TTA Standard

정보통신단체표준(국문표준)

TTAS.KO-12.00XX

제정일: 2018년 XX월 XX일

네트워크 포렌식을 위한 패킷 처리 지침

Guidelines of Packet Processing for Network Forensics

한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 사이버보안 프로젝트그룹(PG503)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	이상진	고려대학교	교수	사이버보안프로젝트그룹 특별위원	
표준 초안 작성자	이상진	고려대학교	교수	사이버보안프로젝트그룹 특별위원	
	김기범	경찰대학	교수		
	한재혁	고려대학교	연구원		
	정병찬	고려대학교	연구원		
사무국 담당	박수정	TTA			

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.XX

서 문

1 표준의 목적

이 표준은 네트워크 패킷이 법정에서 증거로 인정받을 수 있게 하기 위한 패킷의 수집, 보존, 분석 등에 관한 절차를 규정하는데 목적이 있다. 이 표준은 디지털 포렌식 조사의 패킷 처리 과정에서 발생할 수 있는 기술적·절차적 문제를 해소하기 위한 가이드라인으로 활용할 것을 권고한다.

2 주요 내용 요약

이 표준은 네트워크 포렌식 과정에서 패킷을 처리하는 절차를 규정한다. 패킷은 네트워크에서 사용자 행위를 분석하는데 중요한 자료로 활용할 수 있다. 그러나 처리과정의 실수로 인해 데이터가 훼손됨으로써 증거로 사용하지 못할 수 있으며, 개인정보와 같은 민감한 정보를 포함하고 있기 때문에 유출로 인한 사생활 침해가 발생할 수 있다. 따라서 네트워크 포렌식에서 핵심 증거인 패킷을 수집하여 처리할 때에는 투명하고 신뢰할 수 있는 절차가 제시되어야 한다. 본 지침은 네트워크 포렌식 과정을 통해 제시된 패킷이 디지털 증거로서 증거능력을 갖기 위해 패킷의 수집, 보존, 전달 과정에서 지켜야 할 원칙을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

- 해당 사항 없음

3.2 인용 표준과 본 표준의 비교표

- 해당 사항 없음

Preface

1 Purpose

The standard is to establish to make the packet data have an legal validity for network forensics by defining the procedures to be followed in the process of packet collection, preservation, delivery, and analysis.

2 Summary

The standard establish the necessary model and procedure while processing the packet for network forensics. Even though the packet is an important data to analyze user behavior through the network, reliable procedure should be suggested since it is easy be damaged due to careless handling, sensitive contents such as personal information is included, and can be modified intentionally. Therefore the standard defines the principles to be followed in packet collection, preservation, and delivery in order to have legal validity as the digital evidence through network forensic process.

3 Relationship to Reference Standards

3.1 Relationship to Reference Standards

None

3.2 Comparison between This Standard and Reference Standards

None

목 차

네트워크 포렌식을 위한 패킷 처리 지침
(Guidelines of Packet Processing for Network Forensics)

1 적용 범위

네트워크 포렌식은 디지털 포렌식의 한 분야로서, 네트워크를 통해 전송된 데이터를 수집, 처리하여 증거를 추출하고 분석하는 과정을 말한다. 현재 네트워크 포렌식 과정에서 패킷의 수집 및 분석을 위한 도구와 그 요구사항을 정의하는 표준만 존재한다.
따라서 본 표준은 패킷을 처리하는 과정에 대한 표준절차를 규정하고 수집된 패킷이 증거능력을 가지도록 하는 절차를 제시한다. 표준화된 방법으로 네트워크 포렌식이 이루어지면 분석절차의 투명성과 분석결과의 신뢰성을 확보될 수 있을 것이다. 이러한 절차는 사이버 침해 사고, 정보 유출 사건, 내부 통신망의 안전성 분석 등 다양한 영역에서 활용할 수 있다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1 네트워크 포렌식(network forensics)

네트워크 트래픽에서 증거를 획득하고 분석하는 것이다. [출처: 안랩 보안용어 사전]
즉, 네트워크에서 전송되는 정보를 수집, 보존, 분석하는 절차와 방법을 말한다.

3.2 패킷(packet)

데이터 전송에서 사용되는 데이터의 묶음. 패킷 전송은 두 지점 사이에 데이터를 연속적으로 전송하지 않고, 전송할 데이터를 적당한 크기로 나누어 패킷의 형태로 구성한 다음 패킷들을 하나씩 보내는 방법을 쓴다. 각각의 패킷은 일정한 크기의 데이터뿐만 아니라 데이터 수신처, 주소 또는 제어 부호 등의 제어 정보까지 담고 있다. [출처: TTA 정보통신용어사전]

3.3 통신(communications)

정보의 전송에 관련되는 다양한 방법과 절차, 기구와 장치, 중간 매체 등을 포함하는 광범위한 분야를 총칭한다. [출처: TTA 정보통신용어사전]

3.4 프로토콜(protocol)

이메일, 메신저, 파일 업·다운로드, 웹 등 사용자 서비스를 제공하기 위한 통신 규칙으로서, SMTP, HTTP, HTTPS, FTP, SFTP, SSH, TELNET, IMAP, IRC, RDP 등을 총칭한다. [출처: TTA 정보통신용어사전]

3.5 OSI 7 계층 모델(Open system Interconnection 7 layer model)

국제 표준화 기구(ISO)가 1977년에 정의한 국제 통신 표준 규약. 통신의 접속에서부터 완료하기까지의 과정을 7단계로 구분, 정의한 통신 규약으로 현재 다른 모든 통신 규약의 지침이 되고 있다. 이 7계층의 통신 규약군에 대해 각 계층별로 설명, 정의한 것이 OSI 기본 참조 모델이다. [출처: TTA 정보통신용어사전]

명 칭	규정 사항
응용(7) 계층	사용하고 있는 응용 프로세스를 어떻게 인식할 것인가
표현(6) 계층	텍스트, 음성, 화상 등의 정보를 어떻게 부호화할 것인가
세션(5) 계층	통신 경로의 확립이나 단절, 정보 전송 방식을 어떻게 규정할 것인가
전송(4) 계층	정보를 전송할 때 신뢰성을 어떻게 확보할 것인가
네트워크(3) 계층	송신원에서 수신처로 어떤 경로로 정보를 전송할 것인가
데이터링크(2) 계층	인접한 기기 사이에서 정보를 어떻게 전송할 것인가
물리(1) 계층	어떤 신호로 통신을 할 것인가

3.6 해시값

임의의 길이인 입력 메세지를 고정된 길이의 출력값으로 압축시키는 함수의 결과값
[출처: TTA 정보통신용어사전]

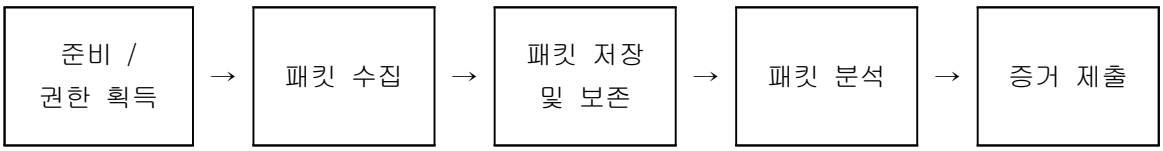
4 약어

CC	Content of Communications
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for CC, IRI)
IP	Internet Protocol
IRI	Intercept Related Information
MAC	Media Access Control
SHA	Secure Hash Algorithm

5 패킷 처리 절차

5.1 네트워크 포렌식 조사 모델

네트워크 포렌식은 송신자와 수신자 간의 통신 데이터를 합법적으로 수집하고 분석함으로써 증거능력을 갖도록 하는 절차와 방법을 말하며, (그림 5-1)과 같이 권한 획득, 패킷 수집, 저장 및 보존, 분석, 증거 제출을 하는 일련의 과정으로 진행된다.



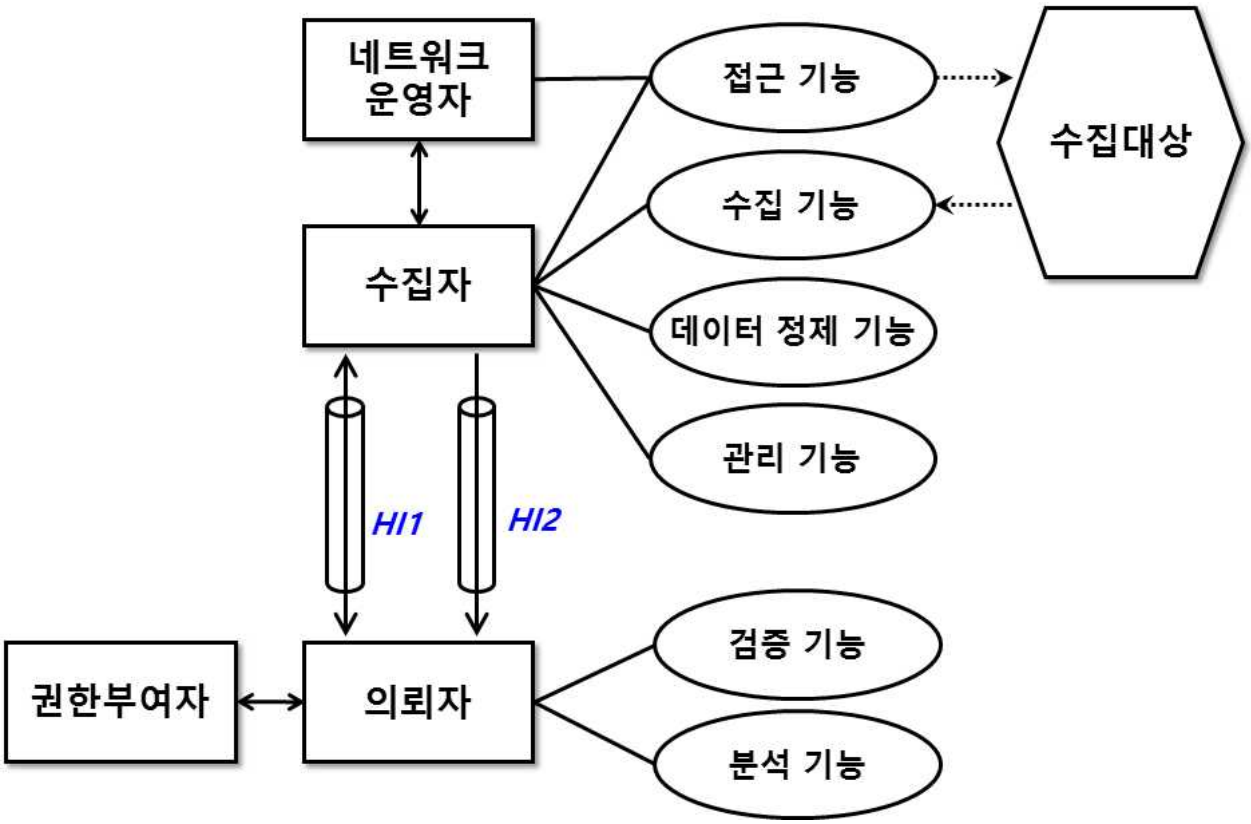
(그림 5-1) 네트워크 포렌식 조사 모델

네트워크 패킷은 수사 또는 보안 감사 등을 위해 분석되는데, 궁극적으로는 책임 소재를 규명하는 원천 데이터로 사용되기 때문에 수집된 데이터의 무결성을 보장할 수 있어야 한다. 또한 패킷 내에는 사생활 정보가 포함되어 있기 때문에 함부로 열람해서는 안되며, 불가피하게 수집, 분석해야 하는 사유가 있을 때에는 패킷의 수집 목적, 대상, 범위, 기간, 방법, 이유 등의 내용을 구체적으로 기술한 문서를 작성하여 합법적인 권한(예: 통신제한조치허가서)을 부여받아야 한다.

패킷수집자는 통신 채널을 통해 의뢰자와 정보를 교환해야 하고, 신뢰성이 검증된 도구를 사용하여야 한다. 만약 의뢰자의 요청이 있거나 패킷을 수집할 수 있는 권한의 유효기간이 만료되면 수집자는 패킷 수집을 즉각 중단해야 한다.

패킷수집의 결과물은 **패킷내용정보**(CC, Content of Communications)와 **패킷부가정보**(IRI, Intercept Related Information)로 구분할 수 있다. 패킷내용정보는 네트워크를 통한 송신자와 수신자가 주고받은 데이터를 의미하고, 패킷부가정보는 대상 통신에 대한 송신자와 수신자 정보(IP, MAC 주소 등), 프로토콜 종류, 패킷 크기, 시간 등과 같이 통신 내역을 설명하는 데이터를 의미한다.

획득된 통신 데이터는 논리적인 단위로 구분하여 해시값(예: SHA) 생성과 같은 방식으로 무결성(integrity)을 검증할 수 있는 수단을 강구해야 하며, 관리연속성(Chain of Custody)을 유지할 수 있는 문서를 작성해야 한다. 만약 패킷이 수집 범위 이상으로 수집되었다면, 수집자는 부여된 범위에 맞는 데이터를 선별하는 정제 과정을 수행해야 한다. 의뢰자는 수집자로부터 전달받은 데이터의 무결성을 검증하고, 분석함으로써 법정 증거로 제출할 수 있다. 본 표준에서 제시하는 패킷 처리 모델은 (그림 5-2)와 같다.



(그림 5-2) 패킷 처리 모델

5.2 참여자별 역할

패킷 처리 모델에서 참여자는 권한부여자(예: 사법기관), 의뢰자(예: 수사기관), 수집자(신뢰할 수 있는 대상), 네트워크 운영자(예: 전기통신사업자), 그리고 네트워크 서비스 이용자이다. 각 참여자의 역할은 <표 5-1>과 같다.

의뢰자와 수집자는 원칙적으로 다른 기관에 소속되어야 한다. 다만, 네트워크 운영자의 협조 없이 자체적으로 데이터를 수집할 수밖에 없는 불가피한 경우에는 동일한 기관에 소속될 수 있다. 그러나 의뢰자와 수집자의 업무가 엄격하게 분리되어 있어야 하며, 수집자만이 수집대상에 접근할 수 있고, 의뢰자는 전달받은 데이터에만 접근하여야 한다.

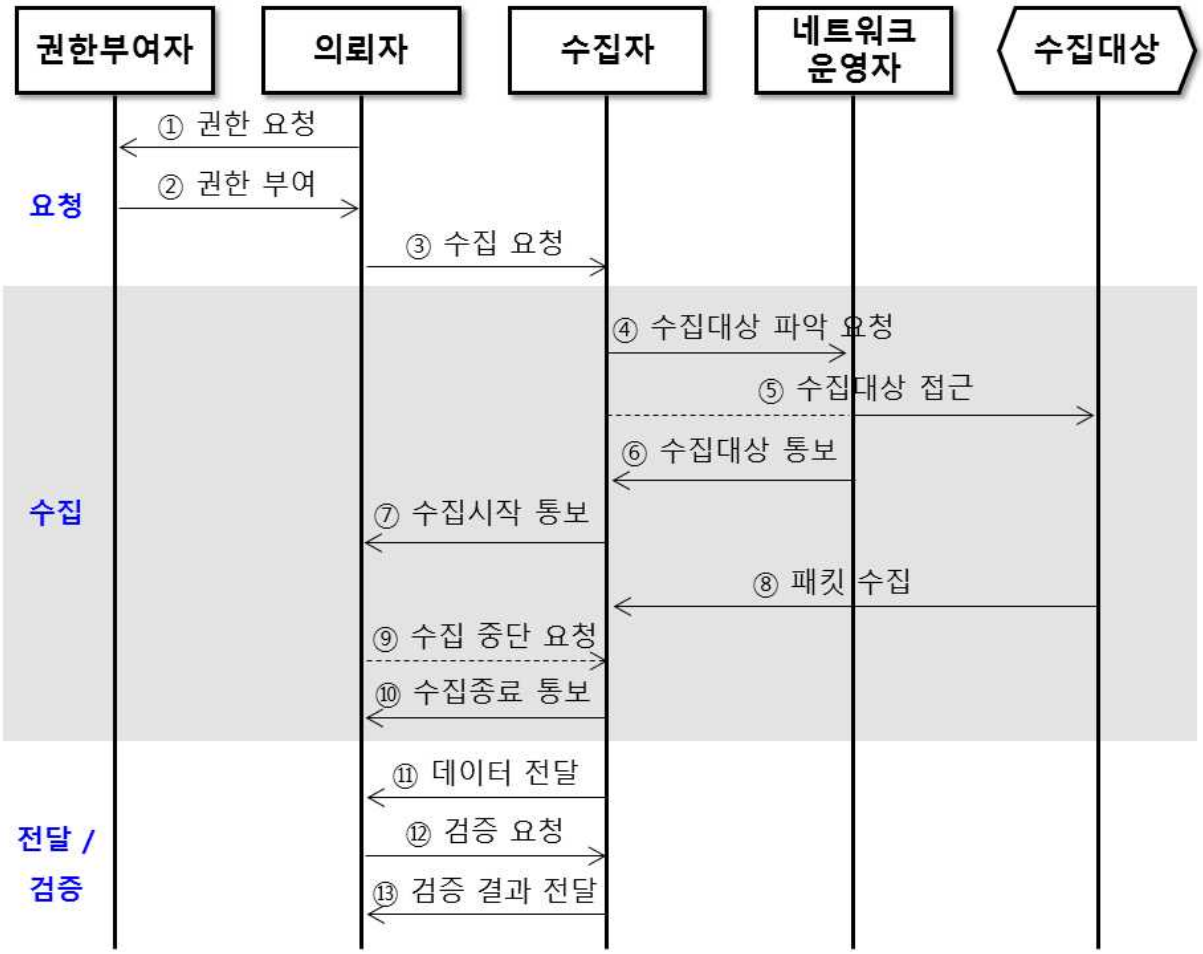
<표 5-1> 패킷 처리 모델에서 참여자별 역할

참여자	역 할
권한부여자	네트워크 패킷을 수집하려는 의뢰자의 요청을 면밀히 검토하고 수집대상과 수집 기간, 범위를 한정하여 수집할 수 있는 권한(예: 통신제한조치허가서)을 부여한다.

