FOCUS

정보시스템의 위협과 통제

황인탁
IRM 대표컨설트

최근 정보화의 역기능에 의한 새로운 산업재해가 등장하고 있다. 본인이 인식하지못한 정보들이 본인의 의지와 상관없이 정보시장에 유통(?)되고 있으며, 기업의 경영자료들이 버젓이 언론매체들에 보도되는 경우도 있다. 최근 필자는 사무실 운영 대행업체로부터 전화를 받은적이 있는데 너무도 상세히 필자의 사무실 운영 현황을 알고 있음에 놀란적이 있다.

이미 정보는 보안측면에서의 정보속성을 유지하기가 어려워지고 있다. 가끔 우리는 금융기관의 정보시스템 장애로 인한 금융업무의 마비를 목격하곤 한다. 이때 그 기관의 손실은 어느정도인가를 생각해 본적이 있다. 자연재해가 발생했을때 이제는 재해로 인한 물리적 손실외에 정보시스템 파괴로 인한 손실의 엄청남에 놀라곤 한다. 정보시스템의 발전과 더불어 정보시스템에 대한 위협도 매우 다양한 형태로 등장하고 있다.

정보사회에서는 정보의 가치가 새롭게 인식되어 정보가 무형의 데이터라는 형태로 수집, 축적, 가공, 이용되어 인간생활에 중요한 영향을 미치고 있다. 공업사회에서는 다종다양한 재화가 생산되고 물질적 풍요를 누리게 된 반면, 공해로 대표되는 많은 문제가 표면화되고 있는것과 같이, 사회의 발전은 풍요, 이익, 편리와 같은 순기능적인 측면이 있는 반면에 손해, 불이익, 장해와 같은 역기능적인 측면을 안고 있다. 정보사회에서도 인간은 많은 시스템에 의존해서 생활하고 있으며 그 풍요를 누리고 있는 반면 역기능적인 측면이 계속 도출되고 있으며 그 심각성이 날로 심화되고 있는 것이다.

본고에서는 정보시스템에 대한 위협과 위험, 그리고 이에대한 적절한 통제를 통한 안전대책을 살펴보고자 한다.

●위협과 위험

위협이라함은 시스템기능의 목적활동을 저해하는 모든 사실과 현상을 말한다. 사회전체 혹은 특정의 시스템을 밖에서 객관적으로 보면 대단히 광범위한 사실과 현상이 위협으로서 존재하게 된다. 그러나 위협은 시스템의 외부에서 시스템에 작용하는 것처럼 보이지만 실은 집행기능의 취약성이 많은 시스템에 더욱 존재한다. 취약성이 없다면 위협도 존재하지 않는다. 그러나 현실적으로 취약성이 없는 시스템은 없기 때문에 시스템에서는 여러가지 사실과 현상이 위협이 될 수 있다. 위협이라는 것은 개개의 시스템이 직면하는 역기능 측면의 사실과 현상으로 정의 할수 있는 반면 위험(Risk)은 그 위협이 현실의 손해와 결부된 위험성의 개념이다. 즉 위험은 그 사실과 현상이 발생하는 확률을 부가한 개념이다.

●보안과 통제

보안이라는 것은 위험을 감소시키는 것이며 보안을 확보하기 위해서는 집행기능의 일부를 삭제해서 위험을 회피하든지 통제기능을 강화해서 위협을 감소시키는 것이 필요하게된다.

그러나 위험회피 수단은 본질적인 보안대책으로는 볼 수 없고 실질적인 보안은 통제기능의 강화에 의해서만 달성된다. 통제에 의해 취약성이 조절되지

만 현실적으로 모든 취약성에 대하여 완벽한 통제를 설정하는 것은 불가능하다. 그러나 통제에 의한 위협이 위협으로서 인식되지 않아도 좋을 정도까지 감소한 경우에는 그 사실과 현상을 통제된 위협의 개념으로 정의 할수 있다. 이상과 같이 통제라는 개념은 대단히 넓은 개념으로서 사용되고 있다. 통제는 보안뿐만아니라 시스템의 신뢰성, 유효성 및 효율성의 확보에도 도움이 된다.

