お客様各位

弊社及び
GFI電子割符®

2020，11

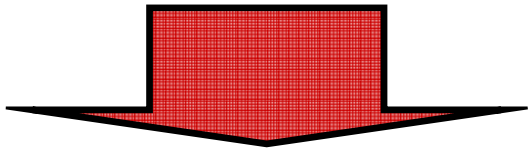
(一部誤記修正)

グローバルフレンドシップ株式会社

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GFIまでお問い合わせください。

エグゼクティブサマリー

GFI創業理念は「たくさんの人を幸せにしたい。」です。
弊社が開発したGFI電子割符®(わりふ)は、世界的な情報資産管理厳格化の潮流の中で、広く社会に解決策を提供し貢献し続けます。



ポイント:
①1999年に世界で最初に電子割符を市場供給
②弊社技術は情報理論的安全性を持つ
③一部の割符の流出は実害発生せず訴訟に至らない
④割符型情報資産管理基盤サービスを世界に供給

現代社会の課題

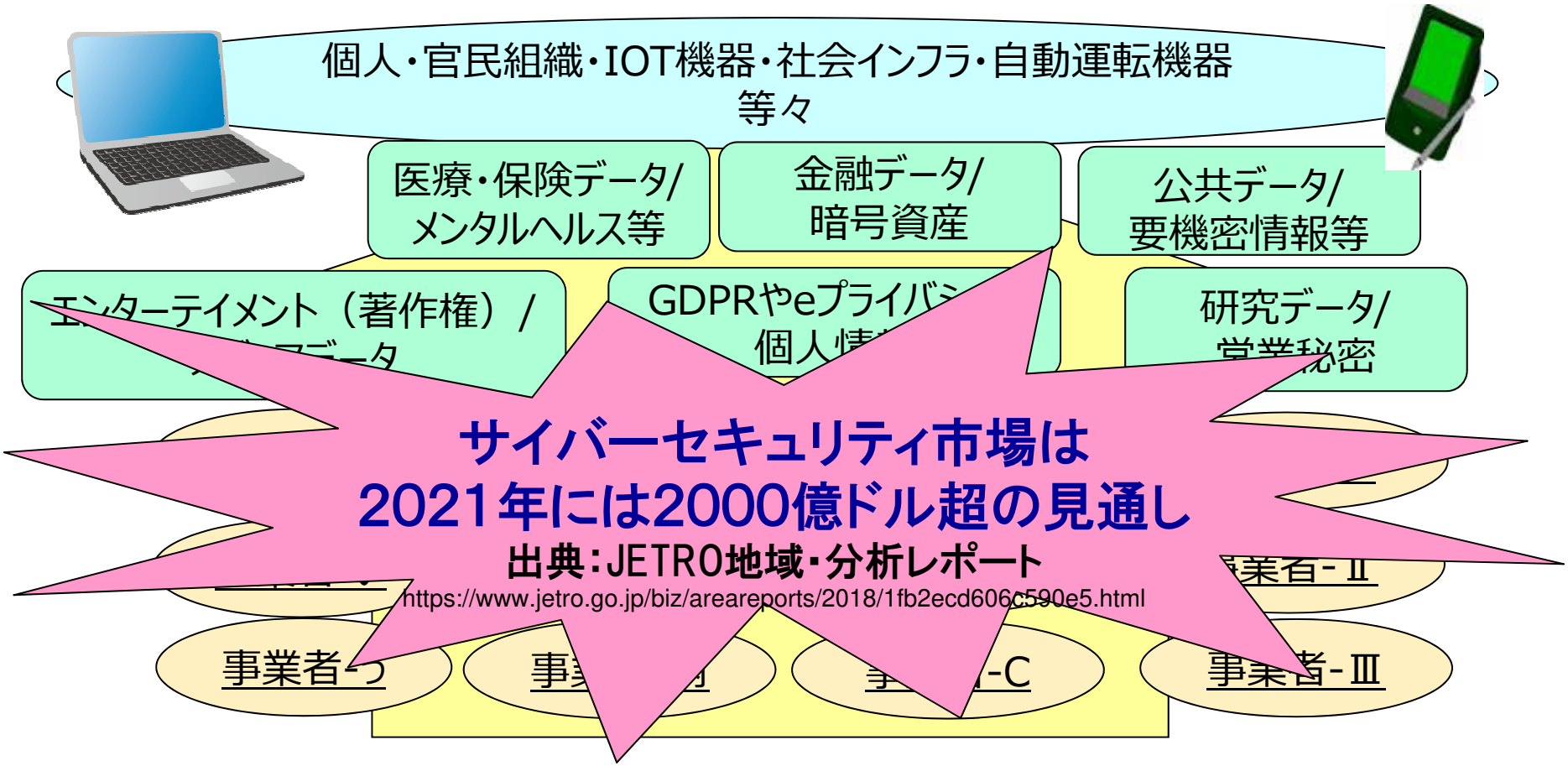
高度化・巧妙化・確信犯化した国際的攻撃者達は、ダークネットも悪用し政府機関や重要施設、民間企業等を含め、攻撃を行っている。国際的協調で犯罪者のボットネットワーク壊滅作成が展開されたが、完全な壊滅には至っていない。また、既存暗号技術では、AIや量子計算機が登場することによりGDPRや個人情報保護法等が求める長期間の情報資産の安全性確保ができない。GDPRの制裁金には損害賠償保険を利用できず企業個人を問わず巨大な損害が今後も発生することは容易に予測でき、世界的規模の重大な懸念事項。**パソコン→インターネット→AI・量子計算機→シンギュラリティ・・・**AI・テレワーク（現在）ワークスタイルやライフスタイルが変化する中で何が求められているのか。

