□ 기술해설 □

CALS 구현을 위한 정보 안전 관리 체계

한국과학기술원 김세헌*

목 차

정보보안의 주요목적은 인가되지 않은 사람이 정보에 접근하거나 인가없이 정보를 사용하는 것을 방지하는 것이다. 이를 위해서는 먼저 정보를 기밀정도에따라 분류하고 각각의 보호정도를 달리할 수 있도록 정보의 기밀등급분류가 이루어져야 한다. 이것이 이루어지게되면 각각의 식별된 중요정보를 어떤 방법으로 유지, 관리 및 이용할 것인지를 규정화해야 한다.

1. 기밀분류대상

원칙적으로 기업운영에 부정적인 영향을 끼칠 수 있는 정보는 모두 기밀분류대상이 된다. 경영층은 기밀분류에 대한 기본적인 정책과 가이드라인을 수립하여야 한다. 이 가이드라인은 균형있게 수립되어야 한다. 정보에 대한 지나친 보안정책(over-classification)으로 너무 많은 정보를 기밀로 분류하게 되면 이를 유지하기위해 과다한 행정력을 필요하게 되어 불필요한 경비발생을 유발시키게 될뿐만 아니라 결국에는 보호하여야 할 정보도 제대로 보호하지 못하는 결과를 초래하기 쉽다. 반면에 너무 허술한 보안정책(under-classification)은 중요한 정보를 제대로 보호하지 못한다. 따라서 경영층은 기업이 보유하고 있는 각종 정보들의 가치를 정확히 인식하여 그에 적절한 보안정책을 수립하여야 한다.

일반적으로 기업에 있어서 보호를 필요로 하는 정보는 다음과 같다.

(가) 노출되었을 때 그 기업에 영향이 큰 정보. 영업전략정보, 신제품개발 관련 정보, 장기 경영계획정보 등이 이에 속한다.

(나) 파괴되었을 때 그 조직에 큰 타격을 주게되는 정보. 고객관리파일, 외상대금파일 등이 이에 속한다.

(다) 허위로 수정되었을 때 기업과 사회에 중대한 영향을 끼치게되는 정보. 금융기관의 예금대장, 공안전산망의 전과관련자료, 국방전산망의 각종 자료, 개인신상자료 등이 있다.

이러한 정보들을 체계적인 방법으로 기밀등급을 분류하여 각각에 합당한 수준으로 보호해 주는 것이 바람직하다.

2. 기밀분류형태

기밀정보로 취급되지 않는 정보는 일반정보로 분류되며 이는 외부에 노출되어도 업무수행에 지장이 없고 생각해보면 충분히 알수있는 정보들을 포함한다. 외부에 발표되어진 정보, 회사내 행사의 공고, 서점에서 입수가능한 책

*종신회원

에 기재되어 있는 정보 등이 일반정보 속한다.

기밀로 분류된 정보는 기밀도의 수준에 따라 다시 등급을 나누는 데 여기에는 분류의 기준에 따라 두가지 분류형태가 있다.

가. 취급허용범위기준 분류

이 형태는 정보를 취급할수 있도록 허용해 주는 범위를 기준으로 분류하는 방법으로서 대개 다음의 4가지로 구분한다.

(1) 극비 정보

극비로 분류되는 정보는 기업이 갖고있는 최고기밀로서 노출되었을때 기업의 존망에까지 영향을 줄 만한 정보이다. 기업의 경우에는 미발표된 신제품의 성능, 내정가격 및 발표시일 등이나 장단기 영업전략등이 극비정보에 속한다. 국가적으로는 국방, 외교 등에 관련된 민감한 자료들이 극비정보에 속한다.

(2) 부외비 정보

부외비로 분류되는 정보는 그 내용으로보아 업무수행상 그 정보를 필요로 하는 부서에게로 한정하는 것이다. 부외비 정보의 배부대상 선정은 기업내에서의 지위와는 관계없이 업무수행상 알 필요(need-to-know)의 원칙에 따라 결정한다. 기업체에서 부외비로 분류되는 정보로는 제조관계의 제원장, 가격설정정보, 인사고과표, 급여표, 인사기록정보 등이 있을 수 있다.

