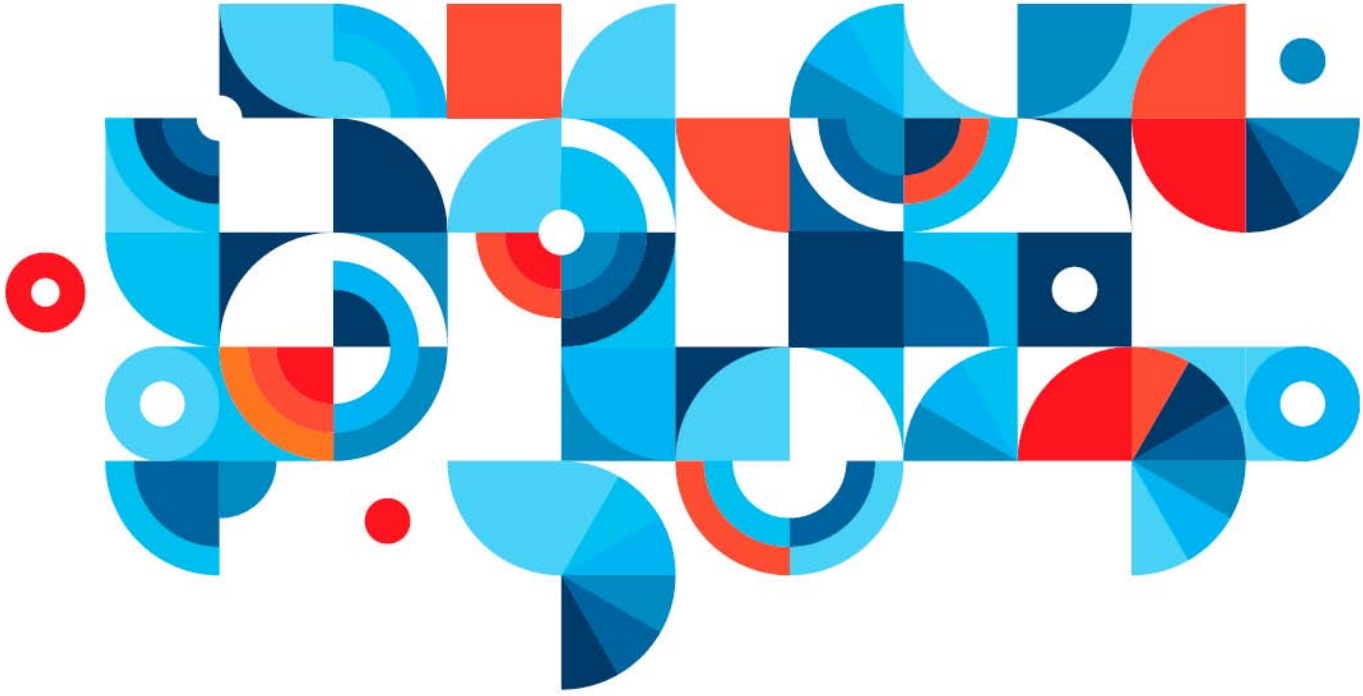
SmarterCloud
ホワイト・ペーパー

IBM SmarterCloud Notesセキュリティー



IBM

目 次

3 はじめに

サービスへのアクセス

4 人材、プロセス、コンプライアンス

5 サービスのセキュリティー

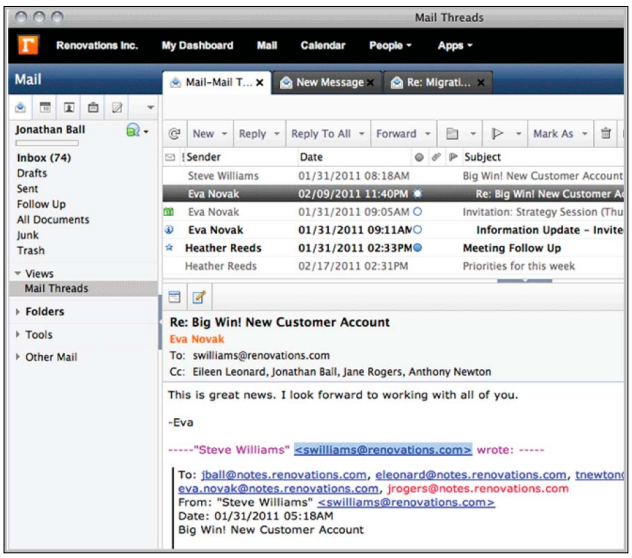
はじめに

IBM SmarterCloud Notesは、ガバナンス、ツール、テクノロジー、運用手法、および運用要員の観点から、お客様情報の保護を考慮しています。個々の詳細は後述いたします。

