信頼できるクラウドストレージの実現に向けて

Dan Dobre　Joao Girao　Ghassan Karame

要 旨

映像配信やEメール、ファイル共有など、パブリッククラウドはオンラインサービスを柔軟に展開する手段として広く利用されています。その一方で、機密データをパブリッククラウドに預けることにはいまだに多くの企業が抵抗感を抱いています。これは、信頼できないクラウドサービスプロバイダにてデータを保管することにセキュリティ上の問題があるからです。本稿では、クラウド基盤のセキュリティ、サービスの可用性、利用者のプライバシーや保管データの機密保持などを保証する一連の最先端技術について、欧州研究所の独自技術を交えて解説します。最後に、これら多様な技術を1つの多目的クラウドサービスに統合した「サービスイメージ」を紹介します。

KeyWords
クラウドへの信頼性とセキュリティ／クラウド攻撃者モデル／マルチクラウドストレージ／
ビザンチン脅威モデル／All-or-Nothing Transformation／Honest but curious Cloud

1. まえがき

企業や個人そして行政が、コスト削減の手段としてクラウドサービスを展開、提供、利用し、それが驚異的な経済効果をもたらし、クラウドコンピューティングを成功へと導きました。今日、数々のアプリケーション分野で、クラウドの重要性と適用性はますます高まっています。データにアクセスし、保管して計算する、その手段を構築することにより、クラウドはビジネスに多大な利益をもたらしています。EメールやSNS（Social Networking Service）などへのアクセスを提供するビジネスは、2020年までにはそのビジネス単独で数十億ドルになるであろうと、調査会社のフォレスターリサーチは予測しています。

クラウドやクラウドを利用したサービスの有用性や規模が増すほど、それらのコンポーネントを不正利用したり、悪用、攻撃したりする動機付けが更に増えるのは明らかです。実際、Dropboxは盗難パスワードを使ってのアカウントへの不正アクセスがスパム攻撃につながったと主張しています。AmazonやGmailでは機能停止によって、サービスにアクセスできないだけではなく、AmazonやGmailのクラウドシステムに依存しているサービス（第三者パーティが提供するサービスを含める）にも影響を及ぼし、数百万の利用者の不満を招く結果となりました。

同様に、クラウドサービスの可用性、その基礎となるクラウドインフラのセキュリティ、クラウドサービスプロバイダそしてその利用者のプライバシーを脅かすケースが、数多く文献で報告されています。実際、欧州政策研究所（Centre for European Policy Studies：CEPS）[1]は、最近の研究で、現在のクラウド技術ではセキュリティに対して十分な対応がなされていないと結論づけ、更に、「クラウド上のコンテンツに対するプライバシー対策は無視されてはいないにしても、軽視されている」と強く主張しています。

本稿では、既存のクラウドの堅牢性やセキュリティを高めるためのソリューションを考察します。すなわち、現実的なクラウドへの攻撃者モデルに即して、多数存在する最先端技術の詳細な分類を示し、それに即してNECの欧州研究所の独自技術も紹介します。最後に、これらのさまざまな技術を、多様な目的に対応できる1つのクラウドサービスに統合する「サービスイメージ」を紹介します。

