침해 대응

> [19반] 정민석_7000

NIST 800-86의 2장을 번역하고 분석해보았습니다. NIST 800-86의 2장은 조직 내 포렌식 역량을 구축의 여러 측면을 다룹니다. 먼저 포렌식의 필요성을 짚고, 포렌식 프로세스를 제시하며, 포렌식 인력 및 외부 팀과의 협업, 그리고 관련 정책 및 지침/절차를 제시하며, 권고사항으로 마무리합니다.

여기에서 보안과 관련된 가이드와 정보보호 정책의 유사성을 발견할 수 있어 보입니다.

먼저 NIST 800-86 2장을 시작할때, 전반적인 내용과 필요성을 다룹니다. 즉, 이 절이 왜 필요한지를 설명합니다. 마찬가지로 정보보호정책의 경우도 이 정책으로 달성하고자 하는 핵심 가치를 정보보호정책이 시작하는 부분에 적어두곤 합니다. 즉, 문서의 서두에 이 문서를 통하여 달성하고자 하는 가치와 목적을 적어두는 공통점을 파악해볼 수 있습니다.

둘째로 이러한 가이드가 적용되는 조직의 범위를 명시하고, 조직 내에서와 외부에서의 차이를 드러냅니다. NIST 800-86 2장 2절에서는 조직의 구성을, 2장 3절에서는 외부 인력과의 협업을 명시합니다. 더하여 정보보안정책에서도 회사 내부의 인력과 외부 인력에게 적용되는 정책의 범위를 달리합니다. 즉, 이 문서의 적용범위가 어디인지를 명시하고, 외부 인력에 대한 것 또한 문서에서 제공한다는 공통점을 찾아볼 수 있습니다.

셋째로 용어의 정의를 명시한다는 특징을 보입니다. 해당 문서에는 소통의 오류를 배제하기 위하여 data라는 누구나 알 법한 용어도 “특정한 방식으로 포맷된 개별 디지털 정보”라는 정의를 내립니다. 정보보호정책 또한 용어의 정의를 명확히하여, 그 의미를 확실히 하는 것을 살펴볼 수 있습니다. 즉, 용어의 명확한 정의를 통하여 오해가능성을 줄입니다.

넷째로 글의 목차에 대한 순서에도 공통적인 부분이 있어보입니다. NIST 800-86의 2장은 용어를 정의하고, 인력에 관한 내용을 제시하며, 실질적인 포렌식 기술에 대한 서술 및 대응과 관련된 내용을 순서로 서술합니다. 정보보호정책 또한 용어정의, 인력, 정보시스템 등과 같은 기술, 대응의 순으로 기술되곤 합니다. 즉, 서술하는 순서가 유사해보입니다.

지금까지 NIST 800-86 2장에서 포렌식과 관련한 내용을 기술하는 방법과 정보보호정책에서 기술하는 방법의 특징을 비교/분석해보았습니다. 보안과 관련한 가이드/문서의 경우 공통된 스키마가 있는 것처럼 보입니다. 해당 스키마를 숙지하고 체화한다면, 추후 새로운 보안 관련 문서를 습득하는 것에 도움이 되리라 생각합니다.

다음은 NIST 800-86 2장을 번역한 내용입니다.

포렌식 역량 구축 및 조직

"데이터(data)"란 특정한 방식으로 포맷된 개별 디지털 정보를 의미한다.
컴퓨터의 전문적 및 개인적 활용이 확산되고 네트워크의 보편화가 진행되면서, 다양한 출처로부터 지속적으로 증가하는 데이터를 기록하고 분석할 수 있는 도구에 대한 수요가 급격히 증가하였다. 예를 들어, 데이터는 표준 컴퓨터 시스템(예: 데스크톱, 노트북, 서버), 네트워크 장비(예: 방화벽, 라우터), 컴퓨팅 주변장치(예: 프린터), 개인용 디지털 보조기기(PDA), CD, DVD, 이동식 하드 드라이브, 백업 테이프, 플래시 메모리, USB 드라이브 및 점프 드라이브 등에 저장되거나 전송될 수 있다. 또한, 휴대전화, 비디오 게임 콘솔, 디지털 오디오 플레이어, 디지털 비디오 레코더와 같은 다양한 소비자 전자기기 역시 데이터 저장 매체로 활용될 수 있다.
이처럼 데이터 소스의 다양성이 확대되면서, 포렌식 도구와 기법의 개발 및 고도화가 촉진되었다. 또한, 이러한 도구와 기법이 범죄 수사, 컴퓨터 보안 사고 재구성, 운영 문제 해결, 우발적 시스템 손상 복구 등 다양한 목적으로 활용될 수 있다는 인식이 확산되면서 발전이 가속화되었다.

본 절(Section)은 조직 내 포렌식 역량을 구축하는 데 필요한 여러 측면을 다룬다. 우선, 포렌식 기술의 다양한 잠재적 활용 사례를 제시하고, 이어서 포렌식 프로세스에 대한 고수준 개요를 설명한다. 이후 포렌식 서비스가 일반적으로 어떻게 제공되는지, 그리고 포렌식 업무를 수행하기 위해 필요한 기술을 구축하고 유지하는 방법에 대해 지침을 제공한다. 또한, 포렌식 활동에는 조직 내 다양한 팀(예: 법률 자문팀, 물리적 보안팀 등)을 참여시킬 필요가 있음을 설명한다. 마지막으로, 포렌식과 관련된 정책, 지침, 절차가 다루어야 할 사항들(예: 역할과 책임 정의, 도구 및 기법 사용에 대한 지침 제공, 정보 시스템 수명주기에 포렌식 통합 등)을 논의한다.

