정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

제로 트러스트 아키텍처

박 춘 식*

요 약

최근 코로나로 인하여 원격 근무의 증대와 디지털 트랜스포메이션(DX)으로 인한 클라우드 사용의 증가, 그리고 사이버 보안에 있어서의 끊임없는 새로운 공격의 등장과 공격 면(Attack Surface)의 확대가 증가 일로에 있다. 특히 기존 네트워크 중심의 보안 방식인 경계 보안(Perimeter Security) 방식은 새로운 네트워크 환경, 새로운 형태의 근무 형태로 인한 컴퓨팅 환경의 변화, 새로운 형태의 사이버 공격 등의 다양한 공격에 대한 방어 한계 등으로 인하여 새로운 전기를 맞이하고 있다. 즉, 기존 경계 보안의 한계를 보완하기 위한 차세대 보안 개념의 하나인 제로 트러스트 보안 방식이 최근 많은 관심을 끌고 있다. 본 고에서는 제로 트러스트 보안에 대하여, 미국 국립표준기술연구소(NIST)가 발표한 제로 트러스트 아키텍처SP 800-207을 중심으로 제로 트러스트 보안 개념, 등장 배경, 제로 트러스트 기본 구성, 제로 트러스트 도입과 성숙도 모델, 제로 트러스트 아키텍처 접근 방식 등에 대하여 살펴보고자 한다.

Ⅰ. 서 론

최근 코로나로 인하여 원격 근무의 증대와 디지털 트랜스포메이션(DX)으로 인한 클라우드 사용의 증가, 그리고 사이버 보안에 있어서의 끊임없는 새로운 공격의 등장과 공격 면(Attack Surface)의 확대가 증가 일로에 있다. 특히 기존 네트워크 중심의 보안 방식인 경계 보안(Perimeter Security) 방식은 새로운 네트워크 환경, 새로운 형태의 근무 형태로 인한 컴퓨팅 환경의 변화, 새로운 형태의 사이버 공격, 그리고 횡 전개(Lateral Movement) 등의 다양한 공격에 대한 방어 한계 등으로 인하여 새로운 전기를 맞이하고 있다.

제로 트러스트 보안이 주목을 받고 있는 이유는, 경계의 내부에 있어서도 그 곳에까지 이르는 통신을 신뢰하지 않으며, 상시 통신의 상황을 가시화하여 검증한다고 하는 생각에 있다. 물론 사내의 직원을 중심으로 한 내부 부정이나 내부 범행에 한정되지 않고, 외부의 공격자가 감행하는 침해에 대해서도, 경계 방어에서는 한번 경계 내부에 대한 침입이 허용되게 되면, 보안 사고로써 현재화하기 까지는 장기에 걸쳐 알아차리지 못하는 일이 많이 발생하고 있다.

제로 트러스트 보안에서는, 통신이 어디로부터 온 것인가라는 것에 따라서 신뢰하는 것이 아니고, 누가 · 어떠한 디바이스 · 어떠한 상황 하에서 엑세스 해 왔는 가라는 사용자나 디바이스 등의 실시간 정보에 근거하여 그때마다 인증과 인가를 실시한다. 이러한 장소를 불문하는 엑세스 제어의 모델이 분산화 · 다양화된 오늘날의 IT 시스템 환경에 적합하기 때문에, 제로 트러스트 보안의 관심이 높아지고 있는 하나의 배경이 되고 있는 것이다.

Ⅱ. 제로 트러스트 기본 개념

2.1. 제로 트러스트의 역사

제로 트러스트라는 보안 개념은, 제로 트러스트라는 용어가 생겨나기 전부터, 사이버 보안개념의 하나로 이미 존재해 왔었다.

2004년부터, 네트워크 경계에서의 정적인 방어에는 한계가 있다는 생각들로 인하여, 네트워크 위치에 근거한 암묵의 신뢰, 즉 경계선을 제거하는 비 경계화(the idea of de perimeterization)의 논의가 개시되었다. 미국의 국방정보시스템청(DISA)과 국방부는 Black Core라고 불리는 안전한 조직 전략에 관한 연구를 발표하였다. 2004년에 개최된 제리코(JERICHO) 포럼에서는 대규모 네트워크 세그먼트상의 단일 정적 방어에 의존하는 것의 한계를 고려하여 비 경계화에 대한 개념을 공개했다.

* 아주대학교 사이버보안학과 (교수, cspark14@hanmail.net)

그 후, 2010 년 경에 비 경계형의 개념은 Forrester Research의 John Kindervag에 의해, 누구라도(사용자), 어디라도(네트워크), 무엇이라도(디바이스) 신용하지 않으며, 엑세스 마다 반드시 안전성을 확인한다는 보다 개선된 제로 트러스트 개념으로 발전하였다. 2017년, 계속적이며 동적인 리스크나 신용을 평가하는 가트너의 CARTA 프레임워크, 2018년 Forrester의 ZTX(Zero Trust eXtended)프레임워크 등으로 개념이 보다 확대되었다.

이후, 클라우드 서비스의 이용 확대나 원격 근무의 보급에 의해, 제로 트러스트라는 개념을 집어 넣은 보안 모델에 대한 관심이 더욱 높아져, 제로 트러스트라는 단어가 널리 사용되게 되었지만, 제로 트러스트 아키텍처는 제품이나 벤더에 따라서 다양한 실현 방법이 있기 때문에, 용어나 개념이 통일되어 있지 않은 상황이었다. 그와 같은 가운데, 2020 년8 월에 미국 국립표준기술연구소가, 용어와 개념의 공통 기반 형성을 시도하는, 제로 트러스트 아키텍처(NIST SP 800-207[1])을 발행하여, 제로 트러스트에 대한 기본적인 개념이 거의 표준으로 정리되게 되었다.

미국 바이든 대통령은 2021년 5월 국가 사이버 보안 개선에 대한 행정 명령 중에서“ 연방정부 사이버 보안 체계 현대화”를 위한 “Security Best Practice”로 ZTNA(Zero Trust Network Access) 를 채택하였고, 2022년 1월 26일 발표한 행정예산관리국(OMB)의 이행 각서에서는 연방정부의 각 부나 청은 60일 이내에 작성된 ZTNA 전략 기준과 목표를 2024년말까지 완료하도록 명령하고 있다.

특히, 미국 국립표준기술연구소의 NIST SP 800-27의 발행과 미국 연방정부에 대한 사이버 보안의 현대화의 일환으로 제로 트러스트 아키텍처 도입을 명령한 바이든 행정부의 사이버 보안 행정 명령으로 인하여 제로 트러스트 개념은 최근 더욱 더 세계적인 관심을 끌게 되었다.