2. 脅威モデル

この章では、クラウドに関してしばしば考慮されるいくつかの脅威について紹介します。第3章でも言及しますが、

攻撃モデルの強度が具体的なソリューションの方法を形作り、リソースの効率性や性能も含め、各ソリューションのアプローチの設計や複雑さに影響を与えます。

2.1 応答しないクラウド

クラウドサービスプロバイダはクラウド基盤の信頼性を確保するため、相当量の資金を投資しているにもかかわらず、多くのプロバイダは今も機能停止に悩まされており[2]、データ利用に障害を来しています。クラウドストレージサービス自体が機能停止に陥らない場合でも、接続障害（例えばネットワーク分割）や利用者にとって不利となるような予想外の契約変更（プロバイダによる顧客の囲い込み）などが、利用者のデータ利用を妨げています。クラウドストレージサービスに依存した最近のアプリケーションの多くは遅延の発生に弱く、データが一時的にでも利用できなくなると、深刻な被害を受ける恐れがあります。データストレージサービスの機能停止やネットワーク機能の停止は、通常無応答クラッシュ（Non-Responsive Crash）モデルに分類されるケースで、ストレージサービスのどれかがクラッシュによって停止したり、ネットワークのどこかがタイムリーにメッセージを送信できなくなったりしています。専門的には、そのような動作（誤動作）に対応できるプロトコルで書かれたストレージは、クラッシュ耐性がある（crash fault-tolerant）、という言い方をします。

2.2 覗き見するクラウド

クライアントの機密データがクラウドシステムの外へ漏れるという事態が頻繁に起こっています。これらは、(1) 顧客の機密データを、高値を払う用意のある第三者に漏えいしかねない、不正なクラウド及びITサービス事業者や、(2) クラウドシステムや設備の中への侵入（ハッカーやマルウェアなど）によって引き起こされています。

こういうクラウドには、それ自体に悪意がなかったとしても、クライアントデータの機密性の確保という点では、完全な信頼を置くことはできません。このケースは、前述の「クラッシュ」モデルを包含する、覗き見（honest but curious）脅威モデルに分類されます。

2.3 利己的なクラウド

覗き見モデルとは異なり、利己的なクラウド（rational cloud）は、有用なサービスとしての機能を装いつつ、自らの利益を最大化しようとする信用できないクラウドです。例えばクラウド運営者が、(1) 表向き主張しているよりも低い冗長度で、あるいは (2) 要望と異なる（ストレージコストがより安い）場所に顧客のデータを保管するなどがこれに当たります。更には、ターゲット広告や関心を持つ第三者のために、ログデータのアクセスパターンを解析してクラウド利用者をプロファイルしたりします。明らかにこれは、指定した振る舞いから意図的に外れる動機をクラウドが持っている恐れがあるという点で、「覗き見」モデル（crash and honest but curious）より格段に深刻なモデルです。

2.4 悪意あるクラウド

ビザンチンクラウド（ビザンチン帝国で権謀術数を尽くして抗争を続けた将軍たちにちなみ、こう呼ばれる）は、自分が経済的損害を被ってでも、あり得る限りの悪事をクラウドが行うと想定している点で、我々の知る限り最も厳しい脅威モデルです。ビザンチン攻撃は、クラウド基盤やサービスの脆弱性に対する内外どちらからの攻撃でもあり得ます。ビザンチン脅威モデルには、「利己的なクラウド」の不正行為を含む全てのタイプの不正行為が分類されます。ビザンチンな振る舞いの例としては、データの整合性や機密性を大規模に、かつ公然と損なうことが挙げられます。ビザンチンクラウドに対処する際の主な困難の1つは、ビザンチンな振る舞いをする構成要素の数を、いかにして一定期間にわたって、ある数以下にとどめるか、ということです。

3. セキュアで信頼できるクラウドの実現

この章では、第2章で述べた脅威モデルに対するソリューションの分類について説明します。第4章では、これらの個々の技術をどのように1つのフレームワーク内へ統合するかについて紹介します。

3.1 応答しないクラウドへの対処

個別のデータストレージサービスの機能停止に対応するため、複数のストレージクラウドを同時に使う（**図1**）ことに依存した手法がいくつも存在します。主な課題の1つは、障害が起きたり、共有データに同時にアクセスが起きる場合にも、高い可用性と強い整合性を確保することです。クライアントに提供する基本機能は、Read/Writeストレージインタフェースです。これは、近年のクラウドストレージサービス

