Tamias：安全かつプライベートな個人向け分散ストレージ

**本レポートでは、IIJ技術研究所で開発中の個人向けストレージTamiasについて紹介します。
Tamiasは、共有を実現しながらプライバシーを保護し、オンラインデータの不正使用を防止する
強力な認証機構を提供するオープンソースのフレームワークです。**

3.1 はじめに

ディジタルストレージへの移行は、確実に浸透してきています。消費者は、この数十年間でディジタル写真を一般に利用するようになり、それに続いて、音楽ライブラリや個人の動画も加わり、個人用ディジタルデータの量は劇的に増えています。

この膨大な個人用ディジタルデータは、安全に保管する必要がありますが、なんらかの災害に会うまでバックアップの必要性をあまり感じないものです。また、個人用ハードディスクにアーカイブしていても、ディスクが故障してしまう可能性は十分あります。

これに対し、オンラインストレージソリューション（最近ではクラウドストレージソリューション）は、手軽さと安全性などの理由から個人ユーザから高い人気を得ています。また、多くの場合、他のユーザとのデータ共有も備えています。この市場には多くの企業が既に参入していて、脆弱性がない低コストなソリューションだと考えられています。

しかし、これらのソリューションには2つの大きな弱点があります。それは、単独プロバイダへの依存とプライバシー保護の欠如です。単独プロバイダの場合、ユニットの不具合やサービス終了によるデータ消失などの欠点があります。一方、プライバシーの点については、コストに直結しています。無料または低価格で提供されているストレージのほとんどが、運用資金をオンライン広告に頼っています。したがって、広告主向けにターゲット広告用のプロファイルを作成するために、ユーザの個人データを情報マイニングに利用しています。ここで、個人データを検索するのが、ロボットの場合と実際の人間である場合で、違いはほとんどありません。

ここでは、IIJ技術研究所で開発中の、プライベートかつ分散型の個人用ストレージTamiasを取り上げ、そのアーキテクチャーについて紹介します。Tamiasは、通常のオンラインストレージの機能の他に、プライベートできめ細かな共有機能も備えています。後半では、無料のストレージソリューションである、Dropbox[*1]との比較を行います。

3.2 Tamiasアーキテクチャー

Tamiasシステムは、2種類の暗号化によりプライバシー保護の課題を解決している分散型ストレージシステムです。サーバに保存されるデータは暗号化されているので、ストレージサーバをサードパーティでホストしてもプライバシーを守ることができます。その上、分散型アーキテクチャーと消失訂正符号（erasure coding）[*2]の利用により、耐故障性も備えています。各ファイルは、消失訂正符号によって冗長なブロックに分割して保存され、一定数の任意のブロックが集まることで、元のファイルが復元されます。Tamiasは、オープンソースのTahoe-LAFS分散ファイルシステム[*3]をベースに、我々の提案する認証と共有機能を実装しています。

3.2.1 暗号化

1番目の暗号化は、対称鍵によって個別のオブジェクトを暗号化するもので、ストレージ提供者による不必要な解析を防止します。この機能は、Tahoe-LAFSのソフトウェアコンポーネントに実装されています。ここでは、ケーパビリティ

＊1　Dropbox（https://www.dropbox.com）。
＊2　Hakim Weatherspoon氏及びJohn D. Kubiatowicz氏、「Erasure Coding vs. Replication: A Quantitative Comparison.」第1回International Workshop on Peer-to-Peer Systems、2002年。
＊3　Tahoe-LAFS Foundation、Tahoe-LAFS（Least Authority File System）（http://tahoe-lafs.org）。

による分散型のアクセス制御を使っています。ここでのケーパビリティは、オブジェクトの保存位置情報と暗号鍵の組で、元のファイルを復元するための完結した情報です。

Tahoe-LAFSでは、ケーパビリティを渡すことでファイル共有を実現します。しかし、ここにはユーザを認証する仕組みが入っていないため、ケーパビリティさえ入手すれば誰でもそのファイルにアクセスできてしまいます。ケーパビリティが第三者に渡り、更に拡散しても、もはや元の所有者にはどうすることもできません。

