情 報 保 護 學 會 誌
第21卷 第6號, 2011. 10

OCTAVE Allegro 위험 평가 방법론 연구 및 소개

박 준 용*, 임 대 운**

요 약

카네기멜론 대학의 SEI(Software Engineering Institute)는 개인 의료 정보의 보안을 규정한 HIPPA(Health Insurance Portability and Accountability Act)의 조항을 미 국방부(DoD)가 제정하면서 직면하게 된 보안 준수의 난항을 해결하기 위해서 TATRC(Telemedicine and Advanced Technology Research Center)와 공동으로 자산 식별 및 정보보호 위험평가를 위한 방법론인 OCTAVE를 개발하였다. 이후 조직의 운영 과정에서 발생하는 위험의 내성을 높이기 위한 질적 위험평가 기준이 개발되었으며 이를 통해 조직의 중요한 자산 및 잠재적 위협과 취약점을 식별하는 위험평가 방법으로 발전하였고, 2005년에는 100명이하의 소규모 조직에 적합한 OCTAVE-S가 발표되었다. 오늘날 급변하고 있는 IT 환경에서 기존의 OCTAVE 보다 간소화되고 최적화된 위험평가 프로세스를 제공하기 위해서 2007년에 OCTAVE Allegro 프레임워크가 개발되었다. 본고에서는 기존의 OCTAVE 방법론의 주요 특징을 살펴보고, 정보자산 중심의 OCTAVE Allegro 위험 평가 방법론을 소개한다.

Ⅰ. 서 론

기업의 생존력은 비즈니스 목적과 연계되고 보유하고 있는 핵심자산의 기밀성, 무결성, 가용성을 유지하기 위한 정보보호 라이프 사이클에 준한 평가활동을 얼마나 잘 하느냐에 달려있다. 오늘날 급변하고 있는 정보기술(IT)의 패러다임에 준한 정보보호 관리(ISM)는 기업의 자산에 대한 안전성 및 신뢰성을 향상시키고 자산에 대한 위협과 취약점을 평가한 후 적절한 보호대책을 선택하는 위험관리 활동과 연계되고 있다. 미국 카네기멜론대학 SEI(Software Engineering Institute)는 정보보호위험을 보다 정확하고 신속하게 대응할 수 있는 평가체계를 제공하기 위하여 OCTAVE(Operationally Critical Threat, Asset, and Vulnerability, Evaluation)^{SM} 위험평가 방법론을 개발하였다. 위험평가 프로세스인 OCTAVE 프레임워크가 개발된 후 정부, 교육, 의료 등에 적용되어왔으며, 100인 이하 조직의 규모에 적합한 OCTAVE-S로 진화되었다. 이후 기업의 핵심 자산 중 정보자산에 초점을 맞추어 평가 효율을 제공하기 위해 최적화된 OCTAVE Allegro 프레임워크가 개발되었다.[1]

본 논문은 OCTAVE Allegro를 소개하기 위해서 다음과 같이 구성된다. 2장에서는 위험평가의 개요를 살펴보고, 3장에서는 OCTAVE Allegro 위험 평가 방법론을 소개한 후 기존 OCTAVE 위험 평가 방법론과 비교하며, 4장에서 결론을 맺는다.

Ⅱ. 위험평가의 개요

위험을 위협의 관점으로 표현하면 위협의 발생가능성과 영향의 함수이며, 자산의 관점으로는 특정 자산의 가치와 취약성 그리고 이에 대한 위협의 발생가능성으로 표현된다. 기업은 프로그램관리 위험, 투자위험, 예산위험, 법적책임위험, 인적위험, 보안위험 등과 여러 유형의 위험을 포함하고 있다.[2] 이중 보안위험은 기업의 중대한 위험요소 중 하나로써, 정보시스템 사용 및 운영과 연계된 정보자산의 취약성으로 인해 가해지는 위협 발생의 가능성과 발생 시 영향의 함수로 표현할 수 있다. 일반적으로 위험 평가 방법론 구성은 크게 1) 자산평가 2)위협평가 3)취약성평가 4)위험산정 5)위험대응으로 이루어진다.[3]

