디지털산업정보학회 논문지 제6권 제4호-2010년 12월

전사적 정보보호 아키텍처에 근거한 금융 정보보호 모델 설계

김 동 수* · 전 남 재** · 김 희 완***

Design of Financial Information Security Model based on Enterprise Information Security Architecture

Kim, Dong Soo · Jun, Nam Jae · Kim, Hee Wan

〈Abstract〉

The majority of financial and general business organizations have had individual damage from hacking, worms, viruses, cyber attacks, internet fraud, technology and information leaks due to criminal damage. Therefore privacy has become an important issue in the community. This paper examines various elements of the information security management system and discuss about Information Security Management System Models by using the analysis of the financial statue and its level of information security assessment. These analyses were based on the Information Security Management System (ISMS) of Korea Information Security Agency, British's ISO27001, GMITS, ISO/IEC 17799/2005, and COBIT's information security architecture. This model will allow users to manage and secure information safely. Therefore, it is recommended for companies to use the security management plan to improve the companies' financial and information security and to prevent from any risk of exposing the companies' information.

Key Words : Information Security Management System, Information Security Architecture, Information Security Risk Management Plan, Security Service

Ⅰ. 서론

국내 IT(Information Technology) 시스템을 운영하는 금융권과 일반 기업대다수의 조직은 해킹, 웜, 바이러스, 사이버테러, 인터넷사기, 기술유출 등 정보 범죄로 인한 피해가 이제는 개인뿐 아니라 사회전체에 영향을 미치게 되었고, 정보보호가 사회의 중요한 이슈가 되었고 각종 보안 위협으로부터 정보 자산을 보호하여 사업의 지속성, 신뢰성, 안전성을 확보하기 위해 기술적, 물리적, 관리적 측면으로 보안정책 및 전략 등을 수립하여 적용하고 있다.

정보화 사업은 정보시스템에 대한 도입, 개발, 운영 및 유지보수를 중심으로 이루어지기 때문에 이러한 정보화 사업 전 과정을 통해 정보보호 측면에서 충분한 고려가 되어야만 시스템의 성공적인 개발은 물론 시스템 인수 이후에도 조직의 정보보호 관리를 보장할 수 있다[1].

* (주)키삭 대표컨설턴트(제1저자)
** 신한데이터시스템 SSC 과장
*** 삼육대학교 컴퓨터학부 교수(교신저자)

국내 정보보호 관리체계에서 많은 기업과 조직들이 다양한 규정 요구사항들을 충족시키기 위해 COBIT, ISO 27001, ITIL 등을 이용하고 있으며, IT운영과 비즈니스의 연계, 프로세스의 통제 등을 통한 보안성 및 신뢰성 향상에 많은 노력을 기울이고 있다. 현재 정보보호관리체계를 수립하고, 인증을 획득한 조직은 많지만, 대부분의 조직들이 정보보호관리체계 본원의 목적인 정보보호 관리 과정 및 통제를 통한 지속적인 개선보다는 형식상의 정보보호 노력을 기울이고 있으며, 정보보호를 일상적인 업무로 수행하지 않고, 단발적인 업무로 인식하는 경향이 있다. 또한 ISO27001 결과는 위험도 완화를 위한 보안대책 수립에 이용된다. 보안 대응책 마련 단계에서 자산을 보호하고 위험을 줄이기 위해 어떤 과정에 초점을 맞출 것인가를 결정하고 구현해야 한다. 위험도 평가나 위험도 완화 과정은 수많은 변수들을 포함하는 복잡한 절차이며, 전사적인 차원에서 위험도 평가와 완화 대책에 대해 체계적으로 접근이 필요하다.

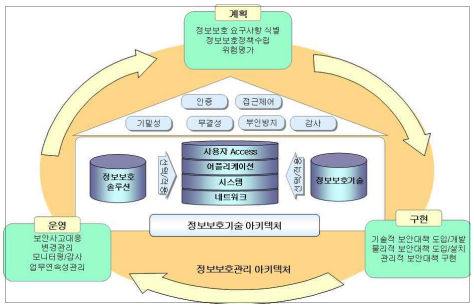
이에 본 연구에서는 기존의 정보보안관리체계로부터 금융권에 적합한 정보보호 현황 분석 및 수준평가 모델을 활용하는 것을 목표로 한국정보보호진흥원의 정보보호 관리체계(ISMS)[2], 정보보호아키텍처의 보안[3-4], 영국의 ISO27001[5], GMITS[6-10], ISO/IEC 17799/2005[11], COBIT 정보보호 아키텍처[12]를 참조하였다. 이를 통해 정보보호 활동의 안전한 보안시스템의 구축과 운영을 수행할 수 있도록 정보보호 위험관리 방안을 제시하였으며, 취약점에 대한 보완과 보안서비스에 대한 보호 대상별 현황 및 수준을 개선하여 금융권, 기업의 정보보호를 강화하는데 활용할 수 있는 방안을 제시하고자 한다.

