お客様各位

GFI電子割符®活用のご案内

サイバー攻撃の結果、勝手に暗号化されてしまう等の事件は総務省やNISC公開資料記載の手段を用いていれば防げました

2022年12月13日
グローバルフレンドシップ株式会社

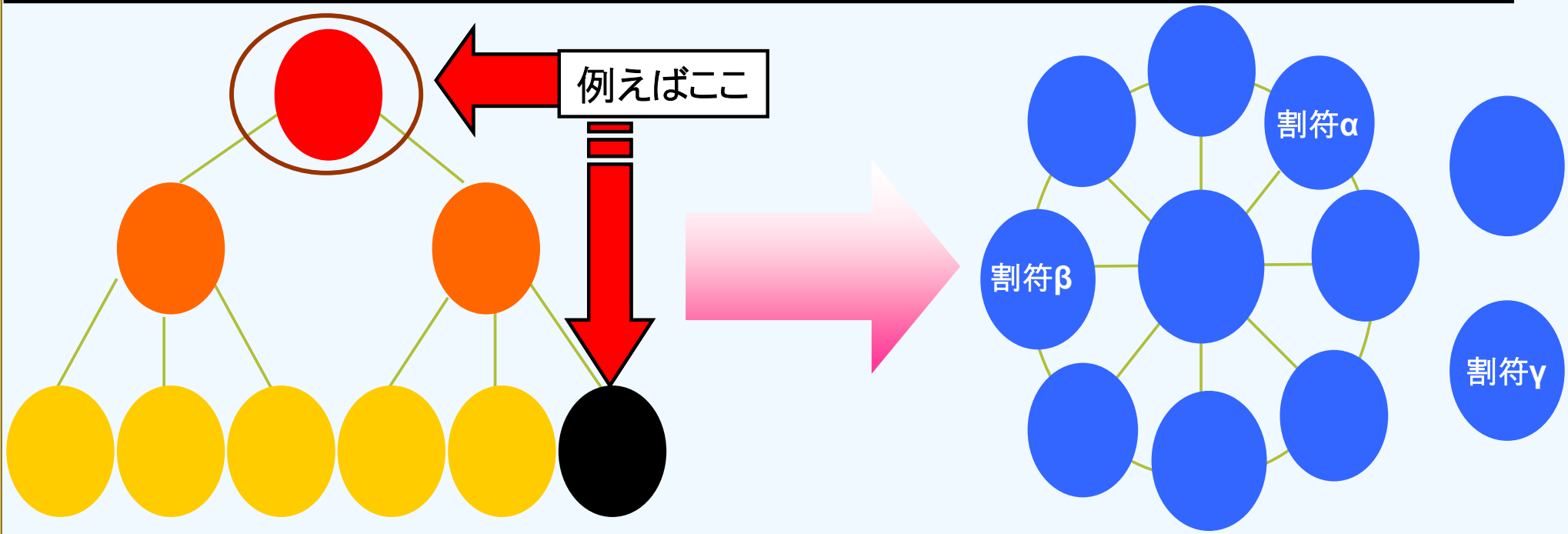
注：GFI電子割符®に関する基本的な説明は別資料となっております。
ご不明な点やご質問等ありましたら、遠慮なく弊社までお問い合わせください。

