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

2024/3/6

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は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。

小型機器編の応用例１

国際基準のセキュリティ要件

「コンポーネントが依存する認証子は、ハードウェアメカニズムによって保護されなければならない。」

※IEC62443-4-2　CR1.5　認証機構管理
　付則１　認証機のハードウェアセキュリティ　より

「支援インフラへの物理的アクセスを管理するために使用される管理策には、たとえば、鍵がかかった配線用ボックス、分離したまたは鍵がかかった予備ジャック、導管やケーブルトレイによる配線の保護、および、通信傍受センサーなどがある。

※SP800-171　3.10　物理的保護
　3.10.2　組織のシステムの物理的施設および支援インフラを保護し、監視する。　より

販売時のセキュリティ課題

左記の要件は、HSM（Hardware Security Module）の実装と鍵付きのケースによる保護で要件を満たすことを要求しています。

しかしメーカがセキュリティ対応モデルを製造していても、セキュリティ対策は販売価格に影響するため、顧客がセキュリティ対応モデルを選択しないことが予想されます。

メーカ側としては、販売時に機器を導入するシステムがどのようなセキュリティ基準への対応が必要かを把握し、セキュリティ対応モデルの採用が必須となることを伝えることが重要となります。

小型機器編の応用例２

設置時のセキュリティ課題

　小型機器では設置業者が必要な設定を（最低限の範囲で）実施する場合が一般的であり、運用を考慮しながら以下のようなセキュリティ機能が有効となるよう設定を合わせて実施する必要があります。
　セキュリティ設定費用を作業項目として顧客に認知いただく必要があります。
※コンシューマ機器ではユーザが実施します。

