お客様各位

弊社秘密分散技術 GFI電子割符® について

2017，11，28版

グローバルフレンドシップ株式会社

代表取締役社長　保倉　豊

注：本資料は弊社の長期継続的な官庁等への確認内容や（現）一般財団法人日本情報経済社会推進協会（英文名称：JIPDEC）が公表した、事実上業界初の秘密分散技術ガイドライン「ECにおける情報セキュリティに関する活動報告2009 http://www.jipdec.or.jp/archives/publications/J0004291 」更に、秘密分散法コンソーシアムが公表している調査確認内容や既公開ガイドラインの技術概要等を根拠として、記載されております。

注：社会動向や技術革新等の事業に影響のある変化によって、予告無く技術内容等は変更される可能性がありますので、最新情報は弊社までお問い合わせください。

目次

GFIは、世界で1999年に世界で最初に電子割符(秘密分散技術)を開発し市場供給を開始した、
当該技術分野のリーディングカンパニーです。

肩の荷を軽くしませんか？

情報セキュリティ。
その責任をとるのですか？
その責任を果たそうとする皆様を応援する技術と商品があります。
GFI電子割符®（わりふ）とその関連商品です。
簡単、便利、経済的です。

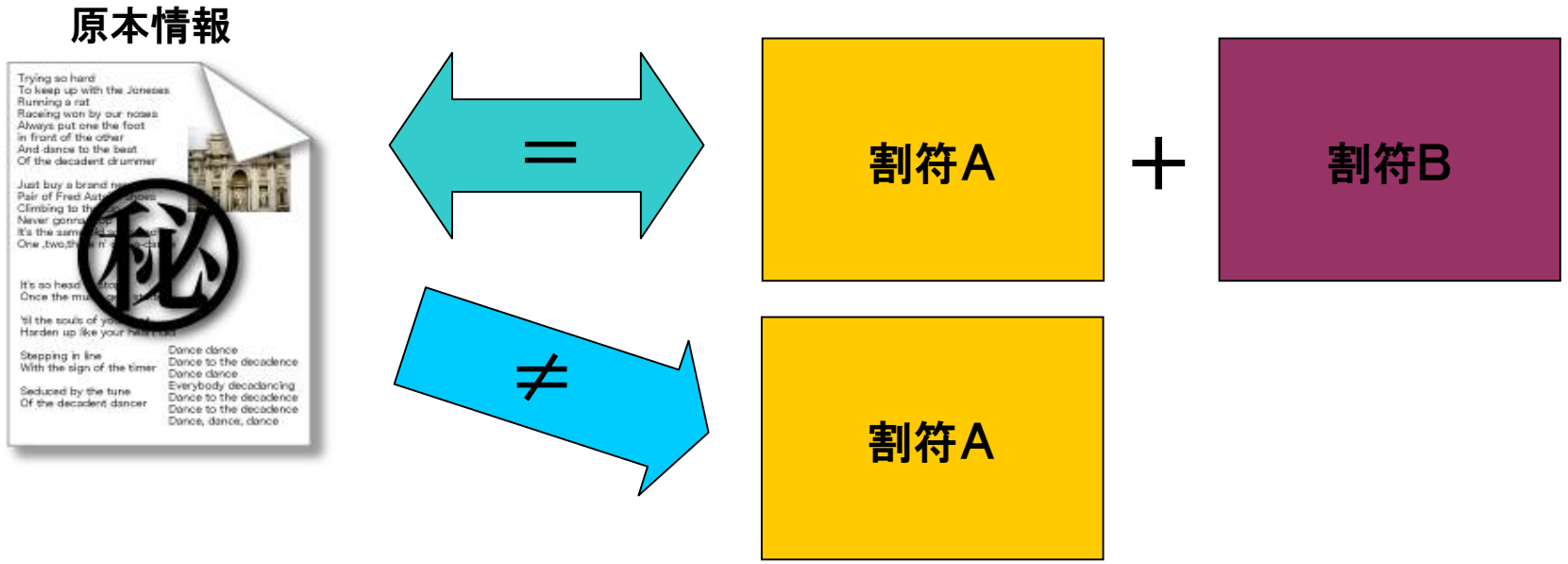
ポイント：
①他の情報と照合できない限り、本人特定できないこと
②ファイル単体からは、何ら原本情報が出てこないこと
③ファイル単体では、法令の定義に該当しないこと
④一般が十分納得できる仕組みであること

会社概要

社名・略称：グローバルフレンドシップ株式会社（Global Friendship Inc.）・GFI
事業内容：電子割符（秘密分散技術）を中心とした情報セキュリティ技術の提供
設　　立：1994年（平成6年）08月28日
資本金・決算：2700万円（2015年07月31日現在）・6月
所　在　地：東京都渋谷区笹塚1-32-2　ソネット笹塚102
代　表　者：代表取締役社長　保倉　豊
技術顧問：東京理科大学　理学部　森田昌宏教授
認　　定：ISMS認証基準認定（ISO27001）・・・事務所移転による再認定準備中
加盟団体：JIPDEC（一般財団法人日本情報経済社会推進協会）、CSAJ一般社団法人（コンピュータソフトウェア協会）、秘密分散法コンソーシアム（発起人・事務局）、他
取得済維持特許：16案件（累計14カ国）累計40件以上取得（即実施予定無いもの放棄）（日本9件、アメリカ3件、中国1件、イスラエル1件、香港2件）上記特許関連開示情報は、http://www.gfi.co.jp/01news20150715_383.html 、http://www.gfi.co.jp/01news20140604_349.html http://www.gfi.co.jp/01news20121030_301.html 、一部共同出願含む、1他
取得済登録商標：　GFI電子割符® 他合計3件
外部評価：4回（東京大学、東京理科大学、私立研究所、産業技術総合研究所（作業中））
公共実証事業等採用例：MEDIS、TAO、経済産業省、総務省、民間（金融系、医療系）
海外記事等：**ISO Management Systems** – July-August 2008　GFI　**世界初割符利用でのISMS取得記事、その他**　http://www.tuv.com/jp/japan/about_us_jp/press_2/news_1/newscontentjp_21163.html

技術標準化に向けた貢献

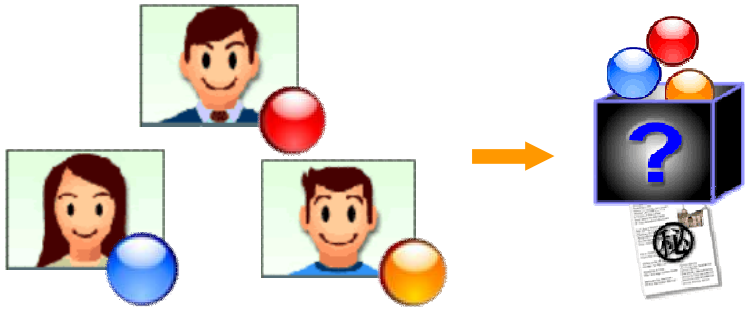
弊社開発の電子割符技術とは、デジタル原本情報を特殊な処理技術を用いてビットレベルで対象情報を分割することにより、割符単体では原本情報に復元する事が出来ない技術です。弊社は一般市民も十分理解できる当該技術に関し、関係省庁等と適宜意見交換等を実施しつつ、技術標準化を推進する秘密分散法コンソーシアムと、本技術の健全な市場普及と技術標準化（JIS化→ISO化等）を推進中。



注：秘密分散技術（電子割符）は、デジタルデータの原理的特性から来る安全性と、各種法令条文等が規定する安全管理措置（義務）の発生する対象情報の法令の定義から除外されている。という二つの意味の安全性を持っています。

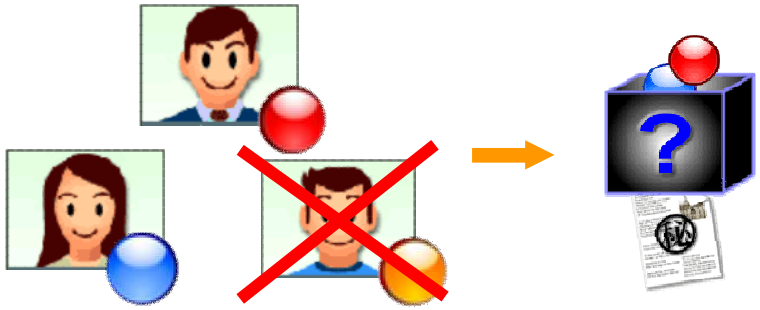
弊社秘密分散技術(電子割符)の基本機能

(1)通常モード(分散管理・完全秘密分散型)



分散した全員の割符が揃ってはじめて、
原本復元を可能にする。

(2)リカバリーモード(分散管理＆BCP対処・しきい値秘密分散型)



一部の割符が揃わなくても、原本復元を、敢えて可能にする。
ただし、それぞれの割符単体から、原本復元はできない。

(3)最小化モード一生成する一つの割符サイズを小さくできます。

(4)自己認証機能一復元する際の条件設定ができます。

弊社秘密分散技術（GFI電子割符®）主要公表可能実績

公表可能な弊社技術（技術区分ーAリファレンス技術）利用・供給実績

公共系

1. MEDIS-DC横浜青葉区医師会電子カルテ地域連携への技術提供
2. 総務省（NICT H13年通信端末内データのセキュリティ確保サービス提供事業）
3. 総務省（H18個人情報保護強化技術実装システムの開発・実証）
4. 経済産業省（平成21年度中小企業等製品性能評価事業）
5. IIJ様（経済産業省平成22 年度産業技術研究開発委託費 ）
6. 国立保健医療科学院（平成24年入札案件）
7. JIPDEC割符事業（J2ETサービス）
8. 日本赤十字社（当時：日本さい帯血バンクネットワーク、現：造血幹細胞移植情報サービス）
9. 沖縄県庁入札案件他、公共機関等の案件等の開示制限事例も有り。

民間系

10. 株式会社アイ・オー・データ機器
11. 株式会社日立製作所、株式会社日立ソリューションズ・クリエイト
12. 凸版印刷株式会社
13. エヌ・アール・アイセキュアテクノロジーズ株式会社
14. 株式会社ソリトンシステムズ
15. 寿精版印刷株式会社
16. ファイブテクノロジー株式会社
17. 三井物産セキュアディレクション株式会社
18. オークシステム株式会社
19. 新日鉄住金ソリューションズ株式会社、他

秘密分散技術（電子割符）は、情報漏洩等の事故後に組織の安全管理措置として利用されることもありますが、最近は未然防止を念頭に積極的に当該技術を適切に利活用して情報資産管理を行うケースが増えており、類似亜種等を誤って採用することや、消費者錯誤による被害を未然防止する意味でも、適切な秘密分散技術が市場に供給されるようにしなければなりません。技術導入検討の際には、秘密分散法コンソーシアム公開の標準化準備資料等を参考として適切な技術選択を実施することに加え、対象となる技術の知的財産の安全性や、技術自体の信頼性や中長期の実績等も合わせてご検討ください。ご不明な場合は、お気軽に弊社までお問合せください。

