기업의 내부 인력 보안을 위한 IT 외주 용역 특성 분석

김지연*, 김형종**

요약

최근 많은 기업들이 경영 관리를 위한 정보시스템을 구축하면서 이를 운영 및 관리하는 IT 외주 용역이 증가하고 있다. 정보시스템은 기업의 자원 통합 뿐 아니라 경영 프로세스 관리도 지원하기 때문에 IT 외주 용역 수행원은 기업의 중요한 정보를 쉽게 획득할 수 있다. 실제로 최근 기업의 정보 유출 사고에서 IT 외주 용역에 의한 사고가 많은 비중을 차지하고 있으며, 따라서 IT 외주 용역에 의한 정보 유출 사고를 방지하기 위한 기업 내의 정보보호 대책 수립이 요구된다. 그러나 현재 국내외 정보보호관리체계 (Information Security Management System, ISMS) 표준에서도 IT 외주 용역에 대한 분류 체계가 제시되어 있지 않기 때문에 기업에서 참고할 수 있는 보안 가이드가 부족한 실정이다. 따라서 본 논문에서는 기업의 망 분리 현황, IT 자원 유형, 용역 수행원의 물리적 위치 및 접근 권한 등 기업의 정보시스템 구조를 고려하여 IT 외주 용역 유형을 분류하고, 각 유형의 특성을 제시하고자 한다.

Analysis of Characteristics of IT Outsourcing for Insider Security of Enterprise

Ji-Yeon Kim*, Hyung-Jong Kim*

ABSTRACT

As many enterprises implement an information system to manage their business, IT outsourcing that operates and manages the system is increasing. Information systems can integrate all business resources and manage business processes, which enables the outsourced employees to obtain critical information about enterprise business. Actually, a large portion of security incidents regarding information leakage of enterprises are being caused by IT outsourcing. However, there is a lack of guidelines that can be used to establish security measures for the outsourcing, because domestic and foreign information security management systems (ISMS) do not specify various types of IT outsourcing even though they provide security requirements for organizations. In this paper, we classify various types of IT outsourcing and define their characteristics considering information system's architecture, such as the status of network isolation, IT resource type, employees' location and their access authorization.

Key Words : IT outsourcing, Enterprise Security, Information security management system (ISMS), Information leakage, Network isolation

* 서울여자대학교 정보보호학과(✉hkim@swu.ac.kr)
· 제1저자(First Author) : 김지연 · 교신저자(Correspondent Author) : 김형종
· 접수일(2012년 1월 18일), 수정일(1차 : 2012년 2월 15일), 게재확정일(2012년 2월 17일)

Ⅰ. 서 론

기업의 정보시스템은 기업의 경영 혁신 수단으로서 모든 경영 자원을 통합하고, 전사적으로 관리할 수 있는 환경을 제공한다. 기업은 정보시스템을 구축함으로써 생산성 증대를 통해 기업의 경쟁력을 강화할 수 있지만, 정보시스템에 대한 보안 공격 발생 시, 기업 업무에 장애가 발생하거나 중요한 기업 및 고객 정보가 유출되는 피해가 발생할 수 있다. 실제로 기업의 정보화가 진행되면서 기업의 정보 유출 피해가 증가하고 있으며, 피해 유형으로는 외부 공격자에 의한 피해보다 내부 공격자에 의한 피해 사례가 더 많이 보고되고 있다 [1]. 특히, 내부 공격자에는 기업에서 고용한 협력 업체도 포함되는데 최근에는 기업의 IT 외주 용역에 의한 정보 유출 피해 사례가 많이 보고되고 있다. 2010년 9월에는 기업의 서버 유지보수 업체 직원이 서버에 해킹 프로그램을 설치하여 개인정보를 유포하였고, 2011년 9월에는 기업의 노후된 문서를 전산화하는 용역 업체 직원이 스캔된 내부 파일을 저장한 외장하드를 분실하는 사고가 발생하였다. 이 외에도 다양한 유형의 IT 외주 용역 업체에 의해 기업의 전산망이 마비되거나 기업의 정보가 유출되는 등의 사고가 발생하였지만, 기업에서 이와 같은 사고를 방지하기 위하여 참고할 수 있는 보안 가이드가 부족하다. 예를 들어, 현재 기업에서 기업의 정보보호 대책 수립을 위해 활용할 수 있는 대표적인 보안 가이드는 정보보호관리체계 (Information Security Management System, ISMS) 이다. ISMS는 조직의 정보자산을 보호하기 위하여 기술적, 물리적 보호조치를 포함하여 정보보호 대책을 수립하고, 이를 문서화하여 관리 운영할 수 있는 종합적인 관리체계로서 국내외에서는 이를 기업에서 반영 수 있도록 인증제도를 시행하고 있다 [2][3]. 그러나 국외 ISMS 인증 제도인 ISO/IEC 27001에는 외주 용역에 대한 통제사항이 명시되어 있지 않고, 국내 한국인터넷진흥원에서 시행하는 ISMS 인증 제도에는 이에 대한 항목이 추가되었지만 구체적인 용역 유형에 대한 정의 및 구현방안은 제시되어 있지 않다. 따라서 ISMS 역시 IT 외주 용역을 위한 정보보호 대책 수립에 활용하기에는 한계가 있다.

