Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.4, Aug. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.4.855

불완전 정보 하의 정보보호 투자 모델 및 투자 수준*

이 용 필†‡
한국인터넷진흥원

Information Security Investment Model and Level in Incomplete Information*

Yong-pil Lee†‡
Korea Internet & Security Agency

요 약

Gordon과 Loeb[1]은 기업의 정보보호 투자 의사결정은 정보보호 투자를 통한 한계편익(MB)과 정보보호 투자의 한계비용(MC)이 일치하는 곳에서 최적의 투자수준이 결정된다고 한다. 그러나, 정보보호 사고를 당하고 있는 많은 기업의 경우, 정보보호 사고를 당하고 있다는 것을 인지하지 못하고 유출되는 피해가 얼마인지 측정하지 못하고 있다. 본 연구에서는 불완전한 정보 상황에서 정보보호 투자 의사결정을 수행하는 모델을 Gordon과 Loeb[1]의 모델을 수정하여 제시하고, 투자수준의 차이를 비교하였다. 불완전정보 하에서 정보보호 투자를 통한 기대수익은 실제 발생하는 정보보호 사고에 비해 낮게 인식되는 경향을 띄게 되고, 정보보호 투자도 적게 되었다. 이는 정부와 같은 제3의 기관이 정보보호 사고발생률, 피해액 규모 등 정확한 정보를 알려주면 기업 스스로 정보보호 투자를 확대 할 수 있음을 보여준다.

ABSTRACT

Gordon & Loeb[1] suggested that the optimal level of investment decision of an enterprise is the point that the marginal benefit(MB) of information security investment is equal to the marginal cost(MC). However, many companies suffering from information security incidents are not aware of the fact that they are experiencing information security accidents and can not measure how much they are affected. In this paper, I propose a model of information security investment decision making under the incomplete information situation by modifying the Gordon & Loeb[1] model and compare the differences in investment level. Under the incomplete information situation the expected return from the information security investment tends to be lower than that of actual information security investment, and the level of investment is also less. This shows that if a third party such as the government gives accurate information such as the rate of incidents of information security accidents and the amount of damages, companies can expand their investment in information security.

Keywords: Information Security Investment, Incomplete Information

I. 서 론

최근 인터넷을 통해 기업들의 중요 정보가 해킹되고, 고객정보가 유출되는 사고들이 빈번하게 발생하고 있으나, 기업들은 정보보호 투자를 많이 하지 않는다고 한다[13].

Gordon과 Loeb[1]은 정보보호 사고들이 발생할 수 있는 취약점이 존재할 때, 위험중립적인 기업이, 기대수익을 계산하여 감내할 수 있는 규모로 최적의 정보보호 투자수준을 정할 수 있는 모델(이하 GL 모델)을 제시하였다. 그러나, 현실적으로 기업들은 정보보호 사고를 당하는지 모르고 지나는 경우가 많

Received(03. 14. 2017), Modified(06. 15. 2017), Accepted(06. 15. 2017)
* 본 논문은 2016년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임
† 주저자, joseph.lyp@gmail.com
‡ 교신저자, joseph.lyp@gmail.com(Corresponding author)

으며, 실제 기업이 겪고 있는 피해규모의 크기를 정확하게 알지 못하는 상황에서 적정수준의 정보보호 투자수준을 정하기 어렵다. 본 논문에서는 정보보호의 특성상 피해규모 등에 대한 정보수집이 불완전한 상황을 가정하여, GL모델을 수정하여 공격발생률, 피해규모 등에 정확하게 인식하지 못하는 상황에서 정보보호 투자에 미치는 영향을 설명하고 그 정책적 대안을 제시하고자 하였다.

II. 선행연구

2.1 GL 모델 : 정보보호 적정 투자 모델

기업은 개인정보, 고객리스트, 거래내역 등의 주요정보를 보호하기 위해 어느 정도의 투자를 해야 최적의 수준인지 질문을 하고 있다. 이에 대해 Gordon과 Loeb은 최적의 정보보호 투자 금액을 계산할 수 있는 경제학적 모델을 개발하여, 정보보호 취약성과 투자금액을 변수로 사용하는 GL 모델을 제시하였다[1].

