



お客様各位

25年間の市場供給実績データセキュリティ技術  
弊社概要とGFI電子割符®  
—電子情報をビットレベルで部分集合化—

2024年01月29日  
グローバルフレンドシップ株式会社

注: GFI電子割符®に関する基本的な説明は別資料となっております。  
ご不明な点のご質問や他社類似技術利用してのお困りごと等ありましたら、遠慮なく弊社までお問い合わせください。

# GFIのISMS取得事例

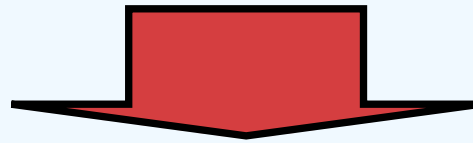


下記の図は、GFIがTUVと提携したきっかけとなった、ISMS取得時の情報管理の概念です。組織内情報資産をGFI電子割符®で処理し、適切に管理することで、経営リスクを軽減。（本社移転による再取得準備中）

重要な情報資産を“丸ごと存在”させない  
全く新しい技術で機密情報を守ります



世界的な情報資産管理厳格化の潮流の中で、企業の情報セキュリティ対策を高度化することが強く求められ罰則も強化されています。経営陣の皆様には市場調達可能な対策のうち、最善の手段等を選択し・組織導入していくことが経営責任として求められます。



## 「GFI電子割符®導入のメリット」

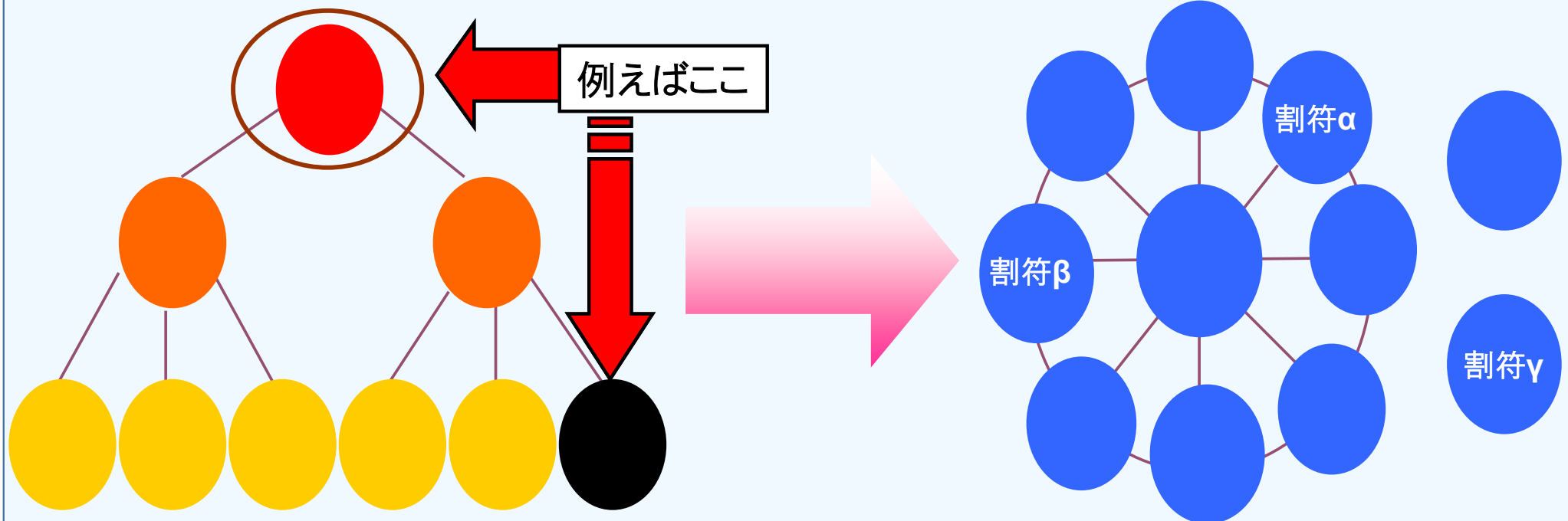
- ①情報資産を「割符化」し実害ゼロ、訴訟リスク最小化
- ②対策決定時の経営陣退任後の訴訟リスクを軽減
- ③異なるセキュリティ技術との高度な多層防御連携が可能
- ④現状利用安全対策にプラスすることで安全性強化
- ⑤サイバーリスク保険引き受けビジネスモデル限界への対策



## 影響の巨大な情報漏洩等の根源を断つ

情報漏洩等が発生する根源は、「そこに情報が存在するから」  
GFI電子割符®を用いて、「情報資産を存在させない」、「あったとしても復元できない数の割符だけ」にすることが、簡明且つ根本的解決策で、経営・管理部門や情シス負荷も軽減できます。

