

「自治体クラウドにおける住民サービス向上のためのアクセス・ 認証方式等に関する調査研究」報告書

概要版

平成24年3月

エヌ・ティ・ティ・コミュニケーションズ株式会社

調査研究の目的と概要

調査研究の目的

自治体クラウドの地方自治体(以下「自治体」という。)業務への適用により、以下の点が期待されている。

○大幅な行政コスト削減

○業務の標準化

○ICTを効果的に利活用することによる住民サービスの質の向上

しかし、自治体クラウド導入のためには、住民及び自治体職員が安心・安全にクラウドサービスを利用するために必要となるセキュリティの課題等について取組んでいく必要がある。

本調査研究は、自治体クラウド推進本部及び自治体の行政改革モデル検証におけるこれまでの検討結果を踏まえた上で、自治体クラウド導入の課題の一つである、クラウドサービス間での相互運用性の確保に向けた、住民及び自治体職員が安心・安全にクラウドサービスを利用するために必要となるセキュリティの課題等に関する調査研究を行うものである。

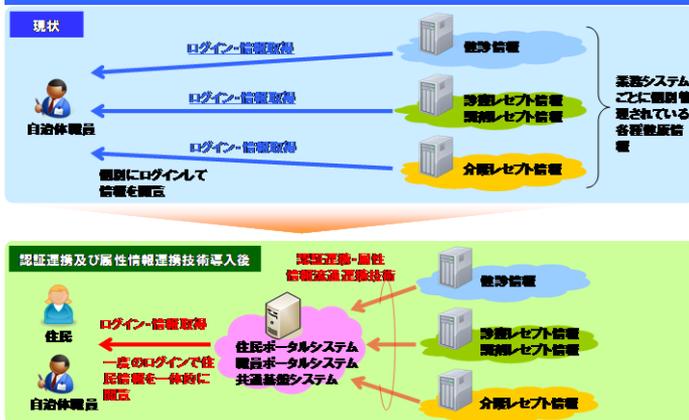
調査研究の概要

クラウドサービス間での相互運用、地域住民及び自治体職員のクラウドサービス利用について具体的なユースケースを想定し、クラウドサービス間での相互運用性やセキュリティ、ユーザビリティなどの調査研究を行った。

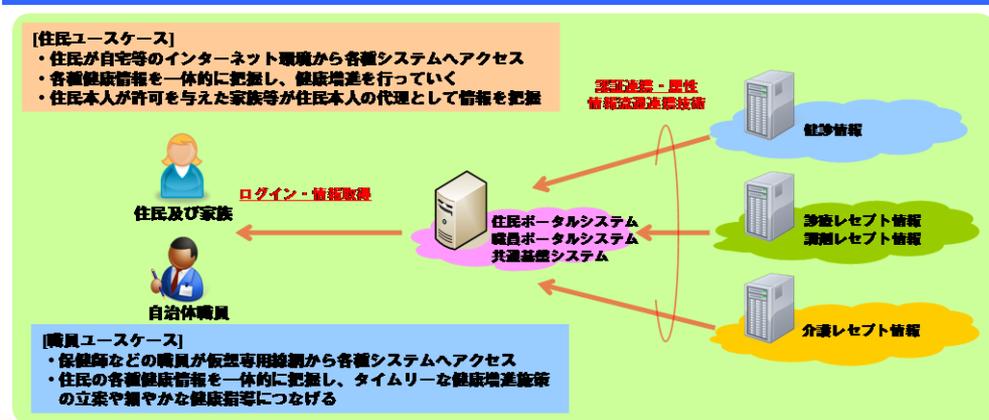
クラウドサービス間での相互運用については、認証連携及び属性情報流通連携の仕組み(以下「共通基盤機能システム」という。)を用いて、これまで自治体の業務システムごとに個別管理されていた各種健康情報を効果的に連携させ、個人に紐づく情報を、住民及び自治体職員へ網羅的・一体的に情報提供するシステムを用意した。

地域住民及び職員がクラウドサービスを利用するケース(住民ユースケース及び職員ユースケース)については、それぞれの具体的な利用の仕方を想定した。

クラウドサービス間相互運用のイメージ



住民ユースケースと職員ユースケースのイメージ



調査研究に対する取組

調査研究に対する取組

○本調査研究フィールド

本調査研究フィールドについては、以下の自治体で実施した。

- ・北海道虻田郡喜茂別町
- ・北海道虻田郡京極町

○データ種別

本調査研究で利用するデータについては、**上記自治体住民から本調査研究への参加モニターを募集し、各種健康情報の提供に関して、同意の上でモニター本人の実データを利用した。**

実データの利用については、**健診情報(過去4年分)、診療レセプト情報及び調剤レセプト情報(過去5件分)を対象とした。**なお、**介護レセプト情報についてはサンプル情報を登録した。**

また、**社会保険加入者及び健診未受診、医療機関にかかっていない国民健康保険加入者については、サンプル情報を登録した。**

○講習会

住民及び自治体職員のユーザビリティに係る調査を行う上で、**住民が実際に自身の各種健康情報を閲覧できる機会を用意した。**

講習会では、**システムの操作説明及び操作サポートに加え、医師・保健師などの専門職による簡単な健康・医療・介護に関するレクチャーも組み合わせ、住民が自らの健康情報を一体的に把握し、より具体的に日々の生活習慣に気づきを与え、健康増進に寄与できるよう考慮した。**

モニター数と登録データ件数について

自治体名 及びモニター数	情報名	データ登録件数
喜茂別町 モニター数:10名	健診情報	8件
	診療レセプト情報	24件
	調剤レセプト情報	7件
京極町 モニター数:37名	健診情報	90件
	診療レセプト情報	113件
	調剤レセプト情報	87件

住民向け講習会風景



ポータルシステムが提供する機能

ポータルシステムが提供する機能

- 住民、自治体職員が本調査研究システムへアクセスするにあたり、住民及び職員ポータルシステムにて、**各クラウドで分散管理されている各種健康情報を一体的に閲覧できるシステムを構築した。**
- 住民の各種健康情報の詳細を参照することで、経年的に自身及び住民の数値の推移を把握することができ、**健康管理、健康指導に役立てることが可能となった。**
- また、各自治体全体における健診結果の傾向を表示することで、**自治体の疾病に関する全体的な傾向を把握できるようにした。**
- なお、認証については、住民向けには**パスワード認証及びマトリクス認証**を実装し、職員向けには**パスワード認証**を実現した。

ポータルシステムのイメージ

パスワード認証

平成24年2月13日

ID/パスワード認証

ログインID
パスワード

ログイン | キャンセル

+

マトリクス認証

※住民向けにのみ実装

平成24年2月13日

マトリクス認証

ログインID user123
マトリクスコード

④,A ①,E ②,B ⑤,D

ログイン | キャンセル

認証後

ポータルトップ画面

各種健康情報を一体的に表示

ようこそ 住民さん 平成24年2月13日

健診情報 / レセプト情報

情報種別	検査項目	検査種別	介護-セプト	検査種別	介護-セプト
受診年月日	平成23年04月10日	受診年月日	平成23年04月10日	受診年月日	平成23年04月10日
受診内容	43歳	検査項目	脂質代謝(コレステロール)	検査項目	脂質代謝(コレステロール)
検査結果	272.5mg/dl	検査項目	血糖(セプテック)	検査項目	血糖(セプテック)
体重	74.6kg	検査項目	尿酸値	検査項目	尿酸値
BMI	25.4	検査項目	血圧(静脈)	検査項目	血圧(静脈)

傾向分析 / お知らせ

実施年度	実施日	実施場所
平成23年04月30日	香取総合市民会館	
平成23年02月14日	香取総合市民会館	
平成23年02月14日	総合市民会館	

傾向分析表示

自治体全体の傾向を表示



健診情報参照画面

健診情報の推移を表示

平成24年2月13日

各種レセプト情報一覧

各種レセプト情報の推移を表示

各種レセプト情報一覧

平成24年2月13日

診療情報 / レセプト情報 / 一覧

情報種別	検査項目	検査種別	介護-セプト	検査種別	介護-セプト
受診年月日	平成23年04月10日	受診年月日	平成23年04月10日	受診年月日	平成23年04月10日
受診内容	43歳	検査項目	脂質代謝(コレステロール)	検査項目	脂質代謝(コレステロール)
検査結果	272.5mg/dl	検査項目	血糖(セプテック)	検査項目	血糖(セプテック)
体重	74.6kg	検査項目	尿酸値	検査項目	尿酸値
BMI	25.4	検査項目	血圧(静脈)	検査項目	血圧(静脈)

