KR Maritime Cyber Security

News from KOREAN REGISTER

Nov 2018

Vol. 007

한국선급 활동

● **해사업계 대상 사이버보안 교육 수행**

지난 10월, 한국선급 사이버보안 대응 TFT는 KR 교육훈련원에서 국가인적자원개발 컨소시엄 교육 과정인 '해사 사이버보안의 이해' 및 '해사 사이버보안 관리 실무' 과정 교육을 수행하였다.

'해사 사이버보안의 이해[8H]' 과정은 해사업계(선사, 선박, 조선소, 기자재업체)에 근무하는 임직원 및 선원들을 대상으로 사이버보안에 대한 이해를 증진시키고, 사이버보안에 필요한 사이버보안 조직, 사이버 자산관리 및 위협, 인적 보안, 물리 보안, 기술 보안 교육을 통해 해사 사이버보안에 대한 인식 제고 향상을 목표로 한다.

'해사 사이버보안 관리 실무[16H]' 과정은 심화과정으로써 사이버보안 IT 해설 및 실습, 사이버 리스크평가 이해 및 실습으로 구성되어 있다. 특히 리스크평가 워크샵을 통해 회사 및 선박 사이버 취약점을 식별하고, 리스크 평가 절차 및 방법, 개선 방안 등을 직접 확인 할 수 있다.

한국선급은 본 교육과정을 통해 IMO와 OCIMF TMSA/SIRE 및 RIGHTSHIP 등의 화주검사에서 요구하고 있는 사이버보안 인식제고 교육 및 사이버 리스크 관리 방법을 국내 해사업계에 전파하였으며, 피드백 사항을 반영하여 다양한 사이버보안 실무 교육 과정을 2019년 개최할 예정이다.

● 2018년 터키/그리스 기술 세미나 개최

한국선급은 지난 10월 30일부터 1일까지 그리스와 터키에서 해사업계 관계자를 대상으로 기술세미나 및 그리스 위원회를 개최하였다. 30일 터키에서 열린 세미나에는 50여명, 31일 그리스에서 열린 세미나에는 100여명의 해운회사, 조선소, 학계 등 해사업계 관계자가 참석하였다. 세미나에서 한국선급은 선박평형수처리시스템(BWMS) 동향, 벌크선 최신 선형, 사이버보안 실사례, 황산화물(SOx) 규제 동향에 대해 발표했다. 특히 최근 국제해사기구(IMO) 해양환경보호위원회(MEPC) 제73차 회의에서 황산화물 경험 축적기(EBP : Experience Building Phase) 도입안이 유보된 내용을 공유하여, 선박 황산화물 규제 시행에 대한 업계 관계자들의 궁금증을 해소하였다. 2일에는 그리스 아테네에서 그리스 위원회를 개최하였다. 그리스와 그리스 인근 지역의 주요 해운회사 등 관련업계의 임원 60여명으로 구성된 위원들은 최근 해사업계의 주요 쟁점에 대해 논의하였다. 이번 위원회에서는 세계적인 조선·해운 분석기관인 클락슨 리서치의 임원인 스티븐 고든(Stephen Gordon)이 해사업계 시장 현황에 관한 발표를 하여 많은 참석자들의 관심을 받았다.

이정기 한국선급 회장은 "지금 해사업계는 강화되는 환경규제와 불확실한 미래로 인해 혼란스러운 상황에 놓여있다"고 하며 "한국선급은 업계에 보탬이 되고자 국내외에서 최신 동향에 대한 정보를 제공하는 자리를 지속적으로 마련하겠다"고 말했다.

