자동화 위험분석도구의 개발 및 적용과정을 통하여 분석한 국내 정보시스템 보안관리체계의 문제점

o
윤정원 신순자 이병만
한국전산원

Evaluation of Domestic IT Management Environment through the Development and Application of Automated Risk Analysis Tool

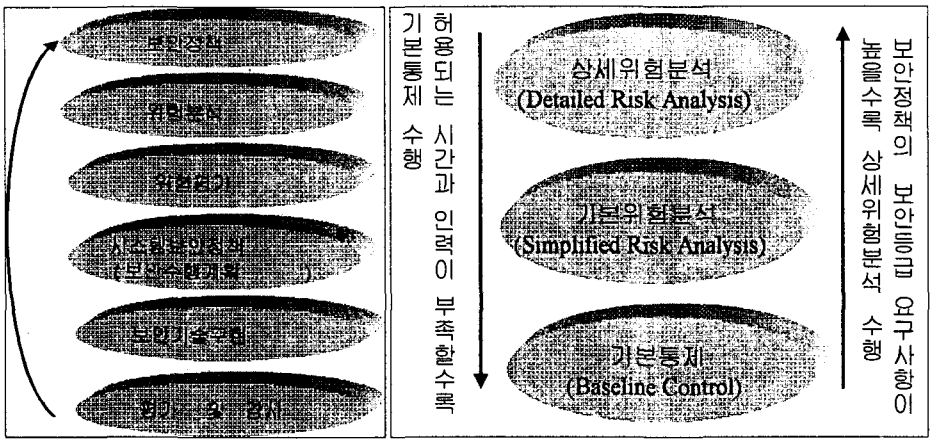
o
Jeongwon Yoon Soonja Shin Byung-Man Lee
National Computerization Agency

요약 : 국내에서도 정보시스템 보안관리가 체계화 되면서 보안컨설팅 분야가 중요한 분야로 대두되고 있다. 보안관리에서 핵심부문인 위험분석에 대한 연구는 진행되어 왔으나 국내환경에 적용하기 어려운 점이 많았다. 특히 정보시스템에 대한 분석기준과 정량화가 전무한 국내에서 외국산 위험분석도구등을 이용한 분석결과가 객관성을 갖기가 매우 어렵다. 따라서 위험분석 자동화 분석도구의 개발과 적용을 통하여 이러한 문제점을 고찰하고 국내 환경에서 위험분석을 실시할 수 있는 환경을 위하여 필요한 해결방안을 살펴보았다.

개요

본장에서는 위험분석의 개념과 국내의 현황을 간단히 살펴보고 국내환경에서 위험분석을 적용할 때 발생하는 문제점을 고찰해 보았다.

위험분석 : 위험분석은 보안관리 단계에서 반드시 필요한 과정이다(그림 1. 참조). 위험분석은 정보시스템 자산을 성질, 가치, 중요도 등에 따라 나누고 분석한 뒤 이에 대한 취약성을 조사하고 발생확률이 있는 위협의 피해를 분석하여 필요대응책을 산출하는 일련의 분석과정이다. 분석기준을 화폐가치에 두는 것을 정량분석이라고 하며 중요도나 판단가능한 상수로 위험도를 평가하는 것을 정성분석이라고 한다(표 1. 참조). 위험분석을 통하여 자산이 파악되고 위험수준이 산출되며 이에 근거하여 필요대응책을 추출할 수 있기 때문에 필요대응책에 대한 비용효과 분석을 가능하게 한다. 뿐만 아니라 "Compliance Evaluation"을 용이하게 해줌으로서 사고대응 및 보안수준의 지속적인 점검이 가능하다.



