NPO法人　市民と電子自治体ネットワーク
平成30年度第5回研究WG＆セミナー　講演資料

「電子割符」概要と導入事例及び今後の展開

2019年03月18日版

秘密分散法コンソーシアム　事務局

（16日講演後、一部資料修正）

注：本資料は、（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 」と、当コンソーシアムが公表している官公庁等への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、最新情報はコンソーシアムまでお問い合わせください。

秘密分散法コンソーシアム

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、利用側組織様、法曹界、学術(数学)界、公的団体様、更に経済産業省様や内閣官房様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。

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、具体的且つ健全な利用モデルから、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)
山口叔史(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

＊「秘密分散技術」とは、NISCが当該技術をNISCドキュメントに記載するにあたり事前にGFI社と打ち合わせをしていた際に、電子割符名称を用いようとしていたが、GFIの商標(GFI電子割符)に抵触等する可能性があるため新たな技術名称を席上で創出したことがはじまりです。

ご存知ですか

EUでも日本でも、暗号化したデータは個人情報です。

EU指令関係資料抜粋：
通常、仮名化データは、**不可逆的に識別が防止されたもの**ではなく、依然として「個人データ」に該当します。
個人データを暗号化した場合、～中略～暗号を解く鍵が存在する限りにおいて、個人の識別が不可逆的に防止された訳ではないため、「匿名化データ」には該当しません。その結果、**暗号化されたデータは、依然として「個人データ」に該当するため、暗号化されたデータの処理および移転についてはGDPRが適用される**ことになります。

出典：「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編） 2016 年 11 月　日本貿易振興機構（ジェトロ）
ブリュッセル事務所 海外調査部 欧州ロシア CIS

日本個人情報保護法ガイドライン抜粋：
「個人情報」（※1）とは、生存する「個人に関する情報」であって、「当該情報に含まれる氏名、生年月日その他の記述等により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ものを含む。）」（法第 2 条第 1 項第 1 号）、又は「個人識別符号が含まれる もの」（同項第 2号）をいう。
「個人に関する情報」とは、氏名、住所、性別、生年月日、顔画像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、評価を表す全ての情報であり、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**。
（※）「他の情報と容易に照合することができ」るとは、事業者の実態に即して個々の事例ごとに判断されるべきであるが、通常の業務における一般的な方法で、他の情報と容易に照合することができる状態をいい、例えば、他の事業者への照会を要する場合等であって照合が困難な状態は、一般に、容易に照合することができない状態であると解される。

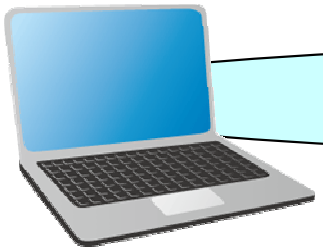
出典：個人情報の保護に関する法律についてのガイドライン（通則編）平成 28 年 11 月（平成 29 年3月一部改正）個人情報保護委員会

