

조선기자재학과 석사과정 학생으로 현재 석사 논문을 준비하려 한다. 관심있는 주제키워드는 자율항해, 안테나, AIS, AIS 데이터 활용, 네트워크이다. 논문주제를 뽑기 위한 브레인스토밍을 하고 싶습니다. 현재 (2024년) 시점 기준으로 최신 연구 근황을 반영하여 논문주제를 도출하고 싶습니다.



메모리 업데이트됨

흥미로운 주제들이 많아 다양한 연구 주제로 발전시킬 수 있겠네요. 최신 연구 동향을 바탕으로 논문 주제를 브레인스토밍해 보겠습니다.

1. 자율항해와 AIS 데이터의 융합 연구

- 주제: "AIS 데이터를 활용한 자율항해 시스템의 충돌 방지 알고리즘 개발"
- 설명: 자율항해에서 AIS 데이터를 활용해 인근 선박의 위치를 예측하고, 충돌 방지 경로를 자동으로 설정하는 알고리즘을 개발해 봄으로 자율 항해의 안전성을 강화할 수 있습니다. 특히 머신러닝을 활용해 예측 정확도를 높이는 방향도 고려해 볼 수 있습니다.

2. AIS 데이터와 네트워크 기술을 활용한 해상 교통 관리 시스템

- 주제: "AIS 데이터 기반의 해상 네트워크 트래픽 분석을 통한 최적화된 교통 관리 시스템 개발"
- 설명: AIS 데이터를 활용해 해상 교통 상황을 분석하고, 교통량이 많은 해역의 데이터 트래픽 패턴을 분석해 네트워크 효율성을 높이는 연구입니다. 이를 통해 특정 해역의 혼잡도를 예측하고, 효율적인 경로 설정에 활용될 수 있습니다.

3. 안테나 최적화를 통한 AIS 데이터 수신 향상 연구

- 주제: "AIS 데이터 수신 효율을 위한 다중 안테나 배열 최적화 연구"
- 설명: 해상에서 AIS 신호 수신은 기상 조건 등 여러 변수의 영향을 받습니다. 다중 안테나 배열을 최적화하여 수신 신호의 안정성과 품질을 높이는 연구는 실제 해상에서의 데이터 수집에 유용할 수 있습니다. 다양한 전파 조건에서의 데이터 수신을 개선할 수 있는 알고리즘을 제안하는 방향입니다.

4. AIS 데이터 분석을 통한 자율항해 시스템의 경로 최적화

- 주제: "AIS 데이터를 활용한 자율 항해 경로 최적화 및 에너지 효율 개선 연구"
- 설명: 항해 경로 최적화는 자율 항해에서 중요한 문제입니다. AIS 데이터를 분석하여 최적의 경로를 설정하고, 이에 따른 에너지 소비를 줄일 수 있는 방법을 연구하는 것입니다. 이는 연료 절감 및 환경 오염 감소에 기여할 수 있는 실용적인 연구가 될 수 있습니다.

5. 해양 네트워크 상에서 AIS 데이터를 통한 실시간 모니터링 시스템 개발

- 주제: "해양 네트워크를 활용한 실시간 AIS 데이터 기반 해양 상황 모니터링 시스템 개발"
- 설명: 네트워크를 통해 실시간으로 수집된 AIS 데이터를 시각화하고 이상 패턴을 탐지하는 모니터링 시스템을 개발하여 해상 사고 및 불법 조업 감시 등의 기능을 강화할 수 있습니다.

이 중에서 흥미가 가는 주제를 더 구체적으로 발전시키거나, 추가적인 키워드를 접목해 특정 연구 방향을 정하면 좋을 것 같습니다.

좋은 주제를 주어서 고맙습니다. 다만 나는 고등학교 때 문과를 전공했고, 대학교는 외국어를 전공을 하였기 때문에 공학적인 지식은 다른 공대분들보다 많이 부족하다. 해서, 문과도 조금 더 접근할만한 논문 주제로 브레인스토밍가능할까요?



메모리 업데이트됨

문과 배경을 바탕으로 접근할 수 있는 주제라면, 기술적인 내용을 다루되 데이터 분석이나 정책, 사회적 영향과 같은 부분에 초점을 맞추는 것이 좋겠습니다. 다음과 같은 논문 주제를 제안드려 보겠습니다.

