

第四回「どこでもMYカルテ」研究会

カルテをクラウドに自動分散保管しセキュアにBCP対策

SecureCube / Secret Share のご紹介と、どこでもMYカルテへの展開案

2011年11月21日

NRIセキュアテクノロジーズ株式会社
イノベーション事業本部
Secret Share 事業部

〒105-7113
東京都港区東新橋1-5-2 汐留シティセンター

クラウドがコモディティ化するも、セキュリティ面での不安から、期待以上の利用促進がされていない。クラウドでのセキュリティ基盤となるプラットフォームが提供できないか。

- 「クラウド、クラウド」と言いますが、院内の機密情報を本当にそのまま預けられますか？

- ヒアリングを通じて、よく聞くお話し
 - クラウドは安いとは言ったものの、独自にセキュリティを実装すると割安感も無くなってしまふ。
 - 院長が外出から戻るなり「時代はクラウドらしいじゃないか。どうして、うちはやらないんだ？」と言われても、簡単ではないと説得するのが大変。

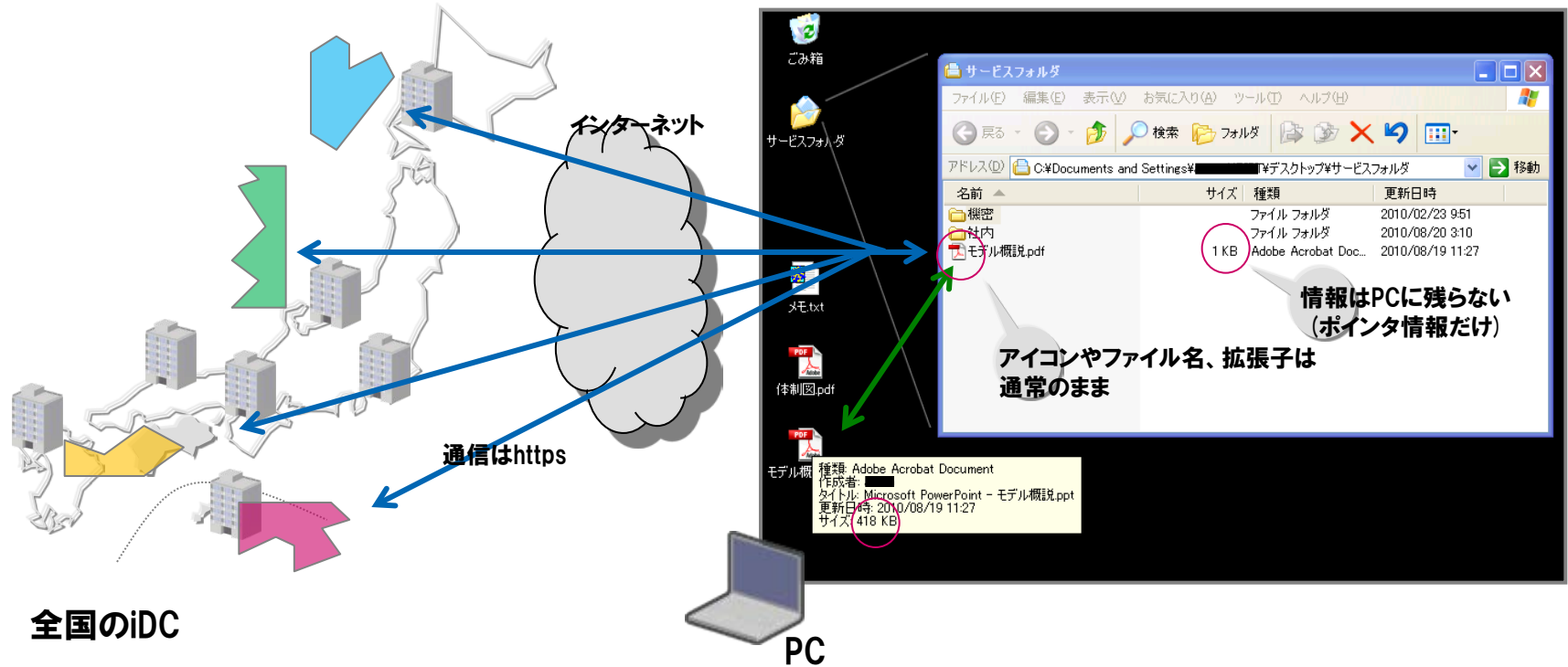
- では、重要な情報を重要でなくしてしまってからクラウドに預けるというのは如何でしょう？