世界標準のRSA暗号は量子コンピューターで解読されることが証明されている

出典：NICT NEWS　https://www.nict.go.jp/publication/NICT-News/1303/02.html

官民問わず深刻な経営課題

個人情報等漏洩の賠償額等は高騰。制裁金は損害賠償保険が使えません。



利用者

医療・保険データ

金融データ

公共データ

エンターテイメント（著作権）/
メディアデータ

GDPRやeプライバシー/
個人情報

研究データ
営業秘密

事業者-Ⅰ

事業者-Ⅱ

事業者-Ⅲ

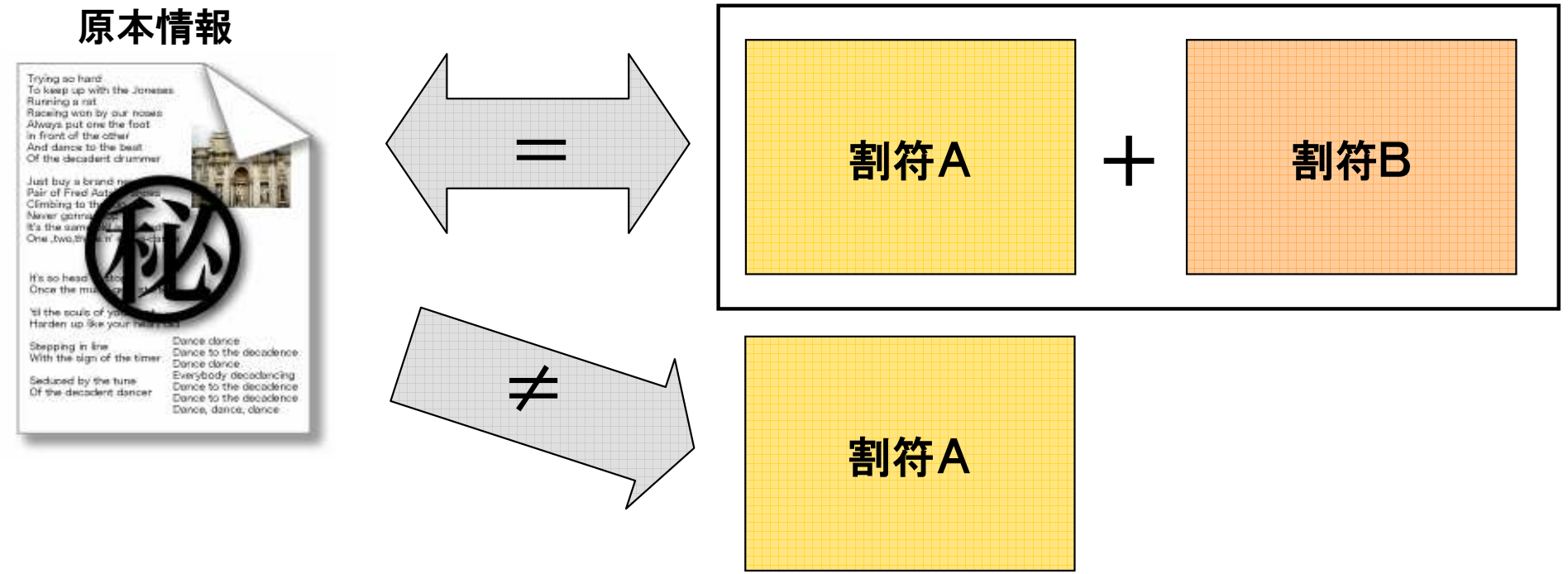
事業者-う

**GDPR制裁金やセキュリティ関連の
被害総額から市場規模は、
少なくとも数十兆円規模**

高度化するサイバー攻撃やウイルス等

代表的秘密分散技術電子割符概要

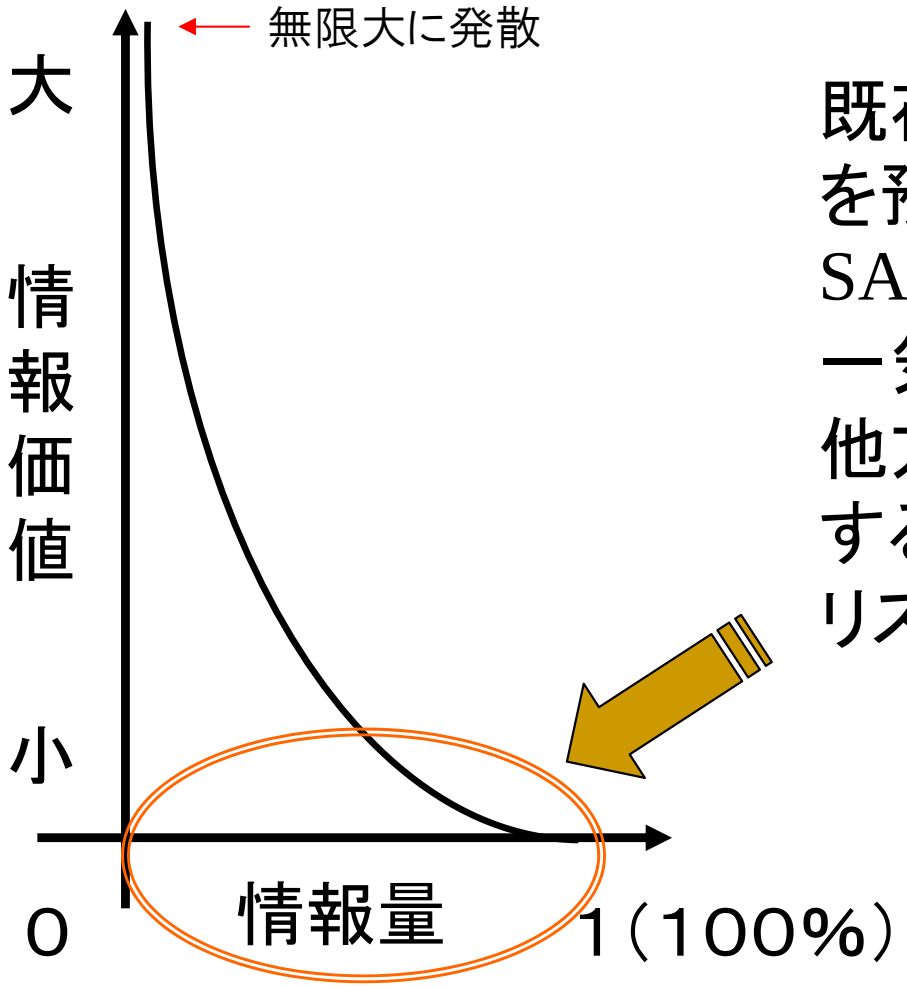
デジタル原本情報を非線形にビットレベルで分割し、復元に至らない数の割符では原本情報に復元出来なくする技術です。



データ移送、保管等で重要情報の安全管理に利活用できます（＊1）。

（＊1）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）
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
（要機密情報移送時の安全確保（強化遵守事項）、モバイルPC内の要機密情報の安全確保）
http://www.nisc.go.jp/active/general/pdf/k303-052c.pdf
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（サーバー装置内の要安定情報の安全確保）
http://www.nisc.go.jp/active/general/pdf/K305-111C.pdf
政府機関等の対策基準策定のためのガイドライン（平成30年度版）（要機密情報移送時の秘密分散技術との記述部分は敢えて一般的な表現として「分割」と修正）
https://www.nisc.go.jp/active/general/pdf/guide30.pdf

情報セキュリティー基本エントロピー



既存暗号技術やクラウドにデータを預けるといった手法は、SAFEorNOTの情報管理であり、一気にリスク顕在化してしまう。
他方、秘密分散技術を利活用すると、他段階の柔軟なリスクヘッジが可能になる。

秘密分散技術の場合、原本情報復元には一定数の割符を糾合することが最低限の条件なので、漏洩等のリスクを段階的に管理できる

代表的秘密分散技術電子割符外部評価

東京大学

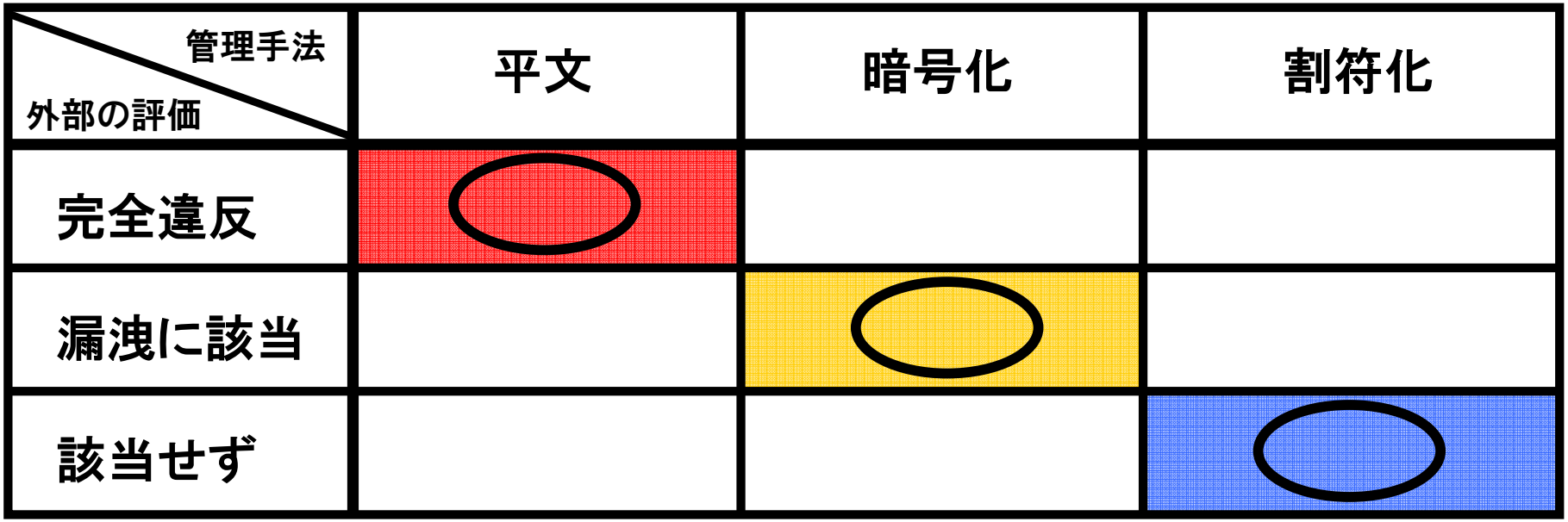
電子割符セキュリティ強度調査報告書　2001年12月20日
電子割符は、秘密情報を分割して安全に伝送（または記録）する目的に開発された符号化法（およびそれを実現するためのソフトウエア）である。秘密情報である平文Sをn個の割符に分割符号化し、n個の割符が全部そろえば、平文Sが複合できるが、n−1個以下の割符からは平文Sの情報が漏れないように工夫されている。（注：通常非公開資料）

産業技術総合研究所（下記参考URL公開情報抜粋）

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（中略）当該技術の安全性はこうした**技術標準化の検討に値する水準**にあるものと期待できると考える。

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

代表的秘密分散技術電子割符特性



個人情報への技術的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**。既存暗号よりも高度な安全管理措置を実施できる。
（平成27年02月20日経済産業省確認ー注：復元に至らない一部の割符が出た場合、一部の割符であって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）

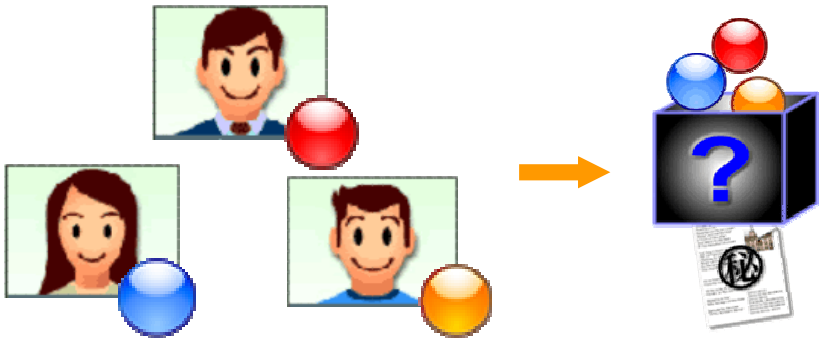
訴訟リスクの回避（＊2）

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。

（＊2）ECにおける情報セキュリティに関する活動報告書2009「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

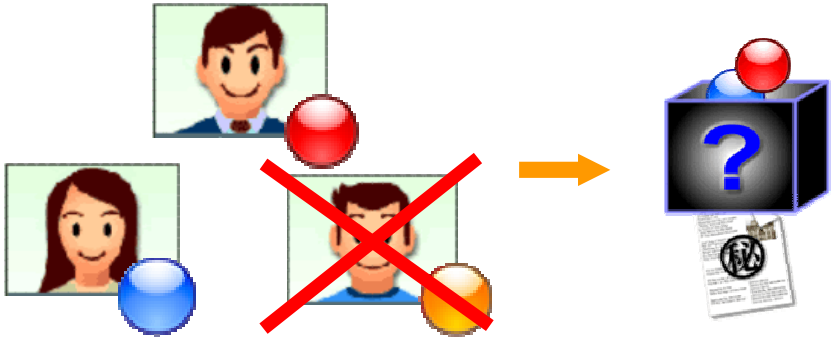
代表的電子割符の基本機能

(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)

