정보보호수준 자가진단 방법론에 대한 연구

안소진° 박진섭 이희성 가소진
대전대학교 컴퓨터공학과
ansolove°@nate.com, jspark@dju.ac.kr, hslee0807@hanmail.net, so_gene@naver.com

A study on the Self-assessment method of Information security level

Sojin An° Jinsub Park Heesung Lee Sojin Ka
Department of computer engineering, Daejeon University

요 약

정보보호는 다양한 측면에서 수행되어야함을 고려 할 때 정보호수준평가는 전체적인 보안수준과 함께 분야별 평가가 수행되고, 평가 점수가 낮은 분야를 우선 보완을 통해 전체적인 수준향상을 목적으로 한다.

본 논문에서는 기존의 시스템 측면에서 이루어지는 정보보호 수준평가의 문제점을 해결하기 위해 국내·외 정보보호 수준 평가 사례를 비교 · 분석한다. 분석된 사례를 통해 물리적/기술적/관리적 측면의 다양한 분야에 대한 가중치측정이 이루어져 기업의 정보보호수준을 향상시킬 수 있는 정보보호 수준 자가진단 방법론을 제시한다.

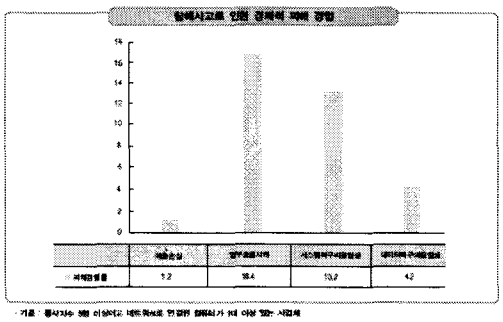
1. 서 론

각종 보안위협으로부터 각 조직은 자신들의 정보를 보호하기 위해 여러 가지 방법론으로 전략을 수립하고 있다. 정보보호는 현재의 보안수준을 평가함으로서 목표수준을 수립 할 수 있으며, 어떤 부분이 높고, 낮은 수준인지를 판별 할 수가 있다. 따라서 다양한 방법으로 정보보호수준을 측정하는 기법이 개발되고 있다.

현재 미국에서는 전자정부법의 3편에 연방정보보안관리법(FISMA : Federal Information Security Management Act)을 통하여 정보보안 현황에 대한 보고서를 작성하여 매년 평가 결과를 발표하고 있다.

국내에서는 공공기관을 대상으로 정보보안관리 수준을 평가하기위한 보안관리수준평가 안전점검 체크리스트를 국가정보원에서 연구하여 적용하고 있다. 그리고 한국정보보호진흥원에서는 주요정보통신기반시설을 대상으로 한 정보보호수준평가 방법론과 중소기업을 대상으로 한 자가진단 도구를 웹상에 만들어 서비스를 제공하고 있다.

다음 [그림 1]은 2006년 정보보호실태조사의 기업편에 나타난 침해사고의 경제적 피해 경험을 나타낸 그림이다. 기업 중 정보보호침해사고로 인한 매출손실이 1.2%로 나타났다.



[그림 1] 침해사고로 인한 경제적 피해 경험
출처 : 2006 정보보호실태조사 기업편

따라서 평가를 위한 정보보호의 문제점과 시스템측면에서 이루어지고 있는 평가를 해결해야 한다. 본 논문에서는 기업의 정보보호수준을 체계적으로 향상시킬 수 있는 평가가 되기 위해 국내·외 정보보호 수준평가 사례 및 방법론을 비교·분석한다. 또한 기업의 정보보호수준을 향상시키기 위해 물리적, 기술적, 관리적인 측면에서의 정보보호수준 자가진단 방법론을 연구했다.

2. 관련 연구

2.1 국내·외 정보보호수준평가 사례 비교·분석

미국은 FISMA의 법에 따라 연방정부기관들의 정보보안관리 실태를 매년 평가하고 있다. 각 연방기관에서 재출된 보고서는 정부감독조사 위원회에서 FIPS 200(Federal Information Processing Standard)지침을 이용하여 보고서를 검토한다. 이 지침은 NIST SP800-53A의 지침을 통하여 구성되어 있다. 연방기관의 보고서 평가 결과는 FISMA에 따라 A*~F까지 측정된다.

국내에서는 국가정보원에서 공공기관을 대상으로 평가사례와 한국정보보호진흥원에서 중요정보통신기반시설을 대상으로 한 정보보호수준평가, 중소기업을 대상으로 한 정보보호수준 평가가 실시되고 있다.

