セキュアな重複排除型マルチクラウドストレージ「Fortress」

Ghassan KARAME　Wenting LI

要　旨

NEC Laboratories Europeのセキュアな重複排除型マルチクラウドストレージは、プライマリストレージの未来像といえます。複数のパブリッククラウドストレージサービスの利用と、キャッシュデータへの素早いローカルアクセスやデータの重複排除、高度なセキュリティ、高い信頼性といった複数のニーズを、非常に低コストで同時に実現します。このため、多くの企業や政府機関、大手通信事業者といった顧客にとって理想的な解決策となります。このソリューションは、セキュリティとストレージ効率に注目しており、パフォーマンスや使いやすさを損なうことなく、データの可用性確保、データの一部が損傷した場合の修復、強力な攻撃者からのデータ保護を確実に行います。結果として、インフラコストを抑え、競争力のあるマージンを確保しつつ、既存のデータセンターのサービスや機能の提供領域を拡張することができます。

KeyWords　クラウドストレージ／機密性／ストレージ効率／重複排除／復元可能性／データ損傷検知

1. はじめに

ストレージやコンピューティングサービス、及びプラットフォーム連携を実現するクラウドサービスは、より身近で重要なものとなり、急速に普及しています。クラウドサービスは、企業にも個人にも、そして公的機関にも大きな経済的利益をもたらそうとしています。アナリストによれば、データストレージの容量は毎年約50%もの勢いで増加を続けています。データストレージの増加分のほとんどは、非構造化データやアーカイブデータです。

そうした一方でクラウドサービスは、アウトソースしたデータの機密性及び完全性に関して、新たなセキュリティ上の脅威をもたらしています。実際、クラウドサービスの利用顧客は自分のデータをコントロールできずにおり、どのようにデータが処理され、保管されるのかについても管理できずにいます。顧客は、こうした点がクラウドサービスを採用する際の大きな障害であることを認識しています。

この問題は、アメリカ国家安全保障局によるPRISM（通信監視プログラム）の存在が突然暴露されたことで注目を集めました。顧客は自分のデータを保護するうえで、プロバイダーに頼れないことが明らかになったのです。内部者による攻撃はよく知られていますが、それに加え、「誠実な」クラウドプロバイダーでさえ、当局によってバックドアのインストールや、顧客のデータの暗号化に使用した秘密鍵の開示などを強要されました。したがって、データを単純に暗号化し[1)]、暗号鍵を保持する既存の一般的なストレージサービスでは、多くの顧客が持つ懸念を払拭するには不十分だと考えます。

NEC Laboratories EuropeのFortressは、この問題に対応し、クラウド利用顧客の懸念を解消できるソリューションです。Fortressは、非常に低いストレージコストと高いパフォーマンスでデータ損傷を防止し、データ修復を自動化して、データの機密性を確保します。Fortressは、マルチパブリッククラウドストレージサービスや、効果的なデータ重複排除、革新的なセキュリティ及び復元可能性技術などを駆使することで、ストレージコストの最小化とセキュリティ保護の最大化を併せて提供します。

その実現のため、Fortressは「クラウド内でのデータ機密保持のための革新的な暗号プリミティブ」と「データの完全性と復元可能性のための革新的なメカニズム」の2つの技術的な柱を組み合わせています。

Fortressの特長を整理すると、以下のようになります。

- 暗号鍵が漏えいした場合でも、複数のパブリッククラウドストレージサービスを利用して、データ

の機密性を保持
- 効果的なデータ重複排除技術を活用して、ストレージ効率を改善
- 新しい復元可能性検証技術を使用して、データ損傷を防止しデータの修復を自動化
- 復元可能性の検証作業で説明責任が果たせる

Fortress独自の特長は、検証可能なサービスを提供できることです。Fortressの利用者は、いつの時点でも操作を検証し、Fortressソフトウェアの正当性について、否認防止のための暗号証明を取得することができます。この機能は、顧客設備にFortressを不適切にインストールしたことによって生じる可能性のある、内部設定ミスに起因したエラーに対して効果を発揮します。