본 논문에서는 기업에서 IT 외주 용역에 대한 보안 관리 체계를 마련할 수 있도록 기업의 정보시스템 구조를 고려하여 IT 외주 용역의 유형을 정의하고, 각 유형별 특성을 제시하고자 한다. 특히, 기업에서 내부 정보보호를 위해 도입할 수 있는 망 분리 기술을 고려하여 IT 외주 용역이 접근할 수 있는 망 유형을 업무망 및 인터넷망으로 구분하고, 접근하는 자원의 종류 및 권한, 접근 경로에 따라 용역 유형을 정의한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로서 현재 시행되고 있는 국내외 ISMS 인증제도를 살펴보고, 망 분리 기술을 설명한다. 3장에서는 본 논문에서 제시하는 IT 외주 용역의 유형을 정의하고, 4장에서 유형별 특성을 제시한다. 또한, 5장에서는 제시된 유형에 대한 비교연구를 수행하고, 6장에서 결론 및 향후 연구를 제시한다.

Ⅱ. 관련연구

2.1 국내외 ISMS 인증제도

ISMS 국제 표준인 ISO/IEC 27001은 영국 표준 기구(British Standard)의 BS 7799에서 발전된 것으로서 BS 7799 Part 1 및 Part 2는 각각 ISMS 관리 지침 및 요구사항을 명시하였다. 이후, Part 1은 2000년 ISO/IEC 17799로 발표되었다가 2007년 ISO/IEC 27002로 변경되고, Part 2는 2005년 ISO/IEC 27001로 발표되었다 [4]. ISO/IEC 27001은 조직의 ISMS 수립, 구현, 운영, 관찰, 검토, 유지 및 개선을 위한 요구사항을 총 11개의 통제 영역, 38개 통제 항목, 113개의 세부 통제 항목으로 구성하여 명시하고 있다 [5][6]. 국내에서는 2002년 한국인터넷진흥원에 의해 ISMS 인증제도가 시행되었

고, 이는 ISO/IEC 27001의 11개 통제 영역에 외부자 보안, 정보보호 교육 및 훈련, 암호통제, 전자거래 보안 분야가 추가된 15개 통제 분야 및 120의 통제 항목으로 구성된다 [6][7]. 이 중, 본 논문에서 다루는 외주 용역 보안과 관련된 '외부자 보안' 통제 분야는 외부 위탁 계약 시 보안 요구사항, 제 3자와의 계약 시 보안 요구사항, 외부 위탁 보안 관리, 제 3자 보안 관리 항목으로 구성된다 [8]. 그러나 각 요구사항이 추상적으로 설명되어 있는 수준이고, 통제 대상에 속하는 '외부 위탁, 제 3자'에 대한 정의나 보호 대상에 해당 되는 '자산'에 대한 구분이 명확하게 제시되어 있지 않은 상황이다.

2.2 망 분리 기술

망 분리 기술은 조직의 정보 자산을 외부의 공격으로부터 보호하기 위하여 조직의 정보시스템이 구축된 주요 업무망과 인터넷망을 분리시키는 기술로서 주로 공공기관 및 금융기관과 같이 중요 정보를 취급하는 조직을 중심으로 도입되고 있다. 국내 공공기관은 2007년부터 국가 정보통신 서비스의 보안성 확보를 위하여 국가기관 트래픽과 민간 트래픽을 분리하기 위한 망 분리 사업을 중앙행정기관 및 지방자치단체에 대해 진행하고 있으며, 망 분리 유형은 물리적 망 분리 기술을 채택하고 있다 [9].

