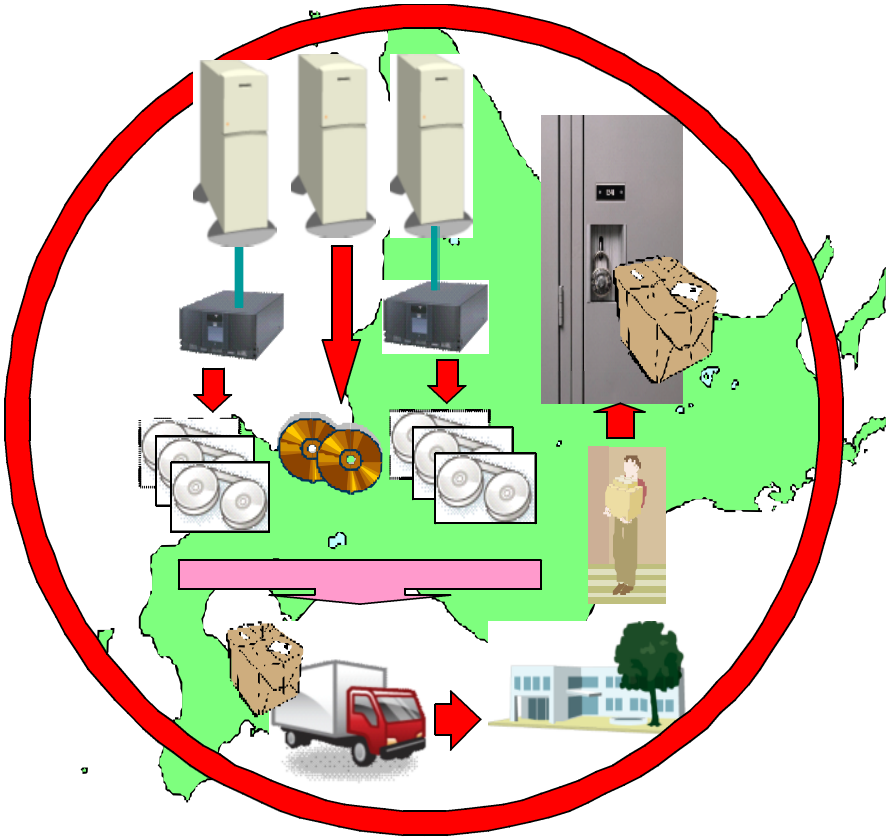
ＩＴ部門の業務継続計画

ステップ１
「情報インフラ等の脆弱性の把握と当面の対策」



平 成 23 年 3 月

北　海　道

～～～　目　次　～～～

第１部　ＩＴ部門の業務継続計画の策定方針　…　Ｐ１
　１　背　景　…　Ｐ１
　２　業務継続計画（ＢＣＰ）策定の趣旨　…　Ｐ１
　３　ＩＴ部門の業務継続計画の策定方針　…　Ｐ２
　　(1) 基本的な考え方　…　Ｐ２
　　(2) ＩＴ部門の業務継続計画（ＢＣＰ）の策定方針　…　Ｐ３

第２部　ステップ１「情報インフラ等の脆弱性の把握と当面の対策」　…　Ｐ５
　Ⅰ　道庁における情報インフラ等の脆弱性　…　Ｐ５
　　１　想定する地震の規模　…　Ｐ５
　　２　札幌市内における地震による被害想定　…　Ｐ６
　　３　庁舎及び庁舎内設備の現状　…　Ｐ７
　　４　庁舎内における情報通信機器の現状　…　Ｐ８
　　(1) 執務室内の情報通信機器の現状　…　Ｐ８
　　(2) 情報システムの現状　…　Ｐ８
　　５　大地震により想定される事態　…　Ｐ12
　　６　情報システムの復元の可能性　…　Ｐ13
　　７　情報インフラ以外のリスク　…　Ｐ14
　Ⅱ　情報システムの復元等に対する当面の対策　…　Ｐ15
　　１　当面の対策の基本的考え方　…　Ｐ15
　　２　執務室内の情報通信機器の保護対策　…　Ｐ15
　　(1) 対策の考え方　…　Ｐ15
　　(2) 対策の実施内容　…　Ｐ15
　　(3) サーバの取り扱いについての考え方　…　Ｐ16
　　３　業務アプリ等の保管対策　…　Ｐ17
　　(1) 対策の考え方　…　Ｐ17
　　(2) 対策の実施内容　…　Ｐ18
　　４　データのバックアップと保管対策　…　Ｐ19
　　(1) 対策の考え方　…　Ｐ19
　　(2) 対策の実施内容　…　Ｐ22
　　５　業務アプリ等の保管及びデータのバックアップと保管対策に関する行動計画の策定　…　Ｐ23
　　(1) 計画策定の対象システム　…　Ｐ23
　　(2) 行動計画書　…　Ｐ24
　　(3) 行動原則　…　Ｐ25
　　(4) 推進体制と役割分担　…　Ｐ25
　　(5) 実施手順と送付方法　…　Ｐ26
　　(6) 災害時の行動計画の取り扱い　…　Ｐ27
　　(7) 行動計画に基づく訓練の実施　…　Ｐ29
　　６　今後の課題等　…　Ｐ29

第１部　ＩＴ部門の業務継続計画の策定方針

１　背　景

我が国は地震大国として知られており、マグニチュード6.0以上の大地震の20%以上が、全世界のわずか0.3%に過ぎない国土の中で起きている。

近年では、平成７年に6,000人を超える死者・行方不明者を出した阪神・淡路大震災（兵庫県南部地震）をはじめ、新潟県中越地震、岩手・宮城内陸地震、本道では、平成５年に奥尻島北方沖で発生した北海道南西沖地震や、翌年の北海道東方沖地震といった大規模な地震が多数発生している。

大地震が発生すると、これまで当たり前のように使用してきた施設や、電気・ガス・水道などのライフラインが使用できず、道民生活に深刻な影響が生じるとともに、産業・経済活動も予期せぬ機能不全の状態に陥る可能性がある。

こうした震災では、道の庁舎も被災し、行政活動は大きな制約を受けることになるが、そうした状況下にあっても道民の生命、財産、経済活動等を守ることが重要な任務であり、道庁業務の機能を継続していくことが必要である。

道の業務を執行する上で、情報システムは必要不可欠なものとなっており、情報システムは平常時、災害時を問わず、業務執行の重要な役割を担っている。

被災対象を情報システムに限ってみても、情報通信関連の機能を担う設備や機器等の転倒や断線による損壊、電力供給の停止や空調設備の損壊による情報システムの停止などの事態に陥る可能性がある。

このような事態に備え、平常時に、災害発生時でも情報システムに関する業務の継続を確保するための対策を策定しておくことは極めて重要である。

総務省においては、このような事態に適切に対処するため、平成20年８月に、各地方公共団体に対し、「地方公共団体におけるＩＣＴ部門の業務継続計画策定に関するガイドライン」を示し、全庁的な取組に先駆けて、まず情報システムを所管する部門が中心となり、業務継続計画の策定に取り組むよう促したところである。

また、平成22年４月には、内閣府（防災担当）から、各都道府県に対し、業務継続体制に係る検討を支援することを目的として、業務継続に必要な事項及び手法等をとりまとめた「地震発災時における地方公共団体の業務継続の手引きとその解説」が示されている。

このような国の動きを受け、道においても、今般、全庁的な情報システムの運用やセキュリティ対策を所管するＩＴ（ＩＣＴ）部門の業務継続計画を策定することとしたものである。

２　業務継続計画（ＢＣＰ）策定の趣旨

「業務継続計画」（ＢＣＰ＝Business Continuity Plan ビジネス・コンティニュイティ・プラン）とは、ヒト、モノ、情報及びライフライン等利用できる資源に制約がある状況下において、応急業務及び継続性の高い通常業務（以下「非常時優先業務」という。）を特定するとともに、非常時優先業務の業務継続に必要な資源の確保・配分や、そのための手続きの簡素化、指揮命令系統の明確化等について必要な措置を講じることにより、大規模な地震発生時にあっても、適切な業務執行を行うことを目的とした計画である。（「地震発災時における地方公共団体の業務継続の手引きとその解説」（平成22年４月、内閣府（防災担当））から）

道では、札幌市内に大きな被害をもたらす大地震によって道の中枢機能が損害を被る事態に備え、非常事態時に道庁各部局等において実施すべき応急業務及び継続の優先度の高い通常業務を「非常時優先業務」と位置づけるとともに、非常時優先業務の業務継続に必要な措置を講じることにより、業務立ち上げ時間の短縮や発災直後の業務レベルの向上を図ることを目的とした計画である「北海道庁業務継続計画［地震編］」を、総務部危機対策局危機対策課が中心となって、現在、策定作業を行っている。

３　ＩＴ部門の業務継続計画の策定方針

(1) 基本的な考え方

札幌市内には道の中枢機能が集中しており、ここに大きな被害をもたらす大地震が起こった場合、道の機能も人的・物的な面から損害を被る。しかし、自らが大きな被害を受けたからといって、応急業務や継続しなければならない通常業務を止めることはできない。職員は自らの職責に基づき、業務を継続する責務がある。

また、いかなる理由があろうとも、道民や企業に関わる情報を消失させることは回避しなければならない。そのためには、平常時から、業務継続に対する十分な備えが必要である。

情報システムをどのように守るか、災害が発生したときにどのように行動するのかなどについてマニュアル化し、訓練を通して問題点を見いだし、さらに点検作業を通じた課題の洗い出し等により、改善のための取組を継続することが必要である。

