creative commons

COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

[UCI]I804:24011-200000266869
조선대학교
CHOSUN UNIVERSITY

2018년 8월
박사학위 논문

개인정보 유출과 정보전이가 기업가치에 미치는 영향에 관한 연구

조 선 대 학 교 대 학 원

경 영 학 과

박 상 수

조선대학교
CHOSUN UNIVERSITY

개인정보 유출과 정보전이가 기업가치에 미치는 영향에 관한 연구

A Study on the Effect of Personal Information Breaches and Information Transfer on Firm Value

2018년 8월 24일

조 선 대 학 교 대 학 원

경 영 학 과

박 상 수

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

개인정보 유출과 정보전이가 기업가치에 미치는 영향에 관한 연구

지도교수 이 현 철

이 논문을 경영학 박사학위신청 논문으로 제출함

2018년 4월

조 선 대 학 교 대 학 원

경 영 학 과

박 상 수

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

박상수의 박사학위논문을 인준함

위원장 조선대학교 교수 이 계 원 (인)

위 원 경상대학교 교수 김 진 수 (인)

위 원 조선대학교 교수 오 갑 진 (인)

위 원 조선대학교 교수 장 지 원 (인)

위 원 조선대학교 교수 이 현 철 (인)

2018년 6월

조 선 대 학 교 대 학 원

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

목 차

I. 서론 ····· 1

II. 개인 정보유출과 정보보안 기술동향 ····· 4

1. 정보보안의 개념 ····· 4
2. 개인정보유출 ····· 6
2.1 개인정보와 프라이버시 ····· 6
2.2 개인정보의 개념 ····· 9
2.3 개인정보의 특징 및 분류 ····· 13
2.4 주민등록번호의 중요성 ····· 14
3. 개인정보보호 정책관련 국내외 동향 ····· 16
3.1 국내동향 ····· 16
3.2 국외동향 ····· 21
3.3 개인정보의 유출 및 노출사고 국내외 사례 및 동향 ····· 26
4. 정보보안 위협요인 ····· 29
4.1 데이터 유출 ····· 30
4.2 보안 취약점 ····· 30
4.3 피싱 ····· 31
4.4 보안 침해 9가지 공격 패턴 ····· 32
5. 4차 산업과 정보보안 ····· 33
6. 4차 산업혁명 시대의 정보보호 기술동향 ····· 34
6.1 디지털 안심생활 인프라 ····· 35

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

6.2 디지털 치안 인프라 구축 ····· 38
6.3 디지털 안보 인프라 ····· 41
7. 정보보안 기술의 미래 ····· 42
7.1 차세대 암호 ····· 42
7.2 디지털 DNA ····· 43
7.3 범죄 행위 예측 ····· 44

III. 이론적 배경 ····· 45
1. 개인정보보호를 위한 규제 ····· 45
2. 개인정보유출의 경제적·사회적 손실 ····· 45
3. 개인정보유출과 주식가격 ····· 47
4. 개인정보유출과 정보보안 기업의 주가반응 ····· 49

IV. 연구모형 ····· 51
1. 사건연구모형 ····· 51
2. 횡단면 회귀분석모형 ····· 55

V. 실증분석 ····· 59
1. 연구자료 ····· 59
2. 실증분석 결과 ····· 62
2.1 개인정보 유출 기업에 대한 실증분석 결과 ····· 62
2.2 전이효과에 따른 정보보안 기업의 실증분석 결과 ····· 66

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

VI. 결론 및 연구의 한계점 ····· 74

참고문헌 ····· 76
ABSTRACT ····· 80

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

<표 목 차>

<표 1> 데이터 보호와 Privacy 관련법과 관련있는 Privacy의 분류 ·· 6
<표 2> 사회 발전에 따른 Privacy 의미 변화 ····· 8
<표 3> 개인정보 보호를 명시하고 있는 개별법(특별법)의 예 ····· 11
<표 4> OECD 프라이버시 가이드 라인 8원칙 ····· 12
<표 5> 개인정보 유형별 종류 ····· 13
<표 6> 개인을 식별할 수 있는 정보로서의 개인정보 유형 ····· 14
<표 7> 주요국의 개인식별번호 현황 ····· 15
<표 8> 정보통신망법 주요 내용 ····· 16
<표 9> 개인정보보호법 주요 내용 ····· 19
<표 10> 주요 국가의 개인정보 정의 ····· 21
<표 11> 미국의 개인정보 관련 주요 법률 ····· 24
<표 12> 국내 개인정보유출 주요 사고 사례 ····· 27
<표 13> 해외 개인정보유출 주요 사고 사례 ····· 28
<표 14> 국내 공격 주요 사고 사례 ····· 32
<표 15> 연도별 개인정보 유출 사건 및 관련 기업 수 ····· 60
<표 16> 연도별 정보보안 기업 현황 ····· 62
<표 17> 개인정보 유출 기업에 대한 AAR 및 CAAR ····· 63
<표 18> 개인정보 유출 기업에 대한 기간별 CAAR ····· 64
<표 19> 개인정보 유출 기업에 대한 회귀분석 결과 ····· 65
<표 20> 정보보안 기업에 대한 AAR 및 CAAR ····· 68
<표 21> 정보보안 기업에 대한 기간별 CAAR ····· 72
<표 22> 정보보안 기업에 대한 회귀분석 결과 ····· 73

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

[그 림 목 차]

[그림 1] 사회 발전에 따른 Privacy 의미 변화 ····· 8
[그림 2] 개인정보의 유형 ····· 10
[그림 3] 4차 산업혁명 시대 정보보안 산업 분류 ····· 35
[그림 4] 개인정보 유출 기업의 AAR 및 CAAR ····· 64
[그림 5] 정보보안 기업의 AAR 및 CAAR ····· 71

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

I. 서론

정보통신기술의 급격한 발전과 더불어 인터넷 및 무선통신망의 전 세계적 구축으로 말미암아 다양한 분야의 기업이 자사의 고객정보를 수집·이용하여 고객의 욕구를 사전에 예측하고 이들의 욕구를 충족시킴으로써 더 높은 부가가치를 창출하고자 노력하고 있다(김광용 등 2016). 이를 위해 정보통신 기업뿐만 아니라 각종 유통 및 소매업체, 제조업체 및 금융기관 등 수 많은 영역의 기업이 개인의 정보를 온·오프라인을 통해 취득하고 이를 분석하며, 그들의 마케팅에 활용하고 있는 실정이다. 개인정보란 '개인을 구별할 수 있는 정보'로, 예전에는 주민등록번호처럼 개인을 명확히 구별할 수 있는 정보에 한정되어 그 범위가 좁았으나, 오늘날엔 다양한 수단을 통해 수집·생성된 개인의 자료로 그 범위가 넓어졌다(양재모, 2010; 김광용 등 2016). 예를 들어, 인터넷 기사에 대한 댓글, 휴대폰의 위치인식 소프트에 의해 수집된 개인의 이동반경 및 경로별 빈도, 휴대폰 번호, 계좌번호, SNS에 작성한 글, 각종 상품의 구매내역 및 네트워크에 접속한 IP주소 등 다양한 것들이 개인정보로 간주되고 있다.

비록 기업에 의해 수집·보관되는 개인정보라 하더라도, 이는 해당 기업의 자산이기 이전에 정보제공자 개인의 소중한 재산으로 볼 수 있다. 법적으로 이에 대한 권리는 적극적 의미 및 소극적 의미의 정보통제권으로 분류된다(한귀현, 2005; 김정연, 2013). 소극적 의미의 정보통제권은 본인의 정보가 자신의 의사와는 달리 다른 사람에 의해 수집되지 않도록 하는 권리를 말한다. 반면 적극적 의미의 정보통제권은 자신의 정보에 대한 열람청구권, 잘못 기록된 자신의 정보에 대한 정정 및 보완 청구권, 삭제·사용 중지 및 봉쇄청구권, 타인의 이용 및 제공에 대한 동의권 등을 포함하고 있다. 정보통제권에 대한 적극적 의미는 소극적 의미에 비해 그 권리 인정의 범위가 대폭 확대된 경우라 하겠다. 그러나 인터넷이 일반인에게 보급되기 시작한 1990년대 이후부터 개인의 정보가 침해되고 있는 사례가 빈번히 발생하고 있다. 개인정보 침해란 "해당 정보주체와 관계된 다양한 정보가 잘못 사용(유출, 변경, 도용 및 훼손 등)됨으로써 개인의 자기정보통제권이 침해되는 것"을 말한다.[1] 이러한 사례의 대표적인 것으로 기업의 개인정보 유출 사건을 들 수 있다.

한국 내 개인정보 유출 사고를 살펴보면, 2008년 1월 중국 해커에 의해 발생된 것

1) 한국인터넷진흥원 개인정보침해신고센터 접수자료에 따르면 2010년 54,832건, 2011년 122,215건, 2012년 166,801건, 2013년 177,736건, 2014년 158,900건의 개인정보 유출 사고가 발생했던 것으로 알려지고 있다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

으로 추정되는 옥션 약 1,800만 건을 시작으로, 2011년 3월 신세계 몰에서 390만 건의 개인정보가 유출되었다. 이 외에도, 2011년 4월 현대캐피탈에서 175만 건의, 2011년 7월경에는 SK커뮤니케이션에서 350만 건의 개인정보가 각각 유출되었다. 그 어느 기업보다 보안이 철저해야할 금융권에서도 개인정보 유출 사고가 발생하였으며, 이의 대표적인 예로 2014년 KB국민카드 5,300만 건, NH농협카드 2,500만 건 및 롯데카드 2,600만 건 등의 사고를 들 수 있다. 이들 규모를 총 합산하면 약 1억 400만 건의 개인정보가 유출된 셈이다. 단지 이는 보도로 들어난 일부에 불과할 뿐이어서, 실질적 사고의 규모는 우리의 상상을 초월할 것으로 생각된다. 한편, 중국의 경우 2011년에 교통은행에서 발생한 7천 만 건을 비롯하여 2014년 중국이동 1만 5천 건 및 차이나 유니콤에서 발생한 1만 5천 건의 개인정보 유출 사고가 있었다(김광용 등, 2016). 유출된 개인정보에는 주민등록번호, 이름, 휴대폰 전화번호, 주소, 직장명 및 신용카드의 사용 내역 등 다양한 정보가 포함되어 있는 것으로 보도되고 있다. 유출된 개인정보는 단순한 정보 유출에 그치는 것이 아니라 개인명의 도용 및 개인 아이디 해킹 등의 2차 피해를 불러올 수 있다.[2] 이는 개인정보 유출 사고에서 그치는 것이 아니라 정보사회의 발전에 심각한 장애를 불러올 수 있으며, 자칫 인터넷 문화의 붕괴를 가져올 수 있다는 점에서 크나큰 문제라 하겠다. 한국의 경우 2011년부터 개인정보보호법이 제정·시행되고 있어 그나마 개인정보 유출에 따른 피해 보상이 이루어지고 있으나, 많은 국가의 경우 개인정보 유출에 대한 법률의 미비로 인해 피해 보상이 이루어지지 못하고 있는 실정이다.

본 연구는 기업의 개인정보 유출이 해당 기업 및 기업들에게 보안시스템을 구축. 운용해주고 있는 정보보안 기업의 주가에 어떤 영향을 미치는지를 살펴보고자 한다. 기존 연구결과는 개인정보 유출 기업은 사건공시일 주식의 가격이 하락하는 것을 보여준다(김광용 등, 2016). 그러나 한국의 상장기업을 대상으로 개인정보 유출 시 정보보안 기업의 주가가 어떻게 변하는가에 대한 사건연구는 거의 보고되지 않고 있는 실정이다. 이는 기업의 개인정보 유출 사고로 인한 정보보안 기업으로의 정보전이 효과를 살펴볼 수 있다는 점에서 매우 흥미로운 연구라 하겠다. 또한, 개인정보유출의 사회적 심각성을 고려할 때 본 연구의 결과는 관련 기업 및 개인에게 매우 큰 의의를 가질 것으로 생각된다.

본 연구는 다음과 같이 구성되어 있다. 제1장의 서론에 이어, 제2장은 정보유출과 정보보안 기술 동향을 알아보고 제3장은 개인정보유출에 대한 선행연구들을 살펴본다. 제4

2) 실제 유출된 개인정보로 인해 개인명의 및 아이디가 도용되는 사례가 각종 언론매체 상에 보도되고 있다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

장은 연구모형을 제시하고, 제5장은 정보보안 기업으로의 정보전이 효과를 실증분석을 한다. 마지막으로 제6장에서는 연구결과를 요약하고 연구의 시사점을 제시한다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

II. 개인정보 유출과 정보보안 기술동향

1. 정보보안의 개념

정보보안은 정보를 여러 가지 위협으로부터 보호한다는 사전적 의미를 가지고 있으나 사용자, 국가, 또는 기관마다 그 정의는 다양하다. 우리나라 정보화촉진기본법 제2조에는 정보보안을 '정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 강화하는 것'이라고 정의하고 있다.

국제표준화기구(International Organization for Standardization, 이하 ISO) ·국제전기기술위원회(International Electronical Committee, 이하 IEC) 17799:2005에 따르면 정보보안은 "정보를 다른 중요한 비즈니스 자산과 같이 비즈니스에 필수적이며, 따라서 적절하게 보호될 필요가 있는 자산이며 비즈니스 연속성을 보장하고, 위험을 최소화하며, 투자와 기회를 극대화하기 위하여 광범위한 위협으로부터 정보를 보호하는 것" 이라 정의하고 있다. 또, ISO·IEC 27000:2009에서는 "정보의 기밀성(confidentiality), 무결성(integrity), 가용성(availability). 추가적으로 진정성(authenticity), 책임성(accountability), 부인방지(non-repudiation), 그리고 신뢰성(reliability)과 관계가 있을 수 있다"고 소개하고 있다.

기밀성이란 허용되지 않은 사용자 또는 객체나 개체가 정보의 내용을 알아낼 수 없도록 하는 것으로써 비밀 보장이라 칭할 수도 있다. 원하지 않는 정보공개를 막는다는 점에서 프라이버시 보호와도 밀접한 관계를 가진다. 무결성이란 허용되지 않은 사용자나 객체가 정보를 임의로 수정할 수 없도록 하는 것으로써, 수신자가 정보를 수신하거나 보관되어 있던 정보를 열람할 때 그 정보가 수정 또는 첨삭된 적이 없는지 확인 가능하도록 하는 것이다. 가용성은 허용된 사용자나 객체가 정보에 접근을 시도할 때 방해받지 않게 하는 것이다. 최근 들어 네트워크의 고도화로 대중에 알려진 공격방법 중 하나인 분산 서비스 거부 공격(Distribute Denial of Service, 이하 DDoS)이 이러한 가용성을 해치는 공격이다.[3)]

경제협력개발기구(:Organization for Economic Cooperation and Development, 이하

3) 디도스 공격으로 알려져 있는 분산 서비스 거부 공격은 많은 수의 좀비 PC를 원격에서 조정하여 서비스 시스템의 네트워크 또는 시스템리소스를 한계치 이상 사용하게 하여 서비스를 방해하는 공격으로 2009년 7월 7일 사이버 테러가 대표적인 사례다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

OECD)가 2002년에 발표한 정보보안 가이드라인에 명시된 정보보안은 기밀성, 무결성, 가용성 세 가지 요소를 관리하는 것이라고 정의하고 있다. 유럽 국가사회보장기금(Caisse Nationale de Securité Sociale, 이하 CNSS)는 2010년에 “인가되지 않은 접근, 사용, 폭로, 붕괴, 수정, 파괴로부터 정보와 정보 시스템을 보호해 기밀성, 무결성, 가용성을 제공하는 것”이라고 정의하였고, 2008년 미국 정보시스템감사통제협회(Information Systems Audit and Control Association, 이하 ISACA)는 “인가되지 않은 접근, 사용, 폭로, 붕괴, 수정, 파괴로부터 정보와 정보 시스템을 보호해 기밀성, 무결성, 가용성을 제공하는 것”이라고 하였다.

정보보안은 고대부터 현재까지 끊임없이 그 중요성이 강조되는 문제이다. 특히 전쟁의 수행이 당연한 일이었던 근대 이전에는 정치적 또는 군사적 목적 때문에 보안이 중요했다. 정보 보안의 개념이 크게 변화하게 된 시점은 디지털시대가 시작되면서 부터이다. IT산업의 발전은 디지털환경에서 정보보안의 필요성을 확대시켰으며, 네트워크의 발전은 공간적 한계를 극복하여 정보 유출에 있어 새로운 패러다임을 만들어냈다.

Loch et al(1992)은 정보보안을 위협하는 요소들을 내부적·외부적 위협으로 나누고 다시 위협을 가하는 대상에 따라 인간과 비인간으로 구분 짓고 있다. 이러한 구분에 따르면 외부에서 위협을 가하는 인간은 해커와 경쟁자이며, 비인간 대상은 자연재해 및 컴퓨터 바이러스를 꼽고 있다. 또한, 내부에서 위협을 가하는 인간은 직원의 행위와 절차 등이며 비인간 대상은 기계적·전기적 장애 및 프로그램 문제로 보고 있다. 그리고 이러한 모든 경우를 고의성에 따라 의도적 위협과 비의도적 위협으로 구분한다.

초연결의 4차 산업혁명시대에서의 정보보안은 그 중요성이 더 중요해지고 있다. 2015년 발표된 세계경제포럼보고서에 따르면 2025년 급격한 사회 변화를 예측하였다.[4] 초연결은 재산은 물론 개인의 신체적 위협에까지 연결되게 되어 악용될 수 있다. 이를

4) 세계경제 포럼보고서(2015)에 따르면 인구 10% 이상이 인터넷에 연결된 의류를 입고(91.2% 확률), 인구 90% 이상이 무한 용량의 무료 저장소를 사용하고(91.0% 확률), 1조 개의 센서가 인터넷에 연결되고(89.2% 확률), 로봇 약사가 등장하고(86.5% 확률), 10%의 인구가 인터넷이 연결된 안경을 쓰고(85.5% 확률), 인 구 80%가 인터넷상 디지털 정체성을 갖게 되고(84.4% 확률), 3D로 제작된 자동차가 처음 생산되고(84.1% 확률), 인구 센서스 대신 빅 데이터를 활용하는 최초의 정부가 등장하고(82.9% 확률), 상업화 된 인체 삽입형 휴대폰이 등장하고(81.7% 확률), 미국 도로를 달리는 차 중 10%가 자율주행자동차가 되고(78.2% 확률), 3D로 제작된 간이 최초로 이식되고(76.4% 확률), 인공지능이 기업 강사의 30%을 차지하고(75.4% 확률), 가정용 기기에 50% 이상이 인터넷 트래픽이 몰리게 된다(69.9% 확률).

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

예방하는 길은 결국 정보보안이며, 4차 산업혁명 시대를 맞아 보안의 중요성은 더욱 높아 질 수밖에 없다.

2. 개인정보 유출

2.1 개인정보와 프라이버시

한국인터넷 진흥원(Korea Internet Security Agency, 이하 KISA)에서는 개인정보의 원천을 프라이버시(privacy)개념에서 파생되었다고 본다. 프라이버시는 1890년 미국의 워렌(Warren)과 브랜다이스(Brandeis)에 의해 “홀로 있을 수 있는 권리(the right to be let alone)”로 정의되었다(Samuel D.Warren, & Louis D. Brandeis, 1890). 또한 개인정보 관련 권리 해석 시 일반적으로 프라이버시라는 개념으로 포괄하여 접근한다. 개인정보 자기 결정권이란 자신에 관한 정보가 언제, 어떻게, 누구에게, 어느 범위까지 이용 및 제공될 수 있는지를 그 정보 주체가 스스로 결정할 수 있는 권리라 할 수 있다(한국인터넷진흥원, 2018). 이러한 의미에서 궁극적인 개인정보의 소유권은 해당 개인정보의 주체에 존재한다고 할 수 있으며, 이러한 소유권의 보호를 위해 이용자의 권익을 보호하는 것은 정보통신서비스제공자 등 개인정보를 이용하여 사업을 영위하는 모든 관련 당사자의 당연한 의무라고 명시하고 있다(권헌영, 2004).

현대사회는 정보통신기술이 발달하여 대부분 프라이버시를 개인정보보호나 개인정보 자기 결정권을 동일 시 하는 경향이 일반적이며, 데이터 보호와 프라이버시 관련법과 관련 있는 프라이버시의 분류는 <표 1>과 같다.

<표 1> 데이터 보호와 프라이버시 관련법과 관련 있는 프라이버시의 분류

구분	개인정보 유형
정보 (information privacy)	개인정보의 수집과 관리를 관장하는 규칙수립과 관련이 있는 Privacy, 정부의 기록, 신용정보, 의료정보 등이 해당
신체 (bodily privacy)	개인의 신체 혹은 물리적 존재와 관련 있으며, 이에 대해 침해하는 것에 초점, 유전자 검사, 마약검사, 체강(bodily cavity)검사 등이 해당

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

지역 (territorial privacy)	한 개인이 다른 개인의 환경에 침입하는 것에 대한 제한에 초점, 환경은 가정에만 국한된 개념이 아니며, 직장이나 공개된 장소도 이에 해당
통신 (communications privacy)	우편, 통화 내용, 이메일 및 여타 방식을 포함하는 통신의 보호와 관련

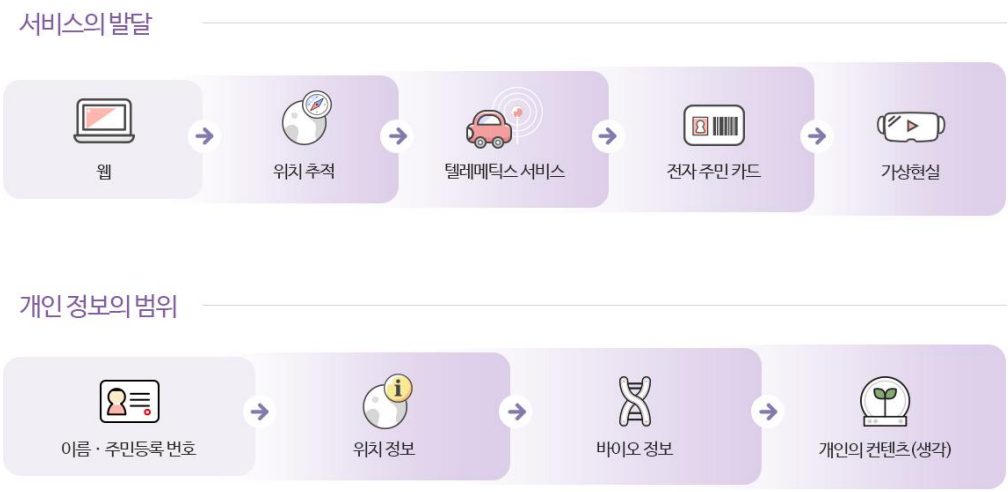
자료:KISA 온라인 개인정보 포털

한국인터넷진흥원 온라인 개인정보 포털에 따르면 [그림 1]와 같이 개인정보는 사회발전과 정보기기 서비스의 발전과 변화에 따라 그 범위는 확대되고 있다. 산업사회에서는 개인정보로 인정되지 않고, 정보항목으로 존재하지 않았던 것들이 기술이 발전함에 따라 개인정보의 영역에 함께 포함되기 시작했다. GPS(global positioning system)기술에 의해 제공되는 위치정보는 GPS기술의 상용화 이전에는 군사기술이나 연구목적 등 제한적으로만 사용되었으며, 개인정보에 해당하는지 여부가 명확하지 않았다. 그러나 현재에 이르러서는 이러한 기술이 일반에도 널리 퍼져 휴대전화기기에 GPS모듈을 내장하는 등으로 개인의 위치정보를 서비스에 활용하면서, 개인의 '위치'를 확인가능하기 때문에 위치정보를 개인정보로서 인정할 수 있는가에 대해서는 반론의 여지가 적다.[5] 이와 같이 개인정보의 개념은 고정불변으로 이해하기보다는, 시대와 기술에 따라 인식이 발전하고 변화하면서 점차 확대되는 개념으로 이해해야 한다.

