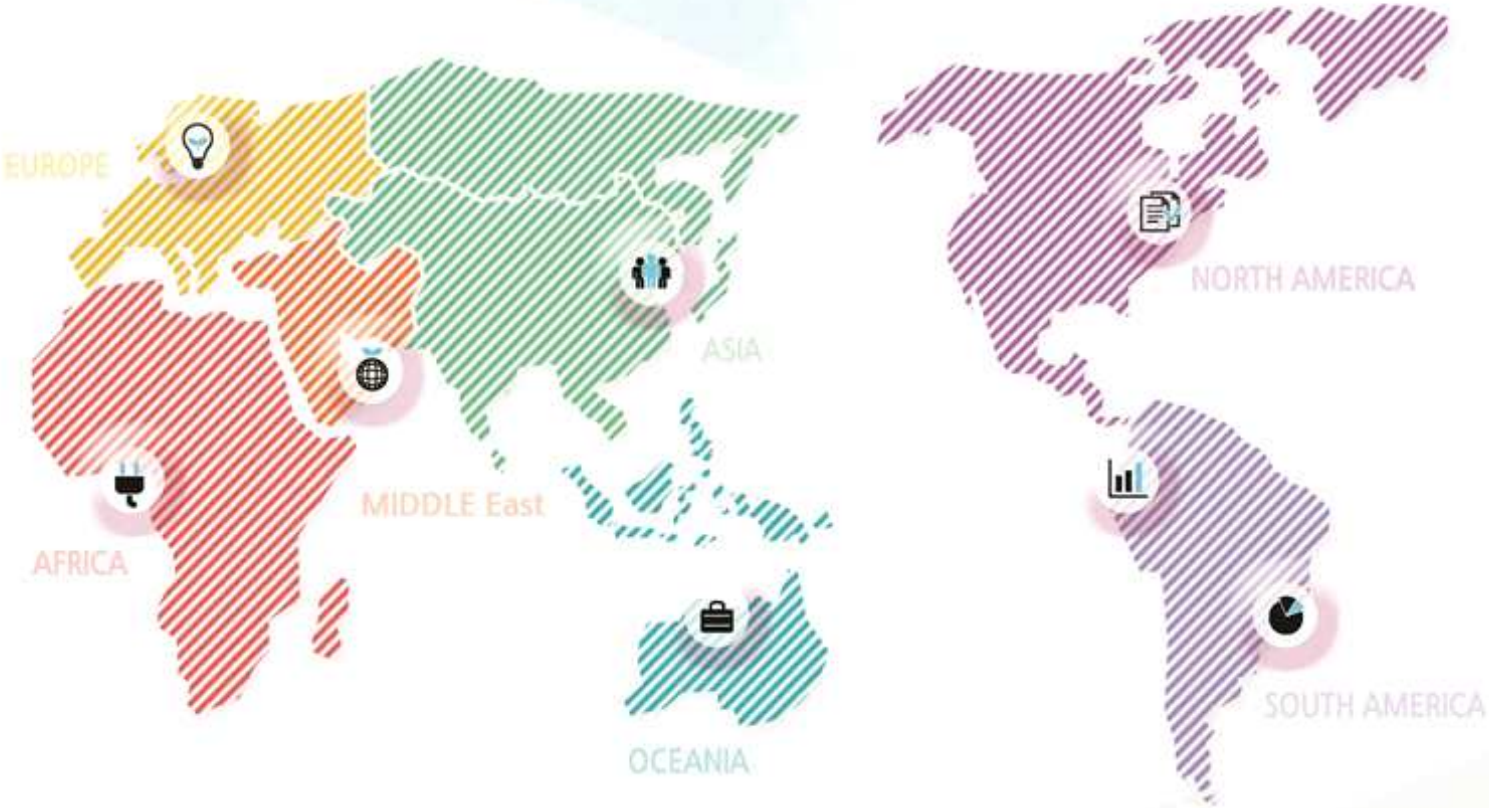
Global Market Report 15-030
2015.07.29



무역사기 발생 현황 및 대응책

kotra
Korea Trade-Investment Promotion Agency

CONTENTS

목 차

요 약 / 1

1. 무역사기 발생 개황 2

2. 지역별 발생 현황 3

3. 유형별 특징 및 대처법 6

[참고자료] 유형별 무역사기 사례

[1] 국제입찰을 도와주겠다는 사기꾼 11
[2] 원부자재 공급을 미끼로 선금 수수료만 챙기고 잠적 12
[3] 위조수표와 맞바꾼 상품 12
[4] 독일 이미지를 이용한 무역사기 13
[5] 10년 바이어를 갈라놓은 이메일 해킹 14
[6] 이메일 해킹 피해를 한국 업체가 보상하라는 바이어 15
[7] 헝가리 계좌의 인출을 막아 주세요 16
[8] 알제항에서 오도 가도 못하게 된 상품 17
[9] 도착한 컨테이너에 쓰레기만 가득 18
[10] 저금리대출을 미끼로 선수금을 노린 사기 19

요 약

최근 인터넷의 발달과 함께 이메일 해킹을 통한 무역사기 사례가 급증하면서 그렇지 않아도 수출 부진으로 고전하는 우리 무역업계를 긴장시키고 있다. 나날이 진화하면서 장소를 가리지 않고 발생하는 무역사기에 효과적으로 대응하기 위해 KOTRA 해외 전 무역관을 동원하여 무역사기 사례를 조사하고 그 특징을 동 보고서에 담았다.

동 조사에서 파악된 최근 3년 동안의 무역사기 건수는 모두 530건이었다. 이는 KOTRA 해외무역관이 분명하게 인지하고 있는 사례만 포함한 것으로 실제 발생하였을 것으로 추정되는 무역사기는 동 수치의 3~5배에 이르는 2,000건 내외로 추정된다. 이와 함께 우리 기업이 입고 있는 피해 규모도 연간 1천억 원에 달할 것으로 예상된다.

무역사기가 가장 많이 발생하고 있는 지역은 아프리카로 나이지리아, 가나, 토고, 베냉 등을 중심으로 집중적으로 발생하고 있다. 이들 아프리카 지역에서 오는 거래 제의에 대해서는 일단 무역사기의 가능성을 염두에 두고 대처하는 것이 바람직해 보인다. 이번 조사에서 드러난 또 하나 재미있는 사실은 선진국이 모여 있는 유럽이 아프리카에 이어 두 번째로 무역사기가 많은 지역이라는 점이다. 선진국의 이미지를 무역사기에 활용하려는 경우들이 많았다. 그리고 중국에서 시도되는 무역사기는 다른 지역에 비해 훨씬 지능적이고 복잡한 형태를 띠고 있고, 일본과 대양주의 호주, 뉴질랜드에서는 단 한 건의 무역사기 사례도 보고되지 않아 무역사기 청정지역으로 분류되었다.

