デジタルデータの特性を活かした究極の情報資産管理

データ自身をGFI電子割符®で
強靭化しパブリッククラウドを活用しきる
事例紹介

2022年2月25日

グローバルフレンドシップ株式会社

デジタルデータと情報資産

古来情報は軍事的にも非常に重要な役割を果たしてきました。シーザー暗号、虎符（割符）、勘合符、エニグマ、パープル暗号、共通鍵暗号、公開鍵暗号・・・。パープル暗号が解読されていたことで日本が敗戦したことは有名です。IT分野では早期から計算結果や電子情報のセキュリティが重要であることは周知の事実でした。国家的危機、侵略者等による人権蹂躙等々歴史的惨劇を招く。

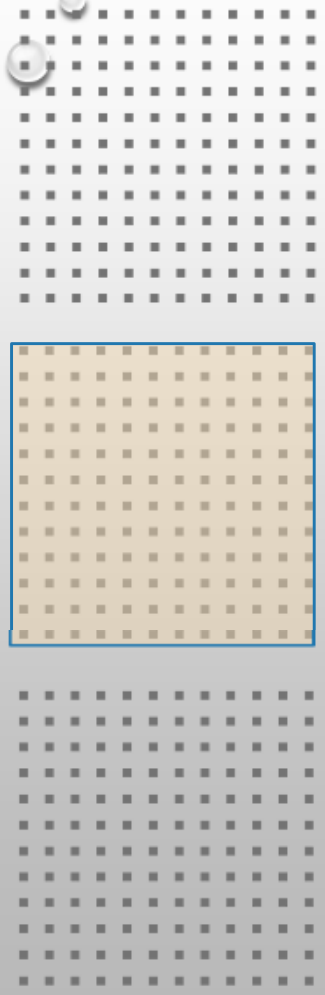
羊飼いと目覚めた子羊の世界

IT環境で自らのアカウントや暗号システムを利用している場合には、暗号鍵やID/PASS情報の管理が必要です。暗号鍵は多くの場合、ITシステム側が管理していて、利用者が意識しないことが多く、実はここも恐ろしい点です。**今後自己情報コントロール権等で問題となるでしょう。**

Nuclear missiles
Dual control
They turn the key

核ミサイル発射要員２人が同時にキーを回します。
（究極の鍵管理例）
認証局やクレジット決済のサーバでの暗号鍵管理も分散型を利用しています。
（非常に高額な投資）

そもそもデジタルデータって



01011101001000101000110010110111010010100101・・・・・

一方向性関数を利用し、
元データよりも小さな情報量で、
同一性を確認する固定長のチェック値は、
常にコリジョン（衝突性）が伴う、
他方、割符ファイルは巨大なチェック値とも言える。

デジタルデータの原理的特徴を利用して、
①変換することで原本情報秘匿
②欠落させることで原本情報秘匿
③そのままどこかに隠す
原理的には①一般的暗号化と②電子割符化の技術的対処。

デジタルデータの原理的特徴を利用して、
①コピーを行い情報消滅対処
②電子割符の閾値機能で対処
①は漏洩リスク増大、②は割符化されているので秘匿性も高い。

デジタルデータに必要な特性

- 同一性
- 秘匿性
- 耐消滅性

暗号化されていてもリスク発生しています

EUでも日本でも、暗号化したデータは個人情報です。

EU指令関係資料抜粋：
通常、仮名化データは、**不可逆的に識別が防止されたもの**ではなく、依然として「個人データ」に該当します。
個人データを暗号化した場合、通常、暗号化されたデータは、暗号を解く鍵なしでは、個人の識別につながり得ない情報となりますが、暗号を解く鍵が存在する限りにおいて、個人の識別が不可逆的に防止された訳ではないため、「匿名化データ」には該当しません。その結果、**暗号化されたデータは、依然として「個人データ」に該当するため、暗号化されたデータの処理および移転についてはGDPRが適用される**ことになります。

