Vol.2020-DPS-182 No.1
Vol.2020-CSEC-88 No.1
2020/3/12

中小企業に NIST SP800-171 準拠を求めた場合の課題と解決策

中川　哲[†1]　後藤厚宏[†2]

概要：米国政府は，今後，防衛産業以外のサプライチェーンに対しても NIST SP800-171 準拠を求める方針で進めている．日本の中小企業に対して NIST SP800-171 準拠を求めた場合「どこから手をつけて始めれば良いか分からない」といった課題が生じると提起する．本稿では，この課題を解決し，中小企業が NIST SP800-171 準拠を達成するために「NIST SP800-171 版 優先順位付けアプローチ」を提案する．そして，このアプローチ手法の妥当性について検証をおこない，課題解決に繋がるか考察する．

Problems and Solutions when SMEs are required to comply with NIST SP800-171

SATOSHI NAKAGAWA[†1]　Atsuhiro GOTO[†2]

Abstract: In the future, the U.S. government is pursuing NIST SP800-171 compliance for supply chains other than the defense industry. When Japanese SMEs are required to comply with NIST SP800-171, they raise the issue of "I don't know where to start." In this report, we propose "Prioritized Approach for NIST SP800-171" to solve this problem and enable SMEs to achieve NIST SP800-171 compliance. Then, we verify the validity of this approach method and consider whether it will solve the problem.

1. はじめに 背景と研究の目的

あらゆる業種や規模の企業が IT で繋がる中，委託先や取引先も含めたサプライチェーン全体のサイバーセキュリティの管理徹底が必要である．また今後，米国や EU 等のレギュレーションにより日本企業もセキュリティ強化が求められることが予想される．このような背景を踏まえ，グローバルサプライチェーンを構成する日本の中小企業が，NIST SP800-171 がベースとなるグローバルスタンダードに準拠する場合の課題を分析し，その解決策を提案する．これにより日本の中小企業のセキュリティ対策の底上げ，ひいてはサプライチェーン全体のセキュリティレベル向上に資することを目的とする．

1.1 研究の対象

近年における IT システムや提供する製品・サービスにおいて，設計・開発・製造・運用・保守・廃棄に至るまでの一連のプロセスにわたり，業務の一部を外部の企業に委託するケースが一般的である．その委託が重層的に連鎖する形態のことをサプライチェーンと言う．このサプライチェーンは，近年の IT 化やグローバル化の流れで企業の海外アウトソーシングの利用が広がった結果，あらゆる国・業種・規模の企業で構成するグローバルサプライチェーンとなった．そして同時にグローバルサプライチェーンから重要情報が流出してしまった場合，経済安全保障上の問題に繋がるとの問題意識が広がっている．本研究では，このグローバルサプライチェーンを研究の対象とする．

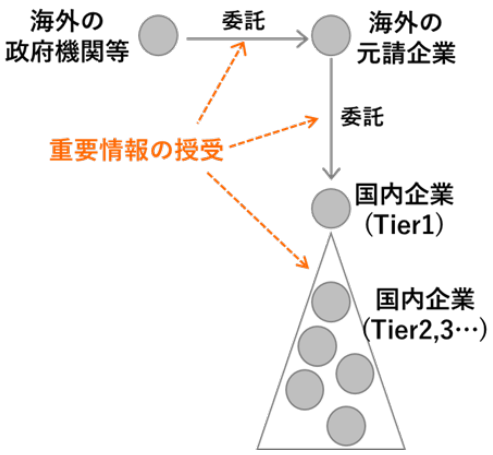

図 1　グローバルサプライチェーン

1.2 グローバルサプライチェーンにおける情報漏洩事例

グローバルサプライチェーンの脆弱な Tier2 以下の中小企業を狙った攻撃は実際に起こっている．2017 年に豪州で起きた防衛関連企業を狙ったサイバー攻撃の事例 [1]がある．豪州の防衛関連業者のネットワーク内に，攻撃者が 4 ヶ月間にわたり不正アクセスをおこない，重要情報を窃取した．その情報は，豪州政府が調達予定であったロッキードマーチン社製の F35 戦闘機，ボーイング社製の P8 哨戒機等に搭載する兵器システムに関するものだった．情報を漏洩した企業は，元請企業から 2～3 階層下に位置する 50 人規模の中小企業であり，情報システム管理者が 1 人しかいない状

†1 情報セキュリティ大学院大学
Institute of Information Security
†2 情報セキュリティ大学院大学
Institute of Information Security

Vol.2020-DPS-182 No.1
Vol.2020-CSEC-88 No.1
2020/3/12

況だった．

この事例で漏洩した情報は，戦闘機等に搭載される製品の仕様書と言われており，米国政府の情報分類においてCUIに該当するものだった(図 2)．CUI とは，機密情報には該当しないが，「管理すべき重要情報」のことである．例えば，情報システムの分野においては，システムの設計書やマニュアル，技術報告書，データセット，実行コード，ソースコードがこれにあたる．