●정보시스템의 취약성

정보시스템의 취약성은 정보시스템의 특성과 관련하며 기술적 측면, 조직적측면, 사회적 측면에 걸쳐 구성되어진다. 정보시스템의 특성에 기인한 취약성은 다음과 같은 것이 있다.

- 대량데이터의 고속처리
- 데이터의 비가시성
- 기능과 정보의 집중
- On-Line 처리
- 기계적 반복처리
- 시스템의 블랙박스화
- 상호의존적 처리 (네트워크화)

이와같은 정보시스템의 취약점은 시스템에 대한 위협을 증가시키면서 보안과 안전에 대한 관심을 불러 일으키게 되었다. 다음은 안전성 확보의 필요성에 대한 배경을 정리한 것이다.

①정보기술의 발달은 기존의 물리적 안전대책만으로는 정보시스템의 안전성 해결을 어렵게 하고 있다.

②데이터의 대량복사가 가능하다.

③해커와 컴퓨터 바이러스에 의한 불법적인 자료열람, 변조, 절취, 파괴 등에 의한 피해와 범위가 광역화 현상을 보이고 있다.

④불특정 개인이 접근할 수 있는 정보환경이 확대되고 있다.

⑤개인 신상정보의 종합적 이용이 가능해져 프라이버시 침해문제가 등장하고 있다.

⑥사회및 조직의 정보시스템에 대한 의존도가 증가하고 있다.

⑦데이터의 휘발성이 강하기 때문에 일순간에 대량의 데이터를 잃어버릴 가능성이 높다.

정보시스템의 안전대책은 정보시스템 자체에 대한 기술적인 안전체제 구축만으로는 해결할 수 없다. 안전에 대한 중요성을 정보시스템의 주요 요건으로 인식하고, 그 바탕위에서 정보시스템 안전에 관한 개념정립이 체계적으로 정립되어야 할 것이다.

즉 인간과 기술의 상호 작용을 고려해야 하며, 사회 기술체제 내에서 해결할 수 있는 통합적이고 체계적인 접근방법이 요구되는 것이다.

정보시스템 위협의 유형

시스템에 대한 위협은 시스템이 갖는 취약성 및 통제의 정도에 따라 그 크기나 종류가 다르며 여러가지 기준에 의한 분류가 가능하다. 분류방법은 그렇게 중요한 것은 아니다. 다만 여러 각도로 분류를 생각하는 것은 발생가능한 위협을 빠짐없이 도출하고 명확히 정의하여 대응방법을 효과적으로 마련하기 위한 것이다.

다음은 위협의 형태적 분류를 나타낸 것이다.

구분	위협의 내용
1. 형태적 분류	범죄, 부정행위, 자연재해, 인적재해, 고장, 오류
2. 장소적 분류	정보시스템운영환경의 내부, 외부
3. 동기 분류	의도적(악의적), 비의도적(우발적)

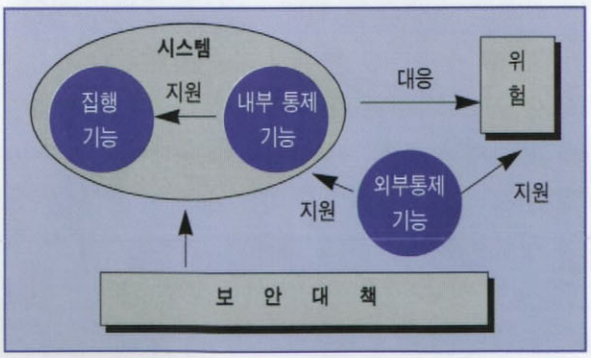
다른 분류방법으로 발생원인 유형에 의한 다음과 같은 분류가 있다.

