ADEC データ適正消去実行証明協議会

クラウドデータ消去認証分科会

消去技術認証基準委員会

【別冊】データ消去技術ガイドブック

暗号化消去技術　編

2023 年 5 月　1.1 版

目次

はじめに

本ガイドブックにおいては、地方自治体、企業、団体にてクラウド環境の調達指針に基づく取組を円滑に実施できることを目的として、導入後のデータのライフサイクルの終了までを考慮した調達が実施できるように実務おいて具体的に検討すべき事項やその検討作業の実施手順、さらには、当該検討に当たっての留意事項等について、データ消去技術、設計・開発、ハードウェア、保守及び運用に係る方法論、分離調達におけるプロジェクト運営や契約に関する事項を中心に記述しております。企業、団体、地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、技術情報を取りまとめ、具体的なソリューション例を提示するものです。

ADEC データ適正実行証明協議会では 2018 年より、データ消去の実行者が適正に消去を実行するためのデータ消去技術 ガイドブック（ダウンロード：https://adec-cert.jp/guidebook/index.html）を作成してきており、それに基づいて消去ソフトおよび消去技術を搭載したハードウェアの認証基準を策定し、認証検証を実施してきておりました。

しかしながら、データ消去技術 ガイドブックでは暗号化消去については扱っておらず、クラウドにおける消去などを考慮すると暗号化消去が不可欠となると考えられることから、暗号化消去についての技術ガイド別冊として暗号技術に特化した解説書を作成することし、クラウドデータ消去認証　分科会を設立して検討・調査および策定の開始をいたしました。

本ガイドブックの経緯

総務省では、地方公共団体における情報セキュリティポリシーの策定を推進するため、平成 13 年 3 月 30 日に「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」を策定しております、その後、令和 2 年 5 月 22 日には、「クラウド・バイ・デフォルト原則」、行政手続のオンライン化、働き方改革、サイバー攻撃による情報流出事件といった新たな時代の要請や「三層の対策」の課題を踏まえた「自治体情報セキュリティ対策の見直しについて」がとりまとめられました。さらに、平成 30 年 7 月の政府機関の情報セキュリティ対策のための統一基準の改定、および、令和元年 12 月に発生した神奈川県庁の神奈川県庁での HDD 転売・情報流出事件で令和 2 年 5 月よりワーキンググループでの検討結果を踏まえて、情報システム機器を廃棄、リース返却等をする場合、機器内部の記憶装置からの情報漏洩リスクを軽減する観点から、情報の機密性に応じた方法により、情報を復元困難な状態にする措置を徹底することを同ガイドラインに追加しました。その意見募集の際にも、近年クラウド環境における仮想化データ（論理記憶領域）においてのデータ消去の措置についても課題として挙げられおり、本ガイドブックにおいて、読者として情報セキュリティポリシーの策定を行う者、セキュリティ上の職責を担う者などを想定して暗号化消去について環境に応じた技術情報、運用方法について記述しています。

また、政府は 2018 年からクラウドサービスの利用を第一候補とする考え方「クラウド・バイ・デフォルト原則」に基づき、政府機関だけでなく官民挙げてのクラウド導入を進めるため、ISMAP 制度を開始することを発表しました。各省庁は原則、ISMAP 制度に登録されたクラウドサービスの中から調達することになります。その調達の仕様検討に役立ててもらうことを想定しております。

政府の成長戦略や新型コロナウイルス感染症の流行拡大などを契機として、テレワークや Web 会議が普及・拡大する中、スマートフォンやタブレット型端末はもちろんのこと、組織配布のモバイルデバイや個人所有のモバイルデバイスで、組織のネットワーク以外の場所から業務情報にアクセスする機会が拡大しています。

モバイルデバイスには、iOS / Android などのスマートフォンタブレット端末のほか、Windows / Mac OS / Linux などのモバイルデバイスなど様々な端末種別や OS を考慮に入れる必要があります。

日本政府においても『政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版）』において、「情報の抹消」に暗号化消去が定義されました。これにより、従来の上書き技術/方法/ツールを使って媒体を複数回上書きする抹消方法や、細断、粉砕、粉砕、または焼却などの破壊によるデータ抹消方法に加え、暗号化消去が選択できる形となっています。

モバイルデバイスは、外部に持ち出すことや私有端末で業務データに触れる可能性もあることから、従来の環境における端末の廃棄のほかにも、紛失や盗難等のリスクも鑑みたデータ抹消の方法をあらかじめ検討しておく必要があります。

このためにはデータドライブ全体を暗号化しておき、暗号化消去が可能な状態にしておくことは大変有効な施策です。このような日本政府の方針と米国の国立標準技術研究所（NIST）が発表している記録媒体のデータ抹消の基準である「NIST SP 800-88 Rev.1」に規定されたデータ抹消レベルを参照して策定したものが本紙【別冊】データ消去技術ガイドブック　暗号化消去技術編となります。

SDGs 17 で 9,11,12 高度循環型社会の実現

データを消去するたびに、情報機器資産の廃棄を実施することは CO2 の排出につながり、循環型社会と言えなくなってしまいます。リサイクル IT 資産は、使用済み IT 資産を原材料として再資源化することで資源確保と廃棄物の発生抑制に繋がりサステナブルな社会の構築に貢献します。データが漏えいしないようにセキュアなリユース・リサイクルを推進しています。安全なデータ消去の作業標準を定め、パートナーシップで啓蒙しています。

SDGs 17 「パートナーシップで目標を達成」

SDGs 9「産業と技術革新の基盤をつくろう」

SDGs 11 「すみつづけられるまちづくりを」

SDGs 12「つくる責任 つかう責任」

※本報告書に掲載されているすべての会社名、商品名、サービス名等は、該当する各社の商標又は登録商標です。本解説書中では、™ Ⓡ Ⓒ表記を省略しています。

第 1 章　ガイドブック概要

ガイドブック発行実施主体：
データ適正消去実行証明協議会（以下　ADEC）

ADEC の活動：
　機密データの抹消に関する高い信頼性を社会的に実現するために、論理記憶領域に保存されたデータの適正な抹消を行い、その事実を第三者機関として電子署名を有する証明書を発行する業界標準ガイドラインの策定

対象読者：
　本ガイドブックにおいて、読者として情報セキュリティポリシーの策定を行う者、セキュリティ上の職責を担う者などを想定して暗号化消去について環境に応じた技術情報、運用方法について記述しています。
　また、クラウドシステムの提供に関わる事業者に活用していただくことで、クラウド利用者にセキュリティレベルの高いサービスを提供できることを期待しております。

実施方法：
　データ抹消に関する技術、知見を持つ会員企業および、協議会外から参加ならびにガイドブック策定にあたり執筆に協力いただける企業を募集いたしました。

ドキュメントの構成
本書は次に示す主要な項目で構成されています。
「第 2 章　暗号化消去」ではデータ抹消における暗号化消去の技術解説と本書で述べる項目の全体像について記載しています。
「第 3 章～第 5 章」では、製品分類に従い、それぞれの分類における暗号化消去の実行と運用方法を記載しています。

付録 A では、本書を作成するにあたり必要となった用語の用語集を掲載しています。

第 2 章　暗号化消去（CE:　Cryptographic Erase）

暗号化消去（CE）について NISTSP800-88Rev.1 では以下のように記載しています。

・CE は、データがメディアに書き込まれるときに、最初の書き込みから暗号化が実行される場合に使うことができる抹消手法であり、データの抹消は、書き込まれたデータの上書き又は物理的な抹消ではなく、データの暗号化に使用される暗号鍵を抹消することによって行われます。

・CE は非常に高速にデータの抹消を実現することができ、部分的な抹消、例えば記録メディアの限定された一部の領域に対するデータの抹消にも利用することができます。部分的な抹消は、選択的抹消とも呼ばれ、クラウド等に用いられる大型サーバーシステム、スマートフォンやタブレット型端末などのモバイルデバイスに対しても有効なデータ抹消の方法です。

日本国内においては、下記の様に 2020 年から急速に暗号化消去が、クラウドを対象とした各種基準やガイドラインに採用されるようになりました。

１．クラウドシステムにおける暗号化消去

クラウドシステムに対しては、国内に於いても米国の FISMA（Federal Information Security Modernization Act：連邦情報セキュリティ近代化法　注：2014 年の改正により、Federal Information Security Management Act：連邦情報セキュリティ管理法から変更）に基づいて標準化されたクラウドソリューションの導入を目的に設立された、FedRAMP（Federal Risk and Authorization Management Program：米国連邦リスク承認管理プログラム）と、管理基準である SP800-53Rev.5 を参考に、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和 2 年 1 月 30 日サイバーセキュリティ戦略本部決定）に基づき、内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省が運営している ISMAP（Information system Security Management and Assessment Program：政府情報システムのためのセキュリティ評価制度）が存在し、その管理基準において、

【1.3.14 消去(もしくは抹消)】

消去には、メディアを物理的に破壊する物理的消去、メディアを消磁装置により抹消する電磁的消去に加え、論理的消去も含む。論理的消去とは、元のデータを暗号化した後、暗号鍵を消去し、元のデータの復号を不可能にする方法を指す。

【1.3.15 暗号】

暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された電子政府推奨暗号、又はそれと同等以上の安全性を有する暗号を指す。

と、明確な記載が行われ、それに引き続き NISC（National center of Incident readiness and Strategy for Cybersecurity：内閣サイバーセキュリティセンター）の「政府機関等のサイバーセキュリティ対策のための統一基準」（令和３年度版）においても、暗号化消去が以下の様に定義されました。

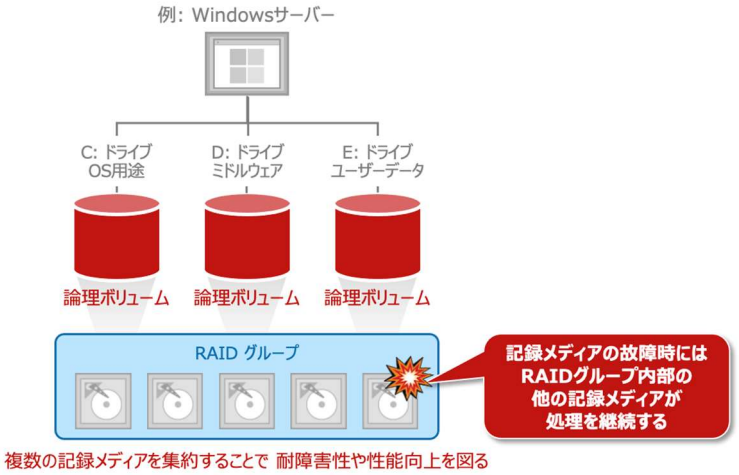
・「暗号化消去」とは、情報を電磁的記録メディアに暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる暗号鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。

・「情報の抹消」とは、電磁的記録メディアに記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録メディアを物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

これらは、2019 年の神奈川県に於ける HDD 流出事件に端を発した「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の改定」により、データの抹消方法の見直しが行われ、NIST SP800-88Rev.1 による「Purge（除去）」レベルの要求等が採用された影響が大きく、前述のようなクラウドシステムに於ける暗号化消去の優位性を認めたと結果とも言えます。

１）．クラウド等大型システムの構造（論理ボリュームと仮想ボリューム）

クラウドサービス等に使用される大型システムにおいては、従来から用いられている代表的な技術として RAID（Redundant Arrays of Inexpensive Disks）技術が存在し、複数の記録メディアを集約し、記録メディアの物理的な故障からデータを保護する機能を持たせていることが一般的となっています。この集約された複数の記録メディアを RAID グループと呼び、この RAID グループから、データの格納先となる論理ボリュームを、下図のように用途に応じた複数の区画（パーティション）として分割し、個別の論理ボリュームとして設定します。この論理ボリュームは、OS からは個別の記録メディア（ドライブ）として認識されます。

