通信情報保護學會誌
第2卷 第3號, 1992. 9

정보보호 개념의 재정립에 관한 소고

남 길 현*

최근 국가기간 전상망사업이 활발히 진행되고 있으며, 각 기업체를 비롯한 사회 각 분야에 컴퓨터와 함께 대량정보유통체계가 확립되어 가고 있는 시점에서 정보보호에 관한 기능과 위협형태 그리고 대응책을 살펴보고 서로 상이한 그룹의 사용자 입장에서 정보보호 요소에 대한 우선순위를 고려함으로써 전반적인 개념을 다시한번 정리해 보는 것도 의미있는 일이라고 생각된다.

본고는 한국전자통신연구소의 1991년도 연구보고서 "선진국 데이타보호 기술동향 분석"의 일부분을 발췌하여 새롭게 정리한 것이다.

1. 정보기술과 정보보호

정보기술과 정보보호 분야는 사실상 그 내용면에서 다르지만 지금까지 정보보호에 대한 개발은 순수하게 기술적인 문제를 언급함으로써 정보기술 분야와 동일하게 발전되어 왔다. 정보기술 분야는 정보보호 분야와는 달리 시스템이 요구하지 않는 다른 방법을 사용하는 잠재적인 적(enemy)이나, 복잡한 논리상의 문제로부터 위협을 받고 있지 않지만, 정보를 보호하는 보안 측면에서는 시스템내에서의 우연 또는 고의적으로 고장이나 정보손실을 발생시키는 능동적이고, 예측할 수 없으며, 인위적인 적의 도전을 추가해야 한다. 또한 정보기술은 생산성에 기여를 하고 기술의 성공 여부에 직접적인 영향을 주며 정보분야의 주를 이루고 있기 때문에 많은 사람들이 관여하고 있지만, 정보보호는 생산성을 감소시키고 효과를 기대하기 어려우며 애매한 점이 많은 분야이기 때문에 사람들이 싫어하는 경향이 있다.

정보기술과 정보보호 분야가 이와같이 상반된 분야임에도 불구하고 기술적인 전문가나 시스템의 관리자는 시스템의 정보손실에 대한 경험이 없고 보안에 대한 훈련이 되지 않았을지라도 어떻게 해서든지 적으로부터 정보를 보호할 책임을 갖고 있다. 그들은 공격하는 적들의 의도나 행동에 대한 정보도 거의 없으며, 사용자들의 정보보호에 대한 요구사항이 무엇인지도 잘 모르면서 무조건 정보보호만을 요구받게 된다.

결과적으로 보안에 관여하는 기술자나 설계자는 그들이 가지고 있는 정보 시스템, 기술, 지식만을 가지고 정보보호를 위한 시스템 제어장치를 만드는 경향이 있으며, 이러한 제어장치는 단지 그들이 상상할 수 있는 적과 제한적이며 이상적인 공격에 대해서만 보호를 하고 미지의 가능한 모든 적과 공격방법에 대해서는 고려할 수가 없게 된다. 이러한 예로서 미국 NCSC(National Computer Security Center)에서 제시한 TCSEC(Trusted Computer

* 정회원, 국방대학원

Systems Evaluation Criteria)을 생각해 보자. TCSEC에서 규정한 특정 수준의 컴퓨터에 침입하여 정보를 알아내고자 하는 적이 만약에 실패해서 들어가지 못하게 되면 대신 정보를 아주 파괴하는 쪽으로 목표를 바꿀 수 있으며, 이는 훨씬 더 큰 피해를 초래할 수도 있는 것이다. 그러나 TCSEC은 시스템 설계시에 비밀성이 떨어지지 않도록 하는데만 강조를 하고 정보를 파괴하거나 가용성이 떨어지는 문제는 크게 고려하지 않았으며 더욱이 정당한 권한이 있는 사람이 시스템 잘못으로 사용을 못하는 경우는 전혀 무시하고 있다. 즉, 자동차 도둑을 방지하기 위하여 문이 절대로 열리지 않도록 해 놓으면 도둑은 창문을 부수기 때문에 오히려 큰 손실을 볼 수 있다는 사실을 간과하고 있으며, 혹시 차 주인이 키를 잃어 차속에 놓고 문을 잠근 경우에는 열쇠가 너무 견고하여 주인도 상당기간동안 차를 쓸 수 없다는 사실을 무시한 경우와 비슷한 것이다.

