情 報 保 護 學 會 誌
第18卷 第5號, 2008. 10

사이버 환경에서의 침해사고대응을 위한 위험도 산정 및 실시간 경보생성에 대한 연구

이 기 혁*, 이 철 규**

요 약

본 논문은 기업들이 정보보호를 위해 침해사고 대응과 관련된 각종 보안 솔루션 및 Network장비의 운영이 주로 사후대응 중심으로 이루어지고 있는 것을 사전에 예측, 방어할 수 있는 체계적인 환경구축을 통하여 효과적인 침해사고 예방체계를 위한 사전적 침해사고 대응체계를 위한 위험도를 산정하고 또한 실시간 경보 생성을 통해서 침해사고대응 시스템 구축 방안을 제시하고 실제 구현한 사례 연구이다.

Ⅰ. 서 론

급격하게 발전하는 IT 환경에 따라 그에 따른 역기능으로 사이버 상의 침해사고 형태 및 방법 또한 지속적으로 발전하고 있다. 최근 피해 현황을 살펴보면 보안 위협 발표 후 Hacking Tool 확산 속도 증가하고[1], 웜·바이러스 전파경로의 다양화 (P2P, Web APP 등), 다양한 서비스의 증가로 인한 보안관리 복잡성이 증가하는 추세이다.

이에 따라 각 기업들은 침해사고 대응과 관련된 각종 보안 솔루션 및 Network장비의 효율적인 운영/관리가 요구되며, 사후 대응 중심에서 사전에 예측, 방어할 수 있는 체계적인 환경구축 필요성 증가하고 있다.

본 연구는 이러한 대내·외적인 환경 변화에 따른 효과적인 침해사고 예방체계의 필요성이 높아짐에 따른 효율적으로 대응할 수 있는 침해사고대응체계를 수립하고 체계 상에서 실제 업무를 수행할 수 있는 침해사고 대응 시스템 구축 방안을 제시한다. 또한 본 연구에서 제시하는 내용은 최근 구축된 'SKTelecom IWS[2]'의 사례를 중심으로 서술한다.

Ⅱ. 본 론

2.1 침해사고대응체계 모델

사이버환경에서 안전성 및 신뢰성을 확보하고, 이상적인 침해사고대응체계를 구축하기 위해서는 실제 시스템의 구축을 위한 적절한 모델을 제시하여야 하며, 이상적인 모델을 제시하기 위한 조건으로 시스템적인 접근 이외에 조직, 업무, 표준, 규제 등을 반영해야 한다.

2.1.1 침해사고대응체계 모델 수립 방안

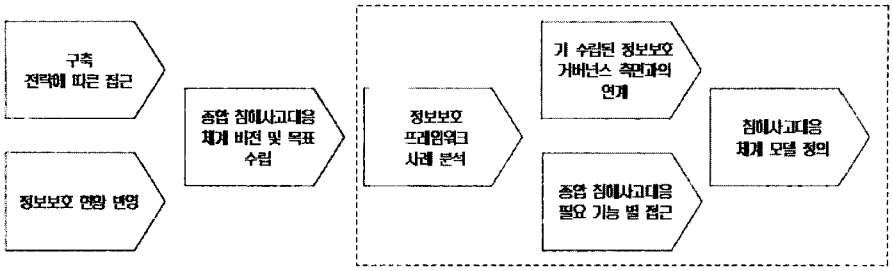
침해사고대응체계는 평소 지켜야 할 자산에 대한 위험평가를 통해 위험도를 관리하며, 사전 정의된 외부로부터의 공격에 대해 즉각적인 인지와 빠른 전파, 정의되지 않은 공격에 대해서는 위험도 프로파일링을 통한 이상징후 파악을 통하여 대응 가능하도록 하며, 지속적인 위험도 관리를 통해 효과적이며 우선순위에 따른 보안 투자가 가능하도록 한다.

침해사고대응 체계 모델을 수립하기 위한 고려사항

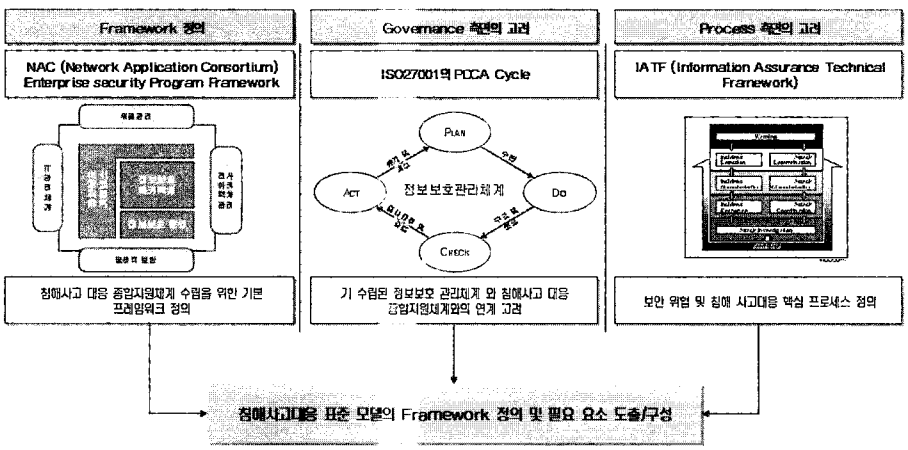
* SK Telecom(주) (kevinlee@sktelecom.com)
** 건국대학교 (cglee@konkuk.ac.kr)

1) 발표된 위협을 이용한 공격방법의 개발은 평균 6.8일 이며, 위협에 대응하는 벤더의 패치발표 기간은 평균 49일 소요됨 (출처 : Symantec ISTR v9)

2) IWS(Incident Warning & control System) : 침해사고대응시스템



〔그림 1〕 침해사고대응체계 모델 수립 절차



〔그림 2〕 침해사고대응체계 모델 수립을 위한 국제 표준 수용

은 크게 3가지 사항(핵심요구사항[3],구축전략[4], 구축요건[5])으로 된다.

침해사고대응 체계 모델을 수립하기 위해 내부적인 현황 및 전략을 파악한 후 가장 중요한 단계가 정보보호 프레임워크를 선정하는 부분이다.

정보보호 프레임워크는 국제적인 표준을 바탕으로, Governance[6], Process[7] 및 Architecture 측면에 필요한 요소를 구성한다.

2.1.2 침해사고대응 체계 표준 모델 정의

국제 표준에 따라 Governance와 Process 측면을 고려한 Framework을 정의한 후 실제 시스템 구축의 밑그림이 될 침해사고대응체계 상의 Architecture 측면을 도출한다. Architecture 도출의 주목적은 시스템의 청사진을 만드는 작업이며, 그 시작은 실제 필요로 하는 기능을 도출하는 작업이 된다. 도출된 기능을 바탕으로 시스템 Architecture를 만드는 일련의 작업[8]을 수행한다.

