특집 07

클라우드 컴퓨팅환경변화에 따른 제로트러스트 네트워크 구현을 위한 보안시스템

조이남 · 박완성 (금융정보시스템연구회), 최우봉 · 한동우 · 이무성 (MLSoft(주))

목 차

1. 서 론

2016년6월 스위스 다보스포럼에서 클라우드 슈밥이 전 세계 환경을 정보통신기술융합으로 인공지능(AI), 사물인터넷(IoT), 로봇공학, 드론, 자율자동차, 가상현실(VR), 3D프린팅, 생명공학, 재료공학, 에너지저장기술, 퀀텀컴퓨팅(Quantum Computing)등이 주도하는 4차산업혁명이 일어날 것이라고 언급했다[9].

우리는 이들의 변화를 “인간을 위한 현실과 가상의 융합[1]”이라고 정의하고 4차산업혁명에서는 AI와 빅데이타를 이용한 새로운 시장인 핀테크, 밀리테크, 바이오테크, 에듀테크, 에그로테크 등 xTech기술에 의한 새로운 시장이 열리고 있음을 감지하게 되었다[10].

1) 현실 : off-line(IoT, Machine Learning)
가상 : On-Line(Cloud, Big Data)
융합 : AT(Analog Tranformation), 출처(KCERN)

2019년 말부터 발생한 신종 코로나바이러스(이하 “COVID-19”라함)로 인하여 WHO가 “펜데믹”을 선언하기에 이르렀다. 우리나라는 2020.1월초 최초COVID-19환자가 발생하여 2월 중순 특정종교 집단에 의한 급격하게 감염화자가 증가하였다. 이로 인하여 직장 폐쇄조치가 실행되고 소극적으로 관망하던 공공기관과 기업들이 원격근무, 분산근무, 재택근무 등 방안을 채택하게 되었다. 그 후 어느 정도 진정국면을 갖다가 이태원 클럽발 2차 감염사태로 인하여 COVID-19가 영속성 위협이 될 것으로 판단되었다.

4차산업혁명과 5G의 초지능, 초연결시대와 더불어 Post COVID-19 시대를 대비한 비즈니스 환경이 on-Premise환경에서 Cloud환경으로의 전환은 불가피하게 확산되고 있다.

현실과 가상의 융합구성 요소인 ICBAM (IoT, Cloud BigData, AI, Machine Learning)은 상호간 Digital Tranformation과 Analog Tranformation

이 이루어지며, 이들은 공개된 인터넷상에서 이루어지고 있어 이에 따른 네트워크 통신보안의 중요성이 강조되고 있다.

2007년부터 미국방성은 GIG(Global Tranformation Grid)블랙코어 네트워크 우선권에 따라 DISA(Difense Information Syatem Agency)에서 수행한 컴퓨터보안 접근방식인 블랙 클라우드(Black Cloud)라고 불리우는 SDP(Software Defined Perimeter)를 도입사용하고 있다.

SDP는 신원기반으로 리소스에 대하여 에세스를 제어하는 프레임워크로 네트워크장치, 단말의 상태, 사용자ID를 체크하여 권한이 있는 사용자 및 디바이스에 대하여만 엑세스 권한을 부여하며 인증받지 못한 단말기에 대해서는 어떠한 서비스 연결정보를 받지 못하게 되며, 인프라 인증 및 인가가 되기 전에는 DNS정보나 IP주소를 알 수 없는 “블랙 클라우드로(Black Cloud)네트워크로 동작이 되어 해커들이 보안을 통과할 수 없도록 되어있다.

따라서 우리나라에서도 SDP의 철학을 갖은 소프트웨어를 도입 사용해야 될 것으로 판단되어 이에 대한 검토를 하고자한다.