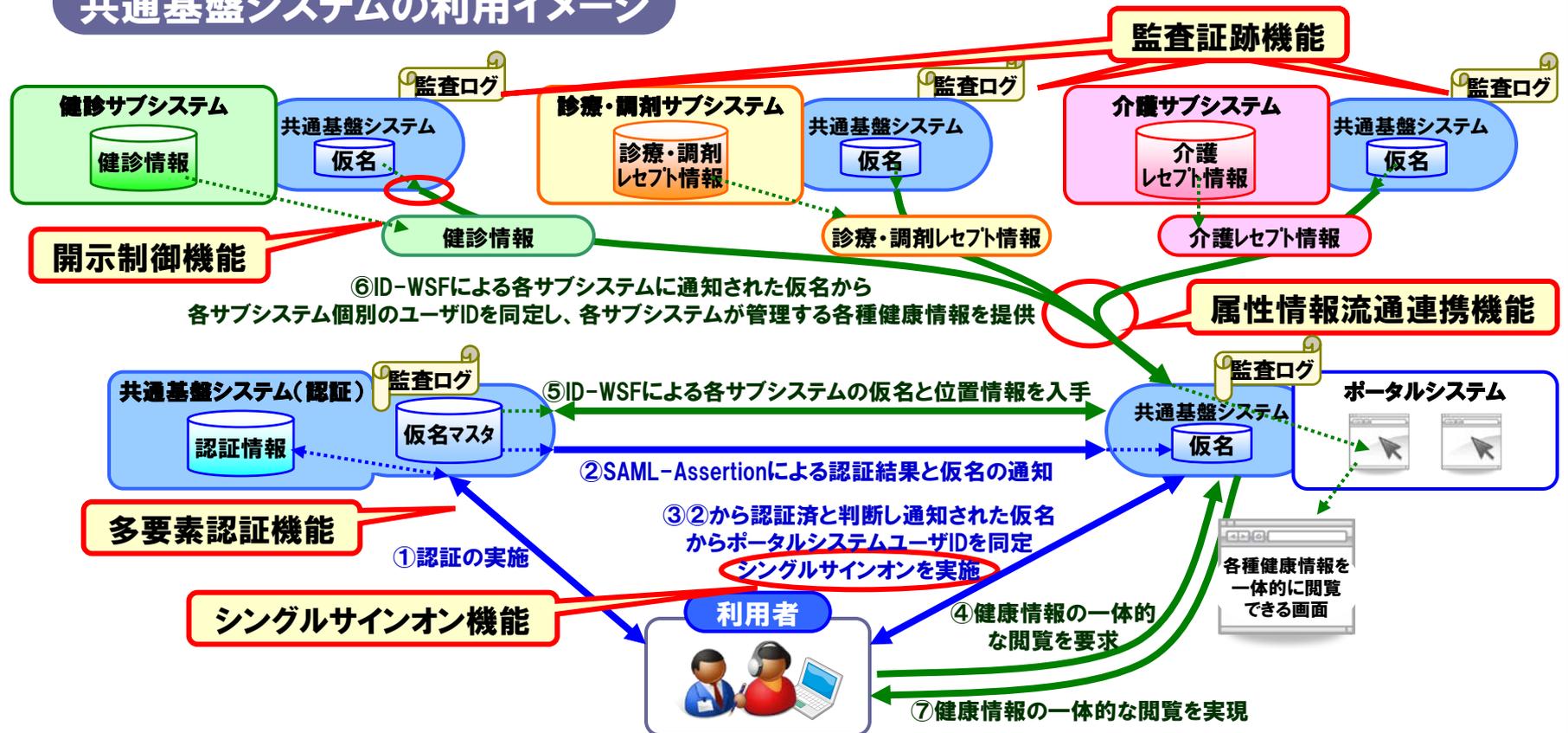
共通基盤システムが提供する機能

共通基盤システムの機能概要

共通基盤システムが提供する主な機能は、以下の通りである。

- シングルサインオン機能** : SAML2.0仕様に基づき、SAML-Assertion(認証結果と利用者の仮名)を通知することで、一度認証を行えば、共通基盤システム全体で認証済であるとみなし、認証の一元化とサービス利便性向上を実現する機能
- 属性情報流通連携機能** : ID-WSF2.0仕様に基づき、SAML-Assertionを用いてユーザの同定し、情報の安心安全な流通を実現する機能
- 多要素認証機能** : 利用者の属性(住民、自治体職員等)等に応じて適切な認証レベルに基づく認証を実現する機能
- 開示制御機能** : 利用者が本人以外の情報を要求する場合に、住民本人の開示許可に基づき情報開示を制御する機能
- 監査証跡機能** : 保健医療福祉情報システム工業会(JAHIS)で定められている証跡監査のメッセージ規約に則った証跡を出力する機能

共通基盤システムの利用イメージ



システム構成概要

システム構成概要

調査研究を実施するにあたり、下図のシステムを構築した。

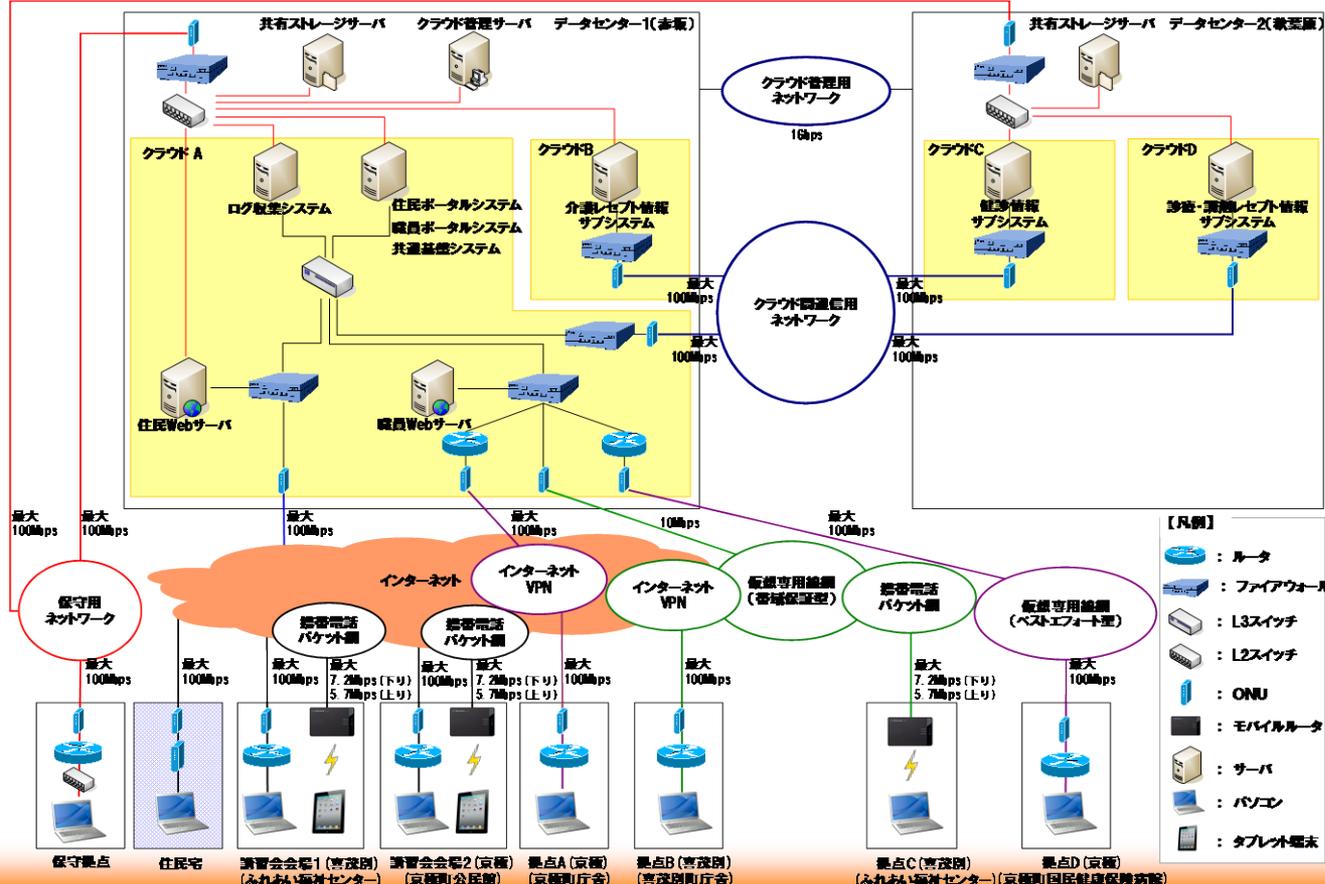
○クラウド環境

- ・クラウドA:住民及び職員ポータルシステム及び共通基盤システム
- ・クラウドB:介護レセプト情報を扱う業務システム
- ・クラウドC:健診情報を扱う業務システム
- ・クラウドD:診療レセプト情報及び調剤レセプト情報を扱う業務システム

○ネットワーク環境

- ・拠点A:インターネットVPN
- ・拠点B:仮想専用線網(帯域保証型) + インターネットVPN
- ・拠点C:仮想専用線網(帯域保証型) + 携帯電話パケット網
- ・拠点D:仮想専用線網(ベストエフォート型)
- ・講習会会場:インターネット回線or携帯電話パケット網

システム構成イメージ



調査研究の全体イメージ

調査研究の全体イメージ

本調査研究環境の全体像は、以下の機能群とユーザの層により構成されている。
本調査研究ではそれぞれの層に関する調査を実施し、それらを複合的に組み合わせてとりまとめを行った。

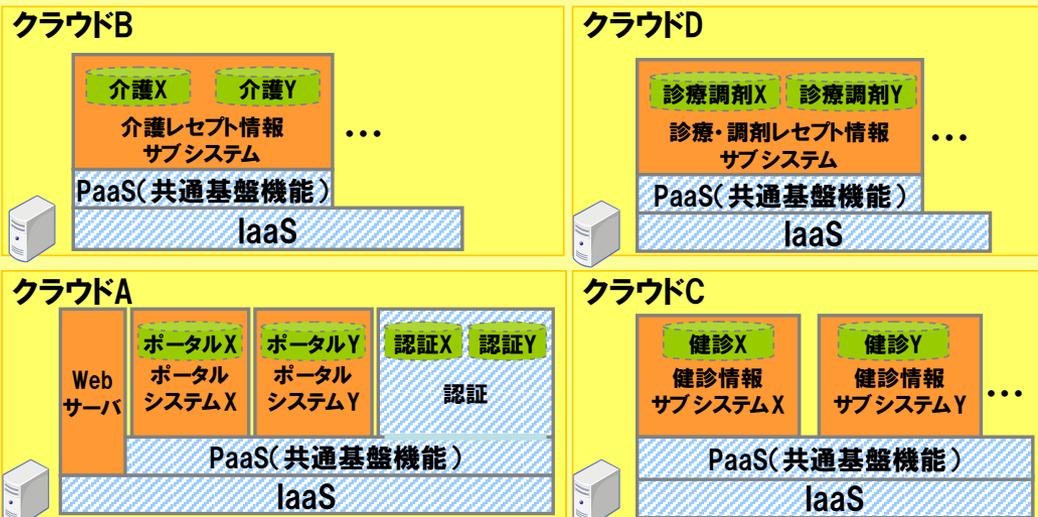
クラウド管理



●クラウドサービスの事業継続性に係る調査

ネットワークをまたいだクラウドシステムとしてのサービス継続に関する調査研究

基盤+アプリケーション



●業務システム間連携の機能に係る調査

●業務システム間のセキュリティに係る調査

業務システムごとに個別管理されている情報を連携させ、一体的に表示させることを可能とする機能及び情報連携時に必要となるセキュリティに関する調査研究

ネットワーク



●ネットワークに係る調査

クラウド拠点と自治体拠点を接続するネットワーク種別の違いに関する調査研究

ユーザ



●住民及び自治体職員のユーザビリティに係る調査

本調査研究システムの利用のしやすさに関する調査研究

●推奨モデルの提示

業務システム間連携の機能に係る調査

調査概要

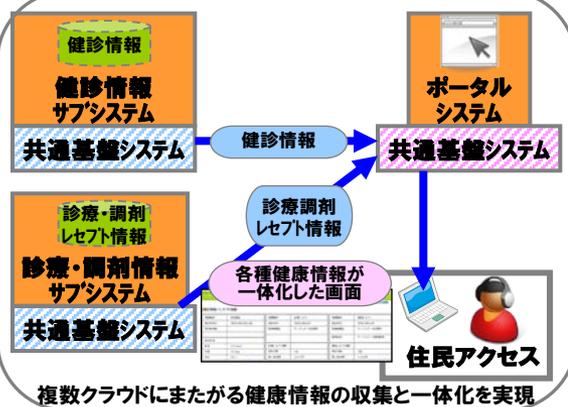
本調査研究システムが複数クラウドにまたがって分割管理された業務システムの間で機微な情報を安心安全に流通させること及び利用者がポータルシステムを介して情報を一体的に閲覧できることを調査した

