Safe Intelligence

외부에 노출된 자산부터 계정 유출까지

SafeIntelligence

JSecurity All for Japan Security | 주식회사 JSecurity (JSecurity, Inc.) safeintelligence.biz

목차

01 제안 배경 03 – 06

02 기능 소개 07 – 14

03 기능 상세 15 – 20

04 회사 소개 21 – 23

01

제안 배경

1 외부 공격표면의 변화

2 관리되지 않는 자산의 위험

3 SafeIntelligence 필요성

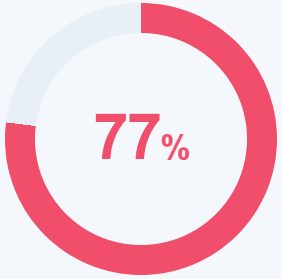
외부에서 보이는 자산이 늘어나고 있습니다

클라우드와 외부 서비스 사용이 늘어나면서 기업의 인터넷 노출 자산도 지속적으로 변화하고 있습니다. 관리되지 않는 서브도메인, 테스트 서버, 만료된 인증서와 외부에 공개된 서비스는 조직이 인지하지 못하는 사이 **새로운 위험 요소**가 될 수 있습니다.



대기업 대비 **중견·중소 규모 조직이 더 많이 공격받는 비율**

Verizon DBIR 2025



웹 애플리케이션 공격이 **탈취된 인증정보로 발생**

Verizon DBIR 2024



침해 발생 후 **발견까지 걸리는 평균 소요 기간**

IBM Cost of a Data Breach 2024

※ 인용 수치는 SafeIntelligence 공식 홈페이지에 표기된 출처를 그대로 사용했습니다.

관리되지 않는 자산은
결국 침해로 이어집니다

발견되지 않고 방치된 자산은 취약점과 설정 오류가 그대로 남아 **공격자가 조직보다 먼저 발견**할 수 있습니다. 시간이 지날수록 **침해로 이어질 가능성**은 빠르게 커집니다.



SAFEINTELLIGENCE로

외부 공격표면과 계정 유출을 하나의 화면에서

SafeIntelligence는 기업의 외부 자산을 자동으로 탐색하고, 발견된 자산의 취약점과 설정 상태를 확인합니다. 또한 기업 도메인과 연결된 임직원 이메일 및 계정정보의 다크웹 유출 여부를 확인하고, 발견된 위험을 지속적으로 관리할 수 있도록 지원합니다.

외부 자산 탐색

도메인을 등록하면 인터넷에 공개된 조직의 자산을 자동으로 탐색합니다.

취약점 진단

발견된 자산의 알려진 취약점과 보안 설정 상태를 확인합니다.

다크웹 유출 모니터링

기업 도메인과 연결된 이메일 및 계정 유출 정보를 확인합니다.

세 가지 기능의 결과가 하나의 대시보드로 모입니다 — 별도의 장비나 에이전트 설치가 필요하지 않습니다.

02

기능 소개

1 SafeIntelligence

2 통합 대시보드

3 외부 자산 탐색

4 취약점 진단

5 다크웹 유출 모니터링

6 통합 파인딩 관리

7 워크스페이스 협업

SafeIntelligence

SafeIntelligence는 **외부 공격표면 관리(EASM)**와 **다크웹 계정 유출 모니터링**을 하나의 화면에서 제공하는 SaaS 보안 플랫폼입니다. 도메인 소유를 확인한 뒤 스캔이 진행되며, 별도의 장비나 에이전트 설치 없이 이용할 수 있습니다.



