https://doi.org/10.33778/kcsa.2020.20.2.029

OCIL기반 보안수준평가를 위한 XML Converter 설계 및 구현

김 종 민*, 김 상 춘**

요 약

사이버안보의 일선에 있는 국가·공공기관 시스템을 대상으로 하는 사이버 공격이 고도화 되면서 꾸준히 증가하고 있다. 이에 국가·공공기관 시스템의 사이버 공격 사고 예방에 대한 보안 평가 기술 개발이 필요하다. 현재 국가·공공기관 정보 시스템의 취약점 분석에 대한 연구는 거의 자동화 분석에 초점을 맞추어 연구되고 있고, 실제로 보안 점검을 수행하다보면 자동화하기 어려운 부분들도 존재한다. 위협에 대한 보안대책만 생각해보더라도 관리적, 물리적, 기술적 분야에서 각기 다른 방안들을 생각하고 실행할 수가 있는데, 이에 대해서는 주관적이든, 상황적이든 간에 특정한 답변들이 제시된다. 이러한 경향들은 OCIL(Open Checklist Interactive Language)로 규격화되어 부분적인 자동화를 이룰 수 있다. 따라서, 본 논문에서는 기존 평가문항을 OCIL기반으로 보안수준평가를 할 수 있게끔 XML Converter를 구현하고자 한다.

XML Converter Design and Implementation for OCIL based Security Level Evaluation

Jongmin Kim*, Sang-Choon Kim**

ABSTRACT

The cyber attacks targeting the systems of national and public organizations in the front line of cyber security have been advanced, and the number of cyber attacks has been on the constant rise. In this circumstance, it is necessary to develop the security evaluation technology to prevent cyber attacks to the systems of national and public organizations. Most of the studies of the vulnerability analysis on the information systems of national and public organizations almost focus on automation. In actual security inspection, it is hard to automate some parts. In terms of security policies for threats, many different plans have been designed and applied in the managerial, physical, and technical fields, giving particular answers no matter how they are subjective or situational. These tendencies can be standardized in OCIL(Open Checklist Interactive Language), and partial automation can be achieved. Therefore, this study tries to implement XML Converter in order for OCIL based security level evaluation with typical evaluation questions.

Key words : OCIL, XML, ISMS, Security Level Assessment, NIST

접수일(2020년 6월 1일), 게재확정일(2020년 6월 16일)

* 경기대학교/융합보안학과 교수(주저자)

** 강원대학교 정보통신공학부(교신저자)

1. 서 론

국내를 기준으로 보안평가체계 관련 시스템은 인성정보의 wise-ISMS(Information Security Management System), 지란지교에스엔씨의 MISO(Management of Information Security Objects)가 있다[1]. 이들은 수검자의 입장에서 보안평가 대응현황과 증적 자료 저장 중심 시스템으로 국내외 다양한 보안평가체계(ISMS, PIMS, PIPL, G-ISMS, ISO27001, BS10012 등)들을 아우르며 보안관리 업무에 많은 도움을 주고 있다. 하지만 공공기관의 경우, 높은 보안 수준을 지속적으로 유지하기 위해 시스템을 이용해 평가를 진행하고 관리하며, 이를 매년 반복한다. 그리고 매해 발전하는 평가항목을 새롭게 반영해야 하는 수작업 요소가 있어 비효율적 부문이 산재하고, 특정 시점의 수준 평가 이후 보완해야할 사항들에 대한 관리, 추적 상의 어려움으로 지속적으로 일정 보안 수준 이상을 유지하기가 어렵다.

따라서, 본 연구에서는 정보보안 관리실태평가를 운영하는 시스템과 이 시스템의 근간이 되는 정보보안 관리실태평가의 평가항목들이 어떻게 시스템에 반영되는지를 살펴보고 이를 토대로, 정보보안 분야에 강점을 지니고 있는 미국의 공공기관 평가시스템과 비교하여, 설문 형식의 보안평가를 실시할 수 있는 OCIL을 사용하기 위한 XML Converter를 설계 및 구현 하고자한다.