## 情報管理を集約型から分散型にシフトし管理責任も軽減





# 留意点・クラウドは万能ではない



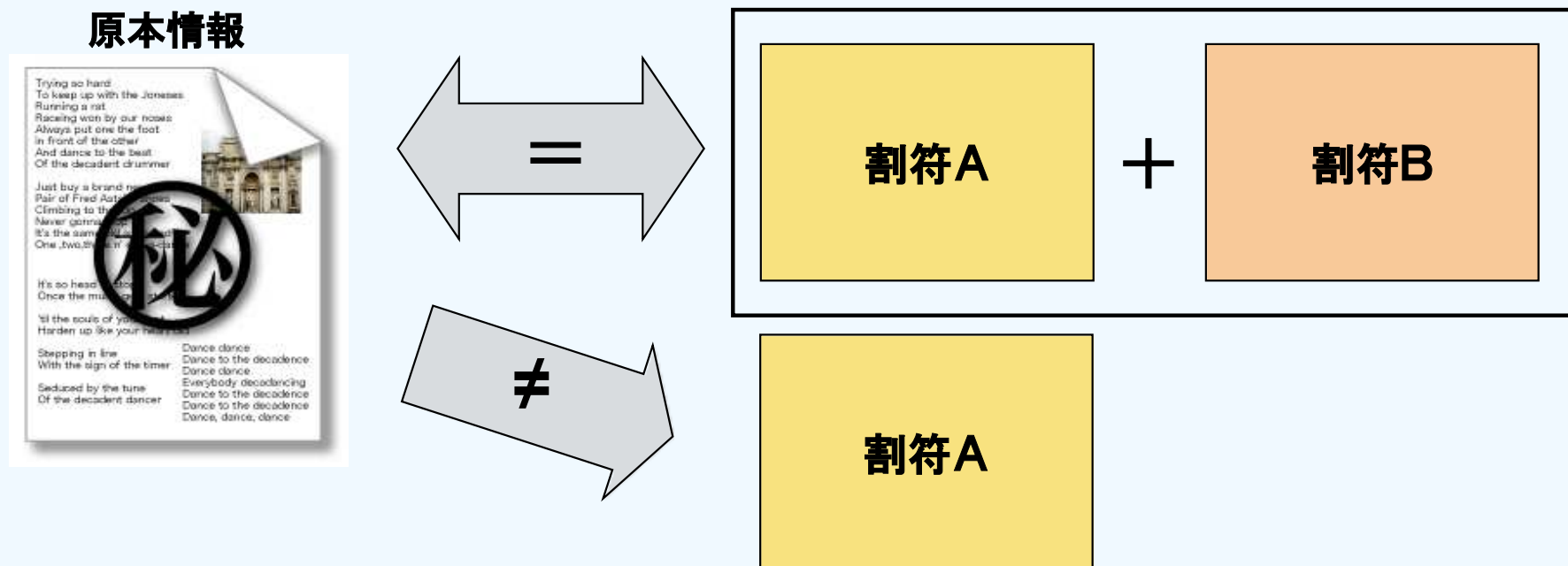
「政府のクラウド バイ デフォルト(ISMAP)」のポイント:

- ①クラウド事業者へ情報資産を預ければ本当に安心ですか
- ②IDや暗号鍵管理は万全ですか
- ③データ管理責任は、利用者にあります

出典: ISMAP管理基準マニュアル 令和3年7月12日 ISMAP 運用支援機関 公開資料より

# GFI電子割符<sup>®</sup>とは

データの種別を問わずデジタル原本情報をビットレベルで分割し、  
 毎回異なる振分けを行い割符を生成することで、**流出しても**  
 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。



**実務時には**復元に必要な割符から原本情報を復元できます。

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)と、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(令和5年度版)(要機密情報移送・運搬時に秘密分散技術利用)

<https://www.nisc.go.jp/pdf/policy/general/guider5.pdf>

# 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ェア)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。(中略)これは、一般に秘密分散法(Secret Sharing Scheme)として知られる方式の特殊な場合と考えることができる。

## 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、十分な**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。

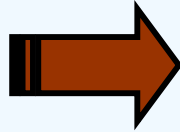
参考:「産総研様との共同研究の第二期結果概要報告」,[2015.12.26]  
[http://www.gfi.co.jp/01news20151226\\_393.html](http://www.gfi.co.jp/01news20151226_393.html)



# GFI電子割符<sup>®</sup>技術の概念図

ビット分散式電子割符技術の基本概念:

対象電子情報

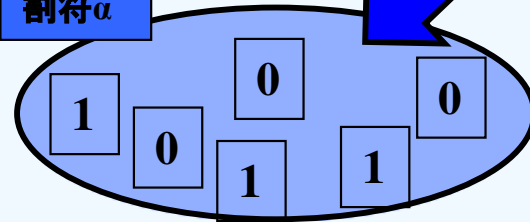


0 1 1 0 10110110111101100101001101001011101110...

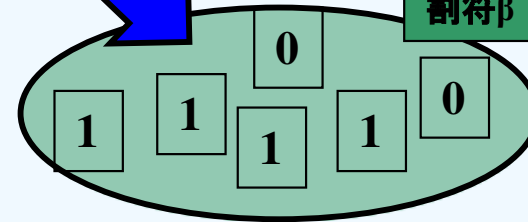
ビットレベルで分割しランダムに分散処理を行い割符ファイル生成

代表的  
秘密分散技術  
(GFI電子割符<sup>®</sup>)

割符 $\alpha$



割符 $\beta$



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、法令解釈上も個人情報とは看做されません

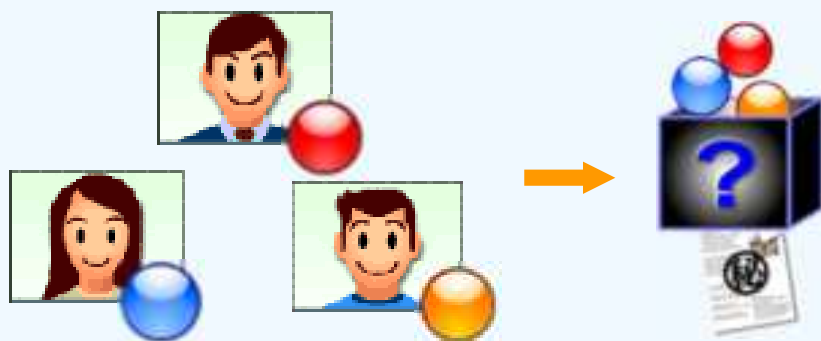
ポイント:

- ①未入手部分は計算では特定できない
- ②事実上情報理論的安全性をすでに持っている
- ③量子計算機の暗号解読が一番苦手とする技術
- ④唯一25年間商用安定動作と複数回外部評価

# GFI電子割符®の基本機能

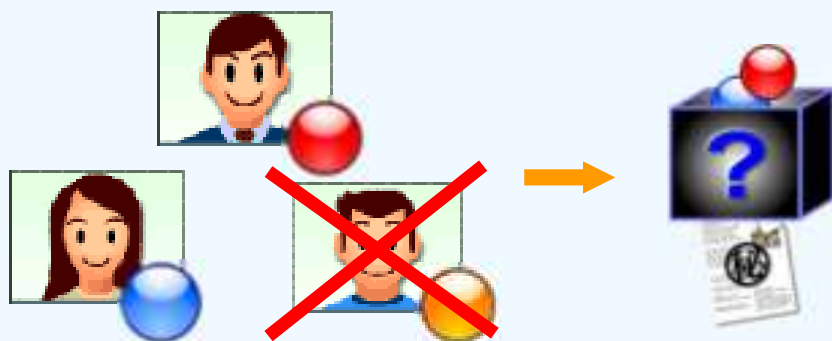


## (1)通常モード(分散管理・完全秘密分散型)



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対応・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。

注:通常ライブラリの分割数は2~10までです。

# 暗号技術と電子割符比較表

| 管理手法<br>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日経済産業省確認一注: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(\*)

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。**

(\*) 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 <https://www.jpdec.or.jp/archives/publications/J0004291.pdf>

## 公表可能な弊社電子割符技術(技術区分一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-福岡県庁及び県下複数自治体等)
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. IJ様(経済産業省平成22年度産業技術研究開発委託費)
6. 総務省(H22年度実施 地域ICT利活用広域連携事業 ICT利用による在宅難病患者遠隔医療支援事業)
7. 国立保健医療科学院(平成24年入札案件)
8. JIPDEC割符事業(J2ETサービス)
9. 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](#))
10. 沖縄県庁入札案件、千葉県成田市役所他、公共機関等の案件等の開示制限事例も有り。

## 民間系

11. 株式会社アイ・オー・データ機器
12. 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
13. 凸版印刷株式会社
14. エヌ・アール・アイセキュアテクノロジーズ株式会社
15. 株式会社ソトシステムズ
16. 寿精版印刷株式会社
17. ファイブテクノロジー株式会社
18. 三井物産セキュアディレクション株式会社
19. オークシステム株式会社
20. 日鉄ソリューションズ株式会社(旧:新日鉄住金ソリューションズ株式会社)、他

弊社秘密分散技術(GFI電子割符®)は、1999年の市場リリース後200万のライセンス数を超えるご利用実績を持ちます。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、最近で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([http://www.gfi.co.jp/01news20201219\\_488.html](http://www.gfi.co.jp/01news20201219_488.html))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。

# IT系インシデント発生時の法的責任



## ・ 漏えい原因: SQLインジェクション攻撃に未対応

被告は[中略]その当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていたと認められる。[中略]

経済産業省は、平成18年2月20日、「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」と題する文書において、[中略]独立行政法人情報処理推進機構(以下「IPA」という。)が紹介するSQLインジェクション対策の措置を重点的に実施することを求める旨の注意喚起をしていたこと、IPAは、平成19年4月、「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」と題する文書において、ウェブアプリケーションに対する代表的な攻撃手法としてSQLインジェクション攻撃を挙げ[中略]SQLインジェクション対策をすることが必要である旨を明示していたことが認められ、これらの事実に照らすと、被告は、平成21年2月4日の本件システム発注契約締結時点において、本件データベースから顧客の個人情報~~が漏洩することを防止するために、~~SQLインジェクション対策として、バインド機構の使用又はエスケープ処理を施したプログラムを提供すべき債務を負っていたということが出来る。

→経産省・IPAが「対策をすることが必要である」

→その当時の技術水準→黙示的に合意され、債務となっていた

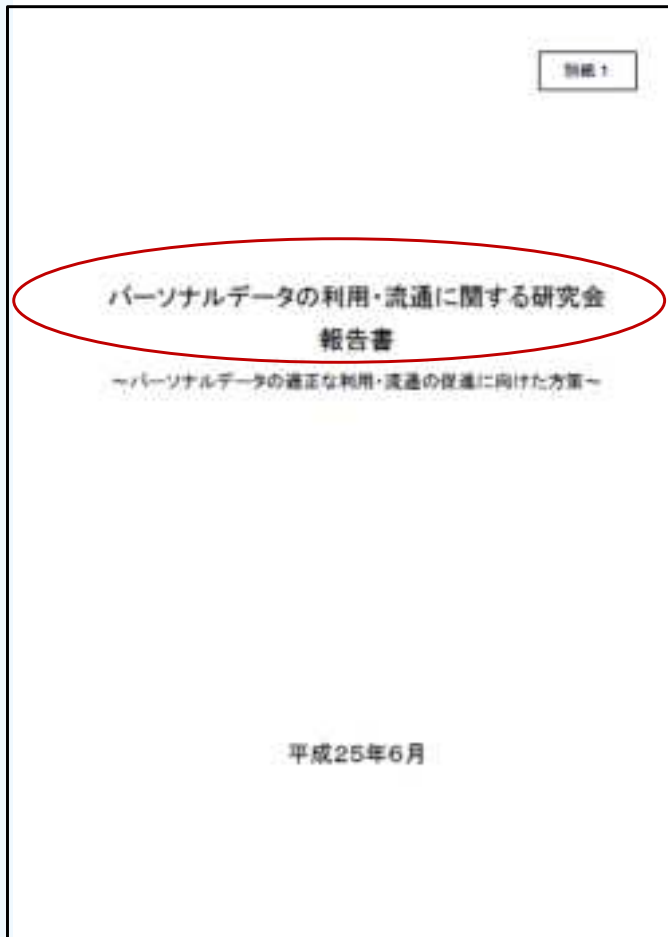
出典:株式会社割符サービス/グローバルフレンドシップ株式会社 2023年02月24日 電子割符オンラインセミナー  
牛島総合法律事務所 影島広泰弁護士 講演資料より



