情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

정보보호 요소의 통합에 관한 선행 연구: COBIT 4.1과 ISO/IEC 27002:2005의 매핑을 중심으로

김 정 현*

요 약

기업의 비즈니스 환경에서 정보보호의 중요성이 높아감에 따라 정보보호와 관련된 표준이나 벤치마크의 필요성도 증대되었다. 이러한 표준에는 ISO/IEC 27001, ISO/IEC 27002, PCIDSS, ITIL, COBIT 등이 유명하다. 본 논문에서는 IT 거버넌스의 프레임워크로서 폭 넓은 범위의 정보보호 플랫폼이 될 수 있는 COBIT 4.1과 정보보호를 위한 상세한 최선의 실무(best practice)를 담고 있는 ISO/IEC 27002의 각 정보보호 요소에 대해 간략히 알아보고, 이들을 서로 매핑하여 "높은 수준"의 프레임워크와 "낮은 수준"의 방법론의 통합에 대한 방향을 제시하고자 한다.

Ⅰ. 서 론

최근 기업의 비즈니스 환경에서 정보보호의 중요성은 더욱 높아지고 있다. 기업의 전략적 목표를 달성하기 위해서는 IT를 활용하지 않을 수 없게 되었으며, 이에 따라 기업의 정보 자산에 대한 중요성도 점점 커져가고 있다.

또한 기존에는 오프라인에서만 운영되던 기업의 비즈니스가 인터넷 환경의 발달로 인해 온라인 비즈니스로 그 활동 터전을 급격히 이동하고 있다. 따라서 기업의 비즈니스 환경을 위협하는 형태도 기존의 오프라인 리스크에서 온라인 리스크로 바뀌고 있으며, 특히 기업의 중요 정보 자산에 대한 침해 사건은 지속적으로 늘어나고 있다.

한 조사 보고서에 따르면, 2012년 미국에서 발생한 데이터 침해 사고 건수는 2,644건으로 전년도의 1,217건에 비해 2배 이상으로 급증했음을 보여 주었다. 또한 이러한 경향이 2009년도부터 계속해서 증가 추세에 있음도 보여 주었다. 특히 유의할 점은 2012년도의 침해 사건 유형 중에서 거의 90%가 전자 데이터와 관련되었다는 것이다. [1]

그러므로 기업으로서는 자사의 정보 자산을 보호하고 관리하는 것이 기업의 비즈니스 연속성 측면에서 필수불가결한 업무가 되었다. 이를 위해 정보보호에 대한 거버넌스를 다루는 표준이나 벤치마크의 필요성도 그만큼 증대되었다.

적정한 수준의 보호가 이루어지고 있는지, 이를 위한 정보 자산이 올바로 사용되는지, 그리고 정보보호를 위한 최선의 실무(best practice)가 조직에서 채택되고 있는지 등은 IT 거버넌스와 관계가 있다. 이러한 IT 거버넌스를 위한 여러 가지 표준(standard)이 개발되었는데, 그 중에서 소위 Big Five라 불리는 ISO/IEC 27001:2005, BS 7799 (ISO/IEC 27002:2005), PCIDSS, ITIL, 그리고 COBIT이 특히 유명하다. [2]

이 중 PCIDSS는 카드결제, ATM, POS 등에서의 거래 데이터 정보보호에서만 사용되는 한정적인 표준이고, ITIL은 정보보호가 아니라 IT 서비스 관리를 위한 표준이다. 그리고 ISO/IEC 27001은 정보보호 관리체계(ISMS)의 요구사항으로 ISMS 인증 심사 시에 심사기준으로 사용되는 국제 표준이기에 일반적인 기업의 정보보호 담당자가 참고하기에는 적당하지 않다.

따라서 본 논문에서는 상기 표준들 중에서 IT 거버넌스의 가장 기본 프레임워크인 COBIT과 국제적인 정보보호관리체계(ISMS)에서 정보보호에 대한 실무지침

* (주)씨에이에스, ISACA 한국협회 보안부문 이사 (kimius@gmail.com)

(code of practice)을 다루고 있는 ISO/IEC 27002에 대해 살펴보고, 양 프레임워크/표준 간 연관되는 정보보호 요소 사이의 매핑을 소개하기로 한다.

Ⅱ. COBIT 프레임워크

2.1 COBIT의 역사

ISACA(Information Systems Audit and Control Association: 정보시스템감사통제협회)와 ITGI(IT Governance Institute)에 의해 1996년 탄생된 COBIT (Control Objectives for Information and related Technology)은 IT 거버넌스를 위한 대표적인 프레임워크 중 하나이다.

