お客様各位

割符技術は既存暗号技術と相互補完関係です

GFI電子割符®活用のご案内

―経営リスク最小化システムの実現―

2022年09月20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。
ご不明な点やご質問等ありましたら、遠慮なく弊社までお問い合わせください。

エグゼクティブサマリ

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

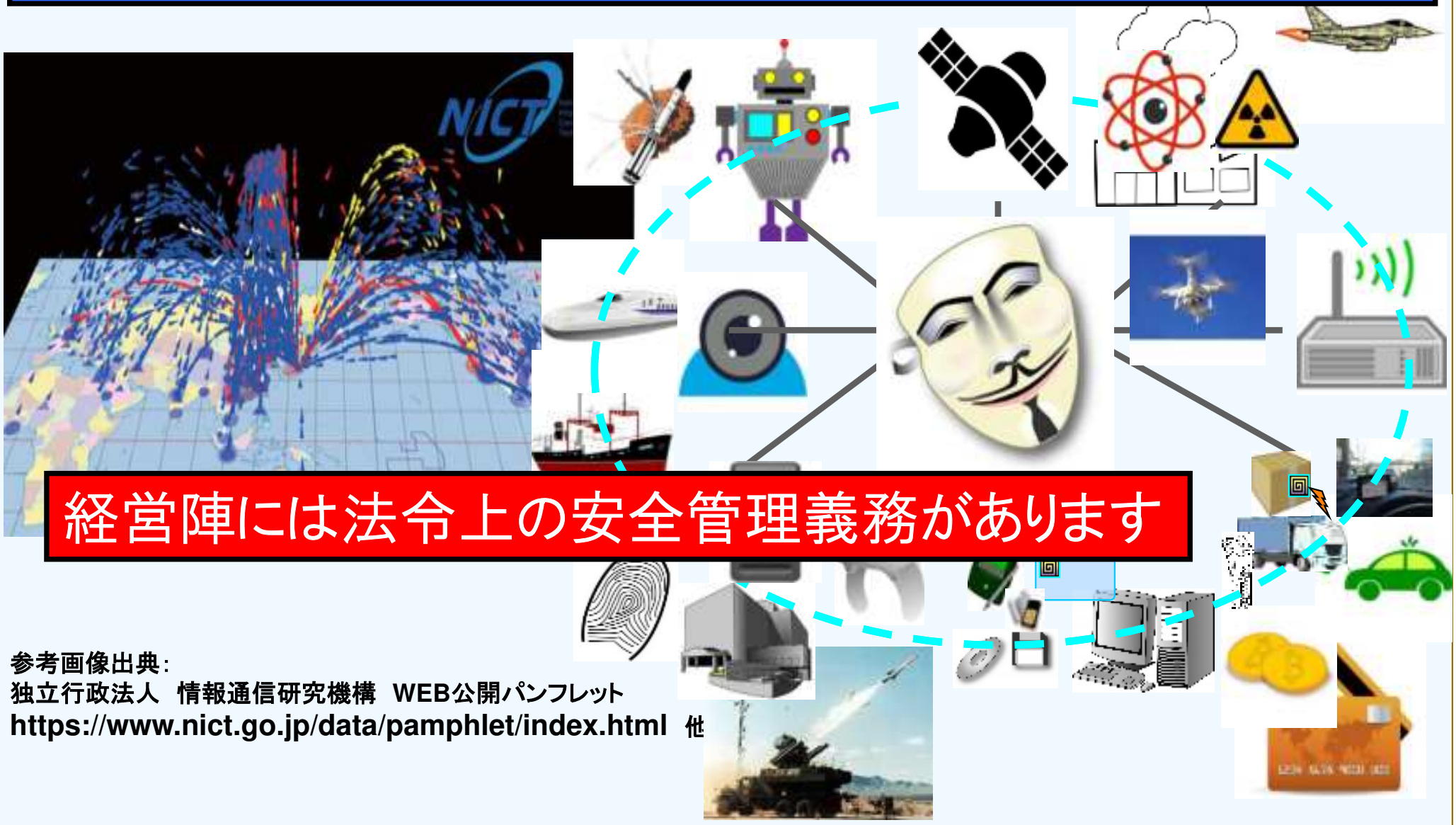
