セキュアIoTプラットフォーム協議会

仕様検討部会活動報告

～　データセキュリティ White Paper 概要　～

2026/02

セキュアIoTプラットフォーム協議会　仕様検討部会
座長　豊島　大朗

仕様検討部会　これまでの活動

～2021年度

・IoTセキュリティ手引書の発行

　仕様検討部会では様々な分野の会員の方々から、それぞれの分野で必要と考えられるIoTセキュリティの課題と対応策について意見を収集し、集約してきました。
　IoTセキュリティ手引書では、集約した意見について、国際的に標準となりつつある国際電気標準会議（IEC）が開発した「産業システムにおけるセキュリティ規格」であるIEC62443と米国立標準技術研究所（NIST）が発行する「非連邦政府組織およびシステムにおける管理対象非機密情報（CUI）の保護」を目的としたSP800-171rev.2を基準に項目の検証を行いました。

CUI: Controlled Unclassified Information

昨年度までの成果

2022年～2023年度

・小型機器編の発行

　IoTセキュリティ手引書では、それぞれに実績を持たれた様々な企業からセキュリティ対策を収集し整理しました。これらは一つ一つが実績をもった有益な情報ではありましたが、実際の機器への適用に際しては一貫性の面で難があると考えました。

　そこで小型機器編では会員企業様が販売されている実際の機器をサンプルに置き、手引書を見直すことで実用性の高い手引き書へ進化させることを目的とし、機器に関するドキュメントをお借りし、これの分析と解釈から始め、手引書を新たに構成しなおしました。