情報セキュリティの根本的解決

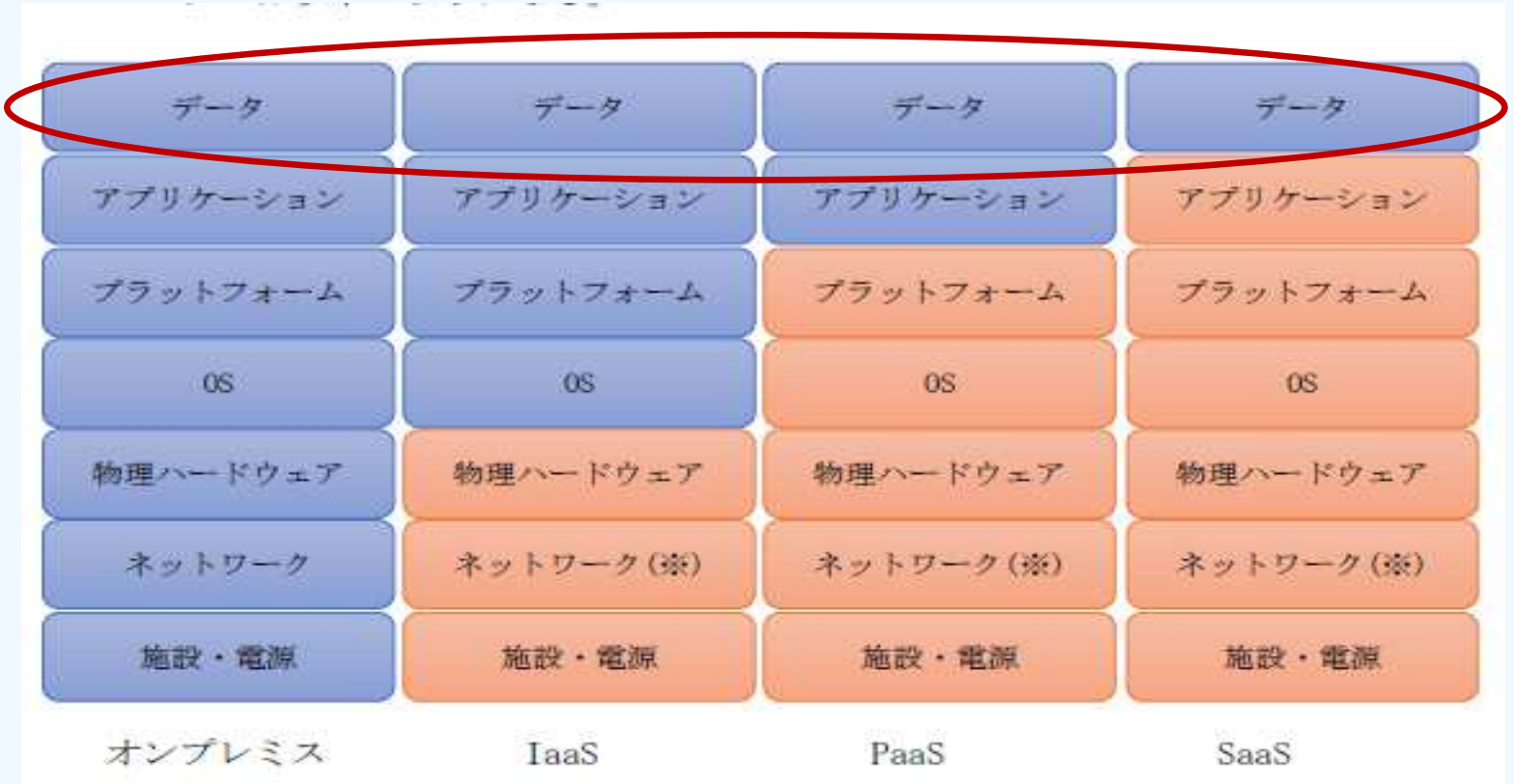
影響の巨大な情報漏洩等の根源を断つ

情報漏洩等（原本データ消失・攻撃者による勝手な暗号化含め）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

