

다. 인도네시아

'18년 GDP(십억달러)	1,048.53
'18년 인구수(천명)	263,000

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 인도네시아의 사이버보안 지수는 한국보다 낮으며, 중상위권 그룹에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
인도네시아	0.776	41	0.424	70	+0.352	+29
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 인도네시아의 전반적인 ICT 발전 수준 중위권을 유지하고 있음

지표명	인도네시아		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	32	-	28
IMD 디지털경쟁력지수(2019)	-	56	-	10
UNCTAD 전자상거래지수(2019)	50.1	84	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.776	41	0.873	15
UN 전자정부 지수(2018)	0.525	107	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 인도네시아의 유선통신 이용률 및 보급률은 하위권, 이동통신은 중상위권 수준을 유지

항목	인도네시아		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	11,208	4.19	25,907	50.63
유선브로드밴드	8,781	3.28	21,286	41.60
이동통신	320,770	119.84	66,356	129.67
인터넷 이용률	39.79%		95.90%	

정보보호 산업 개요

1) 보안 환경

정보보안 환경

- ▶ ITU가 발표한 '글로벌 사이버보안(GCI) 2018'에 따르면 인도네시아의 사이버보안 지수는 0.776으로 전체 194개국 중 41위에 올랐으며 아시아·태평양 권역에서는 9위를 기록
 - 동 지수는 법적·기술적·조직적 대응, 역량 강화, 국제협력 등 5개 부문을 종합 평가한 것
 - 전년도 실적(사이버보안 지수 0.424, 167개국 중 70위, 아태 지역 내 16위)에 비해 크게 발전

- ▶ Digital 2019 Reports에 따르면, 인도네시아는 인터넷 사용 인구 증가에 있어서 인도·중국·미국에 이어 세계 4위이며 그만큼 관련 위협도 상당한 것으로 분석
 - 2018년 한 해 동안 인도네시아에서 감지된 사이버공격은 2억여 건으로 빈약한 사이버 시스템으로 인해 사이버 공격에 대한 노출 빈도가 증가
 - 주요 공격 형태는 해킹이며, 국방부나 통신업체 등 정부 및 기업 웹사이트가 주요 표적
 - 2017년 워너크라이 랜섬웨어 공격 당시 인도네시아 내 대학, 제조업체, 병원 등 12개 조직이 공격당함
 - 최근 조사에 따르면 인도네시아 내 조직의 49%가 사이버공격을 경험했으며, 2018년 Frost & Sullivan는 사이버 공격으로 인한 인도네시아 기업의 직·간접 손실액에 대해 ▲대기업은 최대 670만 달러 ▲중기업은 33,500 달러로 집계
 - 'Norton Cybersecurity Statistics Report'의 2017년 보고서에 의하면, 인도네시아 성인 중 사이버범죄의 희생자 수는 5,945만 명(세계 9위)으로 사이버범죄에 대한 낮은 인식 수준이 주요인

- ▶ 인도네시아 국가사이버안호청(BSSN)은 전국 6개 주에 설치된 21개 센서(HoneyNet)를 통해 수집된 데이터를 기반으로 '2018년 인도네시아 내 사이버공격 실태'에 대한 연간 보고서를 발표
 - 사이버 공격은 연평균 15%씩 증가하고 있으며, 공격을 가장 많이 자행한 국가는 러시아(259여 건), 중국(187여 건), 미국(1,42만 여 건)의 순
 - 한편 2019년 대선 기간 중 총선위원회(General Election Commission) 서버를 대상의 사이버 공격 시도는 2,880만 건
 - 통신정보기술부(KOMINFO)에 따르면, 2019년 인도네시아령 파푸아(Papua)·웨스트파푸아(West Papua) 지역 내 반정부 소요사태와 관련한 거짓정보가 ▲소셜미디어를 통해 20여 개국으로 확산

- ▲사용된 URL은 약 55만 5,000개 ▲확산자 역할을 한 계정의 수는 10여만 개로 추산
- 이에 따라 정부는 8월 21일부로 해당 지역의 인터넷 액세스 제한 조치를 단행

물리 보안 환경

- ▶ 글로벌 인증기관 UL(Underwriters Laboratories)이 발표한 'UL Safety Index(2018)'에서 인도네시아는 66점(글로벌 평균 60점)로 187개국 중 71위(전년 81위)를 기록
 - 구체적으로 ▲기관 및 자원(Institutions & Resources) 부문 52점 ▲안전 체계(Safety Framework) 부문 60점 ▲장애나 사망 추정치 등, 안전 관련 수치(Safety Outcomes) 부문 93점
 - UL Safety Index에 따르면, 인도네시아의 교통 상해의 주원인은 보행자·오토바이·트럭 사고 등이이며, 작업장 내 위험으로부터의 인력 보호 면에서 저조한 것으로 분석
- ▶ 미 해외안보자문위원회(OSAC)의 'Indonesia 2019 Crime & Safety Report: Jakarta'에서는 2018년 자카르타 경찰은 강간 31건, 가중폭행 801건, 강도 1,584건, 절도 637건, 차량 절도 1,226건을 보고
 - 2018년 총 범죄 건수는 32,301 건으로 전년(총 34,227건) 대비 5.62 % 감소한 반면, 범죄 해결 건수는 28,316건으로 전년(총 27,084건) 대비 4.54% 증가
 - 하지만 피해자가 신고를 꺼리는 분위기를 감안할 경우 실제 범죄율은 훨씬 높을 것으로 추정
- ▶ 한편 갤럽의 전 세계 142개국 거주자들을 대상으로 조사한 '2018 Law and Order Report'에서 인도네시아는 총 89점을 기록해 높은 수준의 법률 및 질서를 가진 국가 9위를 차지
 - 동 보고서는 조사 대상자의 거주 지역 경찰에 대한 확신, 거주 지역 내 야간 도보의 안전성, 최근 12개월 내 재산 도난 경험 등에 근거해 조사
- ▶ 테러 사건 빈도는 정점에 이르렀지만, 이슬람 극단주의의 영향력 증대로 관리에 난항이 예상됨
 - 2019년 5월 22일 대선 결과 발표 전후로 이슬람국가(IS) 추종세력에 의한 테러 가능성이 고조되었으며, 검거된 용의자는 대부분은 IS 연계 현지 테러조직 '자마 안샤룻 다올라(JAD)'의 조직원들로 판명
 - 2019년 5월 쉘 자바 주 등에서 검거된 JAD 조직원들의 경우, 2015년 프랑스 파리 연쇄 테러 및 2016년 벨기에 브뤼셀 테러에서 사용된 고성능 폭발물질 TATP(트리아아세톤 트라이페록사이드)를 소지

전자상거래 환경

- ▶ 세계 4위 인구 대국인 인도네시아는 서남아시아의 B2C 전자상거래 시장의 선두주자이며, 현재 모바일 쇼핑 및 디지털 결제수단 활성화로 전자상거래시장이 역동적 성장을 구가
 - 주목할 만한 트렌드로는 모바일상거래(M-Commerce)의 성장을 들 수 있으며,, Katadata Insight Center에 따르면 전자상거래 플랫폼 접속 수단 중 스마트폰이 94%를 차지
 - 2018년 기준 인도네시아 전자상거래 시장 규모는 110억 유로로, 그 중 모바일상거래 부문이 60.2%를 차지하고 있는데 이는 영국(41.0%) 및 미국(39.6%)보다 높은 수치
 - 한편 Google 및 Tamaseck은 2025년 인도네시아의 전자상거래 시장이 연평균 23.4% 증가해 460억 유로(530억 달러)에 달할 것으로 추정
- ▶ 2018년 9월 기준, 결제 수단은 계좌이체(69%), 현금결제(22%), 온라인뱅킹앱을 통한 신용/직불(12%), GoPay · Mandiri E-Money · T-Cash 등의 디지털 지갑(11%) 순으로 나타남
 - 2018년 2분기 디지털 결제서비스 보급률은 46%였으며, 2020년 모바일 결제 시장은 280억 유로에 달할 것으로 전망
- ▶ 전자상거래 관련 현지 자료에 의하면, 인도네시아는 전자상거래 산업 보안 순위가 15개 국가 중 14위
 - 결제 사기 · 신규계정 사기 · 계정탈취 사기 등 전자상거래 관련 사기가 빈발하며, 산업 발전을 위해서는 사이버 범죄에 대한 국민 의식 제고 및 보안 강화가 절실

2) 인터넷 및 통신 환경

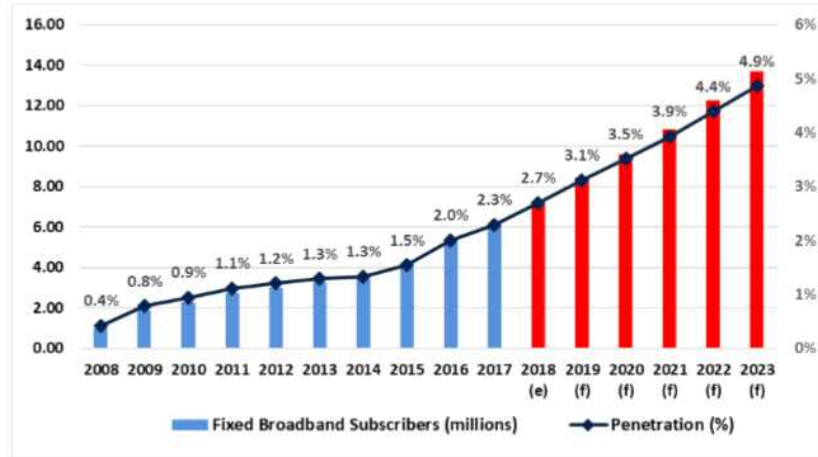
▶개요

- ITU에 의하면 2017년 기준 ▲인구의 99%가 모바일을 보유 ▲3G 네트워크 이용률은 93.8% ▲4G(LTE/WiMax)는 90.4% ▲컴퓨터 보유 가구 비율은 19.1% ▲인터넷 연결된 가구 비율은 57.3%
- yStats에 따르면 2018년 기준 인터넷 보급률은 42%로서 2022년에는 53%로 확대될 전망
- 2018년 인터넷 트래픽의 67.5%가 모바일폰에서 발생, 그 뒤를 이어 데스크톱(31.2%), 태블릿 1.2%
- 17,000여 개의 섬으로 구성된 인도네시아는 지리적 특성상 유선통신 인프라 구축이 어려우며, 브로드밴드 개발이 촉진되고 있음에도 고정 광대역 연결성은 2019년 기준 3%로 상대적으로 저조

▶유선 전화

- 유선 전화는 모바일 및 모바일 브로드밴드의 확산으로 꾸준히 감소하는 추세
- 유선 전화 이용자 수는 2012년 3,800만 명에서 2018년 1,630만 명으로 급감했으며 보급률은 4%

