문헌 연구를 통한 정보보증 개념의 구문 분석

강 지 원*, 최 헌 준*, 이 한 희**

요 약

정보보호(Information Security)는 최근 사이버공간의 출현과 확장으로 인해 그 중요성이 점차 증가하고 있다. 1998년 미국 국방부 정보작전 교리에서 유래된 '정보보증(Information Assurance)'은 기존의 정보보호 개념에 대응과 복구를 포함한 광의의 적극적 보호, 정보체계 전 수명주기에서 보안관리, 위험분석 과정에서의 신뢰성 등을 추가한 개념으로서 현재 널리 사용중이다. 그러나 국내에서는 정보보증 개념을 잘못 이해하거나 정보보호와 혼용하여 사용하는 경우가 종종 발생하고 있다. 본 논문에서는 정보보증 개념의 명확한 이해를 위해 정보보증 관련 기존 문헌들을 고찰하여 정보보증 개념을 정의하고자 하였다. 본 논문에서 제안한 정보보증 용어 정의의 주요 표현들에 대한 구문 분석을 수행함으로써, 용어 정의의 타당성을 제시하였다.

Semantic Analysis of Information Assurance Concept : A Literature Review

Ji-Won Kang*, Heon-jun Choi*, Hanhee Lee**

ABSTRACT

Today, information security (INFOSEC) as a discipline is gaining more and more importance according to the emergence and extension of the cyberspace. Originated from Joint Doctrine for Information Operation (Joint Pub 3-13) by the U.S. Department of Defense, 'information assurance (IA)' is the concept widely used in the relevant field. Grown from the practice of information security, it encompasses broader and more proactive protection that includes countermeasures and repair, security management throughout an information system (IS)'s life-cycle, and trustworthiness of an IS in the process of risk analysis. In Korea, many industry professionals tend to misunderstand IA, remaining unaware of the conceptual differences between IA and INFOSEC. On this account, the current study attempted to provide a combined definition of IA by reviewing relevant literature. This study showed the validity of the wordings used in the proposed definition phrase by phrase.

Key words : Information security, Information Assurance, Risk Analysis, Reliability, Survivability

접수일(2019년 2월 28일), 수정일(1차: 2019년 3월 26일), 게재확정일(2019년 3월 29일)

* 세종대학교 정보보호학과
** 국방부

1. 서 론

현재 우리는 '정보보호' 또는 '정보보안'이라는 용어를 포괄적으로 사용하고 있다. 일반적으로 정보보호나 정보보안은 유사한 개념으로 기밀성, 무결성, 가용성을 보장하여 정보의 안전한 생산·저장·유통을 위한 기술적·관리적 대책을 통칭하는 개념이다. 기술적 측면에서는 '정보보호'라는 용어를, 관리적 측면에서는 '정보보안'이라는 용어를 보다 많이 사용하는 경향이 있다.

한편, 미국 국방부는 정보보호 개념을 확장하여 '정보보증(Information Assurance, IA)'이라는 용어를 사용한다. 정보보증의 정의, 목적, 범주 등에 대한 견해는 연구자마다 매우 다양하며, 각각의 용어 개념은 계속 발전하고 있다. 하지만 국내에서는 정보보호와 정보보증의 개념 및 용어가 혼재하고 있으며 정보보증의 필요성에 대한 인식과 관련 업무절차와 관련한 연구가 미흡한 실정이다.

이에 따라, 본 논문은 국내외 문헌 검토를 바탕으로 정보보증 관련 개념과 용어들을 고찰하고, 정보보증의 개념에 대한 용어 정의를 시도하고자 한다.

2. 이론적 고찰

2.1 정보보호 개념의 발전

2.1.1 통신보안 (COMSEC)

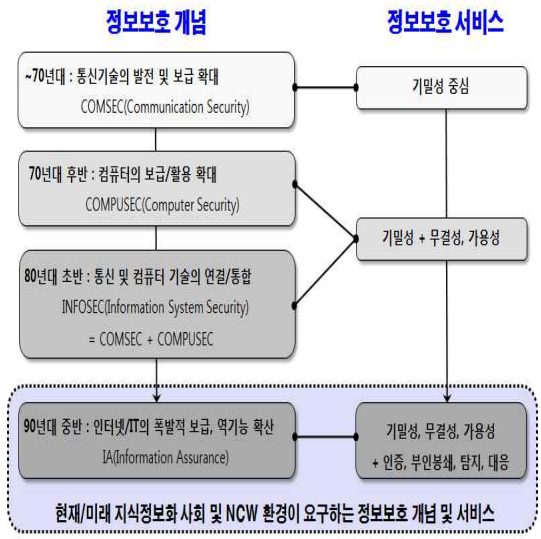
통신에 대한 보안이 전쟁의 승패를 가르는 주요한 요인이 되었던 2차 세계대전 이후부터 암호기술을 기반으로 한 보안장비의 개발이 활발하였다. 1970년대 정보보호 개념은 통신기술의 발전 및 보급 확대로 '통신보안(Communication Security, COMSEC)'이라는 용어를 사용하였다. 이 시기에는 네트워크를 통해 전송되는 정보를 보호하기 위한 수단으로서 기밀성 중심의 서비스가 주를 이루었다.

