

お客様各位

GFI電子割符®

2018, 06

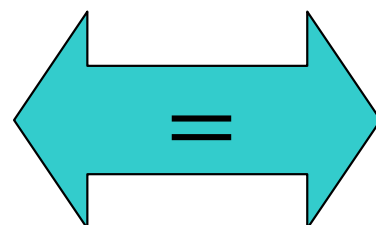
グローバルフレンドシップ株式会社

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。

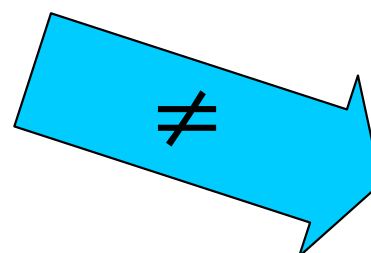
GFI電子割符®

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。

原本情報



+



注：割符ファイルは、デジタルデータの原理的特性から来る安全性と、各種法令条文等が定める安全管理措置(義務)の発生する対象情報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。

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

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

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、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。

弊社秘密分散技術(技術区分一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。(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、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

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

利便性の影に隠れた恐ろしさ

只ほど怖いものは無い。

ITの世界はその典型です。

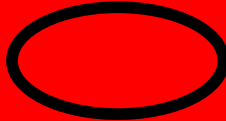
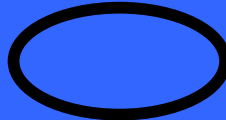
SNS、クラウド、仮想通貨、

更にベーシックインカムとの連携等々。

全情報を牛耳られることになります。

弊社技術実装に関する確認結果

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)