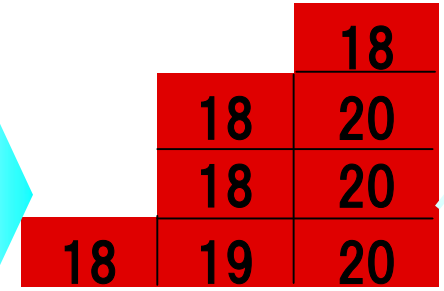
参考事例:弊社の世界初ISMS認証取得モデル

代表的秘密分散技術(GFI電子割符®)で分割・分散

リスク評価のうち、一定ポイント以上の情報資産を割符化して、分割・分散管理。

重要度 / 可能性	1	2	3	4	5
1	1	3	7	13	16
2	2	5	9	16	
3	4	6	11		
4	8	10	14		
5	12	15			

注:現在本店移転に伴い、ISMS認証は効力が切れておりますが、新たな本店所在地でISMSの再取得準備中です。



割符化することで、リスク評価を『最重要機密』から『社内限・一般情報』に軽減。万が一のデータ消滅でも、リカバリーモード(分散管理＆BCP対処)の割符機能で対処。

最重要機密情報が、概念上組織内に存在するが、割符化することで、

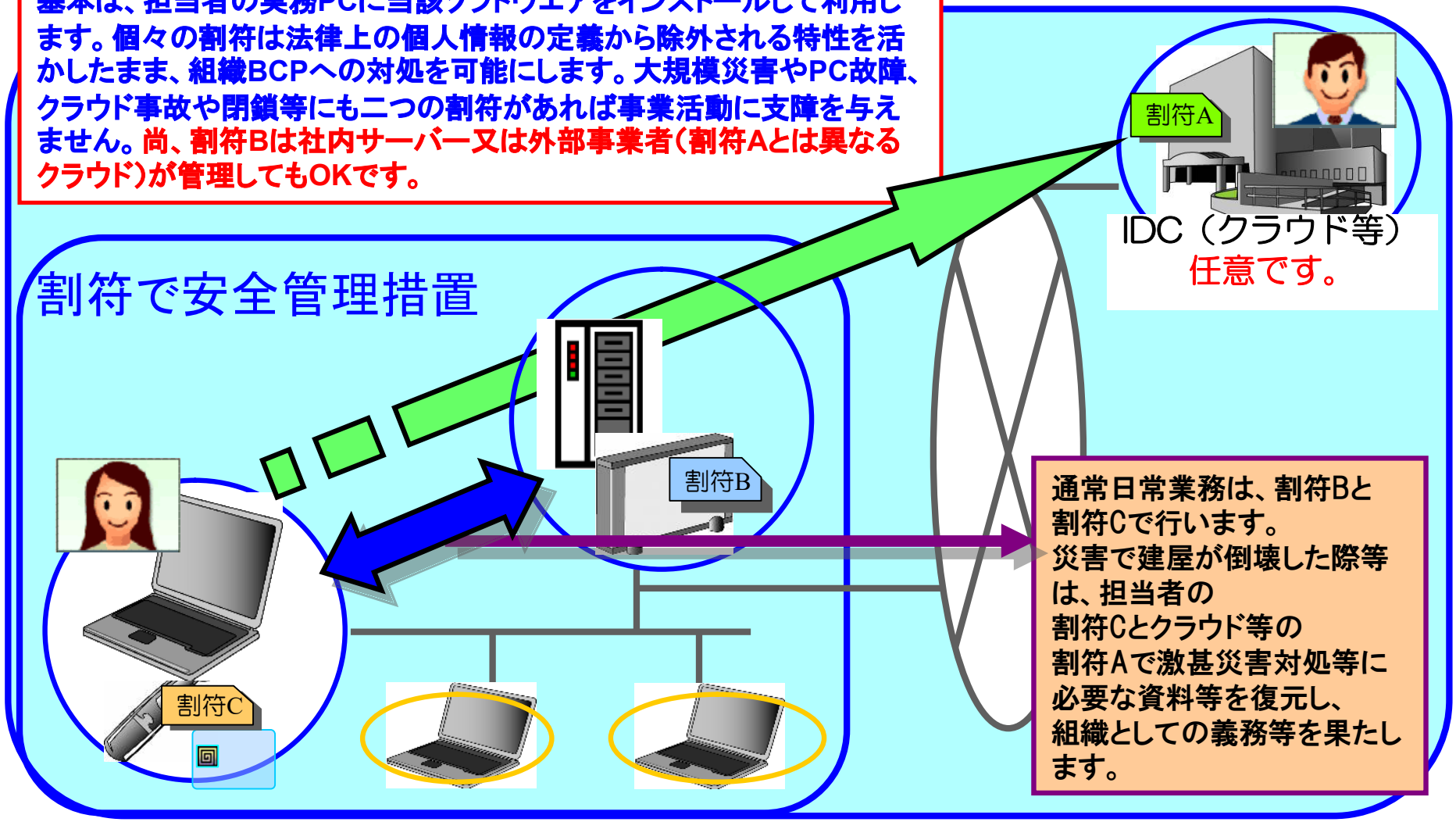
平常時実在しない管理手法が、国際的な認証機関から高い評価を頂き提携認証されました。

本件関連海外ISO関連誌記事:"ISO Management Systems- July-August 2008 Vol.8,No.4"(弊社以外の本文を含めた全体は、約7MBのファイルです)
関連参考:EU個人データ保護認証　秘密分散技術を用いた事例
http://www.tuv.com/jp/japan/about_us_jp/press_2/news_1/newscontentjp_21163.html

組織内情報管理基本形（保管・BCP）

内部情報資産管理概念図

基本は、担当者の実務PCに当該ソフトウエアをインストールして利用します。個々の割符は法律上の個人情報の定義から除外される特性を活かしたまま、組織BCPへの対処を可能にします。大規模災害やPC故障、クラウド事故や閉鎖等にも二つの割符があれば事業活動に支障を与えません。尚、割符Bは社内サーバー又は外部事業者（割符Aとは異なるクラウド）が管理してもOKです。



TUVとの提携

TUVラインランドジャパン様とGFIは、幅広い分野で相互協力していく事を確認し、2005年1月27日に2社提携証書に署名致しました。これは、GFIが自社内部情報を電子割符を活用したシステムで保護し、BS7799とISMSを取得したことに起因します。情報セキュリティ・マネジメントシステムに関連する規格に対し、弊社のBS7799-2（現：ISO27001）認証取得の事例を基にした規格開発協力や、電子割符技術の規格への組入れなどを視野に入れ、当該情報セキュリティー文化の国際普及に相互協力しております。

TÜV

http://www.jpn.tuv.com/

http://www.gfi.co.jp/

（提携認証式　2005/3/2　TUVラインランドジャパン　新横浜office にて）

本件関連海外ISO関連誌記事："ISO Management Systems- July-August 2008 Vol.8,No.4"（弊社以外の本文を含めた全体は、約7MBのファイルです）
関連参考：EU個人データ保護認証　秘密分散技術を用いた事例
http://www.tuv.com/jp/japan/about_us_jp/press_2/news_1/newscontentjp_21163.html

経緯概略

秘密分散技術名称誕生の背景要約

1999年に弊社は世界初の秘密分散技術（電子割符）を日本国内で市場リリース

当時PKIをデファクト化する世界的潮流の中で、いずれ解読等の危機が来る既存暗号技術に対し、当該技術の意義等への理解は容易に進まなかった

学術の世界では、秘密分散法という数学（暗号）理論が存在、しかし、処理速度、データサイズ等の課題に加え、理論実装自体が有限なIT環境では困難なことは周知の事実であった

弊社電子割符技術を、公表予定のガイドラインに記載したいと、内閣官房情報セキュリティセンターより相談が入る。厳格化する法令対処として、既存手法の限界と理論自体は現場に容易に持ち込めないこと等意見交換

更に理論実装した場合の「完全秘匿」は、社会安全保障上の懸念事項となった

この会議の中で、「秘密分散技術」という当該技術の一般名称を提案

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)解説書に、暗号とは異なるセキュリティ手法として秘密分散技術が記載公表

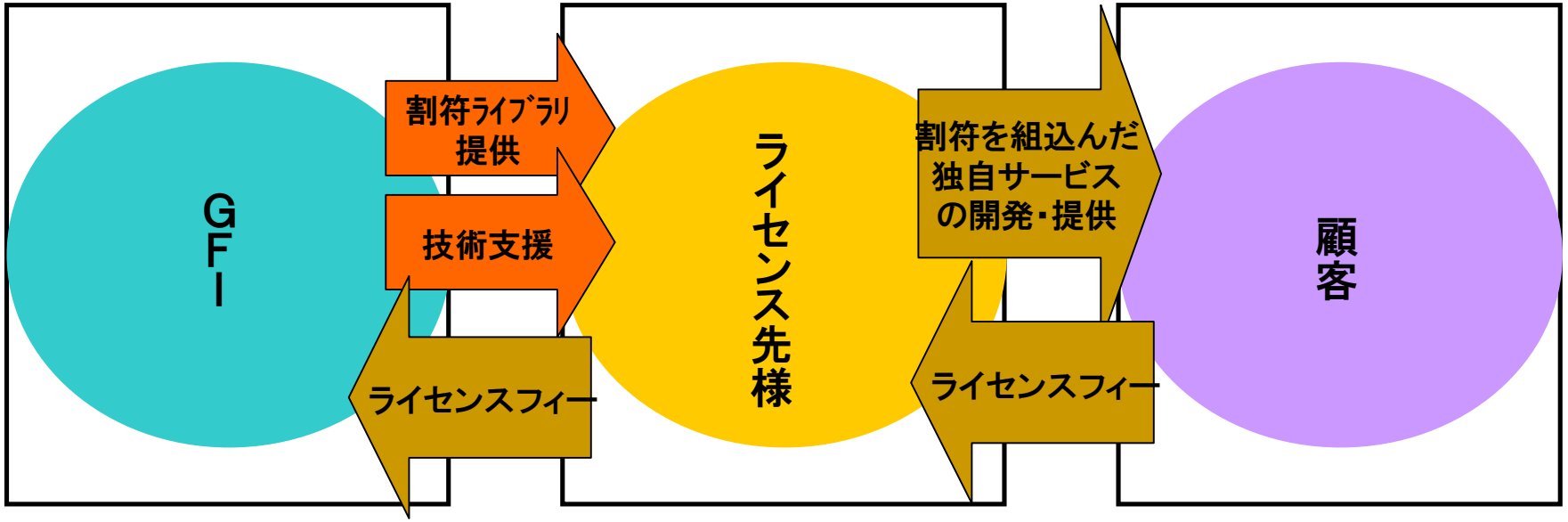
その後も、要機密情報や要安定情報への安全確保の手法として記載される

暗号との相互補完関係を確立しながら、官民の事例を調査しつつ、

秘密分散法コンソーシアムで健全な市場普及と技術標準化を推進中

開発用PRO向けのコア技術ライブラリです。

代表的秘密分散技術　GFI電子割符®　技術供与モデル



注：原理的な秘匿性等が高い為、社会安全保障上の観点も含め、あくまで健全な利用モデルに対してのみ弊社技術はライセンスを行うのが現状方針です。（過去の情報政策官庁様との協議結果）
関連情報開示：http://www.gfi.co.jp/01news20131007_328.html

商品等開発ではなく、**実務等で電子割符を使いたいお客さまは**、ご利用になるシーン等をお知らせいただけましたら、弊社技術ライセンス先各社の商品等のうち適切と思われる商品や問い合わせ先等をご紹介できますので、遠慮なくお申しつけ下さい。

ライブラリライセンスのビジネスモデル等

ビジネス区分(GFI電子割符®は、システム等の開発を行うPRO向けの特殊なソフトウエアです)

①ライブラリ(**GFI電子割符®**)ライセンス

②アドバイス及びコンサルティング(ブレストからビジネス構築、特許ライセンス、特別対応等含む)

ライセンス区分・・・基本国内のみです。

A:試作用(内部用、外部用含む個別見積)

B:実証実験用(公的、民間自主含む個別見積)

C:教育用(個別見積)

D:商用ライセンス(個別見積・・・単品開発用等)

ライセンス料:内訳

1、開発用使用許諾(初期費用)

2、エンド向け使用許諾(1、で開発した商品、サービスを利用するユーザーへの権利付与)

3、保守サポート費用・・・**必須**(個別見積、基本毎年年間費用前払い)

(サポートと追加OS版ライセンスやバージョンアップ時のディスカウント、万が一の損害賠償対策等のメリットがあります。関連情報は、弊社WEBで開示されております。)

GFI瑕疵及び保証範囲等基礎説明図ー http://www.gfi.co.jp/01news20130404/20130403.pdf

ライセンス料解説

1、は、電子割符ライブラリを実装したサービス・商品等を開発する主体に対して、その開発を許諾する内容です。

(ご要望のOS種類をご指定下さい。Win,LINUX,Mac,iOS(各OSでの割符データの互換性確保を実現しています))