調査観点

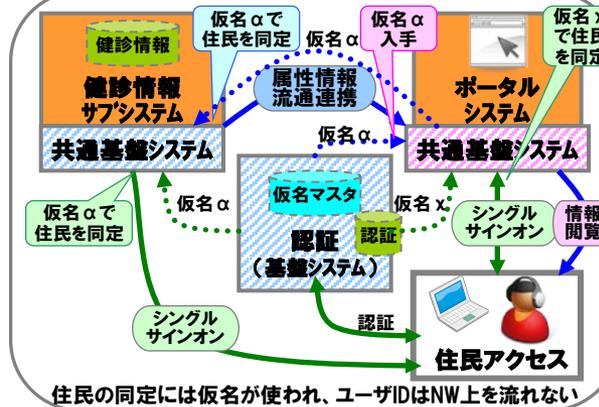
- ①本調査研究システムにより複数クラウドにまたがって分割管理された健康情報が一体的に閲覧できることの調査
- ②仮名等の第三者が名寄せできない方式に基づく、シングルサインオン機能、属性情報流通連携機能の調査
- ③住民本人以外の利用者に対する開示制御についての調査

調査結果

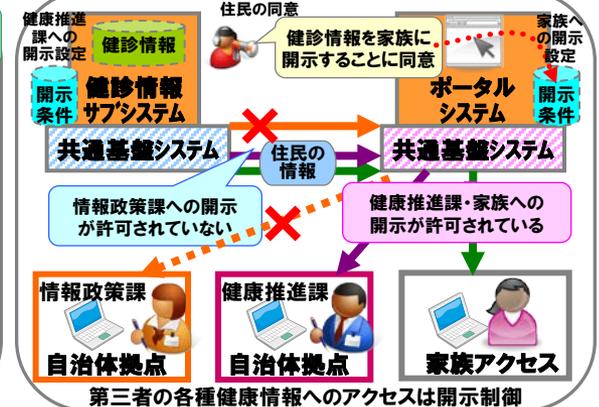
①分割管理された健康情報を一体的に閲覧



②第三者が名寄せできない方式



③本人以外の利用者に対する情報の開示制御



- ①健康情報、診療・調剤レセプト情報が、ポータルシステムを介して一体的に閲覧できていることを確認した。
- ②認証サーバでの認証とポータルシステムを介して各種健康情報の一体的な閲覧を行い、認証が一度しか必要としないことからシングルサインオン機能を、各種健康情報がポータルシステムに集まることから属性情報流通連携機能を、クラウド間の通信記録にユーザーIDが存在しないことから、ネットワーク上では仮名が用いられ第三者が名寄せできない方式であることを、それぞれ確認した。
- ③住民の情報の閲覧が許可されている利用者（家族及び健康推進課職員）は住民の情報が閲覧でき、閲覧が許可されていない利用者（情報政策課職員）は閲覧できないことを確認した。

考察

- 住民、自治体職員共に管理主体毎に分散管理されている情報を**一体的に参照できるポータルシステムは利便性向上の観点で有効であり、共通基盤システムで採用したSAML2.0及びID-WSF2.0の仕様は有効であると評価できる。**
- 共通基盤システムの提供する認証連携機能、開示制御機能、情報流通機能は、ポータルシステム、各サブシステム等の**アプリケーションに対するセキュリティポリシーの統一化、開発工数の低減**を図るために、PaaS機能として整備することが重要であると考えます。
- 共通基盤システムで採用したSAML2.0及びID-WSF2.0は、**ネットワーク上でのユーザIDの秘匿による名寄せ防止や複数の自治体及び民間等の情報の管理主体が異なる場合の利用も可能**であることから、様々なネットワーク形態の複数クラウド間連携に有効である。
- 自治体が保有する各種健康情報をクラウドへ登録する方式は、VPN網によるオンライン方式、媒体配送によるオフライン方式が考えられ、実利用での方式の採用については、**用途、頻度、コスト等により検討をする必要がある。**
- 各種健康情報等を**一体的に表示するための管理主体が異なる情報の本人同定作業**については、データ量が膨大になることから**効率的な実施ができるような仕組みの検討が必要**である。

業務システム間連携のセキュリティに係る調査

調査概要

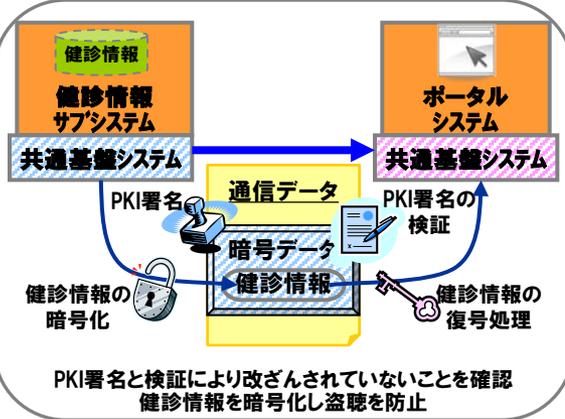
本調査研究システムが複数クラウドにまたがって分割管理された業務システムの間で機微な情報を流通させる上での、考慮すべきセキュリティ項目について調査した

調査観点

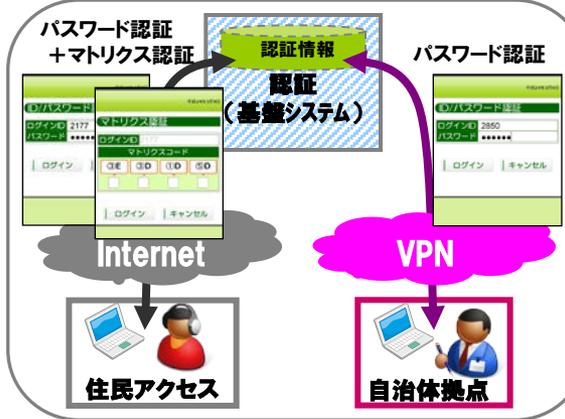
- ① 業務システム間での情報流通における、**情報の盗聴、改ざんを防ぐ仕組み**についての調査
- ② 住民及び自治体職員の認証における、**認証レベルを制御できる仕組み**についての調査
- ③ 本調査研究システムにおける、外部機関による**監査等への対応を想定した証跡記録**についての調査

調査結果

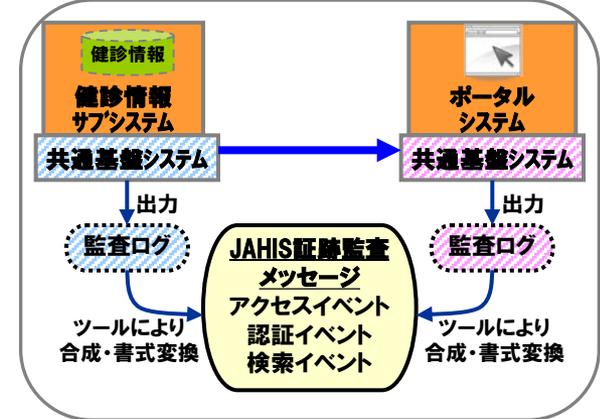
①情報の盗聴、改ざんを防ぐ仕組み



②認証レベルを制御できる仕組み



③監査等への対応を想定した証跡記録



- ① 通信記録から健診情報に対する**暗号化とデジタル署名**が施され、**盗聴防止と改ざん防止の仕組みが備わっていることを確認した。**
- ② 本調査研究システムを利用する際、**住民についてはパスワード認証 + マトリクス認証の多要素認証が求められる、自治体職員についてはパスワード認証**が求められることで、**認証レベル制御の仕組みが備わっていることを確認した。**
- ③ 本調査研究システムを利用することで記録される監査ログ情報が、保健医療福祉情報システム工業会(JAHIS)が取り決めている証跡監査のメッセージ規約に則った形式で記録されていることを確認した。

考察

- 複数クラウド間での連携は、一般的なWebセキュリティ対策はもちろんのこと、ネットワーク上に情報が流通するため情報の盗聴、改ざん防止対策が必要であり、**共通基盤で提供する暗号化、電子署名による真正性の保証機能は有効**であると評価できる。
- 端末、ネットワーク形態等の情報へのアクセス方式の多様化が進んだ場合、情報に対してアクセスする際の認証方式についても、PKI認証、バイオメトリクス認証といった**より認証強度の強い認証方式の採用**を検討する必要がある。
- 自治体クラウドを運用するに当たっては、クラウド上に保存されている情報が適切に活用されていることを監視するために、**監査を実施する必要があり、監査のためのログメッセージの統一化が必要**である。さらに、適正な運用のために自治体の規模によらず、**複数クラウドをまたいだ情報システムとしてのセキュリティ監査を実施できる仕組み**が必要になってくると考えられる。
- 今後、扱う情報種別の増加や普及が進むスマートフォンに代表されるような端末種別の多様化、LTEやWiFiルータを活用したワイヤレスネットワークをはじめとしたアクセスネットワークの多様化に対しては、**PKI等のより認証強度の強い認証方式の採用や端末の情報漏えい対策等の新たな脅威への対策を実施**する必要がある。

