

# クラウド・リスクマネジメントと 災害対策ソリューション

2011年7月5日 富士インフォックス・ネット株式会社 Tomoyuki HAYASHIDA

# 東日本大震災で被災された皆様へ

東日本大震災において被災された皆様には、 心よりお見舞い申し上げます。

皆様の安全と一日も早い復旧、復興をお祈り申し上げます。

### 東日本震災後の災害復旧とBCP

- 企業の情報管理に関する意識の変化
  - ファシリティとして地震や火災などの防災対策が堅牢なクラウドを利用する動きが活性化(中小企業から大企業まで)
  - ▶ 非データ・メディア(紙や記憶媒体等)に関しても、防災設備が整った保管業者に移管する動きも顕著
  - 業務アプリケーションに関しても、DR(災害復旧)環境を整える動きが東日本に本社を置く企業で急速に展開されようとしている
    - 東日本+西日本でのミラーもしくはバックアップシステムを構築
- BCP(事業継続計画)に関する意識の変化
  - > 上場企業中心の内部統制に関するBCP構築のレベル変化
    - 東日本震災以前は、東京都想定のM7.3によるシナリオ準拠
    - 震災後は、M9.0/震度7+津波によるシナリオでBCP再構築
  - 東京都や国のシナリオ待ち(!?)
  - 中小企業も、業務の早期復旧に対する重要性を再認識し、震災対応中心に 検討がはじまる

# 東日本震災後の "情報"災害復旧に対する企業の変化

		震災前	震災後	
オンプレミス派		データ(バックアップデータを含む) と紙などの非データ・メディアは、 同一建造物内に保管 ⇒ 建前:情報管理上、分散管理は しない方針	Case 1. データは、西日本支社などにも分散保管。 Case 2. データは、社内とクラウドで相互ミラーもしくはバックアップ運用。 紙などの非データ・メディアも、専門業者の保管サービスを併用。 プライベートクラウドへの展開も検討されている。	
クラウド派	国産	非データメディアは社内、データは、 クラウドで管理 ⇒ 海外クラウドはリスクが大きい と判断(コンプライアンスや契約)	データは、国産+海外で保管管理 プライベートクラウドへの展開も検 討されている。	
	海外	同上	データは、海外の複数拠点のDC で保管管理	

# 広域大震災が企業ITに与える影響 1/2

- ① 自社ビルの被災によるシステム停止
  - 電力の復旧は、M7.3レベルでは最大3日であったが、東京直下地震による M9.0では、それ以上の日数が必要になる可能性が大きい
  - ボ オンプレミスでサーバ運用している企業は、自家発電などの設備が無い場合には、原則、上記期間システムが停止することになる。
  - が確保されている自宅や近隣事業所からクラウド利用できる可能性もある。
  - iv. 計画停電が設定された時間帯のシステム運用に関しては、蓄電池、自家発電などの対応を取れる可能性がある。
  - v. システムを運用しているエンジニアが人的被災することにより、運用継続不可もしくは運用上影響が大きくなるケースも想定される。

# 広域大震災が企業ITに与える影響 2/2

### ② インターネットの停止

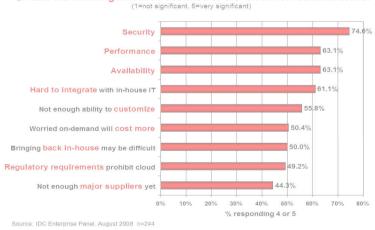
- インターネットサービスプロバイダ(ISP)やキャリアの震災によるノード障害 (ファシリティやNW機器など)で、広域にインターネットが利用出来ない可能 性がある。
- … クラウドが正常でも、クラウドが設置されている箇所でのインターネットが停止すれば、クラウドが利用出来ない可能性がある。

### ③ クラウドの停止

- i クラウドのデータセンタが被災により、システム運用できないケース
- ル クラウドのデータセンタが正常な場合でも、データセンタに接続するネットワークがダウンしている場合、サービス運用できないケース
- iii. クラウドのデータセンタが正常な場合でも、人的被災により、運用できない ケース

# クラウドと情報セキュリティマネジメント

- 現状のISO/IEC27000(情報セキュリティマネジメント、ISMS)は、クラウド利用を前提とした管理項目がない
  - ⇒ ISO化(SC27)が今年スタートしたばかり
  - > ワールドワイド: CSA (Cloud Security Alliance) のガイダンス(v2.1)
  - > 日本: METI(経産省)のガイドライン公表(4/1/2011)
    - ただしMETIガイドラインは、エンドツーエンドのセキュリティに言及せず
  - 企業がクラウドサービスを利用する際、「セキュリティ対策が十分かどうか分からない」が最も多い不安要素 Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model



# クラウド利用者 vs. クラウド事業者

#### 利用者側の不安要素

クラウド利用者は、データおよびアプリケー ションなどの企業資源を外部(クラウド)に移 行することによる「セキュリティおよび環境リ スクの変化」に対して不安を持っている

- > リスク要素が増大するだろうことへの不安
- > リスクが何かを特定出来ないことへの不安

#### 事業者側の論理

クラウド事業者は、データセンタの枠内にお いて、ファシリティを含めたセキュリティおよ び防災対応など対しては、第三者認定など を通して堅牢さをアピールするものの、エン ドツーエンドでのクラウド利用を前提としたセ キュリティ対策および機能サポートについて、 一切責任を負わない立場を取っている。



クラウド利用を前提とした**クラウド・リスク・マネジメント(弊社独自開発)**は、クラウド利用者 が、公表、非公表に関わらず、エンドツーエンドでクラウドを利用する際に懸念される各種 **リスク査定ポイント**を明らかにし、アプリごとの**クラウド利用基準**を設け、その対策案策定 と同時に事業者側への要請の一助として利用されることを目的としている。

