

4가지 해킹유형별 기술유출 절차 및 예방법

안녕하십니까, '생명공학 기술보호 TF' 사무국 산업기술보호협회입니다.

최근 우리 생명공학 분야 기업의 기술탈취를 노린 해외발 해킹시도가 지속적으로 발생하고 있어 대책이 필요한 상황입니다.

이에 따라, 금년 발생했던 해킹시도 유형을 분석하여 '기술유출 절차 및 예방법'을 안내해 드립니다.

참고하시어 기술유출을 막을 수 있도록 활용해주시길 바랍니다.

또한, 아래 법률 조항에 따라 국가핵심기술 또는 산업기술을 보유한 기업에 해킹이 발생한 경우 그 사실을 신고하여야 하므로 생명공학 기술보호 TF 사무국으로 연락주시면 신고 시 도움을 드리겠습니다.

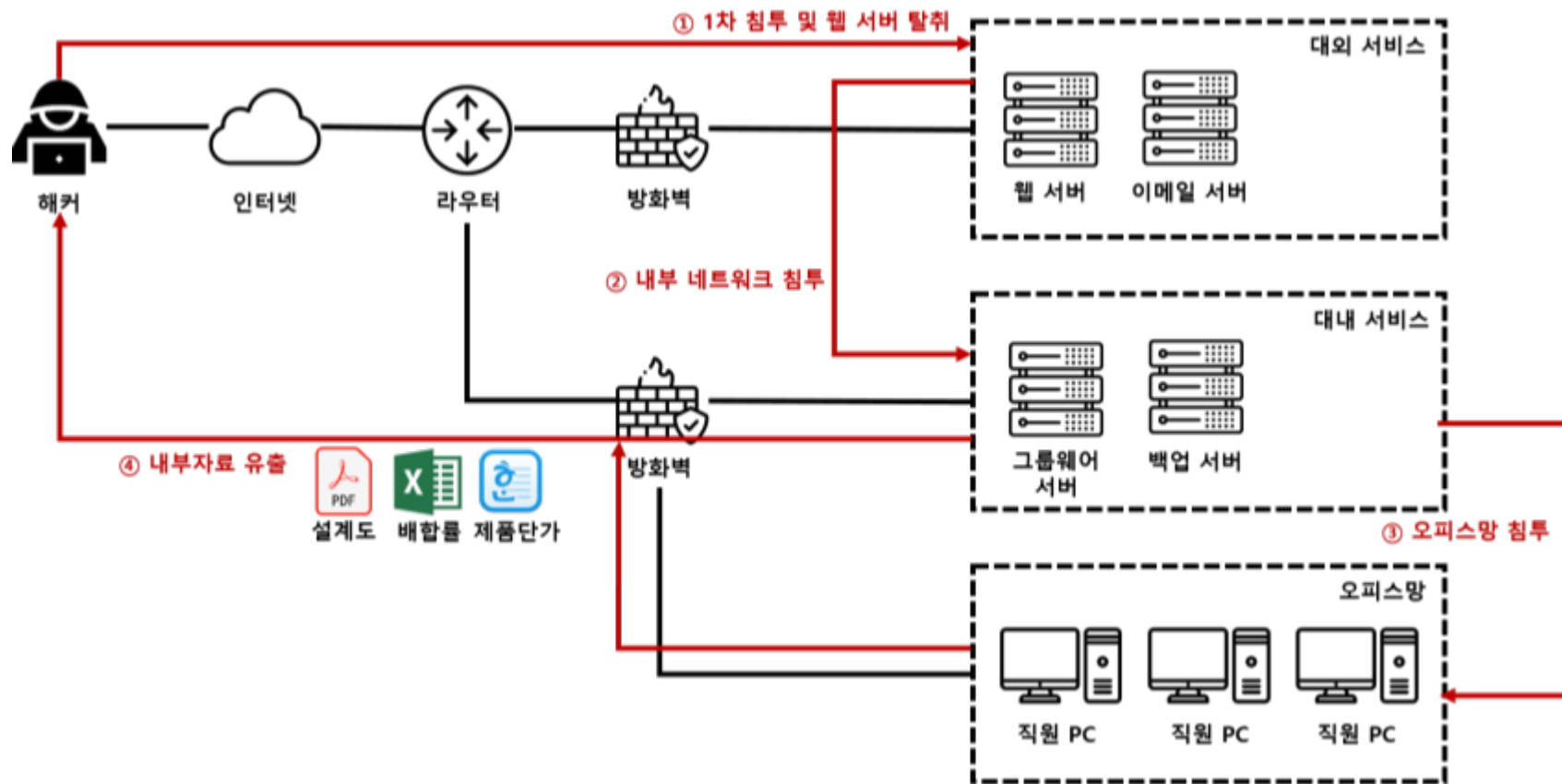
관련 법령

산업기술의 유출방지 및 보호에 관한 법률

제15조(산업기술 침해신고 등)	① 국가핵심기술 및 국가연구개발사업으로 개발한 산업기술을 보유한 대상기관의 장은 제14조 각 호의 어느 하나에 해당하는 행위가 발생할 우려가 있거나 발생한 때에는 즉시 산업통상자원부장관 및 정보수사기관의 장에게 그 사실을 신고하여야 하고, 필요한 조사 및 조치를 요청할 수 있다.
제 14조 1호	절취 · 기망 · 협박 그 밖의 부정한 방법으로 대상기관의 산업기술을 취득하는 행위 또는 그 취득한 산업기술을 사용하거나 공개(비밀을 유지하면서 특정인에게 알리는 것을 포함한다. 이하 같다)하는 행위

생명공학 기술보호 TF 사무국 monitor@kaits-info.or.kr
기술지원 문의 02-3489-7060~7064
서비스 신청 및 기술유출 상담관련 문의 02-3489-7056

