



DAON

Update 202601

Contents


- Introduction to Daon | 기업정보
- About us | 다운기술 소개
- History | 연혁
- Corporate Identity | CI
- Mission | 미션
- Core competence | 핵심역량
- Performance | 숫자로 보는 다운
- Our Business Partners | 주요 파트너사
- Solutions | 솔루션소개



차별화된 가치를 만드는 사람들



설립일	2013.02
대표	조주한
주요사업	보안솔루션 공급 및 구축, 운영 유지
직원수	33명
경영실적	177억원 (25년 기준)
신용 평가 등급	BBB0 나이스 평가정보 (25년 기준)
본사위치	경기도 성남시 분당구 대왕판교로 600 유스페이스 1 B동 706호
대표전화	(031) 696-4870
홈페이지	daont.co.kr



고객의 성공이 곧 우리의 성공이라는 믿음

다운기술은 창의적인 사고방식과 열정을 바탕으로 2013년에 설립된 스타트업입니다. 우리는 정보보호 솔루션 구축 및 컨설팅을 주 업으로 하고 있으며, 이를 통해 고객의 불안과 걱정을 덜어주는 신뢰를 판매하는 기업입니다.

우리는 고객에게 확연히 차별화된 솔루션을 제시하며 경쟁자들과는 다른 가치를 제공하고 고객 비즈니스의 실질적인 성공을 위하여 가장 가까운 곳에서 문제를 분석하고 해결책을 제시하는 신뢰할 수 있는 보안 파트너입니다.

History

- 다운기술(주) 창업
- 기술보증기금 벤처기업 인증
- 시큐아이 프리미엄 채널 계약 체결
- 차세대 위협방지 솔루션 FireEye 파트너 계약 체결

- 다운기술 본사 사업장 확장, 이전
- FireEye 최우수 Gold Partner 선정
- FireEye 중소형(커머셜) 고객 대상 침해대응 어시스턴트 프로그램 파트너사 선정
- FireEye NX Essential 오픈 POC 선정
- FireEye 보안 관제 고도화 전략 세미나 공공기관 대상 로드쇼

- 다운기술 본사 사업장 확장, 이전
- 기업부설연구소 설립
- FireEye Best Performer 선정

- 자본금 80,000,000 유상증자
- 정보통신공사업 면허취득
- FireEye 홈커밍데이 Top of Reseller 선정



2013~2014



2015~2016



2017~2018



2019~2020

- Google Cloud Security Champion of the Year 수상
- Google Cloud Growth of the Year 수상
- Riskmap 솔루션 공식 런칭

- 다운기술 본사 사업장 확장, 이전
- Trellix Special Sales Award 수상
- Trellix The Best Partner Sales person 수상
- Trellix Special Award DLP TFT 수상
- GLIMPS 국내 최초 파트너 계약 체결

- GCS(전 Mandiant) 1Tier 파트너 선정
- Trellix Year's Channel's Recognized Active Partner 수상

- Okta 2022 Premier Partner 선정
- Okta 2022 Best Partner of the year 수상
- Okta 2022 Korea Partner of the Quarter 수상
- Mandiant 2022 Partner of the year 수상

- FireEye Platinum Partner 선정
- FireEye APAC TOP Reseller 선정
- FireEye & Mandiant Catch the Prize 2021 5개 부문수상



2025



2024



2023



2022



2021

Corporate Identity



DAON

차별화된 가치로 고객의 문제를 해결하고 고객의 성공을 돕는다.

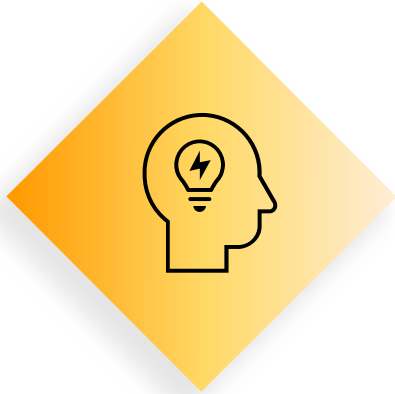
다운기술의 모든 구성원은 '차별화'를 기반으로 모든 일을 수행합니다.

우리의 미션은 앞으로도 영원히 불변하지 않는 다운기술의 고유 문화로 남을 것입니다.

Slogan

Different Value Maker!

Mission



차별화

Different strategy

'누구나 할 수 있는 일을
누구도 우리만큼 할 수 없는 수준' 으로 일 합니
다.



