個人情報配送ソリューション「eすぷりっと便™」

平野　建太郎

業種，業界を問わず，現在さまざまな機密情報が企業間で受け渡しされている。たとえば，商品発送用の住所データ，売上データや取引履歴データ，未発表製品の仕様書，健康診断結果やカルテ等である。これらの情報が，FDやCD等の記録媒体で受け渡される場合に，配送中での「盗難」や「紛失」による情報漏洩事故の報告が増加している。

紛失時の対策として，データを暗号化するケースが一般的だが，果たして十分な対策と言えるであろうか。経済産業省が策定した個人情報保護法に関するガイドラインでは，“「個人に関する情報」は，氏名，性別，生年月日等個人を識別する情報に限られず，個人の身体，財産，職種，肩書などの属性に関して，事実，判断，評価を表すすべての情報であり，～中略～ 暗号化されているかどうかを問わない”[1)] と記載され，暗号化は最終的な情報漏洩対策にはならない。eすぷりっと便™*1) は，情報を複数のデータに分割・暗号化しており，情報の復元には，必要な全ての分割データを揃える必要がある。一片の分割データだけでは，元のデータを復元することができないことにより，高セキュリティが確保できる。

本稿では，eすぷりっと便の概要と活用事例について紹介する。

eすぷりっと便の概要

(1) 情報配送時の課題

企業間で機密情報を受け渡す場合，盗難や紛失による情報漏洩リスクが存在するため，従来は以下のような対策がとられている。

① 施錠されたジュラルミンケースのように，頑丈なケースで情報を格納した媒体を保護し，配送する。
② 媒体に格納する情報を暗号鍵により暗号化し，配送する。
③ 媒体を使用せず，専用線により情報を配送する。

①，②のケースは，ともに「情報が引き出されないように物理的もしくは論理的に鍵をかける」ことによる対策である。鍵は安全に管理され，定期的に交換される必要がある。また，配送は，人手によって行われるため，「紛失」「盗難」などの人為的リスクがある。③のケースは，配送経路で情報が持ち出される危険性が極めて少なく，有効な手段である。しかし，専用線サービスの利用には，通信事業者との年間契約や通信インフラの整備が必要なため，1回きりの配送や，不特定多数宛ての配送には適さない。

(2) eすぷりっと便の基本的なしくみ

eすぷりっと便の基本的なしくみを**図1**に示す。eすぷりっと便では，鍵暗号を使用しない秘密分散法と呼ばれるアルゴリズムを採用し，データを電子割符として取り扱う。

