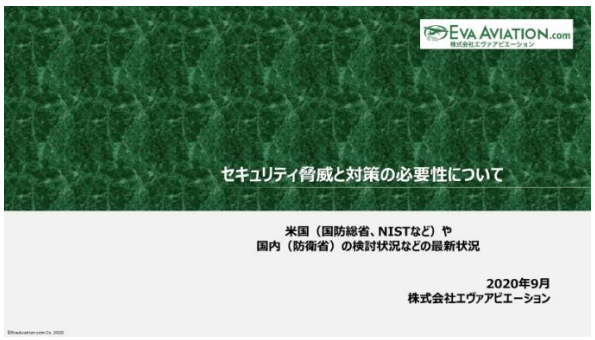
令和2年度 サイバーセキュリティお助け隊 事業説明会

セキュリティ脅威と対策の必要性について

米国（国防総省、NIST など）や国内（防衛省）の検討状況などの最新状況

令和2年9月

株式会社エヴァアビエーション

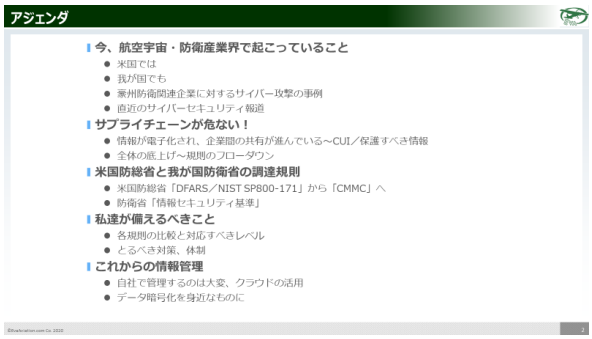


このたびは、サイバーセキュリティお助け隊事業において、弊社グループの企画にご参加いただきありがとうございます。

サイバーセキュリティに関心をお持ちの中小事業者の皆様に、セキュリティ対策が重要かつ具体的に規定されている航空宇宙・防衛業界の動向を重点的にお伝えします。

特に、米国の動向は世界をリードしていますので、米国　および、我が国の防衛省の動向を踏まえたご説明をいたします。

この業界でビジネス活動をしている、あるいはこれからしようとする事業者の方々に、具体的な対応策を検討いただける内容となっておりますので、ぜひご活用ください。

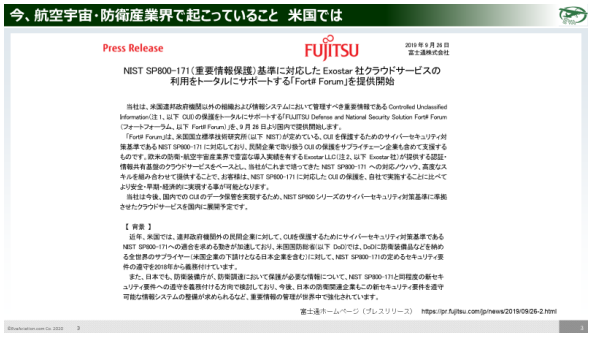


全体の流れです。

最初に、近年防衛産業界で話題となったニュースを通じ、「中小事業者を含む、サプライチェーンの関係者全員が、サイバーリスクに関わっていること」をお話しします。

続いて、米国のNIST（ニスト）およびCMMCについてです。周辺事情を、我が国の対応などもふまえて解説いたします。

最後に、「私達が備えるべきサイバーセキュリティ対策」についてお話しします。



米国の防衛産業で活用されている「情報共有サービス」を提供するエクソスター社と、昨年９月、富士通は提携を発表しました。「米国のサイバー防衛が日本に上陸する」という報道を記憶されている方もいらっしゃるかと思います。

記事の内容は、米国標準となっているNISTの規格に準拠した「情報共有サービス」を、日本国内にも提供するというものです。

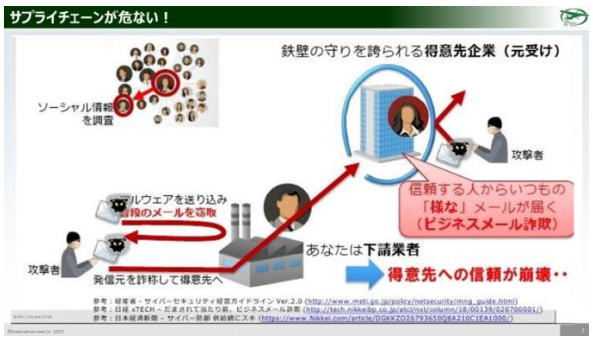
また、今年２月には、防衛省の「注意情報」が、契約業者である民間企業へのサイバー攻撃によって流出するという事案が公表されました。

