<<White Paper>>

米国 NIST SP800-171 による連邦政府調達基準への対応について

～米国の要求背景とその具体的対応方策～

米国は 2010 年 11 月の大統領令（Executive Order 13556 (1)）により、管理すべき重要情報（CUI：Controlled Unclassified Information 以下 CUI）についてどのように取扱われるべきか体系的規定の策定を指示しました。その結果出来上がった指針が NIST(※1) が作成した SP800-171(2) (連邦政府機関以外の組織および情報システムに対する CUI の保護について）であり、具体的な要件が NIST SP800-53(Security and Privacy Controls) (3) , SP800-63 (Electronic Authentication Guideline) (4) などのドキュメントとして整備されています。

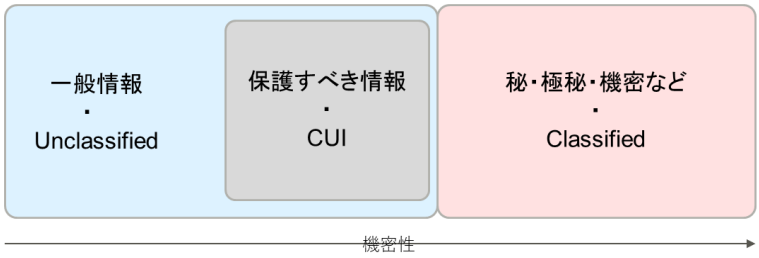
また、国防総省 (DoD;Department of Defense 以下、DoD）は、DFARS(※2) 252.204-7012　Safeguarding Covered Defense Information and Cyber Incident Reporting (5)により、本指針に示された要件の遵守を契約のサプライチェーンに関係する企業すべてに、2017 年 12 月 31 日までという期限付きで対応を求めています。

(1) CUI とは

CUI とはどのような情報か。大統領令には「such as information that involves privacy, security, proprietary business interests, and law enforcement investigations」と書かれており、仕様書や設計図などもその対象とみなせる広範囲なものです。

従って、米国政府調達に関わるすべての企業が、その手にするほとんどの重要情報が対象であり、これは米国に要求されるまでもなくセキュリティ対策として我が国官民においても自主的にも対応すべき水準のものと言えます。

我が国 (防衛省) においても、秘として指定する情報以外の重要情報を「保護すべき情報」として契約企業側でも情報セキュリティの確保態勢を取るように指示してます（契約時の特約条項)。



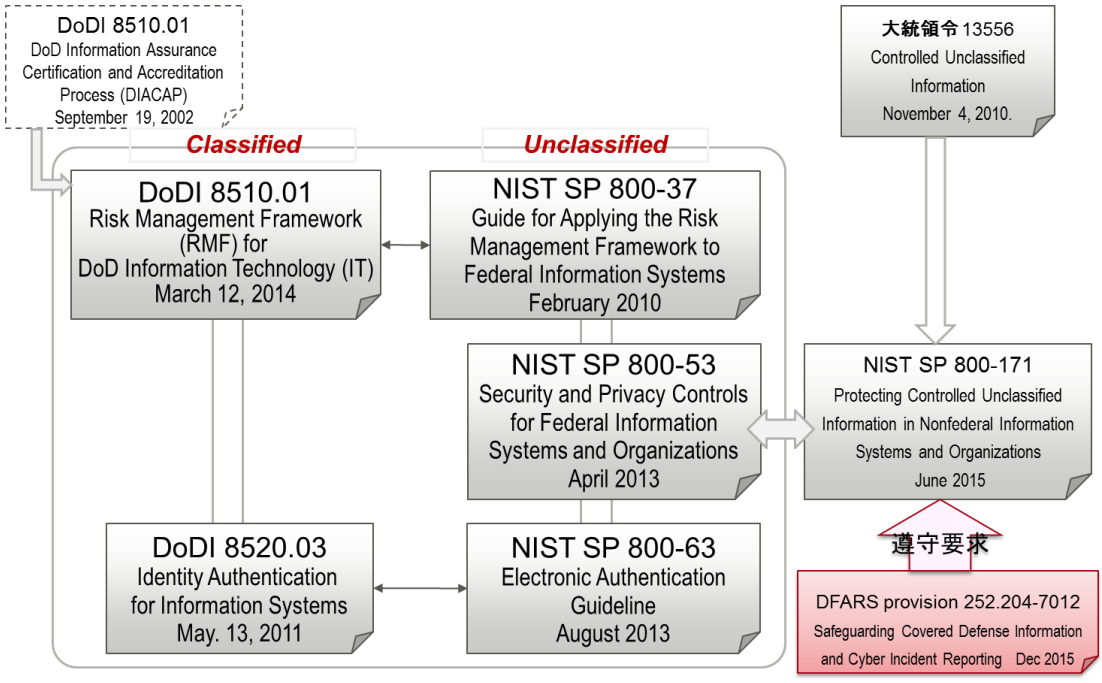
機密性の高さによって対象とする情報をおおまかに分類すると、上図のように秘・極秘・機密など防衛省が特別に取扱いを決めているもの（米国の Classified 情報に相当するが、