그림 _ 유선 브로드밴드 가입자 수와 보급률 전망(2008년~2023년)



[출처] Buddecomm(2019)

- 유선 회선 수 제한 및 모바일 플랫폼의 강제로 유선 브로드밴드 보급률이 상대적으로 저조
- 2018년 유선 브로드밴드 예상 가입자 수는 719만 명, 보급률은 2.7%로 전년 대비 19% 성장
- 시장 성장 동력은 FTTH 부문이며, 현재 Axiata · Biznet · Telkom Indonesia 등이 FTTH 서비스를 개시

▶이동통신

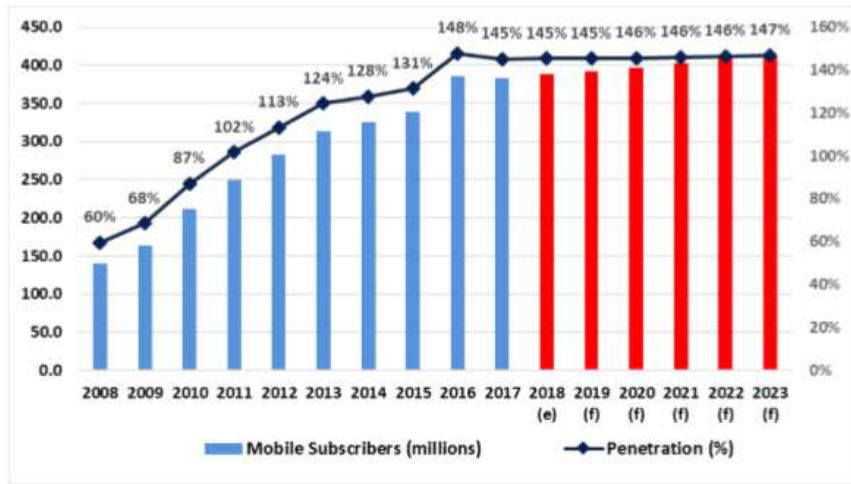
- 인도네시아 내 모바일 사업자는 Telkomsel, Indosat, XL Axiata, 3 Indonesia, SmartFren 등 7개사
- 상위 4개 업체가 시장의 약 90%를 점유하고 있으며, 그 중 Telkomsel의 가입자 수는 1억 9,300만 명(시장 점유율 50.4%)으로 전년에 이어 1위

표 _ 모바일 사업자 및 시장 점유율(2018년)

Operator	Subscribers (million)	Market Share
Telkomsel	193	50.4%
Indosat Ooredoo	64.1	16.7%
XL Axiata	52.9	13.8%
3 Indonesia	58	15.1%
SmartFren	10	2.6%
Bakrie Telecom	1	0.3%
Internux (Bolt)	3.9	1.0%
Total	382.9	100.0%

[출처] Buddecomm(2018)

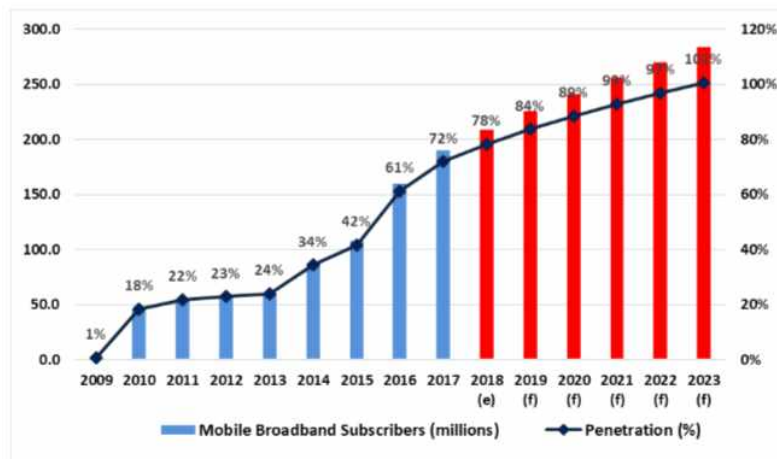
그림 _ 모바일 가입자 및 보급률 전망(2008년~2023년)



[출처] Buddecomm(2019)

- 모바일 가입자 및 보급률은 2016년을 정점으로 성장세가 다소 주춤한 상태
- 2018년 예상 가입자 수 3억8,750만 명, 보급률 145%로 전년 대비 1.2% 성장
- 2019년~2023년까지 향후 5년 동안에도 연평균 성장률은 1.3%로 성장 둔화가 이어질 전망
- 한편 시장의 성장은 4G 및 5G 서비스에 의해 견인될 것으로 예상

그림 _ 모바일 브로드밴드 가입자 및 보급률 전망(2009년~2023년)



[출처] Buddecomm(2019)

- 모바일 브로드밴드 가입자 수 및 보급률은 2013년 이후 매년 급성장
- 2018년 모바일 브로드밴드 예상 가입자 수는 2억900만 명, 보급률 78%로 전년 대비 61.8% 성장

- 모바일 브로드밴드 시장은 아직 초기단계에 있으며, 이를 감안할 때 2019년~2023년까지 향후 5년 동안 연평균 6.3%의 높은 성장세를 보일 것으로 전망
 - 현재 4G 모바일 서비스를 제공하는 모바일 브로드밴드가 강세이며, 이것이 유선 브로드밴드를 대체하는 추세
-

정보보호 시장 현황

1) 시장 규모

시장 개요

- ▶ 인도네시아는 중산층 증가와 함께 스마트폰 및 인터넷 사용자가 급증하고 있으며, 통신 네트워크 인프라 투자가 확대되면서 동남아시아 국가 중 가장 주목받는 정보통신 시장으로 부상
 - BMI에 따르면 2018년 인도네시아의 ICT 지출은 총 117억 달러 규모로, 부문별로는 ▲소프트웨어는 2018년 15억 달러(2022년 29억 달러) ▲IT 서비스는 68억 달러(2022년 118억 달러) ▲컴퓨터 하드웨어는 33억 달러(2022년 40억 달러)로 증가세를 이어갈 전망
 - 한편 IDC는 2019년 인도네시아의 ICT 지출 규모를 332억 달러 규모로 추산했으며, 2022년에는 인도네시아 보안 경보 장비의 10%가 인공지능에 의해 구동될 것으로 전망
 - 인프라 부문에서는 위성 및 지상국, 광섬유 케이블 및 액세서리, 라스트 마일(3G 및 LTE 기지국, 기지국 제어기), IT 네트워크 장비, 모니터링 시스템·SCADA·NMS 등에서 수요가 커질 것으로 예측
- ▶ Frost & Sullivan은 2022년 인도네시아의 ICT 부문별 시장 규모와 관련해 사이버보안 4억 8,79만 달러, 디지털 서비스 95억 2,840만 달러, 이동통신 225억 3730만 달러로 전망

그림 _ 인도네시아 ICT 전체 시장 규모 추이(2017년~2022년)



[출처] Frost & Sullivan Indonesia Market Tracker, Statista(2018)

- 부문별 핵심 영역은 ▲사이버보안은 컨설팅 및 자문 서비스, 네트워크 보안 ▲디지털 서비스는 유료TV, 핀테크, 클라우드 ▲이동통신은 4G 연결성, 고정 무선접근 연결성
- ▶ 인도네시아의 ICT 전략 로드맵은 '국가개발플랜 2005-2025(National Development Plan 2005-2025)'의 일환으로, 국가 연결성 강화를 통한 경제 및 인프라 개발이 목적
- ICT 전략 로드맵은 인프라 및 보안, 채택 및 창조적 활용, 규제 및 법률, 펀딩 등 4개 축으로 구성

표 _ 인도네시아 ICT 전략 로드맵(2005-2025)의 부문별 핵심 목표

부문	핵심 목표
인프라 및 보안	<ul style="list-style-type: none"> • 2019년 고정브로드밴드 보급률을 도시 가구의 71%, 농촌 가구의 49%로 증대 • 고정브로드밴드 속도를 도시 지역은 1Mbps, 농촌지역은 10Mbps로 제고
채택 및 창조적 활용	<ul style="list-style-type: none"> • 2020년까지 800만 개 SMEs의 디지털화 달성 • 정부 네트워크 연결(e-government)
규제 및 법률	<ul style="list-style-type: none"> • 패시브 네트워크 공유 협정 확정 • 2016년 CDMA 셋다운 및 3G/4G 개발과 관련한 스펙트럼 관리
펀딩	<ul style="list-style-type: none"> • 인도네시아 브로드밴드 개발 플랜(IBP)의 핵심인 Palapa Ring 프로젝트 완료 • 충분한 수익 스트림 창조를 통한 자본비용(정부 투자 15억 달러) 회수

[출처] Frost & Sullivan(2018)

- ▶ 인도네시아는 모바일 인터넷 사용률이 높음에도 사이버보안 솔루션 시장의 규모는 작은 편
 - 많은 조직들의 경우, 아직 정교한 사이버안보 솔루션 실행과 관련한 투자 및 스킬이 부족
 - Gartner에 따르면 인도네시아는 GDP의 약 1.6%를 디지털 인프라 구축에 사용하고 있으며, 이는 인접국(싱가포르 6.6%, 말레이시아 4.5%)에 견주어 낮은 수치
 - 2019년부터 5년간 ICT 지출을 GDP의 2.5%로 늘이고, 특히 네트워킹 · 보안 · 클라우드 · 데이터분석 등 10개 트렌드에 194억 7,000만~212억 4,000만 달러의 투자가 필요
 - 인도네시아 내 ICT 및 소프트웨어의 60%는 외국산이며 자국 기업과 공동개발된 제품은 30% 정도로, 순수 인도네시아産 기술 및 솔루션은 소수에 불과
- ▶ 2017년 8월 정부는 전자상거래 육성을 위해 '국가 전자상거래 체계 로드맵 2017-2019 (Roadmap for the National Electronic Commerce System for 2017-2019)'을 대통령령(2017년 제74호)으로 공표
 - 동 로드맵을 통해 전자상거래 운용 지침을 제시하고 있으며, 사이버보안 항목도 포함

표 _ 전자상거래 로드맵 주요 내용

자금 지원	▲자금 지원 및 대부, 자금 조달 계획 ▲양여금, 자금 지원, 보조금 계획 ▲양여금, 자금 지원 조달 대체 방안 ▲대체자금 지원 및 클라우드 펀딩 계획 ▲전자상거래 관련 정보통신 및 금융 분야 투자제한 리스트에서 해지 등
세금	▲납세의무 간소화 ▲전자상거래 비즈니스의 등록 절차 및 가이드라인 작성 ▲해외 전자상거래 기업에도 동등한 조세 부과 도모
소비자 보호	▲전자상거래에 대한 정부 규정 제정 ▲소비자 신뢰 구축 ▲인도네시아의 전자상거래에 대한 통합 결제 시스템(National Payment Gateway) 구축
교육 및 인적자원	▲소비자와 중소기업, 전자상거래 기업, 정책입안자를 위한 교육 프로그램 구축 ▲스타트업 인큐베이션 프로그램 제공 기관 설립 ▲전자상거래 교육 지원인력 양성 등
물류	▲물류 인프라 향상 ▲낙후지역 물류 시스템 개선 ▲물류 서비스 역량 강화 ▲중소기업을 위한 전자상거래 물류 시설 이전 등, 전자상거래의 발전에 따라 물류 서비스 공급자 증대
인프라	▲ICT 인프라 개선
사이버보안	▲전자상거래를 위한 사이버 범죄 감독 시스템 개발 ▲2018년까지 각 전자상거래 기업의 시스템 지원 요건 충족을 통해 전자상거래 보안성 향상
책임 기구	전자상거래 책임관리위원회 설립

