# 분산서비스거부공격 대응 지표 모델 연구

정회원 박 춘 자*, 김 범 재**, 신 용 태***, 김 종 배****°

# A Model of DDoS Correspondence Criteria

Chun Ja Park*, Bum-Jae Kim**, Yong Tae Shin***, Jong bae Kim****° *Regular Members*

요 약

본 연구에서는 정보보호관리시스템이라는 큰 범주 내에서 DDoS대응시스템이라는 특정범주로 초점을 맞추어 이를 정량적으로 측정하여 관리할 수 있는 대응지표를 제안한다. DDoS 대응지표를 개발하기 위해 정보보호관리체계의 측정분야 표준인 ISO27004의 측정지표 중에서 DDoS 대응전략을 연관시켜 설문조사를 통해 SMART기법을 사용, 분석하여 7개의 기준지표를 도출하였다. 이 기준지표를 토대로 KISA의 국가정보보호평가지수모델 및 행정안전부의 개인정보보호수준진단지표 등의 기존연구를 참조하여 측정항목 28개를 식별한 후 이를 다시 한 번 정보보호전문가를 대상으로 설문조사를 하여 요인 분석(Factor Analysis)을 통해 11개 콤포넌트 중 유의한 7개 그룹을 식별하고, 이 7개 그룹의 신뢰도를 Cronbach's Alpha로 검증하여 6개 그룹을 도출하여 이를 DDoS 세부지표로 삼았다. 그리고 마지막으로 도출된 세부지표의 측정항목(메트릭)에 대해 Kitchenham의 접근법에 따라 이론적인 분석을 통한 검증을 실행하였다.

**Key Words** : DDoS, Correspondence Criteria, Information Security Management System, Indicator

ABSTRACT

This paper focused on the specific category called a DDoS correspondence system among a big category called an information security management system, and suggested the correspondence criteria of DDoS in order to measure this quantitatively and be able to manage this. First, the DDoS properties and correspondence strategy were associated among measurement indicators of ISO27004, which is a standard of the measurement field of the information security management system, and then 7 standard indicators were deduced through a questionnaire survey by using and analyzing the SMART technique. The 28 measurement items were differentiated by referring the existing researches such as the national information security assessment index model of KISA and the personal information protection level diagnose indicators of the Ministry of Public Administration and Security, etc. Based on these standard indicators, the 7 significant groups among 11 components were differentiated through Factor Analysis by performing a questionnaire survey targeting information security experts once more, and 6 groups were deduced by verifying the reliability of these seven groups with Cronbach's Alpha, so these were set as detailed indicators of DDoS. And lastly, the verification through theoretical analysis was carried out about measurement items(metric) of deduced detailed indicators according to an approach method of Kitchenham.

※ 본 연구는 숭실대학교 교내연구비 지원으로 수행되었습니다.
* 숭실대학교(woorim9454@hanmail.net), ** (주)엘엔케이시스(bjkim111@naver.com),
*** 숭실대학교(shin@ssu.ac.kr), **** (사)한국해킹보안협회(kjb123@empas.com) (°:교신저자)
논문번호 : 10034-0724, 접수일자 : 2010년 7월 24일

## Ⅰ. 서 론

최근 들어 DoS(Denial of Service, 서비스 거부) 공격이나 DDoS(Distributed Denial of Service, 분산서비스 거부)공격이 날로 증가하고 있다. 지난 2009년 7월 7일 한국과 미국의 정부기관, 금융기관, 인터넷서비스 업체 등 약 46개 사이트를 대상으로 이뤄진 분산서비스거부 공격은 한동안 우리 기억 속에 잊힌 인터넷 보안의 중요성을 다시 일깨워주는 계기가 된 큰 사건이라고 할 수 있다. 더욱 심각한 것은 이러한 DDoS 공격의 기법이 갈수록 진화하고 고도화되고 있다는 점이다 [1].

정부와 기업들은 이 피해를 계기로 다시 한 번 보안 인프라 확충의 필요성을 느꼈으며 양적인 발전보다는 질적인 발전을 위해 정부 차원의 관련 정책 수정 및 마련, IT 서비스 업체에 대한 지원 등으로 보안 인프라 후진국이라는 불명예를 씻어내기 위해 다각적인 노력을 기울이고 있다. 7.7대란이후 정부는 예산을 대폭 증액하여 "해킹 바이러스대응 고도화"라는 큰 주제 하에 범정부 DDoS 대응체계 구축사업을 각 부처별로 발주하여 추진하고 있으며, 정보보호업무에 장비와 소프트웨어 도입 등의 노력을 기하고 있다. 또한, ISP(Internet Service Provider) 등 민간 기업들도 한국인터넷진흥원(KISA)의 지휘하에 대응체계를 점검하고 장비 및 솔루션, 인력 등을 보강하며 이전에 비해 많은 노력을 기울이는 것은 주지의 사실이다.

그러나 아직까지도 정보보호시스템은 사회적 사건의 발생이나, 해당 조직에 대한 직접적인 피해의 사례가 발생하였을 때에만 단기적으로 이슈가 될 뿐, 이를 위한 지속적인 투자에는 여전히 소극적이라는 것이 일반적인 인식이다. 이는 정보보호 시스템의 특성상 사건이 발생하기 전에는 그 효과를 인식하기 어렵고, 사건이 발생한 경우에는 침해 또는 방어라는 결과에 대한 이분법적인 방식의 성패 판단만 있을 뿐, 이것의 효과와 효율에 대한 상세하고 객관적인 측정의 기준이 없기 때문이다.

비록 최근에는 정보보호관리체계에 대한 평가나 인증 작업이 진행 중이나, 이는 정보보호관리시스템에 대한 일반적인 지침이나 기준만을 제시하고 있어, 이를 통해 정부기관이나 기업의 DDoS 대응 체계가 어느 정도의 수준으로 구축되어 관리되어지는지, 또 대응 체계의 구축이 침해 대응에 얼마나 효과적인지 그 성과를 정량적으로 측정할 수 있는 지표로 활용하기는 어려운 실정이다.

그러므로 본 연구에서는 객관적인 측정이 가능한 DDoS 대응지표를 수립하고 이를 측정, 관리할 수 있는 메트릭을 제안한다.