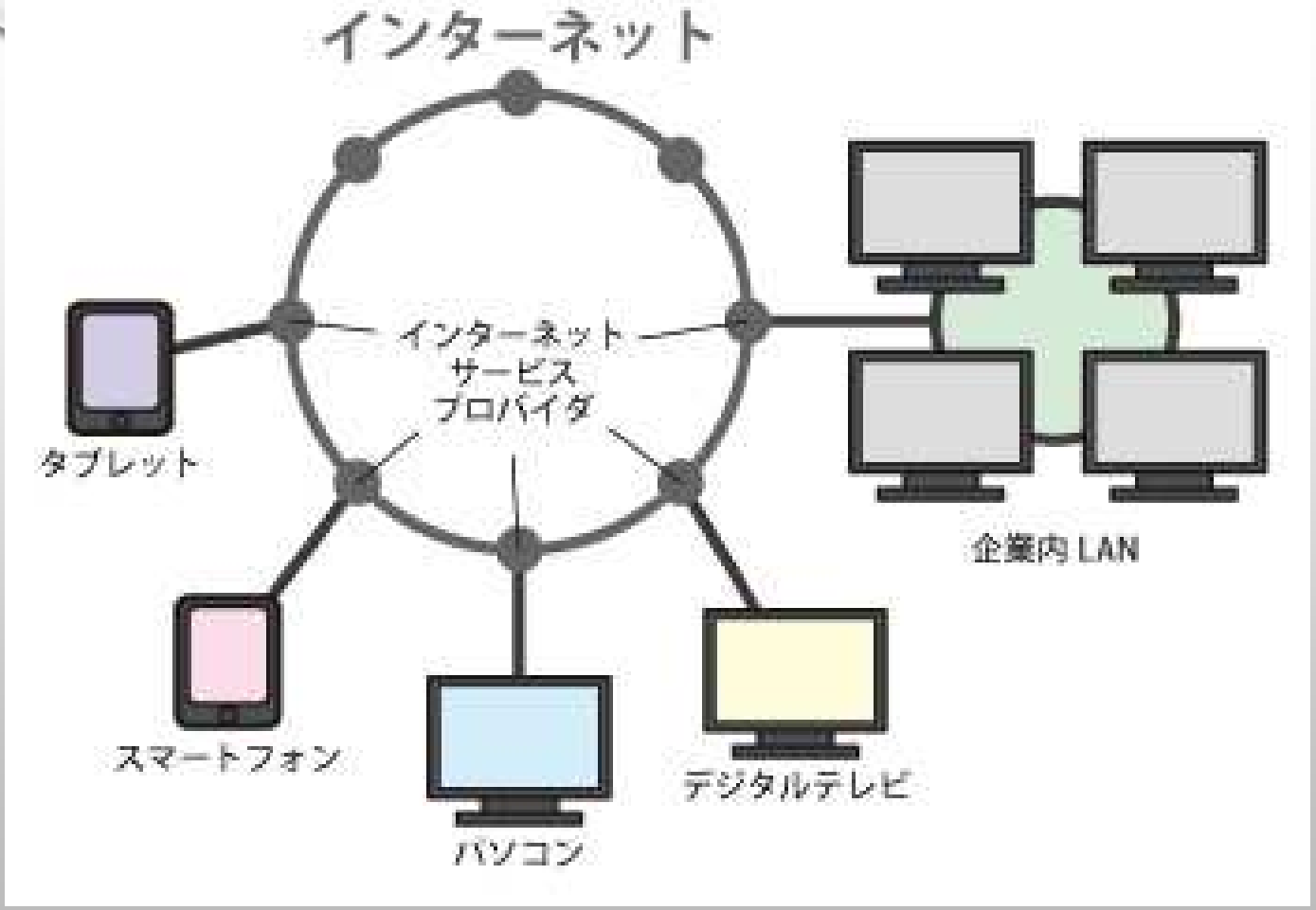
出典：「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編） 2016 年 11 月 日本貿易振興機構（ジェトロ） ブリュッセル事務所 海外調査部 欧州ロシア CIS

日本個人情報保護法ガイドライン抜粋：
「個人情報」（※1）とは、生存する「個人に関する情報」（※2） （※3）であって、「当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができる もの（他の情報と容易に照合することができ（※4）、それにより特定の個人を識別することができるものを含む。） 」（法第 2 条第 1 項第 1 号）、又は「個人識別符号（※5）が含まれるもの」（同項第 2号）をいう。「個人に関する情報」とは、氏名、住所、性別、生年月日、顔画像等個人を識別する情報 に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、**暗号化等によって秘匿化されているかどうかを問わない**。
※4）「他の情報と容易に照合することができ」るとは、事業者の実態に即して個々の事例ごとに判断されるべきであるが、通常の業務における一般的な方法で、他の情報と容易に照合することができる状態をいい、例えば、他の事業者への照会を要する場合等であって照合が困難な状態は、一般に、容易に照合することができない状態であると解される。