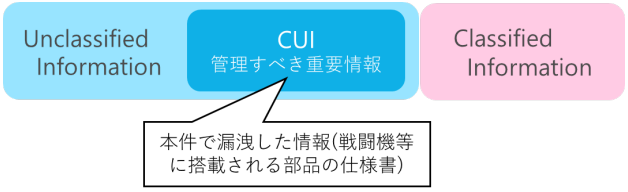

図 2　CUI に該当する情報が漏洩

2. NIST SP800-171 の概要

2.1 これまでの経緯

NIST SP800-171 [2]は，CUI を保護することを目的とした情報システム・組織のセキュリティ要件として 2015 年 6 月に米国政府によって発行された．2016 年 5 月に発行された FAR（連邦調達規則）52.204-21 では，すべての CUI 保有産業について NIST SP800-171 を調達基準とする旨が明記された．続いて 2016 年 9 月に CFR（32 連邦規則）2002.14 が発行され，適用時期は各省庁に委ねられている．

米国防総省は，2016 年 10 月に DFARS（国防調達規則）252.204-7012 [3]を発行し，「米国防総省と契約があり，CUI を取り扱う防衛関連企業は，2017 年 12 月 31 日までに NIST SP800-171 を遵守すること」を義務化した．これにより，元請け企業のみならず下請けとなる中小企業も遵守を求められることとなった（図 3）．それにより，米国防総省と直接契約のない日本企業においても，米国防衛企業の下請け企業として CUI を扱っている場合，NIST SP800-171 の遵守を要求される．

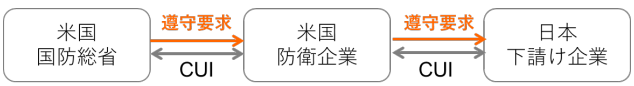

図 3　NIST SP800-171 遵守のフローダウン

2.2 NIST SP800-171 の特徴

NIST SP800-171 とは，米国政府の委託先(外国政府，民間企業）の情報システムにおける「CUI 保護」を目的としたセキュリティ要件である．以下に NIST SP800-171 の特徴 3 つについて述べる．

① NIST SP800-171 は 14 個のファミリーと 110 個のセキュリティ要件で構成され，その 7 割が技術的要件という特徴がある（表 1）．また，多要素認証や FIPS-140 認定の暗号化を必須対策の要件としており，日本で馴染みのある ISO/IEC27001 よりも求められている技術レベルが高い．このことから，NIST SP800-171 準拠を進めるにあたっては，少なくとも企業内に情報システムの技術者が 1 名以上必要と言える．

表 1　NIST SP800-171 の体系

ファミリー	要件数	ファミリー	要件数
① アクセス制御	22	⑧ 記憶媒体の保護	9
② 意識向上と訓練	3	⑨ 人的セキュリティ	2
③ 監査と説明責任	9	⑩ 物理的保護	6
④ 構成管理	9	⑪ リスクアセスメント	3
⑤ 識別と認証	11	⑫ セキュリティアセスメント	4
⑥ インシデント対応	3	⑬ システムと通信の保護	16
⑦ 保守・メンテナンス	6	⑭ システムと情報の完全性	7

② NIST SP800-171 は「機密性」に特化したセキュリティ要件という特徴がある．なぜなら，NIST SP800-171 の目的が「CUI を漏洩することを防ぐ」ことだからである．米国政府は，委託先企業における CUI の保護に注力させるため，NIST SP800-171 の中では完全性や可用性に関する要件を必要最低限に留めている．

③ NIST SP800-171 はセキュリティの「管理策」ではなく，セキュリティの「要件」を規定している．よって，実際に NIST SP800-171 の要件をクリアするためには，何らかの管理策を用いた方が取り組み易い．NIST SP800-171 を規定している文書の中では，付録として NIST SP800-53 や ISO/IEC27001 とのマッピング表が掲載されているが，NIST は必ずしも NIST SP800-53 や ISO/IEC27001 の管理策を用いた要件のクリアを推奨している訳ではない．あくまでも参考情報として掲載しているというのが NIST の意図である．

2.3 今後の展開

2019 年以降，FAR(連邦調達規則)が改定され，米国政府機関すべてに DFARS 252.204-7012 と同様のレギュレーションが展開される方向で進められている．また，民間では AIAG(全米自動車産業協会)が参加企業 2,518 社に対し，NIST SP800-171 に基づくサイバーセキュリティ対策ガイドラインを 2018 年に発行している [4]．このように今後 NIST SP800-171 準拠が防衛産業以外のサプライチェーンにも拡大した場合，サプライチェーンを構成する日本の中小企業にも影響が広がる．そして，もし中小企業が NIST SP800-171 に準拠できない場合，米国政府案件に関して契約できなくなる，もしくは CUI の漏洩時に訴訟によって責任を問われるだろう．

Vol.2020-DPS-182 No.1
Vol.2020-CSEC-88 No.1
2020/3/12

3. 中小企業に NIST SP800-171 準拠を求めた場合の課題

3.1 中小企業におけるセキュリティ対策の実態

独立行政法人情報処理推進機構(以下，IPA)が，2016 年に社員数 300 人以下の中小企業約 4,300 社を対象に情報セキュリティ関するアンケート調査を実施している．この調査結果に基づき，ここでは中小企業におけるセキュリティ対策の実態について概説する．

