Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.5, Oct. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.5.1201

분산 원장 기술을 활용한 온라인 투표에 대한 보안 위협과 대응 방안

박 근 덕,[1†] 김 창 오,[2] 염 흥 열[3‡]
[1]한국아이티평가원, [2]쿠팡, [3]순천향대학교

Countermeasures against Security Threats to Online Voting Using Distributed Ledger Technology

Keundug Park,[1†] ChangOh Kim,[2] Heung-youl Youm[3‡]
[1]KSEL, [2]Coupang, [3]Soonchunhyang University

요 약

최근 한국을 비롯한 전 세계적으로 많은 국가들이 분산 원장 기술(예: 블록체인)을 활용한 온라인 투표를 적극적으로 도입하여 이용하고 있으나, 현재 널리 보급된 정보통신 인프라 기반의 분산 원장 기술을 활용한 온라인 투표 시스템에 대한 잠재적인 보안 위협 분석이 미흡한 실정이다. 본 논문에서는 분산 원장 기술을 활용한 온라인 투표 시스템에 대한 모델을 제시하고 온라인 투표 과정에서 발생할 수 있는 보안 위협을 정보보호 측면에서 분석함으로서 그에 따른 대응 방안을 제시하고자 한다.

ABSTRACT

Recently, many countries around the world including Korea (Rep. of) have actively introduced online voting using distributed ledger technology (e.g. blockchain). However, online voting using distributed ledger technology based on the widely deployed telecommunication/ICT infrastructure. There is insufficient analysis of potential security threats. In this paper, we suggest a model for online voting system using distributed ledger technology and propose countermeasures by analyzing the security threats that may occur in online voting process in terms of information security.

Keywords: countermeasures, security threat, online voting, DLT(Distributed Ledger Technology), blockchain, ICT(Information and Communication Technologies), DLN(Distributed Ledger Network)

I. 서 론

분산 원장 기술(예: 블록체인 등)은 제3자 중개인이 필요 없는 혁신적인 금융·비금융 분야의 분산 서비스(예: 신원 관리, 신용 관리, 군중 기금, P2P 보험, 스마트 계약, 공급망 관리, 온라인 투표, 의료 기록 등)를 가능하게 하는 신흥 기술로서 다양한 응용 분야에서 주목 받고 있다. 분산 원장 기술(DLT, Distributed Ledger Technology)을 활용한 이러한 모든 서비스는 정보통신 인프라를 기반으로 한다.

또한 최근 한국정보화진흥원(NIA)에서 발표한 특별 보고서에 의하면 DLT를 활용한 비금융 분야 서비스 중에 가장 주목할 만한 것으로 온라인 투표를 선정하여 그에 대한 주요 이용 사례, 시사점 등 분석 자료를 제공함으로서 DLT를 활용한 온라인 투표의 도입 및 운용에 대한 선제적 검토가 필요함을 강조하고 있다.[13]

그리고 DLT를 활용한 온라인 투표는 많은 국가에서 DLT를 활용한 비금융 서비스 분야의 성공적인 사례

Received(07. 10. 2017), Modified(09. 15. 2017), Accepted(09. 27. 2017)
† 주저자, jacepark926@gmail.com
‡ 교신저자, hyyoum@sch.ac.kr(Corresponding author)

중 하나이지만, 정보통신 인프라를 기반으로 하고 있는 온라인 투표 과정에서 발생할 수 있는 잠재적인 보안 위협에 대한 분석은 매우 미흡한 실정이다.

최근 몇 년 동안 정보통신 인프라 기반의 다양한 애플리케이션과 서비스는 개인정보 등 중요정보 유출 및 서비스 중단 등의 보안사고 통하여 사회적·경제적으로 막대한 비용을 치룬 경험이 있다. 특히 최근에는 가상 화폐 거래소의 보안사고(가상 화폐 탈취, 개인정보 유출 등)가 끊임없이 발생하고 있고, 기업 내 중요한 정보를 볼모로 금전적 보상을 요구하는 랜섬웨어(예: 워너크라이, 페트야 등)가 기승을 부리고 있어 최신 기술과 관련된 보안 사고에 대한 대응 방안이 절실히 필요하다.[1][2]

따라서 본 논문의 제2장에서는 전 세계 주요 국가의 DLT를 활용한 온라인 투표 이용 사례를 설명하고 DLT를 활용한 온라인 투표 시스템의 모델을 제시한다. 제3장에서는 제2장에서 제시한 온라인 투표 모델에 근거한 투표 과정에서 발생할 수 있는 보안 위협을 식별하고, 제4장에서는 제3장에서 식별된 보안 위협에 대한 대응 방안을 제시하고자 한다.

II. 관련 연구

본 장에서는 전 세계 주요 국가의 DLT를 활용한 온라인 투표 이용 사례를 설명하고, DLT를 활용한 온라인 투표 시스템의 모델을 제시한다.