따라서 정보보호가 너무나 정보기술에만 종속되어 기술적인 사항만으로써 모든 문제를 해결하려고 해서는 안된다고 볼 수 있다.

2. 일반적인 정보보호 개념

정보보호에 대한 일반적인 정의는 정보의 비밀성(Confidentiality) 무결성(Integrity), 가용성(Availability)을 유지하는 것이며, 가용성 대신에 지속성(Continuity)을 말하기도 한다. 여기에 추가해서 정보의 손실은 일반적으로 변조, 파괴, 누출, 사용의 네가지 경우로부터 발생한다고 말한다. 정보보호 세가지 요소는 네가지의 정보손실과 대응되는데 예를 들어, 비밀성은 정보의 누출과 관련이 있고 무결성은 변조, 파괴와 연관성을 갖고 있다. 또한 이러한 정보보호의 요소와 정보손실의 유형은 수년동안 완전하고, 포괄적이며, 적절한 것으로 여겨져 왔다. 이들에 대해서 좀더 자세하게 알아보면 다음과 같다.

2.1 정보보호 요소

(1) 비밀성

비밀성은 정보가 외부로 노출되지 않은 상태를 의미하며 정보에 대한 접근이 허용되지 않은 사람이나 프로세서 등에 의해서 인식되지 않아야 한다. 비밀성을 유지하기 위해서는 권한이 없는 사용자나 프로세서가 데이타를 이용할 수 없도록 제어하여야 하며 이를 위한 기본 메카니즘으로는 DAC(Discretionary Access Control)과 MAC(Mandatory Access Control)등을 이용하는 접근제어 방식과 암호방식 등이 있다.

지금까지 연구 결과로 인해 비밀성을 유지하기 위한 보호대책은 상당한 수준에 있다고 볼 수 있으며, 컴퓨터 네트워크에서는 아직 실현이 되지 않았지만 적어도 간단한 컴퓨터 시스템에서는 정보보호 방법이 가용하다고 본다. 비밀성의 수준을 구체적으로 제시한 예가 미국의 TCSEC과 유럽의 ITSEC등이 있다.

(2) 무결성

무결성은 허가되지 않은 자에 의한 정보의 변조를 막는 것을 말하며, 무결성에 문제가 발생할 경우에는 정보가 변조된 상태로 계속 사용하게 될 수 있다. 무결성을 위한 메카니즘으로는 물리적 통제와 접근제어 등 여러가지 방법을 생각할 수 있으나 이미 변경되었거나 변경될 위험이 있는 경우 이를 탐지 또는 검출 할 수 있는 메카니즘과 복구를 위한 메카니즘이 무결성 제공을 위한 요소가 된다.

(3) 가용성

가용성이란 정보가 분실되지 않고 항상 존재하며 획득 가능한 상태를 뜻하는 것으로 어떤 목적에 필요할 때 즉시 사용할 수 있음을 의미한다. 즉 가용성은 특정 목적상 필요할 때 특정 시간과 장소에서 즉각 사용할 수 있도록 준비되어 있음을 뜻하며 실용성이 있느냐와는 별로 무관하다고 볼 수 있다. 이러한 의미에서 가용성은 회복기법과 백업을 위해서 필요한 것을 제외하고는 보안성 요구특성과는 별로 관계 없는 것으로 인식되어 보안대책에서는 무시되는 경우가 많았다.

가용성을 유지하는데 도움을 주는 중요한 요소는 중복성 유지(redundancy), 데이타의 백업, 물리적 위험요소로부터의 보호 등이다. 시스템이 가용성을 유지하지 못하면 데이타가 파괴될 수 있다.