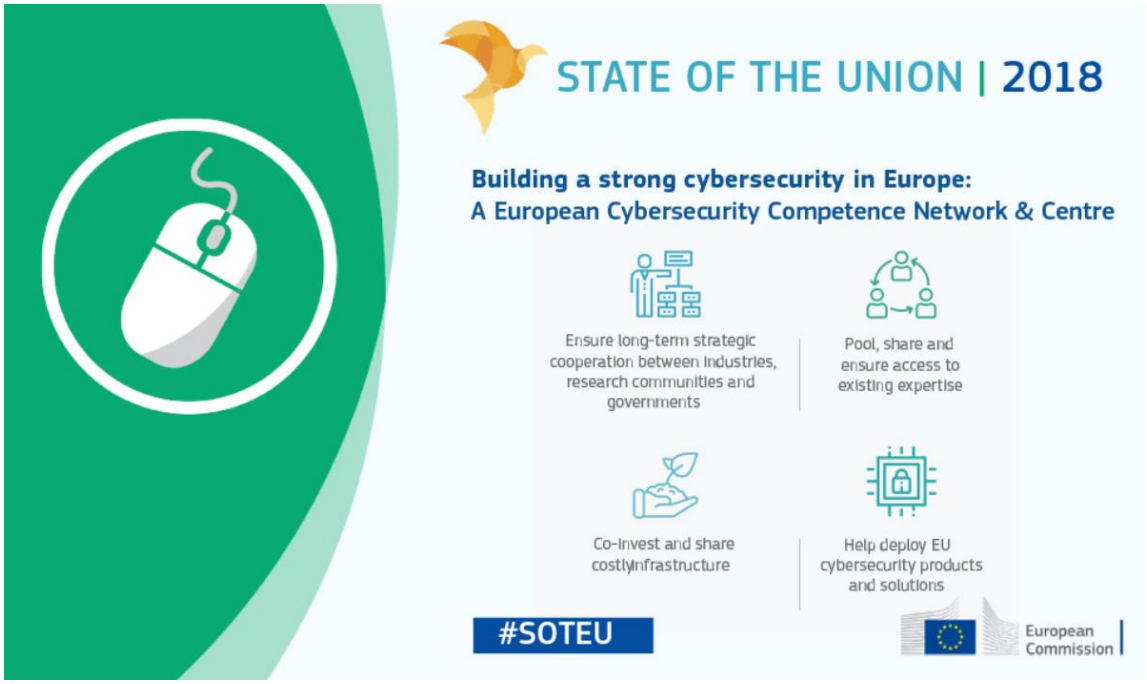
EU 사이버보안 인증 프레임워크 구축

● EU 사이버보안 인증 프레임워크 구축

사이버 복원력을 향상시키기 위해 유럽연합(EU)은 정보통신기술(ICT) 제품, 서비스 및 프로세스에 대한 인증 프레임워크를 구축하고 있다. 2018년 6월 8일, 이사회는 유럽 의회와 협상을 통해 텍스트를 완성하기 위한 제안(사이버 보안법)에 동의했다. 이 제안의 효과 중 하나는 현재의 유럽 연합 네트워크 정보 보안 기관(ENISA)을 사이버 보안을 위한 더 안정적인 EU 에이전트로 업그레이드할 것이라는 점이다.

● 사이버보안 인증

제안된 인증 체계는 포괄적인 일련의 규칙, 기술 요건, 표준 및 절차로서 EU 전체의 인증 제도를 제공한다. 그 계획에 따라 발급된 증명서는 법적으로 유럽 연합 전체에 걸쳐 인정되며, 이 인증은 제도에 따라 ICT 제품과 서비스가 지정된 사이버보안 요건을 준수함을 증명한다. 따라서 인증은 기술이 유럽 사이버보안 보안 스탬프를 받은 것을 의미하고 기업들이 국경을 초월하여 비즈니스를 수행할 수 있도록 하는 것을 의미한다. 현재 이 규정안은 유럽연합 회원국들의 동의를 받은 상태이며, 이제 유럽연합 위원회(EU Committee)의 승인을 받고, 그 다음으로 유럽의회(EU Parliament)를 통과하면 GDPR처럼 정식 도입될 것으로 예상된다.



Ref. : The EU cybersecurity certification framework

나이지리아 해킹그룹, 해상 사이버 공격을 감행하다

● **해운분야에서의 Cyber Security 이슈**

최근 국내/외에서, 선박운항시스템, 항만관리 및 운영, 자율운항선박 등에 다양한 정보통신기술(ICT) 적용이 증가하면서 해운업계 사이버보안 위협도 커지고 있다. 해운산업을 목표로 공격하는 조직이 지속적으로 발견되고 있으며, E-mail 침해 기법, E-mail 스푸핑, 온라인 송금 우회 공격, Spear phishing, 물리적인 탈취가 고루 사용되는 것을 볼 수 있다.

