ＩＣＴ部門の業務継続計画

ステップ３

～業務継続能力を強化するための対策～

平成３０年３月

（令和６年４月改定）

北　海　道

第１章　ＩＣＴ部門の業務継続計画の目的と緊急時の対応

第１部　ＩＣＴ部門の業務継続計画の目的と取組範囲

道では、札幌市に集中している情報通信ネットワークや情報システムの中枢機能が大地震等によって損害を被る事態に備え、これらの情報インフラを守り、かつ、災害時に優先度の高い業務システムの機能を維持・継続するために必要な措置を定める「ＩＣＴ部門の業務継続計画（ＢＣＰ ＝ Business Continuity Plan：ビジネス・コンティニュイティ・プラン。以下「ＩＣＴ－ＢＣＰ」という。）」を平成22年度から段階的に策定し、情報システムを災害から守るハード面の整備や迅速に復旧作業を行うための体制・手順等の計画策定といったソフト面での対策などの取組を進めてきた。

こうした中、本庁舎の免震工事が完了したことなどを受け、平成29年３月「北海道庁業務継続計画」が改定されたところであり、今般、この改訂内容とともに、ＩＣＴを取り巻く社会環境の変化などを踏まえ、「ＩＣＴ－ＢＣＰステップ３」を策定する。

ＩＣＴ－ＢＣＰの策定経緯

ステップ１（H23.3策定）
＜主な内容＞
本庁舎等が被災し、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。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。
・サーバ、パソコン等の転倒防止対策
・業務アプリ、データ等の保管対策　　等

ステップ２（H24.3策定）
＜主な内容＞
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。
・重要システムの選定
・サーバのデータセンタへの移設
・「復旧行動計画」、「代替行動計画」の策定　等

ステップ３（今回策定）
＜主な内容＞
「北海道庁業務継続計画」が改訂されたことなどを踏まえ、想定災害の追加等の見直しを実施。
・重要システムの追加、見直し
・情報セキュリティ対策に関連する取組の追加
・「復旧行動計画」、「代替行動計画」の記載内容の見直し
（振興局等の被災等の対応や代替施設の確保等を追加）　等

１　策定の趣旨

大地震等が発生すると、これまで当たり前のように使用してきた施設や、電気やガス、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に陥る恐れがある。

こうした際には、道の庁舎も被災し、行政活動に大きな制約を受ける恐れがあるが、道民の生命、財産、経済活動等を守るためには、道庁の業務や機能をあくまでも継続していくことが必要である。

こうした道の業務を進める上で、情報システムは平常時、災害時を問わず、重要な役割を担っているが、災害が発生した際には、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などにより、情報システムが停止してしまうことも考えなければならない。

このような事態に備え、予め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として、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「北海道庁業務継続計画」（道庁ＢＣＰ）

業務継続計画（ＢＣＰ）は、人員、資機材、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、応急業務及び継続の優先度の高い通常業務（以下「非常時優先業務」という。）を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。

道では、札幌市内に大きな被害をもたらす大地震等によって、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、その業務の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「北海道庁業務継続計画」（以下、「道庁ＢＣＰ」という。）を策定している。（平成 23 年３月策定、平成 29 年３月改定、令和２年３月改定）

道庁ＢＣＰにおいては、業務継続の基本方針を次のとおり定めている。

＜業務継続の基本方針＞

⑴　道民の生命・身体・財産を保護し、被害を最小限にとどめるため、災害応急対策業務を中心に、非常時優先業務※を最優先に実施する。

⑵ 非常時優先業務を継続実施できるよう、必要となる人員、資機材、庁内相互の連携体制等を確保するため、業務継続の優先度の高い業務以外の通常業務については、一時的に休止・縮小する。

⑶ 業務継続の優先度の高い業務以外の通常業務は、非常時優先業務に影響を与えない範囲で、順次再開する。

※非常時優先業務　……　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（注）及び継続の優先度の高い通常業務

（注）応急業務　……　「北海道地域防災計画」（災害対策基本法第 40 条）等や各部局等で整備している「災害対策実施要領」等（北海道災害対策本部運営要領３の⑴）に基づいて実施する「災害応急対策業務」及び早期実施の優先度が高い災害復旧・復興業務等

３　ＩＣＴ－ＢＣＰの策定方針

ＩＣＴ－ＢＣＰでは、道庁ＢＣＰにおいて選定された「非常時優先業務」を遂行するために不可欠な情報システム（ネットワーク含む）を「重要システム」と位置づけ、これらシステムについて、被害の最小化、迅速な復旧、代替手段の確保に向けた体制を整備するために策定するものである。

（重要システム：災害時においても止めることができないシステムであり、仮に止まることがあったとしても、他のシステムより優先して復旧に努めなければならないシステム。）

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いるため、これを失うと、元の状態に戻すのに膨大な時間と費用と労力をつぎ込まざるを得なくなることから、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る。

また、道民や企業に関わる重要な情報を消失させると、緊急対応や復旧にも大きな支障が出るため、情報を安全に保持するための十分な備えが平常時から必要である。

災害が発生したときにどのように行動するかなどをマニュアル化し、訓練を重ねて迅速・的確に行動できるようにしておくとともに、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。

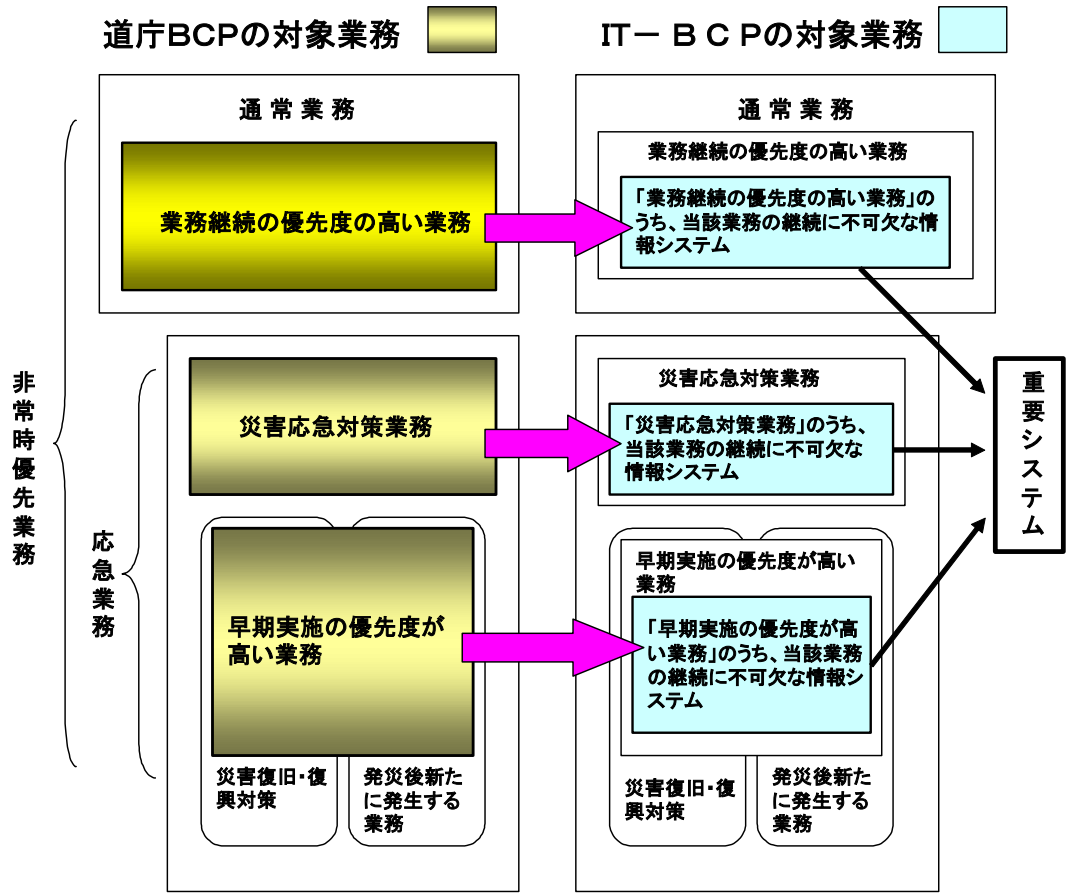
ＩＣＴ部門の業務継続計画は、こうした考え方に基づき策定していくこととする。

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、本庁舎等の周辺整備及び営繕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。
万全な情報セキュリティ対策	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、情報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しておくことが対策の前提となる。

道庁BCP（危機対策課）とIT－BCP（情報政策課）との関係（業務範囲）



※重要システムについては、Ｐ９を参照

４　想定する災害

「道庁ＢＣＰ」が想定している、地震や洪水により想定される被害等は、次のとおりである。

(1) 想定する地震

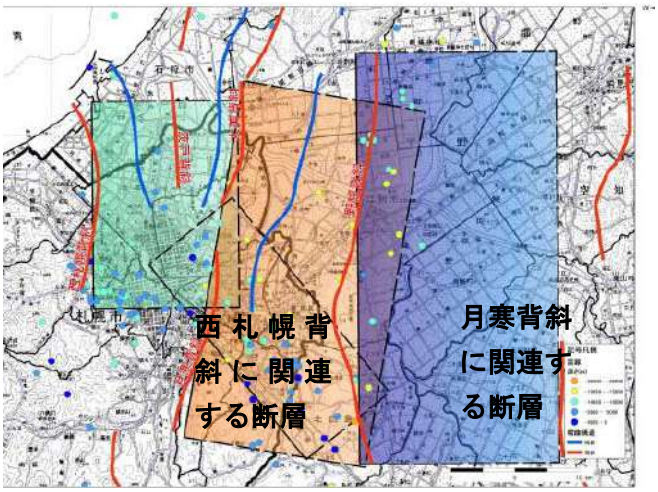
道庁ＢＣＰで想定する地震は、北海道防災会議地震専門委員会で、「北海道の想定地震」として決定された次の「３つの伏在活断層による札幌市直下型地震」とする。