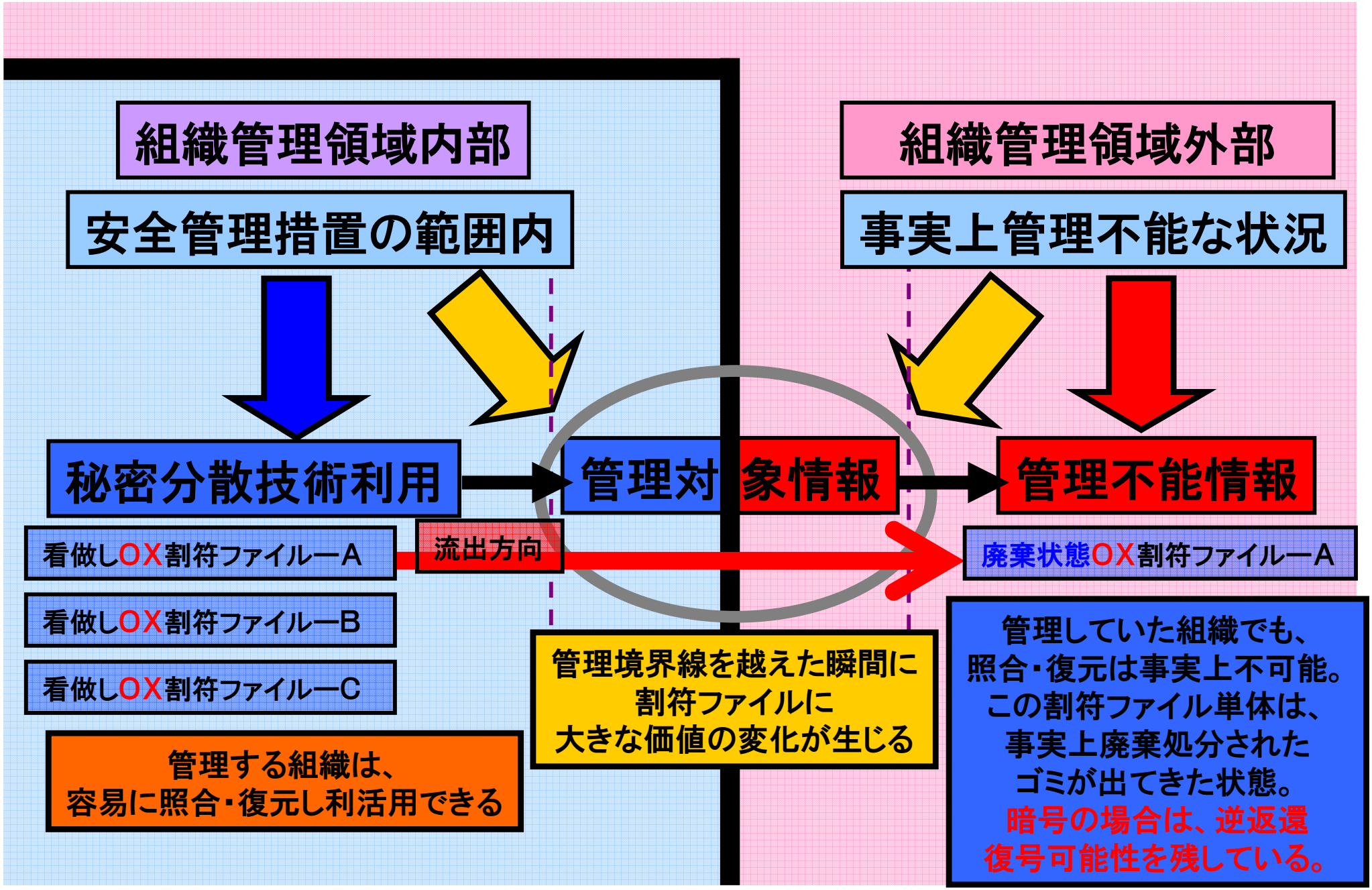


一部の割符が揃わなくても、原本復元を、敢えて可能にする。
ただし、それぞれの割符単体から、原本復元はできない。

(3)最小化モード一生成する割符サイズを小さくできます。
・一般にn,n型は、自由度が大きくしやすい

(4)自己認証機能一復元する際の条件設定ができます。

積極的安全性を持つ割符の特徴



主要実績

公共系：

総務省、経済産業省、厚生労働省、一般財団法人、自治体、
日本赤十字社、等

民間系

株式会社アイ･オー･データ機器
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
凸版印刷株式会社
エヌ･アール･アイセキュアテクノロジーズ株式会社
寿精版印刷株式会社
株式会社ソリトンシステムズ
三井物産セキュアディレクション株式会社
新日鉄住金ソリューションズ株式会社
ファイブテクノロジー株式会社、他

秘密分散技術（電子割符）は、日本が世界に先駆け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、今後必須のセキュリティコア技術です。

参考：ECにおける情報セキュリティに関する活動報告書2009
「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2009(TF1)」、ECOM、2010年3月.
http://www.jipdec.or.jp/archives/publications/J0004291

