経済産業省

資料4

『第３層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性

令和元年7月31日

経済産業省　商務情報政策局

サイバーセキュリティ課

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

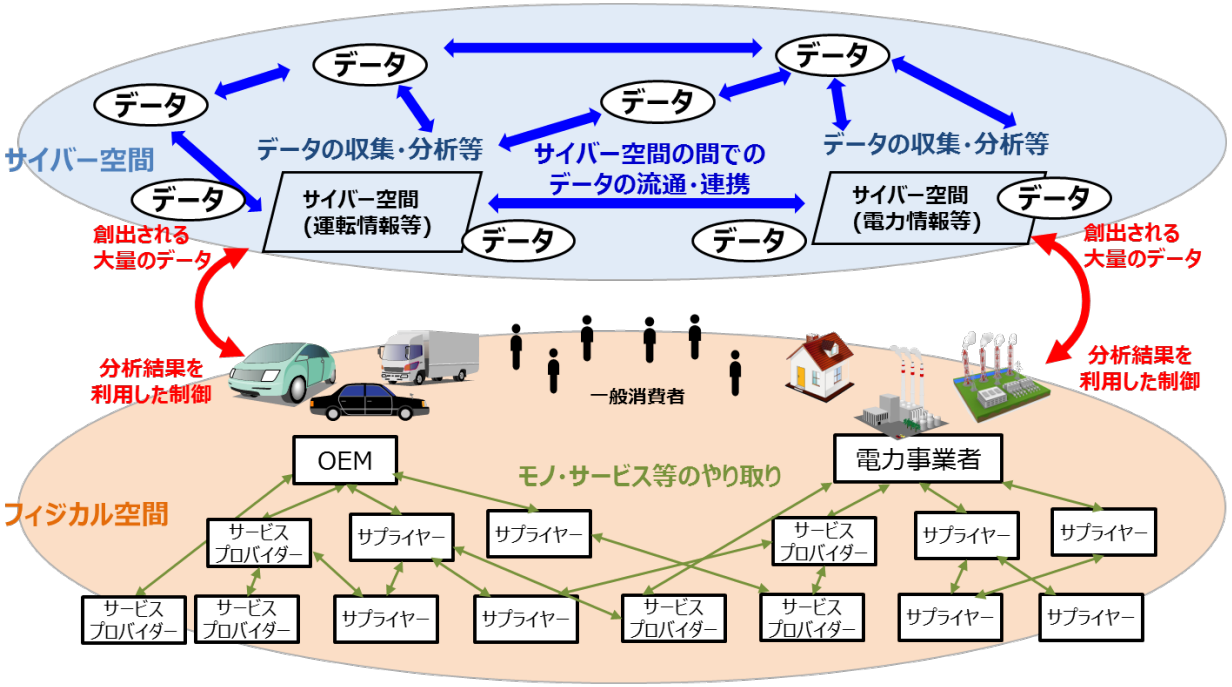
２．サイバー空間のつながりに関わるセキュリティインシデント事例

３．データを守るためのセキュリティ対策に関係する取組
（１）海外の取組事例
（２）国内の取組事例

４．本タスクフォースの検討事項

＜サプライチェーン構造の変化＞
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の策定

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**。
- 経済産業省では、「Society5.0」における**セキュリティ対策の全体像を整理**し、産業界が自らの対策に活用できる**セキュリティ対策例をまとめた、『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）』を平成31年4月に策定。**



Society5.0の社会におけるモノ・データ等のつながりのイメージ

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

＜三層構造と６つの構成要素＞
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造と６つの構成要素**）を提示。

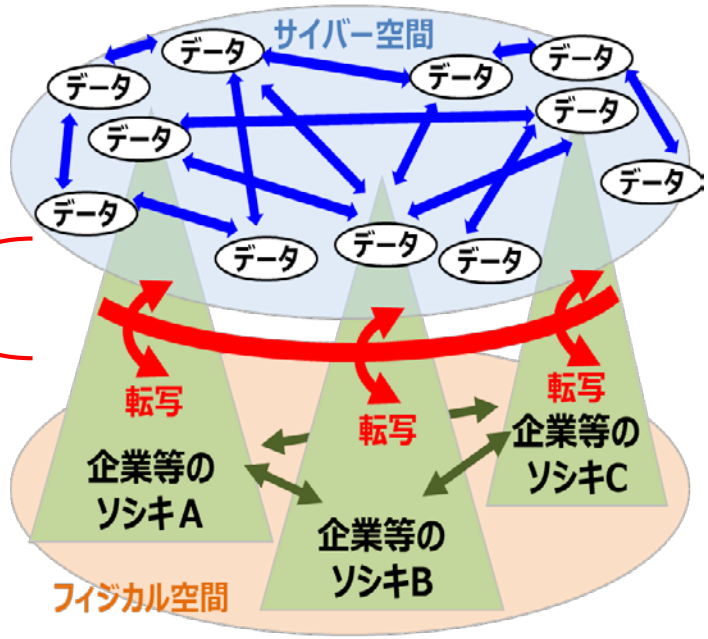
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



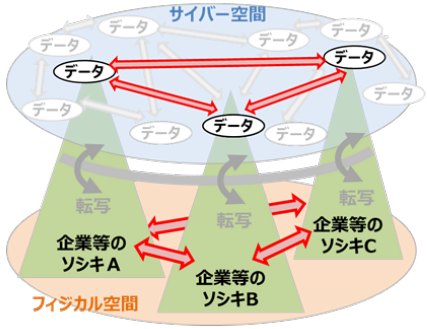
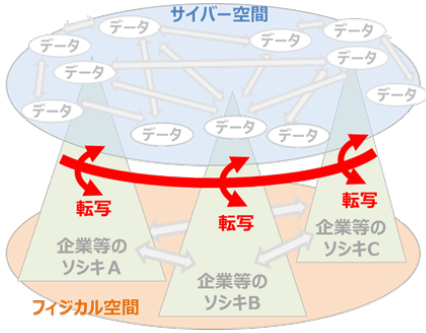
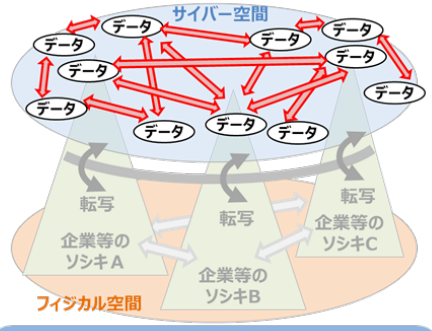
6つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を6つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	• ハードウェア、ソフトウェア及びそれらの部品 操作する機器を含む
データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	• 定義された目的を達成するための一連の活動の手続き
システム	• 目的を実現するためにモノで構成される仕組み・インフラ