・32bit版と64bit版(現在Win版、Linux版、Mac版)、iOSは現状個別対応となっております。

2、エンド向け使用許諾は、各商品やサービスの性質に応じて、協議して個別に設定します。

基本は、御社が本商品やサービスから発生する売上げに対し、事前合意の%を設定します。

これも、初期費用と同様、付帯条件等による価格交渉が可能です。

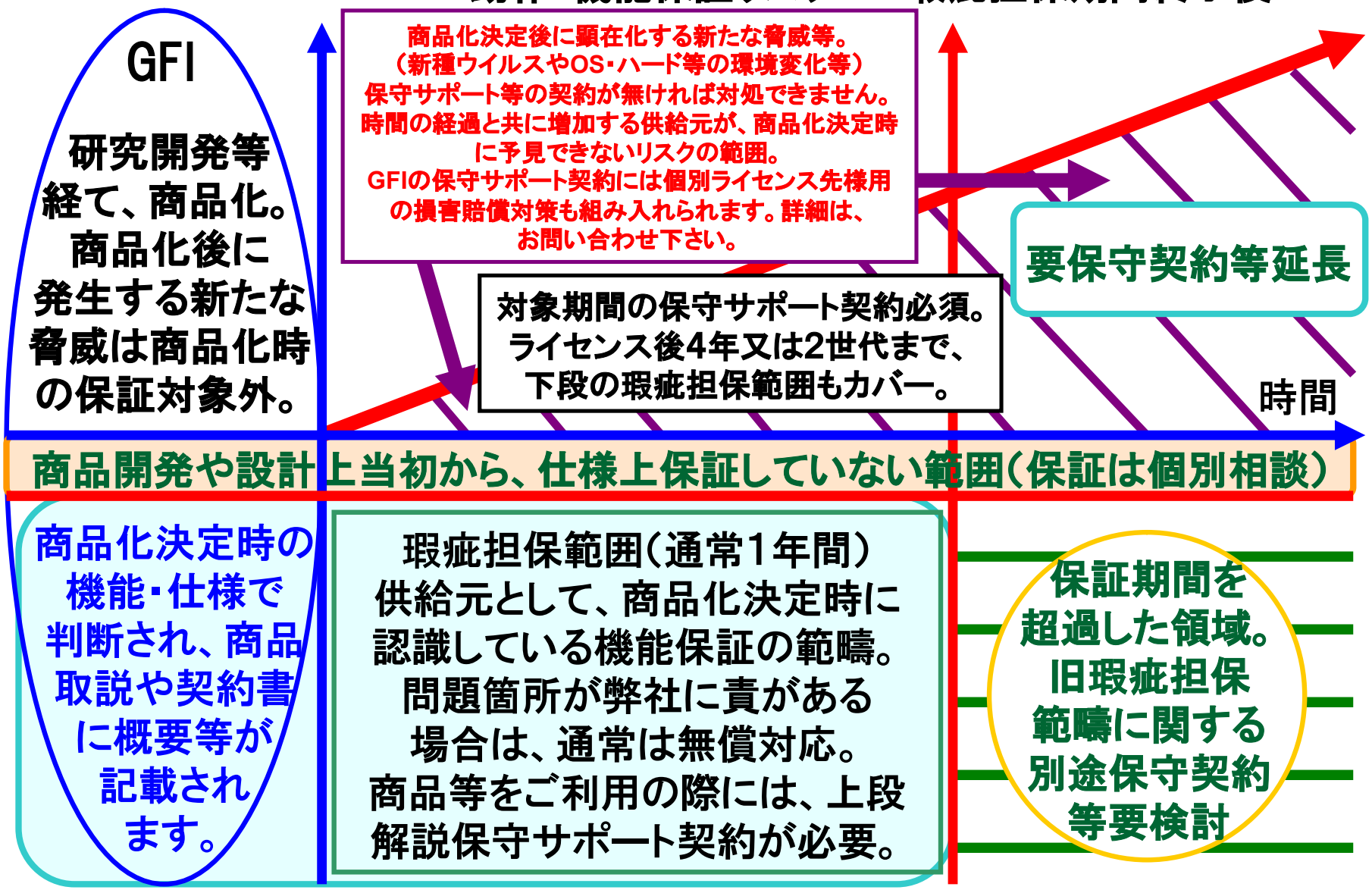
＊特許の使用許諾が個別に必要な場合の特許権使用許諾費用は、別途調整です。

＊＊正式価格や利活用範囲等の解釈等は、必ず弊社まで事前にご相談下さい。

＊＊＊ライセンスは、弊社が情報政策官庁と行ってきた健全な市場普及方針に従う必要があります。

＊＊＊＊個別見積は、許諾先様の組織・事業規模、特別なご要望等を案件個別に勘案し行います。

瑕疵担保等の概要解説図

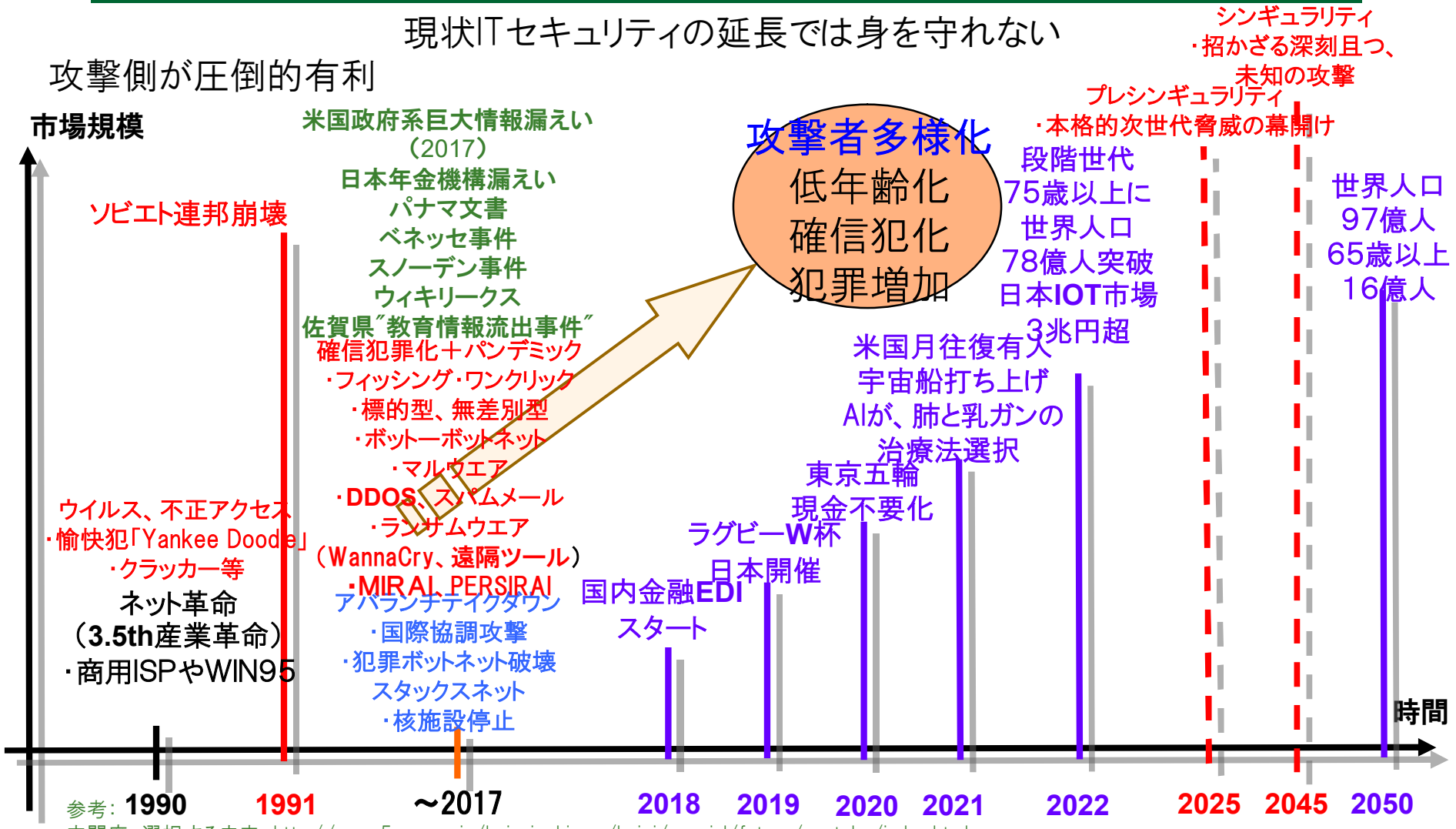


昨今のITを取り巻く社会環境

犯罪組織広域化・複雑化・確信犯化・高度化・巧妙化

現状ITセキュリティの延長では身を守れない

攻撃側が圧倒的有利



参考: 内閣府 選択する未来 http://www5.cao.go.jp/keizai-shimon/kaigi/special/future/sentaku/index.html
野村総合研究所 未来年表 https://www.nri.com/~/media/PDF/jp/opinion/nenpyo/nenpyo_2017.pdf
博報堂生活総合研究所 未来年表 https://seikatsusoken.jp/futuretimeline/ 他独自調査。

電子政府推奨暗号が通用しなくなる

AIやシンギュラリティ等の顕在化により既存情報セキュリティ技術が形骸化する

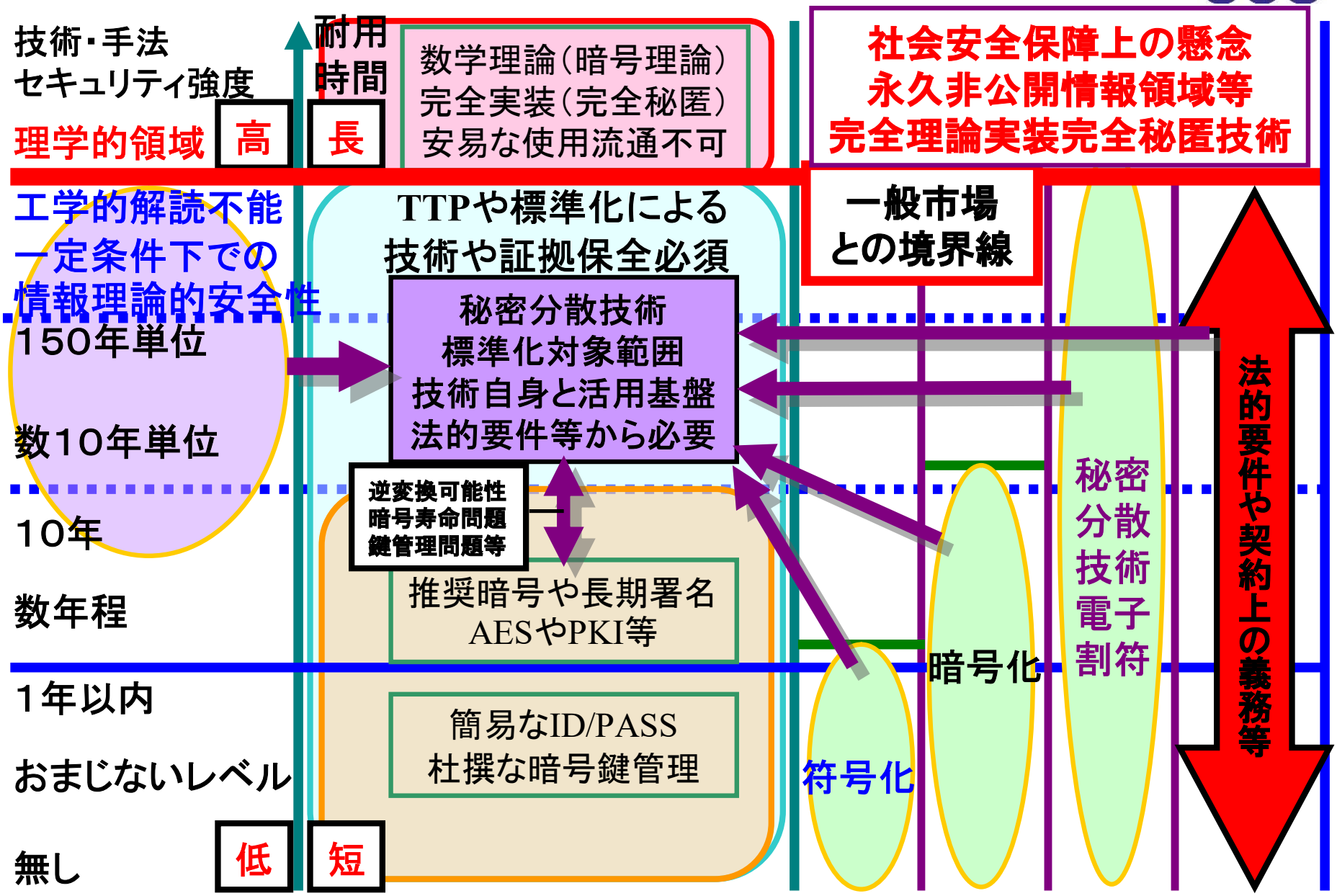
AIやロボット、そしてそうした科学技術の進化により栄華を享受する人類と、その一方で発生する人類が想定しなかった受け入れがたい結果等を、故手塚治虫氏等の未来空想漫画と呼ばれるジャンルで度々描いてきた。内閣府等の公表資料でも多くの場合は、その効能や恩恵がクローズアップされている。参考の内閣府報告書にはそうした環境整備に関し研究が必要と記されている。（すでにRSA暗号は量子暗号で容易に解読されることが証明されている）

下記参考内閣府報告書　P18
利用者が人工知能技術を安心して利用できる環境を整備するために、サイバーセキュリティの強化、データやアルゴリズムの改さん防止など安全性を追求する研究開発が必要である。特に個人情報とプライバシーの保護、それをどこまで利用可能とするかの選択を安全に可能とする技術の開発が求められる。人工知能技術が制御不可能とならない技術（制御可能性）や推論・計算の過程・論理を説明できる技術（透明性）、人と人工知能の制御権の切り替えをスムーズにするインターフェースなどに関する研究が必要である。
（セキュリティ確保、プライバシー保護、制御可能性、透 明性）

参考：
NICT NEWS
https://www.nict.go.jp/publication/NICT-News/1303/02.html
内閣府　人工知能と人間社会に関する懇談会 報告書
http://www8.cao.go.jp/cstp/tyousakai/ai/summary/aisociety_jp.pdf
【全体版】新産業構造ビジョン(PDF形式：23,025KB)PDFファイル
http://www.meti.go.jp/press/2017/05/20170530007/20170530007-2.pdf

AI将棋の例を挙げる必要も無いかもしれないが、暗号解読という限られた範囲に関し、十分な学習材料を与えれば、AIは事も無げに解を導き出す。EU指令をはじめ、個人情報保護法等の目的を踏まえればすでに新たな基礎技術が必要な状態。

時間軸で見る電子割符の社会的役割



特定個人情報における「暗号化」の位置付け

関連するトピカルな情報の一部等：

個人情報保護委員会のQ&A資料より。

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。
（平成27年4月追加）
参考：個人情報保護委員会WEB
http://www.ppc.go.jp/legal/policy/answer/
http://www.ppc.go.jp/legal/policy/answer/#q9-2

番号法の基礎となる個人情報保護法に関しても、ガイドライン（経済産業省公開）でも、
・・・民間向けの法令定義項であるが（行政機関等の場合は、括弧書き中の容易にの記述が無く厳しいものとなっている）
2. 法令解釈指針・事例　2-1. 定義（法第2条関連）　2-1-1.「個人情報」（法第2条第1項関連）法第2条第1項
解説：
「個人情報」※1とは、生存する「個人に関する情報」であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができる※2ものを含む。）をいう。
「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない（ただし、「2-2-3-2.安全管理措置（法第20条関連）」の対策の一つとして、高度な暗号化等による秘匿化を講じることは望ましい。）。

これまで情報セキュリティの主流であった「暗号」は、時代の変化の中で、法令上の要求事項に対し、安全管理措置として不十分な状況になってしまっており、万が一の場合には、過失、注意義務違反等を根拠とした訴訟等のリスクを回避できない。