본 가이드에 제시된 기술과 프로세스는 디지털 포렌식의 원칙에 기반하고 있다.
"포렌식 과학"은 일반적으로 과학을 법에 적용하는 것으로 정의된다. 디지털 포렌식(또는 컴퓨터 및 네트워크 포렌식)은 다양한 정의가 존재하나, 일반적으로 데이터의 식별, 수집, 검토, 분석을 과학적 방법으로 수행하되, 정보의 무결성을 보존하고 증거물에 대한 엄격한 체인 오브 커스터디(Chain of Custody)를 유지하는 활동을 의미한다.
조직마다 적용받는 법률과 규제가 상이하므로, 본 출판물은 디지털 포렌식 수사를 직접 수행

하기 위한 지침서로 활용하거나, 법적 조언으로 해석하거나, 범죄 수사의 근거로 삼아서는 아니 된다.
대신, 조직은 본 가이드를 참고하여 법률 고문, 법 집행 기관, 경영진 등의 폭넓은 자문을 받으며 포렌식 역량을 구축하는 출발점으로 삼아야 한다.

2.1 포렌식의 필요성

지난 10여 년 동안 컴퓨터가 연루된 범죄의 수가 증가함에 따라, 법 집행기관이 컴퓨터 기반 증거를 활용하여 범죄의 '누가, 무엇을, 어디서, 언제, 어떻게'를 규명할 수 있도록 지원하는 기업과 제품이 크게 증가하였다. 이로 인해 컴퓨터 및 네트워크 포렌식은 법정에서 컴퓨터 범죄 증거 자료를 적절히 제시할 수 있도록 발전해왔다.

포렌식 도구와 기법은 주로 범죄 수사 및 컴퓨터 보안 사고 대응(context)에서 활용되는 것으로 인식되고 있다. 즉, 의심되는 시스템을 조사하고, 증거를 수집·보존하며, 사건을 재구성하고, 사건의 현재 상태를 평가하는 데 사용된다. 그러나 포렌식 도구와 기법은 다음과 같은 다양한 업무에도 유용하게 활용될 수 있다.

- **운영 문제 해결(Operational Troubleshooting)**

  포렌식 도구와 기법은 운영 이슈를 해결하는 데에도 적용될 수 있다. 예를 들어, 잘못된 네트워크 설정을 가진 호스트의 가상적 및 물리적 위치를 찾거나, 애플리케이션의 기능적 문제를 해결하거나, 호스트의 현재 운영체제(OS) 및 애플리케이션 설정을 기록하고 검토하는 데 사용될 수 있다.

- **로그 모니터링(Log Monitoring)**

  다양한 도구와 기법을 통해 로그 항목을 분석하고 여러 시스템 간 로그를 상호 연관지을 수 있다. 이는 사고 대응, 정책 위반 식별, 감사 활동 등 다양한 목적에 기여할 수 있다.

- **데이터 복구(Data Recovery)**

  시스템에서 손실된 데이터를 복구하는 수십 종의 도구가 존재한다. 이들 도구는 실수로 또는 고의적으로 삭제되거나 수정된 데이터를 복구할 수 있으며, 복구 가능한 데이터의 양은 사례별로 상이하다.

- **데이터 수집(Data Acquisition)**

  일부 조직은 재배치되거나 퇴역 예정인 호스트로부터 데이터를 수집하기 위해 포렌식 도구를 사용한다. 예를 들어, 사용자가 조직을 떠날 때 해당 사용자의 워크스테이션에서 데이터를 수집하여 향후 필요할 경우를 대비해 저장할 수 있다. 이후 워크스테이션 매체는 원 사용자의 모든 데이터를 제거하여 초기화할 수 있다.

- **준법 감시/규제 준수(Due Diligence / Regulatory Compliance)**

기존 및 신흥 규제 요건은 많은 조직에게 민감한 정보를 보호하고, 감사 목적으로 특정 기록을 유지할 것을 요구한다. 또한 보호된 정보가 외부로 노출된 경우, 관련 기관이나 영향을 받은 개인에게 이를 통지해야 할 수도 있다. 포렌식은 조직이 이러한 요구사항을 준수하고, 적절한 주의의무(due diligence)를 수행하는 데 도움을 줄 수 있다.

상황에 관계없이, 포렌식 프로세스는 다음과 같은 기본 단계를 포함한다:

- **수집(Collection)**

  관련 데이터의 가능한 소스를 식별하고, 라벨링하고, 기록하며, 데이터를 획득하는 단계이다. 이때 데이터의 무결성이 보존되어야 한다. 수집은 일반적으로 신속하게 수행되어야 하는데, 이는 현재 네트워크 연결과 같은 동적 데이터나 배터리 기반 장치(예: 휴대전화, PDA)에서의 데이터 손실 가능성 때문일 수 있다.