< 그림 1. 보안관리과정 및 위험분석 >

<table>
<tr><th>정량 분석(예)</th><th>정성 분석(예)</th></tr>
<tr><td>Quantitative Analysis : Simple Example

ALE = SI x Tf
SI = A x I

ALE : Annual Loss Expectancy Value
SI : Single Impact
Tf : Threat Frequency
A : Asset
I : Impact</td><td>Qualitative Analysis : Simple Example

<table>
<tr><th rowspan="2">A \ T</th><th colspan="3">화재</th><th colspan="3">해킹</th><th colspan="3">도난</th></tr>
<tr><th>상</th><th>중</th><th>하</th><th>상</th><th>중</th><th>하</th><th>상</th><th>중</th><th>하</th></tr>
<tr><td>O.S</td><td></td><td></td><td>V</td><td>V</td><td></td><td></td><td></td><td></td><td>V</td></tr>
<tr><td>서버</td><td>V</td><td></td><td></td><td></td><td>V</td><td></td><td></td><td>V</td><td></td></tr>
</table>
A : Asset
T : Threat</td></tr>
</table>

< 표 1. 정량분석 및 정성분석의 예 >

국내외 환경 : 외국에서는 오래전부터 위험분석을 수행하면서 보안관리 체계를 갖추어 왔다. 위험분석에 대한 모델과 기법이 개발되었으며 보안 컨설팅 산업이 활성화 되면서 전문인력이 많이 양성되었다. 관련 규정과 법령이 마련되면서 공공기관에 대한 위험분석이 의무화 되어 정보시스템 보안에 많은 영향을 미치고 있다. 미국의 경우 OMB A-130, Computer Security Act, DOD 5200 등이 제정되어 있고 영국의 경우 CRAMM이 의무화 되어 있다. 표준분야는 ISO/IEC JTC1 SC27의 GMITS(Guidelines of the Management of IT Security)에서 위험분석 분야를 국제표준으로 다루고 있고 미국 상무부 산하의 국립표준기술원(NIST)에서는 각 부처 및 공공기관을 위한 위험분석 프로세스의 표준(FIBS 65, 191 등)을

제정하여 미국 공공기관의 위험관리를 지원하고 있다. 관련 표준 및 규정과 자체적인 기법에 근거하여 위험분석 자동화 도구들이 보안컨설팅 업체들을 중심으로 개발되어 보안산업의 주요 분야를 이루고 있다. 그러나 국내의 경우 위험분석 관련 기법, 모델, 표준, 법규, 규정 등이 거의 전무하고 실무에 적용된 사례가 드물다. 뿐만 아니라 자산 평가와 위협 분야에 대한 과거자료 부족으로 정확한 위험분석을 하는것이 어렵다는 인식이 있어 왔다. 그러나 선진국에서는 이미 위험분석이 보안관리의 필수 프로세스로 인식되어 있기 때문에 국내의 IT 시장과 인력, 운영, 기술수준이 선진국 수준으로 갈수록 보안관리의 체계를 위하여 위험분석이 필요하게 될 것이다.

문제점 : 국내환경에서의 보안 위험분석 적용의 문제점은 그간 여러차례 언급되어 왔다. 물론 검증되지 않은 부분도 있고 실질적으로 위험분석을 지속적으로 적용해 보지 않은 상태에서 문제점을 검증하기엔 어려운 점도 많았다. 무엇보다도 외산도구를 사용하여 분석한 위험분석의 결과가 타당한지를 평가하기위한 기준조차 없기 때문에 막연히 위험분석 프로세스에 대한 문제점을 거론하는 경우도 많았다. 지금까지 대두된 문제점을 종합해 보면 아래와 같다.

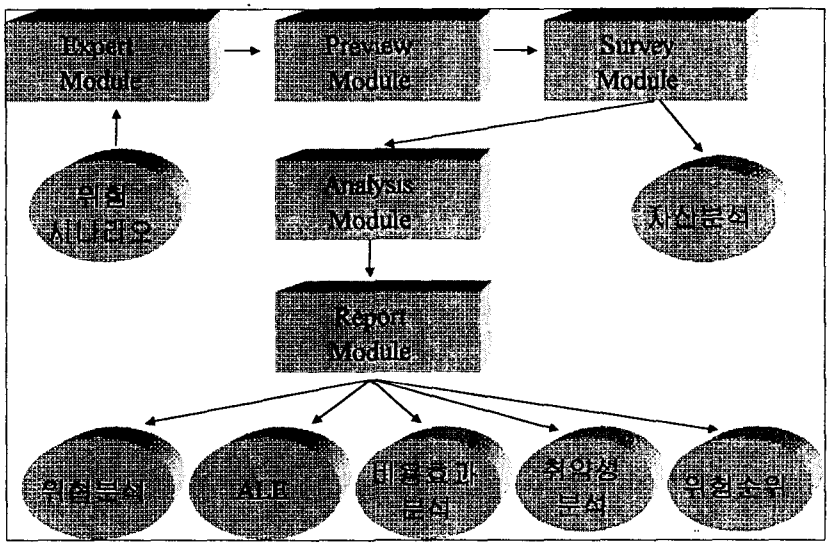
기술 및 인력 문제	o 위험분석에 대한 기술 및 인력 부족 o IT 보안관리의 체계 부재 o 정보 시스템 보안 전담부서의 인력 구성 문제 o 정보자산 가치 산정의 어려움 o 위협에 대한 과거자료의 부족 o 정성분석 등을 위한 객관적 기준 부재 o 위험분석 모델 및 기법 부재
법규, 규정 문제	o 관련 법규, 규정 부재
표준 문제	o 표준 부재
인식 문제	o 위험분석에 대한 인식 부족