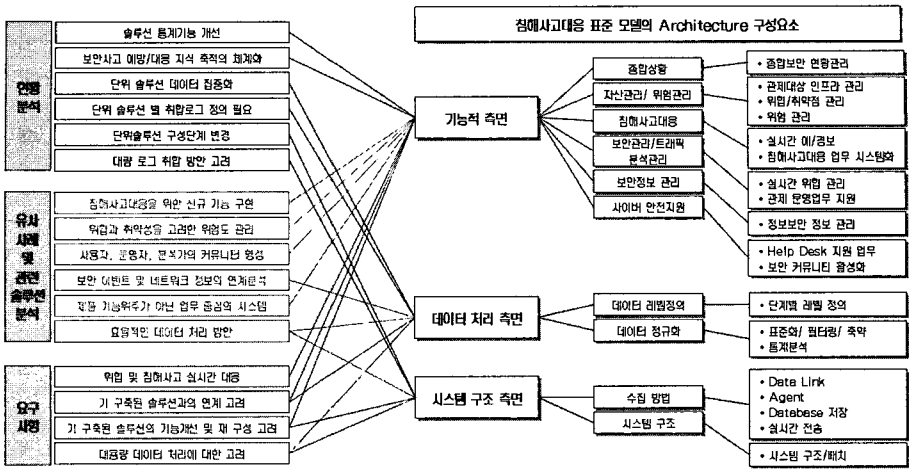
세부 기능을 도출하기 위한 고려사항은 현황분석, 유사사례 및 관련 기술분석, 현업 사용자의 요구사항을 기반으로 기능적, 데이터 처리, 시스템 구조 측면으로 그룹핑 후 그에 따른 관련 기능을 도출한다.

도출된 기능 그룹은 사전에 정의된 Governance와 Process를 연계하여, 종합적인 침해사고대응 체계 모델을 정의한다.

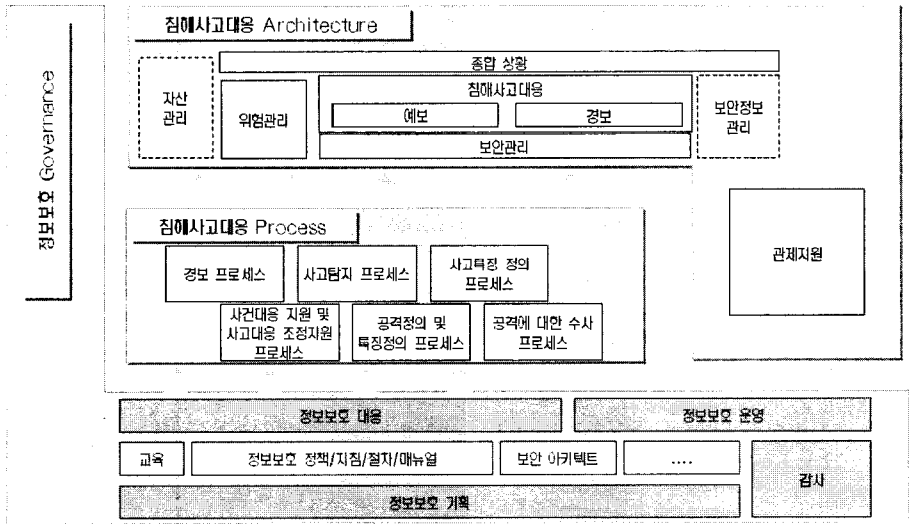
침해사고대응체계의 모델은 Governance 측면의 운영기준에 따른 조직의 구성과, 조직 활동의 근간이 되는 침해사고대응 프로세스 및 해당 프로세스를 수행하기 위한 아키텍처로 구성한다.

---

3) 핵심요구사항 분석 : 사용자 중심, 업무 기반, 해당 기업의 특수성 반영
4) 구축 전략 : 선택과 집중, 현장 중심의 의견 반영
5) 구축 요건 : 능동적인 대응, 종합지원체계, 담당업무 별 정보보호 능력 제고
6) 정보보호관리 체계 상의 조직, 업무, 절차 등과 같은 정책 관련 사항
7) 보안 위협 및 침해사고에 대한 업무 절차 관련 사항
8) 기능(데이터 출력 Layer)-분석(데이터 처리 Layer)-데이터(데이터 수집 Layer) 정의를 위한 일련의 작업 활동



〔그림 3〕 Architecture 도출을 위한 분석작업 예 (SKTelecom TSMA[9] 프로젝트)



〔그림 4〕 침해사고대응 체계 모델 예(SKTelecom TSMA 프로젝트)

2.1.3 단계별 시스템 아키텍처 정의

시스템 아키텍처를 정의하기 위한 작업과정은 국제 표준의 프레임워크를 기반으로 침해사고대응 업무를 위한 단위 프로세스[10]를 도출한다. 도출된 프로세스는 시스템 계층(Layer)[11]으로 구분하여 기능 정의를 위해 각 계층에서 구현되어야 할 사전 사항을 고려한다.

도출된 단위 프로세스를 통하여, 주요 단위 기능을 도출하고 그에 따른 세부 기능 정의 후 유사 기능을 그룹화(모듈화)[12] 하여 하나의 단위 시스템 요건으로 구분한다.

정의된 세부 기능을 실제 구현하기 위한 다음 단계는 단위 프로세스 상에서 도출된 시스템 계층 별 정의가 필요하다.

기능 구현을 위한 Raw 데이터 정의부터 방법과 수집된 데이터의 분석 기법을 통하여 어떠한 형태로 표현할 것인가에 대해 정의한다.

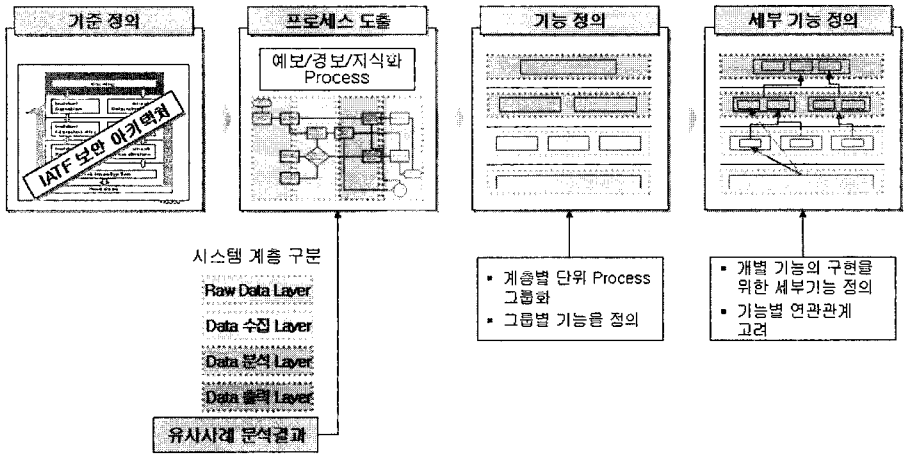
---

9) TSMA(Total Security Management Architecture) : 2007년 SKTelecom 종합 정보보호 관리 체계 수립 프로젝트