의뢰자	법적 근거에 의하여 권한부여자에게 패킷의 수집 허가를 요청할 수 있으며, 권한을 부여받은 경우 수집자에게 수집대상, 기간, 범위와 관련된 정보를 공유하고 패킷의 수집을 요청한다. 권한을 부여받지 않은 상태에서 긴급하게 패킷의 수집을 요청할 수 있으나, 사후에 수집권한을 부여받지 못한 경우에는 수집된 패킷의 파기를 요청해야 한다. 여러 의뢰자가 동시에 동일한 수집대상의 패킷을 요청할 수 있고, 요구사항에 맞는 결과를 수집자로부터 회신받을 수 있다. 또한 의뢰자는 수집대상으로부터 획득된 데이터의 무결성을 검증하기 위한 자료를 수집자에게 요청할 수 있다.
수집자	서비스가 연결된 통신 네트워크에 접근할 수 있어야 하며, 수집대상의 패킷을 수집할 수 있는 설비를 갖추고 있어야 한다. 수집자는 패킷을 수집할 수 있는 권한을 부여받은 의뢰자의 요구사항을 충족하는 데이터를 제공할 책임이 있다. 특히, 획득한 데이터가 증거능력을 갖도록 데이터의 무결성을 검증할 수 있는 정보를 의뢰자에게 제공해야 한다. 의뢰자가 긴급하게 패킷 수집을 요청하였을 때에는 수집된 패킷을 의뢰자에게 제공하기 전에 반드시 수집권한을 확보했는지 확인해야 하며, 미확보시에는 수집된 패킷을 즉각 파기하여야 한다. 수집자는 의뢰자의 요구사항을 충족하거나 관련 있는 데이터만을 제공하기 위해 수집된 패킷을 선별하는 정제 과정을 수행해야 한다.
네트워크 운영자	네트워크 서비스 이용자에게 서비스를 제공하기 위한 환경을 운영·관리하며, 수집권한에 포함된 정보로부터 수집대상을 결정한다. 또한 수집자에게 해당 수집대상에 접근하여 패킷을 수집할 수 있는 환경을 가질 수 있도록 최대한 협조한다.
네트워크 서비스 이용자	네트워크 운영자가 제공하는 서비스를 정상적으로 사용하는 사람을 말한다. 서비스 이용자의 사생활은 원칙적으로 침해되어서는 안된다. 다만, 법원의 허가와 같은 특별한 경우에만 필요 최소한으로 침해가 허용된다. 패킷을 수집하기 위한 설비를 준비하거나 일부 서비스를 추가적으로 작동시켜야 하는 경우에도 서비스 이용자는 패킷이 수집되고 있다는 사실을 감지할 수 없어야 한다.

5.3 패킷 수집 과정

이 절에서는 네트워크 패킷을 수집하는 과정을 기술한다. 의뢰자는 권한부여자로부터 패킷을 수집할 수 있는 권한을 부여받아, 수집자에게 수집 요청을 한다. 수집자는 수집대상으로부터 패킷을 수집하여 의뢰자의 요구사항이 충족되는 데이터를 제공한다. 패킷을 수집하는 과정은 크게 요청, 수집, 전달 및 검증 단계로 구분되며, 단계별 행동은 (그림 5-3)과 <표 5-2>와 같다. (그림 5-3)에서의 점선은 생략되거나 발생하지 않을 수 있는 단계를 의미한다.



(그림 5-3) 패킷 수집 과정

<표 5-2> 패킷 수집 절차에서 단계별 행동 목록

단계	행 동 (Action)	
1	권한 요청	의뢰자는 수집 목적, 대상, 범위, 기간, 방법, 이유 등의 내용을 구체적으로 기술한 문서를 권한부여자에게 제출하여 합법적으로 수집할 수 있는 권한을 요청한다.

2	권한 부여	권한부여자는 수집해야 하는 이유가 타당하면 의뢰자에게 적법한 권한을 부여한다.
3	수집 요청	의뢰자는 합법적으로 패킷을 수집할 수 있는 권한과 함께 수집할 대상, 범위, 기간, 방법 등을 수집자에게 전달한다.
4	수집대상 파악 요청	수집자는 네트워크 운영자에게 의뢰자의 요청사항을 확인시키고 수집대상에 대한 정보를 요청한다.
5	수집대상 접근	네트워크 운영자는 수집자가 요청한 수집대상을 결정하기 위해 네트워크 서비스 이용자 중에서 수집대상을 확정한다. 네트워크 운영자가 수집자의 요청을 거부하거나 비협조할 경우에 수집자는 수집대상에 직접 접근할 수 있다.
6	수집대상 통보	네트워크 운영자는 수집자가 요청한 수집대상을 수집자에게 통보한다.
7	수집시작 통보	수집자는 수집대상을 확정한 사실과 패킷 수집을 위한 관련 조치가 완료되어 패킷 수집이 시작되었음을 의뢰자에게 알린다. 이 과정에서 수집대상과 관련하여 확인된 정보를 추가적으로 전달할 수 있다.
8	패킷 수집	수집자는 수집대상의 통신 활동에 의해 생성된 데이터를 수집한다.
9	수집 중단 요청	의뢰자는 패킷을 수집할 수 있는 권한이 유효함에도 불구하고 수집을 중단해야 하는 상황이 발생하는 경우에 수집자에게 수집 중단을 요청해야 하며, 수집자는 이에 즉각 응해야 한다.
10	수집 종료 통보	수집자는 수집권한에서 명시된 요구사항이 충족된 경우에는 수집을 종료하고 의뢰자에게 해당 사실을 통보한다.
11	데이터 전달	수집대상으로부터 획득된 데이터는 증거능력을 갖도록 조치를 취하고 의뢰자에게 전달한다. 전달되는 데이터는 수집자에 의해 데이터 정제 기능이 수행된 상태일 수 있으며, HI2 채널을 사용한다.
12	검증 요청	의뢰자는 수집자로부터 전달받은 데이터가 증거능력을 갖는지 확인할 필요가 있다. 따라서 데이터를 수집한 당사자인 수집자에게 검증을 요청할 수 있다.
13	검증 결과 전달	수집자는 패킷을 수집하는 과정에서 생성한 패킷검증정보를 이용하여 의뢰자의 요청에 상응하는 결과를 전달한다.

