韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

情報의 기밀등급 分類 方法의 概要

金 世 憲*

정보 보안의 주요 요소는 인가되지 않은 사람이 시스템에 액세스(Access) 하거나 인가없이 사용하는 것을 방지하는 액세스 통제이다. 이를 위해서 정보의 기밀정도에 따라 보호정도를 결정하는 기밀등급분류가 이루어져 정보를 선택관리하는 체계가 이루어 져야한다. 정보를 선택관하기 위해서는 보호할 만한 정보를 식별하고, 식별된 중요정보를 어떤 방법으로 유지, 관리, 이용할 것인지를 규정하는 것이 필요하다. 본 논문에서는 정보 기밀등급의 체계적인 분류방법에 대해 살펴보기로 한다.

1. 보호 대상

원칙적으로 조직운영에 부정적인 영향을 끼칠 수 있는 정보는 누출되어져서는 아니된다. 이것이 명백히 경영층의 임무임은 자명하다. 그러나 경영층의 가이드라인이 정보에 대한 지나친 보안(Overclassfication) 이나, 너무 허술한 보안(Underclassification)의 오류에 빠져서도 아니된다. 경영층은 모든 조직데이타의 가치를 적절히 인식하고 그것의 보호를 위한 대책을 강구해야 한다.

경영정보중 일부는 성격상 민감한 특성을 가질 수 있는데 예를 들면 생산 및 마아케팅 데이타, 재무계획 및 그 결과 등이다. 또, 영업기밀의 경우 그 보호 책임은 경영층 및 종업원 모두에게 부과되도록 해야한다. 상황에 따라서는 데이타의 발생자(Originator) 만이 데이타의 민감성 여부를 알 수 있는 경우가 있게 되는데, 이 경우 정보기밀 분류에 있어 그 정도와 민감도를 데이타의 발생자로 하여금 결정토록 규정할 수 있다[5].

경영정보의 대부분이 그리 민감하지 않은 경우 직원의 불편 및 불필요한 지출을 피하기 위해 이러한 데이타를 분류하지 않을 수가 있는데, 경영층은 무엇보다도 이러한 데이타 관리가 문제점임을 인식해야 한다. 왜냐하면 경영정보에 대한 관리 및 통제의 부재는 전혀 예기치 않은 결과를 초래할 수 있기 때문이다. 공개되어 있지 않다고 판단되는 데이타들을 적절한 분류체계에 따라서 분류하고 또 이러한 데이타가 권한이 있는 사람에 의해서만 접근될 수 있도록 정보분류 체계가 개발되면 불확실성과 위험이 매우 감소하게 된다.

일반적으로 보호를 필요로하는 정보는 다음과 같다.

- 노출되어졌거나 누출되어졌을 때 그 조직에 영향이 큰 정보(예를 들면 기업의 영업전략정보, 신제품개발에 관계된 정보, 장기계획정보 등)
- 파괴되어졌을 때 조직의 존망에 관계된 정보(예를 들면, 외상대금정보, 고객정보 등)

* 정회원, 韓國科學技術院 經營科學科

• 허위로 수정되어졌을 때, 조직과 사회에 중대한 영향을 미치는 정보(예를 들면, 금융기관에 예금대장, 의료기관의 정보, 개인정보 등).

2. 기밀의 분류형태

보호할만한 정보가 무엇인지 명확하게 된 다음에는 각각의 정보를 어떤 정도로 보호할 것인지 결정하여야 한다. 이를 위해서는 각각의 정보가 누출되어졌을 경우의 영향도에 따라서 기밀도를 구분하여 차등적으로 보호정도를 결정하는 것이 바람직하다. 기밀정보로 취급되지 않는 정보는 일반정보로 분류되며 이는 외부에 발표되어진 정보, 조직내 행사의 공고, 서점에서 입수가능한 책에 기재되어 있는 정보 등이 있는데, 외부에 누출되어져도 업무수행에 지장이 없고, 생각해보면 충분히 알 수 있는 정보들을 포함한다.