安全・簡便・コストコンシャスな情報資産管理が必要

参考画像出典：
独立行政法人　情報通信研究機構　WEB公開パンフレット
https://www.nict.go.jp/data/pamphlet/index.html　他

巨大な経営リスク顕在化

個人情報等漏洩の賠償額等は高騰。GDPR制裁金は損害賠償保険が使えません。



参考：GDPR制裁金（民事訴訟は別）の試算。（制裁金が全世界売上の4%の場合そのまま）

ルフトハンザグループ　2016年の売上高は317億ユーロ≒約4兆円（1ユーロ＝128円）

4兆円＊0.04＝1600億円（年間）　https://www.lufthansa.com/mediapool/pdf/82/media_698850082.pdf

VISA 8.9兆ドル（年間売上：2016年12月末時点）≒約1000兆円（1ドル＝113円）

1000兆円＊0.04＝40兆円（年間）　http://www.vja.gr.jp/vja_about/visa_card.html

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

設　　立：1994年（平成6年）08月28日

資本金・決算：4233万円（2020年09月追加登記後）・12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

取得済維持特許：10案件

（維持中特許：日本9件、アメリカ1件）

一部共同出願含む（累計14カ国40件以上取得（EU、ユーラシアも1国とした）
但し即実施予定無いものは放棄）

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）

提携認証：TUVラインランドグループ

主要株主：保倉　豊、株式会社アイ･オー･データ機器、他146名

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/

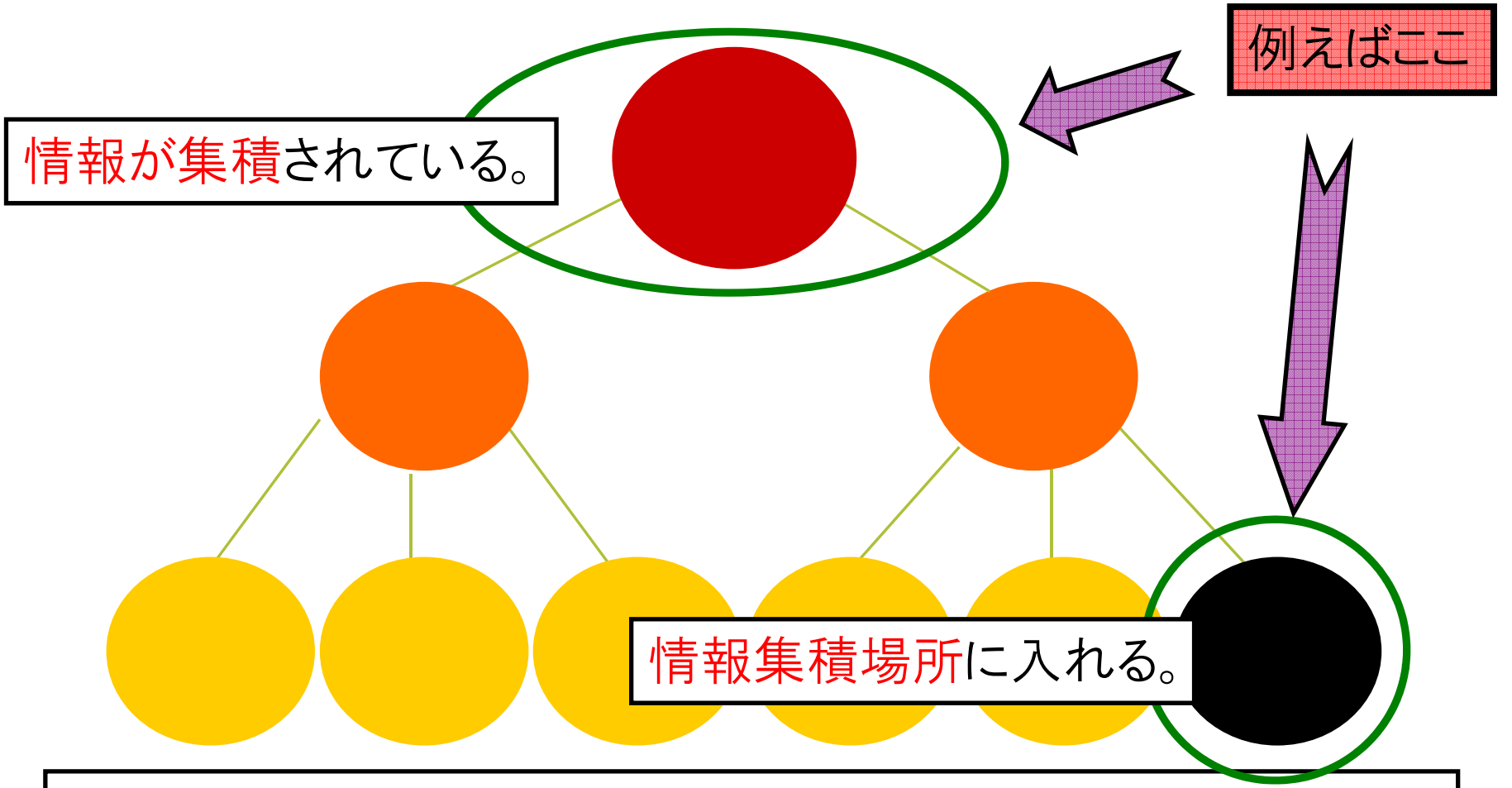
GFI

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

アジア グループ取締役副社長 K.K.ハインツ様 と GFI代表取締役社長 保倉豊
(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

現代IT環境の構造的課題

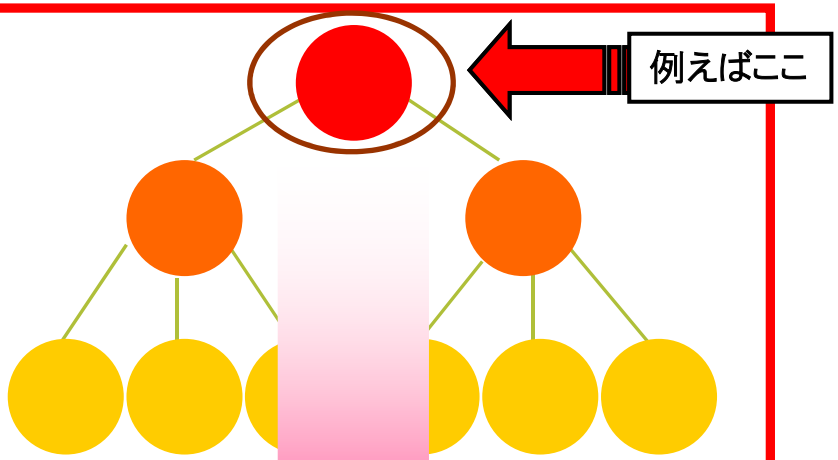


テレワーク端末等からネットワークの一か所に食い入ることで、
組織全体を攻撃し、情報資産を食い荒らす。
プライバシー侵害のみならず、反社会的活動資金源になることも。