특히, 기존의 물리 보안에서 자주 언급되는 현안이었던 해적, 화물 분실/탈취, 밀항/난민 등의 물리적 요인부터 시작하여 최근 새롭게 검토하고 있는 스마트 선박에 적용되는 사물인터넷(IoT), 임베디드 시스템 및 다양한 사이버 자산에 대한 해킹까지 선박에 대한 위협 범위가 넓어지는 양상이다.

올해 4월에 발생하였던 나이지리아의 Gold Galleon Hacking 그룹의 경우, 선사만을 대상으로 사이버 범죄를 일으킨 사례 중 하나이며, 관련 Hacking 사고의 경우 국내 선사의 E-mail 정보가 탈취 부분도 포함되어 있었다.

Ref. : DarkReading

● **나이지리아 해킹그룹 사이버 공격 사례**

해운산업은 Business E-mail 침해(BEC) 기법, Business E-mail 스푸핑(BES) 사기 및 공격에 매우 취약하다. 산업 특성상 업무 공간이 전 세계 퍼져 있고, 이러한 특성으로 V-SAT및 FBB, F33, F77을 통한 위성통신 서비스에 대한 의존도 높은 상황이다. 또한, 중앙 혹은 본사와의 정보 공유가 안전 부문을 제외하면 다른 산업에 비하여 자주 발생하지 않는다. 그렇기에 본사의 고위급 인사로 사칭하는 보안사고가 빈번히 발생한다.

Gold Galleon의 공격 전략과 기술은 굉장히 새롭거나 고급적이지 않다. 다만 공격 표적을 잘 선정하고 그 취약점을 노릴 뿐이다. 그들은 실제 공격 전에 회사 내 시스템에 침투해 내부 및 거래처 연락처, 선박일정, 대금지불 등과 같은 관련 정보를 빼낸다. 그렇게 한 후 표적이 된 회사의 웹사이트를 면밀히 분석하여, 사전 확보된 정보와 결합하여 사기에 이용한다. 즉 신뢰가 가는 E-mail로 Spear phishing 공격을 하는 것이다. 이 때 프레데이터 페인(Predator Pain)이나 포니스틸러(PonyStealer), 에이전트 테슬라(Agent Tesla), 호크아이(Hawkeye) 등과 같은 Malware를 페이로드로서 함께 전송한다.

Secureworks社 Counter Threat Unit의 분석가 벳케는 "Gold Galleon은 볼륨이 그리 크지 않은 스팸 공격을 하면서 Malware 로더를 뿌립니다. 그렇게 한 후 데이터 접근에 성공하면 그 데이터를 검토하여 선적 현황 및 운송 스케줄을 확인합니다. 특히 영수증 및 청구서 관련 날짜를 파악하여 실제 양식의 PDF 파일을 가로챕니다. 그 다음 받는 사람 주소를 살짝 바꿔서 다시 보내죠. 사실 간단한 사기입니다. 선박 및 선적의 스케줄을 전부 알고 있고, 이들이 보내는 가짜 청구서는 진짜 양식을 훔쳐서 정보의 일부만 조작하는 것이기 때문에 보통은 속을 수밖에 없습니다."라고 언급했다.

대응 방안 및 시사점

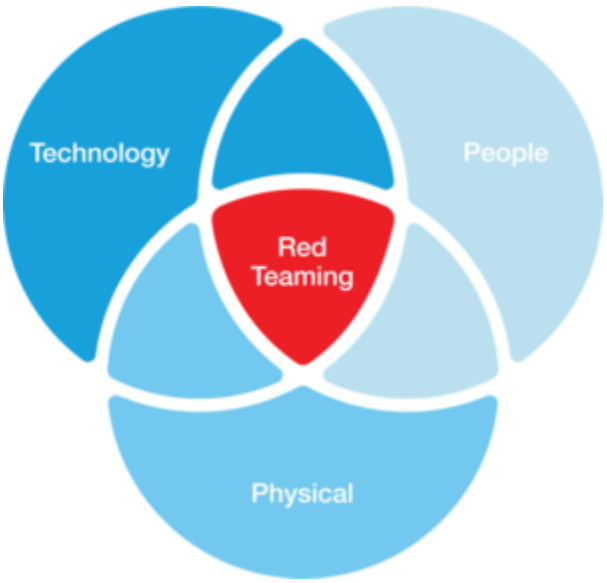
해운산업은 전 세계 교역량의 90~94%가 운송되며, 많은 금전거래와 이해관계자와의 데이터가 교환되는 곳이지만 보안은 물리적인 부분에만 한정되어 있는 상황이다. 하지만, 선원 등 해안산업 관계자를 대상으로 한 설문조사를 보면, 사이버 공격의 피해를 받은 적이 있느냐에 대한 물음에 21%가 그렇다고 대답했다. 또 그로 인한 피해는 IT 시스템의 기능상 문제(67%), 회사 데이터 유실(48%), 금전적 손실(21%), 해상 운송 시스템 기능상 문제(4%) 등이었다고 답변했다. 이를 예방하기 위한 확실한 방법으로 직원 교육, 강력한 비밀번호 설정, 암호화, 이중인증 도입 등이 권고된다.