외부 자산 탐색

서브도메인 자동 탐색 / 공개 포트 · 서비스
웹 서버 · 기술 정보 / DNS · WHOIS



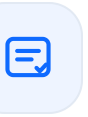
취약점 진단

알려진 취약점 · CVE / TLS · SSL 설정
인증서 상태 / HTTP 보안 헤더



다크웹 유출 모니터링

계정 유출 / 이메일 유출
URL 유출 / 악성코드 감염 신호



통합 파인딩 관리

스캔 결과 · 다크웹 신호 통합 목록
심각도 · 상태별 필터 / 조치 상태 추적



워크스페이스 협업

멤버 초대 / 권한 관리
담당자 지정 / 빌링 분리



지속 모니터링 · 알림

신규 자산 · 변경 사항 확인
새로운 유출 정보 확인 시 알림

통합 대시보드

웹 기반 통합 대시보드를 통해 조직의 **외부 보안 현황을 한 화면에서 확인**할 수 있으며, 도메인별 보안 점수와 위험 분포, 주요 위험 항목으로 **바로 이동**할 수 있습니다.



자산 요약

서브도메인, 열린 발견 항목, 다크 웹 언급, 인증서 만료 예정 건수를 상단에서 확인합니다.

보안 점수 · 등급

도메인 단위 보안 점수와 등급을 제공해 현재 상태를 빠르게 판단할 수 있습니다.

위험 분포 · 주요 위험

심각도별 분포와 우선 확인이 필요한 주요 위험 목록을 함께 확인합니다.

도메인 상세 탭

Overview · 탐지 결과 · 다크 웹 · 인증서 · 보안 점검 탭으로 이동합니다.

외부 자산 탐색

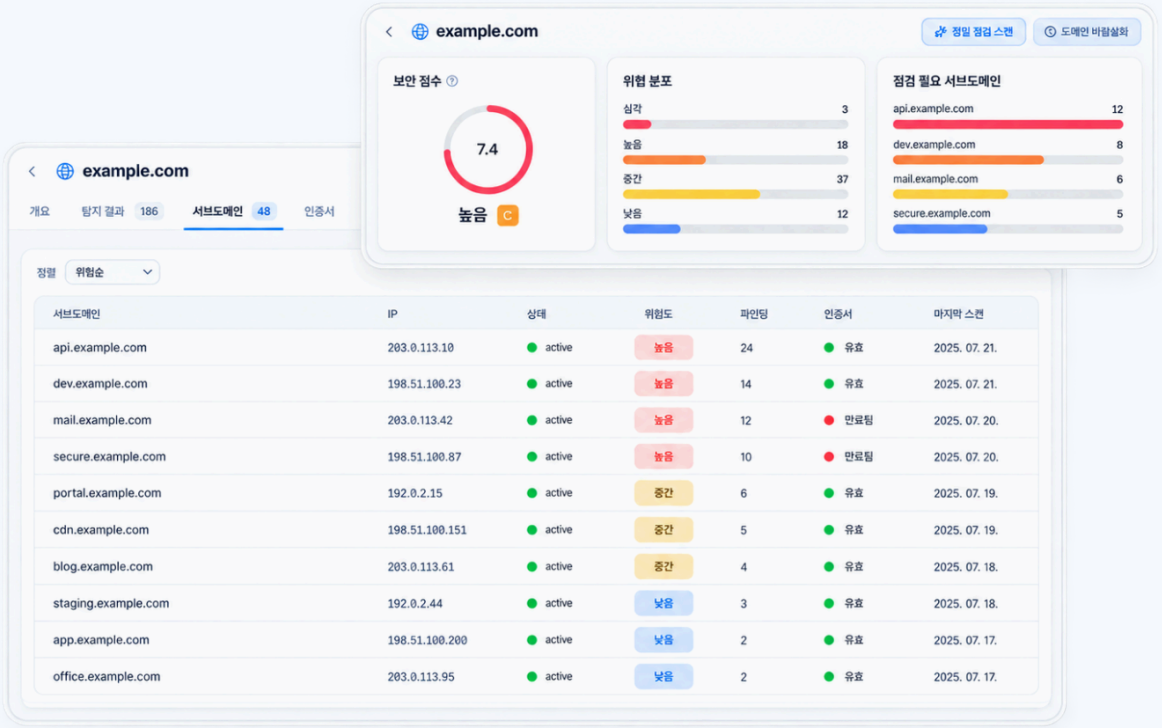
등록한 도메인을 기준으로 **서브도메인을 자동으로 발견**하고, 외부에 노출된 포트와 실행 중인 서비스를 확인합니다. 내부 자산 목록이 아니라 **인터넷에서 실제로 확인되는 자산**을 기준으로 공격표면을 파악합니다.

