情 報 保 護 學 會 誌
第21卷 第2號, 2011. 4

ITU-T SG17 사이버보안 국제표준화 동향

김 미 주*, 정 현 철*, 염 흥 열**

요 약

지난 3월 4일 국내 일부 금융기관과 포털 사이트 등이 분산서비스거부 공격으로 접속이 중단되는 사태가 발생했다. 이번 사건뿐만 아니라 세계 곳곳에서는 범죄적 양상을 띠는 다양한 사이버 범죄 발생이 증가하고 있다. 이에 앞서 미 정부는 2009년 "사이버스페이스 정책 리뷰(cyberspace policy review)"를 발표해 사이버보안의 책임 공유, 사이버보안 사고 발생 시 긴밀한 대응을 위한 유관기관 간의 정보 공유 및 사고 대응을 위한 체계 구축 등의 전략을 내세운 바 있다. 이러한 전략의 연장선으로 예상되는 사이버보안에 대한 국제표준화 활동이 ITU-T SG17 Q.4에서 진행되고 있어 사이버보안 분야 표준화 동향과 함께 Q.4의 주요 의제인 사이버보안 정보 교환 기술에 대한 정보를 제공하고자 한다.

Ⅰ. 서 론

스마트폰, 태블릿 PC 등 기기 및 통신 환경의 발전으로 현대 사회는 시간과 장소에 얽매이지 않고 인터넷을 이용해 뱅킹 서비스를 이용하고 업무도 수행하는 등 생활의 편리함을 영위할 수 있게 되었다. 이러한 현상은 가상의 사이버공간의 양적인 팽창을 초래하였다고 볼 수 있다.

하지만 이 같은 사이버공간의 양적인 팽창 이면에는 개인정보 및 금융정보의 유출, 데이터 위변조, 서비스 거부, 악성코드 감염, 도청 등 다양한 사이버공간의 보안 위협의 발생을 증대시키는 결과를 초래하기도 하였다. 또한 사이버보안 위협의 양상이 점차 세계화되고 피해의 규모 또한 날로 심각해지고 있어, 사이버공간의 질적 팽창 및 진정한 성장을 위한 국제적인 공조 대응 노력이 절실하게 필요한 시점이다.

이에 본 고에서는 사이버보안 분야의 국제적인 공조 대응의 일환으로 ITU-T SG17(보안 그룹) 내 Q.4 (사이버보안 연구과제)에서 추진 중인 사이버보안 관련 표준들의 동향에 대해서 살펴보고, 특히 Q.4에서 미국 등 주요국을 중심으로 비중있게 다뤄지고 있는 사이버보안 정보 교환 기술에 대해서 중점적으로 살펴보고자 한다.

Ⅱ. ITU-T SG17 Q.4(사이버보안) 표준화 동향

ITU-T SG17 Q.4는 사이버보안 연구그룹으로 사이버공간에서 발생하는 침해사고 및 취약점 등에 대한 대응방안 및 정보 공유 등에 대한 보안 표준들을 개발하고 있다. 의장단은 라포처로 미국의 Anthony M. Rutkowski, 부라포처로 한국의 김종현 박사(ETRI) 그리고 일본의 Youki Kadobayashi가 Q.4 연구그룹을 이끌고 있다.

Q.4에서 개발되어 제정된 주요 표준으로 사이버보안의 개요를 정리한 X.1205, OASIS의 XML언어를 ITU-T ASN.1언어로 바꾸는 X.1303, 통신 서비스 제공자용 스파이웨어 및 잠재적 유해 소프트웨어 대응을 위한 가이드라인인 X.1207, 사이버보안 정보 공유 및 교환을 위한 요구사항 및 시나리오를 정의한 X.1209, 한국과 일본의 봇넷 대응 모델을 best practice로 제시한 X.1205 supplement 8 등이 있다.

또한 지난 2010년 12월 SG17 정기회의에서 문서 개발 작업을 마치고 각 국가별로 회람 중인 문서로, 3장에서 본격적으로 다뤄질 사이버보안 정보 교환 기술을 담고 있는 X.1500, 취약점에 대한 표준화된 식별자를 부여하는 X.1520, 취약점 특성에 따라 점수를 부여하는 시스템을 정의한 X.1521 등이 있다.

현재 개발 중인 표준 문서는 [표 1]과 같다.

본 연구는 방송통신위원회의 지원을 받는 방송통신연구개발사업의 연구결과로 수행되었음
* 한국인터넷진흥원 인터넷침해대응센터 침해예방단 연구개발팀 ({mijoo.kim, hcjung}@kisa.or.kr)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