2.2. 제로 트러스트 개념과 기본 원칙

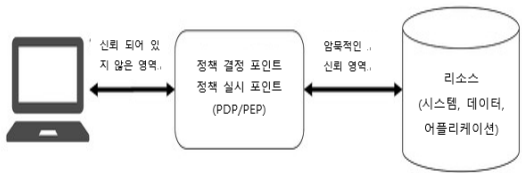
미국 기술 표준인 NIST SP 800-207에 의한 제로 트러스트와 제로 트러스트 아키텍처(ZTA)의 정의는 다음과 같다[1].

“제로 트러스트는 네트워크가 침해당한 경우라 하여도 정보시스템이나 서비스에서 요청한 최소 권한의 정확한 액세스 결정을 시행할 때 불확실성을 최소화하도록 설계된 개념과 아이디어의 집합체이다. 제로 트러스트아키텍처는 제로 트러스트의 개념을 활용하고, 구성 요소들의 관계, 워크 플로우 계획 및 액세스 정책을 포괄하는 조직의 사이버 보안 계획에 해당된다. 따라서 제로 트러스트 조직이나 기업은, 제로 트러스트 아키텍처 계획의 산물로, 조직이나 기업의 물리적이나 가상화 네트워크 인프라와 운용 정책을 가진 조직이나 기업을 가리킨다.”

이 정의는 데이터 및 서비스에 대한 무단 액세스를 방지하고 액세스 제어를 최대한 세분화하는 것을 목적으로 하고 있다. 즉 권한이 부여되고 승인된 주체(사용자, 애플리케이션/서비스, 기기의 조합)는 다른 모든 주체(예, 공격자)를 배제하고 데이터에 액세스하는 것이 가능하다. 한 단계 더 나아가 데이터라는 용어를 자원으로 대체될 수 있으므로 제로 트러스트와 제로 트러스트 아키텍처는 단순한 데이터 액세스가 아니라 자원 액세스(예 : 프린터, 컴퓨팅 자원, 사물 인터넷 등)라는 의미가 될 수 있다.

기업이나 조직이 제로 트러스트를 보안에서의 핵심 전략으로 결정하면, 제로 트러스트 원칙을 고려하여 해당 기업에 적합하게 작성된 계획인, 제로 트러스트 아키텍처를 생성하게 된다. 이 계획이 기업 내에서 제로 트러스트 환경을 구축하기 위해 전개되는 것이다. 따라서, NIST SP 800-207에서는, 이들의 조작을 정확하게 행할 때의 불확실성을 최소화하도록 설계된 개념과 아이디어의 모음으로 제로 트러스트가 정의되고 있는 것이다. 불확실성을 경감하기 위한 방법으로, 데이터나 어플리케이션 등의 리소스의 크기를 가능한 적게 하거나, 인증이나 인가, 암묵의 신뢰 영역의 축소에 초점을 맞추고 있는 것이다.

[그림1]과 같이, 신뢰 되어 있지 않은 영역(예를 들면 인터넷)에 있는 이용자가, 어떤 정책에 따라서 데이터에 엑세스하는 경우를 생각한다. 리소스에 엑세스를 희망하는 이용자는, 정책 결정 포인트(PDP), 정책 실시 포인트(PEP)에서 인증하여, 암묵적인 신뢰 영역을



〔그림 1〕 제로 트러스트 엑세스

통해서 리소스에 대한 엑세스가 허가된다.

제로 트러스트에서는, PDP/PEP와 리소스의 사이를 가능한 한 가깝게 하여, 암묵적인 신뢰 영역을 최소화 하기 위한 원칙과 개념을 제공하고 있다. 더욱이 SP800-207에서는, 이와 같은 제로 트러스트의 원칙에 근거한 네트워크 설계의 접근과, 기업에 있어서 사이버 시큐리티 전략 그 자체를 제로 트러스트 아키텍처로 정의하고 있다.

제로 트러스트 아키텍처 작성의 기본 원칙이 되는 7가지 제로 트러스트 기본 원칙은 다음과 같다. 제로 트러스트 기본 원칙은, 제로 트러스트를 실현하는 데 있어서의 이상적인 생각이 정리되어 있는 것으로,NIST SP 800-207에 제로 트러스트에 대한 중요한 에센스가 집약되어 있다고 생각된다.

1. 데이터 소스와 컴퓨팅 서비스, 모두 리소스로 본다
2. 네트워크 장소에 관계 없이, 통신은 모두 보호된다
3. 조직의 리소스에 대한 엑세스는, 모든 개별 세션마다 허가된다
4. 리소스에 대한 엑세스는 동적인 정책에 의해서 결정된다
5. 조직의 모든 관련 자산의 무결성 및 보안 상태를 모니터링하고 측정한다
6. 리소스의 인증과 인가는, 모두 엑세스가 허가되기 전에 동적이며 강력하게 점검된다
7. 자산 · 네트워크 · 통신 상태에 대해서 가능한 한 많은 정보를 수집하고, 안전성을 높이기 위해 이용한다.

1~4의 원칙에서는 엑세스 요구에 대하는 신뢰의 실현을 요구하고 있다. 이것은, 조직의 시스템에 엑세스가 있을 때마다. 어디로부터, 어느 단말에서, 누가 엑세스 하려고 하고 있는 지를 검증하여, 안전이 확인된 것 만, 엑세스를 허가해 주는 것을 말하고 있다. 5~7에서는, 엑세스 요구를 적절하게 신뢰하기 위해, 제공되어야만 하는 입력에 관한 원칙이 기재되어 있다. 1~4를 실현하기 위한 판단 재료, 즉, 로그나 정보를 모아달라고 하는 것을 요구하고 있는 것이다. NIST SP 800-207은, 제로 트러스트를 체계화 및 정리한 것으로, 앞으로 등장하게 될 각종의 제로 트러스트에 관련되는 서비스나, 솔루션을 평가하는 데에서의 레퍼런스로써 이용될 수 있다고 생각된다.

7개의 기본 원칙에 대해서 구체적인 내용은 다음과 같다.[1][2][3]

■ 데이터 소스와 컴퓨팅 서비스, 모두 리소스로 본다.

엑세스 하는 측/엑세스 당하는 측에 관계 없이 네트워크에 접속되어 있는 모든 기기를 리소스로 본다. 소형의 스토리지 기기, IoT 디바이스 등, 다양한 크기나 기능을 가지고 있는 디바이스도 리소스로 생각한다. 물론, 클라우드 서비스도 리소스의 하나로 생각한다. 더욱이 개인이 소유하고 있는 기기라고 하여도 조직의 리소스에 엑세스한다고 하면 리소스로써 생각한다.

