

Team 12

Capstone Design report

사이버 보안 메시

Cybersecurity Mesh

1726067 민 경 호
1726077 이 민 식
1726081 이 준 용
1726088 최 민 수

Index

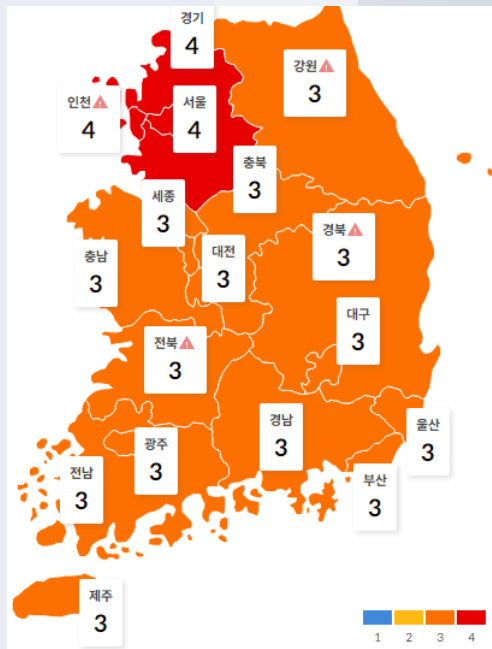
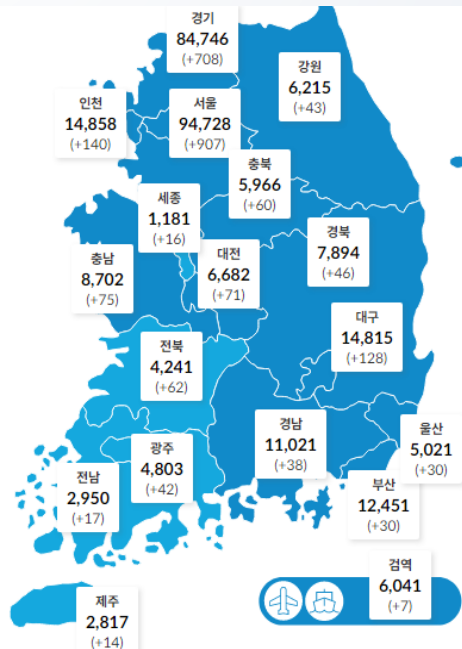
1. 나오게 된 배경
2. 정의
3. 목표, 역할
4. 세부기술 1. 제로 트러스트
5. 세부기술 2. VPN
6. 예시
7. 출처

코로나가 가져온 뉴 노멀 (21.09.24 기준) New normal

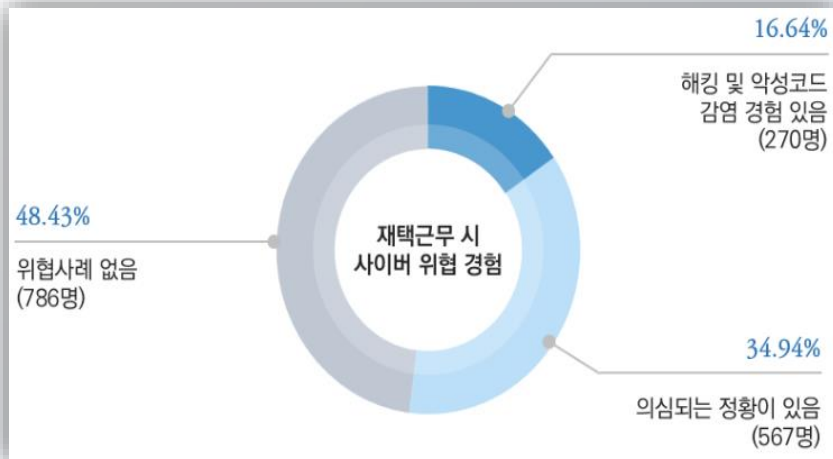
문 대통령 "다음 달쯤 '위드 코로나' 계획 알릴 것"

2021년 09월 24일 06시 07분 [댓글](#)

국내 누적 확진자 수 295,132 명
국내 확진자 수 2,416 명
해외 확진자 수 231,517,476 명



비대면 환경의 확대



- 전 세계 10억 명 이상이 재택근무 경험
- 재택근무 시 사이버 위협 경험율의 증가



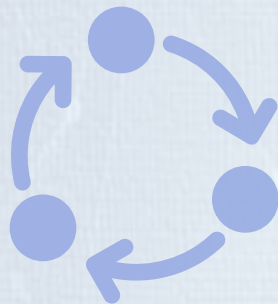
- 초, 중, 고, 대학교의 온라인 원격수업
- 현 상황을 악용한 사이버 공격 대거 발생

사이버 보안 메시란



독립된 환경과 분산화된
컴퓨팅 환경에서도
디지털 자산에 안전하게 접근

개인이나 사물의
정체성에 대한
보안 경계를 재정의



언제 어디서든 정보에
액세스하는 과정에
안전과 안보를 보장하는 기술

What is
{Cybersecurity Mesh} ?