O/T 진단 및 Red Teaming Project란?

● **O/T 진단 및 Red Teaming Project의 필요성**

항만 및 선박에 대한 보안진단은 여러가지 형태로 진행이 될 수 있지만, 현장과 관련 산업에 대한 이해를 바탕으로 운영 환경(OZ : Operation Zone)에서 보안 점검이 수행되는 Red Teaming 프로젝트를 권고한다.

Red Teaming 평가는 회사 내 보안팀에게 실제 IT 만이 아니라 OZ영역에서의 사이버 공격에 대처하는 실질적인 경험을 제공하는 데 중점을 두어서, 이러한 보안 진단 서비스를 통해 회사의 실제 운영 시스템이나 비즈니스에 피해를 입히는 공격을 회피하는 한편, 기존 및 지능형 공격자 Tactics, Techniques and Procedures(TTPs)를 사용하여 Red Teaming Project와 사내 보안팀이 준비한 목표를 표적으로 삼는다.



위 그림과 같이 기존의 Technology 영역에 대한 보안진단을 뛰어넘어 실제 운영 환경에 대한 이해를 통한 물리 침투를 수행하며, 소셜 엔지니어링 해킹 등을 이용하여 육상 및 해상에서 업무를 수행하는 내부 직원(해기사 포함)들에 대한 공격도 함께 진행된다.

신청기관이 공격 목표(보통 최악의 경우를 가정하는 비즈니스 시나리오)를 정하면 보안 업체에서 제공하는 Red Teaming 작업을 시작한다. 최종적으로 Red Teaming은 초기 정찰에서 임무 완수에 이르는 전체적인 공격 수명주기를 시행한다.

공격 형태는 항만 및 선박에 대한 운영 환경에 대한 이해에서부터 시작한다. 이를 통해서 신청기관의 가장 핵심 자산을 정의하고 신청자와의 협의를 통해서 프로젝트의 Goal을 설정한다.

Red Teaming 활동은 가장 중요한 자산을 보호하는 고객의 내부 보안 직원의 능력을 테스트한다. 이 전문가는 사이버 공격의 최일선에서 얻은 경험을 바탕으로 피해 없이 실제 표적 공격의 전술, 기법 및 절차(TTPs)를 시뮬레이션한다.

Red Teaming 운영은 표적 공격으로부터 중요한 자산을 보호하는 능력을 테스트하려는 조직에 적합하다. Red Teaming 보안 활동은 표적 공격으로부터 침해 탐지와 대응 능력을 개선하기 위해 조직의 보안팀을 훈련시키려는 조직에 적합하다.

공격자가 항만 및 선박에 대한 운영 환경에 대한 이해에서 시작이 된다는 점에서, 해당 보안팀과 보안을 담당하는 Officer에 대한 기본 요건에 대해서 생각을 해야 한다.

다음 번에는 Red Teaming 활동을 구체적으로 다루기 전에, Operation Zone 보안을 다루고 있는 ICS/SCADA 영역 보안을 연재할 예정이다.

▪ 본 기사는 (㈜ NSHC & Shield Consulting co.,ltd* 이승준 책임연구원에 의해 작성되었습니다.