IBM SmarterCloud Notes（https://www.ibmcloud.com/social）とは、IBMクラウドでのEメール、カレンダー、連絡先管理、およびインスタント・メッセージといったすべての機能を備えたサービスです。

IBMは、セキュリティーとプライバシーのベスト・プラクティスの実装に尽力しています。

IBM SmarterCloud Notesのセキュリティー管理は、ビジネス遂行とのバランスを取りながら、Eメールに対してさまざまな保護を提供します。



サービスへのアクセス

サービスへの物理的アクセス

IBM SmarterCloud Notesは、データ・センターに設置され、システムやデータを物理的に保護しています。2つ1組み（災害対策用）のデータ・センターが、米国の東海岸および西海岸と、日本の2カ所に配置されています。いずれのデータ・センターもシステムへの物理的アクセスの除去または防止のために設計された、マルチレイヤーのセキュリティー制御を採用しています。各物理的アクセス・ポイントではバイオメトリックによる管理が行われ、権限保持者のみがハードウェアへの物理的なアクセス権限を取得できるようにしています。データ・センターではCCTVによるモニターが常時行われ、担当者のアクティビティーに関する記録がとられています。セキュリティー担当者が、24時間365日常駐しています。

高可用性

データ・センターは強固な建設施工を用いて建設され、自然災害によるサービス中断を最小限に抑えることを目的に設計された、防火システムや電子監視システムを備えています。データ・センターは、公共電力供給網の複数の地点を経由して、複数の公共電力網に接続されており、災害時の電力は予備発電機およびUPSにより供給されます。データ・センターは、予備のネットワーク接続プロバイダーも用意しています。サービスの各論理コンポーネントは、CPUやハード・ディスクの損失により、サービスのどの部分も停止することがないように設計された、複数の物理システムにより多重化されています。お客様のデータはすべて、Dominoレプリカのアクティブ構成で複数のサーバーに重複して保管されます。IBM SmarterCloud NotesのすべてのDominoサーバーは、クリーンな運用やフェイルオーバーが保証されるように毎日再起動されます。内外両面から複数レベルで監視を行い、構成の正常性とサービスのアクティビティーに関する監視を行なっています。法律に基づいたアーカイブやeディスカバリーもオプション・サービスとして利用可能です（IBM SmarterCloud Archiving Essentials）。システムの正常性とパフォーマンス指標に関する情報を運用担当者や開発担当者は毎日分析しています。サニタイズ処理済みの異常終了データも開発チームに報告されます。

サービスへのネットワーク・アクセス

IBM SmarterCloud Notesは多重防御戦略を採用して、無許可アクセスを防止します。IBMでは、実績のある複数レベルのトポロジーを使って、ネットワーク保護の強化目的で設計されたファイアウォールを配置しています。ユーザー認証はすべてイエロー・ゾーン（DMZ）で実施され、認証された接続のみがグリーン・ゾーンにルーティングされます（つまり、ファイアウォールを通過します）。IBM SmarterCloud Notesデータ・センターへのWebトラフィックはすべて、SSL/TLSで暗号化されています。Webサーバーでは、さらに高い保証を行う拡張検証（EV）証明書が使用されますが、これは、ユーザーが確認可能な強力なIBM SmarterCloud Notes認証を提供し、スプーフィングやフィッシング・サーバーによる一般的な「なりすまし攻撃」をユーザーが回避できるようにするものです。128ビット未満のSSL暗号はすべて無効化されています。IBM SmarterCloud Notesとの通信には、128ビット鍵によるNotesポート暗号化が使用されます。外部SMTPサーバーがSTARTTLSもサポートする場合、送受信するSMTPトラフィックにはオポチュニスティックTLS暗号化が使用されます。Dominoサーバー間のすべての内部トラフィックには、NRPCポート暗号化が使用されます。