# クラウド利用におけるリスク項目と分類

### Pier 1. セキュリティとプライバシ

- 1. データ保護と保全
- 2. ID管理
- 3. 認証
- 4. 物理的、人的セキュリティ
- 5. アプリケーション・セキュリティ
- 6. 脆弱性管理と対策
- 7. インシデント対応
- 8. *プライバシ*

### Pier 2. 可用性と事業継続

- 1. 可用性
- 2. 災害復旧(DR)と事業継続(BCM)

### Pier 3. コンプライアンス

- 1. コンプライアンス条件
- 2. ログとシステム利用状況データ

### Pier 4. 法律と契約の問題

- 1. 知的財産
- 2. 債務
- 3. エンドオブサービスのサポート



# クラウド利用における主なリスクとは...

- 情報漏えいリスク
  - データに対する改ざんおよび破壊などのリスク
- 長時間にわたるサービス利用停止に伴うリスク
  - ▼ エンドューザに対するサービス不履行による賠償責任リスク
  - » 事業継続性に関するリスク
- 国内外の法律およびコンプライアンス違反に伴うリスク
  - ▶ 個人情報保護に関するリスク
  - » 守秘義務違反に関するリスク
  - 内部統制のポリシー乖離に伴うリスク
  - > 知的財産権侵害のリスク
  - ► その他、国内外の法律違反に関するリスク