明確な対比は示されていない)、そして、特別な取扱の対象外としているその他一般情報（米国の Unclassified に相当）があります。昨今、その一般情報の中でも「保護すべき情報」（米国の CUI に近いものと推定される）の扱いについて議論されているところです。

(2) 米国の規定類の相関

米国では、Unclassified の取扱いについては NIST が規定し（SP800-37 RMF)、軍事秘密などの情報を加えた Classified を含む体系は DoD が規定しています（DoDI (※4) 8510.01 RMF)。CUI の扱いについては、Unclassified であるところから NIST（SP800-171）が規定し、DoD が調達特約条項の DFARS（252.204-7012）によって遵守を要求するという形になっています。

なお下図は、関連する米国の規定類の相関を示したものです。従来から DoD のセキュリティ要件として知られてきた DIACAP（ダイアキャップ）は、現在では RMF（アールエムエフ）という規定に変更され、このような体系の中で運用され始めています。



(3) CUI の歴史的経過

CUI は、ブッシュ大統領の 2008 年指令で発行された unclassified カテゴリーの一つであり、これまでの「For Official Use Only」(FOUO)や「Sensitive But Unclassified」(SBU)などのカテゴリーを置き換えることになるものです。この覚書は 2010 年の大統領令 13556 で撤回され、そこに含まれていた指針は拡張されて、全連邦政府機関における統一性の改善と、CUI プロセスの標準的方針の開発に至っています。

(4) CUI の背景

unclassified 情報に関して様々な連邦政府機関によって使われてきた簡易的な管理標示は、これまで混乱を生み出し、政府内外での情報共有を阻害してきました。CUI は定義からすれば unclassified ですが、それにもかかわらず、法令、規則、又は連邦政府機関の方針を基に、公開から守ることを必要とすると理解されています。こうした情報にはこれまで連邦政府機関全体に、100 を超える標示が存在し、このその場凌ぎ的な機関固有アプローチは、非効率や混乱を生み出し、保護すべき情報の適切な安全確保に失敗し、逆に情報共有を不必要に制限してきました。新たな CUI の特徴の一つは、各連邦政府機関の CUI に関する自律性を限定し、各機関が一貫した政府全体の標準に従うことを要求していることです。

従って、CUI カテゴリーは、連邦政府機関全体で CUI を明示する唯一の手段であり、各機関は、CUI 外の如何なる unclassified 情報をも管理することは許されず、また何が CUI と看做されるかについて独自に決定することもできない、とされています。

(5) セキュリティ対策の動向

標的型メール攻撃など昨今のサイバーセキュリティー事情から、インターネット接続されているオフィスの PC 内にあるデータは意図を持った情報窃取には無力であることが理解され始めています。しかしながら、平常の仕事を行うためにはリスクの高いインターネットに接続しつつも、少しでも被害を局限化するため、最低限の運用ルールに従うことが重要です。

これまで我が国の産業界は情報システムのセキュリティ対策については ISMS(※3)(ISO/IEC 27001)を中心に対応してきました。しかしながら、米国は ISMS と対比可能な体系でありながら独自の要件を盛り込んだ体系を NIST により策定しています（SP800-53 など)。

