Deloitte.
デロイト トーマツ

サイバーセキュリティ成熟度モデル認証 (CMMC)

はじめに

今年は、サイバーセキュリティ成熟度モデル認証(CMMC)の公開に伴い、米国国防総省(DoD)の請負業者と下請業者(以下、「請負業者」)に関するサプライチェーンに大きな変化が訪れます。2020年1月にCMMC v1.0が公開され、今後、請負業者に関する要件がDoDのRFIとRFPに盛り込まれる予定となっています(それぞれ2020年の6月と9月に要件を盛り込むことを目指しています)。

以下、理解しておくべき事項についてご説明します。

CMMCとは

2016年10月21日、DoDによって、国防連邦調達規則補足(DFARS)を修正するための最終規則が採用されました。この修正によって、DoDのすべての請負業者は、ある特定の種類の管理対象非機密情報(CUI)[1]について、2017年12月31日までに新しいサイバーセキュリティ防御手段およびサイバーインシデント報告手段を導入することが義務付けられました。そして、この期限が過ぎ、以後さまざまな要件が規定されたのに伴い、DoDは、各種の規格やリーディングプラクティスから導き出された幅広いサイバーセキュリティモデルの開発に焦点を移しました。DoDの利害関係者との共同作業により、そのようなモデルとしてCMMCが設計されました。今後、セキュリティをDoDの調達の基盤とする取り組みにおいて、このCMMCが必要不可欠となります。CMMCモデルは5つの成熟度レベル(レベル1〜5)で構成され、レベルが高くなるにつれて達成すべき要件が多くなります。レベル5は達成すべき要件が最も多く、最もセキュリティが高いレベルとみなされます。CMMCは、従来の規則(DFARSなど)といくつか共通点がありますが、従来の規則とCMMCとの大きな違いは、CMMCでは自己認証が認められていない(すなわち、第三者機関による認証を必要とする)という点にあります。今後数か月の間に、認定機関が設立される予定であり、この認定機関がDoDの請負業者に対するCMMC認証を担当する第三者監査機関のトレーニングと認証を行うことになります。

CMMCモデルが対象とするもの

CMMCモデルは、主に、連邦契約情報(FCI)と管理対象非機密情報(CUI)を保護することを目的として設計されました。CMMC v1.0では、アクセス管理から状況認識に至るまでの17のサイバーセキュリティ領域が網羅されています。これらの領域は43の能力で構成されており、各能力は、さまざまなサイバーセキュリティフレームワークとリーディングプラクティスから導き出された171のプラクティスによって裏付けされています。CMMCは、導入レベルに応じた5つの成熟度モデルで構成されています(例えば、レベル1では17のプラクティスしか要求されませんが、レベル5では171のプラクティスをすべて実施することが求められます)[2]。要求される成熟度レベルは、扱われるDoD情報の機密レベルにより異なります。例えば、機密レベルが非常に高い情報を扱う企業は、レベル5の認証を取得しなければなりません。

サイバーセキュリティリスクは主体的に管理する必要があります。DoDのサプライチェーンに連なる企業にとって、CMMCは、第三者機関による評価の対象となる、明確かつ測定可能なサイバーセキュリティ要件を設定するものです。

誰が対象なのか

サイバーセキュリティを調達プロセスの不可欠な要素にするというDoDの取り組みを支持するために、サプライチェーン内のすべての請負業者は、規定された要件に従う必要があります(すなわち、請負業者は契約の入札に参加することはできますが、必要な認証レベルに達するまで落札・受注することはできません)。レベル1が、すべての請負業者が達成すべき最低限の要件になり、個々のRFIまたはRFPにおいてより高いレベルが指定されることになります。

なぜ今なのか

最近の複数のインシデントによって、国防関係の請負業者と下請業者のサイバーセキュリティの脆弱性が明らかになりました。このような脆弱性や、ますます増加しつつあるサイバーセキュリティリスクに対処するため、DoDは、サイバーセキュリティのコンプライアンスを、調達プロセスの重要かつ必須の要素にしました。