(3) 대외비 정보

대외비정보는 기업의 소유권보호나 직원의 권리보호 또는 사업상 판단하기에 그 내용을 기업내로 한정해야할 것 등이다. 각종 규정이나 기업내 업무수행을 위한 지침서 등이 여기에 속할 수 있다.

(4) 일반 정보

비밀로 취급할 필요가 없는 기타 정보들이다.

나. 중요도 기준 분류

이 형태는 정보를 중요도에 따라 구분하는 방법으로서 국가안보에 관련된 기관들에서 주로 사용되어오던 형태이다. 최근에는 이를 다음과 같이 민간기업에 적당하도록 재편성하여 기업에서 사용하고있다.

(1) 1급 비밀(secret)

일급비밀에 속하는 정보는 전략적 성질의 정보로서 노출되면 기업에 심각한 손실을 초래할 수있는 것들이다. 대체로, 노출되는 경우 기업의 총 업무효과의 5% 이상의 감소를 일으킬 만한 정보들이다.

(2) 2급 비밀(confidential)

경영층에게만 이용가능한 정보로서 그외의 사람에게 노출되면 기업의 총 업무효과의 1-5 %의 감소를 초래할 만한 정보들이다.

(3) 3급 비밀(private)

기업구성원에 관련된 것으로 기업외부에 노출되면 안되는 정보로서 기업 내부의 윤리강령이나 직원들의 프라이버시권에 관계된 정보들이다.

(4) 일반정보(unclassified)

위의 그룹에 속하지 않는 정보들이다.

3. 기밀분류기법

정보의 민감성 여부는 데이타의 발생자(originator)가 가장 잘 알 수 있기 때문에 기밀 분류는 원칙적으로 데이타의 발생자가 하는 것이 바람직하다. 이때 정보를 분류함에 있어서 over-classification이나 under-classification의 오류에 빠지지않고 경영층에서 제시한 보안정책에 부합하는 적절한 기밀분류를 하기위해서는 체계적인 분류기법을 이용하는것이 바람직하다. 이러한 분류방법을 문서화하여 지침서로 배부함으로서 서로 다른 분류자간에 발생하기 쉬운 불균형을 어느정도 해소할 수 있다. 정보를 체계적으로 분류하는 방법으로 다음의 두가지가 있다.

가. 점수할당 방법

이 방법은 정보의 각 요인별로 점수를 할당하고 이를 합산하여 정보의 총 점수를 구한 후

표 1 정보의 요인분류와 점수할당

양 식		영 역		성 격		시 의 성		노출시손실		노출가능성	
최종양식	3	마아케팅	3	전략적	8	최 신	3	상	8	상	3
중간단계	2	재 무	2	운영용	4	과 거	1	중	5	중	2
원시자료	1	인 사	1	고객관리	2	없 음	0	하	1	하	1
		기 타	0	직원관리	1						

이 값에 따라 등급을 매기는 방법이다. 표 1은 정보의 요인을 크게 6 가지로 나누고 각 요인별로 할당된 점수를 예시하고 있다. 물론 이러한 요인분류와 점수할당은 기업체의 업종과 상황에 따라 바뀔 수 있다.

최종양식의 자료는 원시자료보다, 그리고 마아케팅 부서의 자료는 다른부서의 자료보다 높은 점수를 할당받는다. 또 전략적 정보는 다른 정보보다 매우높은 점수를 할당받으며 최신 자료는 오래된 자료보다 높은 점수를 할당받는다. 노출시 손실의 경우 상 중 하로 나누어져 있는데 상은 손실이 기업의 총 업무효과의 5%를 초과하는 경우, 중은 1-5% 사이인 경우, 하는 1% 미만일 경우 정도를 기준하면 된다. 노출가능성은 예상발생빈도에 따라 분류한다. 이와같은 방법으로 각 요인별로 산출된 점수의 합이 그 정보의 총점수가된다. 이 총점수에 따라 기밀등급을 정하게 되는데 분류의 기준을 예를 들면 다음과 같다.

표 2 기밀분류기준

총 가 치	등 급
22-28	1급
15-21	2급
6-14	3급
0-5	일반

여기서 설명한 가치할당방식에 따라 다음의 4가지 정보의 기밀등급을 구해보자.

