[별지 제3호서식]

국외출장 보고서

1. 출장개요

<table>
<tr><td>출장목적</td><td colspan="8">해외선진사례 벤치마킹을 통해 개인정보보호 정책 파악 및
개인정보 통합관제를 발전 시키고자 함</td></tr>
<tr><td>출장동기
및 배경</td><td colspan="8">글로벌 정보보안 및 개인정보보호 정책(EU GDPR),
환경 변화에 대한 최신 동향과 트랜드 파악을 위함</td></tr>
<tr><td>출장기간</td><td colspan="8">2018. 11. 12. ~ 2018. 11. 18.(7일간)</td></tr>
<tr><td>출장국
(지역)</td><td colspan="8">영국(런던)</td></tr>
<tr><td>방문기관</td><td colspan="8">다크트레이스 본사, Cyber Security Summit & Expo 등</td></tr>
<tr><td rowspan="6">출장자</td><td rowspan="2">소 속</td><td rowspan="2">직급</td><td rowspan="2">성명</td><td rowspan="2">성별</td><td rowspan="2">연령</td><td rowspan="2">출장중
담당업무</td><td colspan="2">출장경비</td></tr>
<tr><td>금액</td><td>부담기관</td></tr>
<tr><td rowspan="4">개인정보
통합관제센터
운영총괄부</td><td>2급</td><td>김○○</td><td>남</td><td>53</td><td>선진사례 벤치마킹
총괄</td><td></td><td></td></tr>
<tr><td>고급</td><td>정○○</td><td>남</td><td>45</td><td>GDPR 등 EU
개인정보 동향 파악 등</td><td></td><td></td></tr>
<tr><td>중급</td><td>이○○</td><td>여</td><td>28</td><td>통합관제 관련
발전방향 수렴</td><td></td><td></td></tr>
<tr><td>초급</td><td>송○○</td><td>여</td><td>29</td><td>영국 내 정보보호
및 보안 동향 파악</td><td></td><td></td></tr>
<tr><td>경영혁신부</td><td>대리</td><td>박○○</td><td>여</td><td>36</td><td>정보원 소개 및
관련자료 배포 등</td><td></td><td></td></tr>
<tr><td>동행
기관명 및
인원</td><td colspan="8">해당사항 없음</td></tr>
</table>

2. 출장일정

월/일 (요일)	출발지	도착지	방문기관	업무수행내용
11.12.(월)	한국(인천)	영국 런던(히드로)	-	-
11.13.(화)	Glucester Road (숙소)	London Stland Grand Building	-	행사참여 및 회의 사전 준비
11.14.(수)			다크트레이스 본사	인공지능과 머신러닝 이론에 기초한 탐지 엔진을 사용한 악성 공격자 및 자동화된 툴에 의한 정보유출 등 범죄시도를 막기 위한 'Darktrace Enterprise' AI 사이버 방어 솔루션 시연, EU GDPR(General Data Protection Regulation) 관련 논의, Directive(EU법 규정) 이후 인터넷 기술과 관련 서비스 운영 현황
11.15.(목)	Glucester Road (숙소)	London Business Design Centre	Cyber Security Summit & Expo	영국 사이버 보안 전략, 사이버 위험 노출, ePrivacy에 관한 규정, GDPR 진행사항, 장기적 GDPR 전략 전시 부스 탐방: Aruba, Crest, Business Info, DARKTRACE, CybSafe, Deloitte, e2e Assure Limited, Global Legal Group, H-ISAC INC, Information and Records Management Society, Institute Information Security Professionals, IT Governance Ltd, Symantec
11.16.(금)	-	-	-	출장결과 정리 및 내부 논의
11.17.(토) ~18.(일)	영국 런던(히드로)	한국(인천)	-	-

3. 업무수행내용(주요 회의결과 등)

□ 다크트레이스 본사 방문 및 통합관제 관련 회의

○ 주요 기술

- 네트워크 기반의 로그(기록)을 기반으로 관제 수행
- 인공지능, 비지도 학습[1]의 머신러닝 및 베이지안 수학[2]이론에 기초한 탐지 엔진 사용 (시그니처와 룰에 의존하지 않음)
- 비정상 징후, 행위의 데이터 흐름에 대한 실시간 학습 및 탐지

○ 유출 감지 사례

- 거의 접속하지 않는 서버에서 접속한 사용자가 사설 클라우드에 정보주체의 개인정보를 저장 감지
- 기존에 접속하지 않았던 PC에 접속한 사용자를 분석, 사용자 ID공유 감지
- 평소에 개인정보를 조회하지 않은 사용자가 개인정보를 조회하여, 내부유출 여부 확인