5.3.1 요청 단계

의뢰자가 수집대상을 획득하기 위한 권한을 권한부여자에게 요청하고, 패킷을 수집할 수 있는 권한을 확보한 의뢰자가 수집자에게 수집을 요청하는 단계이다.

의뢰자는 권한부여자로부터 권한을 요청하기 위해서 정당한 근거와 필요로 하는 권한의 효력을 명확하게 제시해야 하며 관련 법률 및 판례에 규정된 절차를 따라야 한다. 의뢰자의 요청을 받은 권한부여자는 면밀한 검토를 통해 합당하다고 판단되는 경우에 의뢰자가 요청한 권한을 부여한다. 만약 수집자가 의뢰자의 권한에 대한 확인을 요청할 경우 권한부여자는 이를 확인해주어야 한다.

5.3.1.1 요구사항

- 패킷을 수집할 수 있는 권한을 부여받은 의뢰자는 다음의 내용을 포함하여 수집자에게 데이터 수집을 요청한다. 수집자는 의뢰자의 권한 확인, 수집대상 식별 및 접근 등 수집 행위를 위해 추가적으로 필요한 정보가 있을 경우 의뢰자에게 이에 대한 정보의 제공을 요구할 수 있다.
  ① 권한을 요청하는 주체와 부여받은 권한을 행사하는 주체
  ② 부여받은 권한의 유효기간
  ③ 수집대상을 구분할 수 있는 식별자
    ◦ 수집대상을 확정할 수 있는 네트워크 서비스 이용자의 고유정보
      (예: 이름, 위치 정보, 전화번호, 이메일 주소, 로그인 정보 등)
    ◦ 수집대상의 네트워크 정보
      (예: IP주소, MAC주소, 통신 프로토콜, 패킷 크기 등)
    ◦ 수집대상을 생성하는 하드웨어 및 소프트웨어 정보
      (예: 케이블 모뎀 식별자, 운영체제 등)
  ④ 수집된 패킷을 수집자로부터 전달받는 방법
  ⑤ 긴급상황시 대책 및 의뢰자 비상연락처
  ⑥ 수집자가 데이터를 보존해야 하는 기간 및 방법

5.3.1.2 준수사항

- 권한부여자는 의뢰자의 권한 요청에 대해 법률에 따라 승인 여부를 결정해야 한다.

5.3.1.3 주의사항

- 의뢰자는 권한 확보를 예상하여 사전에 수집자에게 수집을 요청해서는 안된다. 단, 법률에서 허용하는 긴급한 경우에는 예외로 한다.

5.3.2 수집 단계

수집자가 의뢰자로부터 요청받은 대상으로 접근하고 패킷을 수집하는 단계이다. 수집자는 인터페이스를 통해 수집대상을 확인하고 의뢰자가 요청한 내용에 대해 수집이 가능한지를 판단하여 의뢰자에게 통보한다. 수집이 불가능한 경우 이에 대한 사실을 의뢰자에게 통보한다.

수집자가 보존하는 데이터는 패킷내용정보(CC), 패킷부가정보(IRI), 그리고 이러한 데이터의 무결성을 검증하기 위한 데이터(패킷검증정보)로 구분한다. OSI 7 계층 모델에서 패킷내용정보는 5계층에서 7계층까지의 데이터를 포함하고 패킷부가정보는 1계층에서 4계층까지의 데이터를 포함한다. 패킷검증정보는 패킷내용정보와 패킷부가정보의 무결성을 검증하기 위해 수집자가 생성한 데이터이다.

- 패킷내용정보

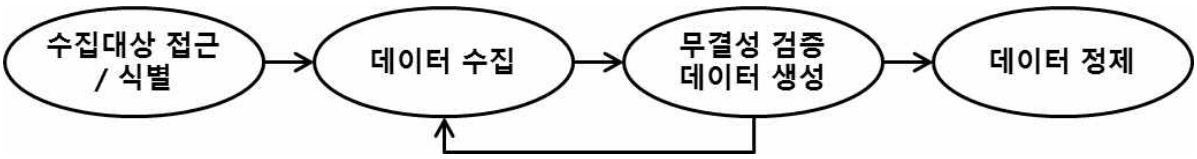
① 네트워크 서비스 이용자가 송·수신하는 데이터

- 패킷부가정보

① 패킷을 주고받는 시각
② IP 정보(출발지, 목적지)
③ 통신 프로토콜 정보(종류, 버전 등)
④ 통신 성공 여부 및 네트워크 상태 정보
⑤ 패킷 크기

- 패킷검증정보

① 패킷내용정보와 패킷부가정보를 수집한 시각
② 데이터 단위별(패킷 수, 수집된 데이터의 크기 또는 시간 등) 해시값
③ 패킷검증정보가 생성되는 방법



(그림 5-4) 수집 단계에서의 패킷 처리 과정

5.3.2.1 요구사항

- 수집자는 의뢰자의 요구사항과 수집 행위가 진행되고 있다는 사실을 관계자 이외에게 누설해서는 안된다.
- 수집자가 소유하거나 관리 권한을 가지고 있는 인터페이스를 이용하여 수집할 수 있어야 하며, 네트워크 서비스의 품질(통신 속도 등)을 과도하게 저하시켜서는 안된다. 만약 네트워크 서비스 이용자가 네트워크 서비스의 품질 차이를 인지할 가능성이 예상될 경우 수집자는 기술적으로 먼저 조치해야 한다.

- 수집자는 수집된 데이터가 외부의 위협으로부터 안전하게 보호될 수 있도록 조치해야 한다. 이때 수집자의 규모 최소화, 별도의 공간 마련, 망 분리와 같은 조치를 취해야 한다.

- 의뢰자는 패킷 수집을 요청할 경우 다음 내용이 포함되어야 한다.
  ① 수집대상 식별/추적과 관련된 사항
  ② 수집 기능의 동작과정(시작/종료시점, 중단시점 및 사유 등)
  ③ 통신 채널(HI1)을 이용한 의뢰자 통신 내용

- 수집자가 행하는 모든 과정은 기록되고 보존되어야 한다.

- 수집자는 수집된 데이터가 변조되지 않았다는 사실을 증명해야 한다.

- 시스템 오류 등 긴급상황이 발생할 경우 의뢰자에게 신속하게 상황을 보고해야 하며, 이에 대비한 적절한 조치를 취해야 한다.