GL모델은 one period model로, 위험중립적 기업을 가정하였고, 정보보호를 정보자산의 무결성, 기밀성, 가용성을 지키는 것으로 정의하고 있다.

변수로 정보 유출사고로 인한 금전적 손실액(λ), 공격발생률(t), 정보자산의 취약성(υ)을 제시하였다.

정보보호 사고 발생 시 금전적 손실액을 λ로 정의하고 고정금액을 가정하였다. 공격발생률을 t로 설정하고, 1번 발생을 가정하고, 고정 값을 사용하였다.

정보자산의 취약성 υ는 정보자산을 대상으로 정보보호 공격이 일어날 때 사고가 발생할 확률을 의미하며, 정보자산에 대한 추가적인 보안이 없는 경우 실현된 위협이 λ의 손실을 발생하게 된다.

2.1.1 정보보호 기대손실

정보보호 사고 발생시 기대 손실(EL)은 정보 유출사고로 인한 금전적 손실액(λ), 공격발생률(t), 정보자산의 취약성(υ)에 의해 결정된다.

정보보호 기대 손실(EL) = 정보보호 사고 발생 시 손실(λ) * 공격발생률(t) * 정보자산의 취약성(υ), (0〈t〈1, 0〈υ〈1) (1)

2.1.2 정보보호 투자

L은 공격발생시 손실액(tλ)이고, 기업의 정보보호 투자로 공격발생률 t를 감소시킬 수 없으므로 t는 고정된 것으로 보았다.

정보보호 투자(z)는 정보자산의 취약성(υ)을 감소시키는 역할을 한다. 정보자산을 안전하게 보호할 수 있는 이상적인 정보보호 투자금액을 z 라고 하고, 시스템의 취약성 υ가 존재할 때, z 만큼의 투자가 이루어졌을 때 사고가 발생할 확률을 새롭게 S(z, υ)라는 함수로 정의한다. S(z, υ) 함수는 보안사고 발생 확률함수(security breach probability function)로, 관련된 핵심적인 가정은 다음과 같다.

(가정) 모든 υ에 대해 υ ∈ (0, 1) 이고, 모든 z에 대해, $S_z(z, \upsilon) < 0$ 이고 $S_{zz}(z, \upsilon) > 0$

즉, S(z, υ)는 z가 늘어나면 υ가 감소하며, z가 늘어날 때 υ가 감소하는 폭은 줄어든다[1].

2.1.3 정보보호 적정 투자 수준

정보보호 투자를 통한 기대 수익(EBIS)은 투자 덕분에 줄어든 기업의 손실 금액과 같다.

$$EBIS(z) = \upsilon L - S(z,\upsilon)L = \{\upsilon - S(z,\upsilon)\}L \quad (2)$$

{υ-S(z, υ)}는 정보보호 투자를 통해 줄어든 기업의 보안시스템 취약성을 의미한다.

정보보호투자의 순수익(ENBIS)은 기대수익과 투자액의 차이로 계산할 수 있다.

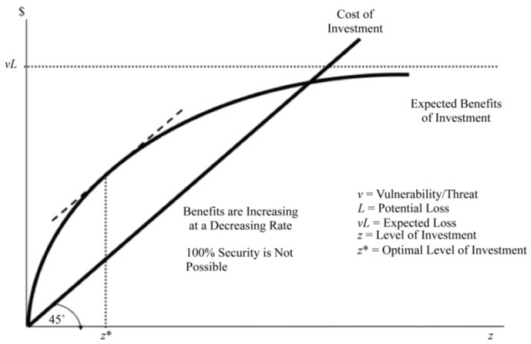

Fig. 1. Benefits and costs of information security investment and optimal level z* of investment

1) 2번 연속 미분가능하며, 볼록함수를 의미

$$ENBIS(z) = \{\upsilon - S(z, \upsilon)\}L - z \quad (3)$$

정보보호 투자를 통한 기대 수익(EBIS)의 기울기인 한계편익(MB)이 정보보호 투자액(z)의 기울기인 한계비용(MC)과 일치하는 z^* 수준일 때, 순수익이 최대가 되며, 정보보호 최적 투자수준이 된다.

참고로, Gordon과 Loeb 모델[1]에서는 z^*를 피해액의 37% 수준이라고 제시하고 있다.