これにより、市場で提供されているほかのソリューション（自社で管理するセキュアなデータセンターであることをうたった高価なソリューションを含め）には実現できない、優れたセキュリティ保証をFortressは提供することができるのです。

このような理由から、Fortressは、保管データに極めて高いレベルのセキュリティを適用したいと考えている企業や政府機関にとって理想的なソリューションであり、ほかのローカルなセキュアストレージソリューションと比べても、ストレージコストを大幅に削減することができます。

続いて第2章では、これまで述べてきたようなセキュリティ上の特長を備えたFortressの技術的な柱について解説します。また、第3章ではFortressの一般的な導入モデルを紹介します。

2. 2つの技術的な柱

Fortressは、2つの主要なセキュリティ上の柱を駆使して、強力な攻撃モデルにおいても機密性と復元可能性を確保しています。最初の柱は、暗号鍵が漏えいした場合でも、NECのプラットフォームを介して既存クラウドに保管されたデータが、高度に保護されることを保証します[2)]。更に、革新的なデータ重複排除技術[3)]を活用し、Fortressは可能な限り低いコストと優れた拡張性を備えた、セキュアなストレージサービスを提供することができます（**図1**）。2つ目の柱は、悪意あるクラウド管理者がかかわったとしても、顧客データを必ず改ざんなしで回収できることを保証します。

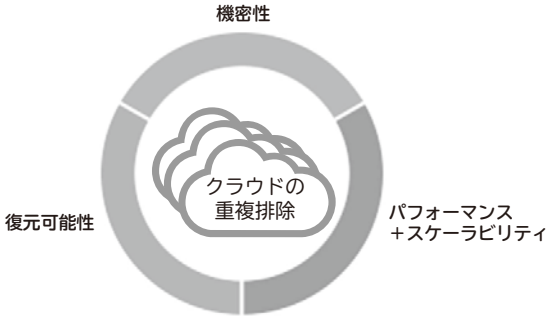


図1　Fortressが提供するクラウドストレージでのセキュリティとパフォーマンスの保証

以下、Fortressのこうした2つの技術的な柱について説明します。

2.1 セキュアな重複排除暗号

暗号鍵を知っており、ストレージサーバの大部分に不正にアクセスすることが可能な攻撃者に対しても、Fortressはデータの機密性を確保できるNECの独自技術を活用しています。Fortressは、暗号鍵の完全な漏えいにも耐え得る、市場で初めてのソリューションです。最近の事例[4)]では、暗号鍵の生成ソフトウェアの欠陥やバックドアの悪用、あるいは暗号鍵を保存しているデバイスへの侵入により、攻撃者はユーザー側からでもクラウド内からでも、暗号鍵を入手できることが分かっています。後者のケースは、管理者/ユーザーによる強度の弱いパスワードの不用意な使用、あるいは設定ミスによるエラーといったシステム上の脆弱性が原因となっている可能性があります。

2.1.1 マルチクラウドに伴う暗号化

NECの技術は、複数のパブリッククラウドの使用と、まったく新しいオールオアナッシング変換とを組み合わせた、特別な暗号プリミティブを採用しています。これにより、もし攻撃者が暗号鍵や大部分の顧客データを不正に入手できたとしても、顧客データが漏えいしないことを保証します[2)]。

NECの技術とAES（Advanced Encryption Standard）のような標準的な暗号プリミティブとを比較すると、AESも複数のクラウドと連携させることができますが、Fortressとは異なり、攻撃者に暗号鍵を入手されてしまうと多くのデータが漏えいすることになります。つ

まり、一般的な対称暗号では、攻撃者（例えば内部者やハッカー）が暗号鍵を入手してクラウドプロバイダーに侵入した場合、攻撃者は侵入したクラウドプロバイダーが保管するすべてのデータを解読できてしまいます。

それとは対照的に、Fortressはまったく新しい暗号プリミティブを用いており、攻撃者がメッセージのほんの一部を読もうとした場合でも、すべての暗号化データ及びすべての鍵材料にアクセスする必要があります。つまり、攻撃者が暗号鍵を何とか入手し、1つのクラウド内のデータ断片にアクセスできたとしても、いかなるデータも手に入れることはできないということです。

