석사학위논문

망분리 적용 및 정착을 위한 기술적 방안에 관한 연구

- 망연계를 통한 웹 데이터 전송 방법을 중심으로 -

A Technical scheme for Network Separation

- Focusing on the Web Data Transmission -

제주대학교 대학원

융합정보보안학협동과정

정 원 치

2020년 2월

망분리 적용 및 정착을 위한 기술적 방안에 관한 연구

- 망연계를 통한 웹 데이터 전송 방법을 중심으로 -

지도교수 변 영 철
지도교수 박 남 제

정 원 치

이 논문을 융합정보보안학협동과정 석사학위 논문으로 제출함

2019년 12월

정원치의 융합정보보안학협동과정 석사학위 논문을 인준함

심사위원장 조 정 원 ㊞

위 원 박 남 제 ㊞

위 원 변 영 철 ㊞

제주대학교 대학원

2019년 12월

목 차

표 목 차

그 림 목 차

초 록

다양한 정보보안 사고가 지속적으로 발생하며, 그 방법과 피해는 점차 증가하고 있으며, 이에 따라 정보보안의 중요성도 강조되고 있다.

기업 또는 기관의 인프라 환경 구성이 중요하며, 안전한 네트워크 토폴로지를 설계하기 위해 많은 노력과 예산을 투입해야 하는 사안이다. 특히, 네트워크 망분리를 선택하는 기업 또는 기관의 도입 이유는 법령, 정보보호 평가 등을 통해 강요받기 때문만은 아니다. 4차 산업혁명시대라고 말하는 초연결 사회(Hyper-connected Society)에서 정보보안 정책으로 선택할 수 있는 네트워크 보안 선택 방법은 정보보호 장비를 통해 서버나 PC를 호스트 관점에서 차단할 수 있지만, 네트워크를 원천적으로 차단하는 망분리가 더욱 효과적이기 때문에 많은 기관과 기업들이 선택하고 있다.

그만큼 정보보안 측면에서 효과적인 것은 사실이지만 모든 기관의 망분리가 성공적으로 적용되고 안전하게 관리 되는 것은 아니다. 경영진의 낮은 의지, 업무 효율성 저하, 직원의 강한 저항, 변화관리의 실패, 기술적은 보완책 미비 등의 다양한 이유로 막대한 예산을 투입했지만 기업 상황에 맞지 않는 환경에 의해 망분리를 재투자 하는 경우가 종종 존재한다. 논리적인 망분리를 적용한 기업이 물리적인 망분리로 전환 하거나, 물리적인 망분리가 다시 논리적인 망분리로 돌아가는 경우도 있으며, 실효성 없는 껍데기 망분리를 운영하는 기관도 다수 존재한다.

이 논문을 통해 제안하고자 하는 것은 망분리 도입 시, 고려 해야 할 정책과 기술적인 망분리를 분석하여, 망분리를 잘 정착할 수 있는 방안에 대해 분석하고, 망분리 정책 안에서 업무 효율성은 증대할 수 있는 방안을 제시하고자 한다.

주요어 : 망분리, 네트워크 보안, 웹 스크래핑, 안전한 웹, 정보보안

Ⅰ. 서 론

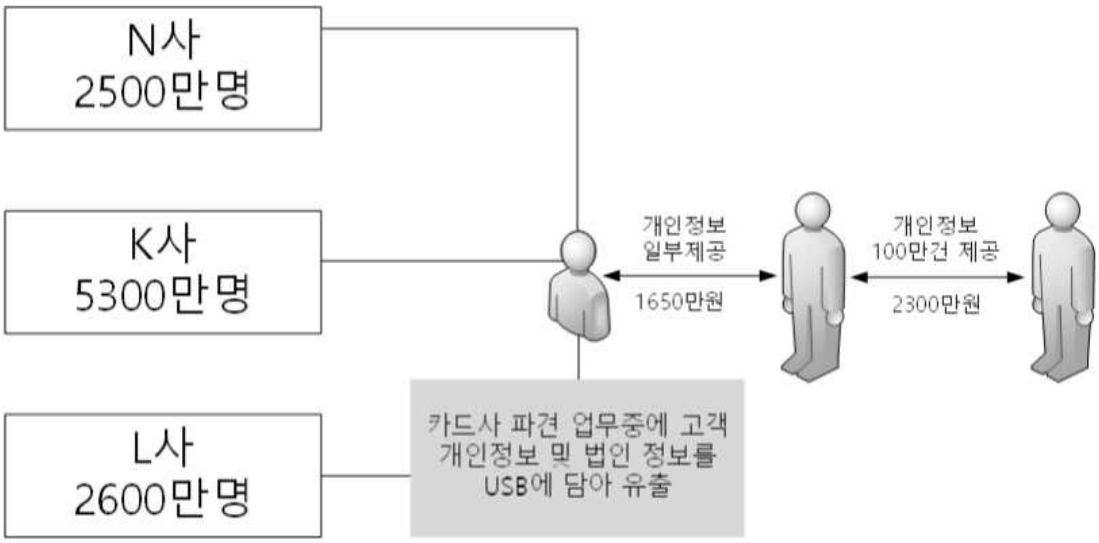
1. 연구의 배경

최근 보안위협이 증대되고, 침입과 공격방식이 날로 교묘해짐에 따라 중요정보를 보관하는 기업 및 금융권은 외부와 네트워크를 원천적으로 분리하는 망분리를 도입이 활발해지고 있다. 침해사고를 당한 기업의 피해 실태는 <그림 I-1>과 같이 나타난다.

<그림 I-1> 보안침해를 당한 기업 피해실태(시스코 2017)

정보유출이 된 기업은 유형적, 무형적 피해 입게 된다. 유형적 피해는 피해자들이 소송을 통해 위자료를 지급 받는 방법이다. 2014년 KB국민·NH농협·롯데카드 정보 유출 피해로 손해배상 청구 공동소송에 참여한 소비자들은 위자료 10만원을 받을 수 있게 됐다. 유출사건은 <그림 I-2>와 같이 금융정보회사 코리아크레딧뷰로(KCB) 직원(박모 차장)이 카드사 시스템을 개발하는 과정에서 보안프로그램이 설치되지 않은 개인용 컴퓨터로 고객 개인정보 및 사망자 폐업법인 정보를 USB에 담아 빼돌리다가 정보가 유출된 것으로 조사되었으며, 유출 규모는 1

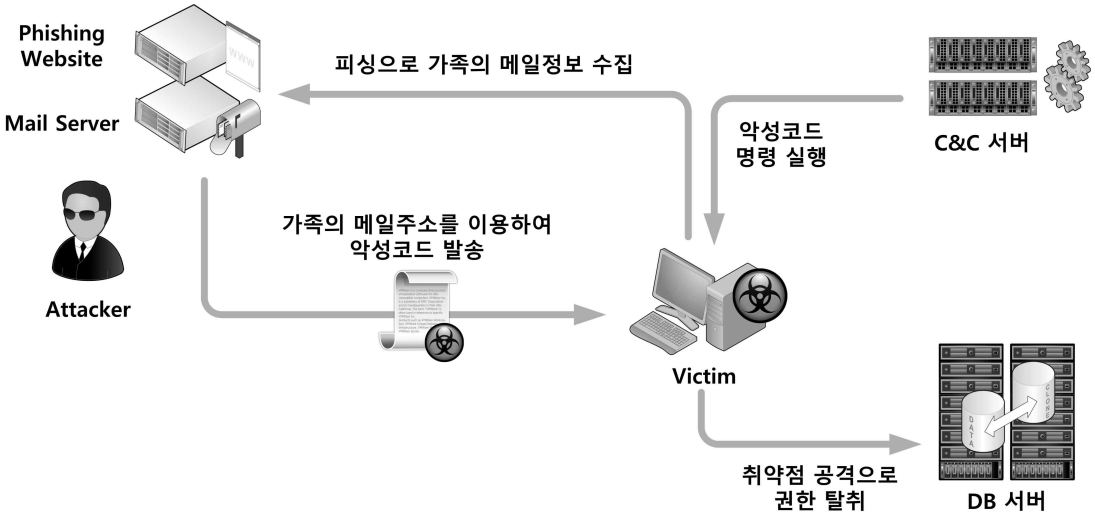
억 400만건으로 알려졌다.



<그림 I-2> 카드사 고객정보 유출사건 개요

또 다른 사례로 쇼핑몰 해킹 사례를 예로 들 수 있다. 온라인 쇼핑몰에서 일하는 직원은 업무 시간 중 사내 PC에서 인터넷 웹 메일을 확인 하던 중 '우리 가족'이라는 첨부가 되어있는 동생의 메일을 의심 없이 열람하였다. 이 과정에서 첨부파일에 있는 악성 실행파일 실행되었다. 이 악성코드는 PC에는 설치되어 공격자의 명령제어 서버(Command and Control, C&C)와 통신하여, 악성코드는 확산되며, 이와 같은 과정을 통해 내부정보를 수집하고 또 수집된 정보를 활용하여, 개인정보를 담당하는 직원의 컴퓨터를 장악하여 회사 내부 DB까지 접근하여, 개인정보를 유출하였다<그림 I-3>.

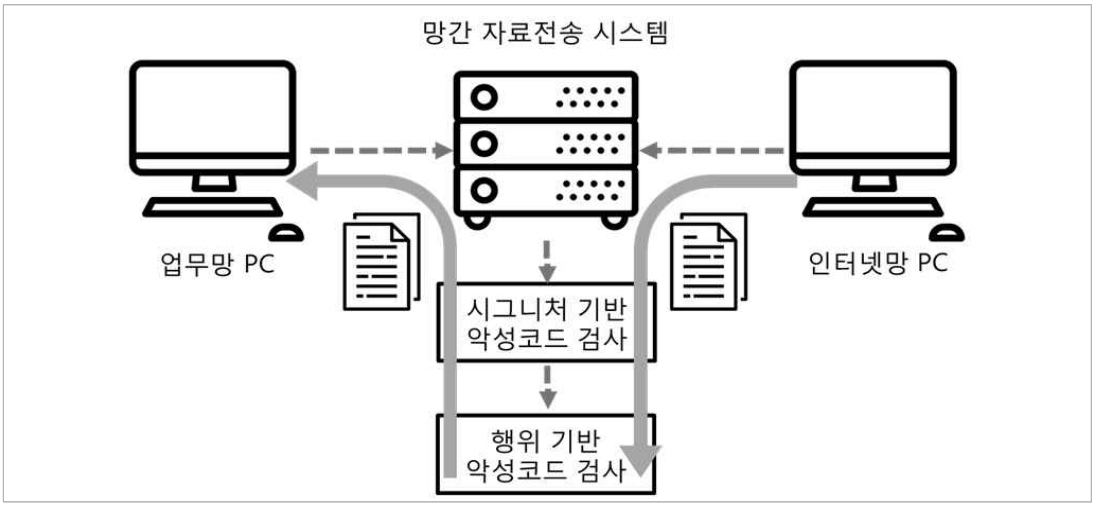
이 쇼핑몰 업체가 업무망과 인터넷 망 사이에 네트워크 망분리가 되었다면, 해킹메일을 통해 악성코드가 다운로드 되고 실행이 되어 PC 제어권이 빼앗기더라도 내부 DB의 연결 접점을 찾아 개인정보가 유출되는 사건으로 피해가 확산되지는 않았을 것이다.



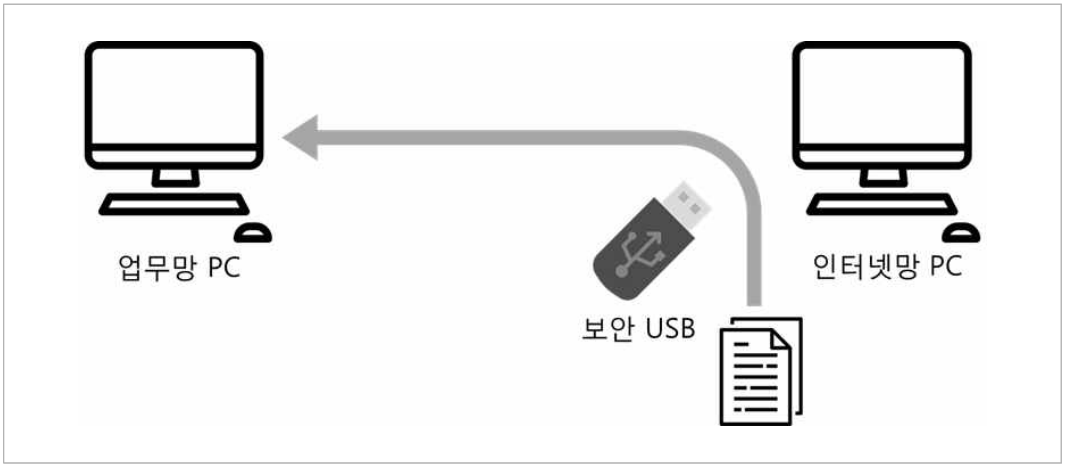
<그림 I-3> 쇼핑몰 개인정보 유출 사건

이처럼 해킹 사건이나 정보유출사건은 기업 또는 기관에게 큰 경영 리스크가 될 수 있다. 3.20 해킹사태, 카드사 개인정보 유출, 쇼핑몰 개인정보 유출 등 많은 정보보안 사고가 발생하였다. 이를 통해 많은 피해자가 속출하였으며, 그로인한 국민적인 관심과 불안감은 매우 높아져있는 상태이다. 그 이유는 많은 국민들이 중요한 업무를 인터넷을 통해 하고 있기 때문이다. 기업의 중요정보를 다루고, 정보를 가치 있게 만드는 일은 인터넷이 없이는 할 수가 없는 시대가 되어버렸으며, 금융, 자산관리, 구매, 계약은 인터넷이 없으면 이루어 질 수 없게 되어버렸다. 사용자는 이러한 개인 혹은 기업의 효율성과 편의를 위해 인터넷과 접점을 늘리려고 하지만, 반면 공격자는 인터넷과 접점을 공격하기 때문에 공격의 범위가 늘어나고 있는 상황이다. 이런 환경에서 정보보안 강화를 위해서 선택할 수 있는 선택지는 많지 않다. 안전한 네트워크 토폴로지를 구성하기 위해서 망분리라는 개념을 도입이 필수는 아니지만 최선책이라고 여겨지고 있다. 즉, 업무를 하는 내부와 외부의 네트워크를 원천적으로 분리하여 인터넷의 정보를 제한적으로 활용할 수 있도록 관리하는 정책을 만들게 되었다. 위에서 언급한 것처럼 정보보안 관점에서는 가장 안전한 최선의 선택을 하였지만, 효율적인 업무를 수행하려 하는 사용자 입장에서는 최적의 선택이라고 보긴 어렵다. 그 이유는 최신 정보나 유용한 정보를 업무에 활용하여 사용하기 위해서는 인터넷 자료를 수집

하여 자료를 만든 후, 망간 자료 전송시스템을 통해 업무망으로 들어오게 해야 한다. 이 과정에서 악성코드를 검출하는 과정을 통해 안전한 파일만을 이동시켜야 한다. 정보보안 관점에서만 말하자면 이동경로(망간접점)을 단순화 하여 접점 관리를 철저히 하는 전략이다. 이미 알려진 악성코드 패턴을 활용하여 악성코드를 판단하는 시그니처 판단과 샌드박스를 통해 가상의 PC에서 실제 파일을 실행하여 악성행위를 하는지 관찰하는 보안 솔루션을 <그림 I-4>처럼 활용한다. 이 과정은 기관의 정보보안 정책에 따라 승인 후 진행되기 때문에 불편하고, 시간이 필요하다. 다른 방법으로는 필요한 정보를 저장하여, 보안USB(보안적으로 인가된 장치)를 이용하여 안전성 조치를 확인 한 후 <그림 I-5>처럼 업무망에서 이용하여야 한다.



<그림 I-4> 망간 자료전송 시스템을 통한 업무자료 전송 프로세스



<그림 I-5> 허용된 보안 USB 업무자료 전송 프로세스

2. 연구의 목적 및 방법

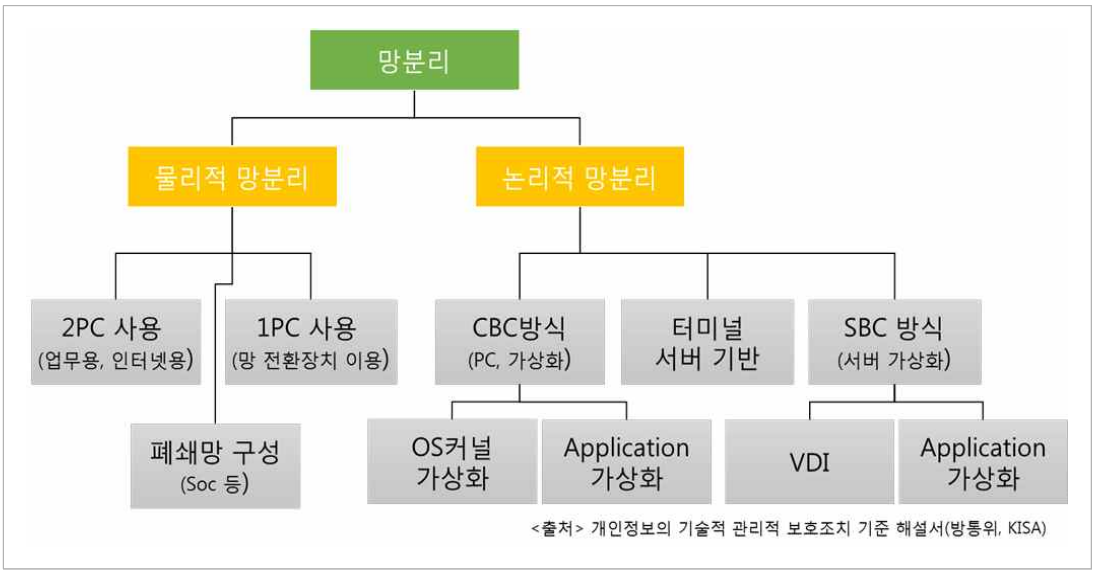
많은 정보보안 기술은 두 가지 방향으로 연구 되고 있다. 바로 차단과 탐지이다. 위에서 언급한 해킹 사건 외에도 3.20 해킹사태, 은행 해킹 사건 및 개인정보 유출 등 사고 많은 정보보안 사고가 발생하였으며, 이를 통해 많은 피해자가 속출하였다. 이로 인하여 국민적인 관심과 불안감이 높아졌다. 오늘날의 세상에서 대부분의 업무와 정보처리는 대부분 인터넷을 통해 이루어지고 있으며, 공격자는 항상 인터넷과의 접점을 공격하고자 한다. 그와 반대 입장인 정보보안 관리자(방어자) 관점에서 접점을 없애거나 최소화 하는 망분리는 효과적인 방법일 것이다.

