低コスト運用でユーザフレンドリな安否情報システムの開発

Development of a low running cost and user friendly safety information system

長谷川孝博，井上春樹，八巻直一
Takahiro Hasegawa†, Haruki Inoue, Naokazu Yamaki

国立大学法人 静岡大学 情報基盤センター
〒432-8561 静岡県浜松市中区城北 3-5-1

Center for Information Infrastructure, Shizuoka University
Johoku 3-5-1, Nakaku, Hamamatsu, Shizuoka 432-8561, Japan

概　要

WEB データベースによる安否情報システムを開発した．本システムは，統合認証システムとの連携や名簿情報等の個人情報の大量初期投入を一切行わずにサービスを始動できる．これらの特徴は，サーバのクラウドコンピューティング化や遠隔地設置を容易なものとし，低リスクで可用性の高いサービスを実現する．管理者は，認証コード付き URL を利用者毎に送信し，これを受けた利用者は文字入力を一切行うことなく，簡易認証を完了できる．安否情報はパソコンや携帯端末からボタン選択のみで投稿することができる．これらの仕組によって，非常時における安否情報の回収率を向上できる．また，安否情報は常時登録可能であるが，最終の登録時刻から一定時間のみインターネット上で検索可能となる．オプトイン方式による利用者の登録確認，パスワードのハッシュ照合，WEB ページのセッション管理，WEB データベースのクラッキング対策においてセキュリティ面での充実を図りつつも，開発した CGI はコンパクトな分量に収めた．本論文では，開発した安否情報システムの仕様およびその背景，システム開発における要点，ならびに静岡大学における導入の報告を行う．

キーワード

Safety Information System, Disaster, WEB Database, BCP

1. はじめに

UPKI イニシアティブ[1]に代表されるように統合認証システムは，これからの大学情報インフラ整備におけるコアシステムのひとつであることは間違いない．一方で，安否情報システム[2,3]は，名簿情報は勿論のこと，通常大学では公式に管理してない携帯電話番号や私的なメールアドレス，その時点の健康状態や所在地などの個人情報との関わりが切り離せないデリケートなシステムと言える．また，自然災害や新型インフルエンザのパンデミックなど，生死に関わる非常時にこそ真価を発揮しなければならない安否情報システムは，情報の機密性(C: Compatibility)，完全性(I: Integrity)，可用性(A: Availability)の重要度や割合が，平常時に活用する情報インフラやサービスとは異なる相(phase)にあると考えられる．そのため，通常のリスク受容基準を超えるシステム仕様も検討に含める必要がある．

本論文では，平常時においては一般の情報システムとほぼ同等のリスクを許容しつつ，非常時にその真価を発揮できるような情報回収率の高い安否情報システムについて，仕様を検討し，簡易な WEB データベースの開発を行った．

その結果，本システムは通常，学内に設置する統合認証システムとの認証連携を行うことはせず，また運用開始時における名簿情報などの個人情報の大

† Corresponding author: cithase@ipc.shizuoka.ac.jp

量投入も不用なものとした．そのため遠隔地やクラウド設置を前提としたシステムの立ち上げを容易に行うことができた.また本システムの最大の特徴は，非常時における安否情報を迅速かつ簡易に高い回収率で実現するための認証の仕組にある．開発した Perl CGI の主要部（利用者に公開している部分）は 700 行程度で見通しが良く，それでいて，利用者の安心が得られるようセキュリティ上の複数の配慮や仕組を実装した.

開発した安否情報システムの仕様や実装方法についてその詳細を報告する．**図 1** は，パソコンによりアクセスしたときのトップ画面である.

2. システムの仕様

2.1 統合認証システムとの非連携について

安否情報システムを統合認証システムに連携させて認証を行わせようという考えは自然であるが，本システムでは他システムとの連携を一切行わないだけでなく,稼働初期値において利用者(安否情報システムに安否情報を登録し公開できる利用者)の名簿情報等を含む一切の個人情報を完全なゼロの状態から始動できるシステム仕様とした．その理由を以下に述べる.