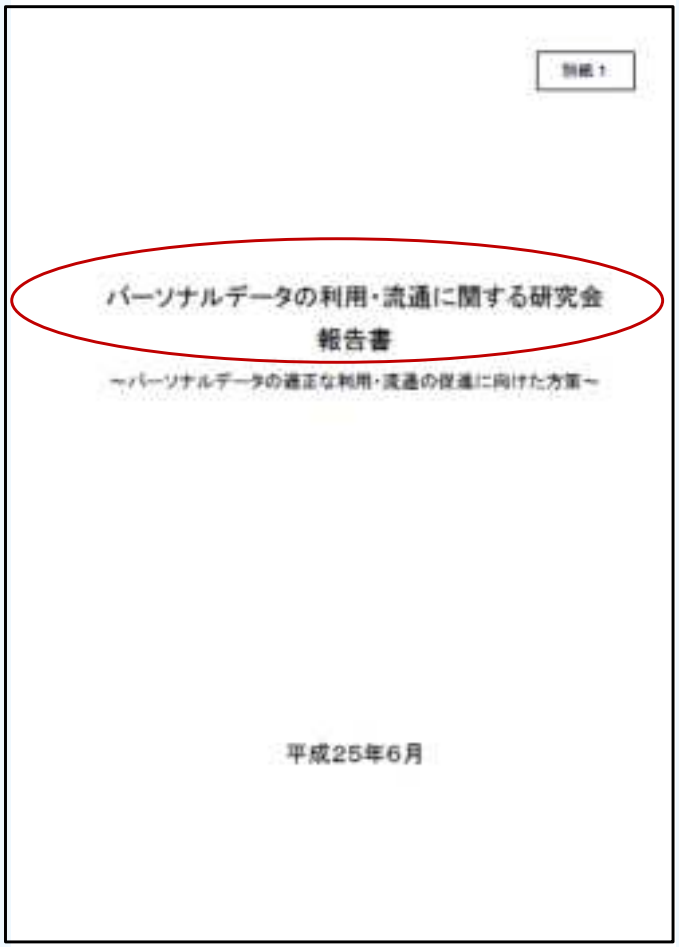
②IDや暗号鍵管理は万全ですか

③データ管理責任は、結局利用者側にあります

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

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。

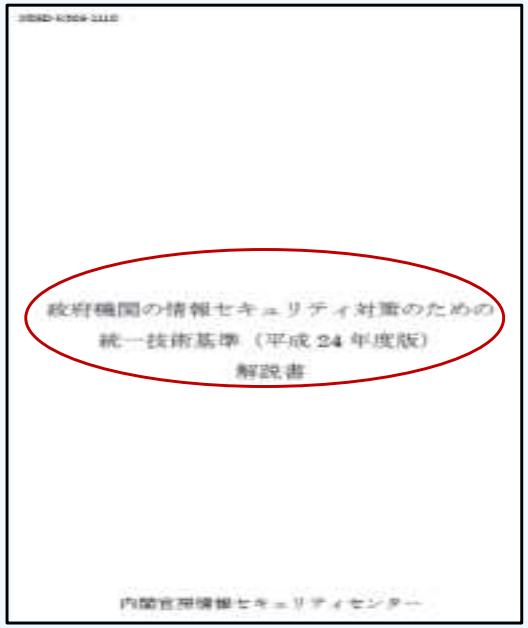
出典：https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000071.html