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			

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。

---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---

昨今の攻撃者の狙い

彼らは情報・コンテンツを換金できます。

だから効率よく情報を取得したい。

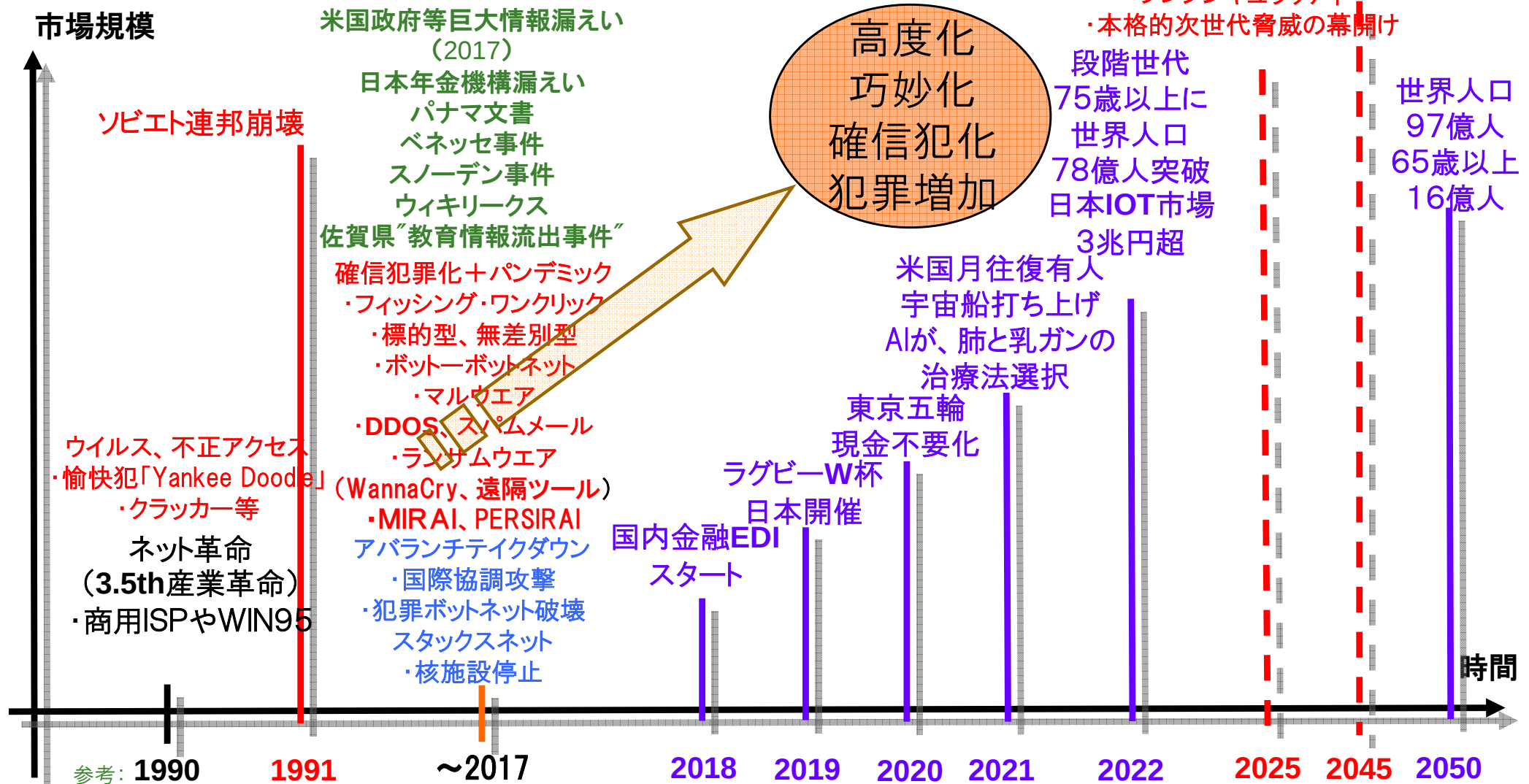
集約された膨大な情報は彼らの資金源。

あなたはそれに賛同しますか。

時代の激変

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



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。

