Vol.2010-FI-98 No.4
Vol.2010-DD-75 No.4
2010/3/4

非常時における運用を念頭においた小規模文書管理システム (第 2 報)

大　野　浩　之[†1]

著者らが ε-ARK プロジェクトで取り組んでいる非常時の自助共助に資する情報通信基盤の研究開発では，ε-ARK デバイスを核とした非常時における運用を念頭においた情報管理機構，情報発信機構，情報流通機構の開発が進んでいる．本報告では，これらの機構のうち，前二者について非常時における文書管理システムの視点で報告する．

Information Management System for Emergency Situations

Hiroyuki Ohno[†1]

The ε-ARK project is currently developing a new information management and information delivery system for using in an emergency. This system has been being realized using ε-ARK devices and will be especially useful for self-help and mutual-help after huge natural disasters. This report describes the newest status of development of these systems mainly from the point of document management.

1. はじめに

大規模な自然災害のような予期せぬあるいは予想を越えた非常事態 (本報ではこれを「非常時」のひとつとしている) が発生した場合，その最も初期の段階においては，被災者が自らで行動して危機的状況を回避したり (この状況を「自助」と呼び，自助が必要な時期を「自助期」と呼ぶ)，被災者同士がお互いに助け合ったり (同様に「公助」および「公助期」と呼ぶ) して，公的な支援 (公助) の継続的な実施 (公助期) をひたすら待つ時期が存在する．過去の大規模災害と復興の歴史を調べてみても自助期および公助期にあっては，水，食糧，衣類，医薬品などの確保だけでなく適切な情報の提供と情報を流通させる環境の提供が必須である．情報源としてラジオが唯一最善だった時代もあるが，現代の日本社会においては，情報通信が発達し人々が日頃から情報通信に深く依存しているため，非常時における自助や共助を継続させるためには，これまで以上に適切な情報共有や情報受発信が必要となる．

ところで，本報では非常時として大規模自然災害を想定して論じるが，大規模自然災害以外にも新興・再興感染症の爆発的蔓延 (パンデミック)，大規模な停電による都市機能の停止，事故や故意による有毒物質の大規模な拡散，大規模なテロリズム発生による社会不安の増大を始めとするさまざまな非常時が考えられる．これらを通信インフラや電力インフラへのダメージに着目して分類すると，電力供給や通信インフラには特段のダメージを与えない非常時[⋆1]と電力供給や通信インフラに大きなダメージが及ぶ非常時[⋆2]とがある．たとえば，パンデミックそのものは，電力供給インフラや情報通信インフラを直接破壊することはなく，自助共助に際して電力も情報通信も平常時と変わりなく利活用できる．しかし，日本における大規模自然災害の典型例である大地震の場合は，被災地周辺では電力供給インフラや情報通信インフラに壊滅的な影響が及ぶことがある．したがって，電力や通信インフラの機能障害に着目した非常時の分類は，非常時における情報通信を考える上で重要であるが，本報ではこれ以上述べず，以下では大規模自然災害の発生時を想定する．

大規模自然災害による非常時にあっては，電力供給や被災地内外の通信が満足に確保できないといった，平常時とは異なる厳しい制約が被災者の活動の大きな障害になる[1)]．よって，被災地域の安全・安心を確保するためには，日常生活に何ら制約がない平常時とも，非常時であっても平常時に近い情報通信環境が提供され始める「公助期」とも異なる，非常時の自助共助期に資する情報通信環境について十分に検討しておく必要がある．

著者が主導する「ε-ARK プロジェクト」は，2007 年からこの問題に取り組んでおり，このプロジェクトの下で研究開発が続けられているのが「ε-ARK デバイス」である．ε-ARK デバイスは，大規模災害発生時等の非常時に必要となると予想されるさまざまな通信機能や情報通信サービスを，必要な時にはいつでも稼働できるよう設定等をあらかじめ整えた上で携帯電話や電子手帳といった日頃から持ち歩いているデバイス上にコンパクトにまとめたものである．ε-ARK デバイスは，いわば「スイス・アーミーナイフ」の電子版なので，「非常時対応電子式アーミーナイフ」(Electronic/Emergency ARmy Knife) の頭文字から

†1 金沢大学 総合メディア基盤センター
Information Media Center, Kanazawa University

⋆1 著者はこれを「分類 1 の非常時」と呼んでいる
⋆2 同様に「分類 2 の非常時」と呼ぶ

Vol.2010-FI-98 No.4
Vol.2010-DD-75 No.4
2010/3/4

ε-ARK と命名した[2)3)]．

現在，著者らは ε-ARK デバイスを核とした新たな情報通信環境を開発し，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．一例として，ε-ARK デバイスを用い，3G データ通信アダプタで対外接続を確保してアドホックな無線 LAN アクセスポイント (ε-ARK/AP) を構築し，平常時にもこれを積極的に利用してきた．近年では無線 LAN (WiFi) 機能を内蔵した小型デバイスが増え，携帯電話にも WiFi 機能が積極的に搭載されるようになり，ε-ARK/AP と同様な機能を提供する製品も販売されるようになった．ε-ARK/AP は，機能的にはこれらの機器と類似するが，ただのルータではなく豊富なプロキシやフィルタ機能を豊富に持つ点が異なり，引続き優位性がある．