탐색 대상

- 서브도메인
- 웹 서버
- 공개 포트
- 실행 중인 서비스
- SSL/TLS 인증서
- DNS · WHOIS
- 기술 스택 · 서버 정보

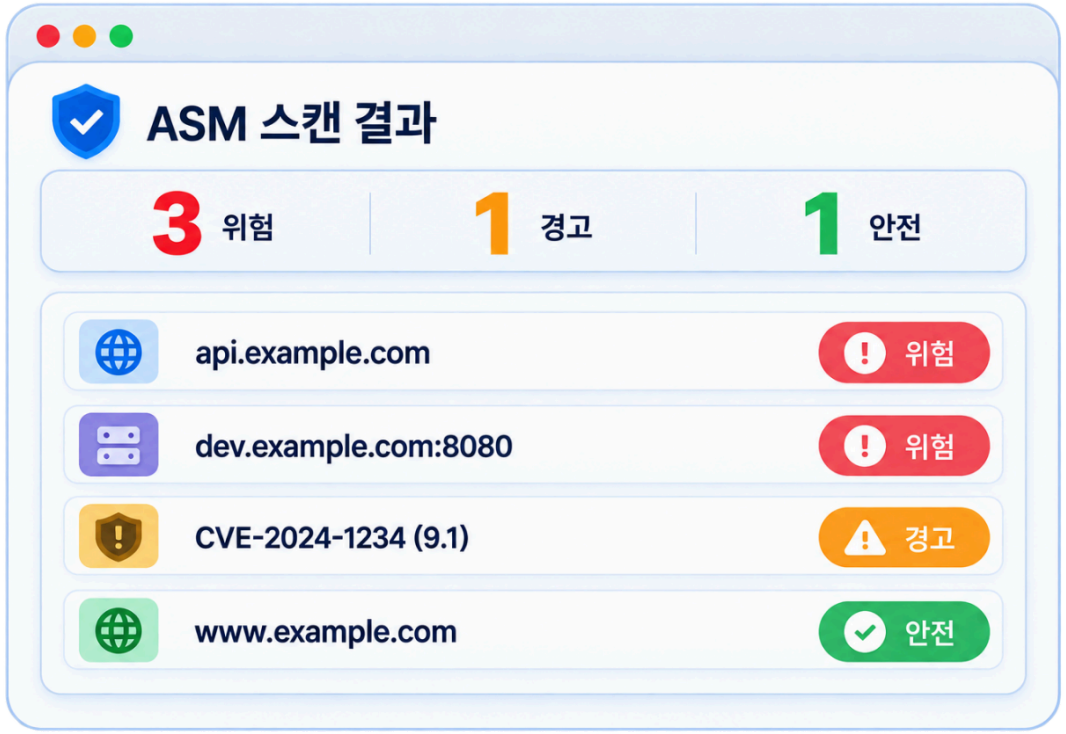
- 도메인 하나를 등록하면 **서브도메인이 자동으로 확장 탐색**됩니다.
- 발견된 자산은 **위험도와 함께 목록**으로 정리됩니다.
- 자산별 **인증서 상태와 만료 예정** 여부를 함께 확인합니다.

IP 주소 단위의 자산 목록 제공 여부는 [담당자 확인 필요]



취약점 진단

발견된 자산의 **알려진 취약점(CVE)과 보안 설정 상태**를 점검하고, 심각도와 함께 제공해 **우선적으로 확인해야 할 위험**을 파악할 수 있습니다.