성장

Development

우리는 현재의 레벨보다 높은 레벨에서 일한다는
마음가짐으로 끊임없이 배움을 추구하며 성장해
나갑니다.



신뢰

Trust

고객을 돕고 고객을 성공시키는 것이 우리의 성공
이라는 믿음으로 고객의 성공을 돕는 일을 가장
우선하며 고객의 이익을 위해 정성과 노력을 제
공합니다.

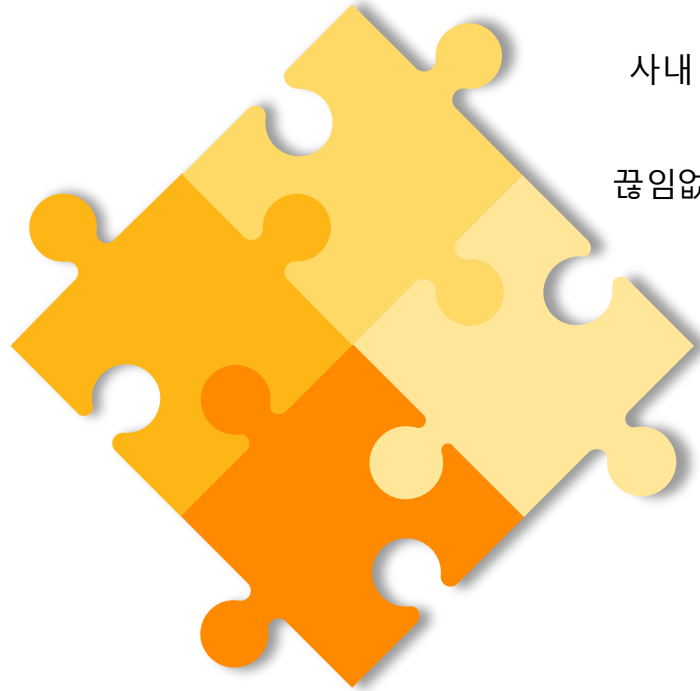
Core competence

차별화된 가치 전달

고객의 안전한 정보보호 수준을 유지하기 위해 새로운 트렌드를 빠르게 파악하여 단순히 제품, 솔루션 공급이 아닌 고객의 도입목적에 맞는 차별화된 서비스를 제공합니다.

끊임없이 탐구하는 전문가로 구성

구성원의 대부분이 고객, 솔루션, 서비스에 대하여 정보보호분야 경력을 보유한 전문가들입니다.



내부 커뮤니케이션 활용

사내 커뮤니티를 통해 업무 및 기술을 활발히 공유하고 끊임없는 탐구와 도전정신, 능동적 사고와 책임감으로 임무를 수행합니다.

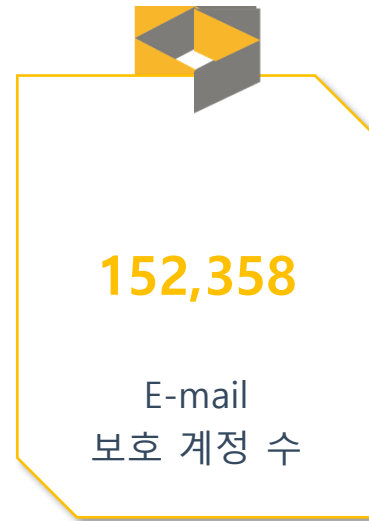
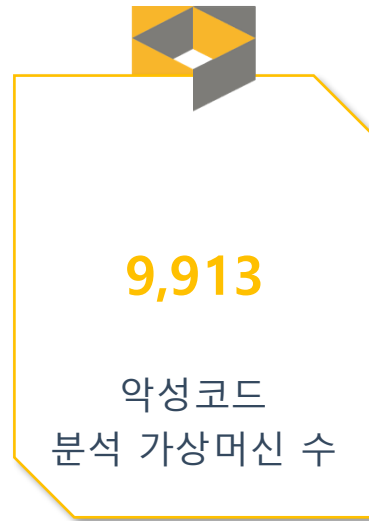
문제해결 능력 보유

수 많은 프로젝트를 성공적으로 수행해내며 쌓은 기술적 노하우와 다양한 고객 경험을 바탕으로 다각도로 문제를 탐구하며 해결합니다.

