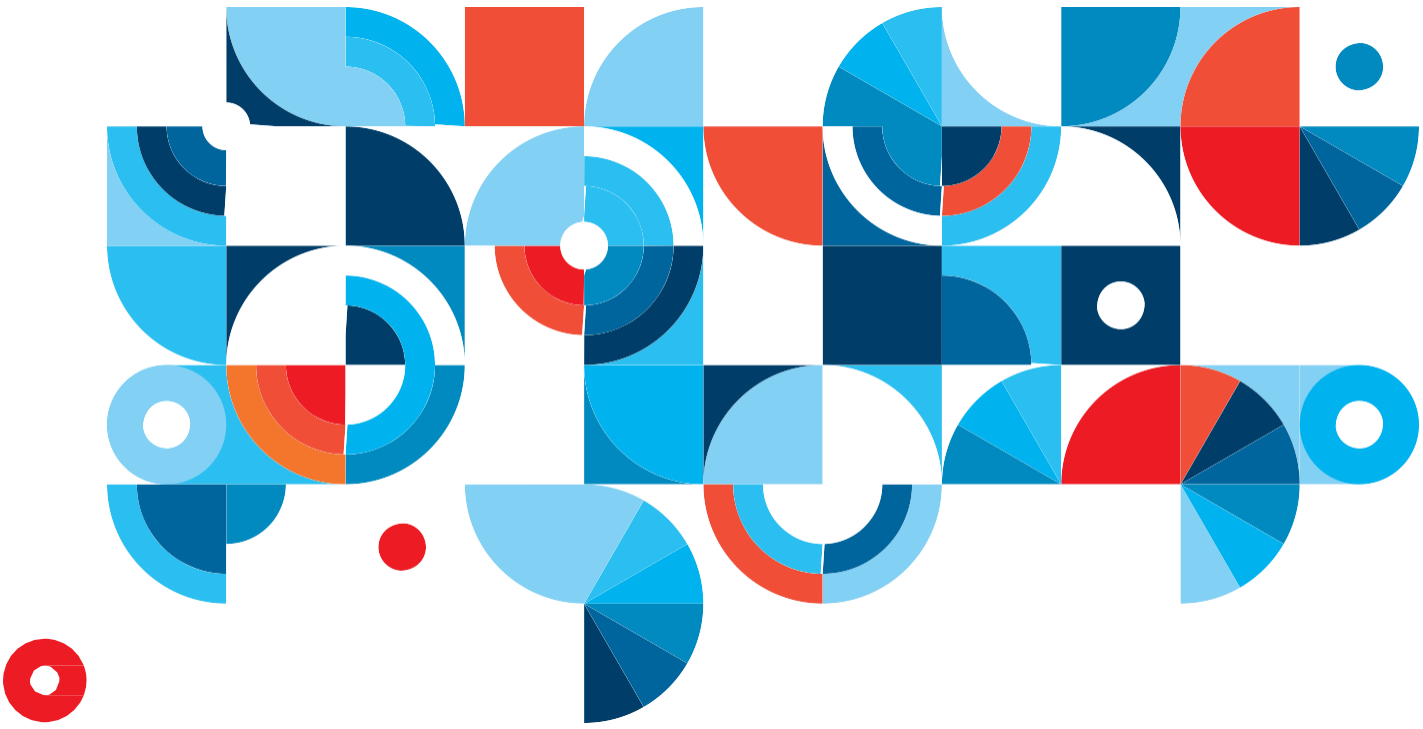
IBM Connections
ホワイト・ペーパー

2014 年 9 月

IBM Connections Cloud セキュリティー概要



IBM

目次

概要

IBM Connections Cloud (https://www.ibmcloud.com/social) は複数のコラボレーション・ツールをまとめた統合スイートで、ご使用のビジネス・ソーシャル・ネットワークと Web 会議機能やコラボレーション機能 (ファイルの保管・共有機能、インスタント・メッセージ機能、アクティビティー管理機能など) を結び付けます。お客様の信頼出来るパートナーである IBM は、セキュリティーを重視したコラボレーション・サービスとして、IBM Connections Cloud を提供します。

IBM Connections Cloud は異なる機能を組み合わせ、サービス・プランに基づいて購入することができます。

このホワイト・ペーパーは、組み込むサービスにかかわらず IBM Connections Cloud に全体として適用可能です。SmarterCloud Notes の E-メール固有のセキュリティー機能、および IBM Web Mail Cloud の E メール・サービスの詳細情報に関する個別のホワイト・ペーパーも入手可能です。