처음 1.0판에서는 감사(audit)에 초점을 맞추었고, 1998년 2.0판에서는 통제(control)에, 그리고 2000년 3.0판에서는 관리(management)에 중점을 두었다.

2005년 4.0판에서는 사후, 사전, 교정 통제를 포함하여 기업의 최상위 수준에서 기업의 목적과 전략을 지원하는 거버넌스 차원, 즉 IT 거버넌스를 구현하는 방법론이자 프레임워크로 자리잡게 된다.[3]

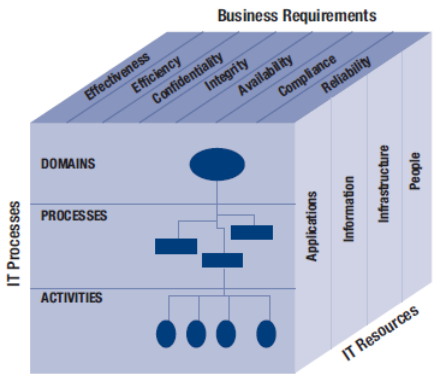
이후 COBIT은 2007년 개정판인 4.1판을 거쳐 2012년에 새로운 판이 나오기 전까지 거의 7년간 IT 거버넌스에서 사실상의(de facto) 국제표준으로 자리를 잡았다.

2.2 IT 거버넌스와 COBIT 4.1의 특징

기업을 이사회 레벨에서 거버넌스하고 통제하는 시스템을 전사 거버넌스(enterprise governance)라고 한다면, 이러한 전사 거버넌스 중에서 특별히 기업의 IT가 기업의 전략과 목표를 유지하고 확대하는 것을 보장하는 지배구조를 IT 거버넌스라고 한다.[4]

이러한 거버넌스를 위해서는 성과(performance; 여기에는 수익, 효과성, 그리고 효율성의 증대가 있다)와 준수(conformance; 여기에는 법률, 내부 정책, 그리고 감사 요구사항의 엄수가 있다) 사이에 균형을 맞출 필요가 있는데, 이사회가 여기에서 거시적인 방향 설정(지휘와 통제)을 한다. 즉, IT 거버넌스에서는 리스크對 IT 수익률 사이에서 이사회가 적절하게 균형 잡힌 방향 설정을 통해 기업의 목표를 달성하는 것이라 할 수 있겠다.[5]

COBIT 4.1은 기업의 IT가 비즈니스 요구사항을 만족시켜 IT의 목적을 달성하기 위해 IT 프로세스를 사용하여 IT 자원을 관리하는 하나의 큰 틀(프레임워크)로 요약될 수 있다. 이는 다음의 [그림 1]로 표현될 수 있다.[6]



〔그림 1〕 COBIT 큐브

기업의 IT가 궁극적으로 지향하는 목적은 기업 비즈니스의 요구사항을 완벽히 지원하여 기업 전체의 비즈니스를 성공적으로 이끄는 것이다. 이를 위해 IT는 일정한 기준이나 규범을 가진 정보(information)를 비즈니스에 제공해야 하는데, 그러한 정보의 7가지 기준이 바로 COBIT 큐브의 한 면을 이루는 효과성, 효율성, 기밀성, 무결성, 가용성, 준거성, 그리고 신뢰성이다.

이러한 의미 있는 정보를 IT가 제공하기 위해서는 기업의 IT 자원을 활용해야 하는데, [그림 1]의 한 면을 이루는 어플리케이션, 정보, 인프라, 그리고 인적자원이 4가지 IT 자원을 구성한다.

COBIT 큐브의 마지막 면은 기업의 IT가 IT 자원을 이용하여 구체적으로 어떻게 정보를 만들어내는가에 해당되며, 이는 IT 프로세스이다. COBIT의 IT 프로세스는 3단계의 층으로 나눌 수 있는데, 제일 상위에 4개의 도메인이 있고, 그 아래에 34개의 프로세스가 있으며, 마지막으로 210개의 구체적인 수행활동(통제목적)이 있다.[3]

COBIT 4.1의 34개 프로세스를 구분하는 4개의 도메인은 PO(Plan & Organise; 계획 및 조직), AI(Acquire & Implement; 도입 및 구축), DS(Deliver & Support; 운영 및 지원), ME(Monitor & Evaluate; 감시 및 평가)로 이루어지는데, 이는 데밍(Deming) 박사의 PDCA

(Plan-Do-Check-Action) Cycle에 기반하고 있다.[4]

이러한 34개의 각 프로세스마다 역할과 책임을 규명한 RACI 차트와 조직의 역량을 진단할 수 있는 성숙도 모델이 각각 제공된다.