情報システムは、設計、開発、調達、運用、保守に、膨大な時間と多くの費用と労力を注ぎ込んで運用している。逆の見方をすれば、情報システムについて、何の対策も講じていない状況で被災した場合、これまで積み上げてきたデータなど、システムの運用に必要な情報資産のすべてを消失しかねず、その場合、元の状態に戻すのに膨大な時間と費用と労力をつぎ込むこととなり、被害をより大きなものとしてしまうおそれがある。

事前の対策なしに、情報システムを災害時に継続・復旧することは困難であり、言い換えれば、ＩＴ部門は平常時からの業務継続の備えが必要な典型的な部門であるといえる。

ＩＴ部門の業務継続計画は、こうした考え方に基づき、策定していくこととする。

なお、策定にあたり、次の点に留意する。

＜策定にあたっての留意点＞

庁内各部等との連携	道全体の業務継続計画を所掌している総務部危機対策局危機対策課や、ファシリティ・マネジメントを所掌している総務部総務課と連携して対策を講じることを基本とする。
万全なセキュリティ対策	災害時におけるシステムの復旧は可能な限り早期に行うことが必要であるが、一方でデータ保護のための情報セキュリティ対策は、ソフトウェアの設定や動作確認など、データの機密性や完全性の確保のために相応の時間が必要とされる。 たとえ災害時であっても、個人情報保護の観点から、情報セキュリティを軽視することは許されないことから、セキュリティ対策を重視して、システムの復旧を行うことを基本とする。
運用保守業者との連携強化	情報システムの復旧は、システムの運用・保守業務を委託している事業者の協力を得なければ難しい。 このため、運用・保守業者との連携を密にし、災害時における連携のあり方を整理することが対策の前提となる。

(2) ＩＴ部門の業務継続計画（ＢＣＰ）の策定方針

震災による被害を最小限に抑え、かつ、災害時においても非常時優先業務に関わるシステムを稼働させるためには、パソコン等の転倒防止対策や業務アプリケーションソフトウェア（道が開発したもの。以下「業務アプリ」という。）やデータのバックアップ対策、サーバの外部保管対策のほか、現庁舎等の今後の整備や執務室の代替施設の確保、総合振興局・振興局（以下「総合振興局等」という。）の関わり方、データセンターの利用のあり方、運用・保守業者との連携のあり方など、検討しなければならない多くの課題を整理していく必要がある。

これらには、ＩＴ部門だけで解決できるものと、ＩＴ部門だけでは解決できず、全庁的な検討の中で解決しなければならない課題が多く含まれる。

また、解決に相当の時間を要するものもあることから、できるところから段階的に課題を整理していく必要がある。

このため、ＩＴ部門の業務継続計画の策定にあたっては、次の三つのステップに分けて段階的に進めていくこととする。

① ステップ１ … 情報政策課主導で実施できる対策

＜対策の主な内容＞

庁舎が被災し、一部損壊及び立入禁止により使用不能となる場合を想定し、現状における情報システムの脆弱性を把握し、当面取り組むべき即応型の対応策を明確化する。

② ステップ２ … 情報政策課が中心となり、業務担当課と連携して検討すべき対策

＜対策の主な内容＞

庁舎が被災し、立入禁止により使用不能となる場合を想定し、非常時優先業務を支える重要な情報システムについて、その代替・復旧に係る対策を明確化する。

③ ステップ３ … 全庁的に検討すべき対策

＜対策の主な内容＞

現庁舎の耐震化、代替施設の確保、総合振興局等の関わり方等、全庁的な検討過程の中で、非常時優先業務を支える重要な情報システムについて、ステップ２における代替・復旧に係る対策を推進、補強し、また、さらに抜本的な対策を構築する取組を全庁的に進める。

各ステップの全体構成イメージは次のとおりである。

ＩＴ部門の業務継続計画の全体構成イメージ

	ステップ１ 情報政策課主導で実施できる対策	ステップ２ 情報政策課が中心となり、業務担当課と連携して検討すべき対策	ステップ３ 全庁的に検討すべき対策
調査・分析	・システム運用に影響を及ぼす設備等の現状把握 ・データに関する現状把握	・非常時優先業務（重要システム）の継続に不可欠な情報インフラの把握 ・外部事業者との運用保守のあり方の見直し検討	・全庁的な検討としては、現庁舎の耐震化、代替施設の確保等がある。 その検討過程において、情報インフラの整備に係る必要な調査を実施する。
対策の対象インフラ	・業務アプリとデータ ・上記２つを格納しているハードウェア	・重要システム（ハードウェア、ソフトウェア、データ、通信回線）	・システム及び通信回線
対応策（想定）	・庁舎が使用不能とならないレベルでの対策 ・庁舎が使用不能となった場合でも、業務アプリやデータが同時被災しないための対策	・庁舎が使用不能となった場合に、最低限、重要システムを一時的に稼働できるスペース等の確保など	・代替施設における通信回線の構築に係る検討など
行動計画	・業務アプリやデータの確保等に関する行動計画の策定	・重要システムに係る代替・復旧行動計画の策定	・業務アプリやデータ及び重要システムに係る代替・行動計画の全庁的な点検・是正による改訂版の策定
訓練計画	・行動計画の一部に位置づけた移送訓練の実施	・重要システムに係る訓練計画の策定及び訓練の実施 ・訓練を通した業務継続計画の課題の洗い出しと解決の整理	・代替・復旧行動計画の見直しに伴う訓練計画の見直し ・訓練の実施

＜今後の進め方＞

ステップ２以降の計画策定については、道全体の業務継続計画における非常時優先業務の選定、さらに、現庁舎の今後の在り方（耐震化等）や災害時の代替施設の確保等今後の道全体での検討状況に合わせ、必要な調査を実施し、策定に向けた作業を進めていくこととする。

第２部　ステップ１「情報インフラ等の脆弱性の把握と当面の対策」

Ⅰ 道庁における情報インフラ等の脆弱性

１　想定する地震の規模

道の業務の中で管理・運営されている情報システムの中枢機能は、そのほとんどが本庁の知事部局、各種委員会、議会などにあり、これらの機関は、本庁舎、別館庁舎、議会庁舎に集中している。

このため、札幌市内に大きな被害をもたらすような大地震が発生すると、道の情報システムは大きな脅威にさらされることとなる。

想定される地震については、平成20年９月に札幌市防災会議が発表した「第三次地震被害想定について（想定結果）」における三つの伏在活断層、いわゆる野幌丘陵断層帯、月寒背斜に関連する断層（月寒断層）、西札幌背斜に関連する断層（西札幌断層）による札幌市直下型地震としている。

想定される震度は、いずれも最大震度が７で、震度６強以上の発生面積では、野幌丘陵断層帯が札幌市内面積の４％にあたる44㎢、月寒断層が同15.1％の169㎢、西札幌断層が同10.9％の122㎢となっている。

	マグニチュード	最大震度	震度６強以上発生面積（㎢）［札幌市内］
野幌丘陵断層帯	７．５	７	４４［ ４．０％］
月寒断層	７．３	７	１６９［15．1％］
西札幌断層	６．７	７	１２２［10．9％］

※札幌市防災会議の資料から抜粋

この想定に基づく本庁舎周辺の震度分布では、本庁舎が最大震度６弱（一部６強）、別館庁舎が同６強、議会庁舎が同６強となっており、非常に大きな揺れに見舞われると考えられている。

＜主な道の施設の震度＞

施　　設　　名	震　　度
北海道庁本庁舎	６弱（一部 ６強）
〃　　別館	６強
北海道警察本部	６強
北海道議会	６強
札幌建設管理部（旧札幌土木現業所）	６弱
道民活動センタービル（かでる２・７）	６強

※ 札幌市防災会議の資料から抜粋

２　札幌市内における地震による被害想定

この札幌市直下型地震が及ぼす札幌市全体の被害想定（札幌市防災会議）は、冬の早朝（午前５時）に地震が発生した場合、一番多くの人的被害が出るとしており、地震発生時期や時間帯によって被害の程度に差が出るとの結果が出されている。

札幌市直下型地震の被害想定（札幌市防災会議による）

①　建物被害

（単位：棟、件）

	野幌丘陵断層帯		月寒断層（最大）		西札幌断層	
	夏	冬	夏	冬	夏	冬
全 壊 棟 数	7,373	8,026	30,218	33,611	18,377	20,336
半 壊 棟 数	33,728	37,366	71,073	78,850	49,044	54,300
全出火件数	21	95	70	314	43	198
焼 失 棟 数	71	382	255	1,405	156	957

②　人的被害

（単位：人）

		野幌丘陵断層帯		月寒断層（最大）			西札幌断層	
		死　者	重傷者	死　者	重傷者	軽傷者	死　者	重傷者
夏	５時	365	1,054	1,789	3,123	27,500	1,046	1,910
	12時	253	754	1,318	2,378	20,919	772	1,479
	18時	254	757	1,325	2,391	21,006	777	1,488
冬	５時	1,707	958	8,234	2,411	28,003	4,690	1,535
	12時	1,282	680	6,574	1,805	21,204	3,766	1,185
	18時	1,293	694	6,619	1,850	21,380	3,793	1,213