- ▶ 물리 보안 영역에서는 테러 등 사회 불안 요소의 증가로 상업 및 공공 안전 제고에 역점을 두고 있으며, 안전 및 보안 장비에 대한 수요가 경찰청 등 정부 기관을 중심으로 민간으로 확대되는 추세
 - 특히 사물인터넷(IoT)은 보안 관련 핵심 기술로서, IDC는 2019년 인도네시아 지방 정부의 20%가 도로, 가로등, 신호등 등의 인프라를 IoT로 구현할 것으로 전망

시장 규모 및 전망

- ▶ Barnes Reports에 따르면, 2018년 인도네시아의 보안 시스템 서비스 시장은 약 13억1,600만 달러 규모
 - 부문별로는 ▲보안 시스템 서비스 8억 6,420만 달러 ▲도난경보 및 모니터링 4억 2,770만 달러 ▲보호 및 보안 장치 6,000만 달러 ▲감시 시스템 3,400만 달러 ▲화재 경보 및 모니터링 3,000만 달러 규모를 형성
 - 보안 시스템 서비스 관련 기업은 총 29,287개로서 총 고용 인력은 142,243여 명
 - 한편, 2018년도 인도네시아의 경비 및 순찰 서비스 시장 규모는 41억 400만 달러로, 2019년에는 전년 대비 7.8% 상승해 44억 2,400만 달러에 이를 것으로 예상
 - 경비 및 순찰 서비스는 ▲경호 서비스 ▲도난 방지 서비스 ▲보안 서비스 ▲지문 서비스 등의 분야로 분류되며, 2018년 기준 관련 업체는 총 37,378개로 총 고용 인력은 238,000여 명

- ▶ 한편 Frost & Sullivan이 집계한 2018년 인도네시아 사이버보안 시장은 약 3억 4,900만 달러 규모이며, 2016~2022년 간 연평균 24.7%씩 증가해 2022년에는 4억 8,700만 달러에 달할 것으로 전망
 - 2016년 사이버보안 시장에서 네트워크 솔루션 부문이 66.2%를 점유했으며, 주로 은행 및 정부 조직에 방화벽·IDS(침입방어시스템)·IPS(침입예방시스템)·SSL VPN 등의 솔루션을 공급
 - 뒤를 이어 보안 콘텐츠 관리 부문이 19.5%를 차지했고 2022년까지 연평균 13.4% 증가할 전망

그림 _ 인도네시아 사이버보안 시장 규모 전망(2016-2022)

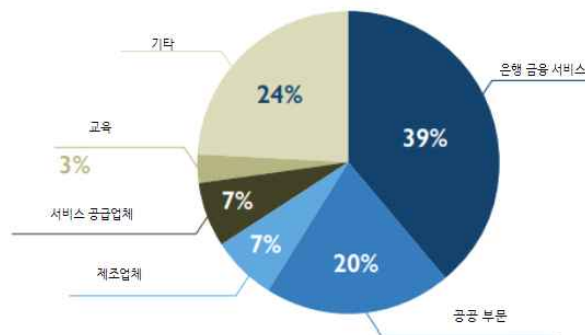
(단위: 백만 달러)



[출처] Frost & Sullivan, Digital Market Overview, Indonesia(2018)

- 고객별로는 해커들의 주요 공격 대상인 은행 및 금융 부문이 사이버보안 시장 매출의 39%를 차지

그림 _ 인도네시아 사이버보안 시장 지출 점유율(고객별)



[출처] Frost & Sullivan, Digital Market Overview, Indonesia(2018)

- ▶ 한편 시장조사기관 6Wresearch에 따르면 보안에 대한 우려 증가, 정보의 보안 지출 및 IT 인프라 확대 등에 힘입어 인도네시아의 물리 보안 시장이 향후 강한 성장세를 나타낼 전망
 - 6Wresearch는 인도네시아의 영상감시 시장이 2022년까지 2억 314만 달러로 성장할 것으로 예상
 - 2016년 1월 자카르타 시내에서 폭탄 테러 이후 정부는 감시 시스템의 확대에 박차

- ▶ 글로벌 국방산업 조사 기관 SDI는 2025년 인도네시아의 국토안보 지출 규모(Homeland Security spending)가 17억 1,586억 달러에 도달할 것으로 예측

그림 _ 인도네시아 국토안보 지출 추이(2016-2025)



[출처] SDI(2016)

2) 분야별 현황

물리 보안 제품 및 서비스

- ▶ 경찰청 등 정부 기관, 또 항만·도로 인프라 구축 사업으로 인해 물리 보안 장비 수요가 증가
 - 2025년에 인도네시아 인구의 70%가 도시에 거주할 것이라는 전망 속에서 인프라 개발에 따른 보안 장비 수요가 증대될 것으로 예상
 - 한편 2017년 11월, 경찰은 범죄자의 얼굴을 탐지해 알람을 활성화시키는 첨단 CCTV 시스템을 개발 중이라고 발표했으며, 향후 경찰서·공항·항구 등에 배치할 예정

- ▶ 2014년 12월 '스마트시티 자카르타(Smart City Jakarta)' 이니셔티브 출범 후, 현재 반둥(Bandung) 등 기타 도시에서 스마트시티 정책이 진행 중
 - ▲자카르트 외곽 신도시 메이카르타(Meikarta)의 경우 모든 대중교통 수단에 센서 및 CCTV를 탑재해 서로 연결되도록 설계 ▲반둥은 관제센터 구축 및 도로 상황 모니터링 시스템을 도입
 - 현재 인도네시아에서는 출입제어 시스템, 알람 시스템, 영상감시 시스템, 금속 탐지기 등 하이테크 보안 장비는 물론, 통합 보안 솔루션이 요구되는 인프라 프로젝트 대부분 해외에 의존

정보보안 제품 및 서비스

- ▶ 시장조사기관 Kable에 따르면 2016~2019년 인도네시아의 보안 하드웨어 및 제품 시장이 연평균 6% 성장해, 2019년에는 약 292만 달러에 이를 것으로 전망
 - 한편 보안 소프트웨어 시장은 2019년까지 매년 3.58% 성장 예상

표 _ 인도네시아 보안 하드웨어 및 제품 시장 추이

(단위: 백만 달러)

분야	2016	2017	2018	2019	CAGR
방화벽 및 VPN 게이트웨이	1.146	1.200	1.246	1.283	3.84%
암호화/SSL 액셀러레이터	0.494	0.528	0.562	0.595	6.40%
콘텐츠 필터링 및 스팸방지	0.431	0.472	0.516	0.560	9.17%
스마트카드 리더기	0.280	0.308	0.336	0.362	8.99%
스마트카드	0.108	0.116	0.122	0.128	5.72%
합계	2.458	2.623	2.783	2.928	6.00%

[출처] Kable(2016)

표 _ 인도네시아 보안 소프트웨어 및 제품 시장 추이

(단위: 백만 달러)

분야	2016	2017	2018	2019	CAGR
인증	0.2220	0.2335	0.2437	0.2525	4.38%
접근 제어	0.1452	0.1557	0.1663	0.1766	6.75%
방화벽/VPN	0.1356	0.1417	0.1469	0.1510	3.64%
보안 제품군	0.1279	0.1350	0.1416	0.1475	4.88%
보안 정보 관리	0.1202	0.1273	0.1340	0.1401	5.22%
스팸방지 및 콘텐츠 필터링	0.0969	0.1016	0.1057	0.1091	4.05%
안티바이러스 필터링	0.0949	0.0998	0.1044	0.1083	4.52%
접근 및 정보보호	0.0928	0.0984	0.1037	0.1086	5.36%

분야	2016	2017	2018	2019	CAGR
침입 감지 및 예방	0.0550	0.0572	0.0589	0.0602	3.04%
안티 멀웨어	0.0491	0.0473	0.0447	0.0415	-5.44%
SWG 소프트웨어 및 웹 안티 멀웨어	0.0458	0.0445	0.0425	0.0398	-4.60%
서버 보안	0.0430	0.0437	0.0439	0.0440	0.76%
애플리케이션 스캐너	0.0374	0.0380	0.0383	0.0385	0.98%
암호화	0.0357	0.0363	0.0366	0.0368	1.00%
기기 취약성	0.0356	0.0365	0.0371	0.0373	1.59%
포렌식 및 사건 조사	0.0241	0.0250	0.0258	0.0263	2.99%
보안 기기 시스템 관리	0.0172	0.0167	0.0159	0.0148	-4.99%
PKI	0.0123	0.0123	0.0125	0.0128	1.42%
합계	1.3907	1.4505	1.5026	1.5456	3.58%

[출처] Kable(2016)

- ▶ 인도네시아의 보안 제품 상당수는 글로벌 벤더의 제품으로 유통업체를 통해 수입되어 리셀러를 거쳐 최종 이용자에게 공급되는 구조이며, 주 수요처는 정부 기관 및 통신, 제조, 금융 업계 등
 - 인도네시아 내 사이버 공격 대부분은 멀웨어와 피싱의 형태이며, 정부 기관 및 금융기관의 정보 시스템을 주로 겨냥하기 때문에 방화벽과 안티바이러스 제품이 주로 유통
 - 한편 보안시장의 성숙도가 낮아 소프트웨어보다는 하드웨어의 비중이 높은 편
 - 소프트웨어 시장의 성장이 더딘 이유 중 하나는 해적판의 범람으로, 2015년 비즈니스 소프트웨어 연맹(BSA) 조사에 따르면 ▲인도네시아 컴퓨터 이용자의 84%가 불법 소프트웨어를 설치 ▲해당 소프트웨어의 상업적 가치는 12억 달러
 - 2019년 BSA는 해적판 소프트웨어의 리스크에 대한 인식 제고 및 정품 소프트웨어 사용의 유익 설파를 위해 인도네시아·태국·필리핀에서 'Legalise and Protect' 캠페인을 진행 중