③異なるセキュリティ技術との高度な多層防御連携が可能

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

サイバー攻撃対策は世界的課題

安全・簡便・訴訟リスク最小化できる情報資産管理が必要



経営陣には法令上の安全管理義務があります

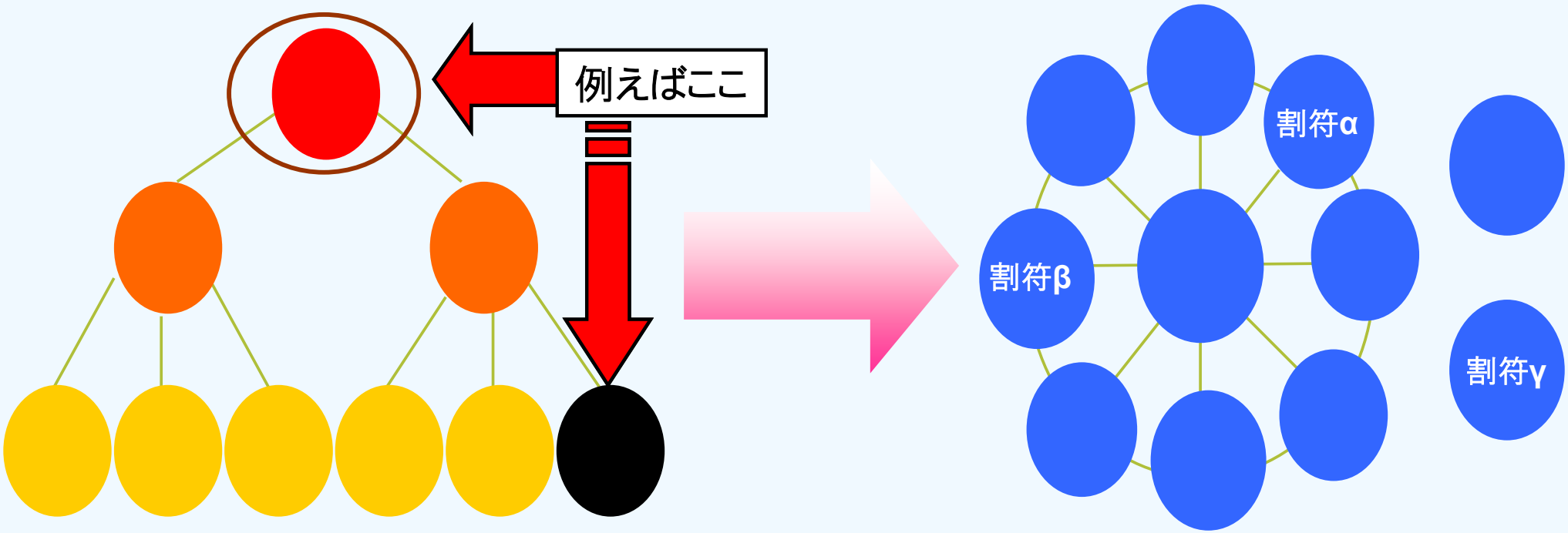
参考画像出典:
独立行政法人　情報通信研究機構　WEB公開パンフレット
https://www.nict.go.jp/data/pamphlet/index.html　他