Ⅱ. 관련 연구

2.1 전사적 정보보호 아키텍처(EISA)

EISA(Enterprise Information Security Architecture)[13]는 기술적, 관리적 정보보호의 통합으로, 크게 ISTA(Information Security Technology Architecture, 정보보호 기술 아키텍처)와 ISMA(Information Security Management Architecture, 정보보호 관리 아키텍처)로 구분된다. ISTA는 사용자 Access, 어플리케이션, 시스템, 네트워크 등과 관련된 아키텍처이며, ISMA는 P-D-S (Plan-Do-See) 사이클이라는 일반적인 관리과정에 기초하여 정보보호 통제수단을 계획, 구현, 운영하는 활동과 관련된 아키텍처이다.

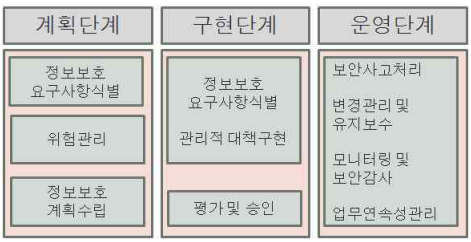
EISA는 <그림 1>과 같이 생명주기(계획, 개발, 적용, 유지보수, 통제)에 따라 지속적으로 관리되고 유지된다. EISA는 EA 생명주기 내에 포함되어 수행될 수 있으나, 위험이 높거나 중요정보가 많은 조직에서는 공식적인 과제로서 별도로 관리될 수도 있다. EISA 생명주기의 성공적인 실행을 위해서는 최고 경영층의 지원, 추진 조직의 구성, 철저한 계획 수립이 선행되어야 한다.



<그림 1> 전사적 정보보호 아키텍처

ISMA(Information Security Management Architecture)는 <그림 2>에서와 같이 조직 내 정보시스템의 위험수준을 파악하고, 이를 수용 가능한 수준으로 낮추기 위한 여러 가지의 대안과 제약조건을 고려하여 적절한 정보보호 대책을 선택하고 이를 구현 및 운영할 수 있도록 한다. 정보보호 절차 중 계획 단계에서는 조직의 정보보호를 효과적으로 수행하기 위해 대내외적인 정보보호 요구사항을 식별, 정보자산을 보호하기 위한 위험관리 수행, 조직의 정보보호를 체계적으로 수행하기 위한 정책 및 지

침을 수립하게 된다. 구현 단계에서는 계획 단계에서 선택된 정보보호 통제를 조직 내에 구현하기 위해 관리적, 기술적, 물리적 정보보호 대책을 수행하게 된다. 운영 단계에서는 기술적, 물리적, 관리적 보안 대책을 관리·운영하는 단계로 보안사고 처리, 유지보수 및 변경관리, 모니터링 및 보안 감사, 업무 연속성 관리 등이 수행된다.



<그림 2> 단계별 정보보호 관리절차

ISTA(Information Security Technology Architecture)는 시스템, 네트워크, 응용시스템, 최종 사용자, 저장·갱신·전송되는 데이터 등 정보기술 자원 전반을 포함하고 있으며 조직의 업무, 전략, 정책과의 연계성 등이 고려된다.

전사적 정보보호 아키텍처인 EISA[13]와 관련하여 다양한 관점과 이해의 차이가 존재하고 있기 때문에 아키텍처 도입 시 혼란과 시행착오가 일부 발생하고 있으며, 정보보호의 중요성이 강조되고 있는 현실에서 기업의 정보보호를 지속적이고 효과적으로 관리할 수 있는 모델을 제안하고자 한다.

2.2 GMITS

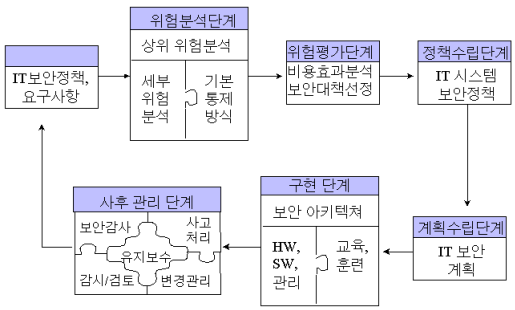
GMITS(Guidelines for the Management of IT Security, ISO/IEC TR1335-1)는 국제표준 ISO/IEC JTC SC27 WG1에서 발생한 기술 보고서(Technical Report) 13335에 명시된 내용으로 5개의 파트로 구성된 위험분석 방법론이며, 구성체계는 다음과 같다.

◦ Part 1: Concepts and models for IT Security(1996)

1부는 고위 경영층을 대상으로 정보기술 보안관리에 관한 기본적인 보안 개념과 모델, 과정을 소개하기 위한 목적으로 작성되었다[6].

◦ Part 2: Managing and planning IT Security(1997)

2부에서는 정보보안관리 기능 및 과정을 소개하고 있으며 정보보안 정책의 계층적 구조와 담당 조직의 역할을 기술하고, 조직 내에 비용 효과적인 정보보안을 구축하기 위해 정보보안계획수립을 강조하고 있으며, <그림 3>과 같이 정보보안관리 과정을 기술하고 있다[7].