* NSHC SECURITY는 ICS/SCADA(OT)사이버보안 분야에서 국내 및 아시아에서 유일하게 사이버 침투테스트 수행가능한 회사이며, 랜섬웨어, APT 공격과 같은 악성코드 분석 및 산업용 기기 대상 침투테스트 및 소스코드 진단을 수행하고 있다. SHIELD CONSULTING은 사이버보안에서 요구되는 물리적 보안(CCTV, 외부자 출입, 전자기기 반입 통제, 잠금장치) 컨설팅을 제공하고 있다.

사이버 위협의 이해

● 사이버 위협 이해하기

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

● 한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

● BSI 10대 위협

ICS에 대한 위협은 기존의 취약성으로 인해 ICS 및 관련 기업에 잠재적으로 손상을 줄 수 있는 공격 또는 이벤트로 인한 것이다. 다음 표는 독일 연방정보 보안국에서 발표한 ICS에 대한 가장 중대한 위협 목록이다. 지난 7월 뉴스레터에 이어 BSI 10대 사이버 위협 중 '**기술적 오작동 및 불가항력**'에 대해서 분석하고자 한다.

No. (old No.)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering and Phishing†	Malware Infection via Internet and Intranet
2 (2)	Infiltration of Malware via Removable Media and External Hardware	Infiltration of Malware via Removable Media and External Hardware
3 (1)	Malware Infection via Internet and Intranet	Social Engineering
4 (5)	Intrusion via Remote Access	Human Error and Sabotage
5 (4)	Human Error and Sabotage	Intrusion via Remote Access
6 (6)	Control Components Connected to the Internet	Control Components Connected to the Internet
7 (7)	Technical Malfunctions and Force Majeure	Technical Malfunctions and Force Majeure
8 (9)	Compromising of Extranet and Cloud Components	Compromising of Smartphones in the Production Environment
9 (10)	(D)DoS Attacks	Compromising of Extranet and Cloud Components
10 (8)	Compromising of Smartphones in the Production Environment	(D)DoS Attacks

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

● **BSI 10대 위협 : 기술적 오작동 및 불가항력**

예상치 못한 오작동을 유발할 수 있는 보안 관련 구성 요소 및 ICS 구성 요소에서 소프트웨어 오류를 배제할 수 없으며 하드웨어 결함 및 순 작업 오류가 발생할 수 있다. 특히 하드웨어 결함은 필요한 사전 조치가 취해지지 않은 경우 기존 환경 조건(먼지, 온도 등)으로 인해 특정 적용 시나리오에서 발생할 가능성이 더 높다.

<가능 시나리오>

▣ 구성 요소 결함, 예를 들어, 하드 디스크 또는 스위치의 고장, 케이블 파손 등

▣ 하드웨어 결함 및 소프트웨어 구성 요소의 오류는 오랫동안 발견되지 않고 남아있을 수 있다. (예 : 시스템이 다시 시작되거나 특정 제한 조건이 적용)

▣ 소프트웨어 오류로 인해 시스템이 오작동 할 수 있다. 예를 들어 중앙 보안 구성 요소의 운영 체제를 업데이트하고 다시 시작하면 시스템 오작동이 발생 수 있다. 이 시나리오는 일반적으로 내부자 거래뿐만 아니라 부주의와 인적 실수로도 발생 할 수 있다.

특히 이러한 사고는 조직의 결점으로 인해 가용성이 크게 제한 될 수 있다.

<대책>

- 잠재적인 대응책, 시스템 복구 절차, 대체 통신 옵션 및 훈련 실시와 같은 측면을 포함하여 비즈니스 연속성 관리를 수립한다.
- 교환 또는 교체 장치를 준비한다.
- 패치, 업데이트 및 새 소프트웨어 구성 요소를 운영 시스템에 설치하기 전에 철저하게 테스트하고 사용한다.
- 중요한 구성 요소를 이중설계한다.
- 사용된 시스템 및 구성 요소를 선택하기 위해서는 식별된 보호 필요성에 따라 충분한 최소 요구 사항을 정의하고 시행하여야 한다. 중요한 몇 가지 측면은 다음과 같다.
  - 제품 공급장의 신뢰성
  - 제품의 견고성
  - 적절한 보안 메카니즘의 존재 (예를 들어, 보안 인증)
  - 예비 부품의 장기간 가용성, 업데이트 및 유지 보수
  - 패치의 적절한 가용성
  - 불필요한 제품 기능을 사용하지 않음

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

인적 보안 체계 수립 가이드

● 인적 보안 필요성

근무하는 임직원의 채용 및 계약, 전출입 시 보안 대책, 사이버보안 교육 훈련 및 사이버보안 위반자에 대한 지침을 정하여, 회사 사이버자산을 적절히 보호하고자 함을 그 목적으로 한다. 적용대상은 모든 임직원(정규직 및 계약직), 외부인력(파견직, 위탁계약, 협력업체 등)을 포함하며, 보안 서약서를 작성해야 한다.