※ 冬：発災後２時間以内に救出されない場合に凍死すると仮定したもの

3　庁舎及び庁舎内設備の現状

災害を想定した本庁舎等の主要な設備の現状を整理すると、次のとおりである。

<table>
<tr><th colspan="2">項　　目</th><th colspan="3">現　　状</th></tr>
<tr><td colspan="2">庁　舎</td><td>建築年次</td><td colspan="2">耐 震 判 定 係 数</td></tr>
<tr><td colspan="2">本　庁　舎</td><td>S43．4</td><td>0.61</td><td rowspan="3">耐震安全性の分類上、求められている耐震判定係数の目標値は1.50以上</td></tr>
<tr><td colspan="2">別 館 庁 舎</td><td>S53.12</td><td>1.13</td></tr>
<tr><td colspan="2">議 会 庁 舎</td><td>S26．1</td><td>0.50</td></tr>
<tr><td colspan="2">電　力</td><td colspan="3">電力の供給が途絶えた場合には、本庁舎（議会庁舎を含む）専用非常用自家発電機（800KW：９時間）及び別館庁舎専用非常用自家発電機（500KW：７時間）により、消防等非常用設備と本庁舎の必要最小限の範囲に供給する。(燃料タンクにＡ重油を補給できれば、さらに継続して使用が可能である。)</td></tr>
<tr><td colspan="2">非常用電力の給電系統</td><td colspan="3">現状では、本庁舎は必要最小限の範囲の給電は可能だが、別館庁舎及び議会庁舎は非常灯、非常用設備のみへの給電で、事務室内への給電はされない。
また、本庁サーバ室の非常用電力は、北海道総合行政情報ネットワーク用の非常用自家発電機から一部システムについて供給を受けるが、空調設備はフォローされていない。</td></tr>
<tr><td colspan="2">水</td><td colspan="3">上水道が停止した場合、本庁舎及び議会庁舎は地下水を使用しているため電力の供給下で継続して使用可能であり、別館庁舎は高架水槽（容量：23㎥）の残留水を供給する。
雑用水は、地下水を使用する。</td></tr>
<tr><td rowspan="2">通　信
手　段</td><td>一般電話回線
（ＮＴＴ回線等）</td><td colspan="3">省庁や総合振興局等、市町村以外の防災関係機関とは、一般電話回線が利用可能な場合に、災害時優先電話により通信を確保する。
携帯電話回線が利用可能な場合には、災害時優先電話により防災関係機関との通信を確保する。</td></tr>
<tr><td>北　海　道
総合行政情報
ネットワーク
（防災無線）</td><td colspan="3">省庁や総合振興局等、市町村とは、地上系及び衛星系の２ルートにより電話（ファクシミリ）回線を整備しており、一般電話回線が不通となっても、これらの機関との通信は確保できる。
（本庁舎が倒壊等使用不能となった場合、ネットワーク機能は失われるが、次の通信は可能である。
・衛星系による相互通信
・地上系による同一総合振興局等管内での相互通信）
また、庁舎が停電した場合も、専用非常用自家発電機により通信機能の確保は可能である。</td></tr>
<tr><td colspan="2">道庁行政情報ネットワーク
（庁内ＬＡＮ）</td><td colspan="3">本ネットワークの主要な管理機能が本庁舎とデータセンター（本庁舎と商用（広域イーサネット）回線で接続）に集中しているため、本庁舎の倒壊等によりこの機能が停止した場合は、総合振興局等をはじめとする出先機関でも、本ネットワーク上で稼動している情報システム（行政情報コミュニケーションシステム、総合文書管理システム、財務会計トータルシステム等）が使用不能となる。
また、本ネットワークの電源については、本庁サーバ室の一部機器を除いて非常用電力の給電系統に含まれていないため、停電時は使用不能となる。</td></tr>
</table>

※ 耐震判定係数とは、その建物に求められている耐震性の理論値に対し、その建物が現在持っている耐震性を表す指標で、その値が1.0以上で「安全」とされる。

４　庁舎内における情報通信機器等の現状

庁舎内における情報通信機器及び情報システムの現状を把握するため、平成22年６月１日現在で、本庁舎、別館庁舎及び議会庁舎に執務室を置く道の機関に対し、書面で実施した調査結果は、次のとおりである。

(1) 執務室内の情報通信機器の現状

本庁舎、別館庁舎及び議会庁舎の各執務室内に設置されている情報通信機器のうち、転倒等防止措置がとられているのはサーバ等の一部の機器であり、ほとんどのパソコンは、転倒等防止措置が全くとられていない。

◇表１　執務室内の情報通信機器の転倒等防止措置状況

（単位：台、％）

区　　分		設置台数	転倒等防止措置済み台数	措置率
デスクトップ型パソコン	本　体	２，９３１	１７	０．５８
	ﾃﾞｨｽﾌﾟﾚｲ	２，９０８	１	０．０３
ノート型パソコン		２，６３３		
サーバ	ラック型	５９	３７	６２．７１
	タワー型	２５	０	０
その他の情報通信機器		２１	７	３３．３３

(2) 情報システムの現状

今回の調査では、本庁舎、別館庁舎及び議会庁舎内にある道の機関が管理するもののうち、札幌市内にシステム本体（サーバ等）がある123の情報システムにおけるハードウェア及びソフトウェアの管理の現状を次のとおりまとめた。

①　情報システムで使用しているサーバの設置状況

執務室内に設置されているサーバは全体の約15％を占めている。

また、庁舎外に設置されているサーバは全体の約79％であるが、国等の機関が管理しているものを除くと、その所在地のほとんどは札幌市内である。

◇表２　情報システムで使用しているサーバの設置状況

（単位：台、％）

	台　数		左の内訳		
			執務室内	本庁サーバ室	庁舎外
サーバ	５５６		８４	３３	４３９
		比率	１５．１	５．９	７９．０

② 道が外部委託で開発した業務アプリ等の保管状況

今回調査対象とした123の情報システムのうち、道が外部委託で開発した業務アプリは全体の約60%の74システムであるが、一部のシステムにおいて、成果物（納品物）が保管されていなかったり、存在が不明となっているものがあった。

業務アプリ等の保管場所は約81%が執務室内のロッカー等であり、残りは運用業者の施設内（データセンター等）であった。

なお、システムを復元させるためには、業務アプリやソースプログラム、復旧手順書等の関係媒体※がきちんと契約書等に明記され、かつ保管されていなければならないが、多くのシステムにおいて復旧手順書が成果物として明記されていなかった。

◇表３ 道が外部委託で開発した業務アプリ等の保管状況

区　　分	件　数
調査対象システム数	１２３
うち、道が開発した業務アプリ	７４
うち、保管なし（不明）のもの	６

※ 業務アプリのほかに、システム設計書、プログラム設計書、ソースプログラム、システム復旧手順書、システムを構成している一連のソフトウェアのＣＤ－ＲＯＭ、プロダクトキー等の契約書上の成果品

③ 開発後に改修等がされているシステムの状況

道が開発した業務アプリで、開発後に改修等がされているものは58システムあり、このうち、最新バージョンの業務アプリが納品されていないシステムが９システムあった。

これらについては、開発時点のシステムに復元することはできても、最新バージョンのシステムに復元することは困難であり、最新データを表示できない場合も想定される。

◇表４ 開発後、改修等がされているシステムの状況

区　　分	件　数
開発後、改修等がされているシステム	５８
うち、最新バージョンの業務アプリが納品されているシステム	４９

④ システム全体のバックアップの状況

システム全体のバックアップとはオペレーティングシステム（ＯＳ）やアプリケーション部分も含めた全体をバックアップする手法のことで、道が管理している情報システムの約46%で行われている。

システムを復元する場合は、業務アプリやソースプログラム、復旧手順書等の関係媒体により作業を行うことになるが、緊急に復元する必要がある場合は、システム全体のバックアップがあれば効率的である。

◇表５ システム全体のバックアップの状況

バックアップ状況	システム数	バックアップメディアの種類				
		磁気テープ	光学ディスク	ハードディスク	ストレージ装置	汎 用 機
バックアップあり	５８	３３	８	５	７	５
バックアップなし	５６					
そ の 他 ※	９					

※ 国等の機関が管理しているシステム

［バックアップメディアの概要］

種　　類	内　　容
磁気テープ	磁性体を塗ったテープをカセットに収めた着脱可能な記憶装置。１巻あたりの記憶容量が数十GB程度の大きさのものもあり、記憶容量からみた価格が安価である。ただし、ほかのメディアに比べ読み書きの速度が遅く、特定の部分の記憶内容を読み書き（ランダムアクセス）することができない。
光学ディスク	レーザー光線を使ってデータを読み書きする。種類は多数あるが、バックアップ用にはCD-R、DVD、Blu-rayなどが使われている。主にパソコン用として用いられている。
外付けハードディスクドライブ（外付けHDD）	ハードディスクドライブ本体を更に金属や樹脂の筐体に入れ、ケーブルによってコンピュータに接続できるようにしたもの。
リムーバブル・ハードディスクドライブ（リムーバブルHDD）	データが記録される磁気ディスク部分だけが取り外せる構造になっているハードディスク。フロッピーディスクなどの記憶装置と同じように、ディスクを交換して使うことができる。読み書きの機構がハードディスクとほとんど同じであることから、他の装置よりも高速にデータの読み書きが行える。
ストレージ装置	多数のハードディスクドライブを搭載する筐体（ケース）で、大容量のデータを高速に処理することができる。
汎用機	安定性や信頼性に優れ、大量のデータを計算したり保存したりする業務に適した大型コンピュータ。

⑤ データの種類

道が運用している情報システム上のデータについて、どのような性質（災害時におけるシステムの継続性を判断する要素となるもの）を有するのか調査を行った。

◇表６ データの種類

データの種類	システム数※
Ａ 通常業務において毎日更新が必要なデータ	３４
Ｂ 大地震等の災害・事故が発生した場合、すぐに使用するデータ	２０
Ｃ 道のみが保有し、消失した場合に元に戻すことが不可能あるいは相当困難なデータ	５３
Ｄ 法令等により保存が義務づけられているデータ	２２
Ｅ 個人情報が含まれているデータ	６６
Ｆ 道民や企業等の権利・義務に関係するデータ	１４
Ｇ 国、市町村等と共有しているデータ	２７
Ｈ Ａ～Ｇのいずれにも該当しないデータ	１８