* 동국대학교 국제정보대학원 홈네트워크보안 연구소 (gsiai@dongguk.edu)
** 동국대학교 공과대학 정보통신공학과 (dwlim01@dongguk.edu)

2.1 정보보호관리

정보보호 관리는 위험관리의 상위개념이며 위험관리는 위험평가의 상위개념이다. 국내·외 보안관리 기준들에서는 정보보호관리, 위험관리, 위험평가 단계별로 다양한 통제 항목이 제시되어 있다. 이러한 통제항목은 단계별 보안 관리의 상위 수준에서 관리적 또는 비 기술적으로 평가하는데 활용될 수 있다.

- 정보보호관리(ISM; Information Security Management): 정보보호관리는 조직의 정보시스템에 대한 전반적인 사항을 다루며 정보보호에 관련된 업무는 몇 개의 통제 분야로 구분되며, 각 통제 분야는 다수의 통제 항목으로 구성된다. ISO/IEC-13335(GMIT), ISO/IEC27000시리즈, 영국의 BS-7799(ISO/IEC 17799), 독일 BSI의 BSI IT Baseline Protection Manual, 미국의 SSE-CMM, 한국의 정보보호 관리기준은 정보보호관리를 위한 표준 및 지침이다.

- 위험관리(RM; Risk Management) 위험관리는 정보보호 관리를 수행함에 있어서 최소의 비용으로 최고의 효과를 달성하고자 통제 분야의 우선순위를 결정하고 수행하는 방법 중의 하나이며 그 범위는 매우 넓다.

- 위험평가(RA; Risk Assessment) 위험평가는 보안 관련 항목별 식별된 자산 중 핵심자산에 대해 잠재적 위협의 발생 가능성과 피해 가능성 등을 정량적 또는 정성적으로 계량적 평가를 하는 것이다.

2.2 위험관리와 위험평가의 비교

위험관리와 위험평가는 상호 호환되지 않는다. [표 1]에서 보는 바와 같이 위험관리는 위험을 비즈니스 전반에 허용 가능한 수준으로 관리하려는 전반적인 노력으로 정의된다. 이해 반해 위험평가는 위험을 감소하기 위해 보안대책을 선정하고 선정된 보안 대책이 어느 정도 위험 수준을 완화하는지와 보안대책들을 모두 구현한 후에도 남을 수 있는 위험에 감당할 수 있는 수준인지 평가하는 활동으로 정의된다. 위험관리와 위험평가의 또 다른 차이점은 각 프로세스의 수행 빈도이다. 일반적으로 지속적으로 수행되는 위험관리는 정기적인 간격으로 다시 시작되어 각 프로세스 단계의 데이터를 갱신한다. 위험평가는 위험관리 프로세스의 필수적인 고유한 단계이지만, 정보보호 조직은 현재 위험관리 단계 또는 예산 주기와는 독립적으로 위험평가를 수행할 수 있다. 정보보호 조직은 새롭게 발견된 위협 및 취약점, 인프라 변경사항 등과 같이 비즈니스 내에서 잠재적으로 보안 관련 변경 사항이 발생하면 언제라도 위험평가를 시작할 수 있다. 이러한 위험평가는 특별 위험평가 또는 제한된 위험평가로 수행되는 경우가 있으며, 이는 공식적인 위험관리 프로세스의 보완 수단으로 검토된다. 특별 위험평가는 일반적으로 비즈니스 내 한 가지 위험 분야에만 중점을 두고 평가하므로 전체적으로 위험관리 프로세스와 동일한 양의 리소스가 필요하지 않다.[4]