2.2 불완전 정보와 관련한 연구

Gordon 등[5]은 정보공유를 통해 더 적은 비용을 들여 높은 보안 수준을 유지할 수 있는 기회를 얻을 수 있음을 의사결정과정의 예시를 통해 가치평가 모형연구방법론으로 보여주었다. Gordon 등[5]과 Gal-Or 등[6]의 연구들은 정보공유를 통해 적은 보안 투자로 더 많은 정보보안수준을 달성할 수 있음을 보여주고 있다. Lucyshyn 등[3]에서는 등생산량곡선(isoquant curve)의 개념을 도입하여 두가지 정보보호 솔루션의 조합에 따라 동일 정보보호수준을 달성하는 조합을 제시하는 곡선에 정부의 규제정책이 미치는 효과를 분석하였다. 기업이 최적의 정보보호 투자조합을 알 수 있는 경우와 그렇지 않은 경우 정부의 규제정책이 정보보호 투자를 확대할 수 있는지 여부를 기업의 투자 증진의지와 관련해서 인풋-아웃풋 분석(input-output analysis)를 이용하여 설명하였다. 그러나, 이러한 연구들은 불완전정보하에 정보공유를 통해 기업의 보안투자의 효과를 높인다거나 정보보호 투자확대를 위한 정부규제의 효과를 분석하고 있지만, 기업들의 투자수준에 미치는 영향에 대해 GL 모델을 확장해서 설명하고 있지는 않다.

Gordon 등[2]은 GL 모델을 정보보호 피해의 외부성을 고려하여 기업 손실에 사회적 외부비용을 추가하여 사회적 적정 투자를 구할 수 있는 모델로 확장하거나, Gordon 등[10]은 GL 모델을 실제 투자에 적용하는 사례를 제시하고 있다.

III. 연구내용

3.1 불완전 정보하의 정보보호 투자 모델

3.1.1 불완전 정보하의 모델

GL 모델에서는 정보보호 투자를 통한 기대수익을 구성하는 내용이 정보보호 사고 발생 시 손실(λ), 정보보호 사고 발생률(t), 정보보호 취약성(υ)에 의해 결정되며, 각 개별 기업의 경제주체가 이들 변수의 정보를 추측하여 매트릭스 형태로 자산을 분류하고, 취약점 수준을 유추하고 정보보호 투자수준에 따라 취약점이 낮아지는 함수를 구하고, 기대수익, 기대비용, 최적 투자수준을 계산하도록 하고 있다[10]. 그러나, 이러한 것을 계산하기 위해서는 많은 정보가 필요한데, 정보보호 사고의 특성상 개별 경제주체가 이러한 정보를 모두 파악하기란 현실적으로 불가능하다.

본 연구에서는 현실적인 모델을 제시하기 위해 사고발생률, 사고피해액에 대한 불완전 정보를 반영하여 모델을 수정하였다.

3.1.2 정보보호 투자 및 기간 가정

GL 모델에서는 정보보호 투자의 종류를 구체적으로 제시하지 않고, 기밀성, 무결성, 가용성을 높여 정보자산의 취약성을 줄이기 위한 것으로 제시하였고, 기간을 one period model로 제시하였다[1].

본 연구의 모델에서는 정보보호 투자가 정보보호 사고발생률, 피해액 등을 추정하기 위한 정보의 정확성 등과 연계가 될 수 있다는 것을 고려하여 정보보호 투자를 세 가지로 구분하여 제시하였다. 또한 기간은 연간 공격이 지속적으로 발생하고 있다는 것을 고려하여, 1년 기간에 투자액을 제시하였다.

정보보호에 대한 투자수준을 공시하는 기준으로 한국인터넷진흥원에서 제시하고 있는 항목은 1) 정보보호 투자 현황, 2) 정보보호 인력 현황을 공시하도록 하고 있다[11].

정보보호 투자는 정보보호 제품 투자와 정보보호 서비스 투자로 구분할 수 있다. 일반 기업에서는 정보보호 제품 투자 이외에 정보보호 서비스를 이용하고 있다, 실제 정보보호 사고가 발생하는 것을 탐지하고 이를 막기 위해서는 관제서비스와 내부 직원이 모니터링을 하고, 사고발생 시 바로 대응하도록 운영되어야 한다. 관제서비스와 내부직원이 없거나 부족한 경우 실제 사고가 발생해도 이를 인지하지 못하거나 대응을 하지 못하므로 정보자산의 피해액(λ)을 파악하지 못하게 된다.