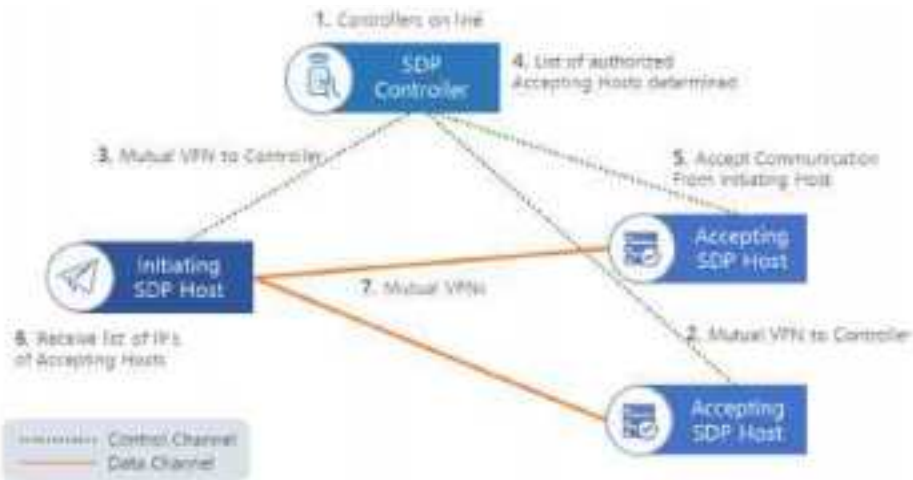
2. SDP의 특징

SDP는 보안을 위한 새로운 접근법으로 Cloud, DMZ Zone 및 데이터 센터 기반 시설들에게 동적으로 규정된 경계(perimeter)를 만들어 네트워크 공격을 최소화 한다.

SDP 아키텍처는 단일 패켓 인증, 상호전송 계층보안, 장치검증, 동적방화벽 및 애프리케션 바인딩의 5개 계층 의 보안 제어로 구성되며 이러한 프로토콜들은 공격자가 보호된 응용프로그램에 접근하는 것을 어렵게 만든다[8].

2.1 Single Packet Authorization(SPA)

SDP의 핵심목표중 하나로 Application기반 시설이 효과적으로 숨겨지거나 감지되지 않도록 해준다. DNS정보 또는 IP주소가 보이지않는다.



(그림 1) SDP Framework developed by CSA

SPA는 SDP가 허가되지 않은 장치로부터 모든 트래픽을 거부한다. Controller의 첫 번째 packet은 보호된 서비스의 접근이 시행되기 전에 허가된 장치인지 암호학적으로 검증된다. 만일 가시성이 부여되면 SPA는 허가된 사용자로부터 발생한 거래인지 확인하기 위하여 Gateway를 다시 enable하고, 모든 거래는 거부한다.

2.2 Mutual Transport Layer Security(mTLS)

SSL로 알려진 TLS는 인터넷상에서 비밀 통신을 시행하기 전에 장치인증을 제공하는 기능인데 표준으로 상호인증하기 위하여 만든 기능이다. 실제 운영 시에는 서버가 고객을 확인하지만 고객이 서버를 확인하지는 않는다. SDP는 완전한 TLS표준을 제공한다. 상호또는 two-way로 암호화된 인증기능을 사용한다.

2.3 Device Validation(DV)

mTLS는 SDP에 접근하는 장치가 취소되지 않거나 유효기간내에 개인키를 소유하고 있는지 검증한다. 다만 그 키가 도용해온 키 인지는 검증하지 않는다. DV는 그 키가 정당한 장치에 의하여 소유되었는지 검증한다. 또한 DV는 그 장치에 신뢰받는 소프트웨어가 실행중인지 그리고 적절한 사용자에 의하여 사용되고 있는지 검증한다.

2.4 Dynamic Firewalls(DW)

일반적으로 IP패킷내에 주소정보를 기반으로 입출을 제한하는 고정된 구성요소를 사용하는 전통적 방화벽에 익숙하다. 대부분의 현재사용중인 방화벽은 아주 많은 방화벽 룰(firewall rull)을 가지고 있다.

SDP는 하나의 룰만 가지고 있는 Dynamic Firewall을 채용하여 모두를 거부하며, 각 장치 간 통신은 방화벽 정책을 동적으로 입력하여 개별적으로 적용한다.

2.5 Application Binding(App B)

장치와 사용자를 허가하고 인증한 후에 SDP는 보호된 사용하려는 프로그램(Application)과 암호화된 TLS를 제공한다. Application Binding은 허가된 프로그램만 사용하도록 제한한다.. 암호화된 터널을 통해서만 접근이 가능 하게된다.