- **검토(Examination)**

  수집된 대량의 데이터를 포렌식적으로 처리하여, 자동 및 수동 방법을 조합하여 관심 있는 데이터를 평가하고 추출하는 단계이다. 이 과정에서도 데이터 무결성은 반드시 유지되어야 한다.

- **분석(Analysis)**

  검토 단계의 결과를 분석하여, 수집과 검토를 수행하게 된 근본적인 질문에 답하는 데 유용한 정보를 도출하는 단계이다. 분석은 법적 정당성을 갖춘 방법과 기법을 사용하여 수행되어야 한다.

- **보고(Reporting)**

  분석 결과를 보고하는 단계이다. 이 단계에서는 사용된 조치들을 설명하고, 도구 및 절차 선택 이유를 명시하며, 추가로 수행해야 할 조치(예: 추가 데이터 소스에 대한 포렌식 검토, 취약점 보완, 기존 보안 통제 강화)를 결정하고, 포렌식 프로세스의 정책, 지침, 절차, 도구 등 개선에 대한 권고사항을 제시할 수 있다. 보고 단계의 형식성(formality)은 상황에 따라 크게 달라질 수 있다.

포렌식 프로세스에 대한 보다 심층적인 논의는 제3장(Section 3)에서 다루어진다. 또한, 제4장부터 제7장(Sections 4 through 7)까지는 다양한 유형의 포렌식 데이터(파일, 운영체제 데이터, 네트워크 트래픽, 애플리케이션 데이터)를 수집, 검토, 분석하는 방법에 대해 추가적인 정보를 제공한다.

> 주: 포렌식 프로세스에는 여러 모델이 존재한다. 각 모델의 단계는 약간씩 다르지만, 기본 원칙과 전체적인 방법론은 유사하다. 모델 간 차이는 주로 각 단계의 세부화 정도(granularity)와 특정 단계에 사용된 용어

> 에 있다. 본 가이드에서 제시하는 모델은 간단한 방식으로 포렌식 프로세스를 설명한다.

2.2 포렌식 인력 구성

사실상 모든 조직은 컴퓨터 및 네트워크 포렌식을 수행할 수 있는 역량을 갖추어야 한다.

이러한 역량이 없다면, 조직은 시스템 및 네트워크 내에서 발생한 사건(예: 보호 대상 민감 정보의 노출 등)을 식별하는 데 심각한 어려움을 겪을 수 있다.

필요성의 정도는 조직마다 다를 수 있으나, 일반적으로 조직 내에서 포렌식 도구와 기법을 사용하는 주요 사용자 그룹은 다음 세 가지로 구분할 수 있다:

- **조사자(Investigators)**

  조직 내 조사자는 대개 감찰실(Office of Inspector General, OIG) 소속이며, 부정행위 의혹을 조사하는 책임을 가진다. 일부 조직에서는 범죄와 연관될 가능성이 있는 사건이 발생할 경우, OIG가 즉시 조사를 인계받는다. OIG는 다양한 포렌식 기술과 도구를 적극적으로 활용한다. 이 외에도 조직 내 법률 고문이나 인사 부서 구성원이 조사 역할을 수행할 수 있다. 그러나 법 집행 기관이나 외부 수사기관은 조직 내부의 공식 조사자로 간주되지 않는다.

- **IT 전문가(IT Professionals)**

  이 그룹에는 기술 지원 인력, 시스템 관리자, 네트워크 관리자, 보안 관리자가 포함된다. 이들은 일상 업무(예: 모니터링, 문제 해결, 데이터 복구) 중 제한된 범위의 포렌식 기술과 도구를 사용한다.

- **사고 대응자(Incident Handlers)**

  이 그룹은 무단 데이터 접근, 시스템 부적절 사용, 악성코드 감염, 서비스 거부(DoS) 공격 등 다양한 컴퓨터 보안 사고에 대응한다. 사고 대응자는 사건 조사 과정에서 폭넓은 포렌식 기술과 도구를 사용한다.

많은 조직은 자체 인력과 외부 인력을 조합하여 포렌식 작업을 수행한다.

일례로, 일부 조직은 표준적인 포렌식 작업은 내부에서 수행하고, 전문적인 지원이 필요한 경우에만 외부 인력을 활용한다.

모든 포렌식 작업을 자체적으로 수행하고자 하는 조직조차도, 물리적으로 손상된 미디어를 복구하기 위해 데이터 복구 전문 업체에 의뢰하거나, 특수 훈련을 받은 법 집행기관 인력이나 컨설턴트를 통해 이례적인 소스(예: 휴대전화)로부터 데이터를 수집하는 경우가 있다.

이러한 작업은 일반적으로 전문 소프트웨어, 장비, 시설, 그리고 고도의 기술 전문성을 필요로 하며, 대부분의 조직은 이를 자체적으로 확보하고 유지하기 위한 높은 비용을 정당화하기 어렵다.

제3.1.2절에서 설명한 바와 같이, 조직은 사전에 어떤 포렌식 작업을 법 집행기관에 위임할지 결정해야 한다. 또한, 법적 절차에서 전문가 증언이 필요한 경우에도 외부 지원을 고려할 수 있다.