사이버 보안 메시의 목표

기밀성 (Confidentiality)

- 비밀 유지
- 비공개상태
- 대표위협

가로채기(interception)
스누핑(snooping)
도청

무결성 (Integrity)

- 진실성
- 일관되고 온전한 상태
- 대표위협
변조(Modification)
위조, 재연, 부인

가용성 (Availability)

- 사용되거나 얻을 수 있는 특성
- 대표위협
DOS(서비스거부)
차단(Interruption)

사이버 보안 메시의 역할

보안이 미비한다면?

소프트웨어 취약점

가로채기 ↑ (기밀성 ↓)

네트워크 취약점

변조 ↑ (무결성 ↓)

인적 관리 취약점

중단 / 손상 ↑ (가용성 ↓)

하드웨어 / 사이트 취약점

위조 ↑ (무결성 ↓)

사이버 보안 메시의 역할

취약점으로 인한 사고들

페이스북서 전 세계 5억명 개인정보
무더기로 유출... 韓도 12만명
포함(종합)

황민규 기자 정우정 기자

입력 2021.04.04 07:56 | 수정 2021.04.04 17:40



전화번호·주소·생일·이력 등 포함된 듯
페이스북 "2019년 발견돼 이미 해결된 것"
"몇 년 되도 사이버범죄에는 악용 여지"

가로채기 ↑ (기밀성 ↓)

• 2019.05

- 중국 바이낸스 480억 상당 암호화폐 도난
- 싱가포르 bitrue 50억 상당 암호화폐 도난



중단/손상 ↑ (기용성 ↓)

[세이프 스마트폰] 수백만 원 나몰라 겠제... 구글 플레

오시영 기자 김평화 기자

입력 2020.05.13 09:19 | 수정 2020.05.13 12:22

#27세 여성 직장인 김씨는 10일 오후 9시 외문의 문자메시지를 다수 받았다. 통신사가 발송한 SMS를 보면, 한번호 해본 적 없는 게임에서 소액결제를 했다는 내용이 담겼다. 엔씨소프트의 다중접속역할수행게임(MMORPG) 라니지 ZM에서 '다이아'라는 재화를 사는데 수십만원쯤을 지불했다는 것이다. 김씨는 자신의 눈을 의심하며 거듭 확인했지만, 정말 이동사가 보낸 SMS가 맞았다.

최근 구글 플레이스토어 게임 해킹으로 금전적 피해를 봤다는 사례가 다수 접수됐다. [스팀 등 게임 플랫폼을 해킹당했다는 사례](#)는 이전에도 많았다. 구글 플레이 계정을 해킹당할 경우 해커가 게임에 등록한 결제 수단을 이용해 실시간으로 금전 피해를 입힌다는 점에서 정신적·물질적 피해가 막심하다.

이런 해킹은 어째서 일까. 당황을 막 어떻게 대처해야 할까. 어떻게 예방할 수 있을까.

변조 ↑ (무결성 ↓)

이메일 위조: 세계적으로 30조원이 넘는
피해를 안긴 해킹 수법

본지 기자
이재민 기자
2019년 10월 27일



예니, 이메일위조. 회사의 CEO가 보낸 메일이 제부, 담당에게 왔다.

"귀사가 실시했던 ROI 관련 데이터를 이 계좌로 최대한 빨리 보내주세요. 오늘 오후로 끝내야 해. 그렇지 않아요."

직원은 발뺌이 없이 이를 계좌로 보냈다. 그날의 말 및 메세지에서 이를 지우고 확인하려 했다.

그러나 문제가 생겼다. 발송되는 기업에서 해 이자 편이 단 몰아당났고 그로 인하여, 큰 것이다.

위조 ↑ (무결성 ↓)

사이버 보안 메시의 역할

보안이 강하다면?