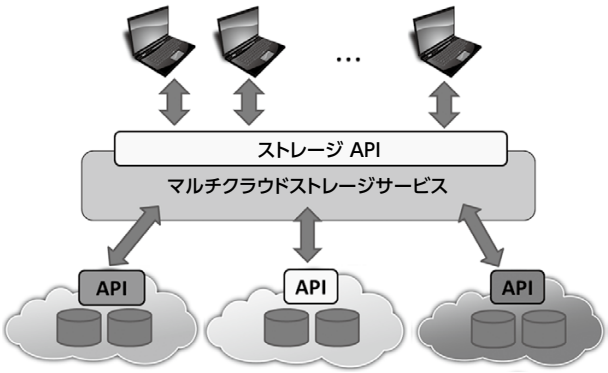


図1　マルチクラウドストレージサービスの概略

のデファクト標準となっている、Key-Value Store（KVS）のAPIの中心を占めるものです。

最近の研究の多くが目指すところは、マルチストレージクラウド上で（RAIDで行われるような）データの複製とストライピングを行うことで、高い可用性と強固な一貫性を実現するクラウドストレージ基盤です。これらの研究は個別のクラウドが提供するKVS APIに依存しています。そういうAPIは通常、*op* ∈ *{Put, Get, Delete, List}*などの基本操作、更により高度な条件付きオペレーション*Conditional <op>*などで構成されています。条件付きオペレーションは基本操作とは異なり、全てのクラウドストレージプロバイダがサポートしているものではありません。しかしながら、条件付きオペレーションは、高い一貫性を持ったデータへのトランザクションアクセスを可能にするので、多くのストレージサービス事業者（例えばWindows Azure Storage、Yahoo! Peanuts、Amazon DynamoDB など）では既にサポートされています。

最近の研究では、Libdeh他がマルチクラウドストレージシステム、RACSを提唱しています[14]。このシステムでは、データは、基本的なKVS APIを提供している一群のストレージクラウド上でストライピングされます。RACSは、クライアントとストレージクラウド間の全てのインタラクションを仲介する外部調整サービス（つまりプロキシ）に依存しています。Basescu他は、IBMが実装したマルチクラウドデータ共有サービス、ICStoreについて述べています[15]。データへのアクセスは、複数のクライアントがクライアント間通信なしに連携する、非集中的な方式で行われます。（論理的に）集中管理されたプロキシサーバを全てのリクエストが流れるRACSとは異なり、ICStoreのスケーラビリティの上限は、そこで使われている個々のストレージクラウドのスケーラビリティのみによって決まります。また、RACSはクラウド上のデータをストライピングしてストレージのコストを抑えていますが、ICStoreはデータ複製方式を採用しています。更には、ICStoreは、ネットワーク障害や、一部のクラウド及び任意の数のクライアントのクラッシュ障害の際にも強い整合性（つまり読み出しは常に最新の更新結果を返す）と、高い可用性を備えています。最良の場合、ICStoreは、保管されたそれぞれのデータ項目に対して、1つのクラウドごとに2データ項目のストレージオーバーヘッドを発生します。これは、単一のクラウドによるソリューションの2倍の要求です。最悪の場合、各保管データ項目について、データ項目を更新する権利を持つクライアントの数に比例した量のストレージオーバーヘッドが必要になります。

3.1.1 NECの特許技術「MCStore」

NECは、既存のマルチクラウドストレージソリューションで発生する使用スペースの軽減を可能にする特許技術を開発しました。Chockler、Dobre、及びShraer[16]が提唱したMCStoreは、個別のクラウドにおける条件付きPutをうまく使ったマルチクラウドストレージサービスであり、常に一定のスペースオーバーヘッドを実現します。各データ項目に対して、クライアントの数に関係なく、MCStoreはクラウドごとに1つのデータ項目を保管するよう要求します。更に、操作ごとのクラウドへのアクセス数で計測したMCStoreのレイテンシ（遅延時間）は、同時アクセスするクライアントの数によって増減します。その結果、同時アクセスがないとき（つまり通常）は、MCStoreは1操作につき2クラウドアクセスという最適なレイテンシを実現します。