기존의 MPLS(Multi Protocol Label Switching), SD-WAN(Software Defined-Wide Area Network), VPN(Virtual Private Network) 등을 사용하는 경우 네트워크와 보안환경 변경시에는 Location, Hardware, Service-Provider 등의 제약조건이 발생한다. SDP사용자는 ID Centric으로 서버부분은 Application Centric으로 구성되어 쉽게 보안환경 변경관리와. 유지가 가능하게 된다.

또한 SDP아키텍처는 Server, Application, Data등 중요 정보자원을 Gateway로 은폐하여 보호하는 방식이며, 사용자는 단말장치에 설치된 Agent를 통하여 신원과 장비를 controller로부터 인증 받은 후에만 Gateway에 접속정보를 전달받아 Gateway로 접근할 수 있다.

SDP는 Gateway, Agent, Controller로 구성되는 소프트웨어 모듈로 구축이 간편하다.

3. SDP 운용방법

기존의 VPN은 선 접속 후 인증인증 방식으로 원격지 접속시 서버정보가 노출될 뿐만 아니라 VPN접속이후 내부 네트워크상의 다른 네트워크 자원에 접근이 가능하게 되는 보안의 위협요소를 내포하고 있다.

SDP는 선 인증 후 접속 방식으로 접속 서버가 노출되지 않으며, 접속 후에도 App-binding[2]을 통하여 지정된 서비스에만 접속하게 되어 기존 VPN을 대체할 수 있다.

기업이 기존 레거시 시스템에서 SDP환경으로 전환 할 경우에는 .복잡하게 구성된 IT환경 때문에 어려움 있지만, 클라우드로 전환하는 시점에서는 쉽게 검토 할 수 있고, SDP는 제로 트러스트 네트워크 모형 도입에 큰 기여를 할 수 있다. 제로 트러스트 모형에 가장 근간이 되는 신원기반으로 화이트 리스트의 사람과 장비만 허용하고, 대상 서비스를 숨길 수 있기 때문이다.

(그림 2) App-binding 시 허용 App연결 외 차단

4. SDP의 일반적인 활용

4.1 업무망과 인터넷망의 환경개선

보안담당자와 네트워크관리자들이 인사이동시 또는 외부근무 시 IoT들에대한 정책변경 및 보안 관리를 위하여 많은 시간을 투자하고 있다. 앞으로 Digital Transformation시대에 적용 하려면 더 많은 변경작업과 빈번한 보안사고가 발생하여 더 많은 노력이 가중될 것이다.

AI와 BigData, 클라우드 환경으로 적용하려면 전환이 필수적이며, 개방형 인터넷도입과 전 세계에 산재해있는 사용자들의 접근을 제어하려면 기존의 보안체제를 유지하기 어렵기 때문에 Network Centric접속관리에서 ID Centric접속 관리로 전화해야하며 SDP가 최적의 솔루션이 될 것이다.

4.2 망분리 체계전환

망 분리는 온 프로미스 환경에서 기존 보안시스템은 최적의 보안 환경이었지만 구축비용이 비싸고 업무효율과 속도가 떨어지고 있으며, 작업공간에 대한 제약이 많고 또 클라우드 환경에서는 적합하지 않다는 단점이 있다.

SDP는 해킹대상을 숨기고 지정된 Appication에만 접속이 가능하며 DDoS공격을 원천적으로 차단하고 화이트리스트 방화벽기능을 갖는다. Third Party Solution을 추가하면 정보유출도 방지할 수 있다.

4.3 원격근무용으로 사용

COVID-19사태와 근무처가 바뀌는 등의 업무 자유도가 높은 환경에서는 SDP와 VDI또는 SDP와 Sandbox등을 사용하면 내부서버 보안과 외부 자료 유출방지가 가능하게 된다. VDI나 Sandbox가 사용 어려운 고객은 원격제어 프로그램(Remote Control Agent)을 이용하여 업무망에 위치한 본인의 PC를 원격으로 접속하여 재택근무가 가능하다.

원격제어를 이용한 재택근무 시에는 기존의 망분리 체계를 그대로 유지한 상태에서 VPN보다 높은 수준의 보안을 제공하고 구축과 운영이 간단하고 쉬우며 향후 증설이 쉽고, 콜센터에도 유사 구

2) App-Binding 이란 네트워크 접속권한을 관리할 때 서버의 IP나 Port외에도 접속이 가능한 App을 지정하여 허가된 App가 아니면 통신이 불가능 하도록 제어하는 기술

축이 가능하다.

