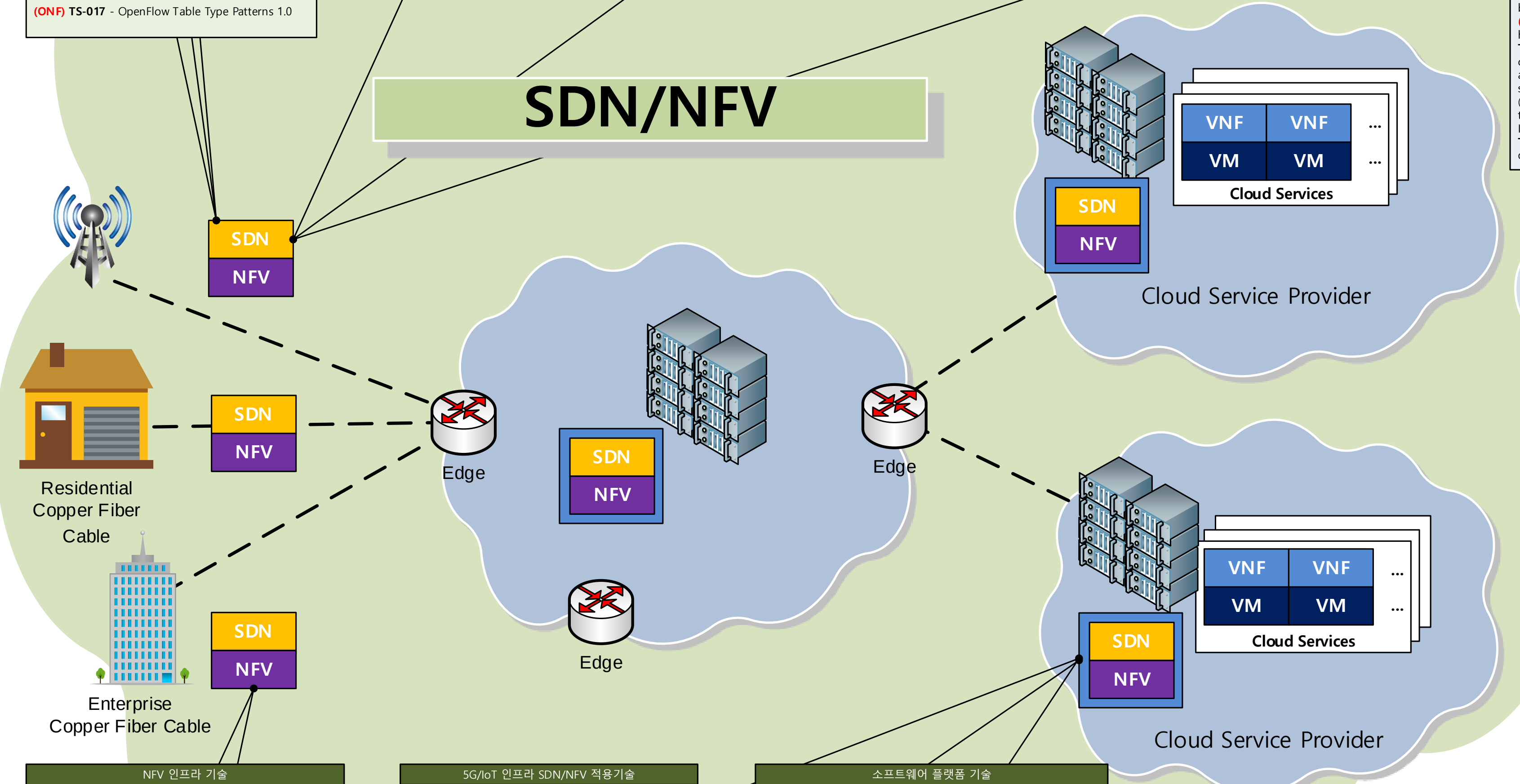
http://www.tta.or.kr

TTA - 16142 - SD

K-ICT 표준 활용·개발 맵 Ver.2017 – 네트워크/정보보호 분야 – 네트워크(SDN/NFV, 미래형창의네트워크, 광통신네트워크), 정보보호(공통기반 보안, 네트워크/디바이스 보안, 서비스/융합 보안)

SDN/NFV



SDN End-to-end 및 하이브리드 연동기술

(병행|적극공략) ~'19, ITU-T, IETF, ONF, 오픈소스

(IETF) **draft-ieft-teas-actn-framework** - Framework for Abstraction and Control of Traffic Engineered Networks

(ONF) **TR-522** - SDN Architecture for Transport Networks, **TR-524** - RFI Template Migration to SDN, **TR-527** - Functional Requirements for Transport API

SDN 응용 인터페이스 및 서비스 추상화 기술

(병행|다각화협력) ~'18, ITU-T, IETF, ONF

(ONF) **TR-517** - Real Time Media NBI REST Specification 1.0

(ITU-T) **Y.3320** - 소프트웨어 정의 네트워킹 정형 명세 검증 요구사항

SDN 데이터 전송 및 추상화 기술

(병행|다각화협력) ~'18, IETF, ONF

(ONF) **TS-017** - OpenFlow Table Type Patterns 1.0

SDN 제어 및 관리기술

(병행|적극공략) ~'17, ITU-T, IETF, ONF

(TTA) **TTAK.KO-01.0187** - 소프트웨어 정의 네트워킹(SDN) 제어기 기능 요구사항

(ONF) **TS-025** - OpenFlow® Switch Specification Ver 1.5.1, **TS-005** - OpenFlow Configuration and Management Protocol 1.1

(IETF) **RFC 5810** - Forwarding and Control Element Separation (ForCES) Protocol Specification, **6457** - PCC-PCE Communication and PCE Discovery Requirements for Inter-Layer Traffic Engineering, **7921** - An Architecture for the Interface to the Routing System, **7920** - Problem Statement for the Interface to the Routing System, **7920** - SPRING Problem Statement and Requirements, **Draft** - Routing Information Base Info Model

(ITU-T) **Y.3300** - Framework of software-defined networking, **3301**, Functional requirements of software-defined networking, **3302** - Functional architecture of software-defined networking, **Y.SDN-usecases** - 소프트웨어 정의 네트워킹 유즈 케이스, **Q.Sup67** - Framework of signalling for software-defined networking

NFV 구조 및 인터페이스 기술

(병행|적극공략) ~'17, ETSI

(ETSI) **GS NFV 001** - Network Functions Virtualisation (NFV); Use Cases, **002** - Network Functions Virtualisation (NFV); Architectural Framework, **003** - Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV, **004** - Network Functions Virtualisation (NFV); Virtualisation Requirements, **PER 002** - Network Functions Virtualisation (NFV); Proofs of Concept; Framework, **NFV-IFA007** - Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification, **NFV-IFA008** - Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification, **NFV-IFA010** - Management and Orchestration; Functional requirements specification, **NFV-IFA011** - VNF Packaging Specification, **NFV-IFA013** - Os-Ma-Nfvo ref point Spec - info model, **NFV-IFA014** - Network service template specification

NFV 관리 및 오케스트레이션 기술

(병행|적극공략) ~'17, ETSI, DMTF, IETF, 오픈소스

(ETSI) **GS NFV 001** - Network Functions Virtualisation (NFV); Use Cases, **002** - Network Functions Virtualisation (NFV); Architectural Framework,
GS NFV-PER 001 - Network Functions Virtualisation (NFV); NFV Performance & Portability Best Practises, **002** - Network Functions Virtualisation (NFV); Proofs of Concepts; Framework, **003** - Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV, **004** - Network Functions Virtualisation (NFV); Virtualisation Requirements,
NFV-IFA007 - Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification, **NFV-IFA008** - Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification, **NFV-IFA010** - Management and Orchestration; Functional requirements specification, **NFV-IFA011** - VNF Packaging Specification, **NFV-IFA013** - Os-Ma-Nfvo ref point Spec - info model, **NFV-IFA014** - Network service template specification
NFV-MAN 001 - Network Functions Virtualisation (NFV); Management and Orchestration, **NFV-SWA 001** - Network Functions Virtualisation (NFV); Virtual Network Functions Architecture, **NFV-INF 001** - Network Functions Virtualisation (NFV); Infrastructure Overview

(DMTF) **DSP0243** - Open Virtualization Format Specification, **DSP0265** - Profile to Enable Automated Deployment of OVF Packages

NFV 인프라 기술

(후행|방어적수용) ~'17, ETSI, 오픈소스

(ETSI) **IFA001** - Acceleration: Use cases report, **IFA002** - Acceleration: VNF Interface, **IFA003** - Acceleration: vSwitch, **IFA004** - Acceleration Management aspect

5G/IoT 인프라 SDN/NFV 적용기술

(선행|차세대공략) ~'20, 3GPP, ETSI, ONF, IETF, ITU-T

(ITU-T IMT-2020 FG) Draft deliverable of Network softwarization for IMT-2020 networks

소프트웨어 플랫폼 기술

(병행|적극공략) ~'18, IETF, 오픈소스(OPNFV, ODL, ONOS)

