様式９

日中韓フォーサイト事業
平成２３年度　実施報告書

１．拠点機関

日本側拠点機関：	東北大学大学院情報科学研究科
中国側拠点機関：	上海交通大学
韓国側拠点機関：	韓国科学技術院

２．研究交流課題名

（和文）：次世代のインターネットとネットワークセキュリティに関する研究

（交流分野：情報通信技術）

（英文）：Research on Next Generation Internet and Network Security

（交流分野：Information and Communication Technology）

研究交流課題に係るホームページ：http:// www.it.ecei.tohoku.ac.jp/a3program/

３．開始年度

平成２３年度（１年目）

４．実施体制

日本側実施組織

拠点機関：東北大学大学院情報科学研究科

実施組織代表者（所属部局・職・氏名）：大学院情報科学研究科長・亀山充隆

研究代表者（所属部局・職・氏名）：大学院情報科学研究科・教授・加藤寧

協力機関：筑波大学、金沢大学、会津大学、情報通信研究機構、東北大学工学研究科

事務組織：東北大学情報科学研究科事務部、東北大学国際交流課

相手国側実施組織（拠点機関名・協力機関名は、和英併記願います。）

（１）中国側実施組織：

拠点機関：（英文）Shanghai Jiao Tong University

（和文）上海交通大学

研究代表者（所属部局・職・氏名）：（英文）

Department of Computer Science and Engineering・Professor・Zhenfu Cao

協力機関：（英文）Beijing University of Posts and Telecommunications、

Tsinghua University、Guangzhou University

（和文）北京郵電大学、清華大学、広州大学

（２）韓国側実施組織：

拠点機関：（英文）Korea Advanced Institute of Science and Technology

（和文）韓国科学技術院

研究代表者（所属部局・職・氏名）：（英文）

Department of Electrical Engineering・Professor・Dan Keun Sung

協力機関：（英文）Soon Chun Hyang University

（和文）順天郷大学

５．全期間を通じた研究交流目標

本事業による研究交流を通じ、日中韓の 3 カ国のそれぞれにおいて次世代ネットワーク並びにネットワークセキュリティの分野で先端的な研究を行っている研究者間の人的ネットワークを構築し、情報通信分野において世界的水準の研究拠点を形成することを目標とする。

技術的な課題としては、(1)次世代のインターネット技術、(2)ネットワークのエネルギー消費やリソース利用の効率化を実現する技術、(3)ネットワークの安全性を向上させる技術の 3 つを 3 カ国で共有する。情報通信分野で最重要課題として位置づけられるこれら 3 つの研究項目について世界最先端の研究を実施することにより、今後の世界の情報通信技術の発展に寄与する学術的価値の高い成果を本研究拠点から発信することを目指す。

世界的水準の研究拠点の形成を目指し、本事業中はもちろん事業終了後も将来的に持続・発展可能な研究者間の人的ネットワークを構築することを目標とする。お互いの強みを生かした共同研究の実施、共同での研究成果の発表、研究者間の交換交流などを軸とした研究交流を展開するとともに、研究課題を共有する複数グループ交流や研究者（研究室）単位での 2 者間交流などの様々なレベルでの研究交流体制を構築することにより、強固で緊密に連携した国際研究拠点を形成する。また、日本側研究者には女性 2 名が含まれており、女性の視点に立った研究交流を進めていけることも本研究チームの特徴である。一方、女性研究者を含む若手研究者の育成にも力を入れる。専門技術に精通するだけでなく、学術の幅広い分野に対する理解力や国際舞台でリーダシップを発揮できる能力を備えた若手研究者育成を目標として、若手研究者（特に大学院生）が主導して企画・運営するジョイントセミナーなどを開催する。

以上のような取り組みを通じ、日中韓を中心とした情報通信技術の世界トップレベルの研究拠点を形成する。さらには、その存在を世界に広くアピールすることにより、アジアはもちろん世界中からの人材流入による研究拠点体制の強化を図る。