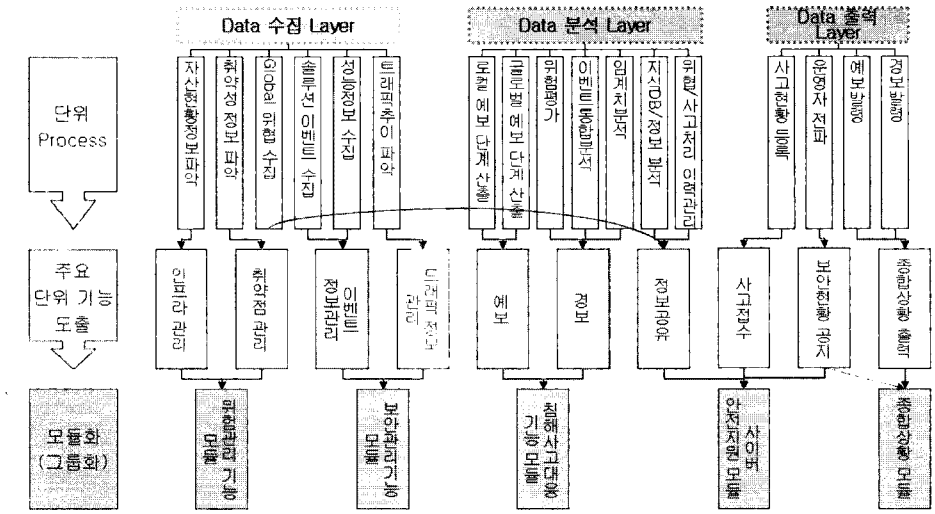
10) TSMA의 경우 예보/ 경보/ 지식화의 3가지 단위 프로세스를 도출

11) TSMA의 경우 정의된 시스템 계층은 Raw 데이터, 데이터 수집, 데이터 가공, 데이터 출력 계층으로 분류하여 정의함.

12) TSMA의 경우 종합상황, 침해사고대응, 보안관리, 관제지원 모듈로 분류하여 정의함.



〔그림 5〕 세부기능 정의 프로세스



〔그림 6〕 단위 계층(Layer)별 주요 기능 도출

침해사고대응을 위한 시스템 세부 기능 구현의 주요 계층은 데이터 수집 계층과 분석 계층으로 정의할 수 있다.

데이터 분석 계층 정의에 대한 세부 사항은 "Ⅱ장의 2. 침해사고대응을 위한 위험도 측정방안"에서 서술한다.

침해사고대응체계 모델을 수립하기 위한 일련의 작업과정을 정리하면,

① 핵심요구사항, 구축전략, 구축 요건을 사전에 정의한다.

② 기반이 될 국제 표준의 프레임워크를 선정한다.

③ 현황분석, 유사사례 및 관련 기술분석, 현업 사용자의 요구사항을 조사하여 선택한 표준과 연계하여 단위 프로세스를 정의한다.

④ 정의된 프로세스를 기반으로 주요 기능을 도출한다.

⑤ 도출된 기능을 구현하기 위해 시스템 계층별로 구분하여 세부 방안을 정의한다.

위와 같은 일련의 작업 과정은 정보보호 Governance와 Process, Architecture를 모두 고려한 침해사고대응체계 모델 정의를 가능하게 한다.

2.2 침해사고대응을 위한 위험도 측정방안

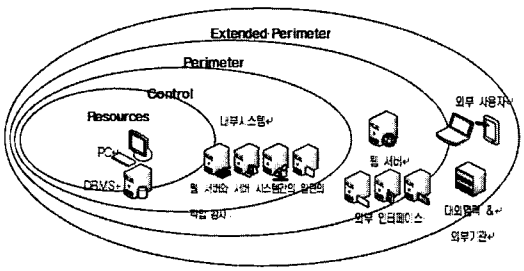
2.2.1 자산(Asset)의 정의

비즈니스 자산은 무형 또는 유형일 수 있으며, 비즈

니스 담당자가 조직의 측면에서 자산 값을 구체화할 수 있도록 충분하게 자산의 유형을 정의한다.

유형 자산에는 데이터 센터, 서버 및 자산과 같은 물리적 인프라가 포함되며, 무형 자산에는 조직에게 가치 있는 데이터 또는 기타 디지털 정보가 포함된다.

침해사고대응을 위한 자산의 정의는 위험도 측정을 위해 초점이 맞추어져 있으며, 위험도 측정을 위험 자산의 범위는 [그림 7]과 같다.



〔그림 7〕 위험도 측정을 위한 자산의 범위

〔표 1〕 각 자산 범위 별 상세 설명

범 위	설 명
Resources	내부 사용자의 PC 및 데이터를 보호하고, 기업인프라의 핵심정보 DBMS를 보호하기 위한 레이어
Control	내부 사용자 및 DBMS와 접속하는 업무 시스템 구간을 말하며, 접근제어/인증 등을 통한 보안 레이어
Perimeter	내부적으로는 Control 보안 레이어와 외부 사용자간의 인터페이스를 담당하는 구간으로 일반적으로 웹 서비스가 이루어지는 레이어
Extended Perimeter	내부 IT자산과 외부와의 경계가 되는 레이어로 외부 사용자의 보안과 최종 경계(방화벽, 침입탐지시스템 등)가 이루어지는 레이어

자산의 등급

평가 범위 내의 자산은 정성적 그룹 또는 등급에 할당되어야 한다. 등급은 보안 위험의 전반적인 영향에 대한 정의를 이끌어낸다. 또한 가장 중요한 자산에 조직이 집중하도록 한다.

또한 각 정보자산에 대한 목록에는 다음과 같은 항목을 포함한다.

- 자산의 명확하고 개별적인 식별자
- 자산의 위치
- 자산의 보안/위험 분류
- 자산 그룹
- 자산 소유자

이중 침해사고대응을 위한 자산의 등급을 정량적으로 나타내기 위해, 자산의 위치는 네트워크 위치, 자산 그룹 및 자산 소유자는 업무 중요도로써 아래와 같이 자산의 등급을 표시한다.