■ 네트워크 장소에 관계 없이, 통신은 모두 보호된다

네트워크의 장소는, 회사 내부 네트워크나 사설 네트워크와 같은, 일반적으로 경계선의 내부나 외부라는 범위를 나타내고 있다. 경계형 시큐리티 모델에서는, 네트워크 경계의 내부는 안전하며, 암묵적인 신뢰를 부여하고 있었다. 제로 트러스트의 기본 원칙에는, 시큐리티 시스템으로 보호된 네트워크 경계 범위 내라고 하여도, 인터넷과 동일하게 이용 가능하는 가장 안전한 방법으로 통신을 보호해야만 한다라고 하고 있다.

■ 조직의 리소스에 대한 엑세스는, 모든 개별 세션마다 허가된다

종래의 네트워크 엑세스의 생각에는, 한번 행하여진 인증이나 허가를 일정 시간 유지하고, 성능을 효율화 한다. 그러나, 제로 트러스트에서는 모든 개별의 세션 요구마다 허가되어야만 한다. 더욱이, 엑세스 시에 허가되는 권한은, 그 엑세스에 필요한 최소한의 권한으로 해야만 한다.

■ 리소스에 대한 엑세스는 동적인 정책에 의해서 결정된다

종래의 네트워크 엑세스의 생각에는, 이미 결정된 정책에 따라서 엑세스 허가가 결정되어 있었다. 예를 들면 사용자 ID와 패스워드의 조합이나 클라이언트 증명서의 확인 등이다. 제로 트러스트에서는, 사용자 계정, 장소나 일시, 행위 및 환경 등 다양한 속성을 파라메터로 하고, 매번 정책에 따라서 계산을 행하고, 엑세스를 허가한다.

■ 조직의 모든 관련 자산의 무결성 및 보안 상태를 모니터링하고 측정한다

조직 내에 존재하는 모든 디바이스가 시큐리티를 유지하여 정상으로 동작하고 있는 상황을 감시하고, 필요에 따라서 시기 적절한 업 데이트나 수정의 실시를 요구하고 있다. 취약성이 발견되었음에도 불구하고 수정이 행하여 있지 않은 디바이스를, 시큐리티가 유지되고 있는 디바이스와 동일하게 취급하지 않는다. 조직에 접속하는 개인의 디바이스도 포함하여 항상 감시를 행하고, 시큐리티를 유지하는 것이 요구된다.

■ 리소스의 인증과 인가는, 모두 엑세스가 허가되기 전에 동적이며 강력하게 점검 된다

종래의 모델에는, 사용자에 있어서 인증 · 인가는 한 번 인정된 결과의 반복 사용이 가능하도록 되어 있었다. 제로 트러스트 기본 원칙에는, 현재 실행 중의 통신에 있어서도 계속적으로 신뢰성의 재평가를 행하고, 경우에 따라서는 재 인증의 실시가 요구되고 있다.

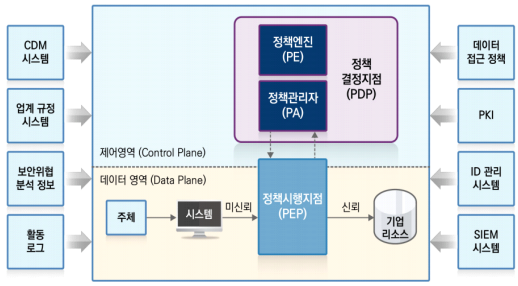
■ 자산 · 네트워크 · 통신 상태에 대해서 가능한 한 많은 정보를 수집하고, 안전성을 높이기 위해 이용한다.

자산의 시큐리티 상황, 트래픽의 상태, 엑세스 요구의 로그 등, 조직의 네트워크나 디바이스에 관련된 정보를 항상 취득하고, 더욱이 분석한 결과를 활용한 정책의 작성이나 보안의 개선을 요구하고 있다. 조직의 성장이나 기술의 진보에 따라 계속해서 변화하는 조직의 네트워크 형태나 디바이스, 사용자의 이용 상황에 따라서, 정책의 작성이나 보안 대응을 항상 업 그레이드하는 것이다.

2.3. 제로 트러스트 구성 요소

제로 트러스트의 기본 개념을 실현하기 위한 제로 트러스트 아키텍처를 구성하는 논리 컴포넌트들은 [그림 2]와 같다. [그림 2]는 제로 트러스트의 개념 프레임워크에 있어서 각 논리 컴포넌트 사이의 관계를 나타내고 있으며, 제로 트러스트 아키텍처를 제공하는 솔루션 벤더들은 논리 컴포넌트[1][2][3]의 역할에 근거한 실장에 따라, 제로 트러스트를 실현하고 있다.

[그림 2] 가운데에서도 제로 트러스트 아키텍처의 핵심(core) 논리 컴포넌트는, 정책 엔진(PE : Policy Engine)과 정책 관리자(PA : Policy Administrator)의 요소로 되어 있는 정책 결정 지점(PDP : Policy Decision Point)와 정책 시행 지점(PEP:Policy Enforcement Point)로 구성되어 있다.



〔그림 2〕 제로 트러스트에 있어서 논리 컴포넌트

- PDP : 이용자(주체)로부터의 리소스에 대한 엑세스 요구를 검증하고, 검증 결과를 정책에 적용시키는 것으로 엑세스 허가의 평가 및 판단을 행한다
- PE : 엑세스 요구의 검증과 정책의 적용
- PA : PE 검증 결과에 따라 엑세스 허가 여부를 PEP에 연계한다
- PEP : 이용자로부터의 엑세스 요구를 받아, PDP에 대한 정보를 받아, 리소스에 대한 엑세스 제어를 행한다

[그림 2]에 대한 제로 트러스트 아키텍처의 핵심 컴포넌트들은 다음과 같다.

■ 제어 영역(Control Plane)과 데이터 영역(Data Plane)

네트워크를 이용하여 수신과 데이터를 주고 받기 위해서는, 경로를 확정하여 데이터를 전송할 필요가 있다. 이때, 경로 계산이나 패킷의 전송 정책, 우선 제어, 부하 분산 등의 복잡한 처리를 행하는 것이 제어 영역이다. 제어 영역에 따라서 결정된 경로와 정책에 따라서 데이터 패킷을 전송하는 것이 데이터 영역에 해당한다. 제로 트러스트 아키텍처의 핵심 컴포넌트 중, PDP(PE와 PA로 구성)가 제어 영역에, PEP는 데이터 영역에 속하고 있다.