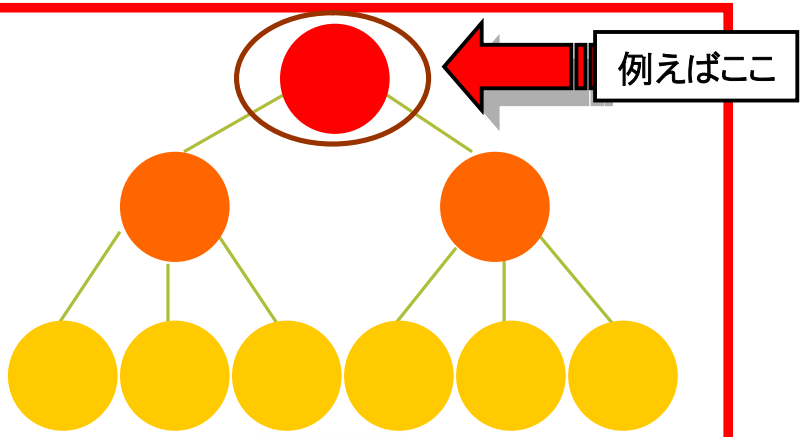
秘密分散技術（電子割符）の概要

要点：

今後の情報資産管理革命の鍵となる技術

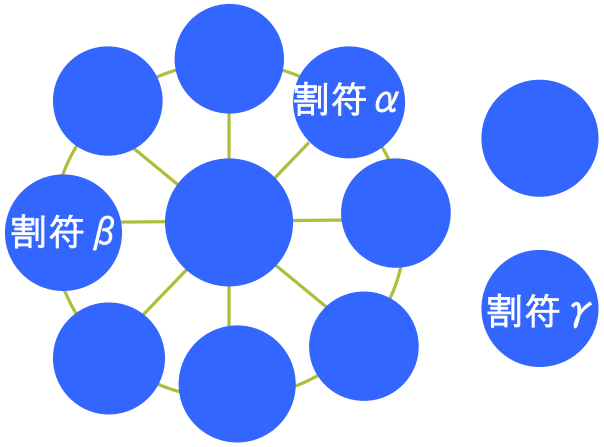
集約型情報管理モデル
―階層構造―

既存社会構造同様
コピー問題、
狭い社会組織・構造に有効
一度の不正での被害が、大きい



分散型情報管理モデル
―水平構造―

インターネットの概念そのもの
広い社会組織・構造にも有効
一度の不正での被害が、限定される
BCP等にも有効、極論どこに置いても良い



PCが不正攻撃で暗号化されてしまった場合も・・・

漏えい等の対象は、実際の情報流出だけではありません。

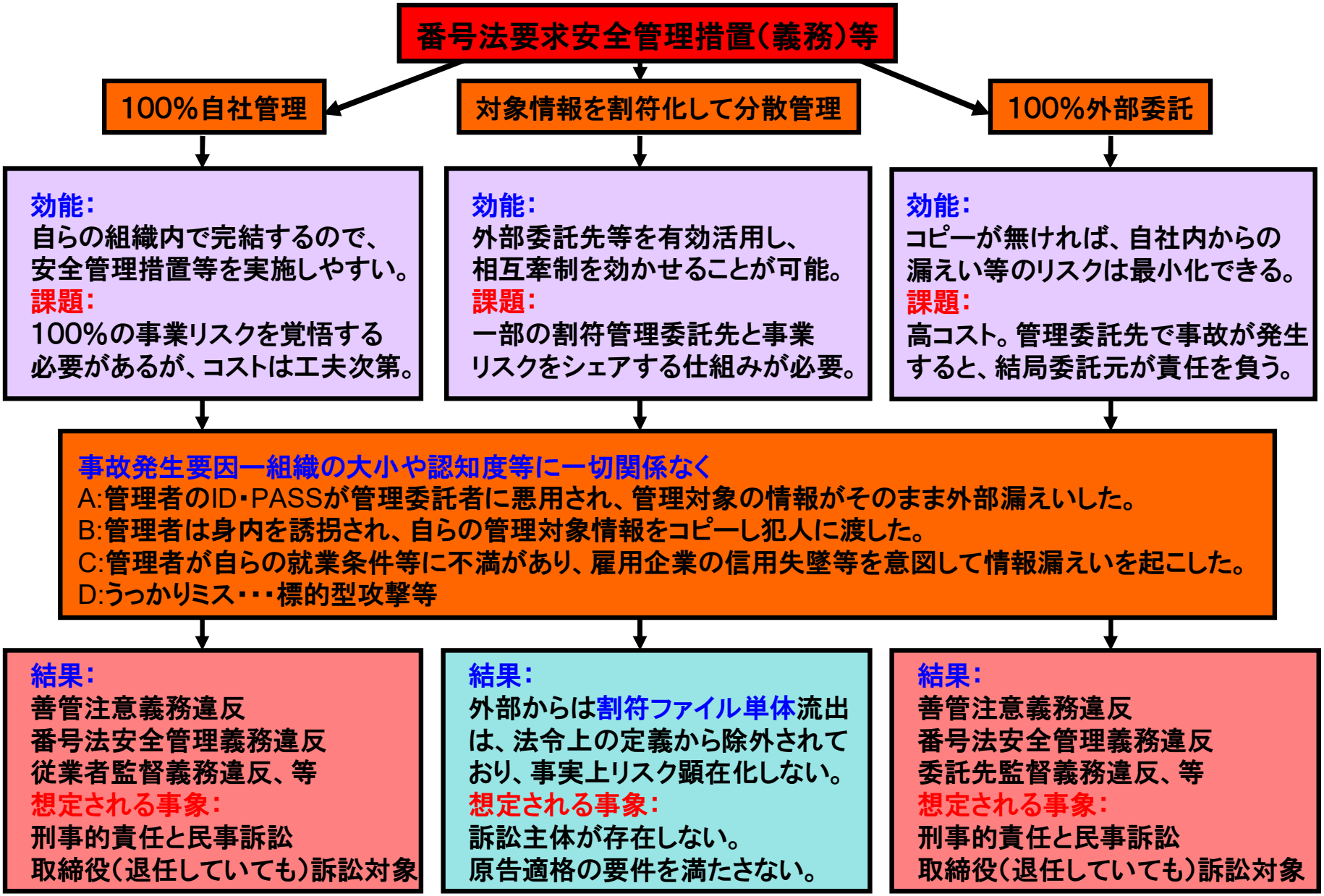
例、個人情報保護法　第20条
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

4 漏えい等の事案が発生した場合等の対応
漏えい等（※）の事案が発生した場合等において、二次被害の防止、類似事案の発生防止等の観点から、個人情報取扱事業者が実施することが望まれる対応については、別に定める。
（※）「漏えい等」とは、漏えい、滅失又は毀損のことをいう（3-3-2（安全管理措置）参照）。

出典：「個人情報保護法ガイドライン（通則編）」 平成28年11月（平成29年3月一部改正） 個人情報保護委員会
https://www.ppc.go.jp/files/pdf/guidelines01.pdf

情報を一部でも消滅させたり、改竄されてしまうことも、滅失又は毀損となり「漏えい等」として安全管理義務違反となります。

参考:対策具体化へのポイント



人事院報道発表と同時期の個人情報保護委員会公開資料

【改正内容】
1　秘密漏えいに係る標準例の追加　秘密漏えいの標準例として掲げている故意の秘密漏えいについて、「自己の不正な利益を図る目的で秘密を漏えいした場合」の標準的な処分量定を明確化する（免職とする）とともに、過失による情報流出の標準例を新設する。
改正する標準例

○　職務上知ることのできた秘密を故意に漏らし、公務の運営に重大な支障を生じさせた職員は、免職又は停職とする。この場合において、自己の不正な利益を図る目的で秘密を漏らした職員は、免職とする。
○　具体的に命令され、又は注意喚起された情報セキュリティ対策を怠ったことにより、職務上の秘密が漏えいし、公務の運営に重大な支障を生じさせた職員は、停職、減給又は戒告とする。

参考出典：人事院　「懲戒処分の指針について」の一部改正について
平成28年9月30日　職員福祉局
http://www.jinji.go.jp/kisya/1609/choukai280930.htm

実際のところ解釈の仕方が幅広く、現場は戦々恐々としている。

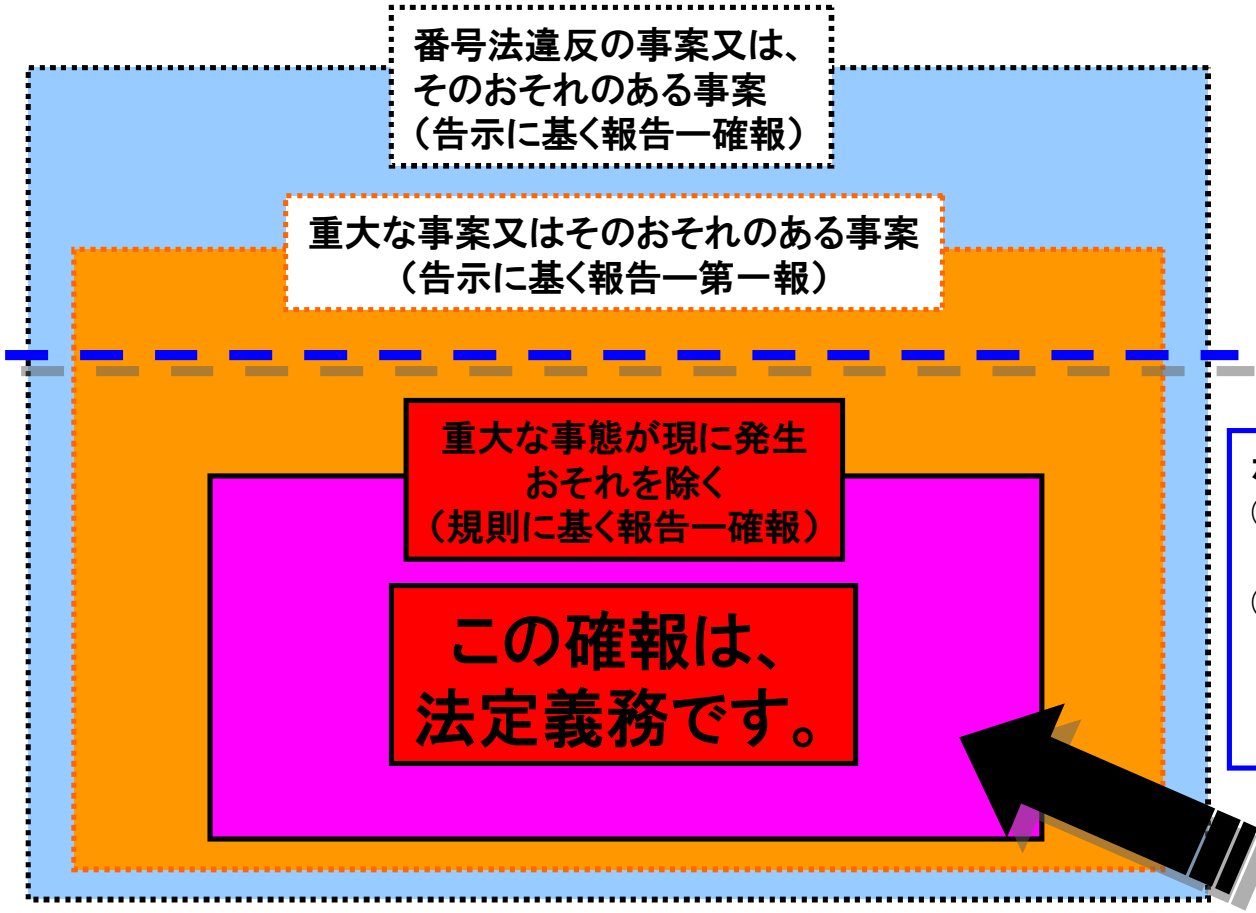
講ずべき安全管理措置の内容
F 技術的安全管理措置
行政機関等及び地方公共団体等は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。
c 不正アクセス等による被害の防止等
≪手法の例示≫
＊ 不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用することが考えられる。

参考出典：個人情報保護委員会　特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）　平成26年12月18日（平成29年5月30日最終改正）
（別添）特定個人情報に関する安全管理措置　（行政機関等・地方公共団体等編）
https://www.ppc.go.jp/files/pdf/my_number_guideline_gyosei-chihou.pdf

ネットワークの遮断自体は、根本的対策ではない。
この「等」や、当該技術は暗号技術ではないが、
高度な暗号化等の「等」に、秘密分散技術（電子割符）の適切な現場利活用が入ると現場導入判断がし易い。

主務大臣や個人情報保護委員会への報告とは、

〇特定個人情報保護委員会規則第五号
行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）第二十八条（注）の四の規定に基づき、特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則を次のように定める。
平成二十七年十二月二十五日　特定個人情報保護委員会委員長 堀部 政男



関係する告示

独立行政法人等及び地方公共団体等における 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
（平成27年特定個人情報保護 委員会告示第1号）

事業者における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
（平成27年特 定個人情報保護委員会告示第2号）