따라서, 정보보호 투자를 할 때, 개별 경제주체가 스스로 하는 정보보호도 있지만, 외부 전문 업체를

통한 정보보호 서비스를 이용하는 경우 보다 정보의 취득에 용이할 수 있음을 모델에 반영하였다.

또한, 내부 정보보호 조직 운영시 모니터링을 통한 침해사고를 탐지하고, 침해사고 발생 시 즉각적인 대응을 통해 손실을 줄일 수 있으므로 정보보호 투자에 내부조직 운영을 하는 것도 모델에 반영하였다.

GL 모델에서는 공격발생률(t)을 0에서 1사이로 보았으나, 불완전 정보하의 모델에서는 연간 공격횟수로 수정하여 적용하였다.

3.1.3 불완전 정보하의 정보보호 투자 모델

관제서비스를 하지 않거나, 정보보호 조직을 운영하지 않는 경우 공격발생건수(t) 및 피해액(λ)을 모르므로 불완전정보 상태에서 기업들이 인식하는 손실(λ′), 정보보호 공격 발생 인지건수(t′)를 대부분 낮게 인식하게 된다.

즉, 공격발생 인지율을 a , 피해액 인지율을 b 라고 할 경우 불완전정보 상태에서 기업들이 인식하는 피해액(λ′)과 정보보호 공격 발생 인지건수(t′)는 다음과 같다.

$$t' = t^{*}a,\ \lambda' = \lambda^{*}b\ (0<a<1,\ 0<b<1) \quad (4)$$

불완전정보(Incomplete Information) 하의 정보보호 투자 기대수익을 다시 정리하면

$$\text{II-EBIS}(z) = \upsilon ta\lambda b - S(\upsilon, z)ta\lambda b$$
$$= \upsilon L' - S(\upsilon, z)L' \quad (5)$$

따라서 불완전정보(Incomplete Information) 상태에서 기업들이 인식하는 정보보호 기대 손실액(L′)은 실제 정보를 정확하게 인식할 때의 기대 손실액(L) 때보다 낮게 될 것이다.

3.2 GL 모델과 불완전 정보하의 정보보호 투자 모델 사례 비교

GL 모델에서 정보보호 투자는 취약성을 감소시키는 역할을 하게 된다.

사례 비교를 위해 피해액, 공격발생건, 취약성, 정보보호 투자 종류별 취약성 감소 효과, 정보보호 피해핵 인지율, 공격발생 인지율 등을 구체적인 수치로 제시하였다. 수치 등은 정보보호 기업들의 침해사고 통계, 전문가 의견 등을 고려하여 제시하였다.

그리고 정보보호 투자수준을 정보보호 제품만 투자하는 경우 ①, 정보보호 제품과 서비스에 투자하는 경우 ②, 정보보호 제품과 서비스와 조직도 같이 운영하는 경우 ③으로 3가지로 구분하였다. GL 모델과 불완전 정보하의 모델에서의 기대수익(EBIS)을 비교하였다[2].

3.2.1 정보보호 투자 기업 가정

현실적인 투자효과 계산을 위해 특정한 기업을 아래와 같이 가정하였다.

1) 정보자산의 가치 :100백만원
2) 투자[3] :
   ① 정보보호 제품 : 1백만원/연
   ② 정보보호 서비스 : 1백만원/연
   ③ 조직 운용 : 1백만원/연
3) 피해액(λ) : 1백만원/회,
4) 연 공격발생건 수(t): 120회/연[4]
5) 취약성(υ) : 1회 공격에 50% 성공[5]
6) 정보보호 투자에 따른 취약성 차단 능력(S(υ, z)) : 정보보호 제품 70%, 정보보호 서비스 70%, 조직 운영 90%
7) 정보보호 피해 인지율(a) : 20%, 공격발생 인지율(b) : 20%[6]