< 표 2. 국내환경에서 위험분석 적용의 문제점 >

Buddy System의 적용과 HAWK(Hankuk risk Analysis Watch-out Kit)의 시험

HAWK 개발 : HAWK는 한국전산원 표준본부 보안기술표준팀에서 1996년도 상반기에 개발에 착수하여 1997년도 하반기에 개발을 끝냈다. HAWK는 그간 외국 위험분석도구의 분

석과 적용을 통하여 파악된 문제점을 개선하여 국내환경에 적용하기에 알맞도록 설계된 위험 분석도구이다. 전반적인 구조를 살펴보면,



< 그림 2. HAWK의 위험분석 구조 및 기능 >

HAWK의 위험분석은 5가지 기본모듈을 통하여 이루어 진다. Expert 모듈은 위험분석 전문가로 하여금 위험 관련 시나리오의 입력을 가능케 한다. 자산종류, 위협, 취약성, 대응책 등을 분류된 기준에 따라 입력하거나 이미 입력된 데이터를 바탕으로 위험시나리오의 맵핑이 허용된다. Preview 모듈에서는 조직의 정보시스템 자산에 대한 사전 분석을 하며 이 단계를 통하여 위험분석 모듈 및 질문 모듈을 조직의 정보시스템 환경에 맞추어 조정해 준다. Survey 모듈에서는 사용자가 위협주기, 실시 대응책, 자산가치 등 필요한 정보를 입력하게 된다. 분석모듈에서는 이들 데이터를 바탕으로 그림 2.에서 나타난 바와 같이 여러분야에 걸쳐 분석된 결과를 산출해 낸다.

Buddy System의 적용과 HAWK의 시험 : 표 3.은 HAWK의 기능과 미국 Countermeasure 사의 Buddy System의 기능을 비교한 것이다. Buddy System은 한국전산원에서 95년도에 구입하여 8개기관에 적용하여 위험분석 결과를 산출하였으며 HAWK 시스템은 97년도 9월에 개발이 완료되어 시험적용 단계를 거치고 있다. HAWK 개발의 목적은 앞서 언급한 바와 같이 "기법의 부재", "외국 위험분석 소프트웨어의 분석 제공 결과 및 분석 환경구성을 국내 환경에 적용하기에 어려운 점" 등을 해결하고자 한것이었다. 그러나 국내 환경에서 위험분석을 실시하기 어려운점이 자동화 분석도구나 위험분석 기법의 부재 등에만 국한된 것이 아님을 발견하였다. 위험분석 도구(Buddy System이나 HAWK의 경우)의 기능을 평가받기 이전에 위험분석을 실시하기 위하여 필요한 조직의 구성, 보안담당 인력의 역할 분담, 예산확보, 위험관리에 대한 인식, 과거 보안관리자료의 관리 등이 제대로 이루어지고 있지 않은부문이 국내 환경에서 위험분석을 적용하기 어려운 문제점들로 발견되었다.

