



LotusLive™ Engage

セキュリティー概説



Lotus software

目次

| | |
|----------------------------------|----|
| 概要 | 3 |
| インフラストラクチャーレベルでのセキュリティ | 4 |
| アプリケーションレベルでのセキュリティ | 6 |
| ユーザー視点に立った 柔軟かつ堅牢なセキュリティ・システム | 9 |
| 今後の機能強化 | 10 |
| まとめ | 11 |

LotusLive Engage

(<https://www.lotuslive.com/>)は、SaaSモデルで様々なコラボレーションツールを提供する、ビジネス向けサービスです。ビジネス用途でSaaSを利用する上で最も懸念されるのがセキュリティーでしょう。IBMでは、LotusLiveの開発時点からセキュリティーの確保を最優先に各種検討を加え、安心してご利用いただける環境を構築しています。これには、コラボレーションツールの黎明期より20年間、Lotus製品で培ってきた経験とノウハウも生かされています。

また、その経験とノウハウを生かし、「堅牢なセキュリティーの実現と柔軟な運用の実現」という、一見相反する目標を実現しています。堅牢なセキュリティーの実現は技術的に解決できても、「日々の業務・運用を阻害することなく」という条件は技術だけでは解決できないものです。

「セキュリティー」が包含する領域は幅広く、実現する技術要素から、それを実装したインフラやアプリケーション、そして監査を含む運用など多岐にわたります。本書は、LotusLiveのセキュリティーに関わる設計思想をご理解いただくために、以下の3つの領域に分けて解説しています。

- インフラストラクチャーレベルでのセキュリティー
- 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

単に「堅牢」だけでなく「堅牢かつ使える」LotusLiveであることをご理解いただければ幸いです。

インフラストラクチャーレベルでのセキュリティ

物理インフラストラクチャー

LotusLive Engage 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。米国バージニア州に置かれたこのデータ・センターでは、様々なセキュリティ管理によってシステムへの物理的な不正アクセスを防止しています。

まず、人が出入りするすべての箇所に生体認証によるアクセス制御を採用し、権限保持者のみがアクセスできるようになっています。また、万一の事態に備えて、CCTV 録画監視システムの設置、さらにはセキュリティ責任者の24時間常駐と、万全の保護・監視体制を敷いています。

加えて、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。

システム・インフラストラクチャー

ネットワークの要衝には、信頼と実績のある技術を駆使した高性能ファイアーウォールを多段構成で設置し、セキュリティを確保しています。クライアントとのHTTP通信はすべてSSLを使い、Lotus Sametimeインスタント・メッセージング・プロトコルでもRC2 による 128 ビット・アルゴリズムですべてを暗号化しています。システム・バックアップでは128 ビット AES 暗号化を採用しています。

また、リアルタイムのアンチウィルス・サービスにより、LotusLive 環境ではオンデマンドでのスキャンが実施されます。IBM では、信頼性の高い業務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部にも展開することにより、ファイル保管時および共

有時などでもリアルタイム・スキャンを即時実行できるようにしています。これにより安全を確保しています。新種のウィルスが発見されパターンファイルが更新された場合、システムレベルの実装だけでは、すべてのファイルをチェックするには時間を要します。しかし、アプリケーションレベルにも実装しておくことで、リアルタイムにリスクを低減できます。

スタッフ体制と運用プロセス

IBM のオンライン・コラボレーション・サービス事業では、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、および関連サービスに関するセキュリティ品質管理活動を実施する専任のセキュリティ組織を配置しています。この専任組織は管理活動の実施のみならず、セキュリティ・アーキテクチャーやコンプライアンス管理、技術/運用プロセスの仕様策定と設計を行います。これに基づいて開発およびテストが実施されたセキュリティ機能が、LotusLive で数多く実装されています。

LotusLive に関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。例えば、システム開発者、オペレーター、顧客サポート担当者などがあり、関係者が管理対象から漏れないようになっています。