1. AIS 데이터의 활용 가능성과 사회적 영향 분석

- 주제: "AIS 데이터의 활용 가능성과 해상 안전에 미치는 사회적 영향 분석"
- 설명: AIS 데이터를 통해 해상 교통 상황을 모니터링하는 것이 사고 예방, 불법 조업 감시 등에 어떻게 기여하는지 사회적 영향을 분석하는 연구입니다. AIS 데이터가 해양 산업의 변화와 정책에 미친 영향을 분석하는 방법으로 접근할 수 있습니다.

2. 해상 교통과 자율항해의 법적 및 윤리적 문제

- 주제: "자율항해 기술의 발전에 따른 해상 교통의 법적 및 윤리적 문제 연구"
- 설명: 자율항해 기술이 발전하면서 발생할 수 있는 법적, 윤리적 이슈에 대해 탐구하는 주제입니다. 예를 들어 자율 항해 시스템의 오류로 사고가 발생했을 때의 책임 문제나, 기존 해양 노동자에게 미치는 영향 등을 분석할 수 있습니다.

3. AIS 데이터 기반 해양 빅데이터의 경제적 가치 분석

- 주제: "AIS 기반 해양 빅데이터의 경제적 가치 분석: 물류와 해양 산업에서의 활용 가능성"
- 설명: 해양 빅데이터로서 AIS 데이터를 이용하여 해양 물류, 항만 운영, 환경 모니터링 등에서 얻을 수 있는 경제적 가치를 분석하는 연구입니다. 이 데이터를 통해 발생하는 시장의 변화를 예측하고, 미래 산업에 미치는 영향을 평가해 볼 수 있습니다.

4. 자율항해와 AIS 기술의 발전이 지역 경제에 미치는 영향 연구

- 주제: "자율항해와 AIS 기술이 지역 해양 경제에 미치는 영향 연구: 새로운 일자리와 경제 활동 중심으로"
- 설명: 자율항해와 AIS 기술이 지역 해양 경제에 미치는 영향을 다룹니다. 기술 발전에 따라 생겨나는 새로운 직업군과 경제적 기회, 기존 직업의 변화 등을 조사하고 이를 통해 지역 경제에 미치는 긍정적, 부정적 영향을 평가해 보는 연구입니다.

5. 해양 네트워크 보안 및 프라이버시 문제에 대한 연구

- 주제: "AIS 네트워크 데이터의 보안 및 프라이버시 문제: 법적, 사회적 측면에서의 고찰"
- 설명: AIS 데이터를 비롯한 해양 네트워크 데이터가 보안 문제를 일으킬 수 있는 다양한 요소와 이를 해결하기 위한 법적·정책적 대응 방안을 다루는 연구입니다. 특히 데이터 유출로 인한 해양 산업의 위험 요소를 문과적 접근을 통해 탐구할 수 있습니다.

위 주제들은 AIS와 자율항해 기술을 사회적, 경제적, 윤리적 관점에서 다루기 때문에 문과적 배경을 바탕으로도 충분히 접근할 수 있을 것입니다.

🔊 📄 📌 🔍 ↺

"해양 네트워크 보안 및 프라이버시 문제에 대한 연구

주제: "AIS 네트워크 데이터의 보안 및 프라이버시 문제: 법적, 사회적 측면에서의 고찰"

설명: AIS 데이터를 비롯한 해양 네트워크 데이터가 보안 문제를 일으킬 수 있는 다양한 요소와 이를 해결하기 위한 법적·정책적 대응 방안을 다루는 연구입니다. 특히 데이터 유출로 인한 해양 산업의 위험 요소를 문과적 접근을 통해 탐구할 수 있습니다."

상기 논문 주제에 대해서 꽤 괜찮은 접근을 할 수 있을 것 같습니다. 해당 주제에 관련된 연구들을 2024년 시점 기준으로 조사해서 알려주세요.



AIS 데이터 보안과 프라이버시 문제는 2024년 현재 다양한 분야에서 중요한 논의로 부상하고 있습니다. 특히 해양 네트워크가 데이터 유출 및 보안 위협에 노출되면서 이에 대한 법적, 정책적 대응이 점차 강조되고 있습니다.