조직이 포렌식 작업을 내부 또는 외부 인력에게 위임할 때 고려해야 할 주요 요소는 다음과 같다:

- **비용(Cost)**

  데이터 수집 및 분석에 사용되는 소프트웨어, 하드웨어, 장비는 구매비용, 업데이트 및 업그레이드 비용, 유지보수비용 등 상당한 비용을 수반할 수 있다. 또한 이들 장비를 변조로부터 보호하기 위한 추가적인 물리적 보안 조치가 필요할 수 있다. 전문 포렌식 인력을 양성하는 데 필요한 교육비 및 인건비 역시 상당하다. 일반적으로, 드물게 필요한 포렌식 작업은 외부 전문업체를 이용하는 것이 비용 효율적이며, 자주 필요한 작업은 내부적으로 수행하는 것이 효율적이다.

- **응답 시간(Response Time)**

  현장에 상주하는 인력이 원격지 인력보다 포렌식 작업을 더 신속히 개시할 수 있다. 그러나 조직이 지리적으로 분산된 경우, 원격지 인력이 해당 지역 시설과 가까운 경우 본사 인력보다 더 빠르게 대응할 수 있다.

- **데이터 민감성(Data Sensitivity)**

  데이터의 민감성과 개인정보 보호 문제로 인해, 일부 조직은 외부 인력에게 하드 드라이브 이미징이나 기타 데이터 접근 작업을 맡기는 것을 꺼릴 수 있다. 예를 들어, 사건의 흔적이 남아 있는 시스템에 의료정보, 금융기록 등 민감 데이터가 포함되어 있을 수 있으며, 이러한 경우 조직은 데이터 보호를 위해 시스템을 내부 통제하에 두고자 할 수 있다. 반면, 팀 내부에 사생활 침해 우려가 존재하는 경우(예: 사고 대응팀 구성원이 사건에 연루된 것으로 의심되는 경우)에는, 독립된 제3자를 통해 포렌식 작업을 수행하는 것이 바람직할 수 있다.

포렌식 작업을 수행하는 사고 대응자는 다음과 같은 역량을 갖추어야 한다:

- 포렌식 원칙, 지침, 절차, 도구 및 기법에 대한 폭넓은 지식
- 데이터 은폐 및 파괴를 위한 반포렌식(anti-forensic) 도구 및 기법에 대한 이해
- 조직 내 주로 사용되는 운영체제(OS), 파일 시스템, 애플리케이션, 네트워크 프로토콜 등에 대한 전문성
- 시스템 및 네트워크에 대한 폭넓은 일반 지식

이러한 역량을 보유함으로써, 사고 발생 시 보다 신속하고 효과적으로 대응할 수 있다. 또한, 특정 포렌식 작업(예: 특수 애플리케이션 데이터 분석 등)에 대해 적합한 기술 전문가를 빠르게 식별할 수 있다.

포렌식 업무를 수행하는 인력은 추가적으로 다음과 같은 역할을 수행할 수도 있다:

- 수사 결과가 법정에서 활용될 경우, 사고 대응자가 법정 증언 및 결과 입증에 참여해야 할 수 있다.
- 기술 지원팀, 시스템 관리자, 네트워크 관리자 및 기타 IT 전문가를 대상으로 포렌식 교육을 제공할 수 있다.

  교육 주제에는 포렌식 도구 및 기법 개요, 특정 도구 사용법, 새로운 유형의 공격 징후 등이 포함될 수 있다.
- IT 전문가 그룹과 상호 소통 세션을 운영하여, 포렌식 도구에 대한 의견을 청취하고, 기존 포렌식 역량의 잠재적 한계를 식별할 수 있다.

사고 대응팀에서는 단일 구성원의 부재로 인해 팀의 포렌식 역량이 심각하게 저하되지 않도록, 다수의 팀원이 주요 포렌식 작업을 수행할 수 있어야 한다.

사고 대응자는 서로에게 포렌식 도구 및 기술적·절차적 주제에 대해 교육할 수 있으며, 실습 기반 훈련 및 외부 포렌식/IT 교육 과정을 통해 지속적으로 역량을 강화해야 한다.

또한, 새로운 포렌식 및 반포렌식 도구를 실험실에서 직접 사용해보는 것도 유익하며, 이는 휴대전화나 PDA와 같은 장치로부터 데이터 수집, 검토 및 분석을 익히는 데 특히 효과적이다.

사고 대응자는 최신 포렌식 기술, 기법 및 절차를 지속적으로 학습하고 최신 상태를 유지해야 한다.

2.3 다른 팀과의 협업

조직 내에서 사용되는 모든 기술(소프트웨어 포함)에 대해 한 사람이 모두 정통하기는 현실적으로 불가능하다.

따라서 포렌식 작업을 수행하는 인원은 필요한 경우 추가 지원을 받기 위해 조직 내 다른 팀 및 인력에게 협조를 요청할 수 있어야 한다.

예를 들어, 특정 데이터베이스 서버와 관련된 사고를 조사할 때, 데이터베이스 관리자가 배경 정보를 제공하고, 기술적 질문에 답변하며, 데이터베이스 문서 및 참조 자료를 제공할 수 있다면, 조사가 훨씬 더 효율적으로 이루어질 수 있다.