このような無秩序な拡散を防いで、きめ細かな共有メカニズムを実現するために、Tamiasでは各ユーザに識別子を与え、このユーザ識別子により所有権を確立して、ケーパビリティの拡散、つまり共有範囲を制御します。ユーザ認証には公開鍵暗号方式を使っています。これが、2番目の暗号化で、ユーザは公開鍵を使って自己紹介し、公開鍵を交換することで交友の輪を広げることができます。

3.2.2 Tamiasにおけるユーザ認証

上記で述べたように、ユーザ認証はTamiasアーキテクチャーのコア部分で、公開鍵暗号方式を使います。公開鍵方式の秘密鍵は署名及び復号用に使われ、公開鍵は、他のユーザと共有され、暗号化や署名照合用に使われます。

ユーザが最初にTamiasに接続すると、ユーザ識別子となる公開鍵ペアの設定を求めます。この際、新たに鍵を生成するか（現行のデフォルトは、RSAアルゴリズムを使った長さ2048ビットの鍵）、あるいは既存の鍵をインポートすることができます。ユーザは、自己紹介を目的として、ユーザ識別子の公開鍵を配布したり、ユーザ識別子を使って複数のデバイスから自分のストレージ空間にアクセスできます。

3.2.3 きめ細かな共有機能

一般に、情報の流出、漏えい、盗難を阻止することは不可能なので、Tamiasでは認証用オブジェクトによってケーパビリティを保護します。このオブジェクトには、ケーパビリティの実体、送信者の識別子、及び正当な受信者の識別子の情報が含まれ、所有者の秘密鍵で暗号署名されます。ストレージサーバは、自身が管理するオブジェクトの所有者の公開鍵を保持し、認証用オブジェクトの署名を検証し、これをコンテンツへのアクセス許可に使用します。このように、所有者の公開鍵は、クライアント側（友人のユーザ識別子）とサーバ側（保管されているオブジェクトに付属）で同時に利用できるため、公開鍵配布のインフラは必要ありません。

公開鍵暗号の特性として、送付先の秘密鍵か所有者の秘密鍵を知らない限り、この署名付き認証情報を偽装したり回避するのは不可能で、保管データのプライバシーは保護されます。つまり、データを要求されたサーバは、要求者のユーザ識別子が認証オブジェクト内の受信者のものであるかを確認します。

3.3 パフォーマンス評価

ここまでで述べたように、Tamiasシステムは、他のオンラインストレージシステムにはない独自の機能を備えているので、このような機能を待たないシステムと比較するとパフォーマンス面で不利となります。

その検証に、ファイルアップロードパフォーマンスをDropboxシステムと比較します。Dropboxは、個人用オンラインストレージシステムで、アマゾンウェブサービス上に構築されており、小容量のオンラインストレージ空間を無料（または大容量のストレージ空間を有料）で提供しています。

今回使ったデータセットは、個人用オンラインストレージの典型的な使用ケースと考えられる、ディジタル一眼レフカメラで撮影した100個の画像です。ファイルサイズの分布を図-1のaに示します。

3.3.1 Dropboxのベンチマーク

評価には、Dropbox APIを使って、100個のファイルをアップロードして削除するスクリプトを作成して用いました。

図-1のbに結果を示します。Dropboxは、アマゾンウェブサービス、特にS3ストレージ[*4]上に構築されていて、テス

*4　Amazon、Amazon Simple Storage Service（http://aws.amazon.com/s3/）。

ト環境では、ほぼ最高性能で動作します。我々の観測では、Dropboxシステムへの1回のアップロード時間は、ファイルサイズに比例しています。その結果をまとめると、次のようになります(エラー率1.5%)。

$$Time_{seconds} = Size_{(MB)} * 0.551 + 3.898$$

この計算では、フィッティングでのエラーが最小となる、25パーセンタイルを使いました。また、90パーセンタイル以上の結果は考慮していません。これは、特定の転送や実行において、アップロード時間が非常に長くなった場合があったからです。測定結果のバラつきは、S3サーバにインターネットを介してデータが転送されることが原因です。つまり、グローバルなトラフィック量によって結果に影響が出るということです。