６．平成２３年度研究交流目標

初年度である今年度は，まずは研究交流課題である「次世代のインターネットとネットワークセキュリティに関する研究」を進めるにあたり，複雑に絡み合い山積する数々の課題の中から優先して取り組むべき課題を選定する．そして，各課題の解決に取り組むにあたり，世界的な研究拠点の構築のために，各拠点がもつ学術的あるいは産業的に優れた技術をどのように効果的に融合・発展させて行けるかについて 3 カ国で協議し，今後持続的に発展可能な研究拠点形成の起爆剤になり得る共同研究の枠組みを確立することを目的とする．またその中において，若手研究者間の交流も並行して行い，若手研究者自身の能力の向上のみならず幅広い世代に渡って緊密に連携した拠点形成への足掛かりとする．

７．平成２３年度研究交流成果

７－１　研究協力体制の構築状況

平成 23 年度は、9 月、11 月、3 月の 3 回、拠点機関所属の研究者を中心とした運営会議を行った。セミナーの開催、共同研究の進め方、共同での論文執筆、来年度の研究交流活動計画などについて議論を交わし、スムーズな研究交流の実施に努めた。

各研究者レベルでは、メールや電話会議などを通じてお互いのアイディアやアプローチなどについて日常的に意見交換および技術検討を行うとともに，研究者の派遣や受入などで直接指導や交流を行い、研究者間の密な連携を図った。

一方、多くの研究者が一堂に会したセミナーでは、複数の研究者による議論などを通じて新たな知見や研究の方向性が得られただけでなく、研究者間の相互理解の深まりによって連携に向けた動きが活発化するなど、研究者間の人的ネットワークを飛躍的に拡大することができた。

以上の通り，今後の拠点形成・強化・発展のための基礎となる研究者間の協力体制を構築することができた。

７－２　学術面の成果

本事業では「次世代のインターネットとネットワークセキュリティ」を研究交流課題として掲げているが、平成 23 年度の研究交流活動により、学術面において次のような成果が得られた。

2012 年 3 月 25 日から 2012 年 3 月 31 日にかけて米国にて開催された国際会議 The 31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012) にて 2 件の論文発表を行った。モバイル通信ネットワークの一形態として、自由に移動するモバイル端末同士が自律的にネットワークを構成するモバイルアドホックネットワークがある。しかしながら、モバイルアドホックネットワークでは、モバイル端末がデータ転

送の役割を担うため、データの転送が不安定になるという問題が存在する。特に、モバイル端末の移動パターンに偏りがある場合や、モバイル端末の密度が小さい場合、この問題はより顕著になる。一方、屋外イベントや災害発生時など、現実にはそのような過酷な状況となる場合は珍しくない。そのため、そのような環境においてもネットワークの接続性を高めて通信を可能にする技術の確立が課題となっている。今回発表した 2 件の論文は、ネットワークの接続性を定量評価するためのモデルを提案したものであり、この課題の解決の一助となるものであり、次世代ネットワークの基盤技術の一端として位置づけられる。当該国際会議は、情報通信分野で世界最大の学会である IEEE が主催する国際会議の中でも採録率が 18% (278/1547) と非常に低く、著名な国際論文誌と同程度のインパクトを持つ会議である。この会議に論文が採択されたことは、当該研究が世界的にみても高く評価されるものであることを裏付けていると言える。

従来の Key Encapsulation/Decapsulation Mechanism (KEM-DEM)方式は効率的な Hybrid 暗号として標準化されており、Threshold KEM (TKEM)方式は分散システムに役立っている。既存のほとんどの TKEM 方式が、システム構築前に結託者を決める静的な結託攻撃しか考えていなかったため、安全性証明が不十分であった。そこで、合成数 order のペアリングに基づいてより強い動的な結託攻撃に対しても安全である TKEM 方式を提案した。関連成果は日本暗号界代表的な国内会議 SCIS2012 で発表し、電子情報通信学会論文誌に投稿した。

中国の拠点機関の Haojin Zhu 准教授の研究グループと合同で、国際会議 2012 IEEE Global Communication Conference (IEEE GLOBECOM 2012)に論文を投稿した。近年、スマートフォンや他の携帯端末の普及に伴い、モバイルベースのソーシャルネットワークの形成が人々の生活に浸透してきている。モバイルソーシャルネットワークにおいて、人々はいつでもどこでも情報を共有したり、さらには外出先などで近くにいる同じ興味や趣味を持つ人を実際に探したりすることが可能になった。しかしながら、意図しない個人情報の漏洩やロケーションプライバシーの侵害などの多くのセキュリティやプライバシーの問題が存在する。今回投稿した論文は、興味やプロフィールを元に、プライバシーを保護しながらマッチングを行うプロトコルを提案している。提案したプロトコルは、セキュリティ解析と実装によって性能が評価され、その安全性と効果が実証された。