그런데 COBIT은 수많은 IT 프로세스를 관리해야 하므로 각각의 IT 프로세스를 그에 맞는 통제 목적별로 분류하는데,[3] 이처럼 COBIT 프로세스가 기본적으로 갖춰야 할 통제 요구사항들을 프로세스 통제(Process Control)라 하고, PC1~PC6까지 모두 6개가 있다.

그리고 COBIT의 IT 프로세스는 일반 IT 통제와 오직 개발 단계의 응용 통제만 다루는데, 이 개발 단계 이외의 나머지 응용 통제는 전부 현업 부서(비즈니스 프로세스 소유자)의 몫이다. 이 때 응용 통제가 갖추어야 할 요구사항으로 응용 통제 목적(Application Control Objective)이 있는데, AC1~AC6까지 모두 6개가 있다.

비록 2012년에 새로운 COBIT 5가 나왔으나 아직까지 실무에서 적용되는 대부분의 COBIT은 4.1판이라는 점을 고려한다면, 정보보호 표준인 ISO/IEC 27002와의 매핑도 여전히 의미가 있으리라고 본다.

2.3 COBIT 4.1과 ISO/IEC 27002와의 매핑

COBIT 4.1의 34개 프로세스 중 ISO/IEC 27000 시리즈의 정보보호와 직접 관련된 것은 “DS5 시스템 보안의 확보“ 하나이지만, 나머지 프로세스 및 하위 통제목적 또한 4개의 도메인 전체에 걸쳐서 정보보호에 대해 조금씩 다루고 있다.[4] 따라서 본 논문에서는 ISO/IEC 27002와의 매핑에 COBIT 4.1의 통제 목적을 정보보호 요소로서 사용한다.

Ⅲ. ISO/IEC 27002

3.1 ISO/IEC 27002의 역사와 특징

ISO/IEC 27002는 원래 영국 규격(British Standard; BS)인 BS 7799에서 유래되었다. 두 개의 파트로 나뉘어 있던 BS 7799는 2000년도에 첫 번째 파트인 BS 7799-1이 ISO/IEC 17799 *Information Technology - Security Techniques - Code of practice for information security management*로 전환되어 국제규격인 ISO 표준이 되었다. ISO/IEC 17799는 2005년도에 개정이 되었고, 2007년도에 ISO/IEC 27002로 명칭만 바뀌어 정식으로 ISO/IEC 27000 시리즈가 되었다. 이 규격의 제목에서 볼 수 있듯이, ISO/IEC 27002는 정보보호 관리에서의 구체적인 실무지침을 다루고 있다.[7]

한편, BS 7799이 두 번째 파트인 BS 7799-2는 2005년에도 ISO/IEC 27001 *Information Technology - Security Techniques - Information security management systems - Requirements*로 전환되었다. 이 표준은 본격적인 정보보호관리체계(ISMS) 인증을 받기 위해 조직(기업)이 갖추어야 할 요구사항에 대해 다루고 있다.[8]

그런데 ISO/IEC 27001 규격서의 뒷부분에 첨부 A (Annex A)라고 해서 통제목적과 통제(Control objectives and controls)라는 제목 하에 133개의 통제항목이 나열되어 있는데, 이는 바로 ISO/IEC 27002의 5항부터 15항까지의 내용을 그대로 인용한 것이다. 다만, ISO/IEC 27002의 내용이 ISO/IEC 27001 첨부 A의 133개 통제항목을 보충하여 더 상세한 권고사항과 최선의 실무(best practice)를 제공해 준다.

ISO/IEC 27002는 5항부터 15항까지 모두 11개의 항(대분류)에 걸쳐 39개의 통제목적(중분류)과 그 하위의 133개 세부 통제항목(소분류)을 가지고 있으면서, 기업 내에서 정보보호관리체계(ISMS)를 구축할 책임이 있는 당사자들에게 유용한 정보를 제공해준다. 즉, IT 거버넌스 프레임워크인 COBIT과 마찬가지로, ISO/IEC 27002도 정보보호를 위해 “무엇”을 해야 하는가를 정의하는데 도움을 준다.[9]

3.2 ISO/IEC 27001과 27002 명칭의 혼용

앞서 설명한 바와 같이 ISO/IEC 27001의 첨부 A의 133개 통제항목의 내용이 ISO/IEC 27002의 5항부터 15항까지의 내용과 겹침에 따라 일부 논문에서 COBIT 및 기타 프레임워크와 매핑을 설명할 때 혼용을 하는 경우가 발생한다.

