セキュアな企業間コラボレーション

ITAR およびその他規制課題の解決



EXOSTAR®

Connect once. Collect once. Certify once. Share many.

ホワイトペーパー目次 ：

エグゼクティブ・サマリー

規制の厳しい業界で事業を展開するには、その性質上、各種の基準に準拠したセキュアな関係企業（社内外のパートナー、サプライヤー、顧客、従業員、および請負事業者との）とのコラボレーションが求められる。しかし、コラボレーション環境をセキュアにすることや、政府/業界の各種規制へのコンプライアンスを確保することは、さらなる課題を呈することになる。顧客が求めるコラボレーション機能を提供できる商用ソリューションは数多く存在するが、規制の厳しい環境下での事業運営に不可欠な優れたセキュリティやコンプライアンス管理を提供できるソリューションはほとんど見当たらない。

例えば、米国の「国際武器取引規則」（ITAR：International Traffic in Arms Regulations）では、防衛及び軍事関連の技術に関する情報と物品（「米国軍需品リスト」（USML：U.S. Munitions List）の掲載品目）は、米国務省からの承認を取得しない限り、または特例でない限り、米国民のみが共用できる旨を定めている。ITAR 規則は、冷戦時代、東側諸国（Eastern Bloc countries）に課したことを反映した一方的な武器輸出規制の施行を目的として 1976 年に制定されたものである。

ITAR に準拠するためには、企業は米国務省の「国務省国防貿易管理局」（DDTC：Directorate of Defense Trade Controls）に登録するとともに、自社の USML 関連製品やサービスに適用される ITAR を理解し従わなければならない。また、ITAR のコンプライアンス要件は貿易に対する規制と同等の厳格な規制を情報コミュニケーションにも課すため、企業はコラボレーションを行う上でもこの課題に直面することになる。企業間で共有する情報は、セキュリティやコンプライアンスに深刻な影響を及ぼす恐れがあるため、各企業は、全ての情報のコミュニケーション、特に安全性が脅かされる可能性の高い電子通信を厳格に保護する必要がある。

これらの課題に対応すべく、Exostar は、企業内および企業の垣根を超えた安全でシームレスかつ生産的なコラボレーションを容易にする、セキュアなクラウドベースの企業間コラボレーション・プラットフォームを開発した。このプラットフォームは、それぞれが個別に、あるいは連携してこの目的

を推進するソリューション群（スイート）から構成されている。

ForumPass は、Microsoft の SharePoint をベースにした企業間コラボレーション・プラットフォームにおけるコラボレーション用のコア機能を提供する Exostar のアプリケーションである。ForumPass は、輸出管理法制および ITAR を含め、セキュリティ、プライバシー、及びコンプライアンスに関する最も厳しい要件に対応していることで、それぞれの法規制義務に直面する世界の企業を支えてきた実績がある。

ForumPass は、ITAR 規制対象の技術データを交換する際に必要となる基盤を各組織に提供する。また Exostar は、企業とその顧客/パートナーの ITAR コンプライアンス基準への適合性を保証するポリシーと実施手順をサポートする管理機能も整備している。これらの管理機能、ポリシー、および実施手順は Exostar とその顧客によって定期的に監査されており、結果として各々が該当する輸出規制に準拠していることを関連行政機関に示すためのソリューションとして活用される。

本書は、ForumPass の高度なセキュリティ/プライバシー機能が如何に多組織間コラボレーションとコンプライアンスに関する課題を解決するかに焦点をあてている。本書は ForumPass の特徴と機能に関する包括的な説明が目的ではなく、どちらかと言えば規格に準拠したセキュアな企業間コラボレーションに対する高まる要求に応えるための様々な方法を説明するものである。

ForumPass 概要

ForumPass は、Microsoft の SharePoint をベースに設計開発されているが、単に SharePoint の機能と性能を拡張するだけにとどまらず、規制の厳しい業界の顧客向けに特に考慮された、複数のティア（層）から成る包括的なセキュリティも備えている。それぞれの利用者はシングルサインオン（SSO）感覚で、Exostar のセキュアな企業間コラボレーション・プラットフォームの内側にある ForumPass にアクセスすることができるが、このアクセスは、Exostar のアイデンティティ・アクセス管理（IAM）ソリューションである MAG（Managed Access Gateway）により制御・保護されている。