2.2 위협 형태

정보보호에 대한 일반적인 개념으로 여겨졌던 비밀성, 무결성, 가용성은 여러형태의 위협을 받으며, 이러한 위협으로부터 데이타를 보호하는데 주력해 왔다. 즉, 비밀성, 무결성, 가용성을 위협하는 형태는 비인가지에 대한 정보 누출(Disclosure), 수정(Modification), 파괴(Destruction), 사용(Use) 등이 있다.

(1) 정보누출

정보누출은 정보보호 시스템이 일차적으로 비밀성을 제공하지 못할 때 발생하는 현상으로 인가된 사람 외에 정보가 전파되는 것을 말한다. 그러나 비밀자료라고 여기는 정보도 사용자가 정보의 내용을 변경시킨다면 그러한 변경이 응용프로그램을 통하여 보호로부터 제외시키도록 할 수 있기 때문에 비밀성을 잃을 수가 있다. 즉, 비밀정책을 위반하지 않고도 다른 방법으로 비밀성을 잃게 할 수 있는 것이다.

(2) 수 정

수정은 정보의 내용을 부당하게 바꾸는 행위를 말하며, 발견되지 않을 경우에는 계속 정확한 정보로 여겨진다. 정보를 불법적으로 수정할 수 있다는 것은 무결성을 유지하기 위한 정책에 문제가 있다는 것을 의미하지만 이는 정보를 실제로 노출시키지 않은 상태로 비밀성을 위협할 수도 있다. 그리하여 정보의 내용을 모르는 상태에서 바꾸었을지라도 비밀성을 잃을 수가 있다.

(3) 파 괴

파괴는 정보의 형태나 내용을 알아보지 못하게 하는 행위를 말하며 정보보호의 요소 중에서 일차적으로 가용성에 대응되는 개념이다.

(4) 사 용

사용자가 정보를 잘못 사용함으로써 비밀성을 위협하거나 정당한 사용자가 정보를 사용할려고 할 경우 정보가 침해되어 사용할 수가 없는 경우가 있다. 이와 같이 정보를 잘못 사용하거나 사용할 수 없는 경우도 정보보호에 대한 위협으로 간주된다.

2.3 보호 대책

정보보호의 요소인 비밀성, 무결성, 가용성을 유지하기 위해서는 예방(Prevention), 탐지(Detection), 회복(Recovery) 등의 기법을 사용하여 이들의 위협요소로부터 정보를 보호하기 위한 보호대책이 필요하다.

(1) 예 방

정보를 침해하는 행위에 대해서는 사전에 예방을 해야 한다. 그러기 위해서는 권한이 있는 자에게만 접근 또는 복사 등의 행위를 허용하도록 접근 제어 기법을 사용하고 내용이 외부로 노출되어도 비밀성을 유지하기 위해서 암호화를 시켜 놓는다. 또는 잠금장치를 통해서 물리적, 기술적으로 정보를 보호할 수 있도록 한다.

(2) 탐 지

정보가 이미 불법적인 방법으로 변형이 되었다면 시스템은 이를 탐지하여 정보의 무결성을 유지해야 한다. 그렇지 않을 경우에는 잘못된 정보가 정확한 정보로 인식되어 피해를 받을 우려가 있다. 정보의 무결성을 유지하기 위한 탐지 기법으로는 체크비트, 일련번호, 누락 데이타의 체크, 테스팅 등의 방법이 있다.

(3) 회 복

정보에 대한 가용성을 유지하기 위해서는 부당하게 변형 또는 손실된 정보가 원래의 상태대로 회복될 수 있어야 한다. 이를 위해서 백업, 회복 계획, 중복성 유지 등의 방법을 이용할 수 있다.

2.4 문 제 점

지금까지 완전하다고 여겨왔던 세가지의 정보보호 요소, 네가지의 위협형태, 정보보호대책 등 이와같은 개념은 사실상 완전하다고 볼 수 없으며, 너무 단순하고 일관성을 유지하기 어려우며 다음과 같은 문제점을 내포하고 있다.

(1) 정보보호 요소, 위협 형태, 보호대책에 대한 명확한 정의가 되어 있지 않고 지금까지 생각했던 바와 같이 서로 일대일 대응관계가 이루어지지 않으며 중복되어 나타난다. 이에 대해서는 기존의 정보보호 요소에 대한 개념을 확장해서 보완할 수도 있겠지만 이미 잘못된 상태로 널리 사용되어 왔기

때문에 다시 적절히 정의하기가 곤란하다.