예를 들어, Razieh Sheikhpour and Nasser Modiri (2012)에서는 ISO/IEC 27001이라고 명기했으나 실제 내용을 보면 ISMS 요구사항이 아니라 첨부 A의 133개 통제항목, 즉 ISO/IEC 27002의 내용임을 알 수 있다.

반면에 *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit (2008)*에서는 같

은 133개의 통제항목이지만 ISO/IEC 27002로 표시하였다.

ISO/IEC 27001의 주 내용은 133개 통제항목이 아니라 ISMS를 위한 요구사항이라는 점을 고려한다면, 이 부분에 있어서는 ISO/IEC 27002로 표시하는 것이 맞다고 본다. 실제로 *COBIT® 5 for Information Security (2012)*에서는 새로 나온 COBIT 5의 프로세스와 매칭을 할 때, ISMS의 요구사항은 ISO/IEC 27001과, 세부 통제항목은 ISO/IEC 27002와 각각 구분하여 대응시키고 있다.[10]

3.3 ISO/IEC 27002와 COBIT 4.1과의 매핑

ISO/IEC 27002의 세부 통제 항목들은 기업의 정보보호에 있어 실무적으로 "어떻게" 하는지에 대한 자세한 지침을 제공해준다. 따라서 본 논문에서는 COBIT 4.1과의 매핑에 ISO/IEC 27002의 통제 항목들을 정보보호 요소로 사용한다.

Ⅳ. ISO/IEC 27002 통제항목을 COBIT

4.1 통제목적에 매핑

IT 거버넌스의 프레임워크인 COBIT 4.1과 정보보호 관리에 있어 최선의 실무를 제공하는 ISO/IEC 27002는 서로 상호 보완적인 관계에 있다.

COBIT 4.1는 범위가 넓은 IT 거버넌스의 프레임워크이기 때문에 정보보호 거버넌스를 위한 좋은 통합 플랫폼(아키텍처)을 제공해주지만, 이 정보보호 거버넌스를 위해 어떻게 하는지에 관한 자세한 지침이 없다. 반면에 ISO/IEC 27002는 "어떻게"에 해당하는 자세한 지침은 제공해주지만, 정보보호에 관한 독자적인 규격이기 때문에 COBIT 4.1이 제공하는 것과 같은 넓은 범위의 플랫폼은 아니다.

따라서 이 둘의 정보보호 요소를 서로 관련되는 것끼리 매칭하는 것은, 정보보호 거버넌스에서 "높은 수준"의 기준 프레임워크로서의 COBIT 4.1과 보다 자세한 방법론을 담고 있는 정보보호를 위한 "낮은 수준"의 지침으로서의 ISO/IEC 27002가 서로 통합되어 기업의 정보보호를 위해 시너지 효과를 얻기 위함이다.[11]

이를 위해 *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit (2008)*에서와 같이 아래의 [표 1]에 ISO/IEC 27002의 통제 항목과 COBIT 4.1의 통제 목적을 서로 매핑하였다.[9]

COBIT 4.1을 기업에 실제 구축한 사례보다 정보보호관리체계(ISMS)를 구축한 사례가 더 많을 것이기 때문에, 이미 구축된 ISMS의 통제 항목별로 COBIT 4.1의 어느 통제 목적이 서로 연관되어 있는지 참고하기 쉽게 매핑 기준을 정하였다.

[표 1]의 ISO/IEC 27002의 분류에서 굵은 글씨체는 통제 목적을, 일반 글씨체는 통제 항목을 나타낸다. COBIT 4.1의 표에서 PC 기호는 프로세스 통제(Process Control)를, AC 기호는 응용 통제(Application Control)를 나타낸다.

