「秘密分散技術（一般名称：電子割符）登録制度」

―　事前チェックシート　―

―初版―

２０１７年　０１月０６日

秘密分散法コンソーシアム

序文

本資料は、我々コンソーシアムと関係省庁等との意見交換の中で、消費者保護等の観点から立ち上げることとなった秘密分散技術（電子割符）の技術等登録制度に関し、別途公開されている資料（参考１、２）の技術概要、更には我々コンソーシアムが継続的に関係省庁等への確認等を実施してきた内容等を充足させる技術を基にして、その技術等の登録を行おうとする者が事前チェックを円滑に行えるように準備された資料である。特に、下記参考資料や内閣官房情報セキュリティセンター（現・内閣サイバーセキュリティセンター、ＮＩＳＣ）から初版の解説書（注）に秘密分散技術が記載公表された当時の情報環境から比べると、更にＩＣＴ等の市場普及が進んだことと、クラウド利活用や激甚災害対処、法令対処等のニーズの高まりもあり、そうした各用途別に適切な秘密分散技術の選択が可能にすることが急務と考えられたことも背景として存在する。

基本的な秘密分散技術の概念図等は、巻末の参考資料図１基本的な秘密分散技術の処理概要や図２単純なファイル分割、図６秘密分散技術区分概念鳥瞰図を参照のこと。

参考：

１、ＥＣにおける情報セキュリティに関する活動報告書 2009

（情報セキュリティＷＧ：ＳＷＧ１／ＳＷＧ２／ＴＦの各報告書）

（現：一般財団法人日本情報経済社会推進協会（JIPDEC）公開資料）

https://www.jipdec.or.jp/archives/publications/J0004291

ＴＦ報告書が秘密分散技術の初期ガイドラインです。

２、秘密分散技術（電子割符）の標準化に向けたガイドライン

（秘密分散法コンソーシアム）

http://www.sss-c.org/?p=165

「秘密分散技術（一般名称：電子割符）の説明書」―　概要説明書　―

http://www.sss-c.org/wp-content/uploads/2016/03/gideline_20160229.pdf

注：

NISD-K303-052C　政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版(全体版初版))　解説書　内閣官房情報セキュリティセンター　**3.2.4** 情報の移送

http://www.nisc.go.jp/active/general/pdf/k303-052c.pdf

NISD-K305-111C　政府機関の情報セキュリティ対策のための統一技術基準（平成 24 年度版）　解説書　内閣官房情報セキュリティセンター　2.3.2.3 サーバ装置

http://www.nisc.go.jp/active/general/pdf/K305-111C.pdf

改定履歴　バージョン、改定概要、改定日

1.0.0、一般公開

「秘密分散技術（一般名称：電子割符）登録制度」―事前チェックシート―初版－、2017,01,06,

１．登録制度の趣旨

当コンソーシアムが２００２年より技術標準化を推進している秘密分散技術（一般名称：電子割符）は、大きな概念で言えば対象データを分割することによる、情報セキュリティの確保に資する基礎技術と言える。しかし、単なるファイル分割では昨今の法令要求事項（中長期間の安全性確保等）や情報処理能力の向上、暗号解読手法の高度化等のノウハウを用いた不正な解読等の攻撃に耐えられない。そこで、我々は本当に安全な技術実装を標準化すべく、多様なモデルの技術実装もファミリーとして扱えるよう技術標準化に向けた活動を継続してきた。しかし当初参画していた複数の当該基礎技術等の研究開発等を実施していた組織内部で、研究方針変更や主要人員の異動等が発生し、継続的に当コンソーシアムに活動参加ができなくなる。といった事態もあり、活動継続は困難を極めたが、そうした環境下でも参加可能なメンバーによる継続的な市場啓発等を行ってきた結果、「法令上の定義項から除外される」という見解を得るに至る代表的秘密分散技術の技術実装のあり方が把握でき、それが代表的秘密分散技術（電子割符）であり（注）今後「技術区分―A」と称される技術となる。その技術は、毎回異なる分割分散手法による割符ファイル生成が実行されることが基本となっており、非線形なビットレベルでの分割分散処理を基本とした秘密分散技術と言える。こうした技術実装が適切に行われているのであれば、実質的には復元に必要な数以下の割符ファイルに対する効果的且つ、現実的な解読手法が現時点見当たらず、強いて言うならば総当たり攻撃を用いることくらいしか手段が無いものと評価され、そうした場合の計算量は工学的に解読不能と考えられる数値に達しており、一定の条件の下で情報理論的安全性を実現している。と外部より評価報告されていることが基本となる技術である。(参考)

同時に、当コンソーシアム設立当初の基本方針は継承されており、昨今の類似技術等の動向も踏まえ、実装される処理手法や技術等は異なるものの、既知の符号化や暗号化を利活用した一定の有用性を備える可能性のあるものや、数学や暗号理論に忠実な実装を目指した技術、更に今後市場に普及するであろう技術等の登録も可能な仕組みを準備した。例えば、技術区分も「技術区分―B」や「技術区分―C」といった形で、各区分に相当する技術実装の違いに起因する特性の違いを含めて技術登録できるようにし、消費者等に錯誤等をさせないよう技術区分設定に配慮した。

注：前述、参考１のＪＩＰＤＥＣ既公開資料

参考：

府省庁対策基準策定のためのガイドライン　平成２８年８月３１日　内閣官房　内閣サイバーセキュリティセンター

http://www.nisc.go.jp/active/general/pdf/guide28.pdf

基本対策事項 3.1.1(6)-2 b)「複数の情報に分割し」について

例えば、１個の電子情報について、分割された一方のデータからは情報が復元できない方

法でファイルを２個に分割し､それぞれ暗号化を施した上で一方を電子メール､他方を DVD、USB メモリ等の外部電磁的記録媒体で郵送する方法が考えられる。

上記内容に関し、秘密分散法コンソーシアムとして内閣サイバーセキュリティセンターに確認した。
～分割された一方のデータからは情報が復元できない方法で～
との記述では、このドキュメントを参考として対策を検討する現場で、実際にどのような技術等を用いれば要件を満たすのかが分からないが、どうすれば良いか。と問い合わせを行った（２０１６年０９月２６日）結果。

①府省庁ガイドラインは本来中央府省庁向けのものであるが、各自治体や民間等が参考として対策を行うことに制限を加えていない。
②具体的な対策検討の際に、ＮＩＳＣの既公開ガイドライン等を参考とすることに制限を加えていない。
といった内容の回答を頂戴しており、分割された一方のデータからは情報が復元できない方法の具体例として、既公開のＮＩＳＣドキュメントを参考として秘密分散技術を現場で利活用することができます。