ε-ARK デバイス開発は，次の段階として非常時の自助共助に資する軽量で効率のよい情報管理機構 (ε-ARK/DMS)[⋆1]について検討を開始し[4)5)]．，対外接続速度が平常時より遅くかつ断続的にしかできない状態であっても，相対的にサイズの大きな写真などのファイルを効率よく被災地外に送り出す機構 (ε-ARK/DDD)[⋆2]の開発や，被災地内で効率よく情報を流通させる機構 (ε-ARK/CDS)[⋆3]の開発にも着手している[6)]．本報告では，ε-ARK/AP に続くこれら 3 つの新機構のうち ε-ARK/DMS と ε-ARK/DDD について述べる．ε-ARK/DMS は，2008 年 9 月に本研究会で発表した第 1 報の延長上に位置する[7)]．

2. ε-ARK/DMS：非常時の自助共助に資する情報管理

2.1 非常時における情報管理の制約

非常時の自助・共助期に被災地で生成されやりとりされる多種多様な情報は，非常時ゆえに管理が行き届かず，後日参照する可能性があってもその場限りで廃棄されてしまい，参照しようとした時にはすでに入手できなかったり，どこかに保管されいることは確かでも見出せなかったり，微妙に内容の異なる報がいくつも見付かり区別できなかったりすることが考えられる．たとえば，近年の大地震や大水害などにおいては，現状を記録してその後の救助や復興に役立てるために，被災者や救援者や行政関係者の手によって大量の写真が多数のデジタルカメラによって撮影されている．このような場合，写真には何らかの統一的な識別番号 (以下 ID) を振った上でネットワーク上のストレージで管理し，ID を頼りに当該写真にアクセスできる体制があるとよい．平常時にはこのような作業は何ら問題なく実現できるが，非常時において以下のような制約がある．

(1) どのような ID も，同じ用途に用いる他の ID と値が重複してはならないので，通常は，事前に一定の範囲の番号をまとめて割り当てもらってそこから必要に応じて切りだしたり，必要になるたびにどこかに申請して割り当てを受ける方法が用いられている．前者では，必要数より多い番号の割り当てを受ける必要があり，効率的でない．また，割り当てを全く受けていない場合には，どこかに申請して割り当てを受ける必要があり，後者と同じ状況になる．後者の場合，非常時においては被災地と被災地外との通信が途絶しているか不安定であることを考慮するなら，ID の割り当てに際してどこかにその都度照会することは現実的ではない．仮に通信が確保できても，割り当て業務を行う組織が被災している場合もあり得るので，割り当て業務を行う組織を前提とせずに，他者が生成した ID と衝突しない ID を独自に生成できなければならない．

(2) あるデータに ID を割り当てる場合，ID 自体や ID が指すデータに改ざんや取り違えが生じることがある．どこかに問い合わせることなく改ざんや取り違えの有無を検証できるしくみが必要である．

(3) 被災地外のデータ保管場所にデータを保存しようとしても，平常時とは異なりすぐにはアクセスできない場合があることに配慮が必要である．

2.2 ε-ARK/iD と X4iD の概要

上述した点を考慮し，ε-ARK/DMS では ε-ARK/iD と ε-ARK/X4iD (あるいは単に X4iD) という二つの ID を新たに定め，デジタル文書の管理に投入した．ε-ARK/iD は，対象となるデータに割り当てる ID で，対象となるデータに対するある種のハッシュ値である．一方，X4iD は，ε-ARK/iD URL (ε-ARK/iD を URL 化したもの) を含む任意の URL に対して 4 組の 12 桁の 10 進数 からなる文字列を割り当てるしくみである．ε-ARK/iD や X4iD の算出にあたっては，良質の乱数に基づくハッシュ関数が必要になるが，この部分に関してはいたずらに独自開発したりせず，アルゴリズムが公開され安全性が客観的に確認されている手法を用いるのが望ましい．検討の結果，ε-ARK/iD では次節で述べる UUID を採用した．

以後，被災地で作成した文書や写真は，PDF 形式や JPEG 形式などにデジタル化されていることを前提とし，これらをデジタル文書と呼ぶことにする．ε-ARK/DMS では，デジタル文書が作成されたら ε-ARK/iD を算出して付与する．その際，デジタル文書のファ

⋆1 DMS = Document Management Service.
⋆2 DDD = Discrete Data Delivery
⋆3 CDS = Contents Delivery Service