この度の DFARS で求められた要件は、米国の DoD 調達案件に対して関係する下請け企業すべてに対して SP800-171 の遵守を要求するものです。従って、DoD の契約案件のうち、別途示される CUI を受理しているプロジェクトは、契約元請けか下請けかによらず本対応を要求されるものと考える必要があります。

(6) NIST SP800-53 と 171 の違い

NIST SP800-53 などは連邦政府機関自身に対する要件として規定されていますが、SP800-171 は連邦政府機関以外（外国政府組織や契約企業等）への CUI の扱いについて遵守を求める事項として新たに規定されたものです。なお、現時点では DFARS として DoD 調達案件のみが適用対象とされていますが、FAR(※5)として連邦政府機関の調達案件すべてについても適用される方針です。

なお、NIST SP800-53／171 と ISMS (ISO/IEC27001)を比較すると、NIST はより具体的な指針であると評されており、ISMS を包含していると見做すことができます。従って、

ISMS を取得している組織は比較的容易に今回の NIST 要件に対応できるものと考えられ、特に米国と取引の多い組織は NIST にも対応させることがビジネス上のメリットになると言えると考えています。

(7) NIST SP800-171 への対応要領

具体的に SP800-171 に対応する、とはどのようなことをすれば良いかという点においては、以下の２点を行うことと考えられます。

- SP800-171 の要件リストに対する対応状況を整理し、未対応事項については今後の対応方針を明記し、そのフォローアップを行うこと
- 適切な第三者によりその内容の確認を得ること

800-171 Security Requirement Identifier	NIST SP 800-171 Security Requirement	SRC Defined Security Requirement Parameters (If Any)	Implementation Status	Control Provider	What is the Solution and how is it implemented	Notional Implementation Date	Actual Implementation Date	NIST 800-53r4 Cross-Reference
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).							AC-2, AC-3, AC-17
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.							AC-2, AC-3, AC-17
3.1.3	Control the flow of CUI in accordance with approved authorizations.							AC-4
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.							AC-5
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.							AC-6, AC-6(1), AC-6(5)
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.							AC-6(2)
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.							AC-6(9), AC-6(10)
3.1.8	Limit unsuccessful logon attempts.	a. 3, b. 15 minutes, locks the account/note for at least 15 minutes or unlocked by an administrator [CNSSI-1253]						AC-7

要件リスト対応表のイメージ（by SRC, Commercial Cyber Security Services）

NIST SP800-171 の要件は、以下に示す 14 項目（ファミリー）に分類されており、さらにセキュリティ侵害を受けやすいユーザ、プロセス、インフラストラクチャを対象とした 109 のセキュリティ管理項目が示されています。

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・認証
⑥ インシデントレスポンス
⑦ メンテナンス
⑧ 記録メディア保護
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・情報の完全性

これらは、使用するシステム要件に関するものと、組織運用規則で対応するものに分けることができます。従って、このセキュリティ管理項目に対応するには、NIST の要件を満たすコンピュータシステム（サーバー、ネットワーク、PC、認証など）を構築し、その運用にあたる適切な規則を決めることとなります。なお、要件を満たせない場合は、満たすための方策と期日を示すことが必要です。

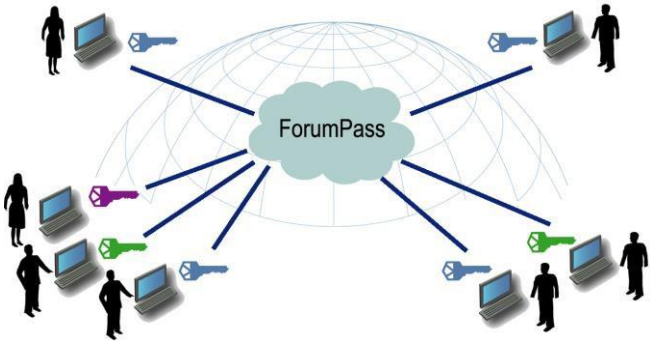
＜第 2 部＞

(1) Exostar ForumPass の概要

Exostar のコミュニケーションサービスは、米国の航空・防衛業界での使用実績も長く、NIST に準拠していると政府・業界から認められているサービスです。特に、データ共有やコラボレーション機能である ForumPass Defense は、マイクロソフトの SharePoint をベースとしており、使い勝手についても世界標準となっているものです。昨年からは、Rights Management Protection（デジタルデータ保護機能）が追加され、ダウンロードしたデータについても暗号化され、電子証明書による認証が検証されない限り開けないという環境を提供します。