① 野幌丘陵断層帯
② 月寒背斜に関連する断層（月寒断層）
③ 西札幌背斜に関連する断層（西札幌断層）

	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%）

※以下掲載の図及び表は札幌市防災会議の資料から抜粋

（３つの伏在活断層）



（本庁舎周辺の震度分布図）

※　３つの断層による地震の震度を重ね合わせ、最大震度を表した分布図

＜主な施設の震度＞

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	６弱
道民活動センタービル（かでる２・７）	６強

(2)　札幌市直下型地震の被害想定

ア 建物被害

	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

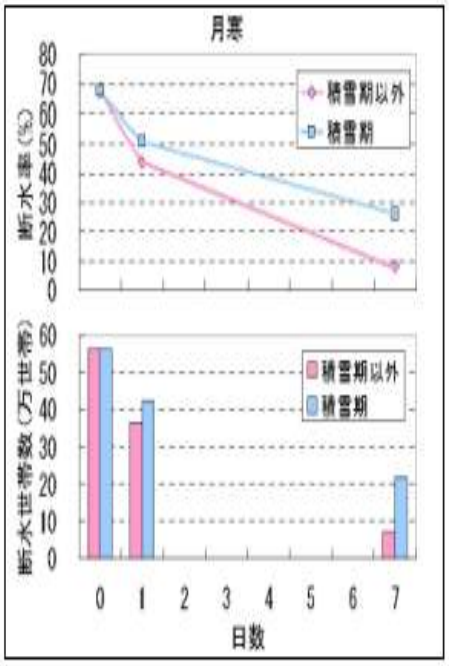
イ 人的被害　（単位：人）

		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

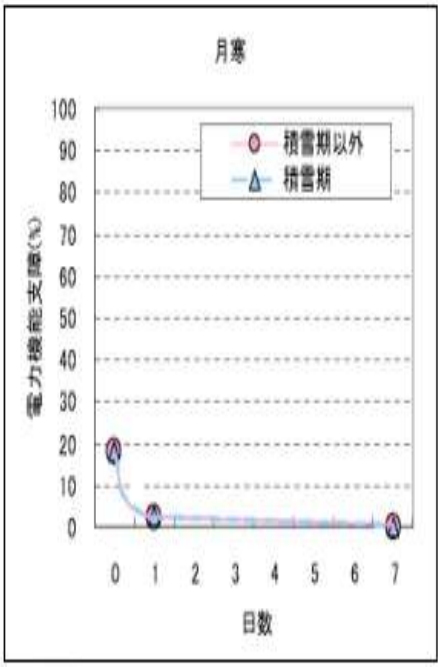
※　冬：発災後２時間以内に救出されない場合に凍死すると仮定したもの

ウ ライフライン被害（月寒断層による地震の場合）

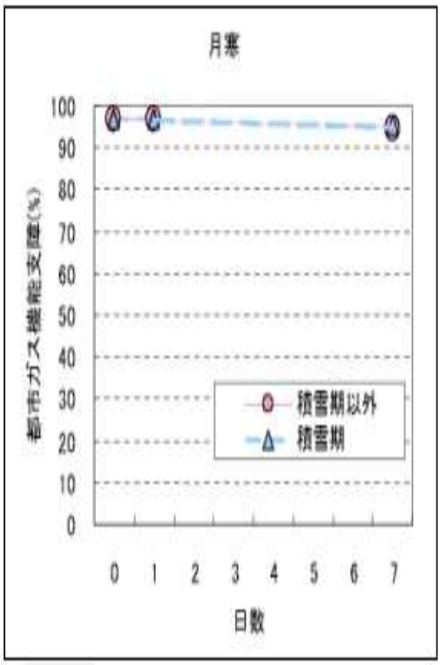
上　水　道



電　　力



都市ガス



(3)　想定する洪水

道庁ＢＣＰで想定する洪水は、札幌市の洪水ハザードマップにより、本庁舎及び別館庁舎周　辺は０．５ｍ未満の浸水深とする。

（本庁舎周辺の洪水ハザードマップ）

(4)　想定する大規模停電

道庁ＢＣＰで想定する大規模停電の期間は「大規模災害発生時における地方公共団体の業務継続の手引き」（平成２８年２月内閣府（防災担当））に基づき、１週間程度とする。

※「大規模災害発生時における地方公共団体の業務継続の手引き」５８ページ

『・・・停電の長期化に備え、１週間程度は災害対応に支障がでないよう準備することが望ましい。』

５ 重要システムの範囲

道には、本庁舎等に入っている部署で管理・運用している情報システムが約 200 システムあるが、その内、「非常時優先業務」を遂行するために不可欠な「重要システム」は次の 25 システムとする。

重 要 シ ス テ ム 一 覧

No.	部局名	システム名	災害時に求められる機能、用途
1	総務部	防災情報システム	北海道地域防災計画で定める防災情報の伝達、被害状況の収集・報告
2	総務部	震度情報ネットワークシステム	道内の震度情報を収集し気象庁に報告して広く一般に公開
3	総務部	原子力防災ネットワークシステム	国、関係町村、原子力事業者などの防災関係機関との原子力防災に関する情報の収集及び連絡
4	総務部	道税総合情報処理システム	道税の減免、徴収猶予等の業務の実施
5	総務部	人事給与システム	職員の適正な人事管理、行政サービスの継続的な提供等
6	総務部	総合文書管理システム	公文書の作成・決定・施行・保存等
7	総合政策部	北海道総合行政情報ネットワーク（防災回線）	道民の生命や財産等を守るために市町村等と災害に関する様々な情報の収集や連絡
8	総合政策部	行政情報コミュニケーションシステム（北海道公式ｳｪﾌﾞｻｲﾄ）	災害広報の実施（ホームページの更新・閲覧）
9	総合政策部	行政情報コミュニケーションシステム	電子メール、電子掲示板、共有ドライブ等、全庁の業務上不可欠なサービスの提供
10	総合政策部	道庁行政情報ネットワーク（庁内ＬＡＮ）	行政情報コミュニケーションシステムや財務会計トータルシステム等の重要システムの運用（道の情報通信の基盤となるネットワーク）
11	総合政策部	総合行政ネットワーク（ＬＧＷＡＮ）	地方公共団体間を相互に接続するネットワーク
12	総合政策部	北海道電子自治体共同システム	インターネットによる行政手続（申請・届出サービス等）の確保
13	総合政策部	北海道庁宛名連携サーバ	個人番号利用事務に係る重要システムとの連携確保
14	総合政策部	北海道自治体情報セキュリティクラウド	災害時における万全なセキュリティ対策の実施
15	保健福祉部	生活保護電算処理システム	被保護者の不利益とならないよう業務の継続
16	保健福祉部	身体障害者手帳発行等システム	避難所の体制整備、避難中の障がい者数把握、台帳損失市町村への情報提供、手帳紛失者の手帳所持証明等
17	建設部	防災情報共有化システム	河川情報、道路気象情報等を庁内、関係機関で共有
18	建設部	道路管理情報システム	道道の被災状況を基に規制情報等を提供
19	建設部	道路気象情報システム	道道の気象状況を収集し、関係者に情報提供
20	建設部	治水ＧＩＳシステム	災害時の河川や管理施設の状況把握
21	出納局	財務会計トータルシステム	財務会計事務全般の確保
22	企業局	財務会計システム	企業局における財務会計事務全般の確保
23	道立病院局	財務会計・固定資産管理システム	道立病院全体の財務会計事務等の確保
24	教育庁	教育局給与情報オンラインシステム	被災時においても円滑な教育活動の確保（全道公立学校教職員の任用状況等管理等）
25	教育庁	教育庁人事給与システム	職員の適正な人事管理等による行政サービスの継続的な提供等

６　ＩＣＴ－ＢＣＰの目的と取組の範囲

災害時にＩＣＴ部門の業務を継続するには、重要システムを災害から守るためのハード面の対策を強化していくことが重要である。

しかしながら、ハード面の対策を強化したとしても、重要システムの停止や消失のリスクをゼロにすることは困難であるため、そのような事態に陥ったとしても速やかに復旧あるいは代替の措置を講じることができるよう、ソフト面の対策として災害時の対応を示す行動計画を事前に策定しておくことが重要である。

また、行動計画の策定だけでなく、スキル面の対策として、行動計画の内容をあらかじめ訓練を通じて職員が経験しておくとともに、行動計画自体を実地検証し、必要に応じて改善を加えることにより、緊急時においても迅速かつ的確な判断や行動ができるようにしておくことが重要となる。

非常時優先業務の遂行にあたっての目標は

災害時において適切に業務を継続できる能力を高めること （業務継続能力の強化）

であり、この実現にあたっては、

情報システムの停止も含め、事前に起こり得る事態を可能な限り洗い出し、その対処方法について行動計画に反映するとともに、訓練を通して職員の対応能力向上と行動計画の検証・改善に努めること

が重要である。

また、市町村のＩＣＴ部門の業務が継続できない場合、被災者の救出・救援活動や民間事業者の経済活動に著しい支障を来すため、ＩＣＴ部門の業務継続に関する事前の対策は、道内市町村においても必要であることから、道としてＩＣＴ－ＢＣＰを策定する市町村に対して支援を行うことも重要である。

ICT－BCPの目的と取組について

危機に備え、迅速に対処できる組織づくり

－災害時に適切に業務を継続できる対応能力を高めることが重要－

目　標

業務継続能力の強化

重要システム等の被害の最小化や迅速な復旧、代替手段の確保・利用

ハード	ソフト	スキル
事前対策	**行動計画**	**対応能力**
システムを災害から守るためのハード面の整備	体制と役割分担、代替手段への切替や復旧作業に係る手順等の整備	訓練による人・組織の危機対応能力の向上

災害時には、ハード・ソフト・スキルの強化が有効

基本姿勢

情報システムの停止も含め、事前に起こり得る事態を可能な限り洗い出し、その対処方法について行動計画に反映するとともに、訓練を通して職員の対応能力向上と行動計画の検証・改善に努める

災害時の業務継続は道だけではなく市町村も重要

市町村におけるICT－BCP策定の取組を促進・支援（ハード面、ソフト面、スキル面）

７　ＩＣＴ－ＢＣＰの取組

ＩＣＴ－ＢＣＰによる具体的な取組は、次のとおりである。

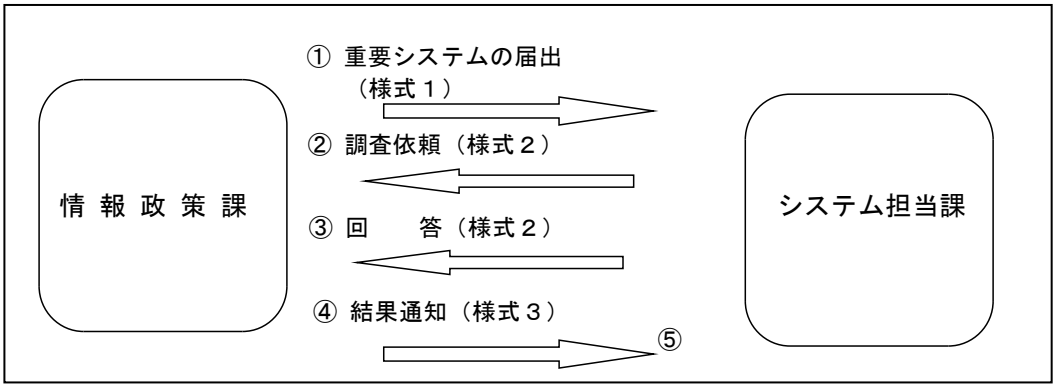
ＩＣＴ－ＢＣＰの主な取組

災害時の対応		・ ＩＣＴ－ＢＣＰの発動 ・ ＩＣＴ－ＢＣＰの発動期間中の対応 ・ ＩＣＴ－ＢＣＰの終結
事前対策	ハード面	・ バックアップデータ等の遠隔地保管対策 ・ 重要システムのサーバを守る対策　など
	ソフト面	・ 重要システムの復旧に係る行動計画の策定（「復旧行動計画」） ・ 重要システムに代わる代替手段の行動計画の策定（「代替行動計画」）
	スキル面	・ 重要システムに係る訓練計画の策定 ・ 重要システムに係る訓練の実施
市町村への支援		・ 市町村のＩＣＴ－ＢＣＰ策定に対する支援