〔표 2〕 자산에 대한 업무 중요도 평가표

항목	업무중요도 평가				
네트워크 위치평가	순위	0	1	2	3
	1	1	2	3	4
	2	2	3	4	5
	3	3	4	5	6
	4	4	5	6	7

위의 표에서 업무중요도는 앞에서 살펴본 자산의 범위(Resource, Control, Perimeter, Extended Perimeter)에 따라 나타낼 수 있다. 또한 네트워크 위치에 대한 평가는 흔히 네트워크는 OA망, Server Zone, DMZ 구간 등으로 나뉘어져 있다. 이에 기준하여 네트워크 위치에 따른 등급을 나눌 수 있다.

아래는 이에 대한 한 예로 볼 수 있다.

- 자산평가(A) = SUM(a,b)
  *a = 네트워크 위치 평가(1~4)-DMZ, Server Farm, 내부망, 오픈망)
  b = 업무중요도 평가(0~3)-평가 무, 갑, 을, 병

2.2.2 취약성 및 위협 정의

취약점은 정보 자산이 위협에 의해 악용되기 쉽도록 하는 약점, 관리 프로세스, 조치 또는 물리적 노출, 즉 위협이 악용할 수 있는 자산 또는 자산 그룹의 약점을 의미 한다.

또한, 위협은 국제표준기구 ISO 13335-1의 정의를 보면 위협은 시스템 또는 조직에 대한 원치 않은 영향의 잠재적인 원인이라고 정의되어 있다

참조로 ISO 17799는 위협을 조직에 잠재적인 영향을 끼치는 원인으로 정의한다. NIST[13]는 위협을 시스

13) 미국표준기술연구소 [美國標準技術研究所, National Institute of Standards and Technology] : 미국상무부 기술관리국 산하의 각종 표준과 관련된 기술을 담당하는 연구소

〔표 3〕 위험평가의 정량적, 정성적 접근법 비교

항목	정량적	정성적
장 점	- 위험이 금전적 영향에 따라 우선 순위가 지정되며, 자산은 금전적 가치에 따라 우선 순위가 지정. - 결과에 따라 보안 투자 수익(ROSI)에 의한 위험 관리를 촉진. - 결과에 따라 관리 특정 용어(예, 위험등급에 따른 위험성 및 조치사항)로 표시 가능. - 조직이 경험을 쌓으면서 데이터를 기록해감에 따라 정확성이 증가하는 경향 발생.	- 위험 순위를 이해하고 가시적으로 볼 수 있음. - 합의에 도달하기가 용이함. - 위협의 빈도를 수량화할 필요가 없음. - 반드시 자산의 금전적 가치를 파악할 필요가 없음. - 보안 또는 컴퓨터 전문가가 아닌 사람들이 보다 쉽게 참여 가능.
단 점	- 위험에 지정된 영향의 가치가 운영자의 주관적인 의견에 기반. - 신뢰할 만한 결과와 합의에 도달하는 프로세스에 많은 시간이 소요됨. - 계산법이 복잡하고 많은 시간이 소요. - 결과가 금액 용어로만 표현되어 기술적 지식이 없는 사람들이 해석하기 어려울 수 있음. - 프로세스는 전문 기술을 필요로 하여, 운영자가 이를 통해 쉽게 교육을 받을 수 없음.	- 중요한 위험간에 차이가 충분하지 않음. - 비용 이점 분석의 기초가 없기 때문에 제어 구현에 대한 투자를 정당화하기 어려움. - 생성된 위험관리 팀의 품질에 따라 결과가 달라짐.

템에 피해를 줄 수 있는 잠재성을 가지고 있는 이벤트 또는 엔터티로 정의한다. 위협으로 인한 영향은 일반적으로 기밀성, 무결성 및 가용성과 같은 개념을 통해 정의된다.

위험평가를 수행하는 데 있어 공통적인 단점은 기술취약점에 중점을 둔다는 것이다. 따라서 침해사고대응을 위해서는 현재 전세계적으로 발생하고 있는 위협에 대해 계속적인 모니터링과 이 위협에 취약한 자산들을 파악을 하는 것이다

2.2.3 위험도정의(Risk)

정보보호 업계에서 사용하고 있는 가장 간결한 위험의 정의는 국제표준기구(International Standards Organization : ISO)에서 발간한 IT보안관리 가이드라인(Guidelines for the Management of IT Security)에서 제시되어 있는 정의는 다음과 같다.

위험은 어떤 위협(Threats)이 하나의 자산이나 여러 개의 자산의 취약성을 이용하여 그 자산에 손실(loss)이나 손상(damage)을 야기할 수 있는 잠재성을 말한다. 위험의 파급효과나 상대적인 심각성은 손상/손실의 비즈니스적 가치와 위협의 예상 발생빈도에 의해서 비례적(proportional)으로 결정된다.

이러한 맥락에서 볼 때, 위험은 다음과 같은 요소로 구성된다.

- 프로세스 및/또는 자산에 대한 위협과 취약점
- 위협과 취약성으로 인한 자산에 대한 영향 (impact)
- 위협이 발생할 확률(발생 가능성과 발생빈도의 조합)

위험평가

위험 평가는 위험을 확인하여 해당 위험의 영향을 파악하는 프로세스로써, 정성적/정량적으로 나눌 수 있다.

정성적 위험 평가는 자산, 위험, 제어 및 영향에 할당하려는 위험관리 접근법이고, 정량적 위험 평가는 객관적인 수치를 자산, 위험, 제어 및 영향에 할당하려는 위험 관리 접근법이다.

위험관리에 대한 정성적 접근법 및 정량적 접근법 모두 나름대로 장점과 단점을 가지고 있다. 어떤 상황에서는 조직이 정량적 접근법을 채택하는 것이 적합할 수 있으며, 소규모 또는 제한된 리소스를 가지고 있는 조직의 경우에는 정성적 접근법을 훨씬 더 적합할 수 있다. 이에 대한 비교는 다음과 같다.

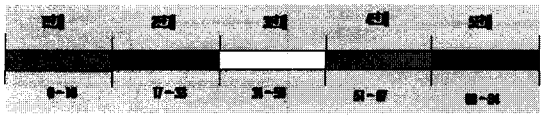
이에 따라 정량적 접근은 시스템으로 장기간 운영인력이 노하우를 쌓아 가야하며, 정성적 접근은 주기적 위험분석으로, 두 가지 방법을 혼합한 접근법으로 통합해야 한다.

아래는 정량적 위험평가에 대한 한 예로 볼 수 있다.

위험도 산출공식 =

$$R_1 = \frac{\sum A_1 * \sum V_1 * \sum T_1}{n_1} \quad R_2 = \frac{\sum A_2 * \sum V_2 * \sum T_2}{n_2} \quad R_3 = \frac{\sum A_3 * \sum V_3 * \sum T_3}{n_3}$$

위의 위험도를 통한 정량적 값에 대한 5단계 등급은 아래와 같으며 [표 4]는 SK Telecom의 예시이다.