また、認証についても NIST SP800-63 に基づく認証レベルによるユーザ管理となっており、多要素認証・シングルサインオンを実現しています。以下に、主要な機能を列挙します。

チームコラボレーション・管理



- チームメンバーが最新状況/スケジュールを確実に認識するよう、案内/通知による連絡
- ForumPass と Outlook カレンダーの統合で予定を一覧表示
- カレンダーのシェアにより、チームの動きを見える化し、業務情報へのタイムリーなアクセスを提供
- グローバルなマルチメディア情報交換のために、リアルタイムまたは計画的な Web ミーティングを無制限に開催可能
- 知識管理リポジトリを作成する wiki とブログの活用
- タスクやスケジュール把握のためにプロジェクト管理を表示
- ビジネス向けソーシャルツールを用い、コミュニケーションを促進

強力なチームサイトによるドキュメント管理

- 迅速なコラボレーションのためにプロジェクトライブラリにチームのドキュメントを追加
- 厳重なチェックイン/チェックアウト手順と最新の制御機能により、ドキュメントの保護と完全性を確保
- Microsoft Office と連携したシームレスなドキュメント管理

ワークフロー管理

- 実行の効率化と一貫したポリシーの遵守のために、ビジネスプロセスを保存また自動化
- あらかじめ設計されたテンプレートで導入を加速
- SharePoint Designer、InfoPath、また Visio との連携により、カスタムのワークフローを作成、維持

MyWorkspace による個人カスタマイズ

- ユーザの生産性を最適化するためのカスタマイズ画面
- プロジェクトに関するミーティング、タスク、通知、また意見交換などを一箇所に表示

複数レベルでのセキュリティ管理

- データ、プロジェクト、また組織要件に対応する、更に強固な認証強度を複数のレベルから選択可能
- ディレクトリサービス発行のトークンを用いてユーザアイデンティティを認証する環境により、複数企業へのセキュアなシングルサインアクセスを実現
- サイト、ライブラリ、データなどへのアクセス許可を役割ベースで設定
- データベースレベルでの暗号化により、情報を保護
- 内部ポリシーと外部規制基準の遵守を促進する監査でユーザの行動を追跡

Rights Management Protection（デジタルデータ保護機能）

デジタルデータ保護機能では、ドキュメント毎に暗号化するきめ細かなセキュリティを設定できます。Microsoft Word や Excel のようなドキュメントをネイティブアプリケーションで復元するには、（多要素認証による）ユーザ認証が成功した場合にのみ復元されます。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の権限に基づき、閲覧、印刷等の機能を動的に設定します。

※1　NIST (National Institute of Standards and Technology)
※2　DFARS (Defense Federal Acquisition Regulation Supplement)
※3　ISMS (Information Security Management System)
※4　DoDI (DoD Issuances)
※5　FAR (Federal Acquisition Regulation)

参考文献

(1) Executive Order 13556 -- Controlled Unclassified Information November 04, 2010
https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

(2) NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations　(NIST 2015)
http://csrc.nist.gov/publications/PubsSPs.html#SP 800

(3) NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

(4) NIST Special Publication 800-63 Digital Authentication Guideline
http://csrc.nist.gov/publications/PubsSPs.html#SP 800
(NIST SPECIAL PUBLICATIONS (SP))
https://www.ipa.go.jp/security/publications/nist/
(日本語訳、IPA/ISEC（独立行政法人情報処理推進機構 セキュリティセンター))

(5) DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
http://www.acq.osd.mil/se/docs/DFARS-guide.pdf

(6) Controlled Unclassified Information : From Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Controlled_Unclassified_Information

(7) Secrecy News : "Controlled Unclassified Information" Is Coming
Posted on May.11, 2015 in CUI, Secrecy, security culture by Steven Aftergood
https://fas.org/blogs/secrecy/2015/05/cui-is-coming/