配送手順と特長は，以下のとおりである。

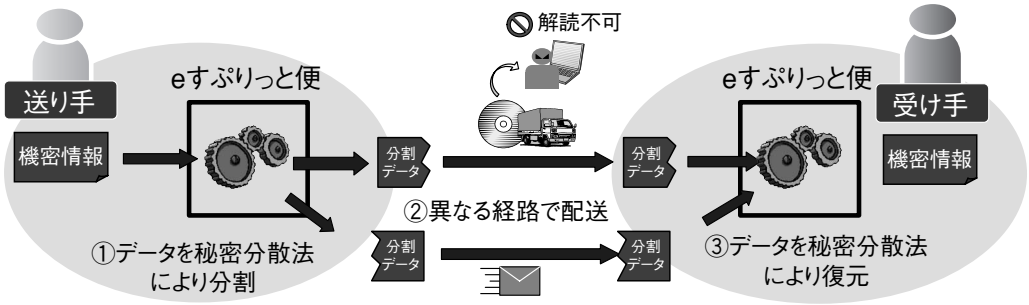

図1　eすぷりっと便の基本的なしくみ

*1)eすぷりっと便は沖電気工業(株)の商標です。また，eすぷりっと便による情報配送方法は特許出願中です。

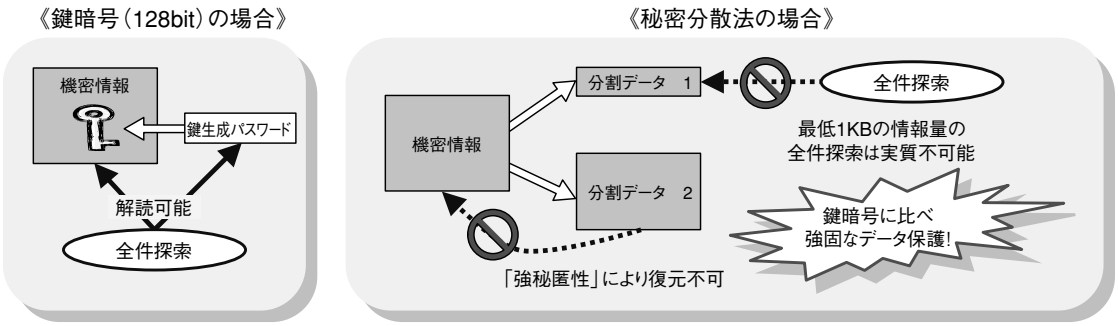

図2　鍵暗号方式との安全性の比較

＜手順＞

手順①において，機密情報を秘密分散法により分割し，
手順②において，分割データを異なる経路で配送し，
手順③において，秘密分散法により機密情報を復元する。

＜特長＞

- 分割データの一片が盗難にあっても，情報の復元ができないため，特別なセキュリティ対策が取られていない一般の宅配便やインターネットを経由した情報の受け渡しが可能となる。
- データ分割には鍵暗号を使用しない。そのため，従来のデータ暗号化対策で必要だった暗号鍵の管理・更新といった運用上の手間が不要となる。
- 生成する分割データのサイズ指定が可能なため，添付ファイルのサイズに上限値が設けられているメールサーバ経由においても，情報を送信することが可能である。

（3）eすぷりっと便と秘密分散法

秘密分散法は，1979年に発表された暗号技術である。従来の暗号方式では，暗号鍵の安全な管理に課題があった。鍵を守るために鍵に別の鍵をかけ，その鍵を守るためにまた別の鍵をかけ，という具合にきりがないからだ。

この課題を解決するための方法として登場した秘密分散法は，「強秘匿性」が数学的に証明されているため，一片の分割データからは平文の一部分すら復元できない（**図2**）。

eすぷりっと便では，秘密分散法の従来仕様に加え，サイズ可変分散方式と呼ばれる分割データのサイズを制御するアルゴリズムを取り込むことで，電子メールに添付できる小さなサイズ（数KB程度）への対応を実現した。

eすぷりっと便のラインナップ

エントリー版，スタンダード版という2つのラインナップを用意している。主な機能を**表1**に示す。

（1）エントリー版（クライアントモデル）

図3（次ページ）に示すエントリー版は，パソコンにインストールしてすぐに利用できるように提供機能をデータ

表1　eすぷりっと便の機能

機能	エントリー版	スタンダード版
データ分割	・手動による分割 ファイルやフォルダを分割ツール上にドラッグ&ドロップして分割。 ・分割サイズの比率指定に対応 分割サイズの比率を1:9、3:7、5:5のいずれかに指定可能。	・アプリケーションによる自動分割 スケジューラにより常駐型アプリケーションが自動分割。 ・分割サイズの比率指定に対応 分割サイズの比率を1:9、3:7、5:5のいずれかに指定可能。
データ配送		・データを自動配送 電子メールやWebによるダウンロード等、事前に指定されたルートに従い、データの自動配送が可能（媒体出力機能はオプション）。
データ復元	・手動による復元 2つの分割データを分割ツール上にドラッグ&ドロップして復元。	・手動による復元 ブラウザ上に分割データをドラッグ&ドロップして復元。 （復元ツールをWebサイトへアクセス時に自動ダウンロード）
取得ログ	・分割／復元ログを取得 分割／復元等の手動操作ログを取得。	・分割／配送／ダウンロードログを取得 自動実行されるデータ分割、メール配送のログを取得する他、Webからのダウンロードログを取得。取得したログは検索画面より検索可。
その他	・合言葉の指定が可能 復元ツールを起動するための合言葉の指定が可能。 ・コマンドによる分割実行が可能 配送データ作成アプリケーション等の外部アプリケーションからコマンド実行することで、処理の自動化が可能。	・合言葉の指定が可能 復元ツールを起動するための合言葉の指定が可能。

の分割・復元のみに絞り込んだ製品である。エントリー版では，画面操作かコマンド処理のいずれかの方法で指定ファイル（フォルダ）から分割データを生成する。配送手段（メール添付，媒体配送等）については，ユーザ自身が選択する。