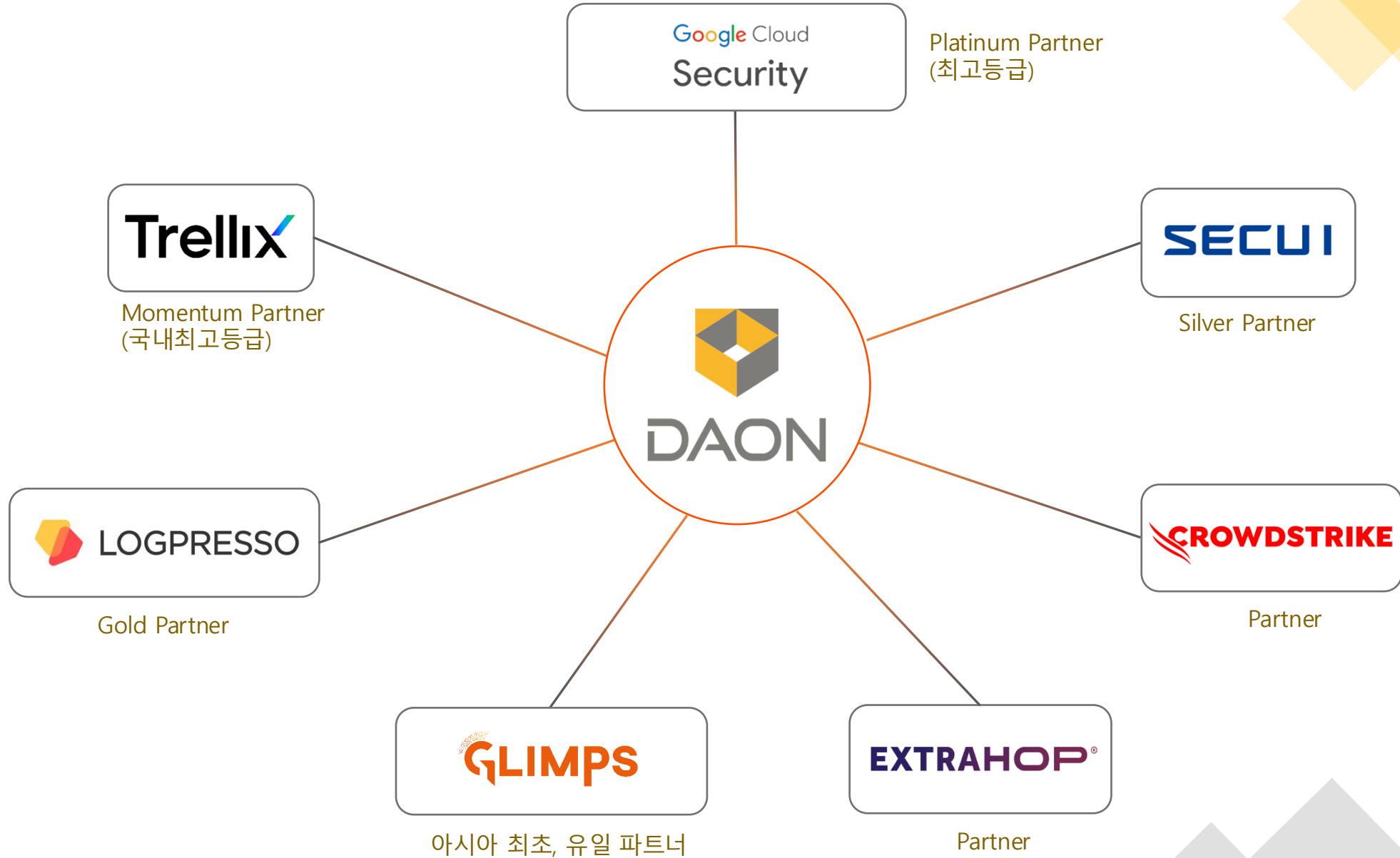
Performance

26년 1월 기준

다운기술은 공공, 금융, 엔터프라이즈등 다양한 분야의 고객들에게
정보보호 솔루션 구축 및 컨설팅을 제공하고 있습니다.



Our Business Partners



Google Cloud Security

**AI로 보다 강력해진 Mandiant. 인텔리전스 기반 보안 운영,
클라우드 보안을 통해 Google을 보안팀의 전문가로 동원할 수 있습니다.**

Security Validation

시뮬레이션이 아닌 실제 파괴적 공격(멀웨어 및 랜섬웨어)을 안전하게 실행하고 공격중에 보안 제어가 어떻게 작동하는지에 대한 가시성과 효과에 대한 정량적 데이터를 제공합니다.

