 정책Rule을 제공하고, 최신 정책은 상업적으로(유료로) 제공한다.

이 책에서는 CentOS 6.x 환경에서 ModSecurity 안정화 버전인 2.9.0 소스코드를 다운로드해 설치해보겠다. 설치는 다음 명령으로 한다.

```
// ModSecurity 설치에 필요한 라이브러리 설치
# yum -y install httpd-devel git gcc make libxml2 pcre-devel libxml2-devel
curl-devel

// 소스 코드 기반 설치
# cd /tmp
# wget https://www.modsecurity.org/tarball/2.9.0/modsecurity-2.9.0.tar.gz
# tar -xvzf modsecurity-2.9.0.tar.gz
# cd modsecurity-2.9.0
# ./configure ; make ; make install
```

설치를 완료하면 다음과 같이 설정 파일을 웹 서버 설정 파일이 위치한 곳에 복사하고, 설정 파일을 수정한 후 웹 서버를 재가동하면 정상적으로 ModSecurity가 적용된다.

```
// Apache 폴더에 ModeSecurity 복사
# cp modsecurity.conf-recommended /etc/httpd/conf.d/modsecurity.conf
# cp unicode.mapping /etc/httpd/conf.d/

// Apache 설정 파일(httpd.conf)에 mod_security2.so 모듈 적용 내용 추가
# echo LoadModule security2_module modules/mod_security2.so >> /etc/httpd/
conf/httpd.conf

// 설정 완료 후 서비스 httpd 재기동
# service httpd restart
```

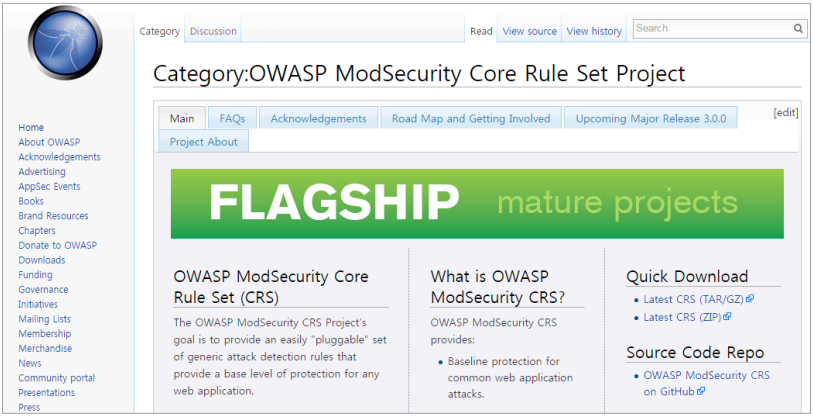
6.2 웹 방화벽 정책 관리

웹 방화벽을 설치했다고 끝나는 것이 아니다. 웹 방화벽이 웹 공격을 탐지 및 대응하려면 웹 공격에 대한 정책을 적용하고 운영해야 한다.

6.2.1 웹 방화벽 정책 적용

ModSecurity에는 OWASP The Open Web Application Security Project에서 일반적인 웹 공격에 대한 탐지와 대응을 위해 제공하는 Rule set과 Trustwave SpiderLabs[01]에서 제공하는 상용 Rule set이 있으며 더 많은 형태의 웹 공격을 탐지할 수 있다. 이 책에서는 OWASP에서 제공하는 Rule set을 적용하는 방법을 알아보겠다.

그림 6-1 OWASP ModeSecurity Core Rule Set Project[02]




```
// Rule 다운로드 및 설치
# cd /etc/httpd
# git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git
# mv owasp-modsecurity-crs/ modsecurity-crs
# cd modsecurity-crs
# cp modsecurity_crs_10_setup.conf.example modsecurity_crs_10_config.conf

// modsecurity_crs_10_config.conf 설정

// 내용 추가
SecRuleEngine On
SecAuditEngine On
SecAuditLog /var/log/httpd/modsec_audit.log
```

01 참고: https://www.trustwave.com/Company/SpiderLabs/

02 참고: https://goo.gl/s9cuJ

```
SecAuditLogParts ABCFHZ
SecDataDir /tmp

// SecDefaultAction에 auditlog 추가
SecDefaultAction "phase:1,deny,log,auditlog"
SecDefaultAction "phase:2,deny,log,auditlog"

// httpd.conf 설정 파일에 ModSecurity Rule set 추가
# echo Include modsecurity-crs/modsecurity_crs_10_config.conf >> /etc/httpd/
conf/httpd.conf
# echo Include modsecurity-crs/base_rules/*.conf >> /etc/httpd/conf/httpd.conf

// httpd.conf 설정 파일 수정
LoadModule unique_id_module modules/mod_unique_id.so // 주석 해제

// 재기동
# service httpd restart
```

재기동한 후 다음과 같이 테스트해 보면 정상적으로 작동하는지 확인할 수 있다.