７－３　若手研究者養成

共同研究においては、各国のシニア研究者が訪問先において若手研究者向けの講演会を行ったほか、実際に研究方針などについて直接指導するなどし、お互いに若手研究者の育成に貢献した。

韓国で開催されたセミナーには、日本から 20 人、韓国から 13 人、中国から 6 人の計 39 人の学生が参加した。若手研究者にとっては、国際的な舞台で発表・ディスカッションを行う経験を積むことができ、一定の自信を得るとともに能力面での課題についても体感するよい機会となった。さらに、同年代の若手研究者と交流は非常に刺激的であり、研究のモチベーション向上につながるとともに、博士前期課程の学生にとっては後期課程への

進学を真剣に考える絶好の機会となった。

国際会議 IEEE INFOCOM にて発表した論文では、当該研究において主体的な役割を担った博士後期課程の学生を筆頭著者としてほか、実際に国際会議に派遣して発表を行わせた。国際的に競争力のある人材育成の点において非常に有意義であったことに加え、当該学生の研究意欲のみならず他の学生に対してもインセンティブとして作用した。研究拠点としてのアクティビティ向上に繋がるとともに、将来に渡る持続的な研究拠点形成にも寄与すると期待できる。

７－４　社会貢献

研究交流活動の成果については本事業のホームページ上で定期的に公開するなどし、本事業によって日中韓の 3 カ国による研究拠点が形成されていることを世界に向けて発信した。一方、学術面での貢献としては、世界的にトップレベルの国際会議において研究成果をまとめた論文を発表することによって、その成果を広く社会に還元することに努めた。なお、発表論文に関する情報はホームページに掲載している。

７－５　今後の課題・問題点

本事業の初年度に当たる平成 23 年度は、主要メンバー間の相互理解を深めることが最大の目的であったが、お互いの問題意識や取り組みが良く一致する点を多数見いだすことができたという点において、一定の成果があったことは確かである。実際、研究交流期間は 8 ヶ月であったにも関わらず、連携の成果として 2 件の国際会議の発表を行うなど、研究者間連携は順調に進んでいると考えられる。来年度以降の課題としては、より緊密な連携による研究拠点形成に向け、平成 23 年度の研究交流で生み出された連携の芽を確かなものとするために、研究者の往来をさらに活発化させ、若手研究者を含めた研究協力体制の基盤を固めることが重要と考えられる。

７－６　本研究交流事業により発表された論文

平成２３年度論文総数	３本
相手国参加研究者との共著	１本

８．平成２３年度研究交流実績概要

８－１　共同研究

平成 24 年 2 月 11 日から 18 日まで、中国・上海交通大学から Zhenfu Cao 教授をはじめとする 4 名の研究者と、中国・北京郵電大学から Licheng Wang 先生が東北大学と会津大学を訪問した。各大学において、日本側の学生を含む研究者と研究内容について議論した。特に、東北大学においては、次世代のネットワーク技術とプライバシー保護のためのセキュリティ技術の両方が求められるスマートグリッドに関する研究課題について、多角的な

視点から意見交換を行った。一方、以前から議論していたネットワークの耐災害性という観点についても、国際会議 IEEE INFOCOM の論文内容を含め議論した。

韓国の Dan Keun Sung 教授の研究グループと合同で、国際会議 2012 IEEE Wireless Communications and Networking Conference（IEEE WCNC 2012）と 2012 IEEE International Conference on Communications（IEEE ICC 2012）にそれぞれ論文を投稿し、ともに採録が決定した。前者は無線ネットワークにおける通信レート制御技術に関するものであり来年度の 4 月に、後者はアドホックネットワークの接続性向上に関するものであり来年度の 6 月に発表予定である。なお、前者は韓国側が、後者は日本側が主体となって研究を進めたものであるが、実験実施や論文執筆に当たって相互に助言・指導を行うなど、お互いに貢献した。

