Fuji Infox
Contributing to the growth of "e-Asia"

【ASIS2011】講演資料

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

Rev.1.01

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*

i. 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

ii. 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。

iii. クラウド利用の場合でも、自社ビルが全停電であれば、クラウドが動いていても、クライアント側が利用出来ないため、システム運用不可。ただし、電源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*

i. 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。

ii. 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

ii. 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

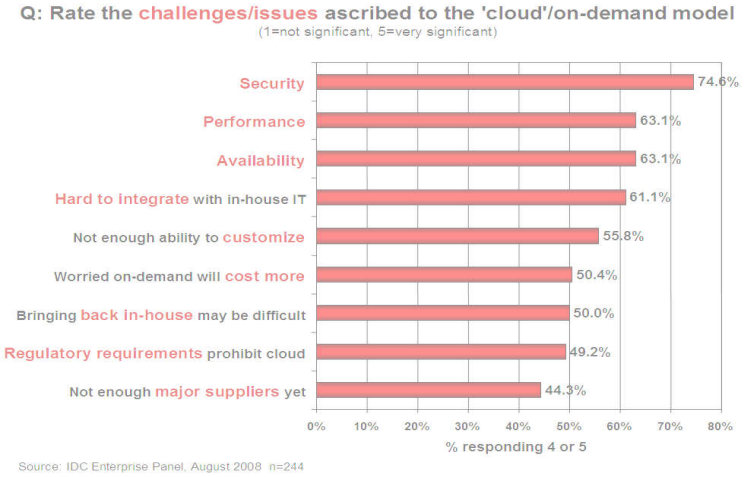
iii. クラウドのデータセンタが正常な場合でも、人的被災により、運用できないケース

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**



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

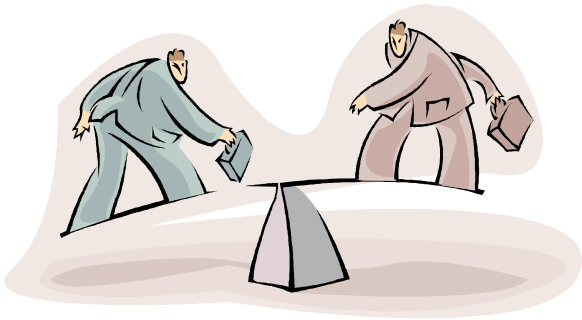
1. 可用性
2. 災害復旧（DR）と事業継続（BCM）

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*
  - *エンドユ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

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
データの保護と保全	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？	C	B	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
	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	B	B	・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
	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	C	B	・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？	B	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

データ保護と保全	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
	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