2) 본 연구에서는 직접적으로 최적투자수준을 비교하지 않고 기대수익의 차이를 비교하였다.
3) 정보보호투자를 구성하는 제품과 서비스의 금액 비율은 정보보호 제품과 서비스의 매출비중을 고려하였다. 일본 정보보호 시장의 경우 제품과 서비스의 비중이 약 53:47의 비율이었으며[14], 단순화하여 50:50으로 반영하였다. 정보보호 조직운영 비용도 이와 같은 금액으로 설정하였다.
4) 정보보호 사고발생률은 글로벌 정보보호 업체인 Akamai 고객사의 2016년 1분기 평균 고객별 DDoS 공격 건수가 29회여서, 분기별 30일, 연간 120일로 추정하였다[13].
5) 취약성은 1회 공격에 50% 성공률로 설정하였다. 38,000대의 시스템을 대상으로 모의해킹 실험에서 65% 성공한 사례와 해커의 70%가 아마추어 해커라는 사실을 참고하였다[7].
6) 피해 및 공격인지율은 영국의 경우 대기업 90%, 중소기업 74%가 피해사고를 경험한 것으로 조사된 것[15]에 비해, 한국의 경우 기업의 3.1%, 개인의 17.4%가 침해사고 경험이 있는 것[16]으로 한국이 낮게 조사.

8) 정보보호 투자에 따른 기대수익 비교 : GL 모델과 불완전 정보하의 모델

GL 모델 : EBIS(z) = υL - S(υ, z)L

불완전 정보 하의 모델 : II-EBIS(z') = υL' - S(υ, z)L'

3.2.2 정보보호 투자수준별 기대수익 비교

투자수준1 = ①, 투자수준2 = ①+②, 투자수준3=①+②+③

① 투자수준 1(z_1): 정보보호 제품 1백만원/연

$EBIS(z_1) = \upsilon L - S(\upsilon, z_1)L$ = 18백만원[7] 〉 1백만원 (6)

$II\text{-}EBIS(z_1) = \upsilon L'-S(\upsilon, z_1)L'$ = 0.72백만원[8] 〈 1백만원 (7)

투자수준 1(z_1) 인 경우 GL 모델에서는 기대수익이 18백만원으로 투자금액보다 높은 기대수익을 내고 있어 투자를 하고자 할 것이나, 불완전 정보하의 기대수익은 0.72백만원으로 투자금액 1백만원보다 낮은 금액으로 정보보호에 투자를 하지 않게 될 것이다.

② 투자수준 2(z_2) : 정보보호 제품 1백만원/연 + 정보보호 서비스 1백만원/연

$EBIS(z_2) = \upsilon L - S(\upsilon, z_2)L$ = 30.6백만원[9] 〉 2백만원 (8)

$II\text{-}EBIS z_2 = \upsilon L'-S(\upsilon, z_2)L'$ = 1.224백만원 〈 2백만원 (9)

투자수준 2(z_2) 인 경우 GL 모델에서는 기대수익이 30.6백만원으로 투자금액보다 높은 기대수익을 내고 있어 투자를 하고자 할 것이나, 불완전 정보하의 기대수익은 1.224백만원으로 투자금액 2백만원보다 낮은 금액으로 역시 정보보호에 투자를 하지 않게 될 것이다.

③ 투자수준 3(z_3): 정보보호 제품 1백만원/연 + 정보보호 서비스 1백만원/연 + 조직운영 1백만원/연

$EBIS(z_3) = \upsilon L - S(\upsilon, z_3)L$ = 33.54백만원[10] 〉 3백만원 (10)

$II\text{-}EBIS(z_3) = \upsilon L'-S(\upsilon, z_3)L'$ = 1.3416백만원 〈 3백만원 (11)

투자수준 3(z_3) 인 경우 GL 모델에서는 기대수익이 33.54백만원으로 투자금액 3백만원 보다 높은 기대수익을 내고 있어 투자를 하고자 할 것이나, 불완전 정보하의 기대수익은 1.3416백만원으로 투자금액 3백만원보다 낮은 금액으로 역시 정보보호에 투자를 하지 않게 될 것이다.

IV. 결 론

본 논문에서는 정보보호 사고의 특성상 정보의 불완전한 상황에서 정보보호 투자를 하는 모델을 설정하고, 정보보호 투자수준에 따라 기대수익이 변하는 모습을 제시하였다.