가. 취급 허용범위 기준 분류

이 방법은 취급 허용범위 기준으로 정보를 분류하는 방법으로서 대개 다음의 4가지로 구분된다.

1) 극비 정보

극비로 구분되는 정보는 조직체에 있어서의 최고기밀로서, 누출되어졌을 경우 조직의 존망에 영향을 줄 만한 정보이다. 예를 들면 미발표제품에 관계된 성능, 가격, 발표기일, 단기/장기의 영업전략 등이 여기에 해당한다. 이 극비정보는 취급시 특별한 배려를 요하는데, 이 정보를 취급하는 자의 이름을 기록하고 해당정보에는 각각 등록번호를 부착할 필요가 있다.

2) 부외비 정보

부외비로 구분되는 정보는 그 정보의 내용으로 보아, 업무상 필요로하는 사람(조직내에서 맡은 역할과 지위에는 관계없이 Need-to-know[3]의 원칙에 따라) 에게만 한정할 만한 것들이다. 이러한 것으로는 제조관계의 제 원장, 가격설정 정보, 인사고과표, 급여표, 인사기록정보 등이 있다.

3) 대외비 정보

대외비로 구분되는 정보는 기업의 소유권, 직원의 권리보호, 사업상 판단하기에 그 사용을 조직내로 한정해야 할 것 등인데, 예를 들면, 각종 규정, 조직내에서 사용할 핸드북(Handbook) 등이 여기에 해당한다.

4) 일반 정보

비밀로 취급할 필요가 없는 기타 정보들이다.

나. 중요도 기준 분류

이 방법은 정보를 중요도에 따라 구분하는 방법으로서 미국 국방성에서 사용되어오던 분류체계를 민간산업체에 적당하도록 재편성한 것이다[4].

1) 1급(Secret)

여기에 해당하는 정보는 전략적 성질의 정보이다. 따라서 노출이 되면 조직에 심각한 손실을 초래할 수 있는 정보로서 조직의 재정적 타격 및 총 업무효과의 5% 이상의 감소를 일으킬 만한 정보이다.

2) 2급(Confidential)

경영층에게만 이용가능한 정보로서 이외의 사람에게 노출되면 조직의 총 업무효과의 1−5%의 감소를 초래할 만한 정보이다.

3) 3급(Private)

조직내의 구성원의 관련된 것으로 조직밖의 사람에게 노출되면 않되는 정보로서 조직의 윤리강령 및 조직구성원의 프라이버시권에 관계된 정보이다.

4) 일반 정보

위의 그룹에 속하지 않는 정보를 일반정보로 분류한다.

3. 기밀 분류 기법

가. 분류 결정 행렬(Classification Determination Matrix)의 방법[6]

이 방법을 이해하기 위해 다음 표를 보자. 여기

표 1. 정보의 구성요인과 할당가치

양식	영역	성격	시의성	노출 코스트	노출위험
Final 3	Marketing 3	Strategic 8	Current 3	High 8	High 3
Partial 2	Financial 2	Business 4	Archival 1	Medium 5	Limited 2
Raw 1	Personnel 1	Customer 2	N/A 0	Low 1	Almost
	Other 0	Staff 1			None 1
		Nil 0			

에는 정보를 구성하는 각 구성 요인과 해당가치들이 할당되어 있다. 정보에 대한 구성요인은 크게 6가지로 나뉘어져 있다. 위 표 1은 정보의 구성요인과 할당 가치를 예로 든 것이다.