국내·외 정보보호수준평가 사례를 비교하면 다음 [표 1]과 같다.

[표 1] 국내·외 정보보호수준평가 사례 비교

	FIPS 200 (NIST SP 800-53A)	보안관리 수준평가	정보보호 수준평가	중소기업의 정보보호 자가측정도구
목적	미국의 연방정부기관들의 정보 및 정보시스템을 보호하기 위한 법	국내의 중앙행정기관의 안전성을 확인하고 보안대책을 수립하여 국가안전을 확보하고자함	주요정보통신기반시설의 안정적인 운영과 관리를 제공하고 성숙도를 평가	중소기업의 저인력, 고비용 보안인식 부족 등의 문제점을 극복하여 보안수준을 향상시키기 위한 도구
특징	- 정보감사위원회를 통하여 FIPS 200과 NIST의 SP 800-53의 지침을 이용하여 평가 - 매년 A*~F까지 연방정부기관의 점수를 공개	- 평가항목에 대한 가중치를 두어 평가 - 평가항목의 수행여부만으로 평가	- 기반시설의 정보보호 수준 성숙도 평가 - 성숙도평가를 통해 기반시설의 수준을 안정적으로 향상시킴	- 중소기업에서 의존하고 있는 정도에 따라 목표치가 결정 - 기업의 목표에 따라 수준이 낮을 경우 보안대책 제시

3. 정보보호 수준평가 방법론 연구

3.2 정보보호수준평가 방법

기업에서의 정보 및 정보시스템의 정보 유출, 정보 악용, 웜/바이러스 등과 같은 여러 가지 위협들로부터 정보의 노출도가 높다. 이러한 위협들은 기업의 매출과 이익 등이 낮아져 기업이 파산까지 나타날 수 있다.

기업에서는 침해사고 발생 위험도가 높은 것을 인식하고 있지만 인력 부족과 고비용으로 인해 정보를 보호하기에는 역부족이다. 기업의 정보보안 위협들은 국가차원에서도 피해도가 높기 때문에 정보보호수준을 평가하기 위한 성숙도 평가가 이루어져야 한다. 관련연구에서 국내·외 정보보호수준평가 사례를 비교·분석한 결과에 따라 본 논문에서는 주요정보통신기반시설의 정보보호수준평가 모델을 바탕으로 기업의 정보보호수준평가 방법론을 도출하였다.

주요정보통신기반시설의 정보보호수준평가 모델은 다음 [표 2]와 같은 통제 분야 및 통제항목수로 구성되어 있다.

[표 2] 주요정보통신기반시설의 정보보호수준평가 통제분야 및 통제항목수

번호	통제분야	통제항목수
1	정보보호 정책 및 조직	2
2	위험평가	5
3	구성관리	2
4	유지보수	2
5	매체보호	5
6	보안인식과 교육	1
7	비상계획	4
8	물리적·환경적 보호	7
9	인적보안	4
10	사고대응	3
11	감사 및 책임 추적성	5
12	시스템 및 통신보호	16

본 연구에서는 주요정보통신기반시설의 정보보호수준평가 모델을 기업의 특성에 맞게 개선하였다. 개선사항은 세부평가항목의 성숙도 단계별 구분이 객관적이고 명확하게 드러나도록 단계별 특징에 따라 정의를 변경하였다. 또한 평가자의 이해를 돕기 위해 성숙도 단계마다 단계에 해당하는 사례, 해설, 증빙자료 등을 제시하였다. 이는 평가자가 평가단계 선정 시 가이드라인 역할이 되록 구성했다.

기업에서는 정보보호를 위한 비용이 적고 인식이 낮으며 기업의 특성에 따라 정보를 보호해야하는 분야가 다

르게 나타난다. 이를 적용시키기 위해 분야별 가중치를 주어 기업의 특성에 맞게 보안수준을 측정해야한다.

기업에서 중요시하고 있는 분야에 대한 가중치를 산정할 때 해당하는 각 분야마다의 특징적인 질문을 통해서 기업의 가중치를 산정한다. 이는 기업의 평가자에 따라 평가결과가 달라지는 오차의 범위를 최소화하기 위해 적용된 방법이다.