일반적으로 망분리는 성벽과 같이 네트워크의 물리적인 접점을 차단하는 역할을 한다. 악성코드와 위협정보를 식별하는 정보보안 장비는 성문의 역할을 하는 성에 집중하여 탐지하는 방어 전략 구사하는 것이 상당하게 효율 적이다. 망분리를 실행하기 위해서 두 가지의 큰 벽이 존재 한다. 첫 번째는 상당한 예산과 상당한 유지보수 비용이다. 망분리를 실시하게 되면, 일차적으로 사용자의 PC가 한 대에서 두 대로 늘어나게 된다. 물리적 망분리인 경우 실제 PC가 한 대 늘어나게 되며, 비용이나 편의성의 목적으로 인하여 <표 I-1><그림 I-6>과 같이 논리적 망분리의 SBC 방식이나 CBC 방식의 가상 PC를 사용할 수 도 있다.

구분		운영방법	보안성	장점	단점
물리적 망분리		물리적인 두 개의 PC	높음	공격자의 직접 접근 차단	고 비용 및 비효율성
논리적 망분리	SBC	서버에서 제공하는 가상화를 별도 PC로 사용	보통	통제가 용이함 (중앙 통제 가능)	SBC 서버의 취약점에 의한 피해 확산, 네트워크 트래픽 증가
	CBC	클라이언트(PC)에 가상화된 영역을 생성하여 사용	낮음	도입비용 최소화	중앙관리 어려움

<표 1-1> 물리적 망분리와 논리적 망분리의 비교자료

망분리에 필요한 예산은 PC 외에도 PC를 구성하기 위한 S/W의 라이선스가 포함 된다. PC와 서버를 이어주는 네트워크도 2배의 장비와 네트워크 비용이 발생한다.



<그림 I-6> 망분리 방식 구분

기관의 네트워크 토폴로지에 따라 2배 이상의 비용과 사업의 난이도가 증가할 수 있다. 네트워크가 증설된 만큼 필요한 보안장비도 기존 장비의 두 배가 필요하다. 정보보안의 가장 기본적인 PC 설치형 백신, IDS, IPS, 방화벽 등도 추가적으로 필요하며, 매체제어 솔루션, WIPS, 패치관리시스템 등도 필수 장비이다. 이 부분에 대해서는 다시 알아보도록 하겠다. 이렇듯 망분리는 내부관리서버, 정보보호 장비, 정보시스템 정책 시스템 등 기존 정보시스템의 구성에 혁신적인 변경이 필요하여, 상당부분은 재투자, 중복투자도 감수해야 한다.

장비도입 및 운영을 위한 인력증원까지 따져보자면 기관의 기존 정보화 예산에 비해 상당한 예산이 필요하다는 것을 알 수 있다. 두 번째는 사용자인 기관 임직원의 변화관리이다. 이미 인터넷의 자료를 활용하여 업무를 수행하던 직원에게 인터넷이 되지 않는 업무망 PC에서 문서작업을 강제하고, 내부메일과 외부메일을 분리 구분하여, 결재 등 불편한 절차를 추가하는 망분리 체계 구축 과정은 임직원의 불만을 표출하게 만들고, 이를 통해 갈등을 야기하게 된다. 정보보안 담당은 이런 변화 관리를 위해 많은 노력을 펼치지만 새로운 정책에 따른 갈등은 심화되는 양상을 보인다. 이러한 갈등은 정보보안 조직갈등의 단계와 유형이 정보보안 종사자의 직무이탈과 정보보안 정책의 추진력을 잃게 만들기 때문에 넓은 의미의 관리·정책적 정보보안의 약화를 가져올 수도 있다.

본 논문은 정보보안을 위한 차단 우선의 정보보안 정책 방향에서 가장 마지막 단계인 망분리 정책을 적용할 경우 정보보안 담당자와 임직원 사이의 갈등의 완충제가 될 수 있는 방안을 제시하고자 한다. 분리된 망분리 환경에서 인터넷을 활용할 수 있는 방안을 제시하고, 또 이런 방법이 망분리의 정책을 위배하지 않으며, 이 방법이 보안적으로 얼마나 안전 한지를 확인하려고 한다.

3. 연구 범위와 구성

본 논문은 망분리 도입 및 정착을 위한 망간 웹 데이터 전송을 통한 연계 방법 제시를 위하여, 망분리 도입 프로세스에 필요한 기술적 방안을 먼저 분석하고 망분리를 정보보호 관리체계 관점에서 정책적 분석을 수행한다. 분석을 기반으로

한계점을 정의하고 이러한 한계를 극복할 수 있는 방안을 제시하는 것을 연구 범위로 설정하였다.

제시하는 방법이 정보보안 관점에서 망 접점이 되지 않는 다는 것은 구성관점에서 확인 하였으며, 실제 변환된 웹 데이터에 악성코드 여부를 확인하기 위해서, 글로벌 백신 업체 의 다양한 엔진을 통해 알려진 악성 시그니처가 포함되었는지를 확인하고 SandBox를 통해 행위를 분석하는 방법을 사용하였다.

이와 같은 연구 범위와 검증 방법은 실직적인 연구를 수행하기 위해 논문 작성자가 구성된 망분리 환경에서 실제 악성코드를 넘겨 보는 것이 실제적인 내부망에 위협이 되기 때문에 정해진 테스트 프로그램을 운영하고 검증하는 방법으로 연구 하며, 효과성 관련 연구도 망분리 적용 기관에 직접 도입 후에 사용자 대상의 연구를 바탕으로 진행해야 하기 때문에 이번 논문 범위에서는 제외 하고자 한다.

본 논문은 총 7개의 장으로 구성되어 있다. 제1장은 연구 배경과 목적, 그리고 범위에 대하여 기술 한다. 제2장은 네트워크 위협요소를 분석하여 망분리에 필요한 정보보안 요구사항을 도출하며, 웹데이터 연계를 위해 사용할 기반 기술을 살펴보고, 제3장에서는 네트워크 망분리 도입을 위한 기반 기술과 웹 스크래핑을 위한 기술을 분석한다. 제4장에서는 정책적 관점에서 망분리를 살펴보고 그 한계점을 분석한다. 제5장에서는 실험프로그램을 정의하고 설계 방안을 제시하며 제6장에서는 실험프로그램의 결과를 제시한다.

II. 관련연구

1. 최근 보안 사고 분석

2013년 이후 우리나라에서 발생한 주요 정보보안 사고를 살펴보고자 한다. 2013년 두 개의 은행에서 총 13만 명의 개인정보가 유출되었다. 내부자에 의하여 고

객정보를 빼돌려 대부업체 등에게 넘긴 사건이 있었다. 그 이후 국가기관인 청와대 홈페이지가 해킹에 의한 개인정보 유출 사건이 발생하였다. 이는 6.25 사이버 공격이라고 불리어 지며, 이름 생년월일, 주민번호, 등 주요 정보가 10만 여건 유출 되었다. 6.25 사이버공격은 청와대 뿐 만 아닌, 새누리당 250만명, 군장병 30만명, 주한미군 4만 여명의 개인정보를 탈취한 것으로 알려져 있다. 2014년에는 신용평가사 직원 한명이 다양한 카드회사에 파견을 나가 주요 카드사의 고객 개인정보를 유출하는 사고가 발생하였다<표 II-1>.

카드사	피해규모
K 카드사	5,300만 건 유출
L 카드사	2,600만 건 유출
N 카드사	2,500만 건 유출
중복을 제외한 피해고객	2,000만 명

<표 II-1> 2014년 카드사 개인정보 대량 유출 사건 피해규모

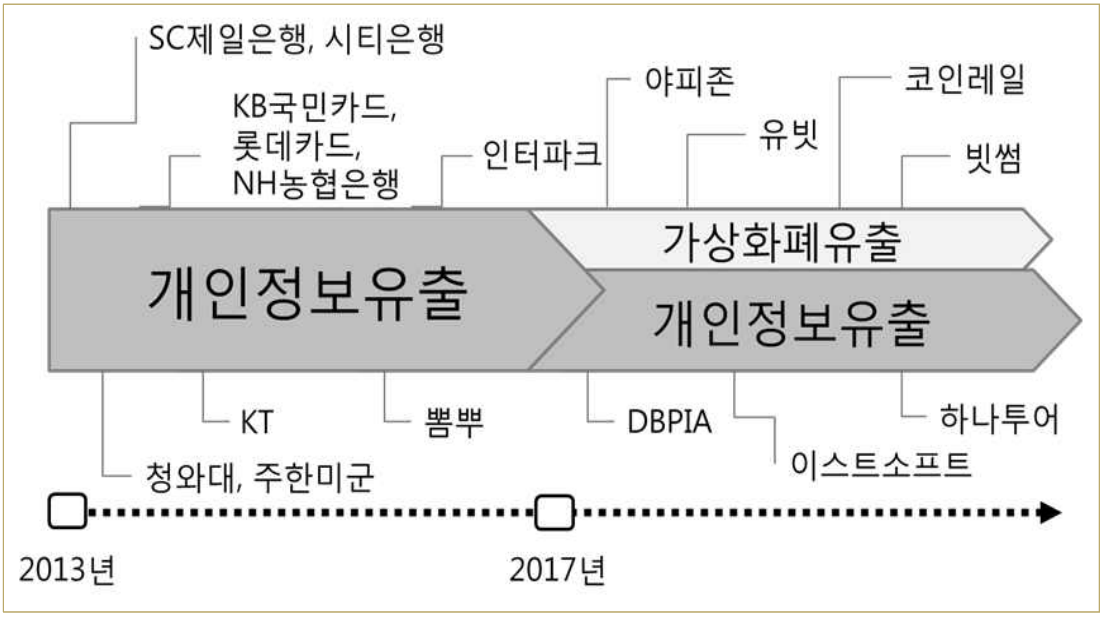
2012년 K통신사 휴대폰 가입자 873만 명의 정보를 빼돌린 일당을 검거하였다. 개인정보를 유출한 내용은 영업대리점이 회원 조회를 하는 것처럼 한 번에 조금씩 빼내는 수법을 통해서 5개월 동안 수행하여, 총 873만 명의 고객정보를 유출하였으며, 주민번호, 휴대폰 번호, 단말기 모델과 변경일 등 차후 불법 영업에 필요한 정보들이 대량으로 유출되었다. 당시 방송통신위원회는 K통신사에 과징금 7억 5300만원을 부과하였다. 그러나 다시 2014년에 K통신사는 홈페이지가 해킹당해 가입 고객 중 1,600만 명 중 1,200만 명의 고객정보가 유출 되었다. 해킹 툴을 이용하여, 하루에 20만에서 30만 명의 개인정보를 유출하여 1년간 모았다. 이들이 유출한 자료에 포함된 개인정보 역시, 이름, 주민등록번호, 휴대전화번호, 직업, 은행계좌 등 주요정보가 포함 되어 있었다.

2016년에 휴대폰 P커뮤니티 사이트에서는 해킹에 의해 190만 명의 회원정보가 유출 되는 사건이 발생하게 된다. 이에 P커뮤니티는 사과문과 함께 2차 피해 우려로 인한 비밀번호 변경을 요청 하였다.

같은 해, 인터넷 종합쇼핑몰 I사는 외부세력으로부터 해킹을 당하게 되어 1,030

만 명의 2,540만 건의 개인정보가 유출되게 된다. 메일을 통해 들어온 악성코드를 실행되어, 회사 직원의 PC가 악성코드에 감염돼 DB의 접근 권한까지 탈취되어 정보가 유출 된 것으로 보고 있다. 인터넷 종합쇼핑몰 I사 사건에서 집중해서 볼 부분은 개인정보 유출 사건으로 인한 과징금이 45억원 상당이 되며, 불복소송 1심, 2심에서도 해당 과징금을 인정했다는 것이다. 재판부는 “방통위의 처분 사유는 충분히 인정되고 과징금 산정에 있어서도 위법하거나 부당하다고 볼 수 없다”며 “이 사건으로 2500만명의 정보가 유출된 중대한 위법행위인 이상 과징금이 과하거나 하지도 않다”라고 판시하여 개인정보 유출과 정보보안 사고에 발생하는 사회적인 피해에 따른 과징금 부과를 수행을 “정보통신망 이용촉진 및 정보보호 등에 관한 법률로 규정하고 있다.(이하, 정통망법)”, 정통망법 제64조의3(과징금의 부과 등)제3호에 따라 “법을 위한하여 개인정보를 이용한 경우 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과 할 수 있다.” 라고 명시되어, 개정이전 카드사, K통신사 등 잇따른 대규모 개인정보 유출에도 적절한 처벌을 하지 않아 불안하던 국민들의 불만을 해소하고자 하며, ‘스팸 공화국’ 오명을 벗기 위한 정부 정책으로 볼 수 있다.

인터넷 종합쇼핑몰 I사의 사례는 정보보안 기업의 정보보호 의무를 확실하게 보여준 최초의 사례가 된다. 이 이후 정보보안 사고는 개인정보 유출과 가상화폐 유출로 나뉘게 된다. 기존 개인정보는 개인정보를 유출하여, 2차, 3차 불법적인 유통경로를 통해 거래를 수행해야 하지만, 가상화폐는 해당 서버를 해킹했을 경우 해당 서버에 있는 해시 값 자체가 금전으로 환산할 수 있는 정보에 해당하기 때문에 가상화폐 거래소를 공격하여 보유한 가상화폐의 해시를 유출 하는 방향으로 진화 되어가고 있다<그림 II-1>.



<그림 II-1> 2013년 이후 주요 정보보안 사고 추이

2. 네트워크 해킹 취약점 분석

1) 스니핑

네트워크 계층에서 공격은 크게 두 가지로 분류할 수 있다. 능동적 공격 방식과 수동적 공격 방법이다. 능동적인 공격 방법 중 대표적인 웜홀(wormhole)공격, 싱크홀(sinkhole)공격, 선택적 포워딩(selective forwarding)이 존재하며, 수동적 공격에서는 악의적 도청으로 알려진 스니핑(sniffing)공격이 대표적이다.

<표 II-2>에서 보는 것처럼 수동적 공격인 스니핑은 스위치 환경이나 종류에 따라 다양하게 구분 될 수 있다. 미러링 포트(mirroring port)기법은 스위치에 만일을 위해 모든 트래픽 데이터의 정보를 복제하는 포트를 이용하여 스니핑을 하는 방법을 말한다. 스위치 재밍(switch jamming)은 스위치는 주소를 저장하는 테이블이 가득 차게 되면 모든 포트로 트래픽을 브로드 캐스팅 하는 특징을 가지는 데, 이 특징을 이용하여 스위치의 주소테이블을 오버플로우 상태를 만들 후 위조된 MAC 주소를 지속적으로 네트워크를 통해 흘려보내서 스니핑을 하는 방

법이다.

공격 분류	주요 공격명	공격방법
능동적 공격	웜홀(wormhole) 공격	두 공격자가 라우팅 되는 메시지를 위조하여, 자신의 방향으로 트래픽을 가져와서 획득한 패킷을 변조하는 공격 형태
	싱크홀(sinkhole) 공격	공격자가 주변 노드들에게 데이터를 수신할 경우 데이터 수신이 완료되면, 잘못된 경로로 재전송, 또는 데이터를 소실 시키는 공격 형태
	선택적 포워딩 (selective forwarding)	메시지가 전송되는 경로에서 공격자가 점유한 노드가 패킷을 포워딩 하지 않아 다음 노드가 수신되지 못하게 만드는 공격 형태
수동적 공격	스니핑(sniffing) 공격	네트워크상에서 자신의 노드와의 통신이 아닌 다른 노드간의 패킷 교환을 도청하는 공격 형태

<표 II-2> 네트워크 계층에서의 주요 공격 분류 및 방법

ARP Redirect 공격방법은 공격자 자신의 호스트 MAC주소를 라우터로 위조하는 방법이다. 즉 ARP Reply 값에 라우터로 위장하여 브로드 캐스팅 하여 스니핑하는 방법이며, 비슷한 공격방법으로 변조된 게이트웨이를 거치게 만들어 스니핑을 가능하게 하는 ICMP Redirect 방법도 존재한다<표 II-3>.

스니핑 공격명	공격 방법
미러링 포트	스위치 모든 데이터 정보를 복제하는 포트를 이용하여 공격
스위치 재밍 (switch jamming)	스위치의 주소테이블의 공간이 없으면 트래픽을 모든 포트로 브로딩캐스팅 하는 특징을 이용하여 공격
ARP Redirect	ARP Reply(응답)을 주기적으로 오인할 수 있는 값을 브로드캐스트 하여 라우터로 오인하게 만드는 공격
ICMP Redirect	ICMP Redirect를 이용하여 공격자 노드를 라우터로 인식하게 만들어서 공격

<표 II-3> 스니핑 공격 분류 및 방법

스니핑은 일반적으로 TCP/IP에서 동작한다. 탐지하는 가장 쉬운 방법은 네트워크에 존재하지 않는 MAC주소로 ICMP를 보냈을 경우 Echo Reply 메시지를 받는다면 공격자가 스니핑 중인 것을 발견 할 수 있다. 보안 대책으로는 TLS, SSL등 암호화 프로토콜을 사용하여, 중요한 패킷을 암호화 하여 송수신 하는 방법이며, 스니핑 툴을 이용하여 탐지하는 방법이다. 또 APR table을 정적으로 구축한다면 공격을 탐지하고 방어할 수 있다.