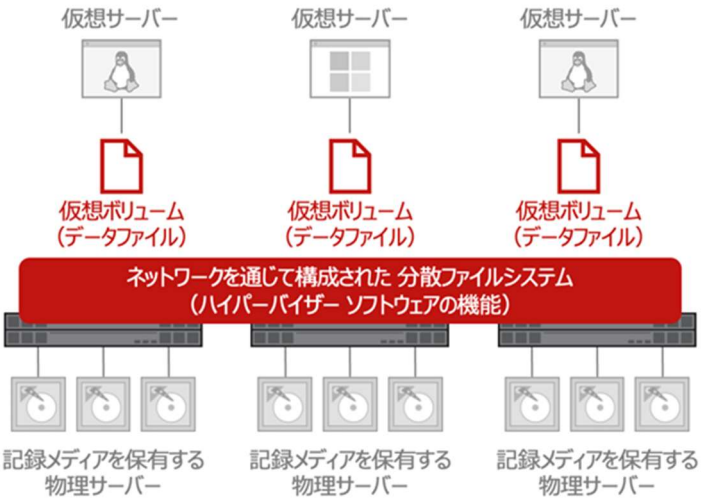


・仮想ボリュームとは

サーバー ハードウェアの性能向上に伴い、近年では 1 台の物理的なサーバーを、ソフトウェア（ハイパーバイザー）により仮想的に複数のサーバーに分割して利用することが一般的になりました。（仮想サーバー環境）

仮想サーバー環境においては、データの格納先である記録メディアも、ハイパーバイザーソフトウェアにより仮想的なオブジェクトとして扱われ、これを仮想ボリュームと呼びます。

仮想ボリュームの構成は、ハイパーバイザーの種類により異なりますが、一般化された技術概念としては、次ページの図の様に、仮想ボリュームはハイパーバイザーが認識するネットワーク上の分散ファイルシステムの上に構成された「個別のデータファイル」であるため、ボリュームの数や容量を必要に応じて増減可能である等、自由度が高いことが特徴ですが、データファイルであるため、占有するメディア内の物理的位置（LBA）が流動的であることや、フラグメント（断片化）の発生や、ファイルスラック領域（ファイルの終端とクラスタの終端の間の余剰領域）を持つ等の特徴も併せ持つことになります。



２）. 記録メディアに対するデータ抹消

ハードウェア機材の保守や廃棄などを目的に、個別の記録メディアに含まれるデータを「Purge パージ(除去)」レベルで抹消するためには、「RAID グループや分散ファイルシステムから該当する記録メディアを外す」、或いは、「RAID グループや分散ファイルシステムの構成自体を解体する」ことを行い、各記録メディアに対して目的に合致したデータ抹消処理を行うことが必要となります。

３）. 論理ボリュームと仮想ボリュームに対するデータ抹消

ソフトウェアにより構成されている個々の論理ボリューム及び仮想ボリュームは、多数の記録メディアに分散された構成となっているので、個々の論理ボリュームや仮想ボリュームを対象としたデータ抹消方法では、SSD や最近の大容量 HDD に採用されている SMR（Shingled Magnetic Recording：瓦記録）における、LBA を持たない、SSD ではオーバ・プロビジョニング等と呼ばれる専用のデータキャッシュ（スプール）領域や、再割り当て済みセクタ等の、OS から認識できない領域にデータが残存する可能性があり、「Purge（除去)」レベルの結果を得ることは出来ません。

しかし、論理ボリュームや仮想ボリュームに記録されるデータ全てに対して事前に暗号化する設定を行い、論理ボリュームや仮想ボリュームが不要となった時点で暗号鍵を廃棄する方法を採用すると、記録メディア上のあらゆる領域に残存する断片化したデータも暗号化されている上に復号に必要な暗号鍵が存在しないので、「Purge パージ(除去)」となります。また、システム上の動作が「暗号鍵」の抹消のみであるため、同一物理サーバー上に存在する他の論理ボリュームや仮想ボリュームの動作に一切の影響を与えることなく実行可能であるという利便性も併せ持っていますので、必要に応じて管理単位でボリュームの細分を行う等により、機密性の向上を図るなどの運用を容易に行うことが可能です。

２．モバイルデバイスにおける暗号化消去

一般的にモバイルデバイスにおいては、小型化を目的に eMMC 等の記録メディアが使用され基板に直接固定されている場合や、HDD や SSD を使用している場合に於いてもメディアの交換（脱着）の作業性が無視されていて、記録メディアに対して直接データ抹消を行う事が困難であることが多く、「Purge パージ(除去)」の結果を得ることは容易では有りません。しかし、このような場合における解決方法として NIST SP8000-88Rev.1 では、iOS（iPad　OS を含む）デバイスでは工場出荷時から暗号化機能が有効に設定されていて、解除も出来ないので、利用者が「工場出荷時状態にリセットする」だけで「Purge（除去）」レベルの結果が得られることを公表しています。

注意：Android デバイスにおいては、機器の製造元や通信キャリアに依存する仕様により、必ずしも初期状態で暗号化が有効に設定されているとは限らず、また利用者により暗号化の設定が解除可能な場合も存在するため、iOS と同様に「工場出荷状態にリセットする」だけで「Purge（除去）」レベルの結果が得られるとすることはできません。

３．CE をデータ抹消方法として有効に利用するための条件

１）．暗号化技術に対する要件

・暗号化技術を利用した情報セキュリティ製品やシステムの安全性を確保するためには、暗号アルゴリズム（暗号化をするための手順）及び暗号鍵などの重要情報の保護機能がハードウェア、ソフトウェア等で適切に実現されていることが客観的に検査された FIPS 140-2/-3 認証暗号モジュールの採用等によって安全性の確保が行われていることが重要です。

参考：NIST と CSEC（Communications Security Establishment Canada：カナダ通信保安局）は 1995 年から CMVP（Cryptographic Module Validation Program：暗号モジュール認証プログラム)の共同取り組みを行い、暗号モジュールのセキュリティ要件標準(FIPS 140) および関連する SP 文書に従って、米国政府標準暗号及び暗号鍵などの重要情報の保護機能が適切に実現されていることを客観的な試験によって認証しています。

日本では、CMVP とほぼ同じスキームで、IPA が JCMVP（Japan Cryptographic Module Validation Program：日本版暗号モジュール認証プログラム)を 2007 年から運用しています。CMVP との大きな違いは、電子政府推奨暗号リスト等に掲載されている暗号アルゴリズムを主な対象にしている点です。

FIPS 140 は、140-1（1994 年 1 月 11 日発行)、140-2（2001 年 5 月 25 日発行)、最新版は 140-3 (2019 年 3 月 22 日発行)となっています。これに伴い、FIPS140-3 認証への移行計画が進行しており、FIPS140-2 の認証申請受付は 2021 年 9 月 22 日に終了、現在は FIPS140-3 の認証申請受付になっています。また、FIPS140-2 認証の有効期限についても、認証取得後原則 5 年となっていますが、最長でも 2026 年 9 月 21 日までに制限されます。

２）. CE を必要とするすべてのデータはメディアに書き込む前に暗号化する。
例：Windows10 以降に付属している BitLocker では、使用途中で暗号化を有効にした場合、OS にファイルとして認識されるデータは暗号化されますが、過去に削除され再使用されていないセクタに残るファイルの残骸や、ファイルスラック領域（削除されたファイルの占有していたクラスタが、それよりサイズの小さいファイルで上書きされた場合に、クラスタ内に元データが上書きされずに残る部分）は、データとして認識されず平文で残存し、一般市販されているデータ復旧ソフトでもファイルの断片として読み出すことが可能であるため、データ消去の最低条件である「Clear」に該当しません。

３）. 暗号鍵が格納されているメディア上の場所が判明しており、適切なメディア固有のデータ抹消手法を使用してその領域を抹消することが可能なこと。

４）. CE を実行するための、機器に依存するコマンドを確実に使用することが可能なこと。

４．ソフトウェアによる暗号化消去の利用に対する留意点
１）. 紛失したモバイルデバイスの迅速なリモートワイプの実行などを目的とする場合、CE を使用することが適切かつ有効ですが、暗号鍵が機器の外部に格納される場合（バックアップまたは外部預託）は、復号のために将来その暗号鍵が使用される可能性があるため、「Purge パージ(除去)」には相当しません。ソフトウェアによる暗号化消去ソリューションは、信頼できる暗号鍵の保護と管理の上で成り立ちます。

５．自己暗号化ドライブ：記録メディアからの情報漏洩防止対策（以下、SED）
　最も技術レイヤーの低い場所における根本対策、且つ、最も平易な対策として、記録メディア自体が保有するデータ暗号化機能を利用する「自己暗号化ドライブ」があります。暗号鍵が格納されているメディア上の場所に対し、機器側システムからの直結アクセスが可能とされていること、メディアが起動時に使用するファームウェア等の関連データの保存されているシステム領域などの明確に識別された領域を除いた、ユーザー領域として LBA の付与された領域に書き込まれるデータのすべてが暗号化されていることです。

第 3 章　モバイルデバイス（パソコン、タブレット、スマートフォン）のデータ消去

iOS 端末（iPhone / iPad）

Apple 社製の iPhone 及び iPad においては、ハードウェア暗号化が動作するように初期状態で設定されているため、端末上の機能を利用したオールリセット（全ての設定の初期化）を行うことで、端末を使用するうえで書き込まれた情報の暗号化消去によるデータ抹消が完了します。

データ抹消のランクと方式

1）「Clear クリア(消去)」、「Purge パージ(除去)」

本体上で、設定>一般>リセット>「すべてのコンテンツと設定を消去」を実行する。

2）「Destroy デストロイ(破壊)」

細断、解砕、粉砕、または焼却炉で機器を焼却する。

注意：データ抹消操作の後、マニュアル操作にて、端末の複数の領域（ブラウザの履歴、ファイル、写真など）に移動して、操作が間違いなく実行され、情報が保持されていないことを確認してください。

Android 端末

Android 端末は、原則として Android 6.0 以降が標準搭載された機種ではハードウェア暗号化が動作するように初期状態で設定されているため、iOS 端末同様に端末上の機能を利用したオールリセット（全ての設定の初期化）を行うことで、端末を使用するうえで書き込まれた情報の暗号化消去によるデータ抹消が完了します。

ただし、Android OS の機器は OS のバージョンだけでなく、機器の製造元や通信キャリアに依存する仕様により、初期状態では「暗号化しない」設定となっている場合もあるため、設定の確認は必須です。暗号化されていない機器での初期化ではデータは消去されますが、ストレージ内に復元できる状態で残存する可能性があるためデータ抹消が完了するわけではないことに注意してください。

暗号化の設定の確認

本体上で、設定>セキュリティ>暗号化と認証情報

スマートフォンの暗号化の項目で「暗号化されています」と表示されることを確認します。暗号化されていない機器等ではこの項目で暗号化を実行することが可能です。

データ抹消のランクと方式

1）「Clear クリア(消去)」、「Purge パージ(除去)」

暗号化が有効となっていることを確認し、スマートフォンを出荷時の設定にリセットし

ます。通常は設定アプリからリセットの実行が可能ですが、前述の通り機器の製造元やキャリアに依存する仕様により、出荷時の設定へのリセットの方法の詳細は端末の製造元、または通信キャリアのサポートサイトなどで確認してください。

２）「Destroy デストロイ(破壊)」

細断、解砕、粉砕、または焼却炉で機器を焼却する。

・SD カード等の外部ストレージの暗号化

Android 端末の多くでは SD カードなどの外部ストレージを利用することが可能となっています。このため Android 端末本体内部のストレージだけではなく、外部 SD カードの暗号化も設定することも肝心です。なお、暗号化された外部 SD カードは暗号化に利用したデバイスのみで利用が可能で、端末を出荷時の状態にリセットすると SD カードも暗号化消去された状態となり、リセット前に暗号化された SD カードの読出しはできなくなります。

・Microsoft Windows 端末（タブレット、パソコン）

Windows 端末のデバイスの暗号化は Windows OS に搭載された暗号化機能「BitLocker」によりサポート対象デバイスで利用できます。 SSD の Trim 機能にも対応しています。
Trusted Platform Module(TPM)が搭載された端末では TPM を用いた暗号化が行われます。
暗号化アルゴリズムは FIPS 準拠の XTS-AES128 ビット方式が利用され、USB など外部ストレージドライブでは AES-CBC 128 ビット方式が用いられます。
ただし、BitLocker によるデバイス暗号化は Windows の OS エディションや利用するハードウェアによっては利用できない可能性もあるため、デバイスの暗号化が可能かどうかは事前に確認が必要です。