２．基本方針

秘密分散技術（電子割符）登録制度に関する事前チェックシートを取りまとめるにあたり、以下の点を考慮した。

（１）登録要件の種類

①必須要件

ア：既公開ガイドライン準拠（実装の在り方）

イ：開発者以外の評価（評価の在り方）

ウ：技術動作の安定性（基礎技術として枯れているか）

②補強要件

エ：採用実績（利用者採用理由や評価）

オ：安定供給実績（供給期間の長さと知財管理を含めた事業者の事業方針）

（２）必須要件

ア：既公開ガイドライン準拠（実装の在り方）

・ 既公開 JIPDEC ガイドラインと SSS-C 公開ガイドライン概要編の内容を満たすこと

イ：開発者及びその関係者等以外の評価（評価の在り方）

・ 学術機関や公的機関での技術外部評価を実施しており、少なくとも５年に一度程度の間隔で実施する

注、採用した原理等の発案者や理論提唱者自身、その周辺人物、更にその帰属組織等に評価依頼することは、関係者等による評価の範疇に入ってしまうので注意

ウ：技術動作の安定性

（基礎技術として枯れているか）

・ 商用技術供給開始から現状に至るまでの年数等と実績数等を示す

（３）補強要件

エ：採用実績（利用者採用理由や評価）

・ 採用理由は健全か

・ 採用後の評価に致命的なものは無いか

オ：安定供給実績

（供給期間の長さと知財管理を含めた事業者の事業方針）

・ 商用での技術供給継続期間と OS のメジャーバージョンアップ等への対処実績

・ 長期間技術供給継続する供給者としての基本方針の確認と宣言

尚、別途公開される「秘密分散技術（一般名称：電子割符）の説明書」―基本技術説明書―に付属する「秘密分散技術（一般名称：電子割符）登録制度」―制度及び手続説明書―

で基本骨子となっているのは下記の事項であり、本チェックシートでも下記の基本骨子が踏襲されている。

・あくまで実社会で利活用できる技術の登録制度であり、学術研究成果や論文等と混同させないこと
・主権者である国民目線で理解・納得できるような内容等とし、一般消費者も含め錯誤等が生じないような記述に留意すること
・独立した基礎技術として、他の要素技術や機器・サービス等からの影響を極力最小化した技術実装であること
・情報セキュリティは、国家安全保障や国際社会の安全・秩序維持等とも密接な関係があることを考慮した記述とすること
・関係する各プレーヤが、適切な当該技術を用いた健全な利用モデルの市場普及に向けた行動を起こす際に参考とできるような記述とすること
・当該技術の日本発の技術標準化を実現し、将来のわが国の安定的外貨収入等の源泉となるべき方向性の一部が示されること

３．留意事項

技術登録時には本事前チェックシートと技術登録時に必要な資料等（注）を添えて当コンソーシアムまで送付いただき、登録審査を実施することとなる。また希望者には、事前面談等も実施する方針。そうした登録申請時の資料や開示情報等は、我々コンソーシアムが開示する登録情報や注意喚起情報の公表を行う際の根拠となるので、必ず確認できる根拠に基づき正しい記述であることを申請者は保証すること。特に当該技術を利活用する場面としては、中長期にわたる安全管理措置等が要求される事例が多く、安定した技術であることが非常に重要であり、そうしたことを証明できることも非常に大きなポイントとなる。当コンソーシアムは、登録申し込み時に提供される資料等が必要な要件を充たしていることを確認し、申し込み要件を充たした案件に対し、別途公開する採点基準に照らし合わせ採点を行い、登録の可否等を決定する。よって申し込み資料や個別面談等での虚偽記載や事実に反する説明等は、コンソーシアムのみならず、技術登録情報を参照等する消費者等への不当表示や必要な説明責任を果たしていないといった法令上の問題になる可能性もあり、コンソーシアムとしてはそうした真実とは異なる登録申し込みによる結果に起因する損害等は、一切負うことはできない。また、そうした事実に反する説明や資料等によりコンソーシアムが誤った判断を行い何らかの損害が生じた場合には、虚偽の申し込みを行った主体等に対し法令に基づき、対処します。

注：登録に必要な資料や費用等（今後コンソーシアムＷＥＢにて順次情報開示します）

参考：開示技術説明資料に関する留意事項としては、

秘密分散技術（電子割符）自体の技術具体化の背景に理論が存在していても全く問題はないのですが、コンソーシアムが行う技術標準化は、あくまで実社会で利用可能な「技術や商品」の標準化になりますので、理論を技術化（商品化）した場合には、理論をどのように技術化・商品化したのかを、一般消費者様にも理解いただけるよう適切に説明していただく必要があります。例えば、よくある暗号化や符号化の話しですが、どのような理論を背景にしても良いのですが、現実の技術（デジタル処理）実装としては、

- 置換
- 変換
- ノイズの付加
- 攪拌
- 技術内部の重要データの安全性確保方策、他の技術や機器等への依存度、他

に加え、秘密分散技術の生命線の一つと言える、

- 分割と分散

といった処理や、重要な役割に担うモジュールとしての安全性確保の仕組みを、実際にどのように実装したか。ということに尽きます。（ただし、無理に内部ノウハウ等を開示要求するものではありませんが、コンソーシアムとして新たな技術区分設定や評価の際に、適切な対処をしやすいことは事実です）

コンソーシアムで進めている技術標準化や技術登録制度では、学術論文のような理論や数式を示すのではなく（登録時の参考資料としてはＯＫです）、そうした理論や数式を技術化・商品化する際に、実際にどのような上記のようなデジタル処理の実装上の「工夫」を、行なったのか。という事実を示すことが第一に重要なこととなります。
そして何より、重要なＩＴセキュリティの基礎技術として、広く安心してご利用できるレベルのものかということの基本的な情報開示が必要です。

４．技術登録

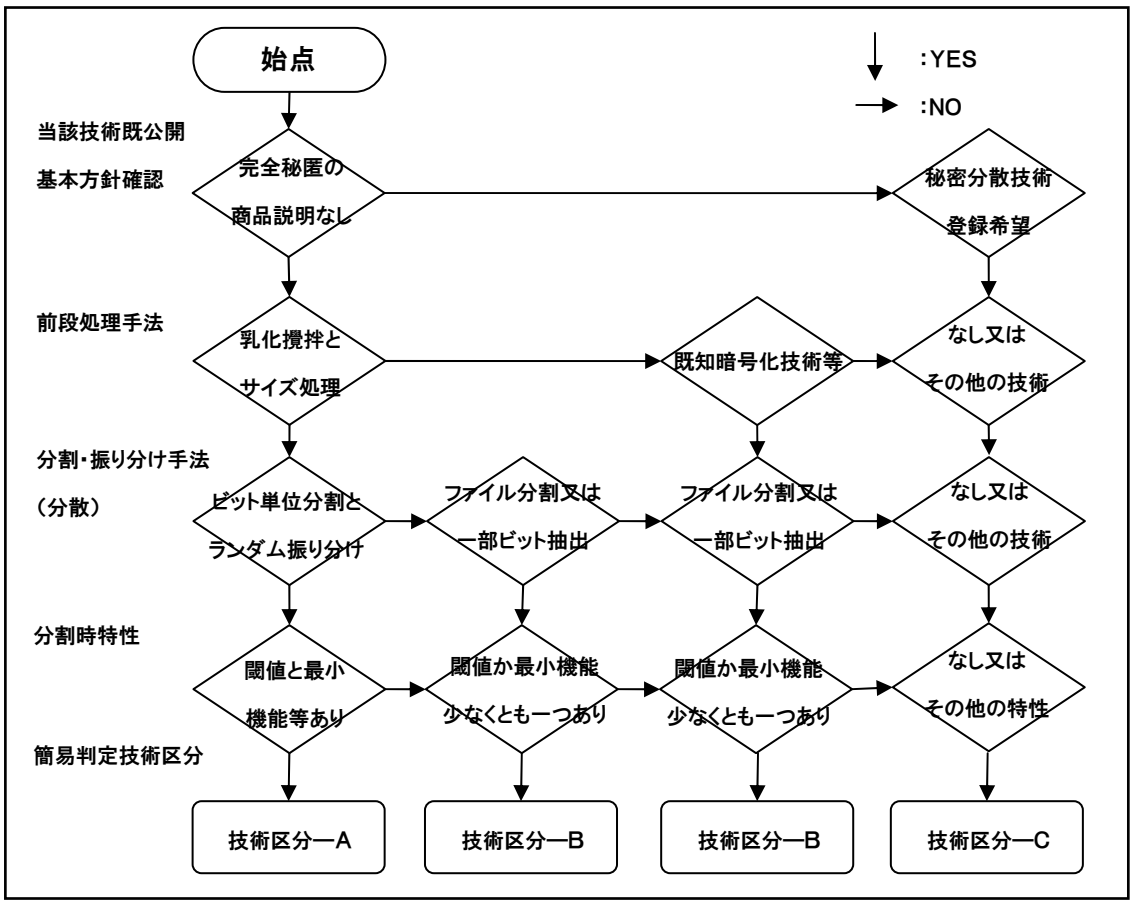
秘密分散技術は、その背景として集合論や順列・組み合わせや秘密分散法等の数学理論等に理論的な安全性等の根拠を求めることもできるが、前述のようにあくまで技術としての標準化の対象であり、理論とは無関係に創出した技術（ソフトウエア等）であったとしても、そうした数学等の理論から見てどの程度の安全性を備えているか、実社会でどの程度利活用可能か。という点が、ポイントとなる。