IPA の調査報告書 [5]によると，「情報セキュリティ関連の被害を防止するために実施している組織面・運用面の対策何か？」という質問に対し ，「ISMS の認証取得」と答えた中小企業(101 人以上)が 11%, 中小企業(100 人以下)が 3.4%, 小規模企業(20 人以下)が 0.6%と ISMS 認証を取得している割合は極めて少ない結果となっている．また注目すべき回答として，「特に対策を実施していない」と答えた小規模企業(20 人以下)が 42.2%あった．この調査結果から，ほとんどの中小企業は組織的にセキュリティ対策に取り組んでおらず，十分なセキュリティ対策が取られているとは言い難い．一方で ISMS 認証を取得している企業も 1 割程度存在する．これは，日本の商習慣上，機密性の高い情報を扱う案件の場合，ISMS 認証取得が契約条件になることが多いため，中小企業においてもコストをかけて対応しているものと推測する．

3.2 中小企業でセキュリティ対策が進まない理由

次に前節で取り上げた調査報告書の中から「情報セキュリティ対策に関する投資が含まれていない理由は何か？」という問いに注目した．この問いに対し，一番目に多かった回答が「費用対効果が見えない」で 20.6%，二番目に多かった回答が「どこから手をつけて始めれば良いか分からない」で 20.2%，三番目に多かった回答が「コストがかかり過ぎる」で 17.8%という結果となっている．これら 3 つの回答については，中小企業が抱える根強い課題であると捉える．そして，これらの課題を解決するような手立てがなければ，今後，中小企業が NIST SP800-171 をベースとしたグローバルスタンダードに準拠することは難しく，ビジネス上の障壁となり得る．

3.3 課題と解決方針

前節で取り上げたデータから，セキュリティ対策が進んでいない中小企業に対して NIST SP800-171 準拠を求めた場合，中小企業から「どこから手をつけて始めれば良いか分からない」という声が上がることは容易に想像できる．一方で「費用対効果が見えない」や「コストがかかり過ぎる」といった声が上がることも想像できないわけではない．しかしながら，中小企業が契約条件として NIST SP800-171 準拠を求められた場合，背に腹は代えられないため，ある程度のコストをかけてでも対応すると推測する．よって，本稿では「どこから手をつけて始めれば良いか分からない」という課題にフォーカスして解決策を提案したい．

この課題を解決するための方針として，「中小企業は，一足飛びに NIST SP800-171 準拠を目指すのではなく，実行性のある計画となるよう段階的に対応して行く」ことが望ましいと考える．そして，この方針を具現化するためのアプローチ手法について本稿で提案する．以降，その提案内容について述べる．

4. NIST SP800-171 版「優先順位付けアプローチ」の提案

4.1 解決策の検討

中小企業でも取り組めるようなアプローチ手法を考案するにあたり，まず米国防総省が DARS-2018-0023 [6]という文書の中で推奨している「DoD Value」に注目した．なぜなら，DoD Value は NIST SP800-171 の 110 個のすべての要件に対して優先度を表した 5 段階のランク付けをおこなっているからである．しかしながら，DoD Value の約 8 割は最も優先度が高いランク「5」であるため，結果的にどの要件から優先的に取り組んだらよいのかが分からない．またマイルストーンも設定されていないため，仮に中小企業が DoD Value に従って NIST SP800-171 準拠を進めたとしても，「どこから手をつけて始めれば良いか分からない」という課題は解決しない．

次に国際カードブランド大手 5 社（American Express, Discover, JCB, Mastercard, Visa）が共同し，カードデータを処理するにあたってセキュリティを確保するための要求事項を纏めた PCI DSS に注目した. なぜなら, PCI DSS は NIST SP800-171 と同様にデータ保護を目的とし，且つ実際にサプライチェーンを構成する企業全体のベースラインセキュリティとして利用されているからである（表 2）.

表 2　PCI DSS と NIST SP800-171 の比較

	PCI DSS	NIST SP800-171
発行者	民間団体（PCI SSC）	米国政府（NIST）
初版の発行日	2004年12月	2015 年6月
目的	クレジットカード会員情報の保護	CUIの保護
適用対象	メンバー機関、加盟店、サービスプロバイダ	米国政府の委託先である外国政府、企業
セキュリティ要件数	415	110
特徴	数値基準を具体的に設定。現場の声を取り入れバージョンアップしている。	パフォーマンスベースで示されているため、具現化が容易ではない。
未遵守時のペナルティ	クレジットカード利用を伴うサービス提供不可	米国政府案件の契約不可

4.1.1 優先順位付けアプローチ

カード加盟店や事業者が PCI DSS に準拠しようとした場合，「何から手を付ければよいか分からない」という疑問や業務負担，コストが要因で進まないということはよくある．このような課題に対応するため, PCI セキュリティ基準審議