〔표 1〕 ITU-T SG17 Q.4에서 개발 중인 표준 문서

구분	약어	표준안 제목	설명
CYBEX	X.cwe	Common Weakness Enumeration	어플리케이션 취약점 목록
	X.cwss	Common Weakness Scoring System	어플리케이션 취약점 스코어링 시스템
	X.oval	Open Vulnerability and Assessment Language	취약점 점검 항목
	X.xccdf	Extensible Configuration Checklist Description Format	확장 가능한 설정 체크리스트 명세 포맷
	X.cpe	Common Platform Enumeration	표준 플랫폼 목록
	X.cce	Common Configuration Enumeration	표준 설정 목록
	X.arf	Assessment Result Format	평가 결과 포맷
	X.cee	Common Event Expression	표준 이벤트 표현
	X.capec	Common Attack Pattern Enumeration and Classification	공격 패턴 목록 및 분류
	X.iodef	Incident Object Description Exchange Format	침해 대상 명세 교환 포맷
	X.maec	Malware Attribute Enumeration and Classification	악성코드 속성 목록 및 분류
	X.pfam	Misuse Enumeration and Characterization	피싱, 사기, 오용 속성 목록 및 분류
	X.cyiql	Cybersecurity Information Query Language	사이버보안 정보 쿼리 랭귀지
	X.cybex-beep	A BEEP Profile for Cybersecurity Information Exchange Techniques	사이버보안 정보 교환 기술을 위한 BEEP(Block Extensible Exchange Protocol) 프로파일
	X.cybex-tp	Transport protocols supporting cybersecurity information exchange	사이버보안 정보 교환을 위한 전송 프로토콜
사이버 보안 일반	X.gopw	Guideline on preventing malicious code spreading in ICT networks	악성코드 예방 가이드라인
	X.abnot	Abnormal traffic detection and control guideline for telecommunication network	비정상 트래픽 탐지 및 통제 가이드라인
	X.bots	Centralized framework for Botnet detection and response	봇넷 탐지 및 대응 프레임워크
	X.csi	Guidelines for cybersecurity index	사이버보안 인덱스 가이드라인
	X.dexf	Digital forensics exchange format	디지털 포렌식 교환 포맷
	X.eipwa	Guideline on techniques for preventing web-based attacks	웹 기반 공격 대응 기술 가이드라인
	X.gpn	Mechanism and procedure for distributing policies for network security	정책 공유를 위한 메커니즘 및 프로시저
	X.sips	Framework for countering cyber attacks in SIP-based services	SIP 기반 서비스에서의 사이버공격 대응 프레임워크
	X.sip-cyber	Security Guidelines for countering cyber attacks in SIP-based services	SIP 기반 서비스에서의 사이버공격 대응을 위한 보안 가이드라인
	X.ssaf	Security standards availability framework	보안 표준 이용 프레임워크
	X.tb-ucc	Traceback scenarios and capabilities	역추적 시나리오 및 요구사항
	X.trm	Traceback mechanisms	역추적 메커니즘

Ⅲ. 사이버보안 정보 교환 기술

3.1 사이버보안 정보 교환 기술 개요

사이버보안 정보 교환 기술은 2008년 6월 독일 하이델베르크에서 개최된 Q.6(현재 Q.4) 사이버보안 연구그룹의 인터림 회의를 통해서 소개되었다. 현재 Q.4의 라포처인 Anthony M. Rutkowski는 사이버 공간의 침해사고에 대한 공조의 일환으로 침해 정보와 같은 사이버보안 정보에 대한 정보 교환 참여자간에 교환을 지원

하는 프레임워크"를 제안하였다. 해당 아이템은 2008년 9월 SG17 정기회의를 통해 공식화되었으며, 이와 관련된 사이버보안 정보 교환 구현을 위한 표준 항목으로 미국의 정보보호 관련 연구 개발 기관인 Mitre의 정보보호 관련 시스템 및 기술들과 NIST의 정보보호 표준 등을 신규 표준화 항목으로 채택하였다. 이와 함께 사이버보안 정보 교환 프레임워크 관련 각 국의 대표단으로부터 제안되어 신규 표준화 항목으로 채택되었다. 일명 CYBEX(Cybersecurity Informaton Exchange)라 불리는 이 표준화 작업은 미국의 주도 및 일본 등 주요국의 적극적인 참여와 함께 인터림 회의 및 텔레컨퍼런스를 수시로 개최함으로써 표준 개발에 박차를 가하는 등 빠른 속도로 진행되고 있다. 그 결과 2010년 12월 SG17 정기회의에서 사이버보안 정보 교환 프레임워크에 관련된 3건의 아이템에 대한 determination이 추진되어 제정을 앞두고 있으며, 나머지 아이템들에 대한 표준 개발도 빠르게 진행되고 있다.

3.2 사이버보안 정보 교환 기술(X.1500)

3.2.1 기본 개념

사이버보안 정보 교환 프로젝트 작업의 첫 표준안으로 2010년 12월 determination 되어 제정을 앞두고 있다. 본 표준안은 사이버보안 정보 교환 개념 및 구성 기술들을 정의하고 있다.

여기서 사이버보안 정보를 교환하는 개체는 보통 사이버보안 정보를 가지거나 찾는 조직, 개인, 장치, 혹은 프로세스로 구성될 수 있으며, 대부분 이러한 개체는 CIRT나 장비, 소프트웨어 혹은 네트워크 기반 시스템 운영자 혹은 제조업체가 이에 해당된다.

사이버보안 정보 교환은 공공 도메인뿐만 아니라 사전에 정책에 동의해서 알아야 할 필요가 있는 신뢰된 커뮤니티 간에도 발생 할 수 있다. 개체 간 교환되는 정보는 보통 위협, 취약점, 침해, 위험 그리고 대응방안 등이다. 이 권고안에 포함된 관련 기술들은 이러한 정보 교환을 가능하게 하고 그렇게 함으로써 향상된 사이버보안을 제공하게 된다.

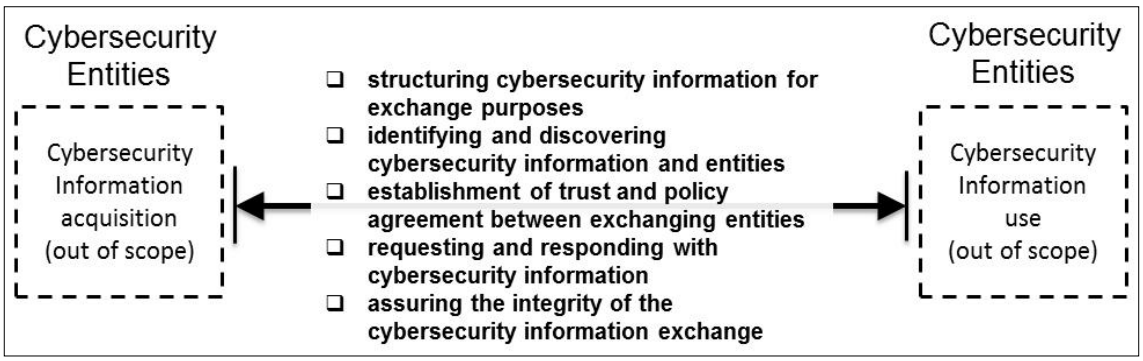
이 권고안에서 사용되는 사이버보안 정보 교환 모델은 [그림 1]과 같은 기본 기능들로 구성된다. 기능들은 개별적으로 혹은 적절히 결합되어 사용될 수 있으며, 높은 수준의 사이버보안 정보 교환을 위해 필요에 따라 확장될 수 있다. 사이버보안 정보 교환 모델의 주요 기능은 아래와 같다.