점검 항목

- 알려진 취약점 · CVE
- TLS · SSL 설정
- 인증서 상태 · 유효기간
- HTTP 보안 헤더
- 공개 포트 · 서비스
- 소프트웨어 · 기술 정보

무료 스캔 결과 등급

- **HIGH** — SSL 만료 · CVE · 취약한 암호화
- **MEDIUM** — 구버전 TLS · 자체서명 인증서
- **INFO** — 기술 스택 · 서버 · 헤더 탐지 정보

다크웹 유출 모니터링

기업 도메인과 연결된 임직원 이메일 및 계정정보가 **외부 유출 데이터나 다크웹에서 발견되었는지** 확인할 수 있습니다. 발견된 계정은 마스킹된 형태로 표시되며, **발견 시점과 출처 구분**을 함께 제공합니다.

01

계정 유출

임직원 계정정보가 유출 데이터에서 발견되었는지 확인합니다.

02

이메일 유출

도메인과 연결된 이메일 주소의 노출 여부를 확인합니다.

03

URL 유출

조직과 연결된 URL이 유출 정보에 포함되었는지 확인합니다.

04

악성코드 감염 신호

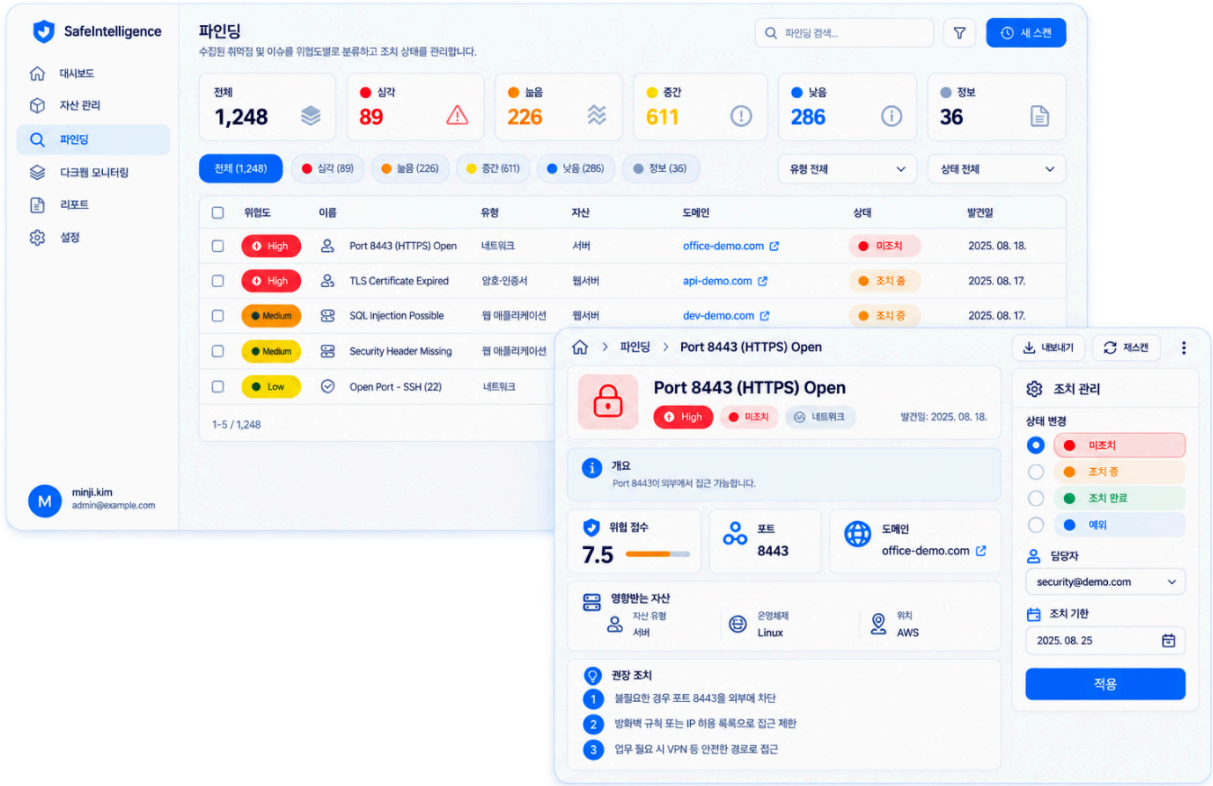
감염 단말에서 수집된 것으로 보이는 정보 노출 신호를 확인합니다.