ネットワークに係る調査

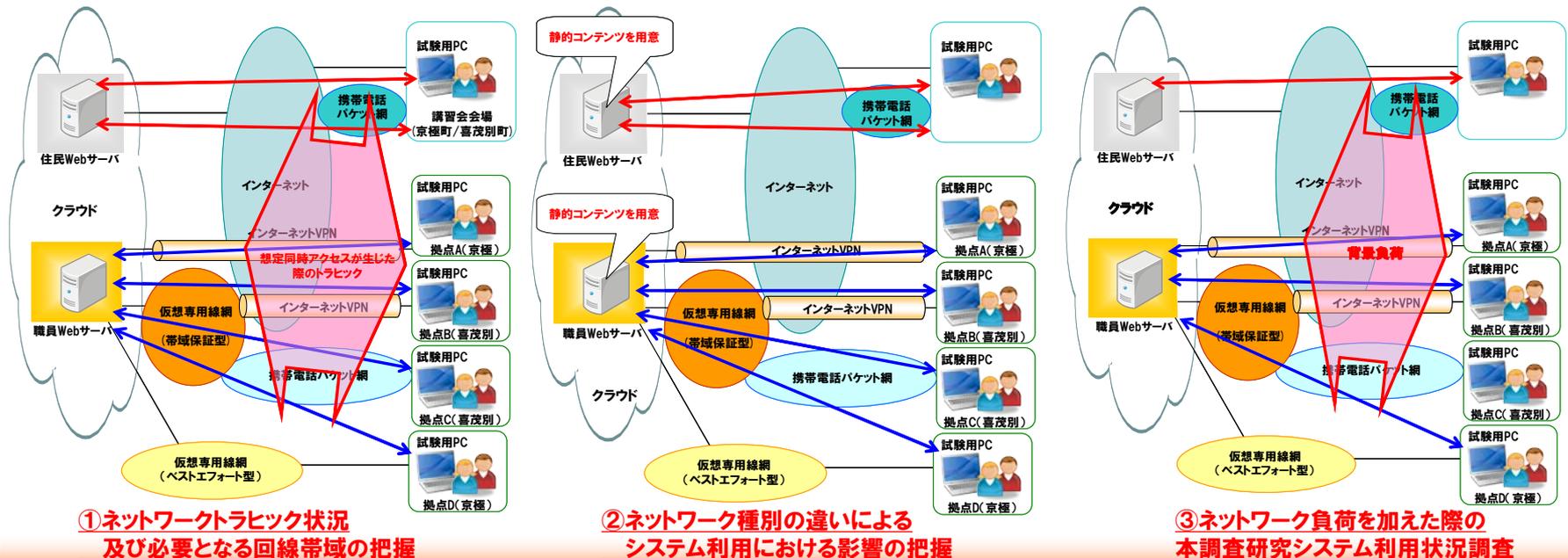
調査概要

自治体拠点から本調査研究システム利用時に必要となる回線帯域やネットワーク種別の違いによる影響を調査した

調査観点と調査方法

- ①: ネットワークトラフィック状況及び必要となる回線帯域の把握 ※1
調査方法: 通常利用時、また行政サービス導入時の同時アクセスを想定し業務影響と必要な回線帯域を把握
- ②: ネットワーク種別の違いによるシステム利用における影響の把握 ※2
調査方法: 各拠点からアクセスした際の画面転送時間の比較を行い回線種別の違いによる業務影響を把握
- ③: ネットワーク負荷を加えた際の本調査研究システム利用状況調査 ※3
調査方法: 回線負荷を増加し、システムの利用状況を確認することで、利用者の最大同時利用ユーザ数を調査

※1 前提条件として、システム利用者が許容できる応答待ち時間の上限は10秒程度であると想定
※2 アプリケーション動作負荷の影響を排除するため、別途配置した静的コンテンツの転送時間を計測
※3 携帯パケット網については、多量な負荷がかかる利用はサービスとして想定されていないため、未実施



ネットワークに係る調査

調査結果

①ネットワークトラフィック状況及び必要となる回線帯域の把握

すべての拠点(ベストエフォート型回線[最大100Mbpsまたは最大7.2Mbps])において、負荷の有無に関わらず、業務への影響は少ない。また、携帯電話パケット網は場所の制約を受けないメリットがあることから、転送時間と業務環境に応じた回線の選択が必要である。

①ネットワークトラフィック状況及び必要となる回線帯域の把握

○本調査研究システム利用者1人あたりのトラフィック結果(負荷なしでのポータルトップ画面転送に要するトラフィック状況)

[上り] 10~40Kbps / [下り] 100~300Kbps程度 (画面転送に伴う回線以外での処理時間も含む)

○回線帯域の把握

本実証実験フィールド規模で想定される同時アクセス数(10名程度)のもと、今回用意した回線で本調査研究システムが利用できるか確認した。

各拠点における平均転送時間(負荷:同時アクセス数10人 ※1)

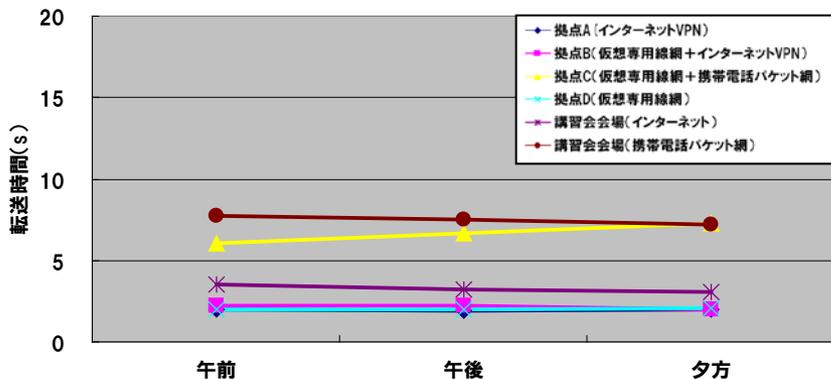
拠点	平均転送時間
拠点A,拠点B,拠点D,講習会会場(インターネット)	2~3秒程度
拠点C,講習会会場(携帯電話パケット網)	7~9秒程度

各拠点における平均転送時間(同時アクセスなし)

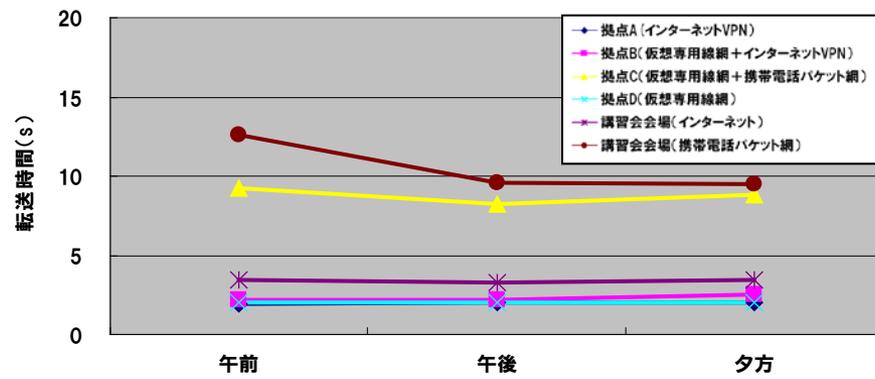
拠点	平均転送時間
拠点A,拠点B,拠点D,講習会会場(インターネット)	2~3秒程度
拠点C,講習会会場(携帯電話パケット網)	7~10秒程度

※1 上記1人あたりのトラフィック結果の10倍のトラフィックのもと計測実施した

負荷の有無に関わらず10秒以下または同等程度であり、各拠点に用意したベストエフォート型回線においても業務への影響は少ない



各拠点における時間帯ごとの転送時間(負荷)



各拠点における時間帯ごとの転送時間(負荷なし)

ネットワークに係る調査

調査結果

②ネットワーク種別の違いによるシステム利用における影響の把握

拠点A (インターネットVPN)・拠点D (仮想専用線網)・講習会会場 (インターネット)は業務への影響が小さいが、
 拠点B (仮想専用線網+インターネットVPN)・拠点C (仮想専用線網+携帯電話パケット網)・講習会会場(携帯電話
 パケット網)は業務への影響が大きい^{※1}ため、利用するシステムのコンテンツ量にあわせた業務の選択が必要である

②ネットワーク種別の違いによるシステム利用における影響の把握

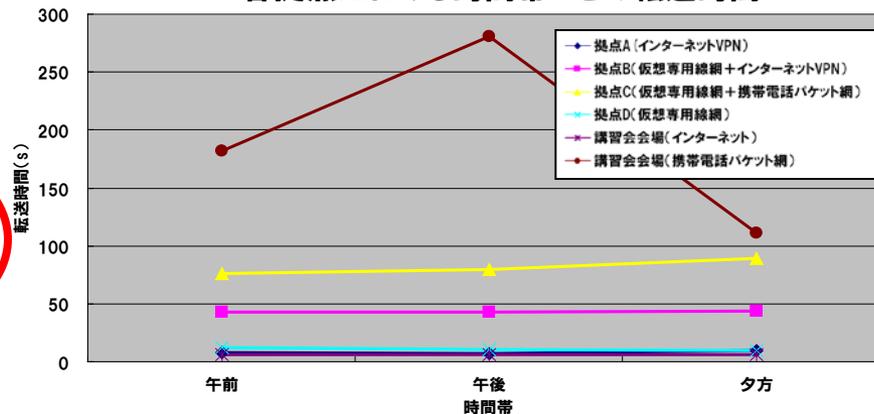
システムによっては画像データを多く利用したコンテンツも用意される可能性があるため、各回線にて10Mbyteの静的コンテンツを閲覧し、それぞれの平均転送時間を計測することで回線種別における差異を確認した。

※1 ポータルトップ画面容量:約70Kbyte程度

各拠点における平均転送時間

拠点	平均転送時間
拠点A, 拠点D, 講習会会場(インターネット)	10秒程度
拠点B	43秒程度
拠点C	82秒程度
講習会会場(携帯電話パケット網)	120~280秒程度

各拠点における時間帯ごとの転送時間



10秒を大きく超える値であり業務への影響が大きい

- 拠点Bはデータセンター側回線帯域が10Mbpsであることによると考えられる
- 拠点Cはデータセンター側回線帯域が10Mbpsであることに加え、拠点側アクセス回線帯域が最大7.2Mbpsであることによると考えられる
- 講習会会場(携帯電話パケット網)は拠点側アクセス回線帯域が最大7.2Mbpsであることに加え、インターネット+携帯電話パケット網というベストエフォート型回線内の混雑状況にも影響を受けたものと考えられる