MAG はそのプラットフォーム上で統合された要求対応型（claims-aware）の認証を行ってはいるが、ForumPass には、更に以下のような重要なセキュリティ機能が組み込まれている。

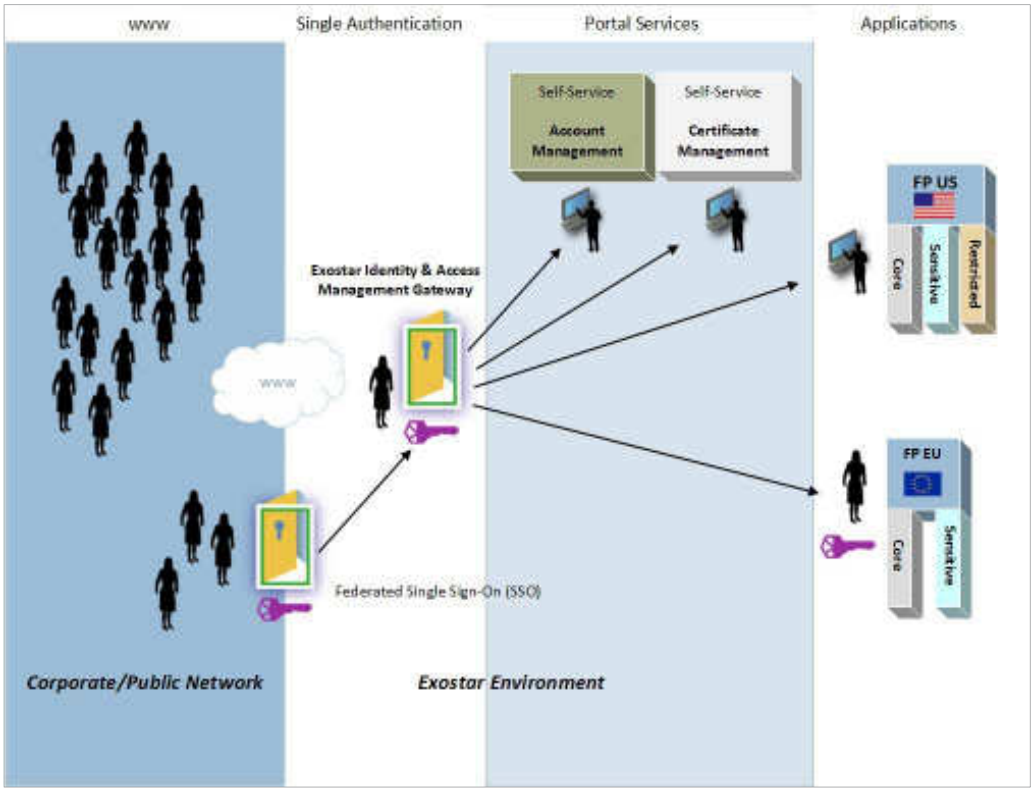
- プロジェクトによって要求される、適切なレベルの情報保護と法規制へのコンプライアンスを可能とする、厳重度別の 4 つのティア（層）から成るセキュリティ・プロファイル
- 保存データを安全に保護する標準的なデータベースレベルの暗号化による、情報共有管理
- 送受信中の情報を保護するエンドツーエンド暗号化のオプション
- 必要なクレデンシャルを持つチームメンバーのみに参加者を限定する、制限付き WebEx 会議のオプション
- デジタル著作権管理

これらの高度な機能により、ForumPass では以下を容易に実施することができる。

- ファイル共有、ドキュメント管理
- セキュアな共同提案管理
- ネット会議、同時併行/リアルタイムの作業環境
- プロセス管理、ルーティング（経路選択）

- 製品設計、コラボレーション

ForumPass は、SharePoint をセキュアなマルチテナント機能に拡張しているため、既存のシステム資産を活かしたまま、あたかも Exostar の設備にホスティングされた単一のソフトウェアを扱う様なイメージで、組織の枠を越えて活動を展開することができる。