Vol.2010-FI-98 No.4
Vol.2010-DD-75 No.4
2010/3/4

イル名を ε-ARK/iD と同じにすると管理が楽になるが，これは必須ではない．次々節で述べるようにε-ARK/iD は文字列としては長く，100 文字を越えるので，デジタルカメラのメモリカードに今も見られる FAT のようなファイルシステムにはなじまない．このような場合や，技術的には可能でも非常時ゆえにそのような作業をする時間的余裕がない場合には，ファイル名を ε-ARK/iD に一致させる必要はない．ε-ARK/iD は，ε-ARK/iD を生成した情報通信機器固有の情報と時刻情報から生成する他とは重ならない一意な値 (ユニーク値) と，対応するデジタル文書のハッシュ値の双方を含むので，ε-ARK/iD に対応するデジタル文書は，ファイル名が不明だったり途中で変更されても検索できる．このため，デジタル文書を被災地から被災地外に送出する際，まず目録として ε-ARK/iD だけをメール等で送りだし，ε-ARK/iD に比べるとはるかに大きなデジタル文書は，対外接続回線の状況に応じて別途送出したとしても ε-ARK/iD から問題なくデジタル文書を見つけ出せる．この場合，ε-ARK/iD が紛失したり改ざんされたりしなければ，デジタル文書の取り違えが回避できるだけでなく，文書の改ざんや破損も検出できる．また，ε-ARK/iD ではユニーク値とハッシュ値を別々に持つため，被災地から同一のデジタル文書が複数回送信された場合，ε-ARK/iD に対応するデジタル文書が見付からなくても，ハッシュ値が等しいデジタル文書があれば，これをもって代用することが可能になる．デジタル文書とε-ARK/iD の双方が同時に改ざんした場合の対処については，次々節で述べる．

ε-ARK/iD には上で述べたような利便性があるが，文字列としては長いため，ファイルとして扱いにくいだけでなく，QR コードなどの二次元バーコードに収容すると QR コードが大きくなってしまうし，数字や一部の記号しか表現できない大多数の一次元バーコードにはなじまない．英数字が利用可能な EAN-128 のような一次元バーコードでも，バーコードが現実的でないくらい長くなってしまう．ε-ARK/iD を文字列として印刷したりこれを口頭で伝達するのも長すぎて適当ではない．そこで，ε-ARK/iD とは別に，任意の URL に 4 組の 12 桁の 10 進数 (48 桁の整数) を割り当てるしくみを作った．これが X4iD である．なお，ε-ARK/iD 自体は URL 形式ではないが，ε-ARK/iD を URL 形式にすることで X4iD を求めることが可能になる．X4iD の詳細については後述する．

2.3 UUID

汎用一意識別子 (Universally Unique Identifier) として，RFC4122 で規定されている UUID は，どこかに問い合わせたり登録することなく手元で簡単に算出でき，必ず一意に決まって他と衝突することのない 128bit 値で，`DBFBF54A-B6C8-42F4-A8B6-88193DCDAB82` のように 32 桁の 16 進数をハイフンで 5 つの部分に区切って表現する．RFC4122 では，主旨の異なる 5 種類の UUID を定められている[⋆1]．

UUID の 5 つのバージョンのうち最も知られているのが UUID version 1 (以後 UUIDv1 と表記．他のバージョンについても同様) で，UUID を生成する機器の MAC アドレスと生成開始時刻を基に，過去から未来に渡って世界中で生成されうるどの UUIDv1 とも異なる 128bit 値を生成する．一般に単に UUID と言った場合はこの UUIDv1 を指すことが多く，すでにさまざまな形で利用されている．本研究でも ε-ARK/iD を算出する際に利用している．

UUIDv1 以外では X4iD が UUIDv5 を利用している．UUIDv5 は，特定の名前空間 (たとえば URL や FQDN) に属する個々の名前に対する 128bit のハッシュ値である．UUIDv5 は，ハッシュ値算出のアルゴリズムに SHA-1 を用いているが，SHA-1 ではなく MD5 を採用したのが UUIDv3 である．MD5 に衝突例が見つかった現在，UUIDv5 を使わず UUIDv3 を積極的に使う理由はない．UUIDv4 は，純粋に 120bit の乱数である (8bit 分は予約されている)．UUIDv1 と類似した UUIDv2 は現在はあまり使われていない．

2.4 ε-ARK/iD の導入

すでに述べたように ε-ARK/iD は，対象とするデジタル文書に対して算出する ID で，非常時における制約にも配慮して以下のように定めた．

(接頭辞)-(版識別子)-(UUID)-(SHA-1)-(オプション) [.(拡張子)]

接頭辞には `e-ARK-iD` を用いる．頭辞に続く (版識別子) は，ε-ARK/iD の構成を識別するための長さ 4 の文字列で，一桁のバージョン番号と一桁のリビジョン番号を，それぞれ文字 `V` と 文字 `R` に続いて記述する．たとえば,「バージョン 1, リビジョン 3」を意味する版識別子は `V1R3` となる．版識別子により，将来 ε-ARK/iD の構成が変わっても混乱を回避できる．(UUID) は，当該 ε-ARK/iD を生成した時点での UUIDv1 なので，この部部分が同じ値を持つ ε-ARK/iD は存在しないことが保証されている．(UUID) の部分は，この ε-ARK/iD が,「いつ」「どこで」生成されたかを確認する際のヒントになる．(SHA-1) は，当該デジタル文書のハッシュ値である．アルゴリズムには SHA-1 を用いる．当該デジタル文書が改ざんあるいは破損していた場合にはそれを検知できる．作成者の公開鍵で署名したり受取人の公開鍵で暗号化する場合には，署名や暗号化を施す前にハッシュ値を計算する必要がある．

⋆1 RFC 4122 では 5 種類の UUID を「バージョン (version)」と呼んでいるが，UUID における「バージョン」は，通常の意味のバージョンと異なり，むしろ「種別」や「タイプ」に近い．すなわちバージョン番号の大小に時間的前後関係はなく，version 1 から version 5 まで，すべてが有効である．