- 교환 목적의 사이버보안 정보 구조화
- 사이버보안 정보 및 개체의 식별 및 발견
- 교환 개체 간의 신뢰 및 정책 동의 설정
- 사이버보안 정보 요청 및 응답
- 사이버보안 정보 교환의 무결성 보장

또한 본 권고안에서는 이러한 기능들을 성취하기 위한 요소 기술들을 함께 기술하고 있다.

사이버보안 정보의 교환은 양방향성 성질을 가지며, 이러한 양방향성 교환은 확실한 정보의 요청 및 응답에 대해서 개체 간에 교환되는 정보의 신뢰성 수준을 보증하거나 전달에 대한 인증을 제공하기 위함이다.

또한 본 권고안은 동의된 정책과 적용된 법률 및 규정을 조건으로, 정보의 사용 및 획득 수단은 권고안의 범위 밖으로 이 권고안에서는 다루고 있지 않다.



〔그림 1〕 CYBEX 모델

3.2.2 사이버보안 정보 교환 클러스터

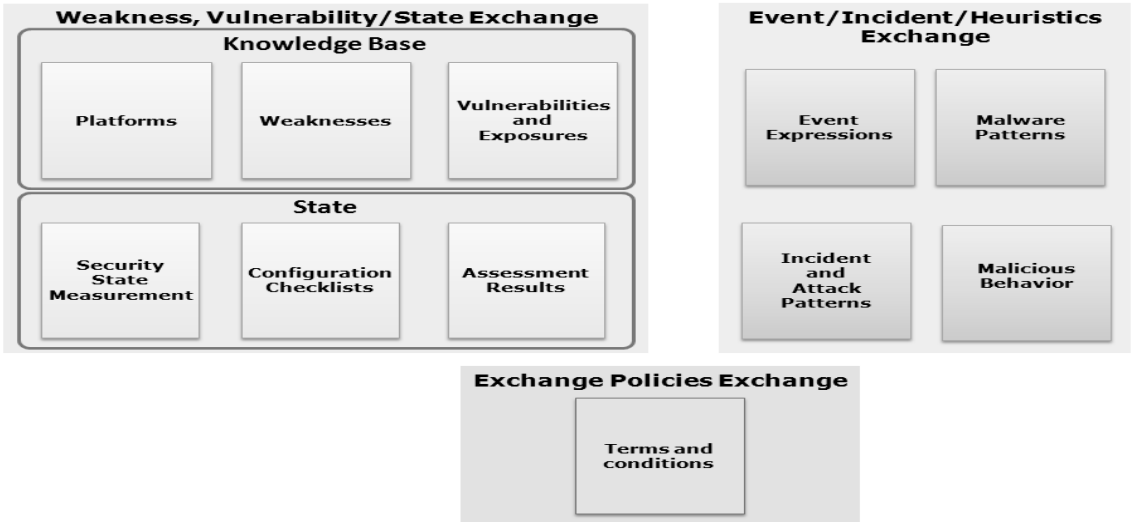
사이버보안 정보의 교환은 두 개체 간에 발생하기 때문에 두 개체 모두에 의해 이해할만한 일관된 매너가 구조화되고 기술되어야 한다. CYBEX는 "공통 목록(common enumerations)"을 포함해 사이버보안 정보의 공유를 위해 규칙을 정의해 교환 활동을 더 쉽게 하는데 그 목적이 있다. 공통 목록은 동일한 데이터 타입에 대한 확실한 정보 값을 순서대로 목록화한 것으로 사이버보안 관련 정보의 비교를 용이하게 한다.

권고안은 사이버보안 정보 교환을 위해 여섯 가지 "클러스터"로 구성된 기술들을 정의하고 있다.

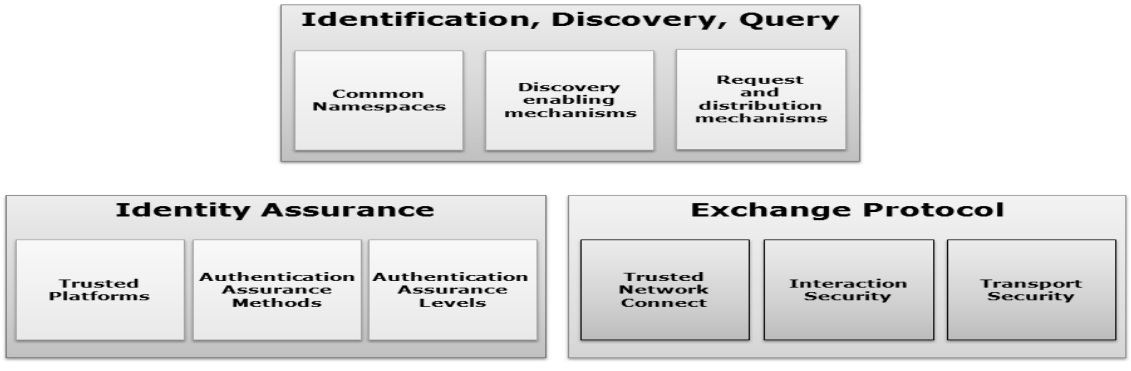
- 약점, 취약점 그리고 상태
- 이벤트, 침해, 휴리스틱
- 정보 교환 정책
- 식별, 발견, 쿼리
- 신원 보증
- 교환 프로토콜

이러한 클러스터는 넓은 분류이고, 실제로 한 클러스터 내에서의 활용은 응용에 따라 하나 혹은 그 이상의 클러스터가 사용될 것이다.

