

인사이트

사내 AI 업무 시스템이 사칭 발주서를 잡았습니다

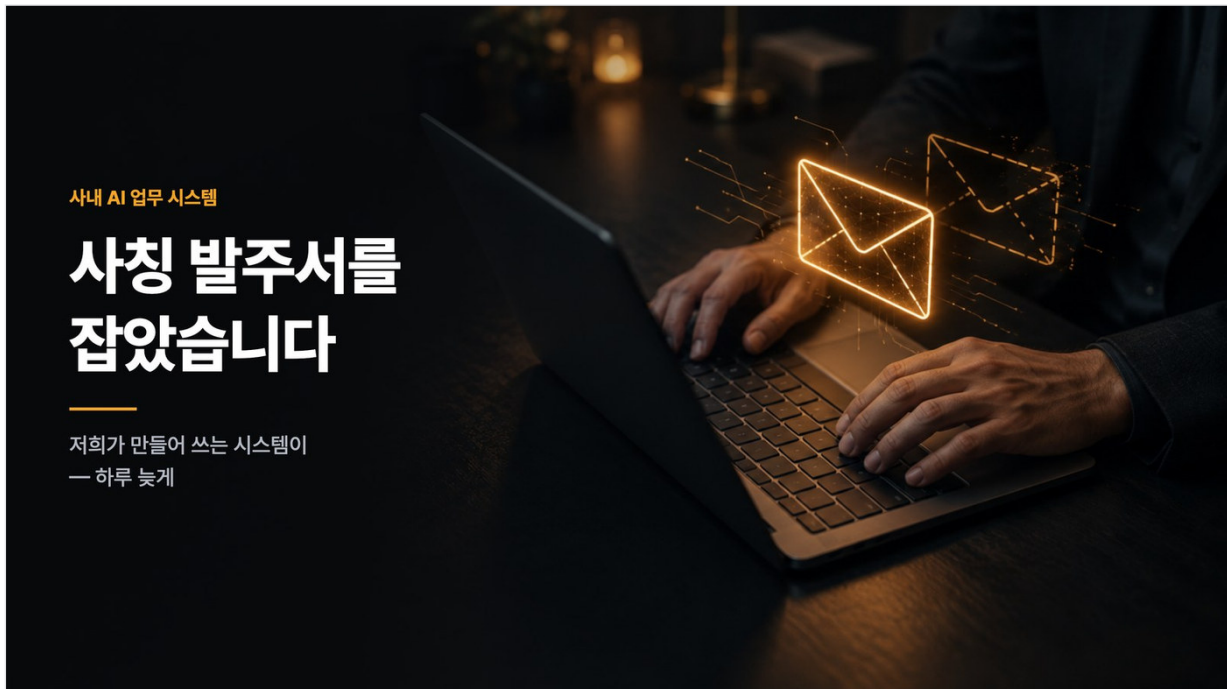
하루 늦게

방동걸 (주)웨이스 대표이사

2026년 9월 8일

지난 9월 8일 아침, 대표가 시스템에 메일 한 통을 확인해 달라고 했습니다. 전날 9,700만원짜리 공공기관 과업지시서를 보낸 그 담당자가, 이번에는 열화상 카메라 5대를 6,490만원에 사 달라는 발주서를 보냈습니다. 웨이스가 VEXPLOR 개발과 나란히 운영하는 사내 AI 업무 시스템에서 실제로 겪은 일입니다.

4분이 지나기 전에 답이 나왔습니다. 사칭이었습시다.



사내 AI 업무 시스템

사칭 발주서를 잡았습니다

저희가 만들어 쓰는 시스템이
— 하루 늦게

사내 AI 업무 시스템이 사칭 발주서를 잡았습니다. 저희가 만들어 쓰는 시스템이, 하루 늦게

저희는 사내 업무를 직접 만든 AI 업무 시스템으로 처리합니다. 메일, 문서, 회의 기록, 작업 이력이 그 안으로 들어오고, 지시를 내리면 시스템이 자료를 직접 열어 판단합니다. 이번에 잡아낸 것도 사람 눈이 아니라 그 시스템이었습시다.