(2) 완전하다고 여겨왔던 정보보호가 보안의 부분적인 면만을 만족해 왔다. 예를 들어, 비밀성을 유지하는 TCSEC의 경우 시스템의 가용성을 저하시키며, Clark-Wilson Integrity System의 경우 정보의 비밀성을 손상시킨다.

(3) 가용성은 단지 정보를 사용할 수 있는 가능성을 제공하는것만 언급하였고, 어떤 목적을 달성하기 위한 실용성(Utility)에 대해서는 언급하지 않았다. 따라서 사용여건을 제공할 뿐만 아니라 정보의 실용성을 유지할 수 있는 또다른 정보보호 요소가 필요하다.

(4) 무결성에 대한 지금까지의 정의는 "잘 정비되고 통제된 방법으로만 데이타를 변경시키도록 보장하는 것"이라고 하였는데, 이는 부분적인 정의에 불과하다. 정보의 사실성에 확신을 가질 수 있는 인증에 대해서는 정보보호 요소에서 언급되어 있지 않다. 또한 무결성은 환경이 변한다면 데이타가 변하지 않더라도 손상될 수 있다.

3. 새로운 정보보호 개념 정립

앞에서 설명한 문제점을 해결하기 위한 방안으로는 기존의 정보보호 요소에 사실 여부를 확인하는 인증성(Authenticity)과 목적에 부합될 수 있는 정보를 편리하게 제공하는 실용성(Utility)을 추가하고 위협 형태도 다른 방향에서 분석함으로써 해결할 수 있다. 또한 무결성에 대한 정의는 "완전성(Completenss), 전체성(Wholeness), 건전성(Sound), 손상되지 않은 상태의 유지"의 뜻을 갖는 일반적이고 좀 더 명확한 의미를 부여함으로써 무결성에 대한 포괄적인 의미를 가질 수 있도록 해야 한다. 위협 형태는 다섯가지의 새로운 정보보호 요소에 대응되는 위협 형태를 설정하고 정보보호 대책 방안에도 새로운 기능들을 추가해야 한다. 컴퓨터 시스템은 보안성을 요구하는 수준에 따라서 하나 또는 둘 이상의 정보보호 요소를 혼합적용해야 한다. 이와같이 정보보호 요소의 미비점을 보완하기 위해 인증성과 실용성을 추가함으로써 세가지 정보보호 요소의 개념을 확장하여 문제점을 해결하려고 하는 시도는 필요없게 된다.

3.1 정보보호 요소와 위협 형태

위협 형태는 모든 인간이 생각하고 행동하는 만큼이나 복잡하며, 이러한 생각과 행동은 고의 또는 무의식적으로 위협을 야기시킬 수 있다. 위협 형태를 분류하기 위해서는 불완전하지만 간접적인 영향을 미치는 위협은 고려하지 않음으로서 분류가 가능하다. 이미 알려진 위협 형태로부터 정보를 보호할 수 있는 방법을 개발하면 지능적이고 새로운 형태의 위협이 다시 나타날 것이며, 따라서 우리는 항상 새로운 문제에 부딪칠 것이다.

흔히 보안은 변조, 파괴, 노출, 불필요한 사용 등의 구체화된 위협으로부터 보호하는 것으로 여겨왔다. 그러나 사보타지(Sabotage)에 의한 기계설비의 파괴나 탈취, 잘못 표현된 규정을 나쁜 방향으로 이용하는 것, 컴퓨터 사용을 지연시키거나 연기시켜서 실제적으로 사용을 거부하는 일, 또는 추론 등 지금까지 설명한 네가지 위협으로부터 유도되지 않는 분야가 존재한다. 또한 보안 실무자들은 네가지 위협 형태를 정보보호 요소와 직접적으로 연관을 시킬려고 노력했으나 실패하였다. 변조는 무결성과 인증성 뿐만 아니라 비밀성과 가용성을 파괴시키며, 변조가 파괴의 부분이 될 수가 있다.

