https://doi.org/10.33778/kcsa.2022.22.2.051

제로트러스트 보안 모델에서 보안관제 시스템 강화 연구★

박 원 형*

요 약

최근 제로 트러스트에 대한 개념이 도입되며 차세대 보안관제 시스템에 필요한 보안 요소 강화가 필요하다. 또한, 4차 산업혁명 시대의 보안 패러다임도 바뀌고 있다. 클라우드 컴퓨팅과 코로나 19로 인해 업무 환경이 변화되면서 발생하는 사이버보안 문제는 지속 발생하고 있다. 그리고 이와 동시에 새로운 사이버 공격기법들도 지능화·고도화되고 있는 상황에서 보안을 강화할 미래의 보안관제 시스템이 필요하다. 제로 트러스트 보안 개념은 모든 것을 의심하며 신뢰하지 않는다는 개념을 기반으로 모든 통신을 감시하고 접근 요청자에 대한 엄격한 인증과 최소한의 접근 권한을 핵심으로 보안성을 높인다. 본 논문에서는 기존 보안관제 시스템의 문제점을 이해하고 이를 해결할 수 있는 제로 트러스트 보안 모델을 통해 보안관제 분야의 보안 강화 방안을 제안 한다.

Enhancement of Security Monitoring & Control System in Zero Trust Security Models

Wonhyung Park*

ABSTRACT

Recently, the concept of zero trust has been introduced, and it is necessary to strengthen the security elements required for the next-generation security control system. Also, the security paradigm in the era of the 4th industrial revolution is changing. Cloud computing and the cybersecurity problems caused by the dramatic changes in the work environment due to the corona 19 virus continue to occur. And at the same time, new cyber attack techniques are becoming more intelligent and advanced, so a future security control system is needed to strengthen security. Based on the core concept of doubting and trusting everything, Zero Trust Security increases security by monitoring all communications and allowing strict authentication and minimal access rights for access requesters. In this paper, we propose a security enhancement plan in the security control field through a zero trust security model that can understand the problems of the existing security control system and solve them.

Key words : Zero Trust Security, Security Monitoring & Control System, Cyber Attack, Cloud Computing

접수일(2022년 05월 31일), 수정일(2022년 06월 30일), 게재확정일(2022년 06월 30일)

★ "본 연구는 2021년도 상명대학교 교내연구비를 지원받아 수행하였음."(2021-A000-0286)

* 상명대학교 정보보안공학과 부교수 (주저자)

1. 서 론

현재, 우리는 ICT 시대와 4차 산업 혁명 시대에 살고 있다. 4차 산업 혁명 시대를 대표하는 3D 프린팅, 빅데이터, 인공지능 등과 같은 혁신적인 기술들은 시간이 흐를수록 계속해서 빠른 속도로 발전하고 있으며 우리는 다양한 분야에서 사용하고 있다. 하지만 동시에 이를 위협하는 지능화·고도화된 사이버위협도 함께 발생하고 있다. 이글루 시큐리티(Igloo Security, 2021)에서 발표한 '2021 상반기 주요 보안위협 트랜드'에 의하면 서드파티 소프트웨어를 이용한 공급망 공격, 산업 전반에 영향을 미치는 랜섬웨어 공격, 코로나바이러스 이슈를 악용한 사이버 공격 등 복합적이고 고도화된 공격이 계속해서 일어나고 있다[1].

코로나바이러스로 인해 전 세계의 환경과 생활 방식이 바뀌고 있고 동시에 국가 안보를 위협하는 수준까지 사이버위협 심각해짐에 따라 기존 보안 관제 체계에 대한 변화 및 개선이 필요하다. 코로나바이러스가 창궐하기 이전 보안관제 체계는 중요한 정보 자산을 보호하기 위해 사이버위협으로 의심되는 외부로부터의 접근을 각종 보안 장비들을 이용해 차단하고, 보안 담당자가 24시간 365일 모니터링하여 최전선에서 보안을 책임졌다. 'SIEM'과 같이 빅데이터 기반 장비를 이용해 방대한 데이터들도 수집하고 분석하여 막대한 피해가 발생하는 가능성을 최소화한다.