3.2 覗き見するクラウドへの対処

覗き見するクラウドに対抗する数々のソリューションが文献で取り上げられていますが、これらのソリューションのポイントは、単独のクラウド運用者にはアクセスできない暗号鍵を使った効率的なデータ暗号化です。そこで主に問題になるのは、キーマネジメント（鍵の管理）です。

覗き見するクラウドに対抗する暗号鍵の管理には大きく3つの方法があります。最も単純な方法は、クラウドの利用者間で暗号鍵を共有し、その鍵を決してクラウドに開示しないことです。この方法は、利用者しかデータを復号できないため、クラウド上のデータの機密性が確保されます。しかしな

がら、この方法では、クラウド利用者間で鍵を共有するために、煩雑な鍵管理プロセスが必要になります。

2つ目の方法は、クラウド上に暗号鍵を保管しながらも、t台以下のサーバには鍵を取得できないように、クラウドサーバ間で秘密分散する[3]方法です。鍵を取得するためには、t+1サーバが結託して秘密分散鍵を再構築する必要があります。同様に、暗号化されたデータを復号するためには、利用者は、鍵を再構築してコンテンツを復号できるよう、鍵の断片のうちt+1個を取得しなければなりません。

覗き見するクラウドモデルに対抗する最も有効な方法の1つとして、「All or Nothing Transformation（AONT）」[4) 5) 6)]を利用する方法が考えられます。AONTは通常キーレス（鍵無し）変換であるため、鍵の管理に必要なオーバーヘッドが発生しません。AONTは暗号化されたデータを異なるクラウドサーバに分散配置し、元のデータが単独のサーバだけからでは読み出せないようにします。このデータを読み出そうとするサーバは、全てのサーバに保管されている全てのデータにアクセスしなくてはなりません。それが「All or Nothing（全てかゼロか）」と呼ばれる理由です。AONTはブロック暗号を使い、暗号文内に暗号鍵を埋め込むことで、実現できます。典型的なAONTスキームの実現方式は、Rivestの記した文献で紹介されています[5]。

3.3 利己的なクラウドへの対処

文献では、クラウドが遠隔地にいる第三者に対して、クラウド自身が正しい処理をしていることを証明するためのソリューションがいくつか知られています。

いくつかのソリューションは、遠隔地にいる第三者に対して、クラウドがデータを保有・保管していることを証明するためのものです。これらは通常、PoR（Proofs of Retrievability：取得可能性の証明）[7]、PDP（Proofs of Data Possession：データ保有の証明）[8) 9)]のプロトコルという名前で、呼ばれています。PoRもPDPの両方とも、通信の複雑さを最小限にしながら、ファイル保有を遠隔検証できるチャレンジ・レスポンスプロトコルです。ここでの基本的な考え方は、データの中に暗号化されたタグを埋め込むことです。クライアントが鍵を持っているので、顧客自身がタグの真正を検証することが可能です。

PoL（Proofs of Location）[10]は、PoRスキームと地理位置情報システムを組み合わせ、特定のファイルが指定された場所に正しく保管されているかを照合するソリューションです。

また、冗長性の証明（Proof of redundancy）は、データが複数のサーバ上で複製されているかを確認するために用いられます[11]。冗長性の証明はPoLを利用して、同じファイルが複数の地理位置情報に保管されていることを確認します。Bowers他は、1つの地理的位置に保管されたデータに冗長性の証明を構築できるスキームを紹介しています。文献には、クラウド上のコンテンツが暗号化されているかどうかの検証など、他のアプローチについても述べています[3]。