代表的秘密分散技術処理概要

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）

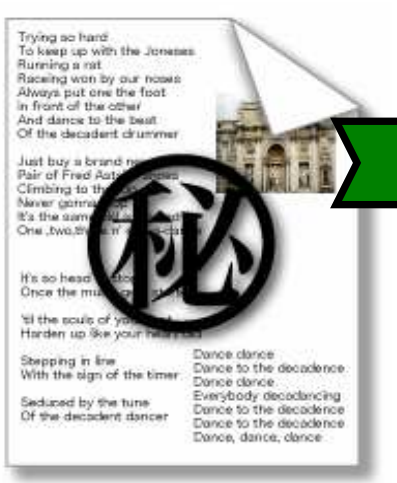
111010
010001
101110
110110
01・・・・・

1
0
0
1
0
1
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。

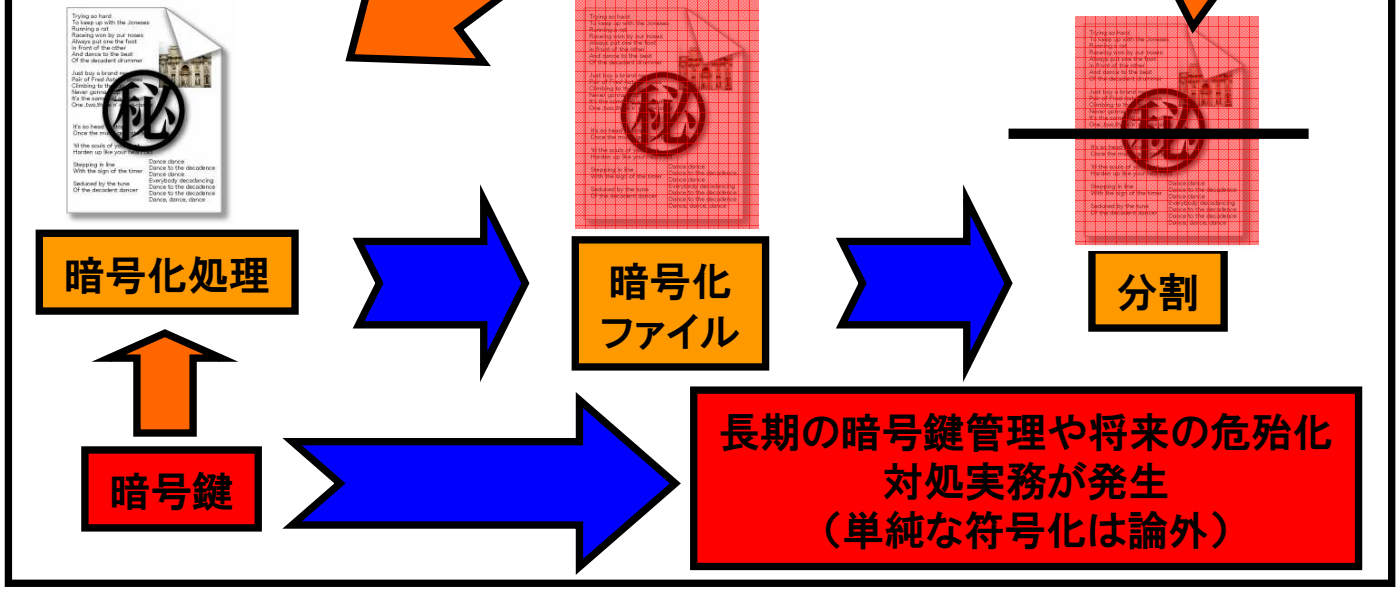
類似亜種技術処理概要例

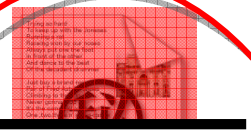
原本情報



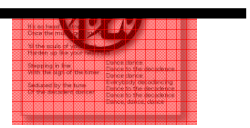
暗号化
（符号化含めた変換手法）
＋
ファイル分割(ビット抽出含む)
技術区分ーB

内部では





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。

今後更にケアすべき法令ルール等①

①サイバーセキュリティ基本法

（定義） 第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

（基本理念） 第三条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。
4　サイバーセキュリティに関する施策の推進は、サイバーセキュリティに対する脅威への対応が国際社会にとって共通の課題であり、かつ、我が国の経済社会が国際的な密接な相互依存関係の中で営まれていることに鑑み、サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、国際的協調の下に行われなければならない。

（地方公共団体の責務） 第五条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

第五章　罰則
第三十七条　第三十条第二項の規定に違反した者は、一年以下の懲役又は五十万円以下の罰金に処する。

なお、サイバーセキュリティ基本法に基づく閣議決定等で地方公共団体のセキュリティ強化・充実は項目として明記されおり、主担当府省庁は、NISC、内閣府、総務省であり、関係府省庁は内閣官房、これに内閣府の番号制度担当室、個人情報保護委員会も関与する。
サイバーセキュリティ戦略　平成30年7月27日
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf

POINT:
ア：漏えい、滅失又は毀損の防止その他の当該情報の安全管理
イ：電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理
ウ：多様な主体の連携により、積極的に対応する
エ：国際的協調の下に行われなければならない
オ：地方公共団体は、自主的な施策を策定し、及び実施する責務を有する

今後更にケアすべき法令ルール等②

②不正アクセス行為の禁止等に関する法律

（定義）
第二条　この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者をいう。

２　この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。
一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号
二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号
三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

（アクセス管理者による防御措置）
第八条　アクセス制御機能を特定電子計算機に付加したアクセス管理者は、当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに、常に当該アクセス制御機能の有効性を検証し、必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。

（罰則）
第十一条　第三条の規定に違反した者は、三年以下の懲役又は百万円以下の罰金に処する。
第十二条　次の各号のいずれかに該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。
第十三条　第五条の規定に違反した者（前条第二号に該当する者を除く。）は、三十万円以下の罰金に処する。
第十四条　第十一条及び第十二条第一号から第三号までの罪は、刑法（明治四十年法律第四十五号）第四条の二の例に従う。

POINT:
ア：符号の適正な管理
イ：身体の全部若しくは一部の影像又は音声
ウ：速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努める

今後更にケアすべき法令ルール等③

③GDPR　2018年5月25日EUからから全世界に向け施行

個人データの取り扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（一般データ保護規則）

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

旧来のEU指令に基づく個人情報保護が強化されている。例えば、72時間ルールなどが知られているが、

・個人情報を開示する者の権利保護の強化（データ最小化含め）
・平易な表現で説明し同意を得ること（子供からのデータ収集には保護者の同意が必要）
・本人が自らの個人情報にアクセスできるようにし、且つ別な会社に渡せるようにすること
・例外を除き本人に忘れられる権利を与えること
・個人情報を利用したダイレクトマーケティングを拒否する権利
・センシティブ・データの特別な保護
・EU当局の承認を得ていない国への個人情報域外データ移転の制限・留意事項
・サービスや商品設計時からデータ保護を組み込むこと（PBD（プライバシーバイデザイン）―DPBD（データプロテクションバイデザイン・デフォルト））
・他社の為に個人情報を取り扱う場合の責任関係等を明確にした契約
・個人情報取り扱いに関する記録義務（雇用250人未満の中小企業や組織の場合は①定期的取り扱い、②自由と権利にとって脅威となる取り扱い、③センシティブ・データや犯罪記録）
・ハイリスクな個人情報取り扱いには影響評価が必要な場合がある（生体認証のようなセンシティブ・データの大規模な取り扱い、個人情報の自動的、体系的な取り扱いと評価等）
・制裁金最大2000万ユーロ又は全世界年間売上の4％のどちらか高い方
・暗号化は追加情報（鍵）により個人情報に戻るため仮名化（Pseudonymisation）であり、不可逆な匿名化（Anonymous）ではないので、暗号化してあってもGDPRの個人情報であるが、新たなセキュリティサービス等が出るまでは利用すべき・・・偽名化pseudonymization？
データ保護の原則は、「匿名の情報、すなわち、識別された、または識別可能な自然人に関係しない情報、またはデータの主題が識別できない、またはもはや識別できないような形で匿名化された個人データ」には適用されない。

POINT:

ア：EU域内の個人の情報を直接又は間接（下請け等）でも収集、保存、利用するのであればGDPR対象
イ：GDPRは官民ともに対象・・・日本も対象
ウ：制裁金は損害賠償保険が利用できないうえに、巨額になるので個人情報管理が不適切だと深刻な組織のリスクとなる（民事・刑事訴訟は別）
エ：現時点暗号が例示されているが、技術革新や新たな匿名化、仮名化、暗号化といった技術が奨励され組織的ソリューションが期待されている

今後更にケアすべき法令ルール等④

④現状個人情報保護法や特定個人情報保護法やガイドライン、及び近く改正された後の法律とガイドライン

個人情報の保護に関する法律 （定義）

第二条　この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。第十八条第二項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により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（注2）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。）

9　この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。
一　第一項第一号に該当する個人情報　当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
二　第一項第二号に該当する個人情報　当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

（安全管理措置）
第二十条　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。

第八十二条　第七十二条の規定に違反して秘密を漏らし、又は盗用した者は、二年以下の懲役又は百万円以下の罰金に処する。
ー以下の罰則条項略ー

POINT:
ア：早期からEU指令をケアしていたので、日本の個人情報保護法の暗号化や匿名化に関する解釈は似ている
イ：ビッグデータ利活用に向けた匿名化に関しては、その情報粒度が問題（オンラインでの本人特定をする人々のスキルは恐ろしい）
ウ：集団訴訟における損害賠償額は高騰
エ：復元に至らない数の割符の流出があったとしても、そもそも重大事態に該当しないし、訴訟にも至らない
オ：割符の一部流出はそもそも実害発生しないが、更に言えば外部流出したその組織でしか情報復元できないので報告を要しない
（割符は高度な暗号化等の「等」と看做せるという一部官公庁意見もある）

注1：「行政機関の保有する個人情報の保護に関する法律」、「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」も、同様に、GDPRの十分性認定後の法改正に向けたケアが必要
注2：「行政機関の保有する個人情報の保護に関する法律」の場合、～容易に～の記述がないので、より厳格