情報セキュリティの根本的解決

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クラウド事業者に情報資産を預ければ本当に安心ですか

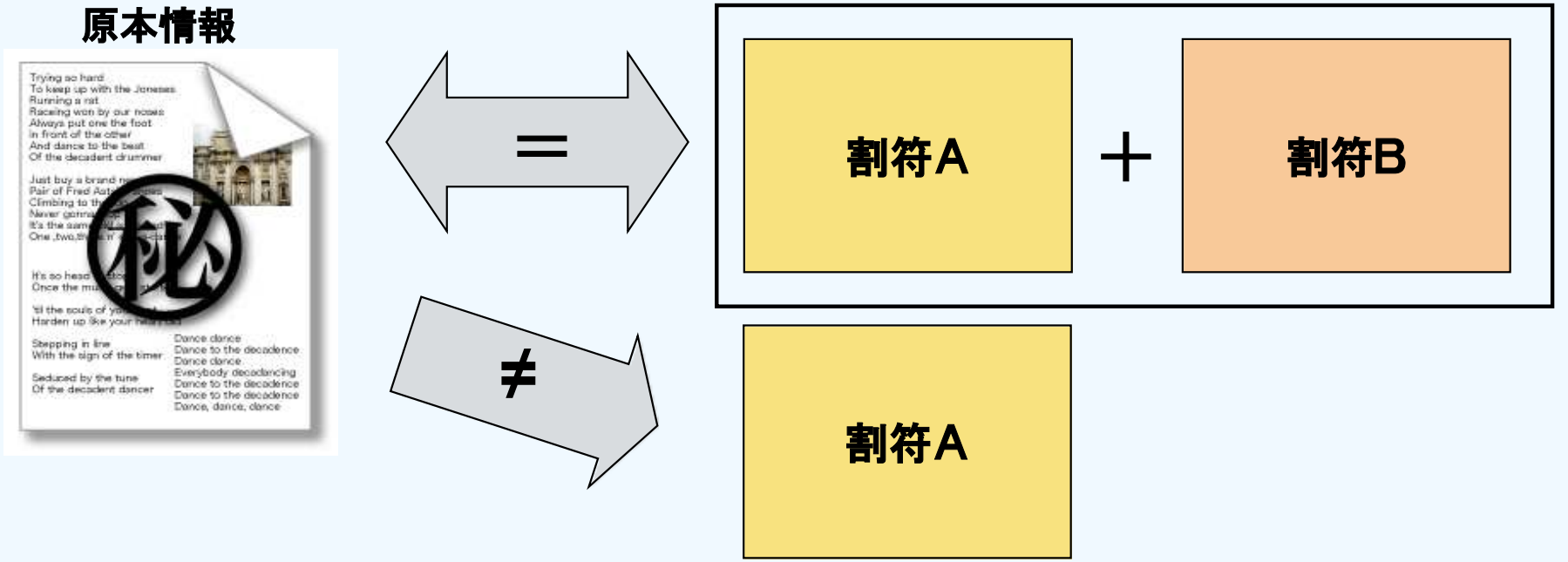
②IDや暗号鍵管理は万全ですか

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®とは

データの種類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。

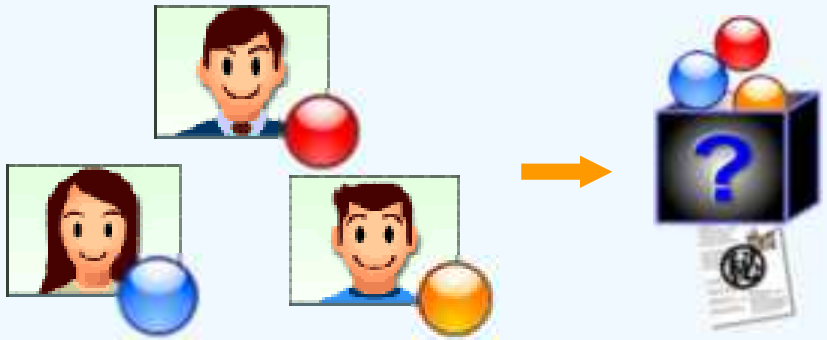


実務時には復元に必要な割符から原本情報を復元できます。

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3年度版)(要機密情報移送時の秘密分散技術利用)
https://www.nisc.go.jp/active/general/pdf/guider3.pdf