継続的にセキュリティを確保していくために、運用プロセスの面では様々なセキュリティ保証活動が規定・実施されています。すべてのシステムおよびインフラストラクチャーのセキュリティ構成についてはレビューを四半期ごとに実施しています。加えて、ネットワークとサーバーの脆弱性スキャンや、アプリケーションとインフラストラクチャーの個別レビューも定期的に行っています。さらに IBM Rational AppScan により、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（偽造）、SQLインジェクションなどの一般的な

Web 攻撃の有無も検査しています。LotusLive 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。安全な環境下による実施と契約によりセキュリティの脅威とはなり得ないもの)によって AppScan など自動化されたツール・セットの機能を補完しています。

これまで述べたスタッフ体制と運用プロセスを確実に実施するために、IBM では提供環境全体にわたってコンプライアンス・プログラムを展開しています。このプログラムの構築・展開にあたっては、階層的に設計すると同時に定期的にも実施することで、その実効性を確保しています。例えば、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ています。このプログラムは既に、最もチェックが厳しいとされる本社レベルで、アプリケーションおよびインフラスト

ラクチャーについて実施されています。このように、すべての処理プロセスでレビューを実施する体制となっています。IBM のコンプライアンス・プログラムでは、コンプライアンス状況の定期的な自己評価および本番環境のスキャンの実施、およびその報告を義務付けています。さらに、お客様情報を確実に保護するためのプライバシー・レビューも実施しています。IBMのプライバシーおよびお客様情報保護に関する総合的な方針は、<http://www.ibm.com/privacy/details/jp/ja/> でご覧いただけます。

IBM のデータ・センターおよび運用プロセスの監査は、SAS70 Type II との整合性が確保されています。また、LotusLive上あるいは連携してサービスを提供するすべてのサード・パーティー・サービス・プロバイダーに SAS70 Type II の認証取得を義務付けているほか、サービス提供環境についても SAS70 Type II の認証取得を計画しています。

アプリケーションレベルでのセキュリティー ＜ポリシー適用により漏れを防ぐ仕組み＞

LotusLiveでは、アプリケーション、ミドルウェア、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ています。このうち、アプリケーションの部分では、ポリシーを用いて各種セキュリティー設定を適用できるようになっています。これにより、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ます。

LotusLive では、個人を識別する認証処理を行う際にポリシーを適用できます。実際には、実績ある IBM

Tivoli Access Manager ソフトウェアによりこれを実現しています。LotusLiveでは、登録済みユーザーはすべての LotusLive コンポーネント(各種アプリケーションなど)へのシングル・サインオンに加え、ユーザー相互での認証(ユーザー識別と信頼関係の設定)も可能です。また、未登録、つまり非認証ユーザーを会議に参加させることもできます。

アプリケーション・レベルのポリシーは、「情報の境界線」として存在する「ビジネス上の組織」の概念を基礎として設定します。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。組織の単位は企業単位や事業部などの単位で設定します。LotusLive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、および電子メールアドレス、LotusLive 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。