2.1.2 컴퓨터보안(COMPUSEC)

70년대 후반부터는 컴퓨터의 보급과 함께 컴퓨터의 군사적 활용이 확대되면서 '컴퓨터보안(Computer Security, COMPUSEC)'이라는 용어가 등장하였다. 컴퓨터에 저장·관리되는 정보의 훼손 및 유출 등과 같은 위협이 대두되면서 기밀성 뿐만 아니라 무결성과 가용성이 중요 보안 목표로 제시되었다.

2.1.3 정보통신보안(INFOSEC)

통신과 컴퓨터 기술이 상호 연결되고 통합되기 시작한 80년대 초반부터는 통신보안과 컴퓨터보안의 구분이 모호해지면서 COMSEC과 COMPUSEC을 합친 '정보체계보안(Information System Security, INFOSEC)'이라는 용어가 등장하였으며, 현재의 '정보보호'의 의미로 널리 사용되고 있다. 이 역시 기밀성, 무결성 및 가용성을 보안 목표이며 중요 서비스로 취급되고 있다.



(그림1) 정보보호 개념의 발전

2.1.4 정보보증(IA)

한편, 90년대 중반에 이르러 인터넷 및 IT기술이 폭발적으로 보급됨과 동시에 그 역기능에 대한 인식이 확산되었고, 이에 따라 기존의 보호수단 위주의 정보보안을 넘어 적극적인 탐지와 대응의 필요성이 커졌다. 이에 발맞춰 현재에는 정보와 정보체계의 생존성(Survivability) 및 신뢰성(Trustwor

thiness/ Reliability)까지를 강조한 보다 포괄적인 개념의 정보보증(IA)이라는 용어가 새롭게 사용되고 있으며, 기밀성, 무결성, 가용성, 인증, 부인봉쇄, 탐지 및 대응 등의 서비스로 그 영역이 확대되고 있다. 정보보증 개념은 당분간 현재와 미래의 지식정보화 사회 및 국방 분야의 네트워크중심전(NCW) 환경이 요구하는 중요한 정보보호 개념 및 서비스로 자리 잡으리라 판단된다.

2.2 정보보증의 특징 및 필요성

2.2.1 美 정보작전 합동교리(Joint Pub, 1998)[1]

정보보증이라는 용어는 미국 정보작전 합동교리에서 최초로 사용하였으며, 여기서 정보보증을 "기밀성, 무결성, 가용성, 인증, 부인봉쇄 등 5개의 보안 목표를 보장함으로써 정보와 정보체계를 방어하고 보호하는 정보작전"으로 정의하였다.

> "Information assurance" is defined as IO that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection,detection, and reaction capabilities.

여기서 기밀성, 무결성, 가용성, 인증, 부인봉쇄 등의 용어는 아래와 같이 정의된다.

- 기밀성(Confidentiality) : 인가되지 않은 상대에게 노출되는 것으로부터 연결의 존재, 트래픽 흐름을 보호
- 무결성(Integrity) : 정보와 여러 프로세스들이 암호화, 전자 서명, 침입 탐지와 같은 방법에 의하여 인가되지 않은 간섭(예 : 데이터 삽입, 삭제, 파괴, 재전송 등)으로부터 정보와 처리과정이 안전하다는 것을 보장
- 가용성(Availability) : 사용자가 필요로 할 때 정보, 서비스, 자원에 접근 가능하고 사용 가능함을 보장
- 인증(Authentication) : 인가(접근 권한에 대한 허가/취소), 위임(한 개체의 권리 일부를 다른 개체에 확대), 사용자 인증(사용자와 데이터 근원에 대한 신뢰성 있는 확인)과 같은 통제 대책을 바탕으로 정보와 서비스에 접근하도록 함
- 부인봉쇄(Non-repudiation) : 데이터를 송수신한 자가 송수신 사실을 허위로 부인하는 것을 방지하기 위해 송수신 증거를 제공

2.2.2 CNSS[1]의 "정보체계 보호" 용어집[2]

CNSS의 "정보체계 보호" 용어집에서는 정보보증을 "정보와 정보체계의 가용성, 무결성, 인증, 기밀성, 부인봉쇄를 보장함으로써, 정보와 정보체계를 보호하고 방어하는 예방조치이며, 이 예방조치에는 보호, 탐지 및 대응 능력에 의한 정보체계의 복구 능력을 포함"한다고 정의하였다.