유형별로는 주로 아프리카에서 많이 발생하는 서류위조와 로비자금이나 수수료 등 금품 사취가 많았다. 하지만 아프리카 지역을 제외할 경우에는 이메일 해킹을 통한 무역 사기가 가장 많았으며, 유럽을 비롯한 거의 모든 지역에서 광범위하게 발생하고 있어 각별한 주의가 필요해 보인다.

무역사기는 당했을 경우 기업의 생존을 위협하는 심각한 범죄이지만 대부분 아주 간단한 확인만으로도 예방이 가능하다는 특징이 있다. 따라서 의심나는 사항을 바로 바로 확인하는 것이 중요하다. 해외 현장 확인이 가능한 KOTRA를 적극 활용할 필요가 있다. 무역사기가 나날이 진화하면서 우리 기업을 노리고 있다. 관련 정보를 공유하고 효과적인 대처법을 찾는 노력이 어느 때 보다 중요하다.

1. 무역사기 발생 개황

□ 최근 3년 우리기업을 대상으로 한 무역사기 530건 발생

o 동 수치는 2015년 6월 KOTRA가 해외 123개 무역관을 대상으로 조사한 것으로 무역관 직원이 구체적으로 인지하고 있는 사례만 포함

– KOTRA에 신고 되지 않은 사례까지 포함할 경우, 실제 발생 건수는 동 수치의 3~5배 규모로 추정

– 또한 우리기업의 피해규모는 연간 1,000억 원에 달할 것으로 추정됨

□ 아프리카, 유럽 순으로 많이 발생

o 전체 발생 건수의 41.7%인 221건이 아프리카에서 발생

– 2위 발생 지역은 104건이 보고된 유럽이 차지하였고, 그 다음으로는 중국, 중동, 서남아 순으로 많이 발생

– 일본은 해당지역 4개 무역관이 인지하는 무역사기는 한 건도 보고되지 않을 정도로 무역사기 청정지역으로 분류됨

< 최근 3년 지역별 무역사기 발생건수 >

(단위 : 건, %)

지역	아프리카	유럽	중국	중동	서남아	동남아	CIS	북미	중남미	일본	합계
발생건수	221	104	63	39	32	26	17	15	13	0	530
비중	41.7	19.6	11.9	7.4	6.0	4.9	3.2	2.8	2.5	0	100

주 : KOTRA 해외무역관이 인지하고 있는 사례만 포함 (실제 발생건수는 3~5배 규모로 추정)

o 최다 발생 국가는 나이지리아, 20건 이상 발생 국가는 6개국으로 조사됨

– 나이지리아(100건), 가나(100), 중국(63), 영국(26), 방글라데시(21), 이라크(20)

□ 유형별로는 서류위조, 금품사취, 결제관련, 이메일 해킹 순으로 많이 발생

– 최근 급증하고 있는 신종 수법인 이메일 해킹을 통한 무역사기는 전 세계에서 광범위하게 발생 중이며, 피해도 심각한 상황

2. 지역별 발생 현황

< 최근 3년 지역별 무역사기 발생현황 >

유형 / 지역	서류위조	금품사취 (로비자금, 수수료)	결제관련	이메일 해킹	선적관련	기타	합계
아프리카	100	70	25	3	12	11	221
유럽	8	8	16	25	10	37	104
중국	2	20	9	5	12	15	63
중동	5	15	3	8	0	8	39
서남아	1	0	17	3	8	3	32
동남아	8	3	2	9	2	2	26
CIS	2	3	6	2	1	3	17
북미	0	0	4	5	3	3	15
중남미	0	0	1	11	0	1	13
일본	0	0	0	0	0	0	0
합계	126	119	83	71	48	83	530

□ **(아프리카)** 전 세계 발생 건수의 41.7%인 221건이 발생하였으며, 나이지리아, 가나, 토고, 베냉 등지에서 집중 발생

o 아프리카가 우리나라 전체 수출에서 차지하는 비중이 1.8%에 불과한 점을 감안한다면 무역사기 발생빈도는 타 지역에 비해 비교할 수 없을 정도로 높은 것이 현실

