ホワイトペーパー
（法令遵守要件）

米国防総省改訂要件への対応

保護対象防衛情報の保全

EXOSTAR®
Connect once. Collect once. Certify once.
06 June 2016

訳　株式会社エヴァアビエーション（29 August 2016）

ホワイトペーパー目次

世界のあらゆるデータは攻撃にさらされています。このところ毎日のように、個人データや財務データが盗まれる大規模な侵害のニュースを耳にします。サイバー攻撃はビジネスや政府の諜報活動から不正行為まで広範にわたり、ハッカーは連日ファイアウォールやその他のセキュリティバリアを迂回・突破しようと取り組んでいます。昨年末、米国連邦政府は人事管理局(OPM)、郵政公社、国務省、海洋大気庁、国税局、及びホワイトハウスなど連邦政府情報システムに対する数多くの侵害に苦しみました。

情報の危殆化は、必ずしも政府ネットワーク、システム、又はアプリケーションへの直接的な攻撃の結果によるものとは限りません。事実、増大しつつあるサイバー攻撃は、政府機関を支える複数層のバリューチェーンから構成される請負企業や下請企業に向けられています。バリューチェーンのセキュリティの強度は結局のところ、最も弱い結合部の強度でしかなく、しかも多くの民間企業は、適切に自社を保護できるリソースとセキュリティ対策を備えてはいません。脅威の種類・巧妙化・ターゲットが増加し続けているため、包括的なソリューションの必要性はますます高まっています。

2150 万人以上の政府職員と契約企業職員の個人情報（PII）に影響を与えた人事管理局(OPM)への侵害事件をうけ、米国防総省(DOD)は新たな国防総省調達規則(DFARS)として「ネットワーク侵害報告ならびにクラウドサービス利用契約に関するサイバーセキュリティ規則」(202、204、212、239、252)の施行に至りました。

契約企業に対する米国防総省の新要件

米国防総省は、保護対象防衛情報(CDI：covered defense information)の保全、防衛関連契約企業へのサイバー攻撃の全容解明、及びクラウド・コンピューティング環境への攻撃脆弱性軽減等への措置が緊急に必要なことから新たな規則を施行しました。DFARS 252 には、元請企業とその下請企業に対して、情報の紛失・悪用・変更・不正アクセスの発生可能性およびその影響の大きさに対応した「適切なセキュリティ」の採用を求める CDI の保全に関する準拠性(compliance)規則が含まれています。このDFARS 条項の核心は、米国国立標準技術研究所(NIST)発行の特別出版物 (SP) 800-171 「連邦政府外の組織と情報システムにおける保護対象非機密情報(CUI：Controlled Unclassified Information)の保全措置」に示されるセキュリティ管理措置を逸脱しないことにあります。コンプライアンスの期限は 2 年足らずの 2017 年 12 月に迫っているうえに、報告と実施が求められる範囲が、各請負企業の枠を超えて、下請企業やサプライヤからなる複数層のバリューチェーンにまで及ぶため、防衛関連契約企業が直面するコンプライアンスに関する課題が拡大されています。また、契約企業および関係企業はすべての新たな落札案件に対して 30 日以内に米国防総省最高情報責任者(CIO：Chief Information Officer)に電子メールにてギャップ分析と実行計画を提出する必要があります。

米国防総省は、一般的な請負企業がこれらの新たなデータセキュリティと報告の義務を履行するには、技術的な専門家の助けがおそらくは必要になるであろうと説明しました。Exostar はその助けとなる最も装備された技術的専門家であり、本ホワイトペーパーはそれを示すものと考えます。

National Institute of Standards and Technology

セキュリティ要件の分類

CDI の保全措置を取るということは、DFARS 252.204-7012 が求めている NIST SP 800-171 に示される要件に準拠することを意味しています。NIST SP 800-171 の要件は、危殆化(compromise)され易いと見なされる人、プロセス、インフラストラクチャを対象とした広範な対応能力と 100 以上のセキュリティ管理措置からなる以下に示す 14 の「ファミリー」にブレークダウンされています。

1. アクセス制御
2. 意識付け・研修
3. 監査・説明責任
4. 構成管理
5. 識別と認証
6. インシデント対応
7. メンテナンス
8. 記憶メディア保護
9. 人的セキュリティ
10. 物理的保護
11. リスク評価
12. セキュリティ評価
13. システム・通信の保護
14. システム・情報の保全