> "Information Assurance" measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

CNSS의 정의는, 정보보증을 정보작전의 한 형태라기보다는 예방조치/사전 대책(measure)으로서 인식하였으며, 정보보호 보다는 광의의 범주로서 기밀성, 무결성, 가용성, 인증, 부인봉쇄 뿐만 아니라, 정보체계 복구를 위한 탐지 및 대응 등 복구 능력도 포함하고 있다.

2.2.3 국방과학기술용어사전 및 군사용어사전

국방과학기술용어사전 및 군사용어사전에서는 정보보증을 "정보와 정보체계의 이용성, 통합성,

1) CNSS(Center for National Security Studies) : 미국 국가보안연구센터(비정부 연구조직)

비밀성, 인증(認證), 부인거부(否認拒否)를 보장함으로써 정보와 정보체계를 보호하고 방어하는 정보작전의 한 분야이며, 정보보증에는 정보체계에 보호 및 탐지와 대응 능력을 설치하여 자체 복구 능력을 포함"한다고 정의하였다.

본 정의에서는 위의 미 정보작전 합동교리와 CNSS의 정보보증 용어 정의 내용을 모두 포괄하고 있으며, 정보보호 개념과의 주요 차이점인 '자체 복구 능력'을 포함시켜 정보보증을 정의하고 있다.

3. 정보보증 특징 분석

3.1 정보보증 특징 요약

정보보증은 정보보호와 유사한 개념이지만 기존의 정보보호 개념과 구분될 수 있다. 다음은 정보보증의 주요 특징을 몇 가지로 간략히 요약하였다.[1][2][3]

- 대응 및 복구를 포함한 보다 광의의 적극적 개념
- 정보 및 정보체계에 대한 위험관리 과정에서의 신뢰성을 의미
- 정보보증 획득을 위해 평가가 매우 중요
- 정보보증은 수명주기를 가지고 관리되어야 함

3.1.1 대응 및 복구를 포함한 광의의 적극적 개념

정보보증은 기밀성 보호에 중점을 둔 수동적 의미의 정보보호와 달리, 기밀성, 무결성, 가용성, 인증, 부인봉쇄 및 탐지, 대응, 복구 등을 포함한 보다 광의의 적극적 개념이다. 다른 말로 표현하면, 정보보증은 "정보보호의 포괄적 관리(comprehensive management of information security)"[3]이며, 정보보증은 사고든 의도적이든 상관없이, 대응 및 복구 등을 통하여 인가된 사용자가 인가된 정보를 인가된 시간에 접근할 수 있음을 보장(ensuring)하는 일련의 과정이라 할 수 있다. 여기서 대응 및 복구 능력의 구비는 정보보증의 주요한 목표 중 하나로서, 기존의 정보보호 개념과의 주요한 차이점으로 인식되고 있다.

3.1.2 위험관리 과정에서의 신뢰성

김승주는 "정보보증이란 정보/정보체계의 신뢰성을 확보케 하고, 이를 검증하기 위한 관리적/기술적 수단"이라고 표현하였다.[4] 정보보증이란 정보/정보체계에 대한 위험관리 과정에서의 신뢰가능성을 의미하며, 따라서 신뢰의 수준은 곧 정보보증의 수준을 의미한다. 여기서 신뢰성의 구성요소는 Security, Safety, Privacy, Reliability, Resilience 등으로 이는 해킹에 안전하고, 기계 오작동 등의 오류가 없으며, 문제 발생 시 재해로 연결되지 않고 재빠르게 원상 복원될 수 있는 능력을 의미한다. 또한 이들 신뢰성 구성요소들은 서로 독립적으로 달성될 수 있는 것이 아니므로, 시스템 요구사항 분석/설계 단계부터 종합적으로 고려할 필요성이 있다.

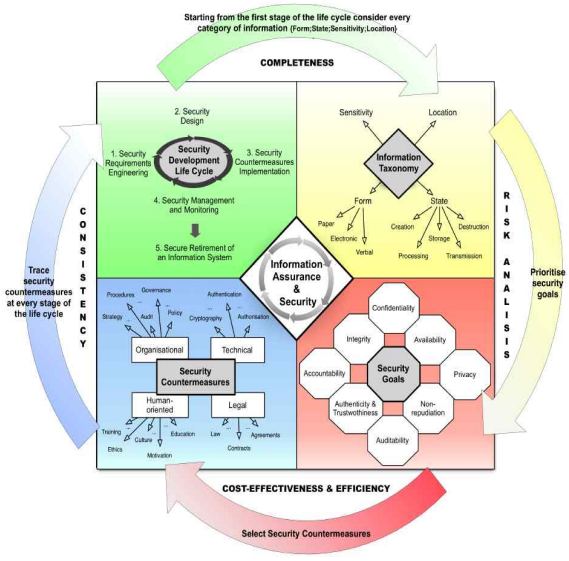
이렇듯 정보보증의 개념은 확대된 정보보호 개념 외에 정보/정보체계에 대한 위험분석 기반의 접근방법으로 신뢰성 확보를 포함하고 있다. 이와 같이 체계 개발 과정에서 정보체계 전 수명주기에 걸쳐 정보보호 요구사항을 체계적으로 관리하여 체계의 신뢰성 향상을 보장하는 것이 중요하다.