HAWK		*Buddy System(미국)*	
주요기능	*평가*	*주요기능*	*평가*
○ 정보자산 조사 기능 ※ 환경사전조사 기능을 통하여 조직의 환경에 맞는 위험분석 질문 모듈 구성	상	○ 정보자산 조사 기능 ※ 정보자산이 세부적인 트리구조로 입력되어 있음	상
○ 취약성 분석 기능 ※ 각 자산의 취약성을 사용자가 입력한 자료를 바탕으로 분석하여 점수산출	상	○ 취약성 분석 기능	상
○ ALE 산출 기능 ※ 각 자산가치와 위협발생시 피해등을 고려하여 연간 발생할 확률상의 피해액을 산출하는 기능	하	○ ALE 산출 기능	하
○ 비용효과 분석 기능 ※ 취약성을 감소시키기 위해 필요한 대응책의 비용과 효과를 비교하여 저비용, 고효율의 대응책을 선별하는 기능	하	○ 비용효과 분석 기능	중
○ 기본대응책(250종) DB ※ 기본적으로 공급되는 대응책. 필요시 사용자가 추가할 수 있음	하	○ 기본대응책(300종) DB ※ 참고로 영국의 CRAMM은 3천여개의 대응책 제공	하
○ 사용의 간편도	상	○ 사용의 간편도	상
○ 위험분석 데이터 베이스 ※ 위험분석에 사용되는 항목(자산, 대응책, 취약성,위협)들의 입력과 이들간의 관계정의	하	○ 위험분석 데이터 베이스	중
○ 다중 시스템 분석 기능 ※ 각 시스템 별로 산출된 분석결과를 통합하여 조직전체의 위험수준을 산출하는 기능	없음	○ 다중 시스템 분석 기능	하
○ 분석기법에 대한 신뢰도 - 시험적용 필요	검증필요	○ 분석기법에 대한 신뢰도 - 미 연방정부를 포함한 20여개 이상의 공공기관에서 사용	상
○ 사용도 - 보급방안 수립 중	해당안됨	○ 사용도 -전세계에서 활용(미국,이태리,일본등)	상
○ 적용분야 - 일반 보안관리(O) - 운영 감리(O) - 개발 감리(X)		○ 적용분야 - 일반 보안관리(O) - 운영 감리(O) - 개발 감리(X)	
○ 특성 - 공공기관에서 개발(비영리) - 국내최초(한글화, 위험분석기본기능) - NCA 개발 표준과 연계가능		○ 특성 - 민간기업에서 개발 - 미 연방정부 정보보안관리규정 만족 - 가격(US $10,000)	

< 표 3. HAWK와 Buddy System의 비교분석 >

물론 HAWK의 개발을 통하여 외국 위험분석 도구의 문제점을 보완하고 국내환경에 맞는 분석 결과를 산출할 수는 있지만 위험분석을 적용하고 분석결과를 활용하기 위한 환경의 조성은 국내 보안관리체계의 문제점을 보완해야만 가능함을 알 수 있었다.

HAWK 등 국산 자동화 위험분석도구의 개발/적용을 통하여 해결될 수 있는 위험분석 적용의 문제점	*보안관리체계의 문제점으로 인해 발생되는 위험분석 적용의 문제점*
ㅇ 외국 위험분석 소프트웨어 사용의 어려움 ㅇ 자동화 분석도구를 사용한 분석 결과 이해의 어려움 ㅇ 분석도구를 다양한 전산환경에 대하여 적용시키기 어려움 ㅇ 정보시스템 환경변화 적용의 어려움 ㅇ 위험분석 방법론의 개발 및 발전 ㅇ 전자정보(Electric Data) 정량화 작업의 어려움 ㅇ 전문가보다 일반사용자(주로 보안담당자) 위주의 위험분석 소프트웨어 개발의 필요	ㅇ 질문 내용에 대한 부정확한 자료 입력 및 불충분한 자료 ㅇ 위험분석을 시행할만한 인력의 부족 ㅇ 위험분석 후 사후 대책 시행 능력의 부족 ㅇ 자산가치 산정기준의 부족 ㅇ 위협분석 시 필요한 과거자료의 부족 ㅇ 보안정책의 실용성 부족

< 표 4. 위험분석의 문제점 비교 >

상기의 문제점은 HAWK가 산출한 위험분석 결과에 대한 정확도를 평가하기 이전에 조직, 인력, 예산 등에서 발생하는데서 오는 것임을 알 수 있었다. 이러한 문제는 국내의 보안관리 체계가 선진국과 같은 형태를 이루지 않고 있기 때문이다. 특히 위험분석시 발생하는 문제점의 대부분이 데이터 입력시에 발생하고 있었으며 이러한 문제는 보안관리 체계의 문제점에 의한 것임을 더욱 확증시켜 주었다. 문제점을 자세히 분석해 보면,