## Ⅱ. 관련 연구

정보보호 평가 측면에서 기존 연구의 내용들은 크게 두 가지 접근방법에 의해 구분된다. 첫 번째는 TCSEC(Trusted Computer System Evaluation Criteria), ITSEC(Information Technology Security Criteria) 등과 같이 제품이나 시스템의 보안 기능과 성능 측면을 중심으로 하는 평가 체계이다. 이러한 기존의 평가기준이 주로 제품별 평가기준을 사용함으로 인하여 민간분야에서 요구하는 다양한 제품을 평가할 수 없어 융통성 면에서 제약을 받고 있다 [2]. 두 번째는 ISO 27001[3], ISO 27002[4]와 같이 관리적 측면을 중심으로 한 평가 체계이다. 특히, ISO 27001과 27002는 BS7799를 근간으로 하고 있으며 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용되도록 개발되었으며, 조직의 보안 표준의 기반이 되도록 고안되었다. 따라서 ISO 27001, ISO27002 표준은 지침과 권고안의 성격을 갖으며, 관리적 측면을 중심으로 한 평가 체계여서, 정보보호관리를 위한 지침으로는 적합할 수 있지만 그 자체로서는 평가대상 조직의 정보보호관리체계 개선이나 향상이 쉽지 않다는 문제가 있다 [5].

한편, 현재 정보보호관리 국제 표준인 ISO/IEC 18028 (Information technology-Security techniques-IT network security) [6]-[9] 에서는 정보보호관리 프로세스를 중심으로 14개의 절차를 제시하고 있다 [10]. 정보보호관리를 위해서는 조직의 정보보호 관리체계의 구축과 더불어, 현재 작동중인 정보보호관리체계에 대한 정확하고 지속적인 측정 및 평가 작업이 필요하다. 이러한 측정과 평가 작업을 통해서 조직은 현재 자신의 정보보호관리체계 수준과 필요한 요구사항들을 파악할 수 있고, 이를 바탕으로 조직의 정보보호관리체계에 대한 지속적인 개선이 가능하다.

또한 중요한 정보자산을 보호하기 위한 정보보호 관리체계방법론으로 현재 ISO 27001[3]이 국제표준으로 제정되어 가장 널리 사용 되고 있다. 이와 유사한 개념으로는 SP800-53[11],[12], COBIT4.x[13]등 국가와 조직별로 다양한 모델이 응용되어 사용되고 있다.

이상에서 살펴본 기존의 표준 및 모델들은 일반적이며 범용적인 특성을 가지고 있어, 표준을 적용하기 위한 구체적인 방법론과 분석방법을 제공하고 있지는 않다.

## Ⅲ. DDoS 대응지표

본 장에서는 DDoS 대응지표를 도출하는 과정과 도출된 대응지표를 측정하기 위한 메트릭을 제안한다.

### 3.1 DDoS 대응 지표 도출 과정

지표는 정보보호관리체계 측정 연구인 ISO 27004를 기반으로 DDoS 대응 전략과의 연관성을 맵핑한다. 대응전략은 현재 언급하고 있는 DDoS 대응 전략을 기반으로 DDoS 대응체계 구축, 기반시설 확충, 지속적인 진화, 개인의 보안의식 고취의 4가지를 도출한다. 맵핑은 SMART 분석 [14]을 통해 DDoS 대응 전략과 연관이 있다고 판단되는 7개의 지표를 기준지표로 도출한다. 도출된 기준지표를 측정하기 위한 측정항목(평가항목)들은 KISA의 국가정보보호수준 평가지수 모델, 행정안전부의 개인정보보호수준 진단지표, ISO 27004를 기반으로 기준지표를 측정하기 위해 필요하다고 판단되는 측정항목을 식별한다. 그림 1은 기준지표와 측정항목의 도출 과정을 보여준다.

식별된 28개의 측정항목에 대해 요인 분석 [15]을 실시하여 결과를 분석하여 6개의 세부 지표를 도출하며, 도출된 세부 지표는 DDoS의 특징을 반영하여 네이밍한다. 또한 6개의 세부 지표를 측정하기 위한 측정항목을 정량적인 측정이 가능하도록 메트릭을 제안한다. 그림 2는 기준지표와 연관되어 있다

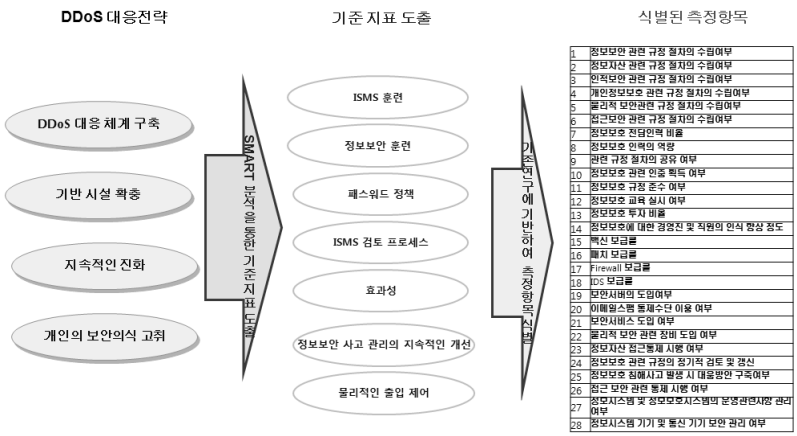


그림 1. 기준지표 및 측정항목 도출 과정

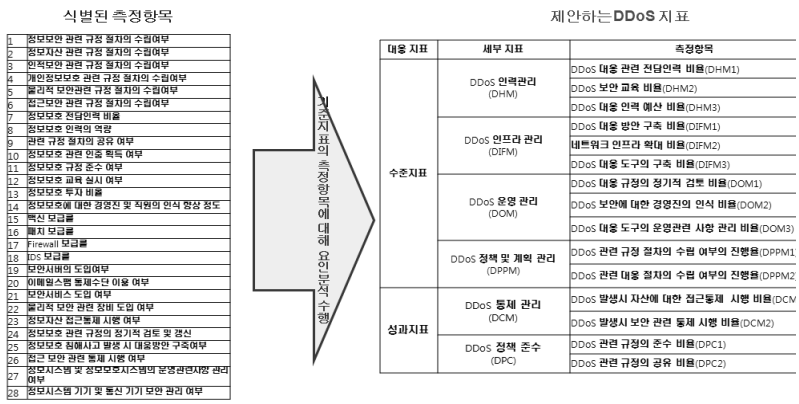


그림 2. 요인 분석 결과에 기반한 DDoS 지표 도출

고 판단되어 식별된 측정항목에 대한 요인분석 결과를 기반으로 DDoS 지표를 도출하는 과정이다.

제안하는 DDoS 지표에서 수준비표와 성과지표에 대한 분류 기준은 현재 조직의 대응 상황을 파악할 수 있는지와 문제 발생 이후의 처리 결과에 영향을 미치는지에 따라 분류한다. 제안한 세부지표는 요인분석의 결과 그룹핑되는 7개의 그룹에 대한 신뢰도를 검증하기 위해 Cronbach's alpha [16]를 적용하여 Alpha > 0.500, 90% 신뢰수준의 그룹인 6개를 식별하여 DDoS 세부지표로 도출하였다. DDoS 세부지표와 측정항목은 DDoS의 특징을 반영하여 일반적인 정보보호시스템이 아닌 DDoS만을 위한 세부지표와 측정항목으로 용도에 적합하게 변경하였다.