Vol.2020-DPS-182 No.1
Vol.2020-CSEC-88 No.1
2020/3/12

会が「PCI DSS 準拠を達成するための優先順位付けアプローチ」[7]を開発している．このアプローチは，PCI DSS の要求事項を導入した場合のリスク低減効果の大きさを根拠に 415 の要件すべてに優先順位を設定している．優先順位は 6 つのマイルストーンとして示されており，マイルストーン 1 が最も優先度が高く，マイルストーン 6 が最も優先度が低い．その内容を表 3 に示す．

表 3　PCI SSC, Prioritized Approach for PCI DSS 3.2

マイルストーン	PCI DSS の目標
1	センシティブ認証データを削除し、データの保持を制限する。
2	システムとネットワークを保護し、システム違反に対応できるよう準備する。
3	ペイメントカードアプリケーションの安全を確保する。
4	システムへのアクセスを監視および管理する。
5	保存されたカード会員データを保護する。
6	残りの準拠作業を終了し、全てのコントロールが実施されていることを確認する。

優先順位付けアプローチには以下のようなメリットがある．

① リスク低減効果が高い順に要件が再整理されているため，より早い段階でリスクを排除することが可能．

② マイルストーン毎にある程度明確な目標が定められており，取り組む上で分かりやすい．

各要件に対する優先順位付けの根拠は，実際の侵害データや認定セキュリティ評価機関，フォレンジック調査機関，PCI SSC の諮問委員会からのフィードバックの情報にあるとされている．確かなデータ分析の上で考案されているが，その根拠データまでは PCI SSC より開示されていない．

PCI DSS の優先順位付けアプローチは，以下 2 つの理論に基づいて設計されている [8]．イメージを図 4 に示す．

① 最初に保持するカード情報を制限することで，漏洩リスクを大幅に低減させる．

② 段階的に多層防御を施すことで，漏洩リスクをゼロに近付ける．

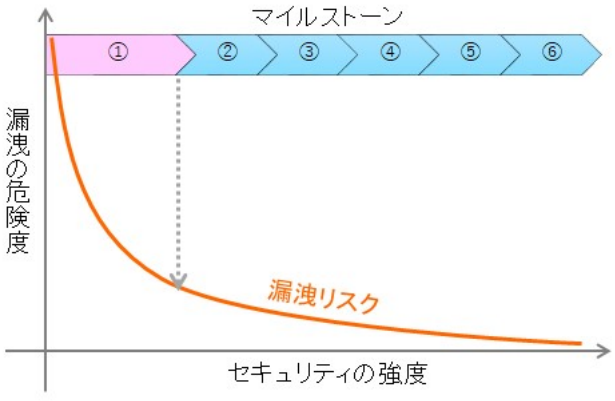

図 4　優先順位付けアプローチのリスク低減効果

4.1.2 解決策の仮説

前項で説明した PCI DSS の優先順位付けアプローチは，実際に PCI DSS 準拠を支援するコンサルティング会社が活用している．また，国際カードブランドやカード加盟店契約会社によって特定のマイルストーンまでの準拠を求めるといった使い方もされている [9]．このようなクレジットカード業界で実績のある PCI DSS の優先順位付けアプローチの理論を NIST SP800-171 にも応用すれば，「どこから手をつけて始めれば良いか分からない」という課題を解決し，さらに段階的な完全準拠と早い段階でのリスク低減を実現できると仮説を立てた．そして，その仮説を具現化するための NIST SP800-171 版優先順位付けアプローチを考案した．以降，考案したアプローチについて説明する．

4.2 NIST SP800-171 版優先順位付けアプローチ

最初に PCI DSS の優先順位付けアプローチで設定されている 6 つのマイルストーンを参考にして，NIST SP800-171 準拠用マイルストーンを作成した．その内容を表 4 に示す．

表 4　NIST SP800-171 準拠用マイルストーン（筆者作成）

マイルストーン	PCI DSS の目標	SP800-171の目標
1	センシティブ認証データを削除し、データの保持を制限する。	・情報資産の棚卸し ・保有するCUIの特定・制限 ・情報漏洩リスクの大幅な低減
2	システムとネットワークを保護し、システム違反に対応できるよう準備する。	・境界・内部・無線ネットワークの保護 ・不正侵入リスクの低減
3	ペイメントカードアプリケーションの安全を確保する。	・CUIを扱うアプリケーションの安全確保 ・ソフトの脆弱性を突かれるリスク低減
4	システムへのアクセスを監視および管理する。	・システムへのアクセスを監視 ・CUIへのアクセスを最小限に制御 ・不正操作リスクの低減
5	保存されたカード会員データを保護する。	・物理的対策・暗号化によってCUIを保護 ・情報の持ち出しリスクの低減
6	残りの準拠作業を終了し、全てのコントロールが実施されていることを確認する。	・残りの要件への対応を完了 ・リスクを限りなくゼロに近付ける。

以下に NIST SP800-171 準拠用 6 つのマイルストーンの概要について示す．

(1) マイルストーン 1

最初のマイルストーンでは，情報資産の棚卸をおこない，保有する CUI を特定し，制限する．特に漏洩しては困る CUI が，業務上の必要性が検討されないまま情報システム内に保存されているケースは少なからずあると推測する．必要なければ保存しないといった，CUI の保存に関するポリシーを定め，必要最小限の CUI 保存と確実な削除を徹底することでリスクの大幅な低減を目指す．