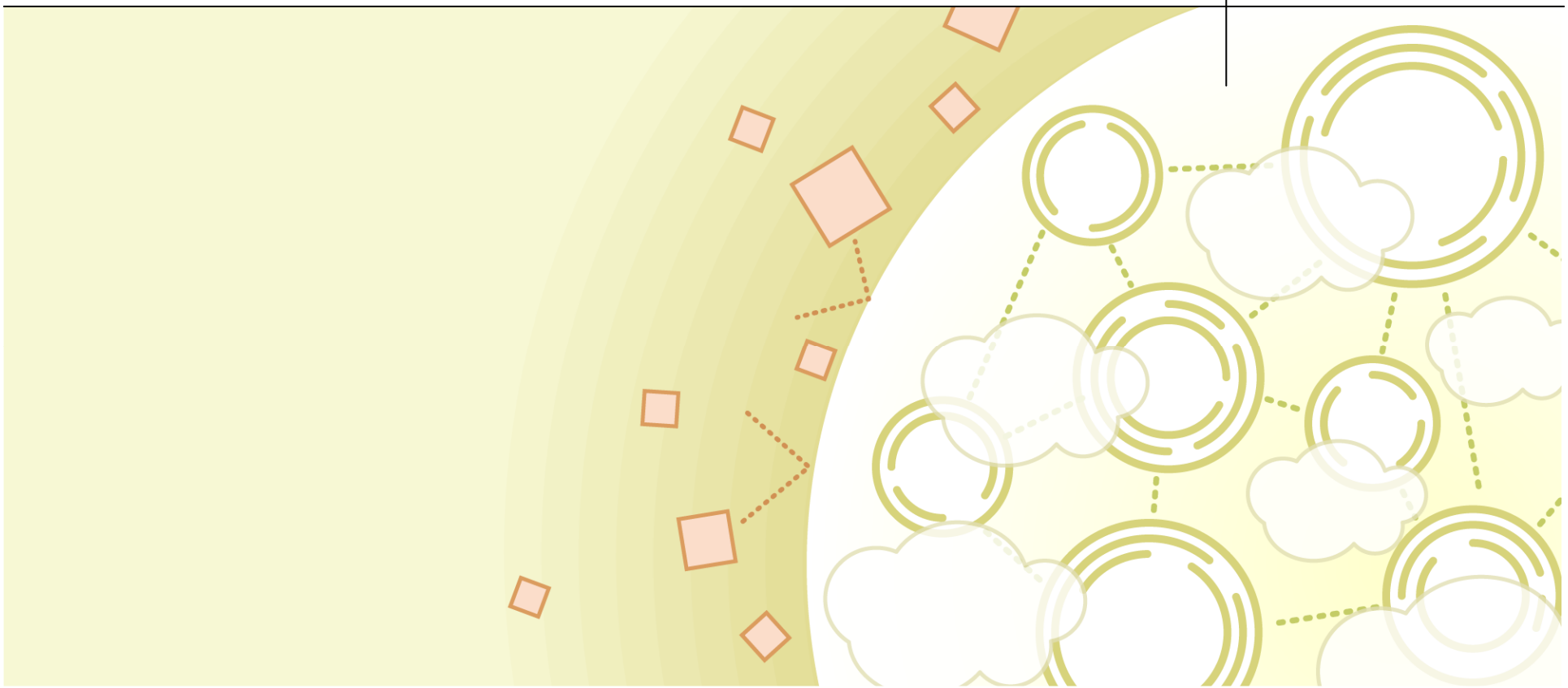
- リスク影響度分析
  - 多くのクラウド事業者は、データセンタ内のデータ保全に関する機能や運用内容について全てを一般に公開することはない。
  - この分野のリスクは、主にクラウド事業者内部あるいはクラウド事業者に関連している第三者からの「情報漏えい」に代表される。
  - 利用者のデータが外部に流出した際に、どのような影響が起こり得るか、を特定し、重要度の重み付けを行う。特に、利用者から見た「顧客データ」が含まれる場合には、重要度を高く設定しなければならない。

- 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）

Fuji Infox

Contributing to the growth of "e-Asia"