ForumPass アクセスポリシー

サポート & コントロール

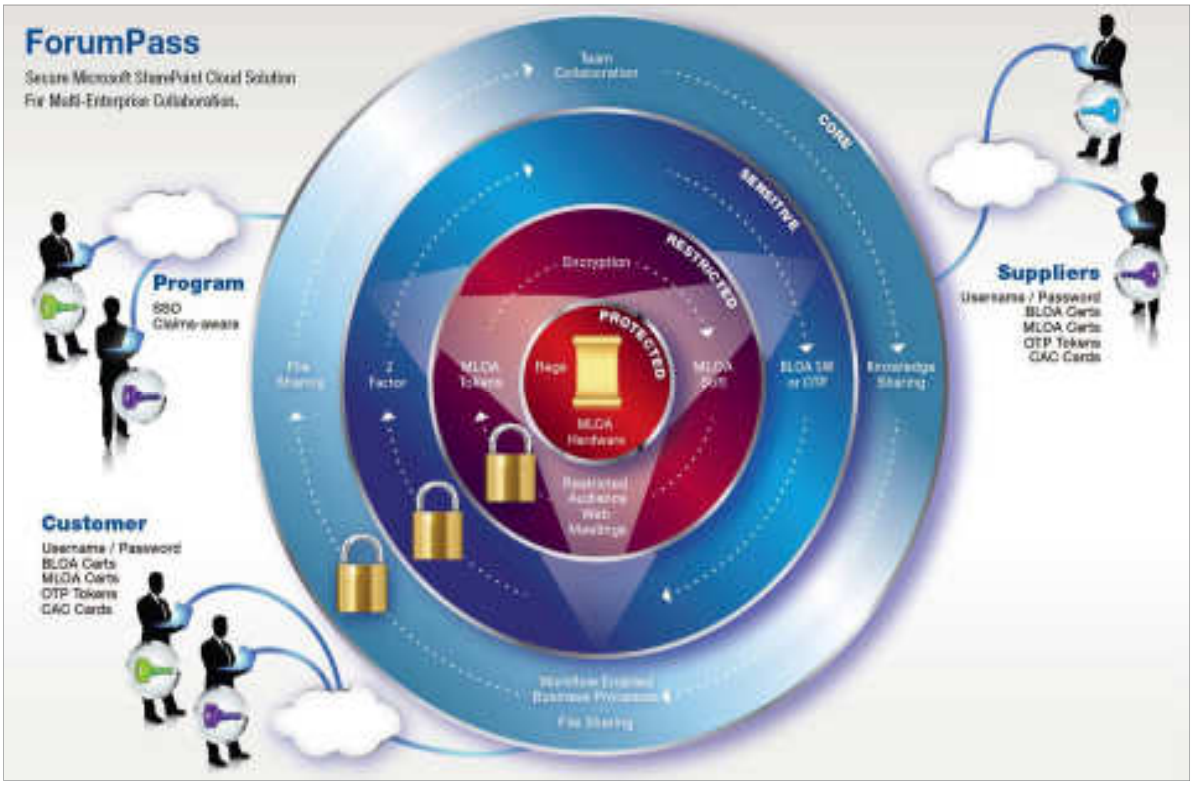
多くの Exostar の顧客（ロールスロイス、BAE システムズ、シーメンス、ハンティントン・インガルス・インダストリーズ、等）は、グローバルなマルチティアのサプライチェーンにまたがって ITAR の規制対象情報を交換する際に、ForumPass を使用している。Exostar は、A&D 業界トップ企業の輸出管理およびコンプライアンスの専門家から構成される「輸出管理ワーキンググループ」（ECWG：Export Control Working Group）を設置した。ECWG は、多国籍企業がコラボレーションによって進められる主要な事業プロセスを、規制違反のリスクを抑えつつ、効率的に実施するうえで役立つツールやベストプラクティスなどを開発することを目的としている。

過去 10 年以上にわたり、Exostar は、すぐに使える（out-of-the-box）SharePoint プラットフォームに独自の変更を加えて真のマルチテナントという概念を導入するとともに、厳重度別の 4 レベルのティアによりコラボレーション環境のセキュリティを更に強化した。4 レベルのティアは、Core、Sensitive、Protected および Restricted に分類されており、企業・実行プログラム・顧客毎に異なるセ