〔표 4〕 정량적 단계에 대한 정성적 접근의 예시(SK Telecom)

위험도	단계	정의
5단계	심각	• 고객 주요 정보 및 사내 정보 유출 • 복구가 불가능하거나 오래 걸리는(1주이상)침해사고 • 대 고객 서비스에 지장을 주는 서비스거부 공격 이벤트 • 전사 네트워크 장애를 유발시키는 신종 웜 등에 의한 조직적인 공격 이벤트
4단계	경계	• 고객 주요 정보의 부분적 훼손 • 해킹 경유지로 이용 • 지속적인 침해시도의 탐지
3단계	주의	• 외부 유출 시 경미한 피해가 예상되는 침해사고 • 정보수집 이벤트 • 해킹 흔적은 있으나 피해 없음 • 일반적인 알려진 웜 등에 의한 공격
2단계	관심	• 일반적인 인터넷상의 보안 위협 상황
1단계	정상	• 해외, 국내 사이버 안전 유관기관 및 보안업체로부터의 최신 침해사고 및 위협정보 상시 확인 • SKTelecom의 침해사고대응 현황 모니터링

2.3 침해사고대응을 위한 종합정보보호 체계

침해사고대응을 위한 종합정보보호 체계 상의 인프라 관리의 핵심 사항은 크게 2개(데이터 수집, 위험도 관리 방안)항목으로 구분된다.

2.3.1 데이터 수집 방안

이상적인 데이터 수집 방안이란 최소의 데이터를 수집하여 최대의 출력을 가능하게 하는 것이다. 따라서 데이터 수집 방안을 연구하기 위한 사전 항목은 적절한 필요 데이터 자체를 정의하고 추후 확장을 고려한 표준화 작업이 선행되어야 한다. 표준화된 데이터를 대상으로 데이터 특성 및 데이터를 생성하는 시스템의 특성, 네트워크 환경, 기업 내부적인 방침 등을 고려하여 최적의 수집 방안을 도출한다.

데이터 표준화를 위한 선행 작업은 현재 내부에서 적용되어 있는 관련 시스템에 대해 현황조사 한다. 앞서 도출된 기능 구현을 목표로 관련 솔루션 별 생성되는

〔표 5〕 데이터 표준화를 위한 현황조사 목록

분류	연동장비	IP	사용포트	발생량(평균/월)	정보유형	표준화/필터링	연동주기(초)
방화벽	Netscreen	0.0.0.0	3458	10,000	세션로그	필요	300
IDS	Real Secure	0.0.0.0	334	550	탐지로그	불필요	60
웹방화벽	WAF	0.0.0.0	332	120	보안로그, 감사로그, 시스템 로그	필요	60

데이터를 조사하고 필요 데이터만 선택한다. 이 과정에서 중복 및 필요 없는 데이터는 제외되며, 새로운 기능이 추가되기도 하며, 현재 인프라에선 구현되지 못하는 주요 기능이 파악된다. 즉, 이러한 일련의 작업을 통해서 보안 투자 사업의 우선순위가 결정된다.

데이터 표준화를 위한 현황 조사는 위 [표 5]와 같은 항목을 최소 기준으로 조사한다.

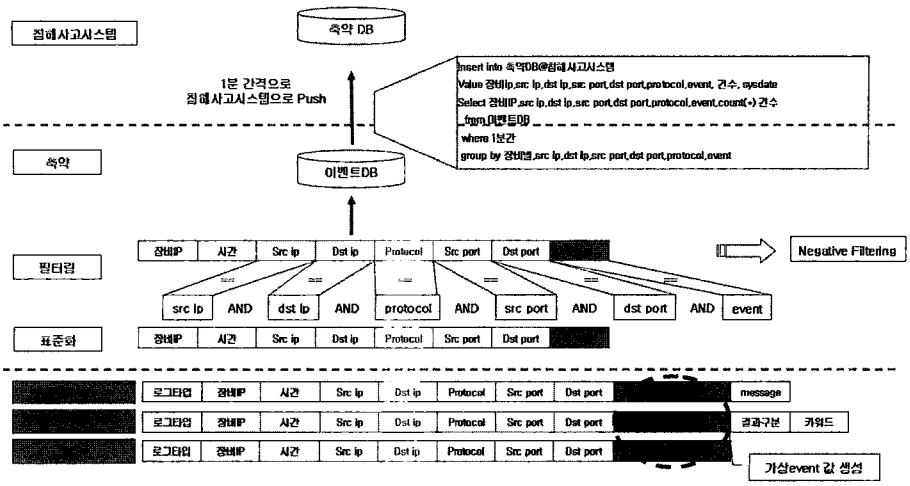
위와 같은 현황분석이 이루어지면 필요 정보 유형만 분류하고 각 시스템 별로 표준 데이터 포맷을 정의 한다. 정의된 포맷에 따라 시스템 구축 시 수집 DBMS의 Table 설계 시 반영된다.

표준 데이터 포맷을 정의하면 위의 [표 5] 현황조사 목록 상에 항목을 추가하여 각각의 데이터를 수집해야 하는 대상 시스템과의 연동 방식을 결정한다. 연동 방식은 표준연동방식[14]을 기준으로 시스템 지원 여부 및 주요 기능 구현을 고려하여 차선책으로 Agent 개발 방식 등을 고려한다.

데이터 정의와 연동방식이 결정되면 최적의 성능 안을 고려한다. 성능과 확장성(유연성) 부분은 서로 대립적인 성질을 갖는다. 따라서 가능한 사전에 명확한 데이터 수집 방안이 고려되지 않은 상태에서 성능 최적화[15]

14) SNMP, SYSLOG : 데이터전송 표준에 따른 방식으로 사전에 규정된 정보 값을 선택하여 전달하는 방식으로 연동 구현방식이 간단하며, 용이하지만 사전에 연동항목에 대한 정의가 이루어져야 하며, 추가항목 발생 시 주기적으로 관리가 필요함.

15) 성능 최적화 작업의 기본적인 성질은 가능한 많은 부분을 표준화하여 처리함을 의미한다. 통상적인 표준화가 아니라면 기본적으로 확장성 및 유연성을 보장하기 힘들기 때문이다. 또한 대용량을 데이터를 최소의 자원으로 처리하기 위해서는 유연성이 떨어지는 바이너리 포맷의 데이터를 직접 사용하거나 메모리 상에서 처리하는 방법을 선택하기도 한다.



