トピックス

ファイル共有のセキュリティ
―情報漏えいと隣り合わせのコラボレーション そのリスクと対策―

ファイルを社内外のメンバーとオンラインで共有（コラボレーション）するクラウドサービスの利用が広がっている。共有機能はデジタルビジネスにおける生産性を高める一方で、設定ミスや悪意による情報漏えいのリスクとも隣り合わせにある。未導入の企業でも、現場では取引先から使用を要請されることもあり、セキュリティ面での対策が急務である。

NRIセキュアテクノロジーズ ソフトウェア事業本部
ソフトウェアビジネス二部 副主任セキュリティエンジニア
土屋（つちや）　亨（とおる）
専門は文書・ファイルセキュリティソリューションの提案・導入

ファイル共有の今

セキュリティ面から、機密情報や大容量ファイルのメール添付が避けられるなか、クラウド上に格納したファイルを複数人が共同で編集（コラボレーション）できるファイル共有機能を備えたクラウドサービス（以下、ファイル共有サービス）が浸透してきている。働き方改革や、デジタルトランスフォーメーション（DX）による業務改革において求められる利便性や生産性の面からも、注目を集めている。しかし、こうしたサービスは設定や使い方を誤れば、意図しない情報の漏えいにつながる上に、意図的に情報を持ち出す際の抜け道として利用されかねない。

これは、ファイル共有サービスを社内に導入している企業だけの課題ではない。導入済みの企業数の増加に伴い、グループ企業や取引先が利用している場合がある。自社で未導入でも、取引先から指定されたサービスを利用せざるを得ないケースがあるため、その都度利用許可を得たり、中には許可なしに利用したりしている現場もあるだろう。どのような企業にとっても、ファイル共有サービスの利用は避けられない状況にある。

ファイル共有の代表的な機能

機能の有無や名称の違いはあるが、ファイル共有サービスの多くはおおむね以下の機能を備えている。

①ファイルの保管

個人や組織のストレージとして、大量のファイルをクラウド上で保管できる機能である。代表的な機能としてファイル保管が目立つサービスもあるが、多くはコラボレーション機能としてファイル共有も提供されている。安価で大量のストレージを利用できるプランがあるものや、サービスによっては容量無制限のものもあることから、自社で構築・管理するファイルサーバーからクラウドストレージサービスに移行する企業もある。

②ユーザーの招待

クラウドに保存した特定のファイルやフォルダを共有し、当該サービスのアカウントを持っている社内外ユーザーに特定のアクセス

権限を付与する機能である。機能制限はあるが、アカウントを個人が無料で発行できるサービスもある。

③共有リンクの作成

特定のファイルやフォルダにリンクしたURLを発行する機能である。アクセスにはアカウントが必要だが、サービスによってはアカウントが不要な共有リンクを選べ、共有の目的に合わせて設定できる。例えば、誰でもアクセスできるよう設定し、カタログなどの公開情報を不特定多数に閲覧させる場合などにも利用できる。

④アクセス権限の設定

招待したユーザーに対して、共有する範囲や操作権限（アップロード、ダウンロード、編集、削除など）を制御する機能である。ファイルの機密レベルや共有先ユーザーの属性に応じたアクセス権限を設定することで、必要な情報にのみアクセスさせるといったコントロールが可能となる。

情報漏えいリスクと対策

ファイル共有サービスは、利用の仕方によっては、情報漏えいのリスクが伴う。考えられるリスクと対策について紹介する。

(1) 不正ログイン

他のサービスから盗まれたアカウント情報などを使用し、権限のないユーザーや第三者がログインすることにより、情報が持ち出されるケースだ。ファイル共有サービスの多くがストレージとしての役割を持つことから、他のクラウドサービスと比較して、個人情報や機密情報が蓄積されやすい。そうした機密情報が丸ごと持ち出された場合、深刻度もまた甚大である。

この対策として、最も効果的なのは認証連携である。こうしたサービスの認証においては、利用者の利便性を考えたシングルサインオンについて語られることが多いが、本質は、サービスにログインする認証処理を自社で自ら行うことにある。これにより、認証強度のコントロール権を自社のIdP（Identity Provider：認証基盤）に移譲し、認証ポリシーを統制することができ、よりセキュリティを高めることができる。サービス側で認証連携が提供されていない場合でも効果が期待できる対策を以下に示す。

①IPアドレス制限

あらかじめ登録されたIPアドレス以外からのログインを制限する機能である。信頼済みネットワーク以外からの不正なログインを防止する。

②デバイス認証

端末のデジタル証明書などを検証し、あらかじめ登録された端末以外のログインを防止する。

③二段階認証

通常の認証処理の後、アカウントに登録されたメールアドレスや携帯電話のSMS（ショートメッセージサービス）に認証コードが送信され、認証コードの入力をもってログインできる機能である。

(2) ログイン不要な共有リンクの放置

共有リンクの設定によっては、誰でもアクセスできるURLを作成することも可能であるが、ログイン不要ということは、誰がアクセスしたのか識別できないということである。想定外の

相手にアクセスされていたとしても、気づくのは難しい。作成した共有リンクは、時間経過とともに作成したことを忘れてしまうことも多く、共有リンクを削除しなければ情報漏えいのリスクが消えることはない。また通常、共有リンクのURLは複雑な文字列で構成されるため、一般には推測が困難である。しかしサービスによっては、印刷や手入力などに対応するため、人が理解しやすい任意の文字列にURLをカスタマイズできる。この場合、短時間で解析されるリスクが高まる。共有リンクは、必要十分な対象と期間の範囲での利用が望ましい。