각 클러스터의 기능에 대해서는 [표 1]~[표 6]에서 설명한다.



〔그림 2〕 CYBEX 클러스터: 구조화된 정보



〔그림 3〕 CYBEX 클러스터: 이용

〔표 1〕 약점, 취약점 그리고 상태 클러스터

기술	설명	참조
Common Vulnerabilities and Exposures(CVE)	CVE는 보안 취약점에 대한 식별 및 교환을 위한 방법으로, 알려진 문제점들에 대한 표준화된 식별자를 제공하는 것이 목적이다. CVE의 목표는 "공통 목록"내에 독립된 취약점에 대한 데이터 공유를 쉽게 하기 위함이다. CVE는 취약점 데이터베이스 및 요구사항들을 서로 연결시키고, 보안 도구 및 서비스의 비교를 가능하게 하도록 하기 위해 만들어졌다. 예를 들어 CVE는 위험, 영향, 해결 정보, 혹은 상세한 기술적인 정보는 포함되지 않는다. CVE는 오로지 상태 지표, 간단한 설명, 그리고 취약점 리포트와 경보와 관련된 참조만을 포함하고 있다.	Recommendation ITU-T X.1520
Common Vulnerability Scoring System(CVSS)	CVSS 프로세스는 ICT 취약점의 특징 및 영향을 전달하기 위한 오픈 프레임워크를 제공한다. CVSS는 세 가지 기준 그룹으로 구성된다. 기본 기준, 시간적 기준, 환경적 기준. 각각의 그룹은 0부터 10까지의 숫자로 된 스코어와 스코어를 도출하기 위해 사용되는 값이 반영된 압축된 문자 표현인 벡터를 만들어낸다. 기본 그룹은 취약점의 본질적인 특징을 표현한다. 시간적 기준 그룹은 시간이 흐름에 따라 변하는 취약점의 특징을 나타낸다. 환경적 기준 그룹은 사용자의 환경에 고유한 취약점의 특징을 나타낸다. CVSS는 ICT 취약점을 점수화하는 공통 언어로 채택됨으로써 ICT관리자, 취약점 뉴스 제공자, 보안 업체, 어플리케이션 업체, 연구원들에게 유용하게 사용될 것이다.	Recommendation ITU-T X.1521
Common Weakness Enumeration(CWE)	CWE는 주요 소프트웨어 공통 취약점 집합을 식별하고 교환하기 위한 프로세스이다. CWE는 소스 코드와 운영체제에서 취약점을 발견하는데 사용하는 소프트웨어 보안 툴 및 서비스에 대한 토론, 설명, 선택 그리고 사용을 더 효과적으로 할 수 있게 한다. 또한 구조와 설계와 관련된 소프트웨어 취약점에 대한 이해를 높이고 관리를 용이하게 한다. CWE 구현은 콘텐츠에 대해서 보증할 수 있는 다양한 산업계, 학계, 정부 기관의 전문가들로부터 편집되고 업데이트된다. CWE는 표준화된 용어를 제공하고 서비스 제공자로 하여금 잠재적인 취약점 및 제안 솔루션을 사용자에게 알릴 수 있게 하며, 소프트웨어를 사는 사람에게 다양한 업체에 의해 제고되는 유사한 제품을 비교할 수 있도록 한다.	MITRE, Common Weakness Enumeration
Common Weakness Scoring System(CWSS)	CWSS는 소프트웨어 취약점의 특징 및 영향을 전달하는 오픈 프레임워크를 제공한다.	MITRE, Common Weakness Scoring System
Open Vulnerability and Assessment Language(OVAL)	OVAL은 오픈되고 공개적으로 이용 가능한 보안 컨텐츠의 이용을 촉진하고 보안 툴 및 서비스의 범위에 있어 정보의 이동을 표준화하기 위한 국제적인 설명서 활동이다. OVAL은 시스템 세부사항을 인코드하기 위해 사용되는 랭귀지, 공동체 내에 콘텐츠 저장소의 집합체를 포함하고 있다. 랭귀지는 3가지의 주요 평가 프로세스 단계를 표준화 한다. 테스트를 위한 시스템 설정 정보의 표현, 명시된 기계의 상태에 대한 시스템 분석, 평가 결과의 보고, 저장소는 랭귀지를 사용하는 공개적으로 이용가능하고 오픈된 컨텐츠의 집합이다. OVAL 스키마는 OVAL 랭귀지의 프레임워크 및 용어로서 제공하기 위해 개발된 XML로 작성된다. 이러한 스키마는 세 가지의 평가 프로세스와 부합한다. 시스템 정보를 표현하는 OVAL System Characteristics 스키마, 특정 기계 상태를 표현하기 위한 OVAL Definition 스키마, 평가 결과 보고를 위한 OVAL Results 스키마	MITRE, Open Vulnerability and Assessment Language
eXtensible Configuration Checklist Description Format(XCCDF)	XCCDF는 보안 체크리스트, 벤치마크, 관련 문서들을 작성하기 위한 명세서 랭귀지이다. XCCDF 문서는 목표 시스템 집합의 보안 설정의 구조화된 집합을 나타낸다. 명세서는 정보 교환, 문서 생성, 조직적이고 상황에 따른 조정, 자동화된 컴플라이언스 테스트, 그리고 컴플라이언스 스코어링을 지원하기 위해 설계되었다. 또한 벤치마크 컴플라이언스 테스트 결과를 저장하기 위한 데이터 모델과 포맷을 정의한다. XCCDF의 목적은 보안 체크리스트, 벤치마크, 설정 가이드의 표현을 위한 단일화된 포맷을 제공하고, 그렇게 함으로써 좋은 보안 practices의 어플리케이션을 더 널리 전파하는 환경을 조성하는데 있다. XCCDF 문서는 XML로 표현된다.	NIST, The eXtensible Configuration Checklist Description Format
Common Platform Enumeration(CPE)	CPE는 엔터프라이즈의 컴퓨팅 자원에서 소프트웨어 시스템과 하드웨어 장비를 식별하고 묘사하는 위해 표준화된 방법이다. CPE는 잘 형성된 CPE 이름의 논리적 구조 및 컴퓨터로 해독할 수 있는 인코딩을 가진 이름들을 바인딩(binding)과 언바인딩(unbinding)을 위한 프로시저를 포함한 네이밍 설명서, 동일한 제품 및 플랫폼을 참조하는지 여부를 결정하는 CPE 이름 비교를 위한 프로시저를 정의하는 매칭 설명서, 식별자 사전의 개념을 정의하고 사전 큐레이터를 위한 높은 수준의 규칙을 규정한 사전 설명서	MITRE, Common Platform Enumeration
Common Configuration Enumeration(CCE)	CCE는 여러 정보 소스 및 툴에서 설정 데이터의 빠르고 정확한 상관관계 파악을 가능하게 하기 위한 시스템 설정에 대한 유일한 식별자를 제공한다.	MITRE, Common Configuration Enumeration
Asset Reporting Format(ARF)	ARF는 평가 툴, 자산 데이터베이스, 그리고 자산 정보를 관리하는 제품 간의 평가 결과 데이터를 장치 간 교환하기 위한 구조화된 랭귀지를 제공하는 명세서이다. 이는 IT 자산에 대한 상세화된 설정 데이터를 수집하는 툴에 의해 사용되게 하기 위해 만들어졌다. 또한 여러 자산에 걸친 정보의 리포팅을 가능하게 하는 종합 리포팅 명세서와 평가 결과 요청을 가능하게 하는 테스트와 쿼리 랭귀지를 포함한다. 보안 자동화 명세서는 데이터 저장소에 평가 컨텐츠를 전달하기 위한 종단간 프로세서, 컨텐츠에 대한 평가 요청, 평가 결과에 대한 리포팅, 엔터프라이즈 레벨의 종합 평가 결과를 서술한다.	MITRE, Assessment Results Format