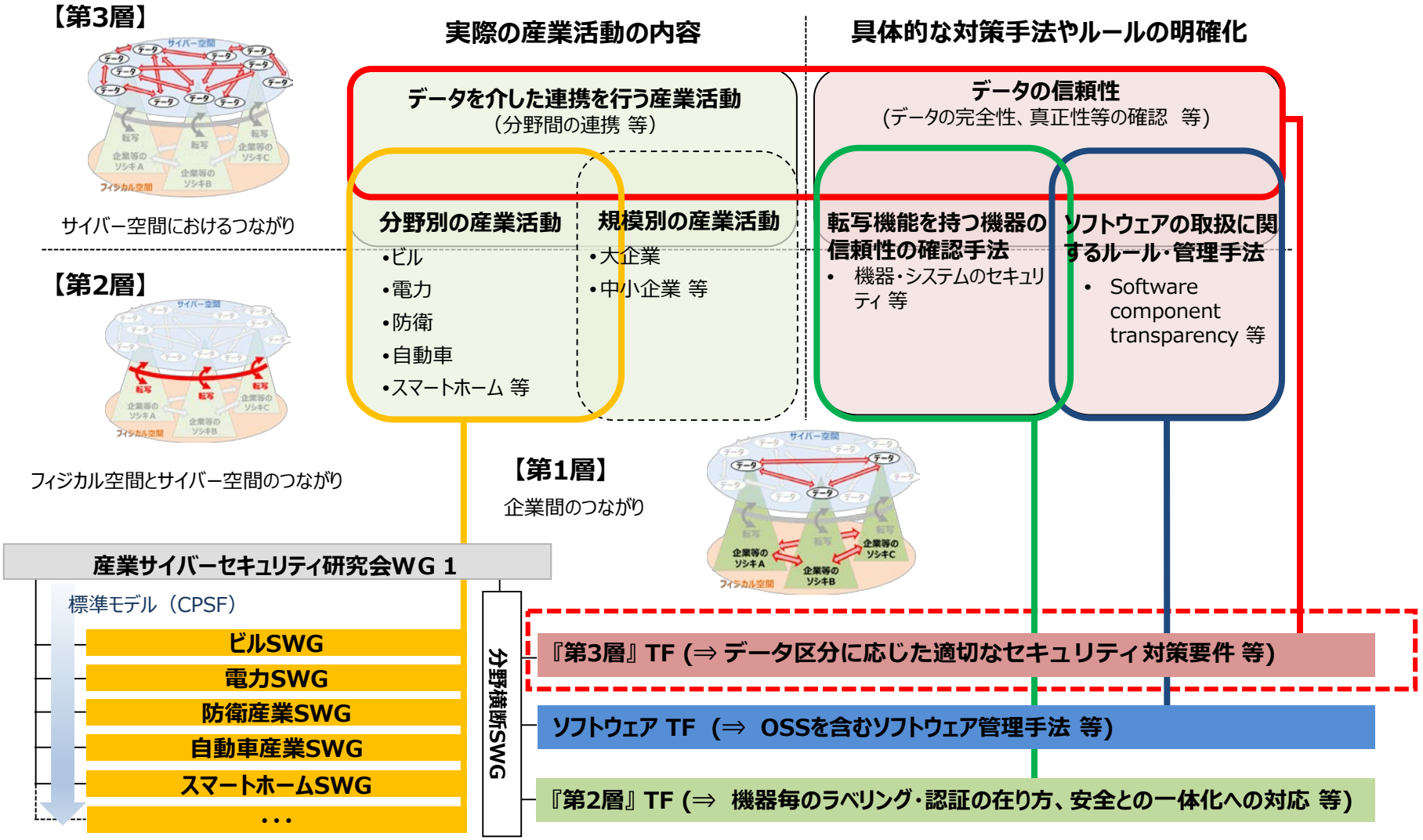
＜CPSFの全体概要＞
三層構造モデルに基づきリスク源、対応方針等を提示

- サプライチェーンの信頼性を確保する観点から、産業社会を３つの層から捉え、それぞれにおいて**守るべきもの、直面するリスク源、対応方針**等を整理。

	企業間のつながり【第１層】	**フィジカル空間とサイバー空間のつながり【第２層】**	**サイバー空間におけるつながり【第３層】**
新たなサプライチェーン構造の整理			
機能（守るべきもの）	• 平時及び緊急時のリスク管理・対応体制の構築と運用 • 企業内及び企業間のリスク管理・対応体制の構築と運用	• フィジカル空間とサイバー空間の境界における情報の正確な転写及び正確な転写の証明	• データの加工・分析 • データの保管 • データの送受信
セキュリティインシデント	• 保護すべき資産の棄損 • 他組織のセキュリティ事象発生に起因する事業停止	• 不正確なデータの送信 • 安全に支障をきたす動作	• 保護すべきデータの漏えい • なりすまし等による不正な組織からのデータ受信
リスク源（構成要素ごとに整理）	• セキュリティリスクに対するガバナンスの欠如 • 他組織との連携状況の未把握	• 不正なIoT機器との接続 • 許容範囲外の入力データ	• 通信経路が保護されていない • 通信相手を識別していない
対策要件	■ マネジメントルールの徹底 ■ 関係者との役割分担	■ 接続相手の認証 ■ 安全なIoT機器の導入	■ 暗号化によるデータ保護 ■ データの提供者の信頼性確認

CPSFに基づくセキュリティ対策の具体化・実装の推進

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置。**



１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

２．サイバー空間のつながりに関わるセキュリティインシデント事例

３．データを守るためのセキュリティ対策に関係する取組
（１）海外の取組事例
（２）国内の取組事例

４．本タスクフォースの検討事項

ランサムウェア"WannaCry"の猛威

- 平成29年５月、世界の少なくとも約150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
- **感染した欧州企業から、サプライチェーン経由で国内企業も感染。**

クラウドサービスにおけるサイバー攻撃の発生

- 世界のクラウドサービス市場規模は931億ドル※1。クラウドサービスを利用している国内企業の割合も56.9%（2017年）と、前年（2016年）の46.9%から大幅に上昇※2。
- その一方で、**クラウドサービスへのサイバー攻撃**（主に不正アクセスによる情報漏えい）**事案は絶えず発生**している状況。

※1　2015年。出典：Cisco VNI: Forecast and Methodology, 2014-2019.
※2　2017年。出典：平成30年度版　情報通信白書

利用者の多いクラウドサービスにおけるサイバー攻撃の特徴

「Office365」への不正アクセス

- 攻撃者は、**2要素認証が導入されていなかったり**、**単純なパスワードが設定**されていたりするアカウントを標的としている。
- 特に**システムアカウント**については、事業者内で共有する必要があることから**単純なパスワードが設定されがち**であり、**使用頻度の低いものが放置されていることも多い**ため攻撃に気づきにくいという傾向がある。

Amazon Web Service（AWS）のクラウドストレージ「Amazon S3」への不正アクセス

- **ディレクトリの設定を「公開状態」**にしていたり、**パスワードが設定されていなかったり**といった、**利用者側のAWS設定ミスが**多くの原因。

→ **基本的なセキュリティ設定の確認が重要**

クラウドサービスにおける主なサイバー攻撃事例

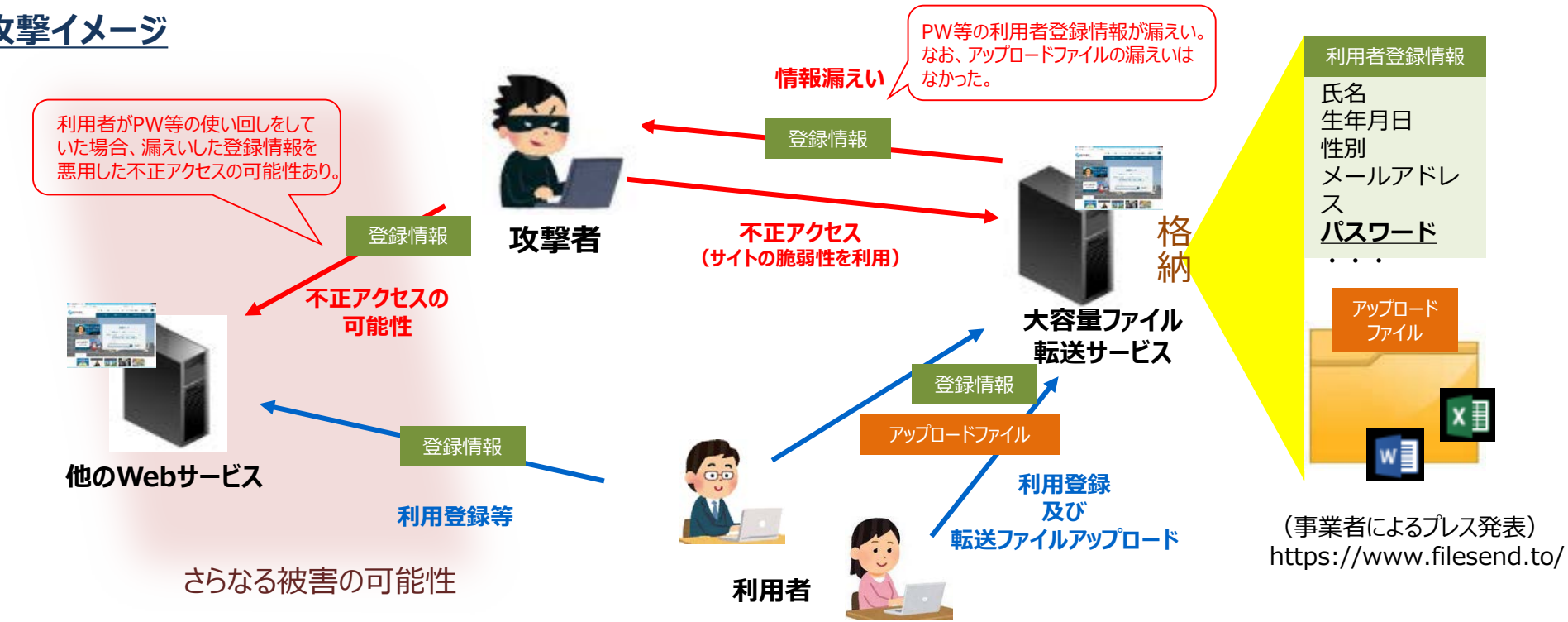
- 米国配車サービス大手のウーバー・テクノロジーズにおいて、2017年11月、顧客とドライバー合わせて**5,700万人の個人情報が流出**したことが判明。**原因はAWSへの不正アクセス**。
- A社のインド子会社において、2018年5月、**5万人以上の顧客情報が流出**したことを発表。**原因はAWSの公開設定ミス**。

大容量ファイル転送サービスにおける不正アクセス（情報漏えい）事案

- 2019年1月22日、大手クラウドサービス事業者による大容量ファイル転送サービスにおいて、一部サーバに対する**不正アクセス**が発生。**481万5,399件の顧客情報※の漏えい**を確認。
- 翌1月23日より、被害状況調査及びさらなる被害防止のため、サービスを停止。**本サービスは当面休止**することとしている。
- **<u>ログインパスワードが平文のまま保存</u>**されており、なりすましによる２次被害の可能性も考えられる。