統合認証システムは，学内の全構成員が日頃から十分に活用していなければ，パスワード忘れ等の認証不能により安否情報の回収率が低下する恐れがある．特に，統合認証システムがあらゆる学内情報サービスと高度に連携していない発展途上の段階では，上級学年になるにつれ，その利用機会が減るため認証成功率もそれに応じて低下する傾向は否めない．同様に，教職員においても専門分野や役職の違いによる利用頻度にばらつきがあり，統合認証システムだからといって高い認証成功率を確保できる保証はない.

また，地域の情報インフラが壊滅的被害を受けるような大規模災害においてもサービスを継続しなければならない安否情報システムは，遠隔地に設置されることが常である．このことは，通常学内設置さ

図 1 安否情報システムトップ画面

れる統合認証システムとの連携の悪さを示唆し，さらには，統合認証システムの持つ厳密なデータ管理の特性が，非常時における安否情報システムの柔軟な運用要求の妨げになる可能性もある．このような理由から，当安否情報システムでは，統合認証システムだけでなく他のシステムとのオンライン連携は行わない仕様とした．

一方，高度に成熟した統合認証環境や学内ポータルサイトの強みを活かした安否情報システムの例に文献[2]がある．

2.2 名簿情報の非投入について

安否情報システムは，名簿情報を初期設定しなくとも稼働開始できる仕様とした．本システムでは，利用者自身がアカウント登録することで初めて個人情報がサーバに蓄積される．このようにした理由は，初期設定として全学の名簿情報を持たせることに対するセキュリティ上の懸念の声や，正規構成員の家族や友人，さらには地域住民に対しても段階的にサービスを公開できるような柔軟な仕様を優先したことによる．このことは，結果的に統合認証システムとの連携を行わないという仕様方針とも馴染みが良い．

2.3 利用者との親和性を高めるための工夫

1) 安否情報の公開制限

本システムでは，通常時の一定公開時間（平常時は 24 時間を設定している）内に安否情報を登録した利用者（以後，「有効登録者」という）の安否情報だけを，インターネット上の不特定多数の閲覧者（以後，「閲覧者」という）が閲覧できる．ただし，閲覧者は，安否情報を確認したい有効登録者の氏名の一部を入力して氏名検索にヒットさせる必要があるため，公開中の有効登録者の安否情報を網羅的に閲覧できるものではない．例えば全有効登録者の氏名リストは管理者でなければ引き出せない．このように閲覧方法や公開時間に制限を設けたのは，全利用者が気軽に安否情報の登録試験を行えるようにとの配慮からである．これは，平常時に馴染んでいないシステムでなければ非常時に有効活用できないだろうという考えに基づく．また，一般に非常時は事態が収拾するまで数日から数週間を要するので，当然ながら管理者は有効安否情報の公開時間を容易に設定変更できるようにしている．ここで，有効安否情報とは，平常時から非常時に移行するインシデント発生時刻後に登録された安否情報のことである．

2) 安否情報の入力の容易さ

管理者は非常時または訓練時には，全利用者に対して安否情報登録を促すメールの一斉送信を行うことができる．一斉送信されるメールには，利用者毎にサーバ側で生成された認証コード付き URL が記載されており，これを受信した利用者はその URL をクリックし，アクセスするだけで，簡易認証を完了し安否情報を登録できる．ただし，この方法で安否情報を登録すると，データベース上の認証コードは変更されるため，同 URL で 2 回目以降のアクセスがなされた場合はその無効を判断して，メールアドレスとパスワードによる認証に切替える．この仕組によって，非常時における安否情報の入力の簡便さとセキュリティのバランスを調整した．