キュリティやコンプライアンスの要件に対応すべくデザインされている。

Exostar 独自のドキュメント・ライブラリを使用した保存データの暗号化は、Core より上位のティアで選択することができる。Secure WebEx 並びに情報アクセスや情報共有の最適な保護と ITAR 規制へのコンプライアンスを目的に設計されたその他の追加機能や機能制限も同様に、Core より上位のティアで選択することができる。

ForumPass は、世界中からアクセス可能なマルチテナント型 SaaS ソリューションである。それぞれのテナントとなる企業には、テナント固有の鍵で暗号化されたテナント固有のデータベース内に格納された、一つ以上の「サイトコレクション」と呼ぶ論理的な領域が割り当てられる。サイトコレクションはデフォルトでは、テナント組織内のユーザーのみがその存在を認識できるように設定されている。さらに、ユーザーは自組織内の他のユーザーのみを認識する（つまり、ユーザーが他のユーザーを検索する際に People Picker を使用した場合、見えるユーザーは各自組織のユーザーに限定される)。ただし、企業枠を越えたコラボレーションを進めるために、テナントの管理人は、他の組織のユーザーのメールアドレスを陽に知っている場合に限り、自身のサイトまたはサイトコレクションに招待することでその中でコラボレーションすることができる。



アクセス制御

ForumPass は、各テナントのサイトコレクションにおいて、二つの次元の異なるアクセス制御フレームワークを設けている。第一は、ドキュメントまたはページ単位という粒度（情報取り扱い単位）によるコンテンツへのアクセス許可。第二に、サイトコレクションが存在するセキュリティ・ティアに基づき、それぞれのティアのレベルに対応した強度のクレデンシャルを使用させるメカニズムである。クレデンシャルとしては、Core のティアでは単一要素認証（ユーザーネーム/パスワード）と統

合シングルサインオン（SSO）を、より上位のティアではワンタイムパスワード（OTP）装置と公開鍵基盤（PKI）証明書を使用した二要素認証を選択することができる。

アクセス許可

SharePoint のアクセス許可フレームワークにより、ForumPass のサイトオーナーおよび管理者は、自サイトに保存されているコンテンツへのアクセスを、簡単にかつ細かい単位で制御することができる。SharePoint には、33 種類のアクセス許可（例えば、アイテム追加、アイテム参照、アイテム編集、アラート指定、印刷管理など）があり、これらを組み合わせて（ほぼ役割に相当する）「アクセス許可レベル（Permission Levels）」を作成することができる。あらかじめ用意されている「アクセス許可レベル」には、「フルコントロール」「デザイン」「承認」「投稿」「読み取り」等がある。

サイト管理者およびサイトコレクション管理者は、個別のユーザーに対して「アクセス許可レベル」を割り当てることができる、もしくはユーザーグループを作成しグループに対してアクセス許可レベルを割り当てることができる。通常、このアクセス許可フレームワークは、サイトコレクションまたはサイトレベルで適用され、サブサイト、ドキュメント・ライブラリ、およびライブラリ内のドキュメントなど下位の情報単位には、上位のアクセス許可を継承する。ただし、この継承はどのレベルでも取り消すことができるため、サイトオーナーは、必要に応じてたとえばあるファイル単位で独自のアクセス許可を作成することができる。

プロファイル

テナントの「サイトコレクション管理者」がサイトを作成する際、または「サイトオーナー」がサブサイトを作成する際、これらのテンプレートに対し、あらかじめ用意されている 5 つのプロファイルのうちの１つ（たとえば Sensitive OTP など）を選択することができる。特定のプロファイルでサイトが作成されていることにより、ForumPass はユーザーに対して、前記のサイトへのアクセス許可だけではなく、必要な強度の、もしくはそれ以上のクレデンシャルを使用したユーザー認証を受けることを求める。すなわち、サイトオーナーが上位のプロファイルでサイトを作成した場合、サイトにアクセスしているユーザーのアイデンティティが本人以外のものではない（つまり、本人のものである）ことに対してより高い保証（LoA : Level of Assurance）を得ることができる。