※ 漏えいした顧客情報は、「ログイン用メールアドレス」、「ログインパスワード」、「生年月日」、「性別」、「職業・業種・職種」、「居住地の都道府県名」、「メールアドレス」等、本サービスを利用するにあたっての利用者登録情報。なお、<u>本サービスで送受信されたファイルについては、漏洩がなかった</u>ことを確認。

攻撃イメージ



（事業者によるプレス発表）
https://www.filesend.to/

ASUS社端末におけるアップデート機能を悪用した攻撃

- 台湾のIT機器大手ASUS社※1において、正規のアップデートサーバが攻撃を受け、当該サーバから**端末向けに配布されたアップデートファイルを介し、数十万の同社端末がマルウェアに感染**する事案が発生。（出典：MOTHERBOAR誌にてKim Zetter氏執筆。さらにKaspersky社が本件の簡易レポート発出。）

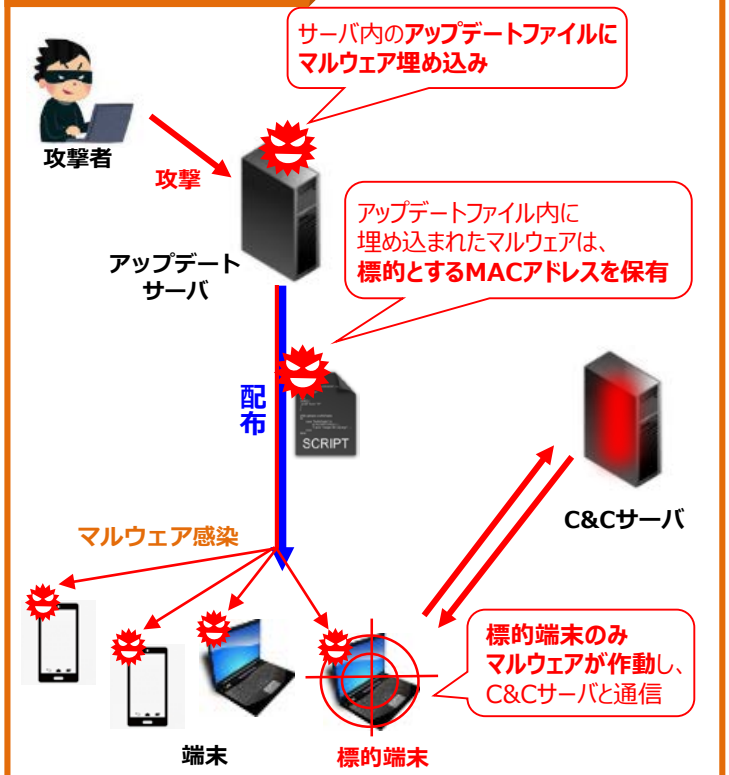
- 正規のダウンロード経路を悪用した同様の攻撃は、2017年に「CCleaner※2」においても発生しており、**マルウェア感染経路の一つ**として警戒を要する。

※1 ASUS社：台北市に本社を置く大手PC、スマートフォン、周辺機器製造メーカー。ソニー、アップル、HP、EPSON等への部品供給も行う。
※2 CCleaner：ハードディスク内部の不要なファイルやレジストリを削除するためのツール。イギリスの Piriform Ltd. が開発。

本事案の詳細（原因・影響等）

- 本攻撃は**2018年6月から11月**にかけて発生。「Shadow Hammer」と呼ばれる。
- 「ASUS Live Update Utility（アップデートサーバ）」による**ソフトウェアアップデートを経由**し、**マルウェア（バックドアファイル）**が**数十万のASUS端末**に感染。　※Kaspersky社は数百万に上る可能性も指摘
- 本攻撃の大きな特徴として、**マルウェアは標的とする端末のMACアドレスをあらかじめ保有**しており、**感染端末のMACアドレスを参照し、それが標的端末であるかを識別**していた。
  ※Kaspersky社は、200の検体サンプルから600の標的MACアドレスを確認している由
- 識別の結果、**マルウェア感染端末が標的端末であった場合、C&Cサーバと通信を開始する攻撃手法**。実際に標的端末が感染。
  - ✓ 標的端末以外ではマルウェアを作動させないことで、事案の発覚を遅らせる狙いがあるとみられる。
  - ✓ 攻撃者はMACアドレスにより、生産ロット等から標的とする特定の出荷先を絞り込んだものと推測される。

事案のイメージ



１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

２．サイバー空間のつながりに関わるセキュリティインシデント事例

３．データを守るためのセキュリティ対策に関係する取組
（１）海外の取組事例
（２）国内の取組事例

４．本タスクフォースの検討事項

データを守るためのセキュリティ対策に関係する海外の取組事例

国	名称	義務・任意	策定主体	策定（施行）年月	保護対象となるデータ	概要
米国	Special Publication 800-171	一部義務 ※1	NIST	2015/06 策定	Controlled Unclassified Information (CUI)	連邦政府外のシステム及び組織に存在している機微な連邦政府情報の保護のため、CUI（管理された非格付け情報）に対する連邦政府外の組織やシステムに求める管理策群。
	NIST Privacy Framework	任意	NIST	策定中	プライバシーデータ	プライバシーデータの保護のために策定中のフレームワーク。 2019年4月にDiscussion draftが公開。 - プライバシーリスクのより適切な識別、評価、管理及び伝達 - プライバシーを保護するための革新的なアプローチの開発 - 製品やサービスの信頼の向上
	医療保険の携行性と責任に関する法律 (HIPAA)	義務	HHS (米国保健福祉省)	1996年	保護対象医療情報 (Protected Health Information)	保護対象医療情報の電磁的な取扱いにおける標準や要件(プライバシー要件やセキュリティ要件を含む)を確立し、医療情報システムの開発を促進することで、ヘルスケアシステムの効率性と有効性を改善すること等を目的とした法律。
欧州	EU一般データ保護規則（GDPR）	義務	EU	2018/05 施行	プライバシーデータ	欧州における個人のデータを保護するための統一的な規則。
業界共通	PCI DSS (Payment Card Industry Data Security Standard)	一部義務 ※2	PCI SSC	最新版 v3.2.1 2018/05 改訂	クレジットカードの会員データ	クレジットカード会員データを保護するために策定されたクレジットカード業界のセキュリティ基準。

※1 米国国防調達に参加する者は、NIST SP800-171のセキュリティ要求事項を満たすことが要求される。

※2 カード会社、加盟店等が順守すべき基準。日本では、割賦販売法で、PCI DSS準拠が要求されている。

【米国における取組事例①】
CUIを守るためのセキュリティ対策：NIST SP800-171

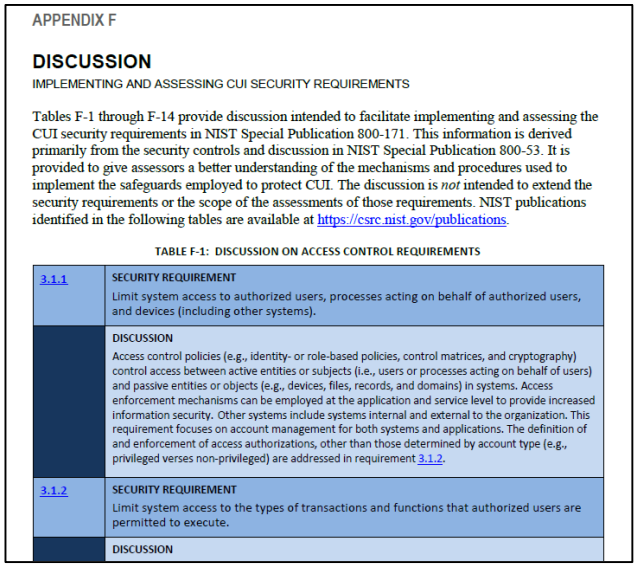
- 2015年6月、CUI*の保護を目的に14個のカテゴリと110の項目から構成されるNIST SP800-171を策定。
- これは、**米国政府がCUIを政府外の組織と共有する場合**に、当該組織がCUIを適切に保護できるようにした**セキュリティ基準**。
- NISTはSP800-171を定期的に更新しており、2018年6月7日にアップデート版を公表。

＊ Controlled Unclassified Information；管理対象となるが秘密指定されていない情報

NIST SP800-171における14個のカテゴリ

(1) アクセス制御：システムへのアクセスが出来る人／機能を制限すること
(2) 意識向上と訓練：セキュリティポリシーを遵守すること
(3) 監査と責任追跡性：システムの監査を行うとともに責任の追及が出来ること
(4) 構成管理：システムを構成する機器に求められるセキュリティ構成設定を確立すること
(5) 識別と認証：システム利用者、デバイスを識別すること
(6) インシデント対応：インシデントの追跡、報告が出来ること
(7) メンテナンス：組織のシステムのメンテナンスを行うこと
(8) 記録媒体保護：CUIをセキュアに格納するとともにアクセスできる者を制限すること
(9) 人的セキュリティ：システムへのアクセスを行う個人を審査すること
(10) 物理的保護：組織のシステム、装置等への物理的アクセスを制限すること
(11) リスクアセスメント：情報資産のリスクを適切に評価すること
(12) セキュリティアセスメント：セキュリティ管理策を定期的に評価すること
(13) システムと通信の保護：システムの鍵となる通信を監視し、制御し、保護すること
(14) システムと情報の完全性：タイムリーに情報及びシステムフローを識別すること

2018年6月アップデート版



APPENDIX F

DISCUSSION

IMPLEMENTING AND ASSESSING CUI SECURITY REQUIREMENTS

Tables F-1 through F-14 provide discussion intended to facilitate implementing and assessing the CUI security requirements in NIST Special Publication 800-171. This information is derived primarily from the security controls and discussion in NIST Special Publication 800-53. It is provided to give assessors a better understanding of the mechanisms and procedures used to implement the safeguards employed to protect CUI. The discussion is *not* intended to extend the security requirements or the scope of the assessments of those requirements. NIST publications identified in the following tables are available at https://csrc.nist.gov/publications.