(TTA) **TTAK.KO-01.0189** - 분산 클라우드 관리 플랫폼 : 서비스 응용 프로그램 인터페이스, **0190** - 분산 클라우드 관리 플랫폼 : 자원 제어 인터페이스, **0200** – 네트워크 기능 가상화 프레임워크

(OPNFV) Open Platform for NFV: 개방형 NFV 플랫폼 오픈소스 프로젝트

(ODL) Open Daylight Platform: 이종 벤더 네트워크 SDN 응용 및 제어 인프라 플랫폼 오픈소스 커뮤니티

(ONOS) Open Network Operating System 글로벌 통신사들과 장비업체 주도의 오픈소스 SDN 제어 플랫폼

서비스 기능 가상화 및 체이닝 기술

(병행|적극공략) ~'18, IETF, ETSI

(IETF) **RFC 7498** - Problem Statement for Service Function Chaining, **7665** - Service Function Chaining (SFC) Architecture, **draft-ietf-sfc-dc-use-cases-03** - Service Function Chaining Use Cases In Data Centers, **draft-ietf-sfc-use-case-mobility-05** - Service Function Chaining Use Cases in Mobile Networks

(IRTF) **draft-irtf-nfvrg-nfv-policy-arch-02** - Policy Architecture and Framework for NFV Infrastructures, **draft-irtf-nfvrg-resource-management-service-chain-02** - Resource Management in Service Chaining, **draft-irtf-nfvrg-service-verification-00** - Verification of NFV Services : Problem Statement and Challenges

하드웨어 플랫폼기술

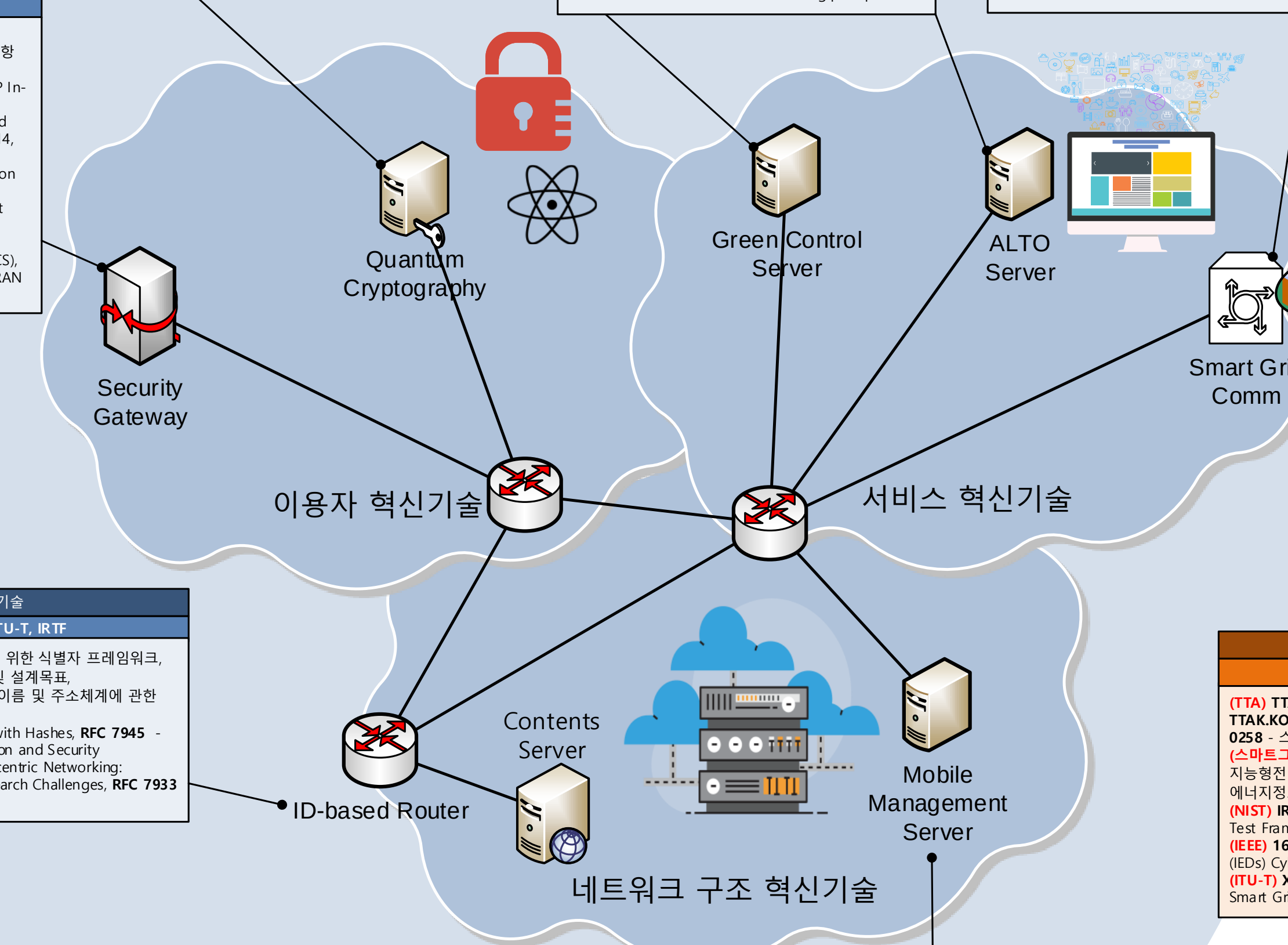
(병행|방어적수용) ~'16, ATCA, IPMI

(TTA) **TTAK.KO-01.0197** - 네트워크 하드웨어 공통 플랫폼 : 네트워크 기능보드 관리기능, **TTAK.KO-01.0198** - 네트워크 하드웨어 공통 플랫폼 : 네트워크 기능 보드 적합성 시험

(ATCA) ATCA/PICMG 3.0

(IPMI) Shelf Manangement

미래형창의네트워크



양자암호통신 기술

(병행|차세대공략) ~'18, IEEE, ETSI, JTC1

(국표원) **KS X ISO/IEC 19790** - 암호모듈 보안 요구사항, **KS X ISO/IEC 24759** - 암호모듈 시험 요구사항

(ETSI) **GS QKD 002** - Use cases, **003** - Components and internal interface, **004** - Application interface, **GS QKD 005** - Security proofs, **GS QKD 008** - QKD module security spec

(IETF) **IPSEC, X509-S/Mine** - Transport Layer Security(SSL)

(NIST) **DES**, computer authentification, secure hash standard, digital signature standard, AES

(ANSI) **X9.17** PIN management - check processing, electronic transfer of funds), **X.9.28** - Common master key, **X9.30** - US Financial Industry Standard based on DSA, **X9.31** - digital signature based on RSA, **X9.40** - Check Correction Strip Specification, **X9.41** - Security Services Management for the Financial Services Industry

에너지 절감 네트워킹 기술

(병행|차세대공략) ~'18, JTC1, IETF, IRTF, ITU-T

(TTA) **TTAE.IT-Y.3021** - 미래 네트워크를 위한 에너지 절감 네트워크 프레임워크

(IETF EMAN) **RFC 6988** - Requirements for Energy Management, **7326** - Energy Management Framework

분산서비스 네트워킹 기술

(병행|다각화협력) ~'17, ITU-T, IETF

(TTA) **TTAK.KO-12.0089** - P2P기반의 비디오 스트리밍 서비스를 위한 보안 요구사항, **TTAE.ITU-X.609** - 관리형 피어투피어 통신: 기능구조

(IETF) **RFC 6708** - Application-Layer Traffic Optimization (ALTO) Requirements, **7285** - ALTO Protocol, **6972** - Problem Statement and Requirements of the Peer-to-Peer Streaming Protocol (PPSP), **7574** - Peer-to-Peer Streaming Peer Protocol (PPSPP), **7846** - Peer-to-Peer Streaming Tracker Protocol (PPSTP)

(ITU-T) **X.609** - Managed P2P communications: Functional Architecture, **X.609.1** - Managed P2P communications: Peer Activity Management Protocol, **Y.2206** - Requirements for distributed service networking capabilities, **X.mp2p-orcp** - Managed P2P communications: Overlay Resource Management Protocol, **X.mp2p-mssr** - Managed P2P communications: Multimedia streaming service requirements, **X.mp2p-mspp** - Managed P2P communications: Multimedia streaming peer protocol

스마트그리드 통신 기술

(병행|차세대공략) ~'18, IEC, ITU-T, IEEE, OASIS

(TTA) **TTAR-04.0001** - 정보통신기술(ICT) 관점에서의 스마트그리드 참조모델(기술보고서), **06.0126** - M2M 기반 공공빌딩 및 시설물 에너지 관리 서비스 적용 사례 (기술보고서)
TTAK.KO-04.0151 - 스마트그리드 댁내 통신 규격 : RS485 통신 프로토콜, **0163** - 개방형 건물 에너지 관리 서비스 프레임워크 참조 모델,
0184~5 - 스마트 플러그 시스템/시험, **0190** - 스마트 유틸리티 네트워크(SUN) 영역 통신 인터페이스,
0200~1 – IP 기반 스마트 플러그 인터페이스/시험, **TTAK.OT-04.0004~6**, 스마트그리드 기술 용어/아키텍처/ 통신 요구사항