물리적 망분리 기술은 업무망과 인터넷망의 물리적 연결을 차단함으로써 보안성을 높일 수 있지만, 모든 직원이 두 대의 컴퓨터를 놓고 사용해야하는 불편함과 구축비용이 비싸다는 단점이 존재한다. 논리적 망 분리 기술은 가상화 기술을 이용하여 구현되기 때문에 물리적 망 분리 기술보다 비용 측면에서는 경쟁력이 있지만, 보안성이 상대적으로 떨어진다. 따라서 최근에는 논리적 망 분리 기술의 보안성을 향상시키기 위하여 암호화 및 네트워크 접근 통제와 같은 보안 기술이 적용된 망 분리 솔루션이 등장하고 있다.

III. IT 외주용역 유형 정의

본 논문에서는 IT 외주 용역의 유형을 용역 업무를 수행하기 위하여 접근하는 망의 유형에 따라 분류하고, 각 유형마다 용역 수행원이 접근할 수 있는 IT 자원 유형 및 접근 경로, 용역 수행원의 물리적 위치를 고려하여 세부 유형을 정의한다.

기업 내에는 크게 내부망 2개, 외부망 1개가 구축될 수 있다. 내부망은 기업의 업무 처리를 위해 별도로 사내에 구축한 망으로서 기업 내부 데이터 및 업무지원 시스템에 접근하기 위한 업무망과 IT 외주 용역을 위해 구축된 IT 외주 용역 자체망이 포함된다. 외부망은 외부 인터넷 사업자가 구축한 망을 사용하는 형태로서 내부망과는 물리적 또는 논리적인 방법으로 분리하여 망을 구축할 수 있다. 따라서 본 논문에서는 IT 외주 용역 업체가 기업 내 세 개의 망 중, 어떤 유형의 망에 접속 하는지를 기준으로 하여 각각 유형 1, 2, 3을 분류하였고, 이는 곧 접근하는 IT 자원 유형 및 접근 경로의 특성과도 연결되기 때문에 유형별로 (표 1)과 같이 정의를 내릴 수 있다. 또한, 각 유형은 IT 외주 용역 수행원의 업무 수행 위치에 따라 상주 및 비상주 용역으로 구분되지만, 모든 IT 외주 용역 유형은 접근 망의 유형 및 용역 수행원의 상주 여부와 관계없이 기업 내부에 어떠한 형태로든 사람 혹은 IT 장치의 유입을 가져오게 되기 때문에 기업 담당자들은 이에 대한 대응책을 마련해야 하는 공통적 특성을 갖게 된다.

표 1. IT 외주 용역 유형 정의
Table 1. Definition of types of IT outsourcing

유형	IT 외부 용역 특성
1	IT 자원에 온라인 접근이 이루어지는 외주 용역
2	IT 자원에 오프라인으로 접근하고, 용역 업무를 위한 독립적인 네트워크를 기업 내에 구축하여 운영하는 외주용역
3	IT 자원에 오프라인으로 접근하고, 인터넷망을 이용한 면담 및 상담을 수행하는 용역

Ⅳ. IT 외주 용역 유형 특성 분석

IT 외주 용역이 접근할 수 있는 기업의 IT 자원 유형은 기업 내부 데이터에 대한 접근인지 IT 시스템에 대한 접근인지에 대한 구분이며, 접근 유형은 온라인을 통한 접근인지 또는 오프라인을 통한 접근인지를 구분한다. 4장에서는 이와 같은 세부 기준에 따라 유형별 세부 특성을 정의한다.

4.1 유형 1

유형 1은 기업 업무망 내의 중요 데이터를 포함한 업무 지원 시스템에 온라인상으로 접근하는 IT 외주 용역 형태로서, 기업 소유의 PC와 같은 IT 시스템을 통한 업무망 접근이 가능하다. 단, (그림 1)과 같이 IT 외주 용역 수행원의 물리적 위치에 따라 업무망에 접근하는 경로가 달라지게 된다. 본 논문에서는 용역 수행원의 물리적 위치를 상주 여부로 구분하여 각각 A, B로 표기하여 세부 유형을 정의하였다.

