資料1-3

2020/08/28

米、独
セキュリティ関連ファンディング状況

JST/CRDS

1.DARPA：Defense Advanced Research Projects Agency
アメリカ国防高等研究計画局

- アメリカ国防総省に属する
- 国家安全保障のための画期的な技術と能力の創造
- PM制度、チャレンジが有名
- FY2020の要求総額は36億ドル（2019は34億ドル）
  - Basic Research　4億9千万ドル
  - Applied Research　14億7千万ドル
  - Advanced Technology Development　15億2千万ドル
  - Management Support　8千万ドル
- そのうち、セキュリティ関連は
  - Basic Research　既存プログラム完了によりゼロ
  - Applied Research　2億6千万ドル

https://www.darpa.mil/
Our researchに詳細
関連するオフィスはI2O

Basic Research

Program Element	Project	Title	FY2018	FY2019	FY2020
DEFENSE RESEARCH SCIENCES	CYBER SCIENCES	TOTAL	44.1	12.8	0.0
		Transparent Computing	18.6	9.2	0.0
		Space/Time Analysis for Cybersecurity (STAC)	15.50	3.6	0.0
		SafeWare	10.0	0.0	0.0

セキュリティ関連の予算0はプログラム完了による。
プログラムの詳細はabout us/budgetに詳細資料あり。
https://www.darpa.mil/attachments/DARPA_FY20_Presidents_Budget_Request.pdf

Applied Research: Cyber Security (1/2)

	FY2018	FY2019	FY2020
Cyber Security Total	262.4	255.9	258.9
Cyber-Hunting at Scale (CHASE)	16.3	21.8	23.6
Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS)	15.3	19.0	22.5
Rapid Attack Detection, Isolation and Characterization Systems (RADICS)	35.4	27.3	22.0
Enhanced Attribution	21.2	20.8	21.5
Dispersed Computing	17.0	18.0	20.0
Computers and Humans Exploring Software Security (CHESS)*	7.5	13.0	18.9
Configuration Security	6.9	16.2	18.0
Cyber Assured Systems Engineering (CASE)	24.9	21.4	17.0
Active Social Engineering Defense (ASED)	10.0	15.5	13.0
Leveraging the Analog Domain for Security (LADS)	16.7	15.3	12.0
Brandeis	17.0	18.9	6.5

Applied Research: Cyber Security(2/2)

	FY2018	FY2019	FY2020
Extreme Distributed Denial of Service Defense (XD3)	20.4	12.5	5.0
Memory Optimization (MemOp)	0.0	9.0	22.2
Resilient Anonymous Communication for Everyone (RACE)	0.0	7.0	17.3
Cora	0.0	7.4	12.4
Searchlight	0.0	3.8	6.9
Cyber Fault-tolerant Attack Recovery (CFAR)	17.0	6.0	0.0
Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT)	9.3	3.0	0.0
System Security Integrated Through Hardware and firmware (SSITH)	18.4	0.0	0.0
Supply Chain Hardware Integrity for Electronics Defense (SHIELD)	5.0	0.0	0.0
Plan X	4.0	0.0	0.0

委託先

- 詳細は不明
- 過去のプロジェクトに関しては、そのプロジェクトの成果である文献、ソフトウェア、データに関して貢献者がDARPAのOpenCatalogに記載されている
- しかし、個人名などが多く定量的には不明
- 一部、組織名が出ているものを調べると、以下のようになる
  - 大学（非常に多い）
    - MIT、CMUなどの一流大学
    - Georgia Institute of Technology, University of Virginiaなど有名大学
    - NYITなど特徴のある大学
  - 企業
    - Lockheed Martin, Raytheonなどの防衛産業（かなり少ない）
    - 特定の技術領域を示す名称を付けたおそらくスタートアップ（かなり多く、しかも大学との連名が多い）
  - 研究所（少ない）
    - Lincoln Lab., Naval Researchなど国立研究所
    - SRI、Draper Lab.など民間の研究所