Case 1. 웹서버 해킹을 이용한 기술 유출



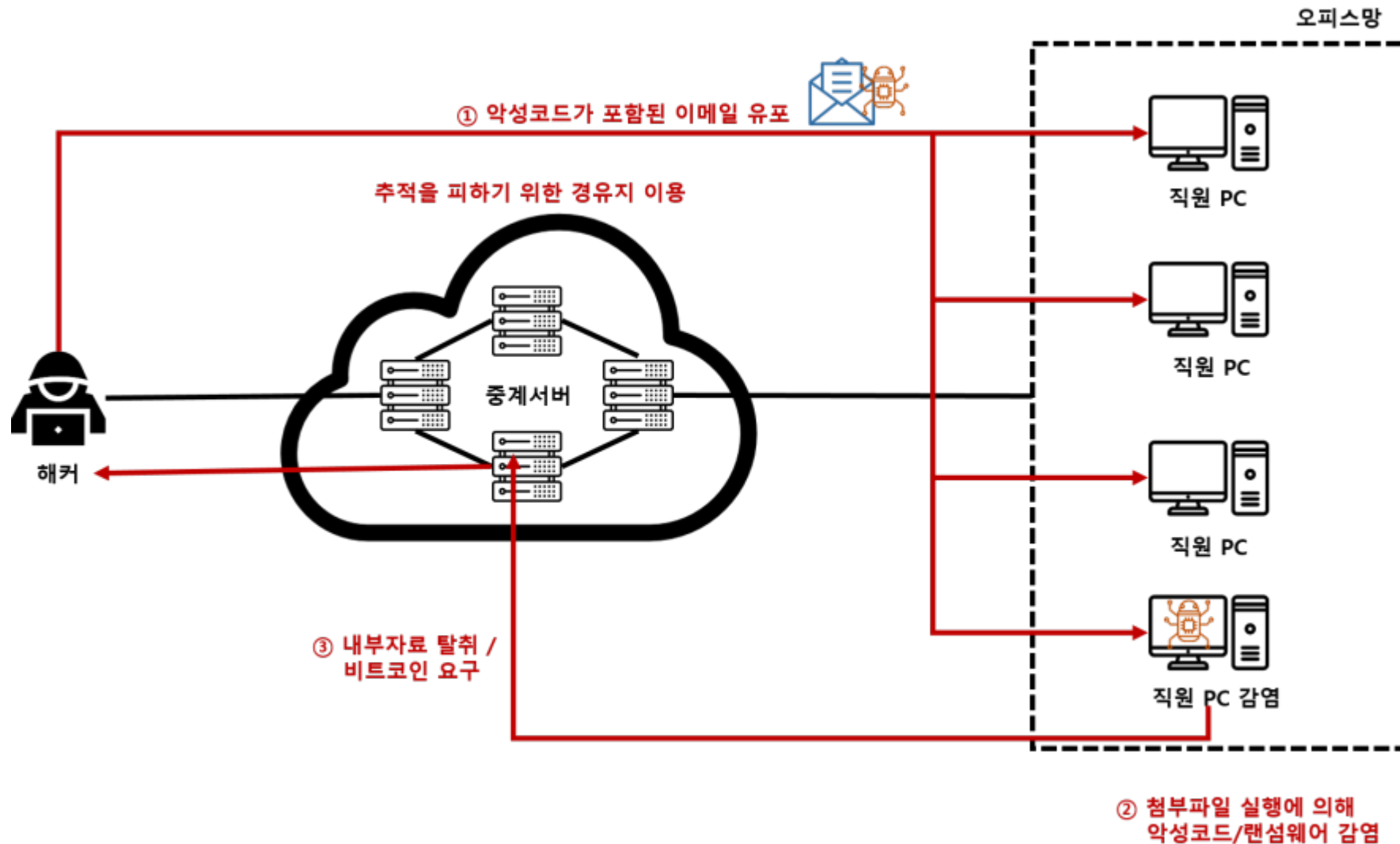
공격 흐름

- 01 대외서비스 중인 웹서버에 대한 해킹 사전준비
- 02 웹서버에 접근, 권한 탈취
- 03 웹서버를 이용하여 내부 네트워크 진입
- 04 오피스망에 침투하여 개인 PC의 계정정보, 개인정보 등 탈취
- 05 내부 네트워크, 오피스망의 중요자료 탈취
- 06 탈취한 자료를 경쟁사에 판매 혹은 피해기업 협박

예방책

- 01 웹서버 관리자 계정 관리(초기 패스워드 변경)
- 02 주요파일(패스워드 파일 등) 접근제한 관리
- 03 불필요한 서비스 제거
- 04 웹방화벽, UTM 설치하여 접근제한 및 모니터링
- 05 웹어플리케이션 진단도구를 활용한 웹백도어 점검
(무료상담: KISA 02-405-5617)
- 06 웹어플리케이션 취약점 진단
(무료상담: KISA 02-405-5665)