<그림 3> GMITS 정보보안 관리과정

◦ Part 3: Techniques for the management of IT Security (1998)

3부에서는 2부에서 제시한 정보보안관리 과정에서 사용될 수 있는 구체적 기법 및 방법을 제시하여 주고 있다. 특히 정보보안관리 과정에서 중요한 위험관리와 위험분석에 대해 상세하게 기술하고 있다. 상세 위험분석 과정은 우선 보호 대상인 정보자산의 가치와 상호의존도를 파악하고 자산에 손해를 미칠 수 있는 위협의 유형을 파악하여 이의 강도와 빈도를 측정하는 위협분석을 수행하며 동시에 자산이 보유하고 있는 취약성을 평가하는 과정을 포함하고 있다[8].

◦ Part 4: Selection of safeguards(2000)

4부에서는 보안요구사항과 조직의 특정환경에 따라

보안대책을 어떻게 선정하는 과정을 기술하고 있으며 적절한 보호수준을 달성하기 위한 방법과 기본적 보안대책(baseline security)을 어떻게 적용할 수 있는가를 보여주고 있다[9].

◦ Part 5: Management guidance on network security (2001)

5부는 4부의 추가적인 문서 성격이 강하며, 인터넷과 같은 외부망과 연결하고자 하는 조직에 도움을 주기 위해 작성되었다. 즉 외부망과의 연결과 이로 인해 제공되는 서비스에 대한 보안대책의 제안, 선정 및 사용에 대한 지침을 제공하고 있다. 여기에서는 13가지 보안위험 시나리오와 8가지 외부망 접속유형에 기초하여 해당되는 보안대책을 제시하고 있다[10].

2.3 현행 정보보호 관리체계의 한계점

국내 글로벌 IT업체나 금융권들은 KISA-ISMS 및 ISO27001에 기반을 두고 시스템의 접근통제와 보안사고 관리 및 사업의 연속성 강화에 초점을 맞추어 정보보호 지표 관리체계를 운영하고 있다. 정보보호 관리시스템의 기존의 표준 및 모델들은 필요사항을 잘 정의하고 있으며 어느 조직에서도 적용 가능한 일반적이고 범용적인 특성을 가지고 있다. 그러나, 표준을 적용하기 위한 방법론 부족으로 정보보호관리체계 도입이 정책 및 문서(Policy and Document)가 작성되는 수준으로 한정되어 있으며, 구축된 정보보호관리시스템을 지속적으로 운영하기 위해 필요한 비용(인력현황, 소요시간, 예산반영) 및 정량적인 운영결과에 대한 분석이 미흡한 형편이다.

정보보호관리체계(ISO27001) 인증제도에서는 정보보호 현황진단 및 일반적인 감사기법을 활용하여 적용성 보고서(SOA : Statement of Application)를 작성한다. 또한 정보보호관리체계(ISO27001) 컨설팅을 통해서 통제항목을 중심으로 정보보호 현황진단을 실시하고 취약성 분석을 통해 계량화 된 보고서가 작성된다. 하지만, IT분야(기술적 보완) 및 위험(Risk)기반으로 제한되어 포괄적(물리적, 기술적, 관리적)이고 적극적(Proactive) 차원의 정보보호 활동과 정보보호 수준관리의 개념과 차이가 있으며, 정보보호 범죄의 지능화, 전문화, 다양화 등으로 정보를 안전하게 보호할 수 없게 되었다. 따라서 정보의 기밀성, 무결성, 가용성을 보장할 수 있도록 조직에 적합한 정보보호 정책을 수립하고 체계적인 정보보호관리체계를 구축, 운영할 필요가 있게 되었고, 금융권의 안전한 정보보안시스템의 구축과 운영을 위해서 기존에 구축된 정보보호관리체계를 활용방안과 효과적으로 이행하고 관리하기 위해서 지속적으로 정보보호 정책을 재검토하고 정기적으로 현황분석 및 위험평가를 실시하여 취약점에 대한 위험들을 제고 또는 완화시키는 일련의 위험관리(Risk Management)과정이 필요하다. 특히 보안 요구사항 및 평가방법은 관련 평가기준과 평가방법론에 개괄적으로만 서술하고는 있어 평가준비 및 평가를 수행하는데 일관성과 정확성 유지하는데 문제가 있다.

2.4 정보보호 관리체계의 개선방향

정보보안 정책 및 계획 또는 필요하다면 정보시스템의 각 영역별 보안 정책을 수립하여 정책을 근간으로 정보보안 시스템을 구현하기 위한 사업으로 전반적인 과정은 ISO/IEC 17799/2005[11] 와 ISO27001[5]의 정보보안 관리체계에서 요구하는 11개의 핵심통제, 그리고 정보보호아키텍처(EISA)의 요구에 대한 점검과 그에 해당하는 대응 방안을 정책과 계획에 수용하는 것으로 정책 수립을 위한 업무 현황분석, 위험분석, 기술과 제도분석 단계와 그를 바탕으로 정보보안 계획을 수립하는 것으로 각 단계를 설정하였다.

정보보호진흥원의 ISMS[2], GMITS[6-10], 정보보호 아키텍처(EISA)의 통제요건을 충족시키는 보안 프로세스 영역 및 하위 프로세스를 파악해 보면 <그림 4>와 같다.