割符利用の意義

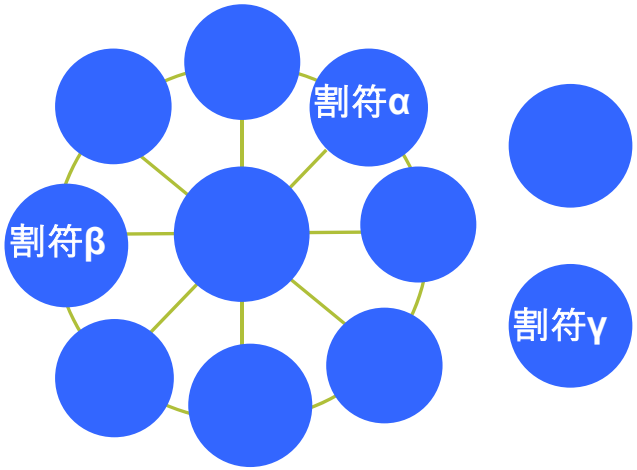
集約型情報管理モデル
―階層構造―

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、大きく
法令解釈上も不利



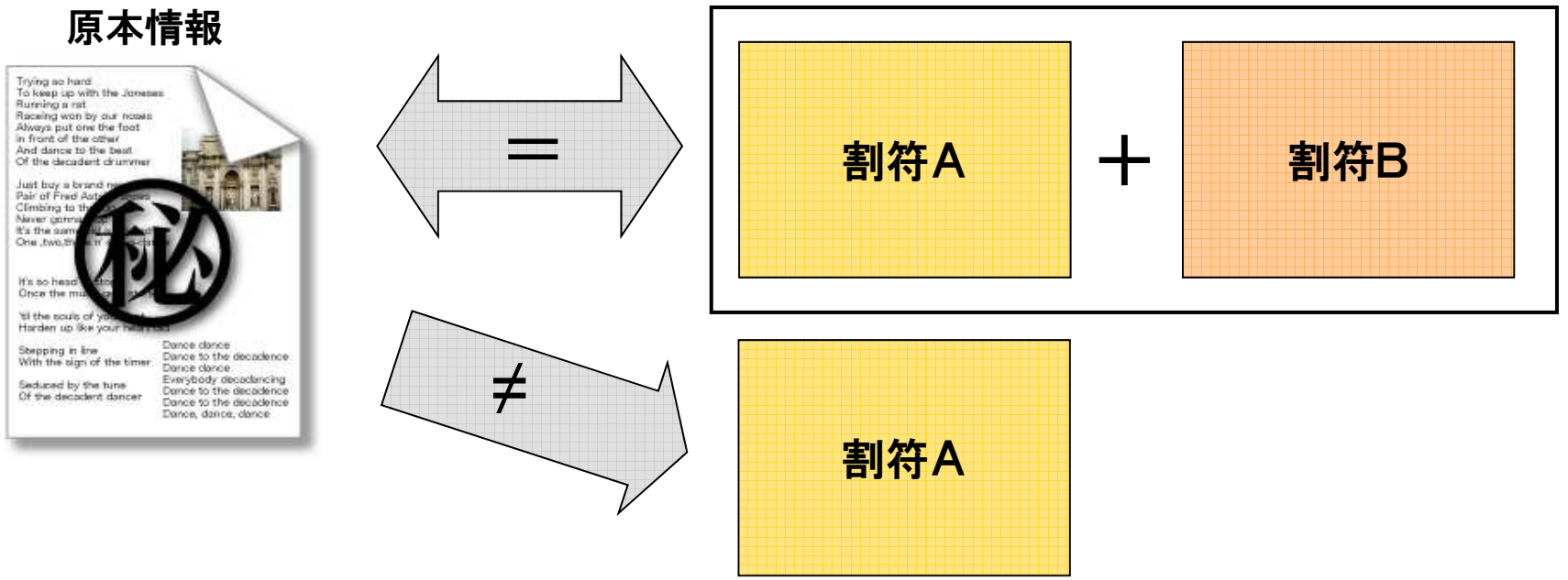
分散型情報管理モデル
―水平構造―

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く
法令解釈上も有利
これからの時代の情報社会基盤となる



GFI電子割符®

デジタル原本情報を独自技術を用いて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。

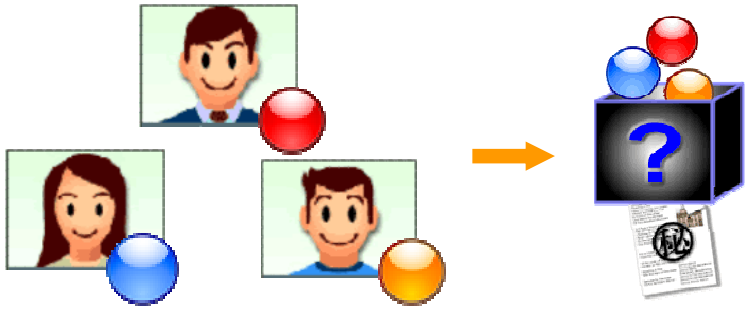


データ移送、保管等で重要情報の安全管理に利活用できます（＊1）。

（＊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

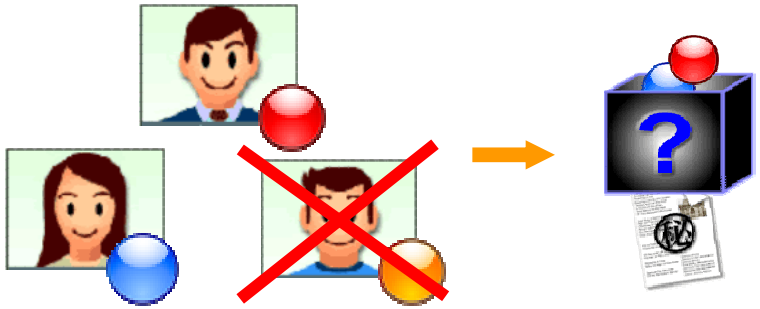
弊社電子割符の基本機能

（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。
（n,n型、AONT理論と極めて近い特性）

（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。
（k,n型、2つロスまで対応を標準機能として実装）