防衛関連契約企業における新要件への適合を支援する Exostar ソリューション群

新たなセキュリティ要件の多くは今日の IT 化された企業では適合できるであろうと Exostar は考えています。 しかし、下記の要件など契約企業や下請企業にとってかなり煩雑な（多大な時間を要する、複雑な、多大な出費を要する）ものも存在します---これらの領域は Exostar がまさに実績あるエキスパートと言えます。

- アクセス制御
- 識別と認証
- インシデント対応
- リスク評価（関連するサプライヤへの展開を含む）

Exostar には、強固なセキュリティと証明された法制度等への準拠性が最優先課題である防衛関連契約企業のニーズを満たすためにデザインされたソリューション群があります。これらのソリューションは、政府契約企業と下請企業がすぐに利用することができ、要件を満たさなければならない差し迫った期限を厳守するための今後の取り組みにおいて、非常に有益となるでしょう。

アクセス制御

アクセス制御は、識別、認証、承認の 3 つの主要機能に分けることができます。

- 識別：システムは如何なる個人ユーザのアイデンティティも判断できなくてはならない。
- 認証：システムが個人ユーザを識別したのち、正規ユーザのみがアクセスを許可されるようにユーザ・アイデンティティの検証が必要である。
- 承認：認証が成功した場合、システムは定められた基準に従い、個人ユーザに対してアプリケーションやデータへのアクセスを許可できる。

Exostar アクセス制御ソリューション

Exostar のアイデンティティ・アクセス管理（IAM）プラットフォームは、社内外の「信頼できる」ユーザ（パーティ）のみに企業のアプリケーションとデータにアクセスを許可するクラウドベースのソリューションです。委任された管理権限により、情報資産オーナーは、アプリケーションやデータへのアクセス管理特権を割り当てます。管理権限者は Exostar のソリューションを実行するために、必要なアクセス用クレデンシャルの種類・強度を割り当てることもできます。Exostar は、防衛関連企業に役立つ 3 種類のアクセス制御ソリューションを提供しています

- CDI を有する可能性がある企業システムに対してアクセスを要求するサプライヤは、クラウド上で Exostar の IAM プラットフォームを使用することができます。
- ネットワークへのアクセスに多要素認証（MFA）を必要とするエンタープライズユーザに対応するため、Exoster は次の 2 つのソリューションを提供しています。
  - 統合アイデンティティソリューション(FIS) --- 中位ハードウェア保証レベルで米連邦政府ブリッジ認証局と相互認証され、（Exostar と米国防総省間の合意書(MOA)に基づき）米国防総省が信頼する PKI サービス
  - Exoster のワンタイムパスワード(OTP)ソリューションをベースにしたエンタープライズ認証サービス

識別と認証

NIST SP 800-171 で規定している多要素セキュリティ管理措置は、14 ファミリー中に示されている 109 のセキュリティ管理措置の一部です。契約企業は次の条項に従う必要があります。

3.5.3	特権アカウントに対してはローカル及びネットワークアクセスならびに非特権アカウントへのネットワークアクセスに多要素認証(MFA)を使用する
3.5.4	特権ならびに非特権アカウントに対してはネットワークアクセスにリプレイアタック耐性を持つ認証メカニズムを採用する
3.5.5	規定された期間内の識別子の再利用を防止する

DFARS 規則に関する米国防総省の FAQ には、ユーザのアイデンティティを確認する際、次の方法の少なくとも 2 つ以上を使用することとしています。

- **ユーザが知っている何か** --- パスワード
- **ユーザが所有しているもの** --- フォブ(key fob）、スマートカード、又はハードウェア装置かスマートフォンのモバイルアプリが生成するワンタイムパスワード
- **ユーザ自身の特性** – 指紋や虹彩パターン等の生体属性

正確なアイデンティティ情報の記録を維持し検証を行うことは、ビジネス関係やパートナー関係および地域の拡大など企業の成長に伴い、問題を起こす可能性のあるところも飛躍的に増加する恐れがあることから、多大な内部リソースが必要になる可能性があります。

ボーイングやロッキードマーチンなどの大手防衛関連企業は現在 Exostar の識別・認証ソリューションを使用しており、この上に法制度等への準拠性の基礎を置くことを計画されています。

Exostar のコラボレーション・ソリューション

Exostar では、ほぼ完璧に法制度等の規制に準拠した企業間コラボレーション・ソリューションは Exostar の IAM プラットフォームであると考えており、このプラットフォームのもとで多要素認証(MFA)により情報資産を保護することで、規制に準拠した CDI のアクセス制御を行うという課題を解決します。このプラットフォームは、社内外のパートナーや地理的に分散しているチームが携わる統合的なプログラム、プロダクト、又はプロジェクトのチームに最適です。また、Exostar の企業間コラボレーション・ソリューションを利用してビジネスを進める利点の一つに、情報セキュリティを強化する「暗号化(Encryption)」と「デジタル著作権管理保護(Rights Management Protection)」の組み合わせがあります。