現在コンソーシアムでは、実際に市場に流通する対象と考えられる技術を調べ、大きく３つの技術区分（Ａ～Ｃ）を設定した。理論的背景と秘密分散技術全体の相関図は、巻末参考の図６「秘密分散技術区分概念鳥瞰図」を参照されたい。

４．１技術区分

技術区分は登録が想定される技術実装モデルによりＡ～Ｃに分かれており、簡易技術区分判定フローとしては、巻末の図１基本的な秘密分散技術の処理概要の処理フローに従いつつ実装される技術処理の要点に焦点を絞り、簡略化して作成したものが下記の参考の図となる。

参考：簡易技術区分判定フロー図



前記の簡易技術区分簡易判定フローと、巻末の「参考資料：技術処理基本概念図」との関係は、基本的には、下記のようになる。

技術区分―Ａ・・・図３代表的秘密分散技術の処理の仕組み
技術区分―Ｂ・・・図４暗号化（ＡＯＮＴ符号化含む）と単純なファイル分割の組み合わせの概念図
技術区分―Ｃ・・・図２単純なファイル分割、図５秘密分散法を実装した際の想定概念図

注：技術区分―Ｃの図２単純なファイル分割を秘密分散技術と言うかに関しては、あくまで広義な秘密分散技術の範疇として区分に加えることとした。
また登録後の対象技術の外部への情報開示時の表記等に関しては、下記のとおり。

登録技術区分表記例：

①	②	③
技術区分－Ｂ	（Ｙ）	－３

上記表記例の①技術区分―Ｂの部分は、前記の登録対象技術の基本的な区分を示す。
技術区分決定は、登録申請者との事前面談（希望者のみ）と、申請者からの本事前チェックシートを含む提出書面による事実確認で行う。

４．２実装環境

基礎技術としての秘密分散技術である為、基本的には他の技術や機器等への依存度が低いことが望ましいことは衆目の意見の一致するところである。そこで、登録しようとする技術・アルゴリズムで必要となる特別なハードやソフトウエア等の要、不要を、登録時の開示項目等として設定している。

上記表記例の②（Ｙ）の部分は、後述の設問中にある、
登録しようとする技術・アルゴリズムで必要となる特別なハードやソフトウエア等がある。に対応する部分で、該当する場合は（Ｙ）、非該当の場合は（Ｎ）と示。なお、基礎技術モジュール単体商品ではなく、そのモジュールが実装されたサービスとして市場供給するモデルの場合には、（Ｓ）と示す。表記決定は、登録申請者との事前面談（希望者のみ）、と申請者からの本事前チェックシートを含む提出書面による事実確認で行う。

４．３実装評価

秘密分散技術を用いる場面では、中長期の安全性や安定性等が要求されることも十分想定あれるため、対象となる技術がどの程度の安全性を有しているか。といった点の外部評価と、安定した動作の実績、更に既存利用者等からの安心感や評価等を得ているかに焦点が当てられている。

上記表記例の③－３

の部分は、下記設問回答と登録時の申請資料等で開示される秘密分散技術（電子割符）としての実装対処評価レベルの表示は、５段階評価で５を最高として示す。

決定は、登録申請者との事前面談（希望者のみ)、と申請者からの本事前チェックシートを含む提出書面、事実確認を元にコンソーシアムで準備する採点表にあてはめ機械的に行う。

注：

あくまで登録時点での技術区分等の表記であり、更新延長や技術更新等での再登録等の際に見直される。現時点での更新期間の制限はないが、原理的な安全性根拠は異なるものの、概ね政府推奨暗号のアルゴリズム危殆化のサイクルに歩調を合わせることを前提としており、最低でも５～６年程度に一度は登録更新を行うことを推奨。

（登録後５年を超えても新たな外部評価や更新期間延長の手続きをしない場合は、上記③の評価レベルが自動的に落ちる）

５．技術区分の詳細

本項記載のように、広義な秘密分散技術のグループに入る多様な技術実装モデルに関し、本資料序文記載の資料（参考１、２）や当コンソーシアム等からの既公開情報のように、技術選択肢の多様化が進んだ市場の現状を踏まえ、複数の技術実装も視野に入れ標準化を進めていることの具体的対処の一つである。

技術実装が異なることに起因する各区分の特徴も踏まえ、参考とされたい。今後も新たな技術実装モデルの商品化等の事実を確認できれば、区分の追加等や記載事項の修正等を行う所存である。

５．１技術区分―A

概要：これまでコンソーシアム等で法令上の有効性等を確認してきた、代表的秘密分散技術の実装モデル。保護対象の原本電子情報に毎回異なるゴミ情報を付加し乳化処理（攪拌）とサイズ調整（自動）を行ったのちに、その乳化後データをビットレベルで分割し、無作為に複数の割符ファイルにそれらビットを毎回異なる振り分け方を行い、割符ファイル生成を行う処理を根底に据えた技術。復元に必要な数の割符ファイルからは原本復元が可能であるが、復元に至らぬ数の割符ファイルから原本復元を行うことはできない。実社会における紙資料等の細断処理による廃棄処分の概念に通じる技術。集合論における部分集合生成の際の要素が、デジタルデータの最小単位（ビット単位）であると言える。

特徴：保護対象電子データをデジタルデータの存立根拠に対し、原理的に直接働きかけ破壊する技術と言える。暗号や数学を専門としない一般読者にも理解しやすい安全性根拠であり、浮動小数点演算等の負荷の高い処理や専用の機器等が不要で、複数ＯＳへの対処を行い相互のデータ互換のある割符ファイル生成が可能。長期にわたる安定した動作実績と導入事例、公共実証事業実績等を持つ代表的秘密分散技術。一定の条件の下における情報理論的安全性を持つと外部評価を受けている技術。既知の秘密分散法に忠実な実装に比べ比較的高速な処理が実現できており、生成される割符ファイルの総和サイズも小さい。

優位点：原本情報に復元できない数の割符ファイルは、保護対象の原本情報（例：個人情報保護法や番号法、著作権法、不正競争防止法（注）、要機密情報、要安定情報等）の法令等の定義項から除外される特性を持つ。現時点、効果的な攻撃手法が発見されておらず、強いて言うならば総当たりによる攻撃のみとなる。（注：個人情報も営業秘密に解する）生成される割符ファイルが原本情報よりも小さく、少なくとも一つの生成する割符ファイルは選択により自動的に安全性に支障の無い最小サイズの割符ファイルを生成できる。また、割符ファイル生成時に復元時の条件設定をした処理も可能な機能を備えている。

考慮点：現時点では、純粋な数学的な評価や理論は存在しない。今後、例えば連立方程式

の関係式が不足していても解を導き出せるような革命的な発見があると、解読可能性が出る可能性がある。復元に至る数の割符ファイルを適切に管理することは最低限の利活用上の条件となる。

概要図：デジタルデータの原理的特性に直接働きかけるＩＴセキュリティ基礎技術の一例と言える。
巻末参考資料：技術処理基本概念図　図３　代表的秘密分散技術の処理の仕組みを参照のこと。

５．２技術区分―B
概要：保護対象の原本電子情報に対し、一定の法則に従い符号化や暗号化を行い生成された変換データをファイル分割する技術で、単なる符号化（暗号化）＋ファイル分割ではない安全性を向上させるための技術処理も実装されていることが本来は必要。利用した符号化技術や暗号化技術への効果的な攻撃手法を知る者による攻撃や、暗号危殆化等に対して、ファイル分割した暗号化ファイル分割片部分の解読ができてしまう可能性が否定できないものの、原本電子情報全体が解読されることを未然防止できる特性がある。集合論における部分集合生成の際の要素が、暗号化データの一定サイズ単位であると言える。