平成 24 年 1 月 4 日から 9 日まで、中国・北京郵電大学から Licheng Wang 先生をはじめとする 3 人が NICT 来訪し、非可換代数構造に基づく暗号、Pairing ベース暗号 （Composite Order ペアリングの性質及び関連暗号方式の設計）について共同研究を実施した。

平成 24 年 1 月 10 日から 11 日まで、金沢大学の満保雅浩教授、上海交通大学から Qingshui Xue 准教授をはじめとする３人も来訪し、NICT のセキュリティ基盤研究室と研究報告会を行った。①NICT のインシデント技術と Oblivious Transfer 暗号の研究、②上海交通大学の位置情報ベース暗号の研究進捗、③北京郵電大学の非可換暗号の研究進捗を紹介し、活発な議論を行った。A3 メンバー8 人を含めて、計 18 人が参加した。

平成 24 年 1 月 12 日から 13 日まで、筑波大学で講演会を開催し、①北京郵電大学の研究紹介、そして、魔方群ベース暗号と Order を持つペアリングに基づいて秘密分散に関する研究進捗の紹介　②上海交通大学の研究紹介、そして、ＩＤベース暗号 Tight Reduction に関する研究の歴史と挑戦を紹介　③筑波大学全体の研究紹介(暗号の設計から、応用、分析、実装まで豊富な研究課題に関連）　④ ＮＩＣＴで行っている長期利用可能な暗号（ポスト量子暗号とクラウド環境に役に立つ暗号)、について紹介した。参加者達は互いに相手の研究に深く興味を示し、活発な議論を行った。中国来訪者 6 人、ＮＩＣＴ2 人、筑波大学 17 人、計 25 人が参加した。

平成 24 年 3 月 20 日から 27 日までの期間中に NICT と金沢大学から合計 2 名が中国・北京郵電大学の Yi Xian Yang 教授と Licheng Wang 准教授のグループを訪問した。中国側の学生を含む研究者と研究内容について議論した。特に、国内シンポジウムで研究発表を行っていた Threshold KEM 方式の論文について議論することを通して改善を行い、論文誌への投稿までつなげた。更に、インタードメイン向けの暗号技術や多数の署名者が関係するディジタル署名についての現状や研究課題について意見交換を行った。

平成 23 年 11 月 4 日から 15 日まで、及び平成 24 年 1 月 2 日から 18 日までの 2 回にわたり、中国・上海交通大学を訪問し Zhenfu Cao 教授、Haojin Zhu 准教授と研究討論や今後の実施方法などについて意見を交換した。特に、次世代ネットワークの一つのモバイルソーシャルネットワークにおけるセキュリティとプライバシーの問題を協議し、互いの研究分野の視点から様々な課題について検討した。この議論が、国際会議 IEEE GLOBECOM へ投稿

した論文の一部に反映している。

８－２　セミナー

本事業を開始するにあたり、3 カ国の主要研究者間で交流を図るとともに技術課題を共有するために、平成 24 年 2 月 9 日から平成 24 年 2 月 10 日の 2 日間に渡り、韓国・大田市にある韓国科学技術院にて ミニワークショップを開催した。初日は 3 つのパラレルセッション形式、2 日目はグループディスカッション形式で開催した。

本事業の若手中心メンバーとなり得る博士後期課程及び前期課程の学生も含め、各国の研究者がこれまでの研究成果について発表・議論を行い、次世代ネットワーク及びネットワークセキュリティに関する重要課題について問題意識などの共有を図った。また、今後の研究・交流活動についても議論した。なお、期間中に 3 カ国の PI を中心とした研究者・事務者打ち合わせを行い、それまでの活動の総括及び以後の研究交流計画について意見交換を行い、研究交流活動の活発化と円滑な実施を図った。