□ Cyber Security Summit&Expo

○ 최신 사이버 공격(낫페트야, 워너크라이 등) 동향

- 낫페트야(NotPetya)* 공격을 받은 조직의 경우, 약 2억 5,000만~3억 달러의 비용손실을 겪었으며, 최대 3억 1,000만 달러 이상의 비용이 발생한 경우도 있었음

*낫페트야:바이러스 감염 시 마스터 파일 테이블을 암호화 하고 파일을 돌려주는 대가로 비트코인 보상금을 요구하는 공격방법

- 150개국 30만대 이상의 컴퓨터에 영향을 준 워너크라이(WannaCry)* 공격으로 인한 전 세계 손실 비용은 약 80억 달러로 추산

*WannaCry: 사용자의 중요 파일을 암호화한 뒤 이를 푸는 대가로 금전을 요구하는 랜섬웨어의 일종

---

1) 비지도 학습(Unsupervised Learning): 기계학습의 일종으로 데이터가 무작위로 있을 때 규칙성 등을 찾는 클러스터링 알고리즘

2) 베이지안 수학(Bayesian mathematics): 추리통계의 한 방법으로, 수리통계 및 사전정보를 이용하여 사후확률을 구함

○ 사이버 레질리언스 관점에서의 보안이슈

- 3대 보안위협: 속도(Velocity), 복잡성(Complexity), 책임(Liability)
- 사이버 공격이 점점 진화에 따라 피해는 나날이 증가하므로 사이버 레질리언스의 이해와 전략적 대응 필요하며, 사이버 장애, 파괴, 위협, 리스크로부터 벗어나 비즈니스 연속성 유지 필요

○ 글로벌화 되어가는 공급망(Supply Chain) 운영과 같이 복잡성과 불확실성이 큰 환경에서 사이버 공격, 보안침해사고는 조직에 매우 큰 타격을 미칠 수 있음

☞ 이에 효과적 대응을 위해 조직은 정보보안, 비즈니스 연속성, 조직의 레질리언스 등을 결합한 사이버 레질리언스에 대한 사전 예방적이고 통합적 접근방식을 취할 필요성 증대

□ EU GDPR 회의

○ Directive(EU 법 규정)이후 인터넷 기술과 관련 서비스 환경변화를 반영

○ 공표일자 : '16.5.4, 발효일자 : '18.5.25

※EU에 진출하였거나, 희망기업은 GDPR내 보호 조치 마련

○ 4년간의 합의과정, 3,000건 이상의 수정안 제출

○ 적용범위 확대, 정보주체의 권리 확대, 막대한 처벌규모

○ Directive는 각 회원국에 대한 입법, 지침, 가이드라인의 역할

○ EU 회원국 개별 입법으로 국가간 법령차이 존재

○ 별도의 입법 행위 불필요

○ 모든 EU 회원국에게 직접 적용

※ 회원국가의 상이한 제도를 단일 형태로 통합하고 보다 강력한 규제를 시행할 것으로 예상

☞ 법인이 EU내 설립한 경우는 물론, EU거주자에게 제품 서비스를 제공하는 경우, EU거주자의 행동을 모니터링 하는 경우에도 적용

4. 출장성과 · 시사점 및 향후 업무 활용계획

□ 통합관제 활용 방안

○ 개인정보 통합관제에서 분석하는 로그는 개인정보를 처리한 로그로서 표준화 된 접속기록이나, 다크트레이스가 분석하는 로그는 네트워크상 로그로 분석 대상이 상이

○ 통합관제의 표준 접속기록을 바탕으로 룰 탐지기반이 아닌 머신러닝 기법을 이용한 개인정보 오남용 분석이 가능한지 방안 검토 예정

○ 사이버 공격 진화 및 글로벌화에 따른 피해가 발생하지 않도록 사이버 레질리언스(Cyber Resillence) 이해를 통한 전략적 대응 방안 강구 예정

○ EU GDPR과 관련하여 Directive 이후, 적용범위 확대 방향을 지속적 모니터링하고, 통합관제 대상에 포함여부를 모니터링 예정

○ 2018년 보건복지부 소속 및 산하기관 개인정보보호 책임자(CPO) 워크숍에서 참석자 100여명을 대상으로 시연 및 설명회 실시로 실시간 관제 의견 수렴

○ 실시간 관제시스템 도입에 대한 지속적인 논의를 하고, 관련 기술동향 등을 모니터링 및 계속적으로 효율적 관제에 대한 방안을 논의(필요 시, 실제 적용기관 추가방문 예정)