### 3.2 대응지표에 대한 측정 메트릭

표 1은 세부지표에 대한 측정항목에 대해 계산하기 위해 사용되는 측정데이터의 값을 정의한 것이다. 각각의 측정항목의 계산은 분자/분모의 형태를 가지며 계산 결과는 비율로써 표현된다.

식별한 세부지표는 수준지표와 성과지표로 분류되며, 세부지표를 표현하기 위해 본 연구에서 다음과 같은 템플릿으로 제안한다.

각각의 세부지표에 대한 정의는 다음과 같다.

- DDoS 인력 관리(DHM) : DDoS 인력에 대한 관리가 잘 되고 있는지를 확인한다. 이를 위해 전담인력의 비율, 전담 교육의 실시, 대응 예산에 대해 확인한다.
- DDoS 인프라 관리(DIFM) : DDoS 공격을 대응하기 위한 인프라 관리가 잘되고 있는지를 확인한다. 이를 위해 대응 방안 구축 비율, 네트워크 인프라 구조, 대응 도구 구축 등에 대해 확인한다.
- DDoS 운영 관리(DOM) : DDoS 공격에 대한 규정이 잘 되어있는지, 경영진의 DDoS 보안 인식이 높은지, DDoS 대응 도구의 운영 관리 사항들이 잘 관리되는지를 확인하여 DDoS 대응 운영에 대한 관리가 잘 되고 있는지를 확인한다.
- DDoS 정책 및 계획 관리(DPPM) : DDoS 관련 절차나 대응 절차가 잘 관리되고 있는지에 대해 확인한다.

표 2. DDoS 인력 관리(DHM)

| 필드 | 설명 |
|---|---|
| 식별자 | DDoS 인력 관리(DHM) |
| 목적 | DDoS에 대응하기 위한 전담 인력의 관리가 잘 되고 있는지에 대해 판단하기 위함 |
| 측정항목 | DDoS 대응 관련 전담인력 비율(DHM1),<br>DDoS 보안 교육 비율(DHM2,<br>DDoS 대응 인력 예산 비율(DHM3) |
| 유형 | 적용 여부를 판단 |
| 공식 | DHM = (DHM1 + DHM2 + DHM3)/3 |
| 목표 | 지표에 대한 결과 값이 높을수록 DDoS에 관련된 인력의 관리가 잘 되고 있다고 판단한다. |
| 구현 내용 | 객관적인 수치로써 결과 값이 계산됨 |
| 빈도 | 분기별로 인력에 대한 정보를 수집해야 함 |
| 책임부서 | 보안 책임자 및 관리자, 예산 담당자 |
| 자료 소스 | 보안 관련 조직도, 교육 일지, 인력관리에 따른 보안 예산서를 가지고 판단 |
| 보고 포맷 | 바 그래프로 표현하며, 이를 통해 지속적인 개선 여부도 체크할 수 있음 |

표 1. 측정을 위한 데이터 정의

| 대응 지표 | 세부 지표 | 측정항목 | 측정데이터(Numerator) | 측정데이터(Denominator) |
|---|---|---|---|---|
| 수준지표 | DDoS 인력관리 (DHM) | DDoS 대응 관련 전담인력 비율(DHM1) | DDoS 대응 전담 인력 수 | 전체 보안 전담 인력수 |
| | | DDoS 보안 교육 비율(DHM2) | DDoS 보안 교육 일수 | 전체 보안 교육 일수 |
| | | DDoS 대응 인력 예산 비율(DHM3) | DDoS 대응 인력 예산 | 전체 보안 전담 인력 예산 |
| | DDoS 인프라 관리 (DIFM) | DDoS 대응 방안 구축 비율(DIFM1) | 현재 구축된 DDoS 대응 방안 수 | 전체 DDoS 대응 방안 수 |
| | | 네트워크 인프라 확대 비율(DIFM2) | DDoS 대응을 위해 증가된 네트워크 인프라량 | 네트워크 인프라 증가량 |
| | | DDoS 대응 도구의 구축 비율(DIFM3) | 현재 구축된 DDoS 대응 도구 구축 수 | DDoS 대응 도구 계획 수 |
| | DDoS 운영 관리 (DOM) | DDoS 대응 규정의 정기적 검토 비율(DOM1) | 검토된 DDoS 대응 규정의 수 | DDoS 대응 규정의 수 |
| | | DDoS 보안에 대한 경영진의 인식 비율(DOM2) | DDoS 보안에 대한 경영진의 중요도 | 보안에 대한 경영진의 중요도 |
| | | DDoS 대응 도구의 운영관련 사항 관리 비율(DOM3) | DDoS 운영관련 사항 중 관리되고 있는 수 | DDoS 운영관련 사항 수 |
| | DDoS 정책 및 계획 관리 (DPPM) | DDoS 관련 규정 절차의 수립 여부의 진행율(DPPM1) | 구현된 DDoS 관련 규정 절차의 수 | 전체 DDoS 관련 규정 절차의 수 |
| | | DDoS 관련 대응 절차의 수립 여부의 진행율(DPPM2) | 구현된 DDoS 관련 대응 절차의 수 | 전체 DDoS 관련 대응 절차의 수 |
| 성과지표 | DDoS 통제 관리 (DCM) | DDoS 발생시 자산에 대한 접근통제 시행 비율(DCM1) | 자산에 대해 실행된 접근 통제 항목의 수 | 자산에 대해 계획된 접근 통제 항목의 수 |
| | | DDoS 발생시 보안 관련 통제 시행 비율(DCM2) | 실행된 보안 통제 항목의 수 | 계획된 보안 관련 통제 항목의 수 |
| | DDoS 정책 준수 (DPC) | DDoS 관련 규정의 준수 비율(DPC1) | 발생시 준수된 관련 규정의 수 | DDoS 관련 규정의 항목의 수 |
| | | DDoS 관련 규정의 공유 비율(DPC2) | 발생시 공유된 관련 규정의 수 | DDoS 관련 규정의 항목의 수 |

