ICS Security Monitor · ICS Asset Manager · ICS Scanner

ICS 보안 제품 선택 가이드

우리 제어망에는 무엇이 필요한가 — 기능 범위, 대응 가능한 상황,
단계적 도입 경로와 투자 규모를 하나의 기준으로 비교합니다.

기능 30개 영역 비교 · 상황 26개 대응 비교 · 페인포인트 12건 · 단계적 도입 경로

v1.0 · 2026. 8.

온시큐리티㈜
경기도 하남시 미사강변한강로 135 미사강변스카이폴리스 다동 1038~1039호 · TEL 031-792-0633

목 차

01 이 문서를 읽는 방법 3

02 제품 한눈에 보기 4

03 기능 범위 비교 5

04 상황별 대응 비교 7

05 상황에 맞는 제품 선택 10

06 단계적 도입 경로 11

07 도입 효과와 투자 규모 12

01 이 문서를 읽는 방법

온시큐리티는 산업제어시스템(ICS/OT) 보안 제품 3종을 공급합니다. 각각의 제품은 서로 다른 문제를 해결하도록 설계되었으며, 적용 구간과 운용 방식이 다릅니다.

본 문서는 세 제품을 같은 기준으로 비교해, 「우리 제어망의 어느 구간에 무엇이 필요한가」를 판단할 수 있도록 작성되었습니다. 비교의 근거는 각 제품의 기능 리스트와 제품별 시나리오별 문제해결 방안이며, 기능 유무는 실제 구현 기준으로만 표기했습니다.

▪ 제품 표기

약어	제품명	국문 명칭
ISM	**ICS Security Monitor**	산업제어시스템 통합보안 모니터링 시스템
IAM	**ICS Asset Manager**	산업제어시스템 자산탐지 및 분류관리 시스템
ISC	**ICS Scanner**	제어설비 자동식별 및 관리 시스템

▪ 문서의 구성

장	주제	이 장에서 알 수 있는 것
02	세 제품 한눈에 보기	각 제품이 무엇을 해결하는 제품인지, 누가 쓰는지
03	기능 범위 비교	30개 기능 영역에서 각 제품의 제공 범위
04	상황별 대응 비교	위협 12 · 운영 14개 상황과 페인포인트 12건
05	우리 상황에 맞는 제품	4개 질문으로 도출하는 제품 선택 기준
06	단계적 도입 경로	나눠서 도입해도 총액이 늘지 않는 구조
07	도입 효과와 투자 규모	제품별로 얻는 것과 요금 체계

▪ 표기 규칙

기호	의미	판정 기준
●	**제공**	해당 기능이 제품에 구현되어 기능 리스트에 등재되어 있음
◐	**부분 제공**	유사 기능은 있으나 범위가 제한되거나 다른 방식으로 구현됨
-	**미제공**	해당 제품에 구현되어 있지 않음

※ 모든 금액은 만원 단위이며 VAT 별도입니다. 서비스 등급은 별도 표기가 없으면 Basic 기준입니다.

먼저 알아둘 것

온시큐리티가 제공하는 3 제품은 모두 패시브 수집 방식입니다. 제어망 트래픽을 복제해 분석만 하며, 능동 스캔이나 패킷 주입을 하지 않고 설비에 에이전트를 설치하지 않습니다. 도입 검토 시 「제어 운전에 영향을 주는가」는 세 제품 모두 해당되지 않습니다.

본 제품군은 보안관제(MSSP) 서비스가 아닙니다. 24×7 상시 대응과 침해사고 대응(IR)은 제공 범위에 포함되지 않습니다.

02 제품 한눈에 보기

3 제품의 성격을 같은 항목으로 나란히 놓으면 다음과 같습니다.