特徴：
長期にわたりＩＴセキュリティの基本セキュリティ技術として利活用されてきた暗号等を利活用した技術実装となる。このことから、暗号そのもののこれまでの実績や実装ノウハウ等を背景に基礎技術開発ができる。仮に暗号化に対する危殆化や脆弱性が出てこないのであれば、暗号化したファイルを単純にファイル分割することで初期の技術開発が可能。また、分割手法が比較的単純なので、処理速度を速くできる可能性がある。しかし、現状の暗号技術は危殆化等のリスクを持っていることと、攻撃者が効果的な攻撃手法を隠し持っている可能性を否定できない為、技術開発や市場流通させる際に超えるべきハードルは低くはない。なお、利用する暗号化（符号化）が完全秘匿の場合は技術区分―Cとなる。

優位点：
少なくとも暗号化のみよりも高度な安全管理措置（技術）と言えであろう。また、一定の分割手段やビット抽出処理で実装されていれば比較的処理速度が速いものと期待でき、処理効率を求める場合等は有効であろうと考える。更に、暗号化したファイルが攻撃者に解読される場合は暗号化による保護対象データ全体が解読されてしまうが、この技術実装の場合は、攻撃を受けた分割片（一部分）の解読（リスク顕在化）で済む可能性がある。内部で利用している暗号鍵や特定のデータ等の管理の安全性と運用上の煩雑さがうまく解消

された実装ができていれば、一つの安全管理措置（技術）として旧来の技術を生かす意味でも意義がある。

考慮点：
暗号化ファイル分割部分の解読可能性が否定できないこともあり符号化・暗号化の範疇となり、法令解釈上の有効性を求めることは現時点できないものと考えられる。また原理的に利用した符号化や暗号化の強度への依存度が高い（注１）ので独立した基礎技術として考える場合には、何らかの実装上の工夫が必要。すでに暗号化商品等を用いている場合には、暗号化を行った後にファイル分割ソフトで分割しても原理的には同様の仕組みを構築できる為、敢えて独立した基礎技術とするには基礎技術単体として更なる付加価値機能等が必要である。符号化や暗号化以外の数学理論等を背景としているが完全秘匿ではないものも、暫定的ではあるが同区分とする。分割手法が単純な場合には、他の分割片のサイズが類推できてしまう可能性を否定できない。また、暗号化等を行ったデータから一定の一部ビットを抽出する技術実装モデルも当区分に該当する。

概念図：既知の暗号化（符号化）技術等を利活用した技術となる。
巻末参考資料：技術処理基本概念図　図４暗号化（ＡＯＮＴ符号化含む）と単純なファイル分割の組み合わせの概念図参照のこと。

５．３技術区分―Ｃ
概要：単純なファイル分割や、未知の技術実装や数学や暗号の学術理論を実装したと主張する技術区分で、技術区分―Ａ、Ｂに該当しない技術が対象となる。なお、理論実装が完全に実現できていれば、基礎技術単体としては完全秘匿の可能性があるが、社会安全保障や法令の規制等を受ける。以下、単純なファイル分割モデルは除外して解説する。

特徴：既知の完全秘匿を可能とする理論や、今後出現する可能性のある革命的な理論等に基づく技術創出であると考えられ、新たな技術区分としての登録対象となる。そうした技術が出現した際に、特徴も確認できると考えられる。

優位点：技術区分―Ａ同様に、現時点未知の革命的な理論等が出ることで解読リスクが浮上してくる可能性がある。今後の商品化と考えられるので、相当程度課題を解消して世に出るか、軍事といった特定特殊分野の中でも最高機密のレベルで用いられる技術となる可能性がある。

考慮点：一般論として、理学的な世界の安全性であり、工学的にシステムに実装する際に

は、どうしてもシステム上必要な環境要件や限界の為に、学術理論上は出てこない技術実装上のセキュリティに対するアキレス腱が浮上してくる。例えば、真性乱数を必要とする場合には、そうした特殊な機器が必要になる可能性がある。仮に完全秘匿を実現しているとすれば、その理論そのものの中には復元が成功したか否かを判断する仕組みが抜けていることも懸念され、理論実装だけでは実務に耐えられないと考えられる。そうなると復元が成功したか否かの何等かの情報を別途管理する必要が生じてしまう。そうした実務で利用するという観点からすると、実際にはベースとなる技術区分―Cが基礎技術の背景とした理論上の安全性レベルがそのまま基礎技術モジュール自体の安全性レベルにはならない（注２）と、現時点では考えられる。今後本格的に商品化が為された場合、中・長期の技術安定性や実績等の確認が難しい。現時点では、量子暗号や秘匿計算、マルチパーティプロトコル等、秘密分散技術とも関連のある複数の技術モデル等も含め、こうした理論の実利用に向けた課題も含む議論は、完全秘匿を証明できるとするワンタイムパッド等多くの議論があるところであるが、当コンソーシアムとしてはあくまで実用可能な技術・商品等を対象としているので、現時点ではその他の技術区分である技術区分―Cの中に含め、そうした技術・商品が具体化した際や登録申請があった時点で、再度区分検討等を行う。

概念図：現時点存在しないので、概念図を示せない。しかし参考例が必要と考えられるので、著名な秘密分散法の論文等を元に、あくまで想定の参考図であるが、その理論を最大限技術実装する解釈をした際の想定技術概念図を描く。
巻末参考資料：技術処理基本概念図　図５秘密分散法を実装した際の想定概念図、として参考掲示する。なお、単純なファイル分割モデルは、図２単純なファイル分割である。

注１：原本電子情報をファイル分割した後に、それぞれの分割片に暗号化を施すといった仕組みは、単純に暗号化（符号化含む）と解釈できるため、当コンソーシアムの秘密分散技術（電子割符）標準化対象のスコープには入らない。
注２：次回公開予定の技術実装者向けガイドラインでも関連する記載を予定しており、現実には基礎技術アルゴリズムだけではなく実装プロトコルも重要であることとも通底する。

６．事前確認事項

４．１技術区分に記載した参考：簡易技術区分判定フロー図で、すでに簡易技術区分判定していると想定するが、技術登録に向けた事前チェック事項等となる。大別すると、登録する技術を所有する事業者等自身に対する確認事項（対象者概要確認事項）と、登録する技術自体に関する確認事項（登録対象技術概要確認事項）となる。

（１）対象者概要確認事項

（２）登録対象技術概要確認事項

(a) 基本区分確認事項

ア：基本的技術区分確認

イ：基本的実装環境確認

ウ：基本的技術実装外部評価確認

(b) 技術実装概要確認事項等

６．１ 対象者概要確認事項

１、

基礎技術（秘密分散技術（電子割符））を開発する主体ですか？（Y，N）

２、

基礎技術（秘密分散技術（電子割符））を開発させる主体ですか？（Y，N）

３、

基礎技術（秘密分散技術（電子割符））を市場供給する主体ですか？（Y，N）

４、

基礎技術（秘密分散技術（電子割符））を市場供給させる主体ですか？（Y，N）

５、

基礎技術（秘密分散技術（電子割符））を開発済みですか？（Y，N）

６、

基礎技術（秘密分散技術（電子割符））を開発検討中ですか？（Y，N）

７、

基礎技術（秘密分散技術（電子割符））の開発拠点は、日本国内ですか？（Y，N）

ー海外の場合の拠点国は？（　　）

８、

基礎技術（秘密分散技術（電子割符））を実装したアプリは、日本国内の開発拠点で開発しましたか？（Y，N）

ー海外の場合相手先国は？（　　）

９、

当該技術等に関し知的財産や著作権上の問題が今後出ることはありませんか？（Ｙ，Ｎ）
１０、
秘密分散法コンソーシアムでは、当該技術が長期間の利用されることを想定した上で利用者への安心提供と、当該技術の健全な普及に資するよう、
知的財産や著作権の管理機能も検討しています。
貴社は、その制度に賛同しますか？（Ｙ，Ｎ）
ー詳細説明必要であれば、別途行う。
１１、
貴社スタッフや外注先等は、反社会的勢力と無関係ですか？（Ｙ，Ｎ）
１２、
貴社は、反社会勢力と無関係ですか？（Ｙ，Ｎ）
１３、
当該技術は、その原理的特性から、不適切な技術利用や商品化は大きな社会的問題を引き起こす可能性があります。そうした認識を十分持っていますか？（Ｙ，Ｎ）
１４、
基礎技術供給や当該技術を実装した本格的サービスは、一過性のビジネスとしてとらえることのできない中長期的な事業になる可能性が高いですが、そうした事業を行う覚悟がありますか？（Ｙ，Ｎ）
１５、
貴社は、秘密分散法コンソーシアムが公表するガイドライン等（注）の資料をご存知ですか？（Ｙ，Ｎ）