〔그림 8〕 데이터 표준화 방안

작업은 무의미해질 수 있다

데이터 수집 방안이 종합정보보호 체계에서 중요한 관리 포인트가 되는 이유는 앞에서 설명한 데이터 정의를 통해서 침해사고대응 체계를 위한 주요 기능의 구현 여부가 결정되며 그에 따라 투자 사업의 우선순위 및 체계적인 Master plan을 구상할 수 있다는 점과 추후 도입되는 솔루션을 선택 시 정의된 수집 방안을 충족시킬 수 있는 기능여부를 함께 검토해야만 한다.

2.3.2 위험도 관리 방안

앞에서 설명한 데이터 수집 방안이 종합정보보호 체계 상에서 보안 인프라에 대한 관리부분에 해당한다면, 위험도 관리 방안은 운영적인 측면에 해당된다. 자산, 위협, 취약성을 고려한 위험도를 정의하여 기본적인 데이터의 생성은 시스템적으로 가능하지만 실제 침해사고

〔표 6〕 위험도 관리를 위한 기본 요소 데이터 항목 자동화

항목	자동화 여부 및 방법
자산	자산관리 시스템으로부터 자산목록을 자동으로 갱신
	자산의 그룹을 사전에 정의하여 신규 자산 등록시 자동 적용
	자산 중요도는 기본적으로 그룹 중요도 값을 상속 (개별 지정 가능)
위협	각 데이터 표준 포맷 별 경보 데이터[16] 자동 생성
	글로벌 위협 (외부 정보를 실시간으로 자동 반영)
취약성	자동화된 취약성분석 센서를 통해 자산에 대한 취약성 지수 생성
	글로벌 취약성(외부 정보를 실시간으로 자동 반영)

〔표 7〕 기본 요소 데이터를 이용한 위험도관리 방안 예

위험도 관리방안	설명
연계 분석	기본요소 데이터를 이용하여 서로 연관성을 부여한 후 의미 있는 데이터를 자동 계산을 통해서 생성 가능하도록 설정. 각 데이터 중 연관성을 부여하는 작업 자체가 위험도 관리의 핵심이며, 운영 노하우를 통해서만 가능 함.
교차 분석	앞서 설명한 자산의 범위와 관련하여, 각 자산의 perimeter[17]상의 발생 데이터를 순차적으로 조사하여 외부와 내부에서 발생되는 연계 현상 또는 순차적으로 발생되는 현상 등을 자동적으로 파악 가능하도록 설정함.
통계 분석	가장 일반적이며, 범용적으로 사용하는 분석 방법으로, 각 데이터의 통계 데이터를 종한 이상징후를 파악하는 방법임. 실시간적으로 현황을 파악하기는 힘들지만 가장 포괄적으로 현황 파악이 가능한 장점이 있음.

대응 체계 상에서 지속적인 위험평가를 통한 침해사고의 예방, 조기 경보 및 즉각적인 대응을 위해서는 지속적인 운영 노하우를 시스템에 적용하는 방법뿐이다.

따라서 위험도를 관리하기 위한 기본 요소 데이터는 가능한 자동으로 생성하도록 구성하고 각각의 요소를 선택적으로 연계하여 필요한 데이터를 확보 가능하도록 유연하게 설계, 구현하는 것이 필요하다.

16) 발생된 데이터의 평균값 대비 현재 발생되는 값에 대해 표준 편차 방식을 적용하여 위협의 등급 적용.
17) [그림 7] 위험도 측정을 위한 자산의 범위 참조

위의 분석방법은 위험도를 관리하면서 파악되는 관리 절차를 시스템화 하기 위한 요소들로 운영자 개개인의 노하우가 녹아 들어간다. 이러한 분석기법을 사용하기 위한 선행과정은 얼마나 현황을 잘 파악하고 있는가와 그에 따라 허용할 수 있는 임계치가 어느 정도 인가를 파악하는 것이 가장 중요하다.

2.3.3 종합침해사고대응 시스템 구현

침해사고대응 체계가 마련되면 실제 대응 업무를 수행하기 위한 시스템을 구축하게 된다.

시스템을 구축하기 위해서는 침해사고대응을 필요로 하는 조직에서 그에 맞는 침해사고대응 체계를 구성해야 한다. 침해사고대응 체계 구성을 위해 고려했던 사항을 토대로 만들어진 주요기능 목록을 시스템을 통하여 구체화 한다.

(1) 유사 구축사례분석

국내 우수한 보안관제센터 중 정부부처를 포괄하는 국가사이버안전센터(NCSC) 및 단위부처 중 가장 규모가 큰 교육사이버안전센터(ECSC)의 정보보호 핵심 시스템 구축 사례 분석을 통해 분석결과를 도출한다.

〔표 8〕 구축사례분석 요약

분석 대상		목적	분석결과(요약)
NCSC[18]	ECSC[19]	핵심 시스템 기능 분석	Zone-h[20] 사이트 정보에 의존한 홈페이지 변조 위주의 모니터링
		국내 우수 보안관제 센터의 벤치마킹	위협/공격/트래픽/트렌드 관점에서 각종 통계 지원
		조직운영현황 분석	관제지원 시스템의 Help Desk를 운영하여 기관내의 커뮤니케이션 유도

시사점 도출

- NCSC의 홈페이지 변조에 대해서는 전세계 해킹 동향과 침해사고 현황을 실시간 제공하는 www.zone-h.org에 의존하여 모니터링하고 있음.
  즉 기존의 인프라 보안 관제에서 홈페이지 위변조에 대한 중요성이 대두됨.
- NCSC의 위협상관관계를 자동 위주 보다는 사용자가 직접 설정하여 분석할 수 있는 기능으로 구현 됨. 즉 운영 노하우 반영이 필요함.
- ECSC의 사이버안전지원 시스템의 Help Desk 기능은 관련 기관의 정보보호대응의 지식화된 DB에 대한 커뮤니티를 활성화 할 수 있게 한 기능으로 정보의 빠른 전달 및 대응을 위한 핵심 기능 모듈로 인식됨.
- ECSC는 수집센서 및 수집 에이전트 모듈을 각 기관별로 설치함으로써, 네트워크 트래픽 최소화 및 연동 비용을 최소화함.
- 유해 트래픽, 이벤트, 위협에 대해서 따로 모니터링 및 분석을 하고 있어서 통합적인 지표관리가 필요함.