ForumPass データ保護

ForumPass は、プロジェクトの把握やドキュメント共有から、掲示板や wiki ライブラリまで、社内外ユーザー間における迅速、簡単、かつセキュアなあらゆる情報共有を個人レベルで容易に実現することができる。ITAR へのコンプライアンスには、保存/送受信情報のアクセス管理や安全性確保など、強化されたデータ保護機能が必要である。ForumPass のデータ保護機能には以下が含まれる。

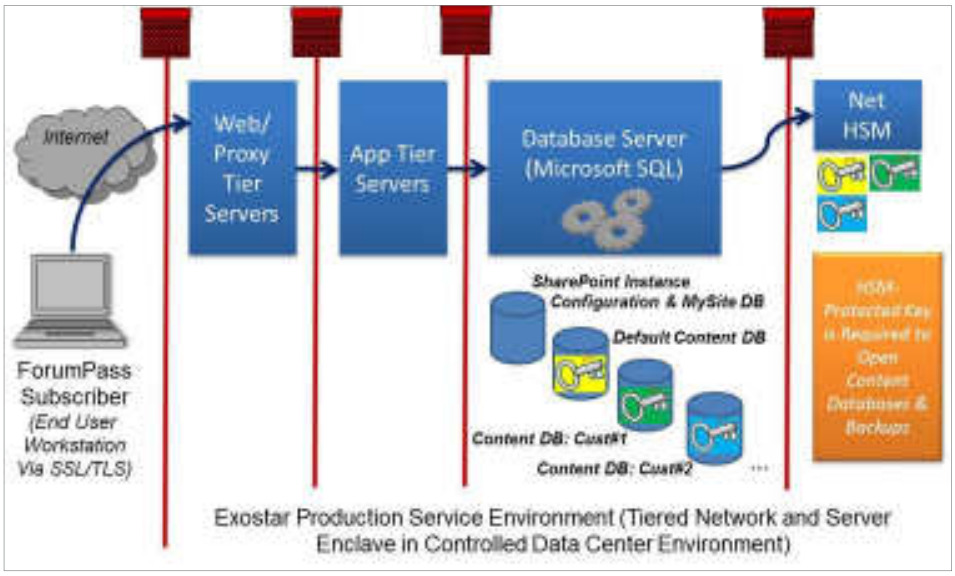
- 顧客データの分離
- 環境隔離
- 物理的・論理的セキュリティ
- **個人情報（PII）保護**

ForumPass は、図に示すように、顧客データを隔離する 3 つの形態を備えている。

- Exostar **は、物理的にも仮想的にも異なる二地域のデータセンターを設けており、一方は米**

国、もう一方は英国に位置する。データは、Exostar により手動または自動で、二地域の間や外部に複製されることはない。

- データセンター内の各顧客データはさらに隔離されている。顧客は、秘密鍵が保存される「ハードウェアセキュリティモジュール（HSM）」を備えた Microsoft 社の「透過的データベース暗号化（TDE: Transparent Database Encryption）」を使用して暗号化されている、一つまたはそれ以上の分離されたコンテンツデータベースが提供される。
- よりきめ細かな単位でデータを隔離するために、顧客は、コンテンツデータベースを分ける物理ディスクを任意で一つ以上所持することができる。



環境隔離

ForumPass は、Exostar のその他の社内インフラストラクチャやサービスとは異なる、隔離された専用の環境で運用されている。環境隔離は一連の物理的、論理的、およびネットワークの管理により実現されている。

本番（実稼働）環境

Exostar の本番環境は、高いセキュリティを備えた商用データセンター内に置かれている。技術・サポートチームは、セキュリティ管理、ネットワーク・エンジニアリング、システム管理・監視、バックアップ/リカバリ、災害復旧等の重要な分野における高度なスキルを有している。Exostar の本番環境は、性能と可用性に対する厳しいサービス品質保証（SLA）を担保すべく管理される。Exostar のデータセンターは、可用性の高い冗長性のある電力、冷却、ネットワーク、およびその他のデータセンターに不可欠な設備を提供しており、100%の電力供給力と 99.99%のネットワーク稼働時間を維持している。

