テープストレージの暗号化機能に関するチェックリスト

一般社団法人 電子情報技術産業協会
（JEITA）
テープストレージ専門委員会

発行年月日：2013 年 5 月 29 日

目次

1. はじめに

1.1. この文書の位置付け

近年、個人情報保護など社会的意識の高まりから情報漏えい対策の導入が急務となっている。その対応としてデータを暗号化して管理することは有効な手段である。データを暗号化しておくことにより、万一、保護対象のデータが記録されたメディア（カートリッジテープ、CD/DVD、PC 等）が盗難などにあった場合の情報漏えいリスクを低減することができる。

一方でデータ暗号化システムは構築、運用を適切に行わないと、所期の目的を達成できるとは限らない。例えば、暗号鍵が誰でも容易に入手可能な状態で暗号化システムの運用を行った場合、データを暗号化しておく意味はなく、期待する機密性も得られない。また、暗号鍵を何らかの原因で紛失した場合、暗号化データの復号は不可となる（すなわちデータの読み取りが不可となる）。このようにデータ暗号化システムの構築、運用では通常の IT システムにおける考慮点に加え、データ暗号化に関する考慮点を事前に認識しておく必要がある。

データを暗号化する場合、守りたいデータの重要度もユーザにより大きく異なるはずで、求めるセキュリティレベル（厳密性、機密性）も異なる。ユーザによっては多大な管理コストをかけても高いセキュリティレベルを実現したいだろうし、ある程度のリスクを許容して管理コストを低減したいユーザも存在するだろう。データ暗号化システムは求められるシステム要件に対して適切なセキュリティレベルを選択することが重要となる。

本チェックリストはテープストレージにデータを保管する際のデータ暗号化を対象として作成している。ユーザの求めるセキュリティレベル毎、又はシステムに対するユーザの立場（統括者、構築者、運用者）毎にどのようなチェック項目があるかをまとめ、付録のチェックリストにてチェックすることができるように作成している。本チェックリストでデータ暗号化システムを構築、運用又は廃棄する際、考慮するべき事項を知り、適切なシステム環境となっているかを判断する指針として役立てていただければ幸いである。

1.2. 章構成についての解説

２章：本チェックリスト読者においてシステム統括者、構築者、運用者毎のチェック内容について
３章：個人情報の保護など各種法規制、データ漏えい時の影響について
４章：テープストレージを使用したデータ暗号化システムの優位性について
５章：データ暗号化技術について
６章：構築するデータ暗号化システムのセキュリティレベル定義について
７章：本チェックリストのチェック項目及びチェック内容の解説について
付録：テープストレージの暗号化機能に関するチェックリスト

2. 本チェックリストの対象者

2.1. IT システム統括者　　「こんな事が必要なのか！」を知る

守るべきデータの重要性や保護対象となるシステム、データの範囲を確認する。データ暗号化のシステム要件について方針を考える。また情報漏えい事故発生時の対応や災害復旧対応についても事前に検討を行う。

2.2. IT システム構築者　　「こういうように作らなければ！」を知る

要求されるシステム要件を満たすためのシステム構築時注意点を確認する。運用時の性能（スループット）や災害復旧手順、暗号鍵の管理、運用手順の作成を行う。

2.3. IT システム運用者　　「こういう運用をしなければ！」を知る

全体のシステム構成をおおまかに把握し、データ暗号化に伴う運用注意点を確認する。また、暗号鍵の管理、運用手順についても事前に確認を行う。

3. 社会的動向によるデータ暗号化への要請

3.1. データ暗号化への社会的要請

個人情報の保護など社会的意識の高まりや関連する各種法規制、多発する情報漏えい事故などに対し企業として対策を行うことは急務となっている。その対応としてデータを暗号化して管理することは有効な手段である。データを暗号化しておくことにより、万一、保護対象のデータが記録されたメディア（カートリッジテープ、CD/DVD、PC 等）が盗難などにあった場合でも情報漏えいのリスクを低減することができる。

本チェックリストで対象としているテープストレージでの暗号化においては、システム構築及び運用を適切に行うことで要求されるセキュリティレベルに見合ったシステムの実現が可能である。

3.2. 各種法規制

データ保管、個人情報の取り扱い等について関連する法規制の例を以下に記す。

また、業種毎に政府指針やガイドラインが発行されている場合もある。詳細は 7.1.2 項「(4)関連法規の有無」を参照の事。

・日本国内における例

個人情報保護法（第 20 条）

e-文書法 ⇒具体的文書及びそのデータ保管期限は251の関連法で定められている

会社法 ⇒「内部統制システム構築の義務化」（大会社）

金融商品取引法（日本版 SOX 法） ⇒内部統制

・アメリカ合衆国における例

SOX 法 ⇒データ保管期間 7 年：US 公開企業・その他連結対象子会社

SEC ルール 17a-4 ⇒データ保管期間 6 年：金融業界

HIPAA ⇒データ保管期間 6 年：医療業界

カリフォルニア州個人情報取扱法（California SB1386）

・欧州連合における例

データ保護指令 European Data Protection Directive

・その他

クレジットカード業界のデータセキュリティ基準 PCI DSS

3.3. データ漏えい時の影響

データ漏えい事故が発生した場合、その内容及び規模などから一概には影響を算出することは難しい。「NPO 日本ネットワークセキュリティ協会」の調査結果[1]では以下のような損害賠償の調査結果が出されている。

・一人あたりの平均想定損害賠償額は 4 万 8533 円

・一件あたりの平均想定損害賠償額は 1 億 2810 万円

また、その他の影響例としては下記のようなことが想定される。

・漏えいの原因と被害の範囲を特定するための調査とその対策費用
・被害者や株主から損害賠償の裁判を起された場合の作業費用
・企業ブランドの信用性に対する毀損と営業活動への悪影響
・法令の罰則規定への対応、など

守るべきデータに対する事前のデータ漏えい対策が必要である。

4. テープストレージの優位性

世界で最初のテープドライブがこの世に登場してからほぼ 60 年になろうとしているが、テープストレージの技術や性能は常に進化し続けてきた。LTO Ultrium 5（以下：LTO 5）テープドライブでは 2:1 圧縮で 3TB の容量を、一時間当たり約 1TB の転送レートで記録できる。実際これは最初のテープドライブと比較して約 60 万倍の性能（転送レート）アップになっている。

60 年もの間、コンピュータシステムの中でテープストレージが使われ続けている主な理由は以下の 3 点に集約できる。

(1) 低コストのストレージ

増え続けるデータに対し、次々とディスク（HDD）を増設して保存するのはあまり賢い方法とは言えない。なぜならそのような運用はコスト的に高くつくからである。コスト計算はハードウェアの購入コストだけでなく、消費電力、空調、さらにはデータセンターのフロア管理コスト、メンテナンスコストなども考慮する必要がある。容量あたりのコスト単価は代表的なテープ媒体である LTO 5 カートリッジでギガバイトあたり約 8 円[2]と安価であり、ディスクシステムと比較すると低コストと言える。また、テープシステムはデータの読み込みや書き込み時以外、カートリッジテープは保管されているだけなので電力コストも低く抑えることが可能である。

(2) データ保護

データ保護はハードウェア障害、人為的なミス、ソフトウェアの問題など様々なデータ損失リスクをどれだけ緩和できるかということに尽きる。データ損失のリスクは多岐にわたるため、一つのテクノロジーで補えるものではないが、ある調査ではハードウェア障害が 40%に対して人為的ミスが 29%と高い割合であった[2]。

より安全にデータを保護するためには、理想的には３つ以上のコピーを異なる場所に保管し、またそのうち 1 つ以上は地震や洪水といった災害に対する復旧用として遠隔地（オフサイト）に保管すべきである。また、オフラインコピーをシステムからデータを分離することで、コンピューターウイルス、意図的な破壊工作、人為的なミスといったリスクからデータを保護できるようにすべきである。オフサイト、オフラインにデータを保管できるカートリッジテープは人為的ミスに対して強さを発揮できると言える。

(3) 長期データ保存

アーカイブソリューションなどで長期にデータを保存する場合、メディアの保管寿命が重要となる。一般的にはカートリッジテープはディスクの 4～6 倍の寿命があると言われており、JEITA での加速テストにおいても LTO カートリッジテープは 19 年以上の保管寿命が確認されている[2]。また、増加する保存データに対してカートリッジテープを増やすことや、新しい世代のテープドライブに交換することで容量の拡張に対応できる。もちろんカートリッジテープのコストパフォーマンスの高さは言うまでも無い。

以上のような理由から使用され続けているテープストレージであるが、「リムーバブルメディア」であることからメディアの盗難や紛失による情報漏えいのリスクがある。情報漏えいが起きた時は単純にデータの紛失にとどまらず、社会的信用の失墜、訴訟等により会社の存続に関わる事態に発展する可能性すらある。こうした背景からメディアの盗難や紛失が発生した場合、データを容易に読めないようにする「暗号化」はデータセキュリティ戦略の最も重要な機能となってきている。

(4)テープストレージにおける暗号化の優位性

カートリッジテープに書き込むデータを暗号化する手段として、ソフトウェアで暗号化する方法とハードウェアで暗号化する方法がある。またハードウェア暗号の場合、テープドライブに実装されているデータ暗号化機能を使用する方法と、サーバ、テープドライブのデータパス間に暗号化専用機器を入れて暗号化を行う方法がある。以下にそれぞれの構成例を示す。

① ソフトウェア暗号（バックアップソフトによる暗号化例）

バックアップソフトなどのソフトウェアで暗号化を行う場合、暗号化の導入が容易であるがサーバのCPU 高負荷や暗号化処理時間大によるデータ転送レートの低下が懸念される。

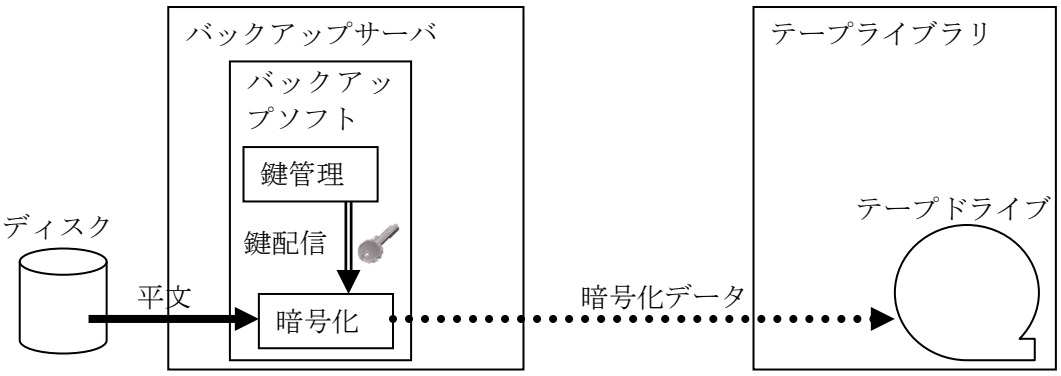


図 4-1 バックアップソフトによる暗号化構成例

② ハードウェア暗号（暗号化装置によるデータ暗号化例）

サーバとテープドライブのデータパス間に暗号化専用機器を入れて暗号化を行う構成。暗号化機能を持たないテープドライブの環境にも導入できる利点がある一方、専用機器が高価であることやテープドライブの高速化に伴う性能への悪影響が懸念される。