・デバイスの暗号化を利用できるかどうかを確認する方法

タスク バーの検索ボックスに「システム情報」と入力し、結果の一覧の [システム情報] を右クリックして、[管理者として実行] を選択します。 または、[スタート] ボタンを選択し、[Windows 管理ツール] で [システム情報] を選択することもできます。
[システム情報] ウィンドウの下部で、[デバイス暗号化のサポート] を見つけます。 この値が "前提条件を満たしています" になっていれば、お使いのデバイスでデバイスの暗号化を利用できます。

・デバイスの暗号化を有効化する方法

管理者権限を有するアカウントで Windows にサインインし、[スタート] ボタンを選択し、[設定] > [更新とセキュリティ] > [デバイスの暗号化] の順に選択します。 [デバイスの暗号化] が表示されない場合は、利用できません。

デバイスの暗号化がオフになっている場合は、[オンにする] を選択します。

前述の方法でデバイスの暗号化が利用できない端末の場合にも、以下の方法で BitLocker を有効化することが可能な場合があります。

管理者権限を有するアカウントで Windows デバイスにサインインし、タスク バーの検索ボックスに「BitLocker の管理」と入力し、結果の一覧から選択します。 または、[スタート] ボタンを選択し、[Windows システム] で、[コントロール パネル] を選択することもできます。[コントロール パネル] で、[システムとセキュリティ] を選択し、[BitLocker ドライブ暗号化] で [BitLocker の管理] を選択します。

[BitLocker を有効にする] を選択し、画面に表示される指示に従って操作します。

・データ抹消のランクと方式

1）「Clear クリア(消去)」、「Purge パージ(除去)」

Windows 10 では PC のリセット機能が搭載されています。リセット機能ではデータを「すべて削除する」モードで、すべての「データ消去」と「データドライブ」の削除を実施することでデータの復元を困難にするクリーニングオプションが搭載されています。

BitLocker のドライブ暗号化でデータドライブが全体に暗号化されている場合には、暗号鍵（回復キー）の廃棄と合わせることで、より一層復号が困難な暗号化消去となります。

[設定]アプリから「更新とセキュリティ」→「回復」→「この PC を初期状態に戻す」で「開始」をクリックし「すべて削除する」オプションを選択。

設定の選択画面にて[データ消去][データドライブ]をともに「オン」にして[確認]をクリック

2）「Destroy デストロイ(破壊)」

細断、解砕、粉砕、または焼却炉で機器を焼却する。

Apple Mac 端末（タブレット、パソコン）

Apple 社製の Mac 端末でディスク全体を暗号化するためには OS X Lion 以降の MacOS で利用可能な「FileVault 2」を利用します。「FileVault 2」の暗号化アルゴリズムは FIPS 準拠の XTS-AES128 ビットが採用されています。

FileVault 2 を有効化し設定する方法

Apple メニュー ＞「システム環境設定」の順に選択し、「セキュリティとプライバシー」をクリックします。

「FileVault」タブをクリックします。

南京錠のアイコン をクリックして、管理者の名前とパスワードを入力します。

「FileVault をオンにする」をクリックします。

データ抹消のランクと方式

1）「Clear クリア(消去)」、「Purge パージ(除去)」

Apple のサポートページにおいては、OS X Lion v10.7 以降および SSD ドライブ搭載の Mac では FileVault 暗号化を有効にしたうえで、標準的な消去を行えば SSD からデータを復元することは困難になると推奨手順が記載されており[1]、Mac を工場出荷時の設定に復元する一番の方法は、ハードドライブを消去して macOS を再インストールすること[2]であると推奨されています。

消去方法はご利用機種により異なりますので、アップル社のサポートページで確認し[3]、ディスクユーティリティから「ボリューム」および「ボリュームグループ」を消去してください。

2）「Destroy デストロイ(破壊)」

細断、解砕、粉砕、または焼却炉で機器を焼却する。

Linux OS Mac 端末

Linux 環境における暗号化と暗号化消去を実施する場合、OS のディストリビューション等によっても推奨方法が異なる可能性があります。このため利用している OS で推奨される方法を確認してください。

たとえば、Linux Unified Key Setup（LUKS）などのディスク暗号化ソリューションを用いて Cryptsetup にてディスク全体を暗号化する手法などがあります。Cryptsetup は暗号化ディスクを作成・管理するデバイスマッパーである dm-crypt を使うためのコマンドラインツールです。dm-crypt は FIPS 準拠の XTS-AES128 ビットなどのアルゴリズムをサポートしています。

データ抹消のランクと方式

1）「Clear　クリア(消去)」、「Purge パージ(除去)」

Windows OS 端末や Mac OS 端末と同様にディスク全体を暗号化している場合、ボリュームの削除やフォーマット等により復号が困難な状態にするデータ抹消が可能となります。

---

[1] *https://support.apple.com/ja-jp/HT201857*

[2] *ハードウェアの修理時に部外秘データを保護する https://support.apple.com/ja-jp/HT201857*

[3] *Apple シリコン搭載の Mac を消去する方法　https://support.apple.com/ja-jp/HT212030*

２）「Destroy デストロイ(破壊)」
細断、解砕、粉砕、または焼却炉で機器を焼却する。

デバイス暗号化を利用できないモバイルデバイスのデータ抹消
現在では OS 種別にかかわらず、多くの端末がデバイス暗号化に対応している状況であるため、理想的にはデバイス暗号化に対応した端末を選択し、暗号化消去による「Clear(消去)」、「Purge(除去)」を選択することが望ましい姿です。
しかし、やむを得ずデバイス暗号化に対応していない古い端末や OS を利用している場合には「Destroy(破壊)」（焼却炉で機器を焼いて細断、解砕、粉砕、または焼却する）を実施するか、または OS 等の種別に応じて以下の策を実行してください。

デバイス暗号化非対応の Android 端末
Android 端末に対するデータ抹消について、NIST SP 800-88 Rev.1 では製造元やキャリアに各端末の詳細な仕様について確認し、最も有効なデータ抹消の方法を選択することを求めており、NIST が対象としている米国の官公庁においては、情報の所有者・管理者である個別の官公庁が、NIST の指導に従って選択した手段を用いることが最適であるとされています。しかしながら、これと同等の作業を、日本国内の組織における標準的なデータ抹消の方法と規定することには無理があるため、ADEC では Android 端末に使用されている記憶媒体が eMMC であることも踏まえ、同様の機能を持ち、同様に NAND 型フラッシュメモリーを使用している MMC や SSD に対応するデータ抹消手法を採用することが適当であると考えます。

※eMMC とは、embedded MMC の略で、MMC のコンポーネントを BGA パッケージに入れ、電子回路基板に直接実装して用いるものです。

１）「Clear クリア(消去)」、（NIST SP 800-88 Rev1. による MMC に対する記述）
組織的に承認され、その有効性が確認されている上書き技術/方法/ツールを使って媒体を複数回上書きする。

注意：データ抹消操作の後、マニュアル操作にて、端末の複数の領域（ブラウザの履歴、ファイル、写真など）に移動して、操作が間違いなく実行され、情報が保持されていないことを確認してください。
※この方法（複数回の上書き）は、ADEC における SSD を対象としたデータ抹消ソフトウェアの消去動作検証を目的とした検体の作成時に、LBA の付与されていない余剰領域（オーバプロビジョニング）上に消去検証用のダミーデータを書き込む際に用いることでも有効性が確認

されています。それにも関わらず Purge として認めない理由は、スマートフォンやタブレット型機器の場合、上書きの対象が eMMC 全体であるか、一部に留まっているかについては、データ抹消の対象となる機器の仕様に依存していることによります。

デバイス暗号化非対応の Windows 端末、Macintosh 端末、Linux 端末

デバイス暗号化非対応の Windows および Mac OS、Linux OS 等の端末に対するデータ抹消については、搭載されたストレージが HDD または SSD であるため、端末が採用しているディスクストレージの種別に応じたデータ抹消方法に関するデータ消去技術 ガイドブックを参照してください。

これまでのデータ抹消は端末の利用終了時や廃棄時などのタイミングにフォーカスが当たっていました。しかしながら、テレワークの拡大などモバイルデバイスを外部に持ち出して利用する機会が増加したこと、自宅や外出先等からスマートフォンやタブレットで Web 会議に参加する可能性が増えたことなどから、端末の紛失・盗難や、退職時の業務データの抹消など、これまでとは異なる意図しない外部流出を防ぐための施策がセキュリティ管理者に求められるようになっています。

暗号化したデバイスの利用における注意事項

暗号化されたディスクの情報を復号するためには必ず立ち上げ時に利用者認証が行われることが必要です。

このため、必ず立ち上げ時にはセキュリティロックがかかっている状態となるように端末を設定し、一定時間端末の利用がない場合にも自動的にロックがかかるようにしなくてはなりません。

ロックの解除は単純な文字列（パスワードや PIN）やパターンによるものでなく、可能な限り指紋認証や顔認証などの生体認証を利用した利用者認証とするなど、利用者が正当であることを確保できる手法を選択すべきです。これは端末の選択時点から考慮が必要になります。このことで紛失や盗難の際にデータが利用できない状態を担保し、データの漏洩が発生する前にリモートワイプ（遠隔消去）を実行できるようにします。

ディスク暗号化による速度等パフォーマンスへの影響について

ディスク全体を暗号化することによりパフォーマンスが低下するのではないかと懸念があります。かつてはディスクの読み書きスピードや CPU の処理能力の問題からパフォーマンスの著しい低下が発生していたことも事実です。ただ、現在では SSD の普及による読み書きスピードの向上や、主要な CPU には暗号化および復号の高速化を行うための機能が搭載されていることなどから、ディスク暗号化がコンピューターの動作に与える影響は軽微なものとなっています。CPU の暗号化の高速化機能としては AES-NI（Advanced

Encryption Standard New Instructions）などが存在し、インテル製や AMD 製の CPU に搭載され、Windows の BitLocker や Mac OS の FileVault 2、Linux の dm-crypt 暗号化にも対応しています。

このように暗号化によるパフォーマンス低下が軽減されたことから、パフォーマンス低下の影響よりも、データ漏洩リスクの軽減効果が上回ることからモバイルデバイスではディスクの暗号化が標準的な対策となっています。

また、パフォーマンス低下の要因としては日々、端末を利用する利用者の負荷の上昇や、管理者の設定管理の負荷が高まることも考えらます。利用者においては、標準的に設定がなされることで、暗号化・復号を意識させない利用形態とすることで負荷の軽減を図ることができます。このような状態とするための管理者用ツールも普及していますので次にご紹介します。

暗号化消去を有効に活用するために（端末管理、遠隔消去等）

モバイルデバイスには、iOS / Android などのスマートフォンタブレット端末のほか、Windows / Mac OS / Linux などのモバイルデバイスなど様々な端末種別や OS を考慮に入れることも重要であり、数多くの端末を管理者が 1 台 1 台すべてに適正な状態であるのかを常に人の手で監視・制御するのは現実的ではありません。

このため、管理者側で機器の廃棄、紛失、盗難、利用者の退職等、様々なライフサイクルの中で、正しくデータの抹消を管理するためには、業務データにアクセスする端末は、自動で一括してすべての端末のストレージ暗号化を行うなど、定められたポリシーを強制する制御や、常にその状態が保たれていることが保証されるよう管理することが重要なポイントとなります。

このような管理者側の管理・制御が実施されることで、紛失や盗難、退職者への対応においてもリモートワイプや自動的な初期化等の措置でデータ抹消を簡易に、かつ、適切に実施することが可能となります。

このような管理を自動化するためのソリューションは統合エンドポイント管理（Unified Endpoint Management=UEM）製品と呼ばれています。モバイルデバイス　のデータ管理やデータ抹消を適正に実施するために必要なツールとして検討することが暗号化消去を活用し、データ流出事故等を防ぐポイントになろうかと思います。