TABLE F-1: DISCUSSION ON ACCESS CONTROL REQUIREMENTS

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	DISCUSSION Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for both systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.
3.1.2	**SECURITY REQUIREMENT** Limit system access to the types of transactions and functions that authorized users are permitted to execute.
	DISCUSSION

セキュリティ要件を満たすために必要な具体的な事項を記載した「APPENDIX F：DISCUSSION」が追加。

【米国における取組事例②-1】

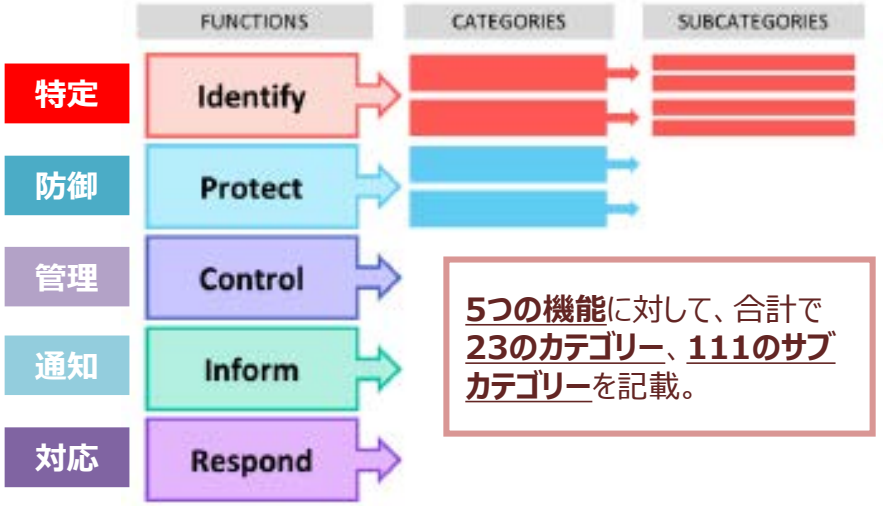
プライバシーデータを守るためのセキュリティ対策：NISTプライバシーフレームワーク

- NISTは、プライバシー保護のための共通フレームワークにすることを目指して**プライバシーフレームワークを策定中**。
- 現在、ディスカッションドラフト（2019年4月）を公表。2019年10月策定予定。
- 全体の枠組みは**NISTサイバーセキュリティフレームワーク(CSF)を踏襲**しているが、個々の機能やカテゴリーについては、CSFと異なるプライバシー固有の内容を記載。

プライバシーフレームワークの構造

NIST Cybersecurity Frameworkの構造を採用。

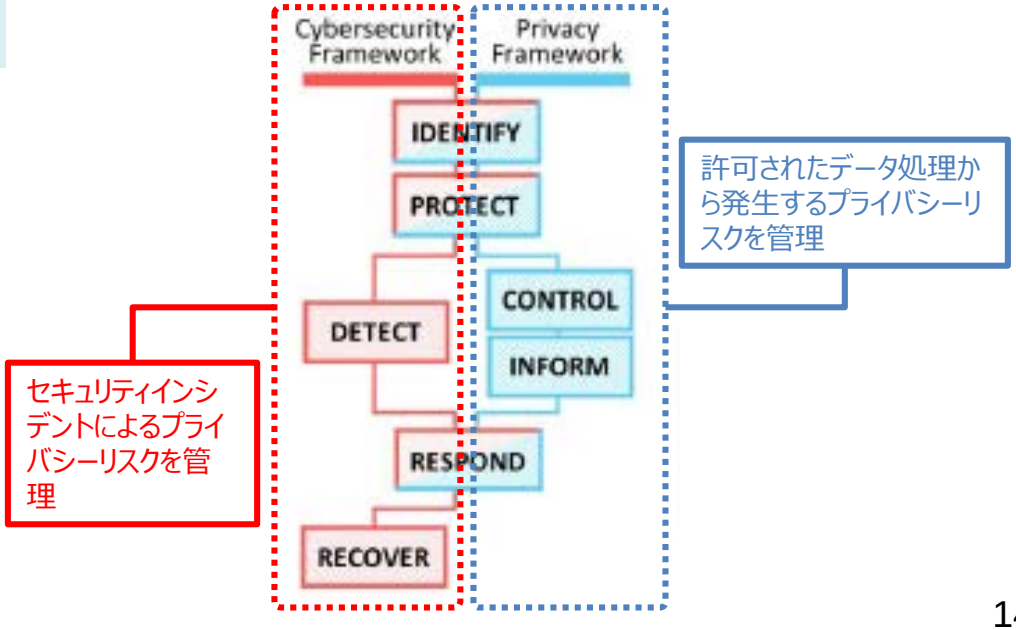
- コア（Core）
- プロファイル（Profile）
- インプリメンテーションティア（Implementation Tiers）



5つの機能に対して、合計で**23のカテゴリー**、**111のサブカテゴリー**を記載。

サイバーセキュリティフレームワーク(CSF)との関係

CSFと併用することで、網羅的なプライバシーリスクの管理が可能。



【米国における取組事例②-2】

プライバシーデータを守るためのセキュリティ対策：米国連邦取引委員会による取組

- **米国連邦取引委員会(FTC)**は、FTC法第5条(a)に基づき、「不公正な競争方法」及び「不公正若しくは欺瞞的な行為又は慣行」の視点から、**企業がプライバシー及びセキュリティデータ保護ポリシーを実行するよう規制**を実施。
- FTCは、**違法行為を行う企業**に対しては、是正するための**積極的な措置を講じることを要求**。さらに、違反企業に対して**罰金を科す**ことも可能。

報復ポルノサイトMyEx.comの事例

- ある事業者が報復ポルノサイトMyEx.comを開設。
- FTCとネバダ州は、報復ポルノサイトMyEx.comが被害者の親密な写真やビデオを、名前、住所、雇用主、ソーシャルメディアのアカウント情報などの個人情報とともに収集していると主張し、サイトの閉鎖、及び200万ドル以上の支払いを要求。
- 裁判所は、サイトの閉鎖、金銭的救済、全ての画像や情報の破棄を命じた。

大手知育玩具会社の事例

- 大手知育玩具会社とその米国子会社が、モバイルアプリを通じて個人情報を収集。
- FTCは、同社が個人情報を保護するために、侵入検知・防止システムの実装などの適切な保護策を講じておらず、その結果、ハッカーはそのコンピュータネットワークと子供を含むユーザーの個人情報にアクセスすることができたと主張。
- FTCと同社は、賠償請求、包括的なデータセキュリティプログラムの実施、20年間独立した隔年監査を実施することで同意。

【米国における取組事例③】

医療情報を守るためのセキュリティ対策：米国保健福祉省(HHS)による施策

- 米国の医療業界では、取扱う医療情報の漏えい時の報告義務や安全管理措置等について規定しているHIPAA＊1、HITECH法＊2及び、HIPAAに付随する規則の遵守を求められる。

米国における医療に係る個人情報の保護制度

- 米国の医療業界では、業界固有の個人情報保護ルールとして、HIPAA、HITECH法及び、HIPAAに付随する規則の遵守を求められる。

名称	概要
医療保険の携行性と責任に関する法律(HIPAA＊1)	保護対象医療情報の取扱いにおける標準や要件を確立し、医療システムの効率性と有効性を改善すること等を目的とした法律。
経済的及び臨床的健全性のための医療情報技術に関する法律(HITECH法＊2)	保護措置違反の基準及び違反に対する罰則を拡大し、取り締まり権限も強化。
HIPAAセキュリティ規則	電子的に保護すべき医療情報のために講じるべき処理及び技術的なセキュリティ対策に関する基準。
HIPAAプライバシー規則	対象となる医療情報のプライバシーを保護するために講じるべき対策に関する基準。

HIPAA及びHITECH法の主な規定事項

◆ **保護対象**

- 下記(i)~(iii)を満たす個人を識別可能な医療情報
  (i) 医療機関によって作成又は受領され
  (ii) 医療又は医療の提供に関連し
  (iii) 当該情報について、個人を特定識別するために用いることができると判断する合理的根拠があるもの