８－３　研究者交流（共同研究、セミナー以外の交流）

平成 23 年度は実施していない。

９．平成２３年度研究交流実績人数・人日数

９－１　相手国との交流実績

派遣元＼派遣先		日本〈人／人日〉	中国〈人／人日〉	韓国〈人／人日〉	合計
日本〈人／人日〉	実施計画		10/20	41/82	51/102
	実績		12/72	29/121	41/193
中国〈人／人日〉	実施計画	10/20		(21/42)	10/20 (21/42)
	実績	11/82		0/0 (11/44)	11/82
韓国〈人／人日〉	実施計画	10/20	(10/20)		10/20 (10/20)
	実績	0/0	(1/2)		(1/2)
合計〈人／人日〉	実施計画	20/40	10/20 (10/20)	41/82 (21/42)	71/142 (31/62)
	実績	11/82	12/72 (1/2)	29/121 (11/44)	52/275 (12/46)

※各国別に、研究者交流・共同研究・セミナーにて交流した人数・人日数を記載してください。（なお、記入の仕方の詳細については「記入上の注意」を参考にしてください。）

※日本側予算によらない交流についても、カッコ書きで記入してください。（合計欄は（　）をのぞいた人・日数としてください。）

９－２　国内での交流実績

実施計画	実　績
20／40　〈人／人日〉	9／15　〈人／人日〉

１０．平成２３年度研究交流実績状況

１０－１　共同研究

<table>
<tr><td>整理番号</td><td>R－1</td><td>研究開始年度</td><td>平成２３年度</td><td>研究終了年度</td><td>平成２６年度</td></tr>
<tr><td>研究課題名</td><td colspan="5">（和文）次世代インターネットとネットワークセキュリティ</td></tr>
<tr><td></td><td colspan="5">（英文）Next Generation Internet and Network Security</td></tr>
<tr><td>日本側代表者
氏名・所属・職</td><td colspan="5">（和文）加藤寧・東北大学大学院情報科学研究科・教授</td></tr>
<tr><td></td><td colspan="5">（英文）Nei Kato・Tohoku University・Professor</td></tr>
<tr><td>相手国側代表者
氏名・所属・職</td><td colspan="5">（中国）Zhenfu Cao・上海交通大学・教授
（韓国）Dan Keun Sung・韓国科学技術院・教授</td></tr>
<tr><td>交流人数
（※日本側予算によらない交流についても、カッコ書きで記入のこと。）</td><td colspan="5">① 相手国との交流
<table>
<tr><td colspan="2">派遣先
派遣元</td><td>日本
〈人／人日〉</td><td>中国
〈人／人日〉</td><td>韓国
〈人／人日〉</td><td>計
〈人／人日〉</td></tr>
<tr><td rowspan="2">日本
〈人／人日〉</td><td>実施計画</td><td></td><td>10/20</td><td>10/20</td><td>20/40</td></tr>
<tr><td>実績</td><td></td><td>12/72</td><td>0/0</td><td>12/72</td></tr>
<tr><td rowspan="2">中国
〈人／人日〉</td><td>実施計画</td><td>10/20</td><td></td><td>(10/20)</td><td>10/20
(10/20)</td></tr>
<tr><td>実績</td><td>11/82</td><td></td><td>(0/0)</td><td>11/82
(0/0)</td></tr>
<tr><td rowspan="2">韓国
〈人／人日〉</td><td>実施計画</td><td>10/20</td><td>(10/20)</td><td></td><td>10/20
(10/20)</td></tr>
<tr><td>実績</td><td>0/0</td><td>(1/2)</td><td></td><td>0/0
(1/2)</td></tr>
<tr><td rowspan="2">合計
〈人／人日〉</td><td>実施計画</td><td>20/40</td><td>10/20
(10/20)</td><td>10/20
(10/20)</td><td>40/80
(20/40)</td></tr>
<tr><td>実績</td><td>11/82</td><td>12/72
(1/2)</td><td>0/0
(0/0)</td><td>23/154
(1/2)</td></tr>
</table>
② 国内での交流　　9/15　人／人日</td></tr>
<tr><td>２３年度の研究交流活動</td><td colspan="5">相互に複雑に作用するインターネット技術とネットワークセキュリティ技術について、各研究者間で意見交換を行い、様々な課題について議論を行うなど、研究者交流を行った。</td></tr>
<tr><td>研究交流活動成果</td><td colspan="5">様々な知見を持つ研究者同士の相互交流と技術的な議論・検討により、複雑に絡み合った問題の明確化と課題認識の共有が図られ、来年度以降の本格的な研究者間連携に向けた動きへとつながった。</td></tr>
<tr><td colspan="6">日本側参加者数</td></tr>
<tr><td colspan="3">34　名</td><td colspan="3">（１３－１日本側参加者リストを参照）</td></tr>
<tr><td colspan="6">中国側参加者数</td></tr>
</table>

