TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx/R1

제정일: 20xx년 xx월 xx일

# 분산원장기술을 활용한 온라인투표 모델 및 보안 위협 대응

Security threats to online voting using distributed ledger technology

TTA 한국정보통신기술협회
Telecommunications Technology Association

| | | | | | |
|---|---|---|---|---|---|
| **표준초안 검토 위원회** | **개인정보보호/ID관리, 블록체인 보안(PG502)** | | | | |
| **표준안 심의 위원회** | **정보보호기술위원회(TC5)** | | | | |
| | | | | | |
| | **성명** | **소 속** | **직위** | **위원회 및 직위** | **표준번호** |
| **표준(과제) 제안** | 박근덕 | 개인정보보호표준포럼 | - | - | |
| **표준 초안 작성자** | 박근덕 | 서울외국어대학원대학교 | 교수 | - | |
| | 김창오 | 카카오모빌리티 | CISO | - | |
| | 염흥열 | 순천향대학교<br>개인정보보호표준포럼 | 교수<br>의장 | PG502 위원 | |
| **사무국 담당** | 박수정 | 한국정보통신기술협회 | 책임 | 사무국 | |



본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx.

# 서 문

## 1 표준의 목적

이 표준의 목적은 정보통신 인프라 및 클라이언트·서버 기반의 분산원장기술을 활용한 온라인투표에 관한 보안 위협을 식별하고 최소한의 대응 방안을 제시함에 있다. 본 표준은 모든 산업군에서 분산원장기술을 활용한 온라인투표 시스템을 구축 및 운영시 적용 가능하다.

## 2 주요 내용 요약

이 표준은 분산원장기술을 활용한 온라인투표 시스템의 모델을 제시하고 해당 모델에 근거한 투표 절차 상의 잠재적인 보안 위협을 크게 5 가지 범주(데이터 기밀성, 데이터 무결성, 서비스 가용성, 비인가된 접근, 악의적인 행동)로 분류하여 분석하고 그에 따라 보안 위협을 최소화 할 수 있는 대응 방안을 포함한다.

## 3 인용 표준과의 비교

### 3.1 인용 표준과의 관련성

해당 사항 없음

### 3.2 인용 표준과 본 표준의 비교표

해당 사항 없음

# Preface

## 1 Purpose

The purpose of this standard is to identify and define security threats to online voting using distributed ledger technology (DLT) based on telecommunication/ICT infrastructure and client·server and to suggest countermeasures against security threats. This standard is applicable to the establishment and operation of online voting system using distributed ledger technology in all industries.

## 2 Summary

This standard proposes a model of an online voting system using distributed ledger technology, analyzes potential security threats to the voting process based on that model in 5 categories (data confidentiality, data integrity, service availability, unauthorized access, malicious behavior), and includes countermeasures which mitigate security threats.

## 3 Relationship to Reference Standards

None

# 목 차

# 분산원장기술을 활용한 온라인투표 모델 및 보안 위협 대응

# (Security threats to online voting using distributed ledger technology)

## 1 적용 범위

본 표준의 적용 범위는 분산원장기술을 활용한 온라인투표에 관한 보안 위협을 식별하고 최소한의 대응 방안을 제시하는 것으로서 다음과 같은 조건을 만족하는 온라인투표 시스템의 모델로 한정한다.[1]

- 정보통신 인프라(Telecommunication/ICT infrastructure) 및 클라이언트·서버 기반의 분산원장기술을 활용한 온라인투표 시스템[1]

## 2 인용 표준

- 해당 사항 없음

## 3 용어 정의

### 3.1 온라인 투표(Online Voting)

정보통신 인프라 기반의 전자적인 방법을 활용하여 기표 및 개표 업무를 보조하거나 처리하는 투표[1]

### 3.2 분산 원장(Distributed Ledger)

물리적으로 분리된 장소(예: 국가, 조직 등)에서 합의에 의해 복제, 공유, 동기화 및 저장되는 전자적인 데이터[1]

### 3.3 노드(Node)

분산 원장을 유지 및 관리하는 데이터베이스 서버[1]