망분리 환경에서 스니핑은 각각의 네트워크 환경에서는 정보보안 관점에서 관리가 되지 않는다면 공격이 가능할 수 있으나, 업무망-인터넷망으로 분리된 망분리에서는 원천적으로 스니핑 공격이 불가능하다. 라우터와 스위치가 물리적으로 분리되어있기 때문이다.

2) 스푸핑

스푸핑은 단어의 뜻 그대로 옮기자면 '골탕 먹이다'라는 뜻이며, 속여먹다 등 뜻으로 사용 된다. 네트워크에서 스푸핑을 송수신의 중요한 정보를 위·변조하여 공격하는 형태를 말한며, 이러한 공격에는 IP스푸핑(IP spoofing), ARP 스푸핑(ARP spoofing), DNS스푸핑(DNS spoofing) 등이 존재한다. ARP 프로토콜을 이용하여 MAC 주소를 속이는 공격을 ARP 스푸핑(ARP spoofing)이라고 하며, 해당 라우팅에 있는 노드들이 게이트웨이로 공격자의 노드를 착각하게 만드는 공격기법이다. IP 스푸핑(IP spoofing)은 IP 주소를 속이는 것으로 다른 이가 쓰는 IP 주소를 강제로 뺏어 권한을 획득 하는 것이다. 신뢰관계가 맺어진 서버, 클라이언트 확인 후 IP주소를 확보한 후 접속 시, 다시 한번 신뢰관계를 확인하지 않는 취약점을 이용한 방법이다. DNS 스푸핑(DNS spoofing)은 DNS 서버의 응답(response) 패킷이 빠른 순서로 웹 접속을 시도한다는 DNS의 특징을 이용한 공격 방법이다<표 II-4>.

네트워크 스푸핑 공격명	공격 방법
APR 스푸핑 (ARP Spoofing)	ARP 브로드캐스트를 통해 네트워크 안에 있는 MAC 주소를 변조하여, 공격노드를 게이트웨이로 바꾸는 등의 형태의 공격
IP 스푸핑 (IP Spoofing)	발신 IP(Source IP), 혹은 목적지(Destination IP)를 위조하는 방법이다. 서버클라이언트 연결이 맺어질 경우 Dos공격을 통해 서비스 거부 상태를 만들고 자신이 클라이언트로 인증 없이 접근권한을 획득하는 형태의 공격
DNS 스푸핑 (DNS spoofing)	DNS(도메인 네임 시스템)에 전달되는 IP 주소를 변조하여 DNS 서버를 장악하거나 응답값을 변조하여 공격자가 원하는 주소로 응답을 변조하는 공격방법

<표 II-4> 스푸핑 방식의 네트워크 공격 방법 요약

제대로 된 망분리 환경에서 스푸핑은 유효한 공격 방법이 될 수 없다. 망분리는 네트워크 라우터, 스위치 등 네트워크 망과 장비가 분리되어 있으며, 허용된 망간 자료전송 장치도 ARP 프로토콜이나 동일한 사설 IP 주소로 접근이 될 수 없는 구조이다. DNS서버도 업무망은 구성 된 내부 DNS서버 외에는 접근이 불가능하기 때문에 위에 살펴본 공격 유형은 망분리 환경에서는 발생할 수 없다. 단, 망이 분리된 방식이 네트워크 단계에서 물리적, 논리적으로 적절한 방법에 의해 분리된 환경이 아니라면, 위에서 살펴본 스푸핑 공격이 유효한 공격이 될 수 있다. 예를 들면, NAC에 의해 시작과 정료 지점 차단하는 방법을 통해 망이 분리되었다면, 이는 ARP를 고정(static)으로 게이트웨이를 지정하므로 NAC영향을 벗어날 수 있어, 이는 망분리를 했다고 보기 어렵다. 또한 논리적인 망 분할을 한 경우 해당 네트워크 장비가 장악되는 경우 망분리 정책을 우회 할 수 있지만 이런 경우는 네트워크 장비의 문제이므로 예외로 하기로 한다.

3) 세션 하이재킹

인터넷을 이용하여 연결을 하는 다양한 서버들은 항상 악의적인 공격에 노출되어 있다. 공격자는 다양한 기법을 활용하는데, 이중 정상적은 연결을 가장하여, 내부 보안을 무력하게 만들 수 있는 공격 기법이 존재하는데 바로 세션 하이재킹(Session Hijacking)이다. 이는 말 그대로 '세션 가로채기'의 뜻을 가진다. 세션이란 유저와 컴퓨터 사이 연결 활성화 된 상태를 의미한다. TCP 세션 하이재킹 공격 기법은 정상적인 IP로 위장하여 공격하는 부분에서 IP스푸핑(IP spoofing)과 유사한 부분이 있다. 하지만 IP 스푸핑(IP spoofing)은 상호 신뢰정보를 이용하여 공격을 시도하는 반면, TCP 세션 하이재킹은 이미 연결되어 활성화된 세션을 RST 신호를 이용하여 빼앗아 가는 부분에서 차이가 있다고 볼 수 있다. 공격 방법은 먼저 스니핑을 통해 시퀀스 번호를 획득하고 중간에 RST신호를 발생하여, 세션을 가로채는 방식으로 공격이 진행된다. 세션 하이재킹 기법에 대한 대응책으로 시퀀스 번호를 암호화 하자는 연구가 진행 되었으나, 시퀀스 넘버의 암/복호화 과정에서 나오는 오버헤드가 지연을 만들 수 있다는 주장도 있어 방어책에 있어 다양한 고려가 필요하다. 망분리 환경에서 세션 하이재킹 공격은 각 구성된 네트워크 안에서는 가능 하다. 하지만 망간을 넘어서서 세션 하지재킹은 할 수 없기 때문에 이를 통해 권한을 획득하는 방법은 망분리를 통해 외부의 공격을 차단 할 수 있다.

3. 네트워크 망분리 방식 및 특성 정의

망분리는 업무망과 인터넷망을 분리하는 강력한 차단을 통한 방법이다. 업무망과 인터넷을 분리한 기관은 그렇지 않은 기관보다 해킹으로 부터 안전하며, 이외에도 자료유출 및 침해사고 등 상당한 정보보안 관점에서도 좋은 성과를 보이고 있다. 하지만 보안강화에 따른 사용자의 불편과 업무의 효율적인 부분에 대한 연구나 개선에 대한 의견은 상대적으로 미미한 상황이다. 망분리 구축은 업무망과 외부망 선로를 두개 구성하며, 업무망과 외부망 사이에는 망간자료 전송 장치, 일방향 전송장치를 제외하고 어떤 통신도 허락하지 않는 네트워크 분리를 의미한다. 네트워크 망분리 체계 구축을 위해서 구축전과 구축후 차이를 기준으로 모

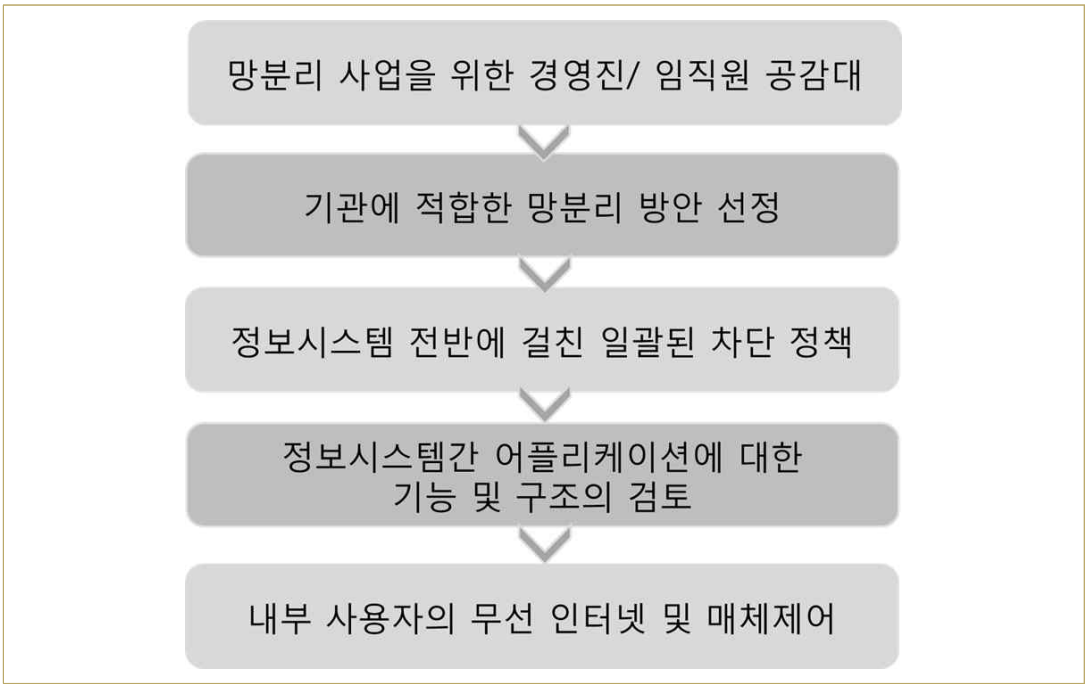
델 수립이 필요하다. 예를들면 국가 정보통신망과 연결해야 하는 공공기관인 경우는 <표 II-5> 처럼 망을 세 부분으로 분리할 필요가 있다. 망구성이 예산이나 인프라의 한계에 의해 2단계로 압축해야 할 경우는 중요한 판단을 해야 한다. 그것은 망분리 상황에서도 기관 또는 기업의 목적을 위해 외부 연동을 할 수 밖에 없는 상황들에 놓이게 된다. 그 상황에서 외부 연동망을 업무망(내부망)으로 할지 아니면 인터넷 망에서 받아 스트리밍 등 장비를 통해 업무망으로 전달 할 지에 대한 고민이 필요하다. 중요도에 따라 혼용하는 경우도 있기도 하지만 권고하는 방법은 전용선을 이용한 전용망이 구성된 경우 업무망, 인터넷 망을 이용하거나 VPN을 이용한 통신을 하는 경우는 인터넷 망을 이용하는 것 안전성이 높다고 할 수 있다.

망의 단계적 분리	망의 사용 범위
1 단계	국가정보통신망, 외부 보안 정보 수신망
2 단계	업무망(내부망)
3 단계	인터넷망(외부망)
4 단계(옵션)	SCADA(감시제어 통제망이 있는 경우)

<표 II-5> 네트워크 구성에 따른 망의 사용 범위

네트워크 망 분리를 위해서는 우선 정보시스템 식별하는 프로세스가 필요하다. 가지고 있는 정보시스템을 성격에 따라 분류 해야 한다. 즉, 대민 서비스를 위한 정보시스템, 내부 업무를 위한 인트라넷 정보시스템 영역, 정보보안을 위한 장비들이 설치된 영역, 네트워크 및 인프라 관리를 위해 필요한 장비 및 서버 영역으로 분리할 수 있으며 기업의 특성에 맞게 재정의 할 필요가 있다. 기업, 또는 기관의 업무 특성상 비밀이나 주요정보를 처리하는 정보시스템, 개인정보 등 민감정보를 다루기 위한 개인정보처리시스템은 다시 구분하여 정보시스템을 분류할 필요가 있으며, 이를 선행 작업으로 수행해야 한다. 분류된 정보시스템을 식별하였으면, 망분리를 수행할 영역을 구분하여 분배하여야 한다. 분류된 정보시스템을 성격과 중요도에 따라 등급으로 분류하고, 기업 또는 기관의 예산과 정보시스템 성격에 맞게 망분리 영역의 개수를 정해야 한다.

기업 또는 기관 망분리를 위한 결정단계를 살펴보면 <그림 II-2> 와 같이 설명할 수 있다.



<그림 II-2> 망분리 고려사항을 반영한 결정 단계

첫째, 망분리 사업 추진 전 기관내부 조직원의 공감대가 필요하다. 망분리는 기관 정보보안 담당자가 정보보호를 위한 모든 행위가 이행되고, 집중되는 단계이며, 이에 따른 책임도 집중 되어 있다.

둘째, 기관에 적합한 망분리 방식을 선정하는 것이다. 적합한 망분리 선정을 위해 정보보호의 3요소(기밀성, 무결성, 가용성)를 기준으로 하여 자산의 가치를 분석하여 분리 방식을 정할 필요가 있다.

셋째, 정보시스템 접점을 완벽하게 차단하여야 한다. 완벽한 네트워크 분리 완성을 위해 정보시스템 망분리를 하여야 한다. 일반적으로 PC, 말단 노드의 분리만을 고려하는 경우가 있는데 정보시스템, 네트워크, 정보보호시스템은 분리되어 망분리의 차단 효과를 완벽하게 구축해야 한다.

넷째, 정보시스템간 어플리케이션에 대한 기능 및 구조의 검토가 필요하다. 수

신된 사용자의 요청을 처리하고 응답하기 위해서는 다양한 응용어플리케이션이 필요하며, 이들은 다양한 프로토콜과 호환성을 담보하여야 한다. 이를 해결하기 위해서 다양한 프로토콜과 API가 망간 자료전송 시스템이나 일방향 전송장치로(스트리밍 장비)로 정상적인 연계가 되는지 확인이 필요하며, 보안적으로 안전한지 검증이 필요하다.

다섯째, 내부 사용자의 무선 인터넷 및 매체제어 통제 대책 마련이다. 대다수의 망분리 사업은 유선망을 이중으로 구성하는 방안에 중점이 되어있다. 하지만 매체나 무선망을 통제할 수 없다면 외부 위협은 망분리 이전과 동일하게 존재한다. 불법적인 매체의 차단을 위해서는 물리적인 USB 포트 차단 방식과 소프트웨어 방식인 매체제어 솔루션을 이용한 차단 그리고 무선망 차단을 위해서는 다양한 형태의 무선카드를 연결할 수 없는 구조를 만들고 업무공간에서 WIPS(Wireless Intrusion Prevention System)등을 설치하여 차단하는 등의 통제 수단이 사전에 고려되어야 한다.

다른 연구에 따르면, 정보보안 조직 갈등을 유발하는 단계 유형을 살펴보면, 잠재적인 조직 갈등의 요인들을 감정적으로 받아들이는 정보보안 종사자의 직무이탈이 높아지는 것으로 나타나고 있다. 갈등의 요소가 많은 즉, 업무편의와 상충되는 부분에서는 미리 관계자들의 의견수렴을 통해 공감대를 형성한다면, 조직내 갈등을 생산적인 방향 전환 할 수 있을 것이다.

Ⅲ. 네트워크 망분리 기반 기술 분석

1. 네트워크 망분리를 위한 보안 기술

1) NAC(Network Access Control)

정보보안 정책을 수립할 때, 앤드포인트(End point) 관리는 가장 중요하지만,

가장 어렵고 많은 업무역량을 투입해야 하는 부분이다. NAC의 주요기능은 <표 Ⅲ-1>과 같이 세 가지로 구분할 수 있다.

첫 번째는 사용자 인증이다. 비인가 장비에 대해 인증을 수행하여 사용자와 PC와 동기화를 수행하여 필요한 네트워크 권한만을 부여 할 수 있다. 기관에 특성에 따라 인사정보 시스템과 사용자 연동을 하여 PC 및 IP 지정 사용자 인증을 지원할 수 도 있다.

두 번째는 네트워크 접근제어 기능이다. 비인가 단말 네트워크 접근통제를 하며, 제조사에 따라 그룹별 네트워크 접근 제한, 불법 우회 경로를 찾아 차단하는 기능등도 제공하고, 불법 DHCP 서버를 탐지하고 차단하고 유해트래픽을 탐지하는 역할을 수행한다.

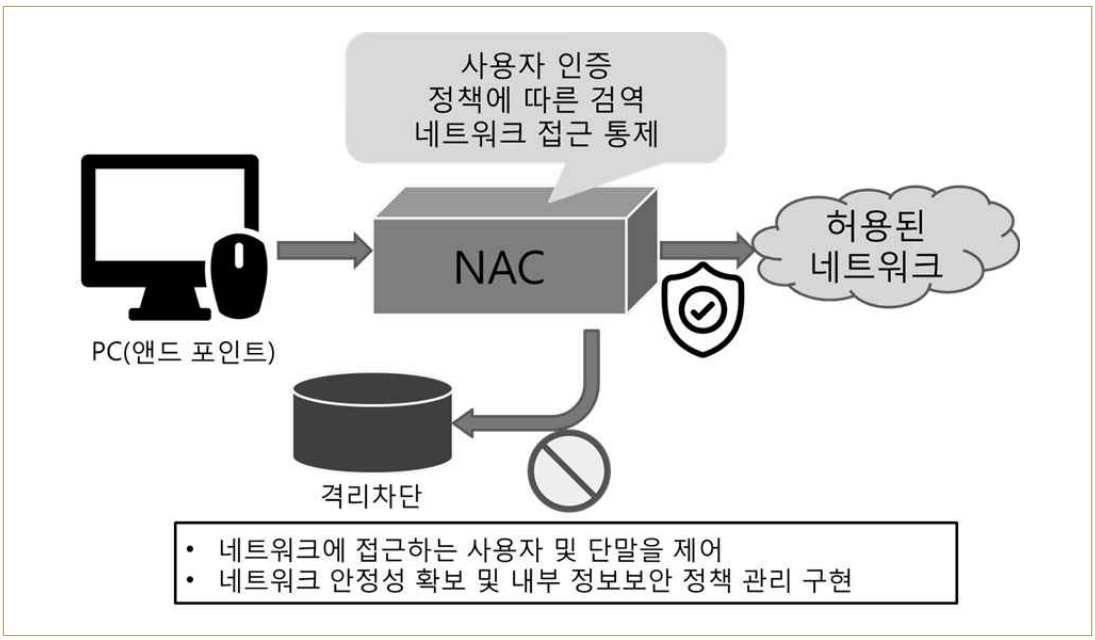
세 번째는 모니터링 및 가시성이다. 네트워크 불법접근 시도한 MAC주소를 리스트로 만들어 보여주거나 접속관리 및 에이전트 미설치자 현황을 파악 할 수 있고, 과다 트래픽을 모니터링 하고 이벤트 로그를 저장하고 이런 일련의 보안적인 요소들을 조회하고 리포트 만드는 기능을 제공한다.

NAC주요기능	기능의 상세 사항
사용자 인증	PC 등 단말에 대한 인증 및 무결성 점검 및 조치, 사용자 정보 동기화 지원
네트워크 접근제어	인가된 장비 및 단말기 네트워크 접근 통제, 그룹별 네트워크 접근 제한 불법 우회 경로 탐지 및 차단
모니터링 및 가시성	인증, 제한 사용자 현황, 단말에 대한 설치 S/W 현황, 사용자별 IP 사용현황 및 이력

<표 III-1> NAC(Network Access Control)의 주요기능

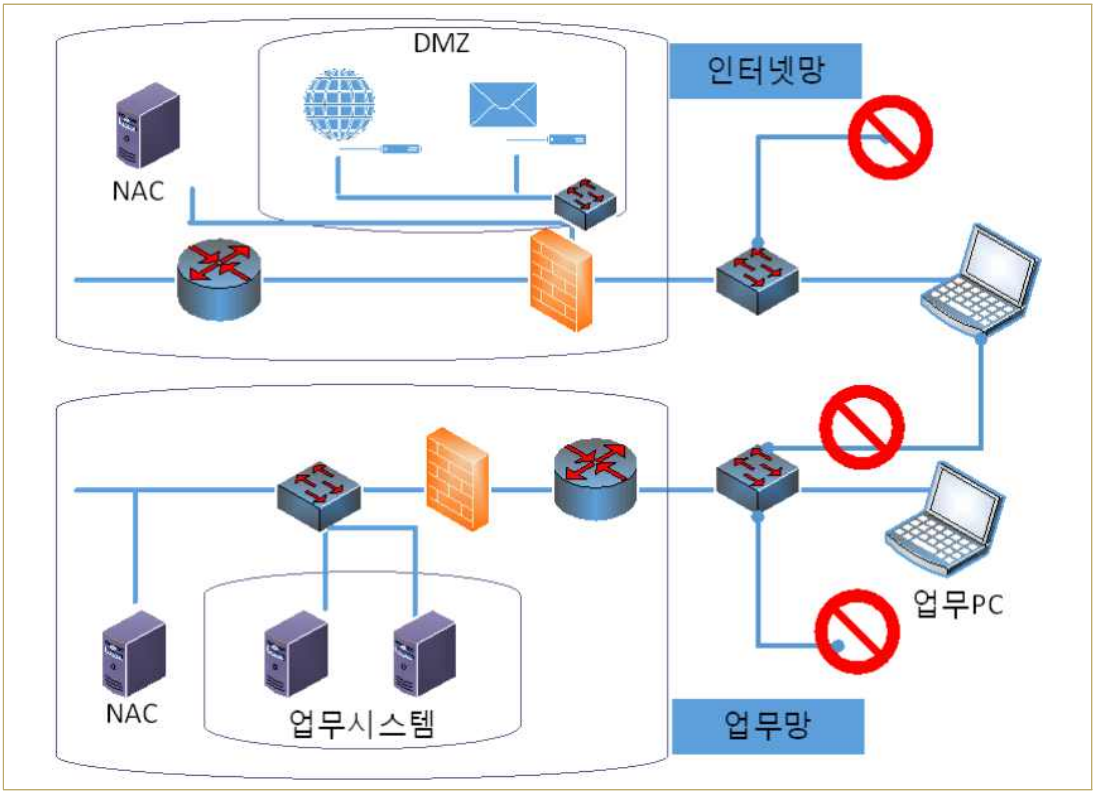
일반적인 방화벽은 외부로부터 내부 네트워크의 접근을 차단하고 관리하는 방식이라면, NAC는 내부에 네트워크를 통제하고 관리하는 기능을 주로 수행한다. 망분리 관점에서 NAC는 필수 솔루션이 된다. 업무망 PC에서 테더링이나 무

선 네트워크를 이용하여, 인터넷을 사용할 수 있다면, 망분리 통제는 이미 실패했다고 봐야 한다. 또한 외부용 PC가 내부 네트워크에 접근 통제 없이, 즉 인가되지 않은 외부 PC가 내부 네트워크에 접근이 허용되는 것도 망분리의 망접점 관리부분에서는 실패할 수 있는 부분이다. 특히 내부망, 외부망 PC의 네트워크를 교차하여 원하는 대로 사용 할 수 있다면, 정보보안 정책이 무용이 된다<그림Ⅲ-1>.



<그림 Ⅲ-1> NAC의 접근통제를 통한 통제방법

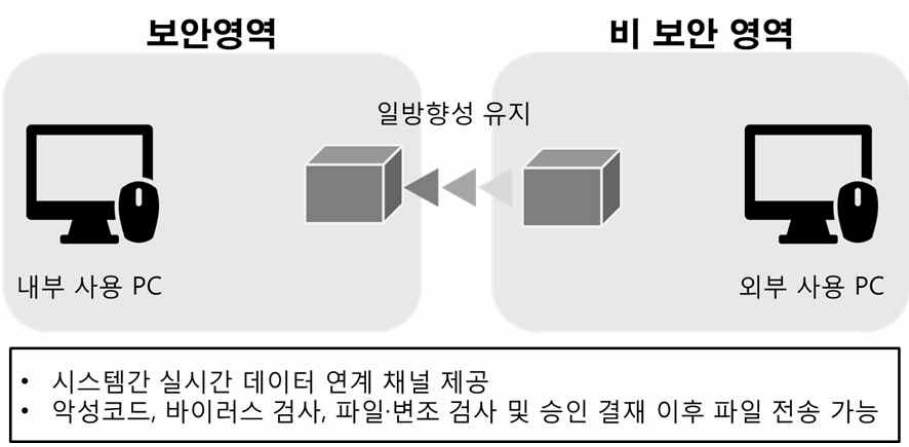
이러한 단말기를 이용한 네트워크 정책을 위해서 NAC는 반드시 필요한 필수 정보보호 장비 중에 하나라고 할 수 있다. 주의할 점은 내부망의 NAC와 외부망의 NAC는 분리해서 사용해야 한다는 것이다. 외부망에서 NAC를 공격하여 제어권한을 획득 할 경우 내부 NAC까지 무력화 되므로 망간 접점이 깨지게 때문에 NAC는 반드시 정책을 분리하여 사용할 수 있도록 해야 한다<그림 Ⅲ-2>.



<그림 Ⅲ-2> NAC가 적용된 망구성도 예시

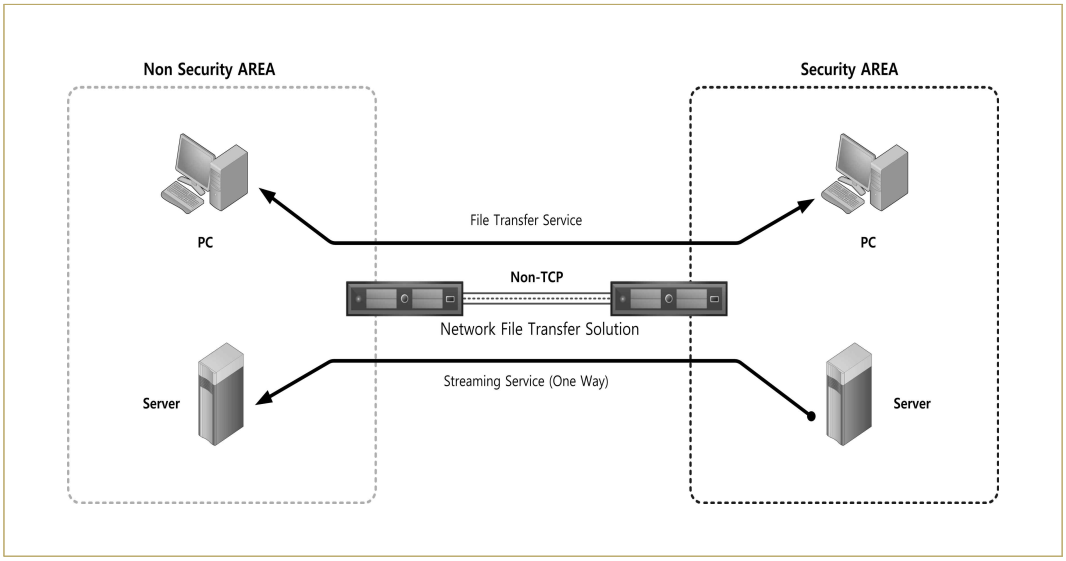
2) 망간 자료전송 장치

망분리는 물리적으로 분리된 두 개의 네트워크를 이용하지만, 망간 자료나 시스템 꼭 필요한 연결이 있을 수 있다. 사용자도 인터넷이 있는 자료를 활용하여 새로운 기획을하고 업무를 해야 하기 때문에 자료전송은 필요한 부분이다. 망분리 이후 업무망과 인터넷 망 사이에 서비스 연계 및 자료전송이 필요하다면 어떻게 구성을 해야 가장 안전한 방법으로 자료를 전송 할 수 있는지에 대해 시작했을 것이다.

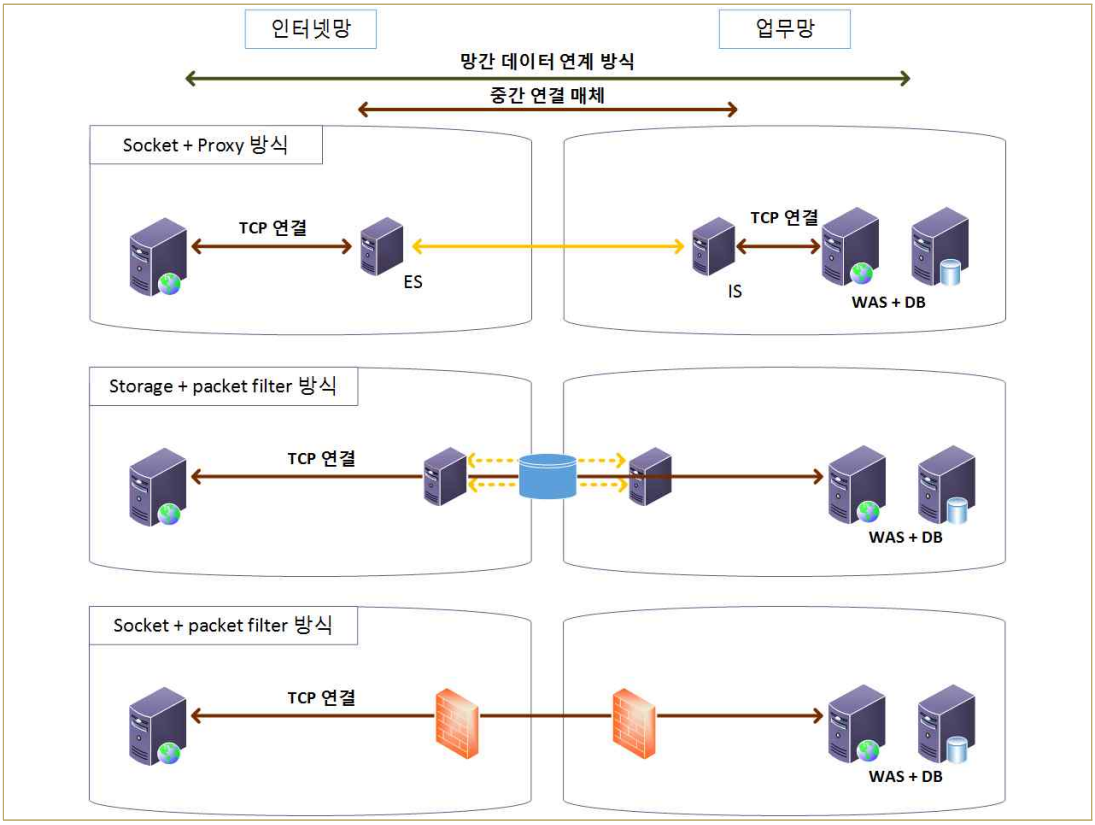


<그림 Ⅲ-3> 자료전송 장치의 기본 구조

첫 번째로 'PC to PC' 간 안전한 자료전송 방안이 필요하다<그림 Ⅲ-3>. 망 연계 방식은 실시간 연동 방식이 있고, 중계 서버 내 공유 스토리지를 통한 데이터 전송 방식이 존재한다<그림 Ⅲ-4><그림 Ⅲ-5>.



<그림 Ⅲ-4> 자료전송 장치의 연동방식 구성도



<그림 Ⅲ-5> 망간 데이터 연계방식

안전한 망간 자료전송 장치를 위해서는 응응계층의 프로토콜을 식별하여 패킷의 흐름을 허용 또는 차단하는 기능을 제공해야 한다. 또, 인가된 서버에 접근할 수 있도록 IP, MAC등에 접근통제 기능을 제공하여 단방향 접근통제를 통해 보안영역에서 비-보안영역으로만 요청이 이뤄질 수 있게 되어야 한다.

파일 및 프로토콜의 제한절차는 반드시 필요하며, 정책적으로 필요하다. 즉 허용되지 않은 비-보안영역의 연결 요청은 정책 등록 시스템에 등록된 여부를 확인하고 비인가 요청인 경우는 네트워크를 단절하여 차단하여야 한다. 또한 연결 시에도 전용 프로토콜 구간을 통해 외부에서 추측되지 않은 채널을 통해 통신하여야 한다. 파일 전송시에는 미승인 파일은 별도 격리 조치를 시켜야 하며, 승인된 파일도 보안정책에 명시된 기간 동안 파일의 전송기록과 원본파일을 보관하여야 한다. 이는 추적가능성 확보를 위해 필요하다. 파일을 전송하기 전 백신을 통해 악성코드 여부를 검사하고, 가능하다면 실제 행위기반 탐지가 가능한

APT장비 등으로 추가 점검을 하는 것을 추천한다. 실행 가능한 일부 확장자(exe, bat, scr)등은 자료 요청단계에서 차단할 필요가 있다.

망분리 환경 구축을 위해서 망연계 솔루션은 비중이 크기 때문에 각각의 솔루션을 비교하고 기관과 기업에 맞는 기술과 방식이 포함된 솔루션을 도입하는 것이 필요하다.

3) WIPS(Wireless Intrusion Prevention System)

일반적인 WIPS는 무선통신을 제공하는 AP를 공격히여 공격자가 인가된 사용자를 통해 침투하거나 내부정보를 AP를 통해 유출 또는 비인가된 AP를 사용하여 내부 네트워크게 침입하는 등의 공격을 막기 위한 방어책이다<표3-2>. 하지만 망분리 관점에서 WIPS는 내부망에 연결되어있는 PC가 외부 무선 네트워크를 통해 망분리의 접점이 생기는 것을 방어하기 위한 방어 체계라고 할 수 있다.

WIPS 주요기능	주요기능 요약
보안 공격자 제거	클라이언트 제외 정책을 통해 IP스푸핑에 대응
네트워크 정찰 및 스니핑 공격 방어	IEEE 802.11w 기반 방어체계로 관리 프레임을 암호하고 인증을 제하여 OTA(Over the Air) 공격을 방어
데이터 도난 방지	암호화 표준을 통해 네트워크와 데이터에 대한 접근을 보호함
악성 AP 잠금	유선포트 인증 모듈을 통해 악성 AP가 유선 네트워크 침범 가능성 배제

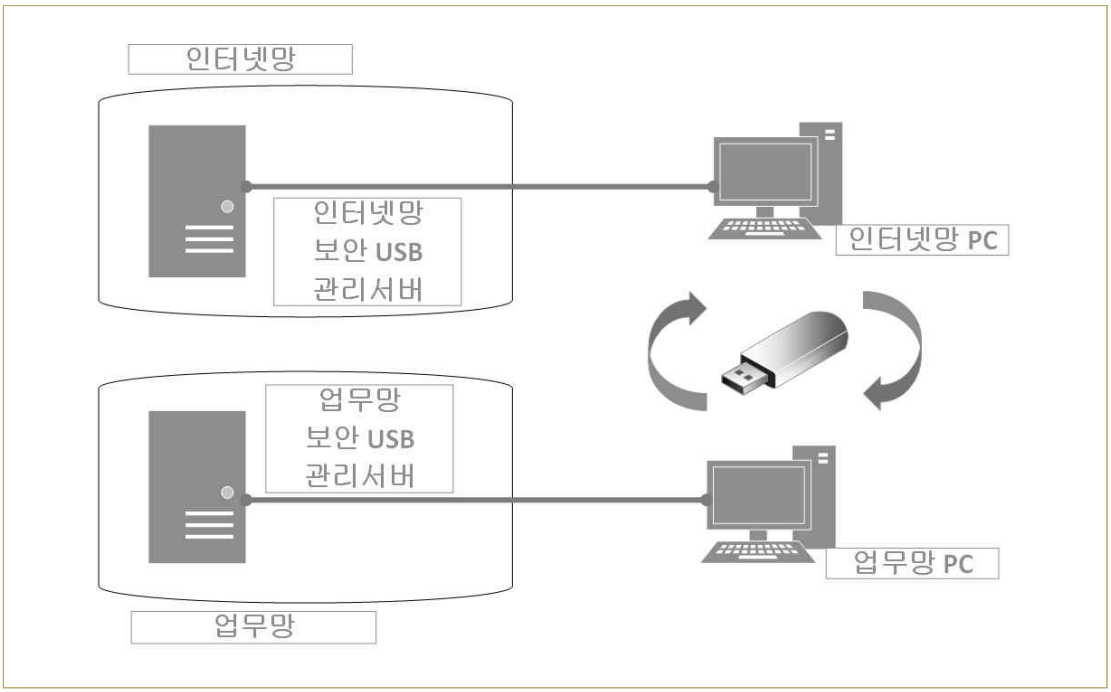
<표 Ⅲ-2> 적응형 WIPS를 통해 수행하는 보안 주요기능

이를 통해 사내에서 사설로 운영되는 불법(Rouge) AP를 차단할 수 있다. 핸드폰 핫스팟 등을 이용하는 것도 차단되기 때문에 내부망에 대한 안전성을 보장받을 수 있다.