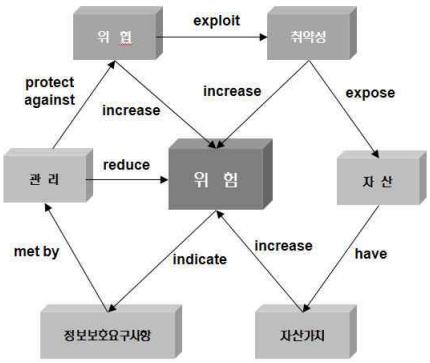
조직의 비즈니스 목표와 발전계획 그리고 그에 따른 정보시스템과 제어시스템의 확장계획 등을 고려하여 장

단기적인 조직의 보안정책과 보안계획을 수립하는 것을 목표로 한다. 보안정책과 계획은 시행결과의 평가와 보안환경의 변화 등을 고려하여 주기적으로 갱신되어야 한다. 업무현황분석, 위험분석, 정보보안계획 수립의 영역으로 구성된다. 이러한 정보보호 계획 수립 중 자산관련 위협, 취약점을 분석하여 위협간의 관계를 파악 후 위험수준을 관리해야 한다.

<그림 4> 정보보호 보안 프로세스 정의

위 정보보호 정책 및 절차 수립을 위해 정보보호업무를 수행하기 위한 정보보호 조직이 구성되어야 하며, 정보보호계획을 수립하여 조직의 정보보호 목표를 수립하고 구성인력의 역할 제시, 정보보호 업무를 수행할 수 있도록 해야 한다. 정보보호조직은 조직의 특성에 적합한 조직을 구성하도록 하며, 정보보호업무를 수행하는데 있어서 필요한 인력들로 구성되어야 한다. 정보보호계획은 정보보호 목표를 달성하기 위해 매년 수립되고 시행되어 구체적인 결과 검토를 통해 새로운 보안 위협 및 보안사고에 대응할 수 있도록 계획되어야 한다. 이를 위하여 필요시 각 조직은 정책 및 지침, 규정 등을 수립하여 운영한다. 또한 위험평가는 정보 및 정보시스템 등의 위험을 평가하기 위해서는 정보 및 정보시스템 등의 자산을 식별하기 위한 계획 및 절차가 수립되어 그 계획 및 절차에 따라 자산이 분류되고 분류된 자산의 중요도에 따라서 자산등급을 부여한다. 정보시스템 및 서비스를 도입할 경우 계획 및 절차에 대한 최소 보안 요구사항 및 취약성 검토가 이행되고 취약성 검토 시 취약성 진단 도구 및 기법을 사용하여 수행되어야 한다. 위험평가 및 취약성 진단 결과에 대한 검토가 이루어지고 위험평가와 관련된 계획 및 절차 개선되어 운영되어야 한다[14].

기존 연구의 문제점을 해결하기 위하여 성숙도 모델인 ISO27001[5] 및 COBIT 프레임워크[12] 등을 활용하여 보안관리체계에서 보안관리, 위험평가 요구사항 및 평가방법을 구체적, 세부적으로 제시한다. 위험평가는 자산분석 > 취약점진단 > 위험분석 > 위험조치계획서 단계로 추진하며, 이런 위험평가 개념 간 연관관계를 파악해 보면 아래<그림 5>와 같다.



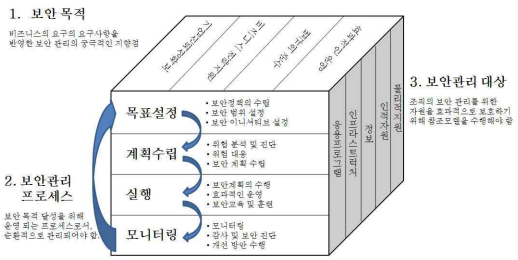
<그림 5> 위험평가 개념간 연관관계

Ⅲ. 금융 정보보호 모델

3.1 정보보호 관리 프레임워크

금융 비즈니스 환경의 다양한 변화 및 니즈(needs)를 수용하고 비즈니스의 연속성을 유지하기 위해서는 정보보안과 관련한 조직 내부의 다양한 이해관계자의 관심과 요구를 통합, 조정하기 위한 정보보호 관리 프레임워크 수립하고, 이를 기반으로 보안계획 수립, 실행, 모니터링(Plan-Do-See)을 통한 보안관리 활동을 실행하고 기술적 보안 조치를 적용해야 한다. 금융부문의 정보보안 프레임워크 <그림 6>은 COBIT[12] 및 한국정보보호진흥원의

정보보호 관리체계(ISMS)아키텍처 프레임워크[2]를 참조하여 보안목적, 보안관리 프로세스, 보안관리 대상 관점에서부터 보안모델을 제안한다.