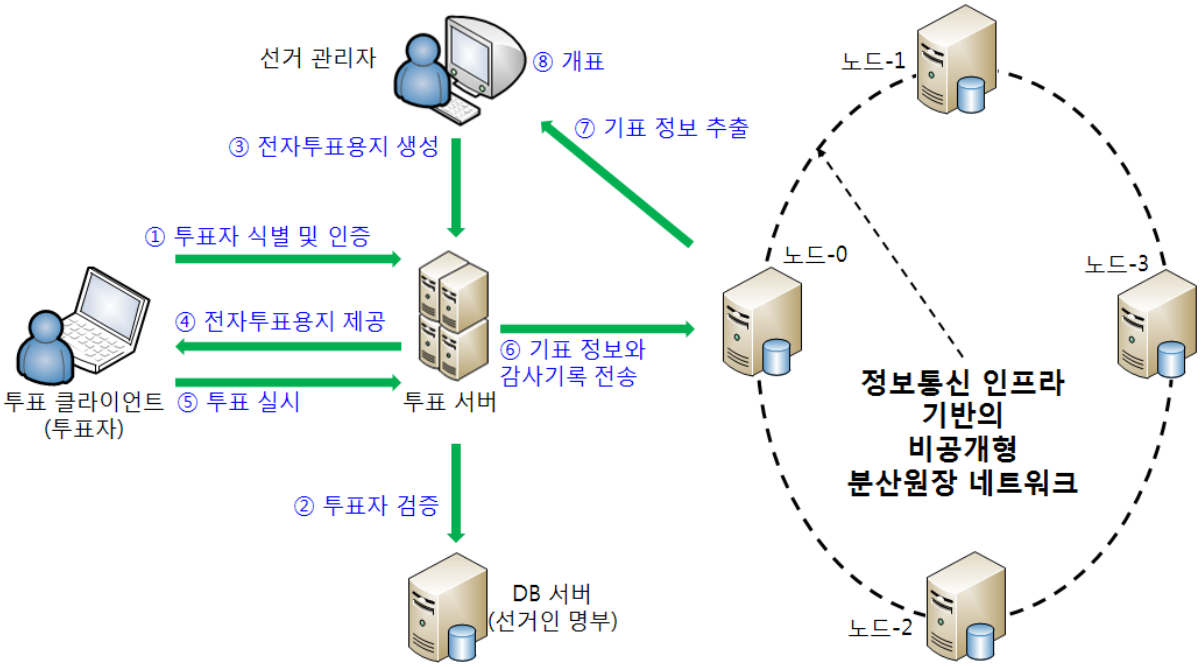
## 4 약어

| | |
|---|---|
| DLT | Distributed Ledger Technology |
| APT | Advanced Persistent Threat |
| IT | Information Technology |

| | |
|---|---|
| PC | Personal Computer |
| DLN | Distributed Ledger Network |
| DDoS | Distributed Denial of Service |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| PKI | Public Key Infrastructure |
| IP | Internet Protocol |
| MAC | Media Access Control |
| NAC | Network Access Control |
| PIN | Personal Identification Number |

## 5 온라인투표 시스템의 모델

정보통신 인프라 기반의 DLT 를 활용한 온라인투표 시스템의 다양한 이용 사례를 분석한 결과 아래의 (그림 5-1)과 같은 모델을 제시한다. 본 표준에서 제시하는 DLT 를 활용한 온라인 투표 시스템 모델의 주요 구성 요소는 투표 클라이언트(투표자), 선거 관리 클라이언트(선거 관리자), 투표 서버, 선거인 명부 서버, 비공개형 분산 원장 네트워크(노드(원장 서버), 데이터베이스, 합의 프로토콜 등) 등 이다.[2]




(그림 5-1) 분산원장기술을 활용한 온라인투표 시스템의 모델[2]

(그림 5-1)에서 보는 바와 같이 DLT 를 활용한 온라인투표 시스템 모델에 근거한 투표 과정은 다음과 같이 설명할 수 있다.[2]

- 1단계 : 투표 서버는 투표자의 신원을 확인하고 인증한다.
- 2단계 : 투표 서버는 선거인 명부를 통하여 투표자의 투표권을 검증한다.
- 3단계 : 선거 관리자는 전자 투표용지를 생성한다.
- 4단계 : 투표 서버는 생성된 전자 투표용지를 투표자에게 제공한다.
- 5단계 : 투표자는 투표 클라이언트에 제공된 전자 투표용지를 통하여 후보자를 선택하고 기표한다.
- 6단계 : 분산 원장 네트워크는 투표 서버로부터 전송된 투표 정보와 감사 기록을 저장한다.
- 7단계 : 선거 관리자는 분산 원장 네트워크로부터 투표 정보를 추출한다.
- 8단계 : 선거 관리자는 개표를 한다.

## 6 보안 위협

본 장에서는 DLT 를 활용한 온라인투표 모델에 근거한 온라인투표 과정에서 발생할 수 있는 잠재적인 보안 위협을 정보보호 측면에서 식별한다. 또한 보안 위협은 데이터 기밀성에 대한 위협, 데이터 무결성에 대한 위협, 서비스 가용성에 대한 위협, 정보시스템에 대한 비인가된 접근, 악의적인 행동 등 크게 5 가지 범주로 분류한다.

본 장에서 식별하는 보안 위협과 상기 (그림 5-1)의 구성 요소 간의 대응 관계는 다음과 같다.

| 보안 위협 | | | (그림 5-1) 구성 요소 |
|---|---|---|---|
| 6.1 데이터 기밀성에 대한 위협 | 6.1.1 투표자의 개인정보 노출·유출 | 6.1.1.1 | '투표 클라이언트' |
| | | 6.1.1.2 | ① |
| | | 6.1.1.3 | ② |
| | 6.1.2 투표 정보 및 감사 기록 유출 | 6.1.2.1 | ⑤ |
| | | 6.1.2.2 | ⑥ |
| | | 6.1.2.3 | ⑥ |
| | | 6.1.2.4 | '노드' |
| | | 6.1.2.5 | '분산 원장 네트워크' |
| | 6.1.3 선거인 명부 유출 | 6.1.3.1 | 'DB 서버(선거인명부)' |
| 6.2 데이터 무결성에 대한 위협 | 6.2.1 전자투표용지 위변조 | 6.2.1.1 | ③, ④ |
| | 6.2.2 투표 정보 및 감사 기록 위변조 | 6.2.2.2 | ⑥ |
| | | 6.2.2.3 | '노드' |
| | | 6.2.2.4 | '분산 원장 네트워크' |
| | 6.2.3 선거인 명부 위변조 | 6.2.3.1 | 'DB 서버(선거인명부)' |
| 6.3 서비스 가용성에 대한 위협 | 6.3.1 분산 원장 네트워크 가용성 저하 | 6.3.1.1 | '분산 원장 네트워크' |
| | | 6.3.1.2 | '노드' |
| | 6.3.2 투표 서버 가용성 저하 | 6.3.2.1 | '투표 서버' |