- **접근(Access)** 기능은 수집자가 소유하거나 관리 권한을 가지고 있는 인터페이스를 이용하여 수집대상에게 접근할 수 있는 기능을 말한다. 수집자는 하나 이상의 연결지점을 확보하고 수집대상과 연결을 유지하고 확인한다. 수집대상이 하나 이상일 경우 각각의 수집대상을 식별하여 접근할 수 있도록 한다. 수집대상으로부터 획득한 데이터가 존재할 경우 인가된 관계자만 접근할 수 있도록 권한을 관리한다. 접근 기능은 아래와 같다.
  ◦ 수집대상 접근 연결 및 해제
  ◦ 수집대상 목록 확인
  ◦ 접근 상태(시도/연결/해제/실패)에 대한 리포트
  ◦ 획득 패킷 접근 권한 관리

- **수집(Collection)** 기능은 수집대상으로부터 수집되는 데이터를 전달받고 저장하며, 필요시 데이터 정제 기능에 데이터를 전달할 수 있는 기능을 말한다. 획득된 데이터는 패킷내용정보와 패킷부가정보로 구분할 수 있으며 식별이 용이하여야 한다. 네트워크 특성상 동일한 패킷을 다시 수집할 수 없기 때문에 신뢰할 수 있는 시스템과 도구를 통해 획득해야 하며, 데이터를 저장할 수 있는 충분한 저장 공간과 백업할 수 있는 시스템을 준비하여 만약의 상황에 대비해야 한다. 또한 인가받지 않은 자에 의한 데이터의 훼손을 방지하며, 해시 함수 등을 이용하여 주기적 또는 일정 크기 단위로 획득한 데이터의 무결성을 검증할 수 있는 패킷검증정보를 생성하여야 한다.

- **데이터 정제(Filter)** 기능은 수집 기능을 통해 획득된 데이터 중에서 사건과 관련 없는 데이터를 배제하는 과정으로 데이터를 재구성하거나 키워드 검색 등의 방법을 사용할 수 있다. 반드시 적용될 필요는 없으나, 적용될 경우 의뢰자에게 전달할 데이터에

대한 무결성이 검증될 수 있도록 동작해야 한다. 의뢰자는 권한을 요청하는 과정에서 수집대상을 명확히 하는 내용을 포함해야 하며 수집자는 데이터를 정제하기 위해 다음과 같은 기준을 적용할 수 있다.

① 네트워크 주소(IP주소, MAC주소, 포트)
② 통신 프로토콜
③ 패킷내용정보를 대상으로 하는 키워드 검색

5.3.2.2 준수사항

- 수집과정에서 사용되는 하드웨어 장비 및 소프트웨어는 법률에서 정해져 있을 경우 사전에 등록되어 있어야 한다.

- 수집자는 고의적으로 정당한 이유없이 수집시작시점이나 수집종료시점을 변경하지 않아야 한다.

- 의뢰자에게 데이터를 전달하기 전에 데이터의 수집 범위를 고려하여 정제 기능을 이행한 후에 제공하여야 한다.

- 수집자는 다음과 같은 상황을 인지하였을 때에는 즉시 의뢰자에게 보고하고, 협력을 통해 조치해야 한다.
  ① 수집대상에 대한 접근을 시도하는 경우
  ② 수집대상에 대한 접근을 완료한 경우 / 수집대상에 접근이 불가능한 경우
  ③ 수집대상의 상태(위치 등)가 변경된 경우
  (예: 갑자기 수집대상이 확인되지 않을 경우, IP주소가 변경되었을 경우 등)
  ④ 수집과정에서 사용되는 하드웨어 장비 및 소프트웨어에 문제가 발생하거나 변경이 필요한 경우 등 (예: 시스템 오작동/복구, 소프트웨어 교체 등)

- 수집대상(패킷내용정보, 패킷부가정보)과 패킷검증정보는 복제본 생성 등의 방법으로 안전하게 보존해야 한다.

- 수집자는 해시값 등 수집대상의 무결성을 검증할 수 있는 데이터를 주기적으로 생성하고 보존해야 한다.

- 수집자는 패킷을 수집할 수 있는 권한이 유효하지 않은 시점이 도래하거나 의뢰자에 의해 수집 중단을 요청받은 시점부터 수집대상에 접근하지 않아야 한다.

- 수집된 데이터를 정제하는 과정에서 수집 범위를 기준으로 복구 불가능한 방식으로 삭제해야 한다.

5.3.2.3 주의사항

- 의뢰자는 수집자가 보존하고 있는 수집대상의 보호를 위해 암호화 등의 기술적인 조치를 요구할 수 있으며 필요시 기술 지원을 할 수 있다. 다만 이 과정에서 수집자가 전달하지 않은 수집대상에 접근할 수 없어야 한다.

- 수집자는 의뢰자의 요청에 의한 행위를 수행하는 것이므로 어떠한 경우에도 의뢰자는 수집자를 보호하기 위한 최선의 조치를 취해야 한다.

- 데이터베이스를 이용한 해시 테이블 생성 등의 방법으로 수집대상의 패킷검증정보를 식별할 수 있어야 한다.

- 수집자는 수집된 데이터를 수시로 관찰하거나 영구적으로 기록해서는 안된다.

5.3.3 전달/검증 단계

수집자는 HI2 통신 채널을 이용하여 의뢰자에게 수집한 정보를 전달한다. 수집 결과물은 패킷내용정보(CC)와 패킷부가정보(IRI)를 포함하며, 의뢰자가 전달받은 데이터에 대한 검증을 수집자에게 요구할 경우에 수집자는 패킷을 수집하는 과정에서 생성한 패킷검증정보로 무결성을 검증할 수 있어야 한다.