Vol.2010-FI-98 No.4
Vol.2010-DD-75 No.4
2010/3/4

(SHA-1) に続く (オプション) は，本報告執筆時点の最新バージョン (V1R3) では暫定的に 00 を挿入しているが，ここに作成者や受取人の公開鍵 ID (GnuPG を想定しているので 8 桁の 16 進数文字列) を挿入できる．作成者の公開鍵 ID の前には S を受取人の公開鍵 ID の前には R を付与し，両者をそのまま連結するので，(オプション) 部分は最大で 18 文字になる．作成者の公開鍵 ID を記した場合には，ε-ARK/iD が指すデジタル文書は，当該公開鍵 ID の所有者 (ε-ARK/iD 作成者) の秘密鍵で暗号化することで電子署名しなければならない．この電子署名により，悪意を持つ者が不適切なデジタル文書を作成し，このデジタル文書に対応する ε-ARK/iD を誰かの名を語って作成してもこれを見破れる．特定の誰かにのみ受け取って欲しい場合には，(オプション) 部分には受取人の公開鍵 ID を挿入し，デジタル文書は受取人の公開鍵で暗号化する．これにより受取人以外は当該デジタルデータを読み取ることができなくなる．作成者の電子署名を施したり受取人のために暗号化するには，自分および受取人の GnuPG の公開鍵が公開鍵サーバに登録し，自分および受取人の 公開鍵 ID を知っている必要があるが，これは平常時から対応して手元の ε-ARK デバイスなどに保管しておけるので，非常時において必要な公開鍵が利用できるというのはそれほど無理な仮定ではないだろう．

最後尾の (拡張子) の長さは任意である．不要なら付与しなくてよい．

以上より，実際の ε-ARK/iD は，以下のような文字列になる．

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

ε-ARK/iD 算出の対象となったデジタル文書は，ε-ARK/iD と同じファイル名で特定のウェブサイト上に置くこととし，ε-ARK/iD の冒頭に http://ホスト名/ディレクトリ名/ を付与して ε-ARK/iD を URL 化する．このような形式の URL を “ε-ARK/iD URL” と呼ぶ．以下はその一例である．

```
http://foo.example.org/baa/e-ARK-ID-V1R3-F2EC7154-03DA-11DF-866F
-0019E308B0E6-A69B11E5-D79AE407-B2D24412-FC192512-0FDA1BCC-00.tgz
```

2.5 UUIDv5 の導入

URL 化した ε-ARK/iD は，ホスト名の FQDN が短くオプション部分がなくても 110 文字程度はあり，通常は 120〜130 文字に達する．オプション部分を活用すればさらに 10〜20 文字増える．そこで，ε-ARK/iD の作成と同時に，ε-ARK/iD の作成者が 当該デジタル文書の最終的な保存場所を示す ε-ARK/iD URL の UUIDv5 を計算して「UUIDv5 と URL のペア」を作成し，デジタル文書の URL の代りに UUIDv5 をアナウンスし，UUIDv5 と当該 URL のペアは別途検索してもらう方法が考えられる．

この方法は，以下の特徴を持つ．

(1) UUIDv5 と対応する URL のペアについては，インターネット上に不用意に置いて誰かが改ざんしても深刻な事態にはならない．なぜなら誰かが UUIDv5 と URL のペアを改ざんしても，取得した URL の UUIDv5 を手もとで再計算し，取得したペアの UUIDv5 と一致するか確認できるからである．もし一致しなければ，このペアは不正なペアなので単に廃棄すればよい．

(2) もし，UUIDv5 の一部が誤って伝わった場合，ハッシュ計算のアルゴリズムに SHA-1 を用いる UUIDv5 の性質により，誤った UUIDv5 に対応する URL が存在する可能性はゼロとみなせる．よって誤ったデジタル文書を手にすることはない．

(3) 適切な UUIDv5 を得ている場合には，適切な ε-ARK/iD URL に到達でき，適切な ε-ARK/iD URL であればその先にあるファイルが真正であるか否かは，ε-ARK/iD を構成する SHA-1 によるハッシュ値やオプションとして付加されている公開鍵 ID を使って検証できる．

(4) もし，悪意によってあるいは錯誤によって，実在するが意図したものではない UUIDv5 と URL のペアが選ばれ，この UUIDv5 が渡された場合には，UUIDv5 を介して意図しない URL を得たことにこの時点では気付けない．もし悪意であるなら，この URL の先に何が待ち受けているかわからない．

(5) しかし，このようにして得た URL であっても，まず ε-ARK/iD URL 形式に則っているかを調べ，次にオプションとして ε-ARK/iD 作成者の公開鍵 ID が付与されていたら，公開鍵を取得して作成者を確認した上で作成者の電子署名を確認し，さらにオプション部分に自分の公開鍵で暗号化されていることを示す自分の公開鍵 ID が含まれていたら，とりあえず当該 URL にアクセスしてファイルを取得し，自分の秘密鍵で開けるか確認すればよい．