소프트웨어 취약점 보완

가로채기 ↓ (기밀성 ↑)

네트워크 취약점 보완

변조 ↓ (무결성 ↑)

인적 관리 취약점 보완

중단 / 손상 ↓ (가용성 ↑)

하드웨어 / 사이트 취약점 보완

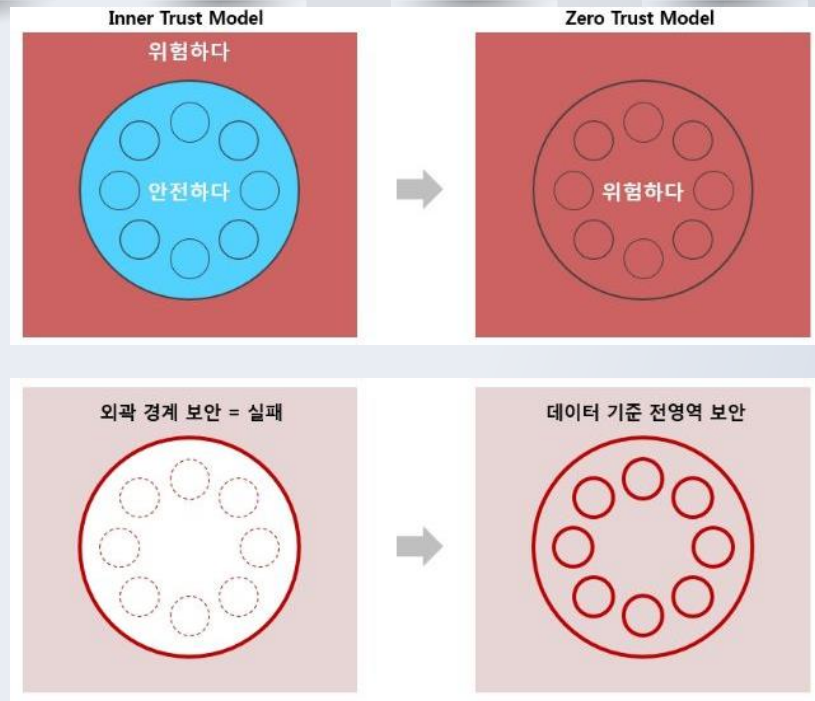
위조 ↓ (무결성 ↑)

아무도 믿지 말라!

제로 트러스트 (Zero Trust)

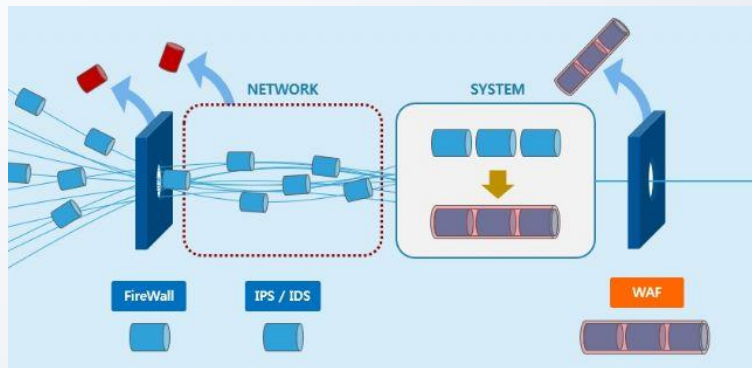
경계 없는 보안을 의미하는 제로 트러스트 모델은
내부-외부, 모든 상황에서의 정보보안을 목표로 하는 모델.

시스템 전체를 지켜야 할 하나의 큰 덩어리로 보지 않고
'미세-분할(micro-segmentation)' 요소로 나누고,
각 요소에 대해
'과립형 경계 시행(granular perimeter enforcement)' 방식



아무도 믿지 말라!

제로 트러스트 (Zero Trust)



지능형 WAF:패킷 아닌 데이터 단위 분석 웹 보안

보안사고가 가장 많이 발생하는 위험한 지점, **웹**을 최우선 방어.