먼저 하나 밝혀 둘 것이 있습니다. 같은 시스템이 하루 전에는 이걸 진짜 딜로 처리했습니다. 제안 폴더를 만들고, 수행 가능하다고 회신하고, 미팅 날짜까지 잡았습니다. 그러니까 이 글은 "저희 시스템이 막아냈다"는 이야기가 아니라, 하루 늦게 잡았고 그 하루를 어떻게 규칙으로 바꿨는가를 적은 기록입니다.

돈은 나가지 않았습니다. 견적서도, 통장사본도, 사업자등록증도 보내지 않았습니다.

짚어 둘 것이 하나 더 있습니다. **사칭당한 기관이 뚫린 것이 아닙니다.** 기관과 무관한 사람이 이름과 부서명을 빌려 쓴 것이고, 메일은 그 기관 서버를 한 번도 거치지 않았습니다.

01

판정은 4분 안에 섰습니다

지시는 "이 메일 확인해 봐" 한 줄이었습니다. 시스템이 연 곳은 여섯 군데인데, **앞의 세 곳에서 이미 답이 나왔습니다.**

무엇을 열었나	무엇이 나왔나	신호
메일 원문 헤더	소규모 메일 호스팅 경유	주의
발신 도메인 조회	첫 메일 사흘 전 등록	결정적
첨부 발주서	취급 안 하는 물품	결정적
파일 속성	발송 5분 전 생성	강함
다른 확장자	예비 도메인 하나 더	강함
공식 담당자 명단	그 이름이 없음	결정적

앞의 세 줄로 4분 안에 사칭이 확정됐고, 나머지 세 줄은 그 뒤 한 시간 안에 확인해 근거를 보았습니다.

메일이 도착한 것은 아침 10시 48분, 지시가 들어간 것은 11시 41분, 증빙을 보관한 것이 11시 44분입니다.

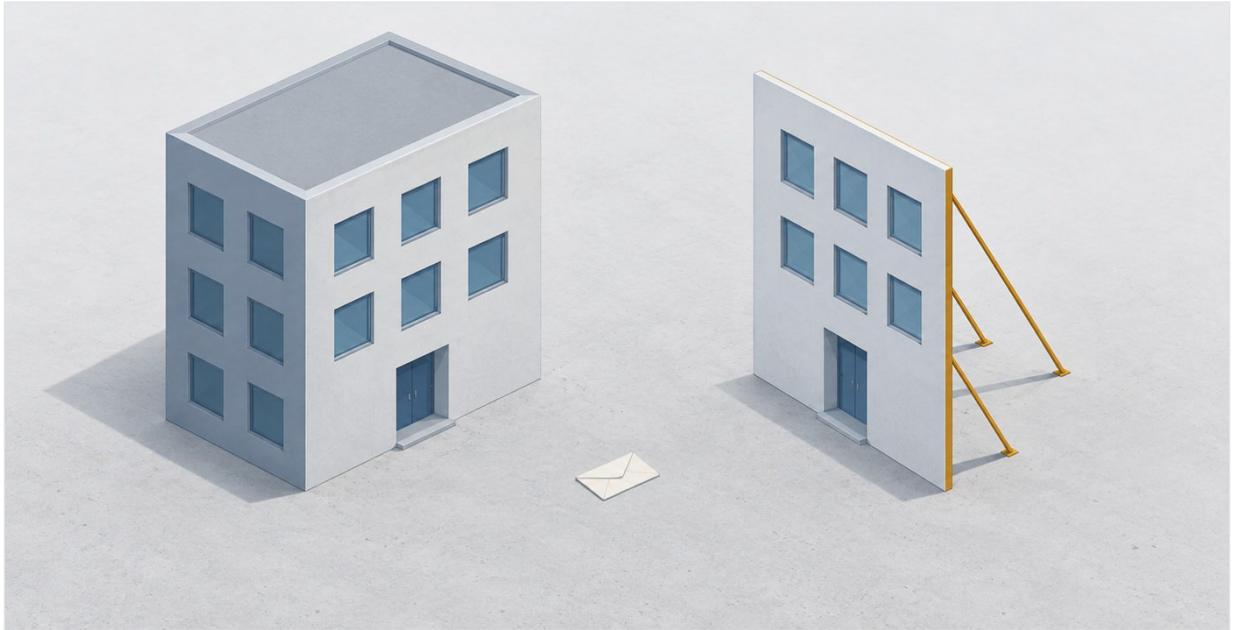
여섯 줄에서 어느 하나만 봐도 이상하지만, **여섯 줄을 한 시간 안에 모으는 것이** 사람 손으로는 잘 안 됩니다. 헤더를 열어 발송 경로를 읽고, 도메인 등록일을 조회하고, 파일 속성을 확인하고, 기관 홈페이지에서 담당자 명단을 찾아 대조하는 일은 각각 몇 분씩 걸립니다. 그 몇 분이 쌓이면 "바쁘니까 나중에"가 됩니다.