출처 구분 예시 : stealer logs · breach database · telegram

통합 파인딩 관리

스캔 결과와 다크웹 신호를 **하나의 파인딩 목록**으로 모아 심각도·상태별로 필터링하고, 담당자를 지정해 **조치 상태를 추적**할 수 있습니다.



담당자 지정

발견된 위험을 담당자에게 할당합니다.

처리 상태 추적

미해결 · 처리 중 · 완료 상태를 추적합니다.

우선순위 분류

심각도를 기준으로 확인 순서를 정합니다.

심각도 · 상태 필터

필요한 조건만 골라 목록을 확인합니다.

자산별 위험 확인

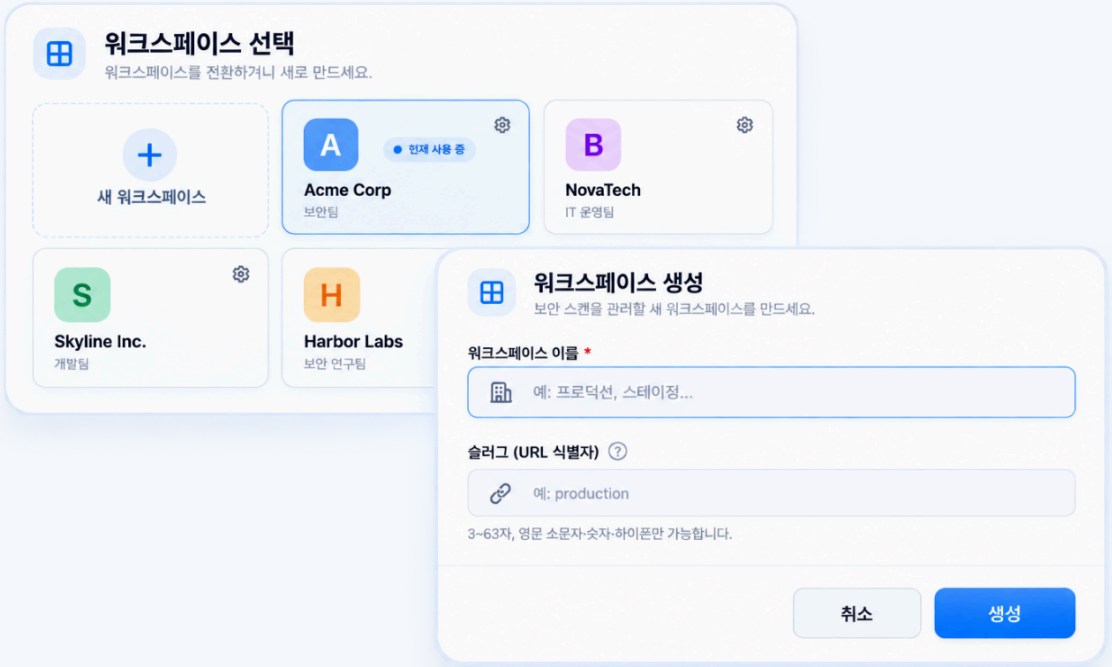
도메인 · 자산 단위로 위험 현황을 확인합니다.

알림

새로운 정보가 확인되면 담당자에게 알림을 제공합니다.

워크스페이스 협업

워크스페이스를 만들고 팀원을 초대해 **같은 데이터를 함께 확인**할 수 있습니다. 권한을 나누어 역할을 분리하고, **빌링을 분리**해 운영할 수 있습니다.



워크스페이스 생성

회사 단위 작업 공간을 만들고 관리할 도메인을 등록합니다.

멤버 초대

보안 담당자와 운영 담당자를 초대해 함께 사용합니다.

권한 관리

관리자 권한을 설정해 역할을 분리할 수 있습니다.