<그림 6> 금융 정보보안 프레임워크

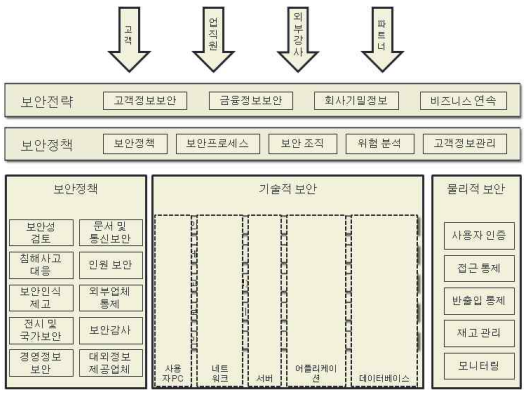
3.2 정보보호 모델의 구성

효과적인 정보보호를 위해서는 사용자 관점에서 영역(레이어)별 접근을 고려하여 보안 전략 및 보안정책을 수립하고, 보호대상에 대해 기술적 보안을 적절히 적용할 수 있도록 보안서비스 및 적용기술을 분류하여 보안 아키텍처를 구성할 필요가 있다. <그림 7>의 보안 아키텍처는 먼저 금융 정보시스템 사용자를 고객, 임직원, 외부감사, 파트너를 구분하고, 금융정보 및 고객정보, 회사기말사항, 비즈니스 연속성 유지를 위한 보안 전략을 수립하며, 보안 전략 이행을 위한 보안 정책을 마련, 이를 관리적, 기술적, 물리적 보안으로 구분하여 이행할 수 있도록 구성하고 있다.

<그림 7>에서 제시한 사례는 보안정책 수립시 금융회사의 중요한 자산인 고객정보를 별도 항목으로 분류하여 비즈니스 관점에서 고객정보의 수집에서부터 폐기까지 인력의 활동을 종합적으로 관리할 수 있도록 하였다.

고객정보관리를 위한 별도 조직을 구성하거나 사전·사후 보안성 검토 프로세스를 마련하여 금융회사간의 비즈니스 협력 확대에 따라 증가하고 있는 고객정보 유출과 관련 보안 위험리스크를 최소화 할 수 있다.

또한, 기술적 보안관리에 기밀성 보장을 위한 내부정보 유출방지 항목을 두어 회사 비즈니스 정보 및 고객정보 등의 유출 방지를 최소화 할 수 있는 보안기술 적용이 가능하도록 하였으며, 전자금융거래의 안정성 및 무결성 보장을 위해 접근통제항목을, 정보시스템 가용성 보장을 위해 침해사고 예방 항목을 각각 포함하였다.



<그림 7> 정보보안 아키텍처

3.3 정보보호 기술 구조 계층

정보시스템 보호 대상 매체를 <표 1>과 같이 사용자 PC, 네트워크, 서버, 어플리케이션, 데이터베이스 계층으로 분류 정의하고 보안서비스 및 적용기술에 따라 계층별 구성이 가능하도록 하였다.

<표 1> 보호대상 분류 및 정의

계층	보호대상	내용 요약
제1계층	사용자 PC	조직이 업무를 수행하기 위하여 내부 네트워크에 연결된 단말기를 지칭
제2계층	네트워크	업무시스템을 운영할 환경을 구성하는 네트워크로 내부망 및 대외망을 포함
제3계층	서버	업무시스템을 운영할 환경을 구성하는 하드웨어로 메인프레임 및 오픈서버를 통칭
제4계층	어플리케이션	조직의 업무목표를 운영, 지원하기 위한 업무정보를 조작/관리하는 업무 기능, 프로세스, 활동
제5계층	데이터베이스	조직의 업무운영에 필요한 모든 정보와 이들 정보간의 관계

3.4 정보보호 보안 서비스 분류

금융회사의 업무특성을 고려하여, 정보 유출방지 및 침해사고 예방에 주안점을 두어 아래<표 2>의 보안 서비스를 분류하였다.

<표 2> 보안기능 서비스 분류

보안 서비스	내용
인증/부인 방지	시스템 기능이나 자원에 대한 접근을 통제하기 위해 사용자(또는 시스템)의 신원을 확인하고 허가 받은 객체로 위장하려는 시도를 막기 위해 사용됨
접근통제 (무결성)	정보자산에 대한 무결성 보장을 위해 내외부자로부터 임의 접근 및 변경을 제한하고, 데이터에 대한 정합성을 보장하는 보안서비스
침해예방 (가용성)	비즈니스 연속성 보장을 위해 침해사고 예방 및 정보시스템 가용성을 보장하는 서비스
내부정보	데이터 대한 기밀성 확보 및 회사의 자산 보호와 정보
유출방지 (기밀성)	유출 방지 요구를 충족시키기 위해 비즈니스 정보에 대한 보호와 기업의 저작권 관리를 이한 보안서비스
모니터링	정보보호 서비스가 적절하게 적용되고 관리되는 것을 모니터링 하는 서비스로 이벤트가 발생한 후 기록을 검색하고 해석할 수 있는 방법과 접근 시간 등에 자세한 기록을 발생시키는 기능들과 결합되며, 실제 사고의 발생시간에 적절한 대응뿐만 아니라 책임 여부를 판별할 수 있는 중요한 보안 서비스

3.5 정보보호 적용기술

보호대상에 따라 적용해야 할 세부보안 적용기술을 <표 3>의 보안서비스별로 구분하여 분류하고, 보안 기술의 발전 및 최근 이슈에 따라 대응 기술을 추가·삭제할 수 있다. 기밀성, 가용성, 무결성 보장을 위한 최신 보안 기술을 조사 분류하였으며, 정보시스템의 무결성 및 안정성 보장, 침해사고 예방, 내부정보 유출방지 관점에서의 적용기술 위주로 작성하였다.