- 例えば、預ける前にファイルの中身をかき混ぜて、引きちぎって、断片を別々のクラウドに預けてしまふ。これが、全自動ならどうでしょう？

クラウドだからこそできた稼働率99.99999%^{※1}を誇る秘密分散ストレージサービス

- 広域災害対策、バックアップ、在宅医療、情報セキュリティ機能も標準

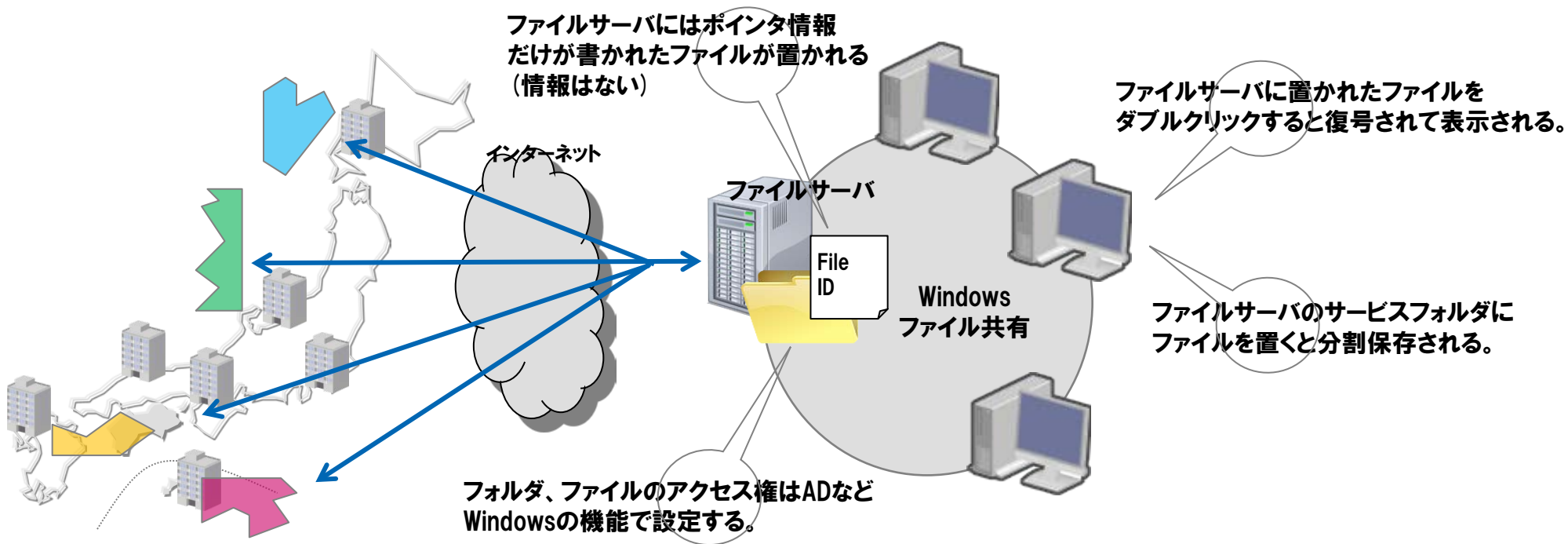
PC上のフォルダにファイルを置くだけの簡単操作
Windowsと見栄え、操作ともほぼ同じ



※1 4分散, 冗長度1, 単一DCの稼働率99.67% (Tier-1, 2相当), 分散片を2セット保管の場合の理論値。
ユーザーサイトのネットワーク障害、Internetの障害は含まない。また、ソフトウェア不具合等による障害も含まない。