4) 매체제어 솔루션

매체제어 솔루션은 USB 메모리, 외장형 HDD, Memory Card, 디지털 카메라, PMP, 휴대폰 등 이동식 저장 장치로 사용되는 저장 매체를 관리 제어 하는 목적의 솔루션이다. 제어하는 장치를 발견하면 보안 정책에 따라 차단/잠금/읽기 전용 등 허용 단계에 따라 허용한다.

이 솔루션은 내부망에 있는 내부 정보를 비인가된 메모리장치 등을 통해 외부로 유출 되는 것을 차단한다. 또, 핸드폰이나 외부 네트워크 장비를 차단하여 비인가 네트워크를 사용하는 것을 차단하며, 외부의 장치로부터 악성코드가 유입되는 것을 원천 차단하게 된다. 일반적으로 매체제어 솔루션은 보안 USB와 같이 사용하게 된다. 물리적 망분리 환경에서는 망간자료전송 시스템을 대신하여, 망간 보안 USB통한 자료 교환이 정책적으로 가능하다. 기관 및 기업에 맞는 방식을 선택할 수 있는 선택지 중하나라고 할 수 있다<그림 Ⅲ-6>.



<그림 Ⅲ-6> 보안 USB 장치를 통한 자료 전송

5) PMS(Patch Management System)

PC에 사용되는 OS, 소프트웨어는 새로운 취약점들이 발견된다. 발견이라는

표현을 사용한 이유는 이전까지 몰랐지만, 기술력의 발전이나 시대의 변화에 따라 이전에 안전하다고 여기는 부분에서도 그것을 이용하여, 공격을 할 수 있는 방안을 찾아내기 때문이다. 영원히 안전한 OS나 소프트웨어는 없을 것이다. 그래서 취약부분이나 버그가 발견되면 제조사는 취약한 부분을 보완할 패치(Patch)를 발표한다. 하지만 기관이나 기업입장에서는 패치가 나올 때 마다 적용하는 것도 어려운 것이 현실이다. 패치로 해결 될 수 없는 제로데이 취약성(Zero-day vulnerabilities)이라고 한다. 소프트웨어 개발사가 인지하지 못해서 패치가 아직 개발되지 않아 대응시간이 제로(zero)라서 제로데이 취약성이라고 하며, 대응하고 방어할 시간적인 여유가 없는 취약성이다. 이런 취약점을 이용한다면, 레이더에 잡히지 않는 스텔스 전투기처럼 상대방의 중심부에 치명적 공격을 할 수 있게 된다. 제로데이 취약점은 각 국 국가기관과 관련된 기업에서 해당 정보를 축적하려고 노력하고 있으며, 블랙마켓으로 불리는 불법시장에서 상당한 금액으로 거래되기도 한다. 이런 불법 거래 시장은 공개(White), 지하(Black), 회색(Gray) 시장으로 구분할 수 있다<표 Ⅲ-3>.

시장 구분	특징
공개(White)	가격이 낮고, 치명적인 취약성 정보는 희귀
지하(Black)	조직범죄, 테러집단이 이용하는 시작이며, 거래된 취약점으로 안보위기 초래
회색(Gray)	사이버공간에서의 지배력과 억지력을 확보를 위한 취약성을 주로 거래

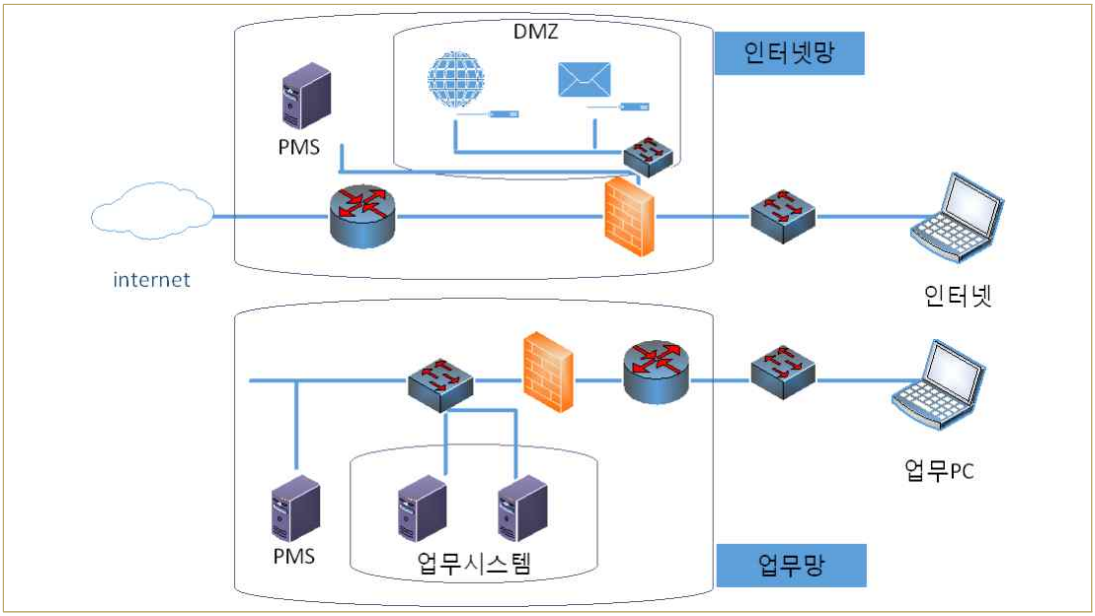
<표 Ⅲ-3> 제로데이 취약점 거래 시장 구분과 특징

공격자의 입장에서 제로데이 취약점은 강력한 무기가 될 수 있지만, 꼭 필요한 타겟에 APT공격을 할 경우에만 제한적으로 사용할 수밖에 없다. 그 이유는 첫 번째 제로데이 취약점을 이용한 공격이 널리 퍼지게 되면 보안 전문가나 사이버안전센터 관제요원 등에 의해서 해당 공격의 존재가 파악되게 되고, 해당 보안취약점 공유 채널을 통해 널리 알려지게 된다. 공유가 된 공개 취약점은 더 이

상 제로데이 취약점으로 사용할 수 없다. 소프트웨어 회사에서는 해당 취약점을 무력화 만들 취약점과 버그를 패치 하는 패치 버전을 내놓기 때문이다. 두 번째는 위에서 살펴본 제로데이 취약점 시장에서 취약점을 구매한다고 해도 상당한 비용을 지불해야 하기 때문에 최소한의 선택적인 사용을 할 수 밖에 없다.

이런 제로데이 취약점 공격에 대한 내용을 뒤집어 생각해보면, 소프트웨어 회사에서 제공하는 패치만 제시간에 업데이트 되어도 대다수의 취약점을 이용한 공격에 기관 또는 기업 보안이 뚫리는 현상은 발생하지 않을 것이다. 패치 관리 시스템(Patch Management System)은 기업에서 근무하는 유저 피씨 및 서버의 OS, 백신, 문서편집기 등 기타 소프트웨어의 패치 담당하여 패치를 권고하거나 강제적인 패치를 진행하게 된다.

망분리에서는 패치 관리 시스템(Patch Management System)은 필수 시스템이다. 그 이유는 업무망(내부망)에 존재하는 PC, 서버, 관리 지정 PC 등은 외부 업데이트 채널을 이용 할 수 없기 때문에 패치를 포기하거나 접점을 허용하는 방식이 되어야 한다. 문제점은 업데이트 서버는 IP 베이스로 특정 업데이트 서버만 오픈해서는 작동되지 않는다. 일반적으로 다양한 배포서버의 운영 때문에 대역대로 IP를 오픈해야 하기 때문에 이는 망분리의 접점관리 위배로 보안약점이 될 수 있다<그림 Ⅲ-7>.



<그림 Ⅲ-7> 망분리 환경에서 PMS 구성 방법

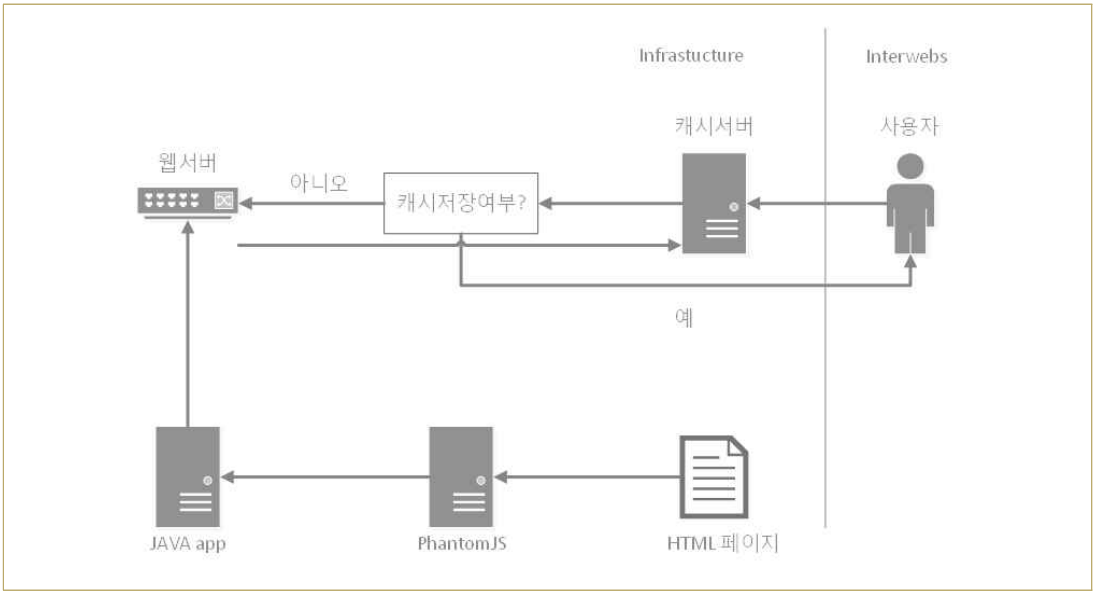
2. 웹스크레핑을 위한 기술

웹을 이용하여 웹 사이트에서 필요한 데이터를 추출하여 원하는 형태로 데이터를 복사 하여 저장하는 방법을 웹 스크래핑이라고 하며, 이를 이용하면 구조화된 체계적인 웹사이트의 정보 중 콘텐츠를 추출하여 응용프로그램을 통해 다양한 파일형식으로 저장할 수 있는 기술을 의미한다.

헤들리스 브라우저(Headless browser)란 그래픽 유저 인터페이스가 없는 웹 브라우저를 의미한다. 즉 헤더가 없는 브라우저를 구현하여 실제 웹브라우저와 유사한 환경을 구축된 프로그램을 의미한다. 이를통해 웹을 통해 할 수 있는 작업을 자동화 할 수 있다.

1) PhamtomJS

팬텀JS(phamtomJS)는 자바스크립트 운영가능한 웹킷(Webkit) 헤들리스 브라우저 플랫폼이다. 팬텀JS(phamtomJS)는 주로 헤들리스 웹 테스팅에서 사용된다. 가볍고 빠른 테스트가 가능하기 때문이고, 또한 페이지 자동화를 가능하게 한다. 접근가능하고 조작 가능한 웹페이지를 표준 DOM API를 이용하거나 JQuery를 이용 할 수 있다<그림 Ⅲ-8>.

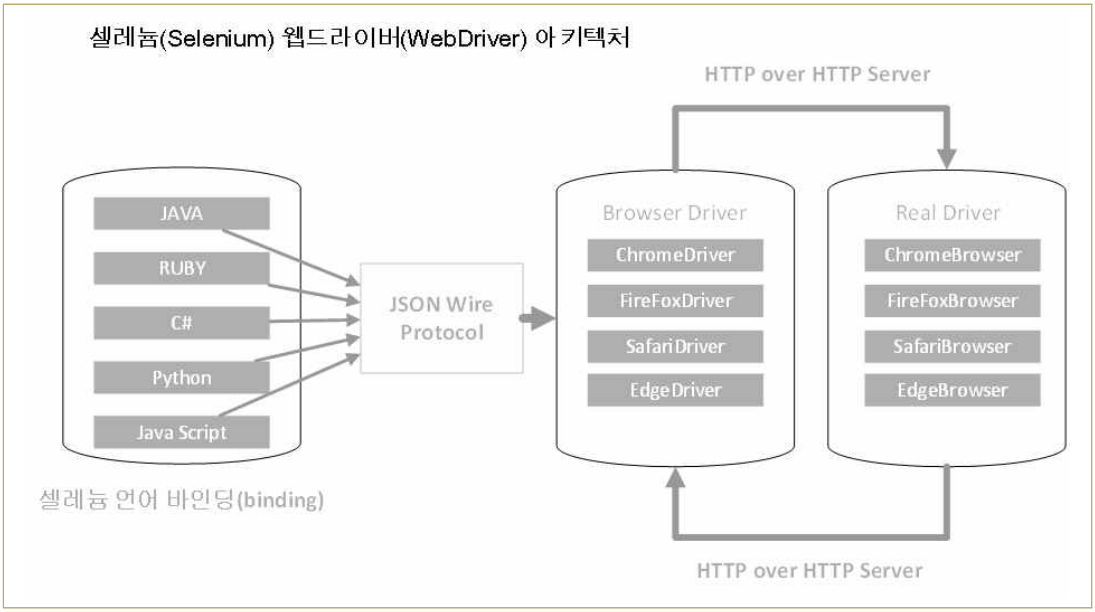


<그림 Ⅲ-8> PamtomJS를 이용한 스크래핑 구조

네트워크 모니터링을 통해 자동화된 성능 분석도 가능하다. 마지막으로 스크린 캡쳐 기능이다. 웹의 콘텐츠를 캡처 한다. 캔처된 웹에는 CSS, SVG 그리고 Canvas 가 포함되며 서버에서 구동되는 그래픽 역시 포함이 된다.

2) Selenium

셀레늄(Selenium)은 브라우저를 자동으로 처리할 수 있도록 해준다. WebDriver API를 제공하며, 이를 이용하며, 다양한 웹과 관련된 일들을 자동화 할 수 있다. 빈번한 자동테스트, 개발자에 대한 신속한 피드백이나 사용자의 정의 결점을 찾고 보고 할 수도 있다. 또 한 로드 된 화면 캡처 기능도 제공하고 있으며 구조는 <그림 Ⅲ-9>과 같다.

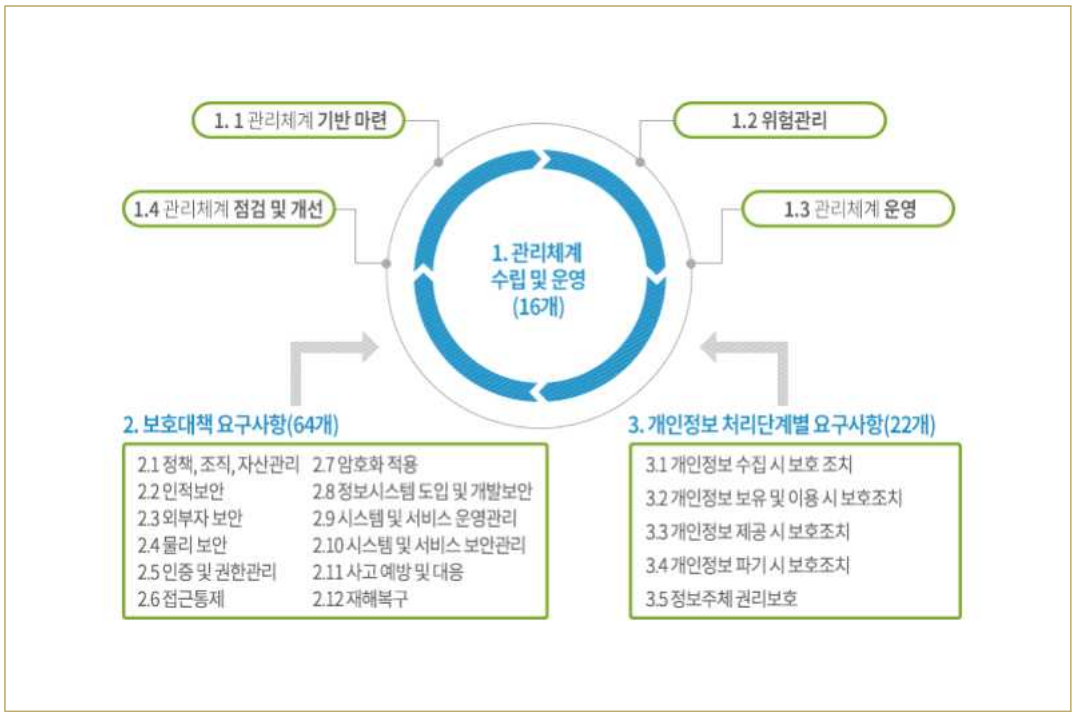


<그림 Ⅲ-9> Selenium을 이용한 스크래핑 구조

Ⅳ. 네트워크 망분리 정책적 적용 방법

1. 정보보호 관리체계 관점에서 망분리

정보보호 관리체계(ISMS)는 안전하고 신뢰있는 정보통신망 확보를 위한 관리적·기술적·물리적보호를 포함하는 종합적 관리체계를 수립하여 IT 확산 및 패러다임의 변화를 관리하고 사이버 침해 위협 증가에 대비하는 <그림 Ⅳ-1>과 같은 체계적인 위험관리체계를 위미한다.



<그림 Ⅳ-1> 정보보호 관리체계(ISMS) 인증 기준(출처:isms.kisa.or.kr)

이를 통해 정보보호 관리체계가 없을 경우 '부분적 보안·일회성 관리·산발적 대응'의 문제점을 해결하여 '균형적 보안·지속적 관리·체계적 대응'을 할 수 있다.

1) 정보보호 관리체계(ISMS) 역사

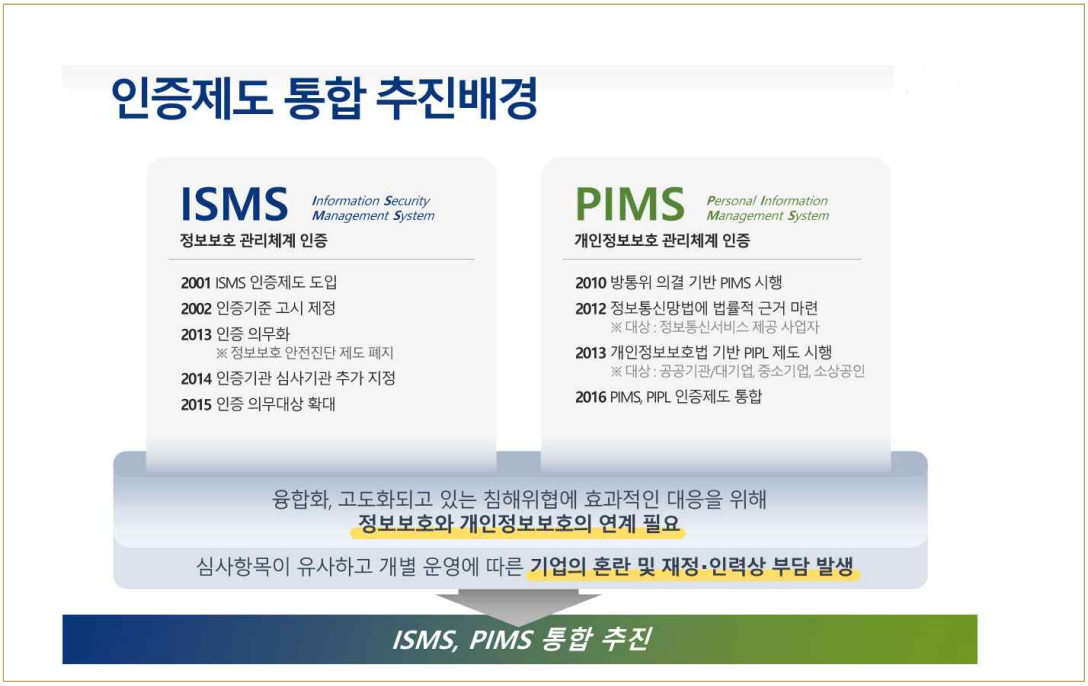
2001년에 정보보호 관리체계(ISMS)인증제도가 처음 도입 되어 관련 근거를 구성하고 2013년 인증 의무화를 추진하게 된다. 의무기관을 확대하여 현재 의무기관의 범위는 <표 Ⅳ-1> 와 같다.

대상자 기준	세부분류	비고
(ISP) 전기통신사업법의 전기통신사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자	인터넷 접속 서비스, 인터넷 전화 서비스	-
(IDC) 타인의 정보통신서비스 제공을 위하여 집적된 정보 통신시설을 운영·관리하는 사업자	서버호스팅 코로케이션 서비스 등	매출 100억 이하 VIDC 제외
(매출액 및 이용자 기준) 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 매출액이 100억 또는 일일 평균이용자 수 100만명 이상인 사업자	인터넷 쇼핑몰, 포털, 게임, 예약, Cable-SO 등	매출 100억 이상 평균이용자 100만명 이상
	상급종합병원 대학교	재학생 수 1만명 이상의 학교
※ 의무대상자 미인증 시 3,000만원 이하의 과태료		

<표 Ⅳ-1> 정보보호 관리체계(ISMS) 의무 인증대상

개인정보보호 관리체계(PIMS)는 별도로 존재 했다. 기업이 개인정보 보호 활동을 체계적·지속적으로 수해하기 위해 필요한 보호조치 체계를 구축하였는지를 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도로 활용되어 왔으며, 기업 및 기관의 부담 완화를 위해 개인정보보호 관련 유사 중복 인증제도를 통합하였다. 그래서 방송통신위원회(PIMS)와 행정자치부(PIPL)의 공동 고시(안)이 개정되었다. 개인정보에 특화된 개인정보의 라이프 사이클을 관리하고 '관리과정 요구사항', 보호대책 요구사항', '생명주기 요구사항' 등의 단계로 나누어 주기적

이고 관리적인 보호체계를 점검하는 구성이 되어있었다.



<그림 Ⅳ-2> 정보보호 관리체계(ISMS) 통합 추진 배경(출처:isms.kisa.or.kr)

(구)ISMS 인증과 (구)PIMS의 인증기준의 유사 공통 항목을 통합하고 개인정보 특화 항목을 분리하여, (구)ISMS 104개 인증기준 중 82개 항목이 PIMS 인증기준과 동일·유사하고 (구)PIMS 86개 인증기준 중 58개 항목이 ISMS 인증기준과 동일·유사하여 유사·공통 항목을 통합하여 ISMS 기준 80개, ISMS-P 기준 22개를 마련하여 인증 통합을 추진한다.

2) 정보보호 관리체계(ISMS) 필요성

지속적인 정보보호관리를 위해서는 체계적·지속적인 관리체계 수립 및 운영이 필요하다. 정보보호의 일회적이고 한시적인 대응으로는 지속적이고 안전한 체계 확립이 어렵기 때문에 새로운 보안위협의 증가에 적절한 대응을 할 수 없고, 신규 자산이 증가하고 구성의 변화에 대처할 수 없으며, 새로운 취약성의 증가에

신속한 대응을 할 수 없다. 정보보호 관리체계(ISMS) 인증을 통해 정보화 수준과 정보보호 수준의 불균형, 타율적인 점검, 부분적 보안 체계 등의 문제점을 해결할 수 있다. 정보화와 정보보호의 균형 있는 수준 확보, 위험 변화에 대응하는 지속적 관리 체계를 구축, 자율적 점검을 통한 점검 수준을 향상, 체계적인 대응과 지속적인 관리를 통해 위험의 변화에 대응하고 일부가 아닌 전사적 보안 활동을 하여 조직 스스로 지속적인 정보보호 수준 제고 및 유지를 위한 활동을 할 수 있는 체계 마련 할 수 있다.

3) 정보보호 관리체계(ISMS) 구성

정보보호 관리체계(ISMS) 인증을 위한 관리체계 수립 및 운영 인증기준은 크게 세 가지 영역으로 구분된다. 바로 '관리체계 수립 및 운영', '보호대책 요구사항', '개인정보 처리단계별 요구사항' 이다. 정보보호 관리체계(ISMS) 인증은 두 가지 인증으로 구분이 되는데 정보보호 관리체계(ISMS)은 앞에 두 항목인 '관리체계 수립 및 운영', '보호대책 요구사항' 항목을 수행하고 정보보호 및 개인정보보호 관리체계(ISMS-P)은 세 번째 항목인 '개인정보 처리단계별 요구사항' 까지 영역을 수행하여야 한다. 이 논문에서 정보보호 관리체계(ISMS) 관점에서 망분리를 바라보기 위해서 개인정보보호는 선택적 사항이기 때문에 앞에 두 가지 큰 항목에서만 분석을 하고자 한다.

정보보호 관리체계 수립 및 운영은 PDCA(Plan-Do-Check-Act)의 구성으로 세부 지표가 구성되어 있다. 세부 항목의 1.1 관리체계 기반 마련 과 1.2 위험관리는 Plan(계획) 단계 절차 확인을 의미하며, 1.3 관리체계 운영은 Do(운영) 단계의 절차 확인을 의미하며, 확인 절차를 위해 최소 2개월 이상 운영을 원칙으로 한다. 1.4 관리체계 점검 및 개선은 Check와 Act(점검 및 개선) 단계의 절차를 확인한다. 관리체계 수립 및 운영은 전사적인 정보보호 체계를 의미하며, 이는 정보보호 정책의 중요한 가이드라인 관점으로 활용 할 예정이다 '관리체계 수립 및 운영'에 관련된 항목은 <표 Ⅳ-2>과 같다.

망분리 구축을 정보보호 관리체계 1.1 관리체계기반마련 기준으로 살펴보면 정보보호 관리체계의 중요한 의사결정에 최고경영자가 의사 결정을 할 수 있도

록 해야 한다. 정보보호 담당자는 망분리의 필요성을 보고하고 망분리의 다양한 방법의 장·단점을 비교하여 의사결정을 할 수 있도록 하여, 망분리의 당위성과 추진력을 확보하는 한편, 향후 불편에 의한 불만을 최고경영진의 의사결정으로 돌릴 수 있다.

구분	분야	항목
관리체계 수립 및 운영	1.1 관리체계기반마련	1.1.1 경영진의 참여
		1.1.2 최고책임자의 지정
		1.1.3 조직 구성
		1.1.4 범위설정
		1.1.5 정책 수립
		1.1.6 자원 할당
	1.2 위험관리	1.2.1 정보자산 식별
		1.2.2 현황 및 흐름분석
		1.2.3 위험 평가
		1.2.4 보호대책 선정
	1.3 관리체계 운영	1.3.1 보호대책 구현
		1.3.2 보호대책 공유
		1.3.3 운영현황 관리
	1.4 관리체계 점검 및 개선	1.4.1 법적 요구사항 준수 검토
		1.4.2 관리체계 점검
		1.4.3 관리체계 개선

<표 Ⅳ-2> 관리체계 수립 및 운영 분야 및 항목

또한, 정보보호 최고 책임자를 지정하도록 되어있다. 망분리의 필요성과 함께 망분리를 하지 않을 경우에 어떤 위협요소가 있는지를 상세히 보고하고, 정보보안 사고 발생 시, 기관이 받는 피해 금액과 정보보호 최고 책임자가 받을 피해를 구분해서 보고하여 정보보호의 주요 사업인 망분리의 예산·인력 등 자원을 할당받을 수 있을 것이다. 이외에도 망분리를 할 수 있는 조직을 구성할 수 있도록 지원을 받을 수 있다. 정보보호를 전담하는 부서 단독으로 망분리를 진행 할 수 없기 때문에 다른 정보화 부서, 시스템 관리부서 등이 참여한 T/F 형태의 협의

체를 구성하여 업무를 추진 할 수 있을 것이다. 한 번에 전사의 모든 정보시스템을 망분리 하는 방법도 있겠지만, 사업의 기간이나 예산에 따라 본사 → 주요지점 → 각 지점의 형태로 점진적으로 진행 할 수도 있을 것이다. 이런 방법을 위해서 망분리의 범위설정이 중요하며, 현재 정보시스템의 구성, 현황을 분석하고 향후 망분리 구성의 모델을 설정할 필요가 있다. 그리고 정책을 수립해야 한다. 내부 정보보호 지침이나 정책에 망분리의 향후 정책을 수립·작성하여 알기 쉬운 형태로 임직원 및 관련자와 커뮤니케이션 하는 것도 중요하다.

다음은 1.2 위험관리 측면에서 망분리 구축을 분석해보면, 위험관리는 가장 중요한 요건이 정보자산의 식별이다. 정보보안 주요한 목적인 기밀성, 무결성, 가용성에 맞게 위험을 분석 하면, 평가방법은 수많은 방법이 존재하지만 여기서는 대표적인 몇 가지 방법을 살펴 보고기로 한다. 우선 접근방식에 따른 방법은 크게 기준선 접근법, 전문가 판단법, 상세위험접근법, 복합적 접근법으로 구분이 되며 방법의 주요내용은 <표 Ⅳ-3>과 같다.

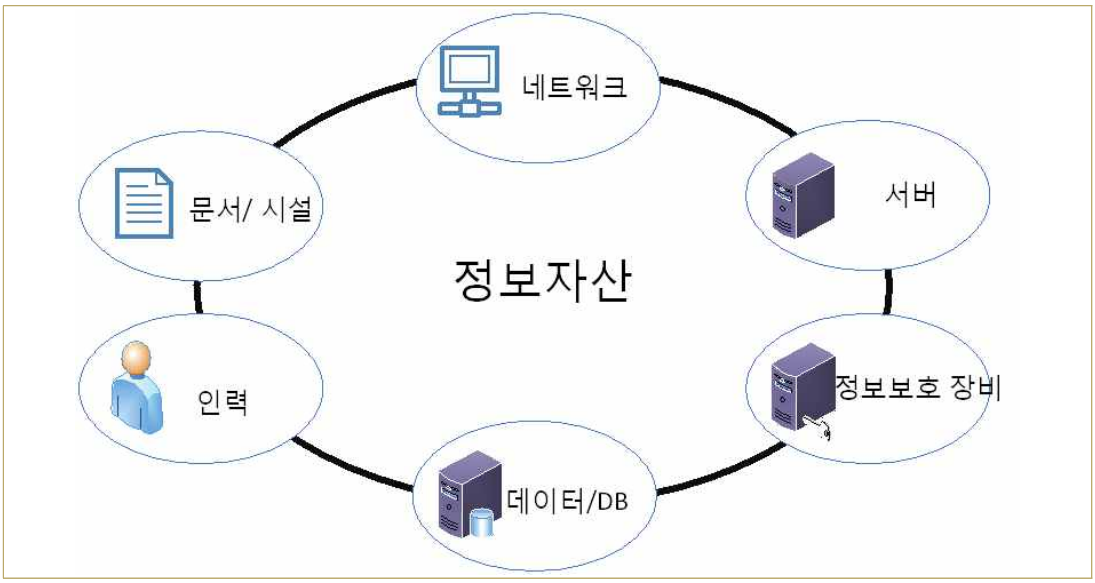
위험분석 방법론	방법의 주요 내용
기준선 접근법	모든 시스템에 적용한 기본수준을 정하고 이에 맞는 보호대책을 선택하는 방법
전문가 판단법	정형화 되지 않은 정문가의 지식과 경험에 따라 위험을 분석하는 방법
상세위험접근법	자산의 가치와 위협의 정도를 측정하고, 취약성을 분석하여 위험의 정도를 결정하는 방법
복합적 접근법	중요도가 높은 시스템에는 “상세위험접근법”을 적용하고 그렇지 않은 시스템에 대해서는 “기준선 접근법”을 적용하는 방법

<표 Ⅳ-3> 위험 분석을 위한 접근 방법론

위험방법을 위해서도 기관 또는 기업에 맞는 가용자원(전문 인력, 기간, 예산 등) 규모 등을 고려한 적절한 방법을 찾아야 한다.

위험관리의 가장 중요한 내용은 기관의 자산을 식별하고, 전 영역에 대한 정보시스템, 정보서비스의 현황과 흐름을 분석하여, 위험도를 평가하고 대책을 수립하는 일련의 과정이다. 망분리 관점에서는 현재 식별된 자선과 업무 흐름을 통해 망분리 구축 시 업무망과 인터넷을 나누는 장비, 서비스의 기준을 잡기가 명확해 지며, 이를 통해 좀 더 현실적인 예산을 산정할 수 있을 것이다. 다른 관점에서 본다면, 현재 망분리가 안되어 있는 구성에서 정보자산을 식별하고 현황을 파악하여 위험평가를 수행했을 때, 그 위험도에 따라 보호대책으로 망분리를 도출 할 수도 있을 것이다<그림 Ⅳ-3>.

지금까지 망분리를 추진하기 위한 계획(Plan) 단계를 통해 망분리 구축을 주장했다면, 1.3 관리체계 운영 관점에서 망분리는 구축이후 운영에 대해 고려할 수 있는 방법을 제공할 것이다. 망분리가 강력한 정보보호대책 중 하나인 것을 명백한 사실이지만, 망분리 이후 정보보호 대책과 그에 따른 정책과 수립된 정책에 운영 활동이 따르지 않는다면, 취약한 부분은 남아 위험요소가 될 수 있다. 또한, 망분리 이후 운영 측면에서 인력 관리에 대한 대책도 고려해야 한다. 예를 들면 네트워크 담당자가 기존에 관리하는 네트워크 장비가 10대이면, 망분리 이후에는 2배 이상 즉, 20대 이상을 관리가 필요하기 때문에 인력 충원이 필요하다면, 관리체계 기반마련 시에 반영하여야 할 것 이다.



<그림 Ⅳ-3> 정보자산의 분류 범위

이런 관리체계는 법적준거성을 확인하고, 정책이 잘 수행되고 있는지 점검하고 필요하다면 개선하는 1.4 관리체계 점검 및 개선의 과정이 필요하다. 현재 분석된 결과(위험분석 결과) 가상시나리오를 적용하고 그 결과를 관찰하여 가장 적합한 보호대책을 도출 할 필요가 있다.

정보보호 관리체계(ISMS)에서 보호대책 요구사항 정의를 위해서는 정보보호대책을 선택하고 결정된 정보보호대책에 따라 관리되어야 할 Risk를 도출 할 수 있을 것이다. 가장 먼저 수용 가능한 위험(Acceptable Risk)와 수용 불가능한 위험(Unacceptable Risk)를 식별하기 위해 DoA(수용 가능한 위험수준)을 결정해야 한다. 위험분석 및 평가에 의거하여 위험 대응 방안의 전략 설정이 필요하다<표 Ⅳ-4>.

구분	내용
위험수용	위험을 받아들이고, 손실비용을 감수 보호대책의 비용 > 손실발생확률 × 손실액
위험감소	위험을 감소할 수 있는 대책을 구현 - 보호대책의 비용 > 손실발생확률 × 손실액
위험회피	위험이 존재하는 프로세스, 사업을 포기
위험전가	잠재적 비용을 제3자에게 이전하거나 할당함 실직적인 보호 대책수립 외 보완 대책으로 사용 가능

<표 Ⅳ-4> 위험 대응 방안 단계

구분	분야	항목
보호대책 요구사항	2.1 정책, 조직, 자산관리	2.1.1 정책의 유지관리
		2.1.2 조직의 유지관리
		2.1.3 정보자산 관리
	2.2 인적보안	2.2.1 주요 직무자 지정 및 관리
		2.2.2 직무 분리
		2.2.3 보안 서약

		2.2.4 인식제고 및 교육훈련
		2.2.5 퇴직 및 직무변경 관리
		2.2.6 보안 위반 시 조치
	2.3 외부자 보안	2.3.1 외부자 현황관리
		2.3.2 외부자 계약 시 보안
		2.3.3 외부자 보안 이행 관리
		2.3.4 외부자 계약 변경 및 만료 시 보안
	2.4 물리보안	2.4.1. 보호구역 지정
		2.4.2 출입통제
		2.4.3 정보시스템 보호
		2.4.4 보호설비 운영
		2.4.5 보호구역 내 작업
		2.4.6 반출입 기기 통제
		2.4.7 업무환경 보안
	2.5 인증 및 권한관리	2.5.1 사용자 계정 관리
		2.5.2 사용자 식별
		2.5.3 사용자 인증
		2.5.4 비밀번호 관리
		2.5.5 특수 계정 및 권한관리
		2.5.6 접근권한 검토
	2.6 접근통제	2.6.1 네트워크 접근
		2.6.2 정보시스템 접근
		2.6.3 응용프로그램 접근
		2.6.4 데이터베이스 접근
		2.6.5 무선 네트워크 접근
		2.6.6 원격접근 통제
		2.6.7 인터넷 접속 통제
	2.7 암호화 적용	2.7.1. 암호정책 적용
		2.7.2 암호키 관리
	2.8 정보시스템 도입 및 개발 보안	2.8.1. 보안 요구사항 정의
		2.8.2 보안 요구사항 검토 및 시험
		2.8.3 시험과 운영 환경 분리

		2.8.4 시험 데이터 보안
		2.8.5 소스 프로그램 관리
		2.8.6 운영환경 이관
	2.9 시스템 및 서비스 운영관리	2.9.1 변경관리
		2.9.2 성능 및 장애관리
		2.9.3 백업 및 복구관리
		2.9.4 로그 및 접속기록 관리
		2.9.5 로그 및 접속기록 점검
		2.9.6 시간 동기화
		2.9.7 정보자산의 재사용 및 폐기
	2.10 시스템 및 서비스 보안관리	2.10.1 보안 시스템 운영
		2.10.2 클라우드 보안
		2.10.3 공개서버 보안
		2.10.4 전자거래 및 핀테크 보안
		2.10.5 정보전송 보안
		2.10.6 업무용 단말기기 보안
		2.10.7 보조저장매체 관리
	2.11 사고 예방 및 대응	2.11.1 사고 예방 및 대응체계 구축
		2.11.2 취약점 점검 및 조치
		2.11.3 이상행위 분석 및 모니터링
		2.11.4 사고 대응 훈련 및 개선
		2.11.5 사고 대응 및 복구
	2.12 재해복구	2.12.1 재해·재난 대비 안전조치
		2.12.2 재해 복구 시험 및 개선

<표 Ⅳ-5> 보호대책 요구사항 분야 및 항목

정보보호 관리체계(ISMS)에서 보호대책 요구사항은 주로 관리적, 기술적 보안에 대한 기준을 수립하고 운영을 하는 방안에 대한 내용이 주를 이루게 된다. <표 Ⅳ-5>를 보면 분류와 항목을 알 수 있다. 우선 2.1 정책, 조직, 자산 관리 부분은 관리체계 수립과 다르게 정책이 있는지를 보는 부분이 아닌 주기적으로 검토하고 필요한 경우 정책을 개정하고 이력을 관리하는 부분을 담고 있다. 조직의 유지관리에서는 책임자와 담당자의 책임성을 명시하고 있는지를 확인하고, 정보자산관리에서는 자산의 취급절차와 보호대책이 수립되었는지를 보고, 책임이 누구에게 있는지를 본다. 2.2 인적보안에서는 주요 직무자를 지정하고 직무를 관

리하고, 보안서약 교육 등 정보보호 인식제고에 관한 부분을 다루고 있다. 2.3 외부자 보안에서는용역 등 외부자에 대해 계약과 현황 등을 관리하는 방안을 다루고 있다. 2.4는 물리보안으로 보호구역을 지정하고 출입을 통제하고 업무환경을 보안하는 통제항목을 지정하였다. 망분리 관점에서 본다면, 아무리 완벽하게 망을 분리했을 지라도 물리적으로 네트워크 장비에 공격자를 접근 시킨다면 아무 소용이 없기 때문에 물리 보안은 중요한 요소이다. 각 지점에 랙(Rack)실을 분리하는 등 망에 따라 장비를 분리해 놓는 등의 조치 등이 추가적으로 필요할 것이다. 2.5 인증 및 권한관리에서는 정보보안에서 중요한 접근통제에 대한 내용을 다루고 있다. 정보보안을 위해서는 세 가지 원칙이 존재하는데 바로 1.식별, 2.인증, 3.인가 세 단계를 관리해야하는데 그 내용을 점검항목으로 가지고 있다. 2.6에서는 실제 각 단계별 접근통제를 하는 부분에 대한 확인 항목을 가지고 있다. 망분리 관점에서 접근통제는 밀접한 연관을 갖게 된다. 네트워크 접근통제는 내·외부망을 분리하였기 때문에 내부망에서는 인터넷으로 나가는 접점 관리로 관리의 영역이 확 줄어들게 되는 것이다. 또 인터넷망 역시 내부로 연결이 되는지를 확인하는 부분이 중요하다. 망분리에서는 망간 접점을 정의하고 그 점점을 안전하게 관리 할 필요가 있다. 앞에서 살펴본 것처럼 망간 자료연계 솔루션 등을 이용하고, 결재 절차를 정책으로 만들어 공유하고 주기적인 점검을 한다면, 접점관리는 잘 되고 있다고 봐도 될 것이다. 간혹 망분리 개념을 혼동하여 단말기 위주로 분리가 되고, 망은 같은 망을 사용하고 있다면, 접점 점검 및 관리는 상당히 어렵게 되며, 안전한 망분리라고 볼 수 없다. 특히 복합기 등이 접점이 되는 경우가 있다. 프린터, 복합기 등은 내부망과 외부망을 분리하여 적용하여야 할 것이다. 정보보호 관리체계(ISMS)에서는 망분리를 필수 요소로 보지 않는다. 하지만 그에 상응하는 보완 조치를 하게 되어있고, 법적 요건에서 이러한 망분리가 강제된 그룹(e.g.금융권)에서는 해당 부분을 <표 Ⅳ-6>과 같이 점검하게 되어있다.

점검항목	상세내용
2.6.7 인터넷 접속 통제	인터넷 접속 통제 부분에서 해당 부분을 점검 하며, 점검기준은 인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
주요확인사항	
1. 주요 직무 수행 및 개인정보 취급 단말기 등 업무용 PC의 인터넷 접속에 대한 통제정책을 수립·이행 여부	
2. 주요 정보시스템(DB서버 등)에서 불필요한 외부 인터넷 접속을 통제	
3. 관련 법령에 따라 인터넷 망분리 의무가 부과된 경우 망분리 대상자를 식별하여 안전한 방식으로 망 분리를 적용	

<표 Ⅳ-6> 2.6.7 인터넷 접속 통제 항목의 상세내용

<표 Ⅳ-6>에서 살펴보는 것처럼 주요 확인사항에 망분리는 세 번째 확인사항에 있지만, 앞에 1도 효율적으로 접속을 통제하기 어려운 부분이 존재한다. 망분리 의무가 부여된 기관<표 Ⅳ-7> 외에도 망분리 없이 1번 확인사항을 충족하기 위해서는 인터넷 사용, 메일 사용, 정보유출 가능 사이트(P2P) 등을 모두 차단하는 정책을 구성해야 한다.

연번	망분리 의무가 부과된 망분리 대상
1	망분리 의무 대상자(정보통신망법 근거) 및 망분리 적용이 필요한 개인정보 취급자
2	전년도 말 직전 3개월간 개인정보가 저장·관리 되고 있는 이용자가 일일 평균 100만명 이상 또는 정보통신서비스부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자
3	개인정보 처리시스템에서 개인정보를 다운로드, 파기, 접근권한을 설정한 경우

<표 Ⅳ-7> 망분리 의무가 부과된 망분리 대상

이외에도 2.6.6 원격접근 통제, 2.10.6 업무용 단말기보안 2.10.8 패치관리 항목도 망분리와 연관이 있거나 망분리를 도입하기 위해서 반드시 고려해야 할 항목이다.

4) 정보보호 관리체계(ISMS) 관점에서 망분리 시사점

망분리는 정보보호 관리체계에 필수 사항은 아니지만 100개가 넘는 인증기준을 충족하기 위해서는 효율적이고 효과적인 방법이다. 특히 정보보호 관리체계에 있는 관리체계 정책 수립을 위한 경영진 참여 및 정보보호 책임자 지정과 같은 경영진에게 의무와 책임을 주는 일련의 과정을 통해 망분리의 필요성을 주지시키고 추진을 위한 인력, 예산, 조직을 확보하는 방법으로 활용하는 것도 좋은 방법이라고 생각 한다. 정보보호 관리체계(ISMS)에서는 사용자와 외부자를 구분하고 있다. 망분리가 없다면, 외부자 관리를 위한 기술적인 관점에서 네트워크 설계나 자산관리 방안, 또는 개발 단계에서 안전한 개발 소스 보관을 위한 방법들을 준수를 위해 관리지점 다시 발생한다.

2. 보안강화(망분리)의 한계

위에서 지금까지 망분리에 다양한 부분을 살펴보면서 망분리의 효율적인 부분에 대해 중점적으로 언급하였다. 관리적 보안은 관리적 보안은 인적자원을 관리하고 보안 정책을 제정하는 역할을 하는 영역이다. 정보보안 정책은 강제성을 가져야하기 때문에 내부 규정 등으로 작성되어야 한다. 정보보안 정책에서는 사용자나 정보관리 부서가 정보시스템 관리나 PC등을 관리할 때 준수해야하는 역할을 정의하고 각종 관리절차를 마련하여야 한다. 정보시스템을 도입하고 보안을 위해 보안성 검토를 하는 방법 및 임직원이 업무 수행 시 접근 할 수 있는 범위와 접근하면 안 되는 범위를 설정하고, 용역사업 등 책임소재를 명확하기 위한 서약서 등의 양식 등을 포함하여야 한다. 특히 침해사고나 정보유출 등 사이버 위기 발생 시 처리해야 하는 역할과 방법을 정의하여 위급상황에 대한 대처를 명시할 필요도 있다. 주기적인 정보보호를 위해 정보보안 및 개인정보보호 점검

을 통해 보안 위협의 요소를 제거하고 개선사항을 발굴하여 개선하는 역할도 포함이 된다.

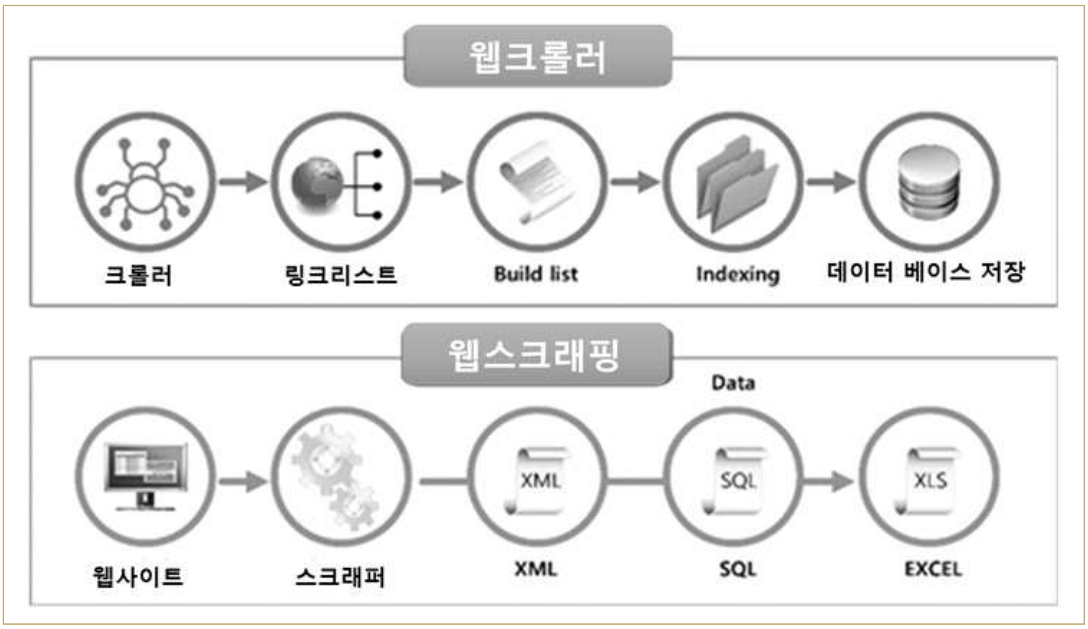
이러한 관리적 보안에서는 정보보호와 관련된 교육을 포함하는데 정보보호 의식 제고 및 확대를 위해 필요하다. 정보보호 담당자의 어려움은 관리적 보안에서 많이 발생된다. 정보보호는 불편하고 비효율적이라는 의식 때문에 강한 항의를 받거나 감정적인 불만 표출에 의해 감정노동을 겪고, 정보보호 담당자는 조직 갈등을 겪고 직무이탈 의도가 발생한다. 네트워크 망분리의 경우 정보보안 측면에서 많은 기술적 이점이 있고, 공공기관이나, 금융권 기업에서는 필수 권고사항으로 피할 수 없는 부분이 존재하지만, 사용자의 변화관리를 위한 노력을 간과할 수는 없다. 조직 갈등은 정보보안 정책에 대한 반감을 키워 정보보안 의식 약화를 가져오고 이는 전체적인 기관, 기업의 정보보안 약화로 이어지게 된다.

인터넷, 통신기술의 발달로 인하여 네트워크로 사람, 데이터, 사물 등 모든 것을 연결한 사회를 바로 '초 연결 사회' 라고 말한다. 이런 사회에서 인터넷을 차단은 일부 폐쇄적인 운영을 해야 하는 일부 기반시설을 제외하고는 실행할 수 없는 조치이며, 인터넷 완전 차단을 한다면 업무의 효율성이 하락하여 정보보안의 목적인 기밀성과 무결성을 지킬 수 있지만 가용성의 하락을 막을 수 없을 것이다. 그래서 인터넷 망을 별도로 구성을 하고 망간 자료연계 등 장치를 통하는 자료 연계는 제한적인 허용 정책을 수립하는 이유이다.

V. 실험용 프로그램 설계

1. 프로그램 구성

일반적인 웹 브라우저는 사용자가 웹을 인식하도록 모니터에 웹 페이지의 결과를 표시한다. 브라우저는 웹 서버에서 HTML, CSS 등을 로딩하여 화면을 구성하여 어떤 화면이 구성되어 있는지, 어떻게 구성되어 있는지를 결정한다. 헤드리스 브라우저 기술은 윈도우가 없는 브라우저를 가능하게 한다. 일반적으로, 검색 엔진은 사이트 정보를 식별하고 수집하기 위해 이 기술을 사용한다. 그것은 또한 자동화된 웹 컨트롤을 목표로 한다. 헤드리스 브라우저를 위한 기법은 팬텀.js, 웹킷 기반 캐스퍼.js, jsdom 기반 좀비.js, 게코 기반 slimer.js이다. 옵션인 헤드리스 브라우저를 갖춘 구글 크롬의 헤드리스 크롬이 있다. 웹에서 특정 정보를 추출하거나 브라우저를 실행하지 않고 원하는 전자 문서로 페이지 전체를 캡처하여 저장할 수 있다<그림 V-1>.

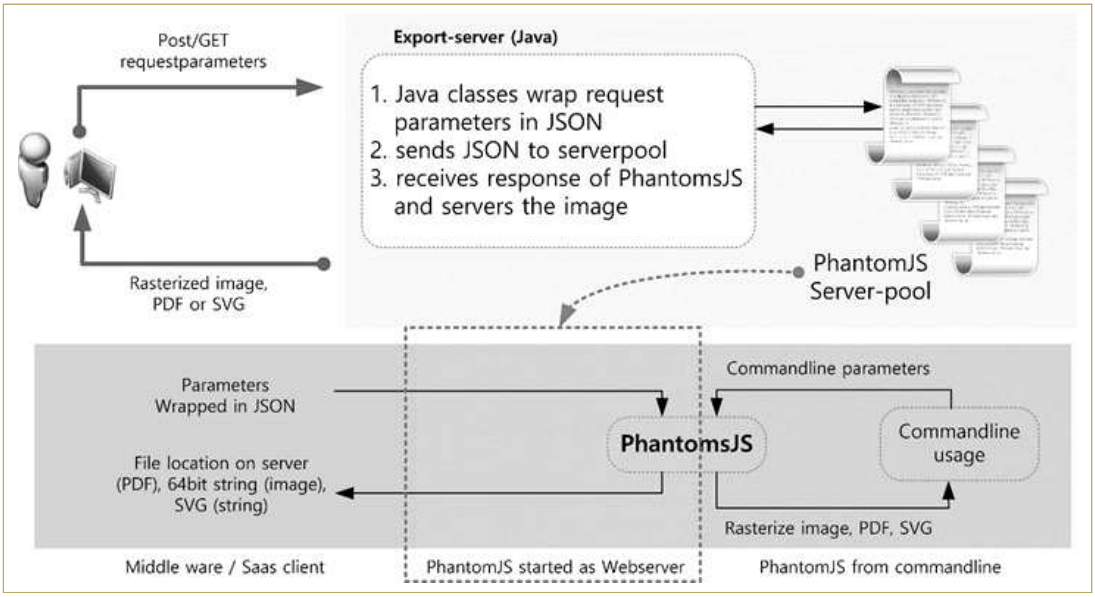


<그림 V-1> 웹크롤러와 웹 스크래핑 비교

네트워크 망분리가 적용된 후 내부와 외부 네트워크가 분리되기 때문에 기본적으로 해킹이나 악성코드가 차단된다. 당연하게도 사용자들은 내부 네트워크로부터 인터넷에 접속할 수 없다. 즉, 업무에 인터넷상의 정보를 이용하기 위해서는 네트워크 분리 정책을 따라야 한다. 파일 전송 시스템이 갖추어져 있을 경우, 사용자는 인터넷 데이터를 다운로드하여 파일 전송 시스템을 통해 내부 네트워크로 전송할 수 있다. 불편은 존재하며 전송해야 할 자료가 더 많을 때 불만이 발생한다. 직원 간 갈등과 정보보안 정책의 한 요소다. 본 논문은 업무 네트워크의 네트워크 분리 원칙을 위반하지 않고 인터넷을 이용하는 방법을 <그림 V-2>과 같이 제안한다.