その後も、同様の事案が何件か報告されています。

こういった状況は日本だけのことではありません。最新鋭の戦闘機・F-35に関する大量のデータが盗まれたというオーストラリアでの報道は、大きな衝撃を業界内外に与えました。

こちらは、昨年の６月中頃から７月中頃に報道されたサイバーセキュリティの記事を、PFUがまとめたものです。

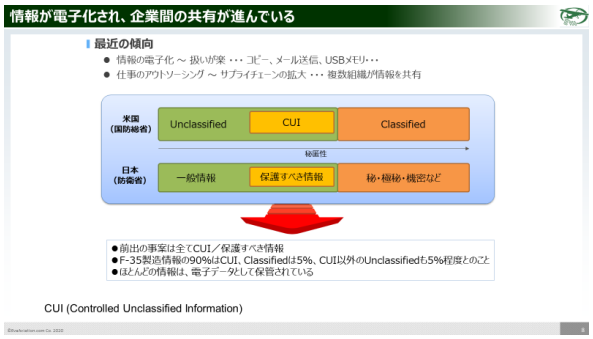
40件中、およそ半数が「Webサイトなどの脆弱性に関する報道」、その次にPC脆弱性の報道がありました。しかし、これでも全てではありません。



これまでにご紹介した事例に多く共通するのは、狙われているのはサプライチェーン、即ち下請け業者ということです。

元請け企業はガードを厳しくしていても、攻撃者は、契約のある下請け業者になりすまして、元請けの情報を盗みにゆく、という攻撃パターンもあるのです。

これでは、得意先との信頼関係が崩壊してしまいます。



昨今は情報の電子化が進み、取扱いが簡単になり、メールでやりとりされたり、USBメモリによる持ち運びが容易になりました。

そのこと自体は、仕事の効率化やコスト削減に、おおいに役だっていることはご承知の通りです。

そして多くのプロジェクトは、１社が単独で行うことは少なく、複数の企業などが共同で実施したり、アウトソーシングすることが一般的となっています。

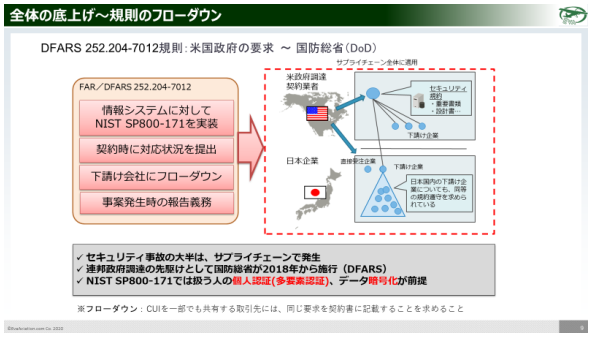
データの流通は活発に行われる一方で、しかし、そのデータを取り扱う関係者全てが、十分なセキュリティ対策を行えているわけではないため、

「サプライチェーン全体の中から、情報セキュリティの穴を探して攻撃する」という手法が台頭しているのです。

ここで狙われる重要な情報のことを、米国連邦政府ではCUI（シーユーアイ）と定義しました。一般情報、英語でUnclassifiedに含まれながらも、「管理すべき情報」として、CUIを定義したのです。日本の防衛省では、同様な情報を「保護すべき情報」と定義しています。

CUIがどのようなものかと言うと、例えばF-35戦闘機の製造情報の90%がCUIにあたり、Classifiedや「純粋な一般情報」は残り10%にすぎないと言われています。