2013年「パーソナルデータの利用・流通に関する研究会報告」の関連記載

[https://www.soumu.go.jp/main\\_content/000231357.pdf](https://www.soumu.go.jp/main_content/000231357.pdf)

## 代表的秘密分散技術GFI電子割符®関連（事実上匿名化技術）



①GFI電子割符®関連：P.32 より

### 6. パーソナルデータの保護のための関連技術の活用

#### (1) 基本的な考え方

パーソナルデータの適正な利活用の促進のためには、プライバシーを保護するために利用可能な技術（プライバシー強化技術：Privacy Enhancing Technologies (PETs)）を最大限に有効活用することが適切である。他方、プライバシーを保護するために利用可能な技術に関しては、当該技術を適用することで、パーソナルデータの利活用に関するルールの遵守がどのように確保されることになるのかについて、具体的かつ分かりやすく説明していくことが必要である。

#### (2) 具体的な方向性

特に、情報理論的安全性を有する秘密分散技術を適用しているデータについて、復号するために必要となる数の分散データが漏えいしていないことが確実である場合には、漏えいしたデータを他の分散データと組み合わせ復号した場合に保護されるパーソナルデータとなるものが含まれているとしても、当該漏えいしたデータのみでは有意な情報がないことから、実質的影響はないものとして捉えることが可能である（68）。

解説：

（68）電気通信事業における個人情報保護に関するガイドライン第22条第1項第2項及びその解説参照。

出典：[https://www.soumu.go.jp/menu\\_news/s-news/01ryutsu02\\_02000071.html](https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000071.html)

総務省 「パーソナルデータの利用・流通に関する研究会」報告書の公表 平成25年6月25日

## 2023年「政府機関等の対策基準策定のためのガイドライン・令和5年度版」 25年安定動作実績を有する代表的秘密分散技術GFI電子割符®関連

GFI電子割符®関連：P.118 - 120 より

遵守事項 (6) 情報の運搬・送信 [基本対策事項]

<3.1.1(6)(b)関連> 3.1.1(6)-3 職員等は、**要機密情報**である電磁的記録を機関等外通信回線を使用して送信する場合には、以下を例とする情報漏えいを防止するための対策を講ずること。  
C) 分割後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて送信する。要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬又は送信する。

解説：

基本対策事項3.1.1(6)-2 b)、3.1.1(6)-2 C)  
「複数の情報に分割し」について

暗号技術の一種である秘密分散技術を用いて、秘匿すべき情報を複数のデータに分割することで、そのうちの一つを窃取しても元の情報を一切復元できないようにすることができる。この分割されたデータのそれぞれを異なる経路で運搬・送信する（例えば、片方を電子メールで送信し、もう片方をDVDやUSBメモリ等の外部電磁的記録媒体で郵送するなど）ことにより、**情報漏えいを防止することができる**。なお、秘密分散技術自体が暗号技術の一種であるので、これにより分割されたデータをさらに暗号化する必要はなく、暗号鍵も必要ない。

注：本記載はNISCからGFIへ情報セキュリティ対策にGFI電子割符®を用いたい。との相談があり様々な意見交換をしたことが発端。

現組織（内閣サイバーセキュリティセンター）が内閣官房情報セキュリティセンターとして発足して間もなく公開された**2005年政府機関の情報セキュリティ対策のための統一基準（2005年項目限定版）**解説資料時から継続され同様の趣旨で記述されている。以下は当時の文章。

【強化遵守事項】(d) 行政事務従事者は、要機密情報を移送する場合には、適切な強度の暗号化を行った上で、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。

出典：<https://www.nisc.go.jp/pdf/policy/general/guider5.pdf>

NISC（内閣サイバーセキュリティセンター）主要公表資料 2023年7月4日

### 政府機関関連

#### 2023年

- 2023年11月24日 政府機関等のサイバーセキュリティ対策のための統一基準に基づく情報セキュリティ監査の実施手引書(令和5年11月)
- 2023年07月04日 政府機関等のサイバーセキュリティ対策のための統一基準
- 2023年07月04日 政府機関等のサイバーセキュリティ対策のための統一基準(令和5年度版)
- 2023年07月04日 政府機関等の対策基準策定のためのガイドライン(令和5年度版)

#### 2022年

- 2022年10月25日 政府機関等のサイバーセキュリティ対策のための統一基準に基づく情報セキュリティ監査の実施手引書(令和4年10月)
- 2022年07月29日 情報システムに発生する被害軽減におけるセキュリティ要件策定マニュアル(5訂改版)