〔표 2〕 이벤트, 침해, 휴리스틱 클러스터

기술	설명	참조
Common Event Expression (CEE)	CEE는 컴퓨터 이벤트에 대한 묘사, 로그, 교환 방법을 표준화한 것이다. CEE의 공통 랭귀지와 syntax를 사용함으로써, 엔터프라이즈 로그 관리, 상관관계, 감사, 그리고 침해 처리를 효과적으로 수행할 수 있게 된다. 이 활동의 주요 목적은 전자적인 시스템으로부터 로그의 표현 및 교환을 표준화하는 것에 있다. CEE는 로그의 기록 및 교환을 네 가지 구성요소로 분리된다. 즉, 이벤트 분류, 로그 syntax, 로그 전송, 권고사항 로깅	MITRE, Common Event Expression
Incident Object Description Exchange Format (IODEF)	IODEF는 컴퓨터 보안 침해에 관해 CIRTs(Computer Incident Response Teams)에 의해서 교환되는 정보의 교환을 위한 프레임워크로 제공하는 데이터 표현을 제공한다. 또한 정보 모델을 묘사하고 XML 스키마로 명세된 관련 데이터 모델을 제공한다.	IEEE RFC 5070 Incident Object Description Exchange Format
Phishing, Fraud, and Misuse Format	Phishing, Fraud, and Misuse Format은 피싱, 사기, 오용에 대한 리포팅을 지원하기 위해 IODEF를 확장한 것이다. 또한 스팸 침해에 대한 정보의 교환을 지원한다.	IEEE RFC 5901 Extensions to the IODEF-Document Class for Reporting Phishing
Common Attack Pattern Enumeration and Classification (CAPEC)	CAPEC은 공격 패턴의 식별, 묘사, 열거에 대한 명세 방법이다. 공격 패턴은 공격자의 관점을 포착하는데 매우 효과적인 메커니즘이다. CAPEC의 목적은 종합적인 XML 스키마와 분류를 포함한 공개적으로 이용 가능한 공격 패턴의 목록을 제공하는 것이다.	MITRE, Common Attack Pattern Enumeration and Classification
Malware Attribution Enumeration and Characterization Format	Malware Attribution Enumeration and Characterization Format은 열거된 속성 및 행위의 공통 용어의 syntax 그리고 이러한 데이터 요소에 관한 구조화된 정보에 대한 교환 포맷 모두를 제공하기 위한 스키마를 포함한 정규 언어이다.	MITRE, Malware Attribute Enumeration and Characterization

〔표 3〕 정보 교환 정책 클러스터

기술	설명	참조
Traffic Light Protocol (TLP)	TLP는 민감한 정보의 공유를 장려하기 위해 만들어졌다. TLP는 정보를 널리 배포하기 위해 고안된 간단한 방법을 제공한다. 이는 신뢰된 방법으로 개개인, 조직 혹은 커뮤니티 간의 정보의 흐름을 향상시키기 위해 설계되었다. TLP는 송신자가 네 개의 색상 중 하나를 정보에 라벨링하는 개념을 기반으로 한다. 더 넓은 전파가 요구되는 경우 수신자는 송신자와 반드시 상의해야한다. TLP는 30개 이상의 국가에서 보안 커뮤니티 간의 신뢰된 정보 교환을 위한 모델로 채택되어 사용되고 있다. • RED - 개인적. 명시된 수신자만을 위한 정보 • AMBER - 제한적인 분배. 알 필요가 있다는 원칙에 기반하여 조직내 사람들과의 정보 공유 • GREEN - 지역사회 전체 특정 커뮤니티 내에서 공유될 수 있음. 하지만 정보는 인터넷 상에서 출판 또는 포스트되거나 커뮤니티 밖으로 공개될 수 없음 • WHITE - 제한 없음. 표준 저작권 규칙을 조건으로, 정보는 제한 없이 자유롭게 배포	Traffic Light Protocol. Information Sharing Levels, CPNI Information Exchange, UK CPNI (April 2010)