サービス・プランについての最新情報は、https://www.ibm.com/cloud-computing/social/jp/ja/planspricing/をご確認ください。

セキュリティーは、IBM Connections Cloud の競争力の一つです。IBM Connections Cloud のビジネス対応セキュリティーは、数十年にわたり IBM や IBM のお客様のデータおよびシステムの管理から培ったセキュリティーとプライバシーのベスト・プラクティスの深い理解から成り立っています。IBM のセキュリティー管理は、事業運営を可能にした上で、機密情報に対するプライバシーと制限付き権限を提供します。IBM Connections Cloud は、ガバナンス、ツール、テクノロジー、技法、およびユーザー (各詳細は後述) を介して、お客様の情報を保護します。

IBM Connections Cloud のセキュリティー・アプローチは、以下の 3 つのテーマから成り立っています。

- 高いセキュリティーを備えたインフラストラクチャー
- アプリケーション・レベルでのセキュリティー
- ユーザー視点に立った柔軟かつ堅牢なセキュリティー・システム

以下テーマごとに解説いたします。

高いセキュリティーを備えたインフラストラクチャー

物理インフラストラクチャー

IBM Connections Cloud は、堅牢なデータ・センターに設置されており、システムやデータを物理的に保護しています。データ・センターは、米国の東海岸と西海岸、および日本の遠く離れた 2 つの拠点に設置されています。データ・センターでは、すべての箇所にセキュリティー制御を採用してシステムへの物理的アクセスを制限・防止しています。物理的なアクセス・ポイントでは生体認証による管理が行われ、権限保持者のみがアクセスできるようになっています。CCTV による監視と記録によって、万一の事態にはさらなる保護が提供されます。セキュリティー担当者は 1 日 24 時間常駐しています。加えてデータ・センターでは、万全な防火システム、電力供給監視システム、建物の堅牢性を実現する免震構造や建築施工方法を採用しており、サービス中断の原因となる自然災害の影響も排除しています。電力は、複数系統の公共電力網から供給されると同時に、予備電源によって冗長構成がとられています。

アクセス制御エリアに関する追加のガイドラインは以下のとおりです。

- 実稼働サービスを提供するエンタープライズ・システムおよびネットワーク・インフラストラクチャー・コンポーネントは、アクセス制御エリアに物理的に設置されます。
- LAN 管理システム、ワイヤレス・アクセス・ポイント、およびその他の小型サーバーは、無人になった場合のために鍵のかかる場所に設置されます。
- アクセス制御エリアへの入り口を、誰もが出入りする建物のエリアに設けることは禁止されています。
- 有人の場合でも、アクセス制御エリアには鍵がかけられます。
- エリアへの無許可のアクセスを防止するために、頑丈な障壁または不正侵入検知が使用されます。
- 制御エリアへは、アクセス権限の手続きが定義付けられ、それが実施されます。
- アクセス権限の保持者は、アクセスに見合う最新のビジネス要件を持っていなければなりません。エリア・オーナーは、ビジネス要件の内容について判断することを求められます。
- 制御エリアへのアクセスを電子的に記録するために、物理的なアクセス制御手段が用いられます。

エリアへのアクセス権限リストは、定期的にエリア・オーナーによって確認、署名されます (ハード・コピーや電子コピー)。

- アクセス権限の保持者が、依頼によって、もしくは退職にともなって暗黙的に権限を取り消された場合、アクセス・リストから削除されます。
- 制御エリアへの個別アクセスの最新ログは保持されます。
- 非常口にはすべて、可聴式の監視付き警報器が取り付けられ、定期的に点検が行われます。

システム・インフラストラクチャー

ネットワーク・セキュリティーは、高性能で最先端のファイアウォールにより、提供されます。すべてのクライアント通信は 128 ビット・アルゴリズムで暗号化されます。HTTP 通信の場合は SSL、Sametime インスタント・メッセージング・プロトコルの場合は RC2 を通じて行われます。システムのバックアップには、128 ビット AES 暗号化を採用しています。リアルタイムのアンチウィルス・サポート・サービスは、オンデマンドのスキャン機能を IBM Connections Cloud 環境に提供します。堅固な商用アンチウィルス製品を、システム・サーバーだけでなくアプリケーション内にも展開しており、ファイル保管時やファイル共有時にリアルタイム・スキャンを即座に提供します。物理的なアーキテクチャーは、サービス妨害 (DoS) 攻撃やスパム攻撃から守るために、多数の制御機能で構成されます。