８　重要システムの見直し（追加等）を行う場合の取扱い

新たに情報システムを構築した場合や制度改正等に伴うシステム改修等により、情報システム担当課において当該システムを新たに重要システム（非常時優先業務の遂行に不可欠な情報システム）とする手続は、次のとおりとする。

［新たに重要システムとする場合の手続の流れ］



＜手続の流れ＞

① 情報システム担当課の情報システム管理者は、様式１により情報政策課長に対し、重要システムの届出を行う。

② 情報政策課長は、情報システム管理者に対し、当該システムの現状等に係る調査票（様式２）の作成を依頼する。

③ 情報システム管理者は、調査票（様式２）を作成し、情報政策課長に提出する。

④ 情報政策課長は、調査票の内容について情報化推進アドバイザーに書面による診断を依頼し、診断後、その結果を記載した診断票（様式３）を情報システム管理者に通知する。

⑤ 情報システム管理者は、診断結果を踏まえ、今後の対応についての検討を行うとともに、速やかに「第２部　ソフト面に係る取組」を実施し、この取組の実施後、「第３部　スキル面に係る取組」を実施する。

［様式１　…　巻末様式集　３－１］
［様式２　…　巻末様式集　３－２］
［様式３　…　巻末様式集　３－３］

第２部　災害時の対応

ＩＣＴ－ＢＣＰの発動、発動期間中の対応、ＩＣＴ－ＢＣＰの終結に係る行動原則は、次のとおりである。

（災害時における行動原則）

■　札幌市内に大きな地震等が発生した場合、重要システム担当課（P9 参照）の情報システム管理者は、直ちに復旧行動計画（P28～31 参照）に基づく初動対応を行う。
■　地震の規模が震度６弱以上の場合は直ちに、震度５強以下の地震及びその他の災害等が発生した場合において、災害の状況が重要システムの使用や維持を困難にする重大なものと総合的に判断される場合に、イノベーション推進監はＩＣＴ－ＢＣＰの発動を宣言し、速やかに庁内に周知する。
■　発動宣言がなされた場合、重要システム担当課の情報システム管理者は、「復旧行動計画」又は「代替行動計画」（P32～34 参照）若しくはその両方を速やかに実行する。
■　重要システム以外の情報システムについては、一時的に（おおむね発災後から 30 日まで）休止・縮小する。
■　発動宣言後、情報政策課長は重要システムの被災状況等の情報を収集・分析し、イノベーション推進監に報告するとともに、パソコン予備機や回線容量などのＩＣＴ資源の庁内配分、光回線などの復旧工事に係る優先順位の調整など、ＩＣＴに関する総合的・緊急的な庁内調整を行う。
■　重要システムの復旧が進み、総合的・緊急的な庁内調整を要しなくなったものと判断される場合、イノベーション推進監はＩＣＴ－ＢＣＰの終結を宣言する。
■　ＩＣＴ－ＢＣＰの終結宣言を受け、情報政策課長は、庁内に周知するとともに上記の総合的・緊急的な庁内調整業務を終了し、平常時の業務体制に復帰する。

１　ＩＣＴ－ＢＣＰの発動

ＩＣＴ－ＢＣＰの発動宣言は、地震の規模に関する速報（第一報）で、震度６弱以上の場合は、直ちに行うものとする。

震度５強以下の地震及びその他の災害等の場合においては、庁舎の被災状況、重要システムの稼働状況、機器の破損状況、ライフラインの状況などから見て、重要システム自体に復旧対応や代替対応を必要とする被災が生じていることが疑いようがない又は災害発生に伴う人員や物資、ライフラインの制約から、重要システムの使用や維持は早晩困難になると考えざるを得ない状況であれば、発動宣言を行うこととする。

災害発生から発動宣言に至るまでの対応は、次のとおりである。

（重要システム担当課の対応）
① 札幌市内に大きな地震（おおむね震度５弱以上）や洪水等が発生し、重要システムの使用、維持が困難になる恐れがある大規模な災害が発生した場合、重要システム担当課の情報システム管理者は、直ちに復旧行動計画に基づく初動対応を行い、職員等の安否確認、重要システムの状況把握を行うとともに、当該情報を情報政策課ＩＣＴ－ＢＣＰ班へ報告する。
② なお、重要システム担当課の情報システム管理者は、被災状況などの緊急性に応じ「復旧行動計画」又は「代替行動計画」、若しくはその両方を発動宣言を待つことなく実行する。

（情報政策課の対応）
①　札幌市内に大きな地震（おおむね震度５弱以上）や洪水等が発生し、重要システムの使用、維持が困難になる恐れがある大規模な災害が発生した場合、情報政策課長は、直ちに、ＩＣＴ－ＢＣＰ班（班長：課長補佐（情報システム））を情報政策課内に設置する。
②　情報政策課ＩＣＴ－ＢＣＰ班は、地震の規模が震度６弱以上の場合は、その情報とその時点で確認できている災害情報と併せ、速やかに、情報政策課長及びイノベーション推進局長を経て、イノベーション推進監に報告する。
　震度５強以下の地震及びその他の大規模災害等の場合は、重要システム担当課の情報をとりまとめるとともに、関係部等から得られた災害情報と併せ、これら被災状況等を情報政策課長及びイノベーション推進局長を経て、イノベーション推進監に報告する。
③　イノベーション推進監は、震度６弱以上の地震の場合は直ちに、震度５強以下の地震及びその他の大規模災害等の場合は災害状況が重要システムの使用や維持を困難にする重大なものと総合的に判断した場合に、ＩＣＴ－ＢＣＰの発動を宣言する。
④　情報政策課ＩＣＴ－ＢＣＰ班は、発動宣言を速やかに庁内に通知する。

《札幌市内に大きな地震等が発生したときに想定される業務の流れ》

震度６弱以上の地震発生	**・震度５弱または５強の地震発生** **・その他、洪水等重要システムの使用や維持が困難になる恐れがある災害の発生**
第３非常配備　「災害対策本部設置」	第２非常配備　「災害対策連絡本部設置」

災害対策本部設置に伴う所掌事務（ＩＣＴ関連を抜粋）		災害対策連絡本部設置に伴う所掌事務（ＩＣＴ関連を抜粋）
危機管理班	・災害情報の収集・提供 ・予報（注意報含む）、警報及び情報等の受理伝達 ・災害の状況、対策措置状況等の収集及び報告など	災害対策本部の所掌事務に準ずる
総　務　班	・道有財産の被害調査及び復旧対策	
総合政策班	・災害広報の実施 ・交通施設等の被害状況の情報収集 ・災害時における通信手段の確保	
建　設　班	・道路の交通不能箇所の調査及び交通の確保 ・河川、空港、港湾、海岸等の被害調査及び応急措置など	

重要システム担当課は発災後、直ちに復旧行動計画の初動対応を実施

政策課ＩＣＴ－ＢＣＰ班	重要システム担当課
・地震の規模に関する情報の確認 ・危機管理班や総務班等からの情報確認 ・重要システム担当課からの情報確認 ※　震度６弱以上の場合は速やかに情報政策課長とイノベーション推進局長に報告	・安否確認（職員・家族） ・重要システムの被害状況の把握 ・被害状況等の報告

報告

情報政策課・イノベーション推進監　内容確認

報告、総合的判断の補佐

イノベーション推進監　発動に関する総合的判断

ＩＣＴ－ＢＣＰの発動宣言

システム被災の場合発動宣言を待つことなく実行

・「復旧行動計画」又は「代替行動計画」、若しくはその両方を速やかに実行

２　ＩＣＴ－ＢＣＰの発動期間中の対応

ＩＣＴ－ＢＣＰの発動宣言がなされた後の重要システム担当課の対応は、次のとおりである。

（重要システム担当課の対応）
① 重要システム担当課の情報システム管理者は、ＩＣＴ－ＢＣＰの発動宣言がなされた場合は、被災状況を踏まえつつ、「復旧行動計画」又は「代替行動計画」、若しくはその両方を速やかに実行する。
② 重要システム担当課は、次の事項について情報政策課ＩＣＴ－ＢＣＰ班へ適宜、報告を行う。
・重要システムの被害状況
・重要システムの復旧の見通し
・代替手段（手作業等）への切替時期
・重要システムによる業務再開（代替手段の終了）の時期など
③ 重要システム担当課は、重要システムの復旧に関して庁内調整が必要とされるものがある場合は、その内容を情報政策課ＩＣＴ－ＢＣＰ班へ連絡する。
④ 上記及びその他庁内調整を行う必要があるものの取扱いについては、情報政策課の指示に従う。

＜ＩＣＴ－ＢＣＰ発動期間中の留意事項（重要システム担当課）＞

・ 行動計画（復旧・代替）に基づいて対応する。
・ 個別の対応項目ごとにチェックを入れ、目標処理時間に対する実際の処理時間を記録する。
・ 想定外の事態が発生した場合は、訓練によって得られた知見を活かし、迅速かつ適切に対応するとともに、処理・措置内容を記録する。

災害時は、重要システムの維持や復旧に必要な物資の調達が交通網の遮断等により困難となる場合があることや、配線工事等に携わる関係業者が被災するなどの理由により必要な人員を確保できないなどといった事態が起こる場合があることから、情報政策課ＩＣＴ－ＢＣＰ班はこれら情報の把握に努めるとともに、適宜、必要な措置を講じ、関係部署に通知することが重要となる。