정보 A : 사내의 워드프로세싱 훈련계획
정보 B : 퇴직연금의 적립계획
정보 C : 제품판매전략 및 기대수익 (곧 공개될 정보)
정보 D : 새로운 회사 인수 후의 재정적 상황에 대한 예측.

이 각각의 정보에 대해 요인별 점수부여 및 기밀등급분류 결과가 표 3에 정리되어 있다.

이 분석에 의하면 워드프로세싱 훈련계획은 총점수가 3 으로서 일반정보로 분류해도 충분한 것으로 판단되며 퇴직연금 적립계획은 3급, 제품판매전략은 2급, 그리고 신규회사인수후 재정적 상황예측은 1급기밀로 각각 분류하는것이 적절한 것으로 판단된다. 특히 정보 D는 전략적 성격의 정보이며 노출시 손실 등이 매우 큰것으로 평가되어 높은 점수가 할당된 것을 알 수 있다. 이 방법은 완전하지는 못해도 분류작업자의 주관적인 판단을 어느 정도 줄일 수 있다.

나. 룰에의한 분류방법

앞에서 논의한 점수할당방법에서는 정보의 총점수가 각 요인의 점수의 단순 합계로 되어 있기때문에 여러 요인간의 상호작용을 충분히 반영하지 못하고 있다. 특히 정보의 요인을 좀

표 3 기밀등급분류의 결과

정보	양식	영역	성격	시의성	노출시 손실	노출 가능성	총점수	분류
A	1	0	0	0	1	1	3	일반
B	3	1	1	3	1	1	10	3급
C	3	3	4	3	5	2	20	2급
D	2	2	8	3	8	3	26	1급

표 4 1급기밀 분류 룰의 예

룰	성격	노출시손실	시의성	노출 가능성	영역	양식
1	전략적	상	최신자료			
2	전략적	상		상		
3	전략적	상			마아케팅	
4	전략적	상				최종양식
5	전략적	상		중	재무	
6	전략적	상		중		중간단계
7	전략적	상			재무	중간단계
8	전략적	중	최신자료	상	인사 이외	
9	전략적	중	최신자료	상		원시자료이외
10	전략적	중	최신자료		마아케팅	원시자료이외
11	전략적	중	최신자료	하 이외	마아케팅	
12	전략적	중	최신자료	하 이외		최종양식
13	전략적	중	최신자료		인사 이외	최종양식
14	전략적	중	과거자료	하 이외	마아케팅	최종양식
15	전략적	중	과거자료	상	인사 이외	최종양식
16	전략적	중	과거자료	상	마아케팅	원시자료이외
17	운영용	상	최신자료		마아케팅	최종양식
18	운영용	상	최신자료	상	마아케팅	
19	운영용	상	최신자료	상		최종양식
20	운영용	상		상	마아케팅	최종양식

더 세분하거나 변경하게 되면 분류방식을 다시 전면적으로 재구축하여야 하는 어려움이 있다. 이러한 한계를 어느정도 극복하기위한 대안으로서 룰에의한 분류방법이 있다.

이 방법은 각 정보의 성격에 따라 어떻게 분류할 것인지를 룰로 정해 문서화 해두는 방식이다. 이 룰들은 각 요인들에 대한 판단결과를 논리적 결합하여 표현 된다. 예를 들어서 표 4에는 1급 기밀을 규정해 주는 룰들이 일부 열거되어 있다. 예를 들어 룰1과 9는 다음과 같은 의미이다.

룰1 : 만일 정보의 성격이 전략적이며 노출시 손실이 상이고 시의성이 최신자료이면 다른 요인들에 대한 평가결과에 관계없이 모두 1급 기밀로 분류한다.

룰9 : 만일 정보의 성격이 전략적이며 노출시 손실이 중이고 시의성이 최신자료이며 노출가능성이 상이며 양식이 원시자료가 아니라면 영역에 대한 평가결과에 관계없이 1급 기밀로 분류한다.