IBM Connections Cloud は IBM Information Protection Services (旧 Arsenal Digital) を活用して、データとシステムの堅固なバックアップおよびリカバリー機能を提供します。ローカル・デバイスを使用して、バックアップ・データおよび情報をキャプチャーし、保持します。ローカル・バックアップは毎日実行され、別の場所にある IBM データ・センターに複製されます。このプロセスは高可用性とリカバリー・サービスを保証するように設計されています。

スタッフ体制と運用プロセス

IBM Connections Cloud サービスには、専門のセキュリティー組織があり、ネットワーク、インフラストラクチャー、アプリケーション、および補助サービスに関連する明確なセキュリティー管理アクティビティーを提供します。この組織はセキュリティー機能の提供だけでなく、セキュリティー・アーキテクチャーの仕様と設計、およびコンプライアンス管理のテクノロジーとプロセスにも責任を負っています。また、組織のセキュリティー開発およびテストに関するアクティビティーを定義し、IBM Connections Cloud に多くのセキュリティー機能を提供します。

IBM Connections Cloud にかかわるすべてのスタッフの役割とアクセス権限は、明確に職掌範囲を定義した職務一覧表に記録されています。これらには、システム開発者、オペレーター、顧客サポート担当者、およびその他の利害関係者が含まれます。IBM Connections Cloud は、ライフサイクル全体を通じて、数々のセキュリティー保証アクティビティーによって守られています。職務一覧表は、会社の資産を悪用したり流用することを可能にする 2 つ以上の責務やアクセスを、1 人の個人に持たせないようにすることを目的に設計されています。サービスだけでなく、管理サポートや IT タスク (開発、テスト、管理など) など、すべてのビジネス・ユーザーのトランザクションを対象に、あらゆるスタッフの役割が文書化され、整合性を確保するために照合が実施されます。例えば、開発者は実稼働環境へのアクセスを絶対に持たないようにします。

業務の一環としてお客様データへの定期的なアクセスを持っていたり、そのようなアクセスを必要とする IBM スタッフは存在しません。通常の運用状況下では、IBM スタッフがお客様のデータを確認することはないため、IBM スタッフには、お客様データへのアクセスは与えられません。お客様のデータのプライバシーに対して、このような率先的な取り組みを支援するようサービスが設計されています。これは実際の監査の後で違反行為を捕らえるのをあてにするより、遥かに効果的といえるでしょう。

IBM スタッフおよびエンド・ユーザーの、双方のアクションがログとして保持されます。ログへのアクセスは、職務一覧表に基づき制限されます。疑わしいアクティビティーがないか、ログは定期的にレビューされます。

アプリケーション・ログに記録される情報には、以下の種類があります。

- あらゆる不正なアプリケーション・アクセスの試行
- ユーザーが実行するのを防げられたアクション
- あらゆるお客様、またはサブスクライバーの変更

データ・センターのログには以下のようなイベントが含まれます。

- 成功 / 失敗したログオン・アクセスの試行
- システム管理権限、またはセキュリティー管理権限を持つユーザー (特権ユーザー) により実行されたアクティビティー
- ネットワーク・アドレス管理システムにおける、成功したすべてのネットワーク IP アドレスの割り当てと解放
- 少なくとも次の情報: アクセス試行またはアクセス・アクティビティーの日付、時間、ユーザー ID、タイプ

お客様管理者は、組織でログに記録されたアクティビティーの日次ジャーナルを有効にし、受け取ることができます。

人事管理部門のセキュリティー対策では、盗難、詐欺、不正利用のリスクを減らすため、従業員、契約社員およびサード・パーティー・ユーザーが各自の責任を理解していることを確かめます。

- すべての職務には、文書化された職務内容説明書があります。
- 従業員ならびに契約社員は、定期的に事業運営およびセキュリティー要件に関するポリシーを理解していることを証明します。
- すべての IBM 機器の返却ならびにアクセス権の削除など、組織内における従業員や契約社員の退職、もしくは雇用形態の変更を管理します。

IBM は、すべてのシステムとインフラストラクチャーに関して、四半期ごとにセキュリティー構成レビューを実施します。ネットワークとサーバーに対しては脆弱性スキャンを定期的に実行するほか、アプリケーションとインフラストラクチャーのレビューを別途、定期的に実行しています。さらに Rational AppScan テストによって、クロスサイト・スクリプティング、クロスサイト・リクエスト・フォージェリー、SQL インジェクションなどの一般的な Web 攻撃の有無を確認しています。IBM Connections Cloud が提供する基本アプリケーションおよびインフラストラクチャーの構成 については、倫理的ハッキング (安全性を確保する目的で敢えて行う、スキルがある技術者によるハッキング) によって AppScan などのツール・セットの機能を補完しています。デリバリー環境全体に IBM コンプライアンス・プログラムが導入されています。IBM は検出されたすべての脆弱性に対して、是正措置を取るよう努めます。セキュリティー・アドバイザリーのパッチは、IBM により指定された制限時間内に、正式な変更制御プロセスを通してインストールされます。

IBM のコンプライアンスに対するアプローチは、サービス環境のすべての要素に対処する定期的なコンプライアンス・プログラムと合わせて階層的に設計されています。システム開発ライフサイクルには、コード・レビュー、コード管理、および説明責任業務が含まれます。このプログラムは、アプリケーションとインフラストラクチャーのレビューを会社レベルで実行できるように設定されています。プロジェクト・サイクルを通じて、ビジネス・プロセスに基づいたレビューが実施されます。IBM のコンプライアンス・プログラムは、定期的な自己評価と、コンプライアンス方針に基づいた実稼働環境のスキャンおよびレポートを義務付けています。プライバシー・レビューは、お客様のデータを保護するために実施しています。プライバシーおよびお客様のデータ保護に関する IBM の総合的な方針は、http://www.ibm.com/privacy/jp/ja/ でご覧いただけます。

設計段階からセキュリティーを確保

IBM Connections Cloud のセキュリティーの鍵となるのは、使用開始時から製品にセキュリティーが組み込まれていることを確実にする、そのプロセスにあります。IBM Connections Cloud は、セキュリティー運用チームとは別に、開発グループの一部である専門のセキュリティー・アーキテクチャー・チームを抱えています。セキュリティー・レビューは、設計、テストおよびリリース・プロセスにおいて中核を成す必須の要素です。

開発プロセス中には、自動もしくは手動によるさまざまな対策を活用しますが、これらはセキュリティーや脆弱性の問題を捕らえられるように設計されています。

手動での対策は以下のとおりです。

1. チーム内の開発者全員を対象にクロスサイト・スクリプティング研修を実施します。
2. 各コンポーネントのどれが確認済みかを調べるために、セキュア・コーディング・チェック・リストを作成します。
3. 新しい機能に対する定期的なコード・レビューを実施します。
4. コンポーネント内のセキュリティーやプライバシーに関するあらゆる問題をチェックするため、すべてのコンポーネント、またはコンポーネントの主要な機能に対しセキュリティー・レビューを実施します。
5. セキュリティーとプライバシーのチェックを継続/中止チェック・リストの一部として、実稼働環境にビルドをデプロイする前に必ず実施します。
6. IBM の問題追跡システムで「脆弱性」カテゴリーにおいて強調表示されるすべての問題に対し、特別な優先対応をとります。

自動化されている対策は以下のとおりです。

1. ビルドの間に、単体テストでコードをスキャンし、コードがセキュア・コーディング・チェック・リストのコンプライアンスに従っているか確認します。コンプライアンスの問題がある場合はフラグが付けられ、ビルドは失敗します。いくつかの用例チェックは、html および XSS の脆弱性をエスケープしません。
2. テスト・チームは、各リリースにおける継続/中止チェック・リストの一部として、Rational AppScan を使用します。

IBM Connections Cloud は IBM の倫理的ハッキング専門家チームを活用し、完全なアプリケーション脆弱性テストを実行します。IBM Connections Cloud チームのメンバーは品質保証

プロセスの一環として倫理的ハッキングに携わり、さらにサービス全体の独立テストを定期的に提供するために外部のサード・パーティーを使用します。

さらに IBM はお客様に、脆弱性の恐れがある場合は IBM にご連絡いただけるよう、IBM Connections Cloud フォーラムに連絡リンクを用意しています。報告されたあらゆる脅威や懸念事項を認識し調査するための正式なプロセスでサポートします。