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

サーバ情報セキュリティ・復元NISC資料

「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（H24）解説書」に準拠

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.50 より

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。

(2) サーバ装置の運用時　【基本遵守事項】

(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。

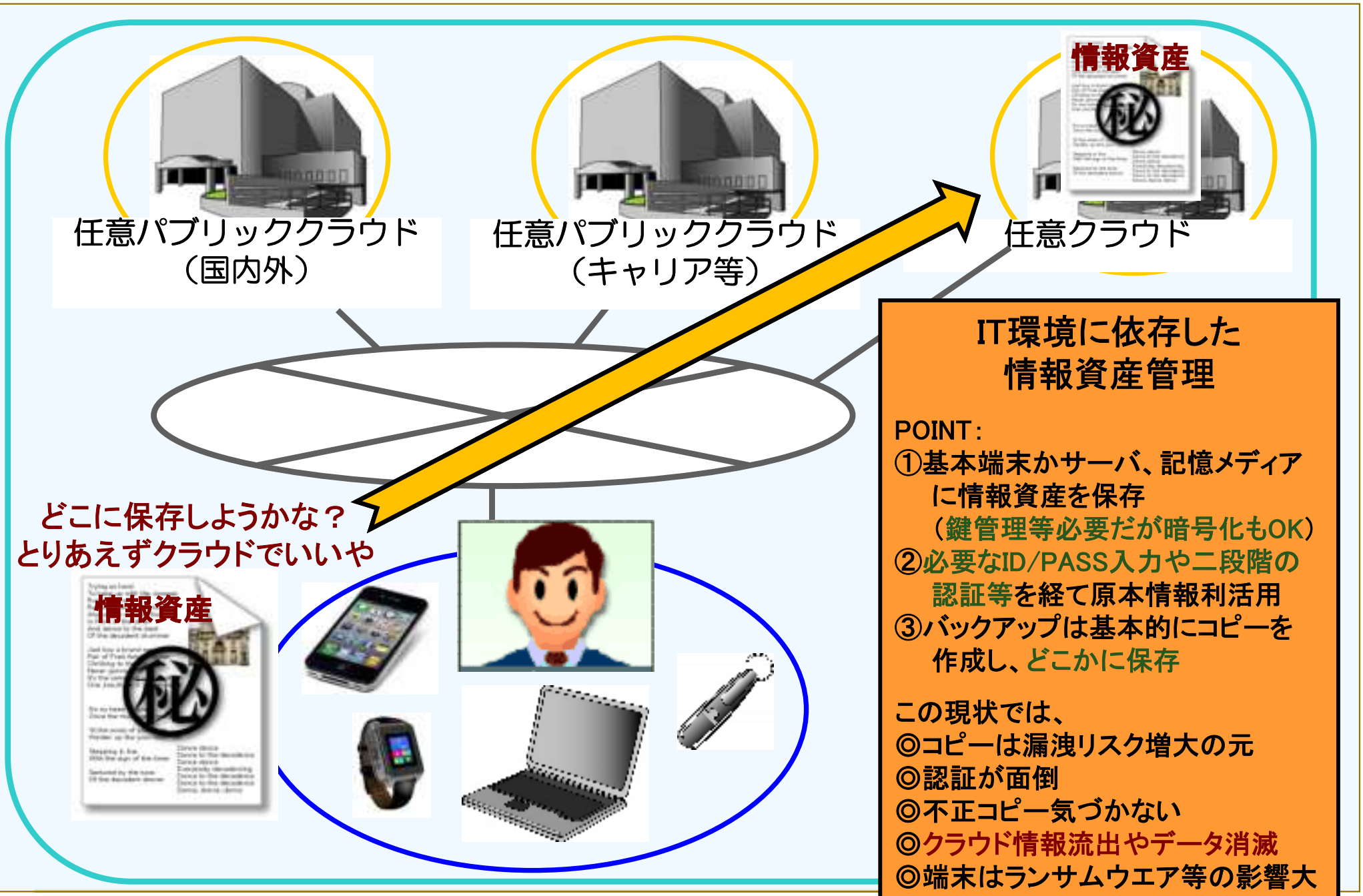
・サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。　・前回内容からの変更部分の定期的なバックアップを実施する。
・サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。
・バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。

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。

注：NISCの一連の秘密分散技術関連記述のあるドキュメントの公開は、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/k305-111C.pdf
NISC（内閣サイバーセキュリティセンター）政府機関総合対策グループ