発動宣言がなされた後の情報政策課の対応は、次のとおりである。

（情報政策課の対応）
① 情報政策課ＩＣＴ－ＢＣＰ班は、重要システムの被災状況等の情報を収集・分析し、情報政策課長に報告する。
② 情報政策課長は、ＩＣＴ－ＢＣＰの発動期間中、次の事項を統括することとし、情報政策課ＩＣＴ－ＢＣＰ班は、情報政策課長の指示により、総合調整を行い、必要な措置について、重要システム担当課へ通知する。
・パソコンやサーバ、通信機器、回線容量等の庁内配分に関すること
・防災無線や庁内ＬＡＮをはじめ重要システムに係る回線等の復旧工事の優先順位等の調整に関すること
・その他ＩＣＴに関する緊急的な庁内調整に関すること
③ 情報政策課長は、これらの内容を適宜、イノベーション推進局長及びイノベーション推進監に報告する。

なお、重要システム以外の情報システムについては、一時的に（おおむね、発災後から 30 日まで）休止・縮小する。

３　ＩＣＴ－ＢＣＰの終結

イノベーション推進監は、すべての重要システムによる業務再開のめどが立ち、情報政策課による総合的・緊急的な庁内調整を要しなくなったものと判断される場合、ＩＣＴ－ＢＣＰの終結を宣言する。

情報政策課長は、終結宣言を速やかに庁内に周知し、また、ＩＣＴ－ＢＣＰ班は、総合的・緊急的な庁内調整事務を終えて、平常時の業務体制に復帰する。

＜ＩＣＴ－ＢＣＰの評価について＞

ＩＣＴ－ＢＣＰがどのように機能したかは、今後の災害対応に極めて重要となるため、災害後の適切な時期に、重要システム担当課に対し評価に関する調査を実施する。

調査内容や方法等については、情報政策課から別途、通知する。

第３部　ＩＣＴ－ＢＣＰの準用

第２部においては、札幌市内に大きな被害をもたらす直下型の大地震や本庁舎周辺における洪水発生等をリスクとして想定したが、重要システムの使用や維持を困難にする重大な被害が発生が見込まれるその他の災害としては、次のようなものが想定される。

＜ＩＣＴ－ＢＣＰ発動が想定されるリスク＞

（本庁舎周辺におけるリスクを対象）

① 大規模な火災による情報通信施設や機器等の損壊及び通信の途絶や通信障害等 ② 大規模な停電 ③ 台風、落雷、水害等による情報通信施設や機器等の損壊及び通信の途絶や通信障害等 ④ テロ等による本庁舎等や通信施設等の破壊　など

また、ＩＣＴ－ＢＣＰの目的は、大規模災害が発生した際における重要システムの使用や維持を図るためのものであることから、

・本庁と総合振興局、振興局等を結ぶ通信ネットワークの大規模障害

・総合振興局、振興局等の庁舎が大地震や洪水等で被災

などといった、重要システムの使用に支障が生じている、あるいは、使用に支障が生じる恐れがある場合においても、影響の大きさや復旧見込等を総合的に判断したうえで、ＩＣＴ－ＢＣＰを発動して対応するものとする。

第２章　ハード面・ソフト面・スキル面の平常時からの事前対策

第１部　ハード面に係る取組

（取組の基本的な考え方）

■ 本庁舎等が大きく損壊するような大きな災害時においても行政サービスを継続するため、重要システムの業務ソフトウェアやデータの遠隔地保管を進める。
■ 非常時優先業務の遂行に不可欠な情報システムである重要システムについては、災害時においてもこれを維持・継続するために必要な建物構造や電源設備等の水準を示し、この水準を満たす施設への機器の移設等を進める。

１　重要システムのデータや業務ソフトウェア等の保護対策

執務室内で保管している業務ソフトウェア等やデータは、本庁舎等が大きく損壊すると、その全部又は一部が消失する恐れがあるが、これらの情報インフラの中には、購入又はリースすること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。

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（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）
ソフトウェア	・業務ソフトウェア ・市販のソフトウェア	・業務ソフトウェアについては、道しか保有していないものもあり、消失するとバックアップをとっていない限り復元は困難 ・市販のソフトウェアは、購入・リースにより復元可能（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

(1) 業務ソフトウェア等の保管対策

ア　対策の考え方

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適切に保管され、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、別の業者により新たなハードウェア上でシステムを復元・稼働させることは可能である。

［業務ソフトウェア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、業務ソフトウェア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。

イ　対策の実施内容

(ｱ) 契約等による関係媒体提出の義務化

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（又は業務処理要領）にシステム復元に必要な関係媒体等を必ず明記し、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があり、常に最新バージョンの成果物を求める必要があるため。）

・ 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）等の外部媒体もしくはメディア
・ 道が開発した業務アプリのＣＤ－ＲＯＭ等の外部媒体もしくはメディア
・ 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）

(ｲ) 関係媒体の遠隔地保管に係る実施方法

契約書（又は業務処理要領）に明記された成果物のうち、前記(ｱ)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。

なお、保管に係る具体的な行動手順等については、後述の「(3) 業務ソフトウェア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」において示す。

(2) データのバックアップと保管対策

ア　対策の考え方

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。

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。

メディアの種類	遠 隔 地 保 管 の 適 否
磁気テープ	持ち運びしやすく遠隔地保管には最も適している。（耐用年数に注意）
光学ディスク	ＤＶＤやブルーレイは容量的な問題も少なく、コストも安価。（ただし、耐用年数に注意） 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。
外付けＨＤＤ	サーバに直接接続して使用するため、遠隔地保管には、最低３台のＨＤＤが必要である。(遠隔地保管用、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、遠隔地保管には不適。
ストレージ装置※	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を行う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。 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。

※ストレージ装置：システム本体とネットワークを通じて接続する記憶装置のこと

以上のことから、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の状態の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、遠隔地保管を行う。

○　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、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。

イ　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。

(3) 業務ソフトウェアやデータの保管対策等に関する行動計画の策定

「業務ソフトウェア等の保管対策及び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、「遠隔地保管に関する行動計画」（以下、「保管行動計画」という。）を策定する。

ア　計画策定の対象システム

保管行動計画を策定する必要がある重要システムは、次のとおりである。

１　業務ソフトウェア等

(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等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、システムの復元に必要な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）に保管しており、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等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）において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
・ 保管先をデータセンターにする場合は、P26 の要件を満たすデータセンターとする。

イ　計画の策定者

「保管行動計画」を策定する必要がある情報システムの担当課は、後述の「実施手順と送付方法」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、計画を策定する。

［保管行動計画　…　巻末様式集　様式１］

ウ　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ソフトウェア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、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。

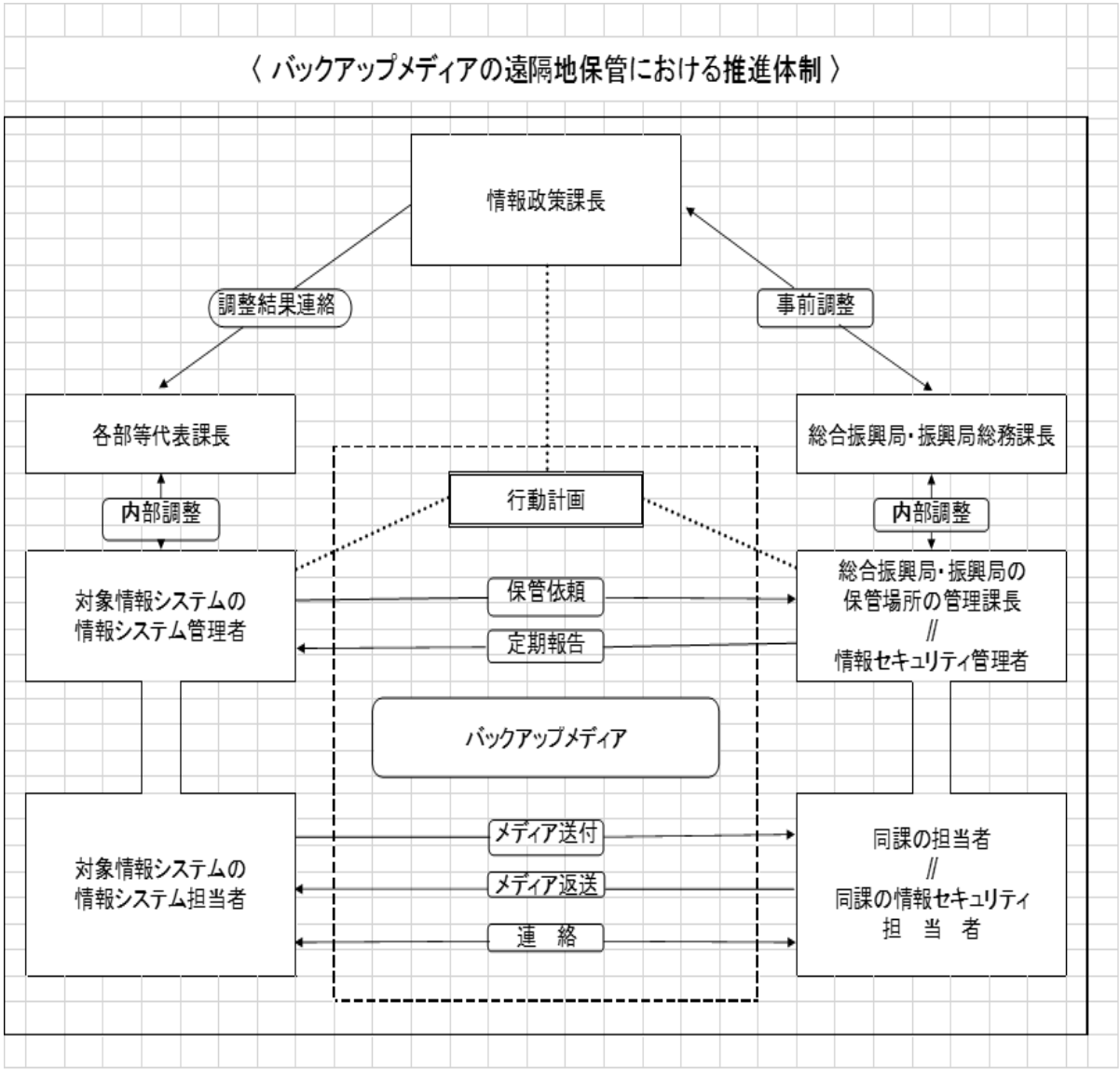
○　保管は、総合振興局等内にある書庫等内の保管庫（ロッカー等）で行うこととし、入室管理、施錠管理等、セキュリティに万全を期すこと。