今後更にケアすべき法令ルール等⑤

⑤NIST SP800-171

NIST(National Institute of Standards and Technology：米国国立標準技術研究所)は、科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関です。
　NIST内には、情報技術に関する研究を行っているITL(Information Technology Laboratory)があります。
　ITLは情報技術に関して6つの分野(Security, Information Access, Mathematics and Computational Science, Software Testing, Networking Research, Statistical Engineering)の研究を行っており、ITLの中でコンピュータセキュリティに関して研究を行い各種文書を発行しているのがCSD(Computer Security Division)と呼ばれる部門です。FIPSやSP800シリーズの文書も、CSDが発行しています。

国際的に見れば前述のEU発のGDPRとこのNISTの要求事項は、官公庁や大手企業等が情報セキュリティ対策を検討するにあたり、非常に重要なファクターと言えます。わが国も、サイバーセキュリティ基本法等を踏まえ、その対処は当然
視野に入りますので、今後の対策や仕様検討の際にはこうした潮流や対策に関する基本認識を踏まえ対処すると良いと考えます。
すでに中央官庁等の調達に関し、対応検討が始まっています。

自治体の皆様の場合には、下記の「行政手続きオンライン化関係三法」等も踏まえ、リスク最小化を具体化すると良いでしょう。

申請・届出などの行政手続をオンラインを通じて行う際の、公的個人認証サービス制度に必要な電子証明書や認証機関などについての決まりごとが盛り込まれています。
以下の3つの法律をまとめて「行政手続オンライン化関係三法」と言います。
行政手続等における情報通信の技術の利用に関する法律(行政手続オンライン化法)
行政手続等における情報通信の技術の利用に関する法律の施行に伴う関連法律の整備等に関する法律(整備法)
電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律(公的個人認証法)
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/06.html

POINT:
ア：高度なサイバー攻撃は世界中から行われるので、情報セキュリティは日本単独の視点で対処すれば良いものではない
イ：対策具体化の際には、サイバーセキュリティ基本法等を踏まえ社会基盤の安全安心を具体化する
ウ：現時点衆目の一致するルール等は、EUのGDPRと米国のNIST SP800-171である

今後更にケアすべき法令ルール等⑥

⑥ 平成30年9月版総務省 「地方公共団体における情報セキュリティポリシーに関するガイドライン」

はじめに
～本ガイドラインを参考として、各地方公共団体においては、必要に応じて内容を取込み、情報セキュリティ強化により一層ご尽力いただくことを願うものである。
第1章　本ガイドラインの目的等　1．本ガイドラインの目的
～地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産を守るにあたって自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。～本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではない。～今後は情報セキュリティポリシーの定期的な評価・見直しを行い、情報セキュリティ対策の実効性を確保するとともに、対策レベルを高めていくことが重要である。

平成30年9月版総務省 「地方公共団体における情報セキュリティ監査に関するガイドライン」

第1章　総則　1.1.本ガイドラインの目的
～本ガイドラインは、情報セキュリティ監査の標準的な監査項目と監査手順を示すものであり、地方公共団体が情報セキュリティ監査を実施する際に活用されることを期待して作成している。
　もとより、本ガイドラインに記述した構成や項目等は参考として示したものであり、各地方公共団体が必要に応じて独自の情報セキュリティ監査項目を追加設定したり、監査方法を修正するなど各団体の実情に応じた変更を加えて、情報セキュリティ監査を実施することを妨げるものではない。

なお、地方公共団体のセキュリティに関し主担当府省庁でもあるNISC公開の下記資料も参考とされたい。（後述の移送モデルも記載されている）
政府機関等の対策基準策定のためのガイドライン（平成30年度版）内閣官房　内閣サイバーセキュリティセンター
https://www.nisc.go.jp/active/general/pdf/guide30.pdf

POINT:
ア：どちらのガイドラインも、各地方公共団体の自主的アクションへの参考でしかない
イ：各地方自治体の自主的なセキュリティの見直しや高度化を求めている
ウ：最終責任は各地方公共団体にあり、このガイドラインを遵守しても無罪放免とはならない

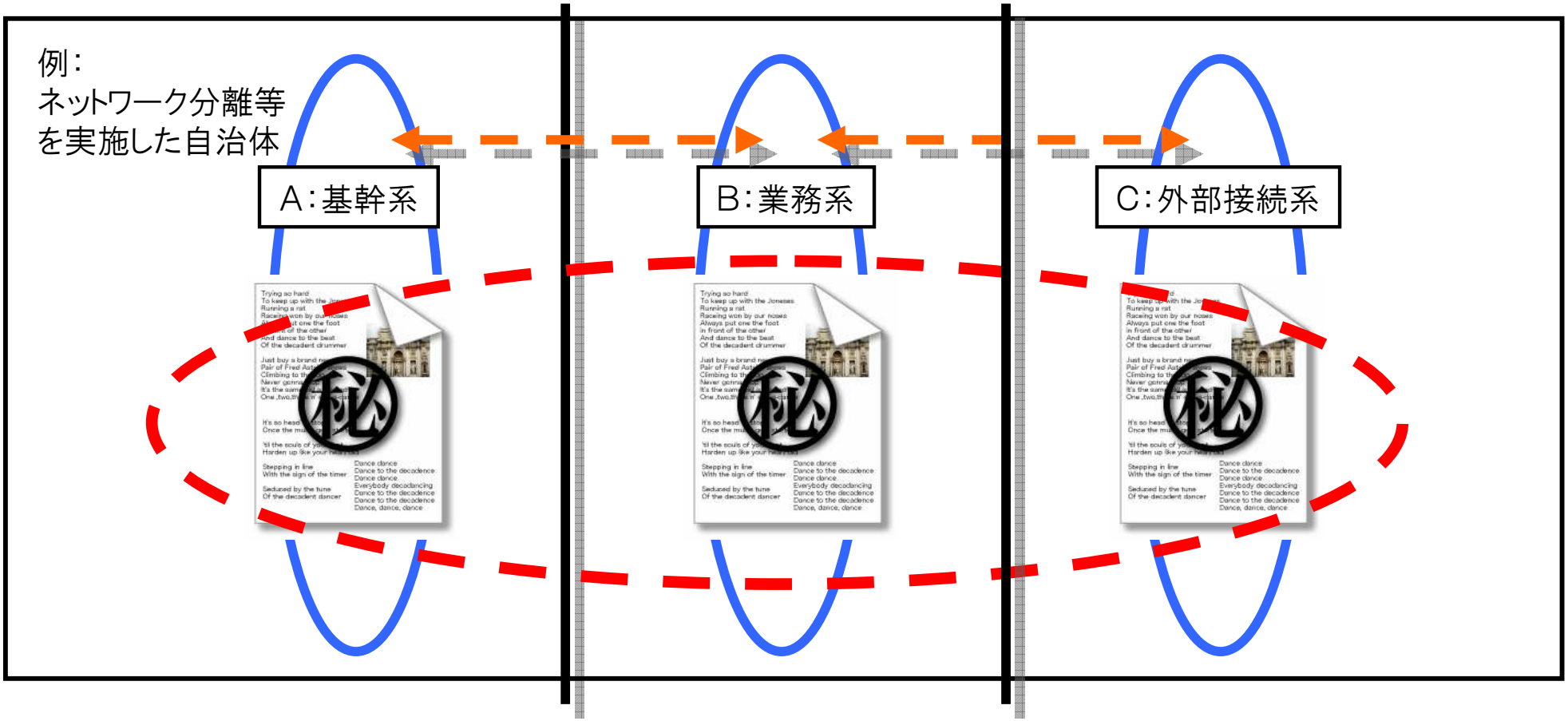
結論：
前述の①サイバーセキュリティ基本法～⑤NIST　SP800-171などを踏まえると、国際的な情報セキュリティ動向を視野に入れ、高度なサイバー攻撃や不正アクセス等を想定した被害を最小化できる現状最善の対策と、事故発生後も含めた具体策を自主的に導入していくことが、無言のうちに求められていると考えられる