サード・パーティーの監査と認証

IBM では、毎年独立した監査法人による毎年コンプライアンス監査を受け、データ・センターおよび運用プロセスが SSAE 16 (旧 SAS70) 制御に準拠していることを確認しています。IBM は、すべてのサード・パーティー・サービス・プロバイダーに SSAE 16/SAS70 Type II 認証取得を義務づけており、お客様 (またはお客様から指定されたサード・パーティー) による施設の監査の許可はしていません。

アプリケーション・レベルでのセキュリティー

アプリケーション、ミドルウェア、およびインフラストラクチャーの 3 地点にセキュリティー・チェックを実施するポイントを設けることで、お客様は組織内や組織間のコラボレーションにおける適切なセキュリティーを確保することができるようになっています。IBM Connections Cloud の認証ポリシーは、幅広く利用されている IBM Tivoli Access Manager ソフトウェアによって提供されています。このソフトウェアは、登録ユーザーがすべての IBM Connections Cloud コンポーネント (各種アプリケーションなど) にシングル・サインオンできるようにすると共に、登録ユーザーを相互認証します。未登録 (および非認証) のユーザーもミーティングには参加できます。アプリケーション・レベルのポリシーは、ビジネス組織の考えに基づいて情報の境界として作成

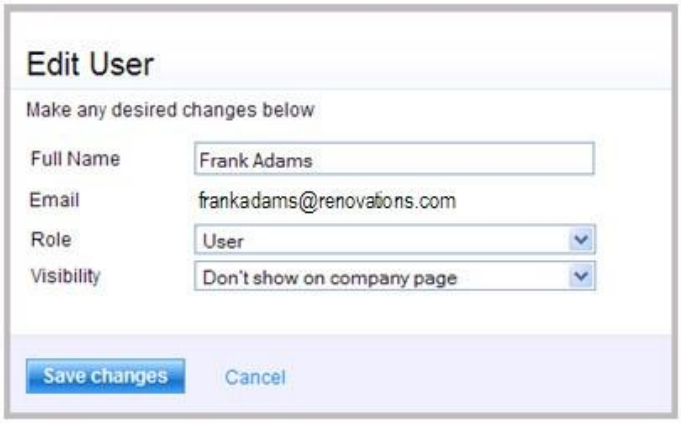


図 1: ユーザー情報の公開を制限・保護する管理者用設定画面

されます。これにより、組織内や組織間で異なる管理/ポリシーを複数適用することが可能です。IBM Connections Cloud 上のディレクトリーでは、ある組織に所属するとして登録されたユーザーは、その組織のメンバー全員 (のみ) に公開されます。境界線が明確に引かれているため、ディレクトリーに職位、写真、および E メール・アドレス、IBM Connections Cloud における役割などを登録・公開して活用することが安心して行えます。その一方で、従業員の ID 情報や個人情報について保護するための手段も提供されており、個人や管理者は、情報の保護とビジネス・ソーシャル・ネットワーキングのバランスを取ることができます。例えば、公開された自社のページや IBM Connections Cloud の検索機能において、組織外のユーザーに個人情報を公開するか否かの設定が可能です。