(6) ここまでしても，誰かが悪意のファイルを作成し，電子署名を用いて誰が作成したかを明らかにし，受取人の公開鍵を使って暗号化してまで ε-ARK/iD URL と UUIDv5 のペアを作成し，さらにこれを公開し，その UUIDv5 を送り付けてきた場合には，当該デジタル文書を開いてしまう可能性がある．しかし，これは確信犯が信念をもって起こすセキュリティ侵害であり電子署名付暗号化ファイルのやりとりでも起きるリスクなので，ここではこれ以上は追求しない

(7) 残る問題は，UUIDv5 とともに公開あるいは検索可能になる URL への DoS 攻撃で

Vol.2010-FI-98 No.4
Vol.2010-DD-75 No.4
2010/3/4

ある．これについても，アクセスの多い WEB ページ上で別の WEB ページの URL が一般公開された場合と同程度のリスクと考えられる．ε-ARK/iD を考える上で重要な問題であるが，ここではこれ以上は検討しない．

繰り返しになるが，デジタル文書に必要なら電子署名や暗号化を施した上で，オプション部に公開鍵 ID を挿入した ε-ARK/iD を ID を生成し，これをもとに作成した ε-ARK/iD と同名のファイルを ε-ARK/iD URL が指す場所において公開し，利用者には UUIDv5 をアナウンスという方法には，非常時の混乱にあってもデジタル文書の安全・安心な管理につながる．また，ε-ARK/iD URL は，短くても 110 文字以上で長さは一定しないが，UUIDv5 ならハイフンを入れても 36 文字の固定長である．相対的に短いという点と固定長であるという点からも，UUIDv5 は取り扱い易さの点で ε-ARK/iD より優れている．

2.6 X4iD の導入

前節で活用のメリットを述べた UUIDv5 と等価で，10 進数とハイフンのみで構成され UUIDv5 と相互変換できるのが X4iD である．X4iD は，UUIDv5 から以下の手順で生成できる．より詳しい生成手順は付録に記した．

(1) UUIDv5 の 128bit 値を 32bit ごとに区切る．
(2) 4 つの 32bit 値をそれぞれ整数で表現する．
(3) 4 つの 32bit 値の順番が失われないように先頭に順番を示す一桁の整数 (1〜4) を付加し，末尾にチェックサムを付加し，4 組の 12 桁の整数を構成する[⋆1]

X4iD は，10 進数とハイフンのみから構成される固定長文字列なので，長く複雑な URL や，X4iD よりは短いが 16 進数である UUIDv5 より扱いやすい．すなわち，X4iD はハイフンを除去すればすべて数字であり，加えて各々の 12 桁の 10 進数の末尾にはチェックデジットがあって単純な錯誤であれば入力した時点で誤りを検出できるので，ε-ARK/iD では対応できなかった，一次元バーコードでの表現，音声での伝達，音声認識装置による受信，電話のタッチトーンなどでの伝達も可能になる．X4iD は大多数の一次元バーコードで表現できるが，特に EAN-13 バーコードとの親和性に配慮している．EAN-13 バーコードは 13 桁の整数で，先頭の 2 ないし 3 桁が国コードあるいは特定目的を示し，その後にメーカーコード (5 桁)，アイテムコード (5 桁) と続き，最後の 13 桁目がチェックデジットとなる．通常，EAN-13 バーコードを作成する者はメーカーコードを正規に取得しなければならず，その上でアイテムコードの 5 桁だけが自由に利用できる領域になる．すなわち，EAN-13 バーコードは X4iD より長い 13 桁だが，12 桁の空間を勝手に利用することは許されない．ただし，先頭の 2 桁が 20〜29 の場合は,「インストア・コード」として自由に利用できる，いわば「ローカルアドレス」空間になっている．X4iD の各組の冒頭の 1 桁は 1〜4 であるので，各組の冒頭に “2” を加えるとそれぞれ 13 桁の整数になり，なおかつ冒頭の 2 桁は 20〜29 の範囲に収まる．よって，最終桁のチェックデジットの算出方法にだけ配慮すれば，先頭に “2” を付与した X4iD は，EAN-13 バーコードと互換性を持つ．X4iD が EAN-13 バーコードと互換性を持つことで，X4iD を EAN-13 バーコードで表現した時，EAN-13 用のバーコードリーダはチェックデジットエラーを起こさずに X4iD を受け入れる．なお，EAN-13 対応バーコードリーダから X4iD を読む場合には，“2” で始まる 13 桁になっているので，X4iD を処理するソフトウェアでは冒頭の “2” を削る必要がある．

さまざまな利用形態が考えられる X4iD は，便利であるが不可逆変換なので，X4iD からは元になった URL を求めることはできない．したがって，X4iD をキーにして URL を取得するしくみが別途必要である．このしくみを充実させて非常時においても検索可能な状態にできれば，X4iD は URL の代用になる．X4iD は元の URL のハッシュ値を SHA-1 を用いて算出しているので，X4iD の一部 (たとえば特定の組) だけを使って検索しても十分実用的な検索ができる．もし X4iD の一部を使って検索して複数の URL がヒットした場合には，X4iD の全部を用いて再検索すれば確実だが，再び X4iD の一部を用いて検索したとしても，当初の検索で用いた X4iD よりも長い一部分や異なる部分を用いて再検索する方法も十分実用的である．もし，検索の結果複数の URL が得られたら，得られた URL から X4iD を算出しなおし，検索に用いた X4iD と一致するか調べれば正しい URL を特定できる．この URL から X4iD を「検算」する方法は，検索の結果得られた URL が一つだけだったとしても，安全確保のために必須である．