Fortressは、既存の標準化されたブロック暗号（AES）をベースに構築されており、既存の暗号プリミティブと比べてもパフォーマンスの低下は3%に抑えられています。

2.1.2 重複排除に伴う暗号化

Dropbox[5]をはじめ多くのクラウドストレージプロバイダーは、ストレージの効率改善のために重複排除技術を利用しています。例えば、アップロードされたコンテンツが、既に他のユーザーによってクラウド内に保管されていることをサービスが認識した場合、重複データによるストレージコストを最小化するために、データの重複排除が強制的に行われます。

最近の調査では、標準的なファイルシステムにおいて、重複排除によりストレージを最大50%節約でき、バックアップアプリケーションであれば、最大90%も節約できることが分かっています。しかし、こうしたアプローチを暗号化されたデータに適用するのは困難です。というのも、ユーザーはそれぞれに異なる暗号鍵を使用して各自のデータを暗号化する傾向があり、結果的にストレージに同じデータが保存されてしまうからです。

Fortressは、これまでにないセキュアなデータ重複排除技術[3]を活用しており、暗号化コンテンツでのストレージ最適化を可能にします。また、異なる（信頼されていないこともある）複数のクライアントが、同じデータコンテンツに対して同じ暗号鍵を入手できるよう、ブラインドBLS署名に基づく忘却型のサーバ支援型鍵生成プロトコルを利用しています。

2.2 セキュアなデータ監査

サービス品質保証（Service Level Agreement：SLA）でデータ損傷まで責任を負うクラウドストレージサービスは、まだありません。クラウドのセキュリティやソリューションの信頼性をうたってはいるものの、既存サービスが保証するのはサービスの可用性だけです。

Fortressは、データ損傷までカバーしたセキュリティSLAを顧客に提供する、市場で初めてのソリューションです。Fortressは、お客様がクラウドに保管したデータの可用性と完全性を、証明可能な方法で検証します[6]。クラウド普及の妨げとなっている主な要因は、顧客がクラウドを信頼していないことと、クラウドインフラへセキュリティ対策を導入するのに高額なコストが掛かることです。

Fortressは、こうしたギャップを埋め、ファイルの状況を常に監視できるという保証を顧客に提供します。

Fortressは、部分的なデータ損傷を検知すると、ただちに修正プロセスを起動し、損傷した情報の修復を行います。一方、外部監査人やユーザーは、データが完全な形で存在していることの証明を受け取ることができます。これによって、プロバイダーの責任が軽減され、クラウド内部の設定ミスによるエラーや管理者の不注意などから保護します。

図2は、Fortressのデータの検証プロセスを示しています。まずFortressは、利用中の各クラウドプロバイダーに暗号で問い合わせを行い、ストレージ内のデータが完全であるかどうか、証明可能で偽造不可能な証拠を取得します。データの損傷/改変が検知されると（つまり、検証が失敗すると）、Fortressは、ほかのクラウドに保管されている情報を利用して自動的にデータを修復します。

