5D-3

通信混雑下でのモバイルサービスアプリケーションの考察

○門脇　保　永澤　弘樹　鈴木　健一　郷　健一
渡辺　俊勝　小梨　貴史　成田　陽広
ＮＥＣソフトウェア東北(株)

１．はじめに

２０１１年の東日本大震災では通信情報量に関して、東北では通常の約６０倍に増加し、呼接続要求が約４～５倍の通信要求が発生していた。このため通信をはじめとする通信サービスに大きな影響を与えた。このような状況下でも確実な通信伝達を行うために、通信関係各社においては処理能力を増強する仕組みを研究している。また、今回の震災では、災害時に発生した火災や津波に対して避難を行う際、身の安全を確保するため、最小限のものしか持ち出すことが出来なかった。所持品の中でも連絡先情報などを記載した紙や手帳、モバイル端末がなくなるなどしていた。

このように重要な個人データや連絡先情報などをモバイル端末や紙媒体として置いておくことにリスクと考え、離れたサーバ上へ預けるストレージサービスが検討されてきている。しかし預けているデータによっては災害発生直後に必要なものであり、通信混雑下であってもサーバへアクセス出来なければならない。また、災害発生から時間が経過し落ち着いてきた頃から、行政サービスなどを受けるために本人証明が必要となってきた。

そのためＮＥＣソフトウェア東北(株)では、東日本大震災での体験から得られた知見を踏まえ、ストレージサービスへ着目し災害に必要なデータへのアクセスが出来、安心安全なセキュリティを可能な限り維持する方法について研究を進めてきた。

２．今後求められるデータ退避とサービス技術

２０１１年３月１１日に発生した東日本大震災では、東北地方を中心に激しい揺れに襲われた。更に沿岸部では最大で約１０ｍを超える津波が襲来し、大惨事となった。こうした時に被災者は避難所へ避難することになるが、停電、断水、ガス停止によるライフラインが寸断された中で、身内や親類などと連絡をとる手段も情報先も失い、厳しい環境に晒されることとなった。また避難者は、身の安全を確保した後、まずは身内、親類や知人との連絡をとることを最優先としていた。

しかし今回の場合、モバイル端末内部だけに連絡先情報が存在したり、連絡先を紙に書いて貼っているような家庭が多かったりしたため避難した先で連絡先の情報が手元になく、外部からの知人や親類が避難所をまわり探しあてるまで待つような状況になり、安否確認が遅れる結果となった。また、災害発生後数日たってから、地方自治体での一時金申請の際に身分証明が必要となり、自分の身元を証明するための情報が必要であった。必要な時期は災害発生から数日後であったが、この提示に苦労した。

これらにより、連絡先情報や個人データについて、ストレージサービスが今後更に重要になってくると考えられるが、個人情報を外部へ置くことには抵抗感が発生するため、セキュリティの知見を得ることを研究目的とした。抵抗感を払拭するためには、このサービスは安心安全で、必要な場合に利用できるサービスである必要がある。また、必要なデータによっては災害時であっても利用できなければ、前述の状況で役に立たないことになってしまう。

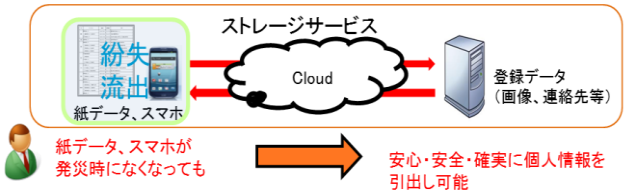


図１．求められるストレージサービス

３．大規模災害時の通信時の問題

東日本大震災では、通信インフラも被災し、通信回線自体も十分な帯域容量ではなかった。そのため携帯電話事業者側では、通信インフラの再構築として、様々な取り組みが検討されている。これらの技術が実用化されれば、通信回線に対してのネットワークの輻輳による混雑は緩和されることになるが、今後の実用化が急が

Effort to solve the congestion problem of the application in the mobile communications service
Tamotsu Kadowaki　Hiroki Nagasawa　Kenichi Suzuki
Kenichi Go　Toshikazu Watanabe　Takashi Konashi
Akihiro Narita

れる段階でありサービスを継続するためには、サービスアプリケーションでも様々な技術が必要と考える。そこで、本研究では、ストレージサービスでの登録されるデータの重要度に合わせた、セキュリティレベルを設定し、通信インフラの状況に応じた認証を行うことで、通信インフラへの負担を軽減する。