現状の情報資産管理状況



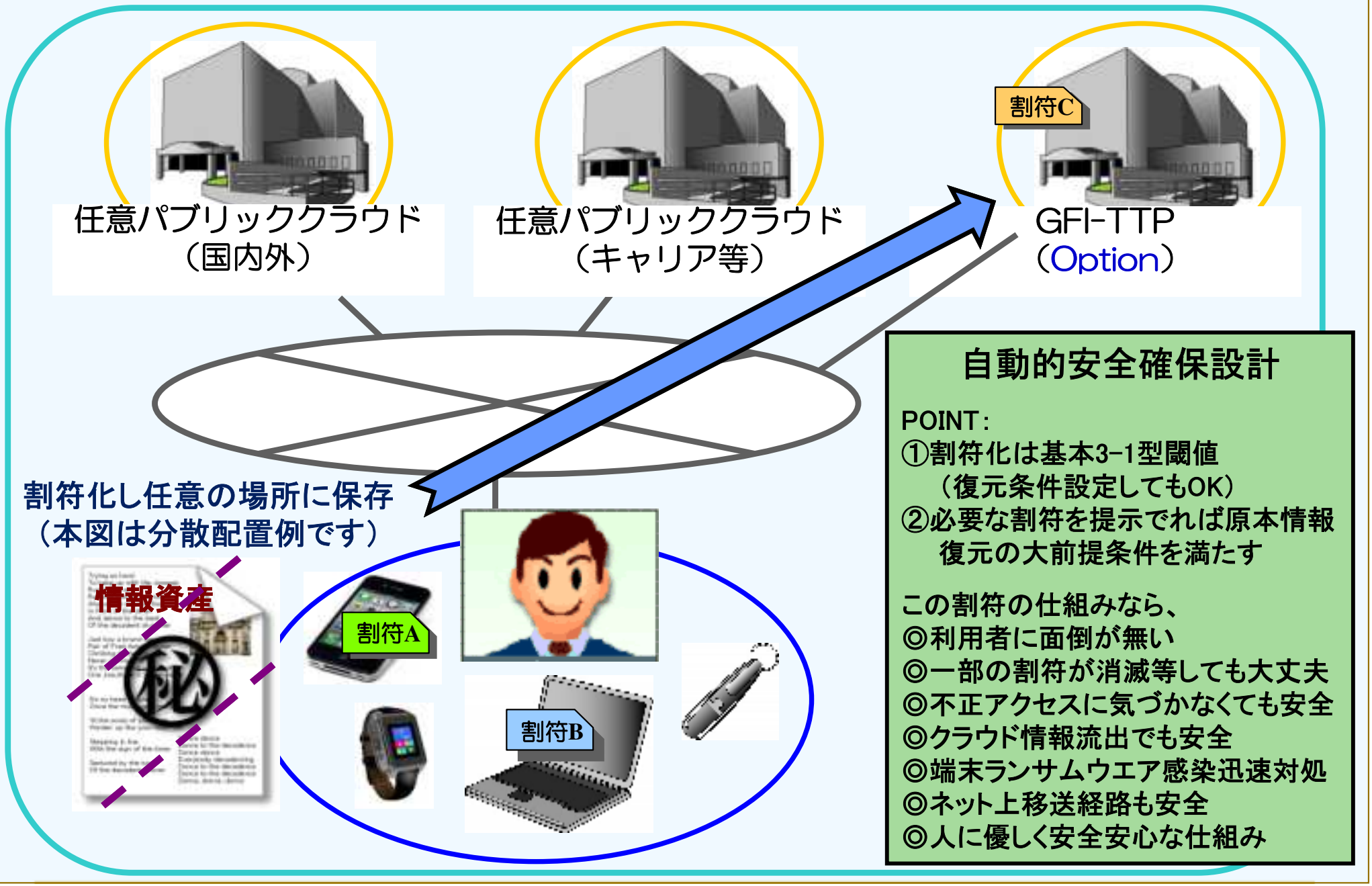
IT環境に依存した情報資産管理

POINT：
①基本端末かサーバ、記憶メディアに情報資産を保存
（鍵管理等必要だが暗号化もOK）
②必要なID/PASS入力や二段階の認証等を経て原本情報利活用
③バックアップは基本的にコピーを作成し、どこかに保存

この現状では、
◎コピーは漏洩リスク増大の元
◎認証が面倒
◎不正コピー気づかない
◎クラウド情報流出やデータ消滅
◎端末はランサムウエア等の影響大

原本情報を割符化し自由に分散配置

弊社取得済特許利用



自動的安全確保設計

POINT：
①割符化は基本3-1型閾値
（復元条件設定してもOK）
②必要な割符を提示でれば原本情報
復元の大前提条件を満たす

この割符の仕組みなら、
◎利用者に面倒が無い
◎一部の割符が消滅等しても大丈夫
◎不正アクセスに気づかなくても安全
◎クラウド情報流出でも安全
◎端末ランサムウエア感染迅速対処
◎ネット上移送経路も安全
◎人に優しく安全安心な仕組み

