平成30年度　委託研究

# 課題195

# 欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発

## 研究計画書

国立研究開発法人
情報通信研究機構

## １．研究開発課題

## 『欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発』

（Advanced technologies combining Security, IoT, Cloud and Big data for a hyper-connected society）

## ２．研究開発の目的

本研究開発課題は、欧州との連携により研究開発の促進が期待できる領域について、欧州委員会（EC: European Commission）と連携して公募(共同公募)を行い、 欧州委員会とともに共同で実施するプログラムである。

具体的には、新たな脅威への機敏な対応、脆弱性自動検出/自動修復、セキュリティツールのオープンソース化、IoTセキュリティ、クラウドセキュリティ、データセキュリティ、プライバシー保護、データ匿名化、IoT／クラウドに関するブロックチェーン、重要インフラ保護、クロスボーダ・アプリケーションの実証といった、セキュリティ、IoT、クラウド及びビッグデータを組み合わせた先端技術の研究開発及び実証を、実データに基づいて実践的に行う。

本共同公募は、ハイパーコネクテッド社会におけるセキュリティの課題の基盤技術の研究において、特に欧州連合（EU: European Union）との連携により研究開発の促進が期待できる領域について、欧州委員会が実施するHorizon 2020と連携して行うものである。日欧双方の強みを戦略的に組み合わせることで、将来の情報通信基盤の基礎となる同分野の研究開発について、国際標準化を睨んだ研究開発力の強化や国際実証環境の構築を軸とした共同研究開発に取り組むことにより、情報通信基盤の共通化を通じた豊かな社会への貢献が期待される。

## ３．採択件数、研究開発期間及び予算

採択件数　　：1件

研究開発期間：平成30年から平成33年までの36か月の予定。

研究開発経費：1件当り62百万円/12か月（税込）を上限とする。
（提案の予算額の調整を行った上で採択する提案を決定する場合がある。）

研究開発体制：本公募は、日欧共同での研究開発プロジェクト（以下、「共同プロジェクト」という）に委託する。日本側の体制については、単独の提案も可能であるが、産学官連携等による複数の研究グループ体制を推奨する。なお、欧州側の体制は欧州委員会の規則に則ること。

課題の日欧対応：本公募は、欧州委員会のHorizon 2020に対応している。

その他　　：本公募は、平成30年度予算成立前に開始するものであるため、予算成立後に課題名称、研究開発期間、研究開発経費、公募内容等

に変更があり得ることをあらかじめご了承ください。

## ４．提案に当たっての留意点

後述する達成目標を実現するための具体的な研究課題を設定し、且つそれら研究課題を担当する機関の役割分担を明確化して提案すること。

各提案には、本公募の「7. 参考」などを参照して、最新技術動向を反映させることを求める。また、本公募は日欧共同公募であるため、次の事項に留意すること。

- 欧州委員会Horizon 2020への提案者との共同プロジェクトとして提案すること。提案者は、情報通信研究機構（以下「機構」という。）(日本側)及び欧州委員会(EU側)のそれぞれに対し、必要な応募書類をそれぞれ提出すること（日本側、或いはEU側の片側だけに対しての提案は受け付けません。）
- 機構は共同プロジェクトの日本側研究機関に研究を委託し、欧州委員会は欧州側研究機関に対して研究資金の提供を行う。
- 採択に関する評価は、日欧共同(機構及び欧州委員会)で行う(詳細は応募要領を参照)。
- 採択後、研究開発の実施過程において、日本側研究機関は欧州側研究機関と共同して活動すること。
- 提案にあたっては機構の「欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発」及び「欧州との連携によるBeyond 5G先端技術の研究開発」の応募要領とともに、欧州委員会の Horizon 2020 Work Programmeを参照すること。
- 提案書のうち、研究開発の内容に係る部分については様式を欧州委員会と共通化しており、 英語で記述すること

## ５．研究開発の到達目標

***Specific Challenge***

Following the integration and federation of IoT with Big Data and Cloud, which has been explored in past coordinated calls, a remaining challenge to address is **enhanced security and privacy** and how the human user deals with the ever-increasing amount of sensors, smart objects and data. Both EU and Japan have excellent competences in the fields of cybersecurity systems and visualisation technologies. Especially, security aspects are of increasing importance in these years. **There is a need for simple, efficient and trustable systems based on advanced technologies combining Security, Cloud and IoT/Big Data technologies** that can provide **intelligent** detection and countermeasures for device malware attacks, automatic vulnerability discovery and

patching, analytics and IoT/Big Data applications. All of these require **advanced cloud and edge computing technologies** and **interoperable IoT devices and platforms.**

These new requirements, including security aspects, will have an enormous impact on the underlying cloud/IoT platforms and associated services, especially for cross-border demonstrations of technologies and applications.

***Scope***

**Advanced technologies combining Security, IoT, Cloud and Big data for a hyper-connected society**

The focus is to research, develop and test advanced technologies combining Security, IoT, Cloud and Big data. The following technologies are expected for research and development: agility against emerging threats; automatic vulnerability discovery and patching; open-sourcing of security tools; IoT security; cloud security; data security; privacy protection; data anonymization; blockchain in the context of IoT/Cloud; critical information infrastructure protection, cross border application demonstrations; etc.

***Expected impact***

- Credible demonstrations based on cross-border business and/or societal applications of robust interoperable technologies identifying policy/legal obstacles (i.e., free flow of data, data protection, data portability etc.).

- Concrete implementations of interoperable solutions that integrate IoT, Cloud and Big Data including security that are candidates for standardisation.

- Facilitation of the development of cloud-enabled, secure and trustworthy IoT/big data applications (i.e., integrating intelligent security systems and visualisation technologies and devices/interfaces).

## ６．研究開発の運営管理及び評価について

- 本研究開発課題における個別課題を日欧共に一体として推進することを目的に、機構は必要に応じて課題間あるいは日欧間の連携を議論・調整する会合を開催する場合がある。受託者はこれらに必ず出席し、連携の推進を図ること。
- 研究開発に当たっては、機構の自主研究との連携を図ること。また、連携を図るため、受託者は連絡調整会議を定期的に設定すること。本公募の性質上、これらの会合は欧州にて開催される場合がある。

- 欧州委員会と機構が共同で行うイベントの例として、合同キックオフ会合（平成30年秋頃を予定）、研究開始から約14か月後及び約26か月後に実施する中間評価（Review）及び研究終了後から約2か月後に実施する終了評価（Review）があり、開催場所は日本と欧州で均等を基本として開催される。
- 機構は、研究開発終了後に追跡評価（成果展開等状況調査を含む）を行う場合がある。
- 機構は、上記以外にも研究開発の進捗状況等を把握するために、ヒアリングを実施することがある。

## 7．参考

研究開発の俯瞰報告書: システム・情報科学技術分野(2017年)
http://www.jst.go.jp/crds/pdf/2016/FR/CRDS-FY2016-FR-04.pdf

2020年及びその後を見据えたサイバーセキュリティの在り方について
https://www.nisc.go.jp/active/kihon/pdf/csway2017.pdf

ITU Cybersecurity Activities
https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

情報通信白書
http://www.soumu.go.jp/johotsusintokei/whitepaper/h28.html

制御システムのセキュリティ
https://www.ipa.go.jp/security/controlsystem/index.html