これまでの手引書の問題点

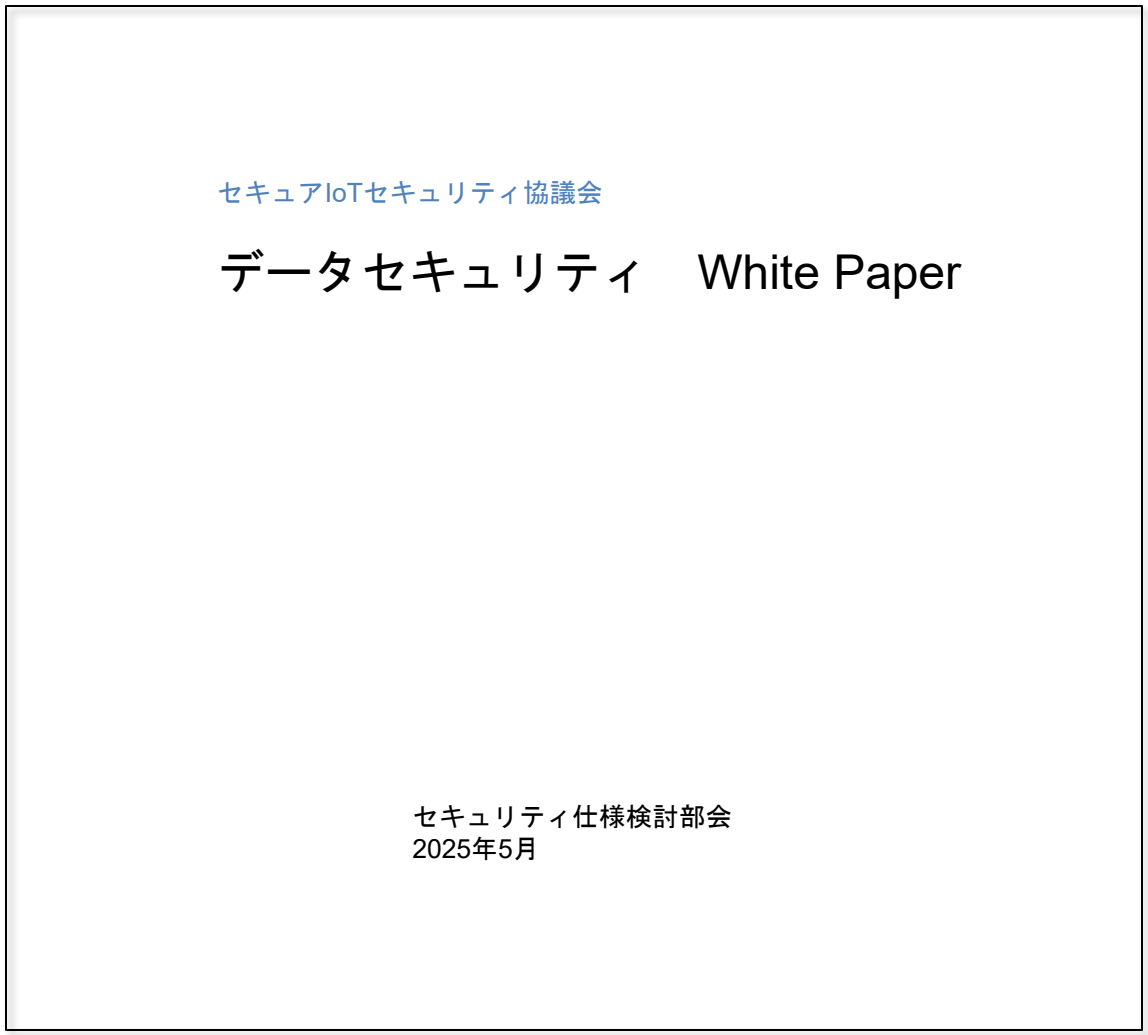
視点がIoT機器に偏っている

視点をIoT機器としているため、「IoTセキュリティ手引書」では特にメーカの開発部門を中心とした、製品ライフサイクル（企画、設計、製造、量産、販売、設置、廃棄）におけるセキュリティ対策が中心となっています。

クラウドやサービスを含めたセキュリティ検討

　IoT機器においては、少なからずクラウドやサーバを絡めたサービスとの連携が必須となります。IoTをシステムとみてセキュリティを検討するためにデータを中心としたセキュリティ検討を実施し、これをWhite Paperとしてまとめてみました。

データセキュリティ　White Paper


セキュアIoTセキュリティ協議会

データセキュリティ　White Paper

セキュリティ仕様検討部会
2025年5月

データセキュリティ White Paper の内容

　データセキュリティに関しては現時点でNISTの NCCoE（National Cybersecurity Center of Excellence：国家サイバーセキュリティエクセレンスセンター）が Data Security として、SP1800-11,25,26,28,29で発表していますが、国際基準としては未だ確定していません。
　またCSAが2021年に Cloud Data Protection を発表されていますが、対象がクラウドサービスとなっています。
　データセキュリティWhite Paperでは、クラウドサービスやデータサーバとIoT機器の連携によるセキュリティを踏まえて検討しました。

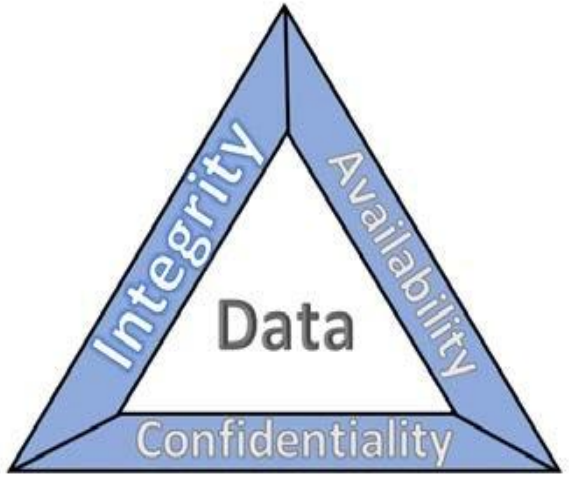
NIST SP1800-11,25,26,28,29概要

NIST-SP1800 Data Security では、情報セキュリティの三本柱としてCIA（機密性、完全性、可用性）をそれぞれ以下のように定義しています。

- 機密性（Confidentiality）NIST SP1800-28,29
  個人的プライバシーや専有情報を保護する手段を含め、情報へのアクセスや開示に対する認可された制限を維持する。