<표 4> 보안 적용기술 분류

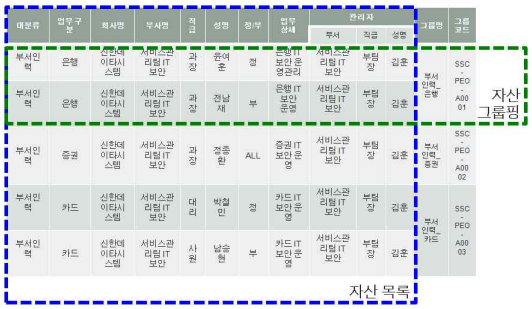
분류	제1계층 (사용자PC)	제2계층 (네트워크)	제3계층 (서버)	제4계층 (어플리케이션)	제5계층 (DB)
인증/부인 방지	사용자인증	사용자인증 장치인증 무선랜인증	사용자인증, 서버계정관리	사용자인증계정/권한관리 PKI	사용자 인증
접근통제 (무결성)	개인방화벽	침입차단 NAC	서버접근로그 모니터링 Secure OS RACF	EAM 웹어플리케이션 방화벽 온라인방화벽 키보드보안 위변조방지 피싱방지	DB 권한 관리
침해사고 예방 (가용성)	보안패치 보안설정진단 백신 악성코드방지	취약점 검 헬스체크 보안패치 IDS/IPS DDoS방지	취약점 검 헬스체크 보안패치 백신/악성코드방지	취약점 점검 스팸메일차단	취약점 점검 헬스 체크
내부정보	파일암호 USB메모리제어	VPN 무선랜 보안 Email통제	HSM 백업/복구 DRM	데이터암호 메일암호화 (보안메일)	DB 암호화
유출방지 (기밀성)	DRM	유해트래픽통제 웹하드통제			
모니터링	불법SW 통제	ESM	SIM	포렌식툴 보안개발방법론	로그 분석
인증/부인 방지	사용자인증	사용자인증 장치인증 무선랜인증	사용자인증 서버계정관리	사용자인증계정/권한관리 PKI	사용자 인증

Ⅳ. 모델의 적용 및 검증

4.1 정보보호 모델의 적용

금융권은 IT서비스 품질향상, 비용절감, IT인력 효율적 운영을 위해 IT인프라를 금융지주 계열사로 개편하고 있으며, 이로 인하여 정보보호 관리체계 등 그룹사 자산의 중요도 및 위협·취약점에 대한 평가를 통하여 자산에 발생 가능한 위험수준을 파악하고, 이에 대한 보안통제를 적용함으로써 자산의 위험수준을 확인하고 있다. 본 논문에 정의된 정보보호 모델은 S그룹사의 운영관리에 적용하여 검증하였다. 위험관리는 ISO27001에서 제시하고 있는 보안 점검 항목들을 토대로 각각 문제 요소들을 개선하기 위한 절차이며, 적용범위는 그룹사 자산 목록 중 문서, 소프트웨어, 물리적 자산, IT인력으로 구분하였으며, 자산의 유사도, 중요도를 고려하여 <그림 8>과 같이 자산목록 작성 및 자산 그룹핑(Grouping)을 하였다.

위험평가는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 측면에서 외부 유출, 변조, 사용 불



<그림 8> 자산목록 작성 및 그룹핑

가 시의 업무 영향도를 평가하고, 관련 위협·취약성의 발생 가능성을 평가하였고, 위험산정 방식은 아래 <표 5, 6>예시와 같으며, 위험분석을 통하여 도출된 위험들 중에서 '관리되어야 할 위험' 을 도출하기 위한 임계치(Degree of Assurance)을 설정하였다.

<표 5> 위험분석 통합 Sheet

자산구분	보호 대상			자산중요도 평가		
				C	I	A
문서	S은행_전자문서_공통프로세스			1	3	1
자산 구분	Concern			위험값		
	상세	Value	Threating	C	I	A
문서	캐비닛 보관 미실시 등 관리 미흡으로 인가 받지 않은 자의 문서 유출, 도난 가능성	1	C, A	5	7	5

위험도(Risk Value) = 자산가치 + (위험취약성의 정도×2)

<표 5>에서 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)에서의 위험도는 (5, 7, 5) 이며, '관리되어야 할 위험'은 기밀성(C)과 가용성(A)을 나타낸다.

DoA(Degree of Assurance)는 위험분석 결과 '관리되어야 할 위험'(Unacceptable Risk)과 '수용 가능한 위험'(Acceptable Risk)을 구분한다.

또한, 판단 기준으로 관리되어야 할 위험(High Risk) 도출은 아래 <표 7>과 같이 위험도가 '7'이상인 경우에

<표 6> 위험분석 방식

위험/취약성 수준		1(Low) X 2	2(Medium) X 2	3(High) X 2
자산가치	1(Low)	3	5	7
	2(Medium)	4	6	8
	3(High)	5	7	9

해당된다. 또한 '관리해야 할 위험'(Unacceptable Risk)에 대해서는 ISO27001 보안통제를 적용하여 위험을 감소 또는 제거 설정을 하였다.

<표 7> 위험도출

위험/취약성 수준		1(Low) X 2	2(Medium) X 2	3(High) X 2
자산가치	1(Low)	3	5	7
	2(Medium)	4	6	8
	3(High)	5	7	9

아래 <표 8>은 S그룹사의 중요도 위험평가 결과에 따라 산출된 위험 값(Risk Value) 중 High Risk 도출하여 위험분석 결과에 대한 통계를 도출하였다.