# 当社独自開発の クラウド・リスクマネジメント・メソッド

	+2.03 +2.03	BES-	There		(本本本(省口四本)	-824	W#.	- 12
項目	740	1007	1000	ラーが開けらいて	LEGAL (AHPIS)		-	<ul><li>・一緒にカラウト軍員を行われる主列所する際、武器会議会に関する技術機</li></ul>
		SECEDIO	202		を表の内具を集のティッ分離について、明確な対抗なとティッチ	: B	- A:	・ 開ルフランに乗用者の研究と利用する(の) 記念指述がに関する(の)の) し家教諭(II) 別記される(記述の) いる音子 (1) 別意信息(関連できまする)
	1	2000000	1	金が快変されていることを明めしているか?		, At .	1995	でには参り、配合のお名類からほとアリングが設ました。
	1 3		1	特に状態のテータ機関				・一般にクラウド事業を必り、ビスだおいて、浄土後級のボーカルをV扱い
				「カラウェ発をは、テータをいかにおいて、作は 「夕散全を明示しているか?	<b>人物の何用者テータについて、下級の項目についての仕憶みやテー</b>	8		についてきるするナース位置とんど家い。のご言葉データのセキュリタン語
	SPORGE		20 202	・作品は他の何思想を一つだ事後がもでいる場	MKとその株会性を体施する仕組みで構造と円度など。株. テータが	-0.	8:	858/萬山県会には、デーサの報金性に構造てビアリンサお登録しい。
				暗号化されて保護されてある9暗号化検皮はどの程度か?	0.0	11.66%		
		ل ا	_	・アウセスに関する部里とアウセス用等学報の社	関する高速とアウセス保等学報の仕組み の背景と本義の助音			
	ターが推進される	$\checkmark$		CHEMIC SENSE CHARLE			-	
		/		*** 花条状態の相関者テータについて、T必の項目についての世権をヤテー			1000	<ul><li>コーセカバのアクセスに関する連集の北領海中級用する事業者はそいが、 が、100円200のコーセデーが配品に関する北部高や選用について開発。</li></ul>
	`			'		101	B	すび事業者は自然の対象(A) 所の対象子と 905のきょうデー電視が高い構成。
				2、関の解析にテークを経過する場合の信頼は・方法		11553	には、データの原本性に関してミアダンフが発生した。	
╵╒═╸╸	<del></del>	$\sim \pm$	عللد	美者の <sup>人</sup>	あまれているかで	- 0	(2)	・データだいがもあるのを取りよう機能量のい可能は明られているが例。 連むもの特別については意义でも多ったが行されている。
	主クラワト	~毒	美			(2)	1165	CONTROL OF THE CASE OF THE CONTROL O
		_	-	· • •	と 第三者が何月春のテータにアクセスすることについての可能		18:	・サウウド事業者が、推議する第三者によるテータデラサルに事業すること。 けられんどもから
中水	麦率は、	1 50	/ Ŧ	中中12	して簡素がれているか?	-0-1	(2.1)	<ul><li>デーラの完全等体については、ララウド等要素がとアリングギャネ構可。</li></ul>
~天才	を坐は、	107	'0个	王/支!( \ ) ~ ~	後前台の可容とその方法を明率しているか?	- 111	-	・日本の海豚をエカカラウド発用矛盾が止った。 かんりと 地名を開北するユー
				V 100 L	ea~nœ	- 07	in .	ぜはほどんと楽したが、美学等権での対応数点を主体の主義ものれてい
				A TOTAL CONTROL OF THE PARTY OF	イリスクを受じなせないことの概要	, vn		COMPANY NESSESTIVE AND SERVICE SERVICES
				テュアに関連リ	る方法・世紀から明本しているまで で明古の流れ1に対する最内方法	D	(3)	・主なりつりと基準の政治があい。日本では、東京となってないが発展が
				ASSESSMENT OF THE PARTY OF THE				as his a
	$\sim$			PO(9フラルサインオン(やつ£ Pレータs	ンセサホートすることの可避とサポートする機能が明明されている。			
				16.7		1,7		
			_	87				
					9) アクセスにおいてすホートしているセキュリティ対策とは?			
	ж	SPAUDID		こ対してリアルを撤走することの「	の アクセスにおいてすホー 34,5いるセキュリティ財体とは? 可容。もしてきるな9歳年化のフォーマッドが対象?(例, SSL,		Til I	
	143 <u>8</u> (43)	SPAUGIO		に対していずりを数定することので がたおいて、フィックングに対体し	の アクセスにおいてすホートしているセキュリティ対策とは? 竹舎、もしてきなの場合をのフォーマッドは何か?(例、881、 に依然未来あるいは数数数数数などを数定することが可能する		<i></i>	ー 用者は、多くのリス・
	34.5k (AU)	GARRES.		ご知っていたする数支することの7 を行わいて、フィックングに対応し をの方はの異体的対処方法はで	の アウミン(よりにマネイ・メルマいる セキュリティ対策とはマ 可含、もしてきるなの場合をのフォーマットが内すで(例、581、 た後見未来るる いけ数数数数数数 などと記述することが可能する (例、エイモ・美術数)		利护	用者は、多くのリスク
	AABE CAUI	SPANCIO		で対していてき数定することの 特において、フィックングに対応し の方性の異性的対応力をはて が立た関して、665日24時間	の アウをえておいてすホール。といるをキュリティ対策とはで 可な。もしてをあるの場合をのウォーマットは対力で(殊、85%。 に使免失失力ないは終免的解決をなどを数定することが可能です (使、二十年失免金) 特別で誘発を変えているがで			用者は、多くのリスク
	[40]	GARRES.	202	で対していて見る数支することので を表して、フィッシングに対象し の方性の異体的対象力をはて を表していていることが可能 異義インコープライド・ピス	91 アクセスにおいてサポートルでいるセキュリティ対策とは? 可多。もいできるの場合ものフォーマットは対力で(例、50%、 が飲み来来するいは飲飲物味が整ちとと数字することが可能を「 (例、二十年来の整」 が終い情報を変わているカラ			
en retsri	CAU	SPPF010	202	に対してVP用を設定することのが を行われて、フィックングに対体し をの方点の異体的状態があった。 を記憶して、456日がイートフラウチャーピス がはスキー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	91 アクセスにおいてサポートルでいるセキュリティ対策とは? 可多。もいできるの場合ものフォーマットは対力で(例、50%、 が飲み来来するいは飲飲物味が整ちとと数字することが可能を「 (例、二十年来の整」 が終い情報を変わているカラ			ー 用者は、多くのリスタ 有してクラウドを利用
ティヒクライイタ	[40]	SPPF010 SPPF020	302	に対してVP用を設定することのが を行われて、フィックングに対体し をの方点の異体的状態があった。 を記憶して、456日がイートフラウチャーピス がはスキー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	9) 子のただにおいてすホールといるをキュリティ対策とはで の、もしできるの場合性のフォーマット対策力で(数、55%。 た他発売乗ることは対象機能を設定さる意味することが可能をつ では、二十年美術を主 物料で誘致性をおっているカラ かといの解析可能と、それが他と分離されているこう りで 対しての長温度をとその概要を表示しているカラ		保	有してクラウドを利用