– 파악이 어려운 건수들을 포함할 경우 실제로는 매년 100건 이상의 무역사기가 발생 중일 것으로 추정됨

* 아크라(가나)무역관장은 무역사기 문의가 하루에 2~3건씩 속출하고 있다고 밝힘

– 나이지리아(100건), 가나(100), DR콩고(10), 남아공(4), 케냐(4) 순으로 많이 발생

o 유형별로는 서류위조를 통한 무역사기 사례가 100건으로 가장 많았으며, 로비자금, 수수료 등 금품사취 사례도 70건을 차지

□ **(유럽)** 전 세계 발생 건수의 19.6%인 104건이 발생하였으며, 서유럽 선진국의 신뢰도를 이용하는 경우가 많았음

o 영국, 독일, 네덜란드 등 서유럽 선진국에 사업장이 있는 것처럼 서류를 조작하는 경우가 많음

– 존재하지 않는 주소를 사업장으로 명기하는 경우가 많고(Google 지도로 사전 확인 가능), 알리바바 등 전자상거래 사이트를 무대로 활동

– 영국(26건), 헝가리(18), 독일(13), 폴란드(8), 이탈리아(7) 순으로 많이 발생

o 유형별로는 이메일 해킹이 25건으로 가장 많았으며 10개 지역 중에서도 최고 수치를 기록

□ **(중국)** 홍콩 및 타이베이를 포함해 모두 63건이 발생하여 전체 건수의 11.9%를 차지

o 사기 수법이 타 지역에 비해 지능적이며, 무역 분쟁을 염두에 두고 진행하는 복잡한 사례들이 많음

* 홍콩 회사의 광저우·선전 지사라고 속인 뒤 홍콩 개인계좌로 입금을 요구하는 경우, 불충분한 계약서 내용 등 계약서의 빈틈을 악용하는 사례 등

– 중국 내 지역별로는 시안(20건), 상하이(12), 정저우(10), 홍콩(9) 순으로 조사됨

o 유형별로는 로비자금, 수수료 등의 금품사취(20건)가 가장 많았고, 선적 관련(12), 결제관련(9)이 뒤를 이음

□ **(중동)** 재건 시장이 형성되고 있는 이라크를 중심으로 기승을 부리고 있으며, 상업 중심지인 두바이에서도 다수 발생

o 로비자금, 수수료 등 금품사취 사례가 많고 최근 들어 이메일 해킹 사례가 급증 추세

– 국가별로는 이라크(20건), UAE(6), 이스라엘(3), 사우디아라비아(3) 순으로 조사됨

o 유형별로는 로비자금, 수수료 등의 금품사취(15건)가 가장 많았고, 이메일 해킹(8), 서류위조(5)가 뒤를 이음

□ **(서남아)** 방글라데시와 파키스탄을 중심으로 대금결제와 관련된 사기가 많음

o 은행직원 연루, 샘플과 실제 선적 물품의 상이 등 후진국형 사기가 많음
  – 방글라데시(21건), 파키스탄(6), 인도(3), 스리랑카(2) 순으로 발생

o 유형별로는 결제관련(17건)이 가장 많았고, 선적관련(8), 이메일 해킹(3)이 뒤를 이음

□ **(기타 지역)** 동남아, CIS, 북미, 중남미, 일본 순으로 발생

o 중남미와 동남아, 북미의 경우 이메일 해킹의 발생 비중이 높았으며, 서류위조(동남아), 결제관련(CIS) 사기도 다수 조사됨

o 일본 및 대양주의 경우, 해당지역 무역관에서 인지되는 무역사기 사례가 전혀 없을 정도로 무역사기 청정지역으로 조사됨

< 최근 3년 무역사기 발생 10대 국가 >

순위	국가명	발생건수	최다 발생 유형 2가지
1	나이지리아	100	금품사취, 서류위조
2	가나	70	금품사취, 서류위조
3	중국	63	금품사취, 선적관련
4	영국	26	이메일 해킹, 선적관련
5	방글라데시	21	결제관련, 선적관련
6	UAE	20	이메일 해킹, 서류위조
7	이라크	20	금품사취, 서류위조
8	헝가리	18	이메일 해킹, 기타
9	독일	13	금품사취, 서류위조
10	DR콩고	10	서류위조, 결제관련
10	미국	10	이메일 해킹, 결제관련

3. 유형별 특징 및 대처법

< 최근 3년 유형별 무역사기 발생현황 >

유형	발생건수	주요 발생 국가 (건수)
서류위조	126	나이지리아(50), 가나(40), DR콩고(7), 필리핀(6), 네덜란드/독일/이라크(3)
금품사취 (로비자금, 수수료 등)	119	가나(40), 나이지리아(30), 중국(20), 이라크(15), 독일(4)
결제관련	83	가나(20), 방글라데시(15), 중국(9), 영국/스웨덴/루마니아(4)
이메일 해킹	71	폴란드(8), 영국/이탈리아/미국/중국(5)
선적관련	48	중국(12), 영국(5), 파키스탄(4), 방글라데시/불가리아(3)
기타	83	중국/헝가리(15), 독일(9), 영국(7), UAE(3)

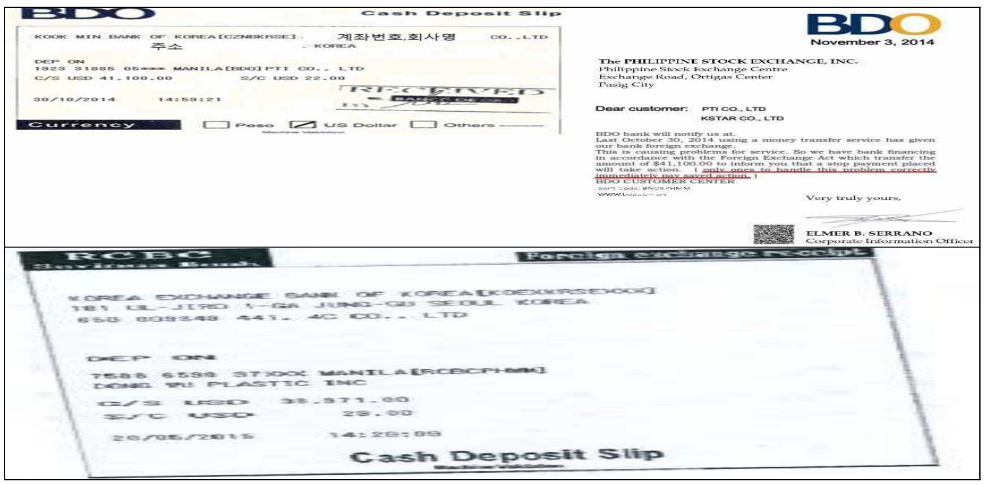
□ 서류위조

o (특징) 오래 전부터 행해져 왔던 사기 유형으로 사업자등록증, 품질보증서, 수출업체증명서, 신분증, 여권 등의 서류를 위조하여 사기에 이용

– 필리핀, 말레이시아 등 동남아 지역에서는 송금영수증, 송금지연 양해공문, 지급보증서류와 같은 은행 서류를 위조하는 경우도 있음

* 필리핀 마닐라무역관에는 위조된 송금영수증을 보내주면서 상품 선적을 유도하는 사기 사례가 2013년 이래 6건이 접수됨

< 필리핀 은행 관련 서류 위조 사례 >



o (대응방법) 신규 거래선에 대해서는 현지 상공회의소 등록 여부를 반드시 확인하고(대부분 인터넷으로 무료 확인 가능), 거래선이 보내온 각종 서류를 꼼꼼히 살피고 의심스러운 부분에 대해서는 반드시 발급 기관을 접촉하여 확인하거나 KOTRA 해외무역관을 통해 현지 실사 추진

□ 로비자금, 수수료 등 금품사취

o (특징) 서부아프리카, 중국에서 발생 빈도가 높은 무역사기 유형이며, 로비자금, 변호사 선임비용, 은행보증료, 공증비, 활동비 등 사취하려는 비용의 종류가 다양

* (말레이지아) 개발 프로젝트 관련 은행보증비용 분담요구
* (나이지리아) 국제입찰 관련 수수료(약 5만 달러) 납부 요구
* (스페인, 중국) 공증수수료 전체 또는 일부 분담 요구