하지만 원격·재택 근무로 업무 환경이 변화하면서 외부에서 내부로의 '인바운드(inbound) 관제'와 내부에서 외부로의 '아웃바운드(outbound) 관제'로 모두 통합하여 관리하고 살펴봐야 한다는 필요성이 있다[2]. 비대면 통신에서 핵심적인 보안 솔루션인 가상사설망 'VPN'을 표적한 공격도 빈번해지면서 기존 전통 보안 방식을 고집하고 보안 정책을 세우는 것만으로는 미흡하다. 또한, 내부는 절대적으로 신뢰하는 것 역시 위험하다. 보안관제 시스템에서는 내·외부를 뿐만아니라 모든 통신에 대한 보안위협 경계를 강화해야 한다. 보안관제 분야에서는 현재 인력 부족 문제에 직면하고 있다. 대부분의 현재 보안관제 시스템에서는 사람이 막대한 데이터를 처리하고 분석한다.

24시간 365일 모니터링을 해야 한다는 단점으로 보안관제 업무를 기피하는 경향이 있다. 사람이 보안관제를 담당하고 있다는 점에서 휴먼 에러(Human error)로 인해 미탐·오탐도 상존 한다. 그래서 인공지능을 이용하면 인력 자원 없이 데이터 분석 처리 및 이상 탐지도 줄일 수 있다고 한다. 하지만, AI 기반 보안관제 시스템은 업무의 효율성과 인력 부족 문제는 해결할 수 있다고 하지만, 언제나 또다른 제약 사항이 존재한다. 이상 탐지 시에 인공지능을 학습시킬 데이터가 충분하고 신뢰성이 갖춰져야 하며, 얼마나 양질의 데이터를 통해 학습하느냐에 따라 탐지, 분석, 대응 등 보안관제의 탐지 성능이 높아 질 수 있다[3].

그 외에도, 인공지능을 전문으로 관리하는 별도의 인력도 준비되어야 한다. 전통 보안 방식의 보안관제 시스템에 인공지능을 무조건 도입하기 보다 언제나 침해당했다는 가정을 두고 내외부 구분 없이 모든 통신을 의심하여 엄격한 접근을 통제해 효율적으로 보안 수준을 높이는 '제로 트러스트(Zero-Trust) 보안' 개념을 도입해야 한다. 제로 트러스트 보안은 전통적 경계기반 보안모델과 달리 정보 자산을 보호하기 위해 모든 접근을 의심한다. 접근 요청자에 대한 엄격한 인증 절차를 진행하고 최소한의 권한을 허용한다. 접근 권한을 최소화하기 때문에 소수의 접근에 대해서만 관리 감독하면 되고, 공격할 수 있는 경로를 최소화하여 경로 우회를 차단한다. 내부보안까지 통제하고 관리할 수 있어 내부 사용자로 인한 데이터 유출과 같은 보안사고도 예방한다는 장점이 있다.

결국, 제로 트러스트의 핵심 철학은 모든 것을 의심하고 최소 접근권한을 통해 최대한의 보안업무 효율을 높이는 것에 있다. 그래서 본 논문은 제로 트러스트 보안 개념을 도입하여 보안관제 시스템을 강화하는 방안을 제안 한다.

2. 관련 연구

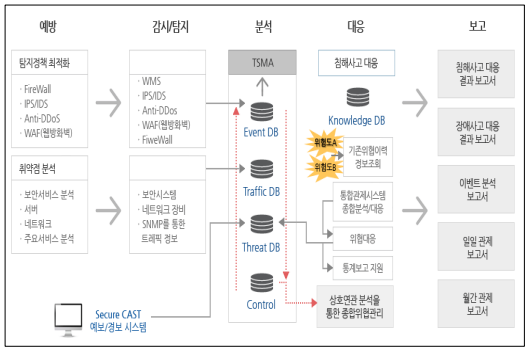
2.1 기존 보안관제 시스템

보안관제는 사이버위협에 대한 대응체계를 수립

하여 보안 정책, 프로세스를 유지하고 정보시스템과 자산을 보호하는 역할을 한다[4]. 보안관제는 네트워크의 전체적인 트래픽이 급증하거나 급감할 때, 내부정보를 탈취하기 위한 해킹시도 및 악성 해킹프로그램 유포와 같은 사이버 공격시도를 실시간으로 탐지한다. 해킹 사실을 통보하고 분석단계에서 파악된 공격자 정보와 취약점 정보를 활용하여 피해시스템이 정상적으로 운영될 수 있도록 신속하게 전문기술을 제공한다[5].

보안 관제센터에 전문인력을 파견하고 운영을 지원하는 등 보안관제 업무를 수행할 수 있는 보안관제 전문기업을 매년 1회 지정하고 있다. 2022년 6월 기준 보안관제 전문기업은 20개의 업체가 있다[6]. 다음 [그림 1]은 윈스의 관제 업무 절차이다. 현재, 보안 관제 시스템은 24시간 365일 보안 인력을 운영하면서 사람에게 의존하고 있어 인력 확보 문제와 예산 문제를 가지고 있다.

기존의 보안관제 시스템은 침입탐지시스템(IDS), 웹 애플리케이션 방화벽(WAF) 등 시그니처(Signature) 기반 탐지이벤트를 받아 탐지이벤트를 줄이고 있지만, 과탐과 오탐이 높다. 정·오탐 판별 건수가 늘면서 경보를 처리할 관제 인력이 부족하기에 과탐과 오탐 문제는 언제나 보안관제의 오래된 문제 중의 하나이다[7].



[그림 1] 일반적인 보안관제 업무 절차[8]

2.2 제로트러스트 도입 동향

제로 트러스트(Zero Trust)는 모든 사용자를 신뢰하지 않고 철저한 확인을 통해 필요한 만큼의 접근 권한을 제공한다[9]. 철저한 사용자 인증과 권한 관리가 제로 트러스트 보안의 핵심이라는 점에서 기존의 시스템 및 데이터베이스 접근통제 솔루션 도입이 곧 제로 트러스트 보안모델 도입이라 하기도 한다[10]. 제로 트러스트는 말 그대로 '0-trust'로, 아무도 신뢰하지 않지 않겠다는 것이 핵심이다. 제로 트러스트는 이 핵심을 토대로, 모든 접근을 의심해 그 행동을 추적하고 필요한 사람에게 필요한 최소한의 접근에 대해서만 접속하도록 만든 새로운 보안 모델이라고 할 수 있다. 또한, 그 어떠한 사용자도 신뢰하지 않고, 한번 신뢰 관계를 형성했다고 하더라도 재접속과 인증 절차를 요구한다. 이 개념은 지난 2010년, 세계적인 연구기관 포레스터 리서치(Forrester Research) 보안 위협 팀의 존 킨더백(John Kindervag) 수석 애널리스트가 제안한 보안모델로, 오늘날 코카콜라, 구글, 웨스트젯 항공 등 다양한 기업에서 쓰는 전략이다[11].

마이크로소프트는 제로 트러스트 원칙을 지킬 수 있는 end-to-end 솔루션을 통합해 내장된 보안 플랫폼으로 제공하며, '애저 액티브 디렉토리(Azure AD)'에 제로 트러스트의 3원칙을 통합시켰다. 애저 AD는 사용자의 환경과 위치, 단말기 위험도를 측정해 액세스를 허용하거나 제한·차단 여부를 판단한다. 암호 없는 인증과 '임시 액세스 패스(Temporary Access Pass)', '조건부 액세스(Conditional Access)'를 사용해 적절한 리소스를 보유한 적절한 사람만 적절한 데이터에 접근할 수 있도록 한다.

엔드 포인트 매니저(End-point Manager)는 기기의 무결성을 검증하고 가시성을 확보해 감염됐거나 허가되지 않은 기기의 무단 액세스를 제어한다. 탈옥·루팅한 모바일 기기의 접근을 차단해 잠재적인 위협을 제거하며, 공유 모드를 이용해 사용자의 프라이버시를 보호하면서 회사 애플리케이션에 액세스하는데 필요한 프로세스를 간소화한다[12][13].

마이크로소프트의 엔드 포인트 보안 솔루션 (Defender for Endpoint)는 관리되지 않은 기기를 검색하고 허가없이 침입을 차단하며 취약성과 설정 오류를 제어하며 알려진 위협과 알려지지 않은

위협 모두 제거 할 수 있다[14].

2.3 제로트러스트 보안관제시스템 적용 방안

클라우드 컴퓨팅과 코로나 19로 인해 전 세계적 근무 형태가 변화하였다. 이에 따라 원격·재택 근무를 노리는 공격들도 활발해졌다. ICT 기술이 발전하면서 동시에 보안기술도 발전 하고 있지만, 취약점도 지속 발견되고 있다.

이를 대응하기 위해 경계 보안 중 하나인 보안관제 체계에도 새로운 변화가 필요하다. 기존 보안관제 체계는 기본적으로 보호해야 하는 정보 자산을 미리 정해놓고 해당 자산에 맞는 네트워크 설계와 보안 시스템을 구축해 알맞게 사고 발생시 대응한다. 여전히 경계 보안을 통한 보안 전략을 기본으로 운영되는 보안관제가 대부분이다. 하지만, 원격에서 네트워크망을 통해 내부로 접속해야 하는 경우가 빈번해진 현 상황에서 내부와 외부를 구분하는 것이 이상 의미가 없을 수 있다.

