

非常時における地域の安全・安心確保のための ϵ -ARK デバイスを核とした 情報通信環境の研究開発

– 第4報 ϵ -ARK デバイス開発の進捗状況 –

大野浩之† 井町智彦† 松島英章‡ 前田明夫‡ 西麻里‡ 米田稔§

† 金沢大学総合メディア基盤センター ‡ 北陸通信ネットワーク株式会社 § 株式会社 COM-ONE

1 はじめに

ϵ -ARK デバイスは、大規模災害発生時等の非常時の自助共助期に必要な可能性が高いさまざまな通信機能や通信サービスを携帯電話や電子手帳のような小型軽量で可搬性の高いデバイスにソフトウェアパッケージとしてコンパクトに実現したもので、いわば「電子版スイスアーミーナイフ」である [1] [2]。著者らは、この ϵ -ARK デバイスを核とした新たな情報通信環境の開発を 2006 年から開始し、非常時における地域の安全・安心確保のため ϵ -ARK デバイスを積極的に活用する環境を地域社会に実装し、その有効性の検証を続けている。[3] 本報では、2011 年 1 月の時点での ϵ -ARK デバイスおよび関連する機構の研究開発の進捗について報告する。

2 研究開発の進捗状況

ϵ -ARK プロジェクトが手がける研究開発事項は数多く、本報で全てに言及せず ϵ -ARK/AP, ϵ -ARK/SS, ϵ -ARK/DMS に焦点をあてる。

2.1 ϵ -ARK/AP

ϵ -ARK/AP (ϵ -ARK Access Point) は「即席の無線 LAN アクセスポイント」を提供する機能で、(1) 無線 LAN アクセス環境を提供するための無線 LAN アダプタと、(2) 対外通信を行うための通信装置 (3G データ通信カードを用いる場合が多いが PHS やアナログモデムなども利用可能) を ϵ -ARK デバイスに装着して実現する。 ϵ -ARK デバイスのベースとなる電子手帳や携帯電話にこのような機能を期待することは、 ϵ -ARK デバイスの研究開発を始めた 2006 年の時点では一般的ではなく、仮に即席の無線 LAN アクセスポイントを実現しても当時の携帯電話には無線 LAN 機能は搭載されていなかったため、携帯電話の所有者が ϵ -ARK/AP を

活用してインターネットにアクセスすることはできなかった。しかし、2008 年 7 月に Apple 社の iPhone が国内発売された頃から状況が変わり始め、スマートホンが携帯電話の主流となりつつある現在、スマートホンだけでなく従来型の携帯電話でも無線 LAN 機能を搭載した機種が増えている。これに伴い、テザリング (Tethering) という言葉や概念も広く認知され、現在ではテザリング可能な携帯電話や同様な機能を提供するモバイルルータが各社から発表されている。

しかし、テザリングできる携帯電話やモバイルルータが、 ϵ -ARK/AP を完全に代替できるわけではない。まず、テザリングあるいは同等のアクセス環境には (1) 同時利用可能なユーザ数に制限があったり、(2) 無線 LAN 側の機材同士が通信することを想定しておらずブロードキャストは当然としてユニキャストも行えなかったり、(3) フィルタリングやルーティングに強いポリシーを導入して不要不急のトラフィックを阻止するといった機能がない。これらは、テザリングできる携帯電話やモバイルルータが想定する利用環境では必須ではないため問題にならないが、 ϵ -ARK デバイスが想定している非常時における情報通信環境では、同一アクセスポイントに接続するデバイス同士が通信することも想定される。また、同時に複数の対外接続を許しそれを静的あるいは動的に切り替える機能もない場合が多い。これらの機能を有する ϵ -ARK/AP (およびポリシー制御を担当する ϵ -ARK/CDS) には引き続きアドバンテージがある。

2.2 ϵ -ARK/SS

ϵ -ARK/SS (ϵ -ARK Service Station) は、 ϵ -ARK デバイスの活動を支援するための機構である。通常は、 ϵ -ARK デバイスの有効活用が想定される「非常時に陥っている地域」(以後、被災地と記す)の外で稼働し、 ϵ -ARK デバイスの活動をインターネット経由で支援する。 ϵ -ARK/SS が提供する重要な機能の一つにリバース WEB プロキシがある。 ϵ -ARK デバイスを使って被災地内で WEB サーバを起動して情報発信を行った場合、被災地外にリバースプロキシがないと外部から被災地へのアクセスが過多になる可能性がある。コンテ

†Hiroyuki Ohno, Tomohiko Imachi
(Information Media Center, Kanazawa University)
‡Hideaki Matsushima, Akio Maeda, Asari Nishi
(Hokuriku Telecommunication Network Co.,Ltd.)
§Minoru Yoneda (COM-ONE Ltd.)
 ϵ -ARK = Electronic/Emergency ARmy Knife

ンツが静的なものであれば、リバースプロキシではなく、被災地で作成したコンテンツを ε -ARK/SS 上に転送して ε -ARK/SS のみから情報発信すれば、被災地で稼働中の ε -ARK デバイスへのアクセスを極力抑えられ、被災地とリバースプロキシ間の通信が間欠的でも対応できる。