조직은 특히 IT 전문가, 사고 대응자 및 기타 초기 대응자들이 포렌식 활동에 있어 다음 사항을 철저히 이해하고 준비할 수 있도록 해야 한다:

- 포렌식과 관련된 역할과 책임
- 포렌식 관련 정책, 지침 및 절차에 대한 지속적인 교육
- 자신이 담당하는 기술이 사고나 기타 사건에 연루될 경우, 다른 팀과 협력하고 지원할 준비

IT 전문가 및 사고 대응자 외에도, 조직 내 다른 부서 인력 역시 덜 기술적인 역할로 포렌식 활동에 참여할 수 있다. 주요 예시는 다음과 같다:

- **경영진(Management)**

  포렌식 역량을 지원하고, 포렌식 정책을 검토 및 승인하며, 특정 포렌식 조치(예: 하드 드라이브에서 데이터를 수집하기 위해 미션 크리티컬 시스템을 6시간 동안 오프라인 상태로 전환하는 작업)를 승인하는 책임을 가진다.

- **법률 고문(Legal Advisors)**

  모든 포렌식 정책 및 상위 수준의 지침과 절차를 면밀히 검토해야 하며, 필요 시 포렌식 작업이 법적 요건을 준수하도록 추가 지침을 제공할 수 있다.

- **인사 부서(Human Resources Personnel)**

  직원 관계 문제를 처리하고 내부 사건에 대응하는 데 있어 지원을 제공할 수 있다.

- **감사 담당자(Auditors)**

  포렌식 활동 비용을 포함하여 사고가 조직에 미친 경제적 영향을 평가하는 데 기여할 수 있다.

- **물리적 보안 담당자(Physical Security Staff)**

  증거물에 접근하거나 이를 물리적으로 보호하는 데 도움을 줄 수 있다.

이러한 부서들은 포렌식 프로세스 전반에서 주도적인 역할을 하지는 않지만, 제공하는 서비스는 포렌식 활동을 지원하는 데 매우 유용할 수 있다.

팀 간 원활한 커뮤니케이션을 촉진하기 위해, 각 팀은 하나 이상의 공식 연락 담당자(Point of Contact, PoC)를 지정해야 한다.

지정된 연락 담당자는 팀 구성원의 전문 분야를 숙지하고, 지원 요청이 발생할 경우 적절한 인원에게 연결해 주는 역할을 수행한다.

조직은 관련 팀이 필요할 때 참조할 수 있도록 연락처 목록을 유지해야 하며, 해당 목록에는 다음이 포함되어야 한다:

- 표준 연락 수단(예: 사무실 전화번호)
- 긴급 연락 수단(예: 휴대전화 번호)

2.4 정책(Policies)

조직은 포렌식과 관련된 주요 고려사항—예를 들어 법 집행기관 연락, 모니터링 수행, 포렌식 정책·지침·절차의 정기 검토—을 명확히 다루는 정책을 수립해야 한다.

포괄적인 수준에서, 정책은 인가된 인력이 적절한 상황 하에서 합법적인 이유로 시스템 및 네트워크를 모니터링하고 조사를 수행할 수 있도록 허용해야 한다.

조직은 또한 사고 대응자 및 기타 포렌식 역할을 수행하는 인력을 대상으로 별도의 정책을 마련할 수 있으며, 이 정책은 보다 구체적인 행위 기준을 제공한다. 이러한 인력은 해당 정책을 숙지하고 이해해야 한다.

법률 및 규정 변경, 새로운 판례 등의 영향으로 특히 여러 관할 구역에 걸쳐 있는 조직은 정책을 자주 업데이트할 필요가 있다.

또한, 조직의 포렌식 정책은 사생활 기대권(Reasonable Expectation of Privacy) 관련 정책을 포함한 다른 조직 정책들과 일관되어야 한다.

2.4.1절부터 2.4.3절까지에서는 포렌식 관련 정책 주제들을 보다 상세히 다룬다.

2.4.1 역할 및 책임 정의(Defining Roles and Responsibilities)

포렌식 정책은 조직의 포렌식 활동을 수행하거나 지원하는 모든 인력의 역할과 책임을 명확히 정의해야 한다.

이는 사고 대응 활동뿐만 아니라, 시스템 관리나 네트워크 문제 해결과 같은 일상 업무에 수행되는 행동도 포함해야 한다.

정책에는 제2.3절에 열거된 내부 팀뿐만 아니라, 법 집행기관, 외주업체, 사고 대응 전문기관과 같은 외부 조직도 포함해야 한다.

또한, 다양한 상황별로 어떤 내부 팀 및 외부 기관과 연락해야 하는지를 명확히 규정해야 한다.

정책은 다중 관할권(jurisdictional conflicts)이 연루된 범죄—예를 들어 여러 관할 구역에서 각각 수사권을 가진 기관이 개입할 수 있는 경우—에 대한 해결 방안도 제시해야 한다.

제2.2절에서 언급했듯이, 일부 조직은 부정행위 의혹 조사를 담당하는 감찰실(OIG, Office of Inspector General)을 두고 있으며, OIG가 관할 충돌을 조정하는 데 적합할 수 있다.