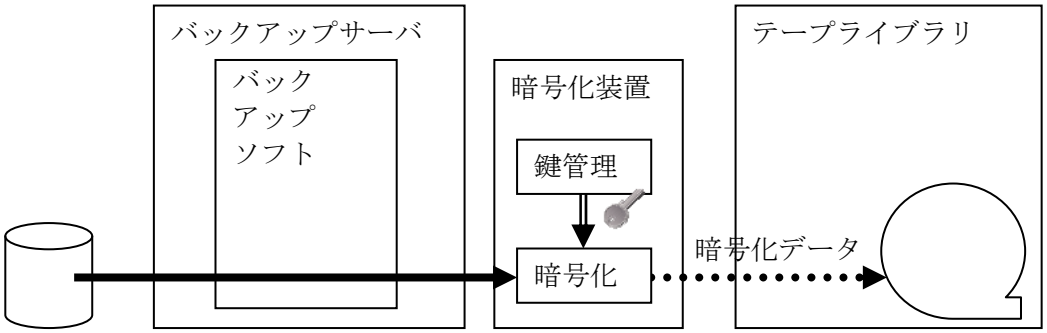


図 4-2　暗号化装置による暗号化構成例

③ ハードウェア暗号（テープドライブによるデータ暗号化例）

テープドライブのハードウェアに標準で実装されている暗号化機能を使用する構成。例として LTO 4 以降の LTO ドライブでは 256 ビット長の鍵でデータを暗号化(AES-256 暗号)する機能を実装しており、テープドライブに暗号鍵を渡すことで、ドライブがデータを暗号化してテープに書き込んだり、復号しながら読み出したりすることが可能となっている。ドライブへの暗号鍵の配信方法は下図のバックアップソフトで行う方法のほか、「鍵管理システム」で行う方法や「テープライブラリ」で行う方法がある。

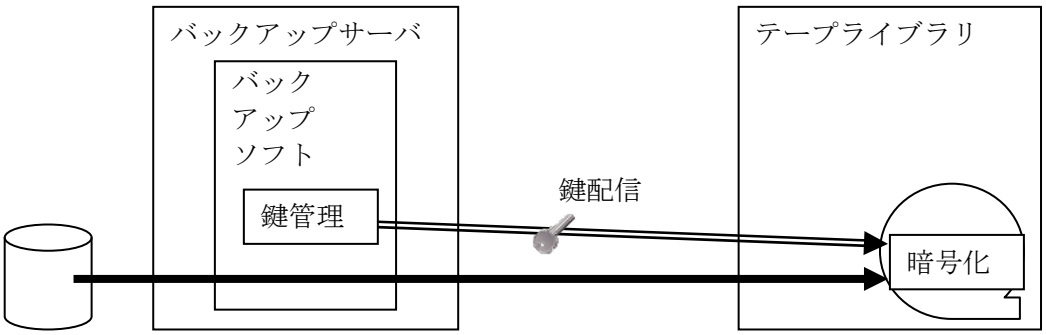


図 4-3 テープドライブによる暗号化構成例

テープドライブでのハードウェア暗号では以下のようなメリットがある（図 4-4 参照)。

・テープドライブ自体がデータ暗号化処理を行うため、暗号化処理に伴うサーバの負荷が低減される。
・テープドライブによるデータ圧縮後に暗号化を行うため、効率よくデータ圧縮を行うことができる。
・ソフトウェア暗号と比較すると暗号化処理にかかる時間が小さく、テープドライブ本来の性能を活用することができる。

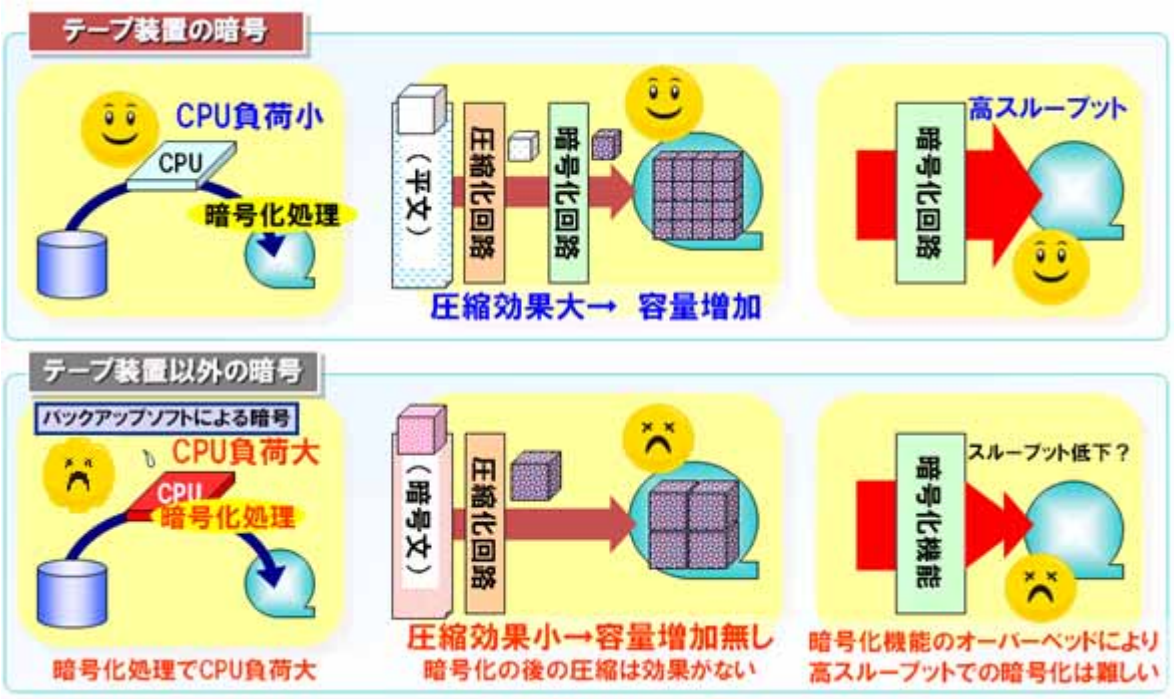


図 4-4　テープドライブでの暗号化処理の優位性

5. データ暗号化技術

5.1. 暗号化の各種方式

この章では現在利用されているデータ暗号化の各種方式について簡単に解説する。

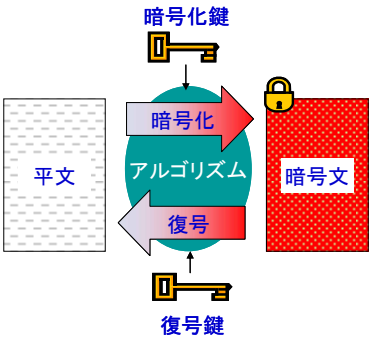
現在データ暗号化に利用されている暗号方式は、共通鍵暗号方式と公開鍵暗号方式に大別できる（表5-1）。

共通鍵暗号方式は対称鍵暗号とも呼ばれ、データの暗号化と復号を行う際に同一の鍵を使用する。テープストレージが使用している AES-256 暗号はこの共通鍵暗号方式に分類される。一方、公開鍵暗号方式は非対称鍵暗号とも呼ばれ、暗号化と復号とで異なる鍵を使用する。通常、一対の鍵を生成し、一方を秘密鍵、他方を公開鍵として用いる。この方式の実施例には RSA 暗号や楕円暗号などがある。

一般的には、共通鍵暗号方式で用いられる鍵の長さは比較的短く、高速なデータ暗号化や復号の処理が可能である。また、専用のハードウェアの開発も比較的容易である。一方、公開鍵暗号方式は、ある一対の鍵を生成するための計算処理に対して、公開されている鍵から他方の秘密鍵を特定するための計算処理が困難となる数学的な非対称性が用いられている。その鍵長は比較的長く、データ暗号化や復号のための計算量が多くなるため高速処理には不向きである。

表 5-1　共通鍵・公開鍵暗号方式の比較

	共通鍵暗号方式	公開鍵暗号方式
暗号化鍵と復号鍵	共通（対称） ［ 暗号化鍵 = 復号鍵 ］ １つの鍵を暗号化、復号の両方に使用	非対称 ［ 暗号化鍵 ≠ 復号鍵 ］ 一対の鍵を生成し、一方を秘密鍵、他方を公開鍵として使用
処理速度	高速	低速
実施例	DES, AES など	DSA, DH, RSA, 楕円暗号など



5.2. 鍵長と安全性

悪意のある第三者が暗号化されたデータの暗号鍵を特定（暗号化データを不正に解読）しようと試みるような場合、一般的には鍵長が長いほど鍵を特定するのが困難であり、安全性が高い。例えば、AES-256 暗号なら「2 の 256 乗」通りの鍵が考えられ、これらの鍵を総当たりで試してデータを解読しようと試みても膨大な時間を要し、現実的には解読が非常に困難である。

他の不正な解読の可能性としては、暗号のアルゴリズムの特徴や弱点をついた試みが考えられる。この観点で、暗号アルゴリズムの安全性が公に評価されている暗号方式を使用した方が良い。仮に独自に暗号方式を考案したとしても、その安全性が公に評価されていなければ、暗号化データが漏えいした場合に第三者がその安全性を評価・判断することができないため、安全性を証明することが困難となる。

表 5-2 にアメリカ国立標準技術研究所（NIST）が公開している各種暗号方式の鍵長と安全性の比較[3]を示す。例えば、80 ビット強度の等価安全性に相当する共通鍵暗号方式は、2 つの鍵を使った Triple DES

であり、公開鍵暗号方式で同等の等価安全性を示すのは、DSA、DH の場合、公開鍵・秘密鍵の長さがそれぞれ 1024 ビット・160 ビットの場合であると評価されている。この表の比較において、ビット強度の数値が小さいほど安全性が低く、大きいほど安全性が高い。テープストレージが使用している AES-256 暗号は、この比較において最も安全な暗号方式の一つと言える。

表 5-2　鍵長と安全性の比較[3]

等価安全性		共通鍵暗号方式	公開鍵暗号方式			
			DSA、DH		RSA	楕円暗号
	ビット強度		公開鍵	秘密鍵		
低い	80	2-key Triple DES	1024	160	1024	160～223
⇕	112	3-key Triple DES	2048	224	2048	224～255
	128	AES-128	3072	256	3072	256～383
	192	AES-192	7680	384	7680	384～511
高い	256	AES-256	15360	512	15360	512～

コンピュータの演算能力の向上に伴い、使用する暗号方式が比較的容易に解読可能となるなど、将来、脅威にさらされる可能性がある。図 5-1 は、NIST や内閣官房情報セキュリティセンター（NISC）が公開している資料[3][4]からまとめたもので、比較的安全性の低い暗号方式は使用の中止や新しい暗号方式への移行が推奨されている。これに対して、テープストレージが使用している AES-256 暗号は 2030 年以降も使用が可能であり、長期の使用が可能と言える。

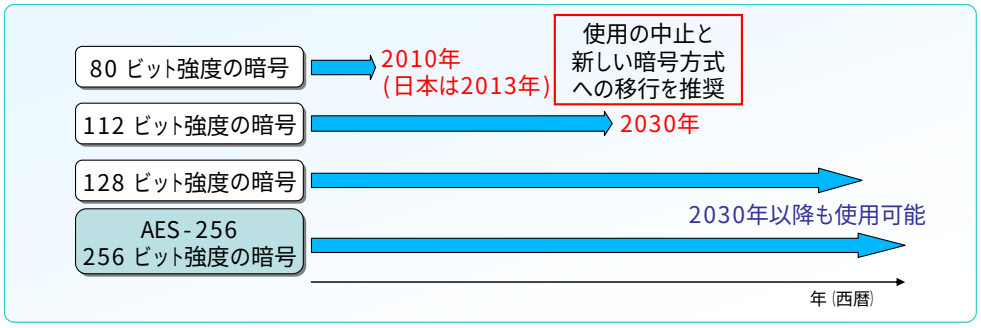


図 5-1　暗号化の安全性と推奨される使用期限

5.3.　鍵の管理が重要

いくらデータの暗号化を完全にしていたとしても、その鍵の管理が疎かだと期待通りの機密性を達成できない。例えば、第三者が容易に入手可能な状態で暗号鍵が放置されているなら、データの機密性はデータが暗号化されていない場合とほぼ同等である。あるいは、データが暗号化されていることで、第三者に対するデータへのアクセス管理が無防備になるなら、データの機密性はより危険な状態になって