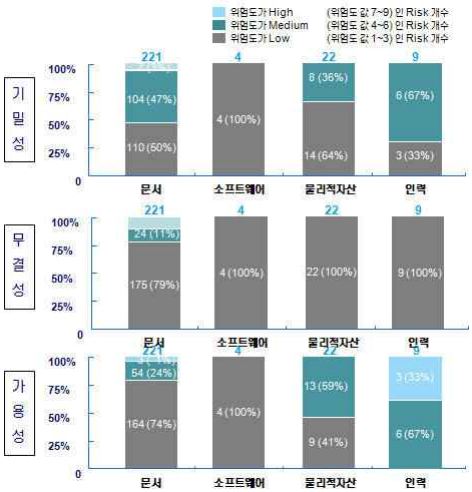
<표 8> 위험평가 통계

구분	기밀성			무결성			가용성		
	L	M	H	L	M	H	L	M	H
문서	110	104	7	175	24	22	164	54	3
	50%	47%	3%	79%	11%	10%	74%	24%	1%
소프트웨어	4	0	0	4	0	0	4	0	0
	100	0%	0%	100	0%	0%	100	0%	0%
물리적 자산	14	8	0	22	0	0	9	13	0
	64%	36%	0%	100	0%	0%	41%	59%	0%
인력	3	6	0	9	0	0	0	6	3
	33%	67%	0%	100	0%	0%	0%	67%	33%

위험분석 결과 아래 <표 8>과 같이 문서, 소프트웨어, 물리적 자산, 인력부분에서 문서의 기밀성, 무결성, 가용성 측면과 인력 가용성 측면의 위험이 높게 평가 되었다.

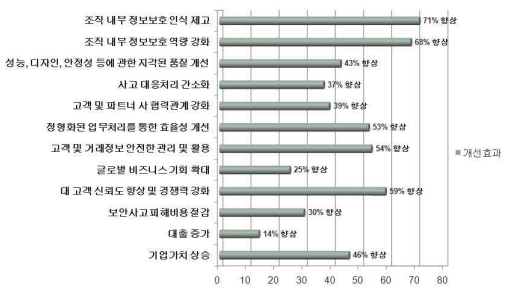
<그림 9>와 같이 정보보호 모형에서 위험관리는

ISO27001에서 제시하는 보안 점검 항목 들을 토대로 적용하며, 각 분석 결과를 토대로 위험수준을 확인 할 수 있었고 통제항목에 대한 위험 조치계획서를 수립하여 지속적으로 관리할 수 있다.



<그림 9> 위험분석 결과

4.2 정보보호 모델 적용 효과



<그림 10> ISMS 구축에 따른 개선효과

제안한 정보보호 관리체계를 통한 효과를 <그림 10>에서와 같이 조직 내부 정보보호 인식제고가 약 71%로 가장 높은 효과를 나타냈고, 다음으로 조직 내부 정보보호 역량 강화(68%), 대 고객 신뢰도 향상 및 경쟁력 강화(59%) 순으로 나타났다. 반면, 매출 증가(14%), 글로벌 비즈니스 기회 확대 효과(25%)는 상대적으로 미비한 것으로 나타났다.

4.3 금융기관 활용 시 고려사항

정보보호의 주요 요소인 기밀성, 무결성, 가용성에 대하여 모두 중요하지만 금융기관 업무 특성을 고려해 볼 때 무결성, 가용성, 기밀성 순으로 우선순위를 정해야 한다. 물론 이것은 상대적 우선순위로 가중치의 차이 또는 금융기관별로 다를 수 있다. 또한 자산별, 유형별로 취약성의 수준을 평가하고 수치화시킬 수 있는 객관적인 기준이 없어, 경우에 따라서 특정 취약성이 부각될 수 있으나 특정 취약성은 무시될 수 있다. 이와 같이 객관적 기준이 마련되지 않을 경우에 식별된 각 취약성을 자산이 가지는 위험도에 반영함에 있어, 취약성의 유형에 따라 자산에 미치는 영향도 및 평가 결과가 평가자의 주관에 크게 의존하게 된다.

정보보호를 위해서는 사용자 관점에서 영역별 접근을 고려하여 보안 전략 및 보안정책을 수립하고, 보호대상에 대해 기술적 보안을 적절히 적용할 수 있도록 보안서비스 및 적용기술을 분류하여 구성할 필요가 있다.

5. 결론 및 향후 과제

본 논문에서는 금융권 및 기업에서 겪고 있는 다양한 형태의 보안사고 위험을 줄이기 위한 측정 도구로써, 객관적이고 실질적으로 적용할 수 있는 정보보호 관리기준 모델을 정립하였다.