物理的／論理的セキュリティ

物理的セキュリティ

データセンターでは、施設への物理的アクセスを制御、監視、および記録するための数々のセキュリティ機器、技術および手続きを使用している。主な物理的セキュリティの特徴は以下のとおりである。

- 米国人職員にアクセスを限定
- 米国永住者（グリーンカード保持者）、業務上物理的なアクセスを必要とするエスコートが求められるメンテナンス請負業者、顧客、そのほかの訪問者の、Exostar **の管理区域への立ち入りを禁止**
- 訪問者は立ち入りの際に身元確認の検査を受け、共同利用の場合は適切な場所までエスコート
- **24 時間 365 日常駐のセキュリティスタッフ**
- 掌形照合装置による生体認証で各入口とケージを保護
- ケージを含めデータセンター全体を撮影でき、リアルタイム分析と記録データ分析のための保存機能を備**えたデジタル** CCTV **システム完備。この** CCTV **システムはアクセス制御システムおよび警報装置と連動**
- 照明範囲や CCTV **撮影範囲のモーション検知**
- 外部入口からの不正アクセスに対する、無音警報と該当捜査当局への自動通知
- 入荷機器すべての確認**/検査**
- **入出荷エリアから壁で隔てられたコロケーション（サーバー等の共同設置）スペース**

論理的セキュリティ

論理的セキュリティは、ファイヤーウォールの管理、侵入検知システム、厳しい制限が設けられたユーザアクセス管理や監査、およびサーバーの耐性強化などから構成される。データセンターは、SSAE-16 SOC-1 Type II 認証による標準に準拠している。（SSAE は「検証業務基準第 16 号（Statement on Standards for Attestation Engagements, No. 16）」であり、2010 年 1 月に「米国公認会計士協会（AICPA）」の「監査基準審議会」により策定され、基本的に、サービス提供会社における内部統制状況を報告するもの。SSAE 16 は、サービス提供会社の米国報告基準を、新国際報告基準 ISAE 3402 に準じ反映するように更新することを意図して作成された。「業務受託会社（サービス提供会社）の内部統制（SOC-1：Service Organization Control-1）」報告書はサービス利用会社への財務報告に重点を置く。）

Exostar は、本番環境を監視し、ほぼどのような環境に関する懸念に対しても復旧手段を用意している。これには、職員による防犯カメラの監視、厳しい建築基準、侵入検知や防止、転送データや保存データの暗号化、ネットワークやアプリケーションのスキャンや分析、およびインシデント対応等を含むが、この限りではない。

個人情報（PII）

PII とは、特定の個人を識別し得るすべてのデータを意味する。個人を他の個人と区別するために使用され得る如何なる情報、および匿名データの匿名性を破るために使用され得る如何なる情報も PII とする。PII には取扱注意のものとそうでないものがある。取扱注意でない PII は、該当個人に害を及ぼさずに、非暗号化形態で情報を転送することができる。取扱注意でない PII は、公記録、電話帳、職員名簿、およびウェブサイトから容易に入手することができる。

取扱注意 PII は、開示された場合、プライバシーを侵害された個人に害を及ぼすおそれのある情報を意味する。よって、取扱注意 PII に関しては、データの送受信中および保存時に暗号化する必要がある。これらの情報には、生体情報、医療情報、個人金融情報（PIFI）、およびパスポートや社会保障番号（Social Security number）等の個人を識別し得るものが含まれる。

Exostar は、PII の取り扱いに関するポリシーと手順を規定している。詳しくは下記の「暗号化」を

参照のこと。

ForumPass 情報交換

社内外の承認済みユーザーとの情報交換を可能にする ForumPass は、特に、使用の容易さを備えながらも ITAR へのコンプライアンスも考慮して設計されている。情報にアクセスする際に 4 レベル、または 4 ティアのセキュリティ制御を行うことで、実際に情報交換が行われる前にリスクを低減している。

上位のセキュリティ・ティアでは、アクセスが許可されると、エンドーツーエンド暗号化により情報はさらに堅固に保護される。

暗号化

ForumPass は、情報を保護するために可能な限り暗号化を行っており、特に取扱注意情報や知的財産にとって有益である。データ暗号化は、保存時と送受信中の 2 つに分類される。