しまう可能性もある。

また、鍵の管理が疎かで、何らかのシステム障害などが理由で鍵を喪失すると、暗号化データを復号することができなくなる。これは、データを喪失することに等しいため、鍵を喪失することのないよう適切な管理が必要である。鍵の管理を容易にするには鍵の数を少なくするのが良いが、一方、万一鍵が漏えいした場合に脅威にさらされるデータ量が多くなり、リスクとのトレードオフがある。

6. 達成したい機密性・厳密性

暗号化システムを構築する際、保護すべきデータに対するセキュリティレベル（機密性、厳密性）の目安をおおまかに説明する。構築するシステムは達成したい厳密性・機密性において「低」と「高」どちらに近いかを考え、文末にあるチェックリストの「低」又は「高」の該当項目内容を事前に確認する。

達成したい厳密性・機密性「低」

カートリッジテープに保管するデータに「暗号化」を導入する場合、事前チェックが必要となる基本的な項目を示す。

達成したい厳密性・機密性「高」

保管するデータの機密性、厳密性に加え、データ暗号化で使用する「暗号鍵」のセキュリティを考慮したシステムを構築、運用する場合にチェックが必要となる項目を示す。
高いセキュリティレベルを求めた場合、システムとして運用管理が複雑になり運用コストも高くなる傾向にある。構築するシステム要件に対し、最適なセキュリティレベルを選択することも重要なポイントとなる。

7. 各フェーズにおけるチェック項目

7.1. 検討/計画

7.1.1. システム全体の位置付け

テープストレージを使用したデータ暗号化システムを構築するにあたり、システム全体の位置付けを明確にしておくことは、暗号化を適用すべきデータ範囲を絞り込んで行くという意味でも重要な作業である。システム全体の位置付けについては、以下の順番に検討を進める。

・対象と考える IT システムの範囲
・外部との情報交換
・情報資産目録
・想定される脅威
・事業継続

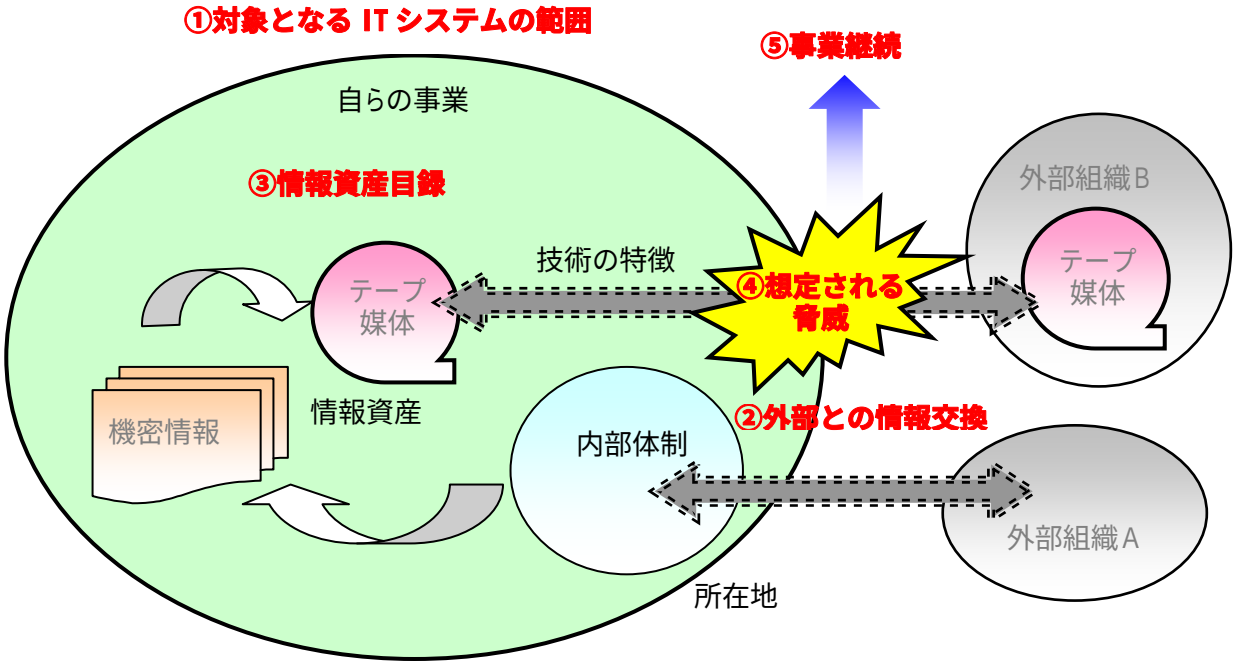


図 7-1 システム全体の位置付け

(1) 対象と考える IT システムの範囲

ここではデータ暗号化システムの導入を検討する上で、対象と考える IT システムの範囲を明確にするため、経済産業省の情報セキュリティ政策を参考に説明する。経済産業省が作成した情報セキュリティ管理基準[5]よれば、情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するためには、検討すべき IT システムの適用範囲を明確にする必要があり、組織は以下の点を

考慮して適用範囲及び境界を定義することになっている。

自らの事業	（自らの事業と外部とのシステムの境界を明確にする）
体制	（内部組織体制によるシステムの境界を明確にする）
所在地	（事業所の所在地でシステムの境界を明確にする）
資産	（情報資産単位でシステムの範囲を明確にする）
技術の特徴	（適応技術の特徴からシステムの範囲を明確にする）

図 7-1 を参考にして対象と考える IT システムの適用範囲の明確化を行う。

(2) 外部との情報交換

ここでは外部と情報交換を行っている内部体制もしくは内部の組織、及びそこで交換されている情報の内容や情報交換の方法を個々に確認する。情報処理施設のセキュリティを維持するためには、外部組織によってアクセス、処理、通信又は管理される情報を明確にし、外部組織が関わる業務プロセスから組織の情報及び情報処理施設に対するリスクを識別しておく必要がある。そして、外部組織にアクセスを許可する前に適切な管理策を実施しておく必要がある。

(3) 情報資産目録

ここでは自らの事業で取り扱うデジタル化された情報資産について保護レベルを明確にするための情報資産目録の確認を行う。組織が扱うデジタルデータは、全ての情報資産を明確に識別しておく必要があり、重要な情報資産については暗号化すべきデータを判別しておく必要がある。以下に経済産業省のセキュリティ管理基準[5]に基づいた資産目録の作成手順を示す。

1) 資産目録には重要度を記録する。
2) 資産目録には資産の種類、形式、所在、バックアップ情報、ライセンス情報及び業務上の価値を含め、災害から復旧するために必要な全ての情報を記載する。
3) 資産目録は他の目録と不必要に重複することなく、その記載内容が他の目録と整合していることを確実にする仕組みを整備する。
4) 資産目録を作成し維持する場合には、各々の資産の管理責任者及び情報の分類について合意し文書化する。
5) 資産の重要度に応じた保護のレベルは、資産の重要度、業務上の価値及びセキュリティ上の分類に基づいて決める。

5,000 人を超える個人情報を取り扱う事業者（法人その他団体又は個人）は個人情報取扱事業者として規定され、個人情報保護法により個人情報の取得、利用、管理等において各種の義務が課せられる。適正・安全な管理に関するルールとして、個人情報保護法 20 条では「個人データの安全管理のために必要かつ適切な措置を行うこと」となっている。これに対する技術的な措置の一例として「情報の暗号化」が内閣府消費者庁の「個人情報保護法に関するよくある疑問と回答」[6]に記述されている。安全管理のため具体的にどの程度の対応が必要かについては一律に定まるものではないが、個人情報に関して

は取り扱う情報の性質や利用方法、情報通信技術の発達などを勘案し、社会通念上合理的な程度の安全管理措置を取る必要がある。

(4) 想定される脅威

ここでは自らの事業の中で扱う情報資産において想定される脅威を確認する。ハードウェア障害などによるデータ損失のほか、不正アクセスなどによるデータ漏えい、改ざんなどが考えられる。個人情報が漏えいした場合、平均想定損害賠償額は一件あたり 1 億 2 千万円以上[1]と言われている。

(5) 事業継続

ここでは自らの事業について事業継続の必要性を確認する。企業は災害や事故で被害を受けても、取引先等の利害関係者から重要業務が中断しないこと、中断しても可能な限り短い期間で再開することが望まれている。また事業継続は企業自らにとっても重要業務中断に伴う顧客の他社への流出、マーケットシェアの低下、企業評価の低下などから、企業を守る経営レベルの戦略的課題と位置付けられる。[7]

7.1.2. 何を守るべきか・どう守るべきか

テープストレージによるデータ暗号化システムの導入を検討するには、対象とする IT システムの範囲を明確にし、そのシステムで想定される脅威から守るべき重要なデータの範囲を明確にする。また、その情報をどのように守るかについて検討する必要がある。

(1) 守るべきデータの範囲

重要な情報が外部に漏れることを防ぐため、7.1.1 項で確認したシステム全体の位置付けを見直し、守るべきデータの範囲を明確にする必要がある。

(2) 現行システムの問題点

守るべきデータに対して、データの損失、情報漏えい、改ざん、など可能性を考慮し、現行システムの問題点を事前に確認しておく必要がある。現行システムの問題点については①第三者監査証跡（アクセスログ)、②セキュリティ事象記録、③運用上の問題点の記録、④故障記録、⑤障害履歴、⑥提供サービスに関連する中断記録等をレビューすることにより把握することも可能である。また、セキュリティレベルを維持する上で、現状の管理コストや機器運用コストの負担が増加する場合には、情報管理の仕組みや使用機器の入れ替え等も考慮しセキュリティ対策を検討する必要がある。

(3) リスクの検討

守るべきデータに対してデータ漏えい、改ざん、破壊、盗難などの脅威で受ける損害額は、おおまかにしか算出することができない。しかしこのようなリスクを最小限に抑えるための対策、例えば「データの暗号化」を行うためのコストを算出することは可能である。リスクマネージメントは事業活動に伴う様々な危険を最小限の費用で食い止める作業である。想定される損害額に対しリスク回避に必要なコストが明らかに低いと考えられるのであれば、そのリスクは高いため、回避すべきである。逆にリスク

回避に必要なコストの方が高いと考えられるのであれば、そのリスクは比較的軽い、もしくはそのリスクに対する回避手段が非効率であると考えられ、他の回避手段の検討が必要と考えられる。ここでは 7.1.1 項で検討した脅威を再確認し、被害者に対する損害賠償額以外にも自らの事業に対する悪影響で受ける損害額についても考慮した上で、リスクの度合いを検討する。

(4) 関連法規等の有無

重要な情報を守る手段として業種毎に政府指針やガイドライン等が発行されている場合がある。この中に「データの暗号化」が示されているか事前に確認しておく必要がある。

例：

・経済産業省：情報セキュリティ関連法令の要求事項集
JIS Q 27001 機密性・完全性・可用性（CIA）と法的保護 完全性（I）に関するもの
完全性を保管する制度　電子署名法　A.12.3 暗号による管理策
http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_kanrenhourei.pdf