3.1.3 보증 관점에서 평가의 중요성

'보증' 관점에서 체계 획득을 위한 전형적 방법은 '평가(Assessment)'이며, 정보보증 또한 평가의 중요성이 매우 강조되고 있다. 따라서 객관성과 일관성이 있는 정보보증 평가가 가능하도록 평가 기준을 마련하는 것이 매우 중요하다.

3.1.4 수명주기 관리의 중요성

정보보증 수명주기 관리의 중요성을 묘사한 사례로서, '정보보증 참조모델'[3]을 들 수 있다. 참조모델은 개발자에게 안전한 정보체계 설계를 위한 청사진 제시를 목적으로 작성되는 것으로서, 정보보증 참조모델은 정보보증 관련 개발자에게 정보보증에 대한 개념적 모델을 제공해 준다.

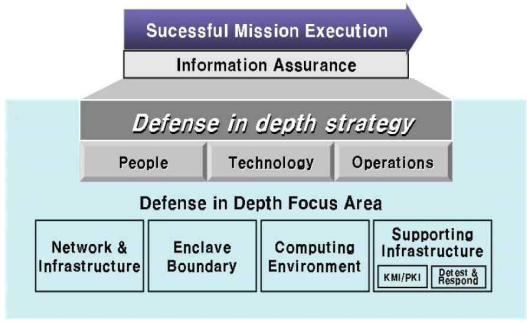


(그림2) 정보보증 참조모델

(그림2) 좌측 상단의 '보안 개발 수명주기'는 보안 요구공학, 보안 설계, 보안 대책 구현, 보안관리와 모니터링 그리고 정보체계 보안 요구 식별의 5단계로 진행되어야 함을 의미한다. 또한, 우측 상단의 '정보 특성(Taxonomy)'는 보호해야 할 대상 '정보의 특성'은 정보의 민감도, 저장장소, 정보의 형태 등을 완전하게 정의하는 단계이다. 그리고 우측 하단의 '보안 목표'는 위험분석에 입각하여 각 보안 하위 목표들(기밀성, 가용성, 무결성, 부인봉쇄, 인증 등) 간의 우선순위를 선정하는 단계이다.[14] 마지막으로 좌측 하단의 '보안 대책'은 비용 대비 효과적이고 효율성 측면에서 적절한 보안 대책(조직적, 기술적, 법적, 인적)을 선정하는 단계이다. 이렇게 선정된 보안 대책은 '보안 개발 수명주기' 각 단계별로 추적·관리 되어야 함을 의미한다.[13][15]

3.1.5 정보보증의 필요성

정보보증이란 컴퓨터 시스템의 보호 그 이상으로서, 정보를 보호하기 위해 필요한 방법(Method), 기술(Technique), 도구(Tool), 인력(People) 및 절차(Process) 등의 총합이다. 현대와 같이 정보에 기반하거나 정보에 의존하는 정부 기관들, 비즈니스 및 기타의 조직 등에서 정보는 매우 중요한 자산이기에 정보보증은 오늘날 조직체의 강건함과 지속성에 있어 필수적인 요소이다.[6]



(그림3) 미군 종심방어 전략

정보보증의 필요성은 정보보증 달성을 위한 미국방부 전략인 "Defense-in-Depth", 즉 종심방어 전략[7]에서 찾아볼 수 있다. 미 국방부는 2004년 정보보증 전략적 계획문서(DOD's IA Strategic Plan)의 임무에 "군의 정보/정보시스템/정보기반구조를 보호 및 방어하고 네트워크과 데이터 중심 작전으로의 군 전력 변환을 지원한다"라고 명시하고, 그 추진 전략으로 종심방어 전략을 채택하였다

종심방어란 해킹, 바이러스 등 역기능에 효율적으로 대응토록 하여 아군의 정보 및 정보체계를 안전하게 보호함으로써 궁극적으로 임무의 성공적인 수행을 보장토록 하는 추진 전략이다[8]. 종심방어는 다중 계층, 다중 차원의 보호수단을 구축하는 접근 방법이다. 쉽게 말해, 중세시대 성의 방어체계처럼 하나의 방어 장벽이 공격자에 의해 침투되거나 돌파되어도 연속적인 또 다른 방어 수단을 통해 이에 대응한다는 개념이다. 이는 다양한 형태의 사이버 위협 및 공격을 단일 보호체계로 모두 방어할 수 없기 때문에 기능 및 용도가 서로 다른 보호체계로 다단계 보호막을 쳐서 안전성을 확보한다는 계층적 접근방법인 것이다.