5) 우리나라는 위치정보의 유출 및 오남용으로부터 사생활의 비밀 등을 보호하기 위해 '위치정보의 보호 및 이용 등에 관한 법률'을 2005년 1월 27일 제정되어 2005년 7월 28일부터 시행하고 있다. 위치정보법에 따르면 사업자는 정보보호 수단을 갖추고 방통위에 신고·허가를 받아야 하고, 개인은 자신의 위치정보 수집·이용 중지를 사업자에게 요구할 수 있으며, 사업자는 이를 거절할 수 없고, 위치정보사업자는 서비스 제공 후 위치정보 수집·이용·제공 사실 확인 자료 외의 개인위치정보는 즉시 파기해야 한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY



[그림 1] 사회의 발전에 따른 개인정보 범위의 확대

산업사회에서 정보사회로 변화하는 시대적 흐름에 따라 정보유통은 물리적, 시간적, 공간적 제약이 축소되었고, 이에 따라 프라이버시의 의미가 점차 변화되었다. 즉, 산업사회 이전에는 프라이버시는 남에게 방해 받지 않는 정도의 소극적 권리에 불과하였다. 이후 산업사회를 거치고 정보화 사회에 도달하면서 프라이버시는 내 정보가 침해로부터 자유로울 권리로 변화하였으나, 이 또한 소극적인 방어에 국한되어 있다는 평가가 있다. 현재 본격적 논의가 진행 중인 스마트시티 사회는 실제사회와 가상사회 간의 통합을 특징으로 하는데, 이러한 경우 프라이버시의 의미는 내 정보의 가치를 보호 받을 권리로 이해가 된다.

<표 2> 사회 발전에 따른 프라이버시 의미 변화

산업사회 (1960년대 이전)	산업・정보화 사회 (1960~2010년)	유비쿼터스 사회 (2010년 이후)
물리적 공간에 의한 제약 존재	시, 공간에 의한 제약 존재	실제사회와 가상사회의 통합
프라이버시는 사전적, 소극적 의미	프라이버시는 소극적 의미	프라이버시는 적극적 의미
물리적 침해로부터 자유로울 권리	내 정보가 침해로부터 자유로울 권리	내 정보의 가치를 보호 받을 권리

자료:KISA 온라인 개인정보 포털

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

2.2 개인정보의 개념

우리나라 정보통신망법에서 정의하는 개인정보란, 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 특정 개인을 알아볼 수 있는 부호, 문자, 음성 및 영상 등의 정보를 말하며, 개인정보의 주체는 자연인이어야 하며, 법인 또는 단체의 정보는 해당되지 않는다. 따라서 법인의 상호, 소재지, 임원 정보, 영업실적 등은 정보통신망법에서 보호하도록 하는 개인정보의 범주에 해당되지 않는다. 또, 개인정보는 [그림 3]과 같이 개인의 성명, 주민등록번호 등 인적 사항에서부터 사회·경제적 지위와 상태, 교육, 건강·의료, 재산, 문화 활동 및 정치적 성향과 같은 내면의 비밀에 이르기까지 그 종류가 매우 다양하고 폭 넓고 사업자의 서비스에 이용자가 직접 회원으로 가입하거나 등록할 때 사업자에게 제공하는 정보뿐만 아니라, 이용자가 서비스를 이용하는 과정에서 생성되는 통화내역, 로그기록, 구매 내역 등도 개인정보가 될 수 있다고 정의하고 있다(한국인터넷진흥원, 2018).

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

[그림 3] 개인정보의 유형

dCollection @ chosun

조선대학교 CHOSUN UNIVERSITY

이강신 등 (2010)은 공공기관의 개인정보보호에 관한 법률을 해석하여 개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보로 정의하였다.[6)]

개인정보는 개인의 성명, 주민등록번호 등 인적 사항에서부터 사회, 경제적 지위와 상태, 교육, 건강의료, 재산, 문화 활동 및 정치적 성향과 같은 내면의 비밀에 이르기까지 그 종류가 매우 다양하고 폭넓으며, 사업자의 서비스에 이용자(고객)가 직접 회원으로 가입하거나 등록할 때 사업자에게 제공하는 정보뿐만 아니라, 이용자가 서비스를 이용하는 과정에서 생성되는 통화내역, 로그기록, 구매 내역 등도 개인정보가 될 수 있다(한국인터넷진흥원, 2018).

한편, 이 개인정보보호법은 일반법으로써 모든 개인정보에 적용되며, 각 산업 분야에서만 제한적으로 적용되는 개별법(특별법)과는 구별된다. 다만, 법 적용에서는 개별법이 일반법에 우선한다. 따라서 정보통신 분야의 개인정보를 다룰 때의 기준이 개인정보보호법과 차이가 있다면, 정보통신망법에서 명시하고 있는 바를 적용한다.

<표 3> 개인정보 보호를 명시하고 있는 개별법(특별법)의 예

분야	법	관련 개인정보
정보통신서비스	정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)	개인정보보호법과 유사한 정의
금융・신용	신용정보법, 금융실명법, 전자금융거래법 등	개인의 신용도, 신용거래 능력 등을 판단하는 정보 등
교육	교육기본법, 초,중등교육법, 고등교육법, 학교보건법등	학생의 학교생활기록 및 건강검사기록
의료	의료법등	개인의 처방전, 진료기록, 병명 등
전기통신사업	위치정보보호법	개인위치정보

자료:KISA 온라인 개인정보 포털

6) 당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

<표 4> OECD 프라이버시 가이드라인 8원칙

수집제한의 원칙	개인정보 수집은 원칙적으로 제한되어야 하고 어떠한 개인정보도 합법적이고 정당한 절차로 수집되어야 하며, 경우에 따라서는 정보주체에게 통지하거나 동의를 얻어야 함
정보 정확성의 원칙	개인정보는 그것의 이용목적에 부합되어야 하고 이용목적상으로 필요한 범위에서 정확하고 완전하며 최신으로 보존되어야 함
목적 구체성의 원칙	개인정보 수집의 목적은 수집할 때에 미리 특정되어 있어야 하고 차후 이용은 구체적인 목적달성과 일치되어야 하며, 수집목적이 변경될 때에는 그 목적이 명확해야 함
사용 제한의 원칙	개인정보가 명시된 목적이 아닌 다른 목적을 위해 공개되거나 이용 및 기타 사용에 제공되어선 안 됨
안전성 확보의 원칙	개인정보는 분실이나 부당한 접근, 파괴, 수용, 수정, 공개 등의 위협으로부터 적절한 안전성확보장치에 의해 보호되어야 함
공개의 원칙	개인정보 처리장치의 개발이나 활용 및 정책은 일반에게 공개되어야 함
개인 참여의 원칙	개인은 정보 관리자에게서 자신과 관련된 자료를 얻을 수 있고 자신에 대한 정보의 소재파악을 할 수 있는 권리가 있음
책임의 원칙	정보 관리자는 모든 원칙이 지켜질 수 있도록 조치를 취할 책임이 음

자료: LG CNS

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

우리나라의 개인정보보호법은 OECE의 프라이버시 보호와 개인정보의 국가 간 유통에 관한 가이드라인의 8원칙을 핵심요소로 개인정보의 라이프사이클 체계를 구축하였다.[7)]

2.3 개인정보의 특징 및 분류

개인정보는 나라마다 모두 비슷한 형태로 정의하고 있으며, 3가지의 특징에 따라 분류 할 수 있다.

첫째, 개인정보는 개인에 관한 정보이다. 즉, 법인이나 단체에 관한 정보는 개인정보의 범주에서 제외된다. 그러므로 개인정보는 <표 5>와 같은 유형으로 존재한다.

<표 5> 개인정보 유형별 종류

유형 구분	개인정보 항목
인적 사항	성명, 주민등록번호, 주소, 본적지, 전화번호 등 연락처, 생년월일, 출생지, 이메일 주소, 가족관계 및 가족구성원 정보 등
신체적 정보	(신체정보) 얼굴, 지문, 홍채, 음성, 유전자정보, 키, 몸무게 등 (의료, 건강정보) 건강상태, 진료기록, 신체장애, 장애등급, 병력 등
정신적 정보	(성향정보) 도서, 비디오 등 대여기록, 잡지구독정보, 물품구매내역, 웹사이트 검색 내역 등 (내면의 비밀) 사상, 신조, 종교, 가치관, 정당, 노조 가입 및 활동 내역 등
재산적 정보	(개인금융정보) 소득, 신용카드, 계좌번호, 동산, 부동산 보유내역, 저축내역 등 (신용정보) 개인신용평가정보, 대출 또는 담보설정 내역, 신용카드사용 내역 등

7) 개인정보 라이프사이클이란 개인정보의 수집, 저장, 이용, 제공, 파기되기까지의 일련의 과정을 말한다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

사회적 정보	(교육정보) 학력, 성적, 출석상황, 자격증 보유내역, 상벌기록, 생활기록부등 (법정정보) 전과, 범죄기록, 재판 기록, 과태료 납부내역 등 (근로정보) 직장, 고용주, 근무처, 근로경력, 상벌기록, 직무평가기록 등 (병역정보) 병역여부, 군번, 계급, 근무부대 등
기타	전화통화내역, IP 주소, 웹사이트 접속내역, 이메일 또는 전화메시지, 기타 GPS 등에 의한 개인위치정보 등

자료:KISA 온라인 개인정보 포털

둘째, 개인정보는 현재 생존한 개인에 관한 정보이다. 즉, 사망자의 정보도 개인정보이기는 하지만 현행 정보보호법의 보호 대상은 아니다.

셋째, 개인정보는 개인을 식별할 수 있다. 즉, <표 6>과 같이, 두 유형으로 구분할 수 있으며, 특히 직접 개인정보는 그 자체로 특정한 개인을 쉽게 식별가능하기에 현존하는 개인정보 중에서 가장 큰 문제점과 파장을 일으키고 있다.

<표 6> 개인을 식별할 수 있는 정보로서의 개인정보 유형

구분	개인 식별 방법	비고
직접 개인정보 (1차 개인정보)	특정 개인을 알아 볼 수 있는 정보	성명, 주민등록번호 등
간접 개인정보 (2차 개인정보)	다른 정보와 용이하게 결합함으로써 특정개인을 식별 가능한 정보	정보주체의 직위, 담당업무 등

2.4 주민등록번호의 중요성

앞에서 프라이버시 및 개인정보에 대해 보았듯 개인정보는 개인을 식별 가능한 정보로써, 직접 개인정보와 간접 개인정보로 구분된다. 특히, 직접 개인정보는 어떤 개인정보보다 중요하고 직접적인 식별기능을 가졌으므로 주민등록번호의 유출은 그 자체로

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

범죄의 시작이고 사회적 또는 경제적 침해로 엄청난 파장을 일으킨다.

주민등록번호는 주민등록제도에 따라 국내에 거주하는 모든 국민에게 발급하고 있는 주민등록증에 기재된 식별 번호이다. 그 시초는 1968년 11월 21일부터 간첩 식별 편의 등의 목적으로 주민등록증이 발급되면서 부여되기 시작했고, 처음 부여된 주민등록번호는 총 12자리였고, 현재처럼 생년월일은 적혀있지 않았지만, 1975년부터 13자리로 바뀌면서 주민등록번호 체계는 앞부분 6자리는 생년월일을 나타내며, 뒷자리는 각각 출생 년대, 성별구분, 최초 주민번호발급 지역코드, 동일한 성 을 가진 지역주민 중 접수 순위, 오류수정번호의 조합으로 구성되어 있다(한국정보진흥원, 2004). 대한민국은 이렇듯 태어날 때 받은 하나의 번호에 지문까지 포함하여 개인의 정보를 모두 담아 관리하는 주민등록제도를 시행 중이며, 비슷하게 개인식별번호를 발급하는 나라도 몇 존재하지만 대한민국처럼 민간의 경제활동에서도 거의 대부분의 곳에서 식별번호를 사용하도록 하는 나라는 적고, <표 7>에서 알 수 있듯이 대부분은 공적 용도로만 제한적으로 사용하도록 한다. 그러므로 이러한 제도를 통해 기본권을 침해하는 문제점이 발생하고 있고, 사회적 문제를 넘어서 경제적 또는 정치적 문제까지 많은 파급효과를 미친다.

<표 7> 주요국의 개인식별번호 현황

국가	개인 식별 번호	형태
미국	사회보장번호	번호 자체만으로 개인정보를 노출 시키지 않는 조합
일본	주민표 코드	생성원칙 없이 무작위로 추출된 10개의 숫자와 1개의 오류 검정 숫자
프랑스	중앙주민등록시스템에 개인식별번호 포함	신원확인을 위한 목적으로 사용하지 않음
스웨덴	우리나라와 유사한 개인식별번호	개인정보보호법에 의해 개인 식별 번호 사용을 엄격히 제한

자료:한국인터넷진흥원

특히, 최근 인터넷과 정보화시대로 바뀐 현실에서 주민등록번호 없이는 아무것도 할 수 없을 정도로 중요함에도 불구하고 오랫동안 주민등록번호는 민간 사업자의 고객관리용으로 아무렇지 않게 사용되거나, 일상생활에서도 본인확인을 위해 대부분 주민등록번호가 사용되어 왔고, 또한 각종 문서나 통신상에서도 주민등록번호가 기본적으

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

로 사용 되어 왔다. 특히, 최근 얼마 전까지 IT 환경은 웹상에서 대부분의 일처리를 하고 있는데 대부분 웹사이트는 회원들의 중복가입을 방지하고 본인 확인이나 성인 인증을 위해 주민등록번호가 활용되어 왔다. 이런 이유로 중국에서의 대한민국 국민의 개인정보를 침해하는 사고가 특히 많이 발생하였으며, 이에 정부는 2014년 8월 7일 개인정보보호법을 개정하여 주민등록번호 수집을 금지하도록 하였다.

3. 개인정보보호 정책관련 국내외 동향

3.1 국내 동향

최근에 개인정보 침해사고는 계속 증가하고 더욱 지능적으로 범죄화 되고 있는데 개인정보보호와 관련된 일반법의 미비로 인한 법 적용의 사각지대가 발생되고 있으며, 다양한 분야에 산재되어 있는 관련법을 통합하여 일원화시킴으로서 일관된 정책과 국민의 권리를 보호하기 위하여 개인정보보호법의 필요성이 제기되었다.

국내에서 이 법의 입법 목적은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현하는 것이다. 이에 따라 개인정보의 수집·이용, 제공 등 개인정보 처리 기본원칙, 개인정보의 처리 절차 및 방법, 개인정보 처리의 제한, 개인정보의 안전한 처리를 위한 관리·감독, 정보주체의 권리, 개인정보 권리 침해에 대한 구제 등에 대하여 규정하고 있다(국가법령정보센터, 2017). 개인정보보호와 관련된 규정 및 그 주요 내용은 <표 8> 및 <표 9>와 같다.

<표 8> 정보통신망법 주요 내용

조문	개정사항	위반 시 처벌	시행일
제 22 조의 2 신설 제 76 조제 1 항 제 1 호 개정, 제 1 의 2 호 신설	스마트폰에 대해 접근권한이 필요한 경우 필수적 권한과 선택적 권한을 각기 구분하여 이용자 동의를 받도록 함 선택적 권한에 대해 미동의시 서비스 제공거부 금지	<3 천만 원 이하 과태료> 선택적 권한에 대해 미동의시 서비스 제공을 거부한 경우 접근권한에 대한 동의방법 마련 등의 조치를 하지 않은 경우	2017 년 3 월 23 일

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

제 24 조 의 제 3 항등 개정	정보통신망법의 취급 누출 개인정보 관리책임자를 처리 유출 개인정보 보호책임자로 조정	-	2016 년 9 월 23 일
제 25 조 제 4 항 개정 제 25 조 제 6 항 등 신설	개인정보 처리 위탁 시 문서에 의하도록 하고, 수탁자에 대한 교육 의무 부여 수탁자는 위탁자의 동의를 얻은 경우에 한하여 재위탁 가능	<관련 매출액 3% 이하 과징금> 위탁자가 관리 감독 또는 교육을 소홀히 하여 수탁자가 개인정보 규정을 위반한 경우 <1 천만 원 이하 과태료> 개인정보 처리 위탁시 문서에 의하지 않는 경우	2016 년 9 월 23 일
제 27 조 제 4 항 신설 제 69 조의 2 제 2 항 신설	기업의 개인정보보호 책임자는 법 위반 사항 발견 시 개선조치 후 대표자에게 보고 방통위는 정보통신망법 위반기업의 임원에 징계 권고	-	2016 년 9 월 23 일
제 32 조의 3 신설	웹에 개인정보가 노출되면 방통위 또는 KISA 는 웹사이트 운영자에게 삭제 차단 요청	직접적인 처벌규정은 없으나 시정조치 명령 후 불이행시 3 천만 원 이하 과태료 부과	2016 년 9 월 23 일
제 32 조의 3 신설	고의 또는 중과실로 개인정보를 유출한 기관에는 가중된 책임을 물어 배상액을 피해액의 최대 3 배까지 중과	-	2016 년 7 월 25 일
제 44 조의 7 제 1 항 제 6 의 2 호 신 설	불법정보의 범위에 개인정보 불법유통 게시 글을 명시적으로 포함	<2 년 이하 징역 또는 2 천만 원 이하 벌금> 게시물 삭제 등 방통위의 명령을 이행하지 않는	2016 년 9 월 23 일

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

		경우	
제 49 조의 2 제 3 항 제 3 호 및 제 4 항 신설	미래부, 방통위, KISA 는 정보통신서비스 제공자에게 접속경로를 차단하도록 요청하거나 이용자가 사기성 정보에 노출되었다는 사실을 이용자에게 통지하도록 조치 미래부, 방통위는 위의 조치를 위해 정보통신서비스 제공자간 정보공유 등 필요한 조치 명령 가능	<1 천만 원 이하 과태료> 필요한 조치 명령을 이행하지 않은 경우	2016 년 9 월 23 일
제 50 조 제 1 항 제 2 호 개정	텔레마케팅시 개인정보 수집 출처 고지 의무화 개인정보 수집출처 고지해야만 수신자의 사전 동의 없이 가능	<3 천만 원 이하 과태료> 개인정보 수집출처를 고지하지 않고 수신자의 사전 동의도 없는 경우	2016 년 9 월 23 일
제 63 조 개정 제 64 조의 3 제 1 항 제 8 호 신설	국외 이전의 유형을 제공(조회 포함), 처리위탁, 보관으로 구분하고 제공은 동의 필요, 처리위탁, 보관은 고지로 갈음	<관련 매출액 3% 이하 과징금> 동의 없이 개인정보를 국외에 제공한 경우	2016 년 9 월 23 일
제 75 조의 2 신설	개인정보 관련 범죄로 인한 이익은 몰수하거나 그 가액을 추징	-	2016 년 9 월 23 일
제 76 조 제 1 항 제 12 호 개정	특정 위반행위에 대한 시정조치 명령 불이행시 과태료를 부과하던 것을 망법 위반 전체 행위에 대한 시정조치 명령 불이행시 과태료 부과로 확대 형사처벌 과태료 부과대상 행위	<3 천만 원 이하 과태료> 시정조치 명령을 이행하지 않은 경우	2016 년 9 월 23 일

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

자료:국가법령정보센터

<표 9> 개인정보보호법 주요 내용

제 70 조	1. 공공기관의 업무를 방해할 목적으로 공공기관의 개인정보를 변경, 말소하여 공공기관의 업무 수행에 심각한 지장을 초래한 자 2. 부정한 방법으로 다른 사람의 개인정보를 취득한 후 부정한 목적으로 타인에게 제공한 자, 이를 교사 알선한 자	10 년 이하의 징역 또는 1 억 원 이하의 벌금
제 71 조	1. 제 17 조 정보주체의 동의를 받지 아니하고 개인정보를 제 3 자에게 제공한자, 제공 받은 자 2. 제 18 조, 제 19 조, 제 26 조, 제 27 조를 위반하여 목적 외로 개인정보를 이용 제공한 자, 제공 받은 자 3. 제 23 조 제 1 항을 위반하여 민감정보를 처리한 자 4. 제 24 조 제 1 항을 위반하여 고유식별 정보를 처리한 자 5. 제 59 조 제 2 호를 위반하여 업무상 알게 된 개인정보를 누설 및 제공한 자, 제공받은 자. 6. 제 59 조제 3 호를 위반하여 권한 밖의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자	5 년 이하의 징역 또는 5 천만 원 이하의 벌금
제 72 조	1. 제 25 조를 위반하여 영상정보처리기기의 설치 목적과 다르게 임의로 조작하거나 녹음기능을 사용한 자 2. 제 59 조 제 1 호를 위반하여 부정하게 개인정보를 취득하거나 처리 동의를 받은 자, 제공 받은 자 3. 제 60 조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자	3 년 이하의 징역 또는 3 천만 원 이하의 벌금
제 73 조	1. 제 23 조, 제 24 조, 제 25 조, 제 29 조를 위반하여 안전성 확보 조치를 하지 않아 개인정보를 분실 유출 훼손당한 자 2. 제 36 조를 위반하여 정정 삭제 등을 하지 않고 개인정보를 계속 이용 제공한 자 3. 제 37 조를 위반하여 개인정보 처리 정지를 하지 않고 계속 이용 제공한 자	2 년 이하의 징역 또는 2 천만 원 이하의 벌금
제 74 조.	1. 직원 등이 회사 업무에 관하여 제 70 조에 해당하는 위반을 하면 행위자를 벌하는 외에 회사도 벌금 2. 직원 등이 회사 업무에 관하여 제 71~73 조에 해당하는 위반을 하면 행위자를 벌하는 외에 회사도 해당 조문의 벌금	7 천만 원 이하의 벌금
제 74	위 죄를 지은 자가 해당 위반행위를 통해 취득한 이익은 몰수	

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

조의 2	할 수 있으며, 몰수할 수 없는 경우 그 가액을 추징할 수 있다. 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있다.	
제 75 조	1. 제 15 조를 위반하여 동의 없이 개인정보를 수집한 자 2. 제 22 조를 위반하여 미성년자 회원가입 시 법정대리인 동의를 받지 아니한 자 3. 제 25 조를 위반하여 화장실 등 사생활 침해 우려가 있는 곳에 영상정보처리기기를 설치 운영한자	5 천만 원 이하의 과태료
제 75 조	1. 수집 이용 제공 시 정보주체에게 알려야 할 사항을 알리지 않은 자 2. 선택 사항 동의를 거절한 이유로 서비스 제공을 거부한자 3. 불필요하게 된 개인정보를 파기하지 아니한 자 4. 법에서 허용한 경우가 아닌데도 주민등록번호를 처리한자. 5. 주민등록번호를 암호화하지 않은 자 6. 주민등록번호를 사용하지 않고 회원 가입할 수 있는 방법을 제공하지 않은 자. 7. 안전성 확보에 필요한 조치를 하지 아니한 자 8. 법에서 정한 범위 외 영상정보처리기기를 설치 운영한자 9. 유출사고를 정보주체에게 알리지 않거나 신고하지 않은 자 10. 정보주체의 요구에도 정당한 사유 없이 열람을 제한하거나 거절한자 11. 정보주체의 요구에도 정당한 사유 없이 정정 삭제 등을 하지 아니한 자 12. 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 아니한 자. 13. 침해우려 등에 의한 처리정지 등의 시정명령에 따르지 아니한 자	3 천만 원 이하의 과태료
제 75 조	1. 개인정보를 분리하여 저장 관리하지 아니한 자 2. 규정을 위반하여 개인정보 수집 동의를 받은 자 3. 안내판 설치 등 필요한 조치를 하지 아니한 자 4. 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자 5. 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자 6. 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자 7. 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자 8. 개인정보 보호책임자를 지정하지 아니한 자 9. 정보주체에게 예외사유, 거절사유, 처리결과 등을 알리지 아니한 자 10. 행안부에 점검 자료를 제대로 제출하지 않거나 검사를 거부	1 천만 원 이하의 과태료

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

	방해 또는 기피한자	

3.2 국외동향

세계 각국은 현재 개인정보보호기관을 설치하여 개인정보보호를 위한 노력을 다양하게 기울이고 있다. 특히 영국, 프랑스, 독일, 호주, 캐나다 등과 같은 국가들은 개인정보를 보호하기 위한 전담기구를 통해 효과적으로 개인정보보호를 수행하고 있다. 이러한 전담기구의 설치는 정보주체의 법적인 이익을 보호하고 불법적 개인정보침해를 효과적으로 방지할 수 있기 때문에 세계적인 추세이다. 그러나 각국의 개인정보보호기관은 기관의 성격이나 기능, 역할, 특성 등의 측면에서 그 나라의 법적 환경이나 사회적, 경제적 특성 등의 측면에서 그 나라의 법적 환경이나 정보화의 진전 여부 등에 따라 각기 다른 모습을 보이고 있는 것 또한 사실이며 각국의 개인정보보호법은 <표 10>과 같다(정보통신정책연구원, 2014).