◆ **対象事業者に対する主な要求事項**

- **漏えい等事案発生時の本人及び監督機関等への報告義務(HITECH法にて規定)**
  - 保護対象医療情報が漏えいした場合、各個人や米国保健福祉省(HHS)に対する通知を義務付けている。
  - 500人以上の対象医療情報が漏えいした場合、メディアに対しても通報するように義務付けている。
- **安全管理措置**
  - HIPAAプライバシー規則及びHIPAAセキュリティ規則の遵守を義務付けている。
  - HITECH法は、対象事業者におけるセキュリティ監査についても義務付けている。

＊1：正式名称は、”Health Insurance Portability and Accountability Act of 1996”
＊2：正式名称は、” Health Information Technology for Economic and Clinical Health Act of 2009”

【欧州における取組事例①-1】
プライバシーデータを守るためのセキュリティ対策：GDPR

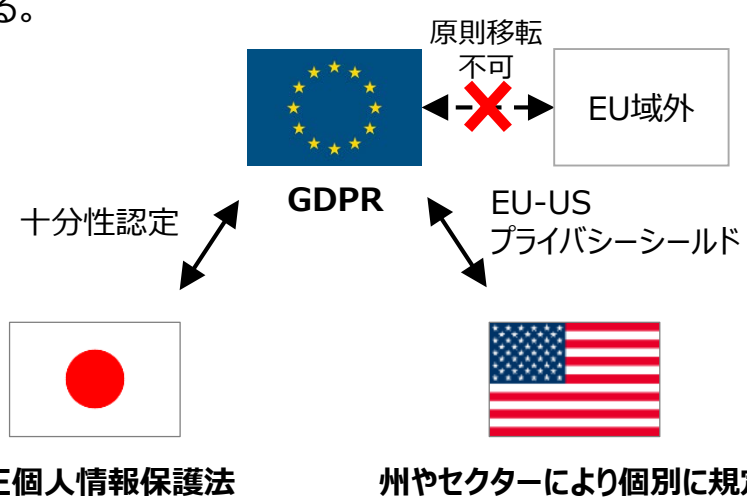
- EU域内の全ての個人データの保護を強化し統合することを意図した**EU一般データ保護規則**(**GDPR**: **G**eneral **D**ata **P**rotection **R**egulation)が、2018年5月25日に施行。
- 規定の違反に対する**高額な罰則金（全世界年間売り上げの4%以下又は2000万ユーロのいずれか高い方）**、個人データ侵害の**検知後72時間以内の監督機関への報告**等、前身であるデータ保護指令と異なる項目が多数設けられている。

GDPRにおける主な対応事項

- 同意の取得等による処理の法的根拠の確保 (6条～11条)
- 処理行為の記録 (30条)
- データ主体への情報通知・権利行使対応 (12条～23条)
- 社内規定の整備 (24条2項)
- 適切な技術的・組織的措置の実施 (24条、25条、32条)
- 個人データ侵害への対応 (33条、34条)
- データ処理契約の締結・更新 (28条、29条)
- データ保護責任者(DPO: **D**ata **P**rotection **O**fficer)・代理人の選定 (27条、37条～39条)
- データ保護影響分析(DPIA: **D**ata **P**rotection **I**mpact Analysis)の実施 (35条、36条)
- 域外移転規制対応 (44条～50条)

パーソナルデータの域外移転に関する規制

- EU域内で不統一であったパーソナルデータ保護法制の基本をGDPRに統一(必要に応じて各国で項目の追加等を実施)
- GDPR44条では、十分性認定に基づく移転等を除き、原則としてパーソナルデータの域外への移転を禁止している。



【欧州における取組事例①-2】
プライバシーデータを守るためのセキュリティ対策：GDPRに基づく制裁事例

- **ポルトガルのデータ保護当局が、病院に対し約5000万円の制裁金を決定(2018年７月)**
  - 病院において、ITシステム上の患者のデータを保護するためにGDPR32条に準拠した適切な技術的・組織的対策が取られていなかったと判断。
  - 医師の専門領域等に関わらず全ての患者のファイルに無制限でアクセスすることができたことなどが不適切とされた。

- **ドイツのデータ保護当局が、Knuddels.de（SNSプラットフォーム）に対し約460万円の制裁金を決定(2018年９月)**
  - ユーザ数十万人のメールアドレスとパスワードがハッキング後に公開された。
  - パスワードが暗号化されていない状態で保存されていたことなどが不適切とされた。

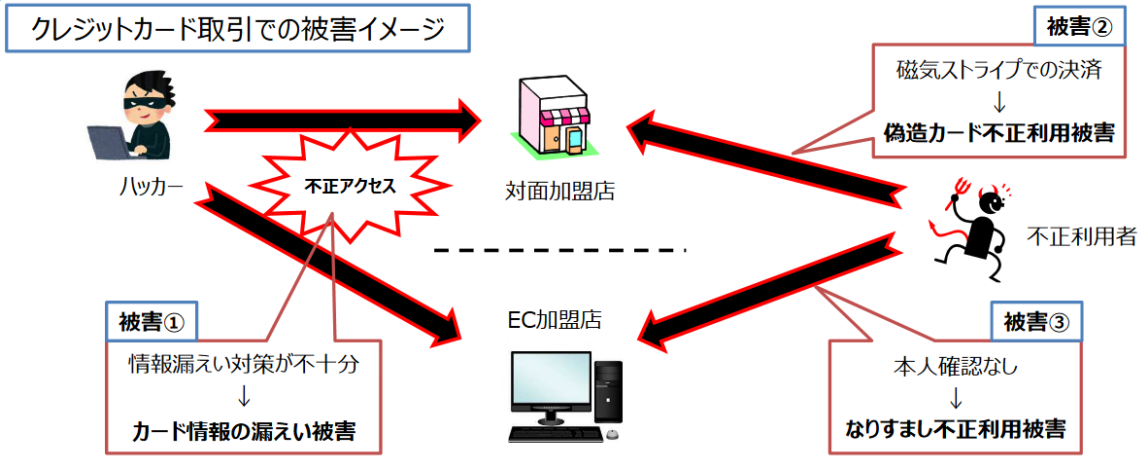
- **フランスのデータ保護当局が、Googleに対し約62億円の制裁金を決定(2019年１月)**
  - 透明性、情報提供義務、同意取得というGDPRの原則に関する重大な違反があったと判断。
  - 情報提供の同意が明瞭と言えるためには積極的な行為による必要があるところ、同意に用いるチェックボックスが事前にチェック済の設定であったことなどが不適切とされた。

- **フランスのデータ保護当局が、不動産サービスプロバイダSERGICに対し約5000万円の制裁金を決定(2019年6月)**
  - 適切なセキュリティ対策を講じなかったこと、契約に至らなかった顧客の個人データの保存期間を定義していなかったことが不適切とされた。

- **イギリスのデータ保護当局が、ブリティッシュエアウェイズに対し約250億円の制裁金を課す方針を発表(2019年7月)**
  - 2018年の顧客の個人情報が盗まれる事件がGDPRを侵害したと判断。

【業界共通の取組事例①】
クレジットカードのデータを守るためのセキュリティ対策：PCI DSS

- PCI DSSは、クレジットカード会員データを保護するために策定された**クレジットカード業界のセキュリティ基準**。
- 6つの目的に対応した12の要件、それを更に細分化した約400の詳細な項目を提示。



引用：

クレジット取引セキュリティ対策協議会
クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-2019-概要版

https://www.j-credit.or.jp/security/pdf/overview_2019.pdf

PCI DSSの構成

目的	要件		テスト手順
安全なネットワークとシステムの構築と維持	要件1	要件1.1	要件1.1.1a	テスト手順1.1.1a
カード会員データの保護	要件2	要件1.2	要件1.1.1b	テスト手順1.1.1b
脆弱性管理プログラムの維持		要件1.3	要件1.1.1c	テスト手順1.1.1c
強力なアクセス制御手法の導入	⋮	要件1.4	要件1.1.2a	テスト手順1.1.2a
ネットワークの定期的な監視およびテスト		要件1.5	⋮	⋮
情報セキュリティポリシーの維持	要件12			