2.1 DLT를 활용한 온라인 투표 이용 사례

최근에 전 세계 주요 국가(덴마크, 에스토니아, 한국, 스페인, 우크라이나, 미국 등)에서는 DLT를 활용한 온라인 투표를 정치적인 정당 내 의사 결정, 지방자치단체 주민에 의한 사업 결정, 주식 시장에서 대리자 투표, 대통령 후보 선출 등에 적극적으로 이용하고 있다. (Table 1. 참조)

Table 1. Use cases of online voting using DLT based on telecommunication/ICT infrastructure

NO	State	Description
1	Denmark	In April 2014, the Danish Liberal Alliance political party has used blockchain technology for an internal vote at the party's annual meeting in Hvidovre, a suburb of Copenhagen.[3]
2	Estonia	In January 2017, Nasdaq Inc. has successfully completed a test using blockchain technology to run proxy voting on its Estonian Tallinn Stock Exchange. The technology allowed investors to vote online during investor meetings or transfer their voting rights to a proxy.[4]
3	Korea (Rep. of)	In February 2017, the province of Gyeonggi-do has made use of a voting system based on blockchain technology to gather a vote on community projects by its residents. The voting completed successfully, with 9000 residents placing their votes both online and offline.[5]
4	Spain	Since 2014, the Podemos political party has used Agora Voting which uses blockchain technology for internal elections.[6]
5	Ukraine	In February 2016, Ukrainian and US-based blockchain firms signed memorandum to develop e-Vox, an electronic voting system. Creators claim the distributed ledger technology will prevent fraud and make elections more transparent.[7]
6	United States	○ In March 2016, the Republican Party of Utah State went online with blockchain based online voting system for choosing the candidate for the Presidential election.[8] ○ In April 8 - 10 2016, the 2016 Libertarian Party of Texas State Convention used blockchain voting system.[9]

2.2 DLT를 활용한 온라인 투표 시스템의 모델

2.1에서 설명한 바와 같이 정보통신 인프라 기반의 DLT를 활용한 온라인 투표 시스템의 다양한 이용 사례를 분석한 결과 아래의 Fig.1.과 같은 모델을 제시하고자 한다. 본 논문에서 제시하는 DLT를 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.

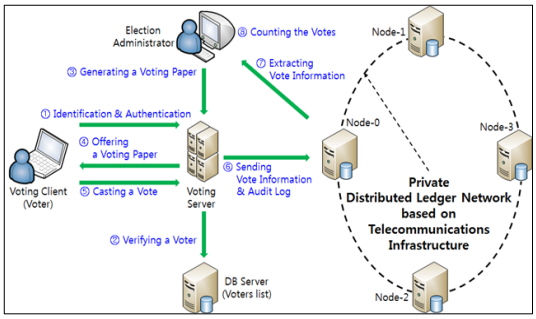

Fig. 1. Model of online voting system using DLT based on telecommunication/ICT infrastructure

Fig.1.에서 보는 바와 같이 DLT를 활용한 온라인 투표 시스템 모델에 근거한 투표 과정은 다음과 같이 설명할 수 있다.

○ 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.

2.3 DLT 관련 국제 표준화 동향

국제전기통신연합(ITU, International Telecommunication Union), ISO(International Organization for Standardization) 등 국제 표준화 기구에서는 정보보호 관점에서 DLT와 관련된 표준화 활동을 활발하게 진행하고 있다.

2.3.1 ITU-T

○ ITU-T 스터디 그룹 17(ITU-T Study Group 17 - Security)[10]
- 의장 : 순천향대학교 염흥열 교수
- 목적 : 정보통신기술(Telecommunication/ICT), 사이버공간(Cyberspace), 애플리케이션(Application), 신원 관리 및 인증(Identity management and Authentication) 등 분야에서 정보보호 국제 표준을 개발하고 유지한다.

○ ITU-T DLT 애플리케이션에 관한 포커스 그룹(ITU-T Focus Group on Application of Distributed Ledger Technology)[11]
- 설립일 : 2017년 5월
- 목적 : DLT 기반의 애플리케이션과 서비스를 식별 및 분석하고, 그에 따른 성공 사례와 가이던스(Guidance)를 제공한다. 또한 ITU-T 스터디 그룹에 표준화 작업을 제안한다.

2.3.2 ISO

○ ISO/TC 307 (Blockchain and distributed ledger technologies)[12]
- 설립일 : 2016년 9월
- 목적 : 블록체인 기술과 DLT에 관련된 참조 구조, 이용 사례, 보안과 프라이버시(Privacy), 신원 확인, 스마트(Smart) 계약 등 분야에서 국제 표준을 개발하고 유지한다.

2.4 DLT를 활용한 온라인 투표에 대한 시사점

최근 한국정보화진흥원(NIA)에서 발간한 특별 보고서(블록체인 활용 전자투표 주요 사례 및 시사점, NIA, 2017)에 따르면 DLT를 적용할 수 있는 비금융 분야 애플리케이션(서비스) 중 온라인 투표를 선정하고 그에

따라 주요 국가별 활용 실태, 유럽연합(EU) 보고서(What if blockchain technology revolutionised voting?, European Union, 2016) 등을 분석하여 다음과 같이 시사점을 제시하였다.[13]

○ 분산 원장 기술(DLT) 등장과 현황
- 현재 DLT를 활용한 서비스는 대부분 금융 분야에 국한되어 있지만 다른 분야로도 적용하는 움직임이 등장하고 있다.
- 그 중 온라인 투표 관련 사례가 활발히 등장하며 금융 분야에 이어 DLT를 적용할 수 있는 분야로 예상한다.
- 유럽연합(EU)은 보고서(What if blockchain technology revolutionised voting?, European Union, 2016)를 통하여 DLT를 활용하여 구현한 온라인 투표를 '블록체인 활용 전자투표(BEV, Blockchain-enabled e-voting)'라고 정의하며 전망, 사전 검토사항 그리고 정책 방향을 제시한다.