표 3. DDoS 인프라 관리(DIFM)

| 필드 | 설명 |
|---|---|
| 식별자 | DDoS 인프라 관리(DIFM) |
| 목적 | DDoS에 대응하기 위한 인프라 관리가 잘 되고 있는지에 대해 판단하기 위함 |
| 측정항목 | DDoS 대응 방안 구축 비율(DIFM1),<br>네트워크 인프라 확대 비율(DIFM2),<br>DDoS 대응 도구의 구축 비율(DIFM3) |
| 유형 | 대응 방안과 대응 도구 및 네트워크 대역폭 확대의 구현 여부를 판단 |
| 공식 | DIFM = (DIFM1 + DIFM2 + DIFM3)/3 |
| 목표 | 지표에 대한 결과값이 높을수록 DDoS 대응을 위한 인프라 관리가 잘 되어있다고 판단한다. |
| 구현 내용 | 대응 방안과 대응 도구에 대한 명확한 정의가 기반이 되어야 한다. |
| 빈도 | 분기별로 인프라 관리에 대한 정보가 수집되어야 함 |
| 책임부서 | 보안 책임자 및 관리자 |
| 자료 소스 | DDoS 대응 체계서와 대응 방안 구축 계획서의 존재 유무와 존재 유무와 진행 사항으로 판단 |
| 보고 포맷 | 바 그래프로 표현하며, 이를 통해 지속적인 개선 여부도 체크할 수 있음 |

표 4. DDoS 운영 관리(DOM)

| 필드 | 내용 |
|---|---|
| 식별자 | DDoS 운영 관리(DOM) |
| 목적 | DDoS 대응하기 위한 운영관리가 잘 되고 있는지에 대해 판단하기 위함 |
| 측정항목 | DDoS 대응 규정의 정기적 검토 비율(DOM1),<br>DDoS 보안에 대한 경영진의 인식 비율(DOM2),<br>DDoS 대응 도구의 운영관련 사항 관리 비율(DOM3) |
| 유형 | 대응 규정과 도구 운영에 필요한 사항들이 관리를 위해 명시화 되었는지를 판단 |
| 공식 | DOM = (DOM1 + DOM2 + DOM3)/3 |
| 목표 | 지표에 대한 결과 값이 높을수록 DDoS 대응을 위한 운영관리가 잘 되어있다고 판단한다. |
| 구현 내용 | 대응 규정의 수립 여부와 도구 운영에 필요한 관리 사항 관리되고 있는지의 수립 여부를 판단함 |
| 빈도 | 분기별로 규정 및 관리 사항에 대해 판단해야 함 |
| 책임부서 | 보안 책임자 및 관리자 |
| 자료 소스 | DDoS 대응 규정서와 대응 도구 운영 계획서의 존재유무와 진행 사항으로 판단 |
| 보고 포맷 | 바 그래프로 표현하며, 이를 통해 지속적인 개선 여부도 체크할 수 있음 |

표 5. DDoS 정책 및 계획 관리(DPPM)

| 필드 | 내용 |
|---|---|
| 식별자 | DDoS 정책 및 계획 관리(DPPM) |
| 목적 | DDoS에 대응하기 위한 정책과 계획이 사전에 수립되어 있는 정도를 판단하기 위함 |
| 측정항목 | DDoS 관련 규정 절차의 수립 여부의 진행율(DPPM1),<br>DDoS 관련 대응 절차의 수립 여부의 진행율(DPPM2) |
| 유형 | 규정 절차와 대응 절차의 구현 여부를 판단 |
| 공식 | DPPM = (DPPM1 + DPPM2)/2 |
| 목표 | 지표에 대한 결과 값이 높을수록 DDoS에 대한 조직의 정책 및 계획 수립이 잘 되어 있다고 판단한다. |
| 구현 내용 | 보안 담당자의 주관적인 판단으로 조직의 DDoS 절차 수립 여부를 판단함 |
| 빈도 | 분기별로 정책 및 계획에 대한 수립을 판단해야 함 |
| 책임부서 | 보안 책임자 및 관리자 |
| 자료 소스 | DDoS 정책수립서와 계획서의 존재유무와 진행 사항으로 판단 |
| 보고 포맷 | 바 그래프로 표현하며, 이를 통해 지속적인 개선 여부도 체크할 수 있음 |

• DDoS 통제 관리(DCM) : DDoS 공격 발생시 자산에 대한 통제와 보안관련 통제가 잘 수행되는지에 대해 확인한다.

표 6. DDoS 통제 관리(DCM)

| 필드 | 내용 |
|---|---|
| 식별자 | DDoS 통제 관리(DCM) |
| 목적 | DDoS 공격시 자산과 보안에 대한 통제가 잘 되는지를 확인하기 위함 |
| 측정항목 | DDoS 발생시 자산에 대한 접근통제 시행 비율(DCM1),<br>DDoS 발생시 보안 관련 통제 시행 비율(DCM2) |
| 유형 | 공격 발생시 통제 항목에 대한 수행 여부를 판단 |
| 공식 | DCM = (DCM1 +DCM2)/2 |
| 목표 | 지표에 대한 결과 값이 높을수록 DDoS 공격 시 통제 관리가 잘 되어있다고 판단한다. |
| 구현 내용 | 통제 항목에 대한 관리가 선행되어야 한다. |
| 빈도 | 분기별로 통제항목에 대한 정보를 갱신해야 하며, 공격 발생 시 통제 결과에 대한 보고가 수행되어야 함 |
| 책임부서 | 보안 책임자 및 관리자 |
| 자료 소스 | 접근통제 항목서와 보안관련 통제 항목서의 존재여부와 진행결과에 따라 판단 |
| 보고 포맷 | 바 그래프로 표현하며, 이를 통해 지속적인 개선 여부도 체크할 수 있음 |

표 7. DDoS 정책 준수(DPC)

| 필드 | 내용 |
|---|---|
| 식별자 | DDoS 정책 준수(DPC) |
| 목적 | DDoS에 대응하기 위한 정책들이 공격 발생 시에 잘 지켜졌는지를 판단하기 위함 |
| 측정항목 | DDoS 관련 규정의 준수 비율(DPC1),<br>DDoS 관련 규정의 공유 비율(DPC2) |
| 유형 | 규정 절차의 준수율과 규정의 공유율의 구현 여부를 판단 |
| 공식 | DPC = (DPC1 + DPC2)/2 |
| 목표 | 지표에 대한 결과 값이 높을수록 DDoS 공격 시 조직의 정책 준수율이 높다고 판단한다. |
| 구현 내용 | 공격 발생시 DDoS 관련 규정의 체크리스트와 공유 유무에 따라 판단함 |
| 빈도 | 분기별로 관련 규정의 체크리스트 항목을 수집해야 함 |
| 책임부서 | 보안 책임자 및 관리자 |
| 자료 소스 | DDoS 대응 관련 규정서 및 체크리스트 존재 유무와 진행 사항으로 판단 |
| 보고 포맷 | 바 그래프로 표현하며, 이를 통해 지속적인 개선 여부도 체크할 수 있음 |

- DDoS 정책 준수(DPC) : DDoS 공격 발생 시 DDoS 관련 규정(절차나 대응 절차)에 따라 적절히 대응 되었는지, 관련 규정의 공유가 제대로 이루어졌는지에 대해 확인한다.