| | | | |
|---|---|---|---|
| | 6.3.3 선거인 명부 데이터베이스 가용성 저하 | 6.3.3.1 | ‘DB 서버(선거인명부)’ |
| 6.4 비인가된 접근 | 6.4.1 선거인 명부에 대한 비인가된 접근 | 6.4.1.1 | ‘DB 서버(선거인명부)’ |
| | 6.4.2 투표 서버에 대한 비인가된 접근 | 6.4.2.1 | ‘투표 서버’ |
| | 6.4.3 분산 원장 네트워크에 대한 비인가된 접근 | 6.4.3.1 | ‘분산 원장 네트워크’ |
| | | 6.4.3.2 | ‘노드’ |
| 6.5 악의적인 행동 | 6.5.1 전자투표용지 생성 부인 | 6.5.1.1 | ③ |
| | 6.5.2 이중 투표 | 6.5.2.1 | ‘투표 클라이언트(투표자)’ |
| | 6.5.3 기표 부인 | 6.5.3.1 | ⑤ |
| | 6.5.4 악성코드 감염 | 6.5.4.1 | ‘투표 클라이언트(투표자)’, ‘선거관리자’, ‘투표 서버’, ‘분산 원장 네트워크’, ⑥, ⑦ |
| | | 6.5.4.2 | ‘투표 클라이언트(투표자)’, ‘선거관리자’ |
| | 6.5.5 강압에 의한 투표 | 6.5.5.1 | ⑤ |
| | 6.5.6 신원 도용에 의한 부정 투표 | 6.5.6.1 | ①, ⑤ |

## 6.1 데이터 기밀성에 대한 위협

본 절에서는 침해사고(예: APT 공격 등) 및 IT 재해(예: 사람에 의한 재해 등)로 인하여 DLT 를 활용한 온라인투표 시스템을 구성하는 주요 정보시스템에서 발생할 수 있는 데이터 기밀성 위협을 식별 및 설명한다.

### 6.1.1 투표자의 개인정보 노출·유출

6.1.1.1 투표자가 사용하는 투표 클라이언트(PC, 응용프로그램 등)를 통하여 투표자의 개인정보(예: 고유식별정보, 성명 등)와 인증정보(예: 아이디, 패스워드 등)가 노출 및 유출될 수 있다. ((그림 5-1)의 ‘투표 클라이언트’ 참조)

6.1.1.2 투표 서버가 투표자의 신원을 확인하고 인증하는 과정에서 투표자가 사용하는 투표 클라이언트와 투표 서버 간의 전송 구간에서 개인정보(예: 고유식별정보, 성명 등) 및 인증정보(예: 아이디, 패스워드 등)가 유출될 수 있다. ((그림 5-1)의 ① 참조)

6.1.1.3 투표 서버가 투표자의 투표권을 검증하는 과정에서 투표 서버와 선거인 명부 서버 간의 전송 구간에서 개인정보(예: 고유식별정보, 성명 등)가 유출될 수 있다. ((그림 5-1)의 ② 참조)

### 6.1.2 투표 정보 및 감사 기록 유출

6.1.2.1 투표자가 사용하는 투표 클라이언트와 투표 서버 간의 전송 구간에서 투표자가 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)가 유출될 수 있다. ((그림 5-1)의 ⑤ 참조)

6.1.2.2 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간에서 투표자가 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)가 유출될 수 있다. ((그림 5-1)의 ⑥ 참조)

6.1.2.3 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간에서 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록이 유출될 수 있다. 감사 기록은 다음과 같은 내용을 포함할 수 있다. ((그림 5-1)의 ⑥ 참조)

- 투표자 신원 확인 및 인증 결과
- 선거인 명부 대조 등을 통한 투표자의 투표권 검증 결과
- 선거 관리자에 의한 전자투표용지 생성 결과
- 투표자에 의한 기표(예: 후보자 선택 등) 결과
- 분산 원장 네트워크(DLN)에 기표된 전자투표용지 저장 여부
- 기표된 전자투표용지 개표 여부 등

6.1.2.4 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스로부터 다음과 같은 내용을 포함한 대량의 중요 정보가 유출될 수 있다. ((그림 5-1)의 '노드' 참조)

- 모든 투표자가 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)
- 모든 투표자의 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록 등

6.1.2.5 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 간의 전송 구간에서 다음과 같은 내용을 포함한 중요 정보가 유출될 수 있다. ((그림 5-1)의 '분산 원장 네트워크' 참조)

- 투표자가 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)
- 투표자의 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록 등

### 6.1.3 선거인 명부 유출

6.1.3.1 선거인 명부 서버 및 데이터베이스에 저장되어 있는 대량의 개인정보(예: 고유식별정보, 성명 등)가 포함된 선거인 명부가 유출될 수 있다. ((그림 5-1)의 'DB서버(선거인명부)' 참조)

## 6.2 데이터 무결성에 대한 위협

본 절에서는 침해사고(예: APT 공격, 랜섬웨어 등) 및 IT 재해로 인하여 DLT 를 활용한 온라인투표 시스템을 구성하는 주요 정보시스템에서 발생할 수 있는 데이터 무결성 위협을 식별 및 설명한다.

### 6.2.1 전자투표용지 위변조

6.2.1.1 선거 관리자가 선거 관리 클라이언트(PC, 응용프로그램 등)를 통하여 생성한 전자투표용지가 선거 관리 클라이언트와 투표 서버 간의 전송 구간, 투표 서버와 투표 클라이언트 간의 전송 구간에서 위변조 될 수 있다. 전자투표용지는 다음과 같은 내용을 포함할 수 있다. ((그림 5-1)의 ③, ④ 참조)

- 후보자 목록 등

### 6.2.2 투표 정보 및 감사 기록 위변조

6.2.2.1 투표자가 투표 클라이언트를 통하여 기표한 전자투표용지가 투표 서버와 투표 클라이언트 간의 전송 구간, 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간에서 위변조 될 수 있다. 투표자가 기표한 전자투표용지는 다음과 같은 내용을 포함할 수 있다. ((그림 5-1)의 ⑤, ⑥ 참조)

- 후보자 목록, 후보자 선택 정보 등

6.2.2.2 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간에서 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록(6.1.2.3 참조)이 위변조 될 수 있다. ((그림 5-1)의 ⑥ 참조)