この仕組は 1)インシデント発生後にメールを受信した全ての利用者は ID やパスワードを忘れていても安否情報が入力できる，2) 携帯 端末の文字入力に不慣れな利用者でもクリックするだけで認証を完了できる，3)非常時におけるあらゆる認証の煩わしさから解放されることで安否情報の回収率を向上できる，などの点で有効に機能すると考える．**図 2** に携帯で受信した場合のメール文例を示す．

静岡大学 安否情報システム
長谷川孝博 様

2009-05-25 08:29:00
【静岡県 震度 3】が発生しました．
安否情報を入力して下さい．
http://xxxxxxxx.shizuoka.ac.jp/xxxx.cgi?opt=xqHoyGWKo2iJhB0Jh&id=32
↑ クリックするだけで安否情報が入力できます！

連絡文・・・
管理者による連絡文を以下に添えることができる．

図 2 認証コード付き URL を含む管理者による一斉送信メールの例

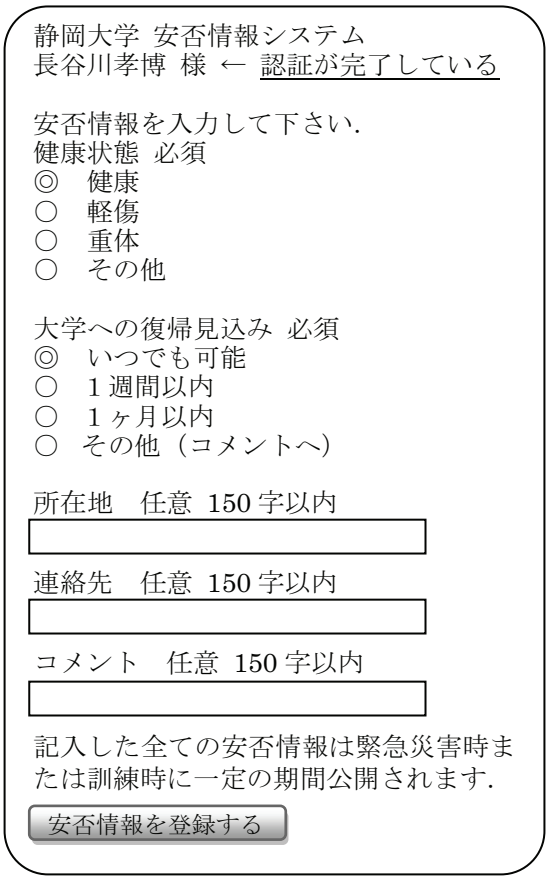

図 3 認証コード付き URL による簡易認証と安否情報入力画面の例

入力項目は,「健康状態」と「復帰見込み」の 2 項目のみをラジオボタンによる必須入力項目とし，所在地，連絡先，コメントなどの文字入力項目は全て任意の入力項目とした．前述の認証コードによる認証を利用すれば，パソコン利用者も携帯端末利用者も文字入力を一切行うことなく，最低限の安否情報を登録できることになる．**図 3** は図 2 の認証コード付き URL をクリックした直後の簡易認証が完了した画面である．利用者は即座に安否情報を入力できる．

3）インシデント発生時刻とメールの一斉送信

管理者が専用ページから全利用者毎に認証コード付 URL メールの一斉送信を行う際には，まず，インシデントのタイトルと発生時刻を分単位で設定できるようにした．ここでインシデントの発生時刻は次のような理由で重要となる．

サーバの性能に任せて 1 万人を超える利用者に性急なメールの連続送信を行うと，多くの利用者を持つ携帯電話キャリアや ISP 側では，この動作を迷惑メールの大量送信と誤認し，以後のメールを転送拒否してしまう可能性がある．これでは安否情報の十分な回収ができなくなる．この問題を回避するためにメールの連続送信間隔を 1 秒としているが，それでは，1 万人への一斉送信の場合は単純に 1 万秒以上を要してしまう．そこで，インシデント発生時刻に基づき，一斉送信ターゲットを 1)全利用者，2)インシデント発生時刻の後に安否情報を登録していない利用者,3）インシデント発生時刻の後に安否情報の登録した利用者，に切替えて，状況に応じて無駄なくメール送信を行えるようにした．