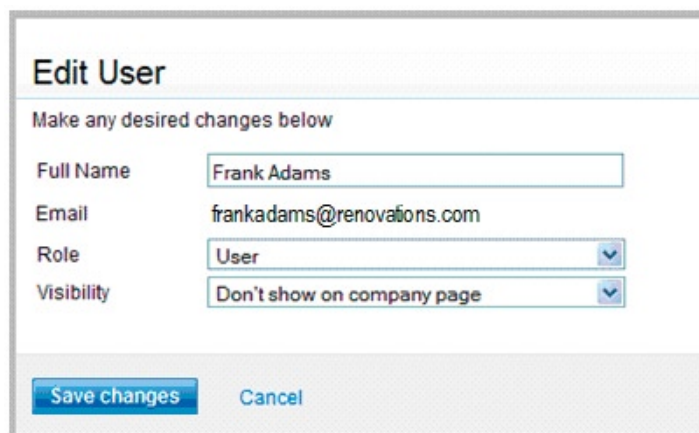


図1:ユーザー情報の公開を制限・保護する管理者用設定画面

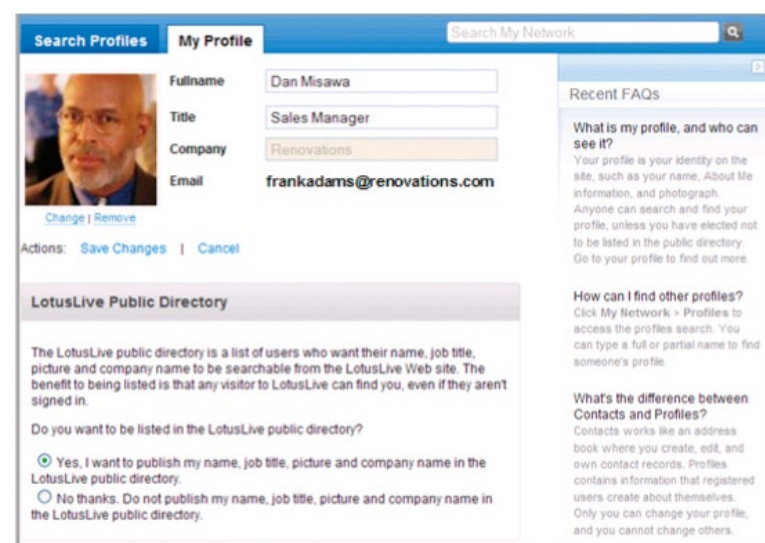


図2:ユーザーごとに設定できる個人情報公開の可否設定

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が個人や管理者に提供されています。これは、情報保護とビジネス・ソーシャル・ネットワーキングのバランスを取りながら両立させるためのものです。各ユーザーまたはその管理者は、公開された自社の LotusLive ページや LotusLive の検索機能において、個人情報組織外のユーザーに公開するか否かの設定ができます。

下図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。

The screenshot displays a LinkedIn profile for 'Misawa and Ling Law Associates'. The header includes 'Profiles' and 'My Profile' tabs, along with a search bar. The company logo 'M&L' is visible. The 'About Us' section provides a description of the firm's 20+ years of experience in environmental law and lists contact details: Address (225 Montgomery Street San Francisco CA 10011), Tel (415-555-1001), Email (info@misawaling.com), and Website (http://misawaling.com). Below this, the 'People' section shows 'viewing 1 - 1 of 1 people' and a profile for 'Dan Misawa' with a small profile picture and buttons for 'Add to My Contacts' and 'Get Connected'.

図3:公開ユーザーの表示例

インターネット・メールアドレスは、ユーザーへの連絡やユーザーの識別に使用される恐れがあることに加え、スパムメール発信やフィッシングなどの攻撃を企てる者にとって格好の材料になります。そのため、LotusLive のすべてのコンポーネントにおいては特に機密性が高いものとして扱われ、組織のディレクトリーを通じて組織内でのみ他のユーザーに表示されます。これに加えて、ユーザーが承認した外部ユーザーにも表示することもできます。

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。ユーザーは、LotusLive への登録を行う際、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、登録された電子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。

LotusLive Engageのどのコンポーネントも、コラボレーション・データに対するアプリケーション・レベルでのアクセス制御が可能です。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」はLotusLive の登録ユーザーなら誰でもアクセスできます。図4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。

Y Share files

File(s): GettingStarted.pdf

Share with:

- People/Groups (give specific file permissions to others)
- My Company (visible to everyone in my company)
- Public (visible to anyone)

Permissions: Type in the name of a person or group to give them permissions.