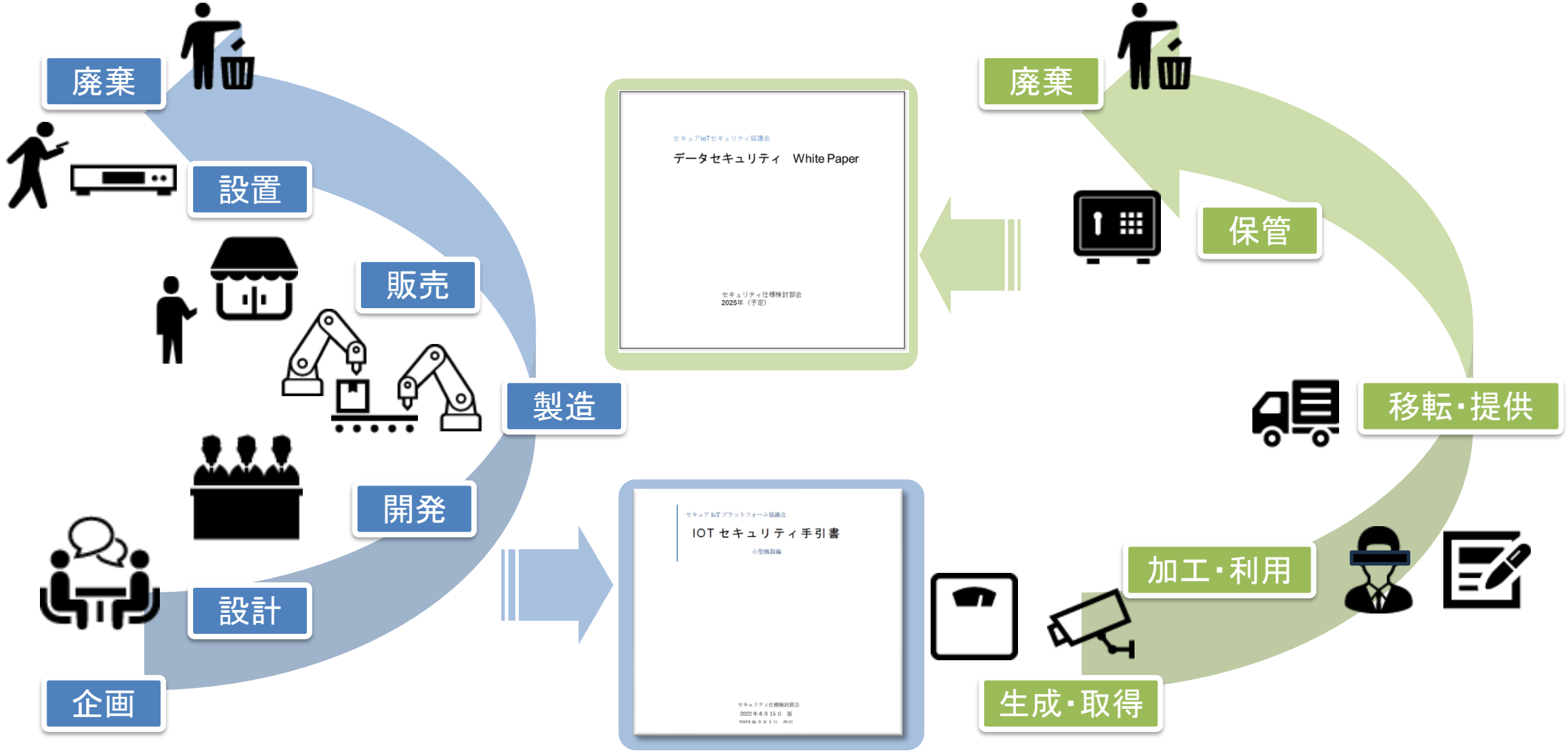
- 完全性（Integrity）NIST SP1800-11,25,26
  情報の不適切な変更や破壊を防止し、情報の否認防止と真正性を確保する。