3.4 悪意あるクラウドへの対処

ビザンチン耐性のある分散ストレージは、任意のデータ改変、可用性の低下そして整合性の毀損などから利用者を守れる、という魅力的な展望のため、研究対象として大きな注目を集めています。HAIL[17]は暗号化を用いた分散ストレージシステムであり、PoRの利用を複数のサーバへ拡張し、複数のストレージクラウドに分散配置されたファイルの正当性の保護と可用性（取得可能性）を保証します。HAILはビザンチンクラウドモデルを前提に、次々に違うサーバを標的にする1人の攻撃者と1台のクライアントが同期してストレージとやりとりするケースを想定しています。IRIS[9]は企業ユーザー用に設計されたPoRベースの分散ファイルシステムで、クラウド上にデータを保管し、ビザンチンであるかもしれないサービスプロバイダに対しても耐性があります。また、IRISは複数のクライアントに対応するように設計されていますが、全ての操作は、論理的に集中管理された信頼できるポータルによって事前に順序付けされます。また、このポータルは信頼できないクラウドとの通信時に決して障害を起こさないゲートウェイとして動作します。Bessani他はDepSkyを提唱しています[20]。DepSkyは消失訂正符号、電子署名や暗号鍵の秘密分散などを利用した機密性の高いデータ保管システムです。DepSkyは、書き込みを行う複数のクライアントをサポートしますが、そのために同時に複数の書き込みが起きないことを保証するための外部ロック機構を用い、これにはクライアントが互いに通信する必要があります。

3.4.1 NECの特許技術「PoWerStore」

弊社は、既存のストレージソリューションの性能を向上する特許技術を開発しました。Dobre他が発表したPoWerStoreは、軽量暗号（暗号学的ハッシュとメッセージ認証コード）に基づく、高い可用性と強い整合性を持つ分散ストレージプロトコルです。PoWerStoreの核心は書き込

みの証明（Proofs of Writing：PoW）のコンセプトであり、コミットメント方式（書き込み意図を事前に周知する方式）から発想された革新的なデータ保管技術です。PoWは2ラウンド書き込み手順を使って、最初のラウンドでは実際のデータを書き込み、2回目のラウンドでは1回目のラウンドが発生したことの「証明」だけを行います。PoWは、メタデータのライトバックやレイテンシ（遅延時間）の小さい読み出しにより、複数のビザンチンクラウドの上で強い整合性を持つストレージの効率的な実現を可能にします。HAILとは異なり、PoWerStoreは特定のサーバだけをずっと標的にし続ける攻撃者を想定していますが、非同期にデータを共有している、分散配置されたクライアント群を想定しています。DepSkyとは対照的に、PoWerStoreは高い可用性を持つ分散PoW技術を使うことで、クライアント間での直接通信を不要にしています。

4. 統合サービスのイメージ

第2章で紹介したクラウド攻撃者モデルは、顧客が求める未来のクラウドストレージを実現するために必要な一連のシステム要件を示唆しています。市場をリードするAmazonが簡易なソリューションを従量制で提供しているとはいえ、手つかずで残された市場はより柔軟性でセキュアなクラウドシステムを求めています。何もかも価格競争に持ち込むのは、高くてもセキュリティのニーズを満たすためにもっと対価を支払う用意がある顧客を無視しています。

これらの新規顧客との対話におけるポイントは、サービス面でシステム要件に対応することです。顧客にデータが確実に保管されることをただ信じることを求めるのではなく、異なる選択肢がサービスやビジネスにどのような影響を与えるのかを理解してもらわなければなりません。

本稿で述べた攻撃者モデルと技術をベースに、我々は、顧客の関心を3つの異なる特性に振り向けます。

- **耐障害性**
  サービスに支障を来さないためには、何台までならサーバに影響が出ても耐え得るか。また、どのような障害に耐え得るか。
- **セキュリティ特性**
  システムはどのようなタイプのセキュリティパラメータを順守すべきか。ここでは機密性と整合性に焦点を当てます。