4. 정보보증과 정보보호 차이 분석

정보보증과 정보보호의 정의, 목적, 범위 등에 대한 견해는 연구자마다 매우 다양하며, 또한 개념이 계속 진화하고 있기 때문에 이들 두 용어에 대한 명확한 관계 정립은 쉽지 않다.

본 논문에서는 정보보증과 정보보호의 차이에 관한 산업계, 협회, 학계의 대표적인 연구 사례들을 분석하였다.

4.1 NovaInfosec 연구

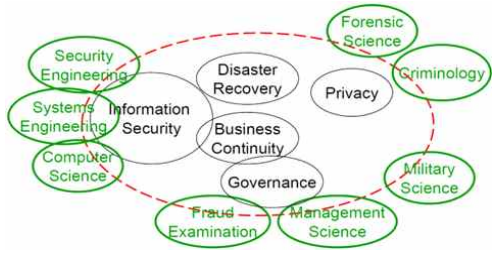
NovaInfosec에서는 정보보증과 정보보호의 차이점을 (그림4)로 요약하고 있다.[11]

(그림4) NovaInfosec 정보보증과 정보보호의 차이

(그림4)에서 보는 바와 같이 정보보증은 정보보호에 비해 전략적인 면에 집중하고 보다 폭 넓은 정보관리/보호를 강조하고 있으며, 조직체의 전반적 위협과 그것을 줄이는데 관심을 갖는다. 반면에 정보보호는 정보보증에 비하여 도구 및 전술적 측면에 집중하고, 기술과 동작을 강조하고 있으며, 보호를 위한 응용체계 그리고 기반구조에 관심을 갖는다. 정보보증의 관심 항목의 예로서는 인증과 인가, 프라이버시, 순응성, 감사, 업무 연속성, 재해복구(DR) 등이 있으며, 정보보호의 예는 안티바이러스, 방화벽, IDS, VPN 등이 해당된다.

4.2 스토리지 네트워킹 산업협회(SNIA) 연구

SNIA(Storage Networking Industry Association)에서는 정보보호란 정보의 기밀성, 무결성, 가용성에 초점을 두는 반면, 정보보증은 보다 광의의 개념으로서, 신뢰성, 접근통제, 부인봉쇄 뿐만이 아니라 전략적인 위험관리(Strategic Risk Management)에 매우 강조를 두고 있다고 하였다.[12] (그림5)에서와 같이 정보보증의 영역은 정보보호, 재해복구, 비즈니스 연속성 등을 포함하며, 보안/시스템/컴퓨터 공학, 경영과학, 군사학, 수사과학 등과도 관련된다고 하였다.



(그림5) SNIA 정보보증 영역 분류

4.3 Cherdantseva의 연구

Cherdantseva는 정보보증과 정보보호에 대한 개념, 업무의 범주, 주요 차이점에 대해 최초로 학문적 연구를 수행하였다. 전 세계적으로 정보보증 관련 산・학・연・군 커뮤니티에서는 Cherdantseva가 정립한 개념이 널리 인용 및 적용되고 있다. (표1)는 Cherdantseva의 저서 중에서 정보보호와 정보보증의 차이점에 대해 기술한 내용을 분석한 내용이다.[5]

<표1> Cherdantseva의 정보보호와 정보보증 영역 차이

구분	정보보호	정보보증
대동 시기	1980년대	1998년
보호의 주체	정보 및 정보시스템	업무 및 영역
목표	기밀성, 무결성, 가용성 (예견된 위협으로부터의 보호)	업무 전 영역의 보호 (예견되지 못한 위협으로부터 보호)
보호되는 정보	주로 전자적(electronic) 형태	모든 유형 (전자적 형태, 페이퍼, 지식 등)
접근방법	기술적 접근이 지배적 (인적요소, 관리영역 등은 초보 수준)	모든 요소를 포함하는 종합적・체계적 접근방법 활용
보호 메카니즘	기술적 보호 메카니즘이 주류	기술/조직/인적/법적 요소 총 망라
업무영역에서의 역할	제한 지원 (공공 업무영역에 제한사항 수반)	업무영역의 통합, 업무영역의 조력자(enabler)
책임 소재	전담 팀장 및 관련 기술팀장	고위간부 및 관련팀장
관련 부서	고위 간부, 전담 팀장 및 관련 기술팀장	조직체의 모든 인원
요구주체	보호상의 요구 (Security-needs driven)	업무상의 요구 (Business-needs driven)
의사결정의 흐름	상향식(Bottom to Top) : 기술 전문가들의 경험이 기초가 되어 고위 간부에게 전달되어 승인	하향식(Top to Bottom) : 고위 간부의 위험분석이 기초가 되어 관련부서로 전달되어 실행

5. 정보보증 용어 정의 및 구문 분석

5.1 용어 정의 필요성

정보체계에 대한 기술적 보호수단으로서의 기능을 충족했던 기존의 정보보호 개념이 체계 자체의 신뢰성, 생존성 향상을 통해 업무의 연속성을 보장하는 '정보보증' 용어로 새로이 등장하고 있다. 하지만 국내에서는 정보보호와 정보보증의 개념 및 용어가 혼재하고 있으며 정보보증의 필요성에 대한 인식과 관련 업무절차와 관련한 연구가 미흡한 실정이다.