主な UEM ソリューション製品

デバイスの構成や管理（MDM）、データ保護などを統合的に実行する統合エンドポイント管理（UEM）ソリューションとして Gartner 社が毎年発表している Magic Quadrant の統合エンドポイント管理（UEM）の 2021 年のレポートにおいて実行能力の面で最も高い評価を得ている企業の製品が選出されています。

これらの製品には端末管理（MDM）の仕組みやアンチマルウェアの仕組み、ログ管理機能も備わっているため、端末管理や利用者のログイン履歴、ファイルアクセス履歴、さらには暗号化消去が行われた履歴も監査ログとして取得できることが多いため、消去が確実に行われたかどうかの自己証明や監査証明を行うことも可能となります。
推奨された暗号化の方法でデバイスやストレージが自動的に暗号化している状態に設定し、適切な消去レベルでのデータ抹消が実行されたことも簡易に証明できることで運用負荷を大幅に軽減しつつ、情報漏洩リスクを軽減することが可能になります。

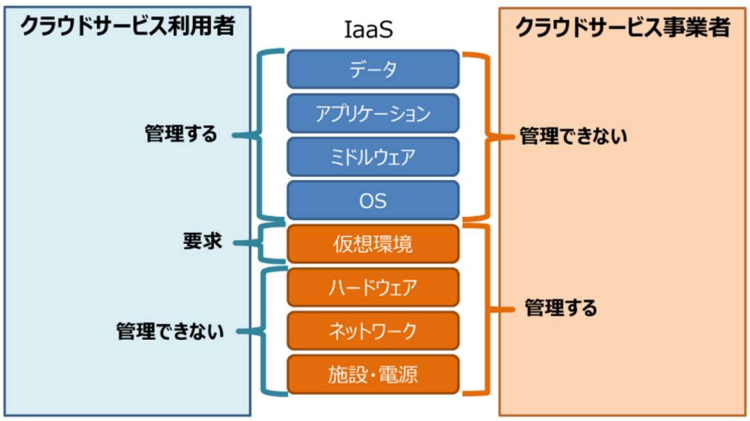
第 4 章　IaaS クラウドの仮想マシンにおけるディスクの暗号化と消去について

本ガイドブックでは、一般に IaaS と呼ばれるクラウドサービスにおけるディスクの暗号化と消去について、情報システムのオーナーないし管理者向けに概略を説明します。ここで扱う IaaS とは主に、事業者が物理マシン上に仮想マシンを稼働させ、インターネットを介してこの仮想マシンをサーバーとして利用させる形のクラウドサービスを指します。また、データの暗号化とは本ガイドブックの主旨に合わせ、仮想マシンのディスクに対する暗号化についてのみ説明を行い、オブジェクトストレージや共有ストレージ、各種データストアの暗号化については取り扱いません。

IaaS における「利用者」と「事業者」

総務省による「クラウドサービス提供における情報セキュリティガイドライン(第 3 版)」では、IaaS の構成要素と、利用者および事業者が各要素の管理責任をどのように分担するかについて、次のように説明しています。

Ⅰ．6．3．IaaS における管理と責任共有



IaaS を利用するクラウドサービス利用者は、クラウドサービス事業者との契約・SLA に基づき、ゲスト OS[8]等が動作するための仮想環境の構築と管理をクラウドサービス事業者に要求できる。クラウドサービス利用者は、仮想環境上で動作している OS を含めたすべてのソフトウェアの管理を行う。OS やミドルウェア層での障害対応や、ミドルウェアに対するパッチ適応やぜい弱性対応などは、クラウドサービス利用者の責任となる。

クラウドサービス事業者は、仮想環境層以下の実装、設定、更新及び運用を管理するとともに、データセンター内のネットワークインフラも管理する。

一般に、情報システムのオーナーや管理者は、システムのセキュリティを高めるための様々な措置を取る必要があります。システムが機密情報を扱う場合には情報が漏洩するリスクを可能な限り減らすために、より一層の対策を講じなければなりません。記録媒体から機密情報を読み取れないようにするディスクの暗号化とその消去もそのひとつであり、本ガイドブックでは、その具体的な手法について解説をしていますが、システムのオーナーや管理者が記録媒体のハードウェアなど比較的低いレイヤーに対して容易にアクセスできることを前提にしています。

2000 年代以降、IaaS をシステムのサーバー基盤として用いることが一般化しました。システムのオーナーや管理者は上図における「クラウドサービス利用者」の立場となり、システムの物理的側面から解放される一方で、仮想環境より下のレイヤーへアクセスすることが困難になりました。例えば機密情報を格納した HDD が故障した際、新品の HDD に交換した上で故障したものを破砕するといった措置をシステムのオーナーや管理者が自分自身で行うことが出来ません。そのようなオペレーションは基本的に IaaS 事業者が自律的に実施するためです。

システムを IaaS 上で構築・運用する場合でもセキュリティについてオーナーや管理者が負うべき責任はそうでない場合と変わりません。自社の機密情報や顧客の個人情報といった情報をサーバーから漏洩させないために、IaaS ではディスクの暗号化とその消去を行う機能が提供されています。以下では、オーナーや管理者が IaaS の利用者の立場となった際に押さえておくべき基礎的な内容について説明します。

IaaS におけるデータ暗号化の概略

IaaS では、事業者がインターネットに接続された仮想マシンを運用・提供します。利用者は事業者と契約を結び、契約の続く限り仮想マシンを専有することが出来ます。IaaS の事業者は膨大な数の仮想マシンを提供する大きなシステムを所有・運用しており、利用者が専有するのはその一部分にすぎません。利用者はいわば、大きなビルの一角を賃貸契約している店子(テナント)のようなものであり、一方で事業者はビルを所有し、各区画をテナントに貸し出すオーナーにあたります。

IaaSは大きなオフィスビルのようなもの

- 利用者はテナントとして、契約に基づきビルの一部を専有する
  → IaaSでも: 契約に基づき大きなシステムの一部を専有する
- 他のテナントと同じ建物や設備を共同で利用する
  → IaaSでも: 他の利用者と同じシステムを共同で利用する
- セキュリティは設備や警備としてビルから提供される
  - エントランスゲートや監視カメラ、警備体制等

  → IaaSでも: 事業者によってセキュリティが確保される
- 可能な範囲で自前のセキュリティ対策を敷くことも出来る
  - 例: テナントの出入口に独自のカードキーゲートを設置

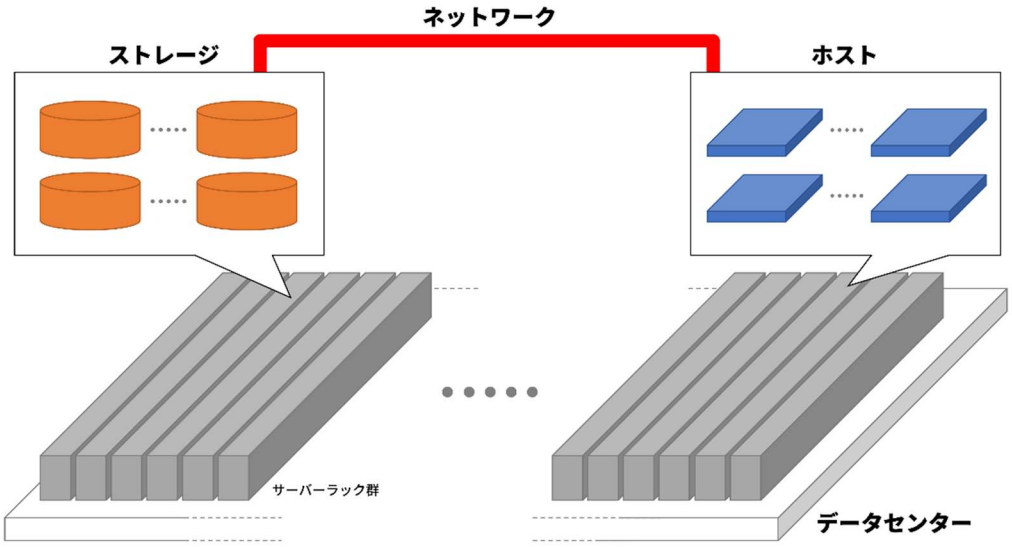
  → IaaSでも: 暗号化用の鍵などを自前で用意することが出来る
- ビルの仕組みだけで絶対安全ではない
  - 例: ビルやテナントに入る鍵や暗証番号を盗まれては意味がない

  → IaaSでも: 利用者はパスワード等の管理を徹底する必要がある

利用者は IaaS という大きなビルを他の不特定多数の誰かと共同で利用することにより、単独では実現出来ないメリットを享受することが出来ます。データの暗号化と消去についても、利用者が自前のシステムでセットアップするよりも容易に、かつ確実に行う仕組みが提供されています。

IaaS の仕組み

暗号化について説明する前に、IaaS のシステム基盤について概略を説明します（以下の内容は特定の IaaS サービスの構成を説明するものではありません）。



データセンター

IaaS のシステムが存在する物理的な施設です。侵入者に対する高い水準の物理セキュリティを備えており、侵入者がデータに対して物理的にアクセスすることを防ぎます。また、データを含んだ状態の機材が不用意にデータセンター外へ持ち出されることを防ぐため、ディスクやストレージ装置といった機材の厳格な管理が行われています。また使用済ディスクを破壊する設備を備え、データを読み取れない状態にして初めてデータセンターの外へ運び出される場合もあります。

ホスト

ホスト上で実行されるハイパーバイザー上でシステムのオーナー/管理者が使用するサーバ(仮想マシン)が稼働します。ディスクの暗号化と復号が実行される場合があります。また、ハードウェア的なハッキング対策が施されている場合もあります。

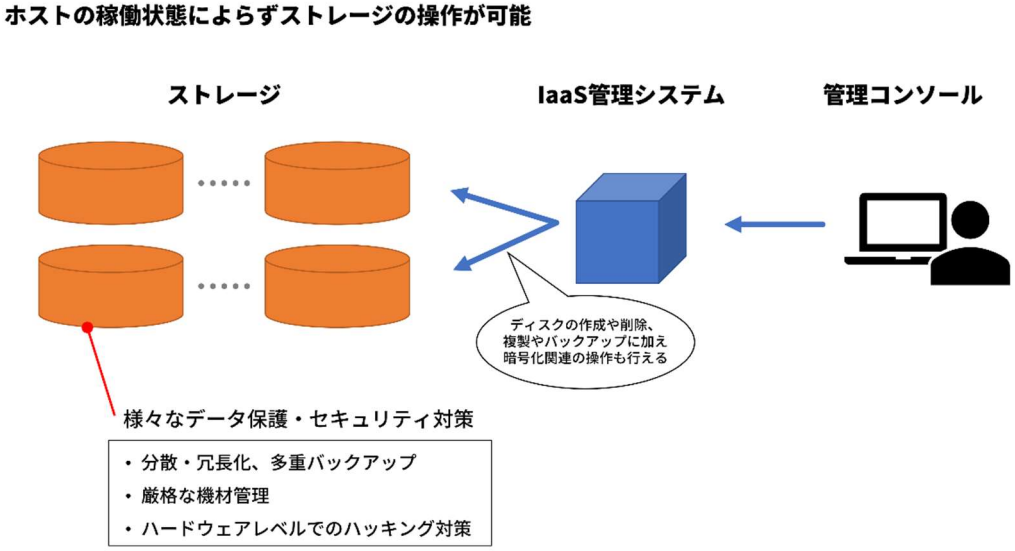
ネットワーク

ホストとストレージを接続し、仮想マシンはこれを介してディスクにアクセスします。物理マシンにおける、ローカルディスクのバスに相当する機能を果たすため、広帯域・低レイテンシである場合が一般的です。

ストレージ

ネットワークを介してホストと接続され、仮想マシンのディスクが実体として存在します。ディスクの暗号化と復号が実行される場合があります。ホスト同様、ハードウェア的なハッキング対策が施されている場合もあります。この中で重要なのが、ホストとストレージが物理的に分離されているという点です。ポイントは大きく 2 つあります。