出典：個人情報の保護に関する法律についてのガイドライン （通則編） 平成 28 年 11 月 （平成 29 年３月一部改正） 個人情報保護委員会

世界標準のRSA暗号は量子コンピューターで解読されることが証明されている

そもそもインターネットって



要素

- IPアドレス
- DNSサーバ
- **誰にも何も保証しない**

参考・出典：総務省　国民のための情報セキュリティサイト
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/service/02.html

クラウドって何でも責任持ってくれるの

2.4　クラウドサービス提供形態における登録プロセス及び責任範囲

2.4.1 責任共有モデル

オンプレミス及びクラウドサービスモデル（IaaS/PaaS/SaaS）における責任共有モデルは以下のようになる。

「クラウド バイ デフォルト（ISMAP）」のポイント：

①なんでも頼ってベンダーロックインされていませんか

②データ管理責任は、利用者にあります

もしも漏えい等してもプライバシーを侵害することがなく、改竄されたとしても元に戻すことができ、
更に消去や勝手な暗号化をされても、正当な権限者であれば復元することが一つの技術でできる。

そんなことができるセキュリティ技術があったら良いと思いませんか。それができるのが、GFI電子割符®技術の凄さです。**データオナー側の立場で情報資産管理に、お役に立ちます。**

デジタルデータを鍛えるGFI電子割符®って

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。

原本情報

＝

割符A ＋ 割符B

≠

割符A

産総研外部評価

現時点での安全性評価で得られてい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**

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。

GFI電子割符®による強靭化 攻撃耐性強化

- 復元時同一性
- 割符秘匿性
- 閾値復元機能

効果確認した事例

- 仮説（実務前提）
- 実証（インシデント）
- 評価（実対応）

仮説（実務前提）

テレワーク実務PCに①GFI電子割符®を用いたデータ管理アプリと、②エンドポイント向けセキュリティアプリ、更に③MFA認証を簡潔に利用できるクラウドストレージを組合せ日常的に「高レベルの情報資産を存在させない」、実務環境を実現し、更にサイバー攻撃等を受けてもリスクを最小化できる仕組みを実現する。最悪マルウエア等に感染し発症しても、割符の閾値機能等を利用し、「代替機ですぐに実務復旧できる」のではないか。
（移送経路の安全性確保にも貢献）