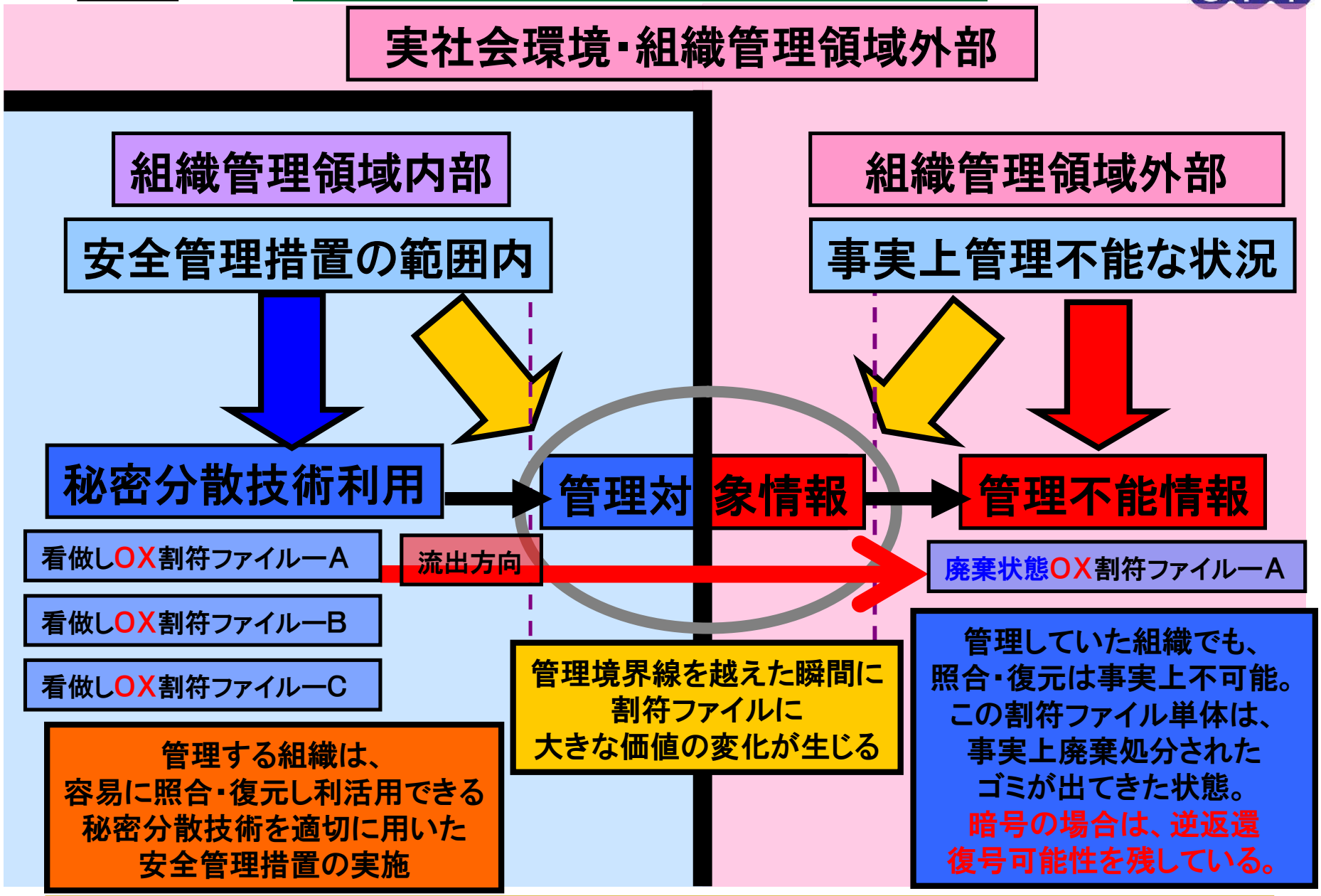
ポイント：
①公的組織は、懸念が生じた段階から、報告が必要
②民間事業者は、重大事態でない場合には、努力義務ですが、
割符でしたので大丈夫です。
と、報告できるように対策しましょう。

万が一の際にも、この報告を出さないで良いような、最善の対策（適切な電子割符の利活用）を実施していることが肝要です。

参考出典：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/

要点：

法令等への有用性既確認概要



官公庁等による弊社秘密分散技術(技術区分ーA)処理に係わる見解等

1、割符ファイル単体は、個人情報保護法の個人情報の定義項から除外される。
(内閣府、NISC、消費者庁、総務省、金融庁、経済産業省等での複数の公的実証事業成果報告や個別確認等より)
注:NISCは統一基準群の解説書で、要機密情報等への秘密分散技術の具体的な利活用法を記載し公表した。

2、上記1、総務省(H18個人情報保護強化技術実装システムの開発・実証)
・実証プロジェクト実施地は福岡県及び県下志免町で良好な成果を収め、総務省へ報告。早期当該成果の市場普及を言い渡される。(実施:福岡県庁と志免町、GFI社)
・「地方公共団体利用共用端末に保存された個人情報保護データの保護ソリューションプロジェクト」

3、上記1・2記載の個人情報と看做せない処理と同様の処理を、著作権の発生する情報等に用いた際、個々の割符ファイルは、原本の著作権者から見て、著作物とは言えない。
(文化庁アドバイスにより、社団法人日本映像ソフト協会、社団法人著作権情報センターへの確認より)

4、会社法、不正競争防止法(営業秘密)、銀行業法、保険業法、証券取引法等における情報管理の法的責任実現にも寄与する。
(JIPDEC ECにおける情報セキュリティに関する活動報告2009 牧野総合法律事務所弁護士法人による法的意見書や経済産業省への一般論としての説明結果より)

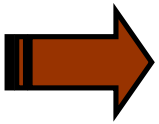
5、情報資産の広域災害対策やBCPに向けた中長期の情報保全への有効性。
(JIPDEC 電子記録応用基盤に関する調査検討報告書2012 付録 秘密分散技術標準化関連市場調査より)

6、マイナンバー法規定の個人番号及び特定個人情報への適用について1、と同様認識。
(当コンソーシアムから特定個人情報保護委員会(現個人情報保護委員会)と内閣府大臣官房番号制度担当室への説明より)

7、秘密分散技術の個人番号該当性(牛島総合法律事務所 弁護士 影島広泰氏 論文)
(15年以上にわたる代表的秘密分散技術(技術区分ーA)の技術実装の場合に関する関係省庁等への確認内容や法令条文を確認し、割符ファイルが全て揃わない限り、マイナンバー法2条8項が定める個人番号に該当しないと考えることができる。との認識が改めて示される(当コンソーシアムへの寄稿)ー当コンソーシアム公開情報(http://www.sss-c.org/?p=553))

秘密分散技術（電子割符）の概要

対象電子情報



01101011011011110110010100110100101101110・・・

既存暗号技術

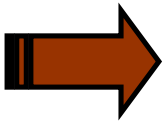
ビットレベルで置換処理を行い暗号化データ生成

11011011111101101010011010010110111000101・・・

一般論として、
短期間・簡便な
利用向き

・暗合化処理では、原本情報を全て反映させた変換データを生成します
・逆変換の可能性を否定できません
・暗合化データは集合論でいうところの写像となります
・暗合化してあっても原本と看做されます

対象電子情報

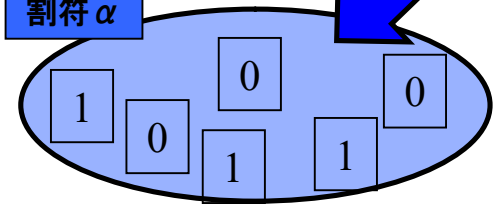


0 1 1 0 10110110111101100101001101001011011 10・・・

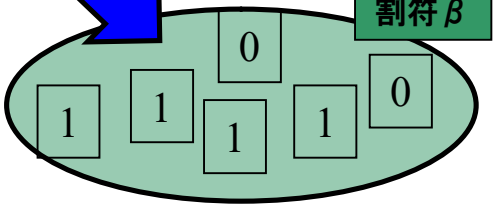
ビットレベルで分割・分散処理を行い割符ファイル生成

秘密分散技術
（電子割符）

割符α



割符β



一般論として、
中長期間・厳格な
利用向き

・割符化処理では、原本情報をビットレベルで分割・分散して割符を生成します
・割符単体からの逆変換が原理的にできません
・割符ファイル単体は、集合論でいうところの部分集合となります
・割符ファイル単体は、法令解釈上も原本とは看做されません

弊社秘密分散技術（技術区分ーA）の外部評価の概要（公共実証実験報告等は除く）

東京大学

電子割符セキュリティ強度調査報告書　2001年12月20日
電子割符は、秘密情報を分割して安全に伝送（または記録）する目的に開発された符号化法（およびそれを実現するためのソフトウエア）である。秘密情報である平文Sをn個の割符に分割符号化し、n個の割符が全部そろえば、平文Sが複合できるが、n-1個以下の割符からは平文Sの情報が漏れないように工夫されている。（注：通常非公開資料）

産業技術総合研究所（参考）

GFI電子割符（R）の安全性評価について　縫田光司　2015年11月03日
通常の暗号技術の標準的安全性レベルである「80bit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。（中略）現時点での安全性評価で得られ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

参考：「産総研様との共同研究の第二期結果概要報告」、[2015.12.26]
http://www.gfi.co.jp/01news20151226_393.html

経済産業省認識概要

安全管理措置の違いによる、実際に漏えいが発生した際の組織外からの見え方の図。
（平成27年02月20日経済産業省確認ー注：割符でも、何か管理ファイルが出たという事実までは消せないが）

管理手法 / 外部の評価	平文	暗号化	割符化
完全違反	○		
漏洩に該当		○	
該当せず			○

・組織等が個人情報を管理するにあたり、何ら技術的安全管理措置を施さず漏洩をした場合（問答無用違反）

・組織等が個人情報を管理するにあたり、高度な暗合化を施していたが漏洩をした場合
・利用している暗号がそもそも危殆化していないことと、鍵管理が完璧で攻撃者に取得されていないこと
・暗号システム自体や鍵管理が、単純なパスワード管理ではないこと
・暗号化したファイルが外部に出ると、個人情報漏洩に該当

・組織等が個人情報を管理するにあたり、秘密分散技術（電子割符）を用いていたが、そのうちの1つの割符ファイルが漏洩した場合（復元に至らない数）
・復元に利用する残りの割符管理が適切であること
・組織の持つ復元用プログラムと復元に必要な他の割符ファイルが無いと復元できない
・個人情報定義項除外ファイルの漏洩でしかなく、個人情報漏洩に該当しない

要点：

機密情報漏洩への最善のリスク回避策

非個人情報としての電子割符の評価

電子割符の場合は、情報を非線形に分割し、オリジナルデータ自体を分離、分割してしまうことから、分割後の割符それぞれには全情報が含まれておらず、単体としては不完全な情報となる。この結果、電子割符は個人を識別する情報を持たないことになり、暗号化された情報とは異なる評価が与えられることになる。個人情報保護法上の「個人情報」であるためには、当該情報から個人が識別され、あるいは暗号などであっても、ある種の措置により復元可能である場合にはなお個人情報となるとされるが、この要件から電子割符を評価すれば、単体としての電子割符の情報は、（他の割符と容易に照合ないし結合できる状態でない限り）個人情報とはいえない情報であるということができる。

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れる。

参考：「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.
TF1法的意見書　牧野総合法律事務所　弁護士　牧野二郎
http://www.jipdec.or.jp/archives/publications/J0004291

参考:「秘密分散技術と個人番号該当性」

秘密分散技術により生成される割符ファイルの性質

秘密分散技術とは、デジタルの原本情報をビットレベルで分割することにより、「割符ファイル」と呼ばれる複数のファイルとする技術をいう。これが理想的に実装された場合、割符ファイル単体では原本情報に復元する事が原理的にできないとされている（2016年11月7日付け「標準化推進中の秘密分散技術（電子割符）について」（秘密分散法コンソーシアム）参照）。

秘密分散技術により生成される割符ファイルの個人番号該当性

秘密分散技術によって作成された割符ファイルは、単体では原本情報に復元することが原理的にできない。（中略）また、以上は、割符ファイルになった原本情報に、個人番号だけではなく別の情報も含まれていたとしても同様に考えることができる。（中略）個人番号を含むデータを秘密分散技術により割符ファイルとした場合、当該割符ファイルが全て揃わない限り、マイナンバー法2条8項が定める個人番号に該当しないと考えることができる。

復元に至らない数の割符ファイルの流出の場合

復元に至らない数の割符ファイルの流出は、重大事態には当たらないものと思料いたします。

参考:2017年2月18日 「秘密分散技術と個人番号該当性」 牛島総合法律事務所　弁護士　影島広泰
秘密分散法コンソーシアム　http://www.sss-c.org/?p=553

参考：秘密分散技術の記述の入ったNISC資料の記述部

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

3.2.4 情報の移送

趣旨(必要性)
行政事務においては、その事務の遂行のために他者又は自身に情報を移送する場合がある。移送の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部記録媒体の運搬及びPC、紙面に記載された情報の運搬等の方法が挙げられるが、いずれの方法を用いるにせよ、情報の移送により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになる。
これらのことを勘案し、本項では、情報の移送に関する対策基準を定める。
遵守事項
(5) 電磁的記録の保護対策
【強化遵守事項】
(c) 行政事務従事者は、要機密情報である電磁的記録を移送する場合には、必要な強度の暗号化に加えて、複数の情報に分割してそれぞれ異なる移送経路を用いること。