○ 시사점
- DLT 활용 온라인 투표는 국가적인 큰 규모보다는 당내 의사결정, 청원, 주민 의견 수렴, 주주총회 등 중·소규모 투표 방식에 현재 적용되고 있다.
- DLT 활용 온라인 투표를 총선·대선 등 범국가적인 규모에 적용시 개인정보, 데이터 보호, 접근성 등 보안 위협에 대한 모든 요소를 반드시 고려하여야 한다.
- 모든 사람이 참여하기 힘든 직접 투표의 물리적 한계를 극복하고 더 많은 시민이 정책 의사 결정에 참가할 가능성이 높다.
- 투표 절차가 간소화되었고 이로 인해 투표 비용 절감 효과도 기대할 수 있다.
- 기존 종이 투표와는 다르게 언제 어디서든 쉽게 참여할 수 있어 전체 투표율 증가 효과를 기대할 수 있다.
- DLT 활용 온라인 투표의 보안성, 접근성, 익명성 등 문제 해결이 필요하다.

2.5 개인정보보호 관련 고시

『개인정보의 안전성 확보조치 기준』(행정자치부고시 제2016-35호), 『개인정보의 기술적·관리적 보호조치 기준』(방송통신위원회고시 제2015-3호)에서 개인정보의 암호화 및 개인정보의 파기 등에 관한 내용은 다음과 같다.

2.5.1 『개인정보의 안전성 확보조치 기준』(행정자치부 고시 제2016-35호)

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과
⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.
⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.
⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.[16]

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제〔16〕

2.5.2 『개인정보의 기술적·관리적 보호조치 기준』(방송통신위원회고시 제2015-3호)

제6조(개인정보의 암호화) ① 정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 바이오정보

③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.〔15〕

2.6 정보보호 관리체계(ISMS) 인증 기준

『정보보호 관리체계 인증 등에 관한 고시』(미래창조과학부고시 제2016-59호)에 근거한 『정보보호 관리체계(ISMS) 인증 기준』의 통제 항목에서 구현 및 시험, 운영환경 이관, 암호 정책 수립, 접근통제 정책 수립, 사용자 등록 및 권한 부여, 사용자 인증, 사용자 식별, 보안시스템 운영, 성능 및 용량 관리, 악성코드 통제 등에 관한 내용은 다음과 같다.

2.6.1 통제 항목 8.2.1 구현 및 시험

안전한 코딩 방법에 따라 정보시스템을 구현하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. 또한 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.〔14〕

2.6.2 통제 항목 8.2.3 운영환경 이관

운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고 실행코드는 시험과 사용자 인수 후 실행하여야 한다.〔14〕

2.6.3 통제 항목 9.1.1 암호 정책 수립

조직의 중요정보 보호를 위하여 암호화 대상, 암호강도(복잡도), 키관리, 암호사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.〔14〕

2.6.4 통제 항목 10.1.1 접근통제 정책 수립

비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.〔14〕

2.6.5 통제 항목 10.2.1 사용자 등록 및 권한 부여

정보시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.〔14〕

2.6.6 통제 항목 10.3.1 사용자 인증

정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고, 필요한 경우 법적 요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.[14]

2.6.7 통제 항목 10.3.2 사용자 식별

정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.[14]

2.6.8 통제 항목 11.2.2 보안시스템 운영

보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템별 정책 적용 현황을 관리하여야 한다.[14]

2.6.9 통제 항목 11.2.3 성능 및 용량 관리

정보시스템 및 서비스 가용성 보장을 위해 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링 할 수 있는 방법 및 절차를 수립하여야 한다.[14]

2.6.10 통제 항목 11.5.1 악성코드 통제

바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다.[14]

2.7 상법 및 시행령

『상법』(법률 제13523호, 2015.12.1) 및 『상법 시행령』(대통령령 제28211호, 2017.7.26)에 근거한 전자적 방법에 의한 의결권의 행사(예: 전자투표) 등에 관한 내용은 다음과 같다.