외부에서 내부로의 '인바운드 관제'와 내부에서 외부로의 '아웃바운드 관제' 두 방식을 토대로 하는 보안관제 방식의 도입이 필요하다. VPN을 이용한 원격접속 증가로 인바운드 트래픽에 대한 모니터링도 필요해진 시점이 되었다. 내·외부를 구분하지 않고 모든 데이터에 대한 접근 검증과 분석이 요구된다. 경계기반 방식의 보안은 내부에 접속이 허용된 자에 대한 신뢰 관계가 생성된다. 하지만 내부자의 접속에 대해 무조건적 신뢰는 위험할 수 있다.

통합보안관제 시스템으로 '내부정보유출 이벤트'에 대한 정보도 수집하고 있지만, 이벤트에 대한 상세한 분석이 필요하며 이벤트 중심 데이터 결과물은 내부 위협을 실질적으로 관리하기에 어려운 부분이 있어 내부 위협을 탐지하기에는 한계가 있다. 내부와 외부를 별도의 영역으로 생각해서 운영되는 경계 보안 방식을 대체할 보안관제의 보안 전략이 필요하다.

3. 제로트러스트 보안관제 적용 효과

3.1 비인가 접근통제

제로 트러스트 보안에서는 다중인증체계(MFA) 기반 사용자 식별 및 철저한 인증을 적용하여 접근 요청자를 검증하고, 검증된 사용자에 한해서 최소한의 권한을 부여한다. 제로 트러스트 보안 환경에서 최소한으로 인증된 세션에서만 해당 권한이 유지된다는 점에서 민감한 데이터에 대한 비인가 접근을 차단할 수 있다.

3.2 우회 접근 차단

사용자의 접근은 알려진 정상적인 경로를 통해 접근하는 것이 일반적이지만, 악성코드 등에 의해 감염된 경우 그 접근 유형 및 경로는 매우 다양하다. 보안 환경에 Multi-Layered 제로 트러스트 모델을 적용하게 되면 정상적이지 않은 경로로 유입된 악성코드의 접근도 차단할 수 있다. 비인가 접근을 모니터링을 통해 악성코드의 유입을 확인할 수 있어 실시간 보안위협에 대한 방어도 가능해 진다.

3.3 보안 범위 식별 및 보안 수준 유지

제로 트러스트 보안에서는 보안 경계를 정의해두지 않고 정보 자산에 대한 모든 접근 주체를 검증한다. 이후에는 접근 주체의 보안 수준을 확인한다. 이 과정을 통하여 기업의 보안 환경에 접근하는 모든 주체에 대한 보안 범위를 식별할 수 있고 동시에 식별된 사용자의 보안 환경을 기업 조직에서 정한 보안 수준으로 개선시킬 수 있는 확장성이 있다.

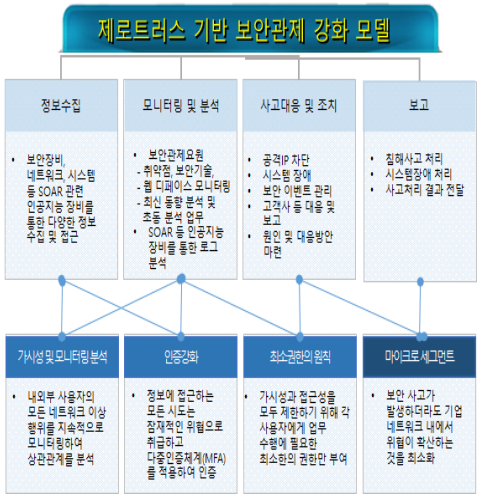
3.4 내부보안 신뢰 향상

최근, 발생한 사이버 공격을 종합해서 보면 대규모의 해킹 공격으로 인한 개인 정보 유출이 발생한 사건의 상당수는 내부직원, 외주 직원, 용역 직원, 외주 업체 직원 등 외부 해킹보다는 내부자에 의한 권한으로 중요 정보에 접근이 허용된 신뢰 관계가 맺어진 사용자에 의해 발생했다. 제로 트러스트 보안 모델을 도입하면, 내·외부 경계를 구분해 두고 보안을 책임지지 않고 모든 통신을 모니터링 하며, 내부로 접근한 사용자에 대한 로깅과 모니터링으로 인해

내부보안을 통한 데이터 유출 사고를 방지 할 수 있다.