- CR1.2　ID認証
- CR1.5　初期認証機能
- CR1.7　パスワード強度
- CR1.11　認証ロック機能
- CR3.2　マルウェア対策

など・・・

※いずれも　IEC62443-4-2　のセキュリティ要件

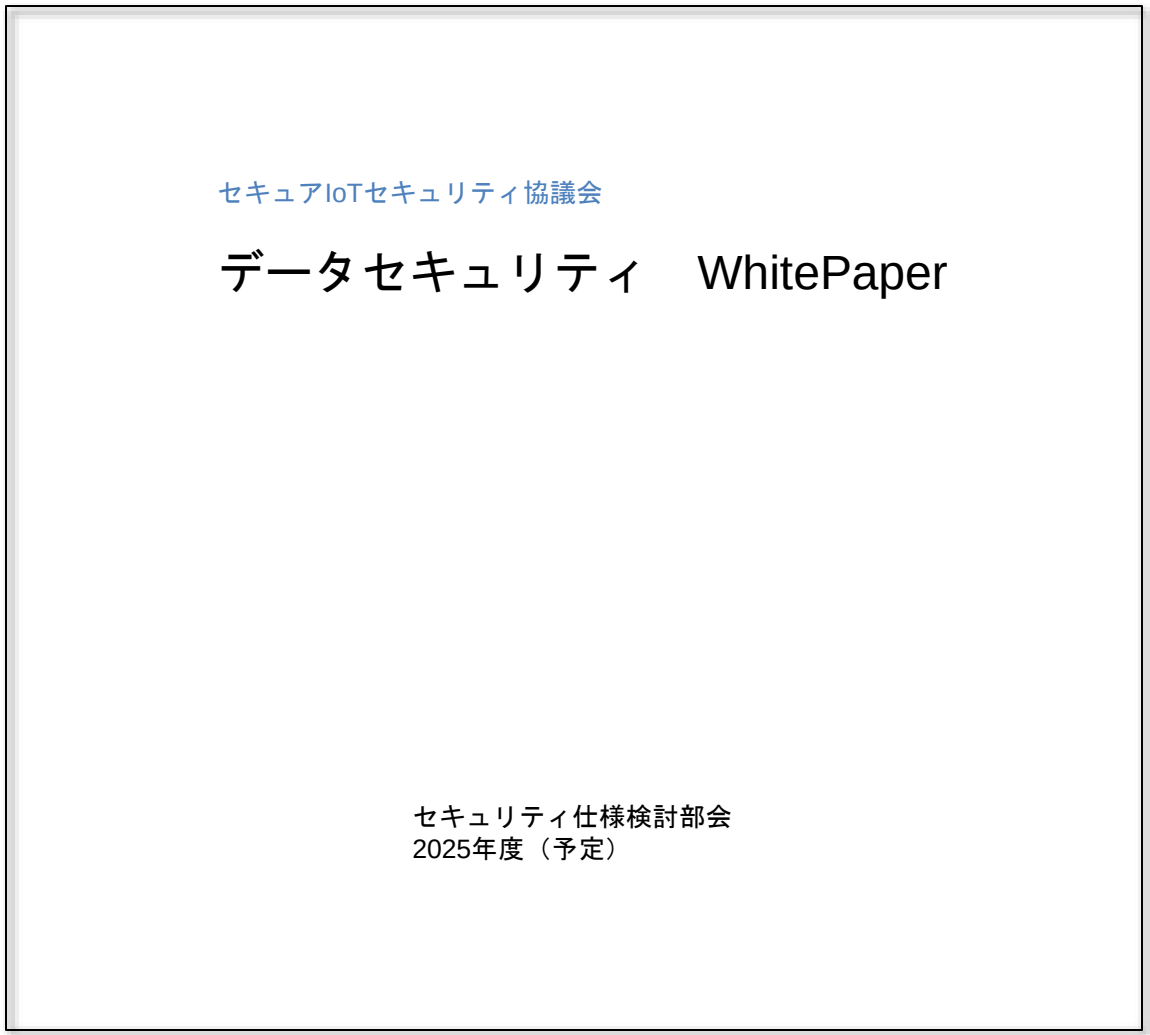
運用時のセキュリティ課題

　運用時には、設置時に設定したセキュリティ機能の有効性を維持する必要があります。
　ID認証で例えれば、移動や退職などにより担当者が変更となった場合、国際基準では旧担当者のIDを削除し新たな担当者にIDを発行することが望ましいとなっています。
　ユーザIDに有効期限を設け、これを超過し更新がない場合、認証ロック機能によって旧IDの不正利用へ対応することも可能ではありますが、タイムラグを考慮し不要なIDは速やかに削除することが望ましいとされています。

「退職や異動などの人事処理中、およびその後において、CUI を含む組織のシステムが保護されていることを確実にする。」

※SP800-171　3.9　要員のセキュリティ　3.9.2　より

仕様検討部会　活動紹介　new steps



データ編　WhitePaper作成に向けて

　仕様検討部会では、これまで「IoTセキュリティ手引書」の発行、同「小型機器編」の発行を実施してまいりました。
　本年度は、「IoTセキュリティ手引書」では少ししか触れられなかった、データそのもののセキュリティ対策について検討を進めています。
　データセキュリティに関しては現時点でNISTがSP1800シリーズで一部発表していますが、国際基準としては未だ確定していません。とはいえIoTセキュリティにとっては、クラウドセキュリティとのつながりがデータセキュリティという観点で今後重要になってくると考えられこれを検討することとしました。
　WhitePaperの発表は来年度を計画しております。