(ITU-T) **Y.2064** - energy saving using smart objects in next generation home network, **Y.2071** - Framework of Micro Energy Grid, **Y.energy-platform** - Framework of Energy Sharing and Trading Platform,

(ITU-T FG Smart) Smart Grid Terminology, Smart Grid Overview, Use Cases for Smart Grid, Requirements of communication for smart grid, Smart Grid Architecture

(IEC) **61970 Part 301** - Energy management system application program interface (EMS-API) –Part 301: Common information model (CIM) base (Edition 5.0), **TR 62939 Part 1** - Smart Grid User Interface – Part 1: Interface overview and country perspectives, **PAS 62746 Part 10-1** - Systems interface between customer energy management system and the power management system - Part 10-1: Open Automated Demand Response (OpenADR 2.0b Profile Specification) (Edition 1.0)

(IEEE) **2030** - Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads

(NIST) **1108R2** - NIST Framework and Roadmap for Smart Grid Interoperability Standards (Release 2.0)

신뢰 네트워킹 기술

(병행|차세대공략) ~'18, IETF, ITU-T

(TTA) **TTAI.KO-06.0390** - 재난안전무선통신망(PS-LTE) : 기능적 요구사항

(IETF) **RFC7024** - Virtual Hub-and-Spoke in BGP/MPLS VPNs, **RFC7246** –Multipoint LDP In-band Signaling in a VRF Table Context

(3GPP) **TR 36.837** - Public safety broadband high power User Equipment (UE) for band 14, **TS 34.121-1** - User Equipment (UE) conformance specification; Radio transmission and reception (FDD); Part 1: Conformance specification, **TS 34.121-2** - User Equipment (UE) conformance specification; Radio transmission and reception (FDD); Part 2: Implementation Conformance Statement (ICS), **TS 33.897** - Rel 13 Study on isolated E-UTRAN operation for public safety; Security aspects

ICN/ID기반통신 기술

(병행|적극공략) ~'18, ITU-T, IRTF

(TTA) **TTAE.IT-Y.3031** - 미래 네트워크를 위한 식별자 프레임워크, **TTAE.IT-Y.3001** - 미래 네트워크 : 원칙 및 설계목표, **TTAE.KO-01.0174** - 미래 인터넷을 위한 이름 및 주소체계에 관한 요구사항

(IRTF ICN) **RFC 6920** - Naming Things with Hashes, **RFC 7945** - Information-centric Networking: Evaluation and Security Considerations, **RFC7476** - Information-centric Networking: Baseline Scenarios, **RFC 7279** - ICN Research Challenges, **RFC 7933** - Adaptive Video Streaming over ICN

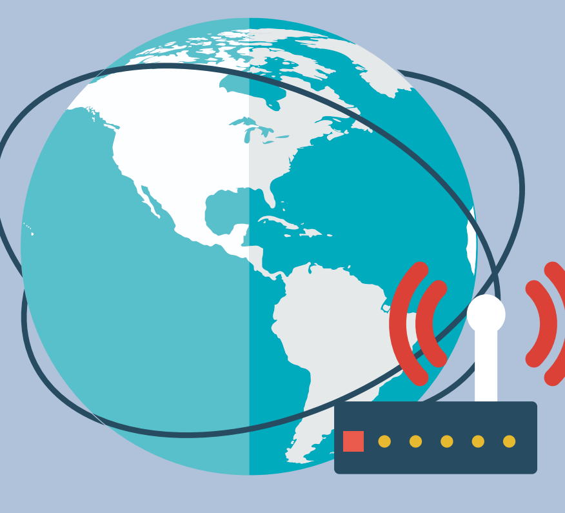
DTN/ID-Locator 분리 기술

(선행|다각화협력) ~'18, IETF, ISO, IRTF

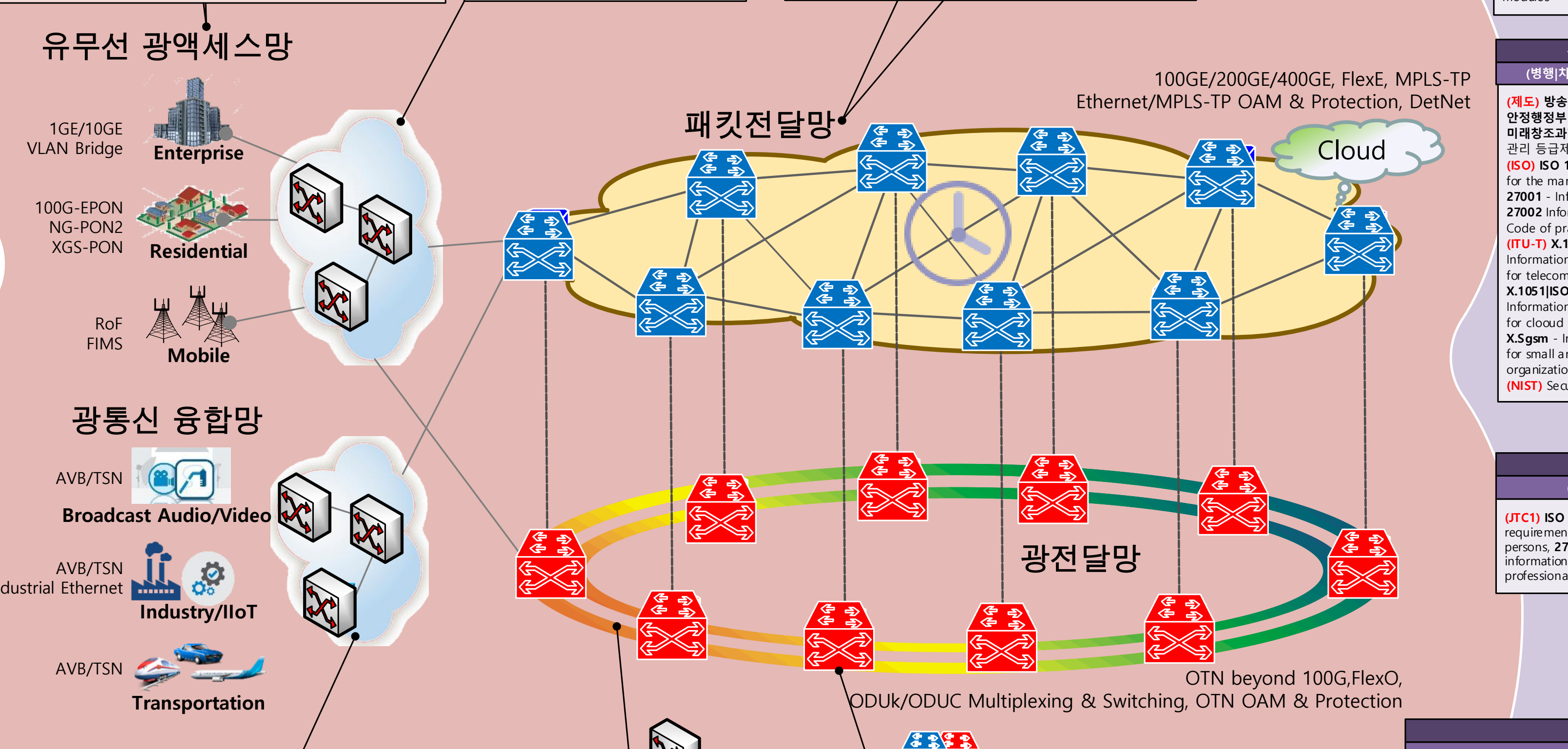
(TTA) **TTAE.IF-RFC4838** - DTN 구조, **5050** - DTN 번들 프로토콜 명세, **6830** - 위치자/식별자 분리 프로토콜(LISP)

(IRTF) **RFC 4838** - Delay-Tolerant Network Architecture, **5050** - Bundle Protocol Specification, **5326** - Licklider Transmission Protocol - Specification

(IETF) **RFC 6830** - Locator/ID Separation Protocol, **6831** - The Locator/ID Separation Protocol (LISP) for Multicast Environments



광통신네트워크



유무선 광액세스 망 / PON 기술

(병행|적극공략) ~'19, IEEE802, ITU-T, FSAN/BBF

(TTA) **TTAK.KO-01.0176** - 10 Gb/s REAM-SOA을 포함하는 XMD형 TOSA 패키지, **04.0198** - 기가 인터넷 제공을 위한 ITU-T 권고 G.996X 기반의 동선 전송기술, **TTAE.IE-802.3bk-2013** - IEEE 802.3 이더넷 표준- 개정1:확장된 이더넷 수동 광가입자망을 위한 물리계층 및 관리 파라미터, **TTAE.IT-L.64** - 인프라스트럭처와 네트워크 장비 관리를 위한 ID 태그 요구사항, **G.698.3** - 단일채널 접속규격을 가진 다중채널 Seeded DWDM 전송, **G.987.1** - 10 기가비트 수동형 광 통신망(XG-PON): 일반적 요구사항, **G.988** - ONU 관리 및 제어 인터페이스 (OMCI) 규격, **G.989.1** - 40기가급 수동형 광통신망 (NG-PON2): 일반 요구사항,