ネットワークに係る調査

調査結果

③ネットワーク負荷を加えた際の本調査研究システム利用状況調査 ※1

拠点D(仮想専用線網(ベストエフォート型))においては、**最大150名程度の同時利用が可能と考えられる**

※1 業務を行う際は、利用者の業務内容に応じて転送時間に差が生じるため、利用者全ての業務内容を考慮した利用者数の選定が必要

③ネットワーク負荷を加えた際の本調査研究システム利用状況調査

各回線において、どの程度の同時アクセスまで本調査研究システムが利用可能か調査し、各回線の最大同時利用ユーザ数を把握した。※2

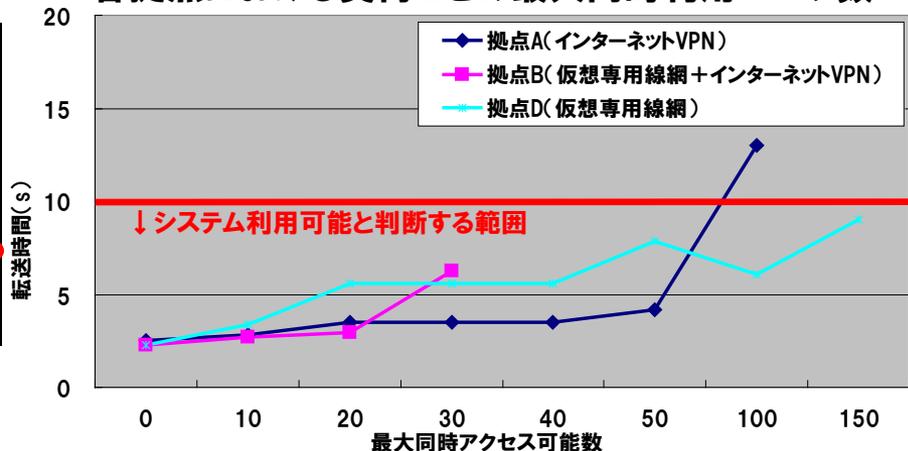
※2 同時アクセストラヒックは調査①で調べた1人あたりトラヒックを整数倍することにより擬似的に発生させた。
また、本調査研究システム利用可能条件は、ポータルトップ画面が10秒以内に表示されることとした。

各拠点における最大同時利用ユーザ数

拠点	最大同時アクセス可能数
拠点A	50アクセス程度
拠点B	30アクセス程度
拠点D	150アクセス程度
講習会会場(インターネット)	計測不可 ※3

※3ネットワーク設備側にて負荷パケットが破棄されている可能性が高いため

各拠点における負荷ごとの最大同時利用ユーザ数



他の拠点よりも100アクセス程度高い値を計測

ネットワークに係る調査

各回線の比較と想定されるユースケース

各調査対象回線について、調査①～調査③の結果とその他特徴をふまえた比較と想定ユースケースを下記に記す。それぞれの回線の性質に応じたユースケースが考えられる。

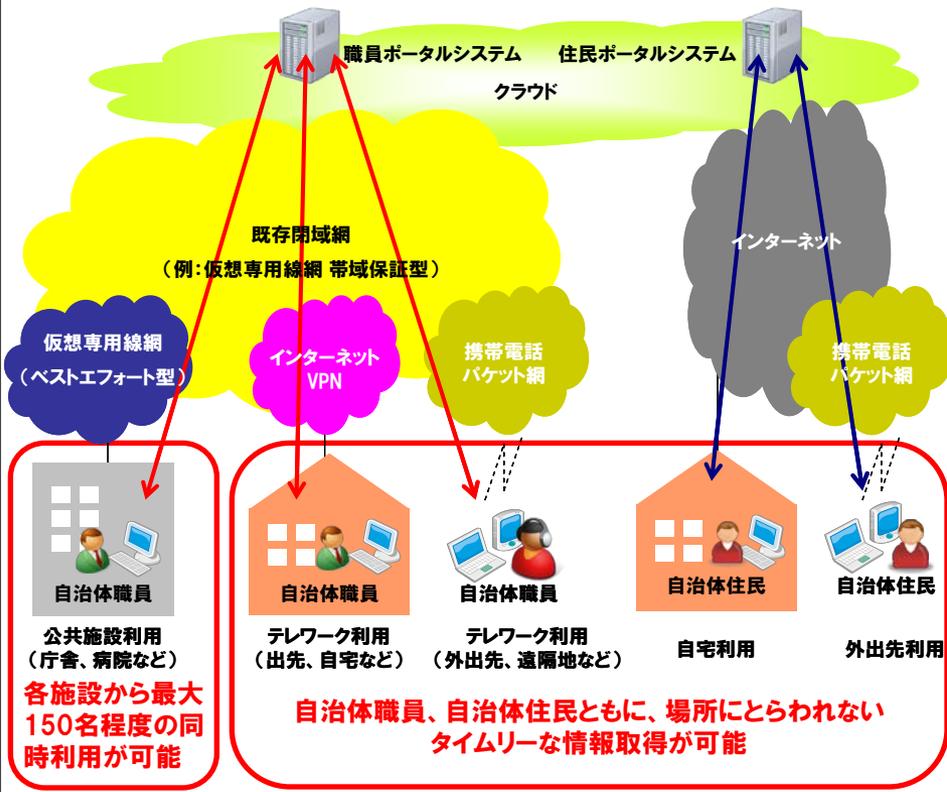
拠点及び回線	想定ユースケース	調査①～③及びその他の特徴を踏まえた調査対象6回線の比較	(参考)月額利用料(両端)
拠点A [インターネットVPN]	テレワーク利用 (在宅型・施設利用型)	<ul style="list-style-type: none"> 平均転送時間は良好、最大同時アクセス数はやや少ない 低コスト 共用網を用いているがIPSecで認証・暗号化実装 	4万円程度
拠点B [仮想専用線網(帯域保証型) +インターネットVPN]	テレワーク利用 (在宅型・施設利用型)	<ul style="list-style-type: none"> 容量の大きいファイル転送は不利、最大同時アクセス数も少ない 高コスト(既存仮想専用線網への追加接続の場合は低コスト) 共用網を利用しているがIPSecによる認証・暗号化実装 	28万円程度 (内25万円は仮想専用線網コスト)
拠点C [仮想専用線網(帯域保証型) +携帯電話パケット網]	テレワーク利用 (モバイル利用)	<ul style="list-style-type: none"> 容量の大きいファイル転送は不利 高コスト(既存仮想専用線網への追加接続の場合は低コスト) 共用網を利用しているがPPPによる認証実装(暗号化は無) 無線利用のため利用場所の制約は少ない 	27万円程度 (内25万円は仮想専用線網コスト)
拠点D [仮想専用線網(ベストエフォート型)]	職場・公共施設利用	<ul style="list-style-type: none"> 平均転送時間、最大同時アクセス数共に良好 低コスト 共用網を利用しているがIPSecによる認証・暗号化実装 	3万円程度
講習会会場 (インターネット)	自宅からの インターネット 利用	<ul style="list-style-type: none"> 平均転送時間は良好 低コスト プライベートネットワーク接続のための認証はないが、SSL(HTTPS)にて暗号化は可能 	2万円程度
講習会会場 (インターネット +携帯電話パケット網)	外出先からの インターネット 利用	<ul style="list-style-type: none"> 容量の大きいファイル転送は不利 低コスト プライベートネットワーク接続のための認証はないが、SSL(HTTPS)にて暗号化は可能 無線利用のため利用場所の制約は少ない 	2万円程度

ネットワークに係る調査

調査結果のまとめ

- 本調査研究システムを利用するにあたっては、**小規模自治体から中核市規模(30万人程度)までは、仮想専用線網(ベストエフォート型:最大100Mbps)を活用したネットワーク構成が適用可能と考えられる**
- 政令指定都市のような大規模な自治体については、**端末利用者数に合わせた専用線網を提供する等、住民数並びに職員の利用規模に合わせた設計を行う必要がある**
- 実際の利用にあたっては**業務内容、回線帯域、品質等を考慮した上で帯域保証型回線も含め適切な回線を選択することが重要である**

調査結果をもとに想定する自治体利用環境



主なユースケースと想定する利用環境

対象者	主なユースケース	想定する利用環境
自治体職員	<ul style="list-style-type: none"> ○各施設から、職員ポータルシステムへアクセスし、住民の各種健康情報を一体的に把握する ○外出先や遠隔地からタイムリーな健康増進施策の立案やきめ細やかな健康指導する※1 	<ul style="list-style-type: none"> ○各施設と共通基盤システム間に仮想専用線網を用いることで、コストを加味し、各種健康情報を把握した業務が可能である ○パソコンやタブレット端末にIPSec対応VPNクライアントソフトウェアを導入することで暗号化のもと、携帯電話パケット網アクセスも可能
住民	<ul style="list-style-type: none"> ○自宅等のインターネット環境を使って住民ポータルシステムへアクセスする 	<ul style="list-style-type: none"> ○インターネット回線や携帯電話パケット網にて自宅や遠隔地から利用可能である

※1 実施にあたっては総務省テレワークセキュリティガイドラインに即した対策が必要

住民及び自治体職員の利用者満足度に関する調査

調査概要

本調査研究に参加した住民及び自治体職員へアンケートやヒアリング等を行い、本調査研究システムのユーザー満足度（利用のしやすさ）や今後に向けた課題についての取り纏め

調査観点

○住民の観点

- ① 自身の各種健康情報を把握する手段として、各種健康情報を取得する容易性についての調査
- ② 本調査研究システムを利用することで、日々の健康増進意識向上に繋がる可能性についての調査
- ③ 本調査研究システムに対して感じた課題についての調査

○自治体職員の観点

- ① 既存業務と比較した本調査研究システムが自治体職員に及ぼす効果についての調査
- ② 本調査研究システムに今後求められる要件や改善要望等の課題についての調査

調査対象

○住民

自治体	アンケート(人)
京極町	33
喜茂別町	8

○職員

自治体	ヒアリング(対象)
京極町	健康推進課、京極町国民健康保険病院
喜茂別町	健康推進課、住民課、総務課

○住民モニター属性

単位:人

	20代	30代	40代	50代	60代	70代	80代
京極町	0	2	6	4	5	15	1

- ・約50%の人が70代以上であり、年代は高齢層である。
- ・パソコンを使ったことがない人が58%であり、ITリテラシーは低い

	20代	30代	40代	50代	60代	70代	80代
喜茂別町	1	6	1	0	0	0	0

- ・全員が40代以下であり、年代は若年層である。
- ・週に5日以上パソコンを使う人が75%であり、ITリテラシーは高い

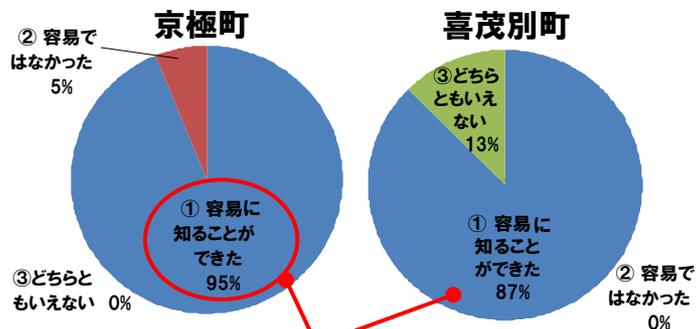
住民及び自治体職員の利用者ビリティに係る調査

まとめ

- 住民ポータルシステムは住民の行動変容に繋がる「**気づき**」を与えるツールとなりえる
- ITリテラシーの低さ、高齢者という属性は、健康への関心が高ければポータルシステムを利用する障害にならない