Readers

Authors

Message: (optional)

Frank - please verify that slide 12 is valid - thanks

Share **Cancel**

図4:共有されたファイルを更新できるユーザーの追加

ユーザー視点に立った 柔軟かつ堅牢なセキュリティ・システム

LotusLive Engage におけるセキュリティ実現のための第3の柱は、エンドユーザーによる安全かつ柔軟な管理方法の提供です。エンドユーザーは、日々発生するコンテンツ(ファイルなど)に対して、アクセス権を設定する必要に迫られます。例えば、ドラフトの資料ならごく限られた範囲内だけに権限を与え、完成した時点で権限を広げるといった作業です。LotusLiveでは、このような現実的な状況を想定して、セキュリティの確保と折り合いをつけていくための仕組みを実装しています。当然、許された範囲内での設定が可能であり、セキュリティの枠組みを脅かすものではありません。

実際の実装、すなわちユーザー・インターフェースについても配慮がなされています。平均的なユーザーにとってわかりにくい、あるいは理解不能なセキュリティ設定画面では、効果が

ないどころか、不適切な設定を行うリスクを発生させます。LotusLive Engage では、わかりやすい仕組みと設定画面を用意することで、ユーザーに負担をかけることなく、また間違ふことなく、同僚、取引先、顧客とコラボレーションを行う環境で実効性の高いセキュリティを提供します。例えば、すべての共有ファイルやアップロード情報を表示し、その共有されたファイルのセキュリティに関する情報をまとめてユーザーに提供するビューが用意されています。このビューでは、そのファイルが誰と共有されたことがあるか、誰がどのバージョンをダウンロードしたか、そのファイルに対してどのようなコメントがついているかが表示されます。さらに、アクセス制御の変更やファイル自体の変更など、ファイルに対する操作もこのビューで行えます。

LotusLive では、セキュリティ確保のために、安全なデフォルト設定を採用しています。例えば、新たにアップロードされるファイルは、デフォルトでは「本人のみ」に設定されます。必要に応じて設定を加える、ユーザーが意識的に加えるようにすることで、不慣れな場合に起こりがちな作業誤りによって意図せずファイルなどが共有される可能性を低くしています。