ㅇ 질문 내용에 대한 부정확한 자료 입력 및 불충분한 자료
ㅇ 위협분석시 필요한 과거자료의 부족

자산파악의 부족과 위협, 장애발생, 사고대응 등에 대한 과거자료와 기록의 부족으로 정확한 자료 입력이 곤란한 경우가 많이 발생하였다. 이는 위험관리 기준에 따라 자산관리를 상세히 하고있지 않기 때문이며 사고대응체계(Incident Reponse)가 제대로 갖추어져 있지 않아 보안사고나 장애 발생시 사고대응 및 원인 분석이 제대로 이루어지고 있지 않기 때문이다. 뿐만 아니라 분석을 위한 각 질문에 대한 입력 자료에 대하여 검증 기능의 부족이 우려되었다. 입력자료에 대한 검증기능의 부족 가능성은 위험분석을 실시할 경우 위험분석 대상인력과 검증하는 인력이 대부분 동일인이기 때문이며 이들이 또한 보안책임자와 시스템 관리자의 임무를 겸하고 있는 경우가 대부분이기 때문에 위험분석을 실무에 적용할 경우 발생할 확률이 매우 높다. 이러한 문제는 위험분석 담당 인력의 부족의 문제와도 연계가 될 뿐만 아니라 보안조직의 구성이 역할 중심으로 이루어져 있지 않고 있기 때문이다.

ㅇ 위험분석을 시행할만한 인력의 부족

위험분석은 보안분야 뿐만아니라 정보시스템 감리분야에서도 적용되는 부문이기 때문에 이들분야에서 많은 경험을 쌓은 전문인력의 경험과 기술을 요구한다. 그러나 이분야의 전문인력이 부족한 관계로 분석한 결과에 대한 해석조차도 어려움을 겪는 경우가 많이 있다.

ㅇ 위험분석 후 사후 대책 시행 능력의 부족

HAWK는 위험분석 결과를 알기 쉽게 구성하여 보안담당자들이 실무에 활용하도록 디자인되었다. 그러나 문제는 분석결과가 알기쉽게 산출되어도 결과에 대한 활용이 이루어지지 않을 가능성이 높았다. 분석결과에서 제안하는 필요대응책의 구현이 예산을 많이 요구하는 경우에 보안책임자의 권한이 이를 수행할 능력이 없을 가능성이 많고 구현을 할 수 있다 하더라도 소위 "Compliance Evaluation"이 이루어지지 않을 확률이 높았다. 위험분석은 1회성 보안 진단이 아니라 지속적인 분석과 검증이 반복되어야만 효과가 이루어질 수 있음에도 불구하고 보안정책과 보안조직의 구조, 예산, 보안관리체계 등이 효과적으로 구성되어 있지 않음으로 인하여 분석결과가 사장되는 경우가 있었다.

ㅇ 자산가치 산정기준의 부족

정보시스템 자산은 일반자산과 달리 무형자산이 많고 자산의 성질이 "Volatile"하기 때문에 가치 산정이 매우 어렵다. 이에 대한 가치산정 방법이나 기준이 국내에 마련되어 있지 않아 정량분석의 경우 정확도가 떨어지고 분석결과에 대한 신뢰도가 떨어지는 경우가 발생하였다. 이는 이 분야에 대한 국내 표준이 없기 때문으로도 볼 수 있다.

국내환경에 적합한 위험분석 환경의 구성

앞서 국내 정보시스템 환경에서 위험분석을 적용하는데 발생할 수 있는 문제점과 외국 위험분석 도구를 국내에서 적용했을 경우 발생하였던 문제점들을 기술하였다. 이러한 점을 해결하기 위해 국내환경에 알맞는 자동화 위험분석 도구(HAWK)를 개발하여 적용해 보았다. 그러나 외국 위험분석 도구를 사용했을 경우 발생했던 문제점을 염두에 두고 HAWK를 개발하여 적용하였음에도 발생할 수 있는 근본적인 문제점들이 앞서 언급한 바와 같이 여러 가지가 있었다. 이러한 문제점들은 위험분석을 적용하기에 국내 정보시스템의 보안관리 체계에 많은 헛점이 있기 때문이며 이를 개선하기 위하여 아래와 같은 몇가지 해결책을 제안한다.