■ 정책 엔진(PE)

정책 엔진은 리소스에 엑세스하려고 하는 사용자에 대해서, 엑세스 허가를 결정하는 컴포넌트이다. CDM(Continuous diagnostics and mitigation)서비스나 위협 정보 인텔리전스 등의 외부 정보 소스로부터 취득한 입력을 기본으로, Trust Algorithm에 의한 신뢰도의 스코어 계산을 행하여, 리소스 엑세스의 허가,

부정, 취소를 판단한다。정책 엔진의 판단은 로그에 기록되어, 정책 관리자에 의해서 실행된다.

■ 정책 관리자(PA)

정책 관리자는, 정책 시행 지점(PEP)에 대한 조작 명령어를 통해서 사용자와 리소스 사이의 통신을 확립, 차단 역할을 하는 컴포넌트이다. 정책 엔진과는 밀접하게 결부되어 있어, 정책 엔진이 결정한 허가, 부정과 같은 판단에 근거하여 정책 시행 지점에 대해서 세션 개시나 차단과 같은 조작을 지시한다. 정책 엔진과 정책 관리자는 하나의 서비스로써 실장되는 일도 있다.

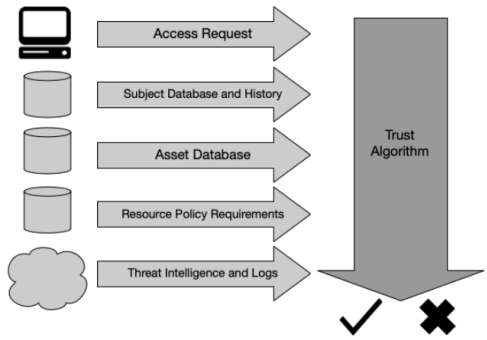
■ 정책 시행 지점(PEP)

정책 시행 지점 컴포넌트는 사용자가 리소스에 엑세스 할 때의 접속 유효화, 감시, 종료를 행한다. 정책 시행 지점은, 정책 관리자로부터 정책의 요청이나, 업그레이드 된 정책을 수신하여 동작한다. 정책 시행 지점의 실장에 대해서는, 클라이언트측 에이전트와 리소스측 게이트웨이로 나누는 방식과, 통신 경로상의 게이트 키퍼 등으로 실장 되는 방식이 있다. 정책 시행 지점과 리소스의 사이는 암묵적인 신뢰 영역이 된다.

제로 트러스트 아키텍처에는, 핵심 컴포넌트 외에도, 정책 엔진이 엑세스의 신뢰도를 계산할 때 사용하는, CDM 시스템, 업계 규정 시스템, 보안 위협 분석 정보, 활동 로그, 데이터 접근 정책, PKI(공개키 기반), ID 관리 시스템, SIEM(Security Information and Event Management)시스템 등의 추가 입력이 있다. 제로 트러스트 아키텍처의 핵심 컴포넌트는, 엑세스 요청이 있은 후 바로 동적으로 정책을 검증하고, 네트워크 엑세스시의 암묵적인 신뢰 영역을 최소화하면서, 데이터에 대한 엑세스를 가능하게 해야 한다.

제로 트러스트의 엑세스를 제어하는 컴포넌트인 정책 엔진(PE)은 [그림 3]과 같은 트러스트 알고리즘[1]에 의해서 신뢰도 스코어를 계산하여 리소스에 대한 엑세스의 허가, 부정, 취소 등을 판단한다.

[그림 3] 에서, 신뢰도 스코어 계산을 통한 신뢰 판정이라는 트러스트 알고리즘은 엑세스 요구 등 복수의 입력을 참고로, 엑세스의 가부를 판정하고 있다. 알고리즘의 입력으로는 엑세스 요구, 사용자 데이터베이스나 이력, 자산 데이터베이스, 리소스의 정책 요구,위협 인텔리전스와 로그가 있다.



〔그림 3〕 제로 트러스트 알고리즘 입력

엑세스 요구로는, 어떠한 리퀘스트가 누구에 의해서 리퀘스트되어 있는 지 입력한다. 그 때, 엑세스 해 온 단말의 OS, 사용되고 있는 소프트웨어(브라우저 버전 등), 패치 적용 레벨 등의 정보도 병행하여 입력되어진다.

사용자 데이터베이스나 이력의 입력으로는, 누가 엑세스 하였는 지에 착안하며, 이 경우 사람만이 아니라 프로그램의 프로세스 등도 포함된다. 엑세스 하는 사람의 시각이나 장소 등 사용자에 관련된 정보와 현재 엑세스 하고 있는 사용자의 입력 정보를 비교하여, 정당한 이용자가 엑세스하고 있는 지를 판정한다.

자산 데이터베이스 입력으로는, 조직이 소유하고 있는 단말의 리스트, OS의 버전, 패치 적용 레벨 등 단말 상태가 엑세스를 허가할 수 있는 레벨인 지, 네트워크 장소 등으로부터 엑세스가 허가되는 단말인지를 판정한다.

리소스의 정책 요구 항목에는, 리소스가 되는 데이터 제공 서비스나 시스템이 가지고 있는 ID, 패스워드를 시작으로, 이용 가능한 IP 주소의 제한이나 다요소 인증, 단말 설정 등 리소스 별 요구 사항에 의해 판정한다.

위협 인텔리전스와 로그 입력으로는, 사이버 공격 등에 이용된 흔적이 있는 IP 주소나 패킷 데이터, 파일 등, 공격자에게 연결될 만한 정 여부를 확인한다.

Ⅲ. 제로 트러스트 도입과 성숙도 모델

3.1. 제로 트러스트 도입[3][5][6][9]

제로 트러스트 시큐리티 개념을 도입하여 실장하는데 있어서 예상되는 기본적인 과제로는 경영진의 이

해, 비용(인력, 시간, 예산), 어디서부터 대처해야만 하는 가, 다른 툴 및 정책과의 통합, 기존 시스템과의 정합, 운용 가능한 제로 트러스트 시큐리티는 무엇일 까 등으로 생각될 수 있다. 제로 트러스트를 도입하고 실장하기 위한 가장 좋은 접근 방법은 제로 트러스트가 사업 계속성을 유지하기 위한 사이버 시큐리티 전략의 일환이며, 비즈니스에 유효한 거라고 평가하는 것이다.