Threat Intelligence

보안 실무자에게 현재 비즈니스에 중요한 위협에 대한 탁월한 가시성과 전문성을 제공합니다. 사이버 범죄 행위자, 조직을 표적으로 하는 동기 및 행동을 이해하여 방어를 할 수 있습니다

Attack Surface Management

오늘날의 동적이고 분산된 공유 환경 전반에 걸쳐 인터넷 자산을 탐색하고 분석합니다. 또한 발견된 자산의 노출 상태를 지속적으로 모니터링하며, 인텔리전스 및 레드팀이 운영 상태를 유지하고 리스크 관리에 필요한 정보를 제공할 수 있도록 지원합니다.

Mandiant 컨설팅

조직의 보안 환경을 더욱 강화할 수 있는 방법 중 하나는 경험 많은 전문가들의 지원을 받는 것입니다. Mandiant가 대응하고 있는 보안 침해 사고는 세계 최대 규모입니다. 더불어 Google과 함께 전문가들의 다양한 경험과 세계적인 공격 패턴을 고려하여 문제에 대처할 수 있습니다.





사이버 범죄자가 점점 더 지능화될수록 보안 시스템도 더 스마트해진다면 어떨까요?

MX(Multi-Vector Virtual Execution) Engine

FireEye 만의 자체 가상머신 기술(다중벡터 가상 실행, MVX)을 기반으로 실시간 위협 탐지 및 방어 능력 강화. 전세계 APT 솔루션 시장 점유율 1위의 위상에 빛나는 핵심 기술

DTI(Dynamic Threat Intelligence) Engine

전 세계의 FireEye 구성요소는 DTI Engine을 통해 실시간으로 위협 정보를 공유
'Mandiant'의 Intelligence가 더해져 기존 AV 제품과는 차별적인 탐지 및 방어 능력을 발휘

다양한 포맷에 대한 악성코드 검사

다양한 어플리케이션, 프로토콜 및 파일 형식이 가진 취약점에 대한 공격자 행위를 폭넓게 탐지할 수 있어, 기존 보안 솔루션 한계 보완

사용 목적에 따른 Platform 구성과 연동

다양한 Platform 보유 : 네트워크, 이메일, 파일공유서버, 엔드포인트 등 CM(Central Management)과의 연동을 통한 장비 관리의 편의성 확보





빠르고 확장 가능한 Falcon 플랫폼으로 기업의 디지털 혁신을 안전하게 지원합니다. “We Stop Breach”

Falcon Insight & Prevent

Falcon Insight와 Prevent는 CrowdStrike Falcon 플랫폼의 핵심 구성 요소로서, 긴밀하게 연동되어 엔드포인트 보안의 전 영역에서 강력한 보호 기능을 제공하며, Insight의 탐지 및 분석 능력과 Prevent의 사전 예방 기능을 결합하여 시너지 효과를 창출합니다.

Falcon Cloud Security

Falcon Cloud Security는 클라우드 환경 전반의 워크로드, 컨테이너, 서버리스 환경에 대한 가시성을 확보하고 위협을 탐지 및 대응하며, 클라우드 설정 오류 및 규정 준수 문제를 지속적으로 모니터링하여 보안 태세를 강화합니다.

Falcon Identity Protection

복잡한 하이브리드 ID 환경에서 즉각적인 가시성을 제공하고 ID, 행동 및 위험 분석을 사용하여 실시간 위협 방지 및 IT 정책 시행을 통해 원활한 보안을 지원합니다.

Falcon Threat Intelligence & Hunting

CrowdStrike의 광범위한 센서 네트워크와 전문 분석가 팀이 수집, 분석한 최신 사이버 위협 정보를 제공하여, 공격자의 전술, 기술, 절차(TTPs) 및 악성코드 분석, 캠페인 정보를 통해 선제적인 보안 전략 수립을 지원합니다.





앱으로 확장되는 보안 오케스트레이션 플랫폼이 자동 대응 시대를 열어갑니다.