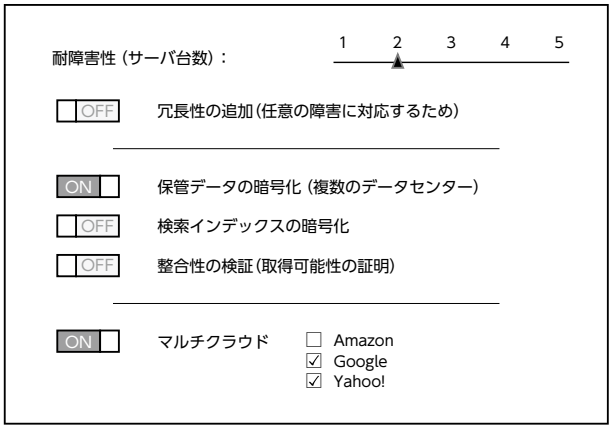


図2　サービスイメージ

- **ポータビリティとマルチドメイン**
  複数のクラウドサービスプロバイダを使えば、情報の漏えいリスクを減らすことができ、信頼性を強化し、データのポータビリティ（可搬性）を改善できます。

図2は、顧客の立場から見たサービスイメージのモックアップです。顧客のニーズに応じて、顧客が必要とする更なるセキュリティや信頼性に関わるサービスが理解できるよう、簡潔に図式化しました。サービスの価格はサービス保証に応じて異なります。追加保証が不要な場合であれば、ストレージサービスは価格で競争することになります。

このシンプルなインタフェースを使って、いくつかのセキュリティ機能を選ぶことで、顧客はどの攻撃者モデルに対処するかを選択することができます。顧客は、攻撃者モデルや機能の背景にある技術を完全に把握する必要はありません。顧客の要求や希望する価格を考慮して、弊社がストレージサービスのセキュリティ特性をバランスよく組み合わせます。

5. むすび

クラウドは、ストレージやコンピューティングに関して多くのパフォーマンスメリットを提供しますが、その一方で、クラウドはセキュリティや個人情報の漏えいという問題を残念ながら多数引き起こしています。企業や政府機関がいまだに機密情報をクラウド上に保管しない大きな理由の1つは、サービスプロバイダへの信頼の欠如です。本稿では、信頼できるとは限らないクラウドプロバイダを前提とした、セキュ

リティ、個人情報保護、信頼性の課題を解決する数々の技術と、それらの技術をどのように顧客に提示すべきかについて述べました。

弊社では、これらの技術を使ったパフォーマンスや機能に焦点をあて、独自のストレージシステムを開発しました。これは、既存のAPIと最高の効率を持つ耐ビザンチン障害分散ストレージプロトコルを使い、マルチクラウド環境での高い容量効率を実現するものです。更に、最速のAONTを開発しました。今後も、クラウドストレージサービスのための検索可能な暗号化、アクセス制御そして検証可能なポリシー適用などの問題に対する、より効率のよいソリューションを研究してまいります。

執筆者プロフィール

Dan Dobre
Research Scientist
NEC Laboratories Europe
NEC Europe Ltd.

Joao Girao
Manager
NEC Laboratories Europe
NEC Europe Ltd.

Ghassan Karame
Research Scientist
NEC Laboratories Europe
NEC Europe Ltd.