(2) マイルストーン 2

2 番目のマイルストーンでは，境界・内部・無線ネットワークを保護することで，外部から情報システムに不正侵入されるリスクの低減を目指す．そのためにシステムへのアクセスが可能となる境界を把握し，ファイアウォールによる通信制御，無線やリモートアクセスの制限，暗号化通信等のネットワークセキュリティ対策を実施する．また，ユーザー認証やパスワードポリシーの強化，定期的な脆弱性

診断等についても実施する．

(3) **マイルストーン 3**

3 番目のマイルストーンでは，CUI を取り扱うアプリケーションを保護することで，ソフトウェアの脆弱性を攻撃に利用されるリスクの低減を目指す．そのためにサーバの要塞化として，サーバ上で稼働する不要なサービスを停止し，OS やミドルウェアに対してセキュリティパッチを適用してセキュリティホールを塞ぐ対策を実施する．また，アプリケーションの脆弱性対策として，開発環境・テスト環境・本番環境の分離，OWASP 等のガイドラインに沿ったプログラムコーディング，不正アクセス手法に対する脆弱性の有無について診断を実施する．

(4) **マイルストーン 4**

4 番目のマイルストーンでは，CUI を保存する情報システムへのアクセスを監視し，CUI へのアクセスを最小限に制御する．それにより外部犯・内部犯による CUI の漏洩に繋がり得る不正操作リスクを低減することを目指す．そのためにシステムへのフルアクセスが可能な特権アクセスや，CUI が保存されるデータベースへのアクセス権を，業務上必要とされる正当な理由がある人に限定する（最小権限の原則）．また，アクセス権を制限するだけでなく，誰が・何に・いつ・どのような方法でアクセスしたかをログに記録し，チェックする仕組みを構築する．それにより，攻撃の早期発見と迅速な対応を実現する．

(5) **マイルストーン 5**

5 番目のマイルストーンでは，外部犯・内部犯がこれまでのマイルストーンで施したセキュリティ対策を回避し，CUI にアクセスできてしまった場合でも，その影響を最小限に留めることを目指す．保存が必要な CUI に該当するデータを洗い出し，暗号化する等の保護を実施する．また物理的なセキュリティ対策についてもこのマイルストーンで実施する．例えば，入退室管理，監視カメラ，情報コンセントの利用制限を実施する．

(6) **マイルストーン 6**

最後のマイルストーンでは，NIST SP800-171 の残りの要件に対応し，すべてのコントロールが実施されていることを確認する．それにより CUI の漏洩リスクを限りなくゼロに近付けることを目指す．具体的には，各種管理策についてポリシー・プロセスを文書化し，教育や訓練，監視，改善を行っていくことで，適切にセキュリティを維持する．

4.3 管理策のマッピング

前節の NIST SP800-171 準拠用の 6 つのマイルストーンに従い 110 すべての要件に対して 6 段階の優先順位をマッピングした表を作成した．さらに日本の中小企業が取り組み易いよう，経済産業省が発行したサイバー・フィジカル・セキュリティ対策フレームワーク（以下，CPSF）[10]の対策要件 ID と対策レベルを NIST SP800-171 の各要件にマッピングした．このマッピング表を本稿の巻末に付録する(付録 A.1). CPSF の対策レベルは, Basic, Advanced, H-Advanced の 3 段階で設定されており，対策を実施する際のコストも加味されている．中小企業が，3 段階の対策レベルのうち一番ハードルが低い対策に取り組むことで NIST SP800-171 の要件をクリアできるようにするため，推奨の対策レベルを●印で示した．例えば，Basic，Advanced，H-Advanced の 3 つの対策例があれば，Basic に●印．Advanced，H-Advanced の 2 つの対策例があれば，Advanced に●印を付けた．

4.4 期待する効果

中小企業がこの NIST SP800-171 版優先順位付けマッピング表に従って準拠作業に取り組むことで，以下のような効果がを期待する．

① NIST SP800-171 準拠のロードマップ作成が可能となる．
② CUI の漏洩リスクを早期に低減することが可能となる．
③ 準拠のためのコストや要員の計画作成が可能となる．
④ 準拠作業の進捗とリスク低減の可視化が可能となる．

これらの効果によって，「どこから手をつけて始めれば良いか分からない」といった課題を解決できるものと仮定する．以降，この仮定の検証について述べる．

5. NIST SP800-171 版優先順位付けアプローチの検証

5.1 検証の方針

本研究では，NIST SP800-171 版優先順位付けアプローチの妥当性について検証をおこなった．妥当性とは，「段階的に完全準拠を目指しながら，早い段階でのリスク排除が可能」と定義した．さらにコスト・難易度が低いものから順番に取り組めるようになっているか，各マイルストーンを無理なく達成できるようになっているか，といった観点で検証をおこなった．次節より 2 つの検証について順を追って説明する．