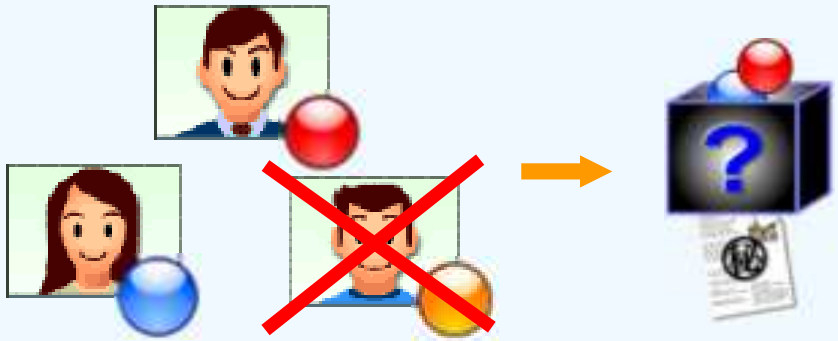
GFI電子割符®の基本機能

（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。

注：通常ライブラリの分割数は2～10までです。

弊社秘密分散技術外部評価概要

東京大学

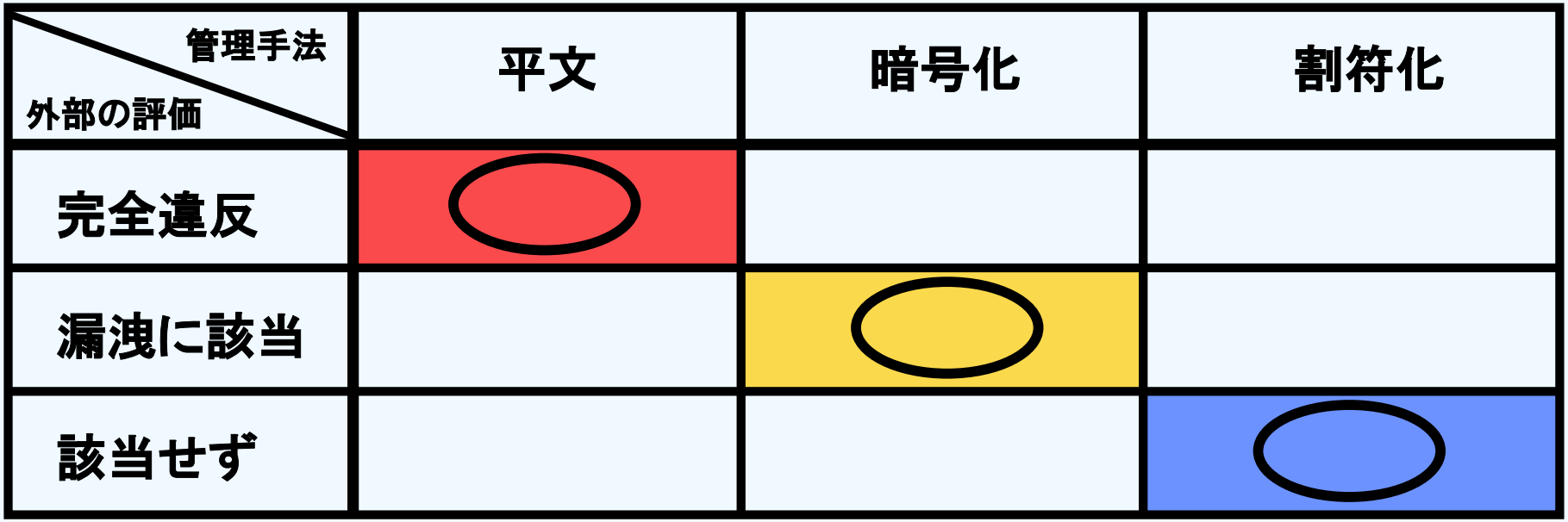
電子割符セキュリティ強度調査報告書　2001年12月20日
電子割符は、秘密情報を分割して安全に伝送（または記録）する目的に開発された符号化法（およびそれを実現するためのソフトウエア）である。秘密情報である平文Sをn個の割符に分割符号化し、n個の割符が全部そろえば、平文Sが複合できるが、n-1個以下の割符からは平文Sの情報が漏れないように工夫されている。（中略）これは、一般に秘密分散法（Secret Sharing Scheme）として知られる方式の特殊な場合と考えることができる。

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、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

暗号技術と電子割符比較表



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（＊）

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　http://www.jipdec.or.jp/archives/publications/J0004291

公開可能な採用実績等

公表可能な弊社電子割符技術(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. 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。

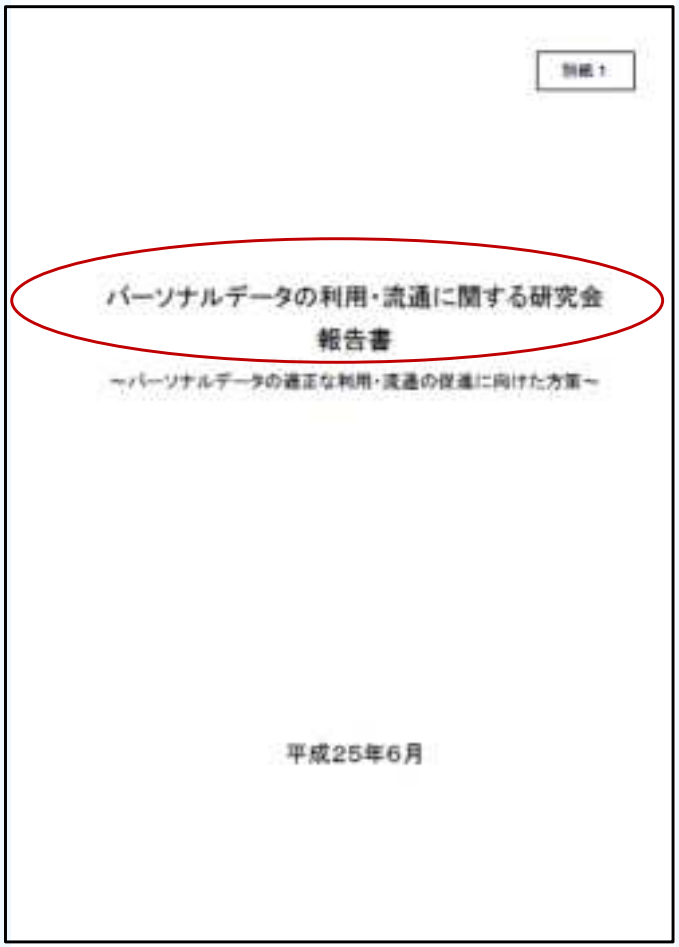
民間系

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. 株式会社ソリトンシステムズ
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)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。