この「CUI／保護すべき情報」がサイバー攻撃で狙われているのです。



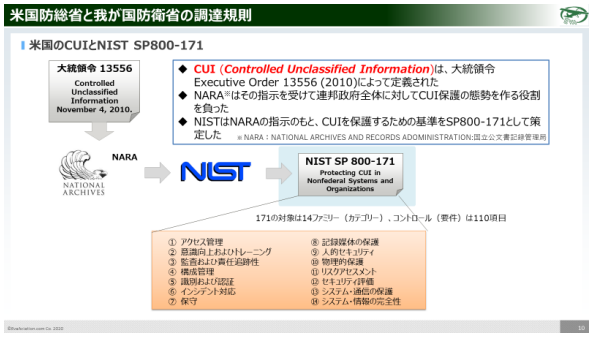
米・国防総省は、DFARS（ディーファース）という調達規則によって、2018年1月から、CUIを扱う契約事業者に対し、以下の４点を遵守させることを定めました。

第1に、NIST SP800-171という110項目のセキュリティ対策を実施すること、
第2にその実施状況を、契約時に提出することです。

第3には、前述の2項目を、CUIを扱う下請業者に対しても課す、いわゆるフローダウンすることが規程されています。

第4には、サイバー事案が発生した場合、72時間以内に米・国防総省まで「直接」報告することが規程されています。

特に、NIST SP800-171においては、情報システムを扱う利用者認証において、ID・パスワード以外の本人確認を求める「多要素認証」を行うことや、データを暗号化することなど、比較的高度な対策を要求しています。

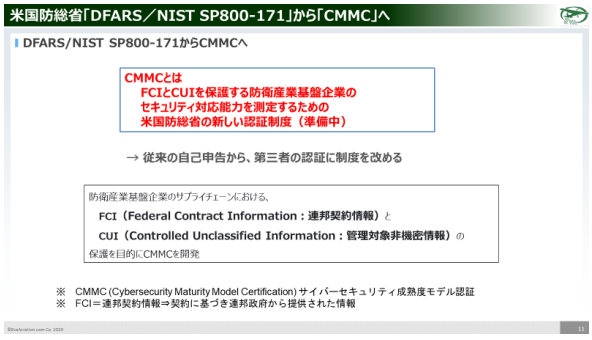


ここで、CUI および NIST SP800-171 の成立背景について整理してみましょう。

2010 年、当時の、オバマ大統領が発した大統領令により①CUI を定義し、②連邦政府全体で管理態勢を作るよう指示されました。

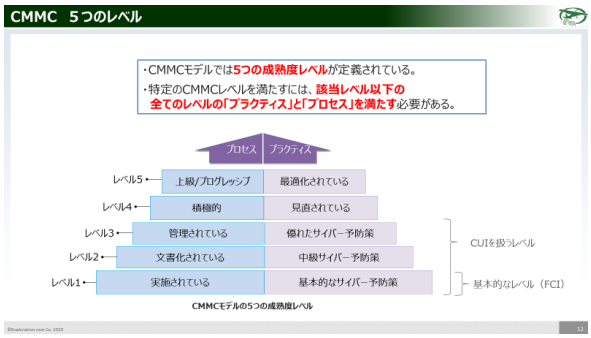
その任にあたったのが、NARA（ナラ）即ち国立公文書記録管理局です。規程を NIST（ニスト）に作らせ、最初の適用を DoD／国防総省に指示しました。NIST は、ここに挙げた、14 種類のファミリーと呼ぶグループに分類された 110 の対応項目を、SP800-171 として規程しました。

ISMS などの一般的な情報セキュリティー基準に比べると、特に「データの秘匿性」について重点をおいて作られています。そのほかの管理態勢については、「当然対策がとられている、という前提のもとに適用される」とアナウンスされました。



しかし、施行から１年程度しか経っていない2019年。米・国防総省は、DFARSによるSP800-171遵守のやり方を見直して、新たに「CMMC」というやり方に変える、と宣言しました。

CMMCとは、契約者全てが関わる「①FCI・連邦契約情報とCUIの両方を保護対象とした、②防衛産業基盤企業のセキュリティ対応能力を測定するための、米・国防総省の新しい認証制度」で、従来の自己宣言方式から、第三者に認証してもらうしくみに変更するものです。