なお，本システムでは，管理者専用 CGI からメールの一斉送信を行っている．このような操作では，全ての送信が完了するまでブラウザのセッションが継続するため，この間にタイムアウトが起こると処理が不完全のまま終了してしまう．この問題は，メール一斉送信の子プロセスを fork 文でバックグラウンドに生成することで完全に解決できた．

4）オプトイン方式によるアカウント登録

システムへのアカウント登録の際には，いたずら登録の防止，メールアドレスの存在および真正性確認のために，登録メールアドレスに送られてきた暗号キー付き URL をクリックしなければ登録が完了しないオプトイン方式を採用した．ここで，オプトイン方式とは，登録確認のための認証コード付き URL が記載されたメールを，利用者の登録したメールアドレスに送信し，利用者がその URL へアクセスして初めて登録が完了するというものである．メールアドレスは主メールアドレスと携帯端末等の副メールアドレスの 2 つが登録できる．主メールアドレスは現在のところ大学のドメイン名を含むものしか受け付けないという単純な制限で，利用者を大学構成員のみに限定している．この制限は設定変数で容易に解除できる.主メールアドレスはユーザ ID の役割も担う．

5）地震 RSS 情報との連携

安否情報システムの設置目的は，地震災害のみを想定しているものではない．しかしながら，前触れもなく一瞬のうちに周辺地域の情報インフラを破壊してしまう地震災害に対しては，自動運行の仕組が

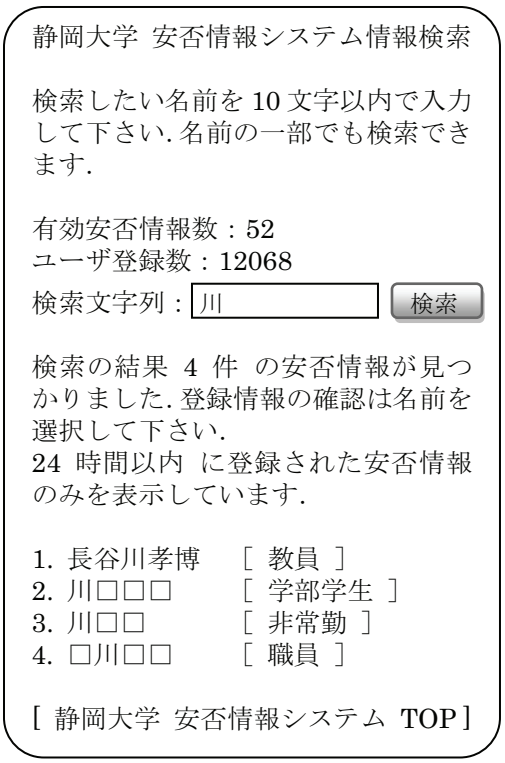

図 4 氏名の一部「川」で検索した場合の安否情報検索画面のイメージ図

実装されることが望ましい．なぜなら，管理者のネットワーク環境がその時点で利用できるか定かではないし，管理者の都合にシステム運用が依存することも極力避けるべきである．そこで，本システムでは，気象庁が速報する地震 RSS 情報を一定時間間隔で監視し，当該およびその周辺地域に大きな震度の地震発生が発表された際には，全登録者に対して安否情報の入力を促すメールを自動通知する仕組を実装した．同様に，数ヶ月に 1 度の定期訓練も自動処理として設定している．

6) その他の WEB データベースセキュリティ

パスワードはハッシュ関数による暗号化を行った後，データベースに記録される．したがって，パスワード照合は全てハッシュ照合によって行われる．アカウント登録時に入力を求められる学籍番号／教職員番号，氏名，所属，キャンパス名，副メールアドレスの基本情報の変更にはランダムに生成されるセッション ID を hidden 情報として埋め込むセッション管理を実装した．プレースホルダによる SQL インジェクション対策や，投稿される値の安全チェックは変数毎に実施している．サーバ証明書を導入し，SSL 通信を確立する(2009 年 8 月予定)．これらは利用者が安心してサービスを利用するための重要な配慮でもある．