[표 2]의 통제 분야를 NIST SP800-53의 관리, 운영, 기술 분야의 항목으로 나누었다. 관리 통제 분야에는 정보보호 정책 및 조직, 위험평가분야로 분류하고 운영분야는 구성관리, 유지보수, 매체보호, 보안인식과 교육, 업무연속성, 물리적·환경적 보호, 인적보안, 사고대응분야로 분류된다. 기술 통제 분야에서는 감사 및 책임추적성, 시스템 및 통신보호로 분류된다.

정보보호수준평가의 통제분야를 관리, 운영, 기술 분야로 나눈 이유는 기업에서 가중치를 부여할 때 생길 수 있는 문제점들을 해결하기 위함이다. 각 분야별로 가중치를 부여하는 것보다 관리, 운영, 기술 통제 분야별로 가중치를 두어 평가하면 평가자의 이해도 및 평가신뢰도가 높아지기 때문이다.

본 논문의 정보보호수준평가 방법은 관리, 운영, 기술 분야로 분류하여 각 분야에 가중치를 주는 방법에 대한 연구를 하였다. 가중치 부여 시 분야별 관리, 운영, 기술 분야에서 위험발생 비율과 취약점 비율에 따라 Low, Medium, High로 산정한다.

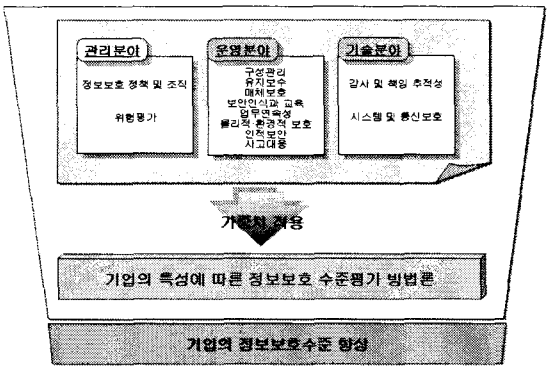
[표 3] 위험발생과 취약점에 따른 가중치

위험발생비율 / 취약점발생비율	Low	Medium	High
Low	1	2	3
Medium	2	3	4
High	3	4	5

위험발생 비율과 취약점 비율이 높게 나타는 분야에서는 침해사고율이 높게 나타나기 때문에 보안에 대한 관심이 높다. 즉, 위험발생 비율과 취약점 비율로 산정된 값이 높은 분야에서 정보보호가 낮게 평가되면 전체적인 기업의 정보보호수준평가가 낮은 결과를 볼 수 있다.

3.2 정보보호수준평가 방법 평가

다음 [그림 2]은 기업의 특성에 따라 가중치를 적용하여 도출된 정보보호수준평가 방법론에 대한 그림이다.



[그림 2] 정보보호수준평가 방법론

정보보호수준평가 방법 평가는 우선 각 통제분야의 세부통제항목의 평가값을 구한다. 통제분야의 값은 세부통제항목의 최소값으로 산정한다. 최소값으로 결정하는 이유는 통제분야를 평균값으로 산출하게 되면 보안의 편차에 따라 값이 달라진다. 또한 보안이라는 것은 취약점을 최소한으로 줄이는 것이 좋은 방법 중의 하나이기 때문에 최소단계를 목표치까지 높이는 것이 중요하다.

통제분야의 성숙도 평가값(CH)에 해당하는 관리, 운영, 기술분야의 위험발생과 취약점에 따른 가중치값을 곱한다.

$$CA = CH \times w$$

(CA: 관리/운영/기술분야별가중치적용값,
CH: 통제분야평가값, w: 관리/운영/기술분야의가중치)

도출된 값을 관리, 운영, 기술분야별로 평균값(CF)을 구하여 3개의 분야를 더하면 기업의 정보보호수준(EAL)이 도출된다.

$$EAL = \sum_{i=1}^{3} CF \quad (CF: \text{관리/운영/기술분야별평균값})$$

3.3 정보보호수준 평가 방법론의 효과성 분석

본 연구를 통해 개발된 정보보호수준 평가 방법론의 효과성을 분석하기위해 모의시범평가를 실시하였다. 국내의 같은 기업들을 대상으로 국가정보원에서 실시하고 있는 보안관리수준평가와 정보보호수준 평가를 평가하였다. [표 3]은 국가정보원의 보안관리수준평가와 본 연구를

통한 방법론의 모의시범평가한 결과를 평균값으로 나타낸 표이다.

국가정보원의 보안관리수준평가는 공공기관을 대상으로 만든 평가방법이기 때문에 공공기관의 특성에 맞는 질문들은 생략하고 결과 값을 산출하였다.