・経済産業省：セキュリティ管理基準
8 情報システムの取得、開発及び保守 8.3 暗号による管理策　（75 頁）
http://www.meti.go.jp/policy/netsecurity/docs/isaudit/IS_Management_Standard.pdf

・経済産業省：電子政府情報セキュリティ管理基準モデル　（35 頁）
9)　媒体の配送においては、デジタル署名及び秘匿のための暗号の使用を考慮すること
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex03.pdf

・内閣府 国民生活局：個人情報保護方に関するよくある疑問と回答
＜４ 適正・安全な管理に関するルール＞ Ｑ４－１
http://www.caa.go.jp/seikatsu/kojin/gimon-kaitou.html

・金融庁：保険会社向けの総合的な監督指針
Ⅱ-3-6 顧客情報管理 主な着眼点 (5) システム ②データの保護 イ（149 頁）
http://www.fsa.go.jp/common/law/guide/ins.pdf

・日本情報処理開発協会：ISMS 認証基準
8.システムの開発及びメンテナンス (3) 暗号による管理策 (9 頁)
http://www.isms.jipdec.or.jp/doc/ismsreq08.pdf

・日本情報処理開発協会：クレジット産業向け ”PCI DSS”/ ISMS ユーザーズガイドガイド
保護すべき会員データ　カード会員番号（PAN）　暗号化の必要性　（22 頁）
http://www.isms.jipdec.jp/doc/JIP-ISMS116-30.pdf

・日本情報処理開発協会：クレジット加盟店向け ”情報セキュリティのためのガイド”
（PCI DSS/ISMS 準拠のためのガイド） カード会員番号 暗号化の必要性 （4 頁）
http://www.isms.jipdec.jp/doc/JIP-ISMS118-20.pdf

（5）情報漏えい保険

情報漏えい対策の一つとして、各保険会社が提供している「情報漏えい保険」の検討も必要である。情報漏えいが発生した場合、対策コスト負担軽減ができ、保険会社が推奨する安全対策を適応することにより保険金額の割引が適応される場合もある。

日本商工会議所：個人情報漏えい賠償責任保険制度
http://www.jcci.or.jp/sangyo/rouei-hoken/
本制度は個人情報保護法（平成 17 年 4 月 1 日全面施行）に対応した商工会議所会員のための保険。

（6）他社、同業者の動向

情報セキュリティに関する最新技術は日々変化している。特にセキュリティに関する新たな手口や被害状況については同業者から得る情報も重要であると考えられる。同業者の動向を調査し、最新技術に対応した効率的な対策等については自社にとっても有益な情報であり、状況に応じては模範となる。

7.2. 設計/構築

7.2.1. 暗号化の対象

データの暗号化を考える為には、どこにあるデータを暗号化するか明確にする必要がある。
現在の IT システムにおけるデータは、①カートリッジテープ上②ディスク、メモリ上③DVD 等のリムーバブル媒体④装置間をつなぐ伝送経路上の何れかに分類される。何れの場所においても、データを暗号化する事は重要となるが暗号化の目的に沿った選択が必要である。

① カートリッジテープには、バックアップデータや、アーカイブデータが書き込まれることが多く大量の保存データを暗号化することによりデータを保護することが目的となる。
② ディスク上には、オンラインのアクセスデータや、一時データ等共有されるデータが書きこまれていることが多いことから、不要なアクセスからデータを保護することが目的となる。また、ディスク装置の障害発生時等に保守部品と交換した場合、取り外されたディスクドライブ内部に書き込まれたデータを保護すると言う目的もある。
③ DVD 等リムーバブル媒体はデータの受け渡し等に使用されることが多く、受け渡し時の情報漏えいなどからデータを保護する事が目的となる。
④ データ転送経路上には、多くのデータが流れることになり、全ての通信データを保護することが目的となる。

本チェックシートでは、カートリッジテープに書き込んだデータを対象としているため上記②～④に関しては対象外としているが、カートリッジテープをデータの受け渡しに使用する場合は③についても

対象となる。

7.2.2. データ暗号化の単位

カートリッジテープに書き込むデータを暗号化する場合、以下の４つの単位で暗号化の有無を管理できる。なお、これらは使用するシステム構成やソフトウェアにより選択できる内容が変わるため事前に確認しておく必要がある。

① ジョブ単位
ジョブ単位では、バックアップやアーカイブといったソフトウェアの１つの処理単位毎に暗号化の有無を管理する。きめ細かな管理が可能となる。

② メディア単位
メディア単位では、１巻のカートリッジテープを単位として暗号化の有無を管理する。１巻のカートリッジテープの中に書き込まれた複数のジョブのデータが暗号化される。カートリッジテープ毎に暗号化されているかどうかを把握しやすいメリットがある。

③ ライブラリスロット単位
ライブラリスロット単位では、ライブラリ装置にあるカートリッジテープを格納する棚（スロット）毎に暗号化の有無を管理する。例えば、マガジン（複数のスロットが固まりで外せるもの）単位等でカートリッジテープを交換運用する場合等に、スロットで暗号化運用しやすいメリットがある。

④ メディアプール単位
メディアプール単位では、ソフトウェアが管理しているカートリッジテープの集まりの単位毎に暗号化の有無を管理する。ソフトウェアがカートリッジテープの集まりを資源として管理しているような場合にメリットがある。

7.2.3. 暗号化の実現方法

(1) 暗号化手段の種別

暗号化手段の種別としては、ソフトウェアで暗号化する方法とハードウェアで暗号化する方法がある。ハードウェア暗号の場合、テープドライブの暗号化機能を使用する方法と、サーバ、テープドライブのデータパス間に暗号化専用機器を入れて暗号化を行う方法がある。詳細は４章(4)を参照頂きたい。

(2) 暗号化の構成例

代表的な暗号化構成例については 4 章(4)を参照頂きたい。

(3) 暗号鍵の競合

テープドライブに実装されているハードウェア暗号化機能を使用する場合、注意する点として暗号鍵の競合がある。図 7-5 は、テープライブラリおよび、バックアップソフトの２箇所から暗号鍵を配信してしまった例である。ライブラリから Key1 を配信した後に、バックアップソフトから Key2 が配信されてしまい、結果的に意図しない Key2 で暗号化が行われてしまう。暗号鍵をどこで管理するかを確認し鍵の競合が発生しないように注意が必要である。

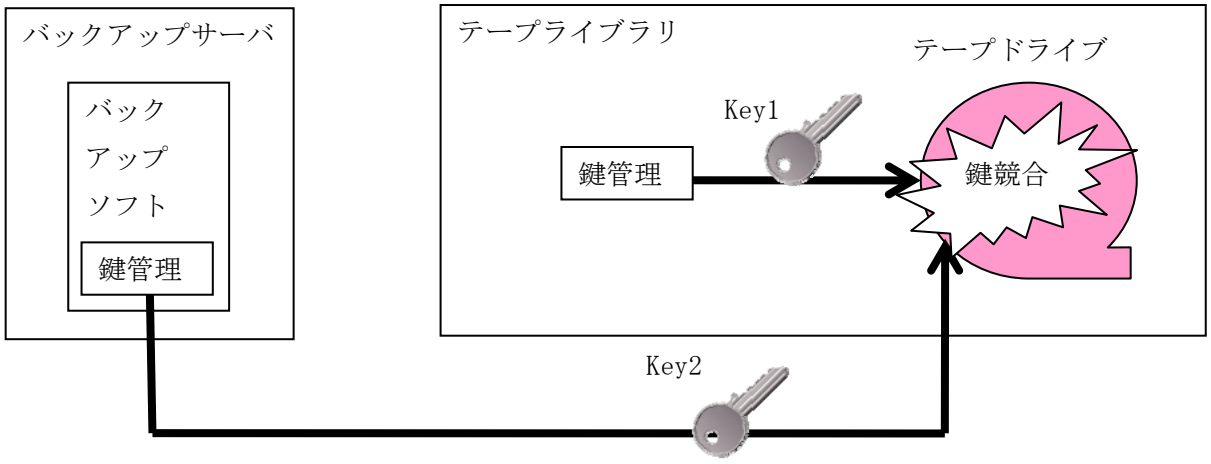


図 7-5　鍵の競合の例

7.2.4. 暗号化の性能

(1) 暗号化のスループット

データ暗号化を行うシステムの場合、暗号化の処理時間を考慮したデータスループットについて検討する必要がある。暗号化の処理時間は 7.2.3 項で述べたデータ暗号化の方法（「ハードウェア暗号」「ソフトウェア暗号」）に大きく影響されるため、以下の特徴を考慮した上でシステムのスループット設計に問題がないか検討が必要となる。また、可能であれば実際のデータを使用して事前に性能検証を実施することも有効な手段である。

① ハードウェア暗号（テープドライブ）における性能

データ暗号化機能を実装しているテープドライブ(例えば LTO 5 ドライブ)の暗号化機能を使用して、カートリッジテープへ書き込み時にデータ暗号を行うもの。テープドライブのハードウェア機能を使用するため、システムへの負荷（CPU 利用率等）が少なくなる。また、カートリッジテープへの書き込み時に実施されるデータ圧縮機能との効率的な連携も考慮されており、データ圧縮後に暗号化を行うなど、高スループットが得られる傾向にある。

②ソフトウェア暗号における性能

バックアップアプリケーション等ソフトウェアによる暗号化機能を使用してデータ暗号を行うもの。ソフトウェアで暗号化を行うためシステムへの負荷が高くなる。また、暗号化されたデータをテープドライブに書き込むためテープドライブのデータ圧縮効果が小さくスループットも低くなる傾向にある。テープライブラリ等を使用して、多重で暗号化処理が実施される可能性があるシステムの場合、多重処理実施時のシステム負荷についても考慮する必要がある。

(2) データの圧縮率

ハードウェア暗号とソフトウェア暗号を比較した場合、テープドライブのデータ圧縮効率に差異がある。テープドライブに実装されているハードウェア暗号機能を使用する場合、データ圧縮後に暗号化が実施されるため、データ圧縮効率は非暗号化時とほぼ同等の圧縮効率が得られる。一方、ソフトウェア暗号の場合、暗号化された後にテープドライブでデータ圧縮を行うためデータの圧縮効率が悪くなる傾向にある。

(3) 暗号強度

「暗号強度」はどのような暗号化アルゴリズムに準拠しているかによって決まるため、使用するデータ暗号方式が対応している暗号化アルゴリズムを事前に確認しシステム要件にあったものを選択する必要がある。例として LTO 5 ドライブのハードウェア暗号を使用する場合、現在の国際標準である AES-256 暗号（256 ビット強度の暗号方式）が使用される。

7.2.5. 暗号鍵の種類と管理・保存方法

(1) 暗号鍵の種類（タイプ）

データの暗号化システムを利用した実際の運用においては、様々な種類の暗号鍵が想定できるが、大きくは下記に分類できる。各々の例を下記に列挙するが、システムによってはこれ以外の例もあり得る。また、実在する具体的なシステム等を想定したものではなく、暗号鍵としての可能性も含めて列挙している。構築したいシステムに適した暗号鍵の種類を選択する。

所望のセキュリティを確保するには、対象となる鍵が不正使用されないよう適切に管理することが必要である。また、鍵の紛失はデータを損失することと等価なので、鍵を紛失しないよう適切な管理と保存が必要である。