〔표 1〕 위험관리와 위험평가의 비교

구분	위험관리	위험평가
목표	비즈니스 전반의 위험을 허용 가능한 수준으로 관리	조직 내 식별된 위험 확인 및 우선순위 지정
단계	평균 네 단계의 전반적인 프로그램	위험 관리 프로그램의 독립적인 단계
주기	지속적	필요에 따라
시기	예산주기에 맞게 조정	해당 없음

Ⅲ. OCTAVE Allegro 위험 평가 방법론 소개

OCTAVE 위험평가 방법론은 조직의 비즈니스를 위한 자산 기반의 정보보호 전략평가와 계획을 위한 방법론이며 3가지 프레임워크로 개발되었다. 300명 이상의 대규모 조직을 대상으로 하는 OCTAVE가 1999년에 최초로 개발된 후, 2005년에는 100명 이하의 소규모 조직에 적합한 OCTAVE-S가 개발되었고, 2007년에는 정보보호자산 중심의 OCTAVE Allegro가 발표되었다. OCTAVE 방법론은 정보보호 평가를 위한 실무기반과 위험을 조정하는 표준 방법론의 하나로 분류되어 있다.[5]

3.1 OCTAVE Family 위험 평가 방법론 개요

OCTAVE는 질적 위험 평가 기준에 따라 조직의 중요한 자산들의 위협과 취약점을 식별하고 비즈니스 목표와 사명을 달성하기 위한 전략적 동인(動因, Driver)

〔표 3〕 OCTAVE과 OCTAVE-S의 단계별 프로세스 비교 및 입·출력 관계 분석[11]

구 분	OCTAVE		OCTAVE-S	
	Process		Process	
Phase 1 자산기반 위협프로파일 구축	Process1: 경영층 지식 정의	I(5), W(5), O(7)	Process1:조직정보 식별	Activity(3)
	Process2: 운영층 지식 정의	I(6), W(5), O(7)	·	·
	Process3: Staff 지식 정의	I(5), W(5), O(6)	·	·
	Process4: 위협 프로파일 생성	I(3), W(3), O(7)	Process2:위협프로파일 생성	Activity(4)
Phase 2 인프라 취약성 정의	Process5: 핵심요소 정의	I(2), W(1), O(3)	·	·
	Process6: 선택된 요소 평가	I(1), W(1), O(3)	Process3:정보인프라 조사	Activity(2)
Phase 3 보안전략 및 계획 개발	Process7: 위험 분석	I(3), W(2), O(3)	Process4:위험 분석 / 식별	Activity(3)
	Process8: 보호전략 개발	I(4), W(5), O(6)	Process5:보호전략 개발	Activity(5)

〔표 2〕 OCTAVE와 다른 방법론의 차이점[8]

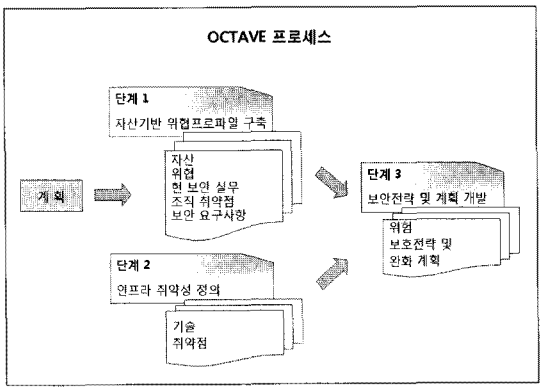
구분	OCTAVE	비 OCTAVE
대상	조직 평가	시스템 평가
형태	보안실무 중심	기술 중심
기준	전략적 이슈	기술적 이슈
특징	자체 감독	전문가 지도

역할을 하는 정보보호 위험평가 방법론이며, 이를 통하여 조직의 운영 위험에 대한 내성을 높일 수 있다.[6] 또한 이 방법론은 IT 보안 요구 사항을 해결하기 위해 조직의 고유한 위험 환경, 보안 목표와 기술 수준에 따라 유연하게 응용 될 수 있고, 위험 기반 관점과 IT 변화에 대응하기 위한 기술적 해결을 제공할 수 있는 진화적인 방법론이다.[7]