기본적으로 제로 트러스트를 도입하는 방법은 NIST SP 800-207 보고서의 내용을 참조하는 것이 좋으며, 이를 실현하기 위해서는, 기존의 시큐리티를 활용하면서, 하이브리드형으로써 small start로 실시하는 것이 현실적이다. 현재, 대부분의 기업이 경계형 방어에 의한 시큐리티를 구축하고 있기 때문에, 제로 트러스트로 일제히 변경하는 것은, 비용면 · 운용면 · 인적 자원면에서 난이도가 아주 높기 때문이다. 먼저 자사의 과제를 정리하고, 무엇을 하고 싶은 지 등의 요건 정의를 정리한 다음에, 과제에 맞는 솔루션을 찾는 것이 제로 트러스트 도입에 대한 첫 걸음이라고 생각된다.

제로 트러스트 도입 후의 운용에 관해서는, 제로 트러스트는 비즈니스 영향이 적은 곳부터, 서서히 확대해 나가는 전개 방법이 되기 때문에, 적용을 해 나가면서, 어느 정도의 기간에서 재검토해 하는 것을 계획해 둘 필요가 있다. 그리고, 도입 당초는, 사용자에게 직접 영향이 나오기 때문에, 문의 등이 늘어나는 것에 대해서도 예상한 준비를 해 두는 것이 중요하다.

또한, 대상을 확대해 나갈 때에는, 업무에 따라서 비즈니스 영향이 바뀌기 때문에, 신용도 레벨의 개념도 맞추어서 보완할 필요가 있다. 그것에 맞추어서 영향을 주는 적용 부서에 알맞은 설명이 필요하게 된다. 적용 후에도 받아들여지도록, 리스크 소통을 의식하여 조정을 해 나가도록 한다. CloudStack은 가상 데이터 센터를 전달하기 위하여 턴키(turnkey) 클라우드 인프라 소프트웨어 스택을 제공한다. 이를 지원하기 위해 서비스와 소프트웨어 패키지를 간단하게 설치할 수 있도록 모든 필수 컴포넌트들을 빌드하고 다중계층(multi-tier) 및 다중 사용자(multi-tenant)의 클라우드 어플리케이션을 관리한다.

3.2. 제로 트러스트 성숙도 모델[4]

제로 트러스트 원칙에 따른 정보보호 제품을 도입하여 구축하고자 할 경우에는, 조직이 중시하는 전략에 기초하여 제로 트러스트 아키텍처를 구축할 필요가 있다. 제로 트러스트 개념 도입은, 보안 어플라이언스의 도입과 같은 단일의 기능 강화 만에 머무르지 않고, 인증 기구와의 통합이나 자동화, 가시화 등과 연계되는 통제된 구조를 구축할 필요가 있다.

제로 트러스트 아키텍처를 구축하는 것은 긴 여정과 같다고 생각된다. 물론 제로 트러스트 아키텍처 구축이 최종적인 목적이 아니며 궁극적으로 효과적인 보안 대책을 마련하고자 하는 것이다.

제로 트러스트 아키텍처 구축에는 보안 대책의 효과를 측정하면서 추진하는 것이 필요하다. 조직이 제로 트러스트 개념에 맞는 보안 대책이 마련되어 있는지를 측정하는 지표로써, 미국 사이버인프라보안청(CISA)이 발표한 제로 트러스트 성숙도 모델이 좋은 참조가 될 수 있다.

제로 트러스트 성숙도 모델은, 미국 정부 기관의 제로 트러스트 아키텍처 구축을 위하여 작성된 것이지만, 성숙도 모델의 대부분은 기업이나 조직이 제로 트러스트로의 이행을 추진하는 데 참조가 된다.

CISA의 제로 트러스트 성숙도 모델은, 제로 트러스트 아키텍처 구축의 로드 맵의 하나로써, 데이터, Identity, 디바이스, 네트워크, 워크 로드의 5가지 요소를 기둥으로 하며, 각 요소에 목표로 해야만 하는 비전과 함께 구체적인 성숙도를 나타내고 있다. 각각의 기둥에는 가시화와 분석(Visibility and Analytics), 자동화와 연계(Automation and Orchestration), 거버넌스(Governance)에 의해서 접속되는 [그림 4]와 같이 구성되어 있다.

■ 종래형(Traditional)

수동에 의한 설정과 속성의 할당으로, 정적 시큐리티 정책, 외부 시스템에 대한 의존도가 조잡한 기둥 레벨의 솔루션, 프로비져닝 시에 확립된 최소한의 기능, 독자로 유연성이 없는 정책 시행의 기둥, 수동에 의한 사고 대응과 완화 조치의 전개

■ 상급(Advanced)

기둥 간의 조정, 집중적인 가시화, 집중적인 Identity제어, 기둥 간의 입력과 출력에 근거한 정책 실시, 사전에 정의된 완화책에 대한 사고 대응, 외부 시스템과의 의존 관계의 상세화, 상황 평가에 근거한

최소 특권의 변경 등

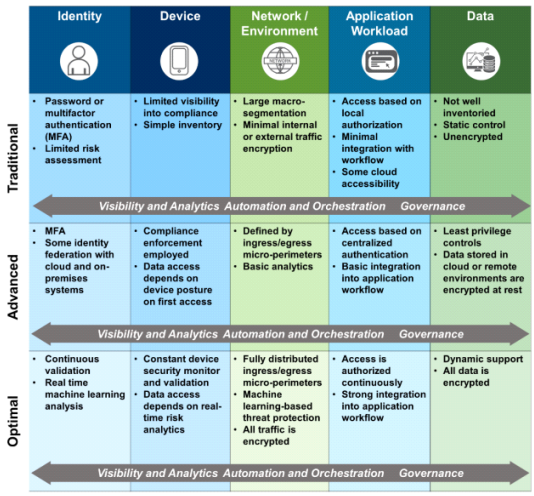
■ 최상급(Optimal)

자산이나 리소스에 대해 완전히 자동화된 속성의 할당으로, 자동화 된/관측된 트리거에 근거한 동적 정책, 자산에는 동적인 최소 특권 엑세스(임계치의 범위내)를 위한 자기 열거형의 의존 관계가 있으며, 기둥 간의 상호 운용성을 위한 개방 표준과의 연계, 포인트 인 타임에서 상태를 거슬러 올라가 확인하기 위한 이력 기능을 갖춘 집중 관리

제로 트러스트 성숙도 모델의 5가지 구성 요소 각각에 대해서 달성 기준이 명확하게 나타내어 있기 때문에, 기업이나 조직이 제로 트러스트의 계획을 세울 때, 자신들의 현 상황과 향후 목표를 명확하게 파악할 수 있다. 제로 트러스트의 이행을 지원하기 위한 제로 트러스트 성숙도 모델의 5개 기둥에 대하여 설명한다.