3) 주요 사업자 현황

시장 특성 및 경쟁 강도

□ 정보보안 시장

- ▶ 인도네시아의 IT 및 정보보안 시장은 글로벌 기업이 주를 이루고 있으며 기업 간 경쟁이 치열

- IT 솔루션 및 네트워크 분야에 진출한 기업은 EMC, HP, Cisco, VMware, Redhat, Radware, Sophos, 등이며 정보보안 분야 진출 기업은 Check Point, Trend Micro, Fortinet, McAfee 등
 - 글로벌 기업들은 정부 및 금융기관 등 높은 수준의 정보보안을 요하는 기관을 중점 공략
- ▶ 정부 기관을 위시해 금융, 전자상거래 등 산업 전반에 걸쳐 사이버보안 서비스에 대한 투자가 이뤄질 전망이며, 특히 클라우드 기반의 서비스 채택에 있어서 SMEs가 주도적 역할을 할 것으로 기대
- 한편 정부 조직들은 하드웨어 기기 기반의 솔루션을 선호하며 DDoS 완화는 벤더 업체에 아웃소싱
- ▶ 현지 이동통신 사업자 및 보안 전문업체 등이 보안관제센터(SOCs) 자체 구축 및 사이버보안 홍보에 박차를 가함에 따라, 향후 사이버보안 서비스 채택률이 더욱 증대될 것으로 예상
- 인도네시아 현지 보안서비스 제공업체 및 이동통신 사업자들은 SOCs 구축 경험 및 운용 역량을 갖춘 글로벌 업체와의 파트너십을 통해 사이버보안 솔루션을 제공하는 추세
 - 또한 Telkom Telstra 등 현지 기업들은 아웃소싱 서비스와 SOC 제공해 투자 회수 속도를 제고

표 _ 인도네시아 3대 현지 사이버보안 업체 전략(2017)

부문	주요 특징	성장 전략	핵심 부문
Telcom Telsta	• 자문 서비스를 통한 추천 채택 및 요구 조건에 기반한 맞춤형 서비스 실시	• Telkom의 국내 및 글로벌 네트워크 역량 및 인프라를 활용해 E2E 솔루션 포트폴리오 제공하기	• 금융 서비스 • 공공 부문 • 제조
Binaryworks	• 맞춤형 보안 시스템을 제 공함으로써 네트워크 및 시스템 보안 증진에 역점	• 다양한 플랫폼에 활용 가능한 자체 제품 제작하기	• 헬스케어 • 금융 서비스 • 교통 · 제조
Xynexis	• 비즈니스 및 산업에 대한 심층 지식, 시연 (hands-on) 기술 스킬, 고객에 특화된 액션 플랜에 기반한 정보보증 (information assurance) 방법론을 구사	• 자회사 Noosc를 통해 새로운 보안 관제서비스(MSS)를 제공 • 동 서비스는 기관들로 하여금 SOC 의 온전한 관리 및 모니터링 하도록 지원	• 공공 부문 • 금융 서비스 • 소매 • 제조

[출처] Frost & Sullivan

□ 물리 보안 시장

- ▶ 인도네시아 물리 보안 시장에 진입한 글로벌 기업으로는 AvTech, Axis Communications, Bosch Security Systems, Dahua, Hikvision, Hanwha(구 Samsung) 등
 - BitRefine가 조사한 2019년 1분기 인도네시아 내 CCTV 브랜드 점유율에 따르면, Axis(37.1%), Hikvision(18.6%), PROvision(11.4%), Ganz(10.0%), Dauha(8.6%), Lilin(8.6%), AVTech(5.7%)의 순
- ▶ 미국 상무부의 'Global Safety and Security Resource Guide'는 인도네시아에서는 중고급 보안 및 안전 장비 시장이 비교적 발달한 것으로 조사
 - ▲중급 제품은 일본·한국·대만·중국 산 ▲고급 제품은 미국·유럽 산이 대부분 ▲인도네시아 자국 제품은 소화기, 자물쇠, 금고, 호신용품 등에 한정

주요 사업자

□ 정보보안 시장

- ▶ Trend Micro
 - 2018년 10월 자사의 보안제품 배포를 위해 인도네시아의 최대 유통업체인 ECS와 파트너십 체결
 - 2019년 4월 Apex One이라는 최신 제품을 출시했으며, 이는 클라우드 기술에 기반해 디지털 비즈니스를 시도하는 기업을 위한 최고의 보안 솔루션
- ▶ Fortinet
 - Unified Threat Management(UMT) 솔루션의 리더로서, Gartner의 '2019년 메직쿼드런트 보고서의 네트워크 방화벽 부문(Magic Quadrant for Network Firewalls)'에 10년 연속 등재
 - Fortinet은 동남아 각국에 리셀러를 두고 있으며, 인도네시아 현지에 파트너 8곳을 통해 영업 전개
- ▶ Q2 Technologies
 - 보안 솔루션에 주력하는 IT 솔루션 업체로서 ICE ACTIMIZE, Paladion, MarkAny, RSA Security, IBM, ACTIVE Identity 등의 보안 솔루션을 유통
 - 2019년 8월 국제 사이버 보안 및 E-비즈니스 인증기관이자 CEH(Certified Ethical Hacker) 및 LPT (License Penetration Tester)로 유명한 EC-Council USA와 전략적 교육 파트너십을 체결
- ▶ PT. Piranti Nusantara Teknologi(PIRANUSA)
 - IT 및 소프트웨어 전문 사업자이며 ZWCAD의 공식 총판이자 ZWSOFT, Microsoft의 파트너사

- 보안 분야에서는 Kaspersky Lab, Symantec의 솔루션을 판매
- ▶ Astra Graphia Information technology(AGIT)
 - TELKOM, Microsoft, Ericsson, Cisco 등의 파트너로 시스템 모니터링 및 데이터 센터 솔루션을 공급
 - 2019 인도네시아에서 가장 혁신적인 기업에게 주는 '혁신 기업상' 수상

□ 물리보안 시장

- ▶ Bosch Security Systems
 - 미국 기반의 보안 장비 업체로서 2008년 자카르타에 PT Robert Bosch라는 순 외자 법인을 설립
 - 인도네시아 Surabaya, Bali 등에 지사 설립 및 Cikarang과 Bekasi에 자동화 제조공장을 운영
 - Bosch Security Systems는 영상감시 시스템, 침입경보 및 화재 경보 시스템, 출입제어 시스템, 공항·철도·회의장 등을 위한 전문 보안 솔루션을 제공
 - GSX 2019에서 신규 카메라, 녹화 및 관리 솔루션 등 50여 개의 신제품 출시 계획에 대해 발표
- ▶ PT. Handal Solutitama (Handal Security)
 - 인도네시아 자카르타 기반의 PT. Handal Solutitama (Handal Security)는 전자보안 시스템 통합 제공업체로서, CCTV, EAS 및 리테일 매장용 알람 시스템, 접근 제어 시스템 등을 취급
 - Handal Security는 Checkpoint Systems의 유일한 유통업체로 활동 중
- ▶ ADV International
 - 중국 기반의 ADV **International**은 싱가포르에 유통 및 생산 조직을 두고 CCTV 제품만을 집중 취급
 - 말레이시아, 인도네시아, 중국(심천) 및 홍콩 등에 CCTV 판매 지사를 설립
- ▶ Certis
 - 싱가포르 기반의 Certis는 인도네시아 Jakarta, Bandung, Batam, Surabaya 등에 지사를 두고 있으며, 광범위하고 전문적인 통합 보안 솔루션 및 원스톱 서비스가 강점

4) 주요 동향 및 이슈

- ▶ 인도네시아 보안업체 PT Professtama, 호주 Red Piranha와 파트너십 체결 (2019.3)¹

- Red Piranha는 차세대 방화벽 'Crystal Eye'를 개발한 호주 기반의 보안 스타트업
 - Professtama 측은 동 파트너십을 통해 Crystal Eye를 비롯해 Red Piranha의 사이버보안 소프트웨어 및 서비스 솔루션을 인도네시아 기업 및 기관에 공급할 예정
 - 특히 향후 1-2년 간 500만 달러 규모의 Crystal Eye 플랫폼을 인도네시아 시장에 독점 조달할 계획
 - 양사는 자카르타 보안운영센터(SOC) 구축에 협력할 것이며, Red Piranha는 호주 교육 기관과 연계해 인도네시아 청년 전문가를 위한 사이버보안 전문지식 교환 프로그램을 지원할 계획
- ▶ Facebook, Agence France-Presse(AFP)와 팩트 체크 파트너십을 체결(2019.4)²
- Facebook은 인도네시아 대선 전에 국외에서의 정치 광고를 금지
 - 한편 인도네시아 정부는 소셜미디어를 통해 유통되는 거짓정보가 선거전에 영향을 준다고 판단해 선거전 동안 80명으로 구성된 팩스체크팀을 구성
- ▶ 2019년 CCTV 시장 규모 15-20% 성장 전망 (2019.5)³
- Statistica에 따르면 2018년 인도네시아의 물리보안 시장 규모가 약 3억 5,000만 달러(USD)
 - 연 평균 55.3% 성장하여 2022년에는 20억 1,000만 달러 규모에 이를 것으로 전망
- ▶ 자카르타 교통경찰국, AI 카메라를 도입해 전자교통단속시스템(ETLE)을 더욱 강화(2019.7)⁴
- 이 시스템은 2019년 7월 1일 기준 10곳의 신규 CCTV 카메라를 통해 작동 중
 - 기존의 CCTV 카메라는 표지판, 도로 표지판, 신호등 위반 사항만 기록한 것에 반해, 동 카메라는 안전벨트 착용 및 운전자의 휴대전화 사용 여부, 가짜 번호판, 속도위반, 자동차 내부의 활동 기록 등 다양한 추가 기능이 탑재
 - CCTV 카메라로 연결된 ERI 프로그램을 통해 교통법규 위반 차량의 번호 및 위치를 교통관리센터(TMC)에 통보하면, 센터에서 차량 및 차주 주소지로 스티커를 발송
- ▶ 인도네시아 수도 이전 계획 및 보안기술 인프라 개발(2019.8)⁵
- 자카르타에서 1,300km 떨어진 보르네오섬 동 킬라만탄(East Kalimantan) 지역이 새 수도로 선정
 - 높은 인구 밀도(3,000만여 명), 2040년 수자원 고갈 가능성, 지진 빈발 등이 수도 이전의 이유
 - 새 수도 건설 공사는 2021년에 착수되며 총 440억 달러의 비용이 소요될 전망

1 Red Piranha, "Red Piranha signs US\$5 Million Cyber Security capability partnership at Indonesia-Australia Free Trade Agreement Signing ceremony", 2019.3.4

2 The Asian Post, "Hoax busters: Fighting fake news in Indonesia", 2019.4.9

3 Marcomm, "UNV Targetkan Pangsa Pasar CCTV 20% di 2019", 2019.5.10

4 HanIn Post, "자카르타 교통국 인공지능 CCTV 카메라 설치", 2019.7.3

5 Tribunn News, "Empat Rekomendasi Teknologi Keamanan Canggih untuk Ibu Kota Baru dari ATISI", 2019.8.8.; ABC, "Indonesia picks Jakarta capital replacement in East Kalimantan province on Borneo", 2019.8.27