### 3.3 DDoS 대응지표 적응

수준 대응 지표는 각 세부지표인 DDoS 인력 관리(DHM), DDoS 인프라 관리(DIFM), DDoS 운영 관리(DOM), DDoS 정책 및 계획 관리(DPPM)의 평균값으로 판단되며, 20% 미만인 경우는 DDoS 대응이 미비한 수준임, 20%~50%는 DDoS 대응이 계획된 수준임, 50~80% DDoS 대응이 잘 되어 있는 수준임, 80~100%는 DDoS 대응이 운영되고 관리되는 수준임으로 판단할 수 있다.

성과 대응 지표는 각 세부지표인 DDoS 통제 관리(DCM), DDoS 정책 준수(DPC)의 평균값으로 판단하며, 20% 미만인 경우는 성과가 미비함, 20%~50%는 성과가 나타남, 50~80% 성과를 확인함, 80~100%는 성과가 관리되는 수준으로 판단할 수 있다. 제안하는 지표는 지속적으로 관리되어야 하며, 결과 값들에 대한 비교 데이터를 얻어야 한다. 제안된 측정 지표를 사용하여, DDoS 대응 지표의 수준지표에 대한 계산은 다음과 같다.

Li는 수준 대응지표를 구성하는 세부지표를 의미하며, L1은 DDoS 인력관리, L2는 DDoS 인프라 관리, L3은 DDoS 운영 관리, L4는 DDoS 정책 및 계획 관리를 지칭한다. 공식에서 n은 i번째 영역의 측정항목에 대한 개수를 의미한다.

DDoS 대응 목표와 비즈니스의 목적에 따라 각 지표의 값을 계산하기 위해 다른 가중치를 측정항목에 할당할 수 있다. Wi의 경우, i번째 세부지표의 가중치를 의미하며, 이러한 가중치는 대응 목표와 조직에 따라 조정할 수 있는 수치이다. 만약 전체적 대응 지표의 총합인 Q의 값의 범위는 0~V이다. 여기서 V는 Wi의 총합이 된다. QL의 수치가 높으면, DDoS 대응 수준이 우수하다는 것을 의미한다.

$$QL = \sum_{i=1}^{4} L_i \times W_i$$

이와 마찬가지로 성과지표에 대해서도 종합적인 판단을 내릴 수 있다.

$$QP = \sum_{i=1}^{2} P_i \times W_i$$

## Ⅳ. 검 증

### 4.1 DDoS 대응지표 적응

기준지표에 해당하는 평가항목을 KISA의 국가정보보호수준 평가지수 모델 [17], 행정안전부의 개인정보보호수준 진단지표 [18], ISO 27004 [19]에서 제시하고 있는 측정항목들을 기반으로 기준지표와 연관성이 있는 28개의 측정항목을 도출하였다. 도출된 측정항목이 실제 DDoS와 관련이 있는지, 즉 기준지표와 연관성이 있게 식별되었는지를 확인하기 위해 SMART 분석을 하였던 동일한 집단에게 설문을 하였다. 설문은 각 측정항목이 DDoS와 연관이 있는지 없는지에 대해서 물어보았으며 설문의 예는 다음 표 8과 같다.

다음과 같은 측정항목이 DDoS를 측정하는데 필요하다고 생각하십니까? 라는 질문을 28개 항목에 대해 실시하였으며, 설문의 답은 (1. 전혀 필요하지 않다 2. 필요하지 않다 3. 보통이다 4. 필요하다. 5.

표 8. 설문의 예

| 순번 | 측정항목 | 다음과 같은 측정항목이 DDoS를 측정하는데 필요하다고 생각합니까? | | | | |
|---|---|---|---|---|---|---|
| 1 | 정보보안 관련 규정 절차의 수립여부의 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 2 | 정보자산 관련 규정 절차의 수립여부의 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 3 | 인적보안 관련 규정 절차의 수립여부의 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 4 | 개인정보보호 관련 규정 절차의 수립여부의 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 5 | 물리적 보안관련 규정 절차의 수립여부의 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 6 | 접근보안 관련 규정 절차의 수립여부의 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 7 | 정보보호 전담인력 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 8 | 정보보호 인력의 역량은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 9 | 관련 규정 절차의 공유 여부의 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |
| 10 | 정보보호 관련 인증 획득 여부의 비율은 어느 정도입니까? | 1. 전혀 필요하지 않다 | 2. 필요하지 않다 | 3. 보통이다 | 4. 필요하다. | 5. 매우 필요하다 |

매우 필요하다) 이 5개 중 하나만을 선택하게 하였으며 1점부터 5점까지의 척도를 사용하였다.

설문의 결과를 가지고 식별한 측정항목이 유의한지 아닌지, 그리고 유사한 그룹에 속하는 것인지를 판단하기 위해 요인 분석을 수행하였다. 또한 요인 분석의 결과로 식별된 그룹의 신뢰도를 검증하기 위해 Cronbach's Alpha[16]를 수행하였다. 이에 대한 결과는 다음 표 9, 표 10와 같다.

28개의 측정 지표에 대한 설문을 요인 분석한 결과 11개의 컴포넌트 중 유의한 7개의 그룹이 식별되었다. 그룹 내에 요소가 1개만 들어간 경우와 신뢰할 수준에 포함되지 않은 경우는 제외하였다. 식별된 7개 그룹의 신뢰도를 Cronbach's Alpha로 검정하여 6개의 그룹을 도출하였다.

Cronbach's Alpha는 그룹 구성의 신뢰도(Reliability)를 의미한다. 신뢰도 값은 0~1 범위이고 1에 가까울수록 그룹의 유사도가 높다. 0.9 이상인 경우, 매우 유사한 수준이며($p < 0.01$), 0.7 이상인 경우 통계학적인 신뢰 수준($p < 0.05$)을 달성하였다고 판단한다. 신뢰도 값이 0.5 이상인 경우 일반적인 신뢰 수준 ($p < 0.10$)을 달성하였다고 판단한다. 요인 분석의 결과로 측정지표의 상관관계 수치가 0.5 이상인 측정지표를 집합으로 묶으면 이들의 신뢰도가 95%의 신뢰할 수 있음을 의미하며, 이는 Cronbach's Alpha의 0.7 이상의 수치와 같은 의미를 가진다.

본 연구에서는 Cronbach's Alpha의 값이 0.5이상인 즉, 신뢰도 90%를 이루는 6개의 그룹만을 최종적으로 도출하였다. 도출된 6개의 그룹을 본 논문에서 제안하는 세부 지표로 삼고 세부지표의 이름은 DDoS 특징을 반영하여 명칭을 부여하였다.