<표 10> 주요 국가의 개인정보 정의

EU	- 식별되었거나 또는 식별 가능한 자연인(정보주체)과 관련된 모든 정보 의미 - 식별 가능한 자연인은 직접적 또는 간접적으로 식별될 수 있는 사람을 의미하며, 특히 이름, 식별번호, 위치정보, 온라인 식별자(online identifier)등의 식별자를 참조하거나, 하나 또는 그 이상의 신체적, 생리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 대한 사항들을 참조하여 식별할 수 있는 사람을 뜻함 - GDPR(general data protection regulation :개인정보보호 규정)
독일	- 자연인(정보주체)을 특정하거나 특정할 수 있는 인적 또는 물적 상황에 대한 일체의 정보 - 독일연방데이터보호법 제3조
영국	- 데이터 관리자가 보유하고 있거나 향 후 관리할 가능성이 많은 해당 데이터와 기타 정보로부터 신원을 확인할 수 있는 생존하는 개인과 관련된 데이터 - 해당 개인에 대해 표현된 의견이나 데이터 관리자의 모든 지시사항, 그 사람

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

	과 관계있는 모든 타인에 관한 의견을 포함 데이터보호법
미국	- 개인에 관한 정보로 개인의 성명 또는 신분번호, 기호, 지문, 사진 등 개인에게 배정된 신분의 식별을 위한 특기사항 - 미연방 프라이버시법 제 552 조의 2
캐나다	- 그 형태가 어떤가를 불문하고 식별 가능한 개인에 관한 정보 - 연방 프라이버시법 제 3 조 - 신원을 확인할 수 있는 개인에 대한 정보 - 개인정보보호와 전자문서에 관한 법 제 2 조
일본	- 생존하는 개인에 관한 정보로서, 당해 정보에 포함되는 성명, 생년월일, 기타 기술 등에 의해 특정한 개인을 식별하는 일이 가능한 것 - 다른 정보와 용이하게 조합되어 식별할 수 있는 정보 포함 - 개인정보보호에 관한 법률 제 2 조
중국	- 전자 또는 다른 방식으로 기록되는 단독 또는 기타 정보와 결합하여 자연인의 개인 신분을 식별할 수 있는 각종 정보를 지칭하는데, 이름, 출생일, 신분증 번호, 개인생물식별정보, 주소, 전화번호 등을 포함 - 네트워크안전법 제 76 조

자료:해외 개인정보보호 집행체계 및 개인정보보호 주요 동향조사(개인정보처리위원회, 2012)

3.2.1 중국

중국은 우리나라 최고의 교역국이며, 모든 경제 분야에서 급속도로 발전하고 있고, 최근 들어서는 네트워크 안전법을 시행하여 국내 기업에서도 이에 대해 대책을 마련 중이다. 중국은 별도의 개인정보 관련법이 없었지만, 분산되어 있던 네트워크 보호 법률과 개인정보 관련 법률을 통합적으로 관리하고자, 2016년 11월 네트워크 안전법을 제정하고, 2017년 6월부터 시행을 시작하였지만 아직은 체계가 부족하고 구체적이지 않아, 미시적인 법이 지속적으로 제정될 것으로 예상된다. 중국은 1980년대 이후 시장 경제 도입 후 경제적으로는 급성장하고 있지만, 공산국으로서 공산당에 의한 정보와 무역에 대한 모든 통제가 필요한 실정이다. 따라서 네트워크 안전법은 네트워크망과

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

핵심정보 기반시설을 통제하여 안전한 국가 관리를 하고자하는 목적 외에도 폭발적인 인터넷상의 정보교류로 인해 당의 방침에 부합하지 않는 정보를 통제하려는 다른 목적도 가지고 있다. 중국에 사업 진출하고자 하는 기업이 염두에 두어야 할 네트워크 안전법에서 규정하고 있는 중요 데이터의 중국 내 저장 원칙은 아래와 같다.

첫째, 핵심정보 기반시설 사업자는 중국내에서 사업운영 중 수집하고 생성한 개인정보들과 주요 업무 데이터를 중국 국내에 저장해야 한다.

둘째. 업무의 필요에 의해 어쩔 수 없이 해외에서 저장하거나 해외의 주체에게 정보를 제공해야 할 경우에는, 국가 네트워크 정보 부처와 국무원의 관련 부처가 제정한 방법에 따른 안전 평가를 진행해야 한다.

단, 개인정보와 중요 데이터 국외 반출 안전 평가 방법 적용은 세계 각 기업의 반발로 18년 12월로 시행이 유예되었다(LG CNS, n.d.).

3.2.2 EU

유럽은 2차 세계대전 당시 나치의 개인정보 오남용을 통한 유태인 학살을 경험한 후 개인정보를 인권적 차원에서 엄격히 보호하며, 이행이 강제되지 않는 자율규제는 효과적이지 않다고 판단하여 법률규제를 선호하고 있다.

2018년 5월 25일 시행이 예정된 GDPR(general data protection)은 개인정보 보호와 EU내에서의 자유로운 개인정보 이동을 보장하려는 목적으로 제정된 규정으로 법적 구속력을 가지며, 28개 회원국에 적용된다. 개인정보 처리에 있어 정보 주체의 동의와 법적 근거를 명확하게 하고, 정보주체의 권리를 강화하며, 개인정보 취급자-위탁자 사이와 개인정보 처리자-수탁자 사이의 의무사항을 파악하고, 기업의 책임을 강화하는 관리활동의 추가·개선이 있다. EU 밖으로의 개인정보 이전은 원칙적으로 금지되며, 예외로 제3국이 적정한 개인정보 보호체계를 갖추고 있다면 이전할 수 있다. 이를 심각하게 위반하는 경우 전 세계 연매출액의 4% 또는 2천만 유로 중에 높은 금액을 과징금으로 부과하고, 일반 위반의 경우에는 전 세계 연매출액의 2% 또는 1천만 유로 중에 높은 금액을 과징금으로 부과하는 강력한 제재가 예상된다(LG CNS, n.d.).

3.2.3 미국

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

개인정보를 잘 활용함으로써 고객에게 더욱 큰 편익을 줄 수 있다고 보고, 개인정보 관련 규제를 최소화하는 경향을 보이고 있다. 개인정보를 보호하기 위해 정부가 지나치게 관여하면 정보기술의 발전이나 기업체들의 자유로운 활동을 저해할 수 있다고 판단하는 것으로써, 원치 않는 정보의 공개 등으로 프라이버시를 침해하지 않는다면 개인정보의 수집과 이용, 매매 및 마케팅 등은 용이한 편이다. 보호 법률이 없어도 소송이라는 사법제도로 충분히 보호할 수 있다는 입장이다. 하지만 미국은 정보사회에서 개인의 프라이버시 침해를 일찍이 인식한 나라로 개인의 프라이버시를 헌법상의 권리로 인정하고 있다. 지리적, 정치적 영향이 복잡하여 하나의 일반화된 법을 적용하기 어렵기 때문에 개별 법률에 의해 특정한 영역의 개인정보를 보호하는, 개별적인 접근방식을 취하고 있다. 대략 20개 부문에서 프라이버시 혹은 데이터 보안법 및 이와 관련된 법률이 수 백개 가량 존재한다(LG CNS, n.d.).

<표 11> 미국의 개인정보 관련 주요 법률

유형	보호 대상	법	보호 대상
공정신용평가법	신용정보	근로자 거짓말 탐지기 보호법	근로자 정보
프라이버시법	정부보유정보	전화소비자보호법	텔레마케팅 거부 정보
정보공개법	정부보유정보	운전자프라이버시 보호법	운전자, 차량정보
가족의 교육권 및 프라이버시법	교육정보	법집행을 위한 통신 지원법	통신정보
금융 프라이버시법	금융정보	전기통신법	통화정보
프라이버시 보호법	출간정보	건강보험관리 및 책임에 관한 법률	의료정보
케이블통신 정책법	케이블통신정보	아동온라인프라이버시 보호법	아동정보
전자통신 프라이버시법	전자기록정보	금융 현대화법	금융정보
컴퓨터사기 및 남용방지법	컴퓨터접근정보	대 테러 감시법	테러방지정보
컴퓨터 보안법	컴퓨터보안정보	전자정부법	전자정부 서비스

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

			정보
비디오프라이버시 보호법	비디오대여정보	비디오감시방지법	CCTV정보 등
컴퓨터정보결함 및 프라이버시보호법	연방수혜자정보		

자료:LG CNS

자율 규제 원칙의 예시로 옵트아웃 방식을 떠올려 볼 수 있다.[8] 미국의 개인정보 이용 동의나 제3자 제공 동의에는 일반적으로 옵트아웃 방식으로 선택권을 제공하며, 건강관련정보, 학생이나 13살 미만의 개인정보, 신용 보고서, 비디오 시청 선택, 통신사용 정보, 정확한 위치 정보 등의 민감정보는 옵트인 방식이다. 이처럼, 개인정보보호 규정을 상세히 규정한 우리나라나 엄격한 중앙으로부터의 통제를 시행하는 EU와 달리 미국의 자율규제는 각각의 장단점을 갖는다. 우리나라나 EU는 명확한 규정과 구체적인 가이드, 이에 따르는 강제력의 제공으로 효과가 상승하는 반면에, 빠른 기술변화에는 유연하지 못하다. 미국은 이익달성을 쫓는 기업의 자발적인 참여와 빠른 기술대응의 장점이 존재하지만 강제력의 결여로 인한 기업의 탈선 우려와 개별 주체 간에 전문기술이나 노하우 공유가 어려운 단점이 존재한다.

엄격하게 프라이버시를 관리하는 EU와 자유로운 관리의 미국 간의 규제 차이로 인해 EU-미국 간에는 2000년 Safe-Harbor 협정이 체결되어 개인정보의 이전을 가능하게 하였다. EU에서는 자국민 데이터의 EU외부로의 반출을 원칙적으로는 금지하고 있지만, Safe-Harbor 협정으로 특별한 혜택을 미국에 부여했다.

그러나 2013년 들어 미 중앙정보국(CIA)에서 근무하던 에드워드 스노든이 미 국가안보국(NSA)의 무분별한 개인정보 수집을 폭로하면서, 2015년 EU 최고법원 유럽사법재판소는 Safe-Harbor 협정이 EU 시민의 프라이버시 권리를 보호하지 못한다며 무효로 판결하여, 양측은 다시 새로운 협상을 벌였고 2016년부터 프라이버시 실드(shield)가 적용 되고 있다(LG CNS, n.d.).

3.2.4 일본

8) 옵트인(Opt-In):Option-in, 체크박스에 체크가 안 되어 있는 상태로 개인정보 이용 동의를 위해 사용자가 별도의 체크를 해야 하는 방식으로 정보 주체의 정보 보호를 우선(우리나라, EU) 한다.
옵트아웃(Opt-Out):Option-out, 체크박스에 체크가 되어 있는 상태로 개인정보 이용 동의를 위해 별도의 체크가 필요 없으며, 이용 미동의 경우에 체크를 해제하는 방식(미국)이다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

일본의 초기 개인정보보호법은 2005년 4월부터 시행되었으며, 이후 2015년 9월 3일 개선 작업이 완료되어 2017년부터는 전면적인 시행을 하고 있다. 미국의 프라이버시법은 공공정보에 대한 규율이며, 우리나라의 경우 민간과 공공분야 모두를 대상으로 하는 데 반해, 일본은 민간 분야만을 대상으로 규율하고 있다. 일본의 공공 분야는 행정기관이 보유하는 개인정보보호법과 독립행정법인 등이 보유하는 개인정보보호법 등으로 별도 관리되고 있다.

일본의 개정된 개인정보보호법은 IT 환경의 변화에 발맞추고 데이터 활용을 촉진하기 위해 규제를 완화했다. 하지만 해외 국가들, 특히 EU와의 조화를 위하여 필요한 보호수준을 올리는 등 규제강화도 동시에 이루어졌다. 규제완화는 이용가치가 높은 개인정보에 대한 활용의 벽을 제거함으로써 신사업 신서비스를 창출한다는 의미로써, 빅데이터로 대표되는 데이터의 활용을 촉진하고자 개인정보를 익명으로 가공하는 개념의 도입 등을 통해 정부 차원에서 발 빠른 대응을 하는 것을 알 수 있다(LG CNS, n.d.).

3.3 개인정보의 유출 및 노출사고 국내외 사례 및 동향

세계적으로 스마트폰, 태블릿 PC, 넷북 등 다양한 IT 제품 및 서비스가 폭발적으로 증가함에 따라 사회전반에 걸쳐 정보의 검색과 공유가 그 어느 때보다 자유로워졌다. 정보의 검색과 공유가 자유로워진 만큼 일상에서 보안 사고를 경험하는 사건들도 늘어나고 있다. 최근 들어 보안위협이 지속적으로 증가하고 방법 또한 진화하고 있으며, 공격방법은 더욱 지능적이고, 지속적으로 이루어진다. 지능형 지속공격(APT: Advanced Persistent Threat)는 해킹을 시도하는 개인이나 그룹이 명확한 목적을 가지고 특정 대상을 겨냥하여 지능적이고 복합적인 방법을 동원하여 지속적으로 공격하는 위협형태를 말하며, 정부의 웹사이트가 공격을 받아 개인정보가 유출되기도 하고, 자신의 컴퓨터가 좀비 PC가 되기도 한다(임설화 등, 2014). 이러한 보안 사고는 정부 뿐 아니라 금융기관이나 온라인서비스 기업을 가리지 않고 빈번히 나타난다. 이런 인터넷상의 각종 부작용 중 그 문제가 가장 심각한 것은 개인정보유출에 대한 부분이며 국내외 개인정보 유출 사례는 <표 12> 및 <표 13>과 같다(이문구, 배춘석 2013).

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

<표 12> 국내 개인정보유출 주요 사고 사례

피해 기관(시설)명	내 용	상세 내용
인터파크해킹 (2016 년 8 월)	고객정보 유출 (2,665 만 건)	- 악성코드가 첨부된 e 메일을 열람하여 악성코드에 감염 - 파일공유서버 접속하여 악성코드 설치 -개인정보 취급자 PC 로 접속 하여 DB 서버로 접속하여 개인정보를 탈취함.
3.20 전산대란 (2013 년 4 월)	주요 방송국 , 금융사 전산망 마비	- 목표 조직의 내부 PC 를 악성코드로 감염시켜 자산관리서버의 로그인 인증 취약점을 이용하여 접근, HDD 파괴 악성코드 배포 - 2012 년 6 월경부터 국내 금융사 전산망에 1,590 회나 침입 - 총 4 만 8 천여 대의 PC, 서버가 피해를 입음
넥슨메이플스토리 해킹 (2011 년 11 월)	고객정보 유출 (1,320 만 건)	- 내부 직원 PC 를 악성코드로 감염, 서버 운영관리자의 PC 또한 뚫림 - 정보 수집을 통해 백업시스템 접근권한 획득, 개인정보 유출
SK 커뮤니케이션즈 해킹 (2011 년 7 월)	고객정보 유출 (3,500 만 건)	- 네이트 DB 의 가입자 3,500 만 명의 계정정보와 이름이나 주민등록번호 및 연락처 등의 개인정보유출 - 웹서버 취약점과 내부의 비인가 SW 사용을 이용하여 악성코드를 유포, 중요서버의 접근권한 획득, 개인정보 유출
농협해킹 (2011 년 4 월)	서비스 마비 (18 일)	- 서버관리용 노트북의 외부 반출 입을 통해 악성코드 감염 - 내부 확산점령. 중요 서버의 계정정보 등 수집 - 서버들이 서로를 공격하여 절반이 파괴
현대 캐피탈 (2011 년 4 월)	고객정보 유출 (175 만 건)	- 퇴직한 직원의 계정을 습득하여, 메일서버 및 업무서버에서 고객정보 해킹
옥션 해킹 (2008 년 2 월)	고객정보 유출 (1,081 만 건)	- 이메일을 통해 내부 PC 에 침투 - 관리자 PC 에 키로거 설치, 서버 접근계정을 통해 고객정보 유출함

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

<표 13> 해외 개인정보유출 주요 사고 사례

피해 기관(시설)명	내용(피해규모)	상세 내용
야후해킹 (2014 년)	개인정보 유출 (5 억 명)	- 야후 가입자 개인정보 유출건수 5 억 여건으로 사상 최대 규모 해킹사건
소니해킹 (2011 년 4 월)	고객정보 유출 (1 억여건)	- 룰즈섹 해커그룹, 16 차례 이상 해킹 - 소니 가입자의 개인정보 유출 1 억 여건
EMC・RSA 해킹 (2011 년 3 월)	보안인증 기술 (OTP) 유출	- SNS 로 공격대상 정보수집, 사회공학적 기법으로 악성코드 감염 - 이후 범용 SW 의 제로데이 취약점을 이용 정보탈취
글로벌 에너지 기업 해킹 (2011 년)	산업관련 기밀자료 유출	- 취약한 웹서버에 SQL 인젝션 공격으로 악성파일 업로드 - 스피어-피싱을 통한 계정정보 획득하여 내부 PC 감염 - 획득한계정정보로 계정 추가수집 및 시스템 접속 - 표적대상서버 서서히 접근, 자료 유출(2009 년~2011 년)
이란원자력발전소 마비 (2010 년 7 월)	핵 발전시설 시스템 마비	- 독일 지멘스사의 산업자동화시스템, SCADA 임의 제어 - 원심분리기 1,000 여대 작동 불능 상태로 만듦 - USB 로 내부망 침투, 제로데이 취약점을 이용해 확산 - 인터넷 연결된 PC 감염, 내부 정보를 스캔
모건 스탠리 해킹 (2010 년)	산업관련 기밀자료 유출	- 구글과 모건스탠리를 해킹, 내부 중요정보를 탈취 - 2009 년 6 월에 시작하여 6 개월간 지속된 것으로 확인됨

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

100여 개국 대사관 및 정부기관 해킹 (2009년)	국가 기밀 유출	- 전 세계 103개국의 대사관과 정부기관 잠입하여 국가기밀 유출 - 감염된 호스트의 평균 활동시간 145일 - 2007년 5월에서 2009년 3월까지
미국국방부, 항공우주국 해킹 (1999년)	국가기밀 유출 (핵무기 정보, 군사 시설 지도, 병력 구성 등)	- 1998년부터 1년 동안 지속되었음 - 미 국방부는 침입자를 역추적하여 구소련 해커의 소행을 주장함, 러시아는 확인거부

4. 정보보안 위협요인

현대 사회는 컴퓨터와 인터넷 등 ICT(information and communication technology) 기술의 발달로 인한 정보화 및 자동화를 주축으로 한 3차 산업혁명에서 인공지능, 로봇기술을 통해 실제와 가상을 통합하여 사물을 자동적이고 지능적으로 제어 가능한 가상 물리 시스템의 구축까지도 기대되는 4차 산업혁명 시대로 들어가고 있다고 볼 수 있다. 4차 산업혁명은 사물인터넷과 클라우딩 컴퓨팅의 발전 및 확산으로 인간과 사물 간의 연결성이 확대되고 인공지능과 빅테이터의 연계 및 융합으로 산업구조의 근본적인 변화가 기대되고 있다. 그러나 4차 산업의 핵심동력인 데이터를 제대로 통제하지 못하여 부정사용, 불법유출이 나타난다면 개인, 사회 뿐 아니라 국가적으로도 큰 파장이 일어날 것이다.

Verizon(2016)은 82개국의 다양한 데이터 유출과 사고들을 정리하였는데, 금전적인 목적으로 공격자나 해커들에 의해 데이터 유출 및 사고가 일어난다는 것을 알 수 있었다. 데이터 유출과 사고의 차이는 데이터 유출이 인증되지 않은 당사자들에게 정보가 노출되거나 유출되는 사고를 말하고, 데이터 사고는 정보의 완전성이나 기밀성 그리고 유용성의 손상을 가져오는 보안 사건을 말한다. 정보보안을 위협하는 요소로서 데이터 유출, 보안 취약성, 피싱 그리고 특히 최근에 드러나는 9가지로 유형화 될 수 있는 공격 패턴이 있다(조성필 2017).

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

4.1 데이터 유출

버라이즌 데이터 유출 수사 보고서(Verizon Data Breach Investigations Report, 이하 DBIR)에 따르면, 2015년 들어 가장 많은 공격을 받은 곳은 데이터 유출만 795건 발생한 금융기관들이었다. 이어서 호텔 및 숙박업에서 282건, 정보 산업에서 194건, 공공 기관에서 193건, 도소매업에서 137건, 의료 및 건강 산업에서 115건 순이었다. POS 공격에 대한 보안인식이 높아짐에 따라 도소매업에서 발생한 정보 유출 사건은 2014년에 비해 줄어들었고, 해커들은 호텔 및 숙박업으로 눈길을 돌려, 이 부분에서는 공격이 늘어났다(문가용, 2016).

파수닷컴과 포네몬 연구소가 발표한 '위험에 처한 기업들: 내부 임직원들에 의한 중요 정보의 유출 위험' 보고서에 따르면, 미국 내 IT 보안 실무자 637명을 대상으로 조사결과 정보유출 주요 원인은 임직원 부주의(56%), 단말기 유실이나 도난(37%), 시스템 문제(28%) 순이었다. 응답자 70%는 중요 정보가 어디 있는지 위치를 파악하지 못했고, 60%는 임직원 문서 사용과 공유 현황 가시성이 확보되지 않았다고 응답했으며, 73%는 지난 12개월 동안 중요 정보가 유출됐다고 답했다. 기업 80%이상이 중요 데이터에 대한 적절한 권한과 보안 레벨 결정에 고민했으며, 중요 정보에 대해 효과적으로 접근 통제를 진행하는 기업은 15%에 불과했다고 한다(김인순, 2016).

4.2 보안 취약점

취약점은 공격자가 시스템의 정보 보증을 낮추는데 사용되는 약점이다. 취약점은 세 요소의 교집합으로 정의할 수 있으며 시스템 민감성이나 결함, 공격자가 결함에 대해 접근할 가능성, 탐색할 가능성이 그것이다. 취약점을 탐색하기 위해 공격자는 시스템의 약점에 접속 가능한 툴이나 기법이 필요하다. 이 경우에 취약점은 공격 영역으로도 불린다.

취약점 관리는 취약점을 확인하여 분류하고 치료 또는 완화시키는 과정이다. 이 과정은 일반적으로 시스템에서 소프트웨어 취약점을 나타내며 보안 위협은 취약점으로 분류될 수 있다. 취약점은 위험과는 다른데, 위험은 심각한 손실가능성과 관련되지만 취약점들 중에는 위험성이 없는 경우도 있다. 공격을 구현하려는 목적으로 사용될 수

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

있는 취약점을 탐색 가능한 취약점이라고 하며, 취약성 창문(window of vulnerability)은 취약점이 나타나 분명해진 때부터 보안이 바로잡혀 접근이 막히고 공격이 비활성화된 때까지이다. 보안 버그는 더 좁은 개념으로 소프트웨어와 무관한 취약점이 있다. 하드웨어와 사이트 및 인적 취약점들이 소프트웨어 차원의 보안 버그와 무관한 것들의 예이다. 프로그래밍 언어에서 적절히 사용되기 어려운 구조체가 많은 취약점들의 근원지이다(위키백과, n.d.).

4.3 피싱

피싱이란 개인정보를 뜻하는 프라이빗 데이터와 낚시를 뜻하는 피싱의 합성어로 금융기관 같은 웹사이트나 공적인 메일로 위장하여 개인정보 등을 빼내 이를 범죄에 이용하는 사기수법이다. 대표적으로 이메일의 발신자명을 금융기관의 창구 주소로 위장한 메일을 무차별적으로 전송하는 것이 있다. 메일을 열면 개인정보를 입력하도록 안내하는 글과 웹사이트로의 링크가 있는데, 클릭해 들어가면 해당 금융기관의 정규 웹사이트와 유사한 디자인의 개인정보입력용 팝업창이 표시된다. 메인 창에 표시되는 사이트는 정말 해당 금융기관 사이트이지만, 팝업 된 페이지는 가짜이다. 진짜를 보고 안심한 사용자는 팝업창의 입력란에 인증번호와 비밀번호, 카드번호 등을 입력하고 이는 피싱을 하려는 자에게 송신된다. 또한 URL에 특수한 서식을 이용하여, 진짜 도메인에 링크된 것처럼 보이게 하거나, 팝업창의 어드레스바를 표시하지 않는 등 그 수법이 교묘하여 피해자가 속출하고 있다.

메일 및 메신저와 같은 웹 기술을 이용하는 피싱은 기존의 전통적인 방식의 사기와는 달라 이에 대한 기술적 대응이 필요하다. 최근에는 DNS 하이재킹 등을 이용해 사용자를 위장 웹사이트로 유인하여 개인정보를 절도하는 피싱의 진화된 형태인 파밍(pharming)도 출현하고 있다.

피싱기술에는 사회공학적인 방법, 링크조작 방법, 웹사이트 위조 방법, 중간자 공격 등이 있으며, 피싱의 대응 방안으로는 브라우저 경고, EV 인증서, 강화된 비밀번호 로그인, 개인정보 관리프로그램 등 기술적인 방안과 피싱의 인식 제고 활동, 피싱 대응 실천문화 확산, 피싱 정보의 공유 및 신속한 대응과 같은 사회문화적 대응 등 마지막으로 법제도적 대응 방안이 있다(정교일 등, 2008).