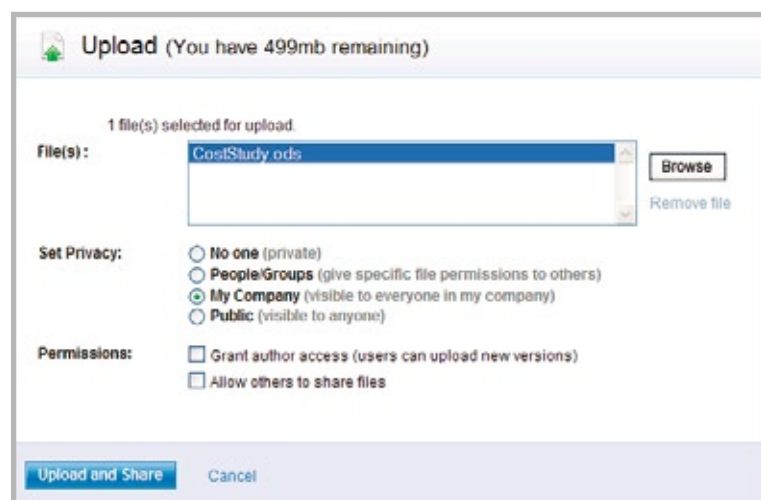


図6:社内でのファイルを共有する設定

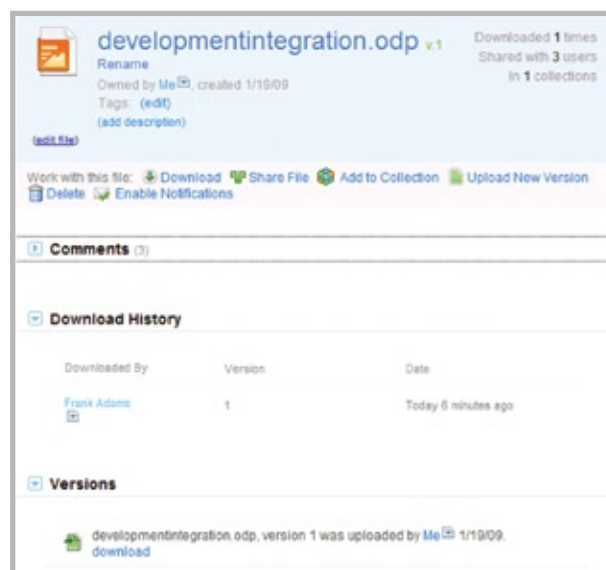


図5:ファイルのセキュリティ、共有、および履歴コンテキスト

また、設定後はユーザーに反映内容を的確にフィードバックする仕組みを設けることで、意図しない設定のリスクを低減しています。

新しいファイルをアップロードする際は、下図にある「No One (本人のみ)」ラジオ・ボタンが常にデフォルトです。新しいコンテンツを作成する際には、ユーザーはこのデフォルト設定を目にすることとなりますが、この設定はいつでも変更することが可能です。図6は、ユーザーが新たにアップロードするファイルを「本人のみ」としてではなく「組織内の全員」で共有するように選択しているところです。

今後の機能強化

LotusLive Engage への近い将来のアップデートとして、様々なセキュリティー関連機能の強化が現在検討されています。以下に一例を示します。

一部のお客様は、ユーザー認証情報のあらゆる点について自ら制御し、LotusLive で直接認証処理を行うことを望んでいます。Tivoli Federated Identity Manager (TFIM) は、LotusLive などのサービス・プロバイダーが、SAML や Open ID などのプロトコルをベースにした標準を使用する組織からの ID アサーションを受け入れる機能をサポートしています。同様の ID 同期機能はパートナーソリューションとの ID 統合においても必要です。パートナーソリューションとの連携では、さらに特定のアプリケーションによるユーザー・データへのアクセスを組織の単位で許可できるような制御も必要になります。OAuth ではこうした制御が可能です。

また、コンプライアンス機能の拡張や監視機能の強化も今後の検討課題の1つです。

エコシステムを形成する LotusLive パートナーの間では、ファイルやその他のコンテンツの暗号化をお客様自身が制御できるようにすることが検討課題として挙がっています。さらにレポート機能の強化として、組織境界をまたがる情報の流れを示すダッシュボード・ビューの追加、Tivoli Compliance InSight Manager (TCIM) から利用できる広範なコンプライアンス・レポート機能との統合なども検討されています。

なお、本書に記載の新機能に関する情報または見通し情報は、製品の全般的な方向性を示すためのものですので、購入を決定する際の判断材料にしないようにしてください。このサービスの新機能に関する情報は、情報提供のみを目的としているものであり、契約の一部とすることはできません。また、資料、コード、または機能の提供に向けた取り組み、確約、あるいは法的義務を意味するものでもありません。本書に記載の製品の開発、リリース、および時期は、IBM がその単独の裁量権に基づいて決定します。

まとめ

LotusLive Engage では、ユーザーがセキュリティ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・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。

LotusLive Engage 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・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。



© Copyright IBM Corporation 2009

本書に記載の製品、プログラム、またはサービスが日本においては提供されていない場合があります。日本で利用可能な製品、プログラム、またはサービスについては、日本アイ・ビー・エムの営業担当員にお尋ねください。以下の保証は、国または地域の法律に沿わない場合は、適用されません。

本書の情報は特定物として現存するままの状態を提供されるものであり、明示もしくは黙示の保証責任を負わないものとします。また、本書は IBM の現在の製品プランまたは戦略に基づくものです。この製品プランまたは戦略は予告なく変更されることがあります。IBMは本書の情報の使用に起因するいかなる損害についても責任を負いません。本書に記載の情報は、IBM(または IBM のサプライヤーもしくはライセンサー)にいかなる保証責任を負わせるものではなく、また、IBM 製品またはサービスの使用に際し適用される、プログラムのご使用条件の内容も変更するものではありません。

IBM、IBM ロゴ、Lotus、およびLotusLive は、世界の多くの国で登録されたIBM Corp.の商標です。他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtmlをご覧ください。他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。