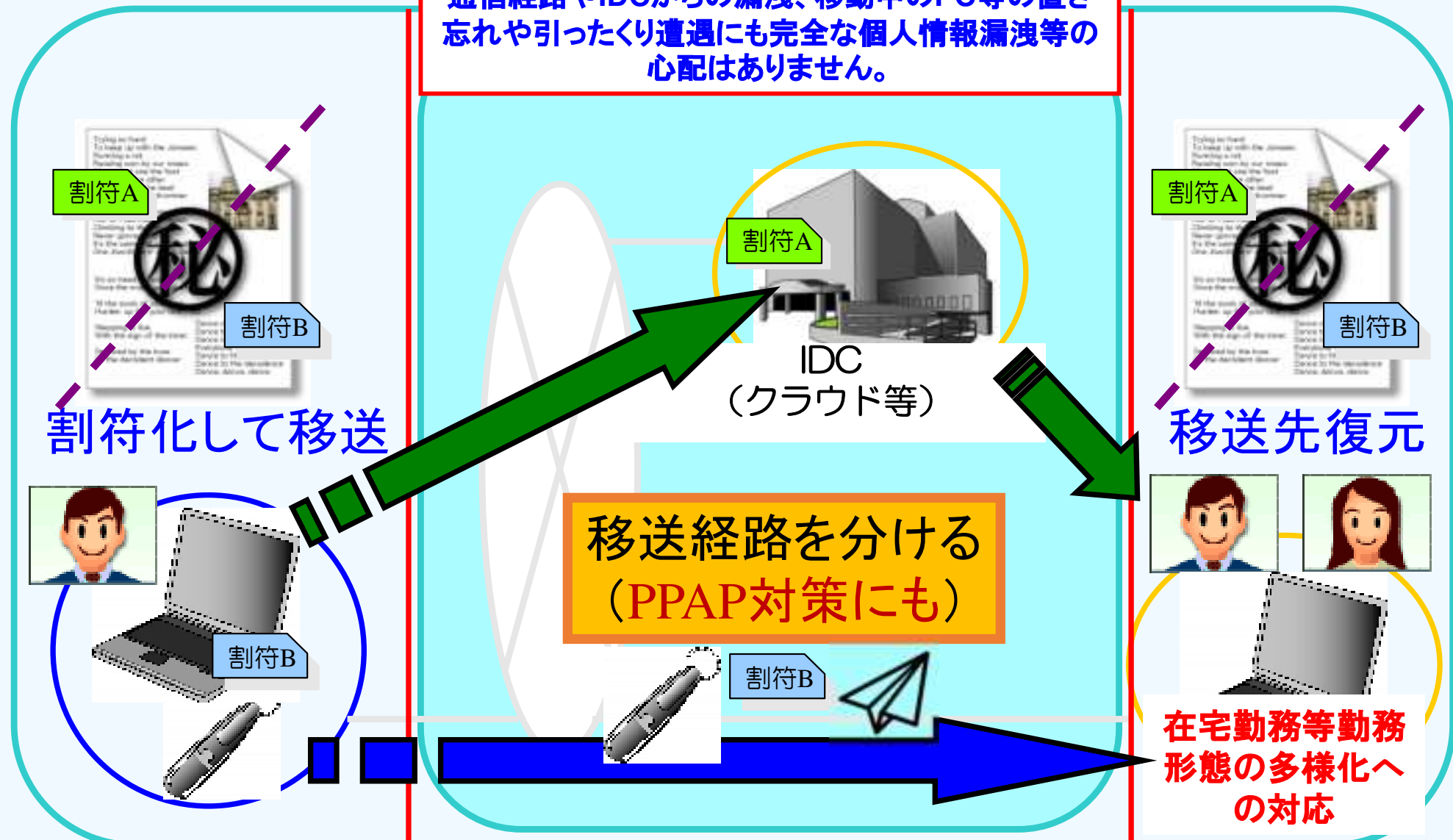
#### 2021年

- 2021年07月07日 政府機関等のサイバーセキュリティ対策のための統一基準
- 2021年07月07日 政府機関等のサイバーセキュリティ対策の運用等に関する指針
- 2021年07月07日 政府機関等のサイバーセキュリティ対策のための統一基準(令和3年度版)
- 2021年07月07日 政府機関等の対策基準策定のためのガイドライン(令和3年度版)
- 2021年07月07日 政府機関等のサイバーセキュリティ対策のための統一基準(令和3年度版) 解説編