결국은 위협 형태를 가용성에 대한 위협, 인증성에 대한 위협, 무결성에 대한 위협, 실용성에 대한 위협, 비밀성에 대한 위협으로 분류해야 한다. 이렇게 보안의 개념을 확장함으로써 정보보호 요소가 중복되지 않고 위협형태도 완전히 포괄적인 의미를 가지게 될 수 있다.

정보보호 요소와 같은 의미의 용어를 다음과 같이 정의함으로써 요소간의 관계를 나타내는데 도움이 될 것이다.

Availability	Presence
Authenticity	Genuineness
Integrity	Completensess
Utility	Usefulness
Confidentiality	Secrecy

3.2 보호 대책

보안은 직접적인 위협이 될 수 있는 위험 요소를 줄이는데 있다. 지금까지 보호방법으로 고려되어 왔던 예방(Prevention), 탐지(Detection), 회복(Recovery) 뿐만 아니라 회피(Avoidance), 억제(Deterrence), 약화(Mitigation), 제재규정(Sanction), 변경(Transeference), 교정(Correction) 등의 보안기능을 추가하여 보안 활동을 조직화함으로써 위협이나 위협이 될 수 있는 위험 요소를 줄일 수 있다. 여기에 추가해서 의무 규정표준안(Standard of Due Care)을 마련하여 위협요소가 존재한다면 최소한으로 줄일 수 있다.

아직까지 위협에 대한 경험요소는 예측을 바탕으로 도출하고 있으며, 구체적인 예를 제시할 통계적 자료가 부족하기 때문에 보안 목적을 위한 위협형태의 다양한 분석은 곤란하다. 즉, 우리가 무엇을 모르고 있는지 우리도 잘 모르고 있으며, 더군다나 만약의 상황을 구체적으로 표현하는 것은 더욱 어려운 일이다.

3.3 정보보호 요소들의 통합

새롭게 정의된 정보보호 요소인 비밀성, 무결성, 인증성, 실용성, 가용성은 각각의 분야가 비교적 중복됨이 없이 독특한 분야를 나타낸다. 보안기술자들은 이미 개발되거나 개발 중에 있는 보안기술을 정보보호 요소에 따라서 분류하고 있는데, 예를 들어, 패스워드제어 시스템은 인증에, 암호제어 시스템은 비밀성에, TCSEC을 적용한 제어 시스템은 비밀성에, Clark-Wilson 모델은 무결성 및 인증으로 분류하고 있다. 그러나 이렇게 분류된 시스템들은 정보보호 요소의 1-2개의 분야만 만족하며, 시스템 공격자들은 여기에 포함되지 않은 분야에 의해서 시스템을 공격할 수도 있다.

또한, 미국의 TCSEC과 유럽의 ITSEC(Information Technology Security Evaluation Criteria)에서는 보안 평가기준을 제시함으로써 시스템이 보호하지 않는 분야에 의해서 더욱 용이하게 공격할 기회를 제공하고 있다. 왜냐하면 규정만으로 위험요소들이나 위협형태를 제거할 수 있는 모든 방안을 완전하게 제시할 수 없으므로 상대적으로 취약점을 노출시키는 결과를 초래할 수 있기 때문이다. 정보보호 요소의 특정 분야가 지녀야 할 보안 정책을 정의하는 것이 이론적으로 목적에 유용할지라도 실제로는 정보보호 요소의어느 한 분야가 누락될 경우 시스템 공격자는 시스템이 제공하지 않는 분야로 공격목표를 바꿀 수 있다.

따라서 정보보호에 대한 정의나 기준을 설정할 때는 공격 목표를 다양하게 설정하는 적에 대해서 정보보호 요소의 모든 분야를 동시에 만족하도록 해야 하며, 정보보호 위원회(Information Security Committee)는 TCSEC이나 ITSEC의 평가 기준대로 정보보호 시스템들이 완성되기 전에 다섯가지의 새로운 정보보호 요소들이 결합된 시스템 보안정책에 대한 프로토타입을 개발해야 할 것이다.