第一に、ストレージがホストと分離されることによって収容効率や耐障害性が向上します。通常、ディスクボリュームは複数の物理ストレージ装置間で分散・冗長化されており、さらにストレージ装置内でも複数の物理ディスクに分散して保存されています。ひとつのディスクボリュームが、物理的に単一のディスクに格納されているといったことはありません。このことは、データセンターにおけるセキュリティおよび厳格な機材管理と合わせ、悪意のある第三者が IaaS のディスクに保存されたデータを読み取ることを難しくしています。



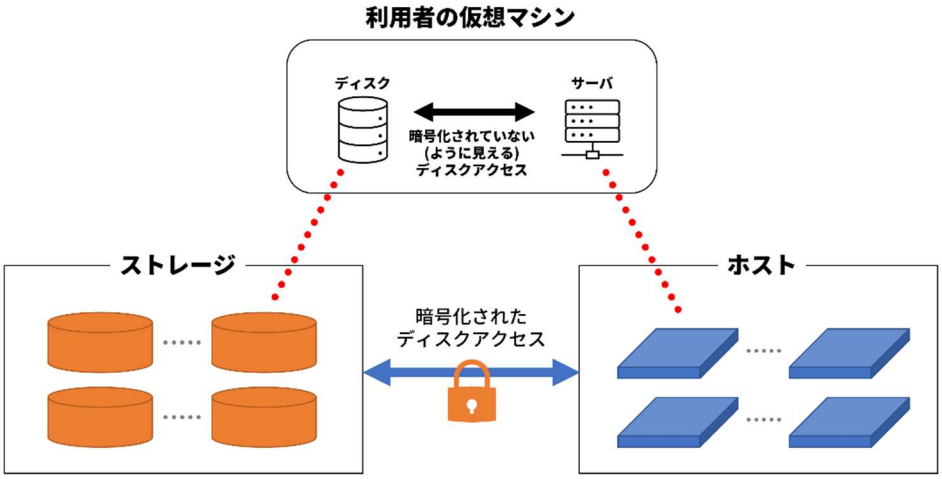
上記のように、IaaS のストレージ様々なセキュリティ対策が施されています。その上で更にディスクを暗号化することによって、データの保護をさらに堅牢にすることができます。

第二に、仮想マシンやホストの稼働状態によらず、ディスクボリュームに対する様々な操作が可能になる点です。管理コンソール上から同じ機能のサーバーを大量に運用するためにディスクを複製する、バックアップを取るなどの操作に加えて、ディスクの暗号化に関する操作も行うことが出来ます。

IaaS 上でのディスク暗号化は容易である

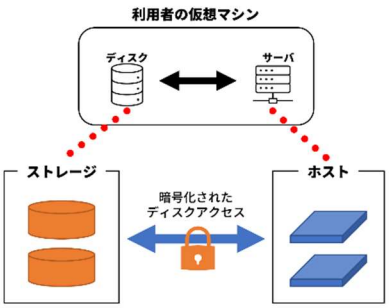
IaaS におけるディスク暗号化は透過的に行われることが一般的です。ディスクへの書き込み・読み出しに伴うデータの暗号化と復号は仮想マシンの外側で行われ、仮想マシン上の OS の中で特別な設定を行う必要はありません。この暗号化と復号は先に述べた通り、ホストあるいはストレージのいずれかで行われます。

ディスクの暗号化は透過的に行われる



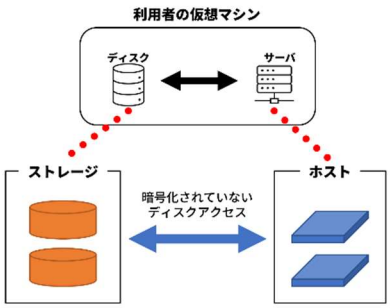
IaaS におけるディスクの暗号化は、IaaS によって、初めから全て自動的に暗号化されている場合と管理コンソールで利用者が作成するディスクを暗号化するよう設定を行う必要がある場合があります。前者の場合、ディスクを暗号化しないという選択肢はなく、その IaaS を利用することは即ち全てのディスクの暗号化を行うことを意味します。利用者は自身のディスクが暗号化されていることを意識することすらないかもしれません。

ディスクが暗号化されている場合



- IaaSによってはこの仕様がデフォルト
  (ディスクが新規作成時点で暗号化されている)
- 暗号化されていない状態に出来ない場合もある

ディスクが暗号化されていない場合



- IaaSによってはこの仕様がデフォルト
  (ディスクが新規作成時点では暗号化されていない)
- 非暗号化ディスクを事後的に暗号化することは可能
- ディスク暗号化をデフォルトの設定にすることも可能

ディスクを暗号化する、あるいは暗号化されたディスクからデータを読み出すためには「暗号鍵」が必要になります。通常この「暗号鍵」の管理は煩雑な作業ですが、これを IaaS

の仕組みに全て任せることで利用者は「暗号鍵」について全く意識することなくディスクを暗号化しデータを保護することが出来ます。一方で「暗号鍵」の管理を全て IaaS の仕組みに任せるのではなく、利用者が制御することも可能です。これについては後段で説明します。

ディスク暗号化のデメリットは少ない

ディスクの暗号化にデメリットはあるのでしょうか。現在、代表的な IaaS では、ディスクが暗号化されることによる性能上のペナルティは殆どないか、あってもごくわずかです。また、ディスクの暗号化は無料で可能となる場合が多く、コスト面での問題も存在しません。高速でありながら低コストにディスク暗号化を実現できる背景のひとつに、ハードウェアの進歩が挙げられます。Intel 社が 2010 年以降、自社 CPU に現在主流の暗号化方式 AES の処理を高速化する機能を組み込んだことで、高速な暗号化処理がコモディティとなりました。現在では Windows や Linux などの OS をはじめ、様々なソフトウェアがこの機能を用いて暗号化によるデータの保護を行っています。IaaS においても同様に恩恵に預かることができるのです。

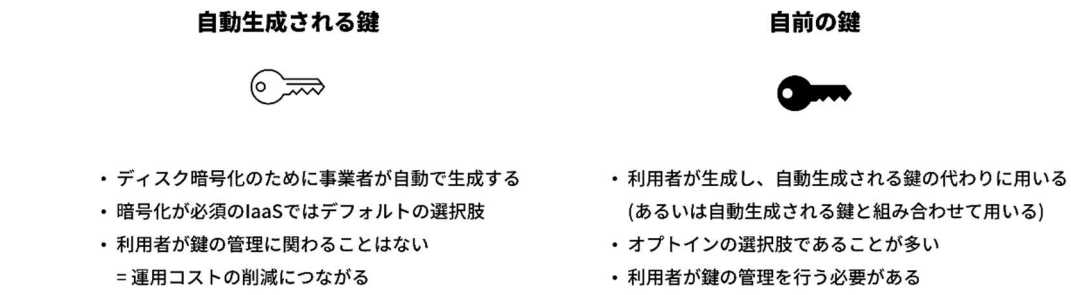
IaaS における暗号化と暗号鍵の管理

システムが利用者の手の届かない場所にある IaaS において、ディスクの暗号化はデータを保護する有効な手段です。利用者は IaaS 事業者が提供する仕組みの上で暗号化を行うことになりますが、そこで重要となるのが暗号化に用いる暗号鍵とその管理です。

暗号鍵管理の選択肢

先にも述べたように、代表的な IaaS では、事業者が用意した仕組みによって利用者は殆ど(あるいは全く)何もせずともディスクが暗号化されます。ディスクは IaaS の仕組みによって自動的に生成された暗号鍵によって暗号化され、ディスクが削除される際には自動的にこの暗号鍵が削除されることでデータの Purge（除去）が完了します。この場合に用いられる暗号鍵は事業者のみが扱うことができ、利用者が制御することは出来ません。この場合、暗号鍵の管理を事業者に預けることで運用の効率化を図ることができます。

一方で IaaS には、自前の暗号鍵を持ち込むことで、利用者が暗号鍵を管理できるようにする仕組みも備わっています。この場合、利用者は持ち込んだ暗号鍵を自らの責任で管理しなければなりません。仮に暗号鍵が第三者の手に渡ればデータが破壊・漏洩される恐れがあり、また暗号鍵を消失した際にはデータが復旧できなくなるなどのリスクを背負うことになるため、管理には細心の注意を払う必要があり、運用コストは増大します。しかしながら暗号鍵を自らが管理することで、データを管理する担当者や責任の所在を明確にし、また暗号鍵を手元で消去することで確実にデータを Purge（除去）したという確証を得られるというメリットがあります。



暗号鍵管理システム（Cryptographic Key Management System: CKMS）

暗号化の要である暗号鍵を適切に運用するために、主要な IaaS には暗号鍵管理システムが備わっています。本ガイドブックでは仮想マシンのディスクについてのみ扱っていますが、それ以外にも IaaS は多岐に渡る機能性を持ち、それぞれの特性に応じた暗号化や暗号鍵の管理を行うためのオプションが存在しています。暗号鍵管理システムでは、そうした暗号鍵や暗号化に関する各種の設定を主に Web 上の管理コンソールから行うことができます。

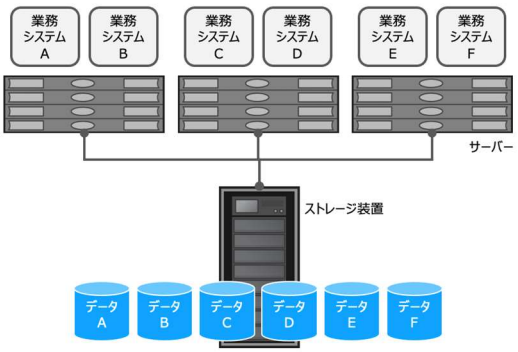
暗号化および暗号鍵の管理に関する概念や用語、各種仕様、暗号鍵管理システムの詳細は各 IaaS 事業者によって異なるため、利用者は自分が利用する IaaS のそれらについて把握する必要があります。詳しくは各 IaaS の技術ドキュメント等を参考にして下さい。

第 5 章　ストレージ装置におけるデータ暗号化の必要性と技術要素

ストレージ装置におけるデータ暗号化の必要性と技術要素

データセンターに設置される ストレージ装置は、多種多様なシステムのデータを集約し一元的に保存・管理する役目を担う装置です。そのため、ストレージ装置自身も格納されるデータを暗号化する機能を保持しています。ストレージ装置の利用者は、情報漏洩防止の観点からも、積極的にこれらの機能を活用することが望まれます。

ストレージ装置



データセンターでは、多数のサーバーが保持するデータを一元的に集約・保管するストレージ装置が利用される。
サーバー装置毎にデータを保持せず一括保管することで、バックアップの一括取得、サーバー故障時の迅速な切替、システム間でのデータの共有などを実現している。
ストレージ装置は、ストレージ サブ システムとも呼ばれ、システムの中で専用のネットワークを通じデータを管理するための様々なソフトウェアと組み合わされて運用される。

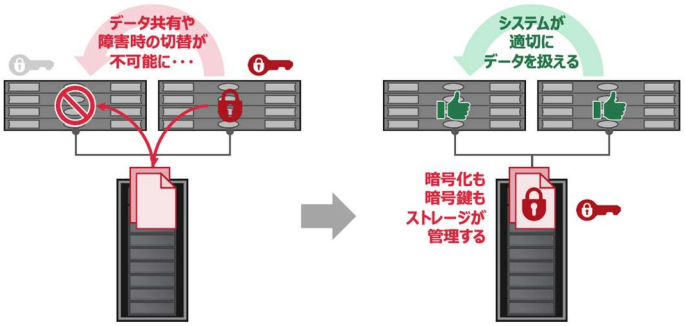
なぜストレージ装置のデータ暗号化機能が必要なのか、という点から始まり、ストレージ装置の暗号化機能で利用される技術に関して、分かり易く解説します。

共有データの暗号化に纏わる技術的な課題

データの暗号化が、なぜストレージ装置で必要なのでしょうか? 多くの暗号化ソフトウェアが存在している中で、利用者自身が データファイルを暗号化して保管する、という方法では不充分なのでしょうか?