(4) 重要システム以外の取扱い

重要システム以外のシステムにおいても、災害等により業務ソフトウェアやデータが消失し、システム復旧が困難となることがないよう、重要システムにおける取扱いを準用し、情報システム管理者は、業務ソフトウェアやデータの保管対策等、適切に取り組むこととする。

(5) 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。



〈 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 〉

担　　当	役　　割
総務部イノベーション推進局情報政策課長	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、保管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。
情報システム管理者	北海道情報セキュリティ対策基準第 13 条に定める情報システム管理者は、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、保管行動計画を策定する。 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	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（北海道情報セキュリティ対策基準第 12 条に定める情報管理者。以下、同じ）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情報セキュリティ管理者	情報システム管理者が行う保管行動計画の策定に協力する。 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。

〈 実 施 手 順 と 送 付 方 法 〉

①	各部等代表課長は、部局内の情報システム管理者と調整の上、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	情報システム管理者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	情報システム管理者は、保管行動計画書を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	情報システム管理者は、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	情報システム管理者は、バックアップメディア等を梱包した上に発送票（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、情報システム管理者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	保管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。

［別紙様式１－１…巻末様式集　２－１］・［別紙様式１－２…巻末様式集　２－２］
［別紙様式２…巻末様式集　２－３］

(6) 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、情報システム管理者と総合振興局等担当課長との協議により、「保管行動計画中」に記載することとする。

２　重要システムのサーバー等の保護対策

(1) 重要システムの現状と目標復旧時間

ア　重要システムの現状

重要システムのうち、本庁舎等にサーバがあるシステムについては、大地震により本庁舎等が使用不能となるほど大きく損壊した場合、システムの全部又は一部が消失する恐れがある。

仮に消失した場合、システムの復元に相当の時間（１ヵ月以上）を要することが見込まれる。

イ　重要システムの中断に伴う目標復旧時間

重要システムは、災害時においても止めることができないシステムであり、仮に止まることがあったとしてもできる限り早期に復旧させなければならないシステムであるが、止まることが許容される時間はシステムの目的や内容によって異なるため、重要システムごとにあらかじめ目標とする復旧時間を設定する必要がある。

その際、システムの中断が道民の生命、身体、財産の保護、業務継続のための環境の維持などに及ぼす影響度に応じて判断することが重要である。

なお、目標とする復旧時間は最長でも、災害による通信施設や電柱等の損壊、伝送路の切断、停電等に対する復旧活動がほぼ収束する時期までとし、東日本大震災では、発災後から約１ヵ月後に通信機能の８～９割が回復したことから、本ＩＣＴ－ＢＣＰでは最長でも１ヵ月（30 日）までとする。

＜目標復旧時間の基本的な考え方＞

・ 目標復旧時間の設定は、重要システム担当課の情報システム管理者が行う。

今後、新たに重要システムとする場合についても同様とする。（P12 の「重要システムの見直し（追加等）を行う場合の取扱い」参照）

・ 重要システムの復旧は、システムごとにあらかじめ設定した目標復旧時間内で行うこととする。

・ 目標復旧時間の設定は、最長でも発災後 30 日までとする。

(2) サーバー等の保護対策の基本的な考え方

重要システムのサーバー等の整備に係る基本的な考え方は、次のとおりである。

① システムのバックアップなど、非常時でも維持・継続できる水準を目指すことを基本とする。
② ただし、本庁舎等の内部に設置しているサーバについては、次期システム更新時に、原則として、次の欄に掲げる要件を満たすデータセンターへ移設すること。
③ 移設するまでの間の災害に備えて、業務アプリの改修を行う必要がないシステム※については、レンタルサーバの活用について事前検討を行っておくこと。
④ 重要システムのハード面の整備を上記②、③以上の水準とする場合は、後述のソフト面、スキル面の取組を踏まえて、システム担当課において検討を行うこと。

※ 業務アプリの改修を行う必要がないシステムとは、サーバ消失に伴って新たなサーバにＯＳやミドルウェア、業務ソフトウェアなどをインストールして復元する際に、これまで使用しているＯＳのバージョンが古く、現在市販されていないなどの理由から、最新バージョンのＯＳに切り替えるなどの仕様変更があったとしても業務ソフトウェアの改修を行う必要がなく、インストールや設定作業のみで再立ち上げが可能なシステムのこと。

このようなシステムは、サーバがあればシステムを再稼働させることができるため、災害時の混乱の中で新規に調達するよりは、レンタルサーバの方が迅速にシステムを立ち上げることができる。

データセンターの要件は、次のとおりである。

（構造・設備上の要件）
① 建物が震度６強以上の耐震（免震）構造、又は床免震構造となっていること
② 津波や液状化のリスクが少ない場所にあること
③ 外部からの電源供給が高圧２系統以上となっていること
④ 自家発電装置による停電対策がとられていること（長時間自家発電を行うための燃料供給に係る対策がとられていること）
⑤ 探知センサー連動型のガス消火設備を有していること
⑥ 類焼を防ぐための耐火構造壁を有していること
⑦ 防湿性・耐熱性の高い漏水検知器を備えていること

（セキュリティ上の要件）
⑧ 建物の出入口からサーバ室の出入口までの間、最低でも２ヵ所以上、生体認証などによる入退室管理体制を整えていること
⑨ 24 時間 365 日の有人監視体制を整えていること

(3) 今後の取組と手順

重要システムのサーバー等の保護対策に係る今後の取組と手順は、次のとおりである。

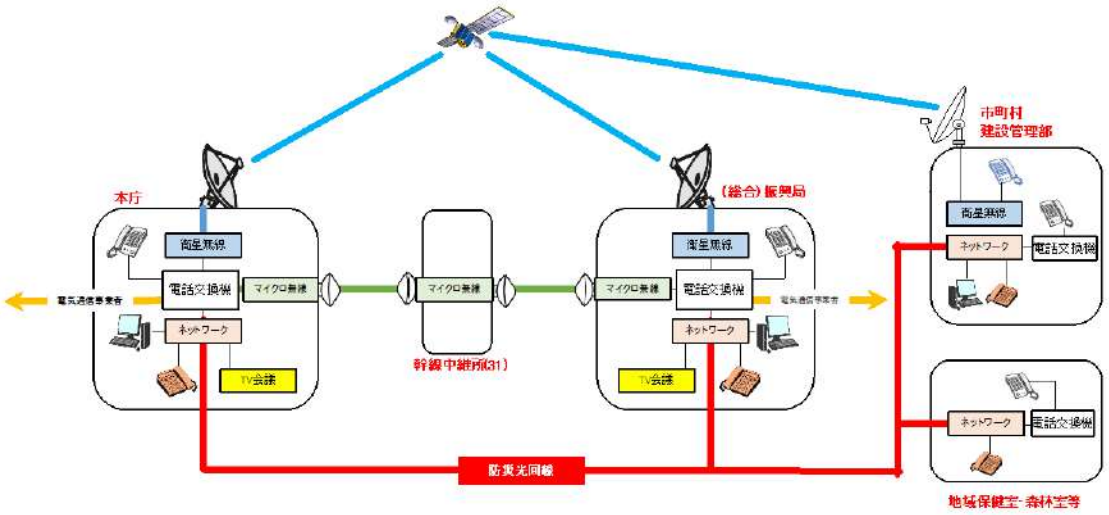
① 重要システムの更新時等において担当課に対し、「ＩＣＴ－ＢＣＰの視点からみたシステム診断」を実施する。
　実施に当たっては、情報化推進アドバイザー（民間の有識者）から助言を求める。
② 診断結果については、「診断票」を重要システム担当課に通知する。
③ 重要システム担当課は、診断結果に基づき次期システム更新に向けての検討を行う。
④ 本庁舎等にサーバ等があり、データセンターへの移設について検討を要する旨の診断結果が出された重要システムについては、重要システム担当課において、システム構築経費やランニング経費等全体のコストと大規模災害時におけるリスクを勘案して、総合的に判断して対応する。

３　庁内の基幹的情報通信ネットワークの整備

道の北海道総合行政情報ネットワーク（防災回線）や道庁行政情報ネットワーク（庁内ＬＡＮ）などの基幹的なネットワークは、本庁と出先機関、市町村を結ぶ電話網や電子メール、共有ドライブなどパソコンを用いた事務処理に必須の機能、更には財務会計トータルシステムなど、道の各機関を結ぶ基礎的で重要な業務に使用されている。

このうち防災回線は、主回線である「光回線（防災光回線）」及び「マイクロ回線」、更に「衛星回線」の３つの種類の異なる通信回線により構成され、万一、回線障害が発生した場合においても相互に補完しあう対策が講じられており、道内で大地震などの大規模な災害が発生した場合においても、基幹的情報ネットワークの維持確保が図られるよう着実に整備を推進する。

〈北海道総合行政情報ネットワークの概要〉



第２部　ソフト面に係る取組

（取組の基本的な考え方）

■ 災害時においても重要システムの維持・確保を図るため、必要な体制と役割分担、安否確認方法、システム被害の確認方法、運用保守業者との連絡方法、システムの復旧に向けての取組内容等を定める「重要システムの復旧に係る 行動計画」を策定する。
■ システムが使用できない期間中においても業務の継続を図るため、代替手段の作業内容や推進体制等を定める「重要システムに代わる代替手段の行動計画」を策定する。

１　重要システムの復旧に係る行動計画（「復旧行動計画」）

東日本大震災では､データセンターに設置されていたサーバの大半は被害を免れ、データセンターの堅牢性が改めて実証された。

このことを踏まえ、ハード面の対策として、被災のリスクを最小限にとどめることができるデータセンターの活用を図ることとしたが、活用するまでの間に被災するリスクがあること､活用後においてもリスクがゼロにはならないことを考慮し、ソフト面の対策においては、データセンター自体やデータセンターまでの回線の被災も想定して、「重要システムの復旧に係る行動計画」（以下「復旧行動計画」という。）を策定する。

(1)「復旧行動計画」の内容

「復旧行動計画」は、各重要システムに共通する項目と、重要システムの目的や形態の違いから個別に整理する項目とに分かれる。

これらについて、主な内容を示す。

＜共通項目の内容＞

復旧行動計画に記載する項目		内　容　等
初動対応	・ システムの復旧・復元に必要な体制と役割分担	・ 指揮命令系統、役割分担、必要な人数などを整理 ・ 必要な人材の確保について整理
	・ 発災時の安否確認方法	・ 電話(固定・携帯)、携帯メール、ＳＮＳなど多様な手段による伝達方法を整理
	・ 参集ルール	・ 災害等対応マニュアルがベース
	・ システム運用保守業者に対する連絡方法	・ 電話(固定・携帯)、携帯メール、ＳＮＳなど多様な手段による伝達方法を整理
	・ 重要システムの被害状況の確認	・ サーバの稼働状況等の確認方法を整理　・ システム運用保守業者との協定締結（連携方法を整理）
・ 総合振興局等に保管しているデータ等の搬送に係る連絡方法		・ 「保管行動計画」に基づき実施