ディヒプライ ガラ	CAU	SPPFCIO	302	に対していアリを制定することのが を行わいて、フィックングに対体し ののフェルの開始的がたが成ます。 かったに関して、その3日2分割倒 関連オフ・ユーラライベートのラウドイーピス がはスキー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	9) 子のただにおいてすホールといるをキュリティ対策とはで の、もしできるの場合性のフォーマット対策力で(数、50%に、 た他発表来あるいは被動物が激素などを起達することが可能をつ (例、二十年美術教生) 物料で誘動業をおっているカラ かといる解析可能と、それが他と分離されているこう りで 対しての各項類を表えるでの概要を表えしているカラ		保	有してクラウドを利用
ティヒプライ ガラ	CAU	SPPFCIO SPPFCIO SPPFCIO SPPFCIO	302	で対していアリを制定することの1 のにおいて、フィックングに対応して ののはの成別時間がたかかない。 がセスに関いて、60日の4時間 原列イン・フライベートルラウドイーとス がはステートので、70日では大いているが、 のラウィルを制定し、金マの原料を代別ではいて、 後来員の確応すアーターアウセスに対して、規定の のラウィルを制定して、配定事業が表が表がある。 の場合者の批判を指令を発行して、規定の のラウィルを制定して、配定事業を発展を指述して、 を記録者の批判を指令を発展して、 の場合者の批判を指令を発展して、 の場合者の批判を指令を発展して、 の場合者の批判を指令を発展して、 の場合者の批判を指令を発展して、 の場合者の批判を指令を発展して、 の場合者の批判を指令を発展して、 の場合者の批判を指令を発展して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 の場合を表現して、 のまた。 のまたた。 のまた。 のまた。 のまた。 のまた。 のまた。 のまた。 のまた。 のまた。 のまた。 のまた。 のまた。 のまた。	タイプウを入ておいてきホールというをキュリティ対策とは? 可念。もいできるの場合ものフォーマットは対かでは、 が免疫を乗るといけが抗性が発生なども数定することが可能をす では、二十七子素を重 物質が動態をされているカイ などいの情報の数と、それが他が特定れているこ で? いとの手が異ないとなっているか? しされているか? 自分はでいるか? 自分はでいるか? 自分はでいるか?		保	
F12354 K9	CAU	SPPFCIO	302	に対していアリを制定することの) 今において、ウィックソウに対体し、 のの方はの異体的対応が放便する。 やなに関して、4866日24時間 周周オフラー・ブライベールララのチャーとの 別はスキー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	タイプウを入ておいてきホールというをキュリティ対策とは? 可念。もいできるの場合ものフォーマットは対かでは、 が免疫を乗るといけが抗性が発生なども数定することが可能をす では、二十七子素を重 物質が動態をされているカイ などいの情報の数と、それが他が特定れているこ で? いとの手が異ないとなっているか? しされているか? 自分はでいるか? 自分はでいるか? 自分はでいるか?		保	有してクラウドを利用
ティとブライ ガラ	CAU	SPPFOID SPPFOID SPPFOID SPPFOID	312	がしていて見る数定することの を定るいた、フィックングに対す。 のの方はの契約的数を力をはて かなに関いて、その自分が特別 関連イン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	91 アクセンにおいてサポートルでいるセキュリティ対域とはで 内容。もしてきるなり場合をのフォーマットは対象で(例、50%、 が必要素することが可能を「 は原、二々な実験記載」 が終しているができないでしなが、 かといる情報可能と、それが他と仲間なれていることが できないでします。 はたの所に調査をその必要を明ましているか? しされているか? 自治して可能の変数を明ましているか? しされているか? 自治して可能の変数を表すした。 動力は、9でブラス(進月)		保	有してクラウドを利用
ティヒプライ パラ	CAU	SPPFG10 SPPFG20 SPPFG40 SPPFG40 SPFFG40	312 312 312 312 312	で対していアリを設定することのの のであいて、フィックングに対する。 のカナルの契約的が大力をはて かった原理で、466日244時間 用原イン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	91 子のを以ておいてきホールというをキュリティ対策とはで 可念。もいをきなり場合ものフォーマットは対かでは、50年、 に使用来来さないは飲み供給をなども数定することが可能をす では、二十年来の表生 物学で誘致を表示といるカイ などいの情報の数と、それが他と呼吸されていることが、で では、これを表示しているかで 自分にでは何の数と、それが他と呼吸されているかで となったことのなどのまでは、10年で	<del>_</del>	保	有してクラウドを利用
F12797 KB	CAU	SPPFOID SPPFOID SPPFOID SPPFOID	312 312 312 312 312	で対していアリを設定することのの のであいて、フィックングに対する。 のカナルの契約的が大力をはて かった原理で、466日244時間 用原イン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	91 アクセンにおいてサポートルでいるセキュリティ対域とはで 内容。もしてきるなり場合をのフォーマットは対象で(例、50%、 が必要素することが可能を「 は原、二々な実験記載」 が終しているができないでしなが、 かといる情報可能と、それが他と仲間なれていることが できないでします。 はたの所に調査をその必要を明ましているか? しされているか? 自治して可能の変数を明ましているか? しされているか? 自治して可能の変数を表すした。 動力は、9でブラス(進月)		保	有してクラウドを利用
ティヒナラ・イ イラ	(AU) 動物が、Aがでキュリティ (PR)	SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPFFOID SPAFOID	312 312 312 312 312 312	に対していアリを制定することのの を行るいて、フィックングに対すし ののプエの場所的がだったがです。 がセスに関いて、600日24時間 原列オンス・100円で、600日24時間 原列オンス・100円で、600日24時間 原列オンス・100円で、600日24時間 原列オンス・100円で、600円で、100円で を発育の概念ターク・アウセスに対して、規定の のラウィ神事を行って、監察基準を発力を設定 の場合の企業を使うである。 200日によりで、それのかくプロフタイプに では他的である。 では他のでは、100円で、100円で、100円で を終わているので、200円におして、000円で、10	91 子のを以ておいてきホールというをキュリティ対策とはで 可念。もいをきなり場合ものフォーマットは対かでは、50年、 に使用来来さないは飲み供給をなども数定することが可能をす では、二十年来の表生 物学で誘致を表示といるカイ などいの情報の数と、それが他と呼吸されていることが、で では、これを表示しているかで 自分にでは何の数と、それが他と呼吸されているかで となったことのなどのまでは、10年で	<del>_</del>	保	有してクラウドを利用
ディセプライ ガラ	CAU	SPPFG10 SPPFG20 SPPFG40 SPPFG40 SPFFG40	312 312 312 312 312 312	を対していずりを制定することの を定まいた、フィックングに対し、 をの方はの契約的数を力をはて かなに関いて、その自分が特別 用型イフ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	91 アクセンにおいてマホー・シャというをキュリティ対策とは? ウタ・もいできるの場合をのフォーマットは対力?(外、2014、 が使み発表するいは放射性解放量などと数定することが可能を「 を持っているができる。 がある情報を使ったこともから では、一年を表現をしているか? はこの形型をそこの構造を表示しているか? ともれているか? 音楽になぜるだ事をになるが解りなわの影響をもしずか を対し、タイプ2(集内) MPのガイドラインに連続して発覚されているか? わたアフリケーションコードに対して、影像のテスト子戦や禁事・ ディのアフリケーション「コンボーネントについては、解検と目等	<del>_</del>	保	有してクラウドを利用
