資料3-5

サプライチェーンリスクに係る国内他分野の動向

事務局参考資料（案）

Agenda/Contents

１．「関係省庁申合せ」への反応（例）

２．防衛装備庁による新たな調達基準

３．金融セクターにおけるサードパーティのサイバーリスクマネジメントに関するG7の基礎的要素

1．「関係省庁申合せ」への反応（例）

- 民間企業に対して特定の国や企業の通信機器等の調達を制限するものではないものの、携帯各社は５G投資において、特定の国の製品の採用を見送る方針を打ち出しました。

背景

未来投資戦略 2018 ―「Society 5.0」「データ駆動型社会」への変革―（平成 30 年６月 15 日）*1

「大容量・高速通信を支える 5G について、本年度末に周波数割当を行い、民間事業者による基盤整備を促進し、2020 年からのサービス開始につなげる。」

⇒携帯各社は５G通信網への投資を今春より本格化し、年内に試験提供、2020年の本格商用化を目指す。

参考：IoT時代のICT基盤となる５Gの特徴*2
- ・超高速：2時間の映画を3秒でダウンロード
- ・超低遅延：タイムラグを意識することなく遠隔操作
- ・多数同時接続：自宅部屋内の約１００個の端末・センサーがネットに接続

携帯各社の反応（例）

企業名	反応
A社	・５G投資ではある企業の製品を採用しない方針。
B社	・４G同様、５G設備もあり企業の製品採用を見送る方針。
C社	・現行設備等への対応は総合的に判断する。

出典： *1 https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf
*2 http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd133420.html

2．防衛装備庁による新たな調達基準

- 防衛装備庁は、防衛調達の新情報セキュリティ基準を、米国の基準NIST SP 800-171と同程度まで強化する方針を明らかにしました。

概要

・米国を始めとする諸外国からの保全信頼性等を目的に、防衛産業のサイバーセキュリティ強化の一環として、**防衛調達の新情報セキュリティ基準をNIST SP 800-171と同程度まで強化する**考えを表明しました。

参考：米国の動向

・**CUI（Controlled Unclassified Information：保護対象となる非秘密情報）について**は、2010年11月の大統領令（E.O.13556）発出以降、米政府全体として、**セキュリティ強化**の取組みを実施。

・特に国防省との契約を通じて**CUIを取り扱う防衛関連企業については、**国防省は、2016年10月、DFARS（国防調達規則）252.204-7012を発出し、**2017年12月末までにNIST SP 800-171相当の情報セキュリティ対応を要求**した。

検討課題

1	**コスト面の課題** 我が国の防衛産業が、新基準に対しより安価に対応するための方策が必要である。
2	**国内クラウドサービスの利用追及に当たっての課題** 現状では、米国のNIST SP 800-171を満たすクラウドサービス事業者が我が国に存在しない。今後、防衛関連企業へのクラウドサービスの提供を図る国内事業者は、新基準を満たす必要がある。
3	**中小企業に対するケア** 新基準への準拠は、プライム企業のみならず下請けとなる中小企業も対象となることを踏まえた対策が必要になるため、適合支援体制構築の検討を行う。

出典： https://www.techdevicetv.com/pdf/hp_180914security_atla.pdf

3．金融セクターにおけるサードパーティのサイバーリスクマネジメントに関するG7の基礎的要素

- 個々の金融機関におけるサードパーティのリスクマネジメントに関するライフサイクル、およびシステム全体のサイバーリスクのモニタリングに係る基礎的要素が策定されました。
- 各基礎的要素は”non-binding”であり、既存のフレームワークを無効化したり、そうしたフレームワークの継続的な適応を妨げるものではありません。

背景等

・背景：サイバーリスクへの対応の一助として、これまで次の基礎的要素を策定してきた。

- 「金融セクターのサイバーセキュリティに関するG7の基礎的要素（2016年10月）」
- 「金融セクターのサイバーセキュリティの効果的な評価に関するG7の基礎的要素（201710月）」

・目的：金融セクターにおけるサードパーティのサイバーリスクマネジメントへの取組みをさらに支援するため。

・想定する活用例：金融機関およびサードパーティ

- 自身のサイバーリスクマネジメントのツールキットの一部として活用。

基礎的要素とその概要

1	**ガバナンス** ・金融機関のガバナンス組織は、サードパーティのサイバーリスクマネジメントの効果的な監視および実行に関する責任を有すること。
2	**サードパーティのサイバーリスクに対するリスクマネジメントプロセス** ・金融機関は、サードパーティのリスクマネジメントのライフサイクル全体を通じ、サードパーティのサイバーリスクを管理する有効なプロセスを有すること。
3	**インシデント対応** ・金融機関は重要なサードパーティを含むインシデント対応計画を策定し、演習を実施すること。
4	**コンティンジェンシープラン** ・金融機関は、サードパーティがサイバー関連のパフォーマンスの期待要件を満たさない場合もしくは金融機関が許容できるリスクを超えてサイバーリスクを発生させた場合に備えて、適切なコンティンジェンシープランを用意しておくこと。
5	**潜在的なシステミックリスクのモニタリング** ・金融セクターを取り巻くサードパーティとの取引がモニタリングされ、潜在的にシステミックなインプリケーションを有するサードパーティのサイバーリスクの要因が評価されていること。
6	**セクターを跨る協調** ・セクターを跨るサードパーティへの依存に関連したサイバーリスクは、それらのセクター間で特定のうえ、管理されていること。

出典： https://www.fsa.go.jp/inter/etc/20181015/20181015.html