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

２．サイバー空間のつながりに関わるセキュリティインシデント事例

３．データを守るためのセキュリティ対策に関係する取組

（１）海外の取組事例

（２）国内の取組事例

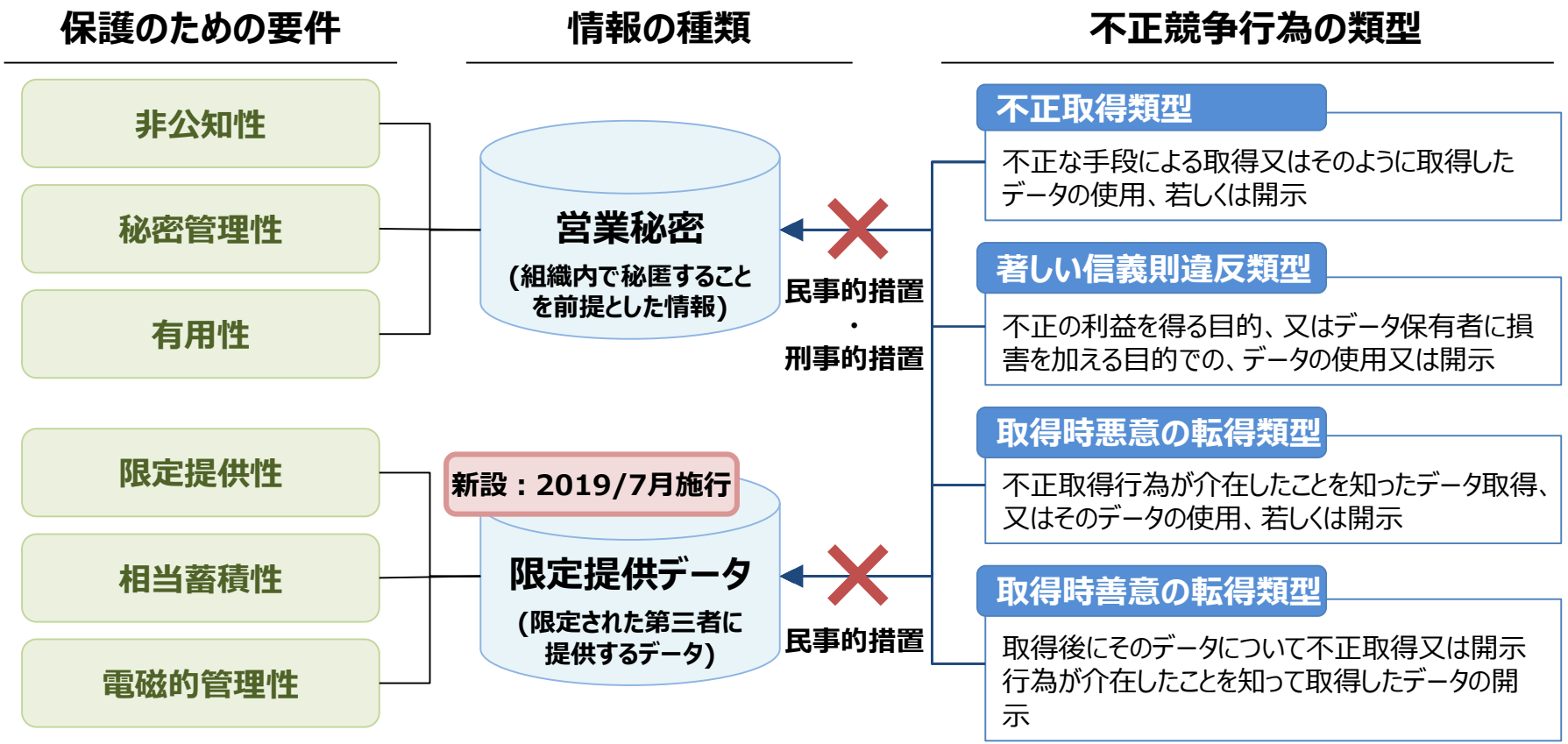
４．本タスクフォースの検討事項

データを守るためのセキュリティ対策に関係する国内の取組事例

名称	策定主体	策定（施行）年月	保護対象となるデータ	概要
営業秘密管理指針 （根拠法：不正競争防止法）	経済産業省	2019/01 改訂	営業秘密	営業秘密として法的保護を受けるために必要となる最低限の水準の対策を提示。 別途、漏えい対策として有効と考えられる対策等を紹介する 「秘密情報の保護ハンドブック」も策定されている。
限定提供データに関する指針 （根拠法：不正競争防止法）	経済産業省	2019/01 策定	限定提供データ	平成30年度の不正競争防止法改正により導入された「限定提供データ」の定義や不正競争に該当する要件等について考え方を整理。
改正割賦販売法	経済産業省	2018/06 施行	クレジットカード番号	加盟店も含めたチェーン全体でクレジットカード番号等の適切な管理を実施するための規定を新たに追加。
個人情報の保護に関する法律	個人情報保護委員会	2017/05 改正	個人情報	個人の権利・利益に係る基本理念の他、民間事業者の個人情報の取扱いを規定。
医療情報システムの安全管理に関するガイドライン （根拠法：個人情報保護法等）	厚生労働省	2017/05 改訂	医療に関する個人情報	医療に関わる情報を扱う全ての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄に関わる人又は組織を対象としたガイドライン。
医療情報を受託管理する情報処理事業者における安全管理ガイドライン （根拠法：個人情報保護法等）	経済産業省	2012/10 改訂	医療に関する個人情報	外部保存等のために医療情報を受託管理する業務を提供する情報処理事業者が、実装すべき管理策を提示。
クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン （根拠法：個人情報保護法等）	総務省	2018/07 策定	医療に関する個人情報	「医療情報システムの安全管理に関するガイドライン」をベースに、クラウドサービス事業者の観点から義務及び対応すべき事項について、要求事項を提示。

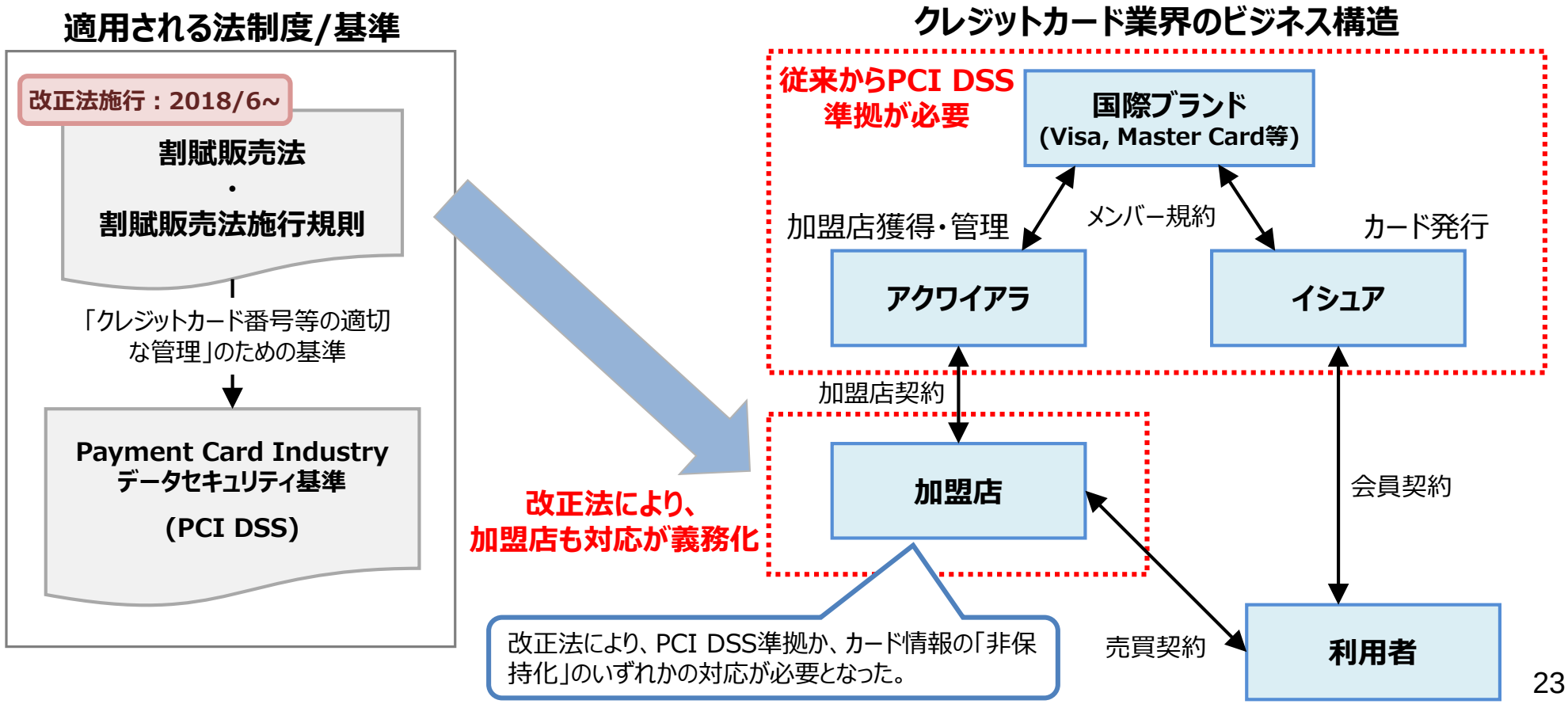
【国内における取組事例①】
組織が保有する情報を守るためのセキュリティ対策：不正競争防止法

- 不正競争防止法(日本)では、従来から「非公知性」、「秘密管理性」、「有用性」の3要件を満たすような**組織内で秘匿することを前提とされた情報を営業秘密として法的に保護**。
- 2018年の改正において、事業者等が取引等を通じて**第三者に提供するデータを念頭に新たに「限定提供データ」を定義**し、不正競争行為に対する保護の範囲を拡大。