『상법』 제368조의4(전자적 방법에 의한 의결권의 행사) ① 회사는 이사회의 결의로 주주가 총회에 출석하지 아니하고 전자적 방법으로 의결권을 행사할 수 있음을 정할 수 있다.
② 회사는 제363조에 따라 소집통지를 할 때에는 주주가 제1항에 따른 방법으로 의결권을 행사할 수 있다는 내용을 통지하여야 한다. 〈개정 2014.5.20.〉
③ 회사가 제1항에 따라 전자적 방법에 의한 의결권행사를 정한 경우에 주주는 주주 확인절차 등 대통령령으로 정하는 바에 따라 의결권을 행사하여야 한다. 이 경우 회사는 의결권행사에 필요한 양식과 참고자료를 주주에게 전자적 방법으로 제공하여야 한다.
④ 동일한 주식에 관하여 제1항 또는 제368조의3제1항에 따라 의결권을 행사하는 경우 전자적 방법 또는 서면 중 어느 하나의 방법을 선택하여야 한다.
⑤ 회사는 의결권행사에 관한 전자적 기록을 총회가 끝난 날부터 3개월간 본점에 갖추어 두어 열람하게 하고 총회가 끝난 날부터 5년간 보존하여야 한다.
⑥ 주주 확인절차 등 전자적 방법에 의한 의결권행사의 절차와 그 밖에 필요한 사항은 대통령령으로 정한다.[17]

『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 지정하

여 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.[18]

2.8 보안 위협 측면에서의 일반 IT 환경과 비공개형 분산원장 환경의 차이점

정보통신 인프라 기반의 온라인 투표 시스템에서 처리하는 중요 정보는 투표 정보(예: 후보자 선택 정보 등), 투표 과정에 대한 감사기록 등 이다. 이러한 중요 정보를 일반적인 IT 환경에서는 중앙 집중형 서버에 저장하게 되고, 비공개형 분산원장 환경에서는 물리적 또는 논리적으로 분산된 노드에 저장하게 된다. 따라서 보안 위협의 주요 대상은 중앙 집중식 서버와 분산 원장 네트워크 및 노드가 될 것이다.

중앙 집중식 서버에 비해 분산 노드에 저장된 중요 정보는 합의(Consensus) 프로토콜 및 해쉬 체인을 기반으로 처리되므로 데이터 무결성 위협 측면에서는 상대적으로 안전하다고 판단된다. 그러나 비공개형 분산 원장 네트워크 및 노드를 대상으로 하는 비인가된 접근, 서비스 가용성 저하, 중요 정보 유출, 중요 정보 삭제 및 위변조(예: 랜섬웨어 등), 악의적인 행동(예: 합의 속임(Consensus cheating)) 등 정보보호 측면에서 다양한 유형의 잠재적인 보안 위협은 여전히 존재한다.

III. DLT를 활용한 온라인 투표에 대한 보안 위협

본 장에서는 2.2에서 제시한 DLT를 활용한 온라인 투표 모델에 근거한 온라인 투표 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 5가지 범주로 분류하여 분석한다.

3.1 데이터 기밀성에 대한 위협

본 절에서는 침해사고(예: APT 공격 등) 및 IT 재해(예: 사람에 의한 재해 등)로 인하여 DLT를 활용한 온라인 투표 시스템을 구성하는 주요 정보 시스템에서 발생할 수 있는 데이터 기밀성 위협에 대하여 설명한다.

3.1.1 투표자의 개인정보 노출・유출

3.1.1.1 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.

3.1.1.2 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.

3.1.1.3 투표 서버가 투표자의 투표권을 검증하는 과정에서 투표 서버와 선거인 명부 서버 간의 전송 구간에서 개인정보(예: 고유식별정보, 성명 등)가 유출될 수 있다.

3.1.2 투표 정보 및 감사 기록 유출

3.1.2.1 투표자가 사용하는 투표 클라이언트와 투표 서버 간의 전송 구간에서 투표자가 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)가 유출될 수 있다.

3.1.2.2 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간에서 투표자가 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)가 유출될 수 있다.

3.1.2.3 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.
- 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

3.1.2.4 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스로부터 다음과 같은 내용을 포함한 대량의 중요 정보가 유출될 수 있다.
- 모든 투표자가 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)
- 모든 투표자의 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록 등

3.1.2.5 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 간의 전송 구간에서 다음과 같은 내용을 포함한 중요 정보가 유출될 수 있다.
- 투표자가 전자투표용지에 기표한 투표 정보(예: 후보자 선택 정보 등)
- 투표자의 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록 등

3.1.3 선거인 명부 유출

3.1.3.1 선거인 명부 서버 및 데이터베이스에 저장되어 있는 대량의 개인정보(예: 고유식별정보, 성명 등)가 포함된 선거인 명부가 유출될 수 있다.

3.2 데이터 무결성에 대한 위협

본 절에서는 침해사고(예: APT 공격, 랜섬웨어 등) 및 IT 재해로 인하여 DLT를 활용한 온라인 투표 시스템을 구성하는 주요 정보시스템에서 발생할 수 있는 데이터 무결성 위협에 대하여 설명한다.

3.2.1 전자투표용지 위변조

3.2.1.1 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.
- 후보자 목록 등

3.2.2 투표 정보 및 감사 기록 위변조

3.2.2.1 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.
- 후보자 목록, 후보자 선택 정보 등

3.2.2.2 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간에서 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록(3.1.2.3 참조)이 위변조 될 수 있다.

3.2.2.3 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스에 저장되어 있는 대량의 중요 정보(3.1.2.4 참조)가 삭제될 수 있다.

3.2.2.4 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 간의 전송 구간에서 다음과 같은 내용을 포함한 중요 정보(3.1.2.5 참조)가 위변조 될 수 있다.