(2) 센터 별 상세 분석

국가사이버안전센터(NCSC)

① 국가정보원 소속기관
② 해킹/웜 등 사이버침해에 대한 공공기관 정보시스템 피해 방지
③ 국가 기밀 유출에 따른 국가안보와 국익손실 예방 및 대응

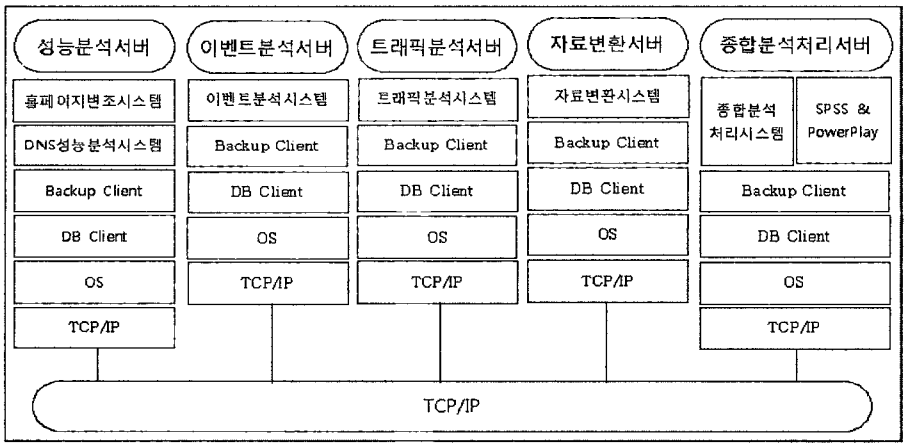
종합분석처리시스템

이기종 보안제품의 로그를 수집하여 성능/보안 이벤트/트래픽 데이터에 대해 가공, 분석을 통해 새로운 공격 형태에 대한 경보 발령 등을 수행할 수 있도록 정보수집/ 정보가공/ 통합관제로 구성됨

- 홈페이지 변조에 대한 모니터링을 zone-h.org에 의존을 하고 있다. 이는 해커들이 홈페이지 해킹(변조) 후 www.zone-h.org에 올리는 방식으로 초동대응이 힘들다는 단점이 있다.
- 위협 분석시 사용자 기능 설정 중심의 상관관계 분석을 실시하여서, 관제요원들의 노하우를 적극적으로 시스템에서 반영할 수 있도록 하고 있다.
- 유해 트래픽, 이벤트, 위협에 대해서 따로 모니터링 및 분석을 하고 있다. 이러한 요소들의 종합적인 정량화 지표가 필요하다.

18) NCSC(National Cyber Security Center): 국가사이버안전센터
19) ECSC(Education Cyber Security Center): 교육사이버안전센터
20) www.zone-h.org, 세계적인 해킹그룹을 통해 전세계 해킹 동향 및 침해사고 현황 정보를 제공

〔그림 9〕 국가사이버안전센터(NCSC) 시스템 구성



〔그림 10〕 국가사이버안전센터(NCSC) 소프트웨어 구성

〔표 9〕 NCSC 주요기능

위협분석/ 상관관계 분석	• 로컬 및 네트워크 위협 • 비 정상적 행위 정밀 조회 가능 • 주요 호스트 등록정보 제공 • 보안 이벤트 및 네트워크 정보의 상관관계 분석
이벤트 분석	• 기간별 구분 검색 기능 제공 • 최근 TOP 5 정보 제공 • 취약성 DB 연관분석 • 포트란 통한 트래픽량 연동 분석 • 최신 취약성 관련된 포트 정보 제공
트래픽분석	• 프로토콜 서비스 프레임 사이즈 분석 기능 • 추이 그래프와 파이차트 제공 • 유해 트래픽 정밀 분석 • 비정상 트래픽 비교 분석
트렌드 분석	• 네트워크 위협 비교 분석 기능 • 공격 유형 트렌드 분석 • 추이 증감 분석 • 취약성 대응 방안 제시
홈페이지 변조모니터링	• www.zone-h.org로부터 목록을 수집 • 관련 산하 기관에 공문 발송 • 홈페이지 변조 모니터링

교육사이버안전센터(ECSC)

ECSC는 시·도 교육청, 대학 등 교육(행정)기관의 정보보호 전담기구로서 해킹/웜 등 사이버 침해에 의한 교육기관 정보시스템의 피해 방지를 위해 사이버 안전 지원시스템이며 단위 CERT 및 이기종 통합보안관리시스템 연동되어 침해사고 접수 처리 및 분석업무를 처리한다.

종합분석시스템

ECSC의 침해사고대응을 위한 종합분석시스템은 종합분석, 위협관리, 보안정보관리, 사이버안전지원시스템으로 구성됨.

- 위협/공격/트래픽/트렌드 관점에서 각종 통계 지원
- 사이버안전지원 시스템의 Help Desk를 운영하여서 기관내의 커뮤니케이션을 유도.

〔그림 11〕 교육사이버안전센터(ECSC) 시스템 구성

위협탐지	• 로컬 및 네트워크 위협 • 비 정상적 행위 정밀 조회 가능 • 주요 호스트 등록정보 제공 • 보안 이벤트 및 네트워크 정보의 상관관계 분석
공격탐지	• 기관별, 공격 유형별, 서비스별 탐지 분석 • 취약성 DB 연관분석 • 포트를 통한 트래픽량 연동 분석 • 최신 취약성 관련된 포트 정보 제공
트래픽 분석	• 프로토콜 서비스 프레임 사이즈 분석 기능 • 추이 그래프와 파이차트 제공 • 유해 트래픽 정밀 분석 • 비정상 트래픽 비교 분석
트렌드 분석	• 네트워크 위협 비교 분석 기능 • 공격 유형 트렌드 분석 • 추이 증감 분석 • 취약성 대응 방안 제시

- ECSC에서는 각 교육기관에 수집센서 및 수집 에이전트를 설치하여 수집데이터를 최소화하고 그에 따른 네트워크 트래픽을 최소화하고, 각 솔루션별 연동 비용을 최소화함.
- 유해 트래픽, 이벤트, 위협에 대해서 따로 모니터링 및 분석을 하고 있다. 이러한 요소들의 종합적인 정량화 지표가 필요.

즉, 침해사고대응을 위한 관제시스템의 중요요소는 웹에 대한 위/변조 감시, 운영 노하우, 빠른 커뮤니케이션, 데이터 수집의 효율성 및 보안 이외의 데이터 통합으로 정의된다.

(3) SKTelecom IWS

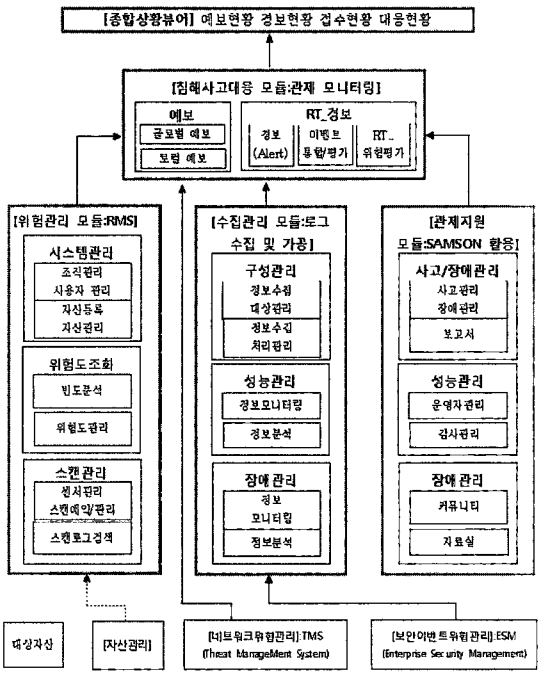
SKTelecom IWS는 위와 같은 일련의 작업을 통해 구현된 종합 침해사고대응 시스템이라 할 수 있다.