이러한 룰에의한 분류방법은 많은 이점을 가지고있다. 첫째, 모든 요인들에 대한 평가를 항상 꼭 해야만 할 필요가 없이 분류할 수 있는 경우가 매우 많아서 분류과정이 단순해진다. 둘째, 표 1과 같은 각 요인의 평과결과에 대한 점수할당이나 각 요인에 매겨진 점수를 합산하는 다소 인위적인 과정이 필요없어지게 된다. 마지막으로, 이 방법은 룰의 변경과 새로운 요인의 도입 등에 있어서 신축성을 가지고 있어서 점수할당 방법보다 용이하게 이루어질 수있다.

4. 기밀정보의 관리

정보의 기밀도 분류는 원칙적으로 그 정보의 발생자가 하는 것이므로 그 업무의 주관부서가 결정할 성질의 일이다. 따라서 그 정보를 사용하게 될 사용자부서에서 그 정보의 기밀도를 마음대로 바꾸는것은 절대로 있어서는 안된다. 주관부서에서의 기밀도 변경을 통지하지 않는 한 그 기밀도는 계속 유효하며 항상 그 기밀도

에 맞는 수준으로 관리하여야 한다. 즉, 10년 전에 작성된 자료와 최근 작성된 자료가 현재 기밀도가 같으것으로 분류되어있다면 둘 다 같은 수준으로 보안관리하여야 한다.

기밀도 분류를 한시적으로 하여야 할 때도 많이 있다. 예를들어, 시제품의 정보와같은 것은 발표전에는 회사 외부는 물론 회사내부에서도 필요이외의 사원들에게는 비밀로 취급하여야 한다. 이러한 정보는 공개적으로 발표할 시기까지 한시적으로 비밀로 취급함을 명시할 필요가 있다. 이렇게 하지않으면 일반에 공개된 정보가 사내에서는 그대로 비밀로 취급되는 상태의 정보가되어 취급에 모순이 발생하게 된다. 이렇게 불필요해진 기밀 정보를 많이 가지게되면 이를 관리하기 위한 많은 행정력과 보관장소를 낭비하게 된다. 이러한 현상이 더욱 극심해지게되면 보안관리가 제대로 이루어지지 못하게되어 꼭 보호해야할 정보까지 보호받지 못하여 기밀관리에 허점이 발생하게 된다. 따라서 기밀의 특성을 잃어버려서 보호의 필요성이 없어진 정보는 즉시 기밀등급분류를 수정하는 것이 중요하다.

기업에서 직원들이 모든 정보의 기밀도구분을 제대로 인식하고 있는 경우는 드물다. 따라서 직원들에게 기밀도 구분의 의미를 설명하고, 모든 정보에 기밀도구분을 부착하여 이를 회사내에 철저히 인식시키는 것이 무엇보다도 중요하다.

5. 정보 안전 관리 체계

여기서는 정보의 안전 관리를 위해 그림 1과 같은 조직도를 제안한다. 제안된 조직도는 정보처리 부서장과 시큐리티 부서장을 독립시켜 역할의 분담을 통한 상호 견제 위치에 있게 하였다. 정보처리 부서장과 시큐리티 부서장은 최고 관리자의 통제 영역안에 있음은 물론, 각 부문의 최고관리자에게 보고의 의무를 진다.

정보처리 부문에서 추구하는 효율성과 시큐리티 부문의 목적인 안전성은 상호 배치되므로 그로 부터 야기되는 갈등은 최고 관리자, 내부 감사 담당자, 정보처리 부문 최고 관리자, 시큐리티 최고관리자 등에 의해 구성되는 보안 대

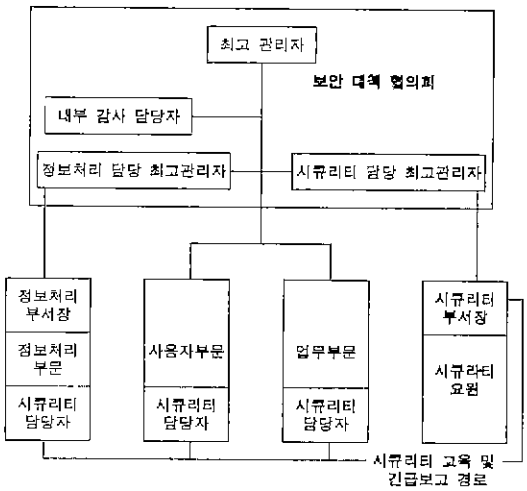

그림 1 정보 안전 관리 체계

책 협의회에서 해소하게 된다. 이는 정보처리 부문과 시큐리티 부문의 실무적인 독립성의 보장을 더욱 공고히 하기위함이다.