구분	ICS Security Monitor	ICS Asset Manager	ICS Scanner
약어	ISM	IAM	ISC
한 문장 정의	제어망 보안 운영을 하나로 통합한 관제 시스템	제어망 자산 가시성과 자산 운영 관리 시스템	설치 없이 노트북으로 수행하는 자산 식별·점검 도구
해결하는 문제	위협을 탐지하고 분석해 조치까지 관리해야 한다	무엇이 있는지 모르고, 관리 책임이 정리되지 않는다	상주 장비를 놓을 수 없는 구간을 확인할 수 없다
운용 방식	상주 · 상시 자동 운용	상주 · 상시 자동 운용	휴대형 · 연결 시 수집
수집 방식	패시브 (미러링)	패시브 (미러링)	패시브 (미러링)
주 사용자	사이버안전센터 · 관제 요원	자산 담당자 · 설비 담당자	점검 수행자 · 진단 인력
적용 구간	전사 통합 관제가 필요한 제어망	자산 관리가 필요한 제어망	독립 · 분리망, 소규모 단독망, PoC
기능 규모	10개 대분류 · 172개 기능	9개 대분류 · 200개 기능	7개 대분류 · 194개 기능
인증	제어시스템 보안 모니터링 구축 가이드라인 대응	GS인증 1등급 (TTA)	GS인증 1등급 (TTA)
공급가 (Lite/단일)	5,000만 원	3,000만 원	1,500만 원

▪ 세 제품의 관계

제품	역할
ISC	점검 도구입니다. 상주 설치가 어려운 구간을 노트북으로 확인하고, 결과를 PDF 리포트로 남깁니다. 전사 도입 전 현황 진단(PoC)에도 쓰입니다.
IAM	관리 시스템입니다. 자산을 상시 식별·분류하고, 물리 배치와 네트워크 구성, 담당자 배정과 인수인계까지 자산 운영 전반을 관리합니다.
ISM	관제 시스템입니다. IAM의 자산 관리 기능을 모두 포함하고, 그 위에 취약점·악성코드 탐지와 위협 스캐닝·상관분석, 이슈 통합 관리를 더해 보안 운영 전 과정을 통합합니다.

ISM은 IAM을 포함합니다 — 선택 기준은 「지금 필요한 단계」입니다

ISM은 IAM의 자산 관리 기능을 모두 포함하고, 그 위에 취약점·악성코드 탐지와 위협 분석, 이슈 통합 관리를 더한 제품입니다. 따라서 IAM을 선택한다고 해서 자산 관리 역량을 포기하는 것이 아니며, ISM으로 확장할 때 IAM의 운영 방식이 그대로 이어집니다.

> 다만 자산 현황이 부정확한 상태에서 ISM을 먼저 도입하면 정책과 탐지의 기준이 서지 않아 효과가 나지 않을 수 있습니다. 「무엇이 더 좋은가」가 아니라 「지금 어느 단계에 있는가」로 판단하시는 것이 맞습니다. 06장에서 설명하듯, 단계를 나누어도 총액이 늘지 않습니다.

03 기능 범위 비교

30개 기능 영역을 여섯 계층으로 나누어 제공 범위를 비교했습니다. 판정은 각 제품의 기능 리스트를 기준으로 하되, 제품에 구현되어 있으나 기능 리스트에 아직 등재되지 않은 항목은 표 아래에 별도로 밝혔습니다.

기능 영역	ISM	IAM	ISC
기반 - 자산과 구성			
자산 자동 식별 (통신 기반)	●	●	●
자산 대장 관리 (등록 · 수정 · 폐기 · Excel)	●	●	◐
자산 상세 정보 (S/W · H/W · 추가 정보)	●	●	-
물리 자산 관리 (시설 · 캐비닛 배치)	●	●	-
네트워크 토폴로지 조회	●	●	●
네트워크 구성도 전용 편집 화면	●	●	-
통신 현황 · 수집 IP 조회	●	●	●
트래픽 통계 (기간 · 자산 · 포트)	●	●	-
정책			
통신 정책 (White/Black · ACCEPT/DETECT)	●	●	◐
IP 주소 · 서비스 포트 목록 관리	●	●	●
정책 다지역 일괄 동기화	●	●	-
취약점 탐지 룰 관리 (Snort)	●	-	-
탐지			
네트워크 이상행위 탐지 (신규 · 비인가 · 자산)	●	●	◐
취약점 탐지 (Snort Community · Custom rule)	●	-	-
악성코드 탐지 (Agentless · Defender 연계)	●	-	-
서비스 포트 사용 탐지	●	●	●
프린터 사용 탐지 · 이력	●	●	-
분석			
패킷 분석 (요청 · 결과 상세)	●	●	◐
외부 PCAP 파일 연계 분석	-	-	●
위협 스캐닝 (자산 기준 이벤트 집계)	●	-	-
네트워크 위협 상관분석 (전파 경로)	●	-	-