6.2.2.3 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스에 저장되어 있는 대량의 중요 정보(6.1.2.4 참조)가 삭제될 수 있다. ((그림 5-1)의 '노드' 참조)

6.2.2.4 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 간의 전송 구간에서 중요 정보(6.1.2.5 참조)가 위변조 될 수 있다. ((그림 5-1)의 '분산 원장 네트워크' 참조)

### 6.2.3 선거인 명부 위변조

6.2.3.1 선거인 명부 서버 및 데이터베이스에 저장되어 있는 대량의 선거인 명부가 위변조 및 삭제될 수 있다. 선거인 명부에는 다음과 같은 개인정보가 포함될 수 있다. ((그림 5-1)의 'DB서버(선거인명부)' 참조)

- 고유식별정보(예: 주민등록번호 등), 성명, 주소 등

## 6.3 서비스 가용성에 대한 위협

본 절에서는 침해사고(예: DDoS 공격 등) 및 IT 재해로 인하여 DLT 를 활용한 온라인투표 시스템을 구성하는 주요 정보시스템에서 발생할 수 있는 가용성 위협을 식별 및 설명한다.

### 6.3.1 분산 원장 네트워크 가용성 저하

6.3.1.1 대량의 중요 정보(6.1.2.4 참조)를 합의에 의해 처리(복제, 공유, 동기화 등)하는 분산 원장 네트워크(DLN) 인프라의 가용성이 저하될 수 있다. ((그림 5-1)의 '분산 원장 네트워크' 참조)

6.3.1.2 대량의 중요 정보(6.1.2.4 참조)를 저장 및 유지하는 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스의 가용성이 저하될 수 있다. ((그림 5-1)의 '노드' 참조)

### 6.3.2 투표 서버 가용성 저하

6.3.2.1 투표 클라이언트(투표자), 선거 관리 클라이언트(선거 관리자), 선거인 명부 서버, 분산 원장 네트워크(DLN) 등과 연계된 투표 서비스(예: 투표자 신원 확인 및 인증, 투표자의 투표권 검증, 전자투표용지 생성 및 전송, 감사 기록 생성 등)를 제공하는 투표 서버의 가용성이 저하될 수 있다. ((그림 5-1)의 '투표 서버' 참조)

### 6.3.3 선거인 명부 데이터베이스 가용성 저하

6.3.3.1 대량의 선거인 명부를 처리(예: 개인정보 조회 등)하는 선거인 명부 서버 및 데이터베이스의 가용성이 저하될 수 있다. ((그림 5-1)의 'DB서버(선거인명부)' 참조)

## 6.4 비인가된 접근

본 절에서는 침해사고(예: APT 공격 등) 및 IT 재해(예: 사람에 의한 재해)로 인하여 DLT 를 활용한 온라인투표 시스템을 구성하는 주요 정보시스템을 대상으로 하는 비인가된 접근을 식별 및 설명한다.

### 6.4.1 선거인 명부에 대한 비인가된 접근

6.4.1.1 대량의 선거인 명부를 처리(예: 개인정보 조회 및 저장 등)하고 있는 선거인 명부 서버 및 데이터베이스를 대상으로 비인가된 접근이 이루어질 수 있다. ((그림 5-1)의 'DB서버(선거인명부)' 참조)

### 6.4.2 투표 서버에 대한 비인가된 접근

6.4.2.1 투표 클라이언트(투표자), 선거 관리 클라이언트(선거 관리자), 선거인 명부 서버, 분산 원장 네트워크(DLN) 등과 연계된 투표 서비스(예: 투표자 신원 확인 및 인증, 투표자의 투표권 검증, 전자투표용지 생성 및 전송, 감사 기록 생성 등)를 제공하는 투표 서버를 대상으로 비인가된 접근이 이루어질 수 있다. ((그림 5-1)의 '투표 서버' 참조)

### 6.4.3 분산 원장 네트워크에 대한 비인가된 접근

6.4.3.1 대량의 중요 정보(6.1.2.4 참조)를 합의에 의해 처리(복제, 공유, 동기화 등)하는 분산 원장 네트워크(DLN) 인프라를 대상으로 비인가된 접근이 이루어질 수 있다. ((그림 5-1)의 '분산 원장 네트워크' 참조)

6.4.3.2 대량의 중요 정보(6.1.2.4 참조)를 저장 및 유지하는 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스를 대상으로 비인가된 접근이 이루어질 수 있다. ((그림 5-1)의 '노드' 참조)

## 6.5 악의적인 행동

본 절에서는 투표자, 선거 관리자, 선거 관련 이해 당사자, 소프트웨어 개발자 등에 의하여 발생할 수 있는 악의적인 행동을 식별 및 설명한다.

### 6.5.1 전자투표용지 생성 부인

6.5.1.1 선거 관리자는 선거 관리 클라이언트(예: PC 등) 및 투표 서버를 통하여 투표자에게 제공한 전자투표용지의 생성(Generating) 사실을 부인(Repudiation)할 수 있다. ((그림 5-1)의 ③ 참조)

### 6.5.2 이중 투표

6.5.2.1 투표자는 투표 클라이언트(예: PC, 스마트폰 등) 및 투표 서버를 통하여 이중(Multiple) 투표를 할 수 있다. ((그림 5-1)의 '투표 클라이언트(투표자)' 참조)

### 6.5.3 기표 부인

6.5.3.1 투표자는 투표 클라이언트(예: PC, 스마트폰 등)를 통하여 전자투표용지에 기표(예: 후보자 선택 등)한 사실을 부인(Repudiation)할 수 있다. ((그림 5-1)의 ⑤ 참조)