'유의미'를 기준으로 단위 분석을 하기에

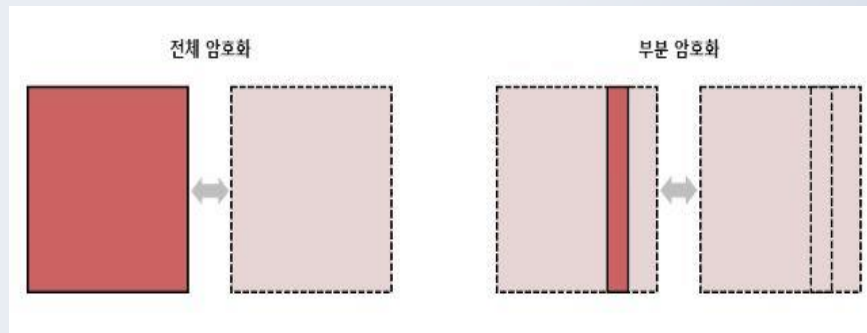
패킷이 모여면서 생기는 데이터를 통한 악의적 침입 또한 막는다.

컬럼 단위 암호화:암호화 공개 범위의 최소화

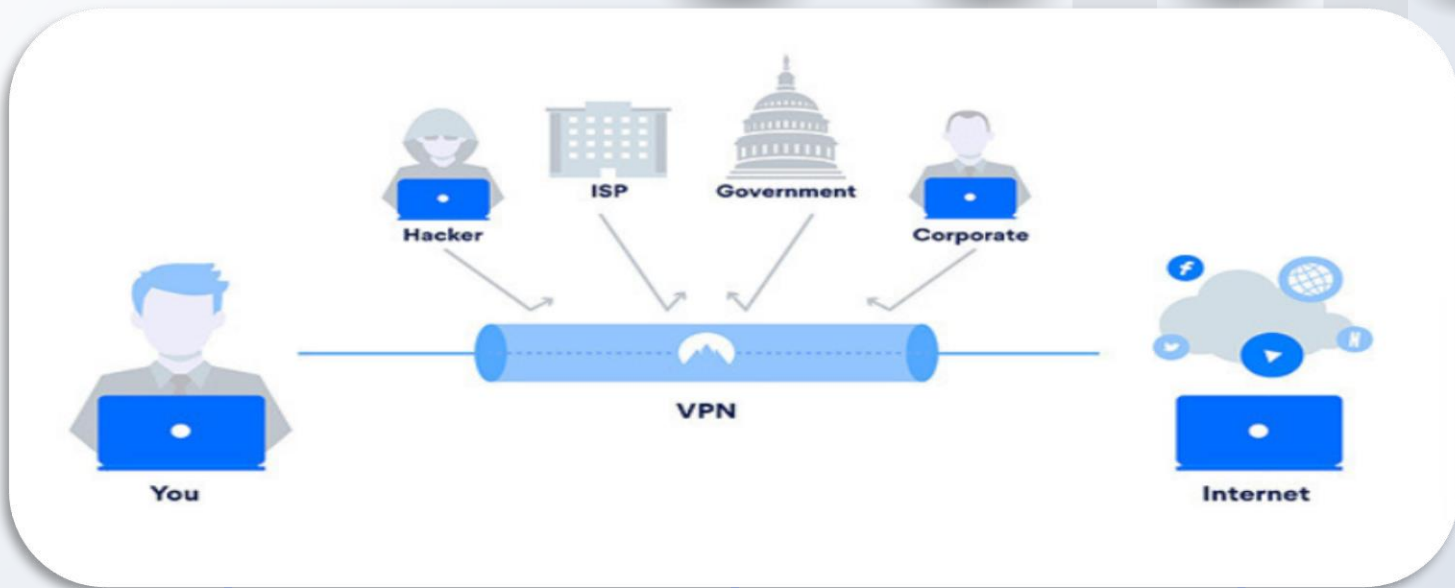
암호화의 **최소** 범위를 **최소** 인원에게 **최단** 시간 동안 노출.

일정한 컬럼형태로 암호화를 하여 필요한 경우,

제한된 사용자에게 제한된 시간에 한정 공개한다.