3.2 OCTAVE Family 위험 평가 방법론 비교

3.2.1 OCTAVE 방법론

OCTAVE는 정보, 데이터, 시스템, 인프라 등과 같은 중요한 자산을 식별하고 그 중 가장 핵심적이라고 판단되는 자산에 대해 초점을 맞추어 위험분석 활동을 수행하는 위험 평가 방법론으로서, 300명 이상의 직원으로 구성된 조직의 위험 평가에 적용된다. OCTAVE 지침서에는 평가수행 절차와 인터뷰 방법, 워크시트, 정보카탈로그, 분석팀 훈련방법이 포함되어 있으며, 전체 활동은 [그림 1]과 같이 3개의 단계로 구성된다. 단계 1에서 분석 팀은 조직 내 중요한 정보자산의 위협을 분석하기 위해 위협프로파일을 구축하고, 단계 2에서는 단계 1에서 수행된 위협 분석을 보완하기 위해 핵심 자산과 연관된 정보기술과 취약성을 정의한다. 마지막으로 단계 3에서 정보인프라 평가를 수행하고 대응전략을 통한 보안전략 및 계획을 개발한다.[9]



〔그림 1〕 OCTAVE 수행 프로세스

3.2.2 OCTAVE-S 방법론

100명 이하 소규모 조직의 위험평가를 위해 개발된 OCTAVE-S는 기존의 OCTAVE와 수행 단계는 동일하나 프로세스는 5단계로 축소되어 적용된다.

OCTAVE-S에서 광범위한 지식과 통찰력이 요구되는 분석 팀은 약 3~5명으로 구성된다. 평가팀은 공식적인 정보의 수집을 워크숍에 의존하지 않으며, 정보자산, 보안요구사항, 위협, 조직의 보안 실무를 수행한다.[10]

[표 3]은 OCTAVE와 OCTAVE-S의 단계별 프로세스 및 세부 활동을 나타낸다. OCTAVE는 프로세스 별 인터뷰(I), 워크시트(W), 산출물(O)의 수를 표기하였고, OCTAVE-S는 프로세스 별 주요 활동 수를 표기하였다. OCTAVE-S는 위험 평가가 진행되는 동안 조직의 특성과 요구 사항에 따라 운영 위험과 기술, 보안 실무에 대한 적절한 균형을 유지한다. 또한 OCTAVE-S는 프로세스 수가 축소되었으나, 기존의 OCTAVE와 동일한 정보보안 위험평가 목적을 달성한다.

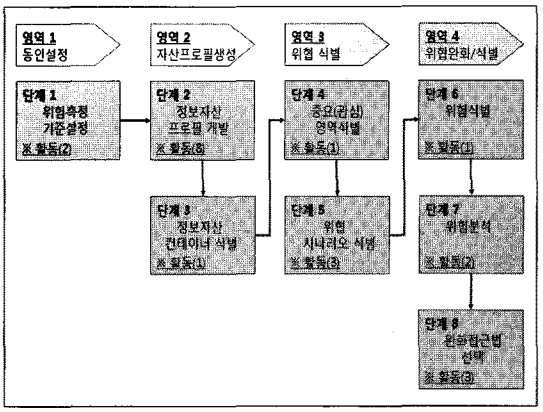
3.3 OCTAVE Allegro 위험 평가 방법론 소개

3.3.1 OCTAVE Allegro 방법론 개요

OCTAVE Allegro는 조직의 운영 환경에 최적화된 위험평가를 신속히 수행하면서도 상세한 결과를 도출할 수 있도록 설계되었다. OCTAVE Allegro는 정보자산을 어떻게 사용하고 저장, 운반, 처리하며 어떤 위협과 취약점에 노출되어 서비스가 중단되는지 등 상황에 주로 초점을 맞추고 있다. OCTAVE Allegro는 기존의 방법론과 같이 별도의 설문지, 가이드, 워크시트를 활용하며, 워크샵과 협업 방식으로 평가를 수행하고 지원할 수 있다. 또한 OCTAVE Allegro는 광범위한 조직의 참여나 전문 지식 없이 위험평가를 수행 하려는 개인에게도 적합하다.