기능 영역	ISM	IAM	ISC
관제 · 조치			
통합 대시보드	●	●	◐
이슈 통합 관리 (다수 이벤트 묶음 · 감사 추적)	●	-	-
조치 내용 기록	●	●	-
알림 담당자 배정	●	●	-
보고서 자동 생성	●	●	●
운영 기반			
담당자 인수인계	●	●	-
사용자 · 권한 관리	●	●	●
사용자 로그 · 연동 로그	●	●	-
전사 · 상위 기관 연계	●	◐	-

▪ 비교에서 읽어야 할 세 가지

1. 탐지와 분석의 깊이는 ISM이 압도적으로 넓다

취약점 탐지(Snort Community rule + 제어망 Custom rule), Agentless 악성코드 탐지, 위협 스캐닝과 네트워크 위협 상관분석, 이슈 통합 관리는 ISM에만 있습니다. 「이상 통신을 알아채는 것」을 넘어 「위협인지 판정하고 전파 경로를 추적하는 것」까지 필요하다면 ISM이 유일한 선택입니다.

2. 자산 관리 계층은 ISM과 IAM이 동일하다

자산 식별·분류, 물리 배치, 네트워크 구성도 편집, 통신 정책과 정책 동기화, 담당자 배정과 인수인계, 사용자·연동 로그 — 이 영역에서 두 제품의 제공 범위는 같습니다. IAM은 그 계층까지의 제품이고, ISM은 그 위에 탐지·분석 계층을 더한 제품입니다. 따라서 IAM 선택은 기능을 포기하는 결정이 아니라 도입 순서의 결정입니다.

3. ISC는 기능이 적은 제품이 아니라 다른 제품이다

ISC는 194개 기능을 가진 완결된 점검 도구이며, 외부 PCAP 연계 분석은 3종 중 ISC에만 있습니다. 다만 노트북을 연결하지 않은 시간의 통신은 수집되지 않으므로, 상시 감시가 필요한 구간에는 적합하지 않습니다.

04 상황별 대응 비교

제품별「시나리오별 문제해결 방안」에서 다룬 상황을 하나의 축으로 모아, 같은 상황에 각 제품이 어디까지 답하는지 정리했습니다.

▪ 보안 위협 상황 12 건

상황	ISM	IAM	ISC	비고
제어망에 인가되지 않은 장비가 연결됨	●	●	●	3종 모두 대응. ISC는 점검 시점 기준
등록 자산의 MAC · IP가 변경됨	●	●	●	ISC는 변경 이력으로 회차 간 비교
정책에 없는 통신이 발생함	●	●	◐	ISC는 포트 기준 탐지로 한정
제어망에서 외부 공인 IP로 통신함	●	●	-	ISM · IAM만 상시 탐지
허용되지 않은 서비스 포트가 사용됨	●	●	●	3종 모두 대응
트래픽 급변 · 통신 중단이 발생함	●	●	-	임계치 · 운영 정지 탐지는 상주 제품만
외부 매체를 통해 악성코드가 유입됨	●	-	-	Agentless 악성코드 탐지는 ISM 전용
제어망 내부에서 정찰 · 스캐닝이 발생함	●	-	-	Snort 기반 취약점 탐지는 ISM 전용
하나의 자산에서 위협이 확산됨	●	-	-	위협 스캐닝 · 상관분석은 ISM 전용
제어 문서가 프린터로 무단 출력됨	●	●	-	ISM · IAM만 이력 수집
설계와 다른 통신 경로가 존재함	●	●	●	ISC는 토폴로지로 즉시 시각화
다른 장비가 수집한 트래픽을 검증해야 함	-	-	●	PCAP 연계 분석은 ISC 전용