본 연구의 기여는 정보보호 사고가 많이 발생함에도 기업들이 정보보호 투자를 적게 하는 이유를 실제 정보와 기업들이 인지하고 있는 정보가 차이가 발생해서 투자를 부족하게 하고 있다는 점을 모델을 통해 구체적인 수치로 보여 주었고, 불완전 정보하의 투자 모델 연구가 필요함을 제시하였다는 점이다. 이 과정에서 정보보호 투자의 구성항목을 제품, 서비스, 조직으로 제시하고 각각의 투자가 기업들의 취약성을 감소시키는데 각기 역할을 함을 보여주었다. 기업별로 적용할 수 있는 공격발생건수, 피해액 등의 정보가 제공될 경우 기업의 정보보호 투자의사결정에 활용될 수 있을 모델이 될 수 있다. 기업들의 피해액 인지율과 사고발생 인지율이 실제와 어느정도 차이가 있는지는 추가적인 연구를 통해 밝혀야 할 것으로 보인다. 정보보호 관련한 정책적 함의로 정보보호 투자를 늘이기 위해서는 기업들이 인식하는 피해 인지율(a)과 공격발생 인지율(b)에 대한 정보를 기업들이 정확하게 인식할 수 있도록, 정부와 같은 제3의 기관에서 기업들에 관련 정보를 계속 제공해주는 것이

이에 국내는 20%로 추정.

7) υ=0.5, λ=1,000,000, t=120, $S(\upsilon, z_1)$=0.5*0.7

8) L'=taλb= 120*0.2*1,000,000*0.2

9) $S(\upsilon, z_2)$=0.5*0.7*0.7

10) $S(\upsilon, z_3)$=0.5*0.7*0.7*0.9

필요할 것이다.

References

[1] Gordon, L. A., and Loeb, M. P. "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp.438-457, Nov. 2002.

[2] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. "Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model," *Journal of Information Security*, vol. 6, no. 1, pp. 24-30, Jan. 2015.

[3] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. "Increasing cybersecurity investments in private sector firms," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 3-17, Nov. 2015.

[4] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. "The impact of information sharing on cybersecurity underinvestment: a real options perspective," *Journal of Accounting and Public Policy*, vol. 34, no. 5, pp. 509-519, Sep. 2015.

[5] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. "Sharing information on computer systems security: an economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461-485, Nov. 2003.

[6] Gal-Or, E. and Ghose, A. "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186-208, June 2005.

[7] Shin, Soojung, Innovation with Security, Elcompany, Apr. 2013.

[8] Kong, H.K., Jun, H.J., and Kim, T.S., "A study on information security investment by the analytic hierarchy process," *Journal of Information Technology Applications & Management*, 15(1), pp. 139-152, Mar. 2008.

[9] Kong, Hee-Kyung and Kim, Tae-sung. "Research trends on information security investment effect," *Korea Institute of Information Security and Cryptology*, 17(4), pp. 26-33, Aug. 2007

[10] Gordon, L.A., Loeb, M.P. and Zhou, L. "Investing in cybersecurity : insights from the Gordon-Loeb model," *Journal of Computer Security*, vol. 7, no. 2, pp. 49-59, Mar. 2016.

[11] Kisa, https://www.kisa.or.kr/notice/notice_View.jsp?cPage=1&mode=view&p_No=4&b_No=4&d_No=1756&ST=T&SV=공시

[12] Symantec, https://www.symantec.com/content/en/us/about/media/pdfs/2012-state-of-information-global.en-us.pdf

[13] Akamai, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2016-state-of-the-internet-security-report.pdf

[14] KISIA, http://www.kisia.or.kr/new_kisia/bbs/board.php?bo_table=s6_board3&wr_id=28

[15] UK, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf

[16] Kisa, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf

〈저자소개〉

이 용 필 (Yong-pil Lee) 정회원
1995년 8월: 서울대학교 경제학과 졸업
2003년 8월: 서울대학교 행정대학원 석사
2016년 2월: 서울대학교 행정대학원 박사
2003년 8월~현재: 한국인터넷진흥원
〈관심분야〉 정보보호정책, 정보보호교육, 개인정보보호