解説：情報を分割し、これを異なる経路で移送することを求める事項である。
要機密情報を移送する場合には、当該要機密情報が情報量的に解読不能となるように、分割して移送を行うこと。この考え方は、専門用語で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CD-ROM 等の媒体で郵送する方法が挙げられる。

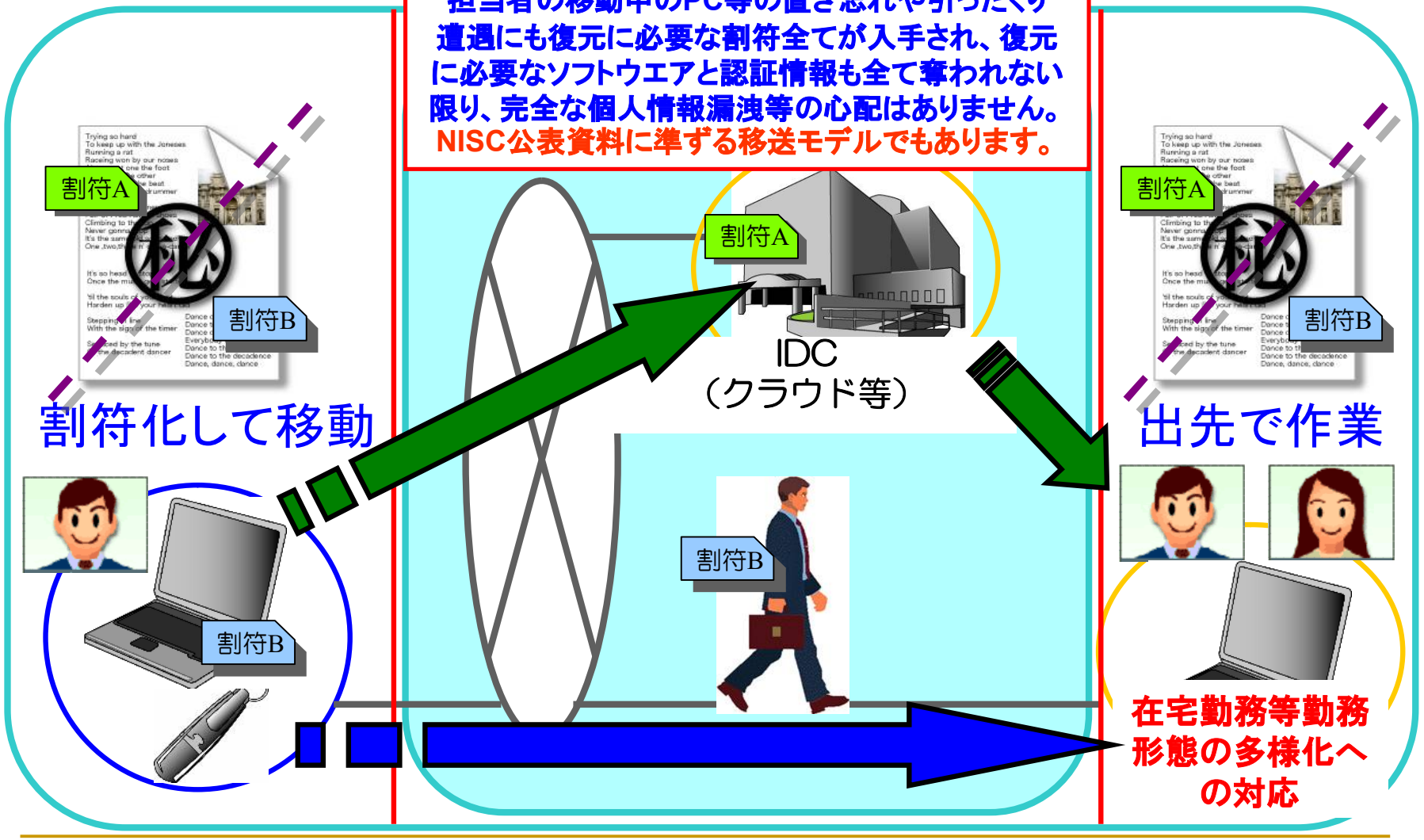
参考：預金保険機構　立ち入り検査後
https://www.dic.go.jp/shiryo/nenpo/h21/gaikyo1-2.html
平成21年11月に検査部内において、検査用書類作成のために用意した金融機関の個人情報が記録された電子媒体が、所在不明になっている事実が判明しました。このため、機構では、再発防止策として、新たに管理要領を制定し、紛失防止に実効性のある管理簿等による電子媒体の管理に加え、搬送時に割符処理を行い、セキュリティの強化を図るなど、再発防止に全力で取り組んでいくこととしております。
②立入検査後のフォローアップ
機構が実施した検査の指摘事項については、金融庁又は財務局等が金融機関に対し銀行法第24条等及び預保法第136条に基づき改善状況の報告を求め、ヒアリングを実施していますが、機構としてもこれに同席して、実効性のある改善が可能となるよう助言等を行っています。

データ移送・持ち出し用

商品利用出先シーン

想定状況：Wi-FI併用

この間、個々の割符は法律上の個人情報の定義から除外されます。通信経路やIDCからの漏洩、担当者の移動中のPC等の置き忘れや引ったくり遭遇にも復元に必要な割符全てが入手され、復元に必要なソフトウエアと認証情報も全て奪われない限り、完全な個人情報漏洩等の心配はありません。
NISC公表資料に準ずる移送モデルでもあります。



参考：秘密分散技術の記述の入ったNISC資料の記述部－2

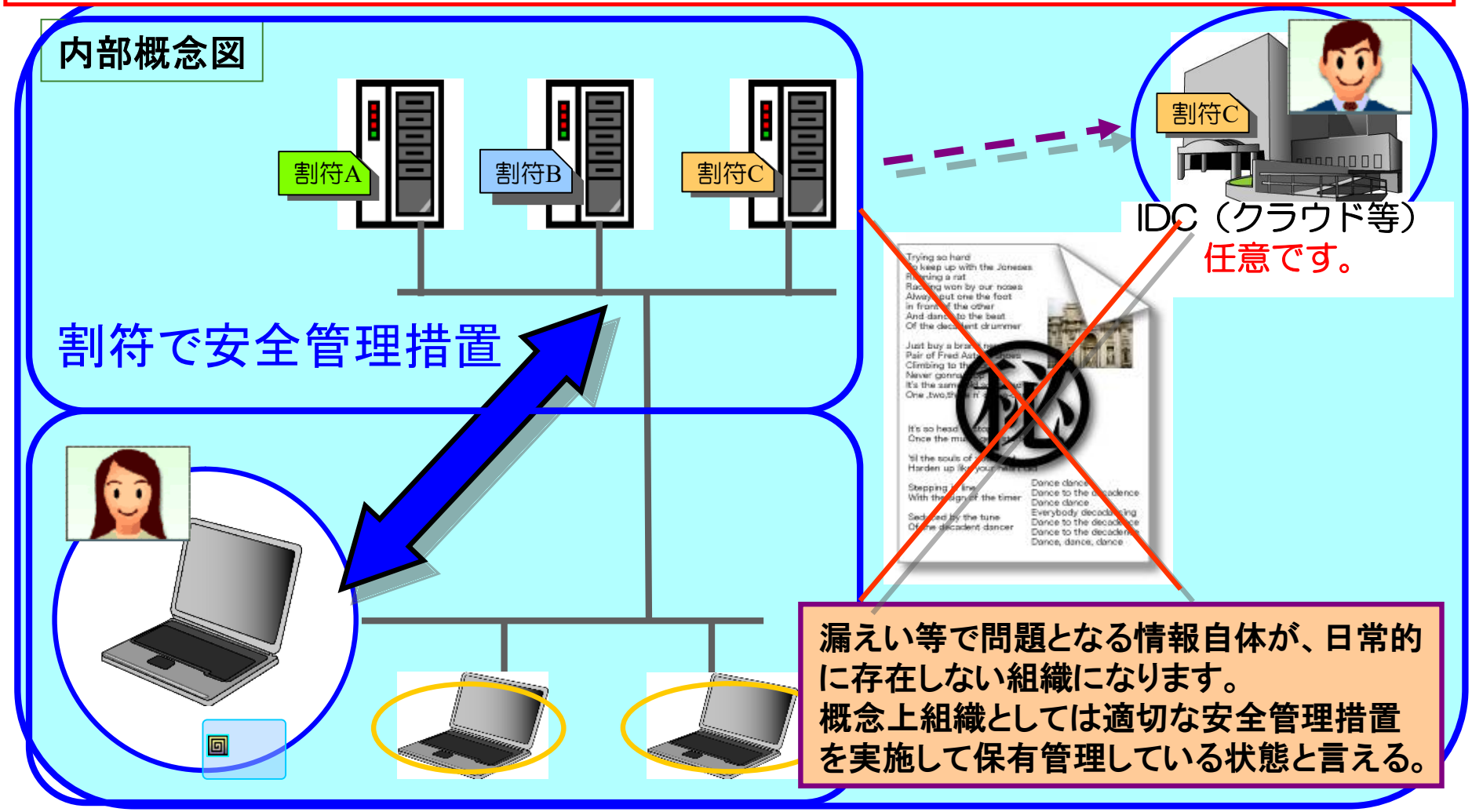
NISD-K305-111C
政府機関の情報セキュリティ対策のための統一技術基準（平成 24 年度版） 解説書
内閣官房情報セキュリティセンター
http://www.nisc.go.jp/active/general/pdf/K305-111C.pdf

2.3.2.3 サーバ装置
趣旨（必要性）
サーバ装置については、当該サーバ装置の電磁的記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入等を受けるリスクが高い。政府機関が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。このようにサーバ装置の利用は、その特性により、電子計算機に共通的なリスク以外にも情報セキュリティが損なわれるおそれを有している。これらのことを勘案し、本項では、サーバ装置に関する対策基準として、サーバ装置の設置時及び運用時についての遵守事項を定める。
遵守事項
(2) サーバ装置の運用時
(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。

地方行政取り組み組織内情報管理基本形

既存庁内システムを大きく変更せずに、サーバーのデータを割符化して管理するモデルです。個々の割符単体が外部流出したとしても、法令上の個人情報の定義から除外される特性を活かしたまま、高度な安全管理措置の実現を可能にします。サーバー故障にも、二つの割符があれば事業活動に支障を与えませんし、ファイルサーバーの移行も容易です。不正アクセスやランサムウエアへの対策としても有効です。



参考：秘密分散技術の記述の入ったNISC資料の記述部ー3

前述のNISC公表資料記載内容は、2005年以降も継続的に記載され続けており、H26年の、
「府省庁対策基準策定のためのガイドライン」
秘密分散技術の記載部分に対し、本来の記述よりも時間経過の中で簡略化等された記載となっておりました。端的に言うと、データ運用手法と独立した基礎技術に対する記述の仕方に混同がみられる状態でした。
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　内閣官房情報セキュリティセンター
http://www.nisc.go.jp/active/general/pdf/guide26.pdf

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。

NISCの組織改編実施後に公開された、H28年の、
「府省庁対策基準策定のためのガイドライン」
では、H26年版の技術と手法に関する記載の混同等もあったと考えられますが「秘密分散技術」記載部分が異なる表記となり、当初の記述に近いものとなりました。
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。

上記修正に関し、秘密分散法コンソーシアムとして、
～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～
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。更に、H28年度版ガイドライン公開後にも、中央府省庁からも電磁的記録の移送に関し、秘密分散技術を利活用したい。というご相談も来ております。

今後等:

法令等への有用性既確認概要

1、法令上の定義項に該当しない
2、訴訟(原告適格)にならない
3、重大事態としての報告に至らない
4、一般人でも安全性を理解できる技術

実害発生させずに、法的課題クリア。
この従来のセキュリティにはない、
現実解としての秘密分散技術の特性を
社会に健全に周知啓発していく

注:復元に至らない数の割符ファイルであることが前提の概要です。

参考:秘密分散法コンソーシアム(SSS-C) 概要

我々秘密分散法コンソーシアム(http://www.sss-c.org/)は、秘密分散法の広範な社会的有効活用と、同理論や集合論等を背景の一つとする、純国産の電子情報処理技術である秘密分散技術(電子割符)の健全な市場普及と標準化を、主たる目的としております。当該技術等の技術標準化を当初から活動の根底に据え、2002年10月10日の創設以来、当該技術等の日本発の世界標準化を目指し活動しております。これまで、IT業界各社、利用側組織、法曹界、学術(数学)界、公的団体、更に経済産業省や内閣官房にも発足時ご出席賜わっている、完全ボランタリーの任意団体です。
これまで継続的に法令の定義項から除外されると確認できている代表的な技術実装の他にも、今後市場に広まる可能性のある技術実装モデルも登録できるよう、複数の技術区分を検討中です。
この方針は、我々コンソーシアム発足時(2002年当時)から不変的な基本方針で、発足直後から当該技術関係の商品化や研究等を行っている複数の企業等も含め活動が始まりました。

秘密分散技術標準化の意義
工業標準化の意義は、具体的には、自由に放置すれば、多様化、複雑化、無秩序化してしまう「もの」や「事柄」について、経済・社会活動の利便性の確保(互換性の確保等)、生産の効率化(品種削減を通じての量産化等)、公正性を確保(消費者の利益の確保、取引の単純化等)、技術進歩の促進(新しい知識の創造や新技術の開発・普及の支援等)、安全や健康の保持、環境の保全等のそれぞれの観点から、技術文書として国レベルの「規格」を制定し、これを全国的に「統一」又は「単純化」することであると言えます。
出典:http://www.jisc.go.jp/std/index.html(日本工業標準調査会のHPより抜粋)