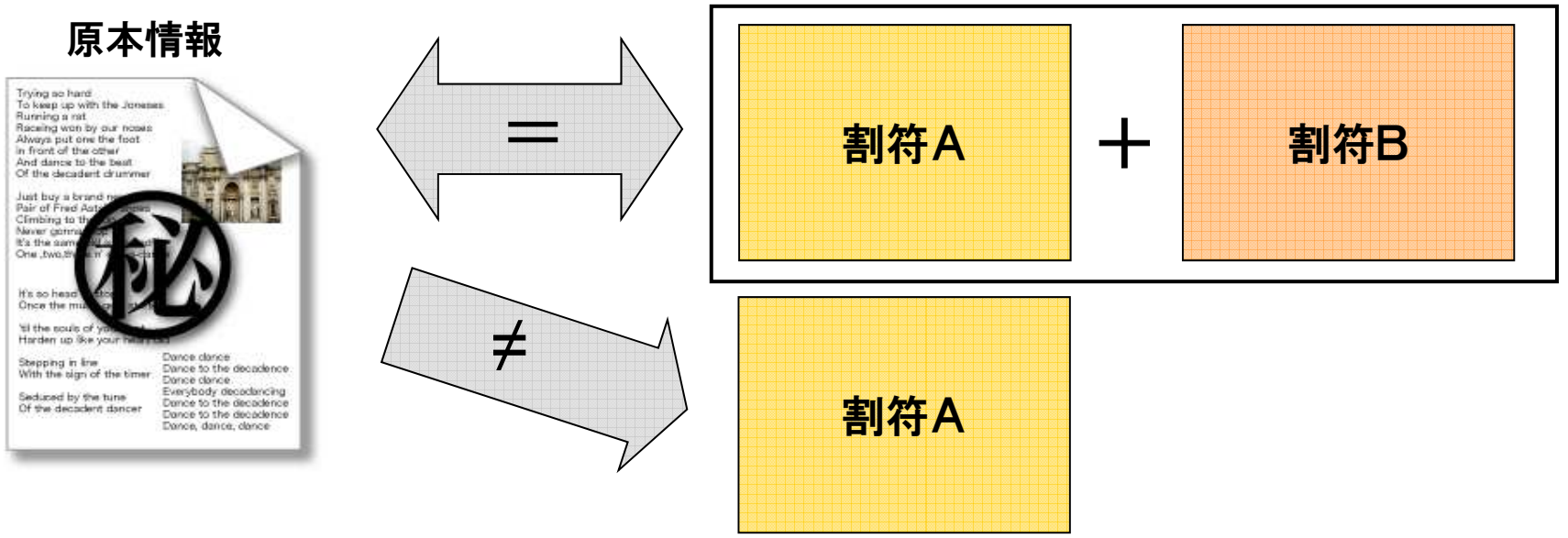
（3）最小化モード－生成する一つの割符サイズを小さくできます。
・特にn,n型は、**Pro V3版から自由度が大きくなりました。**

（4）自己認証機能－復元する際の条件設定ができます。

（5）Win,Linux,Mac(iOS)の各OS版（32bit,64bit）があり、相互にデータ互換しています。
＊通常ライブラリの分割数は2～10までです。

GFI電子割符®とAONTの関係

産総研様の「GFI電子割符(R)の安全性評価について」の調査報告の際、
一部の割符の不足も許さない割符生成の場合、GFI電子割符®はAONT理論に極めて近い特性を持つので、AONTの特性を踏まえた報告をしようかと打診ありましたが、



弊社技術は安全性を落とさずに(k,n)型の機能も保有しているため、利用者様の錯誤を未然防止すべく、AONT理論の特性を持つ記述は削除いただきました。
仮にAONT理論を安全性背景に持つ場合で、ファイル消失等に対し、
リカバリー可能とするには、AONT理論の想定外の分割ファイルのコピー保存等を行なう実装が必要で、そこにセキュリティリスクが発生することが予見できます。
厳格なn,n型に加え安全なリカバリーも可能な、GFI電子割符®をご利用ください。