표준의 필요성 : 국내에는 정보보안관련 표준이 매우 부족하며 외국 보안관련 표준을 사실상 수용하는 부분이 많다. 그중에서도 IT 보안관리와 관련한 부문은 표준이 매우 부족하며 위험분석과 위험관리에 관한 표준은 거의 전무한 상태이다. 간단하게 지금까지 제정된 표준 현황을 살펴보면 아래와 같다.

KIS 6('93) : 전산망 보안관리를 위한 기술지원서(총론)
KIS 7('93) : 전산망 보안관리를 위한 기술지원서
(전산센터의 물리적 보안)
KIS 74('95) : 전산망 보안관리를 위한 위험관리 지침서

KIS 129('96) : 네트워크 보안관리 지침서
KIS 130('96) : 소프트웨어 보안관리 지침서
KIS 131('96) : 자료 보안관리 지침서
KIS 132('96) : 소프트웨어 개발 및 변경에 관한 보안관리 지침서

따라서 위험분석과 위험관리에 대한 표준이 빨리 제정되어야 한다. 참고로 ISO/IEC JTC1 WG1 SC27에서는 보안관리 및 정보시스템 관리분야에서 위험분석과 위험관리 표준의 제정이 거의 끝났으며 미국의 경우 NIST에서 기본적인 표준을 1979년에 이미 제정한 뒤 공공기관별 위험분석 프로세스에 대한 실무지침을 공급하고 있다. 따라서 국내에서도 국내실정에 맞는 표준의 제정이 시급하다.

표준으로 인한 파급효과 : 표준이 제정됨으로서 위험분석시 발생할 수 있는 각종 분석기법과 자산가치 산정, 연간기대손실치 산출 등 정량적인 데이터를 요구하는 부문에 기준을 부여해줌으로서 위험분석의 객관성을 높여줄 수 있다. 이는 현재 시장이 커지고 있는 보안컨설팅 분야에서 국내외 업체들이 위험분석의 기준을 국내표준에 둠으로서 분석결과에 대한 객관적인 평가와 신뢰를 높여주게 된다.

자동화 도구의 개발 및 기법 : 외국에서는 많은 위험분석 기법들이 민간기업이나 정부의 주도하에 개발되어 알맞은 분야와 환경에서 사용되고 있다. 국내에서도 우리실정에 맞는 위험분석 기법을 개발하여야 한다. 이는 앞서 언급한 표준과도 연관성이 있으나 표준은 가장 기본적이고 객관적인 흐름만 제공하는 반면 분석 기법은 기술과 노하우이므로 이를 이용하여 보안컨설팅 산업에 이용할 수 있다. 외국의 경우 대부분의 위험분석 기법이 자동화 도구로 개발되고 있기 때문에 민간기업 등에서 개발된 기법을 이용하여 자동화도구로 개발하여 보안컨설팅을 상품화 시켜야 한다.

보안정책의 실용성 부족 : 보안정책은 일련의 보호대책을 효과적으로 수행하기 위하여 목적을 부여하고 책임을 설정하는 경영진의 방침을 의미한다. 그러나 위험분석없이 보안기술의 적용중심으로 이루어진 국내 대다수 조직들의 보안관리는 보안정책에 많은 의미를 부여하고 있다. 그러나 보안정책이 세부 보안운영 방침을 일일이 설정할 수 없는 까닭에 보안정책과 실제 보안 대응책과의 연결이 제대로 이루어지고 있지 않고 있다. 따라서 보안정책을 일반 정보보안 정책과 위험분석결과에 바탕을 둔 세부 시스템 보안정책으로 나누어 시행함이 바람직하다고 생각된다.