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

2024/3/6

セキュアIoTプラットフォーム協議会　仕様検討部会
データライフサイクル分科会　座長　加藤　貴

分科会の目的

- IoT機器、クラウドに保存しているデータの消去（廃棄）を製品メーカーや事業者の基準となる

ガイドラインの作成

- ガイドラインを準拠することで、データを正しく消去したことを証明し、真実であることの証拠となる

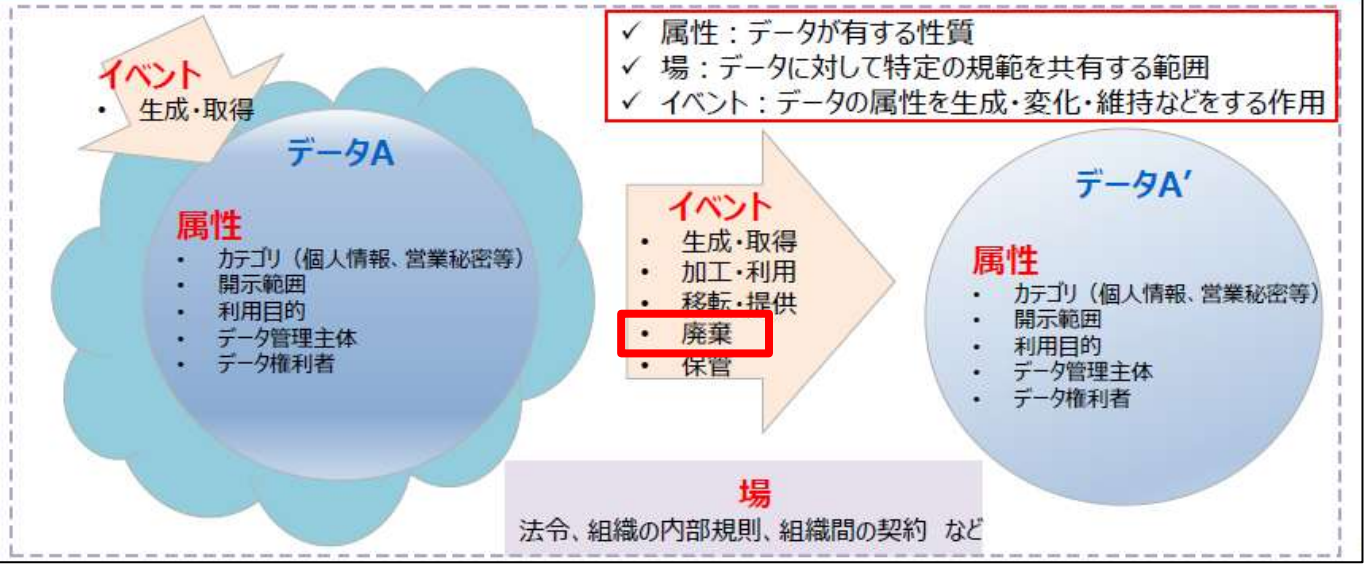
証明書の発行

経済産業省　商務情報政策局 サイバーセキュリティ課
協調的なデータ利活用に向けたデータマネジメント・フレームワーク

機器	データの移転・提供を実行するサーバ、IoT機器、ネットワーク機器等のデータを物理的に取り扱う単体のシステムコンポーネント	● 機器におけるセキュリティ実装が十分でないことにより以下のようなセキュリティ上のリスクが生じうる。 - 機器内の不正なコンポーネントを通じた意図しないデータ移転 - DDoS攻撃等のサービス拒否攻撃による機器の稼働停止

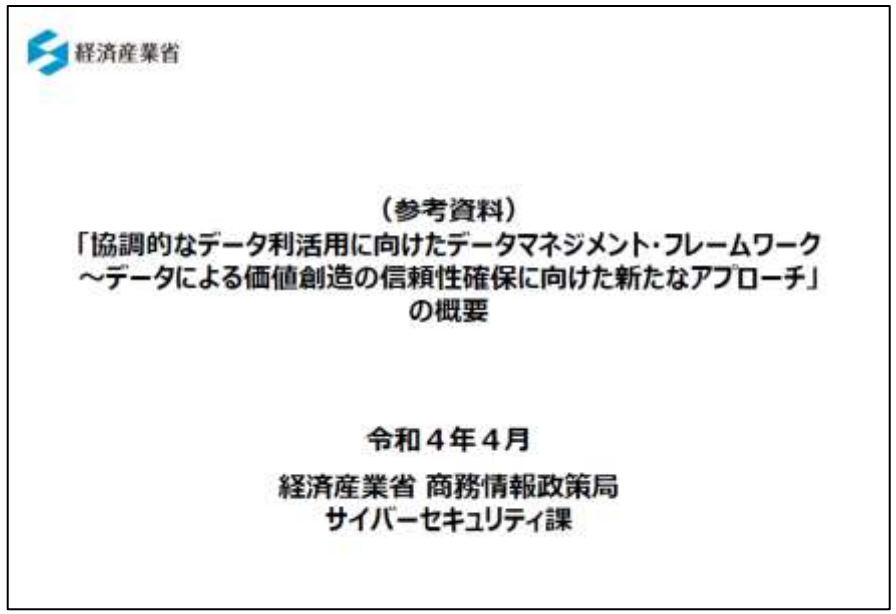
データマネジメントのモデル化の概要

- データマネジメントを「**データの属性が場におけるイベントにより変化する過程を、ライフサイクルを踏まえて管理すること**」と定義。
- **「属性」「場」「イベント」の3つの要素はそれぞれが相互に影響**しあう関係。
- データの遷移による**データの変化に関する一定の予見可能性を確保、ステークホルダーの間で認識を共有しやすく**なる。
- 共通の理解に基づいてそれぞれの主体が実施すべき措置についての検討を進めることが可能となり、**ステークホルダー全体で適切なデータマネジメントを実施していくことができる環境を実現**していく。