図 4 は氏名の一部「川」で氏名を検索して 4 件の登録がヒットした状態である．全ての氏名はリンクになっており，ひとつの氏名をクリックすると**図 5** のような安否詳細情報が表示される．

3. システムの開発と実装

3.1 システムの開発環境

当安否情報システムは，Linux (CentOS) 上で動作する PostgreSQL 8.1.11 と Perl 5.8.8 の CGI による WEB データベースとして開発した．後述するように，安否情報システムは，単純なデータベース構造の管理と検索で成立するシステムであるため，1〜2 万人程度の利用者であれば，それほどハイスペックなサーバは必要としない．システムディスクや電源の二重化など可用性を高くすることがより重要である．可用性を確保する手段として，クラウドコンピューティングによる運用も十分考えられる．

3.2 データベース構造と Perl CGI の単純化

安否情報システムは，個人情報の収集と公開をしかるべきタイミングで迅速に行うデリケートなシステムであることは間違いない．それゆえに，非常時

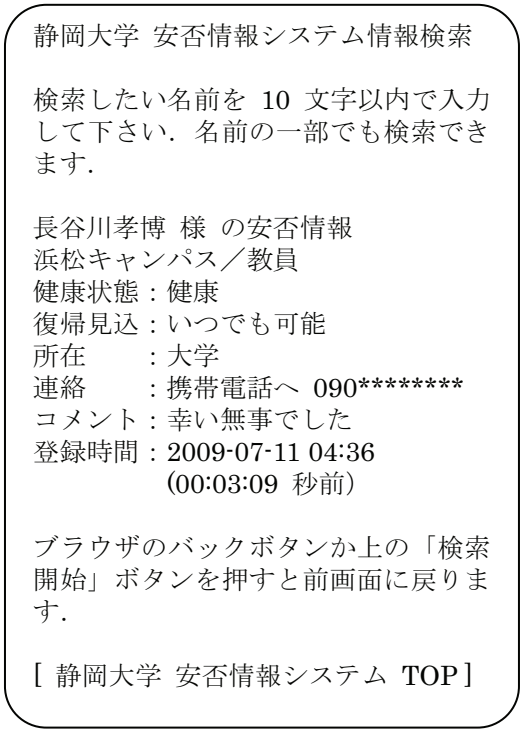

図 5 安否情報の表示画面のイメージ図

に収集すべき個人情報は，健康状態や職場への復帰見込みなど，必要最低限の情報に限られるため，データベースのテーブル構造はそれほど複雑にならない．

RDB(Relational Database)では，その高機能性が故か，例えば部局名，学科名，役職名，健康状態のような限られた個数の定数値しか持たない項目まで，テーブルに細分してしまうケースを見掛ける．または，著者自身がそのような経験を経て，その非効率さに気付き，解決策を見出してきたところがあるので，そのことについて紹介したい．

まず，レコード(項目)数の少ないテーブルを細分してしまうことの短所は，CGI 中の SQL 文を不必要に煩雑にしてしまうことである．項目数の追加，削除，挿入，更新の作業にも注意や手間を要する．これらの変更までを CGI で提供するという手もあるが，その開発コストは少なくない．

当安否情報システムでは，管理者が非常時にデータ投入する組織構成員の名簿テーブル(平常時は空)を除けば，データベース上のテーブルは 1 つしかなく，項目数の少ない定数値は，Perl のハッシュ変数を用いてシステムの定義ファイルで簡単に定義している．健康状態を表わすハッシュ変数で例を示す．

```
%health=(
"GOOD"=>'1. 健康',
"INJR"=>'2. 軽傷',
"SERI"=>'3. 重傷',
"OTHE"=>'4. その他');
```