2. 관련연구

2.1 국내 정보보안 실태평가 동향 분석

국내의 정보보안 실태평가는 국가 정보보안 정책 이행실태 확인을 통해 각급기관이 체계적으로 정보보안 업무를 수행하도록 지원하고 보안 취약요인을 사전 발굴, 제거함으로써 각급기관의 정보보안 수준을 제고하고 국가 사이버안전의 확보를 위해 2004년, 정보보안 관리수준 평가제도 도입으로 시작되었다[2][3]. 이후 2006년 50개 국가기관 대상 시범평가 실시를 시작하며 9개 분야 246개 항목에 대해 종합평가를 시행했고, 계속적으로 평가항목의 발전과 점검 대상인 국가, 공공기관의 확대도 추진해가며 오늘날까지 진행되고 있다[4]. 국가정보원은 매년 평가대상 및 일정을 확정하여 대상기관에 통보하고 정보보안 환경 변화, 최신 사이버위협 실태 등을 반영하여 평가지표, 기준 등을 수정, 보완 후 평가에 적용하고 있는 것이다. 그리고 현재 2020년 기준의 평가 절차와 점검항목은 다음과 같다[5].

평가 단계	주체
① 기관별 자체평가	각급기관
② 현장실사	국가정보원
③ 추가증빙 및 이의신청	각급기관
④ 평가결과 심의·의결	평가위원회
⑤ 최종 평가결과 통보	국가정보원

(그림 1)정보보안 관리실태 평가 절차[4]

<표 1> 2020년 정보보안 관리실태 평가 항목 분류 및 배점표[6]

분 야	평 가 지 표	항 목	배 점	
			지표	분야
1. 정보보안 정책 (18, 19, 19)	1.1 정보보안 규정 및 계획	3개	2점	17점
	1.2 정보보안 조직 및 예산	3개	4점	
	1.3 정보보안 기본활동	7개	5점	
	1.4 기관장 관심도	3개	4점	
	1.5 주요정보통신기반시설 보호	2개	2점	
2. 정보자산 보안관리(16)	2.1 정보자산 승인 및 관리	6개	4점	10점
	2.2 국가용 보안시스템	2개	1점	
	2.3 보호구역 관리	3개	2점	
	2.4 휴대용 저장매체 관리	2개	1점	
	2.5 클라우드 컴퓨팅 보안	3개	2점	
3. 인적 보안(21)	3.1 내부인원 보안	2개	1점	22점
	3.2 용역업체 보안관리	14개	17점	
	3.3 정보보안 교육	5개	4점	
4. 사이버위기 관리 (16, 15, 15)	4.1 사이버위기 관리체계 구축	2개	1점	15점
	4.2 예방활동	5개	4점	
	4.3 사이버위기 대응훈련	5개	7점	
	4.4 사이버침해사고 대응 · 복구	4개	3점	
5. 전자정보 보안(19)	5.1 비밀의 전사적 관리	3개	2점	16점
	5.2 전자우편 보안	2개	2점	
	5.3 웹서비스 보안	4개	4점	
	5.4 전자정보 유출 방지	6개	5점	
	5.5 사용자 인증	4개	3점	
6. 정보시스템 보안(25)	6.1 정보보호시스템 및 네트워크 장비 보안	4개	3점	20점
	6.2 무선랜 보안	2개	1점	
	6.3 정보통신망 보안	5개	7점	
	6.4 정보시스템 운용관리	4개	3점	
	6.5 PC 보안	7개	5점	
	6.6 로그 및 백업	3개	1점	
합 계	28개 지표	115개	100점	

2.2 국외 정보보안 실태평가 동향 분석

미국은 2002년 만료 폐기되는 한시법이었던 정부정보보안개혁법(Government Information Security Reform Act of 2000)의 한시법 조항을 삭제하며, 이를 연방정보보안관리법(FISMA: the Federal Information Security Management Act of 2002)으로 명명했다[7]. 이는 자국의 경제 및 국가 안보 이익에 대한 정보보안의 중요성을 인식하여 정부기관들에게 정보보안을 제공하기 위한 전사적 프로그램의 개발, 문서화 및 구현을 요구하기 위해서 제정되었다. 이후 2014년에 기존 FISMA를 현대화하여 연방정보보안현대화법(FISMA: Federal Information Security Modernization Act of 2014)로 개정하였다[8].