総務省パーソナルデータ関連

「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
代表的秘密分散技術GFI電子割符®関連（事実上匿名化技術）


別紙1

パーソナルデータの利用・流通に関する研究会
報告書
～パーソナルデータの適正な利用・流通の促進に向けた方策～

平成25年6月

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

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

データ移送関連記載NISC資料

「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）」に準拠する

20年を超える実績を有する代表的秘密分散技術GFI電子割符®関連

①GFI電子割符®関連：P.97 - 98 より

3.1.1 情報の取扱い

<3.1.1(6)(a)(b)関連>

3.1.1(6)-2 職員等は、**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機関等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。

b)

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)「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。

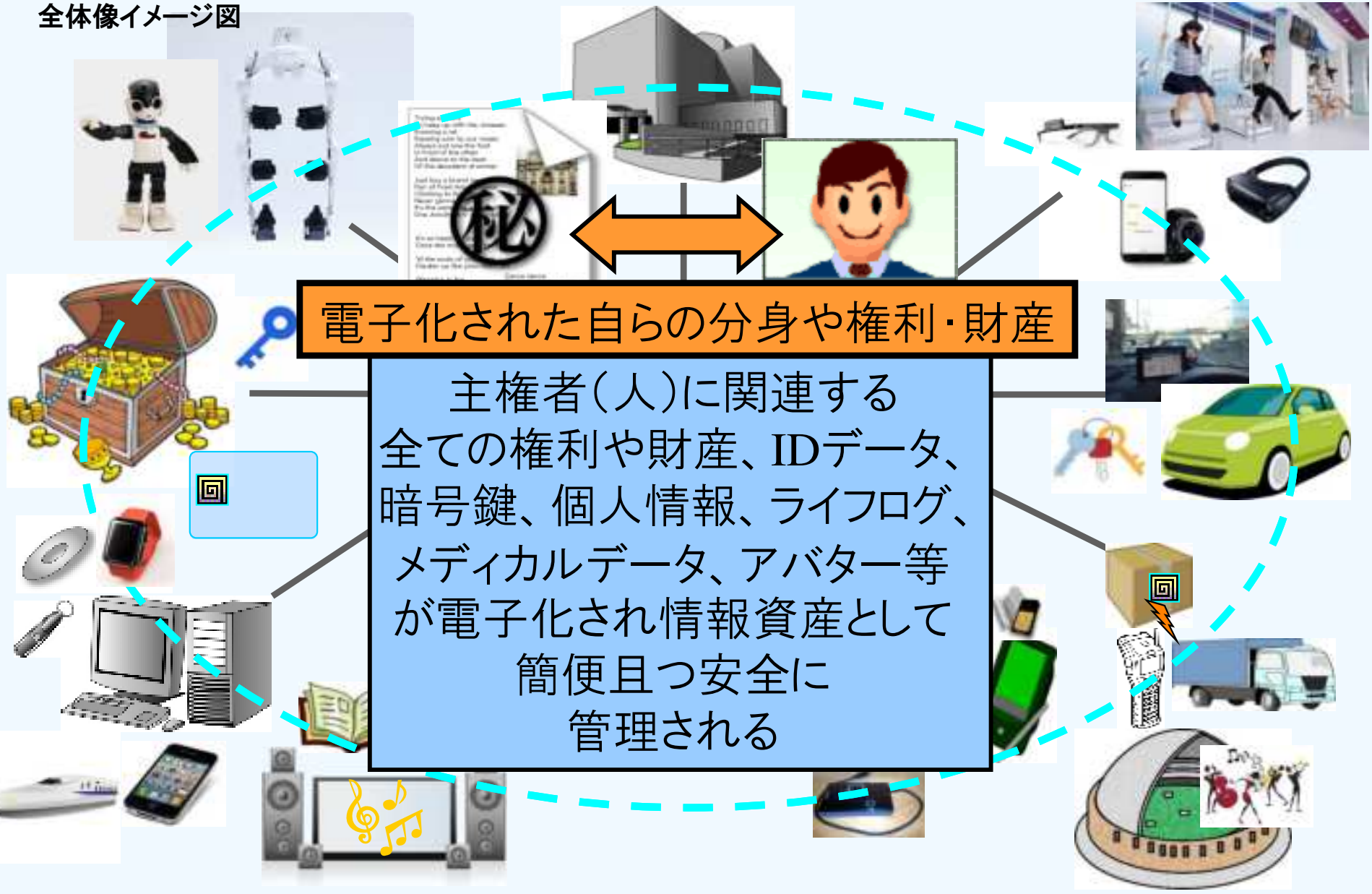
注：本記載はNISCからGFIへの要望で情報セキュリティ対策にGFI電子割符®を用いたい。との相談があり、様々な意見交換をしたことが発端である。