3.3.2 Tamiasのベンチマーク

次に、現在構築中の実証実験システムを使って、Tamiasシステムのテストを行いました。1つ目のテストは、合計18のノードがすべて同じLANセグメントを共有するという最適条件の下で実行しました。2つ目のテストは、世界各地に分配したノードを用い、実験時にオンラインだった、全部で14個のストレージノード(日本:7、米国:4、スウェーデン:3)を使用しました。

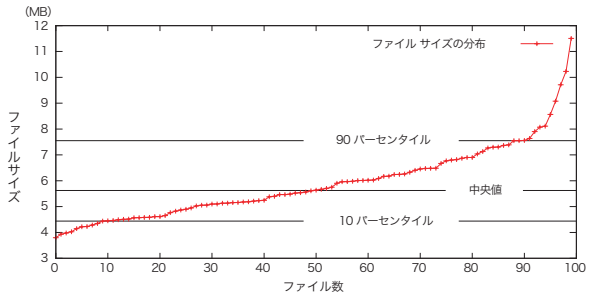
図-2のaは、ストレステスト環境でのTamiasシステムのパフォーマンスを示し、図-2のbは、広域分散テストベッドでの結果をまとめたものです。

これらの2つの結果は、Tamiasパフォーマンスの最善及び最悪のケースを示しています。実際、ストレステスト環境では、すべてのノードが同じLAN上にあり、クライアントとストレージノードの間の最善のスループットが実現できています。それは、アップロード完了までの時間が比例して増えていることからも分かり、まとめると、次のようになります(エラー率1.5%)。

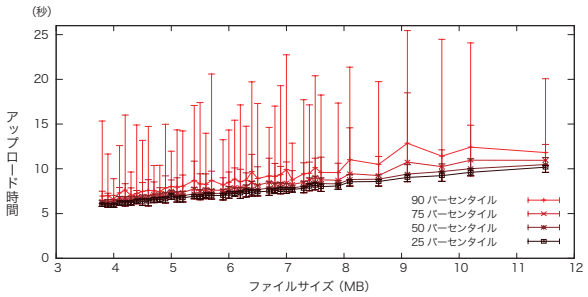
$$Time_{seconds} = Size_{(MB)} * 0.702 + 0.682$$

これを見ると、比例定数がTamiasの場合の方が大きいことから、Dropboxの場合より悪い結果となっています。これは、Tamiasのデータアップロードには、個別のストレージサーバへの転送前に、データの暗号化と消失訂正符号化が行われるオーバーヘッドがあるからです。