● 한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)

보안 교육 (203.1) : 보안활동 관련자는 보안교육 계획에 따라 연 1회 이상 보안교육을 실시하여야 한다.

보안 교육 (203.2) : 신규 입사자(협력업체, 임시직 포함) 및 퇴사자에 대한 보안교육을 실시하여야 하며, 특히 국내외 출장 및 부재자에게 필요한 교육도 실시하여야 한다.

● 보안유지 서약서

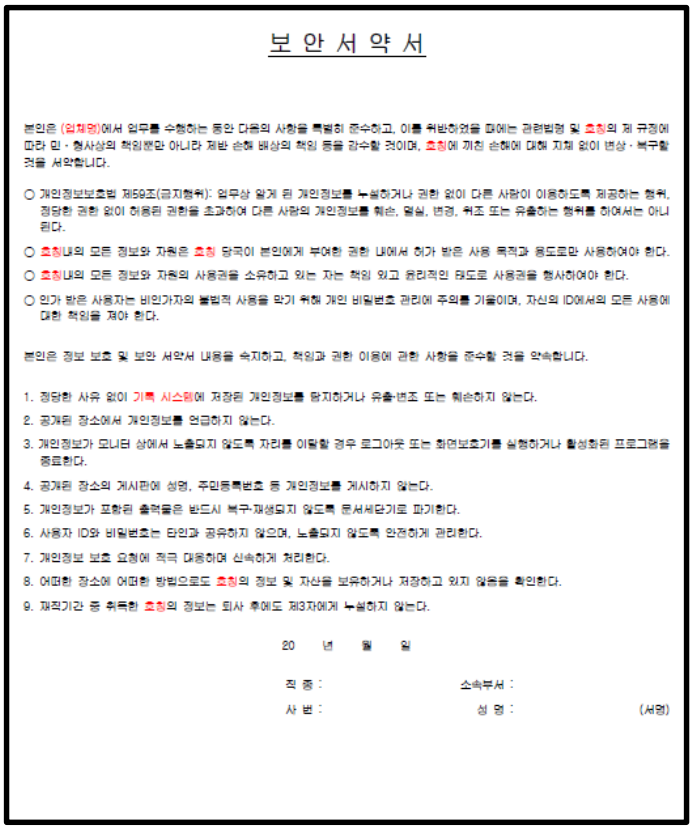
1) **신규로 채용되거나 전입된 인력**은 회사의 중요정보 취급 및 사이버보안의 필요성과 책임에 대해 명시된 **서약서에 서명**하고 회사에 제출하여야 한다.

2) **임직원의 퇴직 시 및 전출 시**에는 직무상 알게 된 조직의 중요 정보에 대한 누출방지를 위하여 보안유지 서약서를 받고 누출 발생시 그에 따르는 법적 책임이 있음을 상기시킨다.

3) 임시직원 혹은 외주용역업체 직원에게 정보자산에 대한 접근권한을 부여할 경우, 사이버보안 준수의무 및 미준수로 인한 사건발생 시 손해배상 청구 등의 내용이 담긴 **보안서약서**에 서명을 받아야 한다.

4) 서약서에 개인정보가 포함될 경우 비인가된 제3자에게 누출되지 않도록 **물리적으로 안전한 장소**에 보관 하여야 한다.

● **보안서약서 및 전출 및 퇴직 확인서(예시)**



보 안 서 약 서

본인은 (입체명)에서 업무를 수행하는 동안 다음의 사항을 준수하고, 이를 위반하였을 때에는 관련법령 및 호칭의 제 규정에 따라 민·형사상의 책임뿐만 아니라 제반 손해 배상의 책임 등을 감수할 것이며, 호칭에 끼친 손해에 대해 지체 없이 변상·복구할 것을 서약합니다.