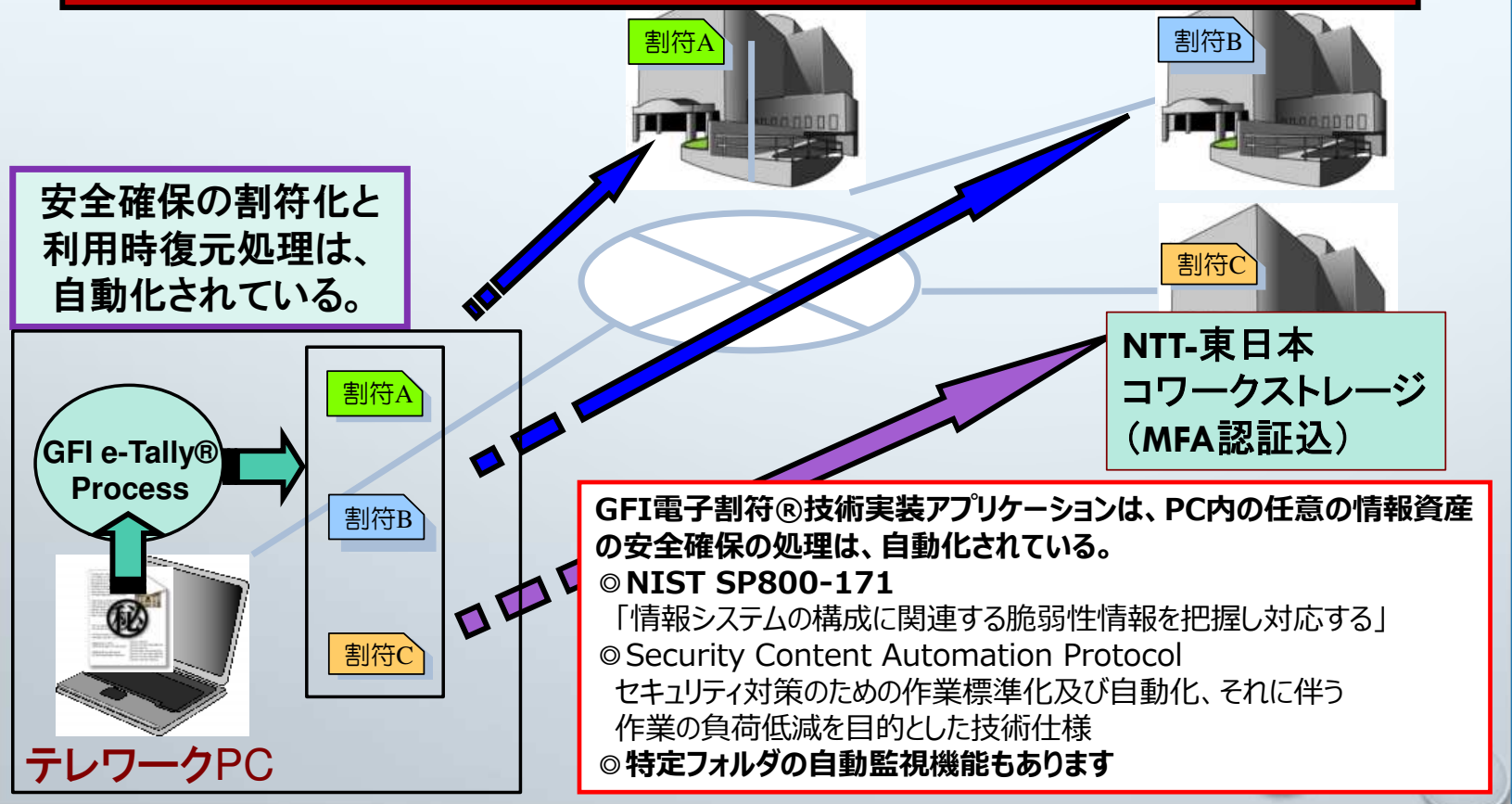
実証（インシデント）

約40分後に、テレワーク環境下で大事なオンライン会議を控えたその日、突然テレワークマシンの電源が入らなくなった。事象としては、事実上マルウエア感染しテレワークマシンが利用できない状況と同じ。早速代替機を立上げ、ネットワーク接続し割符アプリから会議資料等を復元し無事オンライン会議を終了。

評価（実対応）

代替機に割符アプリをインストールし起動させる等を含め、事実上20分ほどで一切他に影響を与えることなく、IT部門への負担もなくインシデント対処ができた。また、クラウドに不正アクセスがあったとしても、復元に至らない数の割符ファイルしか預けておらず、極めて高度な安全管理措置を実施できている。
仮に主務大臣等に報告するとしても、高度な暗号化等を実施できている旨で良い。

データ保護：電子割符によるサイバー攻撃耐性強化
①日常的漏えい漏洩やデータ消滅を未然防止
②有事には代替機ですぐに業務復旧
③BCPや激甚災害発災時に必要な情報等管理



GFI電子割符®技術実装アプリケーションは、PC内の任意の情報資産の安全確保の処理は、自動化されている。
◎**NIST SP800-171**
「情報システムの構成に関連する脆弱性情報を把握し対応する」
◎Security Content Automation Protocol
セキュリティ対策のための作業標準化及び自動化、それに伴う作業の負荷低減を目的とした技術仕様
◎**特定フォルダの自動監視機能もあります**

結果ポイント

①簡単

②早い

③リスクなし

④即実務復旧

⑤激甚災害等への応用も

割符によるデータ自身の強靭化＋効果的手段の併用
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されクラウド等に分散管理され存在せず

攻撃者に最後の一線を突破されても漏洩等はない

第１層：
OSの推奨するセキュリティ機能と、**アンチウイルス等**のセキュリティ対策を実施。

第２層：
OSプロテクト型エンドポイントセキュリティ、**AppGuard®利用**。

第３層：
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。GFI電子割符®を実装した情報資産管理アプリが役立ちます。