정보보호관리체계는 정보보호 목표를 달성하기 위해 매년 수립되고 시행되어 구체적인 결과 검토를 통해 새로운 보안 위협 및 보안사고에 대응할 수 있도록 계획되어야 한다. 이를 위하여 필요시 각 조직은 정책 및 지침, 규정 등을 수립하여 운영한다. 또한 위험평가는 정보 및 정보시스템 등의 위험을 평가하기 위해서는 정보 및 정보시스템 등의 자산을 식별하기 위한 계획 및 절차가 수립되어 그 계획 및 절차에 따라 자산이 분류되고 분류된

자산의 중요도에 따라서 자산등급을 부여한다. 정보보호 관리체계의 평가 모델을 바탕으로 측정모델을 설계한 후 모형 검증 등을 통하여 범용적으로 활용할 수 있도록 제시하였으며, 소개된 측정모델 역시 부분적인 한계점을 지니고 있기 때문에 보다 실용적이고 합리적인 모델로 발전하기 위해서는 지속적인 활용과 함께 보완작업을 거쳐야 한다고 본다.

결과적으로 금융기관 정보보호관리체계 인증 과정에서 위험관리의 위험분석 과정을 금융기관 업무 특성을 고려하여 위험 분석을 보안성 평가 사례로 도출하였으나, 완벽하다는 할 수 없지만 금융권 정보보호 아키텍처 구성요소를 참고하여 위험 관리 표준화 방법론을 연구한다면 금융기관에 기본적인 정보보안관리체계 구축 절차나 분석기법 등에 대한 확보기회와 전환점이 될 것이다.

향후과제로는 본 연구의 결과를 금융기관의 도출과정에서 보다 논리적이고 체계적인 방법론과 사례가 제시되어야 하며, 실제 적용하여 유용성을 검증하고 장단점을 도출하여 지속적인 유지 및 보완작업을 통하여 보다 실용적이고 정교한 정보보호관리체계로의 발전이 기대된다.

참고문헌

[1] 이지용 · 김동수 · 김희완, “정보시스템 감리에서의 정보보호 감리모형 설계,” 디지털산업정보학회논문지, 제6권, 제2호, 2010, pp. 233-245.

[2] 한국정보보호진흥원, 정보보호 거버넌스 개념 도입을 위한 정보보호 관리체계(ISMS) 발전 방안 연구, 2009.

[3] 한국정보사회진흥원, 공공부문 정보보호 아키텍처 구성 방안 연구, 2004.

[4] 한국정보사회진흥원, 정보시스템 보안/통제 감리 지침 연구, 1998.

[5] ISO/IEC 27001, International standard - Information technology - Security techniques - Information security management systems – Requirements, 2005.

[6] ISO, ISO/IEC TR 13335-1, Information technology - Guidelines for the management of IT Security - Part1 : Concepts and models for IT Security, 1996

[7] ISO, ISO/IEC TR 13335-1, Information technology - Guidelines for the management of IT Security - Part2 : Managing and planning IT Security, 1997

[8] ISO, ISO/IEC TR 13335-1, Information technology - Guidelines for the management of IT Security - Part3 : Techniques for the management of IT Security, 1998.

[9] ISO, ISO/IEC TR 13335-1, Information technology - Guidelines for the management of IT Security - Part4 : Selection of safeguards, 2000

[10] ISO, ISO/IEC TR 13335-1, Information technology - Guidelines for the management of IT Security - Part5 : Management guidance on network security, 2001

[11] ISO, ISO/IEC 27001:(FDS) Information Security Management System Requirements, 2005.

[12] ISACA Korea chapter, CoBIT 4.0 한글판, 2006.

[13] 한국정보사회진흥원, 전사적 아키텍처 프레임웍 실무지침 - 포괄적 개념중심, 2004.

[14] 정보통신연구진흥원, 정보보호 수준 평가 적정화 방안 연구, 2008.

■ 저자소개 ■

김 동 수
Kim, Dong Soo

1981 광운대학교 전자계산학과 이학사.
2001 서울산업대학교 전자계산학과 공학석사.
2005 국민대학교 경영정보학과 경영학박사
전자계산기조직응용기술사,
정보통신기술사, 정보시스템 수석감리원
현 재 (주)키삭 대표컨설턴트,
건국대학교 정보통신대학원 겸임교수

관심분야 : 정보시스템 감리, u_city 감리, 프로젝트 관리, 소프트웨어공학
E-mail : dskim@kisac.co.kr

전 남 재
Jun, Nam Jae

2003 충주대학교 제어계측공학과 이학사
2010 건국대학교 정보통신대학원 정보보안전공 공학석사
ISO27001-20000, CEH, CHFI, ECSA, ITIL
현 재 신한데이타시스템-SSC-과장
신한금융그룹사 - 통합보안관제센터,
신한은행 - IT총괄부 - 보안팀

관심분야 : 정보시스템감리, 정보보안, 디지털증거분석
E-mail : namjae@shinhan.com

김 희 완
Kim, Hee Wan

2001년 3월~현재 삼육대학교 컴퓨터학부 교수
2002년 2월 성균관대학교 전기전자 및 컴퓨터공학부(공학박사)
1995년 8월 성균관대학교 정보공학과(공학석사)
1987년 2월 광운대학교 전자계산학과(이학사)
1988년 한국전력공사 정보처리처 정보관리 기술사,
정보시스템 수석감리원

관심분야 : 분산 DB, 보안 데이터베이스, 정보시스템 감리
E-mail : hwkim@syu.ac.kr

논문접수일 : 2010년 11월 9일
수 정 일 : 2010년 11월 25일
게재확정일 : 2010년 11월 30일