※ 一つのシステムのデータで複数の選択肢に該当するものがあるため、回答の計と調査対象システム数（123システム）は一致しない。

ＡからＧに該当するデータを使用している情報システムについて、それぞれどのようなシステムといえるのか整理すると次のとおりとなる。

Ａ　毎日稼働している（稼働が必要な）システム
Ｂ　災害時にも停止させることができないシステム
Ｃ　いかなる場合でも消失させてはならないデータを使用しているシステム
Ｄ　一定期間中、消失させてはならないデータを使用しているシステム
Ｅ　いかなる場合でも情報の流出があってはならないシステム
Ｆ　データを喪失すると業務の継続に著しい支障を来すおそれがあるシステム
Ｇ　仮にデータを喪失しても、復元できる可能性があるシステム

⑥　データのバックアップの状況

道が運用している情報システム上のデータについてのバックアップ状況は全体の約85%のシステムで行われている。

データの保管場所は約57%が執務室内であり、残りは運用業者の施設内（データセンター等）であった。

◇表７　データのバックアップの状況

バックアップ状況	システム数	バックアップメディアの種類				
		磁気テープ	光学ディスク	ハードディスク	ストレージ装置	汎　用　機
バックアップあり	９４	４８	１５	２２	６	３
バックアップなし	１７					
バックアップ必要なし※	１２					

※ 国等の機関が管理しているサーバにアクセスしてデータの入力作業を行うシステムのため、道においてデータのバックアップを行う必要がないもの。

⑦　データの種類に対する「バックアップなし」の状況

表８は、表７で「バックアップなし」となっている17システムを、データの種類で分けたときの状況を表したものである。

ＡからＦに該当するデータは、バックアップが不可欠と考えられるデータであるが、すべての項目において「バックアップなし」に該当するものがあるという結果となった。

◇表８　データの種類に対する「バックアップなし」の状況

データの種類	システム数
Ａ 通常業務において毎日更新が必要なデータ	2
Ｂ 大地震等の災害・事故が発生した場合、すぐに使用するデータ	3
Ｃ 道のみが保有し、消失した場合に元に戻すことが不可能あるいは相当困難なデータ	9
Ｄ 法令等により保存が義務づけられているデータ	1
Ｅ 個人情報が含まれているデータ	6
Ｆ 道民や企業等の権利・義務に関係するデータ	1
Ｇ 国、市町村等と共有しているデータ	4
Ｈ Ａ～Ｇのいずれにも該当しないデータ	4

5　大地震により想定される事態

札幌市内に大規模な地震が発生した場合、庁舎内にある情報システムを構成するハードウェア、ソフトウェア及びデータ（以下「情報インフラ」という。）がどのような状況となるのか、起こり得る事態を、①震度４～６弱未満の地震（庁舎が倒壊せず引き続き使用できるケース）、②震度６強以上の地震（庁舎が倒壊または庁舎の使用が困難となるようなケース）の二つに分けて想定した。

	強い揺れ	天井剥落・壁崩壊	ｽﾌﾟﾘﾝｸﾗｰ作動・漏水	火　　災
① 震度 4～6 弱	・転倒等防止措置未措置の機器は机上から落下し、損壊の可能性大	・落下物の衝撃による機器の損壊の可能性大 ・書庫等に保管のＣＤ－ＲＯＭ、ドキュメント類の損失の可能性大	・水浸しにより機器の使用不能になる可能性大 ・書庫等に保管のＣＤ－ＲＯＭ、ドキュメント類の損失の可能性大	・機器及び書庫等に保管のＣＤ－ＲＯＭ、ドキュメント類の損失の可能性大
② 震度 6強以上	・庁舎の倒壊又は著しい損壊の場合は庁舎への立入禁止措置により、すべての情報インフラは消失又は消失同然			

（注）この想定には、気象庁の「震度階級における人の体感・行動、屋内の状況、屋外の状況」を参考とした。

［ 参 考 ］

震度階級における人の体感・行動、屋内の状況、屋外の状況（気象庁）

震度階級	人の体感・行動	屋内の状況	屋外の状況
0	人は揺れを感じないが、地震計には記録される。		
1	屋内で静かにしている人の中には、揺れをわずかに感じる人がいる。		
2	屋内で静かにしている人の大半が、揺れを感じる。眠っている人の中には、目を覚ます人もいる。	電灯などのつり下げ物が、わずかに揺れる。	
3	屋内にいる人のほとんどが、揺れを感じる。歩いている人の中には、揺れを感じる人もいる。眠っている人の大半が、目を覚ます。	棚にある食器類が音を立てることがある。	電線が少し揺れる。
4	ほとんどの人が驚く。歩いている人のほとんどが、揺れを感じる。眠っている人のほとんどが、目を覚ます。	電灯などのつり下げ物は大きく揺れ、棚にある食器類は音を立てる。座りの悪い置物が、倒れることがある。	電線が大きく揺れる。自動車を運転していて、揺れに気付く人がいる。
5弱	大半の人が、恐怖を覚え、物につかまりたいと感じる。	電灯などのつり下げ物は激しく揺れ、棚にある食器類、書棚の本が落ちることがある。座りの悪い置物の大半が倒れる。固定していない家具が移動することがあり、不安定なものは倒れることがある。	まれに窓ガラスが割れて落ちることがある。電柱が揺れるのがわかる。道路に被害が生じることがある。
5強	大半の人が、物につかまらないと歩くことが難しいなど、行動に支障を感じる。	棚にある食器類や書棚の本で、落ちるものが多くなる。テレビが台から落ちることがある。固定していない家具が倒れることがある。	窓ガラスが割れて落ちることがある。補強されていないブロック塀が崩れることがある。据付けが不十分な自動販売機が倒れることがある。自動車の運転が困難となり、停止する車もある。
6弱	立っていることが困難になる。	固定していない家具の大半が移動し、倒れるものもある。ドアが開かなくなることがある。	壁のタイルや窓ガラスが破損、落下することがある。
6強	立っていることができず、はわないと動くことができない。揺れにほんろうされ、動くこともできず、飛ばされることもある。	固定していない家具のほとんどが移動し、倒れるものが多くなる。	壁のタイルや窓ガラスが破損、落下する建物が多くなる。補強されていないブロック塀のほとんどが崩れる。
7		固定していない家具のほとんどが移動したり倒れたりし、飛ぶこともある。	壁のタイルや窓ガラスが破損、落下する建物がさらに多くなる。補強されているブロック塀も破損するものがある。

６　情報システムの復元の可能性

前記の５のような事態が起こった場合、損壊または消失した情報システムをできるだけ早期に復元する必要があるが、情報インフラの中には、損壊・消失した物品等を購入またはリースにより調達できるものと、製品としては売っておらず消失してしまうと入手が困難となるものがある。

情報インフラの復元の可能性について整理すると、次のとおりとなる。

ハードウェアは同様のものを再度調達することが可能（ただし、生産停止や保守サポート切れになっているものは難しい場合あり。）であるのに対し、道が開発した業務アプリと、道しか保有していないデータについては、消失すると完全に復元することは困難となる。

情報インフラ	内　　容	復 元 の 可 能 性
ハードウェア	・サーバ、パソコン ・ネットワーク機器 ・プリンター　など	・工事の実施や機器の購入又はリースにより復元可能
ソフトウェア	・業務アプリ（道が開発したもの） ・市販のソフトウェア	・業務アプリについては、基本的に道しか保有していないため、消失するとバックアップをとっていない限り、復元は不可能 ・市販のソフトウェアは、購入により復元可能 （ただし、年数が経過したものは、同一バージョンでの購入が難しい場合あり）
データ	・各種情報	・データは道しか保有していないものがほとんどであるため、消失すると復元は不可能

このことを踏まえて、現在の状況で被災した場合の復元の可能性について、震度４～６弱と６強以上の場合に分けると、次のとおり整理できる。

	サーバ	パソコン	ケーブル	プリンター	業務アプリ	データ
① 震度 ４～６弱	損壊しても本体は購入又はリースにより調達可能だが、システムは業務アプリ等がなければ復元不可能（※）	損壊しても購入又はリースにより調達可能	断線しても工事により復元可能	損壊しても購入又はリースにより調達可能	外部にバックアップがなければ復元不可能	外部にバックアップがなければ復元不可能
② 震度 ６強以上	・機器や業務アプリ、データについて想定される状況は震度４～６弱の場合と同様であるが、本庁舎等が使用できない場合を想定し、執務室として活用可能な代替施設の確保が必要。 ・代替施設における情報共有等に必要な庁内ＬＡＮを構築するための設計、ネットワーク機器等の設置、ソフトウェア等のインストールや動作確認、テストなどの作業が必要。 ・代替施設におけるシステム稼働まで、数ヵ月かかることも予想される。					