구분	위협의 내용
자연재해 및 환경에 의한 위협	천둥번개, 태풍, 지진, 홍수, 누수, 화재, 정전기, 곤충/설치류, 먼지, 기타 오염물질 등
인간에 의한 위협	(위협환경에 근접한 요원) • 시스템 운영요원: 데이터입력, 시스템운영, DBA, 프로그래머, 시스템유지보수원, 통신요원 • 관리요원: 안전요원, 감사인, 현업 코디네이터 • 사용자: 현업사용자, 현업부서관리자 • 기 타 : 해커, 산업스파이, 적대세력요원 등..
기술적 위협	• 하드웨어 결함 • 소프트웨어 결함

구분	위협의 내용
기술적 위협	• 주변장비의 결함 • 운영요원의 부적절한 지식이나 결함
절차상의 위협	• 절차나 규정에 대한 이해 미숙 • 절차의 오용 • 경영전략이나 지침에 위배하는 절차와 규정 • 절차나 규정에 대한 의도적인 위반 • 절차적용의 일관성 결여
조직상의 우협	• 정보화로 인한 책임과 권한의 집중 • 사용자와의 책임한계 • 책임과 권한의 불명확 • 불합리한 업무분장 • 특정업무에 대한 부서간의 마찰 • 부적절한 인사관리 • 특정부서, 업무에 대한 통제부재
응용업무시스템	• 프로그램 논리오류/ 데이터 유실 • 입력양식의 항목 누락 • 사용자지침서의 작성오류 • 비 인가된 트랜잭션 처리 • 비인가자의 프로그램/데이터 사용 • 부적절한 입출력 시기 등...

정보시스템 부문의 통제와 절차

정보시스템에 대한 내부, 외부의 위험을 감소하고 효율성, 효과성을 향상시키기 위한 일련의 계획된 행위를 통제라고 한다. 통제는 여러가지 기준에 의해 분류할 수 있으며 크게 내부통제와 외부통제로 구분할 수 있다. 그 상관관계를 도식화 하면 다음과 같다.



내부통제기능은 시스템의 구성요소이기 때문에 집행기능과 분리하는 것이 실무적으로 어려울 수 있다. 집행기능이 없으면 시스템의 활동이 정지해 버리는 것과 같다. 그러나 적절한 통제기능이 없는 시스템은 방향키 없는 배와 같을 것이다.

현실적인 시스템 활동은 통제와 집행기능이 함께 작용한다. 그러나 보안대책을 계획하고 실행하고 평가하기 위해서는 통제의 유효성 판단이 필요하므로 구분하여 정의 할 필요가 있다.

위험에 대처하는 기능으로서의 통제기능을 정의할때 통제기능은 다음의 네가지 기본적 기능으로 분류할 수 있다.

- 억제기능 : 위험의 발생을 적게하는 기능
- 방지기능 : 위험의 실현을 저지하는 기능
- 검출기능 : 위험의 발생, 실현 사실을 발견하고 기록하며 통보하는 기능
- 회복기능 : 위험이 실현됨으로써 끼친 손해를 최소한으로 막아 복원하는 기능

억제기능의 통제 절차에는 내부통제로서 개개의 적용업무시스템에 설치되어 있는 것도 있지만 대부분은 조직전체를 대상으로 실시되고 각 보안 대책에 공통적으로 이용할 수 있는 면을 갖고 있다. 방지기능은 억제기능과 함께 예방기능으로 분류 되기도 한다. 그러나 방지기능은 손해를 일으키게 하는 행동의 달성을 저지하는 기능이고 억제기능과는 달리 자연재해를 포함하는 광범위한 위험에 대처할 수 있다.

방지기능은 위험이 발생하지 않은 상황에서 손해가 발생할 가능성이 있는 경우에 설정된다. 따라서 방지기능의 경우는 위험의 적절한 분석이 선행되어야 한다.

검출기능에 의해 검출된 사실과 현상은 적절한 방지기능없이 회복기능이 작동하도록 인간, 혹은 자동화된 통제시스템에 알려야 한다. 즉 검출기능은 방지기능 또는 회복기능이 효과적으로 작용하기 위한 기능이며 검출기능이 결여된 통제는 효과적 이지 못한 경우가 많다. 손해가 현실로 발생한 경우를 가정해서 회복기능의 통제를 설정할 필요가 있다. 회복기능은 일시회복기능과 재해와 같은 긴급사태가

발생한 경우를 위한 긴급회복기능이 있다. 회복기능의 설정시 고려해야할 중요한 점은 인간의 안전성과 회복절차의 철저한 교육이다. 긴급사태는 자주 발생되는 것이 아니기 때문에 회복기능이 유효하게 작동되도록 하기 위해서는 교육 및 훈련 등을 통해 조직내의 방재체제를 철저하게 인식시킬 필요가 있다.