ファイルサーバに適用すると、運用コスト削減・将来拡張も容易

- ファイルサーバ上の共有フォルダをサービスフォルダに指定することが可能です。
- ファイルサーバへのアクセス管理は、Windowsの機能により、従来どおり行えます。

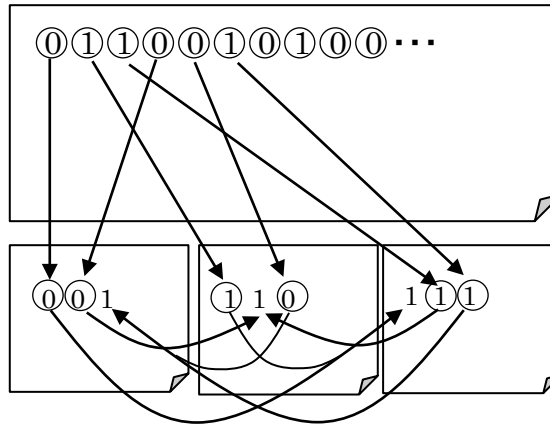


データを分散保管する際に、RAID5に類似したアルゴリズムを採用することにより、データ復元時の可用性を向上。

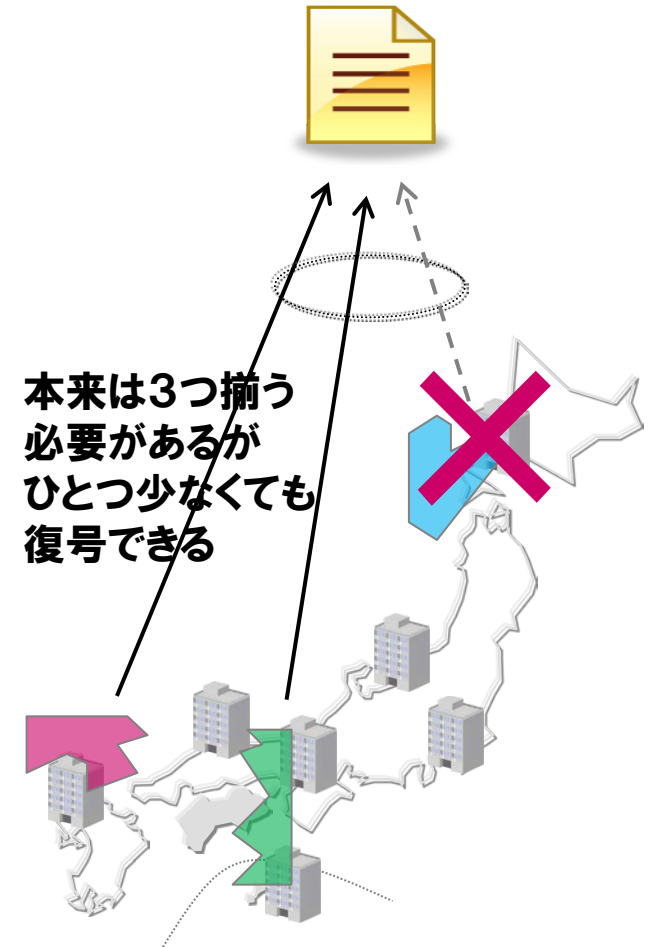
- M個に分散された情報（ファイル）のうち、N個が集まれば情報が復元可能なアルゴリズムを採用（HDDのRAID5とよく似た機能）
 - 例えば、2 out of 3は、個に分散されたファイルのうち、2個が集まれば情報が復元可能