빌링 분리

워크스페이스 단위로 이용 범위를 나누어 운영합니다.

※ 보안 서비스 사업자(MSSP)가 고객사별로 워크스페이스를 나누어 운영하는 방식도 가능합니다. 세부 운영 방식은 [담당자 확인 필요]

03

기능 상세

1 외부 자산 탐색 범위

2 취약점 및 보안 설정 진단

3 다크웹 유출 정보 분류

4 지속 모니터링

5 요금 안내

외부 자산 탐색 범위

조직 내부에서 관리하는 자산 목록뿐 아니라 **인터넷에서 실제로 확인되는 외부 노출 자산**을 기준으로 공격표면을 파악합니다.
도메인 정찰부터 포트 스캔, 인증서·DNS·보안 헤더 점검까지 한 번에 수행합니다.

등록

관리할 도메인 1개

도메인 소유를 확인하는 이메일 인증 후 스캔이 시작됩니다.

기본 점검

- 서브도메인
- 웹 서버
- 공개 포트
- 실행 중인 서비스
- SSL/TLS 인증서
- DNS · WHOIS
- HTTP 보안 헤더
- 기술 스택 · 서버

정밀 점검

- 알려진 취약점(CVE)
- 설정 오류
- 민감 경로

※ 기본 점검은 도메인 정찰·포트 스캔·인증서·DNS·보안 헤더 점검을, 정밀 점검은 발견된 자산 환경에 맞춰 알려진 취약점(CVE)·설정 오류·민감 경로를 점검합니다.

취약점 및
보안 설정 진단

발견된 자산 환경에 맞춰 알려진 취약점을 점검합니다. **CVE, 설정 오류, 민감 경로** 등을 외부 공격자 관점으로 확인하고, 심각도와 함께 제공합니다.

무료 스캔 결과 등급 (공개 정보 기반)

- **HIGH** — SSL 만료 · CVE · 취약한 암호화
- **MEDIUM** — 구버전 TLS · 자체서명 인증서
- **INFO** — 기술 스택 · 서버 · 헤더 탐지 정보

무료 스캔은 도메인 소유 검증 없이 누구나 확인 가능한 공개 정보만 포함합니다.

대시보드 위험 분포 (로그인 후)

- **Critical** — 즉시 확인이 필요한 위험
- **Severe / High** — 우선 조치가 필요한 위험
- **Normal / Low** — 경과 확인이 필요한 항목

두 등급 체계의 공식 통일 표기는 [담당자 확인 필요]

알려진 취약점 CVE	TLS · SSL 설정	인증서 상태 유효기간	HTTP 보안 헤더	공개 포트 서비스	소프트웨어 기술 정보

다크웹 유출 정보 분류

확인된 유출 신호를 **네 가지 카테고리로 분류**하여 추적합니다. 발견 시점과 출처 구분을 함께 제공해 **대응이 필요한 계정을 식별**할 수 있습니다.

계정 유출

임직원 계정정보가 외부 유출 데이터에서 발견되었는지 확인합니다.

이메일 유출

도메인과 연결된 이메일 주소의 노출 여부를 확인합니다.

URL 유출

조직과 연결된 URL이 유출 정보에 포함되었는지 확인합니다.

악성코드 감염 신호

감염 단말에서 수집된 것으로 보이는 정보 노출 신호를 확인합니다.

마스킹 표시

발견된 계정은 **j***@example.com** 형태로 마스킹되어 표시됩니다.

발견 시점 · 출처

유출 확인 일자와 출처 구분(stealer logs · breach database 등)을 함께 제공합니다.

신규 유출 확인

새로운 유출 정보가 확인되면 목록에 추가되고 알림을 제공합니다.

※ 비밀번호 원문 제공이나 복원 기능은 제공하지 않습니다. 유출 여부와 관련 정보를 확인하는 서비스입니다.

지속 모니터링

인터넷에 노출된 자산과 위험은 계속 변화합니다. 한 번의 진단으로 끝나지 않고 **새롭게 발견된 자산과 변경 사항, 새롭게 확인된 취약점과 계정 유출 정보**를 지속적으로 확인할 수 있도록 지원합니다.