出典：https://www.nisc.go.jp/pdf/policy/general/guider3.pdf

NISC（内閣サイバーセキュリティセンター）主要公表資料　2021年7月7日

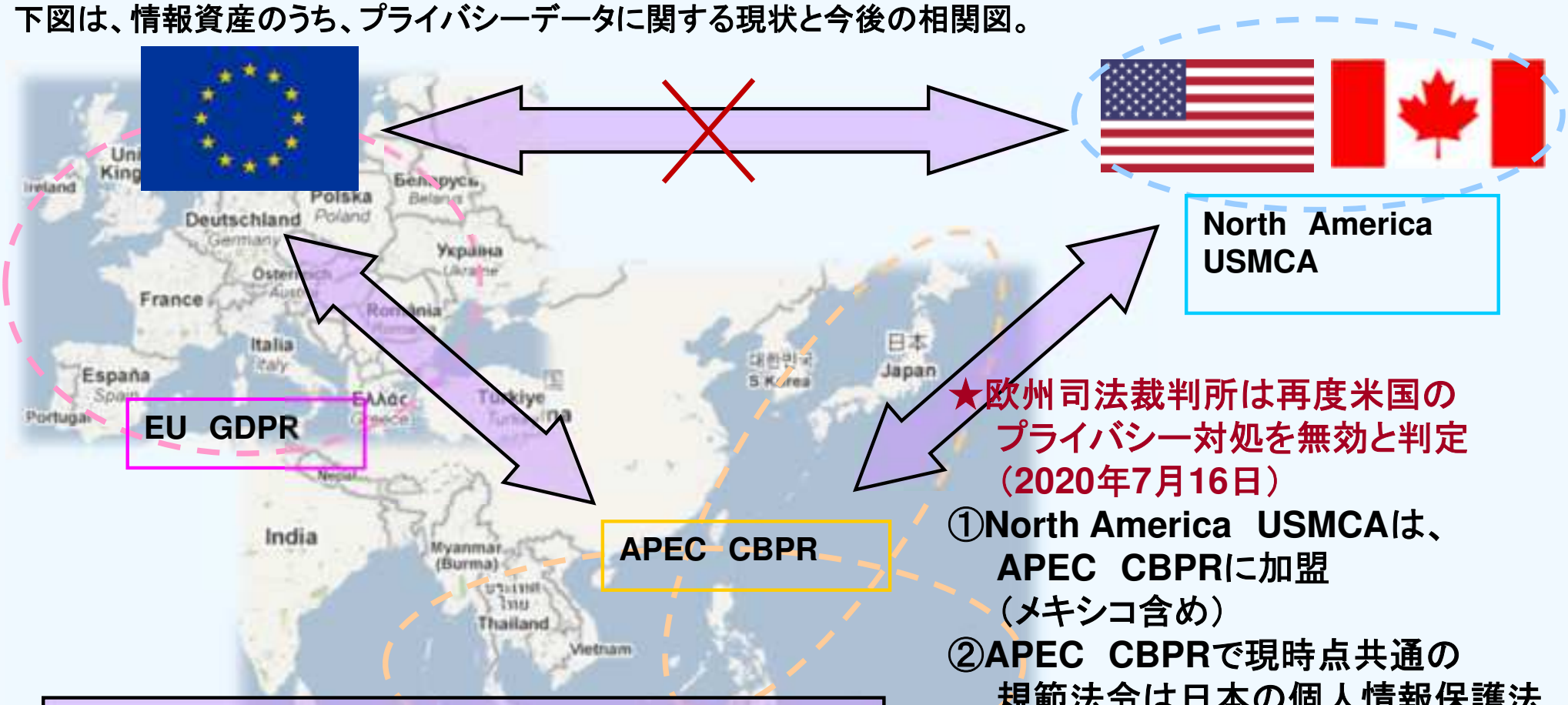
自己情報コントロール権市場

全体像イメージ図



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。



★欧州司法裁判所は再度米国のプライバシー対処を無効と判定（2020年7月16日）

①North America USMCAは、APEC CBPRに加盟（メキシコ含め）

②APEC CBPRで現時点共通の規範法令は日本の個人情報保護法（オーストラリア含め）

③日本の個人情報保護法は、EU GDPRとの十分性認定済み

④世界各国でプライバシー保護法令が順次整備が進むが、GDPRをベースにモディファイ

今後、日本の個人情報保護法の特異な立ち居地が、
プライバシー保護システム構築に向け、
世界的にも重要度が増す。
国内個人情報保護法やGDPRに対する、
GFI電子割符®の法的有用性評価や、
継続してきた技術外部評価、導入実績等が、大いに役立つ。

EU GDPRへのGFI電子割符®の役割

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「集合論で言うとこ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