非定型(構造)ファイル

業務上発生は不可避

実務上多様な情報は系を超えている

基幹系システム内で管理されている定型（構造）ファイルやデータよりも、
圧倒的に実務端末内の情報（非定型（非構造）ファイル等）が増大している
この中には外部流出により被害や損害発生が生じるファイル等も多数存在する



参考：「秘密分散技術勉強会」ー自治体への適用（実証）事例紹介　2016年10月27日　講演資料
総務省報告秘密分散法コンソーシアム資料図を一部修正

不正攻撃で暗号化されたら

情報セキュリティの対象は、情報の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。

出典：「個人情報の保護に関する法律についてのガイドライン（通則編）」 平成28年11月（平成31年1月一部改正） 個人情報保護委員会
https://www.ppc.go.jp/files/pdf/190123_guidelines01.pdf

POINT：

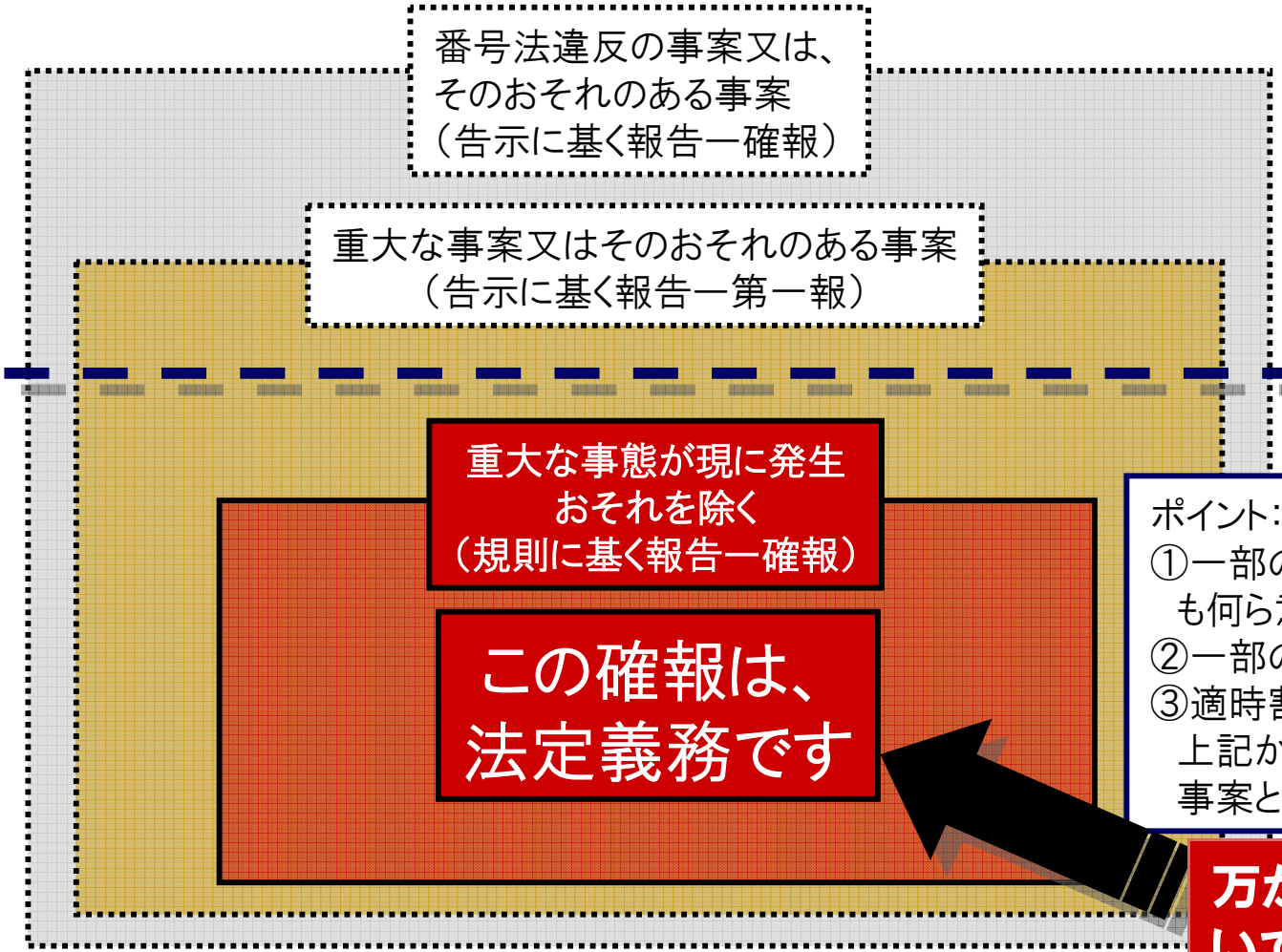
「漏えい等」とは、データの漏えい、滅失又は毀損（加工方法等情報の漏えいも含む）と、これらのおそれが生じた事案を指す

出典：個人情報保護委員会
漏えい等の事案が発生した場合の対応等の概要について
https://www.ppc.go.jp/files/pdf/180717_rouei_gaiyou.pdf
個人データの漏えい等の事案が発生した場合等の対応について
https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

保護対象情報の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。

例えば主務大臣等への報告とは

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：
①一部の割符流出は、それ自体が閲覧できたとしても何ら意味が無く、報告を要しない場合に該当
②一部の割符の消滅や毀損は、残りの割符で復元
③適時割りなおしによる上書きを行えば、更に安全
上記から仮に報告するとしても「おそれ」も生じない事案として報告できる

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。

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
https://www.ppc.go.jp/files/pdf/roueitaiou_gaiyo.pdf
同上　行政機関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
https://www.ppc.go.jp/files/pdf/roueitaiou_gyoseikikan.pdf

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。

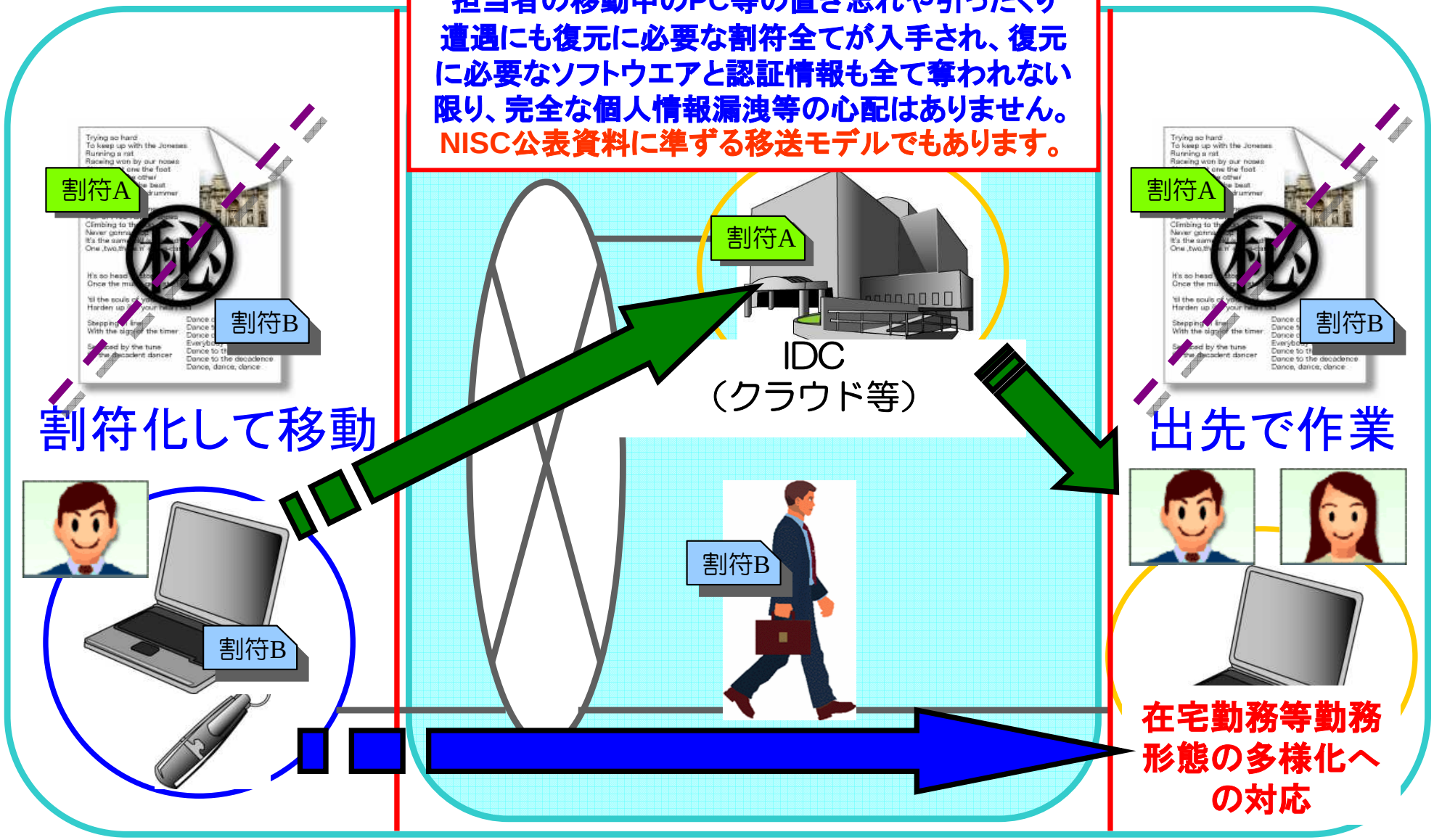
参考出典：平成21年度預金保険機構年報(P28中段以降記述より)
https://www.dic.go.jp/content/000014939.pdf
平成21年11月に検査部内において、検査用書類作成のために用意した金融機関の個人情報が記録された電子媒体が、所在不明になっている事実が判明しました。このため、機構では、再発防止策として、新たに管理要領を制定し、紛失防止に実効性のある管理簿等による電子媒体の管理に加え、搬送時に割符処理を行い、セキュリティの強化を図るなど、再発防止に全力で取り組んでいくこととしております。
②立入検査後のフォローアップ
機構が実施した検査の指摘事項については、金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・出先作業