暗号化は最低限であり今後は不十分

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

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。

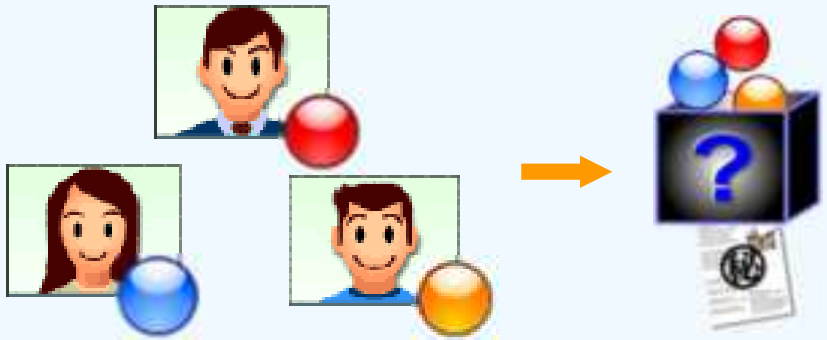
産業技術総合研究所（下記参考URL公開情報抜粋）

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

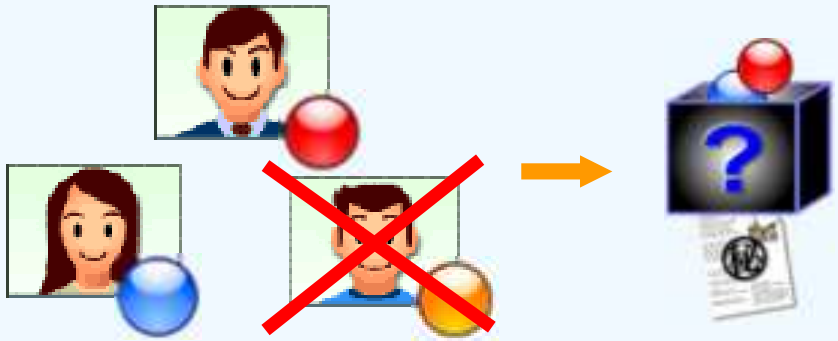
GFI電子割符®の基本機能

（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。

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。

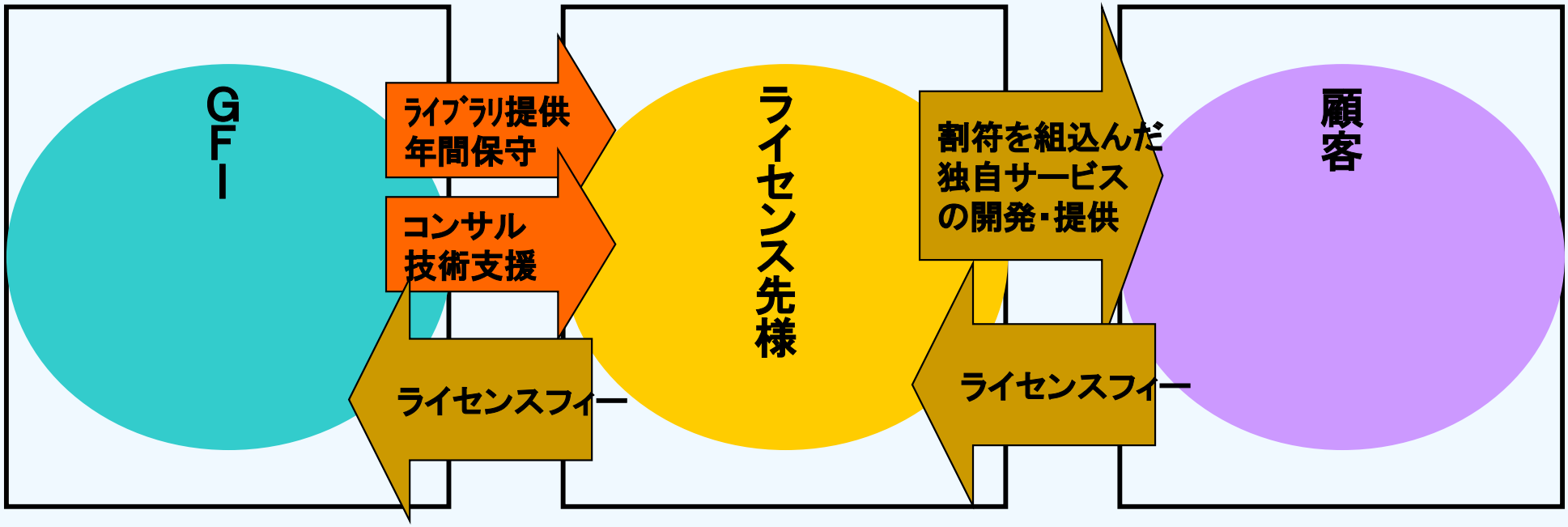
民間系

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。

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

今後弊社は、これまで蓄積した当該技術周辺ノウハウを活用し、自らも当該技術を実装した商品・サービスを開発し、市場供給していく方針です。今後積極的な当該技術の外部ライセンスを控えてまいります。ご関心のある方は、弊社までお問い合わせ下さい。

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

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

GFI創業理念：「たくさんの人を幸せにしたい」