1. **데이터 프라이버시와 보안에 관한 규제 동향:** 유럽연합은 NIS 2 지침을 통해 중요 인프라(특히 항해 시스템)에서 보안 위협에 대한 예방과 대응을 강화하고 있으며, 미국 또한 2024년에는 다양한 주에서 데이터 프라이버시와 보안 규제를 확대할 계획입니다. 특히 여러 주가 개별적으로 프라이버시 및 보안 관련 법안을 추진하면서 통합적인 규제 환경이 부족한 상태가 지속되고 있습니다. 이러한 변화는 AIS 데이터와 같은 해양 네트워크 정보에 적용될 가능성이 큼니다

GREENBERG TRAURIG BIGID

2. **AI 및 자동화 시스템과 보안 문제:** 해양 산업의 자동화 시스템에 대한 데이터 보안 및 프라이버시 문제가 더욱 주목받고 있습니다. 특히 AI와 빅데이터의 활용이 늘어나면서 AIS 데이터와 같은 해양 네트워크 정보의 무단 사용 및 오용이 주요 이슈로 떠오르고 있습니다. 예를 들어, 해양 AIS 데이터는 민감한 항해 정보이기 때문에 유출 시 국가 안보와 산업에 큰 위협을 초래할 수 있습니다

3. **국제적 데이터 이동과 데이터 주권 문제:** 2023년에 체결된 미국과 유럽 간의 데이터 전송 협약은 다국적 기업과 해양 산업에 더 큰 일관성을 제공했지만, 데이터 주권을 지키기 위한 각국의 요구가 강화되면서 AIS 데이터와 같은 해양 정보의 전송과 관련한 새로운 규제와 정책이 논의될 가능성이 큼니다

WELLCOME | O'MELVENY | O'MELVENY

위와 같은 연구 배경을 통해 해양 네트워크 보안 및 프라이버시 문제를 법적·사회적 시각에서 고찰하는 주제는 현재 중요성이 높아지고 있으며, 현행 및 향후 정책 변화와 관련된 심도 있는 연구를 수행할 수 있는 좋은 기반이 될 것입니다.



"해수부는 31일 한덕수 국무총리가 주재한 제48회 국정현안관계장관 회의에서 이와 같은 내용을 담은 '해사 사이버안전 관리 강화방안'을 발표했다. 선사·선박의 사이버 보안 능력 강화를 지원하고, 법적 기반 마련과 관련 기술 개발 등을 추진한다는 목표다.

최근 선박과 운항 시스템이 디지털화되면서 선박의 사이버 공격도 늘어나는 추세다. 해외에서는 선박에 대한 사이버 공격으로 약 10여시간 동안 운항 통제권을 잃거나, 선사 시스템의 랜섬웨어 감염으로 인해 약 3000억원의 손실을 입은 사례 등이 발생했다. 국내에서도 현재까지 852척에 달하는 선박 위치정보(GPS) 교란이 발생했지만, 아직까지 구체적인 피해는 없었다.

관세청에 따르면 한국의 수출입 물동량 중 99.7%는 선박을 통해 오고간다. 그만큼 선박에 대한 사이버 공격이 이뤄진다면 수출입 피해와 해상물류 공급망 훼손이 이뤄질 수 있다. 최성용 해수부 해사안전국장은 "과학기술정보통신부, 중소벤처기업부 등 관계부처와 합동으로 이번 해사 사이버 안전 강화 방안을 마련하게 됐다"고 설명했다.

먼저 해수부는 선사·선박이 활용할 수 있는 표준지침서·매뉴얼을 내년부터 배포하기로 했다. 또 중견·중소 선사를 위해서는 올해부터 보안 취약점을 진단하는 컨설팅을 제공한다. 이외에도 선사·선원을 위한 교육과 더불어 내달부터는 정기적으로 민·관 합동 해상 사이버 사고 대응훈련을 실시할 계획이다.

최 국장은 "선사별로 상황은 다르지만, '선박에 화물을 싣는다'는 공통점이 있기 때문에 이를 기반으로 사이버 공격에 대응할 수 있는 표준 지침을 배포하고, 주요 취약점이 공격받았을 경우 대응할 수 있는 방안을 담은 기술 대응 매뉴얼도 함께 보급된다"고 설명했다. 그러면서 "현재 지침은 의견 조회 등을 거쳐 제작 중이며, 완성도를 높여 내년 본격적으로 배포된다"고 덧붙였다.