5.2 検証①: PCI DSS の要件と NIST SP800-171 の要件を比較評価

5.2.1 検証方法

検証①では，「段階的に完全準拠を目指しながら，早い段階でのリスク排除が可能か」を検証するために，PCI DSS の要件と NIST SP800-171 の要件を比較した．比較の基準として NIST Cyber Security Framework v1.1（以下，NIST CSF）[11]を採用した．理由は，①NIST CSF は広く企業に適用できるように要件を汎用化されており，②サイバー攻撃対策として企業が持つべき 5 つの機能「特定・防御・検知・対応・復旧」を基準に評価できるからである．

まず NIST CSF の 107 つのサブカテゴリーに対して，PCI DSS の要件と NIST SP800-171 の要件をそれぞれマッピングした．次にサブカテゴリー毎に PCI DSS の要件と NIST SP800-171 の要件の一致度を評価した. 評価基準は, PCI DSS と NIST SP800-171 の両方において要件がある場合には「○」

とし，PCI DSS の要件はあるが，NIST SP800-171 の要件がない場合には「×」，それ以外の組み合わせについては「－」とした．比較評価の例を表 5 に示す．この方法で 23 個のカテゴリー毎に比較評価をおこなった．

表 5　PCI DSS と NIST SP800-171 の要件を比較評価した例

CSF v1.1			PCI DSS v3.2.1	NIST SP800-171 r1	評価
機能	カテゴリー	サブカテゴリー			
特定（ID）	資産管理（ID.AM）	ID.AM-1	2.4, 9.9, 11.1.1, 12.3.3	3.4.1, 3.4.2	○
		ID.AM-2	2.4, 12.3.7	3.4.1, 3.4.2	○
		ID.AM-3	1.1.2, 1.1.3	3.1.3, 3.13.1	○
		ID.AM-4	1.1.1, 1.1.2, 1.1.3, 2.4	3.1.20, 3.1.21	○
		ID.AM-5	9.6.1, 12.2	N/A	×
		ID.AM-6	12.4, 12.5, 12.8, 12.9	N/A	×

5.2.2 検証結果と考察

前項で説明した比較評価の結果を基に PCI DSS の要件に対する NIST SP800-171 要件のカバー率を算出し，表 6 のとおり纏めた．

表 6　PCI DSS に対する NIST SP800-171 のカバー率

CSF v1.1		PCI DSS v3.2.1に対する NIST SP800-171 r1のカバー率
機能	カテゴリー	
特定（ID）	資産管理（ID.AM）	83%
	ビジネス環境（ID.BE）	－
	ガバナンス（ID.GV）	75%
	リスクアセスメント（ID.RA）	100%
	リスクアセスメント管理戦略（ID.RM）	100%
	サプライチェーンリスクマネジメント（ID.SC）	0%
防御（PR）	アクセス制御（PR.AC）	100%
	意識向上およびトレーニング（PR.AT）	100%
	データセキュリティ（PR.DS）	86%
	情報を保護するためのプロセスおよび手順（PR.IP）	100%
	保守（PR.MA）	100%
	保護技術（PR.PT）	100%
検知（DE）	異常とイベント（DE.AE）	100%
	セキュリティの継続的なモニタリング(DE.CM)	100%
	検知プロセス(DE.DP)	100%
対応（RS）	対応計画の作成(DE.RP)	100%
	コミュニケーション(RS.CO)	100%
	分析(RS.AN)	100%
	低減(RS.MI)	100%
	改善(RS.IM)	100%
復旧（RC）	復旧計画の作成(RC.RP)	100%
	改善(RC.IM)	100%
	コミュニケーション(RC.CO)	－

表 6 にあるとおり 23 個中 2 個のカテゴリーにおいて PCI DSS の要件と NIST SP800-171 の要件の両方が存在しない．この 2 個のカテゴリー「ビジネス環境」と「コミュニケーション」については，評価の対象外とする．残り 21 個のカテゴリーのうち 17 個において PCI DSS と NIST SP800-171 の両方の要件が存在した．その場合，PCI DSS の要件に対する NIST SP800-171 の要件のカバー率は 100%となる．一方で PCI DSS の要件は存在するが，NIST SP800-171 の要件でカバーしていないカテゴリーが 4 個（サブカテゴリーのレベルで 8 個）あることが明らかになった．これらを抽出し，纏めたものを表 7 に示す．

表 7　NIST SP800-171 でカバーしていない項目

NIST CSF v1.1		
機能	カテゴリー	サブカテゴリー
特定（ID）	資産管理（ID.AM）	**ID.AM-6:** 全労働力と利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。
	ガバナンス（ID.GV）	**ID.GV-2:** サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。
	サプライチェーンリスクマネジメント（ID.SC）	**ID.SC-1:** サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。
		ID.SC-2: 情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。
		ID.SC-3: サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。
		ID.SC-4: サプライヤーおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。
		ID.SC-5: 対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダーと共に行なわれている。
防御（PR）	データセキュリティ（PR.DS）	**PR.DS-6:** 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。