注：
秘密分散技術（電子割符）の標準化に向けたガイドライン
http://www.sss-c.org/?p=165
「秘密分散技術（一般名称：電子割符）登録制度」―制度及び手続説明書―　―初版―
（公表予定）
「秘密分散技術（一般名称：電子割符）の説明書」―　概要説明書　―
http://www.sss-c.org/wp-content/uploads/2016/03/gideline_20160229.pdf
ＥＣにおける情報セキュリティに関する活動報告書 2009
（情報セキュリティＷＧ：ＳＷＧ１／ＳＷＧ２／ＴＦの各報告書）
https://www.jipdec.or.jp/archives/publications/J0004291
ＴＦ報告書が秘密分散技術の初期ガイドラインです。

６．２ 登録対象技術概要確認事項

(a) 基本区分確認事項

ア：基本的技術区分確認

登録しようとする技術は、消費者等への説明時に「完全秘匿」であること。又は消費者が「完全秘匿」と認識するような説明やプロモーション等をしていますか？（代理店等が行っている場合も同様）

（Y，N）

「Y」の場合は、下記の基本区分確認事項イ、ウの設問に回答後、「６．２基本的技術概要確認　（２）登録対象技術概要確認事項　(b) 技術実装概要確認事項等 設問３０」に進んでください。

イ：基本的実装環境確認

登録しようとする技術・アルゴリズムで必要となる特別なハードやソフトウエア等がある。

（Y，N，S）

「Y」の場合、

イ－２：それはどのようなハードやソフトウエア等ですか？

（　　）

注：基礎技術モジュール単体商品ではなく、そのモジュールが実装されたサービスを、商品等開発会社等に市場供給するモデルの場合には、（S）を選択してください。

イ―３：そのハードやソフトウエア等に課題が見つかった場合や、保守等ができなくなる場合の措置をどのように考えていますか？

（　　）

注：Y、N、Sいずれの回答でも、設問ウへお進みください。

ウ：基本的技術実装外部評価確認

対象技術開発者やその関係者以外の第三者からの技術評価を受けていますか？

（Y，N）

（１回目：　　年、　　様、　　概要　　）

（２回目：　　年、　　様、　　概要　　）

（３回目：　　年、　　様、　　概要　　）

（４回目：　　年、　　様、　　概要　　）

（５回目：　　年、　　様、　　概要　　）

ウ―２：対象技術（現状技術実装の状態のもの）は、市場供給開始後何年を経過していますか？（　　年）

ウ―３：対象技術は、既存技術供給先や対象技術実装商品採用先での事故や不満等はありませんか？

（Y，N）
ウ―４：事故や不満等があった場合には、その対処結果は？
（　　）
本項設問「ア」で、「Y」と回答した方以外は、次項設問に進んでください。

(b) 技術実装概要確認事項等
０１、
秘密分散法コンソーシアムが公表するガイドライン等（注）記載の本資料巻末の参考：技術処理基本概念図の図３　代表的秘密分散技術の処理の仕組みに相当する、「前段処理」（乳化処理）を行い「中間ファイル」生成を行い、ビットレベルで「分割・振り分け（分散）処理」を都度ランダムに行うことを基本に据えた技術実装と言えますか？（Y，N）
注：
秘密分散技術（電子割符）の標準化に向けたガイドライン
http://www.sss-c.org/?p=165
「秘密分散技術（一般名称：電子割符）登録制度」―制度及び手続説明書―　―初版―
（公表予定）
「秘密分散技術（一般名称：電子割符）の説明書」―　概要説明書　―
http://www.sss-c.org/wp-content/uploads/2016/03/gideline_20160229.pdf
ＥＣにおける情報セキュリティに関する活動報告書 2009
（情報セキュリティＷＧ：ＳＷＧ１／ＳＷＧ２／ＴＦの各報告書）
https://www.jipdec.or.jp/archives/publications/J0004291
ＴＦ報告書が秘密分散技術の初期ガイドラインです。
―本設問で「Y」の場合は、次の設問へ、
―本設問で「N」の場合は、設問１０へ、

０２、
分割時の付加機能として、閾値設定と少なくとも一つの割符ファイルの最小サイズ生成の両機能を有していますか？
―本設問で「Y」の場合は、次の設問へ、
―本設問で「N」の場合は、設問３０へ、

０３、
新たな創意工夫を実装したポイントがあれば記載ください
注：複数プラットフォームでのデータ互換等、登録技術公開の際のアピールポイント。新たな技術区分制定の可能性があります
(ｉ) 新規ポイント

(ⅱ) 特徴等
(ⅲ) 留意点
(ⅳ) 営業時どのように消費者へ当該技術等の説明を行っていますか。
（参考営業資料やＵＲＬも）
事前チェックいただいた登録対象の技術は、技術標準化ベースとなっている代表的秘密分散技術と推定されますので、「技術区分―A」として別途登録申請手引きに従い、コンソーシアムまで技術登録の問い合わせをご検討ください。

１０、技術概要既公開の代表的秘密分散技術の処理との相違点は、前段処理ですか？
―本設問で「Ｙ」の場合は、次の設問へ、
―本設問で「Ｎ」の場合は、設問２０へ、

１１、対象技術に実装されている前段処理に、「既知の符号化や暗号化技術・理論・学術論文等の内容」が実装されていますか？
―本設問で「Ｙ」の場合は、次の設問へ、
―本設問で「Ｎ」の場合は、設問３０へ、

１２、
利用した符号化や暗号化の種類・名称（理論名や論文）等は何ですか？
（　　）
―次の設問へ、
１３、
分割手法は、ファイル分割か中間ファイルからの一部ビット抽出の処理ですか？
―本設問で「Ｙ」の場合は、次の設問へ、
―本設問で「Ｎ」の場合は、設問３０へ、

１４、
中間ファイルの分割のサイズは、どの程度の大きさ（固定長）ですか？
（　　）
―次の設問へ、
１５、
実装した暗号や符号化の際の暗号鍵や乱数値等の管理は、どのように行っていますか？
（　　）
―次の設問へ、
１６、

採用した数学・暗号理論や学術論文等に脆弱性や理論的課題等が発見された場合等、対処方針は？

（　　）

―次の設問へ、

１７、

分割時の付加機能として、閾値設定と少なくとも一つの割符ファイルの最小サイズ生成のいずれか一つの機能を有していますか？

―本設問で「Ｙ」の場合は、次の設問へ、

―本設問で「Ｎ」の場合は、設問３０へ、

１８、

新たな創意工夫を実装したポイントがあれば記載ください。

特に理論実装したことを安全性根拠としている場合には、電子データ自身に対し、どのような技術的処理を施しているかも記載ください。置換、変換、ノイズの組み入れ、分割手法等、実際のデータ処理技術を解説し、そうした技術実装が何故理論を満たしていると言えるのか（理論を満たしていない場合は、不要）を、一般人も理解できるよう示してください。特に符号化又は暗号化後に単純にファイル分割する処理そのものは、特段秘密分散技術として新たな技術と宣言する必要はなく、暗号化や符号化の応用・利活用の延長モデルでしかありませんのでご注意ください。