※ サーバが庁舎の外部に設置されている場合、同時被災すれば、システム及びデータは復元不可能

７　情報インフラ以外のリスク

前記の５では情報インフラに起こり得る事態を想定したが、このほかに情報システムの復元に関しては、次のような事態が想定される。

なお、これは庁舎が使用可能な場合（一部使用不能を含む）のことであり、倒壊、立入禁止等により使用不能な場合は１～４の項目についてはこの限りでない。

状　　況		リ　ス　ク
1	夜間、休日等勤務時間外に大地震が発生した場合	・復旧に必要な職員が速やかに参集できない。 ・職員が被災し、勤務できない。（※） ・運用業者の職員が被災し、業務の遂行が困難となる。
2	停電の長期化	・庁内ＬＡＮが非常用電力の給電系統外であることから、庁内ＬＡＮに接続されている情報システムは使用できないが、非常用電源が途絶えた場合、庁内ＬＡＮ非接続の情報システム、機器についても稼働できない。
3	空調設備の損壊	・温度、湿度の異常により、情報システムが停止する。
4	電話回線、ネットワーク回線の寸断	・一般電話の不通により、職員間、業者との連絡が困難となる。（携帯電話も輻輳によりつながりにくくなる。） ・ネットワークに接続されている情報システムは停止する。
5	運用業者の同時被災	・庁外に設置しているサーバ等が損壊し、データを消失する。
6	都市機能麻痺や混乱に乗じた反社会的行為、犯罪の横行	・大規模なネットワーク障害を引き起こすコンピュータウイルスの蔓延やサイバーテロの発生により、情報システムが障害を受け使用できない。
7	感染症の発生・流行（パンデミック）	・職員が感染し、勤務できない。 ・情報システムの運用業者の職員が感染し、業務の遂行が困難となる。 ・ライフライン、物流等の社会機能が維持できなくなる。

※ 職員が被災し勤務できない比率は、札幌市内に居住する職員の約２％（月寒断層の地震の場合、最大で38,648人が死傷するとの想定であり、これは全札幌市民の約２％に該当する。…札幌市防災会議による）

Ⅱ　情報システムの復元等に対する当面の対策

１　当面の対策の基本的な考え方

道で運用されている情報システムを巡っては、庁舎の耐震性や電源・非常用電力の給電系統の脆弱性など、情報インフラの設置環境に関わる課題があるほか、パソコン、サーバなどの機器の安全性の確保や、業務アプリやデータなどのバックアップなど、情報インフラそのものが脆弱性を有していることが判明した。

庁舎や庁舎内設備などの耐震性向上や災害時の代替施設の確保などについては、現在、担当部局において検討されている段階であり、現時点ではこれらに対応した情報システムの復元を具体的に検討することは難しいため、これらについてはその検討状況を踏まえて、情報インフラ整備に係る必要な調査を実施し、あり方を整理していくこととする。

このため、ステップ１においては、地震による情報システムの被害をできる限り少なくするための当面の対策を講じることとする。

また、早期復元という業務継続の核となる部分については、ステップ２でその対応策を整理することとし、ステップ１では、システムを確実に復元し再稼働できるための仕組みの構築を中心に整理する。

［当面の対策］

○ 情報インフラの被害をできるだけ最小限度にとどめるための取組の実施
→「２　執務室内の情報通信機器の保護対策」

○ 地震によりソフトウェアやデータが消失しても、確実に復元し、再稼働するための仕組みの構築
→「３　業務アプリ等の保管対策」
→「４　データのバックアップと保管対策」

２　執務室内の情報通信機器の保護対策

(1) 対策の考え方

前述のとおり、本庁舎、別館庁舎及び議会庁舎の執務室内にある情報通信機器、中でもパソコンについての転倒等防止措置はほとんどとられていないのが実情であり、このままの状態で大地震に見舞われた場合の被害額は、相当多額になることが予想される。

このことから、執務室内のパソコン等の機器について、大きな揺れによる物理的被害をできる限り少なくする対策をとる必要がある。

なお、本庁舎の９階以上の階とそれ以外の一部及び別館庁舎については、火災に備えスプリンクラーが設置されており、これが作動した場合、情報通信機器が使用不能となるおそれがあるが、これを水を使わないハロゲン化合物消火設備に変更するとした場合、気密性の高い執務室に変更する必要があるが、気密化工事には100㎡あたり数千万円単位の費用がかかるとされており、現実的な選択ではないと判断される。

(2) 対策の実施内容

執務室内の情報通信機器の保護対策として、次のとおりパソコン等について転倒等防止措置を行うこととする。

このうちサーバについては当面の措置であり、将来的には「(3) サーバの取り扱いについての考え方」で示している方向性等に沿って進めていくこととする。

なお、この対策については、先の調査結果により速やかな実施が必要との判断から、各総合振興局等を含む全庁で、既に取組を進めており、対策の実施状況について、毎年度、情報政策課長に報告することとしている。

区　　分		対　　策
パソコン	デスクトップ型	・ディスプレイと本体を、市販されている耐震用のマットやベルト、ストッパー等を用いて机に固定する。
	ノート型	・耐震用マット等による措置は要しない。 なお、セキュリティ対策上、ワイヤーロック方式による盗難防止を推奨する。
サーバ	ラック型	・ボルトやスタビライザーで固定したラックに収納し、ラック内もボルトで固定する。
	タワー型	・デスクトップ型パソコンと同じ。

(3) サーバの取り扱いについての考え方

サーバについては、執務室内に設置しているもの、本庁舎のサーバ室に設置しているもの、外部に設置しているものの３つの形態があり、それぞれの方向性と今後の進め方は次のとおりである。

設置形態	方向性	今後の進め方
(1) 執務室内に設置しているサーバ	耐震及び免震が施されている外部のデータセンターへの移設に特に支障がないサーバについて、可能な限り移設する。	システム更新時に、「情報システム診断」において、外部へ移設する場合のシステム構成や通信回線などを検討した上で、移設の可否について判断する。
(2) 本庁舎のサーバ室に設置しているサーバ	道庁行政情報ネットワーク（庁内ＬＡＮ）関係については、本庁舎が倒壊等により機能停止した場合でも、総合振興局等で使用可能となるよう、回線網等の整備について検討する。（※） その他のシステムで、移設に特に支障がないサーバについては、耐震及び免震が施されている外部のデータセンターへ可能な限り移設する。	道庁行政情報ネットワークの整備の検討については、「ステップ2」において行う。
(3) 外部に設置しているサーバ	サーバ設置されている外部の建物が、耐震及び免震が施されているかどうか、また、二次災害についての防火・漏水対策や、停電対策としての電源の多重化等を確認し、施されていない場合は、施されているデータセンターへ可能な限り移設する。	全体最適化の取組の一つであるサーバ統合の検討に併せて、通信回線費用などを考慮した上で、移設の可否について判断する。

〈 耐震構造 〉

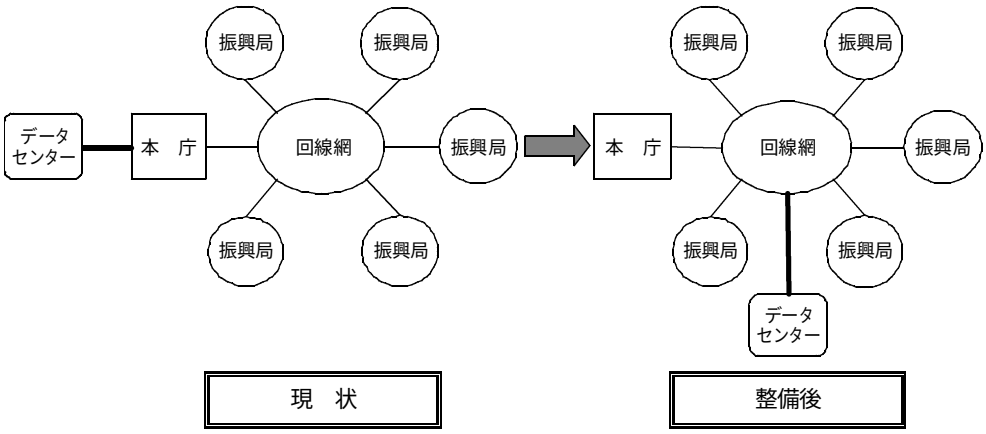
建物の構造（柱や梁）事態が地震に耐えるような強度に造られているもの。地震で生じる揺れに耐えるように設計された構造のこと。地震エネルギーがそのまま家屋に伝わるので、免震、制震に比べ地震時に壁や家具等が損傷しやすい。

〈 免震構造 〉

建物と地盤との間に積層ゴムなどの特殊な装置を付け免震層を造ることで、地震力を建物に直接伝えないようした構造のこと。地震に強いだけでなく、揺れそのものを軽減することによって、室内の損傷などの被害を防ぐことができる。

※

道庁行政情報ネットワークの整備（イメージ）



◇ データセンターと回線網を直結することで、災害時でも
ネットワークの利用が可能となる。

3　業務アプリ等の保管対策

（1）対策の考え方

道が開発している多くの情報システムは、OSやミドルウェア等の既製品の上に、業務アプリ（既製品またはオーダーメイド）を載せて、サーバやパソコン等のハードウェア上で動かす仕組みとなっている。

また、複数のソフトウェアの組合せで構成されているものが多く、それらのソフトウェアをインストールし、正常に起動させるには、各種の設定作業を行う必要がある。

地震等により現在稼働中の情報システムが消失した場合でも、システムを構成している複数のソフトウェアがきちんと保管され、システムを復元するための作業手順書等が存在すれば、仮に運用保守業者が被災し、直ちに運用に入れない場合が生じたとしても、運用保守業者以外でも、新たなハードウェア上でシステムを復元し稼働させることは可能である。

一般的なシステムの復元手順は、次のとおりである。

《システムの復元手順》

① ハードウェア（サーバ等）の修理又は購入
② 必要なＯＳや市販のソフトウェア及び業務アプリのメディア（ＣＤ－ＲＯＭ等）の準備
③ ＯＳの再インストール
④ 再起動
⑤ サービスパックの適用
⑥ 再起動
⑦ 市販のソフトウェア等必要なソフトのインストール
⑧ 市販のソフトウェア等の諸設定
⑨ 業務アプリの再インストール
⑩ 業務アプリの最新バッチの適用・各種設定
⑪ 再起動
⑫ バックアップメディアからデータを挿入