2.7 X4iD の保存と検索

ここまでは，何らかの検索サービスをインターネット上に構築し，このサービスに X4iD の全部あるいは一部を与えて対応する URL を取得し，取得後に X4iD を再計算する「検算」を行う流れを想定していたが,「X4iD と 対応する URL のペア」は，1 ペアあたり高々数 100 バイト程度の大きさであることと，X4iD と対応する URL のペアを検索するサービスが非常時においても確実に稼働する保証が現時点ではないことから，特別なデータベースを新たに用意しなくても，検索エンジンのクロールにかかる形でテキストファイルとしてあちこちに分散して配置する方法もあり得る．また，個人のコンピュータが多数参加する形

⋆1 10 進数 12 桁の整数は，符号なし 32bit 整数の最大値よりも大きいので，電子手帳や携帯電話などの 32bit CPU 機では単一の整数としては扱いにくい．X4iD の算出手順はこれらの事情にも配慮している．

Vol.2010-FI-98 No.4
Vol.2010-DD-75 No.4
2010/3/4

の分散型のファイル共有システムに,「X4iD と 対応する URL のペア」についての情報を「放流」する方法もある．この場合，X4iD や URL が改ざんされる可能性があるが，得られた URL は再計算によって真偽を確認できるので，深刻な問題は生じない．

2.8 ε-ARK/DMS の試作と評価

以上の検討をもとに，UNIX 環境 (Mac OS X 10.5 と Linux (2.4/2.6)) 上で ε-ARK/DMS を試作した．ε-ARK/DMS の中核をなすのは，以下の動作をする 1000 行を越えるシェルスクリプトで， UNIX 系 OS に標準搭載されている各機能に特化した伝統的なコマンド群や，perl, python といったスクリプト言語，convert, ghostscript, netpbm のようコマンドラインから利用できる多機能なツールを等を組み合わせている．上記以外に，一次元，二次元バーコードのイメージを生成する部分は perl モジュールをいくつか取得した上で自作した．また，最終的な印刷イメージを調整する部分も perl で書き起こした．

- PDF あるいは JPEG ファイルを読み込み， ε-ARK/iD と X4iD を生成する．
- X4iD に対応した一次元バーコード (EAN-13, Code39, NW7) や 二次元コード (QR-code, DataMatrix) 等のイメージを生成する．
- 元の画像，上記で作成したバーコードイメージをレイアウトし，最終イメージを作成する．
- 第一報で報告した「MW-260 バッテリ駆動型モバイルプリンタを用いた Bluetooth ラスタープリンタ」に上記の最終イメージを lpr コマンドを介して送る．
- X4iD と URL のペアに関する情報や，URL が指す先に置かれるデジタル文書 (PDF ファイルあるいは JPEG ファイル) を tar.gz 形式でアーカイブして保存．
- このアーカイブは，回線状態がよいと判断された際に，手動で起動する別のスクリプトによって，転送先に scp された後，展開される．

図 1 には，デジタルカメラで撮影した写真を上記のシェルスクリプトで処理した例を示す．左側の作例では，写真だけでなく EAN-13 形式の一次元バーコードと二次元コード (QR コードおよび CodeMatrix) が出力されている．右側の作例では，写真だけで，バーコードは出力されていないが，左側の写真部分も右側の写真部分もその四隅には，X4iD が小さく印刷されている．X4iD 専用サイト (`http://id.e-ark.org/X4iD/`) にアクセスして X4iD を入力すると，作例ではモノクロで印刷されていた写真の原本を入手できる．

図 2 には，X4iD 専用サイトにおいて運用中の「X4iD から URL を検索するサービス」の主な画面を示す．左側が X4iD を入力する画面で，４組の X4iD のうちの最低でも一組入力すれば検索が行われる．この例では NoScript が JavaScript を拒否しているが，検索

図 1 ε-ARK/DMS による出力例
Fig. 1 Sample Output of ε-ARK/DMS

は正常に行われる．もし，JavaScript を拒否しなければ，入力したデータを CGI 側に送る前に桁数やチェックデジットの確認を行いその結果を表示するようになっている．右側は，検索結果の画面で，X4iD に対応した URL が表示されているのがわかる．

上記のスクリプトが安定稼働したので，これを Mac OS X および Linux 2.4/2.6 上の LPD にプリンタフィルタとして組み込んだ．このスクリプトを組み込んだプリンタを e-ARK-DMS とすると，以下のように PDF ファイルや JPEG ファイルを処理すると，内部で上記のスクリプトが動き最終的には図 1 のような印刷出力が得られる．非標準ポートで動かしているのは，Mac OS X や Linux 機の本来プリンタ環境とぶつからないようにするためである．それと同時に tar.gz 形式のアーカイブも作成される．

```
% lpr -Pe-ARK-DMS@127.0.0.1%11515 sample.pdf
% lpr -Pe-ARK-DMS@127.0.0.1%11515 sample.jpg
```

今回利用した LPD による印刷システムは，古くから UNIX システムを触って来た者には手に馴染んだシステムであり， ε-ARK/iD や X4iD の付与や，その後の印刷やアーカイ