これからの情報の安全管理は

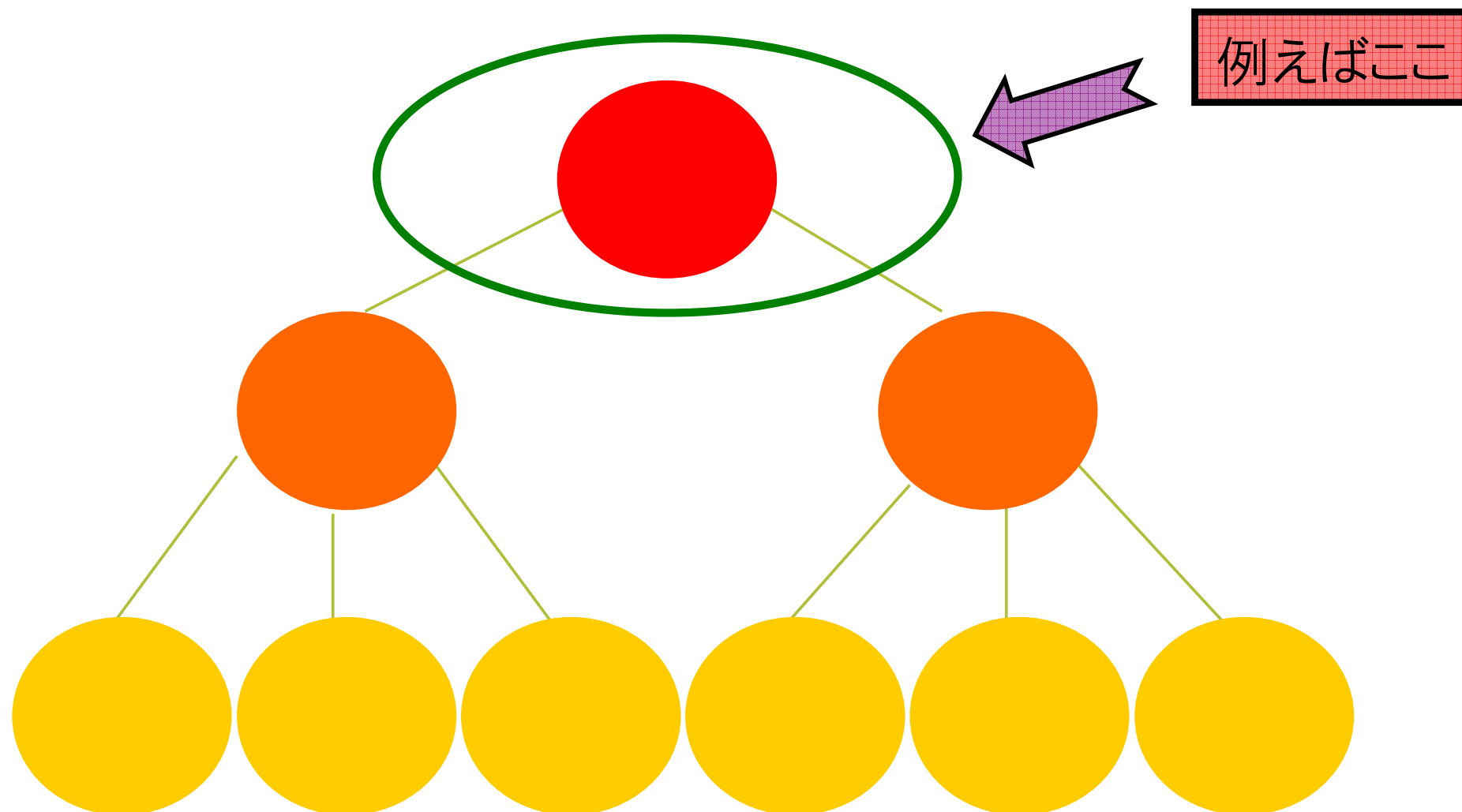
セキュリティの専門家でも、

容易に不正ができない

安全対策を

実施するのが一番です。

構造的な問題があります



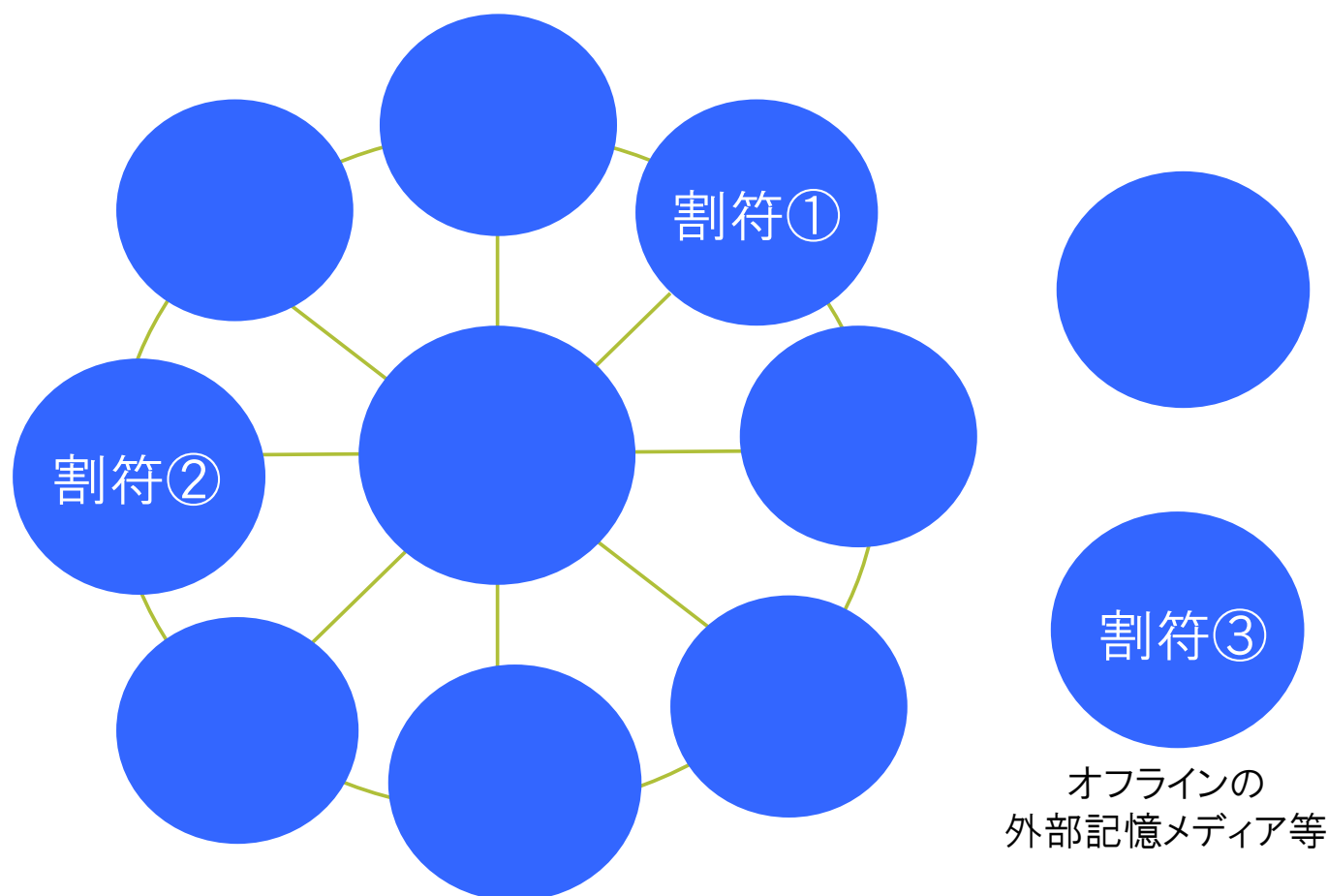
既存社会構造同様、コピー問題、狭い社会組織・構造に有効
一度の不正での被害が、大きい