上記の作業を可能とするためには、業務アプリ等の保管に関して、次のような対策をとる必要がある。

［業務アプリ等保管対策の考え方］

○　システム開発の委託に係る契約書において、業務アプリ等を成果物として道への提出を義務づける

○　同時被災を避けるため、原則として札幌市以外の遠隔地で保管する

なお、システム担当課においては、システム開発時に可能な限り、復旧作業が行いやすい「イメージバックアップ」の導入について検討するよう努めること。

※イメージバックアップ…システムの復元を容易にするため、ＬＴＯなど大容量のテープを用い、データだけではなくＯＳやミドルウェア、業務アプリなどすべてのソフトウェアとデータをコピーすること。

(2) 対策の実施内容

① 契約等による関係媒体提出の義務化

システム復元に必要な関係媒体は、主に次のとおりであり、システムの新規開発及び更新時等の改修の際、委託業者と取り交わす契約書（または業務処理要領）に必ず明記し、成果物として提出を義務づける。

（更新時の改修にも義務づけるのは、改修内容によっては、開発時の成果物では最新のデータを取り込めないこともあり、常に最新バージョンの成果物を求める必要があるためである。）

- 既製品のソフトウェア（ＯＳ、ミドルウェア、業務アプリ(既製品)）のＣＤ－ＲＯＭ（リカバリ用）
- 道が開発した業務アプリのＣＤ－ＲＯＭ
- ソースプログラム（パッケージソフトのものを除く。）
- 復旧手順書（リカバリ手順書）（サーバやネットワーク機器の設定情報を含む）

［システム開発（改修）の委託業者との間で取り交わす契約書または業務処理要領）の記載例］

（委託契約書）

第１条　北海道は、○○システム開発業務の処理を△△に委託し、△△は、これを受託する。

第２条　△△は別紙委託業務処理要領により委託業務を処理しなければならない。

（委託業務処理要領）

○　成果品及び数量

成果品及び数量は、次のとおりとする。

(1) システム設計書　２部
(2) ○○システムのソフトウェア（ＣＤ－ＲＯＭ）　２部
(3) ソースプログラムのＣＤ－ＲＯＭ　２部
(4) 復旧手順書（リカバリ手順書）　２部

・その他、操作マニュアルなど必要な成果品を追加

※　２部のうち、１部は遠隔地保管用、もう１部は担当課の執務室保管用。執務室保管用は、平常時において何らかの原因で業務アプリが壊れた場合のリカバリ用として用いる。

② 関係媒体の遠隔地保管に係る実施方法

契約書（または業務処理要領）に明記された成果物のうち、前記①の関係媒体については、原則として、道の各総合振興局等（石狩振興局を除く）が管理する施設内で保管することとする。

なお、保管に係る具体的な行動手順等については、後述の「５　ステップ１における行動計画」において示す。

４　データのバックアップと保管対策

(1) 対策の考え方

道の情報システムにおけるデータのバックアップメディアの使用状況については、P11の表７のとおり、磁気テープと光学ディスクで全体の７割近くを占めている。

バックアップに際しては、メディアによって手間やコストが異なるため、データの更新頻度などに応じて、効率的なメディアを選択する必要がある。

情報システムは、ハードウェアやソフトウェアの組合せで構成され、運用開始とともに、主に職員ユーザにより、データの蓄積が行われる。

データがなければ、システムとして機能しないため、システム復元に必要な関係書類や媒体を提出させるだけではなく、システムの運用時において、データのバックアップに係る作業も併せて実施する必要がある。

バックアップ作業は、データが入っているサーバからバックアップメディアにコピーをとる作業であり、実施する場合は、運用保守業者に運用業務として委託するのが一般的である。

各バックアップメディアごとのデータの書き込み作業と遠隔地保管の適否については、次のとおりである。

① 磁気テープ

磁気テープの場合は、バックアップ装置（音楽テープを録音・再生するときに使用するテープレコーダのようなもの）をサーバに接続し、テープをセットして、バックアップをとるという作業になる。

磁気テープそのものについては、持ち運びしやすく、遠隔地保管には最も適している。

② 光学ディスク

光学ディスクの場合は、ＤＶＤやブルーレイであれば容量的な問題も少なく、コストもかからない。

コンパクトで保管スペースを取らないため、遠隔地保管がしやすいメディアの一つである。

③ 外付けＨＤＤ

外付けＨＤＤの場合は、サーバに直接接続して使用するため、遠隔地に保管するためには、最低３台のＨＤＤが必要である。(遠隔地保管用(遠隔地送付用が送られてきたら、現に保管しているＨＤＤを送り返す)、バックアップ用、遠隔地送付用の３台)。コストも手間もかかるため、遠隔地保管にはあまり向いていない。

④　ストレージ装置

ストレージ装置の場合は、本体サーバと通信回線で結び、オンラインでリアルタイムにバックアップしていくことが容易であるため、毎日のようにバックアップが必要なデータを遠隔地保管する際に最も適しているメディアである。

ストレージ装置を遠隔地に置くことで解決できるが、ストレージ装置のハードウェア経費のほか、運用保守業務を委託することになるため、毎年度、かなりの運用経費がかかる。

《 バックアップを行うメディアの比較 》

比　較　項　目	運ぶことが可能なメディア（可搬型メディア）			運べないメディア（固定型メディア）
	磁気テープ	光学ディスク	外付けハードディスク／リムーバブルハードディスク	ストレージ装置
遠隔地での保管	◎	◎	△	×
システム全体のバックアップ／リカバリ	◎	×	△	◎
ファイル単位でのバックアップ／リカバリ	△	○	◎	◎
長期にわたるデータの保存	◎	◎	×	× （耐用年数は５年程度）
容量あたりの単価	◎	○	△	△
データの読み取りに係るランダムなアクセス	×	○	◎	◎

◎かなり優れている　○優れている　△普通　×劣っている

○　データ量が多いシステムでは「磁気テープ」が、個人用のパソコンデータをバックアップする場合は「光学ディスク」がよい。共に劣化しにくいため比較的長期間保存が可能である。

○　外付けＨＤＤやリムーバブルＨＤＤは、ここ数年、容量が増大しつつも価格が急落しているため、近年、主流となりつつある。テープと違って、要求するデータを瞬時にアクセスできるなど使い勝手がよい。４～５年で機器更新が必要となるが、価格が安くなっているため、それほど財政的な負担はかからない。

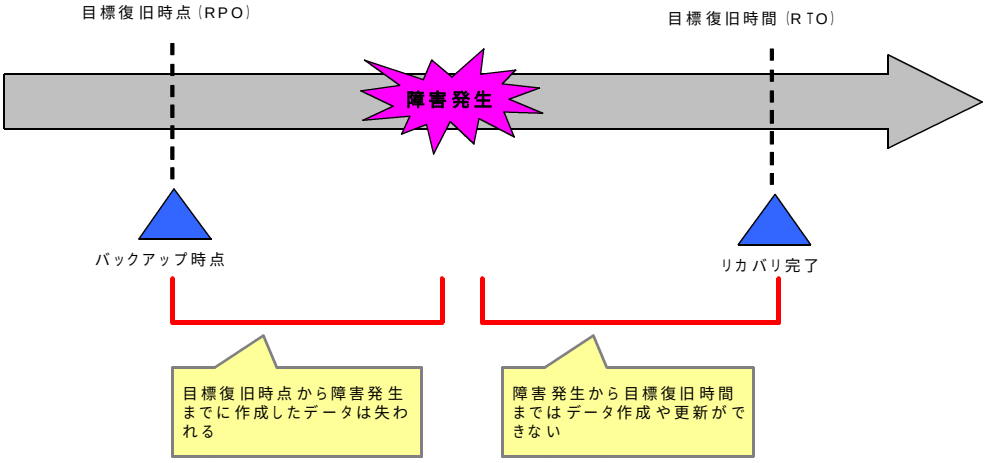
○　ストレージ装置はＨＤＤ同様、頻繁にリカバリしたり短時間でバックアップ／リカバリ処理を完了しなければならないときに有利である。ＨＤＤと異なるのは、大容量のデータの高速処理が可能であることと、本体サーバを通信回線で結び、オンラインで処理をすることができる点である。ただし、４～５年で機器更新が必要であることや運用経費などコストはかかる。

バックアップの頻度(周期)については、情報システムにより異なり、毎日バックアップを行う必要があるシステムもあれば、１週間単位、１ヵ月単位、１年単位で行うシステムもあることから、頻度(周期)については、業務の内容によって整理する必要がある。

その際、地震等の災害により、情報システムがダウンまたは使用不能となり、もう一度システムを再構築しなければならなくなった場合、バックアップの頻度（周期）が業務執行に重大な影響を及ぼすことについて、理解しておく必要がある。

このことについて、次図のとおり、データのバックアップ時点と障害発生時点、システムの復旧時点の関係を参考までに整理した。

障害によるデータや業務再開等の状況



本図は、目標復旧時点（ＲＰＯ：Recovery Point Objective）と目標復旧時間（ＲＴＯ：Recovery Time Objective）との関係を表したものである。

障害が発生すると、ＲＰＯから障害発生時点までの間に作成されたデータは失われてしまう。

また、障害発生時点からＲＴＯまでの間はデータの作成ができない。

つまり、この間の業務執行に損失が生じることになり、損失を最小限とするためには、ＲＰＯとＲＴＯの両方を限りなくゼロに近づける必要がある。

《 遠隔地保管の必要性 》

システムの区分	現在のバックアップデータの状況			遠隔地保管の必要性
道がバックアップデータを保有しているシステム	庁舎内に保管		磁気テープ及び光学ディスクで保管	現状メディアの遠隔地保管が必要
			上記以外のメディアに保管	磁気テープ及び光学ディスクへの移行による遠隔地保管が必要（情報システム診断で検討）
	庁舎外に保管	札幌市内	磁気テープ及び光学ディスクで保管	※ 現状メディアの遠隔地保管が必要
			上記以外のメディアに保管	磁気テープ及び光学ディスクへの移行による遠隔地保管が必要（情報システム診断で検討）
		札幌市外	メディアの種類は関係なし	現状のままで対策不要
道がバックアップデータを保有していないシステム	国や団体がデータを管理している			現状のままで対策不要
	バックアップそのものを行っていない			磁気テープ及び光学ディスクによる遠隔地保管が必要（情報システム診断で検討）