다섯가지의 정보보호 요소를 관련있는 것끼리 묶어서 무결성은 인증에 포함시키고 가용성은 실용성에 포함시키는 방법을 생각할 수도 있겠으나 이렇게 한다면 인증성이나 무결성 중에서 어느 한가지 요소가 보호되지 않는다면 다른 나머지도 동시에 보호되지 않으며 가용성과 실용성의 경우도 마찬가지이다.

3.4 보호 대상

위협 요소로부터 보호해야 할 대상은 정보, 응용프로그램, 하드웨어, 사용자 등이 있으며, 이들은 인증성과 실용성을 추가한 다섯가지의 정보보호 요소를 고려하여 적절히 제어하면 정보보호 목적을 달성할 수 있을 것이다.

(1) 정보(Information)

정보에 대한 비밀성을 유지하기 위해서는 오직 허용된 소수의 인원에게만 정보를 알 수 있도록 하는 것이며, 이를 위해 주체가 객체에 접근할 수 있는 권한을 부여하는 규칙을 정한다. 실제로 비밀성을 달성하기 위해서는 DAC, MAC, 암호화, 레이블, 재사용 금지 등의 방법을 사용한다. 정보의 사실 여부를 확인하는 인증을 위해서는 감사, 회계, 검증 등의 방법을 사용하며, 무결성은 체크비트를 사용

하고, 실용성은 백업, 회복, 테스팅 등을 활용하며, 가용성은 중복성 유지, 백업, 회복기법 등이 사용된다.

(2) 응용 프로그램(Application)

응용프로그램에서 비밀성을 유지하기 위해서는 복사권한의 제한, 암호화, 레이블 등의 방법을 이용하여 실행코드에 직접 접근하지 못하게 하는 것이며 무결성에 문제가 발생할 경우에는 도난, 사기, 변경 등의 행위를 막을 수 없다.

(3) 운영체제(Operating System)

운영체제는 존재하는 형태나 내용면에서 볼 때, 응용프로그램과 거의 유사하기 때문에 보호방법도 거의 일치한다.

(4) 하드웨어(Hardare)

하드웨어에 대한 비밀성을 유지하기 위해서는 물리적으로 접근을 제어하는 잠금장치나 보호패킹을 사용하는 방법이 있다. 인증도 역시 열쇠등의 물리적인 방법에 의해서 할 수 있으며, 이는 장비를 바꾼다든지 변경시키는 것으로부터 보호된다. 또한 무결성과 가용성을 유지하기 위해서 테스팅, 유지보수 등의 방법을 사용한다.

(5) 사용자(User)

사용자도 많은 비밀정보를 다루기 때문에 무형의 형태로 정보를 간직하고 있으며, 이를 보호할 필요가 있다. 개인의 프라이버시와 관련된 정보일 경우 법적으로 규제를 하고 있다. 개인을 확인하기 위해서는 패스워드, 토큰등의 방법을 사용하며, 무결성과 관련된 개인의 특성은 정직성, 윤리성 등과 관련이 있다.

4.4 정보보호 요소의 중요도에 의한 우선순위

다섯가지의 정보보호 요소들 중에서 비밀성에 대한 연구는 미국의 NSA에서 많이 추진하였으며, 그 결과로 TCSEC과 평가 프로그램 등을 작성하였다. 군이 아닌 사회 분야에서는 개인의 프라이버시 보호측면에서 많은 연구를 하였고, 가용성은 사용자나 정보산업에서 많은 노력을 하였다. 그러나 정보보호 기술자나 정보관리자의 관점에서 보면 정보보호 요소의 중요도는 서로가 상반된 입장을 지니고 있다.

(1) 정보보호 기술자 관점에서의 우선순위

정보보호 기술자나 특히 정보보호에 대한 책임을 갖고 있는자는 비밀정보에 가장 높은 관심을 가지고 있으며, 이러한 정보가 외부로 노출되지 않도록 최대한의 노력을 할 것이다. 이들은 정보보호 목적을 달성하기 위한 연구개발에 지원을 하고 정형화된 보호 모델을 개발한다. 또한 당장에 나타나거나 알 수 없지만 만약의 경우, 더 나아가서는 극단적인 상황을 예상하여 위협의 형태를 가시화 한다. 이들에게는 시스템 차원에서의 전체이익이나 사용자의 편이성 보다는 중요 정보를 보호하는데 더욱 치중하면서 정보의 중요성을 값으로 판단하기 어렵다고 생각한다. 이들 관점에서 정보보호 요소를 중요도에 의해 나열하면 ① 비밀성, ② 무결성, ③ 인증성, ④ 가용성, ⑤ 실용성 순이된다.