3.3.2 OCTAVE Allegro 위험평가 영역

OCTAVE Allegro는 4개의 영역(Domain)으로 구성되어 있다. 동인 설정(Establish Drivers) 영역은 조직의 추진 목적에 부합하는 위험 측정 기준을 개발한다. 자산 프로필 생성(Profile Assets) 영역은 위험평가의 초점인 자산의 컨테이너와 정보자산 프로필을 식별하는 영역이다. 여기서 컨테이너는 조직의 정보 자산 사용, 저장, 운반 및 처리를 수용할 수 있는 공간을 의미하며, 프로필은 정보 자산의 독특한 기능, 품질, 특성, 값 등을 표현하는 정보 자산 표현의 집합체를 의미한다. 위협 식별(Identify Threats) 영역은 컨테이너 내 자산의 위협을 구조화된 처리를 통하여 문서화하고 식별한다. 위험 완화와 식별(Identify and Mitigate Risks)영역은 개발된 완화 전략과 위협 정보를 기반으로 조직의 정보자산 위험을 식별하고 분석한다.



〔그림 2〕 OCTAVE Allegro 영역별 단계

3.3.3 OCTAVE Allegro 위험평가 단계

OCTAVE Allegro는 8 단계로 진행된다. 단계 1은 조직의 비즈니스 목적 달성과 연계된 정보 자산의 위험평가에 사용될 조직의 동인을 설정한다. 단계 2는 조직의 정보 자산에 초점을 맞추어서 해당 자산에 대한 프로필을 만들고, 단계 3은 정보 자산에 대해 프로필을 만든 후 컨테이너에 정보 자산이 저장, 운반, 처리되는 과정을 식별한다. 단계 4에서 조직의 정보 자산에 위협이 될 수 있는 상황과 조건은 중요 영역(Area of Concern)으로 정의된다. 이 단계에서는 중요 영역에 관한 브레인스토밍을 통해 위험 함수의 주요 인자인 위협 요소를 도출 한다. 단계 5에서는 전 단계에서 도출된 중요 영역이 위협의 속성을 자세히 기술하는 위협 시나리오로 확장된다. 단계 6에서는 위협이 현실화 되는 경우 조직에 발생될 수 있는 결과들을 도출하며, 이러한 결과들은 위험으로 정의된다. 단계 7은에서는 위험의 영향과 발생 가능성을 정량화하여 위험의 우선순위를 결정한다. 마지막으로 단계 8은 완화가 필요한 위험들을 결정하고, 이러한 위험을 완화하기 위한 전략을 수립한다.

OCTAVE Allegro 방법론을 적용하기 위해서 우선적으로 아래와 같은 요구 사항을 충족해야 한다. 이러한 요구 사항은 수행해야 할 항목, 필요성과 함께 수행 결과를 측정할 수 있는 방법을 포함한다.

- 사용 용이성 향상
- 평가 범위 한정
- 훈련과 사전 지식 축소
- 평가를 위한 필요한 자원 최소화

- 연속적인 위험 관리 절차 제도화
- 기업 전반의 일관적이고 비교할만한 결과 산출
- 위험 평가를 위한 핵심 역량 개발 촉진
- 기업 보안 준수를 위한 활동 지원