최종 데이타는 원시 데이타보다 높은 스코어를 할당받는다. 또 현재의 데이타는 오래된 데이타보다는 역시 높은 스코어를 할당시킨다. 노출 코스트(Cost of Exposure)의 경우 고(High), 중(Medium), 저(Low)로 나누어져 있는데, 높은 경우는 추정되는 손실이 조직의 총 업무효과의 5%를 초과하는 경우이며, 중인 경우는 그 코스트가 총 업무효과의 1%~2% 사이일 경우이며, 저인 경우는 1% 미만일 경우이다. 이들 각각에 대해 스코어는 8, 5, 1로 할당된다. 이와 같은 방법으로 각 요인별로 할당된 스코어의 합이 그 정보의 가치가 된다.

이렇게 해서 각 정보의 가치를 계산하여 기밀등급을 정하게 되는데 해당분류의 기준은 예를 들어 다음과 같이 이루어진다.

표 2. 분류기준

총 가치	분류
22-28	1급
15-21	2급
6-14	3급
0-5	일반

위의 접근방법을 이용해서 다음 각 정보에 대해 구체적으로 평가를 내려보자.

Z=워드프로세싱을 위한 훈련

Y=퇴직연금 분담 평균액

X=제품 판매전략 및 기대수익(곧 공개될 정보)

W=새로운 회사의 인수 후 조직의 재정적 상황에 대한 예측

이들 각각의 정보에 대해 분류 결정행렬을 이용한 기밀도 분류가 아래 표에 정리되어 있다.

표 3. 기밀도 분류의 예

정보	양식	영역	성격	시의성	노출 코스트	노출위험	총가치	분류
Z	1	0	0	0	1	1	3	일반
Y	3	1	1	3	1	1	10	3급
X	3	3	4	3	5	2	20	2급
W	2	2	8	3	8	3	26	1급

나. Schweitzer의 Rule-based 분류방법[7]

앞에서 논의한 방법은 분류 작업자의 판단에 크게 의존하며 정보의 가치(스코어의 합계)는 조직전반에 걸쳐 이 정보가 가지는 각 요인에 대한 효과의 합이다. 그러나 이 방법은 정보분류에 있어 효과적일 수는 있으나 여러 요인간의 상호작용을 충분히 설명하지는 못하고 있다. 또한 위의 분류 결정 행

렬에 새로운 요인이 추가될 때 이것은 현재의 요인들에 영향을 미쳐 분류행렬의 재구축이 필요하게 된다. 이와 같은 한계를 어느정도 극복하기 위한 대안으로 Rule-based 분류방법이 있다.

여기서는 각 정보에 대한 분류에 사용될 룰(Rule)을 문서화한다. 이 룰들은 여러 요인들의 결합으로 구성된다. 표 4에는 1급 기밀을 규정해주는 룰들이 열거되어 있다. 예를 들어 룰 9는 다음과 같은 의미이다.

IF(Strategic) AND(Medium Cost) AND(Current) AND(High Risk) AND NOT(Raw) THEN Classification=Secret.

표 4. 1급 기밀에 해당하는 룰의 예

룰	성격	노출 코스트	시의성	노출위험	영역	양식
1	Strategic	High	Current			
2	Strategic	High		High		
3	Strategic	High			Marketing	
4	Strategic	High				Final
5	Strategic	High		Limited	Financial	
6	Strategic	High		Limited		Partial
7	Strategic	High			Financial	Partial
8	Strategic	Medium	Current	High	not Personnel	
9	Strategic	Medium	Current	High		not Raw
10	Strategic	Medium	Current		Marketing	not Raw
11	Strategic	Medium	Current	not Low	Marketing	
12	Strategic	Medium	Current	not Low		Final
13	Strategic	Medium	Current		not Personnel	Final
14	Business	High	Current		Marketing	Final
15	Business	High	Current	High	Marketing	
16	Business	High	Current	High		Final
17	Business	High		High	Marketing	Final
18	Strategic	Medium	Archival	not A/None	Marketing	Final
19	Strategic	Medium	Archival	High	not Personnel	Final
18	Strategic	Medium	Archival	High	Marketing	not Raw

이 Rule-based 방법은 상당히 많은 이점을 가지고 있는데, 특히 룰의 변경과 등급내에서의 민감도를 규정하는 데에 있어 신축성을 가지고 있다. 룰의 수정과 새로운 요인의 도입 등이, 앞의 분류행렬에서 가중치와 각 등급에 해당하는 점수범위를 변화시키는 것보다 더욱 용이하게 이루어 질 수 있다.