〔표 4〕 식별, 발견 쿼리 클러스터

기술	설명	참조
Discovery Mechanisms in the Exchange of Cybersecurity Information	이 기술에는 사이버보안 정보 소스의 식별 및 위치 찾기, 사이버보안 정보의 유형, 사이버보안 정보의 특정 예, 사이버보안 정보 접근에 적용되는 정책 뿐 아니라 접근을 위해 사용 가능한 방법에 사용될 수 있는 방법 및 메커니즘을 포함한다.	
Guidelines for Administering the OID arc for cybersecurity information exchange	공통 글로벌 사이버보안 식별자 네임스페이스(namespace)는 OID arc의 일부로서 관리상의 요구사항과 함께 ITU-T X.1500.1에서 명시하고 있으며, 사이버보안 정보, 사이버보안 조직, 사이버보안 정책에 대한 식별자를 포함하고 있다.	
Cybersecurity Information Query Language	Cybersecurity Information Query Language는 컴퓨터 보안 침해에 관해 CIRTs(Computer Incident Response Teams)에 의해서 교환되는 정보의 요구를 위한 프레임워크는 제공하는 데이터 표현을 제공한다. 이 명세서는 CYIQL을 위한 정보 모델을 묘사하고 XML 스키마로 명시된 연관된 데이터 모델을 제공한다.	

〔표 5〕 신원 보증 클러스터

기술	설명	참조
Trusted platforms	임베디드 TPMs(Trusted Platform Modules)이 포함된 컴퓨팅 및 통신 제품은 산업체, 학계, 정부 기관, 고객의 신뢰성 있는 정보 교환 능력을 증진시키기 때문에 TPMs은 대부분의 CYBEX 구현과 관련이 있다. TPM은 강력한 사용자 인증 및 기기 인증을 가능하게 하기 위해 다양한 플랫폼에 붙인 특별한 목적의 ICs(Integrated circuits)이다. 기밀 정보 및 민감 정보로의 부적합한 접근을 예방하고 해킹당한 네트워크로부터 보호하기 위해 필수 사항이다. TPM 기술은 혼합된 벤더 환경에서 다양한 제품의 상호운용성을 보장하기 위한 오픈 표준에 기반하고 있다. 일반적인 TPM 표준은 CC(Common Criteria)에 대한 보안성 평가를 위한 보호 프로파일과 함께, TCG(Trusted Computing Group)에 의해 개발되고 유지되는 명세서의 집합으로 구성된다.	Trusted Platform Modules. Trusted Computing Group.
Trusted Network Connect	TNC(Trusted Network Connect)는 네트워크 접근 통제를 위한 오픈 아키텍처이다. 이것의 목표는 네트워크 제공자가 모든 네트워크 연결에서 종단점의 무결성을 제공하는 것을 가능하게 해서, 다중 벤더 네트워크 종단점 간의 상호운용성을 지원하기 위함이다.	Trusted Network Connect. Trusted Computing Group.
Entity authentication assurance	이 표준은 개체의 식별자 및 그것과 관련된 식별 정보의 보증을 관리하기 위한 인증 생명주기 프레임워크를 제공한다. 특히, 개체의 식별자 및 관련 식별자 정보 인증의 보증 레벨을 질적으로 측정하고 할당하는 방법 및 인증 보증 레벨을 전달하는 방법을 제공한다.	Electronic Authentication Guideline, NIST Special Publication 800-63 Version 1.0.2, April 2006
Extended Validation Certificate framework	EVC 프레임워크는 기술, 프로토콜, 식별자 증명, 생명주기 관리, 그리고 인증 주체와 관련된 EV Certificates의 발급 및 유지를 위해 만족되어야 하는 최소한의 요구사항을 묘사하는 감사 업무의 통합적인 조합으로 구성한다.	CA/Browser Forum, Guidelines for the Issuance and Management of Extended Validation Certificates, Ver. 1.3
Policy requirements for certification authorities issuing public key certificates	이 문서는 EVC(Extended Validation Certificates)를 포함한 공개키 인증서를 발급하는 CAs(Certification Authorities)와 관련된 정책 요구사항을 명세한다. 이는 가입자, CA에 의해 인증된 주체, 암호학적 메커니즘 지원을 받는 인증서의 응용성에서 신뢰를 가진 신뢰 당사자와 같은 인증서를 발급하고 관리하는 인증기관의 운영 및 관리 업무 상의 정책 요구사항을 정의한다.	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ETSI TS102042.

〔표 6〕 교환 프로토콜 클러스터

기술	설명	참조
Blocks Extensible Exchange Protocol (BEEP) Profile for CYBEX	사이버보안 정보 교환 기술을 위한 BEEP 프로파일은 CYBEX.BEEP가 RFC3080에서 기술하고 있는 연결 지향의 비동기 상호 작용을 위한 일반적인 응용 프로토콜 커널 내부에서 사용을 위한 BEEP 프로파일을 명세한다. BEEP의 핵심은 개체 간 메시지의 동시의 독립적인 교환을 가능하게 하는 틀을 만드는 메커니즘이다. 모든 교환은 전송 보안, 사용자 인증 혹은 데이터 교환 같은 잘 정의된 어플리케이션과 합쳐져서 채널 안에서 발생한다.	IETF RFC 3080 The Blocks Extensible Exchange Protocol Core
Simple Object Access Protocol (SOAP) for CYBEX	SOAP는 분산된 환경에서 데이터 교환을 위한 경량 프로토콜이다. XML 기반의 프로토콜로 세 가지 부분으로 구성된다. 즉, 메시지 안에 무엇이 있고, 그것을 어떻게 처리해야하는지 묘사하기 위한 프레임워크를 정의한 envelope, 어플리케이션에 의해 정의된 데이터타입의 예를 표현하는 인코딩 규칙의 집합, 원격 프로시저 요청 및 응답을 표현하기 위한 convention 이다. SOAP는 잠재적으로 다양한 다른 프로토콜과 결합하여 사용될 수 있다. 하지만, 이 문서에서는 정의된 바인딩만이 HTTP와 HTTP Extension Framework를 결합에서 SOAP를 어떻게 사용하는지에 대해서만 다루고 있다.	Simple Object Access Protocol. W3C
Transport of Real-time Inter-network Defense (RID) Messages	이 메커니즘은 TLS 상에서 전송되는 HTTP Request와 Response 메시지 내에서 RID (Real-time Inter-network Defense) 메시지의 전송을 명세한다.	IETF RFC 6046 Transport of Real-time Inter-network Defense (RID) Messages