※ 運用業者等の耐震（免震）構造のデータセンターで保管している場合は、緊急に対策を講じる必要性は乏しいと考えられる。

以上のことから、ステップ１においては、できるだけ少ない費用で必要な措置が図られるよう、次のとおり取り組むこととする。

［データバックアップ対策の考え方］

○　現行のバックアップメディアを活かしたまま、遠隔地保管が容易である磁気テープと光学ディスクについて遠隔地保管を進める。

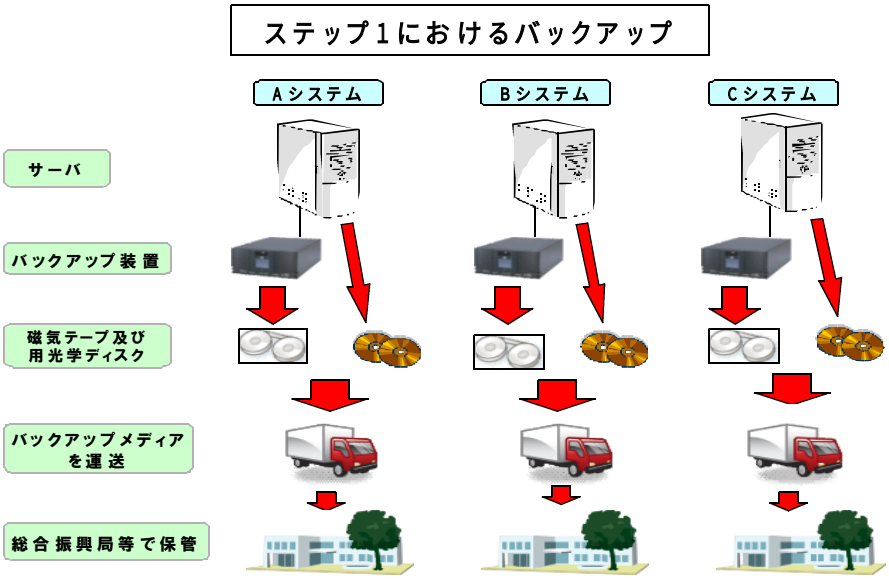
○　その他のメディアやバックアップを行っていないシステムについてはシステム更新時に行う「情報システム診断」において検討する。

※　なお、非常時優先業務の継続に不可欠な重要システムのバックアップメディアについては、復旧時間等の観点から、最良のメディア選択についてステップ２において再整理する。

(2) 対策の実施内容

データのバックアップメディアについては、原則として、道の各総合振興局等（石狩振興局を除く）が管理する建物で保管することとする。

保管に係る具体的な行動手順等については、後述の「５　ステップ１における行動計画」において示す。



５　業務アプリ等の保管及びデータのバックアップと保管対策に関する行動計画の策定

前記「3　業務アプリ等の保管対策」及び「4　データのバックアップと保管対策」を計画的・組織的に進めるため、対象となる情報システム担当課において、行動計画を策定する。

(1) 計画策定の対象システム

ステップ１において、遠隔地保管の対象であって、行動計画を策定する必要がある情報システムの範囲は、次のとおりである。

１　業務アプリ等

(1) 道が委託により開発または調達した情報システムで、システムの復元に必要な関係媒体を本庁舎、別館庁舎及び議会庁舎の執務室内において保管している情報システム

(2) 道が委託により開発または調達した情報システムで、上記関係媒体を札幌市内にある運用業者等の施設内（データセンター等）で保管している情報システムで、情報システム担当課が遠隔地保管を必要と認める情報システム

２　バックアップデータ

(1) 磁気テープ及び光学ディスクを本庁舎、別館庁舎及び議会庁舎の執務室内において保管している情報システム

(2) 磁気テープ及び光学ディスクを札幌市内にある運用業者等の施設内（データセンター等）で保管している情報システムで、情報システム担当課が遠隔地保管を必要と認める情報システム

※　「情報システム担当課が遠隔地保管を必要と認める情報システム」の考え方

- 保管先の建物の耐震（免震）性により判断する
- 保管先がデータセンターの場合は、本庁舎等よりも耐震（免震）性に優れていると考えられるが、近隣火災による延焼や隣接するビルの倒壊等による被害の可能性もあることから、総合的に判断する

(2) 行動計画書

行動計画を策定する必要がある情報システムの担当課は、５－(5)を参考にして、総合振興局等の保管場所を管理する担当課長等と協議の上、次の行動計画書を作成する。

バックアップメディア等の遠隔地保管に関する行動計画書

通し番号	○－○

システム名	○○○○システム					
システム担当部課名	○○部○○課					
保管先名	○○総合振興局共用書庫内保管庫					
保管するバックアップメディア等	種類	LTO	容量	200GB	数量	1巻
	種類		容量		数量	
	種類		容量		数量	
担当者名	A:システム担当課			B:総合振興局等		
	○○部○○課 情報システム担当者 主任 ○○ ○○ (内線:)			○○総合振興局○○部○○課 情報セキュリティ担当者 主任 ○○ ○○ (内線:)		

業務のプロセス	・原則として、次のスケジュールでデータのバックアップメディアの移送を実施する。 1:毎月○○日 ○○課 → ○○総合振興局 2:毎月○○日 ○○総合振興局 → ○○課 ・業務アプリのバックアップメディアは、システムの次期更新時まで、○○総合振興局で保管する。 ・保管中のバックアップメディアの保管状況について、定期的に確認する。(確認月:○月、○月)
目標レベル	バックアップメディアを総合振興局内で厳重に保管し、かつ、緊急時に確実に返送し、システムの復元に資すること。
移送訓練実施月	毎年○月

ﾁｪｯｸ	データのバックアップメディアの遠隔地保管に関する行動手順 ※行動手順を時系列で記入 ※手順を実施後、必要に応じ、左の欄をチェック	実行者

[備考]

(3) 行動原則

遠隔地保管の対象となる情報システムに係る業務アプリやデータのバックアップメディア（以下、「バックアップメディア等」という。）を、遠隔地に保管するための行動原則は、次のとおりである。

○　複数のシステムのバックアップメディア等を一括して送付するなど、遠隔地保管を 効果的・効率的に実施するため、原則として各部局単位で調整の上、行動計画を策定すること。

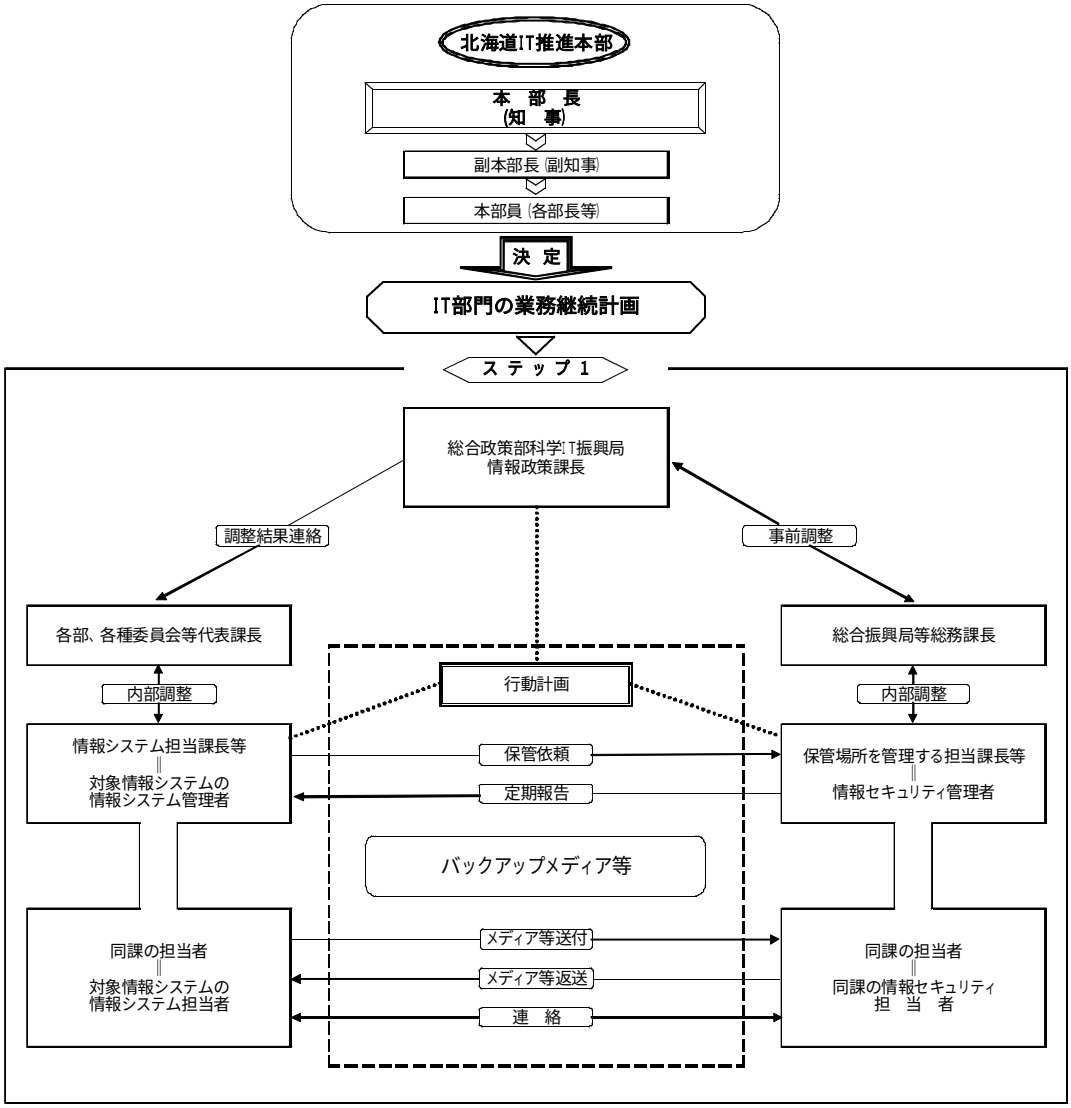
○　セキュリティ上のリスク分散及び業務の負荷分散を図るため、石狩振興局を除く13の総合振興局等において、遠隔地保管を実施すること。

