

OUCH!

今月のトピック...

- ・はじめに
- ・クラウドプロバイダの選定
- ・データの安全確保

クラウドを安全に利用するには

はじめに

「クラウド」は人によってそれぞれ定義が少し変わりますが、簡単に言えば、インターネット上のサービス事業者を使って、システムやデータの保管や管理をするものです。クラウドの利点は、複数のデバイスを使って、世界中のどこからでもデータに対しアクセスでき、それぞれのデバイスでデータなどの同期が取れるだけでなく、このデータを誰とでも共有できることです。このようなサービスは、データが物理的にどこに保管されているか分からないことから「クラウド」と呼ばれています。クラウドコンピューティングの例として、GOOGLE Docsを使ってドキュメントを作成したり、DROPBOXを活用したファイルの共有、AMAZON CLOUD上に自前のサーバを構築したり、SALESFORCEに顧客データを保管したり、APPLEのICLOUDを使って、音楽や画像ファイルをアーカイブするなどがあります。これらのオンラインサービスを使うことで生産性を上げることが可能ですが、特有のリスクも伴います。このニュースレターでは、クラウドを安全に活用しつつ、最大限のメリットが得られる方法を紹介します。

ゲストエディター

デーブ・シャックルフォード氏(@daveshackleford)は、Voodoo Security社の経営者でコンサルタントをしており、SANS Security 579: Visualization and Private Cloud Securityや Security 524: Cloud Security Fundamentalsなどの様々なSANSトレーニングコースの著者でもあります。

はじめに

クラウドそのものには、セキュリティの観点で良い・悪いというものではなく、単に物事を進めるために家でも仕事でも活用できるツールです。しかし、これらのサービスを活用する際、自分自身のプライベートなデータを他人に預け、これらのデータの安全性を保った上で、可用性も保たれることを期待しているでしょう。そのため、クラウドプロバイダを慎重に選択しなければなりません。業務で利用するパソコンや業務上のデータを扱う場合は、上司に相談し、クラウドサービスの利用が可能か否かを確認してください。利用可能な場合は、どのクラウドプロバイダが利用可能で、活用に関する組織のポリシーを確認してください。プライベートにおいてクラウドサービスの利用を考えている場合は、以下を考慮してみるといいでしょう：

1. **サポート**：「手助けや質問に対する回答を得るのが簡単かどうか」連絡窓口となるメールアドレスや質問を投稿できる掲示板、ウェブページによくある質問（FAQ）のページはあるか確認してください。
2. **簡素であるか**：「サービスの利用が簡素かどうか」サービスを利用する手順が複雑な場合、誤って情報を公開、あるいは削除してしまう可能性が高くなります。自分自身が理解しやすく、設定も利用も簡単なクラウドプロバイダを探してください。

クラウドを安全に利用するには

- 3. セキュリティ.** 「クラウド事業者によって収集される情報は何か」自分のパソコンからクラウドに到達するまでの経路や、クラウド上でのデータの保管について、暗号化の有無や、暗号化されている場合に復号できるのは誰かを確認してください。
- 4. 利用規約:** 「まとまった時間を確保して、利用規約を読んでください（驚くことに、それほど複雑ではありません）」。自分のデータにアクセスできる人たちを特定し、法的な権利を確認してください。また、セキュリティに関して、プロバイダ側と自分がそれぞれ負う責任範囲を把握してください。

データの安全確保

プロバイダの選定が完了したら、次のステップは、クラウドサービスを適切に利用することです。自分のファイルに関するセキュリティにおいて、一番影響が大きいのは、自分自身がそれらに対して、どのようにアクセスし、共有しているか、です。データの安全性を確保するためにできることをいくつか記載します：