(ITU-T) **G.698.3** - Multichannel seeded DWDM applications with single-channel optical interfaces, **G.987** - 10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations and acronyms,

(IEEE) **802.3bk** - Extended EPON

유무선 광액세스 망 / 유무선광링크 기술

(병행|적극공략) ~'18, ITU-T, IEC, FSAN

(TTA) **TTAE.IT-G.698.3** - 단일채널 접속규격을 가진 다중채널 Seeded DWDM 전송,

(ITU-T) **G.698.3** - Multichannel seeded DWDM applications with single-channel optical interfaces, **CPRI7.0** –최대 25Gb/s급의 전송속도를 수용하는 CPRI 7.0, **G.Sup.55** –Radio over Fiber technologies and its applications, **G.RoF** – Radio over Fiber systems

(IEC) **IEC 62149-10** - RoF transceiver for mobile front haul

광통신네트워크제어 / SDN기술

(병행|적극공략) ~'18, ITU-T/ONF, IETF, BBF

(TTA) **TTAK.KO- 01.0095** –전달망 소프트웨어 정의 네트워킹을 위한 기본 YANG 데이터 모델

(ITU-T) **G.cca** - Common control aspects, **G.asdtn** - Architecture for SDN control of Transport Networks

(ONF) **TR-504** – SDN architecture, TR-512 – Information modeling

(IETF) **draft-ceccarelli-actn-framework-07** - Framework for Abstraction and Control of Transport Networks

(BBF) **WT-358** - Requirements for Support of SDN in Access Nodes

패킷전달망 / MPLS-TP기술

(병행|적극공략) ~'17, IETF, ITU-T

(TTA) **TTAE.IT-G.8110.1/Y.1370.1/R1** - MPLS-TP 계층 망의 구조, **G.8113.1/Y.1372.1** - 패킷전달망에서 MPLS-TP 운영, 관리, 유지 방법,

(ITU-T) **G.8113.1/Y.1372.1** - Operations, administration and maintenance mechanism for MPLS-TP in packet transport networks

(IETF) **RFC 7167** – A Framework for Point-to-Multipoint MPLS in Transport Networks

패킷전달망 / Ethernet 기술

(후행|방어적수용) ~'17, IEEE802. ITU-T

(TTA) **TTAK.KO-03.0021** - 캐리어 이더넷 연동 게이트웨이 참조모델

(IEEE) **802.1BR-2012** - IEEE Standard for Local and Metropolitan Area Networks- Virtual Bridged Local Area Networks- Bridge Port Extension

(ITU-T) **G.8031** - Ethernet Linear Protection switching, **G.8032** - Ethernet Ring Protection Switching, **G.8013/Y.1731** - OAM functions and mechanisms for Ethernet based networks

광통신융합 / TCN 기술

(병행|차세대공략) ~'19, IEEE, IETF

(TTA) **TTAE.IE-802.1as** - 브리지 LAN에서 시간 민감성 애플리케이션을 위한 동기화, **1588** - 네트워크로 연결된 계측 및 제어 시스템용 정밀 클럭 동기화 프로토콜, **TTAE.IT-G.8262/Y.1362**- 동기식 이더넷 장비의 슬레이브 클럭의 타이밍 특성, **G.8260** - 패킷 네트워크 동기화에 대한 정의 및 용어

(IEEE) **802.1Qav-2009** - Virtual Bridged Local Area Networks- Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams, **802.1Qat-2010** - Virtual Bridged Local Area Networks Amendment 14: Stream Reservation Protocol (SRP), **802.1BA-2011** - Audio Video Bridging (AVB) Systems, **802.1AS-2011** - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks, **1722-2011** - IEEE Standard for Layer 2 Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks, **1723-2011** - IEEE Standard for Layer 2 Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks, **1733-1** - IEEE Standard for Device Discovery, Connection Management, and Control Protocol for IEEE 1722™Based Devices, **802.3bw-2015** - IEEE Standard for Ethernet- Amendment 1: Physical Layer Specifications and Management Parameters for 100 Mb/s Operation over a Single Balanced Twisted Pair Cable (100BASE-T1), **802.1Qbv-2015** - Bridges and Bridged Networks- Amendment 25: Enhancements for Scheduled Traffic, **820.1Qca** - Bridges and Bridged Networks- Amendment 24: Path Control and Reservation

(IETF) **draft-ietf-detnet-use-cases-09** - Deterministic Networking Use Cases, **draft-ietf-detnet-problem-statement-00** - Deterministic Networking Problem Statement, **draft-dt-detnet-dp-alt-00** - DetNet Data Plane Protocol and Solution Alternatives

광전달망 / OTN기술

(병행|방어적수용) ~'17, ITU-T, IEEE802.3

(TTA) **TTAE.IT-G.709/R2** - 광전송 네트워크 신호 인터페이스, G.709 (2012) Amd.4-Interface for the optical transport network Amendment 4, **G.7044** - ODUflex(GFP) 대역폭 제어

(ITU-T) **G.709 (2012)** - Interface for the optical transport network, **G.709 (2012) Amd.4** - Interface for the optical transport network Amendment 4, **G.7041** - Generic framing procedure (GFP), **G.7041 Amd.1** - Generic framing procedure Amendment 2, **G.7044** - Hitless adjustment of ODUflex(GFP), **G.7044 (2011) Amd.1** - Hitless adjustment of ODUflex(GFP): Amendment 1, **G.798** - Characteristics of optical transport network hierarchy equipment functional blocks, **G.798 Amd.2** -Characteristics of optical transport network hierarchy equipment functional blocks Amendment 2, **G.798.1** - Types and Characteristics of optical transport network equipment, **G.798.1 Amd.1** - Types and Characteristics of optical transport network equipment Amendment 1, **G.798 Amd.2** -Characteristics of optical transport network hierarchy equipment functional blocks Amendment 2, **G.872 (2012)** - Architecture of optical transport networks, **G.872 (2013) Amd.1** - Architecture of optical transport networks: Amendment 1, **G.873.1(2011)** - Optical transport network (OTN): Linear protection, **G.873.1 Amd.1(2011)** - Optical transport network (OTN): Linear protection Amendment 1, **G.873.1** - Optical transport network (OTN): Linear protection, **G.873.2** - ODUk shared ring protection, **G.8021** - Types and characteristics of Ethernet transport network equipment, **G.odusmp** - ODU Shared Mesh Protection

광전달망 / 광전송기술

(병행|다각화협력) ~'18, ITU-T, IEC

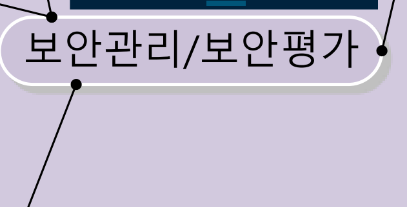
(TTA) **TTAE.KO-03.0022** - 다수의 서브 채널을 갖는 다채널 CWDM 광인터페이스

(ITU-T) **G.694.1** - Spectral Grids for WDM Applications: DWDM Frequency Grid, **G.698.3** - Multichannel seeded DWDM applications with single-channel optical interfaces, **G.959.1** - Optical transport networks physical layer interfaces, **G.metro** - Multichannel bi-directional DWDM applications with port agnostic single-channel optical interfaces

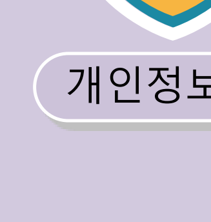
(OIF) **OIF-DPC-RX-01.2** - Implementation Agreement for Integrated Dual Polarization Intradyne Coherent Receivers, **OIF-MSA-100GLH-EM-02.0** - Multisource Agreement for Generation 2.0 100G Long-Haul DWDM Transmission Module - Electromechanical, **OIF-PMQ-TX-01.1** - Implementation Agreement for Integrated Polarization Multiplexed Quadrature Modulated Transmitters

(IEC) **62150-5/Ed.1.0** - Fibre optic active components and devices 0 Test and measurement procedures - Part5: wavelength channel tuning time of tuneable transmitter, **61753-381-2/Ed.1.0** - Fibre optic interconnecting devices and passive components 0 Performance standard 0 Part 381-2: Cyclic arrayed waveguide grating for category C - Controlled environment:

공통기반 보안



보안관리/보안평가



개인정보보호

암호기술

인증기술

유형별 보안성 시험평가기준

(후행|방어적수용) ~'17, JTC1 SC27, CCRA, CCUF

(KS) **KS X ISO/IEC 15408-1~3** - 정보기술보안 평가기준, **18045** - 정보 기술 보안 평가 방법론, **19790** - 정보 기술 - 보안 기술 - 암호모듈 보안 요구사항, **24759** - 정보 기술 - 보안 기술 - 암호모듈 시험 요구사항