VPN



보안 강화

위치 변경

개인 정보 보호

VPN 접근 시 인증 시스템 연동 및 추가



사내 VPN 접근 방법

- 패스워드+OPT
- 패스워드+생체인식
- 패스워드+기타인증



VPN

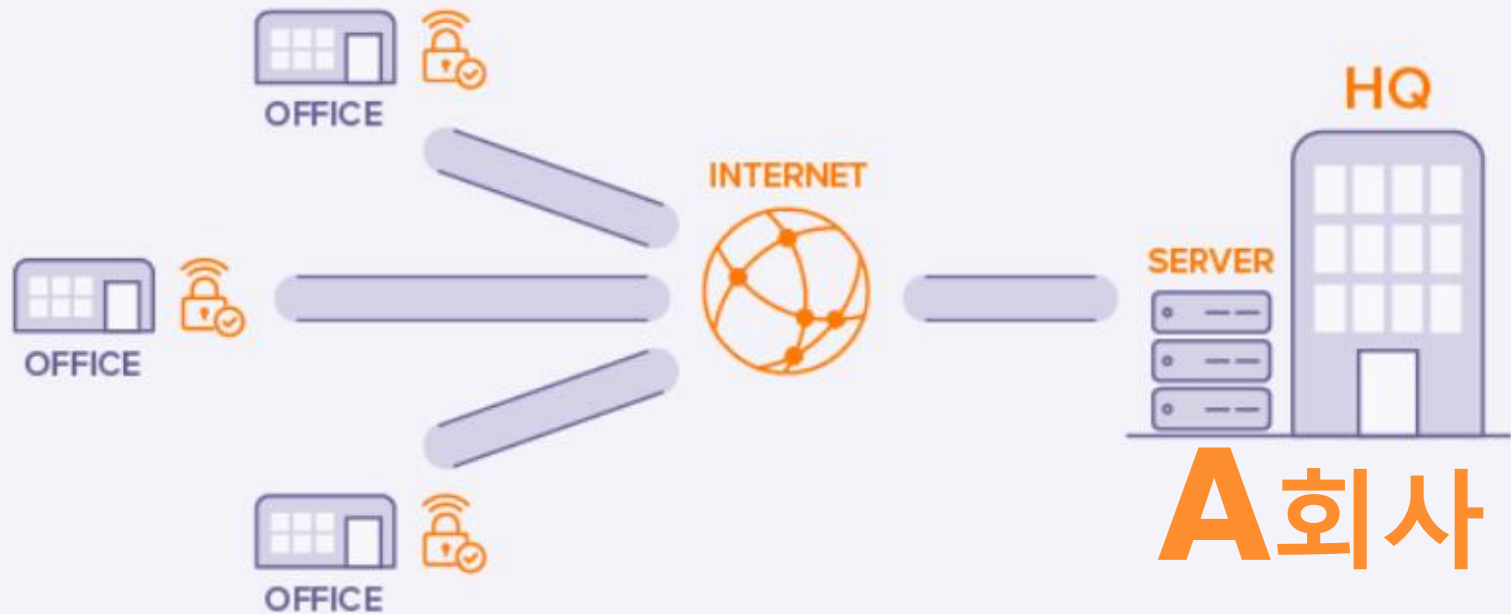


VPN 인증시스템 (OTP, 생체, 단말기 등) 연동



[그림 4] VPN 사용 시 인증 시스템 연동 및 추가

예시



예시



Register employees through any tablet or PC



Employees undergo automated thermal scan at all entrance and exit points



Employee ID, in/out time, and temperature are updated on web-based dashboard



Management can view employee's last check-in / out and temperature data history in real-time



If an abnormally high temperature is detected, an alert is shown on site and on the dashboard

기대효과(가트너)

5 Strategic Benefits of Cybersecurity Mesh

Will support
more than 50
percent of IAM
requests

Delivery of IAM
services =
rise in managed
security service
providers

Identity proofing
tools will be
added to the
workforce identity
life cycle

Decentralized
identity
standards will
emerge

Demographic
bias within
identity proofing
will be minimized

기대효과(국방망)

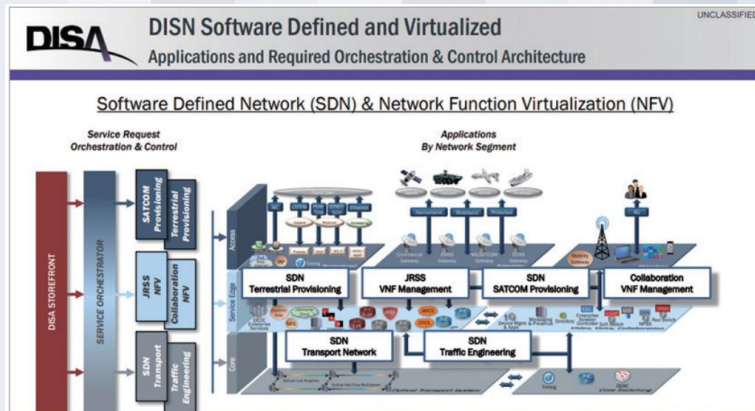
현재의 국방망은

- 대부분의 기존 폐쇄형에서 사용하는 **경계형** 기반의 보안 모델을 사용
- 사용자별로 접근할 수 있는 서비스가 구분X

- 물리적인 망 분리에 의존
- 구역의 개념 ↓

ZeroTrust 도입

1. 내부망의 접근을 **허용하더라도**
데이터에 대한 접근을 근본적으로 차단
2. 각 데이터별로 권한이 **세분화**되어 핵심 등급의
중요 데이터는 **추가인증**을 통해 **보안 강화**