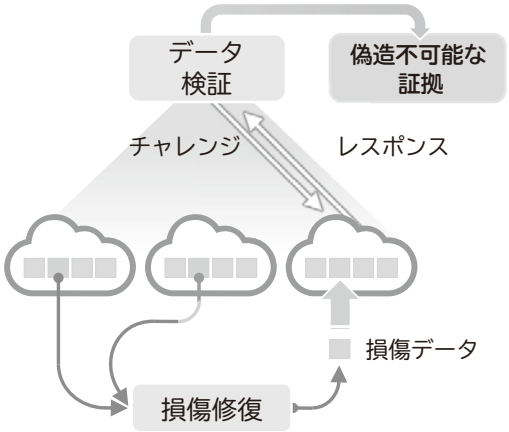


図2　データ検証で損傷が検知された際の自動データ修復

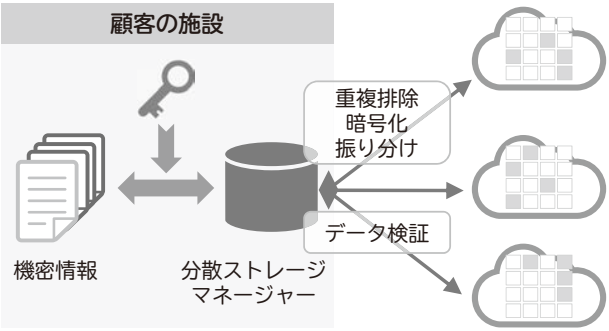


図3　Fortressによって処理されたデータのプロセスフロー

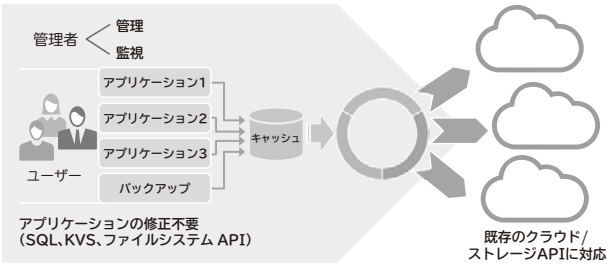


図4　Fortressの導入モデル

データ損失を適切なタイミングで検知するには、頻繁に実施できるよう検証プロセスが十分に効率的である必要があります。この意味で、Fortressでの検証は極めて高いパフォーマンスを実現しています。Fortressであれば、暗号を使ったテラバイト規模のデータの状態監視を、わずか数秒で実行できます。

2.3 まとめ

2つの主要な技術的要素を整理するため、Fortress（分散ストレージマネージャー）がどのように顧客のセンシティブ情報を取り扱っているかについて**図3**に示します。

データの保管を初めて要求されたとき、Fortressはデータの断片を暗号化し、複数のクラウドに振り分けます。そして、必要があれば情報の重複排除を行います。この一方で、すべての保管データについて、Fortressは復元可能性を定期的に検証し、必要があればデータコピーを修復します。

3. 導入モデル

Fortressはソフトウェアレイヤの製品であり、通常、顧客の施設に設置された普及型サーバにインストールされます。Fortressは、標準APIをそのまま修正せずに使用して、AmazonやOneDrive、Box.com、Dropboxといった既存のクラウドプロバイダーとのインタフェースを行います。また、FortressはWebDav準拠のクラウドにも対応しています。

図4で示すように、Fortressは、顧客のアプリケーションが発する、データをディスクに保存するための命令をすべて傍受し、クラウドへリダイレクトします。Fortressへ送られたファイルはすべて、処理され、適切に暗号化されてからクラウドに保存されます。Fortressの技術は、AESやRSAなどの標準の暗号プリミティブをベースにしています。

Fortressは、標準ファイルシステムAPIをはじめ、SQL、キーバリューストア（KVS）などのインタフェースを使ってアプリケーションとの連携が可能です。もちろん、顧客の要望に応じて、ほかのアプリケーションインタフェースに対応するように拡張することもできます。

更にFortressは、パフォーマンスが優れていることから、普及型サーバでの運用に適しているだけでなく、IoT（Internet of Things）デバイスのソフトウェアスタックと統合することができ、こうしたデバイスのストレージをクラウドにまで安全に拡張することが可能です。

4. 最後に

Fortressは、多くの企業や大手通信事業者、政府機関といった顧客のための安全で高パフォーマンスなクラウドストレージソリューションです。Fortressは、データの機密性の強化、ストレージの効率向上、及びデータ損傷検知とデータ修復のための検証可能なサービス提供などに貢献します。

Fortressは、NECのプラットフォームを介して既存のクラウドに保管された機密情報を、たとえ暗号鍵が強力な攻撃者に漏えいしたケースに対しても、高度に保護することを約束します。たとえ悪意のあるクラウド管理者がかかわったとしても、Fortressは顧客のデータをいつでも改ざんなしに復元できることを保証します。また、部分的なデータ損傷がある場合には、情報を自動的に修復します。