SDP는 App-binding기능을 제공하는데 PC Agent를 통하여 지정된 소프트웨어를 사용해야만 서버에 접속할 수 있는 방법과 제공되는 표준 API를 이용하여 그룹웨어, 메신저, 이메일 등의 개별 앱을 개발 연동하여 접속을 제어하는 방법등 2가지를 제공한다.

App-Binding을 할때에는 허용되는 App을 이용하여 서버에 접속한 온라인 상태라도 해당 App 외에 다른 소프트웨어로는 접속이 불가능 하다.

SDP 시스템은 제로트러스트를 제일 중요시하고 필요한 사람과 장비만허용하는 정부기관, 금융기관, 특별한 성격을 가진 군 기관과 보안을 최우선하는 연구기관 등에서 사용하는 것이 좋다.

5. 재택근무

기존의 On-Premise환경에서 각 요소와 단계마다 다양한 전용보안 시스템을 겹겹이 설치하여 네트워크 기반의 보안 체계를 구성하여 운영하고 있다.

금융기관의 예를 들면 내부로의 접점에는 외부 방화벽으로부터 Proxy, IPS, 물리적 망분리에 내부방화벽을 설치하고, 서버 단에는 서버접근제어, DB보안, 서버 백신과 엔드포인트 단에는 IP관리, NAC, 백신, DLP, 개인정보보호, 메시지 제어시스템 등 시스템이 겹겹이 설치되어 있다. 이렇게 제한적으로 접속을 통제하여 강력한 기능으로 중요한 보안을 책임져 왔다. 네트워크, 보안 담당자들이 인사이동이나 지사를 신설하는 경우 또는 COVID-19 사태로 인하여 재택근무 시에 망분리에 대한 예외사항을 만들어 업무에 차질이 발생하지 않도록 해야 한다.

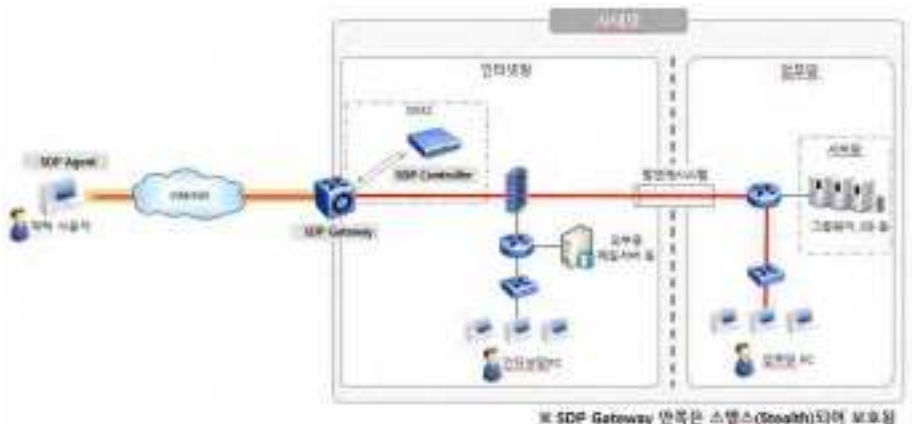
최근 금융보안원에서는 금융회사가 안전하고 신속하게 재택근무 환경을 구축할 수 있도록 필요한 보안 지침서를 안내하여 주고 있다[11].

5.1 SDP사용 재택근무

SDP는 전자금융감독규정 시행세칙 중 망분리 대체 정보보호 통제사항을 대부분 만족하고 있다.

SDP와 NAC 그리고 원격제어 프로그램을 하나의 플랫폼으로 통합한 제품은 서로의 event를 감지하여 재택근무 보안 정책에 대해 NAC의 통제가 원활할 수 있다.

타장비를 사용하여 재택근무를 할 경우에는 금



(그림 3) SDP사용 재택근무시 약도

감원에서 제시한 보안지침서에 알맞은가를 검토해 보아야 한다. .