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

4.4 보안 침해 9가지 공격 패턴

기업에서 발생할 수 있는 대부분의 보안침해 사건은 아래 <표 14>와 같이 9가지 패턴으로 분류된다(Verizon, 2014). 이를 통해 보안위협을 이해하고 보안 관련 업무의 우선순위를 지정할 수 있으며, 위 9가지 패턴이 10만 건이 넘는 보안 사고의 92%를 차지할 뿐만 아니라, 한 업종의 보안사건 가운데 9가지 패턴 중 단 3가지로 설명 가능한 사건의 비율이 72%를 차지하며, 대부분의 업종에서 보안 사건의 50% 이상이 위의 9가지 패턴 중 단 3가지에 해당한다(김태형, 2014).

<표 14> 국내 보안침해 주요 사고 사례

보안침해 패턴 명	설 명
기타 오류	보안을 저해하는 모든 실수를 의미한다. 개인정보를 공개적인 사이트에 실수로 게시하거나 잘못된 수신자에게 전송하거나, 문서나 자산 등을 안전하게 폐기하지 않는 것 등이 포함된다.
크라임 웨어	크라임웨어에는 서버나 데스크톱 등 시스템을 침해하는 멀웨어 사용이 모두 포함되며 피싱도 이 패턴에 포함된다. 공공부문, 정보 유틸리티 및 제조업계의 위험이 가장 높은 것으로 나타났다.
권한의 잘못된 사용	주로 내부자의 잘못으로 발생하지만 공모에 가담한 외부인이나 권한을 가진 파트너가 문제를 일으킨 경우도 있다. 일선 직원부터 이사회에 이르기까지 기업 내 모든 직급에서 문제가 일어날 수 있다.
물리적 도난 및 분실	업무용 장비, 저장장치, 인쇄된 서류와 기타 정보 자산이 분실·도난 되는 것을 의미하며 대부분 사무실에서 발생하지만 차량이나 가정에서도 발생한다. 어디에서나 일어나는 사건이지만, 의료 서비스 부문 보안 사건의 45%가 이런 경우에 해당된다. 공공부문에서도 이 패턴에 해당되는 사건이 자주 발생한다.
웹 앱 공격	콘텐츠 관리 시스템이나 전자상거래 플랫폼 등의 웹 애플리케이션에서 공격자가 자격 증명을 훔쳐 사용하거나 취약성을 악용하는 경우이다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

DoS 공격	보안 침해 시도가 아니라 공격을 의미한다. 공격자가 PC나 강력한 서버를 활용해 악성 트래픽으로 조직의 시스템을 마비시켜 결국 정상적인 운영을 하지 못하도록 경우이다. 금융이나 소매 및 기타 유사한 업종의 상거래 시스템을 주로 공격한다.
사이버 스파이	스파이가 지적 재산을 노려 피싱 공격을 통해 조직의 보안을 침해하는 것이다. 스파이는 정부나 군사 기관만 노리지 않으며, 전문 서비스업 운수업, 제조업, 광업 및 공공부문도 인기 있는 대상이다.
POS 침입	결제 데이터 유출을 위해 POS 컴퓨터 및 서버를 공격해 손상시키는 경우다. 많은 POS 장치를 보유하는 접객 및 소매업 쪽이 최대의 공격 대상이지만 이외에도 의료 서비스나 결제 처리 등 업무 역시 위험하다.
결제카드 조작	'조작 장치'를 ATM이나 주유 펌프 또는 POS 단말기에 설치하여 결제 시의 카드정보를 읽는 것이다. 은행이나 소매 또는 접객 업체가 주요한 대상이다.

5. 4차 산업과 정보보안

스위스 다보스포럼 의장인 Klaus Schwab은 그의 저서 제4차 산업혁명(The Fourth Industrial Revolution:2016)을 통해 현재 인류는 지금까지 아무도 미리 내다보지 못할 정도의 빠른 기술혁신에 따른 제4차 산업혁명 시대를 맞이하고 있다고 선언했다. 산업의 변화는 1760년대 증기기관의 발명으로 1차 산업혁명이 시작되었고 이렇게 촉발된 산업혁명은 110년이 지나 전기를 중심으로 나타난 에너지 혁명으로 2차 산업혁명, 다시 약 100년이 지나 IT 산업의 시작으로 3차 산업혁명이 전개되었고, 미처 50년이 지나기도 전에 또 다른 산업혁명의 모습으로 나타나고 있다.

증기, 에너지, IT에 이어서 제4차 산업혁명의 핵심은 인공지능과 모든 사물을 네트워크로 연결하는 사물인터넷(IoT:Internet of Things)이라고 할 수 있다. 초지능과 초연결은 수십억의 인류와 더 많은 전자기기들이 모바일로 연결되는 환경을 제공한다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

인공지능과 사물인터넷을 통해 나노기술, 3D프린팅, 재료공학, 생명공학, 에너지 저장, 퀀텀 컴퓨터, 로봇공학, 자율주행자동차 등 산업과 생활 전반에 걸쳐 혁명적 변화를 가져오게 된다. 이와 같은 혁신으로 학문이나 기술의 분야 간 경계를 없애고 융합시대를 만들어 나갈 것이다.

초연결의 시대에 도달하면서 가장 큰 우려 사항 중 하나는 정보 보안(information security)이다. Schwab(2015)은 “우리는 일상적으로 사용하는 여러 기기를 통해 편리함을 대가로 기꺼이 사생활을 제공하려는 경향을 점점 보이고 있다”는 것을 지적하고 있다. 문제는 이런 자발적 정보 제공뿐만 아니라 자기도 모르는 사이에 의도적이지 않은 정보누출이 횡행하게 되었다는 점이다. 특히, 악의적으로 대량의 정보 데이터를 누출하는 일은 단순한 개인정보누출을 넘어서 재산과 신체에 심각한 위협을 미칠 수 있다는 것이다.

대규모 온라인 운영자는 큰 규모의 데이터 세트 집적을 통해 사용자의 제공정보보다 훨씬 더 많은 양의 정보를 생성할 수 있다. 빅 데이터의 분석과 추론을 통해 유추된 추가적인 정보는 사용자가 모르는 자신에 대한 정보가 만들어지고, 이것의 비의도적인 유출은 심각한 문제를 야기하는 경우가 생긴다. 실질적인 위험은 금융기관에서 일어나는 정보유출로써, 개인의 자산은 대부분 금융기관에 보관되어지기 때문에 금융기관에 대한 공격은 그 후유증이 매우 크다. 결국 제4차 산업에서의 초연결은 초보안의 필요성이 강조되는 환경을 만들게 된다.

6. 4차 산업혁명 시대의 정보보호 기술동향

보안 산업에 기반이 되는 정보보호 기술은 암호, 인증, 인식, 분석・감시 등의 보안기술이 적용된 제품을 생산하거나, 관련 보안기술을 활용하여 개인・기업・국가의 안전과 신뢰를 보장하는 서비스를 제공하는 기술로 정의된다(정보통신기술 진흥센터, 2016). 네트워크・시스템 기반 정보보안과 안전・안심 생활목적의 물리보안, 보안기술과 전통적인 산업의 융합으로 창출되는 융합보안을 포함하고 있고, 컴퓨터・네트워크 수준의 보안을 넘어 감시, 의료, 전력 등과 같은 사회전반의 보안으로 확장되면서, IT 기반 미래 지식정보사회에서 개인・기업・국가 안보의 핵심역할을 수행한다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

4차 산업혁명 시대의 정보보안 산업은 개인에게 디지털 안심생활 인프라를 제공하고, 사회전반에 걸쳐 안전한 디지털 치안 인프라를 구축하며, 국가적으로는 디지털 안보 인프라 마련을 지향하고 있다.

[그림 3] 4차 산업혁명 시대 정보보안 산업 분류

6.1 디지털 안심생활 인프라

4차 산업혁명시대에 개인 생활과 직접적으로 관련된 대표적인 현안으로는 공인인증서 등 불편한 금융거래와 개인정보 유출에 의한 프라이버시 침해, 지능정보사회의 부작용으로 스마트 자동차·의료·헬스케어의 해킹 위협과 신규 ICT 기술 적용에 대한 불안이 증가되고 있는 상황이다.

[그림 3]와 같이 개인 안심 분야는 사용자가 불편하지 않고, 프라이버시 침해 없는 디지털 안심생활 인프라 구축을 지향하고 있다. 복잡한 금융거래 보안절차로 인한 불편함을 해소하고, 빅데이터 프라이버시 보호로 개인정보 유출 방지하며 개인의 생명과 재산을 위협할 수 있는 신 디지털라이프 서비스에 대한 신뢰와 안전을 보장하는 안심생활 인프라 관련 보안기술이 개발되고 있고 세부 분야별 기술동향은 아래와 같다.

6.1.1 핀테크 보안

바이오, 행위, 환경, 관계 등 정보를 이용한 간편한 인증과 분산 거래 서비스를 위한 O2O(online to offline) 분산거래 보안 플랫폼제공을 목표로 하고 있다. 간편 결제·인증 기술로 편리한 인증과 안전한 거래를 지원하는 신속한 온라인 인증(Fast Identity

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

Online, 이하 FIDO기반 간편 결제·인증 기술이 최신 금융·IT 기술과 접목을 통해 사회 全분야로 빠르게 확산 중에 있으며, FIDO와 TEE2), NFC-HCE3), MST4) 등 최신 IT 보안기술이 적용된 간편 결제 서비스가 미국, 일본, 중국 등에 빠르게 확산되는 중이며, 전자금융, 이동통신, 전자정부 분야에서도 인증수단을 다양하게 적용한 FIDO 간편 인증 서비스도 제공 중에 있다.

6.1.2 빅데이터 프라이버시

클라우드 및 빅데이터 환경에서 개인정보유출에 대한 우려가 커지면서, 개인정보 빅데이터의 비식별화 및 암호화된 상태에서의 연산을 통한 개인정보 유출 방지 기술이 새롭게 주목을 받고 있다. 모바일, 클라우드 환경에서 ICT 신규 산업과 서비스의 출현에 따라 프라이버시 보호를 위해 기존에 없던 암호 응용기술이 요구되고 있고, 단기·실용적인 관점에서 형태보존, 순서보존, 검색가능 암호 등의 연구가 진행되고 있으며, 중장기적으로는 동형암호 연구가 핵심기술로 부각되고 있다. 민감한 개인정보가 포함된 데이터베이스에서 프라이버시를 보호하면서도 필요한 통계량을 정확히 추출하기 위한(Differential Privacy, PPDM(privacy PreservingData Mining)등이 연구되고 있으며, Differential Privacy 기술은 구글의 오픈 소스 래포(Randomized Aggregatable Privacy -Preserving Ordinal Response, 이하 RAPPOR), 애플의 iOS 10 등에 적용되고 있다.

6.1.3 자동차·의료·헬스케어 보안

개인의 생명을 위협할 수 있는 스마트 자동차 및 의료 서비스의 안전한 운영을 보장할 안심케어 기술이 새로운 보안 기술영역으로 주목을 받고 있다. 지능형 차량 보안 기술은 차량 내·외부 네트워크와 내부장치 보안 기술을 위주로 하여 연구개발이 진행되고 있고, 차량과 기반시설 간의 안전한 통신을 위한 인증기술 개발 및 C-ITS 보안 기술개발이 지속 추진될 것으로 예상된다. 차량 간의 통신 기술은 상용화를 앞두고 있으나, 보안 기술 연구는 ECU와 차량내부통신망(CAN) 보안 등에서 제한적으로 진행되고 있다.

의료기기 침해를 방지하기 위한 기술은 헬스케어·의료 기기 및 게이트웨이에서의 보안취약성을 탐지·차단하기 위한 기술 개발이 지속적으로 진행되고 있으며, 미국

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

MIT에서는 의료기기 악성코드 탐지기법 등 60여개 이상의 헬스케어보안(SHARPS) 프로젝트를 진행하고 있고, 퍼듀와 프린스턴 대학은 무선 심박동기 및 인슐린 펌프 등 의료기기용 외장형 방화벽인 MedMon을 개발했으며, Arxan사는 화이트박스암호를 이용한 모바일의료 앱 템퍼링 방지・치유, MHR(medical health record) 데이터 프라이버시, 기밀성보장 솔루션을 개발하였다(정보통신기술 진흥센터, 2016).

6.1.4 증강・자율거래 보안

개인의 일상에서 안전 위협요소와 위·변조 정보를 자동인식하고 지능을 가진 사물이 안전하게 거래할 수 있는 신뢰 기반을 제공하기 위한 솔루션들이 개발되고 있다. 이와 관련하여 바이오인증 및 이상행위탐지 기술은 이용환경이나 행위패턴 등의 사용자 중심으로 기계학습 분석을 통해 인증을 강화하고 효과적인 이상행위 탐지가 가능한 연구 투자가 확대되고 있다.

행위기반 바이오인증(behavioral biometrics)기술은 학계, 스타트업, 글로벌 IT기업 등에서 활발히 연구되고 있으며, 금융권의 적용시도가 증가되는 추세이며, 패스워드를 대체하기 위해 비헤비오섹(behaviosec.com) 인증솔루션, 구글의 Abacus 프로젝트 등은 사용자 기기에서 센싱되는 다양한 행위정보로 사용자를 인증하는 기술을 개발하고 있으며 금융기업과 협업을 진행 중이다.

최근 전자금융 거래의 탈중앙화와 투명성 증대, 확장성과 보안성 강화를 높이기 위한 방안으로 블록체인 기술에 대해 관심이 증가하고 원천 연구가 활발히 진행 중이다. 블록체인 기술의 금융권 적용 방안을 모색하기 위해 글로벌 블록체인 컨소시엄(R3 CEV)이 구성되었으며, 블록체인의 불변성을 응용한 다양한 보안 솔루션이 개발되고 있다. 예를 들어, Blockai는 사진, 그림 등 저작물의 해시를 블록체인에 저장 관리하는 저작권 보호 서비스를 개발하였다.

DAO(decentralized autonomous organization), BaaS(blockchain as a service), Blockchain of Things 등 다양한 응용분야 적용을 위한 프로젝트들이 진행 중이지만 보안에 대한 충분한 검토 없이 진행된 프로젝트들에 대해서는 일부 우려가 제기되고 있다. 세계 제2의 가상화폐인 이더리움의 스마트 컨트랙트 기술을 활용해 운영되는 DAO의 해킹 사례가 나타나 보안의 우려가 증가되는 측면도 있다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

6.2 디지털 치안 인프라 구축

보안 산업 측면에서의 대표적인 사회적 현안으로는 금융망 마비, DDoS, 랜섬웨어 등 지능화·은밀화 되고 있는 표적공격에 대한 실시간 대응 미흡으로 사회 안전 위협이 고조되는 바, 사이버 및 물리적 환경에서 효율적인 사회 안전 시스템 구축이 필요한 상태라고 할 수 있다.

따라서 사이버 범죄 및 물리적 신변 위협에 지능적으로 대응하는 디지털 치안 인프라 구축을 위해 사이버위협 사전·사후 대응을 위한 지능형 침해대응, 시공간 위험 인지의 지능형 도시감시 기술, 초연결 위협에 대응하는 고신뢰 IoT 보안 인프라 및 기계가 스스로 대응하는 자율 해킹 방어 기술 개발이 진행되고 있다.

6.2.1 지능형 침해 대응

날로 고도화된 사이버 범죄의 사전방어를 위한 사이버 자가방어 기술 및 신종 악성코드 대응 등의 클라우드 기반 지능형 보안서비스 기술 개발을 목표로 AI기술을 이용한 지능형 침해 대응기술 개발이 진행되고 있다. 인공지능 기반 침해사고 분석・대응 기술은 딥러닝・머신러닝 등을 이용한 인공지능 기반의 침해사고 자동탐지 및 이를 통한 침해사고 대응정보 자동생성기술 개발로 발전하고 있다.

매사추세츠공과대학교(Massachusetts Institute of Technology, 이하 MIT)에서는 인공지능과 분석가의 직관력을 결합하여 아직 알려지지 않은 공격에 대해서도 사전 탐지를 할 수 있는 AI2를 개발하였으며 또한, 기 분석된 침해사고 보고서 및 현재 발생되고 있는 모니터링 정보의 기계학습을 통해 현재 발생되고 있는 정보 중 침해사고와 연관된 정보와 이를 조치할 수 있는 정보를 분석가에게 제공하는 기술을 연구 중에 있다. IBM의 왓슨 시스템의 보안 적용을 통한 IBM Cognitive Security 서비스를 2016년 말 출시하였으며, 이를 통해 보안 분석가의 수동분석 지원, 침해사고 의심정보 제공 및 의심정보의 대응 방법을 제공하고 있다.

6.2.2 지능형 도시 감시

물리적 시공간에서 발생하는 다양한 위험상황을 전지적 감시 시점으로 인식, 추적,

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

검색, 예방 및 대응하는 차세대 AI치안 플랫폼 개발이 진행되고 있다. 광역 도메인 내의 다중 센서 정보를 복합 연계·분석해서 위험상황을 실시간 탐지, 대응 및 과거 위험을 역추적하고 미래 위험을 예측하는 지능형 영상분석의 시티 서베일런스 연구 개발이 진행되고 있다.

미국은 CCTV, 차량 번호판 감지기, 911 전화, 방사능 측정기 등을 실시간 복합·연계해서 도시 전체의 위험상황을 감지・대응하기 위한 인텔리전트 시티 서베일런스가 운용중이며, DAS(domain awareness system)는 NYPD, MS 등이 공동으로 개발하고 있는 상태이다.

영상기반 시티 서베일런스 기술은 기존의 알고리즘 방식에서 벗어나 기계학습 기반 신경망 기술인 딥러닝 방식으로 발전하고 있으며, 다양한 분야에 확대·접목되고 있다. 구글은 세계 최고수준을 갖춘 딥러닝 기술과 빅데이터를 기반으로 인지와 검색 등에서 독보적인 입지를 구축하고 있으며, MCT(Multi Cameras Tracking), 대규모 이미지・비디오의 분류, 검색 등 지능형 영상분석 원천기술력 확보에 주력하고 있다. 휴먼 바이오인식 기술은 인식 성능과 편리성, 보안성을 모두 보장하는 비제약형 바이오 인식 기술로써 발전하고 있으며, 융합산업 핵심 길목기술로 대두되고 있다. 페이스북은 하루 10억 명 이상의 규모인 사용자 빅데이터를 바탕으로 인간의 시각지능 수준의 딥러닝 기술을 개발해서 얼굴인식・분류・검색에 적용하고 있다. 중국 바이두는 딥러닝 권위자인 앤드류 응 교수를 영입해서 단숨에 세계수준의 영상, 음성인식(deep speech) 원천기술을 보유하고 있고, 매년 인공지능연구에 3억 달러 이상, 300명 이상의 전문연구 인력을 투자하고 있다. 또한, 지문・얼굴・홍채・음성 등의 다양한 바이오인식 센서를 연동해서 위험 인물을 실시간으로 추적하기 위한 NGI(next generation identification) 시스템이 미국 FBI에서 파일럿 프로그램으로 운용 중에 있다.

6.2.3 능동보안 인프라

모든 사물이 초연결 되는 새로운 IoT 환경에서 사물주체, 객체들이 스스로 협력하여 자율적 대응이 가능한 고신뢰 자율 네트워크 인프라 구현을 목표로 진행하고 있다. 각 사물의 실행 환경오염 방지, 정보 위변조 방지 및 악의적 재사용 방지를 위한 IoT 디바이스 별로 암호 키를 별도의 하드웨어를 이용하여 보호하는 신뢰 플랫폼 모듈(trusted platform module) 기술개발이 개발되었다. HP, IBM, MS의 합작으로 설립된

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

신뢰 플랫폼 모듈은 신뢰성 높은 컴퓨팅 플랫폼 표준화를 추진 중이며 저장키 기반의 TPM 표준을 개발 중에 있다.

IoT 기기의 이상 징후를 상황정보 기반으로 스스로 분석·판단하기 위한 경량화된 석·탐지 기술 개발과 악성코드 감염, 취약점 존재 여부 등의 상세분석을 통해 대응 기반 정보 생성을 위한 클라우드 기반 보안 분석 기술이 개발 중이다. 특히, IBM의 Watson IoT Platform은 장비 인증, 통신 암호화, 메시지 체크섬 관련 API 등 Platform 측면에서 보안 기능을 제공하고 있어, IoT 디바이스 측면에서 스스로 분석 판단하여 빠르게 대응 할 수 있는 기술이 대표적이라고 할 수 있다.

6.2.4 자율 해킹 방어

기계가 스스로 신규 보안취약점을 발견하고 공격대상이 스스로 변이하여 해킹에 대응하는 AI기반 능동적 자율방어 기술개발이 진행되고 있다. 취약점 검색 및 분석 기술이 네트워크 시스템 영역에서 웹・IoT 환경 특화된 취약점 스캔으로, 정적・동적 방식의 개별 테스트에서 정적+동적 방식의 결합 테스트로, 취약점 검색은 기존 IP・Port, 시스템 정보 스캔 기술에서 웹 어플리케이션 및 IoT 환경에 특화된 디바이스・통신 프로토콜・소프트웨어 등의 취약점 스캔으로 기술 트렌드가 변화하고 있다.

대표적인 기업은 IBM으로 AppScan, Accunetix WVS 등의 웹 애플리케이션에 특화시킨 취약점 스캔 기능을 제공하고 있고, SHODAN, Censys 등 IoT 환경에서 사용되고 있는 응용 및 암호 통신 프로토콜에 대한 스캐닝 기술에 대한 연구가 본격화 되고 있다.

IoT 디바이스의 경우에는 오픈소스의 사용 비중이 높기 때문에, 오픈소스 기반의 소프트웨어에 내포된 취약점을 스캔하기 위한 오픈소스 취약점 자동 분석 기술 연구가 활발하게 이루어지고 있다. 능동적 자율방어 기술로 대표적인 연구개발 주제인 사이버 자가변이 기술(Moving Target Defense, 이하 MTD)는 지능화 되고 있는 사이버 공격에 능동적으로 대응하기 위한 혁신적인 보안 전략 기술이다. MTD는 미국 백악관이 2011년에 발표한 사이버보안 연구개발 전략 중 가장 주목 받았던 연구 분야로서 2017년 현재 미국 국토안보부(Homeland Security)에서 연구를 수행하고 있다. 네트워크 환경에서 사이버 공격 대상의 주요 속성(IP Address, Port, Protocol, Platform, OS 등)을 이동시킴으로써 공격자의 공격 또는 분석(취약점 분석) 행위를 능동적으로 방어하기

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

위한 보안 기술이다.

6.3 디지털 안보 인프라

최근 정보보안 분야는 국가 안보 분야로서 국가적으로 중요하게 다루어지고 있어 국방·기반시설 보호를 위한 디지털 안보 인프라 구축이 시급한 실정이다. 국방부 전산망 해킹, 워너크라이 등 국가적 인프라에 대한 공격 경로의 복잡·다양화 및 고도화가 되고 있으며, 적대적 국가로부터 국방·기반시설의 사이버 위협이 심화되고 있는 상황이고, 사이버·물리 위협대응을 위해 심층방어 및 자가복원 기술과 사이버전 대응 및 스파이 행위 감시 기술 개발을 추진되고 있다.

6.3.1 사이버 킬체인

사이버 공격을 프로세스 상으로 분석, 사전에 단계별 위협요소를 제거, 영역별 다중 방어체계를 구축하여 공격자 의도와 활동을 분쇄 및 사이버피해의 자가복원(resilience)을 통하여 안전의 지속성을 확보하는 기술이 주목을 받고 있다.

6.3.2 사이버 물리체계 보안

주요 기반시설에 대한 통신채널 통제 기술과 사이버공격으로 인한 현실 공간의 피해 확산을 막는 사이버 킬스위치(Kill-Switch) 기술 개발이 진행되고 있다. 주요 기반시설의 침입차단 기술로 네트워크를 통한 산업제어시스템 침입을 차단할 수 있는 물리적 단방향 게이트웨이 및 제어기기 단위로 제어프로토콜 DPI 기반 침입을 차단할 수 있는 기술을 적용하여 산업제어시스템 네트워크와 중요 제어기기의 보안성을 강화하는 추세이다. 대표적인 기업으로는 워터폴의 USG (unidirectional security gateway), Owl Tech.의 PDS(perimeter defense solutions), CDS(cross domain solutions)와 같은 데이터 다이오드 기술이 산업제어시스템에 적용되고 있다. 토피노사의 인더스트리얼 시큐리티 솔루션등이 상용화되었으며, 다양한 ICS 제어프로토콜을 지원하는 제품이 개발 중이다.