FISMA에 의해 연방 정부에 관한 정보보안활동의 관리, 감독권은 국토안보부에 부여되었으며, 국토안보부 장관은 예산관리국 국장을 지원하도록 하여 연방정부 정보시스템에 대한 공공기관들의 정보보호 이행 활동을 관리할 수 있도록 했다[9].

미국의 국립표준기술원(NIST: National Institute of Standards and Technology)은 실제적으로 연방정보 및 정보시스템의 보안 강화를 위한 관련 지침과 표준을 개발 및 제정한다. NIST는 정보보안 통제 항목으로 18개 분야 256개 항목을 자세하게 정의해 제시하고 있으며, 여기에는 접근통제, 보안의식 교육, 감사가능성, 보안평가, 구성관리, 위기대응, 유지보수, 매체보호, 보안계획, 위험평가 등 생각할 수 있는 모든 통제사항이 나열되어 있다고 할 수 있다[10]. 그리고 NIST는 연방 정보시스템에 대한 위험관리 프레임워크를 제시했으며, 이는 정보보안 라이프사이클로써 위험관리기반의 비용효과적인 정보보안 모형으로 알려져 있고, 다음 (그림 2)에서 보는 바와 같다[11].

NIST의 위험관리 프레임워크는 총 6단계로 구성되어 있다. 첫 단계는 특정 사건 또는 위험이 기밀성, 무결성 및 가용성 관점에서 정보와 정보시스템에 잠재적으로 미치는 영향력에 기반하여 정보와 정보시스템을 분류하고, 2단계는 주어진 가이드라인을 활용하여 통제항목들을 선택하되, 위험 평가와 내부 환경을 고려하여 수정하고 보완한다. 그리고 3단계는 선택된 보안통제 항목들을 시스템과 운영 환경에 맞추어 구현하고, 4단계에서는 구현된 보안 통제 항목들을 대상으로 시스템의 보안 요구사항에 기반하여 적절한 방법이 사용되었는지, 정확하게 구현되었는지, 올바른 운영을 하고 있는지 그리고 원하는 결과를 도출해주는 지를 평가한다. 5단계에서는 기관 운영과 자산 등에 관련하여 확인된 위험 속에서의 시스템 운영과 위험을 수용할 수 있는지를 결정하는 것을 인증하며, 마지막으로 보안 통제의 효과 측정, 시스템 또는 운영 환경 상의 변경 사항에 대한 문서화와 변경된 사항들에 대한 보안 영향도 분석 그리고 시스템의 보안 상태 보고와 같은 시스템의 보안 통제 항목들을 확인하고 점검한다[12].

(그림 2) NIST의 위험관리 프레임워크[13]

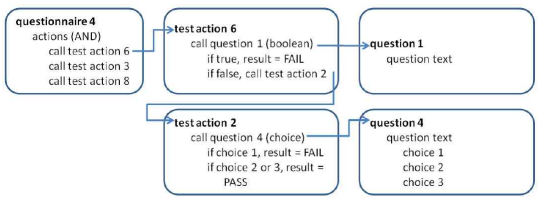
3. OCIL 규격 분석[14]