표 9. 요인 분석 결과

| | Component Matrix(a) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Component | | | | | | | | | | |
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | 정보보호 전담인력 비율 | 0.744 | -0.077 | 0.244 | 0.047 | -0.079 | 0.309 | 0.042 | -0.193 | 0.211 | -0.057 | -0.052 |
| | 정보보호 투자 비율 | 0.616 | 0.301 | 0.019 | -0.022 | -0.050 | 0.480 | -0.198 | 0.185 | -0.141 | 0.251 | 0.041 |
| | 정보보호 교육 실시 여부 | 0.533 | -0.042 | 0.441 | -0.129 | 0.196 | 0.255 | 0.227 | -0.055 | -0.108 | -0.205 | -0.333 |
| | 정보보호 인력의 역량 | 0.532 | -0.107 | 0.160 | 0.329 | -0.005 | -0.162 | -0.262 | 0.417 | 0.263 | 0.134 | -0.112 |
| 2 | 정보보호 침해사고 발생 시 대응방안 구축여부 | -0.582 | -0.134 | 0.302 | 0.157 | -0.003 | 0.371 | -0.071 | 0.177 | 0.185 | -0.330 | 0.001 |
| | 정보시스템 기기 및 통신 기기 보안 관리 여부 | -0.523 | 0.117 | 0.510 | 0.426 | -0.198 | -0.135 | -0.059 | -0.182 | 0.047 | -0.086 | 0.125 |
| | 물리적 보안 관련 장비 도입 여부 | -0.485 | -0.158 | 0.468 | -0.226 | 0.026 | -0.078 | 0.429 | -0.133 | 0.133 | 0.230 | -0.029 |
| 3 | 정보보호 관련 규정의 정기적 검토 및 갱신 | -0.136 | 0.685 | -0.016 | 0.366 | -0.046 | -0.243 | 0.087 | -0.079 | 0.230 | 0.073 | -0.112 |
| | 물리적 보안관련 규정 절차의 수립여부 | 0.124 | 0.579 | -0.026 | 0.163 | -0.262 | -0.378 | 0.274 | 0.116 | 0.110 | -0.191 | -0.233 |
| | 정보보호에 대한 경영진 및 직원의 인식 향상 정도 | 0.075 | 0.555 | -0.013 | -0.051 | -0.396 | 0.322 | 0.051 | 0.225 | -0.271 | 0.072 | 0.262 |
| | 정보시스템 및 정보보호시스템의 운영관련사항 관리 여부 | 0.082 | 0.448 | 0.079 | -0.388 | -0.371 | 0.265 | -0.055 | -0.001 | 0.363 | -0.239 | -0.021 |
| 4 | 정보보호 규정 준수 여부 | 0.515 | -0.649 | -0.027 | 0.216 | 0.009 | -0.097 | -0.056 | -0.123 | 0.342 | -0.085 | 0.128 |
| | 관련 규정 절차의 공유 여부 | 0.019 | -0.582 | 0.393 | -0.040 | -0.226 | 0.017 | 0.131 | 0.302 | 0.164 | 0.393 | 0.152 |
| 5 | 인적보안 관련 규정 절차의 수립여부 | -0.086 | 0.189 | 0.630 | -0.107 | 0.093 | -0.039 | -0.500 | -0.429 | -0.046 | 0.014 | -0.044 |
| | 정보보안 관련 규정 절차의 수립여부 | -0.211 | 0.111 | 0.626 | -0.256 | -0.037 | -0.369 | -0.204 | 0.285 | 0.201 | -0.013 | 0.036 |
| | 접근보안 관련 규정 절차의 수립여부 | 0.110 | 0.316 | 0.523 | 0.187 | -0.098 | 0.177 | -0.011 | -0.341 | -0.155 | 0.436 | 0.105 |
| | 정보자산 관련 규정 절차의 수립여부 | -0.298 | -0.160 | 0.505 | -0.169 | -0.023 | 0.102 | 0.407 | 0.196 | -0.205 | 0.193 | -0.377 |
| 6 | 정보자산 접근통제 시행 여부 | -0.170 | -0.124 | 0.092 | 0.491 | 0.136 | 0.454 | 0.021 | 0.233 | 0.026 | 0.154 | 0.327 |
| | 접근 보안 관련 통제 시행 여부 | 0.390 | 0.031 | 0.212 | 0.488 | -0.035 | 0.036 | 0.263 | -0.281 | 0.446 | -0.071 | -0.087 |
| 7 | 정보보호 관련 인증 획득 여부 | -0.361 | 0.376 | -0.073 | 0.136 | 0.548 | 0.037 | 0.441 | -0.041 | 0.175 | 0.096 | 0.135 |
| | 보안서비스 도입 여부 | 0.327 | 0.322 | 0.406 | -0.129 | 0.485 | 0.185 | -0.376 | 0.107 | -0.056 | -0.065 | -0.104 |
| X | 보안서버의 도입여부 | 0.229 | 0.112 | 0.343 | -0.482 | 0.067 | -0.172 | 0.081 | -0.189 | 0.188 | -0.177 | 0.562 |
| X | DS 보급률 | 0.390 | 0.014 | 0.205 | -0.167 | 0.061 | -0.594 | 0.097 | 0.464 | 0.072 | 0.131 | 0.031 |
| X | Firewall 보급률 | -0.177 | 0.225 | -0.112 | -0.171 | 0.034 | 0.536 | 0.245 | 0.224 | 0.415 | 0.203 | -0.135 |
| X | 이메일스팸 통제수단 이용 여부 | 0.342 | 0.178 | 0.068 | -0.040 | 0.140 | 0.067 | 0.638 | 0.214 | -0.075 | -0.366 | 0.260 |
| X | 패치 보급률 | -0.307 | 0.371 | -0.235 | -0.054 | 0.210 | -0.025 | -0.482 | 0.275 | 0.406 | 0.133 | 0.023 |
| X | 개인정보보호 관련 규정 절차의 수립여부 | -0.139 | -0.215 | -0.385 | -0.446 | -0.067 | 0.219 | 0.007 | -0.312 | 0.455 | 0.178 | -0.092 |
| X | 백신 보급률 | -0.433 | -0.303 | 0.272 | 0.086 | -0.081 | 0.321 | -0.212 | 0.269 | 0.012 | -0.505 | -0.050 |

Extraction Method: Principal Component Analysis.

a 11 components extracted.