パリティによって2 out of 3を実現する例

注) 実装はこれとは異なります。
理解を助けるための解説です。

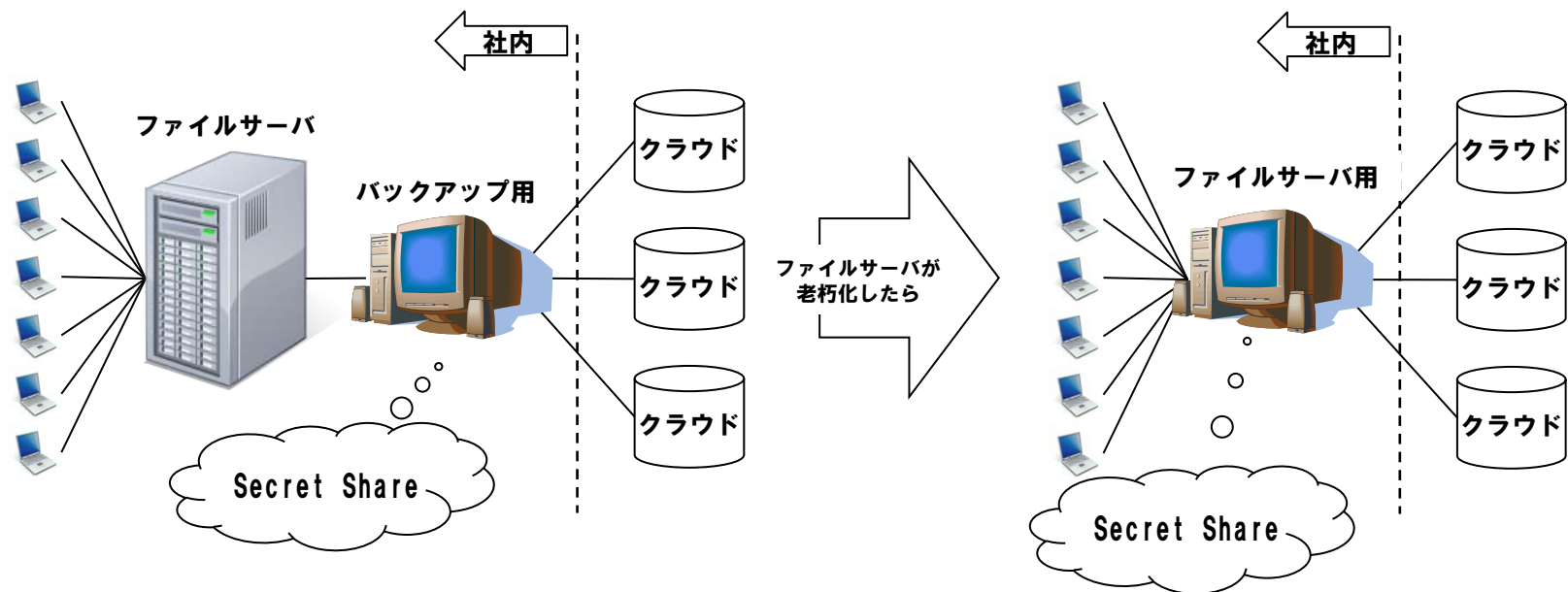


- リアルタイムで自動バックアップされているのと同様であり、DC障害時でも業務継続が可能
- 預け先DCを地域分散すれば、広域災害対策にもなる
- PC故障、紛失時のデータ復旧も可能