3.1 OCIL 분석

미국은 OCIL을 활용해 공공기관의 보안 관련 업무들을 토대로 설문을 실시하여 보안 상태를 측정 및 평가하고 있다. OCIL이 SCAP 형식을 지원하도록 하여 보안평가에 있어 기술적으로 자동화하기 어려운 부분을 반자동화함으로써 현재의 보안평가시스템을 자동화와 반자동화, 양 축을 기반으로 운영하고 있는 것이다. 즉, 보안 평가의 실시를 위해 평가 문항 개발자가 수검자 또는 수검기관이 선택 또는 입력 가능한 답변을 예상하여 문항과 답변 예시를 개발하면, OCIL을 이용하여 설문에 대한 제목, 문항 영역, 평가 항목, 유의사항 또는 설명 그리고 답안 등의 형태를 구분하여 완전한 설문지의 형태로 제공할 수 있는 것이다. 이때 설문에 대한 답안은 문제가 요구하는 답변의 형태에 따라 선택

(choice), 입력(numeric), 양자택일(boolean)로 나뉜다.

이 OCIL을 사용하기 위해서는 먼저, OCIL 데이터 모델의 첫 번째인 The ocil Element을 참조하여 설문 자체에 대한 제목, 생성 시간, 작성자, 설명 그리고 유의사항 등을 기록한다. 그리고 설문을 의미하는 The questionnaire Element는 자신이 상위의 개념인 Top-level questionnaire이 되는 것을 기본으로 하여 test_action을 이용해 호출하는 하위의 개념인 child-level questionnaire를 가질 수 있다. 이렇게 해서 설문의 대분류를 정의하고 이 안에 소분류를 두는 등 분야를 좁혀가며 세부적인 내용으로 접근해가는 단계적인 설문 구성이 가능하다. 이 The questionnaire Element에서는 각 설문 분류에 대해 제목, 설명 및 유의사항 등을 기록할 수 있다. 그리고 The questionnaire Element는 실행될 test_action들에 대한 목록을 지니고 있고, test_action들을 AND 또는 OR로 조합하여 최종적인 평가 결과인 통과, 실패, 적용되지 않음 등의 결과 값을 얻을 수 있게 한다.



(그림 3) OCIL의 데이터 모델에 따른 설문응답 진행 절차

The test_action Element는 설문 진행 시 다음 단계를 지시하는 역할과 응답된 답변의 결과 값을 표시하는 역할을 수행한다. 즉, 그 자체로 적용되지 않음과 같은 상태를 가지거나, 응답이 TRUE 또는 YES로 돌아왔을 때 진행되어야 하는 다음 단계를 지시하는 것과 같은 역할을 하는 것이다. OCIL의 답안 예가 선택, 입력 그리고 양자택일(boolean)로 제시되는 만큼 여러 선택지 중에서 특정 답안이 선택되었을 때나 특정한 값 또는 문장이 입력되었을 때와 같이 다양한 조건들에서도 다음의 단계가 test_action인지 또는 설문 항목인지를 다양하게 지정할 수 있다.

그리고 직접적으로 설문의 문항을 표현하는 The questions Element는 OCIL에서 답안 예로 제시되는 선택, 입력 그리고 양자택일의 활용 방법에 대해 설명하고 있다. 선택(choice_question)은 1부터 n까지의 보기 중에서 단일 또는 다중 선택을 가능하게 해주고 있으며, 입력은 숫자(numeric_question) 또는 문자(string_question)를 지원하고 있고, 양자택일은 TRUE와 FALSE 중 선택하거나 또는 YES와 NO 중에서 선택하는 형식이다.

OCIL을 기반으로 설문 평가를 구현하기 위한 데이터 모델과 각 속성들의 활용 방안은 <표 2>와 같다.