인력 및 조직 : 보안조직의 구성은 인력 위주로 구성되기 보다는 역할 중심으로 구성되어야 하며 역할의 중복을 피해야 된다. 국내기관들의 보안조직 구성은 정해진 인력과 예산의 배당으로만 이루어져 있으며 각 구성인원의 고유권한과 기능이 정확히 고려되어 있지 않다. 이로 인한 문제점은 위험분석을 수행하였을 경우 인력, 자산관리, 장애관리, 사고대응, 감리, 시스템 운영 등의 모든 분야에서 나타날 수 있으므로 분석결과의 정확한 산출과 활용이 어렵다. 특정인에 대한 책임과 권한의 중복, 책임소재 불분명, 보안대응책 계획과 실시여부에 대한 관리부족 등이 실례에서 많이 나타났다. 따라서 최고 경영자가 포함된 보안 위원회를 바탕으로 기능과 역할 중심으로 보안조직을 구성해야 한다. 조직의 규모에 따라 "부문별 보

안 책임자"의 규모와 역할 등이 다를 수 있지만 아래와 같이 구성함이 바람직하다. 최고 경영자와 CIO가 보안위원회에 소속됨으로서 보안예산의 집행 등을 적절하게 수행할 수 있다.

보안위원회(Security Committee) 구성 인력

1) 최고 경영자
2) 조직 전체 보안 책임자
3) 정보시스템 관리 책임자(CIO)
4) 정보보안 책임자
5) 각 부문별 보안 책임자(조직의 규모와 예산에 따라 조정)
   - 암호 보안 담당
   - 감리 담당
   - 접근 통제 담당
   - 인력보안 담당
   - 건물보안 담당
   - 기타 필요 부문,...
5) 시스템 관리자
6) 프로젝트 관리자

관련제도 및 규정의 제정 : 외국과 마찬가지로 적정규모 이상의 조직과 공공기관은 위험분석을 자체적으로 실시하도록 권고하는 규정을 마련하여 보안관리를 국가적으로 체계화 시켜야 한다. 적정규모이상의 정보통신 관련 국가 프로젝트는 위험분석 실시를 의무화 하여 보안사고로 인한 손실을 최소화 하도록 제도적인 장치가 필요하다.

결론

보안관리의 핵심은 위험분석임으로 이를 국내환경에 적용하고자 그간 선진국에 비해 취약했던 이 분야를 위한 자동화 위험분석 도구를 개발하였다. 그간 적용해 보았던 Buddy System의 문제점을 보완하여 외국 위험분석 도구가 국내 환경에 적용하기 어려운점을 분석하여 HAWK 개발에 반영하였다. 따라서 기본적인 위험분석 기능의 구현은 이루었으나 국내 보안관리 체계가 위험분석을 수용하기에 어려운 몇가지 문제점을 발견하였다. 이는 위험분석을 적용하기 이전의 문제임으로 향후 국내에서 외국과 같이 보안관리와 관련한 컨설팅 산업이 활성화되고 위험관리가 본격적으로 적용된다면 몇가지 문제점을 일으킬 가능성이 있었다. 따라서 표준, 인력구성, 자동화도구 및 기법, 관련제도의 제정 등과 같은 몇가지 해결책을 거시적인 관점에서 제안하였다.

참고문헌

[1] 윤정원, 김홍근, 정성적 위험분석을 위한 버디시스템의 구조 분석, CISC'95, 1995
[2] 윤정원, 이병만, 보안사고 대응기능과 위험분석의 역할, 전산망 표준화 심포지움, 1996
[3] 윤정원, 신순자, 이병만, 송관호, 전산시스템 보안을 위한 자동화 위험분석 도구 (HAWK)의 개발에 관한 연구, CISC'96, 1996
[4] 윤정원, 이병만, 정보시스템 보안 위험분석 모델에 관한 연구, WISC'97, 1997
[5] 정보시스템 보안을 위한 위험분석 소프트웨어 개발 연구, 한국전산원, 1996
[6] 전산망 보안을 위한 위험분석 프로그램에 관한 연구, 한국전산원, 1995
[7] 전산망 보안을 위한 위험관리 지침서, 한국전산원, 1994
[8] Frederick G. Tompkins, HOw to Select a Risk Analysis Software Package, Datapro, McGraw-Hill, December, 1995
[9] Zenkins, Buddy, Security Analysis and Management Manual, Countermeasures Inc., 1994
[10] Guidelines for the Management of IT Security, ISO/IEC JTC1/SC27/WG1 N739 & N791, 1996