- 새 수도의 콘셉트는 '숲속 스마트시티(smart city in the forest)'이며 18만 헥타르의 정부 부지를 확보
- 인도네시아 보안산업 및 기술협회(ATISI) 등은 정부의 수도 이전 계획에 지지를 표명
- 수도 이전에 따른 기술 인프라 개발과 관련해 ATISI는 4대 보안안전 기술, 즉 ▲도청 및 도난 방지 기술 ▲계층화된 보안 시스템 ▲CCTV 수량 및 품질(100km²당 CCTV 100대 설치, 온도 센서 및 야간투시 기능 탑재) ▲안면인식 및 인공지능 기술을 권장

5) 정보보호 스타트업 시장 현황

- ▶ 2019년 10월 기준 인도네시아에는 Gojek, Traveloka, Bukalapak, Tokopedia, OVO를 포함해 총 5개의 유니콘 기업이 있으며, 유니콘 대열에 합류한 정보보안 스타트업은 현재로서는 부재
 - 한편 Nodeflux와 Avnos 등 현지 및 해외 기반의 정보보안 스타트업들이 맹활약 중
- ▶ 인도네시아의 비전 AI 스타트업 Nodeflux는 지능형 영상분석(IVA) 기술로 글로벌 기업으로 도약
 - 동 사는 2016년 설립되었으며, 2019년 3월 텍사스에서 개최된 'FSXSW Festival 2019'에 참여함으로써 AI 기반의 지능형 영상분석(IVA) 기술 업체로서의 역량을 인정받음
 - 현재 인도네시아 경찰청(POLRI) 및 인구·시민등록부(DISDUKCAPIL)의 승인 하에 안면인식과 딥러닝 기술을 바탕으로 IVA 기술을 구현 중으로, 두 기관의 대규모 데이터베이스를 추출해 CCTV 카메라에 포착된 인물·사물을 고도의 정확도로 인식
 - 동 기술을 자카르타와 반둥 내 CCTV 카메라에 연결해 스마트시티 관리 및 공공안전을 지원
 - 그 외, 2018년 아시안게임 및 IMF-World Bank 연례회의의 보안을 담당
- ▶ 한편 Avnos는 대표적 외국 스타트업으로서 아태지역 본사를 싱가포르에서 인도네시아로 이전
 - 인도네시아 투자자로부터 시리즈 A에서 1,000만 달러의 투자금을 확보했으며, 향후 인도네시아의 사이버 R&D를 구축함으로써 인재 개발 및 사이버보안 인식을 제고할 전망
 - 자사 제품 DSF/ Avnos 2.0(Avnos Decentralized Software-Defined Firewall)은 기업이 내부 네트워크 또는 공용 인터넷에 관계 없이 시간과 장소를 불문하고 자사 장치에 대해 보호 기능을 제공

Ⅲ 정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

- ▶ 정부는 2008년 '전자정보 및 거래에 관한 법률(Law No. 11 of 2008)'을 제정해 사이버 범죄에 대응하고 있으며, 그 후 2016년 11월에 개정(Law No. 19 of 2016)
 - (Law No. 11 of 2008) 동 법률은 전자정보 거래에 대한 적정 규제를 통해 정보기술 개발·유통·촉진·오용 방지를 도모
 - 전자정보 거래에 관한 규정뿐 아니라, 이와 관련한 전자서명·지식재산권·개인정보보호·분쟁 해결·정부 및 공공 기관의 역할·형벌 규정 등을 총 망라
 - (Law No. 19 of 2016) 동 개정법은 ▲'전자시스템 공급자(Penyelenggara Sistem Elektronik)'를 전자 시스템을 공급·운영·관리하는 개인·공무원(state administrator)·기업·조직으로 그 의미를 구체화 ▲잊혀질 권리 및 정부의 접근 중단 권한을 인정
 - 동 개정법이 개인의 프라이버시 권리를 강화시킨 반면, 표현의 자유 등 대중의 정보권을 제약할 수 있다는 점에서 논란
- ▶ '전자정보 및 처리에 관한 법률'에 근거한 '정보보호를 위한 시스템 운영 규정 (Ministerial Regulation No. 4 of 2016)'
 - 동 규정은 공공 서비스 관련 전산 시스템을 리스크에 기반해 3개 범주, 즉 ▲공익 및 공공서비스·국방 및 안보 등에 중대 영향을 주는 전략적 전산 시스템 ▲특정 지역이나 영역에 한해 영향을 미치는 高 전산 시스템(high electronic system) ▲低 전산 시스템(low electronic system)으로 구분
 - 그 중 전략적 전산 시스템 및 高 전산 시스템의 경우, '정보보호 경영 시스템 인증(Certificate of Management System of Information Protection)' 획득이 필수

표 _ 인도네시아 정보보호 정책 관련 법안 및 내용

법안	내용
Mandate Act 36 of 1999 Article 39.	통신 분야의 보안 의무 언급
Government Regulation no. 52 of 2000 chapter 82.	통신 장애를 피하기 위해 모든 통신 네트워크, 장비, 인프라의 보안 시스템 필수 적용

법안	내용
Law No. 11 of 2008	전자정보거래에 관한 규정 및 이와 관련한 전자서명, 지식재산권, 개인정보 보호 등을 망라
Ministerial Regulation No. 20 of 2016	전자 시스템에서의 개인정보 보호 관련 규정

[출처] ID-SIRTI

표 _ 인도네시아 전자정보법(Electronic Information Law) 위반 시 형벌 기준

위반 내용	징역 (또는 벌금)
불법 접근	징역 4~8년 (6억~8억 루피아)
전송 감청 (interception/wiretapping of transmission)	징역 6~10년 (8억~10억 루피아)
전자정보 또는 전자기록의 변경, 추가, 축소, 전송, 변경, 삭제, 이동, 은닉	징역 8~10년 (20억~50억 루피아)
조작, 파괴, 손상을 통해 만든 전자정보 및 전자문서를 원본인 것처럼 위장하거나 전자정보 프로세싱과 관련한 위반	징역 10~12년 (100억~120억 루피아)

[출처] Chambers

- ▶ 2016년 11월 인도네시아 통신정보기술부(KOMINFO)는 '전자 시스템의 개인정보보호에 관한 규정(Ministerial Regulation No. 20 of 2016)'을 공포
 - 이는 ▲개인정보의 수집·처리·분석·저장·공개·이전·삭제 등 전자 시스템 내 개인정보 취급 단계별 활용 및 보호 방안 ▲불이행 시 경고처분·업무정지 등의 제재에 대해 명시

표 _ 전자 시스템의 개인정보 보호에 관한 규정 주요 내용

구분	주요 내용
수집	<ul style="list-style-type: none"> • 사전에 정한 특정 목적에 한해 개인정보 수집 가능 • 정보 소유자에게서 수집된 개인정보의 기밀 여부를 구체적으로 명시하고, 개인정보의 변경/추가/업데이트가 가능한 옵션을 제공 • 수집된 개인정보는 정확성 보장을 위해 검증이 필수 • 전자시스템 운영자는 상호운용성과 호환성 확보 및 적법한 소프트웨어 활용이 의무
처리 및 분석	<ul style="list-style-type: none"> • 개인정보 처리 및 분석은 공개된 범위로 제한하되 소유자의 동의를 기반으로만 가능 • 처리 및 분석된 개인정보는 정확성을 보장을 위해 검증이 필수

구분	주요 내용
저장	<ul style="list-style-type: none"> • 저장된 개인정보는 정확성 보장을 위해 검증이 필수 • 저장된 개인정보는 반드시 암호화된 데이터어야 할 것(최소 요구조건은 미명시) • 저장된 개인정보의 최소 보존 기간은 5년(명시된 경우는 제외) • 공공서비스 관련 전자 시스템 운영자는 자체 데이터 센터 및 재해복구센터를 구축
표시, 공개, 이전, 배포 및 접근 권한 제공	<ul style="list-style-type: none"> • 개인정보의 표시/공개/이전/배포/접근 권한 제공은 공개된 범위로 제한하되, 소유자의 동의가 필수 • 이러한 과정에 활용되는 개인정보는 정확성 보장을 위해 검증이 필수 • 데이터의 해외 이전은 통신정보기술부와의 조정 하에 진행 • 법집행기관의 유효한 요청에 근거한 법 집행 목적의 개인정보 접근권 제공이 가능
삭제	<ul style="list-style-type: none"> • 데이터 보유 기간 만료, 혹은 소유자의 요청이 있을 경우만 개인정보 삭제 가능 • 개인정보 삭제 시 정보의 소유자가 해당 개인정보 및 동의를 다시 제공하지 않는 한, 전자 시스템 상에 다시 표시될 수 없도록 전자적 및 비전자적으로 조치 필수
기타	<ul style="list-style-type: none"> • 그밖에 동의, 시스템 인증, 데이터 유출, 잊혀질 권리 등에 관한 내용 포함

- ▶ 현재 인도네시아에는 통신법 'Law No 36 of 1999', 의료행위 관련법 'Law No 29 of 2004), 전자정보 및 거래법 'Law No. 11 of 2008' 등 다수의 개인정보보호 규정들이 있지만 구체성이 부족한 실정
 - 예를 들어, 통신 부문의 개인정보 관련법 'Law No 36 of 1999'의 제40조는 텔레콤 사업자에게 네트워크를 통해 전송된 가입자의 정보에 대해 비밀 유지를 요구하고 있지만, ▲현재까지 '텍스트 메시지'에 대한 권리 및 의무에 대한 세부 규정은 부재 ▲개인정보 보호를 위해 데이터 주체가 취할 수 있는 '추적금지' 고려사항이 미포함 ▲영상·텔레비전 등과 관련해 각각의 특별 조항을 마련하지 않고 그 대신 '전자문서'로 일괄 취급하는 등 구체성이 결여

주요 전략 및 정책

- ▶ 인도네시아의 사이버보안 정책은 2007년 수립된 인터넷 프로토콜 기반 통신 네트워크 애플리케이션 보안 법령인 'Regulation No. 26/PER/M.KOMINFO/5/2007'이 그 시초이며, 이는 네트워크 및 인터넷 보안 모니터링 기관 'ID-SIRTII/CC' 설립의 기초
 - 그러나 정보보호를 위한 체계적 법령의 부재 등, 정보보호 정책은 전반적으로 미흡
 - 정부는 정부 기관의 방화벽 강화, 모니터링, 향후 공격 방지를 위해 IT 모니터링 팀을 구축하는 한편, 핵심기반시설 보호(CIP) 강화, 국제 협력 강화, 신규 보안시스템 도입 등을 추진 중