Case 2-1. 이메일 피싱을 이용한 내부자료 유출



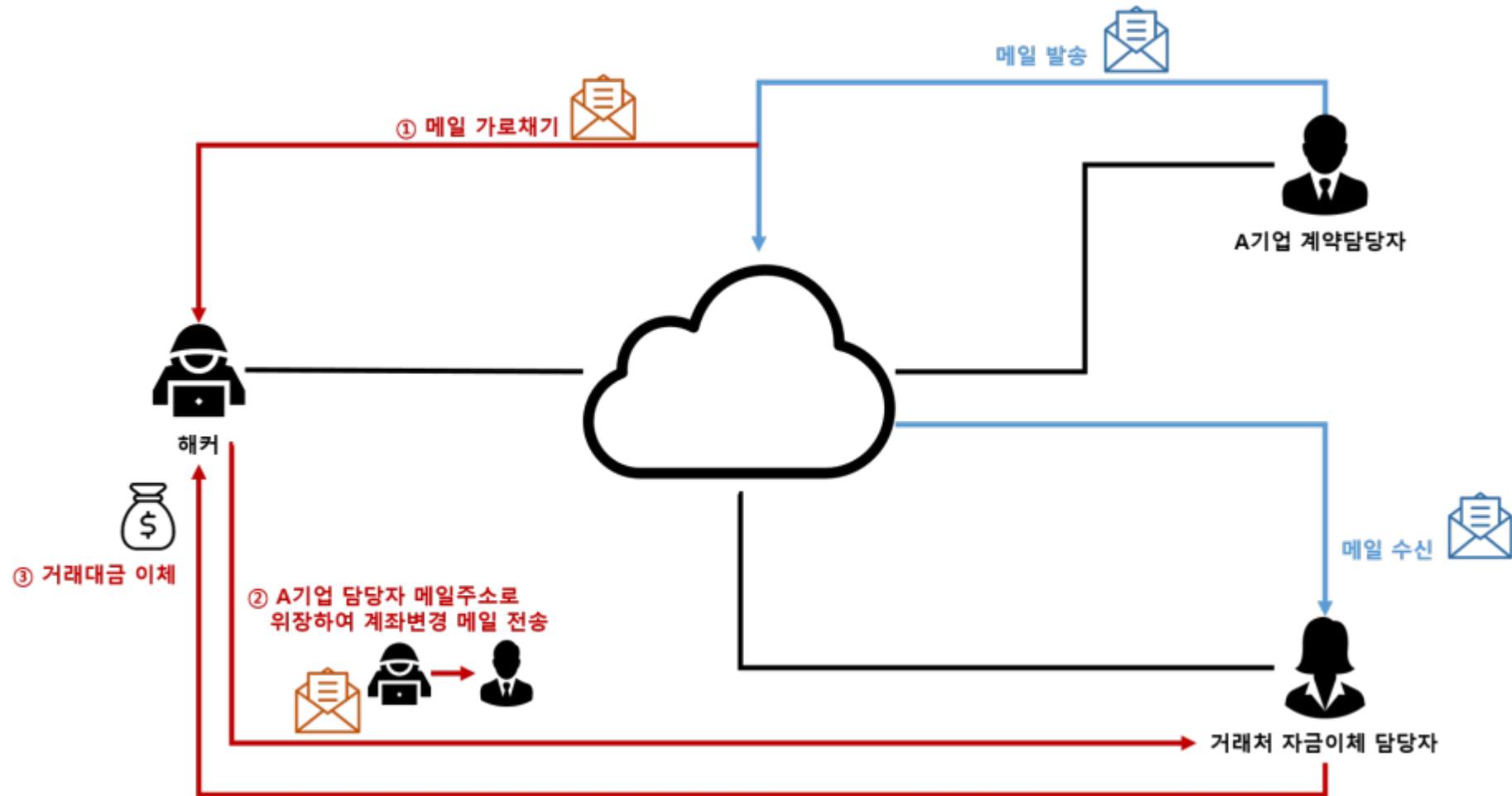
공격 흐름

- 01 공격자는 홈페이지, 인터넷 검색 등으로 피해기업의 이메일 확보
- 02 악성코드가 포함된 이메일/계정정보 입력 유도 이메일 발송
- 03 사용자 부주의로 악성코드가 포함된 첨부파일 열람/계정정보 입력
- 04 탈취한 정보를 이용하여 그룹웨어 침입, 중요자료 탈취

예방책

- 01 스팸필터를 설치하여 악성, 스팸메일 유입 차단
- 02 정기적인 피싱메일 모의훈련 수행
- 03 유행하는 피싱메일 동향 파악 및 임직원 교육 수행