今後の予定

2020年春にCMMC認定委員会が設立される予定であり、この委員会がCMMC第三者評価機関(C3PAO)の統括組織となります。

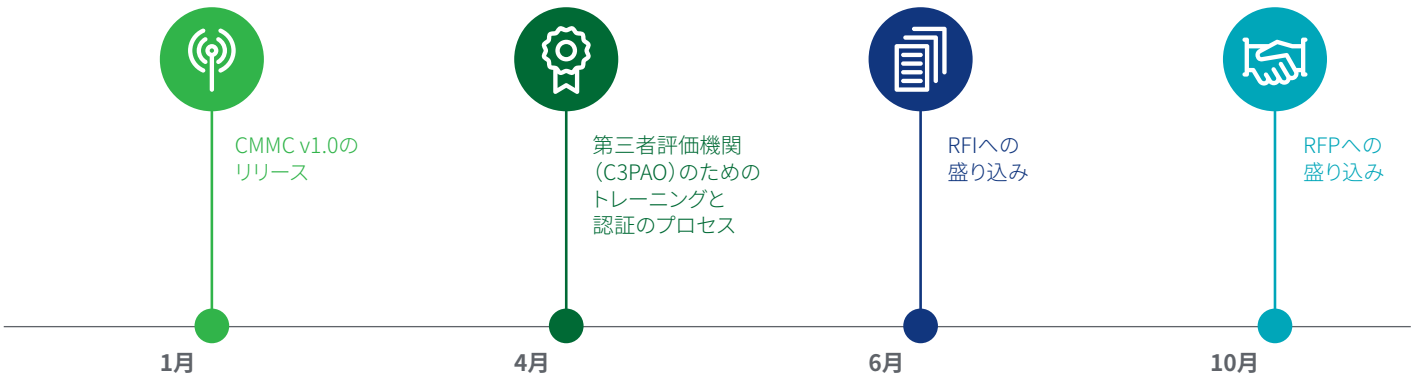
各C3PAOは、将来DoDの請負業者の評価を行うためには、トレーニングを受講し、各種の認証要件を満たす必要があります。また、DoDの請負業者は、2020年の半ばから終わりまでに、C3PAOの監査を受け、サイバーセキュリティ成熟度モデル認証を取得することが期待されています。

課題

今や情報セキュリティのリーダーらは、これまで以上に、変化し続ける情報セキュリティ要件や、侵入・データ漏洩の脅威に見舞われています。請負業者は、自らのビジネス環境に特有のリスクに対処し、しかるべきセキュリティ対策を実施することに関して最終的な責任を負っています。また、CUIを保護し、インシデントの報告に関する要件を満たすために、請負業者は、CUIを特定し、該当する情報を保護するための適切な措置を講じることが求められます。この要件に関して、以下のような、いくつかの陥りやすい落とし穴があります。

・CUIの特定
・メディアの保護とタグ付け
・トレーニング、ポリシー、手続きの策定と実施

2020年のCMMCのスケジュール



デロイトが提供可能な支援

デロイトは、業種に特化した幅広いアプローチを採用し、コスト削減、生産性、リスク軽減に関する目標の達成をサポートします。当社は、DoDの請負業者の皆さまに対して、CMMCの要件を満たすための主体的で持続的なアプローチを採用することを推奨しています。デロイトでは、以下をはじめとするさまざまな方法での支援が可能です。

レディネスサービス

デロイトの専門家が、CMMCフレームワークと照らし合わせて既存のプロセスとコントロール手段を評価し、それらに潜む欠点を見つけ、コンプライアンスの達成を支援します。欠点が見つかった場合は、その欠点に対処するための対応計画の策定と修復活動をサポートします。

サプライチェーンの洗い出し

請負業者の皆さまは、自社組織に関して対応すべきCMMC要件とは別に、サプライチェーンの混乱という間接的なリスクも考慮しなければなりません。サプライチェーンでは下請業者が重要な役割を果たしているため、多くの企業は、特定の契約に関して下請業者がそれぞれのCMMC要件に準拠できないリスクを評価し、そのリスクに対応する必要があります。ある重要な下請業者が所定のCMMC要件を満たせない場合、該当する契約に関してその下請業者を使用できなくなり、ひいては、その元請業者のサプライチェーンに大きな混乱が生じる可能性があります。また、このリスクは特に大きな懸念となるおそれがあります。なぜなら、サプライチェーン内の該当する下請業者やサービスプロバイダーを特定するだけでも、極めて複雑で困難な作業だからです。当社は、幅広い経験と技術リソースを活用して、お客様のサプライチェーンを特定、マッピング、プロファイリングし、サプライチェーンの混乱の軽減に役立つ透明性が高く価値のあるデータポイントを提供します。

CUIの特定

今日の複雑なコンピューティング環境においては、CUIがどこにあり、どこから送信されてきたのかをエンドツーエンドで特定することは、困難で気が遠くなるほどの作業です。当社は、お客様の環境においてCUIの保存場所や送信元となっている部分のインベントリを作成し、お客様のコンプライアンスプログラムを実現するためのロードマップの策定を支援することができます。

システムセキュリティ計画とPOAMの作成

管理が行き届いた環境では、組織の環境の変化に応じて定期的に更新されるシステムセキュリティ計画を作成することが必要不可欠です。また、未実施のセキュリティ要件を削減するために「行動計画とマイルストーン（POAM）」を作成して、それをシステムセキュリティ計画に盛り込むことが可能です。当社は、システムセキュリティ計画とPOAMの作成と文書化のサポートのほか、既存計画の更新に伴うレビューも行います。

CMMC認証のサポート

認証と監査には、多大な時間を要するため、日常業務をこなしながらそうした作業を行うことは困難です。そこで、認証機関との窓口となる担当者を置くことが、認証を取得する上で大いに役立ちます。デロイトは、認証と監査の実施とサポートの両方に関して幅広い経験を備えているため、認証取得の準備、認証機関との窓口対応、指摘事項への対応のサポートが行えます。

インシデントによる損害の評価

CUIが漏洩するようなインシデントが発生した場合、その損害の評価をサポートするとともに、DoDから要求された証拠文書の準備をサポートします。

市場の評価・評判

航空宇宙・防衛業界でのデロイト
デロイト トウシュ トーマツ リミテッド（DTTL）のメンバーファームは、フォーチュン500社に含まれる航空宇宙・防衛関連企業の95%と取引があります。

グローバルリーチ
デロイトの航空宇宙・防衛（A&D）事業には、米国内の600名を超える専門家とグローバルネットワーク内の1,500名を超える専門家が携わり、その多くは業界経験や軍事経験を備えています。

デロイトの加盟組織
米国航空宇宙産業協会（AIA）、米国国防産業協会（NDIA）、米国宇宙財団、米国専門サービス協議会（PSC）

お問合せ

デロイト トーマツ サイバー合同会社
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡

Endnotes

1. US Department of Defense, Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, September 21, 2017, https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf, accessed January 2020.

2. US Department of Defense, Cybersecurity Maturity Model Certification, January 30, 2020, https://www.acq.osd.mil/cmmc/docs/ CMMC_Model_Main_20200203.pdf, accessed February 2020.

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、
本サービス内容がご提供できない可能性があります。詳細はお問合せください。

デロイト トーマツ サイバー合同会社
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約40都市に1万名以上の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人のひとつまたは複数を指します。DTTL（または“Deloitte Global”）および各メンバーファームならびにそれらの関係法人はそれぞれ法的に独立した別個の組織体です。DTTLはクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、オーストラリア、ブルネイ、カンボジア、東ティモール、ミクロネシア連邦、グアム、インドネシア、日本、ラオス、マレーシア、モンゴル、ミャンマー、ニュージーランド、パラオ、パプアニューギニア、シンガポール、タイ、マーシャル諸島、北マリアナ諸島、中国（香港およびマカオを含む）、フィリピンおよびベトナムでサービスを提供しており、これらの各国および地域における運営はそれぞれ法的に独立した別個の組織体により行われています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務およびこれらに関連する第一級のサービスを全世界で行っています。150を超える国・地域のメンバーファームのネットワークを通じFortune Global 500®の8割の企業に対してサービス提供をしています。“Making an impact that matters”を自らの使命とするデロイトの約286,000名の専門家については、（www.deloitte.com）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of
Deloitte Touche Tohmatsu Limited

© 2020. For information, contact Deloitte Tohmatsu Cyber LLC.