# 要機密情報の移送にも電子割符

## 前述NISC要機密情報移送項記述内容準拠モデル

通信経路やIDCからの漏洩、移動中のPC等の置き忘れや引ったくり遭遇にも完全な個人情報漏洩等の心配はありません。



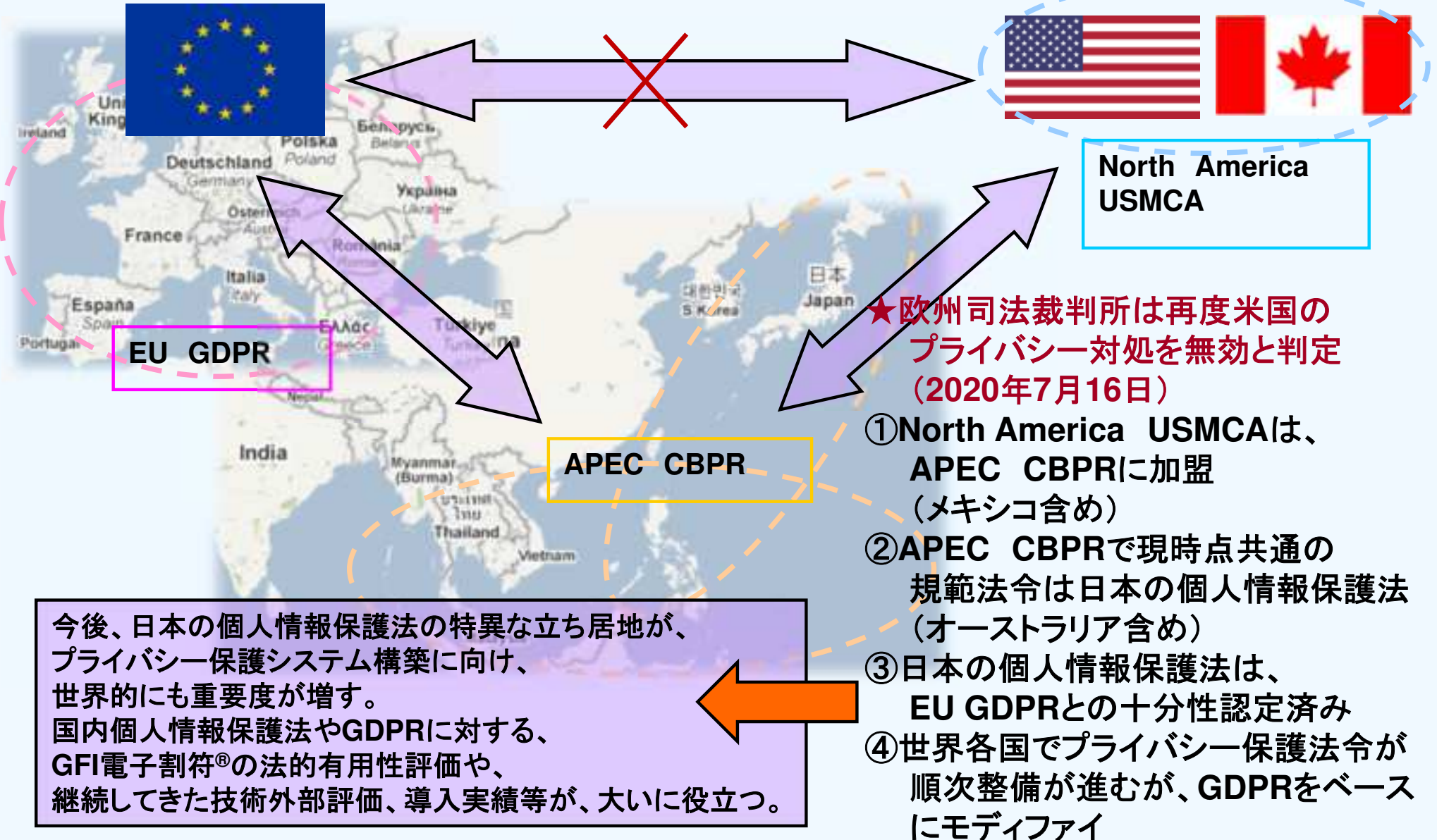




# 時代に最適なGFI電子割符®特性



今後の社会の最重要情報資産の一つは、個人情報である。  
下図は、情報資産のうち、プライバシーデータに関する現状と今後の相関図。





## EU GDPRの制裁金

**規則に違反した場合、最大2000万ユーロ又は前年売上・  
収入額の4%のいずれか高額な方の  
制裁金（上限）可能性**



グループ組織も含め前年度世界売上の4%を上限とした制裁金の規定が注目されるが、32条の他、24条、25条、30条、58条、83条、84条等も踏まえその制裁額は減額等の道筋があることが判る。



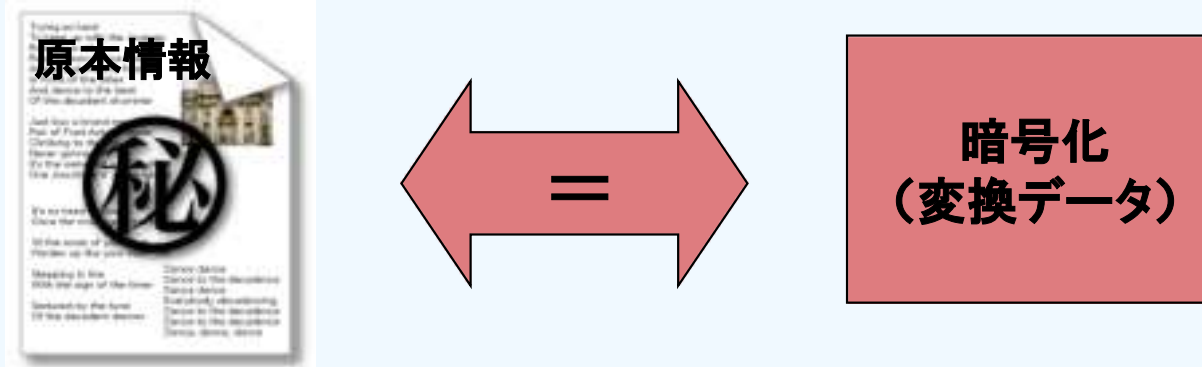
**採用・実施していた安全管理措置の内容を審査して制裁金判断**  
◎ 制裁金に保険は適用できない