본 논문에서는 앞의 많은 연구 결과를 종합하여 <표2>와 같이 정보보증 용어 정의를 제안한다.

<표2> 정보보증 용어 정의 제안

정보보증 : 위험 및 비용/효과 분석으로 도출한 제반 보호대책의 포괄적이고 체계적인 관리에 의해, 정보와 정보체계에 연관된 각종 위험을 감소시킴으로써, 정보와 정보체계의 보호 및 방어, 신뢰성 및 생존성 보장을 목적으로 행하는 활동

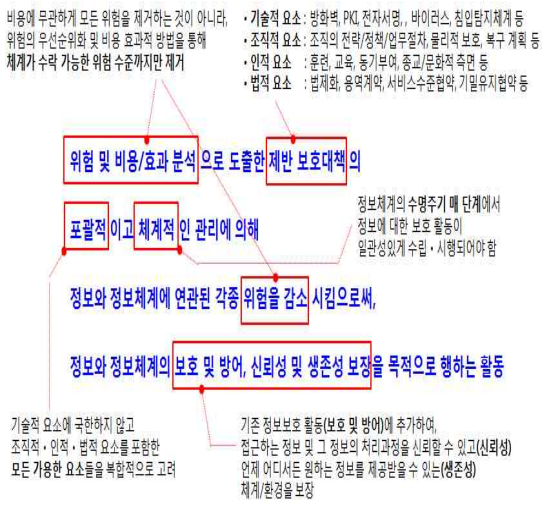
5.2 용어 정의 구문 분석

5.2.1 용어 정의 구문 분석 종합

앞서 서술한 정보보증 용어 정의(안)에는 아래와 같은 주요 개념들을 포함하고 있다.

- 위험, 비용/효과 분석, 위험의 감소
- 제반 보호대책
- 포괄적, 체계적 관리
- 보호 및 방어, 신뢰성 및 생존성 보장

정보보증 용어 정의(안)을 구성하고 있는 주요 개념들 각각에 대해 구문 분석(내포된 의미 및 관련 근거 제시)을 통해 용어 정의(안)에 대한 종합적인 분석 결과는 아래 (그림6)과 같다.



(그림6) 정보보증 용어 정의와 구문 분석 결과

5.2.2 용어 정의 구문 분석 : "위험, 위험분석, 비용/효과 분석"

정보보증 용어 정의(안) 중에서 "위험, 위험분석, 비용/효과 분석"에 내포된 의미는 "정보보증은 비용에 무관하게 모든 위험을 제거하는 것이 아니라, 위험의 우선 순위화 및 비용 효과적 방법을 통해 체계가 허용 가능한 위험수준까지만 제거한다"라는 것이다. 정보보증 용어의 정의에 이와 같은 "위험, 위험분석, 비용/효과 분석" 등의 용어를 포함시킨 근거는 Cherdantseva의 연구[9]에서 찾고 있다.

Risk analysis - IA does not attempt to eliminate all risks, the risks should be prioritized, according to the organization's specifics, and reduced to an acceptable level. 위험분석 - 정보보증은 모든 위험의 제거를 시도하는 것이 아니라, 위험은 조직의 세부 요구사항에 따라 우선순위화 되어, 수용 가능한 일정 수준까지 감소되어야 한다.

Cost-effectiveness - IA does not attempt to achieve security at any price, but in the most efficient and cost-effective way.

비용 대 효과 - 정보보증은 어떤 대가를 치러서라도 달성하는 것이 아니라, 가장 효율적이고 비용 대비 효과적인 방법으로 달성되어야 한다.

5.2.3 용어 정의(안) 구문 분석 : "포괄적 보호대책"

정보보증 용어 정의(안) 중에서 "포괄적 보호대책"이 내포하는 의미는 "정보보증의 제반 보호대책은 기술적/조직적/인적/법적 요소를 포괄적으로 망라하여야 한다"는 것이다.