図 3 は公開された企業ページの一例です。登録されたユーザーの情報がどう表示されるかを示しています。この例では、氏名、写真、および職位のみが表示されています。

図 2: ユーザーごとに設定できる個人情報公開の可否設定

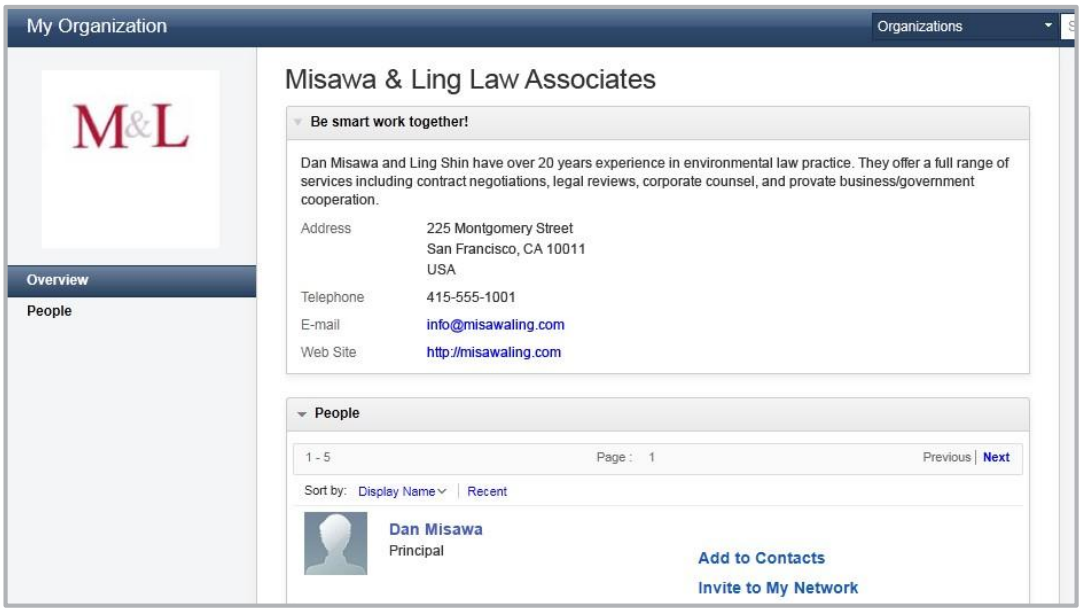


図 3: 公開ユーザーの表示例

E メール・アドレスは、すべての IBM Connections Cloud コンポーネント (各種アプリケーションなど) において、特に機密情報として扱われます。なぜなら、ユーザーの識別やユーザーへの連絡に使用される恐れがあることに加え、スパム攻撃やフィッシング攻撃などの標的にされたりするためです。ユーザーのインターネット・メールアドレスは、組織のディレクトリーを介して組織内でのみ他のメンバーに表示され、社外の IBM Connections Cloud のユーザーには、ユーザーが明示的に承認したユーザーのみに表示されます。E メール・アドレスは、そのユーザーの確認済み/検証済みの個人 ID となり継続的に使われるため、登録時における扱いにも注意を払っています。IBM Connections Cloud へ登録を行う際、そのアドレスに送信されたランダムな文字列を URL に付け加える手順が必要になります。これにより、登録された E メール・アドレスが本人のものであることを確認するようにしています。

ユーザー視点に立った柔軟かつ堅牢なセキュリティー・システム

IBM Connections Cloud セキュリティー戦略の 3 つ目の柱は、企業における自己の職責への理解に基づき、エンド・ユーザーが何を共有し、何を保護すべきかを日常的に決定していることを認識することです。平均的なユーザーが理解できなかったり、ユーザーを混乱させたりするセキュリティーは、価値がありません。ユーザー・アクションに関して非現実的な要求を行うセキュリティーでは、適切な保護を提供しません。IBM Connections Cloud は、同僚、パートナー、および顧客とのビジネス・コラボレーションの中で、有益で、有効なセキュリティーを提供します。例えば、あるファイルのすべての共有情報およびアップロード情報をファイルの単一ビューで提供します。これにより、ユーザーは、ファイルを使用する際に、そのファイルのセキュリティーに関する全情報を知ることができます。ビューには、誰とファイルを共有しているか、誰がどのバージョンをダウンロードしたか、ファイルにどのようなコメントが付けられたかなどが表示されます。また、このビューから、ファイルの共有状態、制御状態、およびファイル自体の変更を含め、ファイルに対するさまざまなアクションを実行することもできます。

IBM Connections Cloud 内の透過的なフィードバックや安全なデフォルト設定により、無理なく、ユーザーのセキュリティー認識を確保します。例えば、新たにアップロードされたファイルは、デフォルトでは非公開になるため、早い段階で誤って作業を共有