– 국제기구 직원을 사칭하고, 홈페이지까지 만들어 접근할 정도로 사기 수법이 치밀함. 주로 국제입찰, 원부자재 공급 등 기대 수익이 큰 대규모 프로젝트 추진에 필요한 적은 비용을 요구하기 때문에 유혹에 넘어가기 쉬움

* (나이지리아) NDDC(Niger-Delta Development Commission), ECOWAS(Economic Community of West African Sttes) 등 국제기구 직원을 사칭하면 접근하는 경우가 많음

o (대응방법) 현지 고위층과의 친분을 이용하여 국제입찰을 지원하겠다거나 각종 현지 활동을 핑계로 선수금을 요구하는 경우는 무역사기의 가능성이 크므로 철저한 신뢰도 확인 후 거래 추진 필요

□ 결제 관련

o (특징) 타 유형과 비교할 때 결제와 관련된 무역사기는 지역별로 고르게 발생하고 있으며, 유령기업임을 모르고 계약을 체결하거나 경영이 악화된 바이어가 의도적으로 결제를 회피하는 경우도 있음

– 구체적인 계약서 없이 단순 인보이스, B/L, 영수증만으로 거래를 진행하였다가 발생하는 결제 미이행 사례, 비교적 안전한 L/C 거래에서도 사기 사례가 보고되고 있음

* (러시아) 서신이나 이메일은 법적 효력이 없고 해외 송금을 담당하는 은행에서 인정하지 않으므로 반드시 계약을 체결하고 거래를 해야 함

* (방글라데시) L/C를 개설했음에도 현지의 관행 및 절차임을 주장하며 개설은행이나 바이어가 의도적으로 대금지급을 지연시킴

– 방글라데시, 중국 상하이, 모로코, 미국 디트로이트에서 많은 사례가 보고되고 있음

o (대응방법) 신용조사를 철저히 함으로써 유령기업, 파산직전 기업과의 거래를 피하여야 하며, 자체적인 신용조사가 어려울 경우, KOTRA 해외무역관에 도움을 요청하는 것이 필요함. 또한 의심 가는 거래선과의 거래가 불가피할 경우에는 무역보험 가입을 적극 고려

□ 이메일 해킹

o (특징) 인터넷 및 모바일을 통한 비즈니스 활성화에 따라 최근 발생 빈도가 급증세에 있고, 무역사기 다발 지역인 아프리카를 제외하고 분석할 경우 전 세계적으로 가장 많이 발생하고 있는 무역사기 유형

– 인터넷 해킹을 통해 결제은행을 변경 통보하는 방법으로 결제대금을 가로채는 방법이 대표적이며, 사기에 걸려들 경우 피해가 즉각적이고 대규모라는 특징이 있음

– 단, 비슷한 방법이 반복적으로 시도되므로 사례 전파 등 사전 교육을 통해 예방이 가능

– 유럽, 중동, 중남미, 동남아, 북미 등 전 지역에서 광범위하게 발생

< 해커들이 사용하는 주요 표현들 >

* (불가리아) 감사로 기존 계좌로의 송금이 안 되니 새로운 중국계좌로 송금해 달라
* (홍콩) 내부감사로 입금계좌를 부득이하게 홍콩 H은행 계좌로 받아야 하니 협조 바람
* (칠레) 기존 국내계좌가 한국정부의 감사를 받고 있으니 중국계좌로 입금해 달라

o (대응방법) 거래처와의 계좌변경, 거래 내용 변경을 통보할 때는 이메일과 함께 반드시 유선으로 확인이 필요하며 바이어와 공동으로 대처하는 것이 중요. 또한 보안이 취약한 대규모 포털 이메일보다는 회사 자체 이메일을 사용하는 등 이메일 보안을 강화하는 것이 필요

□ 선적 관련

o (특징) 대부분 수입과정에서 발생하며, 터무니없이 낮은 가격으로 제공하겠다고 속이거나 약속과 다른 품질의 상품을 선적하는 사례가 많음

– 샘플과는 달리 저급한 품질의 상품을 고의로 선적하거나 심지어 상품이 아닌 쓰레기를 보내는 경우도 있음

* (인도 뭄바이) 계약과는 다른 재질의 파이프를 납품받아 환불을 요청하였으나 거래 상대방이 모르쇠로 일관했고, 결국 40% 금액만 환불 받음

* (파키스탄 카라치) 상품을 컨테이너에 싣는 사진을 믿고 물품을 보냈으나, 실제는 극히 일부가 계약물품이었고 나머지는 산업쓰레기였음

– 중국, 아프리카, 유럽, 서남아시아에서 주로 발생

o (대응방법) 터무니없이 낮은 공급가격에 대해서는 특별히 조심하여야 하며, 지역에 따라서는 현지 출장을 통해 선적 과정에 대한 실사를 진행하는 것이 필요

□ 기타 사례

주요 사례	발생국가
EuroBank라는 유령 은행의 신용장을 활용한 물품 사취사기	아제르바이잔
원부자재를 공급해 줄 것처럼 하면서 보험금 및 선급금 사취 시도	우크라이나
폐업한 독일 회사의 명의를 도용하여 폴란드 계좌로 송금 요구	독일
현지 유명기업 퇴직 직원이 한국기업 속여 대금 수취	대만
저금리대출을 미끼로 선수금을 요청	UAE
화물인수를 지연시키면서 화물보관료, 통관사고용비 등을 지급하도록 유도	이라크

< 무역사기 방지 5계명 >

1. 기본정보 확인을 빼먹지 마라
   - 무역사기의 90% 이상은 거래 전 상대방에 대한 간단한 정보의 확인만으로 예방된다. KOTRA 해외무역관, 현지 상공회의소 등을 적극 활용하라
2. 평소와 다르면 2중 3중으로 확인하라
   - 계좌번호 변경 등 바이어가 평소와 다른 연락을 해 오면 반드시 전화를 걸어 확인하라. 최근 극성을 부리는 이메일 해킹이 방지된다
3. 좋은 조건의 첫 거래를 조심하라
   - 일면식도 없는 바이어가 터무니없이 좋은 조건을 제시하거나 과도한 선수금을 요구해 온다면 무역사기의 함정일 가능성이 크다. 철저하게 확인하고 진행하라
4. 바이어 국적으로 신뢰도를 판단마라
   - 선진국에서 온 편지라고 해서 쉽게 믿어서는 안 된다. 신뢰도 높은 선진국 기업을 가장한 제3국인의 무역사기 가능성에 철저히 대비하라
5. 어려울 때일수록 무역사기에 조심하라
   - 무역사기는 내가 어려울 때를 노린다는 점을 명심하라