これに対する対策は以下の通りである。

・ログイン不要のファイルやフォルダの作成を設定で禁止する、もしくはログイン不要の共有リンクを作成してもよいフォルダを設定やルールで限定する。
・有効期限を設定し、期間が過ぎた共有リンクは自動削除する。
・共有リンクもしくはファイル自体にパスワードを設定する。
・定期的に不要なリンクを削除する。
・ログイン不要な共有リンクは公開情報にのみに限定する、もしくはプレビューのみとし、ダウンロードを禁止する。

(3) 誤共有（不正共有）

メール誤送信によるセキュリティインシデントと同様、ヒューマンエラーによる誤ったファイルの共有リスクをゼロにはできない。正しいファイルがアップロードされたか、共有の範囲は正しいかは、ユーザーの判断に任されている。悪意があれば防ぐことは難しい。

対策としては、メールの誤送信対策と同様、第三者による承認や、ワークフローを使ってファイルをチェックするなどの仕組みが有効である。

(4) 誤設定（不正設定）

ファイル共有のセキュリティは、共有するファイルの重要度と相手の属性に応じた必要最小限のアクセス権限設定を行うことで、初めて機能する。大は小を兼ねるといった安易な設定では、大きなセキュリティーホールをつくることになる。しかしながら、設定に柔軟性があるほど、アクセス制御設定の組み合わせパターンが複雑化する。正しく設定するには、情報漏えいインパクトに対するリスク意識と、ファイル共有機能への高い理解が求められる。

対策としては、ユーザーの設定自由度を下げ、設定を誤っても影響を最小化する設計が有効であり、詳細を以下に示す。

・アクセス権限を過度に緩める設定を、一般ユーザーにはできないようにする。
・外部ユーザーの招待権限は、一部のユーザーにのみ与える。
・ユーザーには、あらかじめ管理者側で設計・構築したフォルダを使用させる。
・外部ユーザーの招待期限を有限にする、もしくは定期的に設定を見直す。
・社外との共有は、特定のフォルダの配下のみに限定する。

(5) サービス単体での対策の限界とCASB

ファイル共有サービスは、そのサービスの特性上、利便性の高い機能設計がされていることが多く、情報漏えい対策に対しては機能が不足しているケースもある。そうした場合に有効なサービスとして、CASB（Cloud Access Security Broker）を紹介する。

CASBは、さまざまなクラウドサービスの

コントロールポイントとして通信を解析・可視化し、サービス単体で不足している制御を代行できるクラウドサービスである。シャドーITの可視化と通信の制御を目的として、導入する企業が近年増えている。

前述した対策のうちのいくつかは、CASBの機能として提供されているものもある。ファイル共有サービスと合わせて導入することで、情報漏えい対策に高い効果を期待できる。以下に主な制御例を挙げる。

・大量のダウンロードが行われたイベントを検知し、通知もしくは遮断する。
・私的なアカウントからのログインを遮断する。
・アップロードされたファイルの中身を分析し、ファイルによっては権限の設定を変更する。
・機密情報に含まれるキーワードをあらかじめ登録しておき、キーワードに合致したファイルを検知、ファイルを削除する。（DLP：Data Loss Prevention）。
・ポリシー違反の設定を検知する。
・特定の機能の操作を制御する。

ファイル共有の限界－ダウンロードされた後のアクセス制御

さまざまな対策を紹介してきたが、これらの対策では、権限のあるユーザーがファイルをPCにダウンロードした後、別の誰かにコピーを渡すことまでは防げない。そこで、仮にファイルが流出してしまった場合にも、継続してアクセス権限をコントロールできるようにすることで、水際で情報漏えいを防ぐことができるIRM（Information Rights Management）と呼ばれる製品もある。IRM製品は対象のファイルを暗号化し、アクセス権限情報をファイル自体またはクラウドサービスに書き込む。閲覧者はあらかじめPCにインストールしたプログラム上で暗号ファイルを開く。書き込まれた権限情報とプログラムに登録されたユーザー情報を識別し、必要な権限でのみ利用させることができる。IRMにおける制御権限は閲覧だけでなく、コピー、編集、画面キャプチャ、印刷などの多岐にわたる。

ファイル共有の今後

業務システムや基幹システムまでもがクラウドに移行していく中、ネットワークにおける社内と社外の境界は明確に線引きしにくくなっている。ファイル共有サービスの役割は、社内ストレージのクラウド化から業務クラウドサービスのストレージ連携基盤として、デジタルビジネスを担う主要プレーヤーに変わっていくであろう。

セキュリティ対策モデルも、機密データは境界内部（社内ネットワーク）にあることを前提としていたペリメタモデル（境界防御型セキュリティ）から、境界を区別せずに機密データへの通信の素性をすべて疑って確認するゼロトラストモデルへと移り変わっている。ファイル共有についても、アクセスの都度、ファイル1つ1つの粒度でアクセス管理を徹底できるセキュリティ対策が必要だ。

DXの時代を深刻な情報漏えい事故の時代にさせないためには、クラウドサービスの持つ性質や機能を正しく理解し、必要な利便性とセキュリティのバランスを考えた組み合わせと使いこなしが求められている。 ■