### 6.5.4 악성코드 감염

6.5.4.1 DLT를 활용한 온라인투표 시스템과 관련된 소프트웨어(예: 클라이언트용 투표 프로그램, 중요 정보 전송 모듈, 개표용 프로그램 등)의 개발 및 배포 과정에서 악성코드가 삽입될 수 있다. ((그림 5-1)의 '투표 클라이언트(투표자)', '선거 관리자', '투표 서버', '분산 원장 네트워크', ⑥, ⑦ 참조)

6.5.4.2 투표자가 사용하는 투표 클라이언트(예: PC, 스마트폰 등), 선거 관리자가 사용하는 선거 관리 클라이언트(예: PC 등) 등이 악성코드에 감염될 수 있다. ((그림 5-1)의 '투표 클라이언트(투표자)', '선거 관리자' 참조)

### 6.5.5 강압에 의한 투표

6.5.5.1 선거 관련 이해 당사자(예: 후보자의 지지자 등) 등의 강압에 의하여 투표자는 원하지 않는 기표(예: 후보자 선택 등)를 할 수 있다. ((그림 5-1)의 ⑤ 참조)

### 6.5.6 신원 도용에 의한 부정 투표

6.5.6.1 타인의 신원을 도용한 부정 투표를 할 수 있다. ((그림 5-1)의 ①, ⑤ 참조)

## 7 보안 위협에 대한 대응 방안

본 장에서는 제 6 장에서 DLT 를 활용한 온라인투표 모델에 근거한 투표 과정에서 발생할 수 있는 잠재적인 보안 위협을 분석한 결과를 토대로 그에 대한 관리적·기술적 대응 방안을 제시한다.

### 7.1 데이터 기밀성 위협에 대한 대응 방안

본 절에서는 침해사고(예: APT 공격 등) 및 IT 재해(예: 사람에 의한 재해 등)로 인하여 DLT 를 활용한 온라인 투표 시스템을 구성하는 주요 정보시스템에서 발생할 수 있는 데이터 기밀성 위협에 대한 대응 방안을 제시한다.

### 7.1.1 투표자 개인정보 노출·유출에 대한 대응 방안

7.1.1.1 투표자가 사용하는 투표 클라이언트(PC 등)에 투표자의 개인정보(예: 고유식별정보, 성명 등)와 인증정보(예: 패스워드 등)를 저장할 경우 안전한 암호 알고리즘(예: AES-128, RSA-2048, SHA-256 이상 등)으로 암호화할 필요가 있다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, [4], [5]의 제6조(개인정보의 암호화), [6]의 제7조(개인정보의 암호화))

7.1.1.2 투표자가 사용하는 투표 클라이언트(PC, 응용프로그램 등)를 통하여 투표자의 개인정보(예: 고유식별정보, 성명 등)와 인증정보(예: 패스워드 등)를 출력할 경우 마스킹(예: '*') 처리

가 필요하다. (근거 : [5]의 제10조(개인정보 표시 제한 보호조치))

7.1.1.3 개인정보(예: 고유식별정보, 성명 등) 및 인증정보(예: 아이디, 패스워드 등)를 안전하게 전송하기 위하여 다음과 같은 전송 구간에 암호화(예: SSL/TLS, 암호화 응용프로그램 등) 조치가 필요하다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, 10.4.1 네트워크 접근, [4], [5]의 제6조(개인정보의 암호화), [6]의 제7조(개인정보의 암호화))

- 투표 클라이언트와 투표 서버 간의 전송 구간
- 투표 서버와 선거인 명부 서버 간의 전송 구간 등

### 7.1.2 투표 정보 및 감사 기록 유출에 대한 대응 방안

7.1.2.1 투표 정보(예: 후보자 선택 정보 등) 및 감사 기록(6.1.2.3 참조)을 안전하게 전송하기 위하여 다음과 같은 전송 구간에 암호화(예: SSL/TLS, 암호화 응용프로그램 등) 조치가 필요하다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, 10.4.1 네트워크 접근, [4])

- 투표 클라이언트와 투표 서버 간의 전송 구간
- 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간
- 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 간의 전송 구간 등

7.1.2.2 대량의 중요 정보(6.1.2.4 참조)를 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스에 저장 및 유지할 경우 안전한 암호 알고리즘(예: AES-128, RSA-2048 이상 등)으로 암호화할 필요가 있다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, [4])

### 7.1.3 선거인 명부 유출에 대한 대응 방안

7.1.3.1 대량의 개인정보(예: 고유식별정보 등)가 포함된 선거인 명부를 선거인 명부 서버 및 데이터베이스에 저장 및 유지할 경우 안전한 암호 알고리즘(예: AES-128, RSA-2048 이상 등)으로 암호화할 필요가 있다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, [4], [5]의 제6조(개인정보의 암호화), [6]의 제7조(개인정보의 암호화))

## 7.2 데이터 무결성 위협에 대한 대응 방안

본 절에서는 침해사고(예: APT 공격, 랜섬웨어 등) 및 IT 재해로 인하여 DLT 를 활용한 온라인 투표 시스템을 구성하는 주요 정보시스템에서 발생할 수 있는 데이터 무결성 위협에 대한 대응 방안을 제시한다.