그 밖에, 시큐리티 부서장은 업무지휘계통의 조직밖에 시큐리티의 지휘계통조직을 업무조직에 밀착시켜 구축한다. 그 조직의 시큐리티 담당자는 각 부서의 장이 임명한다. 지명된 부서의 시큐리티 담당자는 통상업무외에 통상업무와 동일한 레벨로 시큐리티 확보에 대한 업무를 맡는다.

각 부서의 시큐리티 담당자의 수는 조직과 장소에 따라 차이가 있으나, 20－30명에 1인 정도로 지명한다. 일반적으로는 업무의 조직단위에 따라서 시큐리티 부서장이 임명된다. 이렇게 해서 지휘계통이 구축되면 시큐리티에 관한 모든 지시는 이 지휘계통을 따라서 이루어지게 한다. 예를 들어, 전사원에 시큐리티 교육을 실시하도록 요청받는 경우, 각 부서에 임명되어 있는 시큐리티 담당자에 대한 시큐리티 교육은 시큐리티 부서장이 실시한다. 교육을 받은 각 부서의 시큐리티 담당자는 그 부서에 소속되어 있는 모든 사원에게 시큐리티 교육을 실시할 책임이 있다. 그러나 교육을 포함해 시큐리티 확보의 최종책임자는 라인 관리자임을 잊어서는 아니된다. 시큐리티에 관한 보고서는 라인 관리자가 통상업무 지휘계통을 통하여 상부의 라인 관리자에게 보고하게 된다. 그러나,

긴급의 경우 시큐리티 부서장에게 직접 보고할 수 있다.

여기에 제시된 전산망 관리의 조직도는 하나의 방향이며, 완전한 시스템이 한번에 구축 될 수는 없는 것이다. 따라서, 전산망의 종류에 따라 다르겠지만 항상 자체적인 감사 및 외부의 감사를 통하여 리스크를 식별하고, 그에 대한 대책을 수립해 나가는 과정에서 보다 안전한 시스템이 구축될 것이다. 조직 설계에 대한 표준의 방법이 없음은 각 전산망의 내용과 상황이 상이할 것이기에 너무나 당연하다. 그러나 분명한 것은 적절한 업무 분담을 통한 상호 견제 및 보완을 유지하도록 설계되어야 하며, 그것보다 더 중요한 것은 최고 관리층 및 직원들의 의식으로서, 항상 조직의 리스크에 대한 식별과 이에 대한 보다 개선된 안전통제의 조직체계 및 그 규범에 적응하려는 자세이다.

이제 안전관리에 관한 각 부문의 책임을 분리하여 보면 다음과 같다.

가. 최고 관리층

조직체의 경영방침과 영업전략 등에 관한 의사결정을 행하는 최고관리층은 시큐리티에 대한 대책의 강구여부에 대한 최종적 판단의 책임도 있으므로 시큐리티에 대한 관리층의 인식은 매우 중요하다.

나. 내부감사부문

내부감사부문은 업무감사와 회계감사외에도 조직체내의 정보시스템 시큐리티감사도 실시한다. 업무분리가 이루어졌다 하더라도 관련업무 담당자들이 공모를 하면 정보의 유용, 변조, 사기 등이 이루어질 가능성이 있다. 이러한 것을 방지하기 위해 비정기적으로 감사를 수행하여 체크하고 추후 그 성과도 감독할 필요가 있다.

감사부분을 세분화하면, 응용 시스템 감사, 시스템 개발 감사, 일반적 업무 절차에 대한 감사, 안전 통제에 관한 감사, 시스템 소프트웨어의 감사, 보수 절차의 감사 등이 있는데, 안전 통제에 관한 감사는 매우 중요하며 빈번히 실시되어야 한다.