3.3 공통 취약점 및 노출(X.1520)

MITRE의 CVE(Common Vulnerability and Exposure)로도 잘 알려져 있는 본 권고안은 네트워크, 종단 사용자 장치 등에서 사용되는 상업적인 혹은 오픈 소스 기반의 소프트웨어에서의 알려진 문제에 대한 공통 이름을 제공하는 것을 목적으로 하는 보안 취약점 및 노출 정보를 교환하는 구조화된 수단이다. CVE의 목표는 "공통 목록" 내에 독립된 취약점에 대한 데이터 공유를 쉽게 하기 위함이다. CVE는 취약점 데이터를 연결시켜 보안 도구 및 서비스의 비교를 가능하게 하도록 하기 위해 만들어졌다.

예를 들어 CVE는 위험, 영향, 해결 정보, 혹은 상세한 기술적인 정보는 포함되지 않는다. CVE는 오로지 상태 지표, 간단한 설명, 그리고 취약점 리포트와 경보와 관련된 참조만을 포함하고 있다.

본 권고안은 다음의 7가지 측면에서의 요구사항에 대해서 다루고 있다.

- 전제 조건 및 기능 등
- 정확성
- 문서화
- CVE 데이터 사용
- 기존 스타일의 CVE 식별자 지원
- CVE 호환성의 폐지
- 검토국

3.4 공통 취약점 스코어링 시스템(X.1521))

CVSS(Common Vulnerability Scoring System)는 공통 취약점 스코어링 시스템으로 네트워크, 종단 사용자 장치 등에서 사용되는 상업 혹은 오픈 소스 기반의 소프트웨어에서의 ICT 취약점에 대한 특징 및 영향에 대한 전달을 위한 오픈 프레임워크를 제공한다. CVSS는 ICT 취약점에 대한 스코어링을 통해 ICT 매니저, 취약점 뉴스 제공자, 보안 업체, 어플리케이션 업체, 연구원들이 공통된 언어로 취약점에 대해서 말할 수 있게 하는 데 그 목적이 있다.

CVSS는 세 가지 기준 그룹을 기반으로 점수를 책정한다. 즉, 기본 기준, 시간적 기준, 환경적 기준, 각각은 [그림 4]와 같이 기준들의 집합으로 구성된다.

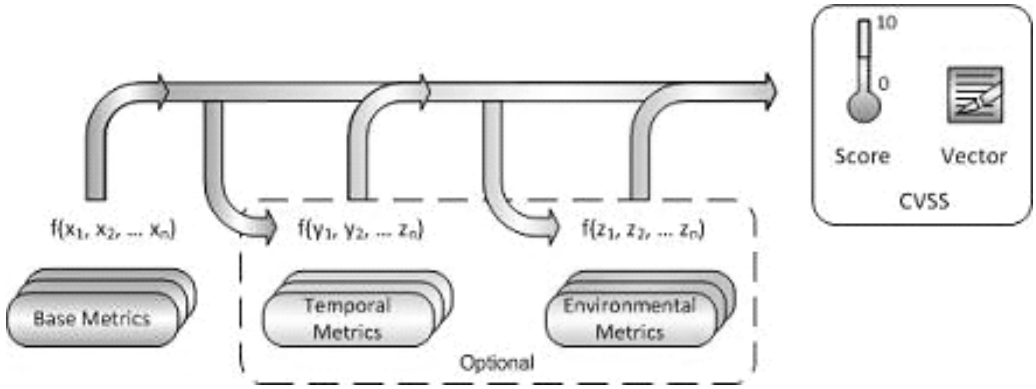
- 기본 기준: 시간의 경과와 사용자 환경에 의존하지 않는 취약점의 본질적이고 근본적인 취약점의 특징을 나타냄
- 시간적 기준: 사용자 환경이 아닌 시간이 지남에 따라 변하는 취약점의 특징을 나타냄
- 환경적 기준: 특정 사용자의 환경에서 고유한 취약점의 특징을 나타냄

기본 기준 값을 할당하면, 기본 방정식은 0에서 10까지의 점수를 계산하고, 그림 5와 같이 벡터가 생성된다. 벡터는 각 기준에 할당된 값을 포함하는 텍스트 문자열이며, 각각의 취약점에 대한 스코어가 어떻게 도출되는지 전달하기 위해 사용된다.

요청에 따라 기본 스코어는 시간적 그리고 환경적인 기준에 값을 할당함으로써 재정의될 수 있다. 이는 사용자의 환경에 의해 야기되는 위험을 더 정확하게 반영함으로써 취약점에 대한 추가적인 정보를 제공한다.

시간적인 스코어가 필요로 하는 경우, 시간적 방정식은 0부터 10까지의 시간적인 스코어를 만들기 위해 시간적 기준과 기본 스코어를 결합하고, 유사하게 환경적인 스코어가 필요로 하는 경우, 0부터 10까지의 환경적 스코어를 만들기 위해 환경적 기준과 시간적 기준과 결합할 것이다.

〔그림 4〕 CVSS 기준 그룹



〔그림 5〕 CVSS 기준 및 방정식

각 기준을 구성하는 구성요소는 아래와 같다.