Case 2-2. 이메일을 이용한 거래대금 탈취



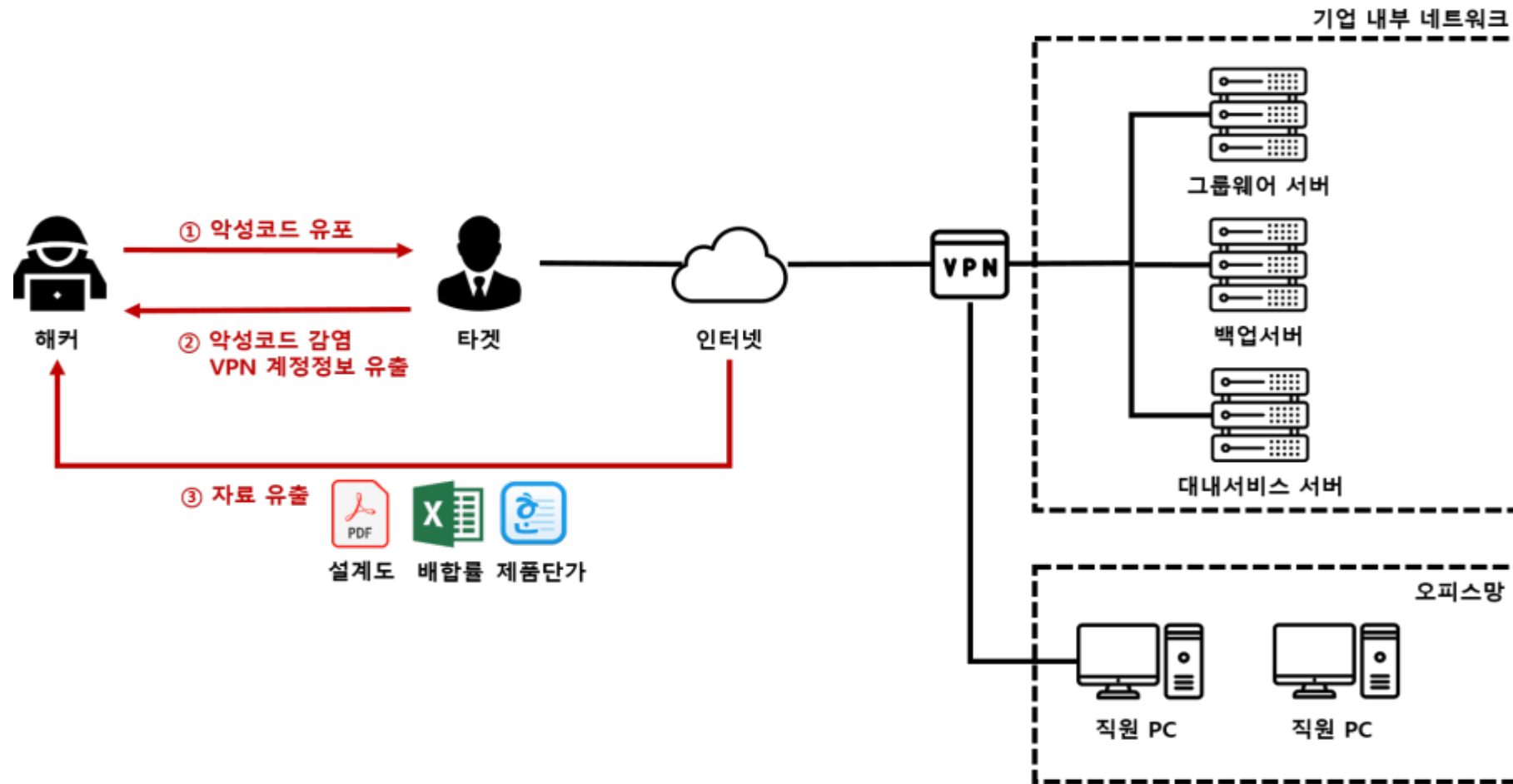
공격 흐름

- 01 사전 공격을 통한 계약담당자-거래처 담당자 메일 가로채기
- 02 A기업 담당자로 위장하여 계좌변경 메일 발송
- 03 거래처 자금이체 담당자 해커에게 거래대금 이체

예방책

- 01 메일 발신인 재확인(유선, 화상전화 등)
- 02 정기적인 피싱메일 모의훈련 수행
- 03 담당자 PC 악성코드 백신 설치
- 04 무역거래 계약서 작성 시 '계좌번호 변경 요청 시 유선으로 확인' 조항 삽입

Case 3. VPN을 이용한 내부자료 유출 절차



공격 흐름

- 01 사용자의 PC에 악성코드 유포
- 02 악성코드 감염 후 VPN 계정정보 해커에게 전송
- 03 회사 내부 네트워크, 오피스망에 접속하여 자료 유출

예방책

- 01 2차 인증(OTP, 핸드폰 인증 등) 도입
- 02 백신 설치로 개인 PC 보안성 강화
- 03 MAC, 공인IP 기반 접근제한 정책 설정
- 04 중요파일 접근 등 비정상 활동 모니터링