○　保管は、総合振興局等内にある書庫等内の保管庫（ロッカー等）で行うこととし、入室管理、施錠管理等、セキュリティに万全を期すこと。

(4) 推進体制と役割分担

遠隔地保管を進める推進体制と役割分担は、次のとおりである。

①　バックアップメディア等の遠隔地保管における推進体制



② バックアップメディア等の遠隔地保管における役割分担

○ 総合政策部科学ＩＴ振興局情報政策課長

バックアップメディア等の保管対策を計画的・組織的に進めるため、行動計画全般を統括するとともに、各部局等の代表課長や総合振興局等の総務課長との調整を行う。

○ 各部・各種委員会等代表課長（以下、「各部等代表課長」という。）

全体を統括する情報政策課長や部局内の情報システム担当課長と調整を行う。

○ 情報システム担当課長等（情報システム管理者）

情報システム担当課長等は、北海道情報セキュリティ対策基準第７に定める情報システム管理者とする。

総合振興局等の保管場所を管理する担当課長等と協議の上、遠隔地保管に関する行動計画書を策定する。

また、遠隔地保管に関する業務の全部又は一部を補助させるため、あらかじめ担当者を指定し、その任に当たらせる。

○ 情報システム担当課の担当者（情報システム担当者）

遠隔地保管に関する業務の全部又は一部を行う。

○ 総合振興局等総務課長

保管場所を確保するため、総合振興局等における情報セキュリティ管理者と調整を行い、その結果を情報政策課長へ報告する。

○ 総合振興局等の保管場所を管理する担当課長等（情報セキュリティ管理者）

北海道情報セキュリティ対策基準第６に定める課長相当職とする。

情報システム担当課長等の遠隔地保管に関する行動計画書の策定に協力する。

また、遠隔地保管に関する業務の全部又は一部を補助させるため、あらかじめ担当者を指定し、その任に当たらせる。

○ 同担当課の担当者（セキュリティ担当者）

遠隔地保管に関する業務の全部又は一部を行う。

(5) 実施手順と送付方法

バックアップメディア等の遠隔地保管を行うための実施手順と送付方法は、次のとおりである。

① 各部等代表課長は、部局内の情報システム担当課長と調整の上、保管リストを作成し、情報政策課長に報告する。

② 情報政策課長は、総合振興局等総務課長に、各部局単位の保管リストを送付する。同総務課長は、保管場所を確保し、情報政策課長に報告する。

③ 情報政策課長は、各部等代表課長に保管先を連絡する。

④　情報システム担当課長は保管先となる総合振興局等の保管場所を管理する担当課長等（以下「総合振興局等担当課長」という。）に対し、バックアップメディア等送付のスケジュール等について協議を行う。

⑤　情報システム担当課長は、行動計画書を３部作成し、１部を自課で保管するほか、残りを１部ずつ保管先の総合振興局等担当課長及び情報政策課長に送付する。
　なお、行動計画書は非公開扱いとし、その管理については厳重に行うこととする。

⑥　情報システム担当課長は、当該業務を実施するにあたり、管理台帳を整備し、各手順の実施後に必要事項を記載する。
　管理台帳の様式は、別紙様式１－１（遠隔地保管台帳Ａ）を参考とすること。

⑦　情報システム担当課長は、バックアップメディア等を梱包した上に送付票（別紙様式２）を貼付し、専用ケース（アルミトランク）に格納して送付することとし、本庁舎地下収発室より貴重品扱いで託送する。

⑧　バックアップメディア等を保管する総合振興局等担当課長は、送付されたバックアップメディア等を梱包状態のまま保管し、情報システム担当課へ返送する場合も同状態のまま、貴重品扱いで託送する。

⑨　バックアップメディア等を保管する総合振興局等担当課長は、当該業務を実施するにあたり、管理台帳を整備し、各手順の実施後に必要事項を記載するとともに、保管状況について、定期的に確認を行い、その結果については、情報システム担当課長に対し報告を行うこととする。
　管理台帳の様式は、別紙様式１－２（遠隔地保管台帳Ｂ）を参考とすること。
　なお、定期的の考え方は、バックアップの頻度によるが、最低でも年２回以上とする。

⑩　行動計画を見直した場合は、各部局の代表課長を通じて、情報政策課長に報告する。

(6) 災害時の行動計画の取り扱い
　道が運用している情報システムが大地震等により損害を受けた場合、遠隔地保管しているバックアップメディア等に基づき、早期にシステムを復元しなければならないが、そのためには、どこに送付するか、どこで復元作業を行うか等、災害時における行動計画も別途必要となる。
　これについては、代替施設の確保など、道全体の業務継続計画に係ることから、ステップ２以降で検討することとする。

別紙様式１－１

遠　隔　地　保　管　台　帳　A

情 報 シ ス テ ム 名　[　　]

情報システム担当課名　[　　]
総合振興局等担当課名　[　　]

保管するバックアップメディア等

種類		容量		数量		備考	
種類		容量		数量		備考	
種類		容量		数量		備考	

番号	発送連絡		到着連絡		返送連絡		到着連絡		定期確認		
	連絡年月日	担当者	受理年月日	担当者	受理年月日	担当者	連絡年月日	担当者	受理年月日	状態	担当者
	①		②		③		④		⑤		

※　遠隔地保管台帳Ａ記載時点

①　総合振興局等担当課への発送時
②　総合振興局等担当課からの到着連絡受理時
③　総合振興局等担当課からの返送連絡受理時
④　返送分バックアップメディア等の到着連絡時
⑤　定期確認報告受理時

別紙様式１－２

遠　隔　地　保　管　台　帳　B

情 報 シ ス テ ム 名　[　　]

情報システム担当課名　[　　]
総合振興局等担当課名　[　　]

保管するバックアップメディア等

種類		容量		数量		備考	
種類		容量		数量		備考	
種類		容量		数量		備考	

番号	発送連絡		到着連絡		定期確認			返送連絡		到着連絡	
	受理年月日	担当者	連絡･保管年月日	担当者	確認･報告年月日	状態	担当者	連絡年月日	担当者	受理年月日	担当者
	①		②		③			④		⑤	

※　遠隔地保管台帳Ｂ記載時点

①　情報システム課からの発送連絡受理時
②　情報システム課への到着連絡及び保管時
③　定期確認報告時
④　返送連絡時
⑤　返送分バックアップメディア等到着連絡受理時

別紙様式２

バックアップメディア発送票

部　　課　　名	
シ　ス　テ　ム　名	
内　　容	
発　送　年　月　日	
返 送 予 定 年 月 日	

(7) 行動計画に基づく訓練の実施

総合振興局等担当課から情報システム担当課へのバックアップメディアの返送は、本行動計画上の定例業務であるが、実際の災害時における対応を考慮すれば、緊急性を意識して行うことも必要と考えられる。

このことから、年に１回は定例の返送業務を訓練として位置づけ、より迅速に行動できるよう目標時間を定めて実施する。

なお、実施月については、情報システム担当課長と総合振興局等担当課長との協議により、行動計画書中に記載することとする。

６　今後の課題等

今回のステップ１は、札幌市内に大きな被害をもたらすような大地震を想定し、仮に稼働中の情報システムが消失したとしても、確実に復元し再稼働できる仕組みを整理したが、今回の仕組みでは、短期間で再稼働するという業務継続本来の目的を達成できるレベルには至っていない。

このことを成し遂げるためには、今後、ネットワークや情報システムのあり方を見直し、少ない投資で最大限の効果が得られるよう「最適化」の考え方を取り入れながら、新たな仕組みを構築していく必要がある。

具体的な検討はステップ２・３で行うことになるが、例えば、道庁行政情報ネットワーク（庁内ＬAN）においては、道庁内のパソコンの多くが情報システム（サーバ）と接続しデータのやりとりを行っているため、災害により、本庁とデータセンターとを結ぶ回線やサーバ等の機能が停止すると、総合振興局等、道のすべての機関において、庁内ＬＡＮ上を動く情報システムが使えなくなり、行政サービスに多大な影響を及ぼす恐れがある。

このネットワークをより強固なものとするための抜本的な対策を講じるまでの間は、情報通信の機能及びそれに依存する基幹的業務等が災害時に大幅に制約される事態においてもなお、各機関の業務を適切に遂行できる対策を各情報システムごとに検討を進めていく必要がある。

ＩＴ部門の業務継続計画

ステップ１

「情報インフラ等の脆弱性の把握と当面の対策」

平成23年３月

北海道総合政策部科学ＩＴ振興局情報政策課
情報企画グループ
〒060-8588 札幌市中央区北３条西６丁目
TEL：(011)204-5170