산업제어시스템 엔드포인트 보안 기술로는 산업용 네트워크 경계구간 보안 연구개

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

발이 진행 중이지만, 산업용 단말을 대상으로 한 엔드포인트 보안기술은 기초 연구 수준이고, 산업용 네트워크 경계구간 보안기술은 적용이 추진되고 있으며, 산업용 네트워크 및 엔드포인트 보안기술에 대한 개발도 활발히 진행되고 있다. 대표적인 기업으로는 Bit9의 시큐리티 플랫폼, McAfee의 어플리케이션 컨트롤과 같은 엔드포인트 보안 제품도 출시되고 있다.

이외에도 공세적인 기술로 사이버 무기체계 개발과 정교한 사이버 적군 타격을 위한 사이버 안보 감시체계 구축 기술 등이 있다.

6.3.3 사이버 무기 체계

사이버전 발생 시 전장상황을 직관적으로 인지하고 효과적인 지휘통제가 가능한 사이버 전장상황 인지기술과 이에 따른 자동 공격 및 대응 수행용 사이버 무기 기술 확보가 절실한 상태이다.

6.3.4 사이버 안보 감시 체계

적대적 국가의 고도화된 정보수집 기술에 대응하기 위해 심층화된 스파이 활동 탐지 기술 및 이의 역추적이 가능한 전술적 포렌식 기술이 요구된다.

7. 정보보안 기술의 미래

양자 컴퓨터 출현, 생체정보 활용, AI기술 등 보안 패러다임 변화에 대응하기 위하여 새로운 보안패러다임을 선도하기 위한 미래 지향적 Beyond Security 원천 기술 개발이 진행되고 있다. 양자컴퓨팅 환경을 위한 암호원천 기술, 융합형 바이오 암호키 기술, 사이버·물리 융합 환경에서 범죄 예측 기술 등의 미래 지향적인 원천 기술 개발이 지속적으로 투자될 것이다.

7.1 차세대 암호

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

양자 컴퓨팅에서도 안전한 퀀텀 세이프(quantum-safe) 암호 및 암호키 관리의 원천적인 문제를 해결하기 위한 인공 신경망 기반 암호 체계 개발을 시작하는 시점이다. 퀀텀 세이프 암호기술은 양자컴퓨터 실현 가능성이 높아짐에 따라 PQC (post-quantum cryptography)에 대한 암호 프로젝트와 공모사업 등으로 본격적으로 연구개발에 착수하였으며 격자, 다변수방정식 및 코드기반 공개키 암호 등의 새로운 PQC 연구가 증가하는 추세이다.

미국 NSA는 2015년 8월 기밀 보호용으로 사용되는 암호 알고리즘을 양자컴퓨터 해독에도 안전한 것으로 변경할 계획이라고 공표하였으며 양자컴퓨터에 안전한 암호 표준이 준비되기 전까지 사용할 목적으로 CNSA(Commercial National Security Algorithm) Suite를 발표하였다. 유럽(EU)은 양자컴퓨터에 안전한 암호기술 연구사업인 SAFEcrypto와 PQcrypto 착수하였다. 퀀텀 세이프 암호 관련 산업계 동향으로, Microsoft는 SIDH SW 라이브러리를 발표 하였으며, 구글은 자사 개발판 브라우저에 격자를 기반으로 한 키교환 프로토콜인 'New Hope'를 탑재하여 시험을 시작하였다.

경량 암호기술은 ICT 디바이스의 소형화와 자원 제약적인 기기의 증가로 경량 암호기술의 필요성이 증대됨에 따라 관련 연구가 활발한 상태이다. 미국 NSA가 ISO・IEC 표준 PRESENT, HIGHT를 비롯한 기존 경량 블록암호 성능을 압도하는 블록암호 SIMON・SPECK을 발표하였고, 룩셈부르크 대학의 암호 연구팀인 CryptoLUX는 8비트 AVR, 16비트 MSP, 32비트 ARM 등 경량 SW 환경에서 암호 알고리즘의 성능을 평가하는 FELICS 프레임워크를 발표하였으며 성능 평가를 진행하였다.

키 은닉, 키 관리 기술은 데이터 보호를 위한 암호 구현의 효율성 경쟁에서 부채널 분석 등 구현상의 키누출 공격의 심화로 인하여 안전구현 및 키은닉 기술의 중요성이 확대되고 있다. 물리적 복제방지 기술인 PUF(Physically Unclonable Function)를 기반으로 안전한 키의 동적 생성 기술 연구가 진행 중이며, NXP에서는 Intrisic-ID의 PUF 기술을 자사 차세대 IC카드 솔루션에 탑재 개발 중이고, ICTK에서는 HW기반 키 은닉 원천 기술인 PUF기술에 대한 연구개발 진행 중이다.

7.2 디지털 DNA

디바이스 및 생체정보 유출을 방지하고 실시간으로 암호키 전 주기관리(생성・사용

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

· 은닉 · 폐기)가 가능한 바이오 암호키 및 디바이스 지문 기술이 활성화 될 것이다.

7.3 범죄 행위 예측

OSINT, HUMINT, IMINT,MASINT등 ICT 전반의 대규모 정보를 지능적으로 분석하여 사전에 사이버·물리환경의 반사회적 범죄 행위를 예측하는 기술이 미래 정보 분석기술로 주목을 받을 것이다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

III. 이론적 배경

1. 개인정보 보호를 위한 규제

한귀현(2005)은 한국의 경우 공공기관의 개인정보 보호에 관한 법률 등이 제정되어 있고 개인정보의 보호와 개인의 자기정보통제권 보장을 위한 각종 법제도적 장치들이 마련되어 있으나, 보호법제의 분산·체계 부조화·각종 개인정보처리시스템의 구축에 있어 법률적 근거의 결여·독립된 통합감독의 결여·권리구제체제의 미흡 등의 문제점이 있음을 지적하였다.

양재모(2010)는 개인정보보호에 대해 정부중심의 규제적 방법과 더불어 시장원리에 따른 업계의 자율규제 방식이 상호 조화를 이룰 필요가 있음을 주장하였다. 개인정보의 보호를 위해 개인정보의 범위를 개별적으로 유형화하고, 필요 이상의 수집행위에 대해 위험책임을 인정할 것을 강조하였다.

오일석(2015)은 개인정보 보호 의무를 위반했을 시 이에 따른 배상 가능한 손해의 범위를 한정할 것을 제안하였다. 특히 그는 개인정보 유출에 대한 한국의 법체계와 판례가 정신적 손해를 광범위하게 인정하고 있는 문제점이 있음을 지적하였다. 이러한 문제점으로 인해 정신적 손해에 대한 배상이 개인정보의 유출 책임이 있는 금융기관, 통신사, 유통업자 등의 개인정보 사용자에게 과도한 부담이 된다고 주장하였다. 또한, 그는 개인정보 보호의무 위반으로 개인정보가 유출된 정보주체는 장래 손해의 위험에 처해 있는바, 자신의 신용을 유지하는데 소요되는 비용을 신용관리비용이라 하는데, 신용관리 비용은 손해를 최소화하기 위하여 구체적으로 투입된 비용으로서 확정 가능하다는 점에서 배상되어야 할 손해로 인정되어야 함을 주장하였다.

2. 개인정보유출의 경제적·사회적 손실

김여라 등(2007)은 개인정보에 대한 가치를 추정하기 위해 가상가치접근법(contingent valuation methods)을 이용하였다. 개인정보 유출에 대한 피해를 예방하기 위한 비용 지불의사는 가구소득이 많을수록, 금융정보에 대한 피해경험이 있을수록, 월

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

통신요금 지불이 많을수록 높은 것으로 나타났다. 또한 개인이 인식하고 있는 정보유출에 대한 심각성은 금융정보의 유출에 대한 심각성이 가장 높으며, 개인고유정보, 통신정보, 영상정보, 바이오정보, 조직정보, 위치정보 순으로 나타났다.

채승완(2008)은 개인정보의 경제적 가치를 분석하고, 이를 이용하여 개인정보보호의 경제적 필요성을 분석하고자 하였다. 분석결과 개인 정보를 이용하는 시장에서의 수요 및 공급은 개인정보 보호수준에 영향을 받으며, 개인정보 보호수준의 강화는 개인정보 시장을 활성화한다고 주장한다. 그러나 개인정보보호체계의 정비로 인해 개인정보 보호수준이 향상된다고 하여도 개인정보 보호 사각지대가 존재하게 되면 개인정보의 이용에 더 많은 비용이 수반된다고 하였다.

이해춘, 안경애(2008)는 기업이 보유하고 있는 개인정보가 유출되어 발생시키는 경제적 손실을 계산하기 위해 우선 정보유출로 피해를 본 개인이 수용 가능한 손해 배상액을 가상가치측정방법을 이용하여 추정하였다. 그리고 이 추정된 값에 언론 매체에 발표되거나 정보보호진흥원에 접수된 개인정보 유출피해에 대한 피해 건수를 곱하여 경제적 손실의 규모를 측정하였다. 또한 기업의 마케팅생산성 향상을 위해 개인정보의 적극적인 활용은 필수적이나, 개인정보 유출로 인한 손실은 오히려 기업의 마케팅 생산성을 저하시킬 수 있을 것으로 보았다. 따라서 그들은 이러한 손실을 최소화하기 위해 개인정보 보호에 투자를 증대시켜야 함을 주장한다.

한창희 등(2011)은 개인정보유출 사고가 발생할 경우 민간기업의 실질적 손실비용과 이를 복구하기 위한 비용을 측정함과 더불어 고객의 손실과 사회적 파급효과 등의 경제적 피해규모를 정량적으로 산출할 수 있는 모형을 우리나라 상황에 맞게 수정하였다. 개인정보 유출에 따른 기업의 피해액은 대응 인건비·IR(investor relations)대응비용·수익손실·법적보상금·법적으로 실제 보상한 개인의 정보가치 등이며, 동시에 개인은 유출된 개인 정보가 갖는 가치만큼의 손해를 보게 되므로 기업이 개인에게 보상한 법적보상금은 유출된 개인정보가 가지는 가치의 일부분이기에 산정 시 중복을 피하고자 기업의 손실로 측정하며, 개인의 순손실은 유출된 개인 정보의 가치 중 기업이 보상한 법적보상금을 제외한 그 나머지를 산정하고, 산정한 기업손실과 개인손실은 관련 산업에 파급효과와 더해져 개인정보유출에 따른 전체 피해액으로 계산할 것을 제안하였다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

3. 개인정보유출과 주식가격

Ettredge & Richardson(2002)은 자본 시장 참여자들이 인터넷 기업들 중 전자 상거래 활동이 인터넷 기업 특유의 정보보안 위험을 점차적으로 증가시키는 것으로 보는지 여부를 조사하였다. IT 의존성으로 인해 발생하는 자체 평가 위험, 즉 인터넷 기술 변화로 인한 위험, 부적절한 인프라로 인한 위험, 온라인 보안 침해로 인한 위험 등 여러 가지 지표에 주목했다. 실증분석으로 2000년 2월에 유명한 인터넷 회사들에 시작된 분산서비스거부공격(DDoS)에 대한 투자자의 반응을 조사했다. 분석결과, 공격으로 인해 전자 상거래 관련 위험이 가장 높고 인터넷 회사의 큰 취약점이 드러났다. 특히 인터넷 기술 변화로 인한 위험, 부적절한 인프라로 인한 위험 및 온라인 보안 침해로 인한 위험 등 정보통신기술에 의존하여 발생하는 자체평가 위험이 있으며, 인터넷 기업의 주가하락은 이러한 위험 요소들과 관련이 있다고 하였다.

Acquisti et al.(2006)은 보안 메커니즘(해킹, 도난 또는 분실된 장비, 불량 데이터 처리 프로세스 등)의 실패로 인하여 개인정보 유출사례에 대한 광범위한 데이터를 수집하였다. 분석 결과, 개인정보 침해사건에 대한 발표 일에 기업의 시장 가치가 하락하는 통계적으로 유의한 영향이 있음을 보여주었다. CAR(누적 비정상 수익률)은 사건 발표 다음날에 규모가 커지며, 수명이 짧지만 통계적으로 유의미하며 음(-)으로 나왔다. 특히 대기업은 시간이 지남에 따라 구축된 신뢰 평판에 대한 개인정보보호 관행에 대한 부정적 보고서의 영향이 더 커진다고 주장하였다.

Ishiguro et al.(2006)은 정보유출사건에 대한 뉴스 보도의 경제적 파급효과가 일본 주식시장의 기업가치에 미치는 영향을 조사하였다. 분석결과, 정보유출사건에 대한 뉴스보도에 대한 반응이 미국시장에 비해 일본시장의 반응속도가 상대적으로 느린 것으로 나왔다. 일본시장은 뉴스보도가 있은 지 약 10일 만에 통계적으로 유의미한 반응을 보였고, 주가순자산비율(price book value ratio, 이하 PBR)은 사고요인이나 기업규모보다 기업의 시장가치에 더 많은 영향을 미치는 것으로 나타났다. 무형자산이 높게 평가되는 기업은 낮게 평가된 기업보다 보안사고가 기업가치에 더 심각한 영향을 받는다고 하였다.

유진호 등(2009)은 개인정보유출이 주가에 부정적인 영향을 미칠 수밖에 없는 근거를 제시하였다. 이들은 개인정보유출로 인한 기업의 직접적이고 정량적인 손실비용의 산출방안을 제시기 위해 개인정보 침해사고에 의해 발생할 수 있는 손실비용을 범주에

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

따라 분류하고 비용을 구성하는 요소들을 구체적으로 분석하였다. 분석결과, 개인정보 침해사고에 의해 기업이 입게 되는 경제적 손실비용은 잠재적인 손해배상금이 총 손실의 약 99% 정도로 대부분을 차지하는 것으로 나타났다. 따라서 잠재적인 위험을 고려하면 기업은 대용량 고객자료의 유출에 의해 파산에 이를 수 있다는 경각심을 가질 필요가 있다고 주장하였다.

개인정보유출이 주가에 미치는 영향에 관한 연구에서 방법론적으로는 개인정보유출 이외의 다른 이벤트가 주가에 미치는 영향을 제거하는 것이 중요한데, Patel(2010)의 연구가 그 시사점을 제공해 주고 있다. 예를 들어, M&A・유·무상증자・주식 병합 및 분할・특별이익 등 이벤트가 정보유출공시 한 달 이내로 발생한 경우 그 주식은 제외함으로써 정보유출 이외에 다른 요인이 주가에 미치는 효과를 사전에 제거하여야 한다. 그는 3일, 8일, 30일 기간별 CAR을 사용하여 분석하였고 또한, 통제기업(개인유출이 없는 기업들 중에서 무작위로 샘플링) CAR을 측정하여 비교하고 있다. 그리고 개별 기업 수준에서 CAR을 측정하여 개별기업의 차이점을 분석하고 있다. 분석결과, 3일 측정치는 유의한 영향력이 없고 8일은 음(-)의 영향을 주고 있다고 밝히고 있다. 그러나 8일의 경우 비 유출기업(통제기업)의 주가에도 부정적인 영향을 주고 있어서 정보유출이 산업 전반의 모든 기업의 주가에 부정적인 영향을 주고 있음을 밝혀냈다. 30일의 경우에는 주가에 대한 영향력이 다시 유의하지 않게 나타나고 있음을 주장하였다. 이 연구에서는 개인정보유출이 장단기(3일, 30일) 주가에 미치는 부정적인 영향은 유의하지 않은 것으로 나타났기 때문에 부정적인 영향을 미치는 다른 변수를 찾는 것이 필요하고, 향후 연구에서는 그 변수를 찾기 위해서 다양한 상황적 변수와 개별기업 변수를 고려하여 통계적으로 유의한 변수를 찾아내는 것이 필요할 것으로 보인다.

김정연(2013)은 개인정보가 유출된 기업의 초과수익률을 사건연구방법론으로 기존 연구결과와 비교하여 실제 개인정보유출사고로 인한 기업가치의 변화가 축소 혹은 확대 되었는지 살펴보았다. 분석결과 반복되는 개인 정보유출사례에도 시장의 반응은 부정적이었는데, 이는 기업가치에 부정적 영향을 미치고 있지만 자본시장에서의 개인정보 유출로 인한 피해인식은 크게 변화되지 않았음을 확인해 주었다.

김태환 등(2014)은 개인정보유출사고가 기업가치에 부정적인 영향을 끼친다는 기존 연구들을 토대로 개인정보유출사고 발생 직후에 나타나게 되는 주가의 변화를 7가지 패턴으로 분류하여 분석하였다. 분석결과, 개인정보유출사고 발생 직후 주가는 평균적으로 2일 동안 1.0% 하락하였다. 개인정보유출사고 발생 전의 주가로 회복하는데 드는 시간은 약 5일 정도이고 2주내에 주가를 회복하지 못하는 경우도 발생했다. 또한, 주가

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

를 회복한 이후에 다시 10% 이상 주가가 폭락한 경우도 있었는데 이는 사고의 시기나 중요도 등 내외적 요인에 의한 것으로 보았다.

홍일유 등(2015)은 정보보안 사고에 대한 공시가 시장에서 주식가치에 미치는 영향을 분석하였다. 이들은 보안사고가 일어난 후 +1일에 기업의 주가에 부정적 영향을 미친다는 것을 도출하였다. 또한, 정보보안 사고・개인정보유출・전산망 마비는 기업의 주가에 부정적 영향을 미쳐 투자자들뿐 아니라 기업의 이해관계자들에게 손해를 입히게 된다는 점을 밝혔다.

주미진 등(2016)은 2006년부터 2014년까지 9년 동안 한국 및 중국에서 발생한 개인정보유출사건(총 104개)이 해당 기업의 주가에 미치는 영향에 대한 사건연구를 실시하였다. 이들은 유출기업을 대상으로 한 사건일 전 170일부터 사건일 후 5일 동안의 주가자료를 이용하여 비정상수익률과 기간별 CAR을 측정하고 이의 통계적 유의성을 검증하였다. 분석결과, 한국의 경우 개인정보유출이 주가에 유의한 영향을 미치나, 중국의 경우 유의한 영향이 없음을 확인하였다. 이들은 한국과 중국의 상이한 연구결과에 대해 한국의 경우 개인정보보호에 관한 법률이 있어 정보유출에 따른 개인적 피해를 법률적으로 보호받을 수 있으나, 중국의 경우 이러한 개인정보보호에 대한 법률의 부재로 인해 개인정보유출에 따른 피해를 법률적으로 구제받을 수 없기 때문인 것으로 양국 간 상이한 결과가 나타남을 주장한다.

4. 개인정보유출과 정보보안기업의 주가반응

일반적으로 정보보안기업은 정보보안 관련된 사건이 일어나도 법적인 책임이 없기 때문에 주가에 큰 타격을 받지 않는 경우가 많았다. 오히려 새로운 소프트웨어 개발 때문에 기업가치 상승을 예상하고 투자자들이 더 많이 주식을 매입하는 경우도 발생할 수 있을 것이다. Cavusoglu et al(2004)은 정보보안 관련 사고는 주가 수익률에 부정적인 효과를 미치는 것을 밝혀냈다. 그리고 이러한 비정상적인 주가 변동은 해당 기업의 규모, 업종, 발생년도 등에 따라서 다르게 나타난다고 주장하였다.

권영옥, 김병도(2007)는 정보보안 사고에 따른 기업의 손실과 보안투자로 인한 수익을 기업 시장가치의 변화를 이용하여 정량적으로 측정하였다. 이들은 정보보호 또는 정보보안을 일반적으로 고의, 과실, 재해 등에 의해 정보시스템이 고장 및 파괴되는 등

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

의 위해를 막기 위한 물리적·논리적 대응으로 보고 고의적으로 발생하는 사고만을 대상으로 하였다. 이들의 사건 연구방법론을 통해 정보보안 사고는 해당 기업의 주가에 부정적인 영향을 미치지만, 보안 관련된 투자는 기업가치 상승에 별다른 영향을 주지 않는 것으로 나타났다. 또한, 국내 기업은 해외 기업에 비해서 정보보안 사고가 주가에 미치는 영향이 미비한 것으로 나타나 아직까지 기업의 보안 사고의 심각성이 인식되지 못하고 있는 점을 시사한다.

Telang & Wattal(2007)은 정보보안사건이 보안 소프트웨어 개발 업체들의 주가에 미치는 영향을 분석하였다. 분석결과, 정보의 유출 사건은 정보보안 개발 업체들의 주가에 부정적인 영향을 미치고 있는 것으로 나타났다. 이러한 현상은 시장 경쟁이 심할수록 개발 업체의 규모가 작을수록 더 커지는 것으로 나타났다. 또한, 정보유출사건의 유형에 따라서 손실 규모에 차이가 발생하며, 보안 프로그램 개발이 늦어질 경우 손실 규모가 더 증가함을 확인하였다.

김민정 등(2016)은 개인정보유출사고가 정보보호업체의 주가에 미치는 영향에 대해 실증분석하여 보안사고가 정보보호업체에 미치는 영향을 연구하였다. 이들은 정보보호 기업들을 IT서비스, 소프트웨어, 장비의 세 가지 업태로 구분하였다. 분석결과, 개인정보의 유출사건은 정보보안 업체의 주가에 긍정적인 영향을 미치는 것으로 나타났다. 또, 정보유출기업의 규모와 업종에는 유의한 차이가 없었지만 정보보호 업체의 업태 구분에 따른 차이는 발생하였다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

IV. 연구모형

1. 사건연구모형

사건연구는 인수 및 합병, 이익공시, 주식분할, 자사주매입, 신규 주식 및 채권의 발행과 같은 기업 고유의 개별사건에 대한 공시정보가 주식시장을 통해 비정상적인 증권가격 변화의 발생유무와 그 크기를 측정하는 효과적인 방법이다. 따라서 사건연구의 중심은 공시정보의 발생시점에서 비정상수익률(abnormal return, 이하 AR)을 측정하는 것이다. 보통 사건연구는 아래의 단계를 거쳐 진행된다.

첫째, 살펴보고자 하는 사건의 정의이다. 사건연구 시 처음 단계는 살펴보고자 하는 기업의 특정 사건을 결정하고 이에 따른 사건기간(event window)을 설정하는 것 이다. 대개의 경우 사건기간은 사건의 공시일과 사건이 공시된 다음 날을 포함한 양일을 많이 이용한다.

둘째, 표본선택에 따른 기준의 설정이다. 살피고자 하는 사건에 대한 설정이 완료되면 분석하고자 하는 표본의 선택 기준을 마련해야 한다. 더불어 이때 고려해야 할 중요한 것은 표본선택 과정에서 발생될 수 있는 잠재적 편의(bias)를 생각해야 한다.

셋째, 정상수익률 및 비정상수익률을 정의하고 주식의 수익률 자료를 이용하여 이를 추정한다. 사건연구에서 무엇보다 중요한 핵심은 AR을 측정하는 것이다. AR은 사건기간 동안에 발생한 사후적인 실제 수익률에서 만약 해당 사건이 발생하지 않았을 경우 주식시장에서 기대할 수 있는 수익률인 정상수익률(normal return)을 가감하여 도출한다. 정상성과모형은 크게 시장모형과 평균수익률모형으로 구분된다. 시장모형은 시장 수익률과 주식 수익률 간에 일정한 선형관계가 성립된다고 가정하며, 이는 자본자산가격결정모형을 기본 모형으로 간주한다. 반면, 평균수익률모형은 주식의 수익률이 시간의 경과와 관계없이 일정한 평균을 가지고 있음을 가정한다. 정상 수익률을 도출하는 모형(이하 정상성과모형)이 설정되면 추정기간(estimation window)의 관측치를 이용하여 모형의 모수를 추정하게 된다. 보통 추정기간은 사건이 발생된 시점의 이전으로 설정한다. 정상성과모형의 모수를 추정함에 있어 살피고자 하는 사건에 따른 영향을 배제시키기 위해 추정기간 내에 사건기간이 포함되지 않도록 추정기간을 설정한다. 대부분의 연구는 모수의 추정을 위해 사건일 전 250일을 추정기간으로 많이 사용

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

한다. 예를 들어, 사건기간을 21일(-20일～+20)일로 설정하면 분석기간은 추정기간인 사건일 전 240일부터 사건일 전 21일까지(-240일～-21일) 총 220일이 되며, 사건일 이전 기간인 20일과 사건일 일어난 이후 20일을 포함하여 총 261일이 된다.

넷째, 통계적 검정단계이다. 시장모형 또는 평균수익률모형을 이용하여 모수를 추정한다. 추정된 모수를 이용하여 AR을 도출하고 AR자료의 표준편차를 이용하여 평균비정상수익률(average abnormal return, 이하 AAR)의 통계적 유의성을 검정한다. 이 단계에서는 AAR이 양(+)의 부호를 가져야 하는지 음(-)의 부호를 가져야하는가에 대한 귀무가설을 설정해야 하며, 더불어 AR을 어떻게 합산(aggregating)할지에 대한 방법을 설정해야 한다.