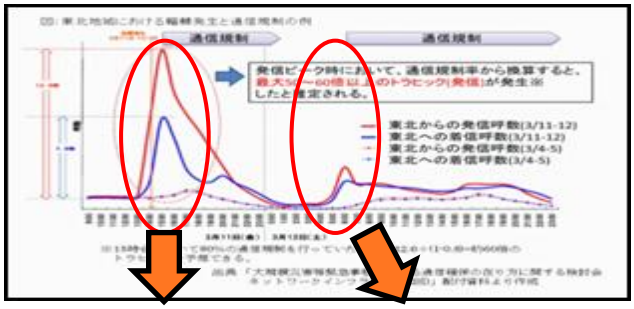
4．サービスとマルチレベルセキュリティ

ストレージサービスでの登録データについては、その内容によって重要度が異なる。扱うデータの内容によっては、パスワードのような簡単な照合で済むものから、高度な認証を要するものなど様々なものが考えられる。そのため本研究で設定したセキュリティレベルを「高・中・低」３段階に設定した。（表１）そして扱うデータにアクセスするためには、それぞれのレベルに　応じた認証方式を設定する方式とした。

これは、災害発生時から時間が経過するごとに必要なデータは変化しており、通信の状況に応じて必要なデータをアクセスで出来なければならない事に注目した。（図２）

表１．扱うデータ種別ごとの重要度

扱うデータ(例)	情報の重要度	認証方式		
		通常時	動的認証方式変更	災害時
機密事項 身元保証など可能なデータ	高	画像比較認証 （クラウド認証）	セキュリティと 変更なし	画像比較認証 （クラウド認証）
家族や友人の共有情報 連絡帳、行動予定	中	画像選択認証 （クラウド利用）	⇒ ネットワーク負荷軽減	画像選択認証 （端末内認証）
端末内のメモ、画像	低	パスワード認証 （端末内認証）	変更なし	パスワード認証 （端末内認証）



直後は、家族や友人との連絡が重要　　経過後は、本人確認や身分証明などが必要

図２．災害発生後からの通信量と必要データ

重要度「高」のデータについては、個人情報としてもセキュリティ上重要であり、通信状況に関わらず認証レベルを変更することなく扱うことにした。結果として通信混雑下ではデータアクセス出来ない場合もあるが、利用シーンが想定される通信状況が改善されてからは問題なくアクセス出来ることを確認した。

このような重要データに関して本当に必要とされる時期は、前述のように発災から数日たった後と想定した場合、個人データを守りその後にデータアクセスすることについて確認をした。

重要度「中」のデータについては災害時にセキュリティレベルを落としてもデータアクセスを優先にするものと想定し、災害時と判断した際にセキュリティレベルを簡易型の認証に動的に置き換えることで、サービスを維持する仕組みが出来ないかを検討した。結果として、通信混雑下では通常型の認証を通じてデータアクセス出来ない場合が発生したが、簡易型の認証に変更することで認証成功率が向上し、データへのアクセスが改善される結果となった。

これらは、ネットワークに大きな通信混雑状態にある時にも応用できるが、発展途上国などインフラの一つとして通信環境が十分でない地域でも、アクセスする認証技術の適用が可能になると考える。そしてこれらが災害に役立つ耐災害サービスアプリケーション内の技術の一つとして検討されていくものと考える。

5．おわりに

災害時に必要となるこれらのサービスについて機能実装を行い、検討した結果、ネットワーク混雑化を模した環境においても、認証を通じたサービス維持が可能となり、認証成功率も向上する結果を得ている。このセキュリティレベルの変更に伴い、サーバとのデータ通信量についても削減される効果も確認できており、混雑化ではネットワーク側にもやさしく、かつ安全安心なサービスとしての結果を得ることが出来た。現在、端末側とクラウド環境によるデータ保持と同期処理を持つサービスがより増加する中で、いかに安全安心なサービスを提供できるかが重要になってくると考える。

参考文献

[1]資料「東日本大震災時の通信状態」：総務省，平成 23 年 8 月

[2]資料「東北地方太平洋沖地震を教訓とした地震・津波対策に関する専門調査会報告」：内閣府，平成 23 年 9 月