그림 6-2 ModSecurity에 의한 비정상 접근 탐지/차단


```
// 앞의 테스트에 대한 /var/log/httpd/modsec_audit.log 로그
Message: Access denied with code 403 (phase 2). Pattern match "\\.\\./" at
ARGS:file. [file "/etc/httpd/conf.d/modsecurity.conf"] [line "230"] [id "50904"]
[msg "Drive Access"] [severity "WARNING"]
Action: Intercepted (phase 2)
```

```
Apache-Handler: php5-script
Stopwatch: 1455878158993805 1113 (- - -)
Stopwatch2: 1455878158993805 1113; combined=345, p1=269, p2=26, p3=0, p4=0,
p5=50, sr=18, sw=0, l=0, gc=0
Producer: ModSecurity for Apache/2.9.0 (http://www.modsecurity.org/); OWASP_
CRS/2.2.9.
Server: Apache/2.2.15 (CentOS)
Engine-Mode: "ENABLED"
```

6.2.2 웹 방화벽 정책 설정

ModSecurity를 처음 운영할 때에는 오탐이 발생할 수 있으므로 ModSecurity 모드를 탐지 상태인 'SecRuleEngine DetectionOnly'로 설정한 상태에서 웹 애플리케이션을 정상적으로 이용 시 오탐이 발생하지 않는지 먼저 확인해야 한다. 방화벽 정책 설정을 위해서는 'modsecurity_crs_10_config.conf' 파일을 확인해 다음과 같이 정책을 어떻게 운영할 것인지 기본 정책 운영 설정을 하도록 한다.

```
// modsecurity_crs_10_config.conf
// modSecurity On:활성화, Off:비활성화, DetectionOnly:탐지만 사용
SecRuleEngine ( On ¦ Off ¦ DetectionOnly )

// 로깅 설정(On: 모든 트랜잭션 로깅, Off: 모든 트랜잭션 로깅하지 않음, RelevantOnly:
Error, Warning 트랜잭션과 SecAuditLogRelevantStatus의 상태 코드만 로깅
SecAuditEngine (On ¦ Off ¦ RelevantOnly )

// 감사 로그 파일 경로 정의
SecAuditLog /var/log/httpd/modsec_audit.log

// 로그 파일에 기록할 항목 정의
// A(Audit log header), B(Request header), C(Request body), F(Response header)
// H(감사 로그 트레일러), Z(로그 끝)
SecAuditLogParts ABCFHZ

// 감사 로그 구조 타입 설정
```

```
// Serial: 파일 하나에만 감사 로그 저장, Concurrent: 트랜잭션별로 나눠서 감사 로그 저장
SecAuditLogType (Serial | Concurrent)

// 정책이 매칭되는 경우 행동 정의
SecDefaultAction "phase:1,deny, log, auditlog"

// 웹 서버 응답 정보 변경
SecServerSignature "Microsoft-IIS/5.0"
```

오탐이 발생하는 경우 정책을 수정하거나 예외 처리를 위한 화이트 리스트 정책을 관리하면서 커스터마이징Customizing해야 한다. 예외 처리 방법은 정책 파일이 존재하는 modsecurity-crs/base_rules에 다음과 같이 특정 정책에 대한 예외 처리를 관리할 whitelist.conf 정책 파일을 생성하면 된다.

```
// 예외 처리 정책을 관리할 whitelist.conf
<LocationMatch .*>
<IfModule mod_security2.c>
    SecRuleRemoveByID 960017        // Rule ID가 960017이면 정책 제거
    SecRuleRemoveByMsg "Injection"  // Msg가 Injection인 정책 제거
</IfModule>
</LocationMatch>

// 특정 URL에 대한 예외 처리
<LocationMatch /upload/upload.php>
<IfModule mod_security2.c>
    SecRuleEngine Off
</IfModule>
</LocationMatch>
```

이와 같이 'DetectionOnly' 상태로 운영하면서 오탐으로 판단되는 정책은 제거하거나 정책을 변경하고 화이트 리스트 정책을 적용한 후 'SecRuleEngine On'으로 설정을 변경해 허용 범위 외의 웹 해킹을 시도하면 탐지/차단될 수 있도록 운영한다.

6.3 정리

웹 방화벽은 호스트 기반과 어플라이언스Appliance 기반으로 구축할 수 있다. ModSecurity와 같은 호스트 기반 방화벽은 중·소형 규모의 웹 서버에 각각 설치하고 운영해야 하는 번거로움이 있지만, 세밀한 웹 방화벽 정책을 운영할 수 있다. 어플라이언스 기반 방화벽은 대부분 Reverse Proxy 또는 In-Line 형태로 구축할 수 있다. 다수의 웹 서비스를 운영하는 경우라면 운영이 편리한 어플라이언스 형태의 웹 방화벽을 운영하는 것이 좋다.