"1-A"는 유형 1 외주 용역 수행원이 기업 내에 상주하는 유형으로서 용역 수행원이 기업 내 IT 시스템을 사용하여 업무망에 접속할 수 있고, "1-B"는 유형 1 외주 용역 수행원이 기업 내에 비상주하는 유형으로서 외주 용역 업체 소유의 IT 시스템에서 원격 접속을 통해 기업 내의 IT 시스템에 접속하고, 접속한 IT 시스템을 통해 업무망에 접속하게 된다. 따라서 "1-A"는 기업 업무망 IT 자원에 온라인으로 접근할 수 있는 '온라인 업무망 접근 권한'을 사전에 부여받아야 하고, "1-B"는 '온라인 업무망 접근 권한'과 더불어 내부 IT 시스템에 원격으로 접속할 수 있는 '원격 접속 권한'을 추가로 부여받아야 한다.

4.2 유형 2

유형 2는 IT 외주 용역 업체가 자체 업무망을 기업 내에 직접 구축하거나 기업에 요청하여 구축 받는 유형이다. 단, IT 용역 자체망은 기업의 업무망과는 분리되어 있기 때문에 온라인상으로 내부 중요 데이터에 접근하거나 시스템을 이용하는 것이 불가능하지만,

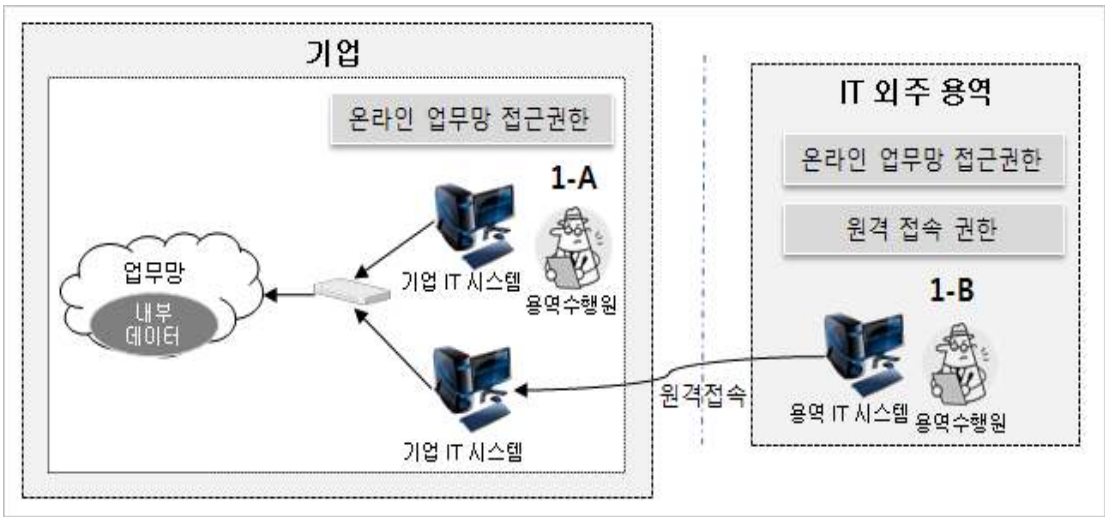

그림 1. IT 외주용역 유형 1 - 업무 유형 및 자원 접근 방안
Fig. 1 Type 1 of IT outsourcing - types of work and methods for accessing resources

용역 수행원들은 '오프라인 IT 시스템 접근권한' 및 '오프라인 업무망 접근권한'을 부여받을 수 있기 때문에 오프라인 상으로 기업의 IT 자원에 접근할 수 있게 된다. 또한, 용역 수행원의 물리적 위치 및 접근하는 IT 자원의 유형에 따라 세부 유형이 정의될 수 있다.

