Empowered by Innovation

NEC

東北大学

２０１３年３月１８日

報道関係各位

日本電気株式会社
東北大学サイバーサイエンスセンター

ＮＥＣと東北大、災害など通信インフラ途絶時に Wi-Fi活用により臨時ネットワークを構築する技術を開発

～緊急時のコミュニケーション手段を迅速に提供

ＮＥＣと東北大学サイバーサイエンスセンター（以下、東北大学）は、災害時など通信インフラが途絶した際に、エリア内に設置したWi-Fiアクセスポイントを臨時ネットワークとして活用し、自治体からの情報配信や住民のコミュニケーションを実現する技術を開発しました。

大規模な災害時には、通信事業者のネットワーク設備の損壊や通信の混雑により、通信インフラが利用不能になり、固定網、モバイル網を利用した情報伝達が困難になります。このため、通信インフラが途絶しても、情報伝達を可能にする技術が求められています。

このたび開発した技術は、利用者の端末から送信された情報をWi-Fiアクセスポイント内に蓄積し、可搬型のアクセスポイントを経由して目的の利用者に近いアクセスポイントに伝達することで、利用者間の通信を実現するものです。また、近接する複数のアクセスポイントを自動的にグループ化し伝達経路の計算量を削減する経路制御技術を開発し、最大1,000台のアクセスポイント間で通信が可能です。これらにより、災害時など通信インフラが途絶した際に、広範囲に渡って利用可能な情報配信・通信サービスを実現します。

さらに本技術は、利用者の端末からネットワーク認証を行う際に、予め設定した優先利用者と一般利用者を区別する機能を有しています。これにより、災害時の膨大な通信から、自治体、警察、消防などからの通知を優先的に配信できます。

このたび開発した技術の特長は、次のとおりです。

1.スイッチの切り替えで公衆 Wi-Fi スポットから臨時ネットワークへモード変更できる、アクセスポイントを開発（ＮＥＣ）

スイッチを切り替えることで、平常時の公衆 Wi-Fi スポットを緊急時の臨時ネットワークへモード変更できる、Wi-Fi アクセスポイントを開発。本アクセスポイントは、接続した利用者の端末から送信された情報を蓄積し、他のアクセスポイントに近づいた際に情報を伝達する DTN(注 1)機能、ソーラーパネルやリチウムイオン電池の電気を利用する機能を搭載。これらにより、災害時に通信インフラや系統電源が途絶されても、アクセスポイントを自動車に搭載したり、スーツケース大の可搬型アクセスポイントを利用したりすることで、通信インフラに依存しない臨時ネットワークの構築が可能。

2.大規模な臨時ネットワークの構築を実現（ＮＥＣ）

アクセスポイント間のネットワーク経路を制御する技術を開発。本技術は、近接する複数のアクセスポイントの接続関係に基づいて自動的にグループ分けを行い、異なるグループに属するアクセスポイント群とグループ単位での経路制御を実行。これにより、個別端末の宛先への経路計算が不要になり、グループ化しない場合と比較して 100 台程度から最大 1,000 台と、大規模なアクセスポイント間の通信を実現。

3.利用者に応じて通信の優先度を設定可能（東北大学）

利用者の認証について、通信インフラから途絶された状態でも、各アクセスポイントとの通信で実現する技術を開発。EAP-TLS(注 2)認証方式を利用し、アクセスポイント内の認証サーバと、利用者の端末内に予め発行したクライアント証明書を通信して認証。クライアント証明書に、予め利用者属性情報を付与することで優先利用者と一般利用者を区別できるため、災害時に大量に発生する情報に対して通信の優先度を設定可能。

ＮＥＣと東北大学は今後も、災害に強い情報通信技術の開発と製品化に積極的に取り組んでまいります。

このたび開発した技術は、平成23年度よりＮＥＣと東北大学が参画している、総務省の「情報通信ネットワークの耐災害性強化のための研究開発（大規模災害においても通信を確保する耐災害ネットワーク管理制御技術の研究開発）」の一環として進めてきた研究成果です。

なおＮＥＣと東北大学は、今回の成果を、3月25日（月）から26日（火）まで、ウェスティンホテル仙台および東北大学で開催される「耐災害ＩＣＴ研究シンポジウム及びデモンストレーション」において出展する予定です。

以上

（参考）

「耐災害 ICT 研究シンポジウム及びデモンストレーション」(3 月 25 日(月)～3 月 26 日(火))

http://www.nict.go.jp/info/event/2013/03/130325-1.html

（注 1）DTN(Delay/Disruption/Disconnection-Tolerant Network)

リンクの切断が多発したり大きな遅延が生じたりする不安定なネットワークにおいても、各ホップでデータの蓄積を行いながら通信可能時に小セグメント単位でデータの転送を行うことにより信頼性の高い通信を実現する方式。

（注 2）EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)

クライアントとサーバの両方が電子証明書を発行し、相互認証を行う方式。相互にデジタル証明書を発行・管理するため、高度なセキュリティを保つことが可能。

＜本件に関するお客様・研究者からのお問い合わせ先＞
ＮＥＣ　知的資産 R&D 企画本部 広報グループ
https://form.nec.jp/nec/276rd/4b126d/Inquiry.do?fid=4b126d

東北大学 サイバーサイエンスセンター
担当：曽根秀昭・後藤英昭
電話：（０２２）７９５－６０９１／７９５－６０９０
E-Mail：csi-staff@isc.tohoku.ac.jp

＜本件に関する報道関係からのお問い合わせ先＞
ＮＥＣ　コーポレートコミュニケーション部　山梨
電話：（０３）３７９８－６５１１
E-Mail：r-yamanashi@ct.jp.nec.com

東北大学 サイバーサイエンスセンター
担当：曽根秀昭・後藤英昭
電話：（０２２）７９５－６０９１／７９５－６０９０
E-Mail：csi-staff@isc.tohoku.ac.jp