① 物理的な鍵

Smart Card、 USB キーなど物理的な媒体を鍵として使用するもの。その物理的な鍵を厳重に管理・保管し、関係者以外からの物理的なアクセスを制限することが必要である。その物理的な鍵が何らかの原因で故障した場合、あるいは、紛失した場合の対応についても事前に調査・検討が必要である。例えば、同一の物理的な鍵を複数保持しておくのも、一つの手段となるであろうし、鍵の製造元が登録番号などから同一鍵を復旧可能であるなら、これも一つの手段となるかも知れない。ただし、利用者が許容可能な時間内で復旧できること、その復旧サービスがデータの保管期間にわたって利用可能なこと、不正な目的のために鍵を容易に複製できないことも、あわせて確認しておくことが望ましい。さらに、物理的な鍵の動作保証期間についても事前に検討することが望ましく、これがデータの保管期間より充分に長いことが望ましい。データの保管期間より短い場合は、定期的に物理的な鍵の媒体交換や、必要ならこれに伴うデータの復号と再暗号化を検討すべきであろう。

②電子データ（ファイル）による鍵

暗号鍵を電子データ（ファイル）の形式で供給・保存して使用するもの。例えば、対象となる鍵の電子データをシステムのハードディスク等に保存する場合は、それへのアクセス権限等を検討して関係者以外からのアクセスを排除することが必要である。保存したデバイスが故障や障害に遭遇した場合に備え、鍵の電子データのバックアップを持っておくことが望ましい。また、その保管しているシステムの動作保障期間、あるいは稼動予定期間とデータの保管期間との関係について事前に検討しておくことが望ましい。対象となる鍵を外部メモリ（デバイス）に保管する場合は①と同様に、物理的なアクセス、外部メモリの動作保障期間などについて事前の検討・配慮が必要である。一方、後述するセキュリティの観点では、鍵の電子データのバックアップが容易に作成できないことが必要である。

(2) 暗号鍵の設定方法

暗号鍵を設定する方法について、事前に調査・検討しておくべきである。この設定に対するセキュリティを含めて、構築したいシステムに適しているかどうかを検討する。

① 暗号鍵の設定はネットワーク経由
② 暗号鍵の設定はホストインターフェース（SCSI、Fibre Channel、SAS 等）経由
③ 暗号鍵の設定はテープライブラリ装置から直接

各設定方法で使用するインターフェースに障害が発生した場合、その影響が下記のどれに該当するかを事前に確認しシステム要件上許容できる範囲であるか検討しておく。

i 問題なし
ii 暗号鍵のインポート/エクスポート不可、データのバックアップ/リストアは可能
iii データのバックアップ/リストア不可

(3) 暗号鍵の同時使用数

同時に使用できる暗号鍵の数について、事前に調査・検討すべきである。考えられる可能性を下記に列挙している。万一、暗号鍵の漏えいが発生した場合やその可能性が疑われる場合、暗号鍵の付け替え（別の暗号鍵によるデータの再暗号化）が必要となる。暗号鍵に対応する暗号化データが大量にある場合、この作業に多大な時間と労力が集中的に発生することになる。これが許容可能かどうかを含めて、適切な暗号鍵の同時使用数を選択すべきである。

① 複数の暗号鍵を同時に使用可能
② 複数の暗号鍵を同時に使用不可（同時でなければ複数の暗号鍵の使用可）
③ 複数の暗号鍵の使用不可

(4) 暗号鍵の使用と管理方法

データの暗号化をしながらバックアップ/リストアを行う場合、暗号鍵の使用方法により鍵管理の方法が異なる可能性がある。下記の列挙のように大別でき、これらはシステム設計に依存する。①及び②の場合、暗号鍵の管理はシステム側に機能の一部として組み込まれていると言えるが、障害・災害時の対応やデータの保管期間の観点で鍵管理の要件が満たされているか調査・検討しておく必要がある。③

の場合、暗号化システムとは別に暗号鍵管理の運用を検討する必要がある。

① バックアップ/リストア時、暗号鍵の設定を意識しない（事前設定）
② バックアップ時のみ鍵の設定を意識する
③ バックアップ/リストア時共に暗号鍵の設定を意識する（暗号鍵管理はユーザ）
（暗号鍵の管理方法の確認が必要）

(5) 暗号鍵情報の冗長性

暗号鍵が何らかの障害や災害などで紛失することは、その鍵で暗号化されたデータを損失することと等価であるため、暗号鍵情報は冗長性が求められる。システム形態としては下記に列挙したものが考えられる。システムに求める要件により適切な形態を選択すべきである。

① 複数システムで暗号鍵管理情報をオンラインで共有
ネットワーク接続などにより暗号鍵情報を複数のシステムで共有し、１つの鍵管理システムがダウンしてもシステムとしては継続運用が可能。ネットワーク障害が発生した場合の影響範囲についても事前に確認が必要
② 暗号鍵情報はバックアップにより保存
③ 暗号鍵情報の保存手段なし
別途、運用管理者が暗号化システムの外で記録

(6) 暗号鍵のコピーは可能か

万一に備えて、暗号鍵のコピーが可能か事前に調査・検討すべきである。暗号化されたデータを暗号化された状態のまま、物理的に他のシステムに移行したりする場合、暗号鍵のコピーが必要となるので事前の調査・検討が必要である。

① オペレータが容易に可能
セキュリティの観点で、コピー作成の操作権限等について配慮が必要。
② システム開発元にコピーを依頼することで可能（Smart Card, USB キーのコピーなど）
許容可能な時間内でコピーを受領できるかどうかの検討も必要。

(7) 暗号鍵の格納場所

暗号鍵が格納されている場所について事前に調査し把握しておくべきである。一般的な例を以下に記す。暗号鍵の格納場所を把握することは鍵の漏えいを防止するための対策を検討したり、暗号鍵の冗長性を確保・検討したりするためにも必要である。

① カートリッジテープ/テープドライブ/テープライブラリ装置
暗号鍵情報の取り外し可能/不可
② バックアップサーバ
バックアップソフトの機能を使用、又は、暗号鍵管理ソフトの機能を使用
③ 暗号専用装置
暗号鍵情報の取り外し可能/不可

④ 暗号鍵管理システム
⑤ 暗号鍵を管理せず（都度、マニュアルで入力）
暗号鍵の入力方法の確認が必要

7.2.6. 暗号鍵のセキュリティ

(1) 暗号鍵のセキュリティ

暗号鍵の漏えいを防止するには、それへのアクセス権限を適切に設定するだけでなく、暗号鍵を別の鍵で暗号化しておくとさらに良い。暗号化システムや暗号化データに求めるセキュリティ性に依存して設計されるべきである。ただし、その暗号鍵を暗号化した鍵の管理が疎かであると、所望のセキュリティを満たせないこと、あるいは暗号鍵を復号できなくなり全データの損失につながることを充分に認識しておくべきである。

(2) 暗号鍵の持ち出し

暗号鍵が容易に取り出せない工夫がなされているかどうか事前に調査し、その機能が必要かどうか検討すべきである。可能性としては下記の通り。

① 物理的な鍵の場合： 容易に取り外せない機構になっているか
② 電子データの場合： 容易にエクスポートできないシステム的な設計(アクセス制限など)がなされているか

(3) 暗号鍵の有効期間

一般的に、同一の暗号鍵を長期間使い続けると暗号鍵が不正に解読されるリスクが高まる。この観点から例えばアメリカ合衆国の国立標準技術研究所（NIST）は定期的な暗号鍵の付け替えを推奨している[3]。同様な理由によりシステムによっては暗号鍵に有効期間を設けている場合があり得るだろうし、あるいは、積極的にそのようにシステム設計をすることが望まれる場合もあり、事前の調査・検討が必要である。

① 暗号鍵の有効期間がある場合
時間に対する有効期間か、イベント（ライブラリからカートリッジテープを取り出したい時など）による有効期間か。有効期間が切れる前にそれを検知もしくは通知する仕組みがあるか。有効期間が切れた場合の対処方法はどうなっているか（有効期間が切れる前に対象データの復号と再暗号化が必要なのか、切れた後でもデータの復号と別暗号鍵での再暗号化が可能なのか等）。
② 暗号鍵の有効期間がない場合
システム自体に暗号鍵の有効期間の概念がない場合でも、運用として有効期間の概念を取り入れることが望ましい場合、暗号化システムの運用ルールでこれを網羅できているか。

(4) 暗号鍵の変更

前項の理由により暗号鍵を変更することが必要になることもあるだろうし、あるいは、一部の暗号化データを他のシステムに暗号化した状態でエクスポートする場合に対象データの暗号鍵をエクスポー

ト先に合わせて変更（つまり再暗号化）することが必要になることがある。この観点でも事前に調査・検討しておくべきである。

① 同一カートリッジテープ上で使用する暗号鍵の変更が可能
暗号鍵変更後、正常に変更前後のデータのリストアが可能か、つまり、暗号鍵を変更されたデータは最新の暗号鍵でのみ復号可能で、暗号鍵を変更していないデータは変更前の暗号鍵でのみ復号可能であること。同一カートリッジテープ上で対応する暗号鍵が一つに限定される場合は、最新の暗号鍵でのみ復号可能なこと。
最新の暗号鍵で書いたデータしか読めないという制限などないか確認する必要がある。

② 同一カートリッジテープ上で使用する暗号鍵の変更が不可能
暗号鍵の変更のためには、別のカートリッジテープにデータを移行しながら実施することが必要。この場合、①に比較して相対的に多くの作業時間を要することになる。保持している暗号化データの量と暗号鍵の変更頻度とを考慮し、この作業がシステムや作業者の許容範囲内であるかどうかを事前に見積もっておく必要がある。許容範囲を超える場合、システムの増強や①の可能性について検討することが望ましい。

7.2.7. コスト

(1) 導入コスト

データ暗号化を導入することによる導入コストの検討は、暗号化の方法（「ハードウェア暗号」「ソフトウェア暗号」）及び7.2.5項で述べた暗号化に使用する暗号鍵の運用管理方法を考慮する必要がある。ハードウェア暗号を使用する場合、ハードウェア暗号に対応した機器（テープドライブなど）の導入コスト、及びハードウェア暗号を使用するためのミドルウェアオプションライセンス有無の確認が必要となる。ソフトウェア暗号を導入する場合、ソフトウェアの暗号化ライセンスコストに加え、ソフトウェア暗号実施によるシステム負荷増を見据えたシステム設計（CPU 数の増など）が必要となる。また暗号鍵の管理、運用に「鍵管理システム」など専用機器を導入する場合は、それらも含めたトータル導入コストの検討が必要である。

(2) 運用コスト

データ暗号化システムの運用コストを検討する場合、暗号鍵の管理、運用についても考慮する必要がある。暗号鍵の数を増すことや、鍵の変更を頻繁に行うことでセキュリティレベルを高くすれば運用も複雑になり運用コストも高くなる傾向にある。導入するシステム要件に対して最適なセキュリティレベルを選択することが重要となる。

7.3. 運用

テープバックアップは人為障害やシステム障害、被災等の対応のため実施するが、暗号化の目的は書き込まれるデータを安全に保管することにある。そのためバックアップデータの暗号化のために以下の検討を行う必要がある。

7.3.1. バックアップ方法

(1) 暗号化/復号の手順の明確化

データのバックアップに暗号化を導入する場合、通常のバックアップ運用の検討に加えて暗号鍵の設定、管理の運用確認が必要となる。

① 鍵管理を行うシステムのセットアップ方法や暗号鍵の設定方法を確認する

② バックアップソフトでデータ暗号化を行う場合、暗号化の設定手順を確認する。暗号化を使うことで生じる制限事項等がないかを確認する。

(2) 鍵管理システムの管理

鍵管理システムを導入する場合、その管理は安全に暗号化システムを運用する上で重要である。鍵管理システムの機能を確認し、必要であれば機能毎に管理者を割り当てる必要がある。以下に機能毎の管理者割り当て例を記す。