<표 2> OCIL 기반 데이터 모델의 주요 속성과 활용 방안

데이터 모델	속성	하위 속성	활용 방안
The ocil Element	generator		설문 제목, 작성자 정보
The questionnaire Element	id		설문 식별자
	child_only		child-level questionnaire only
	actions	test_action_ref	test action 식별자
		operation	test action의 결과 값(AND, OR)
The test_action Element	when_not_applicable		특정 항목은 적용되지 않음 (해당 없음의 의미)
	boolean_question_test_action	when_true	TRUE 또는 YES로 인식하고 다음 단계로 진행
		when_false	FALSE 또는 NO로 인식하고 다음 단계로 진행
	choice	when_choice	선택된 답안에 따라 다음 단계 진행
	numeric_question_test_action	when_equals	특정 값 입력 시 다음 단계 진행
		when_range	특정 범위 값 입력 시 다음 단계 진행
	string_question_test_action	when_pattern	특정 단어 입력 시 다음 단계 진행, 다수의 단어를 지정할 수 있으나 가장 첫 번째로 매칭된 것으로 수행됨
The questions Element	boolean_question		양자택일 선택 문항
	choice_group		단일 답안 선택 문항
	choice_group_ref		다중 답안 선택 문항
	numeric_question		숫자 입력 문항
	string_question		문자 입력 문항

OCIL의 주요 데이터 모델들과 속성들은 각각 제목, 설명 및 유의사항들을 기록할 수 있는 속성이나 하위 속성들도 가지고 있고, 또 상기 표에서 언급하지 않은 증빙자료나 결과치 산정 등에 대한 데이터 모델들도 OCIL은 가지고 있으므로, OCIL을 이용하면 전체적인 설문지를 구성하여 수요조사나 평가 등에 활용할 수 있다.

그러나 하나의 문항에서 선택, 입력 그리고 양자택일 형태의 답안만을 설정할 수 있는 OCIL은 국내의 정보보안 실태조사 항목을 표현하기에 부족하다. 더욱이 이미 국내의 정보보안 실태조사 항목들은 다양한 유형으로 개발되었고, OCIL이 제공하는 설문 유형이 적기 때문에 향후에라도 이에 맞추어 항목들을 개발하기도 어렵다. 하지만 OCIL을 활용하면 일관된 조사, 분석 및 다른 시스템과의 융합 등이 쉽기 때문에, 자체 데이터베이스와 형식을 사용하는 국내 평가시스템은

OCIL을 적용하되, 다양한 평가 항목 유형을 표현할 수 있는 보조적인 수단을 강구하여 함께 활용해야 할 것으로 판단된다.

4. OCIL XML Converter 설계 및 구현

4.1 평가 항목

최초 작성되는 국내 평가항목은 텍스트 형태이며, 평가항목의 유형은 크게 단답형, 선택형, 복수응답형 3가지로 구분된다.

※ 단답형1 예시: 1.1.2 중앙 행정 기관

Q. '전문직위제도'를 도입하여 정보보안분야 '전문관'을 지정하는가? 1. 전문가를 지정하였다 2. 전문가를 지정하지 않았다

※ 선택형 예시: 1.1.4

Q. 기관장에게 정보보안 업무 관련 사항을 보고하고 있는가? 1. 연중 4회(평균 분기 1회) 이상 보고함 2. 연중 2회(평균 반기 1회) 이상 보고함 3. 연중 1회 보고함 4. 보고하지 않음

※ 복수응답형 예시: 2.1.2

Q. 정보시스템 최신 현황을 유지, 관리 하는가? 1. 서버 최신 현황(50%) 2. 네트워크 장비 및 정보보호시스템 최신 현황(25%) 3. IP가 부여된 PC, 복합기 등정보시스템최신현황(25%) 4. 유지관리 일부 미흡

위의 평가 항목들은 Excel 형식으로 관리되며, Excel파일은 데이터베이스에서 활용하기 위해 좌측에 각각의 항목 내용들의 명칭을, 그리고 문항간 탭으로 구분자를 두어 각 항목을 분리하면 다음 그림과 같이 표현되며, 일반적인 엑셀 형식인 xls 또는 xlsx에서 tsv 형식을 가지게 된다.