All-In-One 빅데이터 분석 플랫폼

다양한 데이터의 수집부터 실시간 분석, 적재 및 시각화까지 모든 것을 하나로 해결 가능
기존 통합 로그관리 시스템과는 차별화된 능력 보유

데이터 암호화 및 대용량 압축 보관

디스크에 평문 데이터를 실시간으로 암호화하여 강력한 보안성 확보
대용량 데이터를 압축하여 저장 및 보관하므로, 보다 쾌적한 시스템 상태 유지 가능

사용자 맞춤 기능 구현과 데이터 가시성 확보

LogPresso 전용 쿼리를 사용하여 사용자가 원하는 데이터를 곧바로
대시보드 형태로 만들어 시각화하고, 다양한 위젯 구성이 가능

탁월한 저장 및 검색 성능

원본 1TB 기준 0.2초 이내의 검색 성능
원본 기준 1/3 이하 디스크 용량 사용 (인덱스 포함)



EXTRAHOP[®]

네트워크 트래픽을 실시간으로 분석해 위협과 이상을 동시에 잡는 통합 NDR 플랫폼

실시간 네트워크 위협 탐지 및 대응

머신 러닝과 규칙 기반 분석을 통해 네트워크 트래픽을 실시간으로 분석하고, 성능 저하와 보안 위협을 즉시 식별하여 신속한 대응을 지원합니다. 기존 보안 도구에서 놓치기 쉬운 이상 행위까지 정확하게 탐지합니다.

고급 머신 러닝 기반 위협 분석

5,000개 이상의 고급 머신 러닝 및 분석 기법을 활용해 비정상적인 트래픽 패턴과 잠재적 위협을 자동으로 식별합니다. 클라우드 기반 머신 러닝을 통해 성능 영향 없이 탐지·분석·조사 과정을 자동화합니다.

네트워크 전반에 대한 완벽한 가시성

엔드포인트, SIEM, 기존 NDR 솔루션으로는 확인하기 어려운 전체 공격 표면에 대한 광범위한 가시성을 제공합니다. 모든 연결, 사용자, 애플리케이션의 행위를 네트워크 관점에서 입체적으로 파악할 수 있습니다.

패킷 수준 심층 분석 및 실시간 복호화

패킷 단위의 네트워크 트래픽을 분석해 문제 원인을 정밀하게 식별합니다. 실시간 트래픽 복호화를 통해 기존 보안 솔루션으로는 확인할 수 없었던 숨겨진 위협과 이상 징후까지 가시화합니다.

AI 기반 조사 자동화 및 지능형 대응

AI로 설계된 직관적인 워크플로우를 통해 탐지부터 근본 원인 분석까지 단 3번의 클릭으로 조사가 가능합니다. 자동화된 대응과 간편한 통합을 통해 분석가 개입 없이도 위협을 빠르고 확실하게 차단합니다.





파일 스트림 전체를 대상으로 하는 AI기반 악성코드 탐지 및 특성 분석 솔루션

Power up your security

자동화된 심층 파일 및 코드 개념 분석(Code Concept Analysis)을 통해 알려진 위협과 알려지지 않은 위협을 모두 파악

Improve your operational efficiency

자동화된 IoC 추출 및 초단위의 빠른 페이로드 분석으로 응답 시간을 단축합니다.

Protect your file flow now

간편한 인프라 및 API 통합을 통해 가치 창출 시간(Time-to-value)을 최소화할 수 있습니다.



SECUI

국내 최초의 네트워크 보안을 위한 차세대 방화벽

App 제어

국내 외 애플리케이션에 의한 취약점 증가, 악성코드 배포 등을 방지하기 위해 어플리케이션을 사전 정의하고 분석하여 기존 UTM에서 대응이 어려운 공격에 능동적으로 대처할 수 있는 기능

파일 유형 제어

어플리케이션 사용 시 파일의 유형(문서, 압축 파일, 이미지, 멀티미디어 등)별, 방향별로 제어하여 비인가 파일전송과 내부 정보유출 방지 및 외부로부터 위협 예방

사용자 ID

IP가 아닌 사용자ID 를 인식하여 언제 어디서 네트워크에 접속하여도 동일한 보안정책을 적용받아 사용자의 이동성을 보장하고 사용자 별 통계 자료 조회 가능

Device 제어

사용자 단말의 보안설정, 필수 SW 설치 여부, 보안 업데이트 현황, 백업/암호화 설정 여부를 검사하여 내부망, 중요 업무 시스템에 대한 접근을 제어함으로써 Malware 감염을 원천 차단



Thank you



CONTACT

이메일
sales@daont.co.kr



대표전화
(031) 696-4870



홈페이지
daont.co.kr