표 10. Cronbach's Alpha 수행 결과

| | | Component | | | | | Cronbach's Alpha | 선택 (Alpha > 0.500, 90% 신뢰수준) |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | | |
| 1 | 정보보호 전담인력 비율 | 0.744 | -0.077 | 0.244 | 0.047 | -0.079 | 0.697 | O |
| | 정보보호 투자 비율 | 0.616 | 0.301 | 0.019 | -0.022 | -0.050 | | |
| | 정보보호 교육 실시 여부 | 0.533 | -0.042 | 0.441 | -0.129 | 0.196 | | |
| | 정보보호 인력의 역량 | 0.532 | -0.107 | 0.160 | 0.329 | -0.005 | | |
| 2 | 정보보호 침해사고 발생 시 대응방안 구축여부 | -0.582 | -0.134 | 0.302 | 0.157 | -0.003 | 0.582 | O |
| | 정보시스템 기기 및 통신 기기 보안 관리 여부 | -0.523 | 0.117 | 0.510 | 0.426 | -0.198 | | |
| | 물리적 보안 관련 장비 도입 여부 | -0.485 | -0.158 | 0.468 | -0.226 | 0.026 | | |
| 3 | 정보보호 관련 규정의 정기적 검토 및 갱신 | -0.136 | 0.685 | -0.016 | 0.366 | -0.046 | 0.557 | O |
| | 물리적 보안관련 규정 절차의 수립여부 | 0.124 | 0.579 | -0.026 | 0.163 | -0.262 | | |
| | 정보보호에 대한 경영진 및 직원의 인식 향상 정도 | 0.075 | 0.555 | -0.013 | -0.051 | -0.396 | | |
| | 정보시스템 및 정보보호시스템의 운영관련사항 관리 여부 | 0.082 | 0.448 | 0.079 | -0.388 | -0.371 | | |
| 4 | 정보보호 규정 준수 여부 | 0.515 | -0.649 | -0.027 | 0.216 | 0.009 | 0.522 | O |
| | 관련 규정 절차의 공유 여부 | 0.019 | -0.582 | 0.393 | -0.040 | -0.226 | | |
| 5 | 인적보안 관련 규정 절차의 수립여부 | -0.086 | 0.189 | 0.630 | -0.107 | 0.093 | 0.561 | O |
| | 정보보안 관련 규정 절차의 수립여부 | -0.211 | 0.111 | 0.626 | -0.256 | -0.037 | | |
| | 접근보안 관련 규정 절차의 수립여부 | 0.110 | 0.316 | 0.523 | 0.187 | -0.098 | | |
| | 정보자산 관련 규정 절차의 수립여부 | -0.298 | -0.160 | 0.505 | -0.169 | -0.023 | | |
| 6 | 정보자산 접근통제 시행 여부 | -0.170 | -0.124 | 0.092 | 0.491 | 0.136 | 0.533 | O |
| | 접근 보안 관련 통제 시행 여부 | 0.390 | 0.031 | 0.212 | 0.488 | -0.035 | | |
| 7 | 정보보호 관련 인증 획득 여부 | -0.361 | 0.376 | -0.073 | 0.136 | 0.548 | -0.022 | X |
| | 보안서비스 도입 여부 | 0.327 | 0.322 | 0.406 | -0.129 | 0.485 | | |

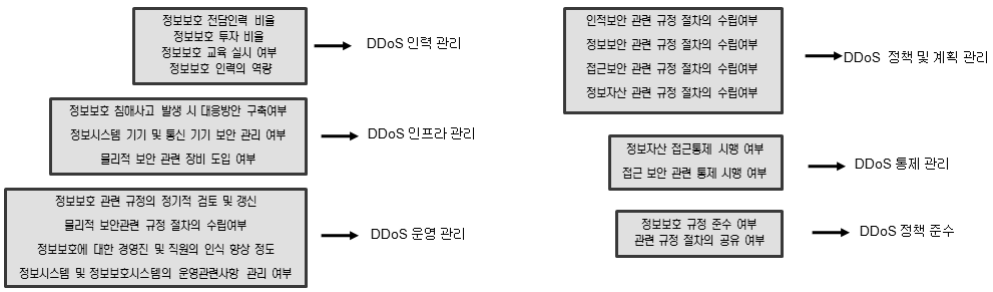


그림 3. 해당 그룹으로부터 세부지표 식별

### 4.2 DDoS 대응지표 적응

기준지표와 이를 측정하기 위한 측정항목으로부터 세부지표를 도출하였지만, 측정항목이 직접적으로 DDoS를 측정한다고 판단하기는 어렵다. 그러므로 이를 DDoS의 수준과 성과를 측정할 수 있도록 해당 측정항목을 용도에 적합하게 변경하였다. 제안된 측정항목들이 올바로 정의되었는지를 검증하기 위해 Kitchenham의 접근[20]에 기반하여 이론적인 검증을 수행하였다. 이론적인 분석은 측정이 정의된 범주안에서 유효한지 유효하지 않은지를 판단하는 근거를 제공한다. 유효한 측정은 attribute, unit, instrument, protocol validity를 가져야 한다고 주장하고 있으며 이에 대해 이론적인 검증을 수행하였다.

- Attribute Validity : 제안한 측정 항목은 ISO 27004를 기반한 기준 지표에 해당하는 측정항목을 식별하였고, 식별한 측정항목에 대한 설문 결과로써 DDoS와 관련이 있는 측정항목인지 아닌지를 판단하였으며 요인 분석의 결과와 Cronbach's Alpha로 인한 7개 그룹의 검증을 통해 DDoS 대응의 측정을 위해 필요한 항목이라는 것을 도출하였다.
- Unit Validity : 모든 측정항목에 대한 결과는 비율로써 통일된 단위를 가지고 있다. 즉, 동일한 측정 단위로써 측정이 가능하기 때문에 세부지표에 대한 결과 값도 동일한 단위인 비율로써 측정된다.
- Instrument Validity : DOM2, DPPM1, DPPM2만이 측정을 위해 담당자의 정성적인 판단으로 측정된다. 이를 제외한 12개의 측정 항목은 모두 정량적인 측정이 가능하다. 예를 들어 DHM1은 전체 보안 관련 인력의 수와 DDoS 대응 관련 전담인력의 수라는 두개의 데이터로써 측정이 가능하다. 제안한 측정항목은 DHM1과 같이 명확한 분자와 분모의 형태를 가지는 두개의 데이터로써 측정이 가능하다. 다음 표는 각 측정항목에 측정 데이터를 보여주고 있다. 즉, 분자와 분모에 해당하는 측정 데이터가 구분되어 있다.

• Protocol Validity : 측정항목을 계산하기 위한 데이터들은 관련 문서로써 명시화 되어있다. DIM1은 관련 부서의 인력 현황 문서로써 도출될 수 있으며, DIM2는 보안 교육일지 문서를 통해 도출될 수 있다. 이렇듯 제안한 도출 항목은 조직 내에서 관리되고 있는 명세와 문서로부터 도출될 수 있다.