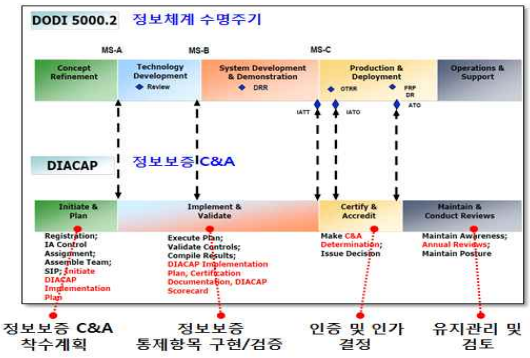
정보보증 용어의 정의에 "포괄적, 제반 보호대책"을 포함시킨 근거는 Cherdantseva가 주장한 정보보호와 정보보증의 "보호 메커니즘"차이에서 찾을 수 있다.[9](<표3> 참조)

<표3> 보호 메커니즘의 차이

구분	정보보호	정보보증
보호 메커니즘	기술적 보호 메커니즘이 주류	기술/조직/인적/법적 요소를 총 망라

5.2.4 용어 정의(안) 구문 분석 : "체계적 관리"

정보보증 용어 정의(안) 중에서 "체계적 관리"에 관련된 부분은 (그림7)과 같다. 정보보증은 정보체계의 수명주기 매 단계에서 정보에 대한 보호 활동이 일관성 있게 수립되고 시행되어야 한다. 정보보증 용어의 정의에 이와 같은 "체계적 관리" 용어를 포함시킨 이유는, 정보체계 수명주기와 정보보증 인증 및 인가(C&A) 프로세스인 DIACAP[2]을 도식화한 (그림7)을 근거로 들 수 있다.[10]



(그림7) 정보체계수명주기와 정보보증(DIACAP)

DIACAP은 조직이 정보시스템에 위험관리를 적용하도록 보장하는 미 국방부의 절차로 정보 시스템이 기밀성, 무결성 및 가용성을 달성하는 방법이나 위험을 관리하고 감소시키는 방법을 표준화한 절차이다.

DIACAP은 정보보증 인증 및 인가에 대한 착수와 계획, 정보보증 통제항목 구현 및 검증, 인증 및 인가 결정, 운용 승인 및 검토 유지, 폐기 등 총 5단계의 절차로 이루어진다.

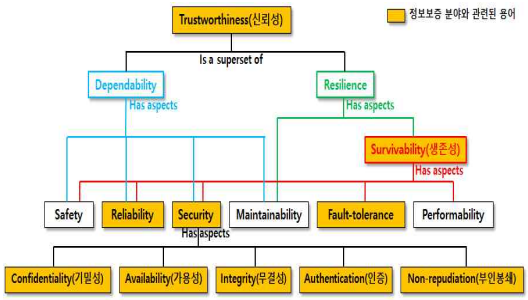
5.2.5 용어 정의(안) 구문 분석 : "보호 및 방어, 신뢰성 및 생존성 보장"

정보보증 용어 정의(안) 중 "보호 및 방어, 신뢰성 및 생존성 보장"은, "정보보증은 기존 정보보호 활동(보호, 방어)에서 더 나아가 , 접근하는 정보와 그 정보의 처리과정을 신뢰할 수 있으며(신뢰성), 언제 어디서든 원하는 정보를 제공받을 수 있는(생존성) 체계와 환경을 보장한다"는 의미를 지닌다.

- "보호 및 방어" : 정보보증은 기존의 보호·방어 활동 위주의 모든 정보보호 개념을 포함하고 있으므로, 보호 및 방어는 정보보증의 세 가지 활동목적 중 하나에 해당된다.(나머지 두 개는 신뢰성과 생존성).
- "신뢰성" : 정보보호/정보보증, 소프트웨어 공학, 시스템 공학 등의 분야에서 사용되는 유사 용어/개념들 간 연관된 온톨로지로서 신뢰성(Trustworthiness)을 정리하면 (그림

2) DIACAP (DoD Information Assurance Certification and Accreditation Process) : 미국 국방부 정보보증 인증과 인가 절차

8)과 같다. 그림에서 보는 바와 같이 Trust worthiness[3]는 하위의 개념/용어들을 모두 포함하는 최상위 용어로서 Reliability도 포함하고 있다.



(그림8) 신뢰성 및 관련 용어들 간의 온톨로지

- “생존성” : 정보보증 영역은 정보보호 뿐만 아니라 재해복구 및 업무연속성 등을 완전히 포함하는 개념으로서, 정보보호 수준을 넘어 정보와 정보체계의 생존성까지를 강조하고 있다. 즉 생존성이란 ‘보호’ 위주의 기존 정보보호 개념에서 더 나아가 ‘탐지, 대응, 복구(Fault-tolerance : 오류탐지, 시스템 복구 및 재구성)’를 포함하는 개념이다.

6. 결 론

정보보호 개념은 기밀성 중심의 최초 통신보안에서 시작하여 90년 중반 이후 인터넷과 정보통신 기술의 발전과 함께 기밀성, 무결성, 가용성과 인증, 부인봉쇄, 탐지, 대응으로 개념으로 확대 발전되었다.