弊社秘密分散技術外部評価概要

東京大学

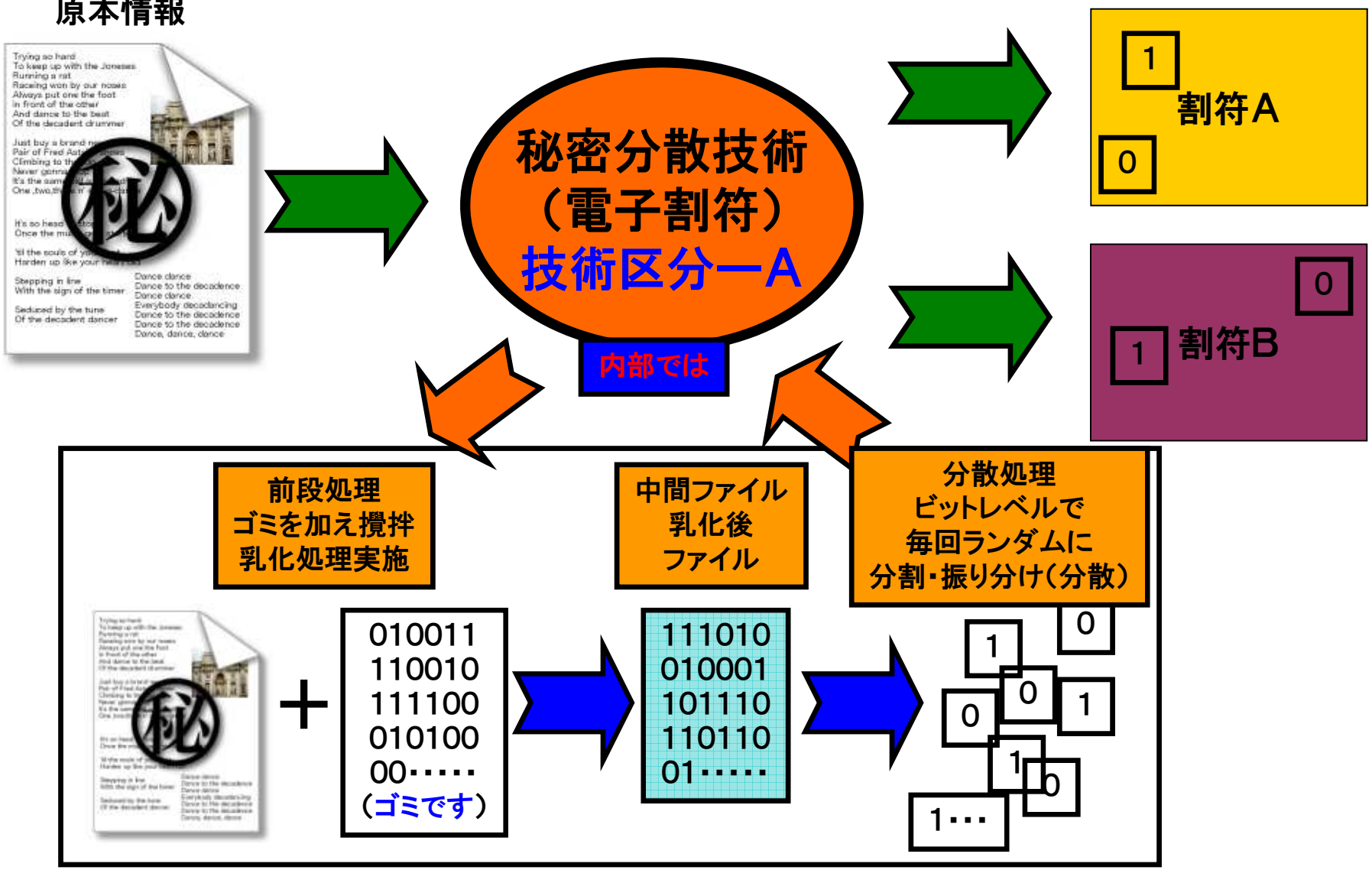
電子割符セキュリティ強度調査報告書　2001年12月20日
電子割符は、秘密情報を分割して安全に伝送（または記録）する目的に開発された符号化法（およびそれを実現するためのソフトウエア）である。秘密情報である平文Sをn個の割符に分割符号化し、n個の割符が全部そろえば、平文Sが複合できるが、n-1個以下の割符からは平文Sの情報が漏れないように工夫されている。（注：通常非公開資料）

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

GFI電子割符技術処理概要



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
（理論上必ず鍵は存在します）

暗号化ファイル
分割片A

少なくともいずれかの分割片には
個人特定できるだけの情報量がある
と考えられ暗号化部分が
解読されるリスクが存在する。

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。

弊社電子割符技術の特性

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			○

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。
（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