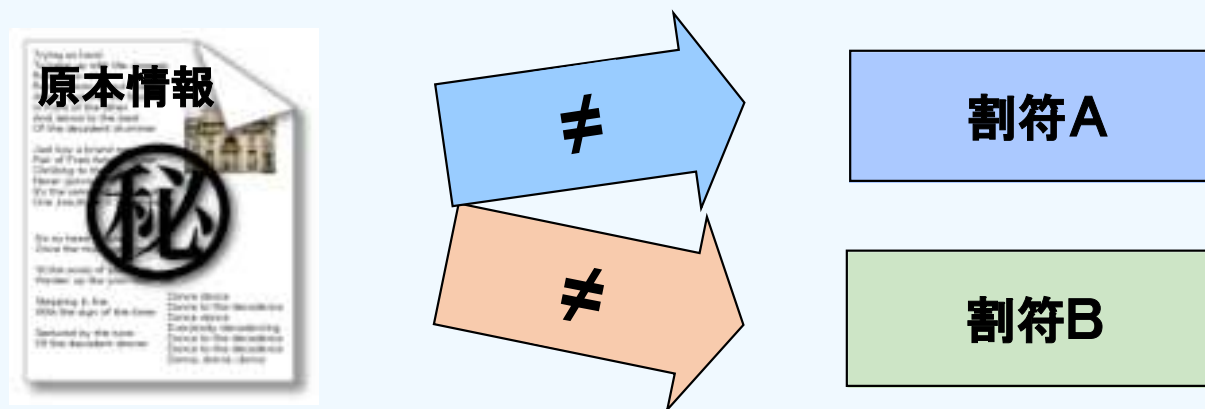
以上から、適切にGFI電子割符®技術や新たな電子割符実装サービスを用いることでGDPR制裁金の強い減免材料となる。そもそも制裁金対象とならない可能性もある

# 暗号化は最低限であり不十分

既存の暗号化技術は「集合論で言うことろの写像を作る処理」  
常に逆変換(復号・解読)可能性を持った状態と言えます



**GFI電子割符®**技術は、原本情報をビットレベルで分割し、  
毎回異なる振分けを行い割符を生成するので、  
「集合論でいうところの部分集合を生成する技術処理」



個々の割符ファイルだけでは原本情報を導き出せません

## 経営リスクとなる情報を割符化し漏洩等の禍根を断つ

割符化と任意の分散保管への格納処理は自動化されている



GFI e-Tally® Process



実務端末



## 必要な時は速やかに情報資産を復元

- ① Win端末のセキュリティ基本設定と一般的アンチウイルスアプリを入れます
  - ② ファイル移送経路及びクラウドでの万が一のファイル流出にも安全です
  - ③ GFI電子割符®技術実装アプリは、PC内の任意の情報資産の安全確保の割符化処理は自動化され任意の場所に保管し、必要時のみ復元します
  - ④: エンドポイントセキュリティAppGuard®を併用し不正プログラム対策も実施
  - ⑤ NTT東日本ワークストレージをクラウドとして利用することも可能
- \* GFIは東日本電信電話株式会社(NTT 東日本)紹介 パートナーです  
○システムとしてはブロックチェーンとの併用も可能です(ご相談ください)

## 基本セット: 高度なサイバー攻撃を受けること前提の対策

第1層: ハードやOS、アンチウイルス

第2層: App Guard® セキュリティ領域

第3層: GFI e-Tally® セキュリティ範囲

情報資産実体は割符化し**分散管理**  
一部消失等にもBCP対処可能

## 攻撃者に最後の一线を突破されても漏洩等はない



第1層:

まずはOSの推奨するセキュリティ機能と、市場で一定の評価を受けるアンチウイルス等のセキュリティ対策を実施。

第2層:

不正な動きをするプログラムの活動を検知し、その動きを制するセキュリティソフトウェアそれが、OSプロテクト型エンドポイントセキュリティ、AppGuard®です。

第3層:

攻撃者が最後の一线を突破しても、そこには何もない。又は単体では無意味な一部の割符ファイルしかない。安全性根拠の頃なる最後の切り札が、GFI電子割符®を実装した情報資産管理アプリ「割りふってますTM」です。

# クラウド利用安全対策比較表



|     | 管理責任<br>最小化         | 管理場所<br>自由度          | データ<br>安全性<br>データ回復<br>手段含め   | ポータ<br>ビリティ        | GDPRや<br>改正個人情報<br>保護法評価 | 当該<br>サービス<br>実績 |
|-----|---------------------|----------------------|-------------------------------|--------------------|--------------------------|------------------|
|     | 集中管理<br>なのか<br>分散管理 | データオ<br>ナー自由度<br>容易性 | 流出時損害<br>大小 <b>注1</b><br>コピー？ | 利用者<br>手間や<br>派生費用 | 市民目線で<br>高度に対応           | 国際市場<br>実績       |
| A社  | ×                   | ×                    | ×                             | △                  | △ <b>注2</b>              | ○                |
| B社  | ×                   | △                    | ×                             | △                  | △ <b>注2</b>              | ○                |
| GFI | ○                   | ○                    | ○                             | ○                  | ○                        | △ <b>注3</b>      |