消費者保護の観点からも正しい標準化を行い、適正な市場創出を促進し、適切な競争が発生するようにしていくことと、日本発世界標準化を実現し、日本が当該分野で世界をリードしていくことが肝要。

会長　細野昭雄(株式会社アイ・オー・データ機器)
オブザーバー　坂下哲也(一般財団法人 日本情報経済社会推進協会)
幹事
永宮直史(特定非営利活動法人 日本セキュリティ監査協会)
佐藤尚秀(寿精版印刷株式会社)
保倉　豊(グローバルフレンドシップ株式会社)―本活動事務局担当

健全な利用事例からの技術標準化

代表的秘密分散技術処理概念図(弊社モデル)

原本情報

秘密分散技術
(電子割符)
技術区分ー A

内部では

1
割符A
0

0
1
割符B

前段処理
ゴミを加え攪拌
乳化処理実施

中間ファイル
乳化後
ファイル

分散処理
ビットレベル
分割・振り分け(分散)

＋

010011
110010
111100
010100
00・・・・・
(ゴミです)

111010
010001
101110
110110
01・・・・・

1
0
0
1
0
1
0
1・・・

注: 法令の定義項から除外される技術処理の基本形である秘密分散技術(技術区分ー A)の概念図。
2つの割符ファイルを生成した処理概念図です。

「暗号＋ファイル分割」方式の違い

原本情報

暗号化
（符号化含めた変換手法）
＋
ファイル分割（ビット抽出等）
技術区分ーB

内部では

暗号化処理

暗号鍵

暗号化
ファイル

分割

長期の暗号鍵管理や将来の危殆化
対処実務が発生
（単純な符号化は論外）

暗号化ファイル
分割片A

暗号化ファイル
分割片B

暗号化してあっても個人情報、特定個人情報となりますので、それをファイル分割しても。外部流出すると法令上、暗号同様、特定個人情報漏洩となります。秘密分散法コンソーシアムによる個人情報保護委員会確認。
（2016年03月29日、04月05日）

注：原本情報を暗号化＋ファイル分割の概念図で、コンソーシアムでは秘密分散技術の一種としていますが、法令上の定義から除外される技術区分ーAとは大きく異なり、法令の定義の範疇のままと見做されます。

参考:標準化に向けた技術登録区分

一般消費者等では、見分け困難な類似技術等が市場に出始めており、コンソーシアムと経済産業省との意見交換（貿易経済協力局での輸出入の相談の中で）で、法令上の有用性に関して、類似亜種等による消費者錯誤による被害発生を未然防止する観点からの助言があり、秘密分散法コンソーシアムでは、これまでの関係省庁等への相談等の中で、法令上も有用な技術処理が適切に実装された秘密分散技術（電子割符）と、今後出現可能性のある技術区分も想定した技術登録制度を本年運用開始予定。

技術区分―A　概要（継続的且つ安定的に法的有効性確認等の対象技術で標準化推進してきた処理モデル）

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・データサイズ最適化）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、個々の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は原理的にも原本復元を行うことはできない。更に、対象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、不正競争防止法等）の法令の定義項から除外される特性を持つ。

技術区分―B　概要（新設―現時点法的有効性評価はない）

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、ファイル分割又は変換データから一部ビットを抽出する技術で、暗号化（符号化）の質が生命線。単なる符号化（暗号化）＋ファイル分割（又は一部抽出（以下同様））にとどまら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やビット抽出後の残りの暗号化ファイル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が、法令解釈上は、残存する暗号化ファイル分割部分が個人特定等が十分可能な量あることに加え解読可能性が否定できないこともあり、符号化・暗号化の範疇となる。また原理的に利用した符号化や暗号化の強度や鍵等管理への依存度が高い（注1）。暗号化ソリューションを導入して場合には、暗号化を行った後にファイル分割ソフトで分割しても同様の仕組みを構築できる為、独立した基礎技術とするには単体で＋αの工夫等が必要である。

技術区分―C　概要（新設―現時点法的有効性評価はなく、各研究成果等の評価が待たれる）

数学や暗号の学術理論を実装したと主張する技術。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、同時に社会安全保障や法令の規制等を受けることとなる。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。秘密計算を組み合わせることも、現時点この区分に入る。実際にはベースとなる基礎技術の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）と考えられる。

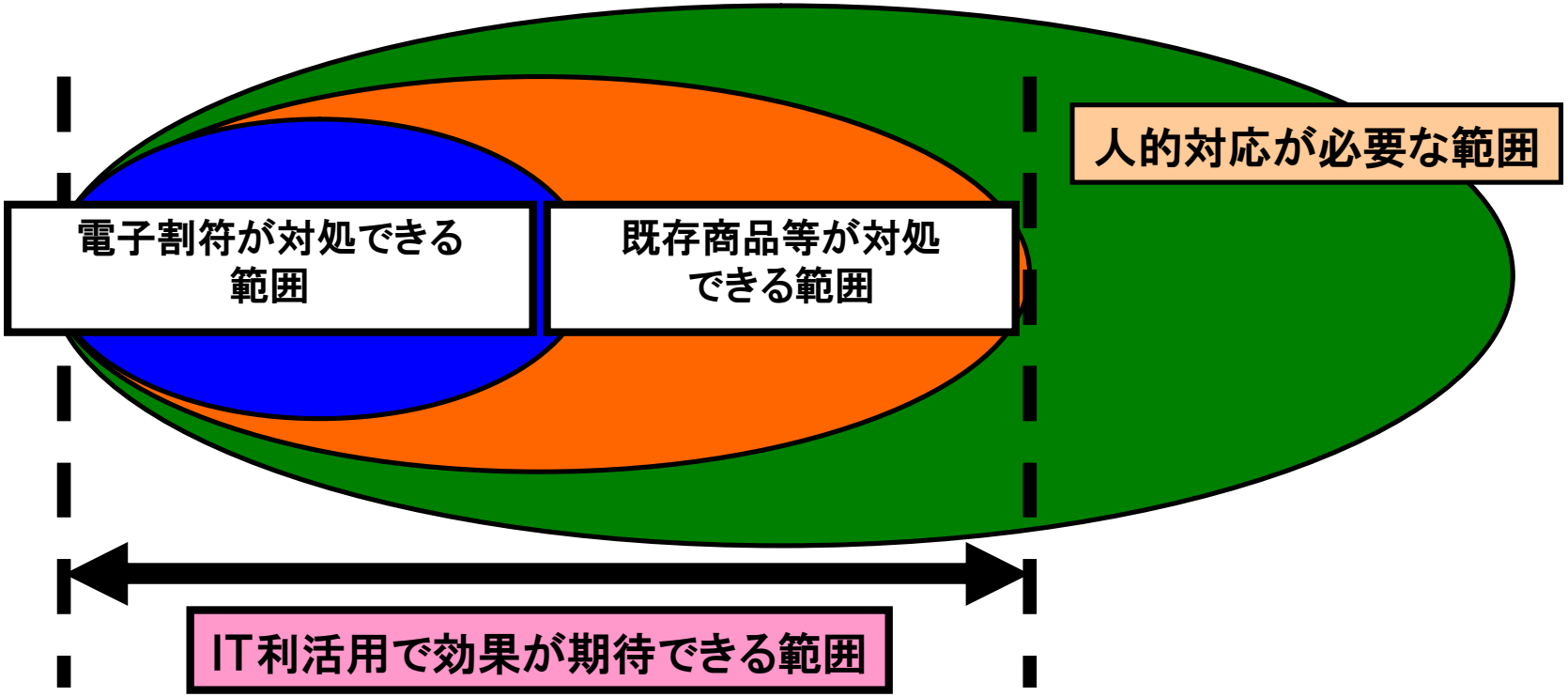
注1：原本電子情報をファイル分割した後に、それぞれの分割片に暗号化を施すといった仕組みは、単純に暗号化（符号化含む）と解釈できるため、当コンソーシアムの秘密分散技術（電子割符）標準化対象のスコープには入らない。

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通底する。関連記載―「府省庁対策基準策定のためのガイドライン」（参照：nisc公表主要資料）

参考：当コンソーシアム既公開資料　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 -　http://www.sss-c.org/?p=447）

残存リスク最小化に向けての課題

求められている安全管理全体の概念



既存商品等：
- IT環境全般に対するセキュリティ商品が存在
- 対処想定レベルはバラバラ
- 商品目利きと組み合わせが必要ー相性も考慮

割符商品等：
- 深刻度の大きな情報管理ほど、貢献度は高まる
- 割符だけでは対処できない残存リスクがある

既存パッケージ側：
- 業務効率向上
- 最低限の安全性確保
- 守備範囲の明確化

割符パッケージ側：
- 高度な安全管理措置の実現
- 外部説明可能な厳格な情報管理対応
- セキュリティの最後の砦ー被害最小化

弊社秘密分散技術処理に係わる内閣府見解

秘密分散法コンソーシアムが特定個人情報保護委員会様経由で内閣官房社会保障改革担当室の中の内閣府大臣官房番号制度担当室様に、公表する文章としてお聞きした結果（平成27年01月23日時点）の文章抜粋を記す。

特定個人情報保護委員会様より内閣官房社会保障改革担当室の中の内閣府大臣官房番号制度担当室様にも我々秘密分散法コンソーシアムが作成した認識内容の文章をお伝えいただき、2015年01月23日に、我々コンソーシアムに対し、その記載内容に関し、特定個人情報保護委員会様経由で、一般論として特段問題無い。との回答を頂戴しました。
（特定個人情報保護委員会様や内閣府大臣官房番号制度担当室様が、当該技術を特別な扱いとして推奨しているという意味ではなく、更に、適切な技術利活用と割符ファイルの運用管理が行われていない場合には、問題が生じる場合もありますので、秘密分散技術（電子割符）で処理しただけで何も問題が発生しないということを確認いただいたという意味ではありませんので、ご注意ください（後述の注3にも関連））我々秘密分散法コンソーシアムとしては、マイナンバー法（番号法）で規定する安全管理措置の対象となる電子データに対しても、基本的には、これまで各省庁様で回答等を受けてきた個人情報保護法（注2）が規定する個人情報に対する有効性の確認結果同様な解釈に至るものと考えられる旨の認識をお伝えしました。結果は下記のように、基本的にこれまでの個人情報保護法に対する有効性確認結果をほぼ踏襲する認識となりました。下記の文章は上記認識内容の文章抜粋です。（認識内容の文章自体が少々長文な為）

---我々が認識できたと考える内容抜粋部、開始---
端的に言えば、個人番号や特定個人情報を秘密分散技術（電子割符）で処理し生成された割符ファイル単体は、個人番号や特定個人情報の定義から除外される。ということです。
～中略～
更に個人情報保護法の定義項記載の（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）の記述もあるので、個々の割符ファイルを適切に管理して容易に照合されないように管理していれば更に安全である。といった当該技術の持つ原理的な特徴を踏まえたうえで、マイナンバー法第二条5項や8項を確認し、上記回答となりました。
---我々が認識できたと考える内容抜粋部、終了---

我々秘密分散法コンソーシアムとしては、今回の認識内容には、当該技術のマイナンバー法（番号法）に対する貢献可能性部分と、既存安全管理措置（技術的安全管理措置）のメインである暗号技術に対する解釈、当該技術を実装したITシステム等を構築する際の留意点等、更に新たな安全管理措置（技術的安全管理措置）として秘密分散技術（電子割符）を市場普及させていく際に正しく技術内容を理解していただくこと（注3）も含まれていると認識しており、個人番号の取得、保管、利用、提供（移送含む）から廃棄に至るまでの間、常に要求される安全管理措置に対し有効活用できることになると考えております。

出典：秘密分散法コンソーシアム http://www.sss-c.org/?p=86 （2015年2月17日）
我々秘密分散法コンソーシアムとしては、本貢献可能性認識内容を継続的に情報開示し、消費者保護の観点からも錯誤や誤認等の問題が生じないよう、標準化も推進してまいります。