Vol.2010-FI-98 No.4
Vol.2010-DD-75 No.4
2010/3/4

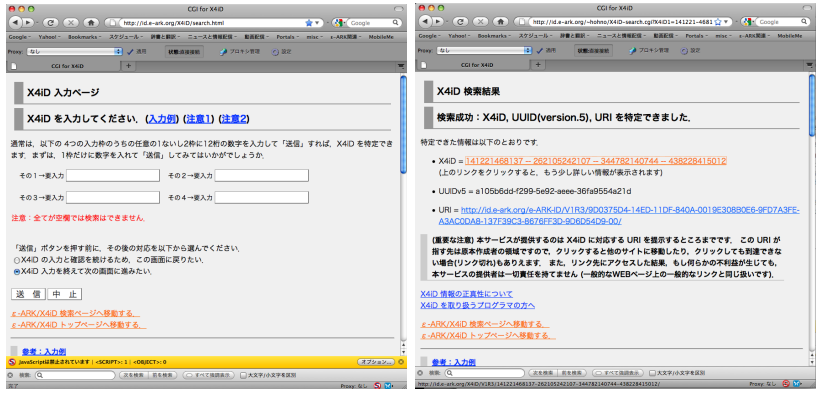

図 2 X4iD から URL を検索する CGI
Fig. 2 CGI for Finding URL from X4iD

ビングまでもが lpr コマンドだけで行えるので十分満足できる．しかし，Mac OS X の一般的なアプリケーションからも利用するには，少なくとも CUPS 環境から利用できなければならない．幸い，CUPS には，LPD プリンタを「IP プリンタ」として駆動するしくみが備わっているので，CUPS 側のプリンタ設定において上記の e-ARK-DMS を「localhost の 11515 番ポートで動く LPD プリンタ」として登録して対応した．ひとたび CUPS プリンタとなると，CUPS 上からは「標準的な PostScript プリンタ」に見えるので，特にプリンタドライバを用意することなく e-ARK-DMS と言う名前の ε-ARK/DMS 対応プリンタを利用できる．

さらに，Mac OS X の場合は，bonjour というゼロコンフィギュレーション機能が利用できるので，ε-ARK/DMS が稼働している Mac OS X 上で e-ARK-DMS プリンタのプリンタ共有を有効にするだけで，ネットワーク上の他の Macintosh から ε-ARK/DMS が利用できるようになる．この場合も，他の Macintosh からは当該プリンタが「標準的なポストスクリプトプリンタ」に見えるため，プリンタドライバのインストールは不要である．

さらに，Windows 機においても，Apple 社が提供する bonjour for Windows という無償提供のソフトウェアをインストールすれば，Macintosh と同様に ε-ARK/DMS は「標準的なポストスクリプトプリンタ」に見えてストレスなく利用できる．Windows 機の場合には，bonjour fro Windows をインストールしなければならないのでゼロインストレーションというわけではないが，でき上がったばかりのプリンタドライバをインストールするのと，リリース後一定時間が経過したある程度汎用性のあるソフトウェアをインストールするのでは後者の方がストレスなく受け入れてもらえることは明らかである．

3. ε-ARK/DDD：非常時の自助共助に資する情報発信

本報では，デジタル文書はあらかじめ特定の ε-ARK デバイス上に集約されていることを想定して議論してきたが，不安定で帯域の限られた対外接続を多くの ε-ARK デバイスが共有している時に，テキストベースのメールなどに比べてサイズが大きい静止画や動画を多くの ε-ARK デバイスが勝手に被災地外へ送信し始めれば，十分な帯域を確保できない不安定な対外接続回線を圧迫してしまうので検討が必要である．

特に写真に関しては，Eye-Fi カードが非常時における情報発信にプラスの意味でもマイナスの意味でも大きな影響を及ぼす可能性がある．WiFi インタフェースを持つ SD メモリカードである Eye-Fi カードは，デジタルカメラに装着して撮影するとデジタルカメラ側からは普通の SD メモリカードに見えるが，あらかじめ設定した無線 LAN にアクセスできる状況になると，メモリカード内の写真の転送を開始する．設定の仕方やファームウェアのバージョンによって挙動は異なるが，無線 LAN に接続した Eye-Fi カードは，(1) Eye-Fi manager というソフトウェアが動いている 自分自身の母艦となるパソコン，(2) Eye-Fi 社の専用サーバ の両方を探し，状態がよい方のサーバに向けて写真の転送を始める．さらに写真転送後に (1) と (2) は同期を行う．したがって，被災地に暫定的に構築された ε-ARK/AP にアクセス権を持つ Eye-Fi カードがあった場合，このカードの母艦となるパソコンが同じ ε-ARK/AP 内に存在しない状態で写真を撮影すると，インターネット上の Eye-Fi 社のサーバに向けて写真の転送を始めてしまう．量と頻度にもよるがこれは対外接続回線の圧迫につながりかねない．

被災地において写真の撮影と写真による情報発信は重要であるが，限られた対外接続回線を写真の転送で埋め尽くすわけにはゆかない．したがって，ε-ARK/AP には以下の機能を持たせる必要がある．