i 1255 1 K3	(ASI) (ASI セキュリディ (pp) イカラン・ション・セキュリディ	SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPFFOID SPAFOID	32 32 32 32 32 32 32 32	に対していアリを制定することのの を行るいて、フィックングに対すし ののプエの場所的がだったがです。 がセスに関いて、600日24時間 原列オンス・100円で、600日24時間 原列オンス・100円で、600日24時間 原列オンス・100円で、600日24時間 原列オンス・100円で、600円で、100円で を発育の概念ターク・アウセスに対して、規定の のラウィ神事を行って、監察基準を発力を設定 の場合の企業を使うである。 200日によりで、それのかくプロフタイプに では他的である。 では他のでは、100円で、100円で、100円で を終わているので、200円におして、000円で、10	91 アクセンにおいてマホー・シャというをキュリティ対策とは? ウタ・もいできるの場合をのフォーマットは対力?(外、2014、 が使み発表するいは放射性解放量などと数定することが可能を「 を持っているができる。 がある情報を使ったこともから では、一年を表現をしているか? はこの形型をそこの構造を表示しているか? ともれているか? 音楽になぜるだ事をになるが解りなわの影響をもしずか を対し、タイプ2(集内) MPのガイドラインに連続して発覚されているか? わたアフリケーションコードに対して、影像のテスト子戦や禁事・ ディのアフリケーション「コンボーネントについては、解検と目等	<del>_</del>	保	有してクラウドを利用
712 <b>3</b> 54 K 9	(ASI) (ASI セキュリディ (pp) イカラン・ション・セキュリディ	SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPAFOID SPAFOID SPAFOID SPAFOID	312 312 312 312 312 312 312 312	に対していずりを設定することの1 のにおいて、フィックングに対すし ののはの契約的がたがかない。 かなた原して、468日24時間 原型オプライマートフラウがオービス がはステー、168日24時間 原型オプライマースでは、10で原本のはでしまう のラウィ運動をは、金マの原体を代別時にして、 使業員の原語ターク・アウセスに対して、規定の の影響の地が影響のの事で、 である対しませなが、それのかイブはファイブに その影響のとなる。それのかイブはファイブに その影響のとなる。それのかイブはファイブに を発力でいるカファインでは を持つアプラインでは のラウドチービスを得見なれているサードに のデモのいしは終れが成だるます。 フラファイム手間について明末をれているか? フラファイム手間について明末をれているか?	91 アクセンにおいてマホートルでいるをキュリティ対策とは? 可多。もいできるの場合ものフォーマットは対力で(例、50%、 対象が発来することが可能が「 (例、二十年来会配金) 特殊(機能を受わているかで かといの情況を受わているかで かといの情況を受わているかで しての存記を受けるのであるを表示しているがで を対しての存記をそその概念を表示しているがで を対しての行うに属をとその概念を表示しているがで  を対しているかで  自分12年間の MPのカイドラインに連絡して拠虑されているかで わたアプソウ・ションコードに対して、解除のテスド子戦や子戦 ディのアプリウ・ション(コンボーネンドについては、解説と目標  「(例、リービスアップリレ・ド、バッチ物)	<del>_</del>	保	有してクラウドを利用
<b>ディとブライ パ</b> ラ	(ASI) (ASI セキュリディ (pp) イカラン・ション・セキュリディ	SPPFOID SPPFOID SPPFOID SPPFOID SPFFOID SPAFOID SPAFOID SPAFOID	312 312 312 312 312 312 312 312	に対していずりを設定することの1 のにおいて、フィックングに対すし ののはの契約的がたがかない。 かなた原して、468日24時間 原型オプライマートフラウがオービス がはステー、168日24時間 原型オプライマースでは、10で原本のはでしまう のラウィ運動をは、金マの原体を代別時にして、 使業員の原語ターク・アウセスに対して、規定の の影響の地が影響のの事で、 である対しませなが、それのかイブはファイブに その影響のとなる。それのかイブはファイブに その影響のとなる。それのかイブはファイブに を発力でいるカファインでは を持つアプラインでは のラウドチービスを得見なれているサードに のデモのいしは終れが成だるます。 フラファイム手間について明末をれているか? フラファイム手間について明末をれているか?	91 アクセスにおいてサポートもでいるをキュリティ対策とはで 可念。もいできるの場合ものフォーマットは対象で「例。をは、 は使え来来きるいは状態を発生を変することが可能を「 では、二十・モデ教を集 物質・医療を受けることものです。 などいの情報の恋と、それが他と呼ばれていることが、 では、これを必要を表示しているので はなった。これを必要を表示しているので はなった。これを必要を表示しているので はなった。これを必要を表示しているので はなった。これを必要を表示しているので がおけ、タイプ2(集内) メキル、タイプ2(集内) メキル、タイプ2(集内) メキル、タイプ2(集内) メーカンプランクンフェードに対して、解除のテストデ戦や被求手戦 ディのアプリケーションコードに対して、解除のテストデ戦や被求手戦 ディのアプリケーション(コンボーネント)については、解決は同等 では、サービステップワレード、バッチ物)	<del>_</del>	保	有してクラウドを利用
ティヒナライ ガラ	(ASI) (ASI セキュリディ (pp) イカラン・ション・セキュリディ	SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPAFOID SPAFOID SPAFOID SPAFOID	312 312 312 312 312 312 312 312	で対していアリを制定することの1 のにおいて、フィックングに対すし ののはの環境情報を必要ながない。 かなた関係して、60日の4時間 原列スマー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	91 アクセスにおいてサポートもでいるをキュリティ対策とはで 可念。もいできるの場合ものフォーマットは対象で「例。をは、 は使え来来きるいは状態を発生を変することが可能を「 では、二十・モデ教を集 物質・医療を受けることものです。 などいの情報の恋と、それが他と呼ばれていることが、 では、これを必要を表示しているので はなった。これを必要を表示しているので はなった。これを必要を表示しているので はなった。これを必要を表示しているので はなった。これを必要を表示しているので がおけ、タイプ2(集内) メキル、タイプ2(集内) メキル、タイプ2(集内) メキル、タイプ2(集内) メーカンプランクンフェードに対して、解除のテストデ戦や被求手戦 ディのアプリケーションコードに対して、解除のテストデ戦や被求手戦 ディのアプリケーション(コンボーネント)については、解決は同等 では、サービステップワレード、バッチ物)	<del>_</del>	保	有してクラウドを利用