① 暗号鍵管理システム設定を行う管理者

② 暗号鍵を管理する管理者

③ 暗号化のバックアップ運用を行う管理者

7.3.2. 暗号化状態の確認

暗号化システムの運用を行う場合、セキュリティが確保されているか監査する必要がある。正しくデータ暗号化運用が行われているか確認する手段を事前に確認し、その確認を定期的に行うことが必要である。例としてバックアップソフトや鍵管理システムのログ情報を参照し、データ暗号化が実施されていることを確認するなどの方法がある。

7.3.3. 定期的メンテナンス

暗号化システムの運用を行う場合、暗号鍵のメンテナンス方針、暗号鍵に対するカートリッジテープの管理方法を事前に検討しておく必要がある。

(1) 鍵情報のメンテナンス

セキュリティを考慮し定期的に暗号鍵を更新する場合、更新する暗号鍵の範囲及び更新に伴う影響度、更新手順、更新された使用済み暗号鍵の取り扱いを明確にしておく必要がある。また、更新後正しく暗号鍵が更新され、使用できるか確認することも重要であり、更新手順には更新後の動作確認手順も含める必要がある。

(2) カートリッジテープの管理

暗号化システムでデータを暗号化してカートリッジテープにバックアップする場合、そのカートリッジテープのバックアップにどの暗号鍵が使用されたのかを管理する必要がある。カートリッジテープにバーコードラベル等、管理番号を記し暗号鍵と相関がとれるよう運用することが必要となる。

例としてバックアップソフト等を使用して運用する場合、バーコードラベルの内容やカートリッジテープの管理領域に書かれたメディア ID 等と暗号鍵の管理情報をバックアップソフトが保持している

ことが一般的であるため、その管理情報をバックアップするなどして失わないようにすることも重要な管理項目となる。

カートリッジテープが何らかの問題で読み出し不可となった場合を考慮し、複数本のカートリッジテープに同じデータをバックアップすることもデータ保護の面では有効な手段である。

7.4. 障害/災害

暗号化システムの暗号化機能が正常に機能していることを確認するためエラー情報、ログ情報の確認、取得手順を事前に確認する必要がある。また、災害復旧手順についてもシステム要件を踏まえた上で事前検討を行う必要がある。

7.4.1. 障害確認方法

暗号化機能がハードウェア障害等で正常に動作しないときにエラー情報やログ情報がどのように出力されるか事前に確認する必要がある。障害が発生した場合、エラー情報及びログ情報は、障害範囲の特定において重要な情報となる。出力される情報が障害部位、範囲の特定において極端に不足していないかなどシステム要件上問題ないか確認が必要である。また、運用時にログ情報を定期チェックすることも検討する必要がある。

7.4.2. リカバリ方法

暗号化システムにおいて人為障害、システム障害、暗号鍵の漏えい等、障害発生時のリカバリ方法を事前に検討、配慮しておく必要がある。以下に障害例を挙げるが導入するシステムにおいて、どのような障害が考えられるかも事前に検討しておく必要がある。

(1) 人為障害

人為障害としては「暗号鍵を忘れる」「暗号鍵を誤って消去、削除する」などが考えられる。
リカバリ方法としては「7.2.5 項 暗号鍵の種類と管理・保存方法」で述べた「暗号鍵の設定方法」「暗号鍵情報の冗長性」「暗号鍵のコピーは可能か」を確認し、人為障害へのリカバリ方法を明確にしておく必要がある。

(2) システム障害

ハードウェア故障などシステム障害に対する暗号鍵のリカバリ方法として「7.2.5 暗号鍵の種類と管理・保存方法」で述べた内容を事前に確認する必要がある。

① ハードウェア交換対応について

ハードウェア故障に伴い装置の保守交換などが発生した場合、システム自体の復旧、再設定手順を明確にしておく必要がある。例としてバックアップソフトの暗号化機能を使用したシステム構成の場合、システムバックアップにディザスタリカバリ機能を使用してシステム全体をバックアップするケースがあるが、ディザスタリカバリ機能でのシステム復旧において暗号鍵情報まで復旧されるか事前に確認する必要がある。暗号鍵情報の復旧がディザスタリカバリに含まれない場合、システムリカバリ後に別途、暗号鍵情報をリカバリする手順が必要となる。

② システムで暗号化したカートリッジテープの読み込みについて

システム障害発生時の対応として暗号化データが記録、保存されたカートリッジテープを別システムで読み込む必要がある場合、暗号鍵情報のシステム間受け渡し方法を確認しておく必要がある。

読み出したいデータを復号するには暗号鍵を渡す必要があるため、暗号化データに対応する暗号鍵の特定手順も明確にしておく必要がある。

(3) 暗号鍵の漏えい

暗号鍵が漏えいした場合やその可能性が疑われる場合、暗号鍵の付け替え（別の暗号鍵によるデータの再暗号化）が必要となる。以下に暗号鍵の付け替え手順例を記す。

① 暗号鍵の漏えい（又は漏えいの疑い）あり
② 漏えいした暗号鍵の使用範囲特定（その暗号鍵で暗号化されたデータ範囲の明確化）
③ 対象範囲の暗号化データのリストア（漏えいした暗号鍵でのデータ復号）
④ 新たに設定した暗号鍵でのデータ再暗号化
⑤ 漏えいした暗号鍵の使用停止処理（又は暗号鍵情報の廃棄）

7.5. データ移行

7.5.1. 鍵のライフサイクル

データを暗号化するための暗号鍵は、鍵の生成段階から廃棄に至るまでをライフサイクルとして捉えることができる。そのライフサイクルにおいては、鍵は幾つかの状態（ステート）と状態遷移に分類できる。システムを構築する際には、想定される鍵の状態と状態遷移にどのような要件が必要かを検討することが望ましい。

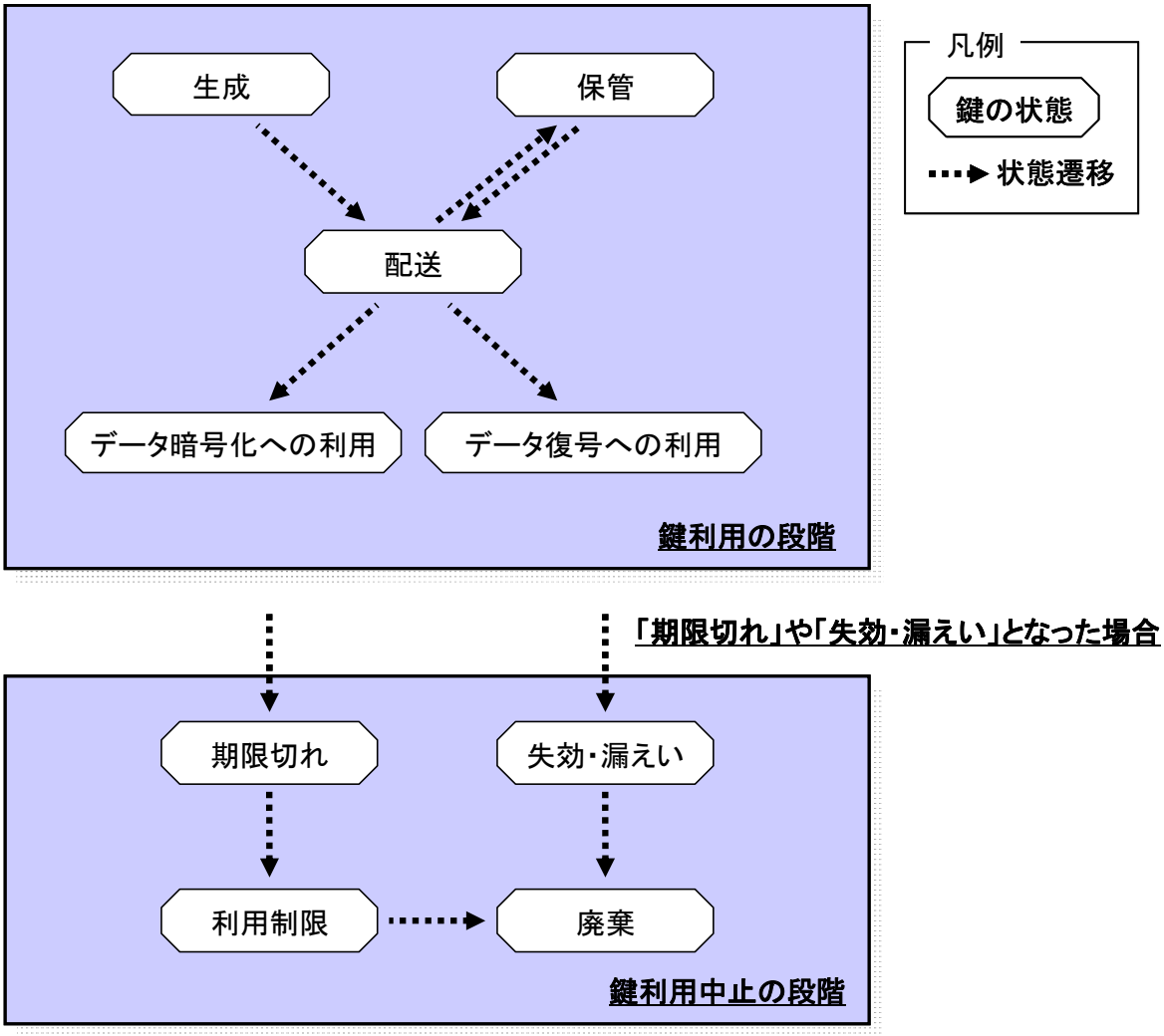


図 7-6　鍵のライフサイクル：　鍵の状態遷移のモデル

図 7-6 は、鍵のライフサイクルの状態遷移をテープストレージに適した形で表現したものである。なお、図に示したモデルはより良いシステムの構築・運用の助けとなるよう概念的に示したものであり、ここではその厳密性を問わない。他にも状態遷移を表すモデルがあり[3][8][9]、適宜参照すると良い。

各状態について以下に簡単に説明する。

生成

鍵を生成する段階で、まだ鍵をデータの暗号化等に利用していない状態。

配送

鍵を生成又は保管しているシステムから他のシステム（例：データの暗号化を実施するシステム等）に鍵を配送する状態。広義には、鍵のエクスポート、インポートを含む。

保管

データの暗号化・復号に備えて鍵が利用可能なように保管している状態。

データ暗号化への利用

実際に鍵を利用してデータを暗号化する状態。

データ復号への利用

実際に鍵を利用してデータを復号する状態。

期限切れ

同一の鍵を長期間にわたってデータの暗号化に利用し続けたり、多量のデータの暗号化に利用し続けたりすると鍵の漏えいに対するリスクが高まる。これを防止するためは、鍵のデータ暗号化への利用に期限を設けたり、使用回数に制限を設けたりすることが望ましい。ここでは、この期限が切れた状態を指す。この状態では、同一鍵を使って新たなデータを暗号化すべきでないが、データの復号には利用できる。