### 7.2.1 전자투표용지 위변조에 대한 대응 방안

7.2.1.1 선거 관리자가 선거 관리 클라이언트를 통하여 생성한 전자투표용지(후보자 목록 등 포함)를 안전하게 전송하기 위하여 다음과 같은 전송 구간에 암호화(예: SSL/TLS, 암호화 응용프로그램 등) 조치가 필요하다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, 10.4.1 네트워

크 접근, [4])
- 선거 관리 클라이언트와 투표 서버 간의 전송 구간
- 투표 서버와 투표 클라이언트 간의 전송 구간 등

### 7.2.2 투표 정보 및 감사 기록 위변조에 대한 대응 방안

7.2.2.1 투표자가 투표 클라이언트를 통하여 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)는 안전한 암호 알고리즘(예: PKI 기반 등)으로 암호화하여 저장할 필요가 있다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, [4])

7.2.2.2 투표자가 투표 클라이언트를 통하여 기표한 전자투표용지(후보자 목록, 후보자 선택 정보 등 포함)를 안전하게 전송하기 위하여 다음과 같은 전송 구간에 암호화(예: SSL/TLS, 암호화 응용프로그램 등) 조치가 필요하다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, 10.4.1 네트워크 접근, [4])
- 투표 서버와 투표 클라이언트 간의 전송 구간
- 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간
- 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 간의 전송 구간 등

7.2.2.3 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록(6.1.2.3 참조)을 안전하게 전송하기 위하여 다음과 같은 전송 구간에 암호화(예: SSL/TLS, 암호화 응용프로그램 등) 조치가 필요하다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, 10.4.1 네트워크 접근, [4])
- 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간
- 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 간의 전송 구간 등

7.2.2.4 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스에 저장 및 유지되고 있는 대량의 중요 정보(6.1.2.4 참조)에 대한 접근 권한(예: 신규 등록, 조회, 변경, 삭제 등)을 차등 부여하거나 변경 및 삭제 권한을 엄격히 제한할 필요가 있다. (근거 : [3]의 보호대책 10.2.1 사용자 등록 및 권한 부여)

### 7.2.3 선거인 명부 위변조에 대한 대응 방안

7.2.3.1 대량의 선거인 명부 내 개인정보(예: 고유식별정보)를 선거인 명부 서버 및 데이터베이스에 저장할 경우 안전한 암호 알고리즘(예: AES-128, RSA-2048 이상 등)으로 암호화할 필요가 있다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, [4])

7.2.3.2 선거인 명부 서버 및 데이터베이스에 저장되고 있는 대량의 선거인 명부 내 개인정보(예: 고유식별정보, 성명, 주소 등)에 대한 접근 권한(예: 신규 등록, 조회, 변경, 삭제 등)을 차등 부여하거나 변경 및 삭제 권한을 엄격히 제한할 필요가 있다. (근거 : [3]의 보호대책 10.2.1 사용자 등록 및 권한 부여)

## 7.3 서비스 가용성 위협에 대한 대응 방안

본 절에서는 침해사고(예: DDoS 공격 등) 및 IT 재해로 인하여 DLT를 활용한 온라인 투표 시스템을 구성하는 주요 정보시스템에서 발생할 수 있는 가용성 위협에 대한 대응 방안을 제시한다.

### 7.3.1 분산 원장 네트워크 가용성 저하에 대한 대응 방안

7.3.1.1 대량의 중요 정보(6.1.2.4 참조)를 합의에 의해 처리(복제, 공유, 동기화 등)하는 분산 원장 네트워크(DLN) 인프라의 가용성 저하에 대한 대응 방안에 다음과 같은 내용을 포함시킬 필요가 있다. (근거 : [3]의 보호대책 10.4.2 서버 접근, 11.2.2 보안시스템 운영, 11.2.3 성능 및 용량 관리)

- 지속적인 네트워크 성능 및 용량 모니터링
- 네트워크 인프라(예: 백본, 회선 등) 이중화 구성
- DDoS 대응 시스템 운용 등

7.3.1.2 대량의 중요 정보(6.1.2.4 참조)를 저장 및 유지하는 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스의 가용성 저하에 대한 대응 방안에 다음과 같은 내용을 포함시킬 필요가 있다. (근거 : [3]의 보호대책 11.2.2 보안시스템 운영, 11.2.3 성능 및 용량 관리)

- 지속적인 성능 및 용량(예: CPU, 메모리, 네트워크, 저장매체 등) 모니터링
- DDoS 대응 시스템 운용 등

### 7.3.2 투표 서버 가용성 저하에 대한 대응 방안

7.3.2.1 투표 클라이언트(투표자), 선거 관리 클라이언트(선거 관리자), 선거인 명부 서버, 분산 원장 네트워크(DLN) 등과 연계된 투표 서비스(예: 투표자 신원 확인 및 인증, 투표자의 투표권 검증, 전자투표용지 생성 및 전송, 감사 기록 생성 등)를 제공하는 투표 서버의 가용성 저하에 대한 대응 방안에 다음과 같은 내용을 포함시킬 필요가 있다. (근거 : [3]의 보호대책 10.4.2 서버 접근, 11.2.2 보안시스템 운영, 11.2.3 성능 및 용량 관리)

- 지속적인 성능 및 용량(예: CPU, 메모리, 네트워크, 저장매체 등) 모니터링
- 투표 서버 이중화 구성
- DDoS 대응 시스템 운용 등

### 7.3.3 선거인 명부 데이터베이스 가용성 저하에 대한 대응 방안

7.3.3.1 대량의 선거인 명부를 처리(예: 개인정보 조회 등)하는 선거인 명부 서버 및 데이터베이스의 가용성 저하에 대한 대응 방안에 다음과 같은 내용을 포함시킬 필요가 있다. (근거 : [3]의 보호대책 10.4.2 서버 접근, 11.2.2 보안시스템 운영, 11.2.3 성능 및 용량 관리)

- 지속적인 성능 및 용량(예: CPU, 메모리, 네트워크, 저장매체 등) 모니터링
- 선거인 명부 서버 및 데이터베이스 이중화 구성
- DDoS 대응 시스템 운용 등

## 7.4 비인가된 접근에 대한 대응 방안

본 절에서는 침해사고(예: APT 공격 등) 및 IT 재해(예: 사람에 의한 재해)로 인하여 DLT 를 활용한 온라인 투표 시스템을 구성하는 주요 정보시스템을 대상으로 하는 비인가된 접근에 대한 대응 방안을 제시한다.