또 2027년 시행을 목표로 민간 선사와 선박의 사이버 안전 관리체계 구축, 선박 및 장비에 대한 보안인증 제도 관련 내용을 법제화하기로 했다. 국제선급협회가 시행 중인 선박·장비의 사이버보안 인증 획득을 위한 기술을 지원하고, 50~70% 수준의 비용을 지원할 계획이다.

아울러 각종 사이버 공격 위협요인을 사전에 탐지하고 대응할 수 있는 연구개발(R&D)도 실시한다. 해수부는 기술 개발과 실증을 지원하고, GPS 전파교란에 대비할 수 있는 통합 단말기를 2026년까지 개발해 보급할 계획이다. 또 국내 기술들이 국제 표준으로 자리잡을 수 있도록 홍보 강화 등도 강조했다.

강도형 해수부 장관은 "해상 물류 공급망이 안정적으로 유지되도록 관계부처와 함께 차질 없이 방안을 이행하겠다"며 "선사 등 민간에서도 선박 안전 강화를 위해 적극적으로 참여해달라"고 당부했다.

권효중 (khjing@edaily.co.kr)의 내용을 반영해서 "AIS 데이터 보안과 프라이버시 문제는 2024년 현재 다양한 분야에서 중요한 논의로 부상하고 있습니다. 특히 해양 네트워크가 데이터 유출 및 보안 위협에 노출되면서 이에 대한 법적, 정책적 대응이 점차 강조되고 있습니다.

데이터 프라이버시와 보안에 관한 규제 동향: 유럽연합은 NIS 2 지침을 통해 중요 인프라(특히 항해 시스템)에서 보안 위협에 대한 예방과 대응을 강화하고 있으며, 미국 또한 2024년에는 다양한 주에서 데이터 프라이버시와 보안 규제를 확대할 계획입니다. 특히 여러 국가 개별적으로 프라이버시 및 보안 관련 법안을 추진하면서 통합적인 규제 환경이 부족한 상태가 지속되고 있습니다. 이러한 변화는 AIS 데이터와 같은 해양 네트워크 정보에 적용될 가능성이 큼니다

GREENBERG TRAURIG

BIGID

AI 및 자동화 시스템과 보안 문제: 해양 산업의 자동화 시스템에 대한 데이터 보안 및 프라이버시 문제가 더욱 주목받고 있습니다. 특히 AI와 빅데이터의 활용이 늘어나면서 AIS 데이터와 같은 해양 네트워크 정보의 무단 사용 및 오용이 주요 이슈로 떠오르고 있습니다. 예를 들어, 해양 AIS 데이터는 민감한 항해 정보이기 때문에 유출 시 국가 안보와 산업에 큰 위협을 초래할 수 있습니다

BIGID

국제적 데이터 이동과 데이터 주권 문제: 2023년에 체결된 미국과 유럽 간의 데이터 전송 협약은 다국적 기업과 해양 산업에 더 큰 일관성을 제공했지만, 데이터 주권을 지키기 위한 각국의 요구가 강화되면서 AIS 데이터와 같은 해양 정보의 전송과 관련한 새로운 규제와 정책이 논의될 가능성이 큼니다

WELCOME | O'MELVENY - O'MELVENY

위와 같은 연구 배경을 통해 해양 네트워크 보안 및 프라이버시 문제를 법적·사회적 시각에서 고찰하는 주제는 현재 중요성이 높아지고 있으며, 현행 및 향후 정책 변화와 관련된 심도 있는 연구를 수행할 수 있는 좋은 기반이 될 것입니다." 해당 연구배경을 업데이트해주세요



AIS 데이터 보안과 프라이버시 문제는 2024년 현재 해양 네트워크와 데이터 유출, 보안 위협에 대한 법적·정책적 대응이 점차 강조되며 중점적으로 다뤄지고 있습니다. 다음은 최근의 정책 및 연구 동향을 바탕으로 한 해양 사이버 보안의 주요 과제입니다.