ε -ARK/SS は、これまでは Linux ベースの実機で実現してきたが、現在 ε -ARK/SS の仮想化を積極的に推進し、あらかじめ設定を済ませた ε -ARK/SS の仮想機のイメージを用意しておき、必要に応じてこれをコピーすることで簡単に複製を増設でき、負荷変動に柔軟に対応できるようにしつつある。

2.3 ε -ARK/DMS

ε -ARK/DMS (ε -ARK Document Management System) は、第1報でも述べたように、非常時の自助共助期に生成されるさまざまな形態のデジタルデータに適用する情報管理の枠組みである。非常時の自助共助期にあつては、電源供給や対外通信が不安定あるいは欠如している場合であっても、被災状況を記録するために大量の写真や動画がデジタルカメラや携帯電話によって撮影されることが最近の災害経験から明らかになっている。これらの静止画や動画はデジタルデータであり ε -ARK/DMS による管理の対象である。著者らは、まずは静止画を対象に、非常時の自助共助に資するデジタルデータの管理方法を検討し、 ε -ARK/iD と X4iD を導入して管理を行っている。 ε -ARK/iD は、任意のデジタルデータをに対して算出可能な以下の形式の ID である。

形式: (接頭辞)-(版識別子)-(新規生成した UUID)-(当該データのハッシュ値)-(電子署名等) [.(拡張子)]

例: e-ARK-ID-V1R3-F2EC7154-03DA-11DF-866F-0019E308B0E6-A69B11E5-D79AE407-B2D24412-FC192512-0FDA1BCC-00.tgz

このような ID を作る場合、ID を一元管理する組織を作つてそこから逐一発行してもらう方法もあるが、非常時においてはそのような組織と通信して ID が取得できるとは限らない。そこで (1)UUID を用いて現在だけでなく過去にも未来にも存在しない 128bit 長の番号を現場で各自が独自に生成し、(2)当該データのハッシュ値追加して改ざんや破損の有無を検出可能にし、(3)必要であればデータを作成者の秘密鍵や受取人の公開鍵で暗号化して電子署名することで悪意の第三者の介入を阻止できるようにした。このようにして生成した文字列はデジタルデータの安全安心な一元管理に有用ではあるがこの文字列の前にホスト名などを加えて URL 化すると全長が 100 文字以上になり、人間が取り扱うには長過

ぎるという問題がある。そこで、これを短縮することを考え、X4iD を定めた。URL の短縮には bit.ly, TinyURL などの既存のサービスがあるが、X4iD は URL を UUID version 5 を用いて 128bit ハッシュ値にし、これを 32bit ずつに区切った上でそれぞれを 10 進数で表現したもので、(1)アルゴリズムが公開されていて誰でも生成できる、(2)X4iD をキーにして URL を取得するサービスが必要であるが、(3)X4iD から本来の URL を取得した際、その URL が正しいものか偽装や改ざんされたものかを受取人側で検証できるため、(2)の URL 取得サービスはそれほど信頼できなくてもよい、という特徴を持つ。以下に示すように、X4iD は決して短くはなく、もとの URL が短い場合にはもとの URL より長くなる場合もあるが、全てが数字でかつ固定長であるため扱いやすく、通常はすべての数字を使う必要はなく、ハイフンで区切られた 4 組の 12 桁の数字のうちの一つを参照すれば十分であるといった特徴を持つ。

URL: <http://www.ipsj.or.jp>

UUIDv5: 7debc1e2-da84-5cbe-b621-ab81d16acd64

X4iD: 132235496346-255940237421-346625439053-453610525803

3 おわりに

本報では、 ε -ARK/AP の優位性、 ε -ARK/SS の仮想化、 ε -ARK/DMS における新たな ID の導入について述べた。いずれも、非常時における地域の安全・安心確保に向けた ε -ARK デバイスの発展に向けた取り組みである。次報(第5報)では、今後研究開発が佳境にはいる案件について述べる。

謝辞

本研究は、総務省戦略的情報通信研究開発推進制度(SCOPE)地域 ICT 振興型研究開発案件として平成 21 年度に新規採択されたプログラムに基づいて実施したものである。総務省および同省北陸総合通信局の関係各位に深謝する。

参考文献

- [1] 猪俣敦夫, 大野浩之. 非常時の自助共助に資する ε -ARK 端末を Apple iPhone で実現するための技術的・制度的考察. 情報処理学会 第 3 回インターネットと運用技術研究会 2008-IOT-3-4, pp. 13-18, 2008.
- [2] 猪俣敦夫, 大野浩之. 乾電池でも運用可能な「非常時対応電子アーミーナイフ」(ε -ARK)を用いた非常時情報通信システムの実装. *Internet Conference 2008*, pp. 15-24, 2008.
- [3] 大野浩之. 非常時における地域の安全・安心確保のための ε -ARK デバイスを核とした情報通信環境の研究開発-第 1 報 総論-. 情報処理学会創立 50 周年記念(第 72 回)全国大会, pp. 3-107-3-108, 2010.