〔표 1〕 ISE/IEC 27002의 정보보호 요소(통제 항목)와 COBIT 4.1의 정보보호 요소(통제 목적) 사이의 매핑

ISO/IEC 27002 분류	COBIT 4.1 통제목적
4.1 보안 리스크를 평가	PO9.4 리스크 평가
4.2 보안 리스크를 처리	
5.1 정보보안 정책	
5.1.1 정보보안 정책 문서	PO6.1, PO6.2, PO6.3, PO6.5 DS5.2, DS5.3, ME2.1
5.1.2 정보보안 정책 검토	PO3.1, PO5.3, PO5.4, PO6.3, PO9.4 DS5.2, DS5.3 ME2.2, ME2.5, ME2.7, ME4.7
6.1 내부 조직	
6.1.1 정보보안에 대한 경영 의지	PO3.3, PO3.5, PO4.3, PO4.4, PO4.5, PO4.8, PO6.3, PO6.4, PO6.5, DS5.1
6.1.2 정보보안 조정	PO4.4, PO4.5, PO4.6, PO4.8, PO4.10, PO6.5, DS5.1, DS5.2, DS5.3
6.1.3 정보보안 책임의 할당	PO4.4, PO4.6, PO4.8, PO4.9, PO4.10
6.1.4 정보처리시설을 위한 승인 프로세스	PO4.3, PO4.4, PO4.9, AI1.4, AI2.4, AI7.6, DS5.7
6.1.5 기밀서약	PO4.6, PO4.14, PO8.3, AI5.1, AI5.2 DS5.2, DS5.3, DS5.4
6.1.6 관계당국과의 접촉	PO4.15, DS4.1, DS4.2, ME3.1, ME3.3, ME3.4
6.1.7 특별 이해 그룹과의 접촉	PO4.15, DS4.1, DS4.2
6.1.8 정보보안의 독립적 검토	PO6.4, DS5.5 ME2.2, ME2.5, ME4.7
6.2 외부 당사자들	
6.2.1 외부 당사자들과의 관련된 위험의 식별	PO4.14 DS2.1, DS2.3, DS5.4 DS5.9, DS5.11, DS12.3

ISO/IEC 27002 분류	COBIT 4.1 통제목적
6.2.2 고객에 대한 보안 언급	PO6.2, DS5.4
6.2.3 제3자 협약에서의 보안 언급	PO4.14, PO6.4, PO8.3 AI5.2, DS2.2, DS2.3 DS2.4, DS5.1, ME2.6
7.1 자산에 대한 책임	
7.1.1 자산 목록	PO2.2, DS9.2, DS9.3
7.1.2 자산의 소유	PO4.9, DS9.2
7.1.3 자산의 수용 가능한 사용	PO4.10, PO6.2
7.2 정보 분류	
7.2.1 분류 지침	PO2.3, AI2.4
7.2.2 정보 라벨링과 취급	DS9.1
8.1 고용 전	
8.1.1 역할과 책임	PO4.6, PO4.8, PO6.3 PO7.1, PO7.2, PO7.3 DS5.4
8.1.2 적격 심사	PO4.6, PO7.1, PO7.6 DS2.3
8.1.3 고용약정과 조건	PO4.6, PO7.1, PO7.3 DS2.3
8.2 고용 중	
8.2.1 경영책임	PO4.8, PO4.10, PO4.11 PO7.3
8.2.2 정보보안 인식, 교육, 훈련	PO4.6, PO6.2, PO6.4 PO7.2, PO7.4, PO7.7 AI1.1, AI7.1 DS5.1, DS5.2, DS5.3 DS7.1, DS7.2
8.2.3 징벌 프로세스	PO4.8, PO7.8, DS5.6
8.3 고용종료 및 변경	
8.3.1 면직 책임	PO7.8, DS5.4
8.3.2 자산의 반환	PO6.2, PO7.8
8.3.3 접근권한의 삭제	PO7.8, DS5.4
9.1 보안 구역	
9.1.1 물리적 보안 경계선	DS12.1, DS12.2
9.1.2 물리적 출입통제	DS12.2, DS12.3
9.1.3 사무실, 방, 시설의 보안	DS12.1, DS12.2
9.1.4 외부 및 환경적 위협에 대한 보호	DS12.4
9.1.5 보안구역에서의 작업	PO4.14, PO6.2 AI3.3, DS12.3
9.1.6 일반인 접근, 배달 및 하역 구역	DS5.7, DS12.1, DS12.3
9.2 장비 보안	
9.2.1 장비설치와 보호	DS5.7, DS12.4
9.2.2 유틸리티 지원	DS12.4, DS12.5
9.2.3 케이블링 보안	DS5.7, DS12.4
9.2.4 장비 유지보수	AI3.3, DS12.5, DS13.5
9.2.5 보안영역에서 벗어난 장비의 보안	PO4.9, DS12.2, DS12.3
9.2.6 장비의 안전한 폐기 또는 재사용	DS11.4
9.2.7 자산의 제거	PO6.2, DS12.2
10.1 운영절차와 책임	
10.1.1 문서화된 운영절차	AI1.1, AI4.4, DS13.1 AC1
10.1.2 변경 관리	AI6.1, AI6.2, AI6.3 AI6.4, AI6.5
10.1.3 업무 분장	PO4.11, DS5.4 AC1, AC4
10.1.4 개발, 시험, 운영 시설의 분리	PO4.11, AI3.4, AI7.4