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



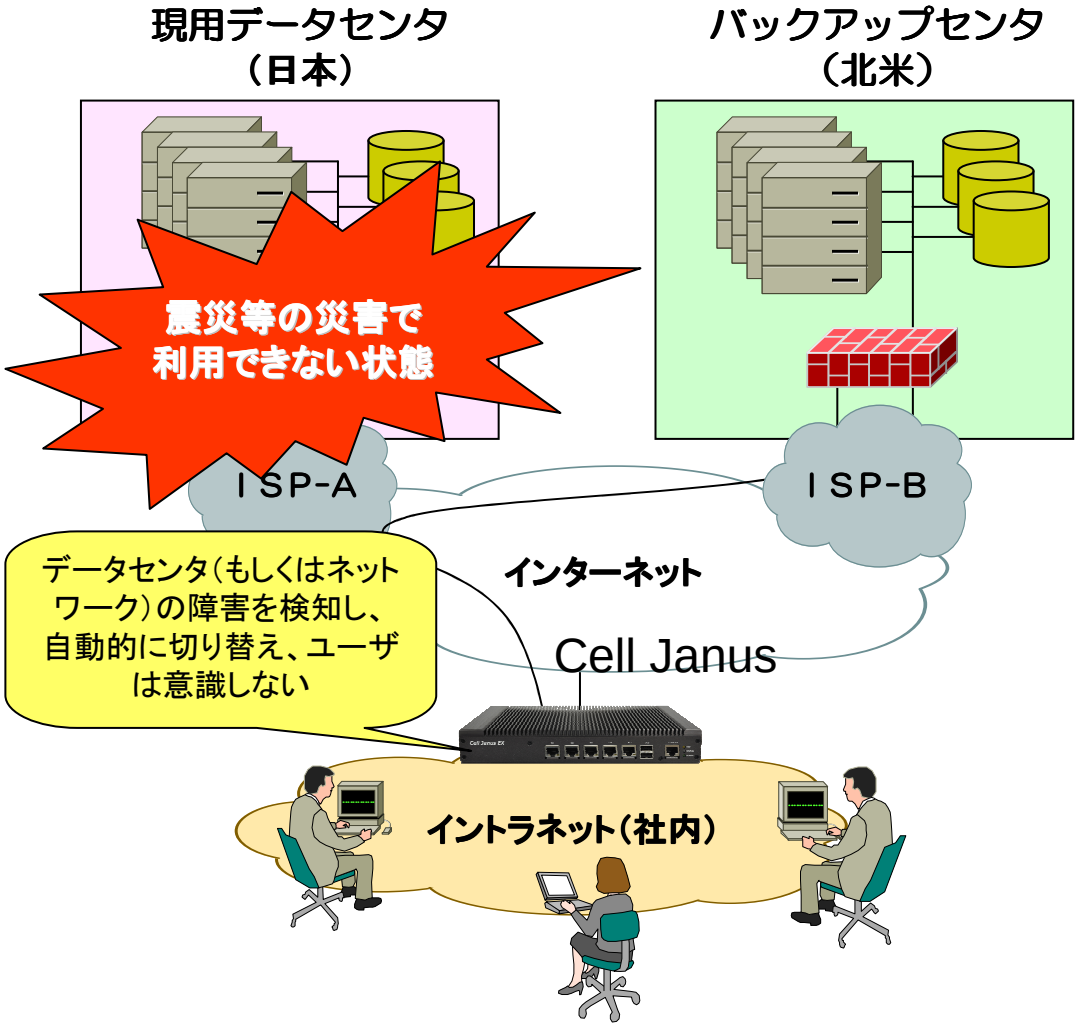
クラウドを利用した震災対応の仕組み

- 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 Technology 社の
マルチホーミングアプライアンス

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

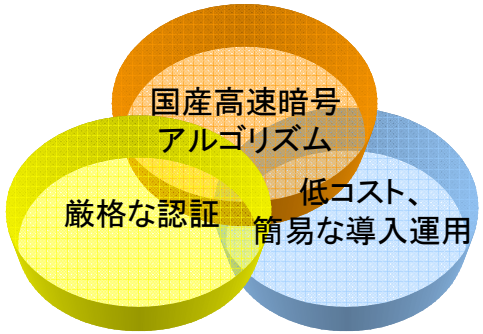
■Cell Janusをクラウド利用者側に設置し、DNSを含め、切り替え制御を自動的に行う

注：両センターのDBの同期の取り方、タイミング、切り替え後の運用は、事前検討が必要

ストレージサービスを暗号化運用する！

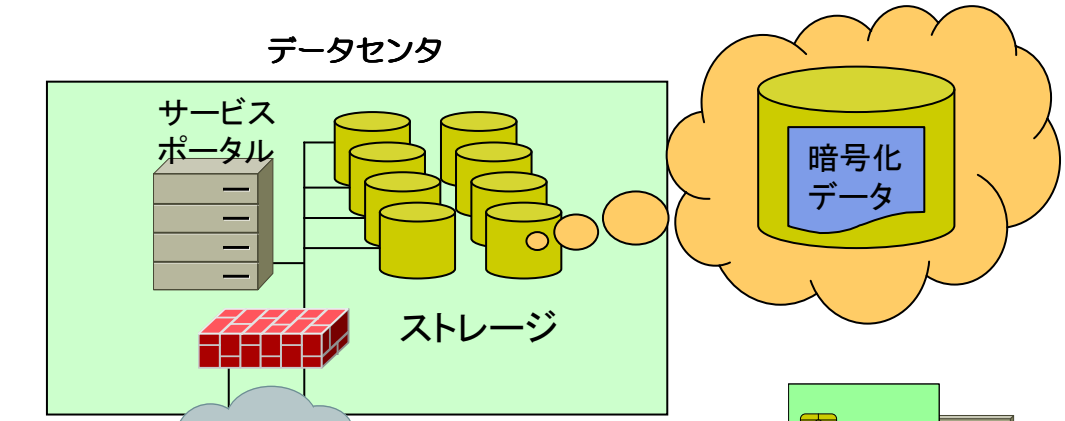
- データの「貸し倉庫」サービスを安心して利用する
  - クラウド事業者：ニフティクラウド、AmazonSC3など
  - 保管するデータは暗号強度の高い国産の暗号方式で暗号化され、特定の認証された担当者とそのPCでのみ復号化できる仕組みが必要
  - FSS: Laurel Intelligent Systems社のICカード利用の認証アプライアンス
  - 震災の影響により、複製データを他の場所に保管しておく要求が増加（海外データセンタに保管したいという要求もあり）

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



クラウドのストレージサービス利用時にもデータを暗号化することによって国内外問わず安全かつ信頼性の高い運用が可能

ICカード挿入時のPCでのみ暗号化/復号化が可能

ICカード未挿入時はPCがロックされ使用不可状態

※ ICカードによるPCロックおよび暗号化システムは、Laurel Intelligent Systems 社のFSSを利用

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。