けんこうかん かつ	(AU) 他を持った計セキュリディ (PP) アプリケーション・セギュリディ (AP)	SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID	302   302   302   302   302   302   302   302   302	で対していアリを制定することのの を定まいた、フィックングに対する ののはの原料的製をのかはで、 かとない原して、その自分が特別 用度のファーイランパートリラウドイーとス を見て、この自分が特別 を見て、こので表示をでした。 のラウド車を帯では、全ての原稿を(知円が1に) 従来員の事件をでしまる。配置基準が表示を担合 のラウド車を帯でよる。配置基準が表示を担合 である機能が最初の事件が同じます。 本を含めてプリファークコン関係において、CM 体液化を約でしる力、表合しログックである を持っているファークコン関係において、CM 体液化を約でしる力、表合しログックでクラットデーとスを用まれている方。 フラウドデーとスを用まれているで、 プラウトデーとスを用まれているで、 プラウンタイと新聞について紹示されているかで サーランタイと新聞について紹示されているかで フラウンタイと新聞について紹示されているかで フラウンタイと新聞について紹示されているかで フラウンタイと新聞について紹示されているかで フラウンタイを新聞について紹示されているかで フラウンタイを新聞について紹示されているかで フラウンタイを新聞について紹示されているかで フラウンタイを新聞について紹示されているかで フラウンタイを新聞について紹示されているかで フラウンタイを新聞について紹示されているかで フラウンタイを表示の表示・リファークをアフリファークラフィーを表示の表示・リファークをアファークをアフリファークをアフリファークをアフリファークをアフリファークをアファークをアフリファークをアフトのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでので	91 アクセンにおいてサポートもでいるをキュリティ対域とは? 可多。もいできるの9時年ものフォーマットは対力で(例、50年、 に使用来来るるいは飲み供給をなどと数定することが可能が「 で使用しても来来なる」 からいの無対面を、それがもの分離されているか? を知らいるか? 自分1 で呼吸を使用をしているか? を知らいるか? 自分1 でディンに連絡して発息されているか?  をからいるか?  一番1 で で ブランス・フェードに対して、原係のテストで戦 中不成 アプリケーションコードに対して、原係のテストで戦 で 被吸 不満 ディッグ・シェンコードに対して、原係のテストで戦 マギモ・アのアプリケーションコードに対して、原係のテストで戦 マギモ・ア・のアプリケーションコードに対して、原係のテストで戦 マギモ・ア・のアプリケーションコードに対して、原係のテストで戦 で 大阪 ブラリ・ア・ファップ・ア・ファ・ア・ファ・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア・ア		保	有してクラウドを利用
F1とプライ Kラ	機関的、人間をキュリティ (pp) アフリケーション・をキュリティ (AP) 株式技能をと対策	SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID	302   302   302   302   302   302   302   302   302	で対していアリを制定することのの のにおいて、フィックングに対すし ののはの成別時間がたかなして、 がとない度して、600日24時間 原列イン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	91 子のを入て多いできホームというをキュリティ関係とは? 可多。もいを含むの場合ものフォーマットは対力で(例、50km、 に使え来きなるいは飲食機能を取って、これが自然で では、二・セチ素を全し かといる様態を表示といるので かといる機能を表示といるので したいているので 自動して利用を表現をとその必要を明ましているので を表示といるので 自動して利用を表現をとその必要を明ましているので を表示といるので 自動して利用を表現をとなるので あから、タイプ2(専用)  WPのカイドラインに連絡して発展されているので わたアプリケーションコードに対して、原係のテスト年間や検索を発 では、ガービスアップクレード、バッチ等) リーション・セキュリティの関係系を終っているかで(例、アプリケーンを発 していることに関するエピテンスを発表しているかで 「プリケーンを発力をといる。	<del>_</del>	保	有してクラウドを利用
DF4E59F4 K9	(AU) 他を持った計セキュリディ (PP) アプリケーション・セギュリディ (AP)	SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID	202   202	で対していて見る数定することのの を定るいて、フィッシンがは対し、 をの方はの関係的数を方をはて かでもに関する。その自分が特別 展度のファーララッドインと、 を見ていての自分が表現で、 を見ていての事業をは、全ての情報を(知内が1)に 従来員の確認をつかってのたれに対して、規定の のラウド車を管とよる、配慮選挙の発表を協力 のラウド車を管とよる、配慮選挙の発表を協力 のの他が表現のを研究と、 その他を自分をの方を向かっています。 本を管のアプリケーション情報にあいて、のの 体温化を特でしる力、まるしロフリッケージをを を持っている方。まるしロフリッケージをと を持っている方。まるしロフリッケージをと を持っている方。まるしロフリッケージを を持っている方とで有点ないる方で、 事業をの原発環境において明末をれている方で、 事業をの原発環境において明末をれている方で、 つラウド車を対象が技術と関すコロランとを のラウド車を対象的は関係しているアンリッケークランリルが、のアンリッケークを のラウド車をを対象をはでいる方で、 のラウド車をを対象をはでいる方で、 のラウド車をものが多ネットワークとアフリット それている方を明末しているまで、 の方の手を表示を対象の表示といる方を発表して、ララウ	91 子りを入て多いできホームというをキュリティ対策とは? 可多。もいを含むの場合ものフォーマットは対力で(例、504、 が使用事業者をいけ被動物が動象をどを創定することが可能を「 検索との機能を変わているかで かっての情報を受わているかで を対しての無力調査とその概要を明ましているかで を対しての手力調査とその概要を明ましているかで を対しての手力調査とその概要を明ましているかで を対しての手力調査とその概要を明ましているかで  を対しての手力調査とその概要を明ましているかで  かが、アプリン・シュンニーは、対して、関係のテスト学職を検察学職 ディのアプリケーションニーは、対して、関係のテスト学職を検察学職 ディのアプリケーション(コンボーネントについては、開発は再業で(例、サービスアップラレート、バッチ物)  かージョン・セネュリティの対象系を促っているかで(例、アプリ ハージョン・セネュリティの対象系を促っているかで 同していることに関すること・アファを受明しているかで		保	有してクラウドを利用
ティヒナライ パラ	機関的、人間をキュリティ (pp) アフリケーション・をキュリティ (AP) 株式技能をと対策	SPPFOID SPPFOID SPPFOID SPPFOID SPPFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID SPAFOID	302   302   302   302   302   302   302   302   302	で対していアリを制定することのの のにおいて、フィックングに対すし ののはの成別時間がたかなして、 がとない度して、600日24時間 原列イン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	91子のを2においてきホールというをキュリティ対域とは? 1798. もいできるの場合ものフォーマッドは対力で(例、形式、 1709. ニャに乗換改生 「1709. ニャに乗換改生 「1709. ニャに乗換改生 「1709. ニャに乗換改生 「1709. ニャに乗換な 「1709. ニャに乗換な 「1709. ニャに乗放な 「1709. ニャにルール・ 「1709. ニャル・ 「1709. ニール・ 「1709. ニ	8	保	有してクラウドを利用