4. 기밀정보 취급방법

대외비이상으로 기밀구분된 정보는 모든 데이타에 기밀로 구분의 라벨을 부착 또는 인쇄하거나, CRT 화면의 일부에 그 구분내용을 표시할 필요가 있다. 기밀도 구분의 라벨이 항상 보이게 함으로써

그 정보를 취급하는 사람의 주위를 환기시켜 규정에 따라 취급하도록 하는 것이다. 한가지 고려할 점은 인쇄출력된 인쇄물의 경우에는 전체의 기밀도 구분이 표지에 인쇄되겠지만 페이지들 마다도 반드시 표지와 동일하게 기밀도 구분을하여 어느 페이지만을 뽑아 사용할 때에도 기밀도 구분이 표시되어 있어서 그것에 맞게 취급할 수 있어야 한다.

출력된 인쇄물, Micro fiche 등의 하드카피의 보관방법은 부외비 이상에는 자물쇠가 있는 서고 등에 보관한다. 또 극비정보는 시큐리티 구역(특별히 시큐리티를 확보하기 위해 지정된 구역)의 자물쇠 달린 보관고, 혹은 이중 장치로된 보관고 등 시큐리티 규정에 따라 보관 관리한다.

정보 액세스의 허가는 부외비이상은 정보의 주관부문에 개별적으로 허가를 신청해서 승인을 받을 필요가 있다. 극비정보의 액세스에 있어 운영부문의 조치로는 액세스의 일지를 만들어, 액세스의 검토가 이루어질 수 있도록 흔적을 남길 의무가 있다.

정보의 복사 권한은 정보의 주관부문이 승인한다. 부외비 이상의 정보의 경우, 그것을 가지고 있는(관리를 위탁받은) 사람의 승인을 얻어 이루어지도록 한다. 이 극비정보는 주관부서로부터 승인받은 특별한 사원이외에는 복사할 수 없도록 규정한다. 극비문서가 문서류인 경우 "복사불허"라는 문자를 새겨두도록 한다.

구내우편의 경우, 일반우편과 부외비 이상의 우편을 서로 구분할 수 있도록 된 봉투를 사용한다. 또 우송 중에 개봉되어진 경우, 최종 수령자가 이를 알아차릴 수 있도록 Seal 등을 사용해 재봉합이 될 수 없도록 한다. 극비정보의 경우 상대방이 확실히 수령했다는 증거를 남기도록 하는 대책을 강구해 둔다. 구내우편이 아닌것을 사용할 시에는 구내우편과는 달리, 얼핏 보아서는 기밀정보임을 알 수 없도록 할 필요가 있으며, 수령자가 개봉했을 시에도 기밀정보가 그대로 보이지 않도록 이중봉합할 필요가 있다.

기밀정보의 휴대이동에 있어서는, 이동중에 도난, 분실 등의 사태를 방지하기 위해 원칙적으로 휴대이동을 금지한다. 그러나, 완전히 금지하다보면 업무의 수행이 원활하지 않게 될 우려도 있으므로, 기밀정보 휴대이동에 관한 주의규정(전철, 택시, 항공기이용 등)을 둔다.

정보의 폐기처분을 가볍게 여겨서는 아니된다. 부외비 이상의 정보인 경우에는, 소각 혹은 세밀하게 잘라 없앤다. 자기매체의 경우에는 재사용이 불가능하도록 물리적으로 파괴한다. 이 모든것에 폐기수속규정을 두어 이에 따르도록 한다. 특히 이 습관을 전직원이 직접 익힐 수 있도록 하는 것이 필요하다.