注：複数プラットフォームでのデータ互換等、登録技術公開の際のアピールポイント。新たな技術区分制定の可能性があります

(ⅰ) 新規ポイント

(ⅱ) 特徴等

(ⅲ) 留意点

(ⅳ) 営業時どのように消費者へ当該技術等の説明を行っていますか。

（参考営業資料やＵＲＬも）

事前チェックいただいた登録対象の技術は、本資料巻末の参考：技術処理基本概念図の図４　暗号化（符号化含む）の概念図の処理の仕組みに相当する、既存の符号化や暗号化を施した後にファイル分割する技術と言えると推定されますので、「技術区分―Ｂ」として別途登録申請手引きに従い、コンソーシアムまで技術登録の問い合わせをご検討ください。

２０、

代表的秘密分散技術の処理との相違点は、「分割・振り分け（分散）」処理ですか？

―本設問で「Ｙ」の場合は、次の設問へ、

―本設問で「Ｎ」の場合は、設問３０へ、

２１、
分割手法は、ファイル分割か中間ファイルからの一部ビット抽出の処理ですか？
―本設問で「Ｙ」の場合は、次の設問へ、
―本設問で「Ｎ」の場合は、設問３０へ、

２２、
中間ファイルの分割のサイズは、どの程度の大きさ（固定長）ですか？
（　　）
―次の設問へ、

２３、
分割時の付加機能として、閾値設定と少なくとも一つの割符ファイルの最小サイズ生成のいずれか一つの機能を有していますか？
―本設問で「Ｙ」の場合は、次の設問へ、
―本設問で「Ｎ」の場合は、設問３０へ、

２４、
新たな創意工夫を実装したポイントがあれば記載ください
注：複数プラットフォームでのデータ互換等、登録技術公開の際のアピールポイント。新たな技術区分制定の可能性があります
(ⅰ) 新規ポイント
(ⅱ) 特徴等
(ⅲ) 留意点
(ⅳ) 営業時どのように消費者へ当該技術等の説明を行っていますか。
（参考営業資料やＵＲＬも）
事前チェックいただいた登録対象の技術は、前段処理までは代表的秘密分散技術と同様の処理ですが、「分割・振り分け（分散）」処理が異なる為、「技術区分―Ｂ」と推定されます。別途登録申請手引きに従い、コンソーシアムまで技術登録の問い合わせをご検討ください。

３０、
対象技術は、本資料巻末の参考：技術処理基本概念図の図２　単純なファイル分割　の概念図のファイル分割技術と言えますか？（Ｙ，Ｎ）
―本設問で「Ｙ」の場合は、次の設問へ、
―本設問で「Ｎ」の場合は、設問４０へ、

３１、
新たな創意工夫を実装したポイントがあれば記載ください
注：複数プラットフォームでのデータ互換等、登録技術公開の際のアピールポイント。新たな技術区分制定の可能性があります
(ｉ) 新規ポイント
(ⅱ) 特徴等
(ⅲ) 留意点
(ⅳ) 営業時どのように消費者へ当該技術等の説明を行っていますか。
（参考営業資料やＵＲＬも）
事前チェックいただいた登録対象の技術は、本資料巻末の参考：単純なファイル分割の組み合わせの概念図の処理の仕組みに相当する技術と言えると推定されますので、「技術区分―Ｃ」として別途登録申請手引きに従い、コンソーシアムまで技術登録の問い合わせをご検討ください。

４０、
登録しようとする技術は、消費者等への説明時に「完全秘匿」であること。又は消費者が「完全秘匿」と認識するような説明やプロモーション等をしていますか？（代理店等が行っている場合も同様）
（Ｙ，Ｎ）
―本設問で「Ｙ」の場合は、次の設問へ、
―本設問で「Ｎ」の場合は、設問５０へ、

４１、
対象技術に実装されている前段処理に、「既知の符号化や暗号化技術・理論・学術論文等の内容」が実装されていますか？
―本設問で「Ｙ」の場合は、次の設問へ、
―本設問で「Ｎ」の場合は、設問５０へ、

４２、
利用した符号化や暗号化の種類・名称（理論名や論文）等は何ですか？
（　　）

４３、
実装した暗号や符号化の際の暗号鍵や乱数値等の管理は、どのように行っていますか？

（　　）
―次の設問へ、
４４、
採用した数学・暗号理論や学術論文等に脆弱性や理論的課題等が発見された場合等、対処方針は？
（　　）
―次の設問へ、
４５、
対象技術が、真に完全秘匿を実現している場合には、一般市場に流通する技術として利用レベルを超える秘匿性等を有していると推定され、技術開発及び商品化には大きな努力等があったと思われます。本資料巻末の参考：技術処理基本概念図の図５　周辺情報セキュリティ技術等と時間軸等からの相関図記載の理学的領域　永久非公開情報領域等完全理論実装完全秘匿技術に該当することとなり、その技術の輸出入に関しても、法令等で定める規制対象となることをご存知ですか？（Y，N）
―次の設問へ、
４６、
完全秘匿を実現している場合には、対象技術は、本資料巻末の参考：技術処理基本概念図の図５　周辺情報セキュリティ技術等と時間軸等からの相関図記載の理学的領域　永久非公開情報領域等完全理論実装完全秘匿技術に該当することとなり、通常の秘密分散技術以上の技術やノウハウ、ライセンス先等の管理が要求されますが、社会安全保障上のそうした技術ノウハウ等を保有する関係当事者等としての認識をお持ちですか？（Y，N）
―次の設問へ、
４７、
完全秘匿を実現している場合には、対象技術は、本資料巻末の参考：技術処理基本概念図の図５　周辺情報セキュリティ技術等と時間軸等からの相関図記載の理学的領域　永久非公開情報領域等完全理論実装完全秘匿技術に該当することとなり、対象技術実装商品の市場供給にも、社会安全保障上の高度な注意が必要ですが、そうした技術ノウハウ等を保有する関係当事者等としての認識をお持ちですか？（Y，N）
―次の設問へ、
４８、
新たな創意工夫を実装したポイントがあれば記載ください。
特に理論実装したことを安全性根拠としている場合には、電子データ自身に対し、どのような技術的処理を施しているかも記載ください。置換、変換、ノイズの組み入れ、分割手法等、実際のデータ処理技術を解説し、そうした技術実装が何故理論を満たしていると言えるのか（理論を満たしていない場合は、不要）を、一般人も理解できるよう示してください。特に符号化又は暗号化後に単純にファイル分割する処理そのものは、特段秘密分散

技術として新たな技術と宣言する必要はなく、暗号化や符号化の応用・利活用の延長モデルでしかありませんのでご注意ください。
注：複数プラットフォームでのデータ互換等、登録技術公開の際のアピールポイント。新たな技術区分制定の可能性があります
ア）新規ポイント
イ）特徴等
ウ）留意点
エ）営業時どのように消費者へ当該技術等の説明を行っていますか。
（参考営業資料やＵＲＬも）
事前チェックいただいた登録対象の技術は、本資料巻末の参考：技術処理基本概念図の図４　暗号化（符号化含む）の概念図の処理の仕組みの特殊系か、図５　秘密分散法を実装した際の想定概念図に相当する、又はその他既知の理論等を実装したものと推定されますので、「技術区分―Ｃ」として別途登録申請手引きに従い、コンソーシアムまで技術登録の問い合わせをご検討ください。

５０、
新たな革新的秘密分散技術の技術区分を検討できる可能性があります。別途、コンソーシアム事務局と打ち合わせを行ってください。コンソーシアムに秘密分散技術（電子割符）の登録申し込みをする際には、別途コンソーシアム事務局まで事前にお問合せください。

あとがき

秘密分散技術は、日本発祥のＩＴセキュリティの基礎技術である。どれだけ時代が変わろうとも、そこに丸ごと情報資産が存在すれば、丸ごと盗まれたり、攻撃者にとって都合の良い改ざん等の危険に遭遇するリスクをゼロにすることはできない。海賊の宝の地図や勘合貿易の勘合符（割符）等、関係当事者で対象情報等をシェアすることで自ずと相互牽制を働かせることができると考える。

我々コンソーシアムは今後も、当該技術の健全な利用モデルからの技術標準化、日本発の世界標準化を推進していく所存である。

尚、コンソーシアムの公表する資料は今後も技術革新や環境変化等で改編が重ねられていくこととなると考える。記憶に新しい読者も多数あると思われるが、広く社会に提供される仕組みの今後の在るべき姿等に関し、都内ビルでの回転ドアによる事故等に関する国会の経済産業委員会の議事録（注）には、多くの示唆に富む発言内容等があり、読者にも是非一読願いたい。理論そのものではなく、実利用される技術そのものの健全な市場普及と標準化等を推進する我々コンソーシアムは、「技術の系譜」の重要性も含め、僭越ながら重大な社会的役割を果たしているものと改めて自らの肝に銘じるものである。

注：

第１６５回国会　経済産業委員会　第４号

平成十八年十一月二十一日（火曜日）

http://kokkai.ndl.go.jp/SENTAKU/sangiin/165/0063/16511210063004a.html

関連し、国土交通省及び経済産業省の共同で「自動回転ドアの事故防止対策に関する検討会」が設置され、「自動回転ドアの事故防止対策について」という報告書も公開されている。

http://www.mlit.go.jp/kisha/kisha04/07/070629_2/03.pdf

お問合せ先：

秘密分散法コンソーシアム

お問合せ　http://www.sss-c.org/?page_id=160

事務局所在地：

東京都渋谷区笹塚 1-32-2 ソネット笹塚 102 グローバルフレンドシップ株式会社内

参考資料：技術処理基本概念図

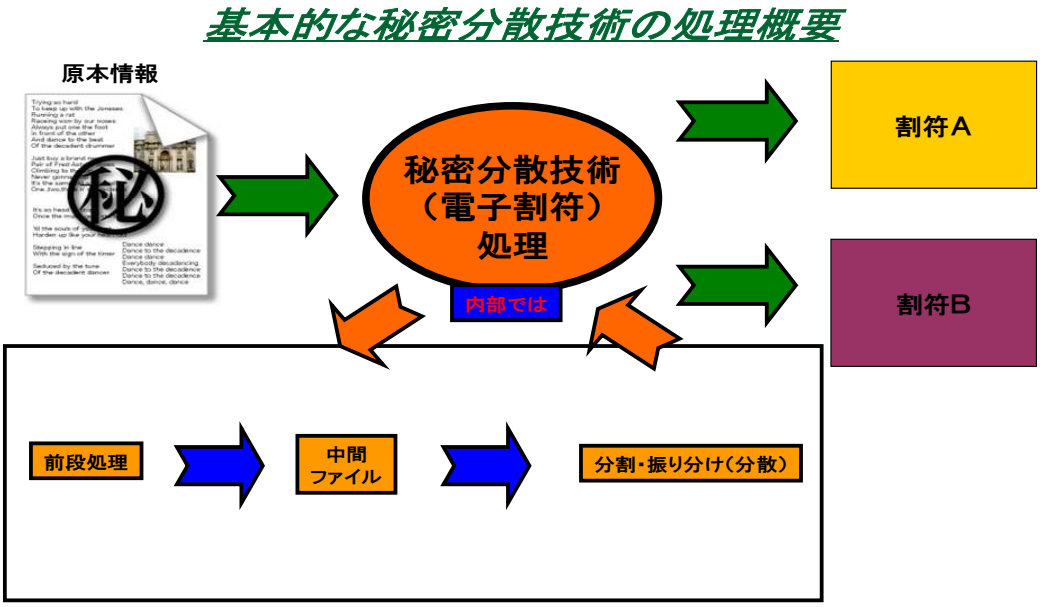


図１　基本的な秘密分散技術の処理概要

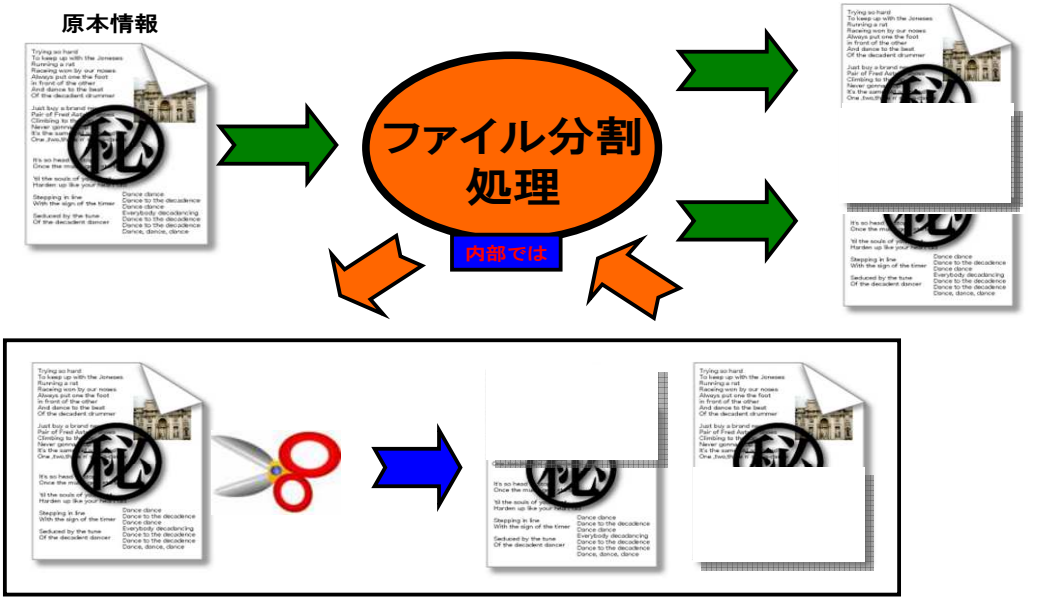


図２　単純なファイル分割

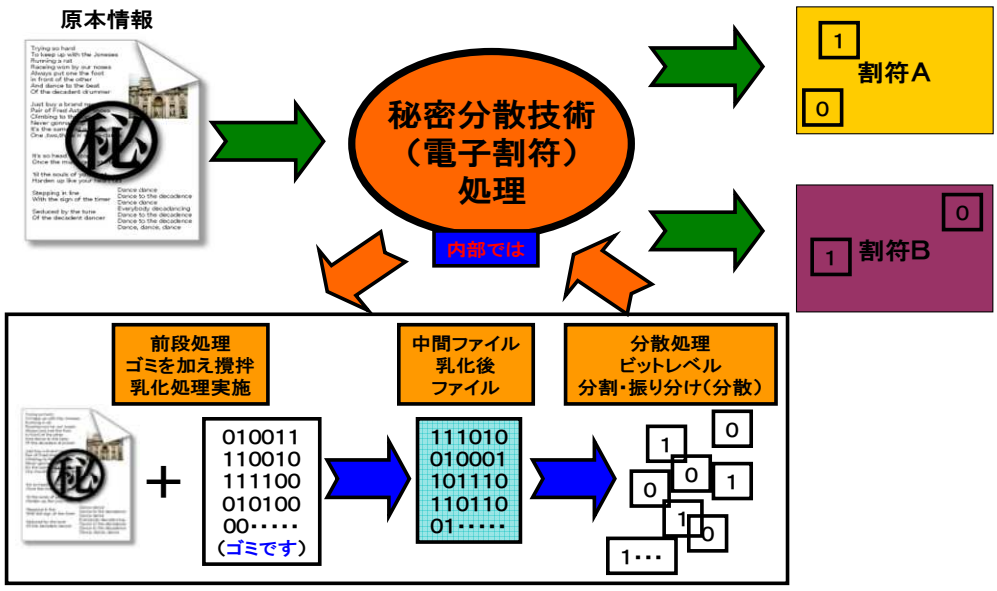


図３　代表的秘密分散技術の処理の仕組み

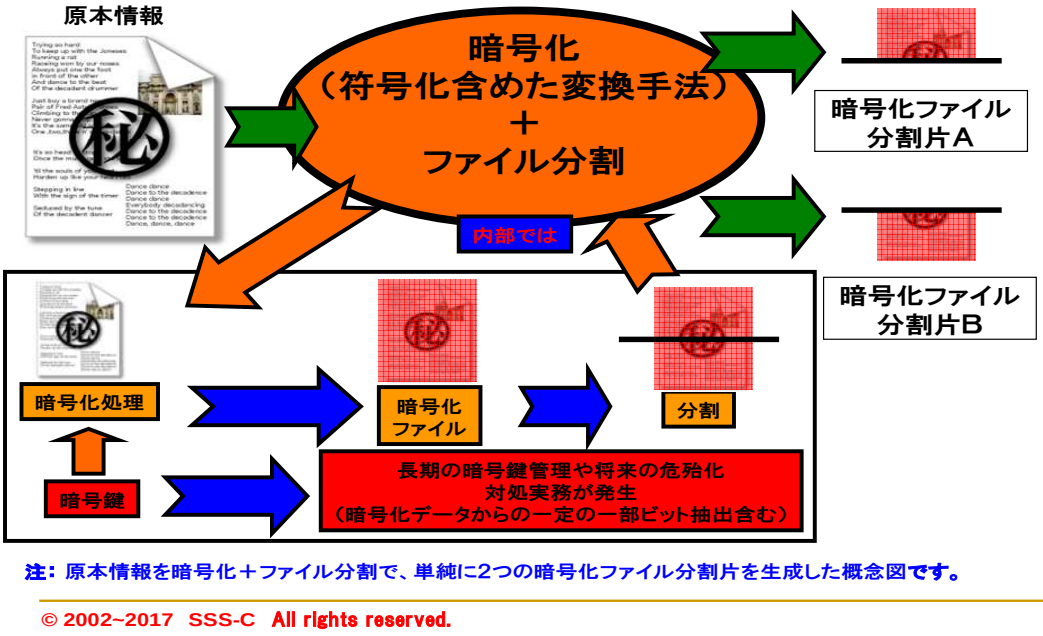


図４　暗号化（ＡＯＮＴ符号化含む）と単純なファイル分割の組み合わせの概念図

上記概念図原典：「秘密分散技術（一般名称：電子割符）の説明書」―　概要説明書　―

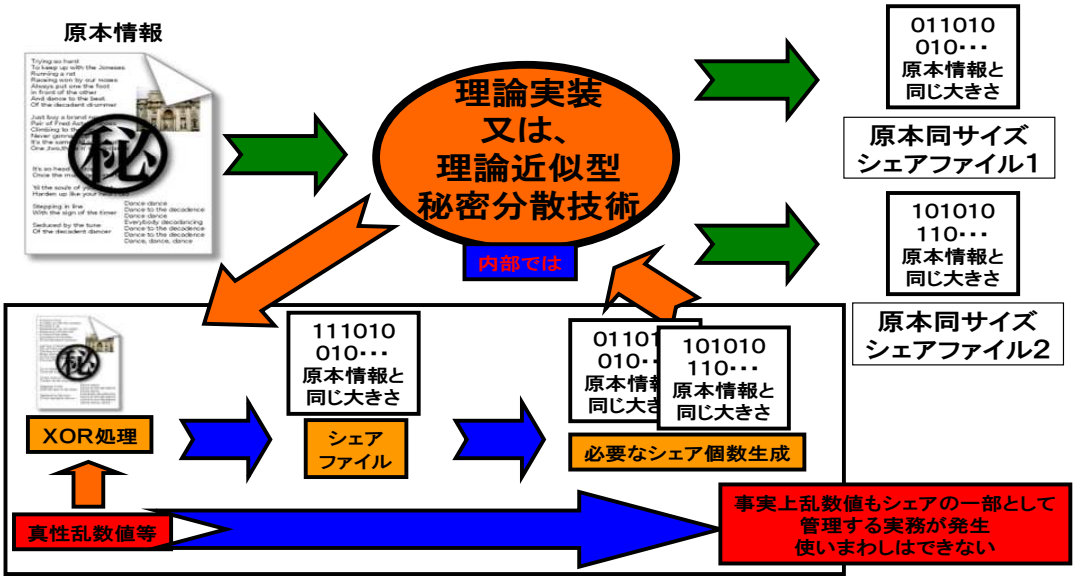


図５　秘密分散法を実装した際の想定概念図

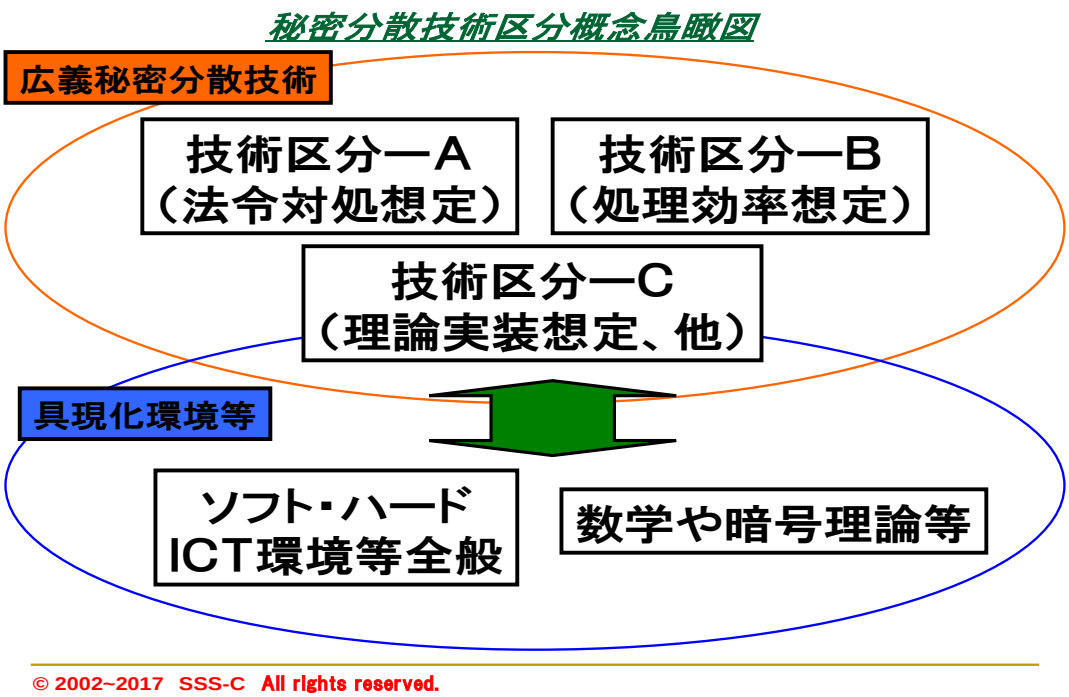


図６　秘密分散技術区分概念鳥瞰図

出典：ＳＳＳ－Ｃ内部資料

以上。

「秘密分散技術（一般名称：電子割符）登録制度」―事前チェックシート―　―初版―

秘密分散法コンソーシアム（SSS-C）

平成 29 年 0 1 月 06 日　第 1 刷発行

発　行：秘密分散法コンソーシアム

〒151-0073　東京都渋谷区笹塚 1-32-2 ソネット笹塚 102

グローバルフレンドシップ株式会社内秘密分散法コンソーシアム事務局

秘密分散法コンソーシアム WEB（http://www.sss-c.org/）

お問合せは、同上コンソーシアムお問合せまで（http://www.sss-c.org/?page_id=160）