IWS의 기본 구축 목표는 SKTelecom의 침해사고 대응 체계를 기반으로 활용성 극대화를 통해 업무 프로세스를 단순화 시키는 것이다.

따라서, 현황분석과 업무 분석, 사용자의 요구사항 및 국제 표준을 통해 생성된 주요기능 목록을 '어떻게 효율적으로 구현하겠는가'에 초점을 맞추었다.

IWS는 종합상황뷰어, 종합관제모듈, 위험관리모듈, 수집관리모듈, 관제지원모듈(기존의 SAMSON[21] 시스템을 활용) 5가지로 구성, TMS, ESM시스템과 연동하여 구성하였다.

21) SKTelecom에서 사용하고 있는 보안 취약성 진단 시스템



〔그림 12〕 종합침해사고대응 시스템 구성
(SKTelecom IWS 예)

〔표 10〕 IWS 입력 데이터 구성

종합상황 뷰어	• 침해예방, 침해대응 등 전체 업무 활동에 대한 종합적인 현황정보 분석을 위한 실시간 상황관제
침해사고 대응 모듈	• 침해시도현황, 위협트래픽 발생현황, 보안패치, 안티 바이러스 설치 현황 등 관리적 관점의 정보 제공 • 「위험관리 모듈」을 통해 도출된 예보, 경보를 각 정보보호 실무자에게 발령
수집관리 모듈	• 이기종 정보보호시스템에서 발생되는 침해공격 정보수집 • 침해공격 정보는 「침해사고대응 모듈」에서 활용 가능한 데이터화
위험관리 모듈	• 「침해사고대응 모듈」내부의 정보보호 자산의 위험을 관리 • 지속적 위협평가, 위험분석을 통해 축적된 침해공격 정보를 침해사고 대응 지식기반으로 활용 • 예·경보 발령에 따른 대응방안 마련, 침해사고대응 모듈에 정보제공, 중·장기적인 대책 수립에 활용
관제지원 모듈 (SAMSON)	• 담당자로부터 직접 침해사고에 대한 신고, 접수를 받고 보안현황 정보를 제공 • 침해사고 접수, 평가, 처리 등의 프로세스를 기반으로 이력을 관리하고 사용자에게 정보를 제공

Ⅲ. 결 론

최근 옥션과 인터넷뱅킹 등의 인터넷 보안 사고들을 통해 알 수 있는 사항은 보안은 투자 사업이 아닌 바로 비즈니스의 수익성과 연결되고 있다는 점이다. 이번 옥션 사고로 인한 금전적 손해도 있지만 매출의 급 하강으로 인해 경쟁사의 매출 급상승이라는 부가적인 효과가 일어났다. 이번 옥션 해킹 사고는 사고 범주 자체는 '내부 개인정보유출'로 정의 할 수 있지만 개인정보유출 방지를 위한 활동만이 대응의 해답이 될 수는 없다.

즉, 어떠한 방법, 유형으로 발생할지 알 수 없는 보안사고에 대해 최소한의 대비책은 정보보호에 대한 침해사고대응체계를 갖추고 그에 따라 투자의 목표와 방향성을 가지고 발전시켜 나가야 한다.

SKTelecom의 IWS는 침해사고대응 체계를 구체화한 시스템의 시작이며, 출력 데이터의 단순화 및 자동화를 통해서 사용자가 운영상에 쉽게 접근 가능하도록 구성하였고, 운영상의 노하우를 통한 위험도 관리가 유연하게 적용할 수 있도록 내부 분석 알고리즘을 최대로 반영한 시스템이며, 침해사고대응을 위한 위험도 산정과 실시간 경보생성에 대한 실제 구현 및 최적의 운영 시스템 구현사례이다.

참고문헌

[1] 마이크로소프트홈페이지, http://www.microsoft.com/korea/
[2] 한국정보보호진흥원 홈페이지 http://www.kisa.or.kr
[3] 국회 홈페이지, http://www.assembly.go.kr
[4] 안철수 연구소, http://www.ahnlab.com
[5] 국제해킹동향 및 정보제공홈페이지 http://www.zone-h.org
[6] 국가사이버안전센터 홈페이지 http://www.ncsc.go.kr
[7] 교육사이버안전센터 홈페이지 http://www.ecsc.go.kr
[8] 전사적 위험관리 : 개념과 사례, LG경제연구원, 2004. 1.
[9] 유비쿼터스 기술과 서비스,진한엔엠비, 2005, 이기혁.
[10] 유비쿼터스 IT혁명과 제3공간, 전자신문사, 2004.
[11] 정보통신망법 및 시행령, 시행규칙 개정에 따른 개인정보보호 조치사항, 한국정보보호진흥원, 2007. 7.

[12] 정보통신망법 개인정보보호규정의 적용범위, 한국정보보호진흥원, 2005. 11.
[13] 이기혁, 윤재동, "민간기업의 개인정보유출 위험에 대한 측정방법과 그 사례에 대한 연구", 정보보호학회지, 2008. 6.
[14] 최승, "불확실성을 고려한 위험분석 방법론 연구", KIPS 논문집 제11권 제2호, 2004. 11.

〈著者紹介〉

이 기 혁 (Lee Gi Hyouk)
정회원

1991년 2월 : 한양대학교 공학석사
2008년 3월~현재 : 건국대학교 공학박사 과정중
1994년 5월~현재 : SK Telecom (주)정보기술연구원 재직중
<관심분야> 정보통신공학, 정보통신정책분야,정보보호학,개인정보보호공학등
<저서>유비쿼터스 사회를 향한 기술과 서비스(2005, 진한엠엔비)
유비쿼터스 컨버전스(2004, 진한엠엔비)
데이터네트워크 구축론(2000, 진한엠엔비)
차세대무선인터넷기술(2003, 진한엠엔비)등 다수

이 철 규 (Lee Cheol Gyu)

1991년3월 : 일본 게이오대학교 공학석사
1997년3월 : 일본 게이오대학교 공학박사
2004년8월~현재 : 건국대학교 대학원 교수, 건국대학교 벤처창업지원센터 소장, 한국창업학회이사
<관심분야> 벤처전문기술, 정보보호학, 경영컨설팅학 등