■ 제1 기둥 : Identity

제로 트러스트 성숙도 모델에서는, Identity는 제로 트러스트의 중핵이며, 제1 기둥으로 쓰여져 있다. 서비스마다 패스워드 인증이나 다요소 인증이 포함되어 있는 상태를 출발점으로써, 클라우드 서비스에 의한 Identity의 통합 관리가 가능한 IDaaS(IDentity as a Service)의 도입이나 계속적인 상태 평가, 기계 학습에 의한 분석과 실시간 검증, 정책에 근거한 엑세스 제어의 자동화 등이 실현된 상태를 이상적으로 하고 있다.



〔그림 4〕 제로 트러스트 성숙도 모델

■ 제2 기둥 : 디바이스

제2기둥은 디바이스 보안이다. 디바이스에는, 컴퓨터나 서버만이 아니라, IoT 디바이스, 스마트 폰, 모바일 디바이스 등, 기업의 시스템에 접속된 하드웨어 디바이스가 포함된다. 더욱이, 기업이나 조직이 관리하는 Managed Device만이 아니라, 직원이 소유하는 단말을 업무 사용하는 BYOD(Bring your own device)도 고려해야만 하는 대상으로 열거되어 있다.

성숙도 모델에서는, 기업이나 조직이 네트워크에 접속되는 보유 디바이스의 가시화를 중심으로, 보안 설정, 취약성 관리의 상태, 이용 가능한 스토리지 용량, 하드웨어 보안 기능의 이용 등 보안 상태 파악과 실시, 이에 근거한 실시간 리스크 분석이 가능한 상태를 이상적으로 하고 있다.

디바이스 그 자체의 소유가 기업／개인 불문하고, 데이터에 엑세스하는 디바이스를 항상 가시화하고, 컴플라이언스를 자동적으로 적용할 수 있는 제어가 요구된다。또한, 어디에서도 사용할 수 있는 모바일 디바이스, 모바일 어플리케이션의 보안 강화도 중요시 되어 있다.

■ 제3 기둥 : 네트워크

제로 트러스트의 기본 사고가 깊이 나타나는 것이 네트워크에 있어서의 보안 대책이다. 제로 트러스트 원칙이, 네트워크 장소에 의존한 암묵의 신뢰를 배제하는 것에 있기 때문에, 데이터에 엑세스 할 때의 네트워크의 범위를 할 수 있는 데까지 적게 하는 것을 목표로 한다. 역시 여기서도, 가시화와 분석의 능력을 향상시켜, 네트워크 상의 행동의 세밀한 감시에 의해서 자동적으로 네트워크 침해에 대한 대응이 이상적인 상태로써 작성되어 있다.

■ 제4 기둥 : 워크로드(어플리케이션)

워크로드는, 온프레미스 서버나 클라우드 서버 상에 구축된 시스템이나 서비스, 프로그램 그 자체를 나타낸다. 더욱이 컨테이너 등의 어플리케이션 실행 엔진도 워크로드의 범위로써 생각된다.

데이터베이스에 보존된 ID와 패스워드의 조합 등의 정적인 속성에 따라서 어플리케이션 마다 인증되는 종래의 상태에서, Identity 관리와 통합된 집중 관리된 인증 인가와 감시, 어플리케이션의 취약성 검증이나 테스트의 자동화, 모든 트래픽의 암호화, 고정적이지

않는 시큐리티 강화와 성능에 따른 자동화 등이 이상적인 상태가 되고 있다.

CISA는, 제로 트러스트 이전부터 CDM 프로그램이라는 취약성의 관리와 대책의 자동화 프로그램을 제공하고 있다. 미국 정부에 제시된 제로 트러스트 이행 계획에는, CISA의 CDM 프로그램을 이용함으로써, 네트워크 상의 자산의 관리나 취약성의 진단과 완화의 구조를 요구하고 있다. 기업이나 조직에서 동일하게, 모바일 단말을 포함하여 보유 디바이스 모두를 관리하는 EMM(Enterprise Mobility Management)이나 MDM(Mobile Device Management)의 활용에 따라서, 자산의 가시화가 가능하다.

■ 제5 기둥 : 데이터

데이터는, 디바이스, 어플리케이션, 네트워크 상에서 보호할 필요가 있다. 기업이나 조직에 있어서, 데이터는 반드시 지켜야만 하는 대상으로써 인식되어 있는 것으로, 모든 것이 적절하게 관리되어 있는 상태는 현실적으로는 어려우며, 많은 기업에서는 중요한 데이터를 수작업으로 분류하여 관리의 대상으로 하는 방법이 채용되고 있다.

Identity나 디바이스의 시큐리티가 높아졌다고 하여도, 지켜야만 하는 데이터의 소재가 파악할 수 없는 상태에서는, 적절한 보안 대책이 될 수 있다고는 할 수 없다. 성숙도 모델에서는, 데이터에 대한 자동적인 추적을 가능하게 하고, 계속적인 인벤터리(장부) 관리를 이상적인 상태로 하여 정하고 있다.

제1기둥에서 제4기둥까지의 대책과 함께, 지켜야만 하는 데이터가 어디에 존재하고, 어떻게 관리되어 있는 가를 계속적으로 제어할 수 있는 구조가, 제로 트러스트 아키텍처에서는 요구된다.

Ⅳ. 제로 트러스트 아키텍처 접근 방식

다른 많은 정보보호 아키텍처와 동일하게, 제로 트러스트 아키텍처를 설계나 구현할 때에도 다양한 접근 방식이 있다. 이러한 접근 방식은 사용되는 구성 요소와 조직에 대한 정책 규칙의 주요 요소에 따라 다르다. 각 접근 방식은 제로 트러스트의 모든 원칙을 구현하지만 정책의 주요 요소로 한두 개(또는 한 구성 요소)를 사용할 수 있다.

완전한 제로 트러스트의 솔루션에는 다음 세 가지 접근 방식의 요소가 모두 포함된다. 접근 방식[1][5]에는 마이크로 세그먼테이션(Micro-Segmentation), 소프트웨어 정의 경계(Software Defined Perimeter), 향상된 ID 거버넌스(Enhanced Identity Governance)가 포함된다. 이러한 접근 방식은 상호 배타적일 필요는 없으며, 서로 조합하는 등의 경우도 생각할 수 있다.

4.1. 마이크로 세그먼테이션

게이트웨이 등 보안 구성 요소로 보호되는 고유한 네트워크 세그먼트에 개별 또는 자원그룹을 배치하여 제로 트러스트 아키텍처를 구현하는 접근 방식이다. 다시 말하면, 네트워크를 작은 논리 세그먼트(마이크로 세그먼트)로 분할하여, 세그먼트 사이에 지능형 스위치 또는 차세대 방화벽과 같은 인프라 기기 또는 게이트웨이 기기를 배치하여 각 자원 또는 관련 자원의 소규모 그룹을 보호하는 PEP 역할을 하는 것으로, 클라이언트, 자산 또는 서비스의 개별 요청에 이러한 게이트웨이는 동적으로 엑세스 권한을 부여한다.