시스템은 그 몇 분을 아끼려고 순서를 건너뛰지 않습니다. 그게 유일한 차이였습니다. 지시는 한 줄이었지만, 그 뒤에 붙은 여섯 번의 확인은 저희가 미리 정해 둔 것입니다.

02

사람 눈으로는 안 보이는 자리에 답이 있었습니다

받은편지함 화면에는 보낸 사람 이름과 제목만 보입니다. 판정에 쓰인 값은 전부 그 화면 바깥에 있었습니다.



왼쪽은 오래 전에 등록된 진짜 도메인, 오른쪽은 첫 메일 사흘 전에 만든 사칭 도메인. 앞에서 보면 같고, 뒤에는 아무것도 없습니다

도메인 등록일이 결정적이었습니다. 발신 주소의 도메인은 첫 메일이 오기 사흘 전에 만들어진 것이었고, 진짜 기관 도메인은 1999년에 등록된 것이었습니다. 두 주소는 하이픈 하나 차이입니다. 저희도 전날 그 주소를 여러 번 봤고 회신까지 보냈지만 아무도 이상하다고 느끼지 않았습니다.

그 도메인에는 홈페이지가 없었습니다. 열어 보면 도메인 판매업체의 기본 안내 화면이 나옵니다. 메일만 받게 설정돼 있고 웹은 처음부터 만들지 않았습니다. 공공기관 도메인에 홈페이지가 없다는 것 자체가 답입니다.

예비 도메인이 하나 더 있었습니다. 같은 이름의 다른 확장자를 훑자 나왔는데, 등록 시각이 첫 메일이 오기 다섯 시간 전이었습니다. 등록업체도 메일 설정도 똑같았습니다. **메일을 보내는 날 아침에 두 번째 신분을 미리 만들어 둔 겁니다.** 그래서 차단도 두 주소에 동시에 넣었습니다. 하나만 막으면 다음 날 다시 옵니다.

발주서 파일은 파워포인트로 만들어 온라인 변환 사이트로 바꾼 것이었고, 만든 시각이 메일 발송 5분 전이었습니다. 기관 결재를 거친 문서에서 나올 수 없는 흔적입니다.

03

인증은 전부 통과했습니다

이 건에서 가장 위험한 부분입니다. 메일 헤더에는 이렇게 찍혀 있었습니다.

검사	결과	실제로 뜻하는 것
SPF	pass	허가된 서버가 보냄
DKIM	pass	중간에 안 바뀜
DMARC	pass (reject)	앞 둘이 일치

세 줄 모두 통과입니다. 그런데 이 셋은 그 도메인에서 실제로 왔다는 것만 증명합니다. 그 도메인이 그 회사 것인지는 말하지 않습니다.

공격자가 자기 도메인을 사서 설정을 정상으로 해 두면 세 검사는 전부 통과합니다. 10분이면 됩니다. 그러니까 이 셋은 위조를 잡는 장치이지 사칭을 잡는 장치가 아닙니다. 메일 프로그램이 경고를 안 띄운 것도 이 때문입니다. 경고할 것이 없었습니다.