共通項目には、災害発生時に直ちに行わなければならない初動対応（安否確認、参集、システム運用保守業者との連絡、重要システムの被害状況の確認）が含まれる。

共通項目の整理にあたって注意しなければならない点は、次のとおりである。

・ 初動対応は、迅速かつ正確さが求められるため、体制や連絡手段等について適切な対応が必要となる。
・ 職員の現在地や被害箇所等の情報をまとめるためには、手元に地図がないと難しい。
・ 発災直後は、情報が集まらない可能性がある。仮に情報を得たとしても断片的であったり不正確であることが多い。
・ しばらくは被害の全体が分からないことが多い。特に激甚エリアからの情報は入手できないことが多い。
・ システムの運用保守業者やＡＳＰサービス事業者からの情報は専門用語が使われることが多く、情報システムに詳しい職員が対応しなければ、理解に窮する場面が出てくる。
・ 発災後からの記録をとっていないと、古い情報や経緯が分からなくなるおそれがある。
・ 重要システム保守業者とのシステム復旧に係る協定の締結について
　災害時において、重要システムに障害が生じた場合に備え、重要システムを迅速かつ的確に復旧させることを目的として運用保守事業者と協定を締結する。

（協定の主な内容
・大規模災害発生時の連絡要員及び連絡方法の明確化、データセンタへの立入許可、機器貸与
・システム復旧の手順確認及び担当課との役割分担）

＜個別項目の内容＞

復旧行動計画に記載する項目	内　容　等
・ サーバ等の調達に係る方法	・ 契約方法（災害時は随意契約が可能な場合有）と業務範囲の明確化
・ 搬送時における道路の渋滞や通行止めへの対応	・ 通行止め等の場所の確認方法
・ 運用保守業者の被災によりシステムの復元が困難となった場合の対応	・ 他の業者との事前の情報交換等
・ システムの復旧に伴う職員ユーザによるテスト対応	・ システムの操作に詳しい職員の確保
・ （総合）振興局等出先機関が被災した場合の対応	・ 指揮命令系統、連絡体制などの明確化 電話（固定・携帯）、携帯メール、ＳＮＳ など多様な手段による伝達方法 ・ 被害状況の確認方法、現地での対応手順の整理

個別項目の整理にあたって注意しなければならない点は、次のとおりである。

・ システムの復旧に係る作業は、運用保守業者に委託をしている業務以外は、原則、道が行うこととなるが、災害時における契約以外の協力関係について、事前に運用保守業者と十分な協議を行っておく必要がある。
・ 運用保守業者が被災し、システムの復旧作業ができない場合は他の業者にその作業を委託する必要があるが、事前に協議を行っておかないと、作業内容が分からず、内容によっては断られる場合がある。システム全体のバックアップを行っているかどうかが重要なポイントとなる場合が多い。

・ システムの復旧に係る作業は、運用保守業者に委託をしている業務以外は、原則、道が行うこととなるが、災害時における契約以外の協力関係について、事前に運用保守業者と十分な協議を行っておく必要がある。
・ 運用保守業者が被災し、システムの復旧作業ができない場合は他の業者にその作業を委託する必要があるが、事前に協議を行っておかないと、作業内容が分からず、内容によっては断られる場合がある。システム全体のバックアップを行っているかどうかが重要なポイントとなる場合が多い。

(2) 「復旧行動計画」策定に係る取組方針

「復旧行動計画」を策定するための取組方針は、次のとおりである。

① サーバの保管場所がデータセンターであるなしに関わらず、重要システムが被災することを前提とする。
② 想定される事態をできる限り洗い出し、その対応策を文書化する。
③ 災害時における協力関係について、運用保守業者と十分な協議を行い、役割分担を明確化する。

(3) 目標とする重要システムの復旧時間

重要システムの復旧は、あらかじめ設定した目標復旧時間内で行うこととする。目標復旧時間の設定は、最長でも発災後 30 日までとする。

(4) 「復旧行動計画」の構成

「復旧行動計画」は、総括表と個別票の２種類の構成とする。
なお、復旧行動計画の様式や記載内容、記入例等については、情報政策課において別に作成する「重要システムに係る代替・復旧行動計画策定のための作業マニュアル」（以下、「作業マニュアル」という。）において示す。

(5) 「復旧行動計画」策定の手順

「復旧行動計画」を策定するための手順は、次のとおりである。

① 重要システム担当課内に、検討のためのチームをつくる。チームの構成員は、管理部門、システム調達部門、システム利用部門等から職員を選抜する。
② 共通項目は必須事項として検討し、個別項目は想定される事態をできる限り洗い出し、その対応策を検討する。
③ 検討にあたっては、情報政策課において別に作成する「作業マニュアル」を参考とする。
④ 検討過程において、運用保守業者に対し意見等を求めるなど、協力を依頼する。
⑤ 必要に応じて、情報政策課や関係課から意見を求める。
⑥ 一連の検討が終わった時点で、重要システム担当課の情報システム管理者を交え、重要システム以外の非常時優先業務の遂行に必要な取組（重要システム停止中の代替手段を含む。）も含めた全体調整を行う。
⑦ 全体調整後、行動計画を確定する。

(6) 「復旧行動計画」の取扱い

「復旧行動計画」は、計画書を所持しなければならない職員（行動計画の中に明記する）に対し、書面により配付（電子データは認めない）するとともに、当該計画を情報政策課長に提出する。

「復旧行動計画」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。書面による自宅での保管は、これを認める。

(7) 「復旧行動計画」の改定・見直しに向けての考え方

「復旧行動計画」は、後述する「訓練」を通して検証し、必要に応じ、適宜、改定・見直しを行うものとする。

少なくとも組織の変更や人事異動が行われたときには、改定・見直しを行う必要がある。

＜改定・見直しを行った場合の「復旧行動計画」の取扱い＞

① 改定・見直しを行った場合の「復旧行動計画」の取扱いについては、当初策定した「復旧行動計画」と同様に、計画書を所持しなければならない職員への書面による配付のほか、情報政策課長に提出するものとする。
② 改定が行われた場合は、その都度、情報政策課長へ提出する。

(8) 情報政策課の役割

「復旧行動計画」の策定に関し、情報政策課では、次の取組を実施する。

① 重要システム担当課による「復旧行動計画」策定を支援するため、「作業マニュアル」を作成し、関係先に通知する。
② 作業マニュアルの精度を高めるため、各重要システム担当課が行う「復旧行動計画」の改定・見直しの内容を活かし、適宜、必要な改定を行う。
③ 「復旧行動計画」の検討にあたり、必要な情報提供等を行うなど、連携・協力を進める。

２　重要システムに代わる代替手段の行動計画（「代替行動計画」）

重要システムが使用できない状態としては、サーバの障害や損壊に伴う復旧作業中である場合や、サーバ自体は動くが停電や光回線の障害により通信が途絶している場合などが考えられる。

このような場合でも、システムの復旧や通信環境の回復がなされるまでは、システムの代わりとなる方法（代替手段）によって非常時優先業務の遂行に努める必要がある。

このため、事前に「重要システムが使用できない期間中における代替手段に係る行動計画」（以下「代替行動計画」という。）を策定する。

(1)「代替行動計画」の内容

重要システムには、データベースの作成や帳票出力といった業務の簡素化・効率化に資するものから、画像や映像を伝達するもの、それらをインターネット上で公開するものなど様々なシステムがあり、これらに対する代替手段はその目的によって異なる。

このため、ここでは「業務の簡素化・効率化のために一般的に用いられるシステム」を想定して、代替行動計画に記載する項目についてその主な内容を示す。

なお、この場合の代替手段としては、書面によるもののほか、ワープロ、表計算などのソフトを活用したファイル生成作業が該当する。

＜主な記載項目の内容＞

代替行動計画に記載する項目	内　容　等
・ 代替手段の遂行に必要な体制と役割分担	・ 指揮命令系統、役割分担、必要な人数などを整理
・ 代替手段への切替を判断する条件の設定	・ サーバの再稼働の時期や、通信回線の復旧の見通し等の把握
・ 代替手段の手順を示した作業手順書※の作成・事前周知	・ 代替手段で作業を行う職員への事前周知方法
・ 代替手段への切替を行うことを作業を行う職員に伝える方法	・ 電話(固定・携帯)、携帯メール、ＳＮＳなど多様な手段による伝達方法を整理
・ 作業を行う職員からの問い合わせ対応	・ 問い合わせ方法の整理
・ 作業を行う職員の作業場所の確保	・ 本庁舎等の立入禁止を想定し、作業人数に応じた作業場所の候補を事前検討
・ 作業により生成した書面やファイルの取扱い方法	・ 作業を行う職員からの書面やファイルの受渡方法の整理
・ （総合）振興局等出先機関が被災した場合の対応（必要時）	・ 連絡先、連絡方法等の明確化 ・ 作業手順書の周知

※ 作業手順書　…　重要システムが使用できない場合に、システムの代わりとなる方法（作業手順や様式等）を定めたもの

記載項目の整理にあたって注意しなければならない点は、次のとおりである。

・ 代替手段の切替時期については、サーバの復旧時期等の見通しによるほか、当該業務の繁忙期・閑散期における許容中断時間（業務の遅れが及ぼす社会的影響が少ない等により中断が許される時間）などを勘案して判断する必要がある。
・ ファイル生成作業は、インターネットなどの通信環境に関わらず、ワープロや表計算などのソフトがインストールされたノートパソコン等の端末機があれば可能である。
　端末機の調達方法のほか、道庁ＢＣＰで想定されている万一、本庁舎等が使用できない場合において、代替施設としている札幌市周辺の道有施設での作業を想定し、その活用について事前に検討しておく必要がある。
・ 代替手段の手順等を示した作業手順書の作成にあたっては、実際の作業時における問い合わせを軽減するため、当該システムを使って作業を行っている職員の意見を十分踏まえる必要がある。
・ 代替手段の作業体制については、業務量と処理時間を正しく見積もった上で整理する必要がある。
・ システムを用いず代替手段を用いて業務を継続していることについて道民等に周知する必要がある場合は、その方法を検討する必要がある。
・ （総合）振興局等出先機関が被災し、重要システムの使用に支障が生じている場合の対応についても、必要に応じて整理する。