# クラウド・リスク・マネジメントの実施手順

- 1. クラウドを利用するに当たってリスク対象となり得るクラウド事業者のサービス内容、 機能などに対し、本資料内のリスク項目によって評価査定を行う。
- ※現時点で未対応の項目があっても将来対応可能かなど、必要に応じて事業者にヒアリングする。
- 2. 全てのリスク項目(全54項目)において、利用者企業がクラウド利用しようとするアプリケーションに対応した重み付けを施し、リスク影響度分析を行い、影響度の評価 (出来れば数値化)を行う。
- ※ここでは一般のリスク・マネジメントのように「頻度」要因を考慮せず、影響度のみで分析する。
- 3. 利用者企業は、利用しようとするアプリケーションごとに、 上記分析を元に、クラウド化の是非に対する総合評価を行う。



### 影響度分析の例

一般的な評価と、適用アプリケーションに対応した評価 (影響度)の両面を査定する。

#### ■ 情報系xxxアプリケーションのクラウド化評価分析

分類	評価項目	一般評価	影響度	コメント
	クラウド事業者のデータセンタは、不特定多数の利用者間の データ分離について、明確な仕組みとデータ保全が保証されて いることを明示しているか?	С	В	データ分離の仕組み、およびデータ保全を 保証するための機能について説明がない
データの保護	クラウド事業者のデータセンタは、停止状態の利用者データについて、下記の項目についての仕組みやデータ保全が明示しているか? ・停止状態の利用者データが蓄積されている場所とその保全性を保証する仕組み(機能と尺度、例. データが暗号化されて保護されてるなら暗号化強度はどの程度か?) ・アクセスに関する認証とアクセス制御手順の仕組み・監査のためのドキュメントの有無	В	В	・停止状態のデータに対する場所の提示は無 ・暗号化による保護機能は現状無しだが 2011/6にサポート予定(AES 256bit) ・アクセスに関する認証方式と手順は明示されている ・監査のためのドキュメントは、ISO27000 ベースがあり参照可能
と保全	クラウド事業者のデータセンタは、稼動状態の利用者データについて、下記の項目についての仕組みやデータ保全を明示しているか? ・ユーザからデータを取得する仕組み・方法 ・設備の移設など、クラウド業者の事由において、別の場所にデータを転送する場合の仕組み・方法	С	В	・稼動状態のデータについて、データの取得 方法が明示され、SFIP、HTTPSでの対応 が明示 ・データ転送についての説明無
	情報漏えい防止に対する対策および機能は明示しているか?	В	A	・ISO27000ベースでの対応のみ

数値化(例): A: 10点、B: 7点、C: 4点、D: 1点

査定を補足するためにコメントは必ず記入する

# クラウド・リスクマネジメントにおけるリスク項目のチェックリスト例

### Pier 1. セキュリティとプライバシ

SPDP010: クラウド事業者のデータセンタは、不特定多数の利用者間のデータ分離について、明確な仕組みとデータ保全が保証されていることを明示しているか?

SPDP020: クラウド事業者のデータセンタは、停止状態の利用者データについて、下記の項目についての仕組みやデータ保全を明示しているか?

- ・停止状態の利用者データが蓄積されている場所とその保全性を保証する仕組み(機能と尺度、例. データが暗号化されて保護されているなら暗号化強度はどの程度か?)
- アクセスに関する認証とアクセス制御手順の仕組み
- ・監査のためのドキュメントの有無と参照の可否

### データ保護と 保全

SPDP030: クラウド事業者のデータセンタは、稼動状態の利用者データについて、下記の項目についての仕組みやデータ保全を明示しているか?

- ・ユーザからデータを取得する仕組み・方法
- ・設備の移設など、クラウド業者の事由において、別の場所にデータを転送する場合の仕組み・方法

SPDP040: 情報漏えい防止に対する対策および機能を明示しているか?

SPDP050: クラウド事業者が利用しているサービスプロバイダなど第三者が利用者のデータにアクセスすることについての可能性とその方法について明示しているか?

SPDP060: サービス終了後の利用者データの完全消去について明示しているか?