- ▶ 2015년 5월 국가개발계획부 기술평가·적용처((BAPPENAS)는 '인도네시아 브로드밴드 플랜-사이버보안 전략을 발표
 - 주요 목표는 ▲사이버 범죄로부터 국가 ICT 인프라 보호 ▲브로드밴드 경제 활성화를 위한 연결성 인프라(Connectivity Infrastructure)와 관련해 투자자들로부터의 신뢰 획득 등

- ▶ 현 정부는 정보보호 및 사이버보안을 주요 정책과제로 선정했으며 '통신정보기술부(KOMINFO) 전략계획(2015-2019)'를 통해 그 의지를 확인
 - 동 전략계획의 4대 우선순위는 ▲광대역 연결 ▲디지털화 ▲인터넷 거버넌스 ▲정부 PR

표 _ 통신정보기술부 전략계획(2015-2019)의 4개 우선순위

4대 우선 순위	주요 내용
광대역 연결	<ul style="list-style-type: none"> • 4G 서비스 포함한 광대역 인프라 개발 <ul style="list-style-type: none"> - 무선 주파수 스펙트럼 자원 정리 - 인도네시아의 위성 궤도의 연속성 유지를 통한 자국의 재산 및 통제권 유지 - 인도네시아 497개 지역 및 도시의 연결을 위해 국가 광섬유 백본 네트워크 (Palapa Ring) 배포 • 통신산업의 효율성 제고 <ul style="list-style-type: none"> - 통신 산업의 효율성을 위해 사업자 간 통합 장려 - 통신 인프라 개발비를 줄이기 위해 수동 공유 인프라(패시브 인프라 공유) 구축 • 통신도구 및 장치의 국산 콘텐츠 장려
디지털화	<ul style="list-style-type: none"> • 아날로그 TV에서 디지털로의 전환 프로세스의 속도 제고 • 디지털 TV로의 신속한 전환을 위한 정책 및 규정 개발
인터넷 거버넌스	<ul style="list-style-type: none"> • 정보 보안 개선 및 인터넷 거버넌스 최적화 <ul style="list-style-type: none"> - 전자 시스템 인증 구현 - 음전하 사이트 처리를 위한 패널 형성 - 전자 등록 시스템 제공 - PSrE 및 LSK 캔디 작성 및 비준 • 전자상거래 성장 촉진 <ul style="list-style-type: none"> - 5-10개년 전자 상거래 로드맵 확립 - 전자 상거래 확산 데이터 수집 • 불법적 콘텐츠 감소를 위한 DNS 구현 • 전자 정부 서비스 통합 <ul style="list-style-type: none"> - 전자정부 구현을 위한 마스터 플랜 개발
정부 PR	<ul style="list-style-type: none"> • 통신네트워크 기관 설립 • 정부 홍보(GPR) 규정 이행 준비 및 모니터링

[출처] KOMINFO

- ▶ 통신정보기술부(KOMINFO)는 'Born to Protect' 운영하고 있으며, 이는 매년 개최되는 국가 사이버보안 프로젝트로서 사이버보안 인력 배출이 주 목적
 - 주관은 보안기업 PTXynexis이 맡고 있으며, 통신정보기술부를 비롯해 정보보안인증업체 EC-Council, RSA Security, University of Gunadarma 등이 지원
 - 동 프로젝트의 진행 방식은, 자카르타(Jakarta), 메단(Medan), 반둥(Bandung) 등 10개 도시에서 보안 인재 1만여 명 모집→준결승전을 거쳐 1,000명 선별→'캡처더프래그(capture the flag)' 챌린지에서 최종 상위 100명을 선발→2주간의 '디지털 캠프'를 통해 사이버보안 전문교육 제공
 - 준결승 통과자 1,000명에게 Certified Secure Computer User (C|SCU) 프로그램의 바우처, 최종 선발자 100명에게는 ANSI가 승인하는 Certified Network Defender (C|ND) 프로그램의 바우처를 수여
 - 한편, KOMINFO가 2019년 1월에 발표한 바에 따르면, 인도네시아 전역의 기업, 공공기관, 중소기업에 필요한 사이버보안 인력은 연간 60만 명

- ▶ 2019년 9월 인도네시아 정부는 인터넷 프로토콜(IP) 상호연결 구현을 위한 로드맵을 발표
 - 상호 연결 IP 기반 구현을 위한 로드맵에는 ▲목표 ▲IP기반 상호연결의 정의 및 모델 ▲기술적 표준 (표준 코딩, 보안 기준, 표준 충전 및 결제) ▲상호연결 충전 및 청구 모델 ▲상호연결 벤치마크 ▲지역사회 준비도(광대역 보급, 광대역 서비스의 속도 및 요금) ▲상호연결 구현 계획 및 실행 단계 ▲관련 규제 ▲상호연결의 배치 등의 내용이 포함
 - 2025년 4G/5G 액세스 네트워크가 전체 운영자 액세스 네트워크의 60% 이상에 도달하게 되면 모든 IP 기반의 상호연결 작업이 실행될 것으로 전망

2) 담당기관

- ▶ 국가사이버암호청(BSSN: Badan Siber dan Sandi Negara)
 - 대통령령(Presidential Regulation No. 53 of 2017)에 기반한 것으로 2018년 1월 3일부로 설립
 - 기존의 국방부 산하 국가암호청(LSN)을 모태로 통신정보기술부(KOMINFO)의 정보보호과 및 침해대응센터(Id-SITII/CC)를 통합
 - 동 기관은 국가 사이버보안의 컨트롤타워로서, ▲정책 개발 ▲침해사고 탐지·대응 ▲유관기관과의 협력 및 조정 ▲사이버보안 마스터플랜 및 중장기 로드맵 등, 국가 전략·정책 수립 및 집행을 총괄 ▲사이버 공격에 대한 탐지·복구·예방·완화 조치를 수행 ▲내부 감독관을 통해 기술 규정을 수립·감독·평가 ▲소셜미디어 활동 모니터링을 통한 반국가적 이데올로기의 확산 억제
 - 한편 BSSN은 사이버 공격에 취약한 10개 국가 핵심 인프라로 ▲사법기관 ▲에너지 및 광물자원 ▲금융 및 बैं킹 ▲보건 ▲ICT ▲농업 ▲국방 ▲비상대응(emergency response) ▲정수처리를 지정

▶ 통신정보기술부(KOMINFO)

- 정보통신서비스 보안을 위한 정책 수립, 제도 도입, 인력양성 등을 총괄
- 정부 네트워크 및 시스템 보안을 위한 Gov-CSIRT를 내부적으로 운영하고 있으나, 전자정부 수준이 낮고 소수의 인력만 배치된 까닭에 실질적인 기능 수행에는 한계가 뚜렷
- 대표적인 산하 조직으로는 민간 분야 네트워크 침해사고대응을 위한 Id-SIRTII/CC
- KOICA 자금으로 PKI 구축 및 네트워크 보안관제 시스템 개발을 추진 중
- 주요 정보통신기반시설 보호(CIIP)를 위한 인증, 심사 등 관련 제도 도입에도 관심을 표명

▶ 정치법률안보조정부(Kemenko Polhukam)

- 국가적 차원에서 사이버보안의 중요성이 강조됨에 따라, 대통령 지시로 국가 사이버보안 전담조직 설립을 위한 임시기구(DCN)를 부처 내 직할로 설립('2014년)
 - ※ DK2ICN(Desk Ketahanan dan Keamanan Informasi Cyber Nasional)에서 DCN(Desk Cyberspace Nasional)로 명칭 변경('16.6월)
- 사이버보안에 직접적으로 관여하지는 않으나 통신정보기술부, 행정개혁부, 국방부, 검·경 등에 대한 조정 역할을 위임받았으며, 이로써 유관부처 및 기관에 대한 영향력을 행사

▶ 국가사이버위원회(Committee on National Security Systems, CNSS)

- 국가 전체의 사이버보안 체계 구축을 위한 법제 정비 및 마스터플랜 수립 등을 담당
- 한국이 주도하여 발족한 글로벌 사이버보안 협력 네트워크(CAMP) 가입 등, 활발한 국제협력 활동을 펼치고 있으며 사이버보안 전담조직으로의 독립 및 역량 강화에 주력

▶ Id-SIRTII/CC

- 통신정보기술부가 2007년 5월 4일 네트워크 및 인터넷 보안 모니터링 기관 'ID-SIRTII'를 설립
- 설립의 법적 근거는 2007년 제정된 인터넷 프로토콜 기반 통신 네트워크 애플리케이션 보안 관련 법령인 'Regulation No. 26/PER/M.KOMINFO/5/2007'
- 동 법령의 주요 내용은 ▲(산하조직) 통신정보기술부 산하 'ID-SIRTII'의 설립 ▲(인터넷을 이용하는 조직) 네트워크 실행 기록 파일의 보관 의무 ▲(통신 사업자) 데이터 보호 및 보안 등 모니터링 시스템 제공 의무 ▲(통신 사업자) 클럭 동기화(Clock Synchronization) 수행 의무 등
- Id-SIRTII/CC는 주요 ISP 네트워크 접속지점(NAP)에 센서 35개를 설치해 24시간 보안관제 (모니터링/분석/대응)를 수행하고 있으며, 자국 내 인터넷 통신량의 50~70%를 커버
- 국가대표(National CSIRT)로서 ISP 등 사업자 및 각계 CERT에 대한 기술 지원, 조정 역할을 담당
- 그 외, 아태침해사고대응팀협의회(APCERT), 이슬람국가연합CERT협의회(OIC-CERT), 글로벌 사이버보안

협력 네트워크(CAMP) 가입 등을 통해 활발한 국제협력 활동을 수행

- ▶ ID-CERT(INDONESIA COMPUTER EMERGENCY RESPONSE TEAM)
 - 1998년 설립된 ID-CERT는 인도네시아 민간 분야의 사이버 보안 커뮤니티로, ▲사이버 공격 및 위협에 대응 ▲자국 네트워크의 사이버 공격에 현황 보고서를 작성 및 배포 ▲국가 보안 시스템 개선에 대한 가이드라인 제공 ▲보안 취약성 개선 보고서 작성 ▲멀웨어 관련 보안 가이드라인 제공 등에 역점

표 _ 인도네시아 내 CSIRT 현황

National	• Id-SIRTII/CC (KOMINFO 산하기관)
Government	• 중앙정부 : Gov-CSIRT (KOMINFO 내부조직) • 지방정부 : 자바(Jawa), 자와티무르(Jatim), 족자카르타(Yogya) 지역별 CSIRT • 군(軍) : Mil-CSIRT
Community	• ACAD-CSIRT : 40개 대학의 CSIRT 연합 • ID-CERT : 민간 분야 CERT 연합
Private	• 주요 사업자(ISP, 통신사, 금융사 등) 별로 존재