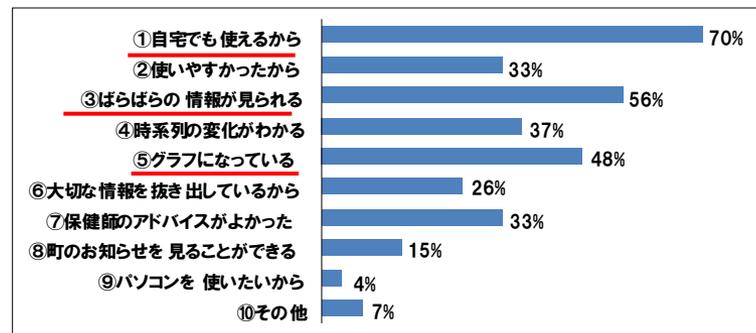
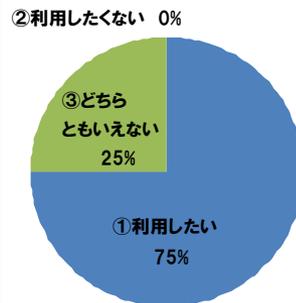
調査結果

【情報を容易に知れたかどうか】全体



高齢者、ITリテラシーに関わらず、本調査研究システムを利用した各種健康情報を取得する容易性を確認

【類似したサービスを利用したいか/理由】高齢者(70代以上)



本調査研究を求めており、今まで紙で管理していた情報が自宅でパソコンを利用して確認できることや、グラフ等わかりやすい表示へのニーズが高い

- 既にお知らせとして広報誌やはがき等で、住民のもとに紙で届いているものもあるが、過去に遡って、ポータルシステムにて**健診情報等が経年的に閲覧できる点、分かりやすくグラフィカルに表示される点、町全体の傾向が確認できる点、あるいは健診情報と各種レセプト情報の両方が一体的に閲覧できる点**が評価された。
- 紙で管理していたばらばらの自身の情報を一体的にポータルシステムにて閲覧できることによって、**住民の生活習慣に対する「気づき」**を与え、日々の生活習慣における行動変容に繋がる**といったことが総合的に評価された。**
- 特にITリテラシーが低い、高齢者といった属性からも**今後もサービスを利用したという高い評価を受けた**ということは、システムの操作サポートやデータ項目の見方などのサポートをすることで、高齢者やITリテラシーが低い住民であっても簡易に自身の各種健康情報を閲覧できたからだと考えられる。

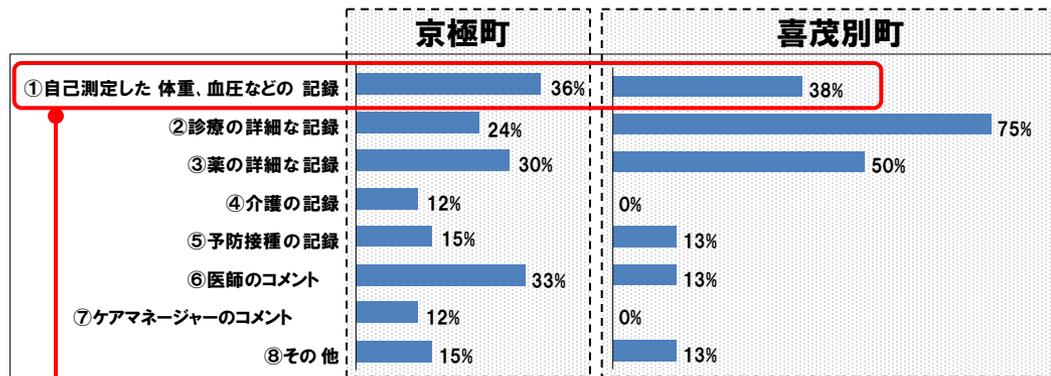
住民及び自治体職員の利用者満足度に関する調査

まとめ

- 情報閲覧型のポータルシステムではなく、**住民が自身の情報を投入できる双方向型のポータルシステムとして機能を具備することで、よりポータルシステムの利用価値を高めていく必要がある**
- ポータルシステムが連携する情報の種類を増やすとともに、自治体が保持している**健診情報等の数値情報のみならず、個人のバイタル情報等の多様な情報を閲覧できるようにすることで、さらなる利便性の向上に繋がる**

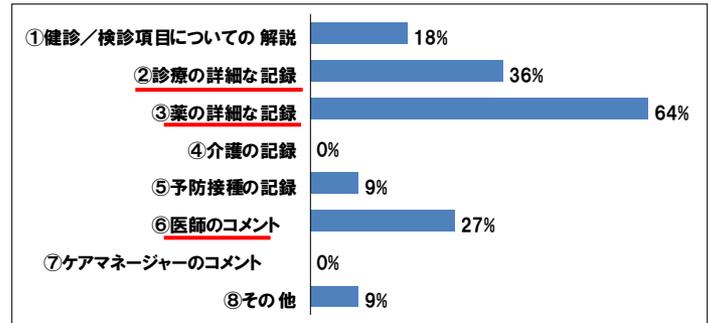
調査結果

【ポータルシステムで欲しい情報】 健診情報、各種レセプト情報以外



自身のバイタル情報を投入できる双方向型のポータルシステムが必要である

【理解度の促進に繋がる情報】 高齢者（70代以上）



自治体が保持する情報に加えて医療機関が保持する情報との連携に対するニーズが高い

- 将来的により住民に即したサービスとしてのレベルをあげるための自治体職員用ツールとなるためには、**健診情報、各種レセプト情報に加えて乳幼児健診情報、妊婦健診情報、予防接種情報などが閲覧できることで更に利便性が向上すると考えられる。**
- 高齢者の属性では、自身が測定したバイタル情報の記録をポータルシステムで閲覧したいというニーズが高いことから分かるように、与えられる情報のみでなく、**住民が自ら測定した自身の情報をポータルシステムに投入できることが必要である。**つまり、将来的にポータルシステムの機能として、**住民、サービス提供者どちらも情報を投入できる双方向機能を備えていく必要がある**と考えられる。
- 住民が計測したデータをシステムに投入することは手間がかかり、住民の負担感があるため、自身のバイタル情報を測定したら**自動的にシステムへ反映されるような機器、インターフェースを整備することが重要だ**といえる。

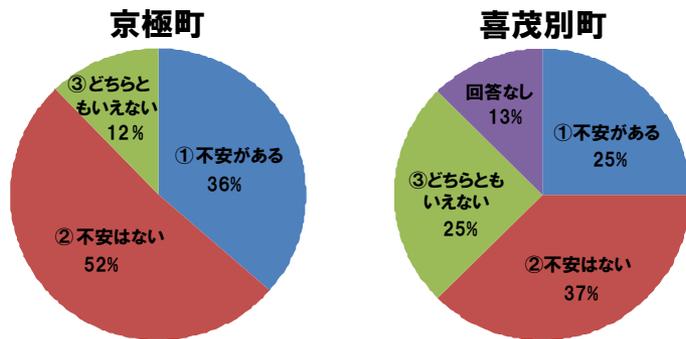
住民及び自治体職員の利用者意識に係る調査

まとめ

- 職員ポータルシステムは、個別に管理されている住民に紐付いた各種健康情報を一体的に表示できることで、**住民を検索すると自治体職員が求めている情報を簡易に確認できる**という点で、住民サービスの向上に繋がる
- 情報の多様化に伴うことで、より強固なセキュリティ施策を実施する必要があり、さらには、**運用者への教育及び住民に対する丁寧なセキュリティに関する説明が必要である**

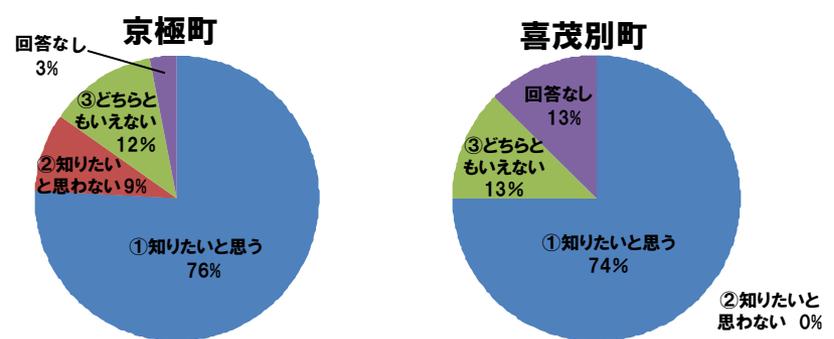
調査結果

【第三者に見られる不安】全体



属性に関わらず、住民は自身の各種健康情報がネットワークを通じて流通することに不安を頂いている

【家族の健康情報を知りたいか】全体



セキュリティに不安はあるものの、家族の各種健康情報を見られることは、属性に関わらず、非常にニーズが高い

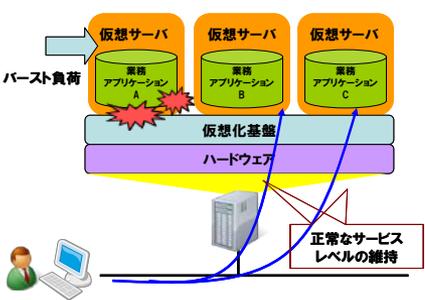
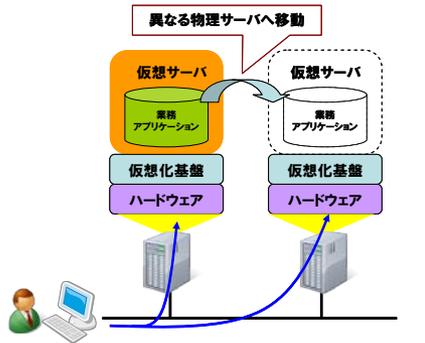
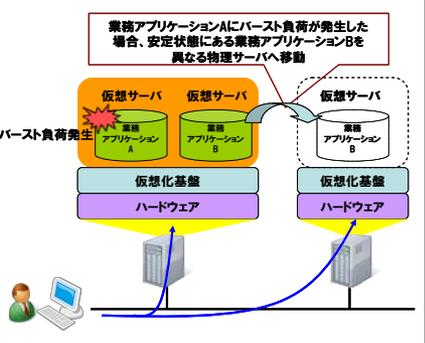
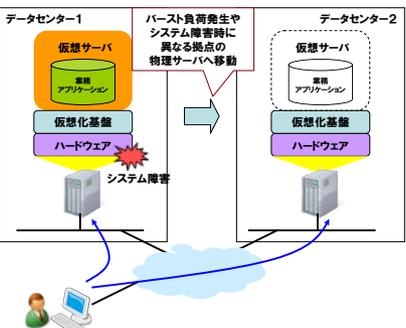
- 目的に応じて、住民に紐付いた健診情報と各種レセプト情報を一体的に閲覧できることは、**業務効率が上がると考えられる**。特に、定量的に評価された数値情報を一体的に確認できることは、然るべきエビデンスに基づいた**住民一人一人に即したきめ細やかなサポートが可能**になると考えられる。
- 今後、自治体職員が庁舎外からアクセスするような用途が制度上許可された場合には、**端末シンクライアント化やICカード等のより強固な認証方式を組み込む等のセキュリティ対策を実施することが必要**となってくる。
- 住民の家族の健康情報を閲覧することに対するニーズが高いことからわかるように、今後、自分以外の数多くの各種健康情報が一体的に閲覧できることになると、**運用者側である職員のセキュリティ教育を実施すると同時に、住民に対して分かりやすく取組を説明することで、住民の不安を払拭し、安心してシステムを利用できるように進めていく必要がある**。