利用制限

鍵をデータの復号のみに利用制限する段階。この段階では、鍵は新たなデータの暗号化には利用しない。

失効・漏えい

外部（例：他企業）との間で暗号化したデータを交換するため鍵を外部に出したりして鍵が失効したような場合や、ある鍵で暗号化されたデータが全て削除されたり、不要になったりした状態。あるいは、何らかの理由で鍵が外部に漏えいしたような状態。このような状態では、該当する鍵を使用して新たなデータを暗号化すべきでなく、また、該当する鍵で既に暗号化されているデータは別の鍵により再暗号化するなどの処置を取ることが望ましい。

誤って同じ鍵を再度生成してしまうことを防止するため、鍵は不要になっても過去の鍵情報として保持しておくことが望ましい。また、鍵を保持しておけば、万一、不要になったはずのデータを復号する必要が生じた場合にも、限定的にデータの復号に利用できるであろう。

廃棄

完全に鍵を廃棄（削除）する状態で、一旦廃棄した鍵は元に戻せなくなってしまう状態。

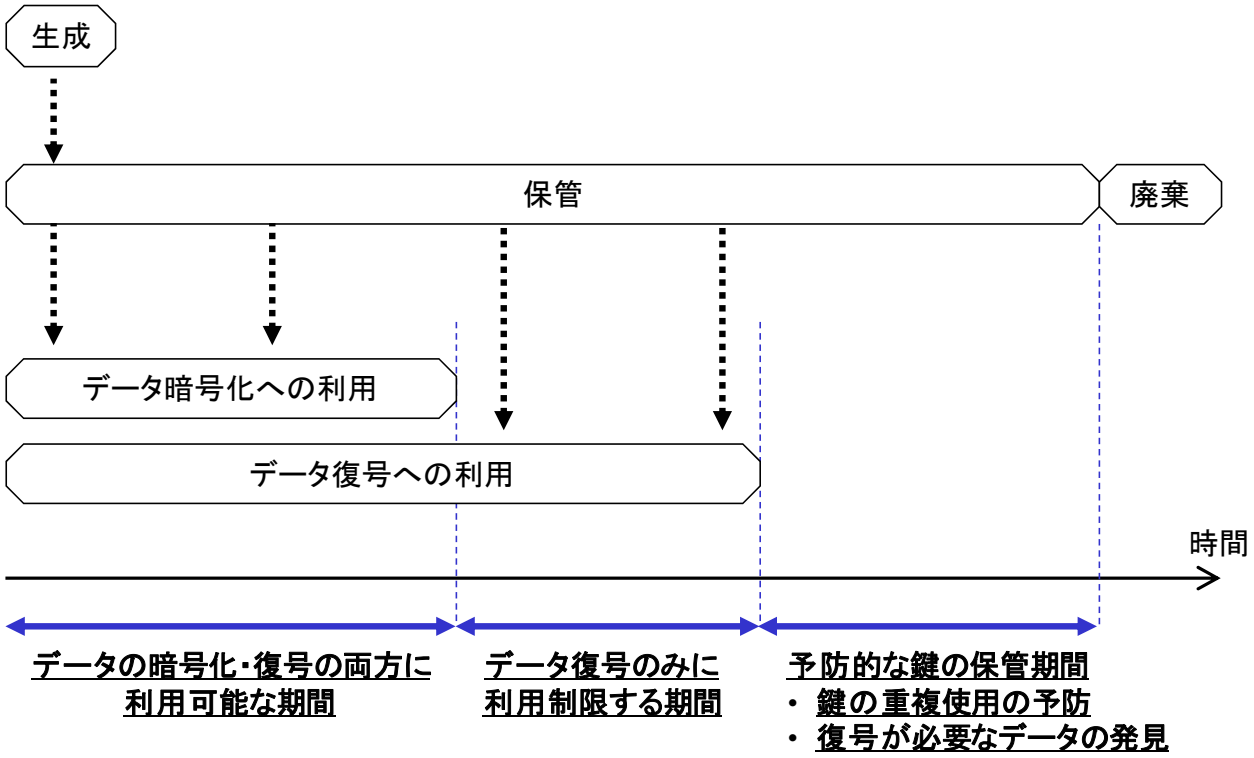


図 7-7　鍵のライフサイクル：　時間軸で捉えた場合の鍵の状態遷移のモデル

図 7-7 は鍵のライフサイクルを時間軸で表した場合のモデルである。図 7-6 に示した鍵の各種状態の内、図 7-7 に示すのが困難なものは表示していない。鍵が生成されてからの最初の期間では、鍵はデータの暗号化と復号の両方に利用されるが、期限に達した段階からデータの復号のみに利用制限した方が良い。

最後の予防的な鍵の保管期間では、該当する鍵そのものの利用は不要なはずだが、誤って重複した鍵を再度生成することを防止したり、万一復号が必要なデータが発見された場合に備えたりするため鍵の保管を続けるような期間である。このような期間は必須ではないが、検討することが望ましい。

7.5.2. 他システムとのデータ交換

暗号化してあるカートリッジテープのデータを他システムとの間でデータ交換する場合について考える。なお、ここでのデータ交換は、例えば遠隔システムとの間や企業間など、独立したシステムとの間のデータ交換を意図している。しかし、将来、システムが老朽化してシステムを移行しようとする際に同様のデータ交換の作業が必要になる場合もあるので、現時点でデータ交換が必要なくてもシステム導入時にデータ交換について検討しておくことが望ましい。

他システムとのデータ交換の方法は下記の 3 つに大別できる。

①暗号データのまま交換

データは暗号化した状態のままで、復号に必要な暗号鍵を交換する

②他システムに合わせて再暗号化して交換

暗号化データに互換性がない場合に、データを他システムに合わせて再暗号化した後、復号に必要な

暗号鍵を交換する

③ 通常データ（非暗号）で交換

データ交換前に一旦復号し、復号したデータを交換する。通常データで交換する場合、暗号化データの観点において他システムとの互換性の可否を検討しなくて良いが、データの移送時にデータ漏えいのリスクを伴う。データ漏えい防止の観点では、暗号化データで交換することが望ましい。

以下では、暗号鍵の交換の観点でまとめる。

7.5.3. 他システムとの暗号鍵の交換

① 暗号鍵の交換が可能

鍵交換を電子ファイル等で実施する場合

鍵をエクスポートしたり、インポートしたりする方法が明確であり、そのデータフォーマットに両者で互換性があることが必要。互換性がない場合、鍵データの変換方法が明らかであるか、もしくは、両者のデータフォーマットが判明していて変換方法を確立することが可能であることが必要。その際には、鍵交換に必要な情報が何であるかが明らかであることが必要。

実際に該当する電子ファイル等を送受する場合は、その電子ファイル等をさらに一時的に暗号化しておくことが望ましい。

物理的な鍵を使用する場合

自システムでも物理的な鍵を使用している場合は、鍵を交換する際の影響についての検討が必要。例えば、予備の鍵があるか。あるいは、鍵の移送時に鍵が紛失することもあり得るが、その場合にもデータ漏えいのリスクに影響ないかどうか。

どちらにも共通する項目

鍵の移送時に鍵が紛失した場合に備えて、データ交換の対象でないデータ（自システムに残しておくデータ）は交換される暗号鍵と異なる鍵で暗号化されていることが望ましい。万一、同じ暗号鍵で暗号化されている場合は、どちらかのデータを別の鍵で再暗号化した方が良い。場合によっては、このために対象となるデータ全てに対して復号と暗号化の処理が必要となり、そのデータ量が多い場合は相当の時間を要することになるので、適切な単位で異なる暗号鍵を使用するような運用を心がけておくことが望ましい。

もし、システム的な要件で暗号鍵の付け替えができない場合は、暗号鍵の交換により自システムのデータが漏えいの危険にさらされることになるとも言えるので、システムの導入段階からの検討が望まれる。

また、鍵交換により他の影響がないかどうか（例：交換前の鍵が使用できなくなる）の事前調査も必要であろう。どの場合においても、実際にテスト等を行い、実運用に問題のないことを検証しておくことが望ましい。

② 暗号鍵の交換が不可能

データ交換はデータを復号して行う必要があるが、データ漏えいのリスク等の観点で許容可能かどうかの検討が必要。

7.6. 終了/停止

暗号化システムの運用を終了/停止する場合、カートリッジテープに保存されていた個人情報等の機密情報が将来外部に流出しないよう、適切な措置を施す必要がある。ここでは暗号化システムの運用が終了/停止した後においても情報の漏えいを防ぐ必要がある場合において、適切な対応方法を説明する。

7.6.1. 暗号化された情報の消去と消去確認方法

暗号鍵を適切に管理していれば、カートリッジテープに書き込まれたデータが解読されることは、現在の技術では考え難い。しかし暗号技術や暗号解読技術は年々進化しており、現在の技術で解読困難と判断していても、将来容易に解読可能になる可能性も考えられる。したがって暗号化したカートリッジテープを廃棄する場合には、適切な対応が必要になる。磁気記憶媒体（磁気テープや磁気ディスク）に記録されたデータは、単純な上書きやフォーマットだけでは完全にデータを抹消することができない。またデータが完全に消去されていることを確認することも困難である。しかし磁気テープは磁気ディスク等他の媒体に比べると取り扱いが容易（金属部品を殆ど含まず、装置からの取り出しも容易）であることから、廃棄時は物理的な破壊、もしくは専門業者に焼却/溶解処理を依頼し、記録されているデータを読み出せなくすることを推奨する。

7.6.2. 暗号鍵設定情報の消去

暗号鍵の設定情報は適切に消去する必要がある。特に設定情報を紙で保管していた場合には、用紙を焼却/溶解処理することを推奨する。設定情報を PC に保管していた場合には、以下の資料を参考に暗号鍵設定情報を消去/廃棄することを推奨する。

パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項[10]

7.6.3. 暗号鍵の使用終了/消去

暗号化システムには、データを暗号化する装置（テープドライブやサーバ）とは別に、暗号鍵を生成管理する専用の装置が存在する場合がある。何れの装置も運用を終了する場合には、適切に暗号鍵を抹消する必要がある。特に暗号鍵を専用の管理装置で保管している場合には、その装置の仕様に従い装置付属の説明書を参照もしくは、装置ベンダーに問い合わせの上、適切に暗号鍵情報を抹消する必要がある。

参考文献

[1] NPO 日本ネットワークセキュリティ協会, 2011 年情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～ 第 1.2 版

[2] JEITA テープストレージ委員会,「テープシステム技術資料 第 1 章 テープストレージの未来」

[3] National Institute of Standards and Technology (NIST), Recommendation for Key Management (NIST Special Publication 800-57), 2007 年 3 月

[4] 内閣官房情報セキュリティセンター (NISC),「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」 , 2012 年 10 月

[5] 経済産業省 情報セキュリティ関連ガイドライン, 情報セキュリティ管理基準 (平成 20 年改正版)

[6] 内閣府国民生活局企画課 個人情報保護推進室, 個人情報保護法に関するよくある疑問と回答, 平成 21 年 6 月 25 日

[7] 内閣府 防災担当 , 事業継続ガイドライン 第二版 わが国企業の減災と災害対応の向上のために , 平成 21 年 11 月

[8] 独立行政法人 情報処理推進機構, 安全な暗号鍵のライフサイクルマネージメントに関する調査鍵管理ガイドライン (案), 2008 年 7 月

[9] IEEE P1619.3, Draft Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data, 2009 年 2 月