한빛 리얼타임

한빛 리얼타임은 IT 개발자를 위한 전자책입니다.

요즘 IT 업계에는 하루가 멀다 하고 수많은 기술이 나타나고 사라져 갑니다. 인터넷을 아무리 뒤져도 조금이나마 정리된 정보를 찾기도 쉽지 않습니다. 또한, 잘 정리되어 책으로 나오기까지는 오랜 시간이 걸립니다. 어떻게 하면 조금이라도 더 유용한 정보를 빠르게 얻을 수 있을까요? 어떻게 하면 남보다 조금 더 빨리 경험하고 습득한 지식을 공유하고 발전시켜 나갈 수 있을까요? 세상에는 수많은 종이책이 있습니다. 그리고 그 종이책을 그대로 옮긴 전자책도 많습니다. 전자책에는 전자책에 적합한 콘텐츠와 전자책의 특성을 살린 형식이 있다고 생각합니다.

한빛이 지금 생각하고 추구하는, 개발자를 위한 리얼타임 전자책은 이렇습니다.

1 **eBook First –**
빠르게 변화하는 IT 기술에 대해 핵심적인 정보를 신속하게 제공합니다

500페이지 가까운 분량의 잘 정리된 도서(종이책)가 아니라, 핵심적인 내용을 빠르게 전달하기 위해 조금은 거칠지만 100페이지 내외의 전자책 전용으로 개발한 서비스입니다. 독자에게는 새로운 정보를 빨리 얻을 기회가 되고, 자신이 먼저 경험한 지식과 정보를 책으로 펴내고 싶지만 너무 바빠서 엄두를 못 내는 선배, 전문가, 고수 분에게는 좀 더 쉽게 집필할 수 있는 기회가 될 수 있으리라 생각합니다. 또한, 새로운 정보와 지식을 빠르게 전달하기 위해 O'Reilly의 전자책 번역 서비스도 하고 있습니다.

2 **무료로 업데이트되는 전자책 전용 서비스입니다**

종이책으로는 기술의 변화 속도를 따라잡기가 쉽지 않습니다. 책이 일정 분량 이상으로 집필되고 정리되어 나오는 동안 기술은 이미 변해 있습니다. 전자책으로 출간된 이후에도 버전 업을 통해 중요한 기술적 변화가 있거나 저자(역자)와 독자가 소통하면서 보완하여 발전된 노하우가 정리되면 구매하신 분께 무료로 업데이트해 드립니다.

3 독자의 편의를 위해 DRM-Free로 제공합니다

구매한 전자책을 다양한 IT 기기에서 자유롭게 활용할 수 있도록 DRM-Free PDF 포맷으로 제공합니다. 이는 독자 여러분과 한빛이 생각하고 추구하는 전자책을 만들어 나가기 위해 독자 여러분이 언제 어디서 어떤 기기를 사용하더라도 편리하게 전자책을 볼 수 있도록 하기 위함입니다.

4 전자책 환경을 고려한 최적의 형태와 디자인에 담고자 노력했습니다

종이책을 그대로 옮겨 놓아 가독성이 떨어지고 읽기 어려운 전자책이 아니라, 전자책의 환경에 가능한 한 최적화하여 쾌적한 경험을 드리고자 합니다. 링크 등의 기능을 적극적으로 이용할 수 있음은 물론이고 글자 크기나 행간, 여백 등을 전자책에 가장 최적화된 형태로 새롭게 디자인하였습니다.

앞으로도 독자 여러분의 충고에 귀 기울이며 지속해서 발전시켜 나가겠습니다.

지금 보시는 전자책에 소유 권한을 표시한 문구가 없거나 타인의 소유권한을 표시한 문구가 있다면 위법하게 사용하고 있을 가능성이 큽니다. 이 경우 저작권법에 따라 불이익을 받으실 수 있습니다.

다양한 기기에 사용할 수 있습니다. 또한, 한빛미디어 사이트에서 구매하신 후에는 횟수와 관계없이 다운로드할 수 있습니다.

한빛미디어 전자책은 인쇄, 검색, 복사하여 붙이기가 가능합니다.

전자책은 오탈자 교정이나 내용의 수정·보완이 이뤄지면 업데이트 관련 공지를 이메일로 알려 드리며, 구매하신 전자책의 수정본은 무료로 다운로드할 수 있습니다.

이런 특별한 권한은 **한빛미디어 사이트에서 구매하신 독자에게만 제공**되며, 다른 사람에게 양도나 이전은 허락되지 않습니다.