4. 제로트러스트 보안관제 시스템 강화 방안

현재, 새로운 보안 패러다임이 변화하고 있는 상황으로 기존 보안관제 시스템의 보안 대응 방식에도 변화가 필요하다.



[그림 2] 제안하는 제로트러스 보안관제 모델

보안관제의 경계기반 보안 전략 대신 보안 시스템을 통과하더라도 신뢰하지 않는 제로 트러스트 보안을 통한 새로운 전략의 도입을 제안한다. 접근이 허용되면 무조건 신뢰하는 대상으로 판단하여 내부에서 어떤 일을 수행하는지 관여하지 않고 F/W, IDS, IPS, VPN 등의 보안 장비들을 통해 외부에서 내부의 접근을 제어하는 방식이 대부분 보안관제의 기본 보안 전략이다. [그림 2]에서 제안하는 보안관제 절차는 크게 정보수집 - 모니터링 및 분석 - 사고대응 및 조치 - 보고 4가지 절차를 따른다.

보안관제 프로세스 중 먼저 정보수집과 모니터링 및 분석단계에서 제로 트러스트 보안 전략을 활용한 솔루션으로 보안 수준을 높일 수 있다. 제로 트러스트 보안은 엄격하게 검증된 접근자에게 최소한의 권한을 부여해 접근을 허용한다는 특징을 이용해 해당 접근자의 통신에 대해서만 집중적으로 관리 및 모니터링이 이루어진다. 이는 보다 효율적으로 보안 기능을 수행한다는 점을 시사한다. 최소한으로 허용된 접근 경로에 대해서만 접근을 가능하도록 운영되기 때문에 공격자들이 경로를 우회해 접근하는 것을 원천적으로 차단해 상대적으로 미탐을 줄일 수 있다. 접근을 허용한 최소 권한에 대해서만 집중해서 관리 및 감독하면 보안관제 요원이 대응해야 하는 업무도 줄어든다. 과도한 탐지로 인해 대응해야 하지만 해결하지 못하는 경보들이 상대적으로 줄어들 것으로 보인다. 공격으로 의심되는 이상 행위 발생 시에도 접근을 허용한 경로를 통한 통신의 트래픽만을 분석하면 되기 때문에 분석 데이터의 양도 현저히 줄어들 것이다. 제로 트러스트 보안은 이미 침해당했다는 것을 전제로 하여 트래픽을 모니터링하고 엄격한 검열이 가능하여 확실한 보안을 기반으로 하는 보안관제 체계를 구성할 수 있다.

제로 트러스트 보안의 도입을 통해 내부에서 외부로 나가는 '아웃 바운드 관제'가 가능해진다. 기존의 보안관제는 외부에서 내부의 보안에 상대적으로 집중되어 있다면 제로 트러스트 보안 기반의 보안관제는 내부에서의 보안도 확충하여 내부 정보 유출 사고 가능성을 줄일 수 있다. 업무 환경이 사내에만 국한되어 있지 않고 자유롭게 외부에서 접속하는 일이 빈번해지는 변화에 따라 내·외부 경계 없이 모든 접근 시도와 트래픽을 감시하는 보안관제 시스템이 필요할 것으로 보인다. 기존의 경계기반 모델과 다르게 제로 트러스트 보안을 도입하면 내부보안의 기반도 확실히 다질 수 있다. 제로 트러스트 보안은 아무것도 신뢰하지 않는다는 개념을 바탕으로 정보보안 책임자의 접근이라 할지라도 의심하여 안전한 보안 체계를 보장 한다.