▪ 운영 업무 14 건

업무	ISM	IAM	ISC	비고
신규 설비를 자산으로 등록	●	●	◐	IAM은 미배정 IP/MAC 목록에서 선택 연결
자산 실사와 대장 현행화	●	●	◐	ISC는 점검 회차 기준 목록화
물리 배치 · 캐비닛 관리	●	●	-	
네트워크 구성도 현행화	●	●	-	구성도 편집 제공
통신 정책 수립과 운영	●	●	◐	
정책을 다수 사업장에 일괄 배포	●	●	-	정책 동기화 제공
오탐 튜닝 (룰 예외처리)	●	-	-	취약점 룰 운영은 ISM 전용
일상 관제 - 이벤트 확인부터 종결까지	●	●	-	ISM은 이슈 단위 통합 관리
정기 보안 보고서 작성 · 제출	●	●	●	ISC는 점검 리포트 4종 PDF
사용자 권한 관리와 접근 감사	●	●	◐	ISM · IAM 모두 사용자 로그 · 연동 로그 제공
담당자 인수인계	●	●	-	담당자별 보유 자산 조회 후 이관 처리
현장 점검 수행과 결과 제출	-	-	●	ISC 전용
점검 구간별 판별 기준 사전 정의	●	●	●	ISC는 스위치 단위 정책 그룹
점검 회차 간 변경분 추적	●	●	●	ISC는 기간 지정 변경 이력 리포트

▪ 대응 범위 집계

구분	ICS Security Monitor	ICS Asset Manager	ICS Scanner
보안 위협 12건	11건	8건	5건 (부분 1건)
운영 업무 14건	12건	11건	4건 (부분 4건)

운영 업무는 ISM과 IAM의 대응 범위가 사실상 같고, 차이는 위협 대응에서 갈립니다(ISM 11건 · IAM 8건). ISC는 두 축 모두에서 「점검 시점 기준」으로 답하므로 건수만으로 비교하기보다 적용 구간으로 판단하는 것이 적절합니다.

▪ 자주 듣는 문제 제기와 해당 제품

제품별 시나리오 문서의 Part C(고객 지원)에서 다룬 문제 제기를 모아 정리했습니다.

문제 제기	ISM	IAM	ISC	해결 방식
"제어망에 무엇이 연결되어 있는지 모른다"	●	●	●	3종 모두 실측 통신 기반으로 자산을 식별. 상시 운용이면 ISM·IAM, 구간 점검이면 ISC
"자산 대장이 현실과 얼마나 다른지 모른다"	●	●	◐	미확인 IP·미배치 자산을 대시보드에 상시 표시. ISC는 점검 회차 기준 목록화
"폐쇄망이라는데 증명할 방법이 없다"	●	●	-	공인 IP 통신을 상시 감시하고 기간별 보고서로 「외부 통신 없음」을 입증
"실태점검 자료를 매번 새로 만든다"	●	●	◐	자산 현황·물리 배치·구성도·정책이 상시 축적되어 발행만 하면 됨. ISC는 점검 리포트 4종
"사고가 나도 원인을 추적할 수 없다"	●	-	-	패킷 분석과 위협 상관분석으로 전파 경로 재구성, 이슈에 조치 이력 축적 — ISM 전용
"설비가 어디 있는지 찾는 데 시간이 걸린다"	●	●	-	시설·캐비닛 배치와 논리 자산 정보를 연결해 현장 확인 동선을 사전 계획
"담당자가 바뀌면 관리가 끊긴다"	●	●	-	담당자별 보유 자산 조회, 인수인계 처리, 알림 담당자 배정과 조치 기록 축적
"본사와 사업소 현황이 따로 논다"	●	●	-	정책 다지역 동기화와 통합 대시보드. 본사에 동일 제품을 배치해 전사 통합
"상주 장비를 놓을 수 없는 구간이 있다"	-	-	●	노트북 한 대로 수집·판별·리포트까지 수행. 설치 승인 절차 불필요 — ISC 전용
"전사 도입 전에 효과를 확인하고 싶다"	-	-	●	실제 제어망에서 미승인 장비·포트 사용·통신 구조를 데이터로 산출 — ISC 전용
"보안 시스템이 제어 운전에 영향을 줄까 걱정된다"	●	●	●	3종 모두 패시브 수집. 능동 스캔·패킷 주입·에이전트 설치 없음
"한 번에 다 하기에는 예산이 부담된다"	◐	●	●	ISC 진단 → IAM → ISM 순으로 확장. 단계를 나눠도 총액이 늘지 않음 (ISM은 최종 단계)

05 상황에 맞는 제품 선택

아래 네 가지 질문에 답하면 적합한 제품이 좁혀집니다. 위에서부터 순서대로 판단하시면 됩니다.