(CCRA) Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 4

(NIST) **FIPS 140-2** - Security Requirements for Cryptographic Modules

(JTC1) **17825** - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

분야별 정보보호 관리체계 및 인증

(병행|차세대공략) ~'19, JTC1 SC27, ITU-T SG17

(제도) **방송통신위원회** 정보보호관리체계, **안정행정부** 개인정보보호인증제, **미래창조과학부** - 정보보호 준비도평가 제도, 정보보호 관리 등급제, 정보보호산업의 진흥에 관한 법률

(ISO) **ISO 13335** - Information technology - Guidelines for the management of IT Security **27001** - Information security management, **27002** Information technology - Security techniques - Code of practice for information security management

(ITU-T) **X.1051|ISO/IEC 27011** - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organization, **X.1051|ISO/IEC 27017** - Code of practice for Information security controls based on ISO/IEC 27002 for cloud services, **X.Sgsm** - Information security management guidelines for small and medium-sized telecommunication organizations

(NIST) Security Self assurance Guide for IT system

정보보호 감사관리 지침

(병행|차세대공략) ~'19, JTC1 SC27, ITU-T SG17

(TTA) **TTAS.KO-12.0036** - 정보보호관리체계 수립 지침

(제도) **방송통신위원회** - 정보보호관리체계, **안정행정부** – 개인정보보호인증제, **금융위원회** – 전자금융거래감독규정

(ISO) **ISO/IEC 13335** - Information technology - Guidelines for the management of IT Security, **17799** - Code of practice for information security management, **27001** - Information security management, **27002** - Information technology - Security techniques - Code of practice for information security management, **27007** - Guidelines for information security management systems auditing (focused on the management system), **27008** - Guidance for auditors on ISMS controls (focused on the information security controls)

(ISACA) COBIT(Control Objectives for Information and related Technology)

(NSA) SSE-CMM(System Security Engineering capability maturity Model)

(KPMG) VAF(Vulnerability Assessment Framework)

(카네기멜론) OCTAVE(Operationally Critical Threat, Asset, and Vulnerability Evaluation)

(NIST) Security Self assurance Guide for IT system

개인정보보호 정책 및 운영관리 기술

(병행|다각화협력) ~'18, ITU-T SG17, JTC1 SC27, W3C

(TTA) **TTAS.KO-12.0051** - 개인정보보호정책 설정 및 협상 규격, **0054/R1** - i-PIN 서비스 프레임워크,0053 - 개인정보 생명주기별 보안 관리 모델, **0105** - 개인정보보호를 위한 DB 보안감사 로그, **0159** - 얼굴 영역 검출을 이용한 CCTV 영상 정보 프라이버시 보호를 위한 보안 요구 사항, **0200** - 개인 정보 관리를 위한 프라이버시 보호 원칙, 0233 - 스마트폰 단말기에서 모바일뱅킹을 위한 개인정보보호 지침
TTAR-06.0013 - RFID 프라이버시 보호 가이드라인, **TTAE.OT-12.0015** - 공공 클라우드 컴퓨팅의 보안 및 프라이버시 보호 지침, **10.0336** - 모바일 웹 애플리케이션을 위한 단말 API 정책 및 개인 정보 보호 요구 사항, **10.0616** - 퍼스널 클라우드 개인정보보호 참조모델

(JTC1) **29134** - Privacy impact assessment - Guidelines, **29151** - Code of practice for personally identifiable information protection, **29190** - Privacy Capability Assessment Model

(W3C) P3P(Platform for Privacy Preferences) 1.1

(OASIS) XACML(eXtensible Access Control Markup Language) 2.0

(Liberty Alliance) ID-WSF Interaction Service 2.0

정보보호 경영 전문가 자격 기준

(병행|적극공략) ~'16, JTC1 SC27

(JTC1) **ISO 17024** - Conformity assessment -- General requirements for bodies operating certification of persons, **27021** - Competence requirements for information security management systems professionals

차세대 암호 및 적용

(후행|차세대공략) ~'19, IETF, JTC1 SC17

(TTA) **TTAK.KO-12.0001/R4** - 부가형 전자서명 방식 표준 - 제2부: 한국형 인증서 기반 전자서명 알고리즘(KCDSA), **0015/R3** - 부가형 전자서명 방식 표준 - 제3부: 타원곡선을 이용한 한국형 인증서 기반 전자서명 알고리즘(EC-KCDSA), **0174** - IPsec에서의 ARIA 암호 알고리즘 운영 방법, **0189/R1** - 결정론적 난수발생기 –1부- 블록암호 기반 난수발생기, **0223** - 128 비트 블록 암호 LEA, **0228** - CMS를 위한 추가암호 알고리즘 : Part3 ARIA, **0040/R1** - 64비트 블록암호 HIGHT, **0201/0202** - MIKEY/DTLS-SRTP에서 ARIA 알고리즘 사용을 위한 파라미터 정의, **0241** - ARIA/SEED 암호알고리즘을 이용한 키 유도함수, **0246** - 128비트 블록 암호 LEA 운영 모드, **0272/0273/0274** - 블록암호/HMAC/패스워드 기반 키 유도 함수, **0275** - 형태 보존 암호 FEA, **0276** - 해시 함수 LSH, **TTAI.OT-12.0011/0012** - SRTP/MIKEY에서 SEED알고리즘 운영방법, **TTAS.IF-RFC3565** - CMS를 위한 추가암호 알고리즘 : Part2 AES, **4010** - CMS를 위한 추가암호 알고리즘 : Part1 SEED, **4162** - TLS를 위한 SEED 암호알고리즘, **4196** - IPsec을 위한 SEED 암호알고리즘, **5669** - SRTP에서 SEED 알고리즘 운영 방법, **5748** - MIKEY에서 SEED 알고리즘 사용을 위한 파라미터 정의, **6188** - SRTP에서의 AES-192/256 운영 방법,

(RRA) **KCS.KO-12.2000/2001** - TLS·RTP·IKEY에서 블록 암호 SEED/ARIA 활용 방법, **TTAE.IF-RFC5763** - SRTP에서 DTLS 활용을 위한 프레임워크, **RFC5996** - 인터넷 키 교환(IKEv2) 프로토콜

(NIST) **FIPS 180-4** - Secure Hash Standard (SHS), **FIPS 202** - SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, **SP 800-38G** - Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption, **SP 800-56C** - Recommendation for Key Derivation through Extraction-then-Expansion, **SP 800-90A, Rev.1** - Recommendation for Random Number Generation Using Deterministic Random Bit Generators, **SP 800-108** - Recommendation for Key Derivation Using Pseudorandom Functions, **SP 800-132** - Recommendation for Password-Based Key Derivation Part 1: Storage Applications, **SP 800-135, Rev. 1** - Recommendation for Existing Application-Specific Key Derivation Functions

(JTC1) **9797** - Message Authentication Codes (MACs), **10116** - Modes of operation for an n-bit block cipher, **10118-3** - Hash-functions, **14888** - Digital signatures with appendix, **18031** - Random bit generation, **18033** - Encryption algorithms, **19772** - Authenticated encryption, **29150** - Signcryption, **29192-1~5** - Lightweight cryptography

(IETF) **RFC 5669** The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP), **5930** - Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol, **5932** - Camellia Cipher Suites for TLS, **6188** - The Use of AES-192 and AES-256 in Secure RTP, **6209** - Addition of the ARIA Cipher Suites to Transport Layer Security, **7251** - AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS, **7253** - The OCB Authenticated-Encryption Algorithm, 7539, ChaCha20 and Poly1305 for IETF Protocols, **7634** - ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and Ipsec, **7693** - The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC), **7714** - AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)

모바일 결제·인증 기술

(병행|다각화협력) ~'19, ITU-T SG17, JTC1 SC27/ISO TC68

(국가기술표준원) **KS X 6928-1** - 모바일 카드, **6928-2** - 대면 거래, **6928-3** - 비대면 거래

(TTA) **TTAK.KO-12.0144** - 차세대 모바일 카드 요구 사항 및 시스템 구성, **0197** - 모바일 전자 영수증 규격, **0198** - IC 칩 기반 모바일 결제 보안 요구 사항, 0199, 비IC 칩 기반 모바일 결제 보안 요구 사항, **0217** - POS 단말기 사용자 인터페이스, **0224** - NFC P2P 기반 모바일 전자 영수증 관리 규격, **0227** - POS 단말기 결제 모듈 인터페이스, **0240** - 모바일 후불 교통카드, **0250** - 대면거래에서의 전자서명 규격, **0251** - 거래번호를 이용한 모바일 결제, **0252** - 모바일 결제를 위한 어플리케이션 보안 지침, **0269-Part1~3** - 모바일 지불결제 상호운용성 시험표준

(JTC1) **14443-1~4** - Identification cards - Contactless integrated circuit cards - Proximity cards, **18092** - Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1), **21481** - Information technology - Telecommunications and information exchange between systems - Near Field Communication Interface and Protocol -2 (NFCIP-2)