5.3.3.1 요구사항

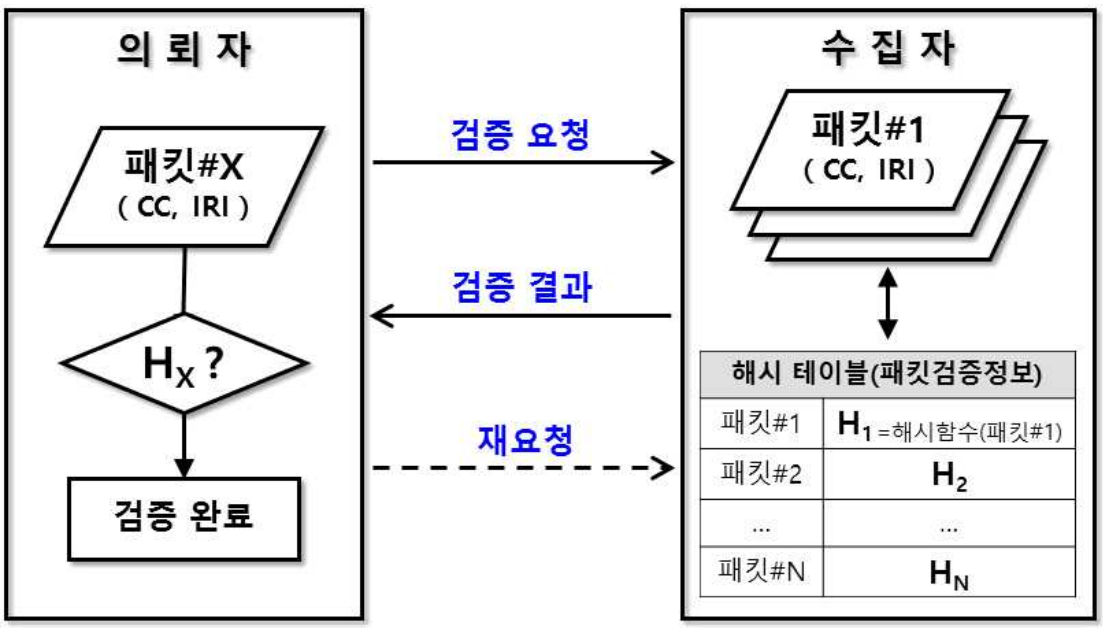
- 수집자가 수집한 패킷내용정보, 패킷부가정보, 패킷검증정보는 안전한 일방향 통신 채널을 통해 제공되어야 한다.

  - 패킷내용정보와 패킷부가정보 간의 관련성을 파악할 수 있어야 한다.

  - 의뢰자가 전달받은 데이터를 분석할 수 있는 형태여야 한다. 만약 암호화된 형태로 저장되어 있다면 복호화하기 위한 정보를 함께 제공해야 한다.

  - 의뢰자는 전달받은 데이터가 손상된 경우 수집자에게 재요청할 수 있다.

  - 수집자는 의뢰자의 요구가 있을 경우 패킷검증정보를 활용하여 검증 요청에 응하거나 수집자의 서명이 포함된 패킷검증정보를 전달할 수 있어야 한다.



(그림 5-5) 수집결과물을 검증하는 과정: 해시 테이블 활용

- **분석(Analysis)** 기능은 수집자로부터 전달받은 데이터를 분석하는 기능을 말한다. 패킷 내용정보와 패킷부가정보를 종합적으로 분석하여 사건과 연관된 타임라인이나 범죄 시나리오 등을 재구성할 수 있다. 데이터 무결성 검증 결과에 이상이 있을 경우에는 수집자에게 데이터를 다시 요청할 수 있다.

- **관리(Administration)** 기능은 수집대상으로부터 획득한 데이터를 보존, 검증, 삭제하는 기능을 말한다. 패킷을 수집하는 과정은 이해관계가 다른 다수의 참여자가 참여할 수 있으므로 다양한 상황이 발생할 수 있다. 하지만 의뢰자와 수집자가 통신할 수 있는 채널은 HI1과 HI2만 존재한다. 따라서 관리 기능은 패킷을 처리하는 과정 중에 목적을 달성하기 위해 권한의 범위 내에서 유연한 대처가 가능하게 하는 기능을 포함한다. 데이터는 사건이 종료되기 전까지 안전하게 보존되어야 하며, 보존기간이 지나면 복구가 불가능한 방식으로 삭제되어야 한다. 의뢰자가 데이터의 무결성 검증을 요청할 경우 이를 증명할 수 있는 기능이 제공되어야 하며, 의뢰자가 사건과 무관한 데이터를 발견하였을 때에는 이를 수집자에게 알려서 해당 데이터는 삭제되어야 한다. 또한 사건 처리 여부가 결정되었을 때에는 수집대상을 사용한 네트워크 서비스 이용자에게 데이터 수집 사실을 통보할 수 있어야 한다.

5.3.3.2 준수사항

- 데이터 전달을 위해서 HI1을 이용한 통신으로 HI2의 연결 상태를 먼저 확인한다.

- 수집대상을 증거로 사용할 경우에는 데이터의 무결성을 검증할 수 있는 자료와 함께 전달하여야 한다.

- 수집자는 수집권한에 명시된 보존기간 동안 백업 등의 방법으로 안전하게 보존해야 하며, 보존기간이 만료될 경우 의뢰자의 요청으로 수집한 데이터 일체를 복구 불가능하게 삭제한다.

5.3.3.3 주의사항

- 수집자는 의뢰자의 데이터 무결성 검증 요청에 협조하기 위해 패킷검증정보 생성 외에도 이와 유사한 방법을 활용할 수 있다.

- 의뢰자는 전달받은 데이터가 네트워크 통신 장애 등 이유로 무결성이 훼손되었는지 확인하여야 한다. 만약 훼손되었으면, 수집자에게 재전송을 요청하여야 한다.

5.4 통신 채널

의뢰자와 수집자 사이의 통신은 핸드오버 인터페이스(HI, Handover Interface)를 적용한다. HI는 관리 정보, 패킷내용정보(CC) 및 패킷부가정보(IRI)가 논리적으로 분리되도록 2포트 구조를 사용한다. 2개로 분리된 포트는 각각 서로 다른 목적을 가지며 정보를 전송하거나 수신하기 위한 채널로 사용한다. 기술 지원이 가능할 경우, 2개의 물리적 채널이나 프로토콜을 달리하여 구분할 수 있도록 한다. 포트가 연결되는 영역은 수집자와 의뢰자에게 전달이 가능한 영역이다.