3.2.3 선거인 명부 위변조

3.2.3.1 선거인 명부 서버 및 데이터베이스에 저장되어 있는 대량의 선거인 명부가 위변조 및 삭제될 수 있다. 선거인 명부에는 다음과 같은 개인정보가 포함될 수 있다.
- 고유식별정보(예: 주민등록번호 등), 성명, 주소 등

3.3 서비스 가용성에 대한 위협

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

3.3.1 분산 원장 네트워크 가용성 저하

3.3.1.1 대량의 중요 정보(3.1.2.4 참조)를 합의에 의해 처리(복제, 공유, 동기화 등)하는 분산 원장 네트워크(DLN) 인프라의 가용성이 저하될 수 있다.

3.3.1.2 대량의 중요 정보(3.1.2.4 참조)를 저장 및 유지하는 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스의 가용성이 저하될 수 있다.

3.3.2 투표 서버 가용성 저하

3.3.2.1 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.

3.3.3 선거인 명부 데이터베이스 가용성 저하

3.3.3.1 대량의 선거인 명부를 처리(예: 개인정보 조회 등)하는 선거인 명부 서버 및 데이터베이스의 가용성이 저하될 수 있다.

3.4 비인가된 접근

본 절에서는 침해사고(예: APT 공격 등) 및 IT 재해(예: 사람에 의한 재해)로 인하여 DLT를 활용한 온라인 투표 시스템을 구성하는 주요 정보시스템을 대상으로 하는 비인가된 접근에 대하여 설명한다.

3.4.1 선거인 명부에 대한 비인가된 접근

3.4.1.1 대량의 선거인 명부를 처리(예: 개인정보 조회 및 저장 등)하고 있는 선거인 명부 서버 및 데이터베이스를 대상으로 비인가된 접근이 이루어질 수 있다.

3.4.2 투표 서버에 대한 비인가된 접근

3.4.2.1 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.

3.4.3 분산 원장 네트워크에 대한 비인가된 접근

3.4.3.1 대량의 중요 정보(3.1.2.4 참조)를 합의에 의해 처리(복제, 공유, 동기화 등)하는 분산 원장 네트워크(DLN) 인프라를 대상으로 비인가된 접근이 이루어질 수 있다.

3.4.3.2 대량의 중요 정보(3.1.2.4 참조)를 저장 및 유지하는 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스를 대상으로 비인가된 접근이 이루어질 수 있다.

3.5 악의적인 행동

본 절에서는 투표자, 선거 관리자, 선거 관련 이해당사자, 소프트웨어 개발자 등에 의하여 발생할 수 있는 악의적인 행동에 대하여 설명한다.

3.5.1 전자투표용지 생성 부인

3.5.1.1 선거 관리자는 선거 관리 클라이언트(예: PC 등) 및 투표 서버를 통하여 투표자에게 제공한 전자투표용지의 생성(Generating) 사실을 부인(Repudiation)할 수 있다.

3.5.2 이중 투표

3.5.2.1 투표자는 투표 클라이언트(예: PC 등) 및

투표 서버를 통하여 이중(Double) 투표를 할 수 있다.

3.5.3 기표 부인

3.5.3.1 투표자는 투표 클라이언트(예: PC 등)를 통하여 전자투표용지에 기표(예: 후보자 선택 등)한 사실을 부인(Repudiation)할 수 있다.

3.5.4 악성코드 감염

3.5.4.1 DLT를 활용한 온라인 투표 시스템과 관련된 소프트웨어(예: 클라이언트용 투표 프로그램, 중요 정보 전송 모듈, 개표용 프로그램 등)의 개발 및 배포 과정에서 악성코드가 삽입될 수 있다.

3.5.4.2 투표자가 사용하는 투표 클라이언트(예: PC 등), 선거 관리자가 사용하는 선거 관리 클라이언트(예: PC 등) 등이 악성코드에 감염될 수 있다.

3.5.5 강압에 의한 투표

3.5.5.1 선거 관련 이해 당사자 등의 강압에 의하여 투표자는 원하지 않는 기표(예: 후보자 선택 등)를 할 수 있다.

IV. 보안 위협에 대한 대응 방안

본 장에서는 제3장에서 DLT를 활용한 온라인 투표 모델에 근거한 투표 과정에서 발생할 수 있는 잠재적인 보안 위협을 분석한 결과를 토대로 그에 대한 관리적·기술적 대응 방안을 『개인정보의 안전성 확보조치 기준』(행정자치부고시 제2016-35호), 『개인정보의 기술적·관리적 보호조치 기준』(방송통신위원회고시 제2015-3호), 미래창조과학부 『정보보호 관리체계(ISMS) 인증 기준』 등에 근거하여 제시한다.