[출처] 각종 자료를 토대로 KISA 재구성

- ▶ CISSReC (Communication & Information System Security Research Center)
 - 2015년 설립된 비영리단체로 정보통신시스템 보안 관련 대중의 인식 제고를 위한 연구를 수행
 - 민간의 ICT 보안 및 암호 분야 전문가들이 참여하고 있으며 ▲정보통신시스템의 보안 강화 및 암호 관련 각종 조사 및 학문적 연구 활동을 수행 ▲일반인 대상의 보안 교육 및 캠페인 실시

3) 규제 및 인증제도

- ▶ 인도네시아 시장은 국제보안인증인 ISO 27001:2013을 채택하고 있으며, 이를 기반으로 SNI ISO/EIC 27001:2009라는 명칭으로 보안 관리를 위한 인도네시아 국가표준을 지정
 - 인도네시아 기술표준청(BSN)은 ISO 27001과 동일한 SNI ISO/IEC 27001 표준을 일반 기업, 정부, 비영리조직 등 모든 형태의 조직에 공통으로 적용
- ▶ 인도네시아는 보안 기술을 위해 ISO/IEC 15408로 알려진 공통 기준을 채택

- 즉, 소프트웨어를 포함한 IT 제품의 보안 속성 평가에 ISO/IEC 15408-1/2/3:2014를 활용
- ▶ 인도네시아 시장은 또한 정보보안 네트워크 등의 제품에 대한 CC 인증도 인정
 - 인도네시아 시장에 진출한 글로벌 기업들은 대부분 국제 CC 인증을 취득하여 시장에 해당 제품의 공신력과 기술력을 입증
 - CC(Common Criteria) 인증은 한국·미국·영국·캐나다·호주 등 세계 20개국에서 사용하는 정보보호 제품의 평가 기준으로, 최고 등급은 EAL 5등급임
 - 국내의 보안 업체는 CC 인증 취득을 통해 인도네시아를 비롯한 동남아 시장에 진입하면서 공신력 및 기술력을 입증하는 마케팅 전략으로 활용

4) 최근 정책 동향 및 이슈

- ▶ 통신정보기술부(KOMINFO)는 28개 대학 · 22개 과학기술학교 · 5개 글로벌 기업(CISCO, AWS, Google, Dicoding, Microsoft)과 협력을 통해 디지털 인재를 양성하는 4개 아카데미 운영 계획을 발표(2019.1)⁶
 - 각 아카데미별 역점 분야는 ▲Fresh Graduate Academy는 사이버보안, 빅데이터 분석, AI, 클라우드 컴퓨팅, IoT, 머신러닝 ▲Vocational School Graduate Academy는 네트워크 관리자, 웹 개발자, 모바일 프로그래머, 그래픽 디자인, 중급 애니메이터 ▲Coding Teacher Academy는 코딩 강사 양성 ▲Online Academy는 사이버 운용 및 CCNA 보안, AI, 프로그래밍 운용, 디지털 기술/정책, 빅데이터 등
- ▶ 인도네시아 통신정보기술부(KOMINFO), 개인정보보호법 초안 완료(2019.5)⁷
 - 동 개인정보보호법 초안은 2016년 12월 공포된 '전자시스템 개인정보 보호 규정'에 기반
 - KOMINFO 산하의 통신감독청(BRTI)은 개인정보 매매를 형벌 및 벌금이 부과되는 위법 행위로 규정
 - 위 두 기관은 전자상거래 및 소셜미디어 플랫폼 공급자에게 개인정보 거래 관련 홍보물 · 광고 등을 내릴 것을 요구
 - 동 법안은 종교 · 헬스 · 육체 및 정신 질환 · 성 질환 · 개인 금융 등 특별 보호를 요하는 민감정보 및 개인정보를 다루고 있으며, 개인 데이터의 보안 제고와 데이터 조작 방지에 역점
- ▶ 사이버보안 핵심 이슈 해결을 위한 'Indonesia Security Summit' 개최(2019.9)⁸

6 KISA, "정보보호 해외진출 전략거점 1월 주요동향", 2019.2.12

7 Tempo.com, "Kominfo Preps Draft Bill on Personal Data Protection, 2019.5.17

8 ITSP Magazine, "Accelerating Cyber Security For A Safer Indonesia | ISS 2019", 2019.9.4

- 9월 3-4일 자카르타에서 '보다 안전한 인도네시아를 위한 사이버 보안 가속화'라는 주제로 개최
 - 이는 정부 인사, CISO, CIO, CTO, 포렌식 전문가, 사이버 법률가 등을 위한 지식 공유 플랫폼
 - 2019년은 ▲인도네시아 사이버 범죄 현황 ▲사기·위반 방지를 위한 최신 기술에 역점
- ▶ 9월, 인도네시아 최초의 사이버보안법 공표 예정(2019.9)⁹
- 인터넷 사용자 수 세계 5위 인도네시아에서 2019년 5월 발생한 사이버공격만 190만여 건으로, 사이버위협에 대한 기민한 대처를 위해 사이버보안법의 통과가 절실한 상황
 - 동 법안에는 사이버암호청(BSSN)을 정부, 군·경 등 유관기관과의 협력을 총괄하는 기관으로 지정
 - 기존에 수립된 '전자정보 및 거래법(Law on Electronic Information and Transactions)'과 '전자시스템 및 거래에 대한 정부 규정(Government Regulation on the Implementation of Electronic System and Transaction)'은 사이버 위협에 대해서는 다루지 않음
 - 법안 통과와 시급성에도 불구하고, ▲사이버암호청이 여타 법 집행기관 위에 군림할 가능성 ▲과다한 권한 부여 ▲사이버암호청의 업무 모니터링에 대한 상세 방안 부재 등이 논란을 야기
 - 비평가들은 정부가 동 법에 기반해 반정부 콘텐츠 감시 및 언론의 자유를 탄압할 가능성을 제기

5) 정보보호 스타트업 관련 정책 동향

- ▶ 정부는 2020년까지 1,000개 스타트업을 창조하겠다는 이니셔티브를 전개
- 그런 가운데 Alibaba Cloud가 2018년 초 데이터센터 1호점에 이어 2호점을 개소했으며, Google Cloud와 Amazon AWS도 인도네시아로 클라우드 사업 확장을 발표
 - 이로써 정부의 스타트업 이니셔티브가 더욱 탄력을 받을 것으로 전망

9 The Conversation, "Indonesia needs to fix 'authoritarian' clauses in bill on cyber security before passing it into law". 2019.9.4.

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트시티

- ▶ '자카르트 스마트시티 이니셔티브'는 2014년 12월에 출범했으며 스마트환경, 스마트 모빌리티, 스마트 경제, 스마트 인물, 스마트 정부, 스마트 생활 등 6개 핵심 요소를 포함
 - 자카르타의 스마트시티 구축 과정을 보면, 기본 데이터분석을 위한 서버 구현->로컬 스타트업 생태계와 협력해 모든 사람이 휴대 전화 및 인터넷으로 다운로드해 사용 가능한 공개 애플리케이션 개발->시민 불만 사항을 실시간 모니터링 할 수 있는 관제센터 및 모니터링 시스템 구축->시민 불만 처리 소요 시간 등을 평가->분석 지원을 위한 빅데이터 분석 플랫폼 구현 및 개발의 순
- ▶ 위 애플리케이션과 관련해, 2016년 설립된 스타트업 Qlue가 자체 앱을 개발해 인도네시아 최초로 '스마트 시티' 개념 구현에 기여
 - 이로써 자카르타 주민은 Qlue 플랫폼을 통해 정부와 직접 소통하게 되었으며, ▲2018년 한 해 동안 Qlue 앱을 통해 접수된 불만은 총 10만여 건 ▲후속 조치가 취해진 비율은 82%

핀테크

- ▶ Frost & Sullivan에 따르면 2017년 인도네시아의 핀테크 시장의 규모가 2억 3,770만 달러이며, 그 후 연평균 39.54%씩 성장해 2022년에는 12억5천만 달러에 이를 것으로 전망
 - International Finance Corporation의 2014년 조사에 의하며, 인도네시아의 전체 마이크로 중소기업 중 ▲신용서비스에 대한 접근성 보유 및 지속가능한 규모로의 성장 가능성을 갖춘 기업은 12%에 불과 ▲은행 등 금융기관으로부터의 자금 지원을 못 받는 기업은 45%
 - Palapa Ring 프로젝트로 인터넷 보급률이 증대되면 핀테크 서비스 수요도 동반 상승할 것으로 예측
 - 특히 디지털 지불 결제 및 P2P(Peer-to-Peer) 대출 서비스 영역이 인도네시아의 개인 및 기업에게 금융 상품 및 서비스에 대한 접근성을 제고할 것으로 기대
 - 2018년 기준 인도네시아 중앙은행에 등록된 핀테크 기업은 PT Toko Pandai Nusantara(Toko Pandai), PT Privy Identitas Digital(PrivyID) 등 총 49개
 - 한편 Statista의 데이터에 의하면, 2018년 기준 인도네시아의 핀테크 시장은 지불결제 시스템(38%),

대출(31%), 개인재산 관리(8%), 상품비교(97%), 인슈어테크(6%), 클라우드펀딩(4%) 등의 순

- ▶ 핀테크 부문 중 P2P 대출 서비스는 상대적으로 새로운 영역이며, 따라서 시장 주자들 대부분은 스타트업으로서 2019년에는 그 수가 39% 증가될 것으로 전망
- 업체별 시장 점유율은 Uang Teman이 46%로 1위이며 그 뒤를 이어 Kredivo, Pinjam, Akulaku의 순

그림 _ 인도네시아 P2P 대출 시장 업체별 점유율(2016년 기준)

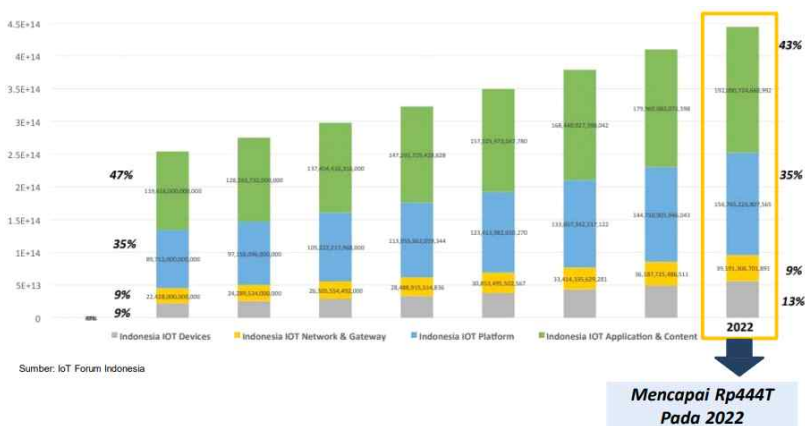


[출처] Frost & Sullivan(2018)

사물인터넷(IoT)