(2) 「代替行動計画」策定に係る取組方針

「代替行動計画」を策定するための取組方針は、次のとおりである。

① 想定される事態をできる限り洗い出し、その対応策を文書化する。
② 代替手段の推進にあたっては、作業の効率化・省力化を図る。
③ 対応策の検討にあたっては、協議を必要とする機関と十分調整して進める。

(3) 「代替行動計画」の構成

「代替行動計画」は、総括表と個別票の２種類の構成とする。
なお、「代替行動計画」の様式や記載内容、記入例等については、作業マニュアルにおいて示す。

(4) 「代替行動計画」策定の手順

「代替行動計画」を策定するための手順は、次のとおりである。

① 重要システム担当課内に、検討のためのチームをつくる。チームの構成員は、管理部門、システム調達部門、システム利用部門等から職員を選抜する。
② 代替手段の手順を示した作業手順書を作成する。この内容を固めた上で、他の項目について具体的な検討に入る。
③ 検討にあたっては、情報政策課において別に作成する「作業マニュアル」を参考とする。
④ 検討過程において、運用保守業者に対し意見等を求めるなど、協力を依頼する。
⑤ 必要に応じて、情報政策課や関係課から意見を求める。
⑥ 一連の検討が終わった時点で、情報システム管理者を交え、重要システム以外の非常時優先業務の遂行に必要な取組も含めた全体調整を行う。
⑦ 全体調整後、行動計画を確定する。
※ なお、作業手順書は、「代替行動計画」と切り離し、作成後、重要システムの職員ユーザに通知する。

(5) 策定した「代替行動計画」の取扱い

「代替行動計画」は、計画書を所持しなければならない職員（行動計画の中に明記する）に対し、書面により配付（電子データは認めない）するとともに、当該計画を情報政策課長に提出する。

「代替行動計画」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。書面による自宅での保管は、これを認める。

(6) 「代替行動計画」の改定・見直しに向けての考え方

各重要システムの「代替行動計画」は、後述する「訓練」を通して検証し、必要に応じ、適宜、改定・見直しを行うものとする。

少なくとも組織の変更や人事異動が行われたときには、改定・見直しを行う必要がある。

＜改定・見直しを行った場合の「代替行動計画」の取扱い＞

① 改定・見直しを行った場合の「代替行動計画」の取扱いについては、当初策定した「代替行動計画」と同様に、計画書を所持しなければならない職員への書面による配付のほか、情報政策課長に提出するものとする。
② 年に数回、改定が行われた場合は、その都度、情報政策課長へ提出する。

(7) 情報政策課の役割

「代替行動計画」の策定に関し、情報政策課では、次の取組を実施する。

① 重要システム担当課による「代替行動計画策定」を支援するため、「作業マニュアル」を作成し、関係先に通知する。
② 作業マニュアルの精度を高めるため、各重要システム担当課が行う代替行動計画の改定・見直しの内容を活かし、適宜、必要な改定を行う。
③ 「代替行動計画」の検討にあたり、必要な情報提供等を行うなど、連携・協力を進める。

第３部　スキル面に係る取組

（取組の基本的な考え方）

■ 平常時からの取組として、ＩＣＴ－ＢＣＰに関する訓練を各情報システム担当課において、年１回以上行い、職員の対応能力を強化する。
■ 訓練を通じて行動計画を検証し、必要に応じて改定・見直しを行う。

１　訓練の方法

「復旧行動計画」や「代替行動計画」を災害時に迅速・的確に遂行するには、その内容をあらかじめ訓練を通して職員が経験し、緊急時においても迷わずに判断や行動ができるようにするとともに、組織としても、情報システムが使えない錯綜した状況の中で、限られた人員によって組織力を十分発揮できるよう、ノウハウを蓄積しておくことが重要である。

また、これらの行動計画を実地に検証し、必要に応じて改定・見直しを行うためにも、訓練は重要である。

訓練には、机上訓練と実働訓練の二つがある。それぞれについて、訓練の目的と方法を示す。

＜机上訓練＞

目的	・ 現実に即した災害イメージを形成し、行動計画の実行可能性の検証と改善点の発見に結びつける
方法	・ 個人での訓練と、集団による訓練を組み合わせて行う。 ・ 行動計画で整理した具体的な対応について、時系列的に展開を予想する訓練を行い、実行可能性を検証する。 ・ 非常用電源の燃料切れなど困難な事態を具体的にリストアップし、行動計画上、どのように対応することになっているかを確認する。 ・ 地図を用いて、職員宅や運用保守業者、データセンターなど行動計画上の関係者の位置と、災害時に想定される事態（例えば公共交通機関の不通）の位置関係を確認しておくことも重要。

＜実働訓練＞

目的	発災時や混乱が続いている状況を想定し、迅速かつ円滑に対処する技能を職員に習得させるとともに、実地に得られた知見をもとに行動計画等を改善する
方法	実技訓練と移動・設置訓練を行う。 （実技訓練） ・ 重要システムの復元やバックアップデータの読み込みを実際に行ってみる。 ・ 安否確認連絡を実践してみる。 ・ 代替手段の作業を行ってみる。 ・ 重要システム担当課内と道庁内の関係課との連携等に要する時間を計測してみる。 （移動・設置訓練） ・ 集合場所への参集や、データセンター、運用保守業者が勤務する建物への移動訓練。 ・ 徒歩帰宅訓練。 ・ 代替施設への机やパソコン、プリンタ等の搬入と設置、接続、起動の訓練。

訓練の実施にあたって注意しなければならない点は、次のとおりである。

・ 机上訓練については、正しい災害イメージを形成することが重要である。
・ 正しい災害イメージとは、単に「被災」、「停止」、「消失」などの抽象的な言葉で想定するのではなく、現実に起きた災害の具体的な事例などを基に、電源の喪失やネットワークの途絶、事業者との連絡不能、職員の出勤困難など対応の難しい事態が幾つも重なって起きることを 想定して形成するものである。
・ 現場情報が不足する中で事態の全体像をつかむことは非常に難しいため、データセンターやサーバ室のイラストや、置かれているサーバとサーバが行っている作業や機能などが分かるような資料を訓練の際に作成し、災害時の状況把握のためにあらかじめ備えることが重要である。
・ 実働訓練については、目標処理時間内に対応できたかどうかを確認するため、チェックリストを作成し、評価する職員を配置して行う必要がある。
・ 訓練の実施により、目標処理時間内での対応が難しく、解決方法としてシステムの改善が必要と判断した場合は、次期システム更新を含めハード面の強化について検討することが重要である。

２　訓練計画策定に係る取組方針

訓練は日頃の積み重ねが重要であることから、実施に向けて計画的な取組が必要である。

１回の訓練で行動計画の項目すべてを点検するのが難しい場合は、数回に分けて実施することとし、あらかじめ策定する「訓練計画」に基づき実施する。

訓練計画の策定に関する取組方針は、次のとおりである。

① 狙いを決めてテーマを整理し、参加者の立場を明確化した上で、訓練の回数や実施時期を決定する。
② 組織間の連携を強化することも目的の一つであることから、運用保守業者等外部の関係者に対し、訓練への理解と協力を求める。

３　訓練計画

行動計画（復旧・代替）と訓練計画の関係が分かるよう、訓練計画には行動計画の総括表や個別票の内容をベースとして、訓練対象項目や参加者等、必要な項目を加える。

４　策定した訓練計画の取扱い

訓練計画は、行動計画（復旧・代替）策定後に、重要システム担当課が策定することとし､計画書を所持しなければならない職員に対し書面により配付するとともに、当該計画を情報政策課長に提出する。

訓練計画は非公開扱いとし、その管理については厳重に行うこととする。

書面による自宅での保管は、これを認める。

５　訓練による行動計画（復旧・代替）の改善

訓練により行動計画（復旧・代替）の内容に改善すべき点があった場合は、当該行動計画を適宜、改定する。

６　情報政策課の役割

訓練に関し、情報政策課では、次の取組を実施する。

① 訓練計画の策定検討及び訓練の実施にあたり、必要な情報提供等を行うなど、連携・協力を進める。
② 災害状況のイメージ力や状況予測能力の向上等を図るため、重要システム担当課を対象とした「ＩＣＴ－ＢＣＰに係る研修会」を実施する。

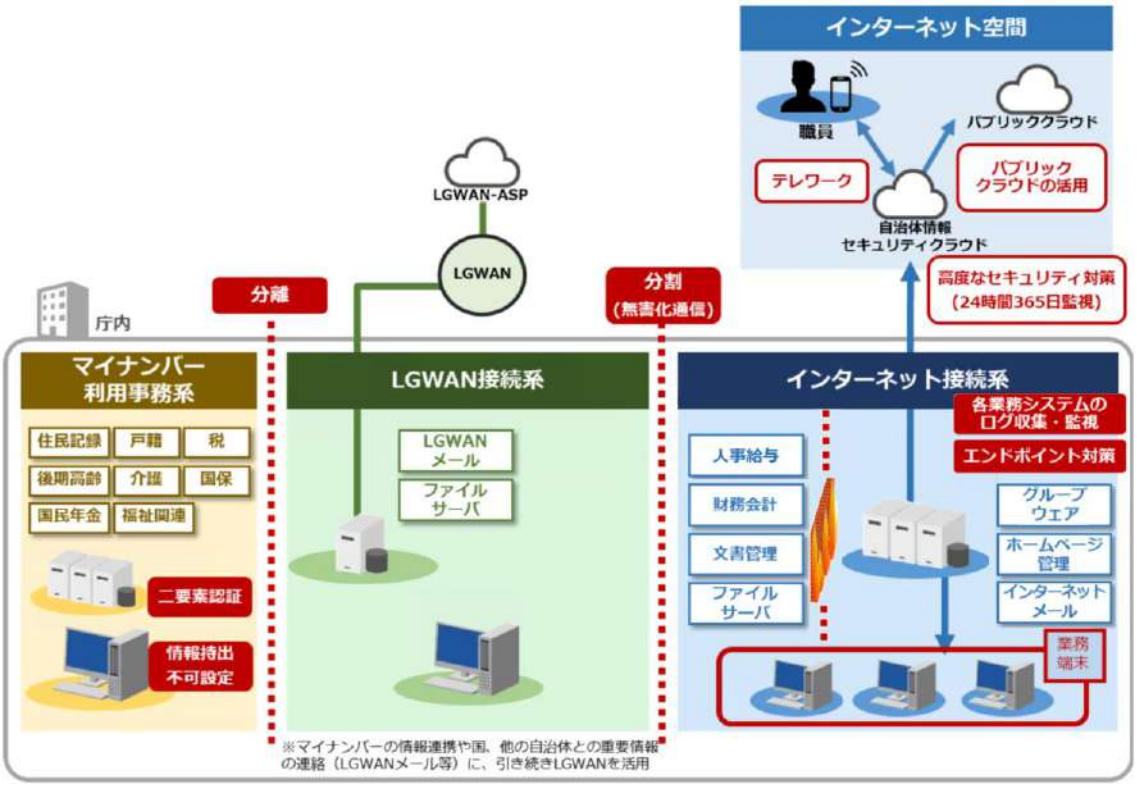
第４部　情報セキュリティ対策に係る取組

災害時における情報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、あわせて道の保有する情報資産を様々な脅威から防御し、道の情報資産の機密性、完全性及び可用性の維持が不可欠となる。