### 7.4.1 선거인 명부를 대상으로 하는 비인가된 접근에 대한 대응 방안

7.4.1.1 대량의 선거인 명부를 처리(예: 개인정보 조회 및 저장 등)하고 있는 선거인 명부 서버 및 데이터베이스를 대상으로 하는 비인가된 접근에 대한 대응 방안에 다음과 같은 내용을 포함시킬 필요가 있다. (근거 : [3]의 보호대책 10.2.1 사용자 등록 및 권한 부여, 10.3.1 사용자 인증, 10.3.2 사용자 식별, 10.4.1 네트워크 접근, 10.4.2 서버 접근)

- 사용자 식별 및 인증
- 사용자별 접근 권한 차등 부여
- 네트워크 또는 호스트 기반 침입차단시스템(방화벽) 등을 통한 접근 통제 등

### 7.4.2 투표 서버를 대상으로 하는 비인가된 접근에 대한 대응 방안

7.4.2.1 투표 클라이언트(투표자), 선거 관리 클라이언트(선거 관리자), 선거인 명부 서버, 분산 원장 네트워크(DLN) 등과 연계된 투표 서비스(예: 투표자 신원 확인 및 인증, 투표자의 투표권 검증, 전자투표용지 생성 및 전송, 감사 기록 생성 등)를 제공하는 투표 서버를 대상으로 하는 비인가된 접근에 대한 대응 방안에 다음과 같은 내용을 포함시킬 필요가 있다. (근거 : [3]의 보호대책 10.2.1 사용자 등록 및 권한 부여, 10.3.1 사용자 인증, 10.3.2 사용자 식별, 10.4.1 네트워크 접근, 10.4.2 서버 접근)

- 사용자 식별 및 인증
- 사용자별 접근 권한 차등 부여
- 네트워크 또는 호스트 기반 침입차단시스템(방화벽) 등을 통한 접근 통제 등

### 7.4.3 분산 원장 네트워크를 대상으로 하는 비인가된 접근에 대한 대응 방안

7.4.3.1 대량의 중요 정보(6.1.2.4 참조)를 합의에 의해 처리(복제, 공유, 동기화 등)하는 분산 원장 네트워크(DLN) 인프라를 대상으로 하는 비인가된 접근에 대한 대응 방안에 다음과 같은 내용을 포함시킬 필요가 있다. (근거 : [3]의 보호대책 10.4.1 네트워크 접근)

- 하드웨어 주소(MAC Address) 사전 등록에 의한 접근 통제
- 네트워크접근통제(NAC)시스템, 네트워크 기반 침입차단시스템(방화벽) 등을 통한 접근 통제 등

7.4.3.2 대량의 중요 정보(6.1.2.4 참조)를 저장 및 유지하는 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스를 대상으로 하는 비인가된 접근에 대한 대응 방안에 다음과 같은 내용을 포함시킬 필요가 있다. (근거 : [3]의 보호대책 10.2.1 사용자 등록 및 권한 부여, 10.3.1 사용자 인증, 10.3.2 사용자 식별, 10.4.1 네트워크 접근, 10.4.2 서버 접근)

- 사용자 식별 및 인증
- 사용자별 접근 권한 차등 부여
- 노드(원장 서버) 간의 양방향 인증
- 네트워크 또는 호스트 기반 침입차단시스템(방화벽) 등을 통한 접근 통제 등

## 7.5 악의적인 행동에 대한 대응 방안

본 절에서는 투표자, 선거 관리자, 선거 관련 이해 당사자, 소프트웨어 개발자 등에 의하여 발생할 수 있는 악의적인 행동에 대한 대응 방안을 제시한다.

### 7.5.1 전자투표용지 생성 부인에 대한 대응 방안

7.5.1.1 선거 관리자가 선거 관리 클라이언트(예: PC 등) 및 투표 서버를 통하여 투표자에게 제공한 전자투표용지의 생성(Generating) 사실에 대하여 부인(Repudiation)할 수 없도록 다음과 같은 내용을 고려한 조치가 필요하다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, [4])

- 전자투표용지 생성시 선거 관리자의 전자서명(PKI 기반) 징구 등

### 7.5.2 이중 투표에 대한 대응 방안

7.5.2.1 투표자가 투표 클라이언트(예: PC, 스마트폰 등) 및 투표 서버를 통하여 이중(Multiple) 투표를 할 수 없도록 다음과 같은 내용을 고려한 조치가 필요하다. (근거 : [3]의 보호대책 11.6.2 로그기록 및 보존, 11.6.3 접근 및 사용 모니터링)

- 감사 기록(예: 투표자 신원 확인 및 인증 결과, 선거인 명부 대조 등을 통한 투표자의 투표권 검증 결과, 투표자에 의한 기표(예: 후보자 선택 등) 결과)에 근거한 전자투표용지 중복 생성 통제 등

### 7.5.3 기표 부인에 대한 대응 방안

7.5.3.1 투표자가 투표 클라이언트(예: PC, 스마트폰 등)를 통하여 전자투표용지에 기표(예: 후보자 선택 등)한 사실을 부인(Repudiation)할 수 없도록 다음과 같은 내용을 고려한 조치가 필요하다. (근거 : [3]의 보호대책 9.1.1 암호 정책 수립, [4])

- 투표자가 전자투표용지에 기표(예: 후보자 선택 등)시 투표자의 전자서명(PKI 기반) 징구 등

### 7.5.4 악성코드 감염에 대한 대응 방안

7.5.4.1 DLT를 활용한 온라인투표 시스템과 관련된 소프트웨어(예: 클라이언트용 투표 프로그램, 중요 정보 전송 모듈, 개표용 프로그램 등)에 악성코드가 삽입되지 않도록 다음과 같은 내용을 고려한 조치가 필요하다. (근거 : [3]의 보호대책 8.2.1 구현 및 시험, 8.2.3 운영 환경 이관)