다섯째, 실증분석 결과를 제시하고 이를 해석함과 더불어 결론을 도출한다. 모든 통계적 실증분석연구와 동일하게 분석 결과를 해석함에 있어 소표본의 경우 연구결과가 극단치(outliner)에 의해 심하게 왜곡될 수 있기 때문에 해석 시 주의해야 한다.

여섯째, 통계적 검정결과를 해석하고 이를 바탕으로 경제적 결론을 도출한다. AR의 검정결과를 바탕으로 가설의 채택 또는 기각 여부가 어떠한 경제적 함의를 가지는지에 대해 결론을 도출한다.

상기의 AR은 기업의 특정 사건이 사건기간 동안 해당 기업의 주식가격의 상승 또는 하락에 미치는 영향을 측정한 것이라 하겠다. 사건연구는 주식가격의 변화가 외생적으로 발생하는 특정 사건에 의해 변화한다고 본다. 따라서 AR에 대한 사건기간과 추정기간이 상호 중첩되지 않도록 설정되어야 한다. 예를 들어, AR도출을 위한 모수 추정기간에 사건기간이 포함되면 사건발생에 따른 주가변화가 정상수익률 및 비정상수익률 추정에 동시에 영향을 미치게 되고, 이는 결과적으로 잘못된 모수를 추정하게 함으로써 사건발생에 따른 주가변화의 영향을 제대로 측정하지 못하는 오류를 범하게 된다. AR의 추정을 위해선 연구하고자 하는 사건이 일어나지 않았을 때 예상할 수 있는 주식의 수익률을 추정할 정상성과모형(normal performance model)을 결정하여야 한다. 일반적으로 AR의 추정모형으로 경제적 모형(economic model) 및 통계적 모형(statistical model)이 있다.

Brown & Warner(1985)는 시장조정수익률모형, 평균조정수익률모형 및 OLS 시장모형을 이용하여 초과 수익률을 측정하는 통계적 모형을 제시하였다. 본 연구는 사건의 공시에 따른 주식 수익률 반응의 분석을 위해 일별 주식 수익률 자료를 이용함으로 Brown & Warner(1985)가 제시한 방법을 중심으로 논하고자 한다. 이들 연구의 핵심은 셋째 단계에서 제시된 AR 추정 시 이용되는 정상성과모형 중 과연 어느 모형의 검

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

정력(power)이 우수한가? 이며, 이는 시뮬레이션 방법을 통해 실시되었다. Brown & Warner(1985)는 “비정상 수익률은 ‘0’ 이다”라는 귀무가설이 진실임에도 불구하고 이를 기각하는 것을 제1종 오류라 하며, 귀무가설이 참이 아님에도 불구하고 이를 제대로 기각하지 못하는 것을 제2종 오류라 하였다. 여기서 제2종 오류의 확률을 검정력이라 하며, 이는 비정상 수익을 정확하게 추정할 수 있는 가능성을 의미한다. Brown & Warner(1980, 1985)는 간단한 시장모형에 기반한 것이 다른 복잡한 통계적 방법에 비해 다양한 조건 하에서 가장 검정력이 큰 것으로 분석되었다. 더불어, 월별 주식수익률 자료를 이용하기보다 일별 주식수익률 자료를 사용할 때 검정력이 훨씬 큰 것으로 나타났음을 확인하였다. 따라서 본 연구는 Brown & Warner(1980, 1985)와 같이 일별 자료를 이용하여 사건연구를 실시한다. 이들은 사건연구를 실시함에 있어 시장모형을 중심으로 AAR과 누적평균비정상수익률(cumulative average abnormal return, 이하 CAAR)의 측정과 이의 통계적 유의성 검정을 위한 검정통계량 측정방법을 제시하였다. 다음은 이들이 제시한 측정방법에 대한 설명이다. 시장모형을 이용한 AAR과 CAAR의 추정을 위해, 우선적으로 표본 개별주식의 일별 주식가격자료를 이용하여 아래 식 (1)과 같이 일별 주식수익률을 계산한다.

$$R_{i,t} = \frac{P_t - P_{t-1}}{P_{t-1}} \tag{1}$$

$R_{i,t}$: 주식 i의 t일 주식수익률

P_t : 주식 i의 t일 종가

P_{t-1} : 주식 i의 t-1일 종가

시장모형을 이용하여 기업별 AR을 추정하고 AAR을 산출한다. 그리고 이 AAR을 누적하여 CAAR을 도출한다(Brown & Warner 1980; 정형찬, 1997).

본 연구는 AR의 추정을 위해 사건 공시 전 170일부터 사건 공시 후 5일까지(공시일 포함) 총 176일 자료를 이용한다. 여기서 사건기간은 사건공시일과 사건공시일 전 5일 및 후 5일(-5일에서 +5일까지 총 11일)로 설정한다. 사건 일 전 170일에서 사건일 전 21일까지 총 150일을 시장모형의 추정기간으로 한다. 추정 시 식 (2)을 이용하여 사건일 전 170일에서 사건일 전 21일까지 기업별 일별 주식수익률과 시장포트폴리오 수익률 간의 회귀분석을 통해 절편($\hat{\alpha}_i$)과 기울기($\hat{\beta}_i$)을 추정한다. 그리고 추정된 절편과

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

기울기를 이용하여 기업별로 일별 AR을 도출한다.

$$AR_{i,t} = R_{i,t} - \hat{\alpha}_i - \hat{\beta}_i R_{mt} \tag{2}$$

여기서, $\hat{\alpha}_i, \hat{\beta}_i$: 표본기업(i)의 절편과 기울기
$R_{i,t}$: t일의 표본기업(i)의 주식수익률
R_{mt} : t일의 시장포트폴리오 수익률
$AR_{i,t}$: t일의 표본기업(i)의 비정상수익률

식 (2)의 $\hat{\alpha}_i$ 및 $\hat{\beta}_i$은 개별주식 및 종합주가지수의 일별수익률 자료를 회귀분석 하여 추정한다.[9] 상기 식 (2)의 과정을 통해 도출한 기업별 일별 비정상수익률의 합을 t일의 표본기업수로 나누어 AAR을 도출하며, AAR의 t 테스트 하기 위해선 -170일 부터의 aar이 필요하고 이는 식 (3)과 같다.

$$AAR_{i,t} = \frac{1}{N}\sum_{i=1}^{N} AR_{i,t} \tag{3}$$

여기서, t : -170에서 5의 값을 가지는 정수
N : 표본기업의 수
$AAR_{i,t}$: 평균비정상수익률

아래의 식 (4)를 통해 CAAR를 도출하며, 이는 AAR을 누적한 것이다.

$$CAAR_t = \sum_{t_1}^{t_2} AAR_{t_1,t_2} \tag{4}$$

여기서, $CAAR_t$: 누적평균비정상수익률

9) 종합주가지수의 일별수익률 측정은 사건 기업이 한국유가증권시장에 상장된 경우 KOSPI지수, 코스닥에 등록된 경우 KOSDAQ지수의 일별자료를 각각 사용한다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

아래의 식(5)와 식 (6)은 AAR과 CAAR에 대한 통계적 유의성 검정을 위한 t통계량을 계산하는 방법을 보여준다. 이는 횡단면 독립성을 가정한 Brown and Warner(1985)와 동일한 방법이다.

$$t_{AAR_t} = \sqrt{N_t} \cdot \sum_{i=1}^{N_t} \frac{AR}{\hat{S}(AAR)} \tag{5}$$

$$\hat{S}(AAR_{i,t}) = \sqrt{(\sum_{t=-170}^{-21}(AR_{i,t} - AR_i^*))/N_t - 1}$$

$$AR_i^* = \frac{1}{N_t}\sum_{t=-170}^{-21} AR_{i,t}$$

여기서, t_{AAR_t} : AAR에 대한 t통계량

$\hat{S}(\bullet)$: 해당 변수의 표준편차

$$t_{CAAR}(t_1,t_2) = \sum_{t=t_1}^{t_2} AR_t / \sqrt{\sum_{t=t_1}^{t_2} \widehat{S^2}(AAR_t)} \tag{6}$$

$$\widehat{S^2}(AAR_t) = \frac{1}{N_i - 1}\sum_{t=170}^{-21}(AR_t - AR^*)^2$$

$$AR^* = \frac{1}{N_t}\sum_{t=-170}^{-21} AR_t$$

여기서, $t_{CAAR}(t_1,t_2)$: t_1일 부터 t_2일까지의 누적평균비정상수익률에 대한 t통계량

2. 횡단면 회귀분석모형

개인정보유출의 공시에 따른 기업가치 변화의 결정요인을 살펴보기 위해 횡단면 회귀분석모형을 설정한다. 본 연구는 설정된 모형을 최소자승법으로 추정하며, 추정 시 사건일 및 사건일 이후 1일에 발생하는 개별 기업의 비정상수익률 및 누적비정상수익률을 종속변수로 한다. 개별 기업의 주가에 긍정적 영향을 미치는 정보는 대개 공시 전 사전

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

유출로 인해 사건 일 전에 비정상수익률이 양(+)의 유의한 결과를 보인다. 반면, 주가에 부정적 영향을 미치는 정보의 경우 기업이 외부로 유출되는 것을 극도로 차단함과 더불어 주식시장이 개장할 때 공시하기보다 시장이 마감할 무렵 또는 마감 이후 공시하는 경향이 있다. 이로 인해 비정상수익률이 지연반응을 보이기도 한다. 아마도 이는 부정적 정보에 대한 투자자의 과민반응에 따른 주식가격의 극심한 하락을 피하고자 하는 경영자의 심리에 기인한 것으로 생각된다.

개인정보유출은 유출 기업에게는 부정적 정보로 작용하기 때문에 본 연구는 아래의 식 (7) 및 (8)과 같이 횡단면 회귀분석모형을 설정한다. 식 (7)의 기업규모인 $LN(ASSET)$은 사건일 직전 연도 말 기업의 총자산에 자연로그를 취하여 계산한다. 이는 개인정보 유출에 따른 기업규모의 효과를 살펴보기 위한 것이다. 기업의 규모가 클수록 외부의 부정적 충격을 흡수할 수 있는 능력이 크기 때문에, 기업규모는 양(+)의 부호를 가질 것으로 생각된다(Acquisti et al., 2006). 성장기회인 ME/BE는 사건일 직전 연도 말 자기자본의 시장가치를 장부가치로 나누어 측정한다. 전략적 제휴, 개방형 혁신등과 같이 기업에 긍정적인 영향을 주는 사건의 경우, 많은 실증연구는 성장기회가 비정상수익률에 양(+)의 유의한 영향을 미침을 확인하였다(Szewczyk et al., 1996; Chan et al., 1997; Das et al., 1998; Kwon, 2006; Lee et al., 2012). 반면 개인정보 유출과 같이 부정적 정보는 성장기회가 큰 기업에게 더욱 큰 영향을 줄 것으로 생각된다. 따라서 성장기회 ME/BE는 음(-)의 부호를 가질 것이다. 기업유형 ($FIRM\ TYPE$)은 인터넷 기업이면 1, 아니면 0의 값을 갖는 더미변수이다. 인터넷 기반의 사업을 영위하는 기업일수록 보안이 더욱 중요한 것으로 생각된다. 따라서 이는 음(-)의 부호를 가질 것으로 기대된다.

$$AR_i = \alpha + \beta_1 LN(ASSET) + \beta_2 (ME/BE) + \beta_3 FIRM\ TYPE_i + \epsilon_i \tag{7}$$

여기서, $LN(ASSET)_i$: i기업의 직전년도 말 총자산액의 자연로그 값
$(ME/BE)_i$: i기업의 직전년도 말 자기자본의 시장가치를 장부 가치로 나눈 값
$FIRM\ TYPE_i$: 사건일 i기업이 인터넷 기업이면 1, 아니면 0

$$CAR_i = \alpha + \beta_1 LN(ASSET) + \beta_2 (ME/BE) + \beta_3 FIRM\ TYPE_i + \epsilon_i \tag{8}$$

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

정보전이로 인한 정보보안관련 기업의 비정상수익률 및 누적비정상수익률이 어떠한 요인에 의하여 영향을 받는지를 확인하기 위하여 아래의 식 (9) 및 식 (10)의 회귀분석모형을 설정한다. 기업규모가 작을수록 외부의 긍정적 영향에 따른 주식 가격의 변화가 클 것으로 생각된다. 따라서 기업규모 $LN(ASSET)$은 음(-)의 부호를 가질 것으로 생각된다. 많은 연구는 긍정적인 사건의 공시에 따른 비정상수익률이 기업규모와 음(-)의 관계임을 보여준다(Szewczyk et al., 1996; Chan et al., 1997; Acquisti et al., 2006; Lee et al., 2012). 성장기회 ME/BE가 클수록 주어진 기회에 보다 적극적으로 반응할 수 있을 것으로 생각할 수 있다. 그러나 본 연구에서 다루는 개인정보유출은 정보보안 기업에게 소위 반사적 이익에 가까운 것이다. 반사적 이익은 성장기회가 큰 기업보다는 이것이 적은 기업에게 보다 큰 영향을 미칠 것으로 생각된다. 따라서 성장기회 ME/BE는 음(-)의 부호를 가질 것이다. 더미변수 PHY(물리적 보안기업의 더미변수), NS(네트워크 및 시스템 보안기업의 더미변수), SOL(보안응용 소프트웨어 기업의 더미변수), CER(암호·인증 기업의 더미변수) 및 SI(시스템 통합 기업의 더미변수)는 정보보안기업을 그 성격에 따라 분류하기 위한 것이다. 이는 과연 어떠한 분야의 정보보안기업에 정보전이 효과가 크게 나타나는가를 확인하기 위한 것이다.

$$AR_i = \alpha + \beta_1 \ln(ASSET)_i + \beta_2 (ME/BE)_i + \beta_3 PHY_i + \beta_4 NS_i + \beta_5 SOL_i + \beta_6 CER_i + \beta_7 SI_i + \epsilon_i \quad (9)$$

여기서, PHY_i : i기업이 물리적 보안 기업이면 1, 아니면 0
NS_i : i기업이 네트워크 및 시스템 보안 기업이면 1, 아니면 0
SOL_i : i기업이 보안 응용 소프트웨어 기업이면 1, 아니면 0
CER_i : i기업이 암호·인증 기업이면 1, 아니면 0
SI_i : i기업이 시스템 통합 기업이면 1, 아니면 0

$$CAR_i = \alpha + \beta_1 \ln(ASSET)_i + \beta_2 (ME/BE)_i + \beta_3 PHY_i + \beta_4 NS_i + \beta_5 SOL_i + \beta_6 CER_i + \beta_7 SI_i + \epsilon_i \quad (10)$$

정보보안은 기밀성, 무결성, 가용성 등의 3요소로 구분할 수 있다. 그러나 이들 요

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

소는 서로 결합하여 사용되기 때문에 정보보안 기업의 분류 기준으로 적합하지 않다. 또한, 한국산업표준분류는 정보보호 관련 업종으로 컴퓨터 보안프로그램 개발업, 보안시스템 운영업 및 보안시스템 서비스업을 구분하고 있다. 이 분류 방식은 보안업종을 너무도 단순하게 다루고 있어, 이는 보안업종에 따른 차별적 주가반응을 분석하고자 하는 본 연구의 목적에 적합하지 않다. 정보보호산업 실태와 기술개발 동향은 정보보호산업을 산업현황에 따라 정보보안산업과 물리보안산업으로 분류하고 있다(데이코 산업연구소, 2013). 그리고 이 보고서는 정보보안산업을 네트워크 보안 제품, 시스템 보안 제품, 컨텐츠·정보유출방지보안 제품, 암호·인증 제품, 보안관리 제품, 보안컨설팅 서비스, 기타 제품 및 서비스로 세분화하고 있다. 이러한 이유로 인해 본 연구는 정보보안 기업을 물리적 보안 기업, 네트워크 및 시스템 보안 기업, 보안 응용 소프트웨어 기업, 암호·인증 기업, 보안 시스템 통합 기업으로 분류하였다.

물리적 보안 기업은 절도, 파괴, 화재 등과 같은 각종 물리적 위협으로부터 정보 시스템 자산을 보호하는 것이며, 대표적인 한국의 기업으로 에스원, 미래아이앤지 등을 들 수 있다. 네트워크 및 시스템 보안 기업은 비인가자가 인터넷 또는 네트워크로 접속 가능한 자원에 접근하려 할 때 관리자가 사용하는 컴퓨터 네트워크 및 하부구조를 보호하고, 시스템에 대한 접근 제어를 통한 보안 서비스를 전문으로 제공하는 회사로, 이의 대표적인 한국의 기업에는 넥스지, 안랩, 파수닷컴 등이 있다. 보안 응용 소프트웨어 기업은 컨텐츠 보호, 안티 바이러스 및 유해사이트 차단 등 특수한 목적의 정보보호를 제공하는 것을 말한다. 이에 포함되는 대표적인 한국의 기업에는 수산아이앤티, 이스트 소프트, SBI 핀테크 솔루션즈가 있다. 암호·인증 기업은 권한 증명을 위하여, 암호 및 생체 인식 기술 등을 이용하여 권한자를 식별하는 서비스를 제공하는 것을 말한다. 미래테크놀로지, 시큐브, 삼성SDS 등이 대표적인 한국의 기업이다. 보안 시스템 통합 기업은 보안 컨설팅 및 보안 시스템 통합 구축 용역을 제공하는 회사이며, 이에는 다우기술, 케이엘넷, 현대정보기술을 대표적인 한국의 기업으로 들 수 있다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

V. 실증분석

1. 연구자료

본 연구는 개인정보 유출에 따른 정보전이 효과를 살펴보기 위해 한국유가증권시장 및 코스닥시장에 상장된 기업을 대상으로 개인정보 유출 사건을 조사하였다. 조사기간은 2006년부터 2017년까지 총 12년이다. 개인정보 유출기업의 검색은 우선 네이버 및 구글 뉴스를 이용하였으며, 다음으로 정보보안 전문 인터넷뉴스에서 제공되는 보안뉴스의 기획기사 중 연간 중요 개인정보유출 사건 정보를 활용하였다. 그리고 행정자치부의 "개인정보보호법 위반 행정처분"에 포함된 기업을 네이버 및 구글 뉴스를 통해 추가 검색하였다. 마지막으로 한국인터넷진흥원의 개인정보유출 신고 접수현황 및 방송통신위원회 개인정보유출 관련 시정조치 고지를 받은 기업에 대하여 상기 검색엔진을 이용하여 보완하였다. 이를 통해 표본기간 동안 30개 기업에 대해 총 47건의 개인정보 유출 사고 표본을 확보하였다. 물론 이 기간 중 개인정보 유출 사건은 100건 이상이었으나, 유출 기업이 한국유가증권시장 및 코스닥시장에 상장되지 않아 표본에서 제외하였다. <표 15>는 최종적으로 선택된 연도별 개인정보 유출 사건 및 관련 기업 수를 보여준다. 개인정보 유출 사건은 2014년 23건 발생하였으며, 이는 전체의 48.9%에 해당한다. 특이한 사실 중 하나는 2007년의 경우 개인정보 유출이 3건 발생하였으며, 이는 국내 최대 이동통신사에서 모두 발생한 것이다. 개인정보 보호에 무엇보다도 신중을 기해야할 이동통신사에서 이와 같은 일이 발생했다는 것은 정보통신업의 강국임을 주장하는 한국에게는 더 없이 부끄러운 일이라 하겠다. 개인정보 유출 기업 수는 총 30개 기업이나, 연도별로 기업 수를 계산하다보니 <표 15>에서 보는 바와 같이 전체 기업 수가 40개 사로 기록되었다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

<표 15> 연도별 개인정보 유출 사건 및 관련 기업 수

(단위 : 건, 사)

구분	사건 수	기업 수
2006년	1	1
2007년	3	1
2008년	0	0
2009년	0	0
2010년	2	2
2011년	3	3
2012년	4	3
2013년	3	3
2014년	23	19
2015년	0	0
2016년	7	7
2017년	1	1
합계	47	40

정보보안 기업은 2000년대 들어와 정보통신기술의 발전으로 인한 새로운 업종의 기업이다. 이는 기존의 컴퓨터관련업에 속한 기업이 사업영역을 확장한 경우, 기존 사업영역에 정보통신기술을 융합하는 과정에서 새로 진입한 경우, 정보보안이라는 세분된 영역을 사업모델로 창업한 경우 등으로 인해 생성되었다. 이로 인해 한국의 표준산업분류 상에는 정보보안이 별도의 산업영역으로 분류되어 있지 못한 실정이다. 이러한 이유로 본 연구는 우선 금융감독원 전자공시시스템의 기업개황 데이터베이스를 이용하여 한국 표준산업분류 대분류 상 "출판, 영상, 방송, 우편통신, 컴퓨터 및 정보서비스업"을 영위하고 있는 상장기업 500여개를 확보하였다. 기업의 전자공시시스템 내 개황정보에서 제공하는 사업내용을 바탕으로 정보보안 기업으로 볼 수 있는 업체를 선별하였다. 선별 시 각 기업이 공시한 사업내용 및 제품을 홈페이지를 통해 모두 검토함과 더불어 2017년 국내 정보보호산업 및 실태조사에서 정보보안 기업으로 분류된 업체와 일치성 여부를 추가적으로 확인하였다.[10] 이러한 과정을 통해 본 연구는 최종적으로 65

10) 국내 정보보호산업 실태조사는 창조과학부와 한국정보보호산업협회가 공동으로 발행한 것으로 개별 기업의

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

개의 정보보안 표본기업을 확보하였다.[11] <표 16>은 본 연구에서 사용된 연도별 정보보안 기업 수이다. 정보보안 기업 수는 2006년 26개사에서 2017년 63개사로 매년 증가하는 추세이다. 시스템 통합 기업을 제외한 나머지 영역의 모든 부문에서 2006년에 비해 2017년 기준 약 3배의 증가를 보인다. 암호·인증 기업의 경우 2006년 0개사에서 2017년 4개사로 증가하였다. 이는 공인인증서 사용에 대한 법률적 규제로 인한 것으로 생각된다. 그러나 향후 생체인식 기술의 발전과 현재 의무적으로 사용되고 있는 공인인증서에 대한 규제가 완화될 경우, 암호·인증 기업의 미래가 지금과 같은 성장세를 보일 것이라 생각하기 어렵다. 기업의 수적 측면에서 판단할 때, 정보보안 기업 중 가장 미약한 성장세를 보이는 분야는 시스템 통합이다. 시스템 통합 기업은 2006년 기준 10개사에서 2016년 13개사로 증가하였다. 한국 내 대부분의 시스템 통합 기업은 자체적으로 개발한 플랫폼에다 외부에서 개발된 솔루션을 포함하여 수요 기업에 납품하는 형태를 취한다. 이러한 사업 방식이다 보니 기업의 주 수입원은 용역비가 주를 이룬다. 이 분야는 인건비를 어떻게 줄일 수 있는가와 얼마나 빠른 시간 내 용역을 완수할 수 있느냐가 핵심이다. 적은 인력을 이용한 고 수익 창출은 네트워크 및 시스템보안과 보안 응용 소프트웨어 기업과 같이 연구개발을 통한 자체 상품의 발굴을 필요로 한다. 향후 이 부분은 한국 내 시스템 통합 기업의 도전과제로 생각된다. 물리적 보안 기업 영역은 2006년 6개사에서 2017년 15개사로 약 2.5배의 성장 추세를 보인다. 4차 산업혁명의 도래는 많은 영역에 있어 무인화와 각종 사물이 단일 통신망 내에서 연결됨과 더불어 기기 간 통신을 통한 자동화를 불러올 것이다. 이러한 시대의 도래는 일상생활 및 각종 물건의 생산에 있어 편리함과 효율화를 가져올 것이다. 그러나 여기서 우려해야할 사실 중 하나는 해킹에 의한 보안사고의 발생이다. 예를 들어 공장에서 생산된 물건이 주인도 모르는 사이에 다른 곳으로 배송되어 불법적으로 거래될 수 있다. 또한 경쟁 사의 생산 시스템을 마비시켜 자사의 이익을 향상시킬 수 있다. 이외에도 다양한 방법으로 보안사고의 피해가 발생할 수 있다. 따라서 향후 많은 기업에서 자체적으로 보안인력을 확보하기 보다는 외부에 자사의 보안을 의뢰할 것으로 생각된다. 이는

자료, 인터뷰 등의 방식으로 정보를 취합·분석하였기에 국내 정보보안 기업 현황을 광범위하게 포함하고 있다.