	질문	예	아니오
1	해당 구간에 상주 장비를 설치할 수 있습니까?	2번으로	ISC (종료)
2	제어망 자산 현황이 실측 데이터로 확인됩니까?	3번으로	IAM 선행 도입
3	취약점·악성코드 탐지와 위협 분석·이슈 관리가 필요합니까?	4번으로	IAM
4	이번 예산으로 ISM 도입이 가능합니까?	ISM	IAM 도입 후 업그레이드

※ ISM은 IAM의 자산 관리 기능을 모두 포함하므로, 2번·4번의 「IAM 선행」은 기능을 포기하는 선택이 아니라 도입 순서의 문제입니다.

▪ 적용 구간별 권장 조합

구간	권장	이유
발전 제어망 (주요 호기)	**ISM**	상시 관제와 위협 분석, 가이드라인 대응이 함께 요구되는 구간
발전본부 · 사업소 자산 관리	**IAM**	자산 현황과 담당 배정, 구성 관리가 주 과제인 구간
신재생 (태양광 · 풍력) 단지	**ISC, ISM(SMB, Lite)**	전사 네트워크에 연결되어 있는 소규모 제어망으로 자산이 적고 관리 효율성 때문에 외부 연결 가능성 높은 구간
CCTV · 기타 분리망	**ISC**	분리.단독망으로 상주 설치가 어렵고 자산 현황 파악 자체가 목적인 구간
전사 도입 검토 단계	**ISC, IAM(SMB), ISM(SMB)**	실제 제어망에서 현황을 진단해 도입 범위를 정하는 단계
본사 통합 관제	**ISM 또는 IAM**	두 제품 모두 정책 동기화와 통합 대시보드 제공. 위협 분석까지 필요하면 ISM

한 사업장에 하나만 골라야 하는 것은 아닙니다

주요 호기에는 상주 제품을 두고, 연결된 신재생 단지는 ISM(SMB, Lite) 모델을 적용하여 보안 모니터링을 강화하거나 ISC 를 적용하여 간단 점검하고, CCTV 등 분리 구간은 ICS Scanner로 주기 점검하는 조합이 일반적입니다. 구간 성격에 맞춰 배치하면 전 구간을 커버하면서도 투자 규모를 조절할 수 있습니다. 만약, 상주 장비를 설치할 수 있으나 도입 예산이 부족할 경우에는 ISM 또는 IAM의 Lite와 SMB 모델을 검토할 수 있습니다.

06 단계적 도입 경로

한 번에 전체 체계를 구축하기 어려운 경우, 아래 순서로 나누어 도입할 수 있습니다.

단계	제품	이 단계에서 확보하는 것	다음 단계로 넘어가는 시점
1단계	**ISC**	실제 제어망의 자산 현황과 통신 구조를 데이터로 진단. 상주 도입이 필요한 구간을 특정	진단 결과로 도입 범위와 예산 근거가 확보되었을 때
2단계	**IAM**	자산 상시 식별·분류, 물리 배치, 네트워크 구성도, 통신 정책 수립·동기화, 담당 배정과 인수인계 운영	자산 관리 체계가 정착하고 위협 탐지 요구가 생겼을 때
3단계	**ISM**	2단계의 자산 관리 기능을 그대로 유지한 채 취약점·악성코드 탐지, 위협 스캐닝·상관분석, 이슈 통합 관리 추가	—

▪ 나눠서 도입해도 총액이 늘지 않습니다

ICS Asset Manager를 먼저 도입한 뒤 ICS Security Monitor로 업그레이드하는 경우, 업그레이드 비용은 전 모델 공통 2,000만 원입니다. 이는 두 제품의 공급가 차액과 정확히 같습니다.

모델	IAM 공급가	업그레이드	합계	ISM 직접 도입	차이
Lite	3,000	2,000	5,000	5,000	동일
SMB (PC)	5,000	2,000	7,000	7,000	동일
SMB (Server)	7,000	2,000	9,000	9,000	동일

※ 단위: 만원, VAT 별도. 업그레이드는 동일 인프라에서 소프트웨어 업그레이드로 진행되므로 하드웨어를 다시 구매하지 않습니다.

> **이것이 의미하는 것**
>
> 「나중에 확장할 거면 처음부터 상위 제품을 사는 게 낫다」는 판단을 하지 않아도 됩니다. 자산 현황이 부정확한 상태에서 상위 관제 시스템을 도입하면 정책도 탐지도 기준이 서지 않으므로, 자산 가시성을 먼저 확보하는 순서가 오히려 효과적입니다. 그리고 그 선택에 금전적 손해가 없습니다.