5.4.1 HI1: 관리 정보 채널

HI1은 수집자와 의뢰자 사이에서 필요한 정보를 통신하기 위해 사용된다. HI1은 패킷처리의 관리(management) 목적으로 통신하기 때문에 양방향으로 통신한다. 만약 의뢰자가 최초에 패킷 수집을 요구한 수집대상이 변경되거나, 패킷 수집의 중단을 요청하거나, 수집자가 사용하는 패킷의 수집 기능에 문제가 발생하면 의뢰자와 수집자 간의 통신이 필요하기 때문에 양방향 통신을 하는 채널을 사용하며, 의뢰자와 수집자가 사용하는 통신채널은 인가받지 않은 다른 참여자에게 어떠한 형태의 접근도 허용되지 않아야 한다.

의뢰자는 수집자에게 패킷 수집을 요청하는 과정에서 HI1을 사용하며 패킷의 수집 범위를 최소화할 수 있도록 구체적인 정보를 제공해야 한다. 필요시 수집자는 의뢰자에게 추가적인 정보를 요청할 수 있다.

- 수집대상, 수집기간 등 패킷 수집을 승인받은 내용(수집권한)의 증명
- 수집대상의 식별자(예: IP주소, MAC주소, 시스템 고유번호 등)
- 수집할 패킷의 유형(프로토콜, 패킷 크기 등)
- HI2 목적지 주소 및 전송 메커니즘
- HI 채널을 통한 통신에서 문제가 발생할 경우 문의할 수 있는 연락처

5.4.2 HI2: 데이터 전송 채널

HI2는 수집자가 의뢰자에게 데이터를 전송하기 위해 사용하는 단방향 채널이다. 전송하는 데이터는 의뢰자의 요청으로 수집한 데이터(패킷내용정보, 패킷부가정보)와 데이터 무결성을 검증할 수 있는 데이터를 포함해야 한다.

의뢰자에게 전송하는 데이터는 수집자가 보존하는 데이터와 동일해야 하며, 최초로 수집한 데이터의 원본성을 확인할 수 있어야 한다. 전송되는 데이터는 훼손되지 않아야 하며, 전송 과정에서 발생한 오류를 확인할 수 있어야 한다. 만약 데이터가 훼손되었을 경우, 재전송하거나 보다 안전한 방법이 강구되어야 한다. 데이터 보호를 위해 암호화된 상태로 전송이 필요할 경우에는 HI1을 이용하여 복호화할 수 있는 정보(비밀키, 암호 알고리즘 등)를 전송한다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

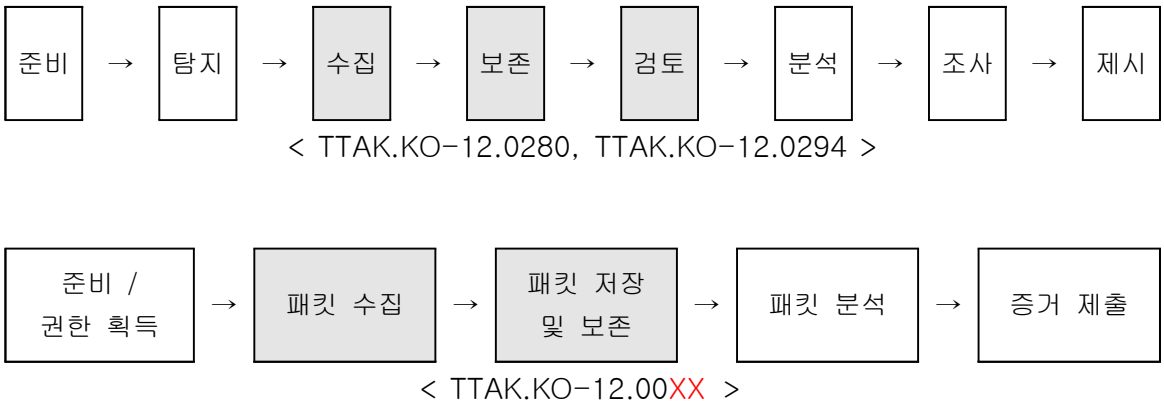
본 표준의 연계(family) 표준

Ⅰ-3.1 TTAK.KO-12.0280

본 표준은 “사이버 침해 사고 분석을 위한 네트워크 데이터 수집 및 보존 도구 요구사항” (TTAK.KO-12.0280, 2015), “사이버 침해 사고 분석을 위한 네트워크 포렌식 분석 도구 요구사항” (TTAK.KO-12.0294, 2016)을 함께 참조할 수 있다.

TTAK.KO-12.0280는 네트워크 포렌식 참조 모델 중 수집, 보존 단계를 위한 도구의 요구사항을 다루고 있으며, TTAK.KO-12.0294은 검토, 분석, 조사, 제시 단계를 위한 도구의 요구사항을 기술한다. 또한 이 표준들이 참조하는 네트워크 포렌식 조사 모델은 (그림 3-1)과 같이 본 표준과 다소 차이가 있으나, 단계를 세분화하였고 절차적으로 크게 다르지 않다.

특히, 본 표준은 네트워크 포렌식 과정에서 수반되는 패킷 수집, 저장 및 보존, 검증 절차를 상세히 기술함으로써, 패킷 데이터를 디지털 증거로서 증거능력을 갖기 위해 지켜야 할 원칙을 정의한다. 따라서 네트워크 포렌식을 위해 패킷의 처리가 필요한 경우에는 본 표준에서 제시된 절차에 따라 수행하고, 그 과정에서 사용할 도구의 요구사항은 연계 표준을 참고할 수 있다.



(그림 Ⅰ-3-1) 연계 표준과 본 표준에서 참조하는 네트워크 포렌식 조사 모델 비교

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] TTAK.KO-12.0280, 사이버 침해 사고 분석을 위한 네트워크 데이터 수집 및 보존 도구 요구사항, 2015.

[2] TTAK.KO-12.0294, 사이버 침해 사고 분석을 위한 네트워크 포렌식 분석 도구 요구사항, 2016.

[3] Public Law No. 103-414(H.R. 4992), 108 Stat. 4279, Couunications Assistance for Law Enforcement Act(CALEA), 1994

[4] J-STD-025, “Lawfully Authorized Electronic Surveillance”, TIA TR45.2 and ATIS T1-Telecommunications, 2000.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.XX.XX	제정 TTAK.KO-12.00xx	-	사이버보안 (PG503)