이러한 이론적 근거를 기반으로 제안한 측정항목은 타당하다고 검증될 수 있다. 물론 경험적인 검증을 통해 제안한 측정항목에 대해 검증하는 것이 중요하나 이러한 적용은 많은 시간이 요구되기 때문에 본 연구에서는 이론적인 검증에만 초점을 맞추었다.

## V. 결 론

본 연구에서는 DDoS 대응 지표를 제안하기 위해 ISO 27004의 지표와 DDoS 대응 전략과의 관계에 대한 설문을 통해 7개의 기준 지표를 도출하였다. 도출된 기준 지표를 측정할 수 있는 측정항목 28개를 식별하여 이에 대한 DDoS 지표 항목으로써의 관계를 설문하였으며, 설문 결과에 대해 요인분석과 Cronbach's Alpha 를 수행하여 전체 11개의 그룹 중 유의한 6개의 그룹을 식별하여 이를 세부 지표로 도출하였다. 그룹핑된 결과는 일반적인 정보보안 업무에 대한 측정 항목이기 때문에 이를 DDoS을 측정하게 하기 위해 측정항목에 대해 변경하였고 이를 측정하기 위해 메트릭을 제안하였다. 제안한 메트릭에 대해 Kitchenham의 접근 방법을 활용하여 attribute, unit, instrument, protocol validity에 대해 이론적 검증을 수행하였다.

DDoS의 대응 체계를 측정할 수 있는 대응지표를 제안함으로써 DDoS 공격에 대한 대응의 조직의 수준 및 성과를 판단할 수 있을 것이다. 제안한 지표가 모든 DDoS 상황을 커버하지는 않는다. 그러므로 제안한 프레임워크를 기반으로 실제 DDoS 대응을 수행하고 있는 조직에 대해 적용해보고, 이러한 적용을 통해 도출한 지표에 대한 지속적인 보완이 필요하다.

## 참 고 문 헌


[1] 인터넷침해사고대응지원센터, 국내 주요 사이트 대상 분산서비스거부공격 분석보고서, 한국정보보호진흥원, 2009. 07.

[2] 이원창, 김용겸, "IT BSC 기반의 서비스수준협약 측정지표, 핵심성공요인, 전략체계도 간 연계", 인터넷전자상거래연구, 제8권, 제3호, pp.257-291, 2008. 09.

[3] ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements, ISO, 2005.

[4] ISO/IEC 27002, Information Technology - Code of Practice for Information Security Management, ISO, 2007.

[5] 이희명, 임종인, "기업의 정보보호수준 측정모델 개발에 관한 연구", 한국정보보호학회논문지, 제18권 제5호, 2008. 10.

[6] ISO/IEC 18028-1, Information technology - Security techniques - IT network security - Part 1: Network security management, ISO, 2006.

[7] ISO/IEC 18028-2, Information technology - Security techniques - IT network security - Part 2: Network security architecture, ISO, 2006.

[8] ISO/IEC 18028-3, Information technology - Security techniques - IT network security - Part 3: Securing communications between networks using security gateways, ISO, 2005.

[9] ISO/IEC 18028-4, Information technology - Security techniques - IT network security - Part 4: Securing remote access, ISO, 2005.

[10] 나윤지, 조영석, 고일석, "기업의 정보보호 수준 평가를 위한 평가지표", 정보보안 논문지 제6권 제3호, 2006. 09.

[11] NIST SP800-55(Rev.1), Performance Measurement Guide for Information Security, NIST, 2008. 7.

[12] NIST SP800-53(Rev.2), Recommended Security controls for Information Security, NIST, 2007. 10.

[13] Information Systems Audit and Control Association, COBIT4.1, ISACA & ITGI,Val IT,CGEIT Exam Resources, 2007.

[14] McShane, S.L., Von Glinow, M.A., Organizational behavior: emerging realities for the workplace revolution(3rd), McGraw-Hill. 2005.

[15] Gorsuch R. L., Factor Analysis, Hillsdale, 1983.

[16] Cronbach L.J., "Coefficient alpha and internal structure of tests", Psycometrika, Vol.16, No.3,

pp.297-334, 1951.
[17] 한국인터넷진흥원(KISA), 국가 정보보호수준 평가지수 모델, KISA, 2006.
[18] 행정안전부, 개인 정보보호수준 진단지표, 행안부, 2007.
[19] ISO/IEC 27004, Information technology - Security techniques - Information security management - Measurement, ISO, 2009.
[20] Barbara Kitchenham, Shari Lawrence Pfleeger, Norman Fenton, "Towards a Framework for Software Measurement Validation", IEEE Transactions On Software Engineering, Vol.21, No.12, pp.929-944, 1995. 12.

**박 춘 자** (Chun Ja Park) 정회원

2010년 8월 숭실대학교 박사과정
2010년 8월 현재 영화초등학교 부장교사
<관심분야> 정보보호, 이런닝(E-learning)등

**김 범 재** (Bum-Jae Kim) 정회원

1988년 3월 서울대학교 독어독문학과 학사
2000년 8월 연세대학교 산업대학원 전자계산전공 석사
2010년 8월 숭실대학교 컴퓨터학과 박사
1992년 7월~1995년 2월 (주)쌍용컴퓨터
1995년 3월~2009년 2월 한국 HP(공공사업본부 e-Gov't 사업부장 이사)
2009년 2월~현재 (주)엘엔케이시스 대표이사
<관심분야> 멀티캐스트, 그룹통신, 인터넷 보안, 이동 인터넷 통신

**신 용 태** (Yong Tae Shin) 정회원

1985년 2월 한양대학교 산업공학과 학사
1990년 Univ. of Iowa 컴퓨터학과 석사
1994년 Univ. of Iowa 컴퓨터학과 박사
1994년~1995년 Michigan State Univ. 전산학과 객원교수
1995년 3월~현재:숭실대학교 컴퓨터학부 부교수
<관심분야> 멀티캐스트, 그룹통신, 인터넷 보안, 이동 인터넷 통신

**김 종 배** (Jong bae Kim) 정회원

2002년 8월 숭실대학교 석사
2006년 8월 숭실대학교 박사
2001년~현재 (주)이엔터프라이즈 대표이사
2004년~2006년 남서울대학교 컴퓨터학과 겸임교수
2006년~현재 서울여자대학교 컴퓨터학부 겸임교수
2009년~현재 (사)해킹보안협회 학술연구위원장
<관심분야> 소프트웨어 개발 방법론, 정보보호, 오픈소스 소프트웨어