ISO/IEC 27002 분류	COBIT 4.1 통제목적
10.2 제3자 서비스 제공 관리	
10.2.1 서비스 제공	DS1.1, DS1.2, DS1.3 DS2.4
10.2.2 제3자 서비스 모니터링 및 검토	DS1.5, DS2.4, ME2.6
10.2.3 제3자 서비스에 대한 변경 관리	DS1.5, DS2.2, DS2.3
10.3 시스템 계획 및 수용	
10.3.1 용량 관리	DS3.1, DS3.2, DS3.3
10.3.2 시스템 수용	PO3.4 AI1.1, AI1.4, AI2.4 AI2.8, AI4.4, AI7.7
10.4 악성 및 모바일 코드로부터의 보호	
10.4.1 악성 코드에 대한 통제	DS5.9
10.4.2 모바일 코드에 대한 통제	DS5.9
10.5 백업	
10.5.1 정보 백업	DS4.9 DS11.2, DS11.5, DS11.6
10.6 네트워크 보안 관리	
10.6.1 네트워크 통제	PO4.1, DS5.9, DS5.11 AC6
10.6.2 네트워크 서비스의 보안	DS5.7, DS5.9, DS5.11
10.7 매체 취급	
10.7.1 이동가능한 매체의 관리	PO2.3 DS11.2, DS11.3, DS11.4
10.7.2 매체 폐기	DS11.3, DS11.4
10.7.3 정보취급 절차	PO6.2, DS11.6, AC5
10.7.4 시스템 문서의 보안	AI4.4, DS5.7 DS9.2, DS9.3, DS13.1
10.8 정보의 교환	
10.8.1 정보 교환 방침과 절차	PO2.3, PO6.2, DS11.1 AC6
10.8.2 교환 협약	PO2.3, PO3.4 AI5.2, DS2.3
10.8.3 수송 중인 물리적 매체	DS11.6
10.8.4 전자 메세징	DS5.8, DS11.6, AC6
10.8.5 업무 정보 시스템	DS11.6
10.9 전자 상거래 시스템	
10.9.1 전자 상거래	AC4, AC6, DS5.11
10.9.2 온라인 거래	AC3, AC4, AC5, AC6
10.9.3 공개적으로 이용 가능한 정보	PO6.2
10.10 모니터링	
10.10.1 감사 로깅	AI2.3, DS5.7
10.10.2 시스템 사용을 모니터링	DS5.5, ME1.2 ME2.2, ME2.5, ME4.7
10.10.3 로그 정보의 보호	DS5.5, DS5.7
10.10.4 관리자 및 운영자 로그	DS5.5, DS5.7 ME2.2, ME2.5
10.10.5 장애 로깅	AI2.3, DS5.7
10.10.6 시간 동기화	DS5.7
11.1 접근통제를 위한 업무 요구사항	
11.1.1 접근통제 정책	PO2.2, PO2.3, PO6.2 DS5.2, DS5.3, DS5.4
11.2 사용자 접근 관리	
11.2.1 사용자 등록	DS5.4
11.2.2 권한 관리	DS5.4
11.2.3 사용자 패스워드 관리	DS5.3
11.2.4 사용자 접근권한 검토	DS5.4