保存データの暗号化

本書の図 4 で先に示したように、ForumPass に保存されたデータはすべて、保存時に暗号化される。Exostar では、ソリューションのアプリケーション層とデータベース層の間に Microsoft 社の「透過的データベース暗号化（TDE）」を実装している。上で述べたように、顧客それぞれの「サイトコレクション」は、データベース層における、Microsoft 社の SQL Server のデータベースクラスタ内の固有のデータベースに保存されている。TDE は、各データベースを固有の鍵で暗号化する。これらの鍵は、FIPS 140-2 レベル 3 の認証を受けた外部ネットワーク HSM で管理される。この暗号化は ForumPass アプリケーションからは見えないため、このプラットフォームはデータの検索を効率的にするインデックスの作成が可能となる。保存データのさらなる保護のため、Exostar はエンドツーエンドで暗号化されたドキュメント・ライブラリを作成した。このライブラリは、独自の Java アプレットと Exostar がホスティングする対応の鍵管理フレームワークによって動作する。これらのライブラリにアップロードされたファイルは、個々の ForumPass ユーザーのワークステーションで動くアプレットによって暗号化されている。暗号化されたドキュメントは、その後 ForumPass にアップロードされ、鍵は安全に鍵管理サーバーに転送される。

暗号化されたドキュメント・ライブラリへのアクセスを許可されたユーザーのみが、ForumPass からファイルを、そして鍵管理サーバーから鍵を取り出すことができる

送受信データの暗号化

MAG と ForumPass を含めた、Exostar の SaaS 型アプリケーションはすべて、プロキシ層のリバースプロキシを経由する。これらのプロキシは HTTPS 通信（HTTP 通信はサポート外）、および「米国立標準技術研究所（NIST）」に承認された暗号アルゴリズムから成る限られた暗号スイート（cipher suite）を実施している。

ForumPass ストレージ ＆ サービス管理

インフラストラクチャ・ハードウェア

Exostar は、上記サービスのホスティングに使用するストレージとコンピューティングハードウェアを保有している。米国と英国のデータセンターおよび本社にある機器は、更なるセキュリティ層を備えたダークファイバーによって接続されている。

管理者アクセス

物理的アクセスおよび論理的管理者アクセスは、身元調査を通過し Exostar の「信頼される役割（Trusted Role)」に認定された、米国国籍の Exostar 職員に限定されている。Exostar は、多くのソリューションに対する更なる予防措置として、物理的アクセスには役割の異なる 2 者による認証を求めている。

また、Exostar のセキュリティ部門による包括的なネットワークセキュリティモニタリングに加えて、より広い脅威動向を把握する為、全ての施設に出入りする全ネットワークトラフィックをモニターしている。

サービス品質保証（SLA）

Exostar のソリューションはすべて、可用性の高いアーキテクチャで提供されている。ForumPass の SLA の稼働率は 99.5％である。前述の MAG のログイン機能による ForumPass へのアクセス管理は SLA 99.9%、そして MAG の管理機能は SLA 99.5%である。

Exostar は、地理的に分散したオフサイトの災害復旧（DR）インフラストラクチャを配備し、米英における ForumPass の本番環境を補っている。目標リカバリーポイント（RPO)、つまり、復旧できる過去の時点は、24 時間もしくはそれ以下の間隔で保証されている。

おわりに

ForumPass は、規制が厳しく求められる業界で事業展開する企業が、情報を保護しつつ ITAR やその他の法規制を遵守しながら、社内外で生産的にコラボレーションするうえで役立つセキュリティ機能を考慮して設計されたソリューションである。法規制へのコンプライアンスには、アプリケーションやドキュメントへのアクセス管理や、保存/送受信情報の安全性確保など、より強化されたデータ保護機能が求められている。データおよび環境の隔離、厳格な物理的および論理的セキュリティ、厳しいアクセス管理、ならびに包括的なエンドツーエンドの暗号化により、ForumPass は、企業間コラボレーション活動の全体にわたって、顧客とその情報に必要な保護機能を提供できる。