PKI 기반 인증 및 응용기술

(후행|다각화협력) ~'19, ITU-T SG17, JTC1 SC27, FIDO Alliance

(TTA) **TTAK.KO-12.0001/R3** - 부가형 전자서명 방식 표준 - 제2부: 한국형 인증서 기반 전자서명 알고리즘(KCDSA), **0015/R2** - 부가형 전자서명 방식 표준 - 제3부: 타원곡선을 이용한 한국형 인증서 기반 전자서명 알고리즘(EC-KCDSA), **0054/R1** - i-PIN 서비스 프레임워크, **TTAK.KO-12.0250** - 대면거래에서의 전자서명 규격, **TTAK.KO-12.0259** - HTML5 로컬 스토리지에 저장되는 데이터의 암복호화 프레임워크

(IETF) **RFC 6664** - S/MIME Capabilities for Public Key Definitions, **RFC 6712** - Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP) , **RFC 6818** - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, **RFC 6844** - DNS Certification Authority Authorization (CAA) Resource Record, **RFC 6960** - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, **RFC 7030** - Enrollment over Secure Transport

(JTC1) **18014-1** - Time stamping services and protocols - Part 1 : Framework, **18014-4** - Time-stamping services - Part 4: Traceability of time sources, **9594-1** - The Directory - Part 1: Overview of concepts, models and services, **9594-8** - The Directory - Part 8: Public-key and attribute certificate frameworks

범용 인증 기술

(병행|적극공략) ~'19, JTC1 SC27, ITU-T SG17, FIDO/W3C

(TTA) **TTAK.KO-12.0128** - 일회용 패스워드(OTP) 통합인증 서비스 프레임워크, **0168** - 일회용 패스워드(OTP) 기반 통합인증 서비스 관리 프로토콜, **0192** - IC칩 기반 보안 매체를 활용한 통합형 사용자 인증 서비스 프레임워크, **0194** - 통합인증 기반 부인방지 서비스 프레임워크, **0218/R1** - 일회용 패스워드(OTP) 통합인증 서비스 프레임워크(개정), **0219** - IC칩 기반 인증 모듈 보안 요구 사항, 0221, 모바일 기기를 이용한 다중 요소 인증 메커니즘, **0244** - 전자거래 단계별 위험수준에 대한 인증서비스 지침, **0245** - 신뢰기관을 이용한 통합인증서비스 보안 요구사항, **0247** - 전자거래 보증 수준별 인증방법 요구사항, 0248, 국내 환경에 적합한 실체 인증 보증 프레임워크, **0270-Part1** - 패스워드와 IBC(ID 기반 암호시스템)를 이용한 키 교환 프로토콜-제1부 ID 기반 암호 이용, **0270-Part2** - 패스워드와 IBC(ID 기반 암호시스템)를 이용한 키 교환 프로토콜 - 제2부 ID 기반 서명 이용, **0274** - 패스워드 기반 키 유도 함수, **0038/R2** - i-PIN 서비스 중복 가입 확인 정보, **0250** - 대면거래에서의 전자서명 규격,
TTAE.OT-12.0017-Part1~11 - FIDO 유니버셜 인증 프레임워크(UAF)

(RRA) **KCS.KO-05.0047** - 모바일 터치 서비스 애플릿 규격, **0048** - 모바일 터치 서비스 동글 인터페이스 규격,

(JTC1) **29115** - Information technology - Security techniques - Entity authentication assurance framework

(ITU-T) **X.1158** - Multi-factor authentication mechanisms using a mobile device, **X.1159** - Delegated non-repudiation architecture based on X.813

(EMV) **EMV 1.1** - PayPass - ISO/IEC 14443, Implementation Specification, **EMV 2.6** - Book D: Contactless Communication Protocol, **EMV 4.3** - Book1 - Application Independent ICC to Terminal Interface Requirements / Book2 - Security and Key Management / Book3 - Application Specification / Book4 - Cardholder, Attendant, and Acquirer Interface Requirements

(FIDO) FIDO Universal Authentication Framework

(W3C) Web Authentication: A Web API for accessing scoped credentials

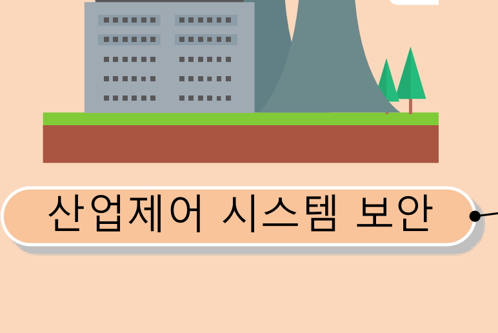
(OASIS) Extensible Resource Identifier(XRI) Syntax V2.0

서비스/융합 보안

웹 보안

클라우드/빅데이터 보안

자동차 융합 보안



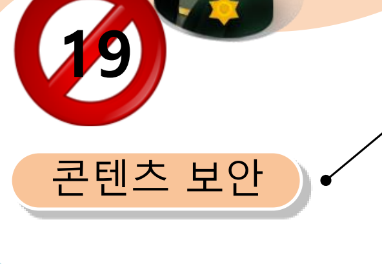
산업제어 시스템 보안

스마트그리드 보안

휴먼/바이오인식

금융 보안

헬스케어 보안



콘텐츠 보안

웹 매쉬업 보안

(병행|차세대공략) ~'18, ITU-T SG17, IETF, W3C

(TTA) **TTAK.KO-12.0184** - 웹 서비스 융합 정보보호 요구사항, **0210** - 웹 오픈 API(Application Programming Interface) 보안 요구사항, **0211** - 웹 신디케이션(Syndication) 보안 요구사항, **0234** - 웹 메쉬업 정보보호 지침, **0259** - HTML5 로컬 스토리지에 저장되는 데이터의 암복호화 프레임워크 **TTAE.IF-RFC5849** - 공개 인증 1.0 프로토콜, **RFC6749** - 공개 인증 2.0 권한관리 프레임워크

(ITU-T) **X.1141**- Security Assertion Markup Language (SAML 2.0), **X.1142** - eXtensible Access Control Markup Language (XACML 2.0), **X.1143** - Security architecture for message security in mobile web services, **X.1144** - eXtensible Access Control Markup Language (XACML) 3.0, **X.1211** - Guideline on techniques for preventing web-based attacksX.websec-5 Security architecture and operations for web mashup services, **X.supp.17** - Threats and security objectives for enhanced web-based telecommunication service, **X.websec-5** - Security architecture and operations for web mashup services

(W3C) CORS(Cross-Origin Resource Sharing)

스마트그리드 보안 기능 구조

(병행|적극공략) ~'17, ITU-T SG17, NIST, ISO/IEC

(TTA) **TTAK.KO-12.0182** - 스마트 그리드 보안 요구 사항, **0209** - 스마트 그리드 시스템 보안 기능 요구사항, **0257** - 스마트그리드에서의 전기차 충전 서비스를 위한 보안 기능 구조

(스마트그리드 표준화 포럼) 스마트그리드 표준의 사이버 보안성 확보를 위한 보안가이드라인

(NIST) **IR 7628** - Guidelines for Smart Grid Cyber Security

(IEC) **62351-10** - Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines

(ITU-T) **X.sgsec-1** - Security Functional Architecture for Smart Grid Services using Telecommunication Network

스마트그리드 보안관리

(병행|차세대공략) ~'18, ITU-T SG17, NIST, ISO/IEC

(TTA) **TTAK.KO-12.0182** - 스마트 그리드 보안 요구 사항, **0209** - 스마트 그리드 시스템 보안 기능 요구사항, **0257** - 스마트그리드에서의 전기차 충전 서비스를 위한 보안 기능 구조

(스마트그리드 표준화 포럼) 스마트그리드 표준의 사이버 보안성 확보를 위한 보안가이드라인

(NIST) **IR 7628** - Guidelines for Smart Grid Cyber Security

(IEC) **62351-10** - Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines

(ITU-T) **X.sgsec-1** - Security Functional Architecture for Smart Grid Services using Telecommunication Network

스마트그리드 기기 보안

(병행|차세대공략) ~'18, ITU-T SG17, NIST, ISO/IEC

(TTA) **TTAK.KO-04.0151** - 스마트그리드 댁내 통신 규격 : RS485 통신 프로토콜, **TTAK.KO-12.0287** - 스마트그리드 댁내 기기 보안 지침, **0258** - 스마트그리드 적용을 위한 HAN 기기 보안 메커니즘

(스마트그리드표준화포럼) **KSC1231-1** - 지능형전력량계 - 제1부: 기능요구사항, 지능형전력량계 - 제2부: 통신 및 보안 기능, 에너지정보 디스플레이 - 제2부: 보안 일반요구사항

(NIST) **IR 7823** - Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework(draft)

(IEEE) **1686-2007** - IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

(ITU-T) **X.sgsec-2** - Security guidelines for Home Area Network (HAN) devices in Smart Grid system

생체신호기반 텔레바이오 인식기술

(병행|차세대공략) ~'18, ITU-T SG17, ABC

(ITU-T) **X.tab** - Telebiometric authentification for bio-signals

바이오인식 응용 서비스

(병행|다각화협력) ~'18, JTC1 SC27, ITU-T SG17, ABC

(TTA) **TTAI.IT-X.bhsm** - 바이오인식 보안토큰을 이용한 텔레바이오인식 인증 프레임워크, **TTAK.KO-12.0266** - 홍채인식 성능평가 상호인정 기준, **0267** - 지문인식 성능평가 상호인정 지침, **0268** - 웹기반 BioAPI 표준적합성 시험 상호인정 지침