- Eye-Fi カードの外部へのアクセスをブロックする機能
- Eye-Fi カードの母艦と同様のふるまいをするソフトウェアを用意し，Eye-Fi カードからの写真転送を引き取り，Eye-Fi manager を搭載した母艦が存在しなくても Eye-Fi カードの写真転送をネットワーク内にとどめる機能．

すでに，Eye-Fi manager の代りになる ruby で書かれたスクリプトが存在するので，これをインストールして Eye-Fi カードの鍵をインストールしたところ，Eye-Fi カードはこ

Vol.2010-FI-98 No.4
Vol.2010-DD-75 No.4
2010/3/4

のスクリプトに対して写真を送ってくるようになった．今後はこのメカニズムを整理し，被災地での写真による情報発信を効率よく適切に行える環境を整備する．

4. おわりに

本報告では，ε-ARK/iD, X4iD を導入し，非常時の自助共助に資する軽量で効率のよい情報管理機構について検討を行った．また，テキストファイルと比べると相対的に大きな写真などのファイルを効率よく被災地外に送り出す機構の一つとして Eye-Fi カードの活用について述べ，実用的な動作を行っていることを述べた．今後は，被災地内で効率よく情報を流通させる機構 (ε-ARK/CDS) の開発にも注力する．

付　　録

付録 1：UUID の算出 UIUD は，python なら以下のような 1 行スクリプトで算出できる．

- UUIDv1
  `python -c 'import uuid; print uuid.uuid1()'`
- UUIDv5
  `python -c 'import uuid; print uuid.uuid5(uuid.NAMESPACE_URL,"http://e-ark.org/")'`

付録 2：X4iD の算出 X4iD の算出手順を “http://www.ipsj.or.jp/” から X4iD を求める過程を例に示す．

(1) URL から UUIDv5 を求める．
- http://www.ipsj.or.jp/ → 7debc1e2-da84-5cbe-b621-ab81d16acd64

(2) UUIDv5 からハイフンを削除し，32 桁の 16 進数文字列を得る．
- 7debc1e2-da84-5cbe-b621-ab81d16acd64
  → 7debc1e2da845cbeb621ab81d16acd64

(3) これを 8 桁ずつに区切り，4 組 (1 組〜4 組) に分ける．
- 7debc1e2, da845cbe, b621ab81, d16acd64

(4) それぞれの組では 8 桁の 16 進数文字列を 4 桁ずつに分け，それぞれを 5 桁の 10 進数文字列に変換する．5 桁に満たない場合は先頭にゼロを補い，5 桁を維持する．以下は 1 組の例．
- 7debc1e2 → 7deb, c1e2
- 7deb → 32235, c1e2 → 49634

(5) こうして得られた 5 桁の 10 進数文字列 2 つを文字列として単純結合して 10 桁とし，さらに先頭に組番号を付与して 11 桁の 10 進数文字列を作る．
- 32235, 49634 → 3223549634 → 13223549634

(6) 書籍の ISBN 表示等で使われている EAN-13 バーコードとの親和性を維持するため，(i) この 11 桁の 10 進数文字列の先頭に暫定的に “2” を付加して 12 桁の 10 進数文字列にし，(ii) EAN-13 バーコードと同じ mod 10 weight 3 を用いて 1 桁のチェックデジットを算出して末尾に付与し，(iii) 先頭に暫定的に付加した “2” を削除して 12 桁の 10 進数文字列にする．
- 13223549634 → 213223549634 → 2132235496346 → 132235496346

(7) 他の組についても同様の処理を行い，12 桁の整数文字列 4 組を揃える．これが X4iD である．
- 132235496346 255940237421 346625439053 453610525803

(8) 4 組の 10 進数文字列 をハイフンで結合し，全長 51 の単一文字列にしてもよい．X4iD と区別したい場合は，X4iD(CAT) と表記する．
- 132235496346 255940237421 346625439053 453610525803
  → 132235496346–255940237421–346625439053–453610525803

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．また，X4iD まわりについては，猪俣敦夫先生 (奈良先端科学技術大学院大学)，すずきひろのぶ氏 (鈴木裕信事務所)，Paul Hoffman 氏 (VPN コンソーシアム) らとの議論が重要であった．ここに記して感謝する．

参　考　文　献

1) 猪俣敦夫，多田浩之，大野浩之ほか：大規模災害等における非常時情報通信システムに対する社会的・制度的課題と提案，情報処理学会第 103 回情報システムと社会環境研究会 2008-IS-103，pp.1–8 (2008).
2) 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).
3) 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).
4) 大野浩之，井町智彦，松島英章，前田昭夫，　西麻里，　米田稔：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，第 50 会全国大会予稿集 6F-1 (2010).
5) 大野浩之，井町智彦，松島英章，前田昭夫，　西麻里，　米田稔：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 2 報) 普及啓発活動と実証実験について，第 50 会全国大会予稿集 6F-2 (2010).
6) 大野浩之，井町智彦，松島英章，前田昭夫，　西麻里，　米田稔：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 3 報) 新たな情報提供環境について，第 50 会全国大会予稿集 6F-3 (2010).
7) 大野浩之：非常時における運用を念頭においた小規模文書管理システム，情報処理学会 第 68 回デジタルドキュメント研究会 2008-DD-68-2，pp.9–14 (2008).