OCTAVE Allegro 방법론에서 특별히 개선된 점은 (1) 리소스 수집과 가이드 간소화 (2) 자산 중심으로 개선(정보자산 프로파일링 및 보안 요구사항 정의) (3) 위협 식별 간소화 (4) 실무관행 제거 (5) 기술적 관점의 분석 축소(취약점 테스트 제거 및 컨테이너 개념 도입, 정보환경 개념 조사 추가) (6) 분석능력 개선(정보자산 위험 워크시트 개발, 정량적 분석 수행) (7) 위험완화 가이드 개선 (8) 훈련 및 지식 요건 간소화이다. 식별된 위험에 대해 기존 OCTAVE 방법론은 정성적 위주의 평가를 수행하였으나, OCTAVE Allegro 방법론은 정량적 평가가 가능한 요소를 도입하여 신뢰성을 향상 시켰다.[12][13]

3.3.4 OCTAVE Allegro 위험평가 수행방법

OCTAVE Allegro 방법론을 위험평가 수행에 보다 효과적으로 적용하기 위해서는, 사전에 평가에 필요한 조직의 자원을 할당하고 평가 활동 영역을 보장해야 한다. 또한 성공적인 수행은 고위 경영진의 적극적인 후원이 있어야 하며 평가팀 구성원이 프로세스 수행에 전념할 수 있는지, 충분한 자원이 프로세스에 할당이 되어 있는지 확인해야 한다. OCTAVE 방법론의 평가 실무 지식을 기반으로 평가를 수행하며, 평가 수행 시 OCTAVE Allegro 방법론과 연관된 설문지와 워크시트를 활용하여 상황별 기술 보고서를 적용할 수 있다. 효율적인 평가수행을 위해서 가이드에 포함되어 있는 워크시트, 설문지, 가이드를 평가에 활용하면 되고 하나 이상의 정보 자산 평가 시에는 [그림 2]의 단계 2를 반복하면 된다.

평가를 실시할 정보 자산을 선택하기 위해서는 조직의 중요 프로세스를 지원하는 자산에 대한 이해가 필요하다. 이를 성공적으로 수행하기 위해서는 핵심 자산을 선택하고 이를 정량화하기 위한 일관적인 방법을 제공할 수 있어야 한다. 따라서 위험측정 기준을 개발할 때는 조직의 위험측정 기준을 만드는 것을 포함해서 위험 내성의 관리 및 의도를 반영해야 하고 범위를 조직의 전체에 보편적으로 적용해야 한다.[14]

3.4 기대효과 및 향후 연구방향

OCTAVE Allegro는 정보보호 위험을 이해하고 신속히 대응 및 관리할 수 있는 조직의 역량을 촉진할 수 있도록 조직 중심의 평가 및 계획 도구를 제공한다.

OCTAVE Allegro 방법론은 조직의 비즈니스 프로세스와 서비스가 연계된 상황에서 위험 완화를 최적화함으로써 조직이 지속할 수 있는 전략과 보호를 보장할 것이다. 또한 조직의 모든 기능 영역을 보장하기 위해 필수적인 활동과 조직 내부의 운영 단위 수준에 맞추어져 프로세스가 집중될 것이다. OCTAVE 방법론은 위험평가 단계별 유지와 운영을 위해 SDLC(Software Development Life Cycle)에 연계되어 적용되었고, 비용 대비 효과를 제공하기 위해 보안 요구사항을 도출하고 정보 자산을 보호하기 위한 필요한 모든 통제 사항을 제공하고 있다.

사실상 OCTAVE Allegro 방법론은 위험 평가 수행에 하나의 표준으로 정보보호 커뮤니티에 수용되어 있으며, 향후 정보보호 및 비즈니스 연속성을 위해 조직이 운영 위험을 관리할 수 있는 방법과 탄력성을 찾고 지속적으로 성장하기 위해 진화할 것이다.[15]