일부 조직에서는 범죄 가능성이 제기되면, OIG가 즉시 조사를 인계받는다.

2.4.2 포렌식 도구 사용에 대한 지침 제공(Providing Guidance for Forensic Tool Use)

사고 대응자, 시스템 및 네트워크 관리자 등 IT 전문가, 그리고 기타 조직 구성원은 다양한 이유로 포렌식 도구와 기법을 사용한다.

이러한 기술은 많은 이점을 제공하지만, 사고 또는 고의로 오용될 경우 인가되지 않은 정보 접근이나 정보 변조·삭제(사건 증거 포함)로 이어질 수 있다.

또한, 일부 상황에서는 특정 포렌식 도구 사용이 부적절할 수 있다(예: 경미한 사건에 수백 시간의 데이터 수집 및 검토를 투입하는 것은 합리적이지 않음).

도구가 합리적이고 적절하게 사용되도록 하기 위해, 조직의 정책, 지침, 절차는 다양한 상황별로 수행해야 할 포렌식 조치와 수행해서는 안 될 조치를 명확히 설명해야 한다.

예를 들면:

- 네트워크 관리자는 운영 문제를 해결하기 위해 정기적으로 네트워크 통신을 모니터링할 수 있어야 하지만, 인가 없이 사용자의 이메일을 열람해서는 안 된다.
- 헬프데스크 요원은 특정 사용자 워크스테이션의 네트워크 통신을 모니터링하여 애플리케이션 문제를 해결할 수 있지만, 그 외 네트워크 모니터링은 허용되지 않는다.
- 일반 사용자는 어떠한 경우에도 네트워크 모니터링을 수행해서는 안 된다.

정책, 지침, 절차는 각 역할별로 평상시(예: 일상적 업무)와 특수 상황(예: 사고 대응) 하에서 허용되는 행위와 금지되는 행위를 구체적으로 정의해야 한다.

정책, 지침, 절차는 또한 **반포렌식(Anti-Forensics)** 도구 및 기법 사용에 대해서도 다루어야 한다.

4장부터 7장에서 설명하는 바와 같이, 반포렌식 소프트웨어는 타인이 데이터에 접근하지 못하도록 데이터를 은폐하거나 파괴하도록 설계되었다.

반포렌식 도구는 예를 들어, 기부할 컴퓨터에서 데이터를 안전하게 삭제하거나 웹 브라우저 캐시를 삭제해 개인정보를 보호하는 등 긍정적인 목적으로 활용될 수 있다.

그러나 포렌식 도구와 마찬가지로 악의적인 목적으로도 사용될 수 있다.

따라서 조직은 누가, 어떤 상황에서 반포렌식 도구를 사용할 수 있는지 명확히 지정해야 한다.

또한, 포렌식 도구는 민감한 정보를 기록할 수 있으므로, 정책, 지침, 절차에는 정보 보호를 위한 필수 보안 조치와,

예기치 않게 민감 정보를 노출했을 경우(예: 사고 대응자가 비밀번호나 환자 정보를 목격한 경우) 대응해야 할 요구사항을 포함해야 한다.

2.4.3 정보 시스템 수명주기에 포렌식 지원 통합(Supporting Forensics in the Information System Life Cycle)

정보 시스템 수명주기에 포렌식 고려사항을 통합하면, 사고 대응을 보다 효율적이고 효과적으로 수행할 수 있다.

다음은 그러한 고려사항의 예이다:

- 시스템의 정기적 백업 수행 및 이전 백업 데이터의 일정 기간 보존
- 워크스테이션, 서버, 네트워크 장비에 대한 감사(auditing) 활성화
- 감사 기록을 보안된 중앙 집중식 로그 서버로 전송
- 미션 크리티컬 애플리케이션에 대해 모든 인증 시도를 포함하는 감사 로깅 구성
- 운영체제 및 주요 애플리케이션 배포판 파일에 대한 해시 데이터베이스 유지 및 중요 자산에 파일 무결성 검사 도구 적용
- 네트워크 및 시스템 구성에 대한 기준(baselines) 기록 및 유지
- 다음을 지원하는 데이터 보존 정책 수립:
    - 시스템 및 네트워크 활동의 과거 기록 검토
    - 소송 및 수사와 관련된 데이터 보존 요청 준수
    - 더 이상 필요하지 않은 데이터의 적절한 삭제

이러한 고려사항 대부분은 기존 조직 정책 및 절차의 확장 개념이며, 일반적으로 별도의 포렌식 정책 문서가 아니라 관련 개별 문서에 포함된다.

2.5 지침 및 절차(Guidelines and Procedures)

제2.4절에서 언급한 바와 같이, 조직은 포렌식 작업을 수행하기 위한 지침 및 절차를 조직의 정책, 사고 대응 인력 구성 모델, 포렌식 활동 참여 팀 등을 기반으로 수립하고 유지해야 한다.

설령 포렌식 작업을 외부 기관이 수행하더라도, 조직의 내부 인력은 여전히 일정 부분 활동에 관여하게 된다.