ISO/IEC 27002 분류	COBIT 4.1 통제목적
11.3 사용자 책임	
11.3.1 패스워드 사용	PO6.2, DS5.4
11.3.2 이석 시의 기기 보안	PO6.2, DS5.7
11.3.3 책상정리 및 화면 삭제 정책	PO6.2, DS5.7
11.4 네트워크 접근 통제	DS5.9
11.4.1 네트워크 서비스 사용에 대한 정책	DS5.9, DS5.11
11.4.2 외부 접속을 위한 사용자 인증	DS5.9, DS5.11
11.4.3 네트워크 장비의 식별	DS5.7, DS5.9, DS5.11 DS9.2
11.4.4 원격진단 및 구성 포트의 보호	DS5.7, DS5.9, DS5.11
11.4.5 네트워크 분리	DS5.9, DS5.11
11.4.6 네트워크 접속 통제	DS5.9, DS5.11
11.4.7 네트워크 라우팅 통제	DS5.9, DS5.11
11.5 운영 시스템 접근 통제	
11.5.1 보안 로그온 절차	DS5.4, DS5.7
11.5.2 사용자 식별 및 인증	DS5.3
11.5.3 패스워드 관리 시스템	DS5.4
11.5.4 시스템 유틸리티의 사용	AI6.3, DS5.7
11.5.5 세션 시간 종료	DS5.7
11.5.6 접속시간의 제한	DS5.7
11.6 어플리케이션과 정보 접근 통제	
11.6.1 정보 접근 제한	DS5.4
11.6.2 민감한 시스템의 분리	AI1.2, AI2.4 DS5.7, DS5.10, DS5.11
11.7 모바일 컴퓨팅과 재택 근무	
11.7.1 모바일 컴퓨팅과 의사 소통	PO6.2 DS5.2, DS5.3, DS5.7
11.7.2 재택 근무	PO3.4, PO6.2 DS5.2, DS5.3, DS5.7
12.1 정보시스템의 보안 요구사항	
12.1.1 보안 요구사항 분석 및 명세화	AI1.2, AI2.4, AI3.2
12.2 어플리케이션에서의 정확한 처리	
12.2.1 입력 데이터 검증	AI2.3, AC2, AC3
12.2.2 내부처리의 통제	AI2.3, AC2, AC4
12.2.3 메시지 무결성	AI2.3, AI2.4, DS5.8 AC6
12.2.4 출력 데이터 검증	AI2.3, AC5
12.3 암호 통제	
12.3.1 암호 통제 사용에 대한 정책	PO6.2, AI2.4, DS5.8
12.3.2 키 관리	DS5.8
12.4 시스템 파일의 보안	
12.4.1 운영 소프트웨어의 통제	DS5.7, DS9.1
12.4.2 시스템 시험 데이터의 보호	AI3.3, DS2.4 DS9.1, DS9.2, DS11.6
12.4.3 프로그램 소스 코드에 대한 접근통제	AI2.4, AI7.4, AI7.6 DS11.3, DS11.6
12.5 개발 및 지원 프로세스에서의 보안	
12.5.1 변경 통제 절차	AI2.6, AI6.2, AI6.3 AI7.2
12.5.2 운영시스템 변경 후 어플리케이션의 기술적 검토	AI2.4, AI3.3, AI7.2 AI7.4, AI7.6, AI7.7 DS9.3
12.5.3 소프트웨어 패키지 변경에 대한 제한	AI2.5, AI6.1, AI6.2 AI6.3, DS9.2
12.5.4 정보 유출	AI2.4, AI7.7
12.5.5 외주 소프트웨어 개발	PO8.3, AI2.7, AI5.2 DS2.4
12.6 기술적 취약점 관리	
12.6.1 기술적 취약점 통제	AI3.3, AI6.2, AI6.3 DS5.5, DS5.7, DS9.2
13.1 정보보안 사건 및 결함 보고	
13.1.1 정보보안 사건의 보고	PO9.3, DS5.6, DS8.2
13.1.2 보안 결함의 보고	PO9.3, DS5.5, DS5.6 DS5.7, DS8.2, DS8.3
13.2 정보보안 사고의 관리와 개선	
13.2.1 책임과 절차	PO6.1, DS5.6, DS8.2
13.2.2 정보 보안 사고로 얻는 교훈	PO5.4, AI4.4, DS8.4 DS8.5, DS10.1, DS10.2
13.2.3 증거의 수집	AI2.3, DS5.6, DS5.7 DS8.2, DS8.3, DS8.4
14.1 업무 연속성 관리 측면에서의 정보보안	
14.1.1 정보 보안을 업무 연속성 관리 프로세스에 포함	PO3.1, PO9.1, PO9.2 DS4.1, DS4.3, DS4.8 DS8.3
14.1.2 업무 연속성 및 위험 평가	PO9.1, PO9.2, PO9.4 DS4.1, DS4.3
14.1.3 정보보안을 포함하는 연속성 계획의 개발과 이행	DS4.2, DS4.8
14.1.4 업무 연속성 계획 프레임 워크	DS4.1, DS8.1, DS8.3
14.1.5 업무 연속성 계획의 시험, 유지 및 재평가	PO3.1, DS4.4, DS4.5 DS4.6, DS4.7, DS4.10
15.1 법적 요구사항에 대한 준거	
15.1.1 적용가능한 법률의 식별	PO4.8, ME3.1
15.1.2 지적 재산권 (IPR)	PO4.8
15.1.3 조직 기록의 보호	PO4.8, DS11.2
15.1.4 데이터 보호와 개인정보의 프라이버시	PO4.6, PO4.8, DS2.2 ME3.1, ME3.3, ME3.4
15.1.5 정보처리 설비의 오용 차단	PO4.14, PO6.2 DS9.2, DS9.3
15.1.6 암호 통제의 규제	PO4.8, DS5.8
15.2 보안 정책 및 표준에 대한 준거성와 기술적 준거성	
15.2.1 보안 정책 및 표준에 대한 준거성	PO4.8, PO6.2, ME2.1 ME2.2, ME2.3, ME2.4 ME2.5, ME2.6, ME2.7
15.2.2 기술적 준거성 점검	DS5.5, DS5.7, ME2.5
15.3 정보 시스템 감사 고려사항	
15.3.1 정보 시스템 감사 통제	AI2.3, DS5.5, ME2.5
15.3.2 정보 시스템 감사 도구의 보호	AI2.3, AI2.4, DS5.7