4.1 데이터 기밀성 위협에 대한 대응 방안

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

4.1.1 투표자 개인정보 노출·유출에 대한 대응 방안

4.1.1.1 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 등)으로 암호화할 필요가 있다.(2.5.1, 2.5.2 참조)

4.1.1.2 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: '*') 처리가 필요하다.(2.5.1 참조)

4.1.1.3 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.(2.5.1, 2.5.2 참조)
- 투표 클라이언트와 투표 서버 간의 전송 구간
- 투표 서버와 선거인 명부 서버 간의 전송 구간 등

4.1.2 투표 정보 및 감사 기록 유출에 대한 대응 방안

4.1.2.1 투표 정보(예: 후보자 선택 정보 등) 및 감사 기록(3.1.2.3 참조)을 안전하게 전송하기 위하여 다음과 같은 전송 구간에 암호화(예: SSL/TLS, 암호화 응용프로그램 등) 조치가 필요하다.(2.6.3 참조)
- 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

4.1.2.2 대량의 중요 정보(3.1.2.4 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 등)으로 암호화할 필요가 있다.(2.6.3 참조)

4.1.3 선거인 명부 유출에 대한 대응 방안

4.1.3.1 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 등)으로 암호화할 필요가 있다.(2.5.1, 2.5.2 참조)

4.2 데이터 무결성 위협에 대한 대응 방안

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

4.2.1 전자투표용지 위변조에 대한 대응 방안

4.2.1.1 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.(2.6.3 참조)
- 선거 관리 클라이언트와 투표 서버 간의 전송 구간
- 투표 서버와 투표 클라이언트 간의 전송 구간 등

4.2.2 투표 정보 및 감사 기록 위변조에 대한 대응 방안

4.2.2.1 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.(2.6.3 참조)

4.2.2.2 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.(2.6.3 참조)
- 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

4.2.2.3 투표 과정에서 발생한 트랜잭션(Transaction)에 대한 감사 기록(3.1.2.3 참조)을 안전하게 전송하기 위하여 다음과 같은 전송 구간에 암호화(예: SSL/TLS, 암호화 응용프로그램 등) 조치가 필요하다.(2.6.3 참조)
- 투표 서버와 분산 원장 네트워크(DLN) 간의 전송 구간
- 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 간의 전송 구간 등

4.2.2.4 분산 원장 네트워크(DLN)의 주요 구성 요소인 노드(원장 서버) 및 데이터베이스에 저장 및 유지되고 있는 대량의 중요 정보(3.1.2.4 참조)에 대한 접근 권한(예: 신규 등록, 조회, 변경, 삭제 등)을 차등 부여하거나 변경 및 삭제 권한을 엄격히 제한할 필요가 있다.(2.6.5 참조)

4.2.3 선거인 명부 위변조에 대한 대응 방안

4.2.3.1 대량의 선거인 명부 내 개인정보(예: 고유식별정보)를 선거인 명부 서버 및 데이터베이스에 저장할 경우 안전한 암호 알고리즘(예: AES-128, RSA-2048 등)으로 암호화할 필요가 있다.(2.5.1, 2.5.2 참조)

4.2.3.2 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.(2.6.5 참조)

4.3 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 설명한다.

4.3.1 분산 원장 네트워크 가용성 저하에 대한 대응 방안

4.3.1.1 대량의 중요 정보(3.1.2.4 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.
- 지속적인 네트워크 성능 및 용량 모니터링(2.6.9 참조)
- 네트워크 인프라(예: 백본, 회선 등) 이중화 구성
- DDoS 대응 시스템 운용 등

4.3.1.2 대량의 중요 정보(3.1.2.4 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.
- 지속적인 성능 및 용량(예: CPU, 메모리, 네트워크, 저장매체 등) 모니터링(2.6.9 참조)
- DDoS 대응 시스템 운용 등

4.3.2 투표 서버 가용성 저하에 대한 대응 방안

4.3.2.1 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.
- 지속적인 성능 및 용량(예: CPU, 메모리, 네트워크, 저장매체 등) 모니터링(2.6.9 참조)
- 투표 서버 이중화 구성
- DDoS 대응 시스템 운용 등

4.3.3 선거인 명부 데이터베이스 가용성 저하에 대한 대응 방안

4.3.3.1 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.
- 지속적인 성능 및 용량(예: CPU, 메모리, 네트워크, 저장매체 등) 모니터링(2.6.9 참조)
- 선거인 명부 서버 및 데이터베이스 이중화 구성
- DDoS 대응 시스템 운용 등

4.4 비인가된 접근에 대한 대응 방안

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

4.4.1 선거인 명부를 대상으로 하는 비인가된 접근에 대한 대응 방안

4.4.1.1 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.
- 사용자 식별 및 인증(2.6.6, 2.6.7 참조)
- 사용자별 접근 권한 차등 부여(2.6.5 참조)
- 네트워크 또는 호스트 기반 침입차단시스템(방화벽) 등을 통한 접근 통제(2.6.4, 2.6.8 참조) 등

4.4.2 투표 서버를 대상으로 하는 비인가된 접근에 대한 대응 방안

4.4.2.1 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 포함

시킬 필요가 있다.
- 사용자 식별 및 인증(2.6.6, 2.6.7 참조)
- 사용자별 접근 권한 차등 부여(2.6.5 참조)
- 네트워크 또는 호스트 기반 침입차단시스템(방화벽) 등을 통한 접근 통제(2.6.4, 2.6.8 참조) 등

4.4.3 분산 원장 네트워크를 대상으로 하는 비인가된 접근에 대한 대응 방안

4.4.3.1 대량의 중요 정보(3.1.2.4 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.
- 하드웨어 주소(MAC Address) 사전 등록에 의한 접근 통제(2.6.4 참조)
- 네트워크접근통제(NAC)시스템, 네트워크 기반 침입차단시스템(방화벽) 등을 통한 접근 통제(2.6.4, 2.6.8 참조) 등