예를 들어, 외부 기관에 지원 요청을 통보하거나, 시스템에 대한 물리적 또는 논리적 접근을 허가하거나, 수사관이 도착할 때까지 사고 현장을 보호하는 등의 역할을 수행한다.

내부 인력은 외부 기관과 긴밀히 협력하여, 조직의 정책, 지침 및 절차가 이해되고 준수되도록 해야 한다.

조직의 포렌식 지침은 포렌식 기법을 사용하여 사고를 조사하는 일반적인 방법론을 포함해야 한다.

모든 가능한 상황에 대해 개별 맞춤형 절차를 수립하는 것은 비현실적이기 때문이다.

그러나 하드 디스크 이미징, 시스템의 휘발성 정보 캡처 및 기록, 물리적 증거(예: 이동식 미디어) 확보 등 일상적으로 수행되는 작업에 대해서는 단계별(step-by-step) 절차를 개발하는 것도 고려해야 한다.

지침과 절차의 주요 목적은 다음과 같다:

- 일관성 있고
- 효과적이며
- 정확한 포렌식 작업을 지원하는 것이다.

이는 특히 향후 **형사 기소**나 **내부 징계 조치**로 이어질 수 있는 사고에 대해 매우 중요하다.

전자 로그 및 기타 기록은 변경되거나 조작될 수 있으므로, 조직은 정책, 지침, 절차를 통해 그러한 기록의 무결성을 입증할 수 있는 체계를 마련해야 한다.

정보는 점점 모든 자산이 **전자적 형태**로 존재하는 방향으로 빠르게 이동하고 있다.

공공 및 민간 부문 모두에서 특정 행위나 결정의 수행 여부, 특정 정보 항목의 존재 여부 등과 같은 전자 기록의 진정성, 신뢰성, 신빙성을 확실히 입증하는 것이 점점 더 중요해지고 있다.

과거에는 비즈니스 기록이 원본과 동등한 것으로 취급되는 경우가 많았다.

그러나 현재는 법조계 및 포렌식 커뮤니티 내 일부에서는 전자 기록이 손쉽게 생성·변경·조작될 수 있다는 점에 대해 우려를 표하고 있다.

또한, 공공 및 민간 부문 모두에서 다양한 규정 준수 이니셔티브로 인해 전자 기록의 무결성을 입증해야 할 필요성이 더욱 커지고 있다.

이러한 문제는 법률 고문 및 IT 고위 관계자와 논의해야 할 사안이며, 본 문서의 범위를 벗어난다는 점을 명확히 전제한 상태에서,

- 체계적이고 문서화되었으며,
- 합리적으로 설명 가능한 포렌식 기법

  을 사용하는 것은 의사결정자와 사고 대응자 모두에게 중요한 자원이 된다.

  여기에 로그 보존 및 분석과 같은 추가적인 방법을 병행하면 더욱 효과적이다.

포렌식 지침 및 절차는 조직의 정책과 모든 관련 법률에 부합해야 한다.

지침 및 절차 개발 시에는 기술 전문가 및 법률 고문을 품질 보증 차원에서 반드시 참여시켜야 한다.

또한, 경영진도 개발 과정에 관여하여 주요 의사결정 지점이 문서화되고,

적절한 행동 방침이 정의되어 모든 의사결정이 일관되게 이루어지도록 해야 한다.

포렌식 지침 및 절차는 증거를 법적 절차에 제출할 수 있도록 지원해야 한다.

구체적으로 다음 사항을 포함해야 한다:

- 증거의 적절한 수집 및 취급 방법
- 도구 및 장비의 무결성 유지 방법
- 체인 오브 커스터디(Chain of Custody) 유지 절차
- 증거의 안전한 저장 방법【7】

사건 대응 과정에서 모든 이벤트나 작업을 기록하는 것은 실질적으로 불가능할 수 있으나, 주요 이벤트 및 작업을 기록하는 것은 다음과 같은 장점을 가진다:

- 사고 대응 과정을 체계적으로 관리(case management)
- 보고서 작성(report writing) 지원
- 법정 증언(testifying) 준비
- 복구 작업에 소요된 시간 등 주요 활동의 날짜와 시간을 기록함으로써, 피해 비용 계산에 기여

또한, 증거를 포렌식적으로 건전하게(forensically sound) 취급하면, 의사결정자가 필요한 조치를 자신 있게 취할 수 있게 된다.

한편, 일단 수립된 지침 및 절차는 지속적으로 유지·관리되어야 한다.

경영진은 지침 및 절차를 얼마나 자주 검토할 것인지 결정해야 하며, 일반적으로 **최소 연 1회** 검토가 권장된다.

또한, 팀의 정책, 지침, 절차에 중대한 변경사항이 있을 때마다 추가 검토를 수행해야 한다.

지침이나 절차를 업데이트할 경우, 기존 버전은 법적 절차에서 활용될 가능성에 대비하여 반드시 보관해야 한다.

지침 및 절차 검토에는 초안 작성에 참여한 동일 팀들이 다시 참여해야 한다.

검토 외에도, 조직은 특정 지침 및 절차의 정확성을 검증하기 위해 실습 연습(exercises)을 수행할 수도 있다.