5.2 SSL VPN을 사용

SSL VPN은 웹브라우저에서 지원되어 인터넷을 이용한 가설망을 구성하며 클라이언트에서 별도의 프로그램 없이 사용이 가능하다. IPsec VPN에비교하여 방화벽 통과와 NAT지원이 쉽다. SSL VPN은 Clientless모드, Thin-Client모드, Tunnel모드 등으로 접속방법을 지원한다.

Clientless모드에서는 웹사용 어프리케이션을 지원하며,Thin-Client모드에서는 자바 애프릿을 이용하여 port-forward기능을 지원하며 웹외에도

〈표 1〉 재택근무 방식비교(SDP, SSL-VPN, VDI)

구분	SDP	SSL VPN	VDI
개념	외부단말의 특정프로그램과 사내 서버의 특정 프로그램과의 네트워크 경계를 만들어 사용	외부단말기와 네트워크를 VPN으로 연결	외부단말기는 Dummy터미날역활을 하고 서버에 있는 OS를 이용 업무연결
인증방법	선 인증 후연결 (제어채널과 데이터 채널 구분)	선 연결 후인증 (광 범위노출)	SDP,사용시;선인증 후연결 SSLVPN사용시,선영결 후인증
연결(노출)	App to App연결방식으로 권한 없는 서버는 노출되지 않음	가상 사설망 내의 모든 서버 IP와 오픈된 서비스포트 노출	SDP사용시;서버노출않됨 SSLVPN사용시;서버노출
터널 생성	외부단말기의 특정 프로그램과SDP G/W간 터널형성	외부단말기와VPN G서버간 터널형성	터널 생산 않함
에이전트 프로그램	전자금융감독규정 시행세칙준수를 위하여 반드시필요(Application binding 지원)	국내는 대부분 에이전트 방식임	VDI공급언체마다 Agent는 선택적임
서비스 대상	Zero trust 환경에서 안전하게 사내 서버에 엑세스하려는 사용자	외부에서 사내의 네트워크 자원에 연결하고자하는 사용자	외부에서 사내 가상 단말기에 연결하고자하는 사용자
방화벽 운영방식	White List방식, IP기반 동적설정(운영 및 관리가 쉬움)	Black List방식,IP기반 정적 설정(운영 및 관리가 어려움)	SDP사용자와 SSL VPN 사용자에따라 다름
서비스보호	서버은폐(해킹위험제거)	서버노출(해킹위험 상존)	SDP사용시 VDI서버은폐 SSL-VPN사용시 서버 노출

주 : 1) SDP와 SSL VPN은 동격 비교, VDI는 개념적 비교를 한 것임
2) Agent방식과 Agentless방식이 있으나 재택근무 시 보안기준 준수를 위하여 Agent는 필수적임

PoP3[3], SMTP[4], SSH[5] 등을 지원한다

Tunnel모드에서는 네트워크 계층 상위모두를 보호하여 주기 때문에 모든 Application을 사용한다.

SSL VPN은 재택근무를 위한 구성이 용이하지만, 별도의 원격접속 프로그램이 필요한 점과 NAC의 통제 및 3rd파트제품이 탑재되어야만 비로서 금융권 보안지침에 준하는 재택근무가 가능하게 되는 구조이다. 서로 상이한 제품의 탑재로 인증의 다단계입력과 정책통제의 어려움, 장애발생가능성과 원인파악의 어려움등이 수반되어 사용자의 편리성 저하 와 비용의 증가가 예상된다.

또한, 다수의 인원이 동시에 접속할 경우 인원수 만큼 공개키 연산을 하여야함으로 응답시간이 저하된다. 외부에 VPN서버가 노출되므로, 사용자 인증 정보가 노출되면 해커의 공격을 받기 쉽다.

5.3 VDI(Virtual Desktop Infrastructure)사용

데스크톱 가상화(VDI)는 호스트 기반 데스크톱 가상화를 만들어주는 서버 컴퓨팅모델이다. 가상화 환경을 지원하는데 필요한 하드웨어와 소프트웨어를 같이 사용해야하는 개념이다. VDI서비스를 위해서는 클라인어트, 세션관리, 가상머신(VM), 스토레지 등으로 이어지는 논리계층 구조가 필요하다.