표 2. 유형 2 용역 수행원 세부 유형 정의
Table 2. Definition of types of employee of Type 2

접근 IT 자원 / 물리적 위치	IT시스템	내부 데이터
상주	2-A-가	2-A-나
비상주	2-B-가	2-B-나

상주 유형에 속하는 "2-A-가"는 용역 수행원이 기업 내 IT 시스템에 물리적 접근을 통해 유지 보수 및 장애 복구 업무를 수행하는 유형으로서 IT 시스템에 대한 접근 권한 외에 IT 시스템을 통해 업무망에 접속할 수 있는 '온라인 업무망 접속 권한'은 부여받지 못한다. "2-A-나"는 상주 용역 수행원이 기업 업무망 내의 중요 데이터에 오프라인으로 접근하는 유형으로서 기업 내에 자체망을 이용하는 업무 공간 내에서 오프라인으로 획득한 내부 데이터를 이용하여 용역 업무를 수행한다. 비상주 유형에 속하는 "2-B-가"는 용역 수행원이 기업의 IT 시스템을 자사의 공간으로 이동시켜 용역 업무를 수행하는 유형이다. 이 유형은 "2-A-가"와 같이 '오프라인 IT 시스템 접근권한'을 획득하였더라도 기업의 업무망에는 외부망을 통해 접속할 수 없기 때문에 '원격 접속 권한'을 가지지 않는 한, 업무망에 접근하는 것이 불가능하다. "2-B-나"는 비상주 용역 수행원이 IT 외주 용역 업체 내에서 '오프라인 업무망 접근권한'을 통해 획득한 기업의 중요 데이터를 활용하여 업무를 수행한다.

4.3 유형 3

유형 3은 유형 2와 같이 IT 외주 용역 업체가 기업 내의 IT 자원에 온라인상으로 접근할 수 있는 권한은 없지만, 기업 내에 IT 외주 용역 자체망을 구축할 수 없기 때문에 오직 인터넷 망을 활용하여 용역 업무를 수행하는 유형이다. 단, 용역 업무의 종류에 따라 기업의 내부 데이터에 대한 접근이 필요한 경우, '오프라인 업무망 접근권한'을 부여받아 접근할 수 있다.

표 3. 유형 3 용역 수행원 세부 유형 정의
Table 3. Definition of types of employee of Type 3

접근 IT 자원 / 물리적 위치	업무망 접근권한 획득	업무망 접근권한 미획득
상주	3-A-가	3-A-나
비상주	3-B-가	3-B-나

상주 유형에 속하는 "3-A-가" 및 "3-A-나"는 용역 수행원이 기업 내에 용역 소유의 IT 시스템을 반입하고 외부망을 이용하여 용역 업무를 수행하는 유형이다. 그러나 "3-A-가" 유형의 용역 수행원은 '오프라인 업무망 접근권한'을 부여받아 용역 업무에 필요한 기업 내부 자료를 획득할 수 있지만, "3-A-나" 유형은 업무망 접근 권한을 부여받지 못하기 때문에 IT 외주 용역 내에서 해결할 수 있는 범위의 용역 업무만 수행하게 된다. 비상주 유형에 속하는 "3-B-가" 및 "3-B-나"의 용역 수행원은 IT 외주 용역 업체 내에서 자체 시스템을 통해 용역 업무를 수행한다. 그러나 상주 유형과 마찬가지로 업무망 접근 권한을 획득할 수 있는 "3-B-가" 유형은 '오프라인 업무망 접근권한'을 통해 기업 내부 데이터를 획득할 수 있지만 "3-B-나" 유형은 IT 외주 용역 내에서 해결할 수 있는 범위의 용역 업무만을 수행해야 한다.

V. IT 외주 용역 유형 비교 분석

세 개의 유형 중, 업무망에 온라인으로 접근할 수 있는 권한을 갖는 유형 1이 기업의 IT 자원에 행사할 수

있는 영향력이 가장 크고, 유형 2와 유형 3은 권한 요청을 통해 업무망에 오프라인 상으로만 접근 가능하기 때문에 상대적으로 행사할 수 있는 영향력이 작다. 유형 1과 유형 2의 가장 큰 차이점은 유형 2가 접속할 수 있는 IT 외주 용역 망의 경우, 기업의 업무망과 분리되어 있기 때문에 기업 내부 데이터에 온라인으로 접근할 수 없다는 것이다. 유형 2와 유형 3의 경우는 두 유형 모두 IT 자원에 온라인상으로 접근할 수는 없지만, 유형 2의 경우 기업 내에 IT 외주 용역 자체망을 구축할 수 있기 때문에 더 많은 자사 기술을 반영하여 더 넓은 영역의 용역 업무를 수행할 수 있다. 따라서 인터넷 망을 통해서만 업무를 수행할 수 있는 유형 3의 경우가 기업의 IT 자산에 행사할 수 있는 영향력이 가장 작다고 할 수 있다.