위험분석과 절차

위험분석은 정보시스템의 안전대책 수립에 있어서 가장 중요한 처리과정의 하나이다. 그 첫번째 단계는 위협의 식별이다. 어떤 하나의 통제로 모든 위험을 극복하는 것은 불가능하다. 따라서 각각의 위험에 대하여 각각의 통제를 검토하는 것이 필요하다. 위협의 식별은 특별한 방법에 의한 것이 아니다.

위협의 식별은 정보시스템을 둘러싸고 있는 위협에 대한 일상에서의 관심정도에 달려있는 경우가 많다. 일반적으로 다음의 방법을 통해 위협을 식별한다.

- 각종 문헌정보를 통한 위협의 식별
- 시스템의 과거의 경험 (사고, 오류보고서 등)
- 신문, 잡지 등에 게제된 사건, 사고
- 각 분야 전문가의 진단

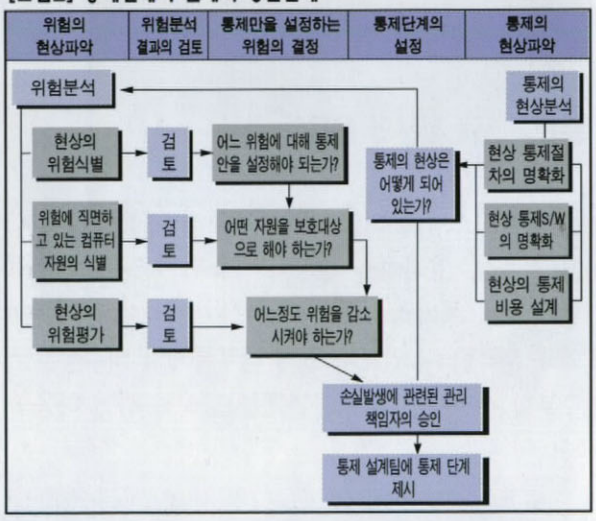
위협에 대한 식별후 위험평가를 실시한다. 위험평가는 구체화되지 암호는 장래의 위협을 그 평가대상으로 하고 있으므로 어려움이 있다. 본래 불확실한 것을 대상으로 하고 있으므로 엄밀한 분석을 실시하는 것은 시간과 노력의 낭비로 인식될 수 있으나 가능한한 정량적인 위험평가는 안전대책에 대한 투자범위를 설정하는데 매우 긴요하다. 위험평가를 위한 방법을 소개하면 다음의 절차가 있다.

- 해당 위협에 의해 손해를 받는 정보자원의 식별과 열거
- 예상 손실액의 결정
  - 파괴에 의한 손실 : 재 취득(구축)을 위한 비용
  - 처리지연에 의한 손실 : 업무마비 또는 지연에의한 경영손실 비용
- 대체절차의 비용 : 수작업 또는 타 시스템에의한 대체처리시 소요비용
- 기회손실비용
- 통계적 방법에의한 발생확률의 산출
- 위험평가 총괄표의 작성

위험평가에 의한 기대손실을 계산한후(기대손실 = 발생빈도×발생건당손실가액) 안전대책의 여러 대안을 평가한다.

위험관리의 목적은 통제에 의해 시스템에 대한 순수 위험을 감소시킴으로써 위험액과 통제비용의 합계액을 최소화하고 궁극적으로 조직의 목적에 공헌하는데 있다. 따라서 안전대책의 실시는 경제성이 충분히 고려되어 결정되어져야 한다. 아래의 도표는 통제를 설계하는데 있어서 단계와 요건의 전체적 상관관계를 도식화 한것이다.

[그림2] 통제설계시 전체적 상관관계



정보시스템의 안전성은 무결성, 가용성, 보안성의 세가지 요소를 확보함으로써 유지된다. 그러나 정보시스템의 적용확대에 따른 많은 위협에의 노출은 정보기술의 발전에도 불구하고 더욱 심화되고있다. 이제 필자는 정보시스템의 구성자원별로 적정한 통제관리 방법과 기술적인 적용방법에 대하여 계속 소개할 예정이다. 본 기고가 독자의 정보자원관리에 다소나마 도움이 되길 기대하면서 정보시스템의 위협과 통제에 대한 소개를 마치고자한다. DC