62　名	（１３－２中国側参加研究者リストを参照）
韓国側参加者数	
71　名	（１３－３韓国側参加研究者リストを参照）

１０－２　セミナー

整理番号	S－1
セミナー名	（和文）JSPS A3 フォーサイト事業ミニワークショップ 2012 in KAIST
	（英文）2012 Mini-Workshop of A3 Foresight Program in KAIST
開催時期	平成２４年２月９日　～　平成２４年２月１０日（２日間）
開催地（国名、都市名、会場名）	（和文）韓国、大田市、韓国科学技術院
	（英文）Korea, Daejeon, KAIST
日本側開催責任者氏名・所属・職	（和文）加藤寧・東北大学大学院情報科学研究科・教授
	（英文）Nei Kato・GSIS, Tohoku Univ.・Professor
相手国側開催責任者氏名・所属・職（※日本以外で開催の場合）	Dan Keun Sung・Department of Electrical Engineering, KAIST・Professor

参加者数

派遣先／派遣元	セミナー開催国（韓国）	
日本〈人／人日〉	A.	29/121
	B.	0/0
	C.	0/0
中国〈人／人日〉	A.	0/0
	B.	0/0
	C.	11/44
韓国〈人／人日〉	A.	0/0
	B.	0/0
	C.	17/34
合計〈人／人日〉	A.	29/121
	B.	0/0
	C.	28/78

A.セミナー経費から負担

B.共同研究・研究者交流から負担

C.本事業経費から負担しない（参加研究者リストに記載されていない研究者は集計しないでください。）

セミナー開催の目的		本事業を開始するにあたり、3 カ国の研究者が一堂に会するキックオフミーティングを開催する。各国の研究者のこれまでの研究成果について発表・議論を行い、次世代ネットワーク及びネットワークセキュリティに関する重要課題について問題意識などの共有を図る。また、今後の研究・交流活動についても議論する。さらに、大学院生などの若手研究者にも発表の機会を与えることにより、若手人材の育成を図るとともに、世代を超えた 3 カ国の協力研究体制の強化につなげる。
セミナーの成果		各研究者が取り組んでいる課題について議論することにより、新たな知見や研究の方向性が得られ、研究者間の人的ネットワークを拡大することができた。また、大学院生などの若手研究者にとっては、国際的な舞台で発表・ディスカッションを行う経験を積むことができ、一定の自信を得るとともに能力面での課題についても体感するよい機会となった。さらに、同年代の若手研究者と交流は非常に刺激的であり、研究のモチベーション向上につながるとともに、将来的なキャリアとしての研究者の選択にプラスの効果があった。なお、3 カ国の PI を中心とした研究者・事務者打ち合わせでは、今後の研究交流計画について意見交換を行った。
セミナーの運営組織		韓国側 PI を含む韓国側参加研究者が運営を行った。日本・中国側参加者はプログラム作成・当日の運営などを補助した。
開催経費分担内容と金額	日本側	内容　旅費　　金額　　2,520,190 円
	中国側	内容　旅費　　金額　約 1,130,000 円
	韓国側	内容　上記以外の開催経費の全て　金額　約 1,500,000 円

１０－３　研究者交流（共同研究、セミナー以外の交流）

平成 23 年度は実施していない。

１１．平成２３年度経費使用総額

	経費内訳	金額（円）	備考
研究交流経費	国内旅費	1,949,150	
	外国旅費	4,700,690	
	謝金	0	
	備品・消耗品購入費	7,996	
	その他経費	102,029	
	外国旅費・謝金等に係る消費税	240,135	
	計	7,000,000	
委託手数料		700,000	
合　　計		7,700,000	

１２．四半期毎の経費使用額及び交流実績

	経費使用額（円）	交流人数<人／人日>
第１四半期	0	0 人／0 人日
第２四半期	218,090	2 人／6 人日
第３四半期	1,187,480	8 人／39 人日
第４四半期	5,594,430	51 人／245 人日
計	7,000,000	61 人／290 人日