クラウドサービスの事業継続性に係る調査

調査概要

本調査研究システムを用いて、クラウド環境における事業継続に有効な機能について調査を実施した

調査観点と実施方法

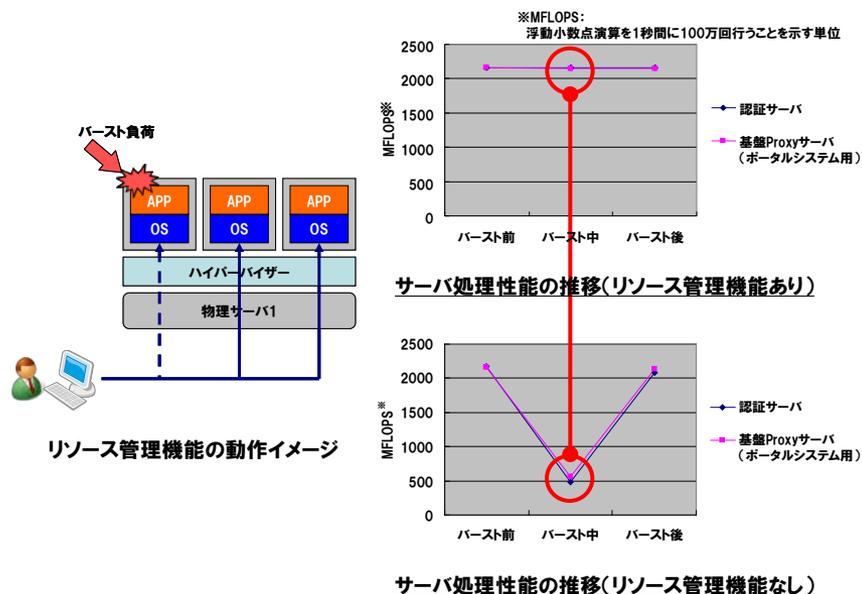
①リソース管理機能の調査	②運用保守を想定した業務アプリケーション移設の調査	③システム障害を想定した動的な業務アプリケーション移設の調査	④災害回避を想定したセンター間での業務アプリケーション移設の調査
<p>リソース管理機能により、特定のサーバリソースで一時的にバースト負荷が発生した場合にも、他のサーバ上で稼動するサービスに影響を与えないことについて調査を実施した。</p>	<p>クラウド環境そのものの運用保守の観点で物理サーバ機器のメンテナンス等を想定し、利用中のサービスを無停止のまま異なる物理サーバへ移動させた際の業務の継続性について調査を実施した。</p>	<p>システム障害として、バースト負荷が発生した場合やハードウェア障害が発生した場合を想定し、物理サーバ間をまたいだ業務アプリケーションの動的な移設を行い、サービスの継続利用が可能か調査を実施した。</p>	<p>クラウドデータセンター間について、専用線網を活用して、業務アプリケーションの移設が可能か、また、その有効性について調査を実施した。</p>
<p><実施イメージ></p>  <p>バースト負荷</p> <p>仮想サーバ</p> <p>業務アプリケーション A</p> <p>業務アプリケーション B</p> <p>業務アプリケーション C</p> <p>仮想化基盤</p> <p>ハードウェア</p> <p>正常なサービスレベルの維持</p>	<p><実施イメージ></p>  <p>異なる物理サーバへ移動</p> <p>仮想サーバ</p> <p>業務アプリケーション</p> <p>仮想化基盤</p> <p>ハードウェア</p>	<p><実施イメージ></p>  <p>業務アプリケーションAにバースト負荷が発生した場合、安定状態にある業務アプリケーションBを異なる物理サーバへ移動</p> <p>バースト負荷発生</p> <p>仮想サーバ</p> <p>業務アプリケーション A</p> <p>業務アプリケーション B</p> <p>仮想化基盤</p> <p>ハードウェア</p>	<p><実施イメージ></p>  <p>データセンター1</p> <p>仮想サーバ</p> <p>業務アプリケーション</p> <p>仮想化基盤</p> <p>ハードウェア</p> <p>システム障害</p> <p>データセンター2</p> <p>仮想サーバ</p> <p>業務アプリケーション</p> <p>仮想化基盤</p> <p>ハードウェア</p> <p>バースト負荷発生やシステム障害時に異なる拠点の物理サーバへ移動</p>

クラウドサービスの事業継続性に係る調査

調査結果

- **リソース管理機能**は、サーバ仮想化環境においては、同一の物理サーバリソース上に複数の仮想サーバが展開されるため、**必須の機能**といえる

①リソース管理機能の調査結果

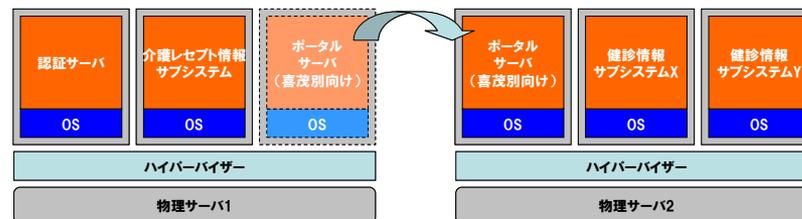


リソース管理機能が有効な場合は、**バースト負荷が発生中**も他の仮想サーバの処理性能に**影響を与えない**が、リソース管理機能が無効な場合は、**影響を与える**ことを確認した。

調査結果

- **ライブマイグレーション機能**は、運用保守を想定した際に利用でき、メンテナンスのためにダウンタイムの計画や、業務を中断することなくハードウェアのメンテナンスを実行することが可能といえる

②運用保守を想定した業務アプリケーション移設の調査結果



ライブマイグレーションの動作イメージ

サーバ	実施回数	失敗回数	失敗率	最短時間	最大時間	平均時間	通信断
ポータルサーバ	289回	1回	0.3%	0ms	364ms	4ms	2s

業務アプリケーション移設時のping応答結果

業務アプリケーションを手動にて、異なる物理サーバへ移動した際のIPLレベルでのネットワーク接続断時間は、**2秒程度**の瞬断であり、**セッションの維持も保たれる**ことが確認できた。

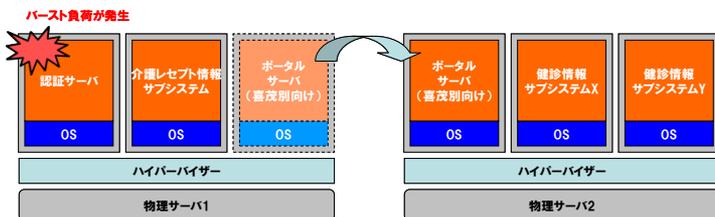
クラウドサービスの事業継続性に係る調査

調査結果

- **動的リソース割当て機能**は、ハードウェアリソースプール全体の使用率を継続的に監視し、使用可能なリソースを仮想マシン全体で動的に割当てる機能であり、**バースト的な負荷が発生した際に、サービスを継続するための有効な仕組みといえる**
- **フェイルオーバー機能**は、**物理サーバに障害が発生した場合、影響を受けた仮想マシンを別の物理サーバ上で再起動する機能であり、ハードウェア障害の復旧手段として有効な仕組みといえる**
但し、セッションは保たれないため、アプリケーションによっては、事前に復旧手順を用意する必要がある

③システム障害を想定した動的な業務アプリケーション移設の調査結果

- 動的リソース割当て機能により、バースト負荷が発生した場合に別の物理サーバに自動移動することが可能



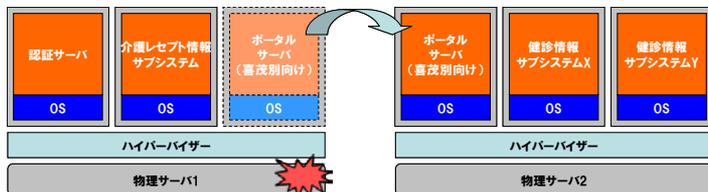
動的リソース割当て機能の動作イメージ

サーバ	実施回数	失敗回数	失敗率	最短時間	最大時間	平均時間	通信断
ポータルサーバ	939回	1回	0.1%	0ms	16ms	0ms	2s

業務アプリケーション移設時のping応答結果

業務アプリケーションを**動的なリソース割当て機能**にて、異なる物理サーバへ移動した際のIPLレベルでのネットワーク接続断時間は、**2秒程度**の瞬断であり、**セッションの維持も保たれる**ことが確認できた。

- フェイルオーバー機能により、物理サーバ障害が発生した場合に別の物理サーバにてサービス復旧が可能



物理サーバ障害が発生

フェイルオーバー機能の動作イメージ

サーバ	実施回数	失敗回数	失敗率	最短時間	最大時間	平均時間	通信断
ポータルサーバ	335回	30回	9%	0ms	397ms	2ms	62s

業務アプリケーション移設時のping応答結果

業務アプリケーションを**フェイルオーバー機能**にて、異なる物理サーバへ移動した際のIPLレベルでのネットワーク接続断時間は、**60秒程度**であり、**セッションは保たれず、業務アプリケーション復旧のためにアプリケーションサーバ(Tomcat)を再起動する必要があった**。但し、再起動後は、正常にサービス復旧することが確認できた。

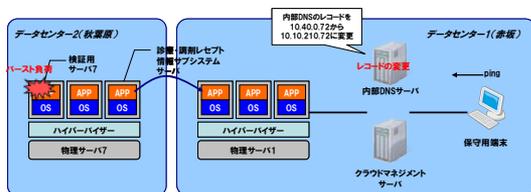
クラウドサービスの事業継続性に係る調査

調査結果

- **動的リソース割当て機能**により、**バースト負荷が発生**した場合に、異なる拠点の物理サーバに自動移動することが可能であり、別のサイトで業務継続するための有効な仕組みといえる
- **フェイルオーバー機能**により、**物理サーバ障害が発生**した場合に、異なる拠点の物理サーバにてサービス復旧が可能であり、ミッションクリティカルシステムを除き一般的なシステムであれば、別のサイトで業務継続するための有効な仕組みといえる

