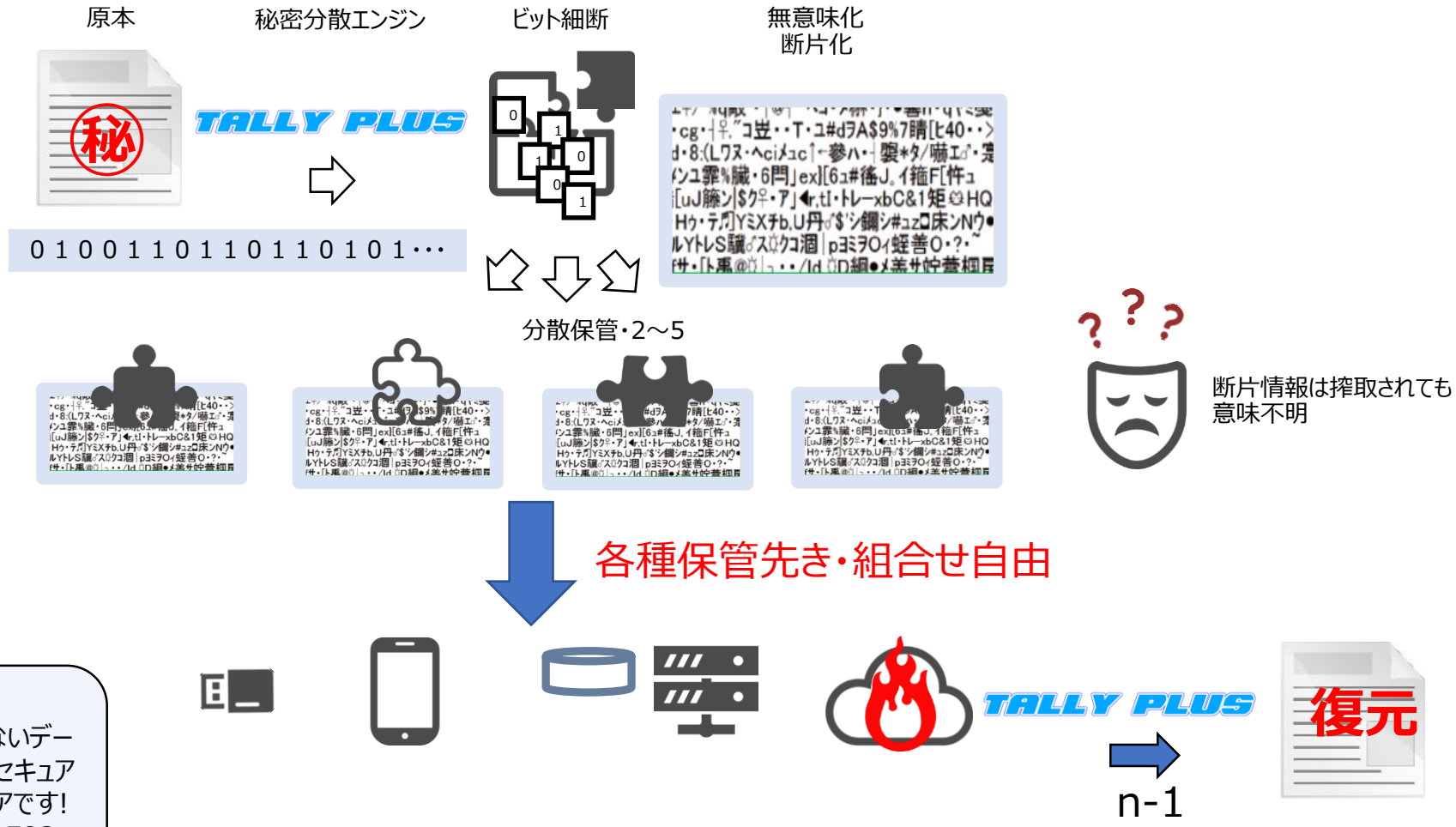
誰にも聞けない、情報漏洩対策基礎知識!

・暗号化より強い秘密分散技術とは!