1. 국내 사이버 보안 정책 강화

최근 한국 해양수산부는 선사 및 선박의 사이버 보안 능력 강화를 위해 표준 지침서와 매뉴얼 배포, 보안 취약점 진단 컨설팅 등을 제공하는 정책을 발표했습니다. 해수부는 특히 GPS 전파 교란에 대비할 수 있는 통합 단말기 개발, 해상 물류 공급망 보호를 위한 해상 사이버 사고 대응훈련을 민·관 합동으로 실시하고 있습니다. 또한, 2027년까지 민간 선사와 선박의 사이버 안전 관리체계를 구축하고 보안 인증 제도를 법제화할 계획입니다

GREENBERG TRAURIG

BIGID

2. 국제적 보안 규제와 프라이버시 문제

유럽연합의 NIS 2 지침은 항해 시스템을 포함한 중요 인프라의 보안 위협 예방을 강화하고 있으며, 미국도 2024년 데이터 프라이버시와 보안 규제를 다수의 주에서 확대할 예정입니다. 이와 같은 변화는 해상 AIS 데이터와 네트워크 정보에도 직접적인 영향을 미칠 수 있으며, 데이터 주권과 규제에 대한 각국의 요구도 점점 증가하고 있습니다

BIGID

WELCOME | O'MELVENY - O'MELVENY

3. AI 및 자동화 기술과 데이터 보안의 중요성

자동화 시스템과 AI 기술이 발전하면서 AIS 데이터와 같은 해양 네트워크 정보의 오용 가능성도 증가하고 있습니다. 예를 들어 랜섬웨어나 GPS 교란 공격이 일어날 경우 국가 안보 및 경제적 위험이 초래될 수 있습니다. 이에 해수부와 과기부는 사이버 위협 요소를 탐지하고 대응할 수 있는 R&D 연구를 강화하고 있으며, 민감한 해양 정보에 대한 보호를 지속적으로 추구하고 있습니다

GREENBERG TRAURIG WELCOME | O'MELVENY O'MELVENY

이처럼 해양 네트워크 보안과 프라이버시 문제는 현재 주요 이슈로 자리 잡고 있으며, 다양한 규제와 기술 개발 노력이 진행 중입니다. 이를 바탕으로, AIS 및 해양 네트워크 보안 문제에 대한 법적·사회적 시각에서의 연구가 필요한 시점이라 할 수 있습니다.

🔊 📄 📌 🔗 ↻

현재 2024년 인터넷 자료를 반영해서, 선사선박관리시스템에 이용되는 보안 프로그램의 개발 현황에 대해서 조사해서 알려주세요. 그리고 취약점이 무엇인지도 반영해주세요.

현재 선박 관리 시스템을 위한 사이버 보안 프로그램의 개발은 주로 안전성과 데이터 보호에 중점을 두고 있으며, 선박의 네트워크 보안을 강화하는 데 초점을 맞추고 있습니다. 예를 들어, 선박 관리 시스템을 위한 소프트웨어는 주로 랜섬웨어와 데이터 유출 위협에 직면해 있으며, 시스템의 복잡성과 다양한 기술 의존도가 보안 취약성을 유발하고 있습니다. 최근에는 노르웨이의 DNV사가 선박 관리 소프트웨어인 ShipManager가 랜섬웨어 공격을 받아 1,000척 이상의 선박 운영이 중단된 사례가 있었습니다. 이는 선박 관리 소프트웨어의 랜섬웨어 및 악성 코드 공격에 대한 대비가 아직 불충분하다는 점을 시사합니다.

또한 선박이 점점 더 디지털화됨에 따라, 엔진 제어, 항해 시스템, 전자 차트 등의 시스템이 해킹에 노출될 가능성이 높아졌습니다. 이러한 시스템이 공격당하면 선박의 안전과 항로가 위협받을 수 있으며, 경우에 따라 심각한 경제적 손실이나 환경적 재해를 초래할 수 있습니다. 특히, 네트워크가 분리되지 않거나 구형 소프트웨어를 사용하는 경우가 많아 보안 취약점이 발생할 가능성이 큼니다. 이를 해결하기 위해 네트워크 분리, 소프트웨어 업데이트, 강력한 암호 정책 적용 등의 보안 조치가 권장됩니다.

IMO(국제해사기구)와 같은 규제 기관은 선박 관리 시스템에 대한 사이버 보안 지침을 제안하고 있지만, 규제 수준은 아직 충분하지 않다는 평가를 받고 있습니다. 따라서 많은 선박 관리 회사들은 자발적으로 보안 점검과 네트워크 격리, 직원 교육 등 자사 차원의 보안 관리 시스템을 강화하는 노력이 요구되고 있습니다.