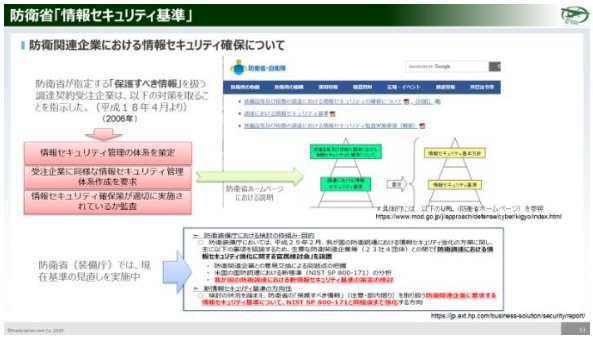
SP800-171では、110の項目「全て」について一律に遵守を要求しましたが、CMMCではレベルを５段階に分け、対象とする情報や契約者によって適用するレベルを決めるという方式になっています。

具体的な適用については、ことしの末に見込まれている発表を待たなくてはなりませんが、国防総省と直接または間接的に契約する全ての事業者は、レベル１の適用が義務づけられることが、アナウンスされています。

レベル１は全部で17項目。比較的難易度の低い要件が規定されています。しかしながら、国防総省の「対象サブ

ライチェーン事業者」は、全部でおよそ35万社と言われており、その全てに要求するということは、非常に画期的な取り組みであると言えます。

なお、従来のSP800-171に相当する110項目は、レベル３。さらに高度な、レベル４と５は、主にNIST SP800-172に規程される要件が適用される計画です。



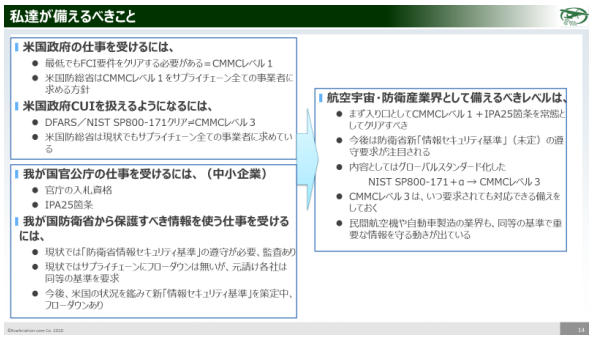
では、我が国の防衛省ではどのような規程があるのでしょうか。

ご存じのように防衛省では、平成18年よりCUIとほぼ同じ範囲を指す「保護すべき情報」に対して、「情報セキュリティ基準」と言われるおよそ70項目の遵守規程を策定しています。冒頭のニュースにあった「注意情報」はこれに含まれるものです。

防衛省は基準に沿った「情報セキュリティ管理体系」を各社に作ることを要求し、契約時にそれを監査する、としています。

この「基準」の元になっているのは「ISMS」であり、「受注企業は、全般的な情報セキュリティ態勢を取れるようになっている」ことを求めています。

なお、数年前より、「米国のNIST SP800-171と同程度まで強化した」新基準の策定にとりかかっており、近く、さらに厳しい基準として示される見通しです。



ここで、これまでお伝えしたことを整理し、「私達が備えるべきこと」を、考えてみましょう。

第1は、「米・国防総省、または連邦政府から直接・間接的に業務を請け負う事業者」は、CMMCレベル１を、クリアすることです。

その上で、「CUIを扱う可能性がある」ならば、CMMCレベル３クリアを目標にする必要がありますが、これはなかなかハードルが高いでしょう。

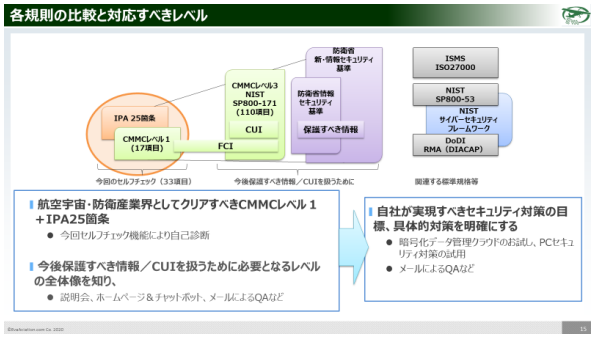
そして、米国政府はさておき、国内の政府系の仕事をしたいと考えている方には、現在明確に出されている「クリアすべき基準」はありませんが、自己宣言型を含めてさまざまなガイドラインが各所から出されています。

もちろん、防衛省と「保護すべき情報を扱う契約」を交わすためには、「防衛省情報セキュリティ基準」、ないしは、これから策定される「新基準」をクリアできる体制が必要です。