○ 개인정보보호법 제59조(금지행위): 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위, 정당한 권한 없이 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위를 하여서는 아니 된다.

○ 호칭내의 모든 정보와 자원은 호칭 당국이 본인에게 부여한 권한 내에서 허가 받은 사용 목적과 용도로만 사용하여야 한다.

○ 호칭내의 모든 정보와 자원의 사용권을 소유하고 있는 자는 책임 있고 윤리적인 태도로 사용권을 행사하여야 한다.

○ 인가 받은 사용자는 비인가자의 불법적 사용을 막기 위해 개인 비밀번호 관리에 주의를 기울이며, 자신의 ID에서의 모든 사용에 대한 책임을 져야 한다.

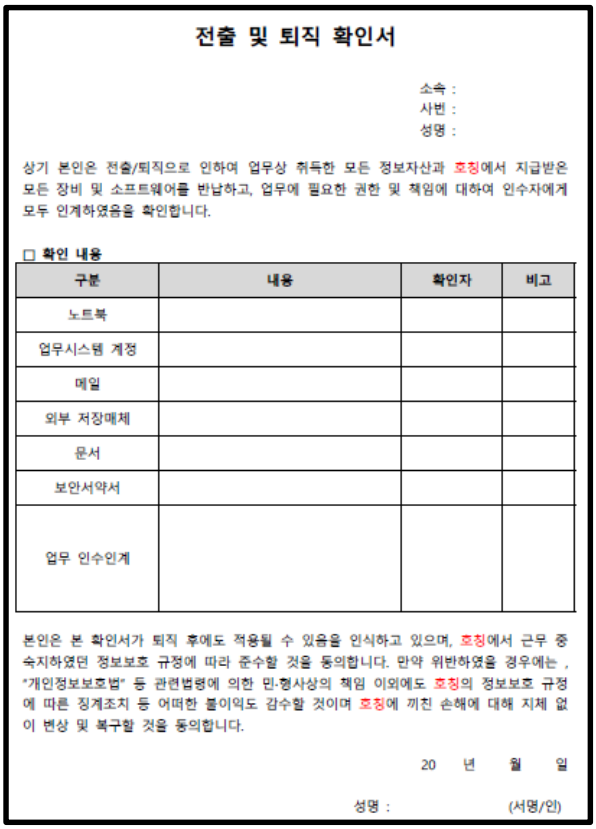
본인은 정보 보호 및 보안 서약서 내용을 숙지하고, 책임과 권한 이행에 관한 사항을 준수할 것을 약속합니다.

1. 정당한 사유 없이 기록 시스템에 저장된 개인정보를 멸지하거나 유출·변조 또는 훼손하지 않는다.
2. 공개된 장소에서 개인정보를 언급하지 않는다.
3. 개인정보가 모니터 상에서 노출되지 않도록 자리를 이탈할 경우 로그아웃 또는 화면보호기를 실행하거나 활성화된 프로그램을 종료한다.
4. 공개된 장소의 게시판에 성명, 주민등록번호 등 개인정보를 게시하지 않는다.
5. 개인정보가 포함된 출력물은 반드시 복구·재생되지 않도록 문서세단기로 파기한다.
6. 사용자 ID와 비밀번호는 타인과 공유하지 않으며, 노출되지 않도록 안전하게 관리한다.
7. 개인정보 보호 요청에 적극 대응하며 신속하게 처리한다.
8. 어떠한 장소에 어떠한 방법으로도 호칭의 정보 및 자산을 보유하거나 저장하고 있지 않음을 확인한다.
9. 재직기간 중 취득한 호칭의 정보는 회사 후에도 제3자에게 누설하지 않는다.

20 년 월 일

직 종 : 소속부서 :

사 번 : 성 명 : (서명)



전출 및 퇴직 확인서

소속 :
사번 :
성명 :

상기 본인은 전출/퇴직으로 인하여 업무상 취득한 모든 정보자산과 호칭에서 지급받은 모든 장비 및 소프트웨어를 반납하고, 업무에 필요한 권한 및 책임에 대하여 인수자에게 모두 인계하였음을 확인합니다.