4.4.3.2 대량의 중요 정보(3.1.2.4 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.
- 사용자 식별 및 인증(2.6.6, 2.6.7 참조)
- 사용자별 접근 권한 차등 부여(2.6.5 참조)
- 노드(원장 서버) 간의 양방향 인증
- 네트워크 또는 호스트 기반 침입차단시스템(방화벽) 등을 통한 접근 통제(2.6.4, 2.6.8 참조) 등

4.5 악의적인 행동에 대한 대응 방안

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

4.5.1 전자투표용지 생성 부인에 대한 대응 방안

4.5.1.1 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.
- 전자투표용지 생성시 선거 관리자의 전자서명(PKI 기반) 징구 등

4.5.2 이중 투표에 대한 대응 방안

4.5.2.1 투표자가 투표 클라이언트(예: PC 등) 및 투표 서버를 통하여 이중(Double) 투표를 할 수 없도록 다음과 같은 내용을 고려한 조치가 필요하다.
- 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

4.5.3 기표 부인에 대한 대응 방안

4.5.3.1 투표자가 투표 클라이언트(예: PC 등)를 통하여 전자투표용지에 기표(예: 후보자 선택 등)한 사실을 부인(Repudiation)할 수 없도록 다음과 같은 내용을 고려한 조치가 필요하다.
- 투표자가 전자투표용지에 기표(예: 후보자 선택 등)시 투표자의 전자서명(PKI 기반) 징구 등

4.5.4 악성코드 감염에 대한 대응 방안

4.5.4.1 DLT를 활용한 온라인 투표 시스템과 관련된 소프트웨어(예: 클라이언트용 투표 프로그램, 중요 정보 전송 모듈, 개표용 프로그램 등)에 악성코드가 삽입되지 않도록 다음과 같은 내용을 고려한 조치가 필요하다.
- 개발 환경에서 운영 환경으로 소프트웨어 이관시 보안 통제(예: 개발자의 이관 업무 겸직 금지, 이관시 결재권자에 의한 승인 등) 이행(2.6.2 참조)
- 소프트웨어 개발(유지보수)시 주기적인 소스코드 취약점 진단 및 후속조치 이행(2.6.1 참조) 등

4.5.4.2 투표자가 사용하는 투표 클라이언트(PC), 선거 관리자가 사용하는 선거 관리 클라이언트(PC) 등이 악성코드에 감염되지 않도록 다음과 같은 내용을 고려한 조치가 필요하다.

- 백신 프로그램 운용(예: 실시간 악성코드 감시 및 치료, 주기적인 악성코드 점검, 백신엔진 최신 버전 유지 등)(2.6.10 참조) 등

4.5.5 강압에 의한 투표 대응 방안

4.5.5.1 선거 관련 이해 당사자 등의 강압에 의하여 투표자의 원하지 않는 기표(예: 후보자 선택 등)에 대응할 수 있도록 다음과 같은 내용을 고려한 조치가 필요하다.

- 투표자가 사용하는 투표 클라이언트(예: PC 등)의 물리적인 위치(예: 공개 투표소, 자택, 직장 등) 및 식별자(예: IP 주소 등)를 투표 시작 전에 사전 등록(2.7 참조) 등

V. 결 론

국내외적으로 큰 관심을 받고 있는 신흥 기술인 분산 원장 기술(예: 블록체인 등)이 금융 및 비금융 분야 애플리케이션(서비스)에 다양하게 적용되고 있다. 특히 비금융 분야 애플리케이션(서비스) 경우, 한국을 포함한 다수의 주요 국가에서 DLT를 활용한 온라인 투표를 적극적으로 검토하여 다양한 의사 결정 방식으로 이용하고 있다. 그러나 최근에 DLT를 활용한 금융 분야 애플리케이션(서비스) 중 가상 화폐 거래소에 대한 보안사고(가상 화폐 탈취, 개인 정보 유출 등)가 빈번하게 발생하고 있어 사회적·경제적으로 큰 손실을 초래하고 있는 바, 금융 및 비금융 분야의 DLT를 활용한 애플리케이션(서비스)을 대상으로 정보보호 관점의 잠재적인 보안 위협을 분석하고 그에 상응하는 보안 대책을 수립하는 것이 절실히 필요하다.

따라서 본 논문에서는 비금융 분야의 DLT를 활용한 온라인 투표 시스템의 모델을 제시하고, 해당 모델에 근거한 온라인 투표 과정에서 발생할 수 있는 잠재적인 보안 위협을 크게 5가지(데이터 기밀성, 데이터 무결성, 서비스 가용성, 비인가된 접근, 악의적인 행동 등)로 분류하여 분석하였다. 또한 식별된 보안 위협에 대한 대응 방안을 『개인정보의 안전성 확보조치 기준』(행정자치부고시 제2016-35호), 『개인정보의 기술적·관리적 보호조치 기준』(방송통신위원회고시 제2015-3호), 미래창조과학부 『정보보호 관리체계(ISMS) 인증 기준』 등에 근거하여 제시하였다.