다. 정보처리 담당 최고관리자

- 정보처리 자산 보호의 문제들에 관해 조직수준의 중심점이 된다.
- 필요하고 가능하다면 정보처리 자산 보호 능력을 키우기 위하여 내부적 노력을 한다.
- 조직 시큐리티 정책, 목표, 방향을 지원하는 차원에서 정보처리 자산 보호의 목표를 설정하고 정책을 추천한다.
- 조직 시큐리티 정책, 목표, 방향을 보완하는 차원에서 정보처리 자산 보호의 시행세칙, 방향, 지침을 설정, 공표해야 한다.
- 조직 시큐리티 관련 시행세칙, 방향, 지침을 검토한다.
- 정보처리 자산 보호에 관하여 조직수준의 방향을 제공한다.
- 정보처리 자산 보호 책임을 가지는 인력의 조직부문에 배치하는 것을 상담한다.
- 정보처리 서어비스의 제공자들에게 정보처리 자산 보호의 책임과 요구에 관해 효과적인 교육과 방향이 제시되는지를 확인한다.
- 정보처리 자산 보호에 관해 정보처리 서비스의 운용, 정보처리 서비스의 공급자들이 제대로 부응하고 있는 지 확인한다.
- 정책, 시행계획등의 정보처리 자산 보호의 요소들을 검토하고, 정보처리 공급자에 대한 계획의 참여성과를 검토한다.
- 감사나, 사용자, 소유자, 시큐리티 스탭들의 교육을 후원해야 한다.

라. 시큐리티 담당 최고관리자

조직체에서 시큐리티를 확보하기 위해서는, 모든 부문의 시큐리티을 통괄하고, 조직전체를 대표해서 최고 관리층에 시큐리티 상태를 직접 보고하며, 기업전체의 시큐리티를 확보할 책임을 질 시큐리티 관리자를 임명하는 것이다.

시큐리티 관리자는 시큐리티에 관한 전사적인 문제에 대한 주관 부서가 되며 정보처리 자산의 보호에 관한 규정을 작성하는 것외에도 다음과 같은 것을 실시할 책임이 있다.

- 조직체의 시큐리티 대책의 실시도에 관하여 목표를 설정한다. 예를 들어 전사원의 시큐리티에 관한 지식을 높이기 위한 대책

으로서 시큐리티 교육을 실시한다. 전사원에 대한 교육을 연간 몇 % 실시할 것인가 하는 것이 대책 실시도의 목표가 된다.
- 주관부문과 사용자 등에 대해, 시큐리티에 관한 조언과 컨설팅을 실시한다.
- 가이드라인과 각종 규정을 작성한다.
- 시큐리티의 평가 수법을 개발한다. 예를 들어, 규정, 기준과 수속의 준수도를 체크 방식으로 채점하여 평가한다.
- 각 부서 단위에 시큐리티에 관한 담당자를 배치하도록 추진한다. 시큐리티 관리자와 그 스텝만으로는 전사원에게 철저할 수가 없으므로 시큐리티 담당자를 배치해서 시큐리티 관리의 집행자 역할을 대행하는 동시에 그 부서의 시큐리티 확보를 위해 노력하도록 한다.
- 시큐리티에 관하여 교육을 실시한다. 말하자면, 시큐리티란 무엇인가? 왜 시큐리티가 중요한가? 시큐리티 확보의 필요성의 인식, 보호할 만한 자산의 식별 등을 포함한 내용의 교육을 실시한다.
- 정보자산의 보호상태에 관해 조직 전체적으로 준수도를 모니터링해서 최고 관리층에 보고한다.

마. 업무 부문, 사용자 부문, 정보처리 부문

업무 부문의 업무가 정보처리 부문에서 컴퓨터로 가동되고 있는 경우에도 업무운영의 책임은 어디까지나 해당업무의 업무 부문에 있다. 업무를 기계화한다는 것은 그 운영을 컴퓨터로 처리한다는 것뿐이기 때문이다. 정보시스템에는 적용업무의 기획 및 개발의 책임을 지는 업무 부문, 컴퓨터 시스템을 운영하는 정보처리 부문, 그리고 단말기등을 이용해서 업무를 수행하는 사용자 부문이 있다. 예를 들면, 인사정보업무의 경우, 업무 부문은 인사부문이 되고, 컴퓨터로 그 적용업무를 가동시키는 부문이 정보처리 부문이 되고, 가동되고 있는 시스템을 이용하는 부문이 사용자 부문이 된다. 업무 부문이 동시에 사용자 부문이 되기도 한다.