Main title	정보보안 정책
Sub title	정보보안 기본활동
Question No	1.1.1
Question	기관 자체 성과평가(BSC 등)에 정보보안 활동을 반영하는가?
choice ref	1.모든조직(또는 개인) 성과평가에 반영함.
choice ref	2.일부조직(또는 개인) 성과평가에 반영함.
choice ref	3.정보보안 업무 수행조직(또는 개인) 외에는 반영하지 않는다.(또는 정보보안 활동을 반영하는 조직이 없다.)
Description	증빙자료: 성과평가 매뉴얼 내 정보보안 활동 반영 지표(반영비율 포함) 평가기준 해설 -기관의 정보보안수준 향상을 위해 정보보안활동(사이버 보안 진단의 날 수행실적, 부서 보안 점검결과, 사이버위기 대응훈련 결과등)를 자체성과평가에 반영할 것을 권고한다. -성과평가시 감점제를 적용할 경우에도 성과평가 반영으로 인정하나, 정보보안 관련 사항을 독립적인 지표로 구성할 것을 권고한다. -기관 성과평가에 정보보안 활동을 반영할 경우, 실효성 확보를 위해 전체 성과 평가에서 5% 이상 반영할 것을 권고한다.

(그림 4) 평가 항목별 명칭 부여

	A	B	C	D	E	F
1	Main title	정보보안 정책	정보보안 정책	정보보안 정책	정보보안 정책	정보보안 정책
2	Sub title	정보보안 기본활동	정보보안 기본활동	정보보안 기본활동	정보보안 기본활동	정보보안 기본활동
3	Question No	1.1.1	1.1.2(중앙 행정 기	1.1.2(공공기관)	1.1.3	1.1.4
4	Question type	Choice	Choice	Choice	Choice	Choice
5	Question	기관 자체 성과평가	전문직위제도'를 도	정보보안부서(담당도	청에 의한 정보수	기관장에게 정보보
6	Choice ref	1.모든조직(또는 개	1.전문가를 지정하	1.성과평가 등에 연	1.자체 도청 탐지등	1.연중 4회(평균 분
7	Choice ref	2.일부조직(또는 개	2.전문관을 지정하	2.성과평가 등에 연	2.자체 도청 탐지등	2.연중 2회(평균 반
8	Choice ref	3.정보보안 업무 수	NA	NA	NA	3.연중 1회 보고하
9	Choice ref	NA	NA	NA	NA	4.보고하지 않았다
10	Choice ref	NA	NA	NA	NA	NA
11	Choice ref	NA	NA	NA	NA	NA
12	Description	증빙자료: 성과평가	증빙자료: 전문관 지	증빙자료: 인센티브	증빙자료: 대도청 탐	증빙자료: 정보보안

(그림 5) tsv 변형

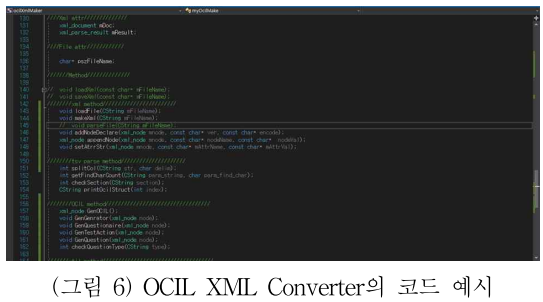
이 tsv 파일을 활용하여 직접적으로 OCIL XML 형태로 변환한다.

4.2 OCIL XML Converter

OCIL XML Converter 모듈을 수행해 tsv 파일을 OCIL 형식으로 변환하며, 개발환경은 다음과 같다.

· 개발환경: window10 · 개발언어: c++/Mfc

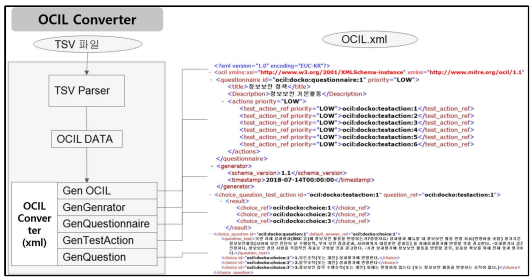
OCIL XML Converter의 코드 예시는 다음과 같다.