参考文献

1) Didier Bigo,et al. : Policy Department C: Citizens' Rights and Constitutional Affairs http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050
2) 2009 Sidekick data loss http://en.wiki-pedia.org/wiki/2009_Sidekick_data_loss
3) A. Shamir: How to Share a Secret? , Communications of the ACM, pages 612–613, 1979.
4) V. Boyko : On the Security Properties of OAEP as an All-ornothing Transform, CRYPTO' 99, pages 503–518, 1999.
5) R. Rivest : All-or-Nothing Encryption and The Package Transform, FSE '97 Proceedings of Fast Software Encryption, pages 210–218, 1997.
6) D. R. Stinson: Something About All or Nothing (Transforms), In Designs, Codes and Cryptography, pages 133–138, 2001
7) K. Bowers, et al. : Hail: a high-availability and integrity layer for cloud storage, CCS, pages 187-198. 2009.
8) G. Ateniese, et al. : Provable data possession at untrusted stores, CCS, pages 598-609. 2007.
9) Emil Stefanov, et al. : Iris: a scalable cloud file system with efficient integrity checks, ACSAC, pages 229-238, 2012.
10)Gaven J. Watson, et al. : LoSt: Location Based Storage, Proceedings of CCSW 2012.
11)Karyn Benson et al. : Do You Know Where Your Cloud Files Are?, Proceedings of CCSW 2011.
12)K. D. Bowers, et al. : How to tell if your cloud files are vulnerable to drive crashes, CCS 2011.
13)van Dijk, et al. : Hourglass schemes: how to prove that cloud files are encrypted, CCS 2012.
14)H. Abu-Libdeh, et al. : RACS: a case for cloud storage diversity, SoCC, pages 229–240, 2010.
15)Cristina Basescu, et al. : Robust data sharing with key-value stores, DSN, pages 1–12, 2012.
16)Gregory Chockler, et al. : Consistency and Complexity Tradeoffs for Highly-Available Multi-Cloud Store, http://people.csail.mit.edu/grishac/mcstore.pdf
17)Kevin D. Bowers, et al. : Hail: a high-availability and integrity layer for cloud storage, CCS, pages 187-198, 2009.
18)Dan Dobre, et al. : Proofs of Writing for Efficient and Robust Storage, http://arxiv.org/abs/1212.3555
19)Emil Stefanov, et al. : Iris: a scalable cloud file system with efficient integrity checks, In ACSAC, pages 229-238, 2012.
20)A. Bessani, et al. : Dependable and secure storage in a cloud-of-clouds, EuroSys, 2011.

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.66 No.1 社会的課題解決に貢献するNECの事業活動特集

社会的課題解決に貢献する NEC の事業活動特集によせて
「社会価値創造型」企業への変革を目指して～事業活動をとおした社会的課題解決への貢献～

◇ 特集論文

信頼性の高い情報通信インフラの構築
新東名高速道路での導入事例にみる次世代交通管制システムの特徴
国際通信を支える光海底ケーブルネットワークの大容量化及び高信頼化技術
基幹系ネットワークを支える要素技術とパケット光統合トランスポート装置
どこでも安定的な通信品質を実現するLTE フェムトセル基地局向け干渉制御技術の開発

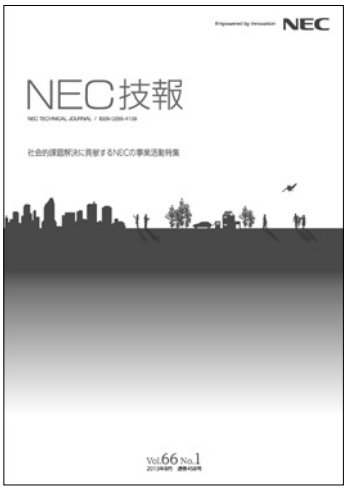
気候変動（地球温暖化）への対応と環境保全
第一期水循環変動観測衛星「しずく」の定常観測
データセンターの省電力化へ貢献する「Express5800 シリーズ」「iStorage M シリーズ」
新原理「スピンゼーベック効果」による熱電変換の可能性

安全・安心な社会づくり
CONNEXIVE 放射線測定ソリューション
市町村同報系防災行政無線システム～災害情報伝達の多様化に向けて～
消防救急無線通信システムのデジタル化推進
NECのBCソリューション～企業の事業継続を支えるiStorage HS～
水中からの脅威に対処する水中監視システム及びその関連技術
監視用小型無人機システムとその関連技術
クラウドを用いたプライバシー保護型データ処理技術
信頼できるクラウドストレージの実現に向けて

すべての人がデジタル社会の恩恵を享受
介護施設における安全確保のための「徘徊防止ソリューション」の実証実験
遠隔地からの聴覚障がい者向け要約筆記作業支援システム
対話のきっかけとなる話題提供によるコミュニケーション活性化技術

◇ NEC Information

社会貢献活動のご紹介
NECの社会貢献プログラムの基本方針と活動事例
ICTによる復興支援への取り組み



Vol.66 No.1
（2013年8月）

特集TOP