このようなハッシュ変数を定義し，

```
@keys =
sort{ $health{$a} cmp $health{$b}} keys %health;
foreach $key (@keys){
$work1.="<input type=¥"radio¥" name=¥"health¥"
value=¥"$key¥">$health{$key}$br¥n";
}
```

でラジオボタンの HTML を生成する．このとき，値冒頭の数字でソートしてその出力順番を決定している．また， データベースには「健康」,「継承」のような値ではなく「GOOD」,「INJR」のようなハッシュ変数のキーを記録する．これによって，例えば，%health の冒頭に

```
"DETH"=>'5. 死亡',
```

を挿入するだけで 5 番目の選択項目が追加され，運用中のデータベースにも大きな影響を与えることはない．

また，CGI の開発および管理コストを抑えるために次のような設計を行った．前述のプログラムで，$br 変数は携帯端末からのアクセスを判断した際にのみ
タグとなり，携帯端末画面上の見栄えを調整する．携帯端末用にはパソコンで表示されるものとほぼ同意の短いメッセージを表示するように分岐で処理を行い，これらを異なる CGI に分離して二重の管理が必要となる設計は極力避けた．以上のような単純化の積み重ねの結果，冒頭に述べたような CGI のコンパクト化が可能となり，仕様の追加や変更に対しても見通しがよいものとなった．

4. 運用について

4.1 卒業・修了・離職者との連絡拠点として

当安否情報システムは統合認証システムとは連携せず，またサービス開始時やその後の平常時において名簿情報をサーバに蓄積しておく必要はない．代わりに，現時点では，大学ドメイン名を持つメールアドレスを主キーとして，オプトイン方式の登録を経なければアカウント登録できない仕組としている．そのため，卒業，退職，離職等により正規の組織構成員ではなくなっても自主的なアカウント削除を行わない限り，安否情報システムにアカウントを残してしまうことになる．しかし，他の重要システムやデータとの連携がないため，サーバ性能が許容する限りこのことは大きな問題にはならない，むしろ組織を去った者も有効に活用してもらえるようなサービスであることが望ましいと考えている．ただし，組織外構成員の失効したメールアドレスへの不達となる無駄を最小限に抑える仕組は実装しなければならない．例えば，「卒業・修了・離職」等の所属を設けて，これを所属として選択した利用者には，副メールアドレスへのみ送信するように調整することは容易である．このとき，主メールアドレスは，入学年の西暦下 2 桁を含むので永年活用におけるユニーク性を維持するために,主メールアドレスを廃止し，副メールアドレスとの交換を行うとよいであろう．

セキュリティ上のリスクを許容できるか，リスクアセスメントを実施して慎重に判断する必要はあるが，これをクリアできれば，当システムを，元組織関係者との連絡拠点として展開して行くこともできる．ただし，現時点では，立ち上げ初期のため，まだ構想のみの段階である．

4.2 名簿情報との照合

正規構成員の名簿情報などと連動しない当システムは，安否情報を登録する構成員やインターネット上の一般利用者を含む，いわゆるエンドユーザレベルの利用には十分に機能する．しかし，非常時には組織運営に携わる管理者によって正規構成員名簿との突き合わせ作業を行うことができなければならない．これは安否情報システムとして必要かつ重要な機能である．この機能は管理者側で大量の名簿情報などをシステムへ投入しまうことで容易に提供できる．だが，その代償として設置や運用の重たいシステムとなることは避けられない．このような矛盾が安否情報システムの運用におけるひとつの問題点である．

