법인간의 해외송금 자금에 대한 사취행위에 주의하십시오 !

고객여러분께

미쓰이스미토모 은행을 이용해주셔서 진심으로 감사드립니다.

법인고객님과 국외 거래처나 모회사·관련회사(이하, '외국법인')간에 송금처리시 송금계좌정보 연락을 e-mail을 통해 취할 때, 가짜 e-mail 또는 내용이 무단 수정된 e-mail에 속아, 해외송금 자금을 사취 당하는 피해가 발생하고 있습니다.

※컴퓨터의 바이러스 감염으로 비밀번호를 해킹 당하여 고객님의 계좌로부터 무단으로 송금이 실행되는 범죄와는 상이합니다.

법인 고객께서는 다음의 대책을 실시해 주십시오.

◆ 발생 사례

- 외국법인을 사칭하여 수신한 e-mail의 송금지시나 e-mail의 첨부 청구서에 따라 해외송금을 실행한 결과, 송금한 자금을 사취 당했음.
- 고객님의 외국 소재 관련회사의 CEO 등 고층간부를 사칭하여 고객님의 회계담당자가 수신한 e-mail 지시에 따라 해외송금을 실행한 결과, 송금한 자금을 사취 당했음.
- 고객님께서 외국법인에 발신한 e-mail 또는 첨부 청구서가 무단 수정되어, 설정하셨던 계좌와 다른 계좌로 송금된 결과, 수령할 자금을 사취 당했음.

◆ 대책 방안

➢송금 전 e-mail이외의 수단(전화나 팩스 등)을 통한 사실 확인

아래 사례와 같이 일반적인 청구·지불관행과 다른 대응을 요청받았을 경우, 외국법인에 e-mail이외의 수단(전화나 팩스 등)을 통해 사실을 확인한다.

·외국법인에서 송금처 계좌를 변경한다는 내용의 e-mail을 수신한 경우
·외국법인의 정규가 아닌 e-mail주소로부터 송금을 의뢰 받은 경우
·긴급 혹은 극비 건으로 송금 의뢰 e-mail을 수신한 경우 등

➢PC 보안성 대책

·송금처리나 그에 따른 연락수단인 PC의 보안성 대책을 세운다.
·또한 외국법인과 송금의뢰 e-mail을 발신·수신 시 평문(plaintext, 암호화되지 않은 데이터)이 아닌 암호화된 첨부파일을 사용하는 전자서명을 첨부하는 등 보다 안전성이 높은 방법을 시행한다.

만일 피해 사실이 판명되었을 시 해당 해외송금의 취급점이나 관할경찰서로 연락하여 문의하십시오.
일본전국은행협회 홈페이지에 접속하셔서 '중요 공지사항'을 참고하시기 바랍니다.
(URL) http://www.zenginkyo.or.jp/topic/sagijiken_remittance/index.html

2015년 11월
주식회사 미쓰이스미토모은행