【国内における取組事例②】
クレジットカードデータを守るためのセキュリティ対策：改正割賦販売法

- 改正割賦販売法（2018/6/1施行）では、**加盟店も含めたチェーン全体でセキュリティ対策水準を向上**させるため、「クレジットカード番号等の適切な管理」、「クレジットカード番号等の不正な利用の防止」について以下のような規定を新たに定めている。
  - **加盟店に、カード番号等の非保持化あるいはPCI DSS準拠を求める。**
  - 加盟店に、決済端末のIC化、なりすまし対策等の不正使用の防止を義務づける。

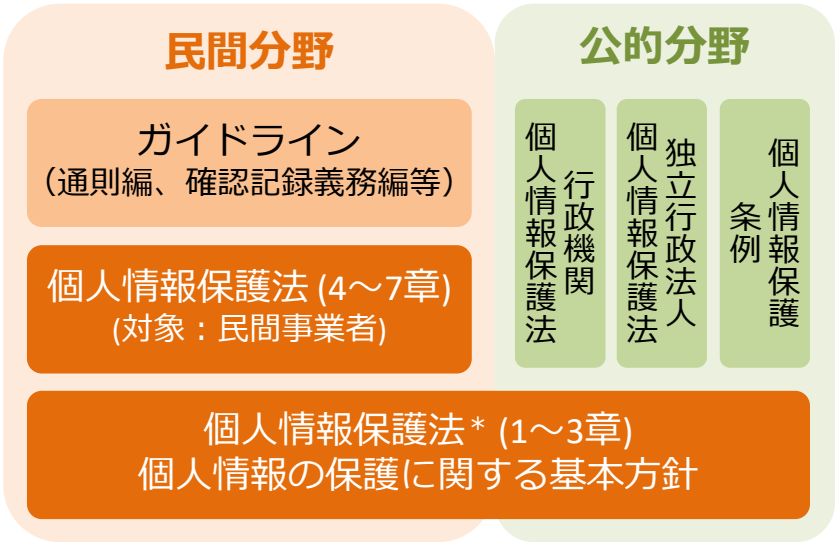


【国内における取組事例③】
個人情報を守るためのセキュリティ対策：個人情報保護法

- 個人情報保護法は、個人の権利・利益の保護と個人情報の有用性とのバランスを図るために2003年5月に成立。
- 2017年5月に改正法が施行され、現在、3年ごとに実施する見直しが行われている。

個人情報保護に係る法律・ガイドラインの体系

- 個人情報保護法*は、個人の権利・利益に係る基本理念の他、民間事業者の個人情報の取扱いを規定。
- 直近では、2017年5月に、右記のような改正がなされている。



2017年改正法の主なポイント

1. 個人情報保護委員会の新設
個人情報取扱事業者に対する監督権限を委員会に一元化。

2. 個人情報の定義の明確化
① 個人情報の定義に身体的特徴等が対象となることを明確化。
② 要配慮個人情報の取得については、原則として本人同意を得ることを義務化。

3. 個人情報の有用性を確保(利活用)するための整備
匿名加工情報の利活用の規定を新設。

4. いわゆる名簿屋対策
① 個人データの第三者提供に係る確認記録作成等を義務化。
② 個人情報データベース等を不正な利益を図る目的で第三者提供、又は盗用する行為を処罰の対象とした。

5. その他
① 取り扱う個人情報が5000件以下の場合も、規制対象とした。
② オプトアウト規定を利用する個人情報取扱事業者は所要事項を委員会に届け出ることを義務化、委員会はその内容を公表。
③ 外国にある第三者への個人データの提供の制限、個人情報保護法の国外適用等に係る規定を新設。

＊：正式名称は「個人情報の保護に関する法律」

【国内における取組事例④】
医療に関する個人情報を守るためのセキュリティ対策：ガイドライン

● **医療業界**では、医師法や個人情報保護法等において保護を規定されている診療録や調剤録等の**医療情報を安全に管理**するため、医療機関や、その委託を受ける情報処理サービス事業者等の対象事業者別に3省から公表されている**3つのガイドラインが適用**。

保護対象

医療に関する患者情報(個人識別情報を含む)を含む情報
例) 診療録(カルテ)、助産録、調剤録、処方せん

	医療機関向け	医療機関に情報処理サービスを提供する事業者向け	
適用されるガイドライン（3省3ガイドライン）	**2017年改訂** **厚生労働省** 医療情報システムの安全管理に関するガイドライン 第5版	**2012年改訂** **経済産業省** 医療情報を受託管理する情報処理事業者における安全管理ガイドライン 第2版	**2018年新設** **総務省** クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン

- 関連して、個人情報保護委員会及び厚生労働省から、居宅サービス事業者等の個人情報の適正な取扱いを定めた「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（2017年）も公表されている。

１．サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

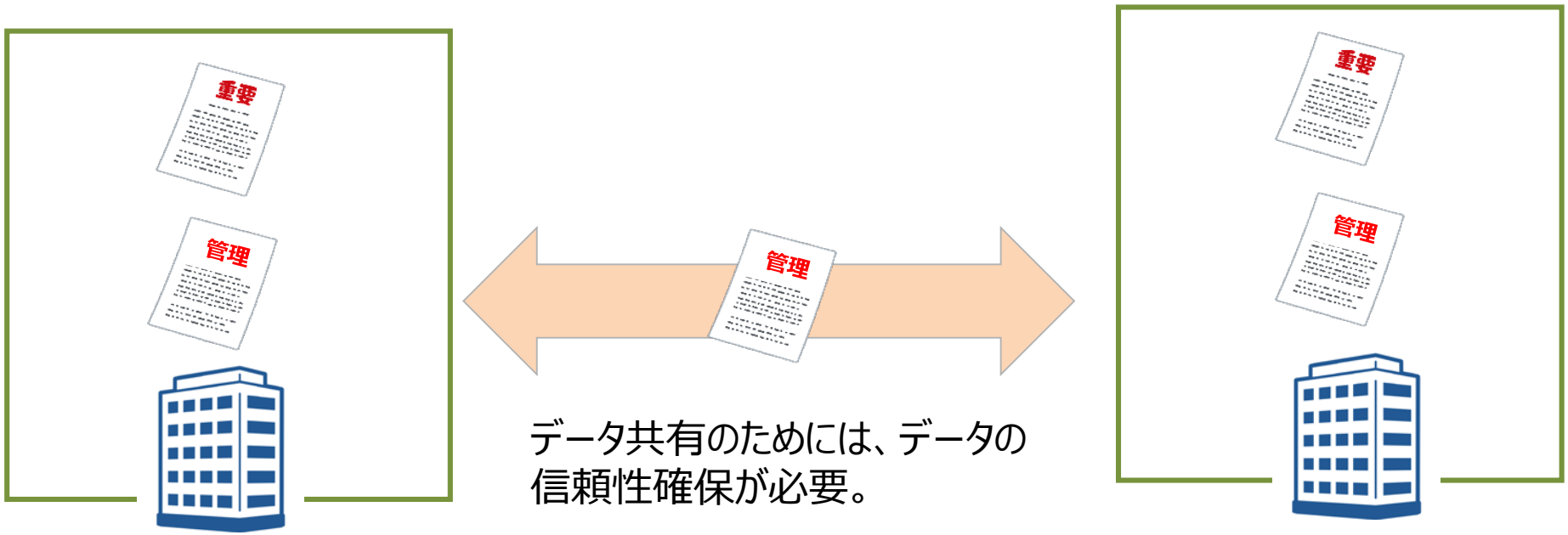
２．サイバー空間のつながりに関わるセキュリティインシデント事例

３．データを守るためのセキュリティ対策に関係する取組
（１）海外の取組事例
（２）国内の取組事例

４．本タスクフォースの検討事項

【本TFにおける検討の背景】
データの信頼性確保の考え方を整理する必要性

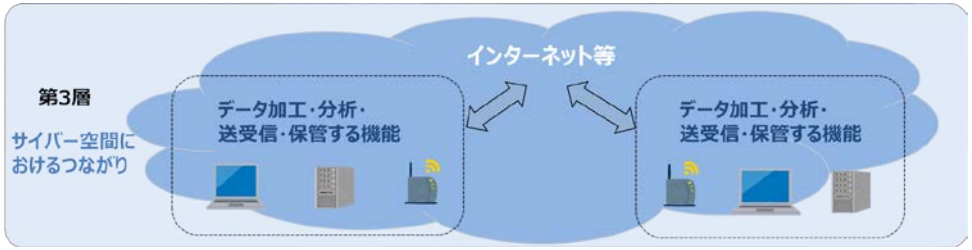
- G20において、**Data Free Flow with Trust (DFFT)**のコンセプトに合意。**プライバシーやセキュリティに関する**消費者や企業の**信頼を確保**していきながら、**自由なデータ流通を促進**していくことが重要。
- DFFTを広く社会に広げていくためには、**一定のセキュリティ対策等による信頼性の確保の考え方を整理し、社会に実装していくことが必要。**