2.6 권고사항(Recommendations)

포렌식 역량을 구축하고 조직화하는 데 있어 주요 권고사항은 다음과 같다:

- **조직은 컴퓨터 및 네트워크 포렌식 수행 역량을 보유해야 한다.**

  포렌식은 범죄 및 부정 행위 조사, 컴퓨터 보안 사고 재구성, 운영 문제 해결, 감사 기록 유지 지원, 우발적 시스템 손상 복구 등 다양한 조직 업무에 필수적이다.

  포렌식 역량이 없으면 조직은 보호 대상 민감 정보 노출과 같은 시스템 및 네트워크 내 사건을 파악하는 데 큰 어려움을 겪게 된다.

  또한, 증거를 포렌식적으로 건전하게(forensically sound) 처리하는 것은 의사결정자가 필요한 조치를 자신 있게 취할 수 있도록 한다.

- **조직은 포렌식의 각 측면을 담당할 주체를 사전에 결정해야 한다.**

  대부분의 조직은 자체 인력과 외부 기관을 조합하여 포렌식 작업을 수행한다.

  조직은 각 작업을 누가 담당할지 결정할 때, 기술력과 능력, 비용, 응답 시간, 데이터 민감성을 종합적으로 고려해야 한다.

- **사고 대응팀은 강력한 포렌식 수행 능력을 갖추어야 한다.**

  각 주요 포렌식 활동을 수행할 수 있는 팀원이 둘 이상 확보되어야 한다.

  실습 기반 훈련(hands-on exercises), IT 및 포렌식 교육 과정, 그리고 신기술 및 도구에 대한 시연(demonstrations)은 기술 습득 및 유지에 큰 도움이 된다.

- **조직 내 다양한 팀이 포렌식 활동에 참여해야 한다.**

  포렌식 작업을 수행하는 인력은 필요 시 조직 내 다른 팀이나 개인에게 지원을 요청할 수 있어야 한다.

  지원을 제공할 수 있는 팀의 예로는 IT 전문가, 경영진, 법률 고문, 인사 부서, 감사 담당자, 물리 보안 담당자가 있다.

  이러한 팀 구성원들은 포렌식 활동에서 자신의 역할과 책임을 이해하고, 포렌식 관련 정책·지침·절차에 대한 교육을 받으며, 포렌식 작업에서 타 부서와 협력할 준비가 되어 있어야 한다.

> 【주】: 본 문서는 법 집행기관을 대상으로 하는 컴퓨터 및 네트워크 포렌식 요건을 다루지 않는다.
>
> 관련 내용은 [Electronic Crime Scene Investigation: A Guide for First Responders] 및 [Forensic Examination of Digital Evidence: A Guide for Law Enforcement] 문서를 참고할 수 있다. (http://www.ncjrs.gov/app/topics/topic.aspx?topicid=158)

- **포렌식 고려사항은 정책에 명확히 반영되어야 한다.**

포괄적인 수준에서, 정책은 인가된 인력이 적절한 상황 하에서 시스템 및 네트워크를 모니터링하고 조사를 수행할 수 있도록 허용해야 한다.

조직은 사고 대응자 및 포렌식 역할을 맡은 인력을 대상으로 보다 구체적 행동 기준을 제공하는 별도 포렌식 정책을 수립할 수 있다.

포렌식 활동에 참여할 수 있는 모든 인력은 이 정책을 숙지하고 이해해야 한다.

추가적인 정책 고려사항은 다음과 같다:

- 포렌식 정책은 포렌식 활동을 수행하거나 지원하는 모든 인력의 역할과 책임을 명확히 정의해야 한다.

  내부 팀 및 외부 기관 모두를 포함하며, 다양한 상황별로 어느 주체가 어떤 기관이나 팀과 연락해야 하는지도 명확히 규정해야 한다.

- 조직의 정책, 지침, 절차는 평상시와 특수 상황(예: 사고 대응) 모두에 대해 수행해야 할 포렌식 조치와 수행해서는 안 될 조치를 명확히 설명해야 한다.

  또한, 반포렌식 도구 및 기법 사용, 민감 정보의 우발적 노출에 대한 대응 방안도 포함해야 한다.

- 정보 시스템 수명주기에 포렌식 고려사항을 통합함으로써, 많은 사고를 보다 효율적이고 효과적으로 처리할 수 있다.

  예를 들어, 호스트에 대한 감사(auditing) 수행, 시스템 및 네트워크 활동 이력 검토를 지원하는 데이터 보존 정책 수립 등이 있다.

- **조직은 포렌식 작업을 수행하기 위한 지침 및 절차를 수립하고 유지해야 한다.**

  지침은 포렌식 기법을 사용하여 사고를 조사하는 일반적인 방법론을 포함해야 하며,

  절차는 일상적인 작업을 어떻게 수행할 것인지에 대해 단계별로(step-by-step) 설명해야 한다.

  또한, 지침 및 절차는 법적 절차에서 증거로 제출할 수 있도록 지원해야 한다.

  전자 로그 및 기타 기록은 변경되거나 조작될 수 있으므로, 조직은 정책, 지침, 절차를 통해 이러한 기록의 신뢰성과 무결성을 입증할 수 있도록 준비해야 한다.

  지침 및 절차는 정기적으로 검토하고 최신 상태를 유지해야 한다.