- 可用性（Availability）
  情報へのタイムリーで信頼できるアクセスと利用を確保する。



※NIST SPECIAL PUBLICATION 1800-25　より抜粋

データを中心とした検討へ



データセキュリティWhite Paper 概要

White Paper 目次は以下となっています。

※データセキュリティ White Paper より抜粋

データセキュリティWhite Paper 概要

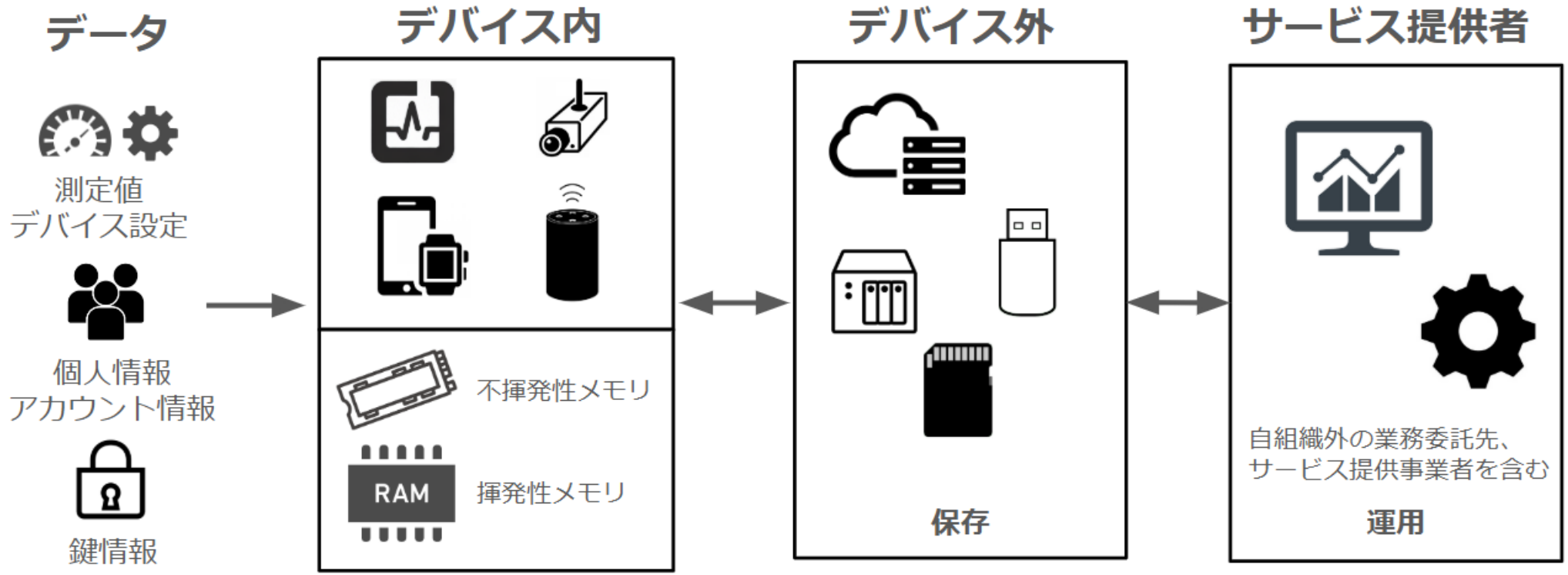
White Paperでは以下の様に、その意義を定義しています。

このWhite Paperは、データのライフサイクルマネジメントについてSIOTP協議会の考え方を整理し、データとデータマネジメントのセキュリティ向上手段を提案するものである。
データマネジメントと言う文言は DAMA International の「データマネジメント知識体系ガイド 第二版」に出てくるが、確立された定義とはなっていない、本White Paperではデータとデータマネジメントについて、IoTプラットフォームでの考え方を整理し、これまで重視してきたセキュアIoTプラットフォームに関わる国際規格に基づいたライフサイクルマネジメントの考え方を適用すべきと考えている。
それにより、各ライフサイクルステージにおける、必要とされるセキュリティレベル、そのためのセキュリティ施策が整理でき、国際規格にもとづく「データマネジメント」ガイドライン作成への道筋を描写することが可能になるであろう。

※データセキュリティ White Paper より抜粋

データセキュリティWhite Paper 概要

White Paperでは以下の様に、検討モデルを設定しています。これを踏まえて、デバイスとサーバサービス、クラウドサービスを想定し検討しています。



※データセキュリティ White Paper より抜粋

データセキュリティWhite Paper 概要

White Paperでは以下の様に、主な保護資産の対象となるデータを参考例として掲載しています。また、これらデータのデータライフサイクルにおける保護対策についても参考例を掲載しました。

分野	具体例	扱うデータ例
パーソナルIoT（家庭）	- スマートホームデバイス - ウェアラブル医療機器	- 音声データ - 個人情報 - 測定値（生体情報など） - デバイス設定 - アカウント情報 - 鍵情報
インダストリアル IoT（法人）	- 工場の機械設備 - スマートシェルフシステム - コールドチェーンモニタリング システム	- 測定値（センサーデータなど） - デバイス設定 - アカウント情報 - 鍵情報
パブリックIoT（行政）	- 交通管理システム - 緊急時対応システム	- 測定値（交通量データ、災害発生データなど） - デバイス設定 - アカウント情報 - 鍵情報

※データセキュリティ White Paper より抜粋

データセキュリティWhite Paper 概要

White Paperでは以下の様に、データのバックアップ方式によるメリットとデメリットを掲載しています。

IoTデータの保存先	メリット	デメリット
クラウドストレージ	- 拡張性が高く、大容量のデータを保存できる。 など	- データ容量や使用頻度によって、費用が高額になる、または想定していた費用と差がでる場合がある など
オンプレミスストレージ（テープ、NAS、サーバなど）	- IoT機器に近い場所に設置できネットワーク遅延が少ない など	- ハードウェア導入時に、数年単位でデータ容量を予測する必要がある など

また、データの性質や利用目的に応じてこれらを含む適切な方法を組み合わせることで、データ保存の効率と安全性を高めることができるため、ハイブリットクラウドやマルチクラウド、エッジコンピューティングの導入にも触れています。

※データセキュリティ White Paper より抜粋

データセキュリティWhite Paper 概要

White Paperでは以下の様に、データの消去についても触れています。

データ消去およびデバイスの廃棄工程におけるリスク

また、NIST SP800-88を参考に消去の手法として「消去（Clear）」「抹消（Purge）」「破壊（Destroy）」の3つに対してそのメリット・デメリットを含めた解説を掲載しています。

※データセキュリティ White Paper より抜粋

今後の予定

セキュリティ要件適合評価およびラベリング制度（JC-STAR）の研究

- IPAより講師をお招きした講演会の実施
- JC-STARの取得方法と活用の研究

ご清聴ありがとうございました

下記QRコードより White Paper がDLいただけます