데스크톱 가상화(VDI)시스템은 가상 데스크톱을 로컬시스템이 아닌 중앙서버에서 작동하는 가상머신 계층, 가상머신 데이터를 저장하는 스토레지 계층, 각 가상머신을 클라이언트에게 연결하는 세션관리 계층 서비스를 받는 클라언트 계층으로 이루어져있다. 즉 VDI기술은 다수 가상데스크톱을 자신의 로컬시스템에서 운영하고있는 것처럼 보여주는 기술이다.

이러한 좋은 이점에도 불구하고 높은 비용과 장애발생시 전체이용자의 피해확산, 네트워크의 Bottle neck등이 문제로 대두되고 있다.

또한 재택근무시 SSL-VPN과같은 가상화 통신 프로그램 및 NAC의통제, 3r파트 제품이 제공되어야만 금융권에서의 재택근무가 가능해진다.

상기 SSL-VPN에서도 분석한바와 같이 서로 상이한 제품의 탑재로 인증의 다단계입력과 정책통제의 어려움, 장애발생 가능성과 원인파악의 어려움 등이 수반되어 사용자의 편리성 저하 와 비용의 증가가 불가피하게된다.

6. 결 론

SDP와 SSL VPN, VDI모두 재택근무 시 보안세부지침에 만족하여야하기 때문에 이에 대한 검토 후 가장 만족스러운 시스템을 사용해야한다.

전자금융감독규정 시행세칙중 정보보호 통제사항을 만족시키기 위하여는 SDP는 NAC와 결합한 하나의 플랫폼으로 통합한 제품으로 운영하면 재댁근무 보안지침에 모두 만족한다.

SSL-VPN의경우에는 별도의 원격접속 프로그램과 NAC의통제 그리고 3rd파트 제품이 탑재해야되고, VDI의경우에도 가상화 통신프로그램 및 NAC통제와 3rd파트의 제품이 제공되어야한다.

또한,SSL-VPN과 VDI에서는 서로 상이한 제품의 탑재로 인증의 다단계입력과 정책통제의 어려움, 장애발생시 원인파악이 어렵고, 장비설치 운영비용이 증가하는 문제점이 있다.

이상의 여러 가지 측면에서 종합 검토한 결과

---

3) PoP3(Post Office Protocal); 메일 클라인언트가 메일을 사용자 자신의 PC로 다운로드해주는 프로토콜

4) SMTP(Simple Mail Transfer Protocal)이메일 전송시 사용하는 프로토콜

5) SSH(Secure SHell)네트워크상에서 다른 시스템으로 파일을 복사할 수 있도록 해주는 응용프로그램 또는 프로토콜

SDP방법이 전환의 민첩성과 경영적인 측면, 또 보안부분의 만족도에서 가장 좋은 것으로 평가 되었다. 또한 재택근무 이외에도 클라우드 시스템으로 전환 할 경우에 SDP사상을 가진 시스템이 쉽게 전환할 수 있는 방법으로 판명되었다.

참 고 문 헌

[1] 박혜숙, 초연경사회의 sdp기반 신뢰 인프라 기술, ERTI 국방 ICT융합연구실, 2019.10

[2] 정부금, 이형규, 박혜숙, 박종대, 초연결 신뢰 네트워크기술, 전자통신연구소,2017

[3] Gartner, “The Internet of Things Revolution; Impact on Operational Technology Ecos Systems,” Aug. 2016

[4] CSA,(Cloud Security Alliance),SDP working Group,SDP Hackthon White paper, Aprial, 2014

[5] Garterner, “Hyper Cycle for Infrastructure Services”, 2016

[6] CISCO, Realizing the value of the IoT Where we Work, live play and learn in Defense ,2017.10

[7] CSA(Cloud Security Alliance) SDP Specification. 10, Apr. 2014

[8] CSA,SDP아키텍처 가이드

[9] 클라우드슈밥,클라우드 슈밥의 제4차 사업혁명,새로운 현재, 2016

[10] 클라우드 슈밥 외26인, 4차사업혁명의 충격, 흐름출판, 2017

[11] 금융보안원, 금융권 재택근무시 보안고려사항(전자금융감독규정 시행세칙)

[12] 피터 전, VPN가상 사설망 완전정복,네버스탑,2016

[13] CSA참고문헌

- https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/(2019.5)https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-as-a-ddos-prevention-mechanism/ (2019.10)
- https://cloudsecurityalliance.org/artifacts/sdp-the-most-advanced-zero-trust-architecture/
- https://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf

저 자 약 력

조 이 남

이메일 : choleenam@daum.net

- 1965년 2월 서울대학교 사범대학 수학교육과 졸업
- 1970년 2월 성균관대학교 경제개발대학원 (EDPS전공) 졸업 (경제학석사)
- 1987년 8월 건국대학교 산업대학원 (전산학) 졸업 (공학석사)
- 1993년 2월 홍익대학교 대학원 (전산학) 이학박사
- 1969년~1970년 한국유니백주식회사
- 1971년~2001년 금융결제원 (전무이사 역임)
- 2002년~2007년 삼성SDS, LGCNS 고문
- 2008년~2015년 넥스지,엑스게이트 (부회장)
- 1977년~2021년 한국정보과학회 (부회장 역임)
- 1984년~2021년 한국정보처리전문가협회 (회장역임)
- 1991년~2021년 한국정보처리학회 (회장역임)
- 2001년~2021년 금융정보시스템연구회 (회장역임, 현재 명예회장)
- 관심분야 : 금융지급결제제도 및 금융보안

박 완 성

이메일 : pwspwspw@naver.com

- 1988년 동국대학교 전자계산학과 졸업
- 2007년 San Jose University 연수과정 수료
- 2014년 서울대 공기업 고급경영자과정 수료
- 2018년 서울대 최고지도자인문학과정 수료
- 1988년~2019년 금융결제원 근무 (금융망개발팀장, CLS 구축반팀장, IT개발부부장, IT기획부부장)
- 2017년~2019년 금융결제원 IT본부장 (CIO,CISO)
- 2019년~2021년 금융정보시스템연구회 회장
- 관심분야 : 금융망관련 기획설계, 금융보안, 및 지급결제

한 동 우

이메일 : dwhan@mlsoft.com

- 1988년 인천대학교 전자공학과 졸업
- 2011년 연세대학교 산업정보경영학과 졸업 (석사)
- 2012년 미래경영 CEO 과정 수료
- 2017년 서울대학교 CHAMP 최고위과정 수료
- 2010년 금융보안원 경영자문위원
- 2010년 한국거래소 운영자문위원
- 1987년~1989년 축협중앙회 (은행공동망 개발 : CD, 타행환)
- 1990년~2011년 현대증권 (시스템운영부, IT연구팀, 차세대시스템 부서장 역임)
- 2012년~2017년 KB증권 IT본부장 (CIO/CISO)
- 2018년~2019년 유진저축은행 기술고문
- 2020년~현재 MLSoft 대표컨설턴트
- 관심분야 : 금융업무 기간계, 정보계, 차세대 시스템, e-BIZ, 금융보안시스템

최 우 봉

이메일 : wbchoi@mlsoft.com

- 1986년 동국대학교 전자계산학과 졸업
- 1990년 동국대학교 정보산업대학원 석사과정 수료
- 2002년 상지대학교 회계정보학과 졸업 (석사)
- 2006년 상지대학교 대학원 경영학과 박사과정 수료
- 1985년~2013년 보험개발원 근무 (시스템개발부장, 퇴직연금센터장, 정보서비스본부장)
- 2015년~2018년 (동부)FIS 시스템 대표이사
- 2018년~2019년 아이티아이즈(주)고문
- 2020년~2021년 현재 MLSOFT(주) 대표컨설탄트
- 2015년~2020년 건국대학교 정보통신대학원 겸임교수
- 2003년~2009년 ISO/TC68/SC2/SC7평가위원
- 관심분야 : 보험관련 요율체계, 보험사기예방, 네트워크보안, 지급결제분야

이 무 성

이메일 : musso@mlsoft.com

- 1983년 한국최초 한글워드프로세서 명필개발 (KIST공동)
- 1995년~현재 MLSoft(주) (전 미디어랜드) 설립, 대표이사
- 2014년 대한항공 NAC개발, 금융감독원 IMP구축
- 2015년 농협중앙회, 신한은행, 수협, 기업은행 등 NAC 구축
- 2018년 신한서대학 경제학박사
- 2019년~2021년 TGATE (SDP) 개발보급
- 관심분야 : 제로트러스트, SDP