商品利用出先シーン

想定状況：Wi-FI併用

移送中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

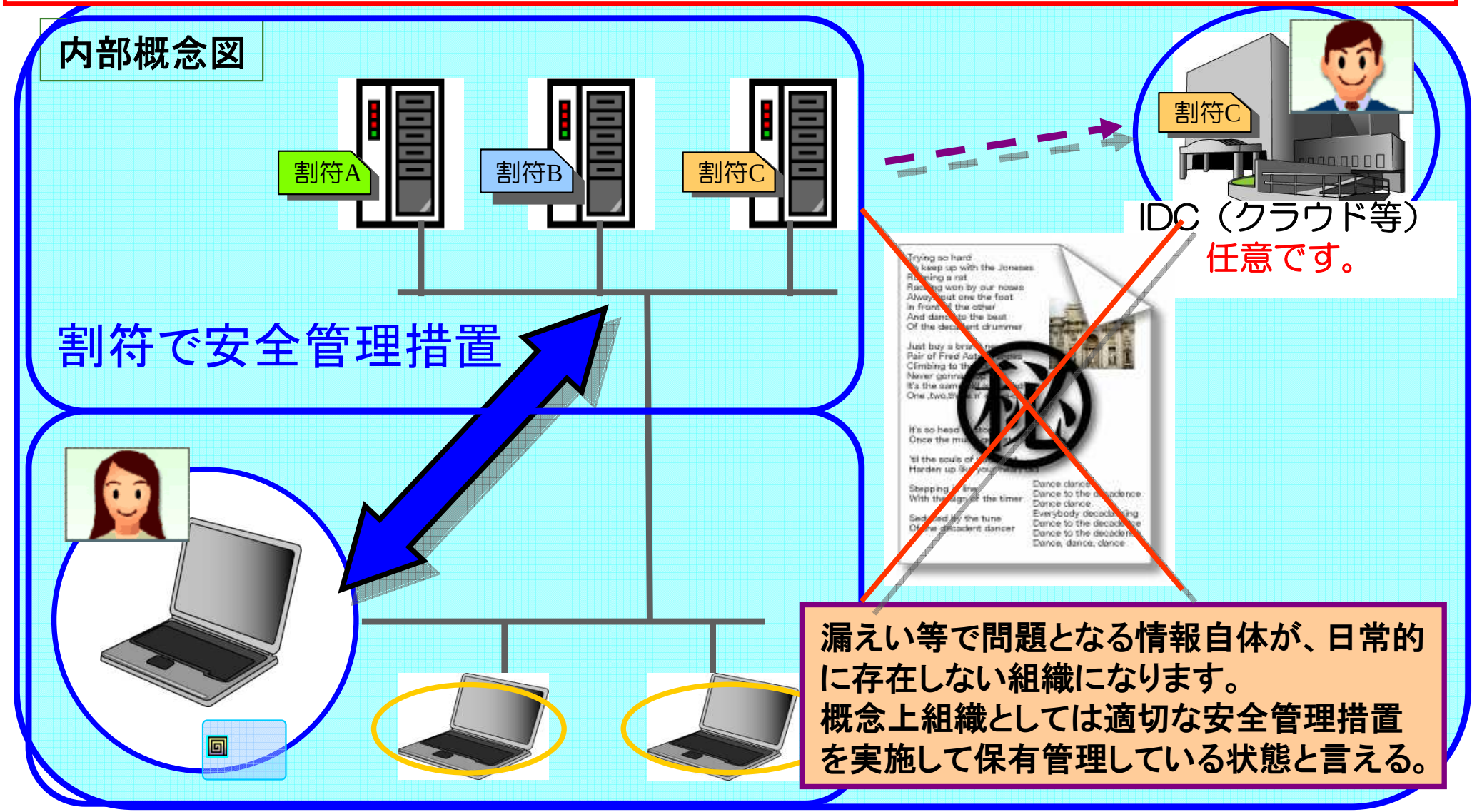
2.3.2.3 サーバ装置
趣旨（必要性）
サーバ装置については、当該サーバ装置の電磁的記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入等を受けるリスクが高い。政府機関が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きい。このようにサーバ装置の利用は、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。

内部概念図



**漏えい等で問題となる情報自体が、日常的に存在しない組織になります。
概念上組織としては適切な安全管理措置を実施して保有管理している状態と言える。**

参考：秘密分散技術の記述の入ったNISC資料の記述部－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）結果は、下記のとおり。