Ⅳ. 결 론

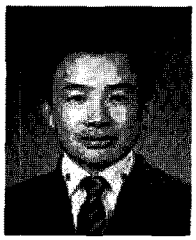
본 논문에서는 카네기멜론대학의 SEI에서 개발한 OCTAVE Allegro 위험평가 방법론을 소개하였다. 정보보호 관리 기반이 취약한 비즈니스는 제한적이기 때문에, 정적인 보안 개념을 동적인 개념으로 승화시켜 구체적으로 시행하고 대응하는 일련의 위험평가 활동을 통해서 비즈니스의 목표와 정보보호의 목표를 일치시켜야 할 필요가 있다. 또한 기업이 전사적 위험을 객관적으로 평가하고 적절한 대응책을 유지할 때 비즈니스 연속성이 보장되는 것은 널리 알려져 있다. 향후 정보보호 관련 위험 평가를 수행 시 본 논문에서 소개한 OCTAVE Allegro 방법론을 기업 규모와 유형에 맞게 적용한다면 충분히 기업의 운영 목적과 비즈니스 연속성을 보장할 수 있을 것으로 기대된다.

참고문헌

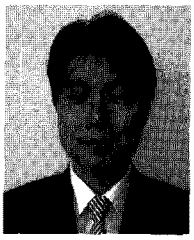
[1] Richard A. Caralli and James F. Stevens, "Introducing OCTAVE Allegro: Improving the Informat-

ion Security Risk Assessment Process," Technical Report of CMU/SEI, pp.1 Introduction, May 2007
[2] NIST Special Publication 800-39, "Managing Information Security Risk," Organization, Mission, and Information System View, pp.10, May 2011
[3] 이재우, 박성준, 홍기웅, 신수정, 김학범, "사이버 보안과 홈네트워크," pp.214-219, 2010년 11월
[4] 한남대학교, "통합시스템 보안성 평가체계 및 방법 연구", 부록 G.위험분석, 2006년 11월
[5] OCTAVE 홈페이지, http://www.cert.org/octave/
[6] Richard A. Caralli, and James F. Stevens, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," pp.1, May 2007.
[7] OCTAVE 홈페이지, http://www.cert.org/octave/
[8] Christopher Alberts, Audrey Dorofee, "OCTAVE-s Implementation Guide, Version 1.0, 2.2 Overview of OCTAVE-s, pp.3-4, Jan. 2005.
[9] Christopher Alberts and Audrey Dorofee, "Managing Information Security Risks," The OCTAVE^{SM} Approach, pp.12, Jun. 2003.
[10] Christopher Alberts and Audrey Dorofee, "OCTAVE-s Implementation Guide, Version 1.0," pp.3, Jan. 2005
[11] Christopher Alberts and Audrey Dorofee, "OCTAVESM Method Implementation Guide Version 2.0, pp.11, Jun. 2001.
[12] Richard A. Caralli and James F. Stevens, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", pp.14, May 2007
[13] Richard A. Caralli and James F. Stevens, "OCTAVE Allegro Guidebook, v1.0," pp.26-28, May 2007
[14] Richard A. Caralli and James F. Stevens, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", pp.23-25, May 2007
[15] Richard A. Caralli and James F. Stevens, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", pp.27-30, May 2007.

〈著者紹介〉



박 준 용 (Jun Yong, Park)
학생회원
2000년 2월 : 동국대학교 반도체과학과 학사
2006년 2월 : 영남대학교 대학원 컴퓨터정보통신공학과 석사
2010년 3월 ~ 현재 : 동국대학교 정보보호학과 홈네트워크보안 석사과정
관심분야 : 융합보안, 스마트그리드, 개인정보보호, 홈네트워크보안, 위험평가



임 대 운 (Dae Woon, Lim)
정회원
1994년 2월 : 한국과학기술원 전기 및 전자공학과 학사
1997년 2월 : 한국과학기술원 전기 및 전자공학과 석사
2006년 8월 : 서울대학교 전기·컴퓨터공학부 박사
1995년 9월~2002년 8월 : LS산전 선임 연구원
2006년 9월~현재 : 동국대학교 정보통신공학과 조교수
관심분야 : 이동통신, 암호학, 정보보안