ファイルサーバのバックアップ用途としてのSecretShareの利用

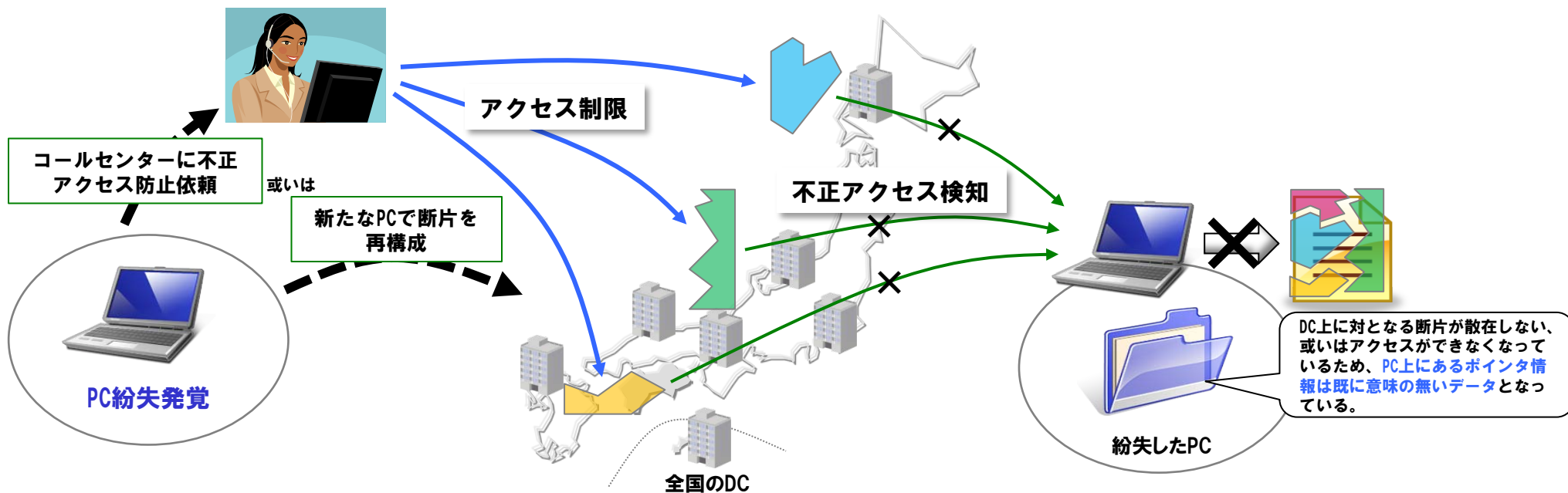
- **まず、既存のファイルサーバのバックアップとしてSecretShareを利用。**
 - SecretShare用サーバは、巨大なストレージを必要としない。
 - ・ バックアップシステムを別途構築するにはコストがかかる。
 - ・ 災害対策機能(DR)を構築するのも大変であるし、切替訓練も容易ではない。
- **将来的には(既存ファイルサーバが老朽化したり、ディスクの大幅拡張が必要になった時には)ファイルサーバをSecretShareに全面的に切り替えることも可能。**