データの暗号化に関連する話題において、よくある質問の一つです。ここではこの疑問に答える形で、ストレージ装置でのデータ暗号化の必要性について、考えて見たいと思います。最もシンプルな必要性の一つの例は、「サーバー システムの間で データを共有したり、引き継いだりする場合に、暗号化が妨げになるのを防止する」という点です。暗号化されたデータファイルをきちんと処理するためには、暗号鍵による復号処理が必要になります。そのため、この暗号鍵が適切に異なるサーバーでも利用できることが重要になります。しかしな

がら、サーバーが複数台存在する構成において、どのデータファイルを暗号化した暗号鍵をどのサーバーで利用することができるか、という点を常に適切に管理することは、技術的な困難さが伴います。その代わりに、データを一元的に扱うストレージ装置で一括して暗号化処理と暗号鍵の管理を行う方がより効率的であり、技術的にも理にかなった方式となります。

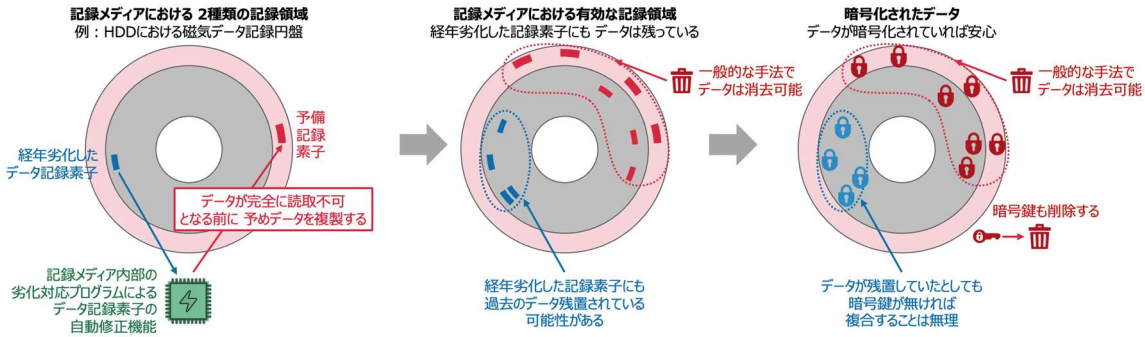


記録メディアからの情報漏洩防止への対応

ストレージ装置は、複数の多様なシステムのデータを一括保管しています。そのため、記録メディアが流出した際に備えて、予め情報漏洩を防ぐ措置が求められます。これには、本章で記載のある通り、データの消去・除去、また、記録メディア自体の物理的な破壊、が望まれる措置となります。

データを暗号化している場合には、以降で示すように、データを消去しなくても暗号鍵を消去することで、データの除去と同様の効果を得ることができます。

ストレージ装置で利用されている記録メディア（ハードディスクドライブ や フラッシュドライブなど）の多くは、下図で示すように、個々のデータ記録素子の経年劣化への対応として、予備記録領域を保持しています。記録素子が劣化によりデータの読取が難しくなった際に、完全にデータを読み取れなくなる前に、予備領域へデータを複製することで、利用者のデータを保護する機能が備わっています。一般的なデータの削除方法では、現在利用可能な記録素子を削除対象としており、これをデータ「消去」と呼びます。データが既に予備領域へ移され現在は利用されていない記録素子までを含めて、記録メディアからデータを削除することを「除去」と呼び、記録メディアに対するデータ削除対応として、最もレベルの高い削除方法となります。



しかしながら、データの「除去」を行うためには、記録メディア内部で自動修正機能により使われなくなった記録素子へのデータの上書きを行う必要があるため、特別なソフトウェア機能を利用して処理を行う必要があります。また、記録メディア自体も、このようなデータの「除去」に対応したファームウェアを搭載している必要があります。

一方で、データが暗号化されていた場合には、これらの記録メディア内部で自動修正機能により使われなくなった記録素子にデータが残置していた場合でも、暗号鍵が無ければデータを復元することができなくなります。そのため、暗号鍵の削除で、データ除去と同様の効果を得ることが可能になります。

記録メディアからの情報漏洩防止策、という観点においても、データの暗号化は非常に効果的な手法であることが理解頂けるかと思います。

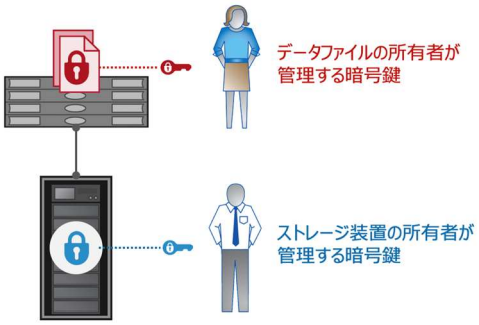
記録メディアからの情報漏洩防止対策としてのデータ暗号化の重要性
暗号化されたデータが記録メディアに保存されたままでも、暗号鍵が適切に削除されていることは、データの「除去」と同様の効果を持つ。

多層暗号化防御の重要性

データの暗号化による対応を考える上で、暗号鍵の取扱いの重要性は直感的に理解頂けるかと思います。暗号化によりデータを保護することがより強固にできる一方で、暗号鍵自体が漏洩した場合の対策を考慮する必要性が出てきます。

これに対するシンプルで効率的な考え方の一つに、多層暗号化防御というアプローチがあります。データが保管される幾つかの技術レイヤー毎に暗号化を実施し、それぞれ異なる暗号鍵を利用する方法です。万が一暗号鍵の一つが流出・漏洩したとしても、何れか一つの暗号鍵だけではデータの復号をできなくするシンプルな手法です。

銀行の貸金庫が分かり易い例えになります。銀行の建物に入館するための鍵と、建物の中の金庫の鍵、更には個々の貸金庫の鍵を、それぞれ異なる鍵を異なる人物が管理することでセキュリティを高めていることと同様のアプローチです。



現在、多くのクラウド事業者や ホスティングサービス・マネージドサービスを提供する企業において、この考え方が採用されています。サービスの利用者である利用者自身がデータファイルを暗号化する、或いは、暗号化保管が可能なサービスを選択利用し、データファイルの暗号鍵は利用者自身が適切に管理します。また、サービスを提供する企業側において、利用者のデータを不測の事態から守るという観点のもと、ストレージ装置における暗号化機能を活用し、暗号鍵の管理は、サービス提供企業の担当者が適切に管理する、という方法です。

多層暗号化防御の重要性
銀行の貸金庫では銀行の建物の鍵と利用者の鍵が異なることでセキュリティを高めている。このように、データファイルの所有者とストレージ装置の所有者が、それぞれデータを暗号化し、適切に暗号鍵を管理することで、より強固なデータセキュリティを実現することができる。

ストレージ装置に備わるデータ暗号化技術要素

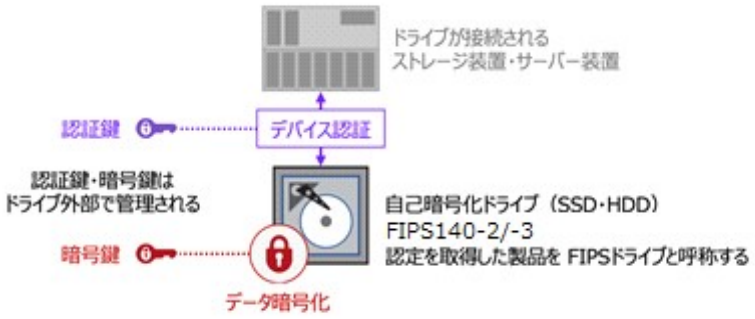
ここでは、これまでに記載したデータ暗号化の考え方に基づいた、ストレージ装置に備わるデータ暗号化機能における主要な機能を説明します。

現在のストレージ装置に搭載可能なハードディスクドライブ(HDD)やソリッド ステートドライブ(SSD)において、SDE(Self Encrypting Drive： 自己暗号化ドライブ)という製品があります。これは、HDD・SSD に書き込まれたデータを、HDD・SSD 自体がデータの暗号化を施し、内部の記録メディアに実際に書き込まれたデータは暗号化されている状態にするものです。

また、前述の多層防御の考え方に基づき、HDD・SSD ドライブ単体が盗難などにより流出した場合に備え、HDD・SSD が接続されるデバイス装置に対するパスワード認証機能も備えています。正しいデバイス利用パスワードを得られない場合には、HDD・SSD ドライブ自体の機能を永久に利用不可能とするデバイス・ロックという機能です。

また、前述の多層防御の考え方に基づき、HDD・SSD ドライブ単体が盗難などにより流出した場合に備え、HDD・SSD が接続されるデバイス装置に対するパスワード認証機能も備えています。正しいデバイス利用パスワードを得られない場合には、HDD・SSD ドライブ自体の機能を永久に利用不可能とするデバイス・ロックという機能です。

また、米国連邦政府での利用に際して発行されている情報処理標準規格である FIPS140-2/-3 に対応した自己暗号化ドライブとして、FIPS ドライブと呼ばれる製品も存在します。最も高いレベルでの情報漏洩防止を必要とする場合には、このような自己暗号化ドライブを利用することが望ましいでしょう。



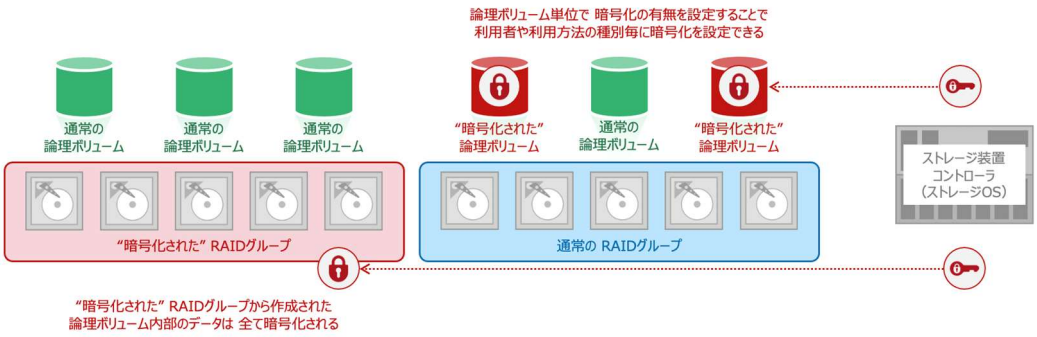
自己暗号化ドライブ：SDE（Self Encrypting Drive）と FIPS ドライブ
HDD と SSD において、ドライブ自身が暗号化機能を保持した製品の呼称 記録メディアの流出による情報漏洩対策としては、最も容易かつ根本的な対応策の一つ ドライブ内部のデータの暗号化に加え、接続デバイスに対する認証機能を保持する。 認証が得られない場合には、永久にドライブを利用不可とする機能（デバイス・ロック機能）を保持 自己暗号化ドライブ製品の中で、米国政府規格である FIPS140-2/-3 に適合し、認証を得た製品を FIPS ドライブと呼ぶ

論理ボリュームの暗号化：記録メディアを共有する環境におけるアプローチ

論理ボリュームの暗号化における基本技術要素

複数の利用者や複数のシステムを一括して集約保管するストレージ装置においては、HDD や SSD を集合体として扱い、記録メディアを共有する方法（論理ボリューム）が一般的です。ストレージ装置の内部で論理的に構成されたデータ記録ボリュームに対してデータ暗号化処理を適用する方法・機能を、論理ボリュームの暗号化と呼びます。そのため、論理ボリュームや”RAID”グループの単位でデータを暗号化することは、前述の自己暗号化ドライブと同様の効果を得ることができます。