近年、標的型攻撃メールを起因とする個人情報の流出事故、ランサムウェアによる被害など世界的な規模でサイバー攻撃が複雑化、巧妙化しており、国内でも行政機関や企業などにおいても甚大な被害が発生するなど、情報セキュリティ対策の重要性は一層増している。

道においては、情報セキュリティ対策の強化に向けて平成 28 年度から庁内ネットワークを「個人番号利用事務系」、「ＬＧＷＡＮ接続系」、「インターネット接続系」の３系統への分離・分割を行ったほか、市町村などと共同で「自治体情報セキュリティクラウド」を構築した後、令和３年度にはテレワーク時における環境整備、業務の効率性や利便性向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置するβ´モデルを採用し、それぞれの構成で必要となるセキュリティ対策を講じている。

【三層の対策とβ´モデルの構成イメージ】



また、「北海道情報セキュリティ対策基準」（以下「対策基準」という。）に基づき、物理的・人的・技術的な面から各種セキュリティ対策を講じるとともに、万一サイバー攻撃等による情報資産への侵害等が発生した場合において、被害の拡大防止や迅速な復旧等を図るため、緊急時対応計画を策定し、対応手順の明確化といった取組を進めている。

なお、庁内において情報セキュリティインシデントが発生した場合においては、当該ＩＣＴ－ＢＣＰに拠らず、「対策基準」に基づき設置している「北海道ＣＳ

ＩＲＴ」において、情報政策課と重要システム担当課が連携協力し、早期の復旧に向けて必要な対応を行う。

令和４年度から公用スマートフォンによるテレワーク環境を整えたことにより、利便性が向上した一方で庁舎外へ端末を持ち出す機会が増加し、紛失等による情報セキュリティインシデント発生リスクが増加することから、職員一人一人が情報セキュリティに対する意識を持ち、対策基準を遵守することが必要である。

北海道 CSIRT（ホッカイドウ・シーサート）

庁内において、情報セキュリティインシデント（以下「インシデント」という。）が発生した場合の対応等を行う庁内組織。（「対策基準」に基づき設置）

インシデントの発生時に事務局である情報政策課が中心となって関係課と連携して、速やかな終息・復旧のために必要な対応を行うほか、庁内及び道内市町村におけるインシデント対応に必要な支援等を行う。

第５部　ハード面・ソフト面・スキル面の継続的な取組

業務継続能力の向上を目指すため、情報システムの更新サイクル（おおむね５～６年の周期で機器更新）を踏まえ、更新から次の更新までの間に、ハード面・ソフト面・スキル面をＰＤＣＡサイクルに基づく継続的な取組として推進する。

Ｐｌａｎ（計画）では、ハード面として、システムの構成や機能要件等を定める調達仕様書の作成や、最適化の取組によるシステム整備の検討（全体最適化によるサーバ統合や個別最適化による情報システム診断の実施）、ソフト面として、行動計画（復旧・代替）の策定に取り組む。

Ｄｏ（実施・実行）では、ハード面として、重要システムの予算化に基づく開発や運用、スキル面として、訓練計画に基づく訓練の実施やＩＣＴ－ＢＣＰに係る研修会の実施に取り組む。

Ｃｈｅｃｋ（点検・評価）では、ハード面として、訓練の実施により判明したシステム上の課題や問題点の整理、ソフト面として、訓練結果に基づく行動計画（復旧・代替）の改定・見直しや作業マニュアルの改定に取り組む。

Ａｃｔ（処置・改善）では、ハード面として、次期システムの改善に向けての検討や、検討のための情報を集めるための手続であるＲＦＩ※の実施、ソフト面として、改定した行動計画（復旧・代替）の管理や業務継続を行う職員に対する内容の周知等に取り組む。

このＡｃｔ（処置・改善）を受けて、再びＰｌａｎ（計画）に移り、現行システムを再構築する作業（調達仕様書の作成や情報システム全体最適化の取組）や、システムの変更点を踏まえた行動計画の策定に入る。

※　ＲＦＩ（リクエスト・フォー・インフォメーション）：「情報提供依頼」のこと。システムの形態や構成、構築や運用保守費用など必要な情報をオープンな形で幅広く求める手続手法。

第３章　市町村ＩＣＴ－ＢＣＰ策定に対する支援

市町村には「地域防災計画」があるが、その性格上、ＩＣＴ機器や情報通信ネットワークが被災した場合の対応やそれまでの事前対策など、ＩＣＴの専門領域に具体的に踏み込むものではない。

市町村においても、職員の多くは、庁内ＬＡＮで結ばれたパソコンからメールサーバやファイルサーバへアクセスし、メールのやりとりや各種ソフトで作成したファイルを共有している。

また、税や福祉、財務などの情報システムを業務遂行の重要な手段として利用しており、市町村においてもＩＣＴ－ＢＣＰを策定し、災害に備えることが重要である。

ＩＣＴ－ＢＣＰを策定している市町村は 76 団体（令和 5 年 4 月 1 日現在）に留まっており、道としてはセミナーの開催やノウハウを提供するなど、市町村におけるＩＣＴ－ＢＣＰの策定促進に向けた必要な支援を行っていく。

１　普及・啓発

市町村のＩＣＴ－ＢＣＰ策定を促進するため、地域情報化推進会議などの会議において、東日本大震災の教訓や道のＩＣＴ－ＢＣＰの取組内容等の周知を行うとともに、国、民間が行うセミナーの活用などを通じて、市町村におけるＩＣＴ－ＢＣＰ策定の普及・啓発を行う。

２　計画策定・技術課題等の支援

通信回線や情報システムの整備など様々な課題について、市町村からの問い合わせを受け付けるとともに、必要に応じ現地での状況確認や意見交換を実施するなど、ＩＣＴ－ＢＣＰ策定や技術的課題の解決に向けた支援を行う。

ＩＣＴ部門の業務継続計画

ステップ３

「業務継続能力を強化するための対策」

平成３０年３月
（令和６年４月改定）

北海道総務部イノベーション推進局情報政策課

〒060-8588 札幌市中央区北３条西６丁目
TEL：(011)204-5980

［様式１］

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]

［様式２－１］

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

［様式２－２］

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

［様式２－３］

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	

［様式３－１］

様式１

非常時優先業務遂行に不可欠な情報システムに係る調査票

部　等　名		局・課名			
		担当者名		内線番号	

1　非常時優先業務名

非常時優先業務名		応急業務・通常業務の別		応急業務		着手目標時期		発災直後
				通常業務				1　時　間
業　務　内　容								1　日　目
								3　日　目
								1　週　間

2　非常時優先業務遂行に不可欠な情報システム名

非常時優先業務遂行に不可欠な情報システム名		不可欠な理由	
		システムの運用業者名	

※　業務とシステムの関係が分かるフロー図を別紙にて添付のこと

3　当該システムを利用している職員数　（令和○年○月○日現在）

当該システムを利用している職員数（本庁分）		人
当該システムを利用している職員数（総合振興局・振興局分）		人

当該システムの担当者及び当該システムに精通している課内の職員数の合計　（本庁分のみ）			人
上記職員の自宅から勤務先までの距離	～　2km		人
	2km　～　15km		人
	15km　～		人

4　当該システムを使用できない場合の代替措置について

停電やサーバの損傷等によりシステムが長期間使用できない事態が発生すると仮定した場合における手作業の状況について記入してください。

システムで行っている業務を手作業で行う場合のマニュアル等を定めていますか。	定めている	
	定めていない	

想定される手作業による業務の遅れ	システム利用と比較し				社会に与える影響度
	システム利用と比較し遅れが生じる	→	1日程度遅		
			3日程度遅		
			1週間程度		
			1ヵ月以上		

5　目標復旧時間について

停電やサーバの損傷等によりシステムが使用できない事態が発生すると仮定した場合におけるシステムの目標復旧時間を選択してください。

システムの目標復旧時間	発災後～1日	
	1日後～3日	
	3日後～1週間	
	1週間後～1カ月	
	1ヵ月後～	

※設問1における着手目標時期よりも遅くなると考えられます

［様式３－２］

様式２

非常時優先業務遂行に不可欠な情報システムの復旧等に関する調査について

本調査は、非常時優先業務遂行に不可欠な情報システム（以下、「重要システム」という。）とされたシステムについて、現状や復旧等に係る費用などを調べるものです。

調査票は(1)～(4)の４種類あります。

(1) 重要システムに係る実態調査

(2) 重要システムの復旧日数に係る調査（サーバ設置がデータセンター以外の場合のみ）

(3) 重要システムの復旧費用に係る調査（設問１～４については、サーバ設置がデータセンター以外の場合のみ）

(4) 重要システムの停止における手作業に関する調査

このうち(2)と(3)については、(1)の回答内容によって、回答を要するものと、要しないものがあります。

(1)～(3)については、システム担当課では回答できないものも含まれているため、当該システムの運用・保守を行っている業者のご協力の下、作成願います。

(4)については、システム担当課において、作成願います。

＜調査にあたっての前提条件等＞

・○年○月○日において、札幌市内に震度６強以上の直下型地震等が起こったと想定する。

・直下型地震等により、本庁舎、別館庁舎、議会庁舎は倒壊または一部倒壊により立入禁止となり、庁舎内にあるパソコンやサーバ、バックアップデータなど情報通信機器類はすべて消失するものとみなす。

・札幌市内のデータセンター（要件を満たすもの）に設置しているサーバやバックアップデータ等は、地震発生後、正常に稼働・保管されているものとみなす。

・札幌市以外に設置しているサーバや保管しているバックアップデータ等については、消失しないものとみなす。

・本庁舎等の立入禁止による新たな執務室（代替施設）におけるLANやクライアント環境等の構築は考慮しない。

・システム（サーバ等）の復旧・復元のみに限定し、調査する。

※調査票１～４については、省略。