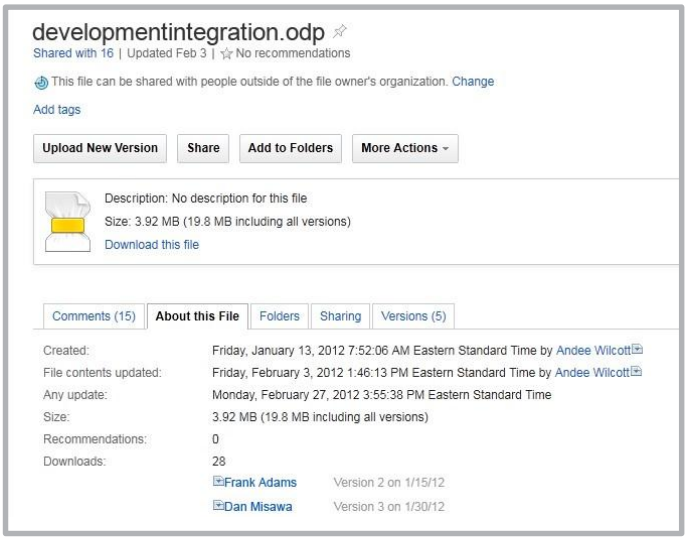


図 4: ファイルのセキュリティー、共有、および履歴コンテキスト

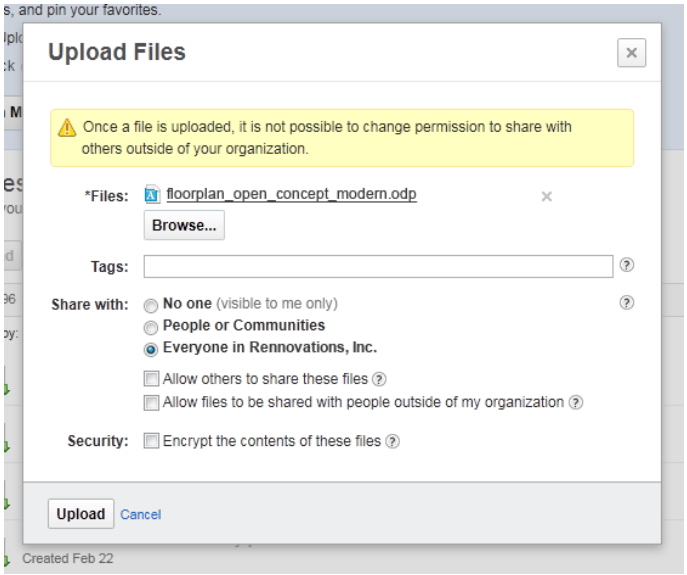


図 5: ファイルを企業内で共有

する可能性を減らします。新規ファイルのアップロード中は、右図にあるラジオ・ボタン「No One」が常にデフォルトです。新規コンテンツの作成時にこのデフォルトを目にしますが、この設定はいつでも変更できます。図 5 では、ユーザーは、新たにアップロードされたファイルについて、非公開のままにする代わりに、組織内で共有することを選択しています。アプリケーション・レベルのアクセス制御を、各 IBM Connections Cloud コンポーネント (各種アプリケーションなど) のコラボレーション・データに対して適用できます。この制御では、ファイル共有の基本単位としての「組織」に加え、「本人のみ」、「グループ」、および/または「一般公開」というレベルで、ファイル共有を行うこともできます。「一般公開 (パブリック・アクセス)」でも、IBM Connections Cloud の登録済みユーザーであることが条件になります。図 6 は、共有ファイルに作成者権限を持つユーザーを追加している様子を示しています。

結論

IBM Connections Cloud では、ユーザーがセキュリティーについて不安を感じることなく、情報交換やオンライン会議などによってコラボレーションを促進できます。そのセキュリティー・アプローチは、インフラストラクチャー、アプリケーション、ユーザー視点のセキュリティー・システムの 3 つに基づいています。それぞれにおいて、ポリシーなどを用いたり、安全なデフォルト値を用いるなどして、安全を確保する仕組みが整っています。IBM Connections Cloud は、IBM ソフトウェア・グループ、IBM サービス、IBM リサーチをはじめとする各部門のセキュリティー・コンピテンシー・センターの成果を利用しています。IBM は、今後もサービスの強化・改善を図ることにより、クラウド・コラボレーションのセキュリティーにおけるイノベーションとリーダーシップを提供し続けていきます。

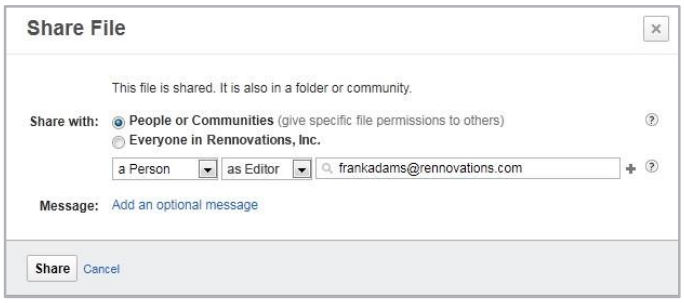


図 6: 共有されたファイルを更新できるユーザーの追加

日本アイ・ビー・エム株式会社

〒103-8510

東京都中央区日本橋箱崎町 19 番 21 号

07-15 Printed in Japan

LOW14028JPJA