まず「特定」機能において NIST SP800-171 の要件が不足しているサブカテゴリーが 7 個あった．そのうち資産管理の「ID.AM-6」，サプライチェーンマネジメントの「ID.SC-1～ID.SC-5」については，サプライチェーンに関する項目である．もともと NIST SP800-171 は，米国政府機関から見た直接の委託先企業における CUI 保護に的を絞り，そのための必要最小限の要件に絞られている．そのため，さらに要求レベルが上がるサプライチェーンに関する要件については，あえて含められていないと推測する．またガバナンスの「ID.GV-2」についても同様の理由から，NIST SP800-171 の要件には含められていないと考えられる．

最後に NIST SP800-171 に不足している項目として「防御」機能のデータセキュリティ「PR.DS-6」が上がっている．この項目の具体的な管理策は，ファイルの変更監視ツールによる完全性のチェックになる．そのため，機密性の担保に特化している NIST SP800-171 としては，完全性についてこのレベルまでの対策を要求していないと推測する．

これらの結果から総合的に判断すると，SP800-171 版優先順位付けアプローチを採用することで，PCI DSS 版と同様に

段階的な完全準拠と，早い段階でのリスク排除を期待できる．よって，妥当性のあるアプローチ手法と言える．

5.3 検証②：NIST SP800-171 準拠に必要な対策を CPSF に基づき整理･分析

5.3.1 検証方法

検証②では，「コスト・難易度が低いものから順番に取り組めるようになっているか，各マイルストーンを無理なく達成できるようになっているか」を検証するために NIST SP800-171 準拠に必要な管理策を CPSF に基づき整理・分析した．その過程の一部を表 8 に示す．

表 8　NIST SP800-171 準拠に必要な管理策を CPSF の対策要件別に整理した表（一部掲載）

NIST SP800-171 版マイルストーン	サイバー・フィジカル・セキュリティ対策　フレームワーク								
	AC-1	AC-2	AC-3	AC-4	AC-5	AC-6	AC-7	AC-8	AC-9
マイルストーン1							3.1.3		
							3.13.5		
マイルストーン2		3.8.1	3.1.16			3.5.3	3.13.7	3.5.1	3.1.18
		3.10.1	3.1.18			3.5.4		3.8.2	3.8.2
		3.10.3	3.1.12					3.13.6	
		3.10.2	3.1.13						
		3.10.4	3.1.15						
		3.10.5	3.1.17						
			3.10.6						
			3.13.12						
			3.13.15						
マイルストーン3									

5.3.2 検証結果と考察

「SP800-171 準拠に必要な管理策を CPSF の対策要件別に整理した表」を使って分析した結果，コスト・難易度が低いものから順番に取り組めることを確認できた．しかしながら，難易度が高い管理策がマイルストーン 2 に集中した．マイルストーン 2 を達成するためには必要な管理策ではあるが，一方で中小企業が早い段階で難易度が高い管理策に取り組んだ場合，心理的負担がかかることを予想できる．この点については，今後の課題として検討する必要がある．

6. まとめ

米国政府機関が，グローバルサプライチェーンを構成する日本の中小企業に対して NIST SP800-171 準拠を求めた場合，「どこから手をつけて始めれば良いか分からない」といった課題が生じると提起した．この課題を解決するために「NIST SP800-171 版優先順位付けアプローチ」を提案し，日本の中小企業が取り組み易いよう CPSF の対策例を紐づけた上で優先順位付けマッピング表を作成した．そして，検証をおこなうことで，NIST SP800-171 版優先順位付けアプローチを採用した場合に，段階的な完全準拠と，早い段階でのリスク排除が可能であることを明らかにした．

昨今”セキュリティ対策は，コストではなく投資として取り組むべき”と言われているが，商売が最優先であり，且つ IT やセキュリティ人材がいない中小企業にとっては，”言うは易く行うは難し”であろう．しかしながら，本稿で取り上げた NIST SP800-171 については，日本で馴染みのある ISMS やプライバシーマークと一線を画すものである．なぜなら，今後 NISTSP800-171 は米国政府案件の契約条件となり得るからである．もし今後，日本の中小企業が NIST SP800-171 に準拠できなかった場合，既存契約については解消し，新規契約については締結できない可能性が高い．それは，日本の中小企業がグローバルサプライチェーンから弾き出されることを意味する．このような問題を回避するために，今後，官民問わず，NIST SP800-171 準拠による負担軽減のための施策につい検討すべきである．

参考文献

[1] The Wall Street Journal, http://jp.wsj.com/articles/SB10922266312659313634204583449643578613634, 2017 年 10 月 13 日
[2] National Institute of Standards and Technology, Special Publication 800-171 Rev1, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171r1.pdf
[3] Department of Defense, Departmentof Defense FAR Supplement 252.204-7012, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
[4] GLOBENEWSWIRE.COM, https://www.globenewswire.com/news-release/2018/05/02/1495137/0/en/Automotive-Industry-Collaborates-on-New-Cybersecurity-Guidelines.html, 2018 年 5 月 2 日
[5] 独立行政法人情報処理推進機構, 2016 年度中小企業における情報セキュリティ対策に関する実態調査 -調査報告書-, 2017 年 3 月 30 日
[6] Department of Defense, DARS-2018-0023-0002, https://www.regulations.gov/contentStreamer?documentId=DARS-2018-0023-0005&contentType=pdf
[7] PCI Security Standards Council，Prioritized Approach for PCI DSS 3.2, https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf
[8] 国の実行計画と PCI DSS は整合しているのか, https://www.nos.co.jp/solution/category/PCI/pcidss/pci-exp/PCI-DSS-seigo.html
[9] 瀬田陽介,井原亮二, 改正割賦販売法でカード決済はこう変わる, 2018 年 4 月 16 日
[10] 経済産業省, サイバー・フィジカル・セキュリティ対策フレームワーク Ver1.0, https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf
[11] National Institute of Standards and Technology, Cybersecurity Framework Version 1.1, https://doi.org/10.6028/NIST.CSWP.04162018