暗号化

Exostar の企業間コラボレーション・ソリューションは、ドキュメントのエンドツーエンド暗号化を提供しており、これによってローカルリポジトリに保存されている(at-rest)データと、企業枠を超えてコラボレーションするユーザ間で通信される(in-transit)データの双方を保護することが可能になります。

Exostar は、ユニークなキー(Database encryption key : DEK)を使用して各データベースを暗号化するマイクロソフトの透過的データ暗号化(Transparent Data Encryption : TDE）を実装しているため、Exostar の企業間コラボレーション・プロラットフォームに保存されているデータはすべて暗号化されます。更に、Exostar の企業間コラボレーション・プラットフォームはプロキシ層のリバースプロキシを経由するため、NIST が承認する暗号アルゴリズムを含む HTTPS 接続や暗号スイート(cipher suite)を実行することによって通信中のデータを暗号化します。

デジタル著作権管理保護

ビジネスの世界では、アプリケーションによる様々なアクセス制御より強固なデータ保護方式への要求が高まりつつあります。サイバーセキュリティの脅威に加え、機密性の高いデータや知的財産を保護する必要性がこのような要求を駆り立てています。

そのため Exostar は、コラボレーション・プラットフォームにデジタル著作権管理機能を導入しました。デジタル著作権管理では、ドキュメント毎に暗号化されるきめ細かなセキュリティを設定できます。マイクロソフトの Word や Excel のようなネイティブアプリケーションのドキュメントの復号に際しては（多要素認証(MFA)による）ユーザ認証が成功した場合にのみ復号されます。ネイティブアプリケーションは、Exostar のコラボレーション・ソリューションにおけるユーザ権限に基づき、ユーザに対して権限（閲覧、印刷等）を動的に設定します。

インシデント対応

DFARS の要件には、企業情報システムのインシデント対応計画の策定が示されています。インシデント対応計画には、インシデントを把握・記録し、企業内外の適切な機関や職員に報告するための適切な準備、検知、分析、格納、リカバリ、およびユーザ対応措置が含まれます。

企業情報システムでインシデントが発生した場合、契約企業は 72 時間以内に米国防総省 (DOD) にインシデントを報告しなければなりません。DFARS の要件では DOD CIO への報告サイトにログインする際には多要素認証(MFA)が必要になります。Exostar の多要素認証クレデンシャルは米国防総省に受け入れられているところから、Exostar のソリューションは、もともとインシデント対応要件に対応していることになります。

リスク評価（関連するサプライヤへの展開を含む）

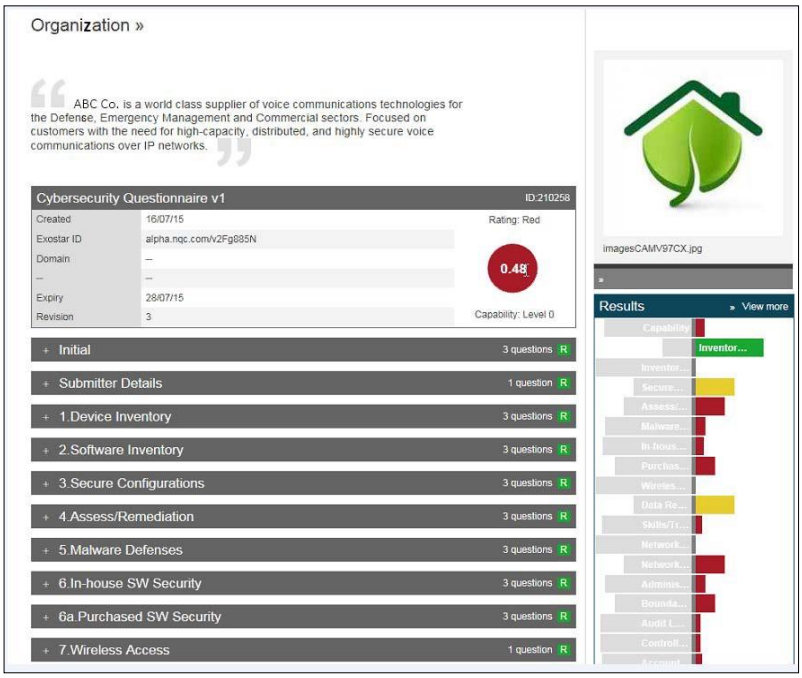
強力なパートナー（契約企業、下請け企業、サプライヤ等）間のネットワークは多くのメリットをもたらしますが課題も伴います。プラス面としては、参加企業は各自の得意分野に集中できるため、製品市場投入までの時間が早まり、設備投資や運用コストが極小化されます。一方、パートナーの数、種類、地理的分布が増加するにつれてリスクも高まるというマイナス面もあります。各パートナーの健全性、パフォーマンス、及びセキュリティへの態勢は、企業内の利害関係者、企業全体の評判、及び契約の安危に直接影響を及ぼします。