主要実績

公共系：

総務省、経済産業省、一般財団法人、自治体、日本赤十字社、等

民間系

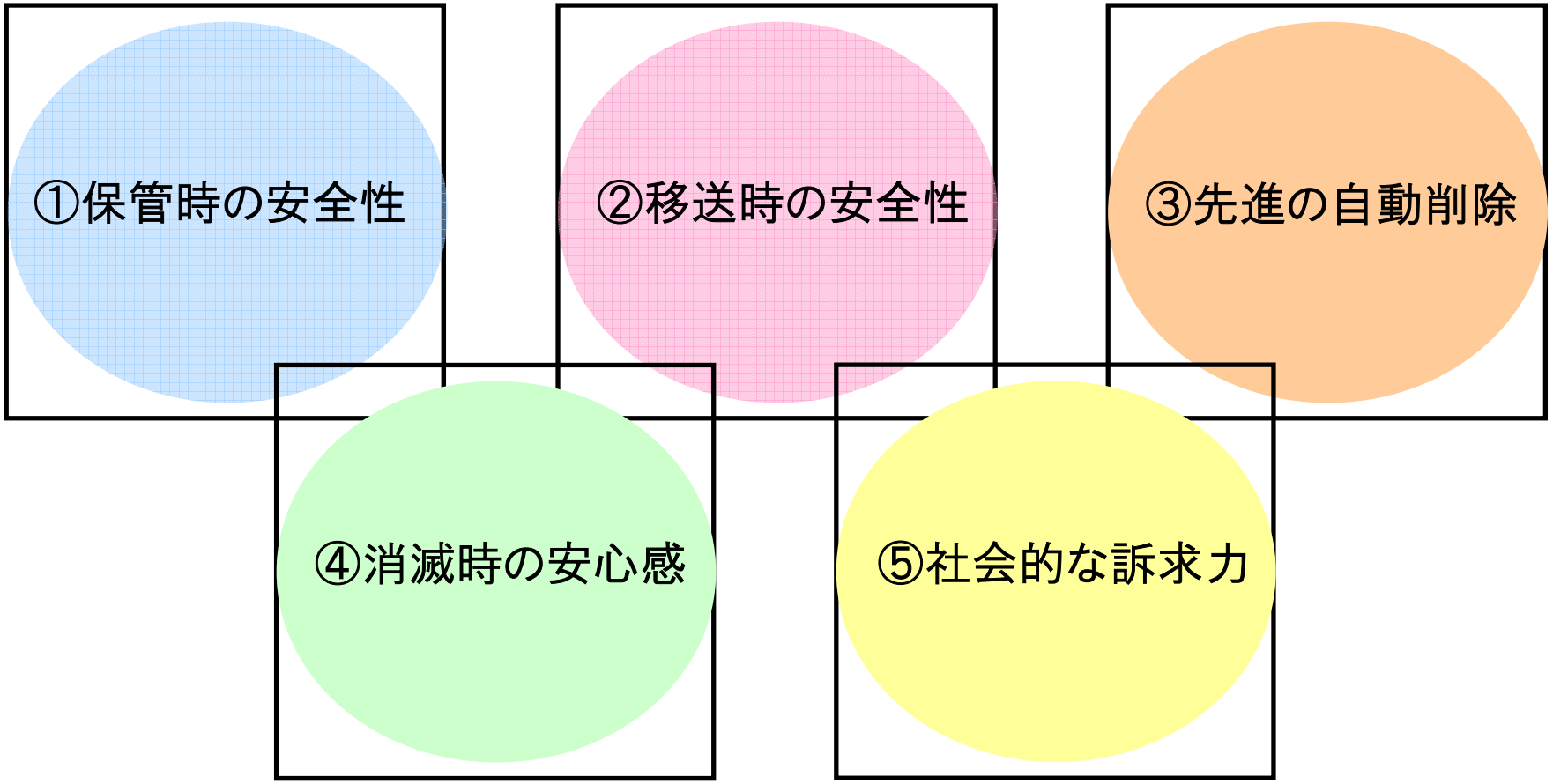
株式会社アイ・オー・データ機器
エヌ・アール・アイセキュアテクノロジーズ株式会社
寿精版印刷株式会社
新日鉄住金ソリューションズ株式会社
凸版印刷株式会社
株式会社日立製作所、株式会社日立ソリューションズ・クリエイト
三井物産セキュアディレクション株式会社、他

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。
弊社技術は、代表的秘密分散技術として公的報告書（＊3）で報告されています。

（＊3）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

電子割符5つの安全・安心

弊社取得済特許利用



①情報資産を割符化して保管した際の原理的特性に起因する秘匿安全性
②割符ファイル移送時に万が一盗難されたとしても訴訟に至らないという法解釈優位性
③端末等盗難や紛失時には割符自動削除を行い原本情報が露呈しない高過失耐性
④クラウドデータ消失やメモリー破壊、誤消去に対し原本復元可能な情報消滅耐性
⑤市民が安全性を容易に理解し、社会的合意が得られやすいという広範な社会合意性

注1：有識者各位評価全文についてご関心のある方は、GFIまでお問合せください。
注2：本資料及び評価等は、あくまでGFI電子割符(R)に実装された技術処理による特性を根拠とするものです。