- 기본 기준
  · 접근 벡터(Access Vector)
  · 접근 복잡성(Access Complexity)
  · 인증 (Authentication)
  · 기밀성 (Confidentiality Impact)
  · 무결성 (Integrity Impact)
  · 가용성 (Availability Impact)

- 시간적 기준
  · 공격가능성 (Exploitability)
  · 복구 수준 (Remediation Level)
  · 리포트 신뢰 수준 (Report Confidence)

- 환경적 기준
  · 2차 피해 가능성 (Collateral Damage Potential)
  · 타겟(취약 시스템) 분포 (Target Distribution)
  · 기밀성 요구사항 (Confidentiality Requirements)
  · 무결성 요구사항 (Integrity Requirements)
  · 가용성 요구사항 (Availability Requirements)

Ⅳ. 결 론

다양한 통신 기기 및 기술의 발전은 사이버공간의 질적 팽창을 가져오고 있지만, 이로 인한 사이버공간에서의 범죄는 날이 갈수록 심각해지고 그 양상 또한 세계화 되고 지능화 되는 등 대응이 어려워지고 있다. 더 이상 국지적인 예방 및 대응은 사이버범죄 소탕에 한계를 가진다고 할 수 있다.

이런 시점에서 사이버공간의 질적 팽창 및 성장을 위해서는 세계화되고 지능화되는 사이버범죄에 대한 국제적인 공조 대응 노력이 절실하게 필요하다.

이에 본 논문에서는 ITU-T SG17 Q.4 사이버보안 분야에 대한 국제표준화 동향을 주요 의제인 사이버보안 정보 교환 기술을 중심으로 살펴보았다. 본 논문에서 다뤄진 사이버보안 표준화 활동 등이 좋은 결실을 이뤄 효과적인 사이버범죄 대응에 기여해 안전하고 편리한 사이버공간이 조성되기를 기대해본다.

참고문헌

[1] ITU-T SG17 TD1420, "Report of Q.4/17"
[2] ITU-T SG17 TD1161 Rev.6, "Recommendation ITU-T X.1500 Cybersecurity information exchange techniques"
[3] ITU-T SG17 TD1162 Rev.2. "Draft New Rec. ITU-T X.1520, Common vulnerabilities and exposures for determination"
[4] ITU-T SG17 TD1177 Rev.2. "Draft New Rec. ITU-T X.1521, Common vulnerability scoring system for determination"
[5] ITU-T SG17 TD1482, "Tutorial Presentation on Application of CYBEX (Cybersecurity Information Exchange) techniques to future networks"
[6] ITU-T SG17 TD1404, "Recommendation Summaries Q.4/17"
[7] Recommendaton ITU-T X.1205, "Overview of

cybersecurity"
[8] Recommendaton ITU-T X.1206, "A vendor-neutral framework for automatic notification of security related information and dissemination of updates"
[9] Recommendation ITU-T X.1207, "Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software"
[10] Recommendation ITU-T X.1209, "Capabilities and their context scenarios for cybersecurity information sharing and exchange"
[11] Recommendation ITU-T X.1205 supplement 8, “Supplement on best practices against botnet threats"
[12] Tony Rutkowski, “Application of CYBEX techniques to future networks,” SG17 Tutorial.
[13] 김미주, “글로벌 사이버보안 정보교류 국제표준화 동향,” TTA ICT Standard Weekly 2009-46호.
[14] MITRE, Assessment Results Format.
[15] MITRE, Common Attack Pattern Enumeration and Classification
[16] MITRE, Common Configuration Enumeration
[17] MITRE, Common Event Expression
[18] MITRE, Common Platform Enumeration
[19] MITRE, Common Weakness Enumeration
[20] MITRE, Common Weakness Scoring System.
[21] Electronic Authentication Guideline, NIST Special Publication 800-63 Version 1.0.2, April 2006
[22] CA/Browser Forum, Guidelines for the Issuance and Management of Extended Validation Certificates, Ver. 1.3
[23] Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ETSI TS102042.
[24] IETF RFC 3080, The Blocks Extensible Exchange Protocol Core
[25] IETF RFC 5070, Incident Object Description Exchange Format
[26] IETF RFC 5901, Extensions to the IODEF-Document Class for Reporting Phishing
[27] IETF RFC 6046, Transport of Real-time Inter-network Defense (RID) Messages
[28] MITRE, Malware Attribute Enumeration and Characterization
[29] MITRE, Open Vulnerability and Assessment Language
[30] W3C, Simple Object Access Protocol
[31] Traffic Light Protocol. Information Sharing Levels, CPNI Information Exchange, UK CPNI (April 2010)
[32] Trusted Computing Group, Trusted Network Connect
[33] Trusted Computing Group, Trusted Platform Modules
[34] NIST, The eXtensible Configuration Checklist Description Format

〈著者紹介〉

김 미 주 (Kim Mijoo)
정회원
2006년 2월 : 순천향대학교 정보보호학과 졸업(학사)
2008년 2월 : 순천향대학교 정보보호학과 졸업(석사)
2008년 9월~현재 : 순천향대학교 정보보호학과 박사과정
2008년 4월~현재 : 한국인터넷진흥원 연구개발팀 주임연구원
관심분야 : 사이버보안, 스마트 그리드 보안, USN 보안, 스마트폰 보안

정 현 철 (Jung Hyun Chul)
정회원
1996년 2월 : 서울시립대학교 전산통계학과 졸업(학사)
1999년 8월 : 광운대학교 전자계산학과 졸업(석사)
2006년 9월~현재 : 고려대학교 정보보호대학원 박사과정
1996년 7월~현재 : 한국인터넷진흥원 연구개발팀 팀장
관심분야 : 침해사고대응, 융합서비스보안, 네트워크보안, 컴퓨터포렌식

염 흥 열 (Youm Heung Youl)
종신회원
1981년 2월 : 한양대학교 전자공학과 졸업(학사)
1983년 2월 : 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월 : 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 회장(현) 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장(역)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 : 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP2 의장
관심분야 : 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