첨부 유형별 무역사기 사례

[1] 국제입찰을 도와주겠다는 사기꾼

□ 사기유형 : 로비자금, 수수료 등 금품사취
□ 발생지역 : 나이지리아
□ 발생시기 : 2015년 4월
□ 피해금액 : 없음
□ 내용

국내에서 기계류 부품을 제조, 초보 수출 중인 A사의 김 대표는 약 2개월 전 나이지리아로부터 한 통의 이메일을 받고 깜짝 놀랐다. 본인을 나이지리아 니제르델타 경제개발기구(NDDC, Niger-Delta Development Commission)의 직원이라고 소개한 바이어는 A사를 알리바바에서 알게 되었고 자기들이 찾는 적격업체라고 표현하면서 3개월 이내에 A사가 생산하는 기계 부품 10만 개(FOB가격 기준 50만 달러 상당)를 입찰에 부칠 예정이라는 정보였다. 바이어는 NDDC 직원증(가짜) 및 구매계획서 스캔본(가짜)을 이메일로 보내고 지불은 계약 시 50% T/T 선불, 나머지는 선적 후 50% 지불하겠다고 밝혀왔다.

A사는 일면식도 없는 바이어가 초도 물량치고는 너무 과한 오퍼를 해온 것에 의심하였으나, 밑져야 본전이라는 생각으로 P/I를 발행하는 등 구체적인 회신을 주고받았다. 게다가 일반 바이어도 아닌 국가기관 소속이라는 말에 가뜩이나 수출 마케팅에 어려움을 겪던 중 큰 은인이라도 만난 듯한 말투로 감사를 표하기도 했다.

그러나 이때부터 바이어 측 얘기는 조금씩 바뀌기 시작했고 내부적으로 결재를 받는 데에 시간이 걸려 주문 자체가 늦어지니 기다려 달라고 했다.

그러던 어느 날, 선금 50%를 A사 계좌로 송금하였으니 확인하라는 이메일을 받고 1주일 내내 거래은행에 확인하였으나 수신 내역이 없어 바이어에 확인하게 되었다. 바이어 측은 자기들이 알아보니 나이지리아 은행에서는 송금이 되었으나 자금이 현재 폴란드 모 상업은행에 머물러 있다고 했다. 그러면서 이러한 송금 지연 사태를 조속히 해결하기 위해서는 먼저 자기들 내부 규정상 필요한 수수료(약 5만 달러 규모)가 필요하다는 의견을 보내왔다.

이 상태에 이르자 A사는 아무래도 미심쩍어 KOTRA 라고스 무역관에 문의해 왔고, 무역관에서는 이 건이 사기사건임을 현지에서 확인, A사에 통보하게 되었다.

A사는 다행히 금전적 피해를 보기 직전 막을 수 있었기에 감사 표시하였다.

[2] 원부자재 공급을 미끼로 선금 수수료만 챙기고 잠적

□ 사기유형 : 로비자금, 수수료 등 금품사취
□ 발생지역 : 러시아
□ 발생시기 : 2015년 6월
□ 피해금액 : US$ 5,600
□ 내용

국내기업 A사(ABW Korea Co.)는 러시아의 대형 석유기업인 Rosneft사를 사칭한 러시아 사기기업으로부터 석유 수입 관련 오퍼를 받았다. A사는 지속적으로 메일로 교신을 해오다 제품 선적(컨테이너 4대분) 관련 선금 50%에 해당하는 5,600달러를 송금하였으나, 러시아 기업 측에서는 송금을 받은 이후 연락을 두절한 상황이다.

무역관에서는 국내업체가 송부해 준 이메일을 분석한 결과, 러시아 기업의 연락처의 경우 여러 대형기업의 연락처를 섞어서 만든 거짓 연락처였으며, 기업의 홈페이지 또한 외국기업에 사기를 치기 위해 가짜로 만들어놓은 것으로 분석됐다.

참고로 러시아의 석유 수출은 국가가 직·간접적으로 관여하는 가운데 대형 글로벌 외국기업에만 공급하는 것이 일반적이고, 중견·중소기업 또는 원유 수입중개상을 통해 공급하는 경우는 없다.

[3] 위조수표와 맞바꾼 상품

□ 사기유형 : 서류위조
□ 발생지역 : 가나
□ 발생시기 : 2015년 3월
□ 피해금액 : US$ 18,867
□ 내용

한국 H사는 2015년 초 가나의 Vertifx Technology Inc.로부터 상품을 수입하고 싶다는 인콰이어리를 접수했다. 계약체결 후, V바이어는 JP모건 은행의 위조된 Swift Code로 결제했으며, H사는 자금 입금을 확인하지 않은 채 상품(US$16,850)을 V에게 발송했다. 또한, 이 과정에서 V바이어는 국내의 H사에 일부제품의 품질문제를 제기하며 강하게 불만을 제기해 2,017.81달러를 환불(은행으로 송금) 받기도 했다.

H사의 문의를 받은 무역관이 V사에 연락을 시도했지만, 이 회사는 전형적인 '사기꾼 그룹(신디케이트)'으로 활동하는 유령기업으로 판단됐다. 무역관은 현지 경찰에 이 사건을 신고했으나 수개월이 지난 현재까지 경찰 측으로부터 어떠한 연락도 받지 못하고 있다.

[4] 독일 이미지를 이용한 무역사기

□ 사기유형 : 서류위조
□ 발생지역 : 독일
□ 발생시기 : 2014년 7월
□ 피해금액 : 없음
□ 내용

A사는 2014년 7월 말 독일의 F사와 복사지 수입을 위해 협상하던 중, F사에서 계약액의 50%를 T/T 송금을 요청해온바, 이에 대해 함부르크 무역관에 문의하였다. 첫 거래인데 선송금을 요청하였다는 사실에 무역관 담당자는 A사에 송금하지 말 것을 당부하는 한편, F사에 대한 자료를 넘겨받아 조사를 시작하였다.