향 후 DLT를 활용한 온라인 투표 서비스를 구축 및 운영할 경우 이해 당사자(서비스 제공자, 투표자, 선거 관리자 등)는 본 논문에서 제시한 보안 위협과 대응 방안을 고려함으로서 최신 기술에 의한 보안 사고를 예방할 수 있도록 도움이 되고자 한다.

References

[1] Internet newspaper of Digital Daily, "http://www.ddaily.co.kr/news/article.html?no=157742," Jul. 2017

[2] Internet newspaper of Boannews , "http://www.boannews.com/media/view.asp?idx=55561&skind=O," Jul. 2017

[3] Internet newspaper of CryptoCoinsNews, "https://www.cryptocoinsnews.com/blockchain-voting-used-by-danish-political-party/," Apr. 2014

[4] Internet newspaper of Reuters, "http://www.reuters.com/article/nasdaq-blockchain-idUSL1N1FA1XK," Jan. 2017

[5] Internet newspaper of Hankyung, "http://news.hankyung.com/article/201702232611h?nv=o," Feb. 2017

[6] Internet newspaper of ChosunBiz, "http://biz.chosun.com/site/data/html_dir/2016/06/13/2016061300015.html?Dep0=twitter," Jun. 2016

[7] Internet homepage of Ambisafe, "https://www.ambisafe.co/blog/ethereum-voting/," Feb. 2016

[8] Internet newspaper of CryptoCoinsNews, "https://www.cryptocoinsnews.com/blockchain-tech-enables-utah-republicans-vote-candidate/," Mar. 2016

[9] Internet newspaper of CoinDesk, "http://www.coindesk.com/libertarian-party-texas-logs-votes-presidential-electors-blockchain/," Apr. 2016

[10] ITU-T Study Group 17 - Security,

"http://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx," Jul. 2017

〔11〕 Internet homepage of ITU-T Focus Group on Application of Distributed Ledger Technology, "http://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx," May. 2017

〔12〕 Internet homepage of ISO/TC 307 Blockchain and distributed ledger technologies, "https://www.iso.org/committee/6266604.html," Sep. 2016

〔13〕 National Information Society Agency, "Key cases and implications of electronic voting using blockchain," pp. 1-12, Apr. 2017

〔14〕 Korea Internet & Security Agency, "Information Security Management System(ISMS) Certification Criteria," May. 2013

〔15〕 Korea Communications Commission, "『Criteria on technical and administrative security measures of personal information』 (Korea Communications Commission Notice No. 2015-3)," May. 2015

〔16〕 Ministry of the Interior, "『Criteria on measures ensuring the safety of personal information』(Ministry of the Interior Notice No. 2016-35)," Sep. 2016

〔17〕 Ministry of Justice, "『COMMERCIAL ACT』," Dec. 2015

〔18〕 Ministry of Justice, "『ENFORCEMENT DECREE OF THE COMMERCIAL ACT』," Jul. 2017

〈저자소개〉

박 근 덕 (Keundug Park) 종신회원
1992년 2월: 동아대학교 전산공학과 학사
2015년 8월: 순천향대학교 대학원 정보보호학과 석사
2015년 9월~현재: 순천향대학교 대학원 정보보호학과 박사과정
2012년 2월~현재: 정보보호관리체계(ISMS) 인증 심사원
2016년 2월~현재: ㈜한국아이티평가원(KSEL) 수석컨설턴트
2017년 2월~현재: ITU-T SG17 전문위원/에디터
2017년 7월~현재: ITU-T FG-DLT/DFC 전문위원
2017년 8월~현재: ISO/TC 307 전문위원
〈관심분야〉 정보보호관리체계, 개인정보보호, 클라우드 컴퓨팅 보안, 분산원장기술 보안

김 창 오 (ChangOh Kim) 정회원
1999년 2월: 동의대학교 전산통계학 이학사
2001년 2월: 동의대학교 대학원 전산통계학과 이학석사
2013년 2월: 고려대학교 정보보호대학원 정보보호학과 박사수료
2011년 11월~현재: 개인정보보호관리체계(PIMS) 인증심사원
2012년 12월~현재: 정보보호관리체계(ISMS) 인증심사원
2014년 6월~현재: ㈜쿠팡 정보보안팀, 핀테크사업부
2015년 1월~현재: ITU-T SG17 전문위원/에디터
2015년 4월~현재: ICT 국제표준전문가
2017년 7월~현재: ITU-T FG-DLT/DFC 전문위원
2017년 8월~현재: ISO/TC 307 전문위원
〈관심분야〉 정보보호관리체계, 개인정보보호, 스팸보안, ITS/IoT 보안, 분산원장기술 보안

염 흥 열 (Heung-youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 9월: 한양대학교 대학원 전자공학과 석사
1990년 2월: 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월: 한국전자통신연구원 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월: 한국정보보호학회 회장(역), 명예회장(현재)
2007년 3월~현재: 한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2009년~2016년: ITU-T SG17 부의장, ITU-T SG17 WP2/WP3 의장
2016년 5월~현재: 개인정보보호표준포럼 의장
2017년~현재: ITU-T SG17 의장
〈관심분야〉 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