11) KISVALUE는 한국표준산업분류에 따른 KISC산업분류와 GICS의 분류에 따른 KIS-IC산업분류 두 가지를 제공한다. 정보보안산업은 기존의 산업형태에 ICT기술이 융합되면서 다양한 형태의 제품과 서비스가 제공되며, 지금 현재도 새로운 사업영역과 제품이 창조되고 있다. 이로 인해 정보보안 기업 목록 작성 시 KIS-IC에 분류된 세분류를 기준으로 판단하기보다 한국표준산업분류 대분류 기준으로 기업목록을 작성하고, 여기서 비 정보보안 기업을 삭제하는 것이 표본기업의 누락을 방지 할 수 있는 보다 효과적인 방법으로 생각하였다. 이에 본 연구는 본문에 기술한 조사방법을 사용하여 정보보안 기업을 선별하였다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

물리적 보안 영역에 대해 현재보다 더욱 많은 수요를 창출할 것이다.

<표 16> 연도별 정보보안 기업 현황

(단위 : 사)

구분	정보보안 기업 수					
	물리적 보안 기업	네트워크 및 시스템 보안 기업	보안 응용 소프트웨어 기업	암호·인증 기업	시스템 통합 기업	합계
2006년	6	8	2	0	10	26
2007년	8	9	2	0	11	30
2008년	8	9	2	0	11	30
2009년	8	9	2	0	11	30
2010년	9	12	3	0	12	36
2011년	9	13	4	1	12	36
2012년	12	15	4	1	12	44
2013년	11	15	5	1	12	44
2014년	12	17	7	2	12	50
2015년	12	17	7	2	12	50
2016년	15	20	9	4	13	61
2017년	15	22	9	4	13	63

2. 실증분석 결과

2.1. 개인정보 유출 기업에 대한 실증분석 결과

<표 17>은 개인정보 유출 기업에 대한 사건 전 -5일에서 사건 후 5일 간의 AAR 및 CAAR을 보여준다.[12] 개인정보 유출 기업에 대한 사건공시는 사건일(0일)에 0.6%

12) 본 연구는 전체 검정기간(test periods)에 포함되는 -20일부터 -4일까지의 기간에 대해서는 유의미한 공시정보의 사전 유출효과를 확인할 수 없었다. 이에 본 연구는 분석의 편의와 지면상의 고려로 -5일에서 사건 당일 후 5일 동안(총11일)의 AAR과 CAAR를 집중적으로 분석, 보고함을 밝힌다. 전체 검정기간의 분석결과의 요구가 있을 시, 본 저자는 즉시 보고할 수 있음을 밝힌다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

의 음(-)의 비정상수익률을 보이며, 이는 5% 유의수준에서 유의하였다. 즉, 개인정보 유출이 기업의 주가에 부정적인 영향을 미침을 알 수 있었다. 비록 5% 수준에서 유의하지 않으나 사건일 이후 첫날(1일)의 주식가격이 음(-)의 AAR값을 보이고 있다. 이는 개인정보 유출의 부정적 정보에 대한 시장의 지연반응으로 생각할 수 있다. 또는 일부 사건의 공시가 주식시장 마감에 근접하여 또는 이후에 이루어짐으로써 사건 일에 정보가 주식가격에 반영되지 못하고 사건일 다음 일(1일)에 반영된 결과로 볼 수 있다. 부정적 정보를 가급적 감추고자하는 인간의 심리를 고려할 때, 사건일 다음 날 음(-)의 주가반응은 아마도 후자의 경우로 생각된다. 사건일 다음 날 CAAR의 t값이 통계적으로 유의한 수준에 매우 근접하고 있다. 다소 특이한 사실은 사건공시 이후 2일차에 5% 수준에서 유의한 양(+)의 AAR이며, 이로 인해 개인정보 유출에 대한 부정적 주가반응이 모두 사라지고 있음을 알 수 있다. 표본수가 47개로 다소 충분하지 않은 측면이 있어 결과에 대해 쉽게 단정하기 어렵다. [그림 4]은 -5일부터 +5일까지의 AAR 및 CAAR을 도식화한 것이다. 사건일과 사건일 다음날에 주식가격이 떨어짐을 알 수 있다.

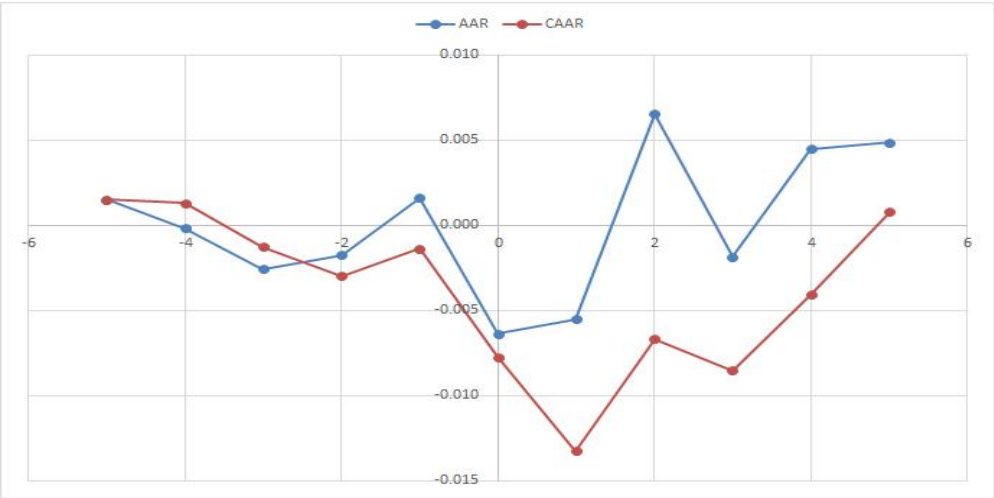
<표 17> 개인정보 유출 기업에 대한 AAR 및 CAAR

사건일	AAR	AAR의 t값	CAAR	CAAR의 t값
-5	0.001	0.519	0.001	0.519
-4	0.000	-0.061	0.001	0.324
-3	-0.003	-0.894	-0.001	-0.252
-2	-0.002	-0.603	-0.003	-0.520
-1	0.002	0.565	-0.001	-0.212
0	-0.006*	-2.215	-0.008	-1.098
1	-0.006	-1.920	-0.013	-1.742
2	0.007*	2.283	-0.007	-0.822
3	-0.002	-0.645	-0.009	-0.991
4	0.004	1.557	-0.004	-0.447
5	0.005	1.693	0.001	0.084

주 1) **, *는 각각 1%, 5% 수준에서 유의함.
2) 관측수(n)는 47개임.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY



[그림 4] 개인정보 유출 기업의 AAR 및 CAAR

<표 18>는 개인정보 유출 기업에 대한 기간별 CAAR을 보여준다. 사건일과 사건일 다음날의 CAAR은 -0.012로 1% 수준에서 유의하다. 결과적으로 개인정보 유출 시 기업의 주가가 약 1.2% 내려감을 알 수 있다. 사건일 이전 1일과 이후 1일의 AAR을 누적한 CAAR은 -0.010으로 5% 수준에서 유의하였다. 0일에서 1일에 대한 CAAR이 -1일에서 1일에 대한 CAAR보다 더욱 유의하다.

<표 18> 개인정보 유출 기업에 대한 기간별 CAAR

기간	CAAR	CAAR의 t값	기간	CAAR	CAAR의 t값
-1일 ~ 0일	-0.005	-1.167	-3일 ~ 3일	-0.010	-1.296
-1일 ~ 1일	-0.010*	-2.061	-5일 ~ 5일	0.001	0.084
-1일 ~ 2일	-0.004	-0.643	0일 ~ 1일	-0.012**	-2.924
-2일 ~ 2일	-0.005	-0.845			

주 1) **, *는 각각 1%, 5% 수준에서 유의함.
2) 관측수(n)는 47개임.

<표 19>는 개인정보 유출 기업에 대한 횡단면 회귀분석 결과이다. 모형 1-a는 AAR의 값이 통계적으로 유의한 사건일의 AR값을 종속변수로, 모형 1-b는 AAR의 값이 유의수준에 매우 근접하는 사건일 이후 1일의 AR값을 종속변수로 설정한 것이다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

모형 2는 기간별 CAAR값이 가장 유의하게 나오는 0일에서 1일까지의 값을 이용하였다. 모형 1 및 2의 기업규모변수 $LN(ASSET)$은 5% 수준에서 유의하지 않았다. 기업규모가 비정상수익률 및 누적비정상수익률에 영향을 미치지 않았다. 성장기회의 대용변수 ME/BE는 모형 1-b의 경우 5% 수준에서 유의하다. 이는 성장기회가 클수록 더 많은 음의 AR이 발생함을 의미한다. 기업유형의 더미변수 $FIRMTYPE$은 5% 수준에서 유의하지 않았다. 조정된 R^2값은 0.1 이하이며, 모형의 적합도를 나타내는 F값은 5% 수준에서 유의하지 않았다.

<표 19> 개인정보 유출 기업에 대한 회귀분석 결과

모형 1 : $AR_i = \alpha + \beta_1 LN(ASSET) + \beta_2(ME/BE) + \beta_3 FIRMTYPE_i + \epsilon_i$

모형 2 : $CAR_i = \alpha + \beta_1 LN(ASSET) + \beta_2(ME/BE) + \beta_3 FIRMTYPE_i + \epsilon_i$

변수	모형 1-a (AR_0)	모형 1-b (AR_1)	모형 2 ($CAR_{0\sim1}$)
상수	-0.025 (-0.735)	-0.027 (-0.836)	-0.053 (-1.005)
$LN(ASSET)$	0.001 (0.581)	0.001 (0.817)	0.002 (0.893)
ME/BE	-0.000 (-0.308)	-0.003* (-2.286)	-0.003 (-1.632)
$FIRMTYPE$	-0.001 (-0.149)	-0.001 (-0.173)	-0.002 (-0.206)
$Adjusted\text{-}R^2$	-0.055	0.092	0.036
$F\text{-}value$	0.195	2.547	1.569
관측수(n)	47		

주) **, *는 각각 1%, 5% 수준에서 유의함. ()안은 t값임.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

2.2 전이효과에 따른 정보보안 기업의 실증분석 결과

<표 20>은 개인정보 유출 기업의 사건공시가 정보보안 기업의 주가에 미치는 영향을 보여준다. <표 20> 내 수치는 정보보안 기업의 사건공시 일 전 -5일에서 사건공시 일 이후 5일 간의 AAR 및 이의 t값과 CAAR 및 CAAR의 t값이다.[13] 정보 유출 기업에 대한 사건공시는 전체 정보보안 기업의 주가에 사건일(0일)에 -0.001, 0.000의 유의하지 않은 AAR 및 CAAR을 보인다. 사건일 이후 1일차 역시 AAR 및 CAAR은 0.001 및 0.001의 5% 수준에서 유의하지 못하다. 이에 본 연구는 정보보안 기업을 물리적 보안, 네트워크 및 시스템 보안, 보안 응용 소프트웨어, 암호·인증, 시스템 통합으로 분류하여 AAR 및 CAAR을 살펴보았으며, 그 결과는 역시 <표 20> 내에 제시되어 있다. 사건일 다음 날인 1일에 네트워크 및 시스템 보안 기업의 AAR은 0.005로 5% 수준에서 유의한 양(+)의 값을 보였다. 반면, 물리적 보안, 보안 응용 소프트웨어, 암호·인증 및 시스템 통합 기업의 AAR 및 CAAR은 어떠한 날에서도 유의한 결과를 보이지 않았다. 이는 개인정보 유출에 따른 정보전이 효과는 정보보안 기업 중 네트워크 및 시스템 보안 기업에서 발생한다는 것을 보여준다. [그림 5]은 정보보안 기업에 대한 -5일부터 +5일까지의 AAR 및 CAAR을 도식화한 것이다. 네트워크 및 시스템 보안 기업의 AAR이 사건일 다음 날 올라감을 알 수 있다.

<표 21>은 정보보안 기업에 대한 기간별 CAAR을 보여준다. 사건일과 사건일 다음 날 전체 정보보안 기업의 CAAR은 0.004로 5% 수준에서 유의하다. 결과적으로 이는 개인정보 유출 시 정보보안 기업으로의 정보전이 효과가 존재함을 거듭 보여주는 것이라 하겠다. 네트워크 및 시스템 보안 기업의 CAAR이 0.004로 다소 유의하지 못했다. 이는 개인정보 유출의 사건공시 일에 네트워크 및 시스템 보안 기업의 AAR이 양(+)의 유의한 값을 보이지 못한 것에 기인한 것이다. 결과적으로 이는 정보전이에 시간이 소요됨을 보여주는 것이다. 다시 말해 어떤 사건에 대한 정보가 주식시장으로 전달될 때 1차적으로 이 정보와 직접적으로 관계된 주식의 가격이 변화하며, 시간적 간격을 두고 2차적으로 정보보완 기업의 주식 가격에 반응이 일어나게 된다.

<표 22>은 정보보안 기업에 대한 횡단면 회귀분석 결과이다. 모형 3-a는 사건일의

13) 정보전이 효과를 살펴보기 위한 정보보안 기업의 공시효과 분석에 대해서, 본 연구는 -20일부터 -4일까지의 기간 동안에 역시 유의미한 공시정보의 사전 유출효과를 확인할 수 없었다. 이에 앞 절(2.1)의 정보유출 해당기업의 공시효과 분석과 같은 맥락에서, 본 연구는 분석의 편의와 지면상의 고려로 -5일에서 사건 당일 후 5일 동안(총11일)의 AAR과 CAAR를 집중적으로 분석, 보고함을 밝힌다. 전체 검정기간의 분석결과의 요구가 있을 시, 본 저자는 즉시 보고할 수 있음을 밝힌다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

AR값을 종속변수로, 모형 3-b는 네트워크 및 시스템보안 기업의 AAR 값이 통계적으로 유의한 사건일 이후 1일의 AR값을 종속변수로 설정한 것이다. 모형 4는 모형 2와 같이 기간별 CAAR값이 가장 유의하게 나오는 0일에서 1일까지의 값을 이용하였다.

모형 3 및 4의 기업규모변수 $LN(ASSET)$은 5% 수준에서 유의하지 않았다. 정보유출 기업에 대한 횡단면 회귀분석결과와 같이 기업규모가 비정상수익률 및 누적비정상수익률에 영향을 미치지 않았다. 성장기회의 대용변수 ME/BE는 모든 모형에 있어 5% 수준에서 유의한 음(-)의 값을 보였다. 이는 성장기회가 클수록 더 많은 음의 AR이 발생함을 의미한다. 기업유형의 더미변수 PHY(물리적 보안 기업의 더미변수), NS(네트워크 및 시스템 보안 기업의 더미변수), SOL(보안 응용 소프트웨어 기업의 더미변수), CER(암호·인증 기업의 더미변수) 및 SI(시스템 통합 기업의 더미변수) 중 NS가 모형 3-b에서 5% 수준에서 유의한 양(+)의 값을 보였으며, 나머지 더미변수는 모두 유의하지 않았다. 모형 4의 NS는 비록 5% 수준에서 유의하지 않지만, 5% 수준에서 유의한 양(+)의 t값에 근접하고 있다. 이는 상기에서 언급한 정보전이 효과의 속도에 기인한 것으로 생각된다. 조정된 R^2값은 최소 0.02에서 최대 0.014의 범위에 있다. 모형 3-a를 제외한 모든 모형의 F값은 1% 수준에서, 모형 3-a의 첫째 열 F값은 5% 수준에서 각각 유의하다.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

<표 20> 정보보안 기업에 대한 AAR 및 CAAR

사건일	AAR	AAR의 t값	CAAR	CAAR의 t값
a. 전체(n=1,535)				
-5	-0.001	-0.609	-0.001	-0.609
-4	0.001	0.583	0.000	-0.018
-3	0.001	0.529	0.001	0.291
-2	0.000	0.222	0.001	0.363
-1	-0.000	-0.129	0.001	0.267
0	-0.001	-0.470	0.000	0.052
1	0.001	0.743	0.001	0.329
2	0.001	0.391	0.002	0.446
3	0.001	0.696	0.003	0.652
4	0.000	0.000	0.003	0.619
5	0.001	0.735	0.004	0.812
b. 물리적 보안(n=384)				
-5	-0.001	-0.479	-0.001	-0.479
-4	0.001	0.435	0.000	-0.031
-3	-0.001	-0.414	-0.001	-0.264
-2	0.001	0.540	0.000	0.041
-1	0.001	0.460	0.001	0.242
0	0.000	0.153	0.001	0.284
1	-0.001	-0.347	0.001	0.131
2	0.002	0.930	0.002	0.452
3	0.003	1.382	0.005	0.887
4	-0.001	-0.390	0.004	0.718
5	0.003	1.401	0.007	1.107
c. 네트워크 및 시스템 보안(n=518)				
-5	-0.001	-0.324	-0.001	-0.324
-4	0.000	0.144	0.000	-0.127
-3	0.004	1.797	0.004	0.934
-2	0.000	0.115	0.004	0.866
-1	0.000	0.123	0.004	0.829
0	-0.001	-0.222	0.004	0.667
1	0.005*	2.022	0.008	1.381
2	-0.002	-0.792	0.007	1.012
3	-0.001	-0.523	0.005	0.780
4	0.001	0.311	0.006	0.838
5	0.002	0.665	0.008	1.000

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

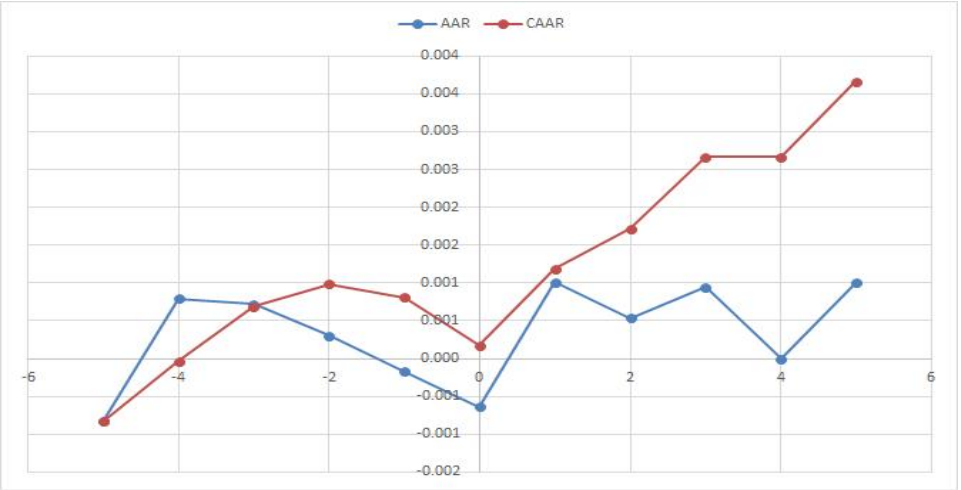
표 계속

사건일	AAR	AAR의 t값	CAAR	CAAR의 t값
d. 보안 응용 소프트웨어(n=173)				
-5	-0.001	-0.268	-0.001	-0.268
-4	-0.001	-0.246	-0.001	-0.363
-3	0.001	0.454	0.000	-0.034
-2	-0.003	-1.671	-0.004	-0.865
-1	0.001	0.686	-0.002	-0.467
0	-0.001	-0.429	-0.003	-0.601
1	0.002	1.154	-0.001	-0.121
2	0.002	1.008	0.001	0.243
3	0.000	-0.212	0.001	0.159
4	0.000	-0.170	0.001	0.097
5	0.002	1.058	0.003	0.412
e. 암호·인증(n=45)				
-5	0.001	0.159	0.001	0.159
-4	0.003	0.514	0.003	0.476
-3	0.002	0.336	0.005	0.583
-2	0.008	1.667	0.013	1.338
-1	0.001	0.166	0.014	1.271
0	-0.002	-0.339	0.012	1.022
1	-0.009	-1.823	0.003	0.257
2	0.007	1.461	0.011	0.757
3	0.009	1.839	0.020	1.327
4	0.007	1.421	0.027	1.708
5	0.000	0.044	0.027	1.642
f. 시스템 통합(n=416)				
-5	-0.001	-0.604	-0.001	-0.604
-4	0.002	0.903	0.001	0.211
-3	-0.002	-1.256	-0.002	-0.553
-2	0.000	0.213	-0.001	-0.372
-1	-0.003	-1.345	-0.004	-0.934
0	-0.001	-0.775	-0.005	-1.169
1	-0.001	-0.803	-0.007	-1.386
2	0.001	0.501	-0.006	-1.119
3	0.002	0.939	-0.004	-0.742
4	-0.001	-0.430	-0.005	-0.840
5	-0.002	-0.891	-0.007	-1.069

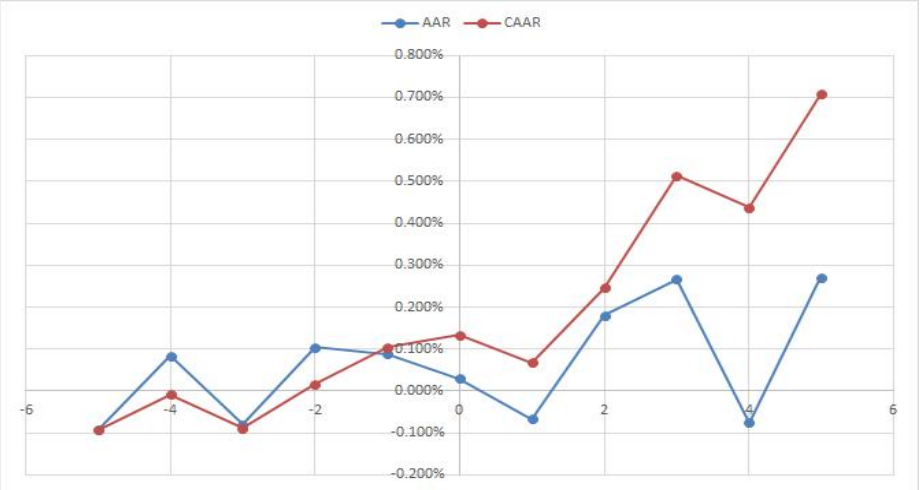
주 1) **, **는 각각 1%, 5% 수준에서 유의함.
2) n은 표본의 관측수임.