Ⅵ. 결 론

본 논문은 기업의 정보시스템 구조를 고려하여 IT 외주 용역 유형을 분류하고, 각 유형별 특성을 정의하는 연구를 수행하였다. 본 논문에서는 IT 외주 용역이 접근할 수 있는 기업 내의 망을 업무망, IT 외주 용역망, 인터넷망으로 구분하고, 각각 IT 외주 용역 유형 1, 2, 3으로 정의하였다. 모든 유형들은 외주 용역이 접근할 수 있는 기업 내의 IT 자원의 종류 및 접근 경로, 용역 수행원의 물리적 위치에 따라 다시 세분화되며, 세부 유형별로 용역 수행원이 부여받을 수 있는 권한 및 수행할 수 있는 업무의 특성이 제시되었다.

세 개의 유형 중, 업무망 내의 모든 IT 자원에 접근할 수 있는 유형 1이 가장 높은 권한을 부여받게 되며, 업무망에 온라인으로 접근할 수는 없지만 기업 내에 자체망을 구축하여 운영할 수 있는 유형 2가 인터넷망을 사용해야 하는 유형 3 보다 좀 더 넓은 범위의 용역 업무를 수행하게 된다. 그러나 유형 2와 유형 3 모두 업무 수행을 위해 필요한 내부 데이터를 오프라인 접근 권한을 부여받아 획득할 수 있기 때문에 이를 관리하기 위한 물리적 보안 대책 및 권한 부여를 위한 관리적 보안 대책 또한 요구된다.

본 논문의 향후 연구로서는 제시한 IT 외주 용역 유형별로 요구되는 정보보호 기술 및 정책 고려사항을 제시할 예정이며, 이는 다양한 IT 외주 용역에 의해 발생할 수 있는 기업의 정보 유출 방지를 위하여 정보보호 대책을 수립하는 데에 활용될 수 있을 것이다.

참고문헌

[1] 지식경제부, 중소기업의 기술보호를 위한 세부 보안통제 실행 지침서, 2011.
[2] 법률지식정보시스템, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 2008.
[3] 한국정보보호진흥원, 정보보호관리체계 인증제도 소개, 2004.
[4] ISO, ISO and International Standards for Security, COPANT Seminar on Security Standards, 2006.
[5] ISO/IEC, ISO/IEC 27001: Information technology – Security techniques - Information security management systems – Requirements, 2005.
[6] 한국정보보호진흥원, 정보보호관리체계 개요, 2008.
[7] 장상수, 이호섭, “정보보호관리체계(ISMS) 인증심사 결함사항 분석에 관한 연구”, 정보보호학회논문지, 20권 1호 , pp. 31-38, 2010.
[8] 한국정보보호진흥원, 정보보호관리체계 통제사항 가이드, 2004.
[9] 행정안전부 홈페이지. 국가정보통신서비스 이용제도. http://www.mopas.go.kr.
[10] 한국정보보호진흥원, 정보보호 거버넌스 개념 도입을 위한 정보보호관리체계(ISMS) 발전 방안 연구, 2009.

감사의 글

이 논문은 2011학년도 서울여자대학교 교내학술특별연구비의 지원을 받았음.

저자소개

김지연(Ji-Yeon Kim)

2007년 서울여자대학교 정보보호공학과 공학사

2007~현재 서울여자대학교 컴퓨터학과 석박사통합과정

※ 관심분야 : 인터넷전화 보안, 클라우드 컴퓨팅 보안, 모델링 및 시뮬레이션

김형종(Hyung-Jong Kim)

1996년 성균관대학교 정보공학과 공학사
1998년 성균관대학교 정보공학과 공학석사
2001년 성균관대학교 전기전자 및 컴퓨터공학과 공학박사
2001년~2007년 한국정보보호진흥원 수석연구원
2004년~2006년 미국 카네기멜론대학 CyLab Visiting Scholar

2007~현재 서울여자대학교 정보보호학과 조교수

※ 관심분야 : 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론