＝

暗号化
（変換データ）

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」

≠

割符A

≠

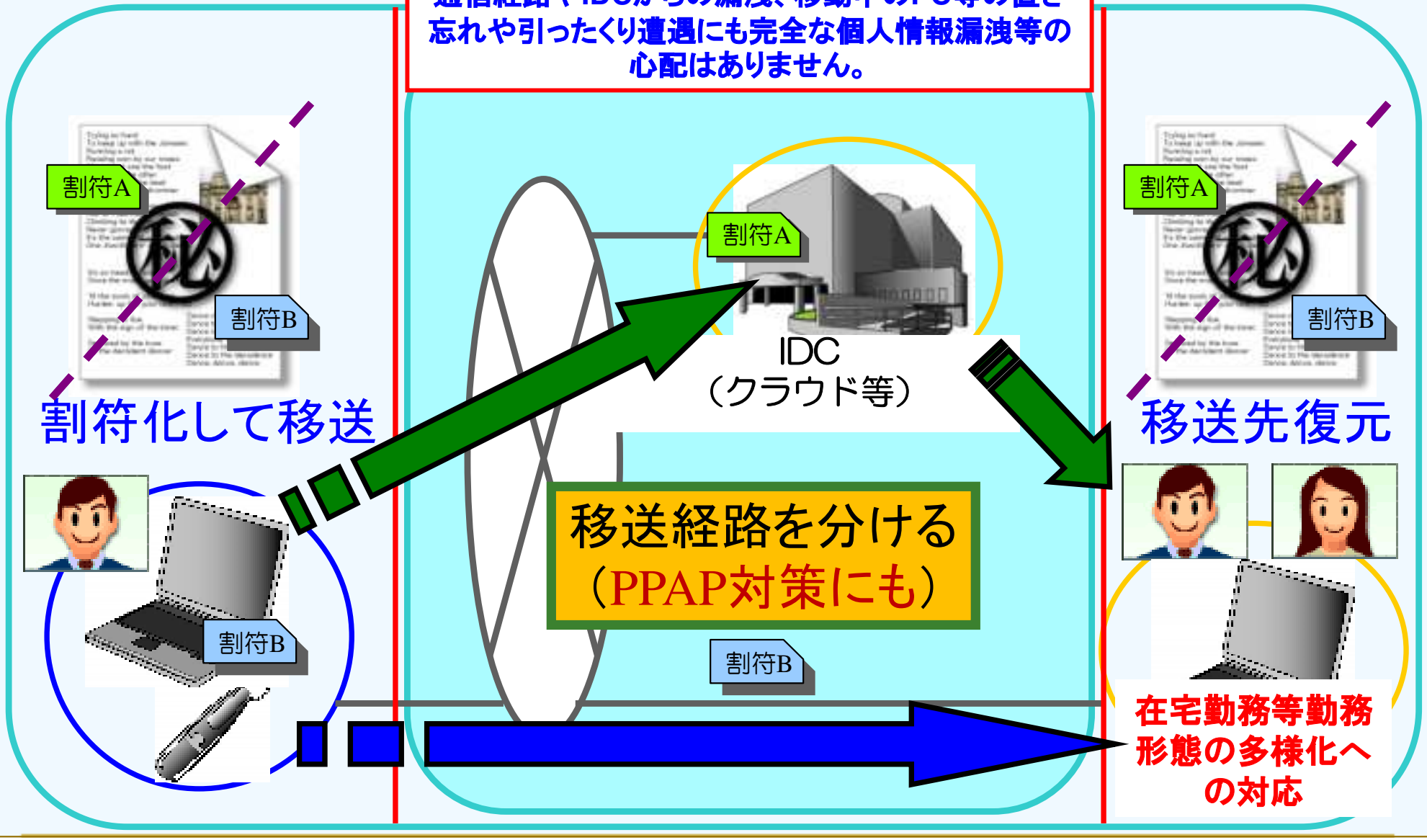
割符B

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

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。



出荷準備中商品

仮称 GFI Sec Pac 4 PIESIS™

経営リスクとなる情報を割符化し漏洩等の禍根を断つ

割符化と分散保管等の処理は、自動化されている

GFI e-Tally®
Process

割符A
割符B
割符C

実務端末

必要な時は速やかに情報資産を復元

①Win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
③GFI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
⑤NTT東日本コ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

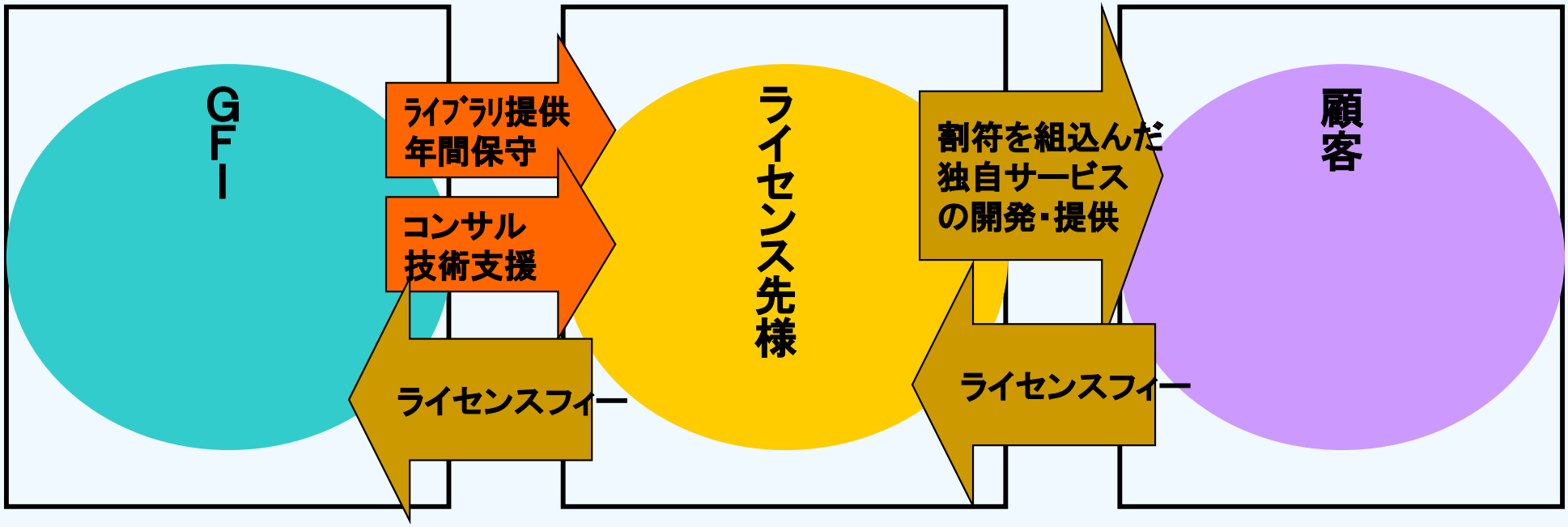
クラウド利用安全対策比較表

	管理責任 対処法	管理場所	サービス 開発 コンセプト	ポータ ビリティ	GDPRや 改正個人情報 保護法評価	当該 サービス 実績
	集中管理 分散管理	データオナー 自由度 容易性	利用者 目線	利用者 主体	市民目線で 高度に対応	国際市場 実績
A社	×	×	×	△	△ 注1	○
B社	×	△	×	△	△ 注1	○
GFI	○	○	○	○	○	× 注2

注１：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２：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

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。

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
代　表　者：代表取締役社長　保倉　豊（情報処理学会会員）
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、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エア協会（SAJ）（旧：コンピューターソフトウエア協（CSAJ））
　　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
　　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145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ー文化の国際普及に相互協力します。

TÜV

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

GFI

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/

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・リトンド様、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

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。」