次に

生成した割符ファイルを、
任意の場所に保管します。

それだけで、
攻撃者はお手上げです。

リスク分散



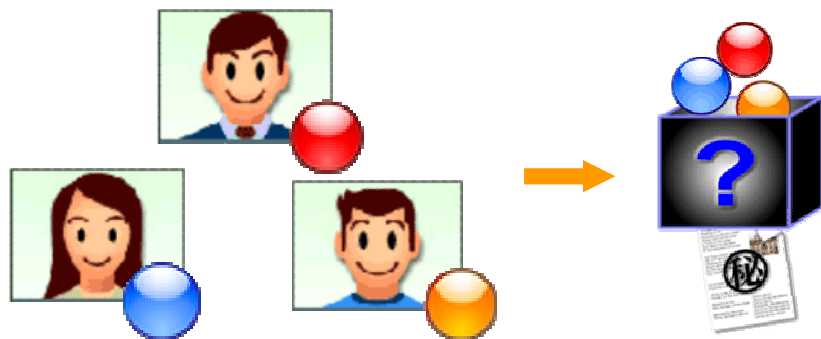
広い社会組織・構造にも有効、一度の不正での被害が限定される
BCP等にも有効、好きな場所に置ける
対象情報をシェアし透明性も確保

電子割符の最大の特長は

全くのIT素人でも、
不正攻撃者等にとって、
一番厄介な情報管理を、
シンプルに実現できることです。

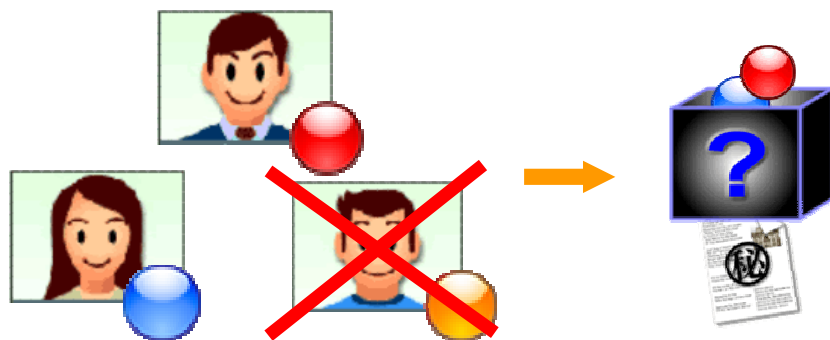
まずは電子割符を利用

(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。

(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。

(4)自己認証機能—復元する際の条件設定ができます。

ポイントは

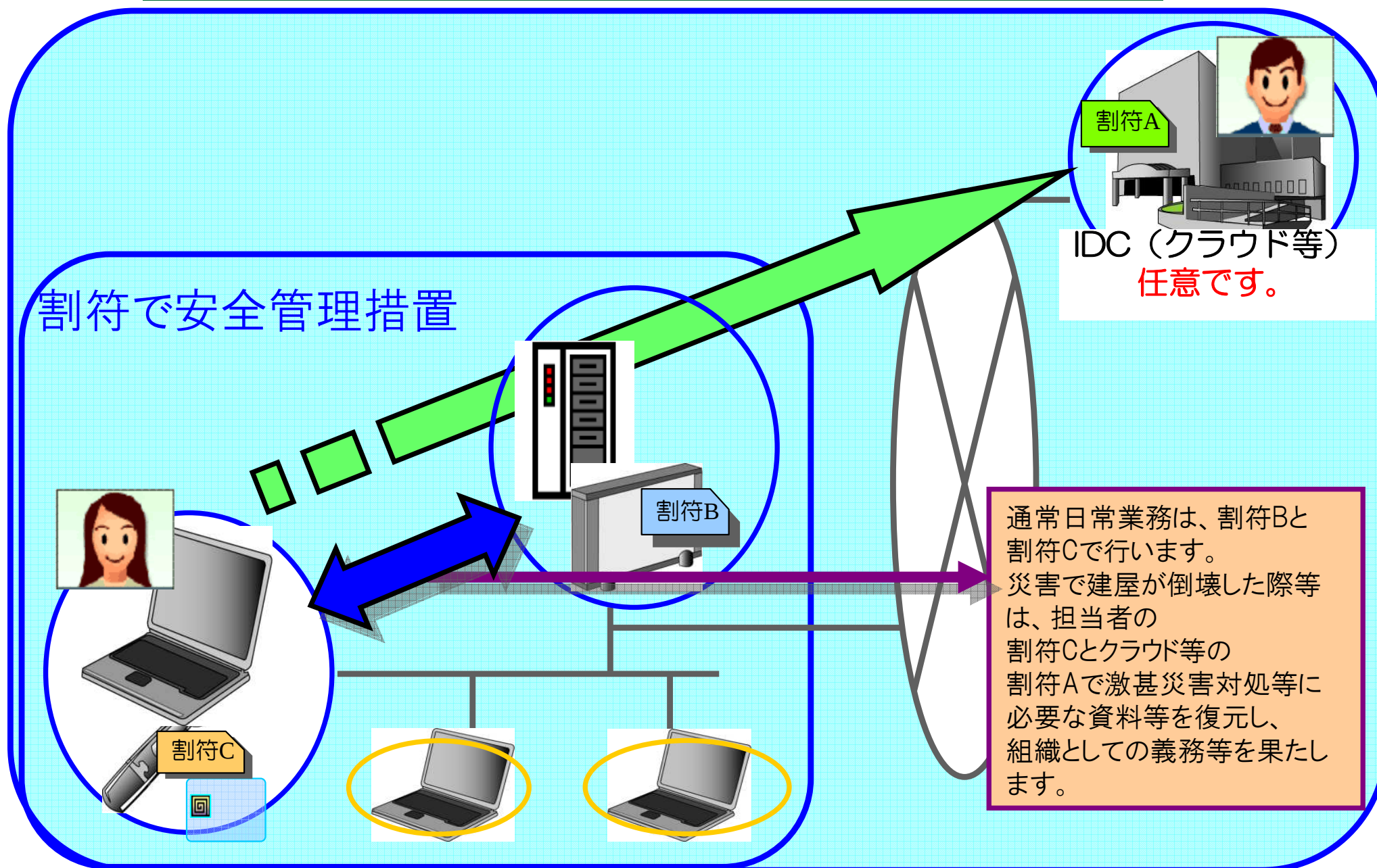
最終責任を負うのは誰か。

本当に誰かが、

最後まであなたを守ってくれますか。

当事者として何が最善かを考えましょう。

弊社ISMS基本形(保管・BCP)



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文化の国際普及に相互協力しております。