이처럼 선박 관리 시스템에서의 보안 프로그램 개발과 관련하여, 랜섬웨어 대응, 네트워크 분리, 소프트웨어 업데이트 등의 강화가 필요하며, 특히 최신 보안 위협에 대응할 수 있는 철저한 관리가 필요합니다.

🔊 📄 📌 🔗 ↻

국내선박의 경우에는 만약 외부에서 사이버 공격이 들어왔을때 막을 수 있는 보안프로그램이 개발되어 있나요?



사이트 3개 검색함

Yes, South Korea has developed cybersecurity programs to defend against external cyber threats targeting its maritime and broader critical infrastructures, though challenges remain. The National Cybersecurity Strategy, updated in 2024, includes measures focused on maritime industries, given the heightened cyberattacks in recent years, especially from state-backed entities like North Korea. South Korean agencies such as the National Intelligence Service (NIS) and the Korea Internet and Security Agency (KISA) actively work to secure critical sectors, including maritime, against various threats like ransomware, supply chain risks, and sophisticated hacking tools.

Despite these advancements, vulnerabilities persist. For example, South Korean systems are prone to supply chain attacks and threats targeting mobile device security and digital assets, which could impact maritime operations if breached. Some cybersecurity improvements are achieved through collaborations with foreign cybersecurity firms, which help to fill technical and operational gaps. However, securing legacy systems on ships and the overall digital infrastructure remains a challenge, requiring continuous upgrades to fend off increasingly sophisticated threats.

Efforts such as implementing zero-trust security models, strengthening infrastructure resilience, and creating rapid response capabilities are part of South Korea's strategic approach. However,



and creating rapid response capabilities are part of South Korea's strategic approach. However, ongoing adaptation and integration of new technologies are needed to ensure maritime cybersecurity aligns with the evolving threat landscape.

For more details, you can review the sources from the CSIS on South Korea's National Cybersecurity Strategy and insights from Trade.gov on South Korea's cybersecurity landscape.

For more details, you can review the sources from the CSIS on South Korea's National Cybersecurity Strategy and insights from Trade.gov on South Korea's cybersecurity landscape.” 한국어로 바꿔주세요



네, 한국은 외부 사이버 위협으로부터 해양 및 주요 인프라를 방어하기 위해 다양한 사이버 보안 프로그램을 개발하였으나 여전히 해결해야 할 과제들이 남아 있습니다. 2024년에 업데이트된 국가 사이버 보안 전략은 특히 해양 산업에 중점을 두고 있으며, 최근 몇 년간 북한과 같은 국가 지원 해커들의 공격이 증가함에 따라 이에 대한 대책이 강조되고 있습니다. 국가정보원(NIS)과 한국인터넷진흥원(KISA)과 같은 기관은 랜섬웨어, 공급망 위협, 정교한 해킹 도구 등 다양한 사이버 위협에 대응하여 해양을 포함한 여러 중요 산업의 보안을 강화하고 있습니다.

이러한 발전에도 불구하고 취약점이 여전히 존재합니다. 예를 들어, 한국 시스템은 공급망 공격이나 모바일 기기 및 디지털 자산 보안 문제에 취약하며, 이러한 보안 취약점이 해양 운송 및 운영에 영향을 미칠 가능성이 있습니다. 일부 사이버 보안 향상은 외국 사이버 보안 회사와의 협업을 통해 이루어지고 있으며, 이를 통해 기술적, 운영적 격차를 해소하고 있습니다. 그러나 선박의 구형 시스템 및 전체 디지털 인프라의 보안을 확보하는 일은 여전히 과제로 남아 있어 점점 더 정교해지는 위협을 방어하기 위한 지속적인 업그레이드가 필요합니다.

한국의 전략적 접근 방식에는 제로 트러스트 보안 모델 도입, 인프라 복원력 강화, 신속 대응 능력 구축 등이 포함되어 있습니다. 그러나 해양 사이버 보안이 빠르게 변화하는 위협 환경에 맞게 조정되고, 신기술이 지속적으로 통합될 수 있도록 끊임없는 개선이 요구됩니다.

추가 정보는 CSIS의 한국 국가 사이버 보안 [전](#) 보고서와 Trade.gov의 한국 사이버 보안 관련 인사이트를 참조할 수 있습니다.