정보보증의 개념은 확대된 정보보호 개념 외에 정보/정보체계에 대한 위험분석 기반의 접근방법으로 신뢰성, 생존성 확보까지를 포함하고 있다. 다시말해 정보보증은 체계 개발 과정에서 정보보증 수명주기 개념을 적용하여 정보보호 요구사항을 체계적으로 관리하여 체계의 신뢰성을 향상시키고 생존성을 보장할 수 있어야 한다.

본 논문에서 제안한 정보보증의 개념들에 대한 구문 분석을 통해 용어 정의의 타당성을 입증하고자 하였다. 정보보호와 정보보증의 개념을 종합적으로 정리하면 <표4>와 같다.

<표4> 정보보호와 정보보증 용어 비교

	정보보호	정보보증	비교 근거
기밀성	○	○	Joint Pub, 1998
무결성	○	○	Joint Pub, 1998
가용성	○	○	Joint Pub, 1998
인증	○	○	Joint Pub, 1998
부인봉쇄	○	○	Joint Pub, 1998
신뢰성	-	○	DoD Defense-in-Depth, Yulia
생존성	-	○	CNSS의 “정보체계 보호” 용어집, Yulia
인증/인가	-	○	NovaInfosec, Yulia, DoD RMF
재해 복구	-	○	NovaInfosec, SNIA, Yulia
업무연속성	-	○	NovaInfosec, SNIA, Yulia
위험 관리	-	○	SNIA, Yulia, DoD RMF
보호 공학	-	○	Yulia, DoD RMF

정보보증 용어는 미국 국방부 각종 문서에 지금도 계속 활용되고 있다. 따라서, 이와 관련된 국방분야 업무 수행자나 연구자들이 용어에 대한 이해를 높이는 계기가 되었으면 한다. 개념의 통일, 용어의 표준이 모든 것이 출발점이기 때문이다.

참고문헌

[1] US DoD JCS, “Joint Doctrine for Information Operations”, Joint Pub 3-13, pp. I-9, 1998. 10

[2] “Committee on National Security Systems Glossary ”, pp. 62, 2015. 4

[3] Yulia Cherdantseva, “Understanding Information Assurance and Security”, pp. 1-42, 2015

3) 고려대 김승주 교수는 2016년 한국정보보호학회 칼람(NSA의 구인공고에는 정보보호 분야가 없다)에서 신뢰성(Trustworthiness)이란 Security, Privacy, Safety, Reliability, Resilience 등을 종합적으로 일컫는 용어라고 하였다.

[4] 김승주, “NSA의 구인공고에는 정보보호 분야가 없다”, 한국정보보호학회 칼럼, 2016
[5] Yulia Cherdantseva, “A Reference Model of Information Assurance & Security”, IEEE proceedings of ARES, pp 1-9, 2013
[6] Ashley, Bradley K. and Jackson, Gary. “Information Assurance through Defense in Depth” URL: http://www.iwar.org.uk/infocon/dtic-ia/Vol3_No2.pdf , Fall 1999.
[7] Hazelwood, Victor “Defense-in-Depth: Information Assurance for 2003” August 2003, URL: www.sdsc.edu/~victor/DefenseInDepthWhitePaper.pdf
[8] United States. Department of Defense. Information Assurance. August 2002. URL: http://www.dtic.mil/whs/directives/corres/html2/d8500 1x.htm
[9] Yulia Cherdantseva, “Understanding Information Assurance and Security”, PhD thesis, 2015
[10] United States. Department of Defense. DoD Information Security Certification and Accreditation Process (DITSCAP), December 1997 URL:http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf
[11] https://www.novainfosec.com/
[12] www.snia.org
[13] 최선규 외, “비용추정방법을 활용한 시스템요구사항 적정성 확인방안 연구” vol 13, no 5 pp. 97-105, 2013, 한국융합보안학회
[14] 김선집 외, “공공 IaaS 클라우드 인증제도에 적용할 위험분석 방법에 대한 연구” vol 15, no 5, pp. 9-15, 2015, 한국융합보안학회
[15] 김양훈 외. “의료융합 환경에서 수용성을 고려한 비용 효율적 보안체계구축 방안 연구: 중소 의료기관을 중심으로” vol 18, no 5, pp 75-81, 2018, 한국융합보안학회

〔저자소개〕

강 지 원 (Ji-Won Kang)
1988년 2월 금오공대 전자공학 학사
1997년 2월 연세대학교 컴퓨터과학 (정보보호 전공) 석사
2012년 8월 경기대학교 정보보호학 박사
2017년 9월~현재 세종대학교 정보보호학과 교수
email : jwkang@sejong.ac.kr

최 헌 준 (Heon-jun Choi)
1988년 2월 전자계산학 공학사
1990년 2월 응용전산학 이학석사
2003년 8월 경영학 박사과정 수료

email : nsri123@empas.com

이 한 희 (Hanhee Lee)
1993년 2월 인제대 이학사
2000년 1월 국방대 전산학 석사
2017년 10월 University of SouthWest America 심리경영학 박사

email : runhoney69@gmail.com