F사의 수출업체증명과 품질 보증서를 확인하여 보니 몇 가지 이상한 점이 발견되었다. 해당 문서가 독일 관청에서 발급되었음에도 독일어로 작성되어 있지 않은 점, 또한 <그림>의 왼쪽 문서 하단에 독일어가 아닌 불어로 작성된 점과 오른쪽 문서 직인의 "Federal" 철자와 직인 밑의 이름에서 Last Name의 철자가 틀린 점 등이 사기의 가능성을 높였다. 해당 문서에 나와 있는 사업자등록 번호를 독일 상업등기소에 조회하여 보았으나 확인이 되지 않았다. 또한 A사에 건네준 전화번호도 없는 번호로 확인되었다.

A사에서 선송금을 하지 않자 해당 사기 의심업체는 A사에 재차 시일 내 송금을 재촉했고, A사에서는 첫 거래이기 때문에 F사의 신뢰도를 먼저 확인해야 한다는 이메일을 보냈다. F사는 즉각 자신들의 인터넷 홈페이지에 있는 선사로 확인을 해보라는 메시지를 보내왔다. (www.fortunepaper.comxa.com)

홈페이지상의 선사 전화번호로 무역관에서 전화를 해보니 물류나 선사와는 전혀 관계없는 가정집이었다. 또한, 해당 홈페이지의 주소가 www. OOOOO.de로 끝나지 않는 점, 그리고 F사 담당자의 이름이 독일 이름이 아니었으며, 영어 이름이라 하더라도 철자가 틀린 점이 더욱 사기 건에 대한 확신을 갖게 하였다.


BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY
Ministerium für Industrie und wirtschaftliche Entwicklung
MINISTRY OF INDUSTRIAL AND COMMERCIAL DEVELOPMENT
Richtung für die Förderung des Handels
DIRECTION FOR THE PROMOTION OF COMMERCE
Richtung externer COMMERCE EXTERIEUR
DIRECTION OF EXTERNAL COMMERCE
N° 235/FG/GCLMINDIC/DPCS/SDCE/SAG
Hamburg, on the Réf : 22 / 03/ 2014
Objet: Exporters License for 2014/2015 fiscal year
Subject: THE MINISTRY OF STATE IN CHARGE OF INDUSTRIAL AND COMMERCIAL DEVELOPMENT
FECPAN INTERNATIONAL
Millerntorplatz 1, Hamburg, 20359,
Hamburg,
The General Manager,
With respect to your application for an Exportation Licence
I have the honour to inform you that you : FECPAN INTERNATIONAL
is authorised to exercise the Power of Exportation for the fiscal year :
Fiscal 2014/ 2015
under Licence No. 183/CPI$W/DE
Subsequently, you are permitted to export Dairy Milk product namely: Full Cream Milk Powder, Skimmed Milk Powder, Whole Milk Powder, from your farm and processing plants. Exportation will be worldwide considering EU and Non EU ports, Asia, USA, Africa and Australia.
Veuillez agréer MONSIEUR LE DIRECTEUR l'assurance de ma considération distinguée.
Pour Copie Certifiée Conforme
Direction Import/Export
Le chef de service des Société des impots Nationaux


BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY
Richtung externer COMMERCE
CHAMBER OF COMMERCE
INSTITUT FÜR QUALITÄT bei Landwirtschaftlichen Erzeugnissen
DEPARTMENT OF QUALITY CONTROL OF AGRICULTURAL PRODUCTS
Kontrollbüro DEUTSCHLAND
INSPECTION MEDICAL OF GERMANY
Date: 28th March, 2014
Ref: MBG/EC/01/14/FECPAN
PROOF OF FACTORY QUALITY AND PLANT AUTHORISATION NUMBER
CERTIFICATE -09102-89- EXPIRES 28/2015
INS/MARCH 28/2014
This is to certify that by order and on behalf of HACCP and ISO regulation and the Ministry of Health and Quality control of dairy products, we have checked the 7 combined plant allocations of FECPAN International (Millerntorplatz 1, Hamburg, 20359). Mentioned below and have reported the following:
Cold Storage warehouse capacity : 5,400 Metric Tons
Quality control(s) : SGS, Halol
Production capacity : 4,700 Metric Tons monthly (7 plants)
Authorized plant number : DE- 04478
PRODUCTS TO BE PRODUCED
FULL CREAM MILK POWDER, SKIMMED MILK POWDER, WHOLE MILK POWDER, INFANT MILK POWDER
Samples : 1 Ton of each product
Quality : MEETS INTERNATIONAL STANDARDS
THE FEDERATIVE REPUBLIC
Chamber of Commerce
German Association of Chambers of Industry and Commerce (DIHK e.V.)
Breite Strasse 29
10178 Berlin
Dr. Christopher Schmaltz

이에 무역관에서는 조사한 내용을 업체에 알려 더 이상 거래가 진행되지 않도록 했다.

[5] 10년 바이어를 갈라놓은 이메일 해킹

□ 사기유형 : 이메일 해킹
□ 발생지역 : 미국
□ 발생시기 : 2014년 2월
□ 피해금액 : US$ 70,000
□ 내용

보안장비를 생산하는 국내 A 기업은 미국 서부에 위치한 Jecolarn(가명)이란 미국 기업과 10년 가까이 거래를 해왔다. 2013년 10월 7만 달러 이상의 거래를 진행하는 과정에서 PI(Proforma Invoice)를 주고받는 시점에서 미국 회사 담당자를 사칭한 제3자가 개입을 했다. 제3자는 A 기업 직원임을 사칭해 미국 회사 담당자와 회계 담당자에게 한국 E은행이 아니라 영국 Santander 은행으로 송금을 유도했는데 미국 바이어는 한국에 있는 기업이 영국으로 송금을 요청한 것에 대해서 별다른 의심이나 사실 확인을 하지 않고 7만 달러를 영국 Santander 계좌로 그대로 송금했다. 바이어는 A 기업이 그동안 H은행을 E은행으로 변경한 내역이 있다 보니 바이어는 다시 변경을 요청한 것에 대해 별다른 의심을 하지 않은 것이다.

대금결제를 조율하는 약 보름가량(11월 중순~12월 초순) 사이 담당자를 사칭한 유사 이메일 계정을 사용한 내역이 사후 확인 과정에서 발견되고, 영어 문체도 평소와 달랐으나 그 당시에는 이를 알아차리지 못했다. 또한 이메일 수신 시 메일주소가 아니라 보낸 사람 이름, 별명 등이 표시되는 경우가 많으므로 자세히 보지 않으면 파악이 어렵다.