2. IARPA

Intelligence Advanced Research Projects Activity

- The Office of the Director of National Intelligence に属する
- 2004年の「情報改革とテロ予防法」によって設立されたDNIを支援する独立機関
- IARPAは、インテリジェンスコミュニティ（IC）の機関や分野の最も困難な課題のいくつかに取り組むために、ハイリスク/ハイリターンのリサーチプログラムに投資
- 予算については不明（research programは$10M程度との情報もあるが詳細は不明）

https://www.iarpa.gov/
https://en.wikipedia.org/wiki/Intelligence_Advanced_Research_Projects_Activity

Current Research

Title	Description	Research Areas
Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR)	Secure multiparty computation, homomorphic encryption, verifiable computing, compilers, programming languages, automated security analysis	Secure multiparty computation Homomorphic encryption Verifiable computing Compilers Programming languages Automated security analysis
Securing Compartmented Information with Smart Radio Systems (SCISRS)	Information security, signals analysis, machine learning, radio frequency communications	
Trojans in Artificial Intelligence (TrojAI)	AI security, Trojan detection, explainable AI	AI security Trojan detection Explainable AI

33件中、3件がセキュリティ関連

詳細はResearch Programs
https://www.iarpa.gov/index.php/research-programs

Past Research(1/2)

Title	Description	Research Areas	Performers
ATHENA	Cybersecurity	ATHENA was a program focused on computer network operations.	
Circuit Analysis Tools (CAT)	Cybersecurity and information assurance, hardware assurance, microelectronics	Cybersecurity & information assurance Hardware assurance Microelectronics	Boston University; Carl Zeiss SMT, Inc.; DCG Systems, Inc.; HRL Laboratories, LLC; JHT Instruments, LLC; Neocera, Inc.; University of Maryland; Varioscale, Inc.
Cyber-attack Automated Unconventional Sensor Environment (CAUSE)	Cybersecurity, cyber-event forecasting, cyber-actor behavior and cultural understanding, threat intelligence, threat modeling, cyber-event coding, cyber-kinetic event detection	Cybersecurity Cyber-event forecasting Cyber-actor behavior and cultural understanding Threat intelligence Threat modeling Cyber-event coding Cyber-kinetic event detection	BAE Systems Information & Electronic System Integration, Inc.; Charles River Analytics, Inc.; Leidos, Inc.; University of Southern California

32件中、6件がセキュリティ関連　　詳細はResearch Programs
https://www.iarpa.gov/index.php/research-programs

Past Research(2/2)

Title	Description	Research Areas	Performers
Security and Privacy Assurance Research (SPAR)	Secure multiparty computation, private information retrieval, privacy and civil liberties protections	Secure multi-party computation Private information retrieval Privacy & civil liberties protections	Applied Communication Sciences; Argon ST; Columbia University; IBM - T.J. Watson Research Center; Raytheon BBN Technologies; Stealth Software Technologies, Inc.
Securely Taking On New Executable Software of Uncertain Provenance (STONESOUP)	Cybersecurity and information assurance, software assurance, vulnerability detection and mitigation	Cybersecurity & information assurance Software assurance Vulnerability detection & mitigation	Columbia University; GrammaTech, Inc.; Kestrel Institute; Leidos, Inc.; University of Illinois, Urbana-Champaign
Trusted Integrated Chips (TIC)	Cybersecurity and information assurance, hardware assurance, microelectronics	Cybersecurity & information assurance Hardware assurance Microelectronics	Carnegie Mellon University; Cornell University; LGS Innovations, LLC; Northrop Grumman Corporation; Raytheon Vision Systems; Stanford University; University of Southern California - Information Sciences Institute

3. ドイツ　BMBF

the Federal Ministry of Education and Research (BMBF)