- 개발 환경에서 운영 환경으로 소프트웨어 이관시 보안 통제(예: 개발자의 이관 업무 겸직 금지, 이관시 결재권자에 의한 승인 등) 이행
- 소프트웨어 개발(유지보수)시 주기적인 소스코드 취약점 진단 및 후속조치 이행 등

7.5.4.2 투표자가 사용하는 투표 클라이언트(예: PC, 스마트폰 등), 선거 관리자가 사용하는 선거 관리 클라이언트(예: PC 등) 등이 악성코드에 감염되지 않도록 다음과 같은 내용을 고려한 조치가 필요하다. (근거 : [3]의 보호대책 11.5.1 악성코드 통제)

- 백신 프로그램 운용(예: 실시간 악성코드 감시 및 치료, 주기적인 악성코드 점검, 백신엔진 최신 버전 유지 등) 등

### 7.5.5 강압에 의한 투표 대응 방안

7.5.5.1 선거 관련 이해 당사자(예: 후보자의 지지자 등) 등의 강압에 의하여 투표자의 원하지 않는 기표(예: 후보자 선택 등)에 대응할 수 있도록 다음과 같은 내용을 고려한 조치가 필요하다. (근거 : [3]의 보호대책 10.4.3 응용 프로그램 접근, [7]의 제368조의4(전자적 방법에 의한 의결권의 행사), [8]의 제13조(전자적 방법에 의한 의결권의 행사))

- 투표자가 사용하는 투표 클라이언트(예: PC, 스마트폰 등)를 안전한 장소(예: 자택, 직장, 투표소 등)에 위치한 단말기로 제한(예: IP 주소 또는 단말기 사전 등록 등)

※ 상법 시행령 발췌

『상법 시행령』 제13조(전자적 방법에 의한 의결권의 행사) ① 법 제368조의4에 따라 주주가 의결권을 전자적 방법으로 행사(이하 이 조에서 "전자투표"라 한다)하는 경우 주주는 「전자서명법」 제2조제3호에 따른 공인전자서명을 통하여 주주 확인 및 전자투표를 하여야 한다.

② 법 제368조의4에 따라 전자적 방법으로 의결권을 행사할 수 있음을 정한 회사는 주주총회 소집의 통지나 공고에 다음 각 호의 사항을 포함하여야 한다.

1. 전자투표를 할 인터넷 주소
2. 전자투표를 할 기간(전자투표의 종료일은 주주총회 전날까지로 하여야 한다)
3. 그 밖에 주주의 전자투표에 필요한 기술적인 사항

③ 전자투표를 한 주주는 해당 주식에 대하여 그 의결권 행사를 철회하거나 변경하지 못한다.

④ 회사는 전자투표의 효율성 및 공정성을 확보하기 위하여 전자투표를 관리하는 기관을 지정하여 주주 확인절차 등 의결권 행사절차의 운영을 위탁할 수 있다.

⑤ 회사, 제4항에 따라 지정된 전자투표를 관리하는 기관 및 전자투표의 운영을 담당하는 자는 주주총회에서 개표가 있을 때까지 전자투표의 결과를 누설하거나 직무상 목적 외로 사용해서는

아니 된다.

### 7.5.6 신원 도용에 의한 부정 투표 대응 방안

7.5.6.1 타인의 신원을 도용한 부정 투표에 대응할 수 있도록 다음과 같은 인증 수단을 2가지 이상 조합하여 투표자 인증을 강화할 필요가 있다. (근거 : [3]의 보호대책 10.3.1 사용자 인증, [5]의 제4조(접근통제) ④항, [6]의 제6조(접근통제) ②항)

- 아이디/패스워드
- 개인식별번호(PIN)
- 생체 정보(예: 지문, 얼굴 등)
- PKI 기반 인증서(예: 공인인증서, 사설인증서) 등

# 부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 지식재산권 확약서 정보

- 해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

# 부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 시험인증 관련 사항

- 해당 사항 없음

# 부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 본 표준의 연계(family) 표준

- 해당 사항 없음

# 부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 참고 문헌

[1] Keundug Park, Changoh Kim, Heung Youl Youm, “ITU-T X.stov (Security threats to online voting using distributed ledger technology)”, Mar. 2018
[2] 박근덕, 김창오, 염흥열, “분산원장기술을 활용한 온라인투표 대한 보안 위협과 대응 방안”, 한국정보보호학회논문지, 제27권 제5호, pp. 1201-1216, 2017년 10월
[3] 한국인터넷진흥원, “정보보호관리체계(ISMS) 인증기준 세부점검항목”, 2013년 3월
[4] 한국인터넷진흥원, “암호 알고리즘 및 키 길이 이용 안내서”, 2013년 1월
[5] 방송통신위원회, “개인정보의 기술적·관리적 보호조치 기준(고시 제2015-3호)”, 2015년 5월
[6] 행정안전부, “개인정보의 안전성 확보조치 기준(고시 제2017-1호)”, 2017년 7월
[7] 법무부, “상법(법률 제13523호)”, 2015년 12월
[8] 법무부, “상법 시행령(대통령령 제28211호)”, 2017년 7월

# 부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 영문표준 해설서

- 해당 사항 없음

# 부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 표준의 이력

| 판수 | 채택일 | 표준번호 | 내용 | 담당 위원회 |
|---|---|---|---|---|
| 제1판 | 20xx.xx.xx | 제정<br>TTAx.xx-xx.xxxx | - | 개인정보보호/ID관리 및 블록체인보안 (PG502) |
| 오류정정 | | | | |
| 오류정정 | | | | |
| 제2판 | | | | |