(ITU-T) **17922(X.bhsm)** - Telebiometric authentication framework using biometric hardware security module

(JTC1) **PDTR-30125** - Use of Mobile Biometrics for Personalization and Authentication, **WD1 30136-1** - Object oriented BioAPI –art 1: Architecture-Amendment 1: Additional specifications and conformance statements, **CD1-24709-1Rev1** - Conformance Test for BioAPI Part1 revision17922(X.bhsm): Telebiometric authentication framework using biometric hardware security module **17922(X.bhsm)** - Telebiometric authentication framework using biometric hardware security module

바이오인식 기반 CCTV 보안기술

(병행|적극공략) ~'18, JTC1 SC37, ITU-T SG17, ABC

(TTA) **TTAK.KO-12.0159** - 얼굴 영역 검출을 이용한 CCTV 영상 정보 프라이버시 보호를 위한 보안 요구 사항, **0216** - 영상감시 시스템에서의 개인 영상 정보보호 지침, **0207** - 네트워크 영상 감시 시스템에서 증거 영상 수집을 위한 지침, **0117/R2** - 영상 보안 시스템들 간의 상호 연동을 위한 인터페이스[개정] **0291** - 지능형 CCTV의 성능 평가용 주석 데이터 교환 포맷

(JTC1) **30137-1** – Use of biometrics in CCTV systems Part1 Design and specification, **30137-2** – Use of biometrics in CCTV systems Part2 Performance testing & reporting

V2X 통신 보안 프레임워크

(병행|차세대공략) ~'17, ITU-T SG16/SG17, ISO, IEEE

(TTA) **TTAK.KO-12.0208** - 차량 간 통신 보안 요구 사항, **0238** - 차량 간 통신 인증 서비스 구조, **0260** - 차량간 통신환경에서의 메시지 암호화 규격, **0286** - 자동차 전자제어장치 간의 통신보안요구사항, **0290** - 차량의 군집주행서비스 보안요구사항

(IEEE) **1609.2-2013** - Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages

(ITU-T) **X.itssec-2** - Security guidelines for V2X communication systems

금융거래 이상 징후 방지

(병행|다각화협력) ~'17, ITU-T SG17, ISO TC68

(TTA) **TTAK.KO-12.0178** - 이상 금융 거래 탐지 및 대응 프레임워크

(ITU-T) **X.1157** - Technical capabilities of fraud detection and response for services with high assurance level requirements

핀테크 서비스 보안 기술

(병행|다각화협력) ~'19, W3C Blockchain CG

(ISO) **20022** - universal financial industry message scheme

(W3C) Blockchain usecases

신뢰 클라우드 연동 보안

(선행|차세대공략) ~'19, ITU-T SG13, CSA, JTC1

클라우드 컴퓨팅 서비스에서의 개인정보 국외교환 프레임워크

(병행|다각화협력) ~'18, ITU-T SG13/17, JTC1 SC27, CSA

클라우드 컴퓨팅 서비스 보안 요구사항

(병행|방어적수용) ~'18, ITU-T SG17, JTC1 SC27, CSA

(TTA) **TTAE.IT-X.1601** - 클라우드 컴퓨팅을 위한 보안 프레임워크

(JTC1) **ISO/IEC 27017** - Information security management for cloud systems

클라우드 인증 및 접근제어 보안 프레임워크

(병행|적극공략) ~'18, ITU-T SG13/17, JTC1 SC27, CSA, DMTF

(TTA) **TTAK.KO-10.0615** - 퍼스널 클라우드 접근제어, **TTAE.OT-12.0015** - 공공 클라우드 컴퓨팅의 보안 및 프라이버시 보호 지침

(ITU-T) **X.1601** - Security framework for cloud computing

(JTC1) **ISO/IEC 27036-4** - Guidelines for Security of Cloud Services

내용기반 빅데이터 접근제어

(병행|차세대공략) ~'19, ITU-T SG17, JTC1 SC27, ODCA, CSA, NIST

(RRL) 빅데이터 산업 및 표준화 분석 보고서

(TTA) **TTAK.KO-10.0778** - 빅데이터 실시간 처리 - 제1부 : 기술개요, **0779** - 빅데이터 실시간 처리 - 제2부: 기능 요구사항

(JTC1) **N2386** - Next Generation Analytics and Big Data - A Reference Model for Big Data

(NIST) Big Data Outline: Combining Brainstorming Deliverables

안전한 단방향 데이터 통신

(병행|차세대공략) ~'19, ITU-T SG17, NIST, ISO/IEC

(NIST) **SP 800-82** - Guide to Industrial Control Systems (ICS) Security, **SP 800-147** - BIOS Protection Guidelines, **SP 800-147B** - BIOS Protection Guidelines for Servers

(IEC) **TS 62443-1-1** - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, **62443-2-1~3** - Security for industrial automation and control systems

개인건강기록(PHR, Personal Health Record) 서비스 보안

(병행|차세대공략) ~'18, ISO TC215, ITU-T SG16, HL7

(TTA) **TTAK.KO-10.0304** - 개인건강정보 보호를 위한 기술적 요구사항, **0750** - 건강라이프로그 서비스 정보보호 참조모델

(ITU-T) **H.810** - Interoperability design guidelines for personal health systems

(ISO/HL7) **16527** - Health Informatics - HL7 Personal Health Record System Functional Model, Release 1(PHRS FM)

전자건강기록(EHR, Electronic Health Record) 보안 프레임워크 기술

(병행|차세대공략) ~'18, ISO TC215, HL7

(TTA) **TTAR-06.0028** - 모바일 RFID 기반의 헬스케어 정보보호 서비스 모델을 위한 응용 요구사항 프로파일, **TTAK.IT-X.1092** - 바이오인식 기반 원격 의료 통합 프레임워크

(ISO) **TS 13606-4** - Health informatics - Electronic health record communication - Part 4 : Security, **14441** - Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment, **21547** - Health informatics - Security requirements for archiving of electronic health records - Principles, **27790** - Health informatics - Information security management in health using ISO/IEC 27002 **TR 11633-1** - Information security management for remote maintenance of medical devices and medical information systems -Part 1: Requirements and risk analysis, **11633-2** - Information security management for remote maintenance of medical devices and medical information systems - Part 1: Implementation of an information security management system(ISMS), **21548** - Health informatics - Security requirements for archiving of electronic health records - Guidelines

(IEC) **TR 80001-2-1:2012** - Application of risk management for IT-networks incorporating medical devices - Part 2-2:Guidance for the communication of medical device security needs, risks and controls

(HL7) **HL7 Version 3** : Privacy, Access and Security Services(PASS), HL7 Healthcare Privacy and Security Classification System(HCS), HL7 FHIR Specification v0.0.82

유해정보 차단 정책 및 기술

(병행|차세대공략) ~'17, ITU-T SG17

융합서비스 환경에서 속성기반 접근제어

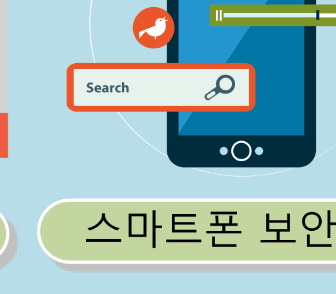
(병행|차세대공략) ~'19, ITU-T SG17, JTC1 SC27

(TTA) **TTAK.KO-12.0236** - 온라인 청소년 보호를 위한 ID 검증 구조, **0285** - 온라인 청소년 보호를 위한 속성 정보 수집 프레임워크

(ITU-T) **X.1258** - Enhanced authenticaton based on aggregated attribute

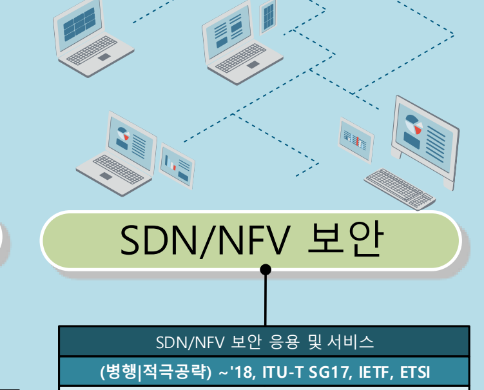
네트워크/디바이스 보안

IoT 보안



스마트폰 보안

사이버 보안



SDN/NFV 보안

IoT 네트워크 및 플랫폼 보안 프레임워크

(선행|적극공략) ~'20, ITU-T SG17/IETF/oneM2M/OCF, ETSI/ISO/IEC, 3GPP

(TTA) **TTAK.KO-06.0321/R1** - 이동통신시스템에서의 IoT/M2M 식별 체계 요구사항, **0365** - 객체 식별자 기반 사물인터넷 디바이스 식별 체계, **0381** - 스마트 디바이스 기반 센서 개인화 서비스 참조, 0388/R1, 사물인터넷 환경에서의 CoAP 기반 기기 상호연동 시험절차