<그림 V-2> 웹브라우저와 비슷한 화면을 캡처

지금까지 네트워크 망분리의 주요 개념과 네트워크 분리환경에서는 데이터. 요컨대, 인터넷에서 얻은 정보나 자료를 내부망에 위치한 업무에 활용하기 위해서는 승인을 과정을 거쳐야 한다. 에이전트 구조상 사후결재 절차를 확보하여 구성한다면, 사용자가 요청한 웹 URL과 캡처된 웹 화면까지 기록에 남아 정보보안의 통제수단으로 효율적인 수단이 될 것이다.

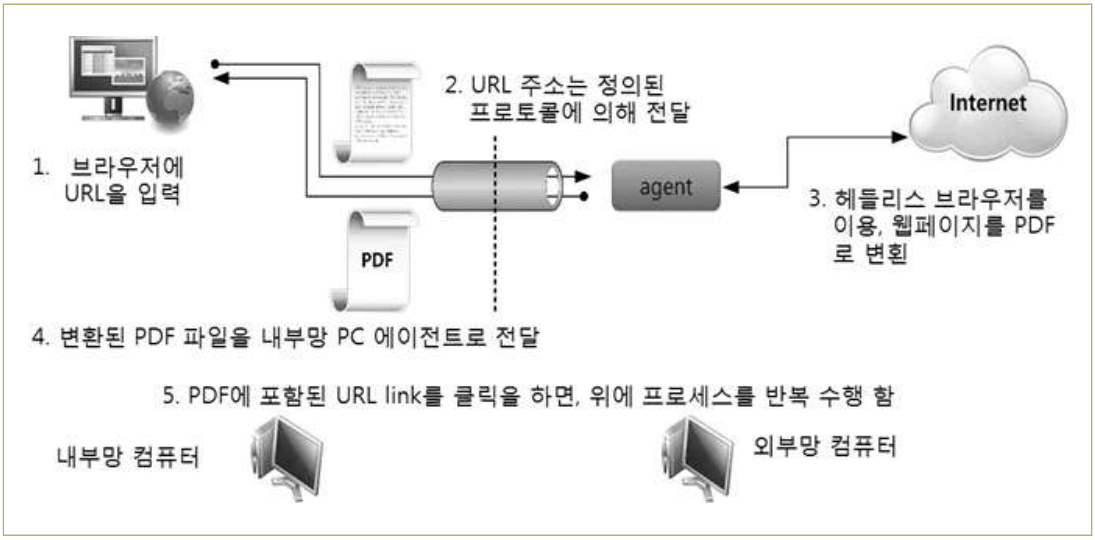


<그림 V-3> PamtomJS를 이용한 스크래핑 설계

2. 모듈별 고려사항

1) 스크래핑을 이용한 안전한 웹 설계

내부망 컴퓨터에서 입력된 URL은 미리 정의된 프로토콜에 따라 내부 네트워크에서 외부 네트워크로 전송된다. 이때, 망분리의 정책을 위배하지 않는 망간자료전송 장치를 이용한다. 망간 자료전송 장치는 승인을 거치게 되어있지만, 사후승인 프로세스를 설정하여, 진행하면 사용자도 결재를 기다리는 불편함 없이 이용이 가능하며, 나중에 어떤 URL을 살펴보았는지 증적이 남아 정보보호의 추적가능성 확보에도 도움이 될 것 이다. <그림 V-4>와 같이 외부 네트워크 PC에 설치된 에이전트는 헤드리스 브라우저를 사용하여 전자 문서(예: pdf 파일)를 생성한다. 캡처 및 변환된 파일이 내부 네트워크로 다시 전송되어 내부 네트워크 브라우저에 표시한다.



<그림 V-4> 스크래핑을 이용한 안전한 웹 설계 내용

2) 구현배경 설명

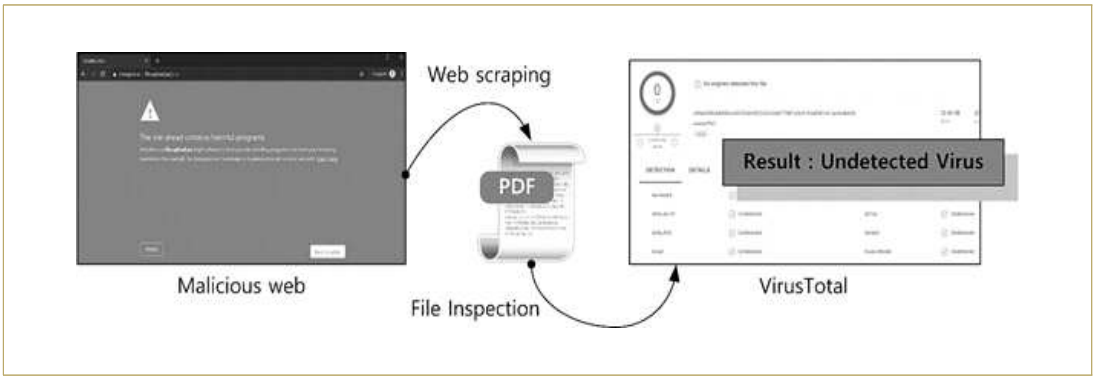
브라우저로 웹을 탐색하다가. 악성코드가 포함된 웹페이지를 브라우저로 보게 되는 경우 PC를 감염시킬 수 있다. 물론, 모든 악성코드가 보기만 했다고 감염시키는 것은 아니다. 악성코드는 보안위협을 만들고, 보안위협은 취약점을 이용하여, 자산을 노출 시키게 된다. 여기서 말하는 자산이란, PC나 서버의 물리적 장치 뿐 만아니라, WAS, OS 등 소프트웨어 등을 포함하며, 중요정보(개인정보)를 포함하는 자산을 의미한다.

드라이브-바이-다운로드(Drive-By-Download) 기법은 악성코드 배포를 주목적으로 하는 공격으로 알려져 있다. 잘 알려진 사건으로는 C(클**)커뮤니티 사건이다. “웹서버 소스 파일 위변조 공격”을 통해 커뮤니티에 접속한 무작위의 사용자에게 미리 준비된 랜섬웨어를 다운로드 받도록 드라이브-바이-다운로드(Drive-By-Download) 기법으로 유포된 사례가 있다. 가장 중심에 놓고 사용한 취약점은 어도비(Adobe)의 플래쉬 파일(swf 파일)로 배포가 된다. 최신 업데이트를 수행한 PC나 익스플로어외 브라우저를 사용한 사용자는 이번 공격을 당하지 않은 것으로 알려져 있다.

VI. 실험용 프로그램 결과

1. 실험프로그램을 통한 악성코드 포함 여부 확인

실험용 악성코드가 들어 있는 웹을 PDF 파일로 캡처했기 때문에 악성코드가 작동 않았다. 악성코드는 보통 특정 파일을 다운로드하고 실행하거나, 프로그래밍이 가능한 영역을 통해 공격자가 원하는 부분의 소스나 실행파일을 실행 한다. 이런 공격은JavaScript, ActiveX, Flash 등에 존재하는 취약성을 이용한다. 실험 프로그램 결과 악성이 존재하는 페이지를 캡처하여 VirusTotal[1]을 통해 악성코드 여부를 확인 했다<그림 Ⅵ-1>.



<그림 Ⅵ-1> 실험 프로그램을 통한 결과

2. 실험용 프로그램 시사점

실험용 프로그램을 통해 웹페이지를 스크래핑 한 상태에서는 악성코드가 검출 되지 않음을 확인했다. 다양한 브라우저(IE, 크롬, 파이어폭스, 사파리, 웨일) 등은 브라우저에서 PDF를 읽을 수 있게 보여주는 기능을 제공 하고 있다. 과거

1) VirusTotal : 여러 개의 백신 엔진으로 검사하여 그 결과를 투명하게 보여 주는 서비스를 제공하는 웹페이지. 약 40개의 보안 업체의 엔진을 통해 알려진 악성코드 여부를 검사할 수 있다.

PDF를 읽기 위해서는 PDF 리더 프로그램을 실행하는 등의 불편함이 없다는 뜻이다. 이것의 장점은 웹을 PDF로 만들면 각 각의 텍스트나 영역의 하이퍼 링크가 살아 있는 상태로 변환이 되기 때문에 PDF가 웹페이지를 보는 것처럼 링크를 클릭하고, 그 링크의 URL이 다시 망간 자료 교환을 통해 다시 웹 브라우저로 보여주는 데 문제가 없다. 물론 웹의 다양한 요소인 동적인 웹페이지 구성이나, input이나 submit, 파일 업·다운로드의 기능은 제약이 존재하지만, 뉴스, 법률, 공공기관의 공시 등의 페이지가 대부분 정적인 구성으로 작성된 것을 고려하면, 망분리 환경에 필요한 정보보안 정책을 위해하지 않으면서 정보 활용을 할 수 있는 방안이라고 생각한다.

웹 스크래핑을 하는 작업을 수행하는 서버를 지정하고 모든 요청을 서버로 보내 수행하는 방법도 있겠지만, 트래픽 사용량과 원래 가지고 있는 인터넷 PC를 활용하는 방법이 좀 더 자원을 효율적으로 사용하는 방법이라고 생각했다.

Ⅶ. 결론 및 향후과제

본 논문의 목적은 네트워크 망분리 환경에서 편의성을 증대하기 위한 방안을 제안하는 것이다. 정부의 의지에 따라 많은 기업과 기관이 네트워크 망분리를 적용하거나, 적용계획을 수립하고 있다. 이 과정에서 고려하고 분석할 부분이 많지만 중요한 부분은 임직원의 업무 환경이 변경되는 부분에서 변화관리이다. 망분리 환경에서 제한된 웹 서핑을 허용하기 위한 웹 데이터 연계 방법을 제시하였다.

웹을 캡처하여 만든 변형 형태의 파일에서는 악성코드가 검출 되지 않았음을 실험을 통해 확인하였다. 즉 악성코드는 캡처된 상태에서 동작할 수 없는 형태이며, 시그니처 기반의 정보보호 솔루션도 악성코드로 검출하지 않았다는 것이며, 이는 이미 알려진 웹상 위협으로부터 자유로운 웹 데이터 연동 방법이라고 할 수 있다.

이러한 웹 데이터 연동방법은 발전하여, 국가용 망 연계 장치 기능에 포함되어

업무망에서도 인터넷을 활용할 있는 제품이 생산되도록 하여야 할 것이다.

웹 데이터 연계시 인증성을 강화하기 위한 프로토콜을 정의하고, 이런 장치를 통해 업무망에서 인터넷을 사용할 경우의 효과에 대한 지속적인 연구가 필요하다.

참 고 문 헌

1. 국내 문헌

김근혜, 박규동, 심미나. (2019). 정보보안 종사자의 조직갈등과 직무이탈 의도에 관한 연구. 정보보호학회논문지, 29(2), 451-463.

김동훈, 손인수. (2019). 네트워크 침입탐지 기술 연구 동향. 전자공학회논문지 56(8), 2019.8, 3-12(10 pages)

길아라. (2013). 스니핑 공격에 대응하는 애드-혹 무선 센서 네트워크를 위한 보안 라우팅 프로토콜. 정보과학회논문지 : 정보통신 40(1), 2013.2, 26-35(10 pages)

최재운, 김세헌. (2010). 무선 센서 네트워크에서 통계적 기법을 활용한 웜홀 공격 탐지 한국경영과학회 학술대회논문집 , 2010.6, 1584-1587(4 pages)

김현우. (2013). 베이지안 정리를 이용한 싱크홀 공격 탐지 기법,의사결정학연구 21(2), 2013.12, 115-124(10 pages)

박준호, 성동욱, 유재수(2011). 무선 센서 네트워크에서의 에너지 효율적인 선택적 전송 공격 탐지 기법, 한국정보과학회 학술발표논문집 38(1D), 2011.6, 248-251(4 pages)

최재영, 백현철, 김상복, 심종채, 박재흥. (2014). 세션 하이재킹 공격에 대한 TCP Sequence Number 암호화. 한국지식정보기술학회 논문지, 2014, vol.9, no.6, pp. 707-714 (8 pages)

김성기, 장종수, 민병준. (2010). 제로데이 공격 대응력 향상을 위한 시그니처 자동 공유 방안. 정보과학회논문지 : 정보통신 37(4), 2010.8, 255-262(8 pages)

오일석. (2019). 미국 정보기관 제로데이 취약성 대응 활동의 법정책적 시사점. 미국헌법연구, 30(2), 143-185.

김영선, 서춘원. (2018). 클라우드 컴퓨팅의 웹 스크래핑을 이용한 텍스트 데이터 분석에 대한 연구. 대한전자공학회 학술대회, 1445-1447.

송동훈, 임현종, 박수진, 신익현. (2018). 원자력시설 사이버보안 강화를 위한 관리적 보안조치 검증 방법론 연구. 한국통신학회 학술대회논문집, (), 1048-1049.

최동근, 송미선, 임종인, 이경호. (2015). 정보보호담당자의 역할이 조직의 정보보호수준에 미치는 영향. 정보보호학회논문지, 25(1), 197-209.

박준경, 김범수, 조성우. (2011). 기업정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인. 경영학연구, 40(4), 955-985.

2. 국외 문헌

3. 기타

시스코, “방위산업 기관 및 공공, 금융기관을 위한 시스코 물리적 망분리 제안”, www.cisco.com

박승철, 한국기술교육대학교 출판부, “정보보호론”, 초판(2017.2)

이민형 기자, 디지털 데일리, “10만건 개인정보유출 사실로 드러나....청와대, 사과문 공지”, www.ddaily.co.kr/news/article/?no=106249

이유지 기자, 디지털 데일리, “금융 고객정보유출 파문 확산…“카드사 외 16개 금융사 개인정보도 127만건 유출”, www.ddaily.co.kr/news/article/?no=113533

김태형 기자, 보안뉴스, “커뮤니티 사이트 뽐뿌 해킹! 회원정보 모두 유출”, www.boannews.com/media/view.asp?idx=47819

구교형 기자, 경향신문, “인터파크 고객정보 1000여만건 유출…경찰, 해킹 혐의 수사 착수”, news.khan.co.kr/kh_news/khan_art_view.html?artid=201607251546001

김은성 기자, 뉴스1, “2540만건 정보유출한 인터파크, 행정소송 1심 패소”, news1.kr/articles/?3364318

송승현 기자, 이데일리, “2500만건 정보유출 인터파크, 과징금 취소 항소심서도 져”, www.edaily.co.kr/news/read?newsId=03411206622681456

과학기술정보통신부, 행정안전부, 방송통신위원회, 한국인터넷진흥원, “정보보호 및 개인정보보호 관리체계 인증제도 안내서”, 2019.1

과학기술정보통신부,한국인터넷진흥원, "정보보호시스템 구축을 위한 실무가이드", 2018.6

과학기술정보통신부,한국인터넷진흥원, "주요정보통신기반시설 기술적 취약점 분석·평가방법 상세가이드", 2017.12

감사의 글

본 논문을 작성하고 완성된 지금까지 도와주신 분들에게 진심으로 감사의 마음을 전합니다.

학업의 길로 이끌어 주시고 직장인으로 배려와 지도를 해주신 박남제 교수님, 바쁘신 와중에서도 논문지도와 수업을 통해 많은 가르침을 주신 변영철 교수님, 논문의 기본을 알려 주시고 부족한 부분을 아낌없이 지도해 주신 조정원 교수님께 감사의 마음을 전합니다.

저는 대학을 졸업하고 7년간을 개발자로 살아왔습니다. 그 당시 나의 가장 중요한 가치는 '효율성' 이었습니다. 그 시절 나는 '정보보안'이 나의 중요한 가치인 '효율성'을 해치는 장애물이라고 여기며 살아왔습니다. 정보보안을 위해 강요된 절차들과 환경을 매우 비효율적이고 못마땅하게 생각했었습니다. 그러나 제주도에서 새로운 직장으로 이직을 하게 되었고, 이곳에서 받은 업무가 공교롭게도 '정보보안'이었습니다. 이 어색한 업무를 5년간 해오면서 정보보안이 왜 중요한지에 대해서 조금씩 이해하게 되었습니다. 아마도 내가 일하던 직장이 망하지 않았던 이유는 숨은 곳에서 정보를 지키는 그들 때문이었음을 이젠 확실하게 이해하게 되었습니다.

항상 저를 믿어주시는 장모님, 장인어른, 할머니, 누나들과 매형들, 처형, 처남에게도 고마운 마음을 전합니다. 특히, 대학 졸업 10년 후에 학업을 시작한 아들에게 등록금을 내주시며 응원해 주신 아버지, 어머니께 감사의 마음을 전합니다. 그리고 직장 정보관리실장님, 그리고 정보보안팀, 정보관리실 직원 모두에게 감사하다고 말씀을 전합니다. 또한 함께 졸업을 준비한 우리 융합정보보안 동기, 후배님들 모두에게 감사의 말씀을 전합니다.

"아빠 논문 그만 쓰고 놀면 안 돼?!" 라며 논문 쓰는 나에게 투정을 부리는 사랑하는 두 딸 주담, 예담, 그리고 이것만 끝나면 안 바쁘게 살겠다고 약속하는 남편에게 항상 속고 사는 사랑하는 아내 혜진에게 이 논문을 바칩니다.