＜廃棄＞

- 本フレームワークにおける**廃棄は、データセット全体を使用不可能な状態とすること**を指す。
- 同意に基づいて収集したパーソナルデータに関して、特定の個人が同意を撤回する等により、当該個人のデータをデータセットから除外する行為は、加工・利用の一形態として捉えるのが適切。
  - 代表的なリスク：廃棄すべきデータが残存して漏えいする、本来は廃棄すべきでないデータまで廃棄してしまうなど。


経済産業省

（参考資料）
「協調的なデータ利活用に向けたデータマネジメント・フレームワーク
～データによる価値創造の信頼性確保に向けた新たなアプローチ」
の概要

令和４年４月

経済産業省 商務情報政策局
サイバーセキュリティ課

経済産業省 令和4 年4 月8 日

総務省

地方公共団体における情報セキュリティポリシーに関するガイドライン

分類	機器の廃棄等の方法	確実な履行を担保する方法
（1）マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（3）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。
（2）機密性2以上に該当する情報を保存する記憶媒体（上記（1）に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述（3）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（3）機密性1に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、（2）に記述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS及び記憶装置の初期化（フォーマット等）による方法は、HDDの記憶演算子にはデータの記憶が残った状態となるため、適当ではない	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。
※上記（1）は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む）		

図表24　情報の機密性に応じた機器の廃棄等の方法

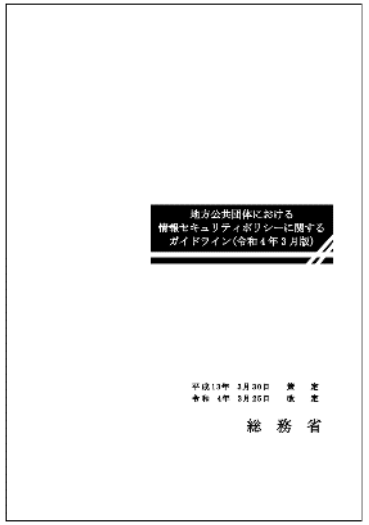
第4編 特則の概要：第4章　情報セキュリティ対策について④

第4章　情報セキュリティ対策について　/　4.物理的セキュリティ

特則のポイント

- ○ 標準準拠システムでは、機密性の高い情報資産を扱うため、これらの情報資産をクラウドサービスに保存する場合は、クラウドサービスを利用する装置等の廃棄の方針及び手順の確認が必要であることを記載。
- ○ 当該確認に当たり、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等の利用が可能であることを記載。

第4章　情報セキュリティ対策について（例文）	
4.物理的セキュリティ	（7）　機器の廃棄等 ②クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。 なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。



令和4年3月25日 改定

データ消去・廃棄の課題

- 総務省、経済産業とでの機密情報の消去（廃棄）の差異
- NIST（米国標準技術研究所）「SP800-88 SP1」は、2014年以降は未更新

IEEE（米国電気電子学会）にて引き継がれ2022年まで更新しています。

IEEE 2883-2022
Standard for Sanitizing Storage

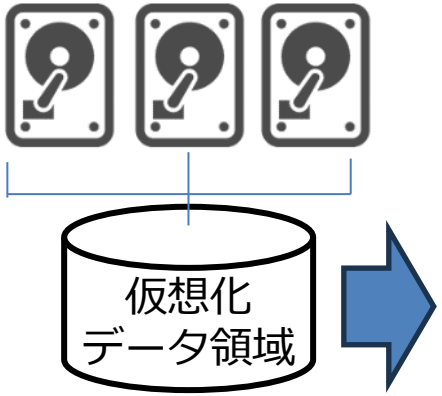
IoT機器が接続するクラウドサービスでのデータ消去の課題

- DXの推進によって、データの記憶媒体はIoT端末（デバイス）から、IoTのデータを保管しているクラウドへ移行しているため、対応した消去方法が必要になる。
- IoT機器が接続するクラウドサービスで保有しているデータの暗号鍵を抹消すれば、復号が現実的には不可能になる。

媒体ごとに

物理破壊

ソフト消去



仮想化データ領域は媒体が一つにまとまっているため、媒体ごとに消去することができない。

暗号化消去

暗号化消去（Purgeレベル：除去）
ディスクボリューム（データ領域）を暗号化して運用し、データを消去する際には、暗号鍵を復元が困難なように適切に除去することで、データの復元が困難になり、パージレベルで除去されたことと同等以上の消去が実行されたことになる

分科会の活動

- 2023年12月11日
  - 発足
  - メンバー募集
- 2024年1月25日
  - 第1回検討会
- 毎月1回の検討分科会を実施