サーバーのセキュリティー

IBMは、商用アンチウィルス製品を使って、IBM SmarterCloud Notesのオペレーティング・システム環境でリアルタイムのアンチウィルス支援サービスを展開しています。また、セキュリティー監査ログが生成、保持、保護され、プロバイダーのシステム管理者が行ったアクセスやアクティビティーが適切かどうかを分析可能です。

人材、プロセス、コンプライアンス

コンプライアンス

IBMは、データ・センターと運用プロセスがSSAE 16（旧SAS70）Type II規制に沿ったものとなるよう努め、外部の独立監査人による監査を毎年受けています。また、IBMは、すべてのサード・パーティー・サービス・プロバイダーがSAS70 Type II認定済みであることを要件としています。IBMのコンプライアンス・プログラムでは、定期的な自己評価、コンプライアンス方針に基づいた本番環境のスキャンとレポートが義務付けられています。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。プライバシー・レビューによって、プライバシーとお客様のデータ保護に関するIBMの包括的なポリシーに合わせてIBM SmarterCloud for Social Businessを調整します。なお、これらのポリシーについてはhttp://www.ibm.com/privacy/jp/ja/でご覧いただけます。

管理者

アクセス権限は、最少特権の原則およびIBM SmarterCloud Notesの職務分離マトリックスに従い、役割とタスクに応じて制限されています。運用担当者が管理作業を行う際には、管理上の特定の認証を用いてサービスにアクセスすることが求められます。IBMの担当者には、ユーザーのパスワードをリセットしたり、ユーザーIDファイルやお客様の認証者IDファイルを抽出したりする権限はありません。また、お客様のメール・ファイルに対する読み取りアクセス権限もありません。プロバイダーのアクセスはすべて、四半期ごとに評価されます。セキュリティー監査ログが生成、保持、保護され、プロバイダーのシステム管理者が行ったアクセスやアクティビティーが適切かどうかを分析可能です。

コード制御

ネットワークとサーバーに対しては周期的に脆弱性スキャンを実行するほか、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。IBM Rational AppScanテストによって、クロスサイト・スクリプティング（XSS）、クロスサイト・リクエスト・フォージェリー（CSRF）、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。手作業による倫理的ハッキングにより、評価の高いAppScanツール・セットを補完し、IBM SmarterCloud Notesの固有のアプリケーションやインフラストラクチャー構成を検証しています。定期的なアプリケーション・テストは、一般的なセキュリティー上のリスクをカバーします。また、セキュリティー・テストも開発サイクルと自動回帰テストに組み込まれています。IBMには、IBM SmarterCloud for Social Businessの全サービスに対応するセキュリティー専門組織があり、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、サポート・サービスなどの周辺のセキュリティー管理アクティビティーを実施しています。セキュリティー機能、セキュリティー・アーキテクチャー、インフラストラクチャー・セキュリティー設計、およびコンプライアンス管理プロセスやテクノロジーの提供については、IBM SmarterCloud Notesセキュリティー組織が担当します。この組織は、システム開発ライフサイクルにおいても、アプリケーションやサービス製品のセキュリティー要件の策定、コード・セキュリティー、セキュリティー機能の開発、セキュリティーのテストなどにかかわるアクティビティーについて責任を負っています。セキュリティー関連の機能は、特定のセキュリティー設計レビューをIBM SmarterCloud for Social Businessセキュリティー組織によって受けます。更新コードはすべて、ピア・レビューを経たうえで開発アーキテクトの承認を受け、コード・ベースに統合されます。それぞれの更新は、エスカレーションされた問題報告や承認を受けた作業項目に関連して行われます。1つの問題報告や作業項目に関連するすべての更新コードについて、テストと検証が行われ、デプロイメントに向けて完全なシステム・ビルドとしてまとめられます。社内でのシステム検査テストの後、開発チームはそのビルドを指定サーバー上にステージングし、運用担当者に引き継ぎます。運用部門にはソース・コードに対するアクセス権限はなく、ビルドに対するアクセス権限もこの指定サーバーに限定されています。運用担当者は、テストステージングサーバー上にシステムをディプロイし、あらためてもう1回、システム検査を行います。システムの更新は、このテストに合格した場合にのみ、本番環境にディプロイされます。