PC内構成

①OS推奨機能

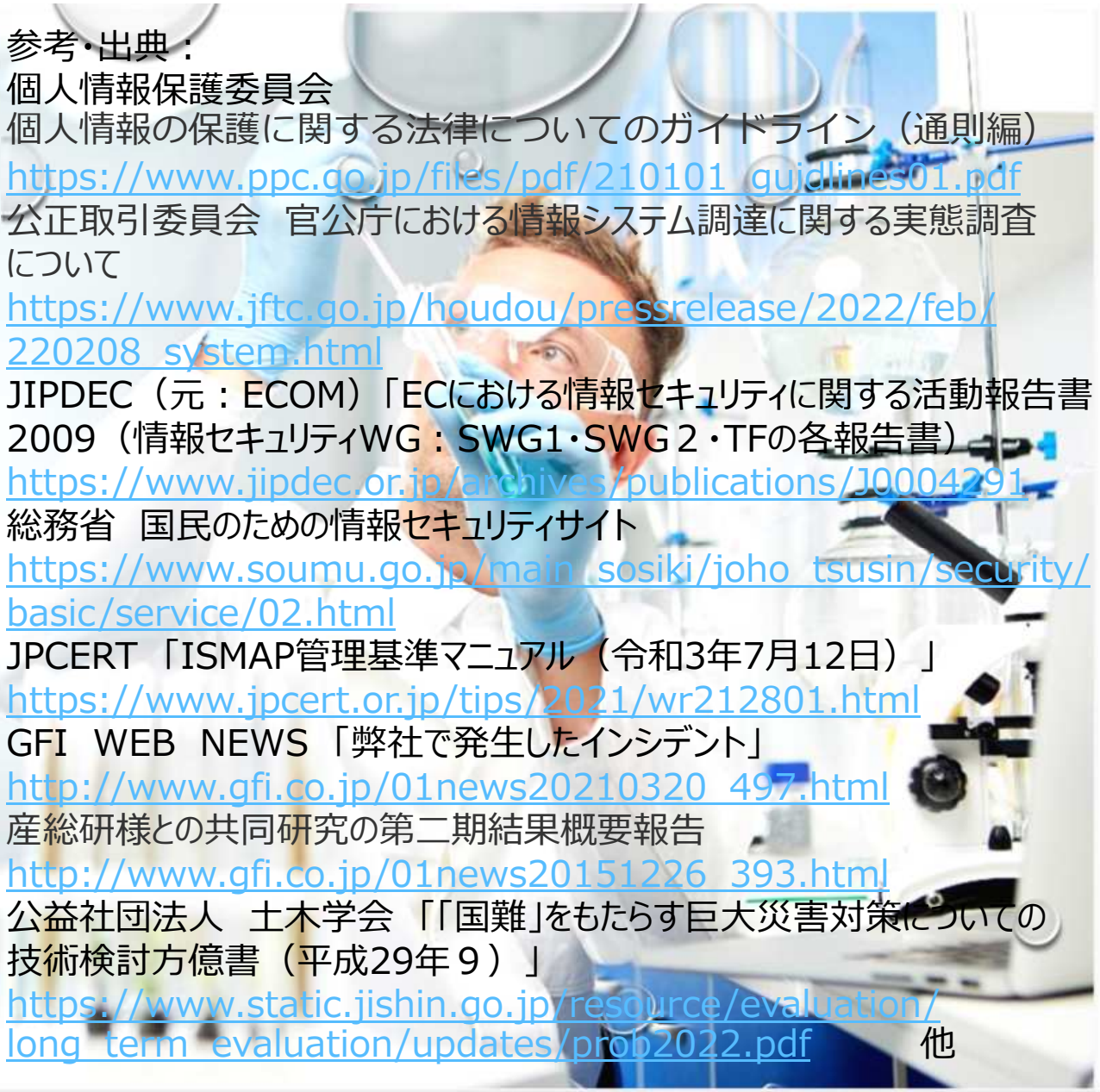
②一般的U/V

③OSプロテクト

④電子割符APL

⑤複数クラウド＋MFA認証

◎近くセット商品化



参考・出典：
個人情報保護委員会
個人情報の保護に関する法律についてのガイドライン（通則編）
https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf
公正取引委員会　官公庁における情報システム調達に関する実態調査について
https://www.jftc.go.jp/houdou/pressrelease/2022/feb/220208_system.html
JIPDEC（元：ECOM）「ECにおける情報セキュリティに関する活動報告書2009（情報セキュリティWG：SWG1・SWG２・TFの各報告書）
https://www.jipdec.or.jp/archives/publications/J0004291
総務省　国民のための情報セキュリティサイト
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/service/02.html
JPCERT 「ISMAP管理基準マニュアル（令和3年7月12日）」
https://www.jpcert.or.jp/tips/2021/wr212801.html
GFI　WEB　NEWS 「弊社で発生したインシデント」
http://www.gfi.co.jp/01news20210320_497.html
産総研様との共同研究の第二期結果概要報告
http://www.gfi.co.jp/01news20151226_393.html
公益社団法人　土木学会 「「国難」をもたらす巨大災害対策についての技術検討方億書（平成29年９）」
https://www.static.jishin.go.jp/resource/evaluation/long_term_evaluation/updates/prob2022.pdf　　他

お問い合わせは グローバルフレンドシップ 株式会社まで

GFI-INFO@GFI.CO.JP

「第二回電子割符オンラインセミナーに関し」

と表題に入れてお問い合わせください。