(IETF) **RFC 7252** - The Constrained Application Protocol (CoAP), **RFC 7390** - Group Communication for the Constrained Application Protocol (CoAP)

(ITU-T SG13) **Y.4000** - Overview of the Internet of things, X.iotsec-2 - Security framework for Internet of Things

(ETSI) **TS 118 103** - Security solutions, **TS 118 108** - CoAP Protocol Binding, **102 690** - Machine-to-Machine communications (M2M); Functional architecture

IoT 정보보호 프레임워크

(선행|적극공략) ~'18, ITU-T SG20/oneM2M/IETF, ETSI/IEEE, 3GPP

(TTA) **TTAT.MM-TR.0008** - oneM2M - Security V1.0.0 : Analysis of Security Solutions for the oneM2M System, **TTAT.MM-TS.0003** - oneM2M - Security Solutions, **TS.0004** - oneM2M - Service Layer Core Protocol Specification,

(oneM2M) **TS-0001-V1.6.1** - Functional Architecture, **0003-V1.0.1** - Security Solutions, **0004-V1.0.1** - Service Layer Core Protocol Specification, **TR 0008**, oneM2M-R-0008-Security-V1.0.0

IoT 디바이스 보안

(선행|차세대공략) ~'20, ITU-T SG17/oneM2M/OCF, ETSI/JTC1 SWG5, 3GPP

(TTA) **TTAK.KO-10.0887-Part1** - ICT DIY 창작소 - 제 1 부: 요구사항 및 운영체계, **0789-Part9** - ICT DIY –제9부: 하드웨어 기본 규격, **0789-Part10** - ICT DIY –제10부: 하드웨어 개발 지침, **0789-Part11** - ICT DIY –제11부: 오픈소스 소프트웨어 지침 **TTAK.KO-12.0290** - 차량의 군집 주행 서비스 보안 요구 사항, **0286** - 자동차 전자 제어 장치 간의 통신 보안 요구 사항

(ISO/IEC) **ISO/IEC 29182-1~4:2013** - Information technology – Sensor networks: Sensor Network Reference Architecture (SNRA)

악성코드 분석 및 보고 형식

(병행|다각화협력) ~'22, ITU-T SG17, JTC1, IEEE

(TTA) **TTAK.KO-12.0147** - 악성 코드 경유/유포지 탐지 프레임워크, **TTAE.IT-X.1500** - 사이버보안 정보 교환 개요(CYBEX) **TTAE.IT-TTAE.IT-X.1520** - 공통 취약점 및 노출(CVE),

(ITU-T) **X.1546** - Malware attribute enumeration and characterization

(IEEE ICSG) **MMDEF** - The Malware Metadata Exchange Format

보안정보공유 및 연동 프레임워크

(병행|다각화협력) ~'20, ITU-T SG17, IETF, JTC1

(TTA) **TTAK.KO-12.0145** - 분산서비스거부 공격의 탐지 및 대응 메시지 교환 포맷, **0061/R1** - 네트워크 공격에 대한 시그니처 교환 프로토콜, **0172** - 사이버보안 정보공유 협상 절차, **0229** - 확장된 침입 탐지 메시지 교환 포맷, **0242** - 세션 정보 메시지 교환 포맷(SIMEF), **0256** - 보안 관제를 위한 시스템 메시지 교환 포맷, **0279** - 보안 정보 메시지 교환 프로토콜, **0282** - 침입탐지시스템을 위한 보안 정책 메시지 및 배포 프로토콜, **0283** - Snort 기반 침입탐지시스템 탐지 규칙 요구사항 **TTAE.IT-X.1570** - 사이버보안 정보 교환에서의 탐색 메커니즘 **TTAE.IF-RFC4766** - 침입 탐지 메시지 교환 요구사항

(ITU-T) **X.1209** - Capabilities and their context scenarios for cybersecurity information sharing and exchange, **X.1500** - Overview of cybersecurity information exchange (CYBEX), **X.1500.1** - Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange, **X.1500 Appendix I** - X.1500 (2011) Amendment 7, Overview of cybersecurity information exchange (CYBEX) **X.1520** - Common vulnerabilities and exposures, **X.1525** - Common weakness scoring system, **X.1526** - Open vulnerability and assessment language, **X.1541** - Incident object description exchange format X.1580 - Real-time inter-network defence, **X.1570** - Discovery mechanisms in the exchange of CYBEX, **X.1581** - Transport of real-time inter-network defence messages, **X.1582** - Transport protocols supporting cybersecurity information exchange, **X.Suppl.18- ITU-T X.1205** - Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks, **X Suppl.20: ITU-T X.1205** - Supplement on framework of security information sharing negotiation,

침해사고 분석을 위한 네트워크 포렌식 도구 요구사항

(병행|차세대공략) ~'21, ITU-T SG17, IETF, JTC1 SG27

(TTA) **TTAK.KO-12.0080** - 디지털 증거 파일 교환포맷, **0113** - 디지털 증거 조사 모델, **0280** - 사이버 침해사고 분석을 위한 네트워크 데이터 수집 및 보존 도구 요구사항

(IETF) **RFC 3227** - Guidelines for Evidence Collection and Archiving, **RFC 5070** - The Incident Object Description Exchange Format

(ITU-T) **X.1541** - Incident Object Description Exchange Format

(JTC1) **ISO/IEC 27037** - Guidelines for identification, collection, acquisition and preservation of digital evidence, **27041** - Guidance on assuring suitability and adequacy of incident investigative method, **27042** - Guidelines for the analysis and interpretation of digital evidence, ISO/IEC 27043 - Incident investigation principles and processes

(ETSI) **TS102232** - Handover Interface and Service-Specific Details (SSD) for IP delivery, **TS102657** - Handover interface for the request and delivery of retained data

SDN/NFV 보안 응용 및 서비스

(병행|적극공략) ~'18, ITU-T SG17, IETF, ETSI

(TTA) **TTAE.IF-RFC6708** - 응용 계층 트래픽 최적화(ALTO) 요구 사항, **RFC7285** - 응용 계층 트래픽 최적화(ALTO) 프로토콜

(ITU-T) **Y.3320** - Requirements of formal specification and verification methods for software-defined networking

SDN/NFV 보안 프레임워크와 메커니즘

(병행|적극공략) ~'22, ITU-T SG13 & 17, IETF, ETSI

(TTA) **TTAK.KO-01.0182** - 소프트웨어 정의 네트워크(SDN)를 위한 제어 플레인의 개방형 인터페이스 요구사항, **Y.3300** - 소프트웨어 정의 네트워킹 프레임워크,

(IETF) **RFC 6708** - Application-Layer Traffic Optimization (ALTO) Requirements

(ONF) OpenFlow Specification 1.3

(ITU-T) **Y.3300** - Framework of software-defined networking, **Y.3301** - Functional requirements of SDN

스마트폰 환경에서의 저장장치 보안 프레임워크

(후행|적극공략) ~'18, ITU-T SG17, OMA, OMTP

(TTA) **TTAK.KO-12.0153** - 모바일 통신 단말용 상황인지형 보안재구성 프레임워크

(ITU-T) **X.1125** - Correlative Reacting System in Mobile Data

(OMA) **OMA-TS-DM_Protocol-V1_3-20091229-D** - Device Management Protocol Draft Version 1.3

(OMTP) **OMTP TR1** - Advanced Trusted Environment

스마트폰 기반의 봇넷 대응을 위한 보안 요구사항

(후행|차세대공략) ~'19, ITU-T SG17

(TTA) **TTAK.KO-12.0110** – 봇넷 탐지 및 대응 프레임워크, **0183/R1** - 스마트폰 앱 보안 검증 절차 및 기준, **0265** – 스마트 폰 보안 관리 제품 보안 요구사항

(ITU-T) **X.bots** – A centralized framework for botnet detection and response, **X.sbb** – Security capability requirements for countering smartphone-based botnets

온라인 배포판

TTA홈페이지(http://www.tta.or.kr)
▼
자료마당
▼
TTA간행물
▼
ICT표준 활용/개발맵

범 례

중점 표준화 항목(표준개발 대상)
(표준화 특성 | 표준화 전략목표) 완료시점, Target SDOs
관련표준 대응 리스트
(표준화기구) 표준번호 - 표준명

[표준화 특성]
- 선행 : 선 표준화 후 기술개발/상용화
- 병행 : 표준화/기술개발 동시 추진
- 후행 : 선 기술개발/상용화 후 표준화

[표준화 전략목표]
- 적극공략: 국제표준 선도경쟁
- 차세대공략: 국제표준 신규제안
- 다각화협력: 전략적 제휴, 부분협력
- 방어적수용: 국제표준 수용/적용

TTA 한국정보통신기술협회
Telecommunications Technology Association

* 본 자료는 정부(미래창조과학부) 정보통신방송표준개발지원 사업의 일환으로 수행된 과제(R0166-16-1005, 정보통신·방송 표준화 전략 및 체계 연구) 연구결과로 발간된 자료입니다.