また、利用用途に応じて、これらのストレージ装置内部の階層毎に暗号化の適応可否を選択できることが、ストレージ装置の提供する機能として重要になります。

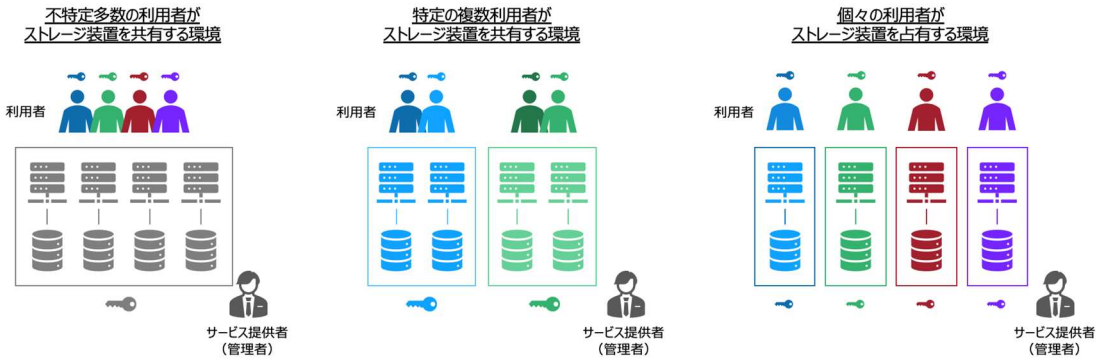


マルチテナント機能：共有環境におけるストレージ装置のセキュアな利用の実現

前述の多層暗号化防御の考え方と、前述の論理ボリュームの暗号化機能を合わせて利用するために、ストレージ装置には、マルチテナントと呼ばれる機能が実装されています。特に複数の利用者でセキュアに共有利用するためには必須の機能となります。

ストレージ装置が「どの程度の複数の利用者でまとまって共有されるのか」という利用環境を模式したものが、下図になります。

暗号鍵の適切な管理を実現する上で、装置を共有利用するグループ毎に暗号鍵を分けて管理できるような、マルチテナント機能やストレージ装置の設計が可能であることが非常に重要な意味を持ちます。



論理ボリュームの暗号化：共有環境における暗号化手法の設計
ストレージ装置が共有される環境においては、論理ボリュームの暗号化が効果的な手法 記録メディアからの情報漏洩対策防止に対する実効性としては、自己暗号化ドライブと同等の機能効果を持つ 「どの程度 複数の利用者により環境を共有されるのか」という利用用途に応じて、適切な運用管理を実現するために、マルチテナント機能と合わせた設計・実装が重要になる

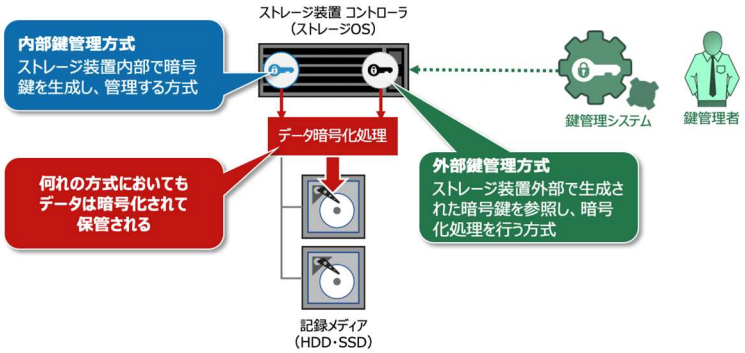
暗号鍵の管理方式

これまでの記載の通り、データ暗号化においては、暗号鍵の適切な管理が重要となります。一方で、利便性とセキュリティは相反する関係でもあります。日々のシステム運用・利用の中で、暗号鍵を紛失したことにより重要なデータにアクセスができなくなる、といった不幸な事故も少なからず存在します。データの暗号化は悪意を持った人々から重要なデータを保護する一方で、万が一暗号鍵を紛失した場合には正しい利用者もデータを復号できずにアクセスできなくなる、という諸刃の剣の側面を含んでいます。

ここでは、ストレージ装置に関連する暗号鍵の管理方式について、適切な暗号鍵管理運用を支援する技術を紹介します。

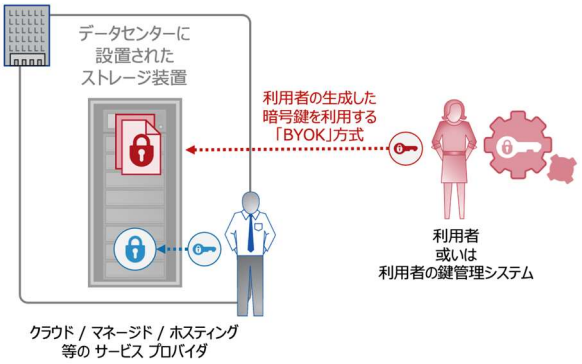
内部鍵管理方式と外部鍵管理方式

ストレージ装置におけるデータ暗号化においては、暗号鍵が必須となります。
この暗号鍵をストレージ装置内部で生成し利用する方法を内部鍵管理方式と呼び、また、ストレージ装置外部で生成された暗号鍵を利用してストレージ装置内のデータを暗号化する方式を外部鍵管理方式と呼びます。



また、ストレージ装置がデータセンターに設置され、クラウド/マネージド/ホスティングサービス事業者からの利用提供を受けている場合には、これらの暗号鍵を サービスプロバイダー事業者が生成・管理するケースと、利用者が自身で生成・管理するケース（BYOK: Bring Your Own Key 方式）が存在します。

前述の多層防御の考え方と、サービスの利用者責任等を含めて考慮すると、利用者は自身のデータに関する安全性を守るためにも自身が生成・管理する暗号鍵を利用することが望ましいと言えます。また、サービスを提供する事業者においても、前述の多層防御の考え方とマルチテナント機能を併用し、利用者データの保護の観点から、ストレージ装置のデータ暗号化機能を利用することが望ましいと言えます。



ストレージ装置における暗号鍵の管理方式：内部鍵管理方式と外部鍵管理方式
データの暗号化処理に必要となる暗号鍵は、生成・管理される場所に応じて、内部鍵管理方式と外部鍵管理方式の 2 種類が存在 内部鍵管理方式：ストレージ装置内部で暗号鍵を生成・管理する方式 外部鍵管理方式：ストレージ装置の外部で生成された暗号鍵をストレージ装置が参照し、暗号化処理を行う方式。暗号鍵の管理は暗号鍵管理システムが行う。 クラウド/マネージド/ホスティングなどの サービスプロバイダーの提供するストレージ装置を利用する際には、暗号鍵をサービスプロバイダー事業者が生成・管理するケースと、利用者が自身で暗号鍵を生成・管理するケース（BYOK）がある クラウド/マネージド/ホスティングなどの サービスを利用する際には、利用者が自身のデータファイルを守る目的で自ら暗号鍵を生成・管理することに加え、サービスプロバイダーが利用者保護の観点からストレージ装置の暗号鍵を利用形態に合わせて生成・管理を行う多層暗号化防御が望ましい

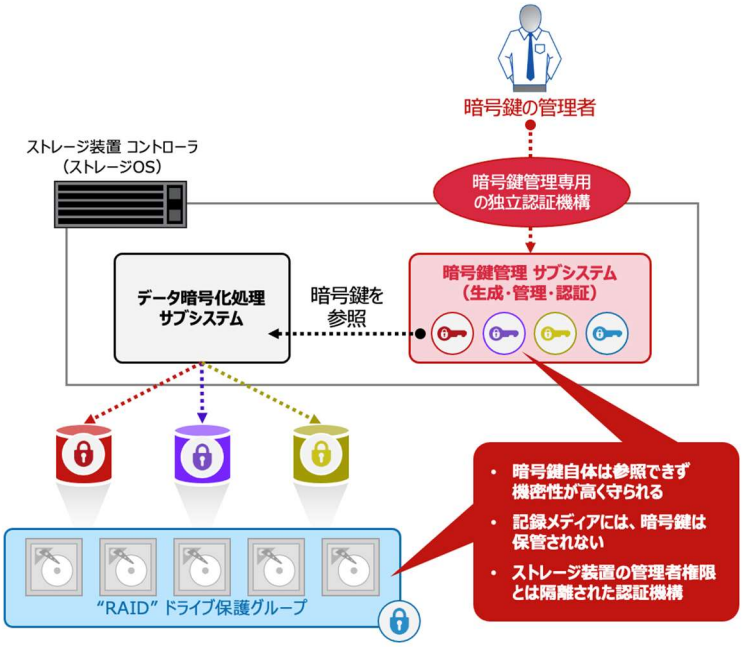
内部鍵管理方式における暗号鍵の取り扱い

ストレージ装置を制御するストレージ OS の内部には、暗号鍵の生成と管理を行うソフトウェア サブシステムを保持しています。このソフトウェア サブシステムは、他の管理制御機能とは論理的に隔離され、独立した認証機構を持ち、稼働しています。ストレージ装置の管理者権限とは別に、暗号鍵管理者用のパスワード認証を必要とします。また、暗号鍵管理者においても暗号鍵自体の内容を閲覧することはできず、暗号鍵の機密性を高く保つように設計されています。

また、暗号鍵は、前述の論理ボリュームやマルチテナント機能に対応し、暗号化を必要とするそれぞれの要素毎に一意な暗号鍵が使用されます。該当する要素が削除されると、これらの暗号鍵も削除されます。

これらの暗号鍵は、暗号鍵管理サブシステムの保持するデータとして、ストレージ OS が稼働する記憶領域に暗号化されて格納されており、利用者のデータが保存される記録メディアには保存されません。このため、記録メディアの盗難などによる流出の際においても、

暗号鍵は参照できず、データを復号することはできません。
内部鍵管理方式においては、暗号鍵管理サブシステムにおける認証パスワードを適切に管理することが重要です。一般的なパスフレーズ管理の原則に従い、想像され難いパスフレーズを特定期間毎に再設定する運用などが重要となります。



内部鍵管理方式：ストレージ装置内部の独立した暗号鍵管理ソフトウェア サブシステムの利用
ストレージ装置内部は機密性が高く保たれた暗号鍵管理ソフトウェア サブシステムが存在独立した認証機構と、要素毎に一意に割り当てられた暗号鍵が利用される。要素が削除された場合には、暗号鍵も削除される。 暗号鍵は、データが保管される記録メディアには保管されず、記録メディアの盗難や流出による情報漏洩を防ぐ暗号鍵管理ソフトウェア サブシステムへの認証パスワードは、適切に運用されることが重要

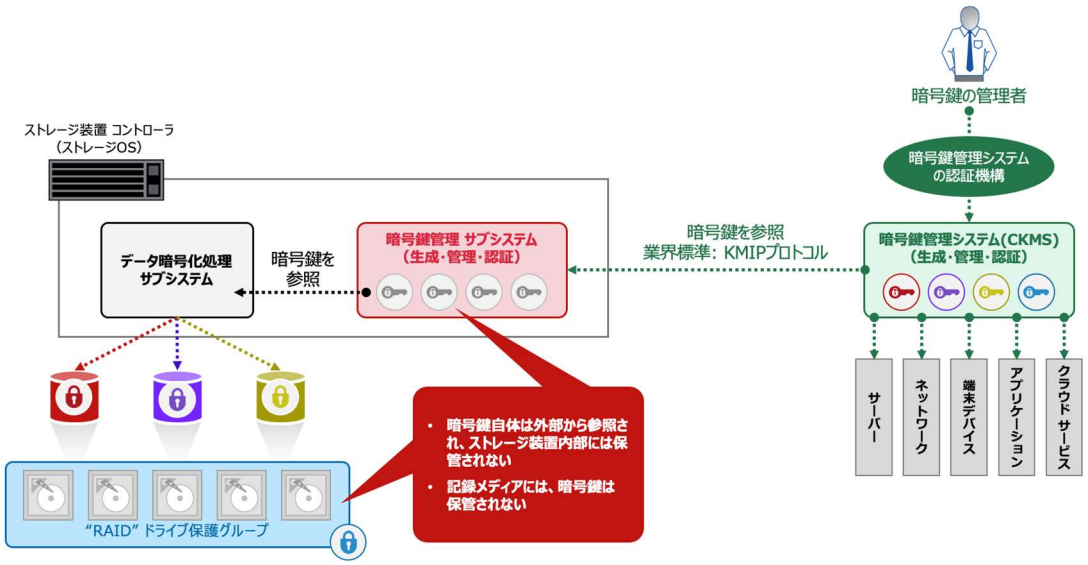
外部鍵管理方式における暗号鍵の取り扱い

外部鍵管理方式においては、暗号鍵管理システムが生成・管理する暗号鍵をストレージ装置がネットワークを経由して参照利用します。暗号鍵を利用するストレージ装置内部の暗号鍵管理サブシステムは、内部鍵管理方式と同様に論理的に隔離されており、機密性が高く維持されています。また、暗号鍵をストレージ装置内部に保持しないため、「暗号鍵を暗号化されたデータの近傍に保管しない」というベストプラクティスの観点からも、内部鍵管理方式よりもセキュアで安全な方式と言えます。