통상의 세그먼트에는 복수의 서버 단말이 배치되고 있지만, 마이크로 세그먼트는 서버마다 전용의 방화벽을 두는 이미지다. 통상, 가상 기반 상의 소프트웨어 방화벽에 의해서 실현되며, 허가된 End Point만이 마이크로 세그먼트 내의 어플리케이션이나 데이터에 액세스할 수 있다.

특정 사용자, 디바이스, 어플리케이션만을 허가하는 독자의 Rule set을 집중 관리하여, 아주 자세하게 제어할 수 있다. 마이크로 세그먼테이션은, 종래의 경계형 시큐리티에 있는 서버 팜의 보호를 더욱이 강화하는 수법이라고 할 수 있다. 지금까지도, VLAN, 라우터, 방화벽, 네트워크 액세스 제어 및 액세스 제어 리스트(ACL)를 사용하여 세그먼트 사이의 통신을 보호해 왔지만, 마이크로 세그먼테이션에서는, 이 정도를 보다 세심하고 엄밀하게 관리하는 수법이 된다.

마이크로 세그먼트 간의 통신은, 최소 권한으로 허가된다. 즉, 기본적으로는 차단되며, 정말로 필요한 어플리케이션 통신만이 흘러가는 것을 허가한다. 이것에 의해, 동일한 네트워크 상에 있는 서버 사이라고 하여도 불필요한 통신은 되지 않는다. 수평 이동이나, 멜웨어 확산을 막는 직접적이며 유효한 수단이다. 그러나, 이렇게 제로 트러스트 아키텍처를 구현하는 데에는 2가지 과제가 있다.

하나는 운용 부하의 문제다. 동적으로 변화하는

ICT 기반에서 마이크로 세그먼테이션을 유지하는 것은, 작업량이 엄청나게 많다. 매일 새로운 어플리케이션, 네트워크, 사용자, 디바이스가 배치되는 데 따라서, 최신의 시큐리티 정책을 유지해 나가는 것은 쉽지 않다. 다른 하나는, 멀티 클라우드와 모바일에 의한 워크로드 분산의 문제다. 자사 데이터 센터에 LAN으로 부터액세스 한다고 하면, 모두 마이크로 세그먼트화가 될 지도 모른다. 그러나, 지금은 복수의 데이터 센터와 클라우드 환경상의 다양한 어플리케이션이나 다양한 장소로부터 액세스해 오는 다양한 사용자가 있다. 더욱이 비즈니스의 변화에 따라서 직원이나 협력 회사가 조직에 참가하거나 퇴직하거나 하는 등, 사용자의 변화가 심해지고 있다.

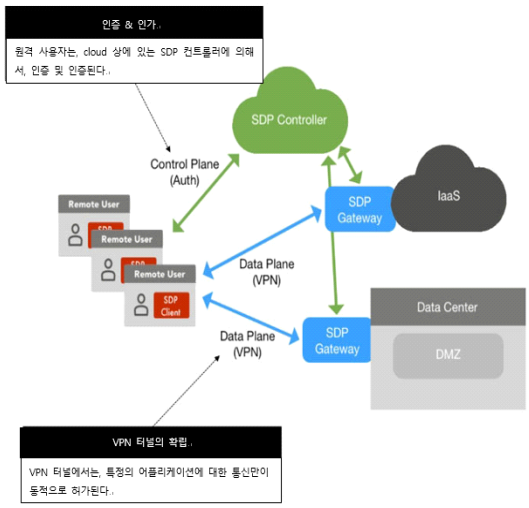
4.2. 소프트웨어 정의 경계(SDP)[7][8][10]

소프트웨어 정의 네트워크(SDN)나 소프트웨어 정의 데이터센터(SDDC)등의 기존 기술과 공통의 개념이 많으며, 오버레이 네트워크를 사용하여 제로 트러스트 아키텍처를 구현할 수 있다. 소프트웨어 정의 한계(SDP:Software Defined Perimeter)는, 사용자와 어플리케이션을 소프트웨어 상에 정의된 정책에 근거하여 접속하도록 하며, 정책이 사용자와 어플리케이션이 되기 때문에, 마이크로 세그먼테이션에 비하여 간단하다.

사용자는, 클라우드 상의 SDP 컨트롤러로 인증, 인가를 받아, 허가되면 IaaS상이나 데이터 센터에 있는 SDP 게이트웨이와 동적으로 통신 Tunnel(IP-SEC이나 TLS의 VPN)을 확립한다. SDP 게이트웨이는 IaaS상에도 배치될 수 있기 때문에, 클라우드에 의해 분산하는 네트워크에도 대응할 수 있다.

종래의 인터넷 VPN에서는, 네트워크 레벨의 접속이 행하여 지게 되며, 통신 내용에 대한 인가는 포함되지 않았다. 그 때문에 공격자가 한번 접속하면, 본래 허가되어 있지 않은 관리자 통신(SSH 등)을 행하거나, 감염 단말이 멜 웨어를 확신하거나 하는 문제가 있었다. 그러나, SDP에서는 SDP 컨트롤러로 관리하여, 허가된 통신만 될 수 있다. 원격 사용자의 ID가 도난당하거나, 직원이 악질 행위에 가담하거나 하여도, 불법 액세스를 방지할 수 있다.

원격 사용자가 접속할 때에, 디바이스의 검증도 행하여진다. OS의 종류, 바이러스 대책의 상황, 액세스



〔그림 5〕 소프트웨어 정의 경계 (SDP)의 아키텍처

시각, 기타의 파라메터를 포함한 검증을 근거로, 인가 정책을 실시할 수 있다. 이것에 의해, 디바이스를 신뢰하지 않는다라는 관점에서도 제트 트러스트 아키텍처를 구현한다. 이러한 관점에서, 종래의 인터넷 VPN과 비교하면, SDP는 인증, 인가, 디바이스 검증에 있어서 안전성을 높이고 있는 기술이라고 할 수 있다.

4.3. 향상된 ID 거버넌스

향상된 ID 거버넌스 접근 방식은 정책 생성의 핵심 구성 요소로 행위자의 ID를 사용하는 것으로 전사적 자원 엑세스 정책은 ID 및 할당된 속성을 기반으로 한다. 향상된 ID 거버넌스 기반 접근 방식은 개방형 네트워크 모델, 방문자 액세스가 있는 기업 네트워크 또는 네트워크에서 빈번한 비 기업용 기기를 사용하여 사용되는 경우가 많다. 네트워크 액세스는 처음에 모든 자산에 부여 되지만 기업 자원에 대한 액세스는 적절한 액세스 권한이 있는 ID로 제한된다.