첨부된 사업자등록증도 마찬가지였습니다. 등록번호도 대표자 이름도 실제 기관 것과 같은, 공개된 진짜 문서였습니다. 첨부가 진짜인 것은 보낸 사람이 진짜라는 증거가 되지 않습니다.

04

검색해도 안 나오는 것이 안전 신호는 아닙니다

시스템은 이 주소가 어디까지 알려졌는지도 함께 확인했습니다. 결과가 전부 0이었습니다.

- 웹 검색에 이 도메인을 언급한 글이 한 건도 없습니다.
- 보안 업체가 쓰는 공개 스캔 서비스에도 기록이 0건입니다.
- 발주서에 적힌 휴대폰 번호를 전화번호 조회 서비스에서 찾으니 신고 0건, 스팸 지수 0퍼센트, 조회수까지 0이었습니다.

조회수 0은 저희가 그 번호를 찾아본 첫 사람이라는 뜻입니다. 깨끗해서 안전한 것이 아니라, 너무 새것이라 아직 아무 기록이 안 쌓인 겁니다.

여기서 판단이 갈립니다. 신고 이력이 없다는 것을 안전 신호로 읽으면 그대로 당합니다. 새로 만든 주소는 기록이 없는 것이 정상이고, 그래서 기록이 없다는 것으로는 아무것도 판정할 수 없습니다. 판정은 등록일로 합니다.

같은 이유로, 이런 사기는 차단 목록이 따라잡기 전에 지나갑니다. 목록에 오르기를 기다리는 대신 등록일이라는, 처음부터 존재하는 값을 보는 편이 빠릅니다.

05

하루 전에는 같은 시스템이 못 잡았습니다

9월 7일에 첫 메일이 왔을 때, 시스템은 9,700만원 규모 과업지시서를 읽고 "수행 가능"으로 판단해 제안 폴더를 만들고 회신 문안을 썼습니다. 그 판단 자체는 틀리지 않았습니다. 요구사항 번호부터 제외 범위, 하자보수 기간까지 갖춰진 문서였고 예산 규모도 그 사업에 어울렸습니다. 문서가 진짜였다면 맞는 판단이었습니

다. 무엇이 달랐냐면 순서입니다.

7일에는 내용을 먼저 읽었습니다. 문서가 훌륭하니 판단이 긍정적으로 나왔고, 그 뒤로는 도메인을 볼 이유가 사라졌습니다. 이미 진짜라고 결론이 났으니까요. 8일에는 발주서가 이상해서 도메인부터 봤습니다. 그 순서 하나가 4분과 하루를 갈랐습니다.

내용이 정교할수록 도메인을 먼저 봐야 합니다. 정교함은 진짜라는 근거가 아니라 공을 많이 들였다는 뜻이고, 큰 금액을 노릴수록 공을 많이 들입니다.

06

그래서 규칙 한 줄을 시스템에 심었습니다

처음 들어온 리드는 내용을 읽기 전에 발신 도메인을 조회한다. 등록일이 최근이면 거기서 멈춘다.

이 한 줄을 회사 작업 규칙 문서와 실패 기록에 넣었습니다. 이제 새 리드가 들어오면 착수 시점에 이 검사가 걸립니다. 다음에 비슷한 메일이 오면 4분이 아니라 처음 몇 초에 걸립니다.

저희가 사내 AI 업무 시스템을 직접 만들어 쓰는 이유가 여기 있습니다. 실수를 사람의 기억에 맡기지 않고 규칙으로 바꿔 시스템에 넣으면, 같은 실수를 두 번째부터는 시스템이 대신 기억합니다. 담당자가 바뀌어도, 바쁜 날에도, 그 검사는 그대로 걸립니다.

이번 건에서 저희가 실제로 얻은 것은 "사기를 막았다"가 아닙니다. 하루짜리 실수를 규칙 한 줄로 바꿔 넣었다는 것입니다. 그게 이 시스템의 쓸모입니다.

07

발주서가 스스로 드러낸 것 5가지

판정이 선 뒤에 다시 읽으니 처음부터 보였어야 할 것들이 있었습니다. 같은 메일을 받으실 경우를 위해 그대로 적습니다.