* 원래 담당자 원래 이메일 : xxxxxfer@jecolarn.com
* 해커 사용 이메일 : xxxxxfer-jecolarn.com@mail.com,
xxxxxfar-jecolarn.com@mail.com

[6] 이메일 해킹 피해를 한국 업체가 보상하라는 바이어

□ 사기유형 : 이메일 해킹
□ 발생지역 : 방글라데시
□ 발생시기 : 2014년 하반기
□ 피해금액 : US$ 50,000
□ 내용

방글라데시 바이어 B사와 한국 수출업체 K사는 수개월의 왕래 끝에 거래조건에 합의하고 계약서 서명을 앞두고 있었다. 결제조건은 T/T 40%, L/C 60%였다. 방글라데시는 T/T에 의한 무역대금 결제가 원칙적으로 불가능하므로 이 경우 T/T는 제3국을 통한 우회송금을 의미한다.

계약 체결을 앞두고 한국 업체가 해외 출장을 간 동안 B사는 K사로부터 중국의 K사 협력업체 계좌로 입금하라는 이메일을 여러 차례 받았다. 그간 이메일로 협의를 문제없이 계속해왔으므로 B사는 홍콩에 있는 B사 협력사를 통해 중국의 K사 협력사로 송금했다. 단, 계약서 체결 전에 확인도 없이 송금을 한 점, K사가 송부한 견적서(PI)에 한국 내 계좌가 입금 계좌로 표시되어 있음에도 불구하고 중국 계좌로 송금한 점 등은 명백한 B사의 과실이다.

이후 K사가 그러한 내용의 이메일을 보낸 바가 없다고 함으로써 분쟁이 시작됐다. 이메일 상에 나온 중국 회사와 K사는 전혀 무관한 것이었다.

무역관에서 바이어가 보는 앞에서 직접 이메일 계정을 접속, 문제 이메일을 확인하고 해당 이메일의 헤더(header) 정보를 출력해 보았다. 헤더 정보 확인 결과, 문제의 이메일은 바이어 이메일 계정(yahoo)가 승인하지 않은 서버로부터 발송된 것이었으며, 발송 지역은 체코로 나타났다. K사는 gmail을 사용하고 있으므로 정상적으로 발송된 이메일이라면 Yahoo 계정에서 승인된 서버(permitted sender)에서 발송된 것으로 표시된다.

한편, 바이어 이메일에서 K사로 발송된 이메일에 K사 주소가 교묘하게 허위로 표시되어 있었다(올바른 이메일 계정 : l@gmail.com / 잘못된 이메일 계정 : I@gmaiI.com). 결국 이 이메일은 K사로 발송되지 않은 것이다. K사가 출장 중이어서 이메일을 완전히 확인하지 못하는 가운데 무역사기꾼이 개입해 이메일을 해킹한 것으로 보인다.

바이어 입장에서는 한국 업체가 정상적으로 보낸 메일(결제 관련 내용 외 다른 내용)과 해커가 보낸 메일(결제 관련 내용)을 같이 받다 보니 의심을 하지 못했던 것으로 보인다. 바이어는 애꿎은 K사를 상대로 반환요구만 계속하고 있다.

[7] 헝가리 계좌의 인출을 막아 주세요

□ 사기유형 : 이메일 해킹
□ 발생지역 : 헝가리
□ 발생시기 : 2014년 11월
□ 피해금액 : US$ 18,984
□ 내용

11월 21일 금요일 점심이 조금 지난 시간, 서울의 한 중소업체로부터 급박한 전화가 걸려왔다. "KOTRA 무역관이지요? 좀 도와주십시오. 무역사기를 당했는데 저희가 송금한 헝가리 계좌를 동결해 주십시오"라는 다급한 음성이 들려왔다.

H사는 중국에서 원부자재를 수입하여 의류 완제품을 수출하고 있는 중소기업이다. 중국 업체에 원부자재 대금을 결제하는 내용의 이메일이 해킹당한 줄 모르고 해커가 지정한 헝가리 계좌로 송금하는 사기를 당한 것이다. 국내은행을 통해 송금 의뢰한 날짜는 11월 19일(수), 사기당한 것을 알고 무역관에 연락한 것은 한국 시각 11월 21일(금) 저녁 9시가 넘었으니 아마도 송금이 완료되고 출금이 되었을 수 있는 긴박한 상황이었다.

다급한 마음에 무역관은 헝가리 R은행에 상황을 설명하고, 출금 확인 및 계좌 동결을 요청하였다. 그러나 R은행은 '정당한 절차에 따라 송금된 것을 수취인의 동의 없이 동결할 수 없다'면서, '경찰의 공식 요청이 있으면 조사할 수 있다'는 원칙적인 입장만 되풀이했다. 또다시 헝가리 경찰에 연락하고 협조를 요청하였으나 헝가리 경찰 또한 '내용을 공문으로 보내면 확인 후 조치 여부를 결정하겠다'고 대답하며 매우 미온적인 태도였다.

언제 인출이 될 지 아니면 이미 인출이 되었는지 한시가 급한 상황, 더구나 금요일 오후에 연락받은 무역관은 정상적인 절차로는 사태를 수습하기 어렵다고 판단하고 대사관과 협조하여 현지 경찰을 움직여 보기로 했다.

가까스로 토요일 오전에는 사태를 파악할 수 있었다. 그러나 송금된 금액은 이미 R은행에서 다시 O은행으로 이체되었고, 이체된 금액이 O은행의 ATM을 통해 인출되었다는 사실을 알게 되었다. 인출 후 헝가리 경찰 측에서 돈을 회수하기는 어렵다고 알려왔다.

[8] 알제항에서 오도 가도 못하게 된 상품

□ 사기유형 : 결제 미이행
□ 발생지역 : 알제리
□ 발생시기 : 2014년 말
□ 피해금액 : US$ 50,000
□ 내용

한국의 건설 기자재 제조기업인 A사는 어느 날 낯선 알제리 바이어 B사로부터 제품 거래 인콰이어리를 접수했으며, 서신 협상을 통해 D/P at sight 결제조건으로 약 5만 달러에 달하는 수출 계약을 체결했다. 관련 계약 조건에 따라 약속된 기일에 제품을 선적해 알제리로 보낸 한국 A사는 해당 선적품이 알제항에 도착한 것을 통보받고 알제리 바이어 B사에 대금 결제를 요구하였다. 하지만 알제리 바이어는 선적품의 알제항 도착 이후 갑자기 결제 대금이 부족하다며 D/P at sight 거래조건을 D/A 외상거래조건으로 변경할 것을 일방적으로 통보하였다.