# リスクの影響度分析と対応ガイドライン例

#### 1. データ保護と保全

### リスク影響度分析

- 多くのクラウド事業者は、データセンタ内のデータ保全に関する機能や運用内容について全てを一般に公開することはない。
- この分野のリスクは、主にクラウド事業者内部あるいはクラウド事業者に関連している第三者からの「情報漏えい」に代表される。
- 利用者のデータが外部に流出した際に、どのような影響が起こり得るか、を特定し、重要度の重み付けを行う。特に、利用者から見た「顧客データ」が含まれる場合には、重要度を高く設定しなければならない。

### 対応ガイドライン

- ▶ 情報漏えいが事業者側の責務において発生した場合の損害賠償について利用 契約時に確認し、明確にしておく。(リスクの移転)
- 利用者のデータ等の情報漏えいが発覚した場合に、速やかに利用者は顧客に 通知し、対処に関する方法を提示できるよう事業者側と調整しておく。(リスクの 低減と保有)



# クラウドとアプライアンスを 利用した災害対策ソリューション

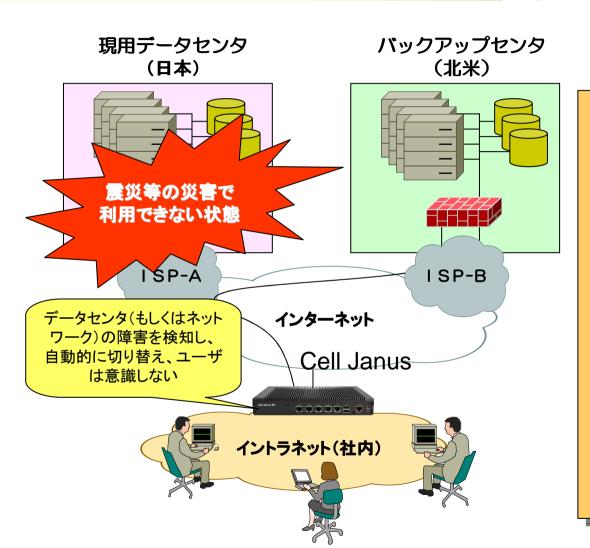


# クラウドを利用した震災対応の仕組み

- バックアップとしてのDR/BCPシステムの提案
  - > Case 1. オンプレミスとクラウドのハイブリッドシステム
  - > Case 2. 異クラウド間のバックアップシステム
    - 現在ニフティクラウドとAmazonEC2でフィージビリティテスト実施中
  - Cell Technology 社のCell Janus シリーズ
    - 本来の機能は、WANの回線のマルチホーミング負荷分散・危険



### Cell Janusシリーズを利用したDR対策



クラウド利用時にも、センタの 冗長構成を取り、震災等、広域 甚大災害時に現用センタが利用 不可な場合に、海外センタなど を利用してバックアップすること で、災害復旧を迅速化し、事業 継続を可能とする。

- ■オンプレミスでは非常に費用 負担の高いDRを、クラウドを利 用することでリーズナブルに構 築可能
- ■Cell Janusをクラウド利用者側に設置し、DNSを含め、切り替え制御を自動的に行う

# ストレージサービスを暗号化運用する!

- データの「貸し倉庫」サービスを安心して利用する
  - > クラウド事業者:ニフティクラウド、AmazonSC3など
  - ▶ 保管するデータは暗号強度の高い国産の暗号方式で暗号化され、特定の認証された担当者とそのPCでのみ復号化できる仕組みが必要
  - FSS: Laurel Intelligent Systems社のICカード利用の認証アプライアンス
  - 震災の影響により、複製データを他の場所に保管しておく要求が増加(海外データセンタに保管したいという要求もあり)

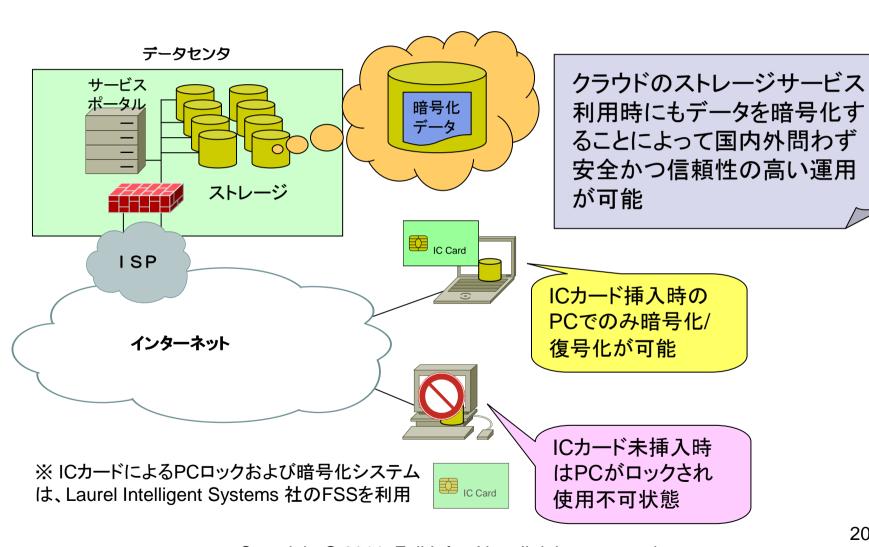


ICカードとICカードリーダライタ



FSSの特徴

# 暗号化ストレージのサービス概要





ご清聴ありがとうございました。

ご質問、コメントなどありましたら、 下記メールアドレスにて、ご連絡下さい。 hayashidatyk@infoxnet.co.jp

また http://www.cloudisms.net/ にもお立ち寄り下さい。