④災害回避を想定したセンター間での業務アプリケーション移設の調査結果

- 動的リソース割当て機能により、バースト負荷が発生した場合に、異なる拠点の物理サーバに自動移動することが可能



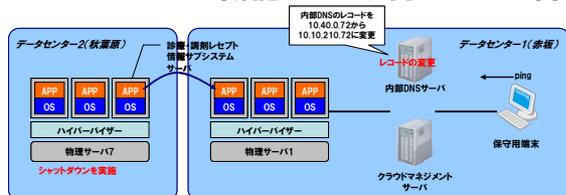
動的リソース割当て機能による拠点間での移設動作イメージ

サーバ	実施回数	失敗回数	失敗率	最短時間	最大時間	平均時間	通信断
診察調剤情報サブシステム (移動元アドレス)	277回	211回	76.2%	0ms	3ms	1ms	33s
診察調剤情報サブシステム (移動先アドレス)	276回	76回	27.5%	10ms	67ms	13ms	

業務アプリケーション移設時のping応答結果

動的リソース割当て機能による異なる拠点への移動について、異なる拠点の物理サーバへ移動した際のIPレベルでのネットワーク接続断時間は、30秒程度であり、セッションの維持は保たれていることが確認できた。本調査では、30秒程度のネットワーク断が発生したものの1分以内で移設が完了していることから、異なる拠点間でも利用できる仕組みであると考えられる。*拠点間移設に用いたネットワークは1Gbpsの専用線

- フェイルオーバー機能により、物理サーバ障害が発生した場合に、異なる拠点の物理サーバにてサービス復旧が可能



フェイルオーバー機能による拠点間での移設動作イメージ

サーバ	実施回数	失敗回数	失敗率	最短時間	最大時間	平均時間	通信断
診察調剤情報サブシステム (移動元アドレス)	61回	42回	68.8%	10ms	11ms	10ms	73s
診察調剤情報サブシステム (移動先アドレス)	62回	37回	59.7%	0ms	3ms	1ms	

業務アプリケーション移設時のping応答結果

フェイルオーバー機能による異なる拠点への移動について、異なる拠点の物理サーバへ移動した際のIPレベルでのネットワーク接続断時間は、70秒程度であり、セッションの維持は保たれなかった。本調査では、1分強の通信断が発生したが、無瞬断の要求のあるミッションクリティカルシステムを除き、一般的なシステムであれば、許容範囲であると考えられる。*拠点間移設に用いたネットワークは1Gbpsの専用線

クラウドサービスの事業継続性に係る調査

考察

可用性	システム種別	システムの特徴	実装が望ましい機能
低	事務支援系システム	<ul style="list-style-type: none"> 自治体内部の事務処理に関する情報を取り扱うシステム システム利用時間が業務時間であり、メンテナンス時間の確保が可能なシステム 従来、システムバックアップやコールドスタンバイ機の用意を行っていたシステム 	<ul style="list-style-type: none"> リソース管理機能 フェイルオーバー機能
	フロントエンド系システム (通年業務)	<ul style="list-style-type: none"> 住民がインターネットからアクセスするシステム 24時間365日サービス提供するシステム システム利用量の変動がないシステム 従来、システムメンテナンスが必要となった場合に、サービスを縮退して、順次メンテナンスを実施していたシステム 	<ul style="list-style-type: none"> リソース管理機能 フェイルオーバー機能 ライブマイグレーション機能
	フロントエンド系システム (季節性業務)	<ul style="list-style-type: none"> 住民がインターネットからアクセスするシステム 24時間365日サービス提供するシステム システム利用量に季節性があるシステム 従来、システム利用のピークに合わせて、事前に大量のハードウェアを用意してきたシステム 	<ul style="list-style-type: none"> リソース管理機能 フェイルオーバー機能 ライブマイグレーション機能 動的なリソース割当て機能
高	基幹系システム	<ul style="list-style-type: none"> 大規模災害等においても、情報の消失や復旧までの長時間サービス提供停止が許されない重要なシステム 住民に与える影響が非常に大きいシステム 従来、ディザスタリカバリーとして、遠隔のデータセンター間を高速回線で接続し、遠隔地バックアップやバックアップサイト対応がなされているシステム 	<ul style="list-style-type: none"> リソース管理機能 フェイルオーバー機能 ライブマイグレーション機能 動的なリソース割当て機能 拠点間でのライブマイグレーション機能

本調査研究結果での推奨モデル

クラウド管理

基盤+アプリケーション

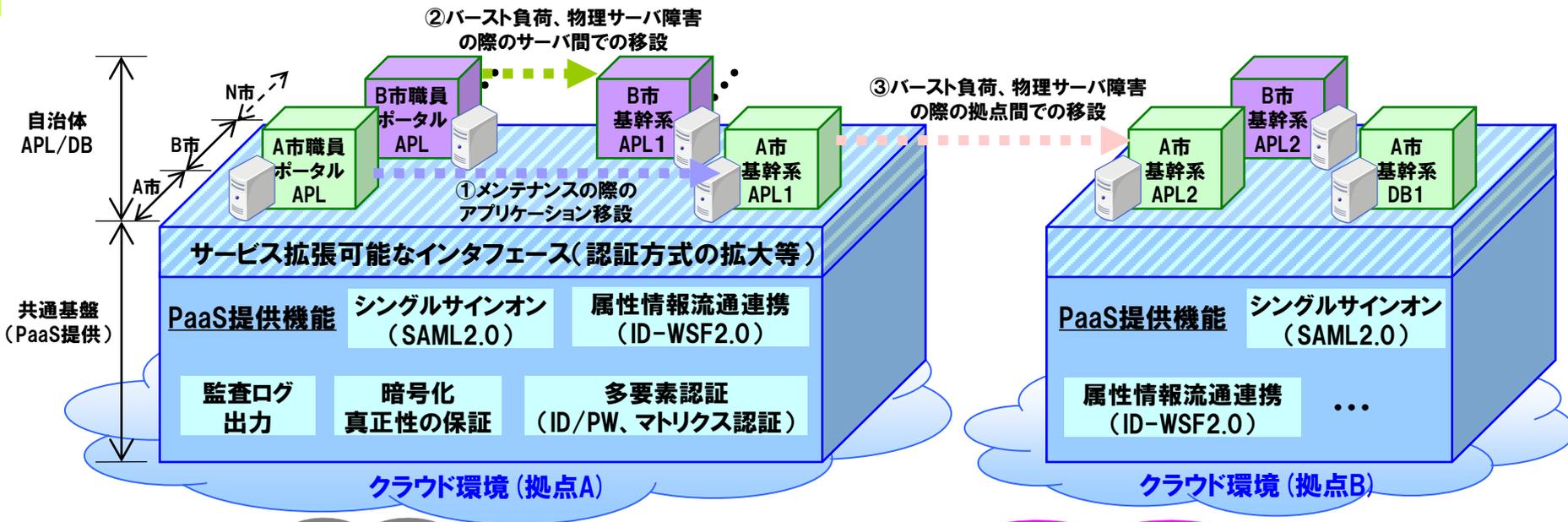
ネットワーク

ユーザ

- ①保守運用事業継続性
・ライブマイグレーション機能(数秒断)

- ②システム障害を想定した事業継続性
・動的リソース割り当て機能(数秒断)
・フェイルオーバー機能(約1分断)

- ③災害回避を想定した事業継続性
・拠点間動的リソース割り当て機能(約30秒断)
・拠点間フェイルオーバー機能(約1分断)



- インターネット網(住民用)
・自宅からのインターネット利用

- 携帯電話パケット網
・テレワーク利用(外出先)
・外出先からのインターネット利用

- インターネットVPN網
・テレワーク利用
(在宅型・施設利用型)

- 仮想専用線網
・職場・公共施設利用
・テレワーク利用
(在宅型・施設利用型)



住民アクセス

- ・自身の情報をインターネットを通じて確認可能
- ・許可した第三者(家族等)が情報を参照可能
- ・携帯端末、PC等、様々な端末からアクセス可能



自治体拠点

- ・きめ細やかな住民サービスの向上
- ・住民の各種情報を一体的に参照可能
- ・仮想専用線網等、閉域網からのアクセス制限

自治体クラウド導入のメリット

本調査研究の結果を踏まえモデル化した自治体クラウドサービスの導入メリットを以下に示す。

導入メリット

住民サービス向上

- ◆ 住民が自身の情報(医療、納税などの行政情報)をインターネットを通して一体的、かつ簡単に把握することができる。
- ◆ 住民が開示許可した家族等が参照可能なため、遠隔地に離れた家族の情報や、高齢者の情報を家族が簡単に把握することができる。
- ◆ 自治体職員も同様に住民情報を一体的に把握することが可能となり、実態に即したきめ細やかな住民サービスの実現につながる。

容易性 ※1

- ◆ 各種ガイドラインで定められた要件やセキュリティ事項を加味した機能を基盤が提供するため、自治体は個別に導入・運用をすることに比べて安全かつ安心して利用することが可能となる。
- ◆ 基盤にてPaaSとして提供される機能を使うことで、自治体は既存システム・アプリケーションに大幅な改造をすることなく、導入に係る手間・煩雑さを回避できる。

コスト低減

- ◆ サービス提供者側が基本的な機能(通信・セキュリティ)を提供するため、複数の自治体が共同利用型のクラウドサービスを導入することで、初期導入時の検討及び設計コストも含め、割り勘効果により、個別調達する場合と比べ安価に導入・運用することができる。

事業継続性の確保 ※2

- ◆ 堅牢なデータセンターで運用されるクラウドサービスを利用することで、庁舎で管理することに比べて災害によるシステム停止等の影響が最小化できる。
- ◆ 拠点が離れたデータセンターに自動でアプリケーションが移設可能なため、データの消失やサービスの長時間断を防ぐことが可能である。

※1 本調査研究実績値: SAML、ID-WSF提供(自治体クラウド開発実証実験適応プロトコル) 提供機能: シングルサインオン、属性情報流通連携、ログ出力、暗号化、真正性の保証、認証

※2 本調査研究実績値: 同一サーバ内移設(数秒断)、物理サーバ間移設(数秒~1分程度断)、拠点間移設(1分程度断)