デフォルトの消失訂正符号化の設定では、3倍のネットワーク帯域を消費しますが、これによって耐故障性と可用性を

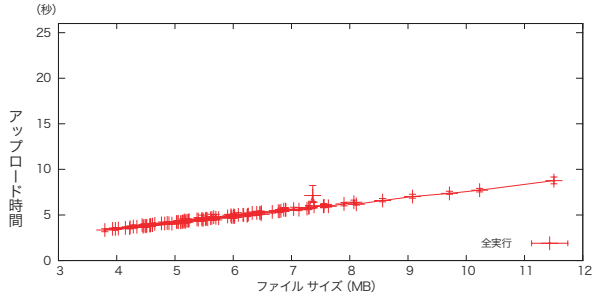


a：実験に使用されたデータセット

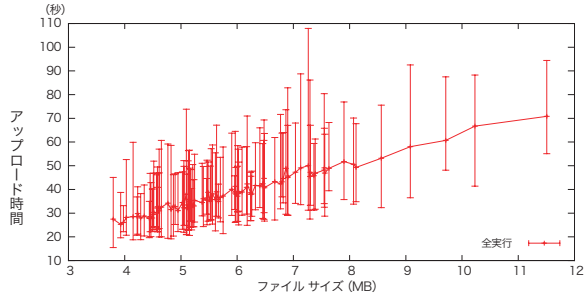


b：Dropbox のアップロードパフォーマンス

図-1 Dropboxベンチマークのパラメータと結果



a：ローカル配備



b：ワールドワイド配備

図-2 Tamiasのアップロード時間

担保できます。いずれにせよ、Dropbox転送に必要なセットアップ時間（一次方程式の定数部分）が非常に大きいので、全データセットに対してTamiasの転送時間の方が短くなっています。

ワールドワイド計測では、ほとんどのノードがNATルータ下のホーム環境にあります。テストベッドのサイズとエンコーディングパラメータについては、アップロードの際に最低1つは遅いノードが使われるように設定してあります。すべての断片ブロックが並行してアップロードされるので、最も遅いノードがボトルネックとなります。つまりアップロード完了までの時間は、この最も遅いノードの転送が完了するまでの時間ということになります。このワールドワイドのセットアップで、アップロード時間の25パーセンタイルでの比例式は、次のようになります（エラー率1.8%）。

$$Time_{seconds} = Size_{(MB)} * 4.903 + 2.114$$

遅延時間の定数部分は、Dropboxより低い値となっていますが、係数部分が大きく、アップロード時間が長くなっています。

3.3.3 スループットの考察

これらの3つの方程式とファイルサイズの分布を使えば、全データセットの転送完了までに必要な平均時間を算出し、実効スループット（この特定のデータセットの転送でユーザが経験するスループット）を導き出すことができます。その結果を表-2に示します。

表-2 実効スループットの比較

	Dropbox	Tamias（ローカル）	Tamias（ワールドワイド）
アップロード時間（秒）	715	482	3105
スループット（KB/s）	845	1252	195

Tamiasパフォーマンスは、ストレージサーバの配置によって実効スループットが決まります。つまり、分散化のトレードオフとして、パフォーマンスが犠牲になるのです。

3.4 まとめ

本レポートでは、Tamiasストレージシステムについて述べました。このシステムは、個人データ用のオンラインストレージシステムで、消失訂正符号と分散型アーキテクチャーによって、高い信頼性を実現しています。また、2種類の暗号化によって、セキュリティとプライバシーが提供されています。

性能評価では、最善の条件下では、Dropboxシステムよりもわずかに優れていることが分かりました。ただし、ストレージノードがワールドワイドに分散されると、予想通りパフォーマンスは落ちます。ユーザは、ストレージノードの配置を慎重に選ぶことによって、コスト（自宅でホストするか、データセンターにある共有ノードを使用するなど）、パフォーマンス（通信性能が高いノードを選択）、及び信頼性（地理的多様性を確保）のバランスをとることができます。以上のことから、Tamiasストレージシステムの付加価値に対するコストは決して高くないといえます。このシステムを友人間で、自宅に置いたノードで利用すれば、低コストで性能も確保できます。

執筆者：

Jean Lorchat（ローシャ ジャン）
株式会社IIJイノベーションインスティテュート 研究員。無線ネットワーク、モバイルアドホックネットワーク、レイヤー2およびレイヤー3モビリティ、最近では、セキュア分散ストレージシステムの研究に従事。2005年にフランス、ストラスブルグ大学より博士号を取得後、慶應義塾大学助手を経て、2008年にIIJに入社。

Cristel Pelsser（ペルサー クリステル）
株式会社IIJイノベーションインスティテュート 研究員。インターネットの経路制御、分散ストレージシステムにおけるプライバシーと認証技術などの研究に従事。2006年にベルギー、ルーヴァンカトリック大学から応用科学の博士号を取得、2007年からNTTネットワークサービスシステム研究所でポストドクター、2009年にIIJに入社。