付録

付録 A.1　NIST SP800-171 版優先順位付マッピング表（一部掲載）

NIST SP800-171 r1		マイルストーン						CPSF 対策例・レベル			
No.	要件	1	2	3	4	5	6	対策要件 ID	Basic	Advanced	H-Advanced
3.1 アクセス制御											
3.1.1	システムへのアクセスは、権限のあるユーザー、あるいは権限のあるユーザーの代理として動作するプロセスまたは（その他のシステムを含む）装置に限定する。				4			CPS.AC-9	―	●	○
3.1.2	システムへのアクセスは、権限のあるユーザーが実行を許可されている各種のトランザクションおよび機能に限定する。				4			CPS.AC-9	―	●	○
3.1.3	承認された権限に従って、CUI の一連の取扱い手続き（flow）を管理する。	1						CPS.AC-7	●	―	○
				3				CPS.AE-1	―	―	●
3.1.4	共謀のない有害行動のリスクを減らすため、個人の職務を分離する。				4			CPS.AC-5	―	●	○
3.1.5	特定のセキュリティ機能および特権アカウントを含め、最小特権の原則を採用する。				4			CPS.AC-5	―	●	○
3.1.6	非セキュリティ機能にアクセスする時には、非特権アカウントまたは役割を使用する。				4			CPS.AC-5	―	―	●
3.1.7	非特権ユーザーが特権機能を実行することを防止し、そうした機能の実行を監査する。				4			CPS.AC-5	―	―	●
3.1.8	ログオン試行失敗回数を限定する。				4			CPS.AC-4	―	●	○
3.1.9	適用されるCUI 規則に則って、プライバシーおよびセキュリティ通知する。				4			CPS.AC-9	―	●	○
3.1.10	非アクティブな時間経過後のデータのアクセスおよび閲覧を防止するために、隠蔽用パターンの表示によるセションロックを使用する。				4			CPS.AC-9	―	●	○
3.1.11	規定された条件が成立した場合には、ユーザーセションを（自動的に）終結させる。				4			CPS.AC-9	―	―	●
3.1.12	リモートアクセスセションを監視し、管理する。		2					CPS.AC-3	―	―	●
								CPS.CM-1	●	○	―
					4			CPS.CM-5	―	●	○
3.1.13	リモートアクセスセションの機密性を保護するために暗号メカニズムを採用する。		2					CPS.AC-3	―	―	●
								CPS.DS-3	―	●	―
3.1.14	管理されたアクセス制御ポイント経由でリモートアクセスをルーティングする。		2					CPS.CM-1	―	●	○
3.1.15	特権コマンドのリモート実行およびセキュリティ関連情報へのリモートアクセスに権限を付与する。		2					CPS.AC-3	―	―	●
3.1.16	接続を許可する前に、ワイヤレスアクセスに権限を付与する。		2					CPS.AC-3	●	○	○
3.1.17	認証および暗号を使用してワイヤレスアクセスを保護する。		2					CPS.AC-3	―	―	●
3.1.18	モバイル装置の接続を管理する。		2					CPS.AC-3	―	●	○
								CPS.AC-9	―	●	○
3.1.19	モバイル装置およびモバイルコンピューティングプラットフォーム上のCUIを暗号化する。					5		CPS.DS-2	―	●	○
3.1.20	外部システムへの接続および使用を検証（verify）し、管理/制限する。		2					CPS.AM-5	―	●	○
3.1.21	外部システム上での組織の可搬型記憶装置の使用を制限する。		2					CPS.AM-5	―	●	―
3.1.22	公衆アクセス可能なシステム上に掲載または処理されたCUI を管理する。					5		CPS.GV-3	●	―	―
3.2 意識向上と訓練											
3.2.1	組織のシステムの管理者、システムアドミニストレーターおよびユーザーが、組織のシステムのセキュリティに関連する適用ポリシー、規格および手続きならびに彼らの活動に関連するセキュリティリスクについて認識していることを確実にする。						6	CPS.AT-1	―	●	○
								CPS.AT-2	●	○	―
3.2.2	組織の要員が、割り当てられた情報セキュリティ関連の職務と責任を遂行するように適切に訓練されていることを確実にする。						6	CPS.AT-1	―	●	―
								CPS.AT-2	―	●	―
3.2.3	インサイダーによる脅威の潜在的兆候を認識し、報告するためのセキュリティ意識向上訓練を行う。						6	CPS.AT-1	―	―	●