출처

- 코로나공식홈페이지: <http://ncov.mohw.go.kr/>
- 사이버 보안 메시 환경:
[http://www.igloosec.co.kr/ig/BLOG_%ED%8C%AC%EB%8D%B0%EB%AF%B9%20%ED%98%84%EC%83%81%EC%9C%BC%EB%A1%9C%20%EC%9D%B8%ED%95%9C%20%EC%82%AC%EC%9D%B4%EB%B2%84%EB%B3%B4%EC%95%88%20%EB%A9%94%EC%8B%9C\(Cyber security%20Mesh\)%EC%9D%98%20%ED%95%84%EC%9A%94%EC%84%B1?searchItem=&searchWord=&bbsCatId=1&gotoPage=1](http://www.igloosec.co.kr/ig/BLOG_%ED%8C%AC%EB%8D%B0%EB%AF%B9%20%ED%98%84%EC%83%81%EC%9C%BC%EB%A1%9C%20%EC%9D%B8%ED%95%9C%20%EC%82%AC%EC%9D%B4%EB%B2%84%EB%B3%B4%EC%95%88%20%EB%A9%94%EC%8B%9C(Cyber security%20Mesh)%EC%9D%98%20%ED%95%84%EC%9A%94%EC%84%B1?searchItem=&searchWord=&bbsCatId=1&gotoPage=1)
- 사이버 보안 메시 환경: <https://www.jjan.kr/news/articleView.html?idxno=2102903>
- 페이스북 사례: biz 조선, https://biz.chosun.com/site/data/html_dir/2021/04/04/2021040400092.html
- 구글 사례: it 조선, http://it.chosun.com/site/data/html_dir/2020/05/13/2020051300982.html
- 암호 화폐 사례: 중앙, <https://www.joongang.co.kr/article/22376175#home>
- 이메일 위조: <https://www.bbc.com/korean/features-49902194>
- 제로 트러스트 정의:
<https://zdnet.co.kr/view/?no=20190610114522>
One Step Ahead 이글루시큐리티 (igloosec.co.kr)
전보국, 최경택, 박규순 (2021). 보안은 불신으로부터, 제로트러스트 모델의 군 적용 필요성 제고. 국방과 기술, (511), 116-129.
- VPN:
<https://got-it0918.tistory.com/88>
[http://www.igloosec.co.kr/ig/BLOG_%ED%8C%AC%EB%8D%B0%EB%AF%B9%20%ED%98%84%EC%83%81%EC%9C%BC%EB%A1%9C%20%EC%9D%B8%ED%95%9C%20%EC%82%AC%EC%9D%B4%EB%B2%84%EB%B3%B4%EC%95%88%20%EB%A9%94%EC%8B%9C\(Cyber security%20Mesh\)%EC%9D%98%20%ED%95%84%EC%9A%94%EC%84%B1?searchItem=&searchWord=&bbsCatId=1&gotoPage=1](http://www.igloosec.co.kr/ig/BLOG_%ED%8C%AC%EB%8D%B0%EB%AF%B9%20%ED%98%84%EC%83%81%EC%9C%BC%EB%A1%9C%20%EC%9D%B8%ED%95%9C%20%EC%82%AC%EC%9D%B4%EB%B2%84%EB%B3%B4%EC%95%88%20%EB%A9%94%EC%8B%9C(Cyber security%20Mesh)%EC%9D%98%20%ED%95%84%EC%9A%94%EC%84%B1?searchItem=&searchWord=&bbsCatId=1&gotoPage=1)
<https://www.avast.com/c-what-is-a-vpn>
- 예시: 삼성 SDS, Untact (비대면) 시대를 위한 비즈니스 솔루션, <http://www.korchamsg.org/?p=10454>
- 기대효과: 출처: <https://stefanini.com/en/trends/news/what-is-cybersecurity-mesh-5-advantages-of-this-top-tech-trend#understandingcybersecuritymesh>