・暗号化VS秘密分散

・情報漏洩対策の今後方向性

暗号化より・『強固な安全性』



TALLY PLUS

様々なデータを秘密分散技術で意味のないデータに変換、分散/復元を実現するターリーセキュアウォレット(株)が独自に開発したミドルウェアです!
秘密分散技術の国際標準ISO/IEC 19592-2:2017に基づいて開発されています。

注)n(分散数)―1でnが一つどれか欠けても復元可能

暗号化とは違う・『秘密分散技術』

暗号化：ビットレベルで置換処理→原本情報は残し読みづらくしている

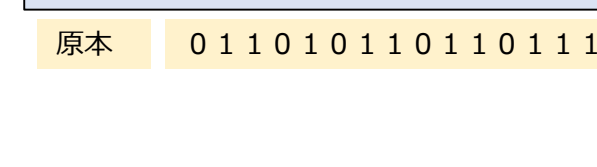
原本	0 1 1 0 1 0 1 1 0 1 1 0 1 1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 1 1 0…
暗号化	1 1 0 1 1 0 1 1 1 1 1 1 0 1 1 0 1 0 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 0 0 1 0 1 1…

原本情報が残り解読できてしまう

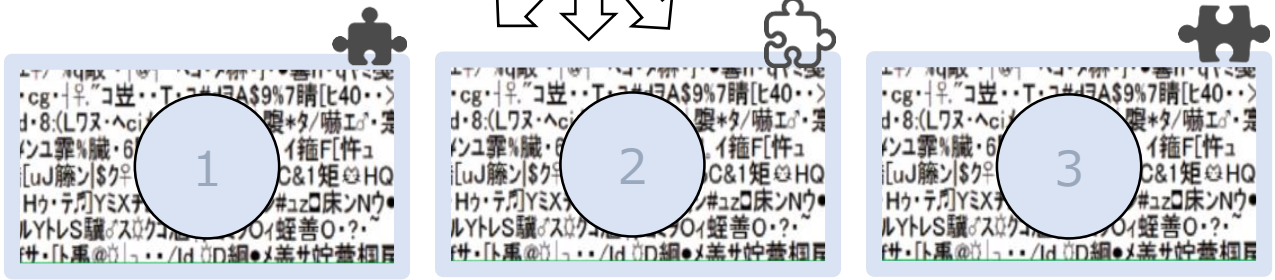
VS

秘密分散：ビット単位で細断・分散→原本情報がなくなり無意味化する

原本	0 1 1 0 1 0 1 1 0 1 1 0 1 1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 1 1 0…



割符断片化



割符断片単体では復元できない→解読されない

暗号化　VS　秘密分散

暗号化との相違点

・暗号化は元データーを解読を難易にする為の暗号化キーが必要

⇒ **秘密分散には、キーが不必要**

・革新続ける高速処理が可能なCPUでは、暗号化は、キー長等の変更が・・

⇒ **現在考えられる高速処理が可能なCPUでも、キーが無い為に、この様な手間が無い**

・暗号化されたデーターは、原則的には、暗号化した場所に存在する

⇒ **秘密分散では、分割保管(最大5ヶ所)されるので、データーそのものが存在しない**

・データーの暗号化については、世界的標準でデーターの安全性が高い

⇒ **弊社の秘密分散方式は、『ISO/IEC 19592-2』に準拠で分散/復元の安全性を確保**

https://www.nisc.go.jp/active/general/kijun30.html

次頁に抜粋

国の考え

政府機関等の対策基準策定のためのガイドライン

内閣官房 内閣サイバーセキュリティセンター（NISC）が国の行政機関、独立行政法人及び指定法人が政府機関等の情報セキュリティ対策のための統一基準の規定を遵守するための対策事項について、対策基準を策定したガイドライン内に、以下のような記載がされた。　（平成30年度版）

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
例えば、1 個の電子情報について、分割された一方のデータからは情報が復元できない方法でファイルを 2 個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方をDVD、USB メモリ等の外部電磁的記録媒体で郵送する方法が考えられる。

公的機関の考え方

割符の場合

確認している機関：内閣府（大臣官房番号制度担当室）、消費者庁、総務省、金融庁、経済産業省

確認している内容：マイナンバーを含む特定個人情報を秘密分散技術（電子割符）で処理し
生成されたファイル単体（割符）は下記の条件が整えば、個人情報保護法
で定める「個人情報」の定義項から除外される。

条　件：①情報流出は復元に至らない数のファイル単体（割符）のみである
②復元に必要な残りのファイル単体（割符）は適切に管理されている

暗号化の場合（マイナンバーの場合）

確認している機関：個人情報保護委員会

確認している内容：個人番号は、仮に暗号化等により秘匿化されていても、その秘匿化された
ものについては個人番号を一定の法則に従って変換したものであることから
番号法第２条第８項に規定する「個人番号」に該当する。