本システムではこの問題を次のように解決した．まず，部局，学科，事務課，共同施設課などの中小組織の責任者（以下，単に「責任者」という）権限を管理者（ここでは防災対策本部などでシステム操作の全権を有する者を意味する）と利用者の間に設けた．各責任者には，自分が緊急時にその安否を確認しなければならない構成員の学籍番号や教職員番号（以下，簡単のために「識別番号」という）の最新情報をリストアップしておくことを義務付ける．緊急時において，責任者はこれらの識別番号リスト（単数とは限らない）を専用 WEB ページから一括投入することで構成員の安否情報を鳥瞰でき，その結果を災害対策本部などの上位組織に報告できる．この機能を活用するために，責任者は管理配下の構成員に対して識別番号の入力徹底を図る必要が出てくる．これはデータの完全性を分散努力で担保していることに他ならない．一方，管理者側でも，例えば，独自に全ての中小組織単位の識別番号を準備または責任者らから収集しておくことができれば，これらを利用して全組織構成員の安否情報を掌握することもできる．すなわち，この方法は，1)安否情報確認のためのタスクを責任と権限のある中間組織責任者にも分散させることで，組織末端にある最新の構成員情報を漏れなく迅速に反映できる，2)情報収集手段の多様化や連絡網の強化を図ることができる，3)利用者自身が登録した情報のグルーピングを識別番号で指示するのみであり，管理者側で追加の個人情報を大量投入する必要がない，などの点で優れている．

5. 今後の展望とまとめ

統合認証システムとの連携や名簿情報等の個人情報の大量初期投入を一切行わずにサービスを始動できる安否情報システムを開発した．これらの特徴は，サーバのクラウドコンピューティング化や遠隔地設置を容易なものとし，低リスクで可用性の高いサービスを実現できた．管理者は，認証コード付き URL を利用者毎に送信し，これを受けた利用者は文字入力を一切行うことなく，簡易認証を完了できる．最小限の安否情報はボタン操作のみでパソコンや携帯端末から投稿することができる．これらの仕組によって，非常時における高い情報収集率を期待できる．安否情報は，その最終登録時刻より一定時間はインターネット上で検索可能となるが，設定時刻を経過すると自動的に非公開となる．煩雑な操作を避け，不必要な情報の公開を避ける意志を持たせることで，利用者の利便と安心を獲得できるシステムとした．開発した CGI ソースコードは簡潔であり，仕様の変更や機能の拡張を妨げない．

今後のシステム開発予定として，管理者専用ページでの安否情報の集計機能や閲覧機能の充実，重要な管理機能の一部携帯端末化を考えている．情報インフラが壊滅的な破壊を受ける可能性のある東海地震を想定すれば，管理者が携帯端末からでも必要最低限の管理機能を操作できることが望ましい．例えば，安否情報の入力を促すメールの一斉送信などのトリガーを携帯端末から起動できるようにする．

また，静岡大学情報基盤センターでは，BCP(Business Continuity Plan/事業継続計画)と環

境問題対策の一環として公式ホームページ[4]のクラウドコンピューティングへ移設を試行してきた．同様に，安否情報システムサーバの遠隔地設置はBCP の観点から一般的に行われている．当安否情報システムも 2009 年 7 月に商用クラウドサービスへの移転を完了した．結果として，近隣の情報インフラ事情に影響を受けることのないサーバの国外設置を安価に実現できた．

謝辞：安否情報システムの開発にあたりご協力を賜りました静岡県立大学の湯瀬裕昭氏に心より厚く御礼申し上げます．

[1] UPKI イニシアティブ：https://upki-portal.nii.ac.jp/

[2] 林能成，梶田将司，太田芳博，若松進，木村玲欧，飛田潤，鈴木康弘，間瀬健二「組織特性を考慮した大学向け災害時安否確認システムの開発」安全問題研究論文集 Vol.3, pp.203-208(2008)

[3] 越後博之，湯瀬裕昭，干川剛史，沢野伸浩，高畑一夫「大規模分散環境におけるロバストネスを考慮した広域災害情報共有システム」情報処理学会論文誌， Vol.48, No.7, pp.2340-2350(2008)

[4] 静岡大学情報基盤センター
http://www.ipc.shizuoka.ac.jp/