[10] 電子情報技術産業協会, パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項

付録　チェックリスト（暗号化するシステム考慮点のまとめ）

項#	リスト対象者			フェーズ	チェック項目	内容概要	解説章	チェック欄	達成したい機密性・厳密性	
	運用者	構築者	統括者						低	高
1				検討/計画			7.1			
					システム全体の位置付け		7.1.1			
1-1			●		対象と考えるITシステム範囲	データ暗号化を導入する対象システム範囲の明確化			●	●
1-2			●		外部との情報交換	外部とのデータ交換有無/範囲の明確化			●	●
1-3			●		個人情報の有無	対象データに個人情報が含まれるか			●	●
1-4			●		情報資産目録	対象データの情報資産目録確認			●	●
1-5			●		想定される脅威	運用上どのような脅威が想定されるか			●	●
1-6			●		事業継続	事業継続の必要性判断			●	●
					何を守るか・どう守るか		7.1.2			
1-7			●		守るべきデータの範囲	暗号化対象となるデータ範囲の明確化			●	●
1-8		●	●		現行システムの問題点	情報漏えいに対する現行システムの問題点確認			●	●
1-9		●	●		リスクの検討	万一の場合のリスク検討			●	●
1-10			●		関連法規の有無	関連省庁からの監督指針やガイドラインの有無確認			●	●
1-11			●		情報漏えい保険	情報漏えい保険の検討				●
1-12		●	●		他社、同業者の動向	技術動向に対する確認及び対応の検討				●
2				設計/構築			7.2			
					暗号化の対象		7.2.1			
2-1		●	●		暗号化の対象	どこにあるデータを暗号化するか？ ①　テープに書き込んだデータを暗号化 ②　ディスクに保存するデータの暗号化 ③　テープ以外のリムーバブル媒体に対する暗号化 ④　データ転送経路の暗号化 ※②～④については、本チェックリストの対象外			●	●

テープストレージの暗号化機能に関するチェックリスト

項#	リスト対象者			フェーズ	チェック項目	内容概要	解説章	チェック欄	達成したい機密性・厳密性	
	運用者	構築者	統括者						低	高
2-2		●	●	設計/構築	データ暗号化の単位	どのような単位で暗号化するか？ ①　ジョブ単位での暗号化 ②　メディア単位での暗号化 ③　ライブラリ装置のスロット単位での暗号化 ④　メディアプール単位での暗号化	7.2.2		●	●
					暗号化の実現方法		7.2.3			
2-3		●	●		暗号化手段の種別	ハード、ソフトどちらの方法で暗号化を実現するか （ハードウェアの暗号化機能のサポート有無確認）			●	●
2-4		●	●		暗号化の実現方法	どのように暗号化を実現するか？ ①　バックアップソフトの機能を使用 ・どのオプションが必要か確認要 ②　バックアップソフト以外の機能を使用 (ア)テープ装置、鍵管理システムなど (イ)バックアップソフトへの影響などの確認			●	●
					暗号化の性能		7.2.4			
2-5		●	●		暗号化のスループット	データ暗号化を実施した場合のデータスループット検討 （S/W 暗号を行う場合システム負荷の考慮も必要となる）			●	●
2-6		●	●		データの圧縮率	データ暗号化を実施した場合のデータ圧縮率検討 （S/W 暗号を行う場合、データ圧縮効率が悪くなる傾向あり）			●	●
2-7		●	●		暗号強度	使用する暗号アルゴリズム強度がシステム要件を満たしているか？			●	●
					暗号鍵の種類と管理・保存方法		7.2.5			
2-8	●	●	●		暗号鍵の種類（タイプ）	使用する暗号鍵の種類を確認する ①　物理的な鍵（Smart Card, USB など） ②　電子データによる鍵（ファイル）			●	●

テープストレージの暗号化機能に関するチェックリスト

項#	リスト対象者			フェーズ	チェック項目	内容概要	解説章	チェック欄	達成したい機密性・厳密性	
	運用者	構築者	統括者						低	高
2-9	●	●	●		暗号鍵の設定方法	暗号鍵の設定方法を確認する ① ネットワーク経由で設定 ② ホスト I/F（SCSI、FibreChannel 等）経由で設定 ③ テープライブラリ装置から直接設定			●	●
2-10		●	●	設計/構築	暗号鍵の同時使用数	同時に使用できる暗号鍵の数を確認する ① 複数の暗号鍵を同時に使用可能 ② 複数の暗号鍵を同時に使用不可（鍵の更新は可能） ③ 複数の暗号鍵の使用不可	7.2.5			●
2-11	●	●	●		暗号鍵の使用と管理方法	運用時の暗号鍵使用方法を確認する ① バックアップ/リストア時、暗号鍵の設定を意識しない（自動で選定され Job 毎にユーザでの鍵指定は不要） ② バックアップ時のみ鍵の設定を意識する ③ バックアップ/リストア時共に暗号鍵の設定を意識する（使用する暗号鍵の指定はユーザが実施する）			●	●
2-12	●	●	●		暗号鍵情報の冗長性	暗号鍵の冗長性、バックアップ手段を確認する ① 複数の鍵管理システムで暗号鍵を管理する （LAN 等オンラインで複数の鍵管理システムにより鍵情報を共有する） ② 暗号鍵情報はバックアップにより保存 （バックアップ方法を確認要） ③ 暗号鍵情報の保存手段なし （運用管理者が暗号システム外で記録等を検討）			●	●
2-13		●	●		暗号鍵のコピーは可能か	暗号鍵のコピーが可能かどうか確認する ① オペレータが容易に可能 ② ベンダーにコピーを依頼することで可能 （Smart Card, USB のコピーなど）				●

テープストレージの暗号化機能に関するチェックリスト

項#	リスト対象者			フェーズ	チェック項目	内容概要	解説章	チェック欄	達成したい機密性・厳密性	
	運用者	構築者	統括者						低	高
2-14	●	●	●	設計/構築	暗号鍵の格納場所	暗号鍵情報の格納場所を確認する。 ＜暗号鍵 格納場所＞ ①　テープ/ライブラリ装置 ②　バックアップソフト ③　暗号専用装置 ④　暗号鍵管理システム ⑤　暗号鍵を格納せず（暗号化実施の際、マニュアルで入力） （※暗号鍵の入力方法の確認が必要）	7.2.5		●	●
					暗号鍵のセキュリティ		7.2.6			
2-15		●	●		暗号鍵のセキュリティ	暗号鍵情報は暗号化されているか				●
2-16		●	●		暗号鍵の持ち出し	暗号鍵を容易に取り出せない工夫がなされているか				●
2-17	●	●	●		暗号鍵の有効期間	暗号鍵の有効期限があるか ①　暗号鍵の有効期間がある ・有効期間の設定内容確認 ・有効期限が切れた場合の対処方法確認 ②　暗号鍵の有効期間がない			●	●
2-18		●	●		暗号鍵の変更	暗号鍵変更時の制限事項確認 ①　同一媒体上で使用する暗号鍵の変更が可能 →暗号鍵変更後、変更前後のデータリストアが可能か ※最新の暗号鍵で書いたデータしか読めないということはないか ②　同一媒体上で使用する暗号鍵の変更が不可能				●
					コスト	暗号化導入を考慮したコスト検討	7.2.7			
2-19		●	●		導入コスト	7.2.3 章で確認した暗号化の方法を考慮した導入コストの確認			●	●
2-20		●	●		運用コスト	7.2.5-7.2.6 章で確認した暗号鍵の管理を考慮した運用コストの確認			●	●
3				運用			7.3			
					バックアップ方法	対人為障害、システム障害、被災対応等	7.3.1			

テープストレージの暗号化機能に関するチェックリスト

項#	リスト対象者			フェーズ	チェック項目	内容概要	解説章	チェック欄	達成したい機密性・厳密性	
	運用者	構築者	統括者						低	高
3-1	●	●	●		暗号化/復号化手順の明確化	暗号化機能に関するセットアップ、バックアップ手順確認			●	●
3-2		●	●	運用	鍵管理システムの管理	鍵管理システムを導入する場合、どのような権限の管理者割り あてを行うか確認				●
					暗号状態の確認	媒体のデータ暗号状態確認	7.3.2			
3-3	●	●	●		媒体の暗号状態の確認	データが暗号化されていることの確認手段を確認 ①　暗号状態の確認が可能 →手順の明確化 ②　暗号状態の確認が不可 →暗号状態を確認する必要はないか検討			●	●
					定期的メンテナンス	暗号鍵の定期メンテナンス	7.3.3			
3-4	●	●	●		鍵情報のメンテナンス	①　暗号鍵情報の更新など定期的なメンテナンスが必要か →必要な場合、メンテナンスする項目は明確か ②　媒体と暗号鍵の相関管理 →暗号時に使用した暗号鍵と媒体の相関管理を確認			●	●
4				障害/災害			7.4			
					障害確認方法	暗号化に関するエラー情報・ログ情報	7.4.1			
4-1	●	●	●		暗号に関するエラー情報	どこに、どのようにエラー情報が表示、出力されるか確認 （暗号化に関するエラー表示はどのようなものがあるか）			●	●
4-2		●	●		暗号に関するログ機能	暗号化に関するログ出力確認 ①　暗号の動作状態を示すログが出力される →ログ内容は充分なものか ②　暗号の動作状態を示すログが出力されない →ログが出力されないことは問題ないか			●	●
					リカバリ方法	人為障害、システム障害、暗号漏えい等	7.4.2			
4-3	●	●	●		人為的障害	想定される人為的障害に対するリカバリ方法、手順の確認			●	●

テープストレージの暗号化機能に関するチェックリスト

項#	リスト対象者			フェーズ	チェック項目	内容概要	解説章	チェック欄	達成したい機密性・厳密性	
	運用者	構築者	統括者						低	高
4-4	●	●	●		システム障害	ハードウェア故障などの想定されるシステム障害に対するリカバリ方法。手順の確認。 （ハードウェア故障に伴う保守作業時（機器の交換）のリカバリ手順の確認）			●	●
4-5	●	●	●		暗号鍵の漏えい	暗号鍵漏えい時の対応手順確認			●	●
5				ﾃﾞｰﾀ移行			7.5			
					鍵のライフサイクル		7.5.1			
5-1		●	●		暗号鍵のライフサイクル	システムの運用要件を考慮した暗号鍵のライフサイクル確認			●	●
5-2		●	●		他システムとのデータ交換	他システムとのデータ交換有無確認	7.5.2			●
5-3		●	●		他システムとの暗号鍵交換可否	他システムとの暗号鍵交換の確認 ① 暗号鍵の交換が可能 →鍵交換に必要な情報は何か、交換方法は →鍵交換の影響はないか ② 暗号鍵の交換が不可能 →暗号鍵の交換は必要ないか	7.5.3			●
6				終了/停止			7.6			
					暗号化された情報の消去と消去確認方法		7.6.1			
6-1	●	●	●		暗号化情報の消去、廃棄	テープ媒体の消去、廃棄方法の確認				●
					暗号鍵設定情報の消去	鍵管理業務の終息、中断、データ漏えいからの防御	7.6.2			
6-2	●	●	●		暗号鍵設定情報の消去	暗号鍵設定情報の消去手順確認 ① 暗号鍵のデータベースなど暗号情報の消去方法がある ② 暗号鍵設定情報の消去方法がない →システム移設、廃棄時の暗号情報はどうするか （媒体のフォーマット？）				●

テープストレージの暗号化機能に関するチェックリスト

項#	リスト対象者			フェーズ	チェック項目	内容概要	解説章	チェック欄	達成したい機密性・厳密性	
	運用者	構築者	統括者						低	高
6-3	●	●	●		暗号鍵の使用終了/消去	暗号鍵の消去手順確認 ①　暗号鍵の消去方法がある ②　暗号鍵設定情報の消去方法がない →システム移設、廃棄時の暗号情報はどうするか （媒体のフォーマット？）	7.6.3			●