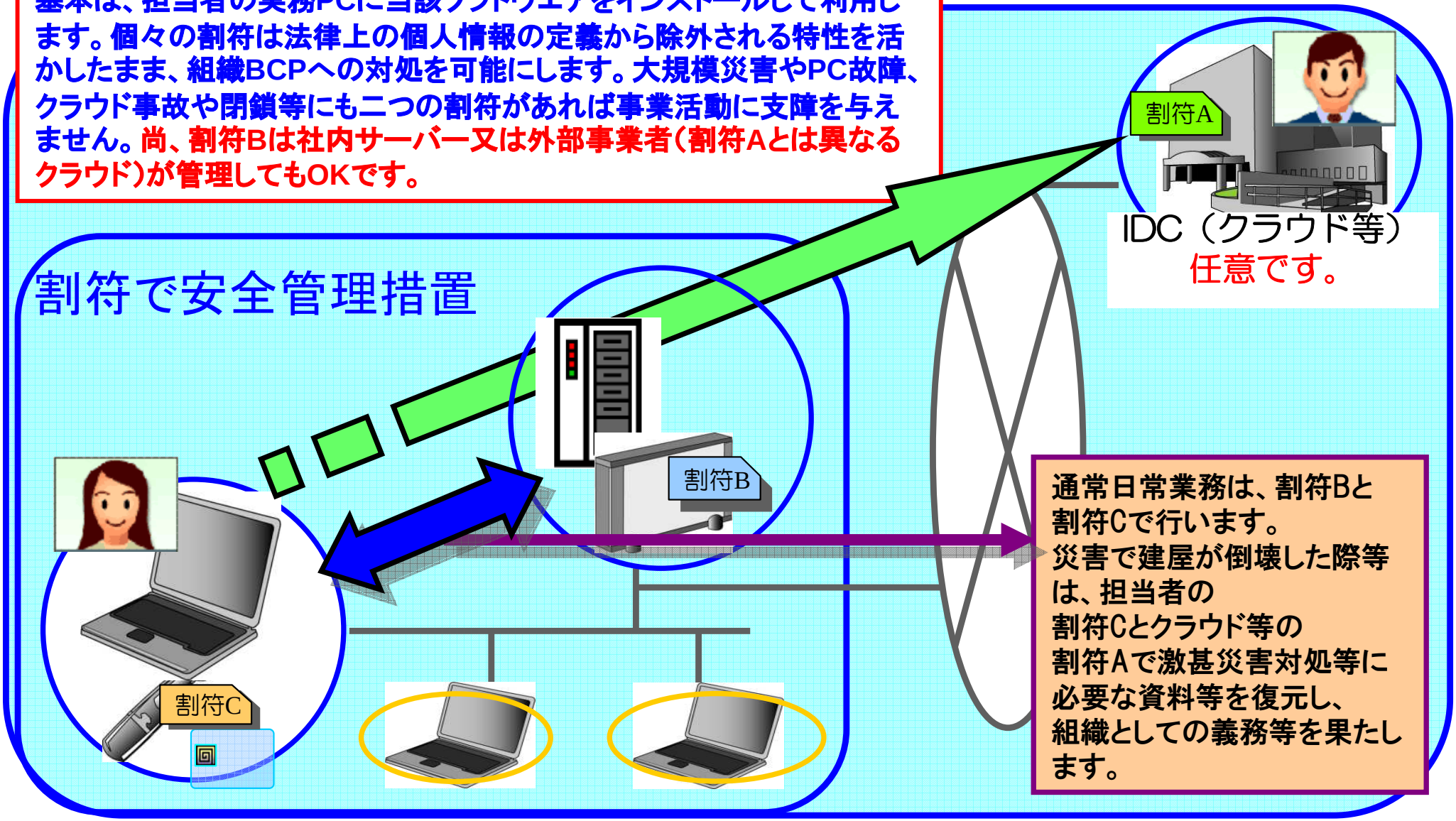
①府省庁ガイドラインは本来中央府省庁向けのものであるが、各自治体や民間等が参考として対策を行うことに制限を加えていない。
②具体的な対策検討の際に、NISCの既公開ガイドライン等を参考とすることに制限を加えていない。

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。

組織内情報管理基本形（保管・BCP）

内部個人情報・特定個人情報管理概念図

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。



参考：代表的既存暗号技術と秘密分散技術の比較表

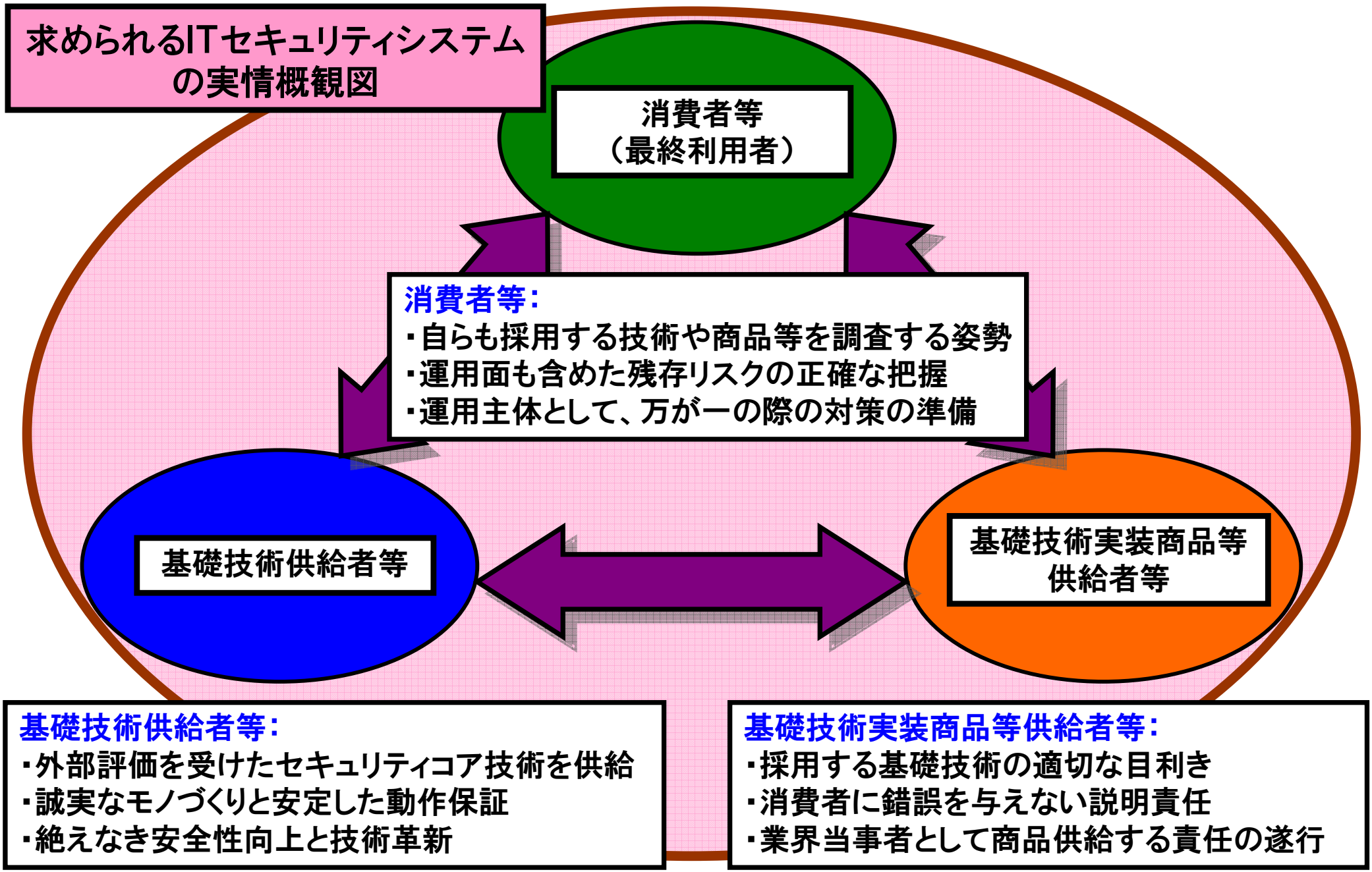
	処理速度	不特定多数	暗号通信	デジタル署名	暗号鍵管理	閾値秘密分散
共通鍵暗号技術	○	×	○	×	×	×
公開鍵暗号技術	×	○	×	○	×	×
秘密分散技術	○	×	×	×	○	○

理論的には実現可能だが商品・サービスとして存在していない

	得意分野	適用例	適用例
共通鍵暗号技術	高速暗号通信	VPN	IP-VPN、ルータ機器、
公開鍵暗号技術	不特定多数暗号	SSL	電子メール、サーバー認証、デジタル署名
秘密分散技術	長期分散データ管理	セキュア アーカイブ	営業秘密や要機密情報管理、情報資産保護、ファイル交換、 データエスクロー、TTP、鍵やID管理、セキュアバックアップ

従来の暗号方式は、Point to Pointの暗号通信を得意としているが、電子文書などの特定ファイルを長期間安全に保管するには、様々なセキュリティ対策が必要となる。
既存暗号と秘密分散技術を組み合わせることで相互補完できる。
例えばID/PASSや暗号鍵、暗号化データの長期間の安全性確保等、これも現代暗号の教科書で秘密分散法の項に出てくる話し。

策定等を進めているガイドライン



今後のリスク最小化デザイン