(1) 업무 부문

업무 부문은 적용업무의 책임자가 되며 업무의 처리과정을 숙지하고 있어야한다. 적용업무의 시큐리티를 확보하기 위해서 업무 부문은 정보자산의 가치 및 중요성을 십분 인식하고 다음과 같은 대책을 강구할 의무가 있다.
- 정보자산의 취급을 규정대로 운영관리 하기위해 정보의 기밀도 구분을 한다.
- 적용업무의 기획 및 개발 단계에서 각종 사업상의 통제와 필요한 가감사성(Auditability)의 구축을 요구하며, 시스템 시동 전에 요구한 대로 되어있는 지 확인한다.
- 적용업무시스템의 사용방법과 오류의 회복과정 등이 사용자에게 충분히 교육되고 있는 지를 확인한다.
- 적용업무의 가동상황, 액세스 관리, Recovery의 순서, 기밀도 구분에 합당한 관리가 규정대로 정확히 운영되고 있는지 정기적으로 확인한다.
- 운영에 있어서는 리스크분석, 리스크 평가, 대책 선택의 타당성을 확인한다.
- 적용업무시스템을 이용해서 업무를 수행하는 사용자에 대해, Need-to-know의 원칙에 의하여 액세스 권한을 부여한다. 또 액세스 권한 부여 리스트를 보유한다.
- 자연재해 또는 화재 등 예측이 불가능한 사태가 발생해서 장기간에 걸쳐 컴퓨터가 정지할 때의 Back-Up 체제, 경우에 따라서는 컴퓨터 시스템이 없는 상태에서의 업무수행을 위한 예측불허사태를 위한 계획에 참여한다.

(2) 사용자 부문

사용자는 적용업무 시스템을 이용하며 On-line/Off-line, 개인용 컴퓨터 및 오피스 컴퓨터를 사용해서 일상업무를 수행하는 부서이다. 사용자 부문은 주관부문과 정보처리 부문이 정한 규칙/수속에 따라 다음 항목을 수행할 책임이 있다.
- 업무목적 이외에 정보처리기기를 사용해서는 아니된다.
- 사용자 측에 설치되어 있는 정보처리 기기를 보호/관리한다.
- 정보자산의 액세스에 관해 주관부문의 허

가를 받아, 허가된 정보자산에만 액세스한다.

- 정해진 방법에 따라 패스워드의 관리 및 갱신을 행한다. 통상 패스워드의 갱신은 정보처리 부문에서 패스워드 발생장치를 이용해서 갱신하지만, 사용자가 패스워드를 지정하는 시스템에서는 타인에게 노출되지 않도록 패스워드를 선정하는 것이 필요하다.

(3) 정보처리 부문

정보처리 부문에는 적용업무의 개발 및 보수를 수행할 그룹과 적용업무를 운용하며 사용자의 요구에 합치하도록 하드웨어와 소프트웨어의 변경을 실행하는 운용 그룹이 있다. 또 사용자에 대한 개인용 컴퓨터와, 사무자동화의 기술적 지원을 하고 사용자의 의문 및 질문에 답해 줄 Help Desk로서의 정보 센타가 있다. 정보처리 부문은 주관부문의 지시에 따라, 주관부문과 사용자 부문에 대해 서비스를 제공할 역할이 있으며, 다음을 실행할 책임이 있다.

- 모든 정보통신망 시스템의 안전관리를 행한다.
- 각 적용업무가 서로 간섭받지 않고 다른 시스템으로부터도 간섭받지 않음을 확인한다.
- 각 정보자산을 주관부문이 규정한 취급방법에 따라 관리한다. 예를 들어 기밀정보는 그 기밀도 구분에 따른 액세스 관리를 실시한다.
- 사용자에 대해 가동시간대(적용업무의 서비스 시간) 등을 알려 놓는다.
- 하드웨어와 소프트웨어의 변경에 따른 환경의 변화를 파악하고, Capacity 조정을 행한다. 예를 들면, 환경이 변화했을 때 On-line 의 응답시간이 길어지지 않도록 조치를 강구한다.