データ共有のためには、データの信頼性確保が必要。

【現状】CPSFにおけるデータの信頼性確保の考え方

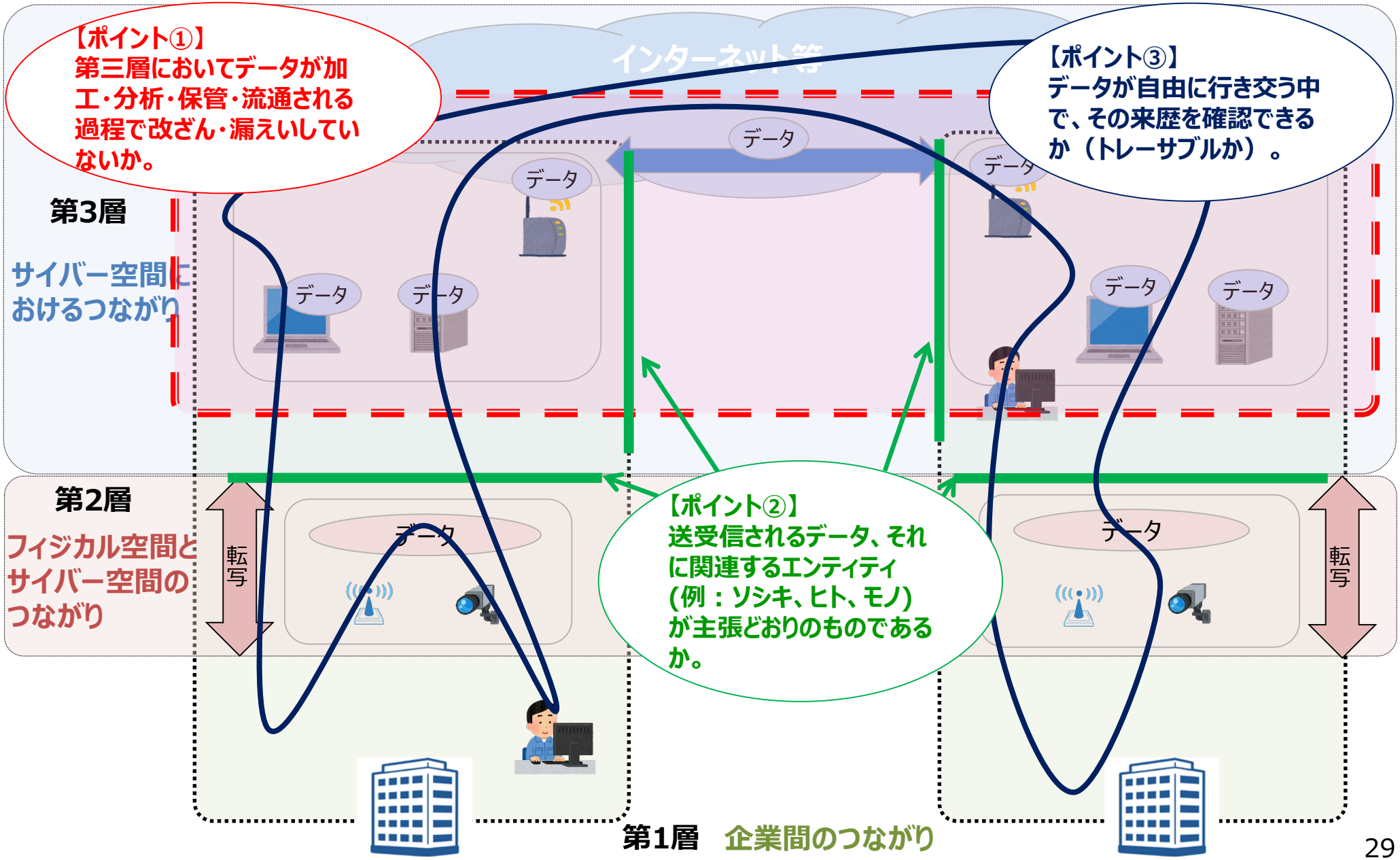
- CPSFでは、**データを第３層サイバー空間のつながりにおける信頼性の基点と設定**し、第3層の機能、想定されるセキュリティインシデントを定め、対策要件及びセキュリティ対策例を整理。
- その中で、**データの区分に応じたセキュリティ対策を実施することを要求**。



- **第3層における機能**
- **想定されるセキュリティインシデント を明確化**

対策要件ID	対策要件	対策例	対策例を実行する主体
CPS.GV-3	各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、**それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護**を行う。	・・・	O
CPS.SC-7	**自組織が関係する他組織との契約上の義務を果たしていることを証明するための情報(データ)を収集**、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	・・・	O/S
CPS.CM-4	**サイバー空間から受ける情報(データ)の完全性および真正性を動作前に確認する。**	・・・	S

【本TFにおける検討の背景】
データの信頼性確保に向けて更なる検討が必要なポイント



【本TFにおける検討の背景】
データの信頼性確保に向けて更なる検討が必要なポイント

データの信頼性確保のために考慮すべき観点	信頼性確保のために必要な要件	
【ポイント①】 データが加工・分析・保管・流通される過程で改ざん・漏えいしていないか。	データをセキュアに管理すること ⇒マネジメント、プロセス、セキュリティポリシー、システム要件等のセキュリティ要件の明確化など	機密性 完全性 可用性
【ポイント②】 送受信されるデータ、それに関連するエンティティ(例：ソシキ、ヒト、モノ)が主張どおりのものであるか	データそのものや生成者の実体の確認 ⇒データの真正性確認、モノ等の確認など	真正性
【ポイント③】 データが自由に行き交う中で、その来歴が確認できるか（トレーサブルか）。	データの来歴の確認 ⇒トレーサビリティの仕組みの検討など	責任追跡性 否認防止

本タスクフォースにおける検討の方向性

- 本タスクフォースにおいて、データの信頼性確保のために、「**データの区分に応じた適切なセキュリティ対策要件**」及び「**データの信頼性の確認手法**」を検討したい。

データの区分に応じた適切なセキュリティ対策要件の検討

データをセキュアに管理すること
⇒マネジメント、プロセス、セキュリティポリシー、システム要件等のセキュリティ要件の明確化など

データの信頼性の確認手法の検討

データそのものや生成者の実体の確認
⇒データの真正性確認、モノ等の確認など

データの来歴の確認
⇒トレーサビリティの仕組みの検討など

（参考）データの信頼性を構成しうる要素の定義

- データの完全性、可用性等の国際標準(ISO/IEC 27000シリーズ等)における定義は下記のとおり。

用語	定義	引用元	備考
情報セキュリティ (information security)	情報の機密性，完全性及び可用性を維持すること。注記 さらに，真正性，責任追跡性，否認防止，信頼性などの特性を維持することを含めることもある。	JIS Q 27000:2014	
機密性 (confidentiality)	認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。	JIS Q 27000:2014	
完全性 (integrity)	正確さ及び完全さの特性。	JIS Q 27000:2014	「正確であるとは、その情報システムに情報を格納したとき以後、正確に維持されていることだけを意味するのではない。情報システムに情報を格納するときに、適切な確認のプロセスを経るなどにより、正確な情報を格納することも含みうる」
可用性 (availability)	認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。	JIS Q 27000:2014	「情報の可用性は、それを保有したり伝達したりする機器が使いたいときに使えることにより確保されるため、機器の可用性で表現されることもある」
真正性 (authenticity)	エンティティは，それが主張するとおりのものであるという特性。	JIS Q 27000:2014	"真正性"という語は二通りの解釈があり得る。ひとつは、「"エンティティ、特に人が、ある情報について、当人に関する事実や当人の意思を正しく表した情報であると確認したものであること"をいう」。もうひとつは、「真正性は、そのエンティティが自ら主張するとおりの本物であるという意味である」。
責任追跡性 (accountability)	あるエンティティの動作が、どの動作から動作主のエンティティまで一意に追跡できることを確実にする特性	JIS X 5004	ISO/IEC 27000:2013の中では定義されていないため、他の規格からの引用としている。
信頼性 (reliability)	意図する行動と結果とが一貫しているという特性。	JIS Q 27000:2014	主体が人であれば"意図する行動"という語が、主体がものである場合は"意図する動作"という語がふさわしい。ISO/IEC 27002:2013の中では、サービス及びアプリケーションの信頼性について言及がなされている。
否認防止 (non-repudiation)	主張された事象又は処置の発生，及びそれを引き起こしたエンティティを証明する能力。	JIS Q 27000:2014	「"否認防止"とは"ある事象が又は処置・行為が発生したこと、及びあるエンティティがそれを引き起こしたことを否認又は否認の可能性に対抗して証明する能力"である」

＊：備考の内容は、中尾康二編著『ISO/IEC 27002:2013 情報セキュリティ管理策の実践のための規範 解説と活用ガイド』を参考に記載している。