- **취급하지 않는 물품** — 소프트웨어를 논의하다가 갑자기 열화상 카메라 5대를 사 달라고 합니다. 저희는 카메라를 팔지 않습니다. 물품 종류가 바뀌는 순간이 수법이 바뀌는 순간입니다.
- **지정 업체에 먼저 입금** — "재고 있는 곳을 소개해 줄 테니 거기서 사라"는 요구는 정상 거래에 없습니다. 공공기관은 대리구매를 시키지 않습니다.
- **통장사본과 사업자등록증 요구** — 받아 간 서류로 다음에는 우리 회사를 사칭합니다.
- **촉박한 납품기한** — 발주일에서 사흘 뒤였습니다. 확인할 시간을 주지 않는 것이 목적입니다.
- **연락처가 개인 휴대폰 하나** — 문서 전체에서 전화번호가 010 번호 하나뿐이고 부서 유선번호가 없었습니다. 기관이 운영하는 상생 플랫폼의 담당자 연락처는 전원 042 국번 유선이었고, 메일에 적힌 이름은 그 명단에 없었습니다.

여기에 하나 더 있습니다. 발주서에는 **외부 공개를 금지하는 조항**이 들어 있었습니다. "자료와 계약정보를 외부에 공개하지 말 것"입니다. 계약 조항처럼 보이지만 실제 기능은 **우리가 기관에 전화해 확인하는 것을 막는 것**입니다. 확인을 막는 조항이 붙어 있으면 그것이 확인해야 할 이유입니다.

08

지금 확인해 보실 것



확인만 도메인 한 곳만 들여다보면 됩니다. 나머지 판단은 그다음입니다

받은 메일함에 열려 있는 신규 문의가 있으시면 이 넷만 보시면 됩니다. 1분이면 됩니다.

- **보낸 사람 도메인을 기관 홈페이지 주소와 글자 단위로 맞춰 보십시오.** 하이픈, 숫자 1과 알파벳 I, 0과 O가 바뀐 자리를 봅니다.

- 그 도메인을 브라우저 주소창에 그대로 넣어 보십시오. 홈페이지가 안 나오면 거기서 멈춥니다.
- 메일에 적힌 번호 말고, 기관 홈페이지에서 찾은 대표번호로 전화해 확인하십시오. 메일에 적힌 번호로 걸면 사칭한 사람과 통화하게 됩니다.
- 통장사본과 사업자등록증은 확인이 끝나기 전에 보내지 마십시오. 이 둘은 다음 피해자를 만드는 재료가 됩니다.

저희가 돈을 잃지 않은 건 시스템이 완벽해서가 아니라, 상대가 하루 만에 물품 구매로 넘어와 준 덕입니다. 그쪽이 조금만 더 참았으면 저희는 다음 주 월요일에 약속 장소까지 갔을 겁니다.

두 도메인은 등록업체와 KISA 에 신고했습니다. 혹시 같은 주소에서 메일을 받으셨다면 회신하지 마시고 두 주소를 함께 차단하시기 바랍니다. 하나만 막으면 다른 하나로 다시 옵니다.

그래서 남은 질문은 이겁니다. 여러분 회사에서는 처음 온 메일의 진위를 누가, 어느 단계에서 판정하시나요? 그 판정이 사람의 기억에 있으면 바쁜 날에 건너뛰어집니다. 저희는 그걸 이번에 확인했습니다.

WACE(웨이스)는 공장이 스스로 판단하고 멈추지 않게 하는 제조 AI 운영체제 VEXPLOR를 만드는 회사다.



원문 blog.vexplor.com/post/in-house-ai-caught-a-fake-order

발행 2026년 9월 8일 · 방동걸 (주)웨이스 대표이사

회사 주식회사 웨이스 (WACE Inc.) · 대표이사 방동걸 · 사업자등록번호 439-87-02852

주소 (18462) 경기 화성시 동탄구 동탄영천로 150, 에이동(A동) 1702·1706호 (영천동, 실리콘밸리동탄)

연락처 전화 070-4730-0629 · contact@wace.me

홈페이지 wace.me · linkedin.com/company/wace-inc



원문



홈페이지



링크드인