07 도입 효과와 투자 규모

제품별로 도입 후 달라지는 것과, 그에 필요한 투자 규모입니다.

▪ 제품별 도입 효과

제품	도입 전	도입 후
ISC	분리망 구간에 무엇이 연결되어 있는지 확인할 수단이 없고, 점검 결과가 담당자 문서로만 남는다	노트북 연결만으로 통신 장비가 목록화되고, 승인·미승인 판별과 변경 이력이 PDF 리포트로 축적된다
IAM	자산 대장이 문서 기준이라 현실과 얼마나 다른지 알 수 없고, 관리 책임과 구성 정보가 개인 파일에 흩어져 있다	실측 통신이 대장의 근거가 되고, 물리 배치·구성도·담당 배정·인수인계가 시스템에 축적된다
ISM	자산은 관리되지만 이상 통신이 위협인지 판정할 수 없고, 사고 후 전파 경로를 재구성할 방법이 없다	IAM의 자산 관리를 그대로 유지한 채 취약점·악성코드가 탐지되고, 위협 상관분석으로 전파 경로가 나오며, 조치 이력이 이슈로 감사 추적된다

▪ 요금 체계

제품	모델	공급가	연 유지보수료	구독 3년	구독 5년
ICS Scanner (ISC)	단일 모델 (노트북)	1,500	150	640	460
ICS Asset Manager (IAM)	Lite (~100 IP · PC)	3,000	300	1,270	930
	SMB (~300 IP · PC)	5,000	500	2,120	1,540
	SMB (~300 IP · Server)	7,000	700	2,960	2,160
	Enterprise (Unlimited · Server)	협의	협의	협의	협의
ICS Security Monitor (ISM)	Lite (~100 IP · PC)	5,000	500	2,120	1,540
	SMB (~300 IP · PC)	7,000	700	2,960	2,160
	SMB (~300 IP · Server)	9,000	900	3,810	2,780
	Enterprise (Unlimited · Server)	협의	협의	협의	협의

※ 단위: 만원, VAT 별도. 서비스 등급 Basic 기준. 소유형 연 유지보수료는 2년차부터 적용되며「공급가 × 등급 요율(Basic 10% · Standard 15% · Premium 20%)」입니다. 구독형은 사용권과 유지보수를 통합해 연 단위로 선납합니다. ICS Scanner는 Basic 등급 전용입니다.

▪ 계약 형태 선택

형태	특징	적합한 경우
소유형	도입 시 공급가를 지급하고 소유권이 고객에 귀속. 1년차 무상지원 포함, 2년차부터 연 유지보수료	자산 취득이 필요하거나 자본예산 집행이 가능한 경우
구독형 3년 · 5년	사용권과 유지보수를 통합해 연 단위 선납. 초기 투자 없이 SLA 즉시 적용. 약정 기간 종료 후 소유권 고객 귀속	초기 투자 부담을 줄이고 운영예산으로 집행하려는 경우

▪ 유지보수 서비스

항목	Basic	Standard	Premium
지원 시간	평일 09–18시	평일 09–18시	평일 09–18시
정기 방문 점검	연 1회	연 2회	연 4회
패치 제공	연 2회	연 2회	연 2회
오탐 튜닝 · 정기 리포트	방문 시 수행	방문 시 수행	방문 시 수행
원격 정기 점검 (C2 원격형)	반기 1회	분기 1회	월간 1회

항목	Basic	Standard	Premium
등급 요율	10%	15%	20%

※ 제품 하자 수정 · 장애 현장 출동 · 기술 문의 대응은 등급과 무관하게 전 계약에 동일 제공됩니다. 운영서비스(원격지원)는 계약 형태·등급과 무관하게 별도 요금 없이 제공됩니다. ICS Scanner는 Basic 등급 전용이며, 정기 방문 점검과 방문 시 수행 항목(오탐 튜닝·정기 리포트·자산/취약점 리포트) 일체, 운영서비스가 제공되지 않습니다.

CONTACT

제품 · 견적 문의

주소 (우) 12902 경기도 하남시 미사강변한강로 135(망월동) 미사강변스카이폴리스 다동 1038~1039호

대표전화 031-792-0633 · Fax 031-792-0635

이메일 info@onsecurity.co.kr

홈페이지 www.onsecurity.co.kr