바이어의 황당한 요구와 관련, 양측의 줄다리기가 계속 이어진 가운데 2014년 말에 알제항에 도착한 수출품은 알제리 세관 창고에 두 달 이상 계류됐다. 한국 수출업체 A사는 바이어의 요구를 수용할 수 없어 제품의 반송(Ship-back)을 결정했다. 하지만 반송하려면 세관 창고에 계류된 기간에 해당하는 보관료를 납부해야 하는데, 이 비용도 매우 부담스러운 것으로 알려졌다.

알제리에서는 통관되지 않은 수입품을 다시 반출하는 Ship-back에 많은 제약이 있다. 알제리 세관에 자초지종을 설명해 수출자 제품의 Ship-back 정당성을 입증해야 하며, 프랑스어로 된 Ship-back 요청 공문으로 작성해 제출해야 한다. 세관의 Ship-back에 대한 허가가 떨어지면 현지 통관사를 고용해 세관 창고 보관료를 납부하고 Ship-back 절차를 밟으면 된다. 만약 세관이 Ship-back을 허가하지 않는다면 수출업체는 바이어한테 반송품의 (재)수출 절차 진행을 요청해야 하는데 바이어와의 관계가 나빠 (재)수출 협조를 받지 못하면 동 수출품은 고스란히 세관에 압류될 수밖에 없다.

[9] 도착한 컨테이너에 쓰레기만 가득

□ 사기유형 : 선적관련
□ 발생지역 : 파키스탄
□ 발생시기 : 2012년 12월
□ 피해금액 : US$ 20,000
□ 내용

한국의 S사는 파키스탄 U사로부터 2만 달러 상당의 폐 씨디(PC CD) 구매 계약을 맺었다. 파키스탄 U사는 PC CD를 선별 작업하는 사진과 수십 포대에 폐 PC CD가 들어있는 사진 등을 S사에 송부했다. 그리고 선적 전 컨테이너 한쪽 문을 열고 폐 PC CD가 들어있는 면과 다른 컨테이너 문에는 컨테이너 넘버가 있는 한 장의 사진을 송부하며 선적이 완료되었음을 한국의 S사에 알렸다. 한국의 S사는 의심 없이 송금했다.

그런데 BL상의 컨테이너 번호는 "TCLU8023700" 이었는데, 바이어가 보낸 사진에는 "TCLU80237"로 되어있었고 사진상에는 컨테이너 번호 7이후에는 폐 PC CD 포대로 가리어져 있었다. S사에서 컨테이너를 열어본 결과, 컨테이너 문 쪽만 폐시디 포대 몇 개가 있었고 나머지는 쓰레기로 채워져 있었다.

이에 S사는 KOTRA 카라치 무역관에 사기 피해 사항을 알리고 도움을 요청했다. 무역관 직원들은 Sender 소재지가 카라치 외곽지역이라는 사실을 알게 되었고, 방문하여 상담했다. 그런데 U사는 완강히 사기 사실을 외면하고 한국 업체가 거짓말하고 있다고 오히려 공격적으로 나왔다. S사가 보내온 사진들과 증거자료들을 가지고 보여주었지만 자기는 아무런 문제없이 정상적으로 선적했다는 말만을 반복했다. 즉석에서 국내 업체 담당자와 연락을 해서 직접 대화하도록 했지만 조금도 자신의 실수와 사기 사실을 인정하지 않았다. S사는 국내에서 컨테이너 쓰레기 처리 비용도 비싸 Ship Back을 요청했지만 파키스탄 S사는 국내 기업의 어떤 요구도 받아들이지 않고 거부로 일관했다. 국내 기업은 결국 U사에 대해서 모든 것을 포기했다.

[10] 저금리대출을 미끼로 선수금을 노린 사기

□ 사기유형 : 보험비용 사취
□ 발생지역 : UAE
□ 발생시기 : 2014년 6월
□ 피해금액 : 없음
□ 내용

한국의 A사는 두바이 B사로부터 연 3.5%의 저이자 대출을 제안받았다. B사는 연간 300만 달러 이상의 투자를 진행하고 수백만 달러의 자금을 운영하는 두바이의 명망 있는 투자 회사라고 소개를 하였고, A사는 두바이 회사가 제시한 저이율 대출에 관심을 보였다. 이 거래를 진행하기 위해서는 지정된 보험회사에 'surety bond'라는 일종의 보증보험을 들으라고 요구하며 이에 따른 보험비용 청구를 하였다.

A사는 B사에 대한 의심을 가지게 되어 두바이 무역관에 B사의 존재여부 및 규모 확인을 문의하였다. 무역관은 사업자등록증 사본을 요청해 송부하면 관계기관에 문의해 회사의 존재 및 규모에 대한 정보를 알려준다고 했으나 사업자 등록증을 요구받은 B사는 이에 대한 거부감을 나타내며 거래를 중단하고자 하였다.

이를 전달받은 무역관은 자체 네트워크를 활용하여 B사를 수소문하였으나 두바이의 명망 있는 투자회사라는 말과 달리 실제로 알려진 바가 없으며 홈페이지에 명시된 두바이 사무실과 세계 전역의 지사에 수차례 전화를 해도 결번이거나 연결이 되지 않았다.

여러 차례 시도 끝에 B사의 CEO라는 사람과 어렵사리 연결이 되어 A사를 대신하여 방문하기 위해 주소확인을 부탁했으나 확인을 해주지 않고 일방적으로 전화를 끊어버렸다. 무역관은 B사에 대한 어떠한 정보도 발견할 수 없었고, 정황상 수상한 점이 많아 A사에 신중하라는 조언을 한 상태이다.

작 성 자

◈ 123개 해외무역관 조사담당자
◈ 정부3.0추진팀 오승희 사원

Global Market Report 15-030

무역사기 발생 현황 및 대응책

발 행 인 ▌ 김재홍
발 행 처 ▌ KOTRA
발 행 일 ▌ 2015년 7월
주 소 ▌ 서울시 서초구 헌릉로 13
(우 137-749)
전 화 ▌ 02) 1600-7119(대표)
홈페이지 ▌ www.kotra.or.kr

Global Market Report

www.kotra.or.kr

kotra
Korea Trade-Investment Promotion Agency