향상된 ID 거버넌스 접근 방식의 대표적인 기술 중의 하나인 ID 인식형 프록시(IAP: Identity Aware Proxy)는, 사용자가 어디에 있어도 공통으로 제트 트러스트 개념을 적용하려고 하는 기술이다. ID 인식형 프록시 방식은 사용자의 ID를 인식하여 인증, 인가를 행하는 프록시 서버를 통하여, 어플리케이션에 액세스하며, 이 때 클라이언트의 검증도 행하여, 단말의 패치 상황 등의 안전성을 확인한 다음에 접속을 허가하는

구조다.

IaaS내, 데이터센터 내에 대한 통신은, SDP에 있어서 SDP 게이트웨이와 같은 컴포넌트인 커넥터를 이용한다. 이 커넥터는, 내부로부터 외부로 향하는 세션만이 행하여지기 때문에, IaaS나 데이터센터에 밖으로부터 내부로의 통신은 발생하지 않아 안전하다. 또한, 인증의 연계 기능에 의해, SaaS에 대한 인증도 포함하여 통일할 수 있다. 이것은 외부의 ID 제공자를 이용하여 인증을 중계하는 패턴과, IAP 자신이 ID 제공자 기능을 가지고 인증을 제공하는 패턴이 있어, 모두 제공 예가 있다.

이와 같이 IAP에서는, IaaS, SaaS, 데이터 센터로 분산하는 멀티 클라우드 환경에 대해서 입구를 통합하여, 간단한 접속과 인증, 인가를 실현할 수 있다. 이 IAP를 사내도 사외로부터의 원격 엑세스도 평등하게 적용하는 것으로, 제트 트러스트 형의 엑세스 제어를 실현한다.

Ⅴ. 결 론

본 고에서는 차세대 보안 분야의 핫 이슈로 떠오르고 있는 제로 트러스트 보안에 대해서, 미국 국립표준기술연구소(NIST)가 발표한 제로 트러스트 아키텍처 SP 800-207을 중심으로 제로 트러스트 보안 개념, 등장 배경, 제로 트러스트 기본 구성, 제로 트러스트 제로 트러스트 도입과 성숙도 모델, 제로 트러스트 아키텍처 접근 방식 등에 대하여 살펴보았다.

본 문에서 살펴본 바와 같이 제로 트러스트 개념은 경계 시큐리티 문제점을 개선한 데이터(리소스) 중심의 시큐리티 개념이다. 또한, 제로 트러스트가 대처하는 것은, 기술적인 문제가 아니라 비즈니스 상의 문제이며, 단일 제품이나 솔루션으로 완성되는 것이 아니라 복수의 기능에 의해서 구성되는 전략적인 대응이며, 단 하나의 방식만이 올바른 제로 트러스트 접근 방식이 아니라 여러가지 방식이 존재할 수 있는 설계 개념, 또는 전략, 문화 그리고 철학이라고 생각된다.

따라서, 제로 트러스트 아키텍처 도입 구현은 경계 방어와 함께 공존하는 하이브리드 형태의 제로 트러스트 접근 방식이 유효할 것으로 생각되며 경영자는 물론이고 조직 전체의 이해가 필수이며 소통이 절대적으로 필요한 긴 여정으로 생각하는 것이 좋을 것으로 판단된다.

제로 트러스트는 종래의 경계형 방어에 있어서 해결책은 되지만, 완벽한 시큐리티 모델은 아니다. 제로 트러스트에 의해서 네트워크 형태에 대한 의존은 해소되지만 위협은 존재한다. 즉, NIST의 SP 800-207에서는 언급한 제로 트러스트 아키텍처에 대한 7가지 위협, 제로 트러스트 아키텍처의 결정 프로세스 전복, 파괴, 서비스 거부, 네트워크 중단, 크레덴셜의 탈취, 내부 위협, 네트워크에 있어서 가시성, 보존된 네트워크 정보, 독자 데이터 포멧에 대한 의존(벤더 의존), AI에 의한 제로 트러스트 아키텍처의 관리 등이 존재한다. 물론 이 외에도 위협은 존재하는 등, 제로 트러스트 보안 모델도 완벽한 것이 아니므로 시큐리티 운용에 있어서 적절한 감시, 검증 그리고 감사 등 적절한 보안 대응은 계속될 필요가 있다.

참 고 문 헌

[1] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207, Aug. 2020.

[2] 최지선, “「美 NIST, 제로 트러스트 아키텍처(ZTA)」 보고서 분석 및 시사점 검토”, 금융보안원, 전자금융과 금융보안, 제22호, pp. 194-214, 2020.

[3] 박춘식, “제로 트러스트(ZT)와 금융 보안에서의 대응”, 금융보안원, 전자금융과 금융보안, 제27호, pp. 2-14, 2022.

[4] CISA, Zero Trust Maturity Model, Pre-decisional Draft, Ver. 1.0, Jun 2021.

[5] @IT, テレワークやデジタルテクノロジーの活用が前提の時代に求められる「デジタルトラスト」とは, セキュリティ, 3.2020.

[6] 獨立行政法人情報處理推進機構(IPA), ゼロトラスト導入指南書, 6.2021.

[7] CSA, *Toward a Zero Trust Architecture,* 2021

[8] Cloud Security Alliance SPD and Zero Trust Working Group. *Software-Defined Perimeter (SDP) and Zero Trust.* Cloud Security Alliance. July. 2020. https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/

[9] PWC, ゼロトラストの現狀調査と事例分析に關する調査報告書, 3. 2021.

[10] Juanita Koilpillai and Nya Alison Murray,

Software Defined Perimeter (SDP) and Zero Trust, 2020.5 https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/

[11] 박춘식, “제로 트러스트 보안(Zero Trust Security) 동향”, 정보통신기획평가원 주간기술동향, 2098호, 2023.7.5.

〈저 자 소 개〉

박 춘 식 (Choon Sik Park)
종신회원
1995년 : 일본동경공업대공학박사
1982년~1999년 : 한국전자통신연구원 책임연구원
2000년~2008년 : 국가보안기술연구소 소장
2009년~2017년 : 서울여자대학교 정보보호학과 교수
2018년~현재 : 아주대학교 사이버보안학과 교수
<관심분야> 클라우드보안,제로트러스트, 사이버안보, 우주안보