신규 자산 발견

새롭게 확인된 서브도메인과 공개 서비스를 확인합니다.

자산 정보 변경

기존 자산의 서비스·설정 변경 사항을 주기적으로 확인합니다.

신규 취약점

새롭게 확인된 취약점과 위험도 변화를 확인합니다.

인증서 상태 변경

인증서 만료 예정과 설정 변경을 함께 확인합니다.

신규 계정 유출

새로운 유출 정보가 확인되면 목록에 추가됩니다.

위험 알림

새로운 정보가 확인되면 담당자에게 알림을 제공합니다.

※ 정기 리포트 및 요약 보고서 기능의 제공 범위는 [실제 제공 여부 확인 필요]

요금 안내

SafeIntelligence는 **루트 도메인 수와 월 제공 크레딧** 기준으로 4개 플랜을 제공합니다. 별도 장비·에이전트 설치 없이 SaaS로 이용하며, **무료 체험**은 공식 홈페이지 무료 스캔으로 먼저 확인할 수 있습니다.

베이직

₩250,000 /월

핵심 자산부터 효율적으로 관리

- 루트 도메인 **3개**
- 월 제공 크레딧 **1,500**

추천

스탠다드

₩500,000 /월

더 많은 도메인과 자산을 지속적으로 관리

- 루트 도메인 **10개**
- 월 제공 크레딧 **15,000**

비즈니스

₩1,000,000 /월

넓은 자산 범위와 강화된 정밀 스캔 제공

- 루트 도메인 **30개**
- 월 제공 크레딧 **37,500**

엔터프라이즈

별도 문의

도메인 수와 점검 횟수를 규모에 맞게 구성

- 루트 도메인 **30개 이상**
- 월 제공 크레딧 **별도 협의**

스캔 크레딧 소비 기준

기본 스캔(Tier 1) 1회당 1크레딧 · 정밀 스캔(Tier 2) 1회당 10크레딧 · 추가 충전 1,000크레딧 = ₩200,000

옵션 상품

다크웹 인텔리전스 프리미엄 — 도메인 1개당 ₩200,000/월 (계정 유출 정보 모니터링 · 알림)

※ 가격 및 조건은 2026년 8월 기준 공식 홈페이지(safeintelligence.biz/pricing) 게시 내용이며 변동될 수 있습니다. 무료 플랜은 제공되지 않습니다.

04

회사 소개

JSecurity 소개

「All for Japan Security」(すべては日本のセキュリティのために) 를 슬로건으로, 기업·기관을 위한 정보보안 제품과 서비스를 개발·판매하고 있습니다. SafeIntelligence는 JSecurity가 제공하는 외부 공격표면 · 다크웹 모니터링 서비스입니다.

회사명	株式会社JSecurity (ジェイセキュリティ)
영문명	JSecurity, Inc.
설립	2018년 1월
자본금	50,000,000엔
대표이사	今村 誉一 (이마무라 요이치)
사업 내용	정보보안 제품 · 서비스의 개발 및 판매
본사	〒105-5117 도쿄도 미나토구 하마마쓰초 2-4-1 세계무역센터빌딩 남관 17층
홈페이지	www.jsecurity.co.jp

SLOGAN

All for Japan Security

すべては日本のセキュリティのために

2018년

일본에서 설립된 정보보안 전문 기업입니다.

50백만엔

자본금 (공식 회사개요 기준)

주요 제품군

MudFix AppCheck DarkWebCheck SECURITY ONE SPAMSNIPER MAILSCREEN PCFILTER GIGAPOD

감사합니다

무료 스캔	safeintelligence.biz
대시보드	dashboard.safeintelligence.biz
사용 가이드	docs.safeintelligence.biz/kr

JSecurity
All for Japan Security

© 2026 JSecurity, Inc. All rights reserved. | 株式会社JSecurity | www.jsecurity.co.jp