サービスのセキュリティー

Notesクライアントは、オンプレミスのDominoサーバーを認証する際に使用されるものと同じIDファイルを使ってIBM SmarterCloud Notesに認証されます。お客様のNotesクライアントはすべて、イエロー・ゾーン内のIBM SmarterCloud Notes認証サーバーに透過的に認証された後、お客様のデータが格納されているグリーン・ゾーンのサーバーに接続されます。Notesクライアントとエンド・ユーザーから見れば、これらのサーバーはお客様の名前付き認証階層の一部です。既存のオンプレミスのDominoインフラストラクチャーを運用していないお客様については、IBM SmarterCloud Notesチームがルート認証局（CA）とそれに関連するすべてのPKIおよび命名情報（ユーザーIDファイル、サーバー証明書）を生成し、管理します。Notesの既存のお客様は、最上位、すなわちOUレベルの認証者IDファイルをIBM SmarterCloud Notesに与えれば、仮想メール・サーバー用の仮想サーバーIDファイルが生成されます。それらのお客様のユーザーIDファイルは、既存のユーザーIDファイルと同じ要領で、Domino管理者によって生成されます。また、IBM SmarterCloud Notesユーザーがお客様のオンプレミスDominoユーザーとシームレスに相互運用することができるように、お客様のオンプレミスDominoディレクトリーの重要部分がIBM SmarterCloud Notesホスト環境と同期されます。IBM SmarterCloud Notesサービスでは、お客様ごとにホスティングされているNotes IDボールトを通じて、自動的かつ透過的にIDファイルのバックアップとIDファイルのパスワード・リセットを実行できます。お客様の管理者は、IBM SmarterCloud NotesのWeb管理インターフェースからユーザーのNotes IDファイルのパスワードをリセットできます。IBM SmarterCloud Notesユーザーは、IBM SmarterCloud Notesによって提供されるDominoベースのSAML IDプロバイダーを介して、Notes8.5.2以降のStandard版クライアント内からその他のIBM SmarterCloud Notesサービスに透過的に認証を受けることができます。IBM SmarterCloud Notes WebとIBM SmarterCloud Notes Administrationは、他のWebベースのIBM SmarterCloud for Social Businessサービスによってサポートされている、シングル・サインオンのログイン・ログアウト機構で統合されています。IBM SmarterCloud NotesユーザーのWebパスワードと認証を独自に管理したい場合は、IBM SmarterCloud Notes用のSAML IDプロバイダーをオンプレミスに構築することで対応できます。

メールのセキュリティー

IBM SmarterCloud Notesは、NotesとS/MIMEの両方の証明書をサポートし、サポート対象のNotesクライアントやWebブラウザーやモバイル・クライアントを使ったEメールの暗号化にも対応しています。IBM SmarterCloud Notesサービスを通過するすべてのSMTPメールに対し、Lotus Protector for E-mail Securityによる、ウィルスやスパムのスキャンが行われます。IBM SmarterCloud Notesで受信するすべてのNRPCメールに対してもウィルス・スキャンが行われます。IBM SmarterCloud Notesのメッセージは、Notesでの閲覧時はNotesクライアントの操作制御リスト（ECL）メカニズムによって、またブラウザーでの閲覧時は、JavaやJavaScriptなどのアクティブ・コンテンツを排除するために設計されたアクティブ・コンテンツ・フィルターによって、Eメール内の悪意あるアクティブ・コンテンツから守られます。ユーザーのトラッキングに使用される可能性のあるEメールに挿入されているリモート画像は、自動的に取得されることはありません。ユーザーは、Eメール内のそういった画像の表示の有無をEメールごとに選択できます。IBM SmarterCloud Notes Webは、Dominoメール・ファイルから取得したすべてのメッセージ・データをブラウザーに返送しますが、その際、「Cache-Control: no-store」というHTTPヘッダー（IE6の場合にはさらに「Cache-control:no-cache」）を付けます。これにより、ブラウザーがEメール情報をブラウザー・キャッシュ内に残すことがなくなります。

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

Produced in Japan
August 2013

LOW14029-JPJA-00