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



<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

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: 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

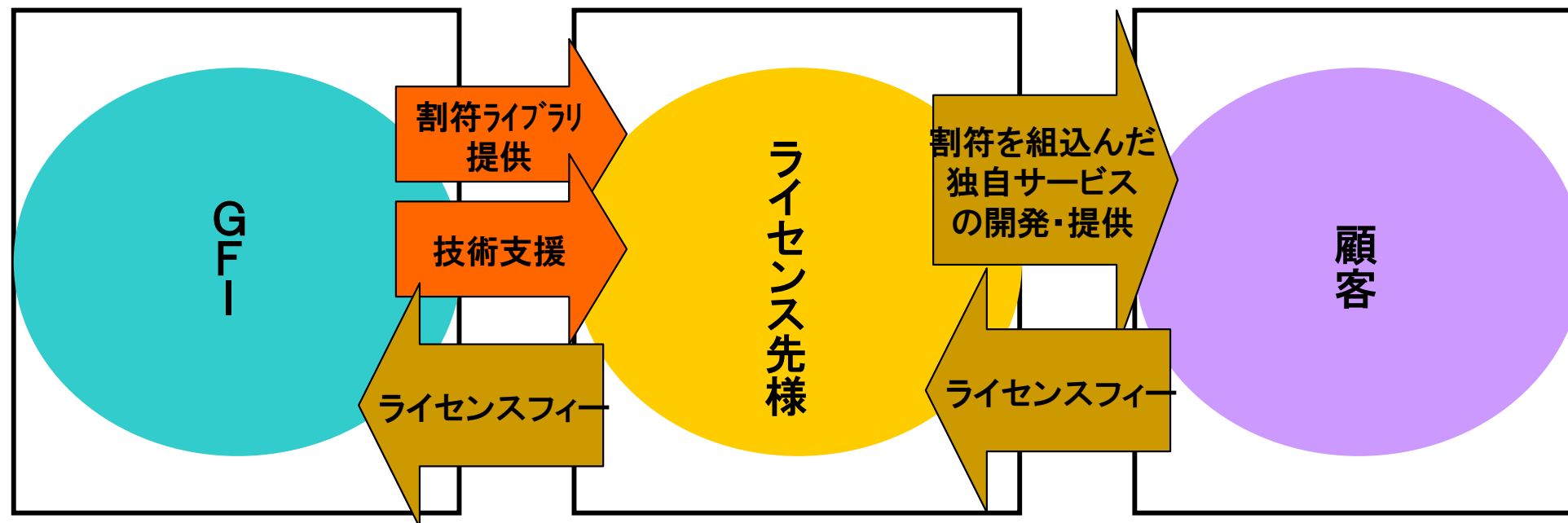
取得済維持特許: 15案件(累計14カ国(EU、ユーラシアも1国とした)累計40件以上取得
但し即実施予定無いものは放棄)

(日本9件、アメリカ3件、中国1件、イスラエル1件、香港1件)一部共同出願含む

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))

主要株主: 保倉 豊、株式会社アイ・オー・データ機器、NTTファイナンス株式会社、他144名

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しますので、遠慮なくお申しつけ下さい。

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。」