注1：データ流出時の損害大小とデータ自身の消滅防止策がデータコピーに依存の場合流出リスク増加問題

注2：GDPRや改正個人情報保護法への対処策として理想的でないが現状サービスで暗号化で対処している

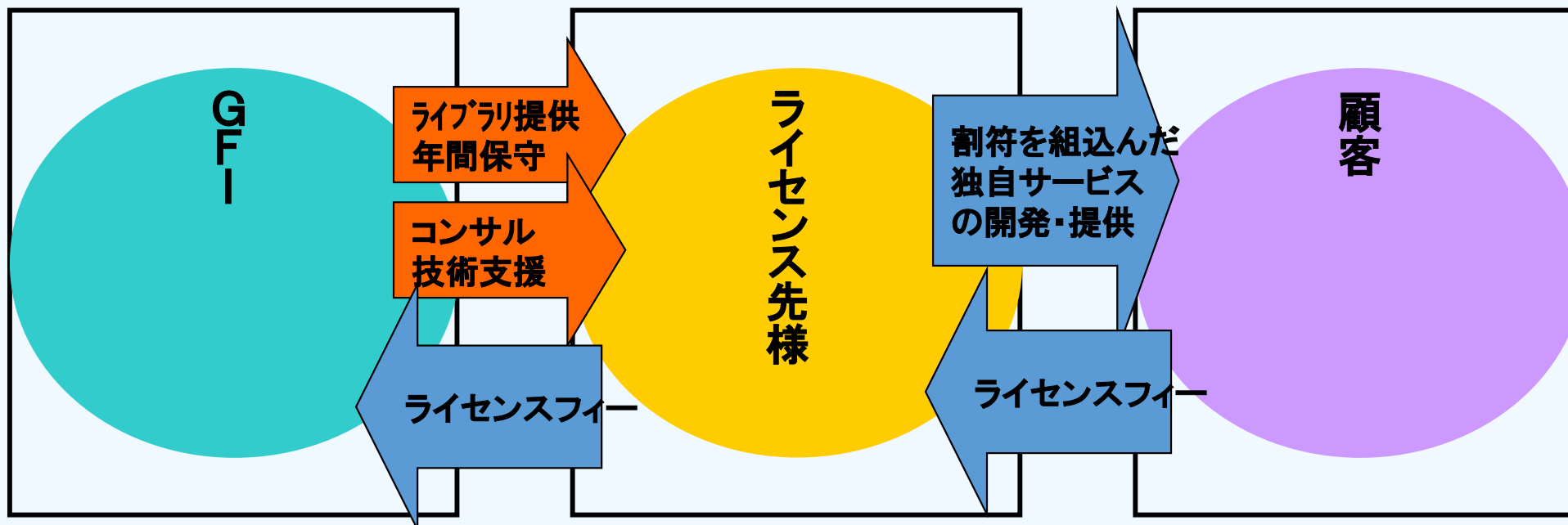
注3：GFIの事業やサービスは、内閣府や経済産業省との意見交換から国内を優先していた（国内向けあり）



# 電子割符ライセンスモデル概要



## 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](http://www.gfi.co.jp/01news20131007_328.html)

商品等開発(C、C++)ではなく、**実務等で早く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、弊社商品や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します。

# 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: 4294万円(2021年04月登記後)・12月

所在地: 東京都渋谷区笹塚1-32-2 ソネット笹塚102

役員: 代表取締役社長(CEO) 保倉 豊、CFO 大山文夫、EA 進藤公彦、他2名

取得済維持特許: 8案件(日本)

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、申請中案件は記載せず)

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)

参加団体: 一般財団法人日本情報経済社会推進協会(JIPDEC)

一般社団法人ソフトウェア協会(SAJ)

一般社団法人次世代センサ協議会(JASST)

独立行政法人日本貿易振興機構(JETRO)・新輸出大国コンソーシアム

防災DX官民共創協議会、仙台 BOSAI-TECH イノベーションプラットフォーム

スマートIoT推進フォーラム、未来共創イニシアチブ(弊社子会社で加盟)

提携認証: TUVラインランドグループ

認可等: 総務省届出電気通信事業者登録

主要株主: 保倉 豊、株式会社アイ・オー・データ機器、他代表を幼少時から知る人等146名

# 認証機関との提携認証



## 国際的観点

TUVラインランドグループ様と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。これは、GFIが自社内部情報を自社電子割符技術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。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文化の国際普及に相互協力します。



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

認証書授与式当日写真 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

関連参考:EU個人データ保護認証国内第一号は、当時弊社ライセンス先様による  
GFI電子割符®を用いた世界発の事例となりました。

<https://www.lexues.co.jp/press/590/>

※テュフラインランドグループは、グローバルに技術サービスを提供する世界有数の第三者認証機関です。

参考: <https://www.tuv.com/world/en/about-us/>

注:弊社本社移転により現在ISMS再取得準備中です。

# ベルギー王国大使館様との協議



## 国際的観点

ベルギー王国大使館様からの招待を受け、GFIは2020年02月05日大使館にてミーティングを実施。GFIやGFI電子割符に関連する事業のEU展開やEUからの世界展開について、様々な可能性等を意見交換しました。GFI電子割符®のGDPR有効性等に関しても同席したベルギー側弁護士からも非常にパワフルな技術であることのご意見を頂戴し、力強いベルギーへの誘致ご案内を受けました。大使館経由でEU本部の管轄部署の紹介や現地パートナー等の紹介、誘致企業への様々な優遇制度等のご案内も頂戴しました。現在コロナで直接訪問等はできておりませんが、継続して現地弁護士等と意見交換等をしており、弊社事業の国際展開におけるひとつの可能性を示すものです。



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

・2020年2月5日（水） 13:30の会議の後、Global Friendship Inc.

ベルギー大使館ロビーにて参加者一同を撮影。

写真左から、ダルデウオルフ弁護士事務所 ニコラ・ヘレマンス弁護士、同席通訳、同弁護士事務所  
ヴァランタン・ドウ・ル・クール弁護士、hub.brussels(ブリュッセル本部)アジア投資部門長  
ローラン・ヴァービスト様、ベルギー王国国旗、GFI代表保倉、ベルギー財務省 国際税務専門官  
ミケラ・ワンド様、ベルギー王国大使館 ブリュッセル首都圏政府貿易局 駐日代表部  
ウイリアム・デルセム代表



[gfi-info@gfi.co.jp](mailto: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。」