秘密分散を利用したユビキタス環境 ～不正アクセス検知

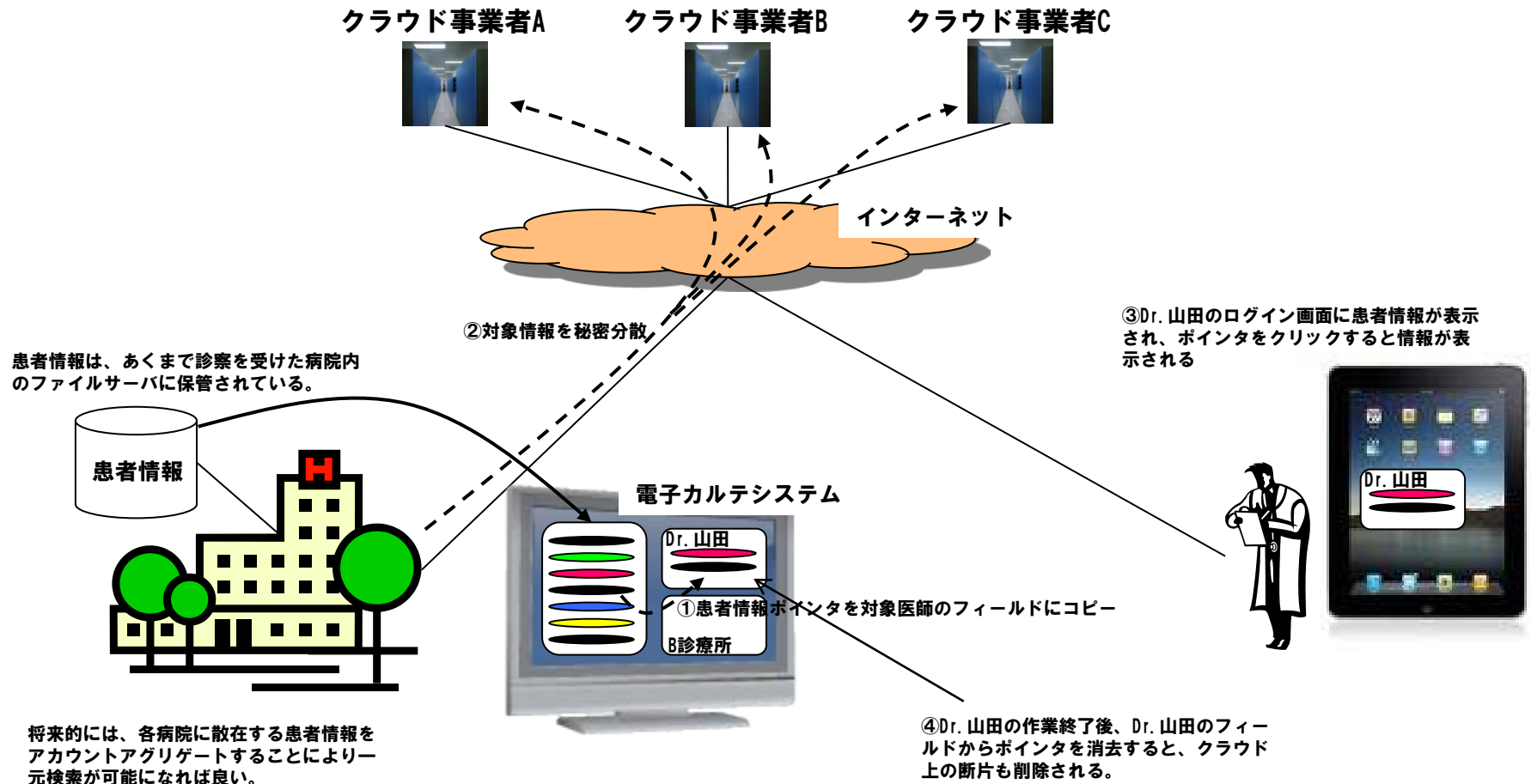
PCを紛失した場合、新たなPCでファイル群を再構成すれば、以前の断片は無効化されるだけでなく、DCで不正にアクセスされたかどうかを検知することが可能になる。

- 暗号化されたファイルを保管したPCを紛失した際の問題点は、そのPCを取得した人物が暗号を解いてファイルを復元したのか、単に廃棄されたのかを知るすべが無い点。
- 秘密分散では、対となる断片がDCに保管されているため、PC取得者が(故意に)ファイルの復元を試みた場合、自動的にDCにアクセスするため、その履歴が把握できる。
- また、PC紛失が報告されれば、直ちにDC上の断片へのアクセスを禁止することにより、第三者によるファイルの再構成を防止することが可能。



NRIセキュアが考える「どこでもMYカルテ」でのサービスイメージ

- 病院に蓄積された患者の情報を指定された診療所や外部の医師に一定期間閲覧可能状態にする。



実証実験を検討しています。ご興味のある方は、是非ご参加を。

- 弊社が考える「どこでもMYカルテ」の仕組みが、業務面でもシステム面でも機能するかどうかを実証実験を通じて検証しようと考えています。
 - 実験のフレームワークを検討する上で、**どういったステークホルダー**にご参加頂くべきか議論。
 - 何を検証し、**どういった課題**が確認され、**どのようにクリア**することによって**実サービスに持ち込む**ことができるかを検証。
 - **ビジネスモデル**の検討。
 - NRIセキュアは、本サービスに必要となる技術実装を併行して実施。
- **賛同いただける事業者様がおられるようでしたら、是非個別にお話しを。**



NRIセキュアテクノロジーズ株式会社

〒105-7113 東京都港区東新橋1-5-2 汐留シティセンター

TEL:03-6274-1055 E-mail:morimoto@nri-secure.co.jp

<SecureCube / Secret Shareのお問合せ> SecretShare事業部 森本・池田・鈴木