Ⅴ. 결 론

IT 거버넌스의 프레임워크로서 정보보호를 위한 폭넓은 범위의 플랫폼이 될 수 있는 COBIT 4.1의 정보보호 요소(세부 통제 목적)와, 정보보호를 위한 상세한 최선의 실무(best practice)를 담고 있는 ISO/IEC 27002의 정보보호 요소(통제 항목) 사이의 매핑을 [표 1]에 나타내었다. 이와 같은 매핑은 두 정보보호 요소 간의 통합을 위한 선행 연구가 될 수 있다. 또한 이러한 "높은 수준"의 프레임워크와 "낮은 수준"의 방법론의 통합은 향후 기업 정보보호 거버넌스 연구에 도움이 될 것으로 판단된다.

앞으로의 연구 과제는 2012년에 새로 나온 COBIT 5의 정보보호 요소(프로세스)와 ISO/IEC 27002:2005의 정보보호 요소(통제 항목) 또는 COBIT 5와 2013년 7월 현재 FDIS (Final Draft) 단계에 있는 ISO/IEC 27001:2013[12]의 정보보호 요소(요구사항) 사이의 매핑과 그에 따른 정보보호 요소의 통합이 될 것으로 본다.

참고문헌

[1] Date Breach QuickView: An Executive's Guide to Data Breach Trends in 2012, Risk Based Security, Inc., February 2013.

[2] H. Susanto, M. N. Almunawar and Y. C. Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five", *International Journal of Electrical & Computer Sciences*, 11(5), pp. 23-29, October 2011.

[3] 조희준, *IT 거버넌스 프레임워크 코빗 - COBIT 4.1을 중심으로*, 인포더북스, 2010.

[4] R. Sheikhpour and N. Modiri, "An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls", *International Journal of Security and Its Applications*, 6(2), pp. 13-28, April 2012.

[5] T. Mataracioglu and S. Ozkan, "Governing Information Security in Conjuction with COBIT and ISO 27001", *Computing Research Repository*, 2011, http://arxiv.org/abs/1108.2150

[6] *COBIT 4.1*, IT Governance Institute, 2007, www.isaca.org

[7] *ISO/IEC 27002:2005 Information Technology - Security Techniques - Code of practice for information security management,* ISO/IEC, Switzerland, 2005.

[8] *ISO/IEC 27001:2005 Information Technology - Security Techniques - Information security management systems - Requirements,* ISO/IEC, Switzerland, 2005.

[9] *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit*, IT Governance Institute, 2008.

[10] *COBIT® 5 for Information Security*, ISACA, 2012.

[11] B. von Solms, "Information Security governance: COBIT or ISO 17799 or both?", *Computers & Security*, 24(2), pp. 99-104, March 2005.

[12] *ISO/IEC FDIS 27001 Information technology - Security techniques - Information security management systems - Requirements*, ISO/IEC, 2013, http://www.iso.org/

〈著者紹介〉

김 정 현 (Kim, Jeong Hyun)
ISACA 한국협회 보안부문 이사
현재 : (주)씨에이에스
<관심분야> COBIT, Val IT, IT 거버넌스, 정보보호