□ 확인 내용

구분	내용	확인자	비고
노트북			
업무시스템 계정			
메일			
외부 저장매체			
문서			
보안서약서			
업무 인수인계			

본인은 본 확인서가 퇴직 후에도 적용될 수 있음을 인식하고 있으며, 호칭에서 근무 중 숙지하였던 정보보호 규정에 따라 준수할 것을 동의합니다. 만약 위반하였을 경우에는 , "개인정보보호법" 등 관련법령에 의한 민·형사상의 책임 이외에도 호칭의 정보보호 규정에 따른 징계조치 등 어떠한 불이익도 감수할 것이며 호칭에 끼친 손해에 대해 지체 없이 변상 및 복구할 것을 동의합니다.

20 년 월 일

성명 : (서명/인)

● **외부자 보안**

외부인력 및 외주용역 활용 시 보안관리가 소홀하면 인적 관리 취약점으로 인한 보안사고가 발생할 수 있다. 그러므로 사전에 보안서약서 작성여부를 확인헤야하며, 전산장비 일체는 보안 담당자의 인가 후 반입/반출 될 수 있도록 한다. 작업용 PC는 유해사이트 접속을 차단해야 하며, 저장 자료를 완전히 삭제해야 한다.

● **한국선급 해상사이버보안 관리시스템 인증 검사항목(CSMS1)**

외부자 보안 (209.1) : 회사는 외부자에 의한 보안 사고를 대비하기 위한 외부자의 정보기술 장비, 데이터 등에 대한 보안정책을 수립하여야 한다.

외부자 보안(209.2) : 회사는 외부자와 계약 시 보안요구사항을 명시하고 사업기간 중 관리·감독에 관한 사항을 명시하여야 한다.

외부자 보안(209.4) : 외부자는 회사 보안요구사항을 준수하여 시스템을 사용하여야 하며 외부자 소유의 장비를 시스템에 연 결하는 경우 보안기능 검사를 사전에 실시하여야 한다.

용어 설명

- **GDPR :** 2016년 5월, 유럽연합(EU)은 디지털 단일 시장에서 EU 회원국간 개인정보의 자유로운 이동을 보장하는 동시에 정보주체의 개인정보 보호 권리를 강화하는 내용의 '일반 개인정보 보호법(General Data Protection Regulation)을 제정하였으며 2018년 5월 25일 발효되었다. GDPR은 기존 Directive와 달리 그 자체로 EU의 모든 회원국들에게 직접적인 법적 구속력을 가지며, GDPR 위반 기업에게 막중한 제재가 가해진다. (과징금 : 전세계 매출 4% 또는 2천만 유로)
- **스푸핑 :** 악의적인 네트워크 침입자가 자기자신의 식별정보(IP주소, DNS이름, MAC주소,포트)를 속여 다른 대상 시스템을 공격하는 기법을 의미한다. 임의의 웹 사이트를 구성해 일반 사용들의 방문을 유도하고, 인터넷 프로토콜인 TCP/IP의 구조적 결함을 이용해 사용자의 시스템 권한을 획득한 뒤 정보를 탈취 혹은 허가 받은 IP를 도용한다
- **스피어피싱 :** 특정 조직을 대상으로 시도되는 이메일이나 전자통신 사기를 말하며, 주로 허가받지 않은 사용자가 기밀 데이터에 접근하여 정보를 탈취하는 것을 목적으로 한다. 스피어 피싱은 일반적인 해커들에 의해 무작위적으로 이루어지기보다는 금전적 목적이나 무역 기밀 및 군사적 정보를 노리는 목적을 가지고 수행된다. 스피어 피싱을 예방하기 위해서는 송신자를 정확히 확인하고, 회신 URL이 믿을만하지 살펴보아야 하며, 패스워드 등 자신의 중요한 개인정보를 제공하지 않도록 주의한다.
- **스캠 :** 기업의 이메일 정보를 해킹, 거래처로 둔갑시켜서 무역 거래 대금을 가로채는 범죄 수법을 일컫는다. 피해 대상 기업에 악성코드를 감염시킨 후 업체가 지불 결제 방식을 바꾸도록 유도한다. 스케머는 이메일 해킹으로 거래업체 간 주고 받는 내용을 지켜보다가 송금과 관련된 내용일 있을 때 주요 거래처가 메일을 보낸 것처럼 속이고 바뀐 계좌 정보를 보내 거래 대금을 빼돌린다.