(그림 6) OCIL XML Converter의 코드 예시

OCIL XML Converter는 tsv 파일을 읽어 OCIL 형

식으로 변경시키는데, 이때 OCIL을 만들어 이의 세부 규격들인 The questionnaire Element, The test_action Element, The questions Element를 생성하여 국내 평가항목들을 이에 맞추게 된다. 그 결과로 xml 파일을 생성하게 된다.



(그림 7) OCIL XML Converter의 동작 흐름 및 결과

5. 결론

XML은 다양한 종류의 DATA에 적용될 수 있는 유연성과 확장성을 가지고 있기 때문에 여러 계층의 응용프로그램에서 적용될 수 있고, 웹뿐만 아니라 다양한 분야에서 사용되고 있다.

본 논문에서는 현행 보안수준평가체계의 문항을 유형별로 분류하여 분석해 본 결과 우리가 적용하고자 하는 OCIL의 규격과 호환 가능하며, OCIL을 통해 현행 평가문항들을 XML로 변환시킬 수 있었다. 이 변환된 데이터들은 향후 Background Engine을 통해 웹으로 서비스될 수 있으며, 새로운 평가항목이 개발되더라도 Background Engine에 이를 반영할 수 있는 경로를 생성해두어, 웹으로 서비스를 계속할 수 있는 연속성을 확보할 수 있을 것이다.

참고문헌

[1] http://www.datanet.co.kr/news/articleView.html?idxno=92177

[2] 최윤철, “금융 정보보호 수준향상을 위한 정보보호 수준측정 및 취약점 개선에 관한 연구”, 연세대학교, 박사학위논문, 2015.

[3] 김협, 엄수정, 권혁준, “공공기관의 정보보안 솔루션 도입이 정보보안 수준 향상에 미치는 영향”, 한국융합보안논문지, Vol.17, No.5, 2017, pp.19-25.

[4] ~국가사이버안전센터, “정보보안 관리실태 평가 소개”, 한국정보보호학회논문지, Vol. 23, No. 5, 2013, pp. 9-11.

[5] 국방정보통신협회, ‘상호운용성 정보보증 평가기준 고도화 방안 연구’, 2017.

[6] http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000097878

[7] 김대호, 오일석, “미국 전자정부 정보보안 법제 동향”, 한국정보보호학회논문지, Vol. 13, No. 3, 2003, pp. 15-22.

[8] 양정윤, 박상돈, 김소정, “미국의 법제도 정비와 사이버안보 강화 : 국가사이버안보보호법 등 제·개정된 5개 법률을 중심으로”, 입법과 정책, Vol. 7, No. 2, 2015, pp. 305-335.

[9] 최명길, 정재훈, “국외 정보보안관리 동향”, 정보보호학회논문지, Vol. 23, No. 5, 2013, pp. 12-19.

[10] https://blog.naver.com/browbear/220617709359

[11] 백영호, “공공 부문 정보시스템 보안통제 취약성 점검 방안연구”, 감사원 감사연구원

[12] 윤오준, “보안 중요도에 따른 정보자산 분류 방법론 연구”, 건국대학교, 석사학위논문, 2013.

[13] JOINT TASK FORCE, ‘Guide for Applying the Risk Management Framework to Federal Information Systems’, NIST Special Publication 800-37 Revision 1, February 2010.

[14] https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/Specifications/ocil

〔저자소개〕

김 종 민 (Jongmin Kim)
2010년 체육학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과
초빙교수

email : dyuo1004@gmail.com

김 상 춘(Sang-Choon Kim)

1999년 8월 충북대 이학박사
1983년 ~ 2001년: ETRI 선임
2001년 ~ 2010년: ETRI초빙연구원
2001년 ~ 현 강원대학교 정교수

e-mail : kimsc@kangwon.ac.kr