要点解説：

標準化関連用語定義の一部

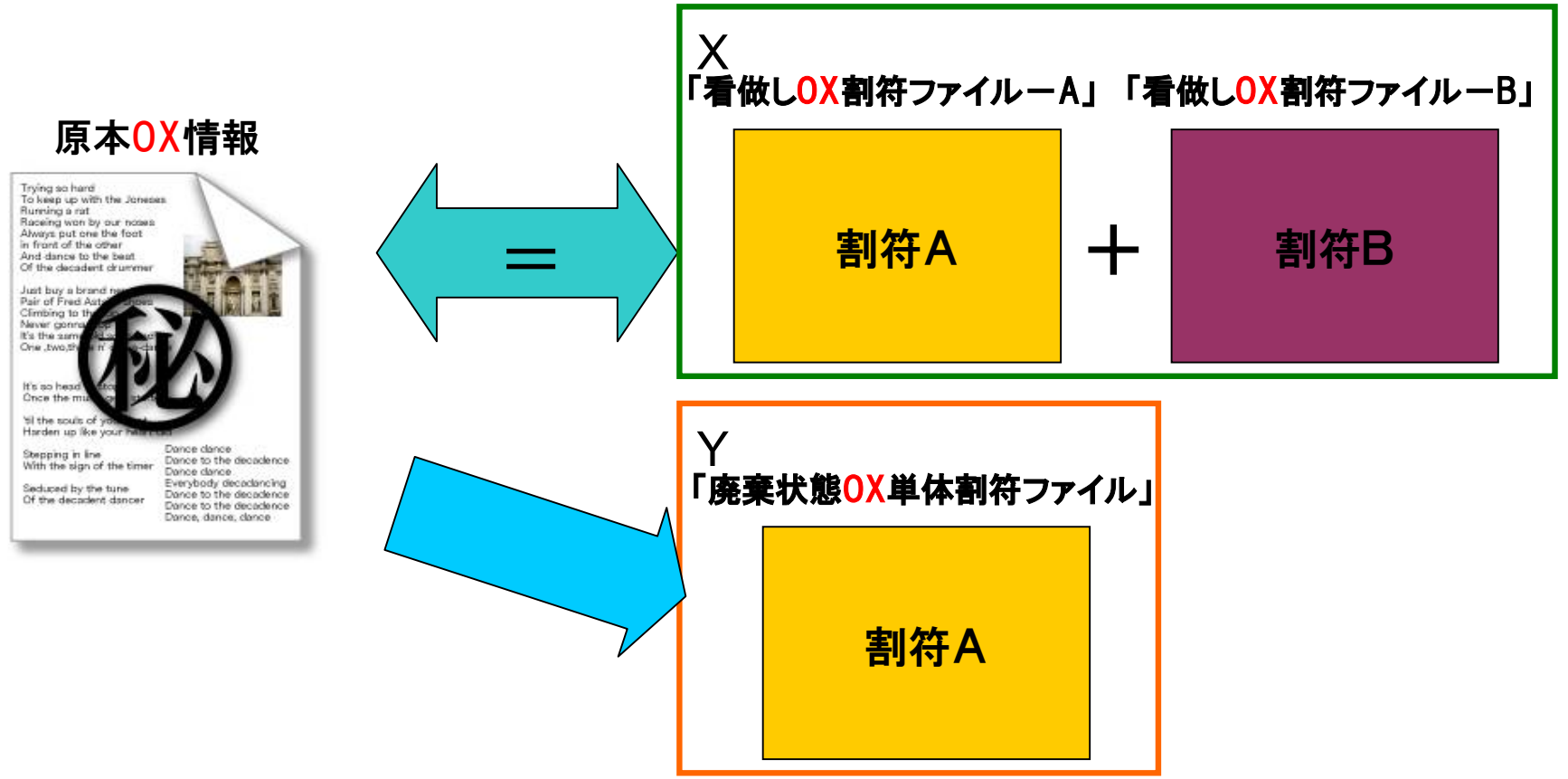
1、用語提唱

X:組織等で容易に照合・復元できる状態で割符ファイルを管理

Y:上記割符ファイルのうち一部が外部に出てしまい照合不能な状態の割符

2、利活用の仕組み・・・実装編ガイドライン検討材料へ

K:電子的資産等廃棄アプリ



総務省　行政情報システム企画課　見解

秘密分散法コンソーシアムが総務省e-Gov電子申請システム担当の行政管理局 行政情報システム企画課に、公表する文章としての了承・確認（平成26年12月19日時点）を経た情報を記す。以下、了承・確認を経た情報。

特定個人情報保護委員会は、すでに事業者向け説明会やガイドラインで暗号化してあっても、個人情報であり、個人番号、更には特定個人情報であることを示しており同法に対応した公的な電子申請基盤も何らかの対処を行なう可能性がある。（経済産業省個人情報保護法ガイドラインも、対象は個人情報であるが同様の解釈）

1、個人番号や特定個人情報が含まれない内容の電子申請は、既存の電子申請の仕組みを大きく変更しないものと考えられる。
2、一方、明らかに個人番号や特定個人情報が含まれる内容の電子申請の場合には、現在その仕様がFixしていないので、今後検討され仕様が公開されると考えられる。尚、そうした際に参考とすると考えられるのは、

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/guide26.pdf
の、P58の　第3部 情報の取扱い　3.1 情報の取扱い　3.1.1 情報の取扱い　目的・趣旨
行政事務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等
（以下、本項において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての行政事務従事者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、行政事務従事者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

の段の、P73の、

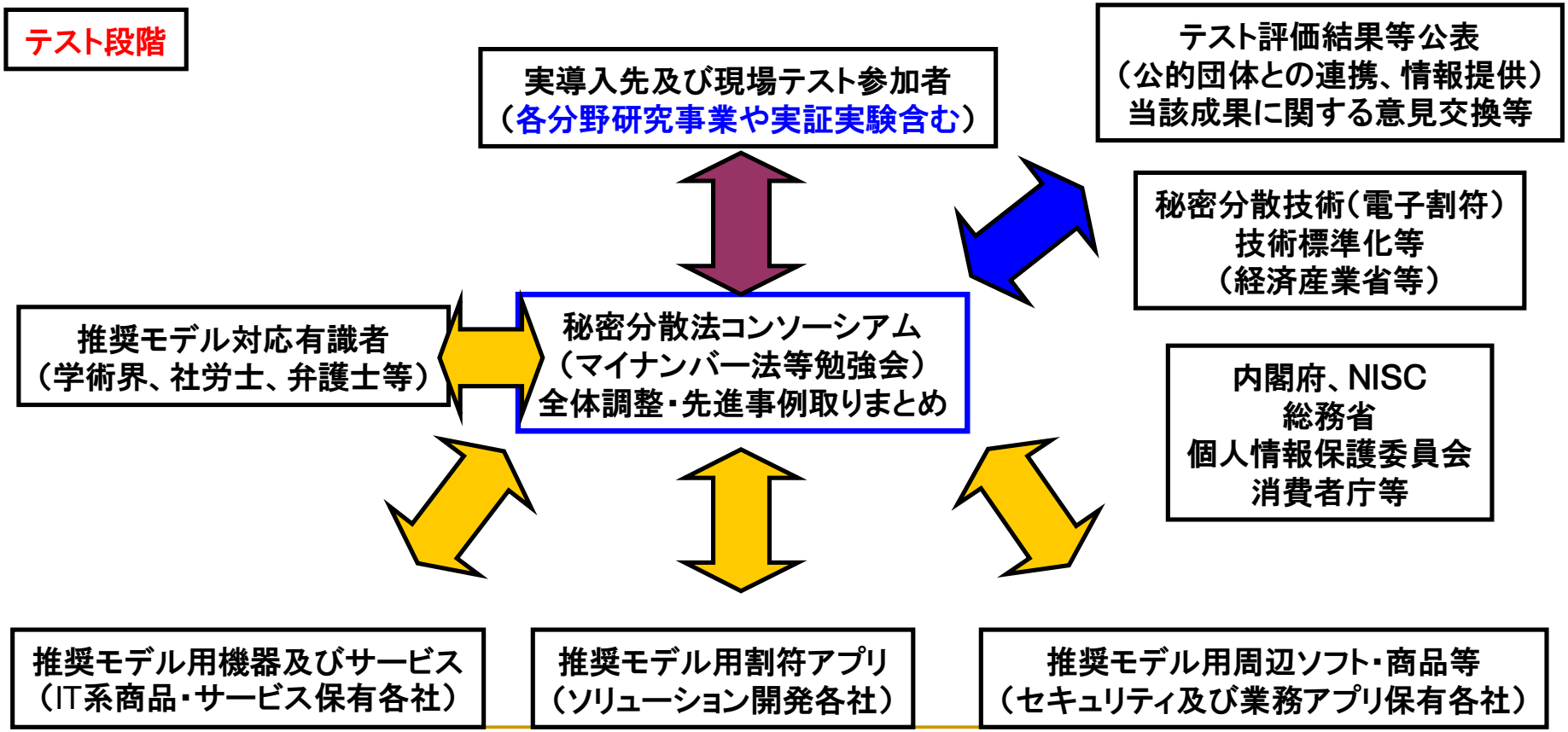
3.1.1(6)-2 行政事務従事者は、要機密情報である電磁的記録を要管理対策区域外に運搬又は府省庁外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。
a) 運搬又は送信する情報を暗号化する。
b) 運搬又は送信を複数の情報に分割してそれぞれ異なる経路及び手段を用いる。
c) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、
これに備わる機能を利用する。

といったあたりではないかと考えられる。
以上。

健全な利用事例からの標準化に向けて

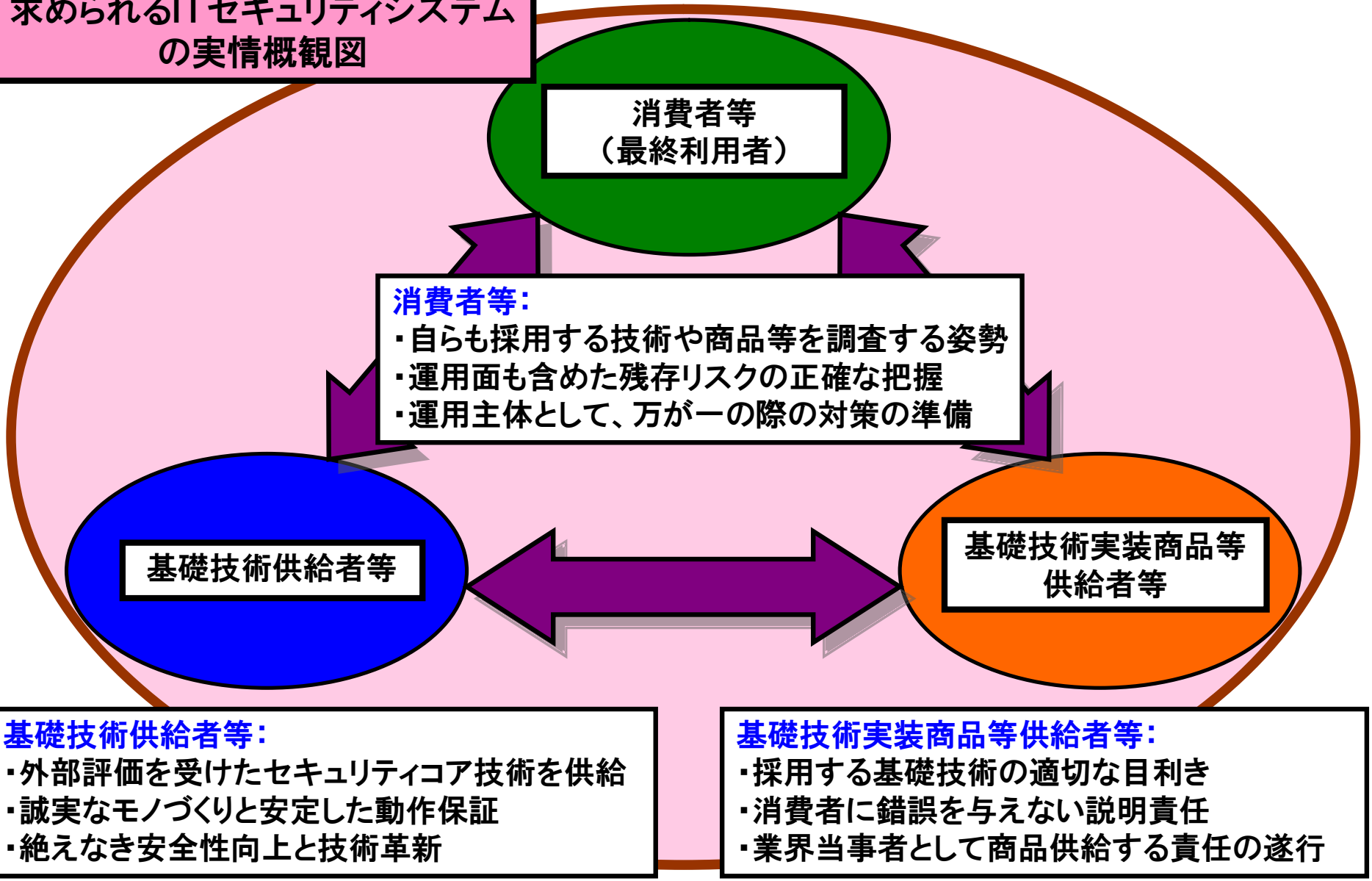
要点：

ポイント：
①コンソーシアムとしての社会貢献と、現実的な法令対処支援モデルを具体化、秘密分散技術標準化の中で、提言されてきている推奨パッケージの具体例を構築する。
②コンソーシアム参加各位の得意分野・商品・サービスを組み合わせモデル化
③全体及びドキュメント等をコンソーシアムとして監修
④コンソーシアム推奨モデルソリューションとして、市場供給
⑤関係省庁等やコンソーシアムで推進している技術標準化等へのフィードバック



コンソーシアムの準備するガイドライン等と課題

求められるITセキュリティシステムの実情概観図



基礎技術供給者等：
- 外部評価を受けたセキュリティコア技術を供給
- 誠実なモノづくりと安定した動作保証
- 絶えなき安全性向上と技術革新

基礎技術実装商品等供給者等：
- 採用する基礎技術の適切な目利き
- 消費者に錯誤を与えない説明責任
- 業界当事者として商品供給する責任の遂行

グローバルフレンドシップ株式会社

〒151-0073
東京都渋谷区笹塚1-32-2ソネット笹塚102
gfi-info@gfi.co.jp
http://www.gfi.co.jp/

GFI創業理念「たくさんの人を幸せにしたい。」