(2) 정보 관리자(사업 관리자) 관점에서의 우선순위

정보보호 기술자와 상반된 입장을 가지고 있는 정보 관리자는 잉여가치를 남기는 사업에 관심이 있으며, 위협은 불이익이 발생한 경험이 있는 것에 관심이 있지 아직 가시화되지 않은 위협에 대해서는 큰 관심이 없다. 이들은 정보도 하나의 재화로서 인식하고, 정보의 누출 또는 손실로 발생될 수 있는 금전상의 손해와 가능성을 판단하여 전체 시스템 차원에서의 손익계산을 하고자 한다. 따라서 사업관리자이면서 정보관리자인 이들은 전체적인 균형과 활용성, 편이성 등에 더 큰 비중을 두게 된다. 이들의 관점에서 정보보호 요소를 중요도에 의해 나열해 보면 ① 실용성, ② 가용성, ③ 인증성, ④ 무결성, ⑤ 비밀성 순이 될 것이다.

4. 결 론

지금까지 정보보호 요소와 위협형태에서 제기되고 있는 문제점을 살펴보고 수정된 정보보호 개념을 제시해 보았다. 앞으로 이러한 개념의 변화에 대한 다각적인 연구가 수행되어야 하며 이러한 개념은 보안정책을 수립하고 표준안, 지침서, 연구보고서, 교육자료 등을 마련하는데 반영되어야 한다고 생각된다. 시스템의 정보보호 능력을 검토하고 감사하기 위해서는 그 시스템이 제공하지 않는 정보보호 요

소로 부터 발생하는 각각의 취약점에 대해서 시험해 보아야 할 것이다. 이러한 시험과정을 거치면서 어떤 제어기능은 중복해서 나타나기도 하고 어떤 것은 전혀 나타나지도 않을 수가 있는데, 이러한 현상은 어떤 취약점이나 제어 기능이 다섯가지의 정보보호 요소를 유지하는데, 직접 또는 간접적으로 영향을 주기 때문이다. 시스템은 다섯가지 정보보호 요소를 모두 고려하기 전에는 제품을 평가하기 곤란하며, 따라서 TCSEC과 ITSEC의 접근방법은 새로운 정보보호 요소로 판단해 보면 충분하다고 볼 수 없을 것이다.

국제적으로 컴퓨터 보안이나 정보보호에 대한 표준화가 진행되고 있는 싯점에서 정보보호 관련 전문인들은 항상 새로운 감각으로 국제적인 추세에 부응할 수 있도록 준비에 최선을 다 해야 할 것이다.

참 고 문 헌

1. 남길현, "선진국 데이타보호 기술동향 분석", 한국전자통신연구소, 1991. 12.

2. C. Jahr, "Europe Persues Different Computer Security Approach", Signal, AFCEA, Jan. 1991.

3. Department of Defense, "Trusted Computer System Evaluation Criteria", National Computer Security Center, DoD 5200. 28-STD, 1985.

4. Donn B. Parker, "Restating the Foundation of Information Security", SRI International, 1991.

5. T.M. Lee, "Security Criteria Evolves to Meet a Changing World", Signal, AFCEA, Jan. 1991.

6. David Clark and David Wilson, "A comparison of Commercial and Military Security Policies", Proceedings of the 1987 IEEE Symposium on Security and Privacy, Arpil. 1987.

□ 著者紹介

남 길 현(正會員)

陸軍士官學校 卒
서울工大 土木科 卒
美海軍 大學院(電算學 碩士)
위스콘신(메디슨) 州立大(電算學 碩士)
루이지아나州立大(電算學 博士)
陸軍士官學校 教授部 專任講師, 現在 國防大學院 副教授