[표 3] 정보보호수준평가 모의 평가 비교

	보안관리수준평가 평가항목(산술값)	기업의 정보보호수준평가
평균 결과	93.04%	2.86(57.2%)

보안관리수준평가의 점검평가 항목의 결과를 평균값으로 나타냈더니 93.04%로 평가되었다. 정보보호수준평가는 가중치값을 적용된 성숙도값은 2.86단계로 나왔고 백분율로 나타내면 57.2%이다. 같은 기관을 대상으로 평가했고 평가 항목이 다른 점을 생각하여 비교했다. 그러나 약 35%이상의 차이가 나타냈다. 평가결과가 이렇게 도출된 큰 이유는 평가자의 잣대의 기준에 따라서 큰 차이를 나타나고 있다.

이 평가 결과는 기업의 정보보호수준평가가 보안관리수준평가보다 평가자의 이해를 돕고 명확하고 객관적인 측정을 할 수 있다는 것을 증명하는 것이다.

국가정보원의 보안관리수준평가는 각 평가항목에 대한 체크리스트로 작성되어 질문에 대한 수행여부만을 체크하고 있어 평가자의 의견에 따라 평가결과산출이 큰 격차를 보인다. 또한 가중치를 주는 부분도 역시 기준이 없어 평가자의 의견에 따라 달라지게 나타나고 있다. 만약 평가자가 평가질문에 대해 10%만 하고 있어도 수행했다고 평가하고 다른 평가자는 80%이상 수행하고 있다고 평가한다면 수행여부의 차이가 크게 달라지는 것을 볼 수 있다.

기업의 정보보호수준평가 방법론은 평가자의 의견에 따라 주관적으로 변할 수 있는 점들을 최소화하기 위해서 성숙도 단계평가를 실시하였다. 각 세부통제항목의 단계별 정의를 명확하게 정의함으로써 평가자의 이해도가 높아졌다. 또한 각 평가 단계별 평가 해설, 사례 및 증빙자료를 제시함으로써 각 항목의 범위에 대한 기준 잣대를 세분화하여 표현하였다.

4. 결 론

정보통신의 의존도가 심화되고 인터넷의 급성장으로 인하여 해킹·웜·바이러스 등과 같은 취약점에 대한 보안위협이 증가하고 있다. 이러한 위협은 국익을 좌우하는 정보에 대한 유출·손실, 불건전 정보의 유통 등과 같은 피해가 증가함으로 국가의 경쟁력을 약화시키고 있다. 이러한 위협들로부터 피해를 축소하기 위해 기업에서는 자신의 올바른 보안수준 측정이 이루어지고 이에 따른 대처방안을 모색해야 한다.

관련연구에서 국내외 정보보호수준 평가의 사례들을 살펴보았고 평가사례들의 장·단점을 분석하여 기업의 정보보호수준을 평가하기 위한 모델을 선택하였다.

본 연구는 주요정보통신기반시설의 정보보호수준평가의 모델을 택하여 기업의 정보보호수준을 향상시키기 위한 가중치를 주는 방법을 도입 및 성숙도 단계 정의를 개선하고 단계별 해설, 사례 등을 통해 기업에서 정보보호에 대한 부담감은 줄이고 정보보호의 수준을 향상시킬 수 있는 방법을 모색하였다.

본 연구를 통한 방법론의 효과성을 분석결과를 통해 물리적/기술적/관리적 측면의 다양한 평가항목을 통해 정량적이고 정성적으로 평가할 수 있다. 또한 본 연구를 통해 측정된 평가방법은 기업의 정보보호 수준을 통한 보안대책을 수립 시 도움이 될 것이다.

향후 본 연구를 통해 정보보호수준 자가진단 방법론을 이용한 기업에서의 저인력, 고비용 등의 문제점을 해결할 수 있는 자가진단 도구 개발에 활용될 수 있다.

[참고문헌]

[1] www.nist.gov

[2] www.kisa.or.kr

[3] KISA. 2006 정보보호 실태조사. 2006

[4] KISA. 주요정보통신기반시설의 정보보호수준평가 방법론. 2005

[5] 국가정보안전센터. 국가사이버안전메뉴얼. 2005

[6] 신영선, 박진섭, 안소진, 유성훈, 이희성. 중소기업 정보보호 수준 측정에 관한 연구. 정보보호학회 충청지부. 2006