- ▶ 인도네시아의 2022년 IoT 시장 규모는 444조 루피아에 이를 것으로 전망

그림 _ 인도네시아 IoT 시장 규모 전망(2015-2022)



[출처] IoT Forum Indonesia

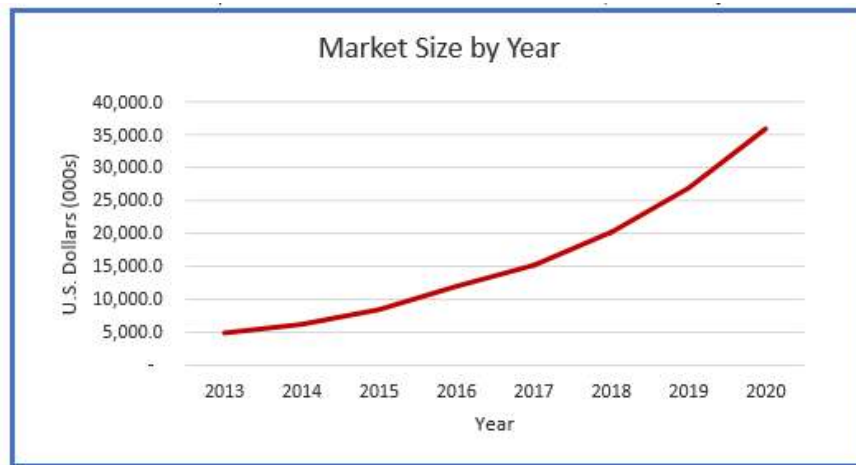
- 부문별 점유율은 IoT 애플리케이션 및 콘텐츠 43%, IoT 플랫폼 35%, IoT 장비 13%, IoT 네트워크 및 게이트웨이 9%의 순
- 2018년 말 기준 IoT를 구현하거나 IoT 관련 투자를 한 기업은 250여 개

인지보안

- ▶ 인도네시아의 인지보안(cognitive security) 장비 시장은 2019년 2,690만 달러에서 2020년 3,590만 달러로 33.6% 성장할 것으로 예측
 - 그 후 2020년부터는 연평균 60.7%씩 성장해 2025년에는 14,480만 달러에 이를 것으로 전망

그림 _ 인도네시아 인지보안 시장 전망(2013-2020)

(단위: 천 달러)



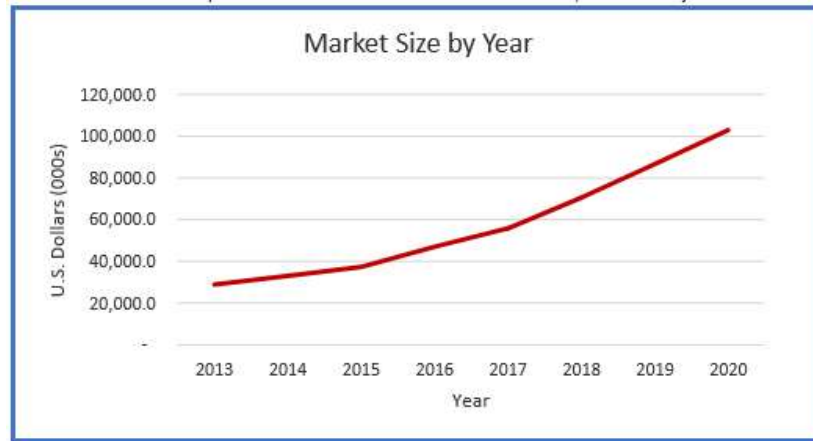
[출처] Barnes Reports(2019)

자동차 사이버보안

- ▶ 인도네시아의 자동차 사이버보안 장비 시장은 2019년 8,670만 달러에서 2020년 18.6% 성장해 1억 290만 달러에 이를 것으로 예측
 - 그 후 2020년부터는 연평균 27.9%씩 증가해 2025년에는 2억 4,670만 달러에 이를 것으로 전망

그림 _ 인도네시아 자동차 사이버보안 시장 전망(2013-2020)

(단위: 천 달러)



[출처] Barnes Reports(2019)

블록체인(가상화폐 포함)

- ▶ 인도네시아 농업에 블록체인 기술을 접목하여 작물 환경 개선 및 빈농 타개¹⁰
 - 국가의 빈곤층 대부분을 차지하는 농민층에서 활발하게 이용 중으로, HARA社의 블록체인 플랫폼을 활용하여 '데이터 민주화(democratize data)' 환경 구축
 - 즉, HARA에 데이터를 제공하는 사람들(주로 농촌의 청년층)이 ▲농부의 신원 ▲재배 품목 ▲농법 ▲비료 ▲경작지 모양·면적 등의 정보를 자발적으로 HARA의 스마트폰 앱에 등록하면 데이터 제공에 따른 보상을 받고, 이 데이터를 은행, 보험회사, 비료회사 등의 기업들이 사들여 자신들의 사업 확장에 활용하며, 농부는 플랫폼에서 HARA가 제공하는 금융상품을 기존 고리의 사채 대비 저리(低利)로 이용하여 빈곤한 경제 상황에 활용

2) 융합보안정책 동향

스마트시티

10 https://news.chosun.com/site/data/html_dir/2019/08/12/2019081201712.html

- ▶ 통신정보기술부 및 국가개발계획부(BAPPENAS)는 2019년까지 스마트시티 100여 곳을 개발하기 위한 '100 Smart City Movement' 이니셔티브를 출범
 - 자카르타, 수라바야, 반둥이 1세대 스마트도시들이며, ▲반둥은 정부 및 관련 기관의 데이터를 통합 ▲수라바야는 교통문제 해결을 위해 감시 카메라에 기반해 교통 상황을 모니터링 ▲스마트시티 생태계의 핵심 도시 자카르타는 도시 내 도로 전역에 CCTV를 설치 외 스마트 조명·스마트 주차·폐기물 관리·커넥티드 맨홀 등 다양한 프로젝트를 탐색 중

핀테크

- ▶ 2018년 9월 인도네시아 금융감독청(OJK)은 혁신적이고 신속하고 저렴한 금융서비스 지원, 금융 포용성 및 투자 증대를 위해 핀테크 기업에 대한 금융 혁신 규제 'No 13/POJK.02/2018'을 발표
 - 주 내용으로는 ▲(규제 샌드박스 절차) 핀테크 업체는 OJK에 등록을 필해야 하며 규제 샌드박스 테스트 통과 후 그 결과에 따라 해당 시스템의 권장 여부를 결정 ▲(포함 및 교육) 사용자에게 정보 제공의 의무 ▲(사용자 안전성) 시스템 투명성, 공정한 서비스, 개인정보보호 등 안전성 제공의 의무 ▲(Fintech Indonesia Center) 인도네시아 핀테크센터를 구축해 규제 샌드박스 프로세스 지원 ▲(자금세탁 및 테러리즘) 자금세탁 및 테러리즘 지원 금지

그림 _ 인도네시아 핀테크 관련 주요 법규

법규	주요 내용
인도네시아 중앙은행법 PBI No. 18/40/2016	<ul style="list-style-type: none"> • 지불거래처리 기관 관련 규정 • 주요 소관 업무는 거래전 단계, 승인, 청산, 정산, 사후 처리 • 국가 지불결제 시스템 관련 규정
인도네시아 중앙은행법 PBI No. 19/8/PBI/2017	<ul style="list-style-type: none"> • 기술 발전에 따른 전자상거래 증대로 안전성, 효과성, 신뢰성을 갖춘 국가 통합 지불 결제 시스템 실현을 목적으로 제정 • 핀테크 조직에 대한 규정
인도네시아 중앙은행법 PBI No. 19/12/PBI/2017	<ul style="list-style-type: none"> • 핀테크 사업자의 정의, 활동 범위, 중앙은행의 승인 획득의 의무, 규제 샌드박스에 대한 내용이 포함
인도네시아 중앙은행법 PBI No. 20/6/PBI/2018	<ul style="list-style-type: none"> • 전자화폐 관련 규정 • 전자화폐의 정의, 유형, 최대 예치규모, 외국인 지분율 제한 등의 내용 포함
금융감독청 OJK No 77/POJK.01/2016	<ul style="list-style-type: none"> • 기술 기반 펀드 대부 서비스(P2P 대출 서비스) 관련 규정 • P2P 대출 서비스 제공에 대한 규제 사항, P2P 대출업자 자격요건 등이 포함 • 금융 서비스 부문의 디지털 금융혁신에 대한 규정
금융감독청 OJK No 13/POJK.02/2018	<ul style="list-style-type: none"> • 디지털금융혁신(IKD, Inovasi Keuangan Digital)을 위한 핀테크 규정 • IKD의 정의 및 범위, 금융감독청 인허가 절차, 정보보안 및 데이터 보호, 규제 샌드박스 등의 내용이 포함

[출처] 인도네시아 중앙은행 등

사물인터넷(IoT)

- ▶ IDC의 조사에 따르면, 2019년까지 인도네시아 지방 정부의 20%가 도로, 가로등, 교통 신호등의 인프라에 IoT를 구현할 예정¹¹

블록체인(가상화폐 포함)

- ▶ 블록체인 기술을 연구하는 국가적 전담팀을 구성, 국가 산업의 전반적인 데이터 관리 문제 극복 도모^{12,13}
 - 인도네시아는 데이터 기록 및 관리에 있어 전문적인 지식과 자원이 부족하여 정확한 기록을 일정하게 유지하는 데에 어려움을 겪어 왔음
 - 그러나 블록체인은 중앙 집중식이 아닌 분산형 네트워크로부터 지속적으로 업데이트되는 정보를 공유하는 형태로서, 정부의 데이터 처리 및 세금의 투명한 사용에 획기적인 발전 가능성을 제공
 - 예컨대, 농촌에 주어지는 정부 보조금은 전년도 수확량을 기준으로 책정되는데, 다수의 수령자가 매년 수확량의 과장을 통하여 과다하게 보조금을 수령하는 경우가 발생해 옴
 - 블록체인 기술을 활용하게 되면 수확량 기록의 정확도가 높아지며 보조금 수령자의 정보 확인도 수월해지게 되므로, 불필요한 보조금의 지급을 줄여 국가 재정 지출의 정확성 및 투명성을 높일 수 있음

11 AS MAG, Smart IoT Indonesia 2019 ready to unveil latest IoT trends, 2018.12.19

12

<https://www.reuters.com/article/us-indonesia-blockchain/indonesia-looks-to-blockchain-to-fix-its-dodgy-data-challenges-idUSKBN11503R>

13

<http://www.dcoinnews.net/%EC%9D%B8%EB%8F%84%EB%84%A4%EC%8B%9C%EC%95%84-%EA%B3%B5%EA%B3%B5-%EB%B0%8F-%EB%AF%BC%EA%B0%84-%EB%B6%80%EB%AC%B8%EC%97%90%EC%84%9C-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%EC%9A%A9%EB%8F%84-%EC%97%B0/>