5. 결 론

본 논문은 기존 보안관제 시스템의 문제점에 대해 알아보고 제로 트러스트 보안 개념을 기반으로 앞으로의 보안관제 시스템을 강화 방안을 제안

하는 논문 이다. 기존 보안관제 분야에서는 인력 부족 문제와 공격 탐지율을 높이기 위해 과탐, 오탐, 미탐과 같이 탐지와 관련한 문제를 해결해야 한다. 제로 트러스트 보안은 모든 것을 의심하고 침해당했다는 가정을 바탕으로 모든 접근과 통신에 대해 감시하며 최소한의 접근 권한만을 허용한다. 이는 공격자가 경로를 우회하여 접근하는 불법적인 공격시도를 원천적으로 막을 수 있어 보안 수준을 높일 수 있다. 엄격한 사용자 인증을 토대로 접근이 허용되면 그 외 모든 것은 의심하고 경계하는 대상이 된다. 이로써 공격에 대한 탐지율을 높여 발생할 수 있는 침해사고를 최소화할 수 있다. 현재 보안관제 시스템에서는 한정된 보안관제 인력이 막대한 양의 트래픽을 처리 및 분석하고 다양한 공격들을 빠르게 대응해야 한다. 제로 트러스트 보안을 도입하게 되면 최소한으로 허용된 소수의 접근 경로만을 관리 감독하고 나머지는 경계하게 되기 때문에 보안관제의 업무 효율성을 높이고 안정적인 보안을 보장할 수 있다.

클라우드 환경과 코로나로 인해 근무 환경이 자유로워지면서 사내뿐만 아니라 회사 외부에서 내부로의 접근도 보안을 고려해야 한다. 근무 환경이 변화하는 것처럼 보안관제 시스템의 보안 전략에도 변화가 필요하다. 제로 트러스트 보안은 내·외부를 분리하지 않는다는 점에서 기존 방식과 차이가 있다. 보안관제 분야에서도 제로 트러스트 보안을 통해 경계를 두지 않고 전체를 아울러 오고 가는 트래픽과 데이터에 대한 철저한 감시와 분석이 필요하다. 기존 보안관제 시스템의 문제점을 해결하기 위해 제로 트러스트 보안에 대한 꾸준한 논의와 분석으로 안전하고 효율적인 보안관제 시스템을 구축 해야 한다.

참고문헌

[1] 국가정보보호백서, 사이버위협 주요 이슈와 전망. 한국인터넷진흥원, 2021.

[2] IT Daily. [기고] 비대면 시대의 통합보안관제 , https://www.itdaily.kr/news/article View.html?idxno=202692, 2021. 05. 21.

[3] 컴퓨터월드. [기고] AI 기반 보안관제, 철저한 준비가 필요하다. , https://www.comworld.co.kr/news/articleView.html?idxno=49533, 2018.10.31.

[4] 월간 보안 동향, 이글루시큐리티, 2021. 09.

[5] 박학수, 정기문, 침해위협 상관분석 기반의 보안관제 시스템 설계. 한국컴퓨터정보학회, 19, 335-338. 2011.

[6] 한국인터넷진흥원. 정보보호산업진흥포털 : 보안관제 전문기업 지정, https://www.ksecurity.or.kr/kisis/subIndex/470.do, 2022.06.

[7] 정일옥, 조창섭, 지재원, 사이버 보안관제 체계 문제점과 머신러닝 적용 기술 현황. 정보보호학회지, 31, 13-19. 2021.6.

[8] 윈스. 서비스/보안관제: 보안관제 , http://www.wins21.co.kr/service/service_040100.html, 2020.10.

[9] 전용진. 금융보안과 신뢰가 비대면 금융거래에 미치는 영향. 디지털 융복합 저널, 19, 147-154. 2021.

[10] 김서영, 정경화, 황유나, 제로 트러스트 모델을 위한 딥러닝 기반의 비정상 행위 탐지. 한국정보처리학회 학술대회, 28, 132-135. 2021

[11] 보안뉴스. 기업 보안 경계를 확장하라! 제로 트러스트 모델이란?, https://www.boannews.com/media/view.asp?idx=92383&page=2&mkind=1&kind=3, 2020. 11. 06.

[12] CloudFlare. ZTNA (Zero Trust Network Access),https://www.cloudflare.com/ko-kr/teams/zero-trust-network-access, 2021.10.

[13] The National Cyber Security Centre. GUIDANCE : Zero trust architecture design principles, https://www.ncsc.

gov.uk/collection/zero-trust-architecture, 2021.
[14] DataNet. [박춘식 칼럼] 포스트 코로나, 제로 트러스트 도입할 때다, https://www.datanet.co.kr/news/articleView.html?idxno=155356, 2021.

[저자소개]

박 원 형 (WonHyung Park)

2002년 서울과학기술대 산업정보시스템 학사
2005년 서울과학기술대 정보산업공학과 석사
2009년 경기대학교 정보보호학 박사
2015년 성균관대학교 컴퓨터교육학과 박사수료
2020년 호주 타즈매니아대학교 컴퓨터사이언스 연구과정 박사수료
현재 상명대학교 정보보안공학과 부교수
email : whpark@smu.ac.kr