わたくし達の見解としては航空宇宙・防衛産業に関わろうとする事業者は、まず「IPA25箇条とCMMCレベル１を組み合わせた基準」を最低限クリアしておくことが必要と、考えています。

その上で、今やグローバルスタンダードになりつつあるNIST SP800-171と同程度と宣言されている「防衛省の新基準」も見据えて、CMMCレベル３を目標に、いつ要求されても良いように備えておくことが重要であると考えています。

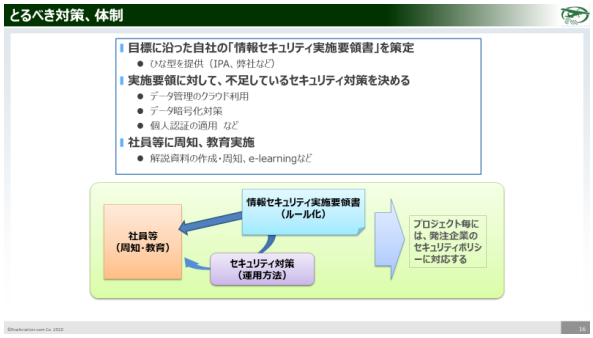
さらに、政府系以外、民間航空機や自動車製造の業界にも、同等の基準で重要な情報を守る動きが出ています。米国では、医薬品などライフサイエンスの業界で、すでに、NIST SP800-171の適用が始まっています。



こちらは、日米の基準の相関関係です。

のちほどご紹介するセルフチェック機能は、一番左のIPA25箇条と、CMMCレベル1をミックスした設問としており、最初に皆様が取り組むべき課題と考えています。

その上で今後、「保護すべき情報／CUI」を扱うために必要となる 各レベルの全体像への理解を深めていただき、みなさまそれぞれが目標とすべき対策を具体的に検討するというのが、わたくし達の提案です。



方針が決まったら、「情報セキュリティ実施要領書」として文書化します。ひな型も公開されていますので、ぜひ参考にしてください。

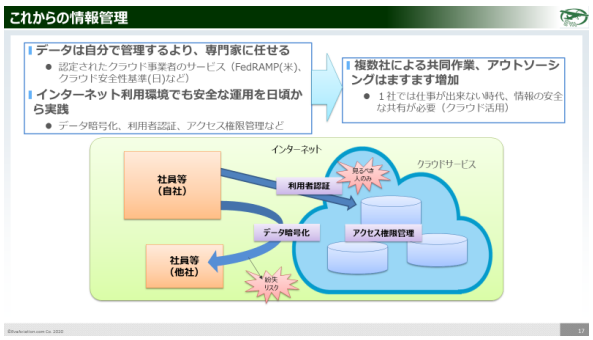
その中でも、CMMCレベル３を目標にした場合、我が国のほとんどの事業者において、まだ対応出来てない主な対策が、

① 「データ管理のクラウド利用」
② 「データ暗号化対策」
③ 「個人認証の適用」などです。

これらについては、今後、ひとつづつ対策を実践しながら、徐々に、セキュリティに強い態勢を作ってゆけば良いと考えます。

そして、実施要領書や具体的な対策が決まったら、社員に周知徹底するための教育や研修を行うことも大切です。昨今のテレワークの普及にあわせて、e-learningで行うことも良いでしょう。

なお、これらの規程の適用は、基本的には「契約」、即ち、プロジェクト毎の適用となります。従って、元請け企業のポリシーによって、若干のやり方や適用する対策も異なってきます。いずれにせよ、基本的な社内態勢が出来ていれば、臨機応変な対応も可能になると期待できます。



こうした規定とその対策を振り返ると、「これからの情報管理」の主流はどういった形態になるのか、推測が出来ます。

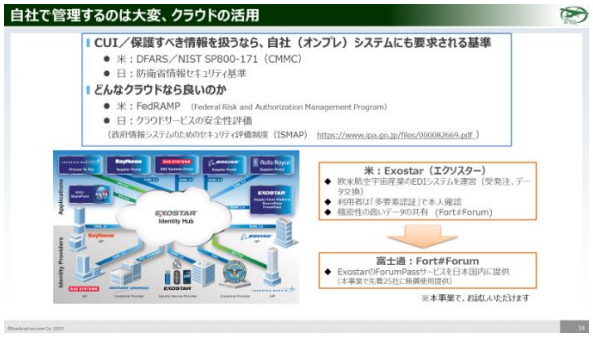
まず、「データは自分で管理するより、専門家に任せるようになる」ということです。日米とも、システムに対し厳しい要件を課しています。