바. 시큐리티 부서

조직 내의 보안을 위한 시큐리티 기능을 갖기 위해 시큐리티 담당 부서는 조직 내에서 다음과 같은 기본 기능을 행하여야 한다.

- 시큐리티 통제에 관한 제안
- 시큐리티 자체 평가
- 통제의 시행에 있어서의 보조
- 사용자, 관리자에게의 시큐리티 교육
- 시큐리티 정책, 기준, 가이드라인의 제공
- 시스템 개발에의 참가
- 컨틴전시 계획 : 예상되는 각각의 긴급상황에 대응할 수 있는 방안들에 대해 구체적인 계획을 수립한다.
- 시큐리티 경영(예 : ID, Password관리)
- 불법적행위, 횡령 등의 발견과 사전대비
- 시큐리티에 관한 책임과 직무를 설정, 유지, 변경
- 대상이 되는 시큐리티 환경의 체크
- 조직 시큐리티와 관련된 제품, 용역의 선정과 평가

사. 시큐리티 부서장

- 조직전체의 시큐리티 목표에 준하여 부문수준의 시큐리티 목표를 선정한다.
- 조직차원의 명령, 회사 정책을 기반으로 시큐리티 부문의 시큐리티 시행 세칙, 명령, 지침 등을 만든다.
- 제안된 시큐리티 부문의 정보처리 자산 보호에 관한 기준, 명령, 지침의 시행안을 검토한다.
- 조직 시큐리티 문제에 관해 부문수준의 중심점 역할을 한다.
- 정보처리 자산 보호에 관해 감사를 한다.
- 시큐리티의 실행을 위해 사용될 정보처리 시스템을 추천한다.
- 정보처리 자산 보호의 책임, 요구에 관해 시큐리티 스탭, 정보처리 서비스 사용자, 정보처리 자산 소유자들이 효과적인 교육과 방향을 공급받는 지를 확인한다.
- 시행되는 시큐리티 시스템의 효율성을 검토한다.

6. 맺는말

현재의 정보통신망의 기본 설계 이념은 주로 작업 효율성 향상에만 치중되어 왔기때문에 안전/신뢰성의 취약점이 자주 발생한다. 예를 들어 사용자 위주 시스템(User friendly system)

은 정당한 사용자에게만 친절한 것이 아니라 부정 사용자에게도 친절하여 부정사용에 필요한 많은 정보를 제공한다. 또한 사용자의 편의 및 작업능률 향상을 위해서 때로는 기본적 보안수칙을 생략하기도 한다. 또 무리한 인원감축을 도모하다 보면 직원들간의 사무가 적절히 분리되지 못하여 내부관리제도가 확립되지 못하고 보안에 관한 책임의 한계가 불분명하여지기도 한다. 컴퓨터 사용자는 업무처리의 속도를 향상시키기 위하여 또는 보안에 관한 인식부족으로 너무 짧거나 너무 자명한 패스워드를 쓰기도 하며 오랫동안 패스워드를 바꾸지 않기도 한다.

하드웨어, 소프트웨어, 그리고 사용자 및 관리자등으로 구성되어 있는 정보통신망에 있어서 안전/신뢰성 문제는 매우 복합적인 성격을 갖고 있다. HW 나 SW 를 통한 기술적인 대책뿐 아니라 사용자 및 관리자 등에 대한 경영관리적 대책과 안전/신뢰성에 대한 의식교육 등 매우 다각적인 관점에서 이 문제를 접근해야 할 필요가 있다. 이러한 대책들이 상호조화를 이루지 못한다면 아무리 첨단의 기술을 도입한다 하더라도 종이벽에 철문을 다는 격을 벗어날 수 없을 것이다. 또 이러한 대책은 어디까지나 대상 정보통신망에 맞추어 알맞게 도입되어야 할 것이다. 정보통신망 안전/신뢰성 문제의 과대평가는 과소평가 못지않게 바람직하지 못한 것이기 때문이다.

김 세 헌

1972 서울대학교 물리학과 졸
1981 미 Stanford 대학 경영과학과 석사,박사
1981~82 미 Systems control 사 근무
1982~현 한국과학기술원 경영과학과 조교수,부교수,정교수
1990~91 한국경영과학회 편집위원장
1991~92 통신정보보호학회 편집위원장