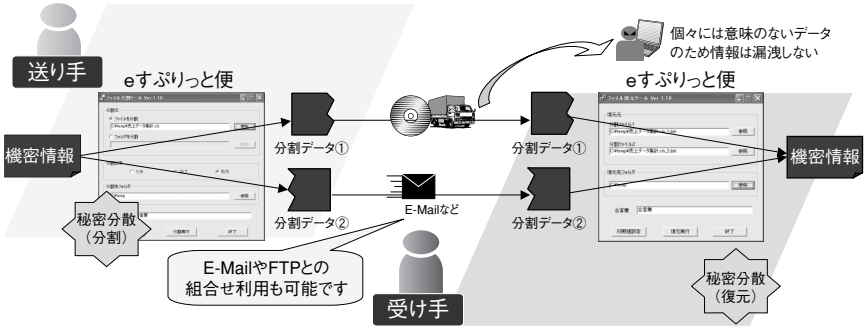

図3　エントリー版（クライアントモデル）

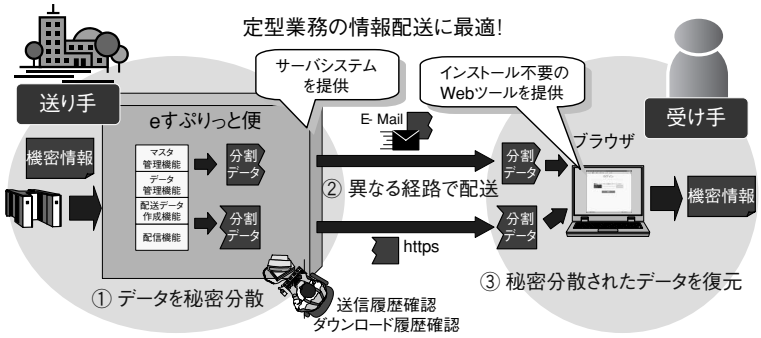

図4　スタンダード版（Webアプリケーションモデル）

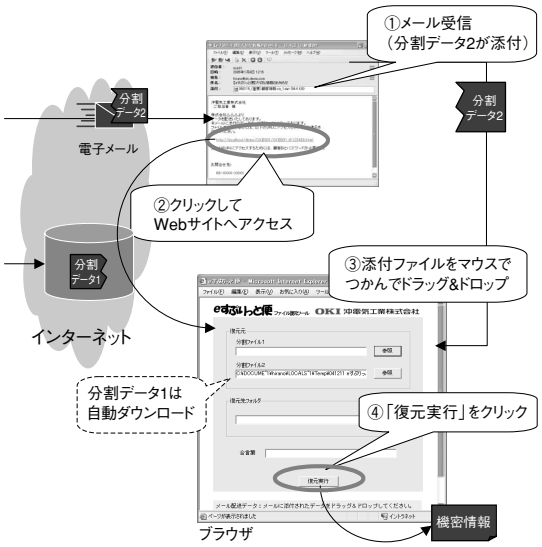

図5　簡易なデータ復元操作

（2）スタンダード版（Webアプリケーションモデル）

図4に示すスタンダード版は，機密情報の受け渡しが定期的・かつ大量に発生する業務システム向けの製品である。データ送信用のeすぷりっと便サーバでは，データの分割・配送を全て自動化することが可能であるため，配送用のデータを出力する既存の業務システムと組合せることで，データの作成から配送までを全て自動化することができる。分割履歴や配送履歴の管理も可能なことから，データ紛失等の問題発生時のトレースも容易である。

データの復元に必要な復元ツールは，ActiveXコンポーネントと呼ばれる配布型のアプリケーションとして提供されるため，利用者は事前のインストールが不要である。ブラウザを起動し指定のURLにアクセスするだけでデータを復元できる。

図5は，電子メールとWebダウンロードによりデータを配送した場合のデータ復元手順である。ブラウザ上への分割データのドラッグ&ドロップ操作だけで，データの復元が可能なため，直感的で分かりやすいものとなっている。分割データの一片をCD-ROMに書き込んで配送する場合は，オートラン機能を利用することで，パソコンへのCD-ROM挿入時にブラウザを自動起動し，残りの分割データにアクセスすることが可能である。