- 1. 認証:** クラウド用のアカウントには、一意で強いパスワードを設定してください。クラウドプロバイダが2段階認証を提供している場合は、有効にすることを強く推奨します。これは、アカウントを保護するためにできる最も重要なステップです。
- 2. ファイルやフォルダの共有:** クラウドは、簡単に、時には簡単すぎる手順でデータの共有が可能です。最悪のケースとして、特定の人物とだけファイルを共有していると思っているにも関わらず、インターネット上にファイルまたはフォルダ全体を公開してしまっていることが考えられます。保護という観点で一番簡単にできることは、デフォルト設定においてファイルを共有しないことです。必要に応じて、人やグループに特定のファイルに対しアクセス権を与えてください。そして、必要が無くなったら共有を解除してください。クラウドプロバイダは、ファイルやフォルダに対し、誰がアクセスできるかを簡単に把握できるようにしてくれているはずですが。
- 3. リンクを使ったファイルやフォルダの共有:** クラウドサービスの一般的な特徴として、ファイルやフォルダを指すウェブリンクを生成する機能があります。この機能を使うことで、ウェブリンクを共有するだけで誰とでもファイルやフォルダの共有が可能になります。しかし、この手法のセキュリティは弱く、このリンクを入手した人なら誰でも自分のファイルやフォルダへのアクセスが可能になってしまいます。このリンクを一人としか共有していなくても、その一人が別の誰かと共有することもあり、さらに検索エンジンの検索結果の中に出てしまうかもしれません。リンクを使ってデータを共有している場合は、必要が無くなり次第、リンクを無効にすることや予め有効期限を設定するようにしてください。また、可能な場合は、パスワードを設定してください。



クラウドは情報へのアクセスを簡単にし、生産性も上げることができますが、情報の共有やアクセスには十分気をつけてください。

クラウドを安全に利用するには

- 4. 設定:** クラウドプロバイダが提供しているセキュリティに関する設定を把握してください。例えば、フォルダを他人と共有した場合において、その中にあるデータを自分の知らないところで共有できてしまうか、などがあります。また、共有したコンテンツを閲覧されたことを確認できる方法があるか、また、それらがいつ閲覧されたかも確認できると良いでしょう。また、共有を「読み書き」ではなく「読み込み」だけに限定することができるか確認してください。前者の場合は、データの中身を変更されてしまう恐れがあります。
- 5. アンチウイルス:** 自分のパソコンやデータを共有するために利用するパソコンには、に最新バージョンのアンチウイルスがインストールされていることを確認してください。共有するファイルが何かに感染してしまっている場合、そのファイルにアクセスしてしまった他のパソコンも感染してしまう恐れがあります。

詳しくは

毎月発行のセキュリティウェアネスニュースレター「OUCH!」をご活用ください。また、OUCH!のアーカイブで過去のトピックも参照できます。詳しくは、SANSセキュリティウェアネスソリューションのサイトをご覧ください。

securingthehuman.sans.org/ouch/archives

日本語版翻訳チーム

日本語版翻訳 - NRIセキュアテクノロジーズ株式会社

NRI セキュアテクノロジーズは、国内最大の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションの提供を通じて、情報セキュリティのあらゆる視点からお客をサポートします。 <http://www.nri-secure.co.jp>

リソース

- 2段階認証について: <https://securingthehuman.sans.org/ouch/2015#september2015>
- パスフレーズについて: <https://securingthehuman.sans.org/ouch/2015#april2015>
- パスワードマネージャ: <https://securingthehuman.sans.org/ouch/2015#october2015>
- マルウェアとは: <https://securingthehuman.sans.org/ouch/2016#march2016>
- SEC524: Cloud Security Fundamentals: <https://sans.org/sec524>

OUCH!はSANS Securing The Human プログラムによって発行され、[Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/)に従って配布されます。このニュースレターを再配布し、もしくは啓発資料としてご利用いただけますが、コンテンツの改変は認められません。翻訳その他に関しては、ouch@securingthehuman.org までお問合せください

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley

Translated By: 内山 貴之, 時田 剛



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus