「秘密分散技術（一般名称：電子割符）の説明書」

―　概要説明書　―

―初版―

２０１６年　０３月

秘密分散法コンソーシアム

序文

秘密分散コンソーシアムは 2002 年から秘密分散技術（電子割符）の標準化や健全な市場育成と普及に向けた啓発活動を継続してきた。この度、秘密分散技術（電子割符）の標準化に向けた活動の一部として、また啓発活動に役立つガイドラインを策定するために、以下の一連の資料を作成することとした。本資料は、その一つとして位置付けるものである。

関連資料一覧

- 「秘密分散技術（一般名称：電子割符）の説明書」―　概要説明書　―
- 「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　―
- 「秘密分散技術（一般名称：電子割符）の説明書」―　実装方法説明書　―
- 「秘密分散技術（一般名称：電子割符）の説明書」―　運用利用説明書　―
- 「秘密分散技術（一般名称：電子割符）の説明書」―　用語定義編　―

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）の説明書」―概要説明書―一初版－１、2016,03,01,

目次

第 1 章　はじめに

私たちの生活は、IT（情報技術）や情報通信の発展のおかげで飛躍的に便利になった。いまや IT は、産業や政府活動、そして私たちの日々の暮らしを支える重要な社会基盤である。しかし、一方で IT 基盤を脅かす脅威が存在することも事実です。IT に依存すればするほど、IT に対する脅威はただちに私たちの経済活動や社会活動そのものへの脅威に転化することになる。高度情報化社会の恩恵を享受するために、情報セキュリティへの取り組みが強く求められている。

情報セキュリティとは、「正当な権利を持つ個人が、情報や情報システムを意図通りに制御できること」であり、情報セキュリティマネジメントの国際標準である ISO/IEC 27002 には、「情報の機密性、完全性、および可用性を維持すること」と定義されている。ここで、気密性とは許可された者だけが情報にアクセスできるようにすることで、完全性とは、情報や情報の処理方法が正確で完全であるようにすることである。また可用性とは、許可された者が必要な時に情報や情報資産にアクセスできることを確実にすることである。

情報資産として、財務情報、人事情報、顧客情報、戦略情報、技術情報などがある。個人および組織には多くの情報資産が蓄えられており、IT の普及に伴い、情報の価値は非常に高くなっている。「リスク」とは、情報資産を脅かす内外の要因（脅威）によって、情報資産が損なわれる可能性を言う。組織に内在している要因は、ソフトウェアの脆弱性、セキュリティ機能の欠如、セキュリティモラルの欠如などで、外部からの要因は、ウィルス、侵入、サービス妨害などがある。また、実際に情報資産が失われてしまった事態をインシデントと呼ぶ。大切な情報の損失は、企業にとっても個人にとっても大きなダメージをもたらす。企業の場合には、その存続を脅かす場合もあり、情報資産を守るための方策やセキュリティ対策は企業経営にとって必要不可欠である。

企業活動などの組織活動においては、電子記録の利活用が重要となる。今や電子文書（電子記録）は社会の隅々にまで浸透し、組織内外の活動は電子文書を抜きにしては考えられない。電子文書を記録として活用・保存していくことによって、組織内外の活動のみならず、社会全体の効率を向上させることができる。これを実現していくために、e-文書法が施行され、法令等で保存を義務付けられている文書を、一部の例外を除き、電子文書・電子化文書で保存できることとなった。また、2009 年には、政府、公共機関で取り扱う記録の全体を規定した公文書管理法が制定された。

クラウドコンピューティングやモバイル端末などの ICT 環境の変化が、電子文書の利活用の安全性に大きく影響を与えている。クラウドコンピューティングの仮想化環境やマルチユーザの場合には、ユーザ間またはプロセス間での情報漏洩、盗み見などが起きる恐れが指摘されている。また、クラウドコンピューティング運営企業における不正利用のおそれもある。モバイル端末を利用する際、重要なデータを保存して持ち歩くことができるため、紛失や盗難の恐れがある。

このような電子記録の利活用環境を想定すると、多くのセキュリティ課題が考えられる

が、ここでは主要な以下の 5 つを挙げる。

（1）データ秘匿（機密性）

これまでは、保護すべきデータは組織内や特定のデータセンターに保管されることが多かったが、近年ではパブリッククラウドに保管されることが多くなり、安全性の課題も大きくなっている、

（2）真正性の確認

真正性とは、文書は作成者本人が作成したこと（本人性)、およびその文書が改ざんされていないこと（完全性）を言う。真正性の確認方法として、デジタル署名やタイムスタンプがある。

（3）可用性

可用性とは、許可された者が必要な時に情報や情報資産にアクセスできることを確実にすることです。コンピュータウィルス感染や自然災害によるシステムダウンなどで情報が使えなくなる、などといったことを防ぐことで確保される。

（4）アクセス制御

「適正な利用者」のみが「適正な権限」でのみ利用できることを確保することが重要である。電子記録管理システムは、クライアントサーバシステムとして提供される。利用者は、自身の端末から LAN やインターネットなどを介して電子記録管理システムにアクセスし、利活用を行う。このため、利用者の識別、認証が重要となる。

（5）法令順守

セキュリティ対策を行わずに情報流出などのインシデントにあった場合に、法的な処分を受けるため、セキュリティ対策は必須となる。情報管理に関する法律としては、個人情報保護法、マイナンバー法（番号法)、不正競争防止法などがある。

本説明書では、組織活動で重要となる電子記録の利活用において、主としてデータ秘匿（機密性）と可用性に関わる安全性に大きく寄与する「秘密分散技術（電子割符)」について、その位置付け、仕組み、適用事例および有効性について説明する。

第 2 章　秘密分散技術（電子割符）の位置付けと仕組み

保護すべきデータの秘匿性を確保する方法として、暗号技術と秘密分散技術を挙げ、まず初めに暗号技術の活用と課題について述べ、つぎに秘密分散技術の位置付けと仕組み概要について述べる。

2.1　暗号技術の活用と課題

（1）推奨される暗号アルゴリズム

暗号化は情報セキュリティ技術に必要不可欠なものとなっており、主に通信の暗号化やデータの暗号化等に利用されている。世の中で利用されている暗号技術には様々なものが

あるが、安全で実装性に優れた暗号技術を利用することが重要である。さらに、電子政府推奨暗号を評価する、暗号評価プロジェクト「CRYPTREC」（Cryptography Research and Evaluation Committees）では、従来から安全性、及び実装性に優れていると判断され、また、市場における利用実績が十分であるか今後の普及が見込まれると判断された「電子政府推奨暗号リスト」を公表している。

（2）クラウドで利用される暗号技術

近年ではクラウドが普及したことに伴い、クラウド上に保管しているデータの秘匿性や情報漏洩等に関して、利用者の不安が多くなってきている。そのため、データを暗号化して保管する等の対策がとられているが、従来のデータ共有サービスでは、再度、重要データ等を暗号化する、鍵を再配布する等、利便性に課題があった。

そこで、クラウドの利便性を損なわないクラウド向けの暗号技術が開発されてきているが、その１つとして再暗号化技術がある。再暗号化技術とは、暗号化されたデータを復号することなく別のユーザの鍵に付け替え可能な暗号方式である。付け替え専用の暗号化鍵を使うことで、暗号化されたデータを復号することなく別のユーザの鍵に付け替えられ、データは常に暗号化されている。そのため、万一、クラウドストレージ上のデータが漏えいしても暗号化前のデータが漏洩する可能性は少ない。

（3）暗号化鍵の管理

クラウド向けの暗号技術が開発されてきてはいるが、データの漏洩と共に鍵も漏洩してしまうと、漏洩したデータが復号されてしまう可能性があるため、鍵を安全に管理することが重要になってくる。そのため、クラウドでは HSM（Hardware Security Module）と言われるハードウエア暗号装置を利用する場合がある。HSM は、対タンパー性（容易に外部から解析できないように様々な防護策を講じ、非正規な手段による機密データの読み取りを防ぐ能力）を備えた製品が各ベンダーから提供されている。

（4）現代における暗号の課題

サイバーセキュリティ基本法をはじめとした IT 関連法や改正個人情報保護法、番号法、更に不正競争防止法等情報管理の厳格化を要求する法令が多くなっていることは否めない。例えば、番号法に関し、つぎの「個人情報保護委員会」の Q&A（Ｑ９－２、Ａ９－２）がある。

Ｑ９－２：個人番号を暗号化等により秘匿化すれば、個人番号に該当しないと考えてよいですか。

Ａ９－２：個人番号は、仮に暗号化等により秘匿化されていても、その秘匿化されたものについても個人番号を一定の法則に従って変換したものであることから、番号法第２条第８項に規定する個人番号に該当します。

この Q&A では、暗号化されたデータであっても個人情報とみなすという判断があり、情報漏洩の防止対象となってしまう、という課題がある。この課題について新たな安全管理措置が必要な時代となってきており、秘密分散技術を適切に用いた方式が提案されている。

2.2　秘密分散技術の位置付け

電子データ秘匿の技術として、秘密分散技術に注目が集まっている。クラウドの利用を踏まえた IT 環境における電子データの秘匿・保護に秘密分散技術の原理的特性が役立つことが注目を浴びている理由である。

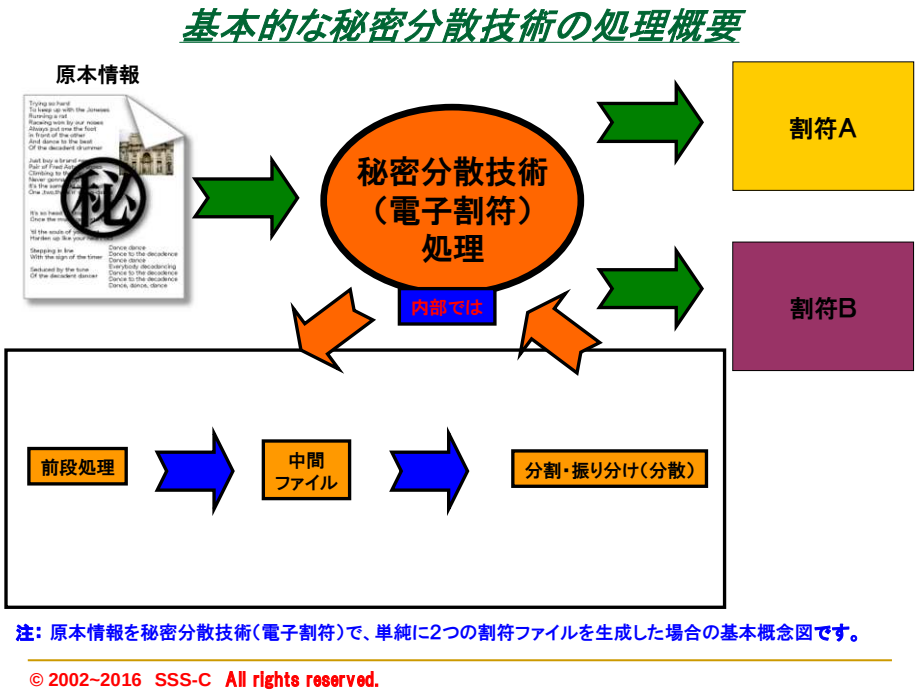
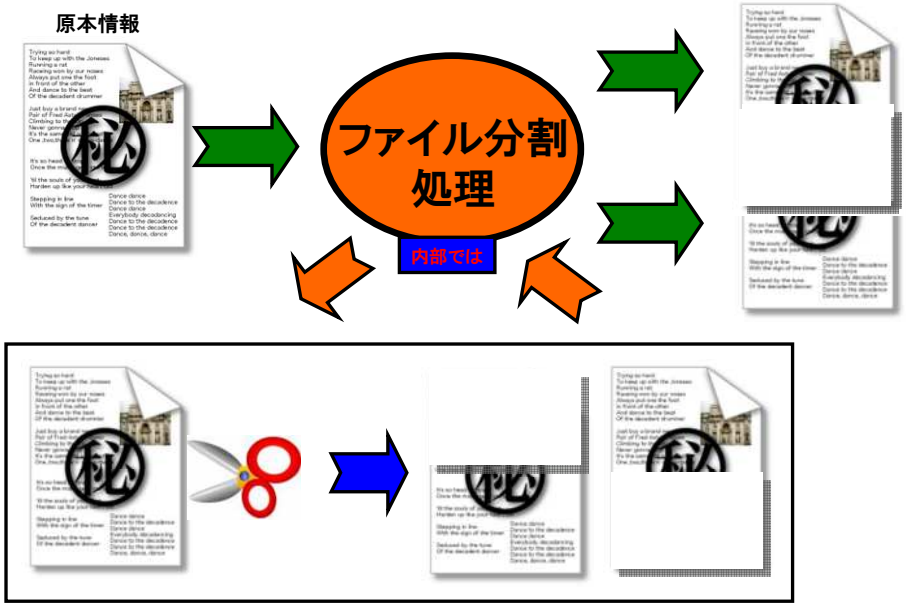


図１　基本的な秘密分散技術の処理概要

秘密分散技術とは上記図１に示すように、基本的には原本情報を割符化して利活用する為の処理。但し、単純に電子情報のファイル等を分割しただけでは、勘合貿易で利用した勘合符のように、に原本情報の一部がそのまま出てきてしまい、これでは現代のデジタル社会で通用する独立した新セキュリティ技術としては役立たない。例えば図２のように単体の割符ファイルから原本情報の一部が解読され、個人情報の一部等が出てしまう懸念が十分残るようでは、法令上の定義にも抵触してしまう可能性を否定できない。



注: 原本情報を、単純に2つにファイル分割した場合の基本概念図です。

図２　単純なファイル分割

この課題を解決したのが秘密分散技術である。但し、既存電子データ秘匿技術の雄である暗号化と同様に論ずることはできない。なぜならば安全性の根拠となる原理原則が既存暗号技術とは大きく異なる為である。原本情報を構成するビットが実際に分割・分散処理され、複数のファイル（割符ファイル）が生成出力されることとなり、そのうちの単体の割符ファイルには原本情報のビットが欠落してしまっている状態となっており、欠落部分が未知の状態になっているからである。

これは、デジタルデータの原理的特性として一定のビット数が意味を成すように連続して並んでいることが大原則であり、そのビットの並びが入れ替わってしまったり、欠落してしまうと、基本的には本来の正しい情報を保有・表現できなくなってしまうという特性を情報セキュリティに応用した技術と言える。秘密分散技術は、デジタルデータの原理的特性を利用した処理を行うことにより、原理的に原本情報の保護等を実現しており、数学理論等を背景として開発当初から理論的な安全性を実現すべく誕生した技術ではなく、原理的特性（敢えて言うならば「集合論」を背景とした現実にビット分割・分散）の処理技術を用いて、実社会で有益に利用できる新たなセキュリティ技術を実現した。というところに、立脚点の違いがある。但し、今後本書に続いて公表予定の「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　―　において、詳細解説予定であるが、原本情報をビットレベルで分割しそれらのビットを複数の割符ファイルに振り分ける処理を行うと言っても、単純なビットの割り振り方をしたのではビットレベルでの分割処理を

行う前の対象情報ビット位置等が容易に推定できてしまい、原本解読までも容易になってしまう危険性が残ってしまう為、基礎技術である秘密分散技術を開発し市場供給する者は、そうした技術実装方法に関しても外部有識者等にアルゴリズム開示したとしても、支障なく実社会で利用できる基礎技術であるといった評価が受けられるレベルの技術として市場に供給しなければならない。

このようにセキュリティに関する土台部分の原理的構造が既存セキュリティ技術と異なることから、内閣サイバーセキュリティセンターが公開する資料等で暗号とは異なる技術として記述されていることも頷けるものである。また、設計思想として共通点のある数学（暗号）理論である秘密分散法も「理論」と「技術」という違いがある。という意味で、一線を画す新技術と言える。

2.3　秘密分散技術の仕組み

2.3.1 秘密分散技術の基本的な考え方

秘密分散技術の基本的な考え方として、電子情報（原本）を実際に分割して複数の割符（割符ファイル）にして秘匿する集合論的な考え方と、数学的なしきい値分散法の考え方の二つについて説明する。

（１）割符の考え方

「割符」の考え方は歴史的に古い時代から存在しており、室町時代の勘合貿易における勘合符、中国における軍割符、忍者同士の合言葉といった手法にも通じるもので、秘匿すべき情報を割符にして関係当事者でシェアし、必要な時に割符を開示し合い対象情報を復元して利活用する。

基本的には原本情報を割符化して利活用するための処理であるが、前述の図２に示すように、単純に原本情報となる電子情報のファイルを分割しただけでは、原本情報の一部がそのまま出てきてしまう。これでは、ファイル分割した分割片から原本情報から一部が抜き出されて個人情報の一部が出てしまうことになってしまう。前述の「個人情報保護委員会」の Q&A で、個人番号は、仮に暗号化等により秘匿化されていても、その秘匿化されたものについても個人番号を一定の法則に従って変換したものであることから、番号法第２条第８項に規定する個人番号に該当します。との認識が示されていることから、単純に暗号化してファイル分割する。といった処理も暗号化の延長線上でしかなく、分割片に暗号化部分がそのまま出てきてしまう（図３）ことから、安全管理措置として問題が生じる。

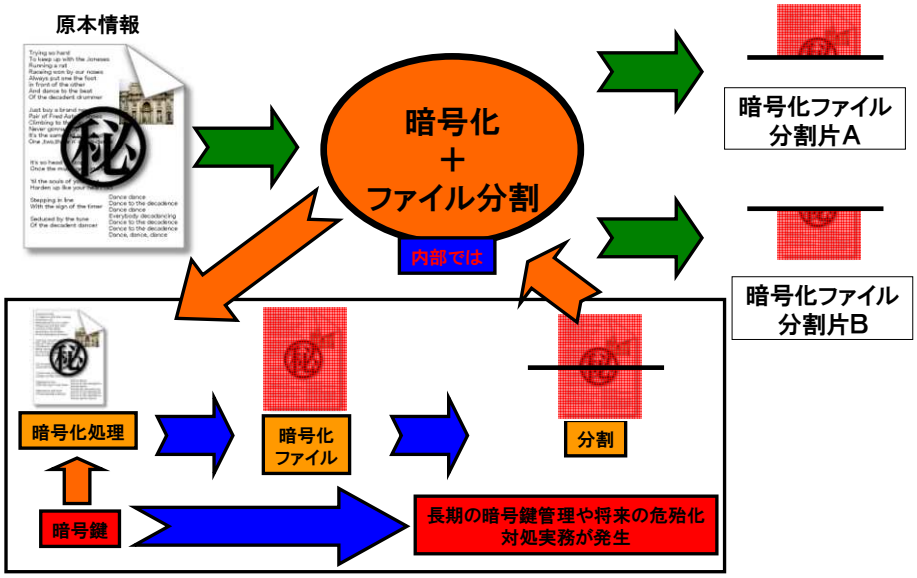


図３　暗号化と単純なファイル分割の組み合わせの概念図

秘密分散技術（電子割符）が既存暗号技術とは異なる技術・手法であるという認識は、参考資料６や７にも明確に記されており、現時点では暗号化とは一線を画す技術として標準化を推進していることもあり、似て非なる亜種や法令解釈上も懸念を残す技術が消費者保護の観点からも問題を起こさないようにするため、原理的に単体の割符ファイルから原本情報の一部でも取り出せなくなるような、次の 2.3.2　秘密分散技術の処理の仕組み　で紹介するビットレベルでの分割処理を行う等の電子割符の仕組みが必要である。尚、新たなアルゴリズム等を標準化に加える可能性を否定しないことは、当初から想定している。

（２）しきい値分散法

秘密分散技術では、元データ（原本情報）を複数のデータ（分散情報：割符ファイル）に分けてデータを秘匿するものである。復元に際しては、分割したうちの決められた数片の「分散情報（割符ファイル）」を集める必要がある。この秘密分散法は、RSA 暗号で有名なシャミア博士により最初に論文発表されたもので、「しきい値分散法」と呼ばれる最も一般的な方法である。その仕組みは、図２に示すように、直線などを表す連立方程式で説明することができる。例えば、ある秘密にしたい元データ S を以下の式で表現できるとする。

$$F(X) = aX + S$$

このとき、a が不明である場合、S を求めるためには直線 F(X)を決める必要がある。直線は直線上の２点（(P、Q）を決めると求めることができ、同時に秘密情報 S を求めること

ができる。このときの２点が「分散情報」に相当する。また、このことから秘密分散技術は「計算量的安全性」ではなく、「情報理論的安全性」に基づいていることが明らかになっている。情報理論的安全性とは、無限の計算能力と記憶装置を持つ計算機でも解けないことをいう。ちなみに、一般に流通する暗号商品は計算量的安全性に基づいている。

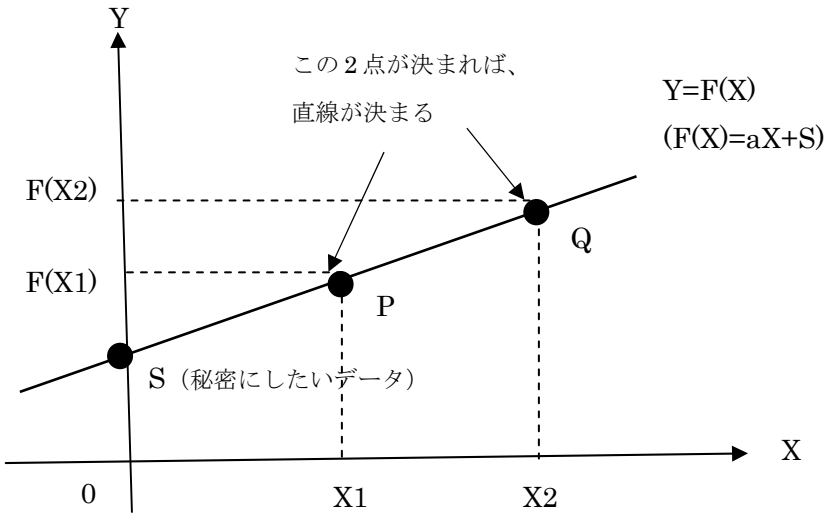


図４　しきい値分散法の概念

但し、秘密分散法でも秘密分散技術でも、復元に必要な分散情報や割符ファイルまであと 1 つというところまで取得し、最後の１つである分散情報や割符ファイルを偶然にも作すことができれば、原本情報復元の可能性はある。こうした攻撃はまさに力技や偶然といった部分が介在するのであるが、そうした最後の分散情報や割符ファイルを作り出すことができる可能性を導き出すとすると「計算量」で表現することとなる。（工学的に可能な計算量か否かは別として）これは想定する攻撃手法等によって表現の仕方や評価の仕方が変わる可能性のあるところであって、一般に十分理解されているとは言い難い。

2.3.2　秘密分散技術の処理の仕組み

現在標準化を進めている秘密分散技術の処理は、（参考資料１０や１５）などの既公開資料や公的実証成果等がベースとなっているが、概要編として暗号や数学の専門的知識を持たなくても一定の理解ができるよう、当該技術の処理概要を以下に解説する。

文書・画像・ソフトウェアなどのデジタルデータ（以下「元データ」と呼ぶ）を秘匿する技術としては、公開鍵暗号が広く用いられている。その暗号文を「金庫」、復号鍵を「錠前の鍵」に例えるならば、元データを「金庫」に収納（暗号化）して「錠前」を掛けることで、「鍵」を持つ人だけが元データを取り出せるようになる、という具合である。一方、電子割符技術の原理はこれと異なる。前提として、デジタルデータである元データはその種類に関わらず、究極的には０や１という数字（ビット）の並びである。秘密分散技術（電

子割符）では、図５に示すように元データをビット単位に分解し、それらを毎回異なる振り分け方で無作為に振り分けて複数の集合（「割符ファイル」と呼ばれている）に分割している。そして、割符ファイルがすべて揃えば、特殊な操作によって元データを復元することが可能となる。一方、割符ファイルが一つでも欠けた状態では元データを復元できない、ということが期待されるようにデータの分割方法が設計されている。

この元データを複数に分割するという設計思想自体は、暗号理論における秘密分散法と相通ずる。電子割符技術の割符ファイルに相当するデータは、秘密分散法では「分散情報」などと呼ばれている。例えば、元データを２個の分散情報に分割する場合、分散情報が二つ揃えば元データを復元できるが一つだけでは復元できない、という具合である【注１】。さらに、理想的な安全性を実現する秘密分散法【注２】は、

- 残りの分散情報が揃わない状態では、分散情報の各々は「完全にランダムなビットの並び」と全く区別できない

という顕著な特徴を持っている。

【注１】秘密分散においては、分散情報が「全部揃うかどうか」だけでなく、例えば３個の分散情報のうちいずれか２個以上揃うと元データを復元できる、といったより複雑な設定も可能であるが、当文書ではそこまで深入りしない。

【注２】例えば、Adi Shamir 教授が 1979 年に提案した方式などが知られている。

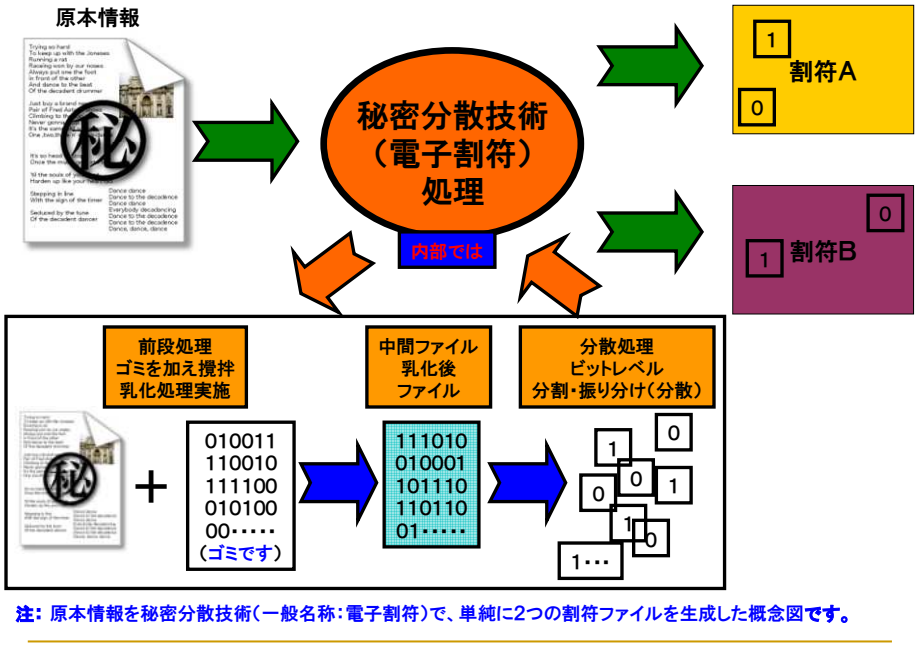


図５　秘密分散技術の処理の仕組み

上述の通り、電子割符技術も秘密分散法と同様の設計思想に基づいていることから、もし電子割符技術が理想的な安全性を実現できていれば、割符ファイルの各々は「廃棄処理後の残渣」と同様に振る舞い、どれだけ長い時間が経ってもその安全性が損なわれないと期待される。例え話としては、元データが白黒の碁石（ビット）を碁盤に並べた盤面であるならば、割符ファイルはその中から取り出されたいくつかの碁石に対応する。このとき、取り出した碁石（割符ファイル）がすべて揃っていない状況では、足りない碁石の色や個数の手がかりが無いため、どれだけ時間をかけて考えても元々の盤面を特定することはできないであろう、という発想である。（中略）

通常の暗号技術の標準的安全性レベルである「80 ビット安全性」では、暗号の解読が 2 の 80 乗（およそ 10 の 24 乗）通りの全数探索と同程度以上に困難であることを要求している。一方、現時点での安全性評価では、例えば、攻撃者が 3 個ある割符ファイルのうち一つのみを入手した状態で元データを完全に復元できる可能性について、およそ 10 の 105,000 乗通りの場合の数から正解を言い当てるのと同程度に困難であるとの見積もりを得ている（なお、この数値は、アイスランド（人口約 33 万人）の国民全員が一斉にコインを投げて全て表が出るのと同程度に「現実にはまず起こらない」確率である）。ここで、「80 ビット安全性」は暗号解読に必要な「計算量」を尺度とする評価である一方、今回の安全性評価は元データを正しく復元する「確率」という異なる尺度を用いているため、両者は直ちに比較できないと思われるかもしれない。しかしながら、「80 ビット安全性」の基準である「2 の 80 乗通りの全数探索」において、探索の最初の候補が偶然にも正解であったために解読が瞬時に成功してしまう確率ですら 2 の 80 乗分の 1 はあることを鑑みると、元データを正しく復元できる確率が 2 の 80 乗分の 1 を下回るならば実用的な暗号技術の安全性レベルとして問題ないものと考えられる。つまり、こうした攻撃者に対する安全性という観点に限れば、電子割符技術の安全性は暗号技術の標準的安全性レベルを大きく上回っている（現時点での安全性評価で得られている内容に限るならば、充分な情報理論的安全性を持っていると考えられるレベルにある）と解釈することができる。

2.3.3　秘密分散技術の運用の基本的な考え方

広く社会に貢献すべき当該技術を実装したシステムを運用する際には、現在及び今後必要となる法令等の要求を見越した機能への対処を、可能な限り実現しているものを選択し、更に、原理的特性から、復元に足る数の割符が全て攻撃者に入手されないよう工夫することや、復元に必要なプログラム利用権限等の管理を適切に実施することは当然である。

これは技術自体の内容（アルゴリズム）も大事であるが、実際の利用シーン等を想定するならば、そうした技術をシステムで利用する際のシステム構築や技術の適切な実装のあり方（プロトコル）が大事であるとする情報セキュリティに於ける公的報告書等（参考資料１２）の基本認識とも符号するところである。

第 3 章　秘密分散技術（電子割符）の基本的な利用モデルと適用事例

3.1　秘密分散技術の基本的な利用モデル

利用モデルの基本は電子記録の「保管」と「移送」の二つである。その他の機能や役割は、これらの二つに関連して実現されるものである。

（1）保管

保管の利用モデルに関連して、BCP、内容証明、廃棄、認証応用などがある

（2）移送

なお、情報管理における秘密分散技術（電子割符）の基本的な利用モデルにおいて「保管」「移送」はそれぞれ別な目的として便宜上分類しているが、運用上の実態としては「時間軸」という運用上不可避な要素をプラスすることで、「保管とは、時刻（場所等の条件含む）A から将来の時刻（場所等の条件含む）B への情報移送」を実行しているにすぎないことが分かる。

また、IT 環境の利活用が多様になってきており、分散情報（割符）の保管場所としてクラウド、モバイル、スタンドアローン、外部記憶メディア、印刷などがあり、多様な保管場所が可能となっている。

3.2　秘密分散技術の適用事例

3.2.1　秘密分散技術の適用事例（保管・BCP）

情報セキュリティ対策について、内閣サイバーセキュリティセンター（旧内閣官房情報セキュリティセンター）から示されている「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」がある。この中の、

2.3.2.3 サーバ装置、遵守事項、(2) サーバ装置の運用時、

において、以下の記述がある。

b) 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置については、サーバ装置の運用状態を復元するために必要な措置を講ずること。

（解説）：サーバ装置の運用状態を復元するための必要な措置を講ずることによりサーバ装置に保存されている情報及びその情報を用いたサービスの可用性の担保を目的とした事項である。サーバ装置の運用状態を復元するための必要な措置の例として、以下のようなものがある。

・サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。

・前回内容からの変更部分の定期的なバックアップを実施する。

・サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。

・バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。

また、取得した情報を記録した電磁的記録媒体は、施錠された保管庫に保存等して、業

務上の必要がある場合にこれらの情報を利用する情報システムセキュリティ管理者に限ってアクセスできるようにする。なお、災害等を想定してバックアップを取得する場合には、記録媒体を耐火性のある保管庫や耐震性の高い施設、同時被災しない遠隔地にある施設に保存することが考えられる。その際には、情報を遠隔地に送信や移送する際のセキュリティ及び取得した情報の保管時のセキュリティを確保する必要がある。セキュリティを確保する措置の例としては、暗号や秘密分散技術を利用して情報の漏えいや改ざんを防止することが挙げられる。

上記のような「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」における記述に対応する対策の実現例として、図６、図７、図８に示す秘密分散技術の適用事例がある。

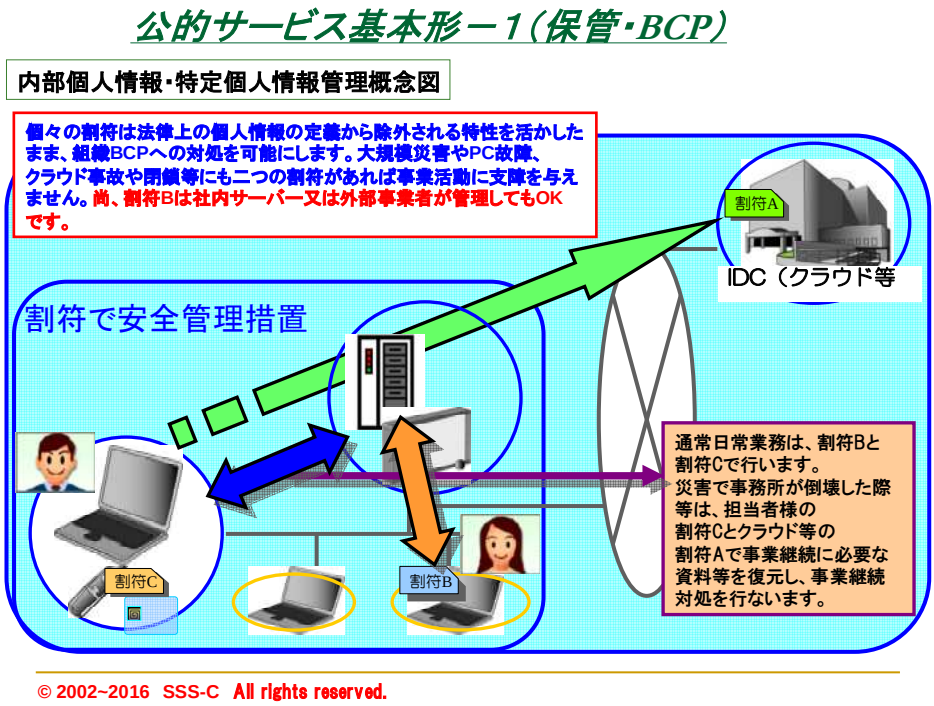


図６　秘密分散技術の適用事例（保管・BCP）－１

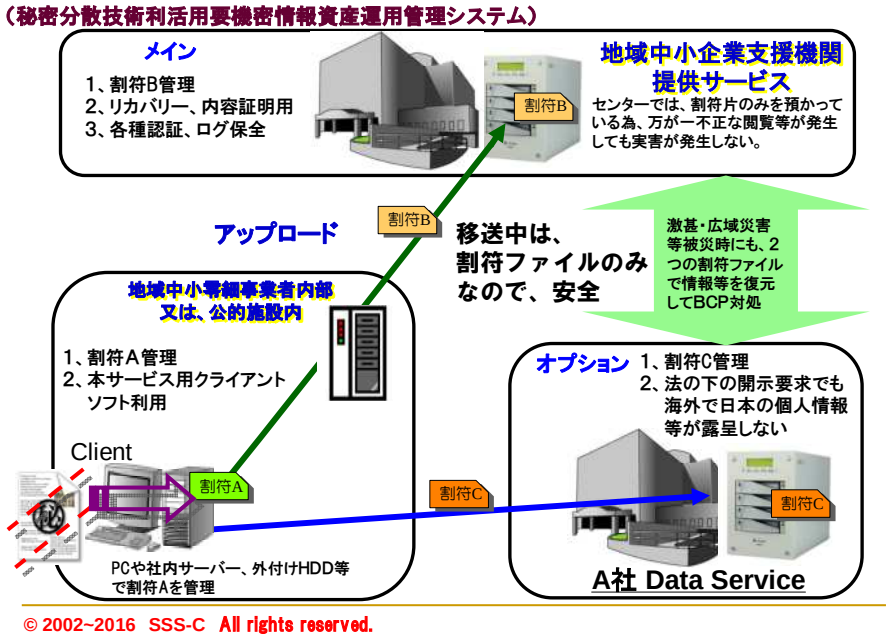


図７　秘密分散技術の適用事例（保管・BCP）－２

図８　秘密分散技術の適用事例（保管・BCP）－３

3.2.2　秘密分散技術の適用事例（移送）

情報セキュリティ対策について、内閣サイバーセキュリティセンター（NISC、旧内閣官房情報セキュリティセンター）から示されている「 府省庁対策基準策定のためのガイドライン　 平成26年5月19日」がある。

この中の 3.1.1 情報の取扱い、(6)情報の運搬・送信、において以下の記述がある。

行政事務従事者は、要機密情報である電磁的記録を要管理対策区域外に運搬又は府省庁外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。

a）運搬又は送信する情報を暗号化する。

b）運搬又は送信を複数の情報に分割してそれぞれ異なる経路及び手段を用いる。

c）主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。

（解説）

基本対策事項3.1.1(6)-2 b)「複数の情報に分割して」について

この考え方は、秘密分散技術といわれ、例えば、１個の電子情報についてファイルを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。

上記引用の「 府省庁対策基準策定のためのガイドライン　 平成26年5月19日」にある通り、秘密分散技術を用いる場面とは、b) 運搬又は送信を複数の情報に分割してそれぞれ異なる経路及び手段を用いる、という記載のとおりであり、上記（解説）での例示のように暗号化との併用が必須ということではない。更に、前述のように法令上の要求事項をクリアすることが難しくなってしまった現状の暗号商品の機能を補完する役目も認められると考えられる。

上記の「 府省庁対策基準策定のためのガイドライン 平成 26 年 5 月 19 日」における記述に対応する対策の実現例として、図９に示す秘密分散技術の適用事例がある。

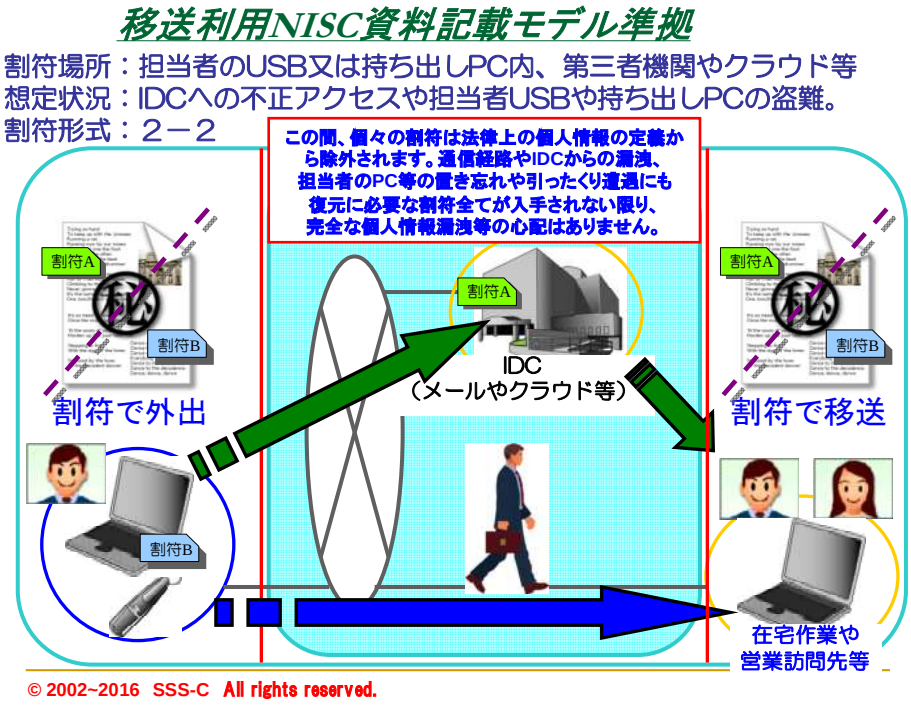


図９　秘密分散技術の適用事例（移送）

3.2.3　秘密分散技術の適用事例（廃棄）

・個人情報保護委員会の Q&A 等を引用

・経済産業省との意見交換結果である、割符単体の漏えい時の大臣報告の方針等を記載。

経済産業分野個人情報保護法ガイドの廃棄の例には、

・　個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に１回又は複数回上書きする。）

ここでいう意味のないデータを媒体に～が、割符ファイル単体も対象と考える。

技術的にも、個々の割符ファイルそのものは原本情報が出てこないことに加え、法令解釈上も定義項に該当しない為、単独の割符ファイルが外部に流出等した場合、外部第三者から見ると単なる「ゴミ（事実上廃棄処理後の残渣）」でしかない。という特長を持つ。

第４章　秘密分散技術の有効性

本章では、秘密分散技術の有効性として、その具体的な効果と法令遵守からの意義について述べる。

4.1　秘密分散技術の効果

前章にて述べたように、秘密分散技術は「データ秘匿」、「移送時の安全性確保」、「BCP（激甚災害対処も含む）」、データの合理的な廃棄処理や認証等へ適用することができる。さらに、割符ファイル単体での流出の際にも、図１０に示すように、データが漏洩されないような仕組みとなっている。また当該技術の原点に戻れば、処理原理が一般人にも理解しやすいことや、心象主義の日本の裁判制度への対処がし易いことなどがある。さらに、原理的な安全性の高さがあること、及び中長期の安全性に寄与する効果もある。また、複数ソリューションが個別に対処していた機能が、秘密分散技術（電子割符）を合理的に用いると１つの仕組みで対処できる可能性があり、トータルコストが抑制される効果もある。

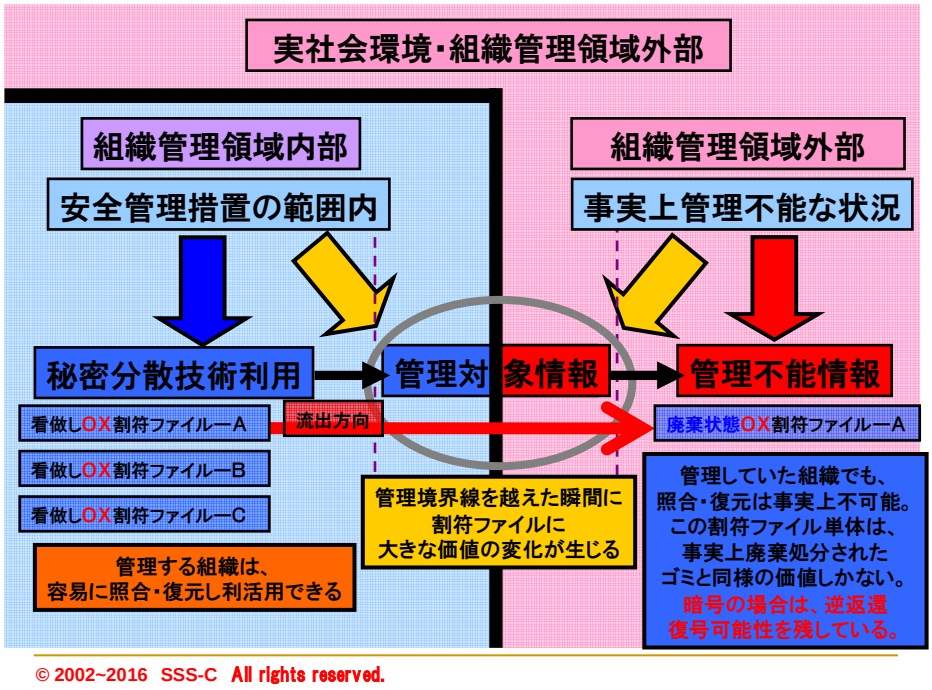


図１０　割符ファイル単体流出の説明図

4.2　法令遵守からの意義

「秘密分散に関する技術ガイドラインおよび秘密分散技術利活用に関するガイドライン、ECOM、2010 年 3 月」報告書において、弁護士・牧野二郎氏からの「情報分散管理技術（電子割符技術を利用した情報管理）に関する法的意見書」が記載されている。この中に、以下の「第６　法的リスクの低減効果」および「第７　まとめ」の記述がある。

―引用部開始―

第６　法的リスクの低減効果

一般に、個人情報の漏えい事故を起こした企業は様々なリスクを負担することになる。

漏えいした事実を公表し、謝罪し、信用を保護すべく多大なコストと作業が必要とされ、また、漏えいした情報の本人が原告となり、訴訟を提起される危険も存在する。こうした社会的、経済的リスク及び訴訟リスクを回避する点で、電子割符は有効に機能すると考えられる。

（１）経済的損失の回避

～仮に個々の電子割符が漏えいしたとしても、それを受領した者は、それが個人情報であるか、その断片であること自体を理解できないとされ、そうであれば、情報本人の識別情報や属性情報が悪用される（負債情報を元に振り込めサギなどが行われる危険など）ことはなく、被害は発生しない。

（２）訴訟リスクの回避

一般に訴訟を提起する場合、原告となろうとする者が、自らの権利を侵害するものであることを示す必要がある（原告適格)。ところが、本件における個々の電子割符の場合、その情報からは識別情報の復元は可能ではないとされ、当該電子割符が誰の情報であるかを特定することができず、結局仮に誰かがこれを取得したとしても、その情報が自身のもの（個人情報）であることを立証することができないため、原告たりえないという結論となる。こうして、電子割符技術により、多くの場合訴訟リスクも回避されると考えらする。ただし、全ての電子割符が事業者の手元に存在する場合、また、それを管理するという関係からは統合・復元が可能である限りにおいて、既に述べたように当該事業者にとって、それらの情報は未だ個人情報であるため、その一部でも漏えいする場合には、個人情報の一部の漏えいと理解される危険が有る。その点で個人情報の管理において、管理ミスがあったと評価されるため、内部統制上は、個人情報の管理体制の確立、充実に向けて厳しく対応しなければならないこととなる。

第７　まとめ

電子割符の技術は、こうして法的観点からも、情報管理体制整備を進める上で、有効な技術と評価することができる。しかし、同時に、電子割符は技術として提供されるため、それを管理する管理手法の整備が伴わなければならないことは言うまでもない。いくら優秀な技術であっても、運用のルールや運用における点検整備が実施されない限りは万全のものとはならない。

以上の「情報分散管理技術（電子割符技術を利用した情報管理）に関する法的意見書」における「第６　法的リスクの低減効果」および「第７　まとめ」の記述にあるように、秘密分散技術は、「経済的損失の回避」と「訴訟リスクの回避」などに対して多大な効果があると言える。

―引用部終了―

更に、特に注目すべきは、実際に組織内で管理している何らかの電子データ等が外部に出た際の、社会側からの見え方の違いである。ここは、既存セキュリティ技術（例えば暗

号化）であると、組織内部からも外部からも法令上何らかの意味のある電子データ等の流出となり法令違反となることに対し、秘密分散技術（電子割符）を適切に用いた組織から割符ファイル単体が外部に出た際に、その割符ファイル単体を入手した社会からは、単に単体では無意味・無価値な法令の定義項から除外された電子ファイルが組織外部に出てきた状態となる。こうした社会の評価の大きな相違点がある。（組織内部にとっては、管理している電子ファイルが外部に出たという事実までは当然消えない）

　このことの意味の違いは、事故発生を想定した情報管理を実施しなければならない組織にとっては非常に大きなもので、参考資料(26)の個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成２６年１２月１２日厚生労働省・経済産業省告示第４号）平成２６年１２月　経済産業省　記載の、

2-2-3-2. 安全管理措置（法第２０条関連）法第２０条

組織的安全管理措置【各項目を実践するために講じることが望まれる手法の例示】

⑤「事故又は違反への対処」を実践するために講じることが望まれる手法の例示

ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。

・漏えい等をした事業者以外では、特定の個人を識別することができない場合

（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合。ただし、（オ）に定める報告の際、漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること。）

や、

（オ）主務大臣等への報告

ｂ．個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合経済産業大臣（主務大臣）に報告を行う。

ｃ．関係機関への報告

・ファクシミリやメールの誤送信（宛名及び送信者名以外に個人情報が含まれていない場合に限る。）以下略。

（カ）事実関係、再発防止策等の公表

ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。

・漏えい等をした事業者以外では、特定の個人を識別することができない場合

（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合。ただし、（オ）に定める報告の際、漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること。）

といった記述内容に合致するものと考えられ、(秘密分散法コンソーシアムの確認では、少なくとも暗号よりは高度な安全管理措置を実施していると考えられる。との回答を得ている。)

実害が発生しないことに加え法令上の記載は無いものの、上記のように、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。

の文言を受け、適切に秘密分散技術(電子割符)を用いて情報管理を実施している組織は、本人への連絡や事実関係、再発防止策等の公表を省略できると考えられますが、今後の社会の健全な発展に寄与させるべき情報提供として、そのような事実関係を把握した際には、そうした事実があったことと秘密分散技術を適切に用いた情報管理を実施していたことを主務大臣に報告することを秘密分散法コンソーシアムは推奨している。

http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf

第5章　おわりに

本説明書では、高度情報化社会における電子記録の利活用に際して、主としてデータ秘匿(機密性)と可用性に関わる安全性に大きく寄与する「秘密分散技術(電子割符)」について、その位置付けと仕組み、利用モデルと適用事例およびその有効性について説明した。

秘密分散技術の仕組みにおける基本的な考え方として、割符の考え方としきい値分散法について説明し、秘密分散技術は多くの人に理解し易い方式であると同時に、安全レベルの高い「情報理論的安全性」を持つことを述べた。また利用モデルとして、特に「保管」と「移送」について、その適用事例と共に説明し、秘密分散技術は公的機関にて示された安全対策のガイドラインを満たすことができる安全性の高い技術であることを示した。また、その効果について、利用における具体的な効果と共に、法令遵守からの意義についても法律専門家からの意見を基に、その有効性について述べた。

＜参考資料＞

(1) 「情報セキュリティ読本(四訂版)」、IPA、2014年11月.

(2) CRYPTREC: http//www.cryptrec.go.jp

(3) 特定個人情報保護委員会：http://www.ppc.go.jp/legal/policy/answer/#q9-2

(4) A. Shamir, “How to share a secret”, Communication of ACM, 22, 11, 1979, p.612-613.

(5) 土井　洋：「秘密分散法とその応用について」、情報セキュリティ総合科学、第4巻、pp.137-149、2012年11月.

(6) 「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」：http://www.nisc.go.jp/active/general/pdf/K305-111C.pdf

(7) 「 府省庁対策基準策定のためのガイドライン　平成 26 年 5 月 19 日」:
http://www.nisc.go.jp/active/general/pdf/guide2014_draft.pdf
(8) 「電子記録管理に関する調査検討報告書 2013」、JIPDEC、2014 年 3 月 :
http://www.jipdec.or.jp/archives/publications/J0005041
(9) 「電子記録管理に関する調査検討報告書 2014」、JIPDEC、2015 年 3 月 :
http://www.jipdec.or.jp/archives/publications/J0005038
(10) 「EC における情報セキュリティに関する活動報告書 2009」:
http://www.jipdec.or.jp/archives/publications/J0004291
(11)「暗号利用技術ハンドブック」　ECOM（現 : JIPDEC）1997 年 2 月 :
http://www.jipdec.or.jp/archives/publications/J0004048
(12)「暗号利用技術ハンドブック（第２版)」　ECOM（現 : JIPDEC）1999 年 3 月 :
http://www.jipdec.or.jp/archives/publications/J0004104
(13)「認証のレベルと本人確認方式に関する提言」　ECOM（現 : JIPDEC）1999 年 3 月 :
http://www.jipdec.or.jp/archives/publications/J0004080
(14)「分散データ管理」　特許庁　標準技術集　クライアント上の情報セキュリティ技術 :
https://www.jpo.go.jp/shiryou/s_sonota/hyoujun_gijutsu/info_sec_tech/e-1-2.html
(15)「電子割符方式の現状の安全性評価　追補版」　共同研究 : 国立研究開発法人産業技術総合研究所、グローバルフレンドシップ株式会社　2015 年 11 月 :
http://www.gfi.co.jp/01news20151226_393.html
(16)「特定個人情報の適切な取扱に関するガイドライン（行政機関等・地方公共団体等編)」
個人情報保護委員会　2016 年 1 月 :
http://www.ppc.go.jp/files/pdf/160101_guideline_gyousei_chikoutai.pdf
(17) 「特定個人情報の適切な取扱に関するガイドライン（事業者編)」
個人情報保護委員会　2016 年 1 月 :
http://www.ppc.go.jp/files/pdf/160101_guideline_jigyousya.pdf
(18)行政機関の保有する個人情報の適切な管理のための措置に関する指針について（通知）
総務省　総管情第 84 号　平成 16 年 9 月 14 日
［一部改正］平成 26 年 12 月 26 日 総管管第 100 号
［一部改正］平成 27 年 8 月 25 日 総管管第 70 号
http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/040914_1.html
(19)行政機関の保有する個人情報の適切な管理のための措置に関する指針について（通知）
総務省　総管情第 85 号　平成 16 年 9 月 14 日
［一部改正］平成 26 年 12 月 26 日 総管管第 101 号
［一部改正］平成 27 年 8 月 25 日 総管管第 71 号
http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/040914_2.html

(20)個人情報の保護に関する法律（平成 15 年法律第 57 号）
平成２８年１月１日施行版　個人情報保護委員会　2016 年 1 月：
http://www.ppc.go.jp/files/pdf/personal_law280101.pdf
(21)個人情報の保護に関する法律（平成 15 年法律第 57 号）
全面施行（公布の日から起算して２年を超えない範囲内において政令で定める日）版
個人情報保護委員会　2016 年 1 月：
http://www.ppc.go.jp/files/pdf/personal_law.pdf
(22)個人情報保護に関する法律・ガイドラインの体系イメージ　個人情報保護委員会：
http://www.ppc.go.jp/files/pdf/personal_framework.pdf
(23)個人情報保護法　法令･ガイドライン等　個人情報保護委員会：
http://www.ppc.go.jp/personal/legal/
(24)「特定個人情報の適正な取扱いに関するガイドライン」　個人情報保護委員会：
http://www.ppc.go.jp/legal/policy/
(25)ガイドライン資料集　Q&A　個人情報保護委員会：
http://www.ppc.go.jp/legal/policy/document/
(26)「 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」
（平成２６年１２月１２日厚生労働省・経済産業省告示第４号）
平成２６年１２月　経済産業省
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf
(27)個人情報保護委員会　特定個人情報の漏えい事案等が発生した場合の対応について
http://www.ppc.go.jp/legal/policy/rouei/
(28)不正競争防止法　経済産業省：
http://www.meti.go.jp/policy/economy/chizai/chiteki/
平成２７年不正競争防止法の改正概要　（営業秘密の保護強化）
経済産業省 知的財産政策室:
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/27kaiseigaiyou.pdf
(28)社会保障・税番号制度＜マイナンバー＞　政府広報オンライン：
http://www.gov-online.go.jp/tokusyu/mynumber/index.html
(29)一般財団法人　安全保障貿易情報センター
http://www.cistec.or.jp/about/sdintro/koumokuIndex.html
（貨物）http://www.cistec.or.jp/publication/hayamihyou/kamotushayami.pdf
（役務）http://www.cistec.or.jp/publication/hayamihyou/ekimuhayami.pdf
(30)経済産業省　安全保障貿易管理
http://www.meti.go.jp/policy/anpo/
(31)経済産業省 貿易経済協力局貿易管理部安全保障貿易管理 外国ユーザーリスト改正
http://www.meti.go.jp/policy/anpo/law_document/tutatu/kaisei/20160122_7.pdf

同　貿易経済協力局

http://www.meti.go.jp/policy/anpo/law_document/tutatu/kaisei/20160122_3.pdf

同　大量破壊兵器等及び通常兵器に係る補完的輸出規制に関する輸出手続等について

http://www.meti.go.jp/policy/anpo/law_document/tutatu/kaisei/20160122_2.pdf

同　マトリクス表

http://www.meti.go.jp/policy/anpo/matrix_intro.html

同　改正情報

http://www.meti.go.jp/policy/anpo/law09.html#501

同　８．コンピュータ、エレクトロニクス、通信関連（別表第1の7の項、8の項、9の項、10の項等）

http://www.meti.go.jp/policy/anpo/qanda08.html

(32)マイクロソフト製品の輸出管理

https://www.microsoft.com/ja-jp/exporting/exportlist.aspx

＜用語説明＞

問い合わせ等の状況から、今後対象語彙を決定する。

「秘密分散技術（一般名称：電子割符）の説明書」―　概要説明書　―

秘密分散法コンソーシアム（SSS-C）

平成 28 年 3 月 1 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

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