自社システムでイチから対策を取るより、すでに認定されたクラウド事業者のサービスを使う方が、どれほど安心で、コスト削減になるでしょう。

認定制度としても、米国のFedRAMP、日本でも「クラウド安全性基準」などが整備されつつあります。

そして、「インターネット利用環境でも安全な運用を日頃から実践するようになる」。

規定への対策としては、特に「データ暗号化、利用者認証、アクセス権限管理など」に慣れておくことが挙げられますが、その結果、複数社による共同作業やアウトソーシングの活用は「ますます加速」し、「クラウドを活用した、情報の安全な共有」のさらなる普及や、重要性の高まりが予測されます。



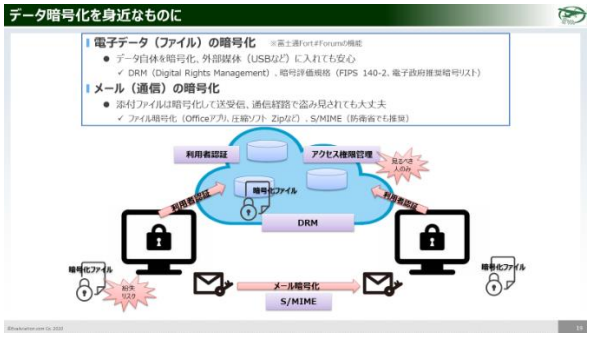
そういった「クラウドベースの、セキュアな情報共有」を何年も前から実現してきたのが、米国の航空宇宙・防衛産業において「ハブ」となっている、エクソスター社のサービスです。

エクソスターは2000年に、ロッキードマーチンやボーイングといった、欧米の航空宇宙・防衛産業企業によって「認証の共同運営を行うため」設立された会社です。

今では、全世界に30万人以上の利用者を持つ、航空宇宙・防衛産業のデファクトスタンダードな認証基盤であり、サービスです。

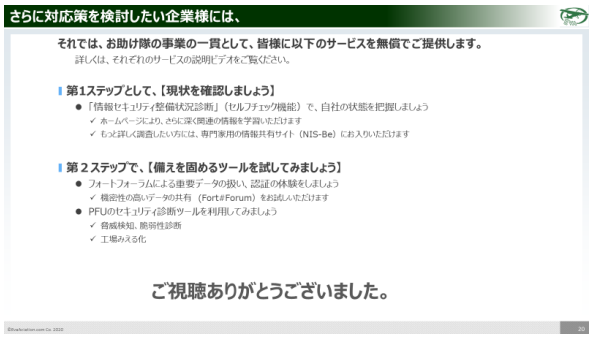
エクソスターのForumPassは、ご存じのマイクロソフト・シェアポイントによる情報共有を、航空防衛産業のニーズに沿って、セキュリティを強化したサービスです。

富士通はこれを「フォートフォーラム」という名称で販売しており、本事業でお試しいただけます。



さらに、フォートフォーラムにはデータの自動暗号化機能であるDRM（デーアールエム）が備わっています。DRMは対象のファイルを常に暗号化することで、サーバー、PC、USBメモリなど、どこにデータがあっても安全なファイル暗号化がされています。そして、「アクセス権限を持つ、限られた利用者だけがそれを参照できる」という仕組みをお使いいただけます。

また、防衛省ではメールの送受信時に通信経路を暗号化するS/MIME（エスマイム）の利用についても、推奨しています。これは、市販の電子証明書を購入して、PCなどの通信端末とメールソフトに設定することで簡単にお使いになることが出来ます。



以上で、「サイバーセキュリティお助け隊事業」における当グループの背景説明を終わります。
このあとは、ご提供するツール毎に説明ビデオをご覧いただきます。

まず、第１ステップの「情報セキュリティ　整備状況診断」をお試しください。
続いて第2ステップとして、機密性の高いデータ共有を実現する「フォートフォーラム」、および、PFUの「セキュリティ診断ツール」をお試しいただけます。

最後までご覧頂き、ありがとうございました。