Exostar のサプライチェーン向米国防総省 DFARS 準拠性管理ソリューション

Exostar は、元請企業がその下請企業やサプライヤのコンプライアンスを把握することができ、NIST SP 800-171 が規定する関係企業への展開要件（flowdown requirement）に対応できるソリューションを導入しました。Exostar のリスク管理ソリューションによりサプライヤは以下を実施できます。

- NIST SP 800-171 に規定される 109 のセキュリティ管理措置それぞれに対する準拠性を記録する
- 準拠性スコアを確認する
- 元請企業が米国防総省 CIO に対する 30 日以内の対応において使用できる、コンプライアンス・ギャップ情報をアップロードする
- 状況の変化に応じて更新する

Exostar のリスク管理ソリューションは、信頼できるソースからの情報を活用してパートナーの顕在および潜在リスクと企業への影響の全体像を描くウェブベースのセキュアなマルチテナント型セルフサービスソリューションです。企業はサプライヤのリスクと準拠性を継続的に把握・管理することができます。このリスク管理ソリューションは、Exostar の IAM プラットフォームと統合されており、アクセスは二要素認証により確実に制御され、機密性の高い情報を危急化から保護すると共に、よりしっかりした DFARS 準拠性を促進します。また、関連組織およびサプライチェーン下流までを対象とする NIST SP 800-171 への準拠性を証明するために必要な、サイバーセキュリティへの取り組み、表明書および各種証明書、その他のベンダー・マスターデータに関するサプライヤ情報の取得等にも役立ちます。



Risk Management Scorecard – an in-depth look at partner compliance details

Exostar のリスク管理が NIST SP 800-171 に対する完全なソリューションである理由

- アクセスは、Exostar の IAM プラットフォームにより制御されます。より強固なセキュリティのためのユーザ・アイデンティティの検証には多要素認証を選択できます。
- 役割ベースのアクセス権限設定により、リスク管理モジュールおよび企業やパートナー情報に対してより細かくアクセス制御を行えます。
- 標準質問様式、テンプレートおよびワークフローは航空宇宙・防衛コミュニティの主要メンバーにより賛同を得ています。
- 一度使えば幾度も利益をもたらすモデルを通じてコミュニティ全体で情報を共有できます。コミュニティの規模は、パートナーの多くが既にメンバーである可能性を示唆しています。複数の購買組織と取引のあるパートナーは、質問票への回答は一回で済むため、事務負担が軽減され、余剰や矛盾もなくなり、またオンボーディングの促進や情報の一元化が行われます。

終わりに

グローバルな下請企業とサプライヤからなる巨大な複数層のパートナーネットワークを抱える契約企業にとっては 2017 年 12 月という期限が刻一刻と迫ってきています。DFARS 及び NIST SP 800-171 の要件を満たすために、Exostar のクラウドベース型ソリューションを今こそご活用ください。BAE システムズ、CSC、ハンティントン・インガルス・インダストリーズ、ロッキードマーチン、ノースロップ・グラマン、レイセオン、ロールスロイスを含む、100,000 社にものぼる企業が、各社の航空宇宙・防衛戦略を支援するサービス・ソリューションとして Exostar を信用され活用されています。この一員に加わってはいかがでしょうか。これら大手企業は、次のような分野において Exostar の非常に優れたマーケット・技術・法制度等への準拠性のノウハウを活用されています。

- 社内外でコラボレーションするとともにセキュリティも強化
- 迅速な展開が可能かつ適正価格のソリューションにより時間と費用を節約
- 貴重なリソースを自社のビジネスに集中
- 法制度等への準拠性に適合しつつ複雑な要件を簡素化 --- 各社のニーズに合わせて、Exostar は即時使用できるソリューションを用意します。

EXOSTAR®

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

Contact Exostar Today
sales@exostar.com 703.793.7733