参考：秘密分散技術の記述入りNISC資料記述部一例

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。

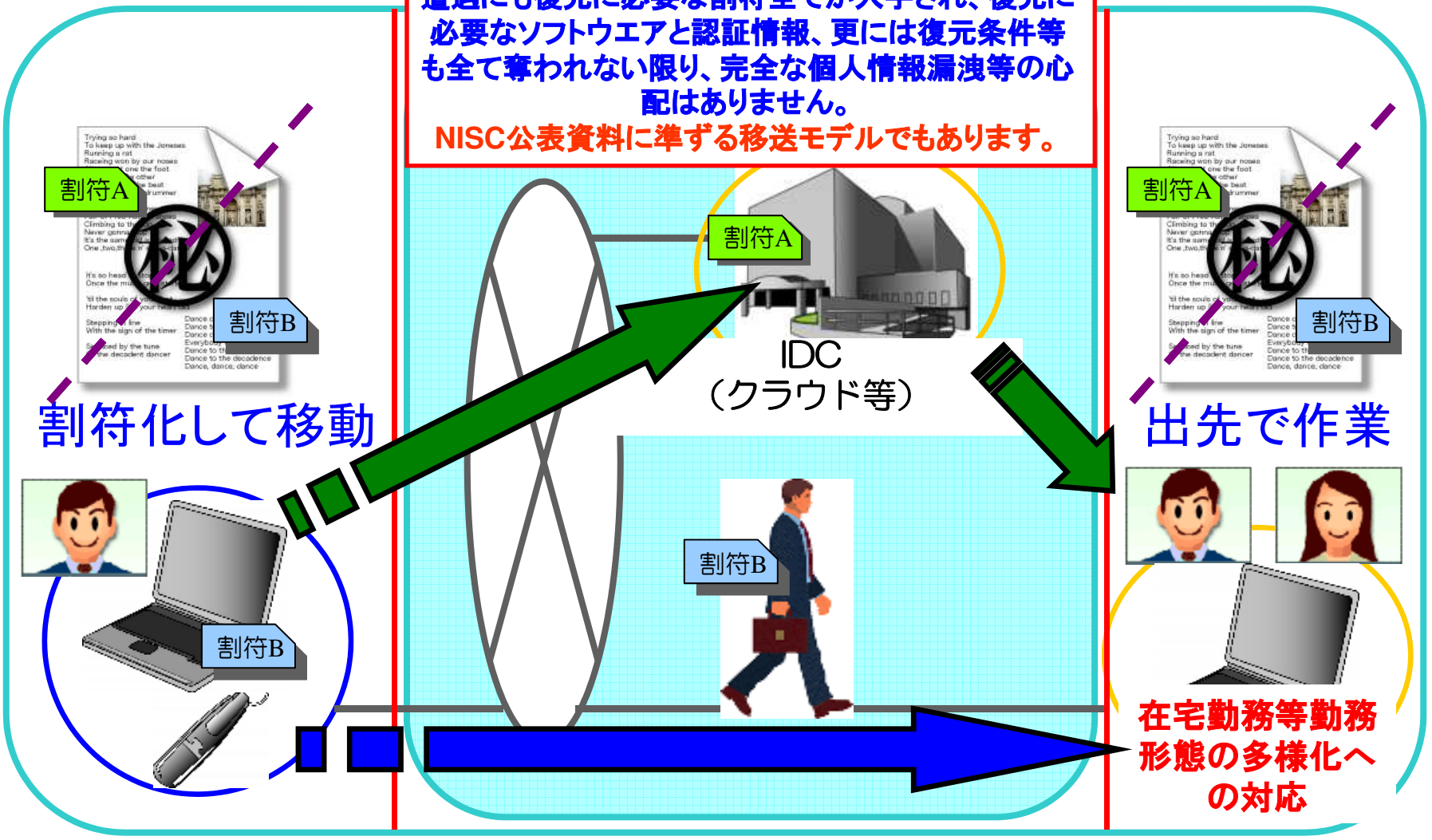
◎上記の内容は、記述の簡素化等はあるが「政府機関等の対策基準策定のためのガイドライン(平成30年度版)平成30年7月25日内閣官房 内閣サイバーセキュリティセンター」でも、要機密情報の運搬・移送の項で継続して記載されている。
出典：内閣サイバーセキュリティセンター 主要公表資料 https://www.nisc.go.jp/materials/
政府機関等の対策基準策定のためのガイドライン(平成30年度版) https://www.nisc.go.jp/active/general/pdf/guide30.pdf

参考：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。

参考：データ移送・持ち出し・出先作業

前述NISC情報の移送
利用モデル

移送中個々の割符そのもの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、更には復元条件等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。



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。」