Collection @ chosun

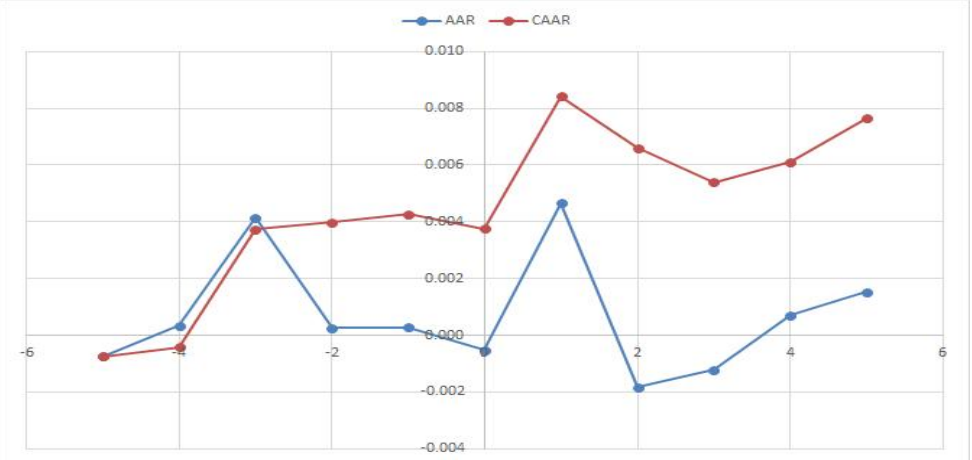
조선대학교
CHOSUN UNIVERSITY



a. 전체



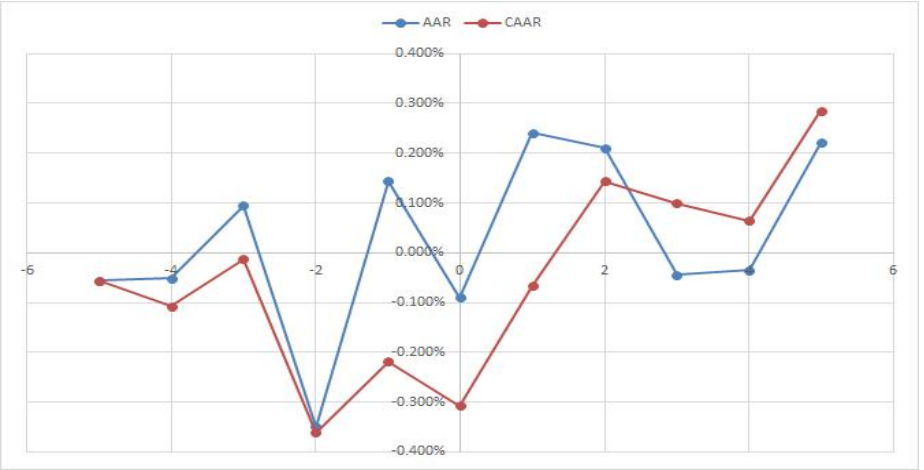
b. 물리적 보안



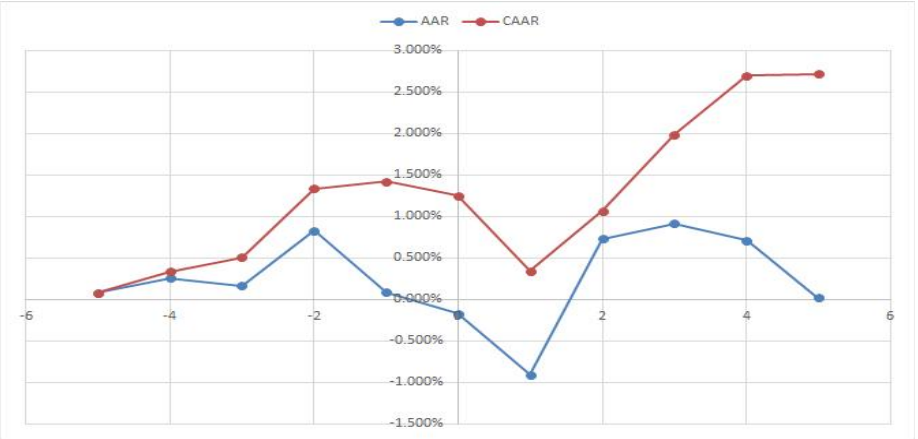
c. 네트워크 및 시스템 보안 기업

Collection @ chosun

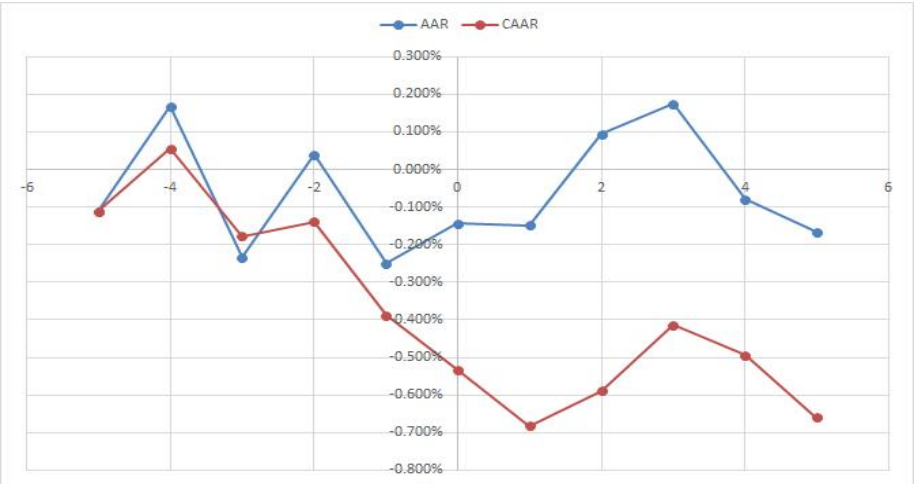
조선대학교
CHOSUN UNIVERSITY



d. 보안 응용 소프트웨어



e. 암호·인증



f. 시스템 통합

[그림 5] 정보보안 기업의 AAR 및 CAAR

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

<표 21> 정보보안 기업에 대한 기간별 CAAR

기간	CAAR	CAAR의 t값	기간	CAAR	CAAR의 t값
a. 전체(n=1,535)					
-1일 ~ 0일	-0.001	-0.424	-3일 ~ 3일	0.003	0.749
-1일 ~ 1일	0.000	0.083	-5일 ~ 5일	0.004	0.812
-1일 ~ 2일	0.001	0.268	0일 ~ 1일	0.0004*	0.196
-2일 ~ 2일	0.001	0.339			
b. 물리적 보안(n=384)					
-1일 ~ 0일	0.001	0.433	-3일 ~ 3일	0.005	1.022
-1일 ~ 1일	0.001	0.153	-5일 ~ 5일	0.007	1.107
-1일 ~ 2일	0.002	0.598	0일 ~ 1일	0.000	-0.138
-2일 ~ 2일	0.003	0.776			
c. 네트워크 및 시스템 보안(n=518)					
-1일 ~ 0일	0.000	-0.070	-3일 ~ 3일	0.006	0.952
-1일 ~ 1일	0.004	1.110	-5일 ~ 5일	0.008	1.000
-1일 ~ 2일	0.003	0.565	0일 ~ 1일	0.004	1.272
-2일 ~ 2일	0.003	0.557			
d. 보안 응용 소프트웨어(n=173)					
-1일 ~ 0일	0.001	0.182	-3일 ~ 3일	0.002	0.374
-1일 ~ 1일	0.003	0.815	-5일 ~ 5일	0.003	0.412
-1일 ~ 2일	0.005	1.209	0일 ~ 1일	0.002	0.512
-2일 ~ 2일	0.002	0.334			
e. 암호·인증(n=45)					
-1일 ~ 0일	-0.001	-0.122	-3일 ~ 3일	0.016	1.250
-1일 ~ 1일	-0.010	-1.152	-5일 ~ 5일	0.027	1.642
-1일 ~ 2일	-0.003	-0.267	0일 ~ 1일	-0.011	-1.529
-2일 ~ 2일	0.006	0.506			
f. 시스템 통합(n=416)					
-1일 ~ 0일	-0.004	-1.499	-3일 ~ 3일	-0.005	-0.954
-1일 ~ 1일	-0.005	-1.688	-5일 ~ 5일	-0.007	-1.069
-1일 ~ 2일	-0.005	-1.211	0일 ~ 1일	-0.003	-1.116
-2일 ~ 2일	-0.004	-0.988			

주 1) **, *는 각각 1%, 5% 수준에서 유의함.

2) n은 표본의 관측수임.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

<표 22> 정보보안 기업에 대한 회귀분석 결과

모형 3 : $AR_i = \alpha + \beta_1 \ln(ASSET)_i + \beta_2 (ME/BE)_i + \beta_3 PHY_i + \beta_4 NS_i + \beta_5 SOL_i + \beta_6 CER_i + \beta_7 SI_i + \epsilon_i$

모형 4 : $CAR_i = \alpha + \beta_1 \ln(ASSET)_i + \beta_2 (ME/BE)_i + \beta_3 PHY_i + \beta_4 NS_i + \beta_5 SOL_i + \beta_6 CER_i + \beta_7 SI_i + \epsilon_i$

변수	모형3-a (AR_0)		모형3-b (AR_1)		모형 4 ($CAR_{0\sim1}$)	
상수	-0.005 (0.219)	0.003 (0.127)	0.007 (0.296)	-0.008 (-0.329)	0.012 (0.380)	-0.005 (-0.158)
$LN(ASSET)$	-0.000 (-0.115)	0.000 (0.012)	-0.000 (-0.0049)	0.000 (13.278)	-0.000 (-0.119)	0.000 (0.349)
ME/BE	-0.002** (2.753)	-0.002** (-2.765)	-0.002** (-3.501)	-0.002** (-3.345)	-0.004** (-4.604)	-0.004** (-4.496)
PHY	0.001 (0.492)		-0.003 (-1.298)		-0.002 (-0.062)	
NS		-0.000 (-0.212)		0.006* (2.518)		0.006 (1.747)
SOL		-0.001 (-0.394)		0.003 (0.952)		0.002 (0.436)
CER		0.000 (0.008)		-0.005 (-0.945)		-0.005 (-0.707)
SI		-0.001 (-0.627)		0.000 (-0.161)		-0.002 (-0.569)
$Adjusted\text{-}R^2$	0.003	0.002	0.007	0.012	0.012	0.014
$F\text{-}value$	2.705*	1.389	4.518**	3.969**	7.176**	4.746**
관측수(n)	1,530					

주) **, *는 각각 1%, 5% 수준에서 유의함. ()안은 t값임.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

VI. 결론 및 연구의 한계점

인터넷을 통한 각종 거래가 활성화되면서 기업에 의해 수집된 개인정보가 무단으로 거래되거나 부주의하게 제3자에게 유출되는 각종 사고 및 이에 따른 다양한 문제가 발생하고 있다. 이에 본 연구는 한국의 기업을 대상으로 기업의 개인정보 유출의 공시가 해당 기업 및 정보보안 기업의 주가에 어떠한 영향을 미치는 지를 살펴보았다. 정보보안 기업의 주가반응을 살펴보는 것은 개인정보 유출에 따른 정보전이 효과를 검증하는 것이며, 이를 위해 본 연구는 한국유가증권시장 및 코스닥시장에 상장된 기업을 대상으로 개인정보 유출 사건을 조사하였다. 조사기간은 2006년부터 2017년까지 총 12년이며, 표본기간 동안 총 47건(30개사)의 개인정보 유출 사고 및 65개의 정보보안 표본기업을 확보하였다. 이렇게 확보한 표본을 이용하여 사건연구를 진행하였으며, 이의 주요 실증분석 결과는 다음과 같다.

첫째, 사건일 개인정보 유출 기업의 AAR은 5% 수준에서 유의한 음(-)의 값을 보였다. 비록 5% 수준에서 유의하지 않으나 사건일 이후 1일차 주식가격이 음(-)의 AAR값을 보였으며, CAAR의 값 또한 통계적으로 유의한 수준에 매우 근접하였다. 사건일과 사건일 다음날의 CAAR은 1% 수준에서 유의한 음(-)의 값을 보였다. 개인정보 유출 시 기업의 주가가 약 1.2% 감소하였다. 또한, 사건일 이전 1일과 이후 1일의 AAR을 누적한 CAAR은 5% 수준에서 유의한 음(-)의 값을 보였다. 결과적으로 개인정보 유출이 기업가치를 감소시킴을 확인하였다.

둘째, 개인정보 유출 기업에 대한 횡단면 회귀분석 결과 모형 1 및 2의 기업규모변수 $LN(ASSET)$은 5% 유의수준에서 의미 있는 결과를 보이지 못했다. 기업규모가 비정상수익률 및 누적비정상수익률에 영향을 미치지 못했다. 모형 1-b의 성장기회의 대용변수 ME/BE는 5% 수준에서 유의한 음(-)의 값을 보였다. 성장기회가 클수록 기업가치가 더욱 크게 하락함을 확인할 수 있었다. 기업유형의 더미변수 $FIRMTYPE$은 5% 수준에서 유의하지 않았다.

셋째, 정보 유출 기업에 대한 사건공시는 전체 정보보안 기업의 AAR 및 CAAR에 유의한 영향을 미치지 못했다. 정보보안 기업을 물리적 보안, 네트워크 및 시스템 보안, 보안 응용 소프트웨어, 암호·인증, 시스템 통합으로 분류하여 분석한 결과 사건일 다음 날(1일) 네트워크 및 시스템 보안 기업의 AAR은 5% 수준에서 유의한 양(+)의 값을 보였다. 반면, 물리적 보안, 보안 응용 소프트웨어, 암호·인증 및 시스템 통합 기

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

업의 AAR 및 CAAR은 어떠한 날에서도 유의한 결과를 보이지 않았다. 개인정보 유출에 따른 정보전이 효과가 정보보안 기업 중 네트워크 및 시스템 보안 기업에서 발생함과 더불어 이 효과가 시간적 간격을 두고 나타남을 확인할 수 있었다.

넷째, 정보보안기업에 대한 횡단면 회귀분석 결과, 모형 3 및 4의 기업규모변수 *LN*(*ASSET*)은 5% 수준에서 유의하지 않았다. 성장기회의 대용변수 *ME*/*BE*는 모든 모형에 있어 5% 수준에서 유의한 음(-)의 값을 보였다. 결과적으로 성장기회가 클수록 주식가격이 적게 올라감을 알 수 있었다. 기업유형의 더미변수 *PHY*(물리적 보안 기업), *NS*(네트워크 및 시스템 보안 기업), *SOL*(보안 응용 소프트웨어 기업), *CER*(암호·인증 기업) 및 *SI*(시스템 통합 기업) 중 *NS*가 모형 3-b에서 5% 수준에서 유의한 양(+)의 값을 보였으며, 나머지 더미변수는 모두 유의하지 않았다. 개인정보 유출 기업에서 정보보안기업으로의 정보전이 효과가 나타나기 위해선 일정한 전이 시간이 요구됨을 거듭 확인할 수 있었다.

개인정보 보호에 대한 중요성이 날로 증가되고 있는 오늘날에 있어, 본 연구의 결과는 개인정보를 수집·활용하고 있는 기업에게는 이에 대한 철저한 보안이 필요함을 말한다. 또한, 국가는 개인정보가 부당하게 유출되어 활용되지 않도록 하는 수단으로 정보보안 기업의 육성을 모색할 필요가 있겠다.

본 연구에서는 정보보안기업을 선정할 때 기업의 전자공시시스템 내 개황정보에서 제공하는 사업내용을 바탕으로 정보보안기업으로 볼 수 있는 업체를 선별하였다. 선별 시 각 기업이 공시한 사업내용 및 제품을 홈페이지를 통해 모두 검토함과 더불어 2017년 국내 정보보호산업 및 실태조사에서 정보보안기업으로 분류된 업체와 일치성 여부를 추가적으로 확인하였다. 그러나 본 연구에서 선정된 정보보안기업의 경우 정보보안사업의 구체적인 사업 범위와 정보보안사업이 전체 매출에서 차지하는 비중 등을 고려하지 못했다. 따라서 향후 연구에서는 정보보안기업에 대한 명확한 정의와 사업분야에 대한 세밀한 검토를 통하여 정보보안 전문 기업들만을 대상으로 한 추가적인 연구가 필요할 것으로 보인다.

또한, 개인정보유출 사건 공시 자료 수집을 뉴스 검색에 의존할 수밖에 없는 한계가 있으며, 당일 해당 기업의 주가 수익률에 영향을 미칠 수 있는 개별 사건들이 있을 수 있기 때문에 이에 대한 통제가 필요하다. 본 연구에서는 단순히 세부 분류 더미로만 이를 통제하고 있는데, 향후 연구에서는 개인정보 유출 사건 이외의 다른 이벤트에 대한 조사를 통해서 주가에 대한 영향력을 통제하는 과정이 필요할 것이다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

참고문헌

강신기, “개인정보보호법 제정경과 및 주요 내용”, 한국정보보호학회, 2011년 2월, pp. 3-14.

권영옥, 김병도, 정보보안 사고와 사고방지 관련 투자가 기업가치에 미치는 영향,” Information Systems Review, 제9권, 제1호, 2007, pp. 105-120.

김민정, 허남길, 유진호, “개인정보 유출 사고 시 정보보호 기업의 주가 변동에 관한 연구,” 정보보호학회논문지, 제26권, 제1호, 2016, pp. 275-283.

김여라, 이해춘, 유진호, 「가상가치접근법(CVM)을 활용한 개인정보보호의 가치 산출 방법론 고찰」, 한국정보보호진흥원, 2007.

김정연, “개인정보 유출이 기업의 주가에 미치는 영향,” 한국전자거래학회지, 제18권, 제1호, 2013, pp. 1-12.

김태환, 이해니, 유진호, “개인정보 유출사고 이후 기업의 주가변동 패턴에 대한 고찰,” 한국경영정보학회 춘계공동학술대회, 2014, pp. 89-92.

선우홍석, “프라이버시의 권리”, 연세대학교, 1986.

양재모, “전자거래상 개인정보보호에 대한 민사적 접근,” 사이버커뮤니케이션 학보, 제27권 제2호, 2010, pp. 91-119.

이강신, 이기혁, 반진식, 최일훈, 「개인정보보호 기초와 활용」. 인포더북스, vol. 1, 2010년 10월, pp.12-15.

이문구, 배춘석 “APT 공격의주요사례에 대한 연구”, 2013년도 대한전자공학회 추계종합학술대회, 2013년 11월, pp. 939-942.

이해춘, 안경애, “CVM을 이용한 개인정보 유출의 손실가치 분석,” 생산성논집, 제22권, 제2호, 2008, pp. 1-24.

임설화, 김종수, 양준근, 임채호, "APT 현황과 신종 악성코드 대응방안", 정보보호학회지, vol. 24, no.2, 2014년 4월, pp.63-72

오일석, “개인정보 보호의무 위반에 따른 배상 가능한 “손해”에 대한 고찰,” 이화여자대학교 법학논집, “제19권 제3호, 2015, pp. 1-31.

유진호, 지상호, 임종인, “개인정보 유·노출 사고로 인한 기업의 손실비용 추정,” 정보보호학회논문지, 제19권 제4호, 2009, pp. 63-75.

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

정형찬, “한국주식시장에 적합한 사건연구 방법론의 고안,” 재무관리연구, 제14권, 제2호, 1997, pp. 273-312.

김광용, 주미진, 김진수, “개인정보 유출이 기업의 주가에 미치는 영향 : 한국 및 중국의 기업을 대상으로,” 인터넷전자상거래연구, 제16권, 제3호, 2016, pp. 53-65.

채승완, “개인정보보호의 경제적 효과,” 소비자문제연구, 제33호, 2008, pp. 43-64.

최승원, 이병준, 이희정, 이현수, 양승미, 김민정, 구슬, “정보통신분야 해외 개인정보 관련 법제도 비교 연구”, 이화여자대학교 산학협력단, 2011.

한국정보보호진흥원, 「인터넷 웹사이트에서의 주민등록번호 수집 및 도용 방지방안에 관한 연구」, 한국정보보호진흥원, 2004.1, p97

한귀현, “개인정보법제의 동향과 개선방안,” 공법학연구, 제6권, 제2호, 2005, pp. 81-107.

한창희, 채승완, 유병준, 안대환, 박채희, “기업의 개인정보 유출로 인한 경제적 피해규모 산출방법,” 한국전자거래학회지, 제16권, 제4호, 2011, pp. 17-31.

홍일유, 이재훈, 강성민, “정보보안 사고에 대한 공시가 시장에서 기업의 주식가치에 미치는 영향,” Entrue Journal, 제14권, 제2호, 2015, pp. 33-56.

국가법령정보센터, 「개인정보 보호법」, 2017.

국가법령정보센터, 「정보통신망법」, 2014.

권헌영, 「개인정보보호의 의의 및 분류체계」, 개인정보보호포럼자료(정부혁신 지방분권위), 2004.

데이코산업연구소, 「정보보호산업 실태와 기술개발 동향」, 2013.

정교일, 이병천, 진승헌, “훤히 보이는 정보보호”, 한국전자통신연구원, 2018.

정보통신기술 진흥센터, “ICT R&D 중장기 기술로드맵 2022”, 2016.

정보통신정책연구원, 「개인정보보호법 개정의 배경 및 개정안의 주요 내용」, 2014.

정승 「Privacy Global Edge」, 중국사회과학원, 2017.

한국인터넷진흥원, 「개인정보보호법」, 2014.

행정안전부, 「유럽 일반 개인정보보호법(GDPR) 1차 가이드라인」, 2017

김인순, “데이터 유출 사고 원인은 ‘임직원 부주의”, 전자신문, http:・・www.etnews.com・20160614000287, 2016.

김태형, “기업 데이터 보안 침해 9가지 패턴과 대응법”, 보안뉴스,

Collection @ chosun

조선대학교 CHOSUN UNIVERSITY

http:・・www.boannews.com・media・view.asp?idx=42679&kind=3, 2014.
문가용 “모바일과 사물인터넷 위기론? 암호가 더 큰 문제”, 보안뉴스,
http:・・www.boannews.com・media・view.asp?idx=50437&kind=4, 2016.
엘지씨앤에스, 「해외주요국가들의 개인정보 보호 방법은」,
http:・・blog.lgcns.com・1584?category=604440, 2018.
위키백과, https:・・ko.wikipedia.org・wiki・보안취약점, n.d.
한국인터넷진흥원, 「KISA온라인 개인정보보호 포털」,
https:・・www.i-privacy.kr・servlet・command.user4.IndexCommand, 2018.

Acquisti, A., A. Friedman, and R. Telang, “Is There Cost Privacy Breaches? An Event Study,” *Working Paper*, 2006, pp. 1563-1580.

Brown, S. and S. Warner, “Measuring Security Price Performance,” *Journal of Financial Economics*, Vol. 8, No. 3, 1980, pp. 205-258.

Brown, S. and S. Warner, “Using Daily Stock Returns: The Case of Event Studies,” *Journal of Financial Economics*, Vol. 14, No. 1, 1985, pp. 3-31.

Cavusoglu, H., B. Mishra, and S. Raghunathan, “The Effect of Internet Security Breach Announcement on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers,” *International Journal of Electronic Commerce*, Vol. 9, No. 1 2004, pp. 69-104.

Chan, S. H., J. W. Kensinger, A. J. Keown, and J. D. Martin, “Do strategic alliances create value?,” *Journal of Financial Economics*, Vol. 46, 1997, pp. 199-221.

Das, P., K. Sen, and S. Sengupta, “Impact of strategic alliances on firm valuation.” *The Academy of Management Journal*, Vol. 41, 1998, pp. 27-41.

Ettredge, M., and V. J. Richardson, “Assessing the Risk in e-Commerce,” *Proceedings of the Thirty fifth Hawaii International Conference on Systems Sciences,* Los ALamitos, CA: IEEE Computer Society Press, 2002.

Klaus Schwab, The Fourth Industrial Revolution, 2016

Ishiguro, M., H. Tanaka, K. Matsuura, and I. Murase, “The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market,” *In Workshop on the Economics of Securing the Information Infrastructure*, 2006,

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

pp. 1-15.

Lee, H., S. Kim, and J. Kim, "Open technology innovation activity and firm value: evidence from Korean firms," *Applied Economics*, Vol. 44, 2012, pp. 3351-3561.

Patel, N., "The Effect of IT Hack Announcements on the Market Value of Publicly Traded Corporations," *Working Paper*, 2010, pp. 1-24.

Privacy International, Privacy and Human Rights 2002, 2002.

Samuel D.Warren, Louis D. Brandeis, The Right to Privacy, Harvard Law Review Vol. Ⅳ, No.5, 1890.

Strategies for Dealing With Advanced Targeted Threats, GARTNER Aug. 2011.

Szewczyk, S. H., G. P. Tsetsekos, and. Zantout, "The valuation of corporate R&D expenditures: evidence from investment opportunities and free cash flow," *Financial Management*, Vol. 25, 1996, pp. 105-110.

Telang, R., and S. Wattal, "An Empirical Analysis of the Impact of Software Vulnerability Announcements on the Firm Stock Price," *IEEE Transactions on Software Engineering,* Vol. 33, No. 8, 2007. pp. 544-557.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

ABSTRACT

A Study on the Effect of Personal Information Breaches and Information Transfer on Firm Value

Park, SangSoo
Advisor : Prof. Lee, HyunChul, Ph.D.
Department of business administration,
Graduate School of Chosun University

Purpose

Targeting Korean companies listed on Korean securities markets (i.e., KOSPI and KOSDAQ markets), this study aims to shed lights the effects of personal information security breaches on stock prices of information security companies. Interestingly, this study is, to the best of our knowledge, the first to examine the information transfer effect on personal information security breaches of companies.

Design · Methodology · Approach

To examine the information transfer effect of personal information security breaches, our study employs the event study commonly used in financial studies. To this end, we investigate a variety of events of personal information security breaches of companies listed on the KOPSI stock market and the KOSDAQ market. We collect the total samples of one hundred and twelve with forty seven of events of personal information security breaches by thirty companies and sixty five of information security companies.

Findings

The principal findings from the empirical study are as follows. First, for companies of personal information security breaches, our event study presents the significantly negative AAR (averaged abnormal return) value on the event day at

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

the 5 % level and the highly significant negative CAAR(cumulative averaged abnormal return) value on the event day and the day after the event day at the 1 % level. The results suggest that personal information breaches significantly contribute to an decrease in value of the information breached companies. The cross sectional regressions in this study estimate the significantly negative coefficient for the ME・BE variable, the proxy for a growth opportunity at the 5 % level. This suggests a reverse relation between the growth opportunity of companies and their value.

As for the various samples of the information security companies categorized by physical security, network and system security, security application software, code authentication, system integration, we find the significantly positive AAR on the day after the event day at the 5% level, only for the network and system security-companies. This addresses that the information transfer effect followed by personal information breaches is uniquely observable for companies categorized into network and system companies. The regressions for the network and system companies estimate the significantly positive coefficient for the *NS* dummy variable (i.e., the dummy of the network and system security companies) at the standard level. This allows us to identify appropriate times needed to make the information transfer effect realized from personal information breached companies to information security companies.

Keyword: Personal information breaches, Information transfer, Event study, Value of company

Collection @ chosun