매체의 전자기록의 경우, 내용이 중요하지 않게 된 때에도 매체 자체는 필요할 때 재사용이 가능하다. 그러나 부외비 이상의 정보를 담고 있는 매체인 경우에 그 정보가 불필요하게 된 때에는 무의미한 데이타를 써놓거나, 자기를 말소시키는 장치를 사용함으로써 기밀정보를 확실히 말소시킬 수단을 강구해 두어야 한다.

5. 기밀도 구분의 변경 및 유효성기간

기밀도 구분은 전술한 바와같이 주관부문이 결정하는 것이고 정보를 사용하고 있는 사용자가 정보의 가치가 없다고 판단해도 주관부문이 기밀도 구분의 변경을 통지하지 않는 한 멋대로 기밀도를 변경하는 것은 있을 수 없으며, 그 기밀도는 영원히 유효하게 계속된다. 10년전에 작성된 데이타와 금일 작성된 데이타가 기밀도가 같다면 옛 것이든 새로운 것이든 관계없이 취급은 동일하다.

또, 신제품의 정보와 같이 발표전에는 조직 밖은 물론 조직안에서도 필요이외의 사원들에 대해서 기밀로 취급되다가 발표가 되어 기밀로 취급될 필요가 없는 정보인 경우, 몇월 몇일까지 혹은 발표할 때까지 기밀로 취급된 것임을 명시할 필요성이 있다. 이 조치를 강구하지 않으면 일반에 공개된 정보가 사내에서는 그대로 기밀로 취급되는 상태의 정보가 되어 취급에 모순이 발생케 된다. 불필요해진 기밀정보를 많이 가지게 되면 보관관리규정에 따라 관리하기위해 보관장소를 많이 필요로 하는 등 여러가지 면에서 효율성을 저하시킬 가능성이 많다. 기밀의 특성을 잃어버려서 보호의 필요성이

없는 정보는 즉시 폐기수속을 취해 말소하는 것이 중요하다.

조직체에 있어 대부분의 경우 기밀도 구분이 있다고 생각되지만 그 조직에 소속한 모든 사람이 그것을 알고 있는 경우는 적다. 기밀구분의 의미를 해설하고, 기밀도구분을 부착, 그것을 조직내에 철저히 인식시키는 것이야말로 시큐리티에 관한 관심을 고양시키는 중요한 방법이라고 할 수 있다.

참 고 문 헌

1. 김세헌, 컴퓨터 범죄와 프라이버시 침해, 희성출판사, 1989

2. 김세헌, 정보통신망의 정보보안체계 설계에 대한 종합적 연구, 89' 전기통신학술연구과제

3. Kcenig, R. C., "Advances in Information Classification," *Computer Security and Privacy Symposium Proceedings*, DM 35, Honeywell Information Systems, Phoenix, Ariz., Apr. 15-16, 1980

4. *Industrial Security Manual for Safeguarding Classified Information*, DOD 5220. 22-M, Superintendent of Documents, U.S. Goverment Printing Office, Washington, D.C. January, 1983

5. Lobel, J., *Foiling the System Breakers*, McGraw-Hill, New York, 1986

6. Feuerlicht, J. and P. Grattan, "The Role of Classification of Information in Controlling Data Proliferation in End-User Personal Computer Environment," *Computers and Security*, Vol. 8, pp.59-66, 1989

7. Schweitzer, J.A., *Protecting Information in the Electronic Workplace-A Guide for Managers*, Reston, 1983

□ 著者紹介

김 세 헌(正會員)

서울文理大 物理學科 卒業
美 Standford大(經營科學 碩士 및 博士)
美 System control, Inc社 勤務
現 韓國科學技術院 經營科學科 教授, 本 學會 編輯委員長
關心分野 : 컴퓨터 犯罪와 프라이버시 侵害 防止 對策, 情報시스템 保安, 暗號學