- 3拠点で研究開発
  - 攻撃や不正アクセスに対して、ITシステムを保護するためのプロセスと技術開発
- 2011年から助成
  - 第2期にあたるハイテク戦略2020(2010-2013)でスタートし、2015年頃にITセキュリティ枠組プログラムとしてまとめられた
  - ITセキュリティ枠組プログラム：
    サイバーセキュリティは省庁横断する課題なので、連邦政府一丸となって取り組む
    2015-2020で1.8億ユーロ
- プログラム自体は終了、2か所は途中で制度化されて常設の研究センターに
  - CISPA(ザールブリュッケン)　ヘルムホルツ研究センター インフォメーションセキュリティ（2019年）
    https://cispa.de/en
  - CRISP(ダルムシュタット)　ナショナルサイバーセキュリティ研究センター　ATHENE（2017年）
    https://www.athene-center.de/en/
    ベースになる研究所内（フラウンホーファーSITなど）に設置されたバーチャルな研究所
  - KASTEL(カールスルーエ)
    独立した研究所にはなっていない
    人材募集がかかっているので大学の研究所あるいは学科として存続か？
    カールスルーエ工科大はヘルムホルツ研究センターと同名組織

https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html

CISPA - Center for IT Security, Privacy and Accountability in Saarbrücken

- モットー「デジタル社会におけるセキュリティとデータ保護」
- 10/2015 - 07/2017、€4M/年
- ザールランド大学の「ITセキュリティ、プライバシー、アカウンタビリティセンター（CISPA）」の200人以上の科学者が、ITセキュリティとプライバシーの保護に関する現在の問題に対処している。
- 参加機関：Max Planck Institute for Computer Science、Max Planck Institute for Software Systems、German Research Center for Artificial Intelligence
- 具体的な目標は、ITシステムの弱点を早期に発見し、改善された設計プロセスと応用研究を通じて将来的にそれらを排除すること
  - ソフトウェアと組み込みシステムの開発プロセスと同じくらい早い段階でセキュリティとデータ保護を考慮に入れるための、開発者向けの新しいツール
  - インターネット上の通信とデータ処理を保護するための新しい暗号化手法の研究
  - 安全でプライバシーに配慮したスマートフォンとウェアラブル
  - 安全でスマートな自動車の基盤を開発

https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/cispa

CRISP-Center for Research in Security and Privacy

- 大規模で統合された複雑なITシステムのセキュリティ
- コーディネーター：ダルムシュタット工科大学
- 参加機関：

  フラウンホーファー安全情報技術研究所（SIT）、ダルムシュタット

  フラウンホーファーコンピュータグラフィックス研究所（IGD）、ダルムシュタットカレッジ
- 予算：年間420万ユーロ（BMBFから100%提供）
- 期間

  2015年10月～2017年7月

KASTEL – Competence Center for Applied Security Technology in Karlsruhe

- モットーは「ネットワーク化された世界における包括的なセキュリティ」
- 研究拠点カールスルーエ
- 協力関係
- 10/2015 - 04/2021、€ 2M/年
- 暗号学、ITセキュリティ、ソフトウェア技術、法律、および社会科学と人文科学の専門家が緊密に連携
- テーマ
  - **Awareness measures for password security**
  - **SDN Intrusion Prevention and Incident Response in Industrial Networks**
  - **Zero-Trust Authentication (ZeTA) with augmented and virtual reality displays**
  - **A European and German Perspective on Data Protection Law in a Digitised World**
  - **HelpMeICS: SECRYPT publication improves Web Application Scanner**
  - **Article on data protection in the mobility sector**

https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/kastel
https://www.kastel.kit.edu/english/

ドイツにおけるサイバーセキュリティ研究動向

- 連邦国防省(BMVg)と連邦総務省(BMI)の共同所管で、サイバーセキュリティイノベーション機構を2020年5月設置
- まだサイトすらない
  - 所在地　ハレ/ライプチヒ
  - 研究ダイレクター Prof. Dr. Christoph Igel
  - 対象領域　外交、安全保障、防衛政策におけるデジタルイノベーション