これらの機能によって、Fortressは、自社設備によるセキュアなデータセンターを売りにしている高価なソリューションをはじめ、市場のほかのソリューションには真似できないセキュリティを保証できるのです。

---

*Dropboxは、Dropbox, Inc.の商標または登録商標です。
*OneDriveは、米国 Microsoft Corporationの、米国およびその他の国における登録商標または商標です。
*その他記述された社名、製品名などは、該当する各社の商標または登録商標です。

参考文献

1) K. Beer, R. Holland：Encrypting Data at Rest, White Paper of amazon web services, 2014.11
2) G. O. Karame et al.：Securing Cloud Data in the New Attacker Model, 2014
3) F. Armknecht et al.：Transparent Data Deduplication in the Cloud, CCS' 15, 2015.10
4) Wikipedia：Edward Snowden, http://en.wikipedia.org/wiki/Edward_Snowden#Disclosure.
5) Dropbox：www.dropbox.com.
6) F. Armknecht et al.：Outsourced Proofs of Retrievability, CCS' 14, 2014.11

執筆者プロフィール

Ghassan KARAME
Senior Researcher
NEC Laboratories Europe
NEC Europe Ltd.

Wenting LI
Research Scientist
NEC Laboratories Europe
NEC Europe Ltd.

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.68 No.3　新たな価値創造を支えるテレコムキャリアソリューション特集

新たな価値創造を支えるテレコムキャリアソリューション特集によせて
変革期を迎えたテレコム産業に向けたNECのソリューション

◇ 特集論文

ネットワークに新たな価値を提供するSDN/NFVソリューション
SDN/NFVソリューション技術体系
ネットワークのインテリジェントな運用管理を実現するMANO技術
vEPCにおけるユーザープレーン制御の実現
付加価値の高いMVNOビジネスを支援するvMVNO-GW
通信事業者向け仮想化IMSソリューションへの取り組み
NFVで実現するIoTネットワーク
通信事業者向けトランスポートSDNソリューション
通信事業者の収益向上を実現するトラフィック制御ソリューション（TMS）
トラフィック制御ソリューション（TMS）の要素技術

トラフィックの増大に対応するトランスポートシステム
大規模データセンター向けOpenFlowイーサネットファブリック
増大するトラフィック対応に向けた10G-EPONの開発
大容量基幹ネットワークを支える要素技術とマルチレイヤ統合トランスポート装置
光デジタルコヒーレント通信技術の開発
光海底ケーブルシステムを支える大容量光伝送技術

無線アクセスの高度化に対応するワイヤレスソリューション
ロシアでの通信事業者向けネットワーク最適化プロジェクト
サウジアラビアモバイル通信事業者向け大容量無線伝送システムを実現するiPASOLINKソリューション提案
世界最高の周波数利用効率を実現する超多値変調方式用位相雑音補償方式の開発
モバイル通信の高度化を支える高密度BDE

通信事業者向けICTソリューション
NEC Cloud Systemの競争力強化とOSSモデル構築SI技術への取り組み
会話解析ソリューションの通信事業者への適用
止まらないキャリアシステム開発への取り組み
通信事業者の業務を下支えするビッグデータ分析基盤

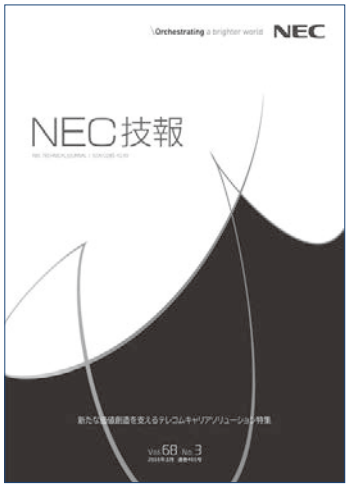
◇普通論文

セキュアな重複排除型マルチクラウドストレージ「Fortress」

◇ NEC Information

C&Cユーザーフォーラム&iEXPO2015　Orchestrating a brighter world
基調講演
展示会報告

NEWS
2015年度C&C賞表彰式開催



Vol.68 No.3
（2016年3月）

特集TOP