eすぷりっと便の活用事例

図6，**図7**，**図8**および**表2**は，eすぷりっと便の配送業務

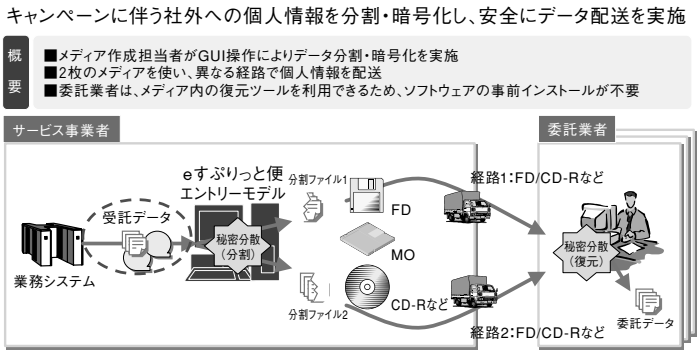

図6　キャンペーンデータ配送業務への適用

eすぷりっと便による自動データ配送に切替え、セキュリティ強化とTCO削減を両立

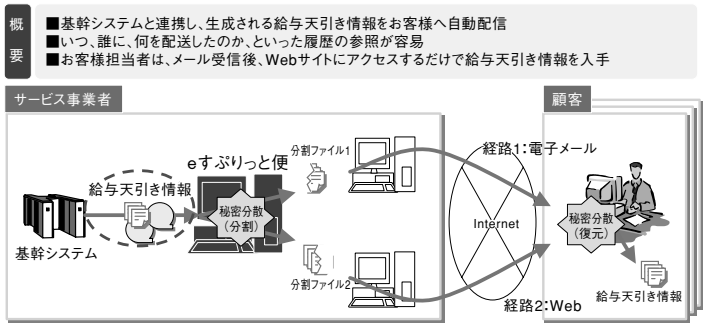

図7　給与天引き情報配送業務への適用

コンバート後のデータを自動分割しメディア出力。業務効率化とデータ保護を実現。

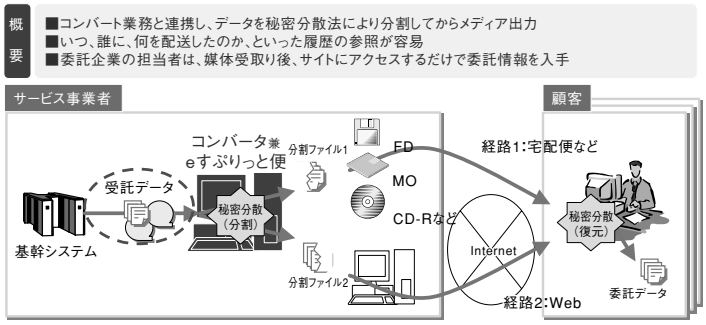

図8　データコンバート業務への適用

への活用事例である。**図7**，**図8**に示す例は，もともと業務システムで生成した配送データを人手で暗号化し，媒体に書き込む運用となっていたが，eすぷりっと便の導入により，配送データの作成→データ分割→データ配送までが全て自動化された。

今後の展望

図9の例は，現在のeすぷりっと便を機能拡張して実現する応用例になる。機密情報を送付したいユーザは，インターネット上のサービスサイトにアクセスし，簡単・安全にデータを送付することができる。受信者についても同様で，インターネットアクセス環境があれば，受信した2つのデータから元のデータを簡単に復元することができる。

この方式によれば，データの送信者と受信者は，いつでも立場を換えることができるため，送信した企画書に沿った設計書を返送させる，等の情報の相互受渡しが必要な業務への拡張が可能である。

本稿では，安全・確実な情報配送を実現するソリューションとして「eすぷりっと便」を紹介した。情報の受け渡しは，企業間の取引や業務委託に伴う情報交換において，欠くことができない。沖電気では，eすぷりっと便を情報配送のためのインフラとして普及させることで，各企業が安心して機密情報を受け渡すことのできる環境作りに貢献したいと考えている。 ◆◆

表2　その他の適用業務例

●業務委託に伴う情報の配送
コールセンタ業務・総務系業務のアウトソースによる、顧客データ・社員データ、パンチ入力業者からの顧客データ
明細書・取引報告書・請求書などのプライベートな内容を含む印刷物のデータ、印刷物・ダイレクトメールの送付先データ
取引データ
検査データや、調査レポート等の機密情報
●長期保管データの配送
伝票書類や取引データなどの倉庫保管データ
●製造業における商品データの配送
新製品の企画書・仕様書・設計図面・デザインの写真など
中国などの製造拠点への設計書・生産計画情報など
●医療情報（カルテ・画像データ）の配送
電子カルテや、CT・MRIなどの画像情報

■参考文献

1）個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン，経済産業省，平成16年6月

●筆者紹介

平野建太郎：Kentaro Hirano. ネットビジネスカンパニー ソリューションコンサルティング部 ソリューションコンサルティング第二チーム

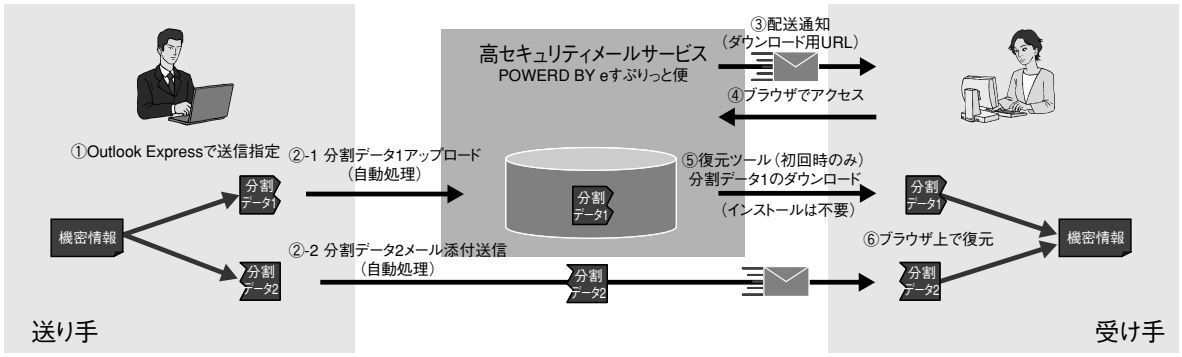

図9　スタンダード版　双方向モデル