ストレージ装置においては、非営利国際コンソーシアム OASIS: Organization for the Advancement of Structured Information Standards, 構造化情報標準促進協会 が策定した、KMIP: Key Management Interoperability Protocol が標準プロトコルとして利用されています。

KMIP は、暗号鍵をネットワーク上で安全に転送するために必要となる技術要素（暗号方式、デジタル証明書、パスワード管理等、ライフサイクル概念等）がプロトコル規約として体系的に策定されています。相互運用性を確保することを目的として常に改善され、その仕様は公開されています。年次で開催される RSA カンファレンス（情報セキュリティを扱う世界最大の技術イベント）を主体の会議としてこれらの議論がなされ、新技術の導入などが決定されています。

外部鍵管理方式を実施する際には、自身が利用する CKMS システムにおいて、KMIP プロトコルに対応していることを確認することが重要と言えます。



外部鍵管理方式：暗号鍵管理システムの生成・管理する暗号鍵をストレージ装置が利用する方式
暗号鍵管理システム（CKMS）：ストレージ装置を含めたデータ暗号化を必要とする様々なデバイス、アプリケーション、クラウドサービスにおける暗号鍵を一元管理するストレージ装置は、KMIP プロトコルを通じて、ネットワーク上に存在する CKMS システムから暗号鍵を参照して利用する 参考情報：暗号鍵の管理方法に関するガイドラインと暗号鍵管理システムの在り方に関して、情報処理推進機構（IPA）より体系的な文書が公開されている（暗号鍵管理ガイドライン：https://www.ipa.go.jp/security/vuln/ckms.html） 暗号鍵を暗号化されたデータの近傍に保管しない、というベストプラクティスに準じており、内部鍵管理方式よりもセキュアな方式 暗号鍵は、データが保管される記録メディアには保管されず、記録メディアの盗難や流出による情報漏洩を防ぐ

デジタル化や IT 技術の活用が進むにつれて、クラウドサービス、オンプレミス環境を問わず、データセンターに設置されているストレージ装置に集約され保管されるデータの容量は、爆発的に増加しています。情報漏洩リスクを逓減するためにも、データの暗号化技術と、暗号鍵の適切な運用管理手法を知ることの重要性は、今後よりいっそう高まることと考えています。

第 6 章　まとめ

エンドポイントデバイスやクラウドサービスで使用する記憶媒体の進化や大容量化等に伴い、最近のドライブの特性に適している抹消方法が必要とされる状況になっています。

複数のデバイスを統合している仮想化領域の場合には記憶領域の特定が困難であり、デバイスからのデータ抹消が困難となってきております。また、過去の規格に囚われ、複数回の上書きによるデータ抹消の手法では長時間の作業となってしまうために消去・抹消作業を実施せずに転売、廃棄することで情報漏えいのリスクとなっている場合もあります。

さらに、クラウドサービスの利用に当たっては、クラウドの記憶領域における情報の運営および保管を総合的に設計（構成）した上で、データセキュリティを確保する必要があり、クラウドサービスの委託先に取扱いを委ねる情報は、適正に保管、消去・抹消されなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが困難である。また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の消去・抹消ことが困難であります。

クラウドサービスの委託先を適正に選択するためには、委託先へのガバナンスの有効性や利用および停止の際のデータセキュリティ確保のために必要な事項を十分考慮することが求められます。

このようなことから、本分科会では、クラウドでのデータ運用・停止・消去抹消の重要性を認識し、安全・確実なデータ消去の環境作りを行っていくことが急務であるという結論にいたり、その模範となるべき暗号化データ消去技術をまとめ、別冊として本ガイドブックを作成いたしました。今後も電子記憶媒体の活用の進化に合わせ、データ消去技術ガイドブックおよび本別冊も必要に応じた改訂を続けて行きます。

付録 A　用語解説書

・Sanitize：抹消（サニタイズ）
　復元が困難なようにデータの抹消すること。抹消手法に応じて。Clear：消去、Purge：除去、Destroy：破壊がある。

・Clear：消去（クリア）Resistant to keyboard attacks.
　一般的に入手できるツールを利用した攻撃に対して耐えられるデータ抹消のこと。

・Purge：除去（パージ）Resistant to laboratory attacks.
　研究所レベルの攻撃に対して耐えられるデータ抹消のこと。

・Destroy：破壊（デストロイ）Resistant to recreation of media.
　媒体の再生（再組立等）に対して耐えられるデータ抹消のこと。

・暗号鍵管理システム　暗号鍵管理基準
　暗号鍵を安全に管理するための基準。データ保管だけでなく、機器間の認証やデータ通信など様々な用途に多くの暗号鍵が使用されるため、厳格な管理・運用体制が必要とされている。暗号鍵の生成・配送・保管・利用・変更・廃棄といったライフサイクル毎に管理基準を定める。

・機密情報（機密データ）
　個人や組織がもつ公開していない情報を指す。
　企業が保有している情報のうち外部への開示が予定されない情報
　秘密として管理されている情報
　開示されれば企業に損失が生じるおそれのある情報
　設計図やマニュアル、企画書、顧客情報はもちろん、人事異動に関する情報や給与情報、在庫・仕入先リストなども保護すべき機密情報にあたる。

・復号鍵（復号キー）、暗号鍵（暗号キー）
　暗号化されたデータを元に戻すときに使う暗号鍵を意味し、公開鍵暗号においては、秘密鍵を指す。英語では Decryption Key

・論理消去
　プログラム処理により、削除フラグを設定する、または、情報の一部を消去する等の方法により、アプリケーションから情報にアクセスできなくすることを指す。情報そのものは、

記憶域に残った状態となる。これに対し、完全消去は、プログラム処理により、記憶域内の情報そのものを、別の情報によって上書きする等により、消去することを指す。また、物理消去とは、プログラム処理ではなく、消磁装置等、物理的な手段によって、情報を消去することを指す

・IaaS

Infrastructure as a Service の略で、クラウドコンピューティングのうちの 1 つで、仮想化技術を利用してハードウェアリソース（CPU／メモリ／ストレージ）などのデジタルインフラをインターネット経由でオンデマンド提供するサービスです。

・PaaS

Platform as a Service の略で、アプリケーションソフトが稼働するためのデータベースやプログラム実行環境などが提供されるサービスです。

・SaaS

Software as a Service の略で、クラウドサーバーにあるソフトウェアを、インターネット経由して利用者が利用できるサービスです。

・RAID

Redundant Array of Independent Disk の略で、複数のディスクにデータを分散し冗長性データを付加して格納し、ディスク障害のときに利用者データの再生を可能とするディスクアレイシステムです。

・HDD、SSD

Hard Disk Drive、Solid State Drive の略で、記憶装置です。
HDD は回転する円盤に磁気でデータを読み書きしていますが、SSD は USB メモリと同じように内蔵しているメモリチップにデータの読み書きをしています。

・ISMAP

政府機関等におけるクラウドサービスの導入に当たって情報セキュリティ対策が十分に行われているサービスを調達できるよう、令和 2 年 6 月に NISC・内閣官房情報通信技術(IT)総合戦略室・総務省・経済産業省の連携の下「政府情報システムのためのセキュリティ評価制度」（英語名：Information system Security Management and Assessment Program、通称：ISMAP（イスマップ）、以下「ISMAP」という。）を立ち上げました。

・政府統一基準群

国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるために国の行政

機関等のサイバーセキュリティに関する対策の基準です。

・多層防御

多層防御とは、ハッカーなどの攻撃を受けて、自社のネットワークやシステムのセキュリティが侵害されないようにするための複数の防御策のことです。

・FIPS 140

NIST*2 が策定した暗号モジュール（ハードウェアやソフトウェアを含む）のセキュリティ要件に関する米国連邦標準規格です。

・デジタル証明書（公開鍵証明書）

暗号技術において、公開鍵証明書とは、公開鍵とその所有者を結び付ける証明書です。

・DNS

Domain Name System の略で、インターネット上のホストのアドレスに使われるドメイン名と、IP アドレスとの対応づけを管理するために使用されているシステムです。

・NTP

Network Time Protocol の略で、パケット交換による遅延時間が変動するネットワーク上のコンピュータシステム間で時刻同期させるための通信プロトコルです。

・マルチテナント

機材やソフトウェア、データベースなどを複数の顧客企業で共有する事業モデルです。

・リモートワイプ

パソコンやスマートフォンなどのモバイルデバイスを遠隔地から操作し、端末に保存されているデータを消去する機能およびサービスのことです。

・CRYPTREC

Cryptography Research and Evaluation Committees の略で、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトです。

・暗号鍵管理システム

CKMS: Cryptographic Key Management System とも呼ばれ、ストレージ装置のみならず、サーバー、ネットワーク装置、アプリケーションやクラウドサービスなど、データ暗号化を必要とする様々なシステムの暗号鍵を一意に管理する役割を持つシステムです。一般的に

は、DNS や NTP などと同様に、ネットワーク上で共通のサービスを提供する独立したシステムとして構成されます。また、暗号鍵をネットワーク上でセキュアに転送するために、様々な通信プロトコルが存在しますが、これらのプロトコルの違いを吸収する役目も担います。

（順不同）

参考情報

以下の団体における規定や技術について調査を実施し、ガイドラインの作成を行っています。データ適正消去実行証明協議会では、データ消去の証明を行うにあたり、このような団体の調査結果も取り入れることで適正な消去証明の発行に必要な規定の検討を行っていきます。

（参考）NIST Special Publication 800-88 Revision 1
米国国立標準技術研究所（NIST：National Institute of Standards and Technology、以下、NIST と称す。）では、連邦政府の情報システムにおいて、費用対効果の高いセキュリティを施し、国家安全保障にかかわらない情報のプライバシーを確保するための、技術的、物理的、管理的および運用のための標準とガイドラインを策定しています。
NIST Special Publication 800-88 は、システムの機密性のセキュリティ分類を考慮した上で、データ抹消処理及び廃棄の決定のための適切かつ適用可能な技術とコントロールを備えた媒体のデータ抹消処理プログラムを米国連邦政府が実施する際のガイドラインである。なお、情報処理推進機構（IPA）より日本語訳が公開されている（「媒体のデータ抹消処理（サニタイズ）に関するガイドライン」：https://www.ipa.go.jp/files/000094547.pdf）

初版作成メンバー

データ適正消去実行証明協議会（ADEC）クラウドデータ消去認証分科会
データ適正消去実行証明協議会（ADEC）消去技術認証基準委員会
一般社団法人ソフトウェア協会

主査：
東京電機大学 研究推進社会連携センター 顧問 客員教授
　佐々木　良一

メンバー：　（五十音順）
　さくらインターネット株式会社
　日本マイクロソフト株式会社
　ネットアップ合同会社
　ワンビ株式会社

意見提供者：
　ADEC 技術顧問　沼田　理
　ADEC 運営実行委員会副委員長／消去技術認証基準委員長　加藤　貴

協力団体：
・デジタル庁
・IPA 独立行政法人情報処理推進機構

出版団体

一般社団法人ソフトウェア協会（Software Association of Japan）

会長：荻原 紀男（株式会社豆蔵 K2TOP ホールディングス代表取締役社長）
設立：1986（昭和 61 年）2 月
会員：624 社・団体（平成 31 年 4 月現在）
目的：コンピュータソフトウェア製品に係わる企業が集まり、ソフトウェア産業の発展に係わる事業を通じて、我が国産業の健全な発展と国民生活の向上に寄与する。
協力：データ適正消去実行証明協議会（ADEC）が目的とする、PC 等の様々な IT デバイスのリユース／リサイクルによる循環型社会への貢献を実現するために、データ適正消去証明書の発行事業を担う。